



Control Bar and Digistat® Environment

DIGISTAT® Version 5.0

USER MANUAL

DIG UD CBR IU 0006 ITA V01

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® 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® 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.

DIGISTAT® product is  marked according to 93/42/CEE directive (“Medical devices”) amended by the 2007/47/EC directive.

ASCOM UMS is certified according to UNI EN ISO 9001:2015 and UNI CEI EN ISO 13485:2012 standards for “Product and specification development, manufacturing management, marketing, sales, production, installation and servicing of information, communication and workflow software solutions for healthcare including integration with medical devices and patient related information systems”.

Contents

1. Using the manual	6
1.1 Aims.....	6
1.2 Characters used and terminology	7
1.3 Symbols.....	8
2. Introduction to DIGISTAT®	9
2.1 Modular Architecture.....	9
2.2 Intended use.....	9
2.2.1 Safety Advisories	11
2.3 “Off-label” use of the Product	12
2.4 CE mark and regulation conformity.....	12
2.5 Manufacturer’s responsibility	13
2.6 Product traceability	13
2.7 Post-market surveillance	14
2.8 Product life	14
3. Software/Hardware specifications	15
3.1 Central & Bedside	15
3.1.1 Hardware	15
3.1.2 Operating System	15
3.1.3 System Software.....	15
3.2 Server	15
3.2.1 Hardware	15
3.2.2 Operating System	16
3.2.3 System Software.....	16

3.3 DIGISTAT® Mobile	16
3.4 DIGISTAT® Web	16
3.5 General Warnings.....	17
3.6 Firewall and Antivirus	18
3.7 Local network features.....	19
3.7.1 DIGISTAT® system impact on the healthcare facility network	19
4. Before starting.....	21
4.1 Installation and maintenance warnings.....	21
4.1.1 Patient Area	22
4.2 Cleaning.....	23
4.3 General precautions and warnings.....	23
4.3.1 Electrical safety	24
4.3.2 Electromagnetic compatibility.....	24
4.3.3 Devices eligibility.....	24
4.4 Privacy Policy.....	25
4.4.1 User credentials features and use.....	26
4.4.2 System administrators.....	27
4.4.3 System logs.....	28
4.5 Backup policy	28
4.6 Out of order procedure.....	29
4.6.1 Reconfiguration/substitution of network equipment.....	30
4.7 Preventive maintenance	31
4.8 Compatible devices	34
4.9 System unavailability	34
5. “Control Bar” and DIGISTAT® environment.....	35

5.1 Introduction.....	35
5.2 Touch screen.....	35
5.3 Launching DIGISTAT®	36
5.4 DIGISTAT® Work Area.....	36
5.4.1 Selecting a module	37
5.5 Accessing the system	38
5.5.1 Disabling the automatic log out	39
5.5.2 Recent users.....	40
5.5.3 How to use the “User List”	41
5.6 DIGISTAT® Control Bar	42
5.6.1 How to read the “Patient” button	43
5.7 Help	44
5.8 DIGISTAT® Main Menu.....	45
5.8.1 Patient reports.....	48
5.8.2 Print reports	48
5.8.3 Statistics.....	55
5.8.4 Change password.....	57
5.8.5 About DIGISTAT®	59
5.8.6 Quit DIGISTAT®	60
6. Manufacturer Contacts	62
7. Residual risks	63

1. Using the manual

1.1 Aims

The effort which has gone into creating this manual aims to offer all the necessary information to guarantee a safe and correct use of the DIGISTAT® system and to allow the manufacturer identification. Furthermore, this document aims to describe every part of the system, it also intends to offer a reference guide to the user who wants to know how to perform a specific operation and a guide for the correct use of the system so that improper and potentially hazardous uses can be avoided.

The use of DIGISTAT® requires a basic knowledge of information systems concepts and procedures. The comprehension of this manual requires the same knowledge.

Always remember that DIGISTAT® systems are highly configurable, in order to satisfy the requirements of every user. This flexibility makes it difficult to provide a description of all the system's possibilities. Hence the manual describes "probable", or "standard" configuration, in an effort to explain the fundamental parts of the system, and their purposes. Consequently, the user may come across descriptions of screens and functions that differ from their actual configuration.

To be more precise, the differences may concern

- The appearance of the screen (a screen may appear different from that shown here).
- The functions (certain operations may or may not be enabled).
- The flow of use (certain procedures can be performed following a different sequence of screens and actions).

Specific warnings are provided when the configuration options allow multiple possibilities.

Should more details regarding a specific configuration be required, please contact your system administrator or the ASCOM/Distributor technical support service.

1.2 Characters used and terminology

The use of DIGISTAT® systems requires a basic knowledge of the most common IT terms and concepts. In the same way, understanding of this manual is subject to such knowledge.

Remember that the use of DIGISTAT® systems must only be granted to professionally qualified and properly trained personnel.

When consulting the online version as opposed to the paper version, cross-references in the document work like hypertext links. This means that every time you come across the reference to a picture (e.g. “Fig 6”) or to a paragraph / section (e.g. “Paragraph 2.2.1”), you can click the reference to directly go to that particular figure or that particular paragraph / section.

Every time a reference is made to a button, this is written “**Bold**”. For example, in expressions like:

➤ Click the “**Update**” button,

“**Update**” is a button featured on the screen being described. Where possible, it is clearly indicated in a figure (with cross references as “See Fig 6 **A**”).

The character ➤ is used to indicate an action which the user must perform to be able to carry out a specific operation.

The character ● is used to indicate the different elements of a list.

1.3 Symbols

The following symbols are used in this manual.



Useful information

This symbol appears alongside additional information concerning the characteristics and use of DIGISTAT® Systems. 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

2. Introduction to DIGISTAT®

The DIGISTAT® clinical modules suite is an advanced patient data management software system that is designed specifically for use by clinicians, nurses and administrators.

The software package consist of a set of modules that can either work alone or be fully integrated to provide a complete patient data management solution.

From the Intensive Care Unit to the Ward, from the Operating Room to the Administrative Department, DIGISTAT® systems can be used in a wide range of environments.

DIGISTAT®'s modular architecture and extensive configuration capabilities allows the patient data management system to be tailored to organizational needs and adaptable to meet new demands when required.

DIGISTAT® system can only be accessed by entering username and password. Every user is defined by a detailed profile and can access only the allowed areas. An audit trail of every login performed is automatically generated by the system.

2.1 Modular Architecture

“Modular Architecture” means that different products (or modules) can be implemented within the same software environment (DIGISTAT® in the present case) that is characterized by a consistent user interface, same overall goals and terms of use.

Modules can be added at different times, and in a way that is agreed with the user. The resultant software suite fits the specific user needs and can change in time, according to the possible changes in the user needs.

2.2 Intended use

The DIGISTAT Software (hereafter “Product”) acquires records, organizes, transmits and displays patient information and patient related data, including data and events from connected clinical devices and systems as well as information entered manually, in order to support caregivers in diagnosis and treatment of patients as well as to establish electronic patient records.

- The Product produces configurable electronic patient records based on acquired data and information, as well as on manual and automated documentation of the clinical unit's activity.
- The Product provides automated, secondary visual and audible announcing and displaying of acquired data, events, current status and operating conditions of connected clinical devices and systems on designated display device(s). The Product can also be configured to forward data and

information about events, statuses and operating conditions to the ASCOM messaging system.

- The Product supports the improvement of nursing workflows related to the management of alarms from the connected clinical devices and systems.
- The Product supports the documentation of the prescribed therapy, its preparation and its delivery.
- The Product supports the recording, validation and display of vital signs charting based on the acquired data and information.
- The Product provides configurable reports, charts and statistics based on recorded data for use by healthcare professionals to analyze the unit's efficiency, productivity, capacity and resource utilization, and the quality of care.

The Product **does not** replace or replicate the original display of data and alarms of the connected devices and systems and **does not** control, monitor or alter the behavior of these connected devices and systems, or their associated alarms.

The Product **is not** intended to be used for direct diagnosis or monitoring of vital physiological parameters.

The Product is intended for use by trained healthcare professionals within a Healthcare Structure environment and relies on proper use and operation of the IT and communication infrastructure in place at the healthcare facility, the display devices used and the connected clinical devices and systems.

Additionally, the Product provides specific functions and interfaces intended to be used by non-professional users in remote locations for non-clinical purposes for display of information, reports, charts and statistics, without the ability to add, change or delete any information or data.

The Product is a stand-alone software that is installed on servers and computers, which must comply with the technical hardware and software specifications provided with the Product.

2.2.1 Safety Advisories

The Product, even if designed to provide very high accuracy, cannot guarantee the complete and correct communication of the acquired data, nor can it substitute the direct verification of the same by the User.

The User shall base therapeutic or diagnostic decisions and interventions solely on the direct examination of the original source of information. The user has sole responsibility to check that the information displayed by the Product is correct and to make appropriate use of it.

In any case, the Product must be used in compliance with the safety procedures reported in the user documentation accompanying the Product.

Only printouts that are signed with digital or ink signature by authorized medical professionals shall be considered valid clinical records. In signing the aforementioned printouts, the User certifies they have checked the correctness and completeness of the data present in the document.

Only these signed documents are a valid source of information for diagnostic or therapeutic processes and/or procedures.

The Product can be used in the proximity of the patient and to the connected clinical devices in order to speed up the data entry, to reduce the probability of errors and to allow the User to verify the correctness of the data through the immediate comparison with the actual data and activities.

When entering patient related data the User shall verify that the patient identity, Healthcare Facility department/care unit and bed information displayed in the Product are correct. This verification is of utmost importance in cases of critical interventions, for instance, drug administration.

The Healthcare Facility must establish and implement appropriate procedures to ensure that potential errors occurring in the Product and/or in the use of the Product are promptly detected and corrected and do not constitute a risk to the patient and the User. These procedures depend on the configuration of the Product and the method of use preferred by the Healthcare Facility.

The Product may provide, depending on the configuration, access to information on drugs. The Healthcare Facility shall, initially and periodically, verify that this information is current and updated.

The Product must not be used in place of the direct monitoring of the alarms generated by the medical devices. This limitation is due, among the other reasons, to the specifications and limitations of the communication protocols of the medical devices.

Where devices used with the Product are located in the patient area or are connected to equipment present in the patient area then the Healthcare Facility shall ensure that

the whole combination complies with the international standard IEC 60601-1 and any additional requirement(s) established by the local authorities.

Use of the Product must be granted, by means of specific configuration of the passwords and active surveillance, only to User who are:

- trained according to Product indications by personnel authorized by the manufacturer or distributors and
- in possession of the professional qualifications to correctly interpret the information supplied and to implement the appropriate safety procedures.

The Product is a stand-alone software that can run on standard computers and/or standard mobile devices connected to the Healthcare Facility local network. The computers, devices and the local network shall be adequately protected against cyber-attacks.


The Product shall be installed only on computers and devices fulfilling the minimum hardware requirements and on supported operating systems.

2.3 “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 Facility.

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”.

2.4 CE mark and regulation conformity

ASCOM UMS DIGISTAT® product is  marked according to 93/42/EEC directive (“Medical devices”), amended by the directive 2007/47/EC, and is therefore compliant with the EU basic safety standards there specified (received in Italy with Legislative Decree n. 37/2010 and subsequent variants and integrations).

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 Facility 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 (e.g. in Italy Dlgs. no. 81/2008) and any additional local site safety.

The ASCOM UMS 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.

2.5 Manufacturer's responsibility

The **CE** Marking is a declaration that the Product complies with the applicable Directives and Regulations.

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 formed and authorized by ASCOM UMS ;
- The Product's usage environment complies with safety regulations;
- The electrical wiring of the environment where the Product is used complies with applicable regulations and is efficient.




Should the electrical supply cause the establishment of a “medical electrical system” through electrical and functional connection of devices, the healthcare facility is in charge of the required safety verification and acceptance tests, even where ASCOM UMS performed in whole or in part the wiring and the necessary connections.

2.6 Product traceability

In order to ensure device tracking and ongoing safety and efficiency checks on site, in compliance with ISO 9001 and EN 13485 quality standards and European law on medical devices 93/42/EEC, amended by the directive 2007/47/EC, the former Product owner is recommended 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 (either paper label provided at installation time or “About box” displayed within the product – see paragraph 5.8.5). In case of doubts/questions about product labeling and/or product identification please contact ASCOM UMS/Distributor technical assistance (for contacts see section 6).

2.7 Post-market surveillance

The  marked 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's health or to environmental safety, the User must immediately give notice to either ASCOM UMS, one of its branches or nearest authorized dealer.

The product details can be found on its labeling.

On reception of a user feedback ASCOM UMS will immediately start the review and verification process and, when required, solve the reported nonconformity.

2.8 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 hardware (computer and server) and is therefore assessed as 5 years since the release date of the Product version. During this period, Ascom UMS is committed to fully support the Product.

3. Software/Hardware specifications

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. If explicitly requested, ASCOM UMS is able to provide information on appropriate devices.

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 x86/x64 Professional
- Microsoft Corporation Windows 10

3.1.3 System Software

- Microsoft .NET Framework v4.6.2 full version (if FluidBalance or ImageBank is going to be installed)
- Microsoft .NET Framework v4.0 full version (if FluidBalance or ImageBank is not going to be installed)

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
- Microsoft .NET Framework v4.6.2 full version (if FluidBalance or ImageBank is going to be installed)
- Microsoft .NET Framework v4.0 full version (if FluidBalance or ImageBank is not going to be installed)

3.3 DIGISTAT® Mobile

DIGISTAT® 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/Distributor for the full list of devices that support DIGISTAT® Mobile.

3.4 DIGISTAT® Web

The following browsers are supported for use with DIGISTAT® web applications:

- Chrome 63
- Firefox 56
- Edge 41
- Internet Explorer 11



Only supported Web Browsers shall be used for Digistat Web.



A Digistat Web workstation shall always have the Web Browser in foreground. Besides, the Web Browser shall never be used for anything else but Digistat Web (which also implies that the Digistat Web homepage shall be the default homepage of the Web Browser).



The Browser's Display Scaling shall always be set to 100%.



When the local network is at least partially based on WiFi connections, given the intermittent nature of WiFi connections, disconnects could occur which activate the Disconnected Mode (grey carpet covering Digistat Web) and thus the system may not be available. The healthcare structure must work to ensure optimal WiFi coverage and instruct the staff on how to handle these temporary system outages

3.5 General Warnings



To correctly use DIGISTAT®, 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® system 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® system 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 Structure shall implement for the DIGISTAT® workstations a date/time synchronization mechanism to a reference source.

3.6 Firewall and Antivirus

To protect the DIGISTAT® system 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 Facility shall ensure that these two protections are activated. ASCOM UMS tested the Product with ESET Antivirus but, considering the strategies and policies already existing in the healthcare facility, the actual choice of the antivirus is left to the Healthcare Facility. ASCOM UMS cannot ensure that the DIGISTAT® system is compatible with any antivirus or antivirus configuration.



Some incompatibilities have been reported between parts of DIGISTAT® 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 system configuration. Please refer to the ASCOM UMS technical assistance for more information.

3.7 Local network features

This section lists the features of the local network on which DIGISTAT® system is installed in order to guarantee the system's full functionality.

- DIGISTAT® system uses a TCP/IP traffic protocol.
- The LAN must not be congested and/or full loaded.
- DIGISTAT® system 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 facility in managing the possible disservices caused by maintenance activities.



If the network does not match the requested features, DIGISTAT® system performance gradually deteriorates until timeout errors occur. The system 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 system unavailability. The Healthcare Facility shall ensure an optimal network coverage and stability, and train the personnel in the management of these temporary disconnections.

3.7.1 DIGISTAT® system impact on the healthcare facility network

DIGISTAT® system impacts the local network of the healthcare facility. This section provides information on the traffic generated by the DIGISTAT® system on the network in order to make it possible for the structure to evaluate and analyze the risks related to the introduction of the DIGISTAT® system.

The bandwidth used by a DIGISTAT® system 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® system configuration and mode of use.

DIGISTAT® bandwidth occupation depends mainly on data acquisition from medical devices. 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® workstations covering 10 beds each, the following bandwidth occupation values can be indicatively predicted:

Average: 0.8 – 6 Mbit/s

Pitch: 5 – 25 Mbit/s

In case of DIGISTAT® configurations with no acquisition from medical devices, bandwidth occupation values are lower than those specified above.

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® product. They must be strictly respected.

DIGISTAT® system must be installed and configured 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® system 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® system must be installed and configured 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 system according to the instructions present in this manual and those provided with the third party devices.
- The DIGISTAT® USB dongle 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 1) it is recommended to use washable waterproof of devices.
- Within the "Patient Area" (see Fig 1) 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).

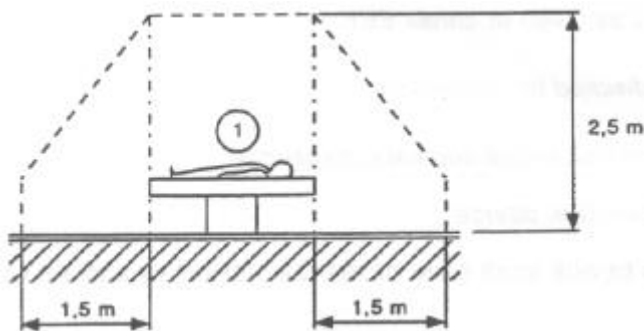
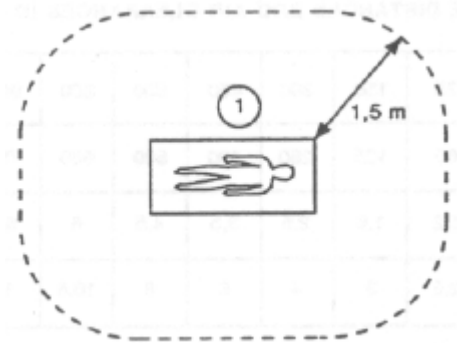


Fig 1 - Patient Area



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 Facility (individual or institution) 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 Facility 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 facility adopts for all the healthcare facility's equipment (both fixed and moveable).



Check the suggested cleaning procedures in the manuals of the hardware products that are used alongside the DIGISTAT® system.

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, thus jeopardizing patient data management system functions.



The Healthcare Facility 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® system must comply with the relevant **CE** mark prescriptions, in particular with those indicated by the 2006/95/EC directive and subsequent amendments.

The device complies with the characteristics envisaged by the **CE** marking in accordance with directive 2006/95/EC and subsequent amendments.



The electrical devices installed within the Patient Area (see Fig 1) must have the same security level of an electro-medical 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 facility is responsible for these measurements.



The healthcare facility 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 the DIGISTAT® system must comply with electromagnetic emission and immunity characteristics envisaged by the **CE** seal, in compliance with Directive 2004/108/EC and following amendments.

4.3.3 Devices eligibility

It is mandatory to use devices that are suitable for the environment in which they are installed and used (meeting, for instance, the directives LVD 2006/95/EC, EMC 2004/108/EC, penetration by liquids, etc.).

4.4 Privacy Policy

The following 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.



“Sensitive data” is personal data that reveal the race, the religious and/or philosophic beliefs, the personal political opinions, the support to political parties and/or trade unions and/or associations and organizations having political, religious or philosophical aims. Moreover, “sensitive data” is data providing information on the health conditions and/or the sexual life of individuals.



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. See paragraph 5.5 for log out procedure.
 - Sensitive data saved in the system, 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 facility is responsible for implementing this software and keep them updated.
 - The user is advised against the frequent use of the lock function (paragraph 5.5.1). Automatic log out protects the system from unauthorized accesses.
-



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.



In some circumstances, personal and/or sensitive data 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 facility is responsible for providing adequate security measures to comply with the local privacy laws and regulations.

4.4.1 User credentials features and use

This section explains the DIGISTAT® 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 the system (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® configuration 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 paragraph 5.8.4 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® configuration manual.

The following information is reserved to system administrators:

The password must match a regular expression defined in the DIGISTAT® 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 system. 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® configuration 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 and deal with personal sensitive data stored in the DIGISTAT® database.

For issues relating to management of personal sensitive data, ASCOM UMS/Distributor adopts procedures and working instructions complying with the current privacy regulation (D.Lgs 196/2003 of the 30th of June 2003).

In performing the above mentioned activities ASCOM UMS/Distributor technical staff are setup as "System Administrator" for the DIGISTAT® system (see regulation of

25/11/2008 of the Privacy Guarantor on “System Administrators”). ASCOM UMS/Distributor staff performing this kind of procedures are appropriately trained on privacy issues and, in particular, in sensitive data treatment issues.

In order to comply with the requests of the “System Administrators” regulations, the Healthcare Facility must:

- define nominal accesses;
- activate the access logs both at operating system and at client and at server level;
- activate the access logs to the database server Microsoft SQL Server (Audit Level);
- configure and manage all these logs to keep track of the accesses for at least one year.

4.4.3 System logs

DIGISTAT® 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® configuration manual for the configuration procedures.

4.5 Backup policy



It is recommended to regularly perform system backups.

The Healthcare Facility using DIGISTAT® system 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 Facility 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 Facility must protect these devices from unauthorized access. When these devices are not used anymore, they must be either securely deleted or destroyed.

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® 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 facility has substitute equipment and an additional PC on which DIGISTAT® is already installed.

In case of a DIGISTAT® workstation is out of order, the substitute equipment can promptly replace the DIGISTAT® workstation.

Always remember that DIGISTAT® 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 facility staff are not authorized to perform installation procedures and/or to modify DIGISTAT® configuration.

The risk related to the DIGISTAT® 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® 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® 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® workstation needs to be deactivated and replaced, the Healthcare Facility staff must promptly call ASCOM UMS (or authorized Distributors) and request the execution of this task.

ASCOM UMS suggests the healthcare facility 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 facility has one or more substitution equipment with all the necessary applications already installed (OS, firewall, antivirus, RDP, ...) and with DIGISTAT® system already installed, but disabled (i.e. not executable by a user without the assistance of an ASCOM UMS technician). In case of out of order of a DIGISTAT® 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® workstation we suggest to adopt the following procedure if a “substitution equipment” is available:

- 1) The healthcare facility’s authorized staff replaces the out of order PC with the “substitution equipment”
- 2) The healthcare facility 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 instruction on how to enable/disable and replace a DIGISTAT® workstation, reserved to system administrators, is in the DIGISTAT® configuration 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® data acquisition, the healthcare facility staff must promptly call ASCOM UMS/Distributor and schedule the substitution/reconfiguration procedure to allow ASCOM UMS staff to either reconfigure DIGISTAT® or provide all the necessary information to the healthcare facility. 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® configuration 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® system 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.

This is the maintenance checklist:

Preparatory checks

- DIGISTAT® system update necessity check.
- Check minimum requirements for a possible DIGISTAT® 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® 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 facility 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® 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® installation language.
- Check if every workstation has a default printer.

DIGISTAT® system

- 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.

Connection to devices

- Check the connections (cables and wiring system) with data acquisition devices.

Instruction for use

- Check that the user documentation in PDF format (PDF provided together with the product) is present on the server and appropriate with DIGISTAT® version.
- Check that the folder containing the user documentation in electronic format on the server is accessible to DIGISTAT® 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® system are updated.

4.8 Compatible devices

Please contact ASCOM UMS/Distributor for the list of available drivers.

4.9 System unavailability

If during start up there are problems connecting to the server the system provides a specific information message.

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 6 for the contacts list).

In rare, often extreme cases, it may be physically impossible to use the DIGISTAT® system, for example cases of natural disasters, or long black outs.

It is responsibility of the healthcare facility using DIGISTAT® 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 system to full availability (back-up policy is part of this management. See paragraph 4.5).



It is responsibility of the healthcare facility using DIGISTAT® to define an emergency procedure to put into effect in case of system unavailability.

ASCOM UMS/Distributor offers full support for the definition of such procedure. See section 6 for the contacts list.

5. “Control Bar” and DIGISTAT® environment

5.1 Introduction

This section of the manual describes the features and functions of the DIGISTAT® environment. This section describes the functions that apply across the DIGISTAT® systems. They are generally independent from the specific modules installed.

Please remember that DIGISTAT® is a software environment that, depending on the modules that are actually implemented, can be used in different areas of the healthcare facility, such as intensive care, operating rooms, outpatients departments etc., and for different goals.



The workstation, patient and bed must be checked before each critical operation, e.g. drug administration and, in general, patient data entry

5.2 Touch screen

DIGISTAT® can run both on touch and non-touch workstations. The same procedures can be performed using fingers or mouse device. In this manual “mouse”, terminology is used throughout, with terms as “click” instead of “tap”, for instance. Here is a quick translation table making it possible to apply this manual to all kinds of workstations and user preferences. When specific gestures can be applied to specific screens/functionalities, it will be highlighted in the relevant context. In general, the main actions can be translated this way:

Mouse	Touch Screen
Click	Tap
Double click	Double tap
Drag	Flick
Use scrollbars	Scroll
Zoom in	Two fingers tap

5.3 Launching DIGISTAT®

To launch DIGISTAT®:

- Double click the desktop icon (Fig 2)



Fig 2

The following splash-screen appears while the system is loading.



Fig 3

5.4 DIGISTAT® Work Area

The DIGISTAT® Work Area is defined and enclosed by Control Bar, a tool that is common to all DIGISTAT® installations (Fig 4).

Control Bar manages the installed modules and systems, the patients, the users. The DIGISTAT® Control Bar is formed by a horizontal command bar (Fig 4 **A**), by a vertical selection bar on the left ("Lateral Bar" - Fig 4 **B**) and by a central Work Area. The different screens of the installed modules are displayed within the Work Area (Fig 4 **C**).

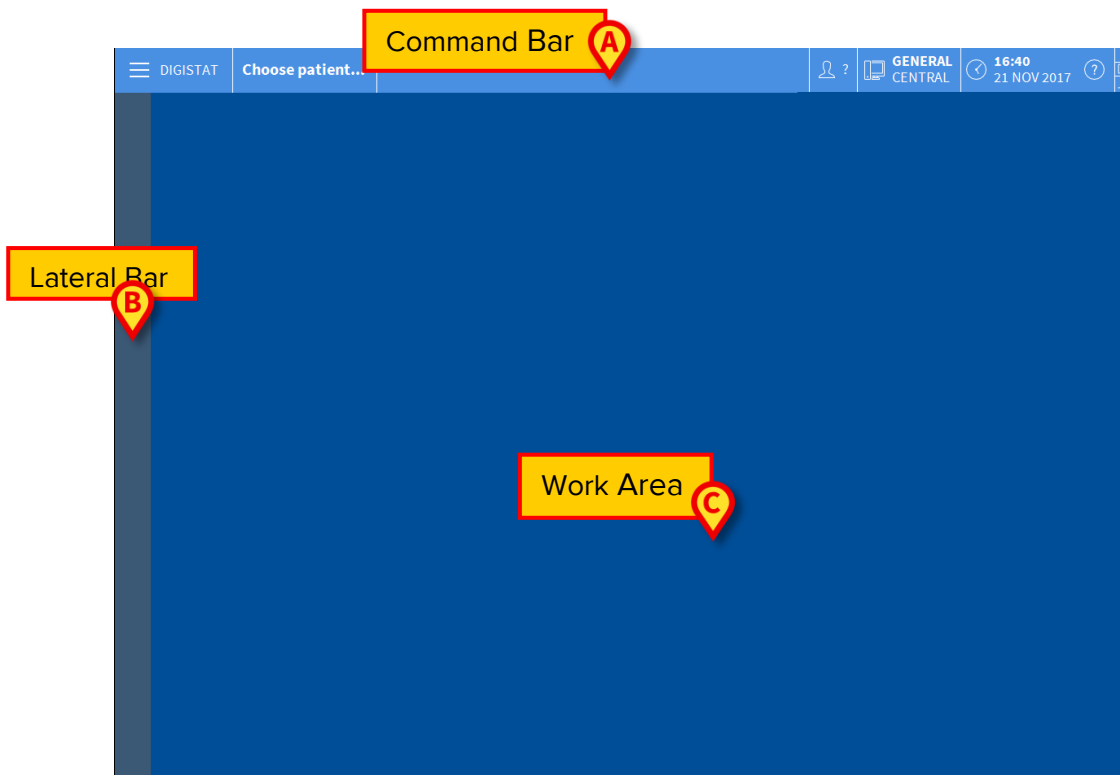


Fig 4

The command bar (Fig 4 **A**) will be described in paragraphs 5.4.1 and beyond.

The lateral bar displays the icons of the currently available modules. See Fig 5.



Fig 5

The module currently selected is highlighted.

5.4.1 Selecting a module

To select a module:

- Click the corresponding icon in the lateral bar

The icon will be highlighted and the module's functionalities will be displayed within the Work Area.

It is only possible to select a specific module after the user log in (see next paragraph).

5.5 Accessing the system

The DIGISTAT® system must be accessed by entering the username and password (“Log in” procedure).

For this reason, at the beginning of every work session, it is necessary to click the **User** button (Fig 6 **A**).

The following screen is displayed.

The screenshot shows the DIGISTAT login interface. At the top, a blue header bar contains a menu icon, the text 'DIGISTAT', a 'Choose patient...' button, and a 'GENERAL CENTRAL' button (callout A). To the right of the header, the date and time '16:50 21 NOV 2017' are displayed. Below the header, there are two input fields: 'USERNAME' (callout B) and 'PASSWORD' (callout C). A virtual keyboard is positioned below the input fields. At the bottom of the screen, there is a 'RECENT' section with a table of login attempts. The bottom bar contains four buttons: '+ MORE...', 'LOCK', 'X CANCEL' (callout E), and '✓ OK' (callout D).

RECENT				
1	ADMIN ASCOM	2		3
4		5		6
7		8		9
10		11		12

Fig 6

To access the system:

- Enter your username in the “**Username**” field (Fig 6 **B**)
- Enter your password in the “**Password**” field (Fig 6 **C**)
- Click the **Ok** button (Fig 6 **D**)

The user is this way logged in. To cancel the operation:

- Click the **Cancel** button (Fig 6 **E**)



The username and password are issued by the system administrator. If you do not have a username and a password you are not authorized to use the DIGISTAT® system.

The user can enter your username and password using either the virtual keyboard displayed on screen (clicking the letters with the mouse or touching them if using a touch screen) or the workstation keyboard.

After accessing the system, an acronym corresponding to the logged user appears on the **User** button on the control bar (the acronym is ADM in Fig 7 A).



Fig 7



The user whose credentials are displayed on the User button is responsible for all the actions performed on DIGISTAT® system. It is strongly recommended to log out before leaving the DIGISTAT® workstation to avoid improper use of the system.

To log out, click the **User** button during the work session. When this button is clicked, the user is disconnected and the acronym of the user disappears from the button.

To log in again, click the **User** button again. The screen shown in Fig 6 will appear again.

DIGISTAT® does not support the Microsoft® Windows® “switch user” functionality.

This means that, for instance, if



- a) User 1 launches DIGISTAT®,
- b) User 1 switches to User 2 without logging out User 1,
- c) User 2 attempts to launch DIGISTAT® again,

Then the second DIGISTAT® instance cannot be launched because the first one is still running.

5.5.1 Disabling the automatic log out

If the system is not used, or remains idle for a certain length of time, the user is automatically disconnected (automatic log out). This length of time depends on a configuration parameter.

To stop automatic log out from happening the user must click the lock button after entering the username and password but before clicking **Ok** (Fig 8 **A**).



Fig 8

If the user is locked, a padlock is shown at the bottom of the user icon (Fig 9).



Fig 9



The user is advised against the frequent use of the lock function. Automatic log out is implemented to protect the system from unauthorized accesses.

5.5.2 Recent users

The “Recent” area of the “Login” screen (Fig 10 **A**) displays the names of users who have accessed the system recently.

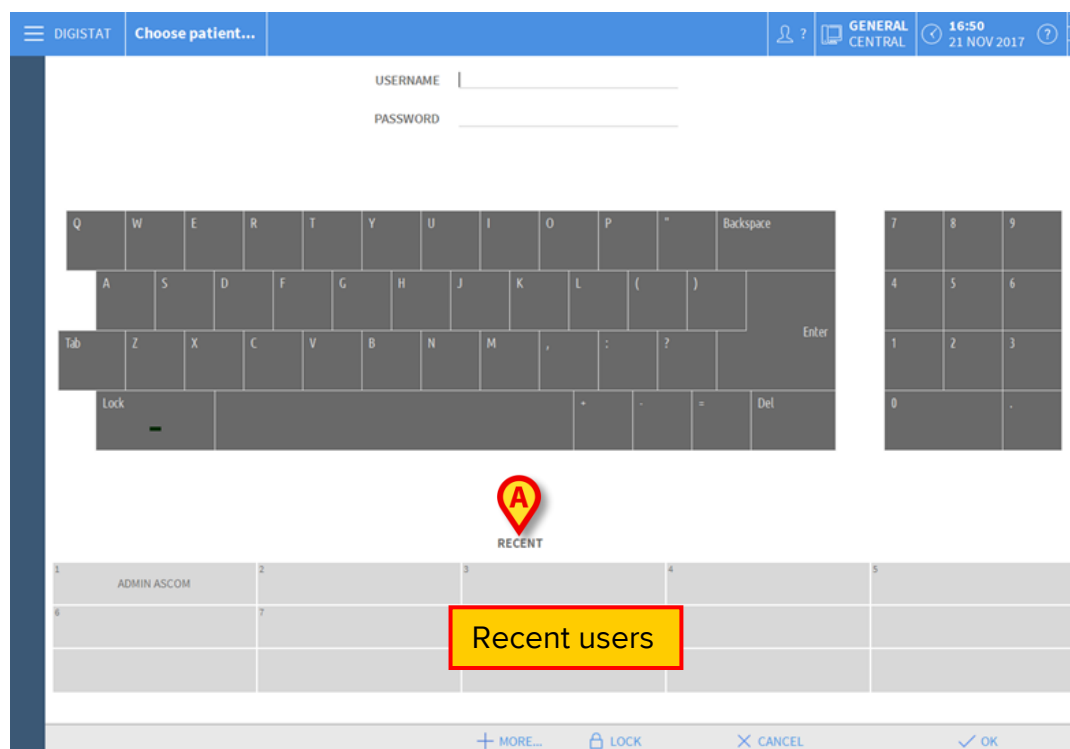


Fig 10

The area is divided into rectangles. The names of the users who accessed the system recently appear inside the rectangles. When any of these rectangles is **clicked**, the “Username” field is automatically filled with the name appearing inside the rectangle.

5.5.3 How to use the “User List”

The **More** button on the control bar (Fig 11) makes it possible to display the complete list of possible users.

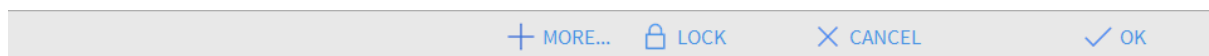


Fig 11

To display the “User List”:

- Click the **More** button

The following window is displayed (Fig 12).

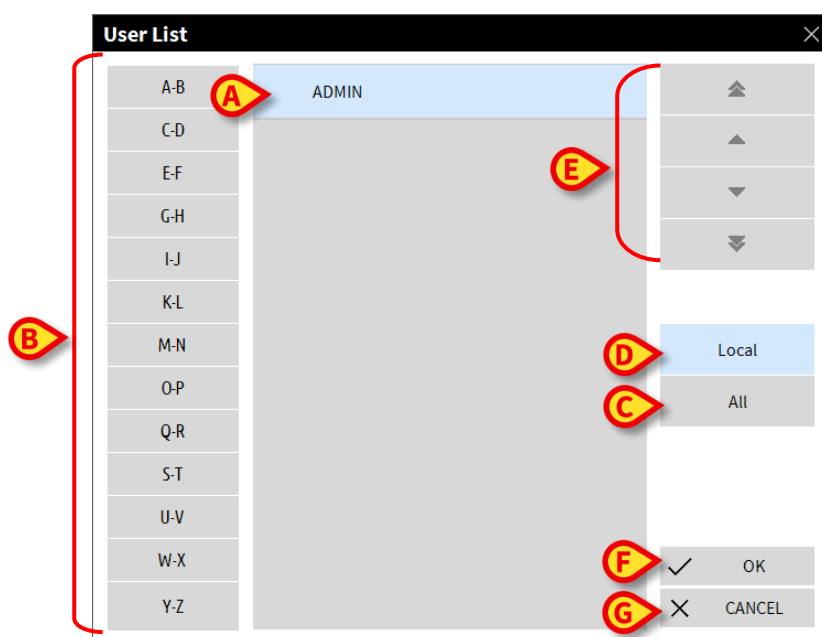


Fig 12

The window shown in Fig 12 can be used as an index book enabling the search and selection of a user in the list of all the possible users.

The central part of the window shows the names of possible users, in alphabetical order (Fig 12 **A**).

The letters on the left side of the window (Fig 12 **B**) work like an index and make it possible to see only the users whose names begin with a specific letter.

For example: click the **C-D** button to see the list of patients whose names begin with the letters C or D.

Use the **All** button (Fig 12 **C**) to see the list of all possible users.

Use the **Local** button (Fig 12 **D**) to see the list of users relating to the specific workstation on which you are currently working.

Use the arrows on the right side of the window (Fig 12 **E**) to scroll up and down the list of users.

To select a user:

- **Click** the name of the user

The name will be highlighted, then

- Click the **Ok** button (Fig 12 **F**)

Otherwise, you can:

- **Double-click** the row displaying the name of the user

After selection, the “**User list**” window closes and the name of the selected user appears in the “**Username**” field on the “**Login**” screen (Fig 6 **B**).

Use the **Cancel** button (Fig 12 **G**) to cancel the operation and close the “User list” window without selecting any user.

5.6 DIGISTAT® Control Bar

The control bar that appears in the lower part of the screen is common to all DIGISTAT® modules. Its main characteristics are listed below, with more detailed explanation of its functionalities provided in the following sections.

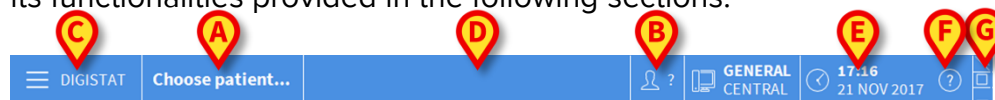


Fig 13

- The **Patient** button (Fig 13 **A**) will contain, after a patient has been selected, the patient's name and, if the patient has been admitted, their bed number.
- The **User** button (Fig 13 **B**) shows the name of the user connected.
- Use the **Menu** button (Fig 13 **C**) to open the following window (Fig 14).

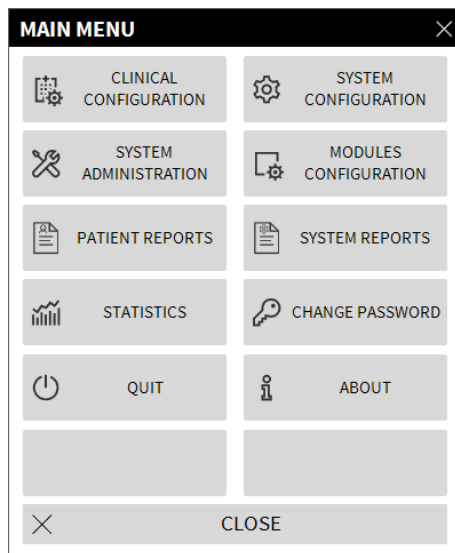


Fig 14

The buttons contained in this window give the user access to functionalities that will be described later.

- The button indicated in Fig 13 **D** is used by the Product to signal that there are notifications for the user.
- Date - time indication (Fig 13 **E**).
- Use the Help button (Fig 13 **F**) to access the online documentation available.
- The small buttons highlighted in Fig 13 **G** can be used to:
 - 1) minimize the DIGISTAT® window;
 - 2) select the full-screen display mode;
 - 3) select the window display mode;



These three buttons are present only if enabled by configuration.

5.6.1 How to read the “Patient” button

Patient selected

When a patient is selected, the **Patient** button displays the name of the selected patient (Fig 15 **A**). See the documentation of the specific modules for the patient selection procedure.



Fig 15

Patient admitted

When a patient is admitted the **Patient** button displays, besides the patient name, the bed number and the name of the department where he/she is admitted (Fig 16).



Fig 16

The department name and the bed number are not highlighted if the patient belongs to the workstation domain (see Fig 16).

The department name and the bed number are highlighted yellow if the patient is located in a domain that does not belong to the workstation domain (Fig 17 - the workstation domain is defined by configuration).

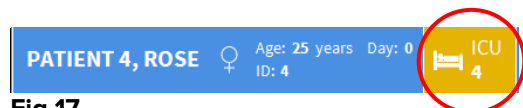


Fig 17



Every workstation is configured to be associated with a set of “beds” (domain). The user is enabled to perform certain actions only on the patients that are admitted to a bed belonging to this set. The red colour in the *PATIENT* button is used to advise the user that the patient selected is not in this set.

The signal “Other location” (Fig 18) appears when, at patient admission time, the user specified that the patient is not in one of the configured departments.



Fig 18

5.7 Help

Click the **Help** button on Control Bar (Fig 13 **F**) to access the online documentation available. The screen shown in Fig 19, or similar, depending on the available documentation, will open.

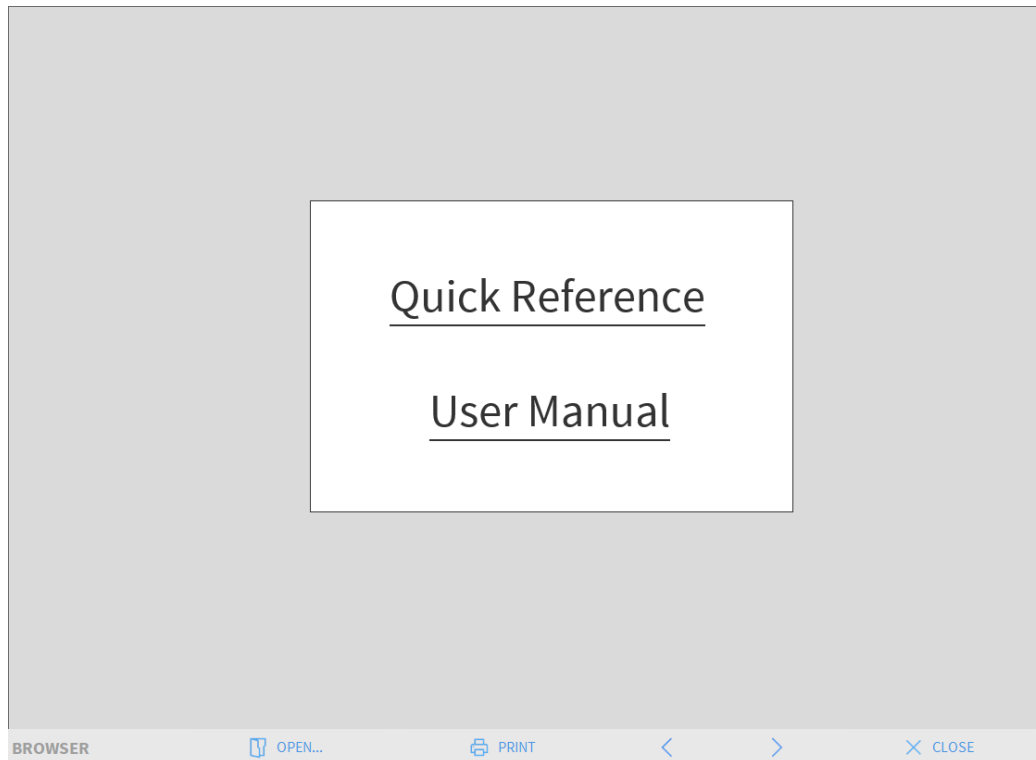


Fig 19

The command bar (Fig 20) offers some navigation possibilities.



Fig 20

- the **Open** button makes it possible to open other documents (if the user has the required permissions);
- the **Print** button prints the currently displayed document;
- the **<** and **>** buttons display either the previous or the next page of the document;
- the **Close** button closes the online help.

5.8 DIGISTAT® Main Menu

The **Menu** button placed on the DIGISTAT® Control Bar (Fig 21).



Fig 21

Opens a menu containing several options (Fig 22).

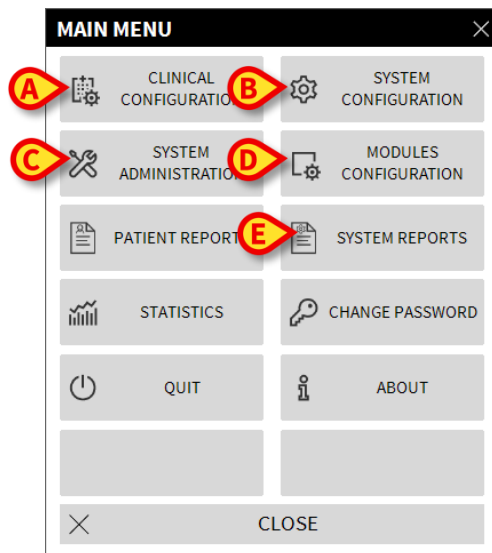


Fig 22

Each button on the menu accesses a specific set of functions.

The procedures associated with the following buttons relate to system configuration and are therefore reserved to the system administrators.

Clinical configuration - (Fig 22 **A**)

System configuration - (Fig 22 **B**)

System administration - (Fig 22 **C**)

Modules configuration- (Fig 22 **D**)

System reports - (Fig 22 **E**)

Contact your system administrator for the procedures associated to these buttons.

The other buttons, indicated in Fig 23, make it possible to access features and functions that some users can perform (according to their permission level). These will be described in the following sections.

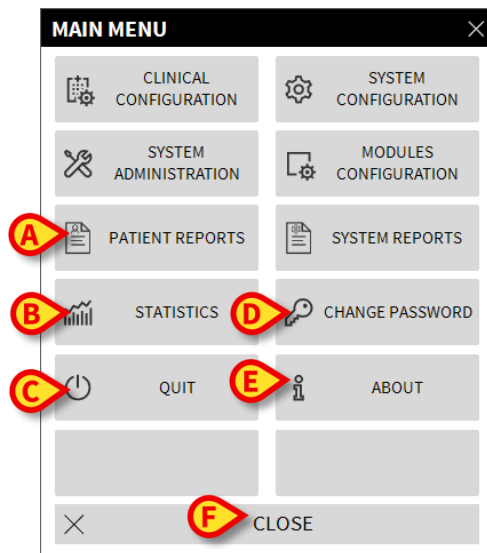


Fig 23

Patient reports - (Fig 23 **A**, paragraph 5.8.1)

Statistics - (Fig 23 **B**, paragraph 5.8.3)

Quit - (Fig 23 **C**, paragraph 5.8.6)

Change Password - (Fig 23 **D**, paragraph 5.8.4)

About - (Fig 23 **E**, paragraph 5.8.5)

The **Close** button (Fig 23 **F**) closes the "Main menu" window (Fig 23).

5.8.1 Patient reports

The “**Patient reports**” button (Fig 23 **A**) can be configured to open a sub-menu displaying various print options, each one making it possible to produce different print reports.

5.8.2 Print reports

This paragraph describes the Product’s general print functionalities. Whenever the print functionality is accessible, it is indicated in the specific section/paragraph of the manual. Refer to the present paragraph for general instructions.

To print a patient report:

- Click the relevant **Print** button

A print preview of the selected document will open (Fig 24).

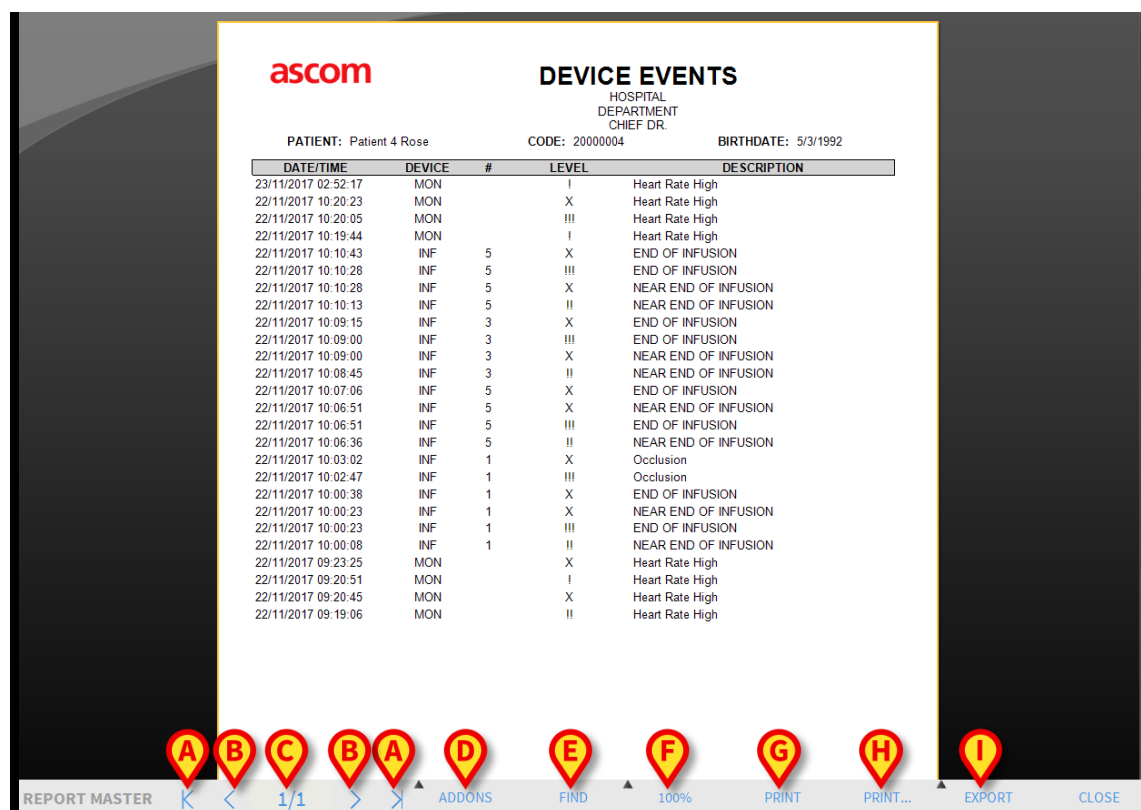







Fig 24

The buttons on the command bar of the “Print preview” screen make it possible to perform various actions, listed below.

Use the  and  buttons to reach the beginning and the end of the document.

Use the  and  buttons to go to the previous or the next page.

The display  indicates the current screen number.

The **Addons** button activates the possible additional print management options (in this configuration the “Watermarks” option is available - see paragraph 5.8.2.1 for a description of these options).

The **Find** button makes it possible to search the displayed document. See paragraph 5.8.2.2 for more instructions.

The button indicating the **100%** percentage is a zoom, making it possible to change the display mode. See paragraph 5.8.2.3 for more instructions.

Use the **Print** button (Fig 24 **G**) to print the report.

Use the **Print...** button (Fig 24 **H**) to display the print options window (Fig 30). See paragraph 5.8.2.4 for a description of this window and the related procedures.

Use the **Export** button (Fig 24 **I**) to export the document contents to different file extensions. See paragraph 5.8.2.5 for more instructions.

Use the **Close** button to close the “Print preview” screen.

5.8.2.1 Addons

The **Addons** button (Fig 24 **D**) activates the possible additional print management options.

To display the available options:

- Click the **Addons** button
- Click the button corresponding to the functionality you want to activate

Addons - Watermark

To add watermarks to the print report (either text or image, if the option is enabled by configuration),

- Click **Addons** and then **Mark**

The following window is displayed (Fig 25).

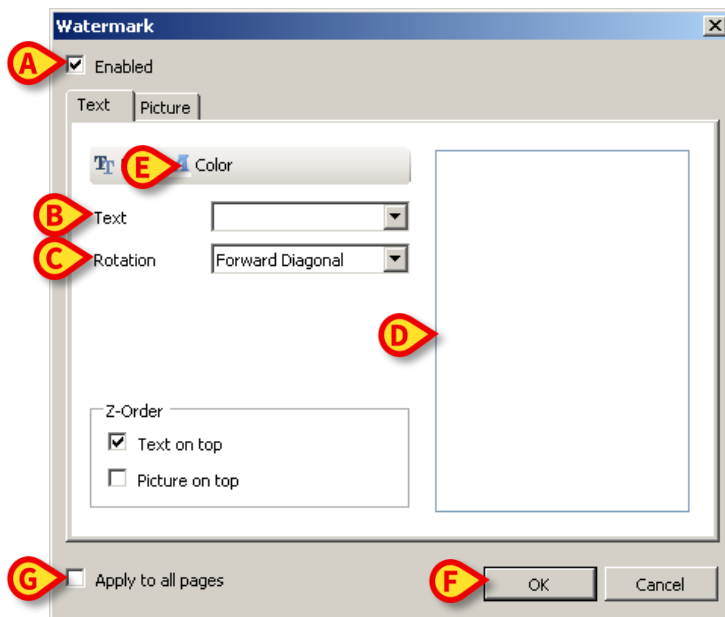


Fig 25

To add a textual watermark:

- Ensure that the “**Enabled**” checkbox is checked (Fig 25 **A**). If not, the window’s contents cannot be edited
- Insert the text in the “**Text**” field (Fig 25 **B**)
- Use the “**Rotation**” menu (Fig 25 **C**) to specify the watermark orientation (diagonal, horizontal, vertical)

A print preview is displayed in the area indicated in Fig 25 **D**.

- Use the buttons indicated in Fig 25 **E** to select the watermark font and color
- Click the **Ok** button (Fig 25 **F**)

The text is this way inserted as watermark.

If the “**Apply to all pages**” checkbox is selected (Fig 25 **G**) the watermark is applied to each page in the document, otherwise it is applied only to the current page.

To insert a picture as watermark:

- Click the “**Picture**” tab indicated in Fig 26 **A**

The following window is displayed (Fig 26).

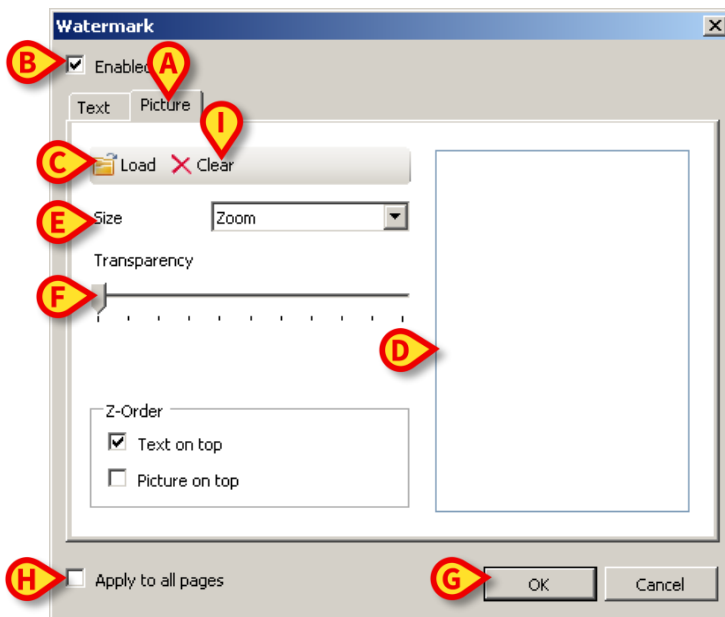


Fig 26

Follow these steps to insert an image as watermark:

- Ensure that the “**Enabled**” checkbox is checked (Fig 26 **B**). If not, the window’s contents cannot be edited
- Click the “**Load**” button indicated in Fig 26 **C**

This opens the window making it possible to browse the computer contents.

- Search and select the image to be uploaded

The image is displayed in the area indicated in Fig 26 **D**.

- Use the “**Size**” drop-down menu to set the size of the image (Fig 26 **E**)
- Use the “**Transparency**” cursor to set the transparency level of the watermark image (Fig 26 **F** - maximum transparency when the cursor is on the left)
- Click the **Ok** button (Fig 26 **G**). The watermark image is this way inserted

If the “**Apply to all pages**” checkbox is selected (Fig 26 **H**) the watermark is applied to each page in the document, otherwise it is applied only to the current page.

To delete an already selected image:

- Click the “**Clear**” button indicated in Fig 26 **I**

5.8.2.2 Find

The **Find** button (Fig 24 **E**) makes it possible to search the print report currently displayed.

To search the print report:

- Click the **Find** button

The following window opens (Fig 27).




Fig 27

- Insert in the window the text to be found in the print report (Fig 28 **A**)



Fig 28

- Click the  button (Fig 28 **B**)

The text specified, if found, will be highlighted in the print report.

- Click the  button again to search for the other instances in the text

5.8.2.3 Zoom

The **Zoom** button (on which, by default, the **100%** size is displayed - Fig 24 **F**) is a zoom, making it possible to change the display size and mode.

To change the display mode:

- Click the **Zoom** button. The following menu is displayed (Fig 29)

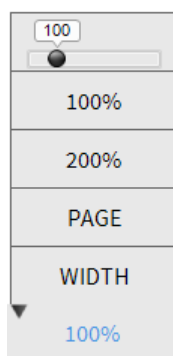


Fig 29

- Click the required zoom option on the menu

The page is displayed accordingly. The mode currently selected is indicated on the button.

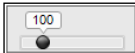
The following options are available:

The **Width** button makes it possible to display the page using the full screen width;

the **Page** button displays the whole page;

the **200%** button doubles the page size (200% zoom);

the **100%** button displays the page in its actual size (100% zoom);

the  area contains a cursor that can be used to zoom the page contents (left is zoom out, right is zoom in). The percentage value corresponding to the page size is displayed above the cursor. Values range from 100 to 200 %. The selected value is also displayed on the **Zoom** button on the command bar after selection.

5.8.2.4 Print

The **Print...** button opens a window offering several print options.

- Click the **Print...** button (Fig 24 **H**) to display the print options window (Fig 30)

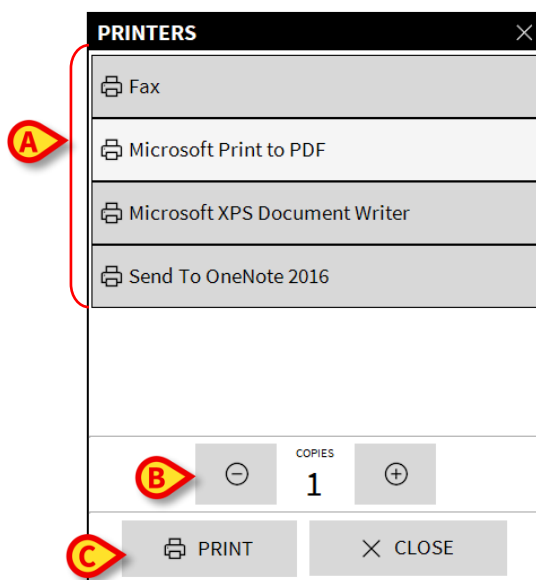




Fig 30

This window makes it possible to select the printer and the number of copies to be printed.

- Click the appropriate printer on the menu to select the printer (Fig 30 **A**)

- Use the  (one less copy) and the  (one more copy) buttons to specify the number of copies (Fig 30 **B**)
- Click the **Print** button (Fig 30 **C**) to print the report

5.8.2.5 Export

The **Export** button (Fig 24 **I**) makes it possible to export the displayed document contents to different file extensions.

- Click the **Export** button to open the “Export” menu

The menu displays all the file formats currently supported by the system in use.

- Click the option corresponding to the required file format

The document is exported to the corresponding file format.

5.8.3 Statistics

The **Statistics** button on the main menu (Fig 31) makes it possible to access the system's statistical calculation tools.

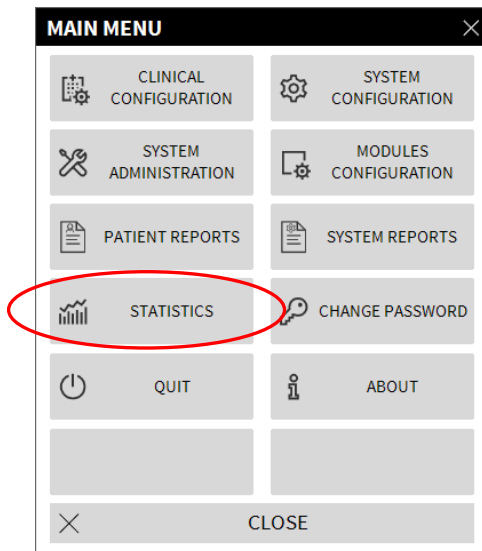


Fig 31

The button opens another menu (Fig 32) that enables access to various distinct tools. The type and number of accessible tools depend on the configuration in use and the specific modules installed.

These tools are mainly reserved for the system administrators. Please see the specific technical documentation for a description.

The “Query assistant” tool, which is accessible for users having specific permissions, is described in the next section.

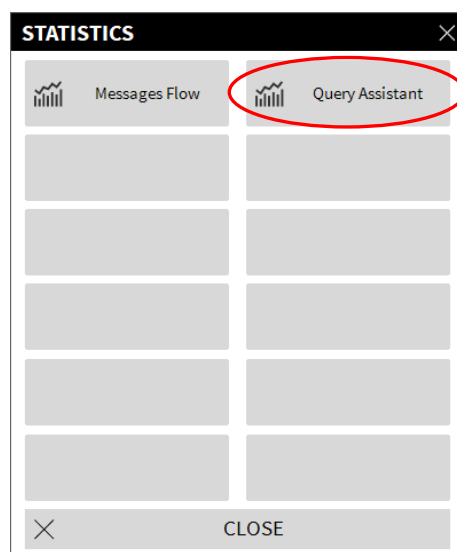


Fig 32

5.8.3.1 Query Assistant

The **Query Assistant** button (Fig 32) accesses a tool to create, save and execute queries on the DIGISTAT® database (Fig 33).

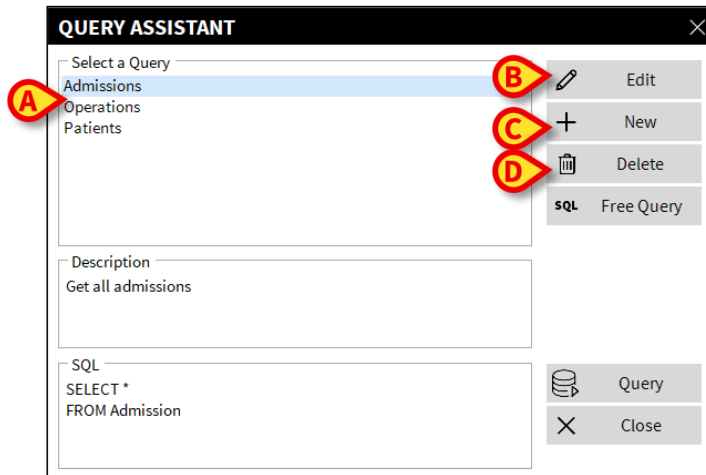


Fig 33

The user can select a query from a list of pre-defined queries, which will execute the query and display the results in a specific window.

The “Select a Query” area displays the list of all the pre-defined queries (Fig 33 **A**).

To run a query:

- Click the corresponding name on the list

The name will be highlighted (Fig 34 **A**).

A textual description of the query is displayed in the “Description” area (Fig 34 **B**).

The “SQL” area (indicated in Fig 34 **C**) displays the content of the query in SQL language (Structured Query Language).

The **Edit** button placed on the right of the “Query Assistant” window (Fig 33 **B**) makes it possible to edit an existing query.

The **New** button placed on the right of the “Query Assistant” window (Fig 33 **C**) makes it possible to create a new query.

The **Delete** button placed on the right of the “Query Assistant” window (Fig 33 **D**) makes it possible to cancel an existing query.



The “edit”, “delete” and “new” query options are reserved for the system administrators.

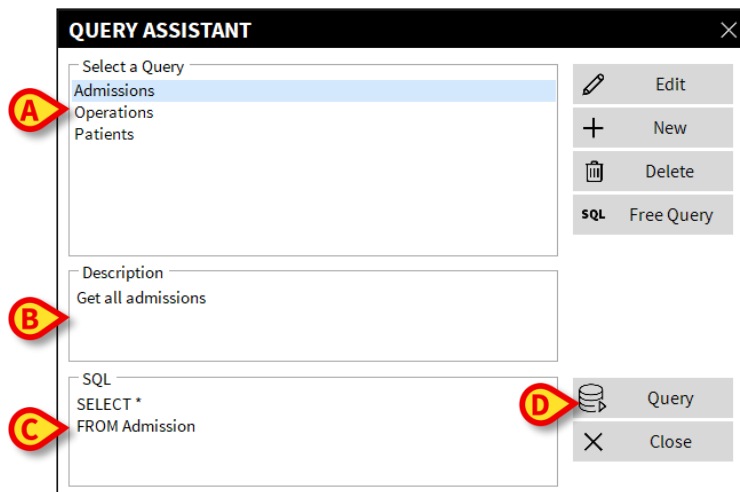


Fig 34

To run the query:

- Click the **Query** button (Fig 34 D - bottom-right)

The results are displayed in a new window, as a table (Fig 35).

ID	Patient Ref	Father Ref	Date Created	Admission Code	Height	Weight
1	1	1	11/22/2017 7:5...	20000001#1	170	80
2	2	2	11/22/2017 7:5...	20000002#1	180	70
3	3	3	11/22/2017 7:5...	20000003#1	180	75
4	4	4	11/22/2017 7:5...	20000004#1	165	55
5	5	5	11/22/2017 7:5...	20000005#1	172	57
6	6	6	11/22/2017 7:5...	20000006#1	174	90
7	7	7	11/22/2017 7:5...	20000007#1	181	90
8	8	8	11/22/2017 7:5...	20000008#1	186	75
9	9	9	11/22/2017 7:5...	20000009#1	161	63
10	10	10	11/22/2017 7:5...	20000010#1	165	52

Fig 35

5.8.4 Change password

The **Change Password** button on the DIGISTAT® main menu (Fig 36 A) opens a window making it possible to change the password of the user currently logged to the system.

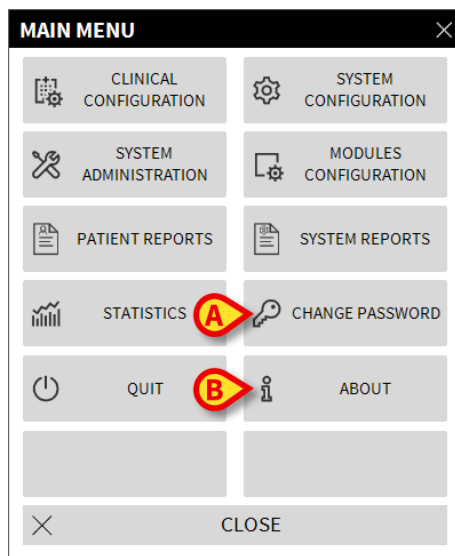


Fig 36

To change the user password:

- Click the **Change Password** button (Fig 36 A)

The “Change password” window will open.

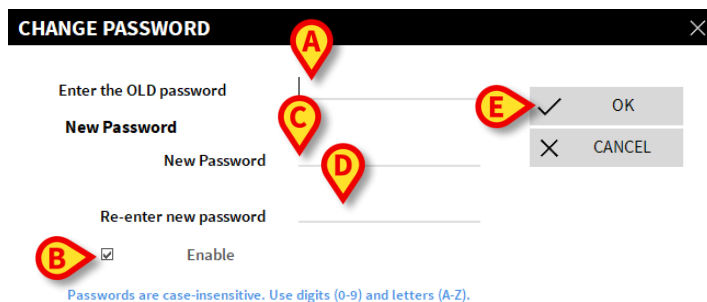


Fig 37

- Type the current password in the “**Enter the OLD password**” field (Fig 37 A)
- Verify that the “**Enable password**” checkbox (Fig 37 B) is selected
- Type the new password in the field indicated in Fig 37 C
- Type again the new password in the field “**Re-enter new password**” (Fig 37 D)
- Click the **Ok** button (Fig 37 E)



The passwords are not sensitive to uppercase and lowercase. The passwords can only be formed by numbers (0 to 9) and letters (A-Z).

5.8.5 About DIGISTAT®

The **About** button on the DIGISTAT® main menu (Fig 36 **B**) displays a window containing information on the DIGISTAT® version installed and the related licenses (Fig 38).

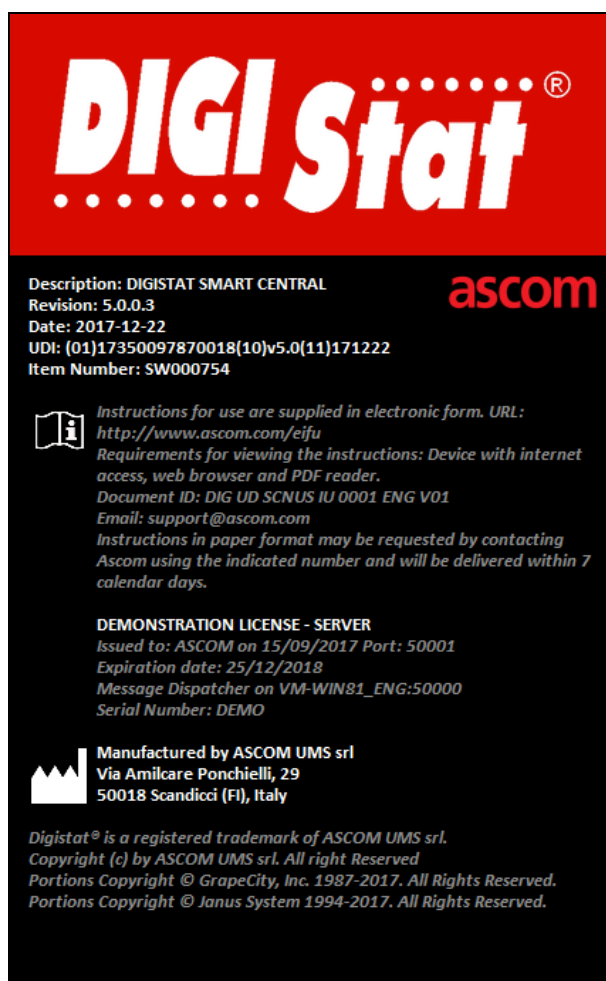


Fig 38

5.8.6 Quit DIGISTAT®

The **Quit** button on the DIGISTAT® main menu (Fig 40 **A**) makes it possible to quit the DIGISTAT® environment.

To quit DIGISTAT®:

- Click the **Menu** button on the control bar (Fig 39)



Fig 39

The DIGISTAT® main menu will open (Fig 40).

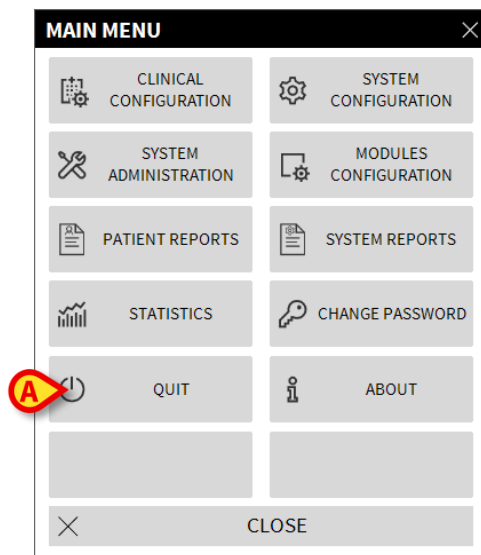


Fig 40

- Click the **Quit** button (Fig 40 **A**)

Another menu is displayed (Fig 41).

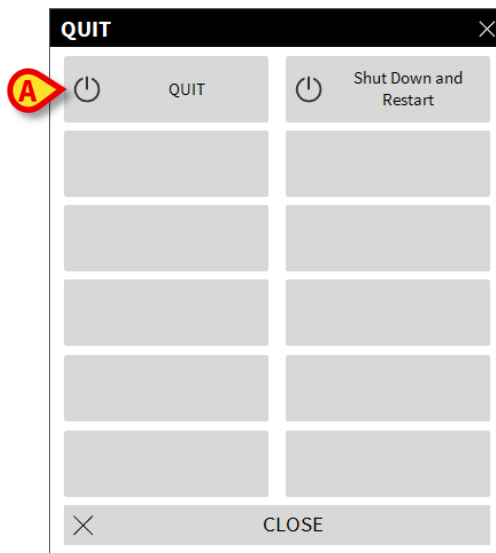


Fig 41

- Click the **Quit** button again (Fig 41 **A**)

User confirmation is required (Fig 42).

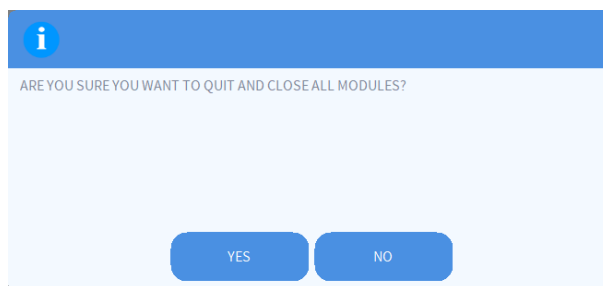


Fig 42

- Click **Yes** to exit DIGISTAT®



Specific permissions are required to exit DIGISTAT®. Not all DIGISTAT® users are enabled to close DIGISTAT.

6. Manufacturer Contacts

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

Here are the manufacturer contacts:

ASCOM UMS s.r.l unipersonale

Via Amilcare Ponchielli 29, 50018, Scandicci (FI), Italy

Tel. (+39) 055 0512161

Fax (+39) 055 8290392

Technical assistance

support.it@ascom.com

800999715 (toll free, Italy only)

Sales and products information

it.sales@ascom.com

General info

it.info@ascom.com

7. Residual risks

A risk management process has been implemented in the life cycle of DIGISTAT® [SI1] adopting the relevant technical regulations (EN14971, EN62304, EN62366). 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® performance, which could cause delays and/or errors in the therapeutic/diagnostic actions.
- Circulation of users’ and/or patients’ sensitive data.
- Unauthorized actions carried out by users, which can cause errors in the therapeutic/diagnostic actions and in the allocation of responsibilities of these actions.
- 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.
- Accidental data deletion, resulting in loss of data, which can cause delays and/or errors in the therapeutic/diagnostic actions.

RISKS RELATING TO THE HARDWARE PLATFORM IN USE

- 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.