Digistat Suite NA
User Manual

Version 5.0

2022-04-12

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 Suite NA version 7.2

Digistat Suite NA is composed by the following products:
Digistat® Smart Central version 7.2
Digistat® Connect version 7.2

Digistat® Smart Central and Digistat® Connect are manufactured by Ascom UMS srl (http://www.ascom.com).

Digistat® Smart Central is a Class II medical device in accordance with 21 CFR §870.2300 provided by the FDA and therefore it is to be installed, configured, maintained and used in US only.

Digistat® Connect is an MDDS in accordance with 21CFR880.6310 provided by the FDA and in accordance with Medical Device Regulation provided by the Canada Food and Drugs Act and therefore it is to be installed, configured, maintained and used in US and Canada only.

SOFTWARE LICENSE

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

LICENSES AND REGISTERED TRADEMARKS

Digistat® is a Trademark of Ascom UMS s.r.l

All other trademarks are the property of their respective owners.

Ascom UMS is certified according to ISO 9001:2015, ISO 13485:2016 and ISO/IEC 27001:2013 standards.

Contents

1 Using the manual

1.1 Aims

This manual provides all the necessary information for a safe and correct installation and configuration of the Digistat Suite NA (hereafter “Product”) and allows the identification of the manufacturer. Furthermore, it provides a reference guide to the user who wants to know how to perform specific operations and a guide for the correct use of the software so to prevent potentially hazardous misuses.

This manual provides all the necessary information to guarantee a safe and correct use of the Digistat Suite NA (hereafter “Product”) and to allow the manufacturer identification. Furthermore, it provides a reference guide to the user who wants to know how to perform specific operations and a guide for the correct use of the software so to prevent potentially hazardous misuses.

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

1.2 Characters used and terminology

The use of the Product 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.
Besides, the use of the Product 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 2”) or to a paragraph / section (e.g. “Paragraph 2.2.1”), you can click the reference to go directly to that particular figure or that particular paragraph / section.

The clinical data displayed in the images contained in Ascom UMS manuals are examples created in a test environment whose only purpose is to explain the structure and the procedures of the Product. They are not, and shall not be considered as, actual data taken from real-life clinical procedures.
Parts related to the configuration of the product are presented in English in Ascom UMS manuals. These configurations depend on the actual procedures and names adopted by the healthcare organization using the Product and consequently will be in the language requested by the healthcare organization.

1.3 Conventions

The following conventions are used in this document:

- Names of buttons, menu commands, options, icons, fields and anything on the user interface that the user can interact with (either touch or click or select) are formatted in **bold**.
- Names/headings of screens, windows and tabs are quoted with “Double quotation marks”.
- Programming code is formatted in Courier.
- The ➢ bullet indicates an action the user must perform to carry out a specific operation.
- References to external documents are formatted in *italic*.

1.4 Symbols

The following symbols are used in this manual.

	Useful information
	This symbol appears alongside additional information concerning the characteristics and use of the Product. This may be explanatory examples, alternative procedures or any “extra” information considered useful to a better understanding of the product.

	Caution!
	This 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
	Indicates the need for the user to consult the instructions for use for important cautionary information such as warnings and precautions that cannot, for a variety of reasons, be presented on the medical device itself.

The following symbols are applicable in US market:

℞ 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.

1.5 Digistat Suite NA - Overview

The Digistat Suite NA is a modular PDMS intended to create solutions to address the needs related to patient data management. The different solutions are created enabling the necessary modules that are part of the two products of the suite, which are:

- Digistat Connect (MDDS in accordance with 21CFR880.6310 provided by the FDA and in accordance with Medical Device Regulation provided by the Canada Food and Drugs Act);
- Digistat Smart Central (Class II medical device in accordance with 21 CFR §870.2300 provided by the FDA).

Digistat Connect is a software that records, transfers, stores, organizes and displays patient information and patient related data.
Digistat Connect is meant to provide patient data to Hospital Information Systems (HIS) or, in conjunction with Unite, to provide secondary alarm notifications to the Unite System. Digistat Connect also supports the collection of patient information manually entered by the clinicians.

Digistat Smart Central is a software that manages patient information and patient related data, including data and events from medical devices and systems, providing information to support treatment, diagnoses, prevention, monitoring, prediction, prognosis and mitigation of disease.

Both products are modular, therefore the specific healthcare organization can choose whether enabling all the available modules or only a sub-set, according to their needs and goals.

Modules can be added at different times. The resultant software suite can change over time according to the possible changes in the organization needs. In these cases, specific additional training is delivered and the configuration is validated again involving the responsible organization.

1.6 Abbreviations and Glossary

The following abbreviations are used in this manual.

ADT	Admissions, discharge, transfer system.
Bed Code	A bed or location code determines the unique identification code needed for integration with external system.
Driver	Software unit meant to retrieve the vital parameters, status, and events from the device from which is physically connected.
DAS	Data Acquisition System.
Dataset	A packet containing header and body. The header shows the data's origin (i.e. X monitor with serial y) and the device status. The body contains a set of parameters.
HU	Hospital Unit.
ICU	Intensive Care Unit.
NIBP	Non-invasive blood pressure.
Patient MRN	Patient Medical Record Number.

1.7 The About Box

The **About** button on the main menu displays a window containing information on the Digistat Suite NA version, the products installed and the related licenses.

The labeling of the product is the About Box displayed on the client workstations, mobile devices and web modules where the Digistat Suite NA is installed.

1.8 Digistat Connect

Digistat Connect is a centralized software solution to acquire information about clinical data, alarms and events, in near real time from a large number of medical devices (monitors, ventilators, infusion pumps, blood gas, etc.). Digistat Connect creates a common, standard, automatic data stream providing patient data to the Hospital Information Systems.

Digistat Connect is device-vendor neutral and able to scale from single departments to multiple wards. Its specific architecture permits to scale up the system in many different ways to adapt to specific topographical configurations.

Digistat Connect is a solution able to interface with a wide range of medical devices, throughout the Hospital infrastructure. Data is captured from devices using serial or networked connections, choosing the right integration for the right care environment.

Digistat Connect captures a wide set of data according to the device:

- Continuous data
- Sporadic data
- Events (user or device related)
- Alarms
- Logs (technical or device related)

Hundreds of device interfaces for many brands are already available and new ones are continuously being developed.

Digistat Connect feeds multiple independent downstream systems with a tailored, normalized, enriched flow of patient data, providing a wide range of benefits:

- Automatic and objective patient data documentation
- Time saving efficiency for nursing staff avoiding transcription errors
- Detailed vital signs parameter collection for clinical records
- Device Log for alarms and user actions

Single source of clinical information for all Hospital IT systems.

1.9 Digistat Connect: intended use and Indications for use

Digistat Connect transfers, stores, converts formats of, and displays patient data and events from connected clinical devices and systems or manually entered, in order to

- acquire clinical data and events from the connected devices in near real-time;
- acquire data from external, clinical and non-clinical systems;
- collect data manually entered by the user;
- store data and events in a central data repository;
- convert formats of collected information according to predefined rules;
- transfer the acquired information to external, clinical and non-clinical systems in near real-time via a subscription interface, or retrospectively via data query;
- display data to help verify connectivity to connected devices and systems.

Digistat Connect **does not** replace or replicate the original display of data of the connected devices and systems, and **does not** control, monitor or alter the behavior of these connected devices and systems.
Digistat Connect **is not** intended to be used in connection with active patient monitoring or to be relied upon in deciding to take immediate clinical action.
Digistat Connect is intended for use by trained healthcare professionals within a hospital/clinical 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.
Digistat Connect is a stand-alone software that is installed on servers, computers and optionally mobile devices, which shall comply with the technical hardware and software specifications provided with the Product.

1.10 Digistat Smart Central

Digistat Smart Central is a software that manages patient information and patient related data, including data and events from medical devices and systems, providing information to support treatment, diagnoses, prevention, monitoring, prediction, prognosis and mitigation of disease.

1.11 Digistat Smart Central: intended use and Indications for use

1.11.1 Digistat Smart Central: 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 behavior 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.

1.11.2 Digistat Smart Central: Indications for 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 from patient monitors, ventilators, infusion pumps, anesthesia machines, incubators and hemodialysis/hemofiltration machines 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 behavior 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.

1.12 “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”.

1.13 Patient Population

The product is a software application intended to be used on selected central stations and mobile devices. It is used to provide a secondary display of physiological and technical parameters and alarms from the connected medical devices and systems for remote monitoring and alarm surveillance.
The product is not in contact with the patient, it is intended to forward the information generated by the connected medical devices and systems, and it does not generate patient related alarms. As a consequence, the patient population and patient conditions are established by the medical devices and systems with which the product is connected.

1.14 Safety Advisories

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.
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.
When entering patient related data, the user has responsibility to verify that the patient identity, Healthcare Organization 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 Organization is responsible to identify 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 Organization.
The Product may provide, depending on the configuration, access to information on drugs. The Healthcare Organization is responsible to verify, initially and periodically, that this information is current and updated.
In order to use the Product in a clinical environment, all the components of the system, which the Product is part of, shall fulfil all the applicable regulatory requirements
In case some devices used for the Product are located in the patient area or are connected to equipment present in the patient area then the Healthcare Organization have responsibility to ensure that the whole combination complies with the international standard IEC 60601-1 and any additional requirement established by the local regulations.
Should the Product be part of a “medical electrical system” through electrical and functional connection with medical devices, the healthcare organization 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.
The Product is a stand-alone software that runs on standard computers and/or standard mobile devices connected to the Healthcare Organization local network. The Healthcare Organization is responsible to protect adequately computers, devices and local network against cyber-attacks and other malfunctions.
The Product shall be installed only on computers and devices fulfilling the minimum hardware requirements and on supported operating systems and browsers.

Use of the Product must be granted, by means of specific configuration of user accounts and active surveillance, only to User 1) trained according to Product indications by personnel authorized by the manufacturer or distributors and 2) in possession of the professional qualifications to interpret correctly the information supplied and to implement the appropriate safety procedures.

1.15 Residual risks

A risk management process has been implemented in the life cycle of the Product adopting the relevant technical standards. Risk control measures have been identified and implemented in order to reduce the risks to the minimum level and make them acceptable compared to the benefits brought in by the product. The overall 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 remove completely them; these residual risks shall be disclosed to the users.

- Inability to use the Product or some of its functionalities as expected, which could cause delays and/or errors in the therapeutic/diagnostic actions.
    - An example of this risk is a failure of the user to detect an alarm (e.g. due to a temporary distraction). An acoustic notification is used to draw the user attention and so reduce the risk.
- Slowdown of the product performance, which could cause delays and/or errors in the therapeutic/diagnostic actions.
- Unauthorized actions carried out by users, which could cause errors in the therapeutic/diagnostic actions and in the allocation of responsibilities of these actions.
- Wrong or incomplete configuration of the Product which could cause delays and/or errors in the therapeutic/diagnostic actions.
- Attribution of information to the wrong patient (accidental patient exchange), which could cause delays and/or errors in the therapeutic/diagnostic actions.
- Wrong handling of patient data, including errors in visualizing, adding, modifying and deleting data that could cause delays and/or errors in the therapeutic / diagnostic actions.
- Off label use of the product (e.g. Product used as a primary alarm notification system, therapeutic or diagnostic decisions and interventions based solely on the information provided by the Product).
- Unauthorized disclosure of users and/or patient's personal data.

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

- Electric shock for the patient and/or the user, which could cause injury and/or death for the patient/user.
- Hardware components overheating, that could cause injury for the patient/user.
- Risk of infection for the patient/user.

1.16 Healthcare organization responsibilities

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 (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.

The product is designed taking into account the requirements and best practices present in the IEC 80001 standard and its collateral technical reports. In particular, the IEC/TR 80001-2-5 has great relevance for the product. As clarified in the IEC 80001 series part of the necessary activities and risk control measures are under the control and responsibility of the healthcare organization. Please refer to the standard and its collaterals to identify the necessary activities and risk control measures; in particular refer to the following documents:

- IEC 80001-1
- IEC/TR 80001-2-1
- IEC/TR 80001-2-2
- IEC/TR 80001-2-3
- IEC/TR 80001-2-4
- IEC/TR 80001-2-5

1.17 Manufacturer's responsibility

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

- Installation and configuration were performed by personnel trained and authorized by Ascom UMS;
- Use and maintenance comply with the instructions provided in the Product documentation (including this User Manual);
- Configurations, changes and maintenance are only performed by personnel formed and authorized by Ascom UMS ;
- The Product's usage environment complies with applicable safety instructions and applicable regulations;
- The environment in which the Product is used (including computers, equipment, electrical connections, etc.) complies with applicable local regulations.

1.18 Product traceability

In order to ensure device traceability and on-site corrective actions, in compliance with ISO 13485, the 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 can be found in the Product label ("About box" displayed within the Product).
In case of doubts/questions about Product identification, please contact Ascom UMS/Distributor technical assistance (for contacts see section 4).

1.19 Post-market surveillance

The Product is subject to a post-market surveillance - which Ascom UMS and Distributor provide for each marketed copy - concerning actual and potential risks, either for the patient or for the User, during the Product's life cycle.
In case of malfunction or deterioration in the characteristics or performance of a device, including use-error due to ergonomic features, as well as any inadequacy in the information supplied that have been or could be a hazard to either the patient or User' health or to environmental safety, the Technician must immediately give notice to either Ascom UMS or Distributor.
On reception of a user feedback Ascom UMS/Distributor will immediately start the review and verification process and perform the necessary corrective actions.

1.20 Product life

The lifetime of the Product does not depend on wearing or other factors that could compromise safety. It is influenced by the obsolescence of the software environment (e.g. OS, .NET Framework) and is therefore set to 5 years from the release date of the Product version (available in the "About box" – see Section 1.7.)

2 Software/Hardware specifications

The Product 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 the Product configuration.

The Product must only be used by trained personnel. The Product 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 standard (Application of risk management for IT-networks incorporating medical devices).

It is responsibility of the healthcare organization to maintain the product execution environment including hardware and software as described in this chapter. Maintenance include upgrades, updates and security patches, of operating systems, web browsers, Microsoft .NET Framework, Adobe Reader, etc. as well as the adoption of the other best practices for the maintenance of software and hardware components.

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.

A supported PDF reader must be installed on the workstation in order to show the online help. See sections 2.1 and 2.2 for the requirements of workstations.

2.1 Requirements for Digistat Connect

2.1.1 Hardware

Minimum hardware requirements (small installation, 20 beds, 4 devices each):

- Intel® I5 processor with 4 cores.
- Memory: 8 GB RAM.
- Hard Disk: 120 GB of available space.
- Ethernet interface 100 Mb/s.

Recommended hardware requirements (medium size installation, 100 beds, 4 devices each):

- Intel® I7 processor with 8 cores.
- Memory: 32 GB RAM.
- Hard Disk: 120 GB of available space.
- Ethernet interface: 1 Gb/s.

2.1.2 Operating System

- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2016
- Microsoft Windows Server 2019
- Microsoft Windows Server 2022

2.1.3 System software

- Microsoft SQL Server 2012
- Microsoft SQL Server 2014
- Microsoft SQL Server 2016
- Microsoft SQL Server 2017
- Microsoft SQL Server 2019
- Microsoft .NET Framework v4.7.2

2.2 Requirements for Digistat Smart Central

2.2.1 Central & Bedside

2.2.1.1 Hardware

Minimum hardware requirements:

- Intel® i3 processor (or faster)
- Memory: 4 GB RAM
- Hard Disk: at least 60 GB of available space
- Monitor: 22'' display, 1920x1080 minimum resolution, with integrated speaker. Touch screen recommended.
- Mouse or other compatible device. Touch screen recommended.
- Ethernet interface 100 Mb/s (or higher)

In case a Central/Bedside workstation is configured to display video streams (feature supported only in Smart Central with camera integration enabled) the minimum requirements are the following:

- Intel® I3 processor (or faster)
- Memory: 4 GB RAM + 50MB every camera stream displayed concurrently (ex. with 20 cameras displayed 4 GB + 1 GB)
- Hard Disk: at least 60 GB of available space
- Monitor: 22'' display, 1920x1080 minimum resolution, with integrated speaker. Touch screen recommended.
- Mouse or other compatible device
- Ethernet interface 100 Mb/s (or higher)

Some examples: with Intel i7 6600 2.60 Ghz, with a streaming of 10 cameras with a bitrate of 3138 kbps, the cpu utilization is about 45%. With I3 7100t 3.4 Ghz, with a streaming of 16 cameras with a bitrate of 958 kbps, the cpu utilization is about 30%.

2.2.1.2 Operating System

- Microsoft Corporation Windows 8.1 x64 Professional
- Microsoft Corporation Windows 10 x64
- Microsoft Corporation Windows 11 x64

2.2.1.3 System Software

- Microsoft Framework .NET 4.7.2
- Adobe Acrobat Reader version 10

The User Manuals are PDF files, version 1.5, compatible with Acrobat 6.x or higher. Digistat Smart Central was tested with Adobe Acrobat Reader 10.
The hospital organization may use a different version of Acrobat Reader. It is part of the verification of the installation of Digistat Smart Central to assure that the help system is working correctly.

2.2.2 Server

2.2.2.1 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.

Recommended hardware requirements (medium size installation, 100 beds, 4 devices each, Connect and Mobile):

- Intel® I7 processor with 8 cores.
- Memory: 32 GB RAM.
- Hard Disk: 120 GB of available space.
- Ethernet interface: 1 Gb/s.

2.2.2.2 *Operating System*

- Microsoft Corporation Windows Server 2012 R2
- Microsoft Corporation Windows Server 2016
- Microsoft Corporation Windows Server 2019
- Microsoft Corporation Windows Server 2022

2.2.2.3 *System Software*

- Microsoft SQL Server 2012
- Microsoft SQL Server 2014
- Microsoft SQL Server 2016
- Microsoft SQL Server 2017
- Microsoft SQL Server 2019
- Microsoft .NET Framework v4.7.2

2.3 Digistat Mobile

Digistat Mobile is compatible with Android devices from version 5.1 up to 10.0. It has been verified on the Ascom Myco SH1 – Wi-Fi and Cellular with Android 5.1 (Myco2), on the Ascom Myco SH2 – Wi-Fi, Cellular and Dect with Android 9 (Myco3) and on Zebra TC51 - Android 7.1.

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.

The CDSS Configurator Mobile module of Digistat Mobile is compatible with Android 6.0+ devices.

2.4 Digistat Gateway

Digistat Gateway is compatible with Android devices from version 8.0 up to 10.0. It has been verified on the Ascom Myco SH2 Wi-Fi/Cellular (Android 9 and 10), Samsung A10 (Android 10). The application is designed to be compatible with other Android devices with a minimum screen size of 5'', and compatibility with a specific device must be verified before clinical use.

In order to be able to access the full Digistat Gateway functionality a SIM card with a voice plan is required. In case of an installation without Wi-Fi connection allowing access to the Gateway driver, also a data plan is required (LTE connectivity is strongly suggested).
Please contact Ascom UMS/Distributor for the full list of devices that support Digistat Gateway.

2.5 Digistat Web

The web component of the Digistat Suite NA is Digistat Web. The following browsers are supported for use with Digistat Web applications:

- Chrome 83
- Firefox 77
- Edge 83

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

2.6 Ascom Telligence

The Digistat Suite NA is compatible with the Ascom Telligence.
Supported version is Ascom Telligence 6.8.

All the Telligence components (server, staff station etc.) must be aligned to the supported version.

2.7 Requirements for High Availability functionality

Minimum Configuration. This type of configuration does not guarantee the HA functionality in case of workstation upgrade, update or substitution.

- Two (2) workstations;
- Satisfied Software requirements for installation (section 2).

Recommended requirements. This configuration guarantees the HA functionality in case of workstation upgrade, update or substitution.

- Three (3) workstations;
- Satisfied Software requirements for installation (section 2).

In any case, the SQL SERVER Always ON feature is required.

2.8 Requirements for Audio/Video streaming functionality

In certain configurations, Digistat Smart Central implements audio/video streaming functionalities.
In the cases in which parts of Digistat Smart Central act as viewer of video streams, Digistat Smart Central US is not the source of the video stream and it does not record this information in any way. It is responsibility of the healthcare organization to manage the system from a data protection perspective including the installation and configuration of source cameras.
Where Digistat Smart Central handles audio or images related to the users and/or patients including acquisition, elaboration and recording, it is responsibility of the healthcare organization to implement the necessary procedures to comply with the local data protection regulation. Including but not limited to definition of boundaries of usage and training of users.
The video streaming functionality on desktop workstations has been tested with H264 and H265 video codecs. Any other video codec natively present or installed by third party applications (e.g. VLC Media Player) has to be tested before use.
Each video source supports a maximum number of simultaneously connected clients. It is responsibility of the healthcare organization to determine this maximum number and to inform the users.
The video streaming functionality on mobile devices only supports RTSP video streams with the following authentication types:

- No authentication.
- Basic authentication.
- Digest authentication.

The video streaming functionality on mobile devices only supports H263, H264 and H265 video codecs.

2.9 General Warnings

For mobile and desktop modules (Digistat Smart Central), the decimal separator and, more generally, the regional settings (e.g. date formats) used by the Product depend on the settings of the operating system of the workstation or mobile device where the Product is installed.
For web modules (Digistat Connect), the decimal separator and, more generally, the regional settings (e.g. date formats) used by the Product depend on the Product configuration.

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 party hardware. These procedures must be performed only by qualified and authorized personnel.

The Product has been verified and validated during installation or upgrade phase and its acceptance testing is performed on the hardware (PC, server, mobile devices) and software (OS) and e.g. operating system) together with other software components (e.g. browser, antivirus, etc.) already present. Any other hardware or software installed may compromise the safety, effectiveness and design controls of the Product.

It is mandatory to consult an authorized Ascom UMS/Distributor before using together with the Product any other software than those validated in the installation or upgrade phase.

If any other software (utilities or applications programs) on the hardware on which the Product runs needs to be installed, healthcare organization shall inform Ascom UMS/Distributor for further validation. 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 workstations on which the Product runs a date/time synchronization mechanism to a reference source.

Hardware and Software requirements of 3rd party devices (including Smart Adapter Module by Project Engineering, Port Servers by Lantronix, etc.) are disclosed in their instructions for use, provided by suppliers. Contacts of the suppliers of 3rd party devices can be provided by Ascom UMS or authorized distributors.

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

2.10 Firewall and Antivirus

To protect the Product from possible cyber-attacks, it is necessary that:

- the Windows© Firewall is active both on the client PCs and the server;
- Antivirus/antimalware 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 the Product is compatible with any antivirus or antivirus configuration.

Some incompatibilities have been reported between parts of the Product 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.

2.10.1 Further recommended precautions for cyber-protection

In order to further protect the Product from possible cyber-attacks, it is highly recommended to:

- plan and implement the “Hardening” of the IT infrastructure including the IT platform that represent the runtime environment for the Product,
- implement an Intrusion Detection and Prevention System (IDPS),
- perform a Penetration Test and, if any weakness is detected, perform all the required actions to mitigate the risk of cyber-intrusion,
- dismiss the devices when they are no longer updatable,
- plan and perform a periodic verification of the integrity of files and configurations,
- Implement a DMZ (demilitarized zone) solution for web servers that need to be exposed on the internet.

2.11 Local network features

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

- The Product uses a TCP/IP traffic protocol.
- The LAN must not be congested and/or full loaded.
- The Product requires at least a 100 Megabit LAN available to the client workstation. 1 Gigabit Ethernet backbone 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.

The healthcare organization shall take into consideration the following points:

a) execution of the software on an IT- network could result in previously unidentified risks to patients, users or third parties;
b) the healthcare organization is responsible to identify, analyze, evaluate and control these risks;
c) subsequent changes to the IT- network could introduce new risks and require additional analysis.

Changes to the IT- network include:

1) changes in IT- network configuration;
2) addition of items (hardware and/or software platforms or software applications) to the IT- network;
3) removal of items from the IT- network;
4) update of hardware and/or software platforms or software applications on the IT-network;
5) upgrade of hardware and/or software platforms or software applications on the IT-network.

If the local network is at least partially based on Wi-Fi connections, given the possible intermittency of the Wi-Fi connection, network disconnections are possible, that cause the activation of the "Recovery or Disconnected Mode" and which in case the consequent product is used for primary notification of alarms, can cause system unreliability. The Healthcare Organization shall ensure an optimal network coverage and stability, and train the personnel users, in the management of these temporary disconnections.

In order to encrypt the data transmitted over wireless networks it is recommended to adopt the highest security protocol available; in any case no less than WPA2.

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

2.11.1 Impact of the Product on the healthcare organization network

This section provides information on the traffic generated by the Product on the network in order to make it possible for the structure to evaluate and analyze the risks related to the introduction of the Product.

The bandwidth used by the Product 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,
- Product configuration and mode of use.

The Product 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 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 configurations with no acquisition from medical devices, bandwidth occupation values are lower than those specified above.

3 Before starting

3.1 Installation and maintenance warnings

The following warnings provide important information on the correct installation and maintenance procedures of the 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.

It is recommended for the healthcare organization using the Product to stipulate a maintenance contract with Ascom UMS or an authorized Distributor. Part of the maintenance shall include the upgrade to the latest version available of the Product.

The Product 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 personnel can store, transport, install, maintain and dispose third party devices.
- 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 USB dongle, if 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.
- The healthcare organization is responsible to select equipment that are suitable for the environment in which they are installed and used. The healthcare organization among the other should consider electrical safety, EMC emissions, radio signal interferences, disinfection and cleaning. Attention shall be payed to devices installed in the patient area.
- The healthcare organization shall define alternative working procedures in case the system becomes unreliable or stops functioning

3.2 Data Protection 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.

'Personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person".

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) and of the Canada Personal Information Protection and Electronic Document Act (PIPEDA).

Protected health information (PHI) 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) and to the Canada Personal Information Protection and Electronic Document Act (PIPEDA), PHI that is linked based on the following list of 18 identifiers must be treated with special care

- Names
- All geographical identifiers smaller than a state,
- Dates (other than year) directly related to an individual
- Phone numbers
- Fax numbers
- Email addresses
- Social Security numbers
- Medical record numbers
- Health insurance beneficiary numbers
- Account numbers
- Certificate/license numbers
- Vehicle identifiers and serial numbers, including license plate numbers;
- Device identifiers and serial numbers;
- Web Uniform Resource Locators (URLs)
- Internet Protocol (IP) address numbers
- Biometric identifiers, including finger, retinal and voice prints
- Full face photographic images and any comparable images

- Any other unique identifying number, characteristic, or code except the unique code assigned by the investigator to code the data

The healthcare organization needs to assure that the use of the Product is in line with the requirements of the applicable regulation on privacy and personal data protection, specifically respect the management of aforementioned information.

The Product manages the following PHI:

- First name and surname
- Birthdate
- Sex
- Patient code (MRN)
- Admission date
- Discharge date
- Patient weight
- Patient height

The Product can be configured to hide automatically in the application screens when no user is logged in the PHI on every application screen that can be used to identify a natural person. The hidden fields are:

- First name and surname
- Birthdate
- Sex
- Patient code
- Admission date
- Discharge date
- Patient weight
- Patient height

The set of fields that are hidden can be adjusted during the configuration of the Product. To do that, on the 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.
- 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 user is advised against the frequent use of the lock function. Automatic log out protects the Product from unauthorized accesses.
- PHI can be present inside some reports produced by the Product. The healthcare organization needs to manage these documents according to HIPAA and PIPEDA 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 Organization'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.
- The healthcare organization is in charge to provide basic training regarding privacy issues: i.e. basic principles, rules, regulations, responsibilities and sanctions in the specific work environment. Ascom UMS/Distributor can provide specialized training on the best use of the Product relating to privacy issues (i.e. database anonymization, privacy mode, user permissions etc.).
- The healthcare organization shall produce and keep the following documentation:
    - the updated list of the system administrators and maintenance personnel;
    - the signed forms of assignment and the certifications of attendance at the training courses;
    - a register of credentials, permissions and privileges granted to the users;
    - an updated list of the Product users.
- The healthcare organization shall implement, test and certify a procedure of automatic deactivation of no-more-active users after a certain period.
- The healthcare organization shall codify, implement and document a procedure for the periodic verification of belonging to the role of system administrator and technical maintenance personnel.
- The healthcare organization shall carry out audits and checks on the correct behavior of the operators.

In some circumstances, sensitive data /PHI are transmitted in non-encrypted format and using a connection that 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.

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 organization's procedures and IT architecture (examples: physical machine, SAN, virtualization environment). Patient data must be treated according to all the current standards on privacy and personal data protection.

PHI can be present inside some reports produced by the Product. Once exported or printed, the healthcare organization is responsible to manage these documents according to HIPAA regulation.

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

It is recommended to configure the database server so that the Product database is encrypted on the disk. This option requires the healthcare organization to adopt SQL Server Enterprise Edition; during its installation it is necessary to enable the TDE (Transparent Data Encryption) option.

3.2.1 User credentials features and use

This section explains the 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 installation and 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 User Manual 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 installation and configuration manual.

The following information is reserved to system administrators:

- The password must match a regular expression defined in the Product 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.

3.2.2 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 Product database and act as “System Administrator” for the Product.
Ascom UMS/Distributor adopts procedures and work instructions complying with the current local data protection regulation, for example in US Health Insurance Portability and Accountability Act (HIPAA) and in Canada Personal Information Protection and Electronic Document Act (PIPEDA).

The Healthcare Organization should evaluate, among the others, the following technical measures:

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

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

3.2.3 System logs

The Product 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 installation and configuration manual” for the configuration procedures.

3.2.4 Forensic log

A subset of the before mentioned system logs, defined according to the policy of each specific Healthcare Organization using the Product as “clinically relevant” or “clinically useful”, can be sent to an external system (either SQL database or Syslog) to be stored according to the Healthcare Organization needs and rules.

3.3 Backup policy

It is recommended to regularly backup the Product database.

The Healthcare Organization using the Product 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.

As specified by the HIPAA and PIPEDA standards, databases cannot leave the hospital without being encrypted.

3.4 Out of order procedure

It is recommended to perform the backup of the image of the hard drive of the workstations, so in case of replacement of the hardware it is possible to restore quickly the operating environment.

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

This section describes the policy suggested by Ascom UMS in case a Product 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 the Product is already installed. In case of a Product workstation is out of order, the substitute equipment can promptly replace the Product workstation.

Always remember that the Product 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 the Product configuration.

The risk related to the Product 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 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 Product 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 Product workstation needs to be deactivated and replaced, the Healthcare Organization 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 the Product 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 Product 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 Product workstation, we suggest adopting 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 workstation, reserved to system administrators, are in the Digistat Suite NA installation and configuration manual.

3.4.1 Reconfiguration/substitution of network equipment

In case it is necessary to either reconfigure or substitute a network device involved in the data acquisition, the healthcare organization staff must promptly call Ascom UMS/Distributor and schedule the substitution/reconfiguration procedure to allow Ascom UMS staff to either reconfigure the Product 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 Product installation and configuration manual.

3.5 Preventive maintenance

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

It is suggested to perform the maintenance of the Product 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.

See the Digistat Suite NA installation and configuration manual for **the Preventive maintenance checklist.**

3.6 Compatible devices

Digistat Smart Central is compatible with Digistat Connect 7.2.0 and it is able to display data from ventilators, patient monitors, infusion pumps, hemodialysis/hemofiltration machines, incubators and anesthesia machines. Please contact Ascom UMS/Distributor for the list of available drivers.

Refer to the document *Digistat Data Acquisition Drivers.pdf* for the full list of available devices.

The document can be downloaded on the Ascom Confluence website:
https://confluence.ascom-ws.com/display/DIG/Drivers+Documentation

For reasons that are outside the control of the software, for instance, the way the actual physical devices are installed/cabled, delays are possible between the alarm generation and the actual alarm display.

The update of data displayed on screen caused by device connection, power off, disconnection and change of status depends on the time required by the device itself to communicate the changes. This time depends on various factors. Among them is the device type and type of connection. For some devices, there are

	conditions in which the delay in communicating changes might be important. Since they might change depending on devices configuration and operational conditions, it is not possible to provide an indication of the delays for all the possible devices.
	The drivers used to read the data from the connected medical devices have a reading-cycle of less than 3 seconds (i.e. all the data from the devices is read every 3 seconds at maximum). However, there are devices that communicate the information less frequently (5-10 seconds interval). Refer to the specific driver documentation for details on the reading-cycle. In a test environment installed and configured as indicated in the installation and configuration manual, as soon as a driver detects an alarm, it takes maximum 1 second to display on the user interface.
	The Product receives data from several sources: medical devices, hospital information systems and manually entered by the user. In addition, the Product calculates derived information (e.g. Scores). Clinical definition and validation of these calculations is made by the Healthcare Organization where the Product is installed. The range, precision and accuracy of these data depends on the external sources, on the data entered by the user and on the underlying hardware and software architecture.
	The Product is not a primary remote alarm system.
	The Product is not designed to verify that connected devices are working correctly.
	Disconnecting a device while it is running causes the interruption of data acquisition on the Product. Device data that is lost during the disconnection period are not recovered by the Product after reconnection.
	Never disable the alarm notification on the medical devices unless explicitly allowed by the medical device manufacturer documentation and the procedure of the healthcare organization.
	The Healthcare Organization is responsible to guarantee (e.g. through appropriate checklists) that the correct reception of alarm is handled in Digistat Smart Central both when notification sounds are disabled and when enabled for a specific patient on the mobile device.
	Never disable the audio on the workstations on which Digistat Smart Central is running.

According to the decision of the Healthcare Organization, Digistat Smart Central could be configured to filter and/or remap alarms generated by the connected medical devices.

The users shall be aware that, depending on the configuration, alarms could be presented with a different priority and/or message or could be not annunciated.
The Healthcare Organization is in charge to provide information and training to the users regarding the configuration of alarm filtering.
Users shall be informed of any following change to the alarm filtering configuration.

Periodically (for instance at the beginning of each shift) check on the central station where Digistat Smart Central is installed that for each bed data coming from the connected medical devices is correctly displayed.

Digistat Smart Central acquires the information generated by the primary medical devices (e.g. pulmonary ventilators, infusion pumps, etc.) and displays them. Therefore, Digistat Smart Central always reports what the primary medical devices communicates. The assignment of alarm priorities is decided according to the primary medical device. In Digistat Smart Central it is possible to decide the order of the medical devices, for every bed, in accordance to the customer preference: per device type, model / manufacturer. This kind of ordering is set up in Digistat Smart Central during deployment of the product according to the user requests/preferences. The color of every bed card (i.e. bed-area) is always the color of the highest priority alarm among all alarms occurring on that bed.

In case a “Nurse call” system is in use, it is recommended to never disable the “Nurse call” system.

Within the Digistat Smart Central the alarms are grouped in “physiological alarms”, “technical alarms” and “other”. This kind of differentiation has no impact on the way the alarms are displayed on the Digistat Smart Central interface.

In case of electrical black-out, it takes a few minutes for Digistat Smart Central to be fully operative again and therefore generate alarm notifications (usually this time is less than 3 minutes, however it depends on the configuration of the used computers).

At the beginning of each shift, execute the sound check procedure to verify if the audio on the workstation/handheld device is correctly working (see documents *USR ENG Smart Central* and *USR ENG Mobile Launcher* for the procedure on desktop workstations and mobile devices). If the Smart Central / Smart Central Mobile modules are not used within the healthcare organization, then the procedure is not relevant.

Up to a distance of 1m (3,28 ft) the Operator is able to read the notifications on the Product. Within a maximum distance of 4m (13,12 ft) it is possible for the Operator to see that there is an alarm.
This is true if:

- the Operator has a visual acuity of 0 on the logMAR scale or 6-6 (20/20) vision (corrected if necessary),
- the viewpoint is at the Operator's position or at any point within the base of a cone subtended by an angle of 30° to the axis horizontal to or normal to the center of the plane of display of the monitoring display or visual indication,
- the ambient illuminance in the range of 100 lx to 1 500 lx.

3.7 Workstation unavailability

In case the workstation (including mobile devices) where the Product is installed encounters issues when connecting to the server, a specific information message is displayed.

The Product tries to recover automatically. If automatic recovery fails, it is necessary to contact the technical assistance (see section 4 for the contacts list).

It is responsibility of the Healthcare Organization using the Product to define an emergency procedure to put into effect in case of system unavailability. 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).

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

4 Manufacturer and Distributor Contacts

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

Distributed in the U.S. 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.com