Digistat® Docs
User Manual

Version 8.0

2022-10-13

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 Docs version 1.3
Digistat® Docs is manufactured by Ascom UMS srl (http://www.ascom.com).

Ascom UMS is certified according to EN ISO 13485:2016 with the following scope: “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”.

Software License
Digistat® Docs must be used only after obtaining a valid license from Ascom UMS or the Distributor

Licenses and registered trademarks

Contents

1. Using the manual

This User Manual shall be used in combination with module-specific manuals, listed below. Refer to the applicable manuals, according to the Digistat Docs modules in use in the Healthcare Organization.

USR ENG Controlbar Web
USR ENG Codefinder
USR ENG Codefinder Web
USR ENG Diary
USR ENG Forms
USR ENG Forms Web
USR ENG Image Bank
USR ENG Messenger
USR ENG Dashboard
USR ENG On Line
USR ENG Nutrition
USR ENG Stock Management
USR ENG OranJ
USR ENG Smart Scheduler
USR ENG Voice Notes Mobile
USR ENG Identity Mobile
USR ENG Collect Mobile
USR ENG On Line Mobile

This User Manual shall also be used in combination with the following documents, being the related Digistat Care modules used by Digistat Docs:

USR ENG ControlBar
USR ENG Patient Explorer
USR ENG Mobile Launcher

Read Paragraph 1.5 for more information.

1.1 Aims

This manual provides all the necessary information for a safe and correct use of Digistat Docs 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.

1.2 Characters used and terminology

The use of Digistat Docs 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 Digistat Docs must only be granted to professionally qualified and authorized, trained personnel, with the exception of lay user for limited functions.

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 directly go 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 Digistat. 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.

1.5 The Digistat Suite - Overview

The Digistat Suite 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 Docs (non medical device);
- Digistat Care (Class IIb medical device).

Digistat Docs is a software that records, transfers, stores, organizes and displays patient information and patient related data in order to support caregivers to establish an electronic patient record.
Digistat Docs is not a medical device.

Digistat Care 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.
Digistat Care is a Class IIb medical device.

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 The About Box

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

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

In compliance with the EU Regulation No 207/2012 of 9 March 2012, instruction for use are provided in electronic format. The About box of the product contains the address of a web resource where the latest version of the instruction for use can be downloaded

2. Digistat Docs

Digistat Docs records, transfers, stores, organizes and displays patient information and patient related data, including data from external systems as well as information entered manually, in order to:

- provide electronic documentation of department activities;
- provide information on the use of materials and human resources;
- produce deferred statistics for quality control;
- display some information to remote users for non-clinical purposes.

Digistat Docs works together with Digistat Care, the other product of the Digistat Suite. See document *USR ENG Digistat Care* for more information.

2.1 Intended use

Digistat Docs (hereafter “Product”) is a software that records, transfers, stores, organizes and displays patient information and patient related data in order to support caregivers to establish an electronic patient record.
The Product includes:

- Configurable electronic patient record based on the recorded information, as well as on manual and automated documentation of the clinical unit’s activity;
- Storage of data and events in a central data repository;
- Conversion of available information according to predefined rules;
- Data transfer from and to clinical and non-clinical systems;
- Planning and documentation of the department activities;
- Retrospective visualization of data and events;
- Recording, validation and display of vital signs charting;
- Configurable reports, charts and statistics to document the patient record and to analyze the unit’s efficiency, productivity, capacity and resource utilization, and the quality of care;
- Specific functions and interfaces intended for lay users in remote locations to display information, reports, charts and statistics.

The Product is not intended to be relied upon in deciding to take clinical action nor to be used for direct diagnosis or monitoring of vital physiological parameters.
The Product is a stand-alone software that is installed on specified hardware and relies on proper use and operation of connected medical devices, systems, display devices and the medical IT network.
The Product works together with Digistat Care the other product of the Digistat Suite;
The Product is installed in healthcare facilities in critical care units, sub-intensive units, normal wards and other departments.
The patient population and patient conditions are established by the connected systems and by the particular configuration of the product requested by the healthcare organization.
The users are trained healthcare professionals with the exception of lay users for limited functions.

2.2 “Off-label” use of the Product

Every use of the Product outside what explicitly stated in the “Intended use” (usually referred to as “off-label” use) is under the full discretion and responsibility of the user and of the Healthcare organization.
The manufacturer does not guarantee in any form the Product safety and suitability for any purpose where the Product is used outside the stated “Intended use”.

2.3 Patient Population

The product is intended to be used in connection with medical devices and systems and the patient population is determined by them. The product has the following technical limits:

- Patient weight between 0.1kg and 250kg;
- Patient height between 15cm and 250cm.

2.4 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 have 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 fulfill all the applicable regulatory requirements.
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.
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.

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 correctly interpret the information supplied and to implement the appropriate safety procedures, with the exception of lay user for limited functions.
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 adequately protect 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.

2.5 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 completely remove 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 documentation activities.
- Slowdown of the product performance, which could cause delays and/or errors in the documentation activities.
- Unauthorized actions carried out by users, which could cause errors in the documentation activities 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 documentation activities.
- Attribution of information to the wrong patient (accidental patient exchange), which could cause delays and/or errors in the documentation activities.
- Wrong handling of patient data, including errors in visualizing, adding, modifying and deleting data that could cause delays and/or errors in the documentation activities.
- Off label use of the product (e.g. Product used as a primary support for taking therapeutic or diagnostic decisions and interventions).
- 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.

2.6 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

2.7 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 environment in which the Product is used (including computers, equipment, electrical connections, etc.) complies with applicable local regulations and safety instructions.

2.8 Product traceability

In order to ensure device traceability and on site corrective actions, 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.
Device data can be found in the Product label ("About box" displayed within the Product – see paragraph 1.6).
In case of doubts/questions about Product identification please contact Ascom UMS/Distributor technical assistance (for contacts see Section 5).

2.9 Post-market surveillance

The product is subject to 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 User must immediately give notice to either Ascom UMS or Distributor.
On reception of a user feedback or if made aware internally Ascom UMS/Distributor will immediately start the review and verification process and perform the necessary corrective actions.

2.10 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 software environment (e.g. OS, .NET Framework) and is therefore set to 3 years from the release date of the Product version (available in the "About box").

3. 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, with the exception of lay user for limited functions. 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 3.1.3 for the Software Requirements of Central & Bedside workstations.

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: 22'' display, 1920x1080 minimum resolution, with integrated speaker. Touch screen recommended.
- Mouse or another compatible device.
- Ethernet interface 100 Mb/s (or higher)

In case a Central/Bedside workstation is configured to display video streams (feature supported only by OranJ 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 another 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 bit rate of 3138 kbps, the CPU utilization is about 45%. With I3 7100t 3.4 GHz, with a streaming of 16 cameras with a bit rate of 958 kbps, the CPU utilization is about 30%.

3.1.2 Operating System

- Microsoft Corporation Windows 8.1 x86/x64 Professional
- Microsoft Corporation Windows 10
- Microsoft Corporation Windows 11

3.1.3 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 was tested with Adobe Acrobat Reader 10. The healthcare organization may use a different version of Acrobat Reader, it is part of the Verification of the installed product to assure that the help system is working correctly.

3.2 Application server

3.2.1 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, 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.

3.2.2 Operating System

One of the following operating systems must be installed:

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

3.2.3 System Software

- Microsoft Framework.NET 4.7.2
- Net Core Runtime & Hosting Bundle (see INST ENG Digistat Web manual for details)

3.3 Database Server

3.3.1 Hardware

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

- Intel® I5 processor with 4 cores;
- Memory: 8 GB RAM;
- Hard Disk: 100 GB of available space;
- Backup Hard Disk: 1TB of available space;
- Ethernet interface 100 Mb/s.

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

- Intel® I7 processor with 4 cores;
- Memory: 16 GB RAM;

- Hard Disk: 100 GB of available space, Solid State Disk;
- Backup Hard Disk: 1TB of available space;
- Ethernet interface: 1 Gb/s.

3.3.2 Operating System

One of the following operating systems must be installed:

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

3.3.3 System Software

One of the following versions of Microsoft SQL Server must be installed:

- Microsoft SQL Server 2012;
- Microsoft SQL Server 2014;
- Microsoft SQL Server 2016;
- Microsoft SQL Server 2017;
- Microsoft SQL Server 2019;

3.4 Digistat Mobile

Digistat Mobile is compatible with Android devices from version 5.1 up to 12.0. It has been verified on the Ascom Myco SH2 – Wi-Fi, Cellular and Dect with Android 10 (Myco3), on Samsung Galaxy 10 with Android 11, on Google Pixel 3a with Android 12 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.

Diary Mobile and Online Mobile modules of Digistat Mobile are compatible with Android 6.0+ devices.

3.5 Digistat Web

The following browsers are supported for use with Digistat® Web (hereafter "Digistat Web") applications:

- Chrome 91
- Firefox 88
- Edge 91

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

3.6 General Warnings

For mobile and desktop modules, 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, the decimal separator and, more generally, the regional settings (e.g. date formats) used by the Product depend on the Product configuration.

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

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 Product has been verified and validated during installation or upgrade phase and its acceptance testing has been performed on the hardware (PC, server, mobile devices) and software (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 or authorized distributors.

3.7 Audio/Video streaming functionality

In certain configurations the Product implements audio/video streaming functionalities.
In the cases in which parts of the Product act as viewer of video streams, the Product 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.
In the cases in which parts of the Product handle audio and 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.

3.8 Firewall and Antivirus

The content of this paragraph is intended to be used by technicians only (e.g. system administrators.

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.

Some incompatibilities have been reported between parts of the Data Acquisition Service and Windows Defender antivirus (note: not the Windows Defender firewall). Therefore an exclusion for the entire ./Server/DAS/DAS3 folder inside the Digistat Suite Server installation folder must be set in case Windows Defender is in use.

3.8.1 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.

3.9 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 backbones would be worthwhile.
- There must not be filters in the TCP/IP traffic between workstations, server and secondary devices.
- If the devices (server, workstations and secondary devices) are connected to different subnets there must be routing in these subnets.
- It is recommended to adopt redundancy strategies to ensure network service availability in case of malfunction.
- It is recommended to schedule, together with Ascom/Distributors, the maintenance calendar in order to let Ascom or the authorized Distributor efficiently support the healthcare organization in managing the possible disservices caused by maintenance activities.

If the 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". The Healthcare Organization shall ensure an optimal network coverage and stability, and train the users in the management of these temporary disconnections.

Further details on the required features of the local network (including the wireless network) where the Digistat Suite is installed are available in the *Digistat Suite Installation* and *Configuration Manuals*.

4. Before starting

4.1 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.

Installation, 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 recommended for the healthcare organization using the Product to stipulate a maintenance contract with Ascom UMS or an authorized Distributor.

The Product 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 the Product 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.

- Use third party devices recommended by Ascom UMS/Distributors.
- Only trained and authorized people can install 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 stops functioning.

4.2 Privacy Policy

Appropriate precautions shall 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 the data defined in "EU general data protection regulation 2016/679 (GDPR)" as "Special categories of personal data".

Special categories of personal data:
(...) Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and (...) genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

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 and displays personal data.
The Product can be configured to automatically hide in the application screens when no user is logged in the subset of personal data 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 "Digistat Configuration Application", set the system option named "Privacy Mode" to "true" (see the Digistat configuration and installation manual 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.
- Personal 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 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 system from unauthorized accesses.
- Personal data can be present inside some reports produced by the Product. The healthcare organization needs to manage these documents according to the current standards on privacy and personal data protection.
- 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 shall 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:
  1. the updated list of the system administrators and maintenance personnel;
  2. the signed forms of assignment and the certifications of attendance at the training courses;
  3. a register of credentials, permissions and privileges granted to the users;
  4. 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.

⚠	Databases containing patient data/sensible information cannot leave the healthcare organization without being encrypted/obfuscated.

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

⚠	In some circumstances, personal 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 organization is responsible for providing adequate security measures to comply with the local privacy laws and regulations.

⚠	It is suggested to configure the database server so that the Product database is encrypted on the disk. To enable this option it is required SQL Server Enterprise Edition and during its installation it is necessary to enable the TDE (Transparent Data Encryption) option.

4.2.1 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.

- 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.
See “Digistat installation and configuration manual” for detailed information on user account creation procedures and password configuration.

4.2.2 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 database and act as “System Administrator” for the Product.

Ascom UMS/Distributor adopts procedures and working instructions complying with the current privacy regulation (“General Data Protection Regulation - EU 2016/679”).

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.

4.2.3 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.

4.2.4 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.

4.3 Compatible devices

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

	The product receives data from several sources: medical devices, hospital information systems and manually entered by the user. 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 designed to verify that connected devices are working correctly but rather to acquire and catalog clinical data.

	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.

	The correctness of parameters currently displayed by Digistat Docs must always be double-checked on the original medical device that generated them.

	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 case of electrical black-out, it takes a few minutes for Digistat Docs to be fully operative again and display data.

4.4 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.

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

The product tries to recover automatically. If automatic recovery fails, it is necessary to contact the technical assistance (see section 5 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 such procedure.
See section 5 for the contacts list.

5. 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