Digistat® Care
User Manual

Version 21.0

2025-01-14

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® Care version 2.2
Digistat® Care is manufactured by Ascom UMS (http://www.ascom.com).

Digistat® Care is CE 2460 marked according to Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices (MDR).

Ascom UMS is certified according to EN ISO 13485:2016 with the following scope: “Product and Specification development, marketing, sales, production, installation and servicing of information, communication and workflow solutions for healthcare including software and integration with medical devices and patient related information systems. Marketing, sales and installation of information, communication and workflow solutions for healthcare including hardware and software.”

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

Trademarks and copyright

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 modules in use in the Healthcare Organization.

USR ENG Controlbar
USR ENG Control Bar Web
USR ENG Smart Central
USR ENG Fluid Balance
USR ENG Fluid Balance Web
USR ENG Infusion
USR ENG Patient Explorer
USR ENG Patient Explorer Web
USR ENG Scoring Calculator
USR ENG Smart Monitor
USR ENG Smart Monitor Web
USR ENG Therapy
USR ENG Therapy Web
USR ENG MDI Web
USR ENG Vitals Web
USR ENG Smart Central Mobile
USR ENG BCMA (Mobile)
USR ENG Vitals Mobile
USR ENG Mobile Launcher
USR ENG CDSS Configurator Mobile
USR ENG Digistat Gateway
USR ENG multiAssist Module

1.1 Aims

This manual provides all the necessary information for a safe and correct use of Digistat Care 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 Care 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 Care must only be granted to professionally qualified and authorized, trained personnel, with the exception of lay users for limited functions (such exception is specified in the related Instructions for Use).
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.

Images 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 when installed into production.

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 Care. These may be explanatory examples, alternative procedures or any “extra” information considered useful to a better understanding of the product.

Warning

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 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, that are:

- Digistat Docs (not a medical device);
- Digistat Care (Class IIb medical device in the EU according to MDR).

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 in the EU according to MDR.

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 main menu displays a window containing information on the Digistat Suite version, the products 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 “Commission Implementing Regulation (EU) 2021/2226” of 14 December 2021, 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 Care

Digistat Care is a patient data management system and alarm system implementing a set of different functionalities.
Digistat Care makes it possible to display dashboards for the near real time monitoring of the patients, to add new collected parameters inside the system, to provide a way to calculate new derived parameters (ex. scores or CDSS).
Digistat Care integrates with selected medical devices (e.g. infusion pumps, patient monitor, ventilator, dialysis machine, etc.) in order to display, on workstation PCs and selected smartphones, a secondary notification of events and alerts to clinical users.
Digistat Care is able to display data both from devices intended to be used in a reliable distributed alarm system and from devices intended to be used in a distributed information system (not reliable).
Digistat Care is designed to provide an overview of the devices status, highlighting alarms and/or warnings occurring on selected connected device, so that the user is informed at a glance about the situation in the ward.
Besides, Digistat Care introduces wearables support. Digistat Care also provides additional information to the clinicians such as scoring systems (even in combination with wearables) and clinical decision support (e.g. automatic fluid balance calculation, drugs interaction or patient's allergy notification).

2.1 Intended Purpose

Digistat Care (hereafter "Product") is a software that transfers, stores, elaborates, aggregates, organizes and displays patient information and patient related data, including data and events from medical devices and systems as well as information entered manually, in order to drive clinical management providing information to:

- Support treatment, diagnoses, prevention, monitoring, prediction, prognosis and mitigation of disease.
- Triage or identify early signs of disease or conditions.

The Product includes:

- Collection of clinical data and events from medical devices and systems in near real-time;
- Collection of data entered by the user;
- Configurable processing/filters to optimize/reduce the frequency and number of event notifications to healthcare professionals in order to present clinically actionable information;
- Visualization of patient data and device status information in near real time and retrospectively, to healthcare professionals on designated display device(s);
- Integrator and Communicators of a distributed information system (DIS) intended to provide healthcare professional notification of physiological and technical alarms together with supplemental clinical and non-clinical data to support the monitoring of patients;
- Integrator and Communicators of a distributed alarm system (DAS/CDAS) intended to reliably forward and deliver physiological and technical alarms from selected source

devices and systems to healthcare professionals on designated display devices and to specified systems;
- Elaborations of data to provide additional information to the clinician such as scoring systems and clinical decision support;
- Transferring the acquired information to external, clinical and non-clinical systems, in near real-time via a subscription interface, or retrospectively via data query.

The Product is 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 Docs, the other product of the Digistat Suite.
The Product is used in healthcare facilities in critical care units, sub-intensive units, general wards and other departments and for limited functions at patient home.
The patient population and patient conditions are established by the connected medical devices and 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.

Intended purpose Information:

- The software supports scoring systems and a clinical decision support system engine; however no clinical scores nor algorithms in the clinical decision support system are provided by default. The software can perform such automated calculations after these are configured according to and validated by the end-users / customers.
- Data and clinical events managed by the software mostly depend on its configuration: the software can transfer, store, elaborate, aggregate, organize and display clinical data and events coming from user input or from any other source that has a data output compatible with the software and configured during the installation phase. Similarly, the data output of the software, such as the aforementioned scoring calculations or the medical devices available on site that are connected to the software, depend on the configuration of the software itself.

2.2 Patient Benefits / Claims

The Product:

- Reduces the number of alert messages received by caregivers, thereby aiming at reducing alarm fatigue;
- Alert messages are delivered in near real-time, with the aim to shorten caregiver response time;
- Alert messages are delivered in near real-time, with the aim to support caregivers in targeting critical alarms;
- Improves workflow efficiency for the healthcare personnel;

- Helps organize patient care;
- Monitoring infusions helps in keeping infusion continuity that is an important aspect for the patient safety;
- Patient data are automatically collected, with the aim to reduce transcription errors.

2.3 “Off-label” use of the Product

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

2.4 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

2.5 User groups

The User Groups of the Product are defined as following: “Users Reacting on Alerts, Nurses, Medical Doctors, Technical Users and Patients”.
The user reacting on alerts are primary users that include Medical Doctor, Registered Nurse, Nurse Assistant, Charge Nurse and Nurse Practitioner. Those users can view and act on alerts that are handled by the Product.
Nurses group include Registered Nurse, Nurse Assistant, Charge Nurse and Nurse Practitioner and together with Medical Doctors manage patient data in the Product to support the patient care, i.e. update patient chart, monitor and record vital parameters, define and document treatment plan, etc.
The Technical Users group is related only to the installation and configuration of the system. Technical Users are secondary users that include Service Engineer, Field Engineer, Support Engineer, Biomedical Engineer and Technical Instructor.
The patients act as users only for limited functions of the product: these functions however do not include in any terms indications on diagnosis or treatment. In those limited functions, the patient can manually enter vital parameters measurements and can view the vital parameters automatically acquired from connected third party medical devices (e.g. wearable devices).

2.6 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.
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 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 correctly interpret the information supplied and to implement the appropriate safety procedures.
The Healthcare Organization is responsible to define a disaster recovery plan; best practices include, but are not limited to, business continuity and data backup policies.

The Digistat Suite provides a solution that can support the Healthcare Organization in the implementation of a business continuity policy. See details about the Export Scheduler component in the Installation and Configuration manuals.

2.7 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 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 when the connected medical devices does not support it; 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.

2.8 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 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

The product is not designed nor provides functions for consulting or storing the generated documentation.
The documents generated are dynamically produced based on the data and configurations available at the time of their creation.
Accordingly, subsequent printouts cannot be guaranteed to maintain the same content or format as previous versions.
It is recommended to store an official digital copy for any verification purposes.

2.9 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.

2.10 Product traceability

In order to ensure device traceability and on site corrective actions, in compliance EN 13485 and MDR 2017/745, 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 section 1.6).
In case of doubts/questions about Product identification please contact ASCOM UMS/Distributor technical assistance (for contacts see section 5).

2.11 Post-market surveillance

The CE 2460 marked device in compliance with MDR 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 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.

2.12 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. 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 section 3.1.3.

3.1 Central & Bedside

3.1.1 Hardware

Minimum hardware requirements:

- x64 processor (for example: Intel® i3);
- 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.
- 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:

- x64 processor (for example: Intel® i3);
- 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%.

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. The Product 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 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):

- x64 processor (for example: Intel® i5) 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):

- x64 processor (for example: Intel® i7) 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):

- x64 processor (for example: Intel® i5) 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):

- x64 processor (for example: Intel® i7) with 8 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 2016;
- Microsoft SQL Server 2017;
- Microsoft SQL Server 2019.
- Microsoft SQL Server 2022;
- Microsoft SQL Server 2022 Express.

3.4 Digistat Mobile

Digistat mobile is compatible with Android devices from version 5.1 up to 13.0. Compatibility has been verified on Myco 3 and Myco 4 devices.
The application is designed to be compatible with other Android devices with a minimum screen size of 3.5'', and compatibility with a specific device must be verified before clinical use.

Vitals Mobile, BCMA and CDSS Configurator Mobile modules of Digistat Mobile are compatible with Android 6.0+ devices.

After the installation of Digistat Mobile, prior to clinical use, in case the selected devices are not Myco 3 or Myco 4, compatibility verification and validation must be performed, according to the detailed steps defined in Digistat Mobile compatibilty checklist ACDM-585-12771 document.

3.5 Digistat Gateway

Digistat Gateway is compatible with Android devices from version 9.0 up to 13.0. Compatibility has been verified on Myco 3 and Myco 4 devices.
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.

	After the installation of Digistat Gateway, prior to clinical use, in case the selected devices are not Myco 3 or Myco 4, compatibility verification and validation must be performed, according to the detailed steps defined in Digistat Gateway compatibilty checklist ACDM-585-13656.

3.6 Digistat Web

The following browsers are supported for use with Digistat Web applications:

- Chrome 126 or later
- Firefox 127 or later
- Edge 127 or later

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

	Do not use more than one browser simultaneously.

	Do not to use the incognito mode.

	In case Digistat Web is used to display notifications produced by the Clinical Decision Support System, the Healthcare organization should evaluate to apply the following mitigations: the web browser of a Digistat Web workstation must always be in foreground. The web browser must be dedicated only to Digistat Web, no other use must be allowed. Therefore, the default homepage of the web browser must be Digistat Web.

	Digistat Web uses Cookies to store information about the current working session. Cookies are linked to the web domain of the applications. Therefore, if Digistat Web modules and components are installed on different servers, it is necessary to adopt a Load Balancer so to use URLs with a common web domain thus allowing cookies consistency. Furthermore, the Load Balancer shall be configured so that https calls are redirected to the correct server. For example: we want to install Vitals Web on a Server and Vitals Web API on another server. The Load Balancer must be configured so that https calls like https://MYDOMAIN/VitalsWeb are routed to the server where Vitals Web is installed, and https calls like https://MYDOMAIN/VitalsWebAPI are routed to the other server.”

3.7 Ascom Telligence

Digistat Care is compatible with the Ascom Telligence.
Ascom Telligence supported versions: 6.10, 7.0, 7.1, 7.3.

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

3.8 General Warnings

In case the Product is used for primary notification of alarms, at least two client workstations must be installed within the same department or, alternatively, at least one Digistat Care workstation and a third party signalizing system (e.g. an Alarm Light Tower).

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 Healthcare Organization shall provide a “Time server” (i.e. a Server that provides a unique, shared reference for date and time); all servers and workstations where the Digistat Suite is installed must use the date/time of the Time Server

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.

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.

3.9 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.

3.10 Firewall and Antivirus

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

To protect the 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 Digistat Suite with WithSecure (formerly F-SECURE) Antivirus using proper exclusions for the "./Server" folder where the Digistat Suite Server is installed. However, considering the strategies and policies already existing in the Healthcare Organization, the actual choice of the antivirus is responsibility of the Healthcare Organization.

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.

Ascom UMS cannot ensure that the Digistat Suite is compatible with any antivirus or anti-malware other than WithSecure (formerly F-SECURE).
Severe incompatibilities (e.g. memory leaks, more than 20 seconds delay for messages exchange, etc.) have been reported between Digistat and other antivirus/anti-malware software. Make sure to set an exclusion for the entire "./Server" folder where the Digistat Suite Server in installed.
Here a list of antivirus that caused proven incompatibilities with Digistat:

- Windows Defender
- Kaspersky
- Trend Micro Apex One

Some antiviruses delegate real-time protection to the Microsoft Windows Defender antivirus. Always check that the Windows Defender antivirus is not present in the servers by checking the "Virus & threat protection" section in the Windows settings. If present, make sure to add the aforementioned exclusion of the Digistat Server folder.

3.10.1 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.

3.11 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 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 WiFi connections, given the possible intermittency of the WiFi connection, network disconnections are possible, that cause the activation of the “Recovery or Disconnected Mode” which in case the 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 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 warning

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 procedures and guidelines only by Ascom/Distributor technicians or personnel trained and authorized by Ascom/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 personnel can install third party devices.
- The Healthcare Organization shall ensure that the installation and 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/or 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.

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 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:
    a. the updated list of the system administrators and maintenance personnel;
    b. the signed forms of assignment and the certifications of attendance at the training courses;
    c. a register of credentials, permissions and privileges granted to the users;
    d. 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 Product 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 Product 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 the Product 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 the Product configuration manual for the configuration procedures.

4.2.4 Forensic logs

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

4.3.1 DAS devices

These are devices enabling the implementation of a reliable distributed alarm system.
Data acquired by this kind of devices are displayed on the Product.
Data acquired by this kind of devices can also be output as HL7. **HL7 output communication is not reliable.**

Supported devices:

- *Hamilton ventilator S1 and C6 and other models supporting the same protocol.*
- *Arcomed Syramed µSP6000 and Volumed µVP7000 infusion pumps connected to Arcomed UniQueConcept rack (and other devices supporting the same protocol).*
- *Medical devices connected to the Dräger Targeted Alarm Service.*

To use the supported devices in a Distributed Alarm System it is necessary to properly configure the communication settings of the devices according to the manufacturer technical documentation.

Hamilton Devices
The Hamilton ventilator supports the "silent ICU option". This means that it can be used, with Digistat Care, to operate in a silent mode.
To use the Hamilton ventilator in a Distributed Alarm System as silent ventilator (e.g. in a silent ICU), it is possible to operate it in a global AUDIO OFF state.
First, the ventilator will be correctly configured. See the device technical documentation for the technical and user instructions on how to operate it in silent mode (AUDIO OFF state).

Refer to the Hamilton Ventilator documentation for detailed instructions.

The maximum delay measured in a test environment between the Hamilton ventilator device connection and the data display on the Product is 22900 ms.
The maximum delay measured in a test environment between the Hamilton ventilator device connection and the data display on the Product (Mobile version) is 20233 ms.

The maximum delay measured in a test environment between the notification display on the Hamilton ventilator and the notification display on the Product is 600 ms
The maximum delay measured in a test environment between the notification display on the ventilator and the notification display on the Product (Mobile version) is 1000 ms.

It can take up to two seconds between the alarm generation and the alarm sending on the Hamilton ventilator.
The ventilator then waits for an acknowledgement from the Product. If such acknowledgement is not received within two seconds a timeout occurs.

Therefore the maximum delay after which an alarm notification is provided is 4 seconds.

If there is a timeout:

- A connection alarm is triggered. The alarm can be canceled by the user. It is also canceled if a new connection with Confirmed Delivery is established.
- Any active AUDIO OFF state is canceled.
- Ventilator data sending and Confirmed Delivery is stopped until a new connection is established. If Digistat Care is not in Reliable state, it immediately attempts to restore connection without Confirmed Delivery.

In case the Hamilton ventilators are configured as part of a Distributed Alarm System, the global AUDIO OFF state is automatically disabled if one of the following conditions occurs:

- The Hamilton driver results unavailable;
- The DAS system results not reliable.

Arcomed Devices

The Arcomed pump / rack supports the "silent ICU option". This means that it can be used, with Digistat Care, to operate in silent mode.
To use the Arcomed pump / rack in a Distributed Alarm System as silent pump / rack (e.g. in a silent ICU), it is possible to operate it in a global AUDIO OFF state.
First, the pump / rack shall be correctly configured. See the device technical documentation for the technical and user instructions on how to operate it in silent mode (AUDIO OFF state).

Refer to the Arcomed pump / rack documentation for detailed instructions.

The maximum delay measured in a test environment between the notification display on the Arcomed pump / rack and the notification display on Digistat Care is 3927 ms.
The maximum delay measured in a test environment between the notification display on the ventilator and the notification display on Digistat Care (mobile version) is 4350 ms.

The maximum delay measured in a test environment between the Arcomed pump / rack device connection and the data display on Digistat Care is 63 s.
The maximum delay measured in a test environment between the Arcomed pump / rack device connection and the data display on Digistat Care (Mobile version) is 63 s.

It can take up to 10 seconds between the alarm generation and the alarm sending on the Arcomed pumps / racks. The pump / rack then waits for an acknowledgement from Digistat Care. If such acknowledgement is not received within 20 seconds a timeout occurs.
Therefore, the maximum delay after which an alarm notification is provided is 20 seconds.
If there is a communication timeout:

- A connection alarm is triggered on the pumps. The alarm can be canceled by the user. It is also canceled if a new connection with Confirmed Delivery is established.
- Any active AUDIO OFF state is canceled.
- If a new connection with Confirmed Delivery is established and if Digistat Care is in Reliable state, the AUDIO OFF state is automatically restored by the infusion pumps.
- Digistat Care attempts to restore communication.

Arcomed Infusion Pumps require a separate network to work as part of a Distributed Alarm System. “Separate network” means: different physical network, VLAN or separate IP subnets. This is required to prevent possible conflicts with a particular network security policy, as indicated by the manufacturer of the pump / rack.

In case the Arcomed pumps are configured as part of a Distributed Alarm System, the global AUDIO OFF state is automatically disabled if one of the following conditions occurs:

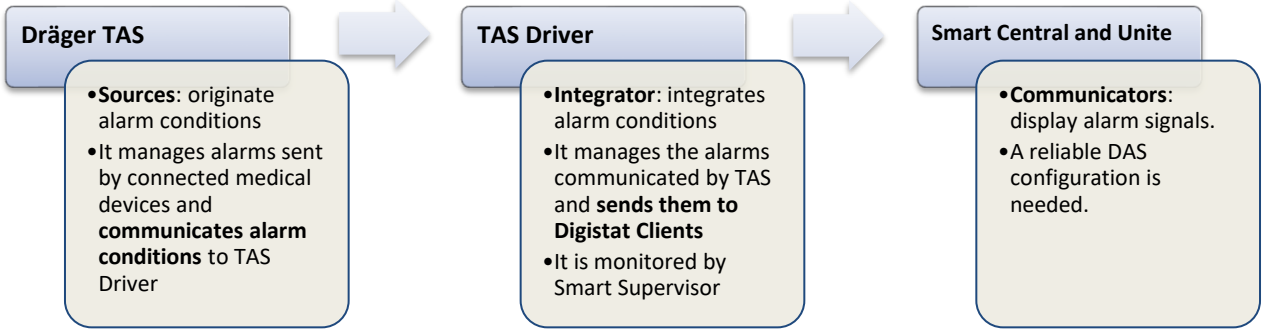
- The Arcomed driver results unavailable;
- The DAS system results not reliable.

Arcomed driver is a multibed driver, so a single rack could be in unreliable state while the others are reliably working.

Medical devices connected to the Dräger Targeted Alarm Service

In a Distributed Alarm System with the TAS Draeger, there must be at least two Medical Devices (AlertProvider) with the shortest Selfcheck time.
Refer to the instructions for use of the TAS Draeger server for further information.

The **Targeted Alarm Service** (TAS) **Driver** acts as an alarm gateway and **Integrator** (according to the IEC 60601-1-8:2020 standard) of **alarm conditions** originated from **medical devices** connected to the Dräger private network. Medical devices in the Dräger private network are communicating with the **Dräger Targeted Alarm Service gateway** (TAS gateway), according to standard SDC communication protocol (IEEE 11073). Dräger TAS forwards alarm conditions to the TAS Driver that delivers them to **Digistat communicators**, such as Smart Central and Unite, where the alarm signals are finally displayed.



The TAS communicates to the TAS Driver through TAS Protocol version 1.1 the alert conditions of the devices connected to the TAS network (up to 100 devices per TAS). The TAS Driver supports an encrypted connection and authentication according to the TLS 1.2 security requirements and the correctness of the messages is guaranteed by the TCP/IP protocol.

The TAS Driver is a DAS-type driver, and it supports **Global AUDIO OFF** status active on medical devices. Together with Dräger TAS Gateway, it can be configured to implement **a Distributed Alarm System** (DAS), that requires a reliable configuration with active **Smart Supervisor** ("System Option" *SmartCentralMode* set to **Reliability** or **Monitoring and Reliability**) and **dual Smart Central**.

The TAS gateway can send alerts in more than one language at the same time. By default, the driver uses the language set for Data Acquisition Node (system option *Language* with application *DASNODE*). Is possible to override the language and set one or more different languages in the TAS Driver. In case the alert language received from the medical devices is different from the language configured, the alert language will be reported together with the alarm text received from the TAS gateway together with a warning about the impossibility of finding a suitable translation.

During configuration, the custom parameter BedNameFormat must be set on the page Edit Device Driver > Custom Parameters > Custom tab (Configurator Web > Connect > Drivers > Device driver management, then select the TAS driver instance) of the TAS driver instance to manage bed mapping.

Depending on the configuration of the devices connected to the TAS, the use of mixed languages for the alarm texts is possible.

If the product is used for primary notification of alarms, any physical device connected to it via the TAS device (manufactured by Dräger) that supports the enabling of GLOBAL AUDIO OFF (as defined by IEC 60601-1-8), must disable the GLOBAL AUDIO OFF in case of:

- a failure of the Distributed Alarm System or
- a disconnection of the physical device (e.g., from the Hospital network, from the TAS device, from the Distributed Alarm System, etc.).

The technician who is in charge of configuring the Digistat TAS Driver must double-check that the certificate received by Dräger corresponds to the one used by the TAS Server using at least two different means (e.g., by mail and by voice).

Delay measurements were executed on a Dräger Babylog VN800 ventilator, connected to the Dräger private network.
The maximum delay measured in a test environment between the notification display on the Dräger Babylog VN800 ventilator and the notification display on Digistat Care is 500 ms. The maximum delay measured in a test environment between the notification display on the ventilator and the notification display on Digistat Care (mobile version) is 900 ms.

4.3.2 DIS devices

These devices don't allow the implementation of a reliable distributed alarm system. This communication is not reliable, therefore it cannot be used to implement a reliable Distributed Alarm System (DAS/CDAS). Therefore, they can only be used to implement a Distributed information System (DIS). Please contact Ascom UMS/Distributor for the updated list of available devices.

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 notification generation and the actual notification 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 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 a notification, it takes maximum 1 second to display it on the user interface.

4.3.3 Warnings

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. scoring).
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.

Depending on the characteristics of the connected medical devices, the Product can be used for primary (DAS/CDAS) or secondary (DIS) notification of alarms. The presence of a single DIS device requires the application to show a warning stating that some of the connected devices do not support primary notification of alarms.

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 is 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 the Product both when notification sounds are disabled and when enabled for a specific patient on the mobile device.

In case an infusion pump is connected to the Product, do not modify the infusion pump Serial Number.

Never disable the audio on the workstations on which the Product is running.

According to the decision of the Healthcare Organization, the product 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.

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.
These two statements are 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 is in the range of 100 lx to 1 500 lx,
- the screen where the User Interface of the Product is shown is at least a 22 inches monitor with Full HD resolution (1.920 x 1.080).

The Healthcare Organization, according to its risk management policy and depending on the environment where Digistat Care is executed (e.g. size of the monitor, monitor color settings, placement of the workstation in the ward, etc.), can define the actual maximum distance for the Operator to see that an alarm is present.

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

Use 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 installed, then the procedure is not relevant.

If the generic Alaris® Driver is in use it is necessary to wait at least ten seconds after disconnecting an infusion pump before connecting another one.

Sound pressure levels below ambient noise can impede user perception of alarms.

The Product acquires the information generated by the primary medical devices (i.e. pulmonary ventilators, infusion pumps, etc.) and displays them. Therefore, the Product always reports what the primary medical devices communicates. The assignment of alarm priorities is decided according to the primary medical device. On the Product 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 the Product 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

4.4 Single Fault Safe Distribution of Alarms

Depending on the characteristics of the connected medical devices, the product can be single fault safe with respect to the distribution of alarms, if installed and configured accordingly. That means that every part of the system involved in the distribution of alarms is constantly monitored, including the “controller” itself (i.e. the monitoring agent) and, if any fault occurs in any of these parts, a notification is provided to the users. In case of fault, the Product stops operating until the fault cause is detected and removed.
For the mobile workstations (Myco devices), in the same conditions described above a notification is provided to all the connected devices. This notification has the same severity level of a clinical alarm and cannot be removed until the cause is removed.
To ensure single fault safety, at least two Digistat Care workstations shall be installed within the same department or, alternatively, at least one Digistat Care workstation and a third party signalizing system (e.g. an Alarm Light Tower).
Each workstation or light tower can this way monitor the correct functioning of the other components. Desktop workstations and the light tower also monitor the “Controller”. See the Product configuration manual for a detailed description of the system’s architecture.

The healthcare organization shall implement internal procedures in order to always assure the presence of at least one clinical staff member near each Digistat Care Desktop workstation and, if present, the alarm light tower, to promptly be aware of any alarm.

The healthcare organization shall implement adequate procedures to bring the Product back to its functionality in the shortest time possible. Also, the healthcare organization shall define alternative working procedures in case the system becomes unreliable or stops functioning.

4.4.1 Alarm Light Tower

Digistat Care is designed to communicate with an optional off-the-shelf alarm light tower using a standard protocol. When Digistat Care is installed and configured for the reliable distribution of alarms, the Light Tower produces visual and audible informative notifications, redundantly informing users if the system is working properly or not.
The light tower can be used as an alternative to the second Digistat Care workstation, that is otherwise mandatory for the reliable distribution of alarms.

The presence of the light tower depends on a system option. If the light tower is present, then the system can be validated as reliable with only one Digistat Care workstation. See the Product configuration manual for more information.
On the light tower:

- the green light is on and no sound is provided if the system is working correctly;
- the red light turns on and an alarm sound is provided when a technical alarm occurs (a system fault - see sections 4.5 and 4.5.3);
- the red light turns on and an alarm sound is provided when the communication between the light tower and the Smart Supervisor (the “controller” mentioned above) is interrupted; at the same time the Smart Supervisor provides a technical alarm when the communication with the light tower is interrupted.

Verification of Digistat Care has been performed with the Network Monitor Signal Tower by Patlite, but other models could be compatible with Digistat Care. For more information contact Ascom UMS/Distributor technical assistance.
The Network Monitor Signal Tower by Patlite is a three-tiered signal tower with a buzzer. It has the capability to report immediately when a network event occurs via network connection.

Fig 1

4.5 System unreliability

In case the system becomes unreliable, a specific “System error” notification is provided on the desktop workstations (Fig 2), on the handheld devices and on the optional alarm light tower (red light on, alarm sound).

When a “System error” that could compromise data validity occurs, in all involved beds no patient data is displayed until the system becomes reliable again.

Possible unreliability causes are listed in paragraph 4.5.3.

4.5.1 Desktop

On the desktop workstations the notifications remain on the lateral bar (Fig 2 **B**) until the unreliability causes are removed and the system is reliable again. In all the beds involved with the unreliability, no patient data is displayed until the system is reliable again.

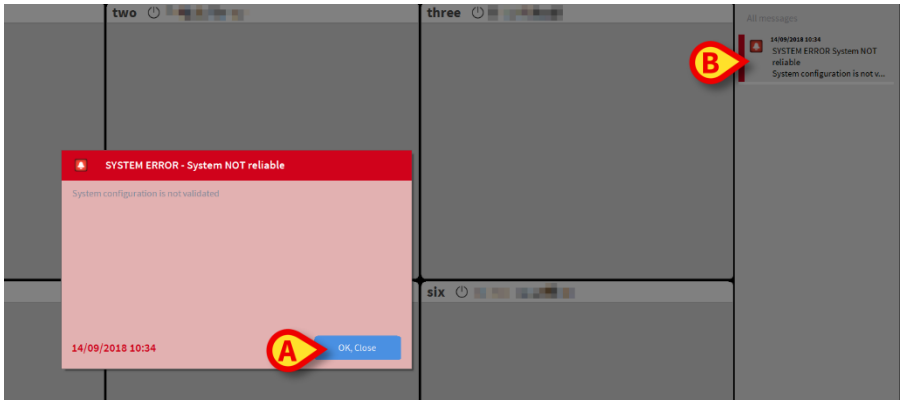


Fig 2 - System not reliable (desktop)

- Click **Ok, Close** on the notification to acknowledge it (Fig 2 **A**).

4.5.2 Mobile

On the mobile devices, a “System error” notification is provided. A sound/vibration alarm is also provided.

- Swipe the notification down to acknowledge it on the mobile. After this action the sound/vibration stops.

A warning remains on top of every screen of the mobile until the unreliability causes are removed and the system is reliable again. In all the beds involved with the unreliability, no patient data is displayed until the system is reliable again.

4.5.3 Unreliability causes

In case of system unreliability a technical alarm is provided. The alarm is a “System error” notification, which also provides a short description of the unreliability causes.
The possible unreliability causes are the following:

- "System configuration is not validated"
- “Smart Central is not working properly. Unmanaged errors. Contact System Administrators.”
- “Light Tower ({0}) connection error”
- "Reply timeout on external CDAS system"
- "External CDAS system disconnected"
- “Error accessing database”
- “Anomaly in component {0} ({1})”
- “Component {0} ({1}) does not respond”
- “Driver {0} on {1} does not respond”
- Free text sent from device driver

NOTE: characters “{0} and {1}” represent the name of the actual component.

When a “System error” that could compromise data validity occurs, in all involved beds no patient data is displayed until the system becomes reliable again.

4.6 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.

The features and functionalities described in sections 4.4 and 4.5 are also applicable when the product is not installed and configured for primary distribution of alarms (e.g.: when the communication protocol of the medical device is not intended for this purpose).
In these cases, the abovementioned features and functionalities work as additional, redundant safety mechanism supervising the components of the product. They may or may not supervise the connection with the medical devices depending on the product configuration and technical characteristic of the medical device.

Under these conditions the entire system cannot be considered single fault safe and cannot be used for reliable, primary communication of alarms.

5. Contacts

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

UK Responsible Person: Ascom (UK) LTD., Wall Island, Birmingham Rd, Lichfield WS14 0QP, United Kingdom

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