

CARESCAPE B850

Service Manual

CARESCAPE Software version 3 (3.2.758)

Version MBC323



CARESCAPE B850

English

2nd edition

5817395-01

© 2020, 2022 General Electric Company.
All rights reserved.

Due to continuing product innovation, specifications in this manual are subject to change without notice.

For technical documentation purposes, the abbreviation GE is used for the legal entity names, GE Medical Systems *Information Technologies*, Inc. and GE Healthcare Finland Oy.

Contents

1	About this manual	13
	Intended use of this manual.....	13
	Intended audience of this manual.....	13
	Manual conventions	13
	Monitor naming conventions	14
	Acquisition module naming conventions	14
	Other naming conventions.....	14
	Illustrations and names.....	15
	Related documents.....	15
	Revision history	16
	Accessing manuals online.....	16
	Product availability	17
	Trademarks	17
	Third party trademarks.....	17
	Manufacturer responsibility	17
2	Safety	19
	Safety message signal words.....	19
	Safety symbols.....	19
	System safety.....	20
	Reporting of serious incidents.....	20
3	System introduction	23
	Short description of the equipment.....	23
	CPU unit.....	23
	Software	24
	Displays.....	24
	B850 system components.....	25
	CARESCAPE ONE.....	27
	CARESCAPE Dock F0 side views.....	28
	Acquisition modules.....	28
	PDM front view	28
	Modules and parameters	29

CARESCAPE Network.....	31
Other system components.....	32
Access to external applications	33
Controls and connectors	33
B850 display front view.....	33
B850 display back view.....	35
B850 processing unit front view.....	35
B850 processing unit back view.....	36
F5 Frame, 5-module frame.....	37
F7 Frame, 7-module frame.....	38
IEC 60601-1	38
IEC 60601-1-2.....	38
IEC 60529.....	39
Equipment markings.....	39
Unique Device Identifier (UDI).....	46
User interface indicators	47
Service requirements.....	51
Product security	52
4 Using the service applications	53
Introduction to the service applications.....	53
CARESCAPE First Use Wizard.....	53
CARESCAPE Service interface.....	54
CARESCAPE Multi Monitor Manager.....	55
Service calibrations.....	55
InSite RSvP	55
User accounts and passwords for service applications.....	55
Accessing the service interface locally from the monitor	55
Accessing the service applications with a service PC	56
Checking the network settings of the target monitor.....	56
Configuring the network settings of the service PC.....	56
Supported web browsers in service PC	57
Secure access with service PC	57
Accessing the service applications locally with a service PC.....	57

Accessing the service applications over IX network with a service PC	58
Accessing service calibrations	60
5 Pre-installation requirements	61
Unpacking	61
Pre-installation checklist.....	61
System compatibility	61
Important security information.....	62
Checking the configuration of the wired CARESCAPE Network infrastructure	62
About the monitor's MAC addresses.....	63
CARESCAPE ONE installation	63
Mounting solutions	63
Unity Network Interface Device (ID).....	64
Power and environmental requirements.....	64
Power requirements.....	64
Environmental requirements.....	64
Electromagnetic compatibility safety precautions	65
6 Hardware installation	67
Hardware installation	67
Installing batteries	67
Installing the PDM battery	68
Installing the CPU	68
Connecting the primary display.....	69
Connecting a secondary display.....	71
Connecting a secondary display with 1 to 5 meter cables.....	72
Connecting a secondary display with 15-meter cables	73
Installing module frames and modules.....	74
Connecting an F5 or an F7 Frame to the CPU	75
Connecting a PDM to an F5 Frame	75
Connecting E-modules.....	76
Connecting a PDM to an ePort connector	76
Connecting CARESCAPE Dock F0 to an ePort connector.....	77
Connecting CARESCAPE Dock F0 with a 1.5- or 4.5-meter cable.....	78

Connecting CARESCAPE Dock F0 with a 30-meter cable	78
Connecting to the mains power.....	79
Connecting to the CARESCAPE Network.....	80
Connecting a Unity Network ID connectivity device to the monitor	80
Connecting USB input devices	81
Connecting iCollect and other data acquisition systems.....	81
Connecting a local printer	82
Connecting a local PRN 50-M+ recorder	82
Connecting to CARESCAPE RAD	83
Connecting a remote-on cable	83
7 Configuration	85
Platform configuration.....	85
Adjusting display	85
Selecting display input signal source.....	85
Adjusting display brightness and picture	85
Setting up the displays.....	85
Calibrating touchscreen	86
Configuring wired CARESCAPE network	86
Configuring the hostname.....	86
Wired LAN Certificate Management	86
Wired CARESCAPE Network configuration	87
Configuring date and time	91
Setting unit and bed name.....	91
Configuring printers.....	92
Adding a printer.....	92
Selecting printout types and print locations.....	93
Printing a test page.....	93
Deleting a printer.....	93
Configuring Citrix	94
MUSE/12SL configuration.....	95
Configuring MUSE/12SL Settings	96
Installing MUSE/12SL certificate	96
Admit settings	97
Configuring patient ID prefix	97

Barcode parser configuration	97
Setting power frequency	102
Selecting language and locale.....	103
Configuring modules.....	103
Configuring module asset number	103
Configuring host asset settings.....	104
Configuring host asset number.....	104
Configuring serial number.....	104
Password management	105
User accounts and passwords.....	105
Password policy.....	106
Changing passwords	107
Resetting passwords.....	108
Configuring CS ONE authentication.....	109
Configuring connectivity.....	109
Configuring remote alarm device.....	109
Restarting the monitor.....	110
Setting up the remote service	110
Enabling or disabling the remote service connection	110
Configuring remote service	111
Settings management.....	111
Settings transfer process.....	111
Downloading clinical and platform settings.....	113
Activating settings.....	114
Resetting to factory settings	116
License management.....	117
Activating host licenses	117
Software packages	118
Uploading license file	119
Backup and restore.....	119
Taking a backup	119
Restoring a backup	120
Certificate management	121
Creating a certificate signing request (CSR)	121

Installing the certificate	122
Viewing the current certificate	122
Software management	123
Software signing.....	123
Software upload	123
Software activation	124
Uploading software.....	124
Activating the host software	125
Activating other software	127
8 Checkout procedures	129
About the checkout procedures.....	129
Required checkout procedures	130
Installation check	130
Planned maintenance check.....	130
Corrective maintenance check	131
Checking the user and service manuals	131
Performing visual inspection.....	131
Performing electrical safety tests	132
Test setup.....	132
Verifying power outlets.....	133
Verifying power cords and plugs.....	134
Ground integrity check	134
Testing earth leakage current	136
Testing touch current.....	137
Patient leakage current tests	139
Completing electrical safety tests.....	144
Performing functional check.....	144
Preparing for the functional check.....	144
Testing the alarm light	144
Checking the startup.....	144
Checking displays.....	145
Checking the status of connected devices.....	145
Testing printing to IX printers	146
Testing InSite RSvP connectivity.....	146

Testing the USB remote control.....	146
Testing the mouse.....	147
Testing the keyboard.....	147
Testing the barcode reader	147
Testing wired MC Network communication	148
Testing Citrix connection	148
Completing the functional check	149
9 Theory of operation.....	151
Main components	151
Power supply	152
CPU assembly.....	152
10 Troubleshooting	157
Troubleshooting guidelines	157
Performing basic troubleshooting.....	157
Viewing configuration and device information.....	158
Information.....	158
Viewing hardware statistics	159
Hardware statistics	160
Pinging a TCP/IP network device.....	160
Viewing log files.....	160
Downloading log files	161
Network status LEDs.....	161
Messages related to various technical issues.....	162
Problems and solutions	174
Troubleshooting startup failures.....	174
User interface issues.....	175
Troubleshooting incorrect system time	177
Troubleshooting license issues.....	177
Troubleshooting MC Network issues.....	178
Troubleshooting IX Network issues.....	179
Recorder troubleshooting.....	180
Troubleshooting acquisition platform.....	180
Troubleshooting CARESCAPE Network communication	182
11 Disassembly and reassembly.....	187

Disassembly guidelines	187
ESD precautions	187
Reassembly precautions.....	187
Required tools.....	188
Preparing for disassembly	188
Disassembly procedures	189
Detaching the top cover	190
Replacing the CPU battery.....	190
Detaching the power supply unit.....	191
Detaching the speaker.....	193
Detaching the front bezel unit.....	195
Detaching the CPU assembly	196
Replacing the bottom enclosure	204
12 Service parts.....	207
Service parts.....	207
Ordering parts	207
Exploded view.....	207
List of FRUs	208
A Display D19KT VER01	211
Disassembly guidelines and precautions	211
Required tools.....	211
Detaching the OSD knob	211
Detaching the trim knob.....	211
Detaching the alarm light cover.....	212
Service parts.....	212
Ordering parts	212
List of FRUs	213
B Multi Monitor Manager	215
Introduction to Multi Monitor Manager	215
Prerequisites for using Multi Monitor Manager	215
Accessing Multi Monitor Manager	216
Software installation to multiple monitors at a time	217
Software signing.....	218
Specifying the target monitors.....	218

Connecting to the target monitors.....	218
Uploading software to the target monitors.....	219
Activating the uploaded software on the target monitors	221
Settings activation to multiple monitors at a time.....	223
Specifying the target monitors for the settings transfer	223
Connecting to the target monitors.....	224
Selecting the settings file and the settings to be transmitted to the target monitors	225
Activating the settings on the target monitors	225
Troubleshooting	226
Authentication statuses.....	226
Software upload statuses.....	228
Software activation statuses.....	229
Settings activation statuses	230
Other issues	231

1

About this manual

Intended use of this manual

The list below indicates the compatible products (brands, models and descriptions as applicable) with which this manual is to be used. Supported products are covered by the manuals that were delivered with those products.

- CARESCAPE B850, version MBC323
- CARESCAPE Software version 3 (3.2.758)
- CARESCAPE D19KT VER01

This manual contains instructions necessary to install, maintain and service the device. It gives an overview of the CARESCAPE B850 patient monitoring system, and contains information needed for system installation, and the planned and corrective maintenance of the CARESCAPE B850 CPU.

Use the manual as a guide for installation, maintenance and repairs considered field repairable. Where necessary the manual identifies additional sources of relevant information and technical assistance.

See the module's service manual for the planned and corrective maintenance of the acquisition module.

See the supplemental information manual for the technical specifications, default settings and compatibility information, including electromagnetic compatibility.

See the user manual for the instructions necessary to operate the device safely in accordance with its function and intended use.

Intended audience of this manual

This manual is intended for service representatives and technical personnel who install, maintain, troubleshoot, or repair this device.

Manual conventions

This manual uses the following styles to emphasize text or indicate an action. Also note the terminology conventions.

Item	Description
bold	Indicates hardware keys and connectors.
<i>italic</i>	Indicates menu options, software keys and messages.
<i>italic</i>	Indicates terms for emphasis.

Item	Description
>	Indicates menu options to select consecutively.
select	The word select means choosing and confirming.
acquisition device	A generic term when referring to both the acquisition modules (PDM, E-modules) and the acquisition platform (CARESCAPE ONE).
supplemental information	In this manual, the phrase supplemental information refers to information that appears in the Supplemental Information Manual or supplements provided.
NOTE	Note statements provide application tips or other useful information.

Monitor naming conventions

In this manual, the CARESCAPE B850 is referred to as the monitor. It may also be referred to as B850.

Acquisition module naming conventions

In this manual, the following naming conventions are used to refer to different modules and module categories:

- PDM: Patient Data Module
- E-modules: All modules with the prefix E-.
- E-COP, E-COPSV
- E-PiCCO
- Pressure E-modules: E-PP, E-PT
- CARESCAPE respiratory modules: E-sCO, E-sCOV, E-sCOVX, E-sCAiO, E-sCAiOV, E-sCAiOVX, E-sCAiOE, E-sCAiOVE
- E-miniC
- Specialty E-modules: E-NMT, E-EEGX, E-BIS, E-ENTROPY
- SpO₂ E-modules: E-NSATX, E-MASIMO
- CARESCAPE Parameter interface module: E-musb

Other naming conventions

For technical documentation purposes, the abbreviation GE is used for the legal entity names, GE Medical Systems *Information Technologies*, Inc., and GE Healthcare Finland Oy.

In this manual, CARESCAPE Network is used to refer to both the IX Network and MC Network except where they need to be differentiated. Then they are referred to as IX Network and MC Network.

In this manual, the CARESCAPE Service interface may also be referred to as service interface.

In this manual, acquisition platform refers to the CARESCAPE ONE acquisition platform. CS ONE may also be used to refer to the CARESCAPE ONE acquisition platform.

In this manual, CARESCAPE Parameters is used as a generic term when referring to all of the following products:

Graphic on the CARESCAPE Parameter	Explanation
CARESCAPE [ECG]	CARESCAPE Parameter for measuring ECG. Note that in the manual, the following name is used instead of the graphic: CARESCAPE ECG.
CARESCAPE [PRES]	CARESCAPE Parameter for measuring invasive pressures. Note that in the manual, the following name is used instead of the graphic: CARESCAPE Pressure.
CARESCAPE [rSO ₂] - INVOS	CARESCAPE Parameter for measuring regional oxygen saturation of blood (rSO ₂) in cerebral and somatic tissues with INVOS technology. Note that in the manual, the following name is used instead of the graphic: CARESCAPE rSO ₂ .
CARESCAPE [TEMP]	CARESCAPE Parameter for measuring temperature. Note that in the manual, the following name is used instead of the graphic: CARESCAPE Temperature.
CARESCAPE [CO ₂] - LoFlo	CARESCAPE Parameter for measuring CO ₂ with Resironics LoFlo technology. Note that in the manual, the following name is used instead of the graphic: CARESCAPE CO ₂ — LoFlo.
CARESCAPE [CO ₂] - Microstream	CARESCAPE Parameter for measuring end-tidal carbon dioxide (EtCO ₂), FiCO ₂ , and respiration rate with Microstream technology. Note that in the manual, the following name is used instead of the graphic: CARESCAPE CO ₂ — Microstream.
CARESCAPE [SpO ₂]	CARESCAPE Parameter for measuring SpO ₂ with GE TruSignal technology. Note that in the manual, the following name is used instead of the graphic: CARESCAPE SpO ₂ .
CARESCAPE [SpO ₂] - Masimo	CARESCAPE Parameter for measuring SpO ₂ with Masimo rainbow SET technology. Note that in the manual, the following name is used instead of the graphic: CARESCAPE SpO ₂ — Masimo.
CARESCAPE [SpO ₂] - Nellcor	CARESCAPE Parameter for measuring SpO ₂ with Nellcor™ sensors with OxiMax™ technology. Note that in the manual, the following name is used instead of the graphic: CARESCAPE SpO ₂ — Nellcor.

In this manual, the following product names are used as generic terms:

- D-lite when referring to D-lite, D-lite+, and D-lite++
- Pedi-lite when referring Pedi-lite and Pedi-lite+
- D-fend Pro when referring to D-fend Pro and D-fend Pro+

Illustrations and names

This manual uses illustrations as examples only. Illustrations in this manual may not necessarily reflect all system settings, features, configurations, or displayed data.

Names of persons, institutions, and places and related information are fictitious; any similarity to actual persons, entities, or places is purely coincidental.

Related documents

- CARESCAPE B850, B650, B450 User Manual
- CARESCAPE B850, B650, B450 Privacy and Security Manual

- CARESCAPE B850, B650, B450 Supplemental Information Manual
 - CARESCAPE ONE Service Manual
 - Service manuals for acquisition modules and module frames
 - CARESCAPE Network Configuration Guide
 - Patient Monitoring Network Configuration Guide
 - CARESCAPE Modular Monitors Mounting Solutions
 - CARESCAPE RAD Service Manual
 - CARESCAPE Citrix Guide
 - Service documentation for displays
 - Unity Network Interface Device (ID) Service Manual
 - iCollect user's manual
 - PRN 50-M+ Writer Service Manual
 - Service documentation for laser printers
 - Cleaning and Disinfecting Supplement
 - Supplies and Accessories Supplement
 - Instructions for use for CARESCAPE rSO₂— INVOS, REF: PMC71V-GE
 - Instructions for use for CARESCAPE CO₂ — Microstream, REF: PMC40M-GE
- For a list of third-party or open-source software included in the device, please contact your GE service representative.

Revision history

Revision	Description
1st edition	Initial release.
2nd edition	Updated for CARESCAPE Software version 3 (3.2.758) release. Introduced new EAP methods (TLS, TTLS-MSCHAPV2, and PEAP-GTC) for IEEE 802.1X port-based authentication to control access to MC and IX networks.

Accessing manuals online

To obtain the latest version of the manual:

1. Go to: <https://www.healthcare.com/documentationlibrary>.
2. Enter the Customer Documentation Portal.
3. Select **Modality > Monitoring Solutions (MS)**.
4. Select **Products** > the products you want to search.
You may also select the **Document Type** and **Language** to narrow down the search.
5. Launch the search.
6. Identify and download the manual.

The manuals are in pdf format. Make sure that your viewing device (e.g., computer) has software to open the pdf files (for instance, Adobe® Acrobat® Reader).

Security related documents can be downloaded from
<https://securityupdate.gehealthcare.com>.

Product availability

NOTE

Due to continual product innovation, design and specifications for these products are subject to change without notice.

Some of the products mentioned in this manual may not be available in all countries. Please consult your local representative for the availability.

Trademarks

GE, GE Monogram, and CARESCAPE are trademarks of General Electric Company.

MUSE, Trim Knob, UNITY NETWORK, D-lite, D-fend, and Entropy are trademarks of General Electric Company or one of its subsidiaries.

Third party trademarks

Masimo SET is a trademark of Masimo Corporation.

Covidien, BISx, BIS, INVOS, and Microstream are trademarks of a Medtronic company.

PiCCO is a trademark of Pulsion Medical Systems SE.

Multi-Link is a trademark of CareFusion Corporation or one of its affiliates.

Manufacturer responsibility

GE is responsible for the effects on safety, reliability, and performance of the equipment only if:

- Assembly operations, extensions, readjustments, modifications, servicing, or repairs are carried out by authorized service personnel.
- The electrical installation of the relevant room complies with the requirements of the appropriate regulations.
- The equipment is used in accordance with the instructions for use.
- The equipment is installed, maintained and serviced in accordance with the instructions provided in the related service manuals.

WARNING

SAFETY HAZARD. To avoid risks to personnel and patient, or damage to the equipment, only perform maintenance procedures described in this manual. Unauthorized modifications can lead to safety hazards.

About this manual

2

Safety

Safety message signal words

Safety message signal words designate the severity of a potential hazard.

DANGER	Indicates a hazardous situation that, if not avoided, will result in death or serious injury.
WARNING	Indicates a hazardous situation that, if not avoided, could result in death or serious injury.
CAUTION	Indicates a hazardous situation that, if not avoided, could result in minor or moderate injury.
NOTICE	Indicates a hazardous situation not related to personal injury that, if not avoided, could result in property damage.

Safety symbols

Symbol	Explanation
	General warning sign. ISO 7010. This symbol is identified by a yellow background, black triangular band, and a black symbol. In this manual this symbol is used only in connection with those warning statements that the labels on the equipment refer to.
	Caution. ISO 7000. This symbol is identified by a white background, black triangular band, and a black symbol.
	Follow instructions for use. ISO 7010. This symbol indicates mandatory action and it is identified by a blue background and a white symbol.
	Consult operating instructions. / Operating instructions.
	WARNING — Electric shock hazard. This equipment must be serviced by qualified service personnel only. ISO 7010. This symbol is identified by a yellow background, black triangular band, and a black symbol.

Symbol	Explanation
	MR Unsafe. Indicates that the device is not intended for use in an MR environment. This symbol is identified by a white background, red or black circular band, and a black symbol.
	Electrostatic sensitive device.
	Non-ionizing electromagnetic radiation. Interference may occur in the vicinity of this device.
	Type BF (IEC 60601-1) protection against electric shock. Isolated (floating) applied part suitable for intentional external and internal application to the patient, excluding direct cardiac application.
	Type BF (IEC 60601-1) defibrillator-proof protection against electric shock. Isolated (floating) applied part suitable for intentional external and internal application to the patient, excluding direct cardiac application.
	Type CF (IEC 60601-1) protection against electric shock. Isolated (floating) applied part suitable for intentional external and internal application to the patient, including direct cardiac application.
	Type CF (IEC 60601-1) defibrillator-proof protection against electric shock. Isolated (floating) applied part suitable for intentional external and internal application to the patient including direct cardiac application.
	Safety ground. Remove power cord from the mains source by grasping the plug. Do not pull on the cable.

System safety

For a complete list of system safety messages that apply to the entire system, refer to the user manual. For safety messages specific to parts of the system or to a certain installation or service task, refer to the relevant sections.

Reporting of serious incidents

Any serious incident related to the use of this device should be reported to both the manufacturer and the health authority/competent authority where the device is installed.

To report to GE, contact your local service representative or report to In-box.complaints@ge.com.

Please provide the following information:

- The catalogue number or the model designation of the device as stated on its identification plate affixed on the device
- The System ID/serial number/lot number of the device
- Date of incident
- Description of incident, including any patient or user impact/injury

- Your contact information (facility, address, contact name, title, and telephone number)

Safety

3

System introduction

Short description of the equipment

The CARESCAPE B850 is a modular multi-parameter patient monitor. The monitor can be used with most patient populations within a professional healthcare facility, but acquisition modules may have limitations for use based on the patient's age, weight, or clinical condition, or on the type of the care unit (for example, OR or ICU only). There are several types of acquisition modules to choose from based on care requirements and patient needs.

The modular system design is inherent in electronics and algorithms: some processing of the measurement signals is done by the acquisition modules and further processing happens on the monitor.

Measurement values are displayed as graphic or numeric values, like waveforms and numbers, and when applicable, also as alarm messages.

The CARESCAPE B850 supports two independent displays, and the screen contents shown on each are user-configurable. The D19KT VER01 display has an integrated alarm light.

The user interface can be used as a touchscreen, or with a Trim Knob or a mouse and a keyboard. The most important and commonly used functions have main keys on the main menu (soft keys). The menu structure design allows access to all functions needed by the clinical user with just a few clicks.

The monitor transfers the measurement data to central stations and to the hospital patient data depositories. It communicates with a variety of other bedside medical devices and monitoring systems.

For all physical and performance specifications, refer to the supplemental information provided. For more detailed information on the intended use of the device, refer to the user manual.

CPU unit

The primary function of the monitor is to render a clinically meaningful display of acquired patient data and allow the caregiver control (alarms, configuration, etc.) of the system through the user interface. The CPU unit is the central processing unit for the patient monitoring system and provides a link between parameter acquisition and input/output devices. It also facilitates network communication and interface to several ancillary devices (for example, printers, displays). The monitor works with multi parameter acquisition devices.

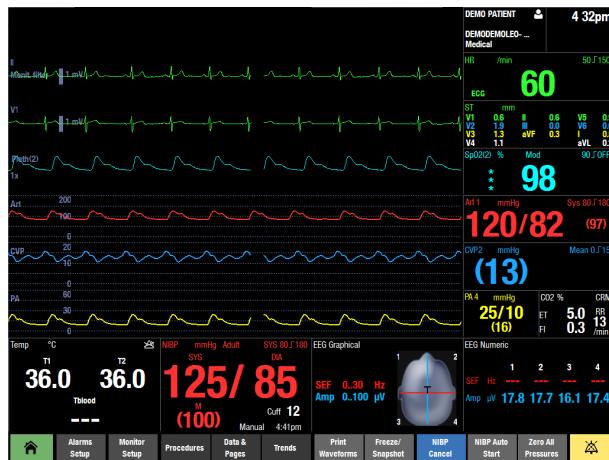


Software

The monitor is highly configurable and provides many monitoring possibilities with a flexible software licensing model.

The monitor supports care area specific software packages for OR, PACU, ICU, ED and NICU. Each dedicated software package provides a comprehensive feature set for the different monitoring needs and can be further extended with the optional feature licenses.

Software license model supports trial licensing and easy field upgrades with license key activation.



Displays

The monitor supports up to two independent, user-configurable displays.



The CARESCAPE D19KT VER01 display provides a Trim Knob and touchscreen control and indicates a power failure alarm with a continuous beep. The display integrates audible and visual alarms and provides USB connectivity.

B850 system components

The typical minimum B850 system configuration consists of the following:

- central processing unit (CPU)
- display
- cables and an adapter for connecting the CPU to the display
 - DVI-D to DVI-D cable
 - USB-A to USB-B cable
 - Display Port to DVI-D Adapter
- module frame
- cable for connecting the frame to the CPU

All components listed below can be used within the patient environment as long as an additional transformer providing at least basic isolation is used with non-medical grade secondary displays and printers.

Your system may not include all these components. Consult your local representative for the available components.



1. 19-inch display D19KT VER01: Touchscreen display that provides Trim Knob control. If a non-medical grade display is used as a secondary display within the patient environment it must always be powered from an additional transformer providing at least basic isolation.
2. Processing unit: Provides a link between parameter acquisition and input and output devices. The processing unit works with multi-parameter acquisition devices.
3. The F7 Frame has seven module slots and the F5 Frame has five module slots that support E-module acquisition modules. The F5 frame supports PDM modules with a slide mount.
4. Frame to CPU cable
5. CARESCAPE ONE acquisition platform (used with CARESCAPE Parameters). For details, refer to its own manuals.
6. CARESCAPE Dock F0 for CARESCAPE ONE.
7. Acquisition modules: Two types of acquisition modules can be used: PDM and E-modules.
8. Remote control: Used to provide all patient monitor controls on a portable component with a Trim Knob control.
9. Barcode reader: Used to scan patient information from barcodes when admitting patients.
10. Keyboard: Allows data entry without using the on-screen keyboard or a touchscreen display.
11. Mouse.
12. Laser printer: This device may be connected to the monitor, network, or to a central station on the network. The laser printer can print waveforms, alarm waveforms, numeric trends, and reports. If it is used within the patient

environment it must always be powered from an additional transformer providing at least basic isolation.

13. PRN 50-M+ recorder: This device may be connected directly to the monitor or over the network to a remote monitor or central station. The recorder can print waveforms, alarm waveforms, and numeric trends.
14. CARESCAPE RAD (remote alarm device): Used to notify a remote location of patient alarms and system alarms.
15. Unity Network Interface Device (ID): Used with the monitor to communicate with other manufacturers' peripheral bedside devices, such as ventilators and gas delivery systems, to centralize patient data on one device.

CARESCAPE ONE

For more information on CARESCAPE ONE, refer to its own manuals.

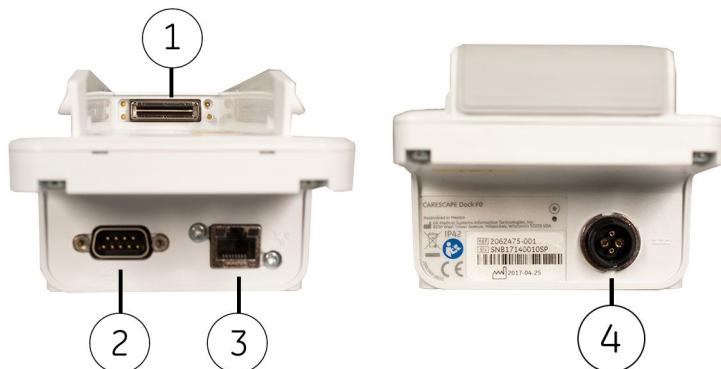


1. CARESCAPE Parameter connectors
2. Tab for removing the acquisition platform from the docking mount
3. Analog out/Defibrillator synchronization connector
4. NIBP hose connector

CARESCAPE ONE is used with CARESCAPE Parameters:

- CARESCAPE ECG
- CARESCAPE Pressure
- CARESCAPE Temperature
- CARESCAPE CO₂ — LoFlo
- CARESCAPE CO₂ — Microstream
- CARESCAPE rSO₂
- CARESCAPE SpO₂
- CARESCAPE SpO₂ —Masimo
- CARESCAPE SpO₂ — Nellcor

CARESCAPE Dock F0 side views



1	Docking interface connector to the CARESCAPE ONE.
2	ePort connector to the host monitor.
3	RJ-45 connector. The service port is configured for direct connection to a service PC only. Do not connect the service port to a network.
4	Power receptacle for the AC mains to DC power supply.

CARESCAPE Dock F0 provides an interface between a CARESCAPE monitor and the CARESCAPE ONE.

Acquisition modules

You can use different types of acquisition modules with the monitor. They provide connection to the patient, process patient data signals, and send patient data signals to the monitor. For a complete list of compatible devices, see the supplemental information provided.

PDM front view



1. ECG (imp.resp.)
2. T1 to T2/C.O.
3. P1/P3 and P2/P4
4. SpO₂
5. NIBP
6. Communication indicator. Illuminates yellow during boot-up and turns green after boot-up; flashes yellow if communication fails; is not illuminated when no power is applied to the PDM.
7. Power indicator. Illuminates yellow during boot-up and turns green after boot-up; illuminates green when the PDM module is powered by the monitor, or when the PDM battery is installed and power is applied to the PDM by pressing the Power On button; is not illuminated when no power is applied to the PDM.
8. Dual function Power On and Zero All button
9. Defib/Sync
10. Tab for removing the module

Modules and parameters

PDM parameters

Parameter	PDM (Masimo)**	PDM (Nellcor)**
ECG	up to 12 leads	up to 12 leads
Imp.respiration	x	x
Invasive pressures	4*	4*
NIBP	x	x
Temperature	2* (or C.O.)	2* (or C.O.)
C.O.	x (or 2 temp.)	x (or 2 temp.)
SpO ₂ Masimo	x	-
SpO ₂ Nellcor	-	x
* A dual adapter cable is required to monitor two invasive pressure or temperature measurements on a single connector.		
** Different SpO ₂ cables are required for each type of SpO ₂ processing. The cable connectors are not interchangeable.		

CARESCAPE Parameters

Parameter	CARESCAPE Parameter
ECG	CARESCAPE ECG up to 12 leads
Impedance respiration	CARESCAPE ECG
Invasive pressures	CARESCAPE Pressure 4
NIBP	No CARESCAPE Parameter required, measurement is available with NIBP hose connected directly to CARESCAPE ONE
Temperature	CARESCAPE Temperature 2
SpO ₂ TruSignal	CARESCAPE SpO ₂
SpO ₂ Masimo	CARESCAPE SpO ₂ – Masimo
SpO ₂ Nellcor	CARESCAPE SpO ₂ – Nellcor
CO ₂	CARESCAPE CO ₂ – LoFlo CARESCAPE CO ₂ – Microstream (also available with the E-musb module)
Surgical Pleth Index (SPI)	CARESCAPE SpO ₂
Regional oxygen saturation (rSO ₂)	CARESCAPE rSO ₂ (also available with the E-musb module)

E-COP, E-COPSV, and E-PiCCO parameters

Parameter	E-COP	E-COPSV	E-PiCCO
Invasive pressures	1	1	1
SvO ₂	-	x	-
ScvO ₂	-	x *	-
C.O.	x (also REF)	x (also REF)	x
CCO	-	-	x

* E-COPSV-01 only

E-PP and E-PT parameters

Parameter	E-PP	E-PT
Invasive pressures	2	1
Temperature	-	2*

* A dual adapter cable is required to monitor two temperature measurements on a single connector.

E-module gas parameters

Module	CO ₂	N ₂ O	O ₂	Anesthetic agents	Agent ID
E-miniC	x	-	-	-	-
E-sCO	x	*	x	-	-
E-sCOV	x	*	x	-	-
E-sCOVX	x	*	x	-	-
E-sCAiO	x	x	x	x	x
E-sCAiOE	x	x	x	x	x
E-sCAiOV	x	x	x	x	x
E-sCAiOVX	x	x	x	x	x
E-sCAiOVE	x	x	x	x	x

* The E-sCO, E-sCOV, and E-sCOVX modules automatically compensate for N₂O in realtime although N₂O values are not displayed on screen.

The E-miniC requires manual selection from the monitor menu to compensate for N₂O and for O₂.

Module	Spirometry	Gas exchange	Aisys CS ² end-tidal control
E-miniC	-	-	-
E-sCO	-	-	-
E-sCOV	x	-	-
E-sCOVX	x	x	-
E-sCAiO	-	-	-
E-sCAiOE	-	-	x
E-sCAiOV	x	-	-
E-sCAiOVX	x	x	-

Module	Spirometry	Gas exchange	Aisys CS ² end-tidal control
E-sCAiOVE	x	-	x
For more information on the use of the end-tidal control, refer to the Aisys CS ² user documentation.			

E-MASIMO and E-NSATX parameters

Parameter	E-NSATX*	E-MASIMO*
SpO ₂ Masimo	-	x
SpO ₂ Nellcor	x	-
* Different SpO ₂ cables are required for each type of SpO ₂ processing. The cable connectors are not interchangeable.		

Specialty E-module parameters

Parameter	E-NMT	E-EEGX	E-ENTROPY	E-BIS
Level of relaxation	x	-	-	-
Nerve stimulation	x	-	-	-
EEG	-	x	-	-
AEP	-	x	-	-
Entropy	-	-	x	-
BIS	-	-	-	x

E-musb parameters

E-musb is an interface module for connecting the following compatible CARESCAPE Parameters to the monitor:

- CARESCAPE rSO₂ for measuring regional oxygen saturation of blood (rSO₂) in cerebral and somatic tissues with INVOS technology
- CARESCAPE CO₂ — Microstream for measuring end-tidal carbon dioxide (EtCO₂), FiCO₂, and respiration rate with Microstream technology

E-musb can host up to two compatible CARESCAPE Parameters: either one CARESCAPE CO₂ - Microstream and one CARESCAPE rSO₂, or two CARESCAPE rSO₂.

CARESCAPE Network

The monitor is compatible with the CARESCAPE Network.

The MC (Mission Critical) Network services include transferring real-time or near real-time patient information between network devices. The information includes numerics, waveforms, alarms, trends, and patient information.

The IX (Information Exchange) Network provides access to the following services:

- MUSE server for viewing MUSE/12SL reports on the monitor screen (a licensed feature)
- Citrix server for viewing other applications on the monitor screen (a licensed feature)
- Printing to IX printers connected to IX Network
- InSite RSvP remote service platform

- Service personnel have centralized access to service interfaces of several monitors from within the hospital

Other system components

For more information, refer to the devices' own instructions.

Input devices	Description
	<p>Barcode reader</p> <p>The barcode reader can be used to scan Patient Information from barcodes when admitting patients.</p> <p>By default, the barcode reader has been configured to US English at the factory. The correct language must be configured to the barcode reader itself before configuring the barcode settings to the monitor. See the instructions provided with the barcode reader.</p>
	<p>Keyboard</p> <p>A washable, antibacterial keyboard is specified for use with the monitor. It may be connected to the monitor or display via one of the USB connectors. The keyboard allows you to enter data without using the on-screen keyboard or a touchscreen display.</p>
	<p>Mouse</p> <p>A standard mouse may be connected to the monitor or display via one of the USB connectors. The mouse allows you to select any on-screen items without a Trim Knob control or a touchscreen display.</p>
	<p>Remote control</p> <p>The remote control provides all patient monitor controls on a portable component with a Trim Knob control. The remote control is connected to the patient monitor via one of the USB connectors.</p>
Recorders and laser printers	Description
	<p>Laser printers</p> <p>A laser printer can print for example waveforms, graphic and numeric trends, snapshots, events history, parameter specific printouts, stored laboratory data, and calculation results and care reports. Refer to the patient monitor's user manual for more information about printing.</p> <p>The patient monitor supports printing:</p> <ul style="list-style-type: none"> • to a laser printer that is connected to IX Network • to a laser printer that is connected directly to the monitor • to a laser printer that is connected to a CARESCAPE Central Station <p>Refer to the printer's service manual for printer installation instructions.</p> <p>PRN 50-M+ Recorder</p> <p>A recorder may print waveforms, alarm waveforms and numeric trends.</p> <p>The patient monitor supports printing:</p> <ul style="list-style-type: none"> • to a PRN 50-M+ recorder connected directly to the monitor • to a PRN 50-M+ recorder connected to a CARESCAPE Central Station or to a remote monitor <p>Refer to the PRN 50-M+ Writer Service Manual for installation instructions.</p>

Central stations	Description
	<p>CARESCAPE Central Station</p> <p>The MC Network establishes communication and allows patient data to be sent to an optional CARESCAPE Central Station. See the CARESCAPE Central Station User's Manual for operating instructions.</p>
Other devices	Description
	<p>Unity Network Interface Device (ID)</p> <p>The monitor can interface with peripheral medical devices, such as ventilators and gas delivery systems, to centralize patient data on one device. A Unity Network Interface Device (ID) is used with the monitor to communicate with peripheral devices.</p> <p>See the Unity Network Interface Device (ID) Service Manual for installation instructions.</p>
	<p>CARESCAPE RAD</p> <p>The CARESCAPE RAD provides alarm notification at a location remote from the monitor. The remote alarm device interfaces to the monitor via a USB port. Its functionality is enabled or disabled during configuration.</p> <p>See the CARESCAPE RAD Service Manual for instructions.</p>

Access to external applications

The Citrix application, viewable from one of the monitor's displays, gives access to desktops created by the hospital IT. These desktops provide patient information from other systems that may be installed at the hospital [e.g., Centricity Clinical Information View (Centricity CIV), MUSE Web, and Picture Archiving Communications System (PACS)]. Desktops can be created with customer defined resolutions using the hospital-wide login and identification process. The access is provided through a Citrix thin client on the monitor so no additional equipment is required at the bedside.

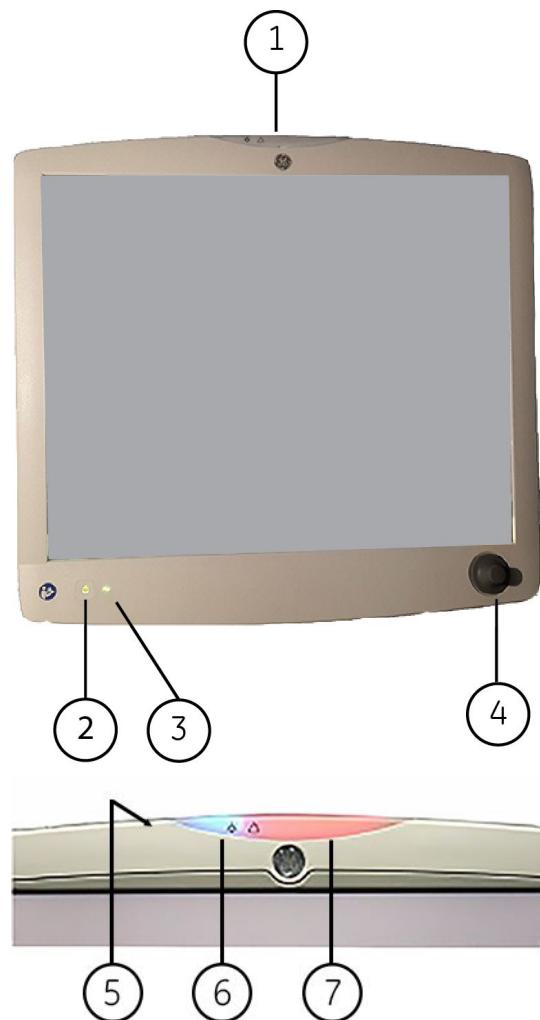
Citrix application is accessible through **Data & Pages** > .

See the supplemental information provided for default settings related to this application.

Controls and connectors

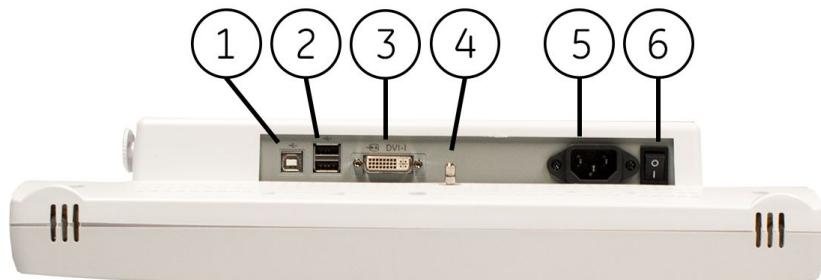
B850 display front view

System introduction



1. Alarm light
2. Power on/standby button
3. Power indicators
4. Trim Knob control
5. Ambient light detector lens
6. Audio alarm paused/off area (blue)
7. Alarm light area (blue, yellow, or red)

B850 display back view



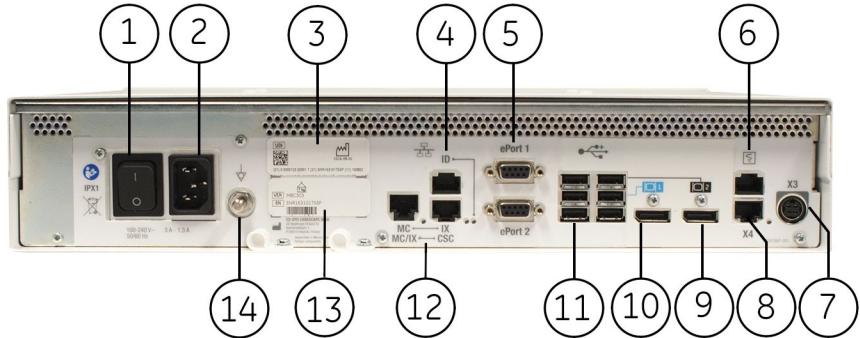
1. Type B USB port
2. Type A USB port
3. DVI-I connector
4. Equipotential connector
5. Receptacle for power cord
6. Power on/off switch

B850 processing unit front view



1. Power connection indicator: Illuminates green when the power on/off switch on the back of the monitor is in the I (on) position.
2. On/Standby button. Illuminates green when the power is turned on.

B850 processing unit back view



1. Power on/off switch.
 2. Power inlet connector.
 3. UDI marking
 4. ID connector: For connecting the monitor to Unity Network Interface Device (ID).
 5. Two ePort connectors: For connecting the PDM and module frames, and CARESCAPE Dock F0 for CARESCAPE ONE.
 6. Connector for PRN-50M+ recorder.
 7. Remote-on connector.
 8. Not in use.
 9. DisplayPort connector for an optional secondary display.
 10. DisplayPort connector for the primary display.
 11. Six USB ports: For connecting the touchscreen display, remote control, keyboard, mouse, and barcode reader.
The USB connector that is connected with a blue line to DisplayPort 1 is reserved for the primary display. The USB connector that is connected with a black line to DisplayPort 2 is reserved for the optional secondary display.
 12. Network connectors for connecting to the CARESCAPE Network.
Monitors can be configured to the MC and IX networks either using two network interfaces (dual wire configuration) or one network interface (single wire configuration). When connected via single wire, the monitor sends MC and IX traffic onto the MC network. The CARESCAPE Router is responsible for passing IX traffic from the MC network onto the IX network. The connection to these CARESCAPE Networks depends on how the network infrastructure at the customer site is configured.
- With dual wire configuration:

- MC: Connects the monitor to the MC Network.
- IX: Connects the monitor to the optional IX Network.

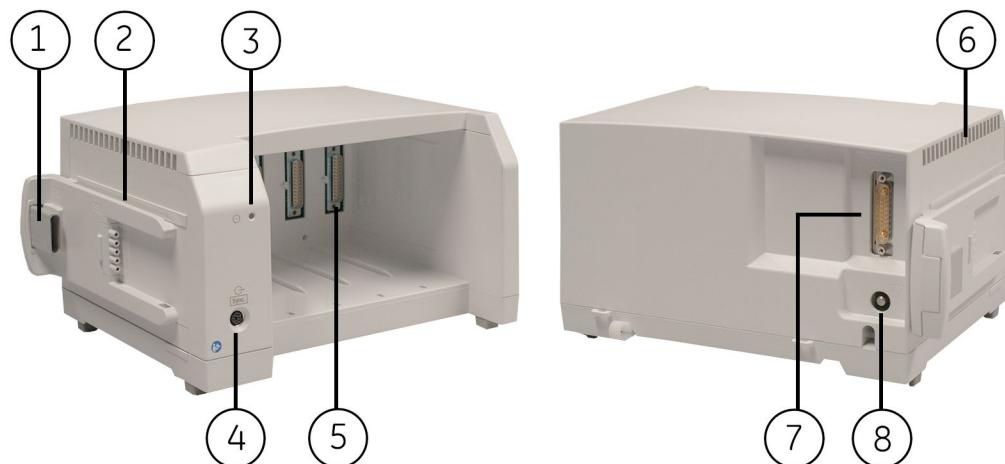
With single wire configuration:

- MC/IX: Connects the monitor to the MC Network and IX Network.
- CSC: This connector is not in use.

13. Device label

14. Equipotential connector. For measurements in or near the heart we recommend connecting the monitor to the potential equalization system (IEC 60601-1) to ensure equal potential levels between the devices in the system.

F5 Frame, 5-module frame



1. Connector for PDM module.
2. Connector for PSM module (not in use).
3. On/Standby LED.
4. Synchronization connector (not in use).
5. Module connector.
6. Communication LED and Link LED.
7. ePort connector for the CARESCAPE monitor connection cable.
8. Equipotential connector.

NOTE

CARESCAPE Software v3 does not support E-PSM(P) modules. Therefore, the PSM and Synchronization connectors are not in use.

F7 Frame, 7-module frame



1. On/Standby LED.
2. Synchronization connector (not in use).
3. Module connector.
4. Connector for the cable of Pole Mount for E-PSM (not in use).
5. ePort connector for the CARESCAPE monitor connection cable.
6. Communication LED and Link LED.
7. Equipotential connector.

NOTE

CARESCAPE Software v3 does not support E-PSM(P) modules. Therefore, the PSM and Synchronization connectors are not in use.

IEC 60601-1

- Type of protection against electrical shock: Class I.
- Degree of protection against electrical shock: applied parts are marked with a symbol indicating degree of protection.
- Degree of safety of application in the presence of flammable anesthetic mixture with air or with oxygen or nitrous oxide: Not suitable.

WARNING

EXPLOSION. Do not use this system in the presence of flammable anesthetics, vapors or liquids.

- Degree of protection against harmful ingress of water: IPX1.
- Mode of operation: Continuous.
- Method(s) of sterilization or disinfection recommended by the manufacturer: see the user manual.

IEC 60601-1-2

The system complies with IEC 60601-1-2:2014-02.

Compliance with the standard IEC 60601-1-2:2014-02 applies only to those products that are currently being manufactured and shipped. It may not apply to older devices

or devices that have their software upgraded. For standards compliance information, refer to the supplemental information provided with the device.

According to parameter-specific IEC 60601-2-xx and IEC 80601-2-xx series standard requirements for ESU (electrosurgical unit) tests, the equipment is protected against malfunction caused by electrosurgery.

IEC 60529

- Degree of protection against harmful ingress of water: Components not marked with an IPXn code are rated as Ordinary (no protection against fluid ingress). All other IPXn rated components have the degree of protection per the 'n' rating.
- B850: IPX1.

Equipment markings

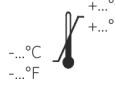
The following markings appear on one or more of the devices.	
	Bell cancel. Audio off.
	Audio pause. Temporary audio off.
	General alarm.
	Fuse. Replace with identical type and rating fuse.
	Battery (monitor): The flashing orange symbol indicates that there is a battery failure/missing battery.
	Battery (monitor): The solid orange symbol indicates that the battery is being charged.
	Battery (monitor). The solid green symbol indicates that the monitor is being used on battery power.
	Battery (monitor). Located on the battery slot cover.
	Battery (monitor): The battery slot cover is open/closed.
	Battery (monitor): Test button on the battery to check the battery charge level.
	Battery.
	Communication indicator.

The following markings appear on one or more of the devices.	
 (black or red)	Power indicator.
	On/standby button.
	Standby or power indicator.
	USB connectors.
	Ethernet connectors.
	Graphical recorder.
	ePort connector.
	DVI connector. Video output connector for digital or analog source.
	Color video input. Video input connector for digital or analog source.
	Gas inlet.
	Gas outlet.
	Zero all.
IPX1	<p>Degree of ingress protection.</p> <p>Degree of protection against harmful ingress of water: Components not marked with an IPX n code are rated as Ordinary (no protection against fluid ingress). All other IPXn rated components have the degree of protection per the 'n' rating.</p> <p>IPX1: This equipment is protected against harmful effects of dripping water per IEC 60529.</p>
	Do not reuse.

The following markings appear on one or more of the devices.

	Use by.
	Latex-free.
	D-fend Pro/Mini D-fend: Add date.
	Home. Return to the main display.
	Alternating current. Green symbol on the monitor front panel: the monitor is being used on mains power.
	Direct current.
	Equipotentiality. Connect device to a potential equalization conductor.
	Protective earth ground. Connectors grounded to the AC power source.
	Defibrillator synchronization connector (monitor). Not in use.
	Stacking limit by number (number varies).
2008-06-13	Date of manufacture. This symbol indicates the date of manufacture of this device. The first four digits identify the year, the following two digits identify the month, and the last two digits identify the day.
GE Healthcare Finland Oy Kuortaneenkatu 2 FI-00510 Helsinki, Finland 2016-01-31	Manufacturer address and date of manufacture. The first four digits identify the year, the following two digits identify the month, and the last two digits identify the day.
	Manufacturer name and address.
	Batch or lot number.
lbl p/n	Abbreviation for label part number.
P/N	Abbreviation for product number.
TYPE	Identifies the device type.

The following markings appear on one or more of the devices.	
REF	Catalogue or orderable part number.
SN	Device serial number.
VER	Device model or type.
UDI	Every device has a unique marking for identification. The UDI marking appears on the device label.
MD	Indicates that the product is a medical device.
CARESCAPE ECG	CARESCAPE Parameter for measuring ECG
CARESCAPE PRES	CARESCAPE Parameter for measuring invasive pressures
CARESCAPE TEMP	CARESCAPE Parameter for measuring temperature
CARESCAPE CO₂ -LoFlo	CARESCAPE Parameter for measuring CO ₂ with Resironics LoFlo technology
CARESCAPE CO₂ - Microstream	CARESCAPE Parameter for measuring end-tidal carbon dioxide (EtCO ₂), FiCO ₂ , and respiration rate with Microstream technology
CARESCAPE SpO₂	CARESCAPE Parameter for measuring SpO ₂ with GE TruSignal technology
CARESCAPE SpO₂ - Masimo	CARESCAPE Parameter for measuring SpO ₂ with Masimo rainbow SET technology
CARESCAPE SpO₂ - Nellcor	CARESCAPE Parameter for measuring SpO ₂ with Nellcor Oximax technology
CARESCAPE rSO₂ - INVOS	CARESCAPE Parameter for measuring regional oxygen saturation of blood (rSO ₂) in cerebral and somatic tissues with INVOS technology
	Mass of typical portable RGM (respiratory gas monitor) configuration. The indicated mass (12 kg in this example) varies per RGM configuration.
	Locked.
	Unlocked.
	No heavy load.
	Maximum total load.

The following markings appear on one or more of the devices.	
	Atmospheric pressure limitations.
	Temperature limitations.
	Humidity limitations.
	Keep dry. Protect from rain.
	Fragile. Handle with care.
	This way up.
	This symbol indicates that the waste of electrical and electronic equipment must not be disposed as unsorted municipal waste and must be collected separately. Please contact an authorized representative of the manufacturer for information concerning the decommissioning of your equipment.
	Recycled materials or may be recycled.
	Recyclable Lithium-Ion.
	European authorized representative.
	Swiss authorized representative.
	European Union Conformity Mark
	Conformity mark. Indicates that the product is certified for both the U.S. and Canadian markets, to the applicable U.S. and Canadian standards. Either of these two symbols can appear on the device.
	UK Conformity Assessed marking.

The following markings appear on one or more of the devices.	
	Conformity mark. TÜV Rheinland product certification mark.
SDPPI	Indonesia only. Ministry of Telecommunication and Informatics certificate number and registrant identification.
	Hong Kong only. Approved under Office of the Telecommunications Authority (OFTA) requirements.
	FCC. USA only. Complies with applicable US government (Federal Communications Commission) radio-frequency interference regulations.
Rx ONLY U.S.	CAUTION U.S. Federal law restricts this device to sale by or on the order of a physician.
	Russia only. GOST-R mark.
	Eurasian Economic Union countries only. Eurasian Conformity mark. Conformity to applicable technical regulations of Customs Union.
	Brazil only. INMETRO certified. Accredited laboratory's marking with accreditation reference replaces the OCP marking.
	<p>The following symbols (required by China law only) are representative of what you may see on your equipment.</p> <p>The number in the symbol indicates the EFUP period in years, as explained below. Check the symbol on your equipment for its EFUP period.</p> <p>This symbol indicates the product contains hazardous materials in excess of the limits established by the Chinese standard GB/T 26572. Requirements for Concentration Limits for Certain Hazardous Substances in Electronic Information Products. The number in the symbol is the Environment-friendly Use Period (EFUP), which indicates the period during which the hazardous substances or elements contained in electronic information products will not leak or mutate under normal operating conditions so that the use of such electronic information products will not result in any severe environmental pollution, any bodily injury or damage to any assets. The unit of the period is "Year".</p> <p>In order to maintain the declared EFUP, the product shall be operated normally according to the instructions and environmental conditions as defined in the product manual, and periodic maintenance schedules specified in Product Maintenance Procedures shall be followed strictly.</p> <p>Consumables or certain parts may have their own label with an EFUP value less than the product. Periodic replacement of those consumables or parts to maintain the declared EFUP shall be done in accordance with the Product Maintenance Procedures. This product must not be disposed of as unsorted municipal</p>

The following markings appear on one or more of the devices.	
	waste, and must be collected separately and handled properly after decommissioning.
	This symbol indicates that this electronic information product does not contain any hazardous substance or elements above the maximum concentration value established by the Chinese standard GB/T 26572, and can be recycled after being discarded, and should not be casually discarded.
	Canada only. Industry Canada certification number indicates that this product meets the applicable Industry Canada technical specifications.
	China only. Chinese Compulsory Certification as required by AQSIQ. Safety & EMC compliance.
	India only. Indian Conformity Assessment Certification granted by the Bureau of Indian Standards.
CMIIT ID	China only. China Ministry of Industry and Information Technology identification number for Radio Transmission Equipment Type Approval.
	Australia and New Zealand only. RCM compliance. Indicates compliance with electrical safety, EMC, electromagnetic energy, and telecommunications requirements applicable to each product.
	Australia only. The product complies with the applicable Australian standard and establishes a traceable link between the equipment and the manufacturer, importer or their agent responsible for compliance.
	Japan only. The PSE mark (Product Safety Electric Appliance and Materials) is a mandatory mark required on Electrical Appliances in Japan as authorized by the Electrical Appliance and Material Safety Law (DENAN). This mark signifies that a product complies with the law according to a set of standards for electric devices.
	Japan only. Approved under Japan TELEC requirements.
	Brazil only. Approved under ANATEL (Agência Nacional de Telecomunicações) requirements.
	South Africa only. Approved under ICASA (Independent Communications Authority of South Africa) requirements.
KCC-XXX-XXX-XXXXXXXXXXXX	Korea only. Approved under KCC (Korea Communications Commission) requirements.

The following markings appear on one or more of the devices.	
	Ukraine only. Mark of conformity with the Technical Regulations. This product meets the requirements of the Technical Regulations on medical devices, approved by Resolution No. 753 of the Cabinet of Ministers of Ukraine on October 2nd 2013
	Vietnam only. MIC Vietnam/MOST Vietnam conformity mark.
	Malaysia only. Malaysian Communication and Multimedia Commission (MCMC) certification mark.
	Taiwan only. Taiwan Regulator National Communications Commission (NCC) approval mark.
	United Arab Emirates only. United Arab Emirates Telecommunications Regulatory Authority (TRA) conformity mark.
TRA RTTE	United Arab Emirates only. United Arab Emirates Telecommunications Regulatory Authority (TRA) product registration number.
Dealer ID	United Arab Emirates only. United Arab Emirates dealer number.
CNC ID	Argentina only. Argentinian Comisión Nacional de Comunicaciones (CNC) identification number.
ictQATAR	Qatar only. Supreme Council of Information and Communication Technology.
Type Approval Reg. No.	Qatar only. Supreme Council of Information and Communication Technology type approval registration number.
Importer No.	Qatar only. Importer identification number.
R-NZ	New Zealand only. Radio label for radio products not harmonized with Australia.
IFETEL	Mexico only. Instituto Federal de Telecomunicaciones or the Mexican Federal Telecommunications Institute.
IMDA	Singapore only. Info-communications Media Development Authority

Unique Device Identifier (UDI)

 <p>(01) 1234567891234(21) SJN14241237HA(11) 150628</p>	<p>Unique Device Identifier. (UDI)</p> <p>Every medical device has a unique marking for identification. For the UDI marking of the device, see the device labeling. For the UDI marking of the software, select Monitor Setup > Defaults & Service > Service. The information is displayed on the screen.</p> <p>Note that this is only an example of a UDI marking. The device may have a linear barcode as in this example, or a DataMatrix code, or only alphanumeric identifiers with no barcode. Also the identifiers vary per product.</p>
--------------------------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

The characters used in the UDI marking represent specific identifiers. In the example above:

Device identifier:

- (01) = GS1 global trade item number (GTIN) of the device.
- 1234567891234 = Global trade item number.

Production identifiers:

- (21) = GS1 application identifier for the serial number of the device.
- SJN14241237HA = Serial number.
- (11) = GS1 application identifier for the manufacturing date of the device.
- 150628= Manufacturing date: year-month-day (YYMMDD).

Note that for some product types the production identifier can have other elements instead of the ones listed above:

- (10) = For the device: GS1 application identifier for the batch or lot number, followed by the batch or lot number. For the software: GS1 Application identifier for the batch or lot number followed by the software version or build.
- (17) = GS1 application identifier for the expiration date of the device, followed by the expiration date.

User interface indicators

The following indicators appear in the software user interface.

	Alarm off indicator. The indicator may not display at the central station or on a remote bedside monitor.
	Alarm priority indicator: High (red). Indicates a high priority alarm.
	Alarm priority indicator: Medium (yellow). Indicates a medium priority alarm.
	Alarm priority indicator: Low (cyan). Indicates a low priority alarm.
	Alarm volume indicator. Adjust the minimum alarm tone volume.
	Alarm volume adjustment for high and medium priority.
	Alarm volume adjustment for low priority.
	Audio alarms off indicator. The indicator will include a text indication of the silenced alarms: ECG (ECG Audio Off) , APN (Apnea Audio Off) , APN ECG (Apnea & ECG Audio Off) , or ALL (All Alarms Audio Off) . Also displays in the screen saver when Pause Monitor (sleep mode) or Pause Monitor & Central has been selected.

The following indicators appear in the software user interface.	
	Audio alarms paused indicator with countdown timer - Indicates all audio alarms are paused and the amount of time remaining for the alarm pause period displays as a countdown timer.
	Alarm pause indicator - Indicates that all alarms are paused. Displays in the CARESCAPE Network bed-to-bed window when no alarms are received from the remote monitor.
	Alarms audio pause indicator. Displays in the upper left corner of the alarm message and indicates that the alarm audio pause has been activated.
	Acknowledge alarms indicator. Displays in the upper right corner of the alarm message and indicates that this alarm can be acknowledged by touching the alarm message or with the pause audio key. In case there are latched alarms, they will all be acknowledged. In 12SL menu: delete.
	Low priority audio off alarm indicator. Indicates that audio indicators have been turned off for low priority alarms (visual indicators are still active).
	General warning sign. Displays when the priority setting deviates from the recommendation of international alarm safety standards.
	Information point sign. Identifies a place where information may be found.
	Reminder volume indicator. Adjust the volume of the tone that sounds every two minutes when audio alarms are turned off.
	Citrix. Access external applications.
	Touch indicator.
	Home indicator. Close all menus/applications displayed on the monitor.
	Patient indicator.
	Patient discharge indicator.
	Other patients indicator. Indicates entry to the Other Patients menu.
	Locking indicator.
	Network connection indicator. Indicates the monitor is connected to a live wired MC Network.

The following indicators appear in the software user interface.

	CARESCAPE ONE battery charging indicator. Indicates the battery is charging.
	CARESCAPE ONE battery gauge indicator. Indicates the charge level of the battery.
	CARESCAPE ONE battery failure indicator. Indicates the battery is not available for use.
	PDM battery charging indicator. Indicates the battery is charging.
	PDM battery gauge indicator. Indicates the charge level of the battery.
	PDM battery failure indicator. Indicates the battery is not available for use.
	CARESCAPE ONE available. Appears in the Continue or Select Patient and Data menu.
	CARESCAPE ONE not available. Appears in the Continue or Select Patient and Data menu.
	Monitor available. Appears in the Continue or Select Patient and Data menu.
	Monitor not available. Appears in the Continue or Select Patient and Data menu.
	PDM available. Appears in the Continue or Select Patient and Data menu.
	PDM not available. Appears in the Continue or Select Patient and Data menu.
	Snapshot indicator. Indicates the event has an associated snapshot.
	Red indicator (blinking) or white indicator (in the ECG Setup menu): beat source indicator.
	Respiration indicator. Indicates a breath is detected by the impedance respiration algorithm.
	Impedance respiration lead I selection indicator.

The following indicators appear in the software user interface.	
	Impedance respiration lead II selection indicator.
	Impedance respiration lead RL-LL selection indicator.
	BIS and Entropy sensor impedance check indicator (gray). Displays for each sensor as the impedance check is in progress.
	BIS and Entropy sensor impedance check error indicator (red). Indicates the specified sensor failed the impedance check.
	BIS, Entropy, and NMT sensor impedance check passed indicator. Indicates the specified sensor passed the impedance check.
	NMT measurement error indicator. Indicates the measurement with the specified electrode has failed.
	NMT indicator: Indicates that the NMT module is connected but no sensor is connected to the NMT sensor cable.
	NMT indicator: Indicates that the ElectroSensor is connected to the NMT sensor cable.
	NMT indicator: Indicates that the MechanoSensor is connected to the NMT sensor cable.
	Post tetanic count indicator.
	Volume indicator. Adjust the volume of the tone that sounds.
	Sound volume adjustment indicator. Increasing bars indicate increase in sound volume level.
	Manual NIBP indicator. Start a manual NIBP measurement.
	NIBP Auto cycling indicator.
	Nellcor™ OxiMax™ SatSeconds™ alarm management indicator. Indicates the amount of time the SpO ₂ saturation is outside the limits before alarms are generated.
	SpO ₂ signal strength indicator. Indicates the signal strength, with three asterisks indicating the normal signal.

The following indicators appear in the software user interface.

	NMT Stimulus beep volume indicator. Adjust the volume of the tone that sounds when a stimulus pulse is generated.
 0 5min	Progress bar indicator. Indicates the amount of time remaining until the next automatic measurement.
	Refresh view indicator.
	Required input indicator.
	12SL print indicator.
	12SL PDF Viewer: Go back one page.
	12SL PDF Viewer: Go back ten pages.
	12SL PDF Viewer: Go to the last page.
	12SL PDF Viewer: Go forward one page.
	12SL PDF Viewer: Go forward ten pages.
	12SL PDF Viewer: Go to the first page.
	12SL PDF Viewer: Fit to screen.
	12SL PDF Viewer: Zoom in.
	12SL PDF Viewer: Zoom out.

Service requirements

Follow the service requirements listed below.

- Refer servicing of the equipment to qualified service personnel only. Service personnel servicing this product must have an appropriate technical qualification, or equivalent work experience, and be familiar with the service requirements

described in this manual and in any related service documentation. Service training for the product is recommended.

- Any unauthorized attempt to repair equipment under warranty voids that warranty.
- It is the user's responsibility to report the need for service to GE or to one of their authorized agents.
- Failure on the part of the responsible individual, hospital, or institution using this equipment to implement a satisfactory maintenance schedule may cause undue equipment failure and possible health hazards.
- Regular maintenance, irrespective of usage, is essential to ensure that the equipment will always be functional when required.

WARNING

PATIENT SAFETY. Do not perform any service activities on the monitor in the patient vicinity while a patient is connected to the monitor. Otherwise there is a risk of compromised patient safety.

CAUTION

DISPOSAL. At the end of its service life, the product described in this manual, as well as its accessories, must be disposed of in compliance with the guidelines regulating the disposal of each product. If you have any questions concerning disposal of a product, please contact GE or its representatives.

Product security

This manual contains instructions how to perform the configurations related to product security. For more information about the privacy and security considerations of the use of CARESCAPE B450, CARESCAPE B650 and CARESCAPE B850 monitors with software version 3.2, see Privacy and Security Manual.

4

Using the service applications

Introduction to the service applications

This chapter introduces the following service applications:

- CARESCAPE First Use Wizard
- CARESCAPE Service Interface
- CARESCAPE Multi Monitor Manager
- Service calibrations
- Remote service (InSite RSvP)

CARESCAPE First Use Wizard

CARESCAPE First Use Wizard opens when you turn on the patient monitor for the first time. The wizard provides you two options to set the passwords for all user accounts:

- You can activate a settings file that contains the passwords.
- You can enter the passwords manually.

The monitor will proceed to the normal monitoring screen only after the initial password setup is completed successfully.

For information about the user accounts, user privileges and password management see the Password Management section in this manual and the CARESCAPE B850, B650, B450 Privacy and Security Manual.

You can access the CARESCAPE First Use Wizard either locally at the monitor or with a service PC.

- To access CARESCAPE First Use Wizard locally, connect a USB keyboard and a USB mouse to the monitor.
- For more information on accessing CARESCAPE First Use Wizard with a service PC, see the Accessing the service applications with a service PC section.

Activating a settings file containing the passwords

Use only a settings file that has been downloaded from a monitor with CARESCAPE Software version 3.2.

Using a settings file that has been downloaded from a monitor with older monitor software will fail and the CARESCAPE First Use Wizard will open again.

1. Select **Choose File** under the **Settings activation**.

2. According to your access method:
 - a. If you are accessing First Use Wizard using a service PC, you can upload the settings file from any storage device connected to the service PC. Search the settings file from the destination drive and folder according to the instructions provided by the web browser. The web browser may also notify you about security issues. Refer to the web browser documentation for details.
 - b. If you are accessing First Use Wizard using the local monitor screen, you can upload the settings file from a USB flash drive:
 - i. Connect the USB flash drive to one of the monitor's USB ports.
 - ii. The service interface automatically detects the connected USB flash drive, searches the directory structure for files with .7z file extension, and requests the user to select the correct file.
 - iii. Choose the settings file you want to activate.

NOTE

Do not disconnect the USB flash drive until the uploading is complete.

3. Enter the password that was used for encrypting the settings file.
4. Select **Activate & Restart**.

The initial passwords setup is completed and the monitor will restart to the normal monitoring mode.

Entering passwords manually

1. Select **Passwords** under the *Set passwords manually*.
2. Enter and confirm passwords for all user accounts.
3. Select **Save & Restart**.

The initial passwords setup is completed and the monitor will restart to the normal monitoring mode.

CARESCAPE Service interface

With the CARESCAPE Service interface you can perform all the commonly needed service tasks to a single patient monitor at a time:

- Configure the platform settings of the monitor.
- Transfer settings from one monitor to another.
- Install software and software licenses.
- Retrieve system information for maintenance and troubleshooting, and access service log files.

You can access the service interface either locally at the monitor or with a service PC.

For more information on CARESCAPE B850 platform configuration, software and license management, and settings transfer, see the Configuration chapter. For information on accessing system and configuration information, troubleshooting tools, and service log files, see the Troubleshooting chapter.

For more information on the use of CARESCAPE ONE service interface, see CARESCAPE ONE Service Manual.

CARESCAPE Multi Monitor Manager

With the CARESCAPE Multi Monitor Manager you can install software and to transfer settings to multiple patient monitors at a time, over the IX Network.

For more information, see the Multi Monitor Manager appendix.

Service calibrations

With service calibrations, you can perform touchscreen, analog output, and parameter calibration. You can access these applications only locally at the monitor.

This manual only describes how to calibrate the touchscreen. For information on performing parameter and analog output calibrations, refer to the related CARESCAPE ONE, PDM or E-Module service manuals.

InSite RSvP

InSite RSvP is the GE remote service platform that provides a set of software applications to manage, diagnose and track systems at customer sites by using the Internet for secure communications between the customer's and GE's firewalls.

InSite RSvP consists of an enterprise server that resides at GE's support center, and a remote service agent that is installed to the monitor. The remote service agent can be configured and enabled using the service interface. Contact GE for more information about the InSite RSvP remote service platform.

User accounts and passwords for service applications

The patient monitor does not have any default passwords. The initial password setup must be completed using the CARESCAPE First Use Wizard when the patient monitor is turned on for the first time. Any future password changes are completed using CARESCAPE Service Interface.

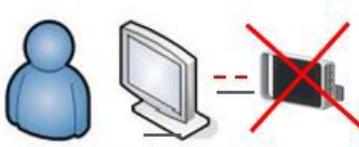
You can access all the following service applications with the same *biomed* and *service* user account and password:

- CARESCAPE Service interface
- CARESCAPE Multi Monitor Manager
- Service calibrations

For an overview about the user accounts, user privileges and password management see the Password Management chapter in this manual and the CARESCAPE B850, B650 and B450 Privacy and Security Manual.

Accessing the service interface locally from the monitor

You can access the CARESCAPE B850 service interface locally from the monitor's user interface.



Bx50 CS ONE

NOTE

No local access to connected CS ONE service interface.

Tools needed:

- A USB keyboard
 - A USB mouse
1. Connect the USB keyboard and the USB mouse to the monitor.
 2. Select **Monitor Setup > Defaults & Service > Service**.
 3. Type your username and password, and select **Log in**.

The service interface opens and defaults to the **Information** tab.

Accessing the service applications with a service PC

Checking the network settings of the target monitor

Check the network settings of the target CARESCAPE B850:

1. Select **Monitor Setup > Defaults & Service > Service**.
2. Write down the following information displayed on the login screen:
 - **Service IP Address**
 - **Service IP Netmask**
 - **Network type (Dual wire or Single wire)**

NOTE

By factory default, the **Network type** is **Dual wire**.

NOTE

- In the dual wire configuration, **Service IP Address /Netmask** is equal to **IX IP Address /Netmask**.
- In the single wire configuration, **Service IP Address /Netmask** is equal to **MC IP Address /Netmask**.

Configuring the network settings of the service PC

Configure your service PC to communicate with the CARESCAPE B850.

NOTE

To avoid IP conflicts, ensure that no other device in the same subnet uses the same static IP address.

1. Configure the service PC to operate in the same subnet with the CARESCAPE B850 monitor's **Service IP Address / Netmask**.

2. If you are connecting the service PC to CARESCAPE Network via a IEEE 802.1X protected network port, either enable IEEE 802.1X authentication on your service PC or utilize MAC Authentication Bypass (MAB). For more information, see CARESCAPE B850, B650, B450 Privacy and Security Manual.

Supported web browsers in service PC

The service applications have been verified to operate correctly with the following web browsers:

- Microsoft Internet Explorer version 11
- Google Chrome version 84
- Mozilla Firefox version 78

Secure access with service PC

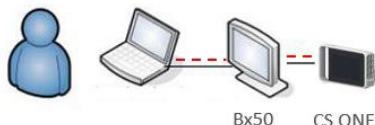
The service applications use the https protocol for secure communications between the monitor and the service PC. If a certificate recognized by the web browser running in the service PC is not installed into the monitor (web server), the web browser in the service PC will report about a certificate error and/or insecure network connection. The message shown depends on the web browser being used. The web browsers typically allow you to ignore the certificate errors and continue accessing the monitor.

By factory default, the monitor has a self-signed certificate installed by GE. To improve access security, GE recommends the responsible organization to install a valid security certificate issued by a trusted certificate authority to all the monitors. For more information, see the Certificate management section and the CARESCAPE B850, B650, B450 Privacy and Security Manual.

Accessing the service applications locally with a service PC

You can access the following service applications of either CARESCAPE B850 or CARESCAPE ONE locally with a direct cable connection from a service PC to the CARESCAPE B850:

- CARESCAPE First Use Wizard
- CARESCAPE Service Interface



NOTE

This connection method is not available in dual wire configuration, if IX Network is configured to obtain IP address from a DHCP server.

Tools needed:

- a service PC
- an Ethernet crossover cable

1. Connect the service PC to the CARESCAPE B850 according to the network configuration and the selected **Network Type**:
 - For dual wire configuration, connect the Ethernet cable to the IX connector of the monitor.
 - For single wire configuration, connect the Ethernet cable to the MC/IX connector of the monitor.
2. Configure the service PC to operate in the same subnetwork with the CARESCAPE B850. (**Service IP Address/ Netmask**).
3. Launch a web browser on the service PC.
 - a. To access the CARESCAPE First Use Wizard:
 - i. Type one of the following addresses in the address field of the browser according to your needs:
 - CARESCAPE 850: [https://\[IP address\]](https://[IP address])
 - CARESCAPE ONE: [https://\[IP address\]:8081](https://[IP address]:8081)

NOTE

[IP address] is the service IP address of the CARESCAPE B850. For instructions on checking this information, see the Checking the network settings of target monitor section. Port information, :8081, is needed as a suffix to access CARESCAPE ONE that is connected to the CARESCAPE B850.

- i. Press **Enter**.
- b. To access the CARESCAPE Service interface, type [https://\[IP address\]](https://[IP address]) in the address field of the web browser and press **Enter**:

NOTE

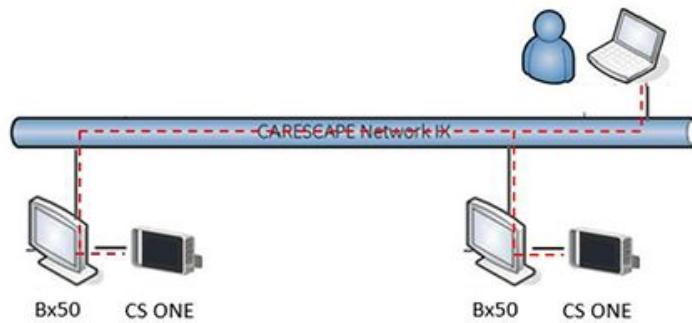
[IP address] is the Service IP address of the CARESCAPE B850. For instructions on checking this information, see the Checking the monitor network settings of the target monitor section.

- i. To access the CARESCAPE B850 monitor's service interface: type your username and password, and select **Log in**.
- ii. To access the CARESCAPE ONE service interface login screen, select **Open** on the CARESCAPE Service interface login screen. When the CARESCAPE ONE service interface login screen opens, use the username and password of the CARESCAPE ONE service interface.
For more information about the CARESCAPE ONE service interface refer to the CARESCAPE ONE Service Manual.

Accessing the service applications over IX network with a service PC

You can access the following service applications of a CARESCAPE B850, or a connected CARESCAPE ONE, over the IX Network:

- CARESCAPE First Use Wizard
- CARESCAPE Service Interface
- CARESCAPE Multi Monitor Manager



Tools needed:

- a service PC
- Ethernet patch cable

1. Connect a service PC either to the IX wall connector (dual wire), or to the MC/IX wall connector (single wire) with an Ethernet patch cable.
2. Configure the service PC to operate in the same subnetwork with the CARESCAPE B850. (**Service IP Address/ Netmask**).
3. Launch a web browser on the service PC
 - a. To access the CARESCAPE First Use Wizard:
 - i. Type one of the following addresses in the address field of the browser according to your needs:
 - CARESCAPE 850: **[https://\[IP address\]](https://[IP address])**
 - CARESCAPE ONE: **[https://\[IP address\]:8081](https://[IP address]:8081)**

NOTE

[IP address] is the service IP address of the CARESCAPE B850. For instructions on checking this information, see the Checking the network settings of target monitor section. Port information, :8081, is needed as a suffix to access CARESCAPE ONE that is connected to the CARESCAPE B850.

- i. Press **Enter**.
- b. To access the CARESCAPE Service interface, type **[https://\[IP address\]](https://[IP address])** in the address field of the web browser and press **Enter**.

NOTE

[IP address] is the Service IP address of the CARESCAPE B850. For instructions on checking this information, see the Checking the monitor network settings of the target monitor section.

- i. To access the CARESCAPE B850 monitor's service interface: type your username and password, and select **Log in**.
- ii. To access the CARESCAPE ONE service interface login screen, select **Open** on the CARESCAPE Service interface login screen. When the CARESCAPE ONE service interface login screen opens, use the username and password of the CARESCAPE ONE service interface.
For more information about the CARESCAPE ONE service interface refer to the CARESCAPE ONE Service Manual.
- c. For the instructions on how to access CARESCAPE Multi Monitor Manager, refer to the CARESCAPE Multi Monitor Manager appendix.

Accessing service calibrations

You can access the following service calibrations from the CARESCAPE B850 user interface:

- touchscreen calibration for B850 displays
 - analog output calibration for a connected CARESCAPE ONE or a CARESCAPE PDM
 - parameter calibrations for connected E-Modules, CARESCAPE PDM or CARESCAPE Parameters
1. Select **Monitor Setup > Defaults & Service > Service /Calibrations.**
 2. Enter your username and password, and then select **Enter.**
- The service calibrations menu opens on the monitor.

5

Pre-installation requirements

Unpacking

WARNING

EXCESSIVE LEAKAGE CURRENT. If the device has been transported or stored outside operating temperature range allow it to stabilize back to operating temperature range before removing it from the plastic bag and connecting it to the power line.

CAUTION

PACKAGING DISPOSAL. Dispose of the packaging material, observing the applicable waste control regulations.

1. Confirm that the packing box is undamaged. If the box is damaged, contact the shipper.
2. Open the top of the box and carefully unpack all components.
3. Confirm that all components are undamaged. If any of the components is damaged, contact the shipper.
4. Confirm that all components are included. If any of the components is missing, contact your GE distributor.

Pre-installation checklist

Before you start installing a monitor ensure the following:

- All the system components are compatible.
- The network infrastructure is properly installed, configured and tested.
- CARESCAPE Dock F0, CARESCAPE ONE and CARESCAPE Parameters are properly installed, configured and tested.
- Mounting solutions are properly installed.
- The Unity Network Interface Device (ID) is properly installed, configured and tested.
- The installation site meets power and environmental requirements.

System compatibility

WARNING

BEFORE INSTALLATION. Compatibility is critical to safe and effective use of this device. Verify the compatibility of all system components and device interfaces, including hardware and software versions, prior to installation and use.

WARNING	PATIENT SAFETY. When using any supply or accessory, make sure that you are familiar with their use to avoid any risk to the patient. For detailed instructions and information regarding supplies and accessories, always refer to their own instructions for use.
----------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Check the compatibility of all the system components before installing the monitor.

Pay special attention before installing a new monitor to an existing CARESCAPE installation. The compatibility may vary between different hardware and software versions.

Refer to the monitor's supplemental information manual for a list of compatible devices, including acquisition modules, input-output devices, network devices, mounts and Unity Network Interface Device (ID). Refer to Unity Network Interface Device (ID) Operator's Manual to see the compatible peripheral devices that can be interfaced to the monitor via Unity Network Interface Device.

For a list of the compatible supplies and accessories, see Supplies and Accessories Supplement.

Important security information

Failure to appropriately implement Network Access Controls on the network and enable them on the monitors, and all security protections (as outlined in the CARESCAPE Network Configuration Guide, Patient Monitoring Network Configuration Guide, and this manual) may result in risks to the functionality and performance of the monitors. As disclosed in the warning statements of these documents, this can impact patient monitoring data and functionality (for example, loss of monitoring), which could contribute to a delay in treatment or missed patient events, potentially leading to serious injury.

Checking the configuration of the wired CARESCAPE Network infrastructure

Before you connect any monitor to a wired network, ensure that the network infrastructure is properly installed, configured and tested. Refer to the CARESCAPE Network Configuration Guide, or Patient Monitoring Network Configuration Guide for details.

Contact the hospital IT for the information you need to properly connect and configure the monitor to the network, or optionally familiarize yourself with the network infrastructure design documents:

1. Check the configuration of the network infrastructure:
 - a. Find out how the network infrastructure is configured at the installation site. Monitors can be configured to the MC and IX Networks either using two network interfaces (dual wire configuration) or one network interface (single wire configuration).
 - In the dual wire configuration, separate Ethernet cables connect the monitor to the MC Network and IX Network.
 - In the single wire configuration, the monitor sends MC and IX traffic onto the MC network interface. The CARESCAPE Router is responsible for passing IX traffic from the MC network onto the IX network.

- b. Find out if the IEEE 802.1X port based authentication is enabled to the monitor's MC and IX network ports at the installation site. For the information needed to configure the monitor to authenticate to the network, see Configuring the wired CARESCAPE Network.
 - c. Refer to the following chapters in this service manual to find out the information you will need to connect and configure a monitor to operate correctly in the MC and IX Networks:
 - Connecting to the CARESCAPE Network
 - Configuring the wired CARESCAPE network
 - Setting unit and bed name
 - d. Ensure that the correct wall jacks and network patch cables are in place for the required network connections.
2. Identify the needed IX Network services and the correct settings for each service:
- Certificates
 - IX printing
 - Citrix
 - MUSE/12SL
 - InSite RSvP remote service
- Refer to the related configuration chapters in this manual for details of information needed.

About the monitor's MAC addresses

You can check the MAC addresses of the monitor's network interfaces on the service interface login screen:

- The **MC MAC address** field shows the MAC address for the **MC/ MC/IX** network interface.
- The **IX MAC address** field shows the MAC address for the **IX/ CSC** network interface.

CARESCAPE ONE installation

The CARESCAPE Dock F0, CARESCAPE ONE and CARESCAPE Parameters shall be properly mounted, installed, configured and tested as a standalone monitor according to the CARESCAPE ONE Service Manual before you connect it as an acquisition module to a monitor.

Mounting solutions

WARNING

PATIENT SAFETY. Use only manufacturer specified mounts to avoid the risk of any part of the equipment falling on the patient.

GE devices provide reliable mounting attachments to the mounts listed in the supplemental information provided. Follow mount manufacturer instructions for installation and loading.

Before installing the following system components, ensure that all the needed mounting hardware is properly installed:

- CPU, if applicable. The CPU can be installed using different kind of mounting options, including the Carestation machines or as a standalone on a table or a shelf.
- CARESCAPE D19KT displays.
- Module frames.
- CARESCAPE PDM.
- CARESCAPE ONE and CARESCAPE Dock F0.
- CARESCAPE RAD
- Unity Network ID connectivity device.

Unity Network Interface Device (ID)

The Unity Network Interface Device (ID) shall be properly installed, configured and tested according to the Unity Network ID Connectivity Device Service Manual before connecting it to the monitor.

Power and environmental requirements

Refer to the supplemental information manual for power and environmental requirements.

Power requirements

Ensure that the electrical installation of the relevant room complies with the requirements of the appropriate regulations.

The installation site shall have hospital-grade grounded power outlets and power cords for all system components.

Environmental requirements

WARNING

INACCURATE RESULTS. Do not use or store the equipment outside the specified temperature, humidity, or altitude ranges, or outside the specified performance range. Using or storing the equipment outside the specified operating environment or outside the specified performance range may cause inaccurate results.

WARNING

ERRONEOUS READINGS. Many factors may cause inaccurate readings and alarms, decreased perfusion, and or low signal strength:

- Environmental conditions:
 - Electromagnetic interference
 - Excessive ambient light
 - Electrical interference
 - Electrosurgery
 - Defibrillation - May cause inaccurate reading for a short amount of time.
 - Excessive patient/sensor motion. Artifact can simulate an SpO₂ reading, so that the device fails to sound an alarm. In order to ensure reliable patient monitoring, the

proper application of the probe and the signal quality must be checked at regular intervals.

Install the monitor to a location that meets the specified environmental requirements of operating temperature, humidity and atmospheric pressure.

Place each device in a location with sufficient ventilation. Observe the ventilation openings of a device and make sure not to obstruct them.

Electromagnetic compatibility safety precautions

WARNING	EQUIPMENT DAMAGE AND PATIENT SAFETY. Do not use the device in high electromagnetic fields (for example, during magnetic resonance imaging).
WARNING	EMC INTERFERENCE. The use of accessories, transducers and cables other than those specified may result in increased emissions or decreased immunity performance of the equipment or system.
WARNING	EMC. Magnetic and electrical fields are capable of interfering with the proper performance of the device. For this reason make sure that all external devices operated in the vicinity of the monitor comply with the relevant EMC requirements. X-ray equipment or MRI devices are a possible source of interference as they may emit higher levels of electromagnetic radiation. Changes or modifications to this device/system not expressly approved by GE may cause EMC issues with this or other equipment. This device/system is designed and tested to comply with applicable standards and regulations regarding EMC and needs to be installed and put into service according to the EMC information stated as follows: This device/system is suitable for use in all establishments other than domestic and those directly connected to the public low-voltage power supply network that supplies buildings used for domestic purposes. Mains power should be that of a typical commercial or hospital environment. Device is compliant to Class A.
WARNING	DEGRADED PERFORMANCE. Do not use portable RF communications equipment (including peripherals such as antenna cables and external antennas) closer than 30 cm (12 inches) to any part of this device/system, including cables specified by the manufacturer. Otherwise, the performance of this device/system may degrade.
NOTE	Electromagnetic disturbance may cause, for example, temporary loss of measurement or changes in the values or the appearance of the waveforms (such as excessive noise or a sine wave) on the CARESCAPE monitor.

Ensure that the monitor is isolated from sources of strong electromagnetic and radio frequency interference. Refer to the supplemental information manual for more information.

Pre-installation requirements

6

Hardware installation

Hardware installation

WARNING	PERSONAL INJURY. To avoid personal injury to users or any other persons moving in the vicinity of the cables or tubing, route all cables and tubing in such a way that they do not present a tripping hazard.
WARNING	EXPLOSION. Do not use this system in the presence of flammable anesthetics, vapors or liquids.
WARNING	PATIENT SAFETY. After transferring or reinstalling the device, always check that it is properly connected and all parts are securely attached. Otherwise, there may be a risk of something falling on the patient and causing injury.
WARNING	PATIENT SAFETY. If the monitor, module, or frame is dropped, have them checked by qualified service personnel before taking them back into use.
WARNING	EXCESSIVE TOUCH CURRENT - To avoid excessive patient leakage current, do not simultaneously touch the patient and the electrical connectors located at the rear panel of the CPU unit or within the module frame.
CAUTION	LOSS OF MONITORING. Leave space for circulation of air to prevent the device from overheating. The manufacturer is not responsible for damage to device caused by improperly vented cabinets, improper or faulty power, or insufficient wall strength to support device mounted on such walls.

Installing batteries

WARNING	EXPLOSION HAZARD. Do not incinerate a battery or store at high temperatures. Serious injury or death could result.
----------------	--------------------------------------------------------------------------------------------------------------------

Refer to CARESCAPE ONE Service Manual for information about CARESCAPE ONE battery installation and maintenance.

Installing the PDM battery

WARNING

EXPLOSION OR FIRE. Using non-recommended batteries could result in injury/burns to the patients or users. Only use batteries recommended or manufactured by GE. The warranty can be voided if non-recommended batteries are used.

NOTE: Refer to the CARESCAPE PDM Service Manual for information about PDM battery maintenance.

1. Open the battery door by gently pulling on the battery door pull tab.



2. Pull the battery tray out of the PDM using the battery tray strap and remove the battery from the battery tray.
3. Insert the new battery with the test button facing up and the arrow pointing into the PDM.



4. Press the battery door closed until it seals the battery compartment.

NOTE

The PDM battery needs to be fully charged before taking into clinical use.

Installing the CPU

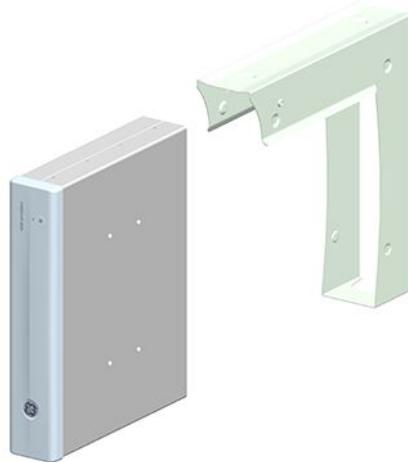
WARNING

PATIENT SAFETY. Never install the equipment above the patient to avoid the risk of any part of the equipment falling on the patient.

WARNING	PATIENT SAFETY. Use only manufacturer specified mounts to avoid the risk of any part of the equipment falling on the patient.
WARNING	EQUIPMENT MALFUNCTION. Using the CPU in a wrong position may result in equipment malfunction. The CPU must only be used in vertical or horizontal position. To avoid the risk of equipment malfunction, make sure that the CPU is not used in any other position.
WARNING	EQUIPMENT MALFUNCTION - When the CPU is used in vertical position, it is not protected against harmful effects of dripping water (IPX1). Therefore, we recommend using the CPU Flush Mount Kit with environment shield to provide protection from drips or splashes of liquids. Without the shield, liquids may enter the equipment and lead to its malfunction.
WARNING	ERRONEOUS READINGS. The device/system should not be used adjacent to, or stacked with, other equipment. Consult qualified personnel regarding device/system configuration.

The CPU has an integrated GCX mounting plate on the bottom enclosure to facilitate all mounting options, including mounting to the Carestation machines. Refer to the CARESCAPE Modular Monitors Mounting Solutions to identify compatible mounting solutions. You can also place the CPU on a table or a shelf.

1. Install the CPU to the mounting hardware according to the installation instructions delivered with the mount.
 - The optional flush mount lowers the probability of the ingress of fluids into the assembly. You can install the mount in two orientations. For details, refer to the installation instructions included with the flush mount.



Connecting the primary display

WARNING	MISSED ALARMS. Using other displays than B850 system specific ones may result in loss of visual alarms and patient monitoring.
----------------	--------------------------------------------------------------------------------------------------------------------------------

WARNING	EQUIPMENT DAMAGE. To prevent liquids from entering the display casing, do not tilt the display more than +/- 15 degrees.
WARNING	PATIENT SAFETY. Use only manufacturer specified mounts to avoid the risk of any part of the equipment falling on the patient.
NOTE	The maximum supported cable length of the USB and display cable is 5 meters. Video signal splitters are not supported.

Cables needed:

Interface	Equip- ment ID	Equipment type	GE Part number
USB	A	USB-A to USB-B cable, length: 1, 3, or 5 meters	For a list of compatible display cables and USB cables, see Supplies and Accessories Supplement.
Video	C	DVI-D to DVI-D cable, length: 1.0, 1.8, 3.0, or 5.0 meters	
	G	DisplayPort to DVI-D Adapter, shielded, 0,2 m	2093022-001

NOTE To ensure the proper operation of the display, touchscreen, alarm light and Trim Knob, always connect the primary display to the DisplayPort 1 and USB 1 connectors (blue).

Note the following:

For instructions on how to calibrate the touchscreen, see the configuration chapter.

For detailed instructions on how to adjust the display, refer to the display's user manual.

1. To connect the primary display:

- a. Connect a DisplayPort to DVI-D adapter (G) to the DisplayPort 1 connector (blue) on the rear panel of the CPU.
- b. Connect a DVI-D to DVI-D cable (C) to the DisplayPort to DVI-D adapter (G) and fasten the thumb screws.



- c. Connect the DVI-D to DVI-D cable (C) to the DVI connector on display and fasten the thumb screws.



- d. Connect a USB-A to USB-B cable (A) to the USB 1 connector (blue) on the CPU and to the USB Type B connector on the display.
2. Secure the USB cable connections to the CPU using the existing retaining clips attached to the CPU.



3. Follow the instructions included in the display package to secure the USB cable connections to the displays.
4. Ensure that the display is configured to accept digital input signal (DVI-I Digital). For more information, refer to the display's user documentation.

Connecting a secondary display

WARNING

EQUIPMENT DAMAGE. To prevent liquids from entering the display casing, do not tilt the display more than +/- 15 degrees.

WARNING

PATIENT SAFETY. Use only manufacturer specified mounts to avoid the risk of any part of the equipment falling on the patient.

WARNING

EXCESSIVE LEAKAGE CURRENT. A display or printer that is a non-medical grade device and is used within the patient environment, must always be powered from an additional transformer providing at least basic isolation (isolating or separating transformer). Using without an isolating transformer could result in unacceptable enclosure leakage currents.

NOTE

Video signal splitters are not supported.

NOTE

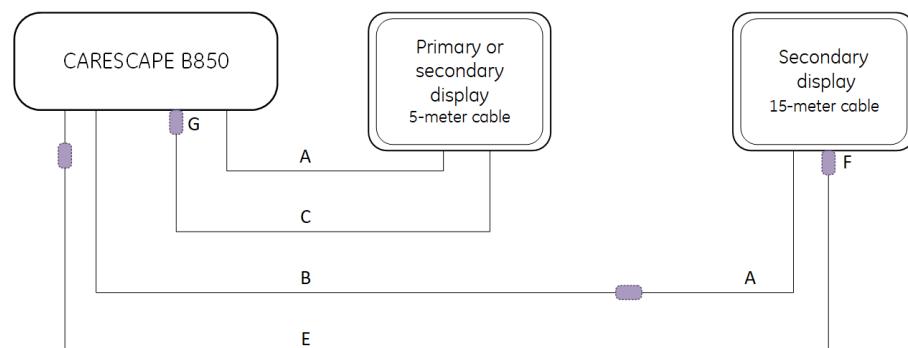
If a non-medical grade display is used as a secondary display within the patient environment it must always be powered from an additional transformer providing at least basic isolation.

The monitor supports one secondary display, that can be either a clone or an independent, user-configurable display. The independent secondary display requires a Dual Video license.

For instructions on how to calibrate the touchscreen, see the configuration chapter.

For detailed instructions on how to adjust the display, refer to the display's user manual.

You have two options to connect the secondary display. You can use either a 5- meter or a 15- meter cable connections.



Connecting a secondary display with 1 to 5 meter cables

Cables needed:

Interface	Equip- ment ID	Equipment type	GE Part number
USB	A	USB-A to USB-B cable, length: 1, 3, or 5 meters	For a list of compatible display cables and USB cables, see Supplies and Accessories Supplement.
Video	C	DVI-D to DVI-D cable, length: 1.0, 1.8, 3.0, or 5.0 meters	
	G	DisplayPort to DVI-D Adapter, shielded, 0,2 m	2093022-001

Note the following:

- To ensure the proper operation of the touchscreen, alarm light and Trim Knob, always connect the secondary display to the dedicated USB connector marked on the rear panel.

1. To connect the secondary display:
 - a. Connect a DisplayPort to DVI-D adapter (G) to the DisplayPort 2 connector (black) on the rear panel of the CPU.
 - b. Connect a DVI-D to DVI-D cable (C) to the DisplayPort to DVI-D adapter (G) and fasten the thumb screws.
 - c. Connect the DVI-D to DVI-D cable (C) to the DVI connector on display and fasten the thumb screws.
 - d. Connect a USB-A to USB-B cable (A) to the USB 2 connector (black) on the CPU and to the USB Type B connector on the display.
2. Secure the USB cable connection to the CPU using the existing retaining clips attached to the CPU.
3. Follow the instructions included in the display package to secure the USB cable connection to the displays.
4. Ensure that the display is configured to accept digital input signal (DVI-I Digital). For more information, refer to the display's user documentation.

Connecting a secondary display with 15-meter cables

Cables needed:

Interface	Equipment ID	Equipment type	GE Part number
USB	A	USB-A to USB-B cable (5 meters)	2044095-001
	B	USB extension cable, USB-A (male) to USB-A (female), (10 meters)	5848541
Video	D	DisplayPort to VGA adapter	5848542
	E	VGA cable (15 meters)	415301-304
	F	DVI-A TO VGA adapter	2042437-001

Note the following:

- To ensure the proper operation of the touchscreen, alarm light and Trim Knob, always connect the secondary display to the dedicated USB connector marked on the rear panel.
1. To connect the secondary display:
 - a. Connect a DisplayPort to VGA adapter (D) to the DisplayPort 2 connector (black) on the rear panel of the CPU.
 - b. Connect a VGA cable (E) to the DisplayPort to VGA adapter (D) and fasten the thumb screws.
 - c. Connect the VGA cable (E) to the DVI-A to VGA adapter (F). Fasten the thumb screws.
 - d. Connect the DVI-A to VGA adapter (F) to the DVI connector on the display and fasten the thumb screws.
 - e. Connect the USB extension cable (B) to the marked USB 2 connector (black) on the CPU.

- f. Connect the USB extension cable (B) to the USB-A to USB-B cable (A).
- g. Connect the USB-A to USB-B cable (A) to the USB Type B connector on the display.
2. Secure the USB cable connection to the CPU using the existing retaining clips attached to the CPU.
3. Follow the instructions included in the display package to secure the USB cable connections to the displays.
4. Ensure that the display is configured to accept analog input signal (DVI-I Analog). For more information, refer to the display's user documentation.

Installing module frames and modules

WARNING

ELECTRIC SHOCK - Do not use the F7 Frame for standalone use. Ventilation holes on the F7 E-module Frame will be covered only if installed within an Aisys CS², Avance CS², or Aespire anesthesia machine.

WARNING

EQUIPMENT MALFUNCTION - Using the module frames in a wrong position may result in equipment malfunction. The frames must only be used in horizontal position. To avoid the risk of equipment malfunction, make sure the frames are not used in any other position.

WARNING

PATIENT SAFETY. Do not use identical acquisition modules or modules that map a measurement to the same channel or parameter window. If such modules have been connected, remove the module that has been most recently connected. You can also remove both modules and reconnect the new module after five seconds. In some cases, using identical modules may lead to misinterpretations and therefore compromise the patient safety.

The monitor supports multiple parameter modules at a time. The two ePorts allow connection of F5 and F7 Frames, CARESCAPE ONE with CARESCAPE Dock F0, and CARESCAPE PDM.

See the following table for possible configuration options. For detailed information on compatibility, refer to the supplemental information manual.

		ePort1			
		CARESCAPE ONE with CARESCAPE Dock F0	CARESCAPE PDM	F5 Frame	F7 Frame
ePort2	CARESCAPE ONE with CARESCAPE Dock F0			X	X
	CARESCAPE PDM			X	X
	F5 Frame	X	X	X	
	F7 Frame	X	X		

In the table above:

- X = supported
- Empty = not supported

For example: If a F5 Frame is connected to ePort 1, you can connect only one of the following devices to the ePort 2:

- CARESCAPE ONE with CARESCAPE Dock F0
- CARESCAPE PDM
- F5 Frame

Connecting an F5 or an F7 Frame to the CPU

Cables needed:

- Frame-CPU Cable

Refer to the patient monitor's supplemental information manual for a list of compatible cables.

1. Connect an F5 or F7 frame to an ePort connector on the rear panel of the CPU.



2. Tighten the thumbscrews with a screwdriver to ensure proper grounding of the frame.

Connecting a PDM to an F5 Frame

1. Connect the module by aligning it with the insertion guides of the docking station on the outside of the frame.
2. Push the module into the docking station until it clicks and stops.



Connecting E-modules

WARNING	ERRONEOUS READINGS. Ensure that the CARESCAPE respiratory modules are in vertical position when used. Tilting them may result in erroneous readings.
WARNING	PATIENT SAFETY. Do not use the E-musb and CARESCAPE ONE simultaneously in the same monitoring system. If you are using the E-musb module, disconnect any connected CARESCAPE Parameters from the E-musb module before connecting CARESCAPE ONE to the monitor and connect them to CARESCAPE ONE instead. If E-musb and CARESCAPE ONE are both connected to the monitor, the measurement with E-musb stops. This may compromise patient safety.
NOTE	An E-module can occupy any slot in the frame, no specific order is required.

1. With the module properly oriented (module release latch facing down), align the insertion guide slot in the module with the insertion guide in the module frame.
2. Push the module into the module frame until it clicks.



Connecting a PDM to an ePort connector

WARNING	PHYSICAL INJURY. Take care when mounting devices to an IV pole. If a device is mounted too high the IV pole may become unbalanced and tip over.
WARNING	PHYSICAL INJURY. Do not install the PDM above a patient. Make sure the battery is completely inserted and the battery door is completely closed. Falling batteries could seriously or fatally injure neonatal or other vulnerable patients.
WARNING	PHYSICAL INJURY. Do not install the PDM above a patient. Leaks from the battery cells can occur under extreme conditions. The liquid is caustic to the eyes and skin. If the liquid comes in contact with eyes or skin, flush with clean water and seek medical attention.
WARNING	PHYSICAL INJURY. For safety reasons, all connectors for patient cables and sensor leads are designed to prevent inadvertent disconnection, should someone pull on the leads. Do not route cables in a way that they may present a stumbling hazard.

WARNING

EQUIPMENT DAMAGE. To avoid accidental ingress of liquids, do not tilt the PDM in any direction or mount the PDM in a vertical position with the patient cables facing up or down.

Mounting options include mounting to a bed headboard or footboard, an IV pole, or a roll stand using one of the docking stations. Mounting kits include all necessary hardware and installation instructions. Ensure that the selected PDM mount is properly installed according to the installation instruction.

Cables needed:

- Cable assembly ePort pod to host cable

For a list of compatible cables, see Supplies and Accessories Supplement.

1. Connect the PDM module to the installed mounting hardware as instructed in the accompanying installation instructions.
2. Connect one end of the ePort cable to the PDM and the other end of the ePort cable to the ePort connector in the rear panel of the monitor.



Connecting CARESCAPE Dock F0 to an ePort connector

Ensure that the CARESCAPE Dock F0, CARESCAPE ONE and CARESCAPE Parameters are properly mounted, installed, configured and tested as a stand-alone monitor according to the CARESCAPE ONE Service Manual before connecting it as an acquisition module to the monitor.

WARNING

PATIENT SAFETY. Do not use identical acquisition modules or modules that map a measurement to the same channel or parameter window. If such modules have been connected, remove the module that has been most recently connected. You can also remove both modules and reconnect the new module after five seconds. In some cases, using identical modules may lead to misinterpretations and therefore compromise the patient safety.

WARNING	PATIENT SAFETY. Do not use the E-musb and CARESCAPE ONE simultaneously in the same monitoring system. If you are using the E-musb module, disconnect any connected CARESCAPE Parameters from the E-musb module before connecting CARESCAPE ONE to the monitor and connect them to CARESCAPE ONE instead. If E-musb and CARESCAPE ONE are both connected to the monitor, the measurement with E-musb stops. This may compromise patient safety.
----------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

CARESCAPE ONE and PDM are considered identical and should not be used simultaneously in the same monitoring system.

CARESCAPE ONE and E-musb cannot not be used simultaneously in the same monitoring system.

There are two options to connect the CARESCAPE Dock F0 to the monitor. The connection method depends on the distance between the monitor and CARESCAPE Dock F0.

Connecting CARESCAPE Dock F0 with a 1.5- or 4.5-meter cable

If a 1.5- or 4.5-meter cable is used, the host monitor provides power for the CARESCAPE ONE and charges the CARESCAPE ONE battery.

Cables needed:

- Cable assembly, ePort CARESCAPE ONE to host, 1.5 m (5 ft) or 4.5 m (15 ft)
1. Connect one end of the ePort cable to the ePort connector in the rear panel of the CPU.
 2. Connect the other end of the ePort cable to the ePort connector in the CARESCAPE Dock F0.
 3. Tighten the thumbscrews with a screwdriver in both ends of the cable to secure the connection.



Connecting CARESCAPE Dock F0 with a 30-meter cable

If a 30-meter cable is used, the CARESCAPE Dock F0 shall be powered by its external power supply.

NOTE	With the 30-meter cable the host monitor does not provide power to the CARESCAPE ONE, or charge the CARESCAPE ONE battery. The CARESCAPE Dock F0 shall always be powered by the external power supply.
-------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Cables needed:

- Cable assembly, ePort Ethernet CARESCAPE ONE to host, 30 m (98.5 ft)
1. Ensure the F0 frame is powered by an external power supply unit.
 2. Connect the cable to the ePort connector in the CARESCAPE Dock F0.
 3. Connect the other end of the cable to the ePort connector in the host monitor.
 4. Tighten the cable locking screws in both ends to secure the connection.

Connecting to the mains power

WARNING	ELECTRIC SHOCK. To avoid the risk of electric shock, use only AC power cords recommended or manufactured by GE.
WARNING	EXCESSIVE LEAKAGE CURRENT. A display or printer that is a non-medical grade device and is used within the patient environment, must always be powered from an additional transformer providing at least basic isolation (isolating or separating transformer). Using without an isolating transformer could result in unacceptable enclosure leakage currents.
WARNING	EXCESSIVE LEAKAGE CURRENT - To avoid summation of leakage currents when interfacing the device with other equipment, the devices may only be interconnected with each other or to parts of the system when it has been determined by qualified biomedical personnel that there is no danger to the patient, the operator, or the environment as a result. In those instances where there is any element of doubt concerning the safety of the connected devices, the user must contact the manufacturers concerned (or other informed experts) for proper use. In all cases, safe and proper operation should be verified with the applicable manufacturer's instructions for use, and system standards IEC60601-1 must be complied with.
WARNING	ELECTRIC SHOCK. To avoid the risk of electric shock, do not under any circumstances remove the grounding conductor from the power plug. Always check that power cord and plug are intact and undamaged.
WARNING	POWER SUPPLY - Always connect the device power cable to a properly installed power outlet with protective earth contacts before connecting any network cables (MC and IX networks). If the integrity of the protective earth conductor is in doubt or there is no protective earth available, do not connect the monitor to the power line. All devices of a system must be connected to the same power supply circuit. Devices which are not connected to the same circuit must be electrically isolated when operated.
CAUTION	POWER REQUIREMENTS. Before connecting the device to the power line, check that the voltage and frequency ratings of the power line are the same as those indicated on the device's label. If this is not the case, do not connect the system to the power line. The manufacturer is not responsible for damage to the device caused by an improper or a faulty power.

1. Connect the power cords to the mains power supply inlet and to a wall outlet on all system components that require AC mains power input, including:
 - the CPU
 - all the connected displays
 - the optional Unity Network ID connectivity device
 - the optional local printer
 - the optional recorder
2. Secure all power cords by routing through the retaining clips or cable clamps, as applicable.



Connecting to the CARESCAPE Network

WARNING

EXCESSIVE LEAKAGE CURRENT. Only devices that are specified compliant with IEC 60950-1 or IEC 60601-1 may be connected to the Ethernet ports.

Connect the monitor to the CARESCAPE Network depending on the configuration of the network infrastructure at the installation site. The following questions can help you to find the right configuration at the installation site:

- Do the Ethernet ports support dual wire or single wire connection?
 - Is IEEE 802.1X port based authentication enabled or disabled?
1. Connect the cables according to the network configuration and the selected **Network type**:
 - For dual wire configuration, connect MC Ethernet patch cable to the MC connector, and the IX Ethernet patch cable to the IX connector in the rear panel of the monitor.
 - For single wire configuration, connect MC/IX Ethernet patch cable to the MC/IX connector in the rear panel of the monitor.

Connecting a Unity Network ID connectivity device to the monitor

Install, configure and test the Unity Network ID connectivity device according to the Unity Network ID Service Manual after completing the monitor installation.

WARNING

BEFORE INSTALLATION. Compatibility is critical to safe and effective use of this device. Verify the compatibility of all system components and device interfaces, including hardware and software versions, prior to installation and use.

1. Connect a Unity Network ID connectivity device to the Ethernet connector labelled "ID" in the rear panel of the monitor.

Connecting USB input devices

WARNING

EQUIPMENT DAMAGE. Use only washable keyboard with at least IPX1 protection against ingress of water. Other types of keyboards may get damaged by water during cleaning.

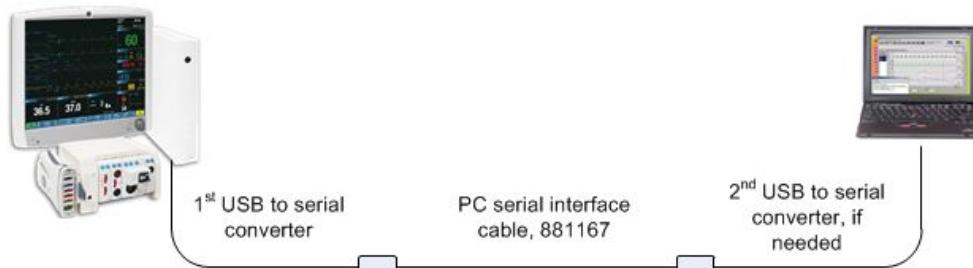
1. Connect the following devices to the USB ports in the rear panel of the monitor or at the bottom of a secondary display:
 - keyboard
 - mouse
 - remote control
 - barcode reader

Connecting iCollect and other data acquisition systems

You can connect iCollect and other data acquisition systems to one of the USB connectors of the monitor.

Cables needed:

- 1 or 2 USB to serial converter
 - PC serial interface cable, 881167
1. Connect a USB to serial Converter to one of the USB connectors of the monitor.
 2. Connect the converter to the PC serial interface cable.
 3. Connect the other end of the PC serial cable to the PC. Use another USB to serial converter, if needed.

**NOTE**

Refer to the iCollect User's Manual for more information about the iCollect.

Contact GE Service to get more information about interfacing other data acquisition systems to the patient monitor.

Connecting a local printer

WARNING

EXCESSIVE LEAKAGE CURRENT. A display or printer that is a non-medical grade device and is used within the patient environment, must always be powered from an additional transformer providing at least basic isolation (isolating or separating transformer). Using without an isolating transformer could result in unacceptable enclosure leakage currents.

WARNING

EXCESSIVE LEAKAGE CURRENT. Laser printers are not IEC 60601-1 certified equipment and may not meet the leakage current requirements of patient care equipment. This equipment must not be located in the patient environment unless the medical system standard IEC 60601-1 clause 16 is followed. Do not connect a laser printer to a multiple socket outlet supplying patient care equipment. The use of multiple socket outlet for a system will result in an enclosure leakage current equal to the sum of all the individual earth leakage currents of the system if there is an interruption of the multiple socket outlet protective earth conductor. Consult your local service representative before installing a laser printer.

NOTE

Refer to the printer manual on how to install and configure the printer. The printer shall be configured to communicate in the same subnet with the patient monitor's IX Network settings.

Cables needed:

- Ethernet crossover cable

You can connect a local laser printer directly to the monitor's IX connector with a crossover cable if the selected **Network type** is **Dual wire** and the monitor is not connected to the IX Network. The monitor considers a local printer to be an IX printer.

1. Connect the Ethernet crossover cable to the IX connector in the rear panel of the monitor.
2. Connect the other end of the Ethernet crossover cable to the connector in the laser printer.

Connecting a local PRN 50-M+ recorder

You can connect a local PRN 50-M+ recorder directly to the recorder port in the rear panel of the monitor.

Cables needed:

- Cable assembly RJ45 white cable

Refer to the patient monitor's supplemental information manual for a list of compatible cables.

1. Connect the cable to the recorder connector in the rear panel of the monitor.
2. Connect the other end of the cable to the connector in the PRN 50-M+ recorder.

After completing the monitor installation: install, configure and test the PRN 50-M+ recorder according to the PRN 50-M+ Writer Service Manual delivered with the recorder.

Connecting to CARESCAPE RAD

Cables needed:

- USB-A to USB-B cable

For a list of compatible cables, see Supplies and Accessories Supplement.

1. Connect the USB cable of the CARESCAPE RAD to one of the USB connectors in the rear panel of the monitor.

Install, configure, and test the CARESCAPE RAD according to the CARESCAPE RAD Service Manual after completing the monitor installation.

Connecting a remote-on cable

Remote-on connection allows you to power-up the monitor from the power switch of a GE anesthesia workstation.

NOTE

Remote-on connection is possible only if the anesthesia workstation supports this feature. Refer to the anesthesia workstation documentation for details.

Cables needed:

- remote-on cable

1. Connect the remote-on cable to the remote-on connector in the rear panel of the CPU.
2. Connect the other end of the remote-on cable to the related connector on the anesthesia workstation.

Hardware installation

7

Configuration

Platform configuration

The configuration of a monitor consists of platform configuration and clinical configuration.

This chapter describes:

- The platform configuration needed before taking the monitor into use for the first time.
- The configuration tasks needed for administration and maintenance.

For information on how to perform the clinical configuration, including care unit settings and user profiles, refer to the user manual.

Adjusting display

Selecting display input signal source

The display shows a **No Sync** message, if the input source is incorrectly configured, or no signal is received. Change the input source from the displays OSD menu as follows:

- For 1 to 5 meter cable connection, select: **DVI-I Digital**.
- For a 15 meter cable connection, select: **DVI-I Analog**.

For more information, refer to the display's user documentation.

Adjusting display brightness and picture

If needed, adjust the display's brightness and picture using the display's OSD menu. For more information, refer to the display's user documentation.

Setting up the displays

With the Dual video license enabled, the user can select the screen where menus, alarms and Citrix applications are shown, and the size of the Citrix application.

1. Select **Monitor Setup > Defaults & Service > Default Setup**.
2. Enter your user name and password, and select **Enter**.
3. Select **Care Unit Settings > Screens**.

Refer to the monitor's user manual for detailed information on how to set up the screens.

Calibrating touchscreen

The calibration data of the connected displays is saved in the monitor CPU assembly. Calibration may be needed when changing the connected displays or after replacing the monitor CPU assembly.

If needed, calibrate a touchscreen as follows:

NOTE Touchscreen calibration is only available if the monitor is in a patient discharged/case end state.

1. Select **Monitor Setup > Defaults & Service > Service /Calibrations**.
2. Enter the username and password, and then select **Enter**.
3. In the **Service /Calibrations** menu, select the touchscreen to calibrate:
 - a. To calibrate the touchscreen of the primary display, select **Touch Screen**.
 - b. To calibrate the touchscreen of the optional secondary display, select **Secondary Touch Screen**.

The Touch calibration screen opens.

4. Touch the cross hairs (+) on the screen one by one until you have touched all three cross-hairs.

The calibration is now completed, and the touchscreen calibration window will close. The touchscreen calibration data for the display will be saved to the permanent memory of the monitor.

Configuring wired CARESCAPE network

Configuring the hostname

The hostname is a unique identifier of a monitor in the network. The factory default value for the hostname is the Serial Number of the monitor.

1. Log in to the service interface.
2. Select **Configuration > Network > Configuration**.
3. Enter the **Hostname** following these rules:
 - Use alphanumeric characters A-Z, a-z, 0-9.
 - You may also use characters “-” and “_”, but not in the beginning or in end of the hostname.
 - The hostname must be 4 to 32 characters long.
4. Select **Save**.

The change will take effect immediately.

Wired LAN Certificate Management

The IEEE802.1X port based authentication supports the use of a CA certificate to control access to wired MC and/or IX Networks. If CA certificate is in use, you must

first upload it to the monitor before you can select it. Certificate can be in PEM or DER format.

Uploading certificates

1. Log in to the service interface.
2. Select **Configuration > Network**.
3. Select **Certificate Management**.
4. In **Upload Certificate**, select the CA certificate and select **Upload**.
5. According to your service interface access:
 - a. If you are using a service PC, you can upload the certificate from any storage device connected to the service PC:
 - i. Search the Certificate file from the destination drive and folder according to the instructions provided by the web browser.
The web browser may also notify you about security issues. Refer to the web browser documentation for details.
 - b. If you are using the local, integrated service interface, you can upload the certificate from a USB flash drive that is connected to one of the monitor's USB ports.
 - i. The service interface automatically detects a connected USB flash drive and requests the user to select the correct file.
 - ii. Choose the Certificate file you want to upload.

NOTE

Do not disconnect the USB storage device until uploading is complete.

The configuration changes take effect immediately.

Deleting certificates

Note that you cannot delete a certificate or a key, if it is currently in use.

1. Log in to the service interface.
2. Select **Configuration > Network**.
3. Select **Certificate Management**.
4. In **Delete Certificate**, select the CA certificate and select **Delete**.

The selected certificate is permanently deleted.

Wired CARESCAPE Network configuration

The configuration of the wired CARESCAPE Network depends on how the network infrastructure has been configured at the installation site:

- In the dual wire configuration, MC and IX network traffic flows through two separate network interfaces, the **MC** and **IX** ports. Therefore, you need to configure two network interfaces, **MC** port for the MC Network and **IX** port for IX Network.
- In the single wire configuration, MC and IX network traffic flows through a single physical network interface, the **MC/IX** port. Therefore, you need to configure only the **MC/IX** network interface to support both the MC and IX Network communication.

Contact the hospital IT for the information you need to properly connect and configure the monitor to the network, or optionally familiarize yourself with the network infrastructure design documents.

NOTE

The following IP addresses are reserved and not valid:
127.0.0.0/8, 172.16.254.254/32, 172.16.255.255/32,
172.18.254.254/32, 172.18.255.255/32, 192.168.249.0/24,
192.168.250.0/24, 192.168.252.0/24, 192.168.253.0/24.

Selecting the network type

1. Log in to the service interface.
2. Select **Configuration > Network > Configuration**.
3. According to the network configuration used at the installation site, select **Network Type: Dual wire** or **Single wire**.

Configuring the dual wire network

1. To configure the MC Network, configure the following settings in the **MC Network** area below **Network**:
 - a. Enter a **Static IP** address.
 - b. Enter a valid **Netmask**.
 - c. If IEEE 802.1X port based authentication is in use for accessing the MC Network, continue as instructed in the Configuring IEEE 802.1X port based authentication section. Otherwise, proceed to the next step.
2. To configure the (optional) IX Network, configure the following settings in the **IX Network** area below **Network**:
 - a. Select **DHCP** (if dynamic IP address is used) or **Manual Configuration** (if static IP address is used).
If you select **DHCP**, the following are obtained automatically from the DHCP server: **Static IP** address, **Netmask**, and **Default Gateway**.
If you select **Manual Configuration**:
 - i. Enter a **Static IP** address.
 - ii. Enter a valid **Netmask**.
 - iii. Optional: Enter the IP address of the **Default Gateway** between the IX Network and the hospital network.
 - b. Enter the IP address for the **DNS Server 1**. You can also leave the **DNS Server 1** field empty, if DNS servers are not in use or if DNS server addresses are provided by the DHCP server.
 - c. To configure additional DNS servers, select **Add DNS server** and enter the IP address for the DNS Server.
You can configure up to 3 DNS servers manually.
3. Select **Save**.

The change will take effect after the next monitor restart.

Configuring the single wire network

1. Configure the following settings in the **MC Network** area below **Network**:
 - a. Enter a **Static IP** address.
 - b. Enter a valid **Netmask**.
 - c. Optional: Enter the IP address of the **Default Gateway** between the IX Network and the hospital network.
 - d. Enter the IP address for the **DNS Server 1**.
You can configure up to 3 DNS servers manually. You can also leave the **DNS Server 1** field empty, if DNS servers are not in use.
 - e. To configure additional DNS servers, select **Add DNS Server** and enter the IP address for the DNS Server.
2. If IEEE 802.1X port based authentication is in use for accessing the MC and IX Network, continue as instructed in the Configuring IEEE 802.1X port based authentication section. Otherwise, proceed to the next step.
3. Select **Save**.

The change will take effect after the next monitor restart.

Configuring the IEEE 802.1X port based authentication

If IEEE 802.1X port based authentication is in use for accessing the network, configure the following settings.

1. Select the **802.1X Authentication** radio button.
2. For the **EAP Method**, select one of the following:
 - **TLS**
 - **TTLS-MSCHAPV2**
 - **PEAP-MSCHAPV2**
 - **PEAP-GTC**

The following table shows which additional settings you must configure, depending on the selected **EAP Method**:

Setting	TLS	TTLS-MSCHAPV2	PEAP-MSCHAPV2	PEAP-GTC
CA Certificate	Recommended	Recommended	Recommended	Recommended
Client Certificate	Yes, if not included in the Private Key	No	No	No
Private Key	Yes	No	No	No
Private Key Password	Optional	No	No	No
Identity	Optional	Yes	Yes	Yes
Password	No	Yes	Yes	Yes
Anonymous Identity	No	Optional	Optional	Optional

3. Select which **CA Certificate** is used.

Before selecting the CA certificate, you must upload it to the monitor in **Configuration > Network > Certificate Management**. Using CA certificate is highly recommended for improved security.

4. Select which **Client Certificate** is used.

Before selecting the client certificate, you must upload it to the monitor in **Configuration > Network > Certificate Management**. The client certificate is only required if the selected EAP method is TLS and it is not included in the private key.

5. Select which **Private Key** is used.

Before selecting the private key, you must upload it to the monitor in **Configuration > Network > Certificate Management**. The private key is required if the selected EAP method is TLS. If a p12 package is used as a private key, it contains both the private key and the client certificate, and you can leave the client certificate selection empty.

6. Enter the **Private Key Password**.

A valid private key password must contain from 0 to 255 visible (printable) ASCII characters. Select **Help** to see the complete list of allowed characters.

7. Enter the **Identity**.

A valid identity string must contain:

- With **TLS** as **EAP Method**: from 0 to 255 visible ASCII characters
- With any other supported **EAP Method**: from 1 to 255 visible ASCII characters
- Select **Help** to see the complete list of allowed characters.

8. Enter the **Password**.

A valid password must contain from 1 to 255 visible ASCII characters. The password is required by all other supported EAP methods except TLS. Select **Help** to see the complete list of allowed characters.

9. Enter the **Anonymous Identity**.

The anonymous identity is used as the unencrypted identity with EAP types that support a different tunneled identity. A valid anonymous identity string must contain from 0 to 255 visible ASCII characters, it is optional, and it is supported by all other EAP Methods except TLS. Select **Help** to see the complete list of allowed characters.

10. For dual wire configuration: perform steps 2-9 for the MC Network and (if used) the IX Network.

11. Select **Save**.

The change will take effect after the next monitor restart.

Configuring date and time

CAUTION

NETWORK DEVICE TIME SYNCHRONIZATION - When adding a new device to the CARESCAPE Network, the existing devices on the CARESCAPE Network will synchronize to the new device's time. To prevent potential time synchronization issues, you should set the new device's time to be as close as possible to the time (within one minute or less) used by the existing GE devices on the CARESCAPE Network.

1. Log in to the service interface.
2. Select **Configuration > Time**.
The **Time Configuration** window displays.
3. **Clock type**, select the type from the drop-down list:
 - a. Select either **12 Hours** or **24 Hours**.
 - b. Select **Save**.
4. **Configure Date and Time**, enter the local date and time:
 - a. To automatically fill in the current date and time, select the **Fill with current monitor time** button.
The current date and time will be filled into the data fields.
 - b. To manually enter the date and the time, enter the following information:
 - **Date**: use YYYY-MM-DD date format.
 - **Time**: use HH:MM:SS time format.
 - **AM/PM**: This applies when the clock type is set to **12 Hours**.
 - c. Select **Save**.
5. **Configure UTC Offset**: Select the Coordinated Universal Time (UTC).

NOTE

- The UTC Offset configuration applies only to the communication with a Citrix server. It does not affect the date and time of the monitor's real-time clock.

- a. Select the local UTC Offset setting from the drop-down list.
- b. Select **Save**.

The manual time configuration takes effect immediately.

Setting unit and bed name

Configure the care unit name and bed name for monitors that are configured to connect to the MC Network.

NOTE

All the monitors and central stations that are connected to the same care unit in the MC Network must have the same unit name. Bed name must be unique to each monitor in the same care unit.

NOTE The clinical user may have a need to change the initially set unit and/or bed name via clinical user interface if the monitor is moved, or roved, to a new location in the CARESCAPE Network. To allow this, configure the related settings through **Monitor Setup > Defaults & Service > Default Setup > Care Unit Settings > Roving**. Refer to user manual for more information about the roving feature.

1. Log in to the service interface.
2. Select **Configuration > Unit and Bed Name**.
3. Enter the **Unit Name**.
4. Enter the **Bed Name**.

NOTE Use only capital letters A to Z, numbers from 0 to 9, dash (-), and space (). The unit name may be up to seven characters long and bed name up to five characters long. Names may not be identical.

5. Select **Save**.

The change will take effect immediately.

Configuring printers

You can configure the monitor to print to up to 12 laser printers connected on the IX Network, or to a local printer that is connected to the IX Network connector in the rear panel of the monitor.

Printer installation consists of the following main steps:

1. Installation and configuration of the printer to IX Network according to the printer documentation:
 - Refer to the supplemental information manual for the list of compatible laser printers.
 - Refer to the printer's service manual for printer installation instructions.
 - Ensure that you have the host names or IP addresses for all connected IX printers available for monitor configuration.
 - Notice that the printer driver is part of the monitor software.
2. Configuration of the monitor to print to the installed IX printers:
 - Use monitor's service interface to add a new printer, and to print a test page.
 - Use monitor's clinical user interface to configure which monitor printouts are directed to which printer. See monitor's user manual for more information about the printing and different printouts.

NOTE If a laser printer is installed directly on a CARESCAPE central station, see the central station service manual for more information.

Adding a printer

1. Log in to the service interface.
2. Select **Configuration > Printers**.

3. Select **Add Printer**.
4. Enter the following information:
 - a. Enter either the **Hostname** or **IP Address** of the printer.
 - b. Provide a user-assigned name for the printer in the **Printer name** field.
 - c. Select **Print test page**.

A successfully printed test page ensures that the printer and the monitor configuration is completed correctly, and there are no incompatibility issues.
5. Select **Add Printer**.

The change will take effect immediately.

Selecting printout types and print locations

1. From the monitor main menu, select **Monitor Setup > Main Setup > Printing**.
2. Select **Devices** tab.
3. Select **Setup**.
4. Select the printout type from the **Printout** list.
For example, select **Waveforms** or **Numeric Trends**.
5. From the printout **Location** options, select the **Network** radio button.
6. From the **Network Device** list, select the correct printer.

The change will take effect immediately.

Printing a test page

1. Log in to the service interface.
2. Select **Configuration > Printers**.
3. From the list of the installed IX printers, select the printer that you want to test.
4. Select **Print test page**

If the printing fails, check that the printer is compatible and correctly configured.

Deleting a printer

NOTE

Before deleting a laser printer, check **Monitor Setup > Main Setup > Printing > Devices > Status**. If a printout is assigned to the printer to be deleted, redirect the printout to another valid printer.

1. Log in to the service interface.
2. Select **Configuration > Printers**.
3. From the list of installed printers, select the printer that you want to delete.
4. Select **Delete**.

The change will take effect immediately.

Configuring Citrix

The CARESCAPE monitor contains a built-in Citrix Client that provides the ability to show external Windows applications or desktops running on the XenApp server as if the applications were executing locally on the monitor.

For more information refer to:

- CARESCAPE Citrix Guide about Citrix implementation, installation and configuration
- Supplemental information manual about the supported Citrix XenApp versions.
- Citrix product documentation at www.citrix.com about Citrix.

Contact the hospital's IT Administrator or biomedical department to get the needed information for the built-in Citrix client configuration.

1. Log in to the service interface.
2. Select **Configuration > Citrix**.
3. Select **Enabled** to enable Citrix configuration.
4. Enter the values to the following fields:

Item	Description
Server Address 1 to 4	Enter the IP address or DNS name of the XenApp server hosting the published application or hosted desktop. You can enter up to four server addresses. The Server Address 1 is always mandatory. To add an other server, select Add a server , and enter the information of the additional server. The Server address consists of IP address or a host name, followed by an optional port number, which is separated by a colon. The maximum length of a host name is 255 characters. An example of an IP address with the optional port number is 3.187.230.30:8080.
Initial Program	The name of the application or desktop resource as published in the XenApp. For example #MUSE. This field is mandatory. The maximum length is 128 characters.
Session Timeout	This client side timeout affects only a normal sized application window when it is hidden behind a menu. A full screen application is never hidden behind a menu and this timeout does not affect it. Keeping the session alive allows users to quickly return to their last session, but locks a Citrix license. Valid values are between 0-99 in minutes. Selecting "0" disables the timeout.

Item	Description
Username Password	<ul style="list-style-type: none"> To enable device specific Citrix credentials configuration, configure the Windows user account and password. Give the username in the form "domain\username". To enable user specific Citrix credentials configuration, leave the username and password fields empty. The user will be prompted to login when Citrix session is initiated (the  button is pressed). <p>NOTE: The user name and password shall be in valid Windows format and the maximum length is 128 characters.</p> <p>For more information about user and device specific Citrix credentials, refer to the CARESCAPE Citrix Guide.</p>
Encryption Level	Select the encryption level: <ul style="list-style-type: none"> Basic RC5 – 128 bit - Login Only RC5 – 40 bit RC5 – 56 bit RC5 – 128 bit
Load balancing:	Select either Enabled or Disabled : If the Load Balancing is disabled, Citrix will connect directly to the first server address. If it is enabled, Citrix client will query the first available server which tells the client where to connect to.

5. Select **Save**.

The change will take effect immediately.

NOTE To disable Citrix client, select **Disabled**. All configuration values will be cleared.

MUSE/12SL configuration

All communication between the patient monitor and the MUSE server, both sending and receiving the 12SL ECG reports, takes place over the IX Network and is encrypted. The supported server version is MUSE NX R1 SP1 or higher.

The communication uses HTTPS protocol and the traffic is encrypted with TLS 1.2 protocol using X.509 certificates. MUSE certificate bundle must be installed into the monitor to facilitate server authentication and encryption key exchange.

Sending 12SL reports to MUSE server requires that a 12SL diagnostics ECG license, either P12D or P12S, is installed into the monitor.

Receiving 12SL PDF reports from the MUSE server requires that the MuseView License, AMSE, is installed into the monitor.

Configuring MUSE/12SL Settings

1. Log in to the service interface.
2. Select **Configuration > MUSE/12SL > MUSE/12SL Settings**.
3. Enter the following data:

Settings	Description
Location ID	Identifies the location ID number (within the range 0 to 999) associated with the patient monitor for searching the MUSE system.
Site Number	Identifies the site number (within the range 1 to 254) associated with the patient monitor for searching the MUSE system.
Web Username	Username used to authenticate with the MUSE Web Server.
Web Password	Password used to authenticate with the MUSE Web Server.
Web URL	Enter the URL of the MUSE Web Server, for example, 'https://muse.example.net'.

4. Select **Save**.

The change will take effect immediately.

NOTE To reset the settings back to factory defaults, select **Reset settings**.

Installing MUSE/12SL certificate

The CA certificate bundle from the MUSE Web Server must be installed into the monitor in order to make authenticated connection between the monitor and the MUSE server.

Exporting the CA certificate from the MUSE Web Server

Follow the instructions in MUSE NX service documentation to export the CA root certificate file from the MUSE Web Server.

Points to note:

1. Certification Path: In the **Certificate** view, ensure that you have selected the top-level certificate, the CA root certificate.
2. Certificate encoding and format: In the **Certificate Export** wizard, select **se-64 encoded X.509 (.CER)** file format. This creates a .cer ASCII file in PEM format that contains the complete certificate chain in a single certificate bundle.

NOTE The steps for exporting a certificate are web browser specific.

Importing the CA certificate into the monitor

Follow the below instructions to import the exported CA certificate into the monitor.

Points to note:

- The certificate installation is only supported when you access the service interface with a service PC.

- The certificate must be in a PEM-encoded file format, which is readable as ASCII text.
1. Log in to the service interface
 2. Select **Configuration > MUSE/12SL > Certificate Management**.
 3. Install the certificate using one of the following methods:
 - a. Paste the certificate from a PEM file that contains the certificate.
 - i. Open the PEM file with a text editor.
 - ii. Copy the certificate information.
 - iii. In the service interface, paste the information into the box under the **Certificate** title.
 - b. Upload the PEM file that contains the certificate.
 - i. Select **load from file** next to the **Certificate** title.
 - ii. Search the drive and folder where the file is located and choose the file to upload. Follow the instruction of the web browser used.
The whole file content populates into the box under the **Certificate** title.
 4. Select **Upload**.

The change will take effect immediately.

Admit settings

Configuring patient ID prefix

The monitor will automatically generate a temporary, unique patient ID when a patient with unknown ID is admitted to the patient monitor. The monitor will use this temporary patient ID for all 12SL reports that are sent to MUSE until the patient is discharged from the patient monitor, or his/her patient ID is changed. The temporary patient ID is generated from the temporary patient ID prefix, care unit name, bed name, and current time.

The temporary patient ID prefix is a hospital defined prefix that is used as the first two characters in a temporary patient ID to ensure its uniqueness inside the hospital.

1. Log in to the service interface.
2. Select **Configuration > Admit Settings > Patient ID Prefix**.
3. Enter a 2 character prefix.
Valid values are uppercase letters and numbers.
4. Select **Save**.

The change will take effect immediately.

Barcode parser configuration

Barcode reader can be used to scan information to a single text field or to several text fields at a time:

- You do not need to configure the parser if you use a barcode reader to scan a simple barcode with only one piece of information to a single field in the monitor's user interface.

- You need to configure the parser if you use a barcode reader to scan complex barcodes with several data items to multiple fields in the **Admit/Discharge** menu. The correct parser configuration ensures that the data items in the barcode string are correctly populated to the related fields in the **Admit/Discharge** menu.

Before you start configuring the parser:

1. Acquire detailed specifications of the character-delimited or length-delimited barcode string that the hospital uses.
2. Acquire sample barcodes, if possible, to verify that you have completed the parser configuration correctly. For more information, see the Testing the barcode reader section in the Checkout procedures chapter.

Refer to the monitor's supplemental information manual for a list of compatible barcode readers.

NOTE The barcode reader has an internal, configurable setting for keyboard locale. The factory default value for this setting is US English. Configure first the keyboard locale setting of the barcode reader to be the same as the keyboard locale setting in the monitor's service interface. Follow the instructions provided with the barcode reader.

The supported barcode symbologies and characters are listed in the table below:

Symbology	Supported characters
Aztec Code	All 8-bit values can be encoded. The default interpretation should be: <ol style="list-style-type: none"> 1. For values 0 - 127, ANSI X3.4 (ASCII) 2. For values 128 - 255, ISO 8859-1 Latin alphabet number 1 See the IEC 24778 standard.
Code 128	Encodes the full ASCII set 0 - 127. See the IEC 15417 standard.
Code 39 (Extended)	Code 39 is restricted to 44 characters, symbols 0-9, A-Z, '-', ':', '\$', '/', '+', '%' and space. The Code39 Extended encodes the full ASCII set 0 - 127. Extended characters are encoded by a pair of normal Code 39 characters. See the IEC 16388 standard.
Data Matrix	Encodes all 8-bit values. The maximum length is 1556 ASCII (8 bit), 2335 alphanumerical or 3116 numeric characters. See the IEC 16022 standard.
Interleaved Code 2 Of 5	Restricted to symbols 0-9. See the IEC 16390 standard.
Pdf417	Encodes all-8 bit values. The maximum length is 1108 ASCII (8 bit), 1850 alphanumerical, 2725 numeric characters. See the IEC 24728 standard.

Selecting and configuring the barcode parser

1. Log in to the service interface.

2. Select the **Configuration** tab.
3. If needed, select **Admit Settings > Barcode Settings**.
4. In **Barcode Settings**, select the parser type:

Parser type	Use with this type of barcode
None	Simple barcode that contains one piece of information, but no data control. There is no need for a parser.
Char-Delimited	Barcode that specifies a special character that separates each data item in the barcode string.
Length-Delimited	Barcode that specifies the beginning position and length of each data item in the barcode string.

5. Depending on your selection:
 - a. If the selected parser is **None**, select **Save** to complete the parser configuration.
 - b. If the selected parser is **Length-Delimited**:
 - i. Enter the starting **Position** and **Length** of each data item included in the barcode string.
See the General notes about parser configuration and Data item specific notes sections for more information to complete the parser configuration.
 - ii. Select **Save**.
 - c. If the selected parser is **Char-Delimited**:
 - i. Enter the **Field Delimiter** character that separates the data items in the barcode string.
The field delimiter can be any ASCII character between 33-126.
If the character selected as a field delimiter exists within a data item in the barcode string, it will be misinterpreted as a field delimiter.
 - ii. Enter the sequence number of each data item included in the barcode string into the **Position** column.
See the General notes about parser configuration and Data item specific notes sections for more information to complete the parser configuration.
 - iii. Select **Save**.

General notes about parser configuration

Follow these general instructions when configuring the barcode parser:

- You can configure the barcode parser to populate the following data items from a barcode string into the related fields in the **Admit/Discharge** menu:
 - **MRN**
 - **First Name**
 - **Last Name**
 - **Day of Birth**
 - **Month of Birth**
 - **Year of Birth**
 - **Age**
 - **Age Unit**

- **Gender**
- **Height**
- **Height Unit**
- **Weight**
- **Weight Unit**
- **Visit Number**
- **Primary Physician**
- **Referring Physician**
- The maximum length of the barcode string is 300 characters. The maximum length of a single data item within the barcode string is 99, except for the following data items that have a fixed length, if included:

Data item	Number of characters
<i>Day of Birth</i>	2
<i>Month of Birth</i>	2
<i>Year of Birth</i>	4
<i>Gender</i>	1

- The **Day of Birth** and **Month of Birth** fields have a fixed length of 2 characters. '0' and space are accepted as padding characters. For example, "01", " 1" and "1" are all accepted and will be interpreted as 1, whereas "1" is not accepted because it has only one character.
- If the data item in the barcode is longer than the space reserved for it in the related field, the rest of the characters are truncated.
- The barcode string can contain data items that have no related field in the **Admit/Discharge** menu. Omit these data items when configuring the parser.
 - In the length-delimited parser configuration: leave the starting **Position** and **Length** fields empty for all data items that are not included in the barcode string.
 - In the character-delimited parser configuration: leave the sequence number in the **Position** field empty for all data items that are not included in the barcode string.
- The data items can be located anywhere within the barcode. They do not have to be in the same consecutive order as they appear in the parser configuration menu or in the **Admit/Discharge** menu.
- If decimal numbers are allowed for a data item, both period (.) and comma (,) are accepted as the decimal symbol.

Data item specific notes

Data item / field name	Maximum number of characters		Valid values in barcode string	Comments
	Admit/Discharge*	Barcode string		
<i>MRN</i>	13	99	Both letters and numbers	–
<i>First Name</i>	10	99		
<i>Last Name</i>	16	99		

Data item / field name	Maximum number of characters		Valid values in barcode string	Comments
	Admit/Discharge*	Barcode string		
Day of Birth	2	2	1-31	If you configure Day of Birth , configure also: <ul style="list-style-type: none"> • Month of Birth • Year of Birth
Month of Birth	2	2	1-12	If you configure Month of Birth , configure also: <ul style="list-style-type: none"> • Day of Birth • Year of Birth
Year of Birth	4	4	1880 to current year	If you configure Year of Birth , configure also: <ul style="list-style-type: none"> • Day of Birth • Month of Birth
Age	Depends on the selected Age Unit	99	Numeric (decimal numbers are not allowed)	If you configure Age , configure also Age Unit .
Age Unit		99	For Custom configuration: <ul style="list-style-type: none"> • A, Y, YR, YRS (years) • MO, MOS (months) • WK, WKS (weeks) • D, DAY, DYS (days) 	If Age Unit is included in the barcode, select Custom and enter the starting position and length for the data item. If Age Unit is not included in the barcode, select one of the following: <ul style="list-style-type: none"> • Years • Months • Days • Weeks
Gender	1	1	For Custom configuration, the allowed characters are between ASCII 32 and ASCII 127	If you configure Gender , you must specify the codes (character) that identify Male and Female . <ul style="list-style-type: none"> • If you select Custom: specify which 1-digit characters represent male and female in the barcode. • If you select Fixed: M or 1 in the barcode is automatically identified as a male, and all other characters as female.
Height	Depends on the selected Height Unit	99	Numeric 9999.9999	Either a period or comma is accepted as a decimal symbol. If you configure Height , configure also Height Unit .

Data item / field name	Maximum number of characters		Valid values in barcode string	Comments
	Admit/Discharge*	Barcode string		
Height Unit		99	For Custom configuration: <ul style="list-style-type: none">• FT (feet)• IN (inches)• M (meters)• CM (centimeters)• MM (millimeters)	If Height Unit is included in the barcode, select Custom and enter the starting position and length for the data item. If Height Unit is not included in the barcode, select one of the following: <ul style="list-style-type: none">• Feet• Inches• Meters• Centimeters• Millimeters
Weight	Depends on the selected Weight Unit	99	Numeric 9999.9999	Either a period or comma is accepted as a decimal symbol. If you configure Weight , configure also Weight Unit .
Weight Unit		99	For Custom configuration: <ul style="list-style-type: none">• KG, KGS (kilograms)• G, GM, GMS (grams)• MCG (micrograms)• OZ, OZS (ounces)• LB, LBS (pounds)	If Weight Unit is included in the barcode, select Custom and enter the starting position and length for the data item. If Weight Unit is not included in the barcode, select one of the following: <ul style="list-style-type: none">• Kilograms• Grams• Micrograms• Pounds• Ounces
Visit Number	20	99	Both letters and numbers	—
Primary Physician	16	99		
Referring Physician	16	99		

* When the monitor is connected to the CARESCAPE network.

Setting power frequency

WARNING

ERRONEOUS PATIENT DATA. Incorrect power line frequency setting could adversely affect ECG, EEG, and rSO₂ processing.

1. Log in to the service interface.
2. Select **Configuration > Power Frequency**.
3. Select the applicable power line frequency.

4. Select **Save**.

The change will take effect immediately.

Selecting language and locale

Select the language used in the clinical user interface and the keyboard locale setting for the alphanumeric keyboard and the barcode reader.

1. Log in to the service interface.
2. Select the **Configuration** tab.
3. Select **Language Settings**.
4. To select the monitor language and keyboard language:
 - a. Select the monitor language from the drop-down list and select **Save**.
The change takes effect after the monitor is restarted.
 - b. Select the keyboard locale from the drop-down list and select **Save**.
The change will take effect immediately.

Configuring modules

You can configure some acquisition module settings via the service interface. These settings are saved to the permanent memory of the connected acquisition module and the settings travel with the module from one monitor to another.

The settings are pre-configured at factory for new products, except the **Assets Settings**. You may need to re-configure them after corrective maintenance, or for administration purposes.

Refer to the CARESCAPE PDM Service Manual and E-PT & E-PP Service Manual for detailed information on how to change these settings.

Setting	Module	Description
ECG Filter Configuration	PDM	This setting allows you to temporarily disable the ECG filter of the PDM.
Licensing	PDM	This setting allows you to manage the PDM invasive pressure licenses.
Assets Settings	PDM	This is an optional, user-assigned unique identifier for the CARESCAPE PDM. You can use it for example for asset management purposes.
P/PT/PP Settings	E-P, E-PT & E-PP	This setting allows you to configure the P/PT/PP setting after replacing the STP board.

NOTE

The platform configuration for CARESCAPE ONE and CARESCAPE Parameters cannot be completed via the monitor's service interface. See CARESCAPE ONE Service Manual for more information.

Configuring module asset number

This configuration applies only to the PDM. The user-assigned asset number can be up to 32 alphanumeric characters.

The **Serial Number** field is view only. The serial number must be edited when the PDM main board is replaced. Contact GE service personnel for more information.

1. Log in to the service interface.
2. Select **Configuration > Modules** and scroll down to the **Asset Settings**.
3. Enter the user-assigned asset number for the device in the **Change value to** field.
4. Select **Save**.

The change will take effect immediately.

Configuring host asset settings

Configuring host asset number

The asset number is an optional, user-assigned unique identifier for the monitor. This identifier can be up to 32 ASCII characters long.

1. Log in to the service interface.
2. Select **Configuration > Host Asset Settings**.
The current value for the asset number, if available, is shown below the **Current value**.
3. Enter the new value into the **Change value to** field.
4. Select **Save**.

The change will take effect immediately.

Configuring serial number

A serial number is a unique, manufacturer-assigned identifier for the monitor. The serial number is printed to the device label and/or UDI label of the monitor. The monitor serial number is also shown in the service interface and stored to the CPU assembly.

If CPU assembly is replaced, the original serial number will be lost, and it needs to be re-entered manually to ensure correct operation of the monitor. The serial number of the spare part CPU assembly is set to factory default "SED08349999GP".

There are two options to re-enter the serial number:

1. If the current value of the serial number is set to factory default, you can enter the new serial number without a serial number reset key and save it.
2. If the current value of the serial number is set to something other than the factory default, you need to contact your local GE representative and request a serial number reset key. When requesting for the serial number reset key, provide the original printed serial number from the device label, the MC MAC address that is displayed on the service interface login screen, and the reason for the request. The serial number reset key you will receive back consists of a **Password** and an **Expiration date**.

NOTE

The created serial number reset key is monitor specific, and it is valid for 5 days.

1. Log in to the service interface.

2. Select **Configuration > Host Asset Settings**.

The **Current value** for the serial number is shown in the **Serial Number** area.

3. Enter a new value into the **Change value to** field. Check the correct serial number of the monitor from the device label.
4. If needed, enter the **Expiration date** you received for the serial number reset.
5. If needed, enter the **Password** you received for the serial number reset.
6. Select **Save**.

The change will take effect immediately.

Password management

The initial password setup must be completed using the CARESCAPE First Use Wizard when the patient monitor is turned on for the first time. Any future password changes, password length and password reuse configurations are completed using CARESCAPE Service Interface.

For the initial password setup, see chapter 4 Service Applications - CARESCAPE First Use Wizard.

For an overview about the concepts and aspects related to access control, user authentication and password management see the CARESCAPE B850, B650 and B450 Privacy and Security Manual.

User accounts and passwords

The patient monitor supports role-based access control for accessing password protected service applications and clinical configurations. The following table lists the supported user accounts for accessing the clinical configuration and the different service applications:

NOTE The patient monitor does not have any default passwords.

User name	Access rights	Password change
service	<p>This user account is intended for GEHC service to access CARESCAPE Service Interface, CARESCAPE Multi Monitor Manager, service calibrations, and password protected clinical configurations:</p> <ul style="list-style-type: none"> • Monitor Setup > Defaults & Service > Service • Monitor Setup > Defaults & Service > Service Calibrations • Monitor Setup > Defaults & Service > Default Setup 	<p>Only the service user can change the password for the service user account. This is done via the CARESCAPE Service Interface:</p> <ul style="list-style-type: none"> • Configuration > Passwords > Change Passwords <p>If the valid password for the service user account is forgotten, contact your GEHC service representative and request for a password reset key for the service user.</p>
biomed	<p>This user account is intended for end customer to access CARESCAPE Service Interface, CARESCAPE Multi Monitor Manager, service calibrations, and password protected clinical configurations:</p>	<p>The service and biomed users can change the password for the biomed user account. This is done via the CARESCAPE Service Interface:</p> <ul style="list-style-type: none"> • Configuration > Passwords > Change Passwords

User name	Access rights	Password change
	<ul style="list-style-type: none"> • <i>Monitor Setup > Defaults & Service > Service</i> • <i>Monitor Setup > Defaults & Service > Service Calibrations</i> • <i>Monitor Setup > Defaults & Service > Default Setup</i> 	If the valid password for the biomed user account is forgotten, either ask a local service user to change the password, or contact your GEHC service representative and request for a password reset key for the biomed user.
clinical	<p>This user account is intended for clinical users and GEHC support personnel to access password protected clinical configurations:</p> <ul style="list-style-type: none"> • <i>Monitor Setup > Defaults & Service > Default Setup</i> <p>See monitor's user manual and supplemental information manual for more information.</p>	<p>The service and biomed users can change the password for the clinical user account in the CARESCAPE Service Interface:</p> <ul style="list-style-type: none"> • <i>Configuration > Passwords > Change Passwords</i>
demomode	<p>This user account is intended for entering the DEMO mode.</p> <p>See the user manual and supplemental information manual for more information.</p>	<p>Only the service user can change the password for the demomode user account. This is done via the CARESCAPE Service Interface:</p> <ul style="list-style-type: none"> • <i>Configuration > Passwords > Change Passwords</i>

Password policy

Password policy can be configured:

- The minimum and maximum password length can be changed.
- The reuse of previously used passwords can be prohibited.

The monitor utilizes also password blacklisting. User assigned passwords are checked against a list of commonly used and compromised passwords, and if the prospective password appears in the list, the use is prohibited.

Changing the minimum and the maximum password length

To change the minimum and/or maximum password length:

1. Login to service interface.
2. Select **Configuration > Passwords > Policy**.
3. Enter the **minimum length** of the password to be between 6 to 14 characters.
4. Enter the **maximum length** of the password.
The **maximum length** can be between 8 to 64 characters, but it cannot be less than the selected **minimum length**.
5. Select **Save**

Preventing the reuse of old passwords

To prevent the reuse of old passwords:

1. Login to service interface.

2. Select **Configuration > Passwords > Policy**.
3. Enter the number of previous passwords you want to prevent from being reused as a new password to the **Prohibit use of previous** field.
The allowed values are 0 and 2 - 10. By default passwords can be reused, so the default value is 0. The maximum number is 10, which means that the previous 10 passwords cannot be reused.
4. Select **Save**.

Changing passwords

WARNING

PATIENT SAFETY. Use strong passwords. Do not store the passwords in insecure manner or share them with unauthorized persons. Failure to do so may compromise patient safety, privacy and security and/or system performance.

NOTE

The username and password are case sensitive. Use only letters A to Z, or a to z, numbers from 0 to 9, and space.

1. Log in to the service interface.
2. Select **Configuration > Passwords > Change Passwords**.
The user accounts for which you can change the password are shown on the screen.
3. Depending on the password you want to change:
 - a. If you are logged in as a **service** user:
 - To change the **service** password:
 - i. In the **Change Password for service** area, re-enter the **service** password in the **Current Password** field.
 - ii. In the **New Password** field, provide a new password for the **service** user account.
 - iii. In the **Confirm password** field, re-enter the new password.
 - iv. Select **Save**.
 - To change the **biomed** password:
 - i. In the **Change Password for biomed** area, re-enter the **service** password in the **Your Password** field.
 - ii. In the **New Password** field, provide a new password for the **biomed** user account.
 - iii. In the **Confirm password** field, re-enter the new password.
 - iv. Select **Save**.
 - To change the **clinical** password:
 - i. In the **Change Password for clinical** area, re-enter the **service** password in the **Your Password** field.
 - ii. In the **New Password** field, provide a new password for the **clinical** user account.
 - iii. In the **Confirm password** field, re-enter the new password.
 - iv. Select **Save**.

- To change the **demomode** password:
 - i. In the **Change Password for demomode** area, re-enter the **service** password in the **Your Password** field.
 - ii. In the **New Password** field, provide a new password for the **demomode** user account.
 - iii. In the **Confirm password** field, re-enter the new password.
 - iv. Select **Save**.

The change will take effect immediately.

- b. If you are logged in as a **biomed** user:
 - To change the **biomed** password:
 - i. In the **Change Password** area, re-enter the **biomed** password in the **Current Password** field.
 - ii. In the **New Password** field, provide a new password for the **biomed** user account.
 - iii. In the **Confirm password** field, re-enter the new password.
 - iv. Select **Save**.
 - To change the **clinical** password:
 - i. In the **Change Password for clinical** area, re-enter the **biomed** password in the **Your Password** field.
 - ii. In the **New Password** field, provide a new password for the **clinical** user account.
 - iii. In the **Confirm password** field, re-enter the new password.
 - iv. Select **Save**.

The change will take effect immediately.

Resetting passwords

If the valid password for the **service** or **biomed** user account is forgotten, you can reset the password. Contact your local GE representative to request a password reset key.

Provide the following information when requesting a password reset key:

- Serial Number of the monitor.
- The user account for which the password reset key is needed for.

NOTE

The created reset key will be monitor and user account specific, and valid for 90 days. If you need password reset keys for several monitors and/or user accounts, provide the requested information for all affected monitors / user accounts.

Once you have received the password reset key:

1. Go to the service interface login screen.
2. Select **Forgot password?**.
3. Enter the **Username** for the user account the password reset key was requested.
4. Enter a new password to the **New Password** field.
5. Confirm the new password to the **Confirm Password** field.

6. Enter the received **Activation Code** to the **Reset Key** field.
7. Enter the received **Expiration Date** for the reset key in format YYYY-MM-DD.
8. Select **Reset Password**.

The new password for the user account is now valid. Try to log into the account with the new password.

Configuring CS ONE authentication

CARESCAPE Bx50 can be configured to support only authenticated connections with CARESCAPE ONEs.

1. Log in to the service interface.
2. Select **Configuration > Device Authentication**.
3. Depending on you need:
 - Select **Allow all connections**, if the host monitor needs to be compatible also with CARESCAPE ONEs with software version 3.0. In this case, the connection is not authenticated. This is the factory default.
 - Select **Allow only authenticated connections**, if the host monitor needs to be compatible only with CARESCAPE ONEs with software version 3.2. In this case, the connection is authenticated.

The setting takes effect immediately. It will affect any new CS ONE connections.

NOTE

The host monitor will show a **CS ONE not authenticated** message on the screen, if you have selected **Allow only authenticated connections** and connected a CARESCAPE ONE with software version 3.0.

Configuring connectivity

Select the serial port speed for the communication with iCollect or other serial interface solutions.

1. Log in to the service interface.
2. Select **Configuration > Connectivity**.
3. Select the serial port speed: either **19200 bits/s** or **115200 bits/s**.
4. Select **Save**.

The change will take effect after next monitor restart.

Configuring remote alarm device

This configuration is related to CARESCAPE RAD. For more information see CARESCAPE RAD Service Manual.

1. Log in to the service interface.
2. Select **Configuration > Remote Alarm Device**.

3. Select the appropriate **Remote alarm device operation** radio button:
 - If you select **Enabled**, the CARESCAPE monitor can send alarms to the connected remote alarm device.
 - If you select **Disabled**, the CARESCAPE monitor cannot send alarms to the connected remote alarm device. The remote alarm device is powered but not operating properly.
4. Select the appropriate **Remote alarm device power failure detection** radio button. This setting determines whether the remote alarm device triggers an alarm condition in the remote alarm system in power loss situations (for example, if a USB cable is disconnected or the monitor shuts down):
 - If you select **Enabled**, the remote alarm device triggers an alarm condition in the remote alarm system if power is lost.
 - If you select **Disabled**, the remote alarm device does not trigger an alarm condition in the remote alarm system if power is lost.
5. Select **Save**.

The settings take effect immediately.

Restarting the monitor

You can use the Restart function in the service interface to restart the monitor after making configuration changes that require a manual restart before the changed setting come into effect. For example, after changing network or language settings, or adding activation codes for licenses.

NOTE

Loss of monitoring - This function is enabled only when the monitor is in a discharged state. Before restarting the monitor, verify that the patient is discharged from the monitor.

1. Log in to the service interface.
2. Select **Configuration > Restart**.
3. Select the **Restart** button.

The monitor will shut down and restart automatically.

Setting up the remote service

Enabling or disabling the remote service connection

You can enable and disable the operation of the remote service agent and connectivity to the GE back office server.

1. Log in to the service interface.
2. Select **Configuration > Remote Service**. You can see the **Current status** of the InSite RSvP agent: **Enabled** or **Disabled**.
3. In **New status**, select the appropriate radio button: **Enable** or **Disable**.
4. Select **Save**.

The change will take effect immediately.

Configuring remote service

1. Log in to the service interface.
2. Select **Configuration > Remote Service**.
The **Enterprise URL** is the GE InSite RSVP back office server web address. It is pre-configured at factory. Do not change this web address unless explicit instructions are given to do so.
3. If a proxy server is in use for accessing Internet:
 - a. Select **Use proxy server**.
 - b. Enter the IP address and Port number of the proxy server.
4. If a proxy server requires user authentication for accessing Internet:
 - a. Select **Use authentication**.
 - b. Enter the **Username** and the **Password** to access the proxy server.
5. Select **Save**.

The change will take effect immediately.

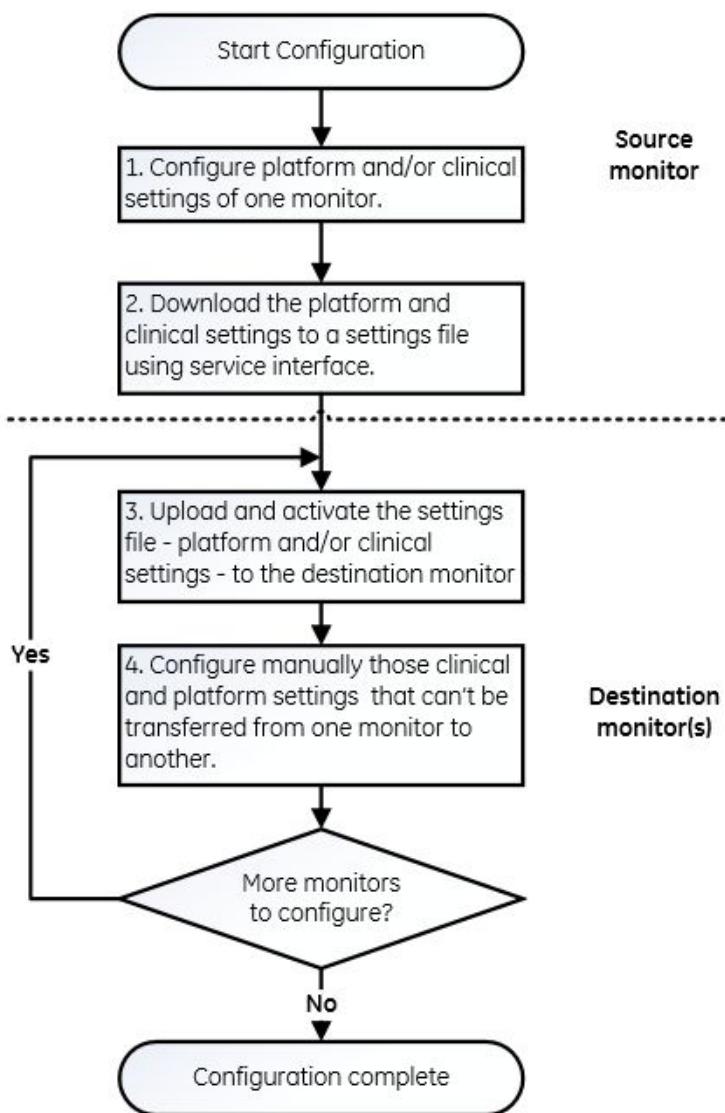
Settings management

This section explains how to:

- Transfer the clinical and/or platform settings configured for one monitor to other similar monitors.
- Reset the clinical and/or platform settings configured for one monitor back to factory defaults.

Settings transfer process

To simplify the installation process for several monitors, you can configure the clinical and/or platform settings manually for one monitor (source monitor) and then transfer the monitor settings to other similar monitors (destination monitors). This figure provides an overview of the settings transfer process.



1. Use the clinical and service interfaces to complete the platform and/or clinical configuration for one source monitor. Note that:
 - Clinical settings cover both care unit settings and profile settings.
 - Many of the clinical settings are either software package and/or profile specific.
 - Some of the platform and clinical settings are monitor type and software version specific.
 Ensure that you have completed the clinical configuration for all applicable software packages and profiles in the source monitor and saved the settings to the profiles before proceeding.
2. Use the service interface to download the platform and clinical settings of the source monitor to a settings file.
 - The downloaded settings file will be encrypted using 7-Zip open-source file archiver (<http://7-zip.org/>) and have a file extension .7z. The file name contains the source monitor serial number followed by the date and time of the download. For example: SNR16410010HP_20170731_115745.7z.

3. Use the service interface to upload and activate the platform and/or clinical settings in the destination monitor.
4. Configure manually those clinical and/or platform settings that cannot be transferred from one monitor to another.
 - The following platform settings are unique to each monitor and must be configured manually:
 - software licenses
 - host asset settings
 - network hostname
 - settings for wired network
 - unit and bed name
5. Repeat steps 3 and 4 for each monitor that you wish to configure.

Settings transfer between different monitor types or software versions

It is also possible to transfer clinical settings between different CARESCAPE monitor types (for example, from a CARESCAPE B450 to a CARESCAPE B850 or vice versa), and between similar monitors with different CARESCAPE software versions (for example, from software version 2.0.7 to 3.1).

However, the clinical settings may differ between CARESCAPE software versions. A newer software version may have some new or changed software features that affect some clinical settings. These new or changed clinical settings remain in the factory defaults in the destination monitor after the settings have been transferred from the source monitor with an older software version. Refer to the monitor's Software Settings Transfer Guide for more information about differences in clinical settings in different CARESCAPE software versions.

Do not transfer platform settings between different monitor types or software versions.

Downloading clinical and platform settings

Download the platform and clinical settings of the source monitor to a settings file.

NOTE

For security reasons, the contents of the settings file are encrypted with a user-selectable password. Store the password in a secure way. You will need the password for uploading the settings file to the destination monitors.

1. Log in to the service interface.
2. Select **Configuration > Settings > Download**.
3. Provide a password for encrypting the settings file.

4. According to your service interface access:
 - a. If you are using a service PC, you can save the settings file to any storage device connected to the service PC:
 - i. Select **Download**.
 - ii. Save the settings file according to the instructions provided by the web browser.
 - b. If you are using the local, integrated service interface, you can save the settings file to a USB flash drive that is connected to one of the monitor's USB ports:
 - i. Select **Save to USB storage** to save the settings file to the USB flash drive.The settings file is saved always to the root directory of the USB flash drive.

NOTE

Do not disconnect the USB flash drive until downloading is complete.

The downloaded settings file is now ready to be uploaded and activated into the destination monitors. The settings file contains both the platform and clinical settings of the source monitor.

Activating settings

You can upload and activate the previously downloaded settings file to the destination monitor(s).

NOTE

Some platform settings cannot be transferred from one monitor to another. They need to be configured manually in the destination monitor after the activation is completed.

1. Log in to the service interface.
2. Select **Configuration > Settings > Activate**.
3. According to your service interface access:
 - a. If you are using a service PC, you can upload the settings file from any storage device connected to the service PC. Search for the settings file from the destination drive and folder according to the instructions provided by the web browser.
The web browser may also notify you about security issues. Refer to the web browser documentation for details.
 - b. If you are using the local, integrated service interface, you can upload the settings file from a USB flash drive that is connected to one of the monitor's USB ports. The service interface automatically detects a connected USB flash drive, searches the directory structure for files with .7z file extension, and requests the user to select the correct file.
 - i. Choose the settings file you want to activate.

NOTE

Do not disconnect the USB flash drive until uploading is complete.

4. Enter the password that was used for encrypting the settings file.

5. Below **Settings that are to be Activated**, select the settings you want to activate.

Choices are:

- **All (clinical and platform) settings**: Activates both the clinical and platform settings.
- **Clinical settings**: Activates clinical settings only.
- **Platform settings**: Activates platform settings only.

NOTE

Do not activate platform settings that have been downloaded from a monitor with CARESCAPE software version 3.1 or earlier.

6. Below **Schedule**, select when you want the setting activation to occur.

Choices are:

- **Immediately**: The settings upload and activation starts immediately.
- **After discharge**: The settings activation starts after the next patient discharge/case end.

NOTE

Immediately option is only available if the monitor is in a patient discharged/case end state.

7. Select the **Activate** button.

NOTE

If you selected the settings activation to take place after the next patient discharge/case end, you can cancel the activation while it is pending. To cancel the activation, select **Configuration > Settings > Activate > Cancel activation**.

a. If the settings activate immediately, do the following:

- Wait until the settings activation is completed and the monitor has performed an automatic restart.
- Check that the settings activation was successful and the monitor is using the activated settings.
- Configure manually those clinical and platform settings that cannot be transferred from the source monitor to the destination monitor.

b. If the settings are activated after the patient is discharged, do the following:

- The monitor shows a **Setting activation after next discharge / Setting activation after next case end** message until the clinical user performs a patient discharge/case end. The patient monitoring can continue normally until then.
- Settings activation will start automatically after the next patient discharge/case end. Wait until the settings activation is completed and the monitor has performed an automatic restart.
- Check that the settings activation was successful and the monitor is using the activated settings.
- Configure manually those clinical and platform settings that cannot be transferred from the source monitor to the destination monitor.

The settings activation will fail if the settings file is invalid, the password is incorrect or the settings file is not found.

Resetting to factory settings

You can reset the platform and/or clinical settings of a monitor to factory defaults.

NOTE

Resetting to factory defaults does not affect the following platform settings:

- licenses
- host asset settings
- passwords

1. Log in to the service interface.
2. Select **Configuration > Settings > Reset**.
3. In **Settings Type** area, select the settings you want to reset.

Choices are:

- **Clinical and platform settings**: Resets both the clinical and platform settings.
- **Clinical settings**: Resets the clinical settings only.

4. In **Defaults** area, select the defaults to be used for clinical settings.

Choices are:

- **Factory defaults**: Resets the clinical settings to the global factory defaults
- **US defaults**: Resets the clinical settings to the US factory defaults.

Refer to the supplemental information manual for a list of the global or US-specific factory default values for clinical settings.

5. In **Schedule** area, select when you want the reset to occur.

Choices are:

- **Immediately**: The reset starts immediately.
- **After discharge**: The reset starts after the next patient discharge/case end.

NOTE

Immediately option is only available if the monitor is in a patient discharged/case end state.

6. Select the **Reset** button.

NOTE

If a patient is admitted or a case is ongoing in the target monitor, the reset takes place after the patient is discharged or the case is ended. You can cancel the reset while it is pending. To cancel the reset, select **Configuration > Settings > Reset > Cancel reset**.

- a. If the reset starts immediately, do the following:
 - Wait until the settings reset is completed and the monitor has performed an automatic restart.
 - Check that the settings reset was successful and the selected settings have been reset to factory defaults.
- b. If the reset starts after the patient is discharged, do the following:
 - The monitor shows a **Setting activation after next discharge / Setting activation after next case end** message until the clinical user performs a

patient discharge/case end. The patient monitoring can continue normally until then.

- Settings reset will start automatically after the next patient discharge/case end. Wait until the settings reset is completed and the monitor has performed an automatic restart.
- Check that the settings reset was successful and the selected settings have been reset to factory defaults.

License management

CARESCAPE monitors support three type of licensed features:

1. Care area specific *software packages* (ED, ICU, NICU, OR and PACU) allow you to customize a monitor to meet care area specific monitoring needs.
2. *Host licenses* are used to enable optional, licensed clinical features, for example, for anesthetic agent measurement or using the auto view on alarm - features.
3. A *base license* may be required when you upgrade a monitor from one host software version to another. For more information about software upgrades and base licenses, see Activating the host software section.

You can enable individual software packages and host licenses by entering the required activation codes for the licenses manually. Alternatively, you can upload a license file that contains activation codes for all acquired software packages and host licenses.

NOTE

The activation codes are monitor specific. Check that the license file and/or printed activation codes are intended for the monitor in use.

Contact GE to acquire activation codes for licenses.

Activating host licenses

Some software features require a specific host license to be enabled. Host licenses are typically valid for all software packages, but there are some exceptions to the rule. Host licenses are available either as permanent or as trial licenses. Activation codes for trial licenses are valid for 45 days. See user manual and supplemental information manual for more information about the host licenses.

To enable a host license manually:

1. Log in to the service interface.
2. Select **Configuration > Licenses > Host License**.

The supported host licenses are listed under **Host License**. The enabled licenses have an activation code next to it. The host licenses are either STANDARD (always enabled) or OPTIONAL (separately purchasable). Trial licenses are marked with a suffix "-TRIAL".

3. For each **Host License** that you want to enable:
 - a. Select **ENABLED** from the **Status** drop-down list.
 - b. For trial licenses only: enter the **Expiration date**.
 - c. Enter a valid **Activation code** for the software package.
4. Select **Save**.

The changes take effect after the next patient monitor restart.

NOTE You can also disable a host license. If you do so, the activation code will be cleared.

Software packages

You can customize CARESCAPE software to meet the needs of different care areas with software package licenses. The supported software packages are: ED, ICU, NICU, OR and PACU.

Many of the monitor's clinical settings are separately configurable for different software packages (care unit settings) and different profiles (profile settings). See supplemental information manual for more information about the configuration and factory defaults for care unit settings and profile settings.

You can have several software packages enabled, but only one of them can be active at a time.

Enabling software packages

To enable software packages manually:

1. Log in to the service interface.
2. Select **Configuration > Licenses > Software Package**.
3. For each **Software Package** you want to enable:
 - a. Select **ENABLED** from the **Status** drop-down list.
 - b. Enter a valid **Activation Code** for the software package.
4. Select **Save**.

All license changes take effect after the next monitor restart.

NOTE You can also disable a software package. If you do so, the activation code will be cleared.

Changing the active software package

WARNING PATIENT SAFETY. If the software package is changed, all clinical settings will reset to factory defaults.

The factory default value for the software package is ICU.

NOTE The operation is not allowed while a patient is admitted.

To change the active software package:

1. Log in to the service interface.
2. Select **Configuration > Licenses > Software Package**.
The currently active software package is shown under **Active Software Package**.
3. Select the new software package from the drop-down list.
4. Select **Save**.

The changes take effect after the next monitor restart.

Uploading license file

NOTE

Contact GE to get the correct license file for your monitor. The license file is a text file that is named according to the monitor's serial number. The activation codes are monitor specific. Check that the license file is intended for the monitor in use.

1. Log in to the service interface.
2. Select **Configuration > Licenses > Upload License**.
3. According to your service interface access:
 - a. If you are using a service PC, you can upload the license file from any storage device connected to the service PC. Search for the license file from the destination drive and folder according to the instructions provided by the web browser.
The web browser may also notify you about security issues. Refer to the web browser documentation for details.
 - b. If you are using the local, integrated service interface, you can upload the settings file from a USB flash drive that is connected to one of the monitor's USB ports. The service interface automatically detects a connected USB flash drive, searches the .txt files, and requests the user to select the correct file.
 - Choose the license file you want to activate.

NOTE

Do not disconnect the USB storage device until uploading is complete.

4. Check that the information populated in the **Host License** and **Software Package** screens is accurate.

These changes take effect after the next monitor restart.

Backup and restore

Take a backup of the platform and clinical settings of each monitor after the initial installation is completed, and every time the platform settings have been changed.

The availability of a valid backup file can save your time if you ever need to replace the CPU assembly, and you need to restore the original settings.

The backup file contains a complete image of the monitor platform and clinical settings, including monitor specific licenses, serial number, IP addresses and other unique settings. The created backup file can be restored only to the same monitor.

NOTE

For security reasons, the contents of the backup file are encrypted with a user-selectable password. Store the password in a secure way, separately from the monitor's backup file. You will need the password later if you have to restore the backup file to the monitor.

Taking a backup

The default file name contains the serial number of the monitor, followed by the date and the time the backup file was created.

NOTE	For security reasons, the contents of the backup file is encrypted with a user-selectable password. Store the password in a secure way. It will be needed for restoring the backup file to the monitor.
-------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

1. Log in to the service interface.
2. Select **Configuration > Backup > Download**.
3. Provide a password for encrypting the backup file. This password is user-selectable.
4. According to your service interface access:
 - a. If you are using a service PC, you can save the backup file to any storage device connected to the service PC.
 - i. Select **Download**.
 - ii. Save the backup file according to the instructions provided by the web browser.

The steps to download the backup file to a service PC depend on the web browser used. The web browser may also notify you about security issues. Refer to the web browser documentation for details.

- b. If you are using the local, integrated service interface, you can save the backup file to a USB flash drive that is connected to one of the monitor's USB ports.
 - i. Select **Save to USB storage** to save the backup file to the USB flash drive.

The backup file is saved always to the root directory of the USB flash drive.

NOTE

Do not disconnect the USB flash drive until downloading is complete.

5. Store the backup file and the password to a secure location.

Restoring a backup

Note that the backup file is monitor specific, and can be restored only to the original monitor with the same serial number. Before restoring the backup file, ensure that the backup file is for the intended monitor, and that you have the password to decrypt the backup file. If restore is done after CPU replacement, first enter the original serial number manually, before restoring the backup file.

1. Log in to the service interface.
2. Select **Configuration > Backup > Restore**.
3. According to your service interface access:
 - a. If you are using a service PC, you can upload the backup file from any storage device connected to the service PC. Search for the backup file from the destination drive and folder according to the instructions provided by the web browser.

The web browser may also notify you about security issues. Refer to the web browser documentation for details.
 - b. If you are using the local, integrated service interface, you can upload the backup file from a USB flash drive that is connected to one of the monitor's USB ports. The service interface automatically detects a connected USB flash

drive, searches the directory structure for files with .7z file extension, and requests the user to select the correct file.

- i. Choose the backup file you want to upload.

NOTE

Do not disconnect the USB flash drive until uploading is complete.

4. To decrypt the contents of the backup file, enter the password that was used to encrypt the backup file.
5. Select **Restore**.

Certificate management

HTTPS protocol is used for secure communication between the CARESCAPE monitor (web server) and the service PC (web client).

The CARESCAPE monitor allows you to use an X.509 certificate to authenticate it to the service web client. The monitor's service interface provides tools to create a certificate signing request, and to install the signed certificate to the monitor.

By factory default, each monitor has a unique self-signed certificate issued by GE. To improve access security, you can send a certificate signing request (CSR) to a publicly trusted certificate authority (CA). The CA validates the information in the CSR and creates a signed certificate, which you can install on the monitor later. The web browsers used to access the service interface recognize and trust the signed certificate. The users who access the monitors via the service interface will know that their peer is actually the monitor which possesses the private key of such certificate. For example, this prevents spoofing or man-in-the-middle attacks which can be mounted in attempt to steal the passwords of monitor users.

Creating a certificate signing request (CSR)

Creating the certificate signing request is only supported when you access the service interface with a service PC.

1. Log in to the service interface.
2. Select **Configuration > Certificates > Certificate Signing Request**.
3. Enter the following information:
 - **Common Name:** Enter the name of the host device. This is the only mandatory field, the rest of the fields are optional.
 - **Organization Name:** Enter the name of the hospital requesting the signed certificate.
 - **Organizational Unit Name:** Enter the unit name (for example, hospital department).
 - **City:** Enter the name of the city.
 - **State or Province:** Enter the state or province information.
 - **Country Code:** Enter the 2-letter country code.
 - **Email Address:** Enter the email address of the hospital requesting the signed certificate.

4. Select **Create**.

The monitor creates a certificate signing request (CSR) file. It also creates a new device-specific private key which will be taken into use when the signed certificate is later uploaded to the monitor.

5. Save the CSR file according to the instructions provided by the web browser.

The steps to save the CSR file to a service PC depend on the web browser used. The web browser may also notify you about security issues. Refer to the web browser documentation for details.

6. Send the CSR to a publicly trusted certificate authority (CA). The CA validates the information in the CSR and creates a signed certificate to be installed on the monitor later.

Installing the certificate

The certificate installation is only supported when you access the service interface with a service PC.

Note that the certificate must be in a PEM-encoded file format, which is readable as ASCII text.

1. Log in to the service interface.

2. Select **Configuration > Certificates > Upload Certificate**.

3. Install the certificate using one of the following methods:

a. Paste the certificate from a PEM file that contains the certificate.

i. Open the PEM file with a text editor.

ii. Copy the certificate information.

iii. In the service interface, paste the information into the box under the **Certificate** title.

b. Upload the PEM file that contains the certificate.

i. Select **load from file** next to the **Certificate** title.

ii. Search the drive and folder where the file is located and choose the file to upload. Follow the instruction of the web browser used.

The whole file content populates into the box under the **Certificate** title.

4. Select **Upload**.

The change will take effect immediately.

Note that the service interface may become unresponsive after the new certificate has been uploaded. In this case, reload the page or restart the browser.

Viewing the current certificate

1. Log in to the service interface.

2. Select **Configuration > Certificates > Upload Certificate**.

3. Under Current Certificate, you can see an overview of the current certificate:
 - the issuer of the certificate
 - the subject of the certificate (issued to)
 - the validity period of the certificate
 - the SHA-1, SHA-256 and SHA-512 fingerprints
4. To see more information about the current certificate, open the certificate view / security report from the address bar of the web browser in the service PC.
Note that this functionality depends on the web browser you use. For example, in Internet Explorer, select the lock symbol or certificate error next to the address bar of the browser to view a detailed certificate view / security report.

Software management

Software installation consist of two main steps:

1. Software upload
2. Software activation

Software installation is supported for the following system components.

Software image	Image type	Target device
CARESCAPE Software package	Host Software	CARESCAPE software for the CARESCAPE B850 CPU.
EMBC Software Package	Devices	EMBC software for F5 and F7 frames.
UIC Software Package	Devices	UIC software for the D19KT display and USB Remote Controller.
E-PiCCO Software Package	Devices	Module software for E-PiCCO module.
PDM Software Package	Devices	Module software for CARESCAPE PDM.
sGAS Software Package	Devices	Module software for CARESCAPE respiratory modules, E-sCAiOVX.

Software signing

Software code for CARESCAPE Software v3.2 (host software) is signed with a digital signature by GE Healthcare. The purpose of code signing is to confirm the software author and to ensure that the software code has not been altered or corrupted since it was signed.

There are two software files for each software build:

1. If you are updating the monitor software from one v3.2 software build to another, upload the software file that is named as "CSP_3.2.X.cas.csmon".
2. If you are upgrading the monitor software from v3.0/ v3.1 to v3.2, or if you are reloading host software to the monitor after CPU replacement, upload the software file that is named as "CSP_3.2.X.cas-unsigned.csmon".

Software upload

Software upload loads a software file from a service PC to a target monitor, but does not activate / install it.

Contact your local GE distributor for any inquiries for software files. Software is delivered using a physical media or electronically.

Software upload is supported only when you access the service interface from a service PC.

Software activation

Software activation installs the uploaded software images to the target devices.

- Software activation for CARESCAPE software is done in **Configuration > Software Management > Host Software**. The host software activation takes place either immediately or after the next discharge. If a patient is not admitted or a case is not started in the target monitor, the activation takes place immediately. If a patient is admitted or a case is started in a target monitor, the activation takes place after the patient is discharged or case is ended. If the activation takes place after the next case end/discharge, the user can cancel pending software activation at any time before the activation starts.
- Software activation for any other software is done in **Configuration > Software Management > Devices**. It is possible only when the monitor is in a patient discharged/case reset state.

A successful software activation will automatically erase the previous version of the installed software from the target monitor or connected device.

Software activation is supported with all access methods to service interface.

Uploading software

NOTE Software upload is supported only when accessing service interface from a service PC.

NOTE Software is delivered as an ISO image file, either using a physical media or electronically. To have access to the software file the ISO image must be mounted first as a logical drive. If software is delivered using a physical media, mounting typically takes place automatically when you attach the USB flash drive to your computer. If software is delivered electronically, you will have to enable the mounting manually by double-clicking the ISO image file.

1. Log in to the service interface.
2. Select **Configuration > Software Management > Upload**.

The currently uploaded software image(s) that are ready to be activated are shown in the **Uploaded Software Image** area. If the monitor does not have any software images uploaded, a message **No uploaded image** is shown.

To see the currently active, running software version of the B850 CPU unit and any connected devices:

- Select **Information > Host Information** to see the currently active CARESCAPE software (host software).
- Select **Information > Acquisition Information – Acquisition Module** to see the currently active CARESCAPE PDM software.

- Select **Information > Acquisition Information – E Module** to see the currently active software in the connected CARESCAPE respiratory module and/or E-PiCCO module.
- Select **Information > Acquisition Information – E Module Frame** to see the currently active EMBC software in the connected F5 /F7 Frame.
- Select **Information > Acquisition Information – USB Port Information** to see the currently active UIC software in the connected CARESCAPE D19KT displays and USB Remote Controller.

NOTE The menu options in steps 3 and 4 depend on the web browser.

3. In the **Upload New Software Image** area, select **Browse** or **Choose File**. An Open / Choose File to Upload -dialog box will open.
4. Browse the drive and folder to find the software file. Select the software file by double-clicking it or by selecting **Open**.
 - a. Select the software file that is named as "CSP_3.2.X.cas.csmon", if you are updating the monitor software from one v3.2 software to another.
 - b. Select the software file that is named as "CSP_3.2.X.cas-unsigned.csmon", if you are upgrading the monitor software from v3.1 to v3.2, or if you are reloading host software to the monitor after CPU replacement.
5. Select **Upload image**.

The software upload will start. The status of the software upload is shown using a progress bar. Do not leave the menu page until the software image is completely uploaded. You can cancel the software upload any time by selecting **Cancel upload**, or by leaving the **Upload** page. Once the upload of the software file is completed, the software images are shown under the title **Uploaded Software Image**.

The uploaded software images are now ready to be activated to the target monitor or connected devices.

NOTE To delete a previously uploaded software images, select **Delete image**.

Activating the host software

WARNING

BEFORE INSTALLATION- Compatibility is critical to safe and effective use of this device. Verify the compatibility of all system components and device interfaces, including hardware and software versions, prior to installation and use.

Before you start activating new host software:

- Note the difference between a software activation in case of a software upgrade and in case of a software update:
 - Software upgrade requires a base license activation code. The activation code is tied to the serial number of the monitor and to the software version to be activated. Software activation is not possible if the activation code is not entered or is invalid. In case of a software upgrade, contact GE Healthcare sales team to order the correct software upgrade kit with the base license activation codes.
 - Software update does not require a base license.

- Verify the compatibility of the new software to be activated with the current monitor hardware, and with all the connected bedside and network devices. Refer to the latest version of the supplemental information manual for a list of compatible network and bedside devices.
- Contact GE to get the latest version of the user and service documentation.
- Change passwords for all user accounts after a monitor software upgrade. You can change the passwords either manually or by transferring platform settings from a monitor with CARESCAPE Software v3.2.

NOTE LOSS OF MONITORING. Software is activated only when the monitor is in a patient discharged/case reset state. Normal patient monitoring is unavailable until the software activation is completed. This may take up to 10 minutes.

NOTE The existing clinical and platform settings of the monitor are saved and are not affected by the activation of the new host software version. However, any new or changed clinical and platform settings in the activated monitor software version are set to their factory default values, and may require manual configuration. For more information, refer to the latest version of the supplemental information manual.

NOTE Do not shut down the monitor until the software activation is successfully completed.

1. Log in to the service interface.
2. Select **Configuration > Software Management > Host Software**.
 - **Current version** shows the currently active CARESCAPE software version.
 - **Uploaded version** shows the new CARESCAPE software version to be activated.
3. To start the host software activation:
 - a. In case of a software upgrade: Enter the base license activation code and select **Activate**.
 - b. In case of a software update: Select **Activate**.

The software activation takes place in either of the following ways:

- immediately if no patient case is currently ongoing (a patient is not admitted / no case started)
- after the next discharge, if there is currently an ongoing patient case (a patient is admitted, or case is started)

Activating the host software immediately

If the host software activation occurs immediately, the monitor shows the following screen saver:

Software activation in progress. Do not disconnect any measurement modules or other peripheral devices, or shut down the monitor until the software activation is complete. Activation may take up to 10 minutes. The device will automatically restart once the software activation is complete.

1. Wait until the software activation completes and the monitor restarts automatically.

2. Verify that the software activation is successful and the monitor runs the activated software.

Activating host software after next case end / discharge

The monitor informs the clinical users about pending software activation with the following message: ***Software activation after next case end / Software activation after next discharge***. The monitoring can continue normally.

NOTE To cancel the pending software activation, select ***Cancel activation***.

The software activation starts automatically after the patient is discharged, or patient case is ended. The patient monitor displays a screen saver that informs about the ongoing software activation:

Software activation in progress. Do not disconnect any measurement modules or other peripheral devices, or shut down the monitor until the software activation is complete. Activation may take up to 10 minutes. The device will automatically restart once the software activation is complete.

1. Wait until the software activation is complete and the monitor restarts automatically.

If the monitor starts up normally and no error messages appear on the display, the activation is successful.

Activating other software

WARNING BEFORE INSTALLATION- Compatibility is critical to safe and effective use of this device. Verify the compatibility of all system components and device interfaces, including hardware and software versions, prior to installation and use.

CAUTION EQUIPMENT DAMAGE. Do not disconnect the power during software update. The software update may fail and the connected device may become unresponsive.

Before you start activating software to connected devices:

- Verify the compatibility of the new software to be activated with the current monitor hardware, and with all the connected bedside and network devices. Refer to the latest version of the supplemental information manual for a list of compatible network and bedside devices.
- Contact GE to get the latest version of the user and service documentation.
- Make sure that the monitor is in a patient discharged/case reset state.
- Make sure that all the target devices are connected to the monitor.

NOTE LOSS OF MONITORING - Software is activated only when the monitor is in a patient discharged/case reset state. Normal patient monitoring is unavailable until the software activation is completed. This may take up to 20 minutes.

NOTE Do not disconnect the connected devices, or shut down the monitor, until the software activation is successfully completed.

To activate the software:

1. Log in to the service interface.
2. Select **Configuration > Software Management > Devices**.

The screen will show a list of connected devices for which there is a new software version available. For each connected device, you can see the currently active software version and the uploaded new software version that is waiting for activation.

To update the list shown (for example, after connecting or disconnecting a device), select **Update list**.

3. Select **Update** next to the device for which to start activating new software. The software activation starts. The service interface will show a message **Update is in progress**.
 - a. Wait until the software activation is complete and the following message is shown: **Update done**.

The connected device performs an automatic restart after the software activation is complete:

- EMBC software: The green On/Standby (Power) LED in the F5/F7 frame turns off when the EMBC software activation is started and illuminates again after the EMBC software activation is completed.
- UIC software: The blue, yellow and red alarm light in the display illuminates momentarily during the UIC board restart.
- PDM/E-PiCCO/sGAS software: The message **PDM module removed, Gas measurements removed**, or **CO measurement removed** is shown on the monitor screen when the software activation starts. This message remains until the module software activation is completed and the acquisition module has restarted.

If the software activation was successful, the information of the new activated software version is updated to the **Current version** column. If needed, refresh the web browser to update the information shown on the screen.

If there are any problems in the software activation, the following message is shown: **Update failed, Try again**. If needed, refresh the web browser to update the information shown on the screen.

8

Checkout procedures

About the checkout procedures

This chapter describes the checkout procedures for the CARESCAPE B850 monitor.

The installation check covers the CARESCAPE B850 monitoring system including the following devices:

- CARESCAPE B850 CPU
- Displays
- F5/F7 Frames
- E-modules
- E-musb with CARESCAPE rSO₂ and CARESCAPE CO₂ – Microteam
- CARESCAPE PDM

The planned and corrective maintenance checks cover CARESCAPE B850 monitor.

- B850 CPU

The relevant planned and corrective maintenance checks and service procedures for the following connected devices are located in their own service manuals:

- F5/F7 Frames
- E-modules
- E-musb with CARESCAPE rSO₂ and CARESCAPE CO₂ – Microteam
- CARESCAPE PDM
- CARESCAPE ONE
- CARESCAPE RAD
- Unity Network ID connectivity device
- PRN 50-M+ Digital Writer

For cleaning and disinfection information that applies to devices, device components, supplies, and accessories manufactured by GE, see the Cleaning and Disinfecting Supplement.

For cleaning, disinfection, and care information for devices, device components, supplies, and accessories made by manufacturers other than GE, see the applicable instructions for use provided by the manufacturer.

To help ensure the equipment remains in proper operational and functional order and maintains its essential performance and basic safety, follow the corrective and planned maintenance recommendations. The tests that are related to the essential performance and basic safety are marked with an asterisk *.

Record the results of the check procedures to the eCheckforms delivered on the electronic media.

Required checkout procedures

Perform the following tests during installation, planned maintenance and corrective maintenance:

Checkout procedure	Required checks		
	Visual inspections	Electrical safety test*	Functional check
Installation check	Yes	No, if there is less than 12 months since the monitor was manufactured. Check the date of manufacture of the device from the device plate.	Yes
Planned maintenance check	Yes	Yes	Yes
Corrective maintenance check	Any corrective maintenance, where the top cover is opened.	Yes	Yes
	Any other corrective maintenance.	Yes	No

Installation check

The purpose of the installation check is to ensure that the patient monitoring system, including the connected devices, is properly installed and configured for use.

Perform the installation check after the hardware installation and platform configuration is completed before taking the monitor into clinical use.

The manufacturer has performed the electrical safety test for the monitor and acquisition modules during final inspection. You do not have to perform the electrical safety tests during the installation checkout, if there is less than 12 months since the monitor was manufactured. Check the date of manufacture of the device from the device plate.

Planned maintenance check

The purpose of the planned maintenance check is to periodically check that the product remains safe to use and maintains its performance characteristics.

Perform the planned maintenance check every two years after installation.

WARNING

SAFETY HAZARD. To avoid risks to personnel and patient, or damage to the equipment, only perform maintenance procedures described in this manual. Unauthorized modifications can lead to safety hazards.

WARNING	PATIENT SAFETY. Planned maintenance must be carried out at the specified interval. Failure to implement the maintenance schedule may cause equipment failure and possible health hazards.
NOTE	The manufacturer does not, in any manner, assume the responsibility for performing the recommended maintenance schedule, unless an Equipment Maintenance Agreement exists. The sole responsibility rests with the individuals, hospitals, or institutions utilizing the device.
NOTE	The planned maintenance check must be performed to the whole patient monitoring system, including all the connected devices. This service manual covers the planned maintenance procedure for the B850 CPU. See the related service manuals for information about the planned maintenance checks for the connected devices.

Corrective maintenance check

The purpose of the corrective maintenance check is to ensure that the product was repaired correctly, and to check that the product is safe to use and maintains its performance characteristics. Perform the corrective maintenance check after any corrective maintenance, before taking the monitor back into clinical use.

Checking the user and service manuals

Start the installation check by checking the manuals:

1. Check that the customer has all user and service manuals for the CARESCAPE monitoring system with SW v3.2 and the customer knows how to use them.

After having confirmed that the customer has the correct manuals, proceed to the visual check.

Performing visual inspection

Perform the following visual inspection to the installed monitoring system:

1. Check that all product labeling, markings and symbols are intact and readable.
2. Check that the monitor and the connected devices do not have any visible damage.
3. Check that the monitor and the connected devices are properly mounted with specified mounting solutions.
4. Check that the cables between the CPU and the connected devices are intact, properly connected and secured to the right connectors. Pay special attention to the following:
 - a. Verify that the power cord and USB cables are properly secured with the supplied retaining clips.
 - b. Verify that the network cable(s) are intact and properly connected to the right connectors.
5. Check that the acquisition modules are properly connected and locked.

Performing electrical safety tests

Electrical safety tests provide a method of determining if potential electrical health hazards to the patient or operator of the device exist.

- WARNING** EXCESSIVE LEAKAGE CURRENT. Do not use a multiple socket outlet or extension cord in an ME system.
- WARNING** EXCESSIVE LEAKAGE CURRENT. A display or printer that is a non-medical grade device and is used within the patient environment, must always be powered from an additional transformer providing at least basic isolation (isolating or separating transformer). Using without an isolating transformer could result in unacceptable enclosure leakage currents.
- WARNING** EXCESSIVE LEAKAGE CURRENT. Laser printers are not IEC 60601-1 certified equipment and may not meet the leakage current requirements of patient care equipment. This equipment must not be located in the patient environment unless the medical system standard IEC 60601-1 clause 16 is followed. Do not connect a laser printer to a multiple socket outlet supplying patient care equipment. The use of multiple socket outlet for a system will result in an enclosure leakage current equal to the sum of all the individual earth leakage currents of the system if there is an interruption of the multiple socket outlet protective earth conductor. Consult your local service representative before installing a laser printer.
- WARNING** EXCESSIVE LEAKAGE CURRENT - To avoid summation of leakage currents when interfacing the device with other equipment, the devices may only be interconnected with each other or to parts of the system when it has been determined by qualified biomedical personnel that there is no danger to the patient, the operator, or the environment as a result. In those instances where there is any element of doubt concerning the safety of the connected devices, the user must contact the manufacturers concerned (or other informed experts) for proper use. In all cases, safe and proper operation should be verified with the applicable manufacturer's instructions for use, and system standards IEC60601-1 must be complied with.

Test setup

The electrical safety test procedure described in this service manual is intended for the following system components in the CARESCAPE B850 monitoring system:

- B850 CPU unit
- D19KT displays
- F5/F7 Frames
- E-modules
- E-musb with CARESCAPE rSO₂ and CARESCAPE CO₂ – Microteam
- CARESCAPE PDM
- CARESCAPE ONE, only if connected to the CARESCAPE B850 with an 1.5 m (5 ft) or 4.5 m (15 ft) ePort cable.

NOTE If CARESCAPE ONE is connected to the CARESCAPE B850 with a 30 m (98.5 ft) Ethernet cable, or used as a stand-alone monitor, perform the electrical safety test for the CARESCAPE ONE according to the CARESCAPE ONE Service Manual.

Perform the electrical safety tests for the PRN 50-M+ and Unity Network Interface Device (ID) according to the product's own service manual.

All system components must be properly connected to the CPU during the electrical safety tests.

Test conditions

Perform electrical safety tests under normal ambient conditions of temperature, humidity and pressure.

Test equipment

The test equipment required to perform electrical safety tests is listed below.

Tool	Part number / requirement
Safety Analyzer / Leakage Current Tester	<p>Perform the electrical safety tests using an electrical safety analyzer according to IEC 60601-1; 3.1 edition, AAMI ES60601-1 + C1 + A1 + A2, EN 60601-1 or CSA CAN/CSA-C22.2 NO. 60601-1:14.</p> <p>The schematics in this section show the principle of the test equipment. The actual configuration of the test equipment may vary.</p> <p>Refer to the instructions delivered with the safety analyzer to perform each test.</p>
Safety Test Body Kit	<p>P/N: M1155870 for E-Modules and CARESCAPE PDM</p> <p>P/N: 2101836-001 for CARESCAPE Parameters</p> <p>Instead of the test bodies in the safety test body kit, you may use other applicable test bodies with all pins connected together.</p>

The patient monitor being tested should be placed on an insulating surface.

NOTE Before proceeding, make sure that all test equipment is properly calibrated, maintained and functioning.

Verifying power outlets

1. Verify that the power outlet is wired correctly according to the country's electrical code standard before starting the following electrical safety tests.

The results of the following tests will be inaccurate unless a properly wired power outlet is used.

Verifying power cords and plugs

1. Verify that the power cords being used with the monitoring system are undamaged:
 - a. Inspect each power cord for wear or damage. If damage is suspected, test for continuity through each conductor of the power cord connector.
 - b. Replace the power cord, as necessary, with a regulatory-approved cord for the country of use.

WARNING

ELECTRIC SHOCK. To avoid the risk of electric shock, use only AC power cords recommended or manufactured by GE.

Ground integrity check

There are two alternative methods for checking the ground integrity:

- Testing ground continuity
- Checking the impedance of protective earth connection

These tests determine whether the device's exposed metal and power inlet's ground connection has a power ground fault condition.

Perform this test separately for the CPU unit and for the displays according to the following instruction.

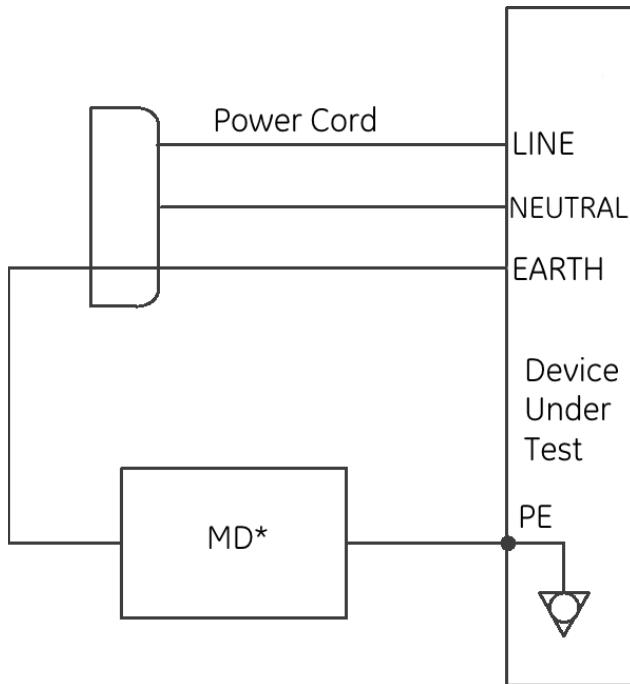
Perform the test in accordance to your local regulations.

NOTE

Refer to the instructions delivered with the safety analyzer to perform each test.

Testing ground continuity

The measuring device (MD) in the diagram below may be a digital multimeter or part of the safety analyzer.



Acceptance criteria:

- For equipment without a power supply cord, the impedance between the protective ground terminal and any accessible metal part which is protectively grounded shall not exceed 0.1 ohms.
- For equipment with a power supply cord, the impedance between the protective ground pin in the mains plug and any accessible metal part which is protectively grounded shall not exceed 0.2 ohms.

Checking impedance of protective ground connection

This test is normally only required as a manufacturing production test to receive safety agency compliance. Some country agencies do require this test after field equipment repairs (i.e., Germany's DIN VDE 0751 standards). Consult your country/local safety agency if in doubt.

Preferably use a safety analyzer and test the equipment with the power supply cord.

Check compliance as follows:

1. A current of 25A from a current source with a frequency of 50 or 60 Hz with a no-load voltage not exceeding 6 V is passed for at least 5 seconds, but not more than 10 seconds, through the protective ground terminal or the protective ground pin in the mains plug and each accessible metal part which could become live in case of failure in basic insulation
2. The voltage drop between the parts described is measured and the impedance determined from the current and voltage drop. It shall not exceed the values indicated.

When taking this measurement, flex the unit's power cord along its length. There should be no fluctuations in resistance.

Acceptance criteria:

- For equipment with a power supply cord, the impedance between the protective ground pin in the mains plug and any accessible metal part which is protectively grounded shall not exceed 0.2 ohms.
- For equipment without a power supply cord, the impedance between the protective ground terminal and any accessible metal part which is protectively earthed shall not exceed 0.1 ohms.

Testing earth leakage current

This test measures the current leakage flowing from the mains part through or across the insulation into the protective earth conductor of the device under test.

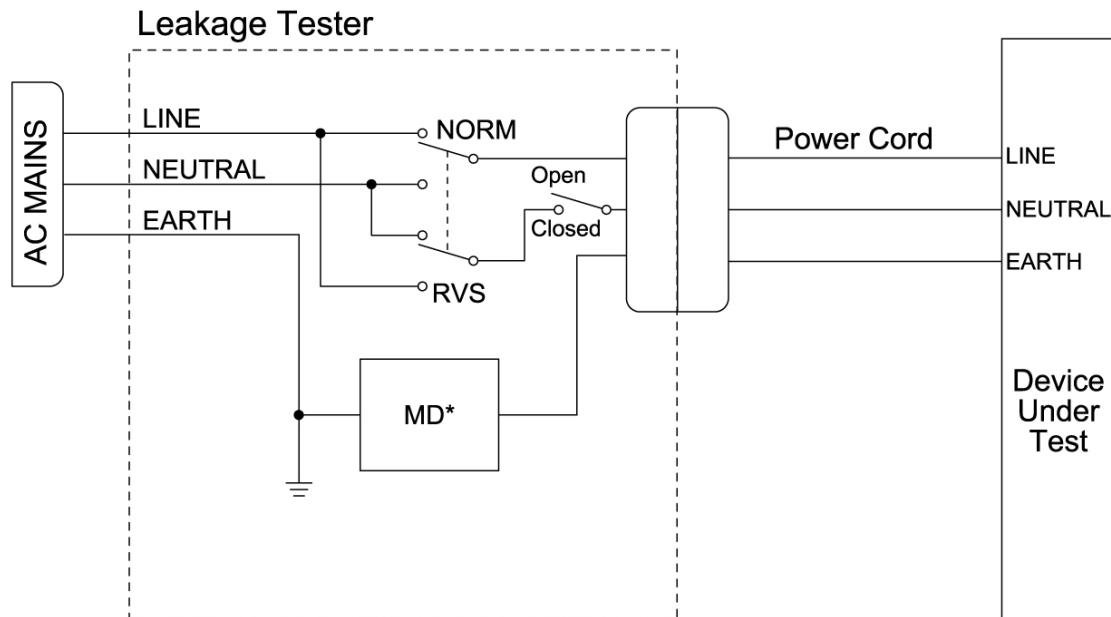
Perform this test separately for the CPU unit and for the displays according to the following instruction.

Perform this test both in Normal Condition (NC) and in a Single Fault Condition (SFC), where one of the supply conductors is open at a time. Perform the test with normal and reverse polarity

The test sequence described below is for reference only. You can also perform the subtests in a different order.

NOTE

Refer to the instructions delivered with the safety analyzer to perform this test.



In the diagram:

* The measuring device (MD) represents the network and voltage measuring instrument and its frequency characters according to IEC 60601-1.

1. Configure the safety analyzer as follows (NC):
 - Polarity: NORMAL
 - Neutral: CLOSED
2. Power on the device under test.

3. Read and record the current leakage indicated on the safety tester.
4. Configure the safety analyzer as follows (SFC):
 - Polarity: NORMAL
 - Neutral: OPEN
5. Read and record the current leakage indicated on the safety tester.
6. Configure the safety analyzer as follows (SFC):
 - Polarity: REVERSED
 - Neutral: OPEN
7. Read and record the current leakage indicated on the safety tester.
8. Configure the safety analyzer as follows (NC):
 - Polarity: REVERSED
 - Neutral: CLOSED
9. Read and record the current leakage indicated on the safety tester.
10. Power off the device under test.

Acceptance criteria in Normal Condition (NC):

- All readings shall be less than or equal to 5 mA for installations that require compliance to IEC 60601-1 requirements.

Acceptance criteria in Single Fault Condition (SFC) – one of the supply conductors open at a time:

- All readings shall be less than or equal to 10 mA.

Testing touch current

This test measures current leakage through the exposed conductive parts on the device under test.

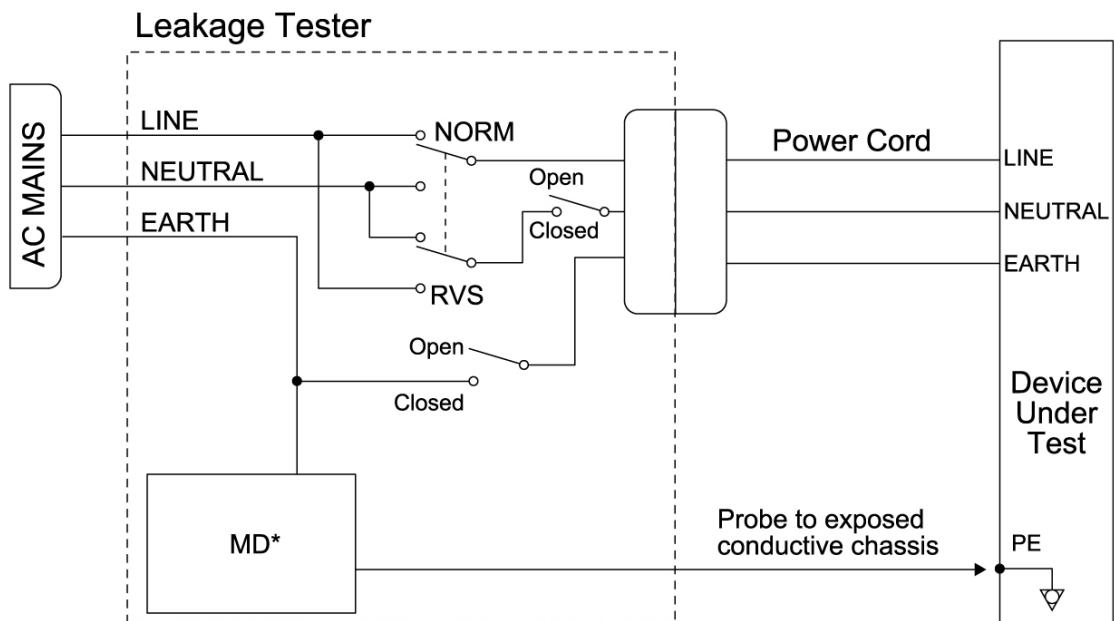
Perform the test in Normal Condition (NC) and in two different Single Fault Conditions (SFC): 1) earth open and 2) one of the supply conductors open at a time. Perform the test with normal and reverse polarity.

The test sequence described below is for reference only. You can also perform the subtests in a different order.

- CPU: You don't have to perform the tests in Normal Condition (NC), because the CPU enclosure is connected to the protective earth.
- Displays: Perform all the conditions. Measure the touch current from one of the screws in the mounting plate in the back of the display.
- CARESCAPE ONE: Perform all the conditions. Measure the touch current from one of the ePort screws, or the RJ-45 connector.

NOTE

Refer to the instructions delivered with the safety analyzer to perform this test.



In the diagram:

* The measuring device (MD) represents the network and voltage measuring instrument and its frequency characters according to IEC 60601-1.

1. Configure the safety analyzer as follows (NC):
 - Polarity: NORMAL
 - Neutral: CLOSED
 - Earth (GND): CLOSED
2. Power on the device under test.
3. Read and record the current leakage indicated on the safety tester.
4. Configure the safety analyzer as follows (SFC):
 - Polarity: NORMAL
 - Neutral: OPEN
 - Earth (GND): CLOSED
5. Read and record the current leakage indicated on the safety tester.
6. Configure the safety analyzer as follows (SFC):
 - Polarity: NORMAL
 - Neutral: CLOSED
 - Earth (GND): OPEN
7. Read and record the current leakage indicated on the safety tester.
8. Configure the safety analyzer as follows (SFC):
 - Polarity: REVERSED
 - Neutral: CLOSED
 - Earth (GND): OPEN
9. Read and record the current leakage indicated on the safety tester.

10. Configure the safety analyzer as follows (SFC):
 - Polarity: REVERSED
 - Neutral: OPEN
 - Earth (GND): CLOSED
11. Read and record the current leakage indicated on the safety tester.
12. Configure the safety analyzer as follows (NC):
 - Polarity: REVERSED
 - Neutral: CLOSED
 - Earth (GND): CLOSED
13. Read and record the current leakage indicated on the safety tester.
14. Power off the device under test.

Acceptance criteria in Normal Condition (NC):

- All readings shall be less than or equal to 100 µA

Acceptance criteria in Single Fault Condition (SFC) – earth open or one of the supply conductors open at a time:

- All readings shall be less than or equal to 300 µA for installations that require compliance to UL 60601-1 requirements.
- All readings shall be less than or equal to 500 µA for installations that require compliance to EN 60601-1 / IEC 60601-1 requirements.

Patient leakage current tests

Patient leakage current tests consist of patient (source) leakage current tests and patient (sink) leakage current tests. Perform these patient leakage current tests for all the E-modules, PDM and CARESCAPE Parameters connected to the monitor.

Patient leakage current tests for acquisition modules

The following table specifies the applied part connections to be tested with each connected E-module and PDM.

Use the safety test body kit, P/N M1155870 (or equivalent), to perform patient leakage current tests. This safety test body kit contains various test connectors where all pins are shorted out together. For information on which test connector to use for each patient connector, refer to the service instructions included in the safety test body kit.

NOTE If not otherwise stated in the table below, connect the test connector directly to the specified connector in the module.

Applied part connections to be tested with each connected E-module and PDM	
Module	Patient connector
E-PT	P3/P7
E-PP	P5
E-COP, E-COPSV	P4/P8
E-PiCCO	P8
E-NSATX	SpO2

Applied part connections to be tested with each connected E-module and PDM	
Module	Patient connector
E-Masimo	SpO ₂
E-NMT	NMT
E-BIS	<p>1. Connect the BISx Digital Signal Processing Unit with the Patient Interface Cable (PIC+) to the E-BIS module.</p> <p>2. Connect the specified test body to the PIC+ cable.</p> <p>The patient isolation is in the BISx Digital Signal Processing Unit, not in the E-BIS module.</p>
E-Entropy	<p>1. Connect an Entropy sensor cable to the module.</p> <p>2. Connect the specified test body to the Entropy sensor cable.</p>
E-EEGX	<p>1. Disconnect the N-EEGX headbox from the E-EEGX module.</p> <p>2. Connect the test body directly to the E-EEGX module.</p>
PDM	ECG & SpO ₂

Patient leakage current tests for E-musb with CARESCAPE rSO₂

Use the safety test body kit, P/N 5851468 (or equivalent), to perform patient leakage current tests. The safety test body kit contains various test connectors where all pins are shorted out together.

Applied part connection to be tested	
Module	Patient connector
E-musb	Connect the test body to one of the INVOS sensor cable connectors.

Patient leakage current tests for CARESCAPE ONE with CARESCAPE Parameters

Perform the patient leakage current tests for each CARESCAPE Parameter connected to the CARESCAPE ONE, including:

- CARESCAPE ECG
- CARESCAPE Pressure
- CARESCAPE Temperature
- CARESCAPE SpO₂
- CARESCAPE SpO₂ Masimo
- CARESCAPE SpO₂ Nellcor
- CARESCAPE CO₂- LoFlo
- CARESCAPE rSO₂

Use the safety test body kit, P/N 2101836-001 (or equivalent). The safety test body kit contains a test connector for each available CARESCAPE Parameter. All pins in a test connector are shorted out together.

Testing patient (source) leakage current

This procedure measures the leakage current from an applied part connector of the device to ground.

Perform this test for all the E-modules, PDM and CARESCAPE Parameters connected to the monitor.

Perform the test in Normal Condition (NC) and in two different Single Fault Conditions (SFC): 1) earth open and 2) one of the supply conductors open at a time.

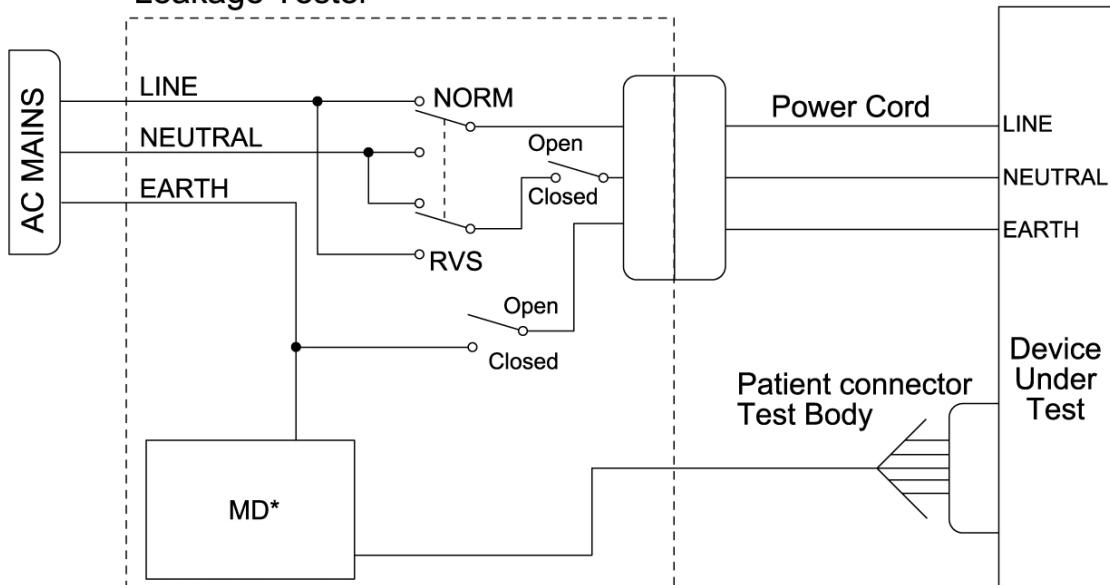
Perform the test with normal and reverse polarity.

The test sequence described below is for reference only. You can also perform the subtests in a different order.

NOTE

Refer to the instructions delivered with the safety analyzer to perform this test.

Leakage Tester



In the diagram:

* The measuring device (MD) represents the network and voltage measuring instrument and its frequency characters according to IEC 60601-1.

1. Configure the safety analyzer as follows (NC):
 - Polarity: NORMAL
 - Neutral: CLOSED
 - Earth (GND): CLOSED
2. Power on the device under test.
3. Read and record the current leakage indicated on the safety tester.
4. Configure the safety analyzer as follows (SFC):
 - Polarity: NORMAL
 - Neutral: OPEN
 - Earth (GND): CLOSED
5. Read and record the current leakage indicated on the safety tester.

6. Configure the safety analyzer as follows (SFC):
 - Polarity: NORMAL
 - Neutral: CLOSED
 - Earth (GND): OPEN
7. Read and record the current leakage indicated on the safety tester.
8. Configure the safety analyzer as follows (SFC):
 - Polarity: REVERSED
 - Neutral: CLOSED
 - Earth (GND): OPEN
9. Read and record the current leakage indicated on the safety tester.
10. Configure the safety analyzer as follows (SFC):
 - Polarity: REVERSED
 - Neutral: OPEN
 - Earth (GND): CLOSED
11. Read and record the current leakage indicated on the safety tester.
12. Configure the safety analyzer as follows (NC):
 - Polarity: REVERSED
 - Neutral: CLOSED
 - Earth (GND): CLOSED
13. Read and record the current leakage indicated on the safety tester.
14. Power off the device under test.
15. Repeat this test for all the connected acquisition modules and patient connectors specified in table Patient connectors to be tested with each module.

Acceptance criteria in Normal Condition (NC):

- All readings shall be less than or equal to 10 µA (d.c.).

Acceptance criteria in Single Fault Condition (SFC) – earth open or one of the supply conductors open at a time:

- All readings shall be less than or equal to 50 µA (d.c.).

Testing patient (sink) leakage current

This procedure measures the leakage current from an applied part connector of the device to ground when the applied part connector is connected to 250 V.

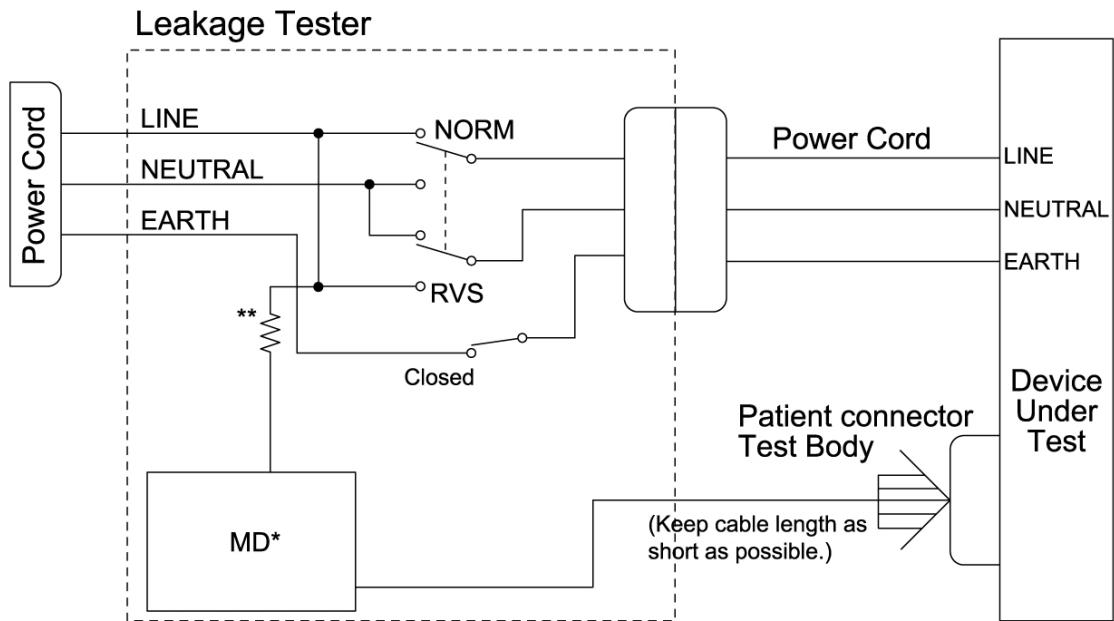
Perform this test for all the E-modules, PDM and CARESCAPE Parameters connected to the monitor.

Perform the test in Normal Condition (NC) with normal and reverse polarity.

The test sequence described below is for reference only. You can also perform the subtests in a different order.

NOTE

Refer to the instructions delivered with the safety analyzer to perform this test.



In the diagram:

* The measuring device (MD) represents the network and voltage measuring instrument and its frequency characters according to IEC 60601-1.

** According to IEC-60601, the impedance to protect the circuitry and the person performing the test, but low enough to accept currents higher than the allowable values of the leakage current to be measured.

WARNING

SHOCK HAZARD. The following step causes high voltage at the test body. Do not touch the test body.

1. Configure the safety analyzer as follows:
 - Polarity: NORMAL
 - Neutral: CLOSED
 - GND: CLOSED
2. Power on the device under test.
3. Read and record the current leakage indicated on the safety tester.
4. Configure the safety analyzer as follows:
 - Polarity: REVERSED
 - Neutral: CLOSED
 - GND: CLOSED
5. Read and record the current leakage indicated on the safety tester.
6. Power off the device under test.
7. Repeat this test for all the connected acquisition modules and patient connectors specified in table Patient connectors to be tested with each module

Acceptance criteria:

- All readings shall be less than or equal to 50 µA (d.c.).

Completing electrical safety tests

1. Disconnect the safety analyzer from the power outlet.
2. Disconnect the test equipment from the patient monitor.
3. Disconnect the patient monitor's power cord from the leakage tester.

Performing functional check

Preparing for the functional check

1. Turn off the CPU power:
 - a. Press the on/standby button on the monitor front panel. When a text on screen prompts you to do so, press the power button a second time.
 - b. Press the power on/off switch located on the back of the monitor to the 0 (off) position.
2. Turn off all the connected displays:
 - a. Press the on /off switch located on the back of the display to the 0 (off) position.The monitor and display are now turned off.

Testing the alarm light

Perform the following tests for all the connected displays:

1. Press the power on/off switch located on the back of the display to the I (on) position.
2. Check the following:
 - a. The power indicator is lit.
 - b. The blue, yellow and red alarm light illuminates momentarily.
 - c. The blue pause audio alarm indicator illuminates momentarily.
3. Repeat steps 1. to 2. for the secondary display, if connected.

Checking the startup

1. Press the power on/off switch located on the back of the CPU to the I (on) position.
2. Check that the green mains power indicator  on the front panel is lit.
3. Press the on/standby button on the CPU front panel.
4. Check that the monitor starts up normally:
 - The green power indicator  on the front panel is lit.
 - Normal monitoring screen appears and there are no system error messages on the screen.
 - The speaker gives a muffled audible beep.
 - The language of the clinical user interface is correct
 - Check that the monitor date and time are correct.

Checking displays

Perform the following tests for all the connected displays.

Checking picture quality

1. Check that all text is readable and all images are clear.
2. Check that the display brightness is adequate in the use environment. Adjust if necessary.

Testing touchscreen control

1. To check the touchscreen operation, touch a corner of an active parameter window.
Check that the related menu is opened.
2. Recalibrate the touchscreen, if needed.
3. Select  to return to the normal screen.

Testing Trim Knob

Perform this test for all displays with Trim Knob.

1. Rotate the **Trim Knob** control in either direction to move from option to option on the display.
2. Press the **Trim Knob** control once to select the highlighted option.
3. Check that the selected menu is opened on the screen or the selected activity is started.

Checking the status of connected devices

Check that the following devices are properly identified and configured. Skip the steps that are not applicable for the installed monitoring system.

1. Log in to the service interface.

2. Select **Information**:
 - a. Select **Host Information**: Check that **Host Serial Number** and **Active Software Version** are correct.
 - b. Select **Host License Information**: Check that all the ordered licenses are enabled.
 - c. Select **Acquisition Information- Acquisition Module**: Check that the connected PDM or the connected CARESCAPE ONE is correctly identified.
 - d. Select **Acquisition Information- E-Module**: Check that all the connected E-Modules are correctly identified.
 - e. Select **Acquisition Information- E-Module Frame**: Check that the F5 or F7 Frame is correctly identified.
 - f. Select **Acquisition Information- CARESCAPE Parameters**: Check that the CARESCAPE parameters connected to the CARESCAPE ONE or to the E-musb module are correctly identified.
 - g. Select **PDM License Information**: Check that the connected PDM has the ordered licenses enabled.
 - h. Select **UnityID Information**: Check that the connected CARESCAPE Network ID interface device is identified.
 - i. Select **Admit Settings**: Check that the **Patient ID Prefix** is correct.
 - j. Select **Power Line Frequency**: Check that the power line frequency is correctly configured according to the line frequency used in your country.
 - k. Select **MUSE/12SL**: Check that the MUSE/12SL is correctly configured.
3. Stay connected to the service interface.

Testing printing to IX printers

Perform the following test only if the monitor is connected to a printer in the IX Network and you did not print a test page while you configured the IX printer.

1. Select **Configuration > Printers**.
A list of all the installed IX printers is shown.
2. Select the printer you want to test and select **Print test page**.
3. Verify that the test page is printed to the selected printer.
4. Repeat steps 2 to 3 for all connected IX printers.
5. Log out from the service interface.

Testing InSite RSvP connectivity

Perform the following test only if the remote service is configured and enabled.

1. Contact the local GE online support center to confirm that they can view the monitor.

Testing the USB remote control

Perform this test only if a USB remote control is connected to the monitor.

1. Press any hard key on the remote control.
Verify that the selected menu opens on the screen, or the related activity starts.
2. Rotate the **Trim Knob** control in either direction to move from option to option on the display until you have an active parameter window or main menu item highlighted.
3. Press the **Trim Knob** control once to select the highlighted option.
Verify that the selected menu opens on the screen, or the related activity starts.
4. Select  to return to the normal screen.

Testing the mouse

Perform this test only if a mouse is connected to the monitor.

1. Move the mouse until the pointer (arrow) is over an active parameter window or a main menu item you wish to select, and click the left mouse button once to select it.
2. Verify that a correct window or a menu opens.
3. Select  to return to the normal screen.

Testing the keyboard

Perform this test only if a keyboard is connected to the monitor.

1. Select **Data & Pages > Admit/ Discharge** (or **Start/ End Case**).
2. Select **Patient** tab > **Edit Name & MRN**.
3. Enter some data into the **Medical Record Number** field using the keyboard. Include characters that are specific to the chosen keyboard locale.
4. Check that the keyboard language configuration is correct.
5. Select  to return to the normal screen.

Testing the barcode reader

Perform this test only if a barcode reader is connected to the monitor.

1. Select **Data & Pages > Admit/Discharge** (or **Start / End Case**).
2. Select the **Patient** tab.

3. Scan a test barcode that is applicable to your system:
 - a. Length delimited or Character delimited parser:
 - i. Select **Scan from Barcode**.
 - ii. Scan a known test barcode obtained from the hospital.
NOTE: The barcode data content must be known and in compliance with the completed parser configuration.
 - iii. Verify that the data content in the barcode is correctly populated to the related fields in the **Patient** and the **Administr. Information** tabs.
 - b. No parser:
 - i. Select **Edit Name & MRN** and press **Enter** to highlight the **Medical Record Number** field.
 - ii. Scan a sample barcode that only contains one piece of information (for example, a Serial Number barcode from a module's device label).
 - iii. Verify that the data is correctly populated into the **Medical Record Number** field.
4. Select  to return to the normal screen.

Testing wired MC Network communication

Perform the following test only if the monitor is connected to a wired MC Network.

1. Make sure that at least one other monitor is on the network. The other monitor must be in an admitted state and have an active ECG measurement with a simulator signal.
2. Check that a network symbol  is displayed in the upper right corner of the screen.
3. Select **Data & Pages > Other Patients > View Patients**.
4. Select a care unit from the **Unit** list.
5. From the **Show** list, select **All Patients**
6. Select a patient bed from the list and select **View**
7. Check that a window with parameters from the other monitor displays on the left side of the screen.
8. Select **Close View** to close the window.

Testing Citrix connection

Perform the following test only if Citrix is configured and in use.

1. Select **Data & Pages >** .
2. Verify that the initial program (configured in the service interface) is launched correctly on the screen.
3. Select  to exit the Citrix thin client.

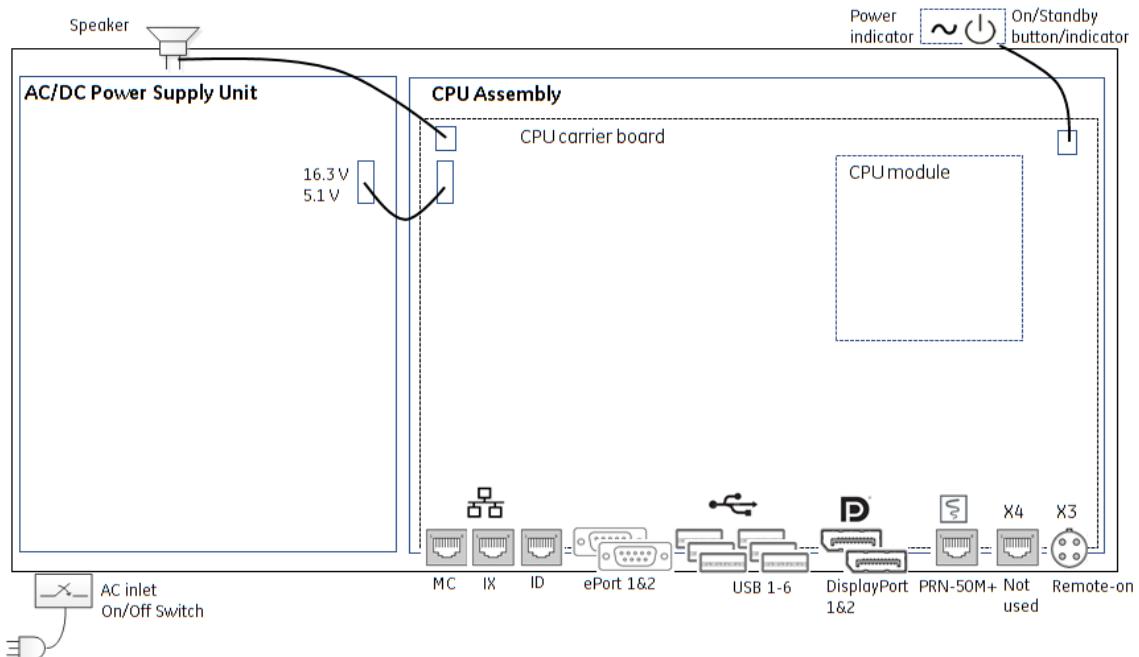
Completing the functional check

1. Select ***Discharge Patient*** or ***Reset Case*** to discard any changes made to the monitor configuration during the functional check.
2. Disconnect the test setup.

9

Theory of operation

Main components



The CPU unit is a key component in the CARESCAPE B850 patient monitoring system. It interfaces with external displays, frames, acquisition modules, acquisition platform, network services, and input devices, and thus composes a functional CARESCAPE B850 patient monitoring system. This chapter provides an overview of CPU operations for troubleshooting purposes.

The CPU unit is housed in a single enclosure. Its main components are:

- AC/DC power supply unit
- CPU assembly:
 - CPU module
 - CPU carrier board
- Speaker assembly
- Front bezel assembly:
 - On/standby button and cable
- Other enclosure parts:

- Bottom enclosure with integrated GCX mounting plate
- Top cover
- Rear panel unit

The CPU unit uses convection cooling. The ventilation openings are in the rear and bottom of the CPU unit. The AC/DC power supply unit and the CPU assembly have integrated heat sinks to enhance cooling.

Power supply

The AC/DC power supply unit is a compact, medical, switched-mode power supply with universal AC input. The power entry module includes an AC input connector and a power on/off switch. The AC input varies between 90–264 Vac, 47–63 Hz single phase.

The power supply unit is designed to output 16.3 Vdc and 5.1 Vdc voltages to the CPU carrier board through the power cable:

- 5.1 Vdc (5V1_ACDC): main supply voltage for the CPU carrier board electronics, CPU module, USB interfaces and DisplayPort interfaces. This voltage is always available when the on/off switch in the back of the CPU unit is in On (I) position. The maximum current provided is 10A.
- 16.3 Vdc (16V7_ACDC): used to provide supply voltage for the F5/F7 Frame, PDM and CARESCAPE Dock F0 that are connected to one of the ePort interfaces. This voltage is enabled only after a device is connected to an ePort. The maximum current provided for each ePort is 3A.

The AC/DC power supply unit provides overload and overvoltage protection.

CPU assembly

The CPU assembly consists of a CPU module and a CPU carrier board. Cooling is arranged with a heat sink that is attached to the CPU module.

The CPU module is an off-the-shelf, highly integrated Qseven computer-on-module (COM) that is based on a dual-core Freescale i.MX6 processor. The main processor of the CPU module manages data processing. The CPU module has non-volatile flash memory for storing software and settings and volatile SDRAM memory for run time code execution. It also provides video, audio, Ethernet, USB and other peripheral interfaces to the CPU carrier board.

The CPU carrier board receives the acquired physiological information from a patient through acquisition modules/platform and processes the acquired data for analysis, display, printing, or transmission to the network. The CPU carrier board contains subsystems for different functions, and provides the interfaces for the external devices connected to the CPU unit.

The following sections describe the different subsystems and functional blocks supported by the CPU carrier board.

Display interfaces

The CPU carrier board provides two DisplayPort connectors for two external displays. The secondary display is capable of displaying different image, if the Dual Video license is installed. The display interfaces meet DisplayPort 1.2a dual-mode standard and support resolutions of up to 1920x1080 @ 60hz. The display interfaces support Extended Display Identification Data (EDID) and identify the capabilities of the

connected displays based on this data. To connect to a CARESCAPE D19KT VER01 display, you must use a DisplayPort to DVI-D Adapter.

DisplayPort1 video signal originates from the HDMI video interface on the CPU module. The HDMI video is converted to DisplayPort video on the CPU carrier board.

DisplayPort2 video signal originates from the LVDS video interface on the CPU module. The LVDS video is converted to DisplayPort video on the CPU carrier board.

Ethernet interfaces

The CPU carrier board has three Ethernet ports (RJ45 connectors) to interface with the CARESCAPE Network MC, CARESCAPE Network IX, and the Unity Network Interface Device (ID). The MC, IX, and ID ports have dual-purpose LED indicators to show the link and activity status for each port. The MC and IX ports have unique hardware (MAC) addresses, and you can configure the IP addresses through the service interface.

The CPU carrier board has two ePort interfaces (DB9 connectors) that use Ethernet communication to interface with PDM, F5/F7 Frames and CARESCAPE Dock F0. The ePort interfaces are also used to supply power for the connected devices.

The MC interface is implemented using 10/100/1000 BASE-T Ethernet communication provided by the CPU module. The IX, ID, ePort1 and ePort2 interfaces are implemented with a PCI Express Gigabit Ethernet controller and an internal switch in the CPU carrier board. They enable 10/100 BASE-T Ethernet communication.

USB interfaces

The CPU carrier board provides six external USB interfaces and internal USB interfaces. The USB interfaces originate from the CPU module.

The internal USB port is used for the recorder serial interface. The external USB ports can be used for connecting to the monitor:

- various input devices (keyboard, mouse, remote control, barcode reader)
- external displays to deliver audible alarms, manage alarm light, touchscreen and Trim Knob, and enable communication with the outbound USB ports on the display
- iCollect or other data acquisition systems that use the DRI protocol
- USB flash drives to save log files or transfer setting files between monitors

NOTE

The USB connector that is connected with a blue line to DisplayPort 1 is reserved for the primary display. The USB connector that is connected with a black line to DisplayPort 2 is reserved for the optional secondary display.

The external USB ports are USB2.0 compatible and they support low-speed, full-speed, and hi-speed operation. The external USB ports are capable of providing 5 V supply voltage with a 500 mA output current.

Recorder interface

The CPU carrier board provides serial interface (RJ-45 connector) for the PRN-50M+ recorder. This recorder interface supports only a 1-wire (RS-232) serial communication needed by the recorder. Ethernet is not implemented on the recorder interface port. The RS232 interface originates from an internal USB interface.

Internal audio subsystem

The internal audio subsystem is used to provide audible alarms and beat tones to the speaker in the CPU unit. The internal audio interface originates from the I2S port on the CPU module. The digital I2S audio signal is converted to analog audio signal with an audio codec on the CPU carrier board and amplified. The amplified analog audio signal is then directed to the internal speaker.

NOTE

In addition to the internal audio interface, the CPU unit provides audible alarms to external displays through the USB interface.

On/standby button/indicator, remote-on interface and power management logic

The front bezel assembly has a circuit board with an on/standby button and power indicators. This board connects to the CPU carrier board with the on/standby button cable.

The rear panel of the CPU unit has a round 4-pin remote-on connector that enables connection to a compatible GE anesthesia machine with a remote-on cable. This provides an alternative method for switching the CPU unit between on and standby states.

The on/standby button illuminates green when it is pressed to on (I) position, or the system is powered on through the remote-on interface. The on/standby button indicator is off when the CPU unit is turned to standby position.

The power management logic monitors the incoming signals from the on/standby button and remote-on connector. It turns the CPU unit into on or standby state in a controlled way, taking care of proper power sequencing and shut-down logic.

DC/DC subsystem

The DC/DC subsystem in the CPU carrier board has step-down converters and load switches to generate the additional supply voltages for other subsystems:

- +5 V (S_VSYS_5V) is supplied for the USB connectors and CPU carrier board regulators.
- +3.3 V (S_3V3_PMC) is supplied for the always-on electronics inside the CPU carrier board (such as the power-up logic).
- +1.8 V (S_1V8_CPUC) is supplied for the CPU carrier board electronics.
- +5 V (S_5V0_Q7) is supplied for the CPU module.

Under-voltage and over-voltage protection

The CPU carrier board has under-voltage and over-voltage detection circuits that monitor supply voltages used on the CPU carrier board, and provide for the CPU module. If any of the monitored supply voltages go beyond their specification limits, the monitor is restarted.

Watchdog circuitry

The CPU module has an internal watchdog timer circuitry, which is refreshed by the software at regular intervals. If the software fails to refresh the watchdog timer circuitry, the monitor restarts automatically.

Real time clock and battery backup

The CPU carrier board has a real-time clock (RTC) with a battery backup. The real-time clock is used to store system date and time when the monitor is turned to off/standby position.

System supervision

The CPU carrier board has A/D converters and temperature sensors that monitor the internal supply voltages and temperatures in the CPU unit. Many of the monitored temperatures and voltages are shown to the service user in the service interface.

10

Troubleshooting

Troubleshooting guidelines

This chapter focuses on troubleshooting technical problems. Refer to the user manual for troubleshooting monitoring problems and clinical configuration issues.

If a problem remains, contact technical support for service. To ensure accurate problem solving, please be prepared to provide the following information:

- Product name and serial number or UDI
- Hardware and software versions
- Detailed problem description
- Error messages, if any
- Configuration information (or settings file)
- Service Logs
- The troubleshooting you have done so far

Perform the specified corrective maintenance check after any corrective maintenance to the product.

Performing basic troubleshooting

Before beginning any detailed troubleshooting, complete the following steps:

1. Check if there are any error messages shown in the message field. For a list of possible causes and solutions, see [Messages related to various technical issues](#).
2. Perform visual inspection to be sure that:
 - There is no physical damage.
 - All peripheral devices are connected properly.
 - The monitor and the connected peripheral devices are properly powered.
3. Verify the compatibility of all system components.

For a list of the compatible devices, see the supplemental information manual.
For a list of compatible supplies and accessories, see [Supplies and Accessories Supplement](#).
4. Verify that the platform and clinical configurations are correct.

For the clinical configuration see user's manual and for the platform configuration see [Configuration chapter](#).

5. If you suspect loose parts or cable connections inside the monitor, disassemble the monitor to a level needed to perform an internal visual check. Check that:
 - a. All screws are tightened properly.
 - b. All cables are connected properly.
 - c. There are no loose objects inside the monitor.
- Perform the electrical safety test and the checkout procedure every time you have disassembled the patient monitor.

Viewing configuration and device information

To view current platform configuration, hardware and software information of the monitor and the connected peripheral devices:

1. Log in to the service interface.
2. Select ***Information***.
3. Select the menu option on the left side of the screen, or scroll down the page to view the information.

Information

Item	Description
Host Information	Active software part number and version, uploaded software part number and version, Host serial number, Host asset number, MC Network IP address, IX Network IP address, MC MAC address, IX MAC address, CPU hardware version.
Network	For dual wire configuration: <ul style="list-style-type: none"> • Active MC Network configuration: IP address and Netmask • Active IX Network configuration: DHCP, IP address, Netmask, and Default Gateway For single wire configuration: <ul style="list-style-type: none"> • Active MC Network configuration: IP address, Netmask, and Default Gateway • IX Network configuration shown as disabled
Active Software Package	Current active software package in use.
Host License Information	Each host license name, its current status (enabled, disabled or trial), feature code, and the expiration date for a trial license.
Default Clinical Settings	Current default clinical settings.
Acquisition Information - Acquisition Module	Shows current information related to a connected acquisition device. <ul style="list-style-type: none"> • For PDM: Active software version, Main board revision, DAS board revision, Serial number, Asset number, MAC address, IP address, Power frequency, ECG filter. • For CS ONE: Active software version, CPU HW version, Serial number and Asset number.
Acquisition Information - E-Module	Label, Software version, Control number, and Serial number.

Item	Description
Acquisition Information - E-Module Frame	E module frame: Frame Serial number, EMBC Serial number, EMBC Software number, EMBC Software version, and EMBC IP address.
Acquisition Information - CARESCAPE Parameters	Shows current information related to the CARESCAPE Parameters: Cable type, Serial number, and Software version.
Installed IX Printers	Printer name, hostname or IP address.
Printer Location Information	Printout type (Alarm Waveforms, Numeric Trends, Reports, Telemetry Waveforms, and Waveforms) and Printer location.
PDM License Information	PDM license option, status, and number of licenses.
UnityID Information	Product ID, Unity Network ID software number and version, Date, Time, Device name and software version of each device connected.
Admit Settings	Patient ID Prefix.
Citrix	Server address, initial program, session timeout in minutes, username and encryption level.
Unit and Bed Name	Unit name and Bed name for CARESCAPE Network.
Remote Service	Status, Enterprise URL, Proxy Address, Proxy port, Proxy username.
Language	Clinical user interface language.
Power Line Frequency	Current power line frequency setting in use.
MUSE/12SL	Location ID, Site number, MUSE web username, and MUSE web URL
Remote Alarm Device Settings	Operation status and power failure detection status.
Remote Alarm Devices	Remote alarm devices currently connected to the monitor.
USB Port Information	Product name, Manufacturer, Vendor code, Product ID, and Serial number.

Viewing hardware statistics

You can view internal supply voltages and temperatures in the **Hardware Statistics** menu.

A value is displayed in red if the current reading exceeds a pre-determined lower or upper limit. A value is displayed either as "0" or as "--" if it cannot be measured.

1. Log in to the service interface.
2. Select **Diagnostics > Hardware Statistics**.
3. Scroll down the page to view the information.

The controlled parameters are measured with voltage monitors and temperature sensors in the specified subsystem.

Hardware statistics

Measurement	Description
S_16V7_ACDC S_5V1_ACDC	Inputs 16.3 V & 5.1 V voltage (in V). These voltages are generated by the AC/DC power supply unit and supplied as input voltages to the CPU assembly. The voltages are measured from the CPU carrier board.
S_VSYS_5V, S_3V3_PMC, S_1V8_CPUC & S_5V0_Q7	<p>These voltages are generated by the step-down converters or load switches in the CPU carrier board. These voltages supply power to the following subsystems:</p> <ul style="list-style-type: none"> • +5 V (S_VSYS_5V) is supplied for the USB connectors and CPU carrier board regulators. • +3.3 V (S_3V3_PMC) is supplied for the always-on electronics inside the CPU carrier board (such as the power-up logic). • +1.8 V (S_1V8_CPUC) is supplied for the CPU carrier board electronics. • +5 V (S_5V0_Q7) is supplied for the Q7 CPU Module. <p>These voltages are measured by the A/D converter in the CPU carrier board.</p>
S_EPORT1_ID_SEN S_V_EPORT1 S_EPORT2_ID_SEN S_V_EPORT2	<p>The S_EPORTx_ID_SEN is the ePort 1 or 2 sensing voltage (in V). If the ID voltage is lower than 1.57 V, the monitor identifies that a device (F5/F7 Frame, PDM or CARESCAPE Dock F0) is connected to the ePort connector, and it will start powering the connected device with the S_V_EPORTx (16.3 V) voltage.</p> <p>These voltages are measured by the A/D converter in the CPU carrier board. The current value is shown as “--” if a device is not connected.</p>
AMBIENT_TEMPERATURE	Ambient temperature (in °C). The internal temperature of the monitor measured by the temperature sensor in the CPU carrier board.
CPU_CORE_TEMPERATURE	CPU core temperature (in °C). The internal temperature of the processor measured by the temperature sensor in the CPU module.

Pinging a TCP/IP network device

You can verify connectivity with a network device on the MC Network and IX Network using **Ping**.

1. Log in to the service interface.
2. Select **Diagnostics >Ping**.
3. In the **Address to Ping** field enter the IP address of a known device on the network and select ping.

If you receive a reply, the monitor is able to connect to the network device.

If you do not receive a reply, make sure that the monitor is connected to an active network.

NOTE

The monitor withstands a maximum packet loss of 5 packets per 1 million and maximum latency of 250 ms without performance degradation.

Viewing log files

1. Log in to the service interface.

2. Select **Diagnostics > View Logs**.
3. Select the log you want to view. The contents of the selected log file are shown on the screen.

Downloading log files

For security reasons, the contents of the log file(s) will be encrypted with a user-selectable password before the download. Provide the password in a secure way only for the authorized receiver of the log file. Use 7-Zip open-source file archiver (<http://7-zip.org/>) and the password to decrypt the downloaded log file.

1. Log in to the service interface.
2. Select **Diagnostics > Download Logs**.
3. Select the log(s) you want to download.
4. Provide a password to encrypt the contents of the log file. This password is user-selectable.
5. Depending on your access to the service interface:
 - a. If you are using a service PC, you can save the log file to any storage device connected to the service PC:
 - i. Select **Download**.
 - ii. Save the log file according to the instructions provided by the web browser.

The steps to download the log file to a service PC depend on the web browser used. The web browser may also notify you about security issues. Refer to the web browser documentation for details.

- b. If you are using the local, integrated service interface, you can save the log file to a USB flash drive that is connected to one of the monitor's USB ports:
 - i. Select **Save to USB storage** to save the log file to the USB flash drive.

The log file is saved always to the root directory of the USB flash drive.

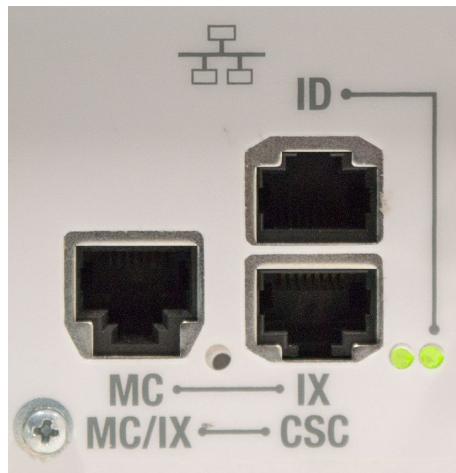
NOTE

Do not disconnect the USB flash drive until downloading is complete.

6. Send the log file and the password in a secure way to GE Service for further investigation.

Network status LEDs

The network status LEDs help in troubleshooting network connectivity and communication problems. The LEDs are located next to each network connector in the rear of the monitor.



There is one dual purpose indicator LED for each network connector:

- The LED is lit to indicate a link. This means that the monitor is physically connected to a network.
- The LED is flashing to indicate activity. This means that the monitor is either transmitting or receiving data packets over the network.

Messages related to various technical issues

The following table lists messages that are not directly related to any parameter or measurement. They are mostly technical messages related to hardware, configuration, network, and similar issues.

To see parameter and measurement related messages, refer to the module's service manual. To see a complete list of the messages, refer to the user manual.

For information regarding alarm priorities and escalation times, see the supplemental information provided.

Make sure you are familiar with the generic layout of the screen. This will help you identify where on screen the following messages appear. The message location is indicated with the following abbreviations:

- al. area = alarm area
- param. = parameter window
- wavef. = waveform area

Message	Location	Possible causes	Suggested actions
• All monitors disconnected	• al. area	The monitor is disconnected from the network.	<ul style="list-style-type: none"> • Re-establish connection. • If the problem persists, check the following: <ol style="list-style-type: none"> 1. The network cable connection and condition. 2. The monitor's network configuration

Message	Location	Possible causes	Suggested actions
			3. The network infrastructure hardware and configuration.
• Analog output malfunction	• al. area	CARESCAPE ONE analog output voltage failure.	• Service CARESCAPE ONE: replace its main board and reinstall the software.
• Application error: Citrix	• al. area	Connection to Citrix application was lost.	• Re-establish the connection. • If the problem persists, contact hospital IT administration to check the Citrix setup and configuration and possible network problems.
• Application error: pdf	• al. area	PDF viewer closes unexpectedly.	• Try to open the MUSE 12SL report again. • If the problem persists, contact GE.
• Application error: Service	• al. area	The local built-in service interface was terminated abnormally.	• Select audio pause to acknowledge the message. • If the problem persists, contact GE.
• Barcode scanned	• al. area	All data has been successfully stored to the monitor.	• No action required.
• Barcode too long	• al. area	The maximum length of the barcode has been exceeded.	• The maximum length of a barcode string is limited to 300 characters. See the Barcode parser configuration section for more information.
• <Bed> Monitor disconnected	• al. area	The monitor with open bed-to-bed view, or with alarm notification enabled, is disconnected from the network.	• Re-establish the connection. • If the problem persists, check the following: 1. The network cable connection and condition. 2. The monitor's network configuration 3. The network infrastructure hardware and configuration.
• Busy Network	• al. area	Printing job cannot be processed immediately.	• Wait. The printing will resume automatically.
• Call Service: Text(s) missing	• al. area	The software text is missing in this language; the text file may be corrupted.	• Reinstall the software and check if the message disappears. Contact GE service representative for support.

Message	Location	Possible causes	Suggested actions
• Call service: Check wired MC/IX certificate.	• al. area	<ul style="list-style-type: none"> The Wired MC/IX certificate for 802.1X authentication will expire in 15 days or less. Incorrect system time. 	<ul style="list-style-type: none"> Contact hospital IT to update the Wired MC/IX certificate for in the monitor. Fix the time and date configuration.
• Call service: Wired MC/IX certificate expired.	• al. area	<ul style="list-style-type: none"> The Wired MC/IX certificate for 802.1X authentication has expired. Authentication to wired network may fail. Incorrect system time. 	<ul style="list-style-type: none"> Contact hospital IT to update the Wired MC/IX certificate for in the monitor. Fix the time and date configuration.
• Case ended	• al. area	OR and PACU software packages: There is no active patient case.	<ul style="list-style-type: none"> No action required.
• Case started	• al. area	OR and PACU software packages: A new case has just been started.	<ul style="list-style-type: none"> No action required.
• Check CS ONE battery	• al. area	<ul style="list-style-type: none"> There is no battery in the indicated device. The indicated device battery is not working properly. 	<ul style="list-style-type: none"> Install the missing battery. Select Monitor Setup > Main Setup > Battery Status > CS ONE and check Slot status. For more information, see the battery diagnostics in the CARESCAPE ONE Service Manual.
• Check PDM battery	• al. area	<ul style="list-style-type: none"> There is no battery in the indicated device. The indicated device battery is not working properly. 	<ul style="list-style-type: none"> Install the missing battery. Select Monitor Setup > Main Setup > Battery Status > PDM and check Slot Status. For more information, see the battery diagnostics in the CARESCAPE PDM Service Manual.
• Configuration change(s)	• al. area	The loaded configuration has changed from the previous one.	<ul style="list-style-type: none"> No action required. The monitor configuration has changed after monitor restart. See Configuration changes. Restart required.
• Configuration changes. Restart required.	• al. area	Pending configuration changes to platform settings that require monitor restart.	<ul style="list-style-type: none"> Restart the monitor. NOTE: You can acknowledge the message, but it will reappear every 6 hours until the monitor is restarted.

Message	Location	Possible causes	Suggested actions
• Configuration error(s)	• al. area	One or more errors have been detected in the configuration.	<ol style="list-style-type: none"> 1. Acknowledge the message. 2. If the message reappears, try the following: <ol style="list-style-type: none"> a. Restart the monitor and check if the message disappears. b. Reset the settings to factory defaults, and restore the original monitor settings from a backup file. c. Reload the software, and then reconfigure the monitor.
• Connecting Measurement	• al. area	An acquisition module has been connected.	• No action required.
• CS Gateway communication failure	• al. area	An error occurred when trying to search for patient on the CARESCAPE Gateway server.	<ul style="list-style-type: none"> • Check the network connectivity. • Retry loading from the network. • Check the gateway configuration.
• CS ONE battery low	• al. area	CARESCAPE ONE battery charge level is low.	<ul style="list-style-type: none"> • Allow CARESCAPE ONE battery to charge. • If message persists, change battery.
• CS ONE battery temp high	• al. area	CS ONE battery temperature error due to a faulty battery or battery management error. Battery charging stops.	<ul style="list-style-type: none"> • For information about the CS ONE battery temperature, select Monitor Setup > Main Setup > Battery Status > CS ONE. • Change battery.
• CS ONE Faulty Device Connected	• al. area	One of the connected CARESCAPE Parameters has a communication failure.	<ul style="list-style-type: none"> • Identify and replace the CARESCAPE Parameter causing the communication failure.
• CS ONE faulty device in port #X	• al. area	CARESCAPE ONE USB port 1 to 8 is reporting an overcurrent. CARESCAPE ONE main board failure.	<ul style="list-style-type: none"> • Refer to CARESCAPE ONE Service Manual for more troubleshooting instructions.
• CS ONE not authenticated: Call service	• al. area	CARESCAPE ONE authentication required. CARESCAPE ONE version 3.0 or an unauthenticated acquisition device connected.	<ul style="list-style-type: none"> • To allow connection, select Configuration > Device Authentication >Allow all connections. • Remove the unauthorized device from the monitor.

Message	Location	Possible causes	Suggested actions
• CS ONE unknown device in port #X	• al. area	An unauthorized device is connected to one of the eight CARESCAPE ONE USB ports is detected.	• Disconnect the unauthorized device.
• CS ONE removed	• al. area	CARESCAPE ONE has been removed.	• Reconnect the CARESCAPE ONE if you want to restart measurements.
• DEMO MODE Not for clinical use!	• al. area	DEMO mode has been enabled.	• To start monitoring a patient, restart the monitor, or select Monitor Setup > Main Setup > Exit DEMO > Confirm .
• E-musb disabled. Connect parameters to CS ONE.	• al. area	It is not possible to use the E-musb module if CARESCAPE ONE is connected to the monitor. The measurement with the connected CARESCAPE Parameter does not start or stops when CARESCAPE ONE is connected to the monitor.	• Disconnect the CARESCAPE Parameter from the E-musb module and connect it to the CARESCAPE ONE instead.
• E-musb faulty device in port X where X = E-musb port A or B	• al. area	E-musb port is reporting an overcurrent situation. This may be due to a defective CARESCAPE Parameter in the indicated E-musb port or due to a hardware failure in the E-musb module.	• Refer to E-musb Service Manual for more troubleshooting instructions.
• E-musb module error	• al. area	There is a hardware error with the E-musb module.	• Disconnect and reconnect the E-musb module. • Replace the E-musb module. • Refer to E-musb Service Manual for more troubleshooting instructions.
• E-musb unknown device in port X where X = E-musb port A or B	• al. area	An incompatible CARESCAPE Parameter or an external USB hub device is connected to the indicated E-musb port.	• Replace the incompatible CARESCAPE Parameter with a compatible CARESCAPE Parameter. E-musb module is only compatible with CARESCAPE CO ₂ – Microstream and CARESCAPE rSO ₂ .

Message	Location	Possible causes	Suggested actions
• External alarm light disconnect. Check USB connection.	• al. area	<ul style="list-style-type: none"> The USB cable between the monitor and the display is disconnected when a patient is admitted/case is started. Display is turned to standby when a patient is admitted/case is started. User interface board communication failure due to a UIC software error. User interface board communication failure due to a user interface board hardware error in the display. 	<p>Depending on the cause:</p> <ul style="list-style-type: none"> Reconnect the USB cable. NOTE: Secure the connected USB cable to the CPU unit. Use the existing retaining clips attached to the CPU unit. Turn on the display. Update the UIC software to the display. Contact the GE service representative to have the display repaired.
• Identical E-musb modules	• al. area	There are two or more E-musb modules in the system.	<ul style="list-style-type: none"> Remove all but one E-musb module.
• Identical IP address noticed	• al. area	IP address conflict. There are two or more monitors or other devices with the same IP address on the network.	<ul style="list-style-type: none"> Disconnect the devices with identical IP addresses from the network, and reconfigure them with a unique IP address(es). Contact hospital IT administration for more information.
• Identical unit & bed name noticed	• al. area	Two or more monitors have the same unit and bed name on the network.	<ul style="list-style-type: none"> Disconnect the duplicate monitor that has the same unit and bed name. Change the bed name of the duplicate monitor.
• Incompatible device: ECG module	• al. area	The module is not compatible.	<ul style="list-style-type: none"> Replace with a compatible ECG module. For a list of compatible devices, refer to the supplemental information provided.
• Incompatible device: Gas module	• al. area	The module is not compatible.	<ul style="list-style-type: none"> Replace with a compatible gas module. For a list of compatible devices, refer to the supplemental information provided.
• Incompatible Module	• al. area	The module is not compatible.	<ul style="list-style-type: none"> Replace with compatible module. See the supplemental information provided.
• Incorrect barcode value	• al. area	The monitor's barcode parser reports about invalid value in the barcode string that was read.	<ul style="list-style-type: none"> Check that the barcode string contains only allowed characters and values. See the Barcode parser configuration section for more information.

Message	Location	Possible causes	Suggested actions
• Invalid barcode configuration	• al. area	The monitor's barcode parser reports about invalid barcode configuration.	• Check that the monitor's barcode parser configuration is correct. Otherwise, the barcode strings cannot be read.
• License(s) expired	• al. area	One or more trial licenses have expired.	• Contact GE to purchase a permanent license. Enable the license in service interface with a new activation code.
• Loading failed	• al. area	Loading a case/patient from an acquisition module or network has been interrupted.	• Check device or network cable connections.
• Loading from CS ONE	• al. area	Patient data is being loaded from CARESCAPE ONE.	• Wait.
• Loading from PDM	• al. area	Patient data is being loaded from an acquisition module.	• Wait.
• Module voltage low	• al. area	Parameters may not be working properly due to a technical fault in the monitor. • One of the supply voltages for the acquisition modules is out of specification.	• If possible, log in to the service interface and select Diagnostics > Hardware Statistics to diagnose which internal supply voltage is out of specification. • The power supply unit or CPU assembly may be defective. Replace the defective unit.
• Monitor restarted. Check patient.	• al. area	Monitor restart (warm start) has occurred unexpectedly when a patient was admitted/case started.	• Reset the alarm by pressing the silence alarms key twice or by discharging the patient/ending the case. • If the problem persists, troubleshoot the root cause for the problem and fix it. Service logs may provide additional information for the restart.
• Multiple Remote Alarm Devices connected	• al. area	There are two or more remote alarm devices connected to the monitor.	• Disconnect all but one remote alarm device.
• Network down	• al. area	No other network device observed on the MC Network.	• Verify that the monitor is connected to an active network.
• No printer selected	• al. area	There is no printer selected on the monitor.	• Select a printer.
• Patient admitted	• al. area	ICU, NICU, and ED software packages: The current patient has just been admitted.	• No action required.
• Patient discharged	• al. area	ICU, NICU, and ED software packages: There is no admitted patient.	• No action required.

Message	Location	Possible causes	Suggested actions
• PDM battery temp high	• al. area	Battery temperature error is caused by a faulty battery or a battery management error. Battery charging stops.	<ul style="list-style-type: none"> For information about the PDM battery temperature, select Monitor Setup > Main Setup > Battery Status > PDM. Change battery.
• PDM charging is denied	• al. area	The PDM battery cannot be charged because the internal temperatures of the monitor or monitor battery is too high.	<ul style="list-style-type: none"> Find the root cause for the high temperature of the monitor or the monitor battery.
• PDM module removed	• al. area	Acquisition module has been removed.	<ul style="list-style-type: none"> Connect the module if you want to restart the measurements.
• Printer error	• al. area	A printer is not present or the printer needs paper.	<ul style="list-style-type: none"> Select Monitor Setup > Main Setup > Printing > Devices to choose a different printer. Add paper to the printer.
• Printing Alarm	• al. area	Recorder: An alarm has triggered printing.	<ul style="list-style-type: none"> Wait for the printing to finish.
• Printing ready	• al. area	Your printing request has been forwarded to the printer.	<ul style="list-style-type: none"> No action required.
• Printing...	• al. area	Printing is occurring. Recorder: Manual printing is initiated for Print Waveforms , ALL ECG, PA Waveform , or Catheter Insertion .	<ul style="list-style-type: none"> Wait for the printing to finish.
• Reconnect CS ONE	• al. area	Monitor does not receive active and latched alarms from the CARESCAPE ONE after connection, or settings transfer failed, or the monitor receives incorrect waveform data.	<ul style="list-style-type: none"> Disconnect the CARESCAPE ONE, wait a few seconds, and then reconnect.
• Reconnect PDM	• al. area	Disconnecting and then reconnecting the PDM too quickly may cause a communication error between the module and the monitor, and result in duplicate waveform data.	<ul style="list-style-type: none"> Disconnect the PDM, wait a few seconds, and then reconnect.
• Recorder out of paper	• al. area	The recorder is out of paper or the recorder cover is open.	<ul style="list-style-type: none"> Replace recorder paper. Close the recorder cover.
• Remote Alarm Device disconnected	• al. area	Remote alarm device operation has been enabled during configuration, but the remote alarm device is disconnected.	<ul style="list-style-type: none"> Connect the remote alarm device, or disable the Remote alarm device operation.

Message	Location	Possible causes	Suggested actions
• Remote Alarm Device service life exceeded	• al. area	The device has reached the end of its expected service life.	<ul style="list-style-type: none"> Stop using the device. Dispose of the device, and contact GE to acquire a new one.
• Saving	• al. area	The recorder is unavailable while printing manual or alarm waveform recording, and the recording is saved for later printing. No recording location has been selected.	<ul style="list-style-type: none"> Check the recorder. Select a recording location.
• Service CS ONE and specific error indication	• al. area	Technical fault in CARESCAPE ONE.	<ul style="list-style-type: none"> See the CARESCAPE ONE service manual for a detailed list of error messages.
• Service E-musb faulty port X where X = E-musb port A or B	• al. area	E-musb is reporting a fault on the indicated E-musb port. This may be due to an internal E-musb hardware error, dirt on the connectors, or a defective CARESCAPE Parameter.	<ul style="list-style-type: none"> Disconnect and reconnect the CARESCAPE Parameter. Try to connect the CARESCAPE Parameter to the other E-musb port. Disconnect and reconnect the E-musb module to the module slot. Refer to E-musb Service Manual for more troubleshooting instructions.
• Service gas module and specific error indication	• al. area	Technical problem in the CARESCAPE Respiratory Module.	<ul style="list-style-type: none"> See the service manual for the CARESCAPE Respiratory Modules for a detailed list of error messages.
• Service Monitor Activation Failed	• al. area	The initiated software activation has failed due to an error situation. The original software version remains active.	<ol style="list-style-type: none"> Check the compatibility of the uploaded software, and try to reactivate the software. If it still fails, reload and active the software. If the problem still persists, contact the GE service representative.
• Service Monitor Error Code 0xHOST1001	• al. area	One of the internal temperature sensors indicate the inside temperature of the monitor is out of specification. The message stays on screen as long as the error condition is valid.	<p>If the temperature is too high:</p> <ol style="list-style-type: none"> Turn off the power. Let the monitor cool down. Check that the ventilation holes are not obstructed. Ensure that the monitor is installed to a location that meets the specified environmental requirements of operating temperature.

Message	Location	Possible causes	Suggested actions
			<p>5. Investigate the monitor thoroughly for potential short circuits and other electrical faults.</p> <p>6. If possible, log in to service interface and select Diagnostics > Hardware Statistics to identify the root cause for the error message.</p> <p>If the temperature is too low (or high) after the monitor has been transported or stored outside the operating temperature, wait for the temperature to stabilize back to the operating temperature range before applying the power.</p>
<ul style="list-style-type: none"> • Service Monitor Error Code 0xHOST1002 	<ul style="list-style-type: none"> • al. area 	<ul style="list-style-type: none"> • One of the internal supply voltages is out of the specification. The message stays on screen as long as the condition is valid. 	<ul style="list-style-type: none"> • Remove any system component connected to the ePort. If the error message disappears, either the connected device or the ePort may be defective. • Log in to service interface and select Diagnostics > Hardware Statistics to identify the supply voltage that is below or above the specification. • The power supply unit or CPU assembly may be defective. Replace the defective unit.
<ul style="list-style-type: none"> • Service Monitor Error Code 0xHOST1004 	<ul style="list-style-type: none"> • al. area 	Disk usage exceeds 90%.	<ul style="list-style-type: none"> • Reinstall the host software and restore clinical and platform settings. • If the problem still persists, contact the GE service representative.
<ul style="list-style-type: none"> • Service Monitor Error Code 0xHOST1005 	<ul style="list-style-type: none"> • al. area 	EMBC error. Communication with E-Modules fails due to one of the following reasons: <ul style="list-style-type: none"> • EMBC software start-up failure. • Incompatible EMBC software version. 	<ul style="list-style-type: none"> • Restart the monitor. • If the problem still persists, activate the EMBC Software Package from the service interface. Select Configuration > Software Management > Devices. NOTE: In case of the EMBC communication error, you cannot update the EMBC software. • If EMBC software activation does not help or is not

Message	Location	Possible causes	Suggested actions
			available, replace the F5/F7 EMBC unit.
• Service Monitor Error Code 0xHOST1008	• al. area	<ul style="list-style-type: none"> The monitor's IX and/or MC network interface is disabled due to traffic overload. <p>The monitor will periodically (once every 5 minutes) check the amount of network traffic in the IX and/or MC Network. The message will disappear and the IX and/or MC network interfaces will be re-enabled once the network traffic overload is over.</p>	<ul style="list-style-type: none"> Find out the root cause for the IX and/or MC Network traffic overload. Consult the hospital IT for troubleshooting support.
• Service Monitor Error Code 0xHOST1100	• al. area	The CPU battery is empty. Time and date may be reset to factory defaults.	<ol style="list-style-type: none"> Replace the CPU battery. Restart the monitor. Adjust the date and time. Restart the monitor again.
• Service Remote Alarm Device	• al. area	One of the relays inside the remote alarm device has a fault.	<ul style="list-style-type: none"> Stop using the device. Dispose of the device, and contact GE to acquire a new one.
• Service the PDM – and specific error indication	• al. area	Technical fault in the PDM.	<ul style="list-style-type: none"> See the CARESCAPE PDM service manual for a detailed list of the PDM error messages.
• Service update certificate	• al. area	<ul style="list-style-type: none"> The installed certificate has expired. Incorrect system time. 	<ul style="list-style-type: none"> Install a new certificate. Fix the time and date configuration.
• Setting activation after next case end	• al. area	Service user has initiated delayed settings activation that will automatically take place after next case end.	<ul style="list-style-type: none"> No action needed. If necessary, you can cancel the pending settings activation from the service interface. Select Configuration > Settings > Activation > Cancel activation.
• Setting activation after next discharge	• al. area	Service user has initiated delayed settings activation that will automatically take place after next discharge.	<ul style="list-style-type: none"> No action needed. If necessary, you can cancel the pending settings activation from the service interface. Select Configuration > Settings > Activation > Cancel activation.

Message	Location	Possible causes	Suggested actions
<ul style="list-style-type: none"> • Software activation after next case end 	<ul style="list-style-type: none"> • al. area 	<p>Service user has initiated delayed software activation that will automatically take place after next case end.</p>	<ul style="list-style-type: none"> • No action needed. • If necessary, you can cancel the pending software activation from the service interface. Select Configuration > Software Management > Host Software > Cancel activation.
<ul style="list-style-type: none"> • Software activation after next discharge 	<ul style="list-style-type: none"> • al. area 	<p>Service user has initiated delayed software activation that will automatically take place after next discharge.</p>	<ul style="list-style-type: none"> • No action needed. • If necessary, you can cancel the pending software activation from the service interface. Select Configuration > Software Management > Host Software > Cancel activation.
<ul style="list-style-type: none"> • SW download failed on CS ONE port #X where X is the CARESCAPE Parameter port number 	<ul style="list-style-type: none"> • al. area 	<p>Software update to a CARESCAPE Parameter failed.</p>	<ul style="list-style-type: none"> • Disconnect and reconnect the CARESCAPE Parameter cable. If the software update fails again, replace the Parameter cable. Refer to CARESCAPE ONE Service Manual for more troubleshooting instructions.
<ul style="list-style-type: none"> • SW update in progress on CS ONE port #X where X is the CARESCAPE Parameter port number 	<ul style="list-style-type: none"> • al. area 	<p>Software update in progress. One of the connected CARESCAPE Parameters is updating software from CARESCAPE ONE.</p>	<ul style="list-style-type: none"> • Wait until the software update to the CARESCAPE Parameter is successfully completed and the message disappears from the monitor screen. This may take up to 1 minute. • Do not disconnect the CARESCAPE Parameter from the CARESCAPE ONE before the software update is completed.
<ul style="list-style-type: none"> • Unable to read licenses 	<ul style="list-style-type: none"> • al. area 	<p>Installed license file is corrupted. The system cannot read the licenses correctly when the monitor starts.</p>	<ul style="list-style-type: none"> • Re-enter licenses or reload the license file. Contact GE to get the correct license file.
<ul style="list-style-type: none"> • Unknown device alarm 	<ul style="list-style-type: none"> • al. area 	<p>One or more alarms not supported by the monitor are active or latched on CARESCAPE ONE during dual monitoring.</p>	<ul style="list-style-type: none"> • Disconnect CARESCAPE ONE, check its alarms and resolve as required.

Problems and solutions

Troubleshooting startup failures

Problem	Possible causes	Recommended action
Unable to turn on the CPU unit.	Power on/off switch located on the back of the CPU unit is set to the off position.	Turn the power on/off switch to the I (on) position and check that the power connection indicator on the front panel illuminates green.
	Power cord is loose.	Ensure that the power cord is connected properly to the wall outlet and to the monitor.
	Power cord is faulty.	Check the power cord for wear and damage, and replace if necessary.
	The power outlet does not meet specified requirements.	<p>Check the power outlet being used:</p> <ul style="list-style-type: none"> Refer to the supplemental information manual for power requirements. Check the power outlet being used.
	The On/standby button cable is loose or defective.	<ul style="list-style-type: none"> Check that the cable is intact and properly connected to the CPU carrier board. Replace the cable if necessary.
	The power supply cable between the power supply unit and the CPU assembly is loose or faulty.	Check that the power supply cable is intact and properly connected to the power board and the CPU carrier board.
	The power supply is faulty.	Replace the power supply unit.
	The CPU assembly is faulty.	Replace the CPU assembly .
Startup procedure does not advance beyond the welcoming screen. Error messages may appear.	<ul style="list-style-type: none"> Unable to read software from the memory. Software is corrupted. 	Replace CPU assembly. Contact your local GE service representative for support.
The monitor starts up with the following text on the screen: Field Replacement Unit, SW version, IP address, and Device MAC address.	<p>The monitor starts up with a special FRU software, because the CPU assembly has been replaced with the CPU assembly FRU.</p> <p>The CARESCAPE software has not been installed after the CPU replacement.</p>	Reinstall the CARESCAPE software and reload the settings. Contact your local GE representative to order the CARESCAPE software. For more information, see the Reloading software and settings section.

User interface issues

Troubleshooting display issues

Problem	Possible cause	Recommended action
There is no picture on the screen even though the CPU unit is turned on.	Display's power cord is loose or defective.	<ul style="list-style-type: none"> Ensure that the power cord is connected properly to the wall outlet and to the monitor. Check the power cord for wear and damage, and replace if necessary.
	Power on/off switch located on the back of the display is set to the off position.	Turn the power on/off switch is to the I (on) position. The power indicator in the front panel should be lit, if in I (on) position.
	The On/Standby button in the front panel of the display is in standby position.	Press the on/standby button into the On position. The on/standby indicator should be lit.
	The display cable, or DisplayPort to DVI-D adapter, is loose or defective.	Check that the display cable and the DisplayPort to DVI-D adapter are properly connected and secured. Replace defective display cable/adapter.
	The display cable is connected to a wrong DisplayPort connector in the CPU Unit.	Check the connections for primary and secondary displays.
	Defective display.	Replace the display. Contact local GE service for support.
Picture is not correctly aligned, or there are some other picture quality issues.	Image is not correctly adjusted.	Select Auto Setup from the display's OSD menu to adjust the picture, or try manual adjustments.
The alarm light, touchscreen, Trim Knob and a device connected to a USB port of the display are all inoperative.	The USB cable between the display and CPU unit is loose or defective, or connected to a wrong connector.	Check that the USB cable is properly connected and secured. Replace defective display cable.
	Defective display (defective main board in the display).	Replace display. Contact local GE service to have the display repaired.
Alarm light does not work.	Defective display (defective alarm light board or cable in the display).	Replace display. Contact local GE service to have the display repaired.
A USB device (keyboard, Mouse, Remote control or Barcode reader) does not work when connected to one of the type A USB connectors in the display.	Incompatible or defective USB device.	<p>Ensure that the connected USB device is compatible with the monitor.</p> <p>Login to service interface and select Information to check the USB Port information.</p>
	Defective display (defective main board in the display).	Replace display. Contact local GE service to have the display repaired.
Trim Knob does not work.	Defective display (defective Trim Knob encoder or UI board in the display).	Replace display. Contact GE service to have the display repaired.

Troubleshooting

Problem	Possible cause	Recommended action
The secondary display is showing the same picture than the primary display. Unable to configure an independent screen to the secondary display.	Dual Video license is not installed.	Contact GE to acquire the Dual Video license.
Touchscreen operation is inaccurate.	Touchscreen is out of calibration	Calibrate the touchscreen.

Troubleshooting USB keyboard and barcode reader

Problem	Possible cause	Recommended action
Wrong character is displayed when a key is pressed on keyboard.	The keyboard locale is not configured correctly.	Configure the keyboard locale correctly.
Wrong character is displayed when a barcode is read.	The keyboard locale is not configured correctly.	Configure the keyboard locale correctly.
	The barcode reader's language configuration is incorrect.	Refer to the instructions supplied with the barcode reader.
Barcode reader does not read a multi-field barcode correctly. The information is not populated correctly to the fields in the Admit menu.	The parser configuration is incorrect.	Configure the barcode settings.
	The parser configuration is incompatible: field lengths, field types, delimiters, symbologies etc.	Check the barcode information content and compare it to the current parser configuration.

Troubleshooting audible alarms and speaker

Problem	Possible cause	Recommended action
Audible alarms do not work.	Audible alarms are turned off.	Enable audible alarms: select Alarm setup > Audible & Visual > Activate All Audible Alarms > Close .
	Alarm volume is too low.	Adjust alarm volume: select Monitor Setup > Sound Volumes .
No audible alarms from CPU unit speaker. Display speakers work normally.	Defective CPU speaker.	Replace the CPU speaker assembly.
The display gives a continuous beeping alarm and the alarm light is flashing yellow.	Power failure alarm is activated. The power failure alarm is activated if one of the following cases occurs during an active patient case : <ul style="list-style-type: none"> • Display or CPU unit is turned to standby or off position. 	<ul style="list-style-type: none"> • The power failure alarm remains active for as long as there is some residual power left, or until it is silenced with the Trim Knob or standby button, or until the USB cable is reconnected, or the supply mains is restored. • If the power failure alarm was activated due to a technical problem, find out the root cause and fix the problem.

Problem	Possible cause	Recommended action
	<ul style="list-style-type: none"> Display or CPU unit power is lost, or monitor is rebooting. USB communication failure due to a USB cable disconnection. USB communication failure due to a technical problem. 	

Troubleshooting incorrect system time

Problem	Possible cause	Recommended action
System time is incorrect when monitor is not connected to network.	CPU battery is empty.	<ol style="list-style-type: none"> Replace CPU battery. Set date and time. Restart the monitor.
	Time is not configured properly.	Configure date and time.
System time is incorrect when monitor is connected to network.	Network device time synchronization error.	<p>When a new device connects to the CARESCAPE Network, the existing devices on the CARESCAPE Network may synchronize to the new device's time. To prevent potential time synchronization issues, set the new device's time to be as close as possible to the time (within one minute or less) used by the existing GE devices on the CARESCAPE Network.</p>

Troubleshooting license issues

Problem	Possible cause	Recommended action
Unable to activate a new monitor (host) software.	<ol style="list-style-type: none"> You are trying to upgrade the monitor software without a valid activation code. You have entered an invalid activation code. 	<ol style="list-style-type: none"> Contact GE Healthcare to get the activation code for the base license. Provide the following information: <ul style="list-style-type: none"> serial number of the monitor current software version software version to be activated Check that the activation code is correct. The activation code is tied to the serial number of the monitor and to the software version to be activated. Software activation is not possible if the activation code is not entered or is invalid. Contact GE Healthcare for more information.
Unable to perform a function, or a feature is not available.	<ul style="list-style-type: none"> A license has not been purchased for the feature. The trial license has expired for the feature. 	See License management chapter.

Problem	Possible cause	Recommended action
	<ul style="list-style-type: none"> The license is not installed properly. 	
Unable to view a certain feature although the license is enabled.	<p>The software package in use does not include the feature in question. For example, Anesthetic agent measurement is not supported by ICU software package.</p>	<ol style="list-style-type: none"> Log in to the service interface. Select Configuration > Licenses > Software Package. Select the correct option and select Save.
Unable to upload a license file.	<ul style="list-style-type: none"> The license file is corrupted. The license file is for a monitor with a different serial number. 	<p>Log in to the service interface. Select Configuration > Licenses.</p> <ul style="list-style-type: none"> If you have printed license information, select Software Package and Host License. If you have a license file, select Upload License.
A wrong software package is in use. (The active software package is displayed on the screen during monitor startup.)	A wrong software package is activated for the device.	<ol style="list-style-type: none"> To view the software package that is currently activated, log in to the service interface. Select Configuration > Licenses > Host License. Make sure that the desired software package is displayed in Currently Active Software Package. If you need to activate a different software package, select Configuration > Licenses > Software Package. Select the correct option and select Save.

Troubleshooting MC Network issues

Problem	Possible cause	Recommended action
There is no MC network traffic.	Incorrect configuration.	Reconfigure the monitor with correct IP address and Netmask.
	The monitor has detected MC network traffic overload, and has disabled network traffic through the MC port.	If the Service Monitor Error Code 0xHOST1008 message is displayed on the monitor screen, contact the hospital IT to resolve the MC traffic overload.
	<p>The MC network port at the installation site has IEEE 802.1X port based authentication enabled, but the monitor is incorrectly configured:</p> <ol style="list-style-type: none"> The authentication has not been enabled on the monitor. Authentication is enabled, but either Identity and/or Password are incorrect, or have expired. If Call service. Wired MC/IX certificate expired message is shown, the CA certificate has expired. 	<ol style="list-style-type: none"> Enable 802.1X authentication on the monitor. Enter correct Identity and Password Contact hospital IT to update the wired MC/IX certificate in the monitor. <p>For detailed instructions, see Wired network configuration chapter.</p>

Troubleshooting IX Network issues

Problem	Possible cause	Recommended action
There is no IX network traffic.	Incorrect configuration. The cable connections do not match the selected network type (dual wire or single wire).	Reconfigure the monitor with correct IP address, Netmask, Gateway and/or DNS server. Verify the selected network type at the installation site and check the cable connections of the monitor: <ul style="list-style-type: none">• In the dual wire configuration, separate Ethernet cables must be connected to the MC and IX connectors of the monitor.• In the single wire configuration, one Ethernet cable must be connected to the MC/IX connector. Connect the cable(s) according to the selected network type or change the network type.
	The monitor has detected IX network traffic overload, and has disabled network traffic through the IX port.	If the Service Monitor Error Code 0xHOST1008 message is displayed on the monitor screen, contact the hospital IT to resolve the IX traffic overload.
	The IX network port at the installation site has IEEE 802.1X port based authentication enabled, but the monitor is incorrectly configured: <ol style="list-style-type: none">1. The authentication has not been enabled on the monitor.2. Authentication is enabled, but either Identity and/or Password are incorrect, or have expired.3. If Call service. Wired MC/IX certificate expired message is shown, the CA certificate has expired.	1. Enable 802.1X authentication on the monitor. 2. Enter correct Identity and Password . 3. Contact hospital IT to update the wired MC/IX certificate in the monitor. For detailed instructions, see Wired network configuration chapter.
Unable to retrieve MUSE 12SL reports to the monitor from the MUSE server.	1. Incorrect MUSE server user name or password. 2. Incorrect MUSE server address. 3. MUSE license not installed. 4. MUSE certificate is not installed or valid.	1. Enter correct MUSE user name and password. 2. Enter correct MUSE server address. 3. Install a valid MUSE license. 4. Install a valid MUSE certificate bundle.

Recorder troubleshooting

Problem	Possible cause	Recommended action
Recorder is printing but nothing appears on the paper.	Paper installed upsidedown.	Turn the paper roll over. To test which side is active: place the paper on a hard surface and draw a line with a fingernail - a dark line will appear on the active (thermal) side.
Recorder does not work.	Printing location is not configured correctly.	Check the configuration: Monitor Setup > Main Setup > Printing >Devices >Setup .
	The cable between the recorder and CPU unit is loose or defective, or connected to a wrong connector.	<ul style="list-style-type: none"> • Check the recorder cable connection • Replace the cable if it is defective.

For more information about the recorder problems, see PRN 50-M+ Digital Writer Technical Manual delivered with the recorder.

Troubleshooting acquisition platform

Acquisition platform refers to CARESCAPE ONE, CARESCAPE Dock F0, and CARESCAPE parameters.

To troubleshoot host monitor issues with the acquisition platform, check first if the CARESCAPE ONE works correctly as a standalone monitor, when disconnected from the host monitor:

1. Disconnect the CARESCAPE Dock F0 from the host monitor.
2. Check if the CARESCAPE ONE works normally:

Yes	Continue troubleshooting in step 3.
No	Refer to CARESCAPE ONE Service Manual for more troubleshooting instructions.

3. Check the following possible causes:

Possible cause	Recommended action
PDM and CARESCAPE ONE were connected simultaneously.	Remove PDM and reconnect CARESCAPE Dock F0 after five seconds.
Some CARESCAPE parameters are not shown on the host monitor screen due to configuration issue.	Configure the measured parameters to the host monitor screen with adequate priority.
Loose or defective cable between CARESCAPE Dock F0 and host monitor CPU unit.	Check that the cable is intact and properly connected. Replace if necessary.

Possible cause	Recommended action
Defective CARESCAPE Dock F0.	Refer to CARESCAPE ONE Service Manual for troubleshooting instructions. If available, try another CARESCAPE Dock F0 to confirm the case.
Defective CPU assembly in the host monitor.	Check if the acquisition platform works correctly when connected to another host monitor. If it does, and there is no other evident reason for the problem, the problem is most likely in the host monitor CPU assembly.

Troubleshooting PDM when connected to the ePort

PDM does not work correctly when it is connected with an ePort pod to host cable to an ePort connector in the host monitor.

Possible cause	Recommended action
Compatibility issue.	Check the compatibility of the connected module, the software, and the accessories. For a list of the compatible devices, see the supplemental information manual. For a list of the compatible supplies and accessories, see the Supplies and Accessories Supplemental.
PDM and CARESCAPE ONE connected simultaneously.	Remove the module that has been most recently connected. You can also remove both modules and reconnect the new module after five seconds. NOTE PDM and CS ONE are considered identical and should not be used simultaneously in the same monitoring system. However CARESCAPE Dock F0 without CS ONE and PDM can be simultaneously connected.
Configuration issue.	Check that the measured parameters are configured to the monitor screen with adequate priority.
Missing licenses.	The cardiac output license from the PDM requires a C.O. license installed on the monitor. Invasive pressure measurement from the PDM requires a PDM license (1-4 channels) installed on the PDM module.
The ePort pod to host cable is loose or defective.	Check that the cable is intact and properly connected. Replace the cable, if defective.
Defective PDM or accessories.	Try to connect another, correctly working PDM with its own accessories to the ePort connector. If the other PDM works correctly, the original PDM, or one of its accessories, is likely to be defective. Refer to CARESCAPE PDM Service Manual for further troubleshooting instructions.
Defective CPU assembly.	Try to connect another, correctly working PDM with its own accessories to the ePort connector. If the other PDM does not work either, and there is no other evident reason for the problem, the host CPU assembly may be defective. Replace the CPU assembly.

Troubleshooting E-module or PDM when connected to a frame

E-module or PDM does not work correctly when connected to the CPU unit using F5 or F7 Frame.

Possible cause	Recommended action
Identical modules connected simultaneously.	Remove the identical modules. Refer to the monitor's user manual for more information. PDM and CS ONE are considered identical and should not be used simultaneously in the same monitoring system.
Configuration issue	Configure the measured parameters to the monitor screen with adequate priority.
Compatibility issue.	Check the compatibility of the connected module and the accessories. For a list of the compatible devices, see the supplemental information manual. For a list of the compatible supplies and accessories, see the Supplies and Accessories Supplemental.
The Frame-CPU cable is loose or defective.	Check that the cable is intact and properly connected. Replace the cable, if defective.
Defective E-module slot in F5/F7 Frame.	Remove the E-module and reconnect it to another module slot. If the module now works correctly, the original module slot is defective. Refer to F5/F7 Frame Service Manual for more troubleshooting information.
Defective acquisition module.	Connect another similar, correctly working PDM/E-Module with its own accessories to the F5/F7 Frame. If the other module works correctly, the original module or the accessories are defective. Refer to the related module service manual for more troubleshooting instructions.
Defective F5/F7 Frame.	Try to replace the suspected F5/F7 Frame with another, correctly working F5/F7 Frame. Use the original modules. If the modules now work correctly, the original F5/F7 Frame is most likely defective. Refer to F5/F7 Frame Service Manual for more troubleshooting information.
Defective CPU assembly.	Try to connect another similar, correctly working PDM/E-Module with its own accessories to the F5/F7 Frame. If the other module does not work either, and no other evident reason for the problem exists, the host CPU assembly may be defective. Replace CPU assembly.

Troubleshooting CARESCAPE Network communication

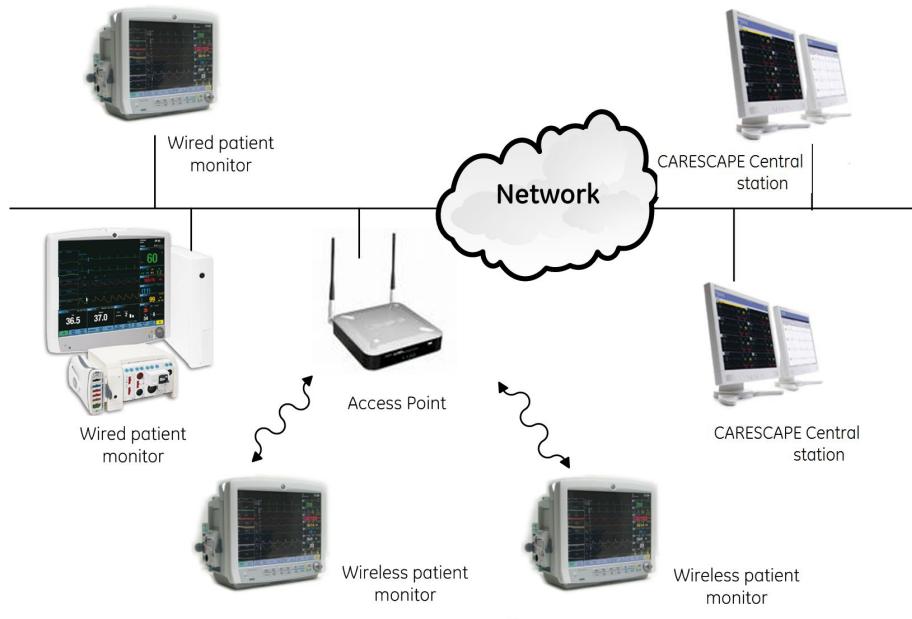
Traffic types

Two main types of communication occurs in the CARESCAPE Network: Broadcast and Unicast.

- Broadcast traffic is sent from one device to all devices on the network. Examples of CARESCAPE broadcast traffic are device discovery, alarms, and time synchronization.
- Unicast traffic is sent from one device to another specific device on the network. An example of CARESCAPE unicast traffic is patient waveforms.

Flow

- Upstream broadcast: The monitor sends broadcasts to other network devices.
- Downstream broadcast: The monitor receives broadcasts from other network devices.

**Types:**

- Broadcasts (discovery, alarms, time)
- Unicasts (waveforms, ping)

Mediums:

- Wired
- Wireless

Flow:

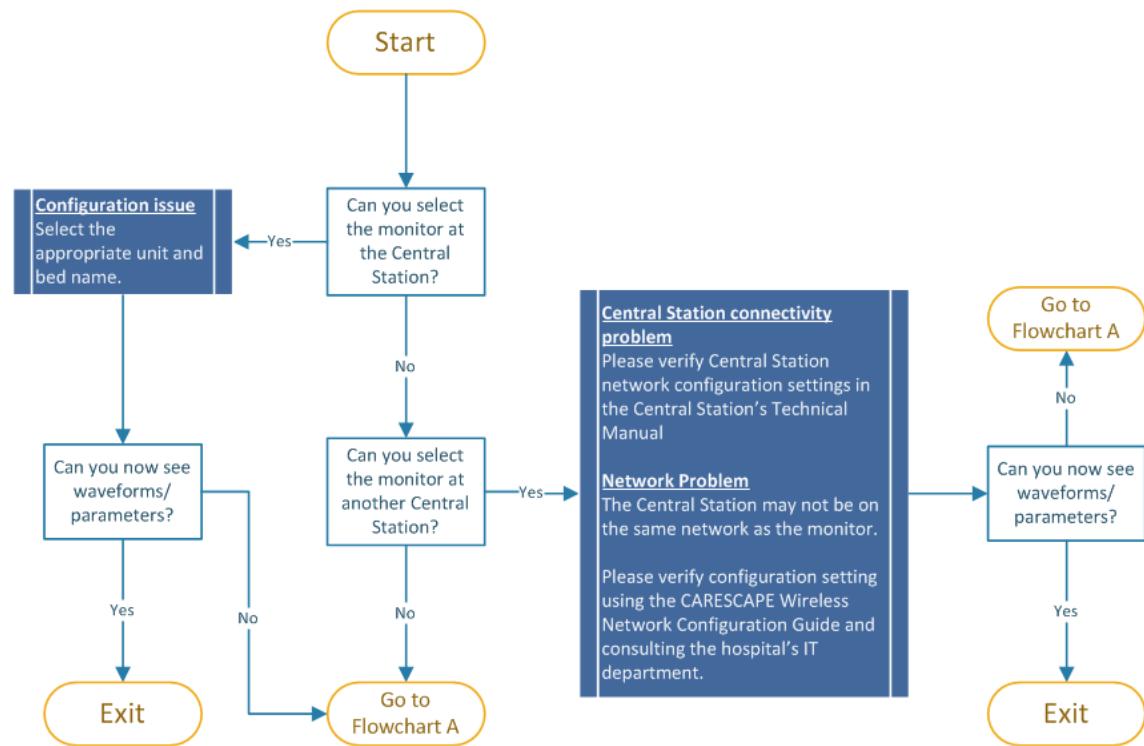
- Upstream Broadcast
- Downstream Broadcast
- Bi-Directional Unicast

Combinations:

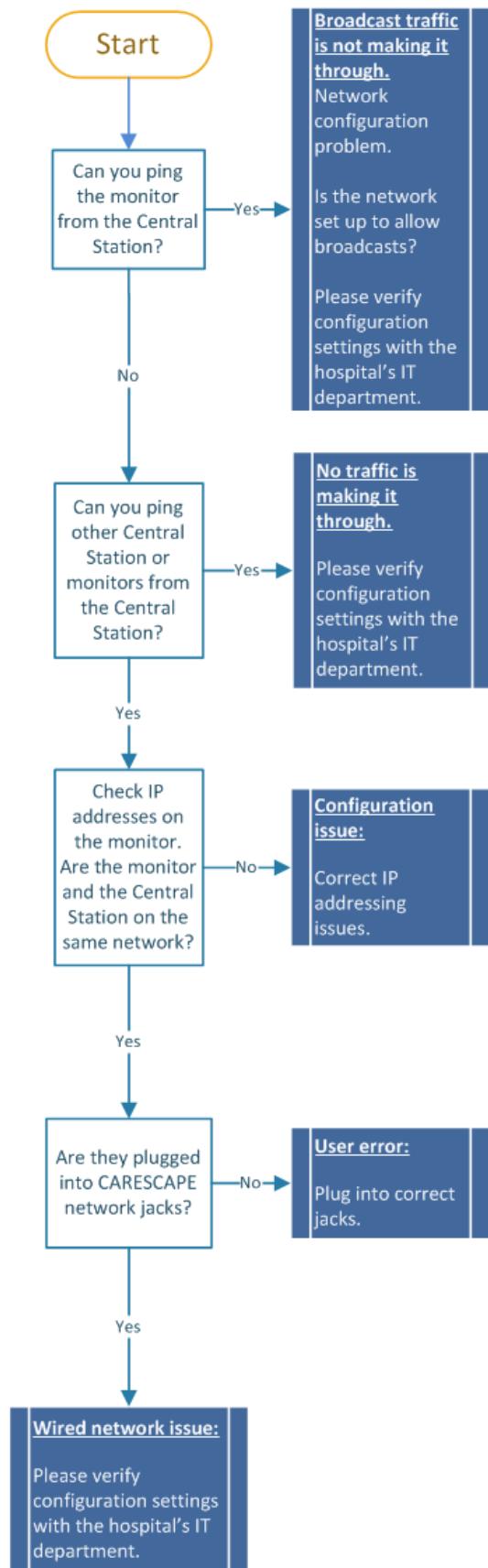
- Wired Broadcast
- Wired Unicast
- Wireless Broadcast
- Wireless Unicast

Waveform or parameter data missing at the CARESCAPE Central Station

Network troubleshooting flowchart



Network troubleshooting flowchart A



Troubleshooting

11

Disassembly and reassembly

Disassembly guidelines

Field repair of the device is limited to replacing field replaceable units (FRUs).

NOTE Only qualified service personnel should perform field replacement procedures.

NOTE Perform the specified corrective maintenance check after any corrective maintenance to the product.

ESD precautions

All external connectors of the device are designed with protection from ESD damage. However, if the device requires service, exposed components and assemblies inside are susceptible to ESD damage. This includes human hands, non-ESD protected work stations or improperly grounded test equipment. The following guidelines may not guarantee a 100% static-free workstation, but can greatly reduce the potential for failure of any electronic assemblies being serviced:

- Discharge any static charge you may have built up before handling semiconductors or assemblies containing semiconductors.
- Wear a grounded, antistatic wristband or heel strap at all times while handling or repairing assemblies containing semiconductors.
- Use properly grounded test equipment.
- Use a static-free work surface while handling or working on assemblies containing semiconductors.
- Do not remove semiconductors or assemblies containing semiconductors from antistatic containers until absolutely necessary.
- Do not slide semiconductors or electrical/electronic assemblies across any surface.
- Do not touch semiconductor leads unless absolutely necessary.
- Store the semiconductors and electronic assemblies only in antistatic bags or boxes.
- Handle all PCB assemblies by their edges.
- Do not flex or twist a circuit board.

Reassembly precautions

Pay attention to the following generic precautions when reassembling the monitor:

- Note the positions of any wires, cables or connectors. Mark them if necessary to ensure that they are reassembled correctly.
- Save and set aside all hardware for reassembly.
- GE recommends using the new fasteners (screws, washers, etc.) provided in the FRU kits rather than reusing the old fasteners. Some fasteners are not intended to be re-used.

When you fasten the screws:

- Visually ensure that the screws are properly attached.
- Do not use too much force, as this may damage the existing thread patterns.
- The maximum recommended torque value for each screw and nut is listed in brackets after each disassembly step.
- If you use a battery-operated tool, ensure that it is equipped with torque limiter and the torque is properly adjusted.
- Use only new screws for the light metal parts. Before fastening a screw, turn it counterclockwise until it drops into an existing thread pattern.

Required tools

NOTE Use torque wrench and torque screwdriver to comply with the given torques.

- Torx screwdriver, size T10
- cross head screwdrivers; Ph1 and Ph2
- a flat blade screwdriver; width 2.5 mm /0.1 in
- small flat blade pliers
- a nut driver or a wrench; size 5 mm
- an antistatic ESD wristband

Preparing for disassembly

WARNING ELECTRIC SHOCK – Always disconnect the device from the power line before you start the disassembly.

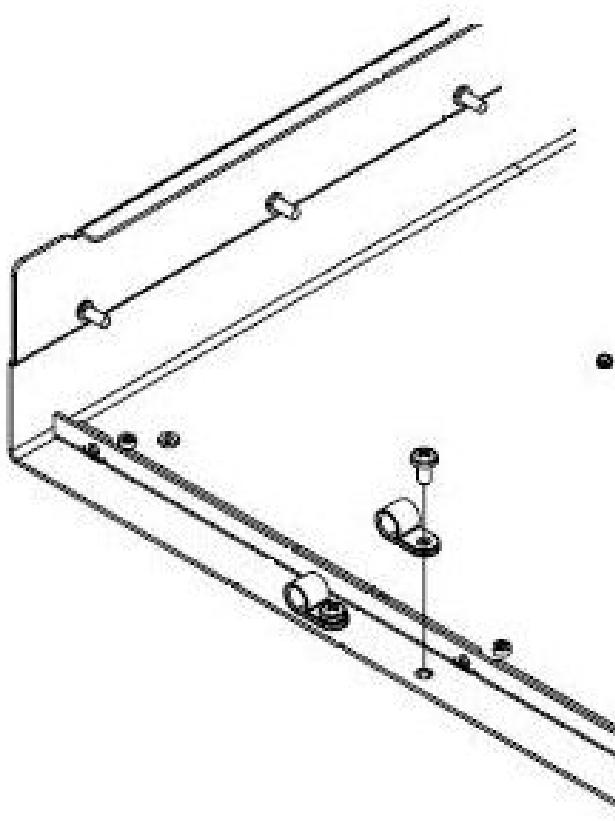
WARNING DISCONNECTION FROM MAINS. When disconnecting the device from the power line, remove the plug from the wall outlet first. Then you may disconnect the power cord from the device. If you do not observe this sequence, there is a risk of coming into contact with line voltage by inserting metal objects, such as the pins of leadwires, into the sockets of the power cord by mistake.

WARNING SAFETY GROUND. Remove power cord from the mains source by grasping the plug. Do not pull on the cable.

WARNING ELECTRIC SHOCK. Always unplug the grounded data cables when not in use. Leaving them connected could result in an electric shock from the ground contact in the other end.

1. Turn off the power:
 - a. Press the on/standby button located on the front panel of the processing unit. Press the button a second time when a message prompts you to do so.
 - b. Press the power on/off switch located on the back of the processing unit to the 0 (off) position.
 - c. To turn off the display, keep the power button of the display pressed for 1 second.
2. Detach the retaining clips for the power cord and USB cables.

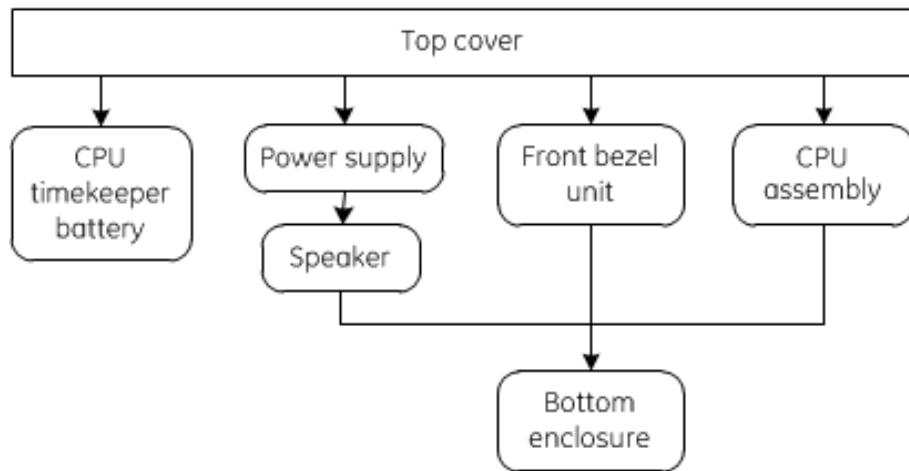
NOTE: Remember to reattach the retaining clips for the power cord and USB cables after reassembly.



3. Disconnect all the interface cables from to the B850 processing unit.
4. Disconnect the power cable, first from the wall outlet and then from the monitor.
5. Disconnect /Remove all acquisition modules.
6. Detach the monitor from the mounting.

Disassembly procedures

Follow the arrows from top to down to identify the required disassembly procedure for each FRU. Perform the steps in the given order.



Detaching the top cover

Electrical safety tests must always be performed after the monitor is reassembled. For more information, refer to the corrective maintenance requirements in the Checkout procedures chapter.

1. Remove 8 (T10) screws, 4 screws on each side of the top cover. Torque [1.1 Nm]



2. Remove the top cover.
3. Reassemble in reverse order.

Perform the maintenance check procedure after you have reassembled the patient monitor.

Replacing the CPU battery

Disassemble first:

1. The top cover. See the Detaching the top cover section.

To remove the CPU battery:

1. Remove the lithium ion battery from the bracket on the CPU assembly.



2. Replace the battery. Place the new battery in the bracket the positive (+) side facing up.
3. Reassemble in reverse order.

Once the battery is replaced, the system time is reset to the factory default. You must re-configure time and date before you connect the monitor to the network. For instructions on configuring the time, see the Configuring date and time section.

Detaching the power supply unit

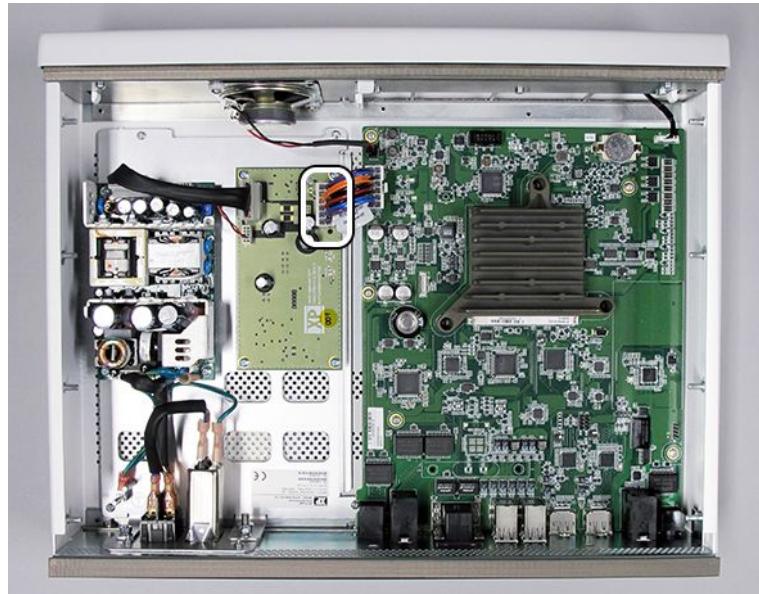
Disassemble first:

1. The top cover. See [Detaching the top cover \(190\)](#).

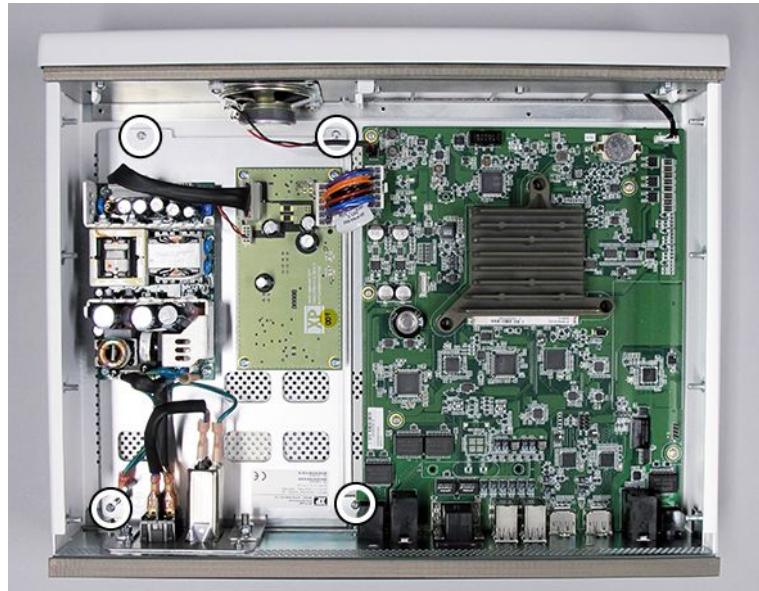
To remove the power supply unit:

Disassembly and reassembly

1. Disconnect the power supply cable from the power supply unit.



2. Remove the 4 (Ph2) screws that attach the power supply unit to the bottom enclosure. Torque [1.1 Nm].



3. Remove the 2 (Ph1) screws that attach the power supply unit to the rear panel. Torque [1.1 Nm].



4. Detach the power supply unit. Be careful not to damage the speaker cable.



The power supply unit FRU contains:

- the power supply unit
- the power cable
- 4 (Ph2) mounting screws
- 2 (Ph1) mounting screws

5. Reassemble in reverse order.

Detaching the speaker

Disassemble first:

1. The top cover. See the Detaching the top cover section.
2. The power supply unit. See the Detaching the power supply unit section.

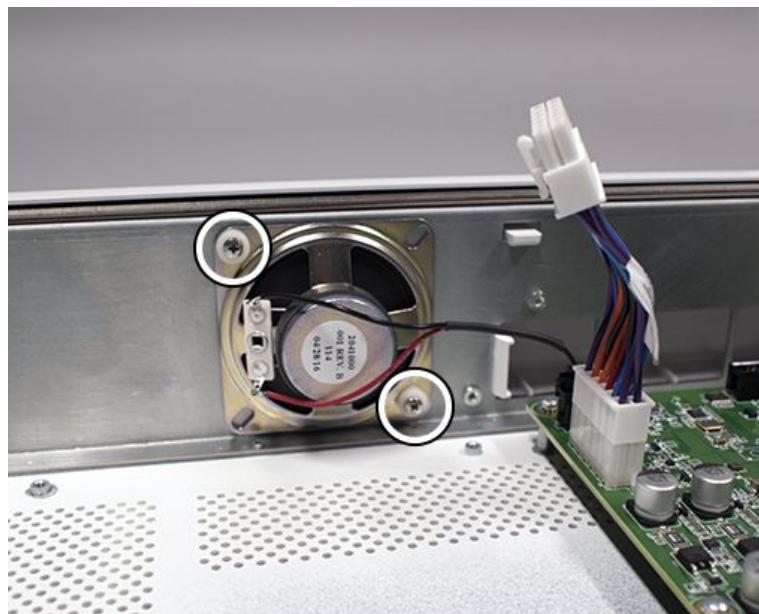
To remove the speaker:

Disassembly and reassembly

1. Disconnect the speaker cable from the CPU assembly.



2. Remove the 2 (Ph1) screws with the nylon spacers and the washers, that hold the speaker to the bottom enclosure. Torque [1.1 Nm]



3. Detach the speaker.



The Speaker assembly FRU contains:

- the speaker with the cable
 - 2 (Ph1) mounting screws
 - 2 nylon washers
 - 2 nylon spacers
4. Reassemble in reverse order.
 - Make sure you attach the screws, the spacers and the washers in the correct order. See the picture above.

Detaching the front bezel unit

Disassemble first:

1. The top cover. See the Detaching the top cover section.

To remove the speaker:

1. Disconnect the On/standby button cable from the CPU assembly.



Disassembly and reassembly

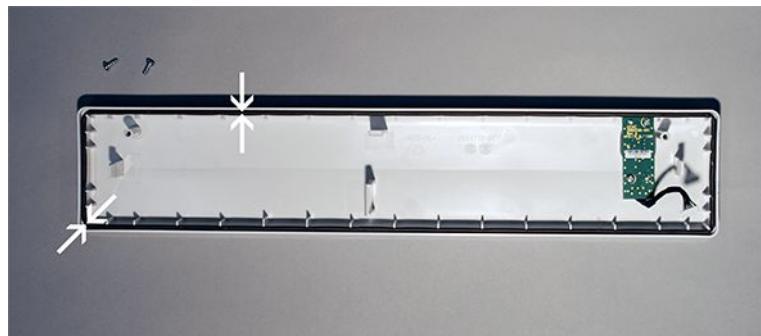
2. Remove the 2 (Ph1) screws that attach the front bezel unit to the bottom enclosure. Torque [1.1 Nm].



3. Release the 4 snaps that attach the front bezel to the bottom enclosure.



4. Detach the front bezel.



The front bezel FRU contains:

- Front bezel assembly with On/standby button and cable.
- Labeled front panel
- Front panel gasket
- Two (Ph1) screws to mount the front bezel unit.

5. Reassemble in reverse order.

- Make sure the gasket is securely in place in the groove.

Detaching the CPU assembly

NOTE

The monitor software and all the settings will be lost when you replace the CPU assembly.

Contact your local GE representative to order the monitor software. Provide the original monitor software version and the serial number of the monitor to ensure that you will get the correct software. Check the serial number of the device from the serial number label attached to the device.

Disassemble first:

1. The top cover. See the Detaching the top cover section.

To remove the CPU assembly:

1. Disconnect the following cables from the CPU assembly:
 - a. The power supply cable.
 - b. The speaker cable.
 - c. The On/standby button cable.



2. Remove the 4 jackscrews (5 mm) around the ePorts. Torque [0.6 Nm].

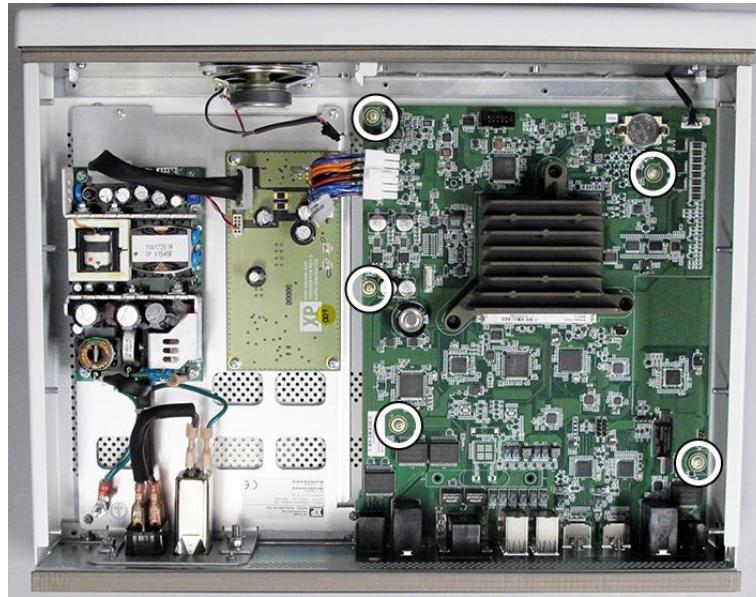


3. Remove the 2 (Ph1) screws above the DisplayPort connectors. Torque [0.6 Nm].

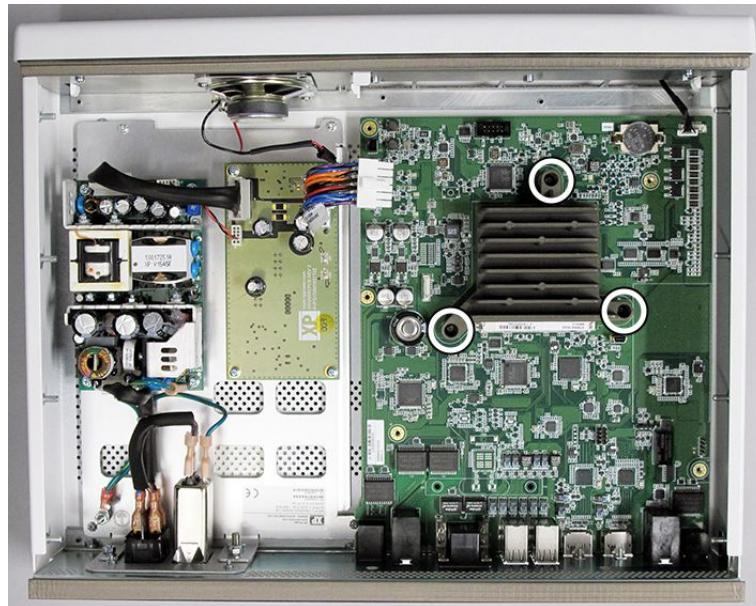


Disassembly and reassembly

4. Remove the 5 (Ph1) combo screws that attach the CPU assembly to the bottom enclosure. Torque [1.1 Nm].



5. Remove the 3 (Ph1) combo screws that attach the heat sink to the CPU assembly and to the bottom enclosure. Torque [1.1 Nm].



6. Carefully detach the CPU assembly from the bottom enclosure.



The CPU assembly FRU contains:

- The CPU assembly includes the CPU carrier board, the CPU module, and the CPU battery attached. It does not include the monitor software.
 - The power supply cable.
 - The heat sink with the thermal pads and the protective film.
 - 10 (Ph1) mounting screws.
 - 4 jackscrews.
7. To reassemble the CPU assembly:
 - a. Attach the CPU carrier board to the bottom enclosure and fasten it with the 5 (Ph1) screws. Torque [1.1 Nm].

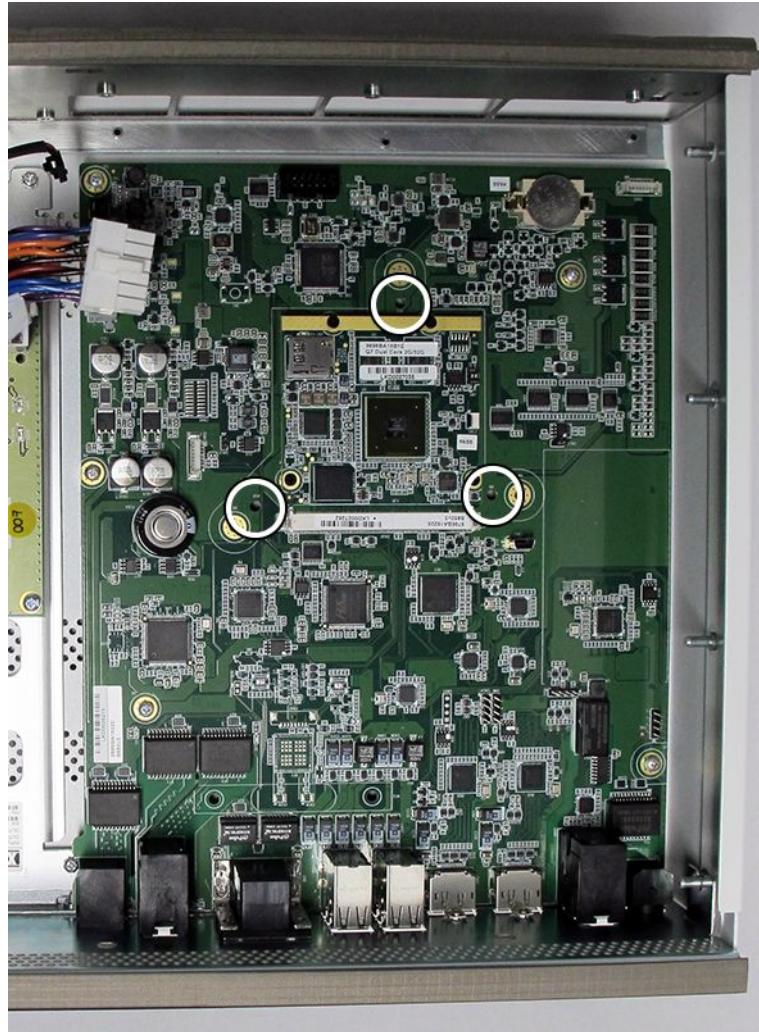
Disassembly and reassembly



- b. Carefully remove the protective film from the thermal pads of the heat sink.
- c. Check that all the thermal pads are properly in place on top of each heat sink boss.

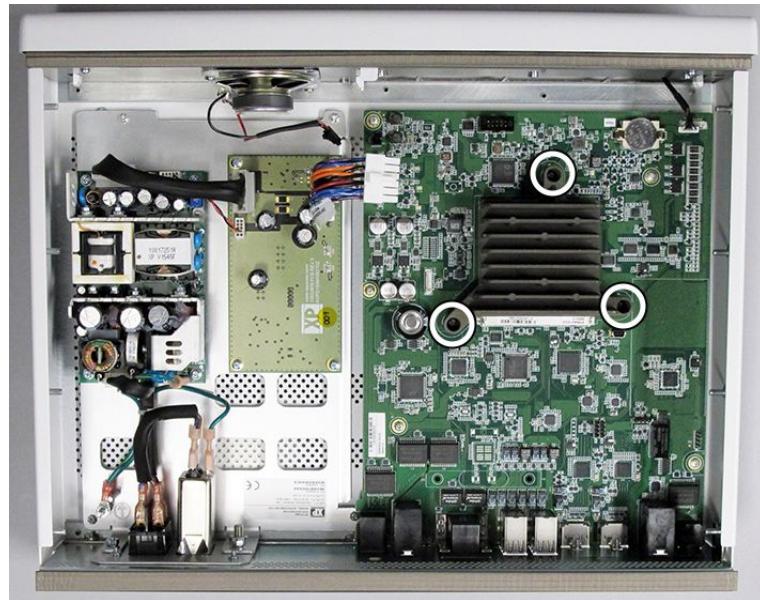


- d. Attach the heat sink on top of the CPU module and align the guiding pins to the holes in the CPU carrier board.



- e. Attach the 3 (Ph1) screws to fasten the heat sink and the CPU assembly to the bottom enclosure. Torque [1.1 Nm].

Disassembly and reassembly



8. Fasten the 2 (Ph1) screws above the DisplayPort connectors. Torque [0.6 Nm].



9. Fasten the 4 jackscrews (5 mm) around the ePorts. Torque [0.6 Nm].



10. Connect the cables to the CPU assembly:

- a. The power supply cable.
- b. The speaker cable.
- c. The On/standby button cable.



11. Reattach the top cover. See the Detaching the top cover section.

After the reassembly:

1. Reload the software and the settings. See the [Reloading software and settings](#) section.
2. The MAC addresses for the network interfaces are changed when CPU assembly is replaced. To ensure network connectivity is maintained when network access controls are in place, inform the hospital IT/ Biomed of the new MC and IX MAC addresses.

Reloading software and settings

The monitor software and all the settings (including passwords) will be lost when the CPU assembly is replaced with the CPU assembly FRU. The CPU assembly FRU is shipped with a special FRU software pre-installed. Replace this FRU software with the CARESCAPE software, and then reload the original settings.

Contact your local GE representative to order the CARESCAPE software (host software). Provide the original monitor software version and the serial number of the monitor to ensure that you get the correct software.

Perform the following tasks after replacing the CPU assembly with the CPU assembly FRU:

1. Turn on the monitor.

The monitor starts up with the special FRU software, showing the text **Field Replacement Unit** and the FRU software version, IP address, and MC MAC address of the monitor.

2. Log in to the service interface locally with a service PC. Use **biomed** user account with **Change Me** password. Follow the instructions in the [Accessing the service interface locally with a service PC](#) section.
3. Upload the host software. Use the software file that is named as "CSP_3.2.X.cas-unsigned.csmon", where X is the software build you need. Follow the instructions in the [Uploading software](#) section.
4. Activate the uploaded host software. Follow the instructions in the [Activating the host software](#) section.
5. Enter the original serial number of the monitor. Follow the instructions in the [Configuring serial number](#) section.

6. Restore the clinical and the platform settings, including licenses and original passwords:
 - If you have a recent backup file of the settings available for this specific monitor, restore the original clinical and platform settings from the backup file. The backup file includes also the passwords, and all unique platform settings like IP addresses and licenses. For details, see the Restoring a backup section.
 - If you do not have a monitor specific backup file available:
 1. Contact your local GE representative and provide the original serial number of the monitor to get the original license file for the monitor. For instructions on uploading the license file, see the Uploading license file section.
 2. Transfer the other clinical and platform settings from another monitor. For details, see Settings management section. Note that some platform settings are unique to each monitor and need to be configured manually. Ensure that the monitor has correct passwords for all user accounts.
7. Perform a complete checkout procedure for the monitor. Follow the instructions in the Checkout procedures chapter.

Replacing the bottom enclosure

Disassemble first:

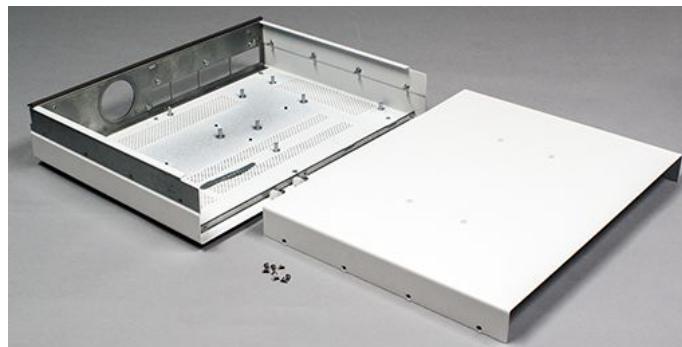
1. The top cover. See the Detaching the top cover section.
2. The power supply unit. See the Detaching the power supply unit section.
3. The speaker. See the Detaching the speaker section.
4. The CPU assembly. See the Detaching the CPU assembly section.
5. The front bezel unit. See the Detaching the front bezel unit section.

To remove the bottom enclosure:

1. Remove the 3 (Ph1) screws that attach the rear panel unit to the bottom enclosure [Torque 1.1 Nm].



2. Detach the rear panel unit.
 - Be careful not to damage the EMI shields on top of the rear panel and the front panel.



3. Replace the bottom enclosure.
4. Reassemble in reverse order.
 - Be careful to attach EMI shield correctly

Disassembly and reassembly

12

Service parts

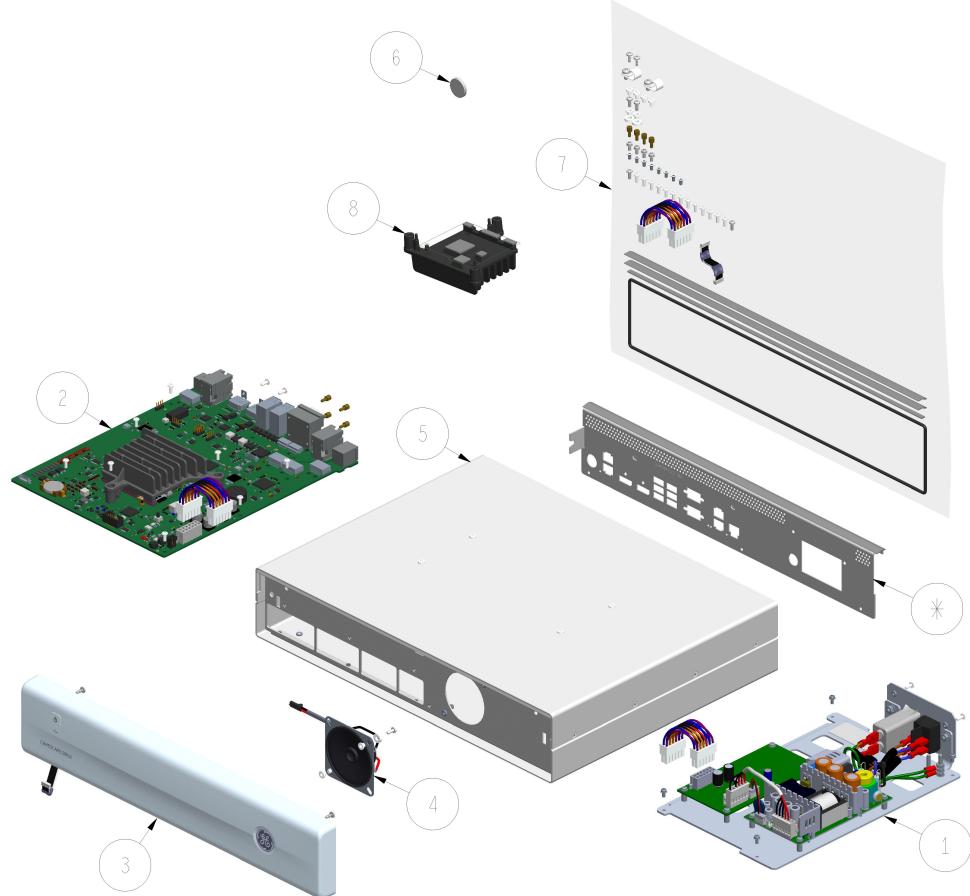
Service parts

Perform the specified corrective maintenance check after any corrective maintenance to the product.

Ordering parts

To order parts, contact your local GE representative. Contact information is available at www.gehealthcare.com. To make sure you get the correct service part, provide the device type and the serial number information.

Exploded view



List of FRUs

Item	Part number	Description
1	2067715-016	<p>FRU, Power supply unit, B850:</p> <ul style="list-style-type: none"> • B850 AC/DC power unit. • The power supply cable that connects to the CPU carrier board. • 4 (Ph2) M3x6 screws with lockwashers to mount the unit to the bottom enclosure. • 2 (Ph1) M3x8 screws with lockwashers screws to mount the unit to the rear panel.
2	2067715-017	<p>FRU, CPU assembly, B850:</p> <ul style="list-style-type: none"> • CPU assembly without the heat sink, including the CPU battery. • CPU heat sink with the thermal pads. • Power supply cable that connects to the power board.

Item	Part number	Description
		<ul style="list-style-type: none"> • 8 (Ph1) M3x8 screws with lockwashers to mount the assembly and the heat sink to the bottom enclosure. • 4 jackscrews + 2 (Ph1) M3x8 screws with lockwashers to mount the assembly to the rear panel. <p>NOTE The monitor software will be lost when the CPU assembly is replaced. Contact your local GE representative to order the monitor software. Provide the original monitor software version and the serial number of the monitor to ensure that you will get the correct software.</p>
3	2067715-018	FRU, Front bezel unit, B850: <ul style="list-style-type: none"> • Front panel assembly with: <ul style="list-style-type: none"> ▪ The On/standby button. ▪ On/Standby switch board ▪ The On/standby cable. ▪ The front panel gasket. • 2 (Ph1) PT 3.5x8 screws to mount the front bezel unit.
4	2021440-005	FRU, CARESCAPE CPU C1 Speaker assembly: <ul style="list-style-type: none"> • The speaker with the cable. • 2 (Ph1) M3x8 mounting screws with threadlocker for the speaker. • 2 nylon washers. • 2 nylon spacers.
5	2067715-019	FRU, Enclosure kit, B850, contains the following parts assembled: <ul style="list-style-type: none"> • The top cover with four nylon screws. • The bottom enclosure with the EMI gaskets attached. • 2 cable clamps for the power cord and the USB cables. • 2 (Ph2) M4x6 mounting screws for the cable clamps. • 8 (white Torx 10 head) M3x6 countersink screws for the top cover.
6	2021440-008	FRU, CPU time keeper battery (20 pcs) <ul style="list-style-type: none"> • CR2032 lithium battery.

Service parts

Item	Part number	Description
7	2067715-021	<p>FRU, Hardware kit, B850:</p> <ul style="list-style-type: none"> • The On/ standby button cable. • The CPU power supply cable. • The front panel gasket. • 2+1 EMI gaskets. • 8 (white Torx 10 head) M3x6 countersink screws for the top cover. • 2 cable clamps for the power cord and the USB cables. • 2 (Ph2) M4x6 mounting screws for the cable clamps. • 4 nylon screws for the top cover. • 2 (Ph1) M3x8 mounting screws with threadlocker for the speaker. • 2 nylon washers for the speaker. • 2 nylon spacers for the speaker. • 2 (Ph1) PT 3.5x8 screws for the front bezel unit. • 4 (Ph2) M3x6 screws with lockwashers for the power supply unit. • 15 (Ph1) M3x8 screws with lockwashers for the rear cover, heat sink, and CPU carrier board. • 4 jackscrews for the e-Ports.
8	2067715-023	<p>FRU, Heat sink assembly, B850:</p> <ul style="list-style-type: none"> • CPU heat sink with the thermal pads.
<p>* The rear panel of the CPU contains the Serial Number and the UDI labels with unique device identification information. Contact your local GE representative, if you need to replace the rear panel.</p>		

A

Display D19KT VER01

Disassembly guidelines and precautions

Before you start, read the following general guidelines in the Disassembly and reassembly chapter and make sure you follow them:

- Disassembly guidelines
- ESD precautions
- Reassembly precautions
- Preparing for disassembly

Required tools

- flat blade screwdriver [5 mm]

Detaching the OSD knob

1. Turn the display power off at the rear power switch and disconnect all cables (USB, display and AC power).
2. Remove the **OSD Knob** by gently pulling the **OSD Knob**.



Detaching the trim knob

1. Turn the display power off at the rear power switch and disconnect all cables (USB, display and AC power).

2. Use a flat blade screwdriver to remove the main **Trim Knob**.



Detaching the alarm light cover

1. Turn the display power off at the rear power switch and disconnect all cables (USB, display and AC power).
2. Use a screwdriver to remove the alarm light cover.



Service parts

Ordering parts

To order parts, contact your local GE representative. Contact information is available at www.gehealthcare.com. Make sure you have all necessary information at hand.

List of FRUs

Part number	Description
2091940-001	Trim/OSD Knobs & Alarm Light Cover, D19KT

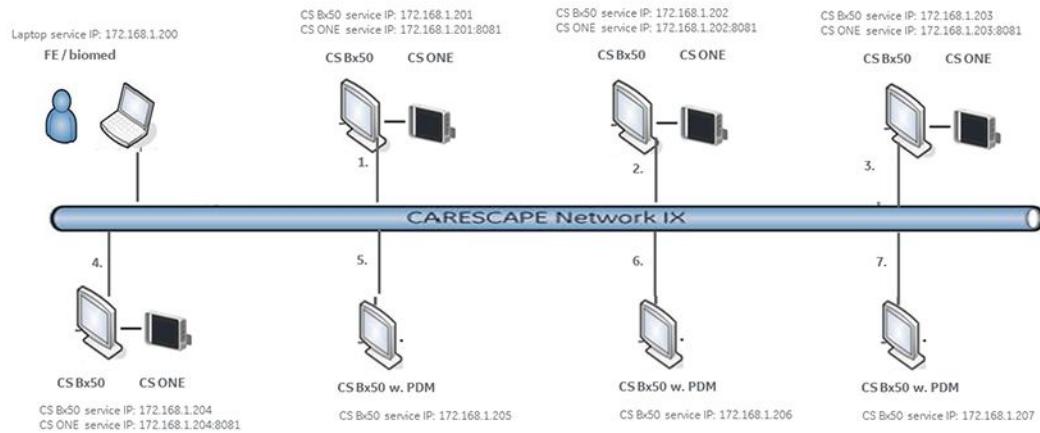
Contact GE if the display is faulty in any other way.

B

Multi Monitor Manager

Introduction to Multi Monitor Manager

CARESCAPE Multi Monitor Manager is a service application that allows you to install software and to transfer settings to multiple monitors at a time.



Prerequisites for using Multi Monitor Manager

You can use Multi Monitor Manager with the monitors that meet the following prerequisites:

1. Supported software versions:
 - At least one of the monitors, the one you use to access the Multi Monitor Manager application, must have CARESCAPE software version 3.2.
 - Software installation: All the other target monitors must have CARESCAPE software version 3.0 or later.
 - Settings transfer: The source monitor and all the target monitors must have CARESCAPE software version 3.2.
2. User authentication: User shall be able to authenticate to all the target monitors with the same username and password.
3. Device authentication: All the target monitors are able to authenticate themselves to the web browser on the service PC. Therefore, all the monitors must have a signed X.509 certificate issued by a publicly trusted certificate authority (CA). See Certificate management chapter for detailed instructions.

NOTE

If you use Multi Monitor Manager with monitors that have the self-signed certificate issued by GE, you will have to specify a browser specific security exception separately for each target monitor. For more information refer to the web browser's instructions.

Accessing Multi Monitor Manager

The Multi Monitor Manager application is hosted by a CARESCAPE monitor (web server) that is running CARESCAPE Software v3.2 (or later). To load the Multi Monitor Manager application to your service PC (web client), you must first connect the PC to a monitor that is running CARESCAPE Software v3.2 or later.

For details refer to the following chapters in Bx50 Service manual section 4 Using the service applications:

- Checking the network settings of the target monitor
- Configuring the network settings of the service PC
- Supported web browsers in service PC
- Secure access with service PC

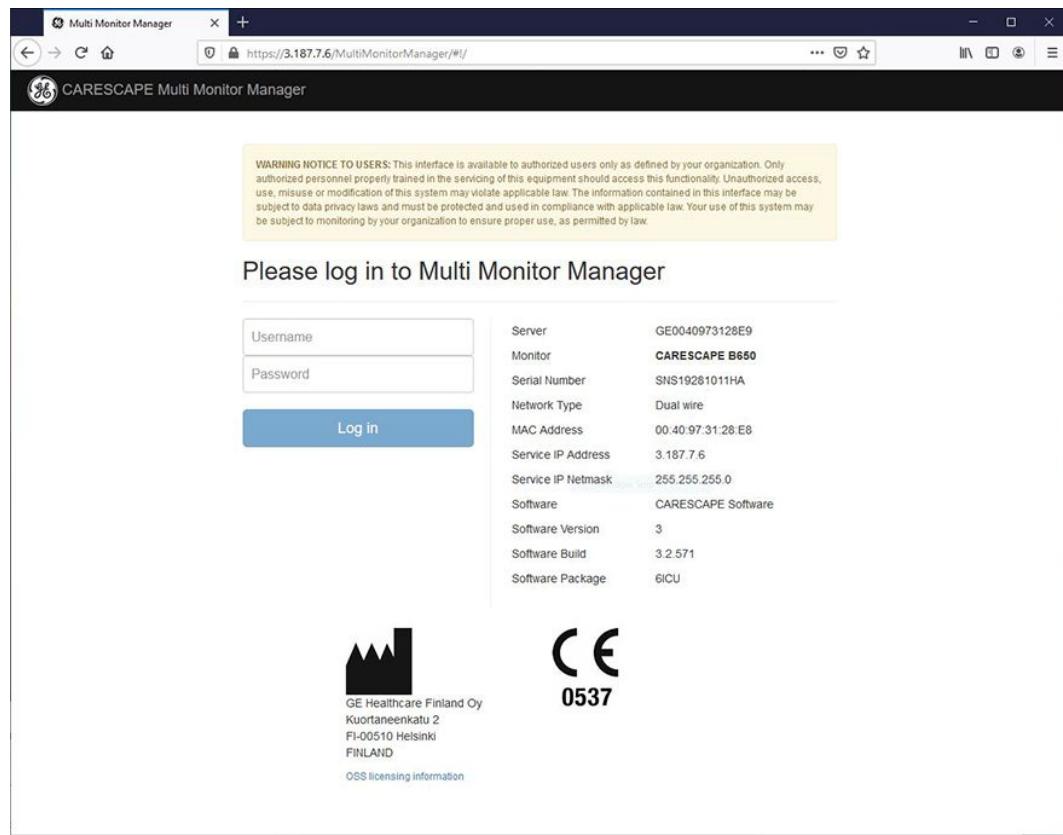
Tools needed:

- a service PC
 - Ethernet patch cable
1. Connect a service PC either to the IX wall connector (dual wire) or to the MC/IX wall connector (single wire) with an Ethernet patch cable.
 2. Configure the service PC to operate in the same subnetwork with the target monitors: **Service IP Address/ Netmask**.
 3. Open a web browser on the service PC.
 4. In the address field of the web browser, enter:
the service IP address of the monitor followed by the suffix:
"/MultiMonitorManager".

For example: <https://172.18.3.201/MultiMonitorManager>.

5. Press **Enter**.

The Multi Monitor Manager login screen opens:



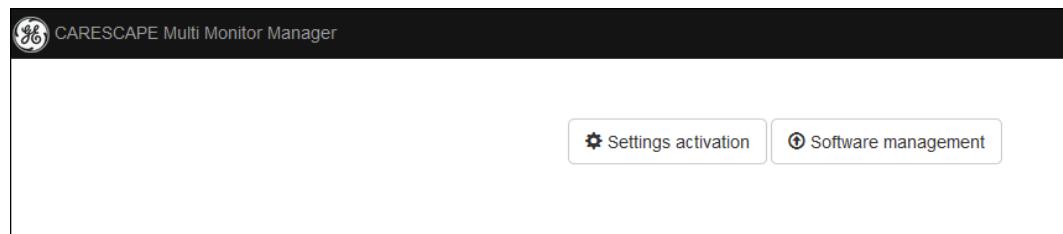
6. Enter the **username** and the **password** and select **Log in**.

NOTE

The user credentials (username and password) are the same as for accessing the service interface of the monitor.

7. Select the function:

- Select **Software management** to upload and/or activate a new software version to multiple monitors at a time.
- Select **Settings activation** to transfer a settings file and activate the new settings to multiple monitors at a time.



Software installation to multiple monitors at a time

You can install new software to multiple monitors at a time with the Software management utility.

Points to note:

- Software installation is possible only either to CARESCAPE Bx50 monitors or to CARESCAPE ONE acquisition devices at a time. In case you need to install software to both type of monitors, complete the activity first to the CARESCAPE Bx50 monitors, and after that to the CARESCAPE ONE acquisition devices.
- Software installation consists of two phases: the software upload and the software activation. You can either perform both phases during the same session, or you can perform the phases during separate sessions.
- Multi Monitor Manager can be used only for the CARESCAPE monitor software (host software) installation.
- Software updates: Multi Monitor Manager can be used both for the software upload and for the software activation.
- Software upgrades: Multi Monitor Manager can only be used for the software upload. Software activation must be completed one monitor at a time using CARESCAPE service interface. See the Activating the host software chapter for more information about the software upgrades and about entering the base license activation code.

Software signing

Software code for CARESCAPE Software v3.2 (host software) is signed with a digital signature by GE Healthcare. The purpose of code signing is to confirm the software author and to ensure that the software code has not been altered or corrupted since it was signed.

There are two software files for each software build:

1. If you are updating the monitor software from one v3.2 software build to another, upload the software file that is named as "CSP_3.2.X.cas.csmon".
2. If you are upgrading the monitor software from v3.0/ v3.1 to v3.2, or if you are reloading host software to the monitor after CPU replacement, upload the software file that is named as "CSP_3.2.X.cas-unsigned.csmon".

Specifying the target monitors

1. To specify all the target monitors to which you want to upload and/or activate a new software image, do one of the following:

- a. Select **load from file** to load the IP addresses from a file on your service PC.

NOTE

Prepare the file beforehand. The file must be a text file. IP addresses and/or host names must be separated with a line break.

- b. Enter the IP addresses or the host names of all the target monitors manually one per line to the **Monitor Addresses** field. Press **Enter** for a line break.

Connecting to the target monitors

1. Enter the **Username** and the **Password**.
2. Select **Contact Monitors** to log in and to authenticate to the target monitors.

The progress of the authentication process is updating on the screen.

3. Wait until the authentication process completes and the ***Operation summary*** appears on the screen:



4. Check the summary for possible issues and select ***Close***.
 5. Review the connection statuses of all the target monitors:

4 Monitor(s) contacted successfully. 3 Monitor(s) failed to contact. 7 total.						
Address	Monitor Type	Current Version	Serial Number	Uploaded Version	Note	Status
172.18.3.201	B650	3.2.551	SNS18170026HP		OK	
172.18.3.202	B450	3.1.376	SNT19281011HA		OK	
172.18.3.203	B450	3.1.376	SNT19360050HA		OK	
172.18.3.204	B450	3.1.376	SNT17421019HP		OK	
172.18.3.205	B450	3.1.376	SNT18231014HP		⚠ Authentication failed	
172.18.3.206					⚠ Invalid address or monitor is not reachable	
172.18.3.207					⚠ Invalid address or monitor is not reachable	

Address	The service IP Address of a monitor. Selecting the IP address will open a new browser tab to access the service interface of the monitor. You can use this link for troubleshooting purposes.
Monitor Type*	B450, B650, B850, or CS ONE. Mixing CS ONE and Bx50 to the same operation is prevented. In case there are both Bx50 monitors and CS ONE devices, the operation will only be performed on the Bx50 monitors. The CS ONE devices will be excluded from the operation.
Current Version*	The current (active) software version in use.
Serial Number*	The serial number of the target monitor.
Uploaded Version*	The current uploaded (inactive) software version. If this field is empty, the monitor does not have an inactive software uploaded.
Status	Software upload and activation is possible only to the monitors with the OK status. For information about other statuses, see the Authentication statuses table in the Troubleshooting section.

* If the field is empty, the Multi Monitor Manager failed to connect to the monitor.

Uploading software to the target monitors

Software upload is possible to all the monitors for which authentication was completed successfully (connection status is **OK**).

NOTE

Software is delivered as an ISO image file, either using a physical media or electronically. To have access to the software file the ISO image must be mounted first as a logical drive. If software is delivered using a physical media, mounting typically takes place automatically when you attach the USB flash drive to your computer. If software is delivered electronically, you will have to enable the mounting manually by double-clicking the ISO image file.

1. Select **Browse** or **Choose File**.

An **Open** or a **Choose File to Upload** dialog box will open.

2. Browse the drive and folder to find the software image file. Select the software file by double-clicking it or by selecting **Open**.
 - a. Select the software file that is named as "CSP_3.2.X.cas.csmon", if you are updating the monitor software from one v3.2 software to another.
 - b. Select the software file that is named as "CSP_3.2.X.cas-unsigned.csmon", if you are upgrading the monitor software from v3.1 to v3.2.
3. Select **Upload image to all monitors** to start uploading the software to the target monitors.

Points to note:

- Multi Monitor Manager uploads the software to the target monitors in batches of five monitors at a time. The rest of the contacted monitors will be queued.
- Closing the menu page during the process will abort all incomplete uploads.

The progress of the software upload is shown on the screen:

Address	Monitor Type	Current Version	Serial Number	Uploaded Version	Note	Status
172.18.3.202	B450	3.1.376	SNT19281011HA		29%	
172.18.3.203	B450	3.1.376	SNT19360050HA		32%	
172.18.3.204	B450	3.1.376	SNT17421019HP		33%	
172.18.3.205	B450	3.1.376	SNT18231014HP		34%	
172.18.3.206	B450	3.1.376	SNT19281010HA		30%	
172.18.3.207	B650	3.1.376	SNS19450029HP		Upload queued...	
172.18.3.208					Upload queued...	

4. Wait until software upload is completed and the **Operation summary** appears:



5. Check the summary and select **Close**.

6. Review the software upload statuses of all the target monitors:
 - a. If the software upload is completed successfully, the **Status** field shows **Uploaded** and the new software version is shown in the **Uploaded Version**-field.
 - b. If the software upload failed, the reason is shown in **Status** field. For more information about the statuses, see Software upload statuses table in the Troubleshooting section.

6 Upload(s) completed successfully. 1 Upload(s) completed unsuccessfully. 7 total.

Address	Monitor Type	Current Version	Serial Number	Uploaded Version	Note	Status
172.18.3.202	B450	3.1.376	SNT19281011HA	3.2.551		Uploaded
172.18.3.203	B450	3.1.376	SNT19360050HA	3.2.551		Uploaded
172.18.3.204	B450	3.1.376	SNT17421019HP	3.2.551		Uploaded
172.18.3.205	B450	3.1.376	SNT18231014HP	3.2.551		Uploaded
172.18.3.206	B450	3.1.376	SNT19281010HA	3.2.551		Uploaded
172.18.3.207	B650	3.1.376	SNS19450029HP	3.2.551		Uploaded
172.18.3.208						⌚ Request Aborted

Activating the uploaded software on the target monitors

Software activation is possible for all the monitors that have an uploaded (inactive) software version installed.

NOTE

BEFORE INSTALLATION- Compatibility is critical to safe and effective use of this device. Verify the compatibility of all system components and device interfaces, including hardware and software versions, prior to installation and use.

Before you start activating a new host software:

- Verify the compatibility of the new software version with all the monitors, and the connected bedside and network devices. Refer to the latest version of the supplemental information manual for a list of compatible network and bedside devices.
- Contact GE to get the latest version of the user and service documentation.
- Ensure that the CARESCAPE B450 and B650 monitors are connected to AC mains power for the duration of the entire software activation.

Points to note:

- A successful software activation will automatically erase (uninstall) the previous version of the software.
- LOSS OF MONITORING. Software is activated only when the monitor is in a patient discharged/case reset state. Normal patient monitoring is unavailable until the software activation is completed. This may take up to 10 minutes.
- The target monitors will retain all the current clinical and platform settings unchanged. However, any new or changed clinical and platform setting will be set to the factory defaults and may require manual configuration. For more information, refer to the latest version of the supplemental information manual

- Do not shut down the monitor until the software activation is successfully completed.
1. Select **Activate uploaded version on all monitors** to start the software activation.
 2. Wait until the software activation is started or initiated in all the target monitors and the **Operation summary** appears:



3. Check the summary and select **Close**.
4. Review the software activation status of all the target monitors:
 - If the software activation is started / initiated successfully, the **Status** is **Activation started** or **Activation is pending discharge**.
 - If the software activation failed, the reason is shown in the **Status** field. For more information, see the Software activation statuses table in the Troubleshooting section.

5 Activation(s) requested successfully. 3 Activation(s) requested unsuccessfully. 8 total. 1 activations pending patient discharge.						
Address	Monitor Type	Current Version	Serial Number	Uploaded Version	Note	Status
172.18.3.201	B650	3.2.551	SNS18170026HP	3.2.552		Activation started
172.18.3.202	B450	3.2.551	SNT19281011HA	3.2.552		Activation started
172.18.3.203	B450	3.2.551	SNT19360050HA	3.2.552		Activation started
172.18.3.204	B450	3.2.551	SNT17421019HP	3.2.552		⚠ Monitor is not in mains power
172.18.3.205	B450	3.2.551	SNT18231014HP	3.2.552	Patient admitted / SW activation pending	Activation is pending discharge
172.18.3.206	B450	3.2.551	SNT19281010HA	3.2.552		Activation started
172.18.3.207	B650	3.2.551	SNS19450029HA			⚠ No uploaded version to activate
172.18.3.208						⚠ Request Aborted

The software activation takes place either immediately or after next case end / discharge, depending on the monitor status.

Software activation immediately:

- Software activation starts immediately in all the target monitors that do not have an ongoing patient case.
- The monitor shows the following screen saver for the clinical user:
Software activation in progress. Do not disconnect any measurement modules or other peripheral devices or shut down the monitor until the software activation is complete. Activation may take up to 10 minutes. The device will automatically restart once the software activation is complete.

Software activation after next case end / discharge :

- The software activation will start after the next case end / discharge in all the target monitors that have an ongoing patient case.

- The monitor informs the clinical user about the pending software activation with the following message: ***Software activation after next case end / Software activation after next discharge***. Monitoring can continue normally.
- The software activation starts automatically after the patient is discharged, or patient case is ended. The patient monitor displays a screen saver that informs about the ongoing software activation:
Software activation in progress. Do not disconnect any measurement modules or other peripheral devices or shut down the monitor until the software activation is complete. Activation may take up to 10 minutes. The device will automatically restart once the software activation is complete.

Settings activation to multiple monitors at a time

You can transfer clinical and/or platform settings to multiple monitors at a time.

Refer to the Settings transfer process chapter for an overview of the settings transfer process.

Before you can activate settings to the target monitors:

1. Complete the platform and/or the clinical configuration in the source monitor.
2. Download the platform and/or clinical settings of the source monitor to a settings file. See Downloading clinical and platform settings chapter for details.

Points to note:

- The source monitor and all the target monitors must have CARESCAPE software version 3.2.
- Settings transfer is possible only either to CARESCAPE Bx50 monitors or to CARESCAPE ONE devices at a time. In case you need to transfer settings both to CARESCAPE Bx50 monitors and CARESCAPE ONE devices, complete the activity first to the CARESCAPE Bx50 monitors and after that to the CARESCAPE ONE devices.
- The following platform settings are unique to each monitor. When you transfer the settings, the existing values for these settings will remain the same. In case you need to change these settings, you must use CARESCAPE Service Interface to change these configurations manually for each monitor.
 - software licenses
 - host asset settings
 - network hostname
 - settings for wired network
 - unit and bed name

Specifying the target monitors for the settings transfer

1. To specify all the target monitors to which you want to transfer a new settings file, do one of the following:

- a. Select **load from file** to load the IP addresses from a file on your service PC.

NOTE

Prepare the file beforehand. The file must be a text file. IP addresses and/or host names must be separated with a line break.

- b. Enter the IP addresses or the host names of all the target monitors manually one per line to the **Monitor Addresses** field. Press **Enter** for a line break.

Connecting to the target monitors

1. Enter the **Username** and the **Password**.
2. Select **Contact Monitors** to log in and to authenticate to the target monitors.
The progress of the authentication process is updating on the screen.
3. Wait until the authentication process completes and the **Operation summary** appears on the screen:



4. Check the summary for possible issues and select **Close**.
5. Review the connection statuses of all the target monitors:

7 Monitor(s) contacted successfully. 0 Monitor(s) failed to contact. 7 total.					
Address	Monitor Type	Current Version	Serial Number	Note	Status
172.18.3.201	B650	3.2.552	SNS18170026HP		OK
172.18.3.202	B450	3.2.552	SNT19281011HA		OK
172.18.3.203	B450	3.2.552	SNT19360050HA		OK
172.18.3.204	B450	3.2.552	SNT17421019HP		OK
172.18.3.205	B450	3.2.552	SNT18231014HP	Patient admitted	OK
172.18.3.206	B450	3.2.552	SNT19281010HA	Patient admitted	OK
172.18.3.207	B650	3.2.552	SNS19450029HA		OK

Address	The service IP Address of a monitor. Selecting the IP address will open a new browser tab to access the service interface of the monitor. You can use this link for troubleshooting purposes.
Monitor Type*	B450, B650, B850, or CS ONE. Mixing CS ONE and Bx50 to the same operation is prevented. In case there are both Bx50 monitors and CS ONE devices, the operation will only be performed on the Bx50 monitors. The CS ONE devices will be excluded from the operation.
Current Version*	The current (active) software version in use.
Serial Number*	The serial number of the target monitor.
Note	Shows Patient admitted , if the target monitor has an ongoing patient case. In this case the settings activation will start after the next case end/discharge.
Status	Settings activation is possible only to the monitors with the OK status. For information about the other statuses, see Authentication statuses table in the Troubleshooting section.

* If the field is empty, the Multi Monitor Manager failed to connect to the monitor.

Selecting the settings file and the settings to be transmitted to the target monitors

Select the settings file that you have previously downloaded from the source monitor to your service PC.

1. Select **Browse** or **Choose File**.

An **Open** or a **Choose File to Upload** dialog box will open.

2. Browse the drive and folder to find the software image file. Select the software file by double-clicking it or by selecting **Open**.
3. Enter the password that was used for encrypting the settings file.
4. Select the radio button of the settings you want to activate:
 - **All (clinical and platform) settings:** Activates both the clinical and platform settings.
 - **Clinical settings:** Activates clinical settings only.
 - **Platform settings:** Activates platform settings only.

NOTE

Passwords are included in the platform settings. If you select either **All (clinical and platform) settings** or **Platform settings**, all the target monitors will receive new passwords from the settings file.

Select settings file <input type="button" value="Choose File"/> No file chosen <input type="button" value="Password for settings"/>	Settings that are to be Activated <input checked="" type="radio"/> All (clinical and platform) settings <input type="radio"/> Clinical settings <input type="radio"/> Platform settings
------------------------------------------------------------------------------------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Activating the settings on the target monitors

Settings transfer is possible for all the monitors for which authentication was completed successfully (**Status: OK**).

1. Select **Activate settings on the target monitors** to start or initiate the settings activation.
2. Wait until the **Operation summary** appears:



3. Check the summary and select **Close**.

4. Review the settings activation status of all the target monitors:

5 Activation(s) requested successfully. 3 Activation(s) requested unsuccessfully. 8 total. 1 activations pending patient discharge.						
Address	Monitor Type	Current Version	Serial Number	Uploaded Version	Note	Status
172.18.3.201	B650	3.2.551	SNS18170026HP	3.2.552		Activation started
172.18.3.202	B450	3.2.551	SNT19281011HA	3.2.552		Activation started
172.18.3.203	B450	3.2.551	SNT19360050HA	3.2.552		Activation started
172.18.3.204	B450	3.2.551	SNT17421019HP	3.2.552		! Monitor is not in mains power
172.18.3.205	B450	3.2.551	SNT18231014HP	3.2.552	Patient admitted / SW activation pending	Activation is pending discharge
172.18.3.206	B450	3.2.551	SNT19281010HA	3.2.552		Activation started
172.18.3.207	B650	3.2.551	SNS19450029HA			! No uploaded version to activate
172.18.3.208						! Request Aborted

- If the software activation is started / initiated successfully, the **Status** is **Activation started** or **Activation is pending discharge**.
- If the settings activation failed, the reason is shown in the **Status** field. For more information, see the Settings activation statuses table in the Troubleshooting section.

The settings activation takes place either immediately or after next case end / discharge, depending on the monitor status.

Settings activation immediately:

- Settings activation starts immediately in all the target monitors that do not have an ongoing patient case.

Settings activation after next case end / discharge:

- The settings activation will start after the next case end/discharge in all the target monitors that have an ongoing patient case.
- The monitor informs the clinical user about the pending software activation with the following message: **Settings activation after next case end / Settings activation after next discharge**. The monitoring can continue normally.
- The settings activation will start automatically after next discharge, or when the patient case is ended. After the settings activation the monitor will restart automatically.

Troubleshooting

Authentication statuses

Status	Possible causes	Suggested actions
OK	Both user and device authentication is successfully completed.	Monitor is ready for the software installation or settings transfer.
Invalid address or monitor is not reachable	Incorrect IP address or host name entered or uploaded into the Monitor Addresses field.	Check that the IP address or host name of the target monitor is correct.

Status	Possible causes	Suggested actions
	<p>Device authentication failed for one of the following reasons:</p> <ol style="list-style-type: none"> 1. The certificate of the target monitor is not valid. 2. The monitor has a self-signed certificate but the web browser does not have a security exception for the target monitor. 	<p>Do one of the following:</p> <ol style="list-style-type: none"> 1. It is recommended to install a valid signed certificate to the target monitor. 2. Alternatively you can specify a security exception for the web browser you use to access the target monitor.
	<p>The target monitor is not accessible for one of the following reasons:</p> <ol style="list-style-type: none"> 1. The monitor is turned off. 2. The monitor is not connected to the IX network. 3. Network error or configuration issue. 	<p>Check that:</p> <ol style="list-style-type: none"> 1. The monitor is turned on. 2. The monitor is connected to the IX network. 3. The monitor's IX network configuration is correct and that there are no network errors.
Authentication failed	<ol style="list-style-type: none"> 1. User authentication failed on all contacted monitors due to entering incorrect Username and/or Password. 2. User authentication failed on one or more monitors due to incorrect password. These monitors might have different passwords than the monitors with successful authentication statuses. 	<ol style="list-style-type: none"> 1. Check that the Username and the Password you entered are correct. 2. Check the password of the target monitor. You have the following options to resolve the issue: <ul style="list-style-type: none"> • Use the service interface to change the password of the monitor to be the same than in those monitors on which the user authentication was successfully completed, and retry to contact the monitor. • Use the service interface instead of the Multi Monitor Manager to install software and/or transfer settings on this monitor. • If several monitors have different passwords, group the target monitors by password, so that all the monitors that share the same password

Status	Possible causes	Suggested actions
		are in the same group. Then use the Multi Monitor Manager to install software and/or transfer settings on the monitors one group at a time.
Operation not possible. Install software image to CS ONE in a separate upload session.	The Monitor Addresses list contains both CARESCAPE Bx50 monitors and CARESCAPE ONE acquisition devices	In case you need to perform an operation (software installation or settings transfer) to both CARESCAPE Bx50s and CARESCAPE ONEs, complete the activity first to the CARESCAPE Bx50s and only after that to the CARESCAPE ONEs. Mixing CARESCAPE Bx50s and CARESCAPE ONEs to the same operation is prevented. In case the Monitor Addresses list contains both monitor types, the operation will only be performed on the CARESCAPE Bx50 monitors. The CARESCAPE ONE monitors will be excluded from the operation.
Monitor is duplicate with X where X = the duplicate IP address or host name	Two or more different monitors have the same IP-address or host name.	Remove all duplicate IP-addresses or host names from the list.

Software upload statuses

Status	Possible causes	Suggested actions
Uploaded	Software upload to the target monitor was completed successfully.	The monitor is available for the software activation.
Invalid file	The uploaded file is not a valid CARESCAPE software image.	Replace the file with a valid CARESCAPE software image. Contact GE Healthcare for more information.
Request aborted	Software upload cannot be started, because the monitor and/or the user authentication failed.	See Authentication statuses table for more information.

Software activation statuses

Status	Possible causes	Suggested actions
Activation started	The software activation was started immediately, because the target monitor did not have a patient admitted /an ongoing patient case.	No action required. The monitor will automatically restart with the new software version after the software activation is completed. This can take up to 10 minutes NOTE: Reconnect to the monitor after the monitor has restarted to confirm that the software activation was completed successfully with the new software version.
Activation is pending discharge	Software activation is initiated with a pending status, because the monitor has currently a patient admitted / case is started.	No action required. The software activation will start automatically after the patient is discharged / case is closed. The monitor will restart automatically with the new software version after the software activation is completed. NOTE: Reconnect to the monitor after the monitor has restarted to confirm that the software activation was completed successfully with the new software version.
No uploaded version to activate	Software activation cannot be started, because the monitor does not have any uploaded (inactive) software to be activated.	Upload a new software image to the target monitor, and restart the software activation.
Monitor is not in mains power	The target monitor (B450 or B650) is being used on battery power. The software activation can be started only when the monitor is connected to the AC mains power.	Connect the target monitor to the mains power, and restart the software activation.

Status	Possible causes	Suggested actions
Unknown error (400)	Software activation with Multi Monitor Manager is not supported if the software version to be activated requires a base license. This is typically the case in software upgrades. See Activating the host software chapter for more information about the base license.	Use service interface Configuration >Software Management >Host Software to activate software on this monitor. Ensure that you have the device specific activation code for the base license available.
Request aborted	Software activation cannot be started, because the device and/or the user authentication failed.	See Authentication statuses table for more information.

Settings activation statuses

Status	Possible causes	Suggested actions
Activation started	The settings activation was started immediately, because the target monitor did not have a patient admitted /an ongoing patient case.	No action required. The monitor will automatically restart after the operation is completed. NOTE: Reconnect to the monitor after the monitor has restarted to confirm that the new settings are effective.
Activation is pending discharge	The settings activation is initiated with a pending status, because the monitor has currently a patient admitted / an ongoing patient case.	No action required. The settings activation will start automatically after the patient is discharged / case is closed. The monitor will restart automatically with the new settings after the operation is completed. NOTE: Reconnect to the monitor after the monitor has restarted to confirm that the new settings are effective.
Invalid settings file or bad password	1. Incorrect password used to decrypt the settings file. 2. The settings file is either invalid or corrupted.	1. Try one of the following: <ul style="list-style-type: none"> • Enter the correct password to decrypt the settings file. • Retry to download the settings file from the source monitor. 2. Retry to download the settings file from the source monitor.

Status	Possible causes	Suggested actions
Cannot activate settings on software older than <version>	The settings activation with Multiple Monitor Manager is not possible on a monitor with a software older than this version.	Use service interface Configuration >Settings >Activate to activate the settings file on this monitor.
Request aborted	Settings activation cannot be started, because the device and/or the user authentication failed.	See Authentication statuses table for more information.

Other issues

Problem	Possible causes	Suggested actions
Contact Monitors – button is inactive.	1. The Monitor Addresses field is empty. There are no specified target monitors. 2. The Username and/or Password field is empty.	1. Enter the IP address or hostname for at least one target monitor. 2. Enter Username and Password .
Upload image to all monitors – button is inactive.	1. No software image file is selected. 2. None of the specified target monitors has been connected successfully.	1. Select Browse to select a software image file. 2. Ensure that at least one target monitor is successfully connected.
Activate uploaded version on all monitors – button is inactive.	None of the connected target monitors has an uploaded (inactive) software version ready to be activated.	Complete the software upload at least to one of the connected target monitors.
Activate settings on all monitors – button is inactive.	1. No settings file is selected. 2. None of the specified target monitors has been connected successfully.	1. Select Browse to select a settings file. 2. Ensure that at least one target monitor is successfully connected.

Multi Monitor Manager

CARESCAPE B850



GE Healthcare Finland Oy
Kuortaneenkatu 2
FI-00510 Helsinki
Finland
Tel: + 358 10 39411

www.gehealthcare.com

www.gehealthcare.com

