GE HealthCare

MAC™ 5 A4/MAC™ 5 A5/MAC™ 5 Lite Resting ECG Analysis System

Operator Manual

5864335-001-6

CE 0197

5864335-001-6
English

Publication Information

The information in this manual applies only to version 1.01 of MAC™ 5 Resting ECG Analysis System. It does not apply to earlier product versions. Due to continuing product innovation, specifications in this manual are subject to change without notice.

This product complies with the requirements concerning medical devices from the following regulatory bodies.

Date of first CE mark - 2022.

For more information about compliance, refer to H Regulatory and Safety Information on page 315.

The document part number and revision are on each page of the document. The revision identifies the document's update level. The revision history of this document is summarized in the following table.

Revision	Date	Comment
1	20 September 2021	Initial Release
2	20 January 2022	Update according to the comments from summative test
3	1 September 2022	Update content for Software SP04
4	19 October 2022	Update content based on FDA feedback
5	2 November 2022	Update content for Software SP05
6	15 January 2024	Update content for Software Version V1.01

Access other GE Healthcare Diagnostic Cardiology documents at the Customer Documentation Portal. Go to https://www.gehealthcare.com/en/support/support-documentation-library and scroll to the bottom of the page.

To access Original Equipment Manufacturer (OEM) documents, go to the device manufacturer's website.

Third-party Licenses

This product includes software developed by:

- Linux Kernel organization (https://www.kernel.org)
- NXP Semiconductors (https://www.nxp.com)
- Apache Software Foundation (http://www.apache.org)
- OpenSSL.org (http://www.openssl.org)
- OpenSSH (http://www.openssh.com)
- GNU Foundation packages (https://www.gnu.org)
- Gentoo software (https://packages.gentoo.org)
- Boost Libraries (http://www.boost.org)

- POCO Project (https://pocoproject.org)
- Debian packages (https://packages.debian.org)
- Yocto project packages (https://www.yoctoproject.org)
- Freedesktop.org (https://www.freedesktop.org)
- FreeRTOS (http://www.FreeRTOS.org)
- Busybox project (https://busybox.net)
- bzip.org (http://www.bzip.org)
- FreeType project (https://www.freetype.org)
- OpenBSD Project (https://www.openbsd.org)
- netfilter.org project (http://www.netfilter.org)
- netcat (http://netcat.sourceforge.net)
- OpenLDAP Project (https://www.openldap.org)
- ws4d.org (http://ws4d.org/projects)
- JS Foundation (https://js.foundation)
- ANGULARJS (https://angularjs.org)
- QT (https://qt.io)
- Massachusetts Institute of Technology (https://web.mit.edu)
- Cyrus IMAP org (https://www.cyrusimap.org)
- rsyslog (https://www.rsyslog.com)
- sshpass (https://sourceforge.net/projects/sshpass/)
- CUPS (http://www.cups.org/)
- cups-filters (https://openprinting.org/)
- zxing-cpp (https://github.com/zxing-cpp/zxing-cpp)

License details of the software used in the product can be viewed in the online help in the *Open Source Licenses* section. Contact GE Service to obtain the source code of the open-source software used in the product, if required.

This document describes the MAC™ 5 Resting ECG Analysis System, also referred to as the “product”, “system”, or “device”. This document is intended to be used by an operator of the MAC™ 5 Resting ECG Analysis System system.

The MAC™ 5 Resting ECG Analysis System is intended to be used under the direct supervision of a licensed healthcare practitioner, by trained operators in a hospital or facility providing patient care.

This document provides information required for the proper use of the system. Familiarize yourself with this information and read and understand all instructions before attempting to use this system. Keep this document with the equipment at all times, and periodically review it.

Illustrations in this document are provided as examples only. Depending on system configuration, screens in the document may differ from the screens on your system. Patient names and data are fictitious. Any similarity to actual persons is coincidental.

Support

GE Healthcare maintains a trained staff of application and technical experts to answer questions and to respond to issues and problems that may arise during the installation, maintenance, and use of this product.

If you require additional assistance, contact your GE Healthcare representative, or GE Healthcare support at one of the following numbers:

- North America: 1-800-558-7044
- Europe: +49 761 45 43 -0
- Asia: +86 21 3877 7888

Training

This document is intended as a supplement to, not a substitute for, thorough product training. If you have not received training on the use of the product, you should request training assistance from GE Healthcare.

To see available training, go to the GE Healthcare training website www.gehealthcare.com/training.

For more self-paced course offerings, tools, and reference guides you may find useful, visit the GE Healthcare Education Store at www.gehealthcare.com/educationstore.

Contents

1 Product Overview

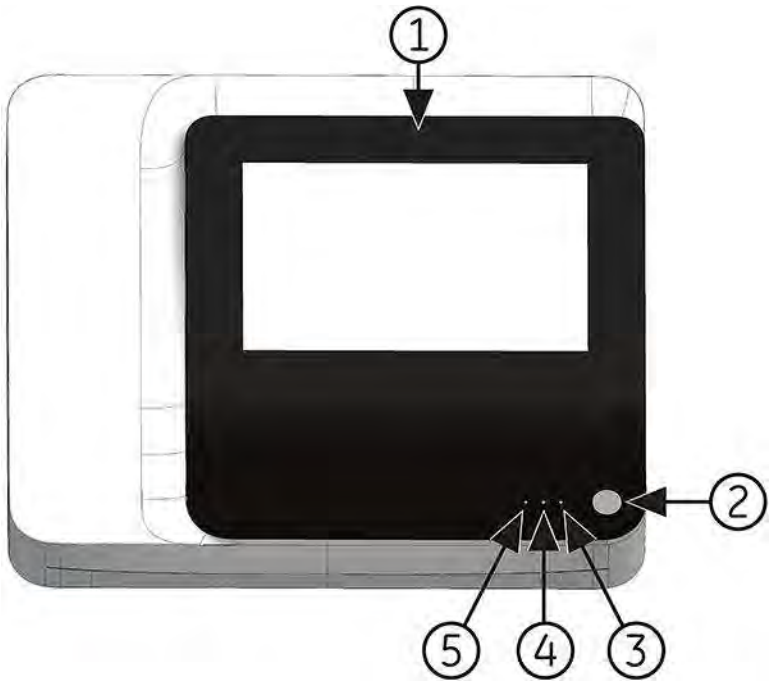
The MAC 5 Resting ECG Analysis System has three modes:

- MAC 5 A4 - This mode includes an A4/Letter paper size thermal printer.
- MAC 5 A5 - This mode includes an A5 paper size thermal printer.
- MAC 5 Lite - This mode does not include a thermal printer.

The MAC 5 Resting ECG Analysis System, (referred to as "the device"), supplies 12-lead ECG measurement and interpretative analysis, prints 12-leads of ECG, and transmits ECG data to and from a central ECG cardiovascular information system.

1.1 Front View

The image below is an example of the MAC 5 A4. The information in the table applies to all MAC 5 devices.



Item	Name	Description
1	Display and Touchscreen	Displays waveform and text data. The touchscreen enables you to interact directly with the device through touch gestures.
2	Power button	Turns the device on or off.
3	Power on LED	Shows if the device is on or off. • Green light - on. • No light - off. • Flashing green light - standby mode.

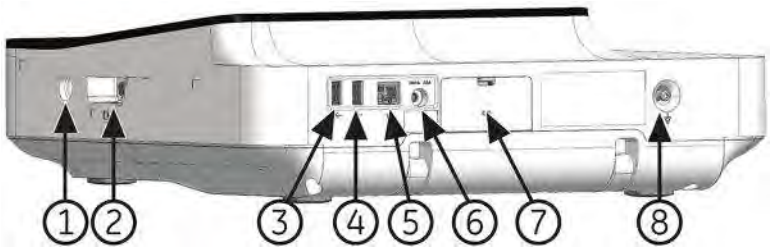
Continues on the next page

Item	Name	Description
4	Battery LED	Battery status: • Flashing amber light at 2 second intervals - battery is charging. • Flashing amber light at a 1 second interval - battery is critically low. • Flashing amber light at a 1/2 interval - battery has a communication failure. • No light - battery is fully charged, not installed, or discharging. The detailed battery status shows on the **Status Bar** of the Acquisition screen, see 1.5 Battery Status on page 20.
5	AC Power LED	AC power status: • Green light - the device is plugged in and receiving power. • No light - the device is not plugged into AC power.

1.2 Side and Rear View

Rear View

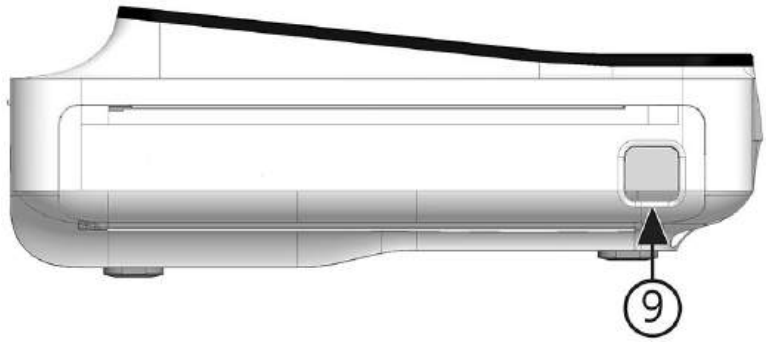
The image below is an example of the MAC 5 A4. The information in the table applies to all MAC 5 devices.



Item	Name	Description
1	KISS Pump Connector	Used to connect a KISS pump cable.
2	ECG Patient Cable Connector	D-sub 15–pin female connector for the acquisition cable.
3	USB Slot A	• Use to connect a USB flash drive or USB cable. You can connect a USB flash drive for a software update, backup/restore or export operations, or a barcode reader USB cable. • Standard USB connector for USB devices, for example, the external barcode reader, USB memory stick, USB keyboard, and USB mouse.
4	USB Slot B	• Use to connect a USB flash drive or USB cable. You can connect a USB flash drive for a software update, backup/restore or export operations, or a barcode reader USB cable. • Standard USB connector for USB devices, for example, the external barcode reader, USB memory stick, USB keyboard, and USB mouse.
5	Ethernet/LAN Port	Use to connect an Ethernet cable.
6	DC Power Inlet	Use to connect the DC power cord.
7	Battery Door	Use to insert the battery.
8	Equipotential Grounding Plug	Use to connect non-grounded peripheral devices.

Side View

The image below is an example of the MAC 5 A4. The information in the table also applies to MAC 5 A5.



Item	Name	Description
9	Printer Door Button	Use to release the printer door.

1.3 Acquisition Screen Overview

The **Acquisition** screen is the main screen that displays when you first log on to the device. You can acquire an ECG from the Acquisition screen.

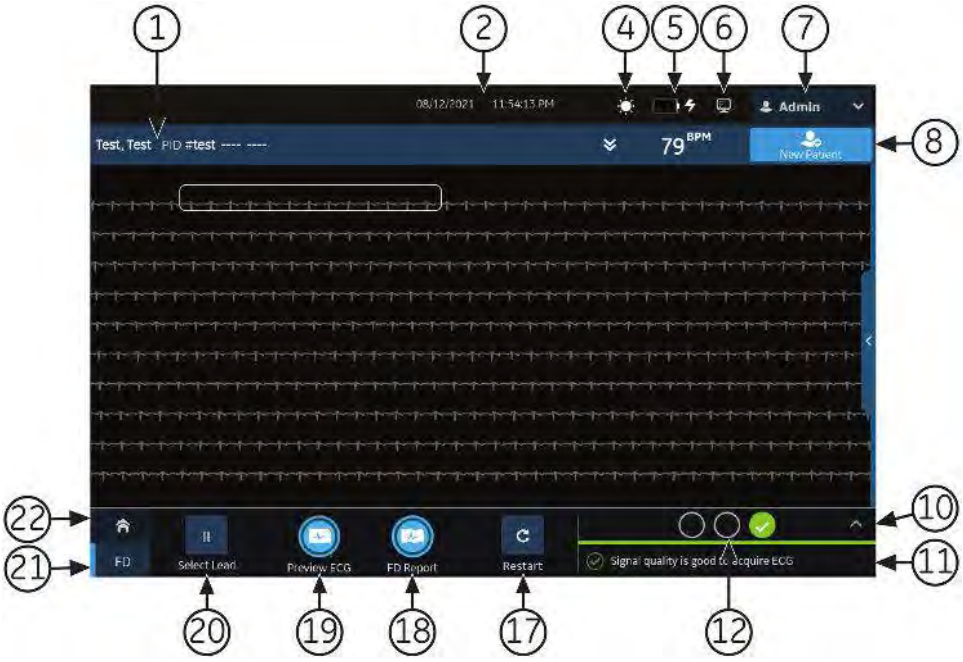


Table 1-1 Acquisition Screen

Item	Name	Description
1	**Patient Information** Banner	Shows **Patient Information** such as the patient first name, surname, and gender. Select anywhere on the banner to add or edit patient information.
2	Date and Time	Current local date and time in the configured date and time format. To configure a date and time format, see 10.10.1 Configure the Date and Time on page 254.
3	**Orders/Patients**, **Files**, and **Queue** tabs	• The **Orders** tab displays when you enable order management. Select **Orders** to open the **Orders** list and view a list of the available orders. • The **Orders** tab does not display if you disable order management, the **Patients** tab displays. Select **Patients** to open the **Patients** list. A list of the last 500 patients displays with ECGs that were acquired on the device. If you double click any information in the **Patients** list, the **Patient Information** banner expands and shows the patient information. • Select **Files** to open the **Files** list and view the list of stored patient reports. • Select **Queue** to open the **Queue** list to view the list of reports in the queue to be transmit to a configured destination.
4	Brightness Icon	Select to adjust the screen brightness.
5	Battery or AC Power Icon	Displays the battery status.
6	Network Status Icon	Displays the wireless or LAN connection status.

Continues on the next page

Table 1-1 Acquisition Screen (Table continued)

Item	Name	Description
7	User Menu	Displays the name of the user logged on to the device. When you select the name, the user menu expands and displays the available menu options. You do not have access to some menu options. Your administrator can assign the proper privileges. If you disable user authentication or configure with Technician ID access, the Default user must log on as a user with sufficient privileges to access a menu option.
8	**New Patient** icon	Select to enter patient data for a new patient test. This action will clear all previous patient data.
9	**Expand** icon	Select the tab (**Orders**/**Patients**, **Files**, or **Queue**) that you want to expand, and select the **Expand** icon to open the list.
10	Electrode Placement Picture	Select the arrow to expand and view the picture that shows the placement of electrodes and the electrode quality of each lead. Each lead quality indicator on the picture changes to yellow, red, or green, based on its connection status. You can enable or disable the auto-expansion of the picture. If you enable auto-expansion of the picture: • The picture automatically expands if the **Hookup Advisor** Lead Quality Indicator is yellow or red. • The picture automatically collapses if the **Hookup Advisor** Lead Quality Indicator is consistently green for a few seconds.
11	Notification Area	Displays messages: • printing status and progress • report transmission status • **Hookup Advisor** lead quality status The messages display one at a time in the sequence of occurrence. The messages do not display when a patient is connected and the hookup advisor is evaluating the waveform.
12	**Hookup Advisor** Lead Quality Status Indicator	Displays the lead quality status indicator in three circles that change to yellow, red, or green, based on the lead quality.
13	Filter, Speed and Gain	Displays the default waveform filter, speed, and gain. Select anywhere around the ellipsis icon and select a different value. You can only make a change before you record an ECG. You can make a change before and during the recording of a rhythm. **NOTE** A change to the filter, speed or gain is applicable to the current patient. For a new patient, the values are reset to default settings.
14	**Start Rhythm** icon	Select to print or digitally record the rhythm report.
15	**Start ECG** icon	Select to record an ECG.

Continues on the next page

Table 1-1 Acquisition Screen (Table continued)

Item	Name	Description
16	Lead Set and Display Format	Displays the default test type and display format. Select anywhere around the ellipsis icon and select a different value. You can only make a change before you record an ECG. You can make a change before and during the recording of a rhythm. **NOTE** Any change to the test type and display format only applies to the current patient. For a new patient, the values are reset to the default settings.
NOTE The items below display only after you purchase and enable **Full Disclosure** in the **Settings** screen.		
17	**Restart** icon	Select to restart the Full Disclosure ECG. A message displays as *The full disclosure data will be cleared. Do you want to proceed?*
18	**FD Report** icon	Select to generate a Full Disclosure report. The Full Disclosure report for the selected lead displays for your review.
19	**Preview ECG** icon	Select anywhere on the Full Disclosure ECG. The 10 seconds of ECG data is selected. Click Preview ECG. A preview of the recorded 10 seconds of data for all leads displays in the configured preview report format in the maximize view. Select the minimize icon to view the report.
20	**Select Lead** icon	Displays the default test type and display format. Select anywhere around the ellipsis icon and select a different value. You can only make a change before you record an ECG. You can make a change before and during the recording of a rhythm. **NOTE** Any change to the test type and display format only applies to the current patient. For a new patient, the values are reset to the default settings.
21	**FD** tab	Displays a full disclosure ECG. **NOTE** The **FD** tab displays after you buy and enable the full disclosure function.
22	Home tab	Displays the live waveform for the current patient connected to the device.

1.4 User Menu Options Description

The **User Menu** is located at the top right corner of the Acquisition screen.

Table 1-2 User Menu Options

Item	Option	Description
1	**<User>**	Displays the name of the user logged into the device as configured by your administrator. Pre-defined users display as follows: • Admin • STAT • Service • Default
2	**Settings**	Displays the **Settings** screen used to configure the device. The administrator must grant you privileges to access this screen. If the user does not have access to the screen and if user authentication is disabled or configured with Technician ID access, the Default user is prompted to log on as a user with sufficient privileges.
3	**Service**	Displays the **Service** screen used to service the device. Your administrator must grant you privileges to access this screen. If the user does not have access to the screen and if user authentication is disabled or configured with Technician ID access, the Default user is prompted to log on as a user with sufficient privileges.
4	**Service Snapshot**	The user can get a service snapshot without the **Service** privileges. Complete the snapshot to help identify a problem on the device.
5	**Change Password**	The Admin user or a local user can change their password. Displays only if you enable full user authentication.
6	**Lock**	Locks the device. Displays only if you enable full user authentication.
7	**Log Out**	Logs off the user. Displays only when you are logged on to the device.

Continues on the next page

Table 1-2 User Menu Options (Table continued)

Item	Option	Description
8	**Standby**	Puts the device in standby mode to save battery power without turning it off.
9	**Power Off**	Powers off the device. **NOTE** Pressing the **Power** button on the front panel can also stop the device.
10	**About**	Displays the device software information.
11	**Help**	Displays help information about the device.

1.5 Battery Status

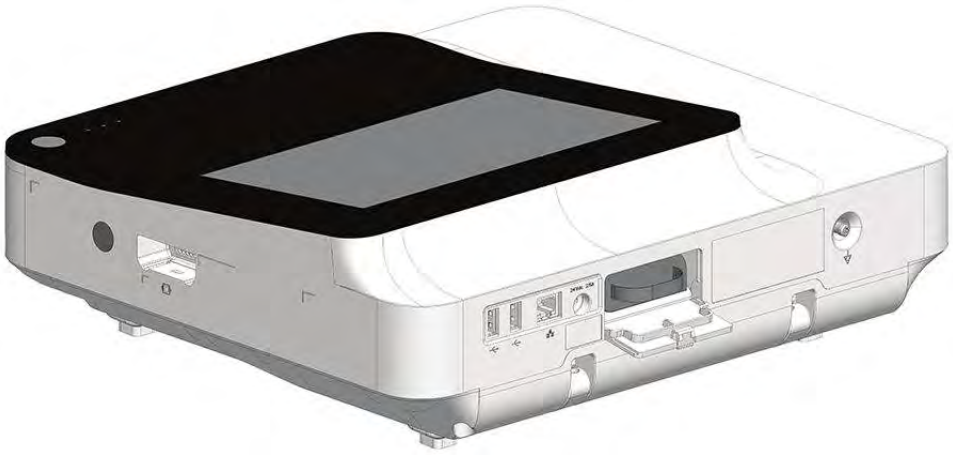
The battery icon shows the stored power of the battery. The power levels are shown in 10% increments. The color of the icons change to show the level of battery life.

You can operate the device connected to the AC Mains power when the batteries are removed. The device can also operate with a single battery installed to allow hot swapping of the battery without plugging into AC Power.

Table 1-3 Examples of Battery and Power Icon Status

Icon	Status	Description
Green 	Connected to AC Mains	The device is connected to the AC Mains power and the battery is charging.
Solid Green 	Battery - Fully Charged and Connected to AC Mains	The device is connected to the AC Mains power and the battery is fully charged.
White 	Operating on Battery	The device is only using the battery and the battery is discharging. The device is not connected to the AC Mains power.
White 	Battery – Fully Charged and Disconnected from AC Mains	The battery is fully charged and the device is disconnected from the AC Mains power.
Red 	Battery – Low or Critically Low	The battery is at low capacity and the device is disconnected from the AC Mains power. If the charge level is below 15%, an error tone sounds. A message opens that tells you the percentage of the remaining battery power. If the charge level is below 10%, the error tone is louder, longer, and sounds every minute. A message opens that tells you the battery is critically low and you should connect to AC power immediately.
No color with red X 	Battery Not Present, AC Mains Power	The battery is not in the device and the AC Mains power is connected. If you select the battery icon, a message opens that tells you the battery is not present.

The image illustrates the battery in the battery compartment.



1.6 Show Battery Status

1. Select the battery icon on the **Status Bar** of the Acquisition screen.
2. An image opens showing the battery life.

1.7 Show Network Connection Status

When the wireless and wired connection is set to **Enable**, the device uses a wired connection when you connect a Local Area Network (LAN) cable. If you remove the LAN cable, the device uses the wireless connection.

To view the status of your device's connection to your LAN or Wireless Local Area Network (WLAN), perform the procedure as follows:

1. Select the **Network Status** icon on the status bar.
2. Review the tables for the description of the network status icon when connected to a LAN or WLAN network.

Table 1-4 LAN Icons

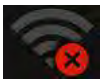
Network Status Icon	Status	Description
	LAN Active	The device is connected to a LAN.
	LAN Connected	The device is connected to a remote server through a LAN and is in the process of obtaining an IP address. If this icon is blinking, the device is acquiring an IP address from DHCP.

Continues on the next page

Table 1-4 LAN Icons (Table continued)

Network Status Icon	Status	Description
	LAN Disconnected	The device is not connected to a LAN; no LAN (Ethernet) cable is attached to the device.

Table 1-5 WLAN Icons

Icon	Status	Description
	WLAN Active	The device is connected to a WLAN and has a valid IP address. The icon shows a number of wireless bars to indicate the strength of the wireless signal.
	WLAN Connected	The device is connected to an access point and is in the process of obtaining an IP address. If this icon is blinking, the device is acquiring an IP address from DHCP.
	WLAN Disconnected	The device is not connected to a WLAN.

For more information about wireless certificate errors, see 13.10 Wireless Network Connectivity Errors on page 283.

3. Close the *Network Status* window by selecting something on the screen outside of the window.

1.8 Change the Brightness of the Screen

To change the brightness of the screen, select the brightness icon on the **Status Bar** of the Acquisition screen.

Follow one of the steps to change the brightness level of the screen from 10% to 100%:

- To increase the brightness of the screen, press **+**.
- To decrease the brightness of the screen, press **-**.

The changes you make are automatically saved to your device and will not change when you turn the device on or off.

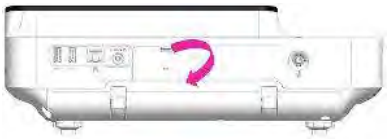
2 Equipment Setup

2.1 Insert the Battery

The device is shipped with one lithium ion battery with minimum charge.

Fully charge the battery before you use the device for the first time. Use the device on AC power while the battery is charging.

1. Place your thumb on the door release tab of the battery compartment door and gently pull it open.



MAC 5 A4

MAC 5 A5

MAC 5 Lite

2. Slide the battery into the battery compartment slots in the correct orientation.

MAC 5 A4

MAC 5 A5

MAC 5 Lite

3. Lift the battery compartment door to close it.

MAC 5 A4

MAC 5 A5

MAC 5 Lite

2.2 Connect the AC Power

This device can run with AC or battery power. When the device is plugged into an AC outlet, it uses AC power and charges the installed battery.

NOTE

If the integrity of the protective earth conductor is in doubt, operate the unit from its battery.

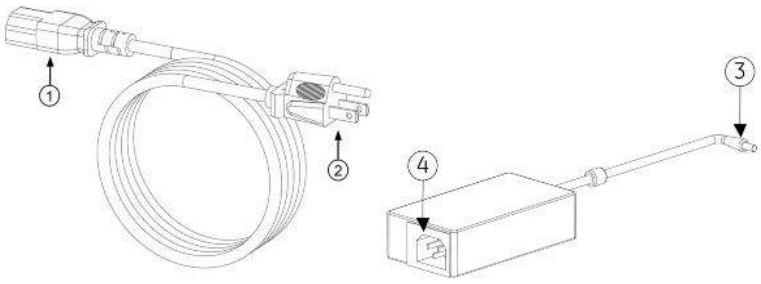


Table 2-1 Power Cord Parts

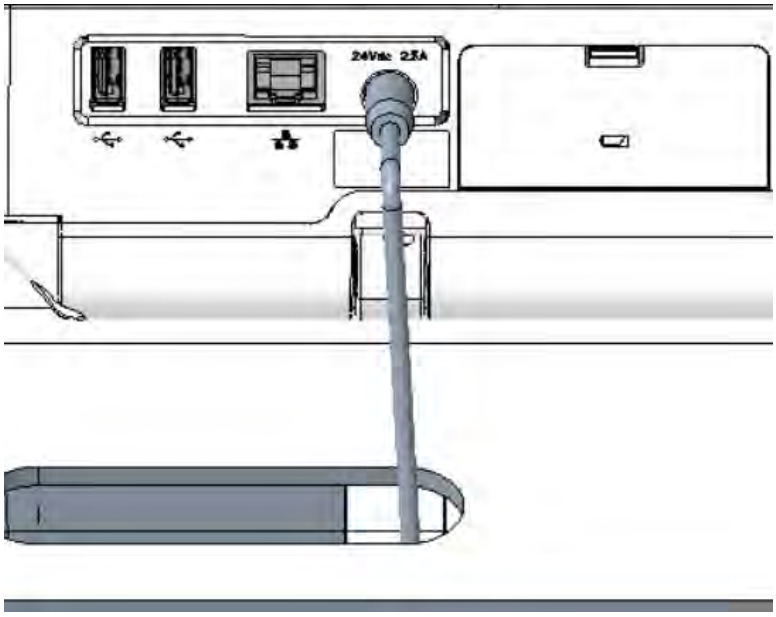
Item	Description
1	Female end of the AC power cord connected to the back of the AC/DC adapter.
2	Male end of the AC power cord connected to an AC outlet.
3	Female end of the AC/DC adapter cord connected to the back of the device.
4	Male end of the AC/DC adapter connected to the AC power cord.

NOTE

Before you connect 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 unit label. If this is not the case, do not connect the system to the power line until you adjust the power source to match the unit power requirements.

1. Connect the female end of the power cord (1) to the AC/DC adapter.

2. Plug the female end of the AC/DC adapter cord (3) to the power connector on the back of the device.



3. Plug the male end of the power cord (2) into an AC outlet.

NOTE

It is recommended that you connect the device into an uninterruptible power supply (UPS) or a surge suppressor.

4. Check the AC Power LED. If the AC Power LED is green, the device is receiving power from the AC outlet.

2.3 Connect the External Barcode Reader

If you purchase the optional barcode reader with the device, connect it to the USB port on the device.

NOTE

The **BRCD - External Barcode Reader** option is activated at the factory when you purchase the barcode reader with the device. Configure the barcode settings for your site before you use the barcode reader.

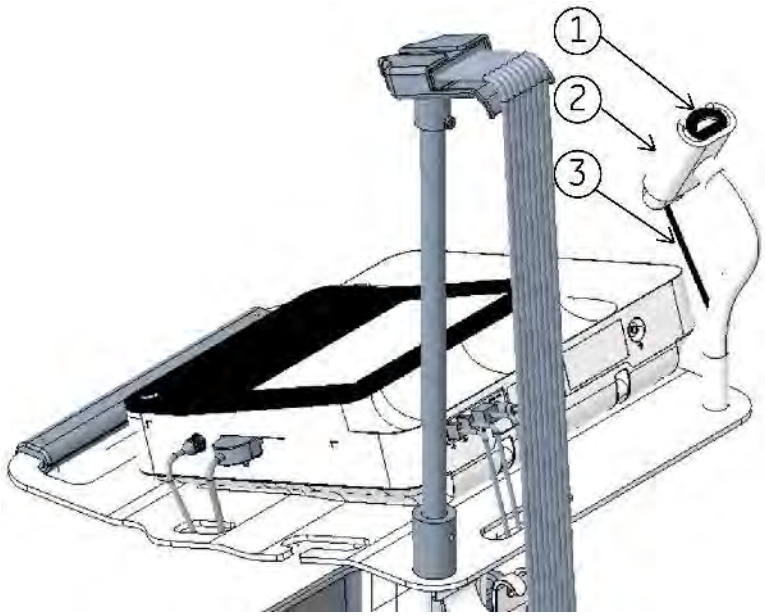


Table 2-2 Barcode Reader Parts

Item	Description
1	Barcode reader
2	Barcode reader holder
3	Barcode reader cable connected to the USB slot

1. Insert the barcode reader cable connector (3) into the USB slot of the device. Make sure that the cable is seated securely.
2. If you have a trolley, place the barcode reader (1) in the barcode reader holder (2) attached to the trolley. Refer to the *Compact Trolley Reference Manual*.

2.4 Adjust the Device for Paper Size

MAC 5 A4 printer supports the paper sizes:

- A4 (8.27 x 11.7 inches) - 2104772-001
- Letter (8.4 x 11 inches) - 2104771-001

MAC 5 A5 printer supports the paper sizes:

- A5 (8.27 x 5.9 inches) - 5684683

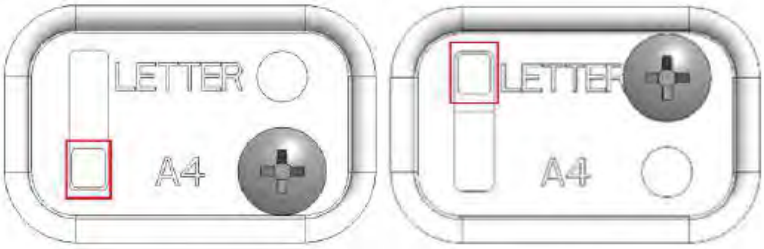
MAC 5 Lite does not support paper printing.

NOTE

Before you use the MAC 5 A4 device for the first time, perform the steps below to check if the device is correctly configured for the paper size you need.

1. Remove all the external cables.
2. Open the printer door and you will see a paper pull tab which is attached inside the printer compartment. Refer to the figures below to check if this pull tab is folded correctly.

3. Carefully flip the device over, then check if the two latches on the bottom cover are in the correct positions. Refer to the figures below.



If any of the above configuration is not appropriate, contact your local GE Healthcare service representative to reconfigure the device.

2.5 Insert the Paper

MAC 5 A4 printer supports the paper sizes:

- A4 (8.27 x 11.7 inches) - 2104772-001
- Letter (8.4 x 11 inches) - 2104771-001

MAC 5 A5 printer supports the paper sizes:

- A5 (8.27 x 5.9 inches) - 5684683

MAC 5 Lite does not support paper printing.

Make sure you put down the handle and place the device on a flat surface. To insert the paper:

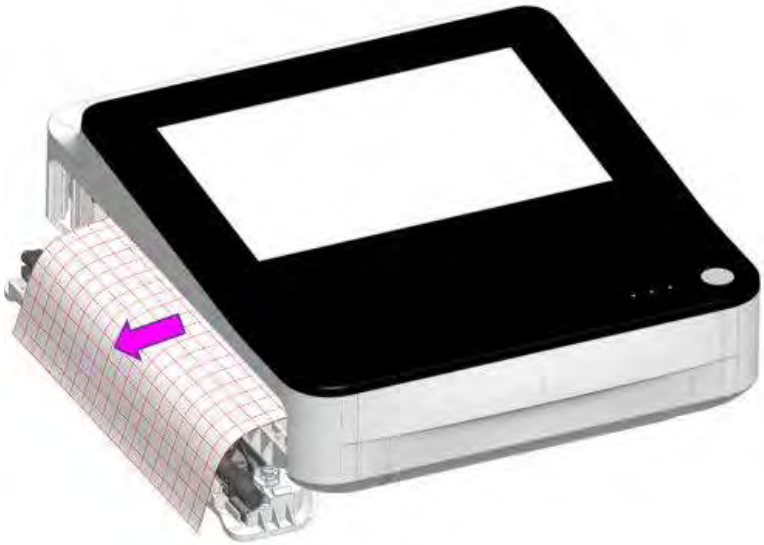
1. Press the printer door button to release the printer door.

2. Pull the paper pull tab and place the paper above it, but do not remove the paper pull tab from the device. Then slide the paper into the device until it is fully inserted.

NOTE

- If the paper has Q holes, the Q holes must be on the top left side.
- If the paper has Q marks, the Q marks must be on the bottom left side.

3. Advance the first sheet of paper.

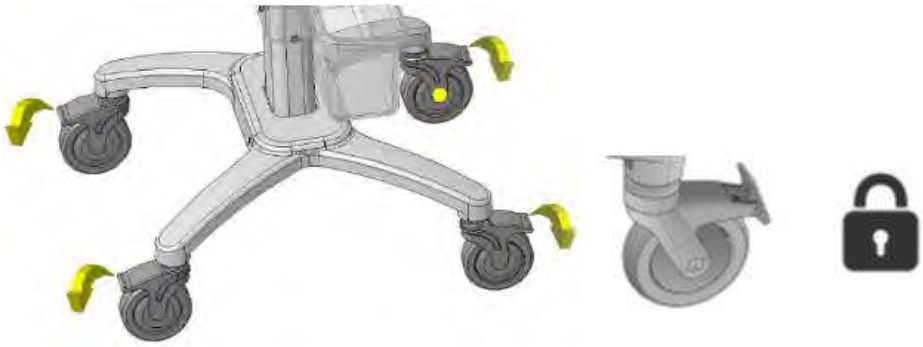


4. Push both ends of the printer door to close it and verify that the unit closes.

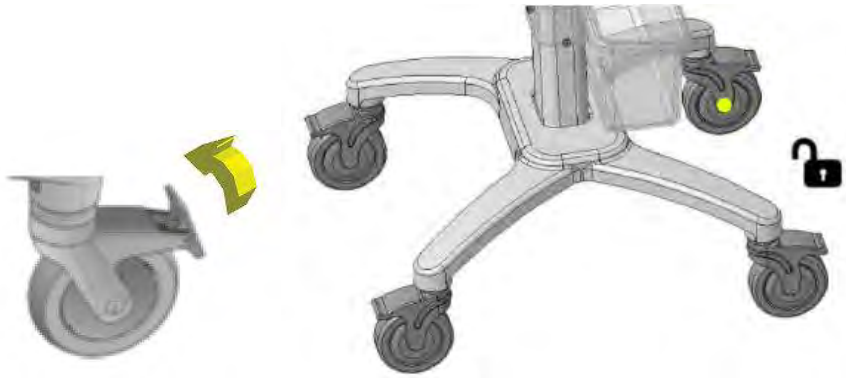
2.6 Lock and Unlock the Trolley Wheels

1. To lock each trolley wheel, press the wheel brake down.

   Lock the wheels before each use for safety purposes.



2. To unlock the trolley wheel, push the wheel brake up.



2.7 Attach the Device to the Trolley

1. Align the positioning holes on the bottom of the device with the positioning pins on the trolley top plate.
2. Gently put the device on the trolley top plate and insert the foot pads on the bottom of the device into the holes on the top plate

MAC 5 A4

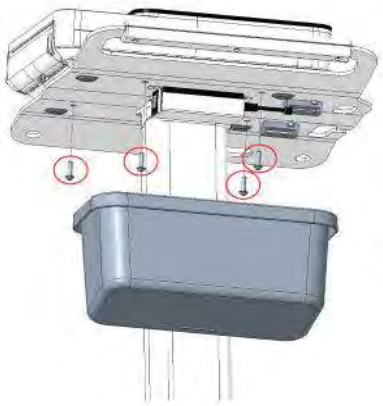
MAC 5 A5

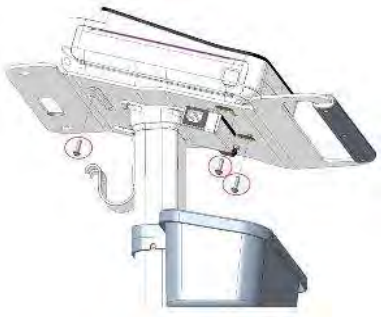
MAC 5 Lite

3. Insert the screws (M6x20 Screw GB/T 70.2-2000) and washers (D12xD6.5x1.5 Plate GB/T 848-2002) provided with the trolley through the bottom of the top plate into the device, and tighten them with 4mm torque spanner.

NOTE

Before you insert the screws, make sure that there are no cables between the device and the top plate of the trolley.





Continues on the next page

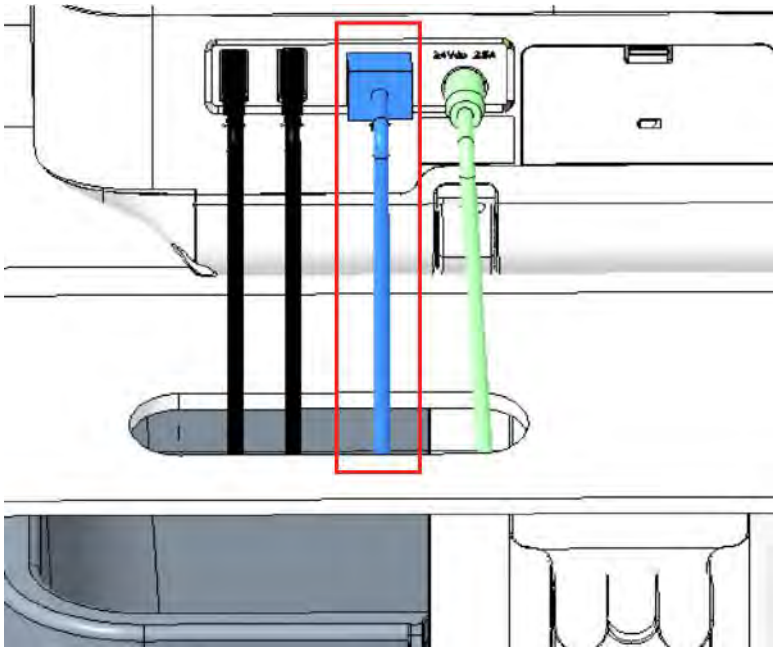
MAC 5 A4 MAC 5 A5

MAC 5 Lite

2.8 Connect the LAN Cable

A wireless module is installed in the device before it is shipped from the factory. If you do not configure the device to connect to a wireless network, you can use a wired connection.

1. To connect to a wired network, insert an Ethernet cable to the RJ45 network connector of the device.



NOTE

This applies only if you use the device as a stationary device. If you use it as a mobile unit, do not connect the device to a LAN until you are ready to import, transmit, or export patient reports.

2. Configure the device to connect to a wired network. See 10.8.3 Configure Wired Network on page 226.

2.9 Configure the Device

When the device is ready for operation, use the information in the manual to configure the system.

If you apply the same settings to more than one device at the site, save the device settings to a USB flash drive to restore them to other devices. See 10.9.3 Export and Import Configuration Settings on page 242.

2.10 Test the Device

1. After you set up and configure the device, test the device before you use it with patients. Use the test recommendations as follows:
   - Record and print a resting ECG.
   - Print a patient report. See 5.9 Print a Patient Report on page 78.

     Delete a patient report. See 5.11 Delete a Patient Report on page 81.

     Transmit a patient report. See 5.8 Transmit a Patient Report to a Configured Destination on page 76.

3 Login and Security

3.1 Power On the ECG Device

1. Press the **Power** button on the front panel for a few seconds to start the device.

   The device is powered on. The **Power on** LED on the front panel is green.

   - The activation screen displays, if you use the device for the first time. You must complete the self registration before logging in. For more information, see Self Registration.
   - A notification message displays, if it is configured by the administrator.

2. Click **Accept**.

   - If user authentication is enabled, you are prompted to log on to the device.
   - If user authentication is disabled, you are automatically logged on to the device as the **Default User**.
   - If the user authentication mode is **Technician ID**, enter the **Technician ID** to log on as a **Default User**.

3.2 Power Off the ECG Device

1. Before you **Power Off** the device, complete pending tasks, for example, acquire an ECG and save configuration settings.
2. Do one of these steps to remove power from the ECG device:

   2.1. From the **User Menu** on the screen, select **Power Off**.

   The *Power off* window opens and displays a message. Select **Power Off**.

   The device is off. The **Power on** LED on the front panel is off.

   2.2. Press the **Power** button on the front panel for a few seconds:

   The **Power Options** window opens with **Cancel**, **Standby**, **Log Out**, **Privacy**, and **Power Off** options. Select **Power Off**.

   The **Power off** window opens and displays a message. Select **Power Off**.

   The device is off. The **Power on** LED on the front panel is off.

3.3 User Authentication

The device supports different modes of user authentication.

Table 3-1 Supported User Authentication Modes

User Authentication Mode	Description
Full authentication with STAT login	The **Login** screen displays with these fields when the device is powered on or unlocked.  The users below can log on to the device: • Pre-defined users (**Admin**, **Service**) • LDAP users (If LDAP-based user authentication is configured) • Local users (If user profiles are locally managed on the device) • **STAT User** if **STAT** button is selected. The user can configure the text for this button.

Continues on the next page

Table 3-1 Supported User Authentication Modes (Table continued)

User Authentication Mode	Description
Technician ID login	The **Login** screen displays when the device is powered on or unlocked.  A technician can access the device with a valid **Technician ID**.
No authentication	A Login screen does not display when you power on the device. You are automatically logged on as the **Default User**. The **Default User** cannot access the device if user authentication is enabled.

3.3.1 Log On to the Device as a Full Authentication User without STAT

Use the username and password to log on to the device through the **Login** screen.

Table 3-2 Type of Users

Type of User	Description
Admin user	The username is **Admin**. The default password to log on as the Admin user is `admin123`. The Admin user is prompted to change the default password immediately after the first login.
Service user	The username is **Service**. This username is intended for use by Service personnel. A user with the user management privilege can set the password for the **Service** user.
Local users	The local user profiles are managed by the device administrator. Obtain your username and password from the device administrator.
LDAP users	LDAP user authentication is available only if you configure the device to support LDAP. The LDAP server administrator manages the LDAP user profiles. Obtain your username and password from the LDAP server administrator. Your privileges are based on the user role assigned to the LDAP group to which your user profile belongs.

1. Perform one of the steps below:
   - If the device is shutdown, power on the device. See 3.1 Power On the ECG Device on page 34.
   - If the device is locked, unlock the device. See 3.7 Unlock the Device on page 40.

The **Login** screen displays.

2. Perform one of the steps below:

   - Enter your username and password.

     NOTE

     - If you are an LDAP user and the default domain name is not configured, or your user profile is part of an LDAP server domain which is not the default domain, enter the domain name and username. For example, Domain\Username.
     - To verify that you entered the correct password, select **Show** to view the password.
     - Contact your administrator to reset your password. Log on to the device using the new password. Change the password immediately for security reasons.
     - If you are the Admin user and forgot your password, perform a system reset to reset the password to the default password `admin123`. For more information, see 3.9 Perform System Reset on page 41.

   - Use an external barcode reader to scan your username barcode, then enter your password.

     NOTE

     For more information, see 2.3 Connect the External Barcode Reader on page 25.

3. Select **Log In**.

   - If the login credentials are correct, you are successfully logged on to the device. Your username displays on the upper-right corner of all of the screens you have access.
   - If your login fails, see the table below:

Table 3-3 Login Errors

Symptom	Cause	Solution
`The username or password is incorrect.`	You entered your username or password incorrectly.	Re-enter your correct username and password again.
	You are a local user and you forgot your password	Contact your administrator to reset your password, then log on to the device again.
	If you are an LDAP user, the error is caused by: • No connection to the LDAP server. Your username cannot be authenticated against cached LDAP user credentials.	• Wait for the connection to the LDAP server to be restored and log on to the device again.
	• You do not belong to any groups authorized access to this device.	• Contact your LDAP administrator to assign your user profile to an LDAP group authorized for this device and log on to the device again.
	• Your current password has expired.	• Contact your LDAP administrator to change your password.
You are prompted to change your password.	You are a local or Admin user and your password has expired.	Perform the procedure 3.4 Change the User Password on page 39 and log on to the device again.

3.3.2 Log On to the Device as a STAT User

If you enable user authentication **STAT**, a **STAT** user can log on to the device to get a patient ECG in an emergency.

1. On the **Login** screen, select **STAT**.

   The Acquisition screen opens.

2. You can get an ECG or other tasks the administrator has assigned to the **STAT** user role. You are not able to review any report generated by other users.

3.3.3 Access the Device using a Technician ID

Make sure that you enable the Technician ID in the **User Authentication** setting.

On the **Login** screen, perform one of these steps:

1. Enter a valid Technician ID in the **Technician ID** field and select **Continue**.
2. **NOTE**

   If you use an external barcode reader, make sure that:

   - The **BRCD - External Barcode Reader** option is activated on the device.
   - You enable External USB Storage in **Settings** > **System** > **Storage** and enable at least one USB port in **Settings** > **Hardware** > **USB Port**.
   - The barcode reader is correctly connected to the device.

   Use an external barcode reader to scan a valid Technician ID barcode. It will automatically fill in the **Technician ID** field.

   A message **Logging in...** displays on the screen. You do not need to select **Continue**.

   You are logged on as the **Default User**. The Acquisition screen displays. You can perform tasks with **Default User** or **Technician ID** assigned privileges.

3.3.4 Log Out of the Device

Log out of your user session when you are done using the device. You must enable User authentication.

1. Complete pending tasks, for example, acquire an ECG or save configuration settings, before you log off from your user session.
2. Perform one of these steps to log off of the device:
   - Press the **Power** button. The **Power Options** dialog box opens. Select **Log Out**.
   - From the User Menu on the Acquisition screen, select **Log Out** to log off the device.

   If you log off before a task is completed, a message displays that you will lose incomplete data.
3. Perform one of these steps:
   - If you have unsaved data, select **Cancel**.
   - If you want to log off, select **Log Out**.

     You are logged off your user session.

3.4 Change the User Password

This procedure applies only to the Admin user and local users. LDAP users must change their password externally as per the instructions provided by their LDAP administrator.

Make sure that the new password follows the password requirements:

- Password must contain at least 8 characters or the minimum password length configured, whichever is higher.
- You can configure the desired password characters. The password must contain at least one occurrence of each of the configured characters:
  - Lowercase letter (a-z)
  - Uppercase letter (A-Z)
  - Number (0-9)
  - All special characters (!,@,#,$,%,^,&,*, single space)
- You can configure the password with repeat characters to the maximum number. You can set up in **Security** settings.
- You can configure the password with sequential characters to the maximum number. You can set up in **Security** settings.
- You can configure the password for the number of times to prevent the reuse of previously used password. You can set up in **Security** settings.
- You can configure the password with characters to change from the password that you used before to the minimum number. You can set up in **Security** settings.
- The password cannot be a commonly used password.
- The username cannot be used as a password.

1. From the **User** menu on the Acquisition screen, select **Change Password**.

   The **Change Password** dialog box opens.
2. Enter the current password and new password, and confirm the new password.
3. Select **Change Password**.
   - If the new password meets the password requirements, a message displays that your password was changed successfully.

     Select **OK** to close the **Change Password** window. You are logged into the device.
   - If the new password does not meet the password requirements, an error message displays.

     Follow the password requirements for a new password and repeat the steps in this procedure to create a new password.

3.5 Activate or Deactivate Privacy Mode

Privacy mode can be activated to prevent the display of confidential information on the screen. During this mode, the screen will be blank. Processes such as ECG acquisition, transmission, and printing continue to work in background, but the device ignores input from a barcode reader.

- To activate privacy mode, press the **Power** button on the front panel.

The *Power Options* window opens with **Cancel**, **Standby**, **Log Out**, **Privacy**, and **Power Off** options. Select **Privacy**.

The GE logo displays on the center of the screen with a black background, and a message displays indicating screen privacy is turned on.

- To deactivate privacy mode, tap anywhere on the screen.

  The screen you were working on before activating privacy mode displays.

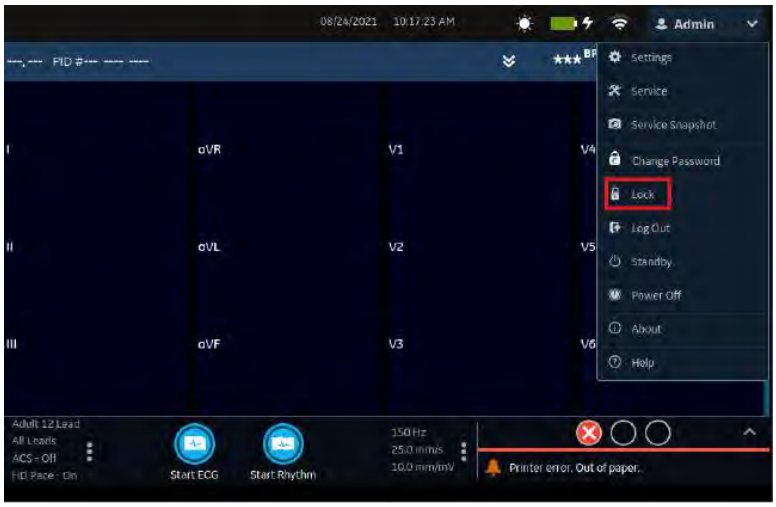
3.6 Lock the Device

You can lock the device if you enable user authentication. You cannot lock the device while ECG or rhythm acquisition or report printing is in progress.

NOTE

The **STAT User** cannot lock the device.

1. Complete your tasks.
2. From the User Menu on the Acquisition screen, select **Lock**.



The device is locked. Your username displays on the lock screen.

3.7 Unlock the Device

1. Tap the lock icon on the screen.

   A message displays prior to login if one is configured by your administrator. Click **Accept**.

   The **Login** screen displays. The **User Name** field displays the name of the user who is logged on.
2. Enter your password and select **Log In** to log on to the device.

   You can also log in as:

   - A **STAT User** (if STAT access is enabled)
   - A different user

     A message displays that the current user will be logged out and any unsaved data will be lost. Select **Continue** to log into the device.

3.8 Put the Device on Standby

1. Perform one of the steps below to put the device on standby:
   - From the **User** menu on the Acquisition screen, select **Standby**.
   - Press the **Power** button.

     The **Power Options** dialog opens. Select **Standby**.

   To exit standby mode, press the **Power** button on the front panel.

   If user authentication is configured, standby mode is off and the lock screen displays. Perform the procedure 3.7 Unlock the Device on page 40 to unlock and login to the device.

3.9 Perform System Reset

Before you start this procedure, make sure that:

- You have the serial number of the device.
- You connect the device to AC Power.
- If the authentication mode of the device is **No authentication**, access the **Settings** screen from the user menu to open the **Login** screen.
- If the authentication mode of the device is **Full Authentication with Stat**, power on the device to view the **Login** screen.
- You must log on to the device as the Admin user.

NOTE

The **System Reset** deletes all data and settings. The system is reset to factory defaults. Use the default admin password to log on to the device. It keeps the previously enabled option codes, serial number, MAC address, and Wireless Country of Operation configuration.

NOTE

The **Restore to Factory Defaults** resets the settings or section of settings.

Use this procedure as a last solution. **Transfer your data from the system before you start the procedure.**

1. When the **Login** screen displays, press ↑↓←→↑↓←→, consecutively, on the soft keyboard.

   The **System Restore** screen displays a warning that the System Restore will return your system to the original factory shipped configuration. All patient data, system setup changes, logs, and user data will be lost and unrecoverable.

2. Enter the serial number of the device in the **Enter the system serial number** field and select **Save**.

   If the serial number is correct, the **Restore** button will be active.

3. Select **Restore** to proceed with system restore.

   The system configuration is reset to factory defaults and all patient data records are deleted. The device reboots. You can access the device as the **Default** user without login credentials.

4. To reconfigure the device, access the **Settings** screen from the user menu. A login screen opens. Log on as **Admin** user with the default password *admin123*.

4 Patient Information

4.1 Patient Information Screen Overview

Patient information helps you to identify the patient. View and make sure the patient information is complete and correct before you start an ECG.

You can update the patient information on the **Patient Information** screen as follows:

- Attach an order from the orders list (if order management is enabled).
- Attach patient information from the recent patients list (if order management is disabled).
- Read a patient barcode with a barcode scanner.
- Use a software keyboard to enter **Patient Information**.
- Do an Admission, Discharge, Transfer (ADT) query.

WARNING

INACCURATE PATIENT DATA

Patient data from the last patient may remain in the patient information banner if the last user did not finish and close out of their session. Incorrect patient data can affect diagnosis and treatment. Make sure to check the patient information screen for each patient. Make sure that you enter patient data for the correct patient.

On the Acquisition screen, the **Patient Information** banner is located above the waveform and shows minimal information about the patient.

Table 4-1 Patient Information Banner

Item	Field	Description
1	**Name**	Shows the last name and first name of the patient.
2	**PID#**	Shows the unique identification number of the patient (patient ID).
3	**Gender**	Shows the patient gender.
4	**DOB (Age)**	Shows the patient date of birth and age. If the **Date of Birth** field is configured to be hidden on the **Patient Information** screen, only **Age** Shows on the bar.
5	Chevron	Select the chevron to collapse or expand the **Patient Information** banner. If the chevron is in a down position, the **Patient Information** banner is collapsed, and if it is in the upward position, the **Patient Information** banner is expanded.

Continues on the next page

Table 4-1 Patient Information Banner (Table continued)

Item	Field	Description
6	**BPM**	Shows the real-time beats per minute (BPM). The heart rate updates whenever the heart rate calculation algorithm reports a change in the heart rate. The heart rate does not display if it drops below 30 bpm, increases above 300 bpm, or the system is not getting ECG data. In cases where the heart rate does not display, three asterisk symbols show instead of the heart rate. 

Select the **Patient Information** banner to expand it into a full screen view. Fields configured by your administrator display in the **Patient Information** screen.

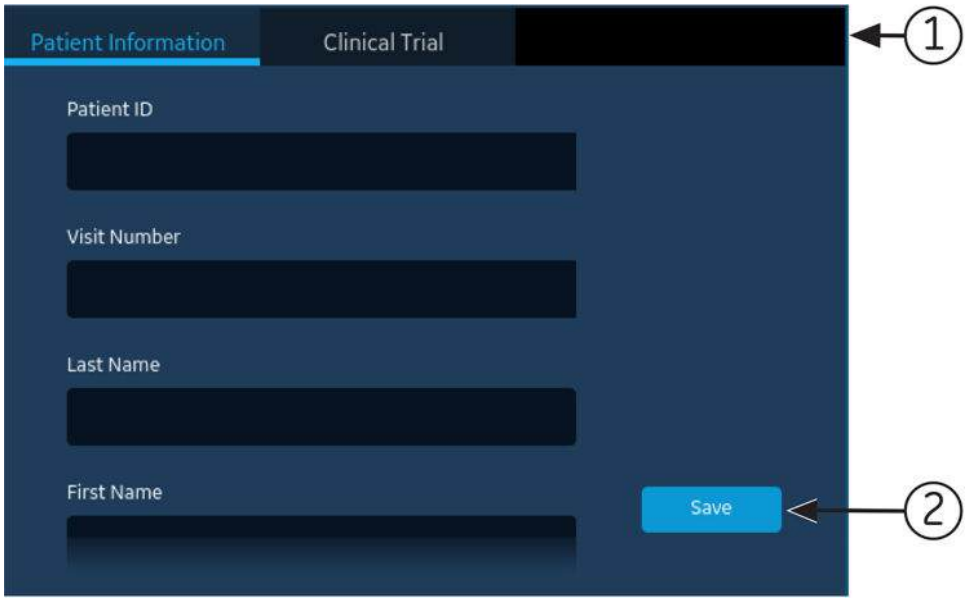


Table 4-2 Patient Information Screen

Item	Field	Description
1	**Patient Information** tab	Shows patient information, such as patient first name, last name, gender, age, and other configured information.
2	**Save** button	Select **Save** to save the patient information.

If the bottom of the **Patient Information** screen is blurred, it indicates that the configured information does not display completely. Swipe your finger in the upward or downward direction on the screen to scroll through the screen. For information on updating data in the **Patient Information** screen, see 4.3 Enter Patient Information on page 45.

Select the **Patient Information** banner to expand it into a full screen view. Select **Clinical Trial**, fields configured by your administrator display in the **Clinical Trial** screen.

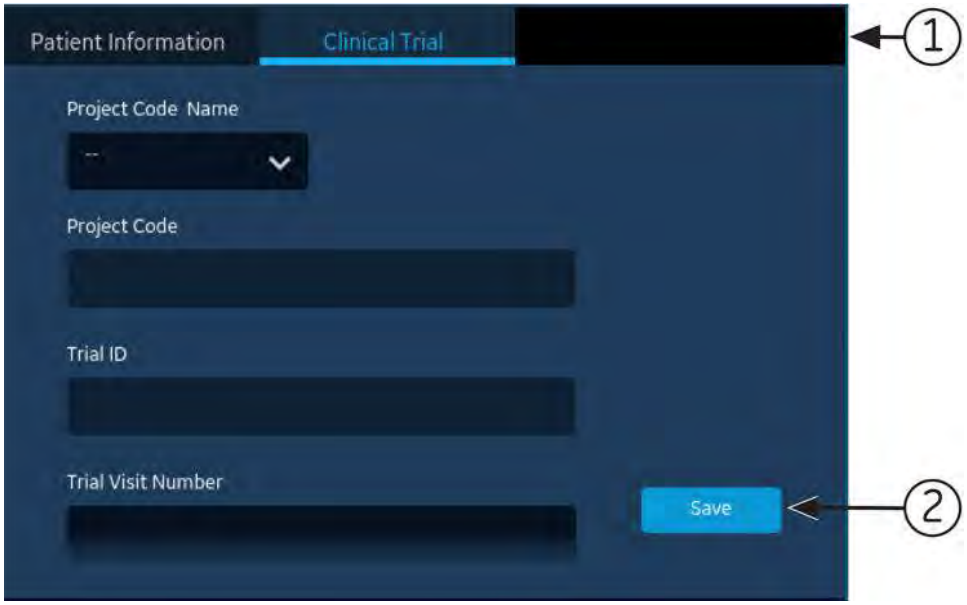


Table 4-3 Clinical Trial Screen

Item	Field	Description
1	**Clinical Trial** tab	Shows clinical trial information, such as project code name, project code, trial ID, and other configured information.
2	**Save** button	Select **Save** to save the clinical trial information.

If the bottom of the **Clinical Trial** screen is blurred, it indicates that the configured information does not display completely. Swipe your finger in the upward or downward direction on the screen to scroll through the screen. For information on updating data in the **Clinical Trial** screen, see 4.4 Enter or Edit Clinical Trial on page 56.

4.2 Start a Test for a New Patient

Start a test for a new patient in the Acquisition screen.

1. Select the **New Patient** icon located in the upper right corner of the Acquisition screen:

If	Then
A patient test is open with unsaved data, a message opens that unsaved patient data will be lost.	Select one: • Select `New Patient`, all unsaved patient data is deleted and you can enter new patient data. • Select `Continue with Same Patient`, the patient information on the screen is used for you to continue with the same patient.

Continues on the next page

If	Then
Electrodes are put on a patient and then removed or disconnected for more than 30 seconds, a warning message displays when the electrodes are put on a patient again.	Select one: • `Yes, Continue` if you put electrodes on the same patient, then the device will continue a test for that patient. • `No, Clear patient info` if you put electrodes on a new patient, then the device will start a test for the new patient.

2. If there are pending print tasks in the queue, a message opens that pending print tasks will be deleted from the queue.
   - Select `Continue` to delete pending print tasks and start the test for the new patient. The **Patient Information** screen expands.
   - Select `Cancel` to cancel the test for the new patient, and complete the pending print tasks.
3. The **Patient Information** screen opens, enter information for the patient.

4.3 Enter Patient Information

Use the methods below to enter or update patient data in the **Patient Information** screen:

- Use a barcode reader, see 4.3.1 Update Patient Information with a Barcode Reader on page 45.
- Do ADT queries, see 4.3.2 Query Orders or ADT for Patient Demographics on page 46.
- Open a patient record in the **Patients** list, see 9.2 Select a Patient from the Patients List on page 114.
- Attach an order, see 6 Work with Orders on page 87.
- Use a software keyboard, see 4.3.3 Enter or Edit Patient Information Using the Software Keyboard on page 55.

4.3.1 Update Patient Information with a Barcode Reader

Using a barcode reader can simplify the entry of patient information and reduce the chance of introducing errors. When you scan a patient's barcode, it retrieves the patient information encoded in the barcode. You can then verify and modify the information.

You can scan a patient's barcode using an external barcode reader.

Before you use an external barcode reader, make sure that:

- The **BRCD - External Barcode Reader** option to use an external barcode reader is activated on the device.
- The barcode reader is connected to the device, and the device is correctly configured to use the peripheral. For more information, see 2.3 Connect the External Barcode Reader on page 25.
- You are in the **Home** tab or **Full Disclosure** ECG screen, or when patient demographics banner is open.

An error message displays if you scan a barcode during the acquisition of a Resting ECG, Rhythm ECG or a Full Disclosure ECG for the patient.

Use the procedure below to scan the patient's barcode:

1. Start a test for a new patient. For more information, see 4.2 Start a Test for a New Patient on page 44.
2. Scan the patient's barcode to populate the **Patient Information** screen.

   Hold the button and position the barcode reader 10 cm to 15 cm (4 inches to 6 inches) above the barcode to be scanned.

   The barcode is automatically scanned.

   The barcode reader emits a sound to confirm the barcode scan. The **Patient Information** screen expands and displays the fields populated with patient information.
3. If there is a mismatch between the data scanned from the barcode and existing patient information, a message displays. Perform one of the steps as follows:
   - Select **Use Scanned Data** to populate the barcode data into the relevant fields on the **Patient Information** screen, and confirm the data entered from the barcode is accurate.
   - Select **Use Current Data** to retain the manually entered information on the **Patient Information** screen, and enter or modify patient information as necessary.

4.3.2 Query Orders or ADT for Patient Demographics

Make sure that:

- You have privileges to see orders and do remote patient query.
- Use orders of ADT data as configured on the device to do remote patient query.
- A barcode reader is connected to the device.

1. Start a test for a new patient. For more information, see 4.2 Start a Test for a New Patient on page 44.
2. Do one of the steps below:
   - Scan the patient barcode.
   - Use the keyboard to enter the **Patient ID** or **Visit Number** on the screen and press **Search** icon on the respective field.

   The device queries
   - orders only
   - or orders and then ADT data
   - or ADT data only

   Depending on how the administrator configured the device.

If	Then Go to
The device searches only orders from the MUSE system.	4.3.2.1 Order Query Workflow from MUSE system on page 47
The device searches only orders from the EMR Gateway system.	4.3.2.2 Order Query Workflow from EMR Gateway system on page 48
The device searches orders and then ADT data from the MUSE system.	4.3.2.3 Orders and then ADT Query Workflow from MUSE system on page 50
The device searches orders and then ADT data from the EMR Gateway system.	4.3.2.4 Orders and then ADT Query Workflow from EMR Gateway system on page 52
The device searches ADT data only or if no matching order is found from the MUSE system.	4.3.2.5 ADT Query Workflow from the MUSE system on page 54
The device searches ADT data only or if no matching order is found from the EMR Gateway system.	4.3.2.6 ADT Query Workflow from the EMR Gateway system on page 54

3. Enter or change patient information, as necessary.

4.3.2.1 Order Query Workflow from MUSE system

The device first searches for local orders with the **Patient ID**.

If	Then
Multiple local orders are found on the device	The orders show on the **Orders** tab in a filtered list. Select the order you will to attach to the patient test.
One local order is found on the device	The order fills in the **Patient Information** screen, if there is no mismatch with the patient data on the screen.
No local orders are found on the device	A message displays in the notification area that no matching local orders are found.

The device first searches for local orders with the **Visit Number**.

If	Then
Multiple local orders are found on the device	The orders show on the **Orders** tab in a filtered list. Select the order you will to attach to the patient test.
One local order is found on the device	The order fills in the **Patient Information** screen, if there is no mismatch with the patient data on the screen.
No local orders are found on the device	A message displays in the notification area that no matching local orders are found.

The device then searches for remote orders in the MUSE system with **Patient ID**.

If	Then
Multiple remote orders are found on the MUSE system	The orders show on the **Orders** tab in a filtered list. Select the order you will to attach to the patient test.
One remote order is found on the MUSE system	The order fills in the **Patient Information** screen, if there is no mismatch with the patient data on the screen.
No remote orders are found on the MUSE system	A message displays in the notification area that no matching remote orders are found.
Remote order query failed on the MUSE system	A message displays in the notification area that remote order query has failed.

The device then searches for ADT data in the MUSE system with **Visit Number**.

If	Then
Multiple ADT records are found on the MUSE system	The matching records show on the Acquisition screen, and a message displays in the notification area that matching ADT data is found. The maximum of five records display on the Acquisition screen. Select the ADT record to search the order using that selected record's **Patient ID**.
Only one ADT record is found on the MUSE system	System searches for the **Patient ID** order found in that ADT record. • If multiple orders are found on the system - The orders show on the **Orders** tab in a filtered list. Select the order you will to attach to the patient test. • If only one order is found on the system - The order fills in the **Patient Information** screen, if there is no mismatch with the patient data on the screen. • If no orders are found on the system - A message displays in the notification area that no matching remote orders are found. • If remote order query is failed on the system - A message displays in the notification area that remote order query has failed.
No ADT records are found on the MUSE system	A message displays in the notification area that no ADT data found.
Remote ADT data query failed on the MUSE system	A message displays in the notification area that ADT query has failed.

When local or remote orders are found, and you try to attach the order:

If	Then
The selected order matches the patient demographics in the **Patient Information** screen	A warning message displays on the screen: *Are you sure you want to attach this order to the current test?* Select **Yes** to attach the order, **No** to cancel the action.
The selected order does not match the patient demographics in the **Patient Information** screen	A warning message displays on the screen: **Name or Patient ID Mismatch** *Are you sure you want to attach this order to the current test?* Select **Yes** to attach the order, **No** to cancel the action.

4.3.2.2 Order Query Workflow from EMR Gateway system

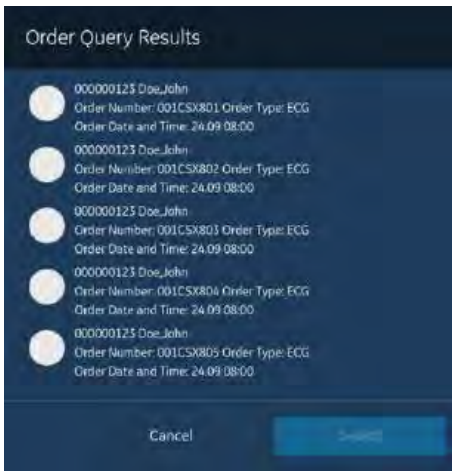
Make sure that you perform all the below steps to query orders from the EMR Gateway system:

- Set the user privileges to view the orders.
- Disable the **Order Management** in **Settings** > **Workflow** > **Order Manager**.
- Configure a DCP destination for the EMR Gateway system.
- Enable the **ADT/EMR Order Query** settings for DCP destination in **Settings** > **Workflow** > **Transmission & Query**.

NOTE

The EMR Gateway system must be V2 or higher.

1. The device searches for remote orders in the EMR Gateway system with a **Patient ID** or **Visit Number**.

If	Then
Multiple remote orders are found on the EMR Gateway system.	More than one matching orders show on the Acquisition screen. Select the order you want to attach to the patient test. 
One remote order is found on the EMR Gateway system.	The order fills in the **Patient Information** screen, if there is no mismatch with the patient data on the screen.
No remote orders found on the EMR Gateway system.	A message displays in the notification area that no matching remote orders are found.
Remote order query failed on the EMR Gateway system.	A message displays in the notification area that remote order query has failed.

2. When, you find remote order.

If	Then
There is no data mismatch.	The patient demographics, order number, and other patient information that are available in the order is populated in the **Patient Information** screen. The order gets attached to the current test. Continue with ECG test.

The patient data (other than patient demographics) does not match the patient data in the **Patient Information** screen.	A warning message displays on the screen:
	`Are you sure you want to attach this order to the current test?`
	`Name :`
	`Order :`
	`DOB :`
	`Existing patient data will be overwritten.`
	Select **Yes** to continue with the test, **No** to cancel the action.

4.3.2.3 Orders and then ADT Query Workflow from MUSE system

The device first searches for local orders with the **Patient ID**.

If	Then
Multiple local orders are found on the device	The orders show on the **Orders** tab in a filtered list. Select the order you will to attach to the patient test.
One local order is found on the device	The order fills in the **Patient Information** screen, if there is no mismatch with the patient data on the screen.
No local orders are found on the device	A message displays in the notification area that no matching local orders are found.

The device first searches for local orders with the **Visit Number**.

If	Then
Multiple local orders are found on the device	The orders show on the **Orders** tab in a filtered list. Select the order you will to attach to the patient test.
One local order is found on the device	The order fills in the **Patient Information** screen, if there is no mismatch with the patient data on the screen.
No local orders are found on the device	A message displays in the notification area that no matching local orders are found.

The device then searches for remote orders in the MUSE system with **Patient ID**.

If	Then
Multiple remote orders are found on the MUSE system	The orders show on the **Orders** tab in a filtered list. Select the order you will to attach to the patient test.
One remote order is found on the MUSE system	The order fills in the **Patient Information** screen, if there is no mismatch with the patient data on the screen.

Continues on the next page

If	Then
No remote orders are found on the MUSE system	A message displays in the notification area that no matching remote orders are found. The device then searches for ADT data in the MUSE system. • If multiple ADT records are found on the MUSE system - The matching records show on the Acquisition screen, and a message displays in the notification area that matching ADT data is found. Select the ADT record to search the order using that selected record's **Patient ID**. • If only one ADT record is found on the MUSE system - The device searches for the **Patient ID** order found in that ADT record. ◦ If multiple orders are found on the system - The orders show on the **Orders** tab in a filtered list. Select the order you will to attach to the patient test. ◦ If only one order is found on the system - The order fills in the **Patient Information** screen, if there is no mismatch with the patient data on the screen. ◦ If no orders are found on the system - A message displays in the notification area that no matching remote orders are found. ◦ If remote order query is failed on the system - A message displays in the notification area that remote order query has failed. • If no ADT records are found on the MUSE system - A message displays in the notification area that no ADT data/remote orders found. • If remote ADT data query failed on the MUSE system - A message opens in the notification area that ADT query has failed.
Remote order query failed on the MUSE system	A message displays in the notification area that remote order query has failed.

The device then searches for ADT data in the MUSE system with **Visit Number**.

If	Then
Multiple ADT records are found on the MUSE system	The matching records show on the Acquisition screen, and a message displays in the notification area that matching ADT data is found. The maximum of five records display on the Acquisition screen. Select the ADT record to search the order using that selected record's **Patient ID**.

Continues on the next page

If	Then
Only one ADT record is found on the MUSE system	System searches for the **Patient ID** order found in that ADT record. • If multiple orders are found on the system - The orders show on the **Orders** tab in a filtered list. Select the order you will to attach to the patient test. • If only one order is found on the system - The order fills in the **Patient Information** screen, if there is no mismatch with the patient data on the screen. • If no orders are found on the system - A message displays in the notification area that no matching remote orders are found. • If remote order query is failed on the system - A message displays in the notification area that remote order query has failed.
No ADT records are found on the MUSE system	A message displays in the notification area that no ADT data/remote orders found.
Remote ADT data query failed on the MUSE system	A message displays in the notification area that ADT query has failed.

When local or remote orders are found, and you try to attach the order:

If	Then
The selected order matches the patient demographics in the **Patient Information** screen	A warning message displays on the screen: *Are you sure you want to attach this order to the current test?* Select **Yes** to attach the order, **No** to cancel the action.
The selected order does not match the patient demographics in the **Patient Information** screen	A warning message displays on the screen: *Are you sure you want to attach this order to the current test?* Select **Yes** to attach the order, **No** to cancel the action.

4.3.2.4 Orders and then ADT Query Workflow from EMR Gateway system

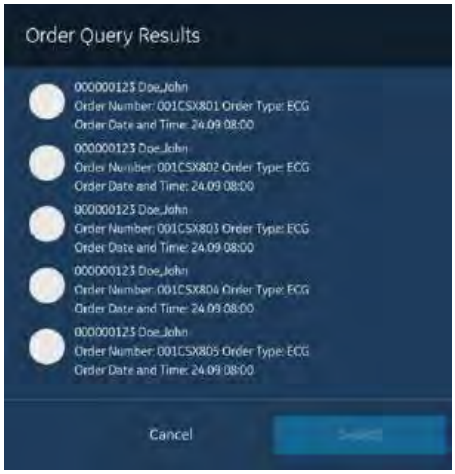
Make sure that you perform all the below steps to query orders then ADT from the EMR Gateway system:

- Set the user privileges to view the orders.
- Disable the **Order Management** in **Settings** > **Workflow** > **Order Manager**.
- Configure a DCP destination for the EMR Gateway system.
- Enable the **ADT/EMR Order Query** settings for DCP destination in **Settings** > **Workflow** > **Transmission & Query**.

NOTE

The EMR Gateway system must be V2 or higher.

1. The device first searches for remote orders in the EMR Gateway system with a **Patient ID** or **Visit Number**.
2. If, no orders found in the EMR Gateway system with a **Patient ID** or **Visit Number**. Then the device searches for ADT on the EMR Gateway system.

If	Then
Multiple remote orders are found on the EMR Gateway system.	More than one matching orders show on the Acquisition screen. Select the order you want to attach to the patient test. 
One remote order is found on the EMR Gateway system.	The order fills in the **Patient Information** screen, if there is no mismatch with the patient data on the screen.
No remote orders are found on the EMR Gateway system.	A message displays in the notification area that no matching remote orders are found. The device then searches for ADT data in the EMR Gateway system. • If only one ADT record is found on the EMR Gateway system: ◦ The patient demographics information fills in the **Patient Information** screen. ◦ A message displays in the notification area that matching ADT data is found. • If more than one ADT records are found on the EMR Gateway system: ◦ The matching records show on the Acquisition screen. ◦ A message displays in the notification area that matching ADT data is found.
No remote order/ADT records found on the EMR Gateway system.	A message displays in the notification area that no remote orders/ADT data found.
Remote order or ADT query failed on the EMR Gateway system.	A message displays in the notification area that remote order/ADT query has failed.

3. When, you find remote order.

If	Then
There is no data mismatch.	The patient demographics, order number, and other patient information that are available in the order is populated in the **Patient Information** screen. The order gets attached to the current test. Continue with ECG test.

Continues on the next page

If	Then

The patient data (other than patient demographics) does not match the patient data in the **Patient Information** screen.	A warning message displays on the screen:
	`Are you sure you want to attach this order to the current test?`
	`Name :`
	`Order :`
	`DOB :`
	`Existing patient data will be overwritten.`
	Select **Yes** to continue with the test, **No** to cancel the action.

4.3.2.5 ADT Query Workflow from the MUSE system

The device searches for ADT data in the MUSE system with the **Patient ID** or **Visit Number**.

If	Then
An ADT record that matches the **Patient ID** or **Visit Number** is found on the MUSE system	The patient demographics fills in on the **Patient Information** screen.
Multiple ADT records that match the **Patient ID** or **Visit Number** are found on the MUSE system	The matching records show on the Acquisition screen, and a message opens in the notification area that matching ADT data is found. Select a ADT record, and click **Select** to fill in the patient demographics on the **Patient Information** screen.
No ADT records that match the **Patient ID** or **Visit Number** are found on the MUSE system	A message opens in the notification area that no matching ADT data is found.
The ADT query failed	A message opens in the notification area that ADT query has failed.

NOTE

If multiple sites are configured on a MUSE system, ADT query is done only on Site 1, if the MUSE system version is MUSE v9 SP5 or earlier. ADT query to the MUSE system for sites other than Site 1 requires MUSE v9 SP6 or later.

4.3.2.6 ADT Query Workflow from the EMR Gateway system

Make sure that you perform all the below steps to query orders from the EMR Gateway system:

- Set the user privileges to view the orders.
- Disable the **Order Management** in **Settings** > **Workflow** > **Order Manager**.
- Configure a DCP destination for the EMR Gateway system.
- Enable the **ADT/EMR Order Query** settings for DCP destination in **Settings** > **Workflow** > **Transmission & Query**.

NOTE

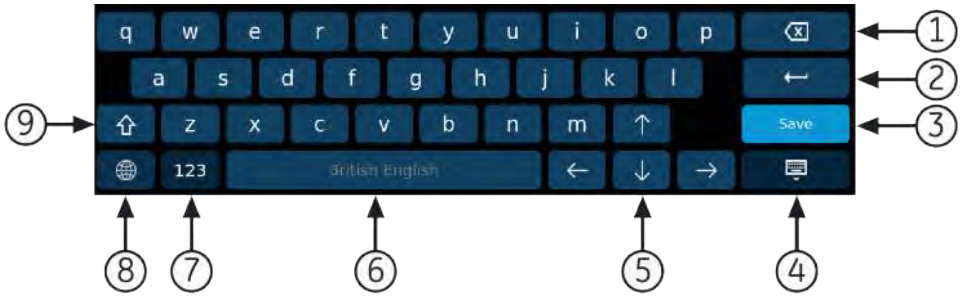
The EMR Gateway system must be V2 or higher.

The device searches for ADT data in the EMR Gateway system with a **Patient ID** or **Visit Number**.

If	Then
An ADT record that matches the **Patient ID** or **Visit Number** is found on the EMR Gateway system.	The patient demographics fills in on the **Patient Information** screen.
Multiple ADT records that match the **Patient ID** or **Visit Number** are found on the EMR Gateway system.	The matching records show on the Acquisition screen, and a message opens in the notification area that matching ADT data is found. Select a ADT record, and click **Select** to fill in the patient demographics on the **Patient Information** screen.
No ADT records that match the **Patient ID** or **Visit Number** are found on the EMR Gateway system	A message opens in the notification area that no matching ADT data is found.
The ADT query failed	A message opens in the notification area that ADT query has failed.

4.3.3 Enter or Edit Patient Information Using the Software Keyboard

Below is the software keyboard information:



Item	Name	Description
1	**Backspace** Key	Deletes inputs.
2	**Enter** Key	Enters inputs.
3	**Save** Key	Saves inputs.
4	**Minimize** Key	Minimizes the keypad from the screen.
5	**Arrow** Keys	Provides movement between columns.
6	**Space** Key	Adds a space between entered characters.
7	**Number** Key	Switches to numbers and symbols.
8	**Input Method**	Switches between different input methods. **NOTE** If you use an English user interface, you cannot switch the input methods from English to Chinese Pinyin. If you use the Chinese user interface, you can switch the input methods freely between English and Chinese Pinyin.
9	**Capitalization** Key	Capitalizes a letter during entering.

1. Enter data in the fields displayed in the **Patient Information** screen using the software keyboard. Only fields that are configured to be displayed in the **Patient Information** screen display. See

C.1 Patient Information Text Box Names on page 297 for a list of fields that can display on the screen.

- If the Pinyin input method is configured, when you enter data in the fields, a number list of matching Chinese characters displays in a drop-down menu. Select or enter the number of the desired value in the list to populate the Chinese character in the field.
- If you enter incorrect data in a field, the field border changes to red.
- An asterisk (*) displays adjacent to mandatory fields in the **Patient Information**.

NOTE

If you go to the **Settings** or **Service** screen before you complete a patient test, the data entered in the **Patient Information** screen clears when you go back to the **Acquisition** screen.

2. To save your entries, select **Save**.

   The information is saved and the **Patient Information** screen closes.

   Based on the **Mandatory fields apply for Transmission** or **Acquisition** settings, the ECG report will not be accepted, transmitted, or printed until you enter the patient demographic data for any of the mandatory fields. You need to complete the data for the mandatory fields.

4.4 Enter or Edit Clinical Trial

1. Enter data in the fields displayed in the **Clinical Trial** screen using the software keyboard. Only fields that are configured to be displayed in the **Clinical Trial** screen display. See C.2 Clinical Trial Text Box Names on page 303 for a list of fields that can display on the screen.
   - If the Pinyin input method is configured, when you enter data in the fields, a number list of matching Chinese characters displays in a drop-down menu. Select or enter the number of the desired value in the list to populate the Chinese character in the field.
   - If you enter incorrect data in a field, the field border changes to red.
   - An asterisk (*) displays adjacent to mandatory fields in the **Clinical Trial**.

   NOTE

   If you go to the **Settings** or **Service** screen before you complete a patient test, the data entered in the **Clinical Trial** screen clears when you go back to the **Acquisition** screen.

2. To save your entries, select **Save**.

   The information is saved and the **Clinical Trial** screen closes.

   Based on the **Make All Clinical Trial Fields Mandatory** setting, the ECG report will not be accepted, transmitted, or printed until you enter the clinical trial data for any of the mandatory fields. You need to complete the data for the mandatory fields.

5 Record an ECG or Rhythm

5.1 Hookup Advisor Overview

The **Hookup Advisor** module is a visual indication of the quality of lead signals. It can help reduce or eliminate poor quality ECGs and prevent the need to take additional ECGs.

The **Hookup Advisor** reports the status based on signals from each leadwire. Connect the RA/R leadwire, and then another leadwire to the patient, an electrode placement image expands in the **Hookup Advisor** panel. If all leadwires are disconnected from the patient, the electrode placement image collapses after a few seconds.

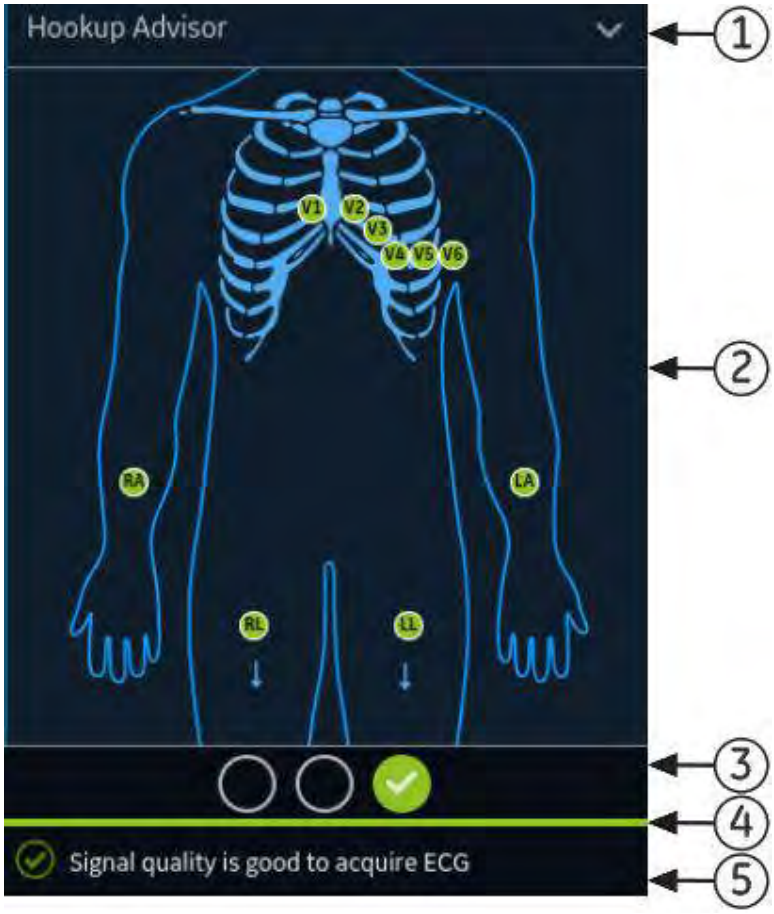


Table 5-1 Hookup Advisor Panel

Item	Name	Description
1	**Collapse** arrow	Select the arrow to collapse the electrode placement image.

Continues on the next page

Table 5-1 Hookup Advisor Panel (Table continued)

Item	Name	Description
2	Electrode Placement Image	Displays electrode placement and quality of each lead. Each lead quality indicator changes color to red, yellow or green, based on its connection status. On the Acquisition screen, the image displays the real-time electrode quality of each lead. During review of a patient report, all electrode lead quality indicators are turned off. You can set up a lead condition indicator in settings, if the **Hookup Advisor** level is configured as: • **Yellow**, the image automatically expands when the **Hookup Advisor** status is yellow or red in the Acquisition screen, or during preview of an ECG patient report. • **Red**, the image automatically expands when the **Hookup Advisor** status is red in the Acquisition screen, or during preview of an ECG patient report. The image collapses during review of a patient report, irrespective of the overall **Hookup Advisor** status. • **Never**, the image does not automatically expand when the overall **Hookup Advisor** status is yellow or red. Only the **Hookup Advisor** lead quality status indicator and status messages display in the Notification Area.
3	Lead Quality Status Indicator	Displays three circles that change color to yellow, red, or green, based on the overall lead quality. This indicator does not apply to review of rhythm reports.
4	Status Bar	Displays a solid color bar that matches the same color as the lead quality status indicator. For example, if the lead quality status indicator is green, the status bar displays a solid green color. In the pre-acquisition (refer to 5.6 ECG Acquisition Overview on page 64) mode , when the lead quality status indicator changes from red or yellow to green, the status bar shows a progress bar of acquiring 10 seconds of ECG data with good quality.
5	Notification Area	Displays lead quality status messages indicating the specific problem in each lead. Messages display one at a time. If there are more than one failures, messages for red states display first. When you resolve a problem, the next message displays. Continue to resolve the problems until the indicator is green.

Table 5-2 Lead Quality Indicators on the Electrode Placement Image

Lead Quality Indicator	Description
Green	The leadwire connection is good. The acquisition module is sending a good signal to the device.
Yellow	The leadwire connection experiences noise, the signal is not clear, or there is a potential lead reversal condition.
Red	The lead is disconnected or not receiving a usable signal.
No color (unlit)	No ECG data is being acquired.

Table 5-3 Hookup Advisor Lead Quality Status Indicators

Indicator	Description
Red 	Shows a lead fail condition or extreme baseline shifts. The red indicator is always the left circle of the indicator. It flashes on and off approximately each second and contains an X symbol. The two circles to the right are black. A message displays with information to help you resolve the problem.

Continues on the next page

Table 5-3 Hookup Advisor Lead Quality Status Indicators (Table continued)

Indicator	Description
Yellow 	Shows muscle artifact, power line interference, baseline wander, or electrode noise. Potential lead reversal condition. The yellow indicator is always the middle circle of the indicator and contains a dash. The left and right circles are black. A message displays with information to help you resolve the problem.
Green 	Shows acceptable signal quality. The green indicator is always the right circle of the indicator and contains a check mark. The two circles to the left are black. A message displays showing that the signal lead quality is good to acquire an ECG.

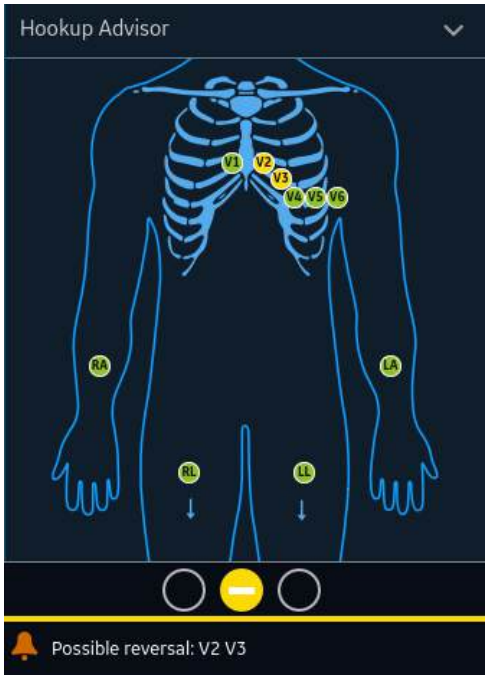
NOTE

The background color of the **Start ECG** icon is green, when the **Hookup Advisor** status is green. The background color of the **Start ECG** icon is blue, when the **Hookup Advisor** status is red or yellow.

If the **Hookup Advisor** status is red or yellow, check the patient's skin, see B.1 Prepare the Patient's Skin on page 295.

Lead Reversal Detection:

- The Hookup Advisor displays the lead quality status in yellow when lead reversal has been detected.



- Lead reversal detection is skipped for any electrode that is NOT green lead quality.
- Lead reversal detection is not performed when the patient age is ≤ 15 years.

NOTE

If you change the patient age from greater than 15 years to less than or equal to 15 years with the leads reversed, the interpretation statement on the ECG report in the

preview screen will not display the lead reversal. The Hookup Advisor in the preview screen will continue to display the lead reversal.

- If the age is not entered, lead reversal detection is performed.
- The chest lead reversal detection is skipped if any reversals are detected in the limb electrodes.
- Lead reversal detection is skipped for extra leads.
- Ten seconds of green lead quality must display on all leads for lead reversal detection to be performed. The Hookup Advisor may display the green lead quality before it changes to yellow when lead reversal is detected.
- Refer to *Marquette™ 12SL™ ECG Analysis Program Physicians Guide* for more information on lead reversal detection.

If a leadwire is disconnected, the overall status shows as failed (red). To determine which leadwire has failed, you need to understand which electrodes are used to form a lead. If RA is the reference electrode and it is not connected, all the electrodes display as failed. If another leadwire is the reference electrode and it is not connected, only that electrode displays as failed.

CAUTION

ELECTRICAL INTERFERENCE

Electrostatic discharges may interfere with the acquisition of ECG recordings. The acquisition module could be temporarily disconnected with an error message displayed due to an ESD event. The device recovers automatically from this error. ECG recordings need to be restarted after the error message is removed and the acquisition module recovers.

If the device does not recover from the error, troubleshoot the error. Restart the ECG after the error is resolved and the **Hookup Advisor** displays a green status. After you resolve the errors, the electrode placement image collapses after the **Hookup Advisor** status indicator is green for at least four seconds.

The preview or review of a patient report is based on the **Hookup Advisor** status at the time of ECG acquisition, and not the real-time status of a currently connected patient.

5.1.1 Acquire an ECG based on the Hookup Advisor status in Post-Acquisition Mode

In post-acquisition mode (refer to 5.6 ECG Acquisition Overview on page 64), the next 10 seconds of ECG data is acquired when you start to record an ECG.

Review the Hookup Advisor status before you start an ECG. If the Hookup Advisor status is green, it shows that the signal quality is good, you can start to record an ECG that acquires the next 10 seconds of ECG data.

- If the status stays green during the 10 seconds ECG acquisition, you can accept the ECG.
- If the quality of the ECG signal has problems during the 10 seconds ECG acquisition, the status changes from green to yellow or red.

  It is recommended to reject an ECG that is acquired in the post-acquisition mode with poor signal quality.

5.1.2 Acquire an ECG based on the Hookup Advisor status in Pre-Acquisition Mode

In pre-acquisition mode (refer to 5.6 ECG Acquisition Overview on page 64), the previous 10 seconds of ECG data is acquired when you start to record an ECG.

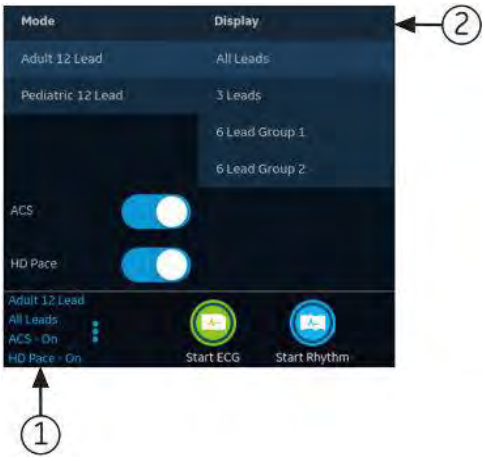
Review the Hookup Advisor status before you start an ECG:

- If the status is green, it shows that the previous 10 seconds of ECG data is good. You can start to record an ECG.
- If the status changes from green to yellow or red, it shows that the quality of the ECG signal is not good. A message displays for the most critical state in the last 10 seconds.
- If the status changes from yellow or red to green, Hookup Advisor displays a message that you need to wait for 10 seconds before you start to record an ECG.

5.2 Change Lead Sets and Lead Formats

The Acquisition screen displays the waveform based on the configured lead format, lead set, speed, gain, and filter. After you start a new patient, you can change the lead set or lead format on the Acquisition screen.

1. At the bottom, left-side of the Acquisition screen, select anywhere to the left of the ellipsis icon (1).



   The **Mode** and **Display** menus (2) are expanded.

2. Select a different lead set below **Mode**.

   If you change the lead set, it resets the acquisition of data and cannot be done while recording or printing a rhythm.

   The selected lead set is applied to the waveform.

3. Select a different lead format below **Display**.

   The selected lead format is applied to the waveform. Select anywhere outside the menu to collapse it.

   These changes apply only to the current patient test(s). If you start a new patient, the changes reset to the values configured for the device.

5.3 Enable ACS Interpretation

You can enable the ACS option on the Acquisition screen before you record an ECG patient test if the ACS option, which detects Acute Coronary Syndrome, is bought and activated on the device.

This option records a resting ECG with ACS interpretation statements. By default, ACS interpretation statements are disabled for each patient. ACS must be enabled on a per-patient basis.

1. At the bottom, left side of the Acquisition screen, select anywhere to the left of the ellipsis icon (1).

   The **ACS** option displays in the expanded menu.

2. Turn the **ACS** option (2) on to enable ACS interpretation statements for the patient report.

   If you enable this option, it will stay enabled for the subsequent patient test(s) for that visit. It must be enabled again for the next patient.

   If the patient demographics show that the patient is younger than 16 years of age, the device records a pediatric ECG with a standard 12SL analysis. The ACS algorithm is not executed.

5.4 Enable HD Pace

The HD Pace option enables or disables the HD Pace Detection, and display the suspected pace annotation for patients with a pacemaker. The pace annotations represent pacemaker pulses.

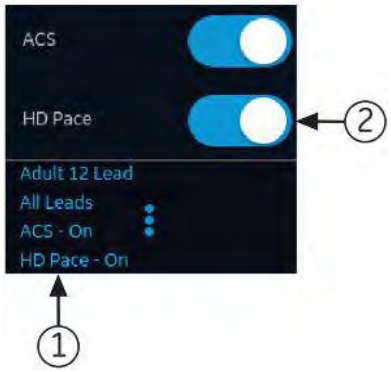
Suspected Pace Annotations

NOTE

It is recommended that a qualified physician or cardiologist review and confirm the suspected pace spike.

By default, the **HD Pace** option is enabled for each patient. You can manually disable the **HD Pace** option on the **Acquisition** screen before you record an ECG patient test.

1. At the bottom, left side of the Acquisition screen, select anywhere to the left of the ellipsis icon (1).



NOTE

The **HD Pace** option will be automatically set as enabled after you start a new patient or reboot the device. Configure the **Default HD Pace** setting to change the default value of the **HD Pace** option, refer to 10.4.1 Configure ECG Acquisition on page 118.

The **HD Pace** option displays in the expanded menu.

2. Turn the **HD Pace** option (2) off to disable the HD Pace Detection.

   When **HD Pace** is off, `HD Pace Off` displays on the footer of the report.

   When **HD Pace** is on, no additional information displays on the report.

5.5 Change Speed, Gain, and Filter

The Acquisition screen displays the waveform from the configured speed, gain, and filter. After you start a new patient, you can change the speed, gain, or filter on the Acquisition screen.

1. At the bottom, right-side of the Acquisition screen, select anywhere to the left of the ellipsis icon.

   The **Filter (Hz)**, **Speed (mm/s)**, and **Gain (mm/mV)** menu expands.

   - If you do not purchase the **F300 - 300 Hz Acquisition** option, the **Filter (Hz)** values are 20, 40, 100 and 150.
   - If you purchase the **F300 - 300 Hz Acquisition** option and the **Acquisition Bandwidth** of the selected lead set is **150Hz**, the **Filter (Hz)** values are 20, 40, 100 and 150.

   - If you purchase the **F300 - 300 Hz Acquisition** option and the **Acquisition Bandwidth** of the selected lead set is **300Hz**, the **Filter (Hz)** value is 300.

NOTE

The 150 Hz acquisition bandwidth setting reduces signal frequencies above 150 Hz. The 300 Hz acquisition bandwidth setting reduces signal frequencies above 300 Hz, providing the least amount of filtering and the highest signal fidelity and may be appropriate for pediatric ECG acquisition. Refer to the *12SL Physician's Guide* for more information.

The 150 Hz filter is commonly used for adult patients and the 300 Hz filter is intended for use for pediatric (usually newborn) patients.

2. To adjust the speed, gain, and filter of the waveform, select a different value from the list that is available on expanding the ellipsis icon.

   The selected values are applied to the waveform. Select anywhere outside the menu to collapse it.

   These changes apply only to the existent patient test(s). If you start a new patient, the changes reset to the values configured for the device.

5.6 ECG Acquisition Overview

You can record an ECG in pre-acquisition or post-acquisition modes.

Table 5-4 ECG Acquisition Modes

Acquisition Mode	Description
Pre-acquisition	When you start recording an ECG: • If 10 seconds of ECG data is available, the system records the previous 10 seconds of data for analysis. • If 10 seconds of ECG data is not available, the system continues recording until 10 seconds of ECG data is obtained.
Post-acquisition	When you start recording an ECG, the system records the next 10 seconds of data for analysis.

If the **Auto-ECG** option is enabled on the device, the device automatically records one ECG for each new patient. For more information on automatic ECG acquisition, see 5.6.1 Automatically Acquire an ECG on page 64.

To record an ECG patient test manually, see 5.6.2 Manually Start an ECG recording on page 65.

5.6.1 Automatically Acquire an ECG

Start a test for a new patient. For more information, see 4.2 Start a Test for a New Patient on page 44.

Make sure that your administrator enables the **AECG - Auto ECG** option.

The system starts to automatically record an ECG:

- When **AECG - Auto ECG** option is enabled.

- If the **Hookup Advisor** status is green.
- If you are viewing the scrolling waveforms in the **Home** tab.

The automatic acquisition of ECG happens only once per patient connection.

The **Stop Auto ECG** icon displays the count of acquisition progress until you record 10 seconds of data. After acquiring 10 seconds of data with good signal quality, the recording stops and a preview of the ECG patient report displays.

If you record the ECG before you enter patient information in the **Patient Information** screen, you can edit patient information before accepting the preview. For more information, see 5.6.4 Accept or Reject an ECG Patient Report on page 67.

Automatic ECG acquisition is triggered only one time for the current patient test. Start any new ECG tests for that same patient manually.

When Auto-ECG is in progress, the **Start ECG** button changes to the **Stop ECG** button:

- If you select the **Stop ECG** button, automatic ECG acquisition stops and the **Start ECG** button displays.
- If you select the **Start ECG** button, ECG acquisition starts manually.

If you perform other functions during automatic ECG acquisition, a message displays in the notification area. For example:

- If you perform New Patient - a message displays that **unsaved data will be lost.**
- If you navigate to Settings - a message displays that **cannot perform this action.**

Select **Cancel**, to continue to perform automatic ECG acquisition and retain current patient data. If you select **Continue**, automatic ECG acquisition stops.

The automatic ECG function is aborted and the device will function in manual ECG mode if:

- An automatic ECG acquisition is stopped before 10 seconds of data is acquired.
- The preview of an ECG that was automatically acquired is rejected.

5.6.2 Manually Start an ECG recording

1. Start a test for a new patient. For more information, see 4.2 Start a Test for a New Patient on page 44.

   NOTE

   If you want to record an ECG for the current patient, do not start a new patient test.

2. Change the lead set or format, gain, speed, or filter, if required. For more information, see 5.2 Change Lead Sets and Lead Formats on page 61 and 5.5 Change Speed, Gain, and Filter on page 63.
3. Select the **Start ECG** icon at the bottom of the **Acquisition** screen to start recording the patient ECG.

   In pre-acquisition mode, the system checks if 10 seconds of ECG data is available.

- If 10 seconds of ECG data is available, the system records the previous 10 seconds of data for analysis. You cannot stop or cancel the acquisition at this time.
- If 10 seconds of ECG data is not available, the system continues recording until 10 seconds of ECG data is obtained. The **Start ECG** icon changes to **Stop ECG**, and the count of acquisition progress displays on the icon until you have recorded 10 seconds of data. You can cancel the acquisition before 10 seconds of data is recorded. For more information, see 5.6.3 Cancel an ECG on page 67.

In post-acquistion mode, the system starts recording the next 10 seconds of ECG data for analysis. The **Start ECG** icon changes to **Stop ECG**, and the 10 seconds count of acquisition progress displays on the icon. You can cancel the acquisition before 10 seconds of data is recorded. For more information, see 5.6.3 Cancel an ECG on page 67.

The patient ECG test report starts generating. Based on the print preview mode configuration and the **Hookup Advisor** status, the recorded ECG patient test opens.

If ...	Then ...
Print preview mode is configured as **Always**	The ECG patient report preview displays for you to accept or reject the report. For more information on how to accept or reject the report, see 5.6.4 Accept or Reject an ECG Patient Report on page 67.
Print preview mode is configured as **Yellow** and the Hookup Advisor Status is **Yellow** or **Red**	
Print preview mode is configured as **Red** and the Hookup Advisor Status is **Red**	
Print preview mode is configured as **Yellow** and the Hookup Advisor Status is **Green**	The ECG patient report preview does not display. The ECG patient report is automatically accepted, saved in the **Files** list, and displayed for review. For more information, see 5.6.5 Review an ECG Patient Report on page 71. The report is automatically printed. For more information, see 5.6.6 Automatically Print an ECG Patient Report on page 72. If a destination is configured for ECG reports to be automatically sent after acquisition, the ECG report is automatically added to the queue of pending reports to be sent to the configured destination. For more information, see 8.1 Display the Report Queue on page 110. **NOTE** Based on the **Mandatory fields apply for Transmission** settings, the ECG report is not added to the transmission queue until you enter the patient demographic data for the mandatory fields. An error message displays in the notification area. You need to complete the data for the mandatory fields and manually resend the report to a configured destination. **NOTE** Based on the **Mandatory fields apply for Acquisition** settings, the ECG report is not accepted, transmitted, or printed until you enter the patient demographic data for the mandatory fields. An error message **Unable to accept. Incomplete patient data.** displays on the **Acquisition** screen. You need to complete the data for the mandatory fields to accept the ECG report.
Print preview mode is configured as **Red** and the Hookup Advisor Status is **Yellow** or **Green**	
Print preview mode is configured as **Never**	

5.6.3 Cancel an ECG

You can stop recording an ECG before 10 seconds of data are recorded.

1. Select the **Stop ECG** icon at the bottom of the Acquisition screen to cancel the ECG acquisition:

The device stops recording the ECG data and the **Start ECG** icon displays.

5.6.4 Accept or Reject an ECG Patient Report

CAUTION

DELAY IN TREATMENT

Unaccepted ECGs in the preview screen will be automatically rejected and deleted when all patient leads are disconnected and the MAC 5 device is inactive for 2 minutes.

A preview of the recorded 10 seconds of data displays in the configured preview report format if:

- The ECG is recorded in automatic ECG mode.
- Your administrator has configured the preview mode to display the recorded 10 seconds of data.
- The 10 seconds of ECG is selected from the Full Disclosure screen.

NOTE

The **FD** tab displays after you purchase and enable the **FLDS - Full Disclosure** option.

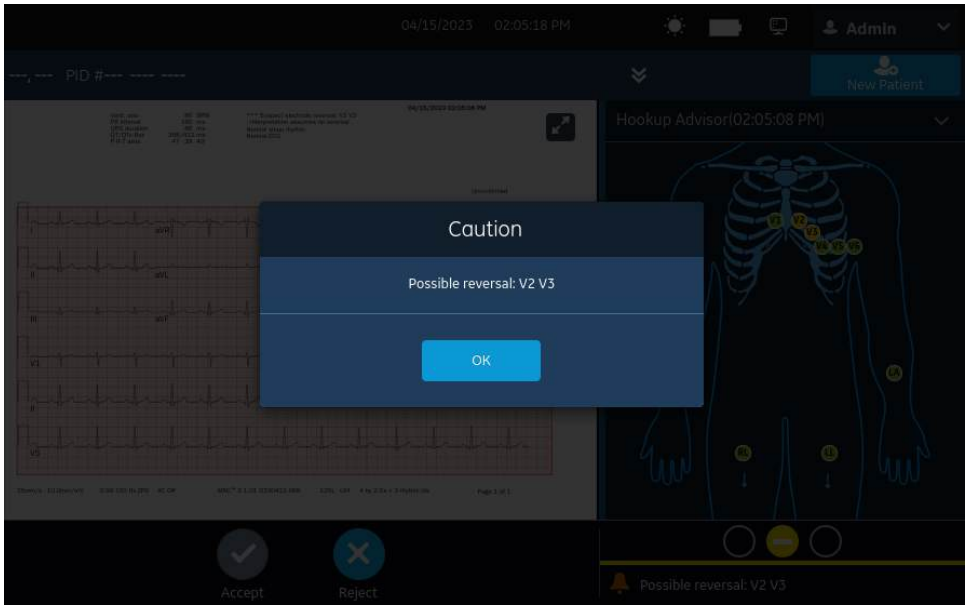
You can accept this preview to save the ECG patient report in the **Files** tab, or reject it and start another ECG.

Table 5-5 Preview of the ECG Patient Report

Item	Name	Description
1	**Patient Information** banner	Displays patient information. Select anywhere in the **Patient Information** banner to edit patient information for the patient report. Modify the information by using the software keyboard, attaching an order, scanning the patient barcode, selecting a patient from the **Patients** tab, or performing an ADT query.
2	Preview of ECG patient report	Displays the preview of the ECG patient report. If a patient report contains multiple pages, a part of another page displays on the right side of the screen. Press the left and right arrows on the screen to navigate from one page to another. For more information on the report formats and the standard layout of the ECG patient report, see A.1 ECG Report Formats on page 286.
3	**Reject** icon	Select the **Reject** icon to return to the live waveform display in the **Acquisition** screen.
4	**Accept** icon	Select the **Accept** icon to accept the preview of the ECG patient report and save it in the **Files** list. The accepted ECG patient report is refreshed and displayed for review with additional options.

To accept or reject the ECG preview, perform the steps as follows:

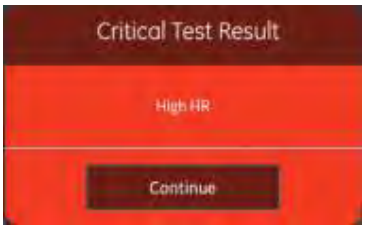
1. Review the patient report and **Hookup Advisor** status.
2. If lead reversal detection is performed during ECG acquisition, a notification displays with lead information. Select **OK** to acknowledge the notification.



NOTE

The lead reversal notification does not display if you set the **Print Preview Mode** to **Never**.

3. If the **CRIT- Critical Value Notifications** option is enabled on the device, and one or more critical values are detected during ECG acquisition, a window opens on top of the screen displaying critical value notifications in the order in which they are detected.



4. Select **Continue** to acknowledge each notification.

   If you try to perform other functions such as accessing the **Settings** or **Service** screen prior to accepting or rejecting the ECG, a message displays indicating that the ECG is not saved, and the preview will be lost if you navigate to the screen.

   Select one of the options as follows:

   - If you select **Continue**, the preview will be lost.
   - If you select **Cancel**, you can proceed to accept or reject the ECG preview.

5. Accept or reject the ECG preview based on the **Hookup Advisor** status.

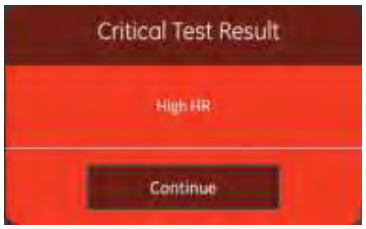
If ...	Then ...	Next Steps
Hookup Advisor status is green, the ECG signal quality is good. The **Accept** icon is highlighted in green. The **Reject** icon is not highlighted.	Select the **Accept** icon: The preview of the ECG patient report is accepted and saved in the **Files** list. The patient report is refreshed and displayed for review with additional options.	• Review the ECG patient report and decide on the next steps. For more information, see 5.6.5 Review an ECG Patient Report on page 71. • The ECG patient report is automatically printed. For more information, see Autoprint an ECG Report on page 72. • The patient report is added to the queue of pending reports to be sent to the configured automatic destination. For more information, see 8.1 Display the Report Queue on page 110. **NOTE** Based on the **Mandatory fields apply for Transmission** settings, the ECG report is not added to the transmission queue until you enter the patient demographic data for the mandatory fields. An error message displays in the notification area. You need to complete the data for the mandatory fields and manually resend the report to a configured destination. **NOTE** Based on the **Mandatory fields apply for Acquisition** settings, the ECG report is not accepted, transmitted, or printed until you enter the patient demographic data for the mandatory fields. An error message **Unable to accept. Incomplete patient data.** displays on the **Acquisition** screen. You need to complete the data for the mandatory fields to accept the ECG report.
Hookup Advisor status is yellow or red, there are issues with the ECG signal quality during the recording of this ECG. The **Reject** icon is highlighted in blue to reflect the status of **Hookup Advisor**. The **Accept** icon is not highlighted.	Select the **Reject** icon:  The ECG patient report is discarded. The **ECG Preview** screen closes and returns to the **Acquisition** screen.	Start a new ECG on the same patient. For more information, see 5.6 ECG Acquisition Overview on page 64.

5.6.5 Review an ECG Patient Report

The reviews of ECG patient reports are automatically closed 2 minutes after disconnecting patient leads and inactivity with the MAC 5 device.

After the 10 seconds ECG is acquired and the ECG preview is accepted, the patient report displays in the configured report format for review.

If the **CRIT - Critical Value Notifications** option is enabled on the device, and one or more critical values are detected during ECG acquisition, a window opens on the top displaying the notifications for the critical values in the order in which they are detected.



Select **Continue** to acknowledge the notification and proceed with other tasks.

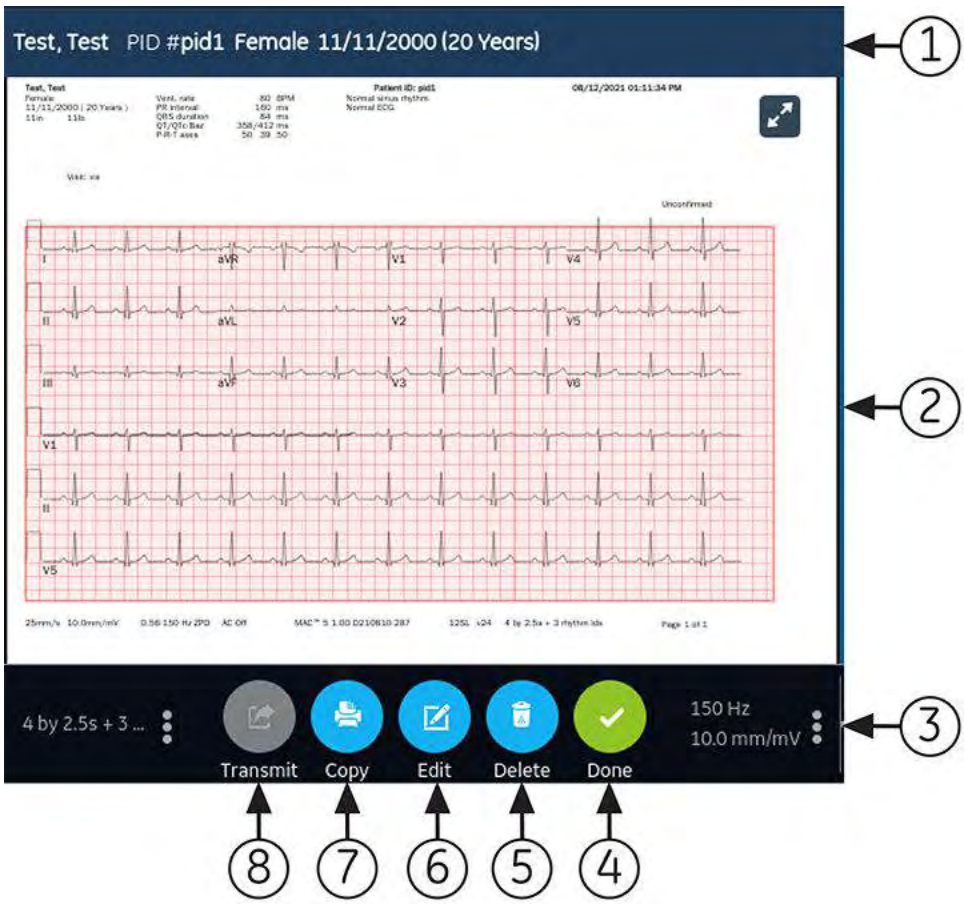


Table 5-6 Displaying an ECG Patient Report for Review

Item	Name	Description
1	**Patient Information** banner	Displays patient information such as patient first name, last name, gender, age, and so on. Select anywhere in the **Patient Information** banner to edit patient information for the patient report.
2	ECG patient report	Displays the ECG patient report. If a patient report contains multiple pages, a part of another page displays on the right side of the screen. Select the left and right arrows on the screen to navigate from one page to another. For more information on the report formats and the standard layout of the ECG patient report, see A.1 ECG Report Formats on page 286.
3	Gain and Filter	To change the waveform gain or filter, select anywhere around the ellipsis icon next to **Gain** and **Filter** and select a new value from the expanded list. The patient report is refreshed with the selected gain and filter.
4	**Done** icon	Closes the patient report after completing your tasks. For more information, see 5.13 Close a Patient Report on page 82.
5	**Delete** icon	Deletes the patient report. For more information, see 5.11 Delete a Patient Report on page 81.
6	**Edit** icon	Edits patient information for the patient report. For more information, see 5.10 Edit Patient Information in a Patient Report on page 81.
7	**Copy** icon	Prints a copy of the patient report. For more information, see 5.9 Print a Patient Report on page 78.
8	**Transmit** icon	Transmits the patient report. For more information, see 5.8 Transmit a Patient Report to a Configured Destination on page 76.

To start a new ECG on the same patient, close the review page to return to the live waveform display in the **Acquisition** screen, and restart the ECG. For more information, see 5.6 ECG Acquisition Overview on page 64.

After you select **Done** on the **Review** screen of an ECG patient report, disconnect patient leads before you select **New Patient** on the MAC 5 device.

To start an ECG for a new patient, select **New Patient**. For more information, see 4.2 Start a Test for a New Patient on page 44.

To start a new 10 seconds ECG on the same patient from the Full Disclosure tab, close the preview page to navigate to the Full Disclosure waveform and application, and select 10 seconds ECG from the Full Disclosure waveform. For more information, see 5.14.1 Record a Full Disclosure ECG on page 83.

5.6.6 Automatically Print an ECG Patient Report

When a patient report is saved in the **Files** list, it is automatically printed in the configured report formats.

The configured report formats determine the following:

- Number of copies printed
- Inclusion or exclusion of 12SL interpretation statements
- Printing of all reports
- Printing of only the reports interpreted by the 12SL analysis as abnormal

The ECG patient report is printed in the order in which it was received. If no other patient reports are printing, the report is printed immediately.

You will see a progress message at the bottom of the screen indicating the printing status.

If the device is configured to print the barcode of the patient ID in the patient reports, the printed patient report includes the barcode. The barcode can be used to perform a query by patient ID in the MUSE system.

If a printer error occurs, the progress message is replaced by the related printer error. The printing restarts automatically after the error is resolved. For more information on printer errors, see 13.3 Printing Errors on page 274.

To stop printing a patient report, select the **Stop** icon in the middle of the screen.

All pending print jobs are cancelled.

5.7 Record a Rhythm

Make sure that sufficient paper is available in the paper tray to print a rhythm report.

If the **DRHM - Digital Rhythm** option is purchased and enabled on the device, a rhythm report can be stored in digital form in the **Files** list or printed on paper, depending on how the device has been configured for your site. A digital rhythm report cannot be transmitted to a configured automatic destination.

1. Start a test for a new patient. See 4.2 Start a Test for a New Patient on page 44.
2. Change the lead set or format, gain, speed, or filter, if required. See 5.2 Change Lead Sets and Lead Formats on page 61.
3. Select the **Start Rhythm** icon on the Acquisition screen to start the rhythm for the patient.

The **Start Rhythm** icon on the **Acquisition** screen changes to **Stop Rhythm**. A count of the recording progress starting at one-second displays on the icon if the configured rhythm mode is **Digital Only** or **Both**.

If the **Delay Rhythm Printing** option is disabled, the rhythm for the patient is recorded and/or printed in real-time.

If the **Delay Rhythm Printing** option is enabled, the rhythm for the patient is recorded and/or printed with the previous 10 seconds data.

If the Rhythm Mode is ...	Then
Paper Only	The rhythm is only printed. It is not digitally recorded. Go to Step 4 to stop printing the rhythm. If you do not stop printing the rhythm, printing continues until the paper tray is out of paper. **NOTE** **Paper Only** is available on A4 and A5 devices.

Continues on the next page

If the Rhythm Mode is ...	Then
Digital Only	The rhythm is only digitally recorded in real-time at the configured speed and for the configured duration. When the configured duration is reached, the rhythm stops recording. The digital rhythm report is displayed in a new **Rhythm** tab and saved in the **Files** list. The rhythm is not printed. Go to Step 4 if you want to stop recording the rhythm before its configured duration is reached, otherwise go to Step 5. **NOTE** **Digital Only** is available only if you enable the **DHRM - Digital Rhythm** option.
Both	The rhythm for the patient is digitally recorded and printed in real-time at the configured speed and for the configured duration. When the configured duration is reached, the rhythm stops recording and printing. The digital rhythm report is displayed in a new **Rhythm** tab and saved in the **Files** list. Go to Step 4 if you want to stop recording and printing the rhythm before its configured duration is reached, otherwise go to Step 5. **NOTE** **Both** is only available on A4 and A5 devices when you enable the **DHRM - Digital Rhythm** option.

If a printer error occurs and rhythm printing is stopped, you need to troubleshoot the error. For more information, see 13.3 Printing Errors on page 274. Digital rhythm continues even if there is a printing error. To restart rhythm printing, you must stop the digital rhythm and then restart both.

4. Select the **Stop Rhythm** icon on the **Acquisition** screen to stop both digital rhythm recording and printing:

Select the **Stop** icon on the Report Printing screen to stop printing the rhythm report while the digital acquisition of rhythm continues.

5. Review the rhythm report. For more information, see 5.7.1 Review a Digital Rhythm Report on page 74.

5.7.1 Review a Digital Rhythm Report

If the Digital Rhythm option is purchased and activated on the device, a rhythm report can be stored in digital form.

After the digital rhythm report is recorded, the report displays for your review.

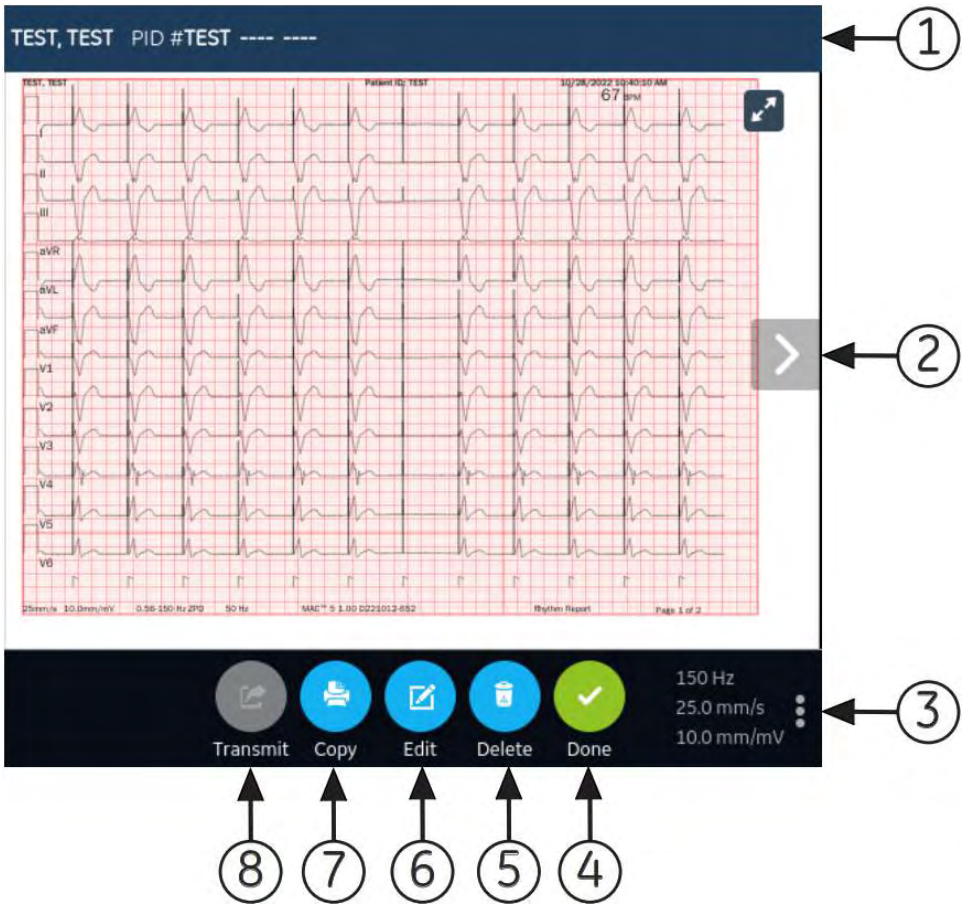


Table 5-7 Rhythm Tab

Item	Name	Description
1	**Patient Information** banner	Displays patient information such as patient first name, last name, gender, age, and so on. Select anywhere in the **Patient Information** banner to edit patient information for the rhythm report.
2	Rhythm report	Displays the rhythm report. If a rhythm report contains multiple pages, press the left and right arrows on the screen to navigate from one page to another. For more information on the rhythm report format, see A.2 Rhythm Report Format on page 290.
3	Gain, Filter, and Speed	To change the gain, filter, or speed of the waveform, select anywhere around the ellipsis icon on the lower, right corner of the **Rhythm** tab and select a new value from the expanded list. The rhythm report is refreshed with the selected gain, filter, and speed.
4	**Done** icon	Closes the rhythm report after completing your tasks. For more information, see 5.13 Close a Patient Report on page 82.
5	**Delete** icon	Deletes the rhythm report. For more information, see 5.11 Delete a Patient Report on page 81.
6	**Edit** icon	Edits patient information for the rhythm report. For more information, see 5.10 Edit Patient Information in a Patient Report on page 81.
7	**Copy** icon	Prints a copy of the rhythm report. For more information, see 5.9 Print a Patient Report on page 78.
8	**Transmit** icon	Transmits the rhythm report. For more information, see 5.8 Transmit a Patient Report to a Configured Destination on page 76.

To start a new rhythm for the same patient, close the review screen to return to the live waveform display in the **Acquisition** screen, and restart the rhythm. For more information, see 5.7 Record a Rhythm on page 73.

To start a rhythm for a new patient, select **New Patient**. For more information, see 4.2 Start a Test for a New Patient on page 44.

5.8 Transmit a Patient Report to a Configured Destination

Before you start the procedure, make sure that:

- You have the privilege to transmit patient reports to a configured destination.
- The USB flash drive supports the FAT32 file system.

Select the correct destination for your patient report. For more information, see the table below:

Patient Report Type	Destination	Supported File Format
Resting ECG	DCP server destination (MUSE v9 or MUSE NX and MUSE DICOM Gateway Pro SP1 or higher)	Hilltop format
Resting ECG	USB R/W flash drive	PDF, Hilltop and Sapphire XML (Sapphire XML format is available if you enable the XML format output in the **Option Manager**) formats.
Resting ECG	SFTP server destination with remote directory path	PDF, Hilltop and Sapphire XML (Sapphire XML format is available if you enable the XML format output in the **Option Manager**) formats.
Resting ECG	Shared directory destination with folder path	PDF, Hilltop and Sapphire XML (Sapphire XML format is available if you enable the XML format output in the **Option Manager**) formats.
Digital Rhythm	USB R/W flash drive	PDF format
Digital Rhythm	DCP server destination (MUSE v9 SP6 or higher, or MUSE NX and MUSE DICOM Gateway Pro SP6 or higher)	PDF format
Digital Rhythm	SFTP server destination with remote directory path	PDF format
Digital Rhythm	Shared directory destination with folder path	PDF format
Full Disclosure	USB R/W flash drive	PDF format
Full Disclosure	DCP server destination (MUSE v9 SP6 or higher, or MUSE NX and MUSE DICOM Gateway Pro SP6 or higher)	PDF format
Full Disclosure	SFTP server destination with remote directory path	PDF format
Full Disclosure	Shared directory destination with folder path	PDF format

To transmit a patient report to the default or configured destination immediately after acquisition, perform the steps below:

1. Review the patient report to confirm that it can be transmitted to the required destination.

   To review an ECG patient report, see 5.6.5 Review an ECG Patient Report on page 71.

To review a rhythm report, see 5.7.1 Review a Digital Rhythm Report on page 74.

To review a Full Disclosure report, see 5.14.2 Review a Full Disclosure Report on page 85.

2. To transmit the report to the required destination, perform one of the steps below:

To transmit the report ...	Perform the following:
To the default destination	Select the **Transmit** icon: 
To another configured destination	1. Select anywhere around the ellipsis icon on the left, bottom corner of the tab to view the **Transmit** menu. 2. From the expanded **Transmit** menu, select the destination where you want to transmit the patient report. 3. Select the **Transmit** icon:  One or more destinations must be configured for the **Transmit** icon to be enabled. If no destinations are configured, the **Transmit** icon is disabled.

The selected patient report is added to the **Queue**, processed and transmitted to the selected destination. The **Job Status** in the **Queue** is updated. For information on the status, see 8.1 Display the Report Queue on page 110.

The status of a manually submitted job displays on the notification bar in the lower, right-side of the screen in the format: `<Destination_Name>: <Job_Status>`.

For example, if the destination name is USB, and the job status is **Failed**, the status displays as follows: `USB: Failed`.

A tick mark displays in the **Sent** column of the **Files** expanded list for patient reports successfully transmitted to the default destination.

If	Then
The transmission queue has reached its maximum limit of 1000 reports, a message displays in the notification area that the transmission queue is full and no additional reports can be added.	Wait for the reports in the queue to transmit and try again.
The patient report has already been transmitted to the selected destination, a message displays in the notification asking you to confirm if you want to re-transmit the already transmitted report.	Perform one of the actions below: • Select **Continue** to re-transmit the patient report. • Select **Cancel** to cancel the report transmission.

Continues on the next page

If	Then
Patient information is incomplete in the patient report (for example, mandatory fields are blank or contain invalid data), a message displays in the notification area indicating that the patient report cannot be transmitted because of incomplete patient data. **NOTE** Based on the **Mandatory fields apply for Transmission** settings, the ECG report is not added to the transmission queue until you enter the patient demographic data for the mandatory fields. An error message displays in the notification area. You need to complete the data for the mandatory fields and manually resend the report to a configured destination. **NOTE** Based on the **Mandatory fields apply for Acquisition** settings, the ECG report is not accepted, transmitted, or printed until you enter the patient demographic data for the mandatory fields. If you manually transmit ECG report, an error message **Unable to transmit. Incomplete patient data.** displays on the **Acquisition** screen. You need to complete the data for the mandatory fields to transmit the ECG report.	Perform the steps below: 1. Edit the patient report to enter missing patient data. 2. Retry transmission.

5.9 Print a Patient Report

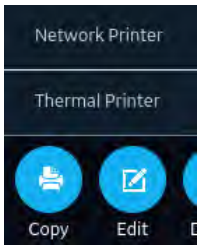
You can print a copy of a Rhythm, Full Disclosure, or ECG patient report in any configured report format for the selected lead set.

If you purchase the **NETP - Network Printer** option and enable it in the **Option Manager**,

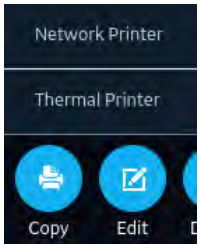
- you can print the copy via thermal printer or send the copy to a network printer on MAC 5 A4 and A5.
- you can only send the copy to a network printer on MAC 5 Lite.

See 10.6.3 Configure Network Printer on page 186 for more information.

1. Before printing a copy of the report, review the patient report and verify:
   - The patient information in the patient report is correct.
   - The ECG or Rhythm or Full Disclosure ECG is acquired with the desired gain and filter.
2. Perform one of the steps below:

To print a copy of the patient report ...	Perform the following:
In the default or selected report format displayed on the report screen	Select the **Copy** icon:  A job to print one copy of the patient report in the default report format is sent to the printer. • For MAC 5 A4 and A5, if you enable the network printer and thermal printer, the **Copy** button shows two options:  Select the **Network Printer** or **Thermal Printer** to send a job to print one copy of the patient report in the displayed report format. • For MAC 5 Lite with only network printer, select the **Copy** button directly to send a job to print one copy of the patient report in the displayed report format.

Continues on the next page

To print a copy of the patient report ...	Perform the following:
In a different report format	1. Select anywhere around the ellipsis icon in the left, bottom corner of the screen to view the **Copy Format** menu. 2. From the expanded **Copy Format** menu, select the desired report format to be used to print a copy of the report. Only the report formats supported for the lead set used to record the ECG or rhythm are available for selection. For example, if a 12-lead ECG is recorded, only 12-lead ECG patient report formats are available for selection. 3. Select the **Copy** button:  The patient report is refreshed and displayed on the report screen in the selected report format. A job to print one copy of the ECG or rhythm in the selected report format is sent to the printer. • For MAC 5 A4 and A5, if you enable the network printer and thermal printer, the **Copy** button shows two options:  Select the **Network Printer** or **Thermal Printer** to send a job to print one copy of the patient report in the displayed report format. • For MAC 5 Lite with only network printer, select the **Copy** button directly to send a job to print one copy of the patient report in the displayed report format.

The patient report is printed in the order in which it was received. If no other patient report are printing, the report is printed immediately. The printing status displays at the bottom of the screen.

NOTE

Based on the **Mandatory fields apply for Acquisition** settings, the ECG report is not accepted, transmitted, or printed until you enter the patient demographic data for the mandatory fields. An error message **Unable to print. Incomplete patient data.** displays on the **Acquisition** screen. You need to complete the data for the mandatory fields and reprint the patient report.

If a printer error occurs, the progress message is replaced by the printer error. The printing restarts automatically after the error is resolved. For more information on printer errors, see 13.3 Printing Errors on page 274.

If the device is configured to print the barcode of the patient ID in the patient reports, the printed patient report includes the barcode. The barcode can be used to perform a query by patient ID in the MUSE system.

3. To stop printing a patient report, select the **Stop** icon in the middle of the screen.

5.10 Edit Patient Information in a Patient Report

Make sure that you have the privilege to edit patient reports.

After a test is acquired, you can edit patient information using the software keyboard or by attaching an order. When an order is attached to a patient test, some fields are read-only.

If you try to edit or attach an order to a patient report that is transmitted to the default destination, an error message displays.

You cannot edit patient information by scanning a patient barcode, selecting a patient record from the **Patients** list, or performing ADT queries.

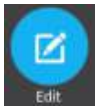
WARNING

INACCURATE PATIENT DATA

Incorrect patient information can cause patient data mismatch. Data assigned to the wrong patient causes erroneous patient data that can affect diagnosis and treatment.

Be sure to check the patient information screen for each new patient. Make sure that you enter patient data for the correct patient.

1. To edit patient information for the patient report, select the **Edit** icon in the **Report Review** page in the Acquisition screen:

   The **Patient Information** screen opens.

2. Edit the patient information using a software keyboard. See 4.3.3 Enter or Edit Patient Information Using the Software Keyboard on page 55.

3. Select **Save** to save your changes for this patient and collapse the screen.

   If you select any other icons at the bottom of the tab prior to saving, the **Patient Information** screen collapses and the edited patient information is saved.

   The updated patient information displays on the patient report.

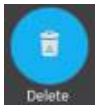
5.11 Delete a Patient Report

Make sure that you have the privilege to delete Rhythm, Full Disclosure, or ECG patient reports.

NOTE

If you do not have the privilege to view patient reports, but you have the privilege to delete patient reports, you can only view and delete patient reports you created in the current session.

1. Select the **Delete** icon in the **Report Review** page on the Acquisition screen to delete the patient report:

A message displays asking you to confirm if you want to permanently delete the patient report.

2. Select **Delete** to delete the patient report.

   The selected patient report(s) are deleted from the **Files** list.

3. A confirmation message may display if you are trying to delete a patient report that has not yet been transmitted to the default destination (if a message has been configured by your administrator). Perform one of the actions below:

   - Select **Delete** to delete the patient report. The selected patient report is deleted from the **Files** list. Deleting the patient report closes the tab where it was opened for viewing, and returns you to the **Home** tab.
   - Select **Cancel** to cancel the deletion. The selected patient report is not deleted from the **Files** list.

5.12 View the Patient Report

You can use the icons in the ECG, Rhythm, or Full Disclosure report tab to view the patient report:

Icon	Name	Description
	Maximize View	Select this icon or double-tap the patient report to maximize the view of the patient report.
	Minimize View	Select this icon or double-tap the maximized patient report to minimize the view of the patient report.
	Previous	Select this icon to navigate to the previous page of the multiple-page reports.
	Next	Select this icon to navigate to the next page of the multiple-page reports.

5.13 Close a Patient Report

1. Review the patient report.
2. After completing your tasks, select the **Done** icon to close the patient report.

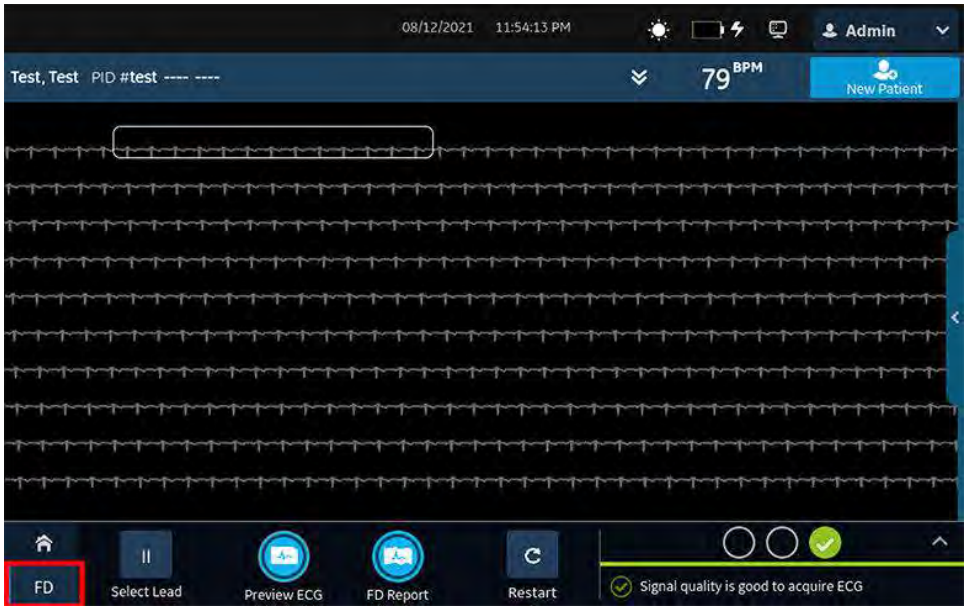
   

   A message displays asking you if you want to start a new patient test.

   Select one of the options below:

   - **New Patient** to start a test for a new patient, see 4.2 Start a Test for a New Patient on page 44. This action will clear the previous patient information.
   - **Continue with Same Patient** to start a new test for the same patient. The live waveform for this patient displays on the screen.

5.14 Full Disclosure Overview



The Full Disclosure ECG option shows one lead of the patient waveform for a maximum of 5 minutes. From this waveform, you can create a Full Disclosure report (FD Report) or create a 12-lead ECG. It starts after you connect a patient to the acquisition module AND you are viewing the waveforms.

This feature may be helpful for clinicians that need to acquire an ECG on:

- A child that will not sit still or is anxious.
- A patient that is experiencing symptoms or stable arrhythmias and would require a 12 lead ECG during those symptoms.

You can acquire a Full Disclosure ECG only if you purchase the Full Disclosure option, and enable it in the **Option Manager**.

Automatic acquisition of ECG does not start while in the **FD** tab.

5.14.1 Record a Full Disclosure ECG

Before you start this procedure, make sure:

- You purchase and enable the **FLDS - Full Disclosure** option in the **Option Manager**.
- You enable the **Full Disclosure** option in the **Settings** screen.

1. Start a new patient test.
2. To view a Full Disclosure ECG, click the **FD** tab on the **Acquisition** screen.
    - One lead of the Full Disclosure ECG displays. The Full Disclosure shows the waveform from the left to right side of the screen.
    - The Full Disclosure ECG records for a maximum of 5 minutes. The recording stops after the 5 minutes is complete.
    - The Full Disclosure screen displays 10 lines of ECG data and each line is of 30 seconds.

- A notification message displays on the **Acquisition** screen after the Full Disclosure ECG records for 5 minutes.
- The Full Disclosure screen displays the previous 5 minutes of Full Disclosure ECG data.

3. To change the lead, click **Select Lead**.

   All the configured leads display. Select the single lead you want to display on the screen and on the printed FD reports. If you connect the leads to a patient after being fully disconnected for at least 30 seconds, all the data will be cleared from the display.

   The ECG recording restarts and the selected lead is applied to the Full Disclosure waveform. All the previous recorded data will be cleared.

4. To restart the Full Disclosure ECG, click **Restart**. All of the current waveform data is deleted.

   The message displays: **The full disclosure data will be cleared. Do you want to proceed?**

5. To record a 10 seconds ECG when in the Full Disclosure screen, do the steps that follow:

   5.1. Select anywhere on the Full Disclosure ECG. The 10 seconds of ECG data is selected.

   5.2. Click **Preview ECG**.

   A preview of the recorded 10 seconds of data for all leads displays in the configured preview report. Select the minimize icon to view the report.

   5.3. To accept or reject an ECG Patient Report, see 5.6.4 Accept or Reject an ECG Patient Report on page 67.

   5.4. To review an ECG Patient Report, see 5.6.5 Review an ECG Patient Report on page 71.

6. To generate a Full Disclosure report, click **FD Report**.

   The Full Disclosure report for the selected lead displays for your review.

7. To review the Full Disclosure report, see 5.14.2 Review a Full Disclosure Report on page 85.

5.14.2 Review a Full Disclosure Report

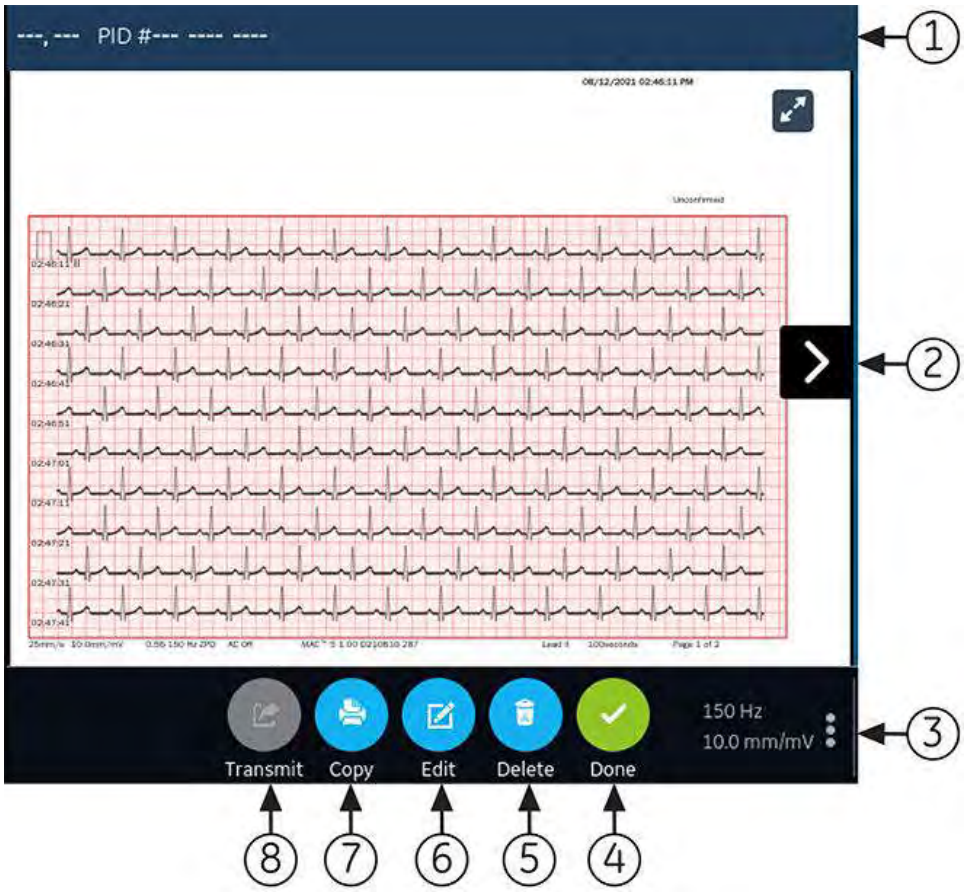


Table 5-8 Full Disclosure Report Tab

Item	Name	Description
1	**Patient Information** Banner	The information that displays on the screen for the patient such as first name, last name, gender, age, and so on. To edit the patient information, click anywhere on the **Patient Information** screen.
2	Full Disclosure Report	Displays the Full Disclosure report. If a Full Disclosure report contains more than one pages, click the left and right arrows on the screen to see the next page. When you record Full Disclosure ECG: • If the acquisition module is disconnected, the Full Disclosure report displays empty space on the screen. • If the lead is disconnected or the ECG waveform does not display, the Full Disclosure report displays a straight horizontal line on the screen, and transforms into square waves on the printed or transmitted FD Report. **NOTE** Only a FD Report or Rhythm Report can have a single tab. The ECG report will always have a tab, but if you enable a Rhythm tab and select a FD Report, the Rhythm tab will be replaced by the FD tab.

Continues on the next page

Table 5-8 Full Disclosure Report Tab (Table continued)

Item	Name	Description
3	Gain, Filter, and Speed	To edit the gain, filter, or speed of the waveform in the report, do the steps as follow: • Click the ellipsis icon that is on the lower right of the **FD Report** tab. • Select a new value from the expanded list. • The Full Disclosure report refreshes with the selected gain, filter, and speed.
4	**Done** icon	Closes the Full Disclosure report. For more information, see 5.13 Close a Patient Report on page 82.
5	**Delete** icon	Deletes the Full Disclosure report. For more information, see 5.11 Delete a Patient Report on page 81.
6	**Edit** icon	Edits the patient information for the Full Disclosure report. For more information, see 5.10 Edit Patient Information in a Patient Report on page 81.
7	**Copy** icon	Prints a copy of the Full Disclosure report. For more information, see 5.9 Print a Patient Report on page 78.
8	**Transmit** icon	Transmits the Full Disclosure report. For more information, see 5.8 Transmit a Patient Report to a Configured Destination on page 76.

To start a new Full Disclosure report for the same patient, click the **FD** tab to navigate to the Full Disclosure waveform and application, and restart the Full Disclosure ECG. For more information, see 5.14.1 Record a Full Disclosure ECG on page 83.

6 Work with Orders

Make sure that the ORDM option is enabled on the device. Contact a GE Healthcare Service Support representative to enable this option.

If order management is enabled, the **Orders** list displays in the Acquisition screen. You can retrieve orders from an order management server (such as a MUSE system) that is connected to your network.

When the orders list is updated, either automatically or manually, new orders are populated in the list.

The figure illustrates the **Orders** collapsed list:

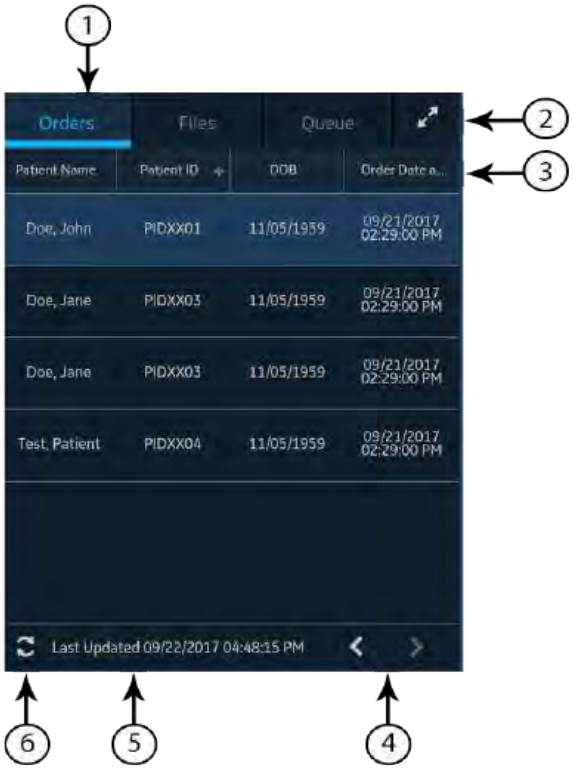


Table 6-1 Orders Collapsed List

Item	Name	Description
1	**Orders** tab	Displays a list of orders downloaded from an order management server. A filter icon next to the tab name indicates that the order list is filtered by a location.
2	**Expand** icon	Opens the **Orders** expanded list.
3	**Orders** collapsed list columns	Displays up to four configurable columns that provide information about the orders. This view will include at least one of the columns: **Patient Name**, **Patient ID**, or **Visit Number**.
4	Navigation arrows	Navigates to the previous and next pages in the **Orders** list.
5	**Last Updated** date and time	Displays the date and time the order list was last updated.
6	**Refresh** icon	Downloads the list of orders.

The figure illustrates the **Orders** expanded list:

Table 6-2 Orders Expanded List

Item	Name	Description
1	**Orders** tab	Displays the **Orders** expanded list. A filter icon next to the tab name indicates that the order list is filtered by a location.
2	**Filter Location** list	Select anywhere on the **Filter Location** field. From the drop-down menu, select the location filter you want to apply to the orders list.
3	**Collapse** icon	Collapses the **Orders** list.
4	**Orders** expanded list columns	Displays up to eleven configurable columns that provide information about the orders.
5	Navigation arrows	Navigates to the previous and next pages in the **Orders** list.
6	**Last Updated** date and time	Displays the date and time the order list was last updated.
7	**Refresh** icon	Downloads the list of orders.

Only one order can be associated with a patient test at any given time.

Only 12-lead order can be displayed on the device.

Orders cannot be attached to:

- Transmitted patient reports, or
- Digital Rhythm patient reports.

If you do not have permissions to edit patient reports, you cannot attach an order to the patient report.

When an order is attached to a patient test, all fields are read-only except for which can be edited below:

- **Blood Pressure**
- **Room Number**

- **Bed Number**
- **Test Indication**
- **Priority**
- **Comments**
- **Technician**
- **Patient History**
- **Location**
- **<Question>**
- **Attending MD ID**
- **Attending MD First Name**
- **Attending MD Last Name**

WARNING

INACCURATE PATIENT DATA

Incorrect patient information can cause patient data mismatch. Data assigned to the wrong patient causes erroneous patient data that can affect diagnosis and treatment.

Be sure to check the patient information screen for each new patient. Make sure that you attach the correct order for the correct patient.

6.1 Automatically Update the Orders List

The auto-update option must be enabled by your administrator to automatically update orders from the order management server. Orders are automatically updated when:

- The device is powered on.
- A user logs into the device or unlocks the device.
- The **New Patient** button is selected.
- A report is successfully sent to a remote device over the network.

The **Last Updated** date and time is updated. No error messages display if orders are not being automatically updated. You can also manually update the **Orders** list.

6.2 Manually Update the Orders List

You can manually update the orders list at any time, even if the auto-update option is enabled.

1. From the Acquisition screen, select the **Orders** tab.

   The **Orders** collapsed list opens.

2. Select the **Refresh** icon to update the orders list .

   The list of orders is refreshed and updated with the latest information. All previous data is overwritten. The date and time when the list was last updated display next to the **Refresh** icon.

If the device is not connected to the network, a message displays in the notification area indicating that the update has failed because the device is not connected to the network. If the message persists, contact your administrator to resolve the network issue.

If the device fails to connect to the order management server, a message displays in the notification area indicating that the update has failed because the connection to the order management server could not be established. If the message persists, contact your administrator.

You can download a maximum of 1000 orders. If the number of orders exceeds this limit, an error message displays asking you to restrict the order download filter.

6.3 Sort Orders in the Orders List

By default, the **Orders** list is sorted in descending order by the **Location** column, if the **Location** column is configured as one of the display columns.

If the **Location** column is not configured to display in the **Orders** list, the list is sorted in descending order by the column configured to display as the first column.

If you select the **Priority** column header or if the **Priority** column is the first column, the orders list is sorted in the order of priority:

- STAT
- ASAP
- Pre-Op
- Call back
- Routine

If you select the **Priority** column again, the sorting order is reversed.

You can change the sort order by selecting any one of the column headers. The orders list is sorted in ascending order by the selected column. If you select the same column header again, the orders list is sorted in the reverse order. If you select another column header, the orders list is sorted in ascending order by that column.

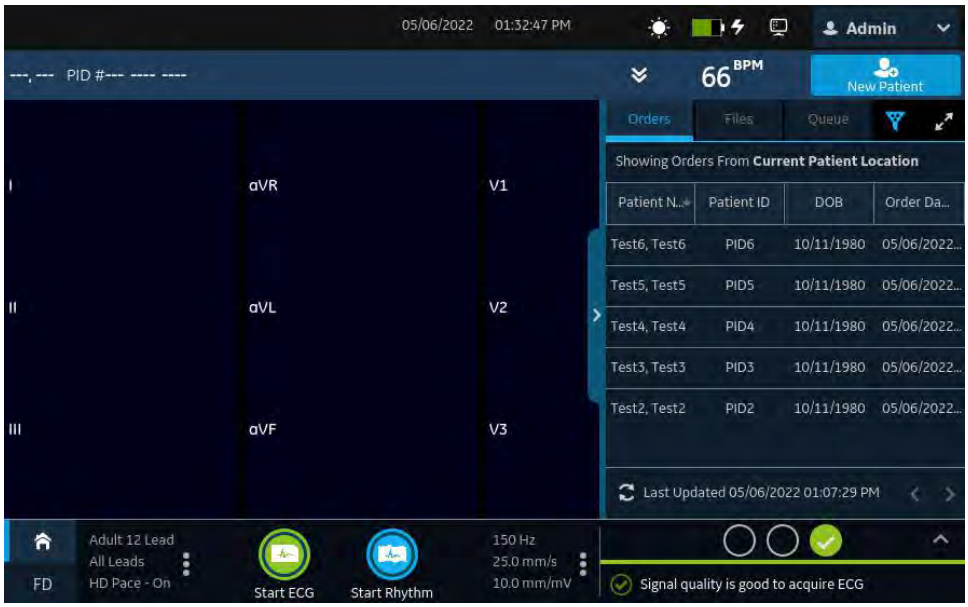
Changes made to the sort order apply until you log out or shutdown the device.

6.4 Filter Orders in the Orders List

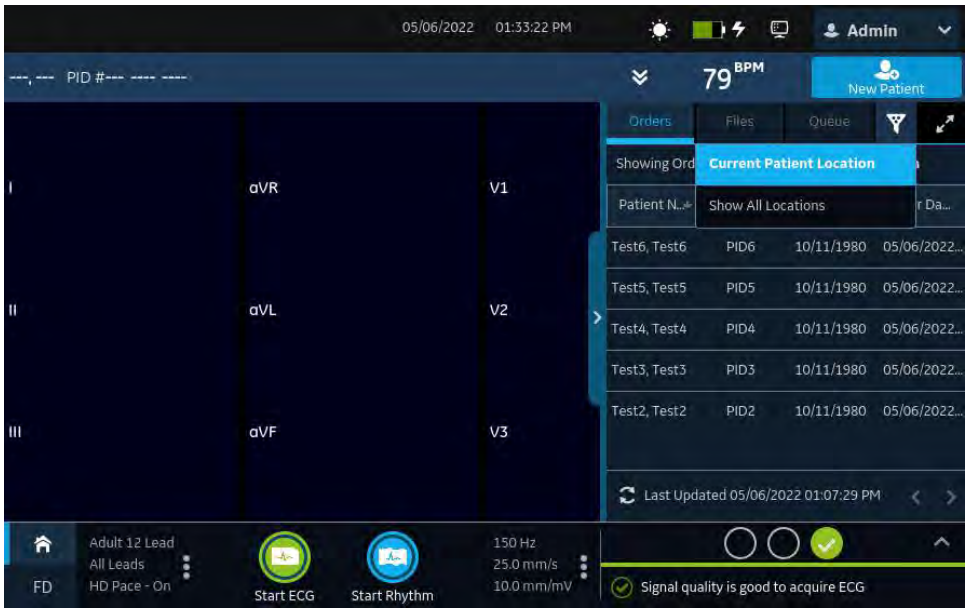
The **Orders** list is filtered by **Show All Locations**, **Current Patient Location**, or 1 out of 10 pre-configured filter groups. All of the order lists display based on the location filter you apply.

1. From the Acquisition screen, select the **Orders** tab.

   The **Orders** collapsed list opens.

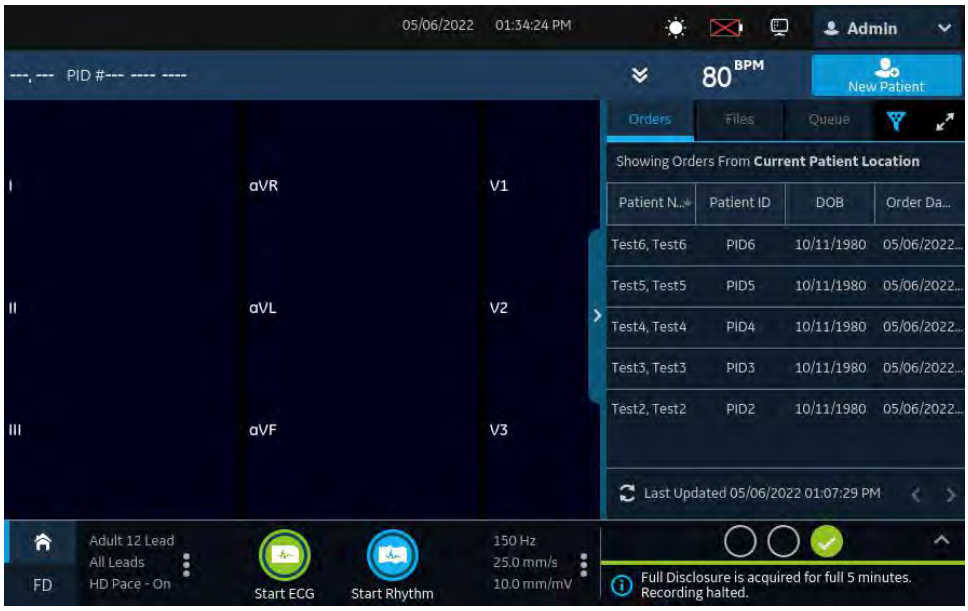


2. Select the necessary filter location from the drop-down list.



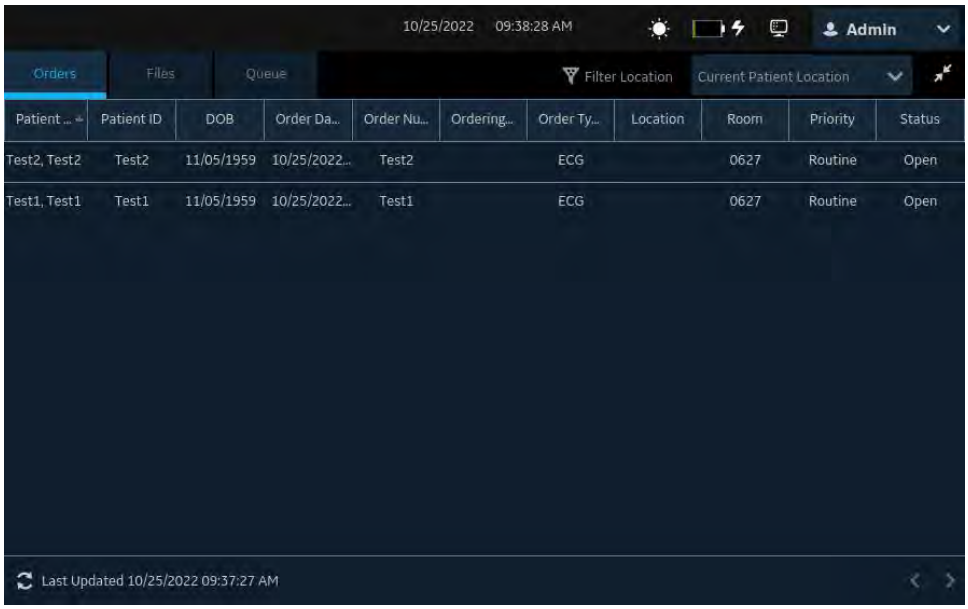
The order list refreshes and displays only the locations in the selected filter. If you select the filter drop-down list, the filter icon changes to . If you apply a location filter in the **Orders** list, the filter icon changes to to indicate that the order list is filtered and does not display all orders.

If you select...	Then...
A pre-configured filter group	The orders list displays orders from the locations in the selected filter group.
The **Current Patient Location**	The orders list displays only the orders from the current location of the device configured in the device settings.
The **Show All Locations**	The orders list displays the orders from all the locations of the device configured in the device settings.



3. To display an expanded list of **Orders**, select the **Expand** icon.

The **Orders** expanded list opens.



By default, the applied filter is **Current Patient Location**

, and displays all orders from the current location of the device.

6.5 Attach an Order when the Patient Test is Not Started

1. Start a test for the new patient. For more information, see 4.2 Start a Test for a New Patient on page 44.
2. Double-tap the order in the **Orders** list to attach it to a patient test.

The order number and other details available in the order are populated in the patient test record and the **Patient Information** screen is automatically expanded.

3. Edit patient information and select **Save** to save the patient data.
4. Record the ECG. For more information, see 5.6.2 Manually Start an ECG recording on page 65.
5. Verify that the status of the order in the **Orders** list is **Attached**.

6.6 Attach an Order to a New Patient Test

NOTE

You cannot attach an order that is already attached to another test. You must first detach the order. See 6.10 Detach an Order from a Patient Test on page 95.

1. Start a test for the new patient. For more information, see 4.2 Start a Test for a New Patient on page 44.
2. Double-tap the order in the **Orders** list to attach it to the current patient test.

If	Then
You did not manually enter patient data in the **Patient Information** screen after starting the test	There is no data mismatch upon attaching the order. Therefore, the order number and other details available in the order are populated in the patient test record and the **Patient Information** screen is automatically expanded. The status of the order is changed to **Attached**. Go to Step 4.
You manually entered patient data in the *Patient Information* screen after starting the test	There is a data mismatch between the order data and the manually entered patient data. A warning message displays indicating a mismatch in the patient name or patient ID and asks you to confirm that the selected order can be attached to the patient test, overwriting existing patient data. Go to the Step 3.

3. Select **Yes** to overwrite the patient information with data from the order. The order is attached to the patient report.
   - All patient demographic fields included in the order are populated in the test, overwriting the existing patient data.
   - The status of the order is changed to **Attached**.
4. Update test demographics in the **Patient Information** screen and select **Save**. For more information, see 4.3.3 Enter or Edit Patient Information Using the Software Keyboard on page 55.
5. Record the ECG. For more information, see 5.6.2 Manually Start an ECG recording on page 65.

6.7 Attach an Order when the Patient Test is Completed

NOTE

You cannot attach an order that is already attached to another test. You must first detach the order. See 6.10 Detach an Order from a Patient Test on page 95.

1. From the **Files** list, open the stored patient report.
2. Double-tap the order in the **Orders** list to attach it to the current patient test.

If	Then
You did not manually enter patient data in the **Patient Information** screen after starting the test	There is no data mismatch, but a message displays asking you to confirm that the selected order can be attached to the patient test, overwriting existing patient data. Go to Step 3.
You manually entered patient data in the **Patient Information** screen after starting the test	There is a data mismatch between the order data and the manually entered patient data. A warning message displays indicating a mismatch in the patient name or patient ID and asks you to confirm that the selected order can be attached to the patient test, overwriting existing patient data. Go to the Step 3.

3. Select **Yes** to update the patient information with data from the order. The order is attached to the patient report.
   - All patient demographic fields included in the order are populated in the test, overwriting the existing patient data.
   - The status of the order is changed to **Attached**.
4. Update test demographics in the **Patient Information** screen and select **Save**. For more information, see 4.3.3 Enter or Edit Patient Information Using the Software Keyboard on page 55.

6.8 Attach an Order that is Attached to a Different Patient Test

NOTE

Only one patient test can be associated with an order at any given time, regardless of the status of the patient test.

1. Start a new patient test.
2. Double-tap an order attached to a patient test in the **Orders** list.

   A message displays indicating that the order is already attached to a patient test.
3. Perform one of the actions below:
   - Select **Detach** to detach the order from the existing patient test and attach the order to the new patient test.

If	Then
The patient test the order is attached to is already transmitted to its default destination	The order cannot be removed from this test. A message displays indicating that the patient test has been transmitted to the default destination and the order cannot be detached. Select **OK**.
If the patient test is not transmitted	A message displays notifying you that the order will be detached from the patient test. Go to Step 4.

   - Select **View Test** to open the patient test and view it as if the test had been opened from the **Files** list.
4. Select **Continue** to detach the order from the existing patient test and attach the order to the new patient test.

6.9 Change the Order Attached to a Patient Test

If an incorrect order is attached to a patient test, use below procedure to detach the order from the patient test and replace it with a different order.

Before you start this procedure, make sure that the patient test is not already transmitted to its default destination. If the test has the **Sent** status of **Yes** (for example, the test was already sent to its default destination), the order can no longer be detached from the test. A message displays indicating that the patient test has been transmitted and the order cannot be detached.

WARNING

INACCURATE PATIENT DATA

Incorrect patient information can cause patient data mismatch. Data assigned to the wrong patient causes erroneous patient data that can affect diagnosis and treatment.

Be sure to check the patient information screen for each new patient. Make sure that you attach the correct order for the correct patient.

1. Detach the incorrect order from the patient test. See 6.10 Detach an Order from a Patient Test on page 95.
2. Attach the correct order to the patient test. See 6.7 Attach an Order when the Patient Test is Completed on page 93.

6.10 Detach an Order from a Patient Test

Before you start this procedure, make sure that the patient test with the incorrect order has not been transmitted to its default destination.

NOTE

If the patient test to which the order is attached has been transmitted to its default destination, the order cannot be detached from the test. A message displays indicating that the patient test has been transmitted and the order cannot be detached.

1. From the **Files** list, select the patient report with the incorrect order that you want to detach.
2. Expand the **Patient Information** screen and scroll down to the **Order Number** field.
3. Select **Detach** next to the **Order Number** field to clear the field.

   A message displays asking you to confirm if you want to detach the order from the selected test.
4. Select **Yes** to detach the order from the current test.

   The order number field is cleared.
5. Select **Save** to save your changes.

   The order is detached from the patient test and moves back to the **Open** status.

6.11 Order Status

Each order in the **Orders** list has one of the states below:

- Open

- Pending
- Attached

When an order is downloaded from the order management server, the status of the order can be **Open** or **Pending**. After an ECG has been acquired for an order, or an order has been attached to an existing ECG patient report, the order is moved to the **Attached** state in the **Orders** list.

The table describes various order status changes:

If...	Then...
You add an order to a patient test from the **Orders** list	• The order status changes from **Open** to **Attached**. • The MUSE server is notified to change the status of the corresponding order on the MUSE system from **Open** to **Pending**, if the device is connected to the network. If the attempt to notify the MUSE server fails, the status remains as **Open**.
The order number is detached from a patient test before acquiring the ECG	The order status changes from **Attached** to **Open**. The order status changes from **Pending** to **Open** on the MUSE server.
An order attached to an acquired, but untransmitted ECG patient test, is detached	The order status changes from **Attached** to **Open**. The order status changes from **Pending** to **Open** on the MUSE server.

When the order list is updated, the orders attached to completed ECG patient reports transmitted to the MUSE server are cleared from the **Orders** list, and new orders are downloaded from the MUSE server.

NOTE

The **Attached** order status is not included in the transmitted patient reports.

7 Work with the Files List

The **Files** list displays stored digital rhythm and ECG patient reports.

The figure illustrates the **Files** collapsed list:

Table 7-1 Files Collapsed List

Item	Name	Description
1	**Files** tab	Opens the **Files** collapsed list that stores the saved patient reports.
2	**Expand** icon	Opens the **Files** expanded list.
3	**Files** collapsed list columns	Displays columns that provide information about the stored patient reports.
4	Navigation arrows	Navigates to the previous and next page in the **Files** list.
5	**Expand** arrow	Expands the **Hookup Advisor** electrode placement image. When expanded, the image overlays the **Files** list.

The figure illustrates the **Files** expanded list:

Table 7-2 Files Expanded List

Item	Name	Description
1	**Files** tab	Opens the **Files** expanded list that stores the saved patient reports.
2	**Print List**	Prints the stored records from the **Files** list. This button is enabled only if the stored records are available.
3	**Collapse** icon	Collapses the **Files** list.
4	**Files** expanded list columns	Displays columns that provide information about the stored patient reports.
5	Navigation arrows	Navigates to the previous and next pages in the **Files** list.
6	Notification status	Shows the progress, error, or successful messages.
7	**Delete** icon	Deletes the selected patient reports.
8	**Edit** icon	Edits patient information for the selected patient report.
9	**Copy** icon	Prints a copy of the selected patient reports.
10	**Transmit** icon	Transmits the patient reports to the selected destination.
11	**Destination** menu	

7.1 Review a Stored Patient Report

Make sure that you have the privilege to view Rhythm, Full Disclosure, or ECG patient reports in the **Files** list. If you do not have the privilege, you can only view the patient reports you created in the current session.

1. From the **Acquisition** screen, select the **Files** tab.

The **Files** collapsed list opens.

2. Select the Rhythm or Full Disclosure or ECG patient report that you want to view.
3. Review and make necessary changes to the patient report, before printing a copy of the report or transmitting the report to a configured destination.

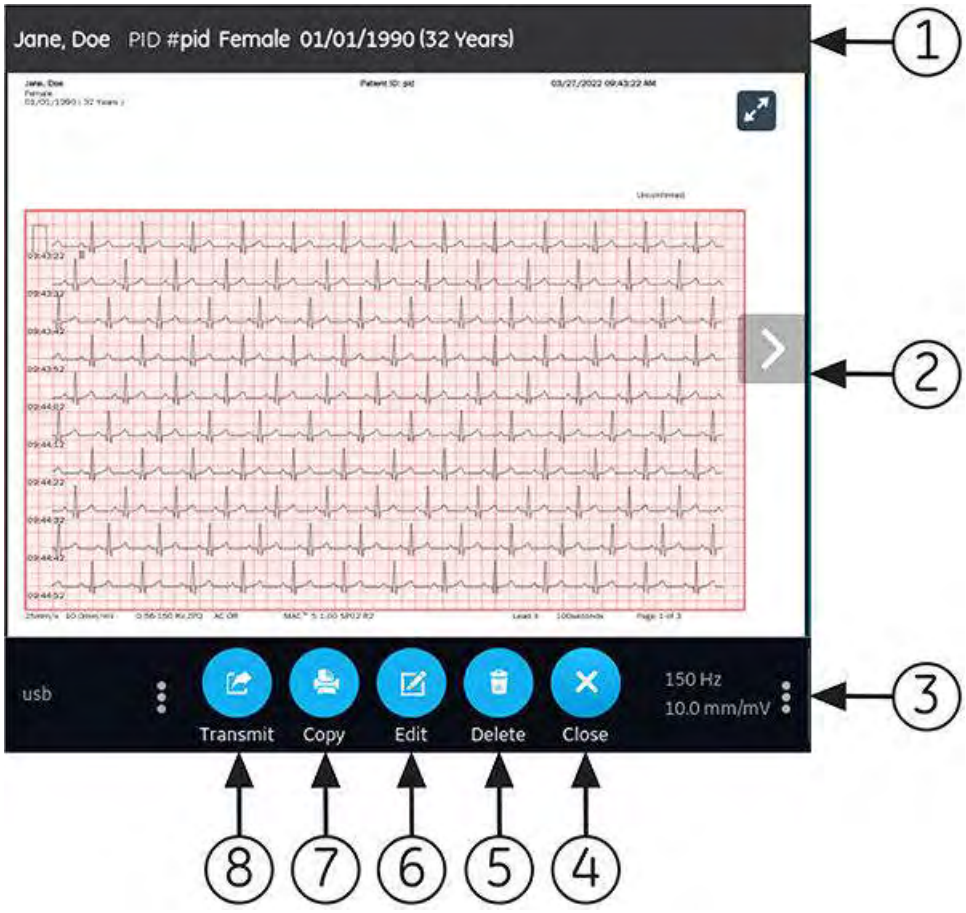


Table 7-3 Displaying a Stored Patient Report

Item	Name	Description
1	**Patient Information** banner	Displays patient information. A grey banner indicates the patient report has been stored in the device. Select anywhere in the banner to expand the screen and edit patient information.
2	ECG patient report, Rhythm report, or Full Disclosure report	Displays the patient report. For more information on the report formats, see A.1 ECG Report Formats on page 286 and A.2 Rhythm Report Format on page 290.
3	Gain, Filter, and Speed	Allows you to change the waveform gain, filter or speed. Select anywhere around the ellipsis icon next to **Gain**, **Filter** or **Speed** and select a value from the gain, filter, or speed options in the menu. The patient report is refreshed with the selected configurations. **NOTE** The **Speed** option displays only for the rhythm reports.
4	**Close** icon	Select the **Close** icon to close the report.

Continues on the next page

Table 7-3 Displaying a Stored Patient Report (Table continued)

Item	Name	Description
5	**Delete** icon	Select the **Delete** icon to delete the patient report from the **Files** list. Deleting the patient report closes the current tab and displays the **Live** tab. For more information, see 7.6 Delete Stored Patient Reports from the Files List on page 106.
6	**Edit** icon	Select the **Edit** icon to expand the **Patient Information** screen and edit patient information for the patient report. For more information, see 7.5 Edit Patient Information in a Stored Patient Report on page 105.
7	**Copy** icon	Select the **Copy** icon to print a copy of the patient report in the default report format. For more information on printing a copy of the report, see 7.3 Print a Stored Patient Report on page 102.
8	**Transmit** icon	Select the **Transmit** icon to transmit the patient report to the default destination. For more information, see 7.2 Transmit a Stored Patient Report to a Configured Destination on page 100.

4. Select  to close.

7.2 Transmit a Stored Patient Report to a Configured Destination

- Make sure that you have the privilege to transmit patient reports to a configured destination.
- Select the correct destination for your patient report.

Patient Report Type	Destination	Supported File Format
Resting ECG	DCP server destination (MUSE v9 or MUSE NX and MUSE DICOM Gateway Pro SP1 or higher)	Hilltop format
Resting ECG	USB R/W flash drive	PDF, Hilltop and Sapphire XML (Sapphire XML format is available if you enable the XML format output in the **Option Manager**) formats.
Resting ECG	SFTP server destination with remote directory path	PDF, Hilltop and Sapphire XML (Sapphire XML format is available if you enable the XML format output in the **Option Manager**) formats.
Resting ECG	Shared directory destination with folder path	PDF, Hilltop and Sapphire XML (Sapphire XML format is available if you enable the XML format output in the **Option Manager**) formats.
Digital Rhythm	USB R/W flash drive	PDF format
Digital Rhythm	DCP server destination (MUSE v9 SP6 or higher, or MUSE NX and MUSE DICOM Gateway Pro SP6 or higher)	PDF format
Digital Rhythm	SFTP server destination with remote directory path	PDF format
Digital Rhythm	Shared directory destination with folder path	PDF format

Continues on the next page

Patient Report Type	Destination	Supported File Format
Full Disclosure	USB R/W flash drive	PDF format
Full Disclosure	DCP server destination (MUSE v9 SP6 or higher, or MUSE NX and MUSE DICOM Gateway Pro SP6 or higher)	PDF format
Full Disclosure	SFTP server destination with remote directory path	PDF format
Full Disclosure	Shared directory destination with folder path	PDF format

To transmit a patient report to the default or configured destination, perform the steps below:

1. From the Acquisition screen, select **Files**.

   The **Files** collapsed list opens.

2. Perform one of the steps below:

If	Then
You want to transmit one patient report	Select the Rhythm or Full Disclosure report or ECG patient report you want to transmit to a configured destination. The selected patient report opens in a new tab (**ECG** or **FD Report** or **Rhythm** tab), depending on the report type.
You want to transmit multiple patient reports	Select the **Expand** icon to expand the **Files** list, and select the check box next to the patient reports to be transmitted. 

3. Perform one of the steps below:

To transmit the report(s) ...	Perform the following:
To the default destination	Select the **Transmit** icon: 
To another configured destination	1. Select anywhere around the ellipsis icon on the lower, left-side of the screen to expand the **Transmit** menu. 2. From the expanded **Transmit** menu, select any configured destination to transmit the patient report(s). 3. Select the **Transmit** icon:  One or more destinations must be configured for the **Transmit** icon to be enabled. If no destinations are configured, the **Transmit** icon is disabled.

The selected patient reports are added to the **Queue**, processed and transmitted to the selected destination. The **Job Status** can be viewed in the **Queue**. See 8.1 Display the Report Queue on page 110.

If you select patient reports for transmission from the expanded **Files** list, the message displays on the notification area in the lower, right-side of the screen: `<Count> reports added to the queue`, where `<Count>` is the number of selected reports.

If you select patient reports for transmission from the collapsed **Files** list, the message displays on the notification area in the lower, right-side of the screen: `<Destination_Name>: <Job_Status>`.

For example, if the destination name is USB, and the job status is **Failed**, the status displays as follows: `USB: Failed`.

A tick mark displays in the **Sent** column of the **Files** expanded list for patient reports successfully transmitted to the default destination.

If	Then
The transmission queue has reached its maximum limit of 1,000 reports, a message displays in the notification area that the transmission queue is full and no additional reports can be added.	Wait for the reports in the queue to transmit and try again.
One or more patient reports have been transmitted to the selected destination, a message displays in the notification asking you to confirm if you want to re-transmit the already transmitted reports.	Perform one of the actions below: • Select **OK** to re-transmit the patient report. • Select **Cancel** to cancel the report transmission.
Patient information is incomplete in one or more patient reports selected for transmission (for example, required fields are blank or contain invalid data), a message displays in the notification area indicating that one or patient reports cannot be transmitted because of incomplete patient data.	Perform the steps below: 1. Edit the incomplete patient report to enter missing patient data. 2. Retry transmission.

7.3 Print a Stored Patient Report

You can print a copy of a stored ECG patient report in any configured report format for the selected lead set.

If you purchase the **NETP - Network Printer** option and enable it in the **Option Manager**,

- you can print the copy via thermal printer or send the copy to network printer on MAC 5 A4 and A5.
- you can only send the copy to network printer on MAC 5 Lite.

For more information of network printer, see 10.6.3 Configure Network Printer on page 186.

1. From the Acquisition screen, select the **Files** list.

   The **Files** collapsed list opens. You can also select the **Expand** icon to open the **Files** expanded list:

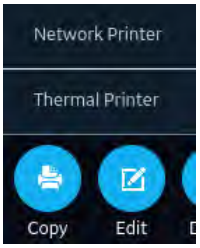
   

If	Then
You are in the **Files** collapsed list	Select the patient report for which you want to print a copy. The patient report opens in a new screen next to the **Files** list.
You are in the **Files** expanded list	Select the check box next to the patient report for which you want to print a copy.

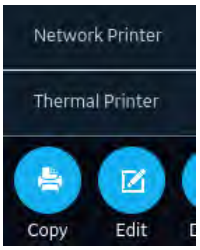
2. Select the Rhythm or Full Disclosure or ECG patient report for which you want to print a copy.

The selected patient report opens in a new screen.

3. Before printing a copy of the report, review the patient report and verify:
   - The patient information in the patient report is correct.
   - The ECG, Full Disclosure, or Rhythm test is acquired with the desired gain and filter.
4. Perform one of the steps below:

To print a copy of the patient report ...	Perform the following:
In the default or selected report format displayed on the report screen.	Select the **Copy** button:  A job to print one copy of the patient report in the displayed report format is sent to the printer. • For MAC 5 A4 and A5, if you enable the network printer and thermal printer, the **Copy** button shows two options:  Select the **Network Printer** or **Thermal Printer** to send a job to print one copy of the patient report in the displayed report format. • For MAC 5 Lite with only network printer, select the **Copy** button directly to send a job to print one copy of the patient report in the displayed report format.

Continues on the next page

To print a copy of the patient report ...	Perform the following:
In a different report format	1. Select anywhere around the ellipsis in the left, bottom corner of the screen. 2. From the expanded **Copy Format** menu, select the report format. For example, if a 12-lead ECG is recorded, you can only select 12-lead ECG patient report formats. 3. Select the **Copy** button:  The patient report is refreshed and displayed on the report screen in the selected report format. A job to print one copy of the ECG or rhythm in the selected report format is sent to the printer. • For MAC 5 A4 and A5, if you enable the network printer and thermal printer, the **Copy** button shows two options:  Select the **Network Printer** or **Thermal Printer** to send a job to print one copy of the patient report in the displayed report format. • For MAC 5 Lite with only network printer, select the **Copy** button directly to send a job to print one copy of the patient report in the displayed report format.

The patient report is printed in the order in which it was received. If no other patient reports are printing, the report is printed immediately. You will see a progress message at the bottom of the screen indicating the printing status.

NOTE

Based on the **Mandatory fields apply for Acquisition** settings, the ECG report is not accepted, transmitted, or printed until you enter the patient demographic data for the mandatory fields. If you manually print, an error message **Unable to print. Incomplete patient data.** displays on the Acquisition screen. You need to complete the data for the mandatory fields to print the patient report.

If a printer error occurs, the progress message is replaced by the printer error. The printing restarts automatically after the error is resolved. For more information on printer errors, see 13.3 Printing Errors on page 274.

If the device is configured to print the barcode of the patient ID in the patient reports, the printed patient report includes the barcode. The barcode can be used to perform a query by patient ID in the MUSE system.

Select the **Stop** icon on the Report Printing screen to stop printing a patient report.

7.4 Print a List of Stored Records

You can print all the stored records that display in the **Files Manager** on MAC 5 A4 and A5 device. Lite device does not support this function.

1. From the Acquisition screen, select the **Files** list.

   The **Files** collapsed list opens.

2. Select the **Expand** icon  to open the **Files** list.

   The **Files** expanded list opens.

3. Select the **Print List** button 

to print the list of stored records.

   The printing starts and a stop icon displays on the screen.

The stored record prints in the order in which it was displayed in the **Files Manager** view.

If a printer error occurs, the printer error message displays. Resolve the error and manually restart the print. For more information on printer errors, see Table 13-3 Printing Errors Encountered During Printing of the List of Stored Records on page 275.

Select the **Stop** icon on the Report Printing screen to stop printing a patient report.

7.5 Edit Patient Information in a Stored Patient Report

Make sure that you have the privilege to open stored rhythm, Full Disclosure, or ECG patient reports from the **Files** list and edit patient information.

You can edit patient information using a software keyboard or by attaching an order, but not by scanning a patient barcode, selecting a patient record from the **Patients** list, or performing ADT queries. When an order is attached to a patient test, some fields are read-only.

If you try to edit or attach an order to a patient report that is transmitted to the default destination, an error message displays.

WARNING

INACCURATE PATIENT DATA

Incorrect patient information can cause patient data mismatch. Data assigned to the wrong patient causes erroneous patient data that can affect diagnosis and treatment.

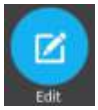
Be sure to check the patient information screen for each patient. Make sure that you enter patient data for the correct patient.

1. From the Acquisition screen, select **Files**.

   The **Files** collapsed list opens. You can also select the **Expand** icon to open the **Files** expanded list:

If	Then
You are in the **Files** collapsed list	Select the patient report for which you want to edit. The patient report opens in a new screen next to the **File** list.
You are in the **Files** expanded list	Select the check box next to the patient report you want to edit.

2. Select the **Edit** icon to edit patient information for the stored patient report:



The **Patient Information** screen opens with a grey background indicating that this is a stored patient report.

3. Edit the patient information using a software keyboard. See 4.3.3 Enter or Edit Patient Information Using the Software Keyboard on page 55.

4. Select **Save** to save your changes for this patient and collapse the screen.

   If you select any other icons at the bottom of the tab prior to saving, the **Patient Information** screen collapses and the edited patient information is saved.

   The updated patient information displays on the patient report.

5. Select  to close.

7.6 Delete Stored Patient Reports from the Files List

Make sure that you have the privilege to delete Rhythm, Full Disclosure, or ECG patient reports from the **Files** list.

If you do not have the privilege to view patient reports, but you have the privilege to delete patient reports, you can only view and delete patient reports you created in the current session.

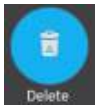
1. From the Acquisition screen, select **Files**.

   The **Files** collapsed list opens.

2. Perform one of the steps below:

If	Then
You want to delete one patient report	Select the Rhythm, Full Disclosure, or ECG patient report you want to delete. The selected patient report opens in a new screen.
You want to delete multiple patient reports	Select the **Expand** icon to expand the **Files** list, and select the check box next to the patient reports to be deleted. 

3. Select the **Delete** icon:



A message displays asking you to confirm if you want to permanently delete the selected patient report(s).

4. Select **Delete** to delete the patient reports.

   The selected patient reports are deleted from the **Files** list.

   An alert may be configured by your administrator to warn you before deletion of untransmitted reports.

   If this alert is configured, and one or more patient reports you are trying to delete have not yet been transmitted to the default destination, a message displays asking you to confirm the deletion.

   Perform one of the actions below:

   - Select **Delete** to delete the selected patient reports. The selected patient reports are deleted from the **Files** list. If the patient report was opened for viewing, deleting the patient report closes the tab, and returns you to the **Live** screen review.
   - Select **Cancel** to cancel the deletion. The selected patient reports are not deleted from the **Files** list.

8 Work with the Queue List

The digital rhythm, FD report and ECG patient reports transmitting to a designated location and incompleted network printing jobs are temporarily stored in the **Queue** list.

The successfully transmitted digital rhythm, FD report and ECG patient reports and completed network printing jobs are immediately deleted from the **Queue** list.

The figure illustrates the **Queue** collapsed list:

Table 8-1 *Queue* Collapsed List

Item	Name	Description
1	**Queue** tab	Displays the list of patient reports in the transmission queue.
2	**Expand** icon	Opens the **Queue** expanded list.
3	**Queue** collapsed list columns	Displays columns that provide information about the patient reports in the transmission queue.
4	Navigation arrows	Navigates to the previous and next pages in the **Queue** list.

The figure illustrates the **Queue** expanded list:

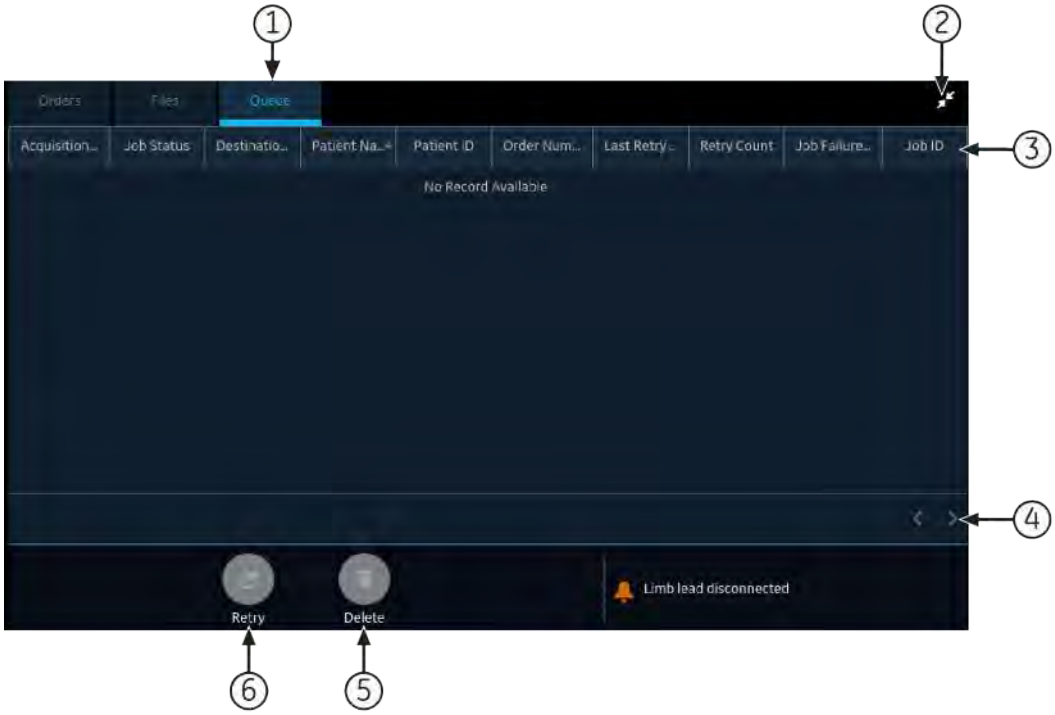


Table 8-2 *Queue* Expanded List

Item	Name	Description
1	**Queue** tab	Displays the list of patient reports in the transmission queue.
2	**Collapse** icon	Collapses the **Queue** list.
3	**Queue** expanded list columns	Displays columns that provide information about the patient reports in the transmission queue.
4	Navigation arrows	Navigates to the previous and next pages in the **Queue** list.
5	**Delete** icon	Deletes the selected transmission or network printing job from the *Queue* list.
6	**Retry** icon	Retries the transmission of an unsuccessful job.

Table 8-3 Columns in the *Queue* List

Column Name	Description
Acquisition Date/ Time	Displays the date and time of the rhythm, FD report or ECG patient report, in the configured date and time format.
Job Status	Displays the status of the job. Below statuses display: • **In Progress**: The job is currently being processed. • **Failed**: The transmission failed. The reason for failure is provided in the **Job Failure Reason** column. • **Not Sent**: The job is waiting to be processed. When the job is completed, the report is removed from the **Queue** list.
Destination Name	Displays the name of the configured destination.
Patient Name	Displays the name of the patient in the format `First Name, Last Name`.
Patient ID*	Displays the unique ID assigned to the patient.

Continues on the next page

Table 8-3 Columns in the *Queue* List (Table continued)

Column Name	Description
Order Number*	Displays the order number.
Last Retry Date Time*	Displays the date and time of the last re-tried transmission, in the configured date and time format.
Retry Count*	Displays the re-tried transmission count in numbers. If the device sends the report on the first attempt, the **Retry Count** is 0.
Job Failure Reason*	Displays the reason for the failed transmission. If the device fails to transmit a report, contact your IT department. If the device sent the report successfully, this field is blank. To troubleshoot the errors, see 13.4 Report Transmission Errors on page 277.

Column names suffixed with an asterisk (*) in the table are visible only in the expanded **Queue** list.

8.1 Display the Report Queue

This procedure describes how to view the queue for the reports that are ready to be sent, were successfully sent, or failed in transmission.

NOTE

For manually transmitted reports, a message `Transmission complete x/y` displays in the notification area indicating that transmission is complete, where *x* is the current count of patient reports being transmitted, and *y* is the total count of reports being transmitted for the current patient.

1. From the Acquisition screen, select **Queue**.

   The **Queue** collapsed list opens.

2. To open the **Queue** expanded list, select the **Expand** icon:

   The **Queue** expanded list opens.

3. Select the **Collapse** icon to collapse the list and return to the Acquisition screen:

8.2 Delete Jobs from the Queue

1. From the Acquisition screen, select **Queue**.

   The **Queue** collapsed list opens.

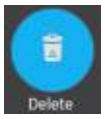
2. To display an expanded list of the **Queue**, select the **Expand** icon:

   The **Queue** expanded list opens.

3. Select the transmission or network printing job you want to delete.

4. Select the **Delete** icon to delete the selected jobs:



- If the job status is **In Progress**, a message displays indicating that the job is in progress and cannot be deleted.

  You cannot delete the job. Wait until the transmission attempt completes and then try again, if necessary.

- If the job is in **Not Sent** or **Failed** status, a message displays asking you to confirm the deletion of the selected job.

5. Select **Delete** to confirm the deletion.

   The selected jobs are deleted from the **Queue**. The patient report remains in the **Files** list. You can transmit the patient report to a destination again, if required.

8.3 Retry Transmission of a Patient Report

NOTE

The system will automatically transmit the pending patient reports in sequence.

If the configured destination is USB server, DCP server, SFTP server or Shared Directory and you select these patient reports, the system will re-transmit the selected reports immediately. If the configured destination is a network printer, you cannot manually re-transmit the patient reports.

Make sure that you have the privilege to transmit Rhythm, Full Disclosure, or ECG patient reports to a configured destination.

The system automatically tries to transmit a patient report. If you need to re-transmit the patient report before the next automatic attempt, you can use this procedure to transmit the patient report immediately.

1. From the Acquisition screen, select **Queue**.

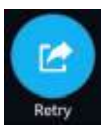
   The **Queue** collapsed list opens.

2. To display the expanded list of the **Queue**, select the **Expand** icon:

   The **Queue** expanded list opens.

3. Select one or multiple patient reports that you want to re-transmit and select the **Retry** icon:

   If no other report transmission is in progress at the time, the selected patient report will be immediately transmitted. If another patient report is in the process of being transmitted, the selected patient report starts transmission as soon as the current patient report is transmitted.

   If a patient report is successfully transmitted, it is immediately deleted from the **Queue**. Review the queue to confirm that the patient report was transmitted. All report transmissions are also logged in the **Report Transmission Log** in the **Service** screen.

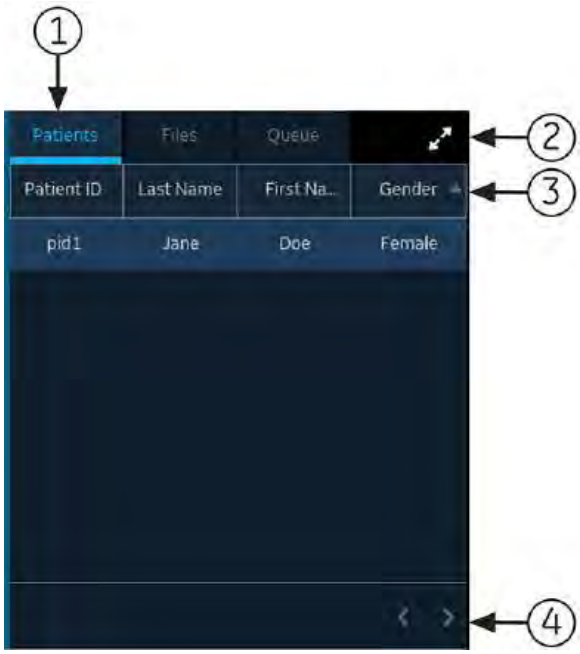
If the patient report is not successfully transmitted (**Job Status** is **Failed**), the reason for the failure is listed in the **Job Failure Reason** field. You can try to re-transmit the report again.

4. Select the **Collapse** icon to close the **Queue** expanded list and return to the Acquisition screen:

9 Work with the Patients List

If the **Order Manager** is disabled in the **Settings** screen, the **Patients** list displays in the Acquisition screen. The information of recent patients is stored in the **Patients** list, and you can view up to 500 recent patient information records.

The figure below illustrates the **Patients** collapsed list:



The figure below illustrates the **Patients** expanded list:

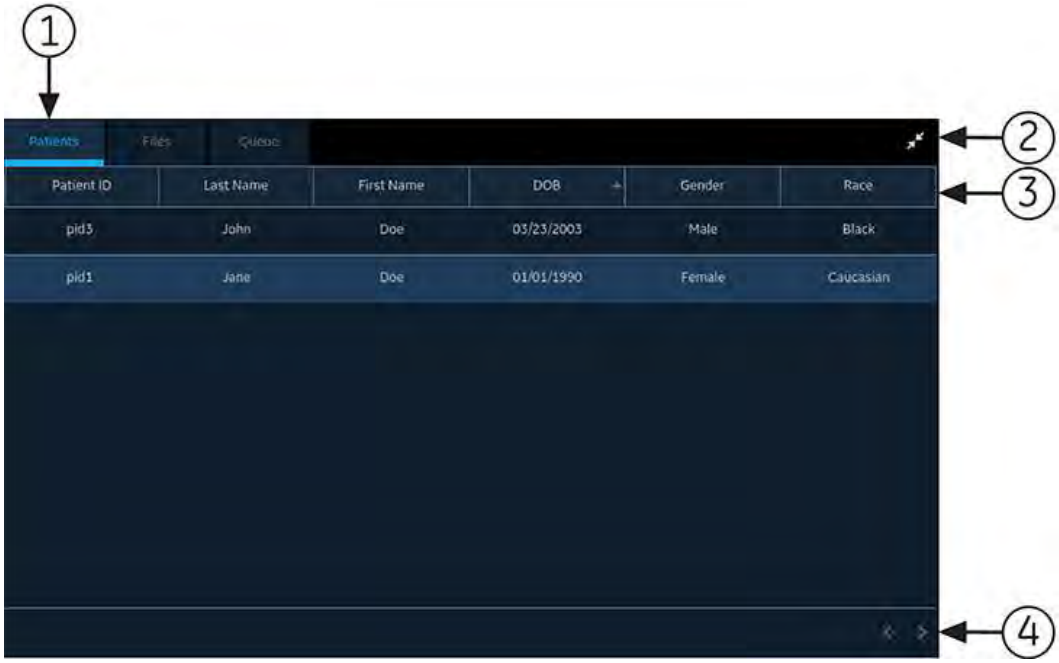


Table 9-1 Patients List

Item	Name	Description
1	**Patients** tab	Displays the **Patients** list.
2	**Expand** or **Collapse** icon	Expands or collapses the **Patients** list.
3	**Patients** collapsed and expanded list columns	Displays these four columns in the collapsed list: • **Patient ID** • **Last Name** • **First Name** • **Gender** Displays these six columns in the expanded list: • **Patient ID** • **Last Name** • **First Name** • **DOB** (Date of Birth) • **Gender** • **Race** By default, the list is sorted by **Last Name** in ascending order. You can sort by any column by selecting the column header. Select the same column header again to sort in descending order.
4	Navigation arrows	Navigates to the previous and next pages in the **Patients** list.

9.1 Open the Patients List

The **Patients** list displays on the Acquisition screen if order management is disabled.

Make sure that you have the privilege to view the patients lists or an error message will display when you try to view it.

1. From the Acquisition screen, select **Patients**.

   The **Patients** collapsed list opens and displays a list of patients.

2. To display an expanded list of **Patients**, select the **Expand** icon:

   The **Patients** expanded list opens.

9.2 Select a Patient from the Patients List

1. Select **New Patient**. For more information, see 4.2 Start a Test for a New Patient on page 44.
2. Select the **Patients** tab on the right-side of the Acquisition screen.

   The **Patients** collapsed list opens and displays a list of patients.

3. Double-tap the patient record that you want to associate with the patient test.

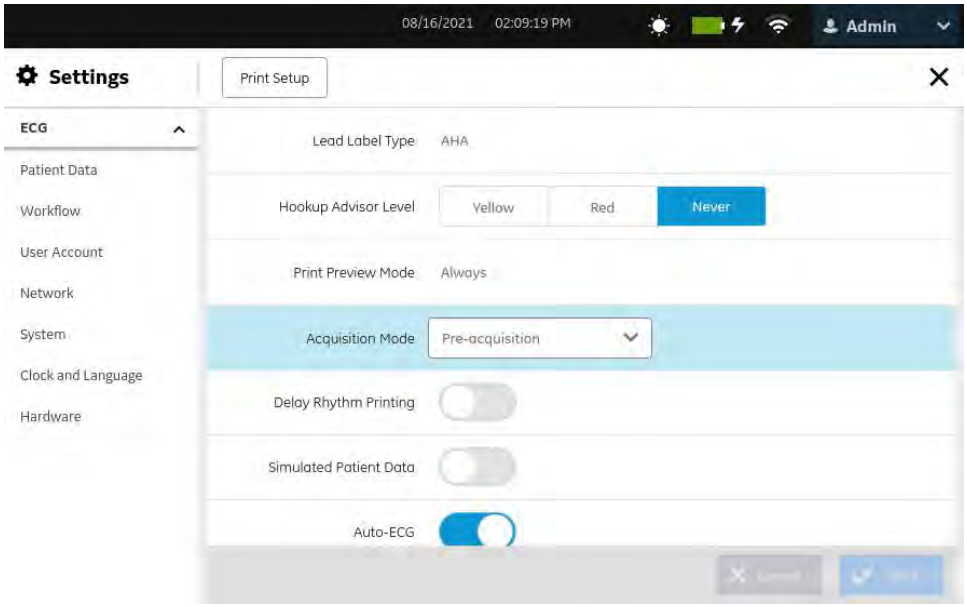
   If the desired patient record is not visible, select the navigation arrows to navigate to the previous and next pages of the **Patients** list and search for the patient record.

The patient data from the selected patient record is populated in the **Patient Information** banner and screen, and the screen expands.

4. Edit patient information in the fields. For more information, see 4.3.3 Enter or Edit Patient Information Using the Software Keyboard on page 55.

10 Configure Settings

10.1 Settings Screen Overview



Select the *Settings* screen to set up the features below.

- ECG - 10.4 Configure ECG on page 117
- Patient Data - 10.5.1 Configure Patient Information on page 139
- Workflow - 10.6 Configure Workflow on page 149
- User Management - 10.7 User Account on page 197
- Network - 10.8 Configure Network on page 223
- System - 10.9 Configure System on page 240
- Clock and Language - 10.10 Configure the Clock and Language on page 254
- Hardware - 10.11 Configure Hardware on page 259

10.2 Open the Settings Screen

Make sure that your user role is assigned the privileges to access the **Settings** screen.

1. Select **Settings** from the **User** menu on the Acquisition screen.

   If you have sufficient privileges, the **Settings** screen opens.

   If you do not have privileges to access the **Settings** screen, a message displays based on your user profile. Log on as a user with sufficient privileges to access the **Settings** screen.

User Profile	Message

Default User	`You do not have sufficient privileges to view the selected screen. Login as a new user with the required privileges.`
	`Attention: Logging in as a new user will log out the current user and any unsaved data will be lost.`
	Log on as a user with sufficient privileges to open the **Settings** screen.

STAT, local or LDAP user	`You do not have sufficient privilege to access the Settings screen.` Log off and log on as a user with sufficient privileges to access the **Settings** screen.

10.3 Configure General Tasks

1. Perform general tasks, as per the information in the table below:

Table 10-1 Configure General Tasks

Button	Action
Print Setup	Select this setting to print the system setup report for the product version. Use this report to configure other devices.
Save	Select this setting to save the system settings. A confirmation message displays: `Saved Successfully.`
Changes	A confirmation dialog displays with a message indicating your changes are not saved and will be lost. Select **Discard Changes** to discard the changes and move to the other screen. Select **Review Changes** to review and save the changes before moving to other screen.
Test Connection	Select this setting to test the particular destination is available and online. • If the connection is successful, a success message displays and the **Save** button is enabled. • If the connection fails due to an error, a failure message displays. Troubleshoot the error and test the connection. **NOTE** This option only tests the destination is available and online. It does not guarantee that the transmit will succeed. At the time of actual connection or transmission, it can fail, even if the test shows **Success**.

10.4 Configure ECG

Select **Settings** > **ECG** menu to configure the following:

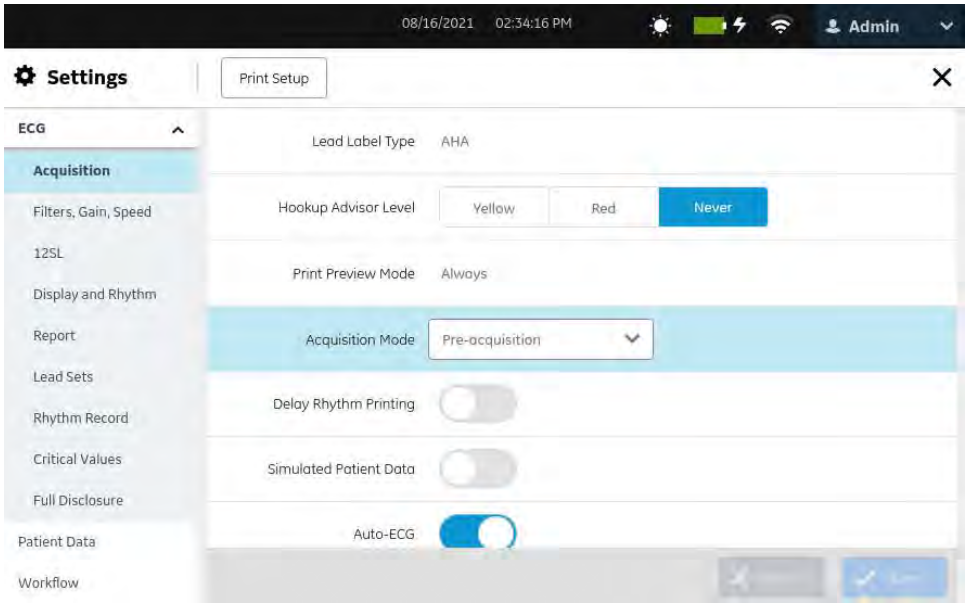
- ECG Acquisition - 10.4.1 Configure ECG Acquisition on page 118
- Filter, Gain, and Speed - 10.4.2 Configure Filters, Gain, and Speed on page 121
- 12SL Interpretations - 10.4.3 Configure 12SL Interpretations on page 123

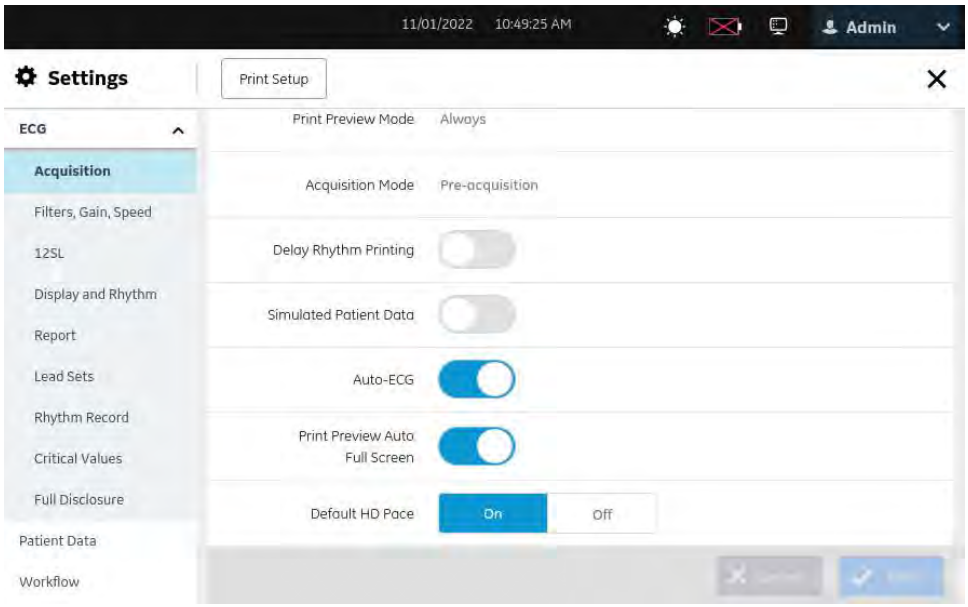
- Display Formats of ECG and Rhythm Leads - 10.4.4 Configure Display Formats of ECG and Rhythm Leads on page 125
- Patient Reports - 10.4.5 Configure Patient Reports on page 128
- Lead Sets - 10.4.6 Configure Lead Sets on page 133
- Rhythm - 10.4.7 Configure Rhythm on page 135
- Critical Value Notifications - 10.4.8 Configure Critical Value Notifications on page 136
- Full Disclosure - 10.4.9 Configure Full Disclosure on page 138

10.4.1 Configure ECG Acquisition

1. Select **Settings** > **ECG** > **Acquisition**.

   The **Acquisition** screen displays.





2. Configure the fields as per the information in the table.

Table 10-2 Acquisition Settings

Field	Action	Description
Lead Label Type	Select a value from the drop-down list to configure the lead label type.	The supported lead labels are from the American Heart Association (AHA) and International Electrotechnical Commission (IEC). The lead label type is automatically set to **AHA** when you change the device language and after you perform restore to factory default settings: • English • Korean • Brazilian Portuguese The lead label type is automatically set to **IEC** when you change the device language and after you perform restore to factory default settings: • Chinese • Danish • Dutch • Finnish • French • German • Italian • Swedish • Japanese • Czech • Norwegian • Portuguese • Russian • Spanish • Polish • Turkish
Hookup Advisor Level	Select a value from the drop-down list to configure when the Electrode Placement Image automatically expands, in case of leadwire failures.	The Hookup Advisor indicator displays yellow or red depending on the severity of the signal failure in a leadwire. • If you select **Yellow**, the Electrode Placement Image automatically expands when the indicator is yellow or red. When the signal turns green, the Electrode Placement Image automatically collapses. • If you select **Red**, the Electrode Placement Image automatically expands when the indicator is red. When the signal turns yellow or green, the Electrode Placement Image automatically collapses. • If you select **Never**, the Electrode Placement Image does not automatically expand or collapse, regardless of the type of signal received. You can manually expand and collapse the Electrode Placement Image at any time. Default value: **Never**

Continues on the next page

Table 10-2 Acquisition Settings (Table continued)

Field	Action	Description
Print Preview Mode	Select a value from the drop-down list to configure the print preview mode.	• If **Always** is selected, a preview of the ECG always displays after ECG acquisition. • If **Yellow** is selected, a preview of the ECG displays after ECG acquisition, if the Hookup Advisor status for the 10-seconds ECG acquired is Yellow or Red. • If **Red** is selected, a preview of the ECG displays after ECG acquisition, if the Hookup Advisor status for the 10-seconds ECG acquired is Red. • If **Never** is selected, a preview of the ECG is never display after ECG acquisition. Always the preview screen will display after ECG acquisition, if you: ◦ Enable **Auto-ECG** or select the 10 seconds of ECG from the **Full Disclosure** screen. ◦ Configure the **Print Preview Mode** setting to **Never**. Default value: **Always**
Acquisition Mode	Select a value from the drop-down list to configure the acquisition mode.	• If **Pre-acquisition** is selected, the system acquires the latest/previous 10-seconds of data for analysis. • If **Post-acquisition** is selected, the system displays the acquisition progress until 10-seconds of ECG data is acquired. Default value: **Pre-acquisition**
Delay Rhythm Printing	Enable or disable this setting.	If this setting is disabled, rhythm printing occurs in real-time. If this setting is enabled, the system waits until 10-seconds of rhythm data is acquired before starting rhythm printing. Default value: Disabled
Simulated Patient Data	Enable or disable this setting.	If this setting is enabled, you can use simulation patient data for demonstrations or troubleshooting. **NOTE** If you enable this setting and power OFF the system, this setting is set to OFF when you power ON the system. If you log OFF the system while the last saved status of Simulated Patient Data is ON, this setting is set to OFF on next login. The system generates and displays simulated ECG waveforms on the Acquisition screen. The label at the top of the screen indicates that the ECG waveform is based on simulated data from the internal simulator, and not actual patient data. If this setting is disabled, the system displays waveforms recorded from a patient attached to the device. Default value: Disabled
Auto-ECG	Enable or disable this setting.	If this setting is enabled, as soon as the ECG signal is good, the device automatically starts recording 10-seconds of ECG data for **only one** ECG per patient connection. Default value: Enabled

Continues on the next page

Table 10-2 Acquisition Settings (Table continued)

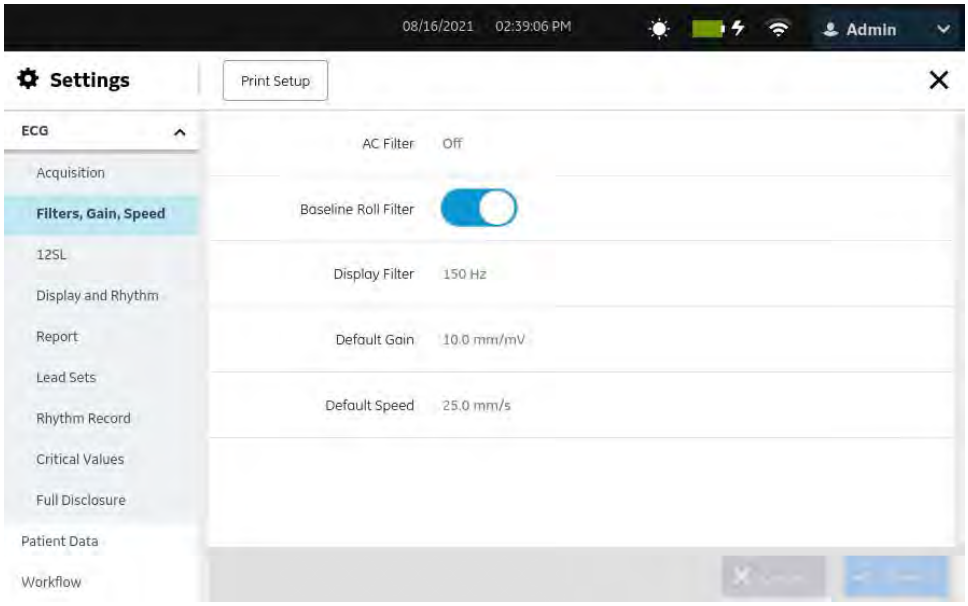
Field	Action	Description
Print Preview Auto Full Screen	Enable or disable this setting.	If this setting is enabled, the system automatically displays the ECG preview window in full screen mode. If this setting is disabled, the system displays the ECG preview window in normal mode. This setting is disabled, if the **Print Preview Mode** value is configured to **Never**. Default value: Enabled
Default HD Pace	Select a value to configure the default status of the **HD Pace** option on the **Acquisition** screen.	If you configure **HD Pace On**, the **HD Pace** option on the Acquisition screen is displayed **On** after you start a new patient or restart the device. If you configure **HD Pace Off**, the **HD Pace** option on the Acquisition screen is displayed **Off** after you start a new patient or restart the device. Default value: **On** **NOTE** You can manually enable or disable **HD Pace** option on the Acquisition screen and override this default configuration.

3. Click **Save**.

10.4.2 Configure Filters, Gain, and Speed

1. Select **Settings** > **ECG** > **Filters, Gain, Speed**.

   The **Filters, Gain, Speed** screen displays.



2. Configure the fields as per the information in the table.

Table 10-3 Filter, Gain and Speed Settings

Field	Action	Description
AC Filter	Select a value from the drop-down list.	The **AC Filter** frequency is set prior to shipping the unit and is based on the country of purchase. The AC filter is used to remove power line interference from the ECG signal. If no power line interference in the ECG signal needs to be removed, it is possible that the AC filter induces noise into the signal. If this is occurring, you can disable the AC filter by changing the setting to **Off**. **NOTE** The **AC Filter** setting does not change when the system is restored to factory defaults. Default value: Based on country of purchase. Allowed values: • **50 Hz** • **60 Hz** • **Off**
Baseline Roll Filter	Enable or disable this setting.	If this setting is enabled, the system applies a 0.56 Hz baseline roll filter to the waveforms. Use the baseline roll filter to remove low frequency components such as motion artifact, respiratory variation, and baseline shift. If this setting is disabled, no baseline roll filter is applied. If at any time the ECG configuration settings are restored to factory defaults, the baseline roll filter setting is reset to its default value, enabled. Default value: Enabled
Display Filter	Select a value from the drop-down list to configure the default filter.	This sets the upper frequency limit for the ECG waveform display on the Acquisition screen and the printout. Selecting a filter eliminates signals that exceed the frequency. The smaller the filter selected, the more signal is filtered. For example, a filter of 40 Hz displays only signals at 40 Hz or less; signals greater than 40 Hz are ignored. Default value: **150 Hz** Allowed values: • **20 Hz** • **40 Hz** • **100 Hz** • **150 Hz**

Continues on the next page

Table 10-3 Filter, Gain and Speed Settings (Table continued)

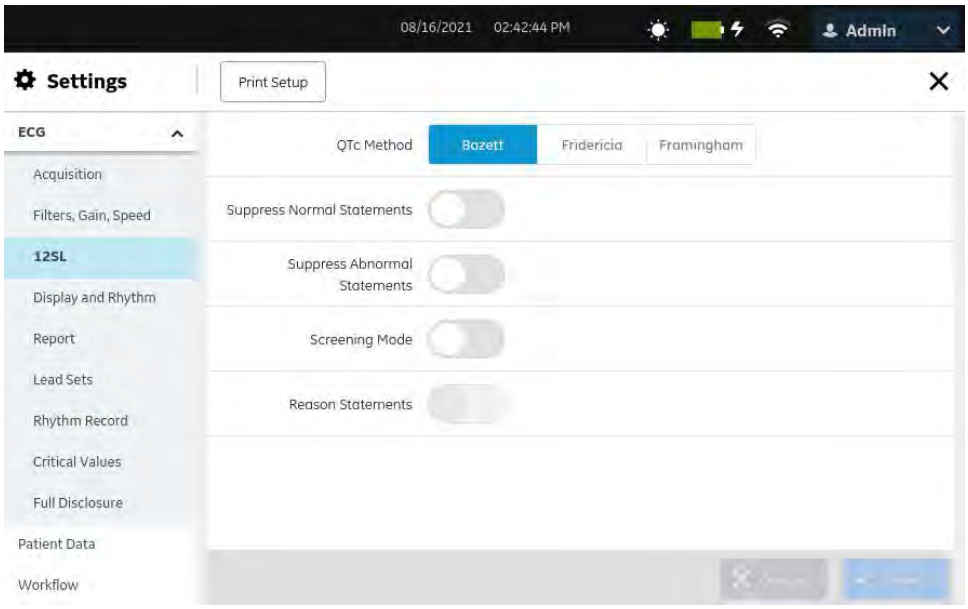
Field	Action	Description
Default Gain	Select a value from the drop-down list, to configure the default gain of the ECG waveform to display on the Acquisition screen.	Gain indicates how many mm represent 1 mV of sample data on the printout. Changing the gain changes the amplitude of the waveforms. A higher gain makes the amplitude of the waveform appear higher; a lower gain makes the amplitude of the waveform appear lower. The 10/5 mm/mV setting is used to display the limb leads (I, II, III, aVr, aVl, and aVf) at 10mm/mV and chest leads (V1 - V6) at 5 mm/mV. This is sometimes done to reduce or prevent waveform overlap in the chest leads, while avoiding tiny waveforms in the limb leads. The standard grid paper is divided into small squares of 1 mm x 1 mm and large squares of 5 mm x 5 mm. When printing 10 mm/mV, 1 mV of data is represented in 10 mm (2 large squares) on the printout. Default value: **10.0 mm/mV** Allowed values: • **2.5 mm/mV** • **5.0 mm/mV** • **10.0 mm/mV** • **20.0 mm/mV** • **10.0/5.0 mm/mV**
Default Speed	Select a value from the drop-down list, to configure the default speed of the ECG waveform to display on the Acquisition screen.	A faster speed makes the waveform display further apart; a slower speed makes the waveform display closer together. The standard grid paper is divided into small squares of 1 mm x 1 mm and large squares of 5 mm x 5 mm. When printing 25 mm/s, 1 second of data is represented in 25 mm (5 large squares) on the printout. Default value: **25.0 mm/s** Allowed values: • **5.0 mm/s** • **12.5 mm/s** • **25.0 mm/s** • **50.0 mm/s**

3. Click **Save**.

10.4.3 Configure 12SL Interpretations

1. Select **Settings** > **ECG** > **12SL**.

   The **12SL** screen displays.



2. Configure the fields as per the information in the table.

Table 10-4 12SL Settings

Field	Action	Description
QTc Method	Select a value to use a QT Correction Method with the 12SL algorithm.	The name of the QT Correction Method and the QTc value display on the report. Default value: **Bazett** Allowed values: • **Bazett** • **Fridericia** • **Framingham**
Suppress Normal Statements	Enable or disable this setting.	If this setting is enabled, no normal interpretative statements generate or display on the report when you do as follows: • View a report on the preview and review screens • View a stored report in the review screen • Print a report • Send a report to a configured destination. If this setting is disabled, normal interpretative statements display on the report. Default value: Disabled

Continues on the next page

Table 10-4 12SL Settings (Table continued)

Field	Action	Description
Suppress Abnormal Statements	Enable or disable this setting.	If this setting is enabled, no abnormal or borderline interpretative statements generate or display on the report when you do as follows: • View a report in the preview and review screens • View a stored report in the review screen • Print a report • Send a report to a configured destination. If this setting is disabled, abnormal and borderline interpretative statements display on the report. Default value: Disabled
Screening Mode	Enable or disable this setting.	If this setting is enabled, the device runs the 12SL algorithm in high-specificity mode, where you will not see certain lower-acuity statements in the interpretation. If this setting is disabled, the device runs the 12SL algorithm in normal analysis mode and you see the lower-acuity statements. Default value: Disabled
Reason Statements	Enable or disable this setting.	You can select this setting only if you enable the **Screening Mode**. If this setting is enabled, reason statements generate or display on the report when you perform the following: • View a report in the preview and review screens • View a stored report in the review screen • Print a report • Send a report to a configured destination. If this setting is disabled, no reason statements generate or display on the report. Default value: Disabled

3. Click **Save**.

10.4.4 Configure Display Formats of ECG and Rhythm Leads

Table 10-5 Default Lead Formats for Each Lead Set

Name	No. of Leads	Lead Format	Leads	Default	Auto-rhythm	Digital Rhythm
Adult 12 Lead						
All Leads	12	4x3	CH1 to CH12: I, II, III, aVR, aVL, aVF, V1, V2, V3, V4, V5, V6	Yes	No	Yes
			Swedish standard: CH1 to CH12: aVL, I, -aVR, II, aVF, III, V1, V2, V3, V4, V5, V6			
3 Leads	3	1x3	CH1 to CH3: V1, II, V5	No	Yes	No
6 Lead Group 1	6	1x6	CH1 to CH6: I, II, III, aVR, aVL, aVF	No	No	No
			Swedish standard: CH1 to CH6: aVL, I, -aVR, II, aVF, III			

Continues on the next page

Table 10-5 Default Lead Formats for Each Lead Set (Table continued)

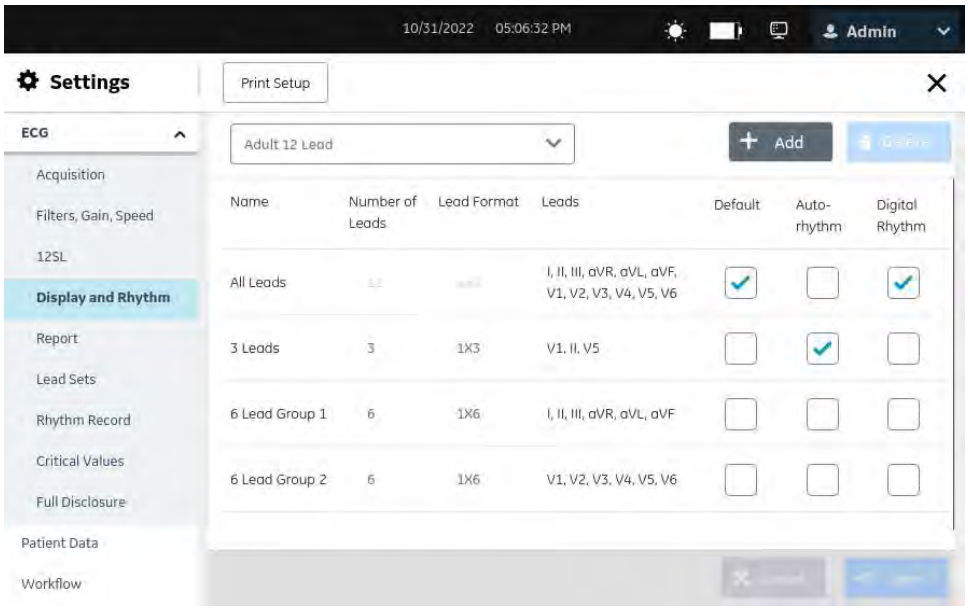
Name	No. of Leads	Lead Format	Leads	Default	Auto-rhythm	Digital Rhythm
6 Lead Group 2	6	1x6	CH1 to CH6: V1, V2, V3, V4, V5, V6	No	No	No
Pediatric 12 Lead						
All Leads	12	4x3	CH1 to CH12: I, II, III, aVR, aVL, aVF, V1, V2, V3r, V4, V5, V6	Yes	No	Yes
			Swedish standard: CH1 to CH12: aVL, I, -aVR, II, aVF, III, V1, V2, V3r, V4, V5, V6			
3 Leads	3	1x3	CH1 to CH3: V1, II, V5	No	Yes	No
6 Lead Group 1	6	1x6	CH1 to CH6: I, II, III, aVR, aVL, aVF	No	No	No
			Swedish standard: CH1 to CH6: aVL, I, -aVR, II, aVF, III			
6 Lead Group 2	6	1x6	CH1 to CH6: V1, V2, V3r, V4, V5, V6	No	No	No

The **All Leads** and **6 Lead Group 1** lead formats for all default lead sets are automatically set to the lead channel sequence mentioned in Table 10-5 Default Lead Formats for Each Lead Set on page 125 when the device language is set as **Swedish**, and the device is restored to factory default settings.

You can add, edit, and delete user-defined ECG lead formats, except the **All Leads** format.

1. Select **Settings** > **ECG** > **Display and Rhythm**.

   The **Display and Rhythm** formats screen displays.



2. To configure a lead format for a selected lead:
   - To add a user-defined lead format, perform Step 3 to Step 6.
   - To edit a user-defined lead format, perform Step 7.
   - To delete a user-defined lead format, perform Step 8.

3. Select the **Add** icon  to add a lead format.

   A new row is added to the lead format table.

4. Configure the lead format as per the information in the table:

Table 10-6 Display Format Settings for ECG and Rhythm Leads

Field	Action	Description
Name	Enter a name for your lead format setting.	Allowed values: Up to 20 characters. Allowed values are: • A to Z • a to z • 0 to 9 • All special characters
Number of Leads	Select the number of leads you want to include in the lead format.	Default value: • For 12 leads: 12 Allowed values: • For 12 leads: 3, 6, 12
Lead Format	Select the layout for the leads in columns by rows.	The different types of lead formats are as follows: • 3 Leads: 1x3 • 6 leads: 1x6, 2x3, or 2x3 Simult • 12 leads: 2x6, 2x6 Simult, 4x3, 4x3 Simult **Simult** refers to display all the leads at the same time. You can add up to 10 new format entries. Default value: • For 12 leads: 4x3 Allowed values: • For 12 leads: 4x3, 4x3 Simult, 2x6, 2x6 Simult
Leads	Select the leads in each channel that you want to display in the waveform for the selected lead set.	Default values: • Adult 12 Lead: I, II, III, aVR, aVL, aVF, V1, V2, V3, V4, V5, V6 • Pediatric 12 Lead: I, II, III, aVR, aVL, aVF, V1, V2, V3r, V4, V5, V6 Allowed values: • Adult 12 Lead: I, II, III, aVR, -aVR, aVL, aVF, V1, V2, V3, V4, V5, V6, V3r • Pediatric 12 Lead: I, II, III, aVR, -aVR, aVL, aVF, V1, V2, V3, V4, V5, V6, V3r
Default	Enable or disable this setting.	If this setting is enabled, this lead set format is the default format for ECGs recorded on this device. Default value: Disabled
Auto-rhythm	Enable or disable this setting.	If this setting is enabled, this lead set format is the default format used for an **Auto Rhythm** report on this device. There can be only one default format used for an **Auto Rhythm** report. If a default format is not selected, the default format for ECGs is used. Default value: Disabled

Continues on the next page

Table 10-6 Display Format Settings for ECG and Rhythm Leads (Table continued)

Field	Action	Description
Digital Rhythm	Enable or disable this setting.	If this setting is enabled, this lead set format is the default format for digital rhythm on this device. There can be only one default format for a digital rhythm recording. If a default format is not selected for digital rhythm, the default format for ECGs is used for digital rhythm. Default value: Disabled

5. Select **Save**.
6. Repeat Step 3 to Step 5 to add more ECG lead format configurations.
7. To edit an existing ECG lead format configuration:
   7.1. Select anywhere in the row of the lead format configuration you want to modify to enable the edit mode.
   7.2. Make changes to the configuration as per the information in Table 10-6 Display Format Settings for ECG and Rhythm Leads on page 127.
   7.3. Select **Save**.
8. To delete an existing lead format configuration:
   8.1. Select the **Delete** icon for the lead format configuration you want to delete.

   NOTE

   You can delete only one lead format configuration at a time. To delete more than one lead format configuration, repeat this step.

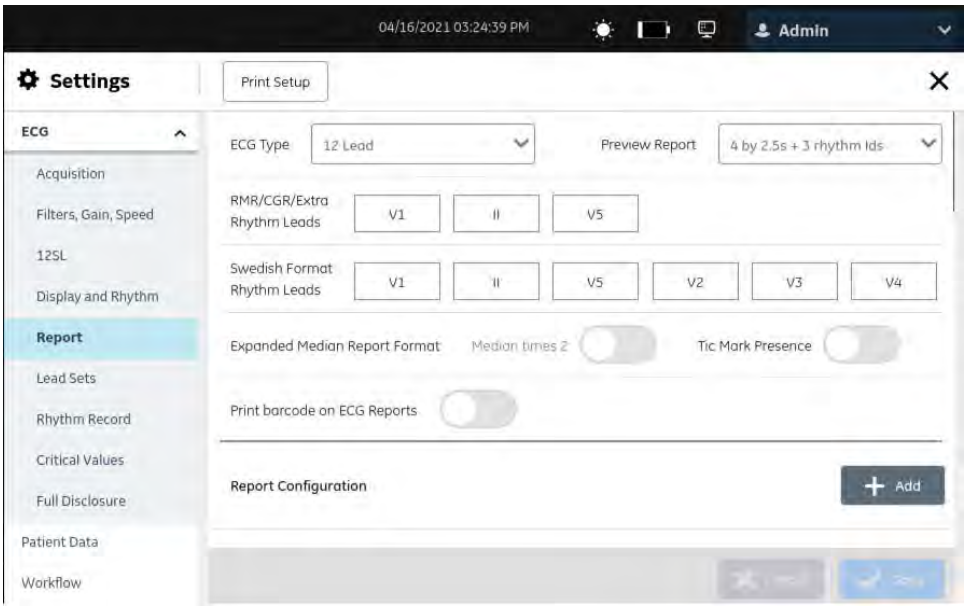
   8.2. Select **Save**.

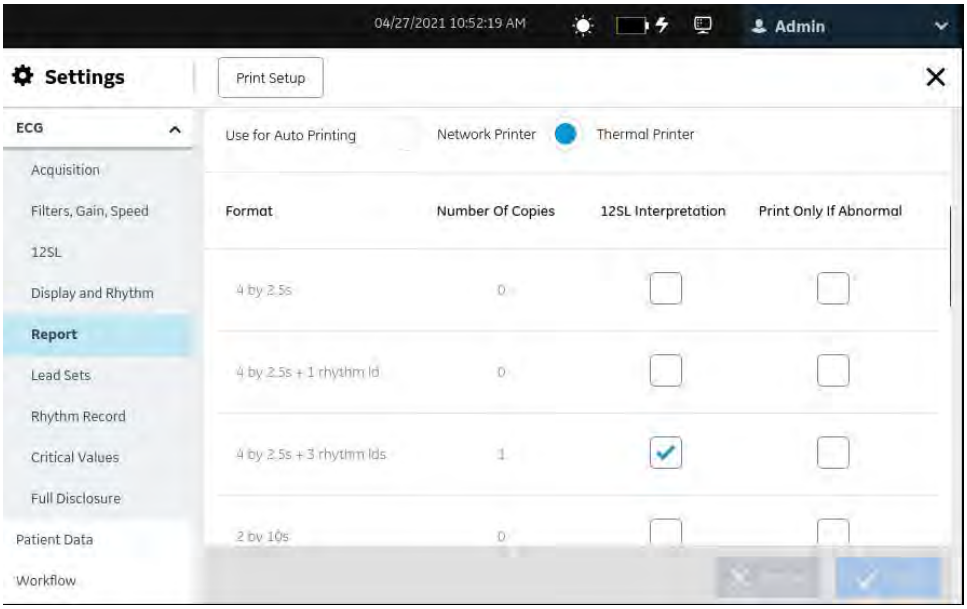
10.4.5 Configure Patient Reports

You can configure a report format for each lead set.

1. Select **Settings** > **ECG** > **Report**.

   The **Report** screen displays.





2. Select **12 Lead** as ECG type.
3. Configure the preview report format and leads as per the information in the table:

Table 10-7 Preview Report Format and Lead Settings

Field	Description	Allowed Values	Default Value
Preview Report	Select a value from the drop-down list to preview the recorded ECG of the selected ECG type before printing. See A.1 ECG Report Formats on page 286 for a list of on ECG report formats.	Supported report formats for 12 lead ECG type	**4 by 2.5s + 3 Rhythm Lds**

Continues on the next page

Table 10-7 Preview Report Format and Lead Settings (Table continued)

Field	Description	Allowed Values	Default Value
RMR/CGR/Extra Rhythm Leads	Select a value from the first column to configure the first rhythm lead. If the ECG report format to be printed consists of only one line of rhythm data, then this rhythm lead is printed on the ECG report.	**V1 to V6, V3R, I, II, III, aVR, aVL and aVF** leads	**V1**
	Select a value from the second column to configure the second rhythm lead.		**II**
	Select a value from the third column to configure the third rhythm lead. **NOTE** The configured rhythm leads are printed on the ECG reports if the report format includes rhythm data.		**V5**
Swedish Format Rhythm Leads	Select a value from the first column to configure the first rhythm lead for the Swedish report format.	**V1 to V6, V3R, I, II, III, aVR, aVL and aVF** leads	**V1**
	Select a value from the second column to configure the second rhythm lead for the Swedish report format.		**II**
	Select a value from the third column to configure the third rhythm lead for the Swedish report format.		**V5**
	Select a value from the fourth column to configure the fourth rhythm lead for the Swedish report format.		**V2**
	Select a value from the fifth column to configure the fifth rhythm lead for the Swedish report format.		**V3**
	Select a value from the sixth column to configure the sixth rhythm lead for the Swedish rhythm report.		**V4**
Expanded Median Report Format			
Median times 2	If you enable this setting, the gain of the expanded median report is double the gain set during the acquisition. If you disable this setting, the gain of the expanded median report is the same as the gain set during the acquisition.	• Enabled • Disabled	Disabled
Tic Mark Presence	Displays or hides the tic marks in an expanded median report.	• Enabled • Disabled	Disabled

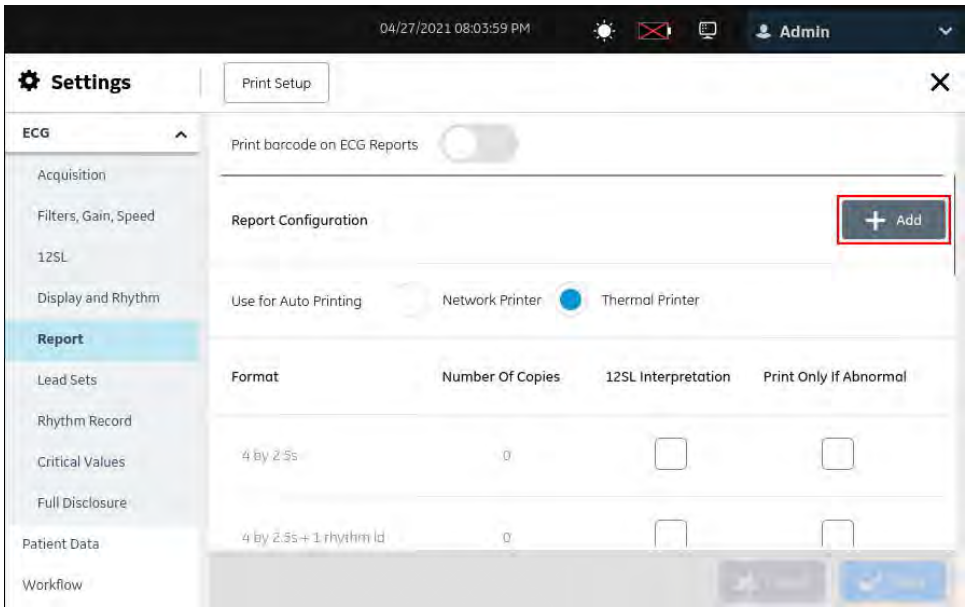
Continues on the next page

Table 10-7 Preview Report Format and Lead Settings (Table continued)

Field	Description	Allowed Values	Default Value
Print barcode on ECG Reports	If you enable this setting, the barcode of the Patient ID prints on the ECG patient reports. If you disable this setting, the barcode of the Patient ID does not print on the ECG patient reports. **NOTE** The network printer does not support printing the barcode of the Patient ID on the ECG reports.	• Enabled • Disabled	Disabled
Use for Auto Printing			
Network Printer	If you enable this setting, you can select the destination to print automatically when you accept a patient report. After you select **Network Printer**, the report prints via the configured network printer. If you do not purchase and enable the **NETP - Network Printer** option, the **Network Printer** setting will not display. The destination defaults to thermal printer.	• Enabled • Disabled	Disabled
Thermal Printer	If you enable this setting, the patient report prints via the thermal printer when you accept a patient report. **NOTE** For the MAC 5 Lite device, the report can only print via the network printer.	• Enabled • Disabled	Enabled

4. Perform any of the steps below to configure report printing for each supported report format:
   - To add a report printing configuration, perform Step 5 to Step 8.
   - To edit a report printing configuration, perform Step 9.
   - To delete a report printing configuration, perform Step 10.

5. Select the **Add** icon Add to add a report printing configuration.



6. Configure report printing as per the information in the table.

Table 10-8 Report Printing Settings

Field	Action	Description
Format	Select a report format from the drop-down list to configure the printing settings for this report format.	See A.1 ECG Report Formats on page 286 for a list of report formats. Default value: No default value Allowed values: All supported report formats
Number of Copies	Select the number of copies to print for this print configuration.	Default value: • 1 for **4 by 2.5s + 3 rhythm lds** report format • 0 for all other report formats Allowed values: 0 to 10
12SL Interpretation	Enable or disable this setting.	Displays or hides the 12SL analysis in the ECG report. Default value: • Not applicable for **1 by 10s @25mm/s**, **1 by 10s @50mm/s** and **Expanded media 12ld** formats. • Enabled for **4 by 2.5s + 3 rhythm lds**
Print Only if Abnormal	Enable or disable this setting.	If you enable this setting, an ECG report prints only if the 12SL analysis indicates that it is abnormal. If you disable this setting, all ECG reports print. Default value: • Not applicable for **1 by 10s @25mm/s**, **1 by 10s @50mm/s** and **Expanded media 12ld** formats. • Disabled for all other formats.

7. Select **Add**.

   A new row is added to the report configuration table.

8. Repeat Step 5 to Step 7 to add more report printing configurations.

9. To edit an existing report printing configuration:
   9.1. To enable the edit mode, select anywhere in the row of the report printing configuration that you want to modify.
   9.2. Make changes to the configuration as per the information in Table 10-8 Report Printing Settings on page 132.
   9.3. Select **Save**.
10. To delete an existing report printing configuration:
   10.1. Select the **Delete** icon for the report printing configuration you want to delete.

NOTE

You can delete only one report printing configuration at a time. To delete more than one report printing configuration, repeat this step.

   10.2. Select **Save**.

10.4.6 Configure Lead Sets

The device includes the default lead set configurations below:

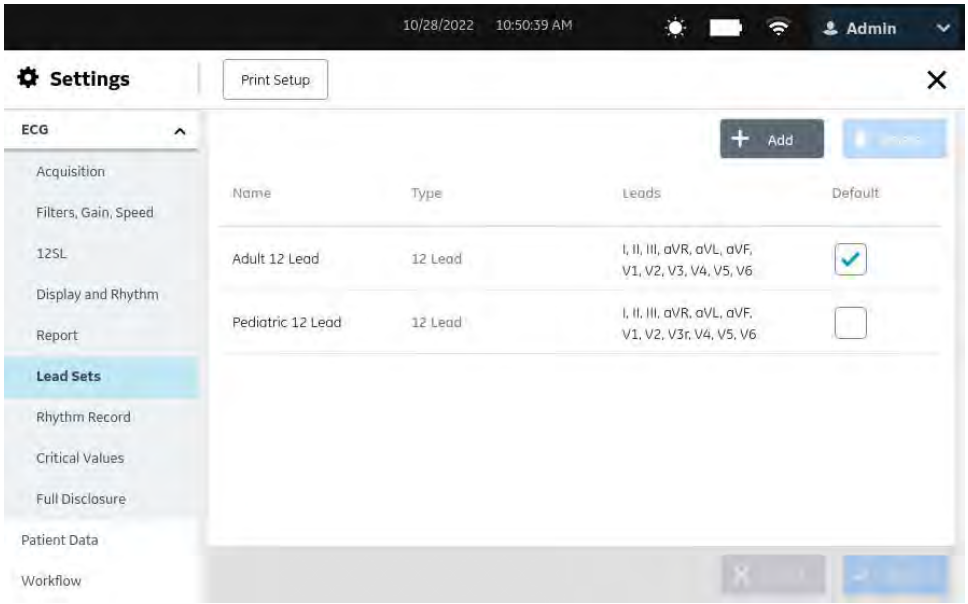
Table 10-9 Default Lead Set Configurations

Lead Set Name	Lead Set Type	Default	Lead Set Channels
Adult 12 Lead	12 Lead	Yes	CH1 to CH12: I, II, III, aVR, aVL, aVF, V1, V2, V3, V4, V5, V6
Pediatric 12 Lead	12 Lead	No	CH1 to CH12: I, II, III, aVR, aVL, aVF, V1, V2, V3r, V4, V5, V6

You can edit or delete the default or user-defined ECG lead set configurations by performing the procedure below:

1. Select **Settings** > **ECG** > **Lead Sets**.

   The **Lead Sets** screen displays.



2. Perform any of the steps below to configure a lead set, as applicable:
   - To add a user-defined lead set, perform Step 3 to Step 6.
   - To edit a user-defined lead set, perform Step 7.
   - To delete a user-defined lead set, perform Step 8.
3. Select the **Add** icon  to add an ECG lead set.

   A new row is added to the lead set table.
4. Configure the ECG lead sets.

   NOTE

   You can configure a maximum of 10 ECG lead sets.

   Table 10-10 ECG Lead Set Configuration

Field Name	Action	Description
Name	Enter a name for your lead set.	User-defined value up to 15 characters. Allowed values: • a to z • A to Z • 0 to 9 • All special characters
Type	Select the lead set type you want to include in the lead set.	Default value: **12 Lead**
Leads	Select the leads that you want to display in the waveform for the selected lead set.	Default value: I, II, III, aVR,aVL, aVF, V1, V2, V3, V4, V5, V6 Allowed values: I, II, III, aVR, -aVR, aVL, aVF, V1, V2, V3, V4, V5, V6, V3r If the **F300 - 300 Hz Acquisition** option is enabled, **Acquisition Bandwidth** displays. Default value: 150 Hz Allowed values: 150 Hz, 300 Hz **NOTE** If you set the **Acquisition Bandwidth** as 300 Hz, the name of the lead set on the **Acquisition** screen will contain **300Hz** as suffix.
Default	Enable or disable this setting.	If this setting is enabled, this is the default lead set used to display the waveform on the Acquisition screen. You can not delete the default lead set. Default value: Disabled

5. Select **Save**.
6. Repeat Step 3 to Step 5 to add more ECG lead set configurations.
7. To edit an existing ECG lead set configuration:

   7.1. Select anywhere in the row of the lead set configuration you want to modify to enable the edit mode.

7.2. Make changes to the configuration as per the information in Table 10-10 ECG Lead Set Configuration on page 134.

7.3. Select **Save**.

8. To delete an existing lead set configuration:

8.1. Select the **Delete** icon for the lead set configuration you want to delete.

NOTE

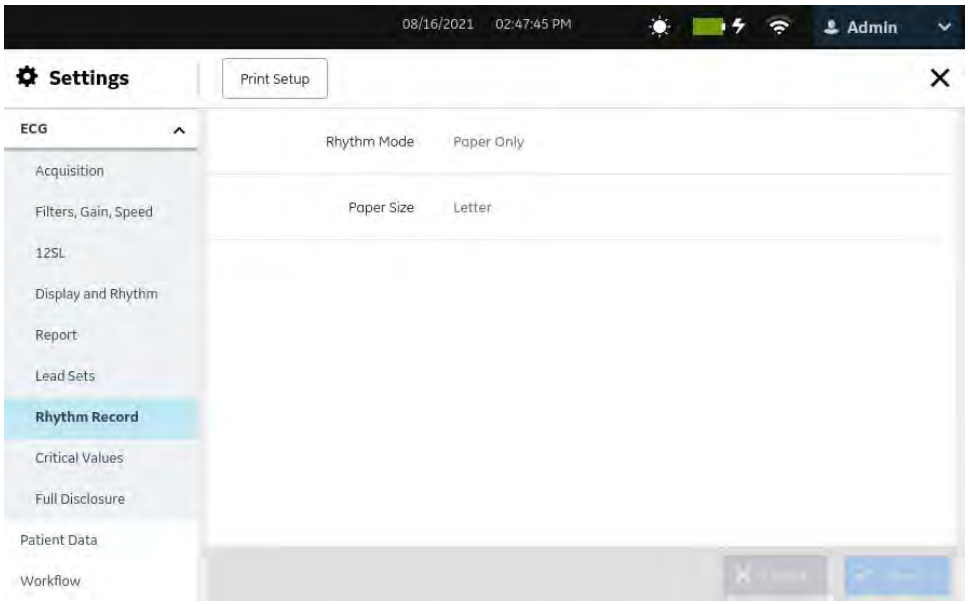
You can delete only one lead set configuration at a time. To delete more than one lead set configuration, repeat this step.

8.2. Select **Save**.

10.4.7 Configure Rhythm

1. Select **Settings** > **ECG** > **Rhythm Record**.

The **Rhythm Record** screen displays.



2. Configure the fields as per the information in the table:

Table 10-11 Rhythm Settings

Field	Action	Description
Rhythm Mode	Select a value from the drop-down list to configure the mode of recording a rhythm.	• If you select **Paper Only**, the rhythm report is printed in paper. • If you select **Digital Only**, the rhythm report is recorded and saved in the *Files* view. • If you select **Both**, the rhythm report is recorded and saved in the *Files* view and also printed in paper. • If you select **Digital Only** or **Both**, configure the rhythm speed and duration of acquisition of the rhythm. Default value: **Paper Only**

Continues on the next page

Table 10-11 Rhythm Settings (Table continued)

Field	Action	Description
Maximum Digital Rhythm Duration	Select a value from the drop-down list to configure the maximum digital rhythm duration.	This field is enabled only when **Rhythm Mode** is configured as **Digital Only** or **Both**. Default value: **300 sec** Allowed values: **10 Sec** to **300 Sec** in multiples of 10.
Rhythm Speed	Select a value from the drop-down list to configure the speed at which the rhythm is recorded.	This field is enabled only when **Rhythm Mode** is configured as **Digital Only** or **Both**. Default value: **25.0 mm/s** Allowed values: • **5.0 mm/s** • **12.5 mm/s** • **25.0 mm/s** • **50.0 mm/s**
Paper Size	Select a value from the drop-down list to configure the paper size for printing.	Default value: **Letter** Allowed values: • **A4** - available on MAC 5 A4 device • **Letter** - available on MAC 5 A4 device • **A5** - available on MAC 5 A5 device

3. Select **Save**.

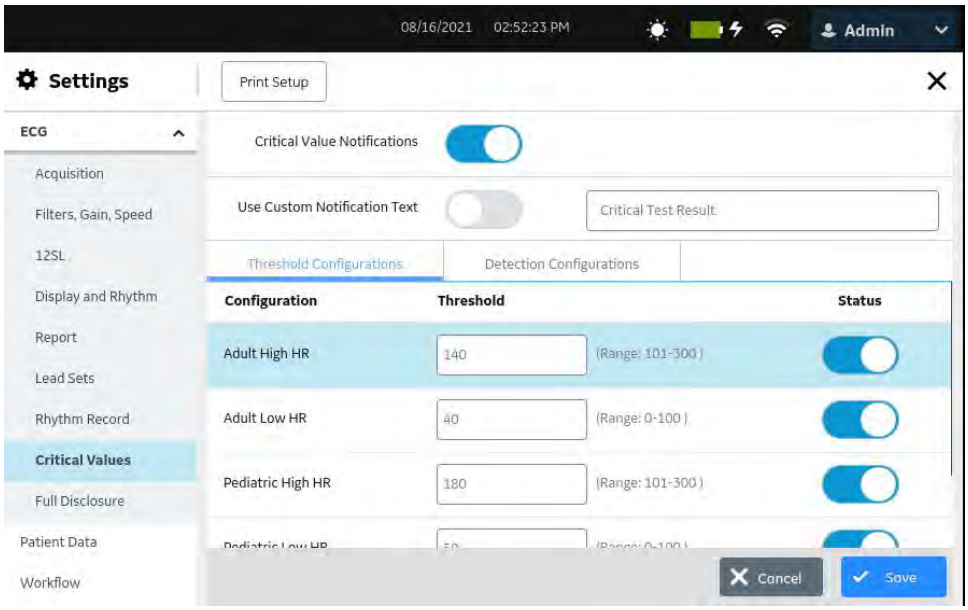
10.4.8 Configure Critical Value Notifications

Before you start this procedure, make sure that:

- The **CRIT - Critical Value Notifications** option is enabled on the device. Contact a GE Healthcare Service Support representative to enable this option.
- Your user role is assigned the privileges to access the **Settings** screen and edit critical value settings. See 10.7.4 Configure User Roles on page 207.

1. Select **Settings** > **ECG** > **Critical Values**.

   The **Critical Values** screen displays.



2. Enable the **Critical Value Notifications** setting to configure notifications to display when configured critical value thresholds are met or prescribed critical conditions are detected.
3. Enable the **Use Custom Notification Text** setting to configure custom notification text in the text field.
4. Edit the default phrase **Critical Test Result** in the text field with a customized phrase. The phrase displays on the screen during preview or review of acquired ECG patient reports, when a critical value or condition is detected.
5. Select the **Threshold Configurations** tab to display the threshold configurations for critical values.
6. Select the default critical value to change the threshold value.

   The selected value is now editable.
7. Enter the threshold for the selected critical value as per the information in the table.

Table 10-12 Threshold Critical Values

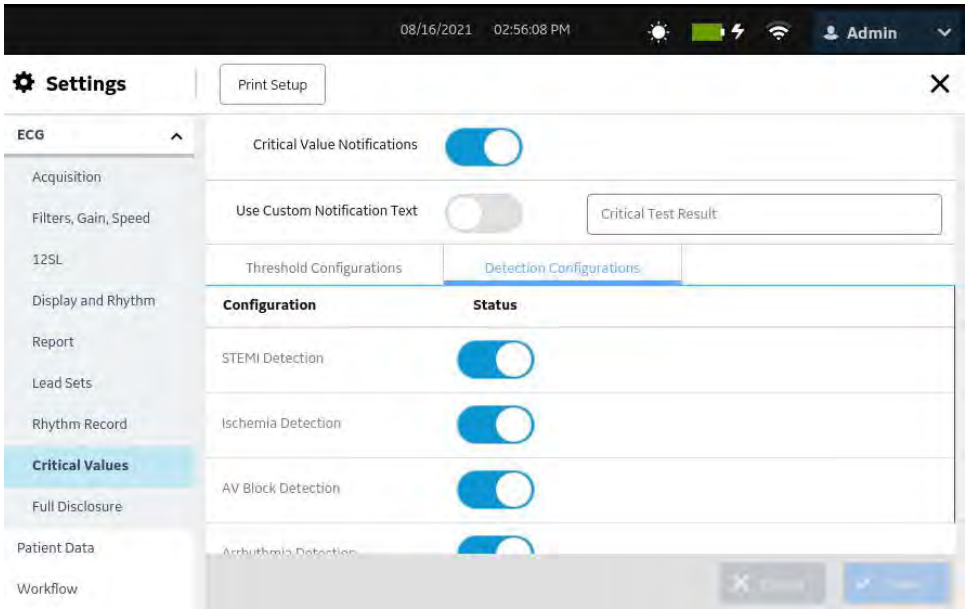
Critical Value	Allowed Threshold Range	Default Threshold Value
Adult High HR	101 to 300	**140**
Adult Low HR	0 to 100	**40**
Pediatric High HR	101 to 300	**180**
Pediatric Low HR	0 to 100	**50**
High QTc	441 to 1000	**550**

NOTE

By default, critical value notifications are enabled. If you do not want to be notified when a threshold for a specific critical value has been met, disable the **Status** setting for the corresponding critical value.

8. Select **Save** to save the changes.

9. Select the **Detection Configurations** tab to display the detection configurations for critical conditions.



10. Enable or disable notifications when the critical conditions below are detected:
    - **STEMI Detection**
    - **Ischemia Detection**
    - **AV Block Detection**
    - **Arrhythmia Detection**

    NOTE

    By default, notifications are enabled.

11. Save and close the screen.

    The **Acquisition** screen displays.

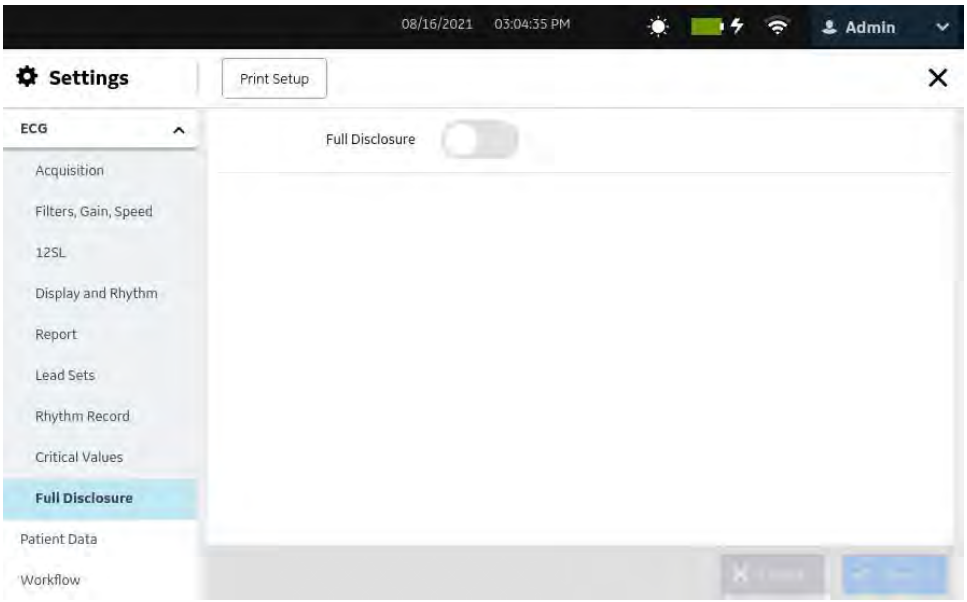
10.4.9 Configure Full Disclosure

Before you start this procedure, make sure that:

- The **FLDS - Full Disclosure** option is enabled on the device. Contact a GE Healthcare Service Support representative to enable this option.
- Your user role is assigned the privileges to access the **Settings** screen. See 10.7.4 Configure User Roles on page 207.

1. Select **Settings** > **ECG** > **Full Disclosure**.

   The **Full Disclosure** screen displays.



2. Do one of the below steps.
   - Enable the **Full Disclosure** setting and select **Save** to activate the full disclosure functionality.

     The **FD** tab is available on the Acquisition screen.
   - Disable the **Full Disclosure** setting and select **Save** to deactivate the full disclosure functionality.

     The **FD** tab is not available on the Acquisition screen.

10.5 Configure Patient Data

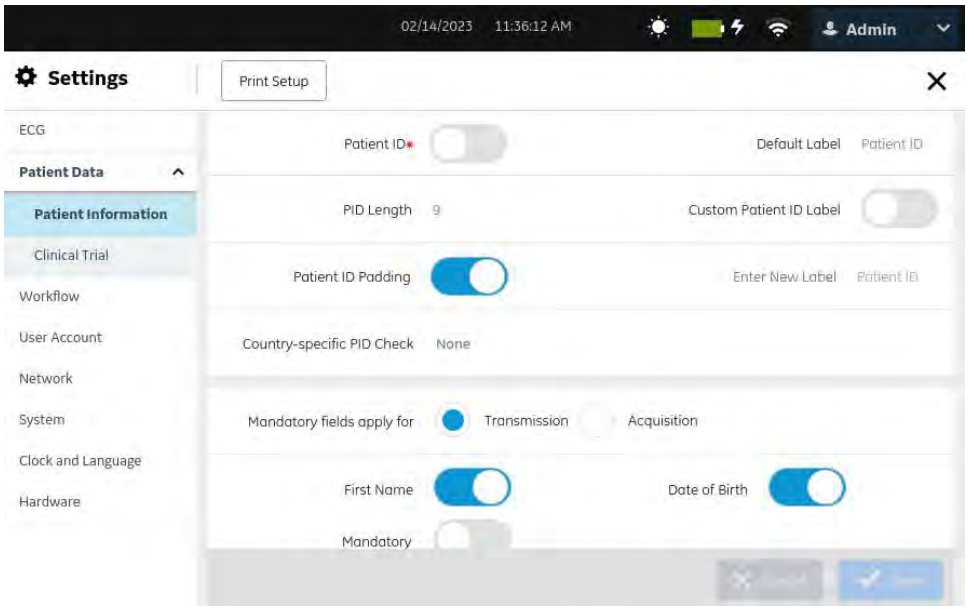
Select **Settings** > **Patient Data** menu to configure the following:

- Patient Information - 10.5.1 Configure Patient Information on page 139
- Clinical Trail - 10.5.2 Configure Clinical Trial on page 145

10.5.1 Configure Patient Information

1. Select **Settings** > **Patient Data** > **Patient Information**.

   The **Patient Information** screen displays.



2. Configure the fields as per the information in the table.

NOTE

If you enable a field in the **Mandatory** column and **Mandatory fields apply for Transmission** or **Acquisition** option, it becomes a required field or option settings and an asterisk (*) displays next to the field on the **Patient Information** screen.

Table 10-13 Patient Information Settings

Field	Action	Description
Patient ID	Patient ID cannot be disabled.	You can enable or disable this field in the **Required** column to make it required or optional in the **Patient Information** screen. Default value: Disabled
PID Length	Enter a value to configure the length of the patient ID in the **Patient Information** screen, if Patient ID is not country-specific. You can edit this field only if **Country Specific PID check** is **None**.	Default value: • **12** for Norwegian • **13** for Swedish • **11** for Danish and Turkish • **9** for other languages Allowed values: 3 to 16
Patient ID Padding	Enable or disable this setting.	• If this setting is enabled, the patient ID is padded with the required number of leading zeros as per the configured PID length. • If this setting is disabled, the patient ID is not padded with leading zeros as per the configured PID length. Default value: Enabled

Continues on the next page

Table 10-13 Patient Information Settings (Table continued)

Field	Action	Description
Country-specific PID Check	Select a value from the drop-down list to enable the configuration of the Patient ID according to the country selected.	The value is automatically set as the country specified, when the device language is set to that country and the device is restored to factory defaults. This is applicable for Danish, Swedish, and Norwegian. The value is automatically set as **None** when the device language below is set and the device is restored to factory defaults. • English • Chinese • Dutch • Finnish • French • German • Italian • Japanese • Korean • Czech • Portuguese • Russian • Spanish • Brazilian Portuguese • Polish • Turkish Default value: **None** Allowed values: • **None** • **Danish** • **Norwegian** • **Swedish**
Custom Patient ID Label	Enable or disable this setting.	• If this setting is enabled, the **Enter New Label** field displays. • If this setting is disabled, the default label **Patient ID** displays in the **Patient Information** screen. Default value: Disabled
Enter New Label	Enter the label name to display in the **Patient Information** screen.	Default value: **Patient ID** Allowed values: • A to Z • a to z • 0 to 9 • All special characters

Continues on the next page

Table 10-13 Patient Information Settings (Table continued)

Field	Action	Description
Mandatory fields apply for	Enable or disable the **Transmission** or **Acquisition** setting.	If the **Transmission** setting is enabled, the mandatory fields need to be set in the **Patient Information** screen. Otherwise the transmission of the ECG report is failed until you set the values for mandatory fields. If the **Acquisition** setting is enabled, the mandatory fields need to be set in the **Patient Information** screen. Otherwise the ECG report will not be saved until you set the values for mandatory fields. Default value: **Transmission**
First Name	Enable or disable this setting.	Displays or hides the field on the **Patient Information** screen. If this field is configured to display, you can enable or disable the field in the **Mandatory** column. Default value: Enabled
Last Name	Enable or disable this setting.	Displays or hides the field in the **Patient Information** screen. If this field is configured to display, you can enable or disable the field in the **Mandatory** column. Default value: Enabled
Height	Enable or disable this setting.	Displays or hides the field in the **Patient Information** screen. Default value: Enabled
Weight	Enable or disable this setting.	Displays or hides the field in the **Patient Information** screen. Default value: Enabled
Age	Enable or disable this setting.	Displays or hides the field in the **Patient Information** screen. **NOTE** If the **Age** field is enabled, the **Date of Birth** field cannot be enabled, and the **Patient Information** screen will not display the **Date of Birth**. Default value: Disabled
Date of Birth	Enable or disable this setting.	Displays or hides the field in the **Patient Information** screen. **NOTE** If the **Date of Birth** field is enabled, the **Age** field cannot be enabled, and the **Patient Information** screen will not display the **Age**. Default value: Enabled
Gender	Enable or disable this setting.	Displays or hides the field in the **Patient Information** screen. Default value: Enabled

Continues on the next page

Table 10-13 Patient Information Settings (Table continued)

Field	Action	Description
Race	Enable or disable this setting.	Displays or hides the field in the **Patient Information** screen. This setting is automatically enabled when the device language below is set and the device is restored to factory defaults: • English • Chinese • Finnish • French • Italian • Japanese • Korean • Portuguese • Russian • Spanish • Brazilian Portuguese • Polish • Turkish • Czech This setting is automatically disabled when the device language below is set and the device is restored to factory defaults: • Danish • Dutch • German • Swedish • Norwegian
Blood Pressure	Enable or disable this setting.	Displays or hides the field in the **Patient Information** screen. Default value: Disabled
Medications	Enable or disable this setting.	Displays or hides the field in the **Patient Information** screen. Default value: Enabled
Referring MD Last Name	Enable or disable this setting.	Displays or hides the field in the **Patient Information** screen. Default value: Enabled
Referring MD First Name	Enable or disable this setting.	Displays or hides the field in the **Patient Information** screen. Default value: Enabled
Ordering MD First Name	Enable or disable this setting.	Displays or hides the field in the **Patient Information** screen. Default value: Disabled
Ordering MD Last Name	Enable or disable this setting.	Displays or hides the field in the **Patient Information** screen. Default value: Disabled
Referring MD ID	Enable or disable this setting.	Displays or hides the field in the **Patient Information** screen. Default value: Disabled
Bed Number	Enable or disable this setting.	Displays or hides the field in the **Patient Information** screen. Default value: Disabled

Continues on the next page

Table 10-13 Patient Information Settings (Table continued)

Field	Action	Description
Comments	Enable or disable this setting.	Displays or hides the field in the **Patient Information** screen. Default value: Disabled
Test Indication	Enable or disable this setting.	Displays or hides the field in the **Patient Information** screen. Default value: Enabled
Location	Enable or disable this setting.	Displays or hides the field in the **Patient Information** screen. If this field is configured to be displayed, you can enable or disable the field in the **Mandatory** column. Enable this field for **Location ID** to be sent to the MUSE server. Default value: Disabled
Room Number	Enable or disable this setting.	Displays or hides the field in the **Patient Information** screen. Default value: Disabled
Priority	Enable or disable this setting.	Displays or hides the field in the **Patient Information** screen. Default value: Disabled
Patient History	Enable or disable this setting.	Displays or hides the field in the **Patient Information** screen. Default value: Disabled
Technician	Enable or disable this setting.	Displays or hides the field in the **Patient Information** screen. If this field is configured to display, you can enable or disable the field in the **Mandatory** column. Default value: Enabled
Visit Number	Enable or disable this setting.	Displays or hides the field in the **Patient Information** screen. If this field is configured to display, you can enable or disable the field in the **Mandatory** column. Default value: Enabled
Order Number	Enable or disable this setting.	Displays or hides the field in the **Patient Information** screen. If this field is configured to display, you can enable or disable the field in the **Mandatory** column. Default value: Enabled
Secondary ID	Enable or disable this setting.	Displays or hides the field in the **Patient Information** screen. If this field is configured to display, you can enable or disable the field in the **Mandatory** column. Default value: Disabled
Ordering MD ID	Enable or disable this setting.	Displays or hides the field in the **Patient Information** screen. Default value: Enabled
Attending MD ID	Enable or disable this setting.	Displays or hides the field in the **Patient Information** screen. Default value: Disabled
Attending MD First Name	Enable or disable this setting.	Displays or hides the field in the **Patient Information** screen. Default value: Disabled
Attending MD Last Name	Enable or disable this setting.	Displays or hides the field in the **Patient Information** screen. Default value: Disabled

Continues on the next page

Table 10-13 Patient Information Settings (Table continued)

Field	Action	Description
Question 1 **Question 2** **Question 3** **Question 4**	Enable or disable this setting.	Displays or hides the fields in the **Patient Information** screen. Default value: Disabled
Question	Enter the question to display in the **Patient Information** screen.	This field is enabled if the related **Question** field is enabled. Default value: No default value Allowed values: 10 characters • A to Z • a to z • 0 to 9 • All special characters
Answer Type	Select a value from the drop-down list to enable the configuration of the answer type for each question.	This field is enabled if the related Question field is enabled. Default value: **Alphanumeric** Allowed values: • **Alphanumeric** • **Numeric** • **Yes or No or Unknown**

3. Select **Save**.

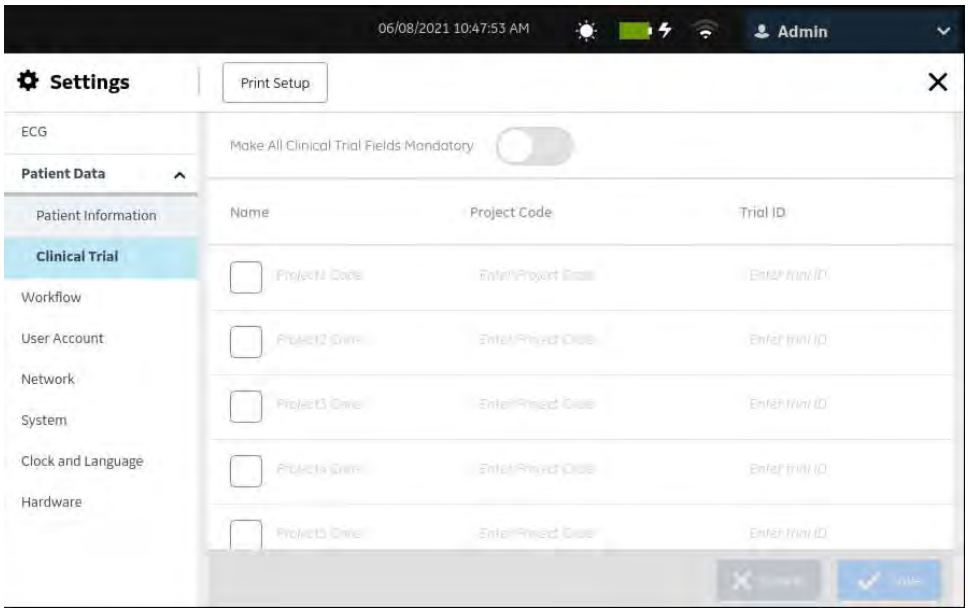
10.5.2 Configure Clinical Trial

Before you start this procedure, make sure that:

- The **PHAR - Pharmacy** option is enabled on the device. Contact a GE Healthcare Service Support representative to enable this option.
- Your user role is assigned the privileges to access the *Settings* screen. See 10.7.4 Configure User Roles on page 207.

1. Select **Settings** > **Patient Data** > **Clinial Trial**.

   The **Clinial Trial** screen displays.



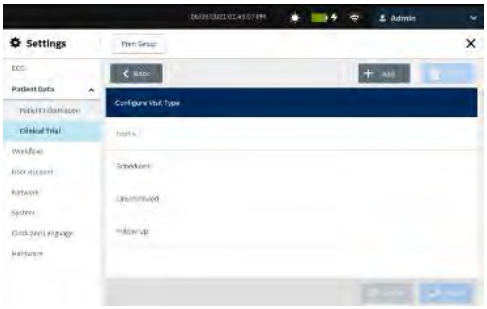
2. Configure the fields as per the information in the table.

Table 10-14 Clinical Trial Settings

Field	Action	Description
Make All Clinical Trial Fields Mandatory	Enable or disable this setting.	If you enable this setting, all the configured clinical trial settings are required fields and an asterisk (*) displays next to each field on the **Clinical Trial** screen. If you disable this setting, all the configured clinical trial settings are optional fields on the **Clinical Trial** screen. Default value: Disabled
Name: • **Project1 Code** • **Project2 Code** • **Project3 Code** • **Project4 Code** • **Project5 Code**	Enable or Disable this setting.	If you select one **Name**, the configured **Project Code** displays in the drop down list of the **Project Code Name** field in the **Clinical Trial** screen. Default value: Disabled
Project Code	Enter the information to display in the **Project Code** field on the **Clinical Trial** screen.	This field is enabled if the related **Name** field is selected. Default value: **Enter Project Code** Allowed value:
Trial ID	Enter the information to display in the **Trial ID** field on the **Clinical Trial** screen.	This field is enabled if the related **Name** field is selected. Default value: **Enter Trial ID** Allowed value:
Trial Visit Number	Enable or Disable this setting.	Displays or hides the field in the **Clinical Trial** screen. Default value: Disabled

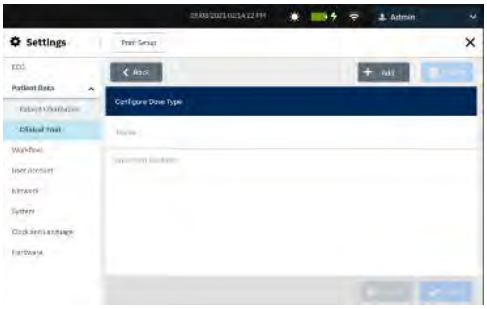
Continues on the next page

Table 10-14 Clinical Trial Settings (Table continued)

Field	Action	Description
Visit Type	Enable or Disable this setting.	Displays or hides the field in the **Clinical Trial** screen. Default value: Disabled If you enable this setting, follow below steps to configure the visit types displaying in the drop down list of the **Visit Type** field in the **Clinical Trial** screen. 1. Select **Configure**. The **Configure Visit Type** screen displays.  Default values: • **Scheduled** • **Unscheduled** • **Follow Up** • **Repeat** • **Early Termination** • **Unknown** 2. Perform any of the below actions to configure a visit type, as applicable: • To add a visit type, select **Add**, then enter the information into the new row. • To edit a visit type, select the text in the row of the visit type you want to modify, then make changes. • To delete a visit type, select the text in the row of the visit type you want to delete, then a massage displays asking you to confirm if you want to delete the visit type. ◦ Select **Yes** to confirm the delete. ◦ Select **No** to cancel the delete. 3. Select **Save**.

Continues on the next page

Table 10-14 Clinical Trial Settings (Table continued)

Field	Action	Description
Dose Type	Enable or Disable this setting.	Displays or hides the field in the **Clinical Trial** screen. Default value: Disabled If you enable this setting, follow below steps to configure the visit types displaying in the drop down list of the **Dose Type** field in the **Clinical Trial** screen. 1. Select **Configure**. The **Configure Dose Type** screen displays.  Default value: **No Record Available** 2. Perform any of the below actions to configure a dose type, as applicable: • To add a dose type, select **Add**, then enter the information into the new row. • To edit a dose type, select the text in the row of the visit type you want to modify, then make changes. • To delete a dose type, select the text in the row of the visit type you want to delete, then a massage displays asking you to confirm if you want to delete the dose type. ◦ Select **Yes** to confirm the delete. ◦ Select **No** to cancel the delete. 3. Select **Save**.
Investigator ID	Enable or Disable this setting.	Displays or hides the field in the **Clinical Trial** screen. Default value: Disabled
Question 1 **Question 2** **Question 3** **Question 4** **Question 5**	Enable or disable this setting.	Displays or hides the fields in the **Clinical Trial** screen. Default value: Disabled
Question	Enter the question to display in the **Clinical Trial** screen.	This field is enabled if the related **Question** field is enabled. Default value: No default value Allowed values: 10 characters • A to Z • a to z • 0 to 9 • All special characters

Continues on the next page

Table 10-14 Clinical Trial Settings (Table continued)

Field	Action	Description
Answer Type	Select a value from the drop-down list to enable the configuration of the answer type for each question.	This field is enabled if the related **Question** field is enabled. Default value: **Alphanumeric** Allowed values: • **Alphanumeric** • **Numeric** • **Yes or No or Unknown**

3. Select **Save**.

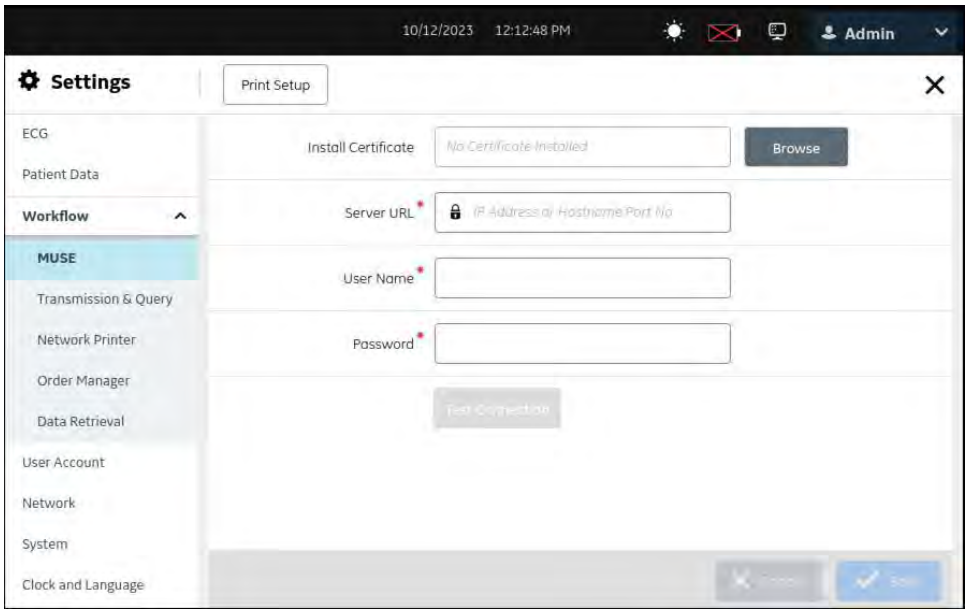
10.6 Configure Workflow

Select **Settings** > **Workflow** menu to configure the following:

- MUSE - 10.6.1 Configure the MUSE Server Settings on page 149
- Transmission & Query - 10.6.2 Configure Transmission & Query Settings on page 154
- Network Printer - 10.6.3 Configure Network Printer on page 186
- Order Management - 10.6.4 Configure Order Management on page 188
- Data Retrieval - 10.6.6 Configure Data Retrieval on page 197

10.6.1 Configure the MUSE Server Settings

1. Select **Settings** > **Workflow** > **MUSE**.



2. Configure the MUSE server settings as per the information in the table.

Table 10-15 MUSE Server Settings for Orders

Field	Action	Description
Install Certificate	Browse and install a valid MUSE CA certificate.	If you configure a https URL, a valid CA certificate is required to authenticate and connect to the MUSE server. Install the CA certificate. See 10.6.1.1 Install MUSE SSL CA Certificate on page 152. **NOTE** The connection to the MUSE server is allowed, if a valid certificate is installed in the system with qualified authentication. To delete the CA certificate, see 10.6.1.2 Delete MUSE SSL CA Certificate on page 153. If you configure a http URL, a valid CA certificate is not required to authenticate and connect to the MUSE server. Default value: Disabled
Server URL	Enter a valid http or https URL of the MUSE server.	**NOTE** **You can secure some communication channels with encryption and authentication. GE Healthcare recommends that you use the encrypted channels, not the unencrypted channels. For example:** • **Upgrade the MUSE server 9.0 API3 version to the MUSE NX API3 version, to have a secure communication between the MAC 5 system and the MUSE server.** The URL must correspond to the MUSE system. Allowed values: A valid http or https URL with defined FQDN or IP address and a port number. Use a Fully Qualified Domain Name (FQDN) or IP address. Add the port number after the URL with a colon (:) specifier. **NOTE** Define the port number if it is not defined. • HTTP - 8100 • HTTPS - 443 Determine which MUSE version you will connect to and configure the URL: • MUSE system V9: HTTP **NOTE** MUSE system V9 default port is 8100. • MUSE NX system: HTTPS

Continues on the next page

Table 10-15 MUSE Server Settings for Orders (Table continued)

Field	Action	Description
User Name	Enter the MUSE account user name.	This field cannot be blank. Default value: No default value **NOTE** This is a MUSE account, not a Windows account. GE Healthcare recommends that this user have restricted privileges, but must have the minimum privilege to download the orders and patient tests. Allowed values: Up to 128 characters • a to z • A to Z • 0 to 9 • All special characters
Password	Enter the MUSE account user password.	Default value: No default value Allowed values: Up to 128 characters • a to z • A to Z • 0 to 9 • All special characters

3. Select **Test Connection**.
   - If the connection succeeds, proceed to save the configuration.
   - If the connection fails, the error messages below display:
     - **Certificate validation failed** - the error is due to an invalid certificate for MUSE NX.
     - **The username or password is incorrect** - the error is due to an incorrect username or password.
     - **Request timed-out** - the error is due to server request time out.
     - **Cannot connect to the server. Host not found** - the error is due to the host being unavailable.
     - **Authorization failed** - the error is due to incorrect site number set in the ECG acquisition device or an insufficient user privilege for a particular site.
     - **Invalid token** - the error is due to an invalid token exception during test connection.
     - **Test failed** - the error is due to other causes which are not included in the list.

   Rectify the errors and retest the connection.
4. Select **Save**.

   If the MAC 5 device is set for LDAP authentication and Order Management with the MUSE system, when a user authenticates through LDAP, the MAC 5 connects to the MUSE server through MUSEAPI3. It checks if any users in MUSE User Setup have a Windows username that matches the user that logged into the MAC 5 device.

- If the users match, the MAC 5 will get the MUSE User ID for that user in the **Technician ID** field on the MAC 5 test entry screen.
- If a matching user is not found, the **Technician ID** field on the MAC 5 test entry screen is not filled.

When a matching user is not found in the MUSE system, the error **(For No user found for userName="x")** , where **x** is the username entered at the MAC 5 device, logs in the MUSE application log.

If you use the **Default** domain, a user can login to the MAC 5 with the username instead of the **domain\username** format.

If a user does not enter their username as **domain\username**, the MUSEAPI3 user lookup call will not find the user.

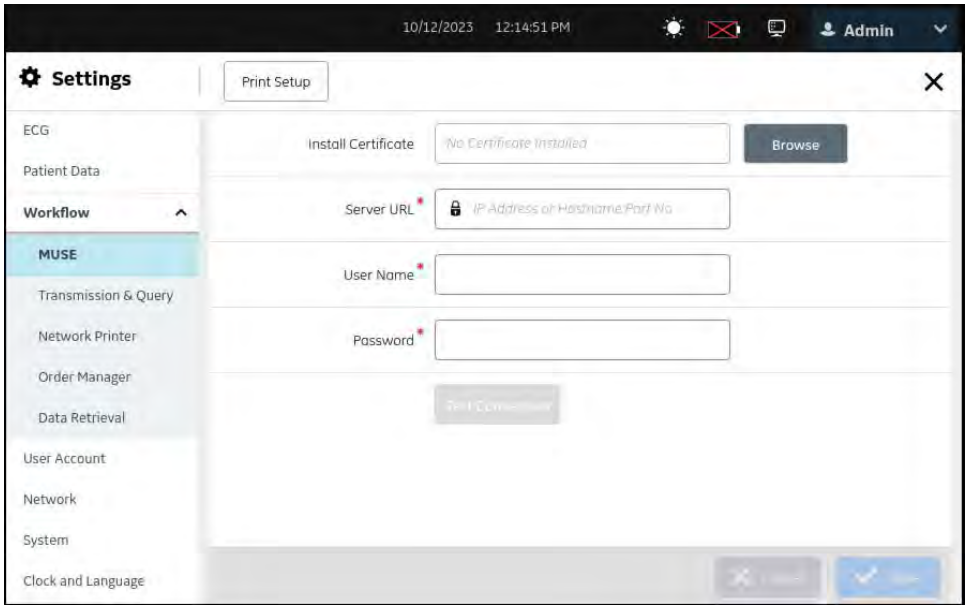
For order download time configuration in the MUSE server, refer to F.4 MUSE Order Download Time on page 307.

10.6.1.1 Install MUSE SSL CA Certificate

Before you start this procedure, make sure that:

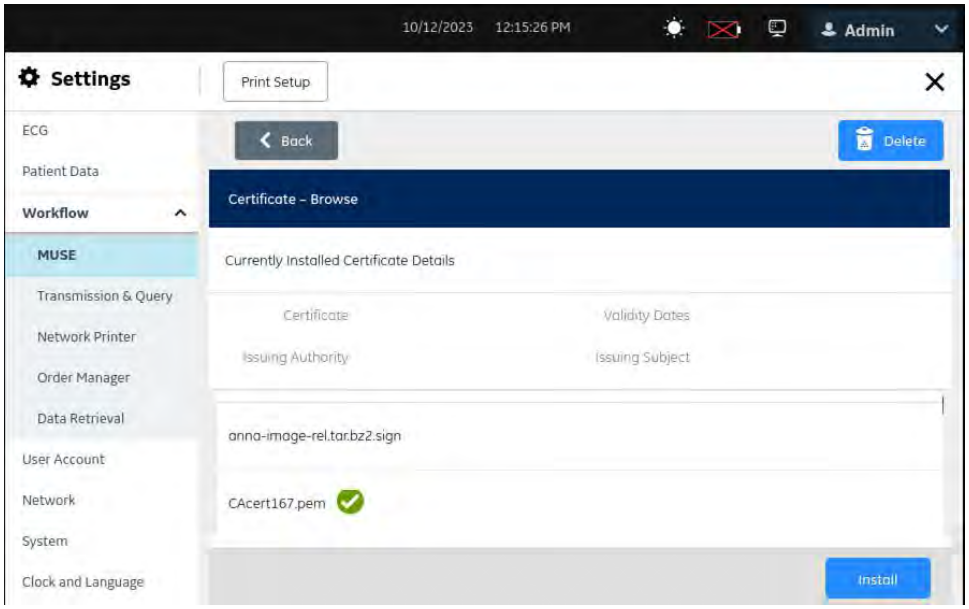
- You obtain the required certificate in the PEM format from your IT department and copy it to the root folder of a USB flash drive for installation.
- The **Enable External USB Storage** is enabled in **Settings** > **System** > **Storage** setting. If this setting is not enabled, access to USB flash drives is blocked.
- You enable at least one USB port in **Settings** > **Hardware** > **USB Port** setting. If this setting is not enabled, the device will not recognize the USB flash drives.

1. Connect the USB flash drive containing the CA certificate to the device.
2. Select **Settings** > **Workflow** > **MUSE** to view the MUSE server settings.



3. Perform the steps below to install a CA certificate:

3.1. Select **Browse** adjacent to the **Install Certificate** field and select the CA certificate from the USB flash drive.



3.2. Select **Install**.

- If the installation is successful, the CA certificate is saved.
- If the installation fails because the certificate is in an unrecognized format, an error message displays.

4. Select **Back** to view the MUSE server setting screen.

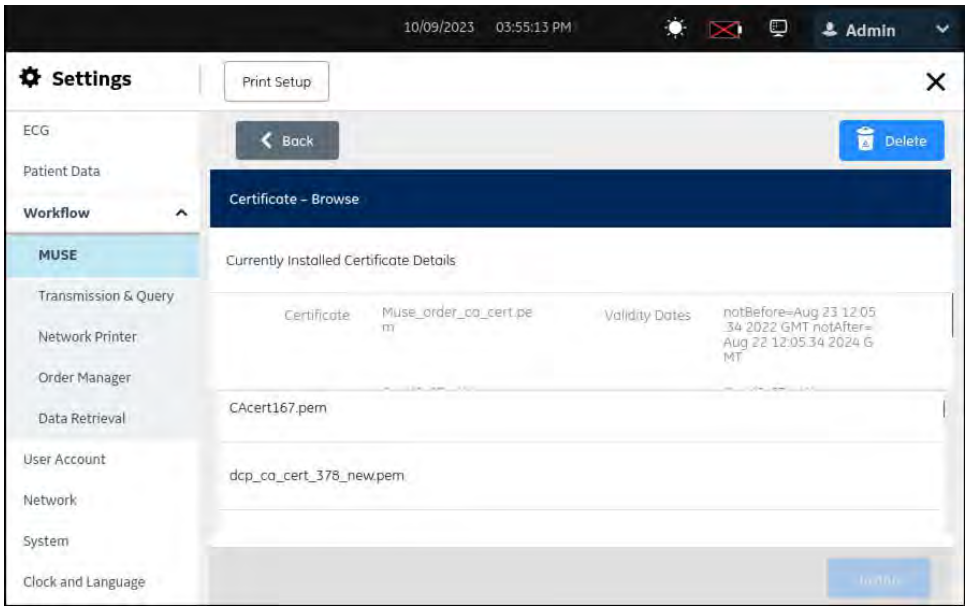
10.6.1.2 Delete MUSE SSL CA Certificate

Before you start this procedure, make sure that your user role is assigned with user management privilege.

1. Select **Settings** > **Workflow** > **MUSE** to view the MUSE server settings.
2. Perform the steps below to delete the currently installed MUSE CA certificate:

2.1. Select **Browse** adjacent to the **Install Certificate** field.

The currently installed certificate displays.



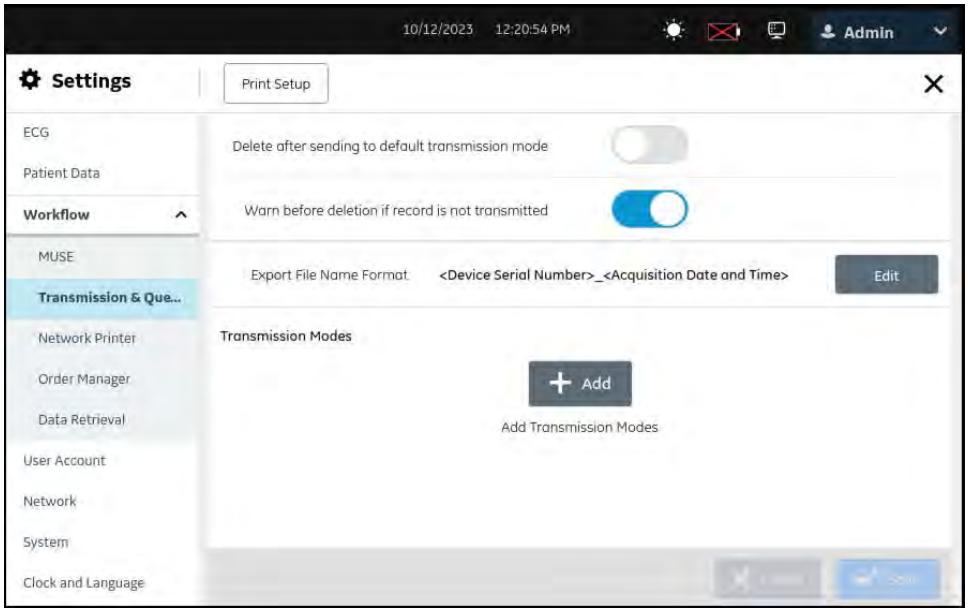
2.2. Select **Delete**.

A message displays asking you to confirm the deletion of the certificate.

2.3. Select **Yes**. The certificate or key is deleted.

3. Select **Back** to view the MUSE server setting screen.

10.6.2 Configure Transmission & Query Settings



1. Select **Settings** > **Workflow** > **Transmission & Query**.
2. Enable or disable **Delete after sending to default transmission mode** to configure auto-deletion of the ECG patient report from the *Files* list after it is sent to the default destination.

   When **Delete after sending to default transmission mode** is enabled and user does not have **Delete Reports** privilege, the report continues to be deleted after transmission.

3. Enable or disable **Warn before deletion if record is not transmitted** to display a warning message before deletion if the ECG patient report has not been transmitted to the default destination. This setting is enabled by default.
4. Select **Save**.
5. Proceed to configure the filename and any of the destinations below for patient report transmission:
   - 10.6.2.1 Configure File name for Transmission on page 155
   - 10.6.2.2 Configure a USB Destination to Transmit Reports on page 160
   - 10.6.2.4 Configure a DCP Server Destination to Transmit Reports on page 162
   - 10.6.2.7 Configure a Shared Directory to Transmit Reports on page 182
   - 10.6.2.6 Configure an SFTP Destination to Transmit Reports on page 176

10.6.2.1 Configure File name for Transmission

You can configure the file name format for transmission to identify the transmitted file in the destination system. The file name format is supported for USB, Shared Directory, and SFTP transmission modes, and all supported file types (.pdf, xml, and .ecg).

Table 10-16 Configure Export File Name Format

Field	Action	Description
Export File Name Format	Select **Edit** to configure the export file name format.	Allows you to configure a file name format for files that are transmitted to USB, Shared Directory, and SFTP destinations. Use any of the below fields to configure a file name format: • Patient ID • Patient First Name • Patient Last Name • Date of Birth • Visit Number • Secondary ID • Acquisition Date and Time • Export Date and Time • Device Serial Number • Product Version • Device Number • Test Type (ECG/RHY/FD) Default value: Device Serial Number_Acquisition Date and Time

The file system utilities and name conventions on different systems prevent below characters from file names during transmission to the destination. The system removes the start and last spaces from the file name field and deletes the below characters from the export file names:

- / (slash) - Used as a path name component separator
- \ (backslash) - Used as the default path name component separator

- ? (question) – Used as a wildcard
- * (asterisk) - Used as a wildcard
- : (colon) - Used to determine the mount point
- | (pipe) - Designates software pipelining
- “ (double quote) - A legacy restriction carried over from DOS
- < (less than) - Used to redirect input
- > (greater than) - Used to redirect output
- . (period/dot) – folder names cannot end with period

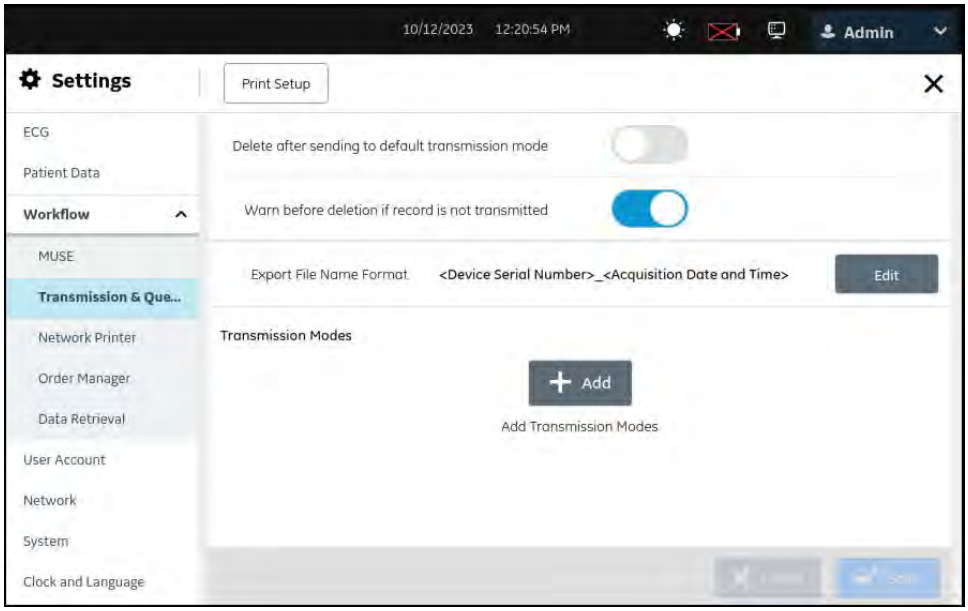
The exported file name appends (_) in the configured field:

- If the file name field is NOT configured in **Patient Data** settings.
- The file name field is configured in **Patient Data** settings, and if the value is NOT entered in the **Patient Banner**.

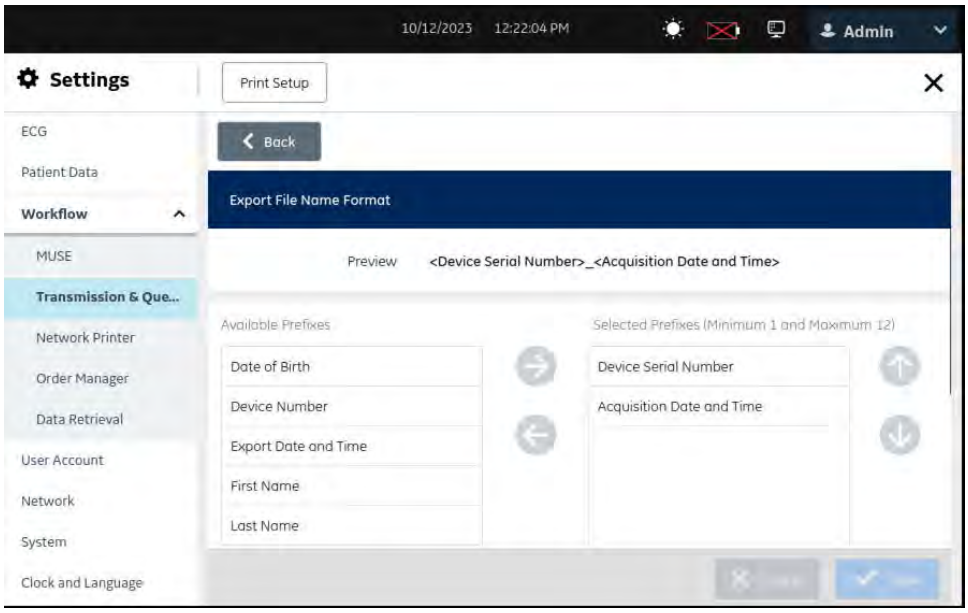
If the file name is > 255 characters, the system limits the file name length to a maximum of 255 characters.

GE Healthcare recommends that you configure unique file name format to prevent overwriting of files to the exported destinations (USB/SFTP/Shared Directory). To configure the file name for transmission, perform the procedure below.

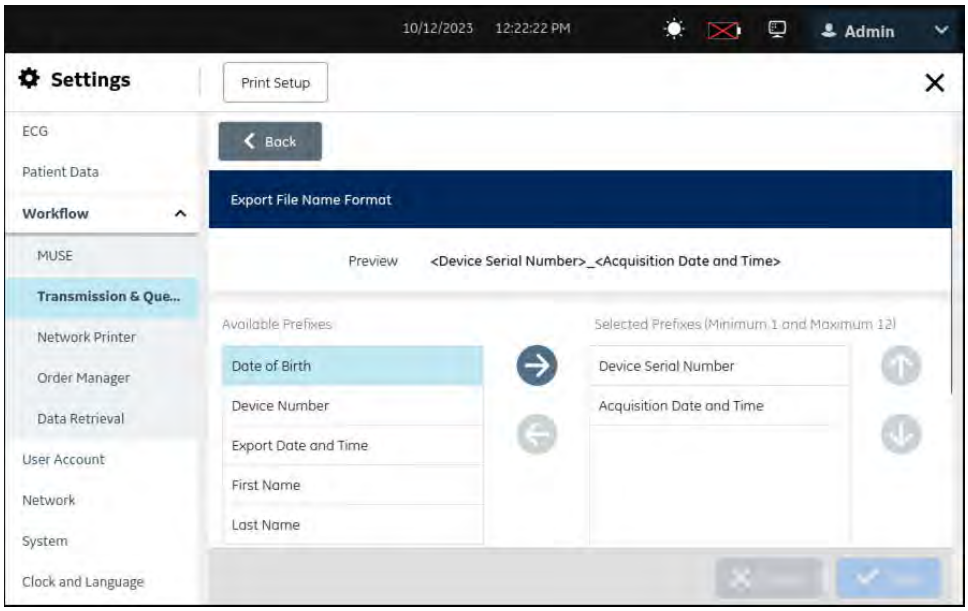
1. Select **Settings** > **Workflow** > **Transmission & Query**.

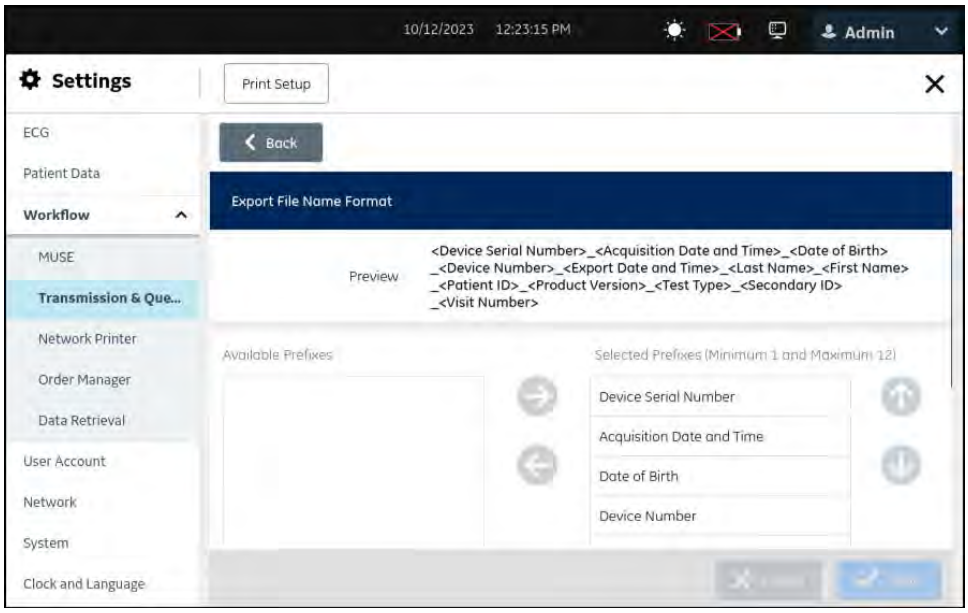


2. Select **Edit** to update the **Export File Name Format**.

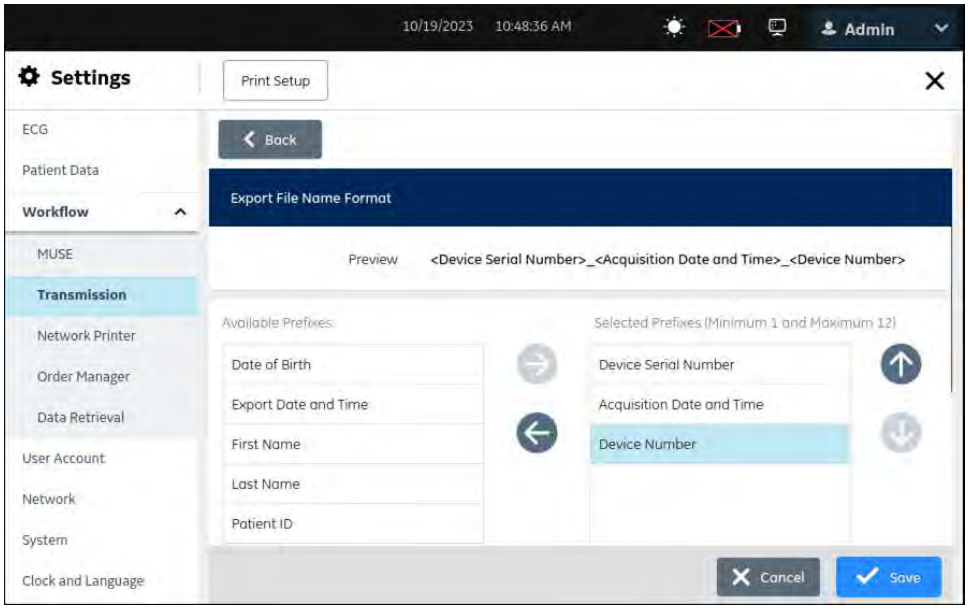


3. You can select and click  to move one or more than one file name prefixes from the **Available Prefixes** list to the **Selected Prefixes** list. You can move all of the available prefixes to the **Selected Prefixes**.





4. Select the fields and click  to move the fields from the **Selected Prefixes** to **Available Prefixes**.



NOTE

You need to add a minimum of one field in the **Selected Prefixes** list to configure the export file name format.

5. Scroll up  and down  to change the prefix position in the export file name format.

NOTE

When you configure a file name, you can configure any prefixes from the **Available Prefixes** list, regardless if it is enabled or disabled in the **Patient Data** settings.

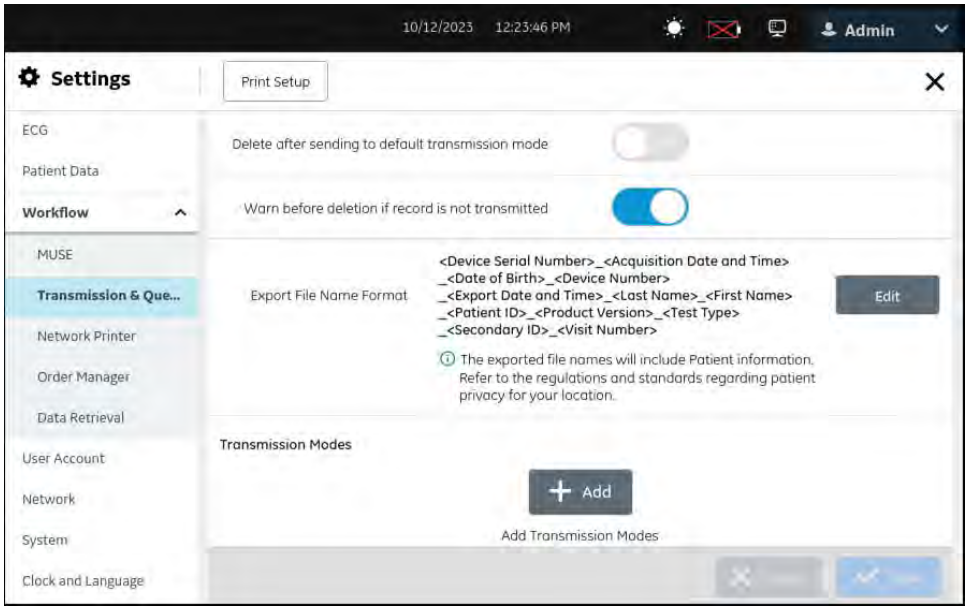
6. Select **Save** to save the configured prefixes to the file name.

NOTE

If you want to configure any of the below patient information to the file name, an additional confirmation window displays to request for your reconfirmation:

- Patient ID
- Patient First Name
- Patient Last Name
- Date of Birth
- Secondary ID

You can cancel and remove the patient information fields from the **Selected Prefixes** and save it again. If you configure the file name with the patient information, the **Workflow** > **Transmission & Query** settings display the patient information along with the preview.



Below are the examples of exported file name formats for supported file types .pdf/.xml/.ecg:

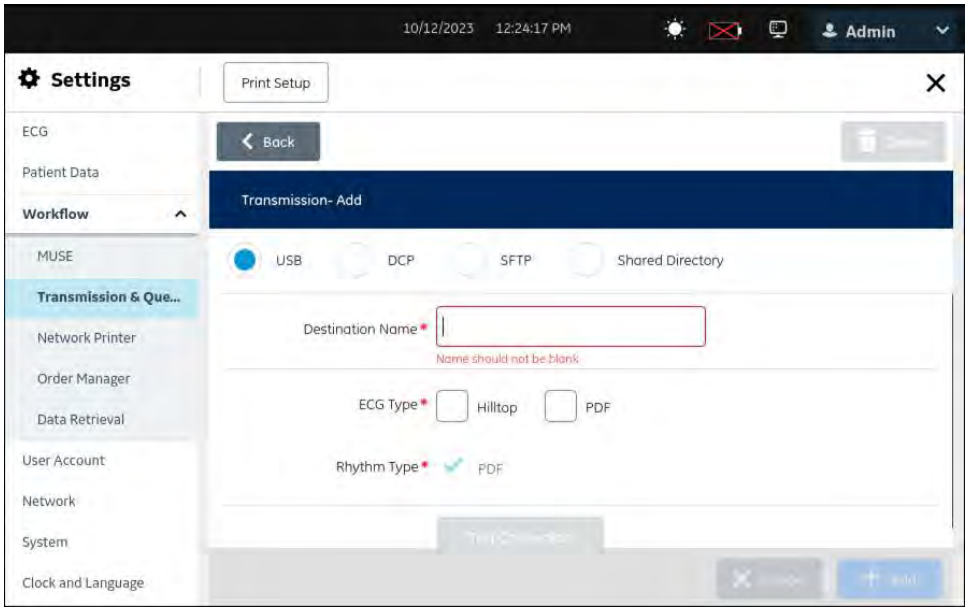
- The file name with default values - *ABC12345678EE_20211202_144157.pdf*
- The file name with empty Last Name, Patient ID, and empty First Name - *_TestPid123_.xml*

The file name can contain translated characters (including accented characters) if the user inputs from the barcode, keyboard, orders, or ADT query for the configured fields.

10.6.2.2 Configure a USB Destination to Transmit Reports

- Make sure that the setting to allow access to external storage devices is enabled in the **System** > **Storage**. See 10.9.2 Configure External Storage on page 241.
- Make sure that **USB port** is enabled and the USB flash drive with a key file is inserted into the device. See 10.11.2 Configure the USB Ports on page 260.

1. Select **Settings** > **Workflow** > **Transmission & Query**.
2. Select the **Add** icon to add transmission modes.
3. Select **USB** to configure a USB server destination.



4. Configure the destination as per the information in the table.

Table 10-17 Configure a USB Destination to Transmit Reports

Field	Action	Description
Destination Name	Enter the name of the USB destination where the reports will be sent.	Allowed values: • A to Z • a to z • 0 to 9 • All special characters
ECG Type	Select the supported file type of ECG report sent through USB by your facility.	You can select multiple format types. Default available values: • **Hilltop** • **PDF** Allowed values (Option): • **XML** (This type is available only if XML format output is enabled in **Option Manager**). • **Hilltop** • **PDF**

Continues on the next page

Table 10-17 Configure a USB Destination to Transmit Reports (Table continued)

Field	Action	Description
Rhythm Type	Select the supported file type of rhythm report sent through USB by your facility.	Default and allowed value: **PDF**

5. Select **Test Connection** to test the configured connection.
   - If the test displays `Test Successful`, you have a successful connection to that destination.
   - If the test displays `Test Failed`, you do not have a connection to that destination. Troubleshoot the connection failure by confirming that the USB flash drive is firmly seated, test, and add the connection.
6. Select **Save**.
7. Repeat steps 2 to 6 to add more USB destinations.
   - To edit a USB destination, perform Step 8.
   - To delete a USB destination, perform Step 9.
8. To edit an existing USB destination:
   8.1. Select anywhere in the row of the destination you want to modify to enable the edit mode.
   8.2. Make changes to the destination as per the information in the table below.

Table 10-18 Modify a USB Destination to Transmit Reports

Field	Action	Description
Destination Name	Modify the name of the USB destination where the reports will be sent, if required	Allowed values: • A to Z • a to z • 0 to 9 • All special characters
ECG Type	Select the supported file type of ECG report sent through USB by your facility.	You can select multiple format types. Default available values: • **Hilltop** • **PDF** Allowed values (Option): • **XML** (This type is available only if XML format output is enabled in **Option Manager**). • **Hilltop** • **PDF**
Rhythm	Select the supported file type of rhythm report sent through USB by your facility.	Default and allowed value: **PDF**

   8.3. Test the connection as per Step 5.
   8.4. Select **Save**.

9. To delete an existing USB destination:

   NOTE

   You can delete only one destination at a time.

   9.1. Select anywhere in the row of the destination you want to delete.

   9.2. Select the **Delete** icon.

   9.3. Select **Save**.

10.6.2.3 System Requirements for DCP Communication

The DCAR Communication Protocol (DCP) is used to support LAN and wireless communication between the MAC 5 Resting ECG Analysis System and the MUSE Cardiology Information System or, the CardioSoft system. The DCP requires the static or dynamic IP address for the MAC 5 system.

The following items are required to configure the wireless connection between a MAC 5 system and a MUSE system or the CardioSoft system.

- An enabled communication option: The **WRLS** option if you use wireless data transfer. The **LAN** option is standard if you use wired data transfer.
- A MUSE system running on V9.0 or later with the DCP communication and MUSEAPI3 service enabled.
- A CardioSoft 7.0 or later system

NOTE

You can secure some communication channels with encryption and authentication. GE Healthcare recommends that you use the encrypted channels, not the unencrypted channels. For example:

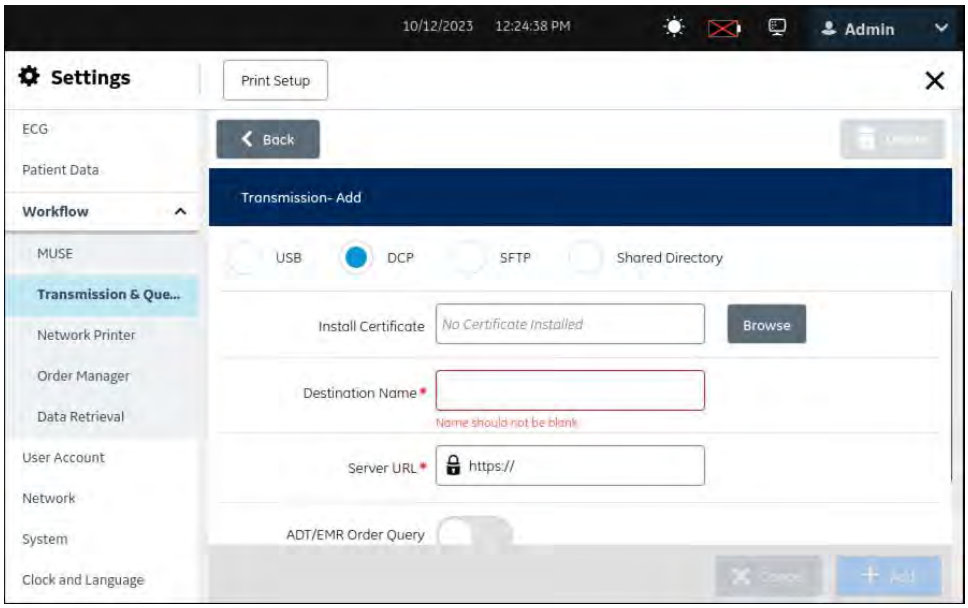
- **Upgrade the MUSE server 9.0 API3 version to the MUSE NX API3 version, to have a secure communication between the MAC 5 system and the MUSE server.**

10.6.2.4 Configure a DCP Server Destination to Transmit Reports

1. Select **Settings** > **Workflow** > **Transmission & Query**.
2. Select the **Add** icon 

to add transmission modes.

3. Select **DCP** to configure a DCP server destination.



You can send a report to the server with the DCAR Communication Protocol (DCP).

The MUSE server and EMR Gateway use DCP.

- If you configure the DCP server destination to the MUSE system, a Hilltop format report is sent to the server.
- If you configure the DCP server destination to the EMR Gateway, a Sapphire XML and PDF report are sent to the server.

4. Configure the fields in the table to add a DCP server destination.

Table 10-19 Configure a DCP Server Destination to Send Reports

Field Name	Action	Description
Install Certificate	Browse and install a valid MUSE CA certificate.	If you configure a https URL, a valid CA certificate is required to authenticate and connect to the MUSE server. Install the CA certificate. See 10.6.2.4.1 Install DCP SSL CA Certificate on page 169. **NOTE** The connection to the MUSE server is allowed, if a valid certificate is installed in the system with qualified authentication. To delete the CA certificate, see 10.6.2.4.2 Delete DCP SSL CA Certificate on page 172. If you configure a http URL, a valid CA certificate is not required to authenticate and connect to the MUSE server. If no certificate installed for the DCP destination, **No certificate Installed** text display. If you install one certificate for the DCP destination, the installed certificate name displays. If more than one certificate installed for the DCP destination, **Multiple certificates installed** text display.
Destination Name	Enter the name of the DCP server destination where the reports will be sent.	A user-defined value up to 20 characters. Allowed values: • A to Z • a to z • 0 to 9 • All special characters

Continues on the next page

Table 10-19 Configure a DCP Server Destination to Send Reports (Table continued)

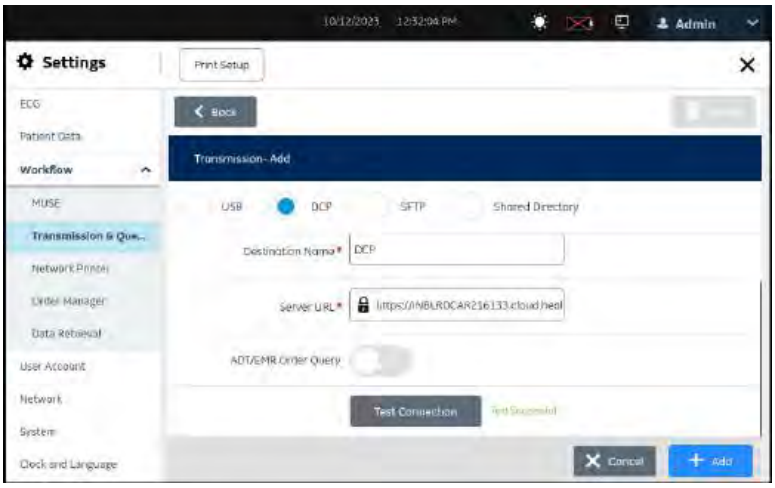
Field Name	Action	Description
Server URL	Enter the URL of the DCP server. **NOTE** • Make sure that you append '/SendTest' to the URL. For example, http://<IP_Address> or <Hostname>:<Port>/SendTest. • Confirm that the URL for the server is correct. • Confirm that the DCP server is running. • Make sure that you enable ADT for DCP communication, configure the same IP address for the DCP destination and the MUSE Orders Server for remote query.	**NOTE** You can secure some communication channels with encryption and authentication. GE Healthcare recommends that you use the encrypted channels, not the unencrypted channels. For example: • HTTPS for remote application (instead of HTTP). • Upgrade the MUSE server 9.0 API3 version to the MUSE NX API3 version, to have a secure communication between the MAC 5 system and the MUSE server. A user defined value. Default value: https. You can append the URL with server details. You can configure the URL with **http** or **https**. The URL must correspond to the MUSE system. Allowed values: A valid http or https URL with defined FQDN or IP address and a port number. Use a Fully Qualified Domain Name (FQDN) or IP address. Add the port number after the URL with a colon (:) specifier. **NOTE** Define the port number if it is not defined in the URL. • HTTP - 9240 • HTTPS - 9241 Determine which MUSE version you will connect to and configure the URL: • MUSE system V9: HTTP • MUSE NX system: HTTPS

Continues on the next page

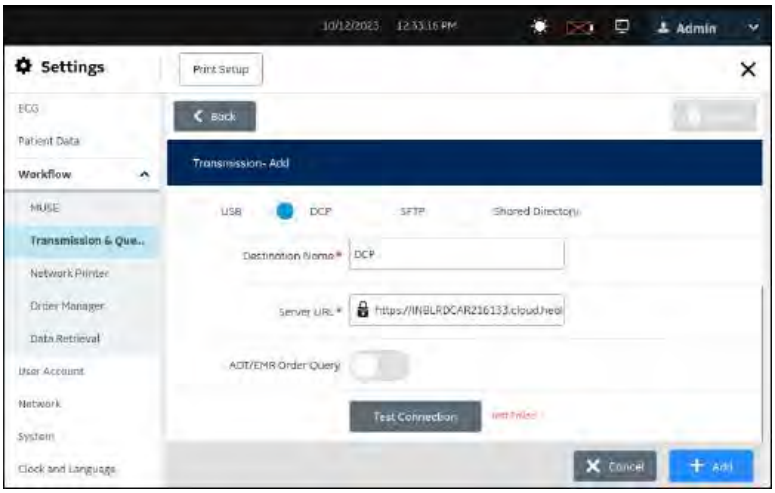
Table 10-19 Configure a DCP Server Destination to Send Reports (Table continued)

Field Name	Action	Description
ADT/EMR Order Query	Enable or disable this setting.	If this setting is enabled, the destination is configured to perform ADT query to MUSE/EMR Gateway system or perform order query via DCP to EMR Gateway system. Default value: Disabled

5. Select **Test Connection**.
   - If the test displays `Test Successful`, you have a successful connection to that destination. Select **Add** to save the destination.



   - If the test displays `Test Failed`, you do not have a connection to that destination. Troubleshoot the connection failure depending on the error, re-test and add the connection.



6. Select **Save**.
7. Repeat Step 2 to Step 6 to add more DCP server destinations.
8. To edit an existing DCP server destination:
   8.1. Select anywhere in the row of the destination you want to modify to enable the edit mode.

8.2. Make changes to the destination as per the information in the table below.

Table 10-20 Modify a DCP Server Destination to Send Reports

Field Name	Action	Description
Install Certificate	Browse and install a valid MUSE CA certificate.	If you configure a https URL, a valid CA certificate is required to authenticate and connect to the MUSE server. Install the CA certificate. See Install MUSE certificate. **NOTE** The connection to the MUSE server is allowed, if a valid certificate is installed in the system with qualified authentication. To delete the CA certificate, see Delete CA certificate. If you configure a http URL, a valid CA certificate is not required to authenticate and connect to the MUSE server. If no certificate installed for the DCP destination, **No certificate Installed** text display. If you install one certificate for the DCP destination, the installed certificate name displays. If more than one certificate installed for the DCP destination, **Multiple certificates installed** text display.
Destination Name	Modify the name of the DCP server destination where the reports will be sent, if required.	A user-defined value up to 20 characters. Allowed values: • A to Z • a to z • 0 to 9 • All special characters

Continues on the next page

Table 10-20 Modify a DCP Server Destination to Send Reports (Table continued)

Field Name	Action	Description
Server URL	Modify the URL of the DCP server, if required. **NOTE** • Make sure that you append '/SendTest' to the URL. For example, http://<IP_Address> or <Hostname>:<Port>/SendTest. • Confirm that the URL for the server is correct. • Confirm that the DCP server is running. • Make sure that you configure the IP address of the DCP destination with ADT enabled and the destination in the MUSE Order Server settings is same for a remote query.	**NOTE** You can secure some communication channels with encryption and authentication. GE Healthcare recommends that you use the encrypted channels, not the unencrypted channels. For example: • HTTPS for remote application (instead of HTTP). • Upgrade the MUSE server 9.0 API3 version to the MUSE NX API3 version, to have a secure communication between the MAC 5 system and the MUSE server. A user defined value. Default value: https. You can append the URL with server details. You can configure the URL with **http** or **https**. The URL must correspond to the MUSE system. Allowed values: A valid http or https URL with defined FQDN or IP address and a port number. Use a Fully Qualified Domain Name (FQDN) or IP address. Add the port number after the URL with a colon (:) specifier. **NOTE** Define the port number if it is not defined in the URL. • HTTP - 9240 • HTTPS - 9241 Determine which MUSE version you will connect to and configure the URL: • MUSE system V9: HTTP • MUSE NX system: HTTPS

Continues on the next page

Table 10-20 Modify a DCP Server Destination to Send Reports (Table continued)

Field Name	Action	Description
ADT/EMR Order Query	Enable or disable this setting.	If this setting is enabled, the destination is configured to perform ADT query to MUSE/EMR Gateway system or perform order query via DCP to EMR Gateway system. Default value: Disabled

8.3. Select **Test Connection**.

- If the test displays `Test Successful`, you have a successful connection to that destination. Select **Update** to save the destination.
- If the test displays `Test Failed`, you do not have a connection to that destination. Troubleshoot the connection failure depending on the error, re-test and add the connection.

8.4. Select **Save**.

9. To delete an existing DCP server destination:

NOTE

You can delete only one destination at a time.

9.1. Select anywhere in the row of the destination you want to delete.

9.2. Select the **Delete** icon .

9.3. Select **Save**.

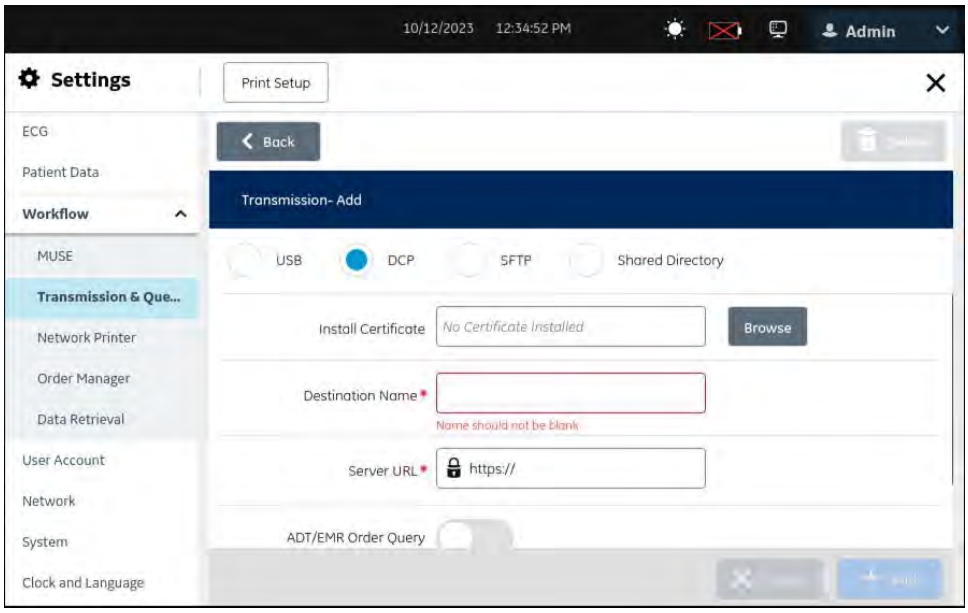
10.6.2.4.1 Install DCP SSL CA Certificate

Before you start this procedure, make sure that:

- You obtain the required certificate in the PEM format from your IT department and copy it to the root folder of a USB flash drive for installation.
- The **Enable External USB Storage** is enabled in **Settings** > **System** > **Storage**. If you do not enable this setting, access to USB flash drives is blocked.
- You enable at least one USB port in **Settings** > **Hardware** > **USB Port**. If you do not enable this setting, the device will not recognize the USB flash drives.

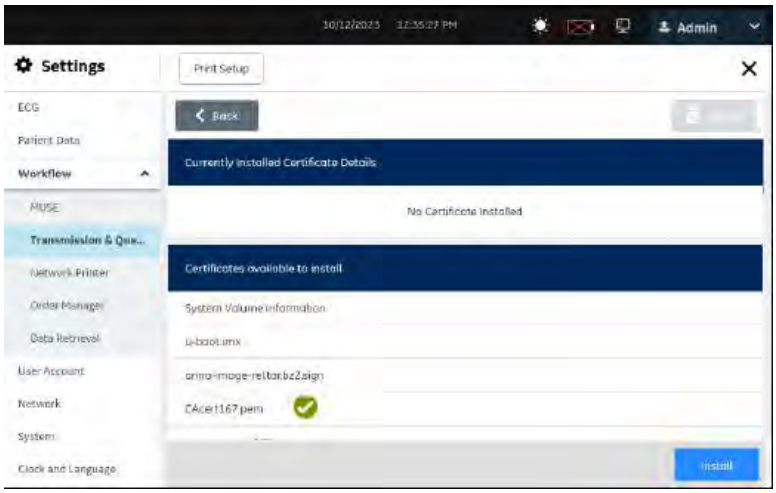
1. Connect the USB flash drive containing the CA certificate to the device.
2. Select **Settings** > **Workflow** > **Transmission & Query**.
3. Select the **Add** icon Add to add transmission modes.

4. Select **DCP** to view the DCP server destination settings.



5. Perform the steps below to install a CA certificate:

5.1. Select **Browse** from the **Install Certificate** field and select the CA certificate from the USB flash drive.



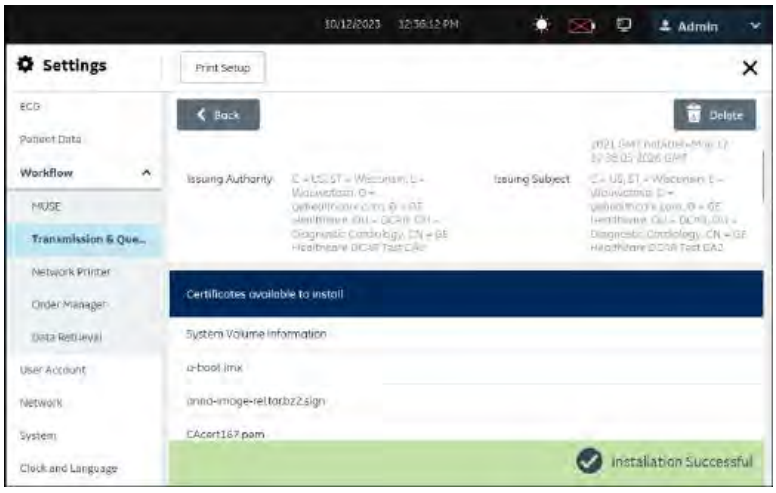
NOTE

If no certificate installed for the DCP destination, **No certificate Installed** text displays.

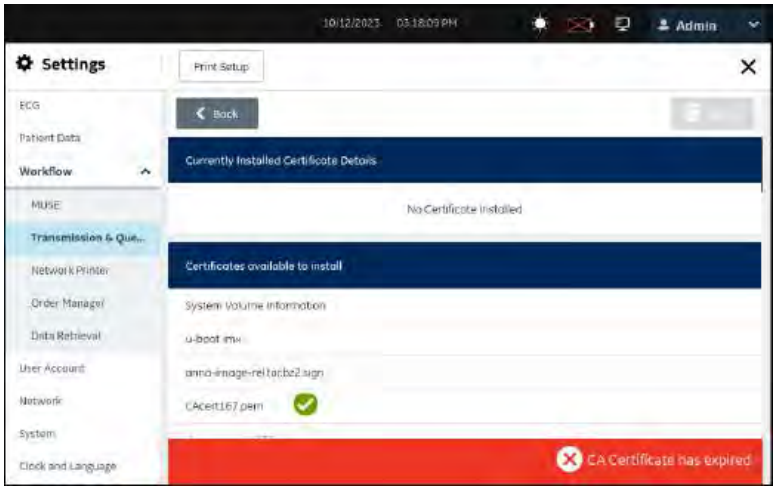
5.2. Select **Install**.

A green checkmark displays adjacent to the selected certificate. If the installation is successful, the CA certificate is saved and displays the certificate details:

- Certificate name
- Certificate validity
- Issuing Authority
- Issuing Subject

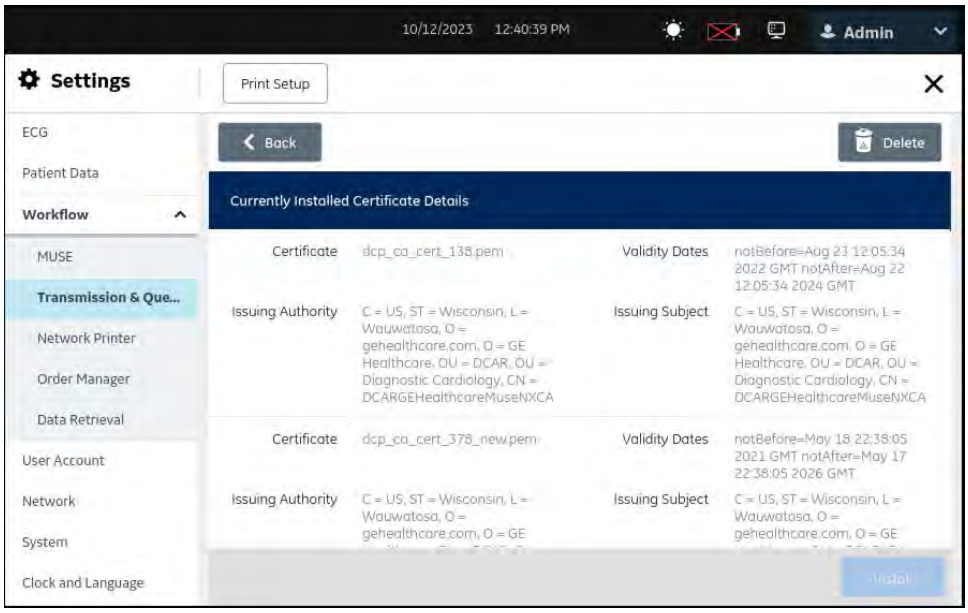


If the installation fails because the certificate is an unrecognized format or an expired certificate, an error message displays. See 13.8 DCP Server Connection Errors on page 280 for more information on CA certificate errors of the DCP server destination.



6. Select **Back** to view the DCP server destination setting screen.

7. Select **Browse** and install more than one certificate from the USB flash drive.



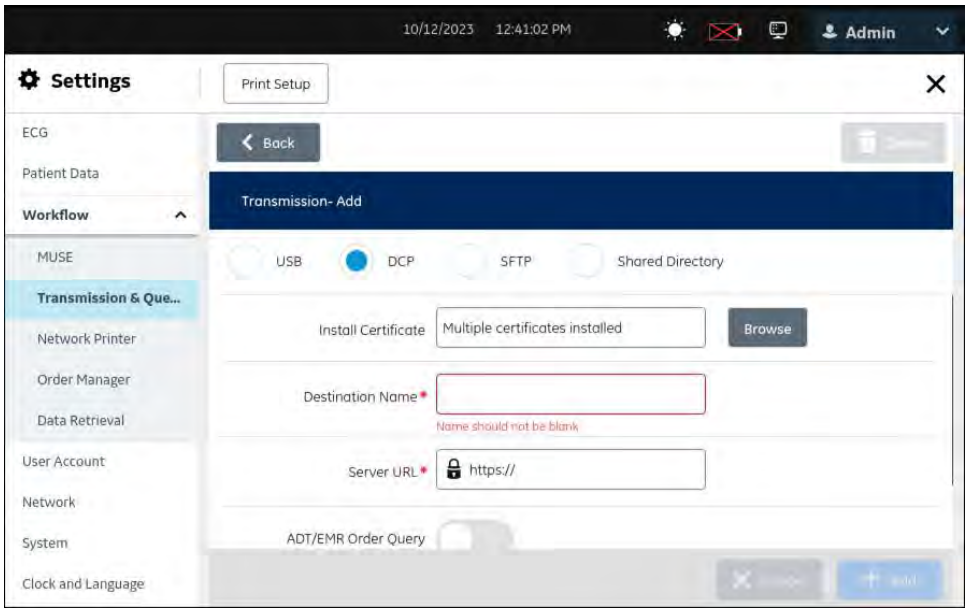
NOTE

You can select only one certificate at a time for installation.

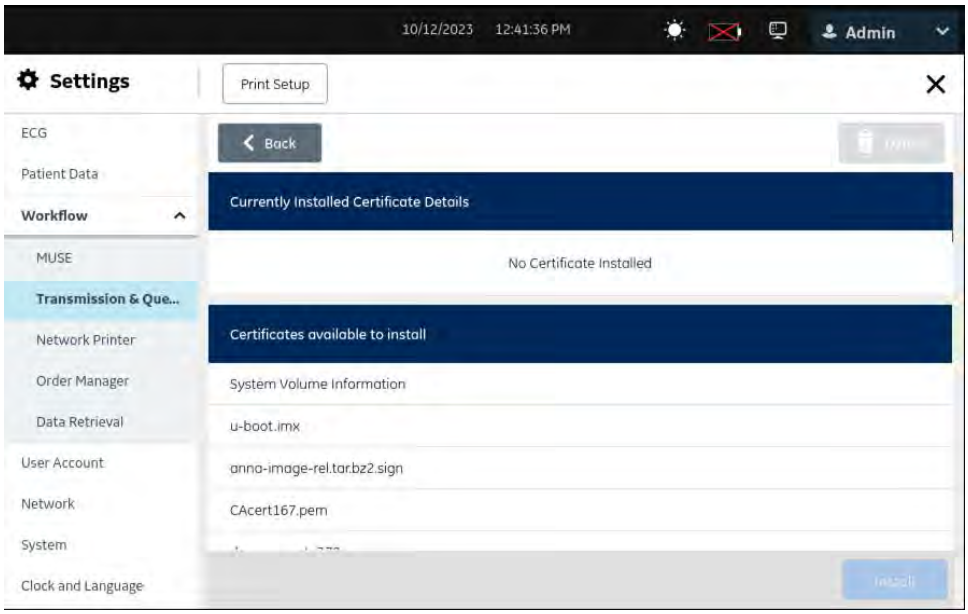
10.6.2.4.2 Delete DCP SSL CA Certificate

Before you start this procedure, make sure that your user role is assigned with user management privilege.

1. Select **Settings** > **Workflow** > **Transmission & Query**.
2. Select the **Add** icon Add to add transmission modes.
3. Select **DCP** to view the DCP server destination settings.



4. Select **Browse** to view all the installed certificates.
5. Select Delete to delete all the installed DCP CA certificates.



All the installed certificates of the DCP destination are deleted and **No Certificate installed** displays.

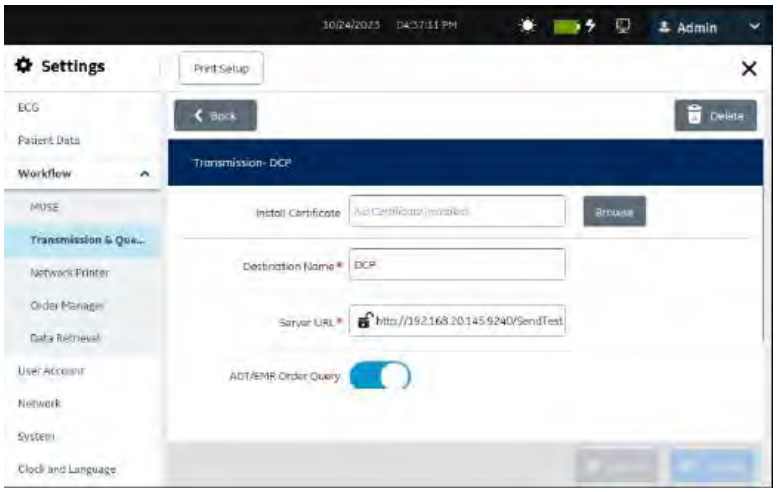
6. Select **Back** to view the DCP server destination setting screen.

10.6.2.5 Configure a DCP Server Destination to Query Orders

You can query the orders with DCAR Communication Protocol (DCP). The EMR Gateway system uses the DCP for order query.

If you have the **View Orders** privilege, use the patient ID or visit number to query orders from the EMR Gateway system. Make sure that you disable the **Order Management** in **Settings** > **Workflow** > **Order Manager**.

1. Select **Settings** > **Workflow** > **Transmission & Query**.
2. Select the **Add** icon Add to add transmission modes.
3. Select **DCP** to configure a EMR Gateway system server destination.
4. Enable **ADT/EMR Order Query** button.



5. Configure the fields in the table to add a EMR Gateway system server as DCP destination to query orders.

Table 10-21 Configure EMR Gateway System Server as a DCP Destination to Query Orders

Field Name	Action	Description
Install Certificate	No action.	The EMR Gateway system is configured only through an http URL which is not a secured connection. A valid CA certificate installation is not required to connect to the EMR Gateway.
Destination Name	Enter the name of the DCP server destination where the orders will be queried. **NOTE** You can use this destination to send the reports to the EMR Gateway system.	A user-defined value up to 20 characters. Allowed values: • A to Z • a to z • 0 to 9 • All special characters
Server URL	Enter the URL of the DCP server. **NOTE** • Make sure that you append '/SendTest' to the URL. For example, http://<IP_Address> or <Hostname>:<Port>/SendTest. • Confirm that the URL for the server is correct. • Confirm that the DCP server is running. • Configure the same IP address or hostname which is the same as the EMR Gateway system server for remote order queries.	GE Healthcare recommends that you use the encrypted channels, not the unencrypted channels. The EMR Gateway system supports only the unencrypted channel, use the http URL. The URL must be same to the EMR Gateway system server. Allowed values: A valid http URL with defined FQDN or IP address and a port number. Use a Fully Qualified Domain Name (FQDN) or IP address. Add the port number after the URL with a colon (:) specifier. **NOTE** Define the port number HTTP - 9240 if it is not defined in the URL. Use EMR Gateway system V2 or higher to connect and configure the URL with HTTP.
ADT/EMR Order Query	Enable this setting.	If you enable this setting, the DCP destination is configured to perform ADT/order query from EMR Gateway system via DCP. Default value: Disabled

6. Select **Test Connection**.
   - If the test displays `Test Successful`, you have a successful connection to that destination. Select **Add** to save the destination.
   - If the test displays `Test Failed`, you do not have a connection to that destination. Troubleshoot the connection failure depending on the error, re-test and add the connection.

7. Select **Save**.
8. To edit an existing EMR Gateway system server as a DCP destination:
   8.1. Select anywhere in the row of the destination you want to modify to enable the edit mode.
   8.2. Make changes to the destination as per the information in the table below.

Table 10-22 Modify a EMR Gateway System Server as a DCP Destination to Query Orders

Field Name	Action	Description
Install Certificate	No action.	The EMR Gateway system is configured only through an http URL which is not a secured connection. A valid CA certificate installation is not required to connect to the EMR Gateway system.
Destination Name	Enter the name of the DCP server destination where the orders will be queried. **NOTE** You can use this destination to send the reports to the EMR Gateway system.	A user-defined value up to 20 characters. Allowed values: • A to Z • a to z • 0 to 9 • All special characters
Server URL	Modify the URL of the DCP server, if required. **NOTE** • Make sure that you append '/SendTest' to the URL. For example, http://<IP_Address> or <Hostname>:<Port>/SendTest. • Confirm that the URL for the server is correct. • Confirm that the DCP server is running. • Configure the same IP address or hostname which is the same as the EMR Gateway system server for remote order queries.	GE Healthcare recommends that you use the encrypted channels, not the unencrypted channels. The EMR Gateway system supports only the unencrypted channel, use the http URL. The URL must be same to the EMR Gateway system server. Allowed values: A valid http URL with defined FQDN or IP address and a port number. Use a Fully Qualified Domain Name (FQDN) or IP address. Add the port number after the URL with a colon (:) specifier. **NOTE** Define the port number HTTP - 9240 if it is not defined in the URL. Use EMR Gateway system V2 or higher to connect and configure the URL with HTTP.
ADT/EMR Order Query	Enable or disable this setting.	If you enable this setting, the DCP destination is configured to perform ADT/order query from EMR Gateway system via DCP. Default value: Disabled

   8.3. Select **Test Connection**.

- If the test displays `Test Successful`, you have a successful connection to that destination. Select **Update** to save the destination.
- If the test displays `Test Failed`, you do not have a connection to that destination. Troubleshoot the connection failure depending on the error, re-test and add the connection.

8.4. Select **Save**.

9. To delete an existing DCP server destination:

NOTE

You can delete only one destination at a time.

9.1. Select anywhere in the row of the destination you want to delete.

9.2. Select the **Delete** icon .

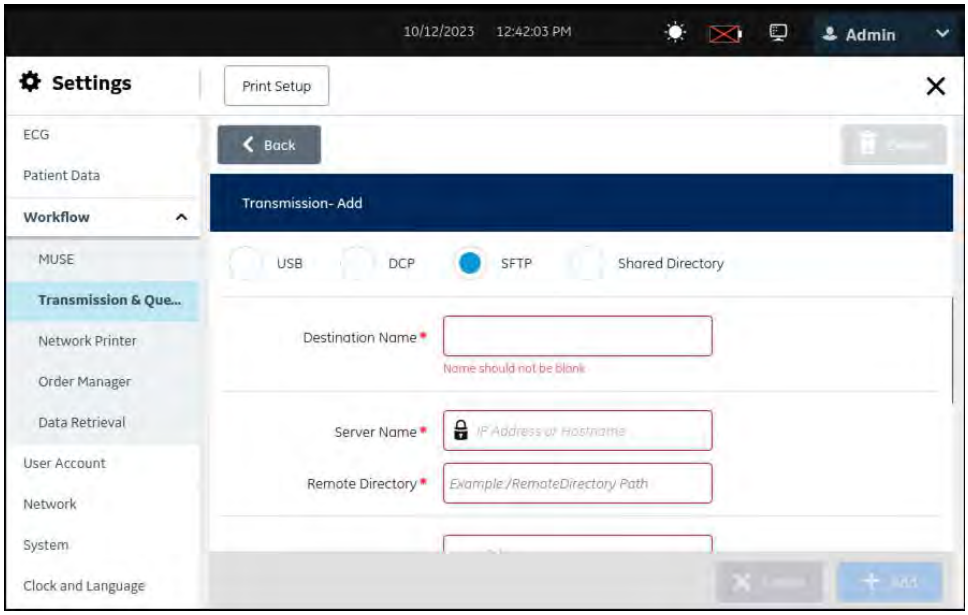
9.3. Select **Save**.

10.6.2.6 Configure an SFTP Destination to Transmit Reports

NOTE

The files saved on SFTP is not encrypted.

1. Select **Settings** > **Workflow** > **Transmission & Query**.
2. Select the **Add** icon to add transmission modes.
3. Select **SFTP** to configure an SFTP destination.



4. Configure the destination as per the information in the table.

Table 10-23 Configure an SFTP Destination to Transmit Reports

Field	Action	Description
Destination Name	Enter the name of the SFTP destination where the reports will be sent.	A user-defined value up to 20 characters. Allowed values: • A to Z • a to z • 0 to 9 • All special characters
Server Name	Enter the IP Address or Hostname of the SFTP server where the reports will be sent.	Allowed values: • A to Z • a to z • 0 to 9 • All special characters
Remote Directory	Enter the path of the remote directory in the SFTP server where the reports will be sent.	Allowed values: • A to Z • a to z • 0 to 9 • All special characters
User Name	Enter the user name allowed to access the SFTP server.	Allowed values: • A to Z • a to z • 0 to 9 • All special characters
Password	Enter the password of the user name allowed to access the SFTP server.	Allowed values: • A to Z • a to z • 0 to 9 • All special characters
ECG Type	Select the supported file type of ECG report sent to the SFTP destination by your facility.	You can select multiple format types. Default available values: • **Hilltop** • **PDF** Allowed values (Option): • **XML** (This type is available only if XML format output is enabled in **Option Manager**). • **Hilltop** • **PDF**
Rhythm Type	Select the supported file type of rhythm report sent to the SFTP destination by your facility.	Default and allowed value: **PDF**

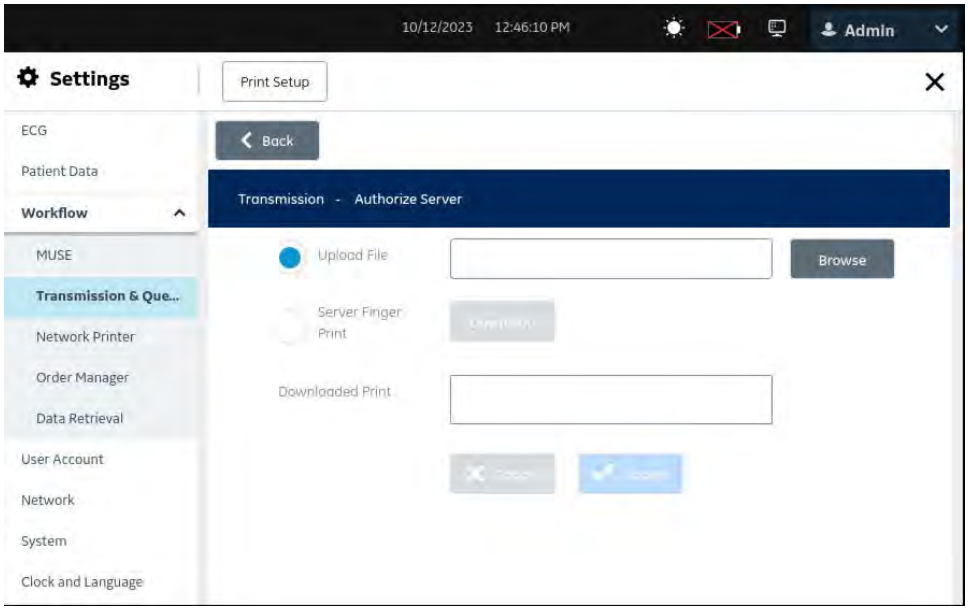
Continues on the next page

Table 10-23 Configure an SFTP Destination to Transmit Reports (Table continued)

Field	Action	Description
Authorize Server	Select **Authorize** to acknowledge, upload the key file, and download the SFTP server advertised finger print key.	The **Authorize** setting is enabled only after entering the values for **Destination Name**, **Server Name**, **Remote Directory**, **User Name**, **Password**, and **ECG Type** mandatory fields. Default value: Disabled The authorize server is configured through one of the settings below: • **Upload File** • **Server Finger Print**
Upload File	Select **Browse** to upload the public key file that is used to sign the server host certificate from USB. The SFTP server should be configured to use OpenSSH host certificate.	You can select the public key file that is used to sign the server host certificate from the USB to authorize the SFTP server. **NOTE** The SHA-1 signed certificates are not supported by the device for SFTP server authorization. The connection to the SFTP server fails if you use the SHA-1 signed certificates for authorization.
Server Finger Print	Select **Download** to download the available finger print from the server.	You can download the finger print from the server to authorize the server.
Test Connection	Select **Test Connection** to test the SFTP server configuration.	You can test the SFTP server configuration.

5. Select **Authorize** to test the configured connection.

   The **Transmission - Authorize Server** screen opens.



6. To authorize a server, perform Step 7 or Step 8.
7. To authorize the server through a public key file that is used to sign the host certificate:

7.1. Select **Upload File** to upload the public key file that is used to sign the host certificate.

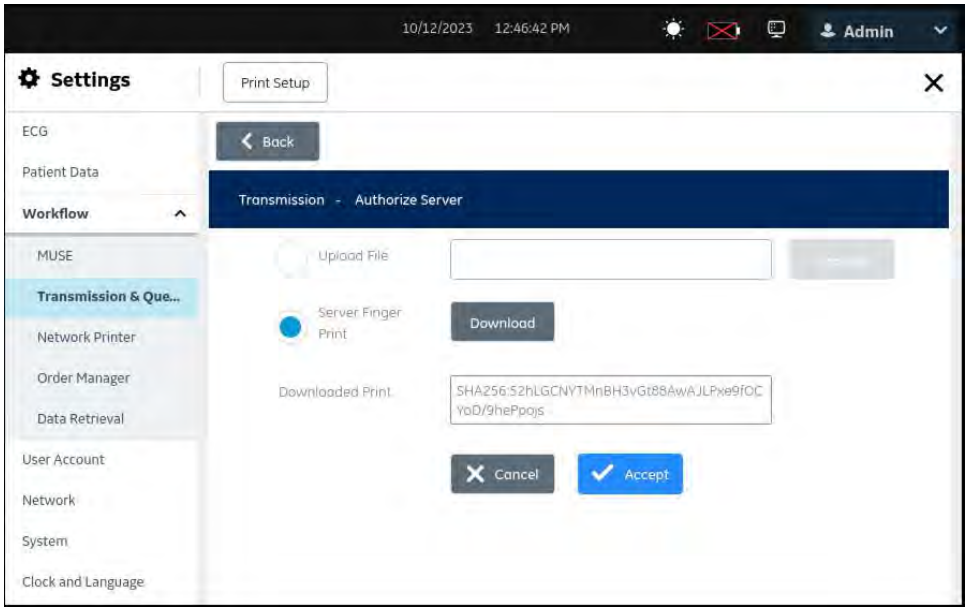
7.2. Make sure that the USB port is enabled and the USB flash drive with a public key file that is used to sign the host certificate is inserted into the device.

7.3. Select **Browse** to choose the public key file that is used to sign the host certificate from the USB.

8. To authorize a server through a finger print:

8.1. Select **Server Finger Print** to download and use the available finger print from the server.

The **Transmission - Authorize Server** for **Finger Print** screen opens.



8.2. Select **Download** to download the finger print.

NOTE

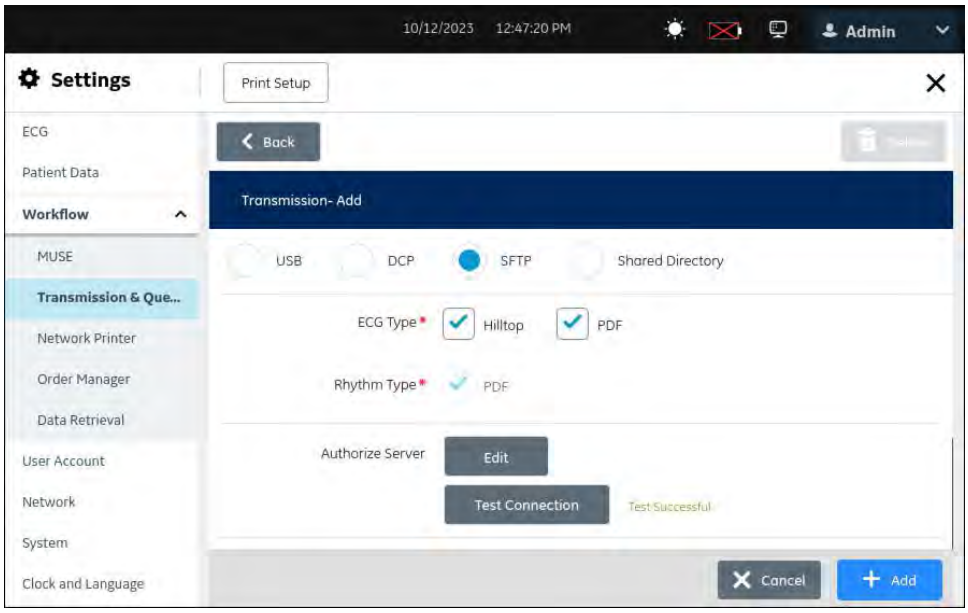
Make sure that you connect to the correct SFTP server by comparing the displayed finger print against the expected server finger print.

- If the download is successful, the finger print displays in the **Downloaded Print** field.
- If the download is failed, you cannot authorize the server. Troubleshoot the SFTP server configuration.

8.3. Select **Accept** to accept and close the authorize server settings screen.

9. Select **Back** to view the SFTP server configuration.

The SFTP server **Transmission-Add** screen opens.



10. Select **Test Connection** to test the SFTP server configuration.
    - If the test connection is successful, the SFTP server is configured and you can transmit the reports.
    - If the test connection is failed, the SFTP server is not configured and you cannot transmit the reports.
11. Select **Save**.
12. Repeat Step 2 to Step 11 to add more SFTP destinations.
    - To edit an SFTP destination, perform Step 13.
    - To delete an SFTP destination, perform Step 14.
13. To edit an existing SFTP destination:
    13.1. Select anywhere in the row of the destination you want to modify to enable the edit mode.
    13.2. Make changes to the destination as per the information in the table.

Table 10-24 Modify an SFTP Destination to Send Reports

Field	Action	Description
Destination Name	Enter the name of the SFTP destination where the reports will be sent.	A user-defined value up to 20 characters. Allowed values: • A to Z • a to z • 0 to 9 • All special characters
Server Name	Enter the IP Address or Hostname of the SFTP server where the reports will be sent.	Allowed values: • A to Z • a to z • 0 to 9 • All special characters

Continues on the next page

Table 10-24 Modify an SFTP Destination to Send Reports (Table continued)

Field	Action	Description
Remote Directory	Enter the path of the remote directory in the SFTP server where the reports will be sent.	Allowed values: • A to Z • a to z • 0 to 9 • All special characters
User Name	Enter the domain and user ID of the SFTP server where the reports will be sent.	Allowed values: • A to Z • a to z • 0 to 9 • All special characters
Password	Enter the password of the SFTP server where the reports will be sent.	Allowed values: • A to Z • a to z • 0 to 9 • All special characters
ECG Type	Select the supported file type of ECG report sent to the SFTP destination by your facility.	You can select multiple format types. Default available values: • **Hilltop** • **PDF** Allowed values (Option): • **XML** (This type is available only if XML format output is enabled in **Option Manager**). • **Hilltop** • **PDF**
Rhythm Type	Select the supported file type of rhythm report sent to the SFTP destination by your facility.	Default and allowed value: **PDF**
Authorize Server	Select **Authorize** to acknowledge and download the SFTP server advertised finger print key.	The **Authorize** setting is enabled only after entering the values for **Destination Name**, **Server Name**, **Remote Directory**, **User Name**, **Password**, and **ECG Type** mandatory fields. Default value: Disabled The authorize server is configured through one of the settings below: • **Upload File** • **Server Finger Print**

Continues on the next page

Table 10-24 Modify an SFTP Destination to Send Reports (Table continued)

Field	Action	Description
Upload File	Select **Browse** to upload the public key file that is used to sign the server host certificate from USB. The SFTP server should be configured to use OpenSSH host certificate.	You can select the public key file that is used to sign the server host certificate from the USB to authorize the SFTP server.
Server Finger Print	Select **Download** to download the available finger print from the server.	You can download the finger print from the server to authorize the server.
Test Connection	Select **Test Connection** to test the SFTP server configuration.	You can test the SFTP server configuration.

13.3. Edit the authorize server as per steps from Step 5 to Step 8.

13.4. Select **Save**.

14. To delete an existing SFTP destination:

NOTE

You can delete only one destination at a time.

14.1. Select anywhere in the row of the destination you want to delete.

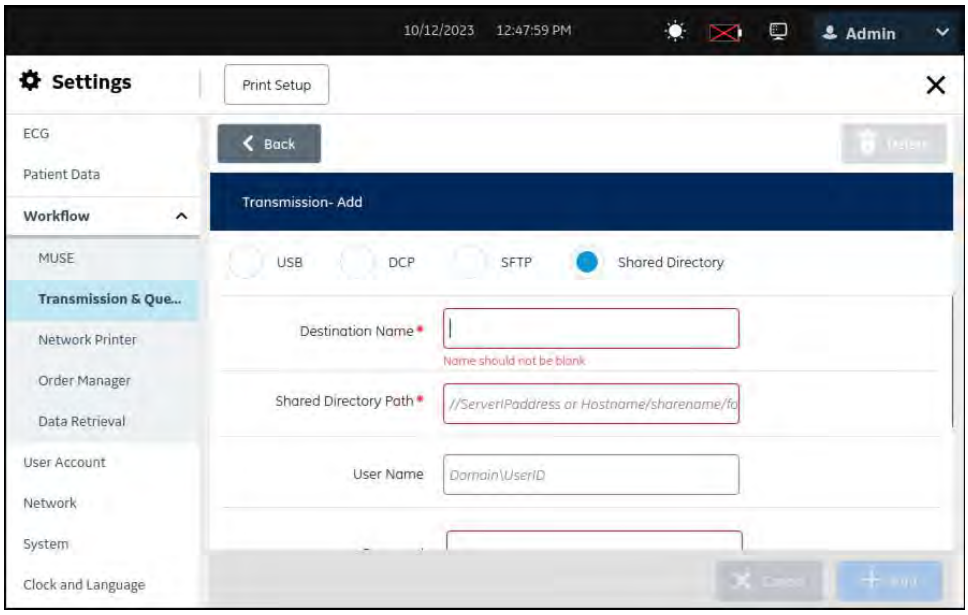
14.2. Select the **Delete** icon .

14.3. Select **Save**.

10.6.2.7 Configure a Shared Directory to Transmit Reports

The shared directory supports only SMB version 3.0.

1. Select **Settings** > **Workflow** > **Transmission & Query**.
2. Select the **Add** icon Add to add transmission modes.
3. Select **Shared Directory**.



4. Configure a shared directory as per the information in the table.

Table 10-25 Configure a Shared Directory Destination to Transmit Reports

Field	Action	Description
Destination Name	Enter the name of the shared directory where the reports will be sent.	A user-defined value up to 20 characters. Allowed values: • A to Z • a to z • 0 to 9 • All special characters
Shared Directory Path	Enter the server IP address or hostname path of the shared directory. For example, `//ServerIPaddress or Hostname/sharename`.	Allowed values: • A to Z • a to z • 0 to 9 • All special characters
User Name	Enter the user name allowed to access the shared directory.	Allowed values: • A to Z • a to z • 0 to 9 • All special characters
Password	Enter the password of the user name allowed to access the shared directory.	Allowed values: • A to Z • a to z • 0 to 9 • All special characters (a single space)

Continues on the next page

Table 10-25 Configure a Shared Directory Destination to Transmit Reports (Table continued)

Field	Action	Description
ECG Type	Select the supported file type of ECG report sent to the shared directory by your facility.	You can select multiple format types. Default available values: • **Hilltop** • **PDF** Allowed values (Option): • **XML** (This type is available only if XML format output is enabled in **Option Manager**). • **Hilltop** • **PDF**
Rhythm Type	Select the supported file type of rhythm report sent to the shared directory by your facility.	Default and allowed value: **PDF**

5. Select **Test Connection** to test the configured connection.
   - If the test displays `Test Successful`, you have a successful connection to that destination.
   - If the test displays `Test Failed`, you do not have a connection to that destination. Troubleshoot the connection failure.
6. Select **Save**.
7. Repeat Step 2 to Step 5 to add more shared directory destinations.
   - To edit a shared directory destination, perform Step 8.
   - To delete a shared directory destination, perform Step 9.
8. To edit an existing shared directory destination:
   8.1. Select anywhere in the row of the destination you want to modify to enable the edit mode.
   8.2. Make changes to the destination as per the information in the table.

Table 10-26 Modify a Shared Directory Destination to Transmit Reports

Field	Action	Description
Destination Name	Enter the name of the shared directory where the reports will be sent.	A user-defined value up to 20 characters. Allowed values: • A to Z • a to z • 0 to 9 • All special characters
Shared Directory Path	Enter the path of the shared directory. For example, `//ServerIPaddress or Hostname/sharename`.	Allowed values: • A to Z • a to z • 0 to 9 • All special characters

Continues on the next page

Table 10-26 Modify a Shared Directory Destination to Transmit Reports (Table continued)

Field	Action	Description
User Name	Enter the user name allowed to access the shared directory.	Allowed values: • A to Z • a to z • 0 to 9 • All special characters
Password	Enter the password of the user name allowed to access the shared directory.	Allowed values: • A to Z • a to z • 0 to 9 • All special characters (a single space)
ECG Type	Select the supported file type of ECG report sent to the shared directory by your facility.	You can select multiple format types. Default available values: • **Hilltop** • **PDF** Allowed values (Option): • **XML** (This type is available only if XML format output is enabled in **Option Manager**). • **Hilltop** • **PDF**
Rhythm Type	Select the supported file type of rhythm report sent to the shared directory by your facility.	Default and allowed value: **PDF**

8.3. Test the connection as per Step 5.

8.4. Select **Save**.

9. To delete an existing shared directory destination:

NOTE

You can delete only one destination at a time.

9.1. Select anywhere in the row of the destination you want to delete.

9.2. Select the **Delete** icon .

9.3. Select **Save**.

10.6.2.8 Configure Transmission Modes

Make sure that at least one of the transmission mode is configured in the device.

1. Select **Settings** > **Workflow** > **Transmission & Query**.

2. Configure the transmission modes as per the information in the table below:

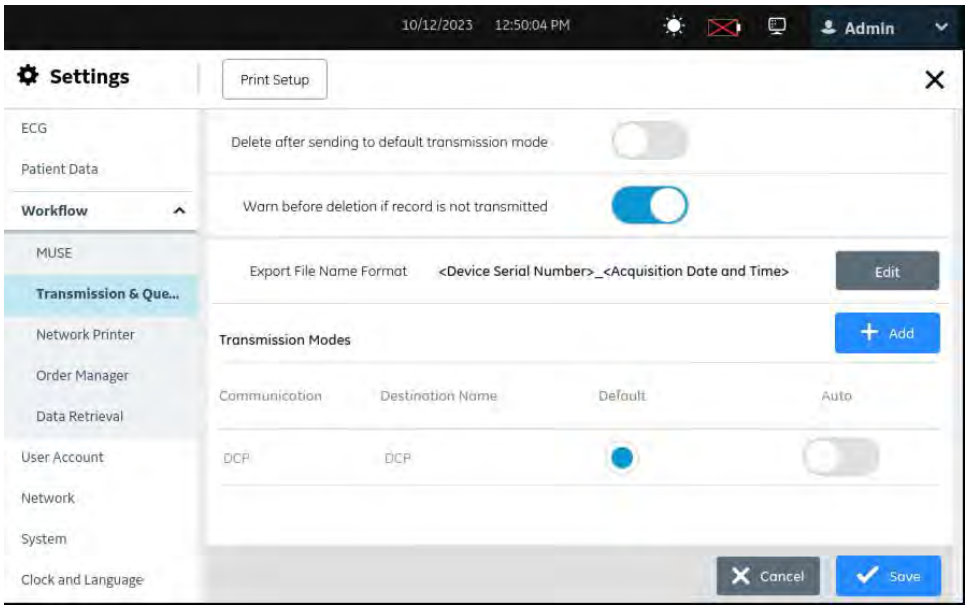


Table 10-27 Configure Transmission Modes

Field	Action	Description
Default	Enable or disable this setting.	If this setting is enabled, all generated patient reports are sent to this destination by default. A destination can be both the default and automatic destination. Default value: Disabled
Auto	Enable or disable this setting.	If this setting is enabled, all generated patient reports are automatically sent to this destination. A destination can be both the default and automatic destination. Default value: Disabled **NOTE** When **Auto** is enabled for transmission and user does not have **Transmit Report** privilege, the report will not be transmitted.

NOTE

You can configure only one transmission mode at a time.

3. Select **Save**.

10.6.3 Configure Network Printer

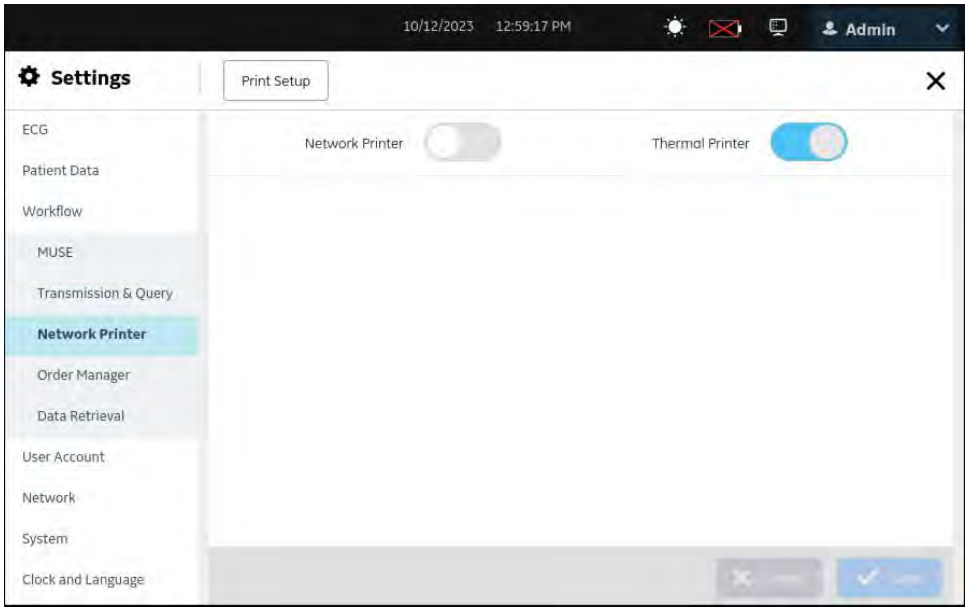
To configure a network printer, make sure the **NETP - Network Printer** option is purchased and enabled in the **Option Manager**.

1. Select **Settings** > **Workflow** > **Network Printer**.

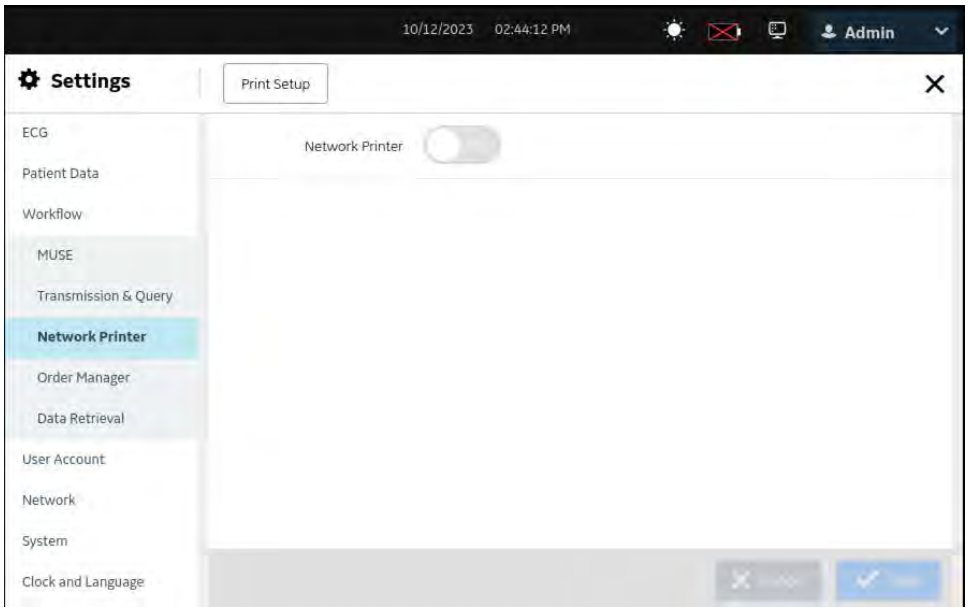
   The network printer setting screen displays.

User Interface on A4 and A5 devices

Continues on the next page



User Interface on Lite device



For MAC 5 devices with printer, the default printer is thermal printer.

For MAC 5 Lite device, the network printer is disabled by default.

2. Enable network printer, and configure the network printer per the information in the table below:

NOTE

Make sure that the device is connected to a LAN or WLAN network, which is the same with the printer you are configuring. For more information, refer to 10.8 Configure Network on page 223.

Table 10-28 Configure Network Printer

Field	Action	Description
Network Printer	Enable or disable the network printer.	If this setting is enabled, the report can be printed via configuerd network printer.
Thermal Printer	Enable or disable the thermal printer.	If this setting is enabled, the report can be printed via thermal printer.
URL	Enter a valid ipp or ipps URL of the network printer.	A user-defined value. MAC 5 device only supports two protocols as below: • Internet printing protocol (***ipp://***) For example, `ipp://xxxyyyzzz/ipp/print` • Secured internet printing protocol (***ipps://***) For example, `ipps://xxxyyyzzz/ipp/print` Allowed values: • A to Z • a to z • 0 to 9 • All special characters
Paper Size	Select a value from the dropdown list to configure the paper size for printing.	Default value: **Letter** Allowed values: • **A4** • **Letter**
User Name	Enter the user name allowed to access the network printer.	Allowed values: • A to Z • a to z • 0 to 9 • All special characters
Password	Enter the password of the user name allowed to access the network printer.	Allowed values: • A to Z • a to z • 0 to 9 • All special characters
Test Print	Select to test the network printer configuration.	You can test the network printer configuration.

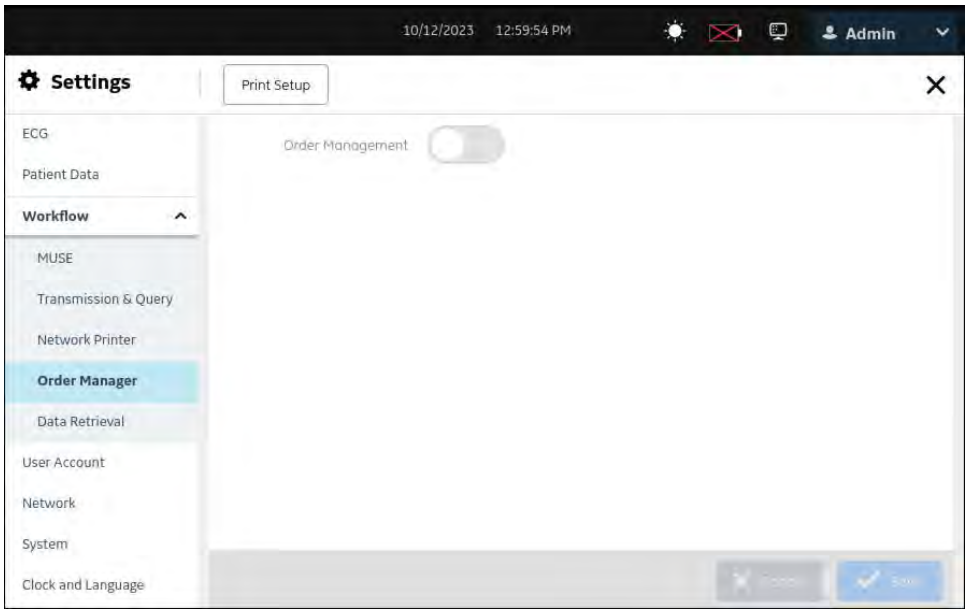
10.6.4 Configure Order Management

Before you start this procedure, make sure that:

- The **ORDM - Order Manager** option is enabled on the device. Contact a GE Healthcare Service Support representative to enable this option.
- Your user role is assigned the privileges to access the *Settings* screen and edit critical value settings. See 10.7.4 Configure User Roles on page 207.

1. Select **Settings** > **Workflow** > **Order Manager**.

   The **Order Manager** screen displays.



2. Configure order management as per the information in the table.

Table 10-29 Configure Order Management

Field	Action	Description
Order Management	Enable or disable this setting.	Order management is available on the device when you enable this setting. The **Orders** and **Columns** tabs display to configure order management. The **Orders** list displays on the Acquisition screen. Order management is not available on the device if you disable this setting. The tabs do not display on the screen to configure order management. The **Patients** list displays on the Acquisition screen instead of the **Orders** list. Default value: Disabled

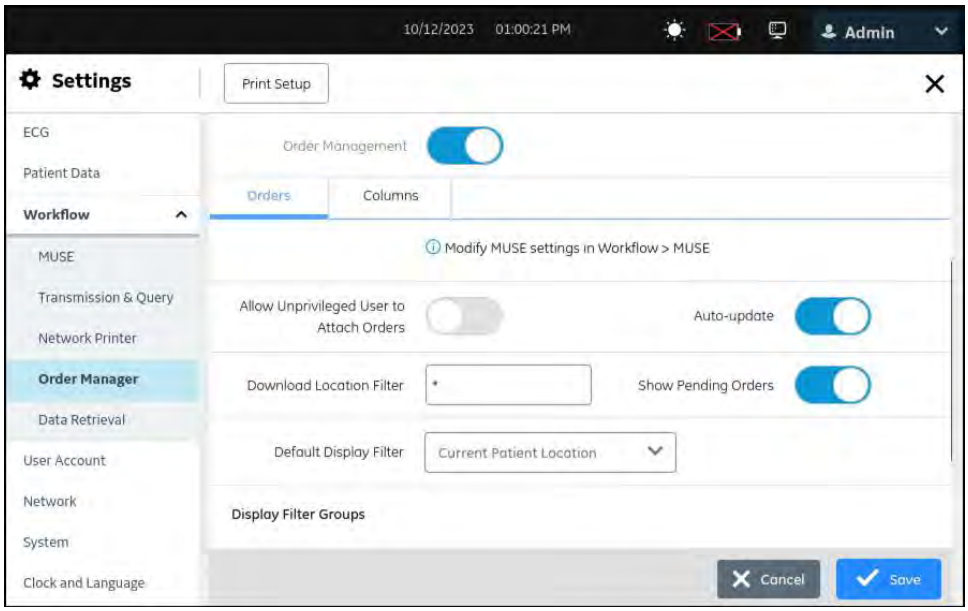
10.6.4.1 Configure Display Filter Groups

Make sure that order management is enabled and the MUSE server is configured. See 10.6.4 Configure Order Management on page 188.

A display filter group displays the configured group of locations at your facility. You can filter the orders in the *Orders* view based on the selected location. You can configure a maximum of 10 display filter groups.

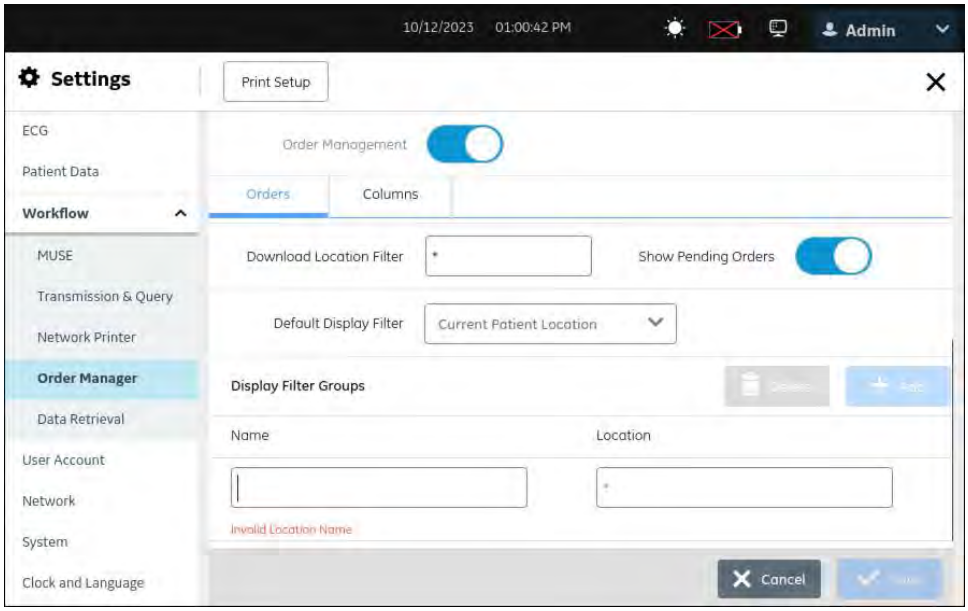
1. Select **Settings** > **Workflow** > **Order Manager**.
2. Select **Orders**.

   The **Order Manager** screen displays.



3. Perform any of the steps below in the **Display Filter Groups** section to configure filter groups.
   - To add a **Display Filter Group**, perform Step 4 to Step 7.
   - To edit a **Display Filter Group**, perform Step 8.
   - To delete a **Display Filter Group**, perform Step 9.
4. Select the **Add** icon  to add a display filter group.

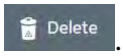
   A new row is added to the table.



5. Configure a display filter group as per the information in the table.

Table 10-30 Configure Display Filter Groups

Field	Action	Description
Name	Enter a name for the display filter group.	The display filter group name must be unique. No default value Allowed values: Up to 20 characters • a to z • A to Z • 0 to 9
Location	Enter the location(s) you want to include for the display filter group.	• If a location of the display filter group is not configured, an asterisk (*) indicating that orders from all locations display to the device. • If an invalid location of the display filter group is configured, an error message displays. Default value: * Allowed values: • 0 to 65534 • Up to 100 characters Individual numbers and number ranges, are supported. Ranges must have a hyphen in between them. For example, 3-50, 45–*. Multiple locations must be comma-separated. For example, to configure download of orders from locations 0, 3, and 10 through 20, enter 0,3,10-20.

6. Select **Save**.
7. Repeat Step 4 to Step 6 to add more display filter groups.
8. To edit an existing display filter group:
   8.1. To enable the edit mode, select anywhere in the row of the display filter group configuration you want to modify in the **Display Filter Groups** section.
   8.2. Make changes to the configuration as per the information in Table 10-30 Configure Display Filter Groups on page 191.
   8.3. Select **Save**.
9. To delete an existing display filter group:
   9.1. Select anywhere in the row of the display filter group configuration you want to delete in the **Display Filter Groups** section.
   9.2. Select the **Delete** icon 

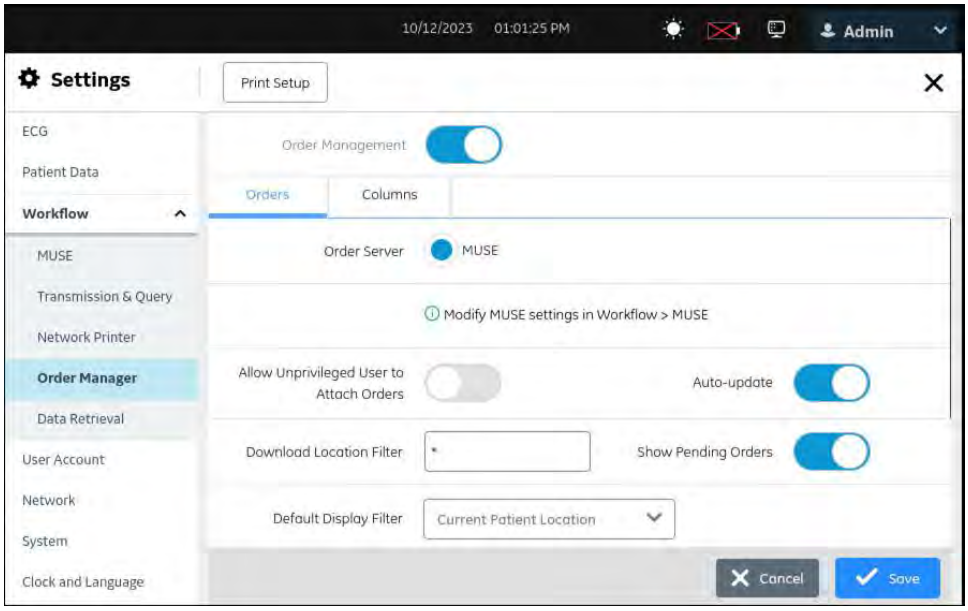
.
   9.3. Select **Save**.

10.6.4.2 Configure Order Settings

Make sure that order management is enabled. See 10.6.4 Configure Order Management on page 188.

1. Select **Settings** > **Workflow** > **Order Manager**.

2. Select **Orders**.



3. Configure order settings as per the information in the table.

Table 10-31 Order Settings

Field	Action	Description
Order Server	Enable or disable this setting.	If this setting is enabled, the orders will be downloaded from the MUSE server. To download orders from MUSE, you need to configure the MUSE server details in **Workflow** > **MUSE** settings. Default value: Enabled
Allow Unprivileged User to Attach Orders	Enable or disable this setting.	• If this setting is enabled, any user who does not have the privilege to view orders can search for a matching order on the device or on the MUSE system using the **Patient ID** or **Visit Number**, and attach the order to the patient test. A patient query mode must be configured and the user should be assigned the **Query Remote Patient Data** privilege for automatic patient query. • If this setting is disabled, users who do not have the privilege to view orders cannot attach orders by searching for them. • This does not apply to the default STAT user role. Default value: Disabled
Auto-Update	Enable or disable this setting.	If this setting is enabled, the **Orders** list is automatically updated from the configured order management server. Default value: Enabled
Show Pending Orders	Enable or disable this setting.	• If this setting is enabled, the system displays all pending orders, regardless of the device used to move the order to the pending state. Default value: Enabled

Continues on the next page

Table 10-31 Order Settings (Table continued)

Field	Action	Description
Download Location Filter	Enter the location from which to download orders.	• If a download location filter is not configured, an asterisk (*) display indicating that orders from all locations download to the device. • If an invalid download location filter is configured, an error message displays. • If the filter exceeds 50 locations, an error message displays. Default value: * Allowed values: • 0 to 65534 • Up to 599 characters Up to 50 location filters, separated by commas and without repetition, can be configured. Individual numbers, as well as number ranges, are supported. A location filter can be: • A single location, for example, 1 • A location range, for example, 5-35. Ranges must have a hyphen in between them. For example, 3-50, or when using an asterisk, 45-*. **NOTE** Only orders within a 40 hour time window will be downloaded (-28 hours before current time and +12 hours past current time). This prevents downloading very large number of orders from the server.
Default Display Filter	Select the default display filter to be displayed on the **Orders** list.	You can select one of the following display filters: • Current Patient Location • Show All Locations • User-configured filter groups If you do not select any of the display filters, the Current Patient Location filter will be applied.

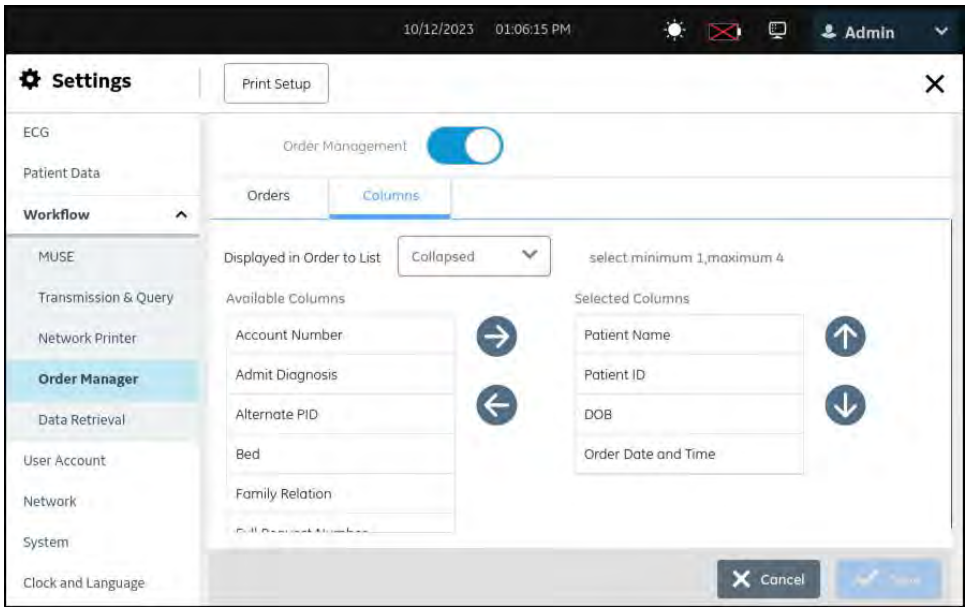
4. Select **Save**.

10.6.4.3 Configure Columns for the Orders List

Make sure that order management is enabled. See 10.6.4 Configure Order Management on page 188.

The columns displayed in the **Orders** list on the Acquisition screen are configurable.

1. Select **Settings** > **Workflow** > **Order Manager**.
2. Select **Columns**.



3. Select **Collapsed** or **Expanded** in the **Displayed in Order to List** drop-down list.

Table 10-32 Column Settings for Orders List

Field	Number of Columns Supported	Default Columns in List
Displayed in Order to List (Collapsed) **NOTE** If this list does not include one or more of the columns below: **Patient Name**, **Patient ID**, or **Visit Number**, an error message displays.	1 to 4 columns	• **Patient Name** • **Patient ID** • **DOB** • **Order Date and Time** **NOTE** Upon a factory reset, these column names display in the same order as in the **Orders** list.
Displayed in Order to List (Expanded) **NOTE** This list includes the columns in the collapsed list by default.	1 to 11 columns	• **Patient Name** • **Patient ID** • **DOB** • **Order Date and Time** • **Order Number** • **Ordering MD ID** • **Order Type** • **Location** • **Room** • **Priority** • **Status** **NOTE** Upon a factory reset, these column names display in the same order as in the **Orders** list.

4. Configure the columns to display in each view:

4.1. To include columns in the **Orders** collapsed or expanded list, select a column name in the available columns list on the left-side and select the right arrow ➔ to move the column name to the selected column list on the right-side.

4.2. To exclude columns from the **Orders** collapsed or expanded list, select a column name in the selected columns list on the right-side and select the left arrow ← to move the column name to the available columns list on the left-side.

4.3. Repeat steps Step 4.1 and Step 4.2 until the desired list of columns to display in the collapsed and expanded lists are included in the selected columns list on the right-side.

5. To reorder the columns in the **Orders** list, select a column name and use the up arrow ^ or down arrow ˅.

NOTE

By default, the **Orders** collapsed and expanded lists are always sorted by location, in descending order. If the **Location** field does not display, the orders list is sorted based on the information in the first column, in descending order.

6. Select **Save**.

10.6.5 Patient Query Overview

NOTE

The ADT and Orders can only be retrieved by the Patient ID or Visit Number and not by both.

The patient query results differ depending on the privileges assigned to the user and the configured patient query setting.

When the **View Orders** user privilege or **Allow Unprivileged User to Attach Orders** setting is on and the **Query Remote Patient Data** user privilege is on:

If the Patient query setting is …	Then …
Query Orders	Searching by the Patient ID or Visit Number retrieves matching orders on the device, the MUSE system or the EMR Gateway system.
Query Orders then ADT	Searching by the Patient ID or Visit Number retrieves matching orders on the device, the MUSE system or the EMR Gateway system. If no orders are found, an ADT query is triggered.
Query ADT Only	Searching by the Patient ID or Visit Number triggers an ADT query on the MUSE system or the EMR Gateway system.

When the **View Orders** user privilege or **Allow Unprivileged User to Attach Orders** setting is off and the **Query Remote Patient Data** user privilege is on:

If the Patient query setting is …	Then …
Query Orders	No records are retrieved.
Query Orders then ADT or **Query ADT Only**	An ADT query is triggered on the MUSE system or the EMR Gateway system.

If the user does not have the **Query Remote Patient Data** privilege, ADT query cannot be triggered, regardless of how you configure the patient query setting.

The search results differ depending on the search criterion and system settings:

Table 10-33 Patient Query Result from the MUSE system

Search criterion	Patient query setting	DCP destination with ADT/EMR Order Query enabled and MUSE order server setting	Search result
Patient ID or Visit Number	**Query Orders**	Configure MUSE Order Server settings.	Patient ID search: Matching local or remote orders are retrieved. Visit Number search: Only matching local orders are retrieved.
Visit Number	**Query Orders**	Configure DCP server with ADT/EMR Order Query enabled corresponding to MUSE Order Server settings and make sure that both IP addresses are same.	Matching local or remote orders are retrieved.
Patient ID or Visit Number	**Query Orders then ADT**	Configure DCP server with ADT/EMR Order Query enabled corresponding to MUSE Order Server settings and make sure that both IP addresses are same.	Matching local or remote orders are retrieved (if found), otherwise matching ADT data (from remote server) is retrieved.
Patient ID or Visit Number	**Query ADT Only**	Make sure that the DCP server destination is enabled with ADT/EMR Order Query.	Only matching ADT data is retrieved from remote server.

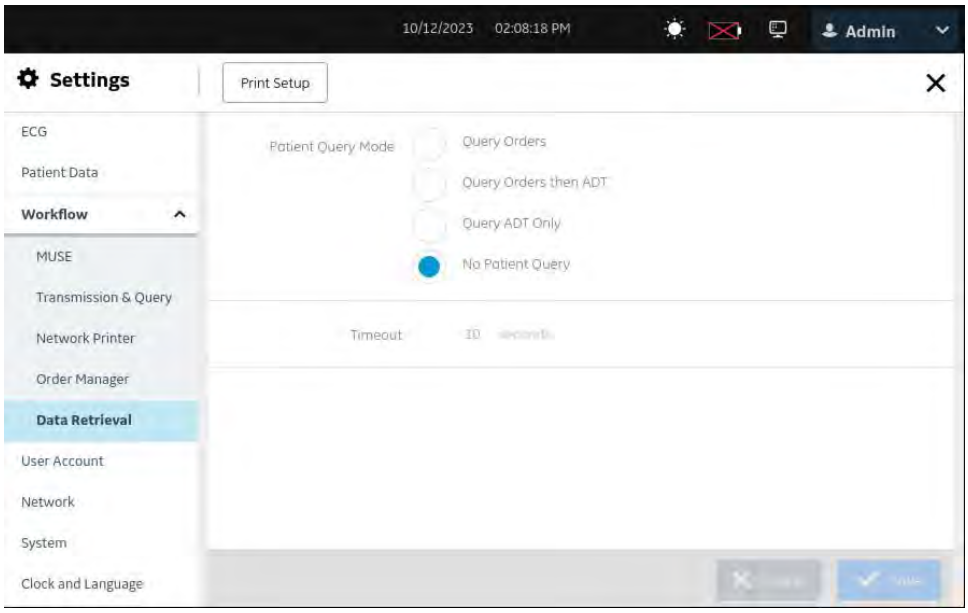
Table 10-34 Patient Query Result from the EMR Gateway system

Search criterion	Patient query setting	DCP destination with ADT/EMR Order Query enabled and EMR Gateway system as configured DCP server	Search result
Patient ID or Visit Number	**Query Orders**	Configure DCP server as EMR Gateway system with ADT/EMR Order Query enabled.	Matching remote orders are retrieved from the EMR Gateway system.
Patient ID or Visit Number	**Query Orders then ADT**	Configure DCP server as EMR Gateway system with ADT/EMR Order Query enabled.	Matching remote orders are retrieved (if found), otherwise system performs ADT search and matching ADT data is retrieved from the EMR Gateway system.
Patient ID or Visit Number	**Query ADT Only**	Configure DCP server as EMR Gateway system with ADT/EMR Order Query enabled.	Only matching ADT data is retrieved from the EMR Gateway system.

10.6.6 Configure Data Retrieval

1. Select **Settings** > **Workflow** > **Data Retrieval**.

   The **Data Retrieval** screen displays.



2. Configure the fields as per the information in the table:

Table 10-35 Patient Query Settings

Field	Action	Description
Patient Query Mode	Select an option to configure the patient query mode.	Default value: **No Patient Query** Allowed values: • **Query Orders** • **Query Orders then ADT** • **Query ADT Only** • **No Patient Query**
Timeout	Enter the duration (in seconds) that the network waits for a response to the ADT query, before a timeout error displays.	Default value: **10** Allowed values: 0 to 1000

3. Select **Save**.

10.7 User Account

Make sure that your user role is assigned to the user account privilege.

If...	Then...
Users are managed locally	Perform the following configurations: • 10.7.5 Configure User Profiles on page 211 • 10.7.4 Configure User Roles on page 207
Users are managed using LDAP	10.7.6 Configure LDAP on page 215.

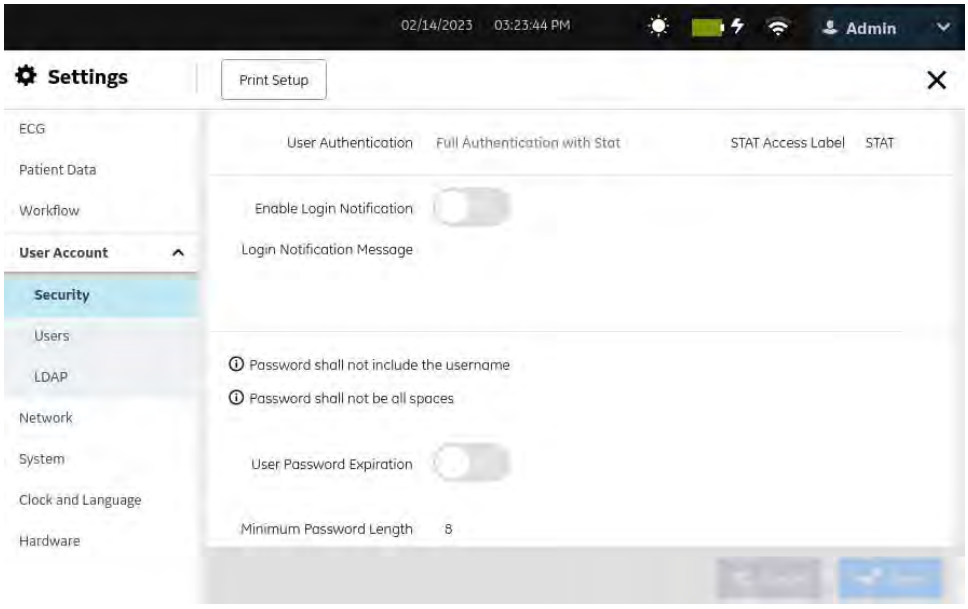
Select **Settings** > **User Account** menu to configure the following:

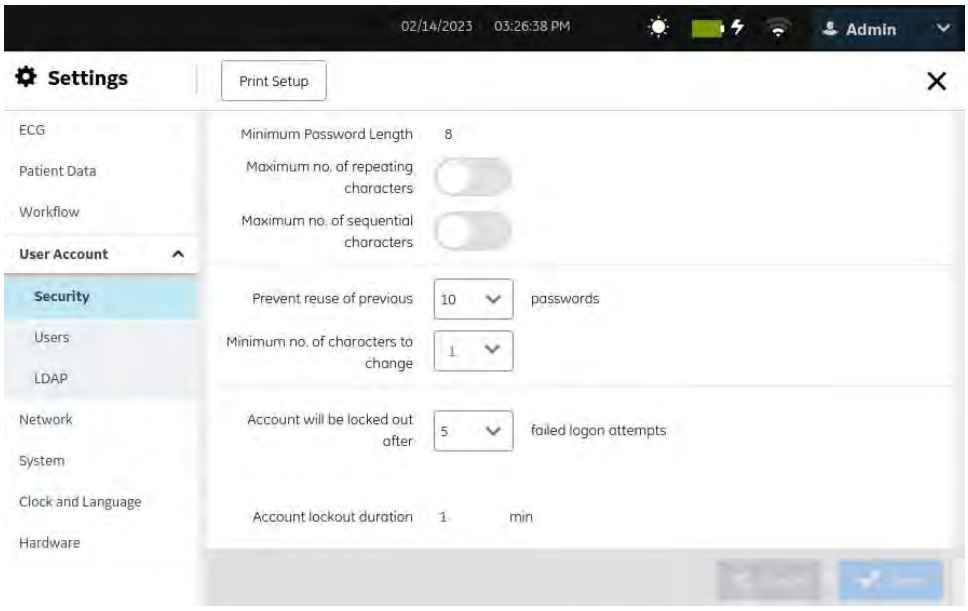
- Security - 10.7.1 Configure Security on page 198
- User Roles:
  - 10.7.2 Types of User Roles on page 204
  - 10.7.4 Configure User Roles on page 207
- User Profiles:
  - 10.7.3 Types of User Profiles on page 205
  - 10.7.5 Configure User Profiles on page 211
- LDAP - 10.7.6 Configure LDAP on page 215

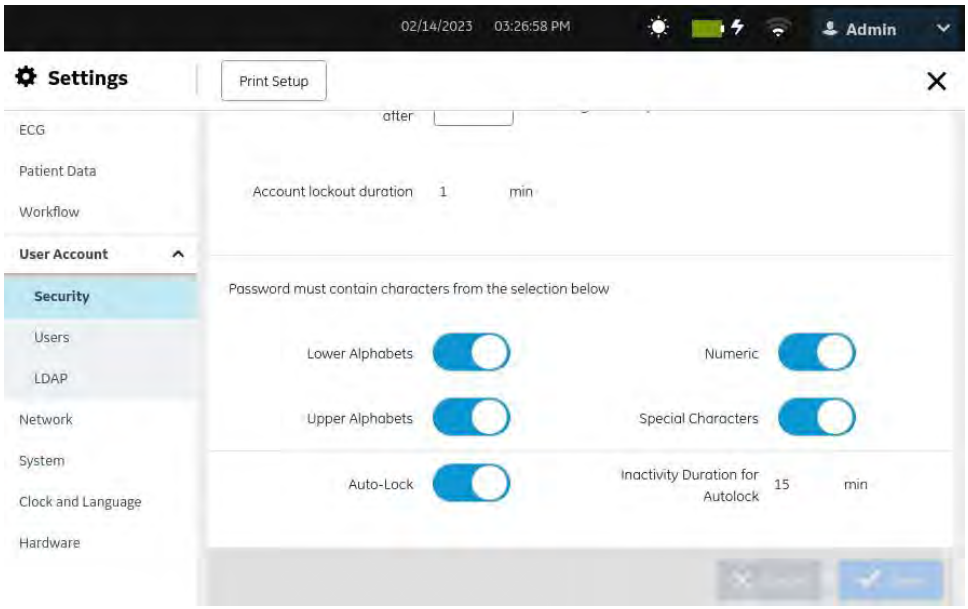
10.7.1 Configure Security

1. Select **Settings** > **User Account** > **Security**.

   The **Security** screen displays.




02/14/2023 03:26:38 PM
Admin
Settings
Print Setup
ECG
Patient Data
Workflow
User Account
Security
Users
LDAP
Network
System
Clock and Language
Hardware
Minimum Password Length 8
Maximum no. of repeating characters
Maximum no. of sequential characters
Prevent reuse of previous 10 passwords
Minimum no. of characters to change 1
Account will be locked out after 5 failed logon attempts
Account lockout duration 1 min


02/14/2023 03:26:58 PM
Admin
Settings
Print Setup
ECG
Patient Data
Workflow
User Account
Security
Users
LDAP
Network
System
Clock and Language
Hardware
Account lockout duration 1 min
Password must contain characters from the selection below
Lower Alphabets
Numeric
Upper Alphabets
Special Characters
Auto-Lock
Inactivity Duration for Autolock 15 min

2. Configure the fields as per the information in the table.

Table 10-36 Configure Security

Field	Action	Description
User Authentication	Select a value from the drop-down list to configure the type of user authentication for the device.	• If **Full Authentication with STAT** is selected, the device displays a login screen.  The **STAT User** selects the **STAT** button to access the device without any password credentials. All other users need to log on to the device with a user name and password. • If **No Authentication** (default) is selected, the device does not display a login screen. Users access the device without a user name and password. • If **Technician ID** is selected, the device displays a login screen. Users access the device with a valid **Technician ID**.  Default value: **No Authentication** **NOTE** If you enable user authentication, you are automatically logged off after saving the settings. The login screen displays. You need to log in to the device with the correct login credentials based on the configured mode of user authentication.

Continues on the next page

Table 10-36 Configure Security (Table continued)

Field	Action	Description
STAT Access Label	Enter the label name to display in the login screen.	This field is enabled only when the **Full Authentication with STAT** setting is selected from the **User Authentication** field. Default value: **STAT** Allowed values: 1 to 20 characters • A to Z • a to z • 0 to 9 • All special characters
Enable Login Notification	Enable or disable this setting.	If this setting is enabled, the **Login Notification Message** field is enabled. You must configure a notification message that displays at the time of login and acknowledged by users who attempt to log in to the device. If this setting is disabled, the **Login Notification Message** field is disabled. Default value: Disabled
Login Notification Message	Enter the login notification message.	No default value Allowed values: Up to 15000 characters • A to Z • a to z • 0 to 9 • All special characters
User Password Expiration	Enable or disable this setting.	If this setting is enabled, set the duration for password expiration in the **Password lifetime duration Minimum and Maximum (days)** fields. The password expires after the configured duration, and the user is prompted to set a new password. If this setting is disabled, the password does not expire. Default value: Disabled

Continues on the next page

Table 10-36 Configure Security (Table continued)

Field	Action	Description
Password lifetime duration (days)	Set the **Minimum** and **Maximum** password expiration duration in days, if **User Password Expiration** setting is enabled.	**Minimum** duration: This specifies the minimum amount of time a password needs to remain unchanged. • If it is set to one day then the password cannot be changed again until tomorrow. • If it is set to seven days then the password cannot be changed again until next week. • If it is set to zero then there is no minimum duration. The password may be changed immediately. **Maximum** duration: This specifies the maximum amount of time a password can exist before it is required to be changed. If it is set to 90 days then the password must be changed after three months. **NOTE** The expired password will still work but must be changed when used. Default value for minimum and maximum: **1** and **90** Allowed values for minimum and maximum: 0 to 364 and 0 to 365
Minimum Password Length	Set the minimum number of characters required for a user password.	While adding or modifying a user, if the user password does not meet the minimum number of required characters, the password is not accepted by the system. The password must contain a number of characters equal to or greater than the **Minimum Password Length**. Default value: 8 characters Allowed values: 8 to 14 characters
Maximum no. of repeating characters	Enable or disable this setting.	If this setting is enabled, a drop-down list displays. You can select a value as the allowed maximum number of repeated characters in the password. Default value for maximum number: **1** Allowed values for maximum number: **1** to **Minimum Password Length** If this setting is disabled, no limit for repeated characters in the password. Default value: Disabled
Maximum no. of sequential characters	Enable or disable this setting.	If this setting is enabled, a drop-down list displays. You can select a value as the allowed maximum number of sequential characters in the password. Default value for maximum number: **1** Allowed values for maximum number: **1** to **Minimum Password Length** If this setting is disabled, no limit for sequential characters in the password. Default value: Disabled
Prevent reuse of previous passwords	Select a value from the drop-down list to configure the reuse of previous passwords.	This specifies the number of previously used passwords that a user is not allowed to change their password to. Default value: **10** Allowed values: 10 to 32

Continues on the next page

Table 10-36 Configure Security (Table continued)

Field	Action	Description
Minimum no. of characters to change	Select a value from the drop-down list to configure the minimum number of characters to change.	This specifies the minimum number of characters that a user needs to change from previous passwords. Default value: **1** Allowed values: **1** to **Minimum Password Length**
Account will be locked out after failed logon attempts	Select a value from the drop-down list to lock the account after failed logon attempts.	This specifies the number of repeated failed login attempts that causes a user account to be temporarily locked. **NOTE** You can login as a STAT user if your account has been locked. Default value: **5** Allowed values: 3 to 99
Account lockout duration (min)	Select a value from the drop-down list to set the duration (in minutes) for account to be locked.	This specifies to configure the duration in minutes to lock the account. If it is set to one minute then the account will be locked for one minute. You cannot log in for the next one minute. Default value: **1** Allowed values: 1 to 120
Lower Alphabets	Enable or disable this setting.	If this setting is enabled, the lower alphabet characters are required to be used in the password. If this setting is disabled, the lower alphabet characters are not required to be used in the password. Default value: Enabled
Numeric	Enable or disable this setting.	If this setting is enabled, the numeric characters are required to be used in the password. If this setting is disabled, the numeric characters are not required to be used in the password. Default value: Enabled
Upper Alphabets	Enable or disable this setting.	If this setting is enabled, the upper alphabet characters are required to be used in the password. If this setting is disabled, the upper alphabet characters are not required to be used in the password. Default value: Enabled
Special Characters	Enable or disable this setting.	If this setting is enabled, the special characters are required to be used in the password. If this setting is disabled, the special characters are not required to be used in the password. Default value: Enabled
Auto-Lock	Enable or disable this setting.	If this setting is enabled, the device is automatically locked after a configured duration of inactivity. If this setting is disabled, the device is not locked automatically. Default value: Enabled

Continues on the next page

Table 10-36 Configure Security (Table continued)

Field	Action	Description
Inactivity Duration for Autolock (min)	Enter the duration of inactivity (in minutes) after which the system must be automatically locked, if the **Auto-Lock** setting is enabled,	Default value: **15** Allowed values: 1 to 60

3. Select **Save**.

10.7.2 Types of User Roles

The roles below are pre-defined on the device:

- **System Admin**
- **Clinical**
- **STAT**
- **Service**

Table 10-37 Pre-Defined User Roles

User Role	Description	Default Privileges
System Admin	The **System Admin** role has all privileges by default. The Administrator can add roles to the locally managed user role list. The privileges of the user-defined role can be changed.	• Access Settings • Activate ECG Simulator • Access Service • Access Audit Logs • View Reports • View Orders • Edit Reports • Delete Reports • Transmit Reports • User Management • Software Update • Edit Critical Value Settings* • View Patient List • Query Remote Patient Data
Clinical	The **Clinical** role is assigned to the **Default User** by default. The privileges of the **Clinical** role can be changed. The role of the **Default User** can be changed.	• View Reports • View Orders • Edit Reports • Delete Reports • Transmit Reports • View Patient List • Query Remote Patient Data

Continues on the next page

Table 10-37 Pre-Defined User Roles (Table continued)

User Role	Description	Default Privileges
STAT	The **STAT** role is assigned to the **STAT User** by default. The privileges of the **STAT** role can be changed. The role of the **STAT User** can be changed.	• Transmit Reports
Service	The **Service** role is assigned to the **Service** user by default. The privileges of the **Service** role can be changed. The role of the **Service** user cannot be changed.	• Access Settings • Activate ECG Simulator • Access Service • Software Update

NOTE

Roles suffixed with an asterisk (*) in the table display in the *User Roles* screen even if the required settings are not enabled in the *Service* screen. See the *MAC 5 Resting ECG Analysis System Service Manual* for information to enable the settings.

10.7.3 Types of User Profiles

The users below are pre-defined on the device:

- **Admin**
- **Default User**
- **STAT User**
- **Service**

Table 10-38 Pre-Defined User Profiles

User Profile	Description
Admin	This pre-defined administrator can access the device with password credentials to set up, edit, and delete configurations. The default password to login as the **Admin** user is admin123. The **Admin** user is prompted to change the default password immediately after the first login. Only one local **Admin** user can exist on the device. The Administrator can add users to the locally managed user list or configure LDAP-based user authentication. The password-related fields of the **Admin** user can be modified. See 10.7.5 Configure User Profiles on page 211. **NOTE** Safeguard the **Admin** user password and make sure that you do not disclose your password to anyone. Do not use the **Admin** user account for day-to-day activities. If the **Admin** user forgets the password for the **Admin** user account: • A user with the **User Management** privilege can change the **Admin** user password in the *Users* settings screen. • A user can initiate system reset by pressing ↑↓←→↑↓←→ in the **Login** screen and entering the serial number of the device, when prompted. System reset is used to reset all settings to the factory default (which includes the admin password). ALL DATA is also deleted when you do a system reset. The fields below cannot be modified: • User Name • Display Name • Role (**System Admin**) You cannot add, delete, or disable the **Admin** user.
Default User	When user authentication is disabled and the device is turned on to acquire and print an ECG, this pre-defined user is automatically logged in without entering a password. Only one **Default User** can exist on the device. The **Default User** is assigned the **Clinical** role by default. The role of the **Default User** can be modified. See 10.7.4 Configure User Roles on page 207. The **Default User** does not have access to the *Settings* or *Service* screens by default, and is prompted to log in as a user with privileges to access these screens. However, if the role of the **Default User** is modified to include these privileges, the user can access these screens without user authentication. You cannot add, delete, or disable the **Default User**.
STAT User	When user authentication with STAT access is enabled, the **STAT User** can access the device without entering a password to acquire, print, and transmit an ECG. The **STAT User** is assigned the **STAT** role by default. The role of the **STAT User** can be modified. See 10.7.4 Configure User Roles on page 207. You cannot add, delete, or disable the **STAT User**.

Continues on the next page

Table 10-38 Pre-Defined User Profiles (Table continued)

User Profile	Description
Service	By default, the **Service** user profile is disabled in the device. The **Service** user profile can be enabled by a user with appropriate privileges. If the **Service** user profile is enabled, this user can access the device with password credentials when user authentication is enabled. The password for the **Service** user is set when the **Service** user profile is enabled. The customer specifies the password for the **Service** user. **NOTE** Once the **Service** user profile is disabled, previously set password will not be valid. When the **Service** user profile is enabled next time, you must set a new password. The **Service** user is assigned to the **Service** role by default. You cannot add or delete the **Service** user profile.

Table 10-39 User-Defined User Profiles

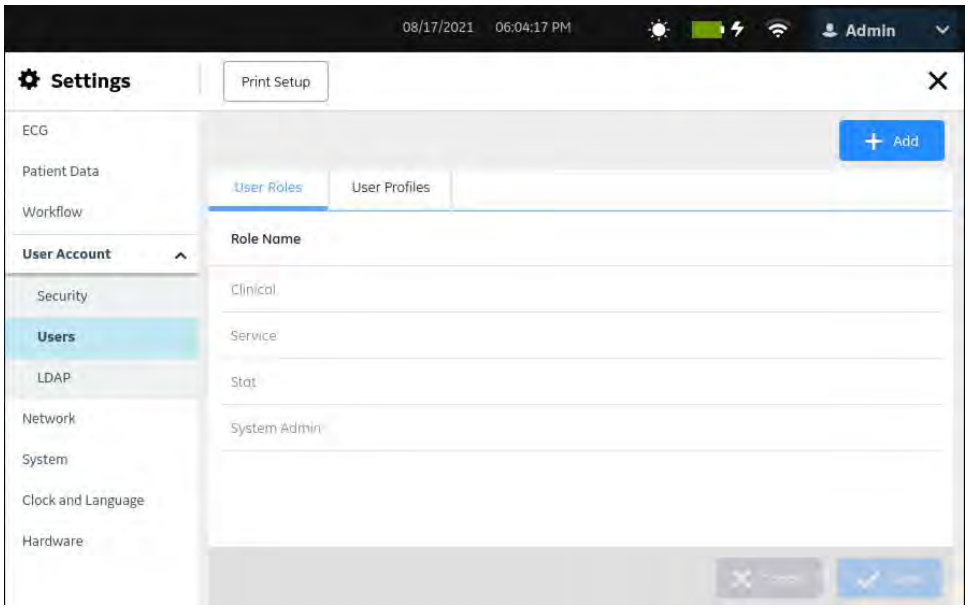
User Profile	Description
Local user	When user authentication is enabled, this locally-added user can access the device with password credentials to perform tasks based on the assigned user privileges. Up to 100 local users can exist on the device. A user with user management privileges can add, modify, delete, or disable a Local user. See 10.7.5 Configure User Profiles on page 211.
LDAP users	When user authentication is enabled and LDAP-based user authentication is configured, an LDAP user can access the device with password credentials to perform tasks based on the assigned LDAP group role privileges. See 10.7.6 Configure LDAP on page 215.

10.7.4 Configure User Roles

Make sure that your user role is assigned to the user management privilege.

1. Select **Settings** > **User Account** > **Users**.
2. Select **User Roles**.

   The **User Roles** screen displays.



3. Perform the required procedures to configure user roles, as applicable:
   - To add a user role, perform Step 4 to Step 7.
   - To edit a user role, perform Step 9.
   - To delete a user role, perform Step 10.
4. Select the **Add** icon Add to add a user role.

   A new row is added to the user roles table.

5. Configure the user role with the appropriate privileges as per the information in the table.

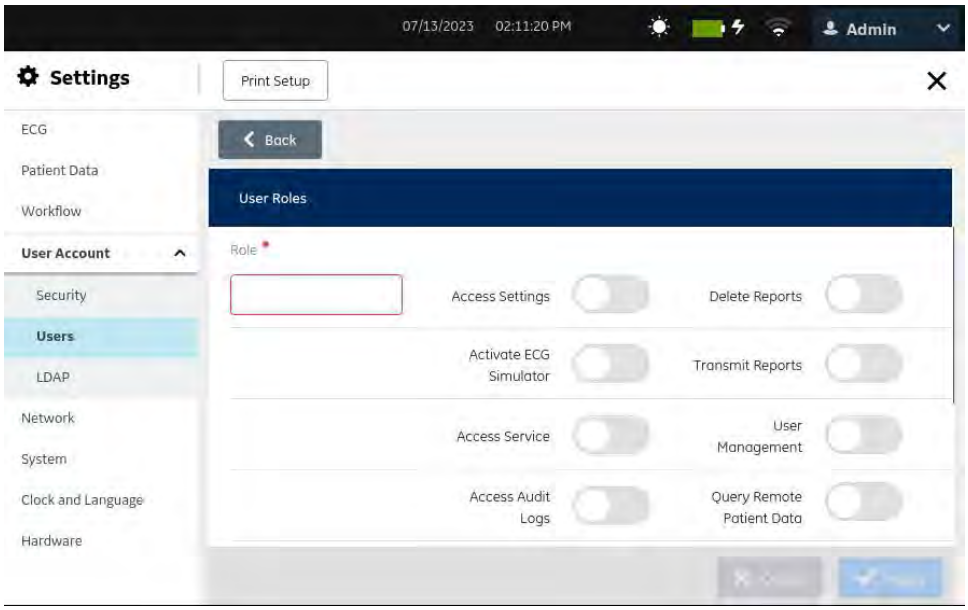


Table 10-40 Configure User Roles

Field	Description
Role	Enter the unique name of the user role. Up to 15 characters are allowed.
Access Settings	Access the **Settings** screen and view the network parameters upon selecting the network status icon. **NOTE** If this privilege is disabled: • The **Activate ECG Simulator**, **Edit Critical Value Settings**, and **User Management** privileges are also disabled. • You can only view the network status upon selecting the network status icon, but cannot view the network parameters such as Device Name, IP address, Subnet Mask, MAC address, Gateway address, and DNS.
Activate ECG Simulator	Access to activate the ECG simulator. **NOTE** If this privilege is enabled, the **Access Settings** privilege is also enabled.
Access Service	Access the **Service** screen. **NOTE** If this privilege is disabled, the **Software Update** and **Access Audit Logs** privileges are also disabled.
Access Audit Logs	Access audit logs. **NOTE** If this privilege is enabled, the **Access Service** privilege is also enabled.

Continues on the next page

Table 10-40 Configure User Roles (Table continued)

Field	Description
View Reports	View patient reports previously stored in the **Files** view. **NOTE** If this privilege is disabled, a user can only view patient reports that acquired during their current login session.
View Orders	View orders in the **Orders** view. Query remote orders from the EMR Gateway system.
Edit Reports	Edit stored patient reports. **NOTE** If the user only has edit patient report privileges and not viewing patient report privileges, they can only edit patient reports they acquired.
Delete Reports	Delete stored patient reports.
Transmit Reports	Transmit patient reports.
User Management	Manage the user profiles and user roles. **NOTE** If you enable this privilege, the **Access Settings** privilege is also enabled.
Software Update	Update the software on the device. **NOTE** If you enable this privilege, the **Access Service** privilege is also enabled.
Edit Critical Value Settings	Edit the critical values setting. **NOTE** This privilege displays only if the CRIT option is purchased and enabled. Contact GE Healthcare Service Support to purchase this option. If you enable this privilege, the **Access Settings** privilege is also enabled.
View Patient List	View the patient list.
Query Remote Patient Data	Query a remote patient data.

6. Select **Apply**.
7. Repeat Step 4 to Step 6 to add more user roles.
8. Select **Save**.
9. To edit an existing user role:
   9.1. To enable the edit mode, select anywhere in the row of the user role configuration you want to modify.
   9.2. Make changes to the user role. For a description of privileges, see Table 10-40 Configure User Roles on page 209.
   9.3. Select **Apply**.
   9.4. Select **Save**.

10. To delete an existing user role:

NOTE

If the role you are attempting to delete is assigned to a user profile or LDAP Group, the role cannot be deleted.

10.1. To enable the edit mode, select anywhere in the row of the user role configuration you want to delete.

10.2. Select **Delete**.

A message displays to confirm if you want to delete the user role.

10.3. Select **Yes** to confirm the deletion of the user role.

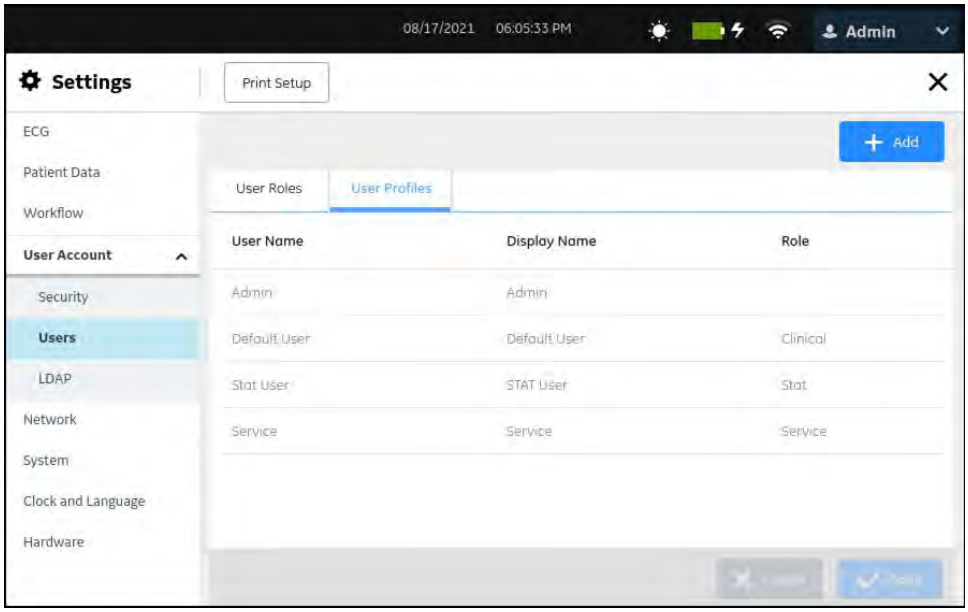
10.4. Select **Save**.

10.7.5 Configure User Profiles

Make sure that your user role is assigned to the user management privilege.

1. Select **Settings** > **User Account** > **Users**.
2. Select **User Profiles**.

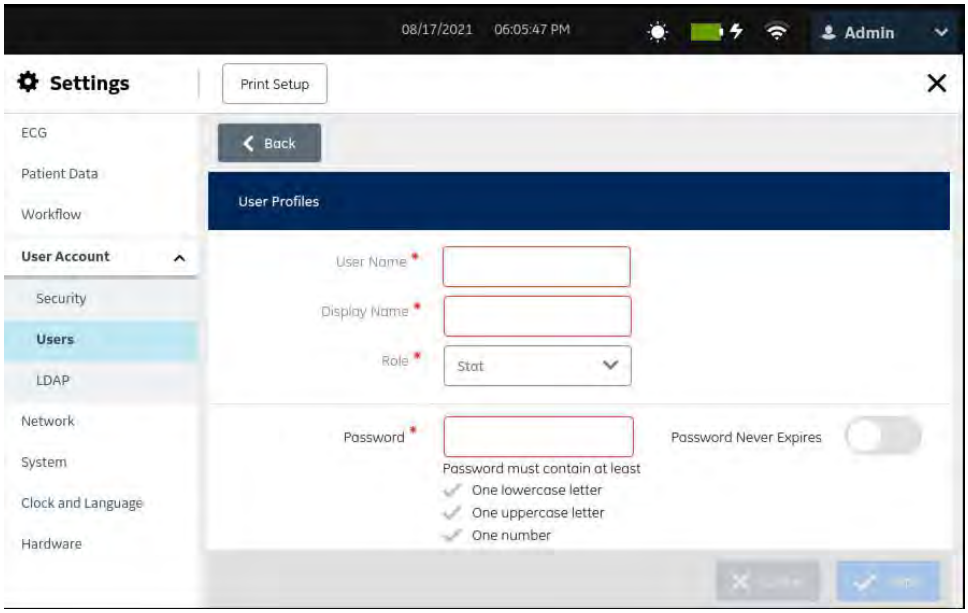
The configured user profiles are listed in the table Table 10-41 Configure User Profiles on page 212. If no user profile is configured, the table is empty.



3. Perform the required procedures to configure user profiles, as applicable:
   - To add a user profile, perform Step 4 to Step 7.
   - To edit a user profile, perform Step 9.
   - To delete a user profile, perform Step 10.
4. Select the **Add** icon Add to add a user profile.

A new row is added to the user profile table.

5. Configure the user profile as per the information in the table.



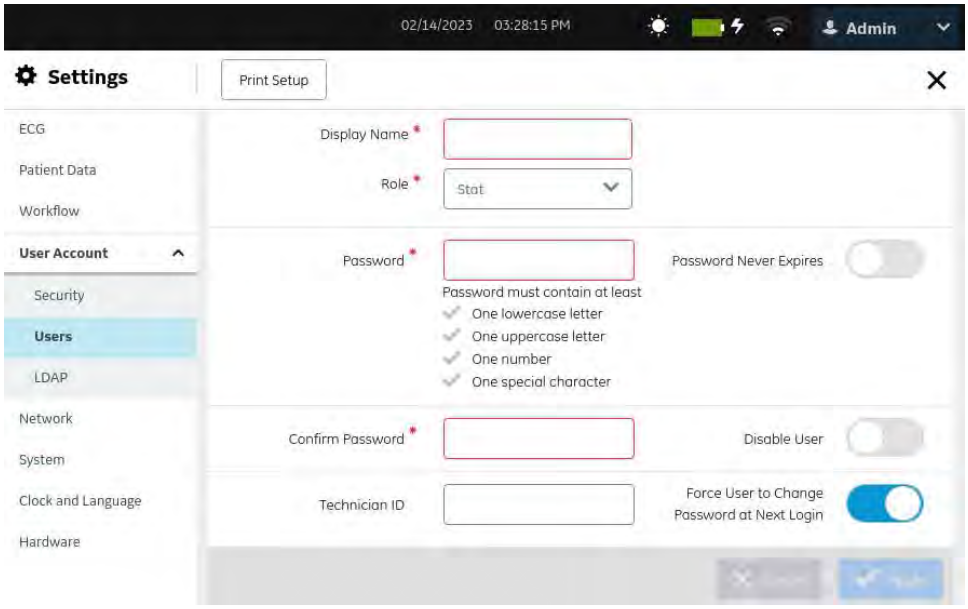


Table 10-41 Configure User Profiles

Field	Action	Description
User Name	Enter a unique name for the user.	If a user with the same user name already exists, an error message displays. This is a required field. No default value. Allowed values: User-defined value up to 15 characters

Continues on the next page

Table 10-41 Configure User Profiles (Table continued)

Field	Action	Description
Display Name	Enter a unique display name for the user.	This name displays on the User Menu on the Acquisition screen. This is a required field. No default value. Allowed values: User-defined value up to 50 characters
Role	To assign a user role to the user, select the role from the drop-down list.	Default value: No default value Allowed values: • **System Admin** • **Clinical** • **Stat** • **Service** • All user-defined roles
Password	Enter the password for the user according to the password rules listed in the Description column.	Each character in the password displays an asterisk (*). If the password rules are not met, the **Password** field display a red box and relevant error messages. Allowed values: • User-defined value up to 126 characters • Minimum number of characters and type of characters allowed is set in the *Security* settings screen. See 10.7.1 Configure Security on page 198. No default value. **NOTE** If a local user forgets the user password, a user with the **User Management** privilege can change the password for the user account in the *Users* settings screen. The local user can log into the device with the changed password.
Confirm Password	Enter the exact duplicate entry of the password entered in the **Password** field	Each character in the password displays an asterisk (*). If there is a mismatch with the password entered in this field and the **Password** field, the **Confirm Password** field displays a red box. Re-enter the password to match the **Password** field. No default value.
Technician ID	Enter the Technician ID associated with the user.	This field can be blank. No default value. Allowed values: • a to z • A to Z • 0 to 9 • All special characters User-defined value up to 20 characters.

Continues on the next page

Table 10-41 Configure User Profiles (Table continued)

Field	Action	Description
Password Never Expires	Enable or disable this setting.	• If this setting is enabled, the password of this user does not expire, even if a duration for password expiration for all users of this device is set in the **Password Expiration Duration** field in the **Security** settings screen. • If this setting is disabled, the password of this user expires when the time of the password exceeds the duration for password expiration set in the **Password Expiration Duration** field in the **Security** settings screen. Default value: Disabled
Disable User	Enable or disable this setting.	• If this setting is enabled, the user is disabled from using the device. • If this setting is disabled, the user is enabled to access the device. Default value: Disabled
Force User to Change Password at Next Login	Enable or disable this setting.	• If this setting is enabled, the user must change the password at the next login. • If this setting is disabled, the user does not need to change the password at the next login. Default value: Enabled **NOTE** This setting is always disabled for default **Service** user.

6. Select **Apply**.
7. Repeat Step 4 to Step 6 to add more user profiles.
8. Select **Save**.
9. If you have the user management privilege, you can use this setting to edit the password of other users. To change your password, go to the **User** menu on the **Acquisition** screen, select **Change Password**.

   To edit an existing user profile:

   9.1. To enable the edit mode, select anywhere in the row of the user profile you want to modify.

   9.2. Make changes to the user profile as per the information in Table 10-41 Configure User Profiles on page 212.

   9.3. Select **Apply**.

   9.4. Select **Save**.

10. To delete an existing user profile:

    10.1. To enable the edit mode, select anywhere in the row of the user profile configuration you want to delete.

    10.2. Select **Delete**.

    A message displays to confirm if you want to delete the user profile.

    10.3. Select **Yes** to confirm the deletion of the user profile.

    10.4. Select **Save**.

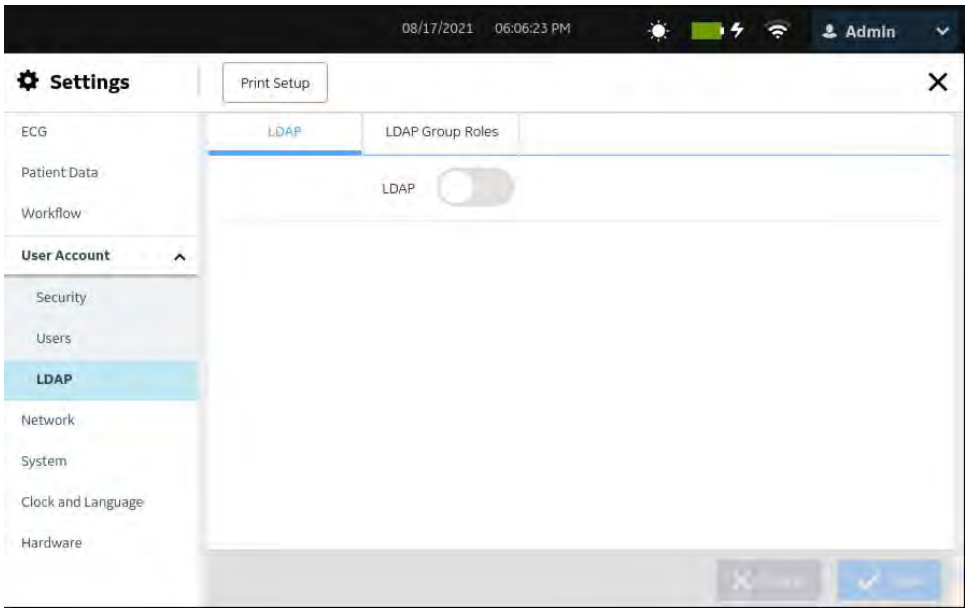
10.7.6 Configure LDAP

Make sure that your user role is assigned the user management privilege.

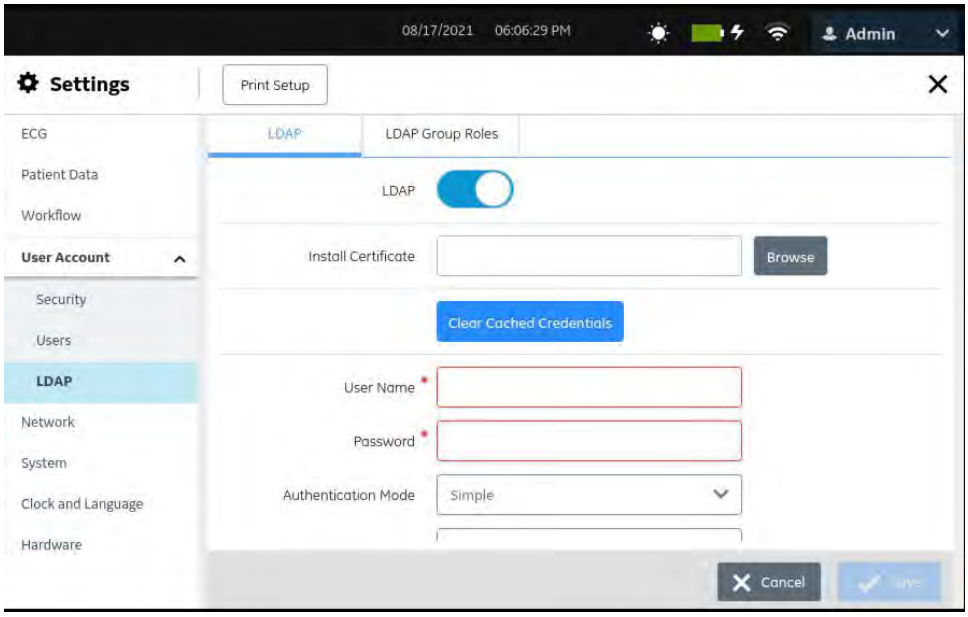
Full Authentication with Stat must be configured for LDAP authentication.

1. Select **Settings** > **User Account** > **LDAP**.
2. Select **LDAP** to view the LDAP settings.

   The **LDAP** screen displays.



3. Enable **LDAP** setting.



4. Configure **LDAP** as per the information in the table.

Table 10-42 Configure LDAP

Field	Action	Description
LDAP	Enable or disable this option.	If this option is enabled, technicians can log in to the device remotely using their network credentials. Default value: Disabled

Table 10-43 Configure LDAP Server

Field	Action	Description
User Name	Enter the valid username.	This field is enabled if the **LDAP** option is enabled. No default value. The LDAP user profiles are managed by the LDAP server administrator. Obtain your username from the LDAP server administrator. This account has read only access to the LDAP hierarchy that contains the details of all users who logs on to the system. Username can be entered in the formats below: • Name (only) • Domain\Name • Email ID
Password	Enter the valid password.	This field is enabled if the **LDAP** option is enabled. No default value. The LDAP user profiles are managed by the LDAP server administrator. Obtain your password from the LDAP server administrator. There is no limit on the maximum number of characters on the device. Different LDAP servers have their own limit. Allowed values: • A to Z • a to z • 0 to 9 • All special characters
Authentication Mode	From the drop-down list, select the desired Authentication Mode.	This field is enabled if the **LDAP** option is enabled. Default value: **Simple** GE Healthcare recommends that you use **ldaps://** server or TLS encryption certificate if you configure **Simple** authentication mode. Allowed value: • Simple • Digest-MD5 • Kerberos Authentication mode is provided by LDAP server administrator.
Kerberos Realm	Enter the Kerberos Realm. It must be entered in upper case.	This field displays only if **Kerberos** authentication mode is selected. No default value. Obtain the domain name from the LDAP server administrator.

Continues on the next page

Table 10-43 Configure LDAP Server (Table continued)

Field	Action	Description
DC Host	Enter the Distribution Center host name.	This field displays only if **Kerberos** authentication mode is selected. No default value. Obtain the host name from the LDAP server administrator.
DC Port	Enter a valid Distribution Center port number.	This field displays only if **Kerberos** authentication mode is selected. Default port for ldaps:// is 636. Default port for ldap:// is 389. Obtain the DC port number from the LDAP server administrator.
User Login Format	Enter the login format.	This field is enabled if the **LDAP** option is enabled. User Login Format is provided by LDAP server administrator. This is a comma separated list of LDAP user name attributes. For example: `cn` and `sAMAccountName`.
Server Name	Enter the IP Address, hostname, or fully qualified domain name.	This field is enabled if the **LDAP** option is enabled. Default value: **ldaps://** Allowed values: A valid ldap or ldaps URL **NOTE** • If you configure an ldaps URL, the **Use CA Certificate** option displays. • If you configure an ldap URL, the **Use TLS Encryption** option displays. **NOTE** **You can secure some communication channels with encryption and authentication. GE Healthcare recommends that you use the encrypted channels, not the unencrypted channels. For example:** • **LDAPS with CA certificate provides encryption and server authentication.** • **LDAPS without CA certificate and LDAP with TLS only provides encryption.**
Server Port Number	Enter a valid LDAP service port number.	This field is enabled if the **LDAP** option is enabled. No default value. Allowed values: 1 to 65535

Continues on the next page

Table 10-43 Configure LDAP Server (Table continued)

Field	Action	Description
Use CA Certificate	Enable or disable this option.	This field displays only if an ldaps URL is configured. If this option is enabled, a CA certificate is required to authenticate and connect to the LDAP server. Install a CA certificate. See 10.7.6.4 Install LDAP SSL CA Certificate on page 222. If this option is disabled, a CA certificate is not required to connect to the LDAP server. The data is encrypted regardless of whether a CA certificate is installed. **NOTE** GE Healthcare recommends that you use a CA certificate when you connect to the LDAP server. If you do not use a CA certificate, the device runs the risk of connecting to an unauthorized LDAP server, potentially enabling an attacker to gain full access to the device and any data that is stored on it. Default value: Disabled
Use TLS Encryption	Enable or disable this option.	This field displays only if an ldap URL is configured. If this option is enabled, the connection to the configured LDAP server is encrypted. If this option is disabled, the connection to the configured LDAP server is not encrypted. Default value: Disabled
Default Domain Name	Enter a valid domain name.	This field is enabled if the **LDAP** option is enabled. This domain name is used if the LDAP user does not enter a domain name to login. If a local user with the same user name exists, then an LDAP user must enter the domain name and user name in the **User Name** field of the Login screen. No default value. Allowed values: • A to Z • a to z • 0 to 9 • All special characters

5. Select **Test Connection** to test the connection to the LDAP server.
   - If the connection is successful, a success message displays.
   - If the connection fails due to an error, resolve the error. See 13.11 LDAP Configuration Errors on page 285.
6. Configure the **Name Path to Groups** as per the information in the table. The **Name Path to Groups** limits the available groups used to determine roles to only those groups within the given path.

Table 10-44 Configure Name Path to Groups

Field	Action	Description
Name Path to Groups	Enter a valid name path to groups (For example, OU=Groups, OU=Clinical Users, DC=domain, DC=com; CN=Roles, O=GE, C=US).	This field is enabled if the **LDAP** option is enabled. Default value: No default value Allowed values: • A to Z • a to z • 0 to 9 • All special characters

7. Select **Test Connection** to test the connection.
   - If the connection is successful, a success message displays.
   - If the connection fails due to an error, resolve the error. See 13.11 LDAP Configuration Errors on page 285.
8. Configure the **Name Path to Users** as per the information in the table. The **Name Path to Users** limits the possible users that can authenticate to the device to only those users within the given path.

Table 10-45 Configure Name Path to Users

Field	Action	Description
Name Path to Users	Enter a valid name path to users (For example, OU=Users, OU=Clinical Staff, DC=domain, OU=Users, DC=com; O=GE, C=US).	This field is enabled if the *LDAP* option is enabled. Default value: No default value Allowed values: • A to Z • a to z • 0 to 9 • All special characters

9. Select **Test Connection** to test the connection.
   - If the connection is successful, a success message displays.
   - If the connection fails due to an error, resolve the error. See 13.11 LDAP Configuration Errors on page 285.
10. Save and close the screen.

    The **Acquisition** screen displays.

10.7.6.1 Configure LDAP Group Roles

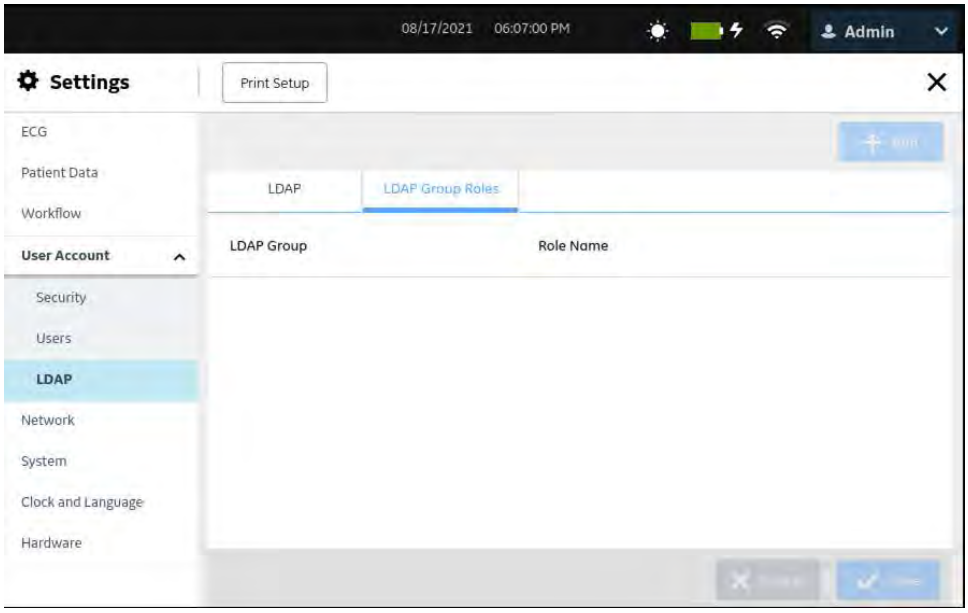
Make sure that your user role is assigned with user management privilege.

Make sure that the LDAP setting is enabled and configured with a valid distinguished name path to groups. See 10.7.6 Configure LDAP on page 215.

When you log in to the device as an LDAP user, you will have the privileges of the first LDAP group role that matches a group in your LDAP account in the list.

1. Select **Settings** > **User Account** > **LDAP**.
2. Select **LDAP Group Roles**.

   The configured **LDAP Group Roles** display on the screen.



3. Perform one of the below steps to configure an LDAP group role:
   - To add an LDAP group role, perform Step 4 to Step 6.
   - To edit an LDAP group role, perform Step 7.
   - To delete an LDAP group role, perform Step 8.
   - To reorder an LDAP group roles, perform Step 9.
4. Select the **Add** icon 

to add an LDAP group role.

   The **Add** panel opens on the right-side of the screen.
5. Configure an **LDAP Group Role**:

   5.1. Enter the search timeout in seconds for the LDAP group search in the **Search Timeout (sec)** field. The default value is 60 seconds. The allowed values are 0 to 999 seconds.

   5.2. Enter a valid search pattern for the LDAP groups in the **Group Name** field.

   Examples of search patterns: ABC, *ABC, ABC*, *ABC*

   NOTE

   You can enter part of the name of the group preceded by or followed by *****, or full name of the group and press the **Search** icon  to show the configured LDAP groups.

   5.3. Select the user role from the **Role** drop-down list to map the role to the LDAP group.

   5.4. Select **Apply** to add the configuration.

The users belonging to the LDAP group are assigned the privileges of the user role mapped to the LDAP group.

6. Repeat Step 4 to Step 5 to add more LDAP group roles. After adding the LDAP group roles, save and close the screen.

   The **Acquisition** screen displays.

7. To edit an existing LDAP group role:

   7.1. Select the **Edit** icon next to the LDAP group role you want to edit.

   - When you are logged in as LDAP user and try to edit the group that you are assigned, an error message displays: **This group is assigned to the currently logged in LDAP user and cannot be edited**.
   - If not, the *Edit* panel opens on the right-side of the screen.

   7.2. Make changes to the LDAP group role as per the information in Step 5.

   7.3. Select **Apply**.

   7.4. Save and close the screen.

   The **Acquisition** screen displays.

8. To delete an existing LDAP group role:

   8.1. Select the **Delete** icon next to the LDAP group role you want to delete.

   - When you are logged in as LDAP user and try to delete the group that you are assigned, an error message displays: **This group is assigned to the currently logged in LDAP user and cannot be deleted**.
   - If not, a message displays asking you to confirm if you want to delete the LDAP group.

   8.2. Select **Yes** to confirm the deletion of the LDAP group role.

   8.3. Save and close the screen.

   The **Acquisition** screen displays.

9. To reorder the LDAP group roles:

   9.1. Select the LDAP group role you want to reorder and drag and drop it to the desired order in the LDAP group role table.

   9.2. Repeat the above step to reorder other LDAP group roles.

   9.3. Save and close the screen.

   The **Acquisition** screen displays.

10.7.6.2 Modify LDAP User

Make sure that your user role is assigned with user management privilege.

1. Select **Settings** > **User Account** > **LDAP**.
2. Select **LDAP** to view the LDAP settings.
3. To modify the added LDAP user, see 10.7.6 Configure LDAP on page 215.
4. When you are logged in as LDAP user and try to configure different LDAP user and server configuration, the error message: **Changes to the LDAP server configuration may affect the added groups** displays.

5. Select **Yes** to confirm.

   The existing LDAP user will be invalid.

6. Save and close the screen.

   The **Acquisition** screen displays.

10.7.6.3 Clear LDAP Cached Credentials

Make sure that your user role is assigned with user management privilege.

Make sure that the LDAP setting is enabled. For more information, see 10.7.6 Configure LDAP on page 215.

1. Select **Settings** > **User Account** > **LDAP**.
2. Select **LDAP** to view the LDAP settings.
3. Enable **LDAP** setting.
4. Select **Clear Cached Credentials** to clear the cache of stored LDAP user credentials.

   When a user successfully logs into the system, the user credentials are stored in the cache. If the network is down, the user can successfully login when in cache. If the cache is cleared, the user will not be able to login unless the network is connected.

   A message displays asking you to confirm if the cached LDAP credentials can be cleared.

5. Select **Yes**.
   - If the action is successful, a success message displays. The cache of stored LDAP user credentials is cleared.
   - If the action fails, a failure message displays.

10.7.6.4 Install LDAP SSL CA Certificate

Before you start this procedure, make sure that:

- Your user role is assigned with user management privilege.
- You obtain the required certificate in the PEM format from your IT department and copy it to the root folder of a USB flash drive for installation.
- You **Enable External USB Storage** in **Settings** > **System** > **Storage** setting. If this setting is not enabled, access to USB flash drives is blocked.
- You enable at least one USB port in **Settings** > **Hardware** > **USB Port** setting. If this setting is not enabled, the device will not recognize the USB flash drives.

1. Connect the USB flash drive containing the CA certificate to the device.
2. Select **Settings** > **User Account** > **LDAP**.
3. Select **LDAP** to view the LDAP settings.
4. Enable **LDAP** setting.
5. Perform the steps below to install a CA certificate:

   5.1. Select **Browse** from the **Install Certificate** field and select the CA certificate from the USB flash drive.

   5.2. Select **Save**.

- If the installation is successful, the CA certificate is saved and the **Install Certificate** dialog is closed.
- If the installation fails because the certificate is in an unrecognized format, an error message displays.

10.7.6.5 Delete LDAP SSL CA Certificate

Before you start this procedure, make sure that your user role is assigned with user management privilege.

1. Select **Settings** > **User Account** > **LDAP**.
2. Select **LDAP** to view the LDAP settings.
3. Enable **LDAP** setting.
4. Perform the steps below to delete the currently installed CA certificate:
   4.1. Select the **Browse** setting.

   The currently installed certificate displays.

   4.2. Select **Delete**.

   A message displays asking you to confirm the deletion of the certificate.

   4.3. Select **Yes**. The certificate or key is deleted.

10.8 Configure Network

You can configure and enable both wired and wireless network connections on the same device. If you enable the wireless and wired connection, the device automatically switches to the wired connection when you connect the LAN cable. If you remove the LAN cable, the device uses the wireless connection.

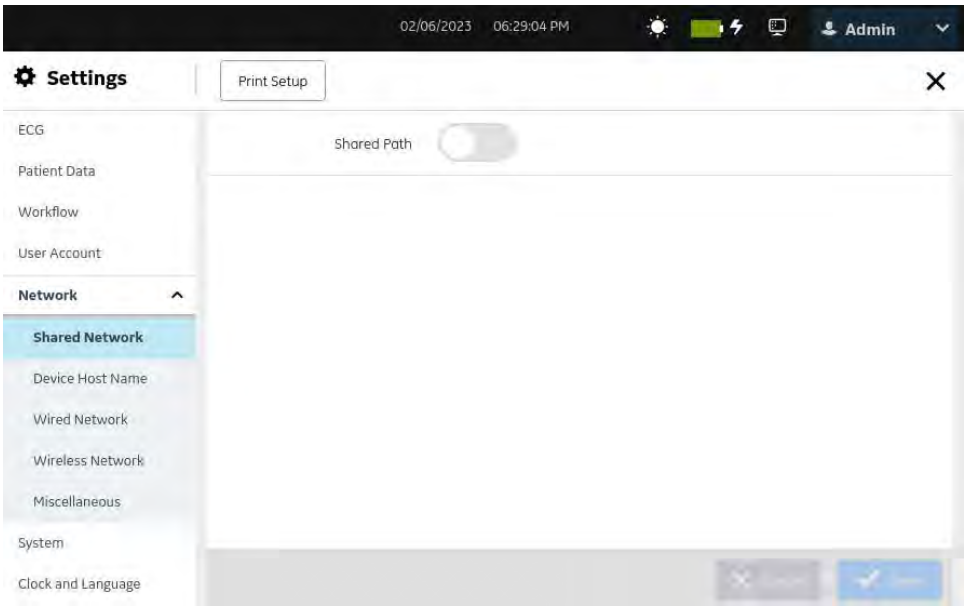
Select **Settings** > **Network** menu to configure the following:

- Shared Network - 10.8.1 Configure Shared Network Settings on page 223
- Device Host Name - 10.8.2 Configure Device Host Name on page 225
- Wired Network - 10.8.3 Configure Wired Network on page 226
- Wireless Network - 10.8.4 Configure Wireless Network on page 227
- Wireless Certificates - 10.8.6 Install Wireless Certificates on page 233
- Miscellaneous - 10.8.8 Configure Proxy Settings on page 237 and 10.8.9 Configure Ping Response on page 238

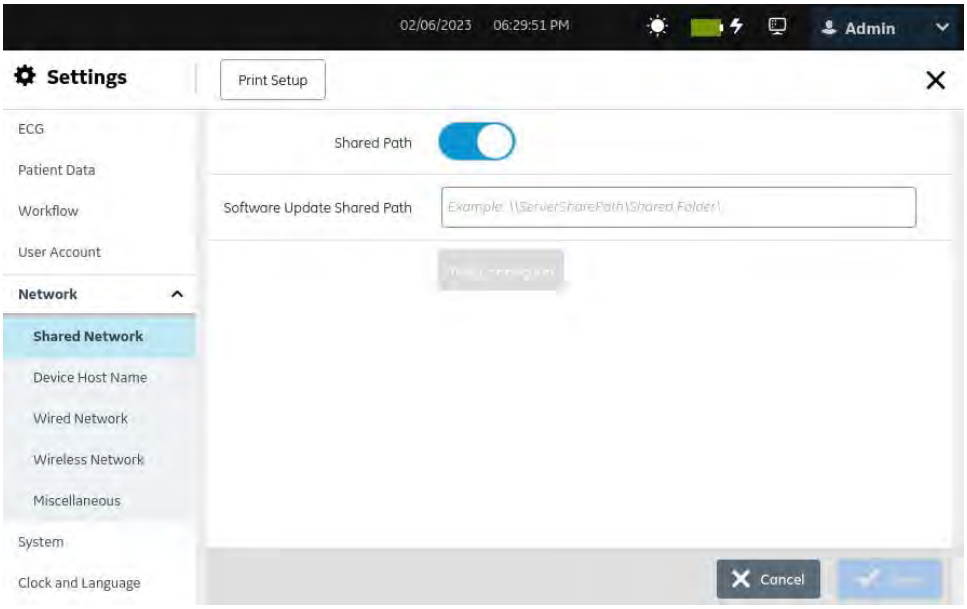
10.8.1 Configure Shared Network Settings

1. Select **Settings** > **Network** > **Shared Network**.

   The shared network setting screen displays.



2. Enable **Shared Path**.



3. Configure the fields as per the information in the table.

Table 10-46 Configure Shared Network Settings

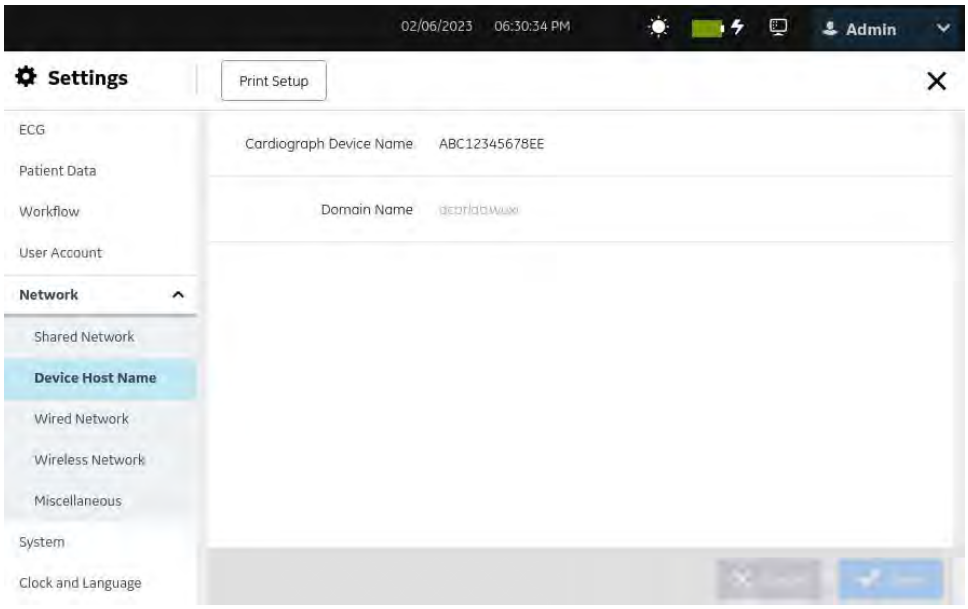
Field	Action	Description
Shared Path	Enable or disable a shared folder in the network to store software files for a software update.	If this setting is enabled: 1. Enter a valid shared path in the text field. Example: `///<IP address> or <Hostname>/<Shared Folder>` 2. Select **Test Connection**. A message displays indicating that the connection has succeeded or failed. In case of failure, see 13.7 Shared Network Connection Errors on page 279. Default value: Disabled

4. Select **Save**.

10.8.2 Configure Device Host Name

1. Select **Settings** > **Network** > **Device Host Name**.

   The device host name setting screen displays.



2. Configure the device host name as per the information in the table.

Table 10-47 Configure Device Host Name

Field	Action	Description
Cardiograph Device Name	Enter the host name of the device in the **Cardiograph Device Name** field.	The host name cannot start or end with a hyphen. The host name cannot be blank as this is a required field. Octets are used to measure the host name field length, instead of characters. Many Unicode characters consist of more than 1 octet. Default value: Serial number of the device Allowed values: • 1 to 63 octets • ASCII characters a to z (case-sensitive) • digits 0 to 9 • hyphen (-)
Domain Name	Enter the domain name in the **Domain Name** field.	Default value: No default value Allowed values: • Up to 61 characters • ASCII characters a to z (case-sensitive) • 0 to 9 • All special characters If the device is configured to obtain the IP address automatically through DHCP, the domain name is assigned by the network.

A combination of the host name (Device Name) and Domain Name configures the device Fully Qualified Domain Name (FQDN). For example, if you enter *myhost* as the **Device Name** and *example.com* as the **Domain Name**, the configured FQDN of the device is *myhost.example.com*.

3. To edit an existing device name:

   3.1. Select anywhere in the row of the device name you want to modify to enable the edit mode.

   3.2. Make changes to the device name as per the information in Table 10-47 Configure Device Host Name on page 225.

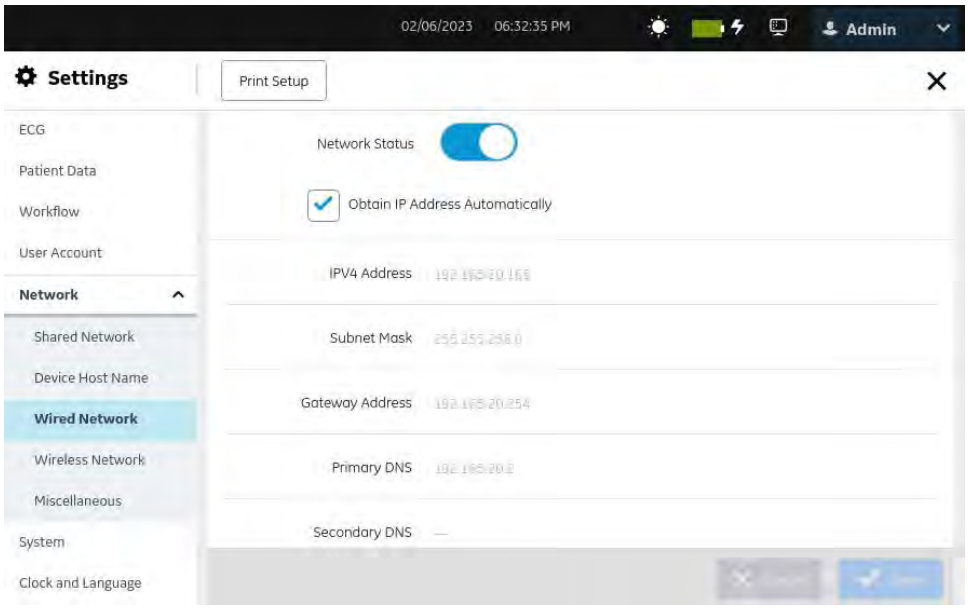
4. Save and close the screen.

   The **Acquisition** screen displays.

10.8.3 Configure Wired Network

1. Select **Settings** > **Network** > **Wired Network**.

   The wired network setting screen displays.



2. Configure the wired network settings as per the information in the table.

Table 10-48 Configure a Wired Connection

Field	Action	Description
Network Status	Enable or disable this option.	• If this option is enabled, the LAN connection to the device is enabled. • If this option is disabled, the LAN connection to the device is disabled. The remaining fields are disabled. Default value: Enabled

Continues on the next page

Table 10-48 Configure a Wired Connection (Table continued)

Field	Action	Description
Obtain IP Address Automatically	Enable or disable this option.	Automatically obtains the IP address. • If this option is enabled, the device automatically obtains an IP address (DHCP) to communicate with the LAN. The remaining fields are read-only and the values cannot be changed. • If this option is disabled, the fields to configure the IPV4 Address, Subnet Mask, Gateway Address, Primary DNS, and Secondary DNS, if any, to communicate with the LAN are made active to change the values. Specify these values in the respective fields. Default value: Enabled
IPV4 Address	Enter the static IPV4 address for the device.	This field is enabled to modify if **Obtain IP Address Automatically** is disabled. No default value Allowed values: A valid IPV4 address
Subnet Mask	Enter the subnet mask identifying the subnet that the device's IPV4 address belongs.	This field is enabled to modify if **Obtain IP Address Automatically** is disabled. No default value Allowed values: A valid subnet mask
Gateway Address	Enter the gateway IP address for the router to use as the default route setting for the device.	This field is enabled to modify if **Obtain IP Address Automatically** is disabled. No default value Allowed values: A valid IPV4 address
Primary DNS	Enter the primary Domain Name Service (DNS) that the device uses.	This field is enabled to modify if **Obtain IP Address Automatically** is disabled. This field is optional. No default value Allowed values: A valid IPV4 address
Secondary DNS	Enter the secondary DNS that the device uses.	This field is enabled to modify if **Obtain IP Address Automatically** is disabled. This field is optional. No default value Allowed values: A valid IPv4 address
Device MAC Address	None	This field is read-only and displays the MAC address of the device. This field displays if **Network Status** is enabled.

3. Save and close the screen.

   The **Acquisition** screen displays.

10.8.4 Configure Wireless Network

To configure a wireless network, make sure **WRLS - Global Wireless** option is purchased and enable them in the **Option Manager**.

NOTE

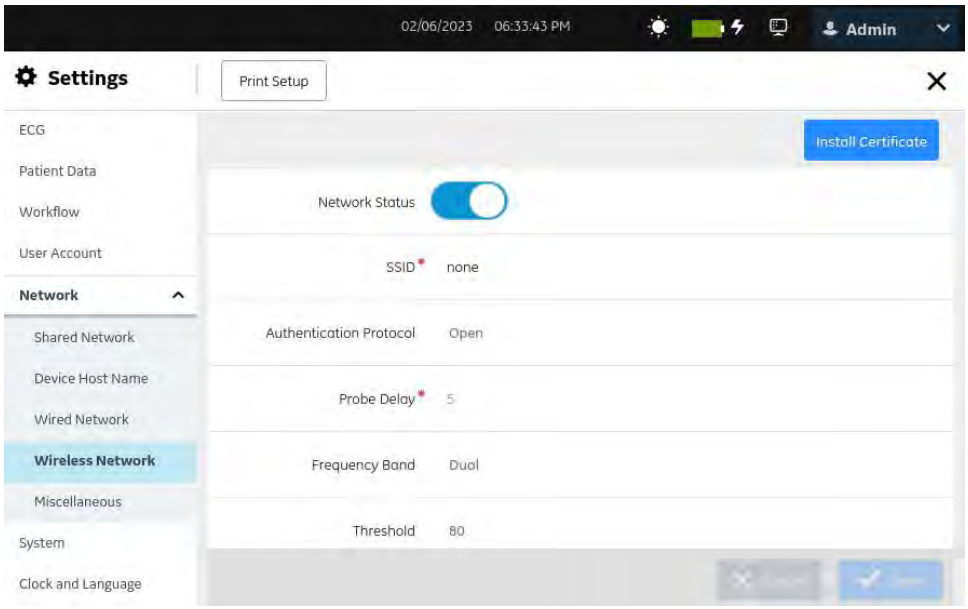
The **VU2** product code is for the **WRLS - Global Wireless** option.

Wireless country of operation is configured on the device at the time of shipping. This configuration is required to enable wireless network connectivity on the device. If wireless country of operation is not configured because the expansion board was replaced or the device does not have a wireless

certification in the specific country, contact your GE Healthcare Service support representative to configure this setting.

1. Select **Settings** > **Network** > **Wireless Network**.

   The wireless network setting screen displays.



2. Enable wireless and configure the authentication protocol as per the information in the table.

Table 10-49 Configure Wireless Authentication Protocol

Field	Action	Description
Network Status	Enable or disable this setting.	• If this setting is enabled, the WLAN connection to the device is enabled. • If this setting is disabled, the WLAN connection to the device and the remaining fields are disabled. Default value: Disabled
SSID	Enter the Service Set Identifier (SSID) for your WLAN.	Default value: No default value Allowed value: Any value (site-specific)
Authentication Protocol	Select a value from the drop-down list to configure the protocol that your site uses to authenticate the transfer of data between the device and other entities on the WLAN.	Different fields display based on the protocol you select. Default value: **Open** Allowed values: • **Open*** • **WEP*** • **WPA*** • **WPA2**
Probe Delay	Enter the number of seconds for probe delay.	When the timer for this delay starts, the device checks if wireless is enabled and the wireless network is connected. If it is disconnected, the device will try to reconnect to the wireless network. Default value: **5** Allowed values: 5 to 120

Continues on the next page

Table 10-49 Configure Wireless Authentication Protocol (Table continued)

Field	Action	Description
Frequency Band	Select a value from the drop-down list to configure the frequency band of wireless operation.	Default value: **Dual** Allowed values: • **Dual** • **2.4 GHz** • **5 GHz**
Threshold (dB)	Select a value from the drop-down list to configure the signal threshold in dB.	To enable the device to roam more frequently, decrease the signal threshold. To prevent the device from roaming frequently, increase the signal threshold. Default value: **80** Allowed values: **50, 55, 60, 65, 70, 75, 80, 85 or 90**

If the configured authentication protocol is:

- **WEP**, go to Step 3.
- **WPA** or **WPA2**, go to Step 4.
- **Open**, go to Step 7.

3. Configure WEP authentication as per the information in the table, and then go to Step 7.

NOTE

You can secure some communication channels with encryption and authentication. GE Healthcare recommends that you use the encrypted channels, not the unencrypted channels. For example, WPA2 for wireless authentication protocol instead of WEP.

Table 10-50 Configure WEP Authentication

Field	Action	Description
Active Passkey	Select a value from the drop-down list to configure the Passkey that you want to make active.	The device uses the Active Passkey to encrypt and decrypt data sent to and received from other entities on the WLAN. The active key needs to match the Passkey on the access point that this device connects to. Default value: **Passkey 1** Allowed values: • **Passkey 1** • **Passkey 2** • **Passkey 3** • **Passkey 4**
Passkey 1 **Passkey 2** **Passkey 3**	A passkey is an encryption key that prevents an unauthorized user or device from accessing a specific wireless network. Only asterisks display in these fields. The actual value is stored in the encrypted database. Enter a maximum of 4 passkeys for this authentication protocol. • If the length of the passkey is 5 or 13, the allowed values are 0 to 9, a to z, A to Z, ! ," ,# ,$,% ,&,' ,(,) ,* ,+ ,, ,- ,. ,/ ,: ,; ,< ,= ,> ,? , @, [,\ ,] ,^ ,_ ,` ,{, |, }, ~, and <space>. • If the length of the passkey is 10 or 26, the allowed values are 0 to 9, a to f, and A to F.	

Continues on the next page

Table 10-50 Configure WEP Authentication (Table continued)

Field	Action	Description
Passkey 4	Default value: No default value Allowed values: 5, 10, 13, or 26 characters	

4. Configure WPA or WPA2 authentication as per the information in the table, and then go to Step 7.

Table 10-51 Configure WPA or WPA2 Authentication

Field	Action	Description
Authentication Mode	Select a value from the drop-down list to configure the authentication mode.	The authentication mode is the client authentication method used to generate unique encryption keys for the device. Default value: **PSK** Allowed values: • **PSK** • **Enterprise**
Encryption Protocol	Select a value from the drop-down list to configure the encryption protocol.	TKIP is the Temporal Key Integrity Protocol. CCMP is the Counter Mode Ciper Block Chaining Message Authentication Code Protocol. Default value: • **TKIP** for WPA • **CCMP** for WPA2 Allowed values: • **TKIP**: This setting is not available for WPA2. • **CCMP**

If the authentication mode is:

- **PSK**, go to Step 5.
- **Enterprise**, go to Step 6.

5. Configure **PSK** authentication mode as per the information in the table.

Table 10-52 Configure PSK Authentication Mode

Field	Action	Description
Passphrase	Enter the passphrase for the authentication mode.	A passphrase is an encryption key that prevents an unauthorized user or device from accessing a specific wireless network. • If the passphrase is 64 characters, the allowed values are 0 to 9, a to f, and A to F. • If the passphrase is 8 to 63 characters, the allowed values are 0 to 9, a to z, A to Z, ! ," ,# ,$,% ,& ,' ,(,) ,* ,+ ,, ,- ,. ,/ ,: ,; ,< ,= ,> ,? , @,[,\ ,] ,^ ,_ ,` ,{, |, }, ~, and <space>. Default value: No default value Allowed values: 8 to 64 characters

6. Configure **Enterprise** authentication mode as per the information in the table.

Table 10-53 Configure Enterprise Authentication Mode

Field	Action	Description
EAP Phase 1	Select a value from the drop-down list to configure EAP Phase 1.	Default value: **PEAP** Allowed values: • **PEAP** • **TTLS** • **TLS**
EAP Phase 2	Select a value from the drop-down list to configure EAP Phase 2.	This field is available only when EAP Phase 1 is configured as PEAP or TTLS. Default value: **MSCHAPv2** Allowed values: • **MSCHAPv2** • **GTC**
Anonymous Identity	Enter the Anonymous identity.	Default value: No default value Allowed values: Any value (up to 256 characters) **NOTE** The default industrial standard for wireless networks is anonymous all lowercase unless the user has created a custom **Anonymous Identity**.
User Name	Enter the user name.	Default value: No default value Allowed values: Any value (up to 256 characters)
Password	Enter the password.	This field is available only when EAP Phase 1 is configured as PEAP or TTLS. Default value: No default value Allowed values: Any value (up to 256 characters)
CA Certificate	Enable or disable this setting.	Only PEM encoded certificate is supported. This field must be enabled when EAP Phase 1 is configured as TLS and cannot be disabled, and optional when EAP Phase 1 is configured as TTLS or PEAP. If **CA certificate** is enabled, make sure that the CA certificate is installed. See 10.8.6 Install Wireless Certificates on page 233. Default value: • Disabled, when EAP Phase 1 is configured as TTLS or PEAP • Enabled, when EAP Phase 1 is configured as TLS
Client Certificate	Enable or disable this setting.	Only PEM encoded certificate is supported. This field must be enabled when EAP Phase 1 is configured as TLS and cannot be disabled, and optional when EAP Phase 1 is configured as TTLS or PEAP. If **Client Certificate** is enabled, make sure that the client private key and client public key are installed. See 10.8.6 Install Wireless Certificates on page 233. Default value: • Disabled, when EAP Phase 1 is configured as TTLS or PEAP • Enabled, when EAP Phase 1 is configured as TLS

7. Configure the setting to obtain the IP address automatically or manually as per the information in the table.

Table 10-54 Enable or Disable DHCP

Field Name	Action	Description
Obtain IP Address Automatically	Enable or disable this setting.	Automatically obtains the IP address. • If this setting is disabled, the fields to configure the IP address, subnet mask, gateway address, primary DNS, and, the secondary DNS, if any, to communicate with the WLAN display. Enter these values in the respective fields. • If this setting is enabled, the device automatically obtains an IP address (DHCP) to communicate with the WLAN. The remaining fields are hidden. Default value: Disabled
IPV4 Address	Enter the static IPV4 address for the device.	This field displays if **Obtain IP Address Automatically** is disabled. Default value: No default value Allowed values: A valid IPV4 address
Subnet Mask	Enter the subnet mask identifying the subnet that the device's IPV4 address belongs.	This field displays if **Obtain IP Address Automatically** is disabled. Default value: No default value Allowed values: A valid subnet mask
Gateway Address	Enter the gateway IP address for the router to use as the default route setting for the device.	This field displays if **Obtain IP Address Automatically** is disabled. Default value: No default value Allowed values: A valid IPV4 address
Primary DNS	Enter the primary Domain Name Service (DNS) that the device uses.	This field displays if **Obtain IP Address Automatically** is disabled. This field is optional. Default value: No default value Allowed values: A valid IPV4 address
Secondary DNS	Enter the secondary DNS that the device uses.	This field displays if **Obtain IP Address Automatically** is disabled. This field is optional. Default value: No default value Allowed values: A valid IPV4 address
Device MAC Address	Display MAC address for the device.	This field is not editable.

8. Save and close the screen.

   The **Acquisition** screen displays.

10.8.5 Configure Wireless Country of Operation

NOTE

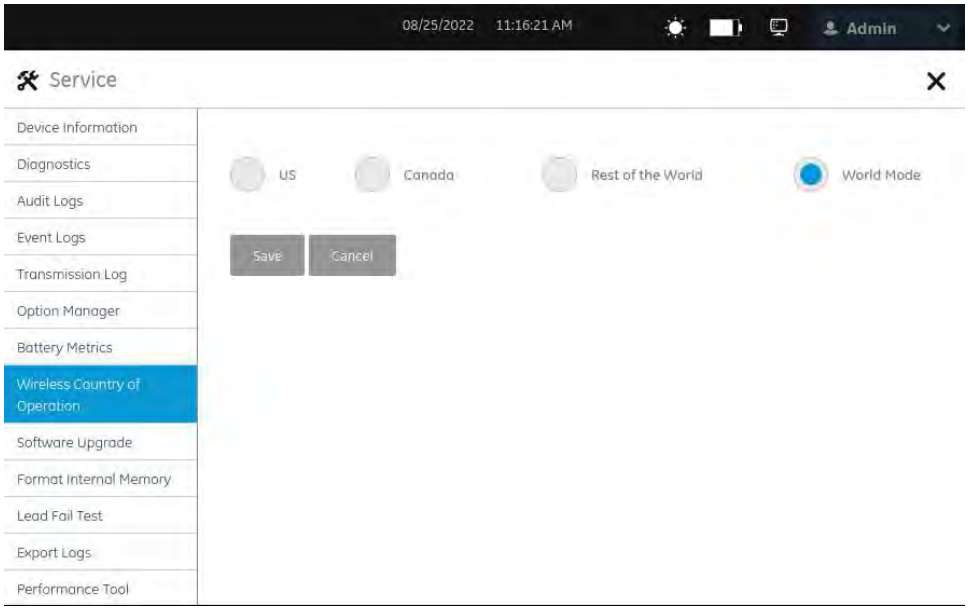
The device ships with configured settings for the Wireless Country of Operation option. You can only edit the country code for the **Rest of the World** setting. If the device is set to **US** or **Canada**, you cannot alter the configuration and the **Wireless Country of Operation** option will not be available in the **Service** menu.

Before you start this procedure:

Disable the Network status option in **Settings** > **Network** > **Wireless Network**. If the WLAN is enabled and you try to configure Wireless, an error message displays: `Disable WLAN to set the Wireless Country of Operation.`

1. Open the **Service** screen.
2. Select **Wireless Country of Operation**.

   The **Rest of the World** screen displays.



3. Configure the country code for the **Rest of the World** wireless option as per the information in the table.

To set Wireless Country of Operation in:	Perform the following steps:
Rest of the World	The **Country of Operation** option displays. 1. Enter a two-character country code in the text field. The list of possible country codes is available at: https://www.iso.org/obp/ui/#search/code/. The allowed values are a to z and A to Z. **NOTE** You cannot enter US and Canada country codes. 2. Select **Save** to save the configuration. The wireless is set as per the country code you select in Step 1 on page 233. If you enter an invalid country code, an error message displays, and the device is set to **00** for World Regulatory Domain. If you do not enter a country code, the device is set to **00** for World Regulatory Domain.

4. Close the screen.

   The **Acquisition** screen displays.

10.8.6 Install Wireless Certificates

Before you start this procedure, make sure that:

- You obtain the required certificates from your IT department and copy them to the root folder of a USB flash drive for installation.

  NOTE

  The client certificate must be signed by the CA that is specified in the CA certificate, and you must install the CA certificate prior to installing the client certificate.

  If the client certificate is self-signed, you need to enable the **Self-signed** setting during the installation process, and the installation of CA certificate is not required. If mutual authentication is needed, you can install the server's public key as the CA certificate.

  The certificate must be self-contained. It cannot point to another certificate.

  Accept only PEM format certificates. Make sure that the certificates are in the right format and you import the correct certificate for each tab.

- You enable:
  - **Enable External USB Storage** in **Settings** > **System** > **Storage** setting.
  - At least one USB port in **Settings** > **Hardware** > **USB Port** setting.

  If these options are not enabled, access to USB flash drives is blocked.

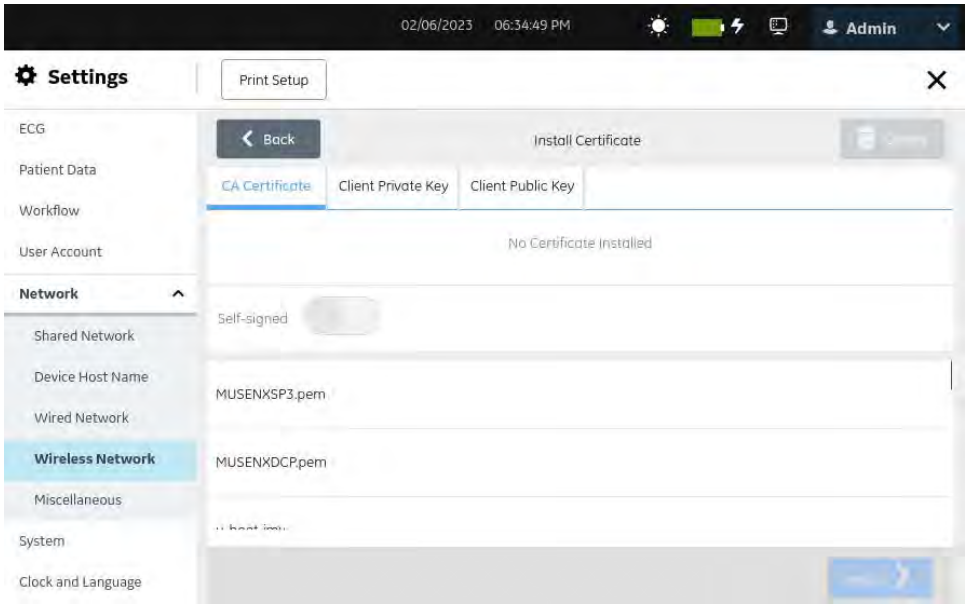
1. Connect the USB flash drive containing the digitally signed CA Certificate, Client Private Key, and Client Public Key to the device.

   NOTE

   If the client certificate is self-signed, a CA Certificate is not required.

2. Select **Settings** > **Network** > **Wireless Network**.
3. In the **Wireless Network** section, select **Install Certificate**.

   The *Install Certificate* screen opens. By default, the **CA Certificate** tab is selected.



4. If the **CA Certificate** setting is on, perform the steps below to install a CA Certificate:

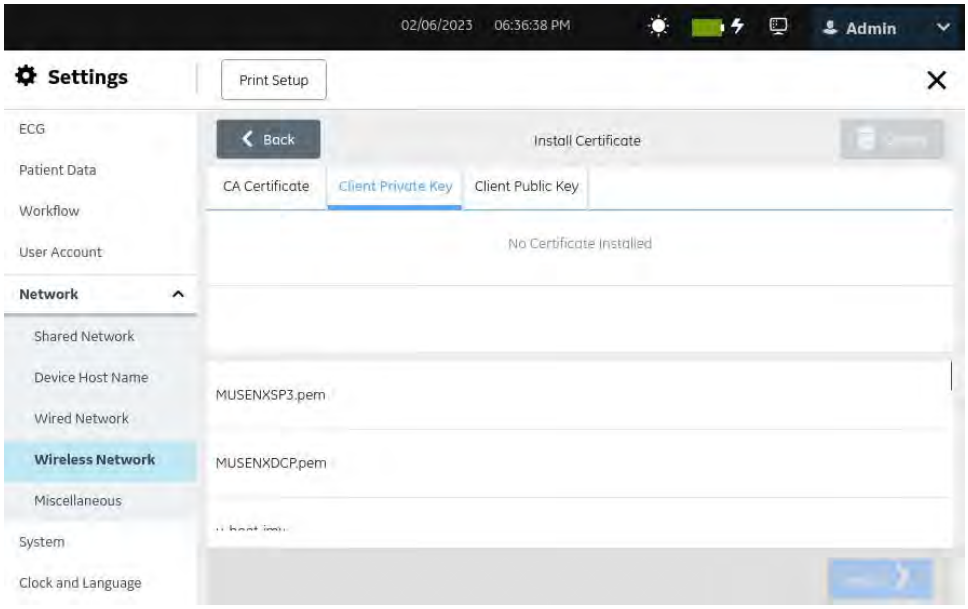
   4.1. Select the CA certificate from the USB flash drive.

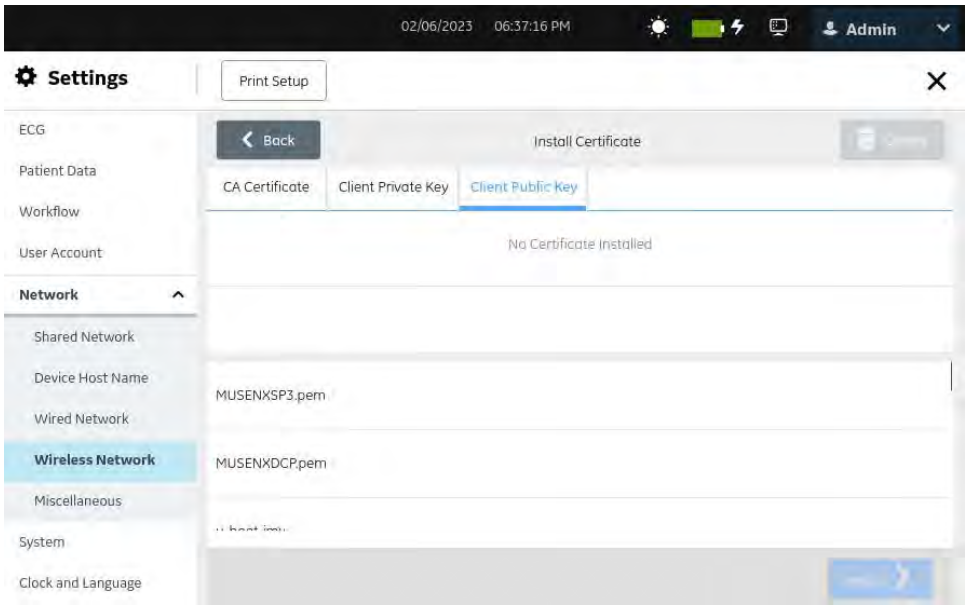
   4.2. Enable the **Self-signed** button.

4.3. Select **Install**.

- If the installation is successful, the **Installed certificate** status displays on the status bar.
- The **Certificate** name, **Issuing Authority**, **Validity Dates**, and **Issuing Subject** details displays in the **Currently Installed Certificate Details** section.
- If the installation fails due to an error, you need to troubleshoot the error. See 13.10 Wireless Network Connectivity Errors on page 283 and 13.9 Errors while Installing Certificates on page 282.

5. If the **Client Private Key** is on for the Client certificate, perform the steps below to install the client private key and client public key:





NOTE

The **Client Private Key** and **Client Public Key** can be in the same certificate.

5.1. Select **Client Private Key**.

5.2. Select a valid client private key from the USB flash drive.

5.3. Enter a valid client private key password in the **Password** field.

5.4. Select **Client Public Key**.

5.5. Select a valid client public key from the USB flash drive.

5.6. Select **Install** to install the selected client private and public keys.

The **Install** button is enabled only after you select client private and public keys.

- If the installation is successful, the **Certificate** name, **Issuing Authority**, **Validity Dates**, and **Issuing Subject** details display in the **Currently Installed Certificate Details** section.
- If the installation fails due to an error, you need to troubleshoot the error. See 13.10 Wireless Network Connectivity Errors on page 283 and 13.9 Errors while Installing Certificates on page 282.

6. Perform the steps below to replace or delete the currently installed CA certificate or client public and private keys:

6.1. Select the tab (**CA Certificate**, **Client Private Key** or **Client Public Key**) where you want to replace or delete the installed certificate or key.

The currently installed certificate or key displays.

6.2. Select **Delete.**

A message displays asking you to confirm the deletion of the certificate or key.

NOTE

If you delete the client private key, the client public key is deleted and vice versa.

6.3. Select **OK**. The certificate or key is deleted.

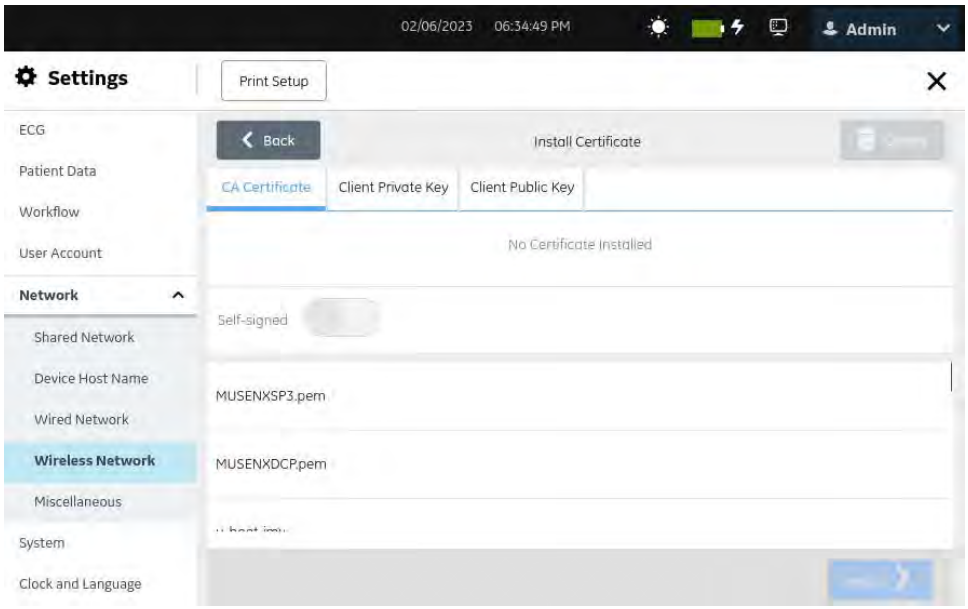
- If you want to replace the CA certificate, perform Step 4.
- If you want to replace the client private and public keys, perform Step 5.

10.8.7 Intermediate Certificates

If your site uses intermediate certificates, you may need to install both the intermediate and the root certificates. Use the steps below to install the intermediate and the root certificates.

1. Select **Settings** > **Network** > **Wireless Network**.
2. In the *Wireless Network* section, select **Install Certificate**.

The *Install Certificate* screen opens. By default, the **CA Certificate** tab is selected.

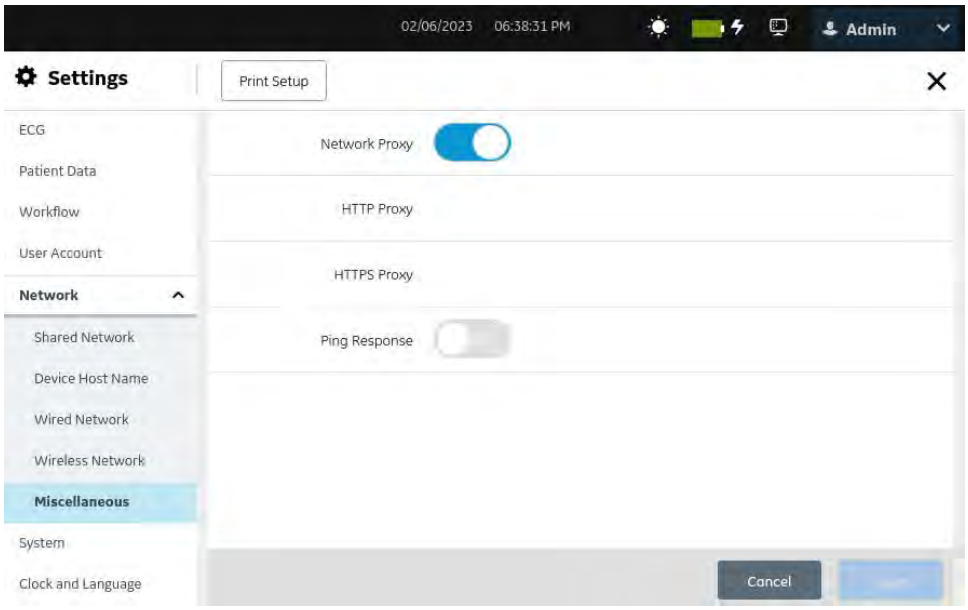


3. If an **Intermediate Certificate** is used, convert the root and intermediate certificates to PEM format.
4. Open the PEM format certificates in a **Notepad** editor.
5. Perform the steps below to create a **Chained CA Certificate**:
   5.1. Concatenate the root and intermediate certificates as explained in the example below.
   5.2. Example, if root signed intermediate1 and intermediate1 signed intermediate2 and intermediate2 signed the client public key, the order of certificates in the Chained CA Certificate file should be: **root->intermediate1->intermediate2**.
6. Install the **Chained CA Certificate** created in Step 5 in the **CA Certificate** tab. See 10.8.6 Install Wireless Certificates on page 233 for more information.

10.8.8 Configure Proxy Settings

1. Select **Settings** > **Network** > **Miscellaneous**.

   The proxy setting screen displays.



2. Configure the proxy settings as per the information in the table.

Table 10-55 Configure Proxy Settings

Field	Action	Description
Network Proxy	Enable or disable this setting.	• If this setting is enabled, the **HTTP Proxy** and **HTTPS Proxy** fields display. You can configure the proxy settings. • If this setting is disabled, the **HTTP Proxy** and **HTTPS Proxy** fields are hidden. You cannot configure proxy settings. Default value: Disabled
HTTP Proxy	Enter the IP address and port number of the HTTP proxy.	Default value: No default value Allowed values: A valid IPV4 address and port number
HTTPS Proxy	Enter the IP address and port number of the HTTPS proxy.	Default value: No default value Allowed values: A valid IPV4 address and port number

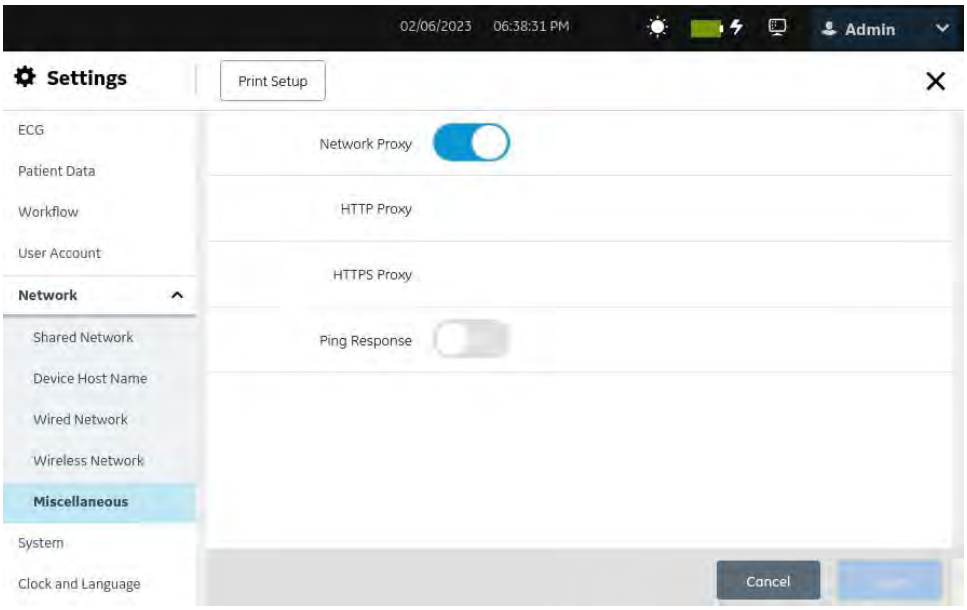
3. Save and close the screen.

   The **Acquisition** screen displays.

10.8.9 Configure Ping Response

1. Select **Settings** > **Network** > **Miscellaneous**.

   The ping response setting screen displays.



2. Configure the ping response setting as per the information in the table.

Field	Action	Description
Ping Response	Enable or disable this setting.	This setting enables/disables a PC pinging device. It tests if a device is available. Default value: Disabled

3. Save and close the screen.

   The **Acquisition** screen displays.

10.8.10 Show Network Connection Status

When the wireless and wired connection is set to **Enable**, the device uses a wired connection when you connect a Local Area Network (LAN) cable. If you remove the LAN cable, the device uses the wireless connection.

To view the status of your device's connection to your LAN or Wireless Local Area Network (WLAN), perform the procedure as follows:

1. Select the **Network Status** icon on the status bar.
2. Review the tables for the description of the network status icon when connected to a LAN or WLAN network.

Table 10-56 LAN Icons

Network Status Icon	Status	Description
	LAN Active	The device is connected to a LAN.

Continues on the next page

Table 10-56 LAN Icons (Table continued)

Network Status Icon	Status	Description
	LAN Connected	The device is connected to a remote server through a LAN and is in the process of obtaining an IP address. If this icon is blinking, the device is acquiring an IP address from DHCP.
	LAN Disconnected	The device is not connected to a LAN; no LAN (Ethernet) cable is attached to the device.

Table 10-57 WLAN Icons

Icon	Status	Description
	WLAN Active	The device is connected to a WLAN and has a valid IP address. The icon shows a number of wireless bars to indicate the strength of the wireless signal.
	WLAN Connected	The device is connected to an access point and is in the process of obtaining an IP address. If this icon is blinking, the device is acquiring an IP address from DHCP.
	WLAN Disconnected	The device is not connected to a WLAN.

For more information about wireless certificate errors, see 13.10 Wireless Network Connectivity Errors on page 283.

3. Close the *Network Status* window by selecting something on the screen outside of the window.

10.9 Configure System

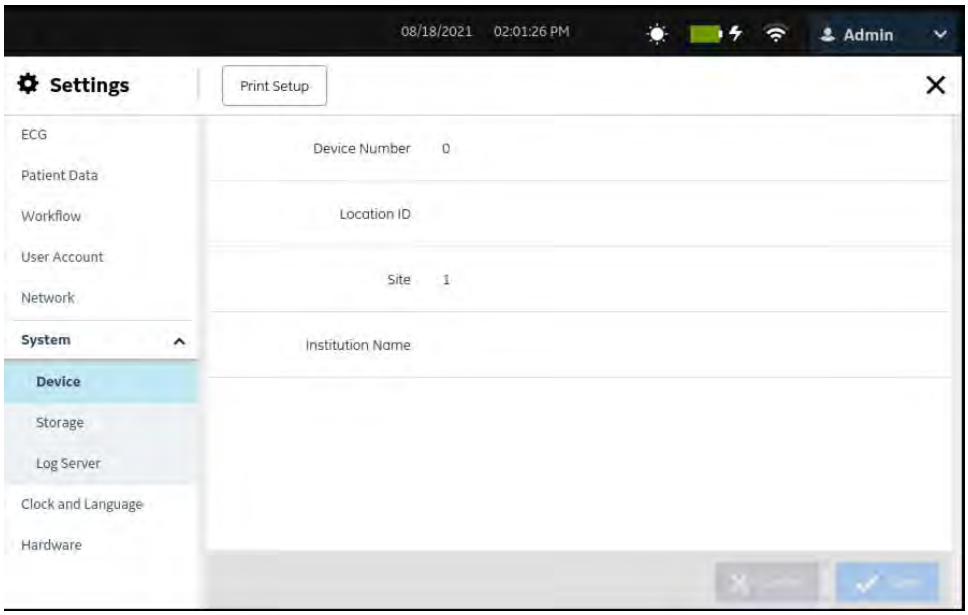
Select **Settings** > **System** menu to configure the settings below:

- Device Parameters - 10.9.1 Configure Device Parameters on page 240
- External Storage - 10.9.2 Configure External Storage on page 241
- Export and Import Configuration Settings - 10.9.3 Export and Import Configuration Settings on page 242
- Import User Settings from release before to V1.01- 10.9.4 Import User Settings from release before to V1.01 on page 248
- Restore to Factory Defaults - 10.9.5 Restore to Factory Defaults on page 250
- Log Server - 10.9.6 Configure Log Server on page 252

10.9.1 Configure Device Parameters

1. Select **Settings** > **System** > **Device**.

   The device parameter setting screen displays.



2. Configure the fields per the information in the below table.

Table 10-58 Device Parameters

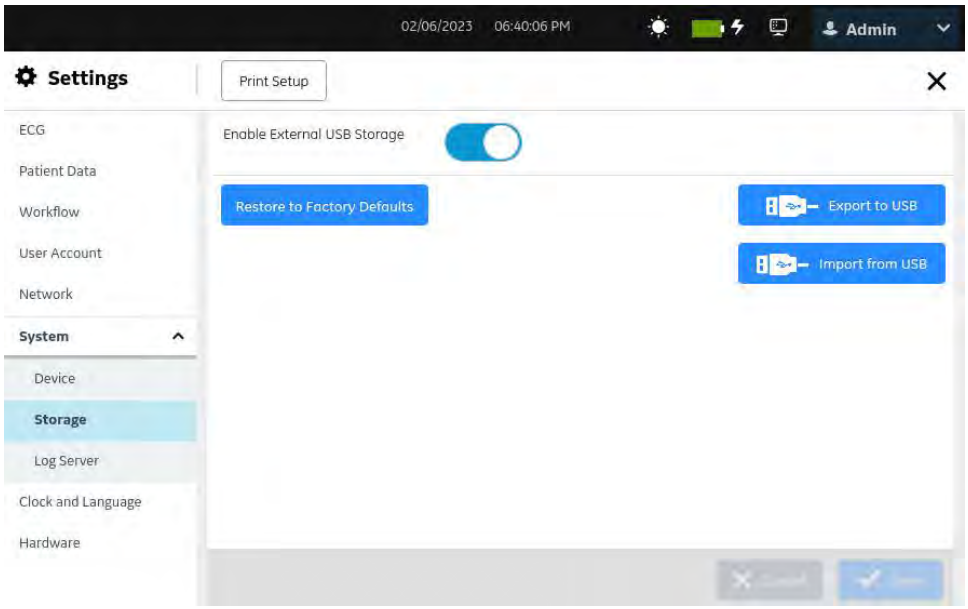
Field	Action	Description
Device Number	Set the default device number.	The device number is unique for each ECG device. Default value: **0** Allowed values: 0 to 65535
Location ID	Set the default location ID.	For each patient test, the location ID is populated in the **Location** field of the **Patient Information** screen. No default value Allowed values: 0 to 65535
Site	Set the site number.	Default value: **1** Allowed values: 1 to 255
Institution Name	Set the name of the institution.	The name of the institution displays in the ECG and rhythm reports. No default value Allowed values: 1 to 25 characters • A to Z • a to z • 0 to 9 • All special characters

3. Select **Save**.

10.9.2 Configure External Storage

1. Select **Settings** > **System** > **Storage**.

   The external storage setting screen displays.



2. Configure the fields as per the information in the table.

Table 10-59 External Storage Settings

Field	Action	Description
Enable External USB Storage	Enable or disable access to USB flash drives for external data storage.	**NOTE** If you try to disable this setting, and a USB destination is already configured as a default or auto-destination, a warning message displays notifying you to change the USB destination to a manual destination to disable the **Enable External USB Storage** setting. See 10.6.2.2 Configure a USB Destination to Transmit Reports on page 160. Default value: Disabled

3. Select **Save**.

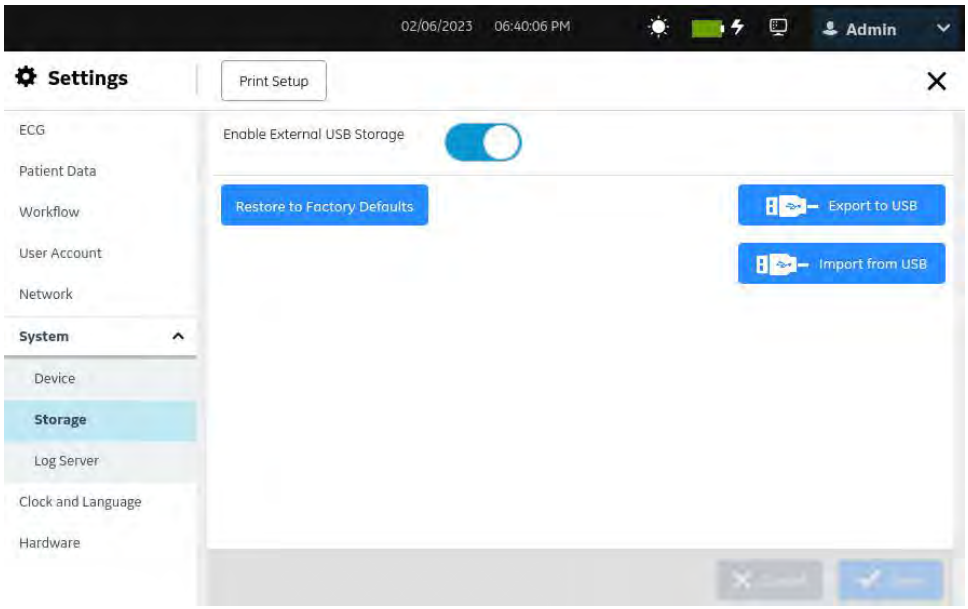
10.9.3 Export and Import Configuration Settings

Before performing this procedure, make sure that:

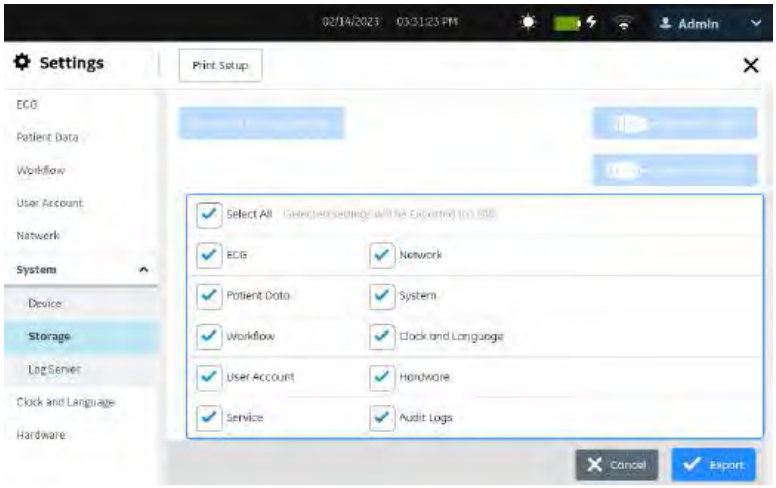
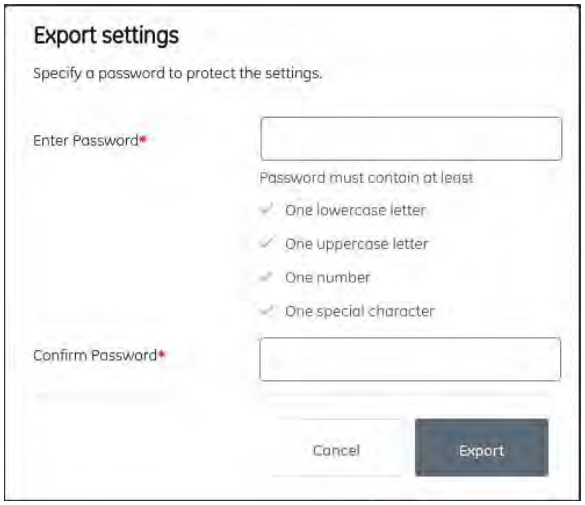
- The USB flash drive is inserted correctly into the drive and has write permissions.
- The **Enable External USB Storage** setting is enabled in the **Settings** > **System** > **Storage**.
- The USB ports are enabled in the **Settings** > **Hardware** > **USB Port**.
- The USB flash drive supports the FAT32 file system.

1. Select **Settings** > **System** > **Storage**.

   The **Storage** setting screen displays.


02/06/2023 06:40:06 PM
Admin
Settings
Print Setup
ECG
Patient Data
Workflow
User Account
Network
System
Device
Storage
Log Server
Clock and Language
Hardware
Enable External USB Storage
Restore to Factory Defaults
Export to USB
Import from USB

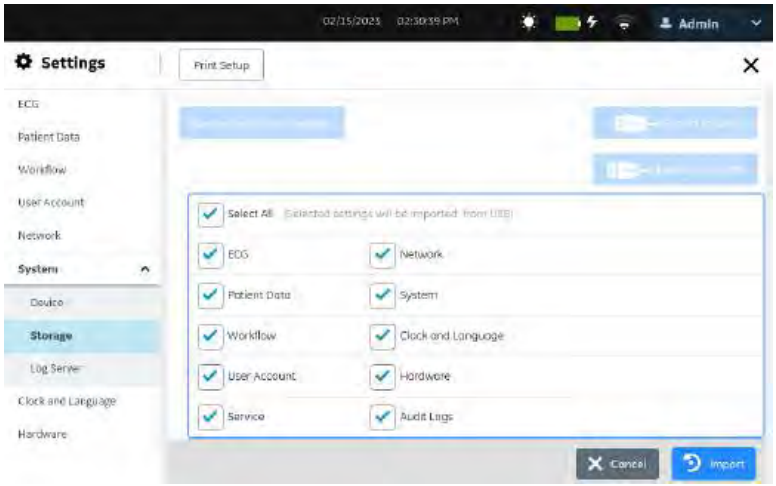
2. Do the steps in the table.

If you want to...	Then...
Export the configuration settings to a USB flash drive	1. Select **Export to USB**. A message displays indicating that the selected settings will be saved to an external USB storage. 2. Select the **Select All** check box or select specific check boxes to export the required settings to the USB flash drive.  3. Select **Export**. The password confirmation window displays.  **NOTE** • The password characters display with asterisks. The **Show** and **Hide** buttons enable/disable you to view the entered password or confirmed password field text. • Enter a password which meets the password requirements that display in the confirmation window. Type again the same password to confirm the **Password** field. • The **Export** button enables, if you use the same passwords.

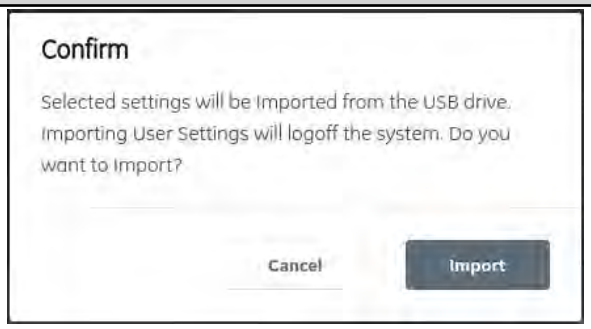
Continues on the next page

If you want to...	Then...
	• Select the **Cancel** button to stop the export of the configuration settings. • The device does not authenticate for duplicate passwords. You can use the same password for any number of exports. The configuration file is exported to the root directory of the USB flash drive in encrypted format, and a confirmation message displays. The configuration file name follows the format: `<product name>_<serial number>.cfg`. If a previously exported file exists, a message displays asking you to confirm overwriting the existing file. Select **Export** to overwrite the file, or insert another USB flash drive to export the file. 4. Remove the USB flash drive and store it carefully for future use.

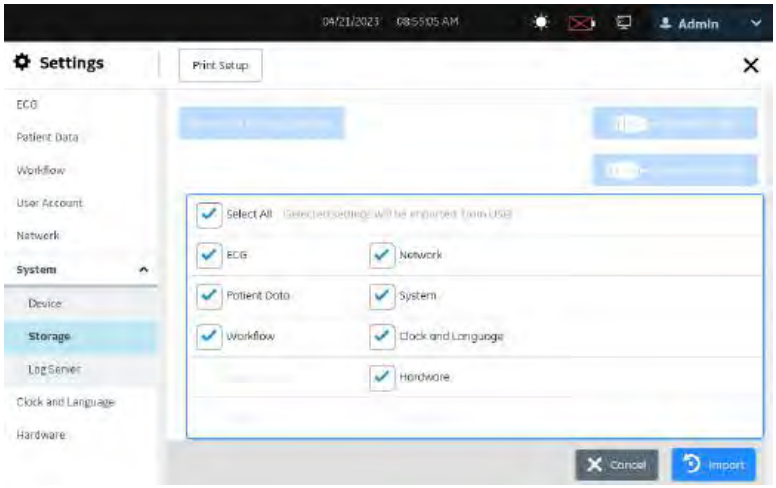
Continues on the next page

If you want to...	Then...
Import the configuration settings from a USB flash drive for release 1.01 or higher.	**NOTE** • You can import configuration settings only if you have exported the settings previously to the USB flash drive. • You can import configuration settings from **.cfg**. 1. Select **Import from USB**. 2. Select the **.cfg** configuration file and press **Import** to proceed. 3. If a configuration file exported from a software version 1.01 or higher is selected, a password confirmation window displays. Continue with 4. If a **.usrcfg** or configuration file exported from a software version lesser than 1.01 is selected, a password confiramtion window does not display. Continue with 5. 4. Enter the same password previously you use to export the configuration file and select **Import** to confirm the action.  5. List of selected settings display. Select specific check boxes to import the required settings from the USB flash drive.  **NOTE** • The **User Account** settings does not display if you do not have the user management privilege. • The **Audit Logs** settings does not display if you do not have the **Access Audit Logs** privilege. • The **Service** settings and **Audit Logs** settings does not display if you do not have the **Access Service** privilege. 6. Select **Import** to confirm the action.

Continues on the next page

If you want to...	Then...
	 The settings are successfully imported from the selected file in the USB flash drive. If user settings are selected, the system logs off.

Continues on the next page

If you want to...	Then...
Import the configuration settings from a USB flash drive for release before to 1.01.	**NOTE** • You can import the configuration settings only if you have exported the settings previously to the USB flash drive. • You can import configuration settings from **.cfg**. 1. Select **Import from USB**. 2. Select the **.cfg** configuration file and press **Import** to proceed. 3. List of selected settings display. Select specific check boxes to import the required settings from the USB flash drive.  **NOTE** When you import the configuration file from a USB flash drive for release before to 1.01, the **User Account**, **Audit Logs**, and **Service** settings are disabled. 4. Select **Import** to confirm the action.  The settings are successfully imported from the selected file in the USB flash drive.

If there are problems with the USB flash drive or the configuration file, the configuration is not successfully exported or imported.

To resolve errors related to the configuration file, see 13.5 Configuration File Errors on page 279.

To resolve errors related to the USB flash drive, see 13.6 USB Flash Drive Errors on page 279.

10.9.4 Import User Settings from release before to V1.01

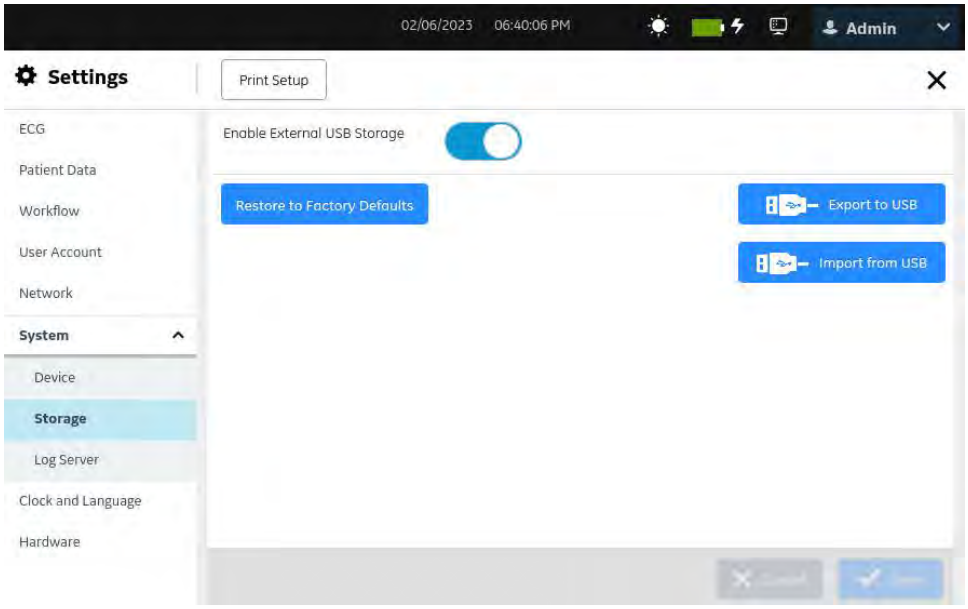
Before you start this procedure, make sure that:

- The **Enable External USB Storage** setting is enabled in **Settings** > **System** > **Storage**.

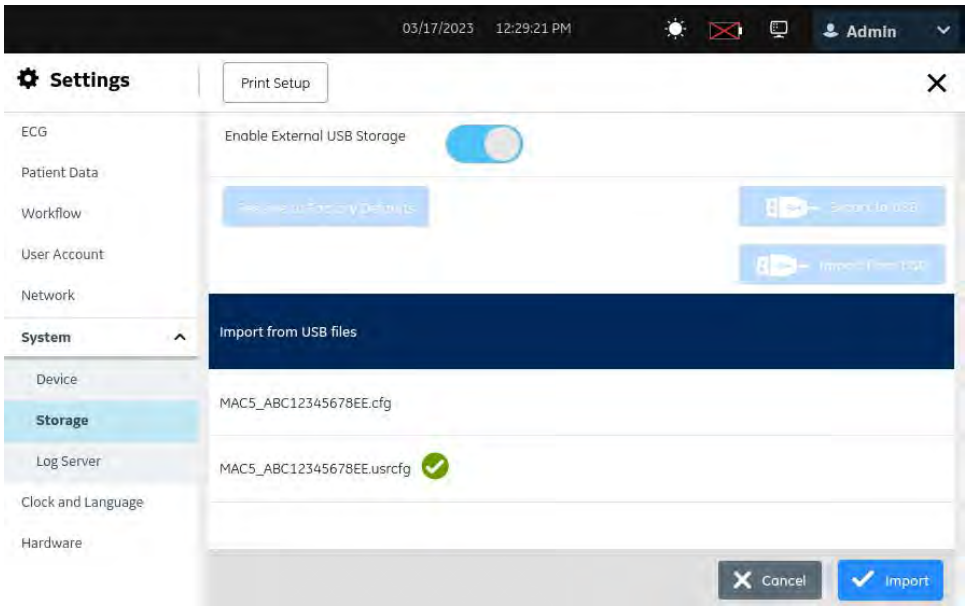
- The USB ports enabled in **Settings** > **Hardware** > **USB Port**.
- Correctly insert a USB flash drive with write permissions into the device. You can only insert one USB flash drive to save user settings.
- The USB flash drive supports the FAT32 file system.
- Your user role is assigned the user account privilege to import user account settings.

1. Select **Settings** > **System** > **Storage**.

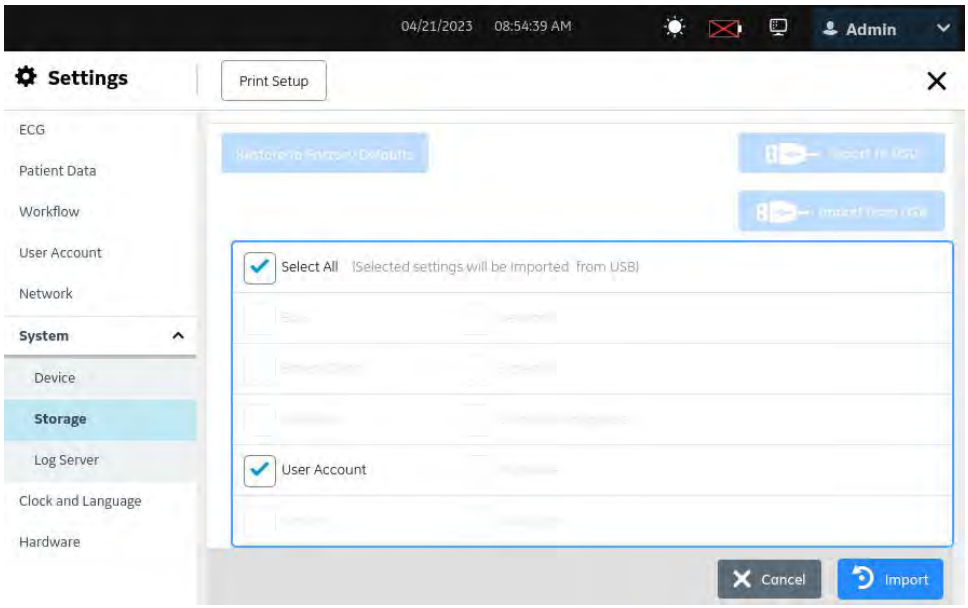
   The **Storage** setting screen displays.



2. Select **Import from USB**.
3. Select the **.usrcfg** file with the correct *Serial Number* of the device and press **OK**.



4. Select **User Account** settings to be imported from external storage and press **Import**.



5. Select **Import** to confirm to import the user settings from USB.

The user settings are successfully imported from the selected file in the USB flash drive, and the system logs off.

If there are problems with the USB flash drive or the user configuration file, the configuration is not successfully exported or imported.

To resolve errors related to the user configuration file, see 13.5 Configuration File Errors on page 279.

To resolve errors related to the USB flash drive, see 13.6 USB Flash Drive Errors on page 279.

10.9.5 Restore to Factory Defaults

NOTE

A **System Reset** is used to delete all data including patient data and settings. The system is reset to factory defaults and the default password for the admin user can be used to log in. It retains the previously enabled option codes, serial number, MAC address, thermal printer, and Wireless Country of Operation configuration.

A **Restore to Factory Defaults** is used to reset the settings or section of settings.

- Make sure that you have backed up the current configuration settings, before you reset the settings to factory defaults. See 10.9.3 Export and Import Configuration Settings on page 242 to back up the current configuration settings.

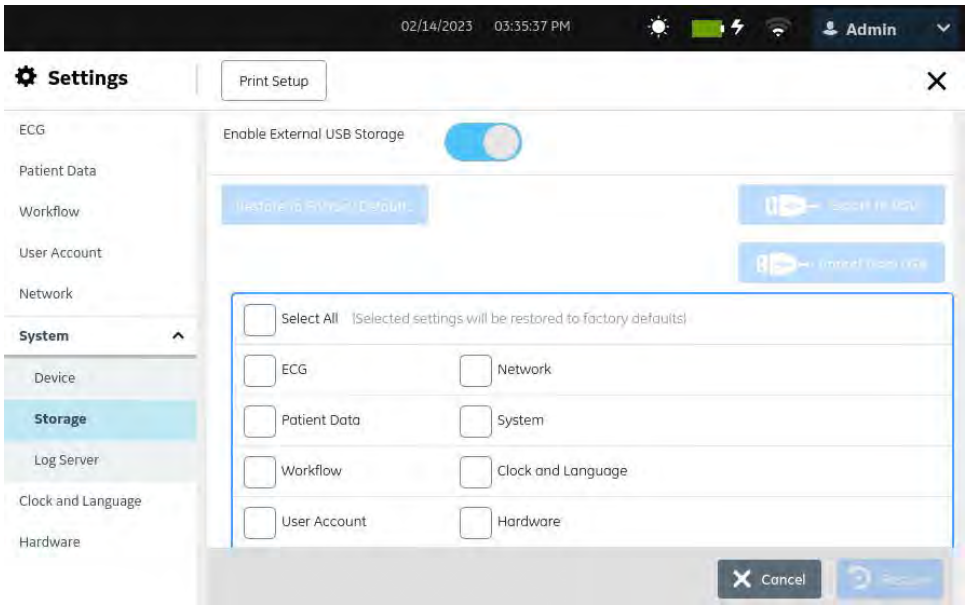
If you do not save the current configuration settings prior to restore the settings to factory defaults, you do not have the option of restoring the current settings later. You need to manually re-configure the settings.

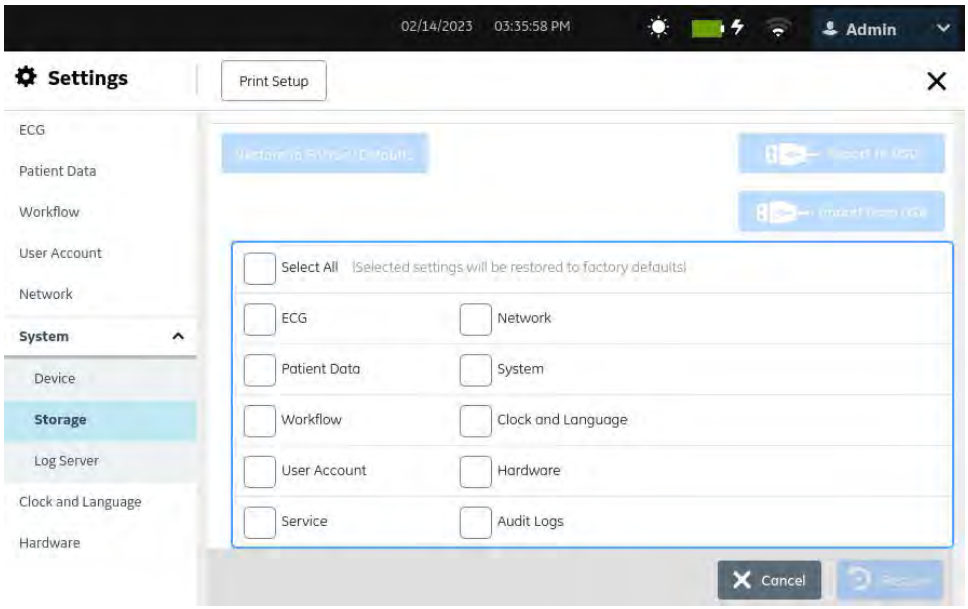
- Make sure that your user role is assigned the privileges to access the **Settings** screen.

NOTE

The enabled options are not reset when the device is reset to factory default settings.

1. Select **Settings** > **System** > **Storage**.
2. Select **Restore to Factory Defaults**.





3. Perform one of the steps below:
   - If you want to restore all the settings to factory defaults, select **Select All**.

- If you only want to restore several specific settings to factory defaults, select the check boxes beside those settings.

4. Select **Restore**.

   A confirmation message displays: **Selected configurations will be reset to default values. Resetting User Settings will logoff the system. Do you want to continue?**

5. Perform one of the steps below:
   - Select **Restore** to confirm the action.
   - Select **Cancel** to cancel the action.
   - If you select all the settings and click **Restore**, all the selected settings are restored to default values and the Acquisition screen displays.
   - If you select a specified settings and click **Restore**, the selected settings are restored to default values. Close the screen to view the Acquisition screen.

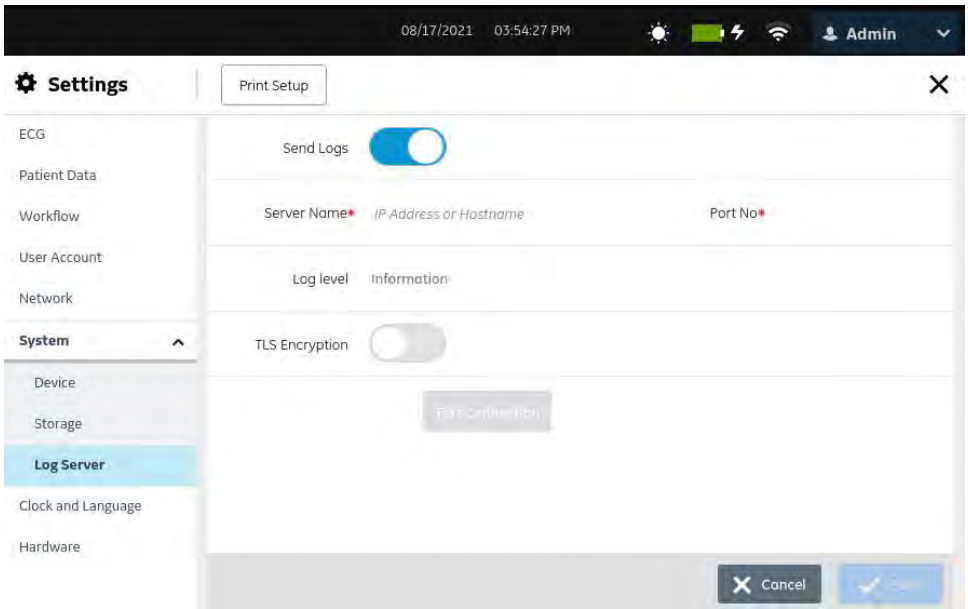
10.9.6 Configure Log Server

Before you start this procedure, make sure that:

- You have access to the **Settings** screen.
- You obtain the required certificate in the PEM format from your IT department and copy it to the root folder of a USB flash drive for installation.
- The **Enable External USB Storage** is enabled in **Settings** > **System** > **Storage** setting. If this setting is not enabled, access to USB flash drives is blocked.
- You enable at least one USB port in **Settings** > **Hardware** > **USB Port** setting. If this setting is not enabled, the device will not recognize the USB flash drives.

1. Connect the USB flash drive that contains the TLS certificate to the device.
2. Select **Settings** > **System** > **Log Server**.

   The log server setting screen displays.



3. Configure the **Log Server** per the information in the below table:

Field	Action	Description
Send Logs	Enable or disable this setting.	If this setting is enabled, the device transmits the captured system logs and event logs to the configured server location. Default value: Disabled
Server Name	Enter IP address of the configured log server.	Allowed values: A valid IP address Default value: *IP Address or Hostname* If you enter an invalid IP address, the outline of IP Address field turns red.
Port No	Enter a valid port number of the configured log server.	Allowed values: 1 to 65535 No default value.
Log level	From the drop-down menu, select the desired Log level.	Default value: Information Allowed values: • Information • Warning • Error • Critical The information related to selected **Log level** type is transmitted to configured server.
TLS Encryption	Enable or disable this setting.	If this setting is enabled, the connection to the configured server is encrypted. If this setting is disabled, the connection to the configured server is not encrypted. Default value: Disabled

4. If TLS Encryption is enabled, the **Install Certificate** field displays, do the steps that follow to install the TLS certificate:

   4.1. Select **Browse**.

   The **Certificate - Browse** window opens and displays the message: `No Certificate Installed`

   4.2. Select the valid certificate from the list.

   4.3. Select **Install**. A success message displays.

   4.4. Select **Back**.

   The **Log Server** window displays. The **Installed** message is shown in the **Install Certificate** field.

5. Select **Test Connection** to test the connection to the configured server.

   NOTE

   The maximum time to complete the test connection for **TLS Encryption** is 60 seconds.

   - If the connection is successful, a success message displays and the **Save** button is enabled.
   - If the connection fails due to an error, an error message displays. Troubleshoot the error and select **Test connection**.

6. Select **Save**, a success message displays.

7. Close the screen.

   The Acquisition screen displays.

10.9.7 Delete TLS Encryption Certificate

Before you start this procedure, make sure that your user role is assigned with user management privilege.

1. Select **Settings** > **System** > **Log Server**.

   The log server setting screen displays.

2. Enable **Log Server** setting.
3. Perform the steps below to delete the currently installed TLS Encryption certificate:

   3.1. Select the **Browse** setting.

   The currently installed certificate displays.

   3.2. Select **Delete**.

   A message displays asking you to confirm the deletion of the certificate.

   3.3. Select **Yes**. The certificate is deleted.

10.10 Configure the Clock and Language

Select **Settings** > **Clock and Language** menu to configure the settings below:

- Date and Time - 10.10.1 Configure the Date and Time on page 254
- NTP - 10.10.2 Configure NTP on page 257
- Region - 10.10.3 Configure Region on page 258

10.10.1 Configure the Date and Time

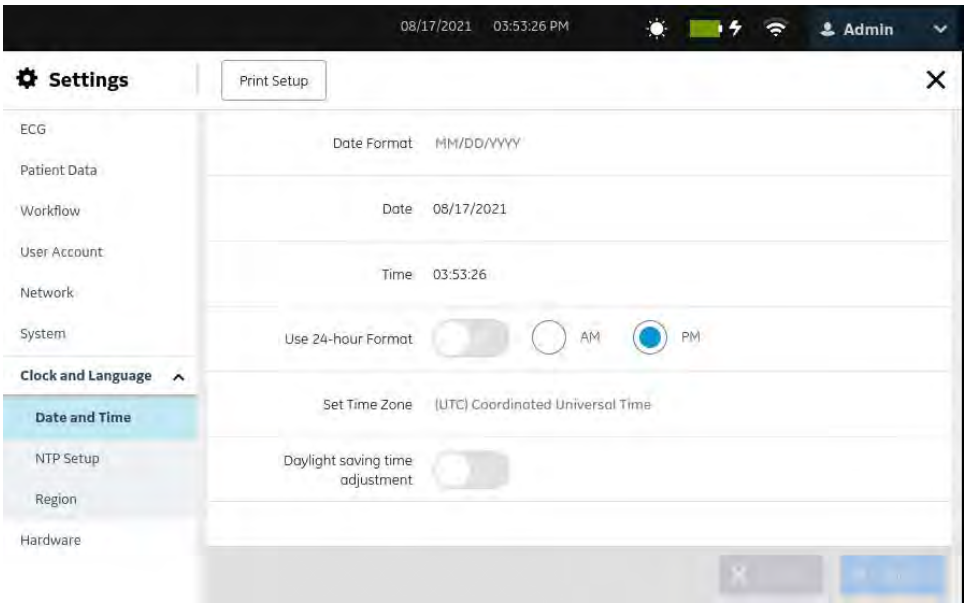
The items below are set by GE Healthcare before the device is shipped.

- Date and time formats based on the customer’s country preferences
- The default time zone (GMT/UTC)

Use this procedure if you want to change the default date and time configurations.

1. Select **Settings** > **Clock and Language** > **Date and Time**.

   The date and time setting screen displays.



2. Configure the fields per the information in the below table.

Table 10-60 Date and Time Settings

Field	Action	Description
Date Format	Select the date format.	The date format is automatically set to the specified country values when you change the device language and after you perform restore to factory default settings: • **DD.MM.YYYY** when the device language is set as **Finnish**, **Portuguese**, **Russian**, **Spanish**, or **Turkish**, or **Czech** and the device is restored to factory defaults settings. • **MM/DD/YYYY** when the device language is set as **English**, **Brazilian Portuguese**, or **Polish**, and the device is restored to factory defaults settings. • **YYYY-MM-DD** when the device languages are set as **Chinese**, **Danish**, **German**, **Swedish**, **Norwegian**, **Japanese** or **Korean**, and the device is restored to factory defaults settings: • **DD-MM-YYYY** when the device languages are set as **Dutch** or **French**, and the device is restored to factory defaults settings: • **DD/MM/YYYY** when the device language is set as **Italian**, and the device is restored to factory defaults settings. where: • MM = the number of the month. For example, January is 01. • DD = the number of the day of the month. • YYYY = the year Default value: Date format set at factory

Continues on the next page

Table 10-60 Date and Time Settings (Table continued)

Field	Action	Description
Date	Click anywhere on the **Date** field to populate the *Calendar*. Select the date from the Calendar. Select **Save**. If you select **Cancel**, the calendar closes and your changes are not applied. The **Restore to Factory Defaults** procedure does not change the date. Default value: Date set at factory	
Time	Enter the current time.	• If the **Use 24-hour Format** setting is disabled, you can configure the hour from 1 to 12 and set **AM** or **PM**. • If the **Use 24-hour Format** setting is enabled, you can configure the hour from 0 to 23 with no selection for **AM** or **PM**. The **Restore to Factory Defaults** procedure does not change the time format. Default value: Time set at factory Allowed values: HH:MM:SS, where: • HH = hour • MM = minutes • SS = seconds
AM or **PM**	Enable or disable this setting.	If the **Use 24-hour Format** setting is disabled, select **AM** or **PM**. This setting is not available if the **Use 24-hour Format** is enabled. This setting is automatically enabled when the device language is set as **English** or **Polish**, and the device is restored to factory defaults settings.
Use 24-hour Format	Configure the time format for the device.	• If this setting is disabled, you can configure the hour from 1 to 12 and set **AM** or **PM**. • If this setting is enabled, you can configure the hour from 0 to 23 with no selection for **AM** or **PM**. This setting is automatically enabled when the device language is set as **Chinese**, **Danish**, **Dutch**, **Finnish**, **French**, **German**, **Italian**, **Swedish**, **Japanese**, **Korean**, **Czech**, **Portuguese**, **Russian**, **Spanish**, **Brazilian Portuguese**, **Turkish**, or **Norwegian**, and the device is restored to factory defaults settings. This setting is automatically disabled when the device language is set as **English** or **Polish**, and the device is restored to factory defaults settings.
Set Time Zone	Select the time zone for the device.	Default value: UTC (Coordinated Universal Time) Allowed values: List of time zones representing all areas of the world.
Daylight saving time adjustment	Enable or disable this setting to automatically adjust the time for daylight savings time according to the selected time zone.	Default value: Disabled

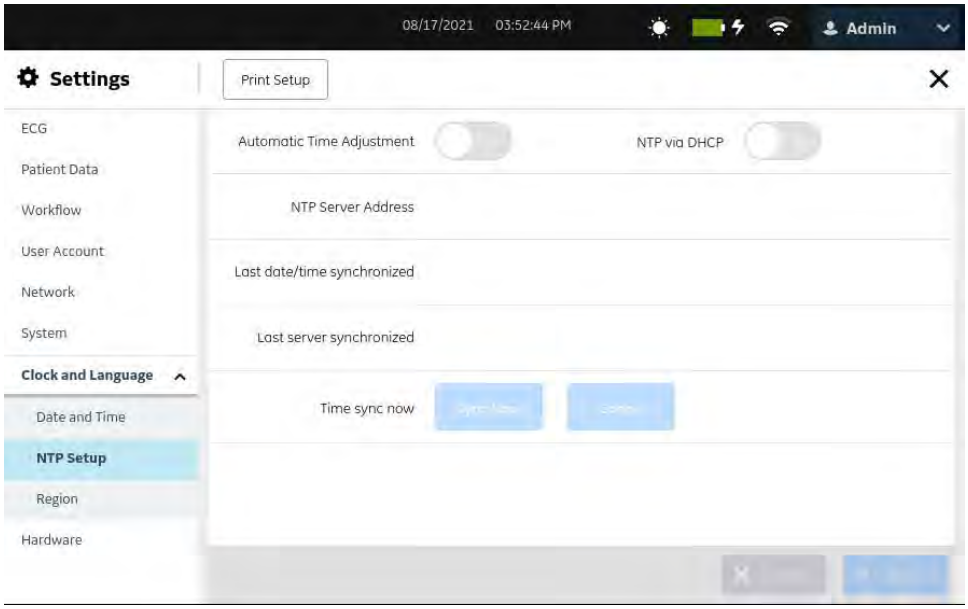
3. Select **Save**.

10.10.2 Configure NTP

Network Time Protocol (NTP) is a networking protocol used for clock synchronization between the device and the configured NTP server.

1. Select **Settings** > **Clock and Language** > **NTP Setup**.

   The NTP setting screen displays.



2. Configure the fields per the information in the below table.

Table 10-61 NTP Setup

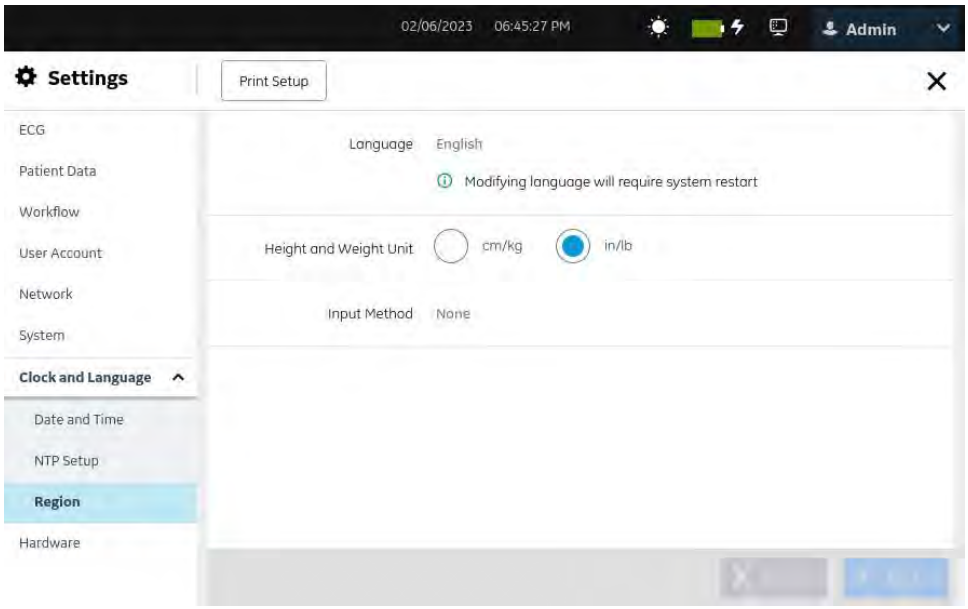
Field	Action	Description
Automatic Time Adjustment	Enable or disable this setting.	The current date and time is automatically synchronized with an NTP server. If this setting is disabled, the **NTP via DHCP** is also disabled. Default value: Disabled
NTP via DHCP	Enable or disable this setting.	If this setting is enabled, the device receives the NTP server configuration through DHCP. Default value: Disabled
NTP Server Address	Enter the IP address of the NTP server that synchronizes the current date and time on the device.	Default value: No default value Allowed values : A valid IP address
Last date/time synchronized	Displays the date and time when the device was last synchronized with the NTP server.	
Last server synchronized	Displays the IP address or URL of the NTP server that synchronized the current date and time of the device.	
Time sync now	Select **Sync Now** to synchronize the date and time on the device with the date and time on the NTP server.	

3. Select **Save**.

10.10.3 Configure Region

1. Select **Settings** > **Clock and Language** > **Region**.

   The region setting screen displays.



2. Configure the fields as per the information in the table.

Table 10-62 Region Settings

Field	Action	Description
Language	Set the default language of the device.	Default value: **English** Allowed values: List of supported languages When you change the language, you need to restart the system to apply the changes.

Continues on the next page

Table 10-62 Region Settings (Table continued)

Field	Action	Description
Height and Weight Unit	Select the height and weight unit of measurement to be used on the device.	The configured unit of measurement is applied in the **Patient Information** screen and the ECG patient reports. The unit of measurement is automatically set to **in/lb** when you change the device language and after you perform restore to factory default settings: • English • Chinese • Finnish The unit of measurement is automatically set to **cm/kg** when you change the device language and after you perform restore to factory default settings: • Czech • Danish • Dutch • French • German • Italian • Japanese • Korean • Swedish • Norwegian • Portuguese • Russian • Spanish • Brazilian Portuguese • Polish • Turkish
Input Method	Select a value from the drop-down list to configure input method editor for the device.	• If you select **Chinese-Pinyin**, the input method is available to the user to enter Simplified Chinese text. • If you select **Korean Input Method**, the input method is available to the user to enter the Korean text. • If you select **Japanese Input Method**, the input method is available to the user to enter **Hiragana** or **Katakana** Japanese text. • If you select **None**, no input method is available to the user. Default value: **None**

3. Select **Save**.

10.11 Configure Hardware

Select **Settings** > **Hardware** menu to configure the below settings:

- Barcode - 10.11.1 Configure the Barcode on page 260
- USB Ports - 10.11.2 Configure the USB Ports on page 260
- Keyboard Tone and KISS Pump - 10.11.3 Configure Keyboard Tone and KISS Pump on page 261

- Standby Modes - 10.11.4 Configure Standby Modes on page 261

10.11.1 Configure the Barcode

NOTE

The device is compatible with the MAC 5 external barcode reader, which supports reading barcodes containing the symbologies below for all supported languages:

- Code-128
- PDF417
- Code 39
- Interleaved Code 2 of 5
- Data Matrix symbology for characters A-Z (upper case), a-z (lower case), and 0-9

If you are using an external barcode reader, make sure that the barcode reader is connected to this device and the **BRCD - External Barcode Reader** option is enabled to test the barcode configuration. Before configuring the barcode, perform the Barcode Diagnostics Test described in the *MAC™ 5 Resting ECG Analysis System Service Manual* to make sure that the barcode reader is functioning properly.

10.11.2 Configure the USB Ports

1. Select **Settings** > **Hardware** > **USB Port**.

   The USB port setting screen displays.

2. Configure the fields per the information in the below table.

Table 10-63 Configure USB Ports

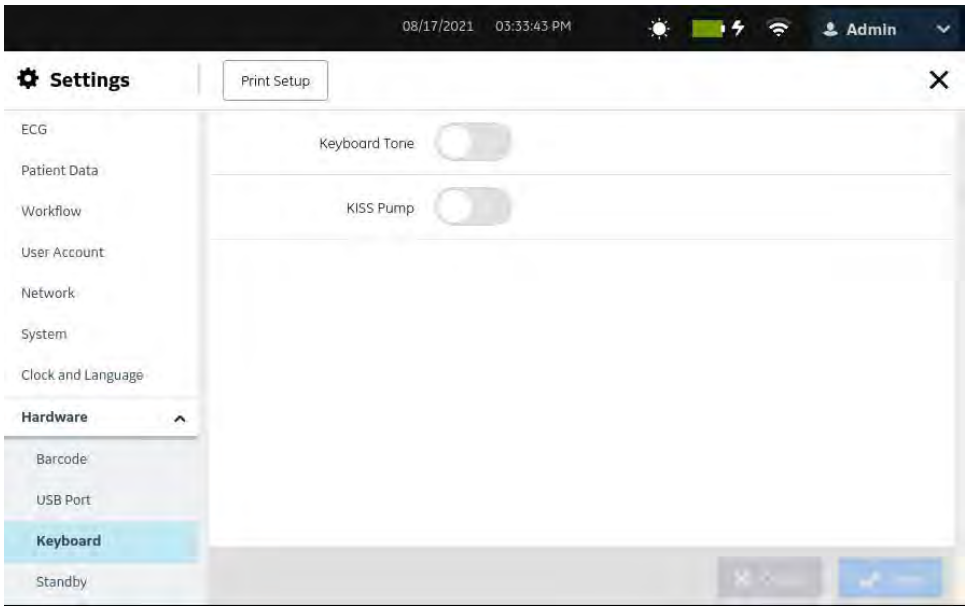
Field	Action	Description
Port A **Port B**	Enable or disable for each USB port.	Default value: Disabled

3. Select **Save**.

10.11.3 Configure Keyboard Tone and KISS Pump

1. Select **Settings** > **Hardware** > **Keyboard**.

   The keyboard setting screen displays.



2. Configure the fields per the information in the below table.

Table 10-64 Configure Keyboard Tone and KISS Pump

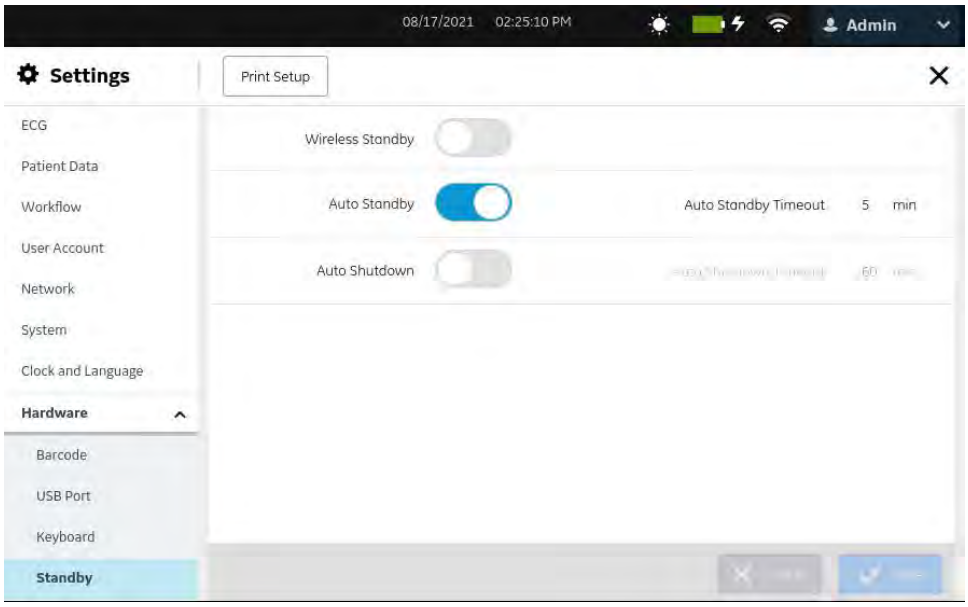
Field	Action	Description
Keyboard Tone	Enable or disable the keyboard tone.	Default value: Disabled
KISS Pump	Enable or disable this setting.	If this setting is enabled, the power supply to the KISS pump is enabled. If this setting is disabled, the power supply to the KISS pump is disabled. Default value: Disabled

3. Select **Save**.

10.11.4 Configure Standby Modes

1. Select **Settings** > **Hardware** > **Standby**.

   The standby setting screen displays.



2. Configure the fields per the information in the below table.

Table 10-65 Configure Standby Modes

Field	Action	Description
Wireless Standby	Enable or disable this setting.	If this setting is enabled: • The wireless connection is put in standby when the device is in standby mode. • The wireless connection is restored to its previous state when the device wakes up. Default value: Disabled
Auto Standby	Enable or disable this setting.	If this setting is enabled, the device is automatically put on standby after a configured duration of inactivity. Default value: Enabled
Auto Standby Timeout (min)	Enter the duration of inactivity, in minutes.	This field is enabled when the **Auto Standby** setting is enabled. After this duration of inactivity, the device is automatically put on standby. Default value: **15** Allowed values: 5 to 120
Auto Shutdown	Enable or disable this setting.	If this setting is enabled, the device is automatically shutdown after a configured duration of inactivity. Default value: Disabled
Auto Shutdown Timeout (min)	Enter the duration of inactivity, in minutes.	This field is enabled when the **Auto Shutdown** setting is enabled. After this duration of inactivity, the device is automatically shut-down. The shutdown timeout duration must be greater than the standby timeout duration. Default value: **60** Allowed values: 5 to 120

3. Select **Save**.

11 Maintenance

11.1 Store Thermal Paper

When imaged and stored properly, ECG tracings resist fading for several years. If your retention requirements exceed five years, consider using GE Archivist paper.

To make sure the tracing is imaged properly, the device must be maintained in accordance with its service and technical manuals.

To make sure the tracing lasts for the paper's expected life span, observe these guidelines when storing your printouts:

- Store in a cool, dark, and dry location.
  - Standard paper

    Temperature must be less than 27°C (80°F).

    Relative humidity must be less than 65%.
  - Archivist paper

    Temperature must be less than 40°C (104°F).

    Relative humidity must be between 40% and 60%.
- Avoid exposure to bright light or UV sources.

  Sources of ultraviolet light include sunlight, fluorescent lights, halogen lights, mercury vapor lamps, and germicidal lamps.
- Avoid contact with cleaning liquids and solvents.

  Solvents to avoid include alcohols, ketones, esters, ether, and so forth.
- Store thermal paper separately in manila folders or polyester or polyimide protectors.

  Plastic document protectors, envelopes, or sheet separators made of polystyrene, polypropylene, or polyethylene do not degrade thermal traces. However, these materials afford no protection against fading from external causes.
- Do NOT store thermal papers with any of the cases below:
  - carbon or carbonless forms
  - document protectors, envelopes, and sheet separators containing polyvinyl chloride or other vinyl chlorides

    non-thermal chart papers or any other products containing tributyl phosphate, dibutyl phthalate, or any other organic solvents

    NOTE

    Many medical and industrial charts contain these chemicals.
- NOT use mounting forms, pressure-sensitive tapes, and labels that use solvent- based adhesives.

  Use only mounting forms and pressure-sensitive tapes made with starch or water- based adhesives.

11.2 Clean the Printhead

If the printer does not operate, you may need to clean the dust and unwanted particles from the printhead.

Use below procedure to clean the printhead:

1. Dip cotton swabs in ethyl alcohol and wring out the excess solution.

   NOTE

   Do not use products that can harm the heating element, such as sandpaper.

2. Open the printer door.
3. Gently wipe the heating element with the cotton swabs.

   NOTE

   - The printhead gets hot when recording. Do not touch the thermal printhead directly.
   - Avoid unnecessary force when handling the printhead.

4. Re-insert the paper and close the printer door when the heating element is completely dry.

   NOTE

   Use only original GE Healthcare writer paper. This paper has a special coating that prevents electrostatic buildup and contamination and debris collection on the printhead. Using other paper may result in recordings of poor quality. Use of other papers may wear out the printhead prematurely and may void the warranty.

11.3 Charge the Battery

You must charge the battery before initial use and in between acquisitions.

- To make sure a fully charged battery before initial use, charge the device before you use it for the first time.
- To make sure a fully charged battery in between acquisitions, power off the system and connect it to an AC wall outlet until you use the system again. This prolongs battery runtime.

The battery status indicator in the upper-right corner of the Acquisition screen shows how much charge the battery has available, and when the device is charging the battery. For more information on the battery status indicator, see 1.5 Battery Status on page 20.

- When the battery is charging, the color of the battery status indicator on the screen is green. The battery LED on the keyboard flashes the amber light at two-second intervals.
- When the battery is low or critically low, the color of the battery status indicator on the screen is red. If the total charge level drops below 15%, an error tone notifies you and a message displays indicating that the battery is low. If the total charge level drops below 10%, the error tone is louder, longer, and sounds every minute, and a message displays indicating that the battery is critically low and you should connect to AC power immediately. The battery LED on the keyboard flashes the amber light at half-second intervals.
- When the battery is completely discharged, the device powers off. To operate your device, you must connect the system to an AC wall outlet. The battery LED on the keyboard turns off.

- If the battery is fully charged or exceeds safe charging temperature, the device will not charge the battery. The color of the battery status indicator on the screen is:
  - Green, if the device is connected to AC power.
  - White, if the device is not connected to AC power.

  The battery LED on the keyboard turns off.

1. Power off the device.
2. Connect the system to an AC wall outlet.
3. Charge the battery for 3 hours or until the battery status indicator displays a full charge.

11.4 Replace the Battery

NOTICE

BATTERY PACK DISPOSAL

Do not dispose of the battery pack by fire or burning. Follow local environmental guidelines concerning disposal and recycling.

1. Place your thumb on the door release tab of the battery compartment door and gently pull it open.

MAC 5 A4

MAC 5 A5

MAC 5 Lite

2. Press the latch beside the battery slot and pull the battery handle in horizontal direction to remove the battery.

MAC 5 A4

MAC 5 A5

Continues on the next page

MAC 5 Lite

3. Insert the new battery. See 2.1 Insert the Battery on page 23.

12 Cleaning and Disinfection

- Do not disassemble and reassemble the device during the cleaning and disinfection process.
- No special accessories are required.

12.1 Inspect the Device

Carefully inspect devices between uses to verify proper function.

Evidence of damage and wear on a device may include but is not limited to discoloration, excessive scratches, wear, and cracks. Improperly functioning devices, damaged, and excessively worn devices should not be used.

12.2 Care at the Point of Use

Clean instruments as soon as possible after use.

Soiled devices must be separated from non-contaminated devices to avoid contamination of personnel or surroundings.

12.3 Preparation for Cleaning

For multi-piece or complex instruments, refer to their disassembly instructions. The disassembly instructions are available in the *MAC™ 5 Resting ECG Analysis System Service Manual*.

Contact your local GE Healthcare service representative for further information. For instruments produced by another manufacturer, reference the manufacturer's instructions for use.

12.4 Clean and Disinfect Guidelines

Observe the guidelines while cleaning and disinfecting the device.

- Follow cleaning instructions and observe hazards exactly as issued by GE Healthcare or other suppliers listed.
- Avoid exposure to hypochlorite solutions and solutions containing iodine or high chlorine content, as these will promote corrosion.
- Avoid exposure to highly alkaline conditions (pH > 11), as this can damage products (for example, aluminum parts).
- Never use conductive solutions or solutions that contain wax or wax compounds to clean the equipment.
- Do not immerse the device in any liquid as this may corrode metal contacts and affect signal quality.
- Do not drip or expose the writer assembly to any liquids.
- Do not allow fluid to pool around connection pins. If this happens, blot dry with a soft, lint-free cloth.

- Avoid contact with open vents, plugs, or connectors during the cleaning and disinfecting procedures.
- Never autoclave or steam-clean the device.
- Do not use until thoroughly dry.
- Do not use any of below materials to clean the device, because their use may damage equipment surfaces.
  - Organic solvents
  - Abrasive cleaners or solvents of any kind
  - Acetone
  - Ketone
  - Betadine
  - Sodium salts

12.5 Visual Inspection, Cleaning and Disinfection Frequency

The table indicates the frequency of visual inspection, cleaning, and disinfection procedures.

Component	Visual Inspection	Cleaning	Disinfection
Device and Trolley **NOTE** Trolley is an optional purchase.	Daily, preferably before the equipment's first use each day	Monthly, or more frequently, as needed	Follow the same frequency as cleaning. Disinfection must be performed after cleaning.
Leadwires	Refer to the supplier's instructions for leadwire cleaning and disinfection.		
Reusable electrodes	Refer to the supplier's instructions for reusable electrode cleaning, disinfection and sterilization.		

12.6 Clean and Disinfect the Device and Trolley

If you purchase a trolley, the device and trolley are designed to require regular inspection and cleaning to function properly. The cleaning instructions for the device includes the touchscreen.

WARNING

ELECTRICAL HAZARD

Improper handling during inspection or cleaning could result in electrical shock.

To avoid potential shock, observe the guidelines at all times:

Before inspecting or cleaning the device, turn it off, unplug it from AC power, and remove the battery.

Do not immerse any part of the equipment in water.

12.6.1 Pre-Clean Inspection and Functional Test

Perform a visual inspection to verify that the device meets the minimum conditions:

- The case and display screen are free of cracks and other damage.
- All plugs, cords, cables, and connectors are free of kinks, frays, and other damage.
- All cords and connectors are securely seated.
- All keys and controls operate properly.
- The trolley exterior is free of cracks and other damage.
- The accessory track is functioning properly.
- All cords and connectors are securely seated.
- The actuation lever is functioning properly.
- The castor wheels are functioning properly.

If you notice any items that need repair, contact an authorized service representative to make the repairs. Discontinue using the device until the appropriate repairs can be made.

12.6.2 Clean the Device and Trolley

NOTE

The automated washer-disinfector is not applicable for MAC 5 A4/MAC 5 A5/ MAC 5 Lite medical devices.

1. Dispense Super Sani-Cloth® Wipe(s) from the canister.
2. If soil is present, thoroughly wipe the surfaces of the device with a fresh Super Sani-Cloth® Wipe for a minimum of two minutes and until soil and organic matter have been visibly removed.

   Treated surfaces must remain visibly wet for a minimum of two minutes. Use additional fresh disinfectant wipes, if needed, to make sure continuous two minutes contact time. Pay attention to the recessed areas and ridges; use a cotton swab to press onto the wipe for scrubbing these areas.
3. Inspect the device and trolley to make sure the complete removal of soil from surfaces, holes, and moveable parts.

   If soil is still present, re-clean the equipment by repeating Step 2.
4. Allow the device to air dry.
5. Discard wipes to clinical waste.

   Do not reuse wipes.

12.6.3 Post-Clean Inspection

GE Healthcare devices should be visually inspected and functionally tested after cleaning and prior to disinfection for below items:

- Cleanliness.
- Damage, including but not limited to corrosion (rust, pitting), discoloration, excessive scratches, flaking, cracks, and wear.
- Missing or worn part numbers.

- Proper functioning, including but not limited to the quality of ECGs; correct movement of hinges, joints, box locks, handles, ratchets, and couplings; proper alignment of jaws and teeth; and secure fastening of all locking mechanisms.

Do not use devices that are not functioning properly, that have unrecognizable markings, that have missing or worn part numbers, or that are damaged. Disassembled devices should be reassembled prior to disinfection unless otherwise instructed.

12.6.4 Disinfect the Device and Trolley

NOTE

The automated washer-disinfector is not applicable for MAC 5 A4/MAC 5 A5/ MAC 5 Lite medical devices.

Make sure that cleaning is carried out to remove all visible soil and organic matter. See 12.6.2 Clean the Device and Trolley on page 269.

1. Dispense fresh Super Sani-Cloth® Wipe(s) from the canister.
2. Apply disinfectant to the entire surface using fresh wipes.

   Treated surfaces must remain visibly wet for a minimum of three minutes. Use additional fresh disinfectant wipes, if needed, to make sure continuous three minutes contact time. Pay attention to the recessed areas and ridges; use a cotton swab to press onto the wipe to moisten these areas.
3. Remove disinfectant residue from the device by thoroughly wiping surfaces with a disposable, lint free wipe moistened with 70% Isopropyl Alcohol (IPA) solution.
4. Allow the device to air dry.
5. Discard wipes to clinical waste.

   Do not reuse wipes.

12.7 Clean and Disinfect Leadwires and Reusable Electrodes

CAUTION

IMPROPER FUNCTIONING

Leadwires and electrodes that are not functioning properly could result in ECG distortion or failure.

Carefully inspect instruments between uses to verify proper functioning

Refer to the supplier's instructions for leadwire cleaning and disinfection.

Refer to the supplier's instructions for reusable electrode cleaning, disinfection, and sterilization.

12.8 Storage

Store the device in a clean and dry, well-ventilated area protected from dust, moisture, insects, vermin, and extremes of temperature and humidity.

12.9 Other Cleaning and Disinfection Agents

Super Sani-Cloth® Wipes is the recommended cleaning and disinfection solution, which has been validated on the device. However, below products are compatible with the device and may be used for cleaning and disinfection.

- PDI Easy Screen Cleaning®
- PDI Super Sani-Cloth®
- PDI Sani-Cloth® Bleach
- Clinell Sporicidal Wipes
- PDI Sani-Cloth® AF3
- PDI Sani-Cloth® Plus
- PDI Sani-Cloth® HB
- Clorox Healthcare® Hydrogen Peroxide Cleaner Disinfectant Wipes
- Oxivir® Tb Wipes
- Clinell Universal Range
- Cleanisept Wipes
- Mikrozid Sensitive Wipes
- Caviwipes
- Phenol 2% (v/v)
- Ethanol (ethyl alcohol) 96% (v/v)
- Hydrogen Peroxide 20% (v/v)
- Sodium Hypochlorite (NaClO) 5% solution)
- Isopropyl alcohol 70% (m/m)

12.10 Additional Information

- GE Healthcare used Super Sani-Cloth® wipes during cleaning and disinfection validation. This cleaning agent is not listed in preference to other available cleaning agents which may perform satisfactorily.
- The cleaning and disinfection information is provided in accordance with ANSI/AAMIST81, ISO 17664. The recommendations provided above have been validated as capable of preparing non-sterile GE Healthcare MAC™ 5 medical devices. It remains the responsibility of the user to make sure that the cleaning and disinfection are performed using appropriate equipment, materials, and personnel and achieves the desired result. This requires validation and routine monitoring of the process. Any deviation from the provided recommendations should be properly evaluated for effectiveness and potential adverse consequences.
- All users should be qualified personnel with documented expertise, competency, and training. Users should be trained on hospital policies and procedures along with current applicable guidelines and standards.

- Users should utilize appropriate Personal Protective Equipment (PPE) when cleaning and disinfecting devices in accordance with the Department of Environmental and Occupational Health and Safety's (OSHA) blood-borne pathogen guidelines or equivalent.

13 Troubleshooting

13.1 System Errors

The table lists messages that you may encounter while using this device.

Message	Cause	Solution
`WARNING: Approaching <xx>% of ECG storage limit. Transmit and delete reports to free memory.`	The device storage capacity is approaching 80% or 90%. This occurs as patient reports are added to the *Files* list.	Transmit patient reports to configured destinations and delete the transmitted reports from the **Files** list to create additional storage space.
`Memory is full. Transmit and delete reports to free memory.`	The device storage capacity is between 99% and 100%.	Transmit patient reports to configured destinations and delete the transmitted reports from the **Files** list to create additional storage space.
`Memory is full. This ECG cannot be saved.`	The device storage capacity is full.	Transmit patient reports to configured destinations and delete the transmitted reports from the **Files** list to create additional storage space.
`Memory is full. New ECGs cannot be saved.`	The device storage capacity is full.	Transmit patient reports to configured destinations and delete the transmitted reports from the **Files** list to create additional storage space.
`Error Loading`	Database loading error.	Select **Retry** to reload ECG reports.
`Battery error. Attach power cord. Contact Service.`	• Power sensor failure • Battery capacity sensor failure	Replace the battery. Contact your GE Healthcare Service Support representative if the error persists.
`Battery unknown error`	An unexpected battery error has occurred.	Replace the battery. Contact your GE Healthcare Service Support representative if the error persists.
`Battery not detected`	The battery is not detected by the device.	Perform below steps: 1. Remove the battery. 2. Re-insert the battery. If the battery is still not detected, replace the battery. Contact your GE Healthcare Service Support representative if the error persists.
`Device date/time is incorrect. Update.`	The date and time set on the device is not correct.	Select **Adjust** to set the correct date and time. For more information, see 10.10.1 Configure the Date and Time on page 254.

Continues on the next page

Message	Cause	Solution
`Touchscreen failure`	The touchscreen is not working.	Contact your GE Healthcare Service Support representative if the error persists.
`Cannot perform action while acquiring ECG data`	You have tried to perform below actions while acquiring an ECG: • Start a test for a new patient • Enter or edit patient information • Change speed, gain, or filter • Access User Menu • Access **Orders**, **Files**, or **Queue** list • Start ECG • Power off, lock, log out, standby or privacy mode	Perform only allowed actions.
`Cannot perform action while acquiring Rhythm data`	You have tried to perform below actions while acquiring a rhythm: • Start a test for a new patient • Access **Orders**, **Files**, or **Queue** list • Start ECG • Power off, lock, log out, standby or privacy mode	Perform only allowed actions.
`Possible reversal: <lead names> (eg: V2 V3)`	This notification displays in the **Preview** screen when lead reversal has been detected during ECG acquisition.	Reject the acquired ECG, correct the lead position, and restart the ECG.

13.2 ECG Acquisition Errors

The table lists messages that you may encounter while acquiring ECG.

Message	Cause	Solution
`Report generation failed`	Unknown error	1. Retry the action. 2. If the error persists, power off and power on the device. 3. If the error persists, contact your GE Healthcare Service Support representative.
`Cannot open report`		
`ECG recording failed`		

13.3 Printing Errors

Table 13-1 Printer Errors Encountered During ECG Patient Report Printing

Error Message	Error Condition	How to troubleshoot:
`Printer error. Paper jam detected.`	Paper is jammed.	Carefully remove the stuck paper from the rollers inside the printer and verify that the remaining papers are loaded correctly in the tray. Printing will restart automatically.

Continues on the next page

Table 13-1 Printer Errors Encountered During ECG Patient Report Printing (Table continued)

Error Message	Error Condition	How to troubleshoot:
`Printer error. Out of paper.`	The paper tray is empty.	Insert sufficient paper in the paper tray. Printing will restart automatically.
`Printer error. Door is open.`	The printer door is open.	Close the printer door. Printing will restart automatically.

Table 13-2 Printing Errors Encountered During Rhythm Printing

Error Message	Error Condition	How to troubleshoot:
`Printer error. Paper jam detected.`	Paper is jammed.	1. Carefully remove the stuck paper from the rollers inside the printer and verify that the remaining papers are loaded correctly in the tray. 2. Select **Start Rhythm** to restart rhythm printing.
`Printer error. Out of paper.`	The paper tray is empty.	1. Insert sufficient paper in the paper tray. 2. Select **Start Rhythm** to restart rhythm printing.
`Printer error. Door is open.`	The printer door is open.	1. Close the printer door. 2. Select **Start Rhythm** to restart rhythm printing.

Table 13-3 Printing Errors Encountered During Printing of the List of Stored Records

Error Message	Error Condition	How to troubleshoot:
`Printer error. Paper jam detected.`	Paper is jammed.	1. Carefully remove the stuck paper from the rollers inside the printer and verify that the remaining papers are loaded correctly in the tray. 2. Select **Print List** from the **Files Manager** to restart printing of the stored records list.
`Printer error. Out of paper.`	The paper tray is empty.	1. Insert sufficient paper in the paper tray. 2. Select **Print List** from the **Files Manager** to restart printing of the stored records list.
`Printer error. Door is open.`	The printer door is open.	1. Close the printer door. 2. Select **Print List** from the **Files Manager** to restart printing of the stored records list.

Continues on the next page

Table 13-3 Printing Errors Encountered During Printing of the List of Stored Records (Table continued)

Error Message	Error Condition	How to troubleshoot:
`Cannot perform action while printing`	You have tried to perform below actions while printing a patient report: • Start a test for a new patient • Delete the patient report • Change speed, gain, or filter • Access User Menu • Access **Orders**, **Files**, or **Queue** lists • Power off, lock, log out, standby, or privacy mode	Perform only the allowed actions.

Table 13-4 Printer Errors Encountered During Printing via Network Printer

Error Message	Error Condition	How to troubleshoot
`Network printer offline`	• The network printer is power off. • The network printer is not connected to network • Network Printer IP address changed	Turn on the network printer, connect it network, and check network printer IP Address is same as configured on MAC 5 device.
`Network printer toner low`	The cartridge of the network printer is nearly out of use.	Replace the cartridge in the network printer
`Network printer media empty`	The network printer paper tray is empty.	Insert sufficient paper in the paper tray.
`Network printer paper jam`	Paper in the network printer is jammed.	Carefully remove the stuck paper from the printer and verify that the remaining papers are loaded correctly in the tray.
`Network printer authentication failure`	Network printer requires a username and password to accept printing job. • User did not configure username and password in network printer correctly • Network printer username and password changed	Correct username and password on the MAC 5 device.
`Network printer unknown error`	Unknown error in printer	Restart the system to check if the error is resolved. If the error persists, contact your GE Healthcare Service Support representative.

Table 13-5 Common Printer Errors

Error Message	Error Condition	How to troubleshoot:
`Low Battery. Printer is disabled. Connect power cord.`	Low battery	Connect the power cord.

Continues on the next page

Table 13-5 Common Printer Errors (Table continued)

Error Message	Error Condition	How to troubleshoot:
`High printer temperature. Printer disabled. Contact Service.`	High printer temperature	Restart the system to check if the error is resolved. If the error persists, contact your GE Healthcare Service Support representative.
`Printer error. Restart system. Contact Service.`	Unknown error or hardware failure in printer	Restart the system to check if the error is resolved. If the error persists, contact your GE Healthcare Service Support representative.
`Incompatible firmware.`	Incompatible printer firmware	Contact your GE Healthcare Service Support representative to upgrade the printer firmware.
`Acquisition error. Fix and retry printing.`	Printing stopped due to acquisition error	Rectify the error with the acquisition module and retry printing.
`Printer error. Retry. If issue persists, restart system.`	Unknown error in printer	Retry printing. If the error persists, restart the system.
`Printer is recovering. Please wait ...`	Printer recovery error	Wait for the printer to recover. If the error persists, restart the system.
`Cannot perform action while printing`	You have tried to perform below actions while printing a patient report: • Start a test for a new patient • Delete the patient report • Change speed, gain, or filter • Access User Menu • Access **Orders**, **Files**, or **Queue** lists • Power off, lock, log out, standby or privacy mode	Perform only allowed actions.

13.4 Report Transmission Errors

Table 13-6 Errors Encountered During Patient Report Transmission

Error Message	Error Condition	How to troubleshoot:
`Transmission queue is full. Additional reports cannot be added to the queue.`	The transmission queue has reached its maximum limit of 1,000 reports.	Wait for the reports in the queue to transmit and try again.
`Unable to transmit. Incomplete patient data.`	One or multiple patient reports cannot be added to the transmission queue because required fields in the patient demographics are blank or contain invalid data.	1. Edit the incomplete patient report(s) to enter missing patient data. 2. Retry transmission.
`Unable to transmit one or more reports. Incomplete patient data.`		

Continues on the next page

Table 13-6 Errors Encountered During Patient Report Transmission (Table continued)

Error Message	Error Condition	How to troubleshoot:
`Report transmission is in progress. Delete job from queue to edit.`	You are trying to edit a patient report that is being transmitted.	Delete the job from the queue to continue editing the patient report.
`Destination unknown`	The destination is not found.	Reconfigure the destination. See 10.6.2 Configure Transmission & Query Settings on page 154
`No USB device detected`	The USB flash drive is not detected.	Verify that the USB flash drive is firmly inserted into the USB port. If the error persists, verify that external USB storage is enabled and the USB port is enabled. If the error persists, use another USB flash drive.
`USB storage is full`	The USB storage is full.	Remove this USB flash drive, and insert another USB flash drive with write permissions.
`USB unknown error`	The USB flash drive has an unknown error.	Remove this USB flash drive, and insert another USB flash drive with write permissions.
`Cannot copy to USB`	The report cannot be transmitted to the USB flash drive.	Make sure that the USB flash drive is firmly inserted into the USB port.
`Hilltop generation unsuccessful`	The file generation is unsuccessful.	Retry transmission. Contact your GE Healthcare Service Support representative if the error persists.
`PDF generation unsuccessful`		
`Sapphire generation unsuccessful`		
`Unknown error`	Unknown error	Contact your GE Healthcare Service Support representative if the error persists.
`Server not connected`	The server connection is unsuccessful.	Retry transmission. Contact your GE Healthcare Service Support representative if the error persists.
`DCP not found`	The DCP connection is unsuccessful.	
`Unknown server version`	The server version is unknown.	
`Server is not accepting the test.`	The server is not accepting the transmission.	
`No network connection`	The network connection is lost.	Reconnect to the network.

13.5 Configuration File Errors

Table 13-7 Configuration File Errors

Error Message	Error Condition	How to Troubleshoot:
`Digital signature validation failed`	The digital signature in the configuration file used for restoring settings is not valid.	Copy the configuration file with a valid digital signature to the USB flash drive.
`Invalid data file format`	The configuration file used for restoring settings is invalid.	Copy a valid configuration file to the USB flash drive.
`Missing data in data file`	The configuration file used for restoring settings was not properly saved.	Copy a valid configuration file to the USB flash drive.

13.6 USB Flash Drive Errors

Table 13-8 USB Device Errors

Error Message	Error Condition	How to Troubleshoot:
`No USB device detected`	The USB flash drive is not inserted properly in the USB port.	Make sure that the USB flash drive is firmly inserted into the USB port.
`USB unknown error`	The USB flash drive has an unknown error.	Remove this USB flash drive, insert another USB flash drive with write permissions.

13.7 Shared Network Connection Errors

Table 13-9 Shared Network Connection Errors

Error Message	Error Condition	How to troubleshoot:
`Network shared path not found`	User-specified shared network path is invalid.	Enter a valid path name and select **Test Connection**.
`Invalid shared network credentials`	User-specified credentials to access shared network path is invalid.	Enter valid credentials and select **Connect**.
`Connection to shared network path failed`	User-specified IP/URL to access shared network path is invalid.	Enter the correct IP/URL and select **Test Connection**.
`Shared network mount path not found`	There is no LAN/WLAN connectivity.	Enable LAN/WLAN connectivity and select **Test Connection**.

Continues on the next page

Table 13-9 Shared Network Connection Errors (Table continued)

Error Message	Error Condition	How to troubleshoot:
`Shared Directory mount failed`	The Configured shared directory mount can be failed because of: • The Shared folder on the server does not have applicable access permissions. • The Windows server which contains the shared directory can use a less secure SMB version (SMB2 and earlier). The connection is rejected by application for security. • Incorrect Universal Naming Convention (UNC) name or path entered while configuring the shared folder on device. **NOTE** The Universal Naming Convention (UNC) are the names provided for network shared folders.	• Make sure that the configured shared directory has applicable access permissions. • Check if the server where the shared path is configured is Windows 2008 R2 or Windows Vista R1 or earlier Windows server version. These Windows server versions support less secure protocol versions for shared directory communications (for example, SMB v2 or earlier). Make sure that you use the later Windows server version that supports secured communication protocol (SMB3.0 or later) for shared directory configurations and for a secured transactions. • Check if UNC name and the shared path are entered correctly while configuring the shared directory.
`Username is required`	User Name field is empty.	Enter valid username and select **Connect**.
`Password is required`	Password field is empty.	Enter valid password and select **Connect**.
`Username and Password are required`	User Name and password fields are empty.	Enter valid credentials and select **Connect**.
`Test Successful`	The **Test Successful** message displays if you have entered **./** in the User Name field while entering the valid shared directory path.	**Test Connection** can pass if the user does not have a write permission on the server while the actual transmission could fail.

13.8 DCP Server Connection Errors

DCP Test Connection Errors

The Test connection failure of secured DCP destinations is because of certificate authentication errors. All the test connection errors stored in the Audit and Event Logs. The list of possible certificate error conditions that occur during test connection in the Audit and Event Logs.

Table 13-10 DCP Server Connection Errors

Error Message	Error Condition	How to troubleshoot:
`MUSE connection failed due to certificate error`	The CA certificate is not present or installed in the DCP server destination.	Obtain a PEM-encoded CA certificate and install it in the DCP server configuration.
	The CA certificate installed, but it does not be a part of the configured DCP server destination.	Configure the PEM-encoded CA certificate in the DCP server destination.

Continues on the next page

Table 13-10 DCP Server Connection Errors

Error Message	Error Condition	How to troubleshoot:
	Any of the certificate for the DCP server destination is expired.	• Verify the validity dates of the installed CA certificate. • If expired, obtain the CA certificate which is not expired. • If the installed certificate is not expired, verify the server certificate validity date.

DCP Transmission Errors

A certificate authentication error occurs during transmission to the secured DCP destination. The transmission failed message display in the transmission queue because of the certification error. All the transmission errors stored in the Audit and Event Logs. The list of possible certificate error conditions that occur during transmission in the Audit and Event Logs.

Table 13-11 DCP Server Transmission Errors

Error Message	Error Condition	How to troubleshoot:
`Record transmission failed due to certificate error`	The CA certificate is not present or installed in the DCP server destination.	Obtain a PEM-encoded CA certificate and install it in the DCP server configuration.
	The CA certificate installed, but it does not be a part of the configured DCP server destination.	Configure the PEM-encoded CA certificate in the DCP server destination.
	Any of the certificate for the DCP server destination is expired.	• Verify the validity dates of the installed CA certificate. • If expired, obtain the CA certificate which is not expired. • If the installed certificate is not expired, verify the server certificate validity date.

Patient Query Errors

The ADT query to the secured DCP destination fails because of the certificate authentication errors. All the ADT query errors stored in the Audit and Event Logs. The list of possible certificate error conditions that occur during ADT query in the Audit and Event Logs.

Table 13-12 ADT Query Errors

Error Message	Error Condition	How to troubleshoot:
`ADT query failed due to certificate error`	The CA certificate is not present or installed in the DCP server destination.	Obtain a PEM-encoded CA certificate and install it in the DCP server configuration.
	The CA certificate installed, but it does not be a part of the configured DCP server destination.	Configure the PEM-encoded CA certificate in the DCP server destination.

Continues on the next page

Table 13-12 ADT Query Errors

Error Message	Error Condition	How to troubleshoot:
	Any of the certificate for the DCP server destination is expired.	• Verify the validity dates of the installed CA certificate. • If expired, obtain the CA certificate which is not expired. • If the installed certificate is not expired, verify the server certificate validity date.

Table 13-13 DCP CA Certificate Errors

Error Message	Error Condition	How to troubleshoot:
`CA certificate has expired`	The CA certificate has expired.	Obtain a PEM-encoded CA certificate that is not expired.
`CA certificate PEM check failed`	The CA certificate format is invalid.	Obtain a valid PEM-encoded CA certificate.

DCP Order Query Errors

The remote orders query to the DCP destination fails because of the URL or port number configuration errors. All the remote order query errors stored in the Audit and Event Logs. The list of possible error conditions that occur during remote order query in the Audit and Event Logs.

Table 13-14 DCP Server Order Query Errors

Error Message	Error Condition	How to troubleshoot:
`Remote order query failed`	Query mode is Orders only and the configured DCP order server URL and/or port number is incorrect.	Make sure that you configure the correct URL and port number.
`Remote Order/ADT Query Failed`	Query mode is Orders then ADT and the configured DCP order server URL or port number is incorrect.	Make sure that you configure the correct URL and port number.

13.9 Errors while Installing Certificates

Table 13-15 CA Certificate Installation Errors

Cause for Error	Error Condition	How to troubleshoot:
Not in PEM format	The CA certificate is not in PEM format.	Convert the CA certificate to PEM format.
Not a valid CA certificate	The CA certificate is in valid.	Check that the certificate is a valid CA certificate and has the CA certificate flag enabled.
Date not valid	Only a warning and not an error condition.	Check that the CA certificate has a valid date.

Table 13-16 Client Certificate Installation Errors

Cause for Error	Error Condition	How to troubleshoot:
Not in PEM format	The client certificate is not in PEM format.	Convert the client certificate to PEM format.
Unrecognized public key algorithm - RSA, DSA, ECDSA.	The client certificate public key algorithm is not recognized.	Check that the client certificate public key algorithm is valid and has the recognizable algorithm including RSA, DSA, and ECDSA.
Signature does not match CA certificate	The client certificate signature does not match with CA certificate.	Verify that the client certificate was signed by the installed CA certificate. Not applicable for **Self-signed** certificate.
Missing link in CA certificate chain	An intermediate certificate in the certificate chain is missing.	Include missing intermediate certificates in the CA certificate. See 10.8.7 Intermediate Certificates on page 236. Not applicable for **Self-signed** certificate.
Incorrect password for private key	The password is incorrect for private key of the client certificate.	Check that the password is correct for private key of the client certificate.
Incompatible public/private key pair	The client private key and client public key are not compatible with each other.	Install a compatible public/private key pair for the client certificate.
Date not valid	Only a warning and not an error condition	Check that the client certificate has a valid date.

13.10 Wireless Network Connectivity Errors

Table 13-17 CA Certificate Errors

Error Message	Error Condition	How to troubleshoot:
`CA Certificate PEM Check Failed`	The CA certificate format is invalid.	Obtain a PEM-encoded CA certificate.
`CA Certificate has expired`	The CA certificate has expired.	Obtain a PEM-encoded CA certificate.
`CA Certificate is invalid`	The CA certificate is invalid.	Obtain a PEM-encoded CA certificate.
`Unrecognized certificate format`	Certificate format is invalid.	Obtain a PEM-encoded CA certificate.

Table 13-18 Client Certificate Errors

Error Message	Error Condition	How to troubleshoot:
`Client Public Key Certificate PEM Check Failed`	The client certificate format is invalid.	Obtain a PEM-encoded client certificate.
`Client Certificate has expired`	The client certificate has expired.	Obtain a PEM-encoded client certificate.
`Invalid Client Private Key Password`	The client private key password is invalid.	Enter a valid client private key password.

Continues on the next page

Table 13-18 Client Certificate Errors (Table continued)

Error Message	Error Condition	How to troubleshoot:
`Client Certificate is invalid`	The client certificate is invalid.	Obtain a PEM-encoded client certificate.
`CA Certificate Compatibility Check Failed`	The client certificate is not compatible with the CA certificate in the device or the CA certificate is not installed in the device.	Obtain a PEM-encoded client certificate which is compatible with the PEM-encoded CA certificate in the device or turn the **Self-signed** option on.
`Unrecognized certificate format`	Certificate format is invalid.	Obtain a PEM-encoded client certificate.

Table 13-19 Errors During Wireless Network Connection

Error Message	Error Condition	How to troubleshoot:
`CA Certificate has expired`	The CA certificate has expired.	Obtain a PEM-encoded CA certificate.
`Client Certificate has expired`	The client certificate has expired.	Obtain a PEM-encoded client certificate.
`CA and Client Certificates have expired`	The CA and Client certificates have expired.	Obtain valid PEM-encoded CA and client certificates.
`CA Certificate is not installed`	The CA certificate is not installed in the device.	Obtain a PEM-encoded CA certificate.
`Client Certificate is not installed`	The client certificate is not installed in the device.	Obtain a PEM-encoded client certificate.
`CA and Client Certificates are not installed`	The CA and client certificates are not installed in the device.	Obtain valid PEM-encoded CA and client certificates.

Table 13-20 Errors During Network Connection

Error Message	Error Condition	How to troubleshoot:
`IP address conflict`	The user entered an invalid IP address.	Enter the correct IP address.
`Invalid subnet mask`	The user entered an invalid subnet mask.	Enter the correct subnet mask.
`Invalid default gateway`	The user entered an invalid default gateway.	Enter the correct default gateway.
`Invalid primary DNS`	The user entered an invalid primary DNS.	Enter the correct primary DNS.
`Invalid secondary DNS`	The user entered an invalid secondary DNS.	Enter the correct secondary DNS.

13.11 LDAP Configuration Errors

Table 13-21 LDAP Configuration Errors

Error Message	Error Condition	How to troubleshoot:
`LDAP Server unavailable`	The LDAP server does not exist or the IP address or server name is incorrect.	Verify and update the IP address, server name, or port and test the connection.
`LDAP Server failure`	The connection to the server fails due to any unknown reasons (for example, the server is down).	Verify that the server is up and test the connection.
`LDAP Server connection timed out`	The connection to the server times out due to a network connectivity issue.	Check the network connection and test the connection again after network connectivity resumes.
`LDAP Server Distinguished Name does not exist`	The distinguished name does not exist in the LDAP server.	Verify and update the configured distinguished name and test the connection again.
`LDAP authentication failed`	User login credentials are invalid.	Enter correct login credentials and test the connection again.

A Report Formats

A.1 ECG Report Formats

Table A-1 Supported 12-Lead ECG Report Formats

Report Format Name	Description	One Page or Multiple Page Report
1 by 10s @ 25mm/s	Shows one column of 12 rows of waveforms. Each column is 10 seconds wide and printed at 25 mm/s.	One page report
1 by 10s @ 50 mm/s	Shows one column of 12 rows of waveforms. Each column is 10 seconds wide and printed at 50 mm/s. 5 seconds are printed on each page. This results in a two page report.	Multiple page report
2 by 5s @ 25mm/s	Shows two columns of six rows of waveforms. Each column is 5 seconds wide and printed at 25 mm/s.	One page report
2 by 5s @ 50 mm/s	Shows two columns of six rows of waveforms. Each column is 5 seconds wide and printed at 50 mm/s. One column is printed on each page. This results in a two page report.	Multiple page report
2 by 5s + 1 Rhythm Ld	Shows two parts: • The upper part consists of two columns of six rows of waveforms. Each column is 5 seconds wide and printed at 25 mm/s. • The lower part consists of one row of 10 seconds of one lead. The rhythm lead shown in the report is configurable.	One page report
2 by 10s	Shows two columns of six rows of waveforms. Each column is 10 seconds wide and printed at 25 mm/s. One column is printed on each page. This results in a two page report.	Multiple page report
4 by 2.5s	Shows four columns of three rows of waveforms. Each column is 2.5 seconds wide and printed at 25 mm/s.	One page report
4 by 2.5s + 1 Rhythm Ld	Shows two parts: • The upper part shows four columns of three rows of waveforms. Each column is 2.5 seconds wide and printed at 25 mm/s. • The lower part shows one row of 10 seconds of one lead. The rhythm lead shown in the report is configurable.	One page report
4 by 2.5s + 3 Rhythm Ld	Shows two parts: • The upper part shows four columns of three rows of waveforms. Each column is 2.5 seconds wide and printed at 25 mm/s. • The lower part shows three rows of 10 seconds of three leads. The rhythm leads shown in the report are configurable.	One page report
4 by 10s	Shows four columns of 3 rows of waveforms. Each column is 10 seconds wide and printed at 25 mm/s. Three leads are printed on each page. This results in a four page report.	Multiple page report

Continues on the next page

Table A-1 Supported 12-Lead ECG Report Formats (Table continued)

Report Format Name	Description	One Page or Multiple Page Report
Pharma	If you purchase the **PHAR - Pharmacy** option, you can select this type for the report. Shows three parts: • The upper part shows four columns of three rows of waveforms. Each column is 2.5 seconds wide and printed at 25 mm/s. • The middle part shows two rows of 10 seconds of three leads. The rhythm leads shown in the report are configurable. • The lower part of the report is text, such as the measurements and patient information.	One page report

Table A-2 Additional Supported 12-Lead ECG Report Formats

Report Format Name	Description	One Page or Multiple Page Report
Computer Graphic Record (CGR)	Shows three columns of four rows of medians at 25 mm/s on the left side and three rows of waveforms printed at 12.5 mm/s on the right side (resulting in 10 seconds of rhythm). The upper part of the report is text, such as the measurements or interpretation. This results in a one page report.	One page report
Swedish Format 1	Shows two columns of six rows of medians at 50 mm/s on the left side and six rows of waveforms printed at 12.5 mm/s on the right side (resulting in 10 seconds of rhythm). The lower part of the report is text, such as the measurements or interpretation. This results in a one page report.	One page report
Swedish Format 2	Shows below parts: • The upper part of the report is six rows of 5 seconds of waveform printed at 50 mm/s. • The lower part of the report is text, such as the measurements or interpretation. Each column (page) is from the first 5 seconds of data. This results in a two page report.	Multiple page report

The figure shows the standard report layout:

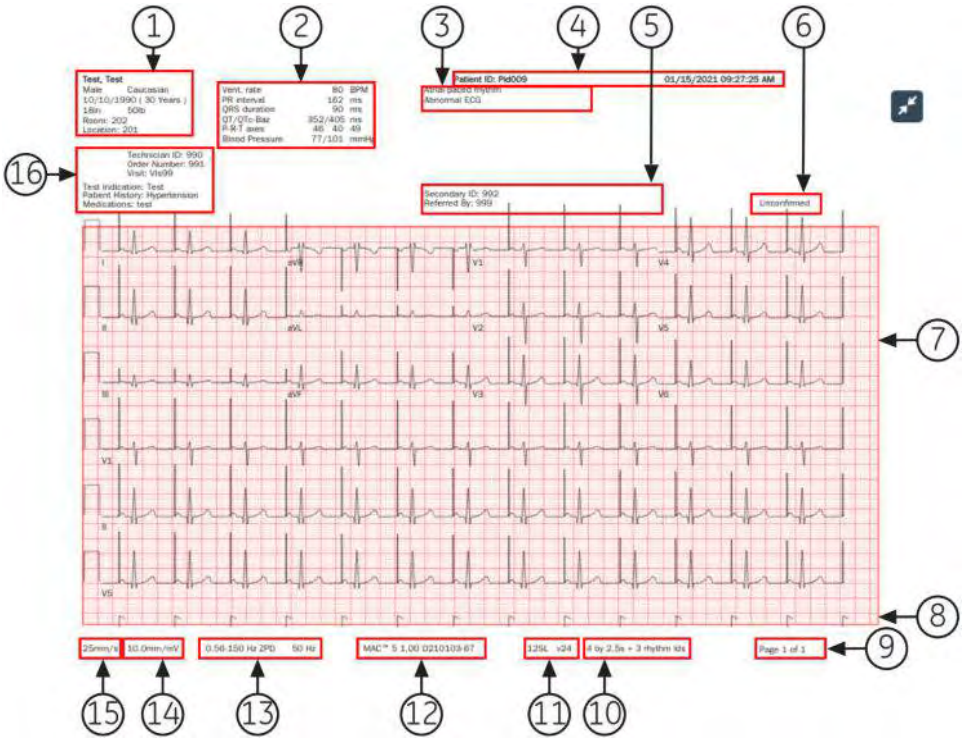


Table A-3 Standard Report Layout

Item	Name	Description
1	**Patient Demographics**	Displays information about the patient, such as: • **First Name** and **Last Name** • **Age** and/or **Date of Birth** • **Gender** • **Race** • **Height** and **Weight** • **Room** • **Location**
2	**Vital Signs**	Displays information about the patient's vital signs, such as: • Heart rate • PR interval • QRS duration • QT/QTc • P-R-T axes • Blood pressure
3	**12SL Interpretation Statements**	Displays automated 12SL interpretation statements if the report format is configured to include 12SL interpretation statements. Clinicians use this information to make decisions about cardiac care for the patient. The patient report includes ACS interpretation statements when the ECG is recorded with the ACS option. The patient report includes lead reversal related statements if reversal is detected in the acquired ECG data. The status of **Hookup Advisor** is based on the 12SL analysis of the patient report.

Continues on the next page

Table A-3 Standard Report Layout (Table continued)

Item	Name	Description
4	**ECG Header**	Displays the **Patient ID**, date and time of ECG acquisition in the configured date and time format, and the name of the institution, if configured.
5	**Physician Information**	Displays the details below: • **Referred by**: Name or ID of the physician who referred the patient. • **Secondary ID**: Alternate identification number of the patient.
6	**Report Status**	Displays the status of the report.
7	**Waveforms**	Displays the 10 seconds ECG patient report in the configured report format for the selected lead set.
8	**Pace Annotations**	Displays pace annotaions for patients with a pacemaker. The pace annotations represent pacemaker pulses. Available only when HD Pace option is enabled. For detailed information, see 5.4 Enable HD Pace on page 62. **NOTE** When two pace annotations are detected so close to each other that they cannot be uniquely shown on the report, a single pace flag with two flag tips is printed to indicate this condition. 
9	**Page Number**	Displays the page number of the ECG patient report in the format page *x* of *y*, where *x* is the current page number and *y* is the total number of pages.
10	**Report Format**	Displays the configured report format title used to preview the ECG patient report.
11	**12SL Version**	Displays the 12SL version used to analyze the ECG patient report.
12	**Product Model**	Displays the product model.
13	**Filter Setting**	Displays the filter of the ECG waveform (measured in Hz), with Zero Phase Distortion (ZPD for High Pass filter).
14	**Gain Setting**	Displays the gain of the ECG waveform (measured in mm/mV).
15	**Speed Setting**	Displays the speed of the ECG waveform (measured in mm/s).
16	**Clinical Data**	Displays the clinical data gathered during the ECG test, such as: • **Technician ID** **NOTE** If the logged-in user has a **Technician ID** associated with their user account, the **Technician ID** is automatically populated in the preview. If the user modifies the value of the **Technician ID** field in the **Patient Information** screen, the preview is refreshed with the updated **Technician ID**. • **Test Indication** • **Priority** • **Visit Number** • **Medical History** • **List of Medications**

A.2 Rhythm Report Format

Rhythm reports contain patient information, waveform data, and ECG acquisition data. A rhythm report is a continuous recording of a patient's ECG in a digital format or in print. A continuous rhythm recording is done for a patient so cardiac events are not missed.
This section describes the information contained in a rhythm report and explains where in the report that the information is located. After generating a rhythm report, it is a recommended best practice to review the report before allowing the patient to leave.

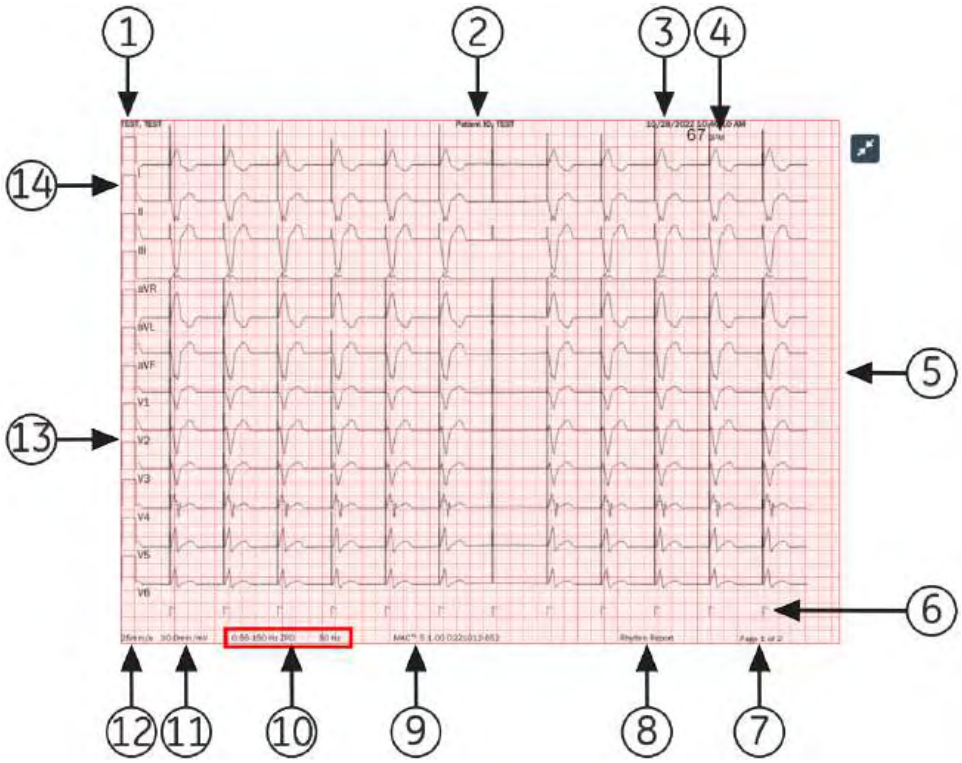


Table A-4 Standard Rhythm Report Layout

Item	Description
1	Patient name
2	Patient ID and the name of the institution
3	The date and time of acquisition for the report. If the report contains more than one page, the time of acquisition changes on each page to the current time of acquisition.
4	The beats per minute (BPM) for the heart rate of the patient. If the report contains more than one page, the BPM changes on each page of the waveform data.
5	The waveform data The rhythm report contains waveform data for 12 leads configured for the rhythm report.

Continues on the next page

Table A-4 Standard Rhythm Report Layout (Table continued)

Item	Description
6	Pace channel. Pace annotations display in this channel for patients with a pacemaker. The pace annotations show pacemaker pulses. Available only when HD Pace option is enabled. See 5.4 Enable HD Pace on page 62 for detailed information. **NOTE** When 2 pacemaker pulses are sensed so near each other that they cannot be uniquely shown on the report, a one pace spike with two flag tips is printed to show this condition: 
7	Page number of the report. The page number increments for each page of the rhythm report. For the digital rhythm report, the page number is shown as **Page <x> of <y>**. For the printed rhythm report, the page number is shown as **Page <x>**.
8	The type of report format (rhythm report).
9	The product name.
10	The **Filter** of the ECG waveform (measured in Hz), indicated with ZPD (for High Pass filter). **NOTE** You can change the filter before or during the recording and/or printing of a rhythm. For the printed rhythm report, the printing stops and restarts at the newly selected filter. A gap is shown on the printed rhythm report where the change occurred. Each time the rhythm printing starts after a change in filter, a calibration pulse is added for each lead that tells which filter on the printed rhythm. For the digital rhythm report, the calibration pulse of the last filter selected during recording is shown on the full report.
11	The **Gain** of the ECG waveform (measured in mm/mV). **NOTE** You can change the gain before or during the recording and/or printing of a rhythm. For the printed rhythm report, the printing stops and restarts at the newly selected gain. A gap is shown on the printed rhythm report where the change occurred. Each time the rhythm printing starts after a change in gain, a calibration pulse is added for each lead that tells the gain on the printed rhythm. For the digital rhythm report, the calibration pulse of the last gain selected during recording is shown on the full report.
12	The **Speed** of the ECG waveform (measured in mm/s). **NOTE** You can change the speed before or during the printing of a rhythm. For the printed rhythm report, the printing stops and restarts at the newly selected speed. A gap is shown on the printed rhythm report where the change occurred. Each time the rhythm printing starts after a change in speed, a calibration pulse is added for each lead that tells the speed on the is printed rhythm. The digital rhythm report is recorded at the configured rhythm speed.
13	The **Leads**.

Continues on the next page

Table A-4 Standard Rhythm Report Layout (Table continued)

Item	Description
14	The **Calibration pulses**. When a rhythm recording is started, a calibration pulse is added at the beginning of each lead in the patient report, which shows the speed and gain at which the rhythm is recorded. Each calibration pulse represents 1 mV of amplitude and 200 ms duration of the waveform. Each time the rhythm recording starts after a change in speed or gain, a calibration pulse is printed for each lead. **NOTE** The standard grid paper is divided into small squares of 1 mm x 1 mm and large squares of 5 mm x 5 mm. When recording 25 mm/s, 1 second of data is shown in 25 mm (5 large squares) on the rhythm report. When recording 10 mm/mV, 1 mV of data is shown in 10 mm/mV (2 large squares) on the printout.

A.3 Full Disclosure (FD) Report Format

Full Disclosure (FD) reports contain patient information, waveform data, and ECG acquisition data in FD buffer at the time of generating report. A FD report is a continuous recording of a patient's ECG in a digital, print, or transmit format for a single lead.

This section describes the information contained in a FD report and explains where in the report that the information is located. After generating a FD report, it is a recommended best practice to review the report before allowing the patient to leave.

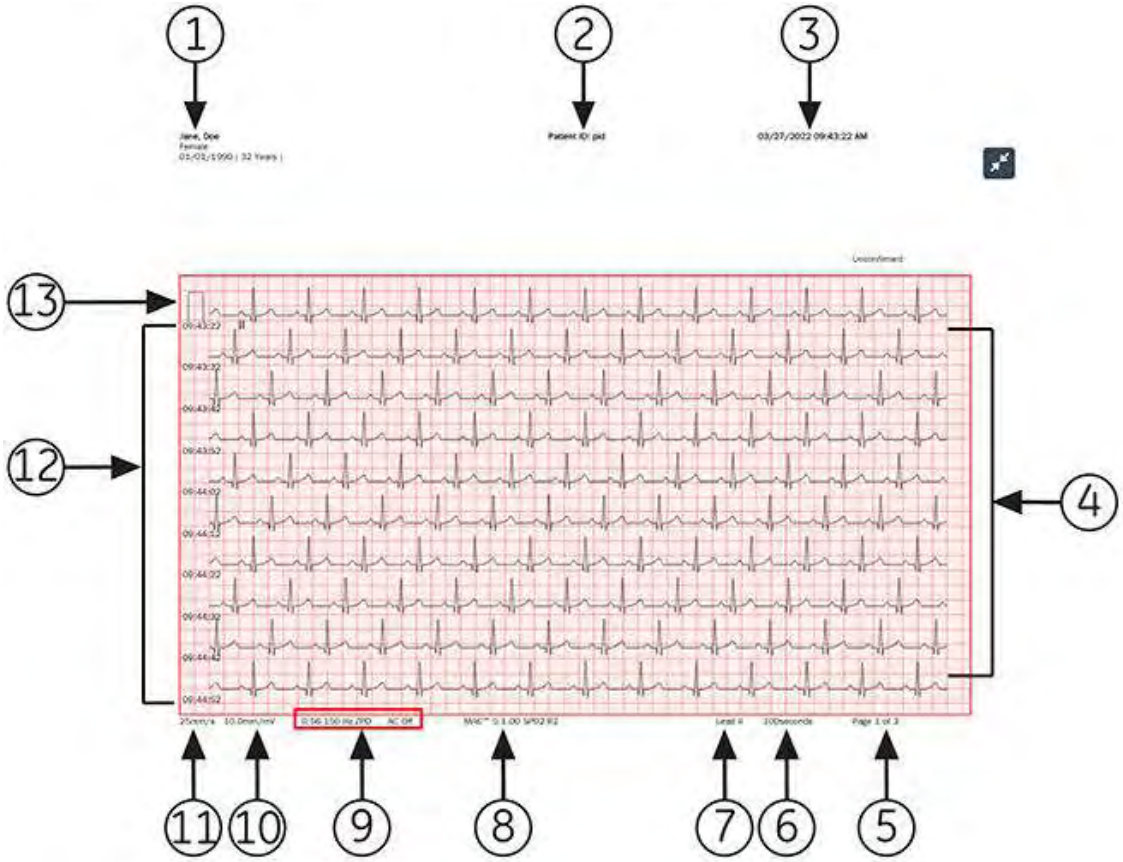
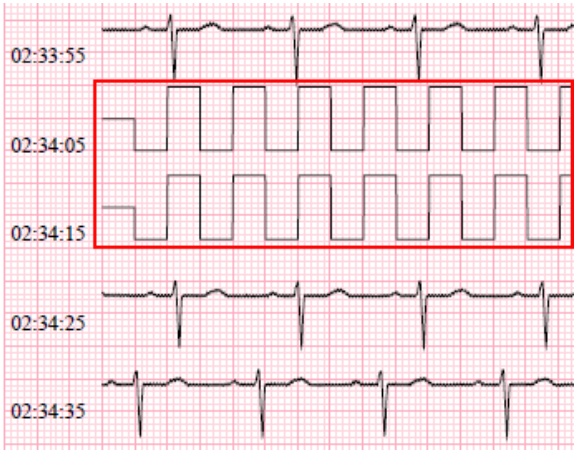


Table A-5 FD Report Layout

Item	Description
1	Prints the patient name.
2	Prints the patient ID and name of the institution.
3	Prints the date and time of acquisition for the report.
4	Prints the waveform. The FD report contains waveform data for a single lead selected in Full Disclosure mode. **NOTE** A square waves is shown on the printed or transmitted FD report when the lead is disconnected. 
5	Prints the page number of the report. The page number increments for each page of the FD report. For the FD report, the page number is shown as **Page <1> of <3>**.
6	Prints the total number of seconds in the rhythm report on each page.
7	Prints the selected single **Lead** information.
8	Prints the product name.
9	Prints the **Filter** of the ECG waveform (measured in Hz), indicated with ZPD (for High Pass filter). **NOTE** You can change the filter after recording and/or printing of a rhythm. For the printed FD report, the recording stops and restarts at the newly selected filter. Each time the Full Disclosure recording starts after a change in filter, a calibration pulse is added for each lead that tells which filter on the printed rhythm. For the digital FD report, the calibration pulse of the last filter selected during recording is shown on the full report.
10	Prints the **Gain** of the ECG waveform (measured in mm/mV). **NOTE** You can change the gain after recording and/or printing of a rhythm. For the printed FD report, the recording stops and restarts at the newly selected gain. Each time the Full Disclosure recording starts after a change in gain, a calibration pulse is added for a single lead that tells the gain on the printed FD report. For the digital FD report, the calibration pulse of the last gain selected during recording is shown on the full report.

Continues on the next page

Table A-5 FD Report Layout (Table continued)

Item	Description
11	Prints the **Speed** of the ECG waveform (measured in mm/s). **NOTE** The digital FD report is recorded at the configured rhythm speed.
12	Displays the time stamp for each row. The time stamp corresponds to clock time when the first sample is acquired in that row.
13	Prints the **Calibration pulses**. When a rhythm recording is started, a calibration pulse is added at the beginning of a single lead in the patient report , which shows the speed and gain at which the rhythm is recorded. Each calibration pulse represents 1 mV of amplitude and 200 ms duration of the waveform. Each time the Full Disclosure recording starts after a change in speed or gain, a calibration pulse is printed for a single lead. **NOTE** The standard grid paper is divided into small squares of 1 mm x 1 mm and large squares of 5 mm x 5 mm. When recording 25 mm/s, 10 rows of data, 10 seconds of data per row is shown in each page on the FD report.

B Patient Preparation

B.1 Prepare the Patient's Skin

Below steps are necessary to properly prepare a patient's skin before acquiring an ECG.

Careful skin preparation is the key to an interference-free ECG. Signal quality is indicated on the device via the **Hookup Advisor** status and messages.

1. Select the electrode placement sites for ECG diagnosis per the protocol specified by the hospital or physician.

   Refer to the electrode placement diagrams and descriptions for the various protocols.

2. Make sure that each site is dry, clean, and free of excessive hair.

   NOTE

   Do not use solvents to clean the skin; solvents trapped under electrodes may lead to abnormal skin reactions.

3. Apply the electrodes to the prepared sites.

   WARNING

   ELECTRIC SHOCK

   Touching the conductive elements cancels the protection provided by the isolated signal input.

   Make sure that conductive parts of the electrodes or leadwires, including the neutral electrode, do not come in contact with other conductive parts, including earth.

4. Check the **Hookup Advisor** for any indication of lead problems.

   NOTE

   Use only electrodes and contact agents recommended by GE Healthcare. The signal quality on the **Hookup Advisor** is not indicated until the RA/R electrode is applied. If RA/R becomes disconnected, the system reports that all electrodes are off the patient.

B.2 Electrode Placement

This section describes various methods for placing electrodes for resting ECGs on a patient.

WARNING

INACCURATE DIAGNOSIS

Improper connection of the leadwires to the electrodes will cause inaccuracies in the ECG.

Make sure the leadwires are connected properly to the electrodes. Trace each leadwire to its colored connector to make sure that it is matched to the correct label leadwire connection location.

B.2.1 Standard 12–Lead Electrode Placement

To acquire a standard 12–lead ECG, use the electrode placement shown in the diagram below.

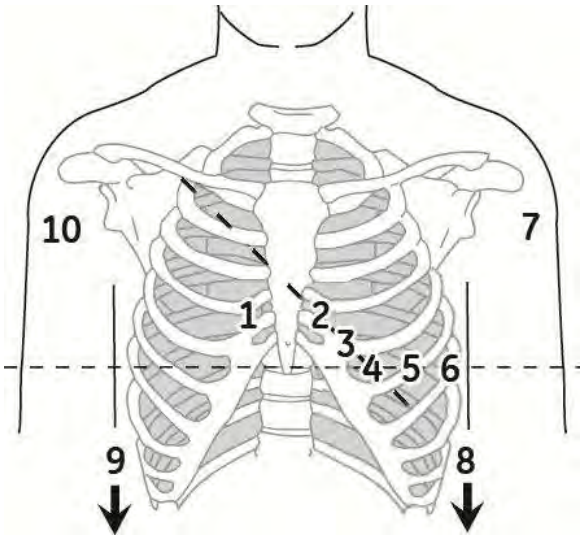


Table B-1 Standard 12–Lead Electrode Placement

Item	AHA Label	IEC Label	Description
1	V1 red	C1 red	Fourth intercostal space at the right sternal border.
2	V2 yellow.	C2 yellow	Fourth intercostal space at the left sternal border.
3	V3 green.	C3 green	Midway between location 2 and 4.
4	V4 blue	C4 brown	Mid-clavicular line in the fifth intercostal space.
5	V5 orange	C5 black	Anterior axillary line on the same horizontal level as 4.
6	V6 violet	C6 violet	Mid-axillary line on the same horizontal level as 4 and 5.
7	LA black	L yellow	Left deltoid.
8	LL red	F green	Above the left ankle (alternate placement— upper leg as close to the torso as possible).
9	RL green	N black	Above the right ankle (alternate placement—upper leg as close to the torso as possible).
10	RA white	R red	Right deltoid.

C Patient Data Fields

C.1 Patient Information Text Box Names

When an order is attached to a patient test, all Patient Information text boxes are read-only. The text box names in the table with an asterisk (*) are not.

Table C-1 *Patient Information* text boxes

Name	Description	Length	Accepted Values
Patient ID	Identification number given to the patient. The Patient ID (PID) can be configured by the administrator for a specified country requirement (for example, Denmark, Sweden, or Norway), customize text box names, and add leading zeroes for specified character lengths. If the Patient ID does not agree with the configuration, an error message opens by the Patient ID text box. If the Patient ID agrees with the configuration, the patient **Date of Birth** and **Gender** text boxes are automatically updated.	Standard Patient ID:	
		1 to 16 characters	• A to Z • a to z • 0 to 9 • All characters are supported.
		Danish Patient ID:	
		10 characters	Valid values: '0 to 9' and '-'. The PID must be in the format *ddmmyyexxg* or *ddmmyyexxg*, where: • *dd* = patient day of birth • *mm* = patient month of birth • *yy* = patient year of birth • *e* = patient year of birth is calculated as follows: ◦ *e* = 0, 1, 2, 3 or 4, if the patient year of birth is between 1900 to 1999. ◦ *e* = 5, 6, 7, 8 or 9, if the patient year of birth is between 2000 to existent year. • *xx* = patient place of birth • *g* = patient gender ◦ male = odd number ◦ female = even number
		Swedish Patient ID:	

Continues on the next page

Table C-1 *Patient Information* text boxes

Name	Description	Length	Accepted Values
		10 (Short) to 12 (Long) characters	Valid values: '0 to 9' and '-' or '+'. The PID must be in one of the below short formats: • *yymmdd+xxgc* • *yymmdd-xxgc* • *yymmddxxgc* or in the long formats as follows: • *yyyymmdd+xxgc* • *yyyymmdd-xxgc* • *yyyymmddxxgc* • *yy* and *yyyy* = patient year of birth • *dd* = patient day of birth • *mm* = patient month of birth • + or - = patient age **NOTE** If + or - is not before the patient age, the age is less than 100 years. • *xx* = patient place of birth • *g* = patient gender ◦ male = odd number ◦ female = even number • *c* = checksum digit
		Norwegian PID:	

Continues on the next page

Table C-1 *Patient Information* text boxes

Name	Description	Length	Accepted Values
		11 characters	Valid values: '0 to 9' and '-'. The PID must be in the format *ddmmyy-efgxx* or *ddmmyyefgxx*, where: • *dd* = patient day of birth • *mm* = patient month of birth • *yy* = patient year of birth • *efg* = patient year of birth calculated as follows: ◦ *efg* = 000 to 499, if patient year of birth is between 1900 to 1999. ◦ *efg* = 500 to 750 and *yy* is more than 49, if the patient year of birth is between 1800 to 1899. ◦ *efg* = 500 to 999 and *yy* is less than 50, if the patient year of birth is between 2000 to current year. • *g* = patient gender ◦ male = odd number ◦ female = even number • *xx* = patient place of birth
Mandatory fields apply for	The mandatory fields that can be configured for **Transmission** or **Acquisition** of the ECG report. Based on the **Mandatory fields apply for Transmission** settings, the ECG report is not added to the transmission queue until you enter the patient demographic data for the mandatory fields. Based on the **Mandatory fields apply for Acquisition**settings, the ECG report is not accepted, transmitted, or printed until you enter the patient demographic data for the mandatory fields.	Not Applicable	• Transmission • Acquisition
First Name	Patient first name	1 to 20 characters	• A to Z • a to z • 0 to 9 • All characters are supported.
Last Name	Patient last name	1 to 40 characters	• A to Z • a to z • 0 to 9 • All characters are supported.
Height	Patient height in inches (in) or centimeters (cm), refer to the configured unit of measurement.	Maximum 3 characters	0 to 127 in 0 to 232 cm

Continues on the next page

Table C-1 *Patient Information* text boxes (Table continued)

Name	Description	Length	Accepted Values
Weight	Patient weight in pounds (lb) or kilograms (kg), refer to the configured unit of measurement.	Maximum 3 characters	0 to 999 lb 0 to 454 kg
Gender	Patient gender	Not Applicable	• Male • Female
Date of Birth	Patient date of birth	Not Applicable	Enter the patient date of birth in the format configured by your administrator. • The date of birth must not be more than the current date. • The date must be less than 127 years from the current date. The date of birth (DOB) also shows in the **Patient Information** bar. The calculated age shows near it.
Age	Patient age	Not Applicable	If the **Age** text box is on the **Patient Information** screen, the **Date of Birth** text box is not on the screen. 0 to 127 Enter the patient age and select the applicable unit of measurement (hours, days, weeks, months, years). The **Age** also shows in the **Patient Information** bar. The date of birth (DOB) does not.
Race	Patient race	Not Applicable	• Caucasian • Black • Hispanic • American Indian • Eskimo • Hawaiian • Pacific Islander • Asian • Unknown • Other
Order Number	Unique order number given to a patient test. If the order number is given by the computer when an order is attached to the patient test, the order number cannot be edited. **NOTE** You can clear the order number which removes the number from the patient test. If you enter an order number manually, you can edit the order number.	1 to 22 characters	• A to Z • a to z • 0 to 9 • All characters are supported.

Continues on the next page

Table C-1 *Patient Information* text boxes (Table continued)

Name	Description	Length	Accepted Values
Secondary ID	An alternative identification method.	1 to 17 characters	• A to Z • a to z • 0 to 9 • All characters are supported.
Blood Pressure*	High and Low blood pressures of the patient measured in mmHg.	Maximum 3 characters	0 to 999
Location	Description of where the ECG is to be done. For each patient test, this text box is filled in from the **Location ID** configured in the *System Settings*. You can edit the location.	Maximum 5 characters	0 to 65534
Room Number*	The room number where the ECG is to be done.	Maximum characters	• A to Z • a to z • 0 to 9 • All characters are supported.
Bed Number*	The bed number where the ECG is to be done.	Maximum 32 characters	• A to Z • a to z • 0 to 9 • All characters are supported.
Priority*	Priority of ECG patient test.	Not Applicable	• Routine • STAT • PreOp The default is **Routine**.
Comments*	Additional information	Maximum 127 characters	• A to Z • a to z • 0 to 9 • All characters are supported.
Medications	Record of the medications the patient uses which is separated by a comma.	Maximum 32 characters	• A to Z • a to z • 0 to 9 • All characters are supported.
Ordering MD Last Name	Physician last name who ordered the ECG.	Maximum 40 characters	• A to Z • a to z • 0 to 9 • All characters are supported.
Ordering MD First Name	Physician first name who ordered the ECG.	Maximum 20 characters	• A to Z • a to z • 0 to 9 • All characters are supported.
Ordering MD ID	Physician ID who ordered the ECG	Maximum 5 characters	0 to 65534

Continues on the next page

Table C-1 *Patient Information* text boxes (Table continued)

Name	Description	Length	Accepted Values
Referring MD Last Name	Referring physician last name	Maximum 40 characters	• A to Z • a to z • 0 to 9 • All characters are supported.
Referring MD First Name	Referring physician first name	Maximum 20 characters	• A to Z • a to z • 0 to 9 • All characters are supported.
Referring MD ID	Referring physician ID	Maximum 5 characters	0 to 65534
Technician*	Technician doing the ECG. • If you are a local user and your user account is configured with a technician name or ID, this text box is filled in with the technician configured to your user account. You can edit this text box. • If you are an LDAP user, this text box is filled in with your HIS user ID, if the HIS server is configured. You can edit the ID.	Maximum 20 characters	• A to Z • a to z • 0 to 9 • All characters are supported.
Test Indication*	The ECG is done because of this.	Maximum 64 characters	• A to Z • a to z • 0 to 9 • All characters are supported.
Patient History*	The patient's medical history	Not Applicable	• Hypertension • CAD • Cardiac Surgery • Unknown
Visit Number	Visit number given to this patient.	Maximum 19 characters	• A to Z • a to z • 0 to 9 • All characters are supported.
<Question 1>* **<Question 2>*** **<Question 3>*** **<Question 4>***	The name of this text box is configured by the administrator. See the accepted values of these text boxes before configuration.	Alphanumeric	
		17 characters	• A to Z • a to z • 0 to 9 • All characters are supported.
		Number	

Continues on the next page

Table C-1 *Patient Information* text boxes (Table continued)

Name	Description	Length	Accepted Values
		10 characters Extra optional one special character (+) or (-) in the beginning	• 0 to 9
		Yes or No or Unknown	
		Not Applicable	• Yes • No • Unknown
Attending MD Last Name*	Attending physician last name	Maximum 40 characters	• A to Z • a to z • 0 to 9 • All characters are supported.
Attending MD First Name*	Attending physician first name	Maximum 20 characters	• A to Z • a to z • 0 to 9 • All characters are supported.
Attending MD ID*	Attending physician ID	Maximum 5 characters	0 to 65534

C.2 Clinical Trial Text Box Names

If you purchase and enable the **PHAR - Pharmacy** option on the device, **Clinical Trial** screen displays when you expand the **Patient Information** banner.

NOTE

If you enable the **Make All Clinical Trial Fields Mandatory** setting in **Clinical Trial** settings screen, all the configured clinical trial settings are required fields and an asterisk (*) displays next to each field.

Table C-2 Clinical Trial text boxs

Name	Action	Length	Allowed Values
Project Code Name	Select a value from the dropdown list	Not Applicable	The name you configured in the **Clinical Trial** settings
Project Code	Not Applicable	Not Applicable	This field automatically displays a value if you select a **Project Code Name**.
Trial ID	Not Applicable	Not Applicable	This field automatically displays a value if you select a **Project Code Name**.
Trial Visit Number	Enter the visit number	1 to 22 characters	• A to Z • a to z • 0 to 9 • All characters are supported.

Continues on the next page

Table C-2 Clinical Trial text boxs (Table continued)

Name	Action	Length	Allowed Values
Investigator ID	Enter the investigator ID	1 to 17 characters	• A to Z • a to z • 0 to 9 • All characters are supported.
Visit Type	Select a value from the dropdown list	Not Applicable	• **Scheduled** • **Unscheduled** • **Follow Up** • **Repeat** • **Early Termination** • **Unknown** • The type you configured in the **Clinical Trial** settings
Dose Type	Select a value from the dropdown list	Not Applicable	The type you configured in the **Clinical Trial** settings
<Question 1>* **<Question 2>*** **<Question 3>*** **<Question 4>*** **<Question 5>***	Enter the answer	Alphanumeric	
		17 characters	• A to Z • a to z • 0 to 9 • All characters are supported.
		Number	
		10 characters Extra optional one special character (+) or (-) in the beginning	• 0 to 9
		Yes or No or Unknown	
		Not Applicable	• Yes • No • Unknown

D Configure the MUSE System for Network Communication

D.1 MUSE Installation

For instructions to install MUSEAPI3 on MUSE V9 servers, refer to *MUSE v9 Devices and Interfaces Instruction Manual*.

For instructions to install WEBAPI on MUSE NX servers, refer to *MUSE NX Installation and Upgrade Manual*.

D.2 Set Up DCP Inbound Communication for MUSE v9.x or NX

For instructions to set up a MUSE v9 server for DCP communication, refer to *MUSE v9 Devices and Interfaces Instruction Manual.*

For instructions to set up a MUSE NX server for DCP communication, refer to *MUSE NX Administrator Manual.*

E Configure the CardioSoft System for Network Communication

E.1 CardioSoft V7 Installation

For CardioSoft installation instructions, refer to *CardioSoft Software Installation and Upgrade Guide*.

E.2 Set Up DCP Port in CardioSoft V7.0

For instructions to set up a CardioSoft v7.0 server for DCP communication, refer to *CardioSoft v7.0 Operator's Manual*.

F System Checkout

Complete these verification procedures to make sure that the device can successfully transmit tests to the MUSE system and CardioSoft system and download orders from the MUSE system.

F.1 DCP Transmission to the MUSE System

1. Transmit an ECG test from the MAC 5 to the MUSE system using the DCP protocol.
2. Verify the test is successfully acquired into the MUSE system.

F.2 DCP Transmission to the CardioSoft System

1. Transmit an ECG test from the MAC 5 to the CardioSoft system using the DCP protocol.
2. Verify the test is successfully acquired into the CardioSoft system.

F.3 MUSE Order Download

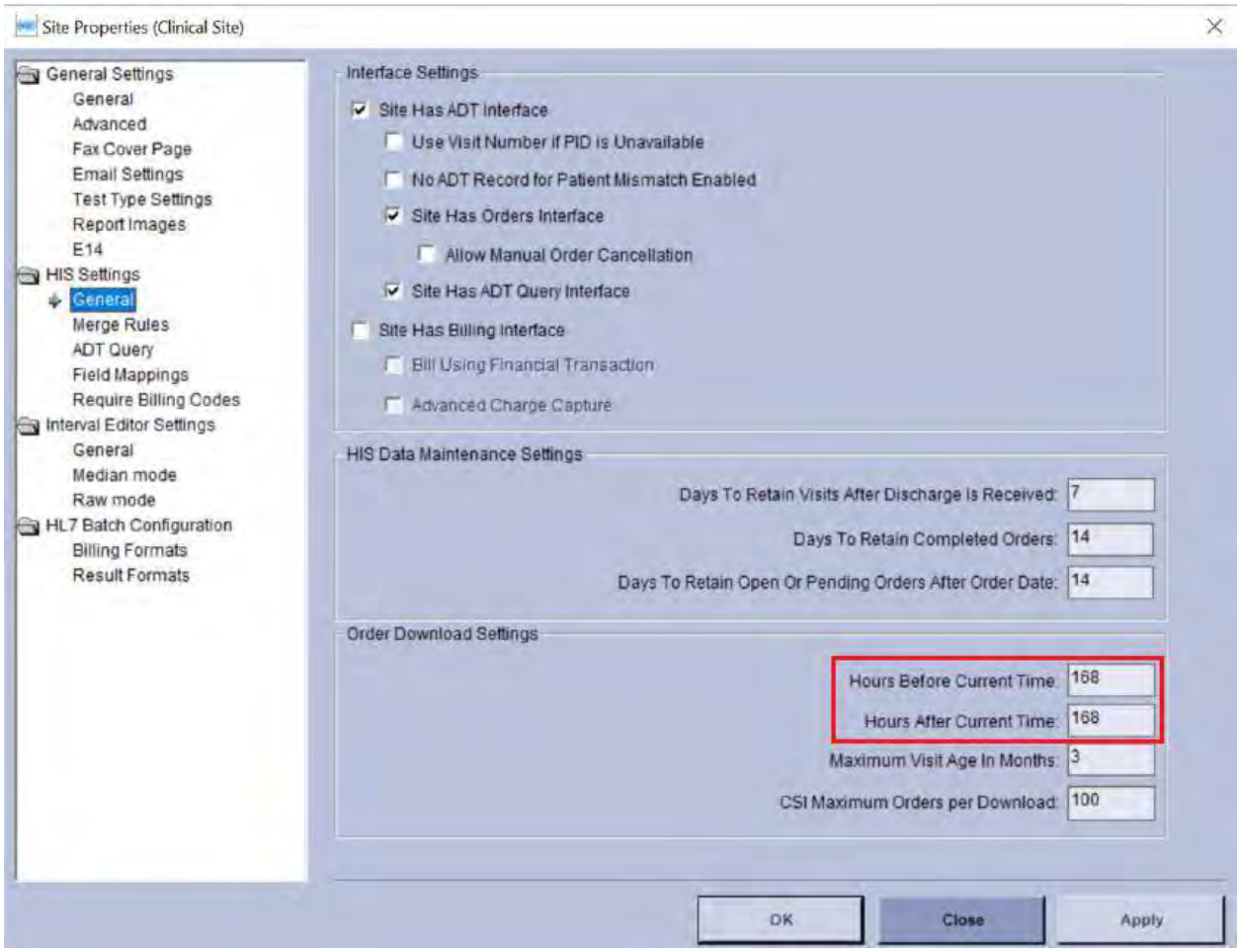
1. From the MAC 5 device, download an order from the MUSE system.
2. Verify the order is successfully downloaded to the MAC 5 device.

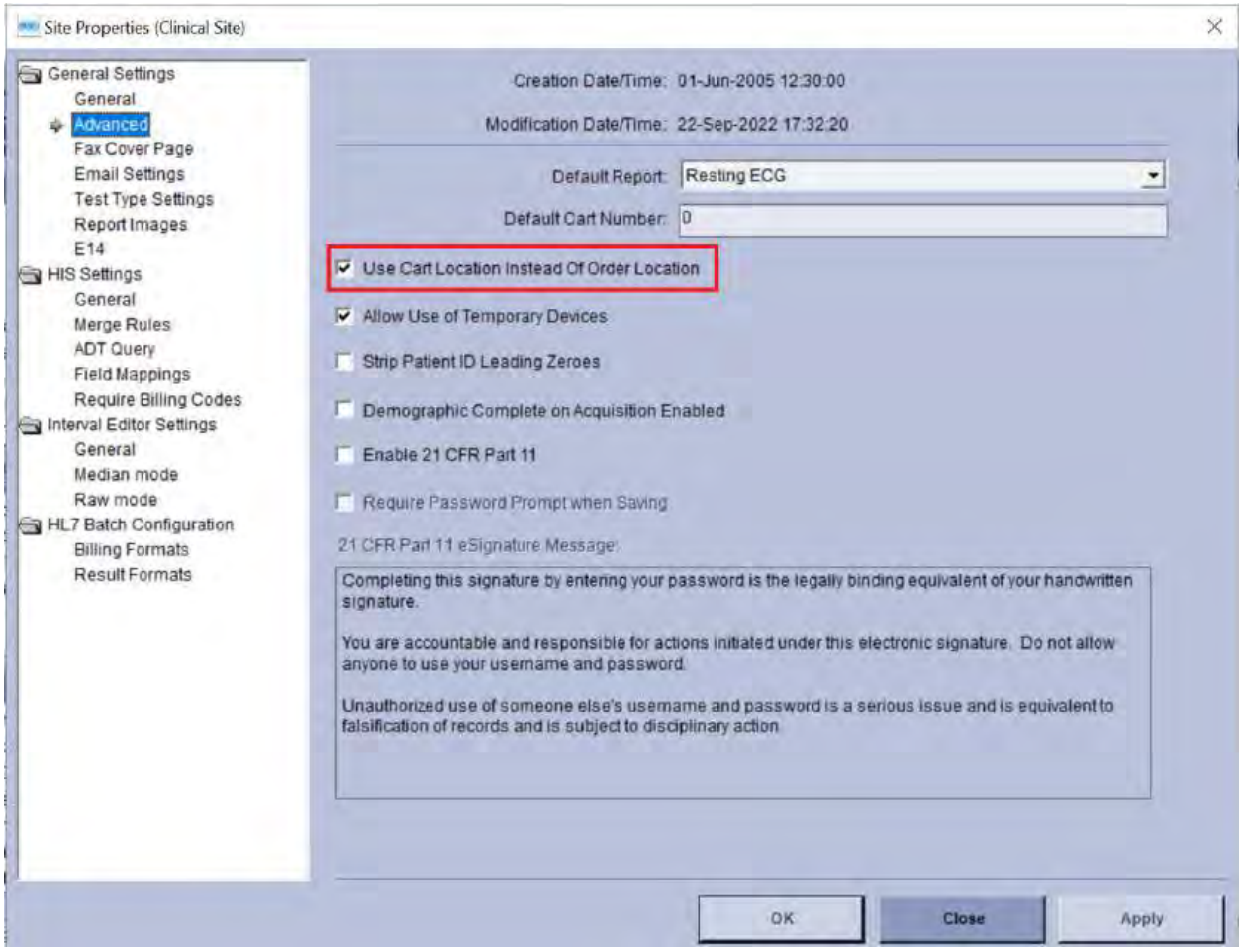
F.4 MUSE Order Download Time

You need to configure the order download time frame for WebAPI and MUSEAPI protocol.

Table F-1 Configure Order Download Time

MUSE version	Order download time window
MUSE V9	-28hr to +12hr of current system time. The time duration for downloading orders to 12 hours ahead and 28 hour back from the current system time, when downloading orders from MUSE server using MUSEAPI3 protocol.
MUSE NX 10.2 or below	-28hr to +12hr of current system time. The time duration for downloading orders to 12 hours ahead and 28 hour back from the current system time, when downloading orders from MUSE server using MUSEAPI3 protocol.
MUSE NX 10.2.1 or above	You need to configure the Order download time window in MUSE server. The device downloads the order as per the MUSE configuration. Configure the below fields in MUSE server. For steps to configure the below fields in MUSE server, refer to *MUSE NX R2 Administrator Manual*: • **Hours Before Current Time** • **Hours After Current Time** • **Use Cart Location Instead of Order Location**


Site Properties (Clinical Site)
General Settings
General
Advanced
Fax Cover Page
Email Settings
Test Type Settings
Report Images
E14
HIS Settings
General
Merge Rules
ADT Query
Field Mappings
Require Billing Codes
Interval Editor Settings
General
Median mode
Raw mode
HL7 Batch Configuration
Billing Formats
Result Formats
Interface Settings
Site Has ADT Interface
Use Visit Number if PID is Unavailable
No ADT Record for Patient Mismatch Enabled
Site Has Orders Interface
Allow Manual Order Cancellation
Site Has ADT Query Interface
Site Has Billing Interface
Bill Using Financial Transaction
Advanced Charge Capture
HIS Data Maintenance Settings
Days To Retain Visits After Discharge Is Received: 7
Days To Retain Completed Orders: 14
Days To Retain Open Or Pending Orders After Order Date: 14
Order Download Settings
Hours Before Current Time: 168
Hours After Current Time: 168
Maximum Visit Age In Months: 3
CSI Maximum Orders per Download: 100
OK
Close
Apply



When you change the **Hours Before Current Time**, **Hours After Current Time**, and **Use Cart Location Instead of Order Location** settings on the MUSE server, you need to restart the MAC 5 device to apply the changes.

G Technical Specifications

G.1 System Specifications

Table G-1 Device Physical Specifications

Item	Description
Device type	Microprocessor augmented automatic electrocardiograph; 12-leadwire acquisition with programmable lead configuration A4: Integrated unit with display and printer A5: Integrated unit with display and printer Lite: Integrated unit with display
Height	A4: 12.4 in (31.5 cm) A5: 12.4 in (31.5 cm) Lite: 12.2 in (30.9 cm)
Width	A4: 14.2 in (36 cm) A5: 10.2 in (26 cm) Lite: 10.2 in (26 cm)
Depth	A4: 4.5 in (11.4 cm) A5: 4.3 in (10.8 cm) Lite: 3.3 in (8.4 cm)
Weight	A4: 4.0 kg A5: 3.4 kg Lite: 2.3 kg
USB Port	2 USB 2.0 ports supplying 0.5 Amps of current each
Mechanical design	Housing with fixed angle graphics display Software on mainboard

Table G-2 Display Specifications

Item	Description
Display	22.6 cm (8.9 in) diagonal graphics LED backlit full HD
Touchscreen	Projected Capacitative (PCAP) multipoint touch input that works while wearing medical exam gloves
Resolution	892 X 558 pixels, with waveform enhancement
Data	Heart rate, patient name, patient ID, date and time, battery power indicator, scrolling waveforms, lead labels, speed, gain and filter settings, warning messages, prompts, hookup advisor, and help messages.

Table G-3 Printer Specifications

Item	Description
Technology	Integrated thermal dot array
Writer speed	5, 12.5, 25, and 50 mm/s
Number of traces	3, 6 and 12
Sensitivity/gain	2.5, 5, 10, 20 mm/mV, and 10/5 mm/mV split gain
Speed accuracy	5, 12.5 mm/s at ±5% 25, 50 mm/s at ±2%
Amplitude accuracy	±5%
Horizontal resolution	40 dots/mm at 25 mm/s
Vertical resolution	8 dots/mm
Paper type	Z-fold thermal with pre-printed grid and perforation
Paper size	A4: 215 mm x 280 mm (8.5 in x 11 in) (modified letter) 210 mm x 297.5 mm (8.27 in x 11.7 in) (A4) A5: 148 mm x 210 mm (5.83 in x 8.27 in) (A5)
Paper tray capacity	Holds up to 150 sheets

Table G-4 Electrical Specifications

Item	Description
Power supply	AC mains or battery operation
Input voltage	100–240 VAC ±10%
Input current range	780 mA @100V AC to 110 mA @240V AC
Input frequency	50/60 Hz ± 3 Hz

Table G-5 Battery Specifications

Item	Description
Type	Replaceable and rechargeable internal battery
Charge time	Approximately 240 minutes from total discharge when device is off (standby).
Battery capacity	120 single page resting ECG recording or 3 Hours of continuous monitoring without printing, at a minimum.

Table G-6 Other Input Device Specifications

Item	Description
External USB barcode reader	Fixed and variable length types Symbologies: Code-128, PDF417, Code 39, Interleaved Code 2 of 5, and Data Matrix symbology for characters A-Z (upper case), a-z (lower case), and 0-9 for all supported languages.

G.2 ECG Specifications

Table G-7 ECG Data Acquisition Specifications

Item	Description
Signal input	Defibrillation-proof type CF applied part Defibrillation protection: Per IEC 60601-2-25:2011
Dynamic range	AC Differential ± 10mV, DC offset ± 600 mV
Common mode rejection	>125 dB (>100 dB with AC filter disabled)
Input impedance	>50 MΩ @ 10 Hz, defibrillator protected
Patient leakage current	<10 µA
Detection of pacemaker pulse	Duration: 0.2 ms to 2.1 ms Amplitude: 2 mV to 700 mV Separation: 1 ms or greater
Pace Annotation	Dedicated pace channel on display and printed reports
Pace digital sampling rate	75,000 samples/second per channel

Table G-8 ECG Data Processing Specifications

Item	Description
ECG Interpretation	Marquette 12SL ECG Analysis Program for Adults and Pediatrics
Computerized measurements	12-lead analysis
Heart rate meter	30 to 300 beats per minute (BPM) with an accuracy of ±10% or 5 BPM, whichever is greater. Heart rates outside this range will not display.
ECG data formats	GE Hi-Fidelity ECG, XML
Pre-acquisition	Provides 10 seconds of instantaneous ECG acquisition
Digital rhythm	Up to 5 minutes of continuous rhythm storage (exportable as a PDF)
Storage	300 records consisting of 10 second Resting ECG records and Digital Rhythm records on the device internal memory
External storage	USB-compliant flash drive supporting the FAT32 file system
Downsampled ECG waveform	Bandwidth: 0.04 to 300 Hz Sample rate: 2 ksps Resolution: 1.22 µV
Analyzed ECG waveform	Bandwidth: 0.04, 0.56 ZPD to 300 Hz Sample rate: 500 and 1000 sps Resolution: 4.88 µV
Additional report filters	20 Hz, 40 Hz, 100 Hz, 150 Hz or 300 Hz
Channels	Up to 12 channels, skew between channels: < 100 µS

G.3 Environmental Specifications

Table G-9 Environmental Specifications

Item	Description
Operating Conditions	
Temperature	10°C to 40°C (50° F to 104° F)
Relative Humidity (RH)	20% to 95% (non-condensing)
Atmospheric Pressure	70 to 106kPa
Transport/Storage Conditions	
Temperature	-20°C to +60°C (–4° F to 140° F)
Relative Humidity (RH)	15% to 95% (non-condensing)
Atmospheric Pressure	50kPa to 106kPa

G.4 Safety Specifications

Table G-10 Safety Specifications

Item	Description
Certification marks	 The medical device has a lifetime of 7 years with respect to the Council Regulation EU 2017/745 Annex I, Requirement 6.
Type of Protection Against Electrical Shock	Class 1, internally powered
Degree of Protection Against Ingress of Liquids	IP20
Patient Mode of Operation	Continuous
Patient Leakage Current	<10 µA Normal Condition (NC), <50 µA Single Fault Condition (SFC)
Degree of Protection Against Electrical Shock	Defibrillation-proof type CF applied part

G.5 Network Specifications

Table G-11 Network Specifications

Item	Description
Frequency bands of transmission	2.401 – 2.461 GHz 5.180 – 5.825 GHz
Maximum radiated power in frequency bands	2.4 GHz: 18.5 dBm 5 GHz: 18.0 dBm

Continues on the next page

Table G-11 Network Specifications (Table continued)

Item	Description
Antenna	Support 2.4G and 5G
Modulation	DSSS, CCK, OFDM, BPSK, QPSK, QAM
Supported certificate key lengths	1024/2048/4096-bit encryption
Supported certificate digest algorithms	SHA1, SHA2
Wireless specifications	
Wireless Standards	802.11a/b/g/n WLAN interfaces Configured manually or via DHCP
Authentication Protocols	• Open • WEP • WPA • WPA2
Authentication Methods	• PSK • PEAP-MSCHAPV2 • PEAP-GTC • EAP-TLS • TTLS-MSCHAPV2 • TTLS-GTC
Wired Specifications	
Ethernet interface	802.3 Ethernet interface via RJ45 connector
Wired Standards	10Base-T and 100Base-T LAN x 1 port Configured manually or via DHCP

H Regulatory and Safety Information

This section provides information about the safe use and regulatory compliance of this system. The system software is considered medical software. As such, it was designed and manufactured to the appropriate medical regulations and controls.

H.1 Intended Use

The MAC 5 ECG Analysis System is intended to acquire, analyze, display, and record electrocardiographic information from adult or pediatric populations. Basic system delivers 3, 6, or 12 lead ECG's and interpretive analysis. Transmission and reception of ECG data and other clinical data to and from a central clinical information system is optional.

The MAC 5 ECG Analysis System is intended to be used under the direct supervision of a licensed healthcare practitioner, by trained operators in a hospital, medical professional's facility or wherever ECG testing is performed.

H.2 Indications for Use

The MAC 5 Resting ECG Analysis System is a non-invasive prescription device.

- The device is indicated for use to acquire, analyze, display and print electrocardiograms.
- The device is indicated for use to provide interpretation of the data for consideration by a physician.
- The device is indicated for use in a clinical setting, by a physician or by trained personnel who are acting on the orders of a licensed physician. It is not intended as a sole means of diagnosis.
- The interpretations of ECG offered by the device are only significant when used in conjunction with a physician over-read as well as consideration of all other relevant patient data.
- The device is indicated for use on adult and pediatric (birth through 21 years of age) populations.

H.3 Contraindications

This MAC 5 Resting ECG Analysis System is not intended in the manners below:

- During patient transport
- With high-frequency surgical units
- As an intra-cardiac application
- As a sole means of diagnosis
- As a vital signs physiological monitor

H.4 Clinical Benefits

The clinical benefits of the MAC 5 Resting ECG Analysis System include: analysis of ECG data (QRS Complex) for diagnostic interpretation by the clinician/physician to assist with clinical decision making in the care of patients with heart disease. These clinical benefits follow the devices' intended uses and indications for use.

H.5 Prescription Device Statement

CAUTION

United States federal law restricts this device to sale by or on the order of a physician.

H.6 Safety Conventions

This section describes the safety conventions used in the documentation for the product.

A Hazard is a source of potential injury to a person, property, or the system.

The manuals for this system use the terms DANGER, WARNING, CAUTION, and NOTICE to point out hazards and to designate a degree or level of seriousness. Familiarize yourself with the definitions below and their significance.

Table H-1 Definitions of Safety Conventions

Safety Convention	Description
DANGER	Indicates an imminent hazard, which, if not avoided will result in death or serious injury.
WARNING	Indicates a potential hazard or unsafe practice, which, if not avoided, could result in death or serious injury.
CAUTION	Indicates a potential hazard or unsafe practice, which, if not avoided, could result in moderate or minor injury.
NOTICE	Indicates a potential hazard or unsafe practice, which, if not avoided, could result in the loss or destruction of property or data.

H.7 Safety Hazards

The safety messages below alert you to potentially hazardous conditions that could arise during the normal use of this product and recommend steps that can be taken to avoid those conditions. Safety messages pertaining to hazardous conditions that may arise during specific actions may also be provided during the discussion of those actions in this or other manuals for this product.

WARNING

PERSONAL INJURY-STUMBLING HAZARD

Patients can become entangled in the cables and leadwires connected to the device, which could cause the patient to stumble or trip.

Route cables and leadwires in a way to avoid creating a stumbling hazard: keep them off the floor, and route leadwires away from the patient's legs and the healthcare provider's work area.

WARNING

MAGNETIC AND ELECTRICAL INTERFERENCE

Magnetic and electric fields can interfere with the acquisition of ECG readings.

Make sure that all peripheral components operated in the vicinity of the device comply with the relevant EMC requirements. X-ray equipment, MRI devices, radio systems (cellular phones) and so forth, are possible sources of interference because they may emit higher levels of electromagnetic radiation. Verify the performance of the system before use.

WARNING

EXPLOSION HAZARD

Using this device in the presence of anesthetic vapors or liquids can cause explosions.

Do not use this device in the presence of anesthetic vapors or liquids. Only persons with adequate training in the correct use of this device may use this device.

WARNING

PERSONAL INJURY

Contact with patients during defibrillation can cause serious injury or death.

Do not contact patients during defibrillation. Patient signal inputs labeled with the CF symbols with paddles are protected against damage resulting from defibrillation voltages. To ensure proper defibrillator protection, use only GE Healthcare recommended cables and leadwires. Proper placement of defibrillator paddles in relation to the electrodes is required to ensure successful defibrillation.

WARNING

INTERPRETATION HAZARD

Results of the automated QT analysis are not considered a diagnosis.

A qualified physician or cardiologist must review and confirm the measurements and waveforms recorded by the system. It should be used only as an adjunct to the clinical history, symptoms, and results of other tests.

WARNING

ELECTRIC SHOCK HAZARD

Devices which connected to the same Ethernet/LAN with MAC 5 should comply with IEC 60950/IEC60601 or equivalent safety standard.

WARNING

ELECTRIC SHOCK HAZARD

The conductive parts of electrodes and associated connectors for leadwire, including the neutral electrode, should not contact any other conductive parts including earth.

WARNING

INTERPRETATION HAZARD

Computerized interpretation is only significant when used in conjunction with clinical findings.

A qualified physician must overread all computer-generated tracings.

WARNING

IMPROPER USE

This is a prescriptive device.

This equipment is intended for use by or under the direct supervision of a licensed healthcare practitioner.

WARNING

ELECTRIC SHOCK HAZARD/SYSTEM MALFUNCTION

Liquids inside a device can cause electric shock or system malfunction.

Do not allow liquids to enter the device. If liquids enter the device, unplug the power cord, remove the battery and inform your service technician. Do not use the device until it is checked by a service technician.

WARNING

ELECTRIC SHOCK

Improper connection of this equipment may cause electric shock.

To avoid risk of electric shock, this equipment must only be connected to a supply main with protective earth.

WARNING

EQUIPMENT MALFUNCTION/INTERFERENCE

Use of portable phones or other radio frequency (RF) emitting equipment near the system may cause unexpected or adverse operation.

Do not use portable phones or other electronic equipment that may emit radio frequency (RF) near this system.

WARNING

EQUIPMENT MALFUNCTION/INTERFERENCE

Do not use the equipment or system adjacent to, or stacked with, other equipment.

If adjacent or stacked use is necessary, test the equipment or system to verify normal operation in the configuration in which you are using it.

WARNING

ACCESSORIES/COMPONENTS

Adding accessories or components, or modifying the medical device or system, may result in increased EMISSIONS or decreased IMMUNITY of the device or system.

CAUTION

EQUIPMENT MALFUNCTION

Any attempt by unauthorized personnel to service the device could result in equipment malfunction and void the warranty. This equipment contains no user-serviceable parts.

Please contact the authorized service personnel to service the device.

CAUTION

EQUIPMENT FAILURE

Polarizing electrodes (stainless steel or silver constructed) may cause the electrodes to retain a residual charge after defibrillation. A residual charge blocks acquisition of the ECG signal.

Whenever patient defibrillation is a possibility, use non-polarizing electrodes (silver-silver chloride construction) for ECG monitoring.

CAUTION

EXPLOSION HAZARD

Do NOT use in the presence of flammable anesthetics vapors or liquids.

CAUTION

ACCESSORIES (SUPPLIES)

To ensure patient safety, use only parts and accessories manufactured or recommended by GE Medical Systems *Information Technologies, Inc*. Parts and accessories used must meet the requirements of the applicable IEC 60601 series safety standards and essential performance standards, and/or the system configuration must meet the requirements of the IEC 60601-1-1 medical electrical systems standard.

CAUTION

ACCESSORIES (EQUIPMENT)

The use of ACCESSORY equipment not complying with the equivalent safety requirements of this equipment may lead to a reduced level of safety of the resulting system. Consideration relating to the choice shall include: Use of the accessory in the PATIENT VICINITY; and Evidence that the safety certification of the ACCESSORY has been performed in accordance to the appropriate IEC 60601-1 and/or IEC 60601-1-1 harmonized national standard.

CAUTION

DISPOSAL HAZARD

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 local, state, or federal guidelines regulating the disposal of such products.

If you have questions concerning disposal of the product, please contact GE or its representatives.

CAUTION

INTERCONNECTED DEVICES

When several items of medical equipment are interconnected, summation of leakage current must meet the leakage current as per IEC 60601-1.

Connect the device only to the GE approved supplies and accessories.

CAUTION

ISOLATION FROM SUPPLY MAINS

Do not position the device so that it is difficult to operate the disconnection of the AC power supply of the device.

NOTICE

DATA LOSS

Formatting the device’s internal flash drive erases all the data in memory and returns the device to its factory settings.

If possible, back up or record any data that you do not want to lose before formatting the device's internal flash drive.

NOTICE

EQUIPMENT COMPATIBILITY

Compatibility is critical to safe and effective use of this device. Please contact your local sales or service representative prior to installation to verify equipment compatibility.

NOTICE

BATTERY EXPLOSION HAZARD

Batteries may explode in fires.

Do not dispose of the battery by fire or burning. Follow local environmental guidelines concerning disposal and recycling.

H.8 Classification of Medical Device

The device is classified as follows according to IEC 60601-1.

Table H-2 Medical Device Classifications

Category	Classification
Type of protection against electrical shock	Class I, internally powered
Degree of protection against electrical shock	Defibrillation-proof type CF applied part
Degree of protection against harmful ingress of solids and liquids	The Ingress Protection (IP) code for this device is IP20.
Degree of safety of application in the presence of a flammable anesthetic mixture with air or with oxygen or with nitrous oxide	Equipment is not suitable for use in the presence of a flammable anesthetic mixture with air or with oxygen or with nitrous oxide
Method(s) of sterilization or disinfection recommended by the manufacturer	Not applicable
Mode of operation	Continuous operation

H.9 Certification Information

Table H-3 Certification Information

CE 0197	This system bears CE mark 0197 indicating it conforms with the provisions of Council Regulation EU 2017/745 concerning medical devices, and it fulfills the requirements of Annex I of this regulation. The system is in radio-interference protection class B in accordance with EN 55011. The country of manufacture is indicated on the equipment labeling. The product complies with the requirements of standard EN 60601-1-2 “Electromagnetic Compatibility – Medical Electrical Equipment”. The medical device has a lifetime of 7 years with respect to the Council Regulation EU 2017/745 Annex I, Requirement 6.
TÜVRheinland C US	**Medical Equipment** With respect to electric shock, fire, and mechanical hazards only in accordance with IEC 60601-1, and CAN/CSA C22.2 NO. 601.1.

H.10 Recording ECGs during Defibrillation

This equipment is protected against the effects of cardiac defibrillator discharge to ensure recovery, as required by test standards. The patient signal input of the acquisition module is defibrillation-proof. It is not necessary to remove the ECG electrodes prior to defibrillation.

When using stainless steel or silver electrodes, a defibrillator discharge current may cause the electrodes to retain a residual charge causing a polarization or DC offset voltage. This electrode polarization blocks acquisition of the ECG signal. To avoid this condition, if there is a situation where a defibrillation procedure is necessary, use non-polarizing electrodes such as silver/silver-chloride types, which do not form a DC offset voltage when subjected to a DC current.

If you use polarizing electrodes, GE Healthcare recommends disconnecting the leadwires from the patient before delivering the shock.

Electrode defibrillation recovery is the ability of the electrode to allow the ECG trace to return after defibrillation. GE Healthcare recommends using non-polarizing disposable electrodes with defibrillation recovery rating as specified in AAMI EC12.5.2.2.4. AAMI EC12 requires that the

polarization potential of an electrode pair does not exceed 100 mV 5 seconds after a defibrillation discharge.

Refer to the supplies and accessories guide for this system for a list of approved electrodes.

H.11 Modulating Effects in Digital Systems

This section describes the modulating effects that may occur in digital systems of the product.

This device uses digital sampling techniques that may produce some variation in amplitudes of Q, R, and/or S waves from one heart beat to the next, which may be particularly noticeable in pediatric recordings. If you observe this phenomenon, be aware that the origin of amplitude variations is not entirely physiological. For measuring voltages of Q, R, and S waves, GE Healthcare advises using the QRS complexes with the largest deflection of the particular waves.

H.12 Electromagnetic Compatibility (EMC)

Before installing or using the device or system, be aware of the proximity of known radio frequency (RF) sources, such as:

- Radio and TV stations
- Portable and mobile RF communication devices (cell phones, two-way radios)
- High-frequency surgical units, such as diathermy, electrocautery, argon beam coagulators, etc.
- X-ray, CT, or MRI devices

  These devices are also possible sources of interference as they may emit higher levels of electromagnetic radiation.

WARNING

EQUIPMENT MALFUNCTION OR INTERFERENCE

Use of this equipment adjacent to or stacked with other equipment should be avoided because it could result in improper operation. If such use is necessary, this equipment and the other equipment should be observed to verify that they are operating normally.

WARNING

EQUIPMENT MALFUNCTION OR INTERFERENCE

Portable RF communications equipment (including peripherals such as antenna cables and external antennas) should be used no closer than 30 cm (12 inches) to any part of the ECG device, including cables specified by the manufacturer. Degradation of the performance of this equipment could result.

WARNING

PATIENT SAFETY/EQUIPMENT FAILURE

Use of accessories, transducers and cables other than those specified or provided by the manufacturer of this equipment could result in increased electromagnetic emissions or decreased electromagnetic immunity of this equipment and result in improper operation.

H.12.1 Guidance and Manufacturer's Declaration—Electromagnetic Emissions

The system described in this document is intended for use in the specified electromagnetic environment below. It is the responsibility of the customer or user to make sure that this system is used in such an environment.

Table H-4 EMC Emissions Test

Emissions Test	Compliance
RF emissions (Radiated) EN 55011	Group 1 Class B
RF emissions (Conducted) EN 55011	Group 1 Class B
Harmonic emissions IEC 61000-3-2	Class A
Voltage fluctuations/Flicker emissions IEC 61000-3-3	Complies

H.12.2 Guidance and Manufacturer's Declaration—Electromagnetic Immunity

The system described in this document is intended for use in the specified electromagnetic environment below. It is the responsibility of the customer or user to make sure that this system is used in such an environment.

Table H-5 EMC Immunity Test

Immunity Test	EN60601 Test Level	Compliance Level
Electrostatic discharge (ESD) IEC 61000-4-2	± 2, ± 4, ± 8 kV contact ± 2, ± 4, ± 8, ± 15 kV air	± 2, ± 4, ± 8 kV contact ± 2, ± 4, ± 8, ± 15 kV air
Electrical Fast Transient/burst (EFT) IEC 61000-4-4	± 2 kV for power supply lines	± 2 kV for power supply lines
Surge IEC 61000-4-5	± 1 kV line(s) to line(s) ± 2 kV line(s) to earth	± 1 kV line(s) to line(s) ± 2 kV line(s) to earth
Voltage dips, short interruptions, and voltage variations on power supply input lines IEC 61000-4-11	voltage dips for 0% of Un for 0.5 cycles and phase angles of 0 °, 45 °, 90 °, 135 °, 180°, 225 °, 270° and 315° voltage dips for 0% of Un for 1 cycle and phase angles of 0 ° voltage dips for 70% of Un for 25 / 30 cycles and phase angles of 0 ° voltage dips for 70% of Un for 25 / 30 cycles and phase angles of 0 ° Voltage interruptions for 0% of Un for 250 / 300 cycles	voltage dips for 0% of Un for 0.5 cycles and phase angles of 0 °, 45 °, 90 °, 135 °, 180°, 225 °, 270° and 315° voltage dips for 0% of Un for 1 cycle and phase angles of 0 ° voltage dips for 70% of Un for 25 / 30 cycles and phase angles of 0 ° voltage dips for 70% of Un for 25 / 30 cycles and phase angles of 0 ° Voltage interruptions for 0% of Un for 250 / 300 cycles

Continues on the next page

Table H-5 EMC Immunity Test (Table continued)

Immunity Test	EN60601 Test Level	Compliance Level
Power frequency (50/60 Hz) magnetic field IEC 61000-4-8	30 A/m	30 A/m
Conducted RF IEC 61000-4-6	3 Vrms 0.15 MHz to 80 MHz 6 Vrms in ISM bands between 0.15 MHz and 80 MHz 6 Vrms in Amateur radio bands between 0.15-80 MHz	3 Vrms 0.15 MHz to 80 MHz 6 Vrms in ISM bands between 0.15 MHz and 80 MHz 6 Vrms in Amateur radio bands between 0.15-80 MHz
Radiated RF IEC 61000-4-3	3 V/m, 80 MHz - to 2.7 GHz, 80 % AM at 1 kHz	3 V/m, 80 MHz - to 2.7 GHz, 80 % AM at 1 kHz

NOTE

- Do not use portable or mobile RF communications equipment closer to any part of the system, including the cables, than the recommended separation distance calculated for the equation applicable to the frequency of the transmitter.
- Field strengths from fixed transmitters, such as base stations for radio (cellular/cordless) telephones and land mobile radio, AM and FM radio broadcast, and TV broadcast cannot, theoretically, be predicted with accuracy. To assess the electromagnetic environment due to fixed RF transmitters, consider conducting an electromagnetic site survey. If the measured field strength in the location the system is used exceeds the applicable RF compliance level listed in this table, observe the system to verify normal operation. If abnormal performance is observed, additional measures may be necessary, such as reorienting or relocating the system.
- At 80 MHz and 800 MHz, the higher frequency range applies.
- These guidelines may not apply in all situations. Electromagnetic propagation is affected by the reflection from structures, objects, and people.

Table H-6 Test specifications for ENCLOSURE PORT IMMUNITY to RF wireless communications equipment

Test frequency (MHz)	Band 1) (MHz)	Service 1)	Modulation 2)	Maximum power (W)	Distance (m)	IMMUNITY TEST LEVEL (V/m)
385	380 – 390	TETRA 400	Pulse modulation 2) 18 Hz	1,8	0,3	27
450	430 – 470	GMRS 460, FRS 460	FM 3) ± 5 kHz deviation 1 kHz sine	2	0,3	28
710	704 – 787	LTE Band 13, 17	Pulse modulation 2) 217 Hz	0,2	0,3	9
745						
780						
810	800 – 960	GSM 800/900, TETRA 800,	Pulse modulation 2)	2	0,3	28

Continues on the next page

Table H-6 Test specifications for ENCLOSURE PORT IMMUNITY to RF wireless communications equipment (Table continued)

Test frequency (MHz)	Band 1) (MHz)	Service 1)	Modulation 2)	Maximum power (W)	Distance (m)	IMMUNITY TEST LEVEL (V/m)
870		iDEN 820, CDMA 850, LTE Band 5	18 Hz			
930						
1 720	1 700 – 1 990	GSM 1800; CDMA 1900; GSM 1900; DECT; LTE Band 1, 3, 4, 25; UMTS	Pulse modulation 2) 217 Hz	2	0,3	28
1 845						
1 970						
2 450	2 400 – 2 570	Bluetooth, WLAN, 802.11 b/g/n, RFID 2450, LTE Band 7	Pulse modulation 2) 217 Hz	2	0,3	28
5 240	5 100 – 5 800	WLAN 802.11 a/n	Pulse modulation 2) 217 Hz	0,2	0,3	9
5 500						
5 785						

NOTE

If necessary to achieve the IMMUNITY TEST LEVEL, the distance between the transmitting antenna and the ME EQUIPMENT or ME SYSTEM may be reduced to 1 m. The 1 m test distance is permitted by IEC 61000-4-3.

1) For some services, only the uplink frequencies are included.

2) The carrier shall be modulated using a 50 % duty cycle square wave signal.

3) As an alternative to FM modulation, 50 % pulse modulation at 18 Hz may be used because while it does not represent actual modulation, it would be worst case.

H.12.3 Essential Performance

The essential performance of the system may be lost or degraded because of electromagnetic disturbances. For expected degradations and instructions of the basic safety and essential performance maintance in the case of electromagnetic disturbances, see the table below:

Essential Performance	Degradation Caused by Electromagnetic Disturbances	Essential Performance Maintainance
Defibrillation Protection	No degradation.	Not applicable.

Continues on the next page

Essential Performance	Degradation Caused by Electromagnetic Disturbances	Essential Performance Maintainance
ECG Measurements *	Temporary function loss during Electrostatic Discharge (ESD) and Electrical Fast Transient/Burst (EFT) disturbances.	The device resumes normal operation within 10 seconds after the disturbance is removed: • No operator setting or stored data loss; • Will continue to perform its intended functions; • Will maintain the essential performance.
FILTERS (Including Line Frequency Disturbance FILTERS)	No degradation.	Not applicable.
* Essential performance is amplitude measurement accuracy as defined by IEC 60601-2-25 Section 202.6.2. The difference for each amplitude measurement shall not deviate from the reference value by more than ± 50 µV for reference values ≤ 500 µV, or by more than 5 % or ±100 µV (whichever is greater) for reference values > 500 µV.		

H.13 Biocompatibility

The parts of the system described in this manual that come into contact with the patient during the intended use, including all accessories, fulfill the biocompatibility requirements of the applicable standards. If you have questions in this matter contact your GE Healthcare representative.

H.14 Legal Notice

GE Healthcare software contains several fields that can be populated before performing an ECG. Some of these fields are required, others are optional and left to the user to assess whether they are needed to perform the exam. The field **Race** is one of these optional fields. Race has been acknowledged by the medical profession as useful to analyze some pathologies. You should be aware that, in some jurisdictions, the processing of data revealing an individual's racial origin is subject to legal requirements, such as obtaining the patient's prior consent. If you elect to collect this type of data, it is your responsibility to make sure that you comply with all applicable legal requirements.

H.15 Supplies and Accessories

This section is in regard to the supplies and accessories you may purchase for your product.

You should use only supplies and accessories recommended by GE Healthcare. For a list of recommendations, refer to the supplies and accessories guide for this system.

Contact GE Healthcare before using anything that is not recommended for this system.

H.16 Responsibility of the Manufacturer

This section describes the responsibility of GE Healthcare as the manufacturer of your product.

GE Healthcare is responsible for the safety, reliability, and performance of hardware supplied by GE Healthcare only if the conditions below are met:

- Assembly operations, extensions, readjustments, modifications, or repairs are performed by persons authorized by GE Healthcare.

- The electrical installation of the room where the device is used complies with the requirements of the appropriate local, state, and other government regulations.
- The equipment is used in accordance with the instructions for use.

H.17 Responsibility of the Purchaser/Customer

The customer is responsible for providing appropriate desks, chairs, electrical wall outlets, network connections, and analog phone lines, and for locating any of the system components described in the manuals in compliance with all local, state, and national codes.

Lack of data security may compromise patient privacy. GE Healthcare recommends that you take appropriate steps to secure the privacy of communication on your network when using this product.

H.18 Notification to Member States

The user and/or patient should report any serious incident that has occurred in relation to the device to the manufacturer and the competent authority of the Member State in which the user and/or patient is established.

H.19 Warranty Information

This device is considered GE Healthcare-supplied hardware. Only authorized GE Healthcare service personnel should service the device. 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 Healthcare or to one of their authorized agents.

H.20 Product and Packaging Information

The illustrations and tables in this section describe the labels and their location on your device and its packaging.

Contact your local GE Healthcare service representative, if the device packaging is:

- Damaged.
- Accidentally opened.
- Exposed to an environment that does not meet the prescribed conditions.

H.20.1 MAC 5 A4 Hardware Label Locations

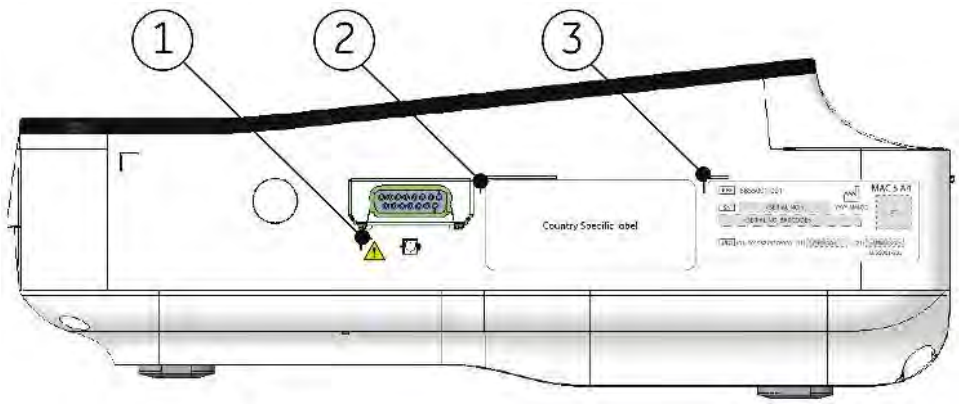


Table H-7 Label Descriptions on the Right Side of the Device

Item	Label	Description
1	General Warning Symbol	See H.23 Symbol Descriptions on page 342 for an explanation of the label.
2	Country-specific Label	Country registration information.
3	Serial Number Label	Device identification. See H.21 Serial Number Label on page 340 for a description of the label contents.

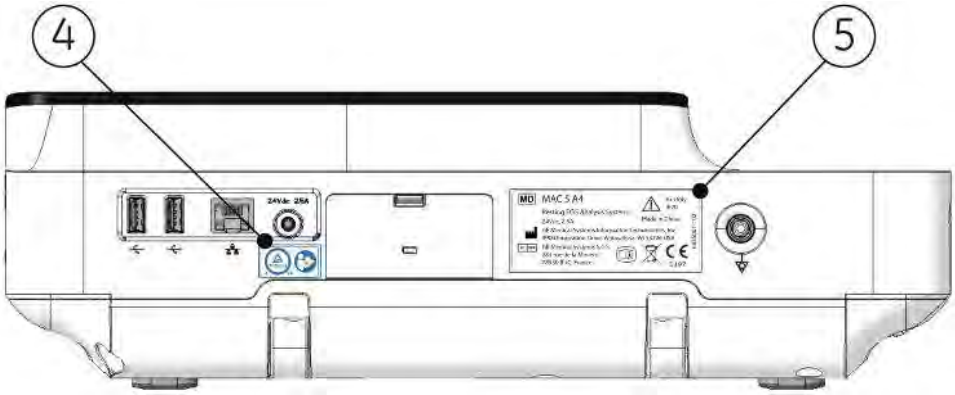


Table H-8 Label Descriptions on the Back Side of the Device

Item	Label	Description
4	TUV and IFU Symbol Label	See H.9 Certification Information on page 321 and H.23 Symbol Descriptions on page 342 for a description of the label contents.
5	Product and Rating Label	Regulatory and cautionary information. See H.22 Device Address Label and Rating Plate on page 341 for an explanation of the label.

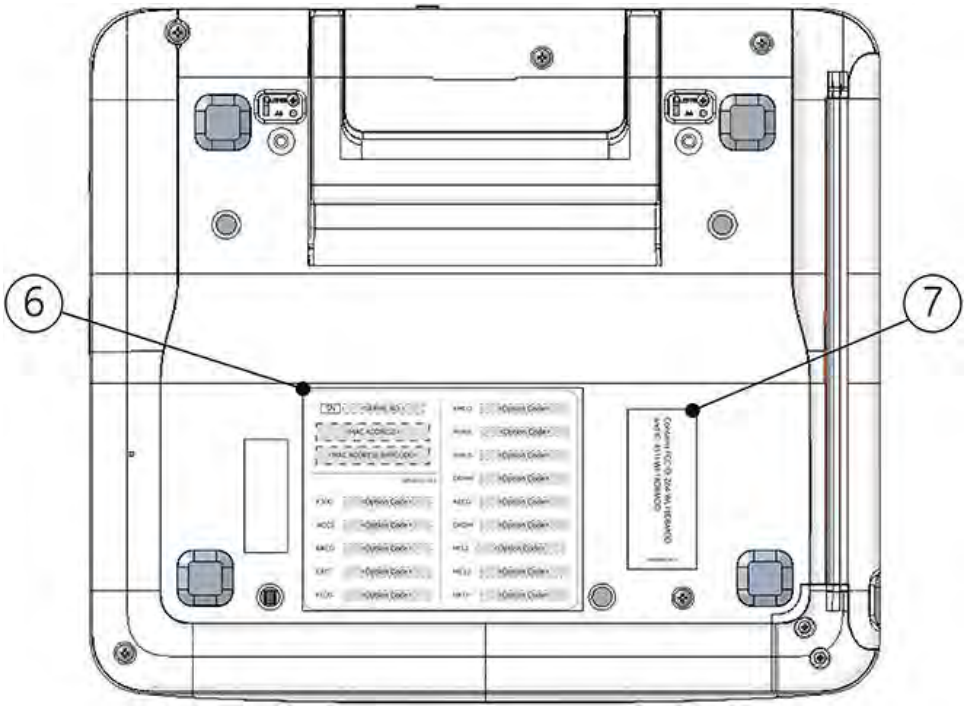
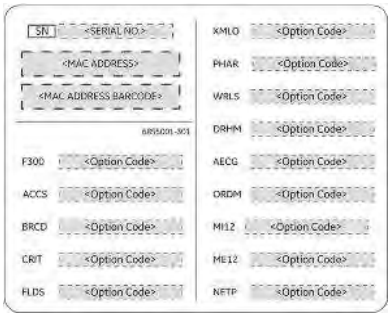


Table H-9 Label Descriptions on the Bottom of the Device

Item	Label	Description
6	Option Code and MAC Address Label	The MAC address of the wired network card. Use the option codes to set up the purchased options in your system. 
7	Wireless Label	The wireless registration information. 

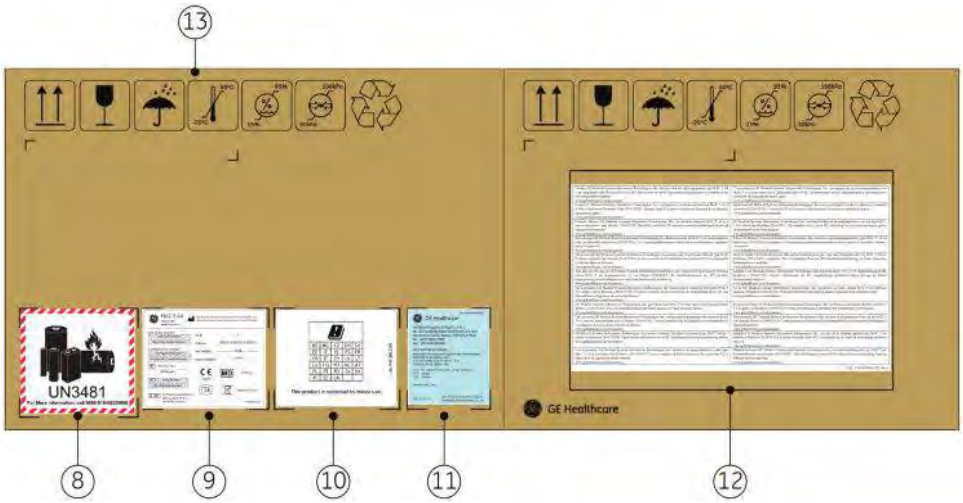
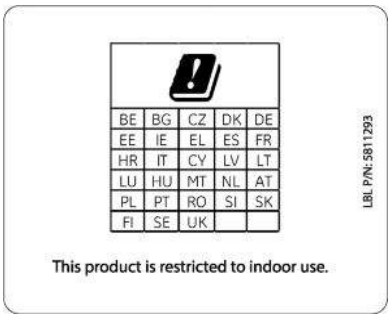
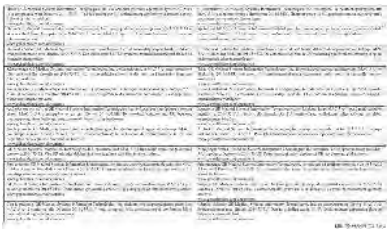


Table H-10 Label Descriptions on the Shipping Package of the Device

Item	Label	Description
8	Battery Shipping Label	Lithium Ion battery damaged caution label. 
9	Shipping Label	Regulatory and safety shipping information. 
10	Radio Equipment Directive (RED) Label	The Radio Equipment Directive registration information. 

Continues on the next page

Table H-10 Label Descriptions on the Shipping Package of the Device (Table continued)

Item	Label	Description
11	Battery Transportation Label	The battery transportation information. 
12	Radio Equipment Directive (RED) European Union Declaration of Conformity Guidance	The Radio Equipment Directive (RED) European Union Declaration of Conformity Guidance. 
13	Environmental Symbols	Safety indicators required for shipping. For a full description of symbols, see H.23 Symbol Descriptions on page 342.

H.20.2 MAC 5 A5 Hardware Label Locations

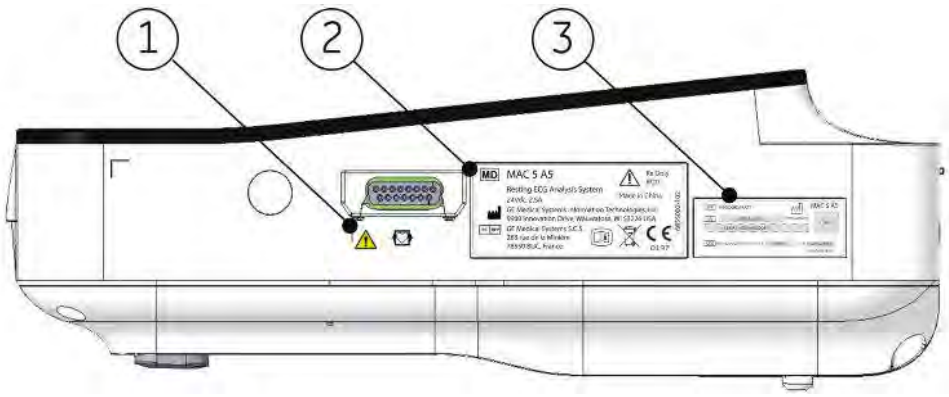


Table H-11 Label Descriptions on the Right Side of the Device

Item	Label	Description
1	General Warning Symbol	See H.23 Symbol Descriptions on page 342 for an explanation of the label.
2	Product and Rating Label	Regulatory and cautionary information. See H.22 Device Address Label and Rating Plate on page 341 for an explanation of the label.

Continues on the next page

Table H-11 Label Descriptions on the Right Side of the Device (Table continued)

Item	Label	Description
3	Serial Number Label	Device identification. See H.21 Serial Number Label on page 340 for a description of the label contents.

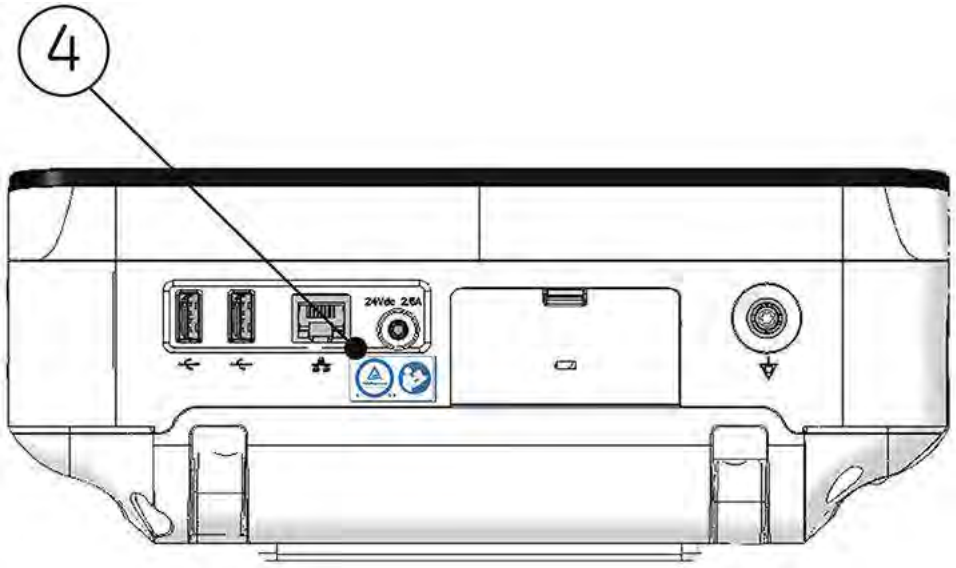


Table H-12 Label Descriptions on the Back Side of the Device

Item	Label	Description
4	TUV and IFU Symbol Label	See H.9 Certification Information on page 321 and H.23 Symbol Descriptions on page 342 for a description of the label contents.

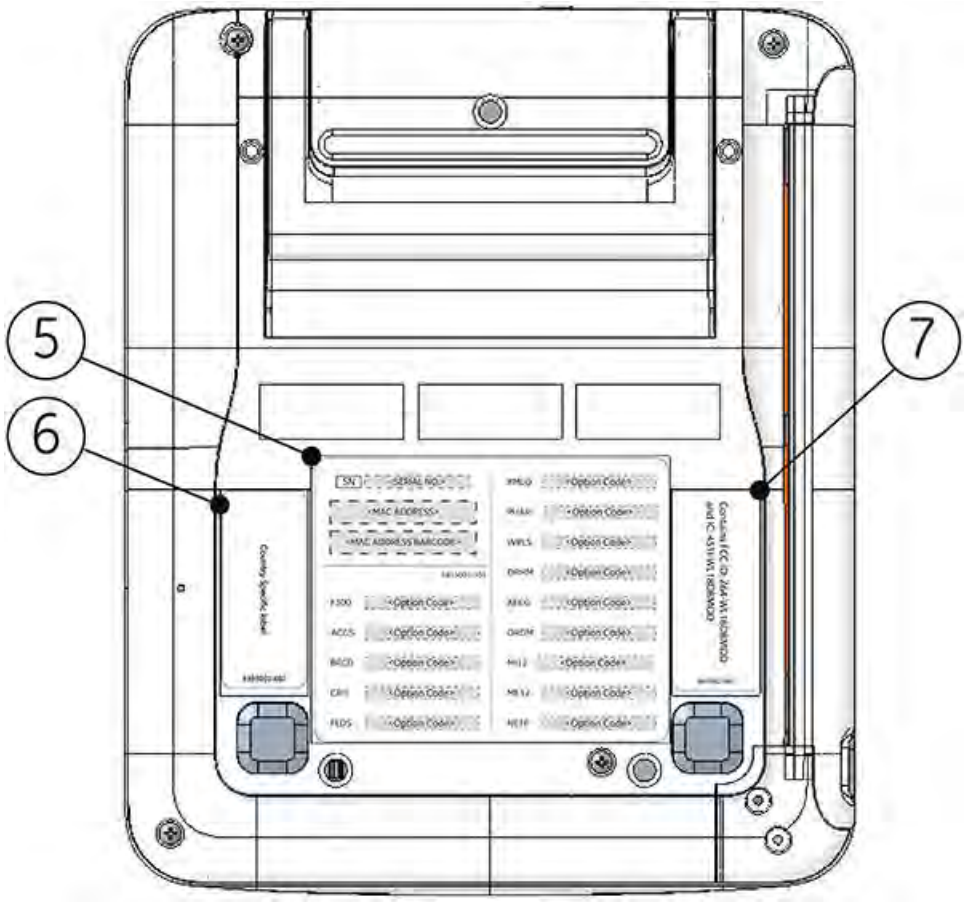
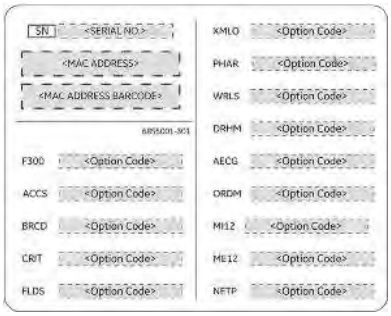


Table H-13 Label Descriptions on the Bottom of the Device

Item	Label	Description
5	Option Code and MAC Address Label	The MAC device address of the device. Use the option codes to set up the purchased options in your system. 
6	Country Specific Label	Country registration information.
7	Wireless Label	The wireless registration information. 

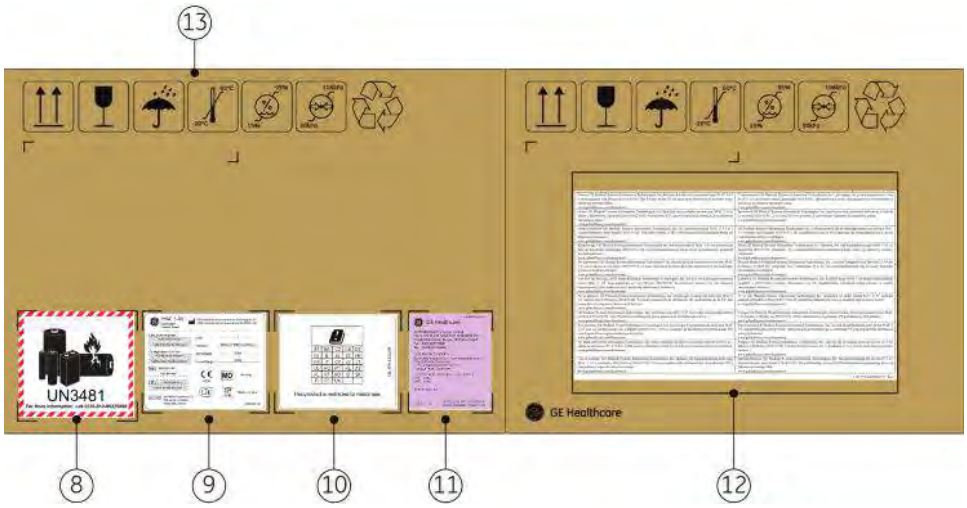
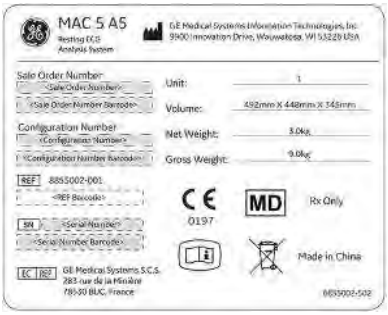
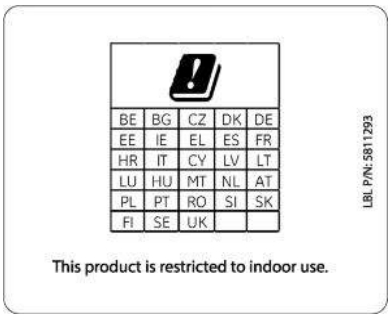


Table H-14 Label Descriptions on the Shipping Package of the Device

Item	Label	Description
8	Battery Shipping Label	FRAGILE—Lithium Ion batteries can cause fire if damaged. 
9	Shipping Label	Regulatory and safety shipping information. 

Continues on the next page

Table H-14 Label Descriptions on the Shipping Package of the Device (Table continued)

Item	Label	Description
10	Radio Equipment Directive (RED) Label	The Radio Equipment Directive registration information. 
11	Battery Transportation Label	The battery transportation information. 
12	Radio Equipment Directive (RED) European Union Declaration of Conformity Guidance	Radio Equipment Directive (RED) European Union Declaration of Conformity Guidance. 
13	Environmental Symbols	Safety indicators required for shipping. For a full description of symbols, see H.23 Symbol Descriptions on page 342.

H.20.3 MAC 5 Lite Hardware Label Locations

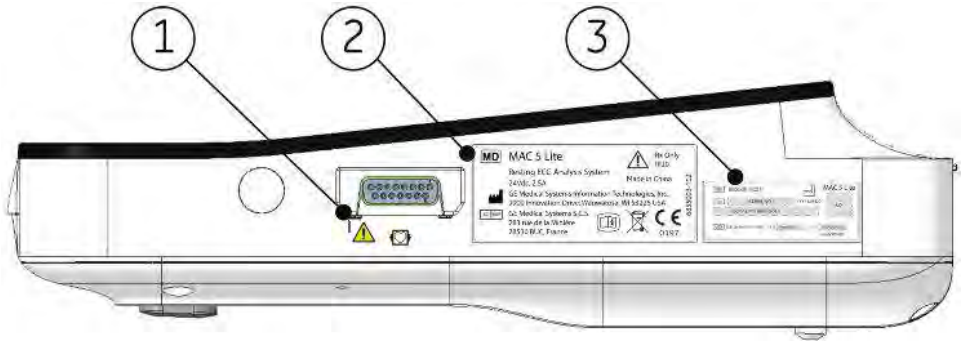


Table H-15 Label Descriptions on the Right Side of the Device

Item	Label	Description
1	General Warning Symbol	See H.23 Symbol Descriptions on page 342 for an explanation of the label.
2	Product and Rating Label	Regulatory and cautionary information. See H.22 Device Address Label and Rating Plate on page 341 for an explanation of the label.
3	Serial Number Label	Device identification. See H.21 Serial Number Label on page 340 for a description of the label contents.

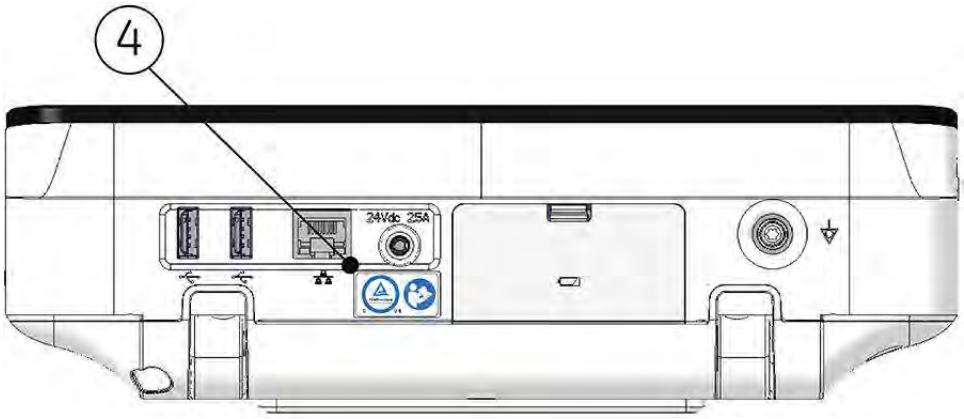


Table H-16 Label Descriptions on the Back Side of the Device

Item	Label	Description
4	TUV and IFU Symbol Label	See H.9 Certification Information on page 321 and H.23 Symbol Descriptions on page 342 for a description of the label contents.

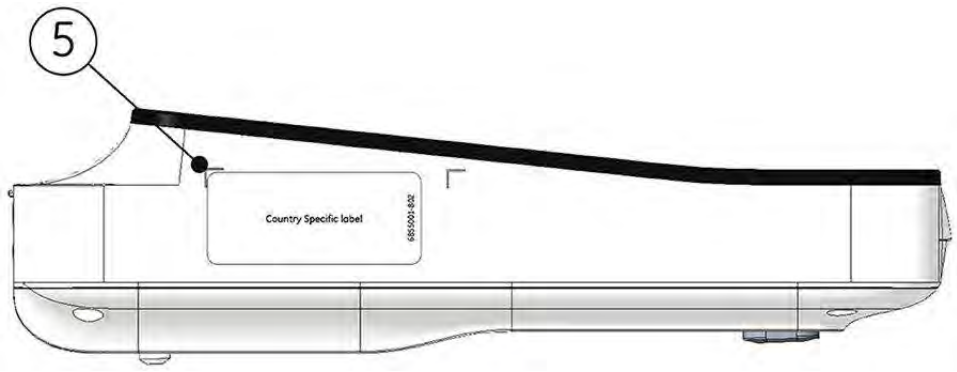


Table H-17 Label Descriptions on the Left Side of the Device

Item	Label	Description
5	Country Specific Label	Country registration information.

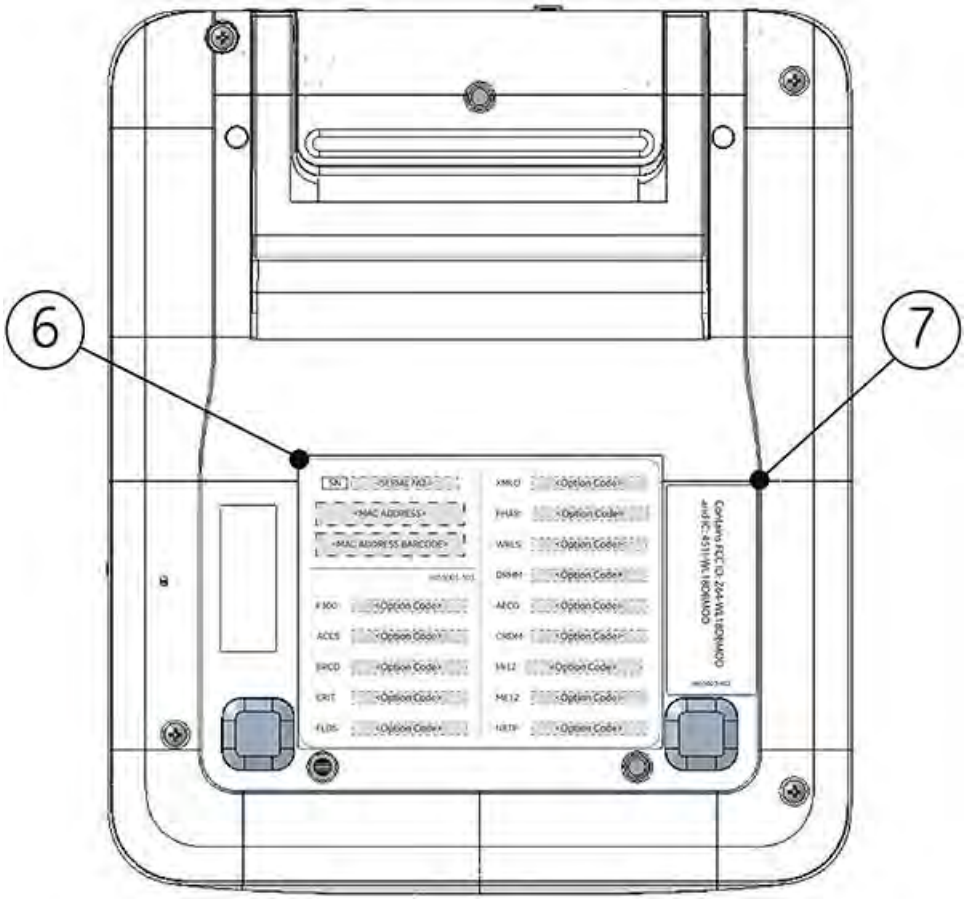
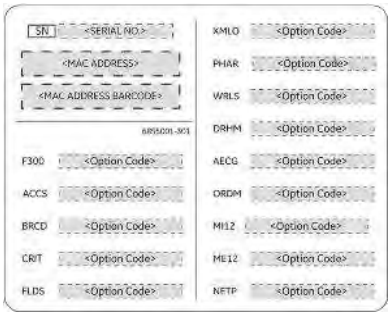


Table H-18 Label Descriptions on the Bottom of the Device

Item	Label	Description
6	Option Code and MAC Address Label	The MAC device address of the device. Use the option codes to set up the purchased options in your system. 

Continues on the next page

Table H-18 Label Descriptions on the Bottom of the Device (Table continued)

Item	Label	Description
7	Wireless Label	The wireless registration information. 

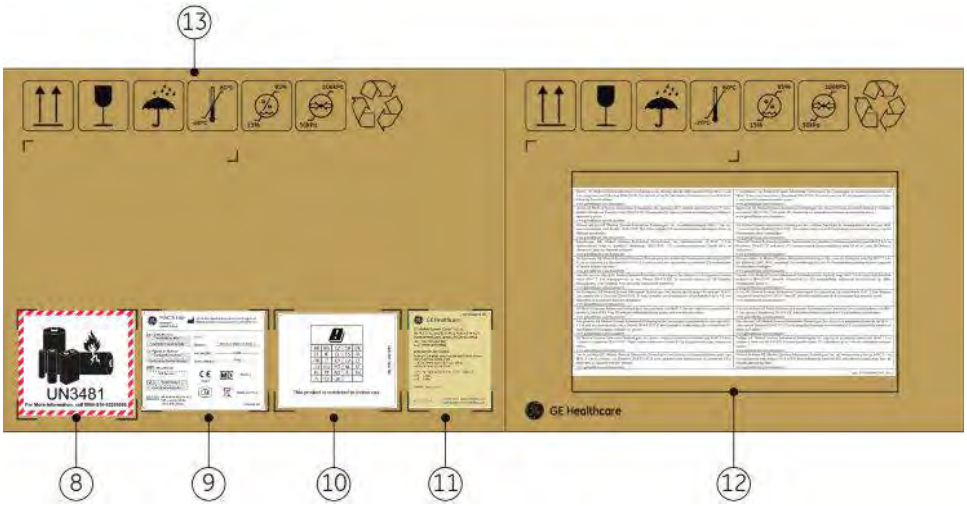
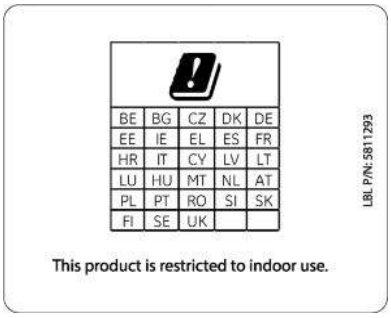


Table H-19 Label Descriptions on the Shipping Package of the Device

Item	Label	Description
8	Battery Shipping Label	FRAGILE—Lithium Ion batteries can cause fire if damaged. 

Continues on the next page

Table H-19 Label Descriptions on the Shipping Package of the Device (Table continued)

Item	Label	Description
9	Shipping Label	Regulatory and safety shipping information. 
10	Radio Equipment Directive (RED) Label	The Radio Equipment Directive registration information. 
11	Battery Transportation Label	The battery transportation information. 
12	Radio Equipment Directive (RED) European Union Declaration of Conformity Guidance	Radio Equipment Directive (RED) European Union Declaration of Conformity Guidance. 
13	Environmental Symbols	Safety indicators required for shipping. For a full description of symbols, see H.23 Symbol Descriptions on page 342.

H.21 Serial Number Label

The serial number labels are in the format as follows:

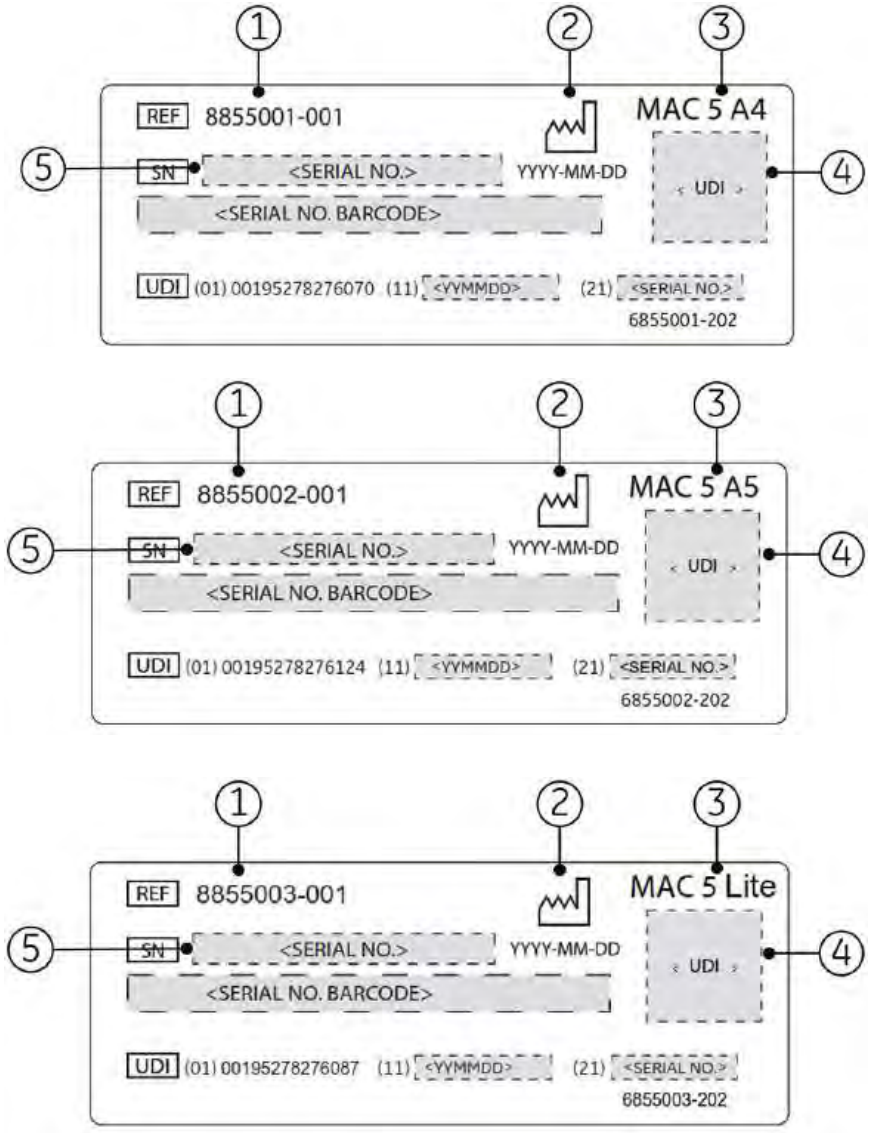


Table H-20 Serial Number Label Format

Item	Description
1	Product Part Number
2	Date of Manufacture in YYYY-MM-DD Format
3	Product Mode
4	UDI Barcode
5	Device Serial Number

H.22 Device Address Label and Rating Plate

The device address label and rating plate is in the format as follows:

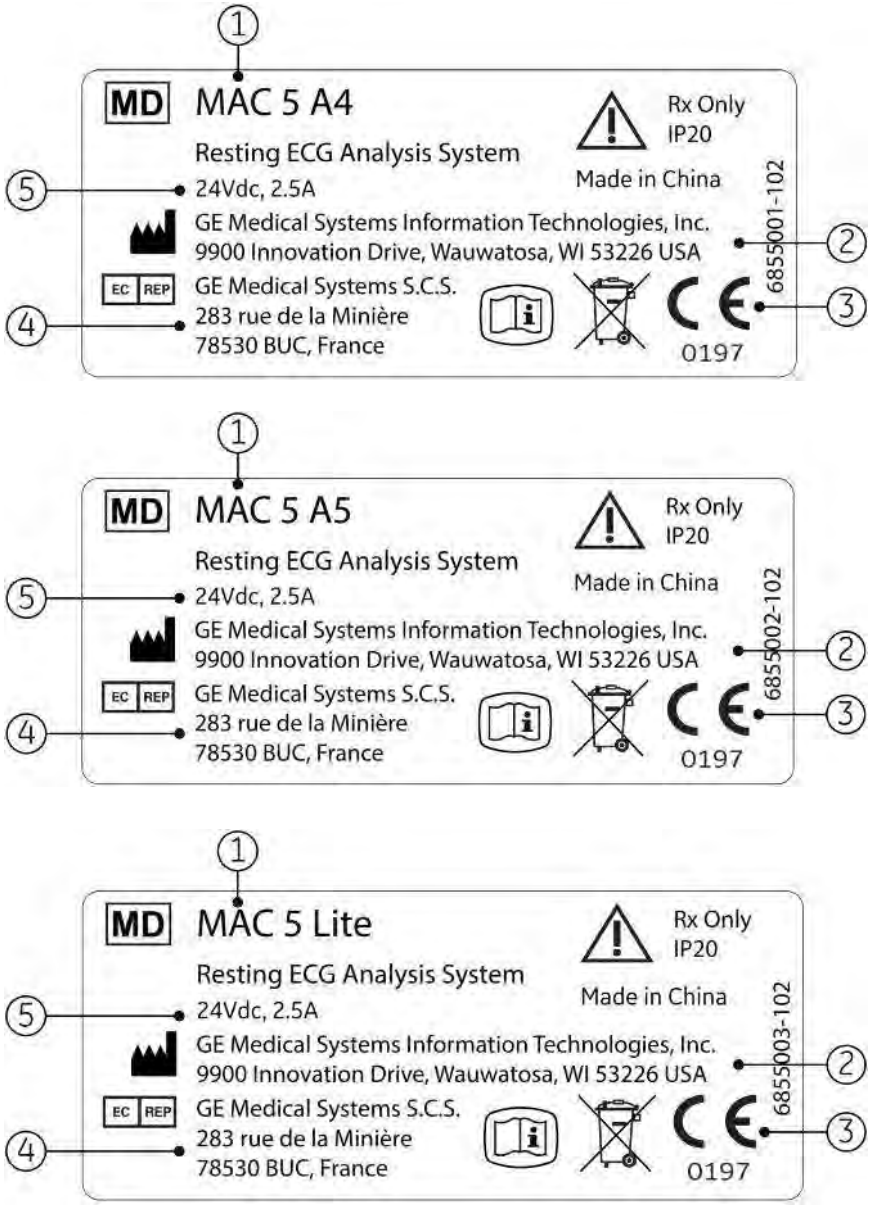


Table H-21 Device Address Label and Rating Plate Format

Item	Description
1	Product Mode
2	Manufacturer Name and Address
3	Symbols See H.23 Symbol Descriptions on page 342 for a description of the symbols used on this label.
4	Authorized European Representative Information
5	Electrical Rating of the Device

H.23 Symbol Descriptions

For equipment symbols not shown, refer to the original equipment manufacturer (OEM) manuals.

Table H-22 Symbols, Icons, and Descriptions on the device or packaging

Symbol	Description
	**Catalog or Orderable Part Number** The manufacturer's catalog or part number.
	**Serial Number** The manufacturer's serial number.
	**Batch Code or Lot Number** The manufacturer's batch code or lot number.
	**Medical Device** The device is used for medical purpose.
	**Date of Manufacture** (Year-Month-Date) The original manufacture date for this device.
	**Manufacturer** The name and address for the manufacturer of this device. It may also include the date it was manufactured.
	**Authorized Representative in the European Community** The name and address of the authorized representative in the European Community for this device.
Rx Only	**Rx Only** US Federal law restricts this device to sale by or on the order of a physician.
	**12SL** The device uses the Marquette™ 12SL ECG Analysis Program to analyze and interpret ECG readings.
IP20	**IP Code (Ingress Protection Rating)** Protects the equipment inside the enclosure against ingress of solid foreign objects having a diameter of 12,5 mm and greater.
	**CE Mark** The device or product conforms with applicable EU (European Union) directives.
	**Regulatory Compliance Mark (RCM)** Compliance with electrical safety, EMC, EME, and telecommunications requirements, as applicable, to the product. Required for Australia and New Zealand.
	**Wireless Communication** The equipment can be connected through wireless communication.

Continues on the next page

Table H-22 Symbols, Icons, and Descriptions on the device or packaging (Table continued)

Symbol	Description
	**Waste Electrical and Electronic Equipment (WEEE)** Indicates this equipment contains electrical or electronic components that must not be disposed of as unsorted municipal waste, but collected separately. Contact an authorized representative of the manufacturer for information for the decommissioning of your equipment.
	**Consult Instructions for Use** Consult the operating instructions.
	**Electronic Instructions for Use (eIFU)** Consult the electronic instructions for use.
	**Follow Instructions For Use** Read and understand the operator's manual before using the device or product. *As a mandatory action sign, this symbol is identified by a blue background and white symbol.*
	**CAUTION**  CONSULT ACCOMPANYING DOCUMENTS There may be specific warnings or precautions associated with the device that are not otherwise found on the label. Consult the accompanying documentation for more information about safely using this device.
	**General Warning Sign** Protection of the ME EQUIPMENT against the effects of the discharge of a cardiac defibrillator is dependent upon the use of GE recommended ECG cables.
	**This Way Up** The correct upright position of the package.
	**Keep Dry** You need to keep the container away from rain and other sources of moisture.
	**Can Be Recycled** You may recycle this material or device. Recycle or dispose of in accordance with local, state, or country laws.
	The upper and lower temperature limits for the transportation and handling of this package. They are indicated next to the upper and lower horizontal lines.
	The upper and lower humidity limits for the transportation and handling of this package. They are indicated next to the upper and lower horizontal lines.

Continues on the next page

Table H-22 Symbols, Icons, and Descriptions on the device or packaging (Table continued)

Symbol	Description
	The upper and lower barometric pressure limitations for the transportation and handling of this package. They are indicated next to the upper and lower horizontal lines.
	**Defibrillation-proof Type CF Applied Part** Identifies a defibrillation-proof type CF applied part on medical equipment that complies with IEC 60601–1. This device meets the requirements for protection against electric shock for an earth-free (floating) applied part (one intended for contact with patients) for cardiac application.
	**No User– or Field-serviceable Parts** Do not open or disassemble the device for any reason.
	**Protective Earth** (ground) Identifies the terminal of a protective earth (ground) electrode or any terminal that is intended for connection to an external conductor for protection against electric shock in case of a fault.
	**Do Not Stack** You should not stack the container or place a load on the container.
	**WARNING**  ELECTRIC SHOCK Indicates the presence of hazardous energy circuits or electric shock hazards. To reduce the risk of electric shock hazards, do not open this enclosure. Refer servicing to qualified personnel.
	Equipotentiality Connect non-grounded peripheral devices to ensure equipotential.
	**Environmental Friendly Use Period (EFUP)** Per Chinese standard SJ/T11364–2014, the number of years from the date of manufacture during which you can use the product before any restricted substances are likely to leak, causing a possible environmental or health hazard. **NOTE** • If the device contains less than the maximum concentration of restricted substances, the symbol contains a lowercase ***e*** • This is also referred to as China RoHS.
	**Fragile** The contents are fragile. Handle with care.

Continues on the next page

Table H-22 Symbols, Icons, and Descriptions on the device or packaging (Table continued)

Symbol	Description
 	**CAUTION** SAFETY GROUND PRECAUTION Pulling on the cable can cause the cord to deteriorate resulting in electrical problems. Remove the power cord from the mains source by grasping the plug. DO NOT pull on the cable.
	**Contains <heavy metal chemical symbol>** This equipment contains heavy metal and must not be disposed of as unsorted municipal waste but collected separately. The example shows Lithium Ion.
	**Pushing Prohibited**
	**Unique Device Identification** Indicates a unique marking for identification of the medical device.
	**Authorised Representative in Switzerland** The name and address of the authorised representative in Switzerland for this device.

H.24 Serial Number Format

Each device has a serial number that uniquely identifies the device and provides important information about the device. The serial number format is shown in the illustration below:

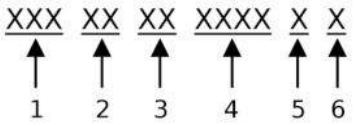


Table H-23 Serial Number Format

Item	Name	Description
1	Product Code	A three-character code that uniquely identifies the product line.
2	Year Manufactured	A two-digit code identifying the year the device was manufactured. Values range from 00 to 99. For example: 00 = 2000, 04 = 2004, 17 = 2017 (and so on).
3	Fiscal Week Manufactured	A two-digit code identifying the week the device was manufactured. Values range from 01 to 52. GE Healthcare's fiscal weeks correspond to the calendar week. For example, 01 = the first week in January.
4	Product Sequence	A four-digit number identifying the order in which this device was manufactured. Values range from 0001 to 9999.

Continues on the next page

Table H-23 Serial Number Format (Table continued)

Item	Name	Description
5	Manufacturing Site	A one-letter code identifying the site where the device was manufactured. For example, F = Milwaukee, N = Freiburg, P = Bangalore, W = Wuxi, H = Helsinki, S = Mexico
6	Miscellaneous Characteristic	A one-letter code identifying manufacturing status. For example, P = the device is a prototype, R = the device was refurbished, U = the device was upgraded to meet the specifications of another product code, A = device is in production.

H.25 Unique Device Identifier

Medical devices require a unique marking for identification—the Unique Device Identifier (UDI). In the event that you need the UDI for this product, check the product label on the back of the device.

H.26 Wireless Regulations

The wireless and wired LAN functionality of the MAC 5 A4/MAC 5 A5/MAC 5 Lite is used to retrieve ECG orders and send ECG reports to an ECG Management System. In addition, the wireless and wired LAN functionality can be used to interface to other hospital information systems to provide additional data to the care giver operating the electrocardiograph. These tasks are an adjunct to the device's intended use of acquiring, analyzing, displaying and printing an electrocardiogram. Because the wireless and wired LAN functionality is not required for the device to fulfill its intended use, network performance is not critical to the performance of the device. Furthermore, the MAC 5 A4/MAC 5 A5/MAC 5 Lite does not transmit any real-time data or alarm information over the network. Network Quality of Service (QoS) parameters such as reliability of data transmission, latency, transfer rate, error rate, and priority levels are not critical to the MAC 5 A4/MAC 5 A5/MAC 5 Lite functionality and are not specified.

H.26.1 FCC Compliance

This device complies with part 15 of the FCC Rules. Operation is subject to the two conditions below: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

"Harmful interference" is defined in 47 CFR §2.1 by the FCC as follows: Interference which endangers the functioning of a radionavigation service or of other safety services or seriously degrades, obstructs, or repeatedly interrupts a radio communication service operating in accordance with the [ITU] Radio Regulations.

CAUTION

CHANGES OR MODIFICATIONS TO THIS UNIT NOT EXPRESSLY APPROVED BY THE PARTY RESPONSIBLE FOR COMPLIANCE COULD VOID THE USER'S AUTHORITY TO OPERATE THE EQUIPMENT.

NOTE

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed

and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the measures below:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Limited by local law regulations, version for North America does not have region selection option.

To satisfy FCC RF exposure requirements, a separation distance of 20 cm or more should be maintained between the antenna of this device and persons during device operation.

To ensure compliance, operations at closer than this distance is not recommended.

H.26.2 IC Compliance

This device contains licence-exempt transmitter(s)/receiver(s) that comply with Innovation, Science and Economic Development Canada's licence-exempt RSS(s). Operation is subject to the two conditions below:

1. This device may not cause interference.
2. This device must accept any interference, including interference that may cause undesired operation of the device.

This equipment complies with radio frequency exposure limits set forth by the Innovation, Science and Economic Development Canada for an uncontrolled environment.

This equipment should be installed and operated with a minimum distance of 20 cm between the device and the user or bystanders.

This device must not be co-located or operating in conjunction with any other antenna or transmitter.

The device for operation in the band 5150-5250 MHz is only for indoor use to reduce the potential for harmful interference to co-channel mobile satellite systems;

H.26.3 RED Information

The MAC 5 embedded wireless module complies with CE RED 2014/53/EU.

This product is restricted to indoor use.

Frequency Range	2.4 GHz frequency bands: 2.4-2.483 GHz 5 GHz frequency bands: 5.15-5.35 GHz, 5.47-5.725 GHz

Continues on the next page

Modulation Type	CCK/DSSS/OFDM
Maximum Effective Radiated Power (ERP)	20 dBm

H.27 Declaration of Conformity

GE Healthcare

EU DECLARATION OF CONFORMITY

Following the provisions of the medical devices regulation 2017/745

ROHS directive 2011/65/EU and Radio Equipment Directive 2014/53/EU.

We:

Manufacturer	EU Authorized Representative
GE Medical Systems Information Technologies, Inc.	GE Medical Systems SCS
9900 Innovation Drive	283 rue de la Minière
Wauwatosa, WI 53226, USA	78530 BUC, France
Single Registration Number (SRN): US-MF-000017529	SRN: FR-AR-000000344

Manufacturing Site

Manufacturing Facility 1

GE Medical Systems (China)Co., Ltd

No.19 Changjiang Road, Wuxi National Hi-Tech Development Zone
Jiangsu, 214028, China

Manufacturing Facility 2

GE Medical Systems Information Technologies

CRITIKON DE MEXICO S. de R.L. de C.V.

Calle Valle del Cedro 1551- Juarez- 32575 CHIHUAHUA-MEXICO

Declare under our sole responsibility that the device:

GE Healthcare

MAC 5 A4/ MAC 5 A5/ MAC 5 Lite Resting ECG Analysis System

Basic UDI-DI: 8406821BUG00244HA

Model Identification/GTIN Numbers:

Model	Identification Number	GTIN Number
MAC 5 A4	8855001-001	00195278276070
MAC 5 A5	8855002-001	00195278276124
MAC 5 Lite	8855003-001	00195278276087

Intended Purpose:

The MAC 5 A4/ MAC 5 A5/ MAC 5 Lite Resting ECG Analysis System is intended to acquire, analyze, display, and record electrocardiographic information from adult or pediatric populations. Basic system delivers 3, 6, or 12 lead ECG's and interpretive analysis. Transmission and reception of ECG data and other clinical data to and from a central clinical information system is optional.

The MAC 5 A4/ MAC 5 A5/ MAC 5 Lite Resting ECG Analysis System is intended to be used under the direct supervision of a licensed healthcare practitioner, by trained operators in a hospital, medical professional's facility or wherever ECG testing is performed.

GMDN Code and description: 16231, Interpretive multichannel electrocardiograph

EMDN Code and description: Z120503, Electrocardiographs

Class: IIa

Classification rule (Annex VIII): Rule 10

SIGNATURE:

15-Feb-2022

Lee Bush
Director, Regulatory Affairs
Wauwatosa, WI

Date

GE Healthcare

To which this declaration relates is in conformity with the requirements of the medical devices regulation 2017/745 that apply to it. In addition, the product is in conformity with the requirements of the directive 2011/65/EU on the restriction of the use of certain hazardous substances in electrical and electronic equipment (as assessed by the manufacturer)

This conformity is based on the following elements:

- Technical Documentation reference DOC2617643, of the product to which this declaration relates.
- EC certificate N HZ 2214580 1.
  - Conformity assessment procedure followed: Annex IX, Chapters I, III
  - Delivered by TÜV Rheinland LGA Products GmbH (0197)
- List of applicable Standards: Refer to General Safety and Performance Requirement (DOC2272151)

We, manufacturer, declare under our sole responsibility that:

MAC 5 A4/ MAC 5 A5/ MAC 5 Lite Resting ECG Analysis System equipped with TI WL18x7MOD WLAN module

To which this declaration relates is in conformity with the requirements of the Radio Equipment Directive 2014/53/EU which applies to it.

This conformity is based on the following elements:

- The device conforms to the Directive 2014/53/EU through Annex II-Internal Production Control.
- List of standards applied : Refer to General Safety and Performance Requirement (DOC2272151)

SIGNATURE:

15-Feb-2021

Lee Bush
Director, Regulatory Affairs
Wauwatosa, WI

Date

End of Document

Glossary

ACS Acute Coronary Syndrome

ADT Admission, Discharge, Transfer

Filter A filter sets the upper frequency limit for the ECG waveform displayed on the Acquisition screen and the printout. Selecting a filter eliminates signals that exceed that frequency. The smaller the filter selected, the more signal is filtered out. For example, a filter of 40 Hz displays only signals less than 40 Hz; signals greater than 40 Hz are ignored.

Gain Gain indicates how many mm represent 1 mV of waveform data on the screen and printout. You can change the gain to modify the display or printout of the waveform to your preference. Changing the gain changes the amplitude of the waveforms. A higher gain makes the amplitude of the waveform appear higher; a lower gain makes the amplitude of the waveform appear lower.

The 10/5 mm/mV setting is used to display the limb leads (I, II, III, aVr, aVI, and aVf) at 10mm/mV and chest leads (V1 to V6) at 5 mm/mV. This is done to reduce or prevent waveform overlap in the chest leads, while avoiding tiny waveforms in the limb leads.

HIS Hospital Information System

LAN Local Area Network

Speed Speed indicates the speed the ECG waveform displays on the screen and rhythm printout. You can change the speed to render the waveform slower or faster to aid in viewing or analysis of the waveform. A faster speed makes the waveform display more stretched out; a slower speed makes the waveform display closer together.

WLAN Wireless Local Area Network

GE Medical Systems *Information Technologies, Inc.*
9900 Innovation Drive
Wauwatosa, WI 53226 USA

GE Medical Systems S.C.S.
283 rue de la Minière
78530 BUC, France

GE Medical Systems *Information Technologies*, Inc., doing business as GE HealthCare.

GE HealthCare

www.gehealthcare.com