

Cell Saver[®] Elite[®]+
Cell Saver[®] Elite[®]

Connectivity Upgrade
User Manual Addendum

CE₀₁₂₃

120857-IE(AB)
June 2017



HAEMONETICS[®]

Publication Information

Publication Date June 2017

Part Number 120857-IE(AB)

Copyright Notice © 2016, 2017 Haemonetics Corporation

The contents of this manual are the property of the Haemonetics Corporation. Any information or descriptions contained in this manual may not be reproduced and released to any of the general public, or used in conjunction with any professional instruction without written consent of Haemonetics Corporation, USA.

Confidential/Proprietary Notices Use of any portion(s) of this document to copy, translate, disassemble or decompile, or create or attempt to create by reverse engineering (or otherwise) the source code from the object code of Haemonetics products is expressly prohibited.

Disclaimer

This manual is intended as a guide to provide the user with necessary instructions on the proper use and maintenance of certain Haemonetics Corporation products. This manual should be used in conjunction with instruction and training supplied by qualified Haemonetics personnel.

Any failure to follow the instructions as described, including use of materials or products not provided or recommended by Haemonetics, could result in impaired product function, injury to the user or others, or void applicable product warranties. Haemonetics accepts no responsibility for liability resulting from improper use or maintenance of its products.

Utilization of Haemonetics products may require the user to handle and dispose of blood-contaminated material. Users must fully understand and implement all regulations governing the safe handling of blood products and waste, including the policies and procedures of their facility.

Handling and use of any blood products collected or stored using Haemonetics equipment are subject to the decisions of the attending physician or other qualified medical personnel. Haemonetics makes no warranty with respect to such blood products.

Patient diagnosis is the sole responsibility of the attending physician or other qualified medical personnel.

The screenshots appearing in this manual are provided for illustrative purposes only and may differ from the actual software screens. All organization, donor/patient, and user names in this manual are fictitious. Any similarity to the name of an organization or person is unintentional.

Document Updates

The document is furnished for information use only, is subject to change without notice and should not be construed as a commitment by Haemonetics Corporation. Haemonetics Corporation assumes no responsibility or liability for any errors or inaccuracies that may appear in the informational content contained in this material. For the purpose of clarity, Haemonetics Corporation considers only the most recent version of this document to be valid.

Trademarks and Patents

Haemonetics, Cell Saver, Elite, and HaemoCommunicator are trademarks or registered trademarks of Haemonetics Corporation in the United States and/or other countries.

Bluetooth is a registered trademark of Bluetooth SIG, Inc. QR Code is a registered trademark of Denso Wave, Inc. DELL and OptiPlex are trademarks of Dell Inc. Intel and Core are trademarks or registered trademarks of Intel Corporation.

Reader Comments

Any comments or suggestions regarding this publication are welcomed and should be forwarded to the attention of:

International Headquarters

Haemonetics S.A.
Signy Centre
Rue des Fléchères 6
P.O. Box 262
1274 Signy-Centre
Switzerland
Tel.: +41 22 363 9011
Fax: +41 22 363 9054

Rx Only

Caution: USA Federal Law restricts the sale, distribution, or use of this device to, by, or on the order of a licensed healthcare practitioner.

Note: Availability of devices may vary from one country or region to another as a result of specific local regulatory approval or clearance requirements. Applicable laws may restrict the sale, distribution, or use of this device to, by, or on the order of a licensed healthcare practitioner.

**Haemonetics
Worldwide**

Please direct any written inquiries to the appropriate address. For a list of worldwide office locations and contact information, visit www.haemonetics.com/officelocations.

Manual Addendum

Connectivity

Introduction	6
What Is the Purpose of This Guide?	6
Data Transfer Options	6
Cybersecurity	7
Wireless Connectivity	7
Radio Equipment Specifications	7
Wired Connectivity	7
Network Setup and Maintenance	9
Wireless Network Setup and Maintenance	9
Creating a Network Configuration QR Code	9
Configuring the Device	11
Viewing the Network Status	12
Tested Network Configuration	13
Exporting Procedure Data	16
Checking the Status of a Procedure Record	16
Mandatory Record Fields	17
Setting Mandatory Fields	18
Event Messages	19

Introduction

What Is the Purpose of This Guide?

This manual addendum provides information about the data acquisition and communication features of the Cell Saver® Elite®/Elite®+ device. The hospital setting must be equipped with a central monitoring software system and an approved server application in order to benefit from these connectivity features. Please read all information in this addendum before operating the device. Use this addendum in conjunction with the associated product user manuals.

Data Transfer Options

The device is equipped with a wireless antenna and an Ethernet connection. These connections enable the device to exchange patient, device, and procedure information with a central monitoring software system (example: Hospital Information System [HIS]) via an approved server application (example: HaemoCommunicator™ software application).

The device sends the following information back to the approved server application during the course of the procedure:

- **Procedure records:** The device sends procedure record information to the server application at the end of the procedure. The device must receive an acknowledgment from the server application before it marks the data as sent.
- **Status update messages:** The device sends messages to the server application with the current device state.
- **Event messages:** The device sends any event messages that may occur to the server application as they occur.
- **Technical data:** The device sends device operational data to the server application at the end of each procedure.
- **Device configuration settings:** When first powered on, the device sends current device configuration settings to the server application after the power-on self-tests (POST) for tracking purposes.

The device receives the following additional information from the server application:

- **Software updates:** The device automatically downloads any available software updates from the server application and then displays a message providing the user with the option to install the update.
- **Device configuration settings:** The server application receives device configuration settings from the device when first powered on. If the device configuration settings have changed since they were last recorded, the server application can update the device with the last recorded settings. It can also push out configuration updates from the central monitoring system. You can configure the server application to automatically update

the settings, either silently or with a notification to the user, or to provide the user with the option to update them.

- **Date and time:** The server automatically updates the device with the current date and time.
- **Network notification messages:** The server application can deliver customizable messages from the central monitoring system to the device.

Cybersecurity

It is the customer's responsibility to ensure the security and integrity of its networks and systems, that its communication networks are configured to support encryption, and that those networks and systems are properly enabled, maintained, and utilized.

The Cell Saver Elite/Elite+ device data that is transferred is encrypted using AES encryption. Additionally, the device allows you to configure the wireless connection to utilize WPA2 Personal and WPA2 Enterprise security protocol.

Wireless Connectivity

The Cell Saver Elite/Elite+ device is equipped with an internal wireless antenna and wireless module communication component that enable the device to communicate with an approved server application. Wireless technology provides the following benefits:

- Enables the device to transmit procedure data electronically to an 802.11a/b/g/n compatible wireless access point connected to the hospital's wireless local area network (WLAN).
- Transmits data in an encrypted standard format that may be used for electronic data collection and management by a central monitoring software system.
- Allows for easier movement of devices in the hospital by eliminating the need for cabling.

Radio Equipment Specifications

The radio equipment specifications for the Cell Saver Elite/Elite+ device are as follows:

Operating Frequency Band	Maximum Transmit Power
2412 to 2472 MHz	+15.5 dBm
5180 to 5825 MHz	+16.0 dBm

Wired Connectivity

If the device is not connected to the wireless network, it can communicate with the server application via an Ethernet connection. The Ethernet port is located on the bottom of the touch screen display.

1. Status beacon
2. Touch screen
3. Barcode reader (laser aperture)
4. STOP key
5. Touch screen mount
6. USB connection
7. Ethernet connection

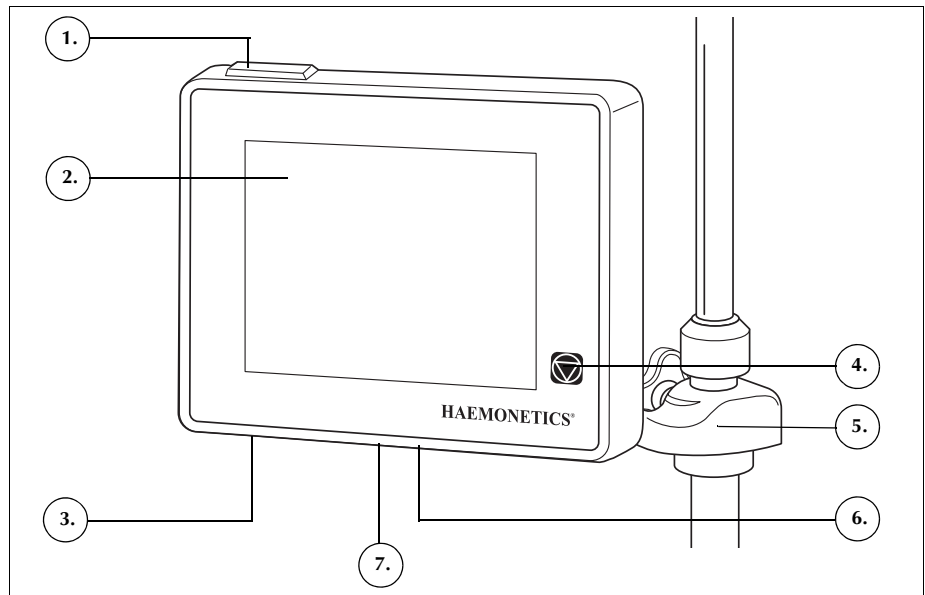


Figure 1, Parts of the device display

Network Setup and Maintenance

It is the customer's responsibility to install, validate, and maintain the network and necessary hardware.

In the event of complete loss of the communication network (For example, the router fails, the wireless or Ethernet card on the server fails, there is severe wireless interference with the network, etc.), a disaster recovery plan is recommended. This may include backup hardware and/or a backup paper system.

Wireless Network Setup and Maintenance

If the network uses wireless technology, it is the customer's responsibility to ensure that the wireless network has enough capacity to simultaneously accommodate a connection to all wireless devices required on the network. You should mitigate risks of wireless interference according to the hospital's needs and SOPs.

Monitor the Cell Saver Elite/Elite+ device and other devices for symptoms of interference. Interference can be caused by any equipment (Examples: microwaves, refrigerators, Bluetooth® devices, fluorescent lights, etc.) that operates on the same frequency band. Interference may cause delays, timeouts, or lack of access. Relocate equipment, change channels, or follow wireless equipment manufacturer instructions to reduce or eliminate interference.

Cell Saver Elite/Elite+ devices should be kept a minimum distance away from each other (approximately 39 in. [1 m]) to prevent interference of data transmission. Also, other electronic devices located in the hospital should be kept a minimum distance away from the Cell Saver Elite/Elite+ device. To calculate this distance, refer to the IEC/EN 60601-1-2 standard requirements located in the user manual.

The performance of the network depends upon proper setup, primarily selection of the channel, SSID (network name), and unique IP address of each wireless module. Evaluate the network signal level in the room for possible conflicting wireless networks and other RF devices in the vicinity. Check the signal level periodically and whenever there is an installation of new wireless networks or other RF devices.

Creating a Network Configuration QR Code

When configuring the device to communicate with the network, you must scan a quick response code (QR Code®) that contains all the network configuration information. The QR Code must be in plain text format and can be created using the CSEliteNetConfig utility. Not all settings are required. The settings you must include depend on your network configuration. [Table 1](#) displays the wireless authentication options that are supported.

Table 1, Options for Wireless Authentication

Value	Description
TLS	802.1X/WPA-Enterprise/WPA2-Enterprise
EAP-FAST	802.1X/WPA-Enterprise/WPA2-Enterprise
TTLS	802.1X/WPA-Enterprise/WPA2-Enterprise
LEAP	802.1X/WPA-Enterprise/WPA2-Enterprise
PEAP	802.1X/WPA-Enterprise/WPA2-Enterprise
PSK	WPA-Personal/WPA2-Personal

To generate a network configuration QR code:

1. Using a computer, download the CSEliteNetConfig utility from the Haemonetics Software Download Center.
 - a. Go to <http://www.haemonetics.com>, select **LOGIN**, and click on **Software Download Center** in the drop-down menu.

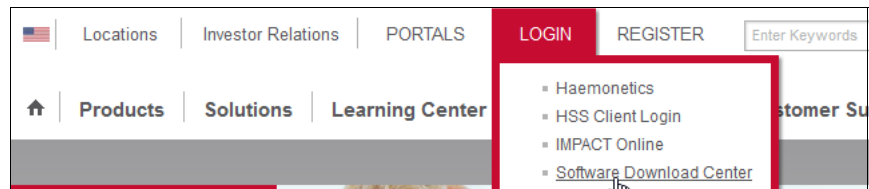



Figure 2, Accessing the Software Download Center

- b. Enter your customer login credentials.
-  **Note:** If you do not already have a login, contact your local Haemonetics representative to request access.

 - c. Locate the CSEliteNetConfig Utility within the designated Cell Saver Elite+ product area.
 - d. Click on **CSEliteNetConfig Utility**.
 - e. Download the html file.
2. Open **CSEliteNetConfig.html** and ensure that javascript is enabled.
3. Complete the form with the appropriate network settings and click **Generate QR Code**. The QR code appears.

Figure 3, Example of the CS Elite network configuration generator.

4. Print the QR code and follow the instructions in “Configuring the Device” on page 11 to use it to configure the device to connect to an approved network.



Note: For assistance, contact your local Haemonetics representative. For a list of worldwide office locations and contact information, visit www.haemonetics.com/officelocations.

Configuring the Device

The *Network Settings* screen is password protected and you must have administrator access in order to change any of the network settings. To configure the device to communicate with the network:

1. Touch (**Menu**).
2. Select **System** from the drop-down list.
3. Touch **Unlock**.
4. Enter your password and touch (**Accept**).
5. Touch **Network**. The *Network Status* screen appears.
6. Touch **Settings**. The *Network Settings* screen appears, displaying the network configuration options.

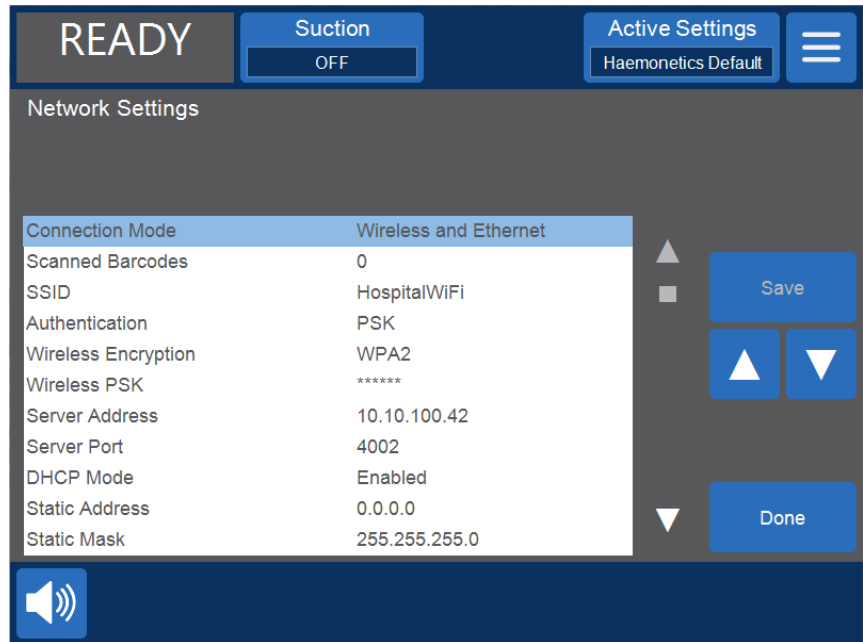


Figure 4, Example of the Network Settings Screen


7. Scan the appropriate QR code using the barcode reader. A dot appears next to any settings that have changed.
8. Touch **Save**. The *Network Status* screen shows “Configuring”, followed by “Network Connected” and then “Server Connected” once it is connected to the server application.
9. Touch **Done** to return to the *System* screen.



Note: In the System screen, you can also export or import network configuration settings to/from a USB flash drive.

Viewing the Network Status

Any basic user can view the device’s network status, To view your device’s current network status:

1. Touch  (**Menu**).
2. Select **System** from the drop-down list.
3. Touch **Network**. The *Network Status* screen appears, displaying the current network status.

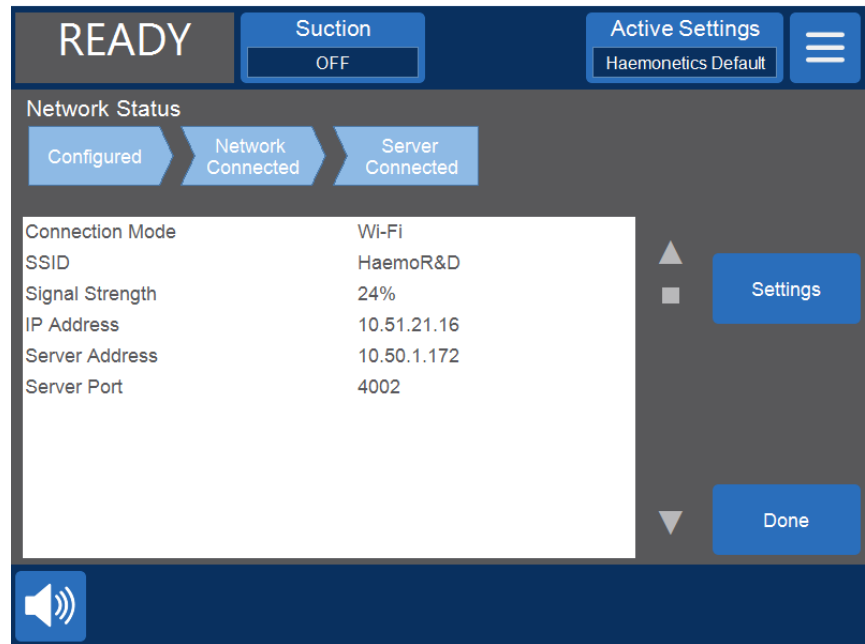


Figure 5, Example of the Network Status screen

Tested Network Configuration

The following list describes the network configuration used to test the effects of external radio frequency (RF) noise and coexistence on the Haemonetics device data transmission in the network, using the Haemonetics HaemoCommunicator software as the data collection application. The list is for reference only and is not intended to be a list of required equipment.

1. Server configuration:

Parameter	Value
Model	DELL™ OptiPlex™ computer
Processor(s)	Intel® Core™ i5-3470 CPU @ 3.20GHz
Physical Memory	4 GB
Internal Hard Disk	500 GB
Video Display	17" LCD Monitor
Network	100 Mbps
IP Address	Static 192.168.1.120
Network Security	Password protected network access Security mode: WPA2 Encryption: AES

2. **Router 1:**

Parameter	Value
Model	D-LINK DIR-803
Channels	Four 10/100 Ethernet ports
Standards	Complies with IEEE 802.11ac, 802.11a, 802.11n or 802.11g wireless clients
IP Address	192.168.1.1
Network Security	Separate SSID for 2.4GHz and 5 GHz wireless bands Password protected network access Security mode: WPA2 Encryption: AES

3. **Router 2:**

Parameter	Value
Model	LINKSYS WRT120N
Channels	Four 10/100 Ethernet ports
Standards	Complies with IEEE 802.3u, 802.11g and 802.11b standards, and compatible with some 802.11n features.
IP Address	192.168.0.1
Network Security	Password protected network access Security mode: WPA2 Encryption: AES

4. **Transmitting device:** Wireless conversion of the Haemonetics device.

5. **Software application for data collection:** Haemonetics HaemoCommunicator software application.

If you use a different configuration than the one described above or use a different software application for data collection, the configuration, devices, and network should be tested for functionality and possible sources of interference.

If a loss of communication occurs between connected devices on the wireless network, power off the router/wireless access point for 30 seconds and then power it back on.

Ensure the wireless network router(s) provide enough capacity to connect to the server, Haemonetics devices, and other devices that may run at the same time. Each of these will use a connection on the router. This information can usually be found in the manufacturer's user manual or labeling.

Exporting Procedure Data

If the Cell Saver Elite/Elite+ device is connected to the server application, it automatically sends procedure records at the end of each procedure, as long as all mandatory data has been collected. (See “Mandatory Record Fields” on page 17 for more information.) The device must receive an acknowledgment from the server application before it marks the data as sent. Once the data is marked as sent, the procedure record displays the date and time of export. If the Cell Saver Elite/Elite+ device is not connected to the server application, the device automatically sends procedure records once it reconnects, as long as a procedure is not active.

1. Exported to network

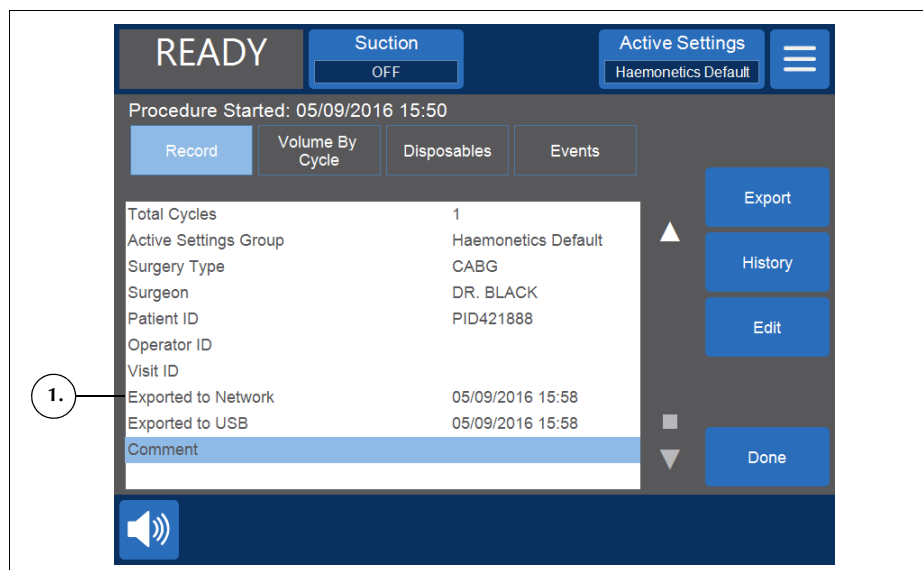



Figure 6, Procedure record

Checking the Status of a Procedure Record

To view if a procedure record has been exported:

1. Touch  (Menu).
2. Select **Records** from the drop-down list.
3. Touch **History** to view the list of procedure records. If a procedure record has been exported, it will have one or two icons beside it to indicate if it has been exported to the network and/or USB flash drive.

1. Exported to USB flash drive
2. Exported to network

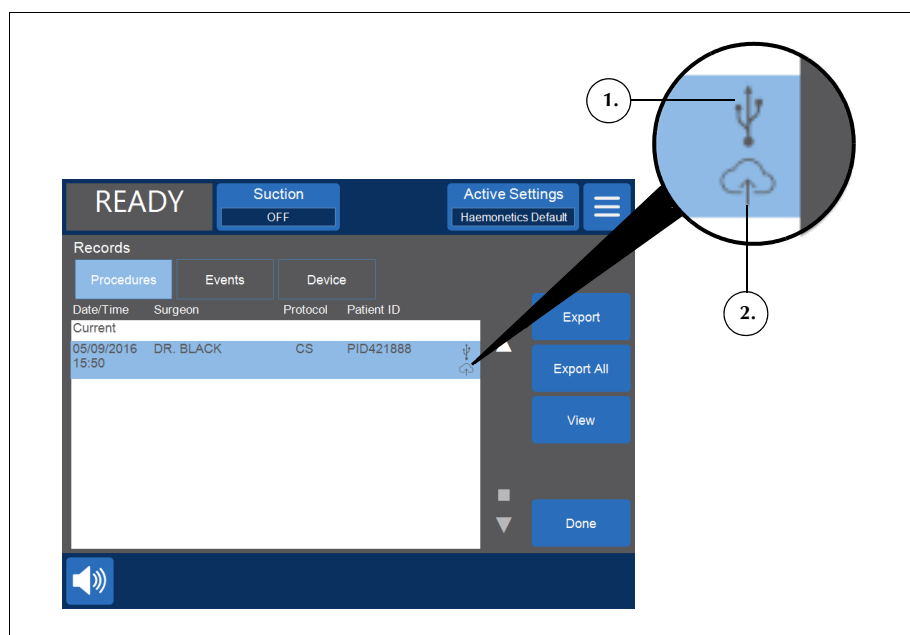


Figure 7, Procedure record history

Mandatory Record Fields

The device provides the option to set mandatory procedure record fields. By configuring the device to use this mandatory field option, the user is required to enter the associated data, ensuring records are complete, before sending the data electronically.

If you do not complete the mandatory fields, the procedure record will not be sent to the server application at the end of the procedure. In this situation, the "Procedure Complete" message and the status beacon will be yellow instead of green.

If you access the *Records* screen and enter the missing information, the device will then send the procedure records automatically if the device is connected to the network.

If you power off the device without completing the mandatory fields for a procedure, once powered on, the device will automatically send all the procedure records that have not been sent, including those missing mandatory information, if connected to a network.

1. Indicates a mandatory field

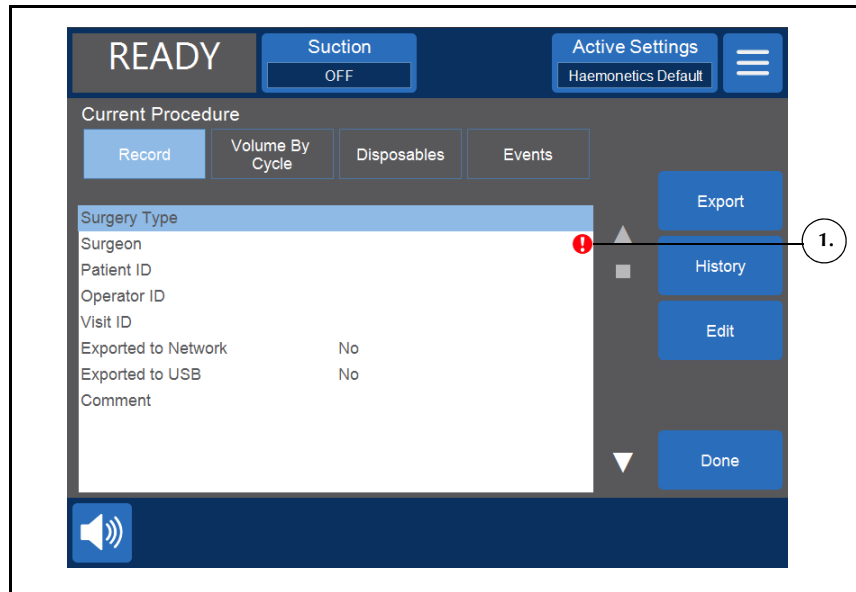


Figure 8, Example of a mandatory field

Setting Mandatory Fields

The Options screen enables you to customize various settings on the device, including determining which fields appear in the Records screen and making a field mandatory.



Note: You must have administrator level access in order to unlock the Options screen.

To make a field mandatory:

1. Touch (**Menu**).
2. Select **System** from the drop-down list.
3. Touch **Unlock**.
4. Enter your password and touch (**Accept**).
5. Touch **Options**.
6. Select a desired field.
7. Touch (**Up**) or (**Down**) to change the field to “Mandatory.”
8. Touch **Done**.

Event Messages

The following are possible event messages related to the connectivity feature that may occur on the Cell Saver Elite/Elite+ device. Refer to the user manual for a comprehensive list of event messages.

Table 2, Event Messages

ID #	Event Message Text
502	<p style="text-align: center;">Software Update Available</p> <p>Explanation: A software update has been downloaded and is available for installation. Operator confirmation is required before the software can be installed.</p> <p>Note: The device cannot be used while the software installation is in progress, which will take several minutes.</p> <p>Corrective Action: Touch Install Update to install the software now. or Touch Skip Update to skip the software installation. This prompt will recur on the next power up.</p>
503	<p style="text-align: center;">Settings Update Available</p> <p>Explanation: System and protocol settings have been downloaded and are available for application. Operator confirmation is required before these settings will be applied.</p> <p>Corrective Action: Touch Apply Update to apply the settings now. or Touch Skip Update to skip the application of the settings. This prompt will recur on the next power up.</p>
504	<p style="text-align: center;">Software Download in Progress</p> <p>Explanation: New device software is downloading. The device can be used normally.</p>
505	<p style="text-align: center;">Settings Applied</p> <p>Explanation: New system and protocol settings have been applied.</p>
506	<p style="text-align: center;">Network Notification</p> <p>Explanation: [Customizable message]</p>

