

# INSTALLATION AND OPERATION MANUAL

## Unite Connect for Patient Monitoring, Cardiomax

## Contents

1.	Introduction .....	1
1.1	How to Use this Document.....	1
1.2	Caution and Notes .....	1
1.3	Intended Use .....	3
1.4	Symbols and Descriptions .....	3
1.5	Requirements .....	4
1.6	Supported Clinical System Device Inputs .....	4
1.7	Technical Support .....	5
1.8	Abbreviations and Glossary .....	5
2	Installation .....	7
2.1	Hardware Installation, Cables and Connectors .....	7
2.2	Information Required for Setup .....	7
2.3	Getting Started .....	7
2.4	Description of LED indicators.....	7
2.5	Error Relay .....	8
2.6	Licenses .....	8
3	Configuration .....	9
3.1	The graphical User Interface (GUI) .....	9
3.2	Authentication Levels and Default Passwords.....	10
3.3	UNS .....	10
3.4	User Server Parameter Settings.....	10
3.5	Logging .....	10
3.6	Time Settings.....	11
3.7	Selecting a Template for Action Configuration.....	12
3.8	Adding Patient Data to Alerts.....	12
4	Clinical System Interface Manager Configuration.....	16
4.1	Changing CSIM Interface Settings.....	16
4.2	Units and Filters .....	18
4.3	Changing Common Settings .....	23
5	Layout Setup.....	25
5.1	Adding Locations.....	26
5.2	Renaming Locations .....	27
5.3	Deleting Locations .....	27
5.4	Defining Conditions .....	27

5.5	Available on Locations .....	28
5.6	Available for Duty .....	29
6	Advanced Administration.....	31
6.1	Backup and Restore .....	31
6.2	Diagnostic Log .....	32
6.3	Upgrade Procedure .....	33
6.4	Event Elements .....	34
6.5	Spacelabs Clinical Systems .....	34
6.6	Philips Clinical Systems .....	35
6.7	Nihon Kohden Clinical Systems .....	37
6.8	Mindray Clinical Systems.....	37
6.9	DigiStat Connect Clinical Systems.....	37
6.10	Default Event Elements.....	38
6.11	Technical Alarms .....	39
7	Network and Security Recommendations.....	40
7.1	Encryption.....	40
7.2	IP Ports .....	40
7.3	Proxy Settings.....	41
8	Module Redundancy .....	42
8.1	Prerequisites .....	42
8.2	Preparing IP Addresses in a Redundant System.....	43
8.3	Configuring Redundancy .....	44
8.4	Replacement of a Broken Module in a Redundant System.....	50
8.5	Data Storage Selection .....	51
9	Related Documents .....	53
10	Document History .....	54
Appendix A	Clinical System Protocols .....	55
A.1	Nihon Kohden Pager Service Protocol.....	55
A.2	Spacelabs Healthcare Clinical Event Interface (CEI) Protocol .....	56
A.3	Systems supporting TAP 1.8 Protocol Output Interfaces .....	58
A.4	Systems Supporting HL7v2 Protocol Output Interfaces.....	59
A.5	Philips IntelliVue .....	61
Appendix B	Cardiomax Filtering Description .....	65
Appendix C	Setting up Access Rights .....	66
Appendix D	Action Tree Templates .....	68

---

D.1	Action Tree for Philips IntelliVue System.....	68
D.2	Action Tree for Nihon Kohden, Mindray Panorama, and Spacelabs Systems .....	69
D.3	Action Configuration.....	71
Appendix E	Basic Module Troubleshooting .....	100
E.1	Log Files.....	100
E.2	Export Diagnostic Data .....	100
Appendix F	Acceptance Test .....	101
F.1	Alarm Specifications .....	102
F.2	Acknowledgment .....	106

## 1. Introduction

This document describes the installation and configuration of Cardiomax. It also describes the administrative part of Duty Assignment, i.e., the configuration and administration of events and actions related to a specific event, and where action chains with success/failure conditions and access rights for the users are handled. These activities require a trained system administrator, and a certified engineer.

Duty Assignment is where the locations, in for example a hospital, and the conditions for events are set up. It is operated on a daily basis by, for example, a nurse. A description of how to assign users to specific locations, and associated events, is found in the Cardiomax Duty Assignment User's Manual TD92904EN.

---

**CAUTION:** A general understanding of the features and functions of Cardiomax and its components is a prerequisite for the proper use of this equipment. Do not operate this equipment before reading these instructions thoroughly, including all appropriate warnings and cautions.

---

Cardiomax is a product based on the Elise3 hardware platform. It receives alarms from medical alarm devices and sends alerts about alarms to professional healthcare personnel via display devices such as handsets, text signs etc. Cardiomax also provides an assignment interface to enable users to dynamically assign alerts to recipients. US Federal and Canadian law restricts this device to sale by or on the order of a licensed medical practitioner.

Figures in this manual are provided for reference purposes only. Screens may differ based on the product configuration, licenses available and system configuration.

### 1.1 How to Use this Document

The document is mainly intended for Ascom installation personnel, and a local administrator for normal system maintenance.

### 1.2 Caution and Notes

Please read and adhere to all of the cautions listed throughout this manual.

A **WARNING** is provided to outline items that if not followed, may result in death or serious injury to the patient or damage to the equipment.

A **CAUTION** is provided to alert the user that special care should be taken for the safe and effective use of the device.

A **NOTE** is provided when additional general information is available.

<b>WARNING:</b>	<i>Shall not be relied upon for receipt of ALARM SIGNALS. The system does not substitute for the primary monitoring system and must only be</i>
-----------------	---

	<i>used as a redundant, parallel notification mechanism to provide remote secondary alerting of alarms</i>
WARNING:	<i>Acceptance testing must be performed for each location supported by this product. Failure to complete acceptance testing may result in failed or delayed notification, resulting in potential patient harm. Functional verification of the products should occur before the product is used in a clinical environment with live patient. Additionally this testing should be repeated after any changes to the configuration or system upgrades.</i>
CAUTION:	The product must utilize the hospital emergency power system. Failure to do so may result in loss of operation during extended periods of power failure. A battery backup system must be in place to maintain operation in the event of a power failure. The minimum battery backup time is based upon the time required for the hospital emergency power system to take effect. With proper emergency and battery backup protection, the product will not experience any service disruption during power failure and restoration.
CAUTION:	The proper installation of the product should include the use of the external error relay to provide auxiliary notification in case the standard notification procedure should fail.
CAUTION:	Only qualified and trained personnel or service personnel should attempt to service the equipment. Service is defined as any activity requiring the cover to be removed for internal adjustments, parts replacements, repairs or software upgrades of any kind to insure compatibility.
CAUTION	To ensure compatibility with the product software, use only approved components to repair any part of the product. Use of unauthorized software, devices, accessories, or cables may render the application unsuitable for its intended use. It may also result in increased electromagnetic emissions or decreased immunity of the system.
CAUTION:	Properly dispose of batteries according to local and national laws.
CAUTION:	Incorrect settings or silencing of display devices can jeopardize the performance of the system.
2 CAUTION:	Operators should check that the current notification events and assignments are appropriate prior to use.
2 CAUTION:	Set the annunciation parameters, including volume levels, of the display devices so that alarms can be heard at all times.
CAUTION:	For proper operation, ensure proper operation of display devices before each use.
CAUTION:	Mobile display devices are wireless devices and may be subject to intermittent signal dropout. A crowded wireless environment or interference from other wireless devices, either intentional or unintentional, may result in a significantly

	increased amount of signal dropout experienced by any one or multiple wireless device(s).
CAUTION:	Only compatible display devices, capable of supporting the outlined minimum characteristics and communication protocols included in this manual, is used with the product.
CAUTION:	Only compatible medical systems, capable of supporting the outlined communication protocols included in this manual, is used with the product.
CAUTION:	Changes or modifications not expressly approved by Ascom (Sweden) AB could void the user's authority to operate the equipment.
CAUTION:	Other systems distributing information on the same messaging system can impact the overall messaging capacity of Cardiomax system.

### 1.3 Intended Use

The intended use of Ascom Cardiomax is to provide an interface with clinical systems to forward information associated to the particular event to the designated display device(s).



For medical, near real-time alarms, Ascom Cardiomax is intended to serve as a parallel, redundant, forwarding mechanism to inform healthcare professionals of particular medical related events.



Ascom Cardiomax does not alter the behavior of the primary medical devices and associated alarm annunciations. The display device provides a visual, and/or audio and/or vibrating mechanism upon receipt of the alert.

Ascom Cardiomax is intended for use as a secondary alarm. It does not replace the primary alarm function on the monitor.

The product must be installed by an Ascom Certified System Integrator authorized to install and provision the Ascom Cardiomax product. Please contact your Ascom service representative for additional information.

### 1.4 Symbols and Descriptions

In the About SW File		Description
	Manufacturer	Indicates the medical device manufacturer, including address and telephone number.
	Date of manufacture	Indicates the date when the medical device was manufactured.

	Catalogue number	Indicates the manufacturer's catalogue number so that the medical device can be identified.
	Consult instructions for use	Indicates the need for the user to consult the instructions for use.
UDI	Unique device identifier	Indicates the need for the user to consult the instructions for use for important cautionary information such as warnings and precautions that cannot, for a variety of reasons, be presented on the medical device itself.
Rx only	Prescription device	Indicates a Unique Device Identifier that adequately identifies a device through its distribution and use.
<b>On Hardware</b>		<b>Description</b>
Module		The module key number of the device1 key
S/N		The serial number of the device
Model		The hardware model

*Can also be found on the hardware. For U.S. only.*

## 1.5 Requirements

### 1.5.1 PC Requirements

These requirements refer to computers that run duty assignments and administer Cardiomax from a Web browser:

- Microsoft® Internet Explorer® 8.0 or later
- Sun™ Java™ Runtime Environment (JRE) 6 or later

The product relies on properly wired and wireless network setup and operations.

The product requires a 10/100 BaseT-switched Ethernet network. Follow the manufacturer's instructions to ensure that wired and wireless networks are properly designed and operational.

## 1.6 Supported Clinical System Device Inputs

Cardiomax is designed to accept inputs from a variety of clinical systems utilizing standardized and proprietary protocols including the following:

- Digistat Connect
- Philips
  - Parameter Data Interface (PDI)



- IntelliVue Information Center iX (PIIC ix) HL7 Interface
- Spacelabs Healthcare ICS
  - Enterprise Network Interface (ENI)
  - Clinical Event Interface (CEI) Protocol
- Mindray Panorama TAP v1.8 Paging Protocol
- Nihon Kohden PagerService Protocol

For additional details on specific system compatibility and functionality, refer to the Data Sheet, Cardiomax TD 92905EN and Appendix A Clinical System Protocols.

## 1.7 Technical Support

For technical assistance, please contact your Ascom service representative. Additional information relating to the installation, servicing and operation of the product is provided in the following documents:

- User Manual, Duty Assignment TD 92904EN
- Configuration Manual, Unite Connectivity Manager TD 92735EN
- Installation Guide, Elise3 TD 92679GB

## 1.8 Abbreviations and Glossary

Action handler	Handles actions in Cardiomax. Set up in Action Configuration.
CSIM	Clinical system interface manager
Elise	Embedded Linux server
Event	Triggers actions in Cardiomax
Groups	Sets up messaging in the Unite Connectivity Manager. If a message is sent from Cardiomax to a group number, the message is sent to all call IDs included in that group. In the group setup, the call IDs to be included are specified. See also User teams.
Intensive care unit (ICU)	Hospital unit.
Interactive message	A message sent from Cardiomax to a handset, requesting a response from the use
Handset	Any type of Ascom handset or pager
Unite	Another name for the Ascom Professional messaging system. The Unite communication protocol is used for communication within the Ascom Unite system

Unite Connectivity Manager	Unite module handling users, communication interfaces, message routing, activity logging and other essential messaging services
Unite name server (UNS)	Unite component that holds the number plan. The number plan is a list of users and call IDs. Mainly used during setup of a system. Preferably prepared prior to installation
User teams	Used in duty assignments in Cardiomax to set up work shifts and define different types of personnel such as doctors or nurses. User team setup is performed in the Unite Connectivity Manager. User teams are also setup in the Unite Connectivity Manager. See also Groups

## 2 Installation

### 2.1 Hardware Installation, Cables and Connectors

The Elise3 hardware is used by Cardiomax. For installation of the hardware, cables and connectors, refer to the Installation Guide, Elise3 TD 92679EN.

---

NOTE: Ethernet and RS232 cables not included in delivery.

---

### 2.2 Information Required for Setup

Make sure the following information is available:

- MAC address – found on the license certificate enclosed in delivery
- License number – found on the license certificate enclosed in delivery
- Network parameters – ask site network administrator
- IP address assigned to product

---

NOTE: The IP address must not change during operation because renew of IP address via DHCP is not handled. Other equipment connected to this product also expects a fixed IP address in some cases. If the IP plan is changed, this product must be re-started to update the IP address. Otherwise there is a risk for IP address collision.

---

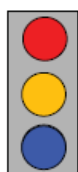
### 2.3 Getting Started

For information on accessing the product, refer to the Getting Started leaflet included in delivery and the Installation Guide, Elise3 TD 92679EN.

### 2.4 Description of LED indicators













The Elise3 hardware has LEDs that indicates the status of Cardiomax software as shown below.



Elise3 module






Color	Indicator
Red	Fault indication
Yellow	Mode indication
Blue	Normal operation (OK)

## Flashing patterns

Status LED				
Status OK	Blue			
Starting up/ shutting down	Blue			
Feedback (1 second)	Blue			
Error/fault	Red			
Warning	Red			
Boot mode	Yellow		Blue	
Demonstration mode	Yellow		Blue	
Waiting for automatic startup (1 minute)	Yellow			
Troubleshoot mode and during firmware upgrade	Yellow			
Mass storage mode			Blue	

Secured settings		Status LED	Mode LED
Indicates that manual confirmation is required		Blue	
Confirmation is done and setting can be activated	Yellow		Blue

Power		Power LED
Power OK	Blue	
Closing down caused by low voltage	Red	
Low voltage*	Red	

\* also used if the Power parameter conflicts with the actual setup.

## 2.5 Error Relay

The error relay output indicates Cardiomax operation. When Cardiomax starts, the error relay operates. When Cardiomax shuts down or restarts, the error relay releases.

The proper installation of the product should include the use of the external error relay in order to provide auxiliary notification in case the standard notification procedure fails.

---

NOTE: The proper installation of the product should include the use of the external error relay in order to provide auxiliary notification in case the standard notification procedure fails.

---

## 2.6 Licenses

For available licenses, see the Unite License Configuration Guide, TD 93113EN.




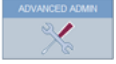
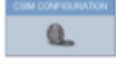

## 3 Configuration

Cardiomax configuration utilizes a Web browser. To configure Cardiomax, enter the IP address in the Web browser address field (<http://xxx.xxx.xxx.xxx>).

### 3.1 The graphical User Interface (GUI)

You can select different functions from the Cardiomax start menu such as duty assignment, action configuration, event trigger assignment, advanced admin and CSIM configuration.



	Administration of the daily duty assignment. Refer to User Manual, Duty Assignment TD 92904EN
	Configuration of available events and actions
	Configuration of different conditions before indicating that an event has occurred
	Advanced administration
	Configuration of the clinical system interface (CSIM) parameters
	Information about manufacturer, markings and device, e.g. item number, description, version number, date of manufacture, UDI and module key number

## 3.2 Authentication Levels and Default Passwords

There are two different authentication levels; an administrator or a defined user.

- **Unite AM Administrator rights** are required for setup, configuration and administration of the product and for simple troubleshooting. The default user names and password are **admin** and **changeme**.
- **A defined user** logs in with a user ID and password that is set up by a local administrator. The user has access to Cardiomax on a level depending on which user teams the user belongs to, see Appendix C.
- Change default passwords to protect the system from unauthorized access. Refer to the Configuration Manual, Unite Connectivity Manager TD 92735EN.

## 3.3 UNS

1. Set the module to forward UNS requests to the Unite Connectivity Manager.
2. Click **UNS** in the menu for parameter settings.

### Operating Mode

Configure the following parameters:

- **Operating Mode:** Select Forwarding from the drop-down.
- **IP address of forward destination UNS:** Set value to the Unite Connectivity Manager's IP address.

## 3.4 User Server Parameter Settings

The module communicates with a user server to understand the available users and user teams, defined in the messaging system. The Unite Connectivity Manager serves as the user server in the messaging system.

Click **User Server** in the menu for parameter settings.

**User Server IP address:** Set value to the Unite Connectivity Manager's IP address.

## 3.5 Logging

System activity logs, and status information from the module must be distributed to a central repository for activity logging and fault handling. The Unite Connectivity Manager serves as the central repository in the messaging system.

When the module is powered off or experiences an unexpected loss of power, no activity log entries are published to the Unite Connectivity Manager. When the Unite Connectivity Manager is powered off or experiences an unexpected loss of power, it cannot receive published activity logs.

Click **Logging** in the menu for parameter settings.

### Status Log

1. Configure the following parameters:
  - **Destinations:** The syntax for these fields is “IP address/SERVICE”. The Unite Connectivity Manager’s FaultHandler service is added to the distribution list. Set the value to “Unite Connectivity Manager’s IP Address/FaultHandler”.
  - **System Activity Log:** The syntax for these fields is “IP address/SERVICE”. Add the Unite Connectivity Manager’s Activity Logger service to the distribution list. Set the value to “Unite Connectivity Manager’s IP Address/Activity Logger”.
2. Click **Activate**. The module sends all status log/activity log messages to the Unite Connectivity Manager.

### Advanced Parameters

Click **View advanced parameters**.

**Error Relay Time for Status Log Failure:** If it is not possible to generate or send status logs on errors, the error relay is released. This might happen if there are major problems in the module, for example if all internal queues are full, or in case there is a communication failure with the Unite Connectivity Manager that is configured to receive the logs, etc.

To define the relay release length, click **View advanced parameters**. The time is defined in seconds between 0 and 900, where 0 means that the error relay is not released at all.

---

NOTE: The error relay should always be connected in order to notify users if an error has been detected.

---

### Extended Activity Log

Click the **Extended Activity** Log link. When enabled, intermediate activity logs are sent while a message passes through the system towards the destination. The extra information is not saved in the log file. It is only displayed in continuously updated log viewers.

---

NOTE: Use this function with caution as it generates more traffic in the system.

---

## 3.6 Time Settings

The time settings control how the module handles the time and date. To ensure that the module has the exact time and date as the rest of the messaging system, it must be set to synchronize its clock to a time server. The Unite Connectivity Manager can be used as the time server for the entire messaging system.

Click **Settings** in the Time section in the menu for parameter settings.

- **Time Source:** Select Time server from the drop down box.

- **Time server address:** Set the value to the IP Address of the time server for the messaging system (i.e. Unite Connectivity Manager).
- **Time zone:** Select the appropriate GMT offset for the given place of operation.

If “Web browser” has been selected as time source, the time must be set manually. Otherwise this setting is not complete.

### 3.7 Selecting a Template for Action Configuration

To facilitate the configuration of events for monitoring systems, you’ll need to apply a template. The templates have preconfigured “action trees”, adapted for different systems. Unite events are included in the template, but you can add new Unite events if necessary.

To add a new template:

1. In Unite AM, click **Integrations**.
2. In the upper left-hand corner, click **Add**. A drop-down menu appears.
3. Select the system, template, name the integration and select an interface.

---

**NOTE:** If an interface is already in use, you cannot use that same interface for another integration.

---

4. Click **Add**. The new template appears below any previously added templates. The list of event elements reflects the new template.

---

**NOTE:** If a template is used, there is normally no need to set up any actions.

---

Refer to Appendix D for an explanation of the Action Tree in Event Configuration, for different monitoring systems.

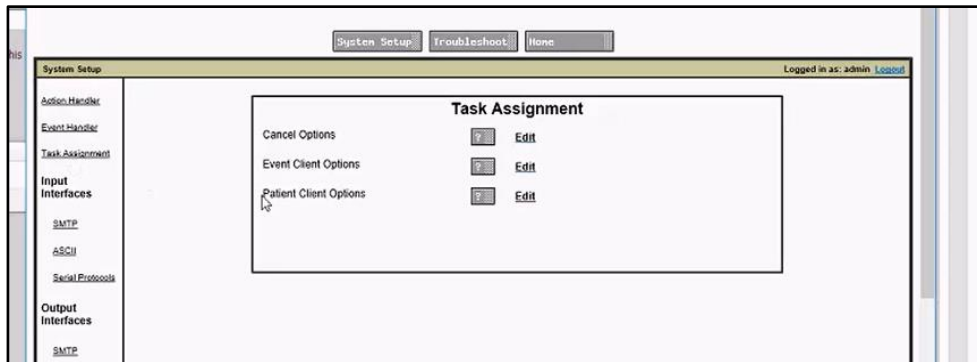
### 3.8 Adding Patient Data to Alerts

Cardiomax is able to retrieve patient information from a Unite EHR Integration with the Task Assignment and Patient Options settings as follows:

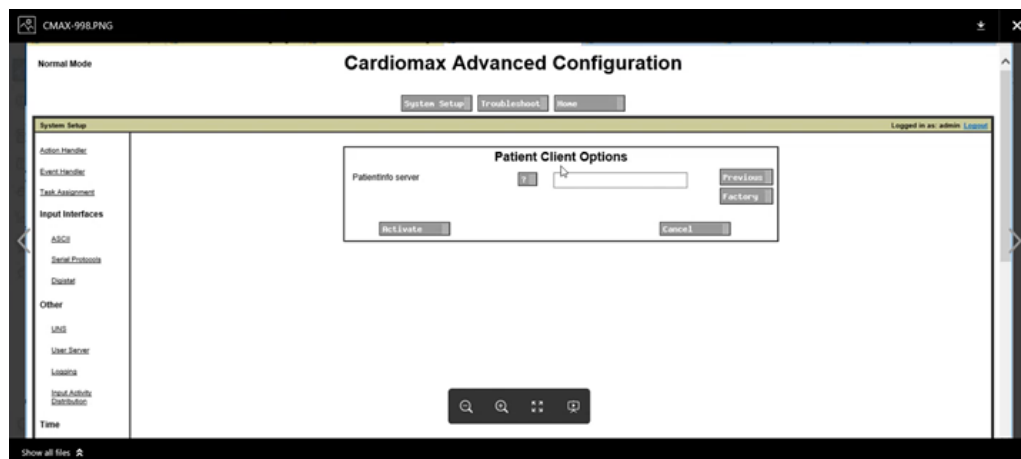
1. Go to the Advanced tab for the module integration and click on Advanced Configuration.



- 2 Under System Setup select the Task assignment option.



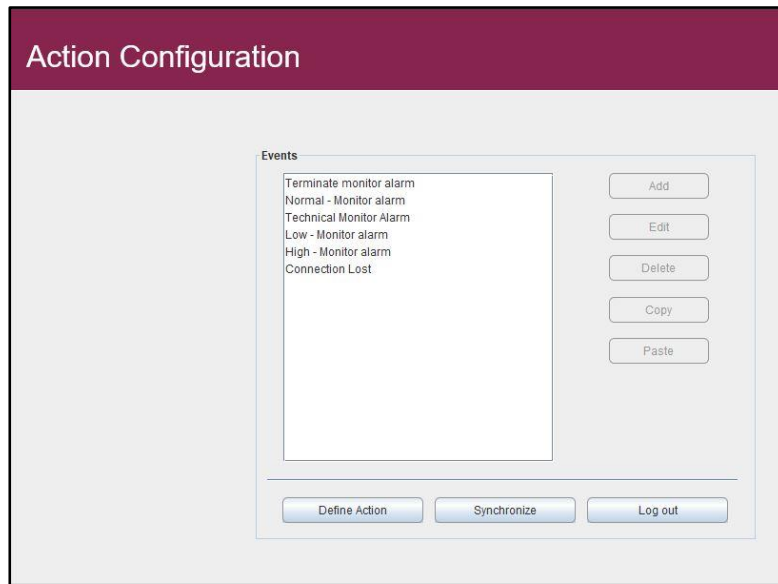
- 3 Go to the Patient Client Option, click Edit and enter the Unite address of the PatientInfo server. The destination should be in the format 'Unite IP address/Service' where the service is URSS. This allows Cardiomax to retrieve patient information (i.e., patient name) from the EHR integration.



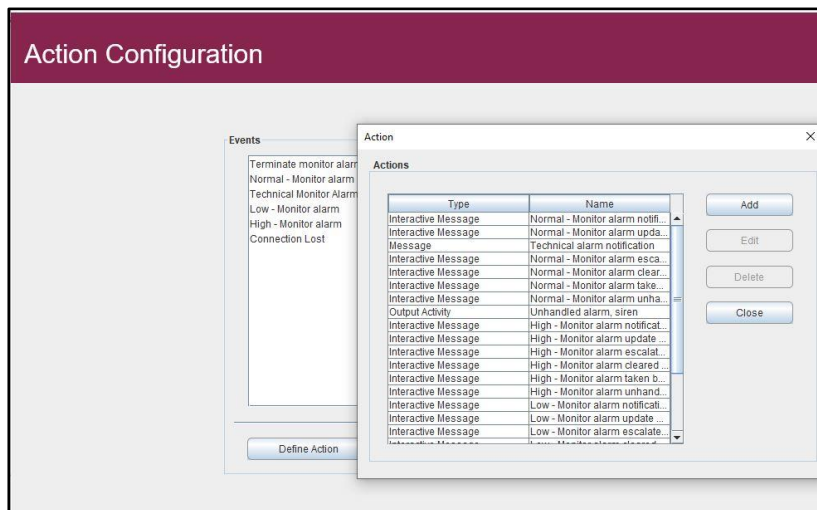
- 4 Hit Activate. This synchronizes all information for admitted patients and makes the information available. When an event is triggered, the patient information can be identified for the location where event is occurring.

For patient information to be added to an alert (in this example, the patient name), include a tag in the message body as follows:

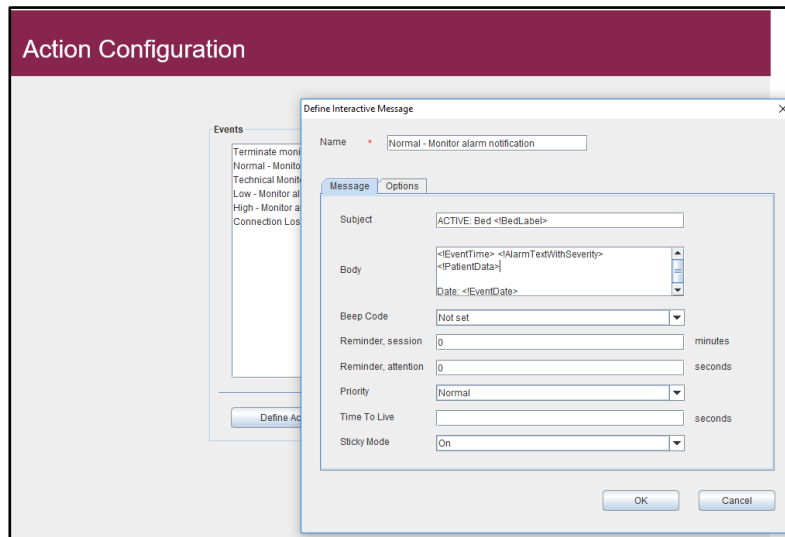
- 1 Go to the Basic tab for the module integration, click on Basic Setup and click on Action Configuration under Action Handler.
- 2 All the configured Events that can be triggered are displayed.



- 3 Click Define Action. The following template information appears.



- 4 Select an item to edit (in this example it is Normal – Monitor alarm notification).
- 5 To include the patient's in the Body field, enter the tag <!PatientData>.



- 6 When the alert is sent out, it will now include the name of the patient who is admitted to the Unite location in the Body field where the alarm is occurring.

## 4 Clinical System Interface Manager Configuration

The CSIM interface enables an administrator to configure interface parameters necessary to interface with the clinical system.

1. Click the CSIM Configuration from the module's start page.
2. To change CSIM Interface setting, see 4.1 Changing CSIM Interface Settings.
3. Click **Activate** to save the CSIM parameters.

---

NOTE: Activation of changes to these parameters could cause a temporary loss of connectivity with the clinical system.

---

### 4.1 Changing CSIM Interface Settings

- **Mindray<sup>1</sup>**
  - *Mindray TAP Settings*  
Parameters associated with the configuration of the serial port TAP parameters used to interface with the Mindray Panorama paging service.
- **Nihon Kohden**
  - *Connection port*  
Enter the port number of the Nihon Kohden server.

- **Phillips**

The following parameters handle incoming alarms:

- *Patient Monitoring System*  
Allows for the selection and identifies the currently enabled Patient Monitoring System Interface.
- *Update Status (True or False)*  
If the status is updated for locations that are experiencing an Active Alarm (True) or not (False).
- *Update On Alarm Clear*  
If terminated alarms indications is notified (True) or not (False).
- *Time Format*  
Set the time stamp format for active alarm notifications.  
Example: hh:mm
- *Date Format*  
Set the date format active alarm notifications.  
Example: mm/dd/yy.
- *Unsolicited Listening Port*  
The port number associated with the Auto Unsolicited out from the HL7 Export Interface of the Intellivue information center.

---

<sup>1</sup> US only

- *Connection Timeout*  
Defines the number of seconds that a socket will wait for PDI data before determining a connection. Changes to this value are effective only for new connections.
- *Display IP on Error*  
Displays the IP address of the remote system on loss of connectivity. Changes to this value are effective only for new connections.

- **Spacelabs CEI & ENI**

Configure the specific parameters necessary for the Spacelabs Healthcare Clinical Event Interface.

- *CEI Address*  
Set the Server IP field to the IP Address of the Clinical Event Interface Server.
- *CEI Port Number*  
Set the Server Port field to the Listening Port of the Clinical Event Interface Server.
- *EventData Start Field/EventData Stop Field*  
The Event Data Start and Stop fields determine the substring derived from the Clinical Event Alarm Message Event Data element received from the Clinical Event Interface. The substring is stored in the AlarmTextParsed Event Element. Set Event Data Start Field to the desired start character count. Set Event Data Stop Field to the desired end character count. The values are 0 indexed; the Event Data Start Field factory default value is 0 and the Event Data Stop Field factory default value is 9:

**Start Index**  
Determines the beginning substring derived from the Clinical Event Alarm Message Event Data element received from the Clinical Event Interface. The value is 0 indexed.  
Close

**End Index**  
Determines the end of the substring derived from the Clinical Event Alarm Message Event Data element received from the Clinical Event Interface. The value is 0 indexed.  
Close

**Cardiomax CSIM**  
Patient Monitoring System: Spacelabs  
CEI Address:   
CEI Port Number: 6868  
EventData Start Field: 0  
EventData Stop Field: 9  
CEI Client Active: Active  
Warning: Activation Of Changes To These Parameters Will Cause A Loss Of Connectivity!  
Activate Cancel

For example, if the Event Alarm Message Data element value is “V1 MON HR =59 A=0 \*ALARM\* HI LIMIT=45” and the Event Data Start Field value is 0 and Event Data End Field is 9, then the AlarmTextParsed event element value is “V1 MON HR.”

- *CEI Client Active*  
Determines whether the module will establish a connection with the Clinical Event Interface Server. Enable Activate Connection by clicking the check box.

Only activate a connection if the module interfaces with the Spacelabs Healthcare Clinical Event Interface.

- **DigiStat**
  - *Listening Port*  
The TCP port on which the MLLP receiver listens on.
  - *Client Timeout*  
Amount of elapsed time (sec) after which the UMS Server shall remove a client from its connection list if that client fails to send a keep alive message.
  - *Time Stamp of Alarms*  
The format of the time associated with alarms (12 hr or 24 hr).

## 4.2 Units and Filters

Units and filters offer centralized filtering in a distributed Cardiomax systems architecture.

---

**NOTE:** Units and filters are only applicable when the configured clinical system is defined for Philips, Digistat Connect clinical systems. If the system is configured for Phillips and includes additional Cardiomax extension modules, Units and filters are only available on Cardiomax central module.

---

Four types of filters exist in Cardiomax; pass, stop, delay and group, fulfilling different system needs. The different filter types and how to use them are explained below.

Filter setting information is collected before the actual configuration starts. All filter settings are set up during configuration of the system.

- 1 **Pass filter:** All alarms with alarm text matching any of the pass filters are accepted and alerts will continue to be by any of the additional configured filters. If no pass filters are configured, then all alarms are accepted for further processing.
- 2 **Stop filter:** All alarms with alarm text matching any of the stop filters are discarded and no alerts are sent out.
- 3 **Delay filter:** All alarms with alarm text matching any of the delay filters must be active for the period of time defined by the filter before an alert are sent out.
- 4 **Group filter:** Determines which alarm updates are considered to be equivalent to a previously delivered alert. Active alarms with updates that matches an active group filter are considered to be equivalent and discarded by Cardiomax.

By setting a group filter, alarm texts with a similar content, such as updated heart rate can be bundled and not sent as updates for each heart rate change.

- 1 From the CSIM page, click **Units/Filters**. The alarm text Filters window opens.

**Alarm Text Filters**

Units ?

Alarm Text Group Filter

Alarm Text Delay Filter

Not Used  
Not Used  
Not Used  
Not Used

Previous  
Factory

- 2 The filtering feature is case sensitive.

### Alarm Text Group Filters

For alarm text group filters, all alarm texts that match the same group filter are considered to be the same alarm. This type of filtering is available only for Philips and DigiStat.

**Alarm Text Group Filters**

Group Filter 1 ? ART? D HI\* Previous  
Group Filter 2 ? ART? D LO\* Factory  
Group Filter 3 ? ART? M HI\*  
Group Filter 4 ? ART? M LO\*  
Group Filter 5 ? ART? R HI\*  
Group Filter 6 ? ART? R LO\*  
Group Filter 7 ? ART? S HI\*  
Group Filter 8 ? ART? S HI\*  
Group Filter 9 ? BT HI\*  
Group Filter 10 ? BT LO\*  
Group Filter 11 ? CO2 HIGH\*

Group Filter 1– 100:

See Appendix B. Cardiomax Filtering Description for details and examples.

### Alarm Text Delay Filters

For alarm text delay filters, all alarms with alarm text matching any of the filters must be active for as long as the time defined for that filter before any alerts are sent out. This type of filtering is available only for Philips and DigiStat.

The screenshot shows the 'Alarm Text Delay Filter' window. It has a title bar with the text 'Alarm Text Delay Filter'. Below the title bar, there is a 'Delay Filter' label with a help icon (a square with a question mark) to its right. To the right of the help icon are two buttons: 'Previous' and 'Factory'. Below this, there are four rows, each labeled 'Delay Filter 1' through 'Delay Filter 4'. Each row has a text input field and a dropdown menu below it. The dropdown menus are currently set to 'Disabled'.

- Delay filter 1– 10:  
Set filter value.  
Select delay time or Disabled.

See Appendix B. Cardiomax Filtering Description for details.

### Unit Configuration

Use this to configure settings specific for a certain unit or department. This type of filtering is available only for Philips and DigiStat.

To add or configure alarm text filters, from the alarm text Filters window, click **Not Used**. The Unit Configuration window appears.

The screenshot shows the 'Unit Configuration' window. It has a title bar with the text 'Unit Configuration'. Below the title bar, there is a 'Name' label with a help icon (a square with a question mark) to its right. To the right of the help icon are two buttons: 'Previous' and 'Factory'. Below this, there is a 'Delay Filters' label with a help icon (a square with a question mark) to its right. Below the help icon, there are four rows, each labeled 'Delay Filter 1' through 'Delay Filter 4'. Each row has a text input field and a dropdown menu below it. The dropdown menus are currently set to 'Disabled'.

- **Name**  
Name of the unit/department. This name must match the unit name in the received alarm (location field).
- **Delay filters 1-10**



Enter delay filter settings as in Alarm Text Delay Filters. These are additional delay filters that are valid only for this unit. Ten delay filters can be set for each of the 25 units that can be configured.

## 4.2.1 Extension Modules

---

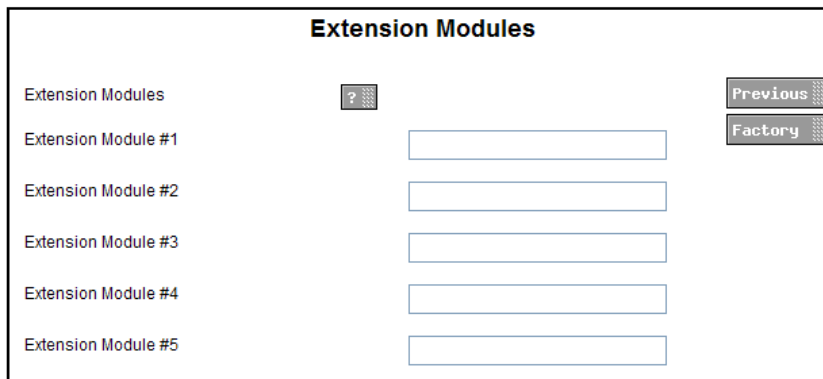
NOTE: Only applicable for the Phillips monitoring system.

---

The location capacity of a Cardiomax system can be increased by adding extension modules. Up to 9 extension Modules can be added. Each extension module added to a Cardiomax system increases the number of clinical systems locations supported by the central Cardiomax unit by an additional 150 locations.

Extension modules are provisioned on the central module by entering the IP address of each extension module. Upon activation each extension module is individually contacted and instructed to send any received alarms to the central module for further processing and eventual delivery to the portable devices.

- 1 From the CSIM page, click **Interface Modules**. The Extension Modules window appears.
- 2 Enter the IP addresses in the text fields.
- 3 Click **Activate**.



## 4.2.2 Reset Location Table for Philips Monitoring Systems

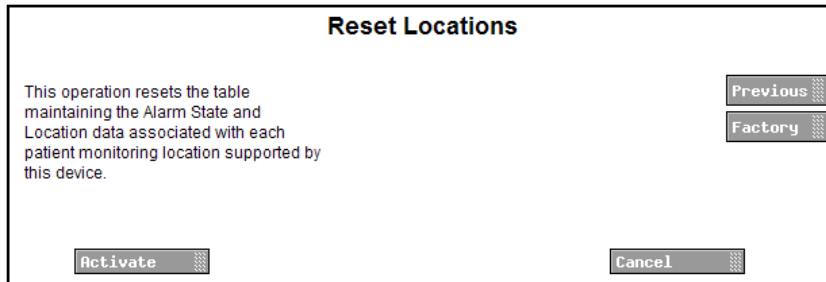
---

NOTE: Applicable for Phillips monitoring system only.

---

The table that maintains the current alarm state and location data for all monitored clinical systems locations supported by Cardiomax can be cleared. The current state of all monitored location is restored on next update interval from the clinical system.

- 1 From the CSIM window, click **Reset Location Table**. The Reset Locations window appears



---

CAUTION: Activation parameter changes cause a connectivity loss.

---

- 2 Click **Activate** to reset the table.

### 4.2.3 Pass Filters

---

NOTE: Available for Digistat, Phillips and Nihon Kohden clinical systems.

---

The pass filter represents an integral function of an optimized Cardiomax system. Pass Filters reduce the number of alerts to alerts recommended and/or requested during clinical consulting.

---

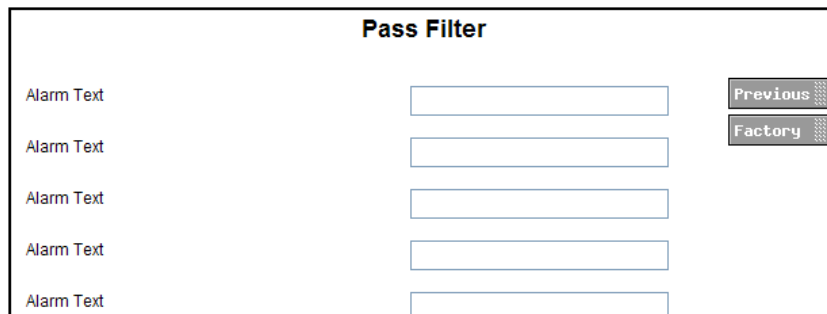
IMPORTANT: All alerts are delivered by default, except when one pass filter is set up, no other alerts except the one specified in the pass filter, are delivered.

---

Failure to properly define parameters within the pass filter may impact performance and increase latency in the delivery of alerts to portable devices.

Each central and extension module provides its own set of pass filters define a multi-unit or site-wide configuration. Each instance defined in the pass filter should represent the syntax of the specific alarm requested. "?" characters represent "wildcard" or variable character strings. One "?" character can match 0 or more characters.

Example: "?HR?>?" matches and therefore allows for passing on any alert text equal to \*\*\*HR160>120 or similar. Alert text NOT matching this syntax is discarded allowing Cardiomax the ability to more quickly process requested alert types.



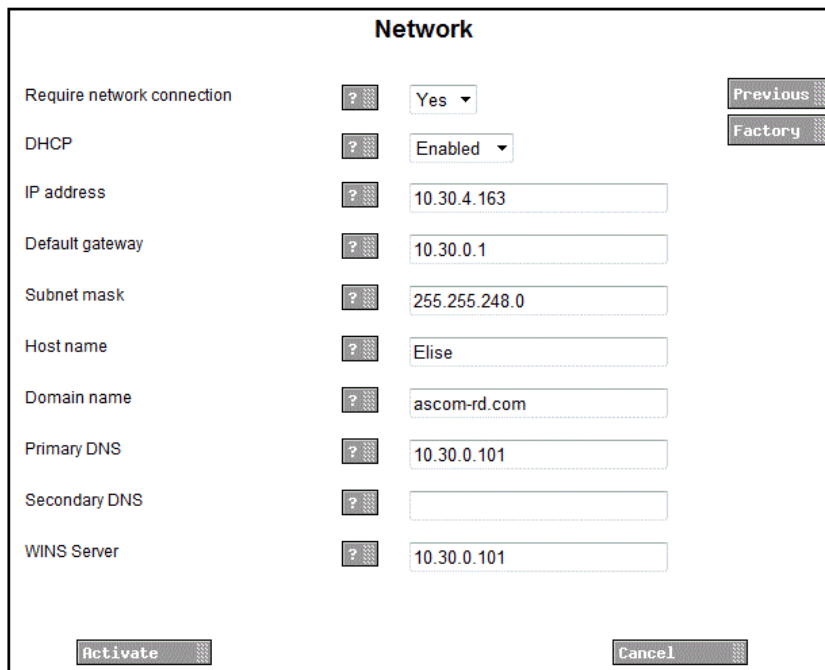
The **Pass Filter** window displays five rows, each with an "Alarm Text" label and an empty text input field. On the right side of the window, there are two buttons: "Previous" and "Factory".

Up to 25 pass filters can be set.

## 4.3 Changing Common Settings

### 4.3.1 Network Settings

- 1 From the start page, click **CSIM CONFIGURATION**.
- 2 Click **Network**. The Network window appears.



The **Network** window contains the following settings:

Setting	Value
Require network connection	Yes
DHCP	Enabled
IP address	10.30.4.163
Default gateway	10.30.0.1
Subnet mask	255.255.248.0
Host name	Elise
Domain name	ascom-rd.com
Primary DNS	10.30.0.101
Secondary DNS	
WINS Server	10.30.0.101

At the bottom of the window are two buttons: "Activate" and "Cancel". On the right side, there are also "Previous" and "Factory" buttons.

- 3 Enter IP settings.
- 4 Click **Activate** to save the settings, or click **Cancel**.

For additional information, see also Installation Guide, Elise3 TD 92679GB

### 4.3.2 License Numbers

Available licenses are shown, and new licenses can be added here.

- 1 Click **CSIM** from the start page. The CSIM window appears.
- 2 Under Common, click **License**. The Module Settings window appears.
- 3 Enter the license number in the License field.

- 4 Click **Activate** to save the settings or **Cancel**.

### 4.3.3 Restarting the System

Cardiomax can be restarted from the CSIM page.

From the Start page, click **Reboot**. You are prompted to reboot or cancel.

The status LED flashes a when rebooting, and once complete, returns to a steady light.

---

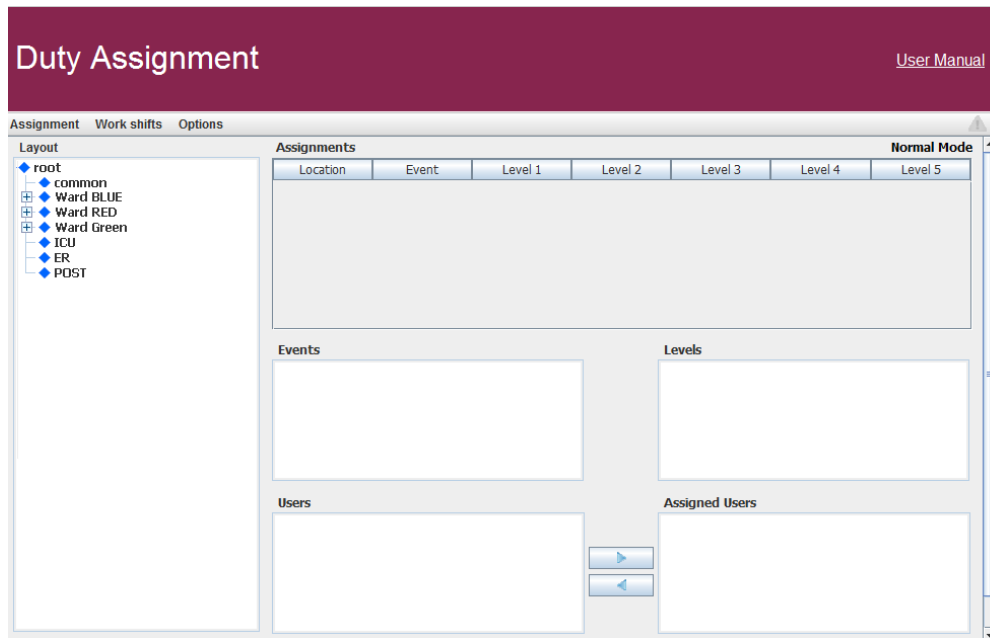
NOTE: NOTE: If the Reboot window is reloaded, this triggers another reboot.

---

## 5 Layout Setup

To set up the layout structure with locations and user teams, and set up available users for duty and location, open Duty Assignment. Only an administrator has permission to set up duties. A separate document for users and administrators describes how to assign events and levels for users. See Cardiomax Duty Assignment User Manual TD92904EN. The document can be reached via the link in the upper right corner on the entry window in Duty Assignment.

- 1 From the start page, click **Duty Assignment** and log in with your user ID and password. A window prompts you to the Duty Assignment application. Click **Run**.



The layout setup is created in the **Options** menu.

Menu	Description
Layout setup:	Add new locations and define conditions for each location. Determines who is available for duty and location.
Auto activate:	Saves the configuration periodically - the time is set in seconds. Disabled as default.

Default locations are “root” and “common”. These cannot be deleted. You can change the default location names to something else. For assignments that all locations have in common, select “common”.

User teams and users are defined in the Unite CM.

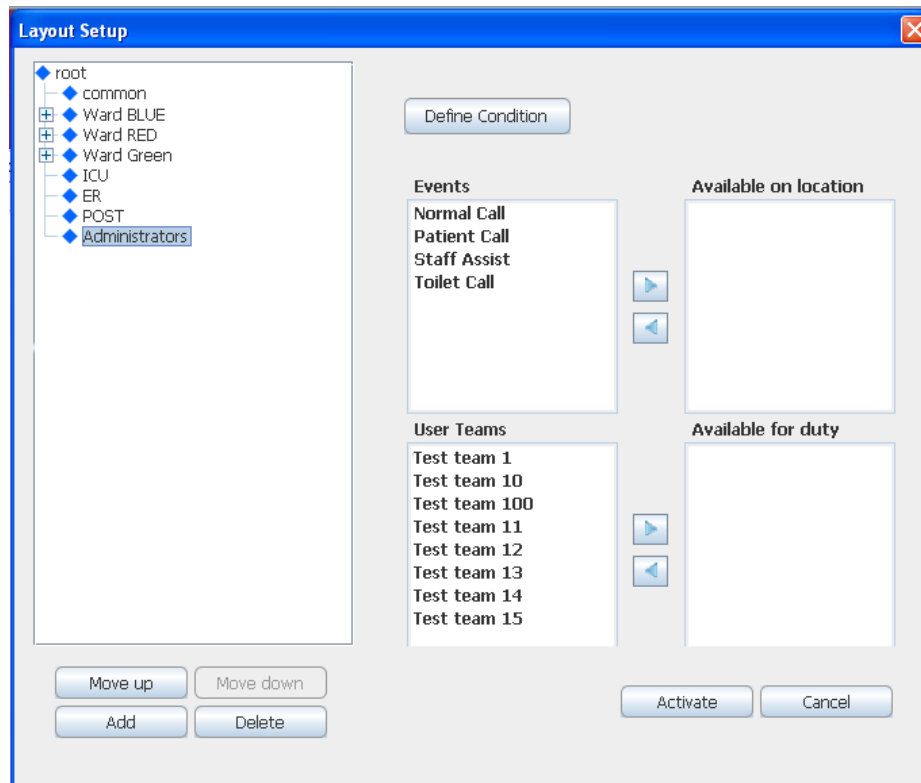
## 5.1 Adding Locations

**IMPORTANT:** When a location is added and the condition for the location is defined, the value must correspond to the value set for that location in the clinical system. If not, the alarms are not distributed. See example below:

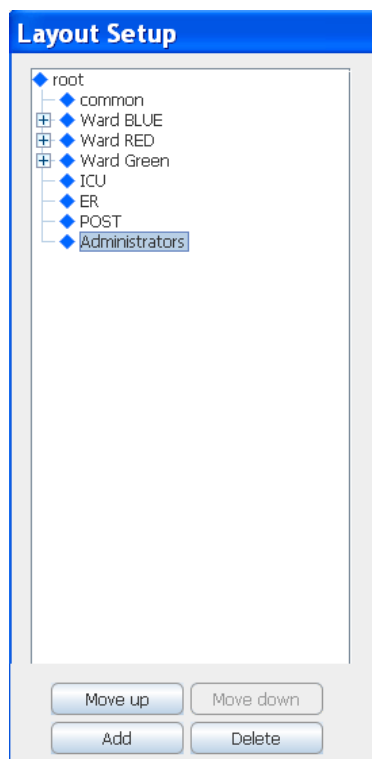
Event Element	Value
Location	ICU^RM201^BED1&1&2

By selecting a predefined event element and entering its value, an incoming event can be connected to a location.

- 1 Click **Option**, and select **Layout Setup**.
- 2 Select “root” and click **Add**.



- 3 Enter a name for the location and press **Enter**. A new field for a location is added every time you press **Enter** after the location name. After all locations are added, click outside the editing frame to stop adding fields.  
To clear an unnecessary empty field, click outside the editing frame, press **Enter** or **Esc**.
- 4 To add levels below a location, select it and click **Add**.



Enter a name for the location.

---

NOTE: To handle alarms for a location, set up conditions first.

---

## 5.2 Renaming Locations

- 1 Select the location you want to rename.
- 2 Enter a new name for the location.

## 5.3 Deleting Locations

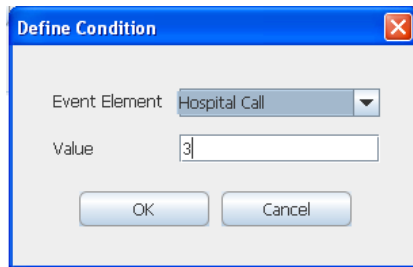
- 1 Select the location you want to delete.
- 2 Click **Delete**.

## 5.4 Defining Conditions

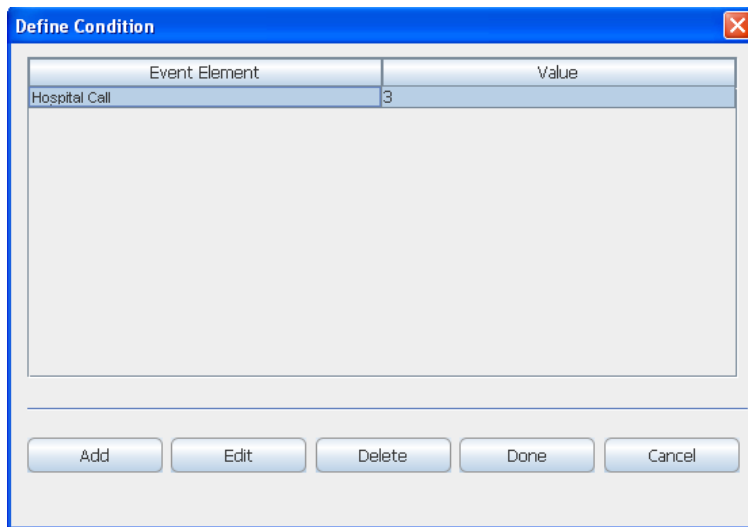
Conditions can be defined for each location, except common which is always active for assignments. By selecting a predefined event element and enter a value for it, an incoming event can be connected to a location.

To set up a condition:

- 1 Click **Define Condition**.
- 2 Click **Add**.



- 3 Select Event Element.
- 4 Enter a value and click OK.



More conditions can be defined by clicking Add. At least one condition must be fulfilled.

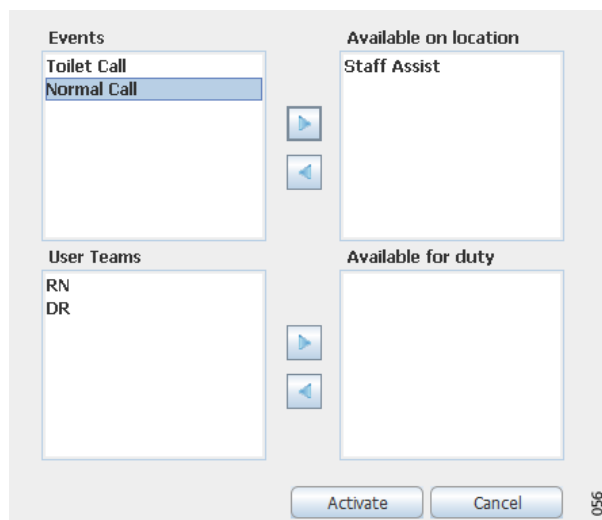
If one location has conditions matching a received event, all locations on the path between the top location and this location in the tree is selected as well, even if they do not have matching conditions.

You can edit or delete a defined condition. When finished, either click Done to save the configuration, or Cancel if you do not want to save the configuration.

## 5.5 Available on Locations

This is how you define events that should be available on a location.

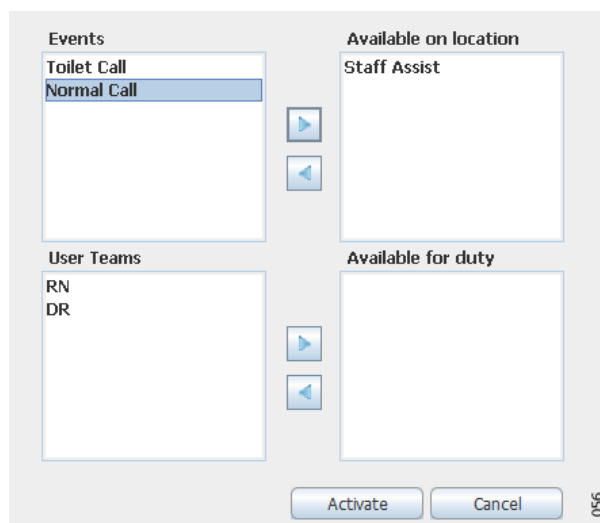




- 1 Select an event. Click the right-arrow button to move it to the **Available on location** box.  
Double-click an event to move it to the **Available on location** box.

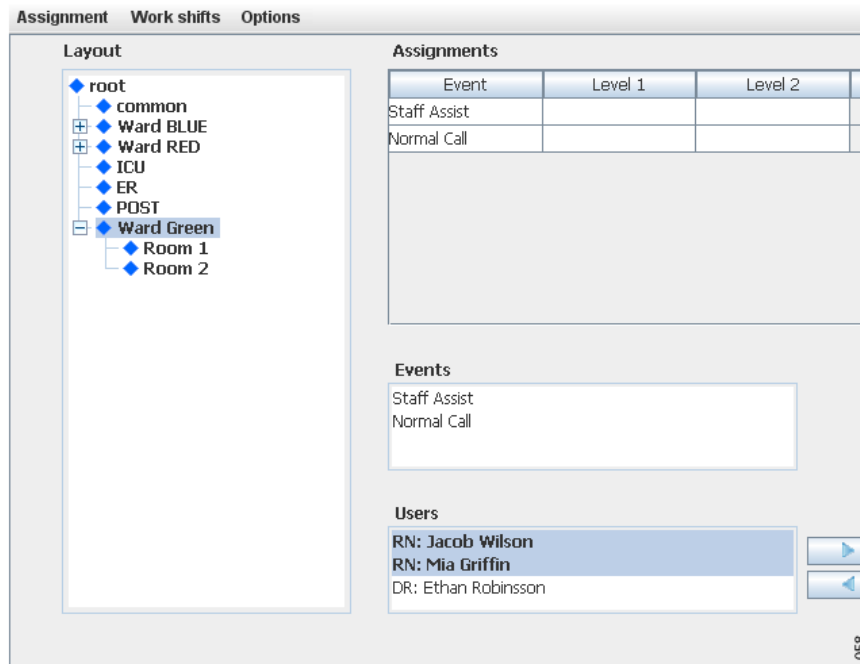
## 5.6 Available for Duty

*Defines an available user team.*

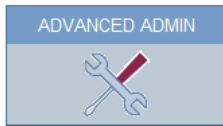


- 1 Double-click available user team.
- 2 Click **Activate**.

Once the configuration is saved, events and user teams display in main duty assignment window and the location is highlighted. Members of a user team are visible.



## 6 Advanced Administration



**Advanced Admin** enables an administrator to configure advanced administration functions. As an administrator, you can:

- Event element configuration, event handler overview, event handler log and event handler administration
- View software information, switch software
- Access rights settings
- Set languages
- Data monitoring
- Perform I/O setup
- Backup and restore configuration
- Turn on or off demonstration mode
- Use a diagnostic log to troubleshoot issues
- Upgrade software

### Removing a User Team from the Access Rights Page

- 1 Click **Access Rights**.
- 2 Click **Select User Teams**.
- 3 Select the user team whose access rights shall be removed. Move the user team from the Selected User Teams section, by clicking on the arrow pointing to the left. The user team are moved to the All User Teams section.
- 4 Click **OK**.
- 5 Click **Yes** to remove the user team from the Access Rights page.

### Deleting Invalid User Teams

Click **Delete invalid User Teams** to delete all unavailable user teams.

## 6.1 Backup and Restore

From the Advanced Admin page, you can backup and restore the configuration. The format of the backup/restore file is xxx.tar.gz.

There is also a backup/restore in the Basic Administration Web page, “xxx.xxx.xxx.xxx/admin”. This is to be used when a module should be replaced with another module in case of hardware failure, and to update the network and system configuration.

Both backup files are necessary to achieve a complete backup of the module.

- 1 To backup or restore the database, go to **Backup/Restore** in the menu on Cardiomax Configuration page.

## Backup/Restore

Backup current settings:

Backup

Restore settings:

Browse...

Restore

### Backup

- 1 Click Backup.
- 2 Click **Save** in the dialog window. The **Save As** dialog window opens.
- 3 Select a location, enter a file name, then save the file.

### Restore

- 1 Click **Browse...** to locate the .tar.gz file.
- 2 Click **Restore**.

When Cardiomax is restored, all changes that have been made since the last backup are discarded.

## 6.2 Diagnostic Log

The diagnostic log contains information that assists in troubleshooting the operation of the module. The maximum size of a log file is 100 KB. When a log file is full, another one is created. The module has capacity to store 50 log files. When the limit is reached, the log is rotated.

All processing related event messages published to the diagnostic log is also published to the Activity Log on the Unite Connectivity Manager.

### Search Page

To search the diagnostic log files, go to Diagnostic Log in the left menu of the Advanced Admin page.

Field	Description
Search for	A regular search expression
in column	Search in columns 1-5. The number of columns depends on what is selected from the drop-down list under <b>View</b>
	<ul style="list-style-type: none"><li>• <b>DefaultDB:</b> 2 columns to search in - one Action list and one Info list</li><li>• <b>Full:</b> 5 columns to search in - Text 1 - Text 5, user defined information</li><li>• <b>Short:</b> 1 column to search in - Text 1, user defined information</li></ul>

Start/End Time	The time interval for the search result
Max no of rows	1- 50

### Downloading Diagnostic Logs

You can download the log file from the module. The log file is compressed. Each line in the log file corresponds to a log entry. The information is separated by a space. The format of the log file is as follows:

Field	Description
Date	The date (local date) when the log entry was written
Time	The time (local time) when the log entry was written
Identity	The host name of the module
Application	The application in the module that generated the log entry
Log type	Indicates the seriousness of the log entry
Application identity	The application has an identifying name
File	This is the file that the log entry concerns
Log info	A text string within apostrophes. The text string can be divided into columns. Each column is separated by a carriage return character

## 6.3 Upgrade Procedure

Cardiomax can be upgraded, but not all later software revisions allow application upgrades. A complete image may be required. Please refer to the software release notes for details.

### 6.3.1 Software Backup

---

**IMPORTANT:** Before upgrading Cardiomax, you must back up your Cardiomax configuration.

---

- 1 From the start page, click **Advanced Admin**.
- 2 Click **Backup/Restore** to restore the backup. Click **Backup**.

### 6.3.2 Software Installation/Upgrade

- 1 From the start page, click **Advanced Admin**.
- 2 Click **Upgrade**. The Software Installation window appears.
- 3 Select a software (.pkg) to upload. The software replaces the previously installed software.
- 4 Select Switch immediately to install the new software.
- 5 Select Use factory default settings when upgrading (only necessary for versions prior to version 6.0.1).
- 6 Click Start Installation.

### 6.3.3 Restoring Software

- 1 From the start page, click **Advanced Admin**.
- 2 Click **Backup/Restore** to restore the backup. Select Restore settings (only necessary for versions prior to version 6.0.1).

## 6.4 Event Elements

Event elements contain information about an event that has occurred. Event elements can be used for filtering, actions, addressing, assignment location conditions, and message content. The following event elements are available.

## 6.5 Spacelabs Clinical Systems

Name	Description
EventTimeDate	Contains the Event Time element value in the Clinical Event Message received from the Spacelabs Clinical Event Interface
PatientName	Contains the Patient Info Name element value in the Clinical Event Alarm Message received from the Spacelabs Clinical Event Interface
PatientID1	Contains the Patient Info ID1 element value in the Clinical Event Alarm Message received from the Spacelabs Clinical Event Interface
PatientID2	Contains the Patient Info ID2 element value in the Clinical Event Alarm Message received from the Spacelabs Clinical Event Interface
BedLabel	Contains the Bed Info Name element value in the Clinical Event Alarm Message received from the Spacelabs Clinical Event Interface
BedNodeID	Contains the Bed Info NodeID element value in the Clinical Event Alarm Message received from the Spacelabs Clinical Event Interface

UnitName	Contains the Unit Name element value in the Clinical Event Alarm Message received from the Spacelabs Clinical Event Interface
AlertText	Contains the Event Data element value in the Clinical Event Alarm Message received from the Spacelabs Clinical Event Interface
Priority	Contains the Priority element value in the Clinical Event Alarm Message received from the Spacelabs Clinical Event Interface
AlarmData_Parsed	Contains a character substring derived from the Clinical Event Alarm Message Event Data element. The start and end character values are configured in the CSIM Administration interface.

## 6.6 Philips Clinical Systems

Name	Description
AlarmState	Contains a value representing the current state of a received HL7 ORU message. For each unique location identifier, when an alert is initiated, the value is “Active” to represent an active alarm. When this alert is no longer present, the value is “Inactive”.
Location	Contains the Assigned Patient Location value in the HL7 ORU message received from the medical device system. This element serves as the location unique identifier value
BedLabel	Contains the Bed Label value in the HL7 ORU message received from the medical device system. The value is the bed label as configured on the Information Center within the medical device system.
RoomLabel	Contains the Room value in the HL7 ORU message received from the medical device system. The value is the room as configured on the Information Center within the medical device system.
UnitName	Contains the Clinical Unit Name value in the HL7 ORU message received from the medical device system. The value is the Point Of Care as configured on the Information Center within the medical device system.

Priority	Contains the group of observation identifier values in the HL7 ORU message received from the medical device system. Includes each priority value for all OBX alert segments, comma delimited.
AlertText	Contains the group of observation result values in the HL7 ORU message received from the medical device system. Includes each alarm text for all OBX alert segments, separated by new lines.
AlarmTextWithSeverity	Contains the group of observation result values in the HL7 ORU message received from the medical device system. Includes each alarm text and severity for all OBX alert segments, new line delimited. Example RED: ***HF > 120
EventTime	Contains the time stamp associated with the clinical event as provided the medical device system.
EventDate	Contains the date associated with the clinical event as provided the medical device system.



## 6.7 Nihon Kohden Clinical Systems

Name	Description
BedLabel	Contains the SourceToken element value in the Send Pager Notification Request message received from the Nihon Kohden Pager Gateway. Token is used to associate a bed number.
AlertText	Contains the Description element value in the Send Pager Notification Request message received from the Nihon Kohden Pager Gateway. Description is the text that is displayed on the device.

## 6.8 Mindray Clinical Systems

Name	Description
TAP_PagerID	Contains the received TAP 1.8 pager ID value in the Alarm Paging Message.
UnitName	Contains the Panorama name value within the message body text in the Alarm Paging Message.
BedLabel	Contains the Bed value within the message body text in the Alarm Paging Message.
AlertText	Contains the alarm text value within the message body text in the Alarm Paging Message.
TAP_MessageBody	Contains the complete message body text in the Alarm Paging Message

## 6.9 DigiStat Connect Clinical Systems

Name	Description
AlertText	Contains the group of active, non-filtered alerts for a device
TranslatedAlertText	Contains the group of active, non-filtered alerts for a device, using translated alert text provided by UMS
DeviceType	Contains a 3 character mnemonic description of device type, e.g. MON=monitor, VEN=ventilator

AlertType	(Physio, Technical, other, unknown)
DeviceTypeLocation	A combination of device type and device location which identifies a unique device.
Status	The status of an alert - (Active, Cleared)
ExternalLocation	The location identifier provided by UMS (Includes unit and bed)
ExternalUnit	The unit component of the location identifier provided by UMS
ExternalBed	The bed component of the location identifier provided by UMS
PatientGender	The patient name provided by UMS
UniteLocationId	This is the unite location identifier
UniteUnitId	This is the unite unit identifier
Priority	High, medium, low - The priority of the highest priority alert in the message
NumericPriority	(2,3,5,7[info]) these map to High/Medium/Low/Info

## 6.10 Default Event Elements

Name	Description
Symbol_High_Priority	Contains the high priority symbol, “!!!”. This event element can be included in the message to provide a priority indication to the user.
Symbol_Medium_Priority	Contains the medium priority symbol, “!!”. This event element can be included in the message to provide a priority indication to the user.
Symbol_Low_Priority	Contains the low priority symbol, “!”. This event element can be included in the message to provide a priority indication to the user.
Clinical_System_Type	Contains the type of clinical system that produced the clinical alarm. This value is “Patient Monitor Event”.

Event_Type	Contains the type of clinical system event. The value of this element is “Clinical” for clinical events and “Technical” for technical events.
Event _Text	Contains the description associated with a technical alarm event.

## 6.11 Technical Alarms

The module will publish technical alarms when certain failures occur during operation. The “Event\_Type” event element value is set to “Technical” and the “Event\_Text” event element value contains the text description pertaining to the technical alarm.

## 7 Network and Security Recommendations

This section describes recommended network scenarios for the highest possible network security.

Other measures taken to prevent automatic scripts, or similar, to force a way into the system are:

- Incoming IP traffic is only allowed on selected ports in use
- No services, (such as web server, mail server etc.) show type and version
- Protection against modification of executable files

It is recommended that the messaging system is placed on a separate subnet (VLAN). Advantages include:

- Isolates system from the LAN
- Broadcasts in the LAN will not load the CPU of the messaging module
- Less traffic handling for the messaging modules

### 7.1 Encryption

All information transferred within the system is encrypted with a 128-bit encryption algorithm.

### 7.2 IP Ports

The following ports on Cardiomax are open:

Port	Application or Unit	Transport protocol
20-21	FTP traffic (inbound) outgoing traffic	TCP
25	Simple Mail Transfer Protocol (SMTP)	TCP
53	Domain Name Server (DNS)	UDP
68	DHCP	UDP
80	Web traffic (HTTP)	TCP
113	Authentication for mail server	UDP
123	Time synchronization (NTP)	UDP
162	Simple Network Management Protocol (SNMP)	UDP
443	Web traffic (HTTPS)	TCP

Port	Application or Unit	Transport protocol
10132-10135	GUI for Duty assignment, Action configuration and Event assignment	TCP
3217	Unite traffic	UDP
8080	Web traffic (HTTPS)	TCP

---

NOTE: The Nihon Kohden Pager Gateway port & Philips Parameter Data Interface port can be changed to match the configuration of the Spacelabs CEI Server or IntelliVue Information Center respectively. Any port number can be chosen as long as it is not used by another application or service.

---

## 7.3 Proxy Settings

If your corporate network is using a proxy server, Cardiomax must send all outgoing requests through the proxy server to be able to send the requests outside the corporate network.

- 1 Click “CSIM CONFIGURATION” from the start page.
- 2 Click “Network”.
- 3 Select “Proxy” under Security in the menu on the Advanced Configuration page.
- 4 Enter/Select the following:

Proxy:	Determines if the proxy settings below are to be used
HTTP proxy address:	The proxy server address
HTTP proxy port:	The port the proxy server is listening to

## 8 Module Redundancy

A redundant system consists of an active Unite module and a standby Unite module. When setting up redundancy in the system, the primary module will act as an active module, and the secondary module will act as a standby module.

If the active module fails, the system will automatically switch to the standby module which then becomes the active module. The modules will indicate that the system is no longer redundant since no data synchronization between the two modules can be performed.

---

**IMPORTANT:** A redundant system does not replace a backup of a module.

---

### 8.1 Prerequisites

In order to set up module redundancy, the following requirements must be fulfilled:

- The hardware variant must be identical on both the primary- and secondary module.
- The installed software application and software version must be identical on both modules.
- The modules must use the same type of SD card of minimum 1 GB capacity.
- The primary module must have the license with redundancy functionality installed.
- The secondary module must NOT have any licenses installed.
- RS232 Data Splitter. Only required if you want to connect equipment via serial interface (for example external equipment via TAP or ESPA protocol).
- Three static IP addresses. Ask your network administrator to obtain the IP addresses.
- Cardiomax must be supervised by a Unite CM. The Unite CM is used to report if Cardiomax goes down. Make sure that the Unite CM is configured to redirect any Cardiomax failures to dedicated users.

## 8.2 Preparing IP Addresses in a Redundant System

### Cardiomax Advanced Configuration

System Setup

Troubleshoot

Home

---

Network

Require network connection

?

Yes ▾

DHCP

?

Disabled ▾

IP address

?

172.20.96.244

Default gateway

?

172.20.96.2

Subnet mask

?

255.255.255.0

---

**NOTE:** It is assumed that your system already has one Unite module installed and that an additional Unite module is installed in order to set up a redundancy system.

---

The three static IP addresses are used as follows:

- Two IP addresses are used by the primary and secondary Unite module.
- The third IP address is used by the equipment (for example IP-DECT Base Stations, VoWiFi handsets etc.) to interact with the active Unite module when the system has become redundant. In this document, the third IP address is called “virtual IP address”.

---

**NOTE:** You can enter primary and secondary IP addresses from different subnets using a virtual IP address. When a system uses a primary and a virtual IP on the same subnet and the secondary IP address is located on a second subnet, redundancy synchronizes and displays “data in sync.” Upon, failover, the secondary IP address takes over, but the virtual IP does not work for the secondary IP address.

---

---

**WARNING:** : When using multiple subnets is not recommended or allowed, you will not be able to enter them.

---

To avoid changing the configured Unite IP address in the equipment that will interact with the active Unite module, follow the instructions below:

#### Network without DHCP

- 1 Replace the IP address in the origin Unite module with the static IP address to be used by the primary module. The replaced IP address can now be used as virtual IP address by the external equipment.
- 2 Make sure the other Unite module to be used as secondary module has been assigned the correct IP address.

#### Networking with the DHCP Server

- 1 Make sure that the origin IP address of the Unite module no longer is reserved to the Unite module's MAC address. Note the IP address still must be available but not reserved to a specific MAC address. Consult your network administrator. This IP address is used as virtual IP address later.
- 2 Ask your network administrator to reserve a new static IP address to the origin Unite module that later is used as primary module. The IP address must be reserved to the module's MAC address.
- 3 Ask your network administrator to reserve a static IP address for the Unite module to be used as secondary module. The IP address must be reserved to the module's MAC address.

## 8.3 Configuring Redundancy

Do the following on the Unite module to be used as primary module:

- 1 Click **CSIM Configuration** from the start page.
- 2 Click **Network**.
- 3 Click the **Home** button.
- 4 Select **Other > Redundancy** on the Configuration page.

### Redundancy

#### Configuration

Configuration of module redundancy

Virtual IP address:	<input type="text"/>
Virtual netmask:	<input type="text"/>
Secondary IP address:	<input type="text"/>
Network monitor IP address:	<input type="text"/>
<div><input type="button" value="Activate"/> <input type="button" value="Deactivate"/></div>	



---

NOTE: Before proceeding, make sure that the SD memory cards are inserted in both modules.

---

- 5 In the Virtual IP address text field, enter the virtual IP address.
- 6 In the Virtual netmask text field, enter the netmask of the virtual IP address.
- 7 In the Secondary IP address text field, enter the IP address of the secondary module.
- 8 In the Network monitor IP address text field, enter the IP address of the equipment to be used as network reference. The Unite module will check that it has connection to the network by sending ICMP (Internet Control Message Protocol) ping inquiries to this equipment every second. If you do not want you use a network reference, set the IP address to 127.0.0.1.

---

NOTE: The network topology used in the system may have impact on which equipment that should be used as network reference.

---

#### 9 Click Activate

---

NOTE: Once “Activate” is pressed, it is not possible to undo the activation of the module redundancy. However, it is possible to deactivate the module redundancy by clicking Deactivate and then click Really deactivate. The module reboots immediately. The GUI is not updated automatically when the reboot is done. To refresh the GUI, press F5.

---

#### 10 Click Reboot now or Reboot later.

The module reboots and copies data from its internal flash memory to the SD memory during the start-up sequence. This can take up to 3 minutes. The GUI is not updated automatically when the reboot is done. Update the GUI by pressing **F5**.

---




NOTE: Primary is stated in the GUI's upper-left corner when the module is up and running again.

---

Do not remove the SD memory card from Cardiomax that acts as primary module. The SD memory card on that module is used as storage even when the module redundancy has been deactivated.

When the data has been copied, the primary module sends configuration settings to the secondary module that reboots and applies the settings. After the reboot, the data is synchronized with the secondary module's SD memory card. It can take up to one hour to synchronize all data to a

SD memory card with 1 GB capacity the first time. During this time, the primary module is fully operational.

		Status LED	Power LED
Active module during synchronization	Red		Blue
Synchronized active module	Blue		Blue
		Status LED	Power LED
Standby module during synchronization	Yellow		Blue
Synchronized standby module			Blue

It is also possible to view the synchronization status via the GUI. Use the virtual IP address to access the active module and the static IP address to access the standby module.

**Status information shown on the primary module's Configuration page.**

## Information

Status	Application problem
Number of Active Faults	0

Software Version	4.02-A
Module Key	00129413
License Number	XXXXXXXX80000818
Additional License Number	XXXXXXXX06BE836B
Hardware type	Elise3 Standard

Data Storage	SD card
Redundancy Sync Status	Data out of sync

MAC Address	00-01-3e-01-f9-85
Host Name	Elise
IP Address	10.30.4.131

Service Discovery Domain	E3-ST-UniteMC1
--------------------------	----------------

NTP Server	10.30.0.101
Time	2011-12-07 13:54:55
Uptime	6d 4h 18m 37s

### Status information shown on the secondary/standby module

Module in redundancy standby	
Software Version	4.00-A
Module Key	00129413
Redundancy Sync Status	Data in sync
Virtual IP Address	10.30.6.246
Primary IP Address	10.30.4.129
MAC Address	00-01-3e-01-f9-85
Host Name	Elise
IP Address	10.30.4.131
Uptime	0d 21h 36m 56s

---

NOTE: You cannot make settings on a standby module.

---

In the Redundancy Sync Status field, the following status can be shown:

- **Synchronizing:** The synchronizing is in progress. Additionally, a counter shows the amount of data (in percentage) that has been synchronized.
- **Data in sync:** The modules are synchronized meaning that all data has been copied to the secondary module that now will act as standby module and the Primary module will act as active module. The system is redundant when this status is shown.
- **Data out of sync:** The modules are not synchronized. This is shown for example if the connection to the other module is lost.

When the system has become redundant, the virtual IP address is used by the module that currently is active.

### 8.3.1 Module Redundancy Testing

---

**IMPORTANT:** ; Perform a module redundancy test to ensure that you have configured the system correctly.

---

- 1 Unplug the active module's power cord from the power source.  
The standby module starts up and becomes an active module which takes up to 80 seconds before all applications are up and running.

The status LED flashes red  indicating that the system no longer is redundant since the connection to the primary module (former active module) is lost.

When the standby module has become active, the power LED changes to steady blue, but the status LED is unchanged as long the system is not redundant.

- 2 Go to the secondary module using the virtual IP address. Note that secondary in the upper-left corner indicates that this module currently is the active module.
- 3 View the log on the Unite CM that supervises the module. From the Unite CM, select **Status > Active Faults** on the Configuration page. The log shows for example that the secondary module is active and that the primary module has failed. Other faults might also be shown.  
TIP: The IP address of the Unite CM that supervises the module can be found in the Logging window on the module.
- 4 Perform an action to ensure that the active module works properly. For example, simulate a test alarm to see if a handset receives the alarm.
  - a. Enter the virtual IP address in a Web browser to access the active module. In this case, it should be the secondary module that has become active.
  - b. In the module start page, select Configuration > Other > Advanced Configuration and click Troubleshoot.
  - c. Click Send Test Message, enter a call ID and click Send message.
  - d. Check the handset to ensure it received the test message.
- 5 Connect the primary module and check if the secondary module starts to synchronize with the primary module. A completed synchronization is as follows:
  - On the secondary module, the status LED and the power LED are steady blue as long the module acts as an active module.
  - On the primary module, the status LED is turned off and the power LED still flashes blue as long the module acts as a standby module.
  - The synchronization status on both modules is changed to data in sync when the data is synchronized.

After the test, switch back to the primary module.

### 8.3.2 Restrictions on an Active Secondary Module

A secondary active module has restricted functionality:

---

**IMPORTANT:** The secondary module can only be up and running as active module for 30 days without a connected repaired primary module. If you shut down the secondary module on day 10, it can still use the remaining twenty days when it is started again. If the repaired primary module is not connected within 30 days, the secondary module falls back as a standby module. This means that no alarm notifications can be forwarded to the users since no module is up and running.

---

It is not possible to:

- Disable the module redundancy

- Use the Troubleshoot mode
- Perform a backup/restore
- Add a license
- Run the wizard
- Activate the demonstration mode

### 8.3.3 Fallback to the Primary Module

When a secondary module has become an active module, it will only switch back to the primary module if the secondary module goes down. It is possible to manually switch back to the primary module when it is in standby mode after repair.

---

**NOTE:** If you reboot the secondary module via the GUI, the primary module will not take over as an active module. However, if the secondary module is not up and running again after 3 minutes, the primary module become active.

---

On the secondary module, perform the following:

- 1 From the Start page, Click **CSIM Configuration**.
- 2 Click **Network**.
- 3 Click **Home**.
- 4 From the Confirmation page, select **Other > Redundancy**.
- 5 Click the **Advanced** tab, then click **Redundancy**.
- 6 Click **Fallback to primary module**.

---

**NOTE:** If you reboot the secondary module via the GUI, the primary module will not take over as an active module. However, if the secondary module is not up and running again after 3 minutes, the primary module become active.

---

The primary module now acts as an active module and the secondary module acts as a standby module.

### 8.3.4 Deactivating Module Redundancies

---

**NOTE:** This setting can only be performed on the primary module.

---

- 1 From the Start page, click **CSIM Configuration**.
- 2 Click **Network**.
- 3 Click the **Home**.
- 4 From the Configuration page, select **Other > Redundancy**.

- 5 Click the Advanced tab and then click **Redundancy**.
- 6 Click the **Deactivate**.
- 7 Select one of the following:
  - Click **Cancel deactivate** to undo the deactivation
  - Click **Really deactive** to perform the deactivation. Both modules immediately reboot. The GUI is not updated automatically when the reboot is done. Update the GUI by pressing **F5**.
- 8 Do one of the following:
  - If the IP address was changed in the primary module: Change the IP address in the former primary module to its origin IP address.

---

**NOTE:** If a DHCP server is used, ask your network administrator to reserve the IP address to the module's MAC address.

---

- If the module's IP address was changed in the equipment that communicates with the module, change back to the module's origin IP address.

---

**IMPORTANT:** Do not remove the SD memory card from the former primary module since the card also is used as storage when the module redundancy has been deactivated.

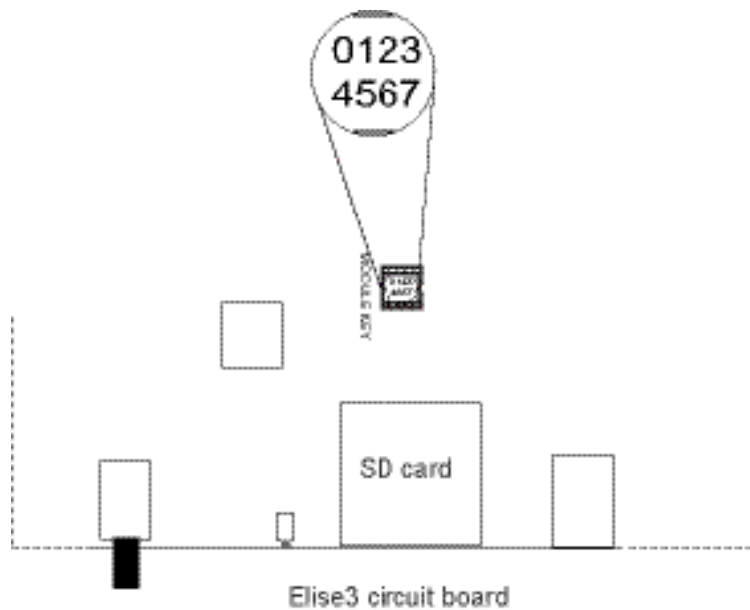
---

## 8.4 Replacement of a Broken Module in a Redundant System

This section describes how to replace a broken (i.e. hardware fault) primary module in a redundant system.

To replace a broken primary module:

- 1 Disconnect the power source and other cable connections from the primary module.
- 2 Loosen the four screws on the backside of the module by using a Torx (T-10) screwdriver.
- 3 Open the housing by pulling top cover towards the backside of the module.
- 4 Remove the module key.



To replace the module:

- 5 Loosen the four screws on the backside of the module by using a Torx (T-10) screwdriver.
- 6 Open the housing by pulling top cover towards the backside of the module.
- 7 Replace the module key with the one from the broken module.
- 8 Connect the power source and other cable connections to the primary module.
- 9 Insert a SD card into the module.

---

**NOTE:** The vendor and capacity must be identical as the SD card inserted in the secondary module.

---

- 10 Configure network settings and license settings.
- 11 Configure the module redundancy.

When the primary module is up and running, it synchronizes with the active secondary module.

## 8.5 Data Storage Selection

It is possible to decide if configurations and data are to be stored on an external SD memory card instead of storing the information on the module's internal flash memory. The SD memory card can be used if higher storage capacity is needed.

---

**IMPORTANT:** Once a SD memory card is selected as data storage, the module uses the SD memory card permanently. This means that it is not possible to roll back to the internal flash memory later on.

---

- 1 From the start page, click **CSIM Configuration**.
- 2 Click **Network**.
- 3 Click **Home**.
- 4 From the on the Configuration page, select **Other > Data Storage**.
- 5 Click **Activate**.



## 9 Related Documents

Data Sheet, Cardiomax	TD 92905EN
-----------------------	------------

Data Sheet, Unite Connectivity Manager	TD 92739EN
--	------------

Installation Guide, Elise3	TD 92679GB
----------------------------	------------

Data Sheet, Elise3	TD 92678GB
--------------------	------------

Data Sheet, Ascom Unite Messaging Suite for Healthcare	TD 92948EN
--	------------

Configuration Manual, Unite Connectivity Manager	TD 92735EN
--	------------

User Manual, Duty Assignment	TD 92904EN
------------------------------	------------

*Documentation for the Unite Application Manager and help text in the application software.*

## 10 Document History

Version	Date	Description
G	27 September 2018	Reflects caution and note acceptance testing and addition of symbol glossary.
H	31 March 2021	Access to URSS from Task Assignment and Patient Client Options settings, and clarification of 0 indexed start index for parsed alarm text.

## Appendix A Clinical System Protocols

This appendix describes the functionality of clinical systems and any protocol specific limitations.

### A.1 Nihon Kohden Pager Service Protocol

#### A.1.1 Nihon Kohden Pager Gateway

The Nihon Kohden Pager Gateway is a software product that allows a Nihon Kohden clinical system device to provide remote pager notification of certain alarm events. The Pager Gateway software collects alarm information from all networked patient monitors in a Nihon Kohden clinical system in order to format and send pager messages to a third party delivery system.

For Pager Gateway configuration within the Nihon Kohden clinical system, refer to the manufacturer's Operator's Manual(s).

---

**NOTE:** Improper Pager Gateway and alarm configuration within the Nihon Kohden clinical system result in improper operation of Cardiomax.

---

---

**NOTE:** The module has been verified for compatibility with NK Pager Gateway Message Schema and Interaction, Version 1.0. Other versions may be compatible, but cannot be guaranteed.

---

#### Interface

The interface is designed to process Pager Notification Request Messages as SOAP/XML Web services procedure transmitted by the Nihon Kohden Pager Gateway. Communication is done over a point-to-point HTTP POST request using SOAP/XML messages.

#### Configuration

The Pager Gateway PagerURL registry key value needs to be set to:

`http://cardiomax_ip_address:8888/cardiomax.aspx`

#### Implementation Variants

None

#### Limitations

This vendor supplied interface does not provide a mechanism by which Cardiomax can detect if the communication between the alarm source and Cardiomax is disrupted

#### Technical Alarms

A technical alarm is published when a parsing error occurs with "Pager Notification Request" messages. A parsing error consists of no data being present in the received Pager Notification

Request Message SourceToken and Description elements. The Event\_Text event element value is "Pager Notification Request Parsing Error".

#### **Presets**

None

#### **Delays**

The average delay time is measured, under normal system operation, from the point that the presentation of the ALARM CONDITION arrives at Cardiomax to the time that the display device is annunciating to the healthcare professional.

The average delay time is 4 seconds.

---

NOTE: The delay time in the customer environment may vary based upon their specific environment and cannot be guaranteed.

---

## **A.2 Spacelabs Healthcare Clinical Event Interface (CEI) Protocol**

### **A.2.1 Clinical Event Interface**

The Spacelabs CEI Server is a Windows Service whose purpose is to query the Spacelabs Database for Clinical Events and send them to connected messaging applications. A clinical event is a discrete patient event, like an ECG alarm, that Cardiomax can transmit to the desired wireless device.

For CEI configuration within the Spacelabs clinical system, refer to the manufacturer's Operator Manual(s).

---

NOTE: Improper CEI and alarm configuration within the Spacelabs clinical system result in improper operation of Cardiomax.

---

---

NOTE: The module has been verified for compatibility with Spacelabs Medical CEI Client Software Interface Spec, 062-xxxx-00 rev. 3.1 and Enterprise Network Interface (ENI) Ver. A. Other versions may be compatible, but cannot be guaranteed.

---

#### **Interface**

Communication is done over a persistent point-to-point TCP/IP socket using XML messages. Cardiomax will establish a single TCP socket connection (if activated) to one CEI server at the following events:

- Start up
- Change in Clinical System Interface Manager parameters that impact the interface with CEI server

Upon connection with the CEI Server, Cardiomax will routinely receive a heartbeat message from the CEI server. If the heartbeat message is ever interrupted or delayed Cardiomax system will automatically attempt to establish a connection until successful.

### **Configuration**

The CEI Server is configured with Clinical Event Message type set for “Alarm Text Only”.

The CEI Server is configured with Vital Sign Update Message notification disabled.

Implementation Variants

None

### **Limitations**

Cardiomax only supports CEI Clinical Event Messages of type ALARM (Alarm Text Only).

### **Technical Alarms**

A technical alarm is published when a CEI server connection is established. The “Event\_Text” value is “CEI Connection Success”.

A technical alarm is published when Cardiomax detects a failure in the established CEI socket connection. The “Event\_Text” value is “CEI Connection Failure”.

A technical alarm is published when a parsing error occurs with a “Clinical Event” message. A parsing error consists of no data being present in the received Clinical Event Message BedInfo Name, BedInfo ID, UnitName, and EventData elements. The Event\_Text event element value is “Clinical Event Parsing Error”.

### **Presets**

None

### **Delays**

The average delay time is measured, under normal system operation, from the point that the presentation of the ALARM CONDITION arrives at Cardiomax to the time that the display device is annunciating to the healthcare professional.

The average delay time is 4 seconds.

---

**NOTE:** The delay time in the customer environment may vary based upon their specific environment and cannot be guaranteed.

---

## A.3 Systems supporting TAP 1.8 Protocol Output Interfaces

### A.3.1 Mindray Panorama Network

The Mindray Panorama Central Monitoring system (Mindray PMS) outputs alarm event information to the module by a point-to-point serial interface using TAP 1.8 protocol.

For alarm paging configuration within the Mindray Panorama Central Monitoring System, refer to the manufacturer's Operator's Manual(s).

---

**NOTE:** Improper alarm paging configuration within the Mindray PMS result in improper operation of Cardiomax system.

---

---

**NOTE:** The module has been verified for compatibility with Mindray PMS software version 8.9.3, Baseline version 10.9. Other versions may be compatible, but cannot be guaranteed.

---

#### Interface

Mindray's PMS default serial port settings are the following:

- Port = 2
- Baud rate = 9600
- Parity = N
- Data bits = 8
- Stop bits = 1
- Error logging = N

The default serial port settings on the module's serial ports are configured to align with the default port settings on the Mindray PMS.

#### Configuration

The module is designed to process received alarm paging messages formatted according to the Paging Demographics Option "Bed". This is the default setting for the Mindray PMS.

#### Implementation Variants

None

#### Limitations

This vendor supplied interface does not provide a mechanism by which Cardiomax can detect if the communication between the alarm source and Cardiomax is disrupted.

The Mindray PMS cannot contain any space characters in the BED label.

#### Technical Alarms

A technical alarm is published when a parsing error occurs with an Alarm Paging Message. A parsing error consists of no data being stored for the Panorama Name (UnitName), Bed (Bed-Label), and alarm text (AlertText).

The Event\_Text event element value is “Alarm Paging Message Parsing Error” when the technical alarm is published.

#### **Presets**

None

#### **Delays**

The average delay time is measured, under normal system operation, from the point that the presentation of the ALARM CONDITION arrives at Cardiomax to the time that the display device is annunciating to the healthcare professional.

The average delay time is 3 seconds.

---

NOTE: The delay time in the customer environment may vary based upon their specific environment and cannot be guaranteed.

---

## **A.4 Systems Supporting HL7v2 Protocol Output Interfaces**

### **A.4.1 Digistat Connect**

Cardiomax supports a clinical alarm-based event interface from Digistat Connect, capable of acquiring alarms and accompanying vital sign data from clinical systems. The extensible interface monitors the active alarm status of those clinical system integrated with Digistat Connect; Data Acquisition Server (DAS), and provides alert based notification to display devices indicating the onset, updates and termination of active alarms. The notification characteristics of Cardiomax supports the independent assignment of alerts based on device category, and the redirection of alerts between individuals and/or care-teams based on availability.

The clinical alarm interface established between Cardiomax and Digistat Connect is supported via persistent TCP/IP socket based connection. In this integration with Digistat Connect, Cardiomax operates as a server responsible for accepting and maintaining connections from the Digistat Connect client. Once a connection is established the two system exchanges data related to the alarm state of the clinical systems currently integrated with Digistat Connect.

This connection represents a supervised interface whereby, if specific data is not periodically exchanged between Cardiomax and Digistat client, a loss of connectivity are reported by Cardiomax in the form of distributed alert and registered as a persistent fault within the applicable Unite supervision node. The Unite supervision node and its accompanying notification methods should be configured and used to properly disseminate information about possible loss of connectivity and other system level errors possibly encountered during the use of this product.

## A.4.2 Clinical System Interface Manager – DigiStat Connect Configuration

The configuration of Cardiomax to establish and maintain the connection to DigiStat Connect begins in the Clinical System Interface Manager. After selecting DigiStat from the available list of clinical system, select the DigiStat Connect Configuration Settings link.

The following settings relate to configuring Cardiomax in combination with DigiStat connect to realize the interface functionality described above.

<b>Listening Port:</b>	Configurable TCP/IP port on which Cardiomax will await for and maintain a connection from the DigiStat Connect client. This port should match the port defined in DigiStat connect as the Unite Listening Port.
<b>Client Timeout:</b>	<p>Amount of elapsed time (in seconds) after which Cardiomax shall indicate a loss of connectivity if proper information is not exchanged over the interface.</p> <hr/> <p><b>CAUTION:</b> After Cardiomax has lost, and is unable to re-connect, the connection will be terminated and notified as cleared.</p> <hr/>
<b>Time Stamp of Alarms:</b>	The format of the time stamp associated with onset of the alarm provided in the alert distributed to display devices. The format is configurable for 12 or 24-hour format.

## A.4.3 Alarm Filters

In combination with DigiStat Connect, Cardiomax offers an array of filters that can be used to better assure that the correct alarms are being delivered to display devices. The type of filters available for use in with Clinical System supported by DigiStat Connect include, Pass, Stop, Delay and Group.



The filter operation and sequence of execution are defined in the following table.

For additional information related to the filter of alarms please see Appendix B. Cardiomax Filtering Description for details and examples.

#### **A.4.4 Clear Message Indication**

---

**CAUTION:** If Cardiomax loses connectivity for a period of time not to exceed 60 seconds, all active alarms are cleared by Cardiomax. Notifications are sent to display devices. The Cleared Alarm notification should not be used as absolute indication of a terminated alarm from a clinical system.

---

#### **A.4.5 Technical Alarms**

A technical alarm is initiated by Cardiomax if specific data is not periodically exchanged between Cardiomax and Digistat client. The sequence of events is indicated as a loss of connectivity and will be reported by Cardiomax in the form of a distributed alert.

##### **Presets**

None

##### **Delays**

The average delay time is measured, under normal system operation, from the point that the presentation of the ALARM CONDITION arrives at Cardiomax to the time that the display device is annunciating to the healthcare professional. The average delay time is 4 seconds.

---

**NOTE:** The delay time in the customer environment may vary based upon their specific environment and cannot be guaranteed.

---

### **A.5 Philips IntelliVue**

Cardiomax supports a distributed architecture in order to maximize the number of Philips clinical system locations supported by a single system. Cardiomax is based on a Hub-and-Spoke architecture, where the Hub or Central is able to provide support for up to 100 Philips clinical system locations, as well as centralized filtering and management for up to 9 Spokes or extension Modules. Each extension module provides support for up to an additional 200 Philips clinical system locations. Individual capacities for each module are based on simulations representing bursts as well as average occurrences of simultaneous alarms for any supported system size, taking in account average active alarm durations, and active alarm updates.

---

**CAUTION:** Extension modules do not maintain a persistent connection to the central module, a loss of connectivity between the extension and Central may not be detected and can result in a loss of alerts. Each extension module should be supervised separately to assure that failures are reported.

---

The Philips IntelliVue HL7 Parameter Data Interface (PDI) outputs alert data to Cardiomax (Central and extension Modules) by persistent point-to-point TCP/IP sockets using HL7, version 2.x protocol. The HL7 messages are formatted according to Phillips IntelliVue Information Center (IIC) release L HL7 PDI programmer's guide.

For PDI/HL7 Export configuration within Phillips IntelliVue, refer to the manufacturer's Operator's Manual(s).

Improper PDI/HL7 Export and alarm configuration within Phillips IntelliVue results in improper operation of Cardiomax.

The module has been verified for compatibility up to release L & M HL7 PDI programmer's guide and Philips Intellivue Information Center iX (PIIC ix) HL7 Interface (A.0x & B.00-B01)

---

**NOTE:** Other versions may be compatible, but cannot be guaranteed.

---

## **Interface**

Cardiomax supports interfacing with PDI directly and indirectly through PDI interfaces provided on the central module, as well as with additional extension modules. Each PDI interface supports up to 10 concurrent connection from PDI transmitting centrals or database servers.

Within larger systems, each extension module provides its own independent pass filter functionality, but relies on the central module for additional filtering and message routing and delivery.

The PDI client initiates TCP connection with a central or extension module, and if the connection is broken or closed, the PDI client attempts to reestablishes the connection and continues to do so until the connection is reestablished or the system is shut down.

PDI allows multiple connections, but only one connection at one time to one particular client machine as identified by the IP address.

## **Capacity**

- Max messages (pages)/hour: 6000
- Max simultaneous actions: 50
- Max alarm broadcasts/sec: 20 (central)/40 (extensions)

## **Configuration**

PDI (HL7 export)

The following parameters define those values that are not the typical default values provided by the IIC Config Wizard for HL7 Export:

- Network devices should be defined as either Cardiomax central module or available extension modules based on system size.
- The PDI unsolicited messages interface outputs alert data at a configured interval. The configured interval is set to 5 seconds (lowest possible).
- The PDI unsolicited messages interface is configured to transmit OBX for alerts and the Information Center is configured to send alerts.
- Time of day transmissions (HL7 NMD messages) is disabled in the PDI to avoid unnecessary processing by the module.
- Auto-unsolicited is enabled in the PDI.

### **Limitations**

The module does not respond with HL7 MLLP acknowledgment messages because the PDI disregards them and will not resend messages that have not been acknowledged. This is done to avoid unnecessary processing by the module.

The module only processes OBX alert segments within the HL7 ORU messages, except to determine the end of an alert by the absence of the OBX Alert segments after the onset of an alert for a given location.

### **Technical Alarms**

A technical alarm is published when a PDI server TCP/IP connection is established. The Event\_Text value is "PDI Connection Success".

A technical alarm is published when a PDI server TCP/IP disconnection occurs. The Event\_Text value is "PDI Connection Failure".

A technical alarm is published when a parsing error occurs with OBX Alert segments of an HL7 ORU message. A parsing error consists of no data being present in OBX Alerts segment field 3, component 1 and in OBX Alerts segment field 5. The Event\_Text event element value is "HL7 Message Parsing Error".

### **Presets**

None

### **Delays**

The average delay time is measured, under normal system operation, from the point that the presentation of the ALARM CONDITION arrives at Cardiomax to the time that the display device is annunciating to the healthcare professional.

The average delay time is 4 seconds.

---

NOTE: The delay time in the customer environment may vary based upon their specific environment and cannot be guaranteed.

---



## Appendix B Cardiomax Filtering Description

The filtering feature can be used to filter alarms to avoid spamming of handsets.

Four types of case-sensitive filters can be used:

- 1 Pass filters (alarms matching complete pass filter texts are accepted)
- 2 Stop filters (alarm levels and texts that match a stop filter are not sent, must be case-sensitive)
- 3 Group filters (matching alarm texts are considered to be the same alarm)
- 4 Delay filters (matching alarm texts must still be active for as long as defined in Cardiomax before the alerts are sent out)

When using delay filters, the alarm level is combined with the alarm text and must be taken into consideration when writing the filter, for example “6HR LO”.

Definitions:

- “?” equals exactly one character
- “\*” can be zero or more characters
- “|” is used as a logical OR operator (only allowed in group filters)
- “;” is used as a comment sign. A filter string beginning with a “;” will ignore all alarm text strings.

---

NOTE: The filtering feature is case sensitive.

---

Examples:

- “HR ?O” matches “HR LO” and “HR HO” but not “HR O”.
- “HR \*O” matches “HR LO”, “HR HO”, “HR O” and “HR NNO”.
- “HR LO ?|HR LO ??” matches “HR LO 9” and “HR LO 10”.
- “HR ?O” matches “HR LO” but not “AAAHR LO”.
- “HR LO;Heartrate low” also describes in plain text which alarm text that this filter will match.
- “;HR LO” is a comment and will not match anything.
- “4\*” in Alarm delay filters delays all alarms with alarm level 4.

## Appendix C Setting up Access Rights


For user administration, different access rights are given to different user teams in order to log into access rights, action configuration, event and duty assignments.

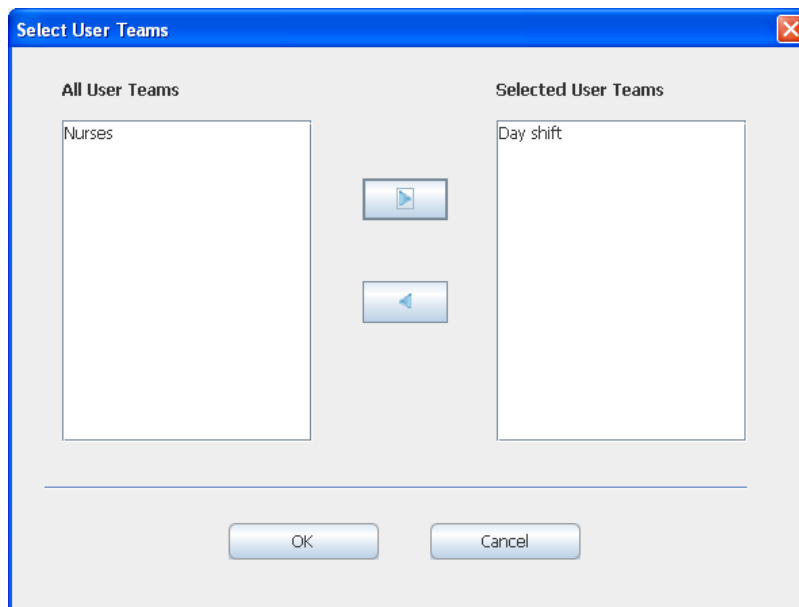
You can grant level of access to users: admin, user or none access to the GUI.

Authority	Description
Admin:	rights to administrate duty assignments
User:	rights to make assignments in duty assignments
None:	no access rights to duty assignments

User teams are set up in the Unite Connectivity Manager, see Configuration Manual Unite Connectivity Manager TD 92735EN.

To set up access rights:

- 1 From the Start page, click **ADVANCED ADMIN**. The Backup/Restore window appears.
- 2 Click **ACCESS RIGHTS** and log in with your username and password.
- 3 Click **Select User Teams**.
- 4 Select the user team that is granted access rights.
- 5 Click  to move the user team to the selected user teams.



- 6 Click **OK**.
- 7 Select which applications the user team should have access to by selecting or clearing the check boxes for access rights.

- 8 Select between, Admin, User or None for the Duty Assignment.
- 9 Click **Submit** to save the changes.

#### **Removing a User Team from the Access Rights Page**

- 1 Click **Access Rights**.
- 2 Click **Select user teams**.
- 3 Select the user team whose access rights is removed. Move the user team from the selected user teams, by clicking on the arrow pointing to the left. The user team is moved to the all user teams.
- 4 Click **OK**.
- 5 Click **Yes** to remove the user team from the Access Rights page.

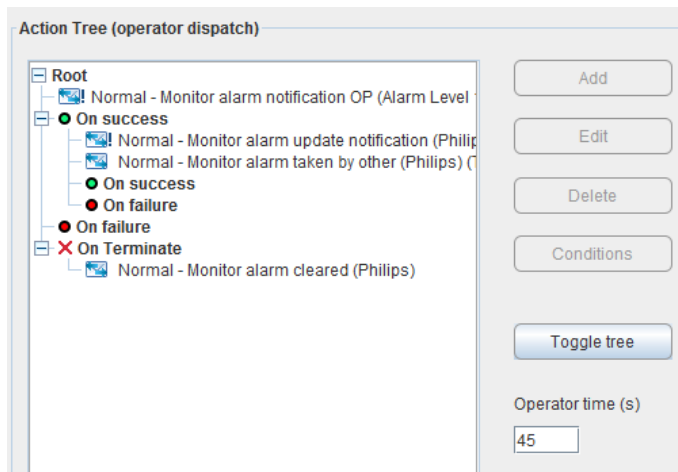
#### **Deleting Invalid User Teams**

By clicking the delete invalid user teams, all user teams not available in the system are deleted.

## Appendix D Action Tree Templates

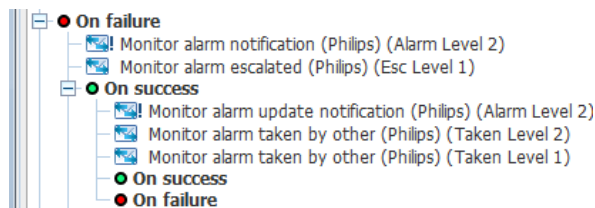
By using an Action Tree template for monitor alarm in event configuration, no actions or messages need to be set up. Four templates are available for Philips IntelliVue, Nihon Kohden, Mindray Panorama, and Spacelabs systems.

### D.1 Action Tree for Philips IntelliVue System



When a monitor alarm is received, an interactive message is sent to a recipient. If the notification is accepted, the first level “On success” is followed. The other recipients in the hunting chain is notified that the alarm has been accepted by someone, and a confirmation message is sent back to the recipient that acknowledged the alarm. All further updates for this patient will now be sent to this recipient as long as any alarm is active for the patient.

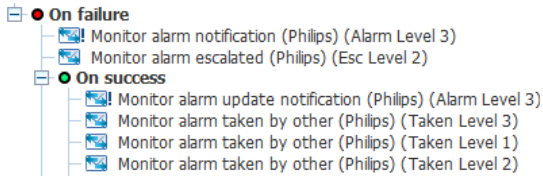
If the notification was not accepted within a specified time, the first level “On failure” is followed. Under the first “On failure” level, there are actions for what is done if the first recipient did not accept the message. These actions send the same interactive message to the second recipient and notifies the first recipient that the message was forwarded. In a similar way, a second recipient may accept or reject a message.



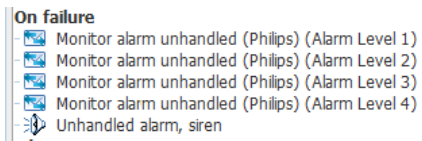


If the notification is accepted, the second level “On success” is followed, but if the notification was not accepted within a specified time, the second level “On failure” is followed.

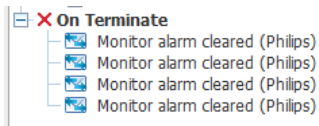
Under the second “On failure” level, actions for what is done if the second recipient did not accept the message are set up. In a similar way, a third recipient may accept or reject a message and so on.



The template has four escalation levels. For the last “On failure” level, if no recipient has accepted, a high priority message is sent to all recipients that the alarm has not been handled and an output is activated. This output could, for example, be connected to a siren.



When the alarm is cleared at the monitor a notification is sent to the recipient who accepted the alarm or, if no one has accepted yet, to all recipients that has received the alarm so far.



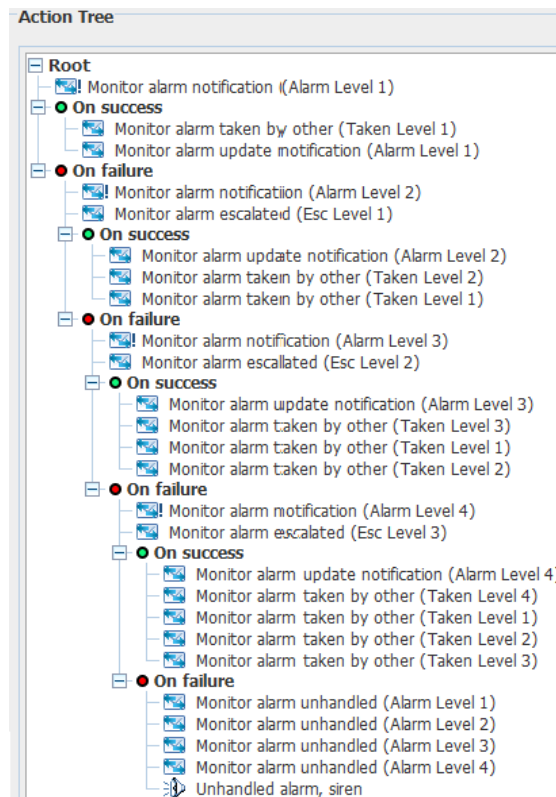
## D.2 Action Tree for Nihon Kohden, Mindray Panorama, and Space-labs Systems

---

NOTE: Nihon Kohden and Mindray Panorama is applicable for US only.

---

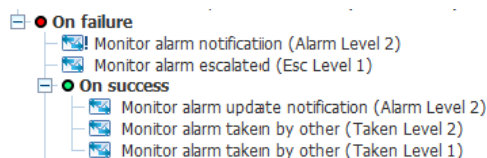
The Action Tree templates for monitor alarms for Nihon Kohden, Mindray Panorama and Space labs systems are similar. The difference to the Philips template is that there are no actions taken when the alarm is cleared. This also means that even if a recipient accepts the alarm, new or updated alarms will start a new escalation chain.



When a Monitor alarm is received, an interactive message is sent to a recipient. If the notification is accepted, the first level “On success” is followed. The other recipients in the hunting chain is notified that the alarm has been accepted by someone, and a confirmation message is sent back to the recipient that acknowledged the alarm.

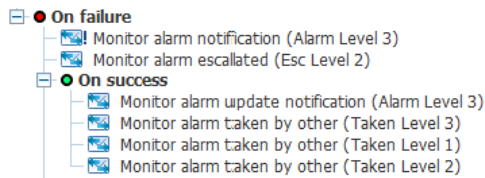
If the notification was not accepted within a specified time, the first level “On failure” is followed.

Under the first “On failure” level, actions for what is done if the first recipient did not accept the message are set up. These actions send the same interactive message to the second recipient and notifies the first recipient that the message was forwarded. In a similar way, a second recipient may accept or reject a message.

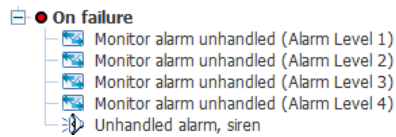


If the notification is accepted, the second level “On success” is followed, but if the notification was not accepted within a specified time, the second level “On failure” is followed.

Under the second “On failure” level, there are actions for what is done if the second recipient did not accept the message. In a similar way, a third recipient may accept or reject a message and so on.



The template has four escalation levels. For the last “On failure” level, if no recipient has accepted, a high priority message is sent to all recipients that the alarm has not been handled and an output is activated. This output could, for example, be connected to a siren.



## D.3 Action Configuration

---

NOTE: If one of the included templates is used, there is normally no need to set up actions.

---

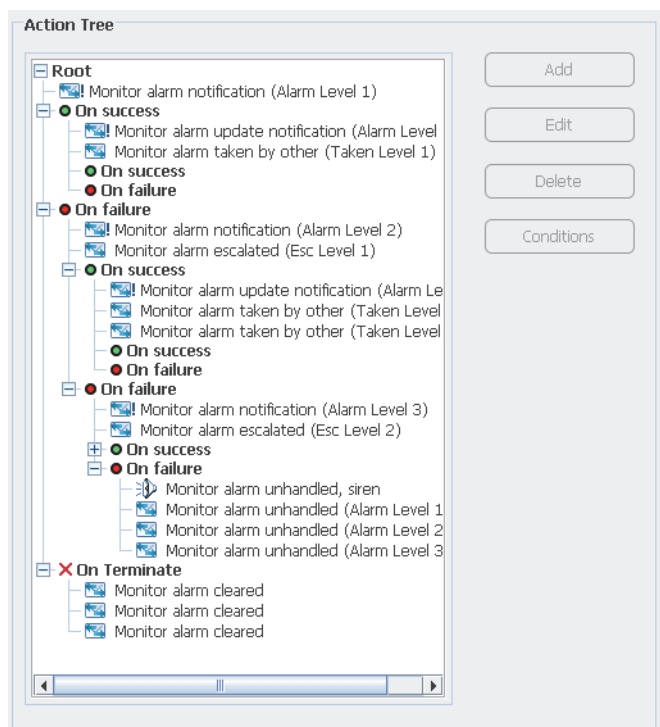
### Action Tree

---

**IMPORTANT:** Changing the action configuration may cause the Cardiomax to behave in unexpected ways. Do not change the action configuration unless necessary. Changes are made by authorized system administrators only.

---

Before describing the action configuration setup, the action tree shown in event configuration is explained.



When a monitor alarm is received, an interactive message is sent to a receiver. If the notification is accepted, the first level “On success” is followed. If the notification was not accepted within a specified time, the first level “On failure” is followed.

Under the first “On failure” level, there are actions for what is done if the first receiver did not accept the message. In a similar way, a second receiver may accept or reject a message and so on.

For the last “On failure” level, if no receiver has accepted, an output on Cardiomax is activated. This output could, for example, be connected to a siren.

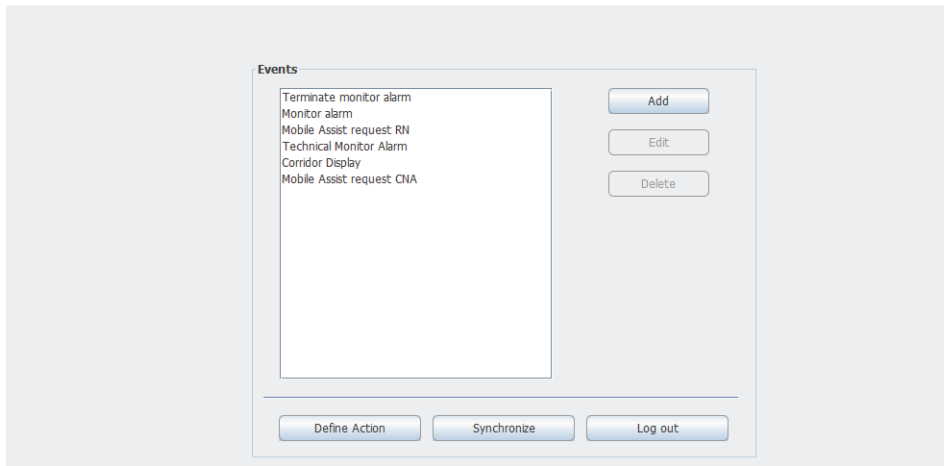
If a “Terminate monitor alarm” is received when handling the Monitor alarm, the status of the Monitor alarm will be updated in the handsets, which is shown in the bottom lines, under “On Terminate”.

### Event Configuration

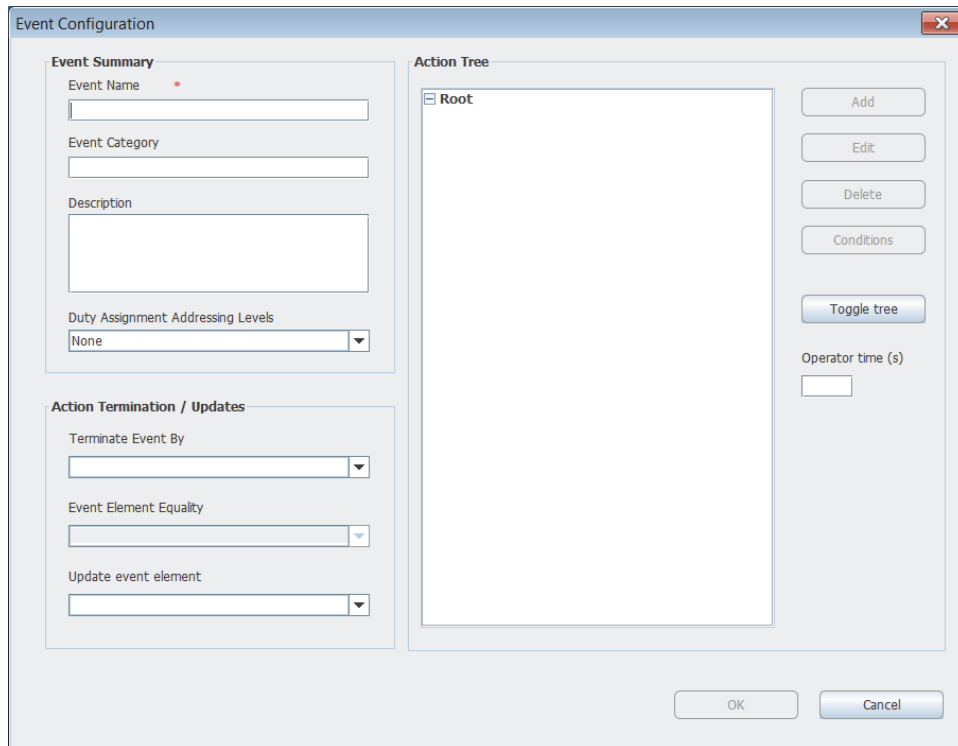
This describes how to set up an action for an event that has occurred, such as what to transmit and success and failure conditions.

- 1 In the Cardiomax start page, click **Action Configuration**.
- 2 Log in with your user ID and password.

### Action Configuration



3. Click **Add**.



4. Enter a name of the event and a description.
5. Optionally, enter a category for the event. The category will be set for all actions within this event and is a help in the search and sorting function for system activity logs.
6. Optionally, select event type for the Event. The event type tells which kind of event it is (e.g. Patient call or Emergency call). This information is used when assigning staff in Unite AM because staff, for example, can be assigned to different kind of events (i.e. event types).

- 7 Optionally, select a color for the Event. The color will be shown in the supporting display device (Myco) that receives the alert about the Event. This can, for example, be used to visualize the type of the event by color.
- 8 Select from the drop-down list duty assignment addressing levels, if duty assignment is to be used. The levels are:
  - None: Events will not be visible in the Duty Assignment.
  - 1-5: up to five addressing levels can be selected.
- 9 Mark Root in the Action Tree and click Add to configure actions for an event.

The screenshot shows a configuration window with the following elements:

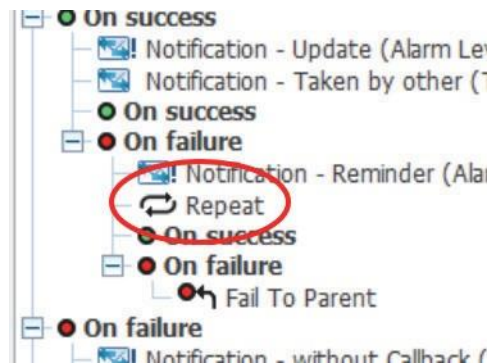
- Action Type:** A dropdown menu with 'Message' selected.
- Actions:** A dropdown menu with 'Assist notification' selected.
- Reference:** An empty text input field.
- Work Shift:** A dropdown menu with 'Always' selected.
- Message ID:** An empty text input field.
- Exclude replier address:** A checkbox that is currently unchecked.
- Define Action:** A button to the right of the Actions dropdown.

- 10 Select an **Action Type** from the drop-down list:

Action Type	Description
Message	To send messages to a specific destination and with a confirmation request.
Interactive Message	To send messages with different response options included. The response is sent back with chosen option.
Output Activity	To set or reset an output, for example to remotely turn on a siren or close a door.
Erase Message	To erase a sent message.
Repeat	<p><i>To repeat an action specified number of times at an interval defined by the failure</i></p> <p><i>To set the interval, see Adding Success/Failure Conditions.</i></p> <p><i>Example: If the repetition for the Notification - Reminder (Alarm) action is set to 3 times and the Failure Timeout is set to 10 seconds, the action will be</i></p>

*repeated 3 times with 10 seconds  
between each interval.*

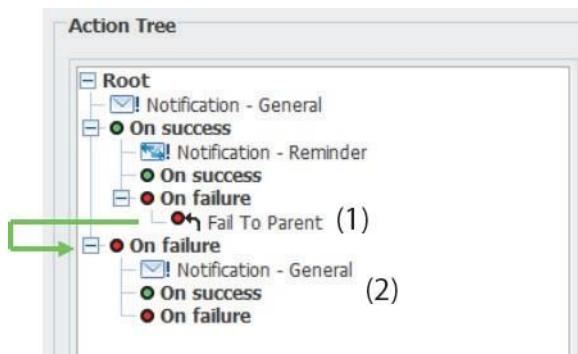
*Optionally; by utilizing the Failure on  
Timeout Only setting (available on the  
condition), a repeat node can continue run  
when other messaging components are  
unavailable. (see Failure on Timeout  
setting below)*



Example: If the Notification - Reminder within the child node fails (1), the event will be escalated to the first un-executed on failure condition on the parent node (2). In this case, the Notification - General is executed once again.

### Fail to Parent

To escalate an event to the first un-executed On failure condition on the parent node.



- 1 Select **Actions** from the drop-down list. If it says "No Items" in the drop-down list, click Define Action to add items to the action list. See Define action to add new actions.
- 2 Enter a reference. in a "message" a reference is set for the message that is going to be sent and the same reference is used to erase that message.
- 3 When the action type erase message is selected and the Exclude replier check box is selected, the message will be kept in the handset that most recently fulfilled a success condition.

- 4 When message and interactive message are selected and the Exclude replier check box is selected, the message will not be sent to the handset that most recently fulfilled a success condition.
- 5 Enter a message ID. This enables a possibility to update messages in a handset. If this field is left empty it is not possible to update that message later.

An example on how to use message IDs, based on the Ascom standard template:

- A new alert is sent to a user on level 1 with Message ID "Id Level 1".
- The user does not respond, so the alert is escalated to level 2.
- The alert is sent to the user on level 2.
- A notification about the escalation is sent to the level 1 user with the same message ID as in the first alert (Id Level 1). The handset updates the message.

### Defining Actions

- 1 Click **Define Action** and click **Add**.
- 2 Select Action Type from the drop-down list:

- Message
- Interactive message
- Output activity

In this example, the interactive message has been selected.

The screenshot shows a dialog box titled "Define Interactive Message". At the top, there is a "Name" field with the text "Monitor alarm notification". Below this, there are two tabs: "Message" and "Options". The "Message" tab is currently selected, displaying several input fields: "Subject" with the text "ACTIVE <!LocRight>", "Body" with the text "<!AlarmLevelText>", "<!Alarm text>", and "Date: <!Date>", "Beep Code" with a dropdown menu showing "Not set", "Reminder, session" with a text field containing "0" and a "minutes" label, "Reminder, attention" with a text field containing "0" and a "seconds" label, "Priority" with a dropdown menu showing "<!NumericPriority>", "Time To Live" with a text field and a "seconds" label, and "Sticky Mode" with a dropdown menu showing "On". At the bottom of the dialog, there are "OK" and "Cancel" buttons.

### Message Tab

Enter the following:



Name	Enter a descriptive name of the action
Subject	Enter the subject for the message
Body (optional)	Enter the text that should be included in the message. Select the message alert to be played in the handset when it receives this message.
Beep code	Select the message alert to be played in the handset when it receives this message.
Reminder, session (optional)	Enter the interval between indications for unread message. Values: 1-255 seconds.
Reminder, attention (optional)	Enter the time between indications before any option has been selected in this message.  Typically, if the recipient has opened the message, but has not select an IM option, a message alert will sound. Values: 1-255 seconds.
Priority (optional)	Enter the message priority.
Time to Live (TTL) <sup>a</sup>	Enter the time this message should remain in the handset. When the TTL expired, the message is deleted in the handset.
Sticky mode (optional)	Select if the display should be locked for the message. When receiving that message, the display will lock and remain locked until the sticky mode is turned off. Typically, one option has to be selected before leaving the message.

a. TTL is not supported by all handsets.

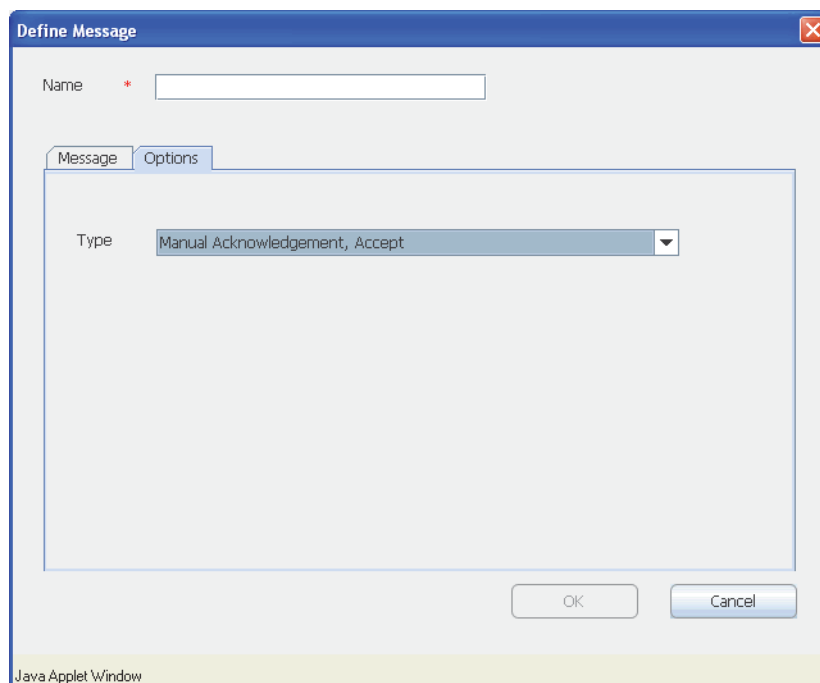
**TIP:** Right-click in the text fields for Subject and Body, to insert predefined event Elements. This is only possible if a synchronization has been done, see D.3 Action Configuration.

Options are set for Message and Interactive Message response. The information in the Option folder will look different depending on which Action Type that has been selected.

#### Options Tab – Message

When sending a message, you can add a message response. It can be with acknowledgement accept only where you will know that the user has acknowledge the message or acknowledgement with accept and reject where the user also will have the possibility to reject the message. If nothing is chosen it will be with no message response, which is the default type.

- 3 Click the **Options** tab to add a type of message.



The screenshot shows a 'Define Message' dialog box with a blue title bar and a close button. It has two tabs: 'Message' and 'Options', with 'Options' being the active tab. At the top, there is a 'Name' label with a red asterisk and an empty text input field. Below the tabs, there is a 'Type' label and a dropdown menu currently showing 'Manual Acknowledgement, Accept'. At the bottom right, there are 'OK' and 'Cancel' buttons. The bottom of the window has a yellow status bar that reads 'Java Applet Window'.

- 4 Select **Type** from the drop-down list:
  - Normal; Default, no message response.
  - Manual Acknowledgement, accept if you want acknowledgement with only accept.
  - Manual Acknowledgement, accept/reject if you want acknowledgement with the possibility to accept and reject.
- 5 Click **OK**.

#### Options Tab – Interactive Message

Text	ID	Function Key ID
Accept	91	A
Busy	2	C
Assist	4	B
Call	5	B
Close	3	C
RN	6	A
CNA	7	B
Back	8	C
Close	9	A
Image	1	A
Live stream	10	

When sending an Interactive message and using options, Option ID and Option text must be filled in. The Function Key ID will only be used for certain handsets when adding option text for soft keys. By marking the checkbox you can enter an ID for the Function Key.

You can set a layer that the option belongs to and to add extra layers to be displayed. This is used to group the options in different layers for quicker and easier usability, for example you can have all main actions in one layer and all sub action data in another layer. You can change the priority and the time to live for sent messages.

- 6 Click the **Options** tab.
- 7 Click **Add**.

## General Options

## Description

Option ID	1-99, Cardiomax provides a default value.
Option text	Enter text for the option
Display layer	1-99, the layer that the option belongs to. <b>NOTE:</b> Not all handsets support the use of display layers and function key IDs in combination.
Ack type	The acknowledge type tells the device if the Acknowledge option is a positive one (Accept) or a negative (Reject) one. The acknowledge type determines how the option should be visualized in the device.
New priority	The previous priority can be changed.

New TTL	The time to live can be changed.
Content type	<p>The Content Type tells how an IM option should be visualized in devices. If another value than “None” is set, the IM option is visualized as an icon.</p> <p>NOTE: Displaying of icons must be supported by the devices.</p>
Embed in option	If the option should be embedded in another option, enter the ID of the other option.
Use Function Key IDs	<p>When marked, enter Function Key ID. This is used when adding an option text for a soft key (only for some handsets)</p> <p>NOTE: Not all handsets support the use of Display Layers and Function Key IDs in combination.</p>

### Data Tab – Interactive Message

The screenshot shows a configuration window with four tabs: Data, Call, Properties, and Option Condition. The 'Data' tab is selected. Inside the Data tab, there are two input fields. The first is labeled 'Response Data' and contains the number '1'. The second is labeled 'User Response Prompt' and contains the text 'temp='.

Data options	Description
Response Data	Data entered here will be replied by the handset when the user selected that option. Enter a number or a short text.
User Response Prompt	Data entered here will be viewed in the display of the Handset. Enter a short text.

### Call Tab – Interactive Message

### Call Options

### Description

Administration Dial Digits

Enter telephone number, for example 123456.

Connect Call: A new call is connected to the number.

Call and Disconnect: A new call is connected to the number and then disconnected

DTMF during an ongoing call

DTMF during an ongoing call and then disconnected.

Response Data on Disconnect

Data entered here will be replied by the handset when the call is disconnected. Enter a number or a short text.

Disconnect Call

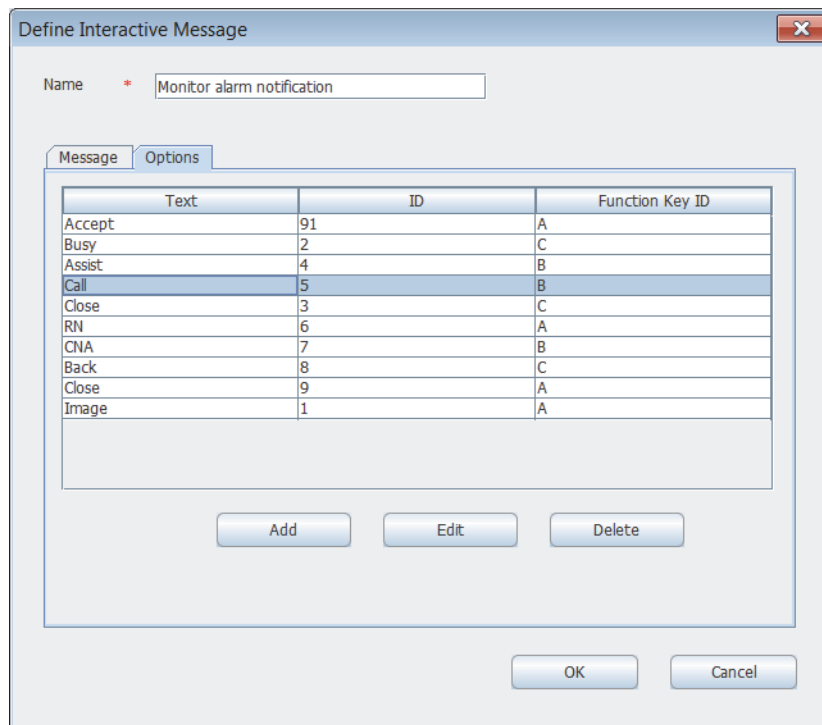
When marked, the ongoing call is disconnected. This option will not be used in combination with the Dial Digits.

### Properties Tab – Interactive Message

Property Options	Description
Close Message:	The message will be closed.
Erase Message:	The message will be erased.
Disable Option ID:	This Option ID will be disabled.
Erase Option ID:	Entered Option ID will be erased.
Enable Option ID:	Entered Option ID will be in use again.
Show Display Layer:	Entered layer will be displayed in the handset.
URI:	Link to an external resource. This is used if an external resource should be launched when pressing the IM option. Data can also be sent along with the link to the resource by adding event elements to the link. The elements can be added by right-clicking in the field.
Sticky mode	<p>The message is locked in the display when set to On. It will remain locked until the Sticky mode is turned off or message is deleted.</p> <p>No Change: keeps the old settings.</p> <p>On: the display becomes locked.</p> <p>Off: the display becomes unlocked.</p>

### **Option Condition Tab – Interactive Message**

Options can be removed from an IM by matching a condition defined for that option. This is done by adding different conditions on the IM option, and if any of the defined conditions for that option match, the option is removed from the outgoing IM.



- 8 Mark the option to be edited.
- 9 Click **Edit**.
- 10 Click "Option Condition".
- 11 Click **Add**.
- 12 Define conditions for the option.

#### *Options*

##### *Event Element:*

#### *Description*

*The event element to compare the specified value with.*

##### *Comparison:*

*String Equals: The option is removed if the specified value matches the value in the event element.*

*String Not Equals: The option is removed if the specified value does not match the value in the event element*

*Is empty: The option is removed if the value in event element is empty.*





Output Options	Descriptions
<i>Name</i>	<i>Enter the name of the output activity.</i>
<i>Output &gt; Output name</i>	Select one of the outputs.
<i>Activation</i>	Select between, Activate/Deactivate
<i>Duration</i>	The time for how long the activation should stay active. 0 = unlimited.

## Addressing

This is where destination is set up for the actions. It can be addressed to a User, call ID and to a user via the Duty Assignment. Note that Users and call IDs are defined in the Unite Connectivity Manager.

13 Select a type from the drop-down list:

- Duty assignment sends to users via Duty Assignment.
- User sends to users.
- Call ID send to call IDs, typically a telephone number.
- Replier, only updates send updates for this event to the handset that most recently fulfilled a success condition.
- Replier send to the handset that most recently fulfilled a success condition.
- Reference, keep old send to all handsets that previously received a message with this reference.
- Reference, set new send to all handsets that previously received a message with this reference. This will also update the reference for the previous message.

Depending on which addressing type that is selected, the next box will change.

Address Types	Descriptions
---------------	--------------

<i>Duty Assignment</i>	<i>None or Level 1 to Level 5 – if defined in the event Configuration.</i>
<i>User</i>	<i>Defined users.</i>
<i>Call ID</i>	<i>Enter call ID – call IDs are defined in the Unite Connectivity Manager.</i>
<i>Replier, only updates</i>	<i>No selection available.</i>
<i>Replier</i>	<i>No selection available.</i>
<i>Reference, keep old</i>	<i>Existing references</i>
<i>Reference, set new</i>	<i>Existing references</i>

- 14 For Duty Assignment and User, select from the drop-down list. For call ID, enter the call ID. If the types Replier, updates only and Replier are selected, the next box disappears. These types have no selections, they are just added. For Reference, keep old and Reference, set new select from the drop-down list.
- 15 Click **Add** to add the addressing type.

The screenshot shows a software window titled "Addressing". At the top, there is a "Type" dropdown menu currently showing "User". To its right is a text input field containing "Doris D". Further right are two buttons: "Add" and "Delete". Below these elements is a table with two columns: "Type" and "Name". The table contains two rows of data: the first row has "Duty Assignment" in the "Type" column and "Level1" in the "Name" column; the second row has "User" in the "Type" column and "Doris D" in the "Name" column. Below the table is a large empty rectangular area. At the bottom right of the window are two buttons: "OK" and "Cancel".

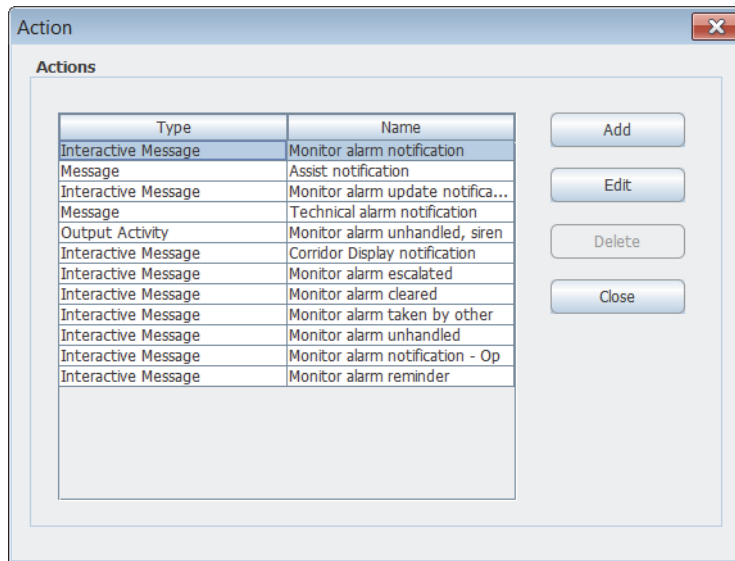
Type	Name
Duty Assignment	Level1
User	Doris D

### Deleting Destinations

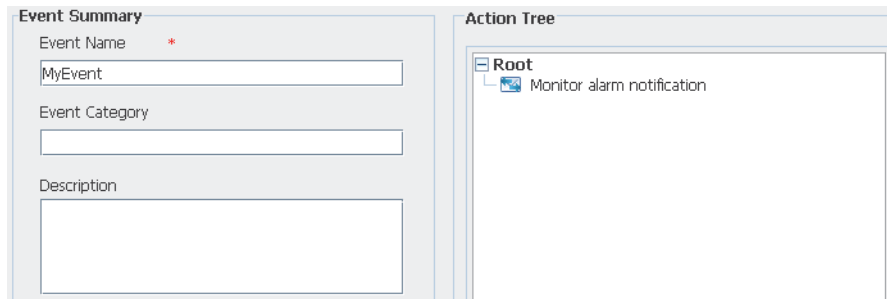
Destinations can be deleted if you mark the destination and then either click Delete button or right click on marked "type" and then click on the displayed Delete. In both cases you will be asked if you want to delete or not.

- 16 Click **OK** when finished.

If an action of each type has been added, the Action page may now look like this.



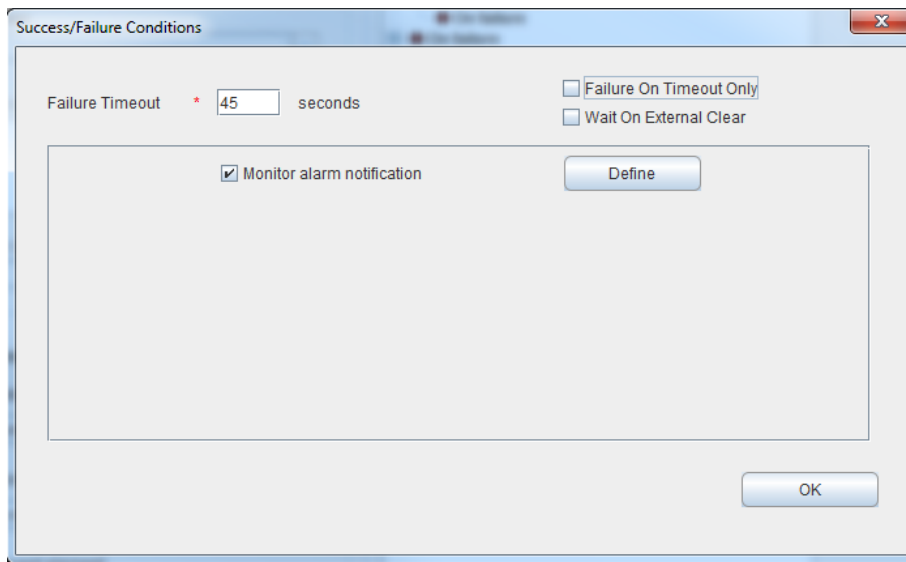
- 17 Click **Close**, to return to the event Configuration Actions page. Click **Close** to return to the event Configuration page.



### Adding Success/Failure Conditions

To get delivery and status response on a sent message, success and/or failure conditions are set up.

- 18 Mark the action under Root and click **Conditions** to add success/failure conditions.
- 19 Enter the time for the Failure Timeout. When this time expires, the action fails.



	<i>Description</i>
<i>Failure Timeout</i>	<i>Time out for the condition if no response is received.</i>
<i>Failure on Timeout Only</i>	<i>Indication that this event should only ever fail due the Failure Timeout timer. This options can be optionally configured to avoid a condition from failing due a delivery failure.</i>
<i>Wait On External Clear</i>	<i>Allow this condition to remain active until the Event is terminated by an external event (i.e. Clear).</i>

- 20 Select the check box for the action, in this example “Monitor Alarm Notification” and click **Define**.

In the Action tree, “On success” occurs as soon as one receiver of one action fulfils the specified success conditions. This means that “On failure” occurs when every action has failed for every address sent to or after the specified failure timeout.

Add delivery and status response for the success/failure conditions.

21 Select a requested status from the drop-down list:

Status	Description
<i>Don't Care</i>	
<i>In progress</i>	<i>Message valid</i>
<i>Sent</i>	<i>Message sent</i>
<i>Delivery Receipt</i>	<i>Reached final destination</i>
<i>Failure if</i>	<i>Redirected – when message diversion has occurred in the Unite Connectivity Manager and it is important for the message to reach a specific person.</i>
	<i>Not Available – absent</i>


22 Check one or both of the **Failure if** boxes, when **Redirected** or/and **Not Available** should be handled as a fault.

Adding a Response Condition for the Success/Failure Condition

This describes response conditions for an interactive message. For a message, it is done in a similar way, but the dialogues will look slightly differently.

23 Click **Add**.

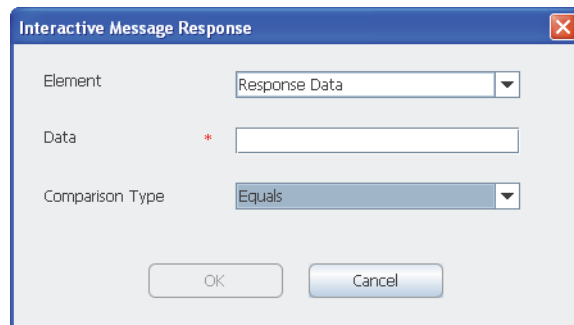
24 Select **On success** or **On failure** from the drop-down list.



The 'Add Response Conditions' dialog box has a title bar with a close button. It contains two fields: 'Type' with a text input showing 'Interactive Message Response', and 'Result' with a dropdown menu showing 'On success'. At the bottom are 'OK' and 'Cancel' buttons.

25 Click **OK**.

26 Select an element, enter data and select a comparison type.

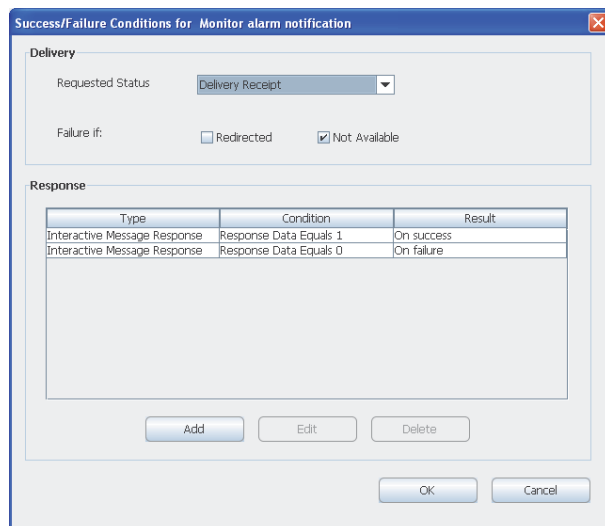


The 'Interactive Message Response' dialog box has a title bar with a close button. It contains three fields: 'Element' with a dropdown menu showing 'Response Data', 'Data' with a text input field preceded by a red asterisk, and 'Comparison Type' with a dropdown menu showing 'Equals'. At the bottom are 'OK' and 'Cancel' buttons.

Possible alternatives for elements include:

- Response Data, if the response data that has been set for the selected option.
- User Response, according to the response that the user has entered in the handset.

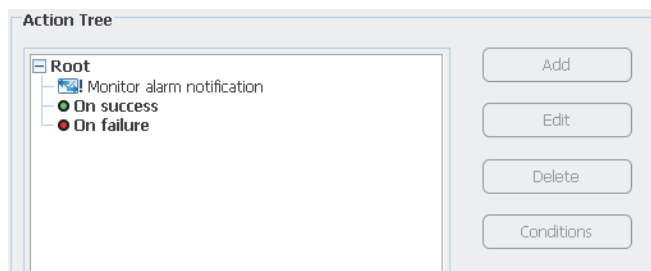
27 Click **OK**.



The 'Success/Failure Conditions for Monitor alarm notification' dialog box has a title bar with a close button. It is divided into two sections: 'Delivery' and 'Response'. The 'Delivery' section has a 'Requested Status' dropdown menu showing 'Delivery Receipt' and a 'Failure if:' section with two checkboxes: 'Redirected' (unchecked) and 'Not Available' (checked). The 'Response' section contains a table with three columns: 'Type', 'Condition', and 'Result'. Below the table are 'Add', 'Edit', and 'Delete' buttons. At the bottom of the dialog are 'OK' and 'Cancel' buttons.

Type	Condition	Result
Interactive Message Response	Response Data Equals 1	On success
Interactive Message Response	Response Data Equals 0	On failure

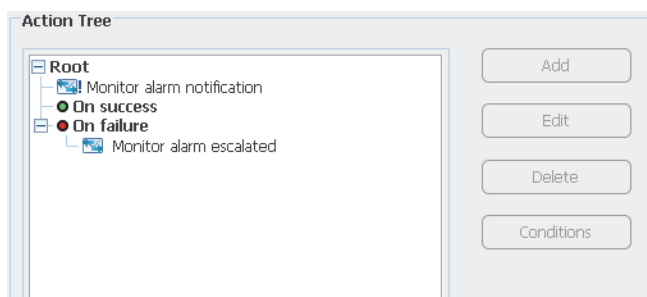
- 28 Click **Add** to add other conditions or click **OK** and **OK** again in the next window that opens, to return to the Action Configuration page.



Additional actions can be made by marking the Root in the action tree and click Add. An action can also be edited or deleted by clicking the action and click **Edit** or **Delete**. In the example above the action is monitor alarm notification.

Additional success and failure conditions can be made by marking one of the conditions in the action tree. You can delete conditions.

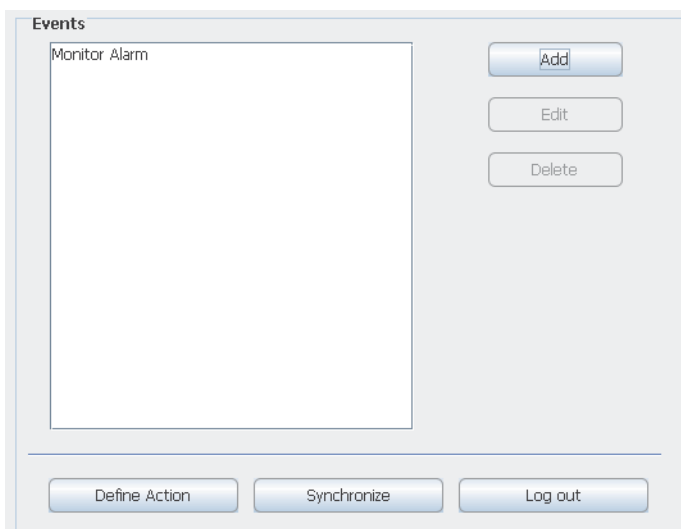
You can add an action on the success and/or failure conditions, for example start a siren on failure. This is done by marking one of the conditions and then clicking Add. See D.3 Action Configuration on how to make the configuration.



All actions in the action tree that are on the same node will be sent at the same time.

- 29 Click **OK**, to return to the Action Configuration page for events.





### Synchronize

- 1 Click **Synchronize** to add all the Events that have been created and configured into to the event Assignment User interface. *A new event is added to the Action Configuration page.*
- 2 Click **Log out** and then **Cancel** to close the Action Configuration page.

### Editing an Event

- 1 To edit an event, click **Edit**.
- 2 The Event Configuration page opens where the name of the event can be changed. You can also edit the action for the event from the same page.

### Delete an Event

- 1 To delete an event, click **Delete**.
- 2 A dialog window opens, click **Yes** to delete the event.

### Copy and Paste Event

You can create a new event based on another one.

- 1 Select the event for which action tree you want to copy from.
- 2 Click **Copy**.
- 3 Click **Paste**.

The event Configuration dialog window opens.

- 3 Make the appropriate changes to the cloned Event.
- 4 Click **OK** to save the settings.

### Copying an Event and Pasting it into Another Event

You can copy an event and paste it into another Event. This can be used if you want to edit an existing event with an action tree from another Event.

---

**NOTE:** When pasting into another Event, the configuration for that event will be overwritten.

---

- 1 Select the event for which action tree you want to copy from.
- 2 Click **Copy**.
- 3 Select the event for which you want to copy the action tree to.
- 4 Click **Paste**. The event Configuration dialog window opens.
- 5 Make the appropriate changes to the event.
- 6 Click **OK** to save the settings.

### Action Termination/Updates

Action Termination is used to set conditions that can stop an ongoing event when a certain new event is activated.

Updates are used to set the conditions that can update an ongoing event. Termination:

The screenshot shows the 'Event Configuration' dialog window. It is divided into two main panels. The left panel, titled 'Event Summary', contains fields for 'Event Name' (with a red asterisk indicating it is required), 'Event Category', 'Description', and 'Duty Assignment Addressing Levels' (a dropdown menu set to '1'). Below these is a section titled 'Action Termination / Updates' which includes three dropdown menus: 'Terminate Event By', 'Event Element Equality', and 'Update event element'. The right panel, titled 'Action Tree', shows a tree structure with a 'Root' node and two child nodes: 'Monitor alarm notification' (with a blue icon) and 'On success' (with a green circle icon). Below the tree are buttons for 'Add', 'Edit', 'Delete', and 'Conditions'. At the bottom of the dialog are 'OK' and 'Cancel' buttons.

To terminate a current event, select one from the **Terminate Event By** dropdown. Any event that is already defined can be used in this field. When the selected event is activated, all ongoing instances of the current event will be terminated. If no terminating event is wanted, the field should be left empty.

You can set an extra restriction on which event instances that will be terminated, based on the content of an event element. This is done by selecting an event element in the Event Element Equality field.

When setting this parameter, only instances where the chosen event element's value is equal to the value of the same event element in the "Terminate Event" instance will be terminated. If the box is left blank, all ongoing events of the selected type will be considered to match.

### Updates

When a new event arrives, a search is done to check whether a new instance of the event will be created or if it will be considered to be an update to an ongoing event instance. The Update event element field specifies (based on the content of an event Element) if an update to a currently active instance of this event will be done instead of creating a new instance. To decide if this is an update or not, select event element to compare in the Update event element drop-down list. If the box is left blank, no updates will be made and a new event instance is always created.

### Termination example scenario:

Configuration: For the created event Monitor Alarm, the Terminate Event By field is set to the already configured Event, Terminate Monitor Alarm. In the field event element Equality, Location is selected.

- 1 The event "Monitor Alarm" is activated and the event includes the event element "Location" with value "ICUIBED1".
- 2 The event "Monitor Alarm" is activated again and the event element Location equals "ICUIBED2". Now two instances of "Monitor Alarm" are running.
- 3 The event "Terminate Event" is activated, with the Location "ICUIBED1". This will terminate the first instance since the values of the event Elements match, but it will leave the second instance running.

---

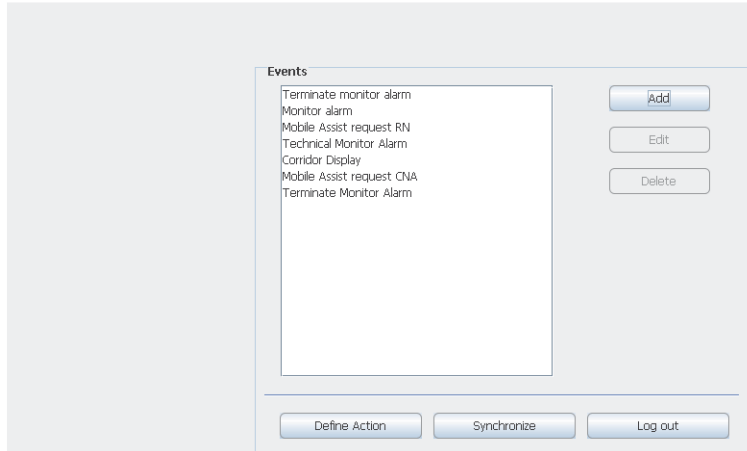
NOTE: If nothing is selected in the **Event Element Equality** field, both instances would have been terminated.

---

### Adding Termination Event Names

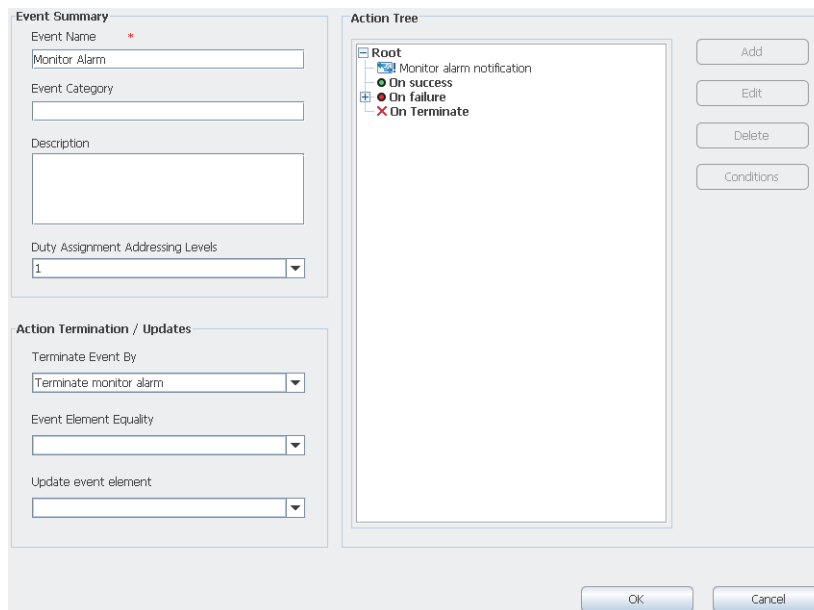
- 1 From the Action Configuration start page, click **Add**.
- 2 Enter the new termination event name in the **Event Name** field.
- 3 Click **OK**.

### Action Configuration



### Setting Termination Actions

- 1 Mark the event that will be terminated and click **Edit**.
- 2 Select which event that terminates the current event in the **Terminate Event By** drop-down list.



- 3 Select an event element to be an extra condition for an event element from the event element Equality drop-down list.
- 4 Click **OK**.

You can add an action to the termination by marking On Terminate in the action tree and then click **Add**. It could for example be that you want to erase the message or have a notification sent when a termination of an event has started. It is not possible to define success/failure conditions

on “On Terminate” actions. When “Monitor Alarm” is terminated the terminate action “Monitor alarm cleared” is executed.

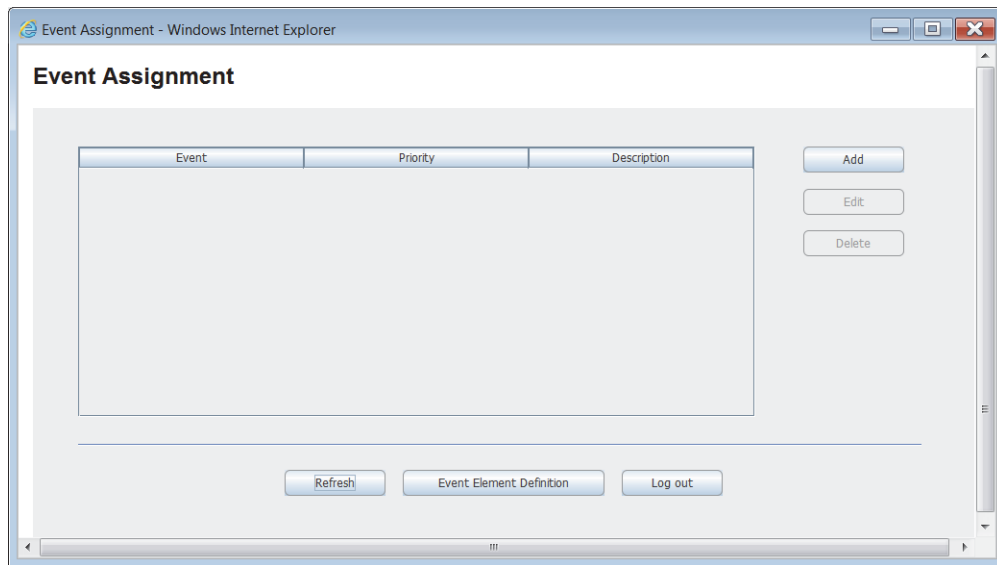
### Delete an Action Termination

This is done by opening the drop-down list under Terminate event By and select the empty row first in the list. You will then be asked if you want to lose the termination node or not. Click **Yes**.

### Adding Event Assignments

It is now time to make the connection between the event Elements and the Events that have been defined in the Action Handler. This is done by adding different conditions on the event Elements. For example, if the event element “\_Type” is defined, you can add a condition so that if for example the event element \_Type has the value “4” a specific action will start.

- 4 Click “Event Assignment” and log in with user ID and Password.



- 5 Click **Add** to create a connection between the event Elements and the Events.

Event	<input type="text" value="Terminate monitor alarm"/>	Description	<input type="text"/>
Priority	<input type="text" value="Not set"/>		

- 6 Select event from the drop-down list.

---

**NOTE:** If the event that you are looking for is not in the list, go back to the event Assignment page and click “Refresh”. If it is still not there, log in to Action Configuration and click

---

---

“synchronize”. Return to the event Assignment page, click “Refresh” and then click **Add**. The event should now be found in the list.

---

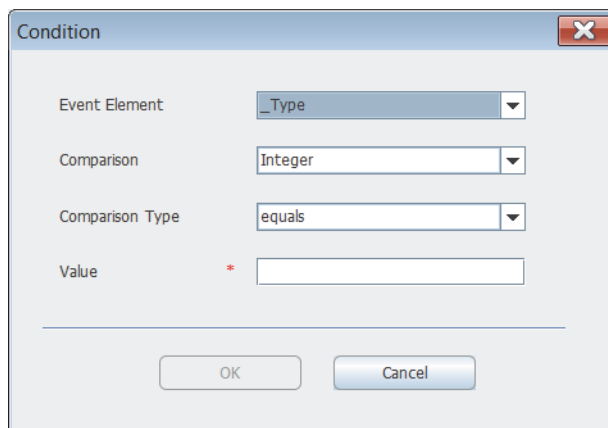
- 7 Enter a description of the event if needed.
- 8 Select which priority the event will have. This setting is used to indicate the severity of the event when sending an alarm message to the receiving display devices and applications (e.g. Unite View).

---

**NOTE:** How the severity is to be indicated in the receiving device is pre-configured in the Action Handler, but can be adapted if needed. If so, see Action Handler Parameter.

---

- 9 Click **Add**, to add conditions.



- 10 Select **Event element** from the drop-down list.
- 11 Select Comparison from the drop-down list. These are expression types:

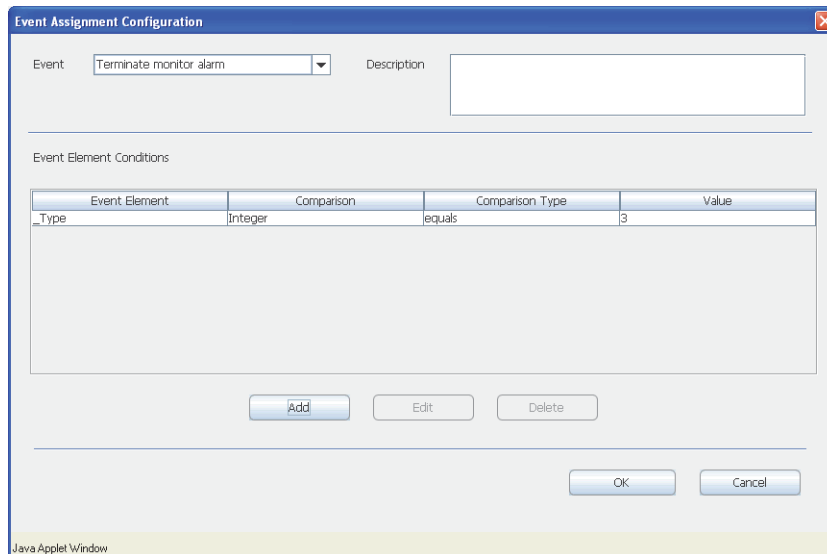
Expression types	Description
Integer:	Numerical comparison.
String:	Alphanumerical comparison.
Regular Expression:	Special syntax for advanced comparisons
Select Comparison Type from the drop-down list.	

Comparison Types	Description
equals:	The event element will be equal the set value
not equals:	The event element will not be equal the set value.

greater than: The event element will be greater than the set value for integer

less than: The event element will be less than the set value for integer.

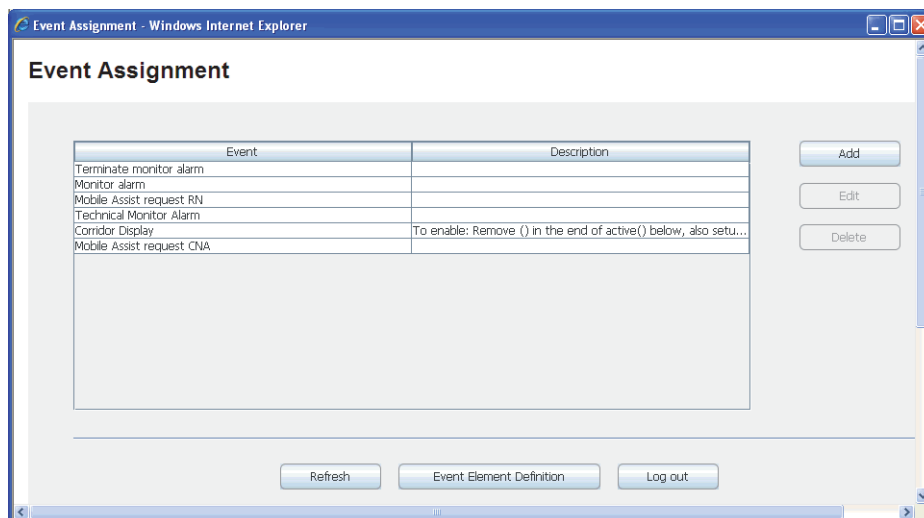
12 Click **OK**.



The 'Event Assignment Configuration' dialog box is shown. It has a title bar with a close button. Inside, there's a section for 'Event' with a dropdown menu set to 'Terminate monitor alarm' and a 'Description' text box. Below this is the 'Event Element Conditions' section, which contains a table with columns: 'Event Element', 'Comparison', 'Comparison Type', and 'Value'. The table has one row with 'Type' under 'Event Element', 'Integer' under 'Comparison', 'equals' under 'Comparison Type', and '3' under 'Value'. Below the table are 'Add', 'Edit', and 'Delete' buttons. At the bottom right are 'OK' and 'Cancel' buttons. A 'Java Applet Window' label is at the bottom left.

Event Element	Comparison	Comparison Type	Value
Type	Integer	equals	3

13 Click **Add** to add more conditions or click **OK** to save the settings and return to the event Assignment page. When more than one condition is used, all of them must match. You can edit or delete the event element conditions by marking the event element and then clicking Edit or **Delete**.



The 'Event Assignment - Windows Internet Explorer' window is shown. It has a title bar with standard window controls. The main content area is titled 'Event Assignment' and contains a table with columns 'Event' and 'Description'. The table lists several events: 'Terminate monitor alarm', 'Monitor alarm', 'Mobile Assist request RN', 'Technical Monitor Alarm', 'Corridor Display', and 'Mobile Assist request CNA'. To the right of the table are 'Add', 'Edit', and 'Delete' buttons. At the bottom of the window are 'Refresh', 'Event Element Definition', and 'Log out' buttons.

Event	Description
Terminate monitor alarm	
Monitor alarm	
Mobile Assist request RN	
Technical Monitor Alarm	
Corridor Display	To enable: Remove () in the end of active() below, also setu...
Mobile Assist request CNA	

## Appendix E Basic Module Troubleshooting

### E.1 Log Files

When troubleshooting, you should examine the log files, since they provide additional useful information. The first log you should examine is the status log, found under Status on the Configuration page, but when reporting an error to your supplier more advanced logs might be needed. Always include the appropriate log file.

To find the Info log and Error log:

- 1 From the start page, click **Configuration**.
- 2 From the Configuration page, select **Other > Advanced Configuration**.
- 3 From the Advanced Configuration page, click **Troubleshoot**.
- 4 Click **View Info Log** or **View Error Log**.

### E.2 Export Diagnostic Data

You can export diagnostic data to a file, that includes logs, configuration files etc. That file can be provided when requesting technical support from Ascom.

---

**NOTE:** The diagnostic data in the file is encrypted and can only be read by an Ascom technician.

---

- 1 From the Start page, click **CSIM**. The CSIM window appears.
- 2 Click **Troubleshoot**. The Cardiomax Advanced Configuration window appears.
- 3 Click **Troubleshoot**.
- 4 Click **System diagnostics**.
- 5 Under Export Diagnostic Data, click **Export**.
- 6 You are prompted to open or save the diag.bin file.



## Appendix F Acceptance Test

The acceptance test ensures that the functionality of the Ascom messaging system installed, complies with the expectations of the customer.

The approval sheets, found on the following pages in this appendix, should be completed to record that the system configuration conforms to established installation standards.

When the test is completed and verified according to customer requirements, the approval sheets are to be signed by both parties, i.e. the installer from Ascom and the customer.

By signing the approval sheets, the parties agree that the equipment meets the requirements after installation and configuration. The intended functionality should be operational to a degree only limited by needs associated with adjunct or supporting peripherals that Ascom has no control over. Operational deficiencies should be noted, and appropriate actions specified, in the approval sheets.

Acceptance testing must be performed for each location. Failure to complete acceptance testing may result in failed or delayed notification, resulting in potential patient harm. The following needs to be tested and verified:

Locations <sup>1</sup>	Perform a function check for each location
Alarm types:	All alarm types, possible to send from a location, need to be tested.
Alarm priorities:	Make sure the alarm priorities are in accordance with the customer requirements.  The alarm priority from patient monitoring systems are not automatically forwarded to the handsets, but, to provide a priority indication to the user, priority symbols can be added to the alarm message.
Escalation chains:	Verify that the escalation chains work.
Default destination:	Verify that a default destination has been configured in the escalation chains.
Filter settings:	Verify that filtering settings works as intended.  Filters are used for reducing the number of non-relevant alarms, and thereby minimizing the number of messages sent to clinicians.

<sup>1</sup> A location is a place from where an alarm can be sent.

## F.1 Alarm Specifications

Assigned priority of alarm in primary system	Delay (in secs) to level 1 end device	Accept & Busy buttons on handset	Repeat escalation across all levels if unacknowledged x 1	Escalation time from level 2 to level 3	Escalation time from level 1 to level 2	Recipient Level 3	Recipient Level 2	Recipient Level 1	Escalation Levels	Alarm Choice	Unit	Location	Filter	Filter setting	Tested	Comments
e.g. Per monitoring company	e.g. no	e.g. Yes/No/Other	e.g. Yes/No	e.g. 60 seconds	e.g. 60 seconds	e.g. Charge RN	e.g. Backup co-worker	e.g. Primary CG		e.g. Tachy	e.g. ECU	e.g. BED 1	e.g. STOP	e.g. *PVC	e.g. OK, Nok	

### Group Filter Identification

Identify the filters by way of the syntax used to define the filters in the following table.

Group Filter 1	Group Filter 2	Group Filter 3	Group Filter 4	Group Filter 5	Group Filter 6	Group Filter 7	Group Filter 8	Group Filter 9	Group Filter 10
(e.g. HR *)									

### Group Filter Verification

Verify the operation of each of the defined filters above to assure that they operate as intended and do not interfere with the effectiveness of the product to distribute other alerts.

Step	Description	Expected Result	Actual Result	Pass/Fail
1	Trigger alert corresponding to one of the defined group filter syntax defined above.	Alert received by the display device. Not suppressed by the established Group Filter.		
2	Trigger another alert that matches the configured group filter.	Alert NOT received by the display device. Alert suppressed by the established Group Filter.		
3	Trigger a third alert that does not match the group filter	The new Alert is received by the display device. Not suppressed by the established Group Filter.		
4	Trigger the original alert defined in the first test case.	Alert is once again received by the display device.		

### Delay Filter Identification

Identify the filters by way of the syntax used to define the filters in the following table.

Global or Unit Description	Delay Filter 1	Delay Filter 2	Delay Filter 3	Delay Filter 4	Delay Filter 5	Delay Filter 6	Delay Filter 7	Delay Filter 8	Delay Filter 9
e.g. Global	e.g. Leads*								

### Delay Filter Verification

Verify the operation of each of the defined filters above to assure that they operate as intended and do not interfere with the effectiveness of the product to distribute other alerts.

Step	Description	Expected Result	Actual Result	Pass/Fail
1	Trigger alert that does not match any configured delay filter	Alert received by correct display device without delay		
2	Trigger another alert that match a configured delay filter, which remains active longer than define delay time.	Alert received by display device after configured delay		
3	Repeat step 2 for every configured delay filter	All delay filters are working as expected		
4	If units are configured, verify that unit filter settings always override common (global) settings	Unit filter settings always override common settings		

## F.2 Acknowledgment

*Alarm specifications are used for configuration programming and post-installation testing. This alarm configuration is active in the production system unless otherwise noted in superseding documentation such as the post installation checklist.*

<i>Date</i>	
<i>Facility name:</i>	<i>Unit(s)</i>
<i>Site representative</i>	
<i>Name:</i>	
<i>Signature:</i>	<i>Date:</i>
<i>Title:</i>	<i>Phone/e-mail:</i>
<i>Ascom project manager</i>	
<i>Name:</i>	
<i>Signature:</i>	<i>Date:</i>
<i>Title:</i>	<i>Phone/e-mail:</i>
<i>Ascom Clinical Application Specialist</i>	
<i>Name</i>	
<i>Signature:</i>	<i>Date:</i>



**Ascom (Sweden) AB**

Grimbodalen 2  
SE-417 49 Göteborg  
Sweden  
Phone +46 31 55 93 00  
[www.ascom.com](http://www.ascom.com)

**ascom**