Installation and Operation Manual

Ascom Unite Connect for Clinical Systems, Cardiomax

28 April 2017/ Ver. F

About this document

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 *User Manual, Duty Assignment TD 92904EN*.

How to use this document

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

Reading instructions:

- Ascom installation personnel
  For installation and configuration, see 2. Installation on page 69 and, 3. Configuration on page 71
- Local administrator
  For administration see 6. Advanced Administration on page 89.
- For the daily operation refer to *User Manual, Duty Assignment TD 92904EN*.

CE

Address

Ascom Wireless Solutions
Ascom (Sweden) AB
Grimbodalen 2
SE-417 49 Göteborg
Sweden

www.ascom.com/ws

1. Introduction

This manual intends to provide information required to operate Cardiomax.
For additional information and technical assistance, please contact your Ascom service representative.

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.

NOTE: 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 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.

WARNING: Shall not be relied upon for receipt of ALARM SIGNALS.
The system does not substitute for the primary monitoring system and must only be used as a redundant, parallel notification mechanism to provide remote secondary alerting of alarms.

WARNING: 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.

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.

CAUTION: Operators should check that the current notification events and assignments are appropriate prior to use.

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.

1.2 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 behaviour 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.

1.3 Symbols and Descriptions

In the SW "About" File	Description
	Indicates the manufacturer's name and address
	Attention, consult accompanying documents
Module	The module key number of the device[1] key
	The ''About'' section shows the software version, year of manufacture and the CE mar.
On Hardware	**Description**
S/N	The serial number of the device
Model	The hardware model

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

1.4 Requirements

1.4.1 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.

1.5 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

1.6 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:

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

For additional details on specific system compatibility and functionality, refer to the Data Sheet, Cardiomax TD 92905EN and Appendix A. Clinical System Protocols on page 108.

1.7 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 page
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 92679GB.

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 restarted to update the IP address. Otherwise there is a risk for IP address collision.

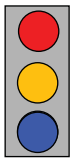
2.3 Getting Started

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

2.4 Description of LED indicators

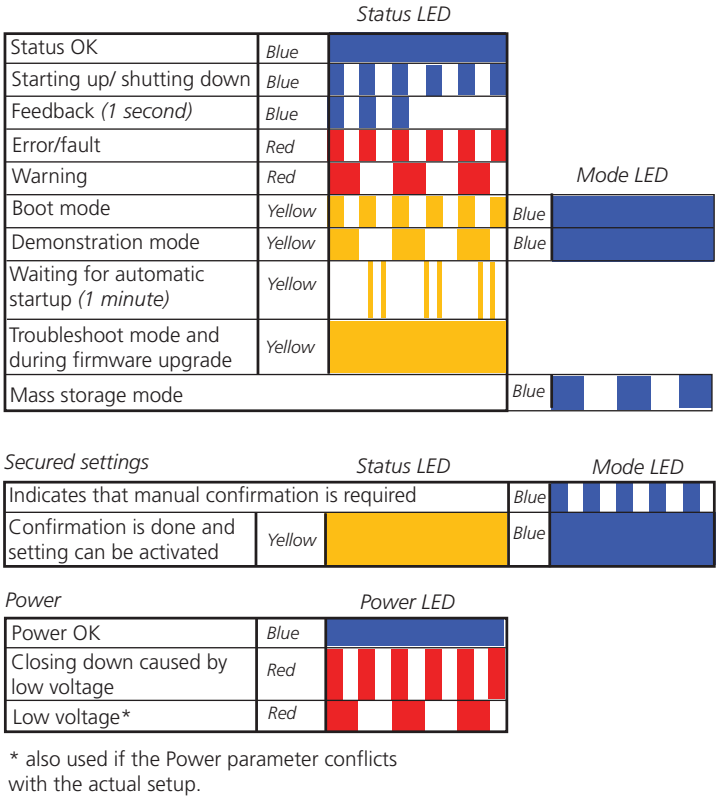
The Elise3 hardware has LEDs that indicates the status of Cardiomax software as shown in figure 1.

Figure 1. Elise3 module



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

Figure 2. Flashing patterns



* 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.

For connections of the error relay and error relay output configuration, see the *Installation Guide, Elise3 TD 92679GB*.

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

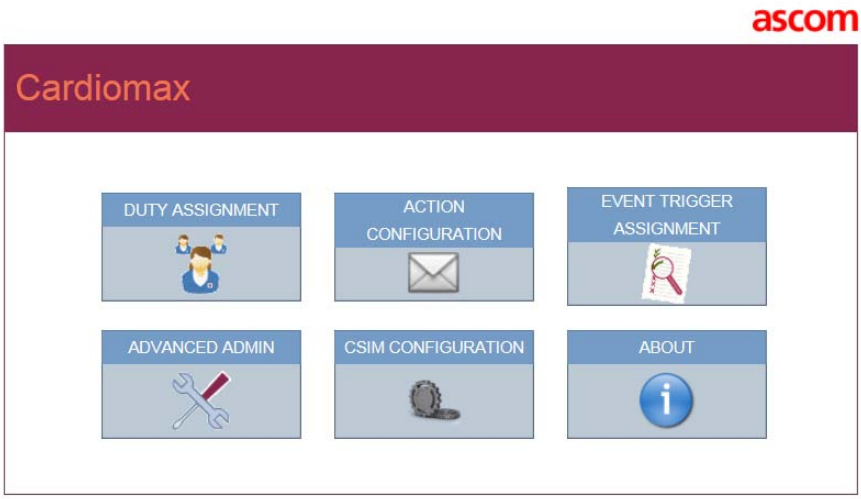
For available licenses, see the *Unite License Configuration Guide, TD 93113EN*.

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. Setting up Access Rights on page 117.
- 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 done.

3.7 Selecting a Template for Action Configuration

To facilitate the configuration of events for monitoring systems, a 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. Action Tree Templates on page 119 for an explanation of the Action Tree in Event Configuration, for different monitoring systems.

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 settings, 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**[1]
  - 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**[1]
  - *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.
  - Connection Timeout
    Defines the number of seconds that a socket will wait for PDI data before

1. US only

determining a connection. Changes to this value are effective only for new connections.

- Displays the IP address of the remote system on loss of connectivity. 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.
- For parameters concerning Units /Filters, see 4.2 Units and Filters on page 77.

- **Spacelabs CEI & ENI**

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

  - *Server IP*
    Set the Server IP field to the IP Address of the Clinical Event Interface Server.
  - *Server Port Number*
    Set the Server Port field to the Listening Port of the Clinical Event Interface Server.
  - *Event Data Start Field / Event Data 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 CEI_AlarmData_Parsed Event Element.
    Set Event Data Start Field to the desired start character count. Set Event Data Stop Field to the desired end character count.
    For example, if the Event Alarm Message Data element value is ''this is a test'' and the Event Data Start Field value is 9 and Event Data End Field is 14, then the CEI_AlarmData_Parsed event element value is ''a test''.
  - *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**
  - Patient Monitoring System
    Allows for the selection and identifies the currently enabled Patient Monitoring System Interface.
  - DigiStat Connect Configuration Settings
  - 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).

- **XprezzNet**
  - All XprezzNet configuration utilizes the installer in the Unite AM configuration section.

  The use of test alarm functionality does not replace the end-to-end acceptance procedure described in Alarm Specifications on page 63.

  Send test alarms which contain event element data to a handset from Cardiomax.

Event Type: Content should represent the Alert Type (Clinical or Technical).

Alert Text: Content should reflect the description of the alert, this element typically serves as the triggering event element.

Unit Name: Content should reflect an optional Unit name where the event is triggered.

Priority: Content should represent an optional priority assigned to a given alert.

Bed Label: Content should represent the Bed Label assigned to a location, this location is considered the unique identifier (NK, MR, SL).

Alert Type: Content should represent the Alert Type (Clinical or Technical).

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, Spacelabs XprezzNet & 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.

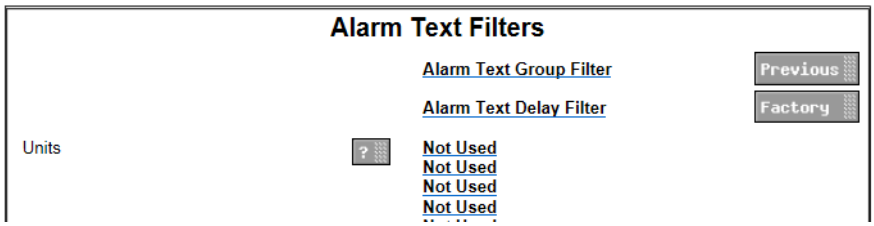
2 Stop filter: All alarms with alarm text matching any of the stop filters are discarded and no alerts are sent out.

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.

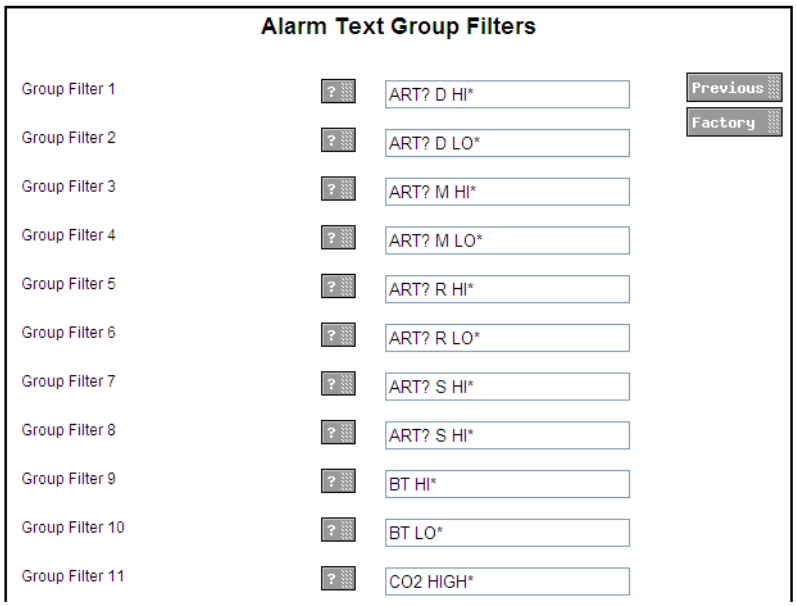
1 From the CSIM page, click **Units/Filters**. The alarm text Filters window opens.



NOTE: The filtering feature is case sensitive.

Alarm Text Group Filters

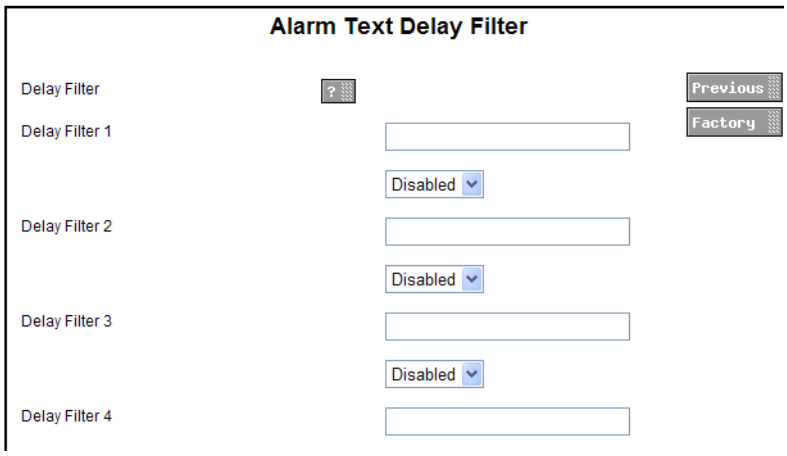
For alarm text group filters, all alarm texts that match the same group filter are considered to be the same alarm. This type of filtering is available only for Philips, XprezzNet and DigiStat.



- *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, XprezzNet and DigiStat.



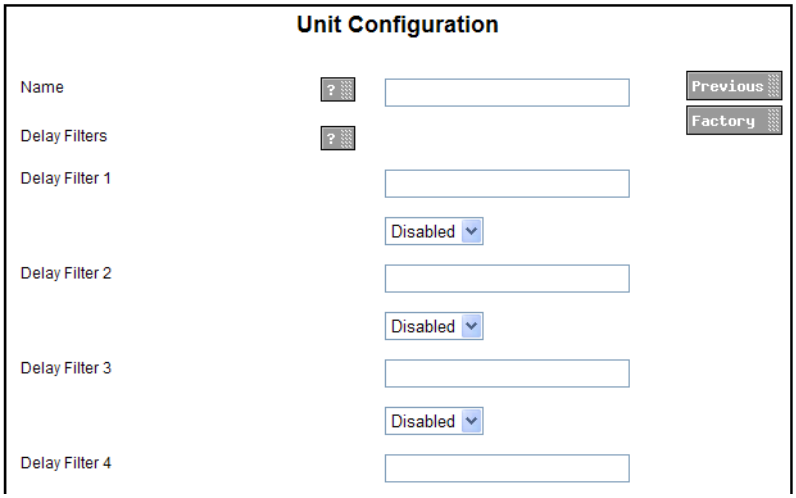
- *Delay filter 1– 10:*
  Set filter value.
  Select delay time or Disabled.

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, XprezzNet and DigiStat.

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



- **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.

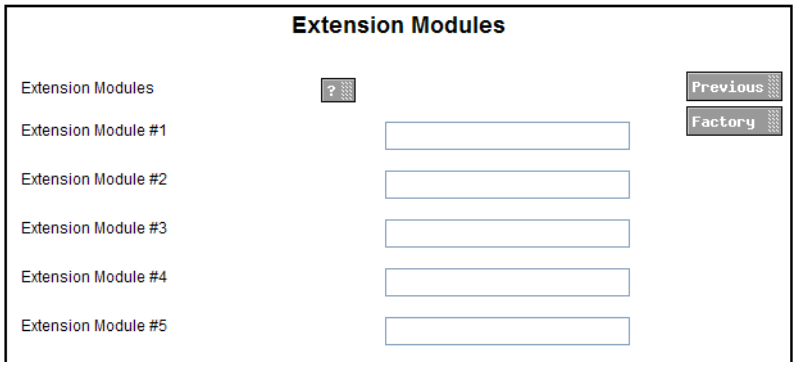
4.2.1 Extension Modules

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**.

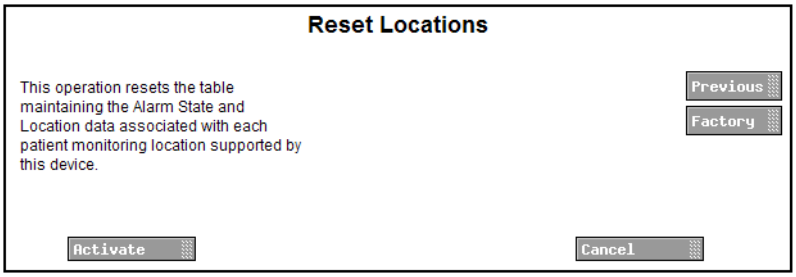
4.2.2 Reset Location Table for Philips Monitoring Systems

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.

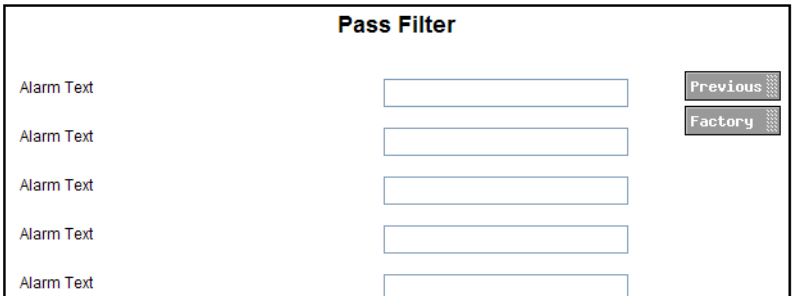
The pass filter represents an integral function of an optimized Cardiomax system. Pass Filters reduce the number of alerts to alerts recommended and/or requested during clinical consulting.

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.



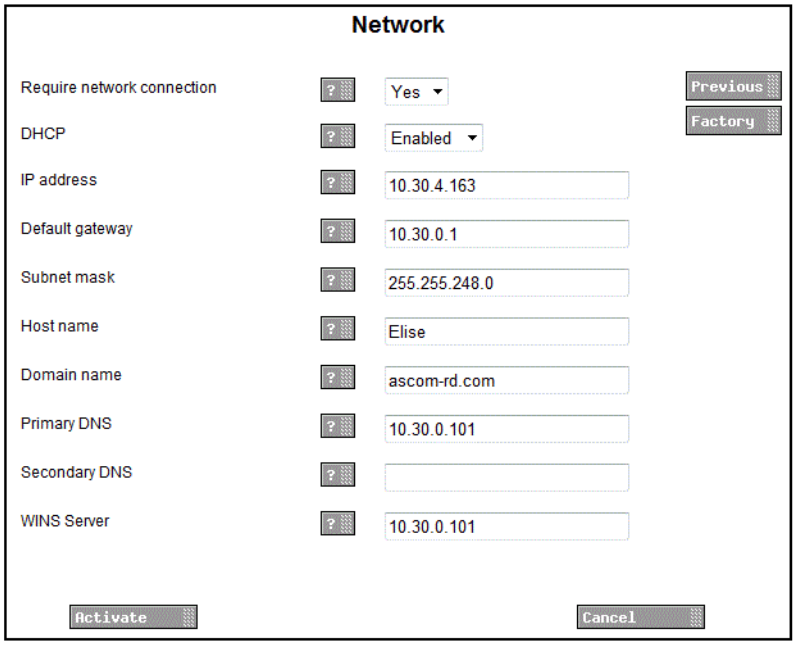
Up to 25 pass filters can be set.

4.3 Changing Common Settings

4.3.1 Network Settings

From the start page, click **CSIM CONFIGURATION**.

1 Click **Network**. The Network window appears.



2 Enter IP settings.

3 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.

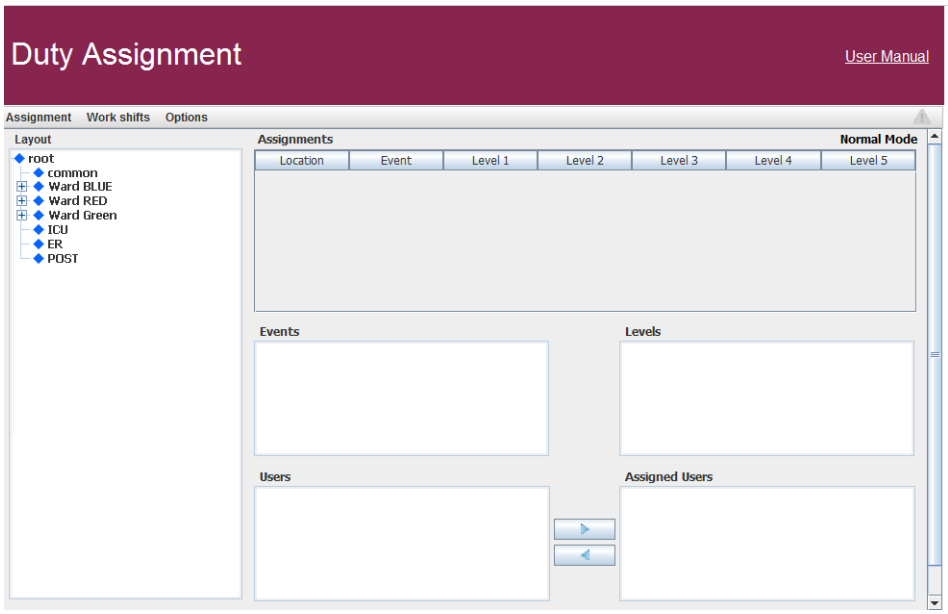
NOTE: If the Reboot window is reloaded, this triggers another reboot.

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 *User Manual, Duty Assignment TD 92904EN*. 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 whether or not you want to the Duty Assignment application. Click **Run**.

Figure 3. The Duty Assignment window indicating a layout example.



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, see *Configuration Manual, Unite Connectivity Manager TD 92735EN*.

Adding Locations

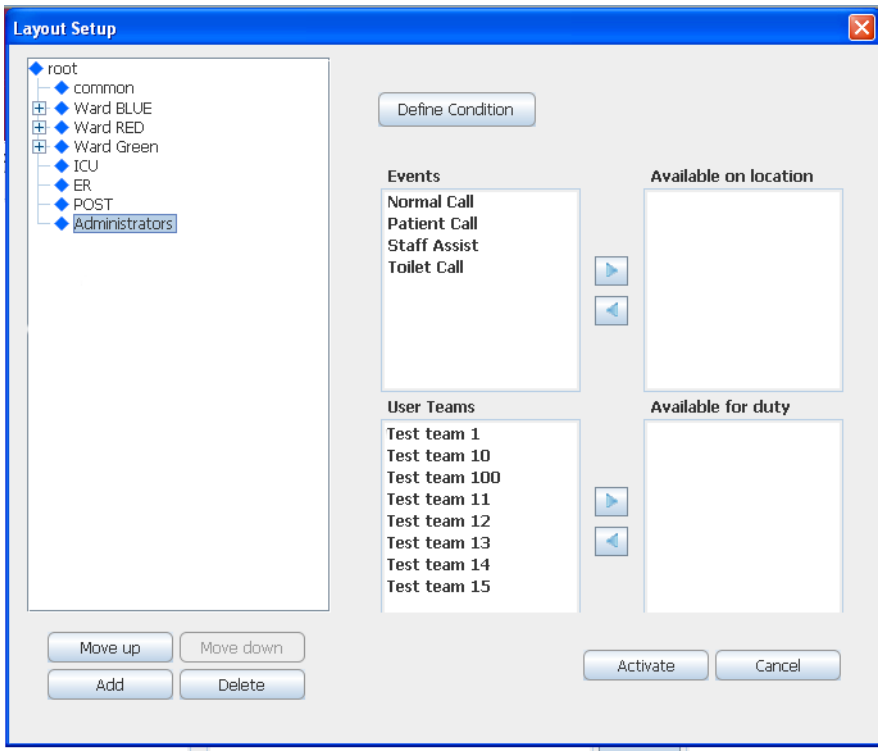
IMPORTANT: When a location is added and the condition for the location is defined, the value must correspond to the value set for that location in the clinical system. If not, the alarms are not distributed. See example below:

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.

2 Click **Option**, and select **Layout Setup**.

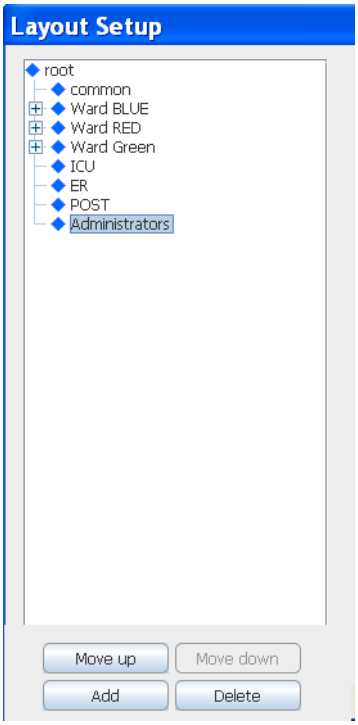
3 Select ''root'' and click **Add**.



4 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**.

5 To add levels below a location, select it and click **Add**.



6 Enter a name for the location.

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

Renaming Locations

1 Select the location you want to rename.

2 Enter a new name for the location.

Deleting Locations

1 Select the location you want to delete.

2 Click **Delete**.

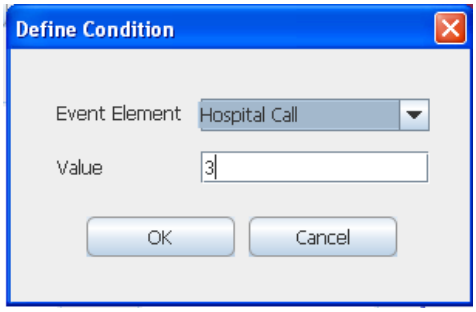
Defining Conditions

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:

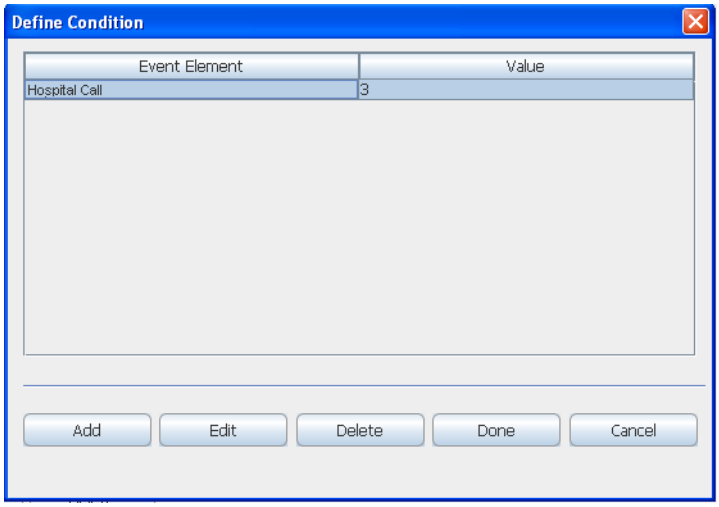
1 Click **Define Condition**.

2 Click **Add**.



3 Select **Event Element**.

4 Enter a value and click **OK**.



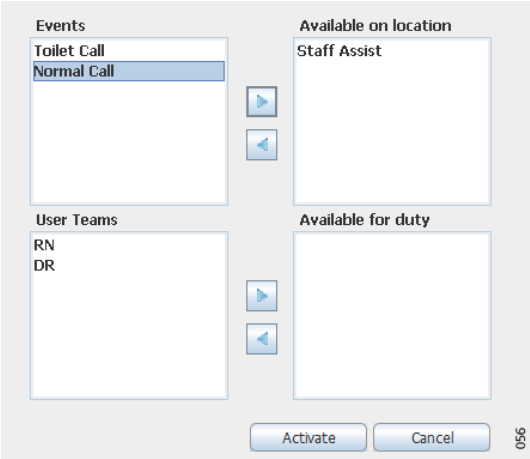
More conditions can be defined by clicking **Add**. At least one condition must be fulfilled.

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 have 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.

Available on Locations

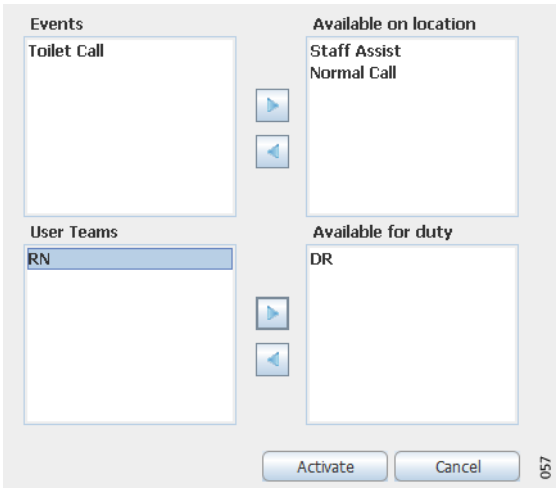
This is how you define events that should be available on a location.



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.

Available for Duty

Defines an available user team.

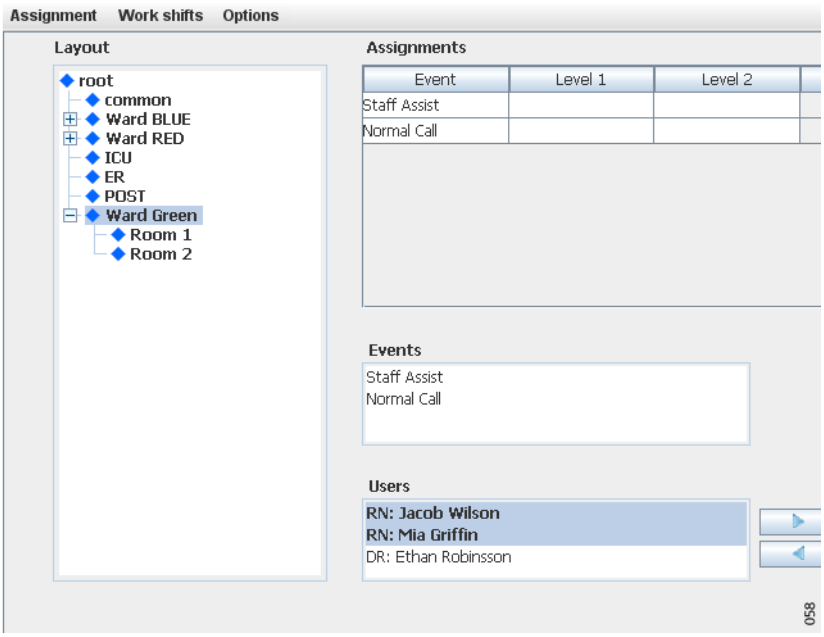


2 Double-click available user team.

3 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.

Figure 4. The layout configuration.



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.

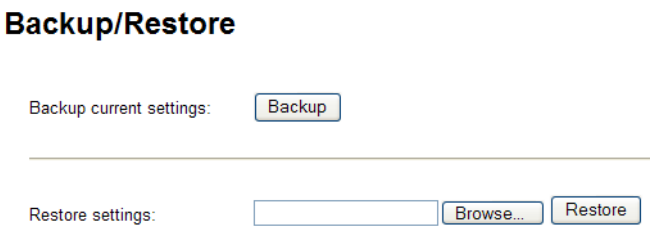
6.1 Backup and Restore

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

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 **View**
	• **DefaultDB:** 2 columns to search in - one Action list and one Info list • **Full:** 5 columns to search in - Text 1 - Text 5, user defined information • **Short:** 1 column to search in - Text 1, user defined information
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 configure 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
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

For details in the latest version, see change bars in the document.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. Refer to *Data Sheet, Elise3 TD 92678GB* for more information on which SD cards that currently are supported.
- 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.
  TIP: See also *Preparing IP Addresses in a Redundant System*.
- 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. See *Configuration Manual, Unite Connectivity Manager TD 92735EN*.

8.2 Preparing IP Addresses in a Redundant System

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''.

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 DCHP Server

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 correct IP address.

Network with DCHP 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 on.

2 Ask your network administrator to reserve a new static IP address to the origin Unite module that later on 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

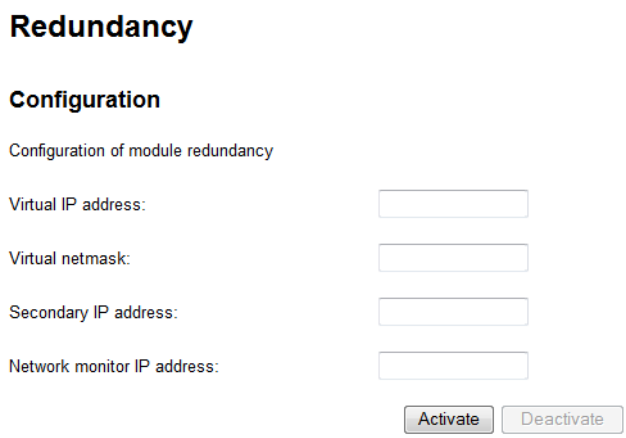
Do the following on the Unite module to be used as primary module:

1 Click **CSIM Configuration** from the start page.

2 Click **Network**.

3 Click the **Home** button.

4 Select Other > Redundancy on the Configuration page.



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, see appendix in the *Configuration Manual, Unite Connectivity Manager TD 92735EN*.

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**.

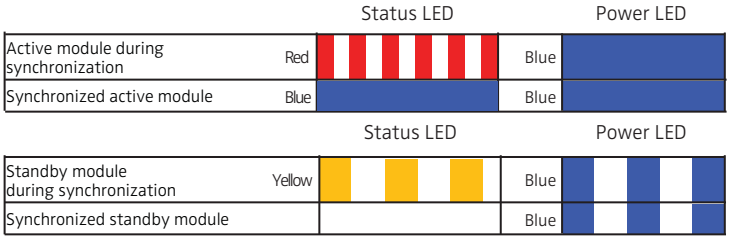
NOTE: Primary is stated in the GUI's upper-left corner when the module is up and running again.

IMPORTANT: 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.

Figure 5. The LEDs on each module indicate the status of the synchronization.

.



It is also possible to view the synchronization status via the GUI. See figure 6 and figure 7. Use the virtual IP address to access the active module and the static IP address to access the standby module.

Figure 6. 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

Figure 7. 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 indicating 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. See 8.3.3 Fallback to the Primary Module on page 104.

8.3.2 Restrictions on an Active Secondary Module

A secondary active module has redistricted 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: It is only possible to press the button if the data has been synchronized with the primary module.

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 DCHP 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.

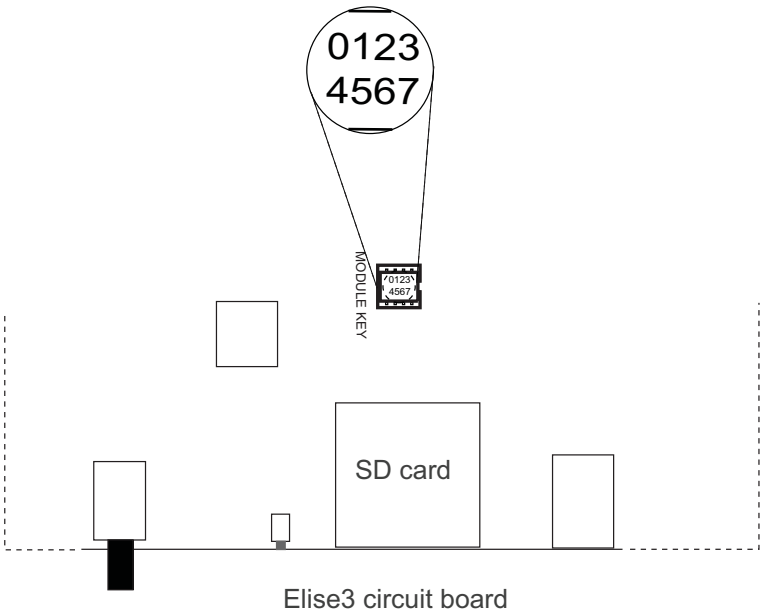
To replace a broken primary module:

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, see 4.3.1 Network Settings on page 81 and 4.3.2 License Numbers on page 82.

11 Configure the module redundancy, see 8.3 Configuring Redundancy on page 100.

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. For information about which SD memory cards that currently are supported, see *Data Sheet, Elise3 TD 92678GB*.

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.

Appendix A. Clinical System Protocols

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

A.1 Nihon Kohden PagerService 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 (BedLabel), 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

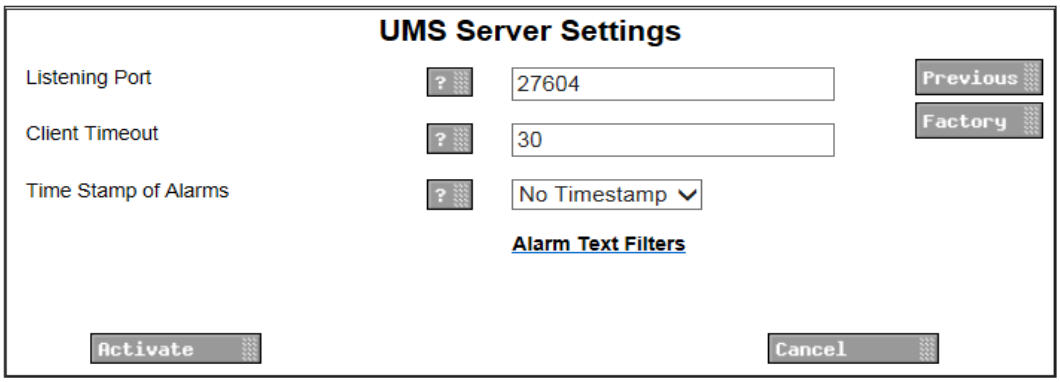
Cardiomax supports a clinical alarm based event interface from Digistat Connect, capable of acquiring alarms and accompanying vital sign data from clinical systems. The extensible interface monitors the active alarm status of those clinical system integrated with Digistat Connect; Data Acquisition Server (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 where by, 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.

Listening Port:	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.
Client Timeout:	Amount of elapsed time (in seconds) after which Cardiomax shall indicate a loss of connectivity if proper information is not exchanged over the interface. Caution: After Cardiomax has lost, and is unable to re-establish, connectivity with DigiStat Connect for a period of time not exceeding 60 seconds, all active alarms are terminated and notified as cleared.
Time Stamp of Alarms:	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 are indicated as a loss of connectivity and will reported by Cardiomax in the form of a distributed alert.

A.4.6 Presets

None

A.4.7 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).

NOTE: 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 it's 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 do 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:

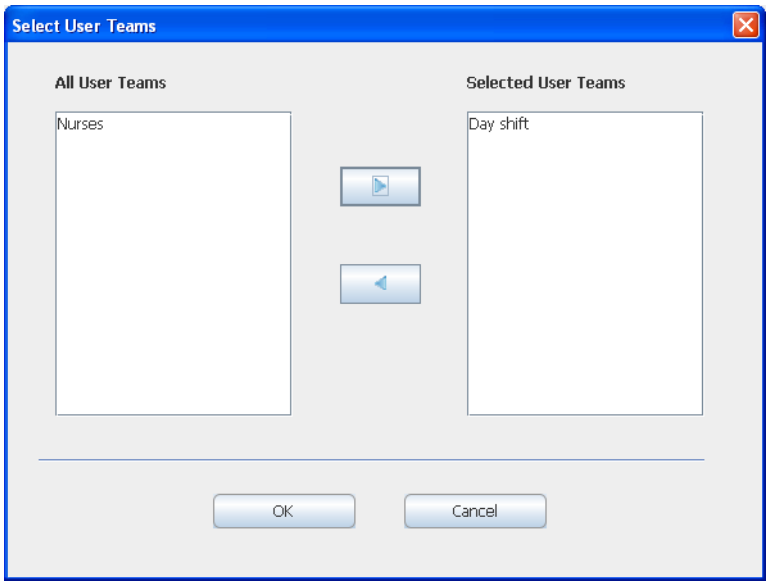
1 From the Start page, click **ADVANCED ADMIN**. The Backup/Restore window appears.

2 Click **ACCESS RIGHTS** and log in with your user name 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

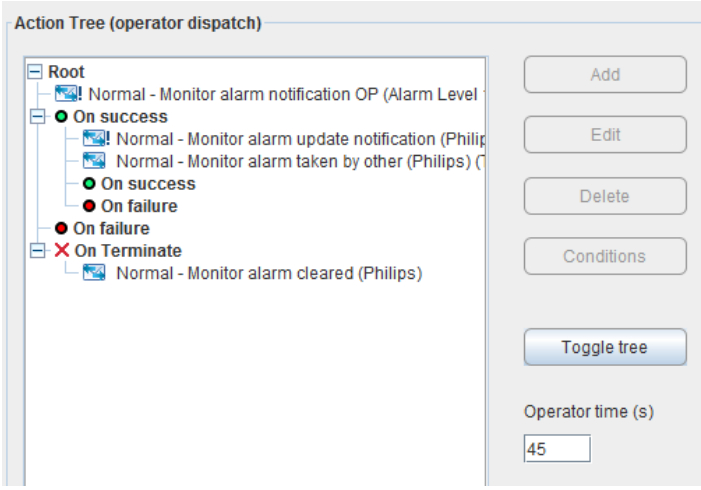
By clicking the delete invalid user teams, all user teams not available in the system are deleted.

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

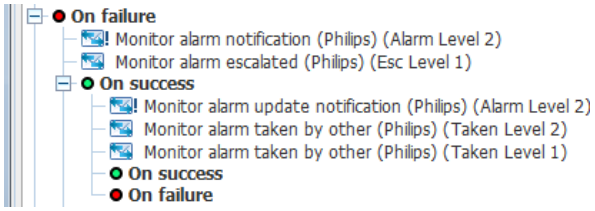
The Action Tree for Monitor Alarm in the Template for Philips IntelliVue



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 sends 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.

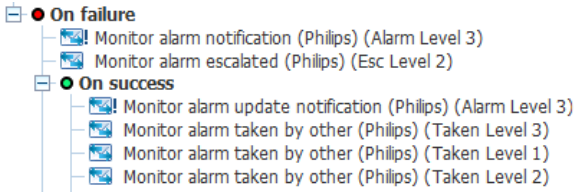
Figure 8. Actions under the first ''On failure'' level



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.

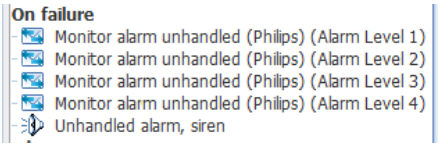
Under the second ''On failure'' level, actions for what is done if the second recipient did not accept the message are set up. In a similar way, a third recipient may accept or reject a message and so on.

Figure 9. Actions under the second ''On failure'' level

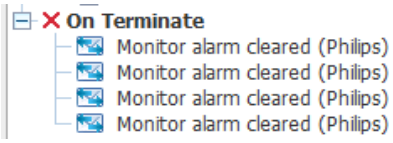


The template has four escalation levels. For the last ''On failure'' level, if no recipient has accepted, a high priority message is sent to all recipients that the alarm has not been handled and an output is activated. This output could, for example, be connected to a siren.

Figure 10. Actions under the last ''On failure'' level



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.

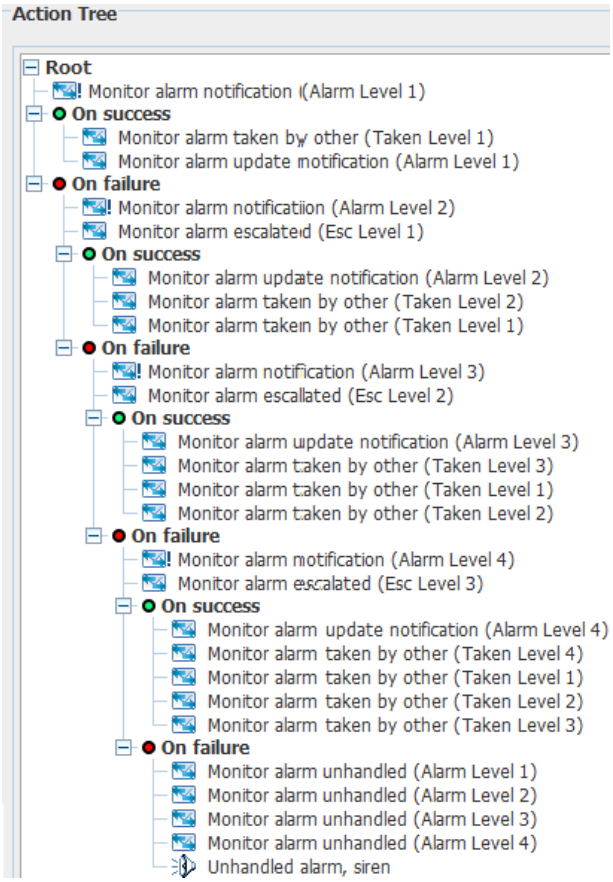


D.2 Action Tree for Nihon Kohden, Mindray Panorama, and Spacelabs Systems

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.

Figure 11. The Action Tree for Monitor Alarm in the Templates

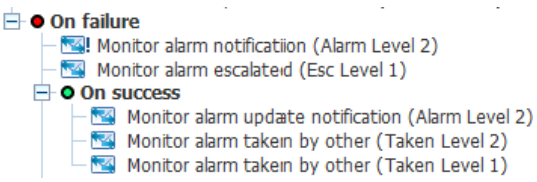


When a Monitor alarm is received, an interactive message is sent to a recipient. If the notification is accepted, the first level ''On success'' is followed. The other recipients in the hunting chain is notified that the alarm has been accepted by someone, and a confirmation message is sent back to the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

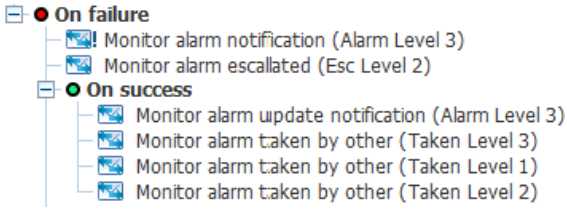
Figure 12. Actions under the first ''On failure'' level



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.

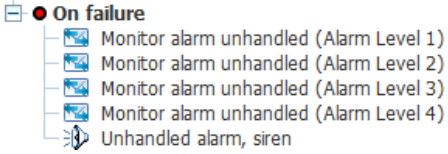
Under the second ''On failure'' level, there are actions for what is done if the second recipient did not accept the message. In a similar way, a third recipient may accept or reject a message and so on.

Figure 13. Actions under the second ''On failure'' level



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.

Figure 14. Actions under the last ''On failure'' level



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. he 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.

WARNING: 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 [1]	**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 works.
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.

Figure 15. Actions under the last ''On failure'' level.

[1] A location is a place from where an alarm can be sent.

Unit	Location	Filter	Filter Setting	Tested	Comments
e.g. CCU	e.g. BED 1	e.g. STOP	e.g. *PVC	e.g. Ok, NOk	

Alarm Specifications

Assigned	Delay (in secs)	Accept & Busy	Repeat	Escalation time	Escalation time	Recipient Level 3	Recipient Level 2	Recipient Level 1	Escalation Levels	Alarm Choice
e.g. Per	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-	e.g. Primary CG		e.g. Tachy

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.

Date		
Facility name:	Unit(s)	
Site Representative		
Name		
Signature	Date	
Title	Phone/email	
Ascom project manager		
Name		
Signature	Date	
Title	Phone/email	
Ascom Clinical Application Specialist		
Name		
Signature	Date	
Title	Phone/email	