CONFIGURATION MANUAL

Ascom Mobile Monitoring Gateway (MMG)

ascom

About this Document

This document is intended for anyone who needs to understand MMG. The document is mainly intended for the following target uehns; Ascom installation personnel and a local administrator for normal system maintenance. Reading instructions for these groups are:

- Ascom engineers:
  - For installation, see 4 Installation.
  - For configuration, see 5 Configuration.
- Local administrator:
  - For administration, see 8 Administration. For administration of Duty Assignments, see 8.4 Setting up Access Rights.
  - For troubleshooting, see Troubleshooting Guide, Alarm Management for GE Patient Monitoring, TD 92717GB.

Intended Use of the Product

The Ascom Mobile Monitoring Gateway (MMG) is intended to interface with the GE Healthcare patient monitoring network and the Ascom Messaging System. The MMG is used as a secondary means to automatically provide patient alarm information, to healthcare professionals, via display devices.

The MMG does not alter the behavior of the monitoring system. Neither is it intended to replace or alter the primary alarm function on the patient monitor. The MMG is not intended to be used for diagnostic purposes.

The MMG is intended for use by professional clinical personnel and relies on proper use and operation of both the communication infrastructure in place at the healthcare facility and the display devices used.

The MMG software is installed on specified hardware located in a computer hall or similar, where the MMG cannot come into physical contact with patients.

Contents

1 Introduction 1
1.1 Caution and Notes 1
2 Requirements 4
2.1 Computer Requirements 4
2.2 GE CARESCAPE MC Network Requirements 4
2.3 Requirements on Ascom Equipment 4
2.4 Abbreviations and Glossary 4
2.5 Symbols and Descriptions 5
3 MMG General 7
3.1 The MMG Start Page 7
3.2 Authentication Levels and Default Passwords 7
3.2.1 Log in to Configuration and Service Pages 8
4 Installation 9
4.1 Description of LED Indicators 9
4.2 Internal Outputs 10
4.3 Error Relay 10
4.4 Licenses 10
4.5 Demonstration Mode 10
5 Configuration 11
5.1 Basic Configuration 11
5.1.1 Basic Setup 12
5.1.2 Setting Language 12
5.1.3 Backing up or Restoring 13
5.1.4 Selecting a Template 14
5.2 Advanced Configuration 14
5.2.1 GUI Translation 15
5.2.2 Input and Output Setup 18
5.2.3 CARESCAPE Network Test Alarm 19
5.2.4 CARESCAPE Locations 19
5.2.5 Software Information 20
5.2.6 Software Installation/Upgrade 21
5.2.7 Software Upgrades in a Redundant System 22
5.2.8 Module Redundancy 22
5.2.9 Configuring Redundancy in MMG 23
5.2.10 Module Redundancy Test 26
5.2.11 Restrictions on an Active Secondary MMG 28
5.2.12 Fallback to the Primary MMG 28

5.2.13 Access Troubleshooting Pages 29
5.2.14 Deactivate module redundancy 29
5.2.15 Replacement of Broken Module in a Redundant System 30
5.2.16 Demonstration Mode 31
5.2.17 Basic Administration 31
5.2.18 Elise3 Setup 31
5.2.19 Action Handler Parameter Settings 32
5.2.20 Event Handler 34
5.2.21 GE CARESCAPE 34
5.2.22 Units and Filters 37
5.2.23 Security 52
5.2.24 License Activation 52
5.2.25 Rebooting MMG 53
5.2.26 Setting passwords 53
6 Integration with Alert Management 55
6.1 Integration Steps 55
6.2 Common Modifications 57
7 Operation 61
8 Administration 62
8.1 Action Configuration 62
8.1.1 The Action Tree 63
8.1.2 Event Configuration 63
8.1.3 Defining Actions 66
8.1.4 Synchronize 82
8.1.5 Editing an Event 82
8.1.6 Deleting an Event 82
8.1.7 Copying and Pasting an Event 82
8.1.8 Copying an Event and Pasting it into Another Event 83
8.1.9 Action Termination/Updates 83
8.1.10 Adding Termination Event Names 84
8.1.11 Setting Termination Actions 85
8.1.12 Deleting an Action Termination 85
8.2 Adding Event Assignments 86
8.3 Layout Setup 88
8.3.1 Locations 88
8.3.2 Defining Conditions 90
8.4 Setting up Access Rights 91
8.5 IM Including Airstrip 93

9 Troubleshooting 97
10 Related Documents 98
11 Document History 99
Appendix A Used IP Ports 100
Appendix B MMG Overview Picture 102
Appendix C MMG Filtering Description 103
Appendix D Ascom Unite Application Manager 106
Appendix E Network Monitoring in a Redundant System 107
Appendix F LDAP User Authentication 109
Appendix G Supervision of GE CARESCAPE Network and MMG 112
G.1.1 Logging 112
G.1.2 Fault Log settings 112
G.1.3 Configuring Fault Actions (Send E-mail) 114
G.2.1 Supervision 114
Appendix H Acceptance Test 116

1 Introduction

The Mobile Monitoring Gateway (MMG) is a Unite module that runs on Elise3 hardware. It receives alarms from the GE CARESCAPETM Network. It converts the CARESCAPE alarms to actions in the Unite system and also provide an assignment interface to offer the ability for users to dynamically assign recipients to alerts.

This document describes the installation and configuration of MMG. For the daily operation refer to MMG Duty Assignment User Manual TD 92691GB. Information about administration of the GUI and an overview picture of the MMG runtime are also found in this document.

Different system configurations can be made depending on capacity requirements. The following picture shows the basic configuration.

Figure 1. MMG connected to the CARESCAPE Network and the Unite Connectivity Manager.

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

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

NOTE: Figures in this manual are provided for reference purposes only. Screens will likely 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 supported by this product. Failure to complete acceptance testing may result in failed or delayed notification, resulting in potential patient harm. Functional verification of the products should occur before the product is used in a clinical environment with live patient. Additionally this testing should be repeated after any changes to the configuration or system upgrades.

WARNING:	This product provides methods to temporally suppress alerting and redirection for the duration of a silenced alarm and (optionally) for the duration of all active alarms after silenced on the patient monitor. Failure to take into account operation of the silence feature of the monitor by unqualified or un-trained personal may lead to improper delays and/or suppression of notifications leading to potential patient harm.

CAUTION:	The product must utilize the hospital emergency power system. Failure to do so will 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 will be 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:	Only qualified and trained personnel or service personnel should attempt to service theequipment. 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 insure compatibility with the product software, use only approved components to repair any part of the product. Use of unauthorized software system.

CAUTION:	Properly dispose of batteries according to local and national law.

CAUTION:	Incorrect settings or silencing of display devices can jeopardize the performance of the system.

CAUTION:	Operator 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, will be used with the product.

CAUTION:	Only compatible medical systems (i.e. GE CARESCAPE), capable of supporting the outlined communication protocols included in this manual, will be 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.

2 Requirements

2.1 Computer Requirements

See Data Sheet, MMG TD 92653EN

2.2 GE CARESCAPE MC Network Requirements

See Data Sheet, MMG TD 92653EN.

2.3 Requirements on Ascom Equipment

Ascom handsets. It is recommended to use handsets with support for Interactive Messaging (IM).

2.4 Abbreviations and Glossary

Action Handler	The part of MMG that handles Actions. This is set up in Action Configuration.
Template	A template with settings for a sample unit, provided by Ascom
ECG (Electrocardiogram)	An ECG is a diagnostic tool that measures and records the electrical and muscular function of the heart.
Elise3	Embedded Linux Server
Event	In MMG, events are used to trigger actions.
GEC (GE Client)	The image presentation server subsystem responsible for communicating with GE CARESCAPE Gateway.
GE CARESCAPETM Network	Ethernet-based network that connects GE patient monitoring equipment and servers.
Groups	Used to set up messaging in the Unite Connectivity Manager. If a message is sent from MMG to a group number, the message is sent to all **call ID**s belonging to that group. In the group setup, the **call ID**s to be included are specified. See also Appendix F, F.1 Creating User Teams in Unite CM.
ICU	Intensive Care Unit: Hospital unit used as an example in templates and use cases
image presentation server	A server that generates ECG images upon request from MMG, when an alarm has occurred and a snapshot is taken. The image presentation server has two main subsystems: IMGS and GEC.
IMGS	Image Server. The part of the image presentation server that generates ECG waveform images and communicates with the MMG.

Interactive Message	A message sent from MMG to a handset, requesting a response from the user.
MMG	Mobile Monitoring Gateway
Output Activity	Setup of physical outputs on the Elise3 board that can be used to trigger customer applications.
Handset	Any type of Ascom handset, pager or smart device
RWhat	A discovery protocol used by GE
Unite	The Unite system is 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.
UNS	Unite Name Server - Unite component that holds the number plan. The number plan is a list of users and **call IDs**. It is mainly used during setup of a system and is preferably prepared prior to installation

2.5 Symbols and Descriptions

In the SW "About" File	Title of symbol	Description
	CE mark	Indicates the conformity of the device with the provisions of Council Directive 93/42/EEC of 14 June 1993 concerning medical devices to enable it to move freely within the Community and to be put into service in accordance with its intended purpose.
	Manufacturer	Indicates the medical device manufacturer, including address and telephone number.
	Date of manufacture	Indicates the date when the medical device was manufactured.
	Catalogue number	Indicates the manufacturer's catalogue number so that the medical device can be identified.
	Consult instructions for use	Indicates the need for the user to consult the instructions for use.
	Caution	Indicates the need for the user to consult the instructions for use for important cautionary information such as warnings and precautions that cannot, for a variety of reasons, be presented on the medical device itself.

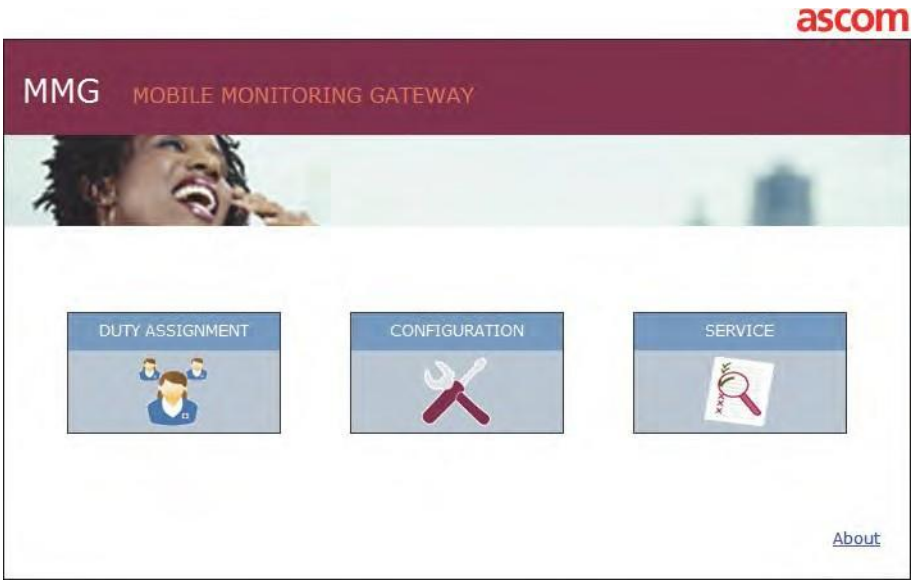
UDI	Unique Device Identifier	Indicates a Unique Device Identifier that adequately identifies a device through its distribution and use.
Rx only	Prescription device	
		CAUTION: Federal law restricts this device to sale by or on the order of a licensed medical practitioner.

3 MMG General

3.1 The MMG Start Page

From the MMG start page you can select different functionality.

Figure 2. The MMG Start page.



Duty Assignment

This is where to configure the layout for locations and to assign recipients to events. See Duty Assignment in 5.1.1 Basic Setup.

Configuration

This is where configuration and administration of MMG is done. It is only possible to log in as admin or sysadmin.

Service

This is where the verification can be done that MMG is properly configured. You will find the manufacturer name and address by clicking the about link.

3.2 Authentication Levels and Default Passwords

To enter MMG, a user ID and Password is required. The users are admin, sysadmin or a defined user. A defined user logs in with a user ID and password that is set up by the local administrator. To change passwords, see 5.2.26 Setting passwords.

System administrator rights gives full access to all administration pages, permission to change all passwords and is required for advanced troubleshooting. Default user name and password are “sysadmin” and “setmeup.”

Administrator rights are required for setup, configuration and administration of MMG. Simple troubleshooting and changing passwords (except for the sysadmin password) are also allowed. Default user name and password are “admin” and “changeme.”

User rights gives access to MMG on a level depending on which User Teams the user belongs to, see 8.4 Setting up Access Rights.

3.2.1 Log in to Configuration and Service Pages

When clicking the Configuration page or the Service page, you will be prompted to log in. Once logged in to one of these pages you do not need to log in to the other page because the login session is shared between the pages. For example, if you have logged in to the Configuration page and then navigates to the Service page, you do not need to log in to the Service page.

NOTE: The login session is not shared with Access Rights, Action Configuration, event Assignment and Duty Assignment applications, which can be accessed from the Configuration page. This means that you will be prompted to log in each time you click on these applications. The login session expires when clicking **Log out** on the page or when closing the web browser.

Figure 3. Login page for Configuration and Service pages.

4 Installation

This chapter is intended for installation personnel. For mounting and connection of cables, refer to the Installation Guide, Elise3 TD 92679GB.

4.1 Description of LED Indicators

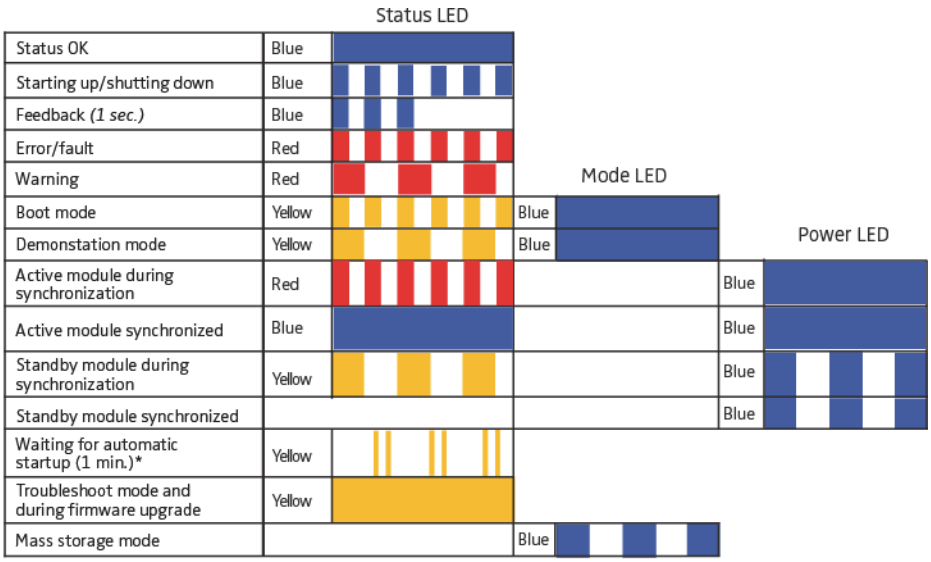
The Elise3 hardware is used by the Mobile Monitoring Gateway (MMG) and also by the Unite Connectivity Manager (Unite CM). The Elise3 hardware has LEDs that indicate the status of the MMG software, see Flashing Patterns below.

The LEDs show different colors to determine type of information and have different flashing frequency for showing the priority, see below.

Figure 4. Elise3 Hardware

Colors	Description
Red	Fault indication
Yellow	Mode indication
Blue	Normal operation (**OK**)

Flashing Patterns



* also used while in Troubleshoot mode and during firmware upgrade

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

Fixed light indicates normal state
Slow flashing light indicates medium attention
Quick flashing light indicates high attention

4.2 Internal Outputs

MMG has two configurable outputs. By default, output one is used to indicate alarms that have not been taken care of. For connections and a more detailed description of the outputs, see Installation Guide, Elise3 TD 92679GB.

4.3 Error Relay

The error relay output can be used to indicate if MMG is operating. When MMG starts, the error relay operates. When MMG is shutting down or restarting, the error relay releases.

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

4.4 Licenses

For available licenses, see Data Sheet, MMG TD 92653EN.

4.5 Demonstration Mode

When needed, MMG can be started in Demonstration mode. MMG will have full functionality for 2 hours. When the time for Demonstration mode runs out, the MMG needs to be restarted, either physically or from the MMG Administration page.

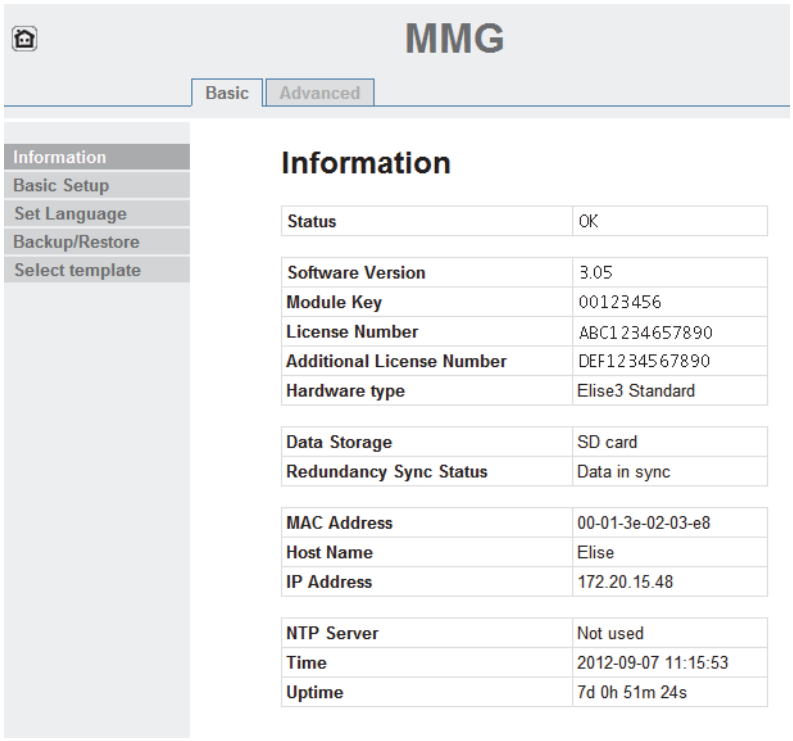
5 Configuration

This chapter is intended for system administrators during setup of MMG. The configuration pages can be reached from the MMG start page.

Figure 5. The Configuration icon on the MMG start page.

With system administrator or administrator rights you will be able to access the Configuration page. After you have logged in, system information will be shown such as host name, IP address and MAC address. Links to documentation are also found in the Configuration page.

Figure 6. System information on the Configuration page.



The system information can later on be viewed by selecting the Basic tab > Information. Use the  symbol to return to the MMG start page.

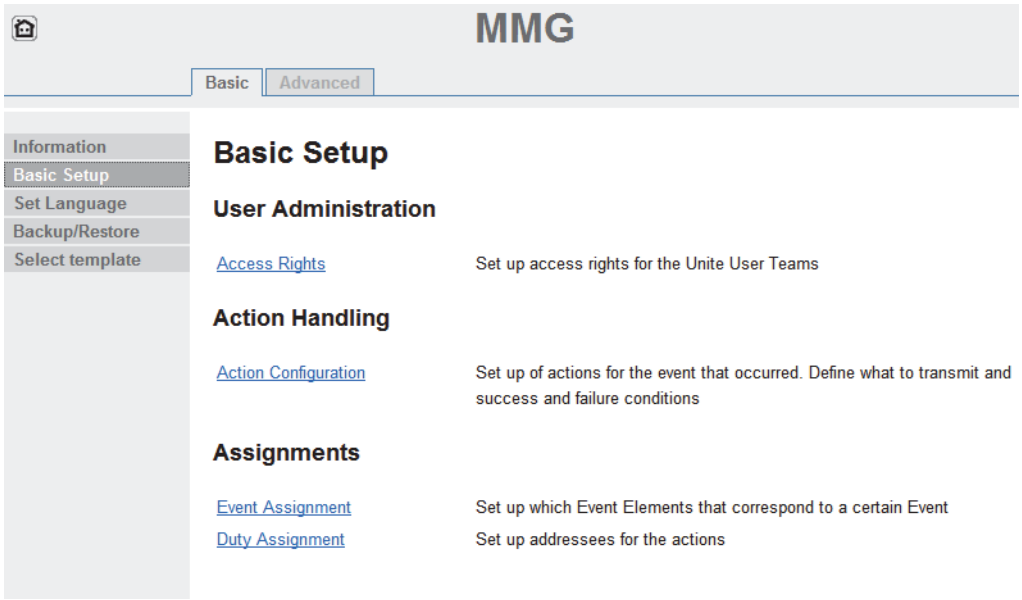
The Configuration page is divided into two pages as follows:

- 5.1 Basic Configuration
- 5.2 Advanced Configuration

5.1 Basic Configuration

The Basic configuration page can be reached by clicking the “Basic” tab and then click “Basic Setup.” This page has two tabs, one for basic settings and one for advanced settings. The Basic tab is used for configuration and assignments.

Figure 7. The Basic Setup Configuration Page



This section describes how to change the language, and how to backup and restore the MMG database. There are two types of users for the basic setup:

- First time set up by a system administrator (sysadmin) Full access rights.
- Local Administrators (admin)

Full access rights, except for advanced troubleshooting (to view certain logs and for debugging) and setting password for sysadmin.

There is also another type of user that the administrator sets up:

Normal users. These users can have access right to all GUIs, except the advanced configurations found in the Basic Administration page.

5.1.1 Basic Setup

Access Rights

In this page, access rights for User Teams are set up. See 8.4 Setting up Access Rights.

Action Configuration

Action Configuration is where actions for the events are configured. See 8.1 Action Configuration.

Event Assignment

Event Assignment is where event Elements are defined and assigned Events are administrated. See 8.2 Adding Event Assignments.

Duty Assignment

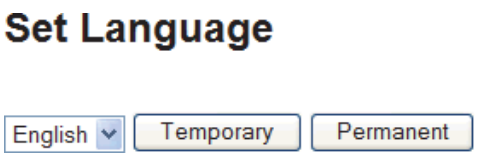
See 7 Operation.

5.1.2 Setting Language

The default language in MMG is English. The texts that appear in the GUI are stored in a database. Several languages can be stored in the database, but it is not possible to edit or remove the default language. Additional languages can be imported.

Additional languages can be imported.

1. Select the **Basic** tab, and then select **Set Language**.
2. Select language from the drop-down list. If the language you want to use is not in the drop-down list, import the language.



3. If you only want to change the language for the current browser window, click “Temporary,” otherwise click **Permanent**.
4. The windows Duty Assignment, event Assignment, Action Configuration and Access Rights need to be closed and reopened for the new language to take effect.

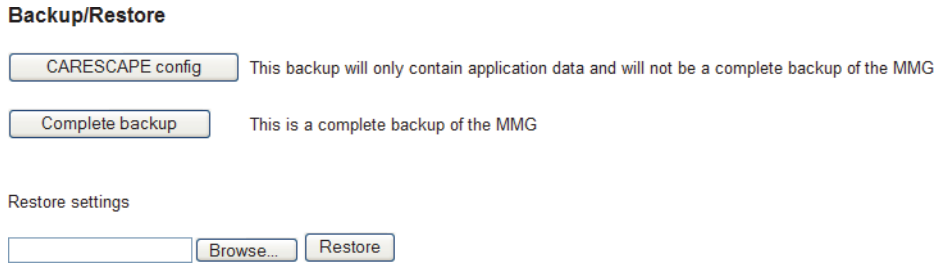
5.1.3 Backing up or Restoring

Backing up the CARESCAPE configuration, can for example be used when information is to be copied from one MMG to another MMG or to restore the database in MMG. The extension of the backup/restore file is .tar.gz.

The CARESCAPE config backup includes settings for Duty Assignment and Action Configuration.

NOTE: The backup does only include the CARESCAPE specific parameter settings from the Basic Administration page.

Figure 8. Backup/restore of the application data settings in MMG.



Backup

1. Select the **Basic** tab, and then select “Backup/Restore.”
2. Click “CARESCAPE config” or “Complete backup.” Complete backup is used to back up the whole configuration.
3. Click **Save** in the File Download window. The Save As dialog window opens.
4. Select a location, enter a file name, then save the file.

Restore

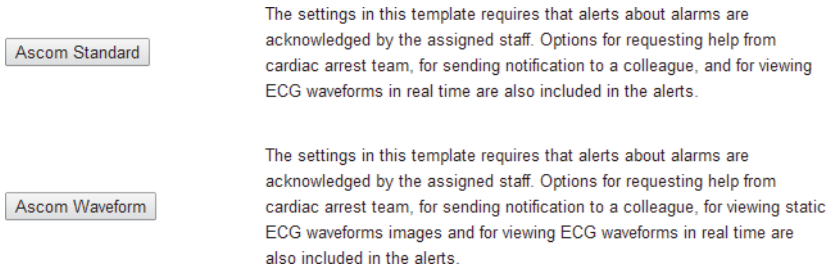
1. Select the **Basic** tab, and then select “Backup/Restore.”
2. Click “Browse...” to locate the .tar.gz file.
3. Click “Restore.”

NOTE: When MMG is restored, all changes that have been made since the last backup will be discarded.

5.1.4 Selecting a Template

A template is a backup file that is delivered with the product and so, by choosing to load a template, the previous settings in MMG are replaced with the settings in the template. Note that no template is selected from factory; this must be made manually before configuration of user-specific settings.

1. Select the **Basic** tab, and then select **Select template**.



2. The following templates can be selected:

– **Ascom Standard:** The settings in this template require that alerts about alarms are acknowledged by the assigned staff. Options for requesting help from cardiac arrest team, for sending notification to a colleague, and for viewing ECG waveforms in real time are also included in the alerts.

– **Ascom Waveform**: The settings in this template require that alerts about alarms are acknowledged by the assigned staff. Options for requesting help from cardiac arrest team, for sending notification to a colleague, for viewing static ECG waveforms images and for viewing ECG waveforms in real time are also included in the alerts.

5.2 Advanced Configuration

The advanced configuration can be reached by selecting the “Advanced” tab. The advanced configuration is normally only used by system administrators during configuration and database administration. You can configure and administer MMG, to add translations, set up inputs and outputs and enter the MMG Basic Administration page.

Figure 9. The MMG Advanced setup tab with the Translation page selected.

In the left menu, the following choices can be selected:

- Translate GUI
- I/O Setup
- CARESCAPE Test Alarm
- CARESCAPE locations
- Software Information
- Switch Software
- Software Installation
- Redundancy (license dependent feature)
- Demonstration Mode
- Basic Administration

5.2.1 GUI Translation

1. In the MMG start page, click **Configuration**.
2. Click Advanced.
3. In the left menu, select **Translation**.

The file that needs to be translated is an XML file generated from MMG. To save the file for translation or editing purposes, click the language link in the list of languages and save the file.

In the language file, there are numerous tags but only two tags and one attribute that needs to be translated:

- <language id="English">

the "id" attribute is the text that appears in the drop-down list

<translation>

- name of menus, buttons, tabs etc.

<helptext>

- online help text

Below is an example of a language file (just showing two buttons with help text, for simplicity).

Figure 10. An Example of a Language File.

```
<?xml version="1.0" encoding="ISO-8859-1"?>
- <translations>
  - <language id="English" type="complete">
    - <app id="XGATE">
      - <text id="BUTTON_APPLY_LANGUAGE_TO_SESSION">
          <translation>Apply</translation>
          <helptext>Click this button to apply the selected language to this session</helptext>
        </text>
      - <text id="MENU_XGATE_BASIC_SETUP">
          <translation>Basic Setup</translation>
          <helptext>Links to administration tools for basic XGate settings</helptext>
        </text>
      </app>
    </language>
</translations>
```

006

When the file is translated, it must be imported to the database. Click **Browse** to locate the translated file and click **Import**.

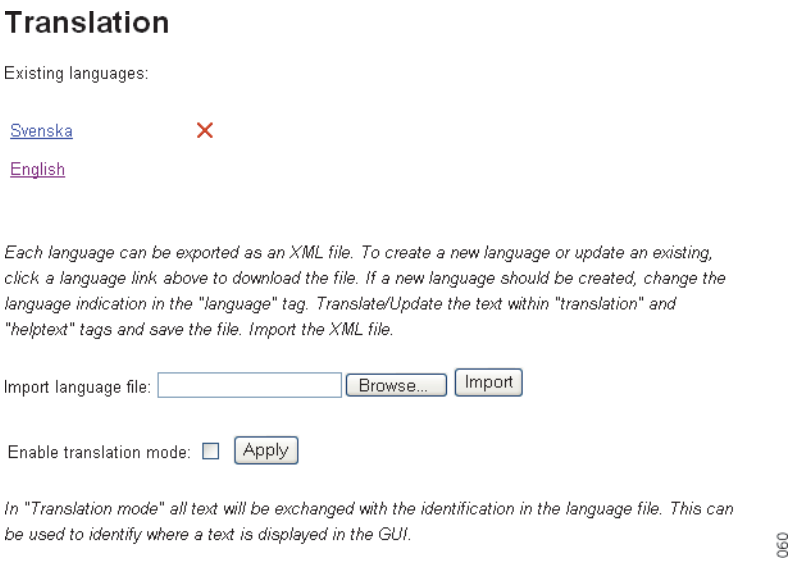
The name of the translated language (the language "id" attribute) will appear as a link in the Existing Language list and can be down loaded for editing purposes.

The MMG GUI only supports the Latin-1 character set.

Deleting a Language

A language file can be deleted from MMG by clicking the **Delete** icon. It is not possible to remove the default language.

Figure 11. A language file to be deleted.



GUI Updates

When a new version of MMG is released, there might be changes in the GUI that need to be translated.

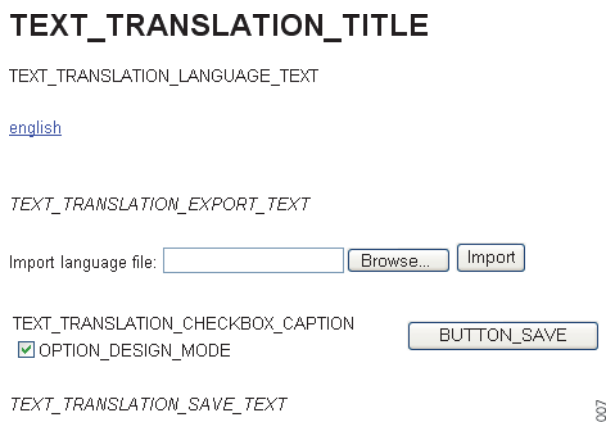
1. Import your old translated file to the new MMG software version. New text and buttons in the GUI will be shown in English, since this is the default language. It will now include the additions.
2. Click the language file link and save it.
3. Open the file and all tags that are not translated are marked with the comment:
4. <!-- The text identifier below couldn't be translated
5. Translate the new text and import the translated file again

Translation Mode

All texts, buttons, menus etc. are identified with labels (for example MENU_MMG). With the translation mode function, you can view the label for each button, menu etc. This can be helpful when translating the language file.

1. Check the **Enable translation mode** box in the Translate page. Click **Apply** and all the labels on the pages are shown, see example below.

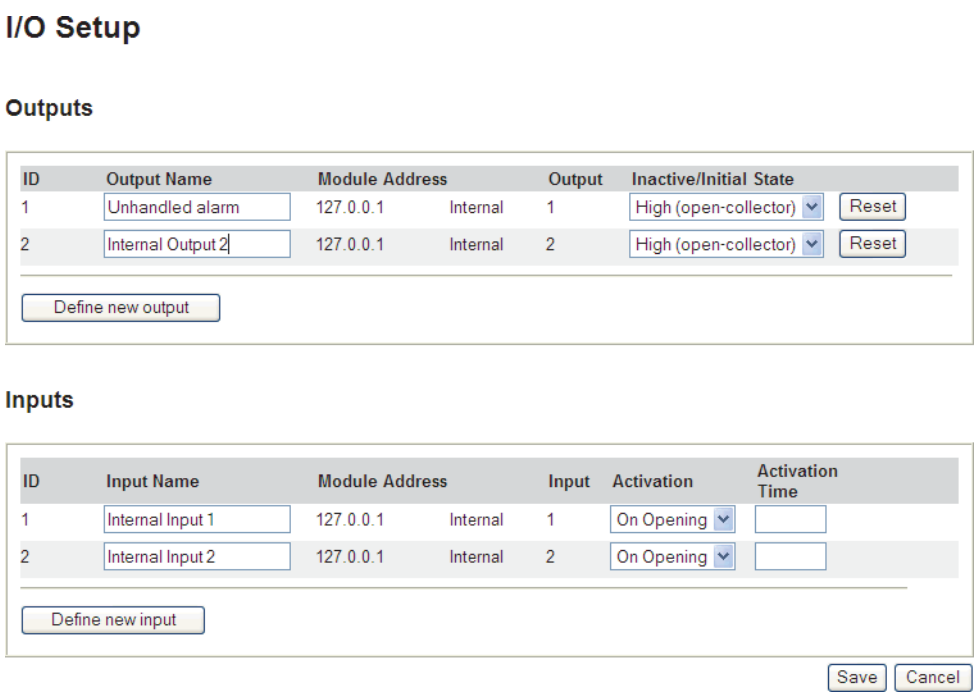
Figure 12. Design mode of the Translation page.



2. Clear the **Enable translation mode** box and click **BUTTON_SAVE** to return to standard view.

5.2.2 Input and Output Setup

1. In the MMG start page, click Configuration.
2. Click Advanced.
3. In the left menu, click I/O Setup. The initial state for the output can be low or high. The inputs can be selected to be activated on opening or on closing.



For the outputs, the state is set to the opposite of the inactive state when activated. For example, if output 2 isset to low in inactive state, the output will automatically be set to high.

Inputs and outputs are placed on the rear side of the module, refer to Installation Guide, Elise3 TD 92679GB.

Defining Outputs

1. Click Define new output.
1. Every time a new output is defined an automatic ID is created. The ID is a running number which can manually be changed into another number or a text if wanted. When an output has been deleted, MMG will not remember that the previous ID number is free to be used again. The numbering will just continue on the number after the last created one (see figure above). You can use outputs on other modules.
2. Enter output name, module address and output number.
3. Select initial state.
4. Click **Save**.

Defining Inputs

Not applicable in MMG.

5.2.3 CARESCAPE Network Test Alarm

In the CARESCAPE Test Alarm page you can send a test alarm to the CARESCAPE Network port of MMG. This feature is intended for troubleshooting purposes. See also Troubleshooting Guide, Alarm Management for GE Patient Monitoring, TD 92717GB.

Figure 13. The upper part of the CARESCAPE Test Alarm page.

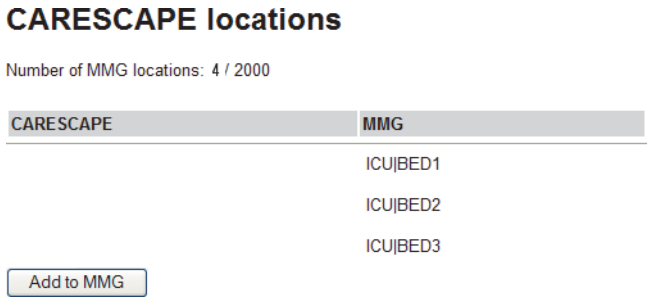
Select simulated alarm location origin and click **Send**.

This page can also be reached directly from the MMG start page by clicking **Service**.

5.2.4 CARESCAPE Locations

A list of locations can be shown in the CARESCAPE locations page. The list includes locations that MMG has received from CARESCAPE and locations that have been set up in Duty Assignment. This list is mainly used for troubleshooting purposes. See also Troubleshooting Guide, Alarm Management for GE Patient Monitoring, TD 92717GB.

Figure 14. An Example of a Location List in MMG.



NOTE: Number of locations includes all locations that have been set up, but the MMG list only shows locations.

below the top level i.e. ICU is a location but is not presented on a separate row in the list. You can also add missing locations, if a matching unit is defined in MMG.

For example, in order to add missing beds to the ICU there must be a location defined in Duty Assignment with an arbitrary name and a condition for the location event element to equal ICU.

5.2.5 Software Information

All information about the installed software is shown in this view. Two software versions can be installed on the hardware.

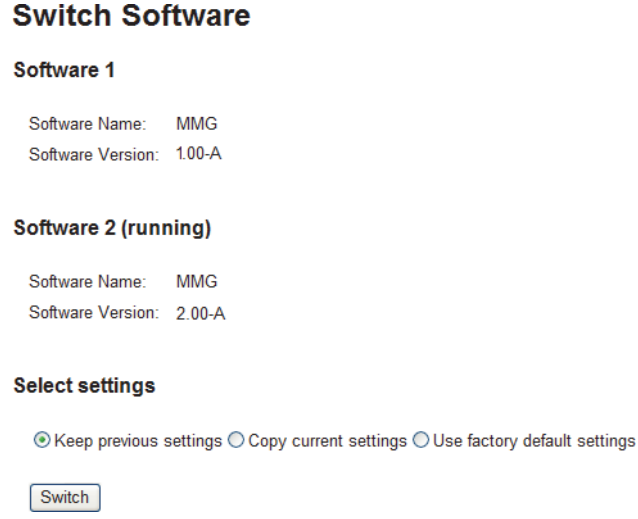
1. Click **Configuration** on the start page.
2. Click Advanced.
3. Select **Software Information** in the menu.

The software name, versions, the date they were installed and also which software that currently is running are shown.

Switch Software

If two software versions are installed on the Elise 3 hardware you can switch between them. The options are only visible if two versions are installed.

1. Click **Configuration** on the start page.
2. Click Advanced.
3. Select **Switch Software** in the menu.



1. Under Select settings, select one of the following

- **Keep previous settings** - select this option if you do not want to change the software's settings you want to switch to.
- **Copy current setting** - select this option if you want to copy the active software´s settings to the software you want to switch to.
- **Use factory default settings** - select this option if you want to apply the factory default settings for the software you want to switch to.

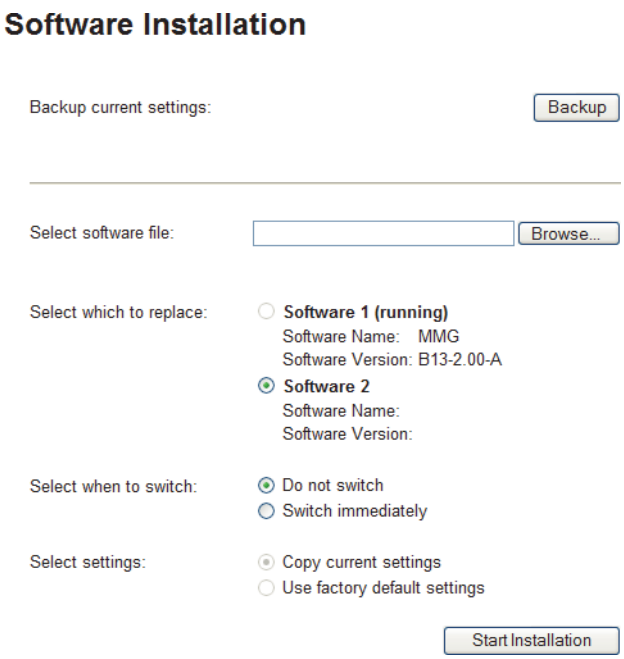
NOTE: The active software's current network settings will be kept and will also be applied to the software you want to switch to.

2. Click Switch.

5.2.6 Software Installation/Upgrade

NOTE: It is recommended to take a backup of the parameters before upgrading/installing the software to be able to keep the settings, see 5.1.3 Backing up or Restoring. It is not recommended to use the module's Management port when installing software.

1. Click **Configuration** on the start page.
2. Click Advanced.
3. Select Software Installation.
4. Select software (.pkg) to upload. The software will replace the not running software.
5. Select **Switch immediately** to run the new software.
6. Select **Copy current settings** in order for the new software to inherit the settings currently used.
7. Click Start Installation.



lo

8. Restore the backup, see 5.1.3 Backing up or Restoring.

5.2.7 Software Upgrades in a Redundant System

In a redundant system where the data between the primary MMG and the secondary MMG are synchronized,

it is only needed to install the software on the primary MMG. The software will also be installed on the secondary one automatically. Follow the instructions in 5.2.6 Software Installation/Upgrade.

5.2.8 Module Redundancy

A redundant system consists of an active MMG and a standby MMG. When setting up the module redundancy in the system, the primary MMG will act as an active MMG, and the secondary MMG will act as a standby MMG. When the active MMG goes down, the standby MMG will be activated and takes over the operation from the other MMG. The MMGs will indicate that the system no longer is redundant since no data synchronization between them can be performed.

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

Prerequisites

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

- The installed software version (3.10 or higher) must be identical on both MMGs. The MMGs 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 MMG must support module redundancy (license dependent feature).

- The secondary MMG must not have any licenses installed.
- Three static IP addresses. Ask your network administrator to obtain the IP addresses.
- The MMGs must be supervised by a Unite CM. The Unite CM is used to report if the MMGs goes down. Make sure that the Unite CM is configured to escalate any MMG fails to dedicated users. See “System Supervision and Security” in Unite Connectivity Manager, Configuration Manual TD 92735GB.

Preparing IP Addresses in a Redundant System

It is assumed that your system already have one MMG installed and that an additional MMG will be installed in order to set up a redundant system.

The three static IP addresses will be used as follows:

- Two IP addresses will be used by the primary- and secondary MMG.
- The third IP address will be used by the equipment (for example the GE CARESCAPE equipment and Unite CM to communicate with the active MMG when the system has become redundant. In this document, the third IP address will be called "virtual IP address."

Network without DCHP Server

1. Replace the IP address in the origin MMG 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 MMG to be used as secondary module has been assigned correct IP address.

Network with DCHP Server

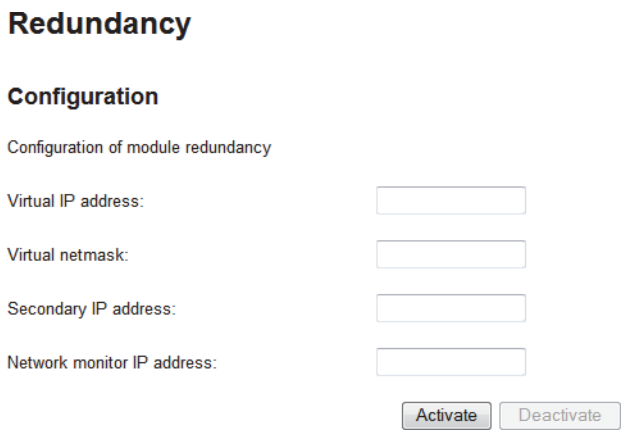
1. Make sure that the origin IP address of the MMG no longer is reserved to the MMG’s MAC address. Note the IP address still must be available but not reserved to a specific MAC address. Consult your network administrator. This IP address will be used as virtual IP address later on.
2. Ask your network administrator to reserve a new static IP address to the original MMG, to be used later as a 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 MMG to be used as secondary module. The IP address must be reserved to the module’s MAC address.

5.2.9 Configuring Redundancy in MMG

Do the following on the MMG to be used as primary MMG:

1. Click Configuration on the start page.

2. Click the "Advanced" tab, then click **Redundancy**.



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

1. In the Virtual IP address text field, enter the virtual IP address.
2. In the Virtual netmask text field, enter the netmask of virtual IP address.
3. In the Secondary IP address text field, enter the IP address of the secondary MMG.
4. In the Network monitor IP address text field, enter the IP address of the equipment to be used as network reference. The MMG 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: Primary, secondary and virtual IP addresses on different subnets are not supported in a redundant system.

NOTE: The network topology used in the system may have impact on which equipment that should be used as network reference. See Appendix E. Network Monitoring in a Redundant System.

5. Click Activate.

NOTE: Once **Activate** is pressed, it is not possible to undo the activation of the module redundancy. However, you can deactivate the module redundancy by clicking "Deactivate" and then click "Really deactivate." The module will reboot immediately. The GUI will not be updated automatically when the reboot is done. Update the GUI by pressing **F5**.

6. Click Reboot Now or Reboot Later.

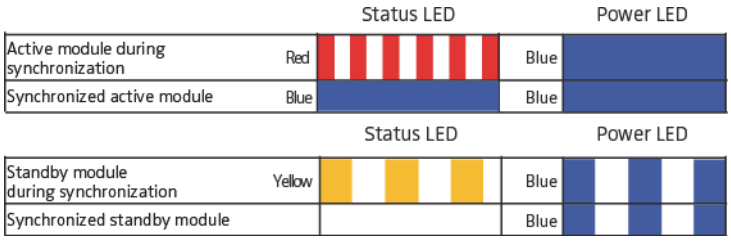
The MMG reboots and copies data from its internal flash memory to the SD memory during the startup sequence. This can take up to 3 minutes. The GUI will not be updated automatically when the reboot is done. Update the GUI by pressing **F5**. Note that Primary will be stated in the GUI's upper left corner when the module is up and running again.

IMPORTANT: Do not remove the SD memory card from the MMG that acted as primary module. The SD memory card on that module will still be used as storage even when the module redundancy has been deactivated.

When the data has been copied, the primary MMG sends configuration settings to the secondary MMG that in turn reboots to apply the settings. After the reboot, the data will be synchronized with the secondary MMG'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 MMG is fully operational. The LEDs on each MMG indicate the status of the synchronization.

Figure 15. LEDs showing the status of synchronization.



You can view the synchronization status via the GUI, see Figures 16 and 17. Use the virtual IP address to access the active MMG and the static IP address to access the standby MMG.

Figure 16. Redundancy synchronization status on the primary module's Configuration page

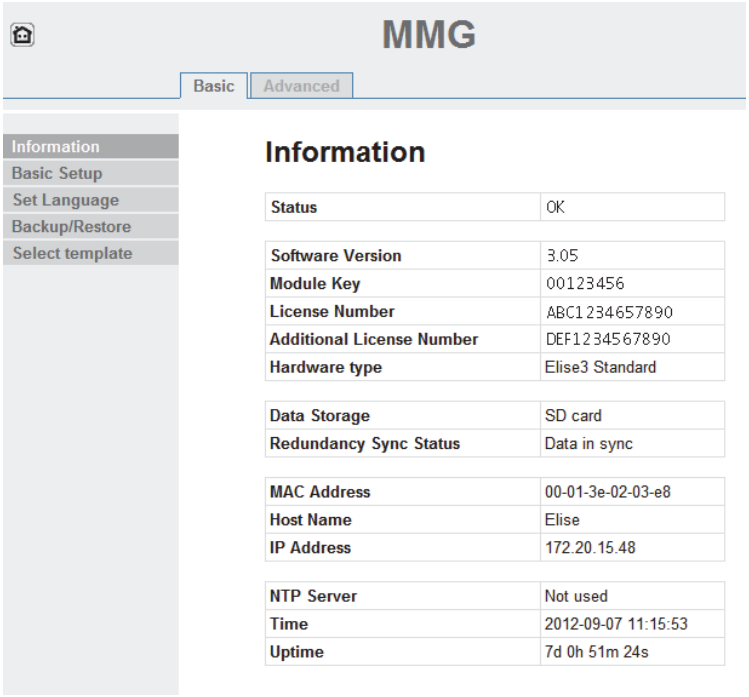
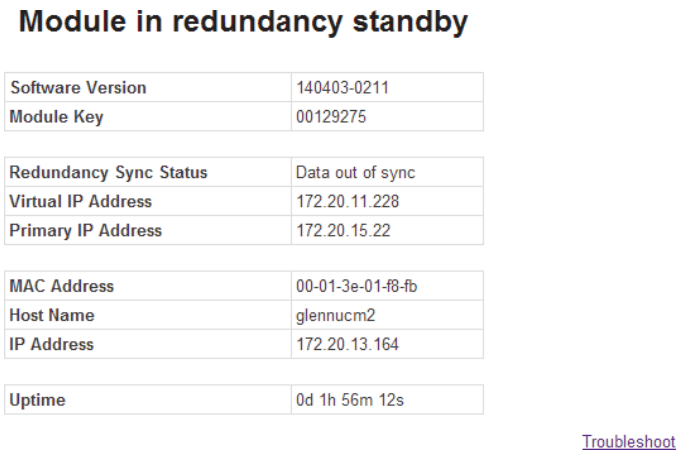


Figure 17. Redundancy synchronization status on the secondary/standby module.



Module in redundancy standby

Software Version	140403-0211
Module Key	00129275

Redundancy Sync Status	Data out of sync
Virtual IP Address	172.20.11.228
Primary IP Address	172.20.15.22

MAC Address	00-01-3e-01-f8-fb
Host Name	glennucm2
IP Address	172.20.13.164

Uptime	0d 1h 56m 12s

Troubleshoot

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

- Synchronizing - The synchronizing is in progress. Additionally, a percentage indicator shows the amount of data that has been synchronized.
- Data in sync - The data in the modules is synchronized. 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 MMG is lost.

When the system has become redundant, the virtual IP address will be used by the MMG that currently is active. That is, the module that has become a primary module.

5.2.10 Module Redundancy Test

IMPORTANT:	It is important to perform a module redundancy test to ensure that you have configure the system correctly.

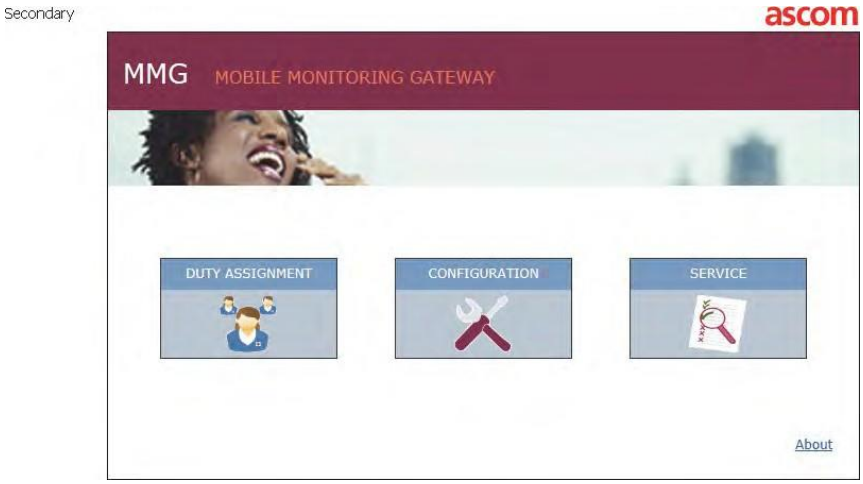
1. Unplug the active MMG's power cord from the power source.

The standby MMG will now start up to become an active MMG which takes up to 60 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 MMG (former active MMG) is lost.

When the standby MMG 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 MMG using the virtual IP address. Note that Secondary is stated in the upper left corner indicating that this module currently is the active MMG.



3. View the log on the Unite CM that supervises the MMG. On the Unite CM, select Status > Active Faults on the Configuration page. The log shows for example that the secondary MMG is active and that the primary MMG has failed. Other faults might also be shown.

TIP: The IP address of the Unite CM that supervises the MMG can be found in the Logging page on the MMG, see Logging in 0

Units and Filters.

4. Perform an action to ensure that the active MMG works properly. For example, simulate a GE CARESCAPE test alarm to see if a handset receives the alarm.
- Enter the virtual IP address in a web browser to access the active MMG. In this case, it should be the secondary MMG that has become active.
- In the MMG start page, click **Service**.
- In the CARESCAPE Test Alarm page, select a location (for example ICU|BED1) and click **Send**.
5. Check if the handset received the alarm message. If not, see Troubleshooting Guide, Alarm Management for GE Patient Monitoring, TD 92717GB for more information on how to solve the problem.
6. Connect the primary MMG and check if the secondary MMG starts to synchronize with the primary MMG. A completed synchronization is indicated as follows;
- On the secondary MMG; the Status LED and the Power LED will be steady blue as long the module acts as an active module.
- On the primary MMG; the Status LED is turned off and the Power LED will still flash blue as long the module acts as a standby MMG.
- The synchronization status on both MMGs will be changed to Data in sync when the data is synchronized.

After the test, it is recommended to switch back to the primary MMG again. See 5.2.12 Fallback to the Primary MMG.

Fault Handler Notification on Redundancy Failover

By properly utilizing the Fault Notification capability of the Unite System it is possible to generate notifications when a fault in the primary module has occurred, causing a fail-over to the secondary module. Proper configuration should occur by identifying the ip address of the defined Fault Handler (typically the Unite Connectivity Manager UCM) within the Status Log configuration of the MMG. (See Logging in 0

Units and Filters).

The Unite CM can be configured to perform a fault action if it receives a Status log from the MMG. A fault action can, for example, be an e-mail or a message sent to an IT individual responsible. See Appendix G. Supervision of GE CARESCAPE Network and MMG for more information.

5.2.11 Restrictions on an Active Secondary MMG

A secondary MMG that has become active has redistricted functionality as follows:

IMPORTANT:	The secondary MMG can only be up and running as active MMG for 30 days without a repaired primary MMG connected. If you for example shut down the secondary MMG day 10, it can still use the remaining twenty days when it is started again. If the repaired primary MMG is not connected within 30 days, the secondary MMG will fallback as a standby MMG. This means that no alarms can be escalated to the users due to no MMG will be up and running.

- It is not possible to disable the module redundancy
- It is not possible to perform a backup/restore
- It is not possible to add a license
- It is not possible to run the wizard
- It is not possible to activate the demonstration mode.

5.2.12 Fallback to the Primary MMG

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

NOTE:	The network monitoring setting might affect the fallback behavior, see E.1 Fallback behavior when Network Monitoring is Not Used.

NOTE:	If you for some reason reboot the secondary module via the GUI, the primary module will not take over.

as active module. However, if the secondary module is not up and running again after 3 minutes, the primary module will become active.

On the secondary MMG, do as follows:

1. Click **Configuration** on the start page.
2. Click Advanced tab and then click **Redundancy**.
3. Click **Fallback** to primary module.

NOTE: It is only possible to press the button if the data has been synchronized with the primary MMG. The primary MMG will now act as an active MMG and the secondary MMG will act as a standby MMG.

The primary MMG will now act as an active MMG and the secondary MMG will act as a standby MMG.

5.2.13 Access Troubleshooting Pages

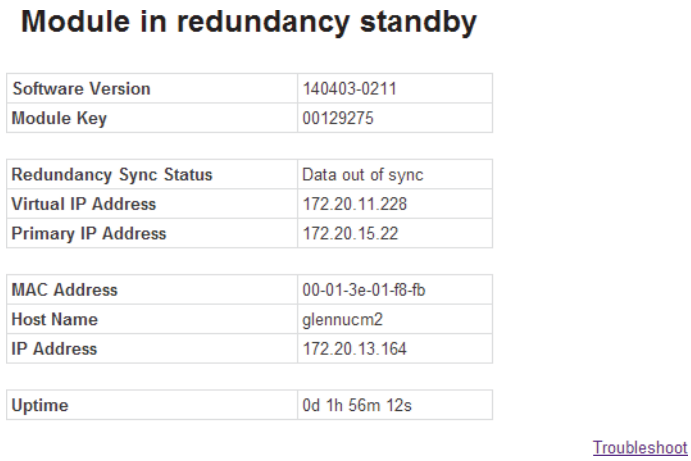
If a module fails or it does not work as expected, the logs on the Troubleshooting page can give you information about the status of the module.

Troubleshooting page on active module

1. Click **Configuration** on the start page.
2. Click the "Advanced" tab and then click **Redundancy**.
3. Click Basic Administration
4. Click the “Troubleshoot” button on the Advanced Configuration page.
5. Click “View Info Log” or “View Error Log.”

Troubleshooting page on standby module

Click the “Troubleshoot” link on the Standby page.



NOTE: When entering the Troubleshoot page on a synchronized standby module without any errors, "License Error" and "Module Error" are shown. This is normal and no action is required.

5.2.14 Deactivate module redundancy

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

1. Click **Configuration** on the start page.
2. Click **Advanced** tab and then click **Redundancy**.

3. Click **Deactivate**.
4. Select one of the following:

- Click **Cancel deactivate** to undo the deactivation.
- Click **Really deactivate** to perform the deactivation. Both MMGs will now reboot immediately. The GUI will not be updated automatically when the reboot is done. Update the GUI by clicking **F5** on your keyboard.

5. Do one of the following:

- If the IP address was changed in the primary MMG: Change the IP address in the former primary MMG to its origin IP address.

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

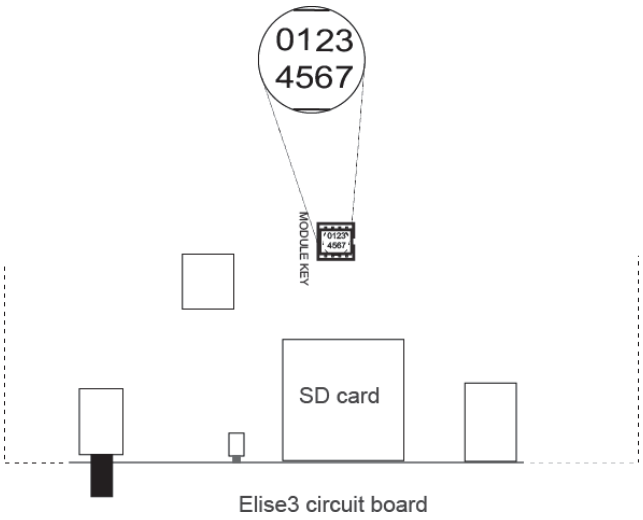
- If the MMG's IP address was changed in the equipment (GE CARESCAPE etc.) that communicates with the MMG, change back to the MMG's origin IP address.

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

5.2.15 Replacement of Broken Module in a Redundant System

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

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.



5. Untighten 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. Run the Setup Wizard to configure network settings and license settings.
11. Configure the module redundancy, see 5.2.9 Configuring Redundancy in MMG.

When the primary module is up and running, it will synchronize with the secondary module, that currently is the active one.

5.2.16 Demonstration Mode

Demonstration mode makes it possible to run MMG for two hours with full functionality. Demonstration mode can be set from the advanced page or manually by using the Mode button. The module will automatically return to previous license and parameters (without restart) after 2 hours. From the application's advanced page:

1. Click **Configuration** on the start page.
2. Click **Advanced**.
3. Select "Demonstration Mode" in the menu.

4. Click **Activate**.
5. Click **Deactivate** to exit before the 2 hours have passed.

Using the Mode button:

1. Press and hold the Mode button for 10 seconds.

Demonstration mode is indicated by the status LED with red, slow flashing light and by the Mode button LED with blue fixed light.

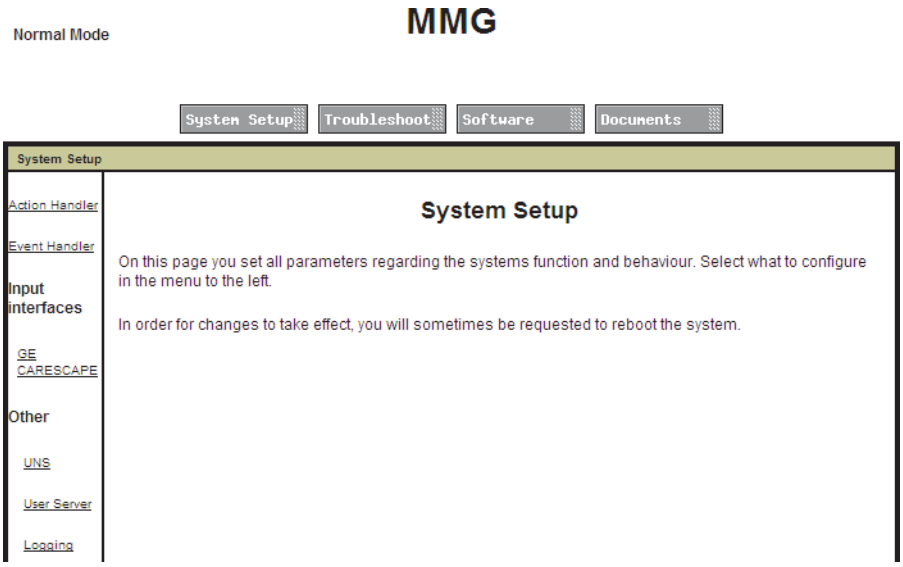
5.2.17 Basic Administration

The system setup done in the Basic Administration is described in 5.2.18 Elise3 Setup to 5.2.26 Setting passwords.

5.2.18 Elise3 Setup

1. In the MMG start page, click **Configuration**.

2. Click **Advanced**.
3. Select **Basic Administration** to enter the System Setup page.



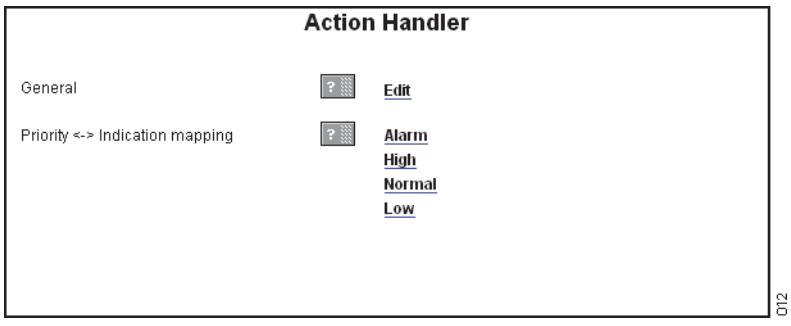
From there it is also possible to view logs for troubleshooting, to view current software versions and to get related documents.

5.2.19 Action Handler Parameter Settings

NOTE: If one of the included templates is used, there is normally no need to set up actions. Special consideration should be made prior to adjusting these settings.

Message indications can be modified dependent on the priority of the message. Different priority levels can be given different beep signals and be mapped to different colors as an additional indication to the recipient of the message. The priority color will be shown in the receiving display devices and applications (e.g. Unite View).

1. In the MMG start page, click **Configuration**.
2. Click Advanced.
3. Click Basic Administration.
4. In the left menu, click “Action Handler” for parameter settings.

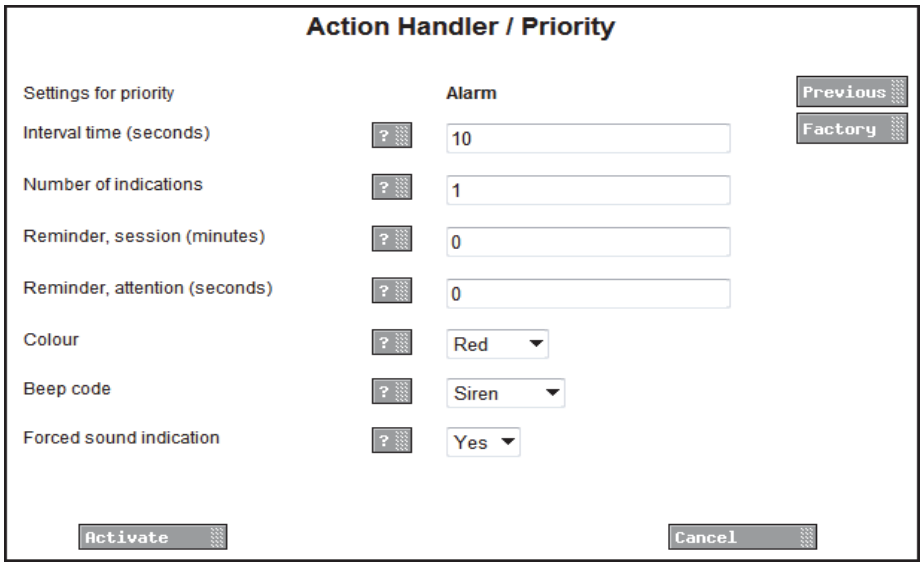


General Parameters

- Individual group member response: Set to **Yes** if an action sent to an address that is diverted to two or more members, will wait for responses from all members before deciding the action to be a failure. Default value is **Yes**.
- Call digits prefix: Enter the call digit prefix so that devices which receive interactive messages over an external carrier are able to properly route calls.

Priority Indication Mapping

In each of the priorities you can set up how the indication should be repeated. Special consideration should be made prior to adjusting these settings.



Parameter Descriptions

- Interval time (seconds): Determines the time to be elapsed between each repetition of the indication.
- Number of indications: Determines the number of indications to be repeated
- Reminder, session (minutes): Enter the interval between indications for an unread message.
- Reminder, attention (seconds): Enter the time between indications before any option has been selected in this message. Typically, if the recipient has opened the message, but an IM option has not been selected, a reminder alert will sound. Values: 1-255 seconds.
- Colour: Determines which color coding messages with this priority will have. If not set, the message will be sent according to the default setting in the Unite Connectivity Manager.
- Beep code: Determines which default beep code messages with this priority will have. The setting might be overridden in the individual messages, defined in Action Configuration.
- Forced sound indication: Determines if sound indication for messages with this priority level (High, Normal, and Low) always will breakthrough in a device, even though the device is set to silent.

NOTE: Use this parameter with care. It is strongly recommended to only enable this parameter for messages that really have to breakthrough in a silenced device.

Messages with alarm priority level will always breakthrough in a silenced device regardless of this setting.

5.2.20 Event Handler

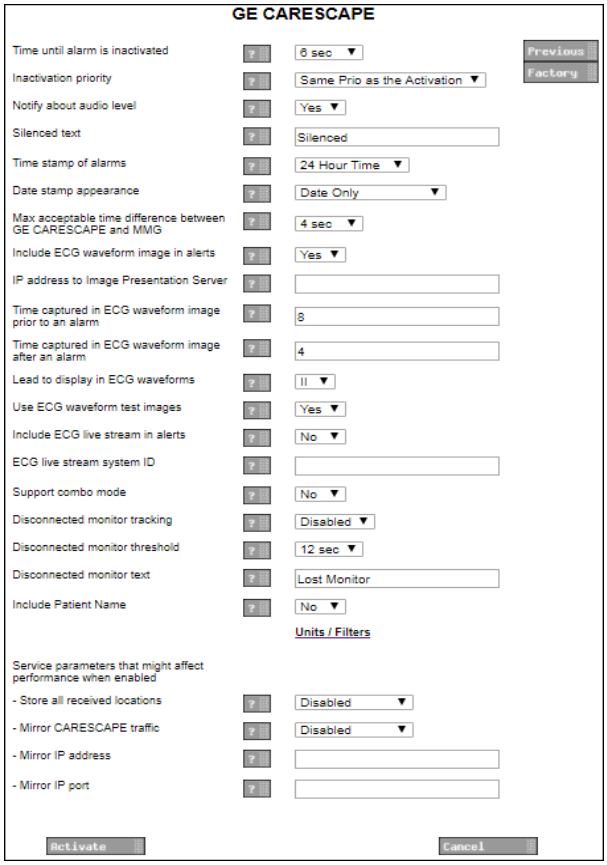
This page is only used for advanced debugging.

5.2.21 GE CARESCAPE

1. In the MMG start page, click **Configuration**.
2. Click Advanced.
3. In the left menu, click **Basic Administration**.

The application opens the GE CARESCAPE page in a new window.

These parameters handle incoming alarms from CARESCAPE (the alarms are handled as alerts in MMG).



The following parameters can be set:

Parameter	Descriptions
Time until alarm is inactivated	The time passed after the last alarm broadcast before the alarm is considered inactive.
Inactivation priority	Select which priority an inactivation of alarm will be sent with.

Notify about audio Level	Determines if the staff assigned to a location (i.e. GE CARESCAPE monitor) should be notified if someone is silencing an alerting patient monitor. This makes it possible to see which alarm that has been silenced. **No:** The staff will not be notified if the alerting patient monitor has been silenced **Yes:** A predefined text will be sent to the staff if the alerting patient monitor has been silenced. The text is set in the *Silenced Text* parameter.
Silenced text	Determines the text to be displayed in the handset if an alerting patient monitor has been silenced. The text is shown after the alarm text that belongs to the alarm that has been silenced. This setting is only used if the *Notify about audio Level* parameter is set to *Yes*.
Time stamp of alarms:	If selected to be attached, the time when the alarm first appeared will be added to the alarm text using the selected time format.
Date stamp appearance	• **Date Only:** Displays only the date**Date + 12hr Time:** Displays the date and time using 12-hour time format**Date + 24hr Time:** Displays the date and time using 24hour time format
Max acceptable time difference between GE CARESCAPE and MMG	CARESCAPE Network, the time is compared with the local MMG time. If the time differs more than this value, an entry is written to the fault log.
Include ECG waveform image in alerts	Select if the MMG requests an ECG waveform image from the image presentation server to be included in an alert message.
IP address to image presentation server	The IP address to the image presentation server that will provide ECG waveform images when requested by MMG. The default port is 8000, for example 10.30.1.2:8000.
Time captured in ECG waveform image prior to an alarm	The GE CARESCAPE equipment sends a continuous image after an alarm stream of ECG waveform data to the image presentation server connected to MMG. When an alarm is triggered, MMG will request a snapshot of the ECG Use this parameter to determine the number of seconds of ECG waveform data to be captured prior to the alarm. Value (seconds): 1 – 10. NOTE: The number of seconds of ECG waveform data to be captured *after* the alarm is also required
Time captured in ECG waveform image after an alarm	The ECG waveform data captured prior and after the alarm should be together up to 12 seconds.

Lead to display in ECG waveforms image prior to an alarm	In electrocardiography “lead” refers to the difference in voltage between electrodes on different parts of the body. The system supports sending one of three different leads: • **Lead I** is the voltage between the right arm electrode and the left arm electrode. • **Lead II** is the voltage between the right limb and the feet. • **Lead III** is the voltage between the left leg and the left arm
	IMPORTANT:: It is important to ask the hospital staff how they fasten the electrodes before you configuring the lead. Wrong settings might cause false alarms if the electrodes are not fasten according to the lead setting. This setting applies for all locations (GE CARESCAPE monitors) connected to the MMG.
Use ECG waveform test images	Determines if an image presentation server connected to the MMG will provide a fictitious ECG waveform image, instead of retrieving ECG waveform data from a GE CARESCAPE monitor.
	IMPORTANT:: This parameter will only be set to YES for test purposes. Else, make sure that the parameter is set to NO. If not, this may lead to hospital personnel taking the wrong action in critical situations.
Include ECG live stream in alerts	Select if an option for viewing ECG waveforms in real time (i.e. live stream) should be included in the alerts.
	NOTE: The “ECG live stream system ID” parameter must also be set. Additionally, live stream is only supported by smart devices with an Airstrip ONE® application installed.
ECG live stream system ID	If live stream of ECG waveforms should be used, enter the unique system ID required to log in to the smart device application used for viewing ECG waveforms in real time. The system ID is unique for each installation. Consult the system administrator to obtain the correct system ID.
Support combo mode	Select if both a fixed patient monitor and a telemetry monitor should be treated as the same location. To distinguish which monitor that triggered the alarm, the location in the alert is shown as follows: Fixed patient monitor: | (e.g. ICU|BED1) Telemetry monitor: | (e.g. ICU|BED1*)
Disconnected monitor tracking	Select if notification of a disconnected monitor from the CARESCAPE network is requested.
Disconnected monitor threshold	Defines the number of seconds a monitor can be disconnected before notification is sent.
Disconnected monitor text	Defines a textual description of the event.

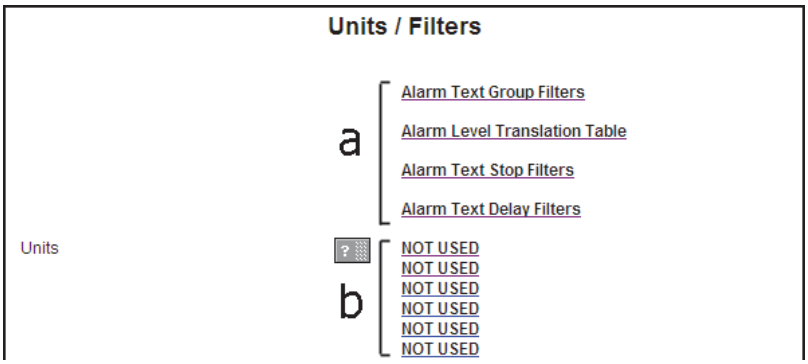
Include Patient Name	Select to provide the option to have the patient name available as content in alerts.
Unit and Filter Parameters For parameters concerning to Units / Filters, see 0 Units and Filters. The Service parameters can be used for troubleshooting purposes. Note that the performance will be affected when enabled, so be sure to disable when the troubleshooting is finished.	
Store all received locations	Select between Disabled, Alarms, RWhat or “Alarms+RWhat.” The result is displayed in the location list, see 5.2.21 GE CARESCAPE.
The following parameters are used to mirror communication received from the GE CARESCAPE Network. Select which traffic that will be mirrored. The Service parameters can be used for troubleshooting purposes. Note that the performance will be affected when enabled, so be sure to disable when the troubleshooting is finished.	
Mirror CARESCAPE traffic:	Select between Disabled, Alarms, RWhat or “Alarms+RWhat”
Mirror IP port	The MMG port used to mirror communication received from the GE CARESCAPE Network. All received packets will be sent to this port. For best result, an application on the configured IP address will be configured to receive UDP traffic on the

5.2.22 Units and Filters

NOTE: Some filters are configured by default (factory settings). If any filter is removed, it might increase the messaging load in the system due to a high amount of alarms will pass the MMG filters.

The Units/Filters page links to other pages for settings.

1. In the MMG start page, click **Configuration**.
2. Click Advanced.
3. In the left menu, click **Basic Administration**.
4. Click “GE CARESCAPE” in the menu.
5. Click the “Units/Filter” link on the GE CARESCAPE page.



a) Filters that will be used for all units.
b) Additional filters that will be used for a certain unit only.

For filter settings, see:

- Alarm Text Group Filters
- Alarm level translation table
- Alarm text delay filters

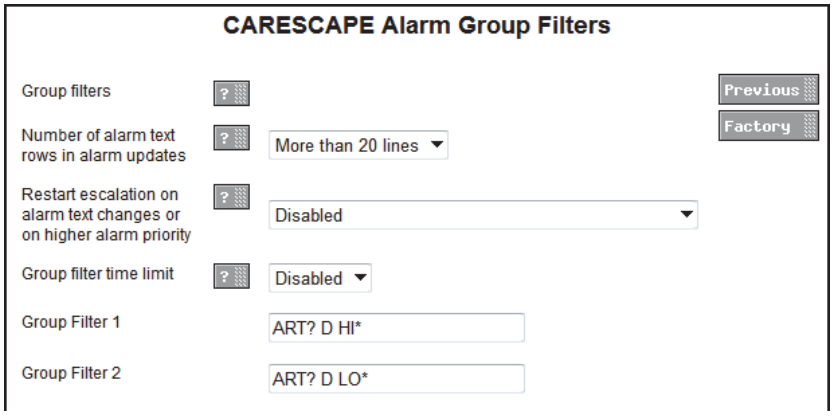
See also Appendix C for a detailed description.

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 will be considered to be the same alarm. The advantage with group filters is that no additional alarm messages will be sent to a device when the alarm is considered to the same. This decreases the messaging load to a device

Figure 18. The Alarm Text Group Filters page.



The following parameters can be set:

Parameter	Description
Group Filter 1 - 100	Determines which alarm updates that are considered to be the same as previously received alarms. Alarm updates with texts that match an active group filter will be considered as an unchanged alarm and will be discarded by the MMG. The group filter must match the complete alarm text and is case sensitive. If the alarm text does not match an active group filter, or the alarm priority is changed, the alarm update will pass the MMG. The majority of these filters have been given default values.
Number of alarm text rows in alarm updates	Determines the maximum number of alarm text rows, that were included in previously sent alarms, to also be shown in the latest alarm update sent to the handset.

Restart escalation on alarm text changes or on higher alarm priority	By default, when a user on another level than Level 1 acknowledge an alarm, any additional alarms will be sent to this user directly. By enabling this parameter, the user on Level 1 will get the possibility to receive alarms once again. The parameter determines if the escalation chain should restart from the beginning when one of the following occurs: • The alarm update is not considered to be the same as previous alarm due to it matches another group filter. That is, the alarm text in the alarm update has been changed. • The priority of the alarm update is higher than previous alarm. See also Apendix C, C.1 Example of Group Filter Configuration for more information.
Group filter time limit:	Determines for how long time an active group filter will block an alarm update considered to be the same as the initial alarm. The group filter becomes active when it matches an alarm. Possible values: • Disabled (a matching filter will always block alarm updates) • 60, 75 or 90 seconds (a matching filter will only block alarm updates for a preset time) If the filter is not disabled and an alarm passes the MMG, the time starts and the group filter becomes active. When the time elapsed, any alarm updates will pass even though they match this group filter. Each time an alarm update passes a group filter, the time will start from the beginning. For example; the time for Group filter 1 has been started. An alarm update matches Group Filter 2 and the alarm update passes the MMG. Now, the time for Group Filter 1 is stopped and the time for Group Filter 2 is started. This means that only one filter can be active at the time. Use this parameter to letting through some alarm updates in intervals to handsets, even though the alarm update is considered to be the same as previous alarm. NOTE: If this parameter is used, it may increase the messaging load in the system due to additional alarm updates that will sent to the handsets.
Group filter time limit:	Determines for how long time an active group filter will block an alarm update considered to be the same as the initial alarm. The group filter becomes active when it matches an alarm. Possible values: • Disabled (a matching filter will always block alarm updates) • 60, 75 or 90 seconds (a matching filter will only block alarm updates for a preset time) If the filter is not disabled and an alarm passes the MMG, the time starts and the group filter becomes active. When the time elapsed, any alarm updates will pass even though they match this group filter. Each

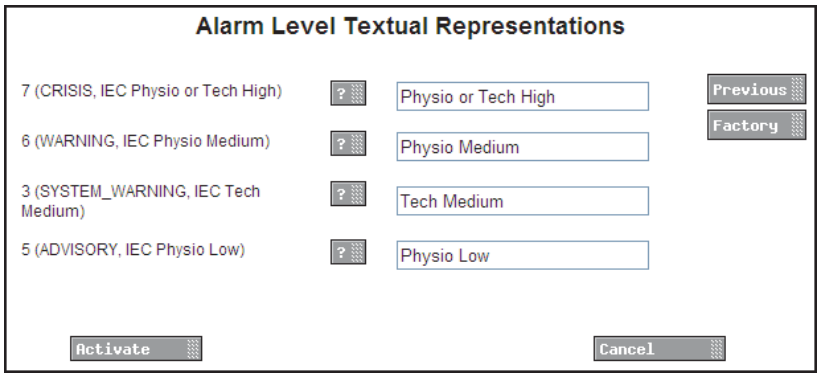
	time an alarm update passes a group filter, the time will start from the beginning. For example; the time for Group filter 1 has been started. An alarm update matches Group Filter 2 and the alarm update passes the MMG. Now, the time for Group Filter 1 is stopped and the time for Group Filter 2 is started. This means that only one filter can be active at the time. Use this parameter to letting through some alarm updates in intervals to handsets, even though the alarm update is considered to be the same as previous alarm.
	NOTE: If this parameter is used, it may increase the messaging load in the system due to additional alarm updates that will sent to the handsets.
Group filter time limit:	Determines for how long time an active group filter will block an alarm update considered to be the same as the initial alarm. The group filter becomes active when it matches an alarm. Possible values: • Disabled (a matching filter will always block alarm updates) • 60, 75 or 90 seconds (a matching filter will only block alarm updates for a preset time) If the filter is not disabled and an alarm passes the MMG, the time starts and the group filter becomes active. When the time elapsed, any alarm updates will pass even though they match this group filter. Each time an alarm update passes a group filter, the time will start from the beginning. For example; the time for Group filter 1 has been started. An alarm update matches Group Filter 2 and the alarm update passes the MMG. Now, the time for Group Filter 1 is stopped and the time for Group Filter 2 is started. This means that only one filter can be active at the time. Use this parameter to letting through some alarm updates in intervals to handsets, even though the alarm update is considered to be the same as previous alarm.
	NOTE: If this parameter is used, it may increase the messaging load in the system due to additional alarm updates that will sent to the handsets.
Group filter time limit:	Determines for how long time an active group filter will block an alarm update considered to be the same as the initial alarm. The group filter becomes active when it matches an alarm. Possible values: • Disabled (a matching filter will always block alarm updates) • 60, 75 or 90 seconds (a matching filter will only block alarm updates for a preset time) If the filter is not disabled and an alarm passes the MMG, the time starts and the group filter becomes active. When the time elapsed, any alarm

	updates will pass even though they match this group filter. Each time an alarm update passes a group filter, the time will start from the beginning. For example; the time for Group filter 1 has been started. An alarm update matches Group Filter 2 and the alarm update passes the MMG. Now, the time for Group Filter 1 is stopped and the time for Group Filter 2 is started. This means that only one filter can be active at the time. Use this parameter to letting through some alarm updates in intervals to handsets, even though the alarm update is considered to be the same as previous alarm.
	NOTE: If this parameter is used, it may increase the messaging load in the system due to additional alarm updates that will sent to the handsets.

Alarm Level Translation Table

The settings in this page translates CARESCAPE alarm levels to readable text, for example, if a CARESCAPE alarm level 6 occurs, the text in a message will be “Physio Medium” (default)

Figure 19. The Alarm Level Textual Representations page.



The following alarm levels can be given textual representations:

- 7 (CRISIS, IEC Physio or Tech High) Default value: “Physio or Tech High.”
- 6 (WARNING, IEC Physio Medium) Default value: “Physio Medium.”
- 3 (SYSTEM_WARNING, IEC Tech Medium) Default value: “Tech Medium.”
- 5 (ADVISORY, IEC Physio Low) Default value: “Physio Low.”

Alarm Text Stop Filters

For Alarm Text Stop filters, all alarms with alarm text matching any of the filters will be discarded and no alerts will be sent out.

Figure 20. The Alarm Text Stop Filters page.

- Stop Filter 1 - 10:

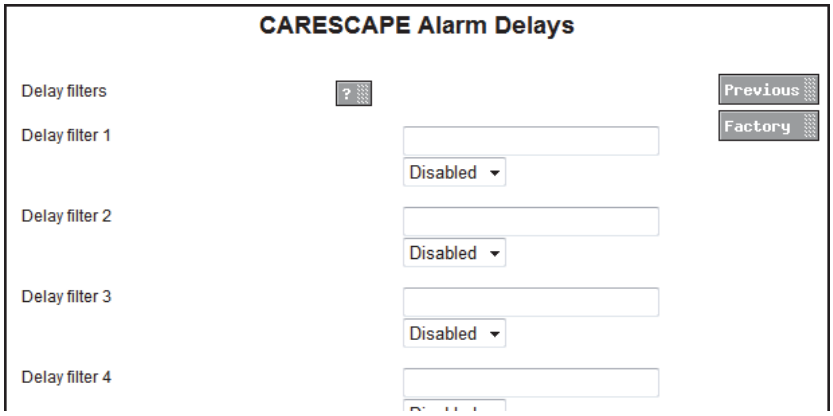
Enter stop filter settings.

There are 10 stop filters. See Appendix C for details.

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 will be sent out.

Figure 21. The CARESCAPE Alarm Delays page.



- Delay filter 1 - 10: Set filter value.

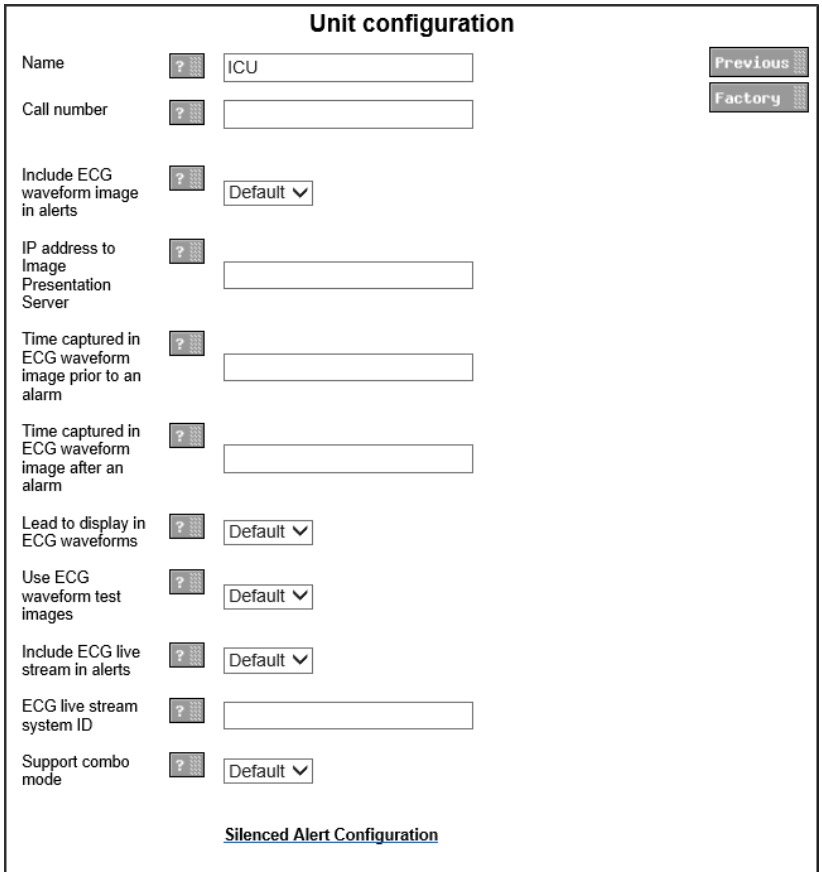
Select delay time or Disabled.

There are 10 delay filters. See Appendix C for details.

Unit Configuration

This page is used to configure settings specific for a certain unit or department.

Figure 22. The Unit configuration page



Parameter	Description
Name	Name of the unit/department. This name must match the unit name in the received alarm (location field).
Call number	The call number used for the call option available in the Interactive Messages (IMs) that are sent out. The staff that handles the IM may have an option to call for help using a single button press. This is the number that will be called for alarms originating from monitors belonging to this unit.
Include ECG waveform image in alerts	Select if the MMG requests an ECG waveform image from the image presentation server to be included in an alert message.
	NOTE: The Interactive Message property Include image must also be set in order to include the image in the alert. See 8.1.3 Defining Actions.
	Set **Default if this Unit** uses the corresponding setting on the global level instead, see 5.2.21 GE CARESCAPE.
IP address to image presentation server	The IP address to the image presentation server that will provide ECG waveform images when requested by the MMG. The default port is 8000, for example 10.30.1.2:8000.

Time captured in ECG waveform image prior to an alarm	The GE CARESCAPE equipment sends a continuous stream of ECG waveform data to the image presentation server connected to the MMG. When an alarm is triggered, the MMG will request a snapshot of the ECG waveform data to create an ECG waveform image. Use this parameter to determine the number of seconds of ECG waveform data to be captured prior to the alarm. Value (seconds): 1 - 10
	NOTE: The number of seconds of ECG waveform data to be captured after the alarm should be together up to 12 seconds.
Time captured in ECG waveform image after an alarm	The GE CARESCAPE equipment sends a continuous stream of ECG waveform data to the image presentation server connected to the MMG. When an alarm is triggered, the MMG will request a snapshot of the ECG waveform data to create an ECG waveform image. Use this parameter to determine the number of seconds of ECG waveform data to be captured after the alarm. Value (seconds): 1 - 10
	NOTE: The number of seconds of ECG waveform data to be captured prior to the alarm is also required, see Time captured in ECG waveform image prior to an alarm. The ECG waveform data captured prior and after the alarm should be together up to 12 seconds.
Lead to display in ECG waveforms	In electrocardiography, lead refers to the difference in voltage between electrodes on different parts of the body. The system supports sending one of three different leads: • Lead I is the voltage between the right arm electrode and the left arm electrode. • Lead II is the voltage between the right limb and the feet. • Lead III is the voltage between the left leg and the left arm. Set Default if this Unit uses the corresponding setting on the global level instead, see 5.2.21 GE CARESCAPE.
Use ECG waveform test images:	Determines if an image presentation server connected to the MMG will provide a fictitious ECG waveform image, instead of retrieving ECG waveform data from a GE CARESCAPE monitor.
	IMPORTANT:: This parameter will only be set to YES for test purposes. C parameter is set to NO. If not, this may lead to hospital pe in critical situations.
	Set Default if this Unit uses the corresponding setting on the global level instead, see 5.2.21 GE CARESCAPE.

Include ECG live stream in alerts	Select an option for viewing ECG waveforms in real time (i.e. live stream) should be included in the alerts. **Set Default if this Unit** uses the corresponding setting on the global level instead, see 5.2.21 GE CARESCAPE.
	NOTE: The “ECG live stream system ID” parameter must also be set. Additionally, live stream is only supported by smart devices with an Airstrip ONE® application installed
ECG live stream system ID	If live stream of ECG waveforms should be used, enter the unique system ID required to log in to the smart device application used for viewing ECG waveforms in real time. The system ID is unique for each installation. Consult the system administrator to obtain the correct system ID **Set Default if this Unit** uses the corresponding setting on the global level instead, see 5.2.21 GE CARESCAPE.
Support combo mode	Select if both a fixed patient monitor and a telemetry monitor should be treated as the same location. To distinguish which monitor that triggered the alarm, the location in the alert is shown as follows: Fixed patient monitor: <Unit>|<Bed> (e.g. ICU|BED1) Telemetry monitor: <Unit>|<Bed*> (e.g. ICU|BED1*) **Set Default if this Unit** uses the corresponding setting on the global level instead, see 5.2.21 GE CARESCAPE
Silence Alert Configuration	Settings related to the behavior alerts associated with silenced alarms, see Silence Alert Configuration.
Stop filters 1-10	Enter stop filter settings as in Alarm Text Stop Filters. These are additional stop filters that are valid only for this unit.
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.
Group filters 1-100	For Group filters, all alarm texts that match the same group filter will be considered to be the same alarm (that is, they will not cause an update).

A filter must match the complete text string. Wildcard characters may be used. The supported wildcard characters are listed in the table below.

Wildcard Characters	**Meaning**	**Example**
;	Disables the filter if in the first position	;6HR*
?	Equals any one character	HR ?O 10 matches all of: HR LO 10 HR JO 10 but not HR O 10

*	Equals zero or more characters	HR *O 10 matches all of: HR LO 10 HR JO 10 HR O 10
|	Means "or"	HR LO ?|HR LO ?? matches both of HR LO 9 HR LO 10

There are 10 stop filters and 10 delay filters that can be set for each of the 25 units that can be configured in MMG.

Silence Alert Configuration

WARNING: This product provides methods to temporally suppress alerting and redirection for the duration of a silenced alarm and (optionally) for the duration of all active alarms after silenced on the patient monitor.

Failure to take into account operation of the silence feature of the monitor by unqualified or un-trained personal may lead to improper delays and/or suppression of notifications leading to potential patient harm.

By utilizing the silence feature of the Patient Monitor it is possible to suppress alerting & temporarily discontinue redirection of alerts distributed by the MMG. This capability is not available as part of the default configuration, and requires additional configuration per unit.

The capabilities of the feature are managed via the parameters defined in the remainder of this section. It is important to understand the purpose and interaction of each of these parameters in order to safely and properly configure the available feature.

When configured properly this feature provides a means by which alerts may be temporarily paused during the time that the patient monitor is silenced. Upon expiration of silence on the monitor, or the generation of a new alarm, alerting provided by the MMG will resume. Optionally the product can be configured to persistently pause redirection and alerting for the duration of all active alarms, after silence has been engaged by the monitor.

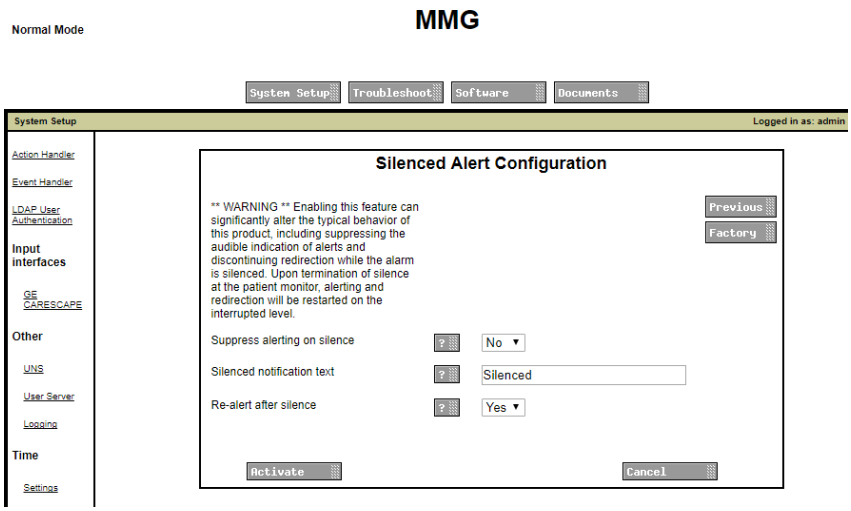
After the silence on the patient monitor has expired (or a new unsilenced alarm condition occurs), when **Suppress Alerting on Silence** is enabled, and **Re-alert after silenced** is enabled, alerting will restarts at same redirection level it was at when initially silenced.

Alternatively after silence on the patient monitor has expired, when **Suppress Alerting on Silence** is enabled, and **Re-alert after silenced** is disabled, alerting will NOT restart until all alarms are inactive on the monitor.

Recipients of alerts which are silenced will receive notification that an alarm has been silenced (configurable) and include options for Assistance and dismissal (Close). Similar to what would be provided if responsibility for the Alert were to have be accepted.

The description accompanying silenced alerts can be configured by modifying the content of the setting **Silenced notification text**, and is provided as part of the content delivered in updates to display devices.

The Silenced Alert Configuration is accessible and configurable at the Unit level filter configuration of the product.

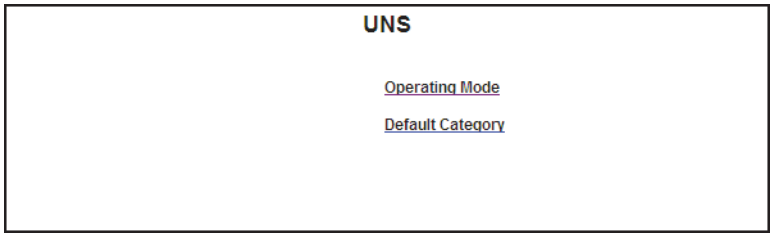


Parameter	Description
Suppress Alerting on Silence	Setting this option to **Yes**, will suppress audible alerting and redirection when an alarm is silenced at the monitor. The default setting for all units is “off” or disabled.
Silenced Notification Text	The text defined here will be indicated in the Subject line (default) for all alerting suppressed by silence if the Suppress Alerting on Silence option is enabled.
Re-alert after silence	Setting this option to **Yes** allows indication and redirection to resume when silence for active alarm expires on the monitor (default). Setting this option to **No** will prevent indication and redirection to resume when silence expires for an active alarm.

UNS

The UNS is used to resolve addresses into complete destinations. MMG will be configured to forward all requests to a centralized UNS (forwarding mode).

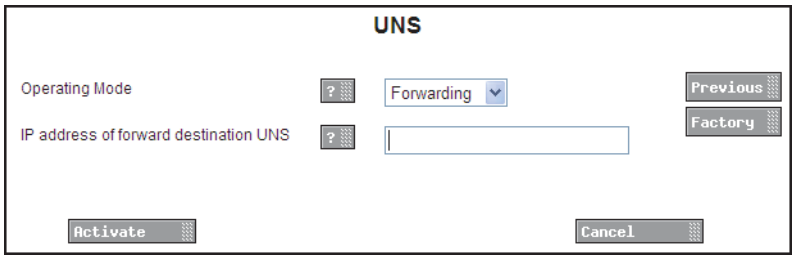
1. In the MMG start page, click **Configuration**.
2. Click Advanced.
3. Click **Basic Administration** in the menu on the Configuration page.
4. Click **UNS** under Other on the Advanced Configuration page.



Operating Mode

Operating mode will be changed to forward messages to a Unite Connectivity Manager (Unite CM).

1. Click “Operating mode.”

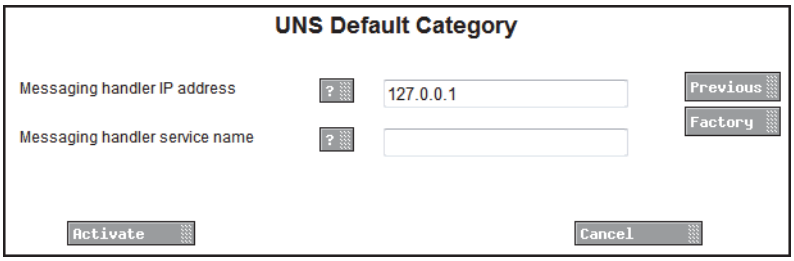


2. Set operating mode to Forwarding and enter the Unite CM’s IP address.
3. Click Activate.

Default Category

You can set a UNS default category as a fallback, i.e. if for some reason forwarding to the Unite CM should fail, all requests are forwarded to the messaging interface specified here.

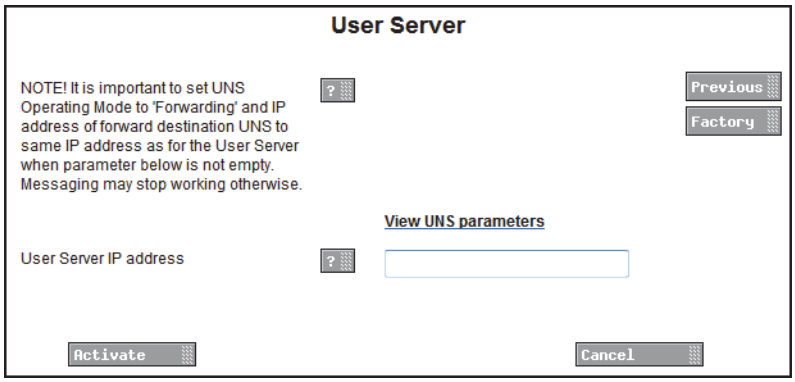
1. Click Default Category.
2. Enter values for Messaging handler IP address and Messaging handler service name.
3. Click Activate.



User Server

To use the defined users in a Unite CM, the user server IP address is set to the Unite Connectivity Manager that is set up as a user server.

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



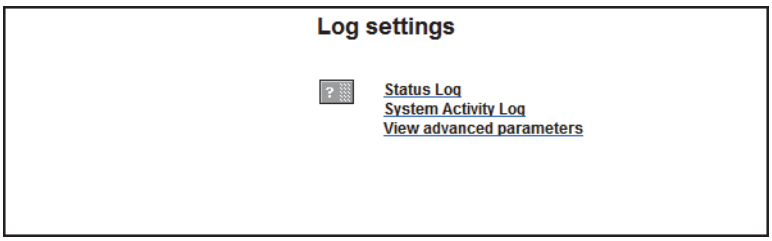
2. Enter the IP address of the User Server (e.g Unite CM).
3. Click **Activate** to save the settings.

Logging

The Status Log can store faults and the System Activity Log can store activities such as messages, alarms, faults, input/output activities, etc. which is useful for troubleshooting. To store and view logs, a Unite CM is needed since MMG has no functionality to receive and show log messages.

To enter the log settings page:

1. In the MMG start page, click **Configuration**.
2. Click **Advanced** tab.
3. Click Basic Administration.
4. Under Other, click **Logging**.



5. To set destinations for the logs:
6. Click Status Log or System Activity Log.
7. For Status Log enter xxx.xxx.xxx.xxx/FaultHandler, and for System Activity log enter xxx.xxx.xxx.xxx/ActivityLogger.
8. Click **Activate**. The module will from now on send all status log/activity log messages to the Unite CM.

NOTE: The Unite CM can be configured to perform a fault action if it receives a Status log from the MMG. A fault action can, for example, be an e-mail or a message sent to an IT responsible. See Appendix G. Supervision of GE CARESCAPE Network and MMG for more information.

Viewing Advanced Parameters

To configure advanced parameters:

In the Log settings page, click “View advanced parameters.” To configure the parameter “Error Relay Time for Status Log Failure” go to “Extended Activity Log” parameter is configured.

- **Error Relay Time for Status Log Failure**

If it is not possible to generate or send Status Logs on errors, the error relay will be 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.

The time for how long the relay will be released can be defined by clicking “View advanced parameters.” The time is defined in seconds between 0 and 900, where 0 means that the error relay will not be released at all.

- **Extended Activity Log**

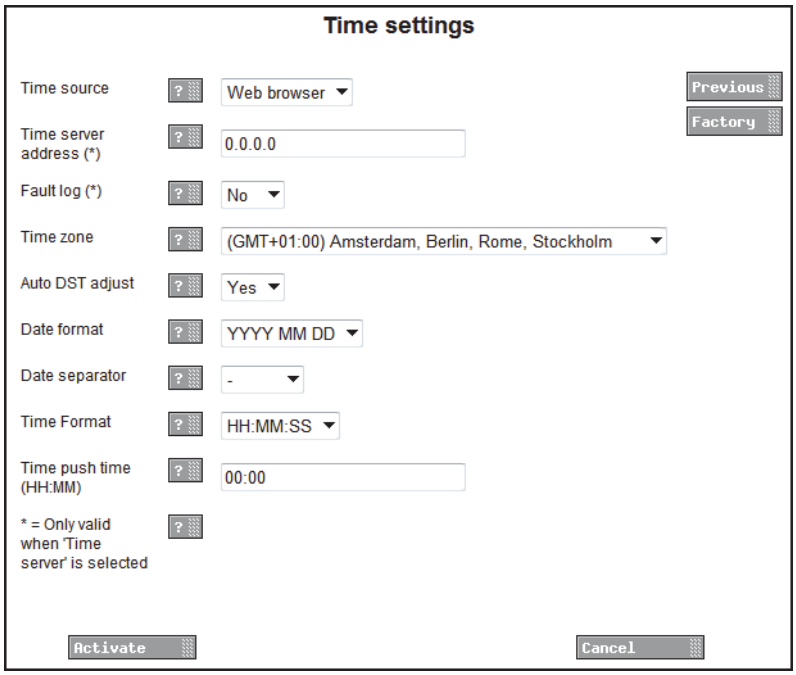
On the same page as the time setting for the error relay is a link to the Extended Activity Log. When enabled, intermediate activity logs will be sent while a message passes through the system towards the handset. The extra information will not be saved to the log file, but only displayed in Log Viewers that are updated continuously.

Use this function with care as it generates more traffic in the system.

- **Time Settings**

You can select where to fetch the time from, such as the local clock (set from a web browser) or a time server. The following parameters can be set via the Basic Administration page.

1. Click **Configuration** on the start page.
2. Click Advanced.



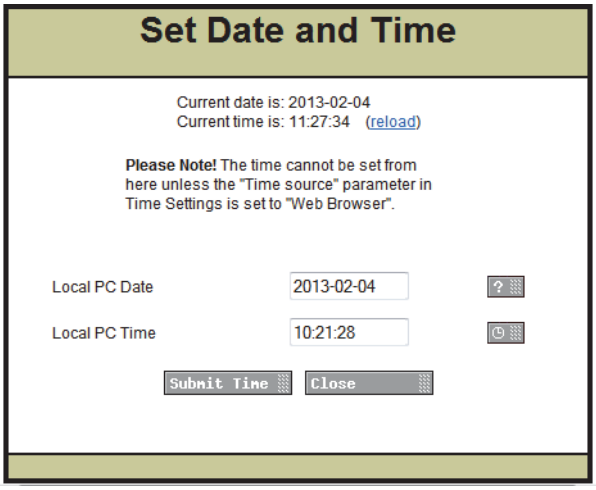
3. In the left menu, click **Basic Administration**.
4. Under Time, click **Settings**.
5. Enter time settings.
6. For Time source, Time server (via NTP) is recommended.
7. Click Activate.

Setting Times

If Web browser has been selected as time source, the time must be set manually. Otherwise this setting will not be done.

1. In the left menu, under Time, click **Set time**.

2. Enter date and time. Click **Submit time**.

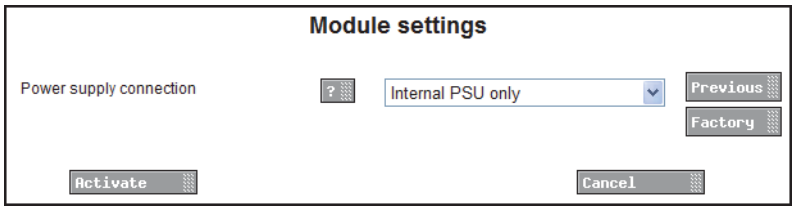


Setting Power Supply Connection

There are four power supply choices for the Elise3 hardware:

- Internal PSU only
- External PSU only
- Internal and external PSU
- Internal PSU and external battery

1. Click **Configuration** on the start page.
2. Click Advanced.
3. In the left menu, click **Basic Administration**.
4. Under Common, click **Power supply**.



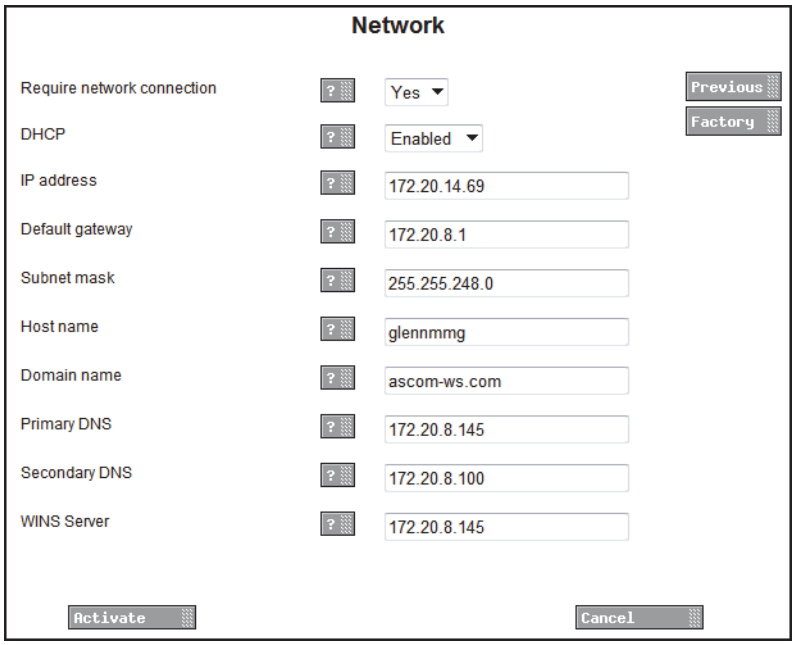
5. Select power supply connection in the drop-down list.
6. Click Activate.

If there is a mismatch between the physical power supply configuration and the power supply connection setting, the power LED will slowly flash red. For example, the power LED will flash red slowly if the Elise 3 hardware has an internal power supply only, and the setting is "Internal and external PSU."

Network Settings

1. In the MMG start page, click **Configuration**.
2. Click Advanced.
3. In the left menu, click **Basic Administration**.
4. Under *Common*, click “Network (LAN1).”

5. Enter IP settings.



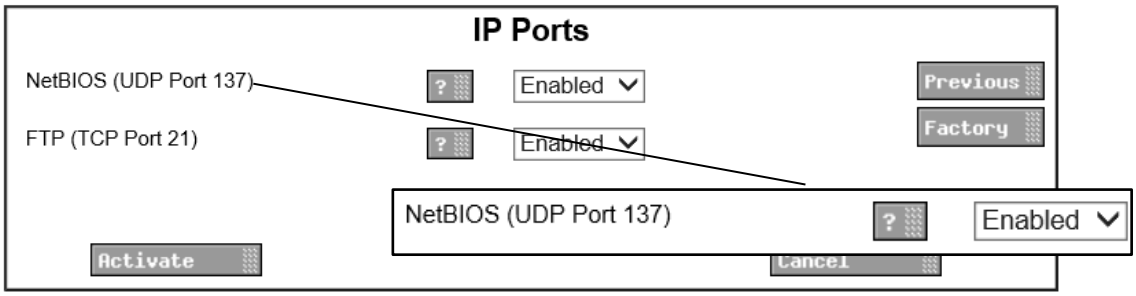
5.2.23 Security

NetBIOS Port

You can determine if the NetBIOS port (UDP 137) shall be open or closed. The NetBIOS makes it possible to access the Unite module with the NetBIOS name “elise-XXXXXXXX”, where XXXXXXXX is the module key number. If the port is closed, only the Unite module’s IP address can be used to access the Unite module.

The NetBIOS port is enabled by default.

1 Click “Configuration” on the start page.
2 Select Other Settings > Advanced Configuration.
3 Select “IP Ports” under Security on the Advanced Configuration page.
4 Select if the port should be closed (disabled) or open (enabled) in the NetBIOS (UDP Port 137) drop-down list.



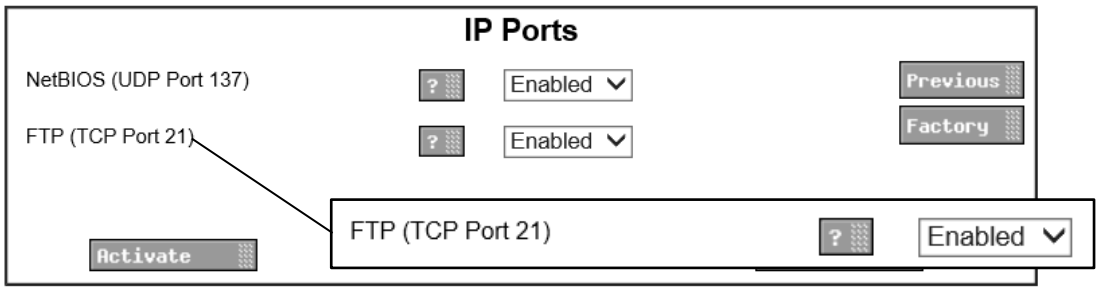
5 Click “Activate.”

FTP Port

You can determine if it should be possible to access the FTP area or not. The FTP area can only be accessed when the FTP port is open.

1. Click **Configuration** on the start page.
2. Select Other Settings > Advanced Configuration.
3. Select “IP Ports” under Security in the menu on the Advanced Configuration page.

4. Select if the FTP port will be open (enabled) or not (disabled) in the *FTP (TCP Port 21)* drop-down list.



5. Click Activate.

5.2.24 License Activation

Enter the license number via the Basic Administration page.

1. In the MMG start page, click **Configuration**.
2. Click Advanced.
3. In the left menu, click **Basic Administration**.
4. Under Common, click **License**.
5. Enter license number stated on the License certificate as follows:

– In the License 1 field, enter the License Code 1 key

– In the License 2 field, enter the License Code 2 key (if any)

NOTE: The other fields are currently not used.

6. Click Activate.

5.2.25 Rebooting MMG

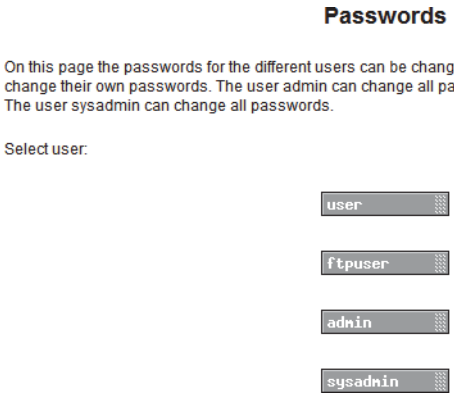
You can reboot the MMG via the Basic Administration page.

1. In the MMG start page, click “Configuration.”
2. Click “Advanced.”

3. In the left menu, click “Basic Administration.”
4. Under Common, click “Reboot.”
5. To reboot the MMG, click the “Reboot” button.

When the reboot is complete and the system is operational, the Status LED changes to a blue steady light.

5.2.26 Setting passwords



You can set passwords for the different users via the Basic Administration page.

1. Click **Configuration** on the start page.
2. Click Advanced.
3. In the left menu, click **Basic Administration**.
4. Under Common, click **Passwords**.
5. Click the user to change password.
6. Enter your user name and password (leave empty if you not have any password). Enter the new password and confirm the password.
7. Click Ch. Passwd..

6 Integration with Alert Management

This section deals with the configuration settings needed to set up MMG in an integrated Alert Management system.

For details, see 5 Configuration.

6.1 Integration Steps

Entering the MMG GUI

1. Power on the MMG module.
2. In a browser, enter **http://elise-nnnn/admin**, where *nnnnn* is the module key number found on the enclosed license certificate (starting zeros can be excluded). The MMG System Setup page appears.

Setting a License

1. Under Common, click **License**.
2. In the License number text field, enter the license number for MMG.
3. Click Activate.

NOTE: The GUI prompts you to reboot the MMG to activate the changes. Do not reboot the MMG in this case.

---

1. Network Settings
2. Click “Network (LAN1)” under Common.
3. Set IP settings for MMG.
4. Click Activate.

Time Settings

1. Click **Settings** under Time.
2. Select Time source (recommended: Time server).

Enter the IP address for the Time server (recommended: Unite Connectivity Manager or other NTP source). It is strongly recommended to use the same time source for Unite Connectivity Manager and MMG either directly (pointing at the same server) or indirectly (by configuring MMG to use the Unite Connectivity Manager as time source).

Enter or select Time zone, daylight saving adjustment (DST), Date format and Time format.

3. Click Activate.
4. Click Set time under Time.
5. If the computer’s local time can be used, click Submit time.

Rebooting MMG

1. Under Common, click **Reboot**.

Message Routing Settings

1. Under “Othe,r” click **UNS**.
2. Click Operating Mode.
3. Enter the IP address for the Unite CM to be used as number plan (UNS) in the text field.

4. Click Activate.
5. Under Other, click **User Server**.
6. Enter the IP address of the Unite CM to be used as number plan in the text field.
7. Click Activate.

Logging Settings

1. Under Other, click **Logging**.
2. Click Status Log.
3. Enter destination to <Unite Connectivity Manager IP address>/Faulthandler.
4. Click **Logging**.
5. Click System Activity Log.
6. Enter destination to <Unite Connectivity Manager IP address>/ActivityLogger.

NOTE: The Unite CM can be configured to perform a fault action if it receives a Status log from the MMG. A fault action can, for example, be an e-mail or a message sent to an IT responsible. See Appendix G. Supervision of GE CARESCAPE Network and MMG on for more information.

CARESCAPE Settings

Set the configuration settings for CARESCAPE. A detailed description of filters is found in 0

Units and Filters.

1. To set the CARESCAPE message configuration, click **GE CARESCAPE**. The GE CARESCAPE page appears.
2. Enter and select settings for time to inactive alarm, inactivation priority, notify about audio level, silenced text and time stamp of alarms.
3. Click **Activate**.

Setting Alarm Text Group Filters

1. In the GE CARESCAPE page, click **Units/Filters**. Click **Alarm Text Group Filters**.
2. In the Alarm Text Group Filters page, enter Group Filters. Click **Activate**.

Setting Alarm Text Stop Filters

1. In the GE CARESCAPE page, click **Units/Filters**.
2. Click Alarm Text Stop Filters.
3. In the Alarm Text Stop Filters page, enter the stop filters.
4. Click **Activate**.

Setting Alarm Text Delay Filters

1. In the GE CARESCAPE page, click “Units/Filters.” Click **Alarm Text Delay Filters**
2. In the CARESCAPE Alarm Delays page, enter Delay Filters and select a delay time. Click **Activate**.

Setting the Alarm Level Translation Table

1. In the GE CARESCAPE page, click **Units/Filters**.
2. Click Alarm Level Translation Table.
3. In the Alarm Level Textual Representations page, enter texts to be displayed for the different alarm levels.
4. Click Activate.

Loading Templates

1. In the MMG start page, click **Configuration**.
2. In the Basic tab, click **Select Template**.
3. Click a button to select the template. The template is loaded.

For customer requirements, see 6.2 Common Modifications. Check that MMG is configured according to customer requirements including setup of Duty Assignment.

6.2 Common Modifications

Some common modifications of the template are listed here. These modifications are usually made by an Ascom engineer.

- Text changes
- Change of escalation time
- Adaptation of template

Text Changes

You can change the texts in messages sent from CARESCAPE via MMG to handsets or text displays. This is done using event elements.

1. In the MMG start page, click **Configuration**.
2. In the Basic tab, click **Basic Setup**.
3. Click Action Configuration.
4. Login with your user ID and password.

5. In the Action Configuration page, select the event to change text.
6. Click Define Action. The Action window appears.
7. Select action to change text for. Click Edit. The Define Interactive Message window opens.
8. Note that two actions need to be updated. This is for example the case for “Monitor alarm notification” and “Monitor alarm update notification,” since the latter action is an update of the first action.
9. In the Body field, enter text or right-click and click Insert event Element.
10. Select event element and click Add.
11. Example with a row with a text and an event element: “Date: <!Date>.”
12. Click OK.
13. Click Close.

Changing Escalation Time

You can change which escalation time to use when an alert is not accepted before it is escalated to the next level of recipients. This change has to be done for all escalation levels in the Action Tree. It is recommended to use the same value for all levels.

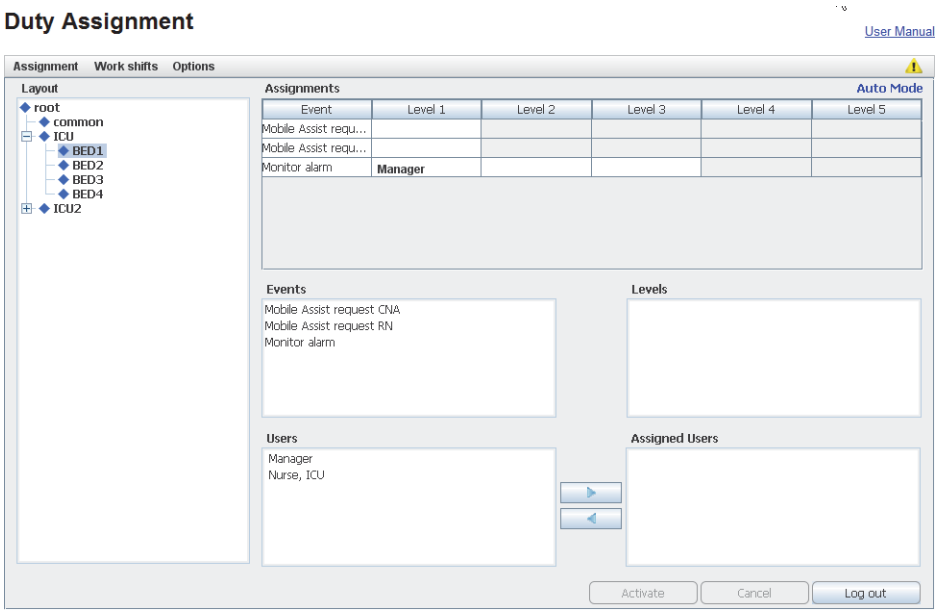
To change escalation time:

1. In the MMG start page, click **Configuration**.
2. In the Basic tab, click **Basic Setup**.
3. Click Action Configuration.
4. Login with your user ID and password.

5. Select a monitor alarm, click Edit. The event Configuration window opens.
6. In the Action Tree, for each level, select Monitor alarm (failed). Click Conditions.
7. In the Conditions dialog window, change Failure Timeout to the new escalation time.

Adaptation of Selected Templates

This is normally done at first time setup. After setup it is maintained by a nurse on a daily basis. To change unit conditions:



1. In the MMG start page, click Duty Assignment.
2. Click Options > Layout Setup.
3. In the Layout Setup page, under ICU, select BED1.
4. Click Define Conditions. The Define Condition window opens.
5. If necessary, change, for example the name of the bed.
6. Click Done.
7. Click Save.

Setting up Recipients

This section describes how to set up recipients to be selectable as soft keys in a handset display or as automatic recipient of certain alarms.

The following recipients are handled:

- Assist: generates an event to ask for assistance
- Call: calls a predefined number
- Technical Monitor Alarm, which is not selectable as a soft key. All technical alarms are automatically sent to this call ID.

To change the “Assist” soft key settings:

1. In the MMG start page, click **Configuration**.
2. In the Basic tab, click **Basic Setup**.
3. Click Duty Assignment.
4. In the Duty Assignment window, select the location for which you want to change the settings.
5. Set which users to be assigned for Assistance request for the different levels.

To change the “Call” soft key settings:

1. In the MMG start page, click **Configuration**.
2. In the Basic tab, click **Basic Setup**.
3. Click Action Configuration.
4. In the Action Configuration window, click **Define Action**.
5. In the Action window, select “Monitor Alarm Notification” and click **Edit**.
6. In the Define Interactive Message window, click Options, then select ID number 5 and click **Edit**.
7. In the Define Option window, do the necessary changes.
8. Click **OK** twice and **Close**.

NOTE: To change the “Technical Monitor Alarm”1 recipient settings:

1. In the MMG start page, click **Configuration**.
2. Click Action Configuration. The Action Configuration window opens.
3. In the Action Configuration window, select “Technical Monitor Alarm”[1] and click **Edit**.
4. In the event Configuration window, in the Action Tree, select “Technical alarm notification” and click **Edit**.
5. In the event Configuration Actions window, in Addressing, select the type User, select a Name and click **Add**.
6. Click **OK** twice.

You can remove any alternative from the handset display by deleting the option in the interactive message.

[1]Technical Monitor Alarm: all alarms with alarm level 3 are delivered to the user who's address is defined here.

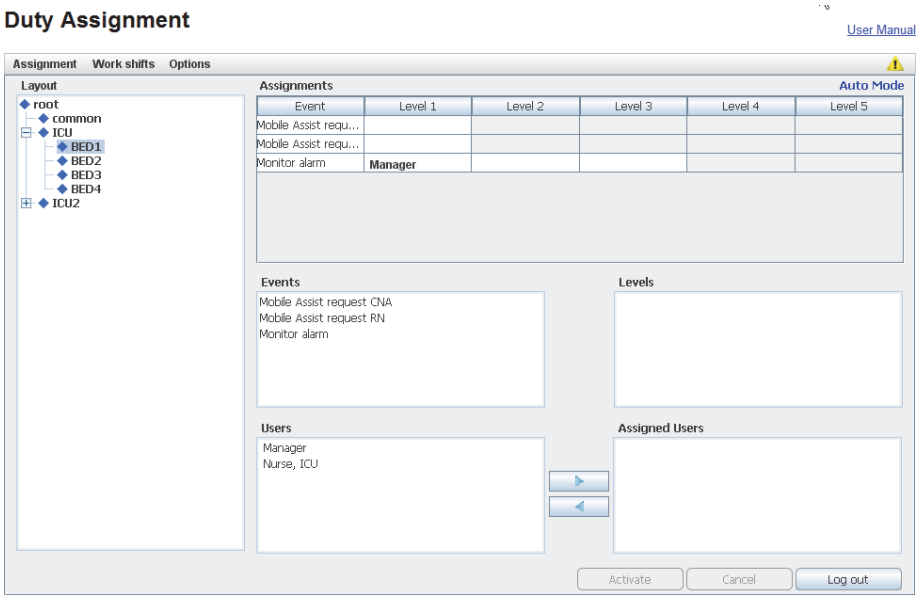
7 Operation

The Duty Assignment pages can be reached from the MMG start page.

Figure 23. The Duty Assignment Icon in the MMG Start Page.

The operation of Duty Assignment is described in MMG Duty Assignment User Manual TD 92691GB. It is operated on a daily basis by a nurse.

Figure 24. The Duty Assignment Page.



8 Administration

This chapter is intended for local administrators. It is a general description on how to work with action configuration and will assist in understanding how to work with and adapt the included templates.

An overview picture of how events and alarms are handled in MMG is shown in Appendix B. MMG Overview Picture.

If event elements are already defined, the normal workflow is described in this section. The list below is an overview of the administration tasks described in this chapter.

Setting up Actions in Action Configuration

- Configure events
    - Define actions for the event configure a message for the action
    - Configure options (for a message/interactive message/output activity) configure addressing for the action
    - Add success/failure conditions for the action
    - Add delivery and status response conditions for success/failure conditions add response conditions
    - Synchronize configured events
    - Edit an event
    - Delete an event
    - Action termination/updates
    - Add termination event names
    - Set termination actions
    - Delete an action termination
- Add event assignments
- Layout setup
    - Locations
    - Conditions
    - Assign events and users
- Set up access rights

8.1 Action Configuration

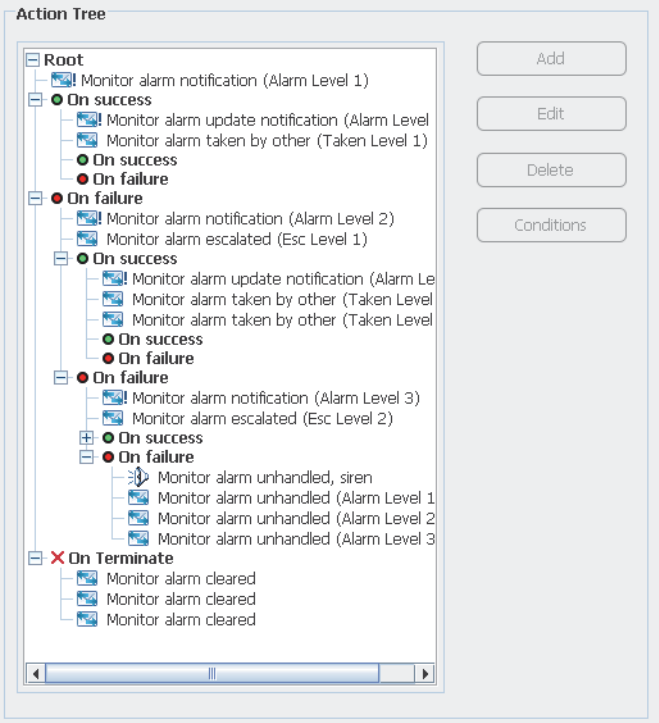
NOTE: If one of the included templates is used, there is normally no need to set up actions.

8.1.1 The Action Tree

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

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

Figure 25. The Action Tree for Monitor Alarm in the Ascom Standard Template.



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

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

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

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

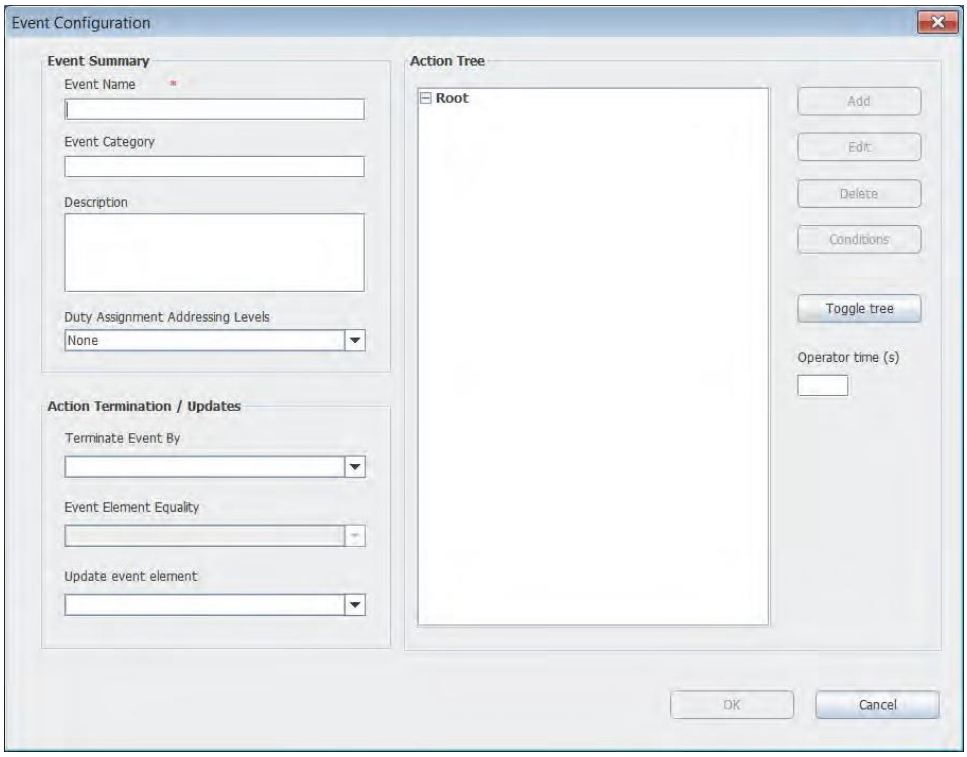
8.1.2 Event Configuration

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

1. In the MMG start page, click **Configuration**.

2. Click Action Configuration.
3. Log in with your user ID and password.

4. Click **Add**.
5. Enter a name of the event and a description.

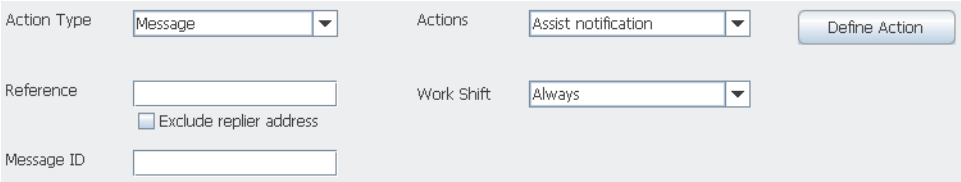


6. Optionally, enter a category for the event. The category will be set for all actions within this event and is a help in the search and sorting function for system activity logs.
7. Optionally, select event type for the Event. The event type tells which kind of event it is (e.g. Patient call or Emergency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

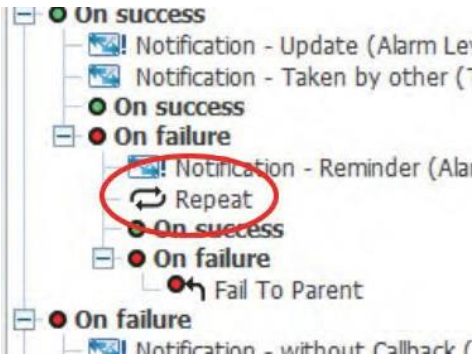
8. Optionally, select a color for the Event. The color will be shown in the supporting display device (Myco) that receives the alert about the Event. This can, for example, be used to visualize the type of the event by color.
9. Select from the drop-down list duty assignment addressing levels, if duty assignment is to be used. The levels are:

- None: Events will not be visible in the Duty Assignment.
- 1-5: up to five addressing levels can be selected.

10. Mark Root in the Action Tree and click **Add** to configure actions for an event.
11. Select an **Action Type** from the drop-down list:



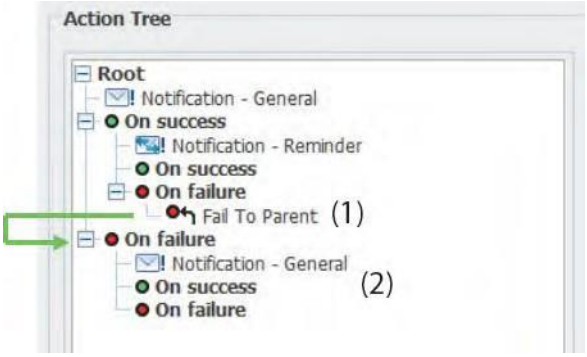
Action Type	Description
Message	To send messages to a specific destination and with a confirmation request.
Interactive Message	To send messages with different response options included. The response is sent back with chosen option.
Output Activity	To set or reset an output, for example to remotely turn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



Fail to Parent:

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

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



12. Select **Actions** from the drop-down list. If it says “No Items” in the drop-down list, click Define Action to add items to the action list. See 8.1.3 Defining Actions.
13. Enter a reference. in a “message” a reference is set for the message that is going to be sent and the same reference is used to erase that message.
14. When the action type erase message is selected and the Exclude replier check box is selected, the message will be kept in the handset that most recently fulfilled a success condition.
15. When message and interactive message are selected and the Exclude replier check box is selected, the message will not be sent to the handset that most recently fulfilled a success condition.
16. Enter a message ID. This enables a possibility to update messages in a handset. If this field is left empty it is not possible to update that message later.

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

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

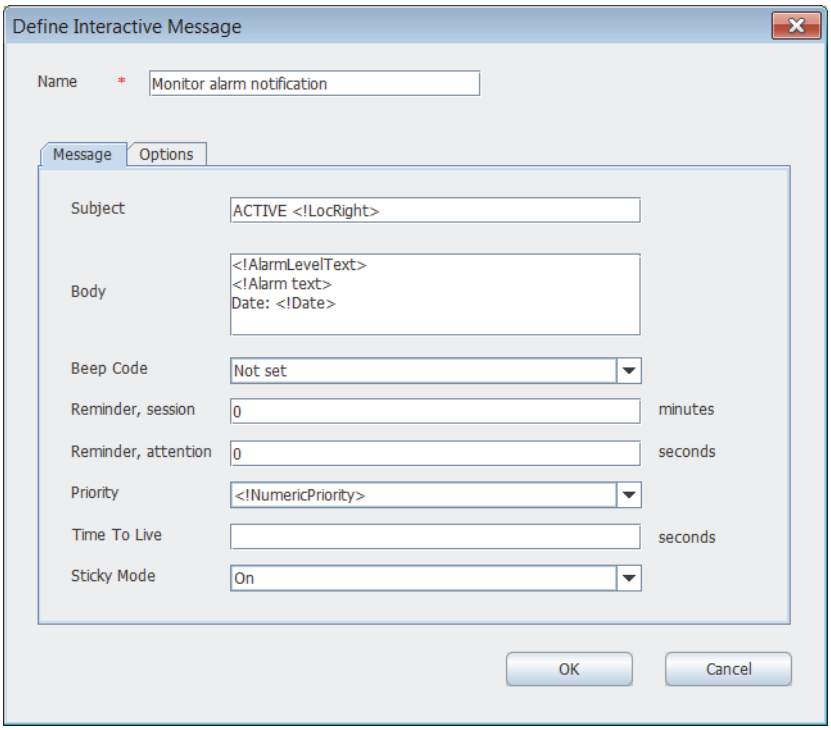
8.1.3 Defining Actions

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

- Message
- Interactive message
- Output activity

In this example, the interactive message has been selected.

Figure 26. Example of define actions for interactive message.



Message Tab

Enter the following:

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

TIP: Right-click in the text fields for Subject and Body, to insert predefined event Elements. This is only possible if a synchronization has been done, see 8.1 Action Configuration.

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

Options Tab – Message

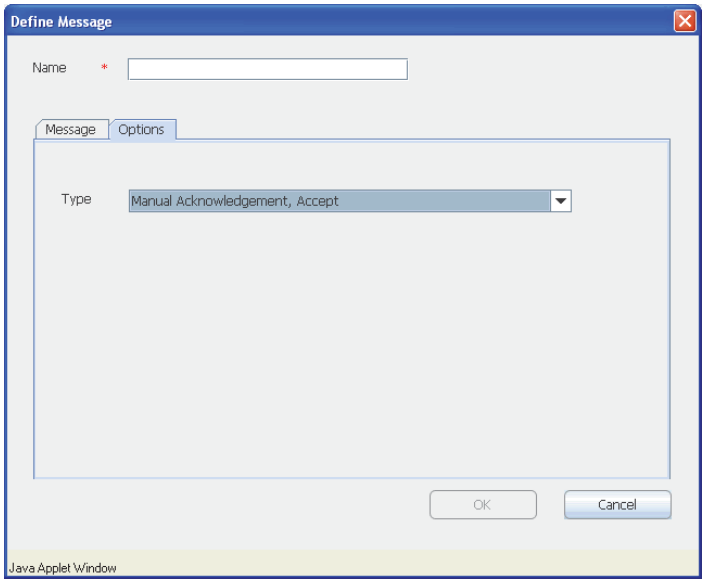
When sending a message, you can add a message response. It can be with acknowledgement accept only where you will know that the user has acknowledge the message or acknowledgement with accept and reject where the user also will have the possibility to reject the message. If nothing is chosen it will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

1. Click the Options tab to add a type of message.
2. Select **Type** from the drop-down list:

- Normal; Default, no message response.
- Manual Acknowledgement, accept if you want acknowledgement with only accept.
- Manual Acknowledgement, accept/reject if you want acknowledgement with the possibility to accept and reject.

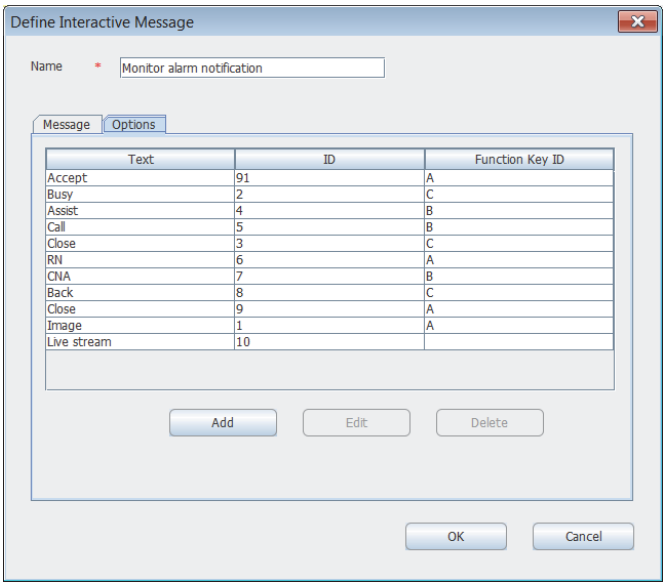
3. Click **OK**.

Figure 27. The type Manual Acknowledgement, Accept, is chosen as option to the action.



Options Tab – Interactive Message

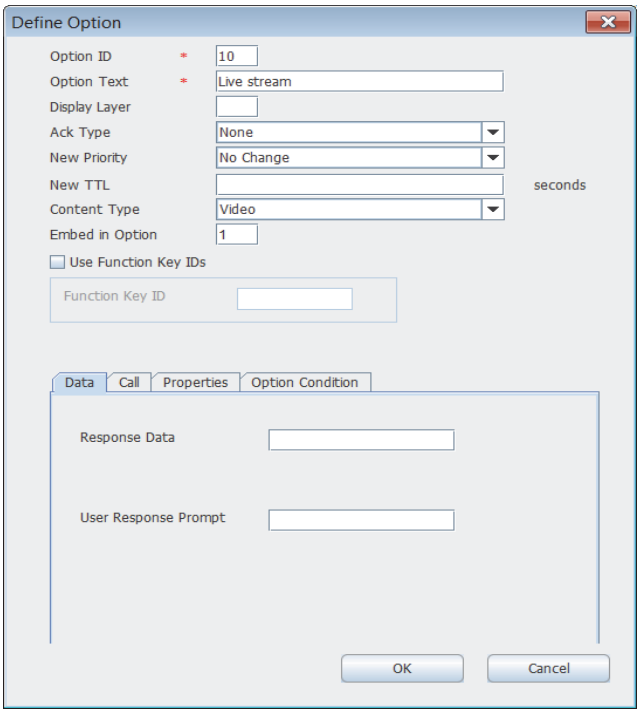
Figure 28. Example of options included in an IM.



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

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

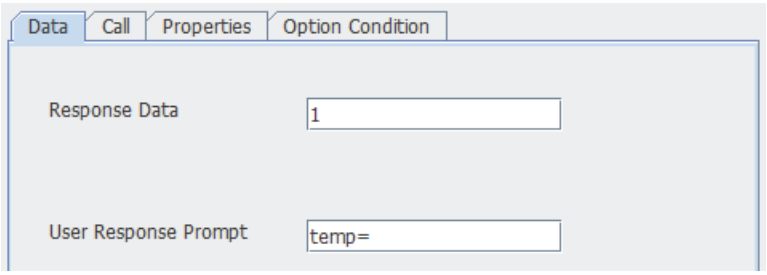
1. Click the **Options** tab.
2. Click **Add**.



General Options	Description
Option ID	1-99, MMG provides a default value.
Option text	Enter text for the option
Display layer	1-99, the layer that the option belongs to. NOTE: Not all handsets support the use of display layers and function key IDs in combination.
Ack type	The acknowledge type tells the device if the Acknowledge option is a positive one (Accept) or a negative (Reject) one. The acknowledge type determines how the option should be visualized in the device.
New priority	The previous priority can be changed.
New TTL	The time to live can be changed.
Content type	The Content Type tells how an IM option should be visualized in devices. If another value than “None” is set, the IM option is visualized as an icon. NOTE: Displaying of icons must be supported by the devices. See also Example: 8.5 IM Including Airstrip.
Embed in option	If the option should be embedded in another option, enter the ID of the other option. See also 8.5 Example: IM Including Airstrip.
Use Function Key IDs	When marked, enter Function Key ID. This is used when adding an option text for a soft key (only for some handsets) NOTE: Not all handsets support the use of Display Layers and Function Key IDs in combination.

Data Tab – Interactive Message

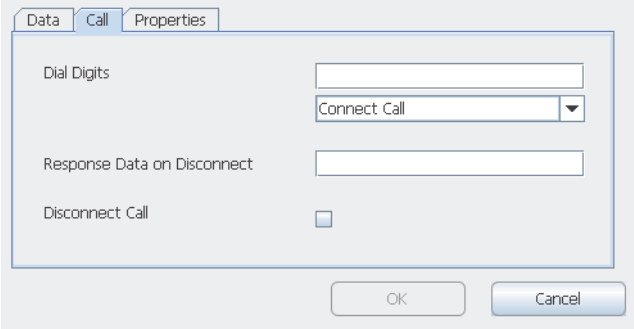
Figure 29. An example of Interactive Message option settings, “Data.”



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

Call Tab – Interactive Message

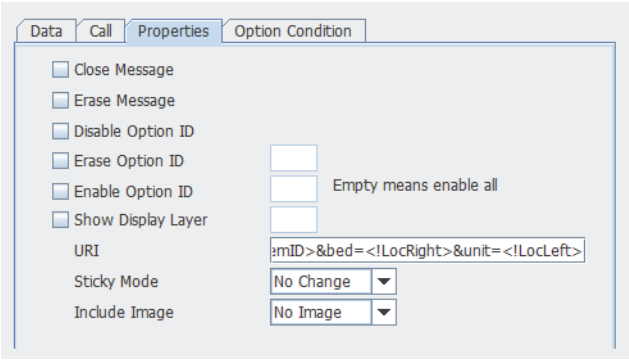
Figure 30. An example of Option settings, “Call”



Call Options	Description
AdministrationDial Digits	Enter telephone number, for example 123456. Connect Call: A new call is connected to the number. Call and Disconnect: A new call is connected to the number and then disconnected DTMF during an ongoing call DTMF during an ongoing call and then disconnected.
Response Data on Disconnect	Data entered here will be replied by the handset when the call is disconnected. Enter a number or a short text.
Disconnect Call	When marked, the ongoing call is disconnected. This option will not be used in combination with the Dial Digits.

Properties Tab – Interactive Message

Figure 31. An example of Option settings, “Properties.



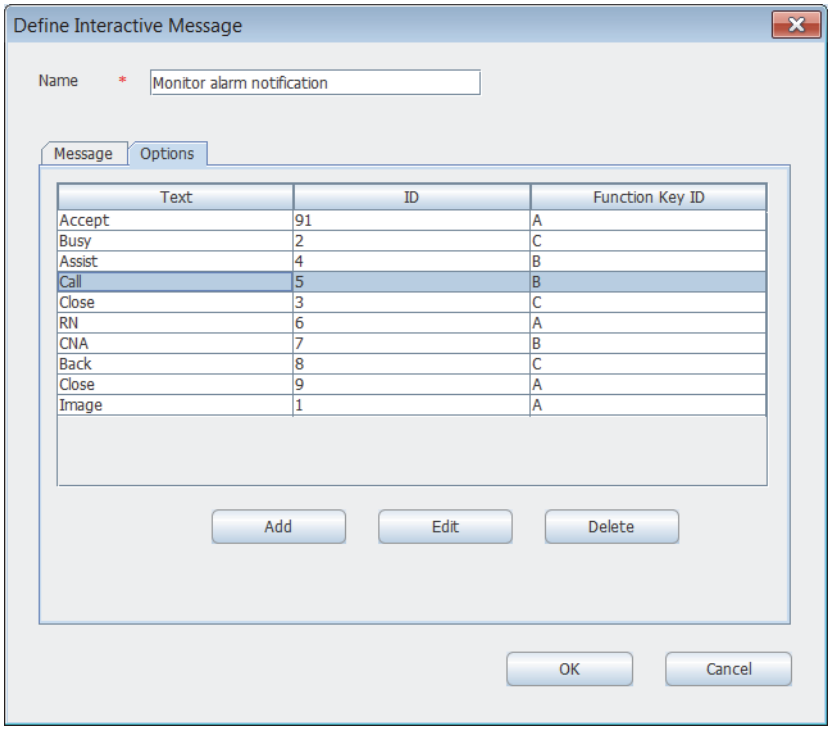
Property Options	Description
Close Message:	The message will be closed.
Erase Message:	The message will be erased.

Disable Option ID:	This Option ID will be disabled.
Erase Option ID:	Entered Option ID will be erased.
Enable Option ID:	Entered Option ID will be in use again.
Show Display Layer:	Entered layer will be displayed in the handset.
URI:	Link to an external resource. This is used if an external resource should be launched when pressing the IM option. Data can also be sent along with the link to the resource by adding event elements to the link. The elements can be added by right-clicking in the field. See also 8.5 Example: IM Including Airstrip
Sticky mode	The message is locked in the display when set to On. It will remain locked until the Sticky mode is turned off or message is deleted. 10) No Change: keeps the old settings. 11) On: the display becomes locked. 12) Off: the display becomes unlocked.
Include Image:	Determines whether an ECG waveform image URL is included in the message[a]. 13) No Image: No image URL is included in the message. 14) Image 1: An image URL is included in the message. 15) Image 2-5: Not used for ECG waveform images. [a]. If this option is on, the “Include ECG waveform image” parameter on the GE CARESCAPE page must also be enabled. See 5.2.21 GE CARESCAPE

Option Condition Tab – Interactive Message

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

Figure 32. Example of defined options included in an IM.



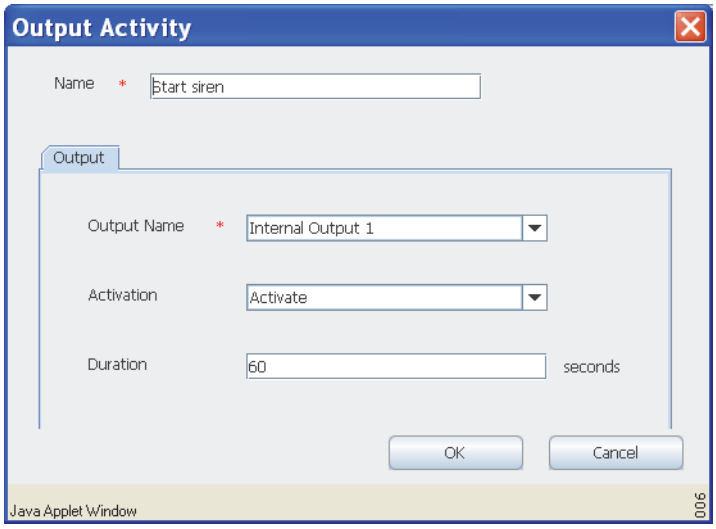
1. Mark the option to be edited.
2. Click **Edit**.
3. Click “Option Condition.”
4. Click **Add**.

Options	**Description**
Event Element:	The event element to compare the specified value with.
Comparison:	String Equals: The option is removed if the specified value matches the value in the event element.
Value:	String Not Equals: The option is removed if the specified value does not match the value in the event element

Options Tab – Output Activity

An Output activity is used to remotely activate or deactivate an output, for example turn on a siren or open a door. When Output Activity is going to be used, a name of the output activity must be entered and an Output Name must be selected. It can be triggered on activation or on deactivation and a duration for how long the activation should stay active can also be set.

Figure 33. An example of Option settings, “Outputs.”

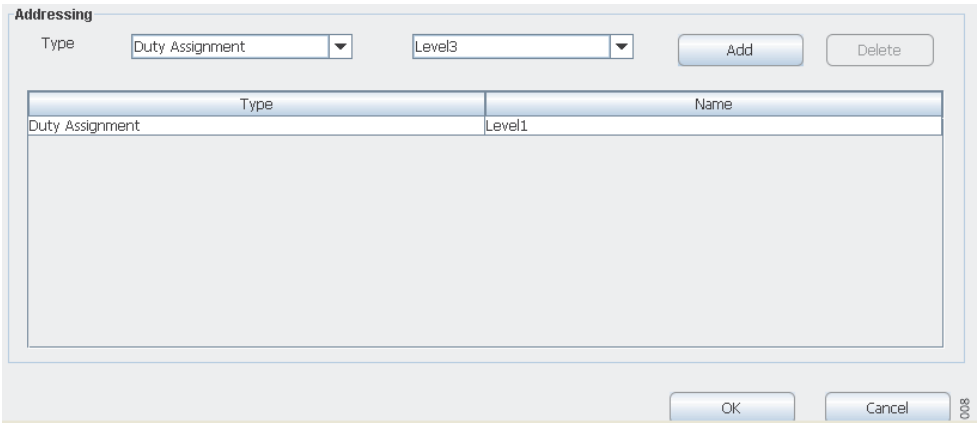


Output Options	Descriptions
Name	Enter the name of the output activity.
Output > Output name Activation Duration	Select one of the outputs. Select between, Activate/Deactivate The time for how long the activation should stay active. 0 = unlimited.

Addressing

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

Figure 34. Destinations are taken from assigned users at level 1 in Duty Assignment



1. Select a type from the drop-down list:

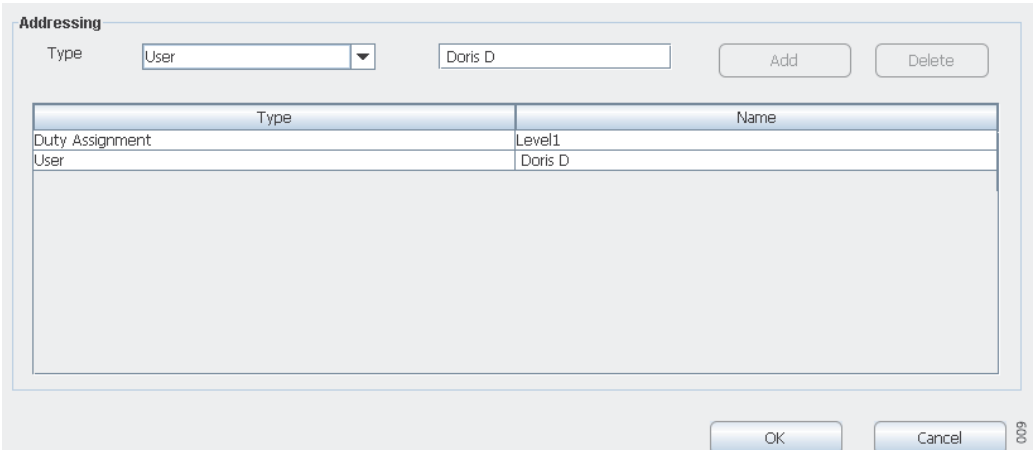
- Duty assignment sends to users via Duty Assignment.
- User sends to users.
- Call ID send to call IDs, typically a telephone number.

- Replier, only updates send updates for this event to the handset that most recently fulfilled a success condition.
- Replier send to the handset that most recently fulfilled a success condition.
- Reference, keep old send to all handsets that previously received a message with this reference.
- Reference, set new send to all handsets that previously received a message with this reference. This will also update the reference for the previous message.

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

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

2. For Duty Assignment and User, select from the drop-down list. For call ID, enter the call ID. If the types Replier, updates only and Replier are selected, the next box disappears. These types have no selections, they are just added. For Reference, keep old and Reference, set new select from the drop-down list.



3. Click **Add** to add the addressing type.

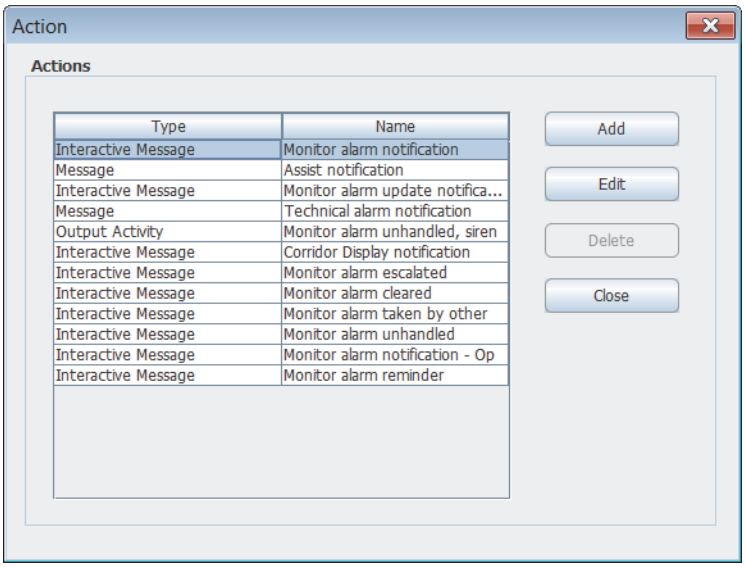
Deleting Destinations

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

1. Click **OK** when finished.

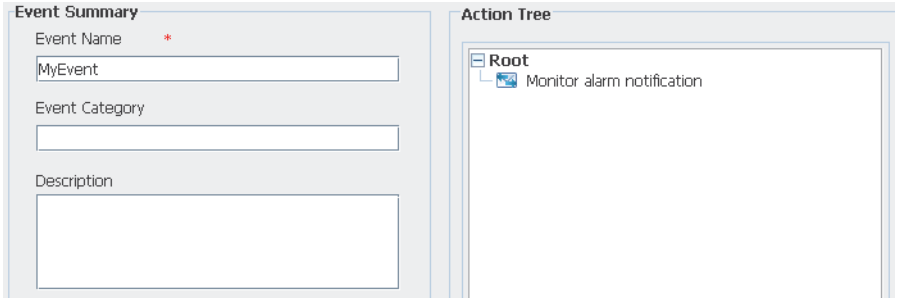
If an action of each type has been added, the Action page may now looks like this.

Figure 35. A list of Added Action Types.



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

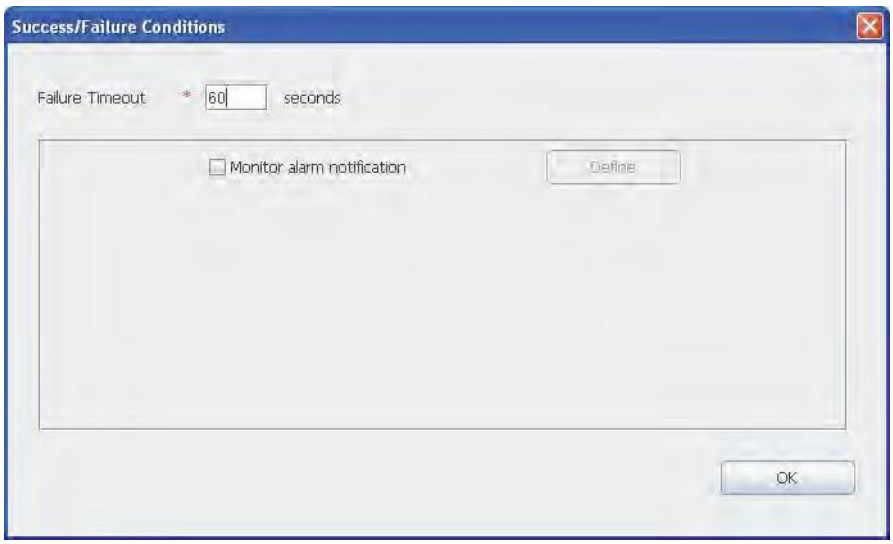
Figure 36. A new action has been added.



Adding Success/Failure Conditions

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

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



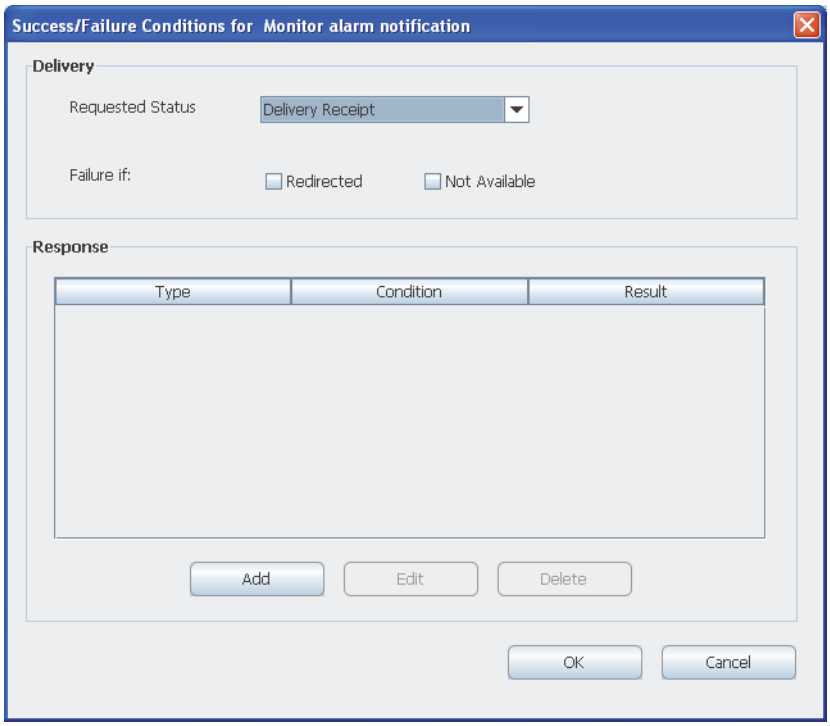
3. Select the check box for the action, in this example “Monitor Alarm Notification” and click **Define**.

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

NOTE: Avoid using the reject option in group messages sent to the 900 system. The reason is that MMG is not aware of that it is a group number and will consider it as a failure and escalate the message as soon as one of the members in the group selects reject. MMG can still escalate the group message, if no one accepts the message, after the specified timeout.

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

Figure 37. Add delivery and status response for the action.



4. Select a requested status from the drop-down list:

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

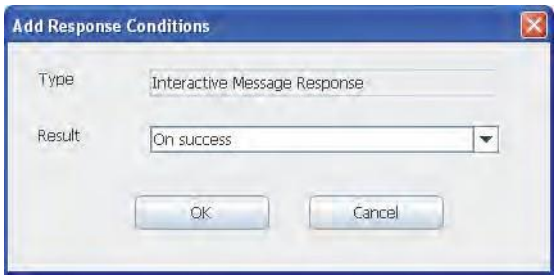
5. Check one or both of the **Failure if** boxes, when **Redirected** or/and **Not Available** should be handled as a fault.

Adding a Response Condition for the Success/Failure Condition

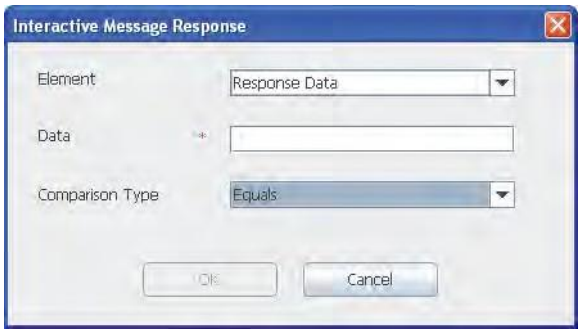
This describes response conditions for an interactive message. For a message, it is done in a similar way, but the dialogues will look slightly differently.

1. Click **Add**.

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



3. Click **OK**.
4. Select an element, enter data and select a comparison type.

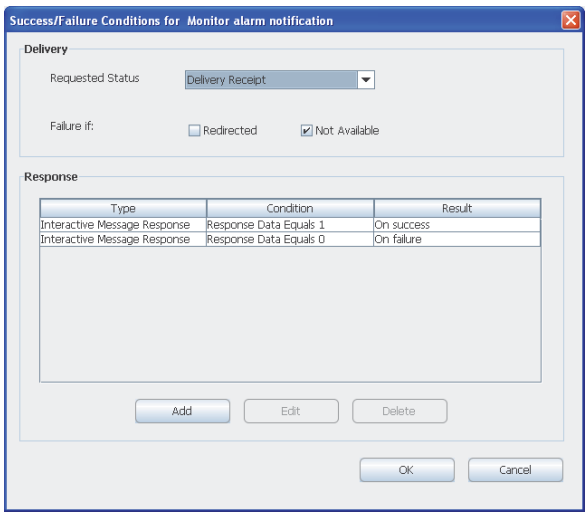


Possible alternatives for elements include:

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

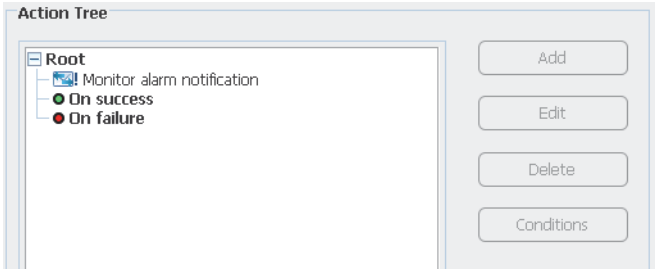
5. Click **OK**.

Figure 38. Response type, condition and result have been defined with success and failure result.



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

Figure 39. Action conditions have been added to the action tree

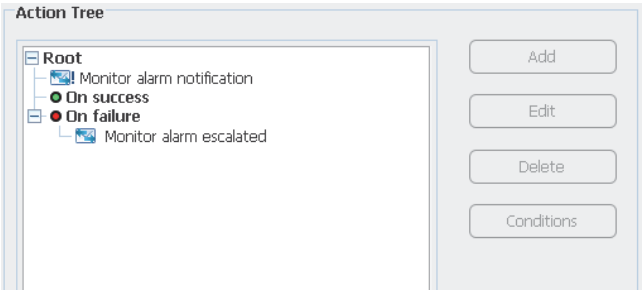


Additional actions can be made by marking the Root in the action tree and click Add. An action can also be edited or deleted by clicking the action and click **Edit** or **Delete**. In the example above the action is monitor alarm notification.

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

You can add an action on the success and/or failure conditions, for example start a siren on failure. This is done by marking one of the conditions and then clicking Add. See 8.1 Action Configuration on how to make the configuration.

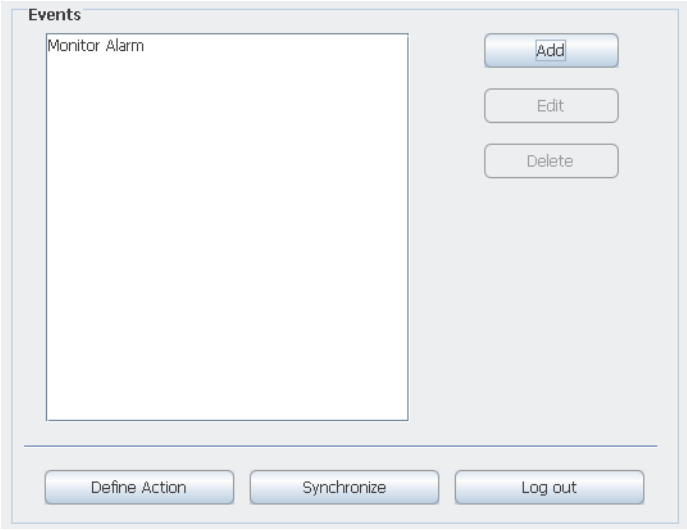
Figure 40. An escalation has been selected as a new interactive message



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

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

Figure 41. A new event is added to the Action Configuration page



8.1.4 Synchronize

1. Click Synchronize to add all the Events that have been created and configured into to the event Assignment User interface. See Figure 41 A new event is added to the Action Configuration page.
2. Click Log out and then Cancel to close the Action Configuration page.

8.1.5 Editing an Event

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

8.1.6 Deleting an Event

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

8.1.7 Copying and Pasting an Event

You can create a new event based on another one.

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

The event Configuration dialog window opens.

1. Make the appropriate changes to the cloned Event.
2. Click OK to save the settings.

8.1.8 Copying an Event and Pasting it into Another Event

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

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

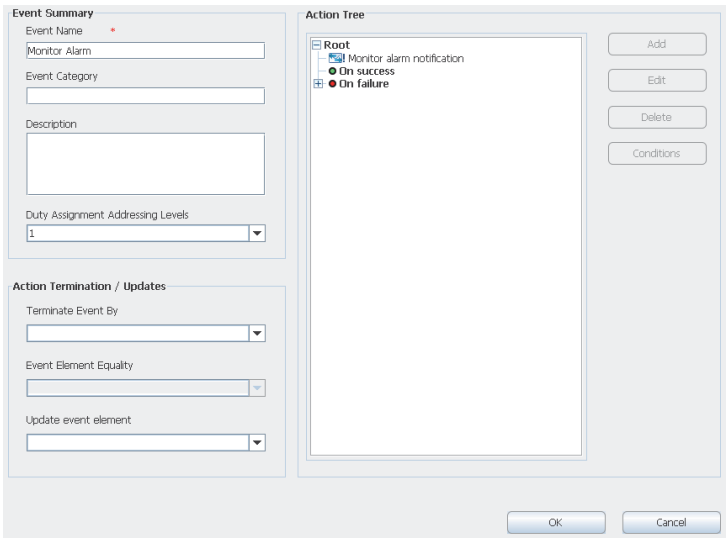
1. Select the event for which action tree you want to copy from.
2. Click Copy.
3. Select the event for which you want to copy the action tree to.
4. Click Paste. The event Configuration dialog window opens.
5. Make the appropriate changes to the event.
6. Click OK to save the settings.

8.1.9 Action Termination/Updates

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

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

Figure 42. This is where termination of actions is set.



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

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

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

Updates

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

Termination example scenario:

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

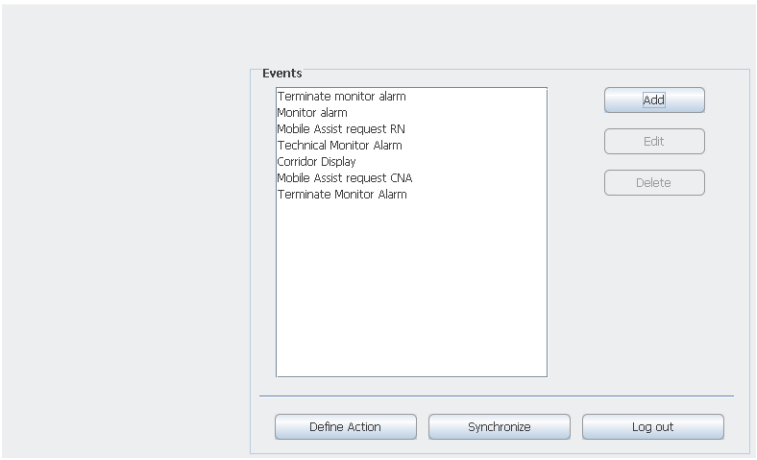
1. The event “Monitor Alarm” is activated and the event includes the event element “Location” with value “ICU|BED1.”
2. The event “Monitor Alarm” is activated again and the event element Location equals “ICU|BED2.” Now two instances of “Monitor Alarm” are running.
3. The event “Terminate Event” is activated, with the Location ”ICU|BED1.” This will terminate the first instance since the values of the event Elements match, but it will leave the second instance running.

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

8.1.10 Adding Termination Event Names

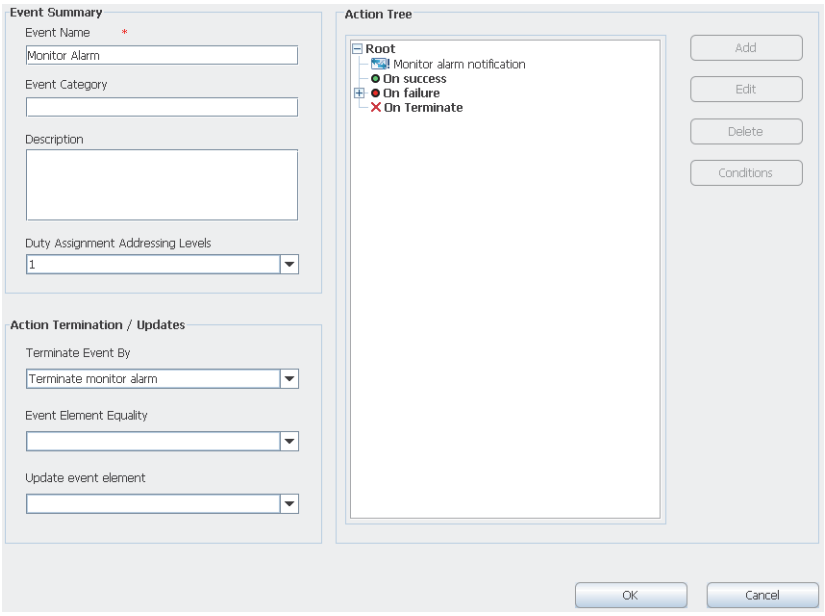
1. From the Action Configuration start page, click Add.
2. Enter the new termination event name in the Event Name field.
3. Click OK.

Figure 43. This example shows an added Terminate event name.



8.1.11 Setting Termination Actions

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



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

You can add an action to the termination by marking On Terminate in the action tree and then click Add. It could for example be that you want to erase the message or have a notification sent when a termination of an event has started. It is not possible to define success/failure conditions on “On Terminate” actions. When “Monitor Alarm” is terminated the terminate action “Monitor alarm cleared” is executed.

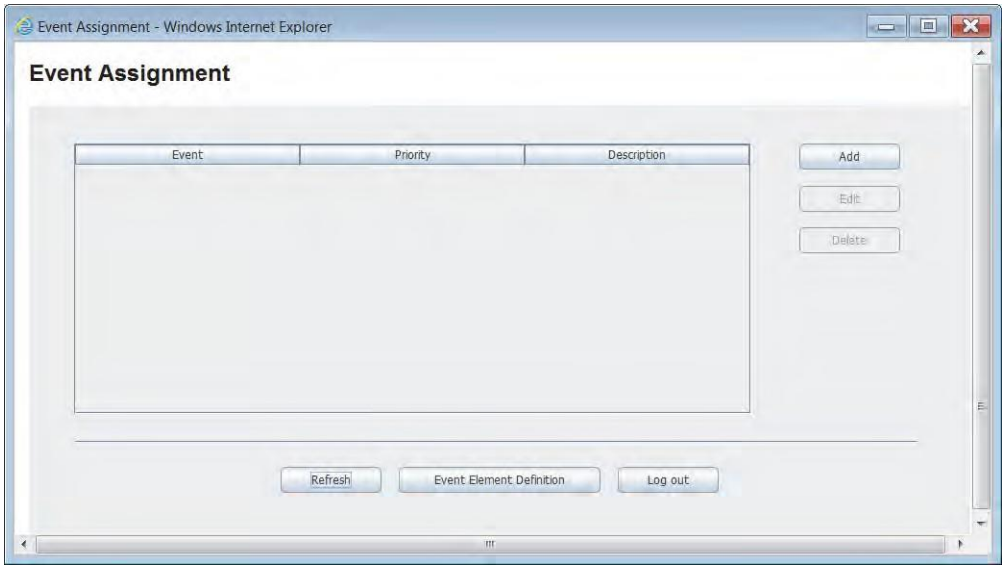
8.1.12 Deleting an Action Termination

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

8.2 Adding Event Assignments

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

1. Click "Event Assignment" and log in with user ID and Password.



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

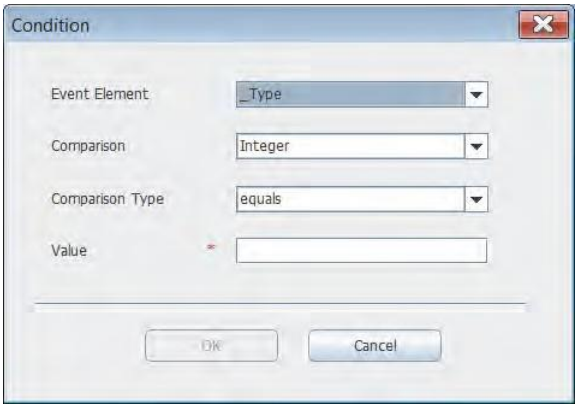
3. Select event from the drop-down list.

NOTE: If the event that you are looking for is not in the list, go back to the event Assignment page and click "Refresh." If it is still not there, log in to Action Configuration and click "synchronize." Return to the event Assignment page, click "Refresh" and then click Add. The event should now be found in the list.

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

NOTE: How the severity is to be indicated in the receiving device is pre-configured in the Action Handler, but can be adapted if needed. If so, see 5.2.19 Action Handler Parameter Settings.

6. Click Add, to add conditions.



7. Select Event element from the drop-down list.
8. Select Comparison from the drop-down list. These are expression types:

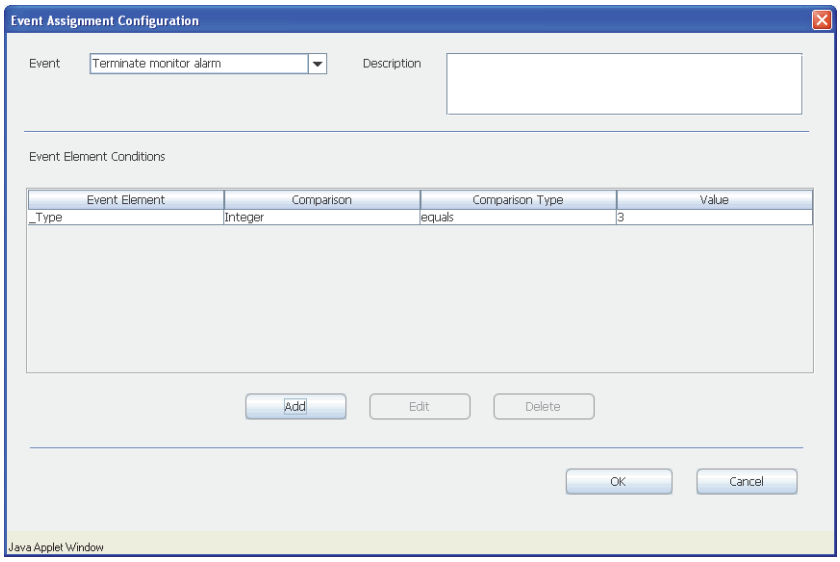
Expression types	**Description**
Integer:	Numerical comparison.
String:	Alphanumerical comparison.
Regular Expression:	Special syntax for advanced comparisons

9. Select Comparison Type from the drop-down list

Comparison Types	**Description**
equals:	The event element will be equal the set value
not equals:	The event element will not be equal the set value.
greater than:	The event element will be greater than the set value for integer
less than:	The event element will be less than the set value for integer.

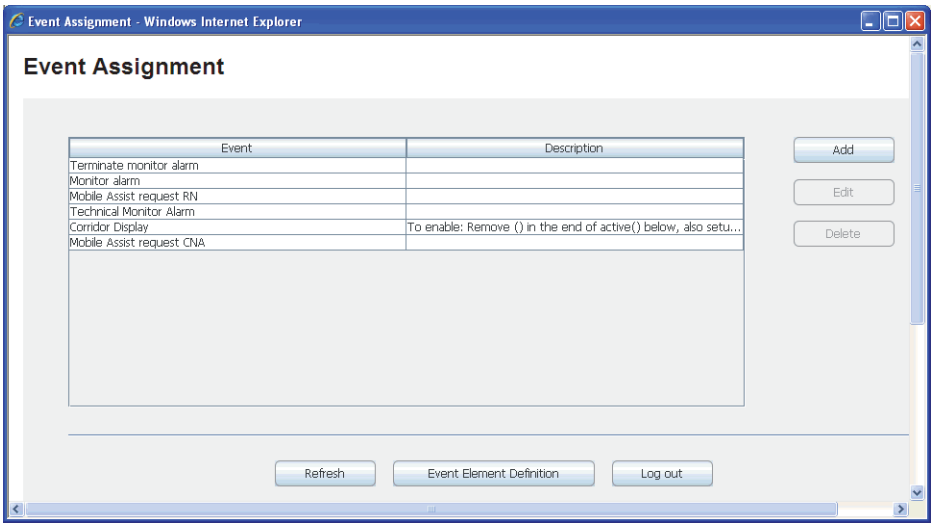
10. Click OK.

Figure 44. Conditions on the event element have been added.



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

Figure 45. The event Assignments page with the events that are included in the Ascom Standard Template



8.3 Layout Setup

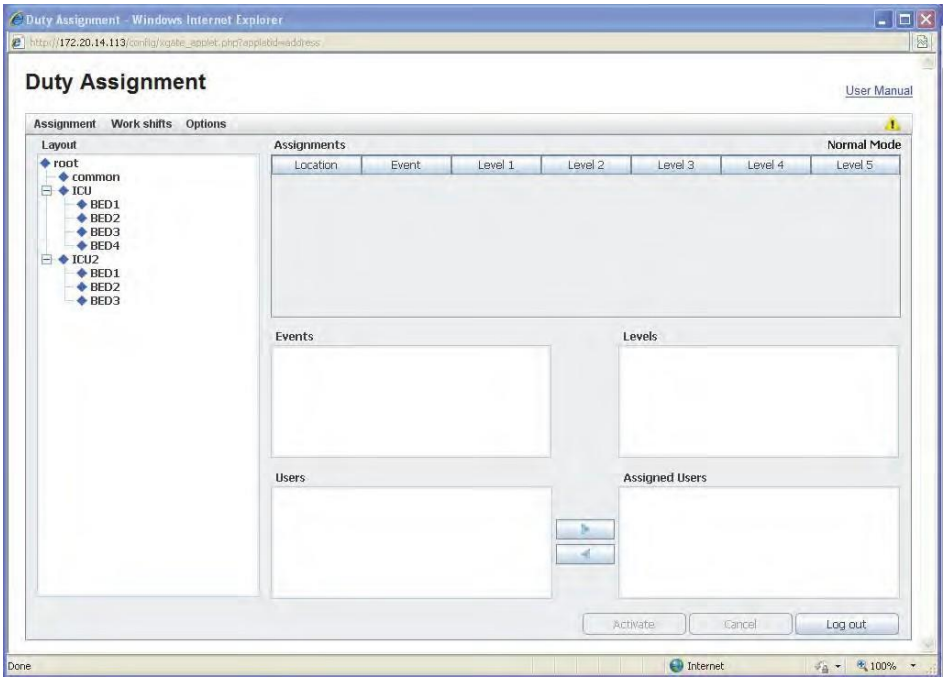
The Layout Setup section describes how to set up the layout structure with locations and User Teams in Duty Assignment and to set up who should be available for duty and on which location. This requires system administrator or administrator rights.

There is a separate for users and administrators which describes how to assign events and levels for users, see Appendix D, D.1 Duty Assignment.

8.3.1 Locations

In the MMG start page, click Duty Assignment.

Figure 46. The Duty Assignment page is displayed with an example of a layout



The layout setup is created in the Options menu.

Menu	**Description**
Layout Setup	Add new location and define conditions for each location. Decide who will be available for duty and on which location.
Auto Activate	Activates the configuration periodically - the time is set in seconds. Disabled as default

The root and common are default locations. They cannot be deleted, though the default names can be changed to something applicable for the business. The location common is used for assignments that all locations have in common.

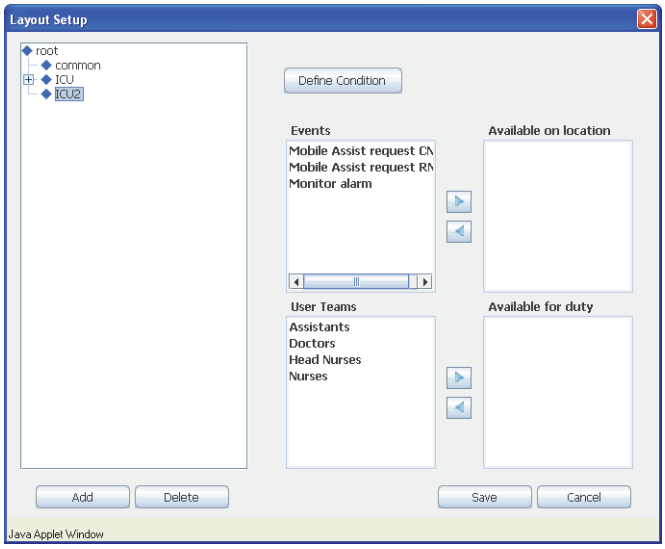
User Teams and users are defined in the Unite Connectivity Manager. See Unite Connectivity Manager, Configuration Manual TD 92735GB.

If Duty Assignment is used on several clients simultaneously and one user enters Layout Setup, the other clients will enter “Immediate mode.” The user who started Layout Setup will not be affected. The other users of Duty Assignment will notice that if a user is moved between “Users” and “Assigned Users,” the change will be activated immediately. This mode will last until the Layout Setup window is closed.

Add Locations

1. In the Duty Assignment window, click **Option** and select Layout Setup.

2. Mark root and click **Add**.



3. Enter a name for the location and click enter on the keyboard, a new field for a location will be added every time you click enter after entered location name. When all locations are added you can click somewhere outside the editing frame to stop more added fields.

To get rid of an empty field that you do not want you can click somewhere outside the editing frame, click the enter tab on the keyboard or click “Esc” on the keyboard.

4. To add levels below the location, keep the location marked and click “add.”
5. Enter a name for the location.

NOTE: To be able to handle alarms for this location, conditions for the location has to be set up, see 8.3.2 Defining Conditions.

Rename Locations

1. Mark the location you want to rename (double-click or triple-click).
2. Enter a new name for the location.

Delete Locations

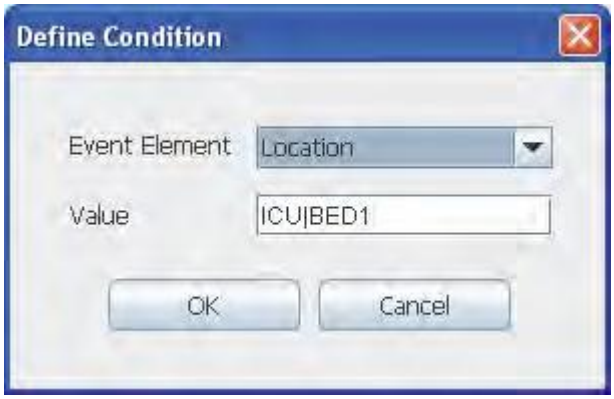
1. Mark the location you want to delete.
2. Click **Delete**.

8.3.2 Defining Conditions

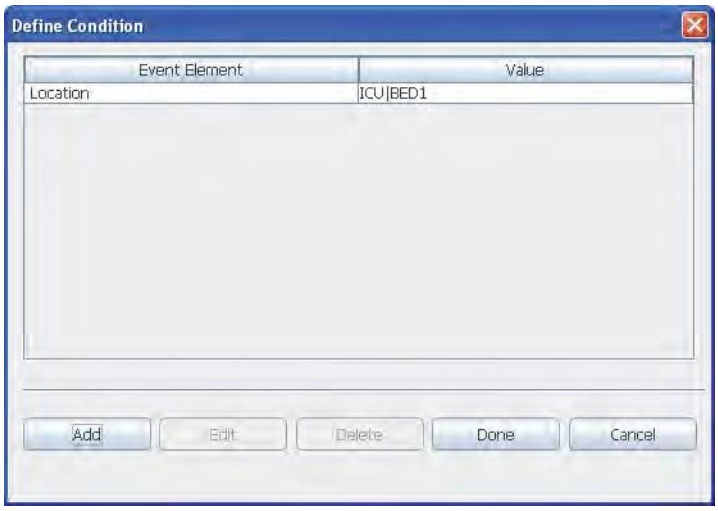
Conditions can be defined for each location, except common which is always active for assignments. By selecting a predefined event element and enter a value for it, an incoming event can be connected to a location.

NOTE: It is important that this setup is performed correctly. To set up a condition,

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



3. Select an event element from the drop down.
4. Enter a value.



More conditions can be defined by clicking **9.4**. 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 conditions themselves that do not match.

Consider a hospital consisting of two ICUs with three beds each. If an alarm from BED3 in ICU2 matches a condition, then not only BED3 but also ICU2 is considered to have a match.

A condition that has been defined can be edited or deleted. When finished, either click **Done** to save the configuration or Cancel.

8.4 Setting up Access Rights

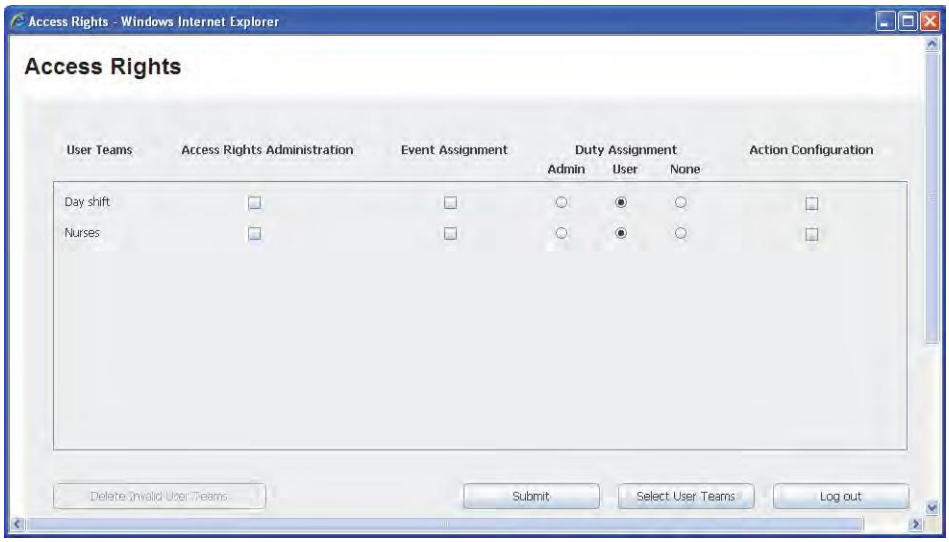
For user administration, different access rights are given to different User Teams to be able to log in to Access Rights, Action Configuration, event Assignment and Duty Assignment.

For Duty Assignment, select the user teams that will have Admin, User or None access to the GUI.

Authority	Description
Admin:	Rights to administrate Duty Assignments
User:	Rights to make assignments in Duty Assignment
None	No access rights to Duty Assignment

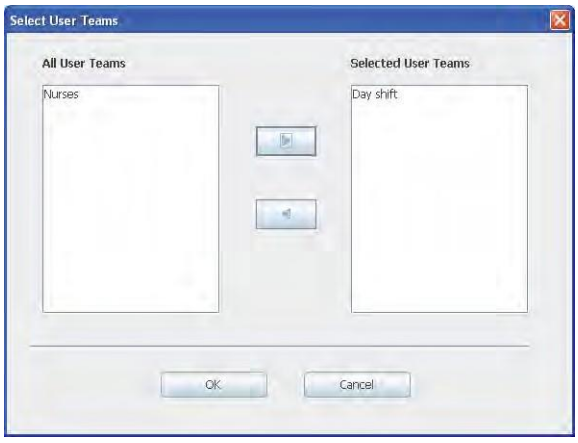
User teams are set up in the Unite Connectivity Manager, see Unite Connectivity Manager, Configuration Manual TD 92735GB. To set access rights:

1. In the MMG start page, click **Configuration**.
2. Click **Basic**.
3. Click “Access Rights.”



4. Click **Select User Teams** to add user teams.

Mark the user team that will be granted access rights. Move the user team from the All User Teams list box, by clicking on the arrow pointing to the right. The user team will be moved to the Selected User Teams.



5. Click OK.

6. Select which applications the user team should have access to by selecting or clearing the check boxes for access rights.
7. Select between, Admin, User or None for the Duty Assignment.
8. Click Submit to save the access rights.

Removing a User Team from the Access Rights Page

1. Click “Access Rights.”
2. Click “Select User Teams.”
3. Mark the user team whose access rights will be removed. Move the user team from the Selected User Teams, by clicking on the arrow pointing to the left. The user team will be moved to the All User Teams.
4. Click **OK**.
5. A dialog opens, 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 that are not available in the system will be deleted.

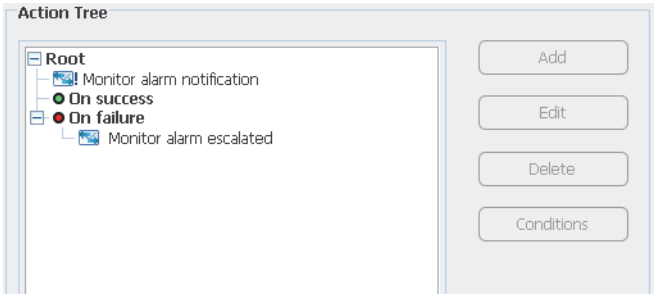
8.5 IM Including Airstrip

If the template including Airstrip settings has not been applied, the settings can be added manually as described in this section.

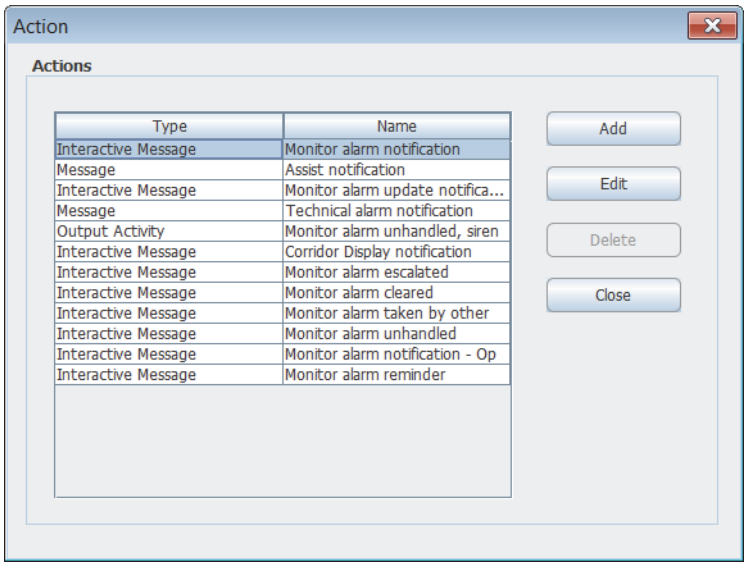
NOTE: This feature is only supported by Unite Axess for Smart Devices with the Airstrip ONE® application installed.

1. Mark the event you want to edit.

2. Click Edit.

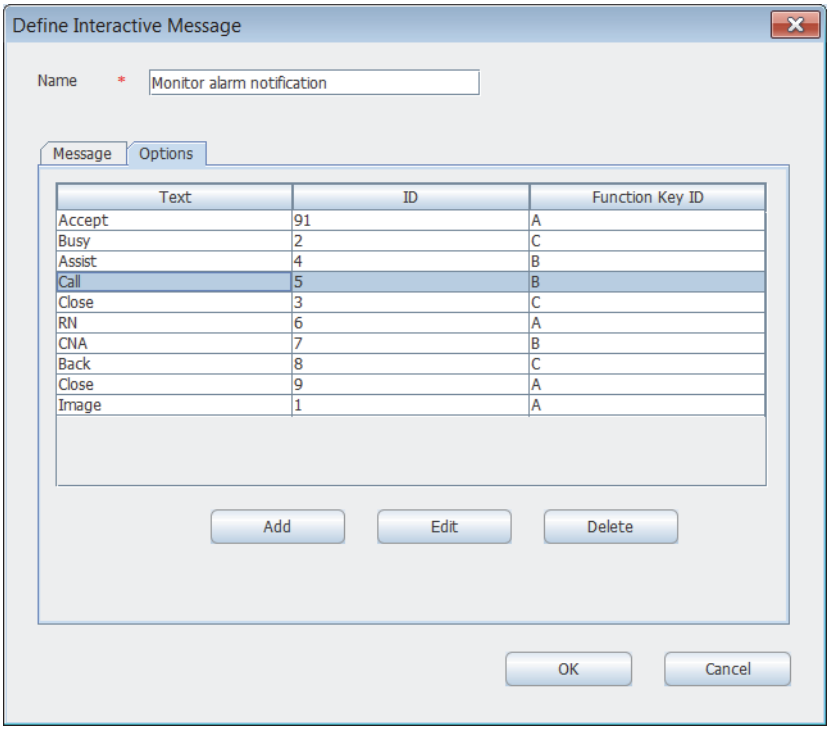


3. Mark the action you want to edit in the Root tree.
4. Click Edit.
5. Click Define Action.
6. Mark the interactive message you want to edit.

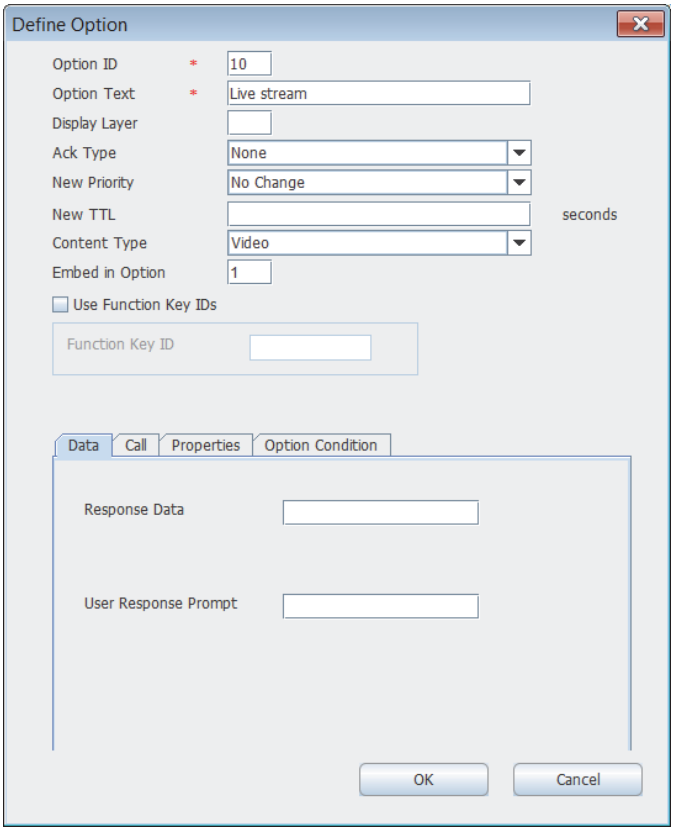


7. Click Edit.

8. Click the Options tab.



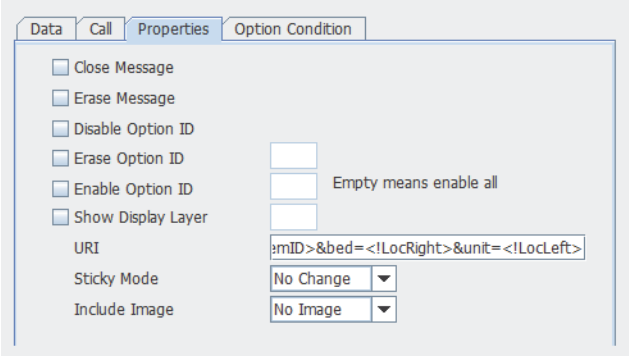
9. Click Add to add an option to the IM. In this case, the option should be used to launch an Airstrip application for viewing ECG waveforms in real time.



10. Enter/select the following: (only the parameters below are required in this example):

General options	Description
Option ID:	Keep the value provided by the MMG.
Option Text:	Enter text for the option (e.g. “Livestream”).
Content Type:	Select “Video” to show the option as a video icon.
Embed in Option:	In this case, we want that users should be able to press the video icon embedded in an ECG waveform image to launch the Airstrip application for viewing the ECG waveforms in real time. Enter the ID for the option to open the image.

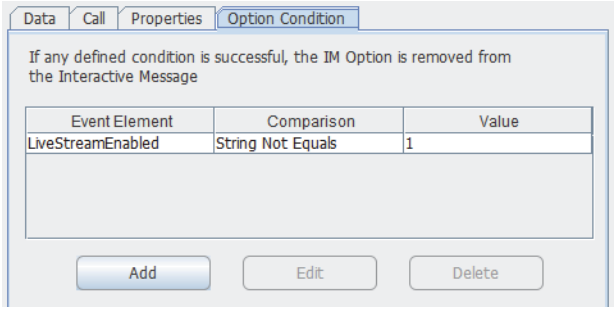
11. Click the Properties tab.



12. In the “URI” text field, enter the following link used for launching the Airstrip application when pressing the embedded video icon.

airstripone://ascom/pm-mon?siteid=<!LiveStreamSystemID>&bed=<!LocRight>
&unit=<!LocLeft>

13. Click the Option Condition tab.



14. If the parameter for live stream of ECG waveforms is not enabled in the MMG, the video icon should be hidden in the IM. Click Add and configure as shown in the figure above.

9 Troubleshooting

Fault	Probable Cause	Action or Comment
It takes time to open Access Rights, Action Configuration, Event Assignment, and Duty Assignment. Additionally, a Java warning dialog appears after a while telling that the application may be a security risk	The module is not connected to Internet meaning that the Ascom certificate, used to sign the Java application, cannot be verified.	If the module do not have a connection to Internet, you can disable the verification of the certificate. 1. Open Java Control Panel in Windows. 2. Click the “Advanced” tab. 3. Under Perform Certificate revocation checks on,” click “Do not check.”

10 Related Documents

MMG Duty Assignment User Manual	TD 92691GB
Data Sheet, MMG	TD 92653EN
Data Sheet, Elise3	TD 92678GB
Troubleshooting Guide, Alarm Management for GE Patient Monitoring	TD 92717GB
Installation Guide, Elise3	TD 92679GB
Unite Connectivity Manager, Configuration Manual	TD 92735GB
Pre-configuration of Windows for Unite Applications, Configuration Notes	TD 92993EN

11 Document History

Version	Date	Description
L	31 March 2018	First released version
M	30 September	Updated document format, added more details about handling faults in Appendix G.1, and added Security subsection to 5.2 Advanced Configuration.

Appendix A Used IP Ports

This section describes IP ports that can be used when a connection between a server and a client is established. It is always the client that initiates a connection by sending a request to a well-known (fixed) port used by the application/unit on the server. Each time a client initiates a connection it is assigned a temporary (i.e. ephemeral) port number to use for that connection. Additionally, the client sends its temporary port number to the server so the server know which port it should respond to. These temporary port numbers are assigned in a random way within the port range 1025 - 65535.

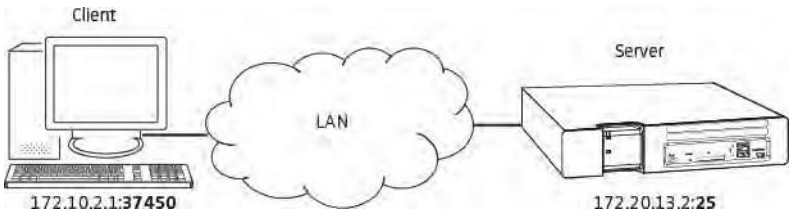
NOTE: If a firewall is used, the well-known port (fixed) must be available for communication in the network. The table below describes the well-known port used by the application/unit acting as server.

Example 1:

In this example the FTP area on the MMG should be accessed. An FTP client installed on a computer is used to access the FTP area. In this case, the MMG acting as a server and the computer acting as a client.

Port 25 is a well-known one for FTP requests and port 37450 is a temporary one assigned to the client.

Figure 47. MMG acting as a server

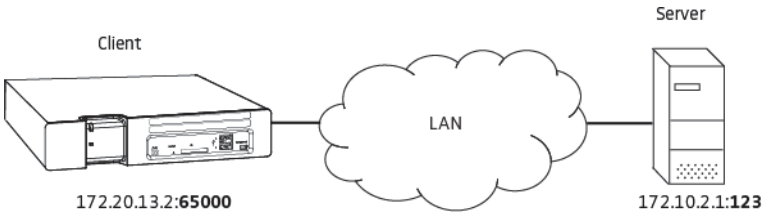


Example 2:

In this example, the MMG should obtain time and date from an external source acting as a NTP server. In this case, the MMG is acting as a client since it initiates the connection to the NTP server.

Port 123 is a well-known one for NTP requests and port 65000 is a temporary one assigned to the client.

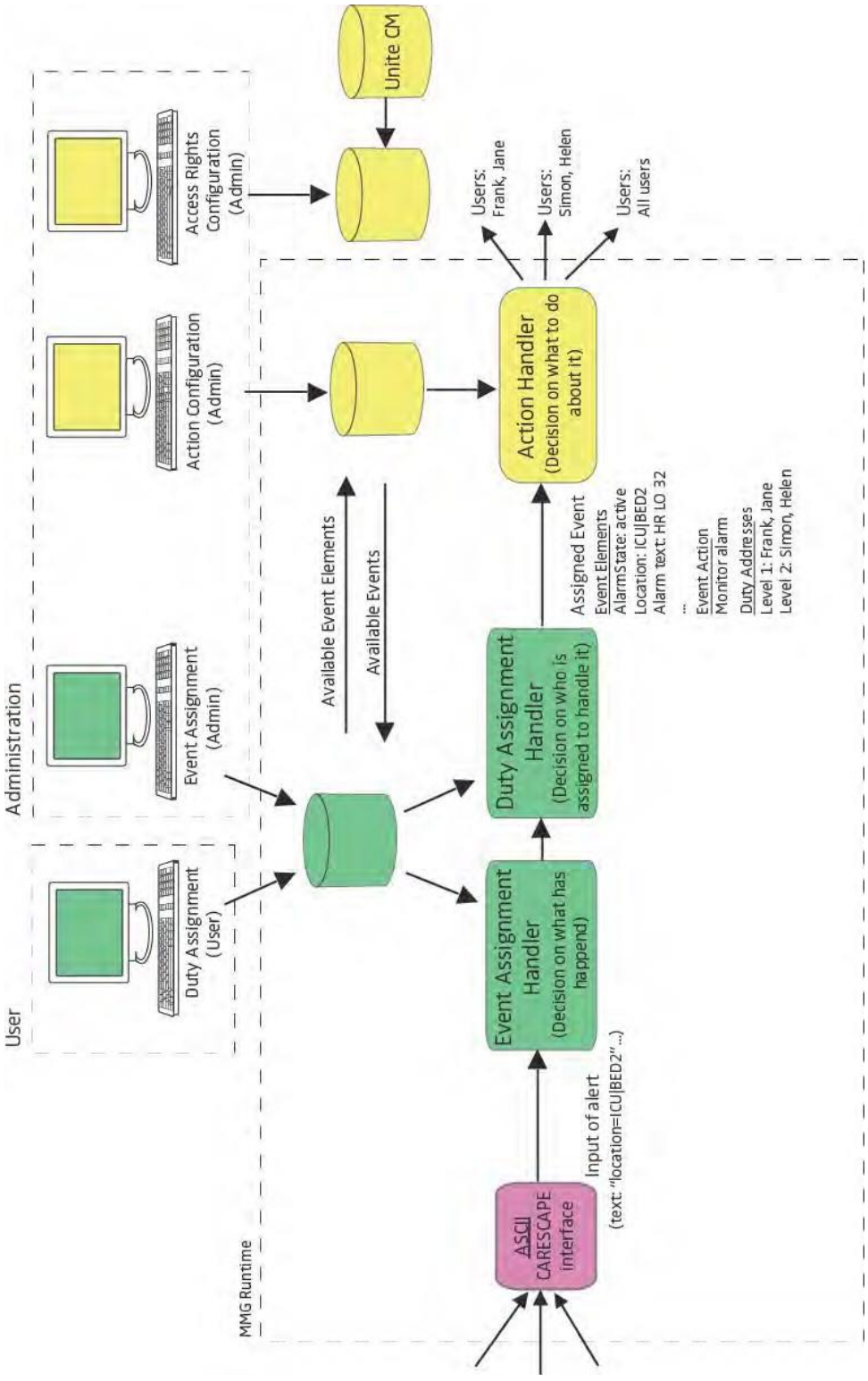
Figure 48. MMG acting as a client



The following table shows IP ports used by applications/units acting as a server.

Port	Application or Unit	Transport Protocol
21	File Transfer Protocol (FTP)	TCP
22	Secure Shell (SSH)	TCP
53	Domain Name Server (DNS)	UDP
80	Web traffic	TCP
123	Network Time Protocol (NTP)	UDP
2000	Time Updates (used by CARESCAPE)	UDP
3217	Unite traffic	UDP
7000	RWhat (used by CARESCAPE)	UDP
7001	Alarm (used by CARESCAPE)	UDP
8000	image presentation server	TCP
10101	Remote connection - TCP and RS232 conversi	on TCP
10132	Applet communication (Event Assignment)	TCP
10133	Applet communication (Duty Assignment)	TCP
10134	Applet communication (Access Rights)	TCP
10135	Applet communication (Action Handler)	TCP

Appendix B MMG Overview Picture



Appendix C MMG Filtering Description

This appendix gives a description of the filtering feature in MMG.

NOTE: It is highly recommended to use the filtering feature to avoid spamming of handsets and also to avoid heavy traffic loading of the carrier system (for example IP-DECT or VoWiFI) used.

Three types of filters can be used:

- Alarm Text Group filters (all matching alarm texts will be considered to be the same alarm)
- Alarm Text Stop filters (no alerts will be sent out for alarm texts that matches the filter)
- Alarm Text Delay filters (all matching alarm texts must still be active for as long as defined in MMG before the alerts are sent out)

When using **text stop filters** and **text 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:

Filter	**Matches**
?	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.

NOTE: If the text strings received by the MMG comes in a language other than English, and filtering is needed, then the filters have to be edited/updated. Consult GE Healthcare at the installation to check what text strings the MMG will receive.

Examples:

Filter	Matches
HR ?O	“HR LO” and “HR HO” but not “HR O” or “AAAHR LO”
HR *O	“HR LO,” “HR HO,” “HR O” and “HR NNO”
HR LO ?|HR LO ??	“HR LO 9" and “HR LO 10”
HR LO; Heartrate low	also describes in plain text (in this case Heartrate low) 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.

IMPORTANT: Do NOT use “*” alone due to the filter will stop ALL alarms.

C.1 Example of Group Filter Configuration

This example affects the behavior of the alarms flow as follows.

- The staff assigned to a specific location will receive periodic updates of an alarm to be able to follow a trend of a heart rate.

By default, the MMG discards all alarm updates that are considered to be the same as the initial alarm, but the MMG can be configured to letting through some alarm updates in intervals by setting a Group filter time limit parameter.

- The staff on Level 1 in the escalation chain will always receive alarm updates that are not considered to be the same as previously alarms, due to the alarm text has been changed, or the priority of the alarm has increased.

By default, if an alarm is escalated to another level than Level 1, the level that acknowledged the alarm will receive all alarm updates (if any) directly. The MMG can be configured to restart the escalation chain if an alarm is not considered to be the same by setting a Restart escalation on alarm text changes or on higher priority parameter.

The following parameters have been configured in this example:

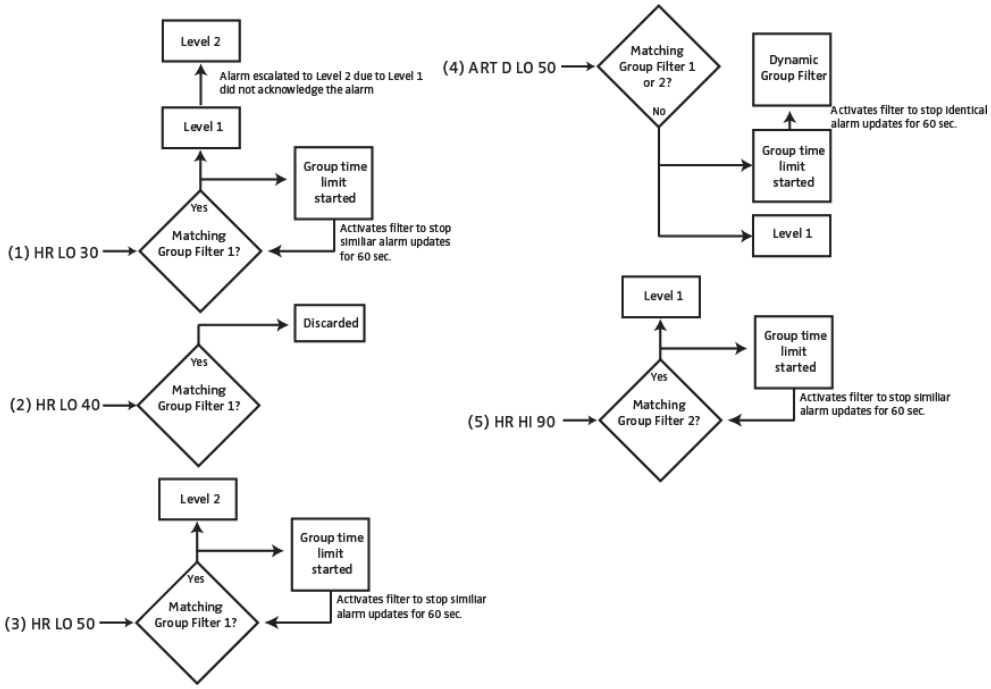
Parameter **Value**

Group Filter 1: HR LO* Group Filter 2: HR HI*

Group filter time limit: 60 sec

Restart escalation on alarm text changes or on higher priority: Restart on alarm text changes.

Figure 49. Group Filter with Group Time Limit settings.



1 An alarm that matches a Group Filter for the first time will always pass the filter. In this case the alarm HR LO 30 passed the Group Filter and was first sent to the staff on Level 1. Since the Level 1 did not respond to the alarm, the alarm was escalated to Level 2 that acknowledged the alarm.

Each time an alarm is passing a Group filter, the matching group filter will be activated. This means that any alarms that match that filter will be discarded until the Group Time limit elapsed. In this case, the Group Filter 1 is activated for 60 seconds.

2 An alarm update HR LO 40 is received within 60 seconds. It matches the active Group

Filter 1 and is considered to be same as previous received alarm (HR LO 30). The alarm update is discarded.

3 An alarm update HR LO 50 is received after 60 seconds. It matches the Group Filter 1 and is considered to be same as previous received alarm (HR LO 40), but since the Group Time Limit has expired this alarm update will pass the Group Filter 1. Since the alarm passed the Group Filter 1, the filter is once again activated for 60 seconds.

The alarm update is sent to the staff that acknowledged the latest passed alarm (HR LO 30). In this case the staff on Level 2.

4 An alarm ART D LO 50 is received within 60 seconds, and it does not match any Group Filters meaning that the alarm will be sent to the staff. The MMG will now create a dynamic group filter that only will match alarm updates with the alarm text ART D LO 50.

Since another group filter has been activated and the escalation parameter is set to Restart on alarm text changes, the alarm is sent to the staff on Level 1. The Group Time Limit for the dynamic group filter is started, and Group Time Limit for the Group Filter 1 expires automatically. The Group Time Limit is only used by the latest activated group filter.

5 An alarm HR HI 90 is received within 60 seconds and matches Group Filter 2.

Once again another group filter has been activated. The Group Time Limit for Group Filter 2 is started, and Group Time Limit for the dynamic group filter expires automatically. The alarm is sent to the staff on Level 1.

Appendix D Ascom Unite Application Manager

The MMG can either be used as a stand-alone module, or be used together with a Windows-based Ascom Unite Application Manager (Unite AM). Depending on the installed software[1] on Unite AM, You can manage some features in the MMG. When a feature is enabled in the Unite AM, the corresponding feature is disabled or hidden in the MMG. Refer to Pre-configuration of Windows for Unite Applications, Configuration Notes TD 92993EN for more information.

Depending on the features enabled in the Unite AM, the following features might be affected in the MMG:

D.1 Duty Assignment

Duty Assignment is where locations, in for example a hospital, and definitions of conditions for event Elements are set up.

When Unite Assign is enabled in the Unite AM, the Duty Assignment option will be hidden in the MMG. In this case, the work is done in the Unite AM.

D.2 Action Configuration

Events and actions and conditions for events, are configured here. The administration of access rights is also done in Action Assignment.

When the action configurations is managed from the Unite AM, the action configurations cannot be edited in the MMG. However, you can view the settings in MMG.

1. Currently Messaging Suite for Healthcare.

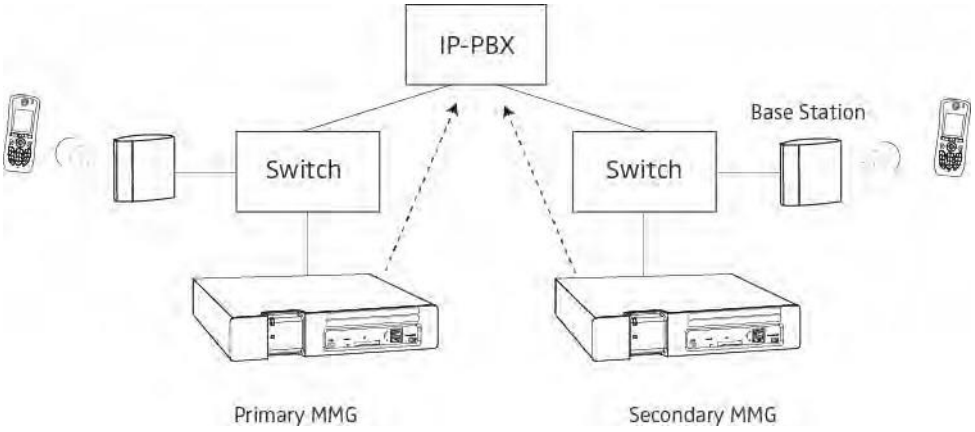
Appendix E Network Monitoring in a Redundant System

NOTE: Primary, secondary and virtual IP addresses on different subnets are not supported in a redundant system.

In a redundant system, both the primary MMG and the secondary MMG can check if they have connection to the network by sending ICMP inquiries to an optional equipment in the same network. It is recommended to use the equipment that is centrally installed in the network, for example an IP-PBX. See the example below for more information.

If the active MMG loses the connection to the network, the standby MMG will become active instead.

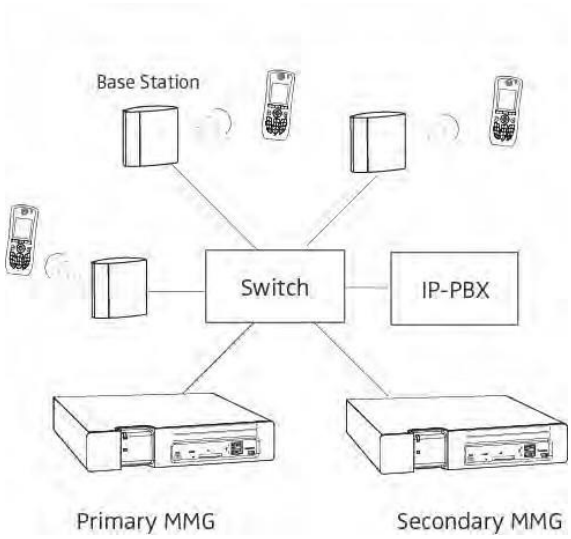
Figure 50. Illustration of using a centralized equipment as network reference.



In the above figure, both the primary MMG and the secondary MMG are using the IP-PBX as network reference since it is centrally installed in the network.

NOTE: The use of the network monitor function is optional, but it is strongly recommended to use when the modules are connected to different switches. If the function is disabled and the modules cannot communicate with each other, both modules might become active since they consider that the other module has failed. The result is that the one part of the system will write data to the primary MMG, and the other part will write data to the secondary MMG. This behavior is called “split brain behavior.”

Figure 51. Illustration of a network when no network monitoring is required.



If the primary MMG and secondary MMG are connected to the same switch (see Figure 51), no equipment (for example an IP-PBX) is needed as network reference. If the secondary MMG do not receive any response from the primary MMG, the primary MMG has actually failed and the secondary MMG becomes active.

E.1 Fallback Behavior when Network Monitoring is Not Used

If the primary MMG loses the connection to the LAN (the power source is still connected), the secondary MMG takes over as an active one. When the primary MMG is reconnected to the LAN, the system switches back to the primary module immediately.

If the primary MMG fails for other reasons than LAN disconnection, the secondary MMG will also take over, but the system will not switch back to the primary MMG automatically when it is repaired. In that case, fallback to the primary MMG has to be done manually.

Appendix F LDAP User Authentication

NOTE: This section is applicable for Access Rights, Action Configuration, event Assignment and Duty Assignment only.

An LDAP server can be used if the passwords for the applications above should be managed from an external database (e.g. Active Directory). This can be useful if the passwords should be centrally managed instead of managing them locally for the applications.

F.1 Creating User Teams in Unite CM

To be able for users (admin and sysadmin are excluded) to log in to the applications mentioned above, the users have to be included in User Teams. Then, the User Teams can be given access to the applications.

For more information about how to create User Teams and add members to the teams, refer to Unite Connectivity Manager, Configuration Manual TD 92735GB.

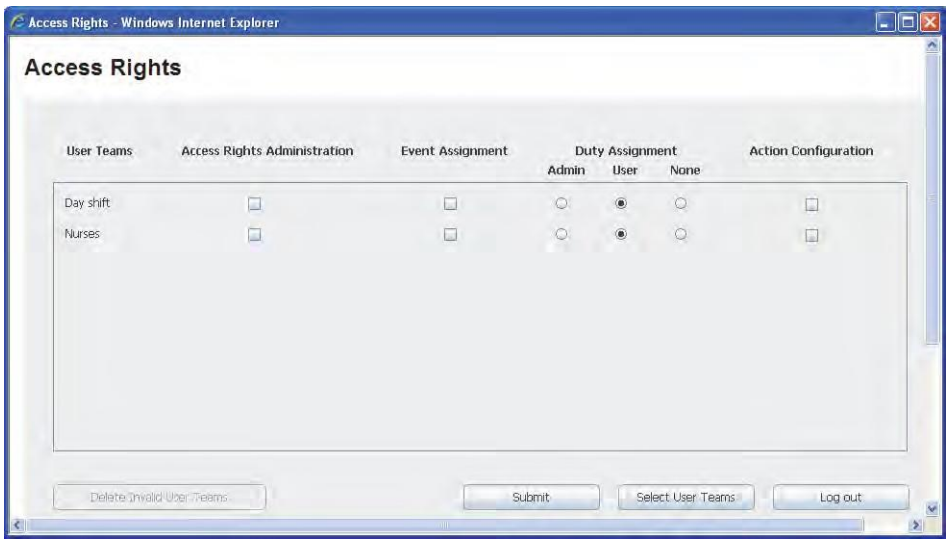
F.2 Setting Up Access Rights

The User Teams created in Unite CM have to be given rights so the users included in the teams can log in to the applications. Different access rights can be given to different User Teams.

For Duty Assignment, you can select the User Teams should have admin, user or none access to the GUI.

Authority	**Description**
Admin:	Rights to administrate Duty Assignments
User:	Rights to make assignments in Duty Assignment
None:	No access rights to Duty Assignment

1. In the MMG start page, click **Configuration**.
2. Click the “Basic setup.”
3. Click “Access Rights.”
4. Log in with user ID: “sysadmin” and password: “setmeup.”
5. Click “Select User Teams” to add User Teams.
6. Mark the user team that will be granted access rights. Move the user team from the All User Teams list box, by clicking on the arrow pointing to the right. The user team will be moved to the Selected User Teams.
7. Click **OK**.
8. Select which applications the User Team(s) should have access to by selecting or clearing the check boxes for access rights.

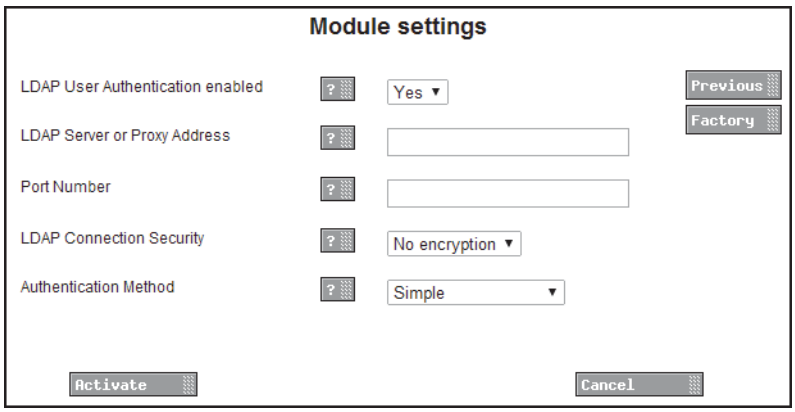


9. Select between, Admin, User or None for the Duty Assignment.
10. Click Submit to save the access rights.

F.3 Select LDAP Server for User Authentication

This section describes the settings needed if the users should log in by using the login credentials administrated in an LDAP server. When the users log in to the application, the MMG sends a request to the LDAP server to check if the users are authorized to log in.

1. Click **Configuration** on the start page.
2. Click the **Advanced** tab.
3. Click Basic Administration.
4. Click “LDAP User Authentication.”



5. Select if the settings below should be enabled or not, in the LDAP User Authentication enabled drop-down list.
6. Enter the IP address or host name to the LDAP server in the LDAP Server or Proxy Address field.
7. Enter the port number used by the LDAP server in the Port Number field.
8. If the field is empty, port 389 will be used for non-encrypted connection, and port 636 will be used for encrypted connection (LDAP over SSL, called LDAPS).
9. Select if the connection to the LDAP database is to be encrypted in the LDAP Connection Security drop-down list.

10. Select how to authenticate to the LDAP server in the Authentication Method drop down list.
11. Simple: Authentication method that sends user and the password in clear-text to the LDAP server.

NOTE: To avoid exposing the password, you can use the simple authentication together with the encryption method LDAPS.

SASL/Digest-MD5: Authentication method that uses a hash algorithm to convert the password, which means that it is not sent in clear-text.

NOTE: If the authentication method “SASL/Digest-MD5” is selected, the IP address for primary DNS server must be entered in the DNS server field on the Network setup page. Continue in Network Settings in 0

Units and Filters

Appendix G Supervision of GE CARESCAPE Network and MMG

This chapter describes the recommended settings for supervision of both GE CARESCAPE Network and MMG.

G.1 Supervision of GE CARESCAPE Network

This section describes how to supervise the communication between the GE CARESCAPE Network and MMG.

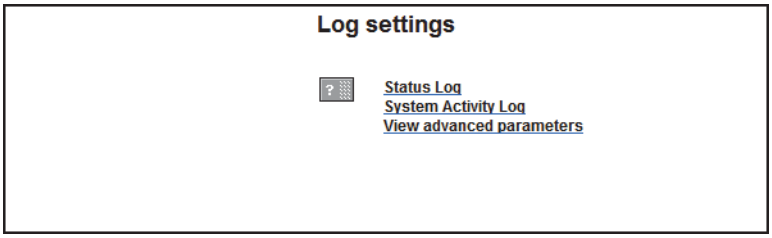
If the MMG has not received any discovery message (i.e. RWhat packet) from the GE CARESCAPE Network for 60 seconds, the connection is considered to be lost.

If the connection is lost, we want that a Status log should be sent to the Unite CM and also that an e-mail should be sent to an IT technician.

G.1.1 Logging

The MMG must be configured to send Status logs to the Unite CM. The Status log is used to store faults. Additionally, Activity logs can also be sent to the Unite CM for storing activities, such as messages and alarms. However, Activity logs cannot trigger a fault action (e.g. send an e-mail).

1. In the MMG start page, click **Configuration**.
2. Click **Advanced** tab.
3. Click Basic Administration.
4. Under Other, click **Logging**.



5. Click Status Log or "System Activity Log."

- For Status log, enter “xxx.xxx.xxx.xxx/FaultHandler,” where xxx.xxx.xxx.xxx is the IP address of the Unite CM.
- For System Activity log, enter “xxx.xxx.xxx.xxx/ActivityLogger,” where xxx.xxx.xxx.xxx is the IP address of the Unite CM.

6. Click Activate.

G.1.2 Fault Log settings

In all modules (MMG, Unite Connectivity Manager etc.), different levels of “seriousness” are set up for different kinds of faults. The default settings should normally be used but can be changed.

CARESCAPE Fault Log settings in the MMG

Some faults are CARESCAPE specific and the settings of the corresponding parameters are described here. It is possible to change and set the parameter “Seriousness” for different fault types in the logs. This is used for setting up actions in the Unite Connectivity Manager fault handler for all errors of a certain level of “seriousness.”

1. In the MMG start page, click “Configuration.”

2. Click the “Advanced” tab.
3. Click “Basic Administration.”
4. In the MMG System Setup page, click “Troubleshoot.”
5. Click “Module Fault List.”
6. The following CARESCAPE specific settings are found under the heading Ascii input module. Here, it is possible to set parameters regulating the seriousness of the different fault types.

Code	**Status**	**Persistent[1]**	**Seriousness[2]**
4-3-13	GE CARESCAPE network lost	Yes	Error
4-3-35	GE CARESCAPE protocol error	No	Warning
4-3-36	GE CARESCAPE Time_in_Alarm delta greater than 3 seconds	No	Warning
3-3-25	Module near capacity limit	Yes	Error
3-3-35	Capacity limit reached	Yes	Error
11-3-37	GE CARESCAPE time synchronization error	No	Warning

[1]Persistent means that the fault is shown in the Active Faults page as long as it remains.

[2]Default value.

NOTE: This information may be improved without prior notice.

CARESCAPE Log Entry information

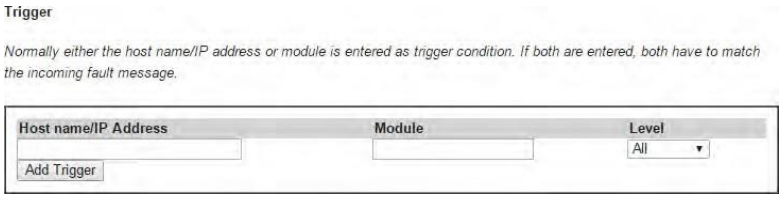
If a CARESCAPE related log entry is found in the Fault log, check this list for possible causes.

- GE CARESCAPE network lost:
  - Check network connection and router.
- GE CARESCAPE protocol error:
  - The MMG cannot interpret the received information.
- GE CARESCAPE Time_in_Alarm delta greater than 3 seconds:
  - A packet might have been lost for an ongoing alarm.
- Module near capacity limit:
  - CPU load is nearing capacity (more than 80% CPU load lasting for 50 seconds or more).
- Capacity limit reached:
  - more than 50 simultaneous alarms or
  - CPU load too high (more than 100% CPU load lasting for 50 seconds or more).
- GE CARESCAPE time synchronization error:
  - The time difference between CARESCAPE and MMG exceeds the pre-set limit.

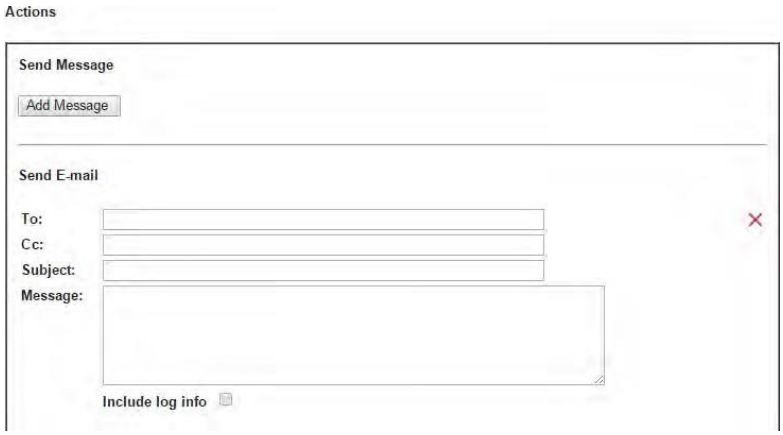
G.1.3 Configuring Fault Actions (Send E-mail)

The Unite CM can be configured to send an e-mail if the Unite CM receives a Status log.

1. From the Unite CM's Start page, click **Configuration**.
2. Select Fault Handling > Fault Actions.
3. Click "Add Action."
4. In the "Action Name field," enter an appropriate name.
5. In the "Trigger" section, enter the following:
6. Hostname/IP address: The IP address of MMG
7. Level: Select "All" to trigger on all levels of severity



8. In the "Actions" section, click the "Add E-mail" button.



9. In the "To"- and "Subject" fields, enter the recipient of the e-mail and subject, respectively.
10. Mark the "Include log info" check box to include the status log text in the e-mail.
11. Click the **Save**.

G.2 Supervision of MMG

This section describes how to supervise the MMG. There are two ways of supervising the MMG. Both ways must be configured.

- Configure the MMG to send Status logs to Unite CM. The MMG can only send Status logs if it is up and running. See G.1.1 Logging.
- Configure the Unite CM to ping the MMG to check if it is up and running. See G.2.1 Supervision.

If a Status log is sent from the MMG, or if the connection between MMG and Unite CM is lost, we want that an e- mail should be sent to an IT technician.

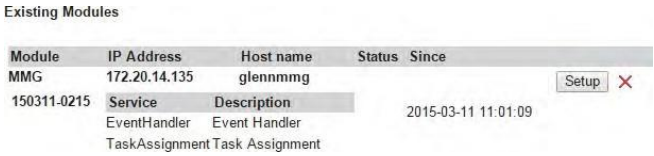
G.2.1 Supervision

The MMG can be supervised by the Unite CM, that sends supervision requests to the MMG with a specified interval (default 30 seconds). If the error relay is released on the MMG due

to error in the module, or if it does not respond to the request, the Unite CM generates a Status log.

1. From the Unite CM's Start page, click **Configuration**.
2. Select Supervision > Unite Modules.
3. In the text field, enter the IP address to the MMG to be supervised.
4. Click the "Survey Module" button.
5. Click the **Add** button next to the MMG in the list over modules.

6. Click the "Setup" button next to the MMG.
7. In the "Interval" field under the Supervision section, change how often the Unite CM should ping the MMG. Default is 30 seconds.



8. Click the **Save** button.

Appendix H Acceptance Test

The acceptance test is to ensure 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 is 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.

The following needs to be tested and verified:

Locations[a]:	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 is 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.
Suppression of Alerts on Silence	Verify a complete understanding and acceptance of the responsibility of enabling silence suppression capabilities.

[a]. A location is a place from where an alarm can be sent (bed, room, corridor, etc.)

Approval sheet
Location and test verification

Unit	Location	Monitor type	Tested	Comments
e.g CCU	e.g BED1	e.g DASH 4000	e.g Ok, Nok	

Sign off

Date:_____

Ascom FE:_____

Customer:_____

Site:_____

Approval sheet
Filter configuration, test and verification

Unit	Location	Filter	Filter setting	Tested	Comments
.g CCU	e.g BED1	e.g STOP	e.g *PVC	e.g Ok,NOk	

Sign off

Date:_____

Ascom FE:_____

Customer:_____

Site:_____

Approval sheet
Filter configuration, test and verification

Unit	Location	Filter	Filter setting	Tested	Comments
e.g CCU	e.g BED1	e.g STOP	e.g *PVC	e.g Ok,NOk	

Sign off

Date:_____

Ascom FE:_____

Customer:_____

Site:_____

Approval sheet
Suppression of Alerts on Silence

WARNING: This product provides methods to temporally suppress alerting and redirection for the duration of a silenced alarm and (optionally) for the duration of all active alarms after silenced on the patient monitor. Failure to take into account operation of the silence feature of the monitor by unqualified or un-trained personal may lead to improper delays and/or suppression of notifications leading to potential patient harm.

By utilizing the silence feature of the Patient Monitor it is possible to suppress alerting & temporarily discontinue redirection of alerts distributed by the MMG. This capability is not available as part of the default configuration, and requires additional configuration and acknowledgement of the deviation from the product standard notification behavior.

When configured properly this feature provides a means by which alerts may be temporarily paused during the time that the patient monitor is silenced. Upon expiration of silence on the monitor, or the generation of a new alarm, alerting provided by the MMG will resume.

Alternatively the product can be configured to persistently pause redirection and alerting for the duration of all active alarms, after silence has been engaged by the monitor.

A clear understanding of these features should be considered and risk managed by any organization before authorizing the use of this feature in individual units.

Unit	Silence Suppression	Re-alert after Silence	Tested	Comments
e.g CCU	e.g Enabled/Disabled	e.g Enabled/Disabled	e.g Ok,NOk	

Sign off

Date:_____

Ascom FE:_____

Customer:_____

Site:_____

TD 92654EN / 30 September 2020 / Ver. M

Ascom (Sweden) AB

Grimbodalen 2
SE-417 49 Göteborg
Sweden
Phone +46 31 55 93 00
www.ascom.com