DECT Messenger Fundamentals
Avaya Communication Server 1000

7.5
NN43120-120, 04.02
March 2012

Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer

“Documentation” means information published by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya generally makes available to users of its products. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of documentation unless such modifications, additions, or deletions were performed by Avaya. End User agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked Web sites referenced within this site or documentation provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Avaya provides a limited warranty on its Hardware and Software (“Product(s)”). Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language, as well as information regarding support for this Product while under warranty is available to Avaya customers and other parties through the Avaya Support Web site: http://support.avaya.com. Please note that if you acquired the Product(s) from an authorized Avaya reseller outside of the United States and Canada, the warranty is provided to you by said Avaya reseller and not by Avaya.

Licenses

Copyright

Third-party components

Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements (“Third Party Components”), which may contain terms that expand or limit rights to use certain portions of the Product (“Third Party Terms”). Information regarding distributed Linux OS source code (for those Products that have distributed the Linux OS source code), and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply to them is available on the Avaya Support Web site: http://support.avaya.com/Copyright.

Preventing Toll Fraud

“Toll fraud” is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of Toll Fraud associated with your system and that, if Toll Fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya Toll Fraud Intervention

If you suspect that you are being victimized by Toll Fraud and you need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support Web site: http://support.avaya.com. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Trademarks

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support Web site: http://support.avaya.com.

Contact Avaya Support

Avaya provides a telephone number for you to use to report problems or to ask questions about your Product. The support telephone number is 1-800-242-2121 in the United States. For additional support telephone numbers, see the Avaya Web site: http://support.avaya.com.

Contents

Chapter 1: New in this release

Features

There are no new features introduced with this release.

Revision history

March 2012	Standard 04.02. This document is up-issued to support Avaya Communication Server 1000 Release 7.5, and contains additional changes relating to updates in Release 4.1 of the Messenger software.
November 2010	Standard 04.01. This document is up-issued to support Avaya Communication Server 1000 Release 7.5.
June 2010	Standard 03.01. This document is up-issued to support Avaya Communication Server 1000 Release 7.0.
May 2009	Standard 02.01. This document is up-issued to support Communication Server 1000 Release 6.0.
October 2008	Standard 01.06 This document is up-issued to support Communication Server 1000 Release 5.5, and contains additional changes relating to updates in Release 4 of the Messenger software.
September 2008	Standard 01.02. This document is up-issued to support Communication Server 1000 Release 5.5, and contains changes relating to updates to the Messenger software.
May 2008	Standard 01.01 This document is issued to support Communication Server 1000 Release 5.5. Some of the information in this

new document was previously in DECT Fundamentals, NN43120-114.

Chapter 2: Avaya DECT Messenger Administrator Guide

This chapter contains information on the following topics:

Preface

This chapter contains an overview of Avaya DECT Messenger in general, and information for users of the eCONFIG module specifically. It contains important information on the underlying structure of the eCONFIG module, and on creating, deleting, and making changes to Users, Devices, and Groups.

This chapter does not cover all of the menus and associated menu items that are available in the eCONFIG module. Menus and associated menu items that are not covered require detailed technical background knowledge.

For information about the other menu parameters in the eCONFIG module, or information for any of the other modules in Avaya DECT Messenger, refer to *Avaya DECT Messenger Installation and Commissioning, NN43120-301.*

Avaya DECT Messenger overview

DECT Messenger provides a software tool, the eCONFIG, for making changes to the configuration. The eCONFIG is on either the same PC as the DECT Messenger software, or on another PC in the TCP/IP network. After you run eCONFIG on another PC, the number of items you can change is limited.

What is Avaya DECT Messenger

DECT Messenger is a software platform that allows message generation, message routing, and message protocol conversion. Figure 1: Avaya DECT Messenger on page 10 shows the inputs and outputs of DECT Messenger.

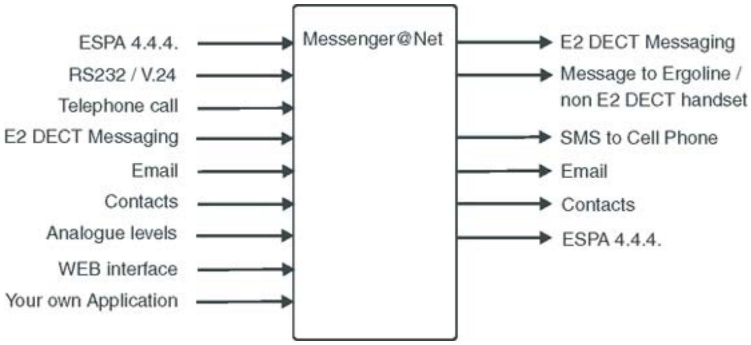


Figure 1: Avaya DECT Messenger

Message input

The following input can generate messages in DECT Messenger:

- ESPA 4.4.4 pager protocol: DECT Messenger can receive pager messages from ESPA 4.4.4-compatible pager equipment.
- RS232/V.24 serial input: many protocols are supported as input for generating a predefined message or a user defined message.
- DECT handset with E2 (Low Rate Messaging Services [LMRS]) messaging.
- E-mail to the DECT Messenger server PC: send a message from e-mail to a telephone set or SMS to cell phone or any other output on DECT Messenger.
- Switches (push button, toggle): message alerts generated by alarm contacts, door contacts, fire contacts, and so on.

- Analogue voltage/current levels: this form of message generation is used to guard industrial equipment. For example, equipment output messages can indicate pressure, temperature, and so on.
- Web interface from which you generate messages manually.
- Programs you write that communicate (using TCP/IP socket) with DECT Messenger: DECT Messenger provides a port on TCP/IP that is open to receive input data from this type of unique program.

Message output

DECT Messenger supports the following output:

- DECT E2 messages (up to 160 characters)

  Although DECT Messenger supports up to 160 characters, the DECT equipment or the handset can limit this number to 128, or even 48, characters. If the handset supports only 48 characters, the message is broken into sections and sent in parts to the handset.
- Messages sent to Ergoline or DECT extensions during ringing and after a call is connected

  Each device type can specify message length. Messages that are too long to be displayed are broken into sections suitable for the display devices.
- SMS messages to cell phones

  DECT Messenger can send SMS messages to cell phones. A modem or a box that behaves like an actual cell phone with a Subscriber Identity Module (SIM) card can be the interface to the cell phone provider.

  This option is mainly used as an alternative device. You can forward the message to a cell phone if a message to a DECT handset is not acknowledged.
- E-mail messages

  DECT Messenger can send e-mail using Simple Mail Transfer Protocol (SMTP) to any e-mail server.
- Digital output to control relays or similar equipment

  In the event of an alarm, use the relay contacts to control equipment such as lamps, door-contacts or hooters. Contacts are used as alternative devices (overflow) in case a message is not confirmed.
- ESPA 4.4.4 pager protocol

  DECT Messenger can send messages to paging equipment using the ESPA 4.4.4 protocol.

Modules overview

DECT Messenger consists of separate modules. There are three main groups of modules:

- Core—core components of the software, including security and maintenance tools.
- Input/Output modules—used for sending or receiving messages to or from supported devices.
- Add-Ons—optional expansion modules adapted for specific customer needs.
- Web Administrator—a web application that enables web-based access to a limited set of functions.

The following sections provide an overview of the modules. Detailed module descriptions are provided in *Avaya DECT Messenger Installation and Commissioning, NN43120-301*.

Core modules

The following core modules are available:

- eKERNEL

  The eKERNEL is the core software in the system and must always be present. eKERNEL is between the incoming and the outgoing modules and must always be running. The system does not operate if eKERNEL is absent or nonfunctional.

- eCONFIG/eGRID

  The eCONFIG module is used to set up and configure the system, messages, and message flows. The eCONFIG is a user-friendly variant of the eGRID.

- eGUARDIAN

  The eGUARDIAN is a integrated into eKERNEL and is used in conjunction with an input module that receives data at regular intervals. The eGUARDIAN module checks the data input at regular intervals. If the input is not received within a specified time period, the eGUARDIAN module sends a message indicating that an input is down.

- eBACKUP

  The eBACKUP module takes care of making a backup of the configuration database at regular intervals. -

- eTM

  The eTM (Task Manager) is a background module that automatically starts up other DECT Messenger modules in case they are down. Most of the core modules are typically deployed on the server PC. Exceptions are eCONFIG, which can optionally be deployed and used from a client PC (with limited configuration capabilities) and eTM, which is recommended to run on every DECT Messenger PC, client or server.

Incoming and outgoing modules

There is a wide range of incoming and outgoing modules available. They all communicate with the eKERNEL module. Each module has a specific incoming or outgoing function. This means that the incoming modules can receive messages and outgoing modules can send messages. provides an overview of the modules.

Table 1: Incoming and outgoing Modules

Module Name	Function	Incoming	Outgoing
eCAP	V.24/RS232 interface and protocol converter.	Yes	-
eESPA	Input/Output module for the connection to pager interfaces.	Yes	Yes
eAPI	Input device for custom-made programs.	Yes	-
eIO	Digital and analogue inputs and digital outputs (contacts and switches).	Yes, analogue levels and digital levels (contacts)	Yes, switches
eWEB	Web interface.	Yes	-
eSMTP-server	Receiving e-mail messages.	Yes	-
eSMTP (client)	Sending e-mail messages.	-	Yes
eDMSAPI	Sending and receiving E2-DECT messages using the CSTA interface.	Yes, receiving E2-DECT messages	Yes, sending E2-DECT messages
eASYNC	Asynchronous modem interface to cell phone SMS provider, or to wide area paging system.	-	Yes
eLOCATION	Location detection after a call is made from a DECT handset or when LRMS (E2) is sent from DECT handset.	In addition to the eCSTA module.	
eVBVoice	Interactive Voice Responds used to various message types	Yes	Yes
eSNMP	Receive an SNMPv1 or SNMPv2c trap from an SNMP sending process or equipment	Yes	
eSMS	Send SMS message to a mobile phone. Inbound SMS can be used to confirm alarm	Yes (to confirm)	Yes

Add-on modules

The add-ons are input/output modules tailored to specific customer needs. They are not covered by the standard product documentation.

- Web Administrator

  The Web Administrator is a web-based user interface that offers access to certain configuration functions, sending messages to users and groups, reporting functions, and so on.
- Logging

  The eKERNEL has built-in logging functionality for technical purposes known as eLOG. The log files are located in the following directory: [INSTALLDIR]\Logs where [INSTALLDIR] is the installation directory. The default installation directory is: C:\Program Files\Avaya\Avaya DECT Messenger\.

eCONFIG basic concepts

The system configuration is stored in a database. You use the eCONFIG module to make changes to the configuration. This section explains how the eCONFIG module uses the database.

You can use the eCONFIG on the local DECT Messenger server PC. You can also install the eCONFIG on a remote PC to do remote configuration maintenance. Database handling is different for local and remote situations.

eCONFIG (local) on the DECT Messenger server PC

After the eCONFIG is installed on the DECT Messenger server PC, the database is handled as shown in eCONFIG (local) on the server PC.

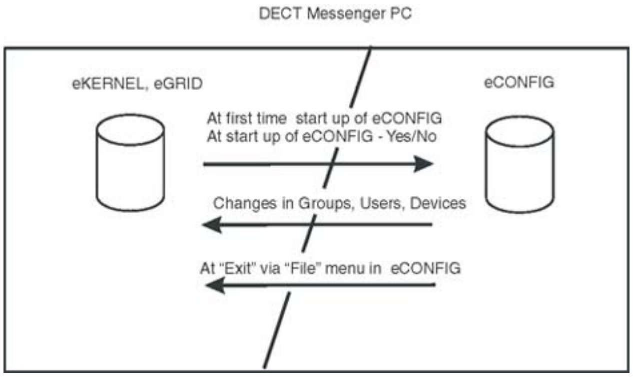

DECT Messenger PC
eKERNEL, eGRID
eCONFIG
At first time start up of eCONFIG
At start up of eCONFIG - Yes/No
Changes in Groups, Users, Devices
At “Exit” via “File” menu in eCONFIG

Figure 2: Database handling after eCONFIG is on local PC

After you open the eCONFIG for the first time, the eCONFIG makes a copy of the operational configuration database in DECT Messenger. This copy is stored locally on the server PC where eCONFIG is running. If you make configuration changes using the eCONFIG, these changes are stored in the local working copy of the database in the eCONFIG. To make these changes active, you must close down all the DECT Messenger modules and then close the eCONFIG using the **File > Exit** menu. The operational database is deleted automatically, and the database from the eCONFIG is saved into the DECT Messenger directory and becomes the new operational database. After you restart the modules that you closed down, the new configuration becomes active.

After you make changes in Users, Groups, or Devices, the changes are saved in the eCONFIG database, as well as in the operational database, and so are immediately activated.

Note:

While making configuration changes with eCONFIG, ensure that no one else is making changes in the operational database. If there are other pending changes, an error may occur after you shut down the eCONFIG and attempt to apply the configuration changes.

Note:

If there are monitored devices in the active configuration, and one of these devices initiates a follow-me, the diversion information is stored in the active database. Therefore, you cannot restore the eCONFIG database, and all the changes that you make are lost (except for the changes in Users, Groups, and Devices).

eCONFIG (remote) on remote PC (client) in the network

After the eCONFIG is installed on a remote PC (not the DECT Messenger server PC) in the network, the database is handled as shown in Figure 3: Database handling after eCONFIG is installed on a remote PC on page 15.

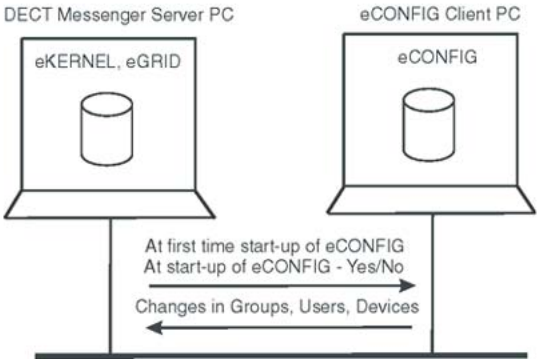

DECT Messenger Server PC
eCONFIG Client PC
eKERNEL, eGRID
eCONFIG
At first time start-up of eCONFIG
At start-up of eCONFIG - Yes/No
Changes in Groups, Users, Devices

Figure 3: Database handling after eCONFIG is installed on a remote PC

After you open the eCONFIG for the first time at the remote PC, a copy is made of the configuration database of DECT Messenger. This copy is stored on the remote PC where the eCONFIG is running. You cannot make system configuration changes in this database, but you can make changes in Users, Groups, and Devices.

After you make changes in Users, Groups, or Devices, these changes are stored in the eCONFIG database on your PC. The changes are also immediately stored in the operational database on the DECT Messenger (server) PC and are, therefore, immediately active.

Note:

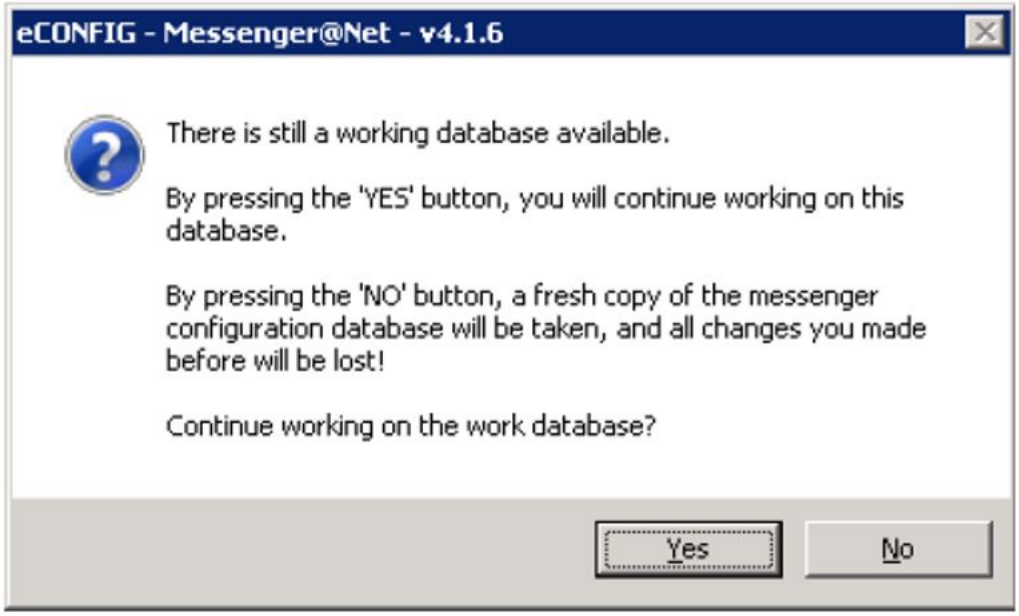
If there is more than one eCONFIG active at the same time, on different PCs, the individual eCONFIG databases are not updated/synchronized after a user makes a change in one eCONFIG. Only the database in the eCONFIG module where the change is made is updated, together with the operational database. Changes made in Groups using the eWEB interface are not written into the databases of the eCONFIG modules — these changes are only written into the operational database.

Note:

The database is never saved to the server PC when you work on a remote PC.

Restarting eCONFIG

When you start eCONFIG, the program may find a working database in the local maintenance directory. If so, eCONFIG asks you whether you want to continue with this database or retrieve a fresh copy from the operational database.



eCONFIG - Messenger@Net - v4.1.6

There is still a working database available.

By pressing the 'YES' button, you will continue working on this database.

By pressing the 'NO' button, a fresh copy of the messenger configuration database will be taken, and all changes you made before will be lost!

Continue working on the work database?

Figure 4: Message box asking which database to use

Avaya recommends choosing **No** to make a fresh copy of the operational database and ensure that there is no database inconsistency.

DECT Messenger concepts

DECT Messenger receives alarms (messages) from input modules. Understanding how these incoming alarms are processed is an important step towards understanding the eCONFIG menu structure.

Figure 5: Alarm processing structure on page 17 shows the relation among the modules and how messages are processed.

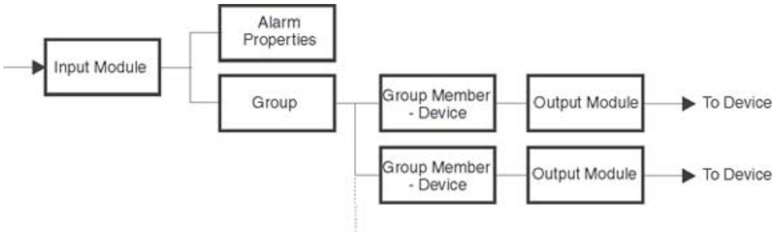
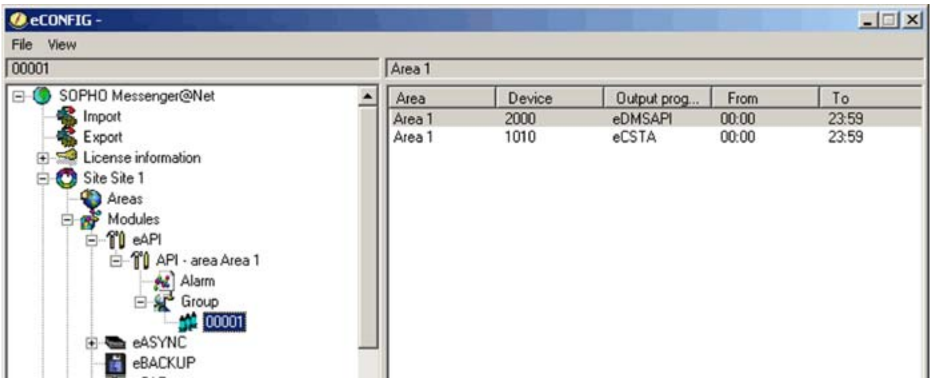


Figure 5: Alarm processing structure

Alarms originate at an input program (input module). An incoming alarm carries an alarm identifier and a group identifier. The alarm identifier must match an identifier in the Alarm Properties functional block, which specifies how the alarm is processed (priority, time intervals, and so on). The group identifier determines the final destination. The incoming group identifier must match a group identifier in the Groups functional block, which contains one or more output destinations (that is, the group members). The group members are the devices assigned to a Group.

Figure 6: eCONFIG on page 17 shows the main window of eCONFIG with an example of an input module (the application programming interface [eAPI]). The eAPI input module is found in eCONFIG in the **Modules > eAPI** menu. Select the instance of the module as it appears on your screen (in this example, the menu selection is **Modules > eAPI > API - area Area 1**). Each input module displays different properties.



Area	Device	Output prog...	From	To
Area 1	2000	eDMSAPI	00:00	23:59
Area 1	1010	eCSTA	00:00	23:59

Figure 6: eCONFIG

The following explanations relate to the blocks in Maintaining DECT Messenger using eCONFIG on page 19:

- Input Module

  The Alarm carries two different identifiers from the input module to the actual Kernel: the alarm identifier and the group identifier. The identifier provides the message for the output device.

You can set or change the properties of an input module.

- Alarm Properties

  The alarm identifier is used to determine how the alarm is processed. Specifications are in the **All Alarms** menu (for more information, see eCONFIG main window on page 20). Examples of the alarm properties are Priority, Repeat Interval Time, and so on.

  Note:

  There are alarm identifiers predefined in the system configuration. Therefore, it is not necessary to define all alarm identifiers. For information on available alarm properties, see *DECT Messenger Installation and Commissioning, NN43120-301*.

- Group

  The group identifier that originates at the input module determines the group to which the alarm must be sent. In Maintaining DECT Messenger using eCONFIG on page 19, the group identifier is 00001. The group identifier can be a group name or any string of characters.

- Group Member -- Device

  The group is composed of group members, and each group member is an actual device (for example, an Ergoline, a DECT handset, or an e-mail address). The output device can be a member of more than one group. For example, a DECT handset with extension number 2000 can be assigned to more than one group as a group member. In Figure 6: eCONFIG on page 17, Group 00001 has two devices (2000 and 1010). Device 2000 uses the output program eDMSAPI, which means that Device 2000 is a DECT handset using E2 messaging.

- Output Module - Output Program

  An output device makes use of an output module, also referred to as an output program. You can specify settings in the output module to process the output alarm.

Refer to the following sections for instructions on creating, deleting, and changing parameters for Groups, Users, and Devices:

- Managing devices on page 22
- Managing groups on page 31
- Managing group members on page 37
- Managing users on page 42

Maintaining DECT Messenger using eCONFIG

This chapter explains the eCONFIG user interface and available functionality.

- Starting the eCONFIG on page 19

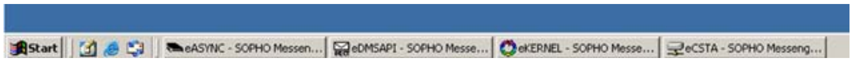
Starting the eCONFIG

The procedures below describe the steps necessary to start the eCONFIG module.

Before starting eCONFIG:

1. Ensure that DECT Messenger is correctly installed and already preconfigured by a technician.
2. Ensure that the Kernel software is installed and running.

   If you are on a remote PC (not the server PC), ensure that the main server is booted. If you are using the server PC, an icon appears in the Windows task bar to indicate that the eKERNEL is running.

   If other modules are also running, an icon is displayed for each (for example, the eDMSAPI).

To launch the eCONFIG configuration utility:

1. Use the shortcut available in the Start Menu:

   Start > Programs > Avaya DECT Messenger > eCONFIG
2. Enter your login information.

   Log in with the username and password provided by your system manager. If you are the system manager, and you have not changed any usernames and passwords yet, log in with the default login. The default login is admin (username), admin (password).
3. Select the database.

   Note:

   The eCONFIG asks you which database you want to use. Ensure that you read the information on database handling in eCONFIG basic concepts on page 14 before proceeding.

You have two options for database selection:

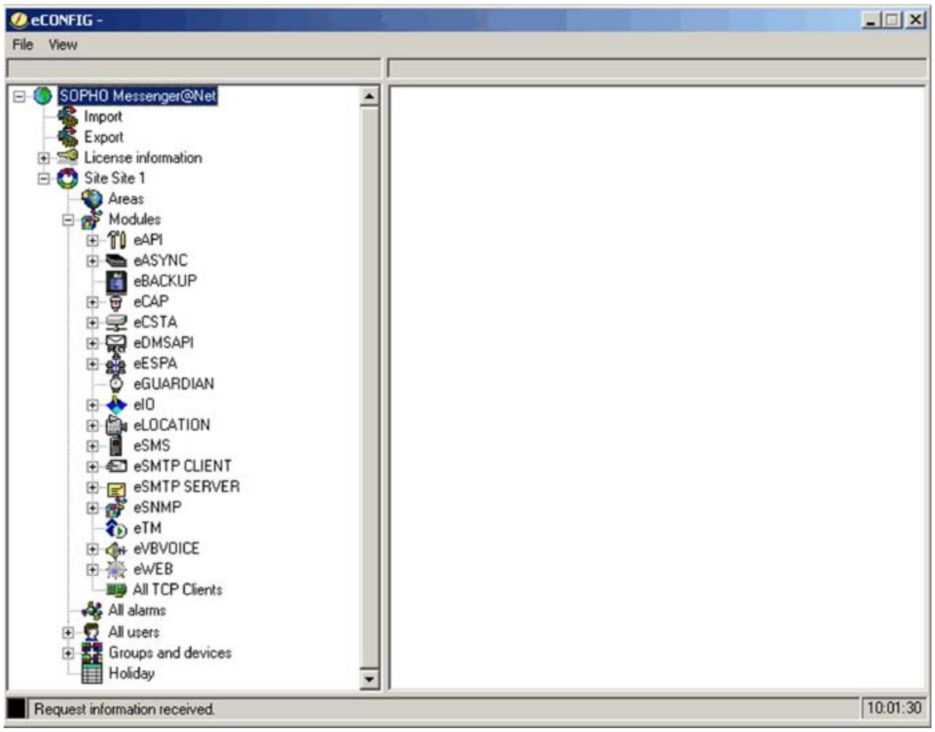
- Click **YES**: the eCONFIG uses the database that is still available in the eCONFIG module from a previous session. This database can be an old database.
- Click **NO**: the eCONFIG makes a fresh copy of the operational database from the DECT Messenger server. Avaya recommends that you choose this option. It ensures that you have a copy of the actual operational database. If you work on a remote PC, you must select this option to avoid conflicts with changes made from other locations by other users.

4. The eCONFIG main window opens.

   Detailed information is provided in eCONFIG main window on page 20.

eCONFIG main window

The main eCONFIG window is shown in eCONFIG main window.



Request information received.

10:01:30

Figure 7: eCONFIG main window

Note:
The contents of the eCONFIG window are different for each user or for each system configuration. eCONFIG main window shows all the menu items that are possible.

The following menu items are available:

- Import/Export menu: provides the option to import configuration data into tables in the configuration database, or to export configuration data from the configuration database tables. The file type is .csv.

  Note:

  Do not use the Import/Export menu items if you do not have detailed configuration database knowledge. If you make mistakes, it can corrupt your system.
- License information: provides information about the current licenses that are active in your DECT Messenger. You cannot make license changes from this menu.
- Site Site 1: indicates the location of the eKERNEL (core) software. There is typically only one eKERNEL in a system, so there is only one site displayed. (In exceptional cases, there can be more than one site, but only one eKERNEL (that is, one site) can be active at any given instant.
- Areas: indicates the subdivisions in a site. Areas are used only if you have a connection from your DECT Messenger to more than one DECT Mobility Card (DMC) with DECT. For each connection from your DECT Messenger to a DMC system or an IP DECT system, you must specify a different area. Use a number to identify the area. The area number is used in the various modules in DECT Messenger. Note that in almost all installations you have only one area.
- Modules: provides an overview of all the modules in the Messenger.

  Note:

  The list of modules can differ for each user. The list of modules is displayed only if you have view/edit rights.

  Note:

  The **All TCP Clients** menu item is not a module. **All TCP Clients** provides information about the module TCP/IP connections. You cannot make any configuration changes from this menu.
- All Alarms: provides a list of all alarm specifications available in Messenger.

  Note:

  The alarm specification is linked to an input module. Therefore, to create a new alarm specification, you must use the Module menu. From the All Alarms menu, you can make changes only to existing alarm specifications.
- All Users: defines all users. Note that there are two separate groups of users: eCONFIG users and eWEB users. If you have sufficient rights, you can change user settings and add new users from this menu.
- Groups and devices: use this menu to make changes in group and device characteristics. You cannot create new groups here because a group is always uniquely linked to an input

module. You can, however, create new devices here because a device does not have a unique relationship with only one group.

- Holiday: use this menu to specify the public holidays. This information is used for the group members. You enable the specified holidays in the properties for each group member.

Note:

If you are using the eCONFIG on a remote PC, you cannot make changes to property settings. You can change only Users, Groups, and Devices.

Managing devices

The following sections provide information that explain the following DECT Messenger tasks:

- creating a new device
- changing the parameters of an existing device
- editing device parameters

The following are examples of device types in DECT Messenger:

- DNR in the DMC
- Directory Number (DN) in SIP DECT
- e-mail address
- cell phone number (for SMS)
- relay contacts

You must know the properties of each device type relative to the equipment that hosts it (that is, device properties in the DMC, in the Mail Server, and so on).

Note:

Task procedures are explained in the following sections. To carry out these procedures, you must have sufficient user rights to access all the menus that are used in these procedures. If you do not have sufficient rights, you cannot see the menu options described, or you see them but cannot make changes.

Creating a new device

Complete the following steps to create a new device.

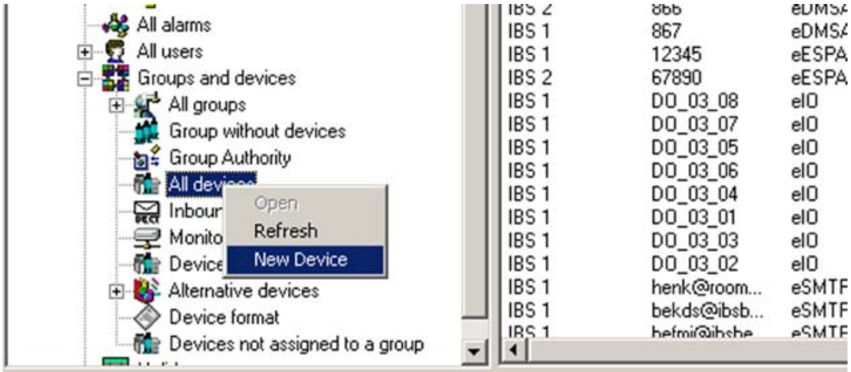
Creating a new device

1. Access the eCONFIG **Groups and Devices** menu.
    - Open eCONFIG.

- Expand the **Groups and Devices** menu by clicking the **+** to the left of it.

2. Add a new device.

   - Right-click the **All Devices** parameter.
   - Select **New Device** as shown in the following example:

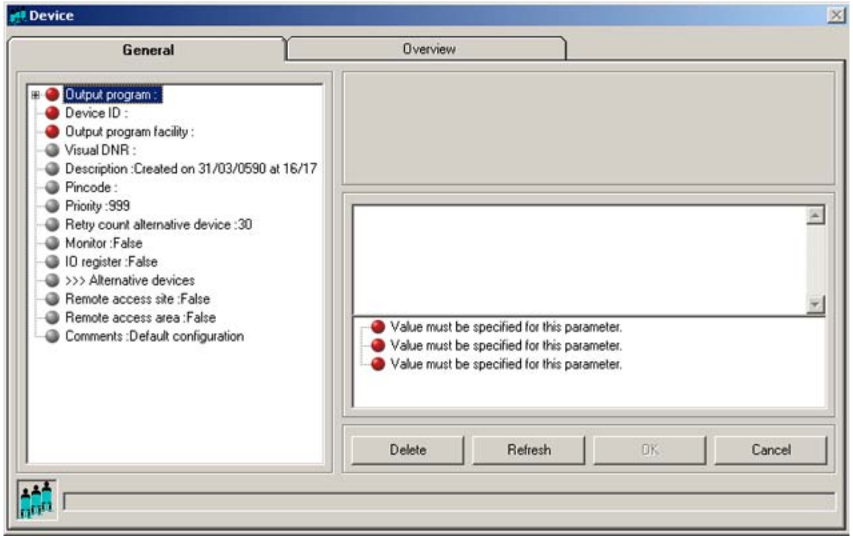


IBS 2	866	eDMS
IBS 1	867	eDMS
IBS 1	12345	eESPA
IBS 2	67890	eESPA
IBS 1	DO_03_08	eIO
IBS 1	DO_03_07	eIO
IBS 1	DO_03_05	eIO
IBS 1	DO_03_06	eIO
IBS 1	DO_03_04	eIO
IBS 1	DO_03_01	eIO
IBS 1	DO_03_03	eIO
IBS 1	DO_03_02	eIO
IBS 1	henk@room...	eSMTP
IBS 1	bekds@ibsb...	eSMTP
IBS 1	hefmi@ibshe	eSMTP

3. Set parameters for the new device.

   Note the following when setting parameters:

   - A red bullet before an item indicates that the item is mandatory.
   - Some items contain default parameter values.
   - Avaya recommends that you use the **Browse** option, when present, to define a location, rather than typing an entry.



- Output program :
- Device ID :
- Output program facility :
- Visual DNR :
- Description :Created on 31/03/0590 at 16/17
- Pincode :
- Priority :999
- Retry count alternative device :30
- Monitor :False
- IO register :False
- >>> Alternative devices
- Remote access site :False
- Remote access area :False
- Comments :Default configuration

- Value must be specified for this parameter.
- Value must be specified for this parameter.
- Value must be specified for this parameter.

   The parameters are described in Device parameters on page 25.

4. Confirm your choices.

   Click **OK** and follow the instructions on screen.

5. Assign the new device to a group (optional).

Select **All Groups** from the **Groups and Devices** menu, or **Group** from the input module menu of your choice.

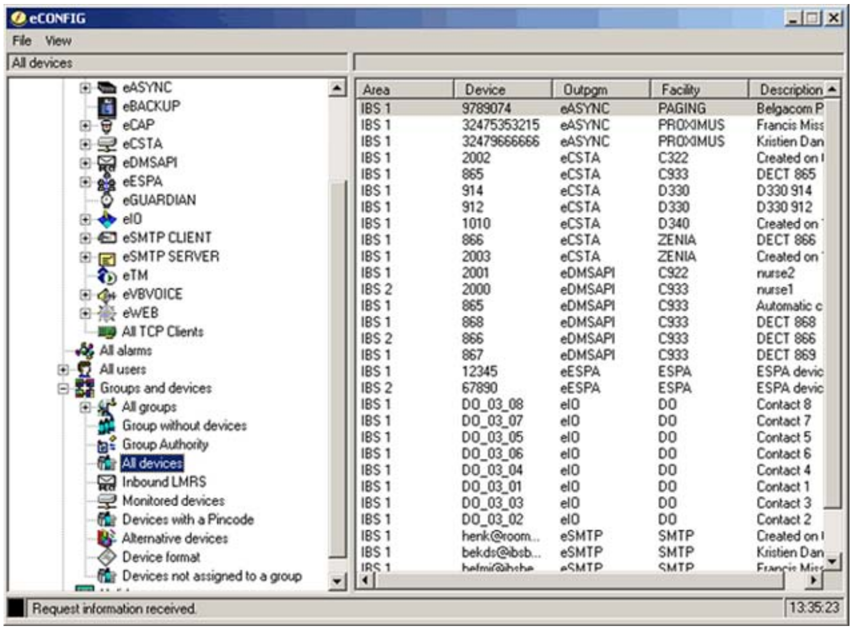
Changing device parameters

Complete the following steps to change device parameters.

Changing device parameters

1. Access the eCONFIG **Groups and Devices** menu.
   - Open eCONFIG.
   - Expand the **Groups and Devices** menu by clicking the **+** to the left of it.
2. Open the All Devices information window.

   Left-click the **All Devices** parameter. The following window appears:

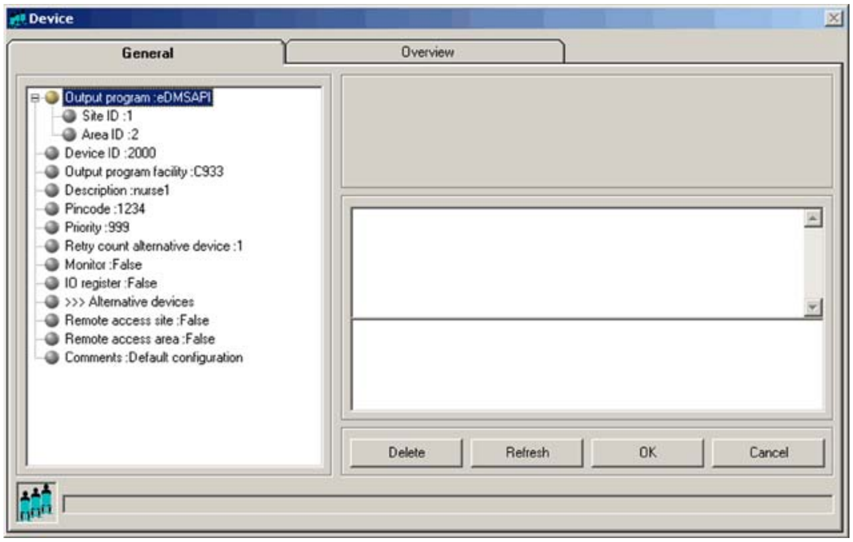


Area	Device	Outpgm	Facility	Description
IBS 1	9789074	eASYNC	PAGING	Belgacom P
IBS 1	32475353215	eASYNC	PROXIMUS	Francis Miss
IBS 1	32479666666	eASYNC	PROXIMUS	Kristien Dan
IBS 1	2002	eCSTA	C322	Created on
IBS 1	865	eCSTA	C933	DECT 865
IBS 1	914	eCSTA	D330	D330 914
IBS 1	912	eCSTA	D330	D330 912
IBS 1	1010	eCSTA	D340	Created on
IBS 1	866	eCSTA	ZENIA	DECT 866
IBS 1	2003	eCSTA	ZENIA	Created on
IBS 1	2001	eDMSAPI	C922	nurse2
IBS 2	2000	eDMSAPI	C933	nurse1
IBS 1	865	eDMSAPI	C933	Automatic c
IBS 1	868	eDMSAPI	C933	DECT 868
IBS 2	866	eDMSAPI	C933	DECT 866
IBS 1	867	eDMSAPI	C933	DECT 869
IBS 1	12345	eESPA	ESPA	ESPA devic
IBS 2	67890	eESPA	ESPA	ESPA devic
IBS 1	DO_03_08	eIO	DO	Contact 8
IBS 1	DO_03_07	eIO	DO	Contact 7
IBS 1	DO_03_05	eIO	DO	Contact 5
IBS 1	DO_03_06	eIO	DO	Contact 6
IBS 1	DO_03_04	eIO	DO	Contact 4
IBS 1	DO_03_01	eIO	DO	Contact 1
IBS 1	DO_03_03	eIO	DO	Contact 3
IBS 1	DO_03_02	eIO	DO	Contact 2
IBS 1	henk@room...	eSMTP	SMTP	Created on
IBS 1	bekds@ibsb...	eSMTP	SMTP	Kristien Dan
IBS 1	hefmi@ibsbe	eSMTP	SMTP	Francis Miss

Request information received.

13:35:23

3. Select the device of your choice.
   - In the right panel, browse in the list of devices in DECT Messenger.
   - Double-click the device that you want to edit. The Properties window of the device opens:



- Output program :eDMSAPI
  - Site ID :1
  - Area ID :2
- Device ID :2000
- Output program facility :C933
- Description :nurse1
- Pincode :1234
- Priority :999
- Retry count alternative device :1
- Monitor :False
- IO register :False
- >>> Alternative devices
- Remote access site :False
- Remote access area :False
- Comments :Default configuration

4. Change the parameters.

   Click the name of the property you want to change. If you edit the parameters, note the following:

   - You cannot change the **Output Program**, the **Site ID**, the **Area ID**, or the **Device ID**.
   - Avaya recommends that you use the **Browse** option, when present, to define a location, rather than typing an entry.

   The parameters are described in Device parameters on page 25.

5. Confirm your choices.

   Click **OK** and follow the instructions on the screen, if applicable.

Deleting a device

To delete a device, follow Changing device parameters on page 24; at Step 4, click the **Delete** button. DECT Messenger asks you to confirm the action. After you confirm the action, the device is deleted immediately.

Device parameters

As in previous sections, you can specify the following parameters for a device:

- Output Program

  This field specifies the output program that processes a request. A device can be defined in more than one module. The indicated application threads the message using the capabilities of the infrastructure. The eDMSAPI can, for example, send E2 messages (non-voice-call to extensions such as DECT C4050 and C4060). The supported output programs are currently:

- eASYNC for sending SMS to PROXIMUS, or KPN and PAGING to BELGACOM.

- eDMSAPI for sending E2 messages to DECT handsets that support E2 (LRMS).

- eESPA for sending messages to an ESPA 4.4.4 interface (pager equipment).

- eIO for enabling/disabling discrete output contacts.

- eSMTP for sending e-mail to an e-mail provider.

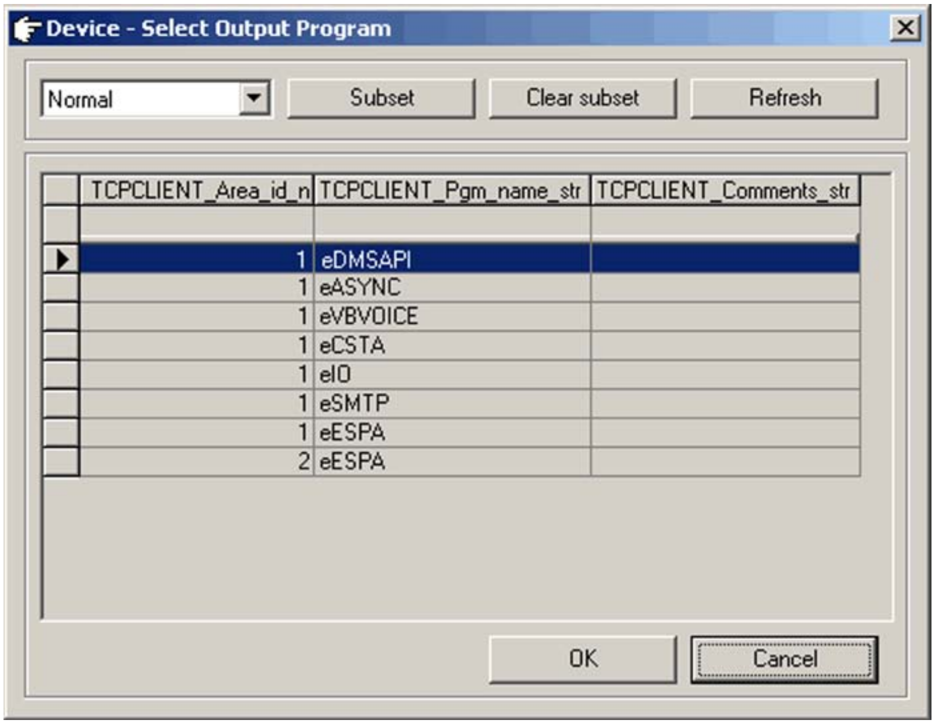
- eSMS for sending SMS messages to GSM phones.

Note:

The output program is associated with a Site ID (which is typically 1) and an Area ID. If there is more than one entry of the same output program, each one can have a different area. Select the correct area.

Note:

Selecting the output program is only possible when you create a new device. Always use the **Browse** button to select the output program. Figure 8: Select Output Program browser window on page 26 shows the browser window.



TCPCLIENT_Area_id_n	TCPCLIENT_Pgm_name_str	TCPCLIENT_Comments_str
1	eDMSAPI	
1	eASYNC	
1	eVBVOICE	
1	eCSTA	
1	eIO	
1	eSMTP	
1	eESPA	
2	eESPA	

Figure 8: Select Output Program browser window

- Device ID

The device ID is the actual identifier of the device in the output equipment.

Device ID consists of <board-id> and <index> delimited with #. For example, 04#01.

Table 2: Variable definitions

Variable	Definition
<board-id>	A fixed length value, in the range of 01 to 32, which indicates the DMC card ID in a PBX.
<index>	A variable length value, in the range of 00 to 509, which indicates the index of a DECT handset subscribed to a DMC card.

The <board-id> value is calculated differently against a system type as follows:

- For a small system, such as Option 11C, the <board-id> of a DMC card placed in the Main Cabinet/Chassis is the same as the card slot number where the DMC card is installed (in the range of 01 to 10). DMC card numbering in Expansion Cabinets/ Chassis continues sequentially in the range 11 to 20.

  The following table illustrates Device ID numbering for a small system.

  Table 3: Device ID numbering for a small system

Cabinet/Chassis	Card slot	<board id>	Device ID
Main Cabinet or Main Chassis + Chassis Expander	1	1	01#xxx
	2	2	02#xxx
	…	…	…
	9	9	09#xxx
	10	10	10#xxx
Expansion Cabinet or Expansion Chassis 1 + Expander	1	11	11#xxx
	2	12	12#xxx
	…	…	…
	9	19	19#xxx
	10	20	20#xxx

- For a large system, such as Avaya Communication Server 1000E, <board-id> falls in the range of 01 to 32, and is calculated with the formula: <board-id> = 16 * <shelf_number> + <card_slot_number> + 1

  The following table illustrates Device ID numbering for a large system.

  Table 4: Device ID numbering for a large system

Shelf	Card slot	<board id>	Device ID
0	0	1	01#xxx

Shelf	Card slot	<board id>	Device ID
0	1	2	02#xxx
…	…	…	…
0	14	15	15#xxx
0	15	16	16#xxx
1	0	17	17#xxx
1	1	18	18#xxx
…	…	…	…
1	14	31	31#xxx
1	15	32	32#xxx

The following table shows examples of valid device IDs.

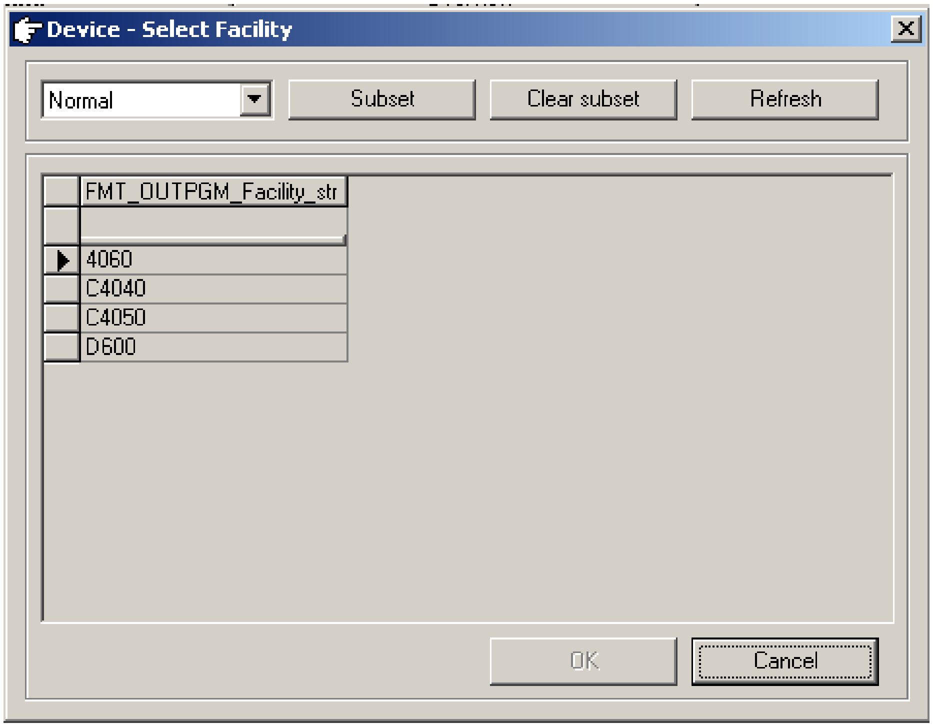
Table 5: Example device IDs

DMC Card installed in	Device ID
2nd slot on Main Cabinet on Avaya CS1000 M, handset is subscribed with index 01	02#01
7th slot of shelf 0 on CS 1000E, handset is subscribed with index 123	08#123
14th slot of shelf 1 on CS 1000E, handset is subscribed with index 03	31#03

- Output program facility

  The indicated application threads the message using the capabilities of the output device. The display of extensions can differ in character length, and so on. Therefore, DECT Messenger must know to which device type the message is being sent (for example, C4050 or 4060 for eDMSAPI).

  Use the Browse button to select the correct output program facility. Figure 9: Device Select Facility on page 29 shows the selection window for the eDMSAPI.



FMT_OUTPGM_Facility_str
4060
C4040
C4050
D600

Figure 9: Device Select Facility

- Description

  The Description field is used to enter a description of the device. The description is used to show information about the devices in the web interface (for example, DECT: John Peterson).

- Pincode

  The pincode is used to confirm messages using the eDMSAPI (IC). Confirmation means that an active alarm on the device is reset from the same or another extension. To reset the alarm using eDMSAPI (IC), the CLI of the calling extension must be entered here as the pincode.

- Priority

  Reserved for future use.

- Retry count alternative device

  Retry count alternative device defines how many times the application tries to deliver the message before switching to an alternative device (if one is defined in the list of **Alternative Devices** in the **Groups and Devices** menu). The default value is 30. Therefore, if an alarm has a silence interval (defined in the alarm properties) of 120 seconds, the alarm is removed for this device after one hour (and set for the alternative device, if defined).

  A value of 0 indicates that the application never tries to send the message to an alternative device, and that the alarm is sent to the device every silence interval until the alarm is reset by the input program, for example (a reset). A value of 1 indicates that after one attempt, the application clears the message for this device and send the message to the alternative device, if defined.

Note:

In this second case (value=1), the switch to the alternative device is immediate (that is, there is no silence interval between the two calls). Therefore, you must ensure that there are no loop conditions defined in the list of alternative devices.

A value of 2 indicates that the alternative device is contacted after the second attempt.

- IO Register

  This parameter is only applicable for devices that are assigned to output program eDMSAPI.

  All devices with this value set to **True** are monitored by the eDMSAPI to see if an E2 message is sent. After a device sends an E2 message, the message always goes to DECT Messenger directly (and not to the destination number). Messages sent to DECT Messenger are processed by DECT Messenger in the same way that messages from other input devices are processed. There must be a correct specification in the eDMSAPI inbound configuration that points to a group and an alarm. The message is sent to the group members in the group that is assigned to the inbound configuration in the eDMSAPI.

- Alternative devices

  Use this parameter to assign one or more alternative devices to a device. After you click this item, a panel at the right side of the window displays the list of possible alternative devices. Select **New** from the menu to add an alternative device. Select **Edit** to make changes in the list of alternative devices already assigned to this device.

- Remote access site

  The **Remote access site** parameter is only applicable when you have more than one site, and you are using the web interface. A web server (eWEB) and a device are each assigned to only one site; if both are assigned to the same site, you can see the device from the web interface. Devices assigned to sites other than that to which the web server is assigned are only visible if the **Remote access site** parameter is set to **True**.

- Remote access area

  The **Remote access area** parameter is only applicable when you have more than one area, and you are using the web interface. A web server (eWEB) and a device are each assigned to only one area; if both are assigned to the same area, you can see the device from the web interface. Devices assigned to areas other than that to which the web server is assigned are only visible if the **Remote access area** parameter is set to **True**.

- Comments

  This field is informational only, and can contain remarks from the administrator.

Managing groups

Creating a new group

Complete the following steps to create a new group.

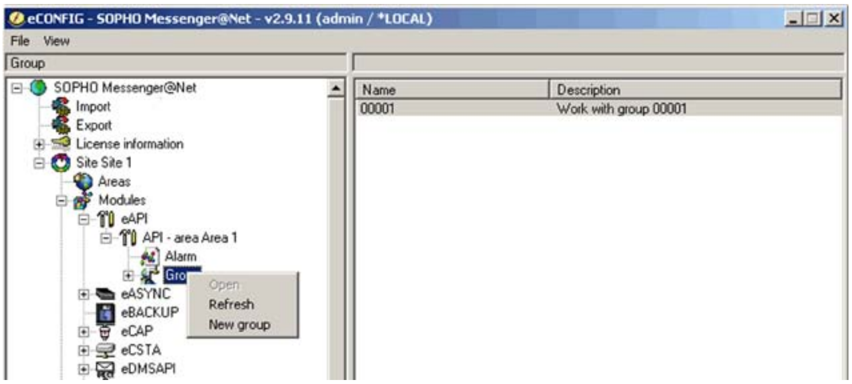
Creating a new group

1. Open eCONFIG.
2. Access the pop-up menu of the input module for which you want to create the new group.

   - Select the input module for which you want to create a new group from the **Modules** menu.

   Note:

   A group is always associated with an input module. You cannot create a new group in the **Groups and Devices** menu.

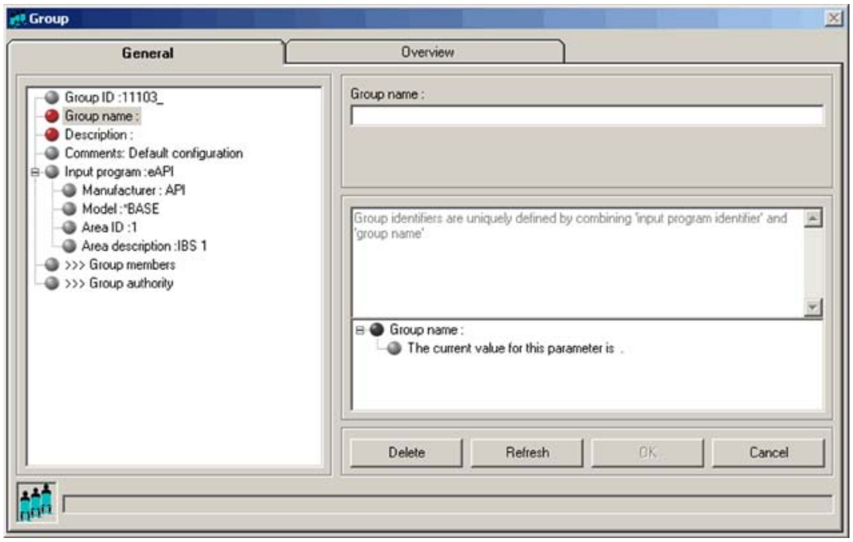


Name	Description
00001	Work with group 00001

   - Expand the input module for which you want to create a new group. The instances (**eAPI - area Area 1** in this example) of the input module are displayed.
   - Expand the instance. The submenu items **Alarm** and **Group** are displayed.
   - Expand **Group** to view all the groups for this instance of the input module.
   - Right-click the **Group** parameter. A pop-up menu opens.

3. Create the new group and set the parameters.

   - Select **New** Group from the **Group** pop-up menu.
   - Enter values for the group parameters.



Group ID :11103_
Group name :
Description :
Comments: Default configuration
Input program :eAPI
Manufacturer : API
Model :*BASE
Area ID :1
Area description :IBS 1
>>> Group members
>>> Group authority

Group name :

Group identifiers are uniquely defined by combining 'input program identifier' and 'group name'

Group name :
The current value for this parameter is .

After you enter the parameters, note the following:

- A red bullet before an item indicates that the parameter is mandatory.
- Some items contain default parameter values.
- Avaya recommends that you use the **Browse** option, when present, to define a location, rather than typing an entry.

Note:

The group name that you enter must match the group name entered for the input module. If the input module is an eAPI, eCAP, or eESPA, the group name matches that in the external system. Therefore, you must know the external system that delivers the group name.

Note:

The input module provides not only a group name, but also an alarm. Ensure that the alarm from the input module corresponds to an alarm in the alarms list. Ask a system specialist if you are uncertain about this.

The parameters are described in more detail in Group parameters on page 34.

4. Confirm your choices.

   Click **OK** and follow the instructions on the screen, if applicable.

Changing group parameters

Complete the following steps to change group parameters.

Changing group parameters

1. Open eCONFIG.
2. Select the input module for which you want to change the group parameters.

Select the input module for which you want to change group parameters from the **Modules** menu.

Note:

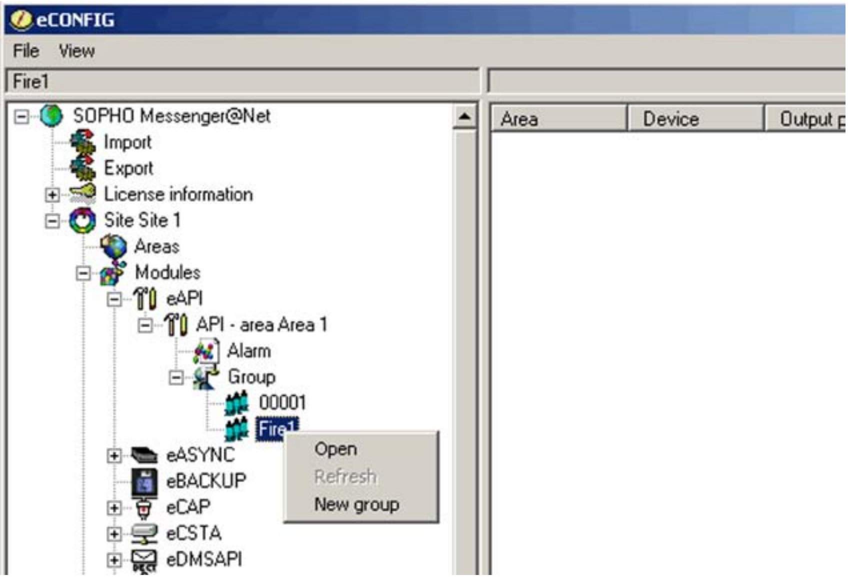
A group is always associated with an input module. However, to change group parameters, you can also select a group from the **Groups and Devices** menu.

3. Open the group.

    - Expand the input module for which you want to create a new group. The instances (eAPI - area IBS 1 in this example) of the input module are displayed.
    - Expand the instance. The submenu items **Alarm** and **Group** are displayed.
    - Expand the **Group** item to view all the groups for this instance of the input module.
    - Right-click the **Group** parameter. A pop-up menu opens.

    Note:

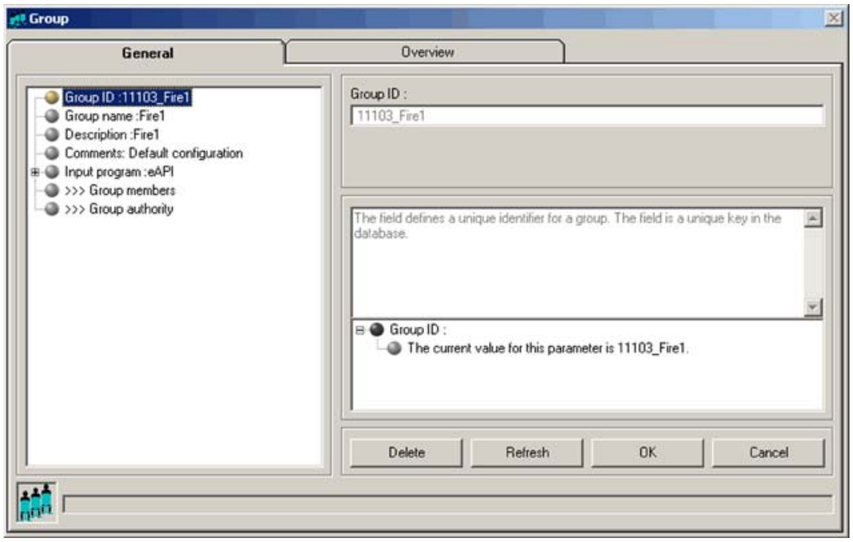
    This illustration shows the eAPI input module.



- Select **Open**. The Group Properties/Parameters window opens.

4. Change group parameters.

    The parameters are described in section Group parameters on page 34.



- Group ID :11103_Fire1
- Group name :Fire1
- Description :Fire1
- Comments: Default configuration
- Input program :eAPI
- >>> Group members
- >>> Group authority

Group ID : 11103_Fire1

The field defines a unique identifier for a group. The field is a unique key in the database.

Group ID :
The current value for this parameter is 11103_Fire1.

5. Confirm your choices.

   Click **OK** and follow the instructions on the screen, if applicable.

Deleting a group

To delete a group, follow Changing group parameters on page 32; at Step 4, click the **Delete** button. DECT Messenger asks you to confirm the action. After you confirm the action, the group is deleted immediately.

Group parameters

You can specify the following group parameters for a device:

- Group ID

  The **Group ID** field defines a unique identifier for a group. The field is a unique key in the database that is created automatically after you create a new group. The ID consists of an input program identifier and the group name that you (initially) assigned to the group. This group ID has an internal (that is, in the database) link to the group members.

- Group name

  The **Group name** field shows the group indicator that is typically received from the external alarm system through the input program (or generated by the input program itself if the external alarm system does not provide a group name). In many environments, alarm systems are capable of sending destination information in the alarm string. For instance, destination information can be referred to with terms such as paging number, group, or destination. In most cases, the group names are determined by third-party vendors and cannot be changed.

Note:

You can use the same group name for more than one input program. You can use the same group name because the DECT Messenger software adds the input program ID to the group name, which makes the group ID unique. This group ID is created automatically after you create the group. However, you can change the group name later. The Group ID remains the same.

- Description

  Administrators can easily recognize the group (for example, Intensive Care) by reading the descriptive text in the **Description** field.

- Comments

  The **Comments** field contains additional information. For example, "Warning: minimum three DECT extensions required".

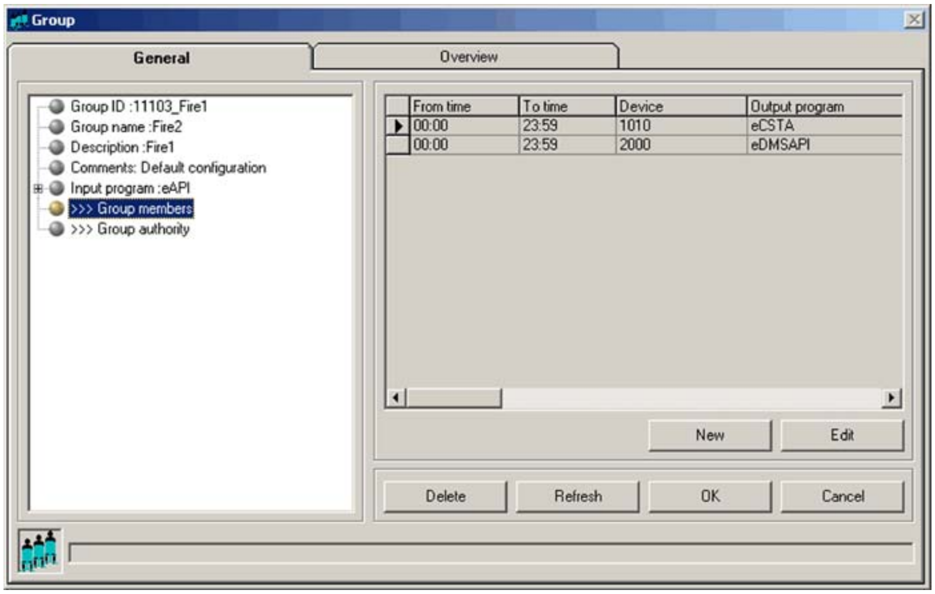
- Input program

  The **Input program** parameter provides information about the input program. You cannot change this parameter. After you create a new group for an input program, these parameters are assigned automatically.

- Group members

  Use the **Group members** parameter to assign group members to the group (assign devices to the group from the list of devices). After assigned, these devices become group members. If the device (for example, an extension) that you want to assign is not in the list, create that device first according to the procedures Creating a new device on page 22.

  Use the **Group members** menu to open the window shown in Figure 10: Group members window on page 36.



- Group ID :11103_Fire1
- Group name :Fire2
- Description :Fire1
- Comments: Default configuration
- Input program :eAPI
- >>> Group members
- >>> Group authority

From time	To time	Device	Output program
00:00	23:59	1010	eCSTA
00:00	23:59	2000	eDMSAPI

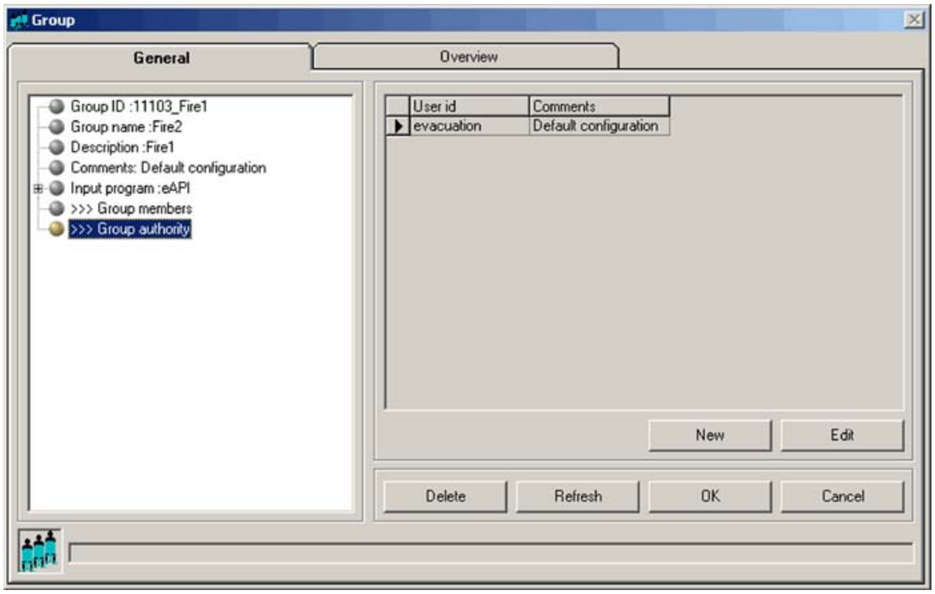
Figure 10: Group members window

The section Changing group member parameters on page 40 provides information on assigning new members, editing members, and deleting members.

- Group authority

The **Group authority** field defines which users are granted access to the group to make changes using the eWEB interface, or to use the eCONFIG. If you specify ALL, all users have access to this particular group, and you do not need to enter all individual users. As a result, however, you have no granular authority definition, because all users are granted access. Note that eWEB allows only maintenance of the groups that are assigned to input programs of the same site as the eWEB. For example, an eWEB instance of site 1 allows only maintenance of groups of site 1.

Use the **Group authority** menu to open the window shown in Figure 11: Group authority on page 37.



- Group ID :11103_Fire1
- Group name :Fire2
- Description :Fire1
- Comments: Default configuration
- Input program :eAPI
- >>> Group members
- >>> Group authority

User id	Comments
evacuation	Default configuration

Figure 11: Group authority

Click the **New** button to give a new user the authority to make changes in the group. Click the **Edit** button to edit a user authority.

⚠ **Warning:**

If you want to delete a user from this group, do not click **Delete** in the window shown in Figure 11: Group authority on page 37, because that deletes the entire group. Instead, click **Edit**. A window specifically for that user opens. Click **Delete** in this window to remove the user from the group.

Managing group members

A group has group members. These are devices to which an alarm for that group is sent. You can assign new members to a group, and you can delete members from a group. These procedures are described in the following sections:

- Assigning a new member to a group on page 37
- Changing group member parameters on page 40
- Removing a group member on page 40
- Member parameters on page 41

Assigning a new member to a group

Complete the following steps to assign a new member to a group.

Assigning a new member to a group

1. Open eCONFIG.

   Ensure that the member that you want to assign to the group is already in DECT Messenger as a device. (A group member is a device that is assigned to a group.) If the member does not exist as a device, see Creating a new device on page 22.

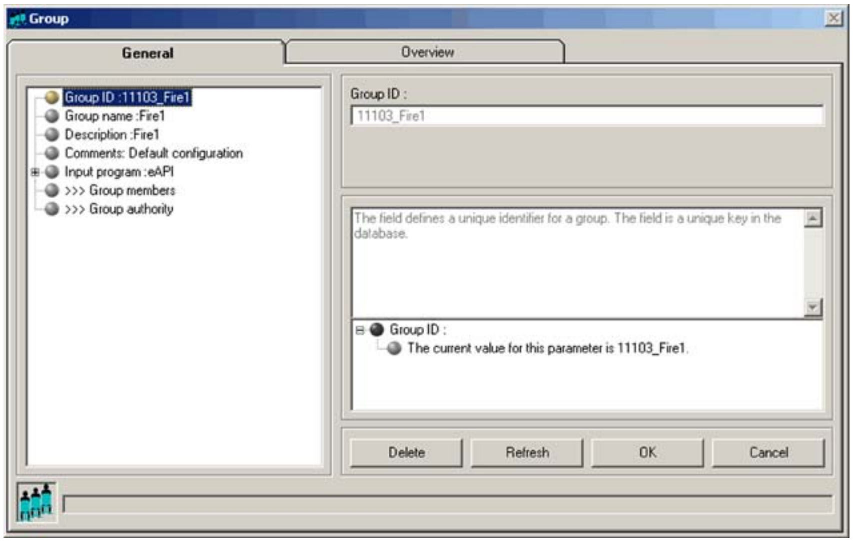
2. Access the Group Properties window.

   Use one of the following methods to access the Group Properties window:

   - Select **Input Module** from the **Modules** menu.
   - Expand the input module for which you want to create a new group.
   - Expand the module instance. The submenu items **Alarm** and **Group** display.
   - Expand the **Group** item.
   - Right-click the **Group** parameter. A pop-up menu displays.
   - Select **Open**. The Group Properties/Parameters window opens.

   or

   - Expand the **Groups and Devices** menu in the eCONFIG main window.
   - Expand the **All groups** menu. All the groups are displayed.
   - Open the group properties window by either double-clicking the group that you want to edit, or right-clicking on the group and selecting **Open**.



Group ID :11103_Fire1
Group name :Fire1
Description :Fire1
Comments: Default configuration
Input program :eAPI
>>> Group members
>>> Group authority

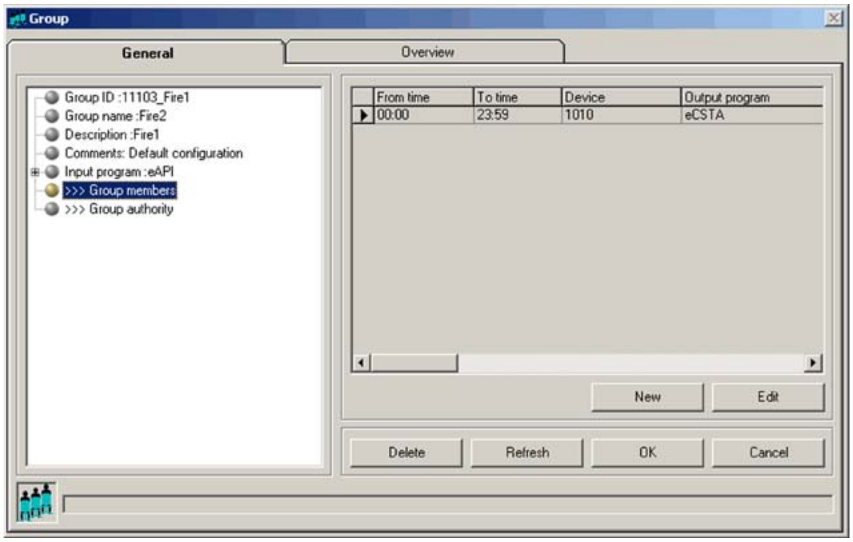
Group ID :
11103_Fire1

The field defines a unique identifier for a group. The field is a unique key in the database.

Group ID :
The current value for this parameter is 11103_Fire1.

3. Open the Group members window.

   Click the **>>>Group members** item.



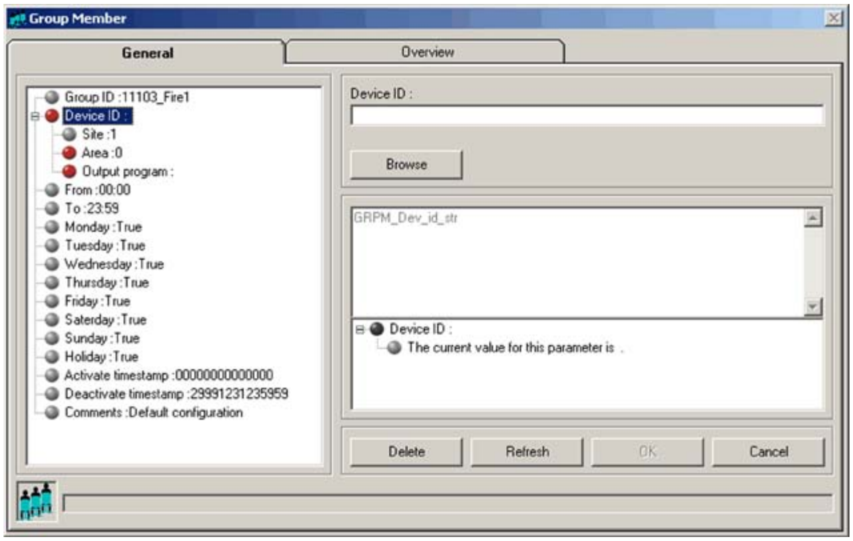
- Group ID :11103_Fire1
- Group name :Fire2
- Description :Fire1
- Comments: Default configuration
- Input program :eAPI
- >>> Group members
- >>> Group authority

From time	To time	Device	Output program
00:00	23:59	1010	eCSTA

A list of group members displays (the example shows only one group member: device 1010).

4. Add a new member.

   - Click **New**. The following window opens.



- Group ID :11103_Fire1
- Device ID :
  - Site :1
  - Area :0
  - Output program :
- From :00:00
- To :23:59
- Monday :True
- Tuesday :True
- Wednesday :True
- Thursday :True
- Friday :True
- Saterday :True
- Sunday :True
- Holiday :True
- Activate timestamp :00000000000000
- Deactivate timestamp :29991231235959
- Comments :Default configuration

Device ID :

GRPM_Dev_id_str

- Device ID :
  - The current value for this parameter is .

   - Click the **Device ID** menu item.
   - Use the **Browse** button to select the device that you want to add as a member to the group.

Note:

After you select a device, the area and output program are defined automatically for the member.

For more information on the parameters, see Member parameters on page 41.

5. Confirm your choices.

Click **OK** and follow the instructions on the screen, if applicable.

Changing group member parameters

Complete the following steps to change the parameters for a group member.

Changing group member parameters

1. Open the Group members window.

   Follow Steps 1, 2, and 3 in Assigning a new member to a group on page 37.
2. Select the group member to edit.

   In the right panel of the window is a list of one or more group members that are assigned to the group. Select the group member that you want to edit, and click **Edit**.
3. Change the parameters.

   A window, similar to the one in Step 4 of Assigning a new member to a group on page 37, opens, however all parameters are entered.

   - Click the item you want to change.

   Note:

   You can change all parameters except the group ID and the parameters for device ID.
4. Confirm your choices.

   Click **OK** and follow the instructions on the screen, if applicable.

Removing a group member

Complete the following steps to remove a member from a group.

Removing a group member

1. Open the Group members window.

   Follow Steps 1, 2, and 3 in Assigning a new member to a group on page 37.
2. Select the group member to remove.

   In the right panel of the window is a list of one or more group members that are assigned to the group. Select the group member that you want to edit, and click **Edit**.
3. Remove the member from the group.

A window, similar to the one in Step 4 of Assigning a new member to a group on page 37, opens, however all parameters are entered.

- Remove the member by clicking the **Delete** button.

4. Confirm your choices.

   Click **OK** and follow the instructions on the screen, if applicable.

Member parameters

Member parameters are parameters that are added to a device for a specific group. These parameters are only applicable for the combination of a device and a group, and can be different after the same device is assigned to another group.

The following parameters can be specified for a group member:

- Group ID

  The **Group ID** field defines a unique identifier for a group. The field is a unique key in the database that is created automatically after you create a new group. You cannot change the Group ID at this parameter.

- Device ID

  Use the Device ID parameter to assign each device as a member of a group. Always use the **Browse** button that is active after you click this menu item.

  The parameters display after you select each device, because these are linked to the device that you select.

- From:

  The **From:** value contains a value in format xx:xx, where a valid hour and time must be specified. Valid range is 00:00 to 23:59. Incorrect values give unpredictable results. The value denotes the start of the time interval during which the defined device is active as a member of the group. For example, a value of 00:00 indicates that the group member is active at midnight. Value 12:00 specifies that the group member starts at noon. The time interval ends in the time specified in the **To:** value.

- To:

  The **To:** value contains a value in format xx:xx, where a valid hour and time must be specified. Valid range is 00:00 to 23:59. Incorrect values give unpredictable results. The value denotes the end of the time interval during which the defined device is active as a member of the group. For example, a value of 23:59 indicates that the group member becomes inactive at midnight. A value of 12:00 specifies that the group member stops its activity at noon. The time interval begins at the time specified in the **From:** value (see the previous bullet). The **From:** value can be larger than the **To:** value. In this case, the active time can start at 21:00 and end at 06:00 (night-shift). Also note that a member can be active from both 08:00–12:00 and 13:15–17:30. To define two time intervals for the same device, you must define it as two group members (same device): one active from 08:00–12:00, and the other active from 13:15–17:30.

- Monday . . . . Saturday

  This value is a Boolean value: True or False. After set to **True**, the member is active on that day.

- Holiday

  This value is a Boolean value: True or False. After set to **True**, the member is to be present on holidays. The holidays are defined in the **Holiday** parameter of the eCONFIG menu.

- Activate Timestamp

  The **Activate Timestamp** value specifies the time after the member record is activated. The timestamp is formatted as follows: YYYYMMDDHHMMSS (for example: 20010101000000). The **Activate Timestamp** and **Deactivate Timestamp** is used to define a time interval during which records are active. This functionality is typically used in environments where there is extensive up-front planning of staff resources, flexible schedules, holiday periods, and so on.

- Deactivate Timestamp

  The **Deactivate Timestamp** value specifies the time after the member record is deactivated. The timestamp is formatted as follows: YYYYMMDDHHMMSS (for example: 20010101000000). The **Activate Timestamp** and **Deactivate Timestamp** is used to define a time interval during which records are active. You can use this functionality to anticipate future changes in availability of staff, and is typically used in environments where there is extensive up-front planning of staff resources, flexible schedules, holiday periods, and so on.

- Comments

  The **Comments** field contains additional information for administrative purposes.

Note:

If a group member is not active because of the member settings, overflow to alternative devices is not activated.

Managing users

DECT Messenger makes a distinction between the users for eWEB and users for eCONFIG. The mechanisms for handling these users are exactly the same. The only difference is that the eWEB users are applicable for Login and Authority levels in eWEB, and eCONFIG users are applicable for Login and Authority levels in eCONFIG.

Creating a new user

The following procedure describes how to create a new user.

Create a new user

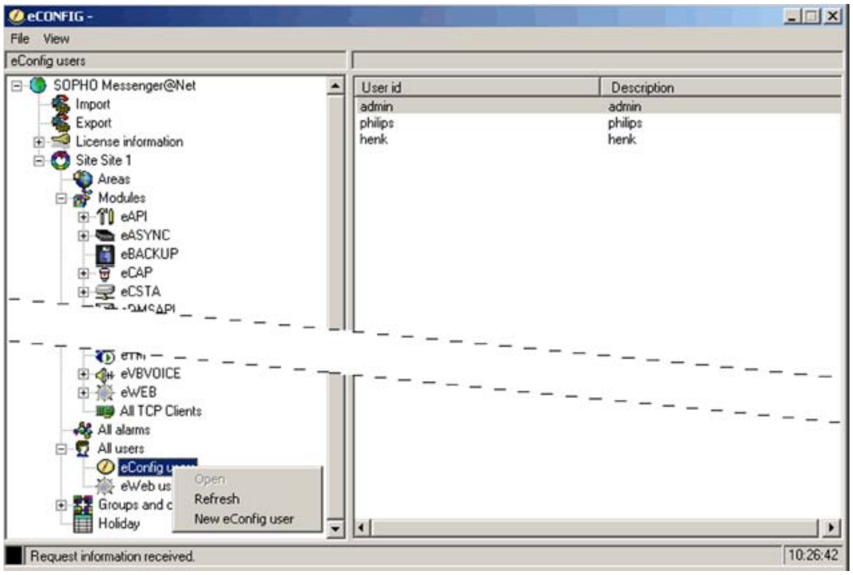
1. Open eCONFIG.
2. Expand the **All Users** menu.

   Note:

   Two submenu items are listed: eWEB and eCONFIG. eWEB contains the users for eWEB, while eCONFIG contains the users for eCONFIG. These are separate from each other, however the approach and authority mechanism is the same, so the steps in this section apply to both.

3. Access the pop-up menu.

   In the **All users** menu, right-click either **eCONFIG** or **eWEB**.



User id	Description
admin	admin
philips	philips
henk	henk

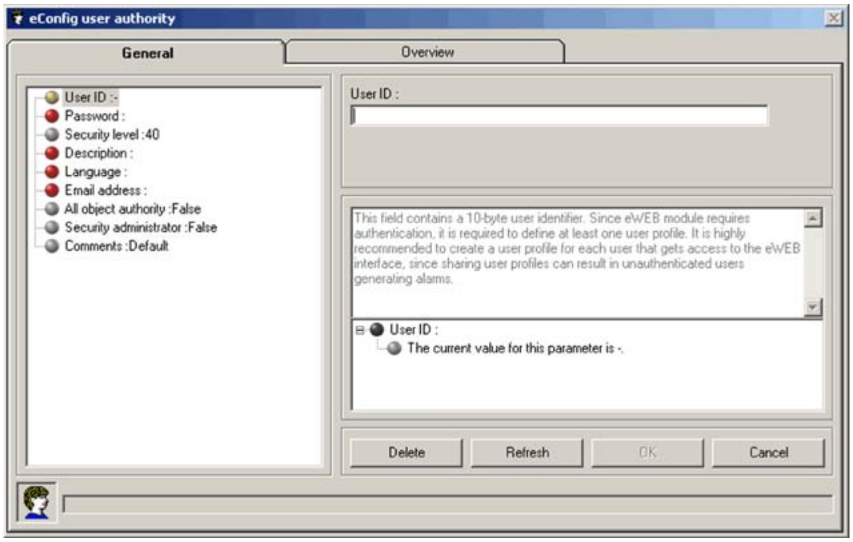
4. Create a new user.

   Depending on the option you chose in step 3, select one of the following:

   - **New eConfig User**
   - **New eWEB User**

5. Enter the parameters for the new user.

   Select each item in the left panel and enter parameters.



User ID :-
Password :
Security level :40
Description :
Language :
Email address :
All object authority :False
Security administrator :False
Comments :Default

User ID :

This field contains a 10-byte user identifier. Since eWEB module requires authentication, it is required to define at least one user profile. It is highly recommended to create a user profile for each user that gets access to the eWEB interface, since sharing user profiles can result in unauthenticated users generating alarms.

User ID :
The current value for this parameter is -.

The parameters are explained in User parameters on page 45.

6. Confirm your choices.

   Click **OK** and follow the instructions on the screen, if applicable.

Changing user properties

The following procedure describes how to change the properties for user.

Changing user properties

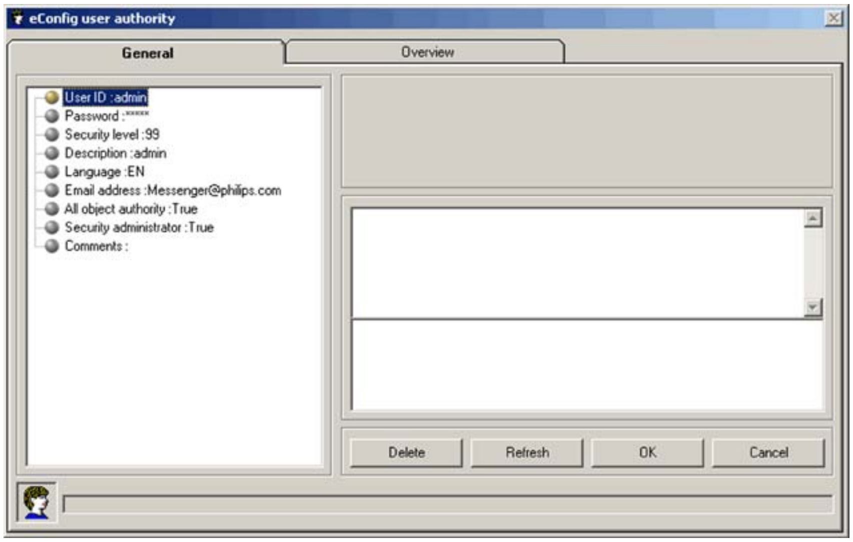
1. Open the Group Members window.
2. Expand the **All Users** menu.

   Two menu items are available: eWEB and eCONFIG. eWEB contains the users for eWEB and eCONFIG contains the users for eCONFIG. These are separate from each other, however the approach and authority mechanism is the same, so the steps in this section apply to both.
3. Select the menu item that contains the user you want to edit.

   Select either **eCONFIG** or **eWEB**, depending on where the user resides. A list of users opens in the right panel.
4. Open the Properties window for the user you want to edit.

   Double-click the user for which you want to change the properties.
5. Change the parameters.

   Change the parameters by clicking the item and changing the field contents.



User ID :admin
Password :*****
Security level :99
Description :admin
Language :EN
Email address :Messenger@philips.com
All object authority :True
Security administrator :True
Comments :

The parameters are explained in User parameters on page 45.

6. Confirm your choices.

   Click **OK** and follow the instructions on the screen, if applicable.

Deleting a user

The following procedure describes how to delete a user.

Deleting a user

1. Open the User Properties window.

   Follow Steps 1, 2, 3, and 4 of the procedure in Changing user properties on page 44.

2. Delete the user.

   Click the **Delete** button.

3. Confirm your choices.

   Click **OK** and follow the instructions on the screen, if applicable.

User parameters

The following parameter descriptions are applicable for the parameters for both eWEB and eCONFIG users.

- **User ID**

  This is the username that must be entered in the login dialog box. Maximum length is ten characters. Avaya recommends that you create a user profile for each user who has access to the eWEB interface. Sharing user profiles can result in unauthenticated users, which generates alarms.

- **Password**

  This field contains a password with a maximum length of ten characters. Users can change their own password using the eWEB interface. You can create new users with default passwords (for example, the same as the user identifier), and request that the users change their password at first usage.

  Note:

  Passwords are stored without encryption in the DECT Messenger structure. Therefore, hackers can retrieve authentication information from the system. Also, table information can be made available through eWEB (depending on your configuration). Because the security mechanism is limited, Avaya recommends that you not use any passwords that are used on other systems that contain secured information. Using identical passwords across both secured and less-secured environments leads to severe security exposure. Inform all users of this issue.

- **Security level**

  You can use the **security level** parameter to define a number in the range of 00–99. The higher the number, the more authority a user is given. The value 99 is the highest level which gives full access to all menu items, and allows read and edit. This value can be assigned to top-level administrators. The value 00 is the lowest possible value. Avaya recommends that you limit the number of initially assigned values to 2 or 3 levels, and handle increments by 10. Good start values are 20 for low-end users, 40 for mid-range users, and 60 for administrators. As you become familiar with user patterns, a more granular level of security can be defined for users.

  Note:

  The level is related to the values specified in the table of contents of the eWEB module where a read and edit threshold level is assigned to each individual menu. For example, a user with level 20 can execute all the functions with level 00 up to 20.

  Note:

  In the eCONFIG, the level thresholds for the menus are fixed. For all menus, the read level threshold is 10, and the edit level threshold is 30.

- **Description**

  This is a text description of the user, and is for administrative purposes only. The real name of the user is often stored in this field.

- **Language**

  You must enter a four-digit code representing the language for the eWEB module. For the eCONFIG you must fill in a two-character representation for the language (for example, EN represents English). If you make a mistake, only menu icons are displayed, and not the menu items.

  - **Language field for eWEB user**

The language field contains a four-digit identifier that represents the language used for eWEB and eGRID access. The codes are those used in an iSeries 400, and are in the range of 29xx. Currently supported values in eWEB are the following:

- 2909: Belgian English
- 2963: Belgium Dutch
- 2966: Belgium French

Check the commercial documentation to determine if other languages are available. If other languages are available, the codes are as follows:

- 2922: Portuguese
- 2923: Dutch Netherlands
- 2924: English
- 2925: Finnish
- 2926: Danish
- 2928: French
- 2929: German
- 2931: Spanish
- 2932: Italian
- 2933: Norwegian
- 2937: Swedish
- 2980: Brazilian Portuguese

- **Language field for eCONFIG user**

The language identifier for the eCONFIG consists of a two-character identifier. For example, EN represents English, NL represents Dutch, and so on. Check with the commercial department to determine which languages are available.

- **e-mail address**

The **e-mail address** field contains the e-mail address of the user. After the user sends an e-mail using the web interface (**Send SMTP Message** menu), this e-mail address is used in the **From:** field (that is, the originator address).

- **All object authority**

The user can maintain all groups in DECT Messenger with the **All object authority** parameter. Remember that a user can be assigned to a group. After assigned to a group, the user (when logged in) can make changes in the group configuration of the groups to which this user is assigned. However, if the **All object authority** option is set to **True**, the user is allowed to maintain and make changes in all groups in DECT Messenger. This gives the user administrator privileges for all groups.

In most cases, the **False** value is used so that the user does not have all object authority.

- **Security administrator**

  The **Security administrator** value is set to either **True** or **False**. Set the option to **True** to allow the user to maintain the user settings of other users (that is, to give the user Administrator rights for all other users, including the right to change passwords, and so on).

  There is a difference in implementation between the eWEB and the eCONFIG:

  - Security administrator rights in eWEB

  After a user with security administrator rights logs in to the web interface, that user has access to view the eWEB_USER_AUTH table in which the user passwords are visible in ASCII text. The user can also change the passwords for all users using the **Change Password** option.

  - Security administrator rights in eCONFIG

  Users with security administrator rights in the eCONFIG see a list of all users in the **All users > eConfig user** menu. These users can change settings and passwords for all users, delete users, and create new users.

  Users with no security administrator rights see only their name in the **All users > eConfig user** menu, and can change only their password (and no other settings).

- **Comments**

  The **Comments** field contains additional information for administrative purposes.

Adding a DECT device to the Messenger system

Use the following steps to add the basic configuration for a DECT handset.

Adding a DECT device to the Messenger system

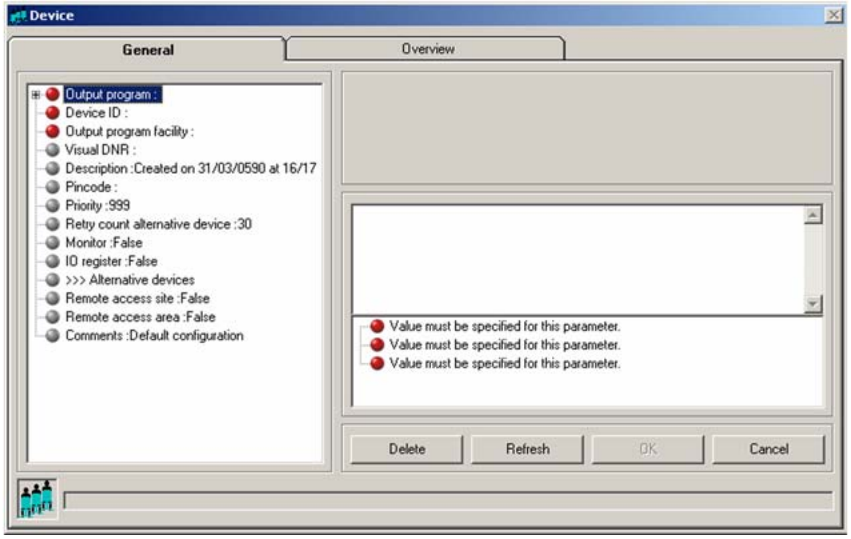
1. Configure a device format.

   Ensure that you have a Device Format for this type of DECT handset. For information about configuring device formats, refer to *Avaya DECT Messenger Installation and Commissioning, NN43120-301*.

   Browse to **Groups and Devices > Device Format**. If your DECT Handset is configured under Device Format on the eConfig module, your DECT handset type is shown beside the eDMSAPI output program.

2. Add new Device.

   Within **Groups and Devices**, right click **All Devices**, and choose **New Device**.



- ● Output program :
- ● Device ID :
- ● Output program facility :
- ● Visual DNR :
- ● Description :Created on 31/03/0590 at 16/17
- ● Pincode :
- ● Priority :999
- ● Retry count alternative device :30
- ● Monitor :False
- ● IO register :False
- ● >>> Alternative devices
- ● Remote access site :False
- ● Remote access area :False
- ● Comments :Default configuration

- ● Value must be specified for this parameter.
- ● Value must be specified for this parameter.
- ● Value must be specified for this parameter.

3. Configure the new device.

   Make the following configuration changes:

   - Select **eDMSAPI** as the Output program.
   - For Device ID, enter either: Board_Number#Index_Number if you are configuring traditional DECT handsets **OR** a DN if you are configuring SIP DECT handsets. Example: For a DMC Card in Slot 4 of an Option 11c Cabinet, and a DECT handset subscribed to index 2, the Device ID is 04#02.

     For more information about Device ID, see Device parameters on page 25
   - Configure the Output Program Facility according to the type of DECT handset you have. Example: C4050
   - Visual DNR The Directory Number (DN) of the DECT handset. Example: 2947
   - Description Add a description of the handset. This can be the name of the handset owner. Example: Emmett Lee This description is displayed on the eWeb 'Send DMS-API Message' Extension box.
   - Set IO Register to True

4. Check alarms.

   - In eCONFIG, open the menu **Modules**, and expand the eDMSAPI module by clicking the **+** beside it. Under the eDMSAPI module, the instances of the input module (For example, eDMSAPI - area One) are listed. Expand this instance. The items **Alarm** and **Group** appear. Click **Alarm**.
   - Ensure that you have at least two Alarms, as follows:

     - E2_MSG_N

     - E2_MSG_U

5. Add a group.

   - In eCONFIG, open the menu **Modules**, and expand the eDMSAPI module by clicking the **+** beside it. Under the eDMSAPI module, the instances of the input module (For example, eDMSAPI - area One) are listed.
   - Expand this instance. The items **Alarm** and **Group** appear.
   - Right-click **Group**, and select **New Group** in the pop-up menu.

6. Configure the new group.

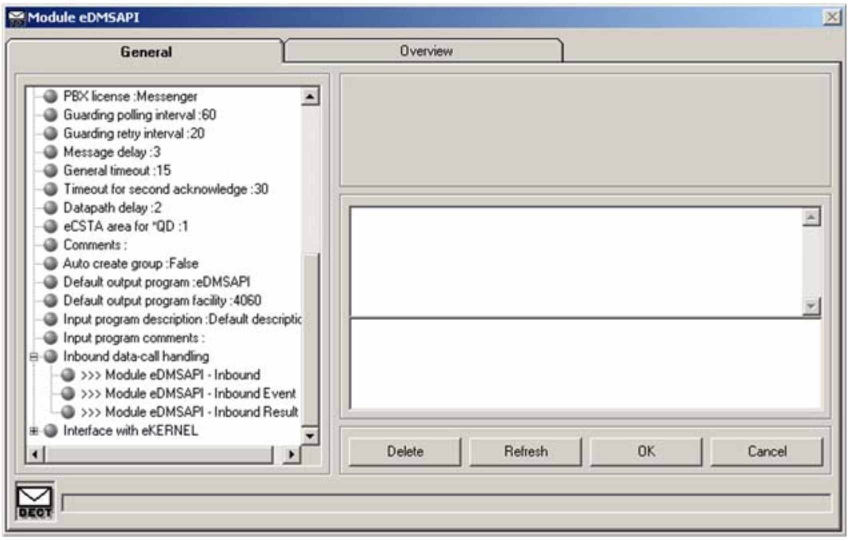
   Make the following configuration changes:

   - Populate the Group_Name. If you are adding a single DECT handset, use the DN of this handset as the group name.
   - Populate the Description
   - Group Members. Click **New**. Browse under Device_ID for the device you created in Step 2.
   - Group Authority. Click **New**. Under User_ID browse for *ALL

7. Open the Inbound data call handling menu.

   - In eConfig, open the menu **Modules**, and expand the eDMSAPI module by clicking the **+** beside it. Under the eDMSAPI module, the instances of the input module (For example, eDMSAPI - area One) are listed.
   - Right-click the instance of the eDMSAPI module (For example, eDMSAPI - area One), and click **Open** in the pop-up menu.
   - Scroll to the bottom of the menu and expand Inbound data-call handling.
   - 3 choices are displayed:

     - Inbound
     - Inbound Event
     - Inbound Result



PBX license :Messenger
Guarding polling interval :60
Guarding retry interval :20
Message delay :3
General timeout :15
Timeout for second acknowledge :30
Datapath delay :2
eCSTA area for *QD :1
Comments :
Auto create group :False
Default output program :eDMSAPI
Default output program facility :4060
Input program description :Default descriptic
Input program comments :
Inbound data-call handling
>>> Module eDMSAPI - Inbound
>>> Module eDMSAPI - Inbound Event
>>> Module eDMSAPI - Inbound Result
Interface with eKERNEL

8. Configure Inbound data call handling.

   Make the following configuration changes for Inbound:

   - Click **New**
   - Called Device: Enter the DN of the DECT handset
   - Called type: *IA

   Make the following configuration changes for Inbound Event:

   - Click **New**
   - Called device: Enter the DN of the DECT handset
   - Calling Device: *ALL
   - Alarm ID for normal messages: Browse and select the alarm E2_MSG_N
   - Alarm ID for urgent messages: Browse and select the alarm E2_MSG_U

   Make the following configuration changes for Inbound Result:

   - Click **New**
   - Called device: Enter the DN of the DECT handset
   - Calling Device: *ALL
   - Group name: Browse and select the Group you created in Step 4
   - Message: [msg] [Calling number]

Chapter 3: DECT Messenger Customer Engineer Manual

This chapter contains information on the following topics:

Preface

This chapter is for Avaya DECT Messenger version 4.0, and is designed to be used in conjunction with the information found in other chapters. This chapter describes the steps necessary to configure and begin using the system. It describes how various modules work, but does not go into detail. For detailed descriptions of modules and how they work, consult *Avaya DECT Messenger Installation and Commissioning, NN43120-301*.

The process for installing DECT Messenger is described in *Avaya DECT Messenger Installation and Commissioning, NN43120-301*.

Note:

No legal rights can be obtained from the information in this manual.

About the manual

This chapter is the Customer Engineer Manual for DECT Messenger, and is intended to assist the engineer in understanding the structure of DECT Messenger.

The modules and related database tables are described in detail in the publication *Avaya DECT Messenger Installation and Commissioning, NN43120-301.*

Guidelines for maintenance and administration of a server or specialized computer

The following are general rules for administering and maintaining a server or other specialized computer:

1. Keep operating system and application software up-to-date.

   Servers are a critical part of business infrastructure. The operating system and application software must be current to ensure stable, secure operation. An automated or semiautomated process for upgrades and patches can be used, however upgrades and patches can have unpredictable interactions with running services. Contact Avaya for detailed information concerning the possible impact of specific updates or fixes.

2. Do not run unnecessary services or applications.

   To reduce risk, do not run any non-essential service or application. Problems with such services or applications include the potential for unwanted interactions between them (for example, ports that are used by other applications), insufficient server capacity, and security issues that are introduced by those applications. If you must run a combination of applications, contact Avaya for more information.

   Check the manufacturer's features for other products, and determine whether those features require resources that DECT Messenger requires.

3. Back up your data.

   All computers eventually fail (hardware or software), and after servers fail, the data stored on them is often lost. Keeping current backups of the system, and data stored on it, is essential for every production system (servers, specialized machines, and so on). The backup procedure depends on many factors, such as the following:

- volume of data
- rate of data change
- recovery procedure
- time for backup and recovery
- response of the applications

There are many issues to consider for your backup process:

- Automatic backups can fail
- Certain other applications must be aware when the backup process is taking place, to avoid conflicts and so on.

Create a backup policy that is built on the existing IT infrastructure. Refer to the specifications (requirements) for the products involved for detailed information.

4. Keep a record of account maintenance and authorized users.

   Keep a current list of the accounts that have access to the server and the account privileges. If unauthorized users have access to the server, the entire server activity can be compromised. Consequently, the business can be compromised (for example, after confidential information is accessed).

5. Use specialized software for servers.

   Consider installing specialized software to provide anti-virus protection, maintenance tools, and firewall protection.

   Firewall policies can be implemented in the entire network based on enterprise firewalls. Where these are not available, a desktop solution is acceptable. Avaya applications can use a range of ports and access types. Contact Avaya for information about ports and access. Anti-virus and firewall software must be included in the list of applications that require periodic updates.

   Popular maintenance tools include ScanDisk and Defrag. After an unpredictable event, scanning the disk can be performed automatically or manually. Database applications are very sensitive to this fragmentation, leading to potential performance bottlenecks or application errors, so Avaya recommends scheduling regular defragmentation during off-peak hours.

6. Provide physical security for the system.

   A power failure is one of the most common problems in a server environment, and also one of the most dangerous, because power failures can cause data loss after the system shuts down without closing data files and applications. An Uninterruptible Power Supply (UPS) filters the current and, in the event of a general power failure, provides the system with enough power that the applications can close properly.

Also consider location and environment (air conditioning, ventilation, and so on) for the equipment.

7. Avoid renaming computers.

   Avoid changing the name of a computer. This type of change can have far-reaching implications, sometimes necessitating the reinstallation of applications.

DECT Messenger overview

This section contains the following topics:

- Avaya DECT Messenger functional description on page 56
- Modules overview on page 58
- Linking modules on page 61

Avaya DECT Messenger functional description

DECT Messenger is a software platform that allows message generation, message routing, and message protocol conversion. DECT Messenger can be used as alarm equipment, because messages can be configured to indicate an alarm situation. In fact, in the terminology of DECT Messenger, a message is also called an alarm.

Figure 12: Input and Output on page 56 shows the various inputs and outputs of DECT Messenger.

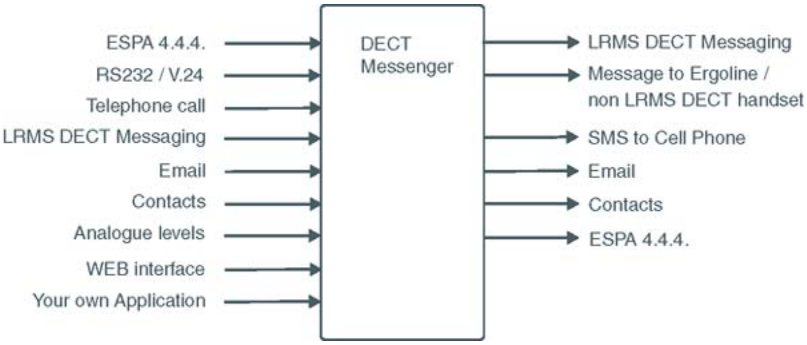


Figure 12: Input and Output

Message input

The following input can generate messages in DECT Messenger:

- ESPA 4.4.4 pager protocol: DECT Messenger can receive pager messages from ESPA 4.4.4-compatible pager equipment.
- RS232/V.24 serial input: many protocols are supported as input for generating a predefined message or a free message.
- DECT handset with E2 (Low Rate Messaging Services [LMRS]) messaging.
- E-mail the DECT Messenger server PC: send a message by e-mail to a telephone set, SMS to cell phone or any other output on DECT Messenger.
- Switches (push buttons, toggles): message alerts generated by alarm contacts, door contacts, fire contacts, and so on.
- Analogue voltage/current levels: this form of message generation is used to guard industrial equipment. For example, equipment output messages can be pressure indication, temperature, and so on.
- Web interface from which you generate messages manually.
- Programs you write that communicate (using TCP/IP socket) with DECT Messenger: DECT Messenger provides a port on TCP/IP that is open to receive input data from this type of unique program.
- Calling a specific telephone number. In this case the extension number that is dialled in combination with the originator telephone number (CLI) is used to generate a predefined message.
- An SNMPv1 or SNMPv2c trap can generate a message.

Message output

DECT Messenger supports the following output:

- DECT E2 messages (up to 160 characters)

  Although DECT Messenger supports up to 160 characters, the DECT equipment or the handset can limit this to 128, or even 48 characters. If the handset supports only 48 characters, the message is broken into sections and sent in parts to the handset.
- Messages sent to Ergoline or DECT extensions during ringing and after a call is connected.

  The first part of the message is sent as an alert phase. The remaining part (if there is more) is sent in call connect status.

  Message length can be specified for each device type. Messages that are too long to be displayed are broken into sections suitable for the display devices.

- SMS messages to cell phones

  DECT Messenger can send SMS messages to cell phones. The interface to the cell phone provider can be a modem, or a box that behaves like an actual cell phone with SIM card.

  This option is mainly used as an alternative device. If a message to a DECT handset is not acknowledged, the message can be forwarded to a cell phone.

- E-mail messages

  DECT Messenger can send e-mail, using SMTP, to any e-mail server.

- Digital output to control relays or similar equipment

  In the event of an alarm, the relay contacts can be used to control equipment such as lamps, door-contacts, or hooters. Contacts are used as alternative devices (overflow) in case a message is not confirmed.

- ESPA 4.4.4 pager protocol

  DECT Messenger can send messages to paging equipment using the ESPA 4.4.4 protocol.

- Windows pop-up message.

  The capabilities of the Windows operating system can be used to send a popup message, similar to the NET SEND command.

Modules overview

DECT Messenger consists of separate modules. There are four main groups of modules:

- Core software modules
- Configuration modules
- Input and output modules
- Security modules

The following sections provide an overview of the modules. Detailed module descriptions are provided in corresponding chapters.

Core software modules

There is one core software module:

- eKERNEL

The eKERNEL is the core software in the system and must always be present. eKERNEL is between the incoming and the outgoing modules and must always be running. The system does not operate if eKERNEL is absent or non-functional.

Configuration modules

There are two configuration modules:

- eGRID

  The eGRID module is used to make inquiries and to edit the configuration database. The configuration database (an MS Access database) stores all the configuration data.

- eCONFIG

  The eCONFIG module is used to set up and configure the system, messages, and message flows. The eCONFIG is a user-friendly variant of the eGRID, and can be used either on the DECT Messenger PC, or on a remote PC.

Incoming and outgoing modules

There is a wide range of incoming and outgoing modules available. They all communicate with the eKERNEL module. Each module has a specific incoming or outgoing function. This means that the incoming modules can receive messages and outgoing modules can send messages.

Table 6: Incoming and outgoing modules on page 59 provides an overview of the modules.

Table 6: Incoming and outgoing modules

Module Name	Function	Incoming	Outgoing
eCAP	V.24/RS232 interface and protocol converter.	Yes	-
eESPA	Input/Output module for ESPA 444 protocol.	Yes	Yes
eAPI	Input on eKERNEL for locally made programs. A Visual Basic source is available, which can be used as basis to make your own input application.	Yes	-
eIO	Digital and analogue inputs and digital outputs (contacts and switches).	Yes, analogue levels and digital levels (contacts)	Yes, switches
eWEB	Web interface	Yes	-
eSMTP-server	Receiving e-mail messages.	Yes	-

Module Name	Function	Incoming	Outgoing
eSMTP (client)	Sending e-mail messages	-	Yes
eDMSAPI	Sending and receiving LRMS (E2) DECT messages using the CSTA interface.	Yes, receiving LRMS (E2) DECT messages	Yes, sending LRMS (E2) DECT messages
eASYNC	Asynchronous modem interface to cell phone SMS provider, or to wide area paging system.	-	Yes
eLOCATION	Always in combination with eCSTA or eDMSAPI; after location alarm is triggered, the location of the DECT handset is detected. This information is available in the message that is generated.	Yes	No
eVBVOICE	Interactive Voice Responds used to various message types. Only available through Professional Services!	Yes	Yes
eSNMP	Receive an SNMPv1 or SNMPv2c trap from an SNMP sending process or equipment.	Yes	No
eSMS	Send SMS message to a mobile phone. Inbound SMS can be used to confirm alarm.	Yes	No

Security modules

The security modules are used (in addition to an operating system) to provide extra security. Security provided is based on the module type. The following gives a brief overview of the available security modules:

- eBACKUP

  The eBACKUP module creates a backup of the configuration database at regular intervals.
- eGUARDIAN

  The eGUARDIAN module is used in conjunction with an input module that receives data at regular intervals. The eGUARDIAN module checks the data input at regular intervals. If the input is not received within a specified time period, the eGUARDIAN module sends a message indicating that an input is down.
- eWATCHDOG

  The eWATCHDOG is a software module that works with the Watchdog card. The eWATCHDOG sends a code to a V.24 interface (COM port) on the DECT Messenger PC.

This COM port is connected to a Watchdog card that expects the code within certain time intervals. If the code is not received within the time interval, the Watchdog card assumes that the system is down and restarts the PC or activates a alarm indication.

- eTM

  The eTM is the Task Manager, which ensures that the DECT Messenger modules remain active. If a module fails, the eTM reboots the module automatically. You can specify which modules are monitored by the eTM. The eTM can be installed on the DECT Messenger PC where the eKERNEL is located, and on other PCs if there are DECT Messenger modules also running on other PCs. The eTM is always used in conjunction with the eCONFIG module.

Logging module

The eKERNEL has a built-in logging function that provides technical logging data. For a more user-friendly logging function, the eLOG module is also available.

- eLOG

  The eLOG module generates log files. These files contain information about processing individual alarms/messages. The eLOG module is part of the eKERNEL.

Linking modules

All the modules are software modules (e-modules such as eCAP). The core module is the eKERNEL. All other modules are input/output modules or security modules that communicate with the eKERNEL module. Modules do not communicate with each other, except through eKERNEL. The communication between a module and the eKERNEL passes through a TCP/IP socket. (A socket consists of an IP address and a port number.) The modules can be anywhere in a TCP/IP network. Figure 13: Example of logical representation of module links on page 62 shows logical links between the modules. Figure 14: Example of module links (practical) on page 62 shows a practical example of module linking.

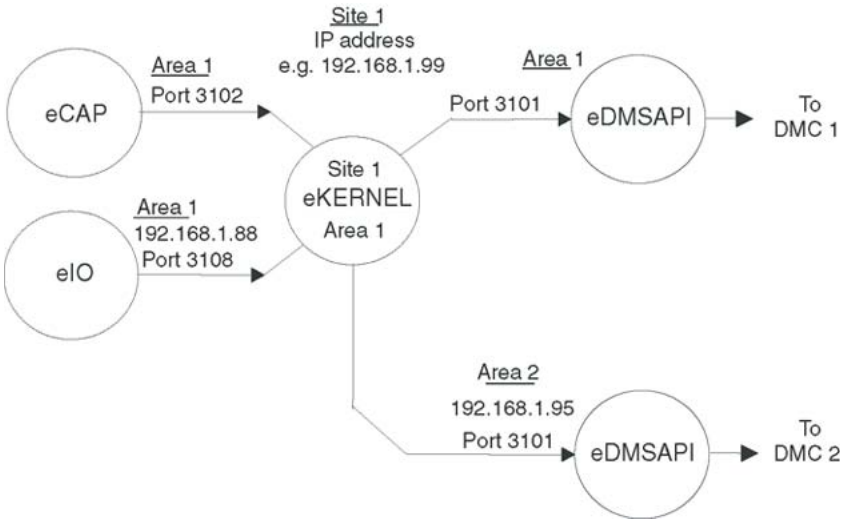


Figure 13: Example of logical representation of module links

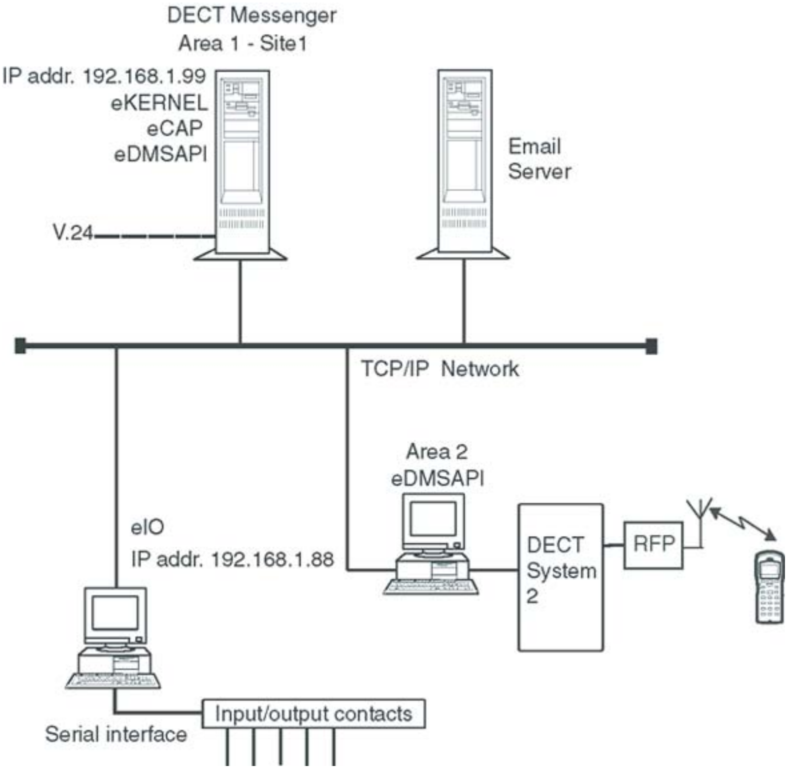


Figure 14: Example of module links (practical)

In Figure 13: Example of logical representation of module links on page 62, four DECT Messenger modules are shown (eCAP, eKERNEL, eIO, and eDMSAPI). These modules are grouped around the eKERNEL. Each input/output module (eCAP, eIO, eDMSAPI) communicates with the eKERNEL through a socket. The default port numbers are shown in Figure 13: Example of logical representation of module links on page 62. The IP addresses are the same if the modules are all on the same PC, but the IP addresses are different if the modules are on more than one PC. After a module starts, it contacts the eKERNEL and exchanges data. During this data exchange, the module indicates the IP address (PC) on which the module is found.

The illustrations show an example with a site and two areas defined. These concepts are defined as follows:

- Site

  The site is the place where the eKERNEL resides. A site has a fixed relationship with only one eKERNEL. If you have more than one site, you have more than one eKERNEL. Also, you can have only one eKERNEL for each PC. This results in a fixed relationship among site, eKernel, and IP address (PC).

  Although you can have more than one site in a network with PCs, only one site can be active at a time. With only one site active at a time, you can set up a second eKERNEL (that is, a second site) offline. After the configuration is set, you can shut down the first site, and start the second one.

  Table 7: Example of the site definition table on page 63 shows an example of the site definition table on the DECT Messenger PC, which shows the link between a site and the IP address of the computer where the eKERNEL for that site resides.

  Table 7: Example of the site definition table

Site	IP address
1	192.168.1.99
2	192.168.1.34

- Area

  An area is a subdivision in a site. An area refers to a connection from an eDMSAPI module to a PBX. For each PBX you must create an area. The eDMSAPI modules can exist on the PC where the eKERNEL is running, and also on another PC.

  Referring to Figure 13: Example of logical representation of module links on page 62 and Figure 14: Example of module links (practical) on page 62, the site and area structure is shown in Table 8: Site and Area structure on page 63.

Table 8: Site and Area structure

Site	Area	Module	To DMC
1	1	eDMSAPI	1
1	2	eDMSAPI	2

You can use this modular structure to do the following:

- install modules on different computers in the TCP/IP network
- set up a standby eKERNEL on a second site
- connect more than one DMC to DECT Messenger

DECT Messenger in a WAN or MAN network

DECT Messenger can be used in a multiunit MAN (IMP network), or in a multinode WAN (DPNSS network). If DECT Messenger is installed in a multiunit DMC network (MAN), you can send LRMS (E2) messages to DECT handsets in units other than those in which DECT Messenger is connected. The IMP links support LRMS (E2) messaging, but this generates a heavy load on the interunit links. Therefore, Avaya recommends that you avoid sending LRMS (E2) messages over interunit links. If you must send LRMS (E2) messages to handsets in a unit other than the one having the DECT Messenger connection, Avaya recommends that you make a direct DECT Messenger connection to those other units, as well. Figure 15: DECT Messenger in a multiunit or multinode environment on page 64 shows a configuration in which DECT Messenger has connections to more than one DMC. The connection between the units can be either an interunit (IMP) link (MAN) or a DPNSS connection (WAN), because there is no messaging passing through the links between the units.

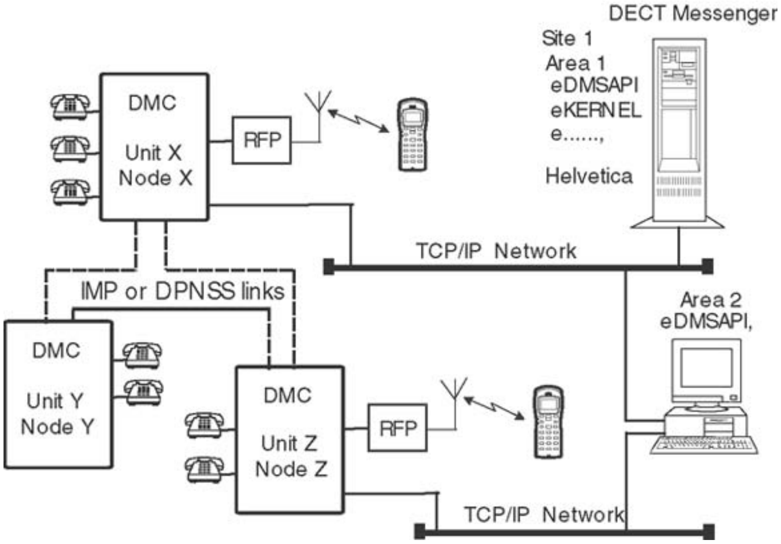


Figure 15: DECT Messenger in a multiunit or multinode environment

Figure 15: DECT Messenger in a multiunit or multinode environment on page 64 shows a multiunit or multinode network. DECT Messenger must be able to send messages to DECT handsets in Unit X/Node X and Unit Z/Node Z. On the DECT Messenger computer (Area 1), the eKERNEL is running with other modules and an eDMSAPI to send messages to Unit X/ Node X. The second computer (Area 2) provides messaging to Unit Z/Node Z. DECT Messenger contains a table that provides data about the location of the DECT handsets. If

there is a message for a DECT handset in Unit Z/Node Z, the message is transferred first to the Area 2 computer, and then to Unit Z/Node Z.

Licensing

Licensing is done by means of the following mechanisms.

- CSTA Connection licenses in the ISPBX. See CSTA connection (link) license on page 65.
- DECT Messenger License Manager. See Figure 16: DECT Messenger License Manager on page 66.
- DECT Messenger CTI Licenses (for each DECT system). See SOPHO CTI module License Manager licenses on page 68.

CSTA connection (link) license

Each application connected to the DMC through CSTA is licensed through one or more application license and seat license. For Avaya DECT Messenger 4.0, the number of application licenses depends on the configuration.

For each DECT Messenger link to a DMC, one application license is needed for the DMS (DMSAPI).

DMS is needed for sending and receiving LRMS (E2) messages using the CSTA link.

In addition to the application license, you must have seat licenses. For DMS, the total number of seat licenses is the sum of the following items:

- total number of simultaneous outgoing messages coming from the eKERNEL
- total number of simultaneous outgoing messages coming from the web interface
- total number of DECT handsets that can send LRMS messages to DECT Messenger

Note:

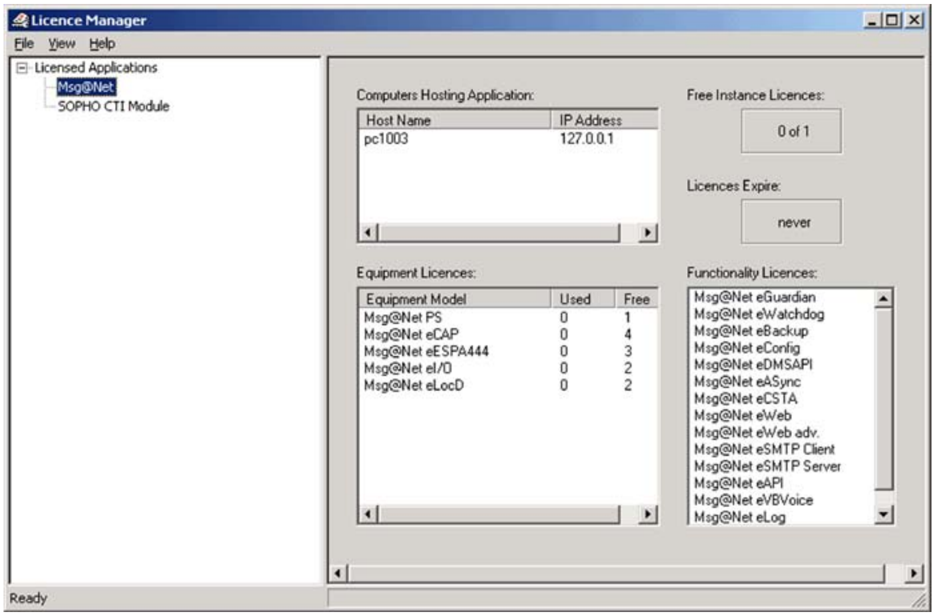
Messages sent to DECT Messenger can be incoming messages to other devices or incoming confirmation.

At startup, DECT Messenger immediately reserves the licenses needed, although there is no call yet. If the number of seat licenses in the DMC is less than the number of seat licenses specified in DECT Messenger, DECT Messenger cannot reserve the licenses and, therefore, cannot make a call.

DECT Messenger License Manager licenses

The DECT Messenger License Manager is the Avaya License Manager. This license manager uses a dongle (using either a parallel connection or USB) and a license file.

Figure 16: DECT Messenger License Manager on page 66 shows the License Manager.



Computers Hosting Application:

Host Name	IP Address
pc1003	127.0.0.1

Free Instance Licences: 0 of 1

Licences Expire: never

Equipment Licences:

Equipment Model	Used	Free
Msg@Net PS	0	1
Msg@Net eCAP	0	4
Msg@Net eESPA444	0	3
Msg@Net eI/O	0	2
Msg@Net eLocD	0	2

Functionality Licences:

Msg@Net eGuardian
Msg@Net eWatchdog
Msg@Net eBackup
Msg@Net eConfig
Msg@Net eDMSAPI
Msg@Net eASync
Msg@Net eCSTA
Msg@Net eWeb
Msg@Net eWeb adv.
Msg@Net eSMTP Client
Msg@Net eSMTP Server
Msg@Net eAPI
Msg@Net eVBVoice
Msg@Net eLog

Figure 16: DECT Messenger License Manager

Note:

Figure 16: DECT Messenger License Manager on page 66 also shows the CTI application as a licensed application. You require this CTI application license only if a connection exists to the DECT system.

The following licenses are available through the License Manager:

- Application module licenses

  These licenses allow you to use a limited set of functionality licenses. Check the commercial documentation for the list of modules allowed with these licenses.

  The following licenses are available:

  - Basic Package
  - Full Package
  - Professional Package (PS)

Note:

The application module license is shown under the equipment licenses in the License Manager.

- Equipment licenses

  Use equipment licenses to add extra equipment to DECT Messenger. Equipment can be an I/O module, a V.24 connection to an external system, a V.24 connection to ESPA equipment, or connection to a DECT system for location detection.

  Equipment for which you can acquire licenses is as follows:

  - DECT Messenger eI/O
  - DECT Messenger eCAP
  - DECT Messenger ESPA444
  - DECT Messenger eLOCATION
  - eSMS (with SMS_service)
  - eSNMP

- Functionality licenses

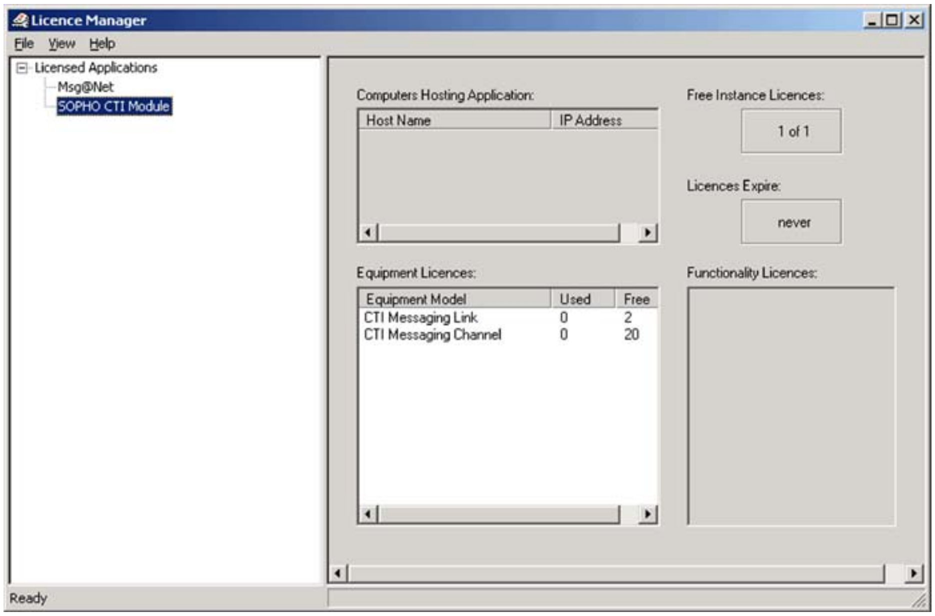
  These licenses allow you to implement certain functionality. The functionality licenses are submitted to the PC application module licenses. If the PC application licenses do not allow you to use a specific functionality, you cannot select this functionality in the functionality list.

  Items that appear in the functionality list are as follows:

  - DECT Messenger eGuardian
  - DECT Messenger eWatchdog
  - DECT Messenger eBackup
  - DECT Messenger eCONFIG
  - DECT Messenger eDMSAPI
  - DECT Messenger eASync
  - DECT Messenger eWEB
  - DECT Messenger eWEB Adv
  - DECT Messenger eSMTP Client
  - DECT Messenger eSMTP Server
  - DECT Messenger eAPI
  - DECT Messenger eLog
  - DECT Messenger eBVOICE

SOPHO CTI module License Manager licenses

You must have SOPHO CTI module application licenses to connect to the DECT system.



Computers Hosting Application:

Host Name	IP Address

Free Instance Licences: 1 of 1

Licences Expire: never

Equipment Licences:

Equipment Model	Used	Free
CTI Messaging Link	0	2
CTI Messaging Channel	0	20

Functionality Licences:

Figure 17: SOPHO CTI Module License Manager

For each connection to a DECT system, you require a CTI application license.

The number of CTI message channel licenses you require is the sum of the following items:

- total number of simultaneous outgoing LRMS messages coming from the eKERNEL.
- total number of simultaneous outgoing LRMS messages coming from the web interface.
- total number of DECT handsets that can send LRMS messages to DECT Messenger.

At startup, DECT Messenger immediately reserves the licenses needed, although there is no call yet. If the number of CTI licenses (application and seat licenses) is less than the number of licenses that are specified in DECT Messenger, DECT Messenger cannot reserve the licenses and, therefore, cannot make a call.

Detailed module descriptions

This section provides detailed information for the following modules:

- eKERNEL on page 69
- eDMSAPI on page 70
- eIO on page 70
- eSMTP on page 70
- eSMTP_Server on page 71
- eAPI on page 71
- eWEB on page 72
- eGRID on page 73
- eTM on page 73
- eLOG on page 74
- eCAP on page 74
- eESPA on page 74
- eLOCATION on page 74
- eSMS on page 74
- eSNMP on page 75
- eFR on page 75
- Web administrator on page 75

eKERNEL

The eKERNEL module is the main module of the DECT Messenger application.

Depending on the incoming alarm message, a message is sent to a specific group of devices. The kernel ensures that all necessary devices receive the message. After a confirmation is required, the eKERNEL sends the message repeatedly until a confirmation is received. A maximum of 30 modules can communicate with the eKERNEL module.

The configuration is done with either the eCONFIG or the eGrid module.

It is possible to use one eKERNEL for multiple units in a DMC multiunit network (MAN), multiple units in a DMC DPNSS network (WAN), and/or to one or more Mobile DECT systems. (For more information on using DECT Messenger in a multiunit environment, see eDMSAPI on page 70.)

eDMSAPI

The eDMSAPI module is both an input and an output module, which can send and receive normal and urgent LRMS (E2) messages to and from LRMS DECT handsets such as 4060, C4050, C4040, industrial handset. The Windows 2000 CSTA service must be running for the eDMSAPI module to function. The CSTA service supports simultaneous connections to one or more DMC units for eDMSAPI. If the DECT handsets are in more than one unit, you can use an eDMSAPI module on one PC, or you can install eDMSAPI modules on other PCs as well.

The External Application Interface (EAI) – used for LRMS messaging with the web or external applications – supports normal, urgent and emergency messages. In previous releases the SNDEMSG was not available.

The EAI also supports LRMS messages up to 160 characters in length when messaging with SIP DECT. The EAI only supports LRMS messages up to 48 characters in length when messaging with the DECT Messenger CPU.

eIO

The eIO module is an input and output module that requires specific additional hardware from National Instruments. If no COM port in the PC is available, a multi-IO board is required. The additional hardware uses an RS-232 connection. The eIO module connects external hardware to the Avaya DECT Messenger. Use either digital or analogue input devices for alarm generation. These devices connect to the National Instruments panel. The panel informs the eIO module of the presence of DECT Messenger. Switches, motion detectors, or fire detectors are used as input devices. Voltage or current levels are used as analogue input devices. An alarm is activated based on the level of the voltage/current. You also use the National Instruments panel to switch external hardware on or off when the output component of the eIO module is being used. More information on the National Instruments panel can be found on the National Instruments web site (www.ni.com).

eSMTP

The eSMTP module is an output module. Use it to send e-mail alarm messages to a specific e-mail address. To send e-mails, you must enter the IP address of an SMTP-protocol e-mail server on the network. An e-mail message is sent to one e-mail address only. No option exists to send the same message to multiple e-mail addresses simultaneously, although you can send the same message more than once to different e-mail addresses. The subject of the message is alarm message, and the body is the alarm message. An SMTP mail server is not included in the eSMTP module because eSMTP behaves as an e-mail client sending e-mail messages.

eSMTP_Server

The eSMTP_Server is an input module, and is not an SMTP or mail server. This module must be used in conjunction with the Internet Information Server (IIS). The IIS is a Windows 2000 component that is automatically installed with Windows 2000 Server. In Windows 2000 Professional, the IIS must be separately installed. Alarms are sent based on the e-mail address entered in the **To:** field. The alarm message appears in the **Subject** field of the e-mail. The e-mail can be empty, because the content is ignored.

E-mail handling procedure in DECT Messenger

After you send an e-mail message to DECT Messenger, the message enters at the SMTP port of the IIS SMTP Server. The IIS SMTP Server drops the message in a directory on the hard disk. The eSMTP_Server module checks this directory at regular intervals for newly arrived e-mail messages. If there is an e-mail, eSMTP takes the message from the directory and analyses it. The e-mail address entered in the **To:** field of the e-mail is translated into a device (or group of devices) to which the e-mail must be sent. The **Subject:** field of the e-mail informs the devices of the nature of the message. After the message is processed, the eSMTP_Server sends a confirmation to the address entered in the **From:** or **X-sender** field of the message to inform the user whether the message is accepted or not.

eAPI

The eAPI module is simply a TCP/IP socket input on the eKERNEL. You can write your own program to send data to the eKERNEL and generate an alarm with the eAPI. You can write your program in any programming language, because the eAPI interface is a socket interface. For more information on the eAPI interface, see Module eAPI in *Avaya DECT Messenger Installation and Commissioning, NN43120-301*. Also included in the chapters are examples of programming code you can use to write your own eAPI program in Visual Basic. A sample program is also available that ships with the software, called eAPI. The eAPI program is an .exe file, and is supplied as source code for Visual Basic. If you are familiar with programming in Visual Basic, you can use the eAPI to create your own interface DECT Messenger.

The eAPI module is often used to develop an application to convert an unsupported protocol to the DECT Messenger protocol. This requires a detailed specification of the unsupported protocol, and a test system that uses the unsupported protocol.

eWEB

The eWeb module can send messages (entered using a web interface) to:

- LRMS (E2)-compatible DECT handsets (C4040, C4050, 4060, Industrial handset, and so on)
- e-mail using eSMTP (Client)
- Any other output module in DECT Messenger, for example:
  - Global System for Mobile Communications (GSM) phones using SMS
  - Switch on/off an alarm contact

The eWeb server runs on an Apache web server; IIS web server is not supported. To access the eWEB application, a username and password are required. The eWeb module offers two interfaces: basic and advanced.

Basic

Using the eWEB Basic module you can send messages directly to a single device only. After sending messages directly to a single device (LRMS [E2] compatible DECT handsets and e-mail addresses), no control mechanism is available that keeps track of the messages. The eKERNEL module does not control the messages. For example:

- Person A has a DECT phone with number 1234. Currently this person is not in the office, and has forwarded their phone to colleague B, with the phone number 1256:
  - If a third party uses the web interface Send DMS-API message to send a message to Person A, the message arrives on the DECT handset of person Al; it is not forwarded to Person B.
  - If a third party sends a Group, Server or User message to a group of which person A is a part, the message is forwarded to colleague B. (A group can consist of one member.)

After sending messages to other devices or a group of devices, you can send to a Server, Group, or User message.

- Using eWEB Server messages, you can send a text message with a maximum length of 8,16 or 32 characters to a group. You cannot see the members of this group. The eKERNEL handles this message request as an incoming alarm.
- Using eWEB Group messages, you can send predefined and plain-text messages to a group of devices. The predefined messages can be split into messages for all groups and group-specific messages. You can see the members of this group. The eKERNEL handles this message request as an incoming alarm.
- Using eWEB User messages, you can send predefined and free-text messages to a group of devices. The predefined messages can be split into messages for all users and user-

specific messages. You can see the members of this group. The eKERNEL handles this message request as an incoming alarm.

Advanced

The eWeb Advanced application is an expansion on the eWeb Basic application. Use the advanced application to perform system management tasks using the web interface, and to use script messages for emergency situations.

Use these system management tools when you need a quick overview of the configuration of the system, or to make changes to groups settings or composition. A Script message contains actions that must be taken in the event of an alarm. The web user can follow the status of this alarm using the web browser.

eCONFIG

The eCONFIG module is the module most commonly used to make changes in the configuration. eGRID can be used to make changes in the configuration directly on the database level, but eCONFIG is a shell over the configuration, providing a more user-friendly way of making configuration changes. The eCONFIG module can be installed on the local PC (where the eKERNEL is running), or on a remote PC. If the module is used on the local PC, almost all parameters in the system can be changed, and new items can be added. If the module is used on a remote machine, only the Users, Groups, and Device parameters can be changed, and new users, groups, and devices can be added.

eGRID

The eGRID module is used for configuration purposes only. You can use MS-Access instead of the eGRID module; however, the most user-friendly way of making changes in the configuration database is using the eCONFIG module.

eTM

The eTM module is the Task Manager in DECT Messenger. eTM is not a scheduler, but serves as a monitor to ensure that the modules in DECT Messenger are running. If a module stops, the Task Manager restarts the module within two seconds. If the Task Manager is running, Windows cannot be shut down.

eLOG

The eLOG module provides information on how DECT Messenger has processed an incoming alarm from the input up to the output device. This can be necessary if, for example, no response is received to indicate whether a recipient received a message or not. The eLOG module does not have a user interface, and does not provide charts. However, eLOG provides three *.csv files that contain detailed information about how the alarm was processed.

eCAP

The eCAP Module handles a V.24 interface. Over the V.24 interface, there can be many protocol variants. A number of protocols are predefined in the eCAP. For the latest list of supported protocols, refer to *Avaya DECT Messenger Installation and Commissioning, NN43120-301*, or check the most recent commercial documentation. You can use the eCAP_Generic module to set up your own protocol for incoming character strings using the V.24 interface. If you need a special protocol over the V.24 connection, you can request that Avaya create this protocol for you; you must provide a detailed protocol specification.

eESPA

The eESPA module supports the ESPA 444 protocol. Incoming and outgoing eESPA also supports both types of ESPA stations: Controlling station and Polling station.

eLOCATION

You can use the eLOCATION module to determine the approximate location of a DECT handset after the handset calls a predefined number. The location information relates to the Radio Cell from which the call originated. The precision of the location depends on the area covered by the Radio Cell. The smaller the area covered, the greater the precision of the location.

eSMS

eSMS is a new output module capable of sending SMS messages to mobile GSM Phones. It uses a GSM terminal instead of an asynchronous modem to connect to the mobile provider. As a result there are no longer restrictions on mobile provides, which was the case with aASYNC module. Also eSMS is more scalable as it can transmit messages faster. Finally eSMS is capable of handling inbound SMS with a specific syntax to confirm alarms based upon CLIP or pincode.

eSNMP

eSNMP is a new input module and can receive SNMPv1 and SNMPv2 traps to set or reset an alarm. Configuration tables are available to map the parameters from SNMP environment (address, community, OID, generic, specific…) into the parameters of Messenger environment (group, message, set/reset…)

eFR

eFR is an add-on module for Messenger that implements fault reporting.

eFR performs the following:

- monitors the DISK state and threshold level
- monitors the NETSTAT like connectivity (client/server)
- performs PING to check responsiveness on ICMP level

Notification at begin and end condition is possible through various transport mechanisms, such as e-mail, SNMP, NET SEND and SMS.

Web administrator

Although eWEB is still supported, a new Web Administrator is available, with a more attractive user interface and additional functionality, covering maintenance and reporting.

The Web Administrator must be positioned as the maintenance tool of choice for concurrent daily maintenance by end-user. For more detailed low-level configuration tasks, for example regarding system restart - the eCONFIG or eGRID remain the confirmation tool of choice.

Web Administrator provides the following functionality.

- Sending messages directly to devices such as the following.
    - DECT handset
    - Mobile GSM phone
    - Windows pop-up message
    - E-mail.
- Sending group and user messages
- Sending script messages

- Reporting functions
    - Inquiry active alarms and ended alarms
    - Inquiry active scripts and ended scripts
- Basic maintenance
    - Work with group members
    - Work with alternative devices
- Advanced maintenance
    - Work with groups
    - Work with users
    - Work with devices
    - Work with facilities
- Expert maintenance
    - Import Template configuration

Refer to *Avaya DECT Messenger Installation and Commissioning, NN43120-301* for more information.

What is required to run DECT Messenger

Hardware Requirements

The hardware requirements for DECT Messenger are grouped into mandatory requirements and optional requirements. The optional requirements depend mainly on the number of modules and users, and the type of modules.

- Mandatory PC Requirements
    - Intel® Pentium® 4 processor, 1.8 GHz.
    - 256K cache 256MB SDRAM.
    - 10/100 MB Network interface card.
    - 3.5 Floppy Drive.
    - 10 GB free Hard disk space.

  - CD-ROM player.
- Optional PC requirements
  - Analogue Modem for remote maintenance/support.
  - Analogue Modem for dialling to GSM provider to send SMS messages. Only required if you must send SMS messages to a GSM (cell phone) provider using a dial-in option.
  - Internal Serial Watchdog (type 1120 from Berkshire Products, www.berkprod.com).
  - National Instruments equipment for Digital input, Digital output (contacts), and analogue input options (for software module eIO). See the chapter dealing with National Instruments products in*Avaya DECT Messenger Installation and Commissioning, NN43120-301* for more information.
  - V.24 multi port card.

Software Requirements

DECT Messenger works with the following required and optional software:

- Required software
  - Windows 2000/XP Professional or Windows 2000/2003 Server.
  - If you decide to use MS SQL Server as the database engine, you must have Windows 2000/2003 Server. Windows 2000/2003/XP Professional is not supported for SQL Server. (MSDE is supported under Windows 2000/2003/XP Professional.)
  - Minimum required Service Package is SP4.
  - WINZIP to unzip the DECT Messenger files during installation.
  - Virus scanner, because your DECT Messenger is connected to a network.
- Optional software.
  - Internet Information Server (IIS) under Windows 2000. This is only required if you use the eSMTP-Server module for receiving e-mail.
  - Apache WEB server under MS Windows. Apache Web server is an optional component that is included on the CD-ROM, and can be installed during set up of DECT Messenger.

DMC Configuration

This section describes DMC configuration requirements and options.

General

DECT Messenger version 4.0 and later require the following firmware on Avaya DECT Mobility Cards (DMC):

- DMC-4 Firmware: 45100404.dwl firmware
- DMC-8 Firmware: 47000404.dwl firmware

Connection to a DMC

The DECT Messenger Server can be connected to the DMC (DECT system) using a TCP/IP connection. Verify that your network allows traffic from DECT Messenger to the DMC.

DECT Messenger uses a CTI port to send and receive LRMS messages, requiring one CTI Messaging Link for each connection to a DECT system. On the DMC card, the default port number to be used for LRMS Messages is 1025.

To connect to the DECT system you must have the following applications running on your DECT Messaging Server.

- DECT Messenger eKERNEL
- CSTA_Service (runs in the system tray)
- DECT Messenger eDMSAPI

The CSTA_Service provides the CTI link to the DMC.

Connection to Multiple DECT Systems

To connect to more than one DECT system you must have a CTI link for each DECT system. Check your license for the number of CTI links available to you.

For each DECT system, you must configure a new eDMSAPI module instance. Each DECT System must be configured in a different Area, as shown in Figure 18: Connecting to two DECT systems on page 79.

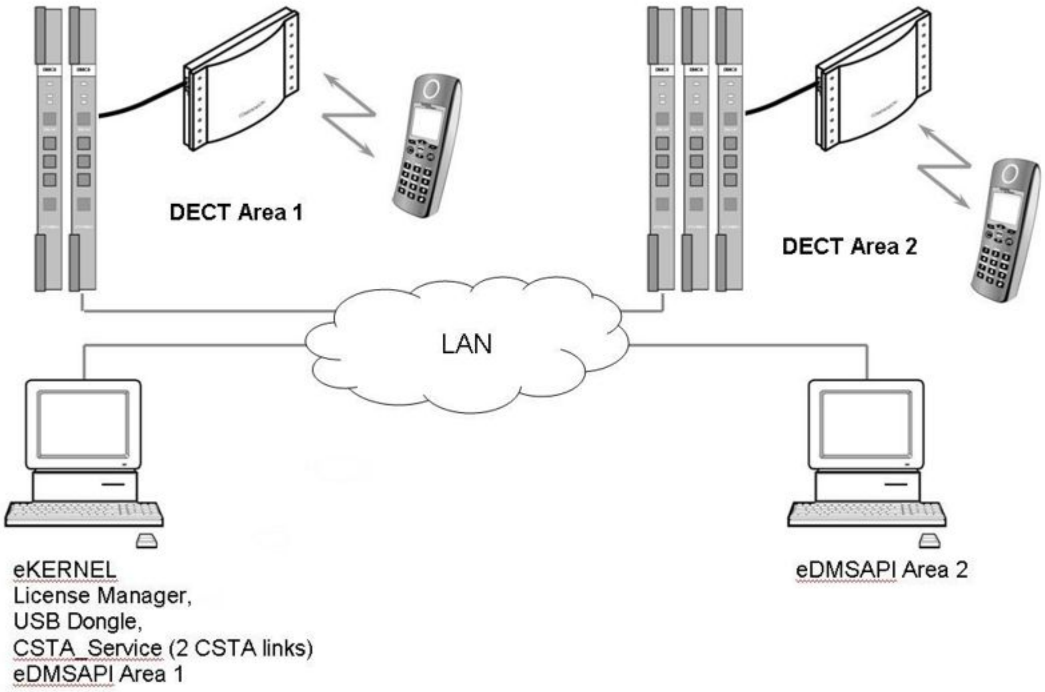


Figure 18: Connecting to two DECT systems

Example: Connecting to Two DECT systems.

eKERNEL and eCONFIG are on PC One, as shown in both Figure 18: Connecting to two DECT systems on page 79 and Example: Connecting to Two DECT systems. on page 79. Within the eCONFIG are two eDMSAPI module instances configured for two areas.

- eDMSAPI Area 1 contains the IP addresses for PC 1, and PBX IP address for DECT System 1.
- eDMSAPI Area 2 contains the IP addresses for PC 2, and PBX IP address for DECT System 2.

Table 9: Example: Connecting to two DECT systems

PC 1:	PC 2:
License, Dongle, License Manager eKERNEL eCONFIG CSTA_Service (With at least 2 CTI links) eDMSAPI module - Area 1	eDMSAPI module - Area 2

DATABASES in DECT Messenger

This section describes the databases used by DECT Messenger.

Supported Database types

DECT Messenger uses two databases:

- Configuration Database

  In this database, all configuration data is stored. You can make a copy of this database as a configuration backup. This database is always an MS Access type, and has file name: Messenger_CFG.mdb.

- Dynamic Database

  The dynamic database contains all data about messages. There are three types of databases possible:

  - MS Access

  This is a simple solution that does not require extra database setup actions. The disadvantage of the MS-Access type of database is that the database slowly grows, eventually consuming significant resources. After you shut down the eKERNEL, a database compression function runs to reduce the size of the database.

  The database has the file name: Messenger_DATA.mdb.

  The DECT Messenger eKERNEL has direct access to the database. The eWEB module has access to the database through ODBC.

  - MSDE

    The MSDE (MicroSoft Database Engine) is the database engine that is used in the MS SQL database. However, no user interface is available, and the maximum number of concurrent users is five. This is not a problem for DECT Messenger because you do not need database maintenance on the DECT Messenger database. To install the database under MSDE, a Batch file is available. The number of concurrent users is normally less than five.

    The DECT Messenger eKERNEL and the eWEB modules have access to the database through ODBC. You must set up the ODBC link in the ODBC, which is described in Installing ODBC.

  - SQL Server

This is the most extended type of database. SQL Server provides a user interface to perform Database maintenance. You must install the DECT Messenger database in MS SQL Server manually.

MS SQL Server is a licensed product. For more information about the license structure, consult the Microsoft WEB Site. The MS SQL Server also requires MS Windows 2000/2003 Server.

The DECT Messenger eKERNEL and the eWEB modules have access to the database through ODBC.

You must set up the ODBC link in the ODBC, which is described in Installing ODBC.

How to set up the Databases

Setting up the databases is described in Installing and getting started on page 81. However, you must decide which type of database to use (MS Access or MSDE).

Note:

If you decide to change database type after the installation is completed, in most cases you can easily switch between the two. However, you cannot change database type from MS Access/MSDE to SQL Server, if you are running Windows 2000/2003/XP Professional, because for SQL Server you must have Windows 2000/2003 Server.

Installing and getting started

After installation you must make some changes to have a functioning system. To install the software, follow the actions in the procedures in the following sections.

Switch the Default WEB access in IIS **off** to avoid conflicts with the Apache WEB server in DECT Messenger

Stopping IIS WEB Services

Note:

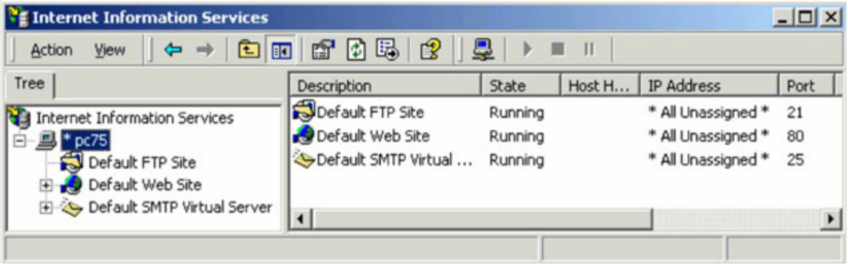
This section is only applicable if Internet Information Services (IIS) is installed in your Windows 2000 configuration, and the Apache Server is installed for DECT Messenger WEB access.

If the Microsoft Internet Information Services (IIS) is installed in Windows, you must stop the IIS WEB Services, otherwise IIS conflicts with the Apache Server. Stopping the WEB services of IIS is described in Stopping WEB Services IIS for DECT Messenger on page 82.

Stopping WEB Services IIS for DECT Messenger

1. Open the Internet Information Services (IIS) window.

   Open IIS by clicking **Start** on the Windows task bar, and choosing **Settings Control Panel > Administrative Tools > Internet Services Manager**.


Internet Information Services
Action
View
Tree
Internet Information Services
* pc75
Default FTP Site
Default Web Site
Default SMTP Virtual Server

Description	State	Host H...	IP Address	Port
Default FTP Site	Running		* All Unassigned *	21
Default Web Site	Running		* All Unassigned *	80
Default SMTP Virtual ...	Running		* All Unassigned *	25

2. Expand the PC name.

   If the PC name is not expanded, click the **+** sign next to the name to expand the list and access options for the FTP, WEB, and SMTP services.

3. Stop the Default Web Site.

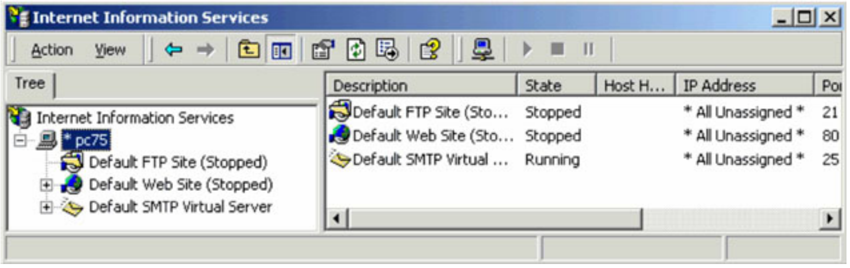
   Right-click **Default Web Site** to access the pop-up menu. Select **Stop** in this menu.

   Note:

   If the Default Web Site is already stopped, IIS has detected that a conflict on port 80 has occurred with the Apache Web server. Stopping the Default Web Site prevents this conflict.

4. Verify that the service is stopped.

   Ensure that the State column indicates **(Stopped)** next to **Default Web Site**.


Internet Information Services
Action
View
Tree
Internet Information Services
* pc75
Default FTP Site (Stopped)
Default Web Site (Stopped)
Default SMTP Virtual Server

Description	State	Host H...	IP Address	Po
Default FTP Site (Sto...	Stopped		* All Unassigned *	21
Default Web Site (Sto...	Stopped		* All Unassigned *	80
Default SMTP Virtual ...	Running		* All Unassigned *	25

   IIS no longer starts the Web services.

Installing DECT Messenger

The software installation process is described in *Avaya DECT Messenger Installation and Commissioning, NN43120-301*.

Installation of DECT Messenger Software

1. Verify that the licenses and Options are set correctly in the DMC.
2. Verify that the CSTA link to the DMC is installed and operational.
3. Verify license availability.

   Ensure that you have a DECT Messenger application license available, and that you have sufficient Seat licenses for DECT Messenger.

   > **Note:**
   >
   > After DECT Messenger starts, the eDMSAPI module reserves the number of licenses that are specified in the eDMSAPI configuration. If the DMC does not have sufficient seats for these reservations, the connection to the DMC generates errors.

4. Follow the Installation instructions.

   The installation procedure is described in *Avaya DECT Messenger Installation and Commissioning, NN43120-301*.

After the installation of DECT Messenger, carry out the next procedure, Stopping IIS WEB Services on page 81.

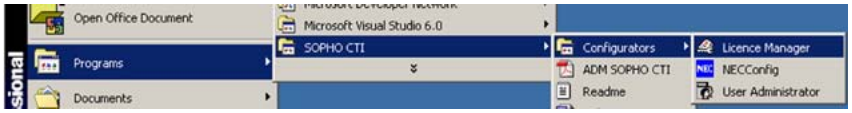
Getting Started

After installation, you can start DECT Messenger by restarting the PC. Getting Started provides the procedure to start using the system.

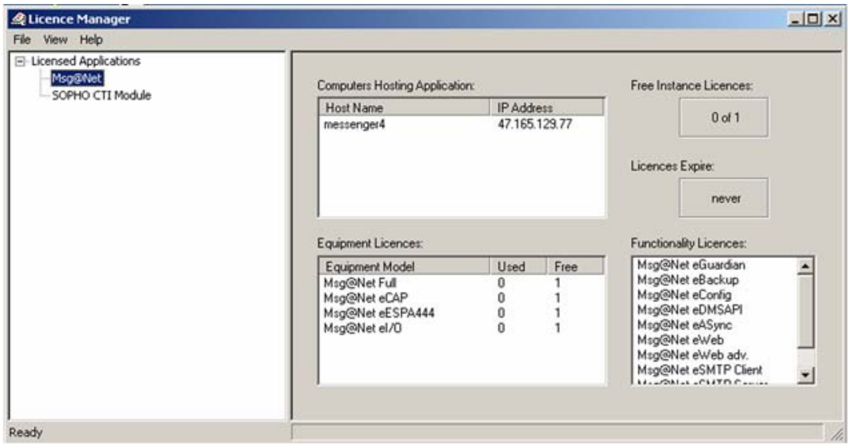
> **Note:**
>
> To load your license file you must first acquire the License file licxxxx.lic and the DECT Messaging USB Dongle

Getting Started

1. Install the dongle and start the License Manager.
   - Click **Start** on the Windows task bar and choose **Programs > SOPHO CTI > Configurators > License Manager**:



   - The License Manager window appears, and a dialog appears requesting a license file.
2. Select the license file.
   - Browse to the location where your license file is located, and click **Open**.



Computers Hosting Application:

Host Name	IP Address
messenger4	47.165.129.77

Free Instance Licences: 0 of 1

Licences Expire: never

Equipment Licences:

Equipment Model	Used	Free
Msg@Net Full	0	1
Msg@Net eCAP	0	1
Msg@Net eESPA444	0	1
Msg@Net eI/O	0	1

Functionality Licences:

Msg@Net eGuardian
Msg@Net eBackup
Msg@Net eConfig
Msg@Net eDMSAPI
Msg@Net eASync
Msg@Net eWeb
Msg@Net eWeb adv.
Msg@Net eSMTP Client

- Close the License Manager.

3. Install a preconfigured database, if you have one.

   DECT Messenger already contains a configuration database with data. However you must adapt the data in the database to your needs.

   However, if you have a preconfigured database, specifically made for your system, you must install that database into the database directory, by carrying out the following steps:

   - Open the following directory using the Windows Explorer: `c:\SOPHO Messenger@net\mdb\`.
   - If the file messenger_CFG.mdb file exists, rename it with the following name: `previous_messenger_CFG.mdb`.
   - Copy the preconfigured database into the directory: `c:\SOPHO Messenger@net\mdb`.
   - Rename the copy with the following name: `messenger_CFG.mdb`.

4. Configure eGRID tables.

   If you are not familiar with eGRID, skip to step 5. If you are familiar with eGRID, edit the following tables:

   - eKERNEL_AREA
   - eKERNEL_SITE
   - eDMSAPI
   - eKERNEL_DEVICE
   - eWEB

   Use the help information to fill in the tables.

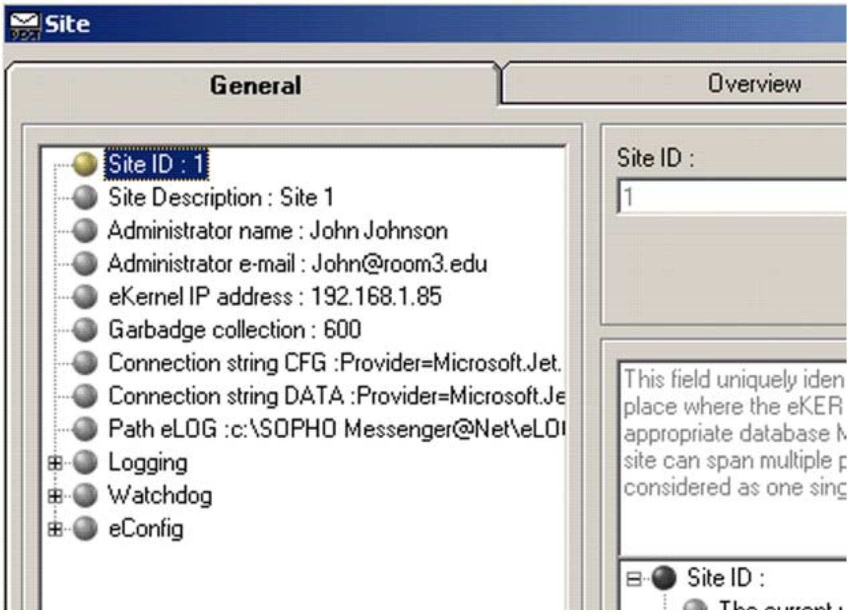
5. Start eCONFIG.

If you have already edited the tables using the instructions in step 4, skip to step 7. If not, start eKERNEL:

- Click **Start** on the Windows task bar, and choose **Programs >... eKERNEL**.
- Start the module eCONFIG.
- Log in as user: `admin`, with password: `admin`.

6. Enter configuration values.

- In the eCONFIG window, double-click the **Site Site1 line**. The following window opens:



Site ID : 1
Site Description : Site 1
Administrator name : John Johnson
Administrator e-mail : John@room3.edu
eKernel IP address : 192.168.1.85
Garbadge collection : 600
Connection string CFG :Provider=Microsoft.Jet.
Connection string DATA :Provider=Microsoft.Je
Path eLOG :c:\SOPHO Messenger@Net\eLO
Logging
Watchdog
eConfig

Site ID :
1

This field uniquely iden
place where the eKER
appropriate database M
site can span multiple p
considered as one sing

Site ID :

- Enter the Administrator name and Administrator e-mail.
- Enter the IP address of the PC where the eKERNEL resides in the field: eKERNEL IP Address.
- Click **OK**.

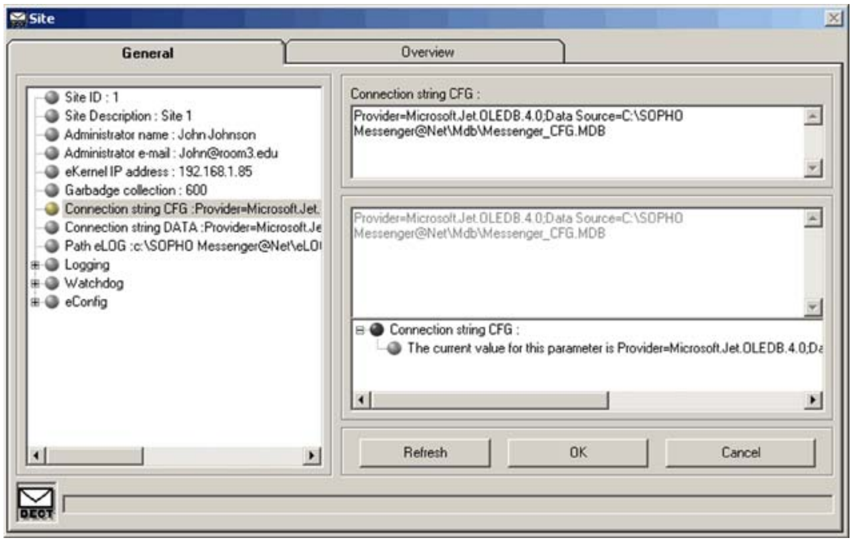
7. Verify the Configuration database path.

Still in the eCONFIG window, you must specify the database locations (the default database path are usually correct).

- Set the path to the Messenger Configuration database to the following directory: `c:\SOPHO Messenger@net\Mdb\` (unless you have installed to a directory other than the default). The file name is Messenger_CFG.mdb.
- Verify the path setting for the Configuration database; normally you do not need to change this.

Note:

The Configuration database type is always MS Access and always points directly to a file (not using ODBC). The default setting is shown in the following illustration:



Site ID : 1
Site Description : Site 1
Administrator name : John Johnson
Administrator e-mail : John@room3.edu
eKernel IP address : 192.168.1.85
Garbadge collection : 600
Connection string CFG :Provider=Microsoft.Jet.
Connection string DATA :Provider=Microsoft.Je
Path eLOG :c:\SOPHO Messenger@Net\eLO
Logging
Watchdog
eConfig

Connection string CFG :

Provider=Microsoft.Jet.OLEDB.4.0;Data Source=C:\SOPHO Messenger@Net\Mdb\Messenger_CFG.MDB

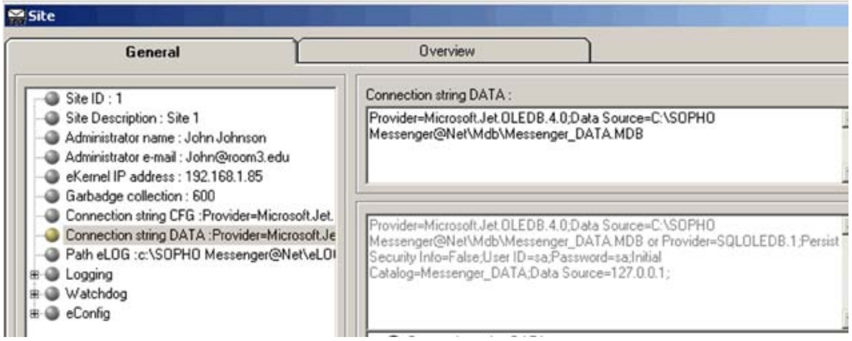
Provider=Microsoft.Jet.OLEDB.4.0;Data Source=C:\SOPHO Messenger@Net\Mdb\Messenger_CFG.MDB

Connection string CFG :
The current value for this parameter is Provider=Microsoft.Jet.OLEDB.4.0;Da

8. Check the Dynamic database path.

   eKERNEL must have a valid path to the dynamic data database (the default database path are usually correct). Determine which type of database you are using: MS Access, MSDE, or SQL Server. The settings for MSDE and SQL Server in this window are the same as the settings in eCONFIG.

   - If you are using the MSDE or SQL Server database, ensure that you have set up the ODBC configuration for the eWEB correctly. Ensure that you have installed the Messenger_Data database in MSDE (by running a Batch file), or in SQL Server, using the instructions in *Avaya DECT Messenger Installation and Commissioning, NN43120-301*.
   - Set the path to the MS Access database: By default this database resides in the following directory: `C:\SOPHO Messenger@net\Mdb\`. The file name is Messenger_DATA.mdb. The following illustration shows the setting for the default configuration.



Site ID : 1
Site Description : Site 1
Administrator name : John Johnson
Administrator e-mail : John@room3.edu
eKernel IP address : 192.168.1.85
Garbadge collection : 600
Connection string CFG :Provider=Microsoft.Jet.
Connection string DATA :Provider=Microsoft.Je
Path eLOG :c:\SOPHO Messenger@Net\eLO
Logging
Watchdog
eConfig

Connection string DATA :

Provider=Microsoft.Jet.OLEDB.4.0;Data Source=C:\SOPHO Messenger@Net\Mdb\Messenger_DATA.MDB

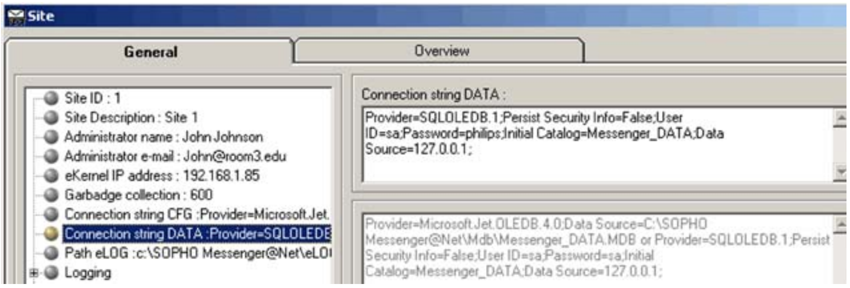
Provider=Microsoft.Jet.OLEDB.4.0;Data Source=C:\SOPHO Messenger@Net\Mdb\Messenger_DATA.MDB or Provider=SQLOLEDB.1;Persist Security Info=False;User ID=sa;Password=sa;Initial Catalog=Messenger_DATA;Data Source=127.0.0.1;

- Configure the path for the MSDE or SQL Server database: The path setting for the MSDE or SQL Server database must point to the ODBC link that you created after you installed the eWEB module.

Note:

The path setting for the MSDE or SQL Server database must be assigned as System DSN in ODBC.

Before you continue, ensure that you know the username and password for the database. Normally the User ID (login name) for the database is `sa`, and the password is `sa`. The following illustration shows the eKERNEL settings for the Messenger_DATA database with User ID `sa` and password `philips` (the default password is sa).



- Site ID : 1
- Site Description : Site 1
- Administrator name : John Johnson
- Administrator e-mail : John@room3.edu
- eKernel IP address : 192.168.1.85
- Garbadge collection : 600
- Connection string CFG :Provider=Microsoft.Jet.
- Connection string DATA :Provider=SQLOLEDE
- Path eLOG :c:\SOPHO Messenger@Net\eLO
- Logging

Connection string DATA :

```
Provider=SQLOLEDB.1;Persist Security Info=False;User
ID=sa;Password=philips;Initial Catalog=Messenger_DATA;Data
Source=127.0.0.1;
```

```
Provider=Microsoft.Jet.OLEDB.4.0;Data Source=C:\SOPHO
Messenger@Net\Mdb\Messenger_DATA.MDB or Provider=SQLOLEDB.1;Persist
Security Info=False;User ID=sa;Password=sa;Initial
Catalog=Messenger_DATA;Data Source=127.0.0.1;
```

Note:

The Data Source =127.0.0.1 points to the local host. If you do not enter this information, the eKERNEL automatically assumes that the data source is local. Therefore, if the ODBC is on the same PC as the eKERNEL, you do not need to enter the Data source at all, as shown in the following line:

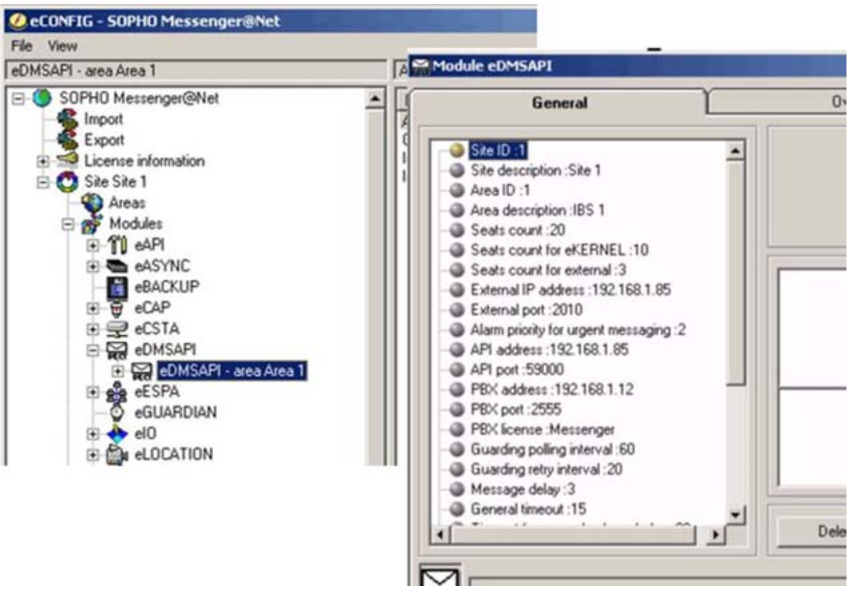
```
Provider=SQLOLEDB.1;Persist Security Info=False;User
ID=sa;Password=philips;Initial Catalog=Messenger_DATA;
```

9. Set Area.

   Double-click the menu **Areas**. Change the Area name of Area 1. If necessary remove or change Area 2. This field defines the Area number/name relationship for administrative purposes.

10. Open the property settings for eDMSAPI.

    - Expand the module eDMSAPI, by clicking the **+** sign in front of it.
    - Double-click the instance of the eDMSAPI to open the parameter/property settings.



Site ID :1
Site description :Site 1
Area ID :1
Area description :IBS 1
Seats count :20
Seats count for eKERNEL :10
Seats count for external :3
External IP address :192.168.1.85
External port :2010
Alarm priority for urgent messaging :2
API address :192.168.1.85
API port :59000
PBX address :192.168.1.12
PBX port :2555
PBX license :Messenger
Guarding polling interval :60
Guarding retry interval :20
Message delay :3
General timeout :15

11. Enter configuration information.

    Enter the correct values for the IP addresses:

    - Area Description - Description field for the DECT system you are connecting to. Seats Count - Total number of seats you require. (See the Note at the end of this list)
    - Seats count for eKERNEL - Default value = 10
    - Seats count for external - Number of seats for eWEB - Default = 3
    - External IP address - The IP address of the PC on which the eDMSAPI runs External Port - Default = 2010
    - API Address - IP address of the PC where the CSTA_Service is running API Port - Default = 59000
    - PBX Address: IP address of the DMC on the DECT System you are connecting to.
    - PBX Port - Always 1025 for DMC PBX Type – CS 1000
    - PBX License - Always Messenger
    - PBX Type - Always Avaya

    Note:

    Only specify the number of seats you anticipate requiring, (not the total number of seats allowed by your license), as takes longer for seats to register. Ensure that you do not exceed the number of seats (CTI Messaging Channels) as specified in your license Manager. If the number of seats is not sufficient in the License, you cannot make an LRMS (E2) message call.

12. Add a DECT Device.

13. Configure eWEB module.

    - Expand the item **Modules > eWEB Module**. One instance of the eWEB module: eWEB - area <x> is shown.
    - Double-click the eWEB instance to open the parameters/properties. Click **IP addresses**, as shown in Figure 19: eWEB Properties on page 90. The first line in the right pane contains the loop back address (127.0.0.1) of the PC. Do not change this. The second line contains the correct IP addresses.
    - Select the second line, and click **Edit**.
    - Enter the IP address of the PC where the Apache server resides in the field: **eWEB_address_str**.
    - Enter the IP address of the PC where the eKERNEL resides in the field: **eWEB_ekernel_address_str**.
    - Any data in additional lines is normally not relevant, and can be deleted.

      Note:

      To delete a line:

      - select the line.

      - click **Edit**.

      - click **Delete**.

    Warning:

    Do not select a line and click **Delete**, because that deletes the entire module.

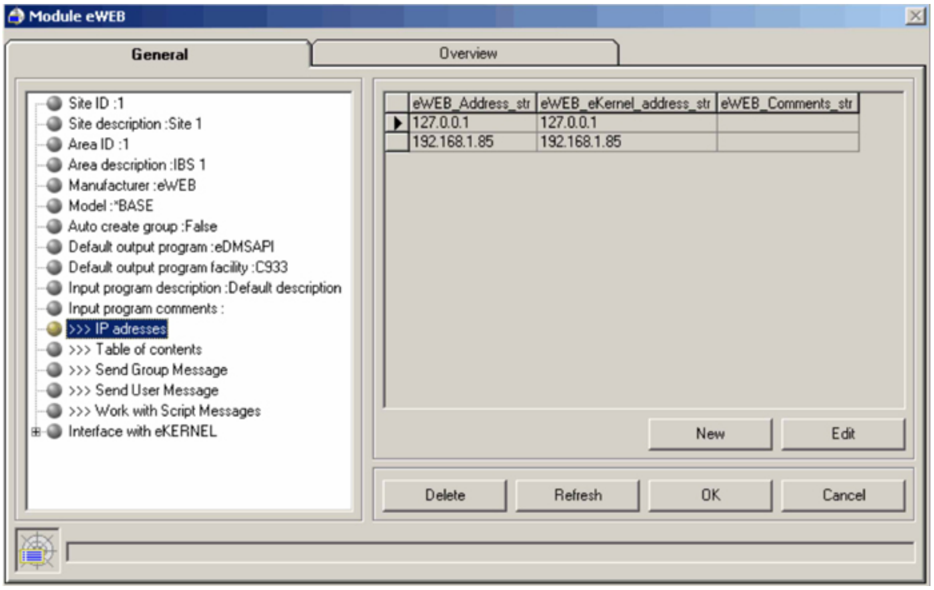
    - Click **OK** to save the new settings.

14. Verify the operation of DECT Messenger.

    - Start the eKERNEL from the shortcut in the Windows **Start** menu.
    - Start the CSTA_Service. This appears in the system tray.
    - Start the eDMSAPI module.
    - Open your WEB browser, and enter the correct DNS name or the IP address of the PC where the Apache WEB server resides.
    - Log in with the name that you specified in the table eWEB_USER_AUTH. The web page opens.
    - In the left pane, go to **Send DMS-API Message**. Enter a message, and select an extension from the list. Note that the information in the list comes from the table: eKERNEL_DEVICE.
    - Click `Enter` to send the message.

    Verify that the message arrives at the extension that you have specified; if the message arrives, your DMS-API is working correctly.

    Now you can set up the other modules as needed.



- Site ID :1
- Site description :Site 1
- Area ID :1
- Area description :IBS 1
- Manufacturer :eWEB
- Model :*BASE
- Auto create group :False
- Default output program :eDMSAPI
- Default output program facility :C933
- Input program description :Default description
- Input program comments :
- >>> IP adresses
- >>> Table of contents
- >>> Send Group Message
- >>> Send User Message
- >>> Work with Script Messages
- Interface with eKERNEL

eWEB_Address_str	eWEB_eKernel_address_str	eWEB_Comments_str
127.0.0.1	127.0.0.1	
192.168.1.85	192.168.1.85	

Figure 19: eWEB Properties

Using eCONFIG

The eCONFIG Module is the tool most commonly used for making changes in the configuration. The configuration is stored in a Database. Be cautious when editing the database, because incorrect or invalid entries can interfere with the operation of DECT Messenger.

You can use the eCONFIG on the local PC that is the DECT Messenger server PC. You can also install the eCONFIG on a remote PC to perform remote configuration maintenance. The database is handled is differently for local and remote maintenance.

Using eCONFIG (Local) on the DECT Messenger Server PC

After the eCONFIG is installed on the DECT Messenger server PC the database is handled as shown in Figure 20: Database handling with eCONFIG on the DECT Messenger Server PC (Local) on page 91.

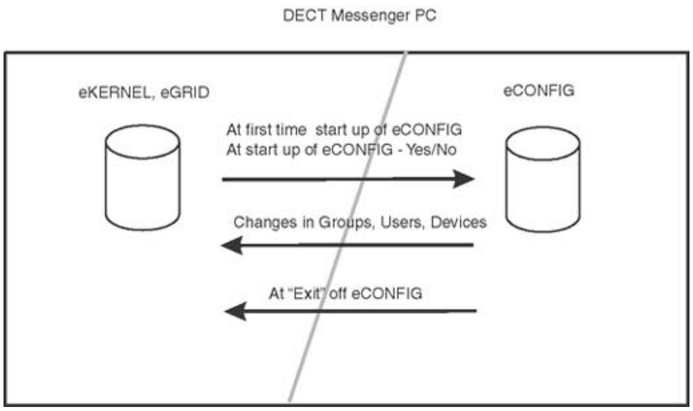

DECT Messenger PC
eKERNEL, eGRID
eCONFIG
At first time start up of eCONFIG
At start up of eCONFIG - Yes/No
Changes in Groups, Users, Devices
At "Exit" off eCONFIG

Figure 20: Database handling with eCONFIG on the DECT Messenger Server PC (Local)

After you start the eCONFIG for the first time, a copy is made of the configuration database of DECT Messenger (Messenger_CFG.MDB). This copy is stored in the eCONFIG directory: C:\SOPHO Messenger@net eConfig\Mdb with the file name: Messenger_WRK.cfg. After you make configuration changes using the eCONFIG, these changes are stored in the copy of the database (Messenger_WRK.cfg) in the eCONFIG directory. To make these changes active, you must:

Making configuration changes active

1. Close down eTM, eKERNEL, eWEB, and so on.
2. Close eCONFIG using the menu option **File > Exit**. The operational database is deleted automatically. The database from the eCONFIG is stored into the DECT Messenger directory, and renamed to Messenger_CFG.MDB, which is the new operational database.
3. Restart the modules that you closed down; your new configuration is active.

Note:

After you make changes in the copy of the database in eCONFIG, ensure that nobody else is making changes in the operational database, as that causes an error if you try to shut down the eCONFIG and write the database back into the DECT Messenger directory.

Note:

If there are Monitored devices in the active configuration, and one of these devices initiates a follow-me, the diversion information is stored in the active database. Therefore, you cannot restore the eCONFIG database, and any changes you have made are lost (except for the changes in Users, Groups, and Devices, as explained in the following paragraph).

If you make changes in Users, Groups or Devices, these changes are stored in the eCONFIG database (Messenger_WRK.cfg) and in the operational database (Messenger_CFG.mdb), and are therefore immediately activated. Saving this information into the operational database is done by sending an XML string from the eCONFIG to the eKERNEL. The eKERNEL stores this information into the operational database.

- Starting up the eCONFIG again

After you start the program again, eCONFIG finds a database in its directory. eCONFIG asks you whether you want to continue with this database or retrieve a fresh copy from the operational database. Avaya recommends that you make a fresh copy of the operational database, because then you are sure there is no database inconsistency.

Using eCONFIG (Remote) on remote PC (client) in the Network

After the eCONFIG is installed on the DECT Messenger server PC the database is handled as shown in Figure 21: eCONFIG database handling when used on a remote PC (client PC) on page 92.

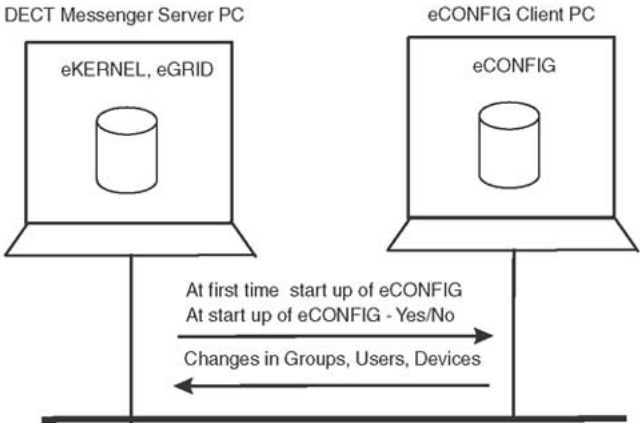

DECT Messenger Server PC
eCONFIG Client PC
eKERNEL, eGRID
eCONFIG
At first time start up of eCONFIG
At start up of eCONFIG - Yes/No
Changes in Groups, Users, Devices

Figure 21: eCONFIG database handling when used on a remote PC (client PC)

After you start the eCONFIG for the first time on the remote PC, a copy is made of the configuration database of DECT Messenger (Messenger_CFG.MDB). This copy is stored on the remote PC where the eCONFIG is running, in the eCONFIG directory: C:\SOPHO Messenger@net\eConfig\Mdb with the file name: Messenger_WRK.cfg. You cannot make system configuration changes in this database, only changes in:

- Users
- Groups
- Devices

After you make changes in Users, Groups or Devices, these changes are stored in the eCONFIG database (Messenger_WRK.cfg) and in the operational database (Messenger_CFG.mdb), and are therefore immediately active. Saving this information into the operational database is done by sending an XML string from the eCONFIG to the eKERNEL. The eKERNEL stores this information into the operational database.

Note:

If more than one eCONFIG is active at the same time on different PCs, the individual eCONFIG databases are not updated or synchronized after changes are made in one eCONFIG. Only the operational database, and the database in the eCONFIG module where the change is made, are updated. Changes made in Groups using the eWEB interface are not written into the databases of the eCONFIG modules. These changes are only written into the operational database, not into the eCONFIG databases.

- Starting up the eCONFIG again

  After you start the program again, eCONFIG finds a database in its directory. eCONFIG asks you whether you want to continue with this database or retrieve a fresh copy from the operational database. Avaya recommends that you make a fresh copy of the operational database, because then you are sure there is no database inconsistency.

Using eTM

The eTM is the Task Manager in DECT Messenger. The eTM opens in the Windows system tray, and monitors the modules of DECT Messenger. If a module shuts down, eTM restarts it.

eTM searches for the following key in the system registry to find out which modules to start, and which PC to start them on:

(HKEY_Current_User/Software/Philips/c:\SOPHO Messenger@net/eTM).

The registry is not filled in automatically. You must edit it manually, with the help of a registry file, which is generated after you close down the eCONFIG using the **File > Exit** menu. You can also create the registry files using eGRID, using the button **Generate Registry files for eTM** in the right-top corner of the interface. The registry files are stored in the following directory:

C:\SOPHO Messenger@net\exe\

An example of the file name is as follows:

eTM - Site 1 - Environment: LOCAL.reg for the local PC, which is the PC where the eKERNEL is running.

If you have modules running on other PCs, other registry file names are given, which are to be executed on the PC where the modules are running. For example:

eTM - Site 1 - Environment: 192.168.1.81.reg for the PC with IP address 192.168.1.81.

Note:

On these PCs you must also have eTM running if you want to use the Task Manager.

Note:

An Environment is specified in the name of this registry file. The Environment is the IP address of a PC where a module is running. On that PC you must install the registry file, if you want to use the eTM on that PC.

Environments defined as LOCAL refer to the PC where the eKERNEL is running, whereas environments that have an IP address refer to the IP address of the PC where the modules are running.

To add the contents of the registry file into the registry, double-click the *.reg file. To remove the contents from the registry again, open the registry, go to (HKEY_Current_User/Software/Philips/), and remove the key of a module from the registry.

eDMSAPI Inbound

The eDMSAPI supports inbound LRMS (Low Rate Message Services) calls from DECT handsets that support LRMS (E2) messaging.

There are several types of incoming calls, which are briefly explained in the following subsections.

Incoming Alarm (IA) from DMC

Incoming Alarm is an LRMS (E2) message that is sent from an LRMS DECT extension to an extension number (DNR) in the DMC. However, the DECT handset from which the LRMS (E2) message is sent is monitored (IO Registered) by DECT Messenger. The message is delivered to DECT Messenger, instead of to the intended destination. Therefore, if you send a message from one DECT handset to another, and the originating handset is IO Registered by DECT Messenger, this message is not sent to the intended destination directly; DECT Messenger decides what to do with the message. DECT Messenger treats this incoming message in the same way as any incoming message, and sends it to the devices specified in a group.

Note:

A message sent from an IO registered DECT handset to another DECT handset always uses DECT Messenger, with a Group-to-Group Member-to-Device structure.

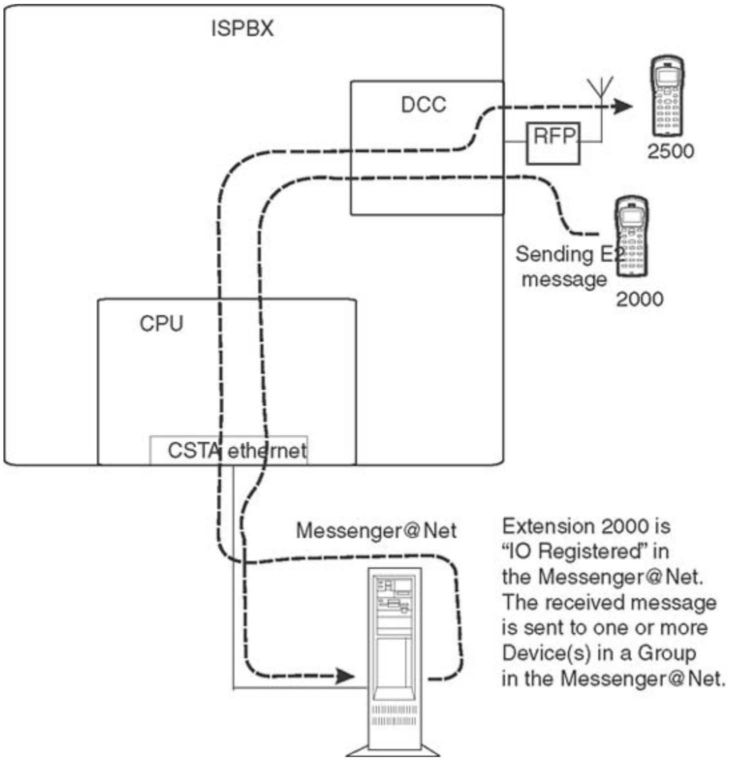

ISPBX
DCC
RFP
2500
Sending E2 message
2000
CPU
CSTA ethernet
Messenger@Net
Extension 2000 is "IO Registered" in the Messenger@Net. The received message is sent to one or more Device(s) in a Group in the Messenger@Net.

Figure 22: Incoming alarm (IA) in eDMSAPI

Figure 22: Incoming alarm (IA) in eDMSAPI on page 95 illustrates the handling of an incoming message (IA) in the eDMSAPI module, as follows:

- DECT extension 2000 sends a message to extension 1200. DECT extension 2000 must be IO Registered in the Device settings for extension 2000. Therefore, all LRMS (E2) messages that extension 2000 sends are sent to DECT Messenger.
- DECT Messenger checks the intended destination of the message. If that destination is in the Inbound configuration in the eDMSAPI module, the message is regarded as a valid call.
- Based on the combination of the Originator (2000, in this example), and the intended destination (2500, in this example), the message is transferred to a Group in DECT Messenger with an appropriate Alarm Identifier. The Group contains Group members (Devices) to which the message is to be sent.
- If the Group member is extension 2500 (DECT) then the message arrives in the display of extension 2500.

Incoming Alarm (IA) from IP DECT

Incoming Alarm is an LRMS (E2) message that is sent from an LRMS DECT extension to another extension number (DNR). In an IP DECT configuration, no direct messaging between handsets is possible. Instead, the message is available at a TCP/IP port on the IP DECT system. The DECT Messenger system retrieves Incoming Alarms from IP DECT through this TCP/IP port.

If a DECT handset needs to send messages to DECT Messenger, the extension number of the handset must be IO monitored (IO Registered) in DECT Messenger. After an incoming message is received by DECT Messenger from a handset, the message goes to a group that contains devices. The incoming message is sent to all the devices specified in the Group.

Note:

The IP DECT system does not support sending a message from one DECT handset to another directly. For sending a message from one DECT handset to another, you always need a DECT Messenger system.

Incoming Confirmation (IC)

Incoming Confirmation is an LRMS (E2) message that is sent to an extension number (DNR) in the DMC, and is used to reset an outstanding alarm on a device. The DECT handset from which the LRMS (E2) message is sent, is monitored (IO Registered) by DECT Messenger. The CLI of the DECT extension is used as identifier for resetting an outstanding Alarm on a Device. The PIN code that is specified in the device settings must match this CLI of the DECT extension. The message that the DECT extension sends is simply ignored.

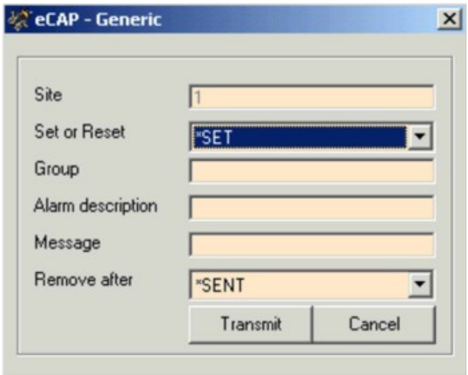
The extension number to which the message is sent for IC can be a hardware-less Directory Number (DN) in the DMC.

Note:

A message sent from an IO registered DECT handset to another DECT handset uses DECT Messenger, with a Group-to-Group Member-to-Device structure.

Parameters required to set an alarm

The structure of DECT Messenger is based on five parameters that are required for generating an alarm. Those five parameters can come from the input device. The input modules eAPI and eCAP show that these parameters are required. Figure 23: eCAP Sending Message option on page 97 shows the Sending Message option of the eCAP generic, and shows the parameters.



eCAP - Generic

Site: 1

Set or Reset: *SET

Group:

Alarm description:

Message:

Remove after: *SENT

Figure 23: eCAP Sending Message option

Not all input devices are capable of generating all five input parameters. If parameters are missing (for example, if a switch is connected to the eIO module), the parameters are taken from fields in tables.

The following five parameters are needed.

- *SET/*RESET

  This is described in SET/RESET structure on page 103.

- Group

  The Group is used to define the destination. The Group contains group members, each of which is a device.

  Note:

  This requires that the Group must be defined in DECT Messenger, otherwise an alarm for a certain group comes in but there is no group specification, which means that the alarm cannot be delivered.

- Alarm Description

  The Alarm Description refers to the eKERNEL_Alarm table, which contains all the properties that are associated with that specific alarm, such as Priority, ringing time of an extension, the repeat interval time, and so on.

- Message

  This is the actual message that is transferred to the device.

- Remove After: *SENT, *RESET, *CALCULATE

  This is described in SET/RESET structure on page 103.

Alarm handling is shown in Figure 24: Alarm handling on page 98, which illustrates an input program that provides the input parameters.

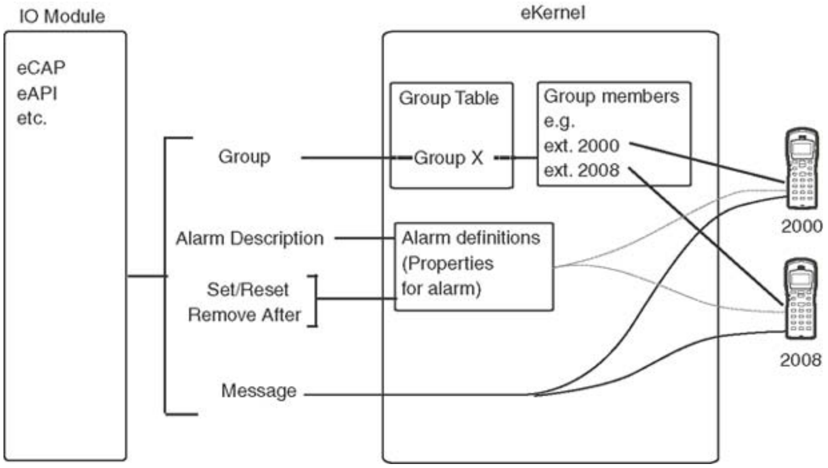


Figure 24: Alarm handling

Note:

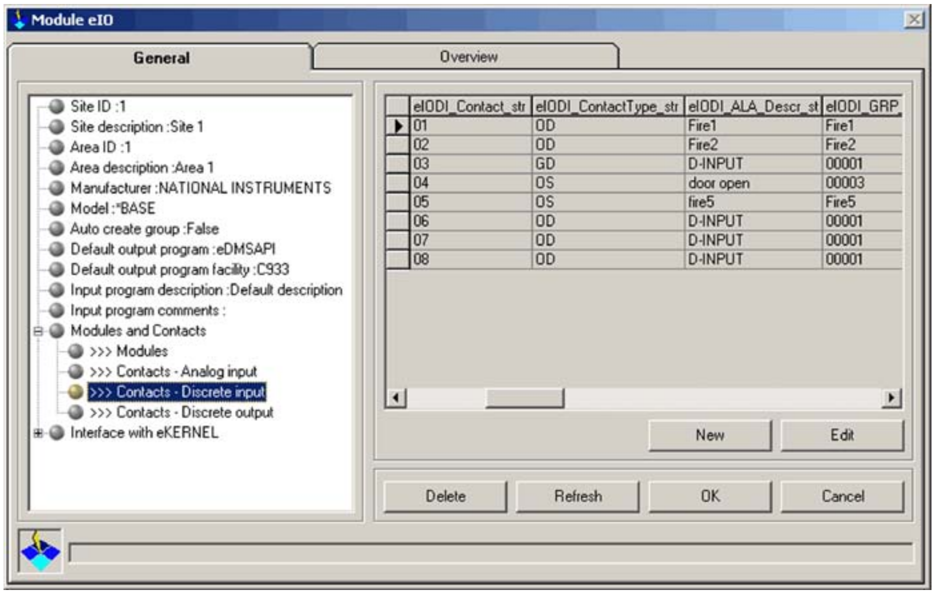
These input parameters can come from external sources (for example, eCAP or eAPI) or partly from configuration tables.

Detailed explanation of the five parameters

- Group

The input program provides a Group name to which the alarm must be sent. This Group name must be defined in the eKERNEL_GROUP table. From this eKERNEL_GROUP table a reference is made to the eKERNEL_MEMBER table. Here, the members in the group are defined. These members are already the actual devices to which the alarm must be sent. Therefore, the Group name defines to which devices the alarm is sent; the Group name is needed to connect the input program with the output devices. In fact, the tables eKERNEL_GROUP and eKERNEL_MEMBER in the configuration database are filled in correctly after you use the eCONFIG module for configuration.

Figure 25: Input/output relationships on page 99 shows an example of the relation between the input program and the output devices, and uses the eIO Module as input module.



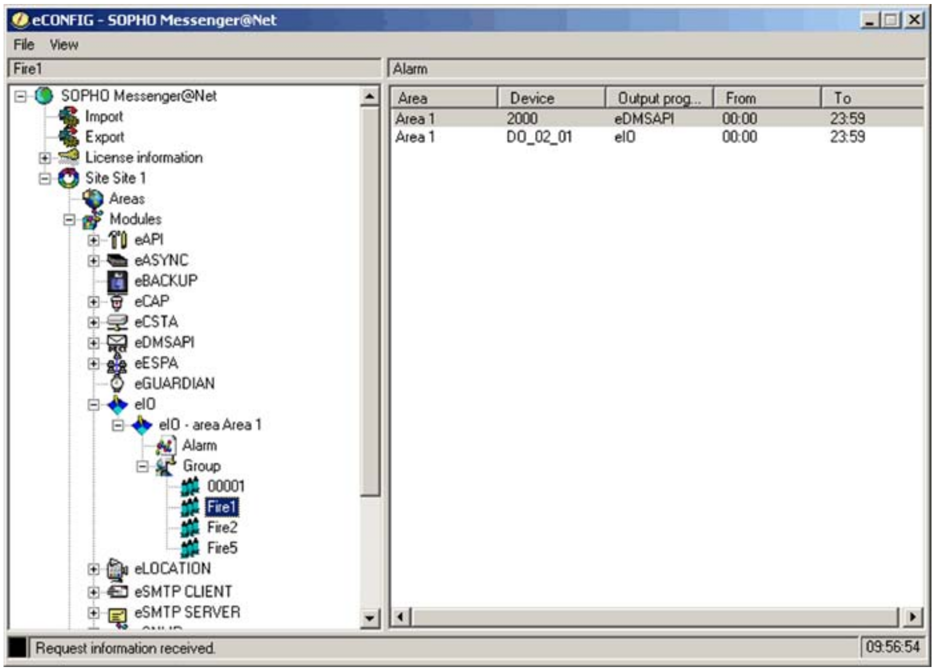
- Site ID :1
- Site description :Site 1
- Area ID :1
- Area description :Area 1
- Manufacturer :NATIONAL INSTRUMENTS
- Model :*BASE
- Auto create group :False
- Default output program :eDMSAPI
- Default output program facility :C933
- Input program description :Default description
- Input program comments :
- Modules and Contacts
  - >>> Modules
  - >>> Contacts - Analog input
  - >>> Contacts - Discrete input
  - >>> Contacts - Discrete output
- Interface with eKERNEL

eIODI_Contact_str	eIODI_ContactType_str	eIODI_ALA_Descr_st	eIODI_GRP_
01	OD	Fire1	Fire1
02	OD	Fire2	Fire2
03	GD	D-INPUT	00001
04	OS	door open	00003
05	OS	fire5	Fire5
06	OD	D-INPUT	00001
07	OD	D-INPUT	00001
08	OD	D-INPUT	00001

Figure 25: Input/output relationships

Figure 25: Input/output relationships on page 99 shows the settings in the input module IO, and illustrates the relation between the contacts (push buttons, switches) that are connected to the module. For example, contact 01 under eIODI_Contact_str has the Group name Fire1 in the column eIODI_GRP_str. Only eIODI_Group_ is shown in Figure 25: Input/output relationships on page 99.

Under the eIO Module in the eCONFIG, two menus appear: Alarm and Group. Under the Group menu, the groups that are specified in the eKERNEL for that input module are displayed, as shown in Figure 26: Groups in an input module on page 100.



Area	Device	Output prog...	From	To
Area 1	2000	eDMSAPI	00:00	23:59
Area 1	DO_02_01	eIO	00:00	23:59

Request information received. 09:56:54

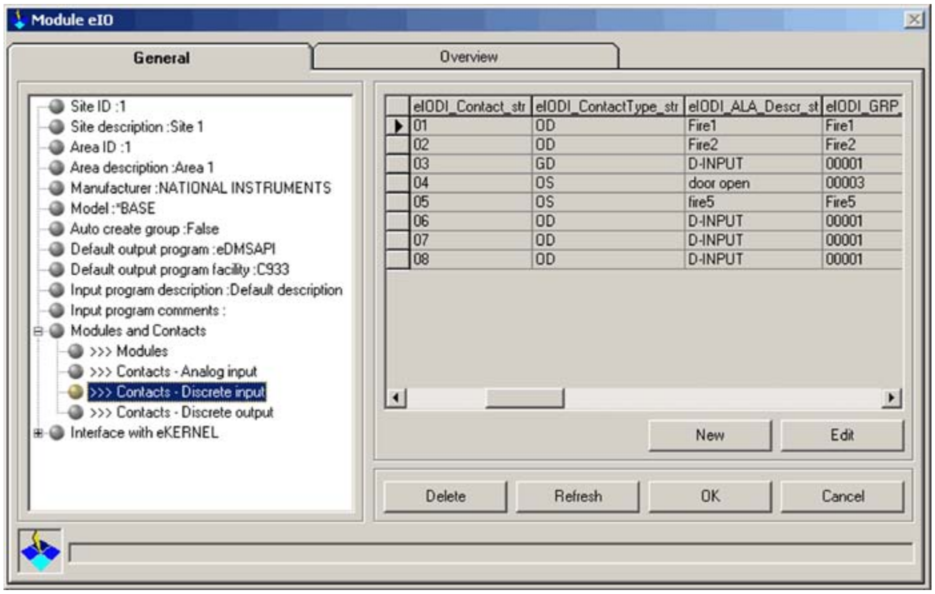
Figure 26: Groups in an input module

A Group name must match a Group name that comes from the input module. In this example, the Group name (Fire1) must match the Group name that is assigned to the input contact (01) in Figure 26: Groups in an input module on page 100. Under the Group name Fire1, two Members are listed, which are actual output Devices (Device 2000 and Device DO_02_01).

If a user presses the button connected to Contact 01, the Input Program eIO generates an Alarm for group Fire1. eIO sends this information to the eKERNEL, where a group is present with the name Fire1 for the eIO Module. The alarm is passed on to the group Members: 2000 and DO_02_01.

- Alarm

The Alarm description also comes from the input program, and can be the identifier of the input program or a character string that is received from an external device (for example, eCAP, eAPI).

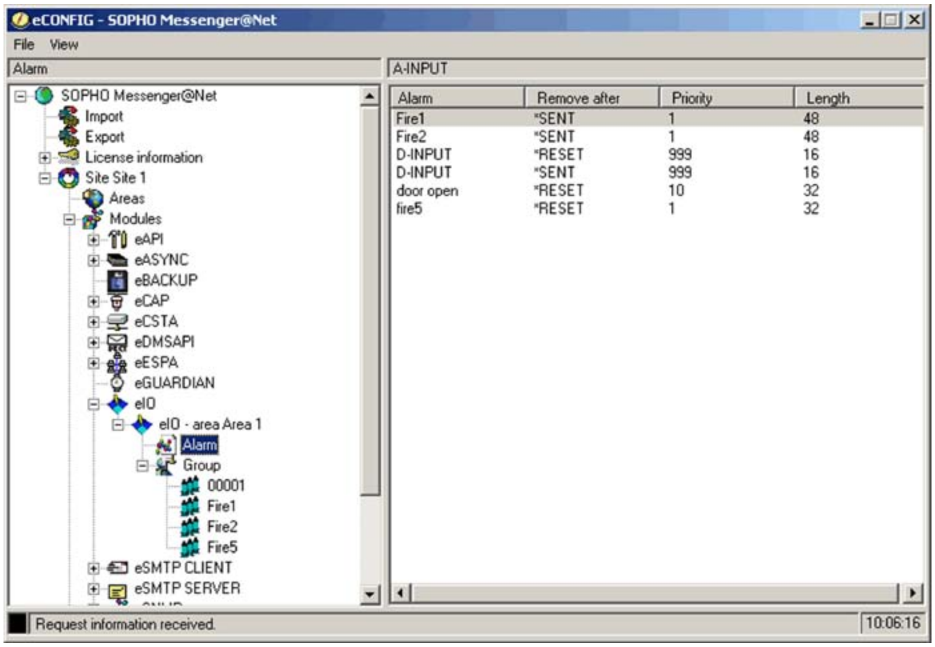


- Site ID :1
- Site description :Site 1
- Area ID :1
- Area description :Area 1
- Manufacturer :NATIONAL INSTRUMENTS
- Model :*BASE
- Auto create group :False
- Default output program :eDMSAPI
- Default output program facility :C933
- Input program description :Default description
- Input program comments :
- Modules and Contacts
  - >>> Modules
  - >>> Contacts - Analog input
  - >>> Contacts - Discrete input
  - >>> Contacts - Discrete output
- Interface with eKERNEL

	eIODI_Contact_str	eIODI_ContactType_str	eIODI_ALA_Descr_st	eIODI_GRP
▶	01	OD	Fire1	Fire1
	02	OD	Fire2	Fire2
	03	GD	D-INPUT	00001
	04	OS	door open	00003
	05	OS	fire5	Fire5
	06	OD	D-INPUT	00001
	07	OD	D-INPUT	00001
	08	OD	D-INPUT	00001

Figure 27: Input contact 01

Figure 27: Input contact 01 on page 101 shows an example of an input contact 01 in the Input Module eIO. The input contact 01 in the column eIODI_Contact_str is related to the alarm identifier Fire1 under the column eIODI_ALA_Descr_str. Therefore, if the contact is activated, the alarm Identifier Fire1 is sent to the eKERNEL. This also means that there must be an Alarm Identifier in the eKERNEL_ALARM table called Fire1. This Alarm Identifier for the eKERNEL is found in the eCONFIG, under the eIO Module (because the Alarm identifier is used for the eIO).



Alarm	Remove after	Priority	Length
Fire1	*SENT	1	48
Fire2	*SENT	1	48
D-INPUT	*RESET	999	16
D-INPUT	*SENT	999	16
door open	*RESET	10	32
fire5	*RESET	1	32

Request information received.

Figure 28: Alarm identifier

The Alarm Identifier, illustrated in Figure 28: Alarm identifier on page 102, is used as an Alarm Description, and contains properties for the alarm (for example, ringing time, repeat intervals, scroll intervals if messages are chopped). These properties determine, in part, how the alarm is displayed. Other properties include: priority of the alarm, message length, silence interval, and so on.

- Set/Reset

  Set/Reset determines if the alarm is activated or deactivated. See SET/RESET structure on page 103.

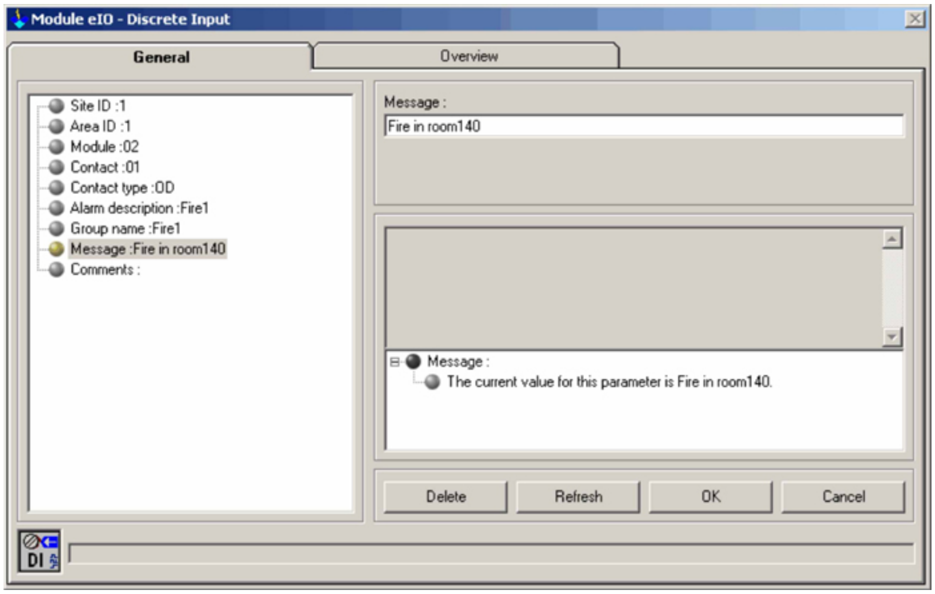
- Remove After

  Remove After specifies what is to be done with the alarm after the eKERNEL has received the alarm. Valid settings are as follows: Remove after sent, Remove after Reset or Remove after Calculate. This is discussed in SET/RESET structure on page 103.

- Message

  The message coming in through an IO Module is passed directly to the device. The way the message is displayed depends on the properties of that specific device, and the setting in the eKERNEL_ALARM table for that specific alarm. The message coming in the Input Module is transferred through the Input Module to the eKERNEL, and then to the Output Device. However, after the Input Module does not receive a message from outside, you must specify a message in the Input Module.

  An example of an Input Module that does not receive a message from outside is the eIO Module. In the eIO Module you must assign a message to a switch or button. Figure 29: Message assigned to a button on page 103 shows the message assigned to a button.



Site ID :1
Area ID :1
Module :02
Contact :01
Contact type :0D
Alarm description :Fire1
Group name :Fire1
Message :Fire in room140
Comments :

Message :
Fire in room140

Message :
The current value for this parameter is Fire in room140.

Figure 29: Message assigned to a button

SET/RESET structure

The SET/RESET structure of alarms is complex; you can Set an Alarm and wait for a Reset, or you can Set an Alarm from an Input Module to a Device. In the following section, the various aspects of the SET/RESET structure is explained.

- SENT

  The type SENT is the simplest type of alarming. Figure 30: Sent Alarm structure on page 103 shows the structure.

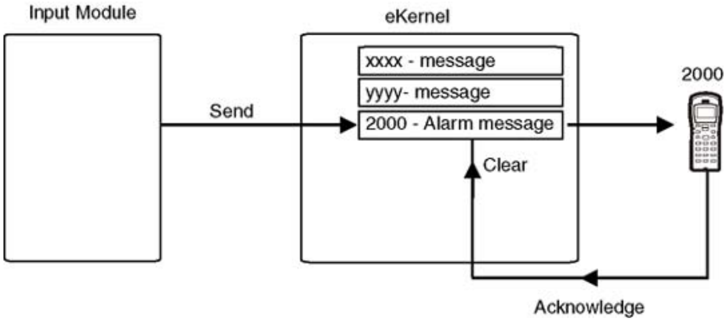


Figure 30: Sent Alarm structure

In this figure, there is an input module that generates an alarm as a sent. Therefore, the alarm is sent to the eKERNEL, and stored in an alarm database (data table). Immediately after sending, the input module withdraws the alarm, so the alarm condition is only present in the database table, with a fixed reference to the device for which the alarm message is meant. If the device acknowledges this alarm, the alarm condition is removed from the database. The acknowledgment from the device differs for each device type. If the device is an LRMS (E2) DECT handset, and the alarm was sent as a normal message, the acknowledgement is automatically generated at the moment that the message arrives at the device. If the alarm message was sent as an urgent message to an LRMS (E2) DECT handset, the acknowledgement is received after the user presses the **accept** or **del** button on the handset. See Figure 33: Acknowledge sequences for Normal and Urgent messages using DECT handsets on page 105.

- SET/RESET

An alarm can also be generated, based on a set command. This command must always be followed by a reset from the same input module, after the alarm condition is no longer active. Figure 31: SET/RESET Alarm Structure on page 104 illustrates the SET/REST alarm structure.

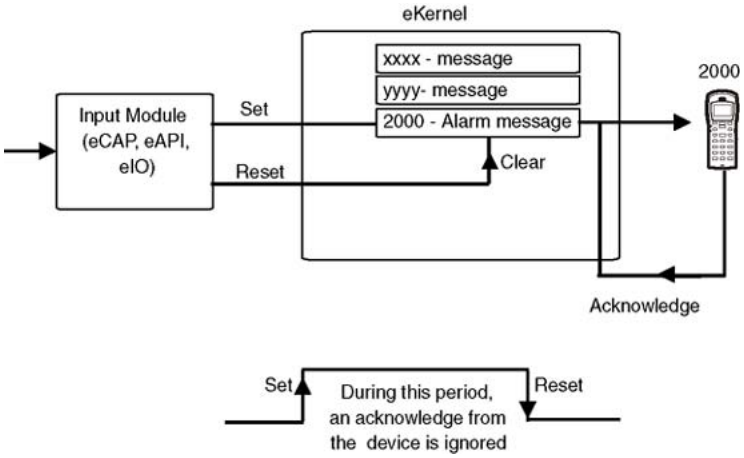


Figure 31: SET/RESET Alarm Structure

The input modules eCAP, eAPI, and eIO can generate a set/reset command. (eIO set/reset is explained in more detail later on in this document.) An acknowledgment from a device does not clear the alarm condition on that device in the database. Therefore, even if the call on the device is answered, the alarm is not reset. As long as the eKERNEL does not receive a reset from the Input Module, the alarm is repeated on the device with a time interval that you must have specified in the eCONFIG.

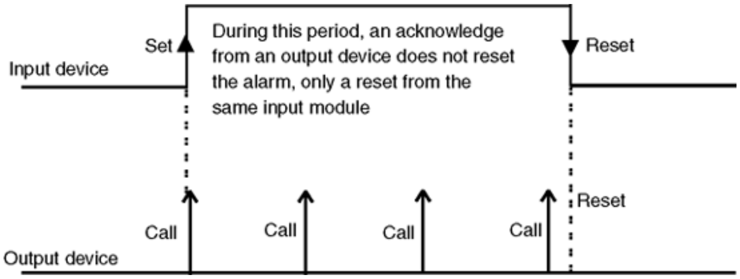

Input device
Set
During this period, an acknowledge
from an output device does not reset
the alarm, only a reset from the
same input module
Reset
Reset
Call
Call
Call
Call
Output device

Figure 32: Alarm processing

The way an alarm is processed in an LRMS (E2) DECT Handset depends on the Acknowledge/ Negative Acknowledge (ACK/NAK) structure, as shown in Figure 32: Alarm processing on page 104.

- ACK/NAK

  A message can be sent to an LRMS (E2) DECT handset as a Normal message, or as an Urgent message. After a message is sent as a Normal message, the DMC sends an Acknowledge at the moment that the message arrives at the handset. No manual confirmation is required. If the message was sent as a sent message (reset after sent) the alarm call is cleared on this Acknowledge. If a message is sent as an Urgent message, the alarm call is cleared after the second Acknowledge arrives. After the user presses the Delete or OK key on the handset, the message call is acknowledged.

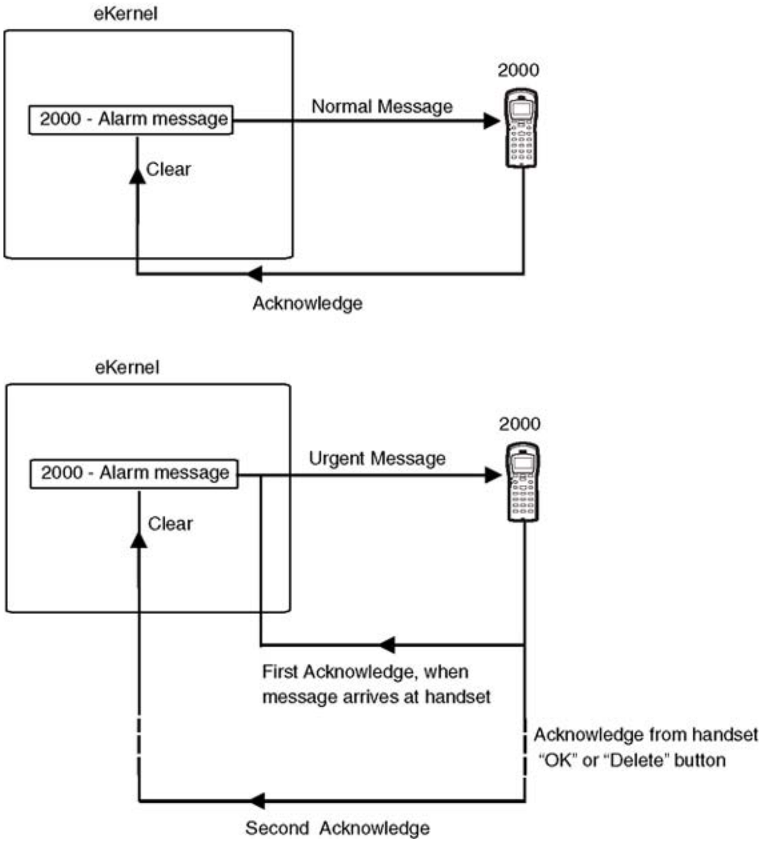


Figure 33: Acknowledge sequences for Normal and Urgent messages using DECT handsets

For alarm handling, bear in mind the following when setting up the system:

- An alarm is set in a data table in the eKERNEL.
- Although the alarm is set in a table in the eKERNEL, the alarm is always set on a Device.
- Because an alarm is set on a device, the alarm can only be reset on a device.

- Resetting an alarm can be done from:
    - The device on which the alarm is set. Alarm is reset after the call is Acknowledged (LRMS [E2] messaging)
    - The Input Module from which the alarm was set (eCAP, eAPI or eIO).
    - An Incoming Confirmation call from eDMSAPI.
- You can use the I/O to set an alarm using a push button. This is issued after the button is pushed, and is handled as a SENT alarm. The alarm cannot be reset by a push button.
- The SENT, SET, and RESET commands:
    - SENT. An incoming alarm that uses the specification SENT (Remove after SENT) is sent to the device, and withdrawn after an Acknowledge from the handset. If the device answers the call (Acknowledge), the alarm is reset.
    - SET. This command sets an alarm that is only reset after a Reset is sent from the same Input Module to the same Group/Alarm Id. In the case of a V.24 input module that sends a message string, the same message string must appear in the reset command.
    - RESET. This command can reset an alarm that was earlier set using a SET command. For the command to be successful, the alarm input must be exactly the same as that set by the SET command, with exactly the same message. In the eAPI Module, the Alarm ID, and the Group must be the same, but the message can be different. Note that in the eAPI all outstanding alarms are reset, after receiving a reset command.
- If an alarm is set, and you have set an overflow to an Alternative device, the overflow is only activated after the device gives a NAK at each retry and the retry counter is expired.

  If you send a normal message to a DECT extension that is within reach of the radio signals and is switched on, the overflow never takes place because DECT Messenger receives an ACK. Only if the handset is switched off, or not in reach of radio signals, does the DMC generate a NAK; then the message goes to the Alternative device after the specified number of retries.

  If you send an urgent message to a DECT extension, and the user of the DECT extension does not press **OK** or **Delete** on the handset, the DMC sends a NAK after 30 seconds ringing time. The message goes to the Alternative device after the specified number of retries.
- If an alarm is set, and an overflow occurs to an alternative device, the alarm can only be reset, with an alarm input from the same Input Module with the same Alarm Identifier, however, with the properties: *RESET after *SENT.
- After you receive an alarm through eAPI, the options shown in Table 10: Options for alarm handling on page 107 apply to alarm handling:

Table 10: Options for alarm handling

Field: set or reset	Field: Remove after	DECT Messenger action
*set	*sent	Alarm processed as sent alarm.
*set	*reset	Alarm set and waits for a reset.
*set	*calc	System sets the alarm. The system searches in the eKERNEL_ALARM table for a Remove_after SENT for that Input Module with the same Alarm Description. If the system cannot find this, it searches for a Remove_after Reset with the same alarm description. If the system cannot find this, it searches for the alarm description *Other in for the same Input Module.
*reset	*sent	Resets all alarms from this input program.
*reset	*reset	Invalid input.
*reset	*calc	Invalid input.

eLOCATION

You can use eLOCATION to determine the approximate location of a SIP DECT handset in a SIP DECT environment after the handset sends a message to a predefined special number. eLOCATION is specifically used to support emergency situations. The location information provided relates to the Radio Cell from which the call originated. The precision of the location is related to the area covered by the Radio Cell. The smaller the area, the greater the precision of the handset location.

eLOCATION has the following characteristics:

- requires the eDMSAPI module

  All SIP DECT extensions that should be able to generate a location alarm must be correctly set in the DMSAPI module. For User 2 User messages, ensure that all user 2 users have been configured.

- requires a predefined extension number

  Predefined special numbers must be set in the eDMSAPI module with the type *LA. The Called device can be for example 911 or 112.

- location of the handset is only retrieved after a short message is sent to the predefined extension number. In all other cases, no location information is retrieved.
- requires an IP connection to a DAP Controller (DCC) in the SIP DECT environment
- location detection only works on SIP DECT extensions

eLOCATION can support configurations with more than 255 radios. If more than 255 radios are used, the first 255 radios use a 2-byte definition from 00 to FF. The remaining radios use a 3-byte definition, for example 100, 101, 102, and so on.

Important:

IMPORTANT

eLOCATION can handle location registration for one DECT cluster only. eLOCATION works with SIP DECT only.

How it works

A handset sends a short message to the predefined extension number. This extension number must have the property Location Alarm in DECT Messenger. Based on this property, DECT Messenger activates location retrieval for the handset. This means that DECT Messenger sets up a connection to a DAP Controller through IP, and asks for the location of the calling line ID (CLI) in the call. This CLI is the extension number of the DECT handset making the call. The DAP Controller responds by sending the RPN (Radio Part Number) to DECT Messenger. This RPN number is not meaningful location information. There is a conversion table (eLOCATION_RPN) that translates the RPN to meaningful location information. This location information can be used in the message that is sent.

The message can be sent to any output device. The relation between the generated message and the destination group is defined in the table: eLOCATION_INBOUND_RESULT. In this table, the relation is established between the Calling Line ID, the Called Line ID and the Group to which the message is sent. The message (string) is also defined in this table.

The message can contain variables that are filled in by DECT Messenger before it is sent. You can use this feature of DECT Messenger to generate a message similar to the following message.

```
SOS at location [Location] at [Location time] on [Location date] from [Calling
number] to [Called number]
```

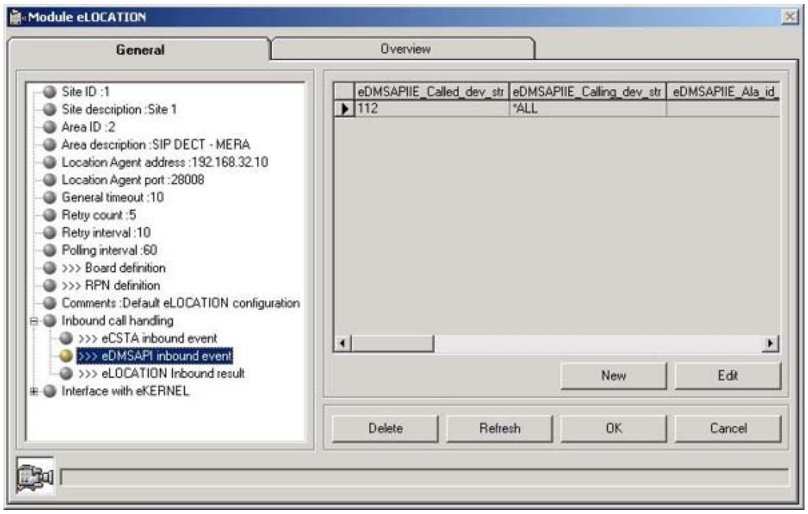
Where:

- [Location] = the contents of the eLOCRPN_Message_str field in the table eLOCATION_RPN
- [Location time] = current time
- [Location date] = current date.
- [Calling number] = calling number.
- [Called number] = called number

The destination group, the message, and the Alarm ID are used to dispatch the message to the appropriate destination(s).

eLOCATION Module in eCONFIG

The eLOCATION module is configured through eCONFIG.



- Site ID :1
- Site description :Site 1
- Area ID :2
- Area description :SIP DECT - MERA
- Location Agent address :192.168.32.10
- Location Agent port :28008
- General timeout :10
- Retry count :5
- Retry interval :10
- Polling interval :60
- >>> Board definition
- >>> RPN definition
- Comments :Default eLOCATION configuration
- Inbound call handling
  - >>> eCSTA inbound event
  - >>> eDMSAPI inbound event
  - >>> eLOCATION Inbound result
- Interface with eKERNEL

eDMSAPIIE_Called_dev_str	eDMSAPIIE_Calling_dev_str	eDMSAPIIE_Ala_id
112	*ALL	

Figure 34: eLOCATION module

A number of parameters, for example Site, Area, and so on, are the same for all modules and therefore, are not explained here. However, the following parameters are new in the eLOCATION module and require some explanation:

- **Location Agent Address**

  This is the IP address of the DAP Controller (DCC) to which the IP connection is made.

- **Location Agent Port**

  This is the port number on the DAP Controller (DCC) to which the IP connection is made. The port number must be 28008 for a SIP DECT system.

- **General Timeout**

  Protocol guarding. Always is 10 seconds.

- **Retry Count**

  Retry counter for retrieving information from the DAP Controller. Default = 5.

- **Retry Interval**

  Retry Interval time between retries. Default = 10 seconds.

- **Polling Interval**

  Polling interval is the interval time between poling message to the DCC to check if the connection is still alive. Default = 60 seconds.

- **>>>Board Definition**

  Refers to the table: eLOCATION_BOARD. This table defines the relation between the DAP Controller and the predefined extension number. Each DECT extension is subscribed at one DAP Controller only.

  Note:
  DCC board numbers ranges from 01 to 32.

- **>>>RPN Definition**

  Refers to the table: eLOCATION_RPN. This table defines the relation between the RPN number and a meaningful message. This message must contain the location information.

- **Inbound Call Handling >>> eDMSAPI inbound event**

  Refers to the table: eDMSAPI_Inbound_Event. This table defines the relation between the Calling Line ID, the Called Line ID and the Alarm Identifier. The Alarm Identifier determines how the Alarm is processed.

- **Inbound Call Handling >>> eLOCATION inbound result**

  Refers to the table: eLOCATION_ INBOUND_RESULT. This table defines the relation between the Calling Line ID, the Called Line ID and the Group (destination) to which the alarm/message must be sent.

Connecting National Instruments modules

General

The Digital Input, Digital Output, and Analogue Input options are achieved using FieldPoint modules of National Instruments. Figure 35: Rail with National Instruments FieldPoint IO Modules on page 111 shows the National Instruments IO modules on a rail.

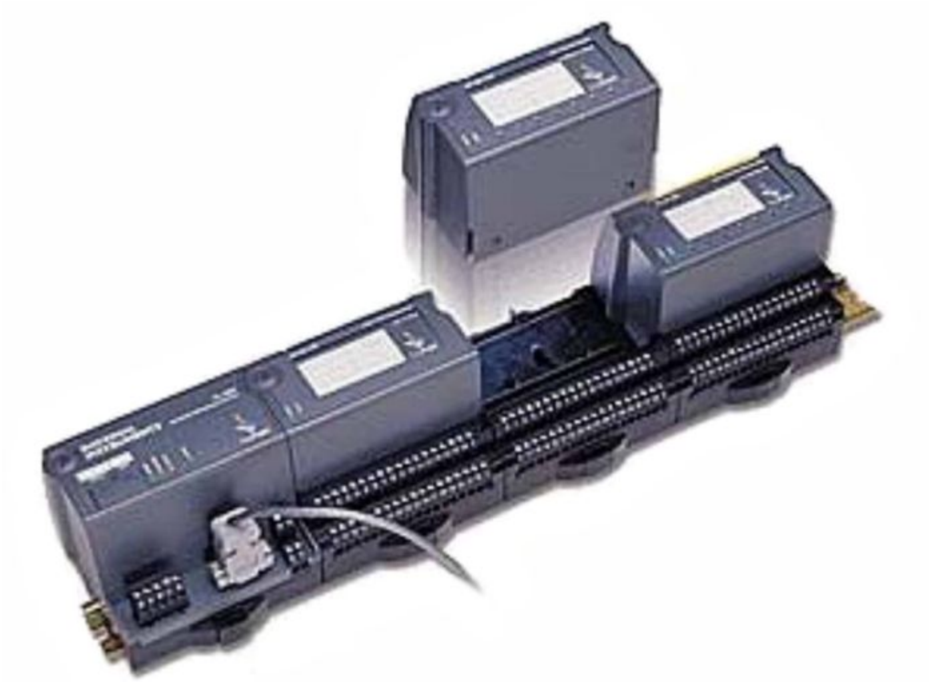


Figure 35: Rail with National Instruments FieldPoint IO Modules

The various types of IO modules that are supported for DECT Messenger can be classified as control modules or I/O Modules. Table 11: Overview of supported control modules on page 111 and Table 12: Overview of supported IO modules on page 112 give an overview of these modules.

Table 11: Overview of supported control modules

Module Type	Description	Additional info
FP-1000	Control Module with V.24 interface to DECT Messenger	This module is as interface module between the I/O modules and DECT Messenger. The FP-1000 can control up to 9 I/O modules directly. Up to 24 FP-1001 modules can be connected through RS485 bus to expand the system with extra I/O modules.
FP-1001	Expansion Control Module	Must be connected to the RS485 interface on the FP-1000. One FP-1001 can control up to 9 I/O modules. The maximum number of FP-1001 modules one RS485 bus is 24.
PS-2	Power Supply	24 Volts DC.
Din rail	Mounting rail	The modules must be mounted on this rail.

Table 12: Overview of supported IO modules

Module Type	Description	Additional info
AI-100	Analogue input Module	8 Analogue inputs, each can be set to one of the following ranges: 30V, 15V, 5V, 1V, 0-30V, 0-15V, 0-5V, 0-1V, 20mA, 0-20mA, 4-20mA.
DI-300	Digital Input	8 discrete input channels. These inputs are sinking inputs for 24VDC.
DI-301	Digital Input	16 discrete input channels. These inputs are sinking inputs for 24VDC.
DI-330	Digital Input	8 discrete input channels. Universal inputs work with any voltage from 5V TTL up to 250VDC/VAC. Compatible with sourcing, sinking, or power sensing applications.
DO-400	Digital output	8 discrete output channels. Max. 2A for each output, max 8A for each module. Maximum voltage 30VDC.
DO-401	Digital output	16 discrete output channels. Max. 2A for each output, max 8A for each module. Maximum voltage 30VDC.
For each I/O module, one Terminal Base is required - TB-1		

Figure 36: National Instruments rail connected to DECT Messenger on page 112 shows how one rail with National Instruments I/O modules is connected to DECT Messenger. On this rail there can be various types of I/O Modules. The maximum number of modules for each rail is eight. The modules shown in Figure 36: National Instruments rail connected to DECT Messenger on page 112 are examples only.

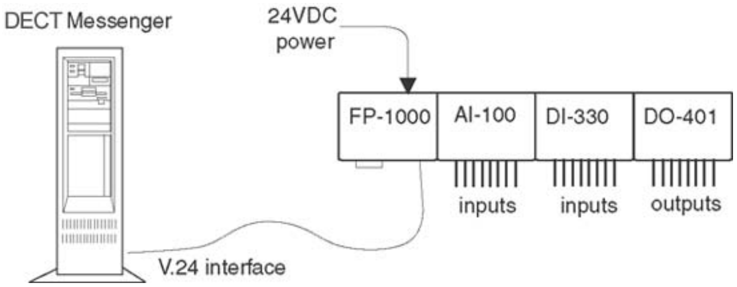


Figure 36: National Instruments rail connected to DECT Messenger

Note:

The maximum number of contacts for each eIO Module in DECT Messenger is 128.

Figure 37: National Instruments Modules connected to DECT Messenger on page 113 shows a configuration of three rails with National Instruments modules connected to a DECT Messenger. The three rails with modules are connected together through the RS-485 bus.

Note:

A multi rail configuration is not part of the standard product, and is only available on a Project basis.

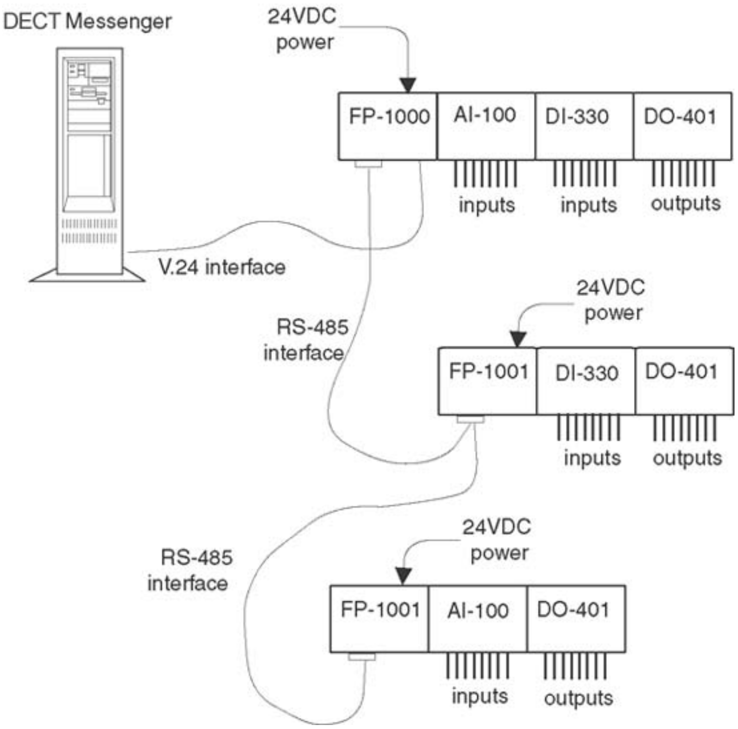


Figure 37: National Instruments Modules connected to DECT Messenger

Note:

The connection between the DECT Messenger computer and the first rail is achieved using V.24. Therefore, the maximum cable length is determined by the V.24 characteristics and the cable type.

If you have more than one rail (only available on Project basis), the connection between the rails (and therefore the connection between the FP-1000 and FP-1001 modules) is achieved using an RS-485 connection. This is a four wire bus connection that allows a maximum distance of approximately 1000 metres.

Instead of using an FP-1000 module as Controlling Module on a rail, the FP-1601 module can be used. The FP-1601 module has an Ethernet interface to DECT Messenger instead of the V.24 interface. However, this module is not supported in the standard DECT Messenger product.

Hardware Installation

Hardware installation is described in the documentation from National Instruments.

Software Installation

Note:

Due to subsequent software releases, the contents of this section can differ slightly from your actual product.

The software for the I/O modules is based on the industry standard OLE for Process Control (OPC) Server software. After you install the software for the National Instruments modules according to the installation procedure in *Avaya DECT Messenger Installation and Commissioning, NN43120-301*, this OPC software is installed. The FieldPoint software is also installed, including FieldPoint Explorer. You must set up the National Instruments module configuration using FieldPoint Explorer, before you can use the National Instruments module in the DECT Messenger software.

The software for the National Instruments modules consist of three main parts.

- The eIO module that is part of the DECT Messenger software.
- The FieldPoint Explorer software for setting up the configuration of the FieldPoint modules.
- OPC (Object Linking and Embedding for Process Control) Server.

Figure 38: Software Parts for the I/O modules on page 114 shows how these modules are related.

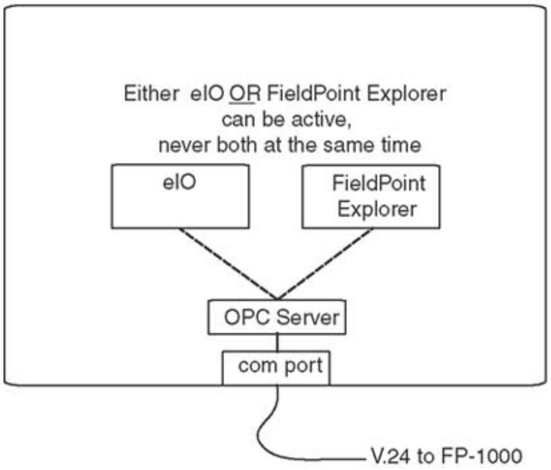


Figure 38: Software Parts for the I/O modules

The OPC Server software can be controlled by ONE application only. Therefore, you can have either the eIO Module active OR the FieldPoint Explorer.

Note:

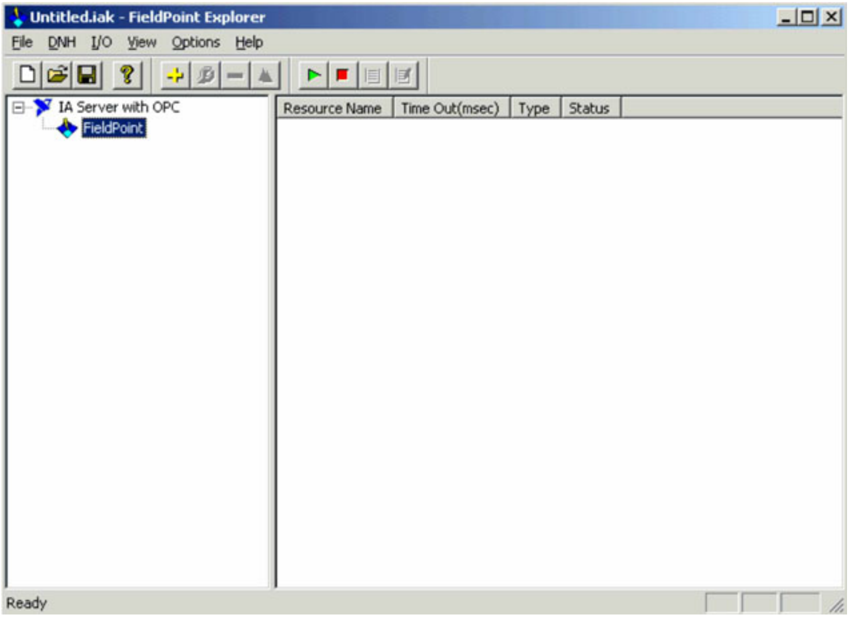
Do not forget to close down the FieldPoint Explorer before you start the eIO module. Conversely, do not forget to close down the eIO Module before starting up the FieldPoint Explorer.

Using the National Instruments FieldPoint Explorer software on page 115 describes the steps needed to use the FieldPoint Explorer software:

Using the National Instruments FieldPoint Explorer software

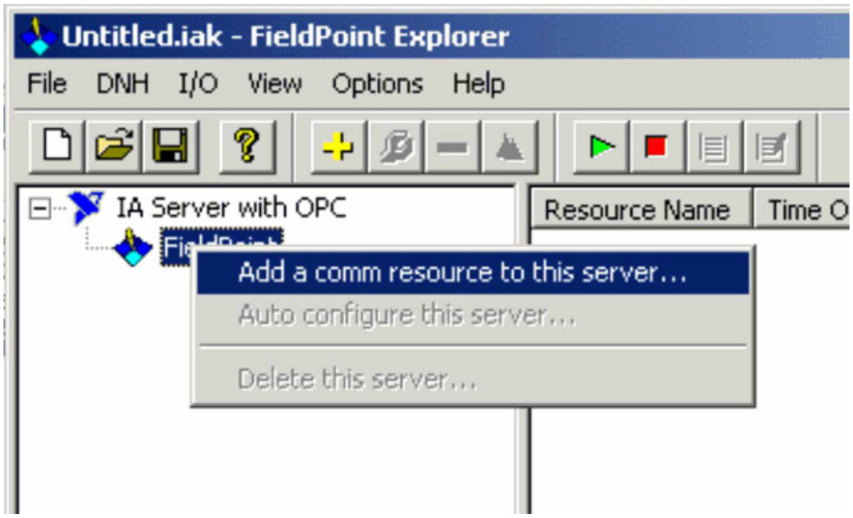
1. Ensure that the National Instruments FieldPoint Explorer software is installed correctly.
    - Ensure that you have installed the National Instruments FieldPoint Explorer software as described in the installation procedure on the CD.
    - Verify that the National Instruments FP-1000 is connected to a free COM port on your DECT Messenger PC.
    - Ensure that the eIO Module is not running.
    - Open the FieldPoint Explorer window.
2. Open the FieldPoint Explorer.

    Click **Start** on the Windows task bar, and choose **Programs > National Instruments FieldPoint 2.0 > FieldPoint Explorer**.

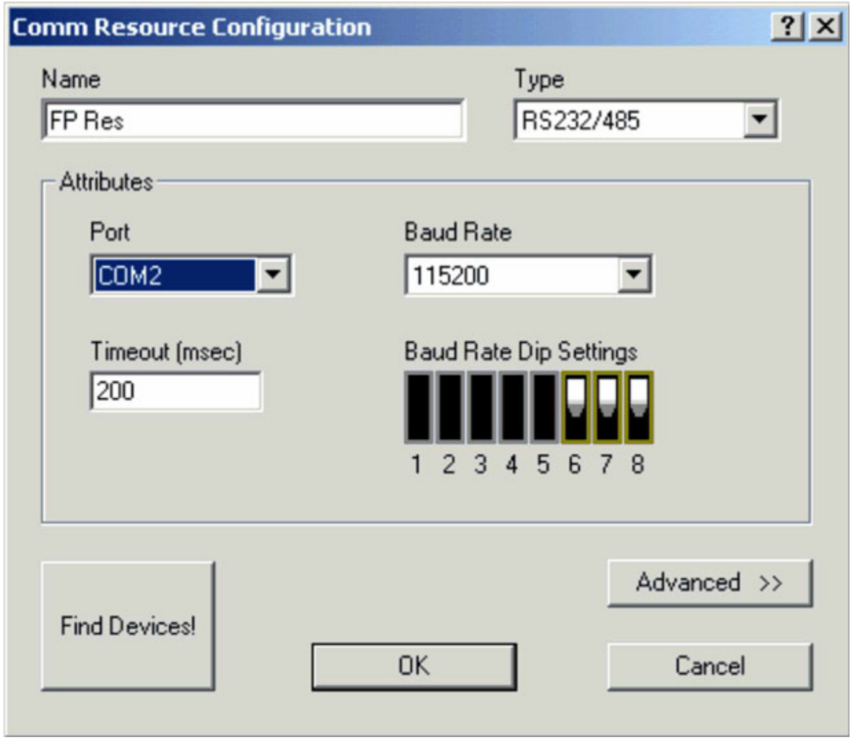


3. Add a comm resource.

    Right-click **FieldPoint** to open the following menu:


Untitled.iak - FieldPoint Explorer
File DNH I/O View Options Help
IA Server with OPC
FieldPoint
Resource Name
Time O
Add a comm resource to this server...
Auto configure this server...
Delete this server...

In this menu select **Add a comm resource to this server....** The following window opens:



Name: FP Res

Type: RS232/485

Port: COM2

Baud Rate: 115200

Timeout (msec): 200

4. Configure the comm resource

   In the Comm Resources Configuration window, set the following:

   - Name

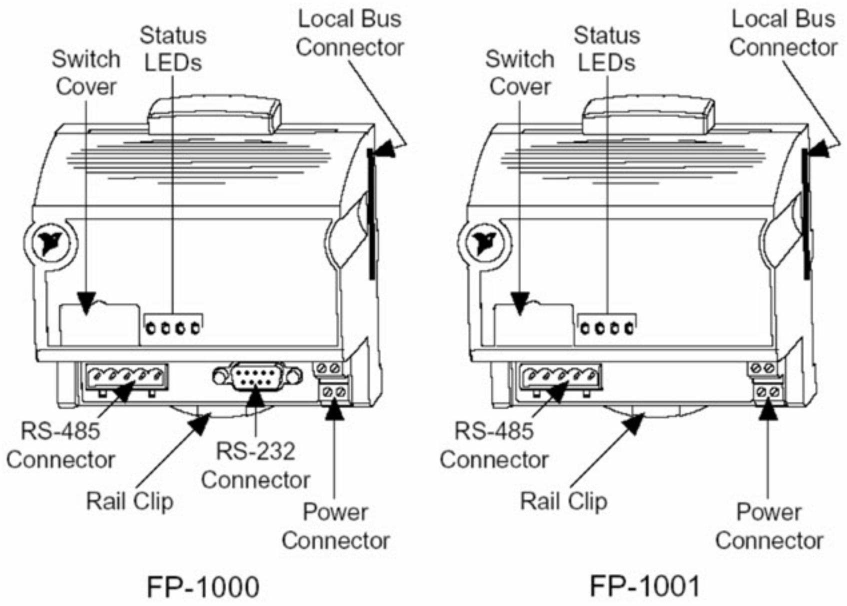
   Accept the default name (FP Res).

   - Port

This is the COM port on your computer to which you have connected your V.24 interface from the FieldPoint FP-1000 module.

- Baud Rate

Communication speed over the V.24 line. Default this is 115200 b/s. The DIP switch settings associated with the speed are displayed. Ensure that the DIP switches for the Baud rate on the FP-1000 module are in the same position as displayed in your screen. The DIP switches on the FP-1000 module are under a small cover on the top of the FP-1000 module.



- Time-out (msec.)

Time out counter on the V.24 communication. Accept the default (200 msec).

Note:

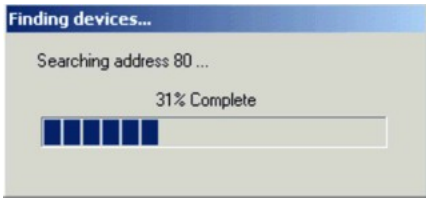
Do not close this window yet; proceed to the next step.

5. Search for connected modules

- Click **Find Devices**

This scans the FieldPoint Module address through the V.24 interface, and automatically detects that modules are connected. Click this button if you are sure that all the other settings in this window are correct.

The following window is displayed.



Finding devices...

Searching address 80 ...

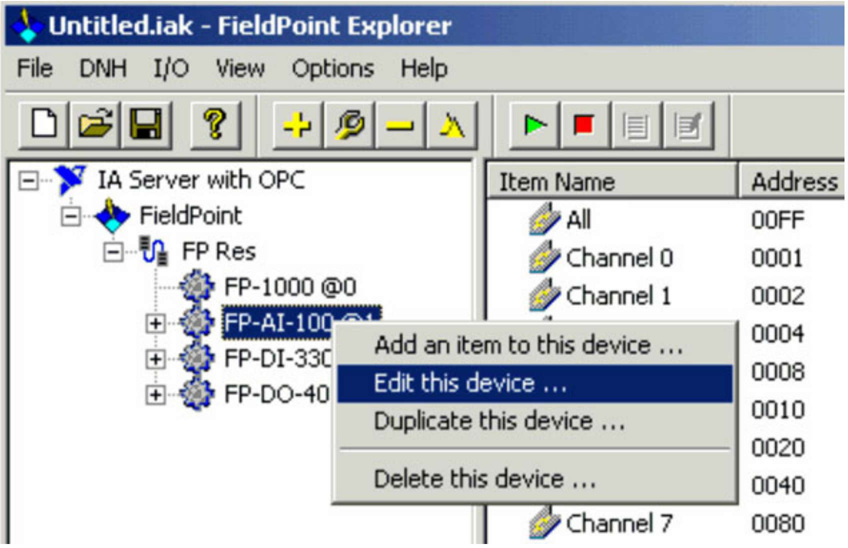
31% Complete

6. Expand the communication name.

   After all the devices are detected, they are displayed in the left pane. If not, click the **+** sign in front of the communication name (FP Res by default).

7. Right-click the device you wish to edit.

   - Right-click a device.
   - In the pop-up menu, select **Edit this Device...**



8. Set channel configuration values.

   Click **Configure channels.**

   In the Channel configuration window that is displayed, enable the lines that you use, and select the correct settings (this depends on what you have connected to the channels).

   Click **Apply**, and then **OK**.

9. Edit the remaining devices.

   - Click **OK** to close the Device configuration window.
   - Repeat steps 7 and 8 for each device.

10. Start Monitoring channels.

    Your devices are now set up. If you right-click an individual channel, and select **Edit this item...** from the pop-up menu, information about the channel is displayed, including channel connections.

    Now you can start monitoring the channels. Click the **Start Monitoring** menu from the menu **I/O** or click the associated button in the tool bar. Now line monitoring is started. If you select a device in the left pane, the channel status is displayed in the right pane. If the input on that device module changes, the display is updated to show the changed channel status.

11. Close the FieldPoint Explorer.

    If you do not close FieldPoint Explorer, the eIO Module does not receive information from the FieldPoint modules.

    Note:
    Setting up the eIO Modules is described in Module-eIO.

Understanding Security features

Session Guarding

Session Guarding is applicable for the input programs eAPI and eCAP. Session Guarding checks to see if there is input on a regular basis. This assumes that the equipment that is connected to the V.24 interface or eAPI interface sends character strings at regular intervals. If these strings stop arriving, the eGuarding module times out and generates an alarm.

In the eGuarding configuration, you must specify the following items:

- The input program you expect input from at regular intervals
- The time of day you expect input
- The days in the week you expect input
- The Alarm Group and Alarm Description the alarm must be sent with (if there is a time out)
- The Expected time interval between inputs
- The Message to be sent in case of an alarm

Watchdog

General

The Watchdog guards the eKERNEL activity. Watchdog is a card that is installed in the PC as an internal device. For DECT Messenger the Internal Serial PC Watchdog from Berkshire Products is supported. Figure 39: Berkshire Product Inc. Internal serial PC Watchdog on page 120 shows this card.

Figure 39: Berkshire Product Inc. Internal serial PC Watchdog

The Watchdog card is designed to monitor PCs used in critical applications such as: File Servers, Voice Mail Systems, Internet Service Provider (ISP) systems, industrial applications, and so on. The purpose of the Watchdog card is to ensure the PC is always available; especially for systems that are not continuously monitored. After power is applied to the Watchdog, or after a reset of the PC, the Watchdog waits 2.5 minutes (shorter times allowed in Command Mode) before arming itself. This allows the PC to complete its reset and initialization sequence.

The standard Watchdog package contains the following items:

- The Berkshire Watchdog manual on diskette as a PDF file
- The Watchdog timer on a standard PC I/O bracket
- A disk drive Y style power cable to power the board
- A DB-9 to DB-9 serial cable
- A 3.5 program diskette
- A reset cable

The Watchdog card is an internal PC card but without an ISA or PCI connector. The unit consists of a bracket with a small card that receives power from the PC by means of a Power Cable with standard Disk Drive Power connector. All the signal connections are made externally. Figure 40: Configuration of the Watchdog card on page 121 shows how the Watchdog is used in DECT Messenger.

There is a mini jack connector available at the bracket of the Watchdog card, which provides two relay contacts. However, these are not used in the DECT Messenger configuration. The contacts can only be activated after an application sends the correct commands to the card using V.24 (RS232). DECT Messenger cannot send such commands to the Watchdog.

The Watchdog resets the PC if the eKERNEL is not running.

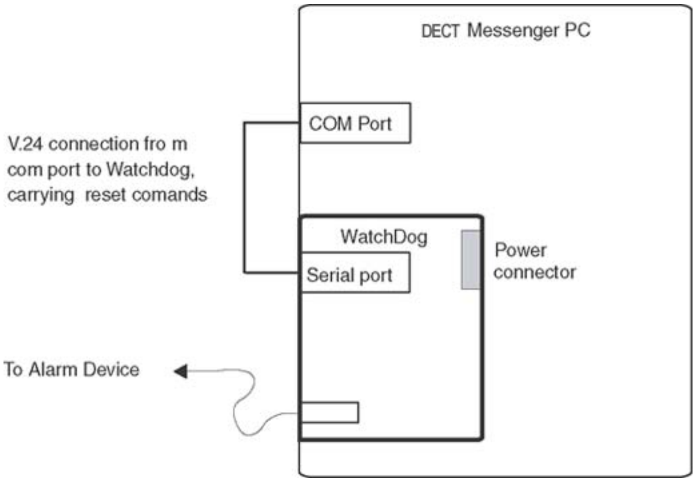


Figure 40: Configuration of the Watchdog card

Note:

To use the reset and automatic startup, ensure that the Reset button signals the PC to restart, instead of signalling Windows to restart. If the reset button signals for Windows to restart, and Task Manager is running, Task Manager blocks the restart command.

Watchdog Installation

The following procedure describes how to install the Watchdog.

Installing and connecting the Watchdog

1. Set DIP switches.

   To enable command mode and set the timer (in this example, to 30 seconds), make the following DIP switch settings on the Watchdog card:

SW1	SW2	SW3	SW4	SW5	SW6	SW7	SW8
OFF	ON	OFF	OFF	OFF	OFF	ON	OFF

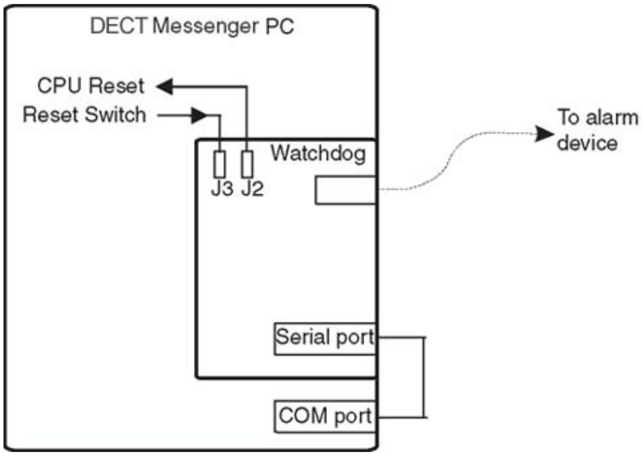
   Note:

   The switches are only read at power up, and after each time that the timer expires. A switch that is DOWN is OFF, and a switch that is UP is ON. For more information about these switch settings, see the Watchdog User's Manual that comes with the card.

2. Change the PC reset cable connection.

   - Disconnect the PC reset cable from the motherboard.
   - Plug the cable onto the J3 header in the upper left corner of the Watchdog.

   The PC Reset connections are as follows:



3. Attach the reset cable.

   Plug the supplied reset cable onto J2 on the Watchdog board, and plug the other end onto the original reset header on the motherboard.

4. Install the Watchdog.

   Install the Watchdog in a free slot/bracket position.

5. Connect the power.

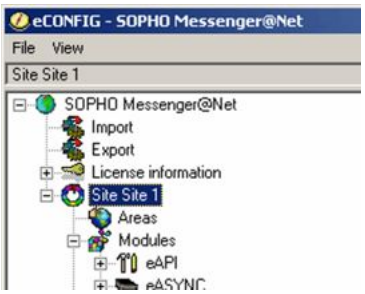
   Connect the power cable to the Watchdog card.

6. Connect the serial cable.

   - Connect the DB-9S end of the serial cable to a free COM port on the PC.
   - Connect the other end of the cable (DB-9P) to the Serial Input port on the Watchdog.

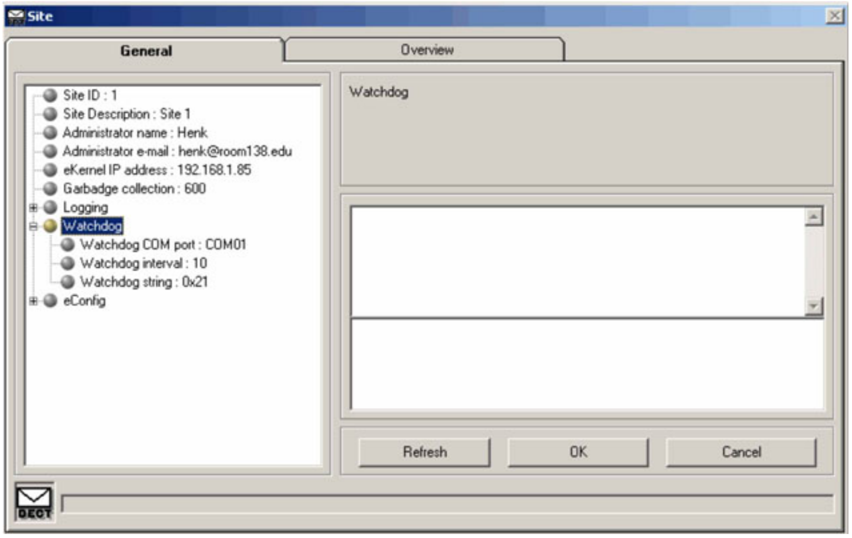
7. Open the Site configuration window.

   Start the PC, and start the eCONFIG. In eCONFIG double-click the Site menu:



8. Configure the Watchdog

   - Select the time period
   - Select the COM port



- Site ID : 1
- Site Description : Site 1
- Administrator name : Henk
- Administrator e-mail : henk@room138.edu
- eKernel IP address : 192.168.1.85
- Garbadge collection : 600
- Logging
- Watchdog
  - Watchdog COM port : COM01
  - Watchdog interval : 10
  - Watchdog string : 0x21
- eConfig

Note:

If you followed the instructions in Step 1 of this procedure, you set the Watchdog timer to 30 seconds. Therefore, you must fill in a time period that is significantly lower than this value, for example, 8 seconds.

Note:

After selecting the COM port, keep in mind that other Modules use COM ports as well, such as eCAP, eESPA, eIO.

9. Verify correct operation.

   To test the operation of the Watchdog, set the time in the eKERNEL_SITE table to a higher value (for example, 40 seconds). As a result, the signal does not arrive within 30 seconds, the Watchdog timer expires, and the alarm relay contacts are closed. After you finish testing, remember to set the time value in the eKERNEL_SITE table back to its original value (for example, 10 seconds).

   See the following section, Watchdog settings and indicators on page 123, for additional information about the Watchdog card.

Watchdog settings and indicators

- LEDs

Table 13: Top LED Indications

Top LED Indication	Meaning
Flashing at 1 second ON - 1 second OFF	This condition appears at power up of the PC for 2,5 minutes, to let the PC power up.

Top LED Indication	Meaning
Flashing at 350 msec. rate	Watchdog operational. No alarm condition.
Flashing rapidly at 100msec.	3 seconds before timer expires, and no reset received yet.

Table 14: Bottom LED Indications.

Bottom LED Indication	Meaning
Steady on.	Alarm condition. The timer in the Watchdog is expired, and the alarm contact is activated.
Flashing at 1 second rate, each flash 100 msec.	Input signal detected.

- Switches

  The function of the DIP switches on the card are described in the Watchdog User's Manual. However, for the DECT Messenger application, use the switch settings are defined in Installing and connecting the Watchdog on page 121. If you want to use another delay time, change the delay time using switches 6,7, and 8. See Table 15: Switches 6 to 8. on page 124 for the settings.

  Note:
  Also adapt the eKERNEL_SITE table in DECT Messenger.

  Table 15: Switches 6 to 8.

Switches 6-8	Delay Time
OFF-OFF-OFF	5 Seconds
OFF-OFF- ON	10 Seconds
OFF- ON-OFF	30 Seconds
OFF- ON- ON	1 Minute
ON-OFF-OFF	10 Minutes
ON-OFF- ON	30 Minutes
ON- ON-OFF	1 Hour
ON- ON- ON	2 Hour

- COM Port Settings

  The Watchdog requires that the COM port on the PC be set to 1200 Baud, 8 Data Bits, No Parity Bit, and 2 Stop Bits. The requirement for 2 stop bits is important because the processor uses the idle time between characters to process input data, and take care of other processing tasks.

Note:

These settings are fixed in DECT Messenger.

Automatic Watchdog Startup

The Watchdog is connected to the reset button of the PC. Watchdog automatically restarts the PC if Watchdog detects that the software is no longer running.

Note:

Automatic startup with automatic logon is only possible in Windows 2000 professional in a Work Group environment. If you must log on to a Windows 2000 domain, you must always log on manually.

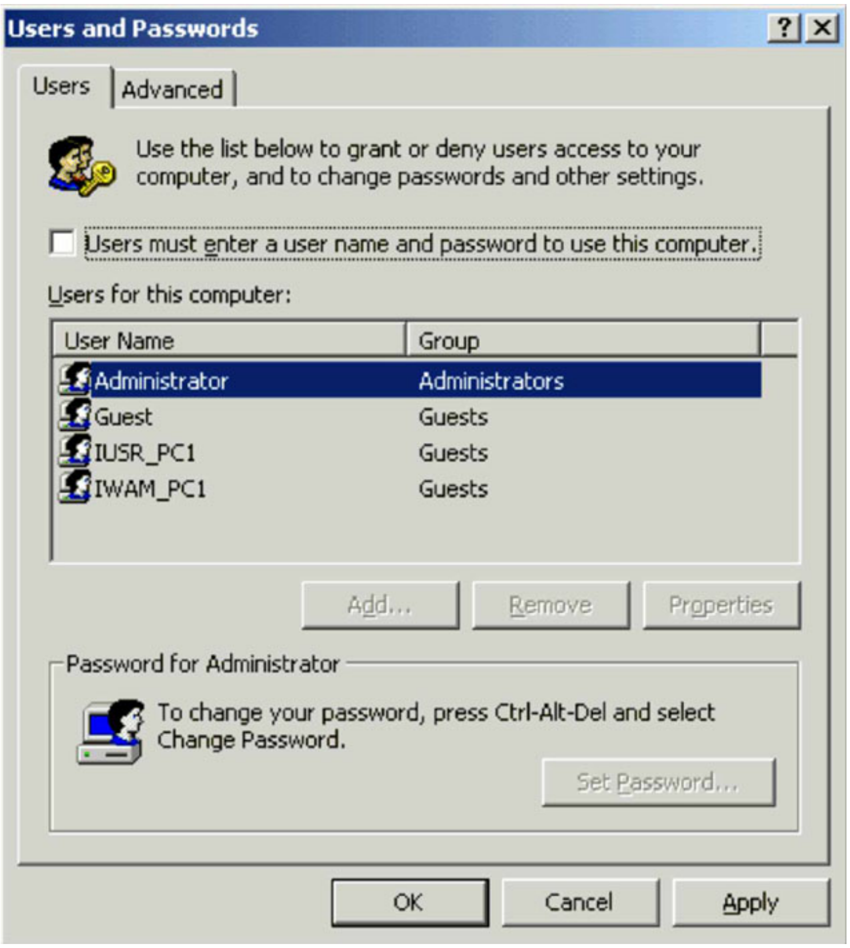
Automatic startup with login in Windows 2000 Professional

1. Open the Users and Passwords window.

   Click **Start** on the Windows task bar, and choose **Settings > Control Panel > Users and Passwords**.

2. Disable login.

   - Clear the check box **Users must enter a user name and password to use this computer** as shown in the illustration.
   - Click **Apply**, and, and then **OK**.



Use the list below to grant or deny users access to your computer, and to change passwords and other settings.

□ Users must enter a user name and password to use this computer.

Users for this computer:

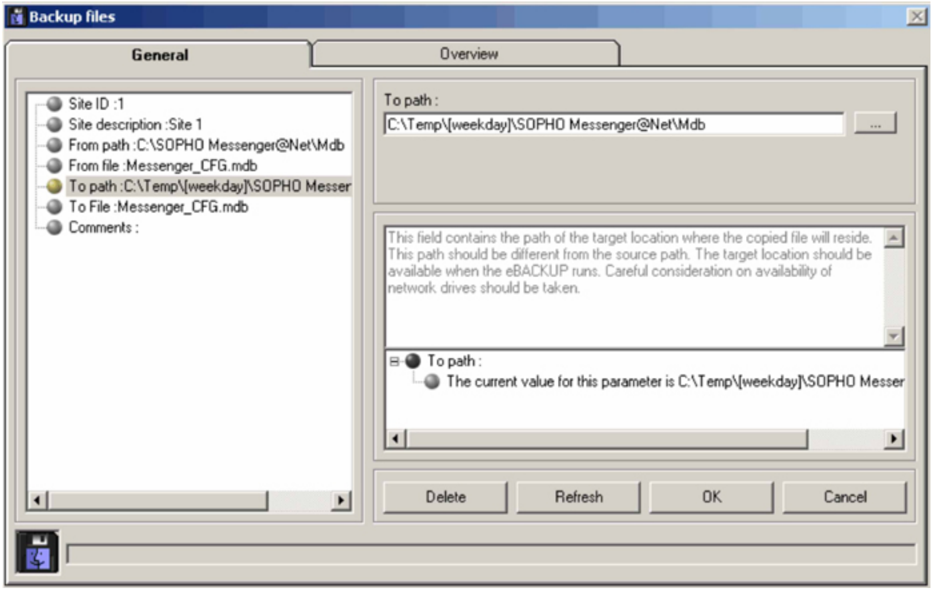
User Name	Group
Administrator	Administrators
Guest	Guests
IUSR_PC1	Guests
IWAM_PC1	Guests

Password for Administrator

To change your password, press Ctrl-Alt-Del and select Change Password.

Using eBackup

The eBACKUP module provides a means to back up files. Use the eBACKUP configuration to specify which files must be backed up, and in what directory to store the copies.



Site ID :1
Site description :Site 1
From path :C:\SOPHO Messenger@Net\Mdb
From file :Messenger_CFG.mdb
To path :C:\Temp\[weekday]\SOPHO Messer
To File :Messenger_CFG.mdb
Comments :

To path :
C:\Temp\[weekday]\SOPHO Messenger@Net\Mdb

This field contains the path of the target location where the copied file will reside. This path should be different from the source path. The target location should be available when the eBACKUP runs. Careful consideration on availability of network drives should be taken.

To path :
The current value for this parameter is C:\Temp\[weekday]\SOPHO Messer

Figure 41: The Backup window

In the Path settings, you can specify fields that are filled in by the system:

[weekday] 1 ... 7, where 1=monday up to 7=sunday

[timestamp] for example, 20030930124506

[weekdayname] Monday ... Friday

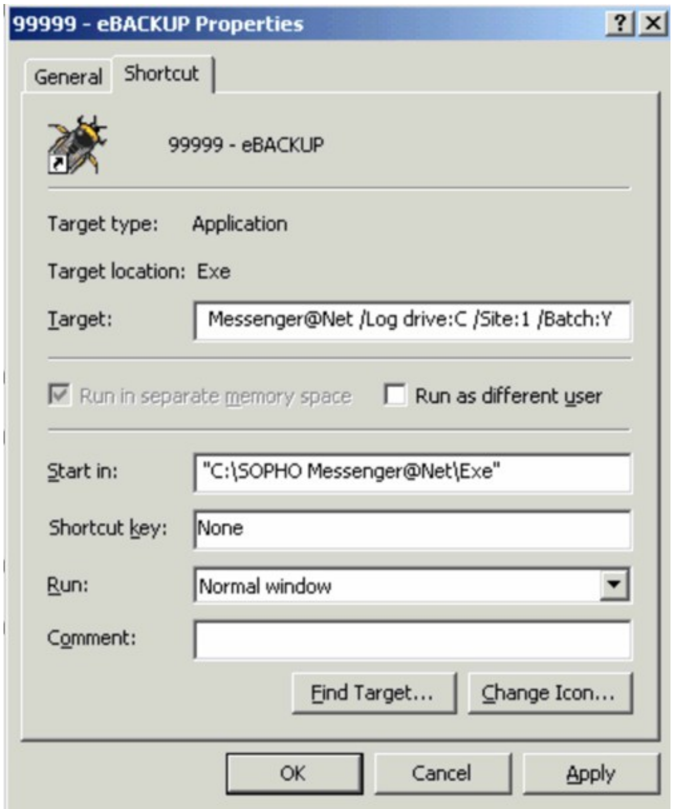
The eBACKUP Module is NOT a scheduler. There are two ways to generate a BACKUP using eBACKUP:

- Manually

  After you double-click the **eBACKUP** program shortcut, the program does one of the following:

  - Creates a backup without manual intervention
  - Opens a window in which you can select the site that you want to back up.

  Which of these two things the software does depends on the specifications in the target field in the shortcut. See Figure 42: Shortcut definition to eBACKUP on page 128. If there is specified Batch:N, eBACKUP opens the Site selection window. If there is specified Batch:Y, eBACKUP generates a backup immediately.



99999 - eBACKUP Properties

99999 - eBACKUP

Target type: Application

Target location: Exe

Target: Messenger@Net /Log drive:C /Site:1 /Batch:Y

☑ Run in separate memory space ☐ Run as different user

Start in: "C:\SOPHO Messenger@Net\Exe"

Shortcut key: None

Run: Normal window

Comment:

Figure 42: Shortcut definition to eBACKUP

> **Note:**
> Figure 42: Shortcut definition to eBACKUP on page 128 shows only a part of the line. The whole line in the Target field of the shortcut is:

```
C:\SOPHO Messenger@net\Exe\eBACKUP.exe / Path:C:\SOPHO
Messenger@net /Log drive:C /Site:1 /Batch:Y
```

- Scheduled, using Windows Scheduler

  If you want automatically created backups of files, you must use the Scheduler in Windows to start the Backup module. If activated from the Scheduler, eBACKUP makes a copy of the files that you have specified in the eBACKUP configuration tables, in the directories that you have specified.

> **Note:**
> It is not sufficient to start the eBACKUP.exe file from the scheduler. You must specify the correct parameters in the scheduler as well.

How to set up a Scheduled task for eBACKUP

1. Open the Scheduled Tasks wizard.

Click **Start** on the Windows task bar, and choose **Settings > Control Panel > Scheduled tasks > Add scheduled task**. The Scheduled Task wizard is displayed.

2. Open the Scheduled Tasks window.

   In the Scheduled Task wizard, click **Next**. Now you are in the Window, where you must select a program.

3. Browse to the eBackup program.

   Use **Browse** to go to the **eBACKUP.exe** program in the `C:\SOPHO Messenger@net\Exe\eBACKUP.exe`, and click open.

   ```
   C:\SOPHO Messenger@net\Exe\eBACKUP.exe /Path:C:\SOPHO
   Messenger@net /Log drive:C /Site:1 /Batch:Y
   ```

4. Set the frequency of the backup.

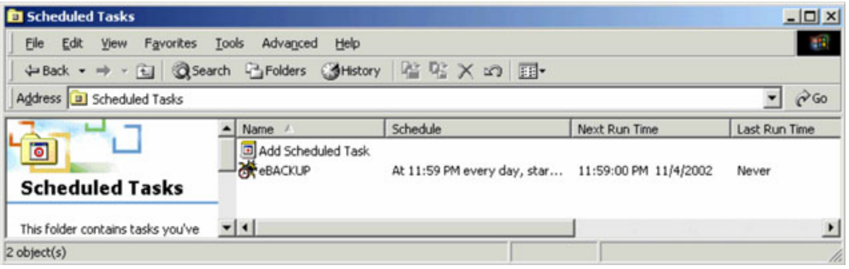
   Select **Daily** or another desired time scale. Click **Next**.

5. Select the time and the day, and select the user name to run the task under.

   - Fill in the desired start time and date.
   - Click **Next**.
   - In the window that is now displayed, select the Windows user under which the task must run. This is usually the administrator.
   - Click **Next**.
   - Click **Finish**.

6. Open the eBACKUP Properties.

   Right-click the **eBACKUP** line in the window. In the pop-up menu, select **Properties**.



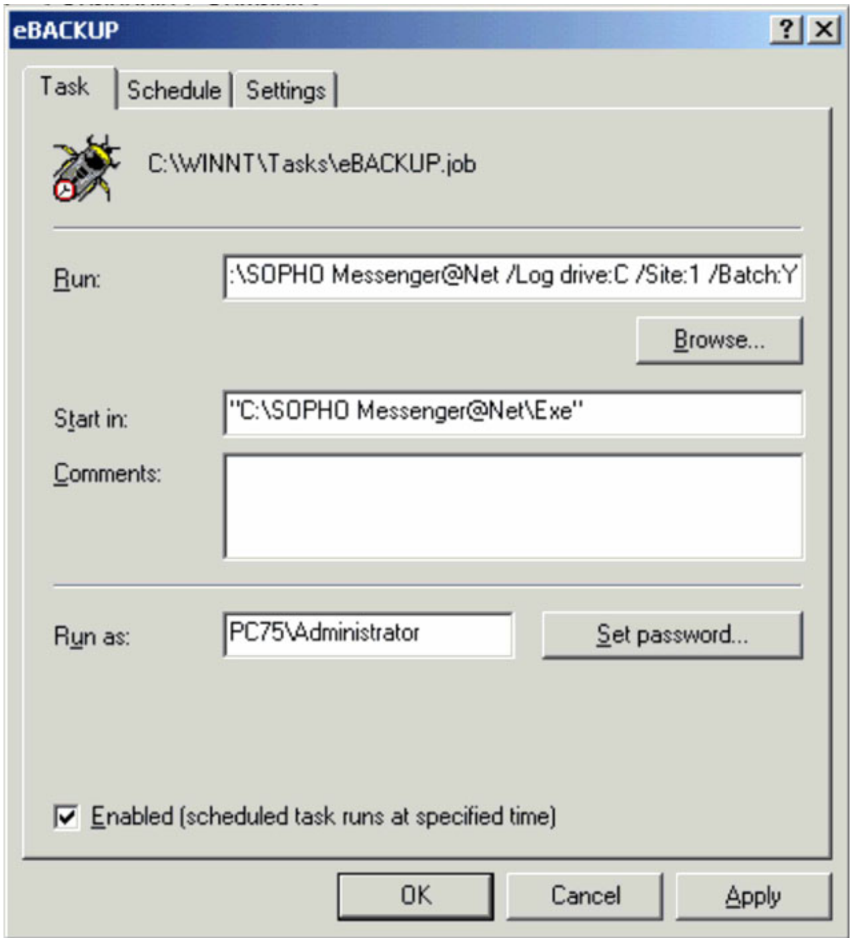
Name	Schedule	Next Run Time	Last Run Time
Add Scheduled Task			
eBACKUP	At 11:59 PM every day, star...	11:59:00 PM 11/4/2002	Never

7. Edit the command arguments.

   Clear the field **Run**. Fill in the following string in this field:

   ```
   C:\SOPHO Messenger@net\Exe\eBACKUP.exe / Path:C:\SOPHO
   Messenger@net /Log drive:C /Site:1 /Batch:Y.
   ```

   Click **OK** to close the **Properties** window.



C:\WINNT\Tasks\eBACKUP.job

Run: :\SOPHO Messenger@Net /Log drive:C /Site:1 /Batch:Y

Start in: "C:\SOPHO Messenger@Net\Exe"

Comments:

Run as: PC75\Administrator

☑ Enabled (scheduled task runs at specified time)

8. Select the file to back up.

   In the eCONFIG module **eBACKUP**, select which file you want to back up.

Setting up e-mail integration (eSMTP_Server/eSMTP)

General

DECT Messenger can both send and receive e-mail messages. The following modules are available for e-mail:

- eSMTP_Server

  This module is capable of receiving and handling e-mail messages. Figure 43: Sending e-mail from client to DECT Messenger on page 131 shows the path of an e-mail message from client to DECT Messenger.

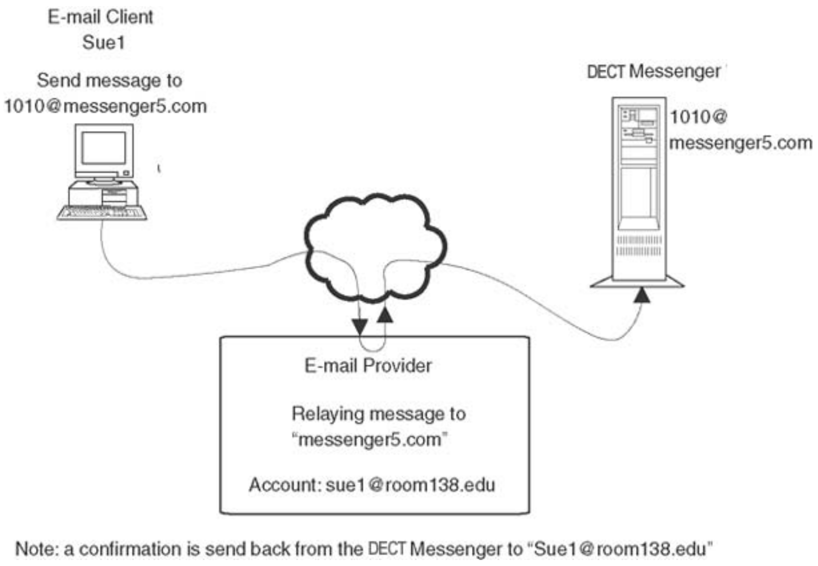


Figure 43: Sending e-mail from client to DECT Messenger

In DECT Messenger, the eSMTP_Server works in cooperation with the Microsoft Internet Information Services (IIS). It is possible that other e-mail servers can be used instead of IIS, but they are not supported.

- eSMTP (client)

  eSMTP behaves like an e-mail client program that sends e-mail messages to an e-mail server. The format is the standard SMTP (Simple Mail Transfer Protocol) defined in the RFC 821 specification.

  If a Lotus Notes Domino server is installed on the system, there must also be a Lotus Notes SMTP server that is capable of receiving SMTP messages from DECT Messenger. You cannot send an e-mail message from DECT Messenger directly to a Domino server.

Using eSMTP Server

How eSMTP Works

The eSMTP_Server handles incoming e-mail messages, working in cooperation with IIS. In Figure 44: e-mail handling in DECT Messenger on page 132 the structure of the e-mail path is depicted.

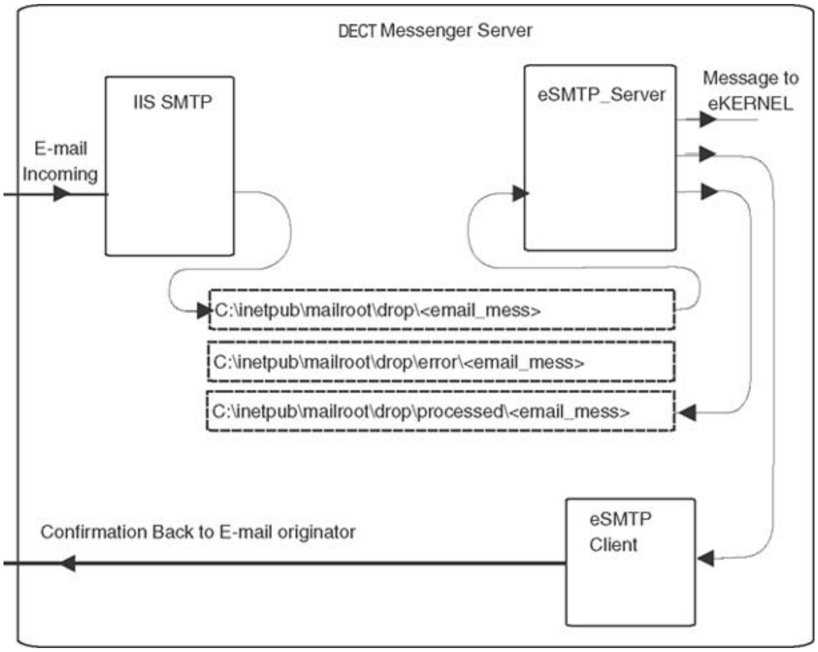

DECT Messenger Server
IIS SMTP
eSMTP_Server
Message to eKERNEL
E-mail Incoming
C:\inetpub\mailroot\drop\<email_mess>
C:\inetpub\mailroot\drop\error\<email_mess>
C:\inetpub\mailroot\drop\processed\<email_mess>
Confirmation Back to E-mail originator
eSMTP Client

Figure 44: e-mail handling in DECT Messenger

After an e-mail is sent from the e-mail client to DECT Messenger, the e-mail generally goes through an e-mail provider (through a server). In this e-mail Server, relaying must be switched on, otherwise the e-mail is not transferred to DECT Messenger. Also, the e-mail Server must know to which PC the e-mail message is to be sent. Therefore, a DNS Server must be assigned in the e-mail Server, and within that DNS server, an MX record must define the relation to the DNS name of the DECT Messenger PC.

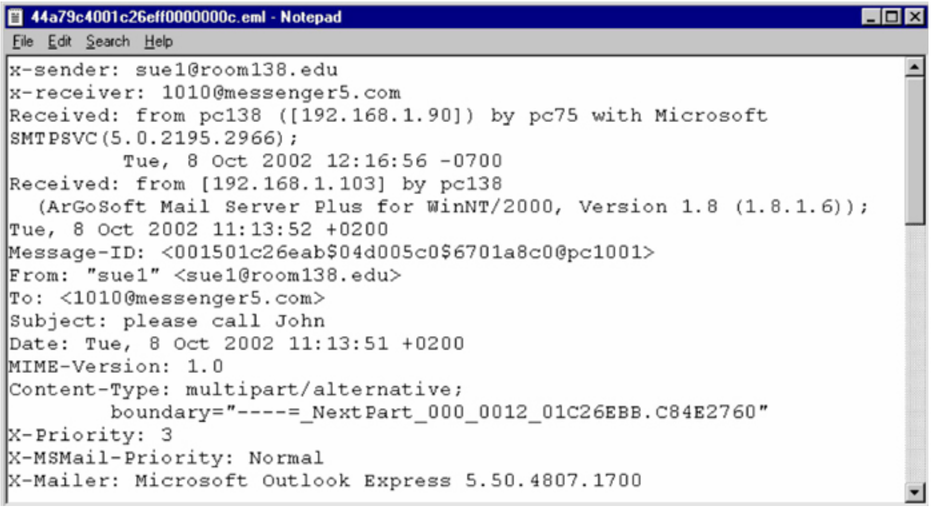
After an e-mail is sent to DECT Messenger, the message arrives at the IIS SMTP server. The IIS SMTP Server stores the mail message as a file in a specified directory on the hard disk. This directory is the interface between IIS and the eSMTP_Server software. The eSMTP_Server checks the contents of this directory every 10 seconds. If there is a mail message, eSMTP_Server loads and analyses it as follows:

- The e-mail address on DECT Messenger (for example, 1010@messenger5.com) is the message destination (a Group in the DECT Messenger configuration).
- The subject of the e-mail message is the message that is sent.
- The originator's e-mail address is the address to which the confirmation message is sent using the eSMTP client.

After processing the e-mail message, the eSMTP_Server puts the message in the directory C:\inetpub\mailroot\drop\processed. If the message cannot be properly processed, eSMTP_Server does not put the message in the processed directory, but in the directory C:\inetpub\mailroot\drop\error.

Note:

You do not need to create users in the IIS. IIS is used for incoming SMTP only. On incoming e-mail, no authentication check is done. A message to any user (the address part preceding the @ in the e-mail address) is accepted. However, the domain name (part after the @) is checked by IIS.



```
x-sender: sue1@room138.edu
x-receiver: 1010@messenger5.com
Received: from pc138 ([192.168.1.90]) by pc75 with Microsoft
SMTPSVC(5.0.2195.2966);
         Tue, 8 Oct 2002 12:16:56 -0700
Received: from [192.168.1.103] by pc138
  (ArGoSoft Mail Server Plus for WinNT/2000, Version 1.8 (1.8.1.6));
Tue, 8 Oct 2002 11:13:52 +0200
Message-ID: <001501c26eab$04d005c0$6701a8c0@pc1001>
From: "sue1" <sue1@room138.edu>
To: <1010@messenger5.com>
Subject: please call John
Date: Tue, 8 Oct 2002 11:13:51 +0200
MIME-Version: 1.0
Content-Type: multipart/alternative;
        boundary="----=_NextPart_000_0012_01C26EBB.C84E2760"
X-Priority: 3
X-MSMail-Priority: Normal
X-Mailer: Microsoft Outlook Express 5.50.4807.1700
```

Figure 45: Example of e-mail message

The following fields in the message are processed:

- x-sender: sue1@room138.edu

  The part that follows after x-sender: is the originator of the message; a confirmation message is sent to this address. If you have an e-mail server program other than IIS, there is no x-sender: field. Then the eSMTP_Server uses the field: From: sue1 <sue1@room138.edu> instead.

- x-receiver: 1010@messenger5.com

  The part that follows after x-receiver: is used to determine to which DECT Messenger group the message must be sent. (A group contains devices which are assigned as members). The conversion is made in the eKERNEL_Group and eKERNEL_Member tables. If you do not have IIS but another e-mail server program instead, there is no x-receiver: field. Then the eSMTP_Server uses the field: To: <1010@messenger5.com> instead.

- Subject: please call John

  The message please call John is sent as message to the destinations (devices).

Because DECT Messenger uses IIS, you must install and set up IIS. If you are using Windows 2000 Server, IIS is installed automatically, and you only have to configure IIS. If you are using Windows 2000 Professional, you must install IIS separately, and then configure IIS. Installing IIS is described in Installing IIS on page 134. Configuring IIS is described in Configuring IIS for DECT Messenger on page 135.

In the eCONFIG you must set up the configuration for the eSMTP_Server. For further information on setting up the eSMTP_Server, see *Avaya DECT Messenger Installation and Commissioning, NN43120-301*.

Installing IIS

The following procedure guides you through the IIS installation process.

Note:

You must have the Windows CD-ROM on hand to complete this procedure.

Note:

In Windows 2000/XP Professional, IIS is not installed by default. In Windows 2000/2003 Server, IIS is installed by default.

Install IIS

1. Open Add/Remove Programs.
    - Click **Start** on the Windows task bar, and choose **Settings > Control Panel**.
    - Double-click **Add/Remove Programs**.
2. Open **Add/Remove Windows Components**.

    Click **Add/Remove Windows Components**
3. Add Internet Information Services (IIS).
    - In the Windows Components window, check the check box **Internet Information Services**.
    - Click **Next**.
    - Insert the Windows CD-ROM after the system asks for it.

Note:

After installing IIS, you must reinstall Windows 2000 Service Pack 4.

Configuring eSMTP_Server in eConfig

You can use the default settings for the eSMTP_Server module in eCONFIG.

You must create a Group Name for each e-mail address you wish to associate with DECT Messenger. Each group must contain the destination device to which messages must be sent.

For example: A user wishes to send a message from their e-mail client to the DECT handset owned by Security1. The following steps are required:

Sending an e-mail message to a DECT handset

1. Assuming DECT Messenger has a domain name configured as messenger.com, create a group within the eSMTP_Server module called Security1@messenger.com.
2. Within this group add the eDMSAPI device 04#32, which is a DECT handset owned by Security1.

Configuring IIS for DECT Messenger

The IIS must be configured to work with DECT Messenger. Use the following procedure to configure IIS for DECT Messenger.

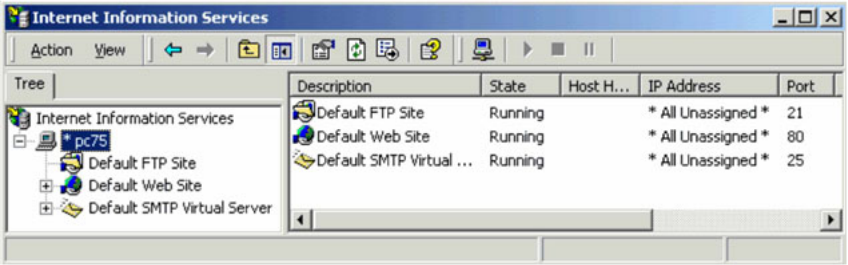
Configure IIS for DECT Messenger

1. Open the Internet Services Manager (IIS).

   Click **Start** on the Windows task bar, and choose **Settings Control Panel > Administrative Tools > Internet Services Manager**.

2. Disable the default ftp/web sites.

   - Expand the PC name to access the FTP, WEB, and SMTP services under it.
   - Right-click the **Default FTP Site**, and select **Stop** in the pop-up menu.

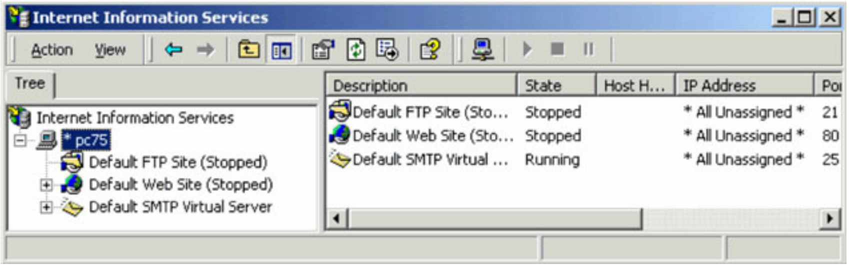

Internet Information Services
Action
View
Tree
Internet Information Services
* pc75
Default FTP Site
Default Web Site
Default SMTP Virtual Server

Description	State	Host H...	IP Address	Port
Default FTP Site	Running		* All Unassigned *	21
Default Web Site	Running		* All Unassigned *	80
Default SMTP Virtual ...	Running		* All Unassigned *	25

- Right-click the **Default Web Site**, and select **Stop** in the pop-up menu.

Note:

If the Default Web Site is already stopped, IIS has detected that your Apache Web server is running. You can have only one web server running on port 80, which is the reason why IIS web server must be stopped. Check to ensure the State column changes to read Stopped, as shown in the following image:



Internet Information Services
- pc75
  - Default FTP Site (Stopped)
  - Default Web Site (Stopped)
  - Default SMTP Virtual Server

Description	State	Host H...	IP Address	Poi
Default FTP Site (Sto...	Stopped		* All Unassigned *	21
Default Web Site (Sto...	Stopped		* All Unassigned *	80
Default SMTP Virtual ...	Running		* All Unassigned *	25

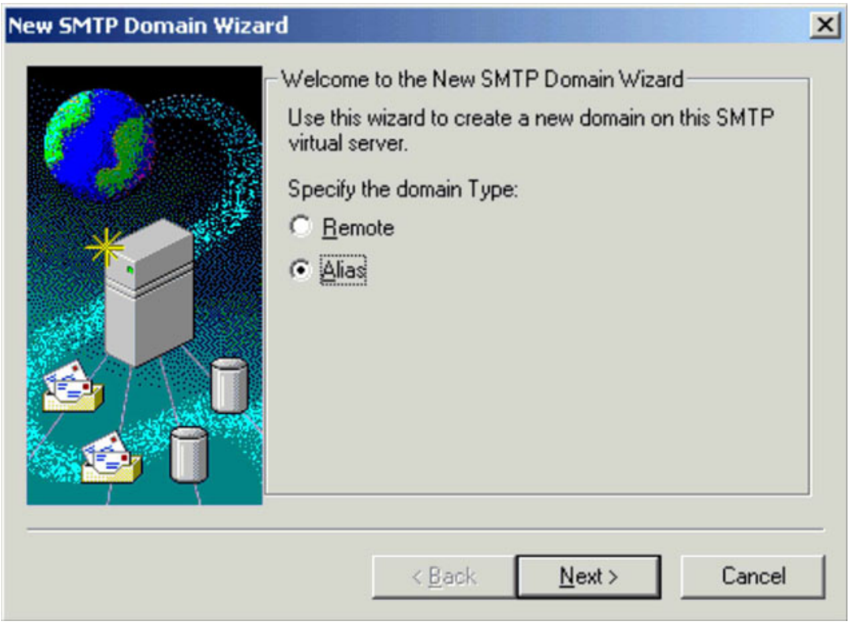
Hereafter, IIS does not start the FTP and WEB services. Only the SMTP Services are running.

3. Create a new domain.

   - Expand Default SMTP Virtual Server, by clicking on the **+** sign in front of it. Two submenu items are shown: Domains and Current Sessions.
   - Right-click **Domains** (under Default SMTP Virtual Server), and select **New > Domain** in the pop-up menu.

4. Specify the domain type.

   Select **Alias**, and click **Next**.



New SMTP Domain Wizard

Welcome to the New SMTP Domain Wizard

Use this wizard to create a new domain on this SMTP virtual server.

Specify the domain Type:

○ Remote

● Alias

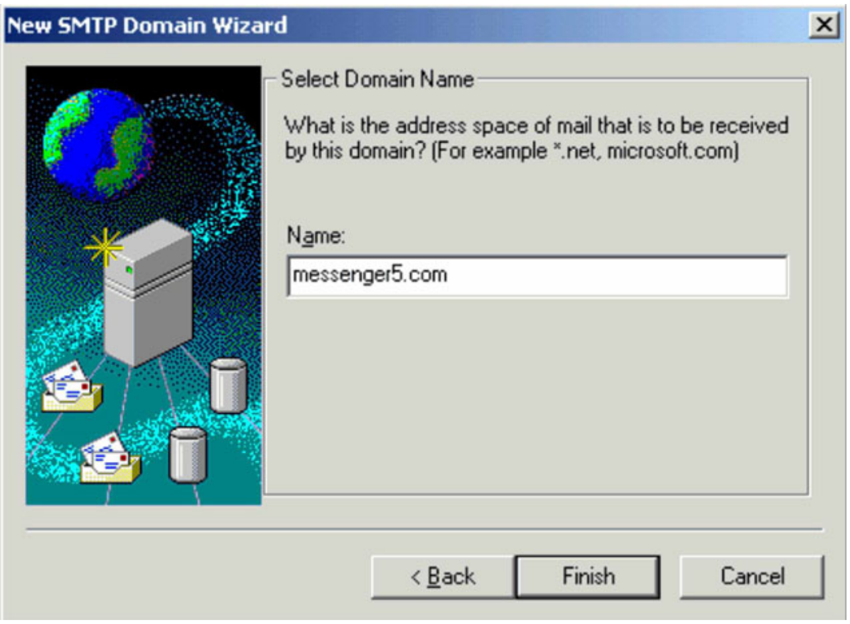
5. Set the domain name.

   Enter the domain name. If necessary, contact your system administrator to verify the domain name. This name must be defined in a DNS Server with a reference to the IP address of the DECT Messenger server PC (the PC where IIS has been installed, together with the eSMTP_Server module).

   Note:

   This domain is also the part after the @ in the e-mail message. Therefore, if you send an e-mail message to DECT Messenger with, for example e-mail address

2000@messenger5.com, the part after the @ (in this example, messenger5.com) must be specified as Alias in IIS.

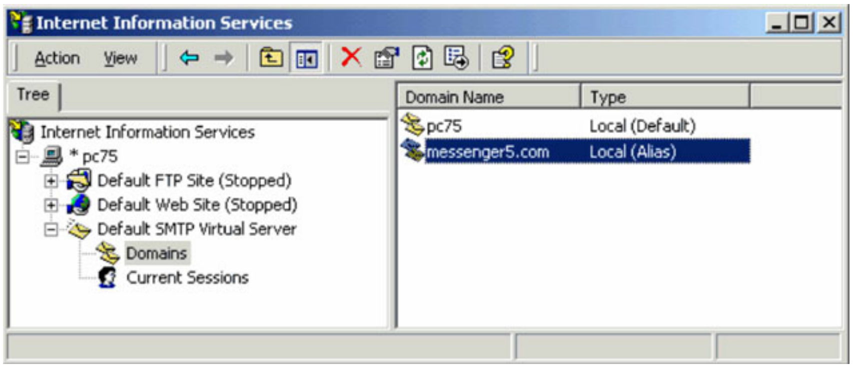


What is the address space of mail that is to be received by this domain? (For example *.net, microsoft.com)

Name: messenger5.com

6. Verify the Domain Name list.

   After entering the Alias, the IIS window must look like the following example:


Internet Information Services
Action
View
Tree
Internet Information Services
* pc75
Default FTP Site (Stopped)
Default Web Site (Stopped)
Default SMTP Virtual Server
Domains
Current Sessions

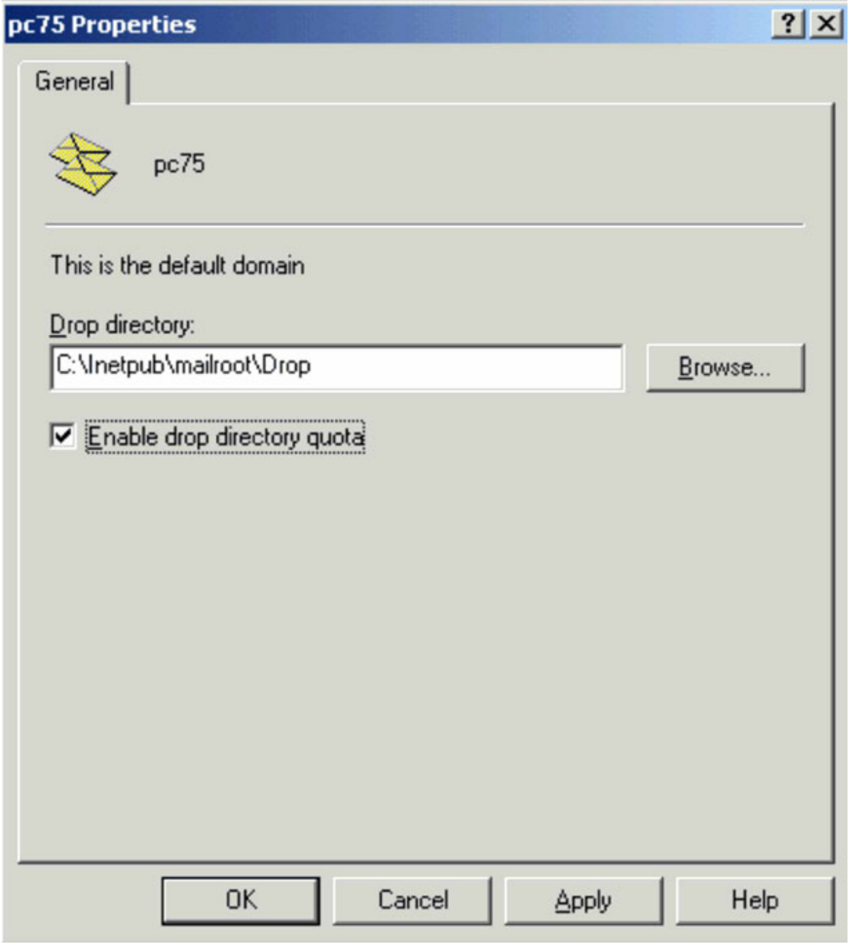
Domain Name	Type
pc75	Local (Default)
messenger5.com	Local (Alias)

Note:

The name Alias in this window is an example. In your configuration a different name appears.

7. Set the Drop Directory path.

   - Right-click the PC name (in this example: PC75), and select **Properties** from the pop-up menu. The following window opens:



This is the default domain

Drop directory: C:\Inetpub\mailroot\Drop

☑ Enable drop directory quota

The **Drop Directory** field specifies a directory where IIS drops all incoming messages.

- Leave the default value in place.
- Click **OK**.

Using eSMTP

The eSMTP module behaves like an e-mail client such as MS Outlook Express. Therefore, you must enter the Domain name and IP address of the SMTP Server to which you send e-mail messages.

Sending SMS messages

eSMTP

Many Global System for Mobile Communications (GSM) Service providers have an SMTP gateway into their SMS Centre, either directly, or through a third-party company.

Consult with your local GSM provider to see if this facility is available. They can provide you with an e-mail address and format.

For example: A DECT Messenger user wishes to use a GSM handset as an alternative device to the DECT handset. The following steps are required:

Using a GSM handset as an alternative to the DECT handset

1. Create a new device called +353849947269@serviceprovider.COM with output program eSMTP.

   (The GSM Service provider must have this GSM mobile number configured in their database, or extract the number from the format: GSMmobileNumber@domain.com.)

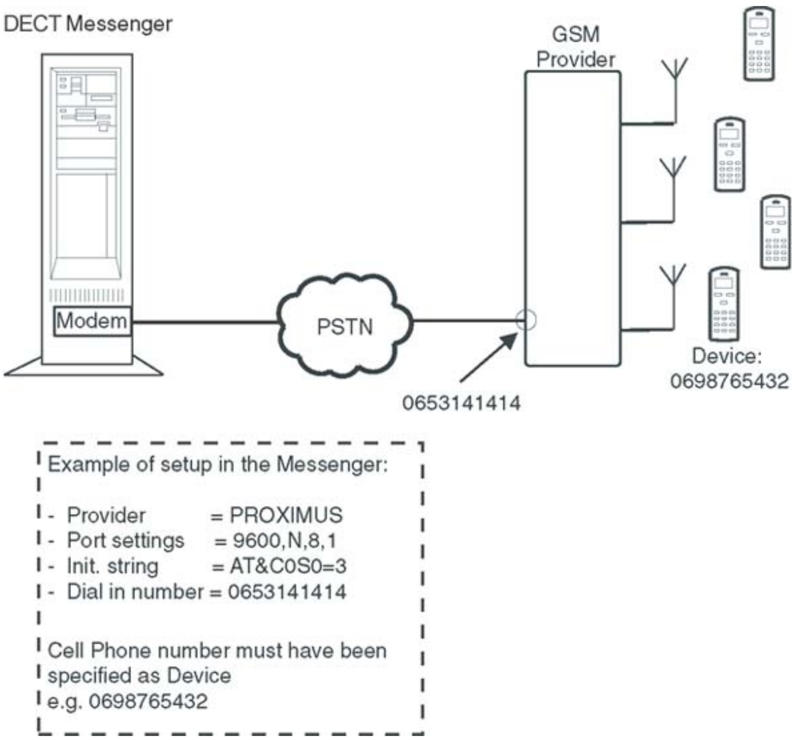
2. Add this eSMTP device as an alternative device in the DECT handset device properties.

3. Set the number of retries for the DECT device = 2.

   If DECT Messenger sends an urgent message to the DECT handset and the DECT handset does not respond after two attempts, the message is sent as an SMS to the GSM handset.

eASYNC

The eASYNC module is capable of sending short message service (SMS) messages to any GSM mobile phone, worldwide, from your DECT Messenger computer. Figure 46: Setup for sending SMS Messages (or Wide Area Paging messages) on page 140 shows the configuration.



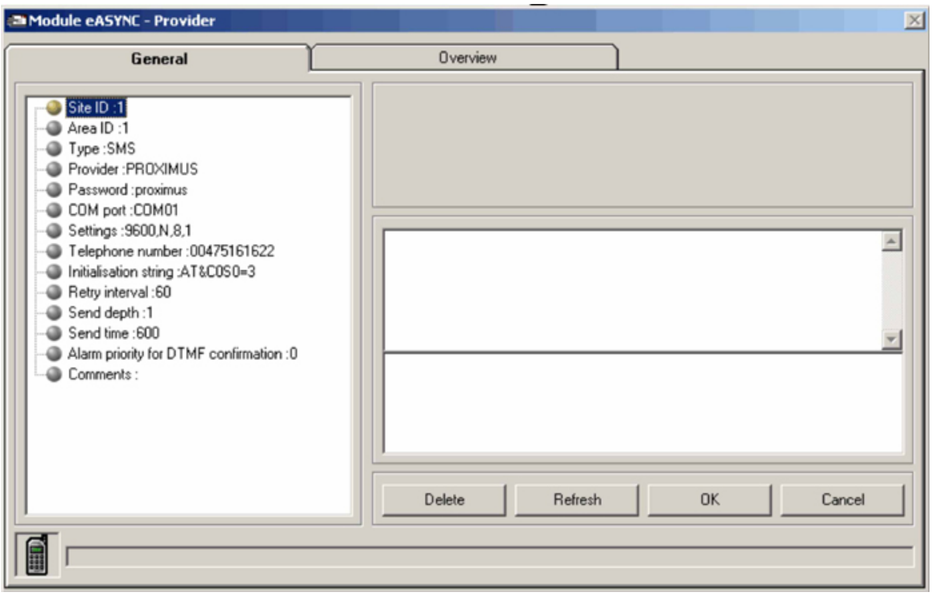
Example of setup in the Messenger:

- Provider = PROXIMUS
- Port settings = 9600,N,8,1
- Init. string = AT&C0S0=3
- Dial in number = 0653141414

Cell Phone number must have been specified as Device e.g. 0698765432

Figure 46: Setup for sending SMS Messages (or Wide Area Paging messages)

The connection between DECT Messenger and the GSM SMS provider is made through a modem connection using the PSTN. In DECT Messenger, you must specify the correct settings for this connection. In the eCONFIG, go to the eASYNC Module to change the settings; the window shown in Figure 47: eASYNC settings on page 141 opens.



- Site ID :1
- Area ID :1
- Type :SMS
- Provider :PROXIMUS
- Password :proximus
- COM port :COM01
- Settings :9600,N,8,1
- Telephone number :00475161622
- Initialisation string :AT&C0S0=3
- Retry interval :60
- Send depth :1
- Send time :600
- Alarm priority for DTMF confirmation :0
- Comments :

Figure 47: eASYNC settings

The following overview explains the eASYNC settings:

- Type

  The type is either SMS for SMS messages to GSM phones, or Paging for Wide Area Paging.

- Provider

  This is the name of the (GSM) provider that provides the dial-in option for SMS or Wide Area paging.

  Note:

  This field only supports the following names: BELGACOM, PROXIMUS, and KPN:

  - BELGACOM refers to the Wide Area paging protocol.
  - PROXIMUS and KPN refer to the Universal Computer Protocol (UCP) for SMS messages, where PROXIMUS is the Belgium provider, and KPN the Dutch provider. The difference between PROXIMUS and KPN is that PROXIMUS requires a password (proximus) to dial in, and KPN does not require a password. In both cases the UCP protocol is used, and that protocol is supported by many other GSM SMS providers.

- Settings/Serial port settings

  The serial port settings depends on the settings that are supported by the provider. Almost all providers support the following settings: 9600 b/s, no parity, 8 bits, 1 stop bit (9600,N,8,1).

- Telephone Number

The messenger must know what number to dial to access the provider. (This is not the extension number of the cell phone [GSM phone] to which the message must be sent.) As example, for PROXIMUS, this is number 00475161622.

- Initialization string

  This is the initialization string for modem initialization. The string depends on the type of modem that you use. A generic modem initialization string can be for example: AT&C0S0=3. Consult the modem reference guide for your modem.

- Retry Interval

  If a message cannot be delivered to the Provider (for example, because the modem line is busy), the system tries again after the specified time period.

- Send Depth

  DECT Messenger collects a number of messages before sending the messages. Send Depth determines how many messages are collected, before making a connection to the provider. Default = 1, which means that messages are processed as soon as they arrive.

- Send Time

  Time delay before processing received messages. If the Send Depth is set to a value higher than 1, eaSYNC waits to send the messages until the number of messages received equals the Send Depth value; that can take a long time, particularly during off-peak hours. To prevent DECT Messenger from waiting for a long period, you can specify a Send Time. After a message arrives, eASYNC waits for the number of seconds specified in this field, and DECT Messenger sends the message, ignoring the Send Depth value.

- Alarm Priority for DTMF confirmation

  This is a priority threshold. If the priority that comes with the alarm is higher than this threshold, the alarm requires a confirmation from external. If the Priority is lower that this threshold, the alarm does not require a confirmation: successfully sending the message to the SMS Provider makes that the alarm is withdrawn, and not repeated anymore.

V.24 - RS232 connections (eCAP, eESPA)

The eCAP and the eESPA modules allow you to connect RS232 devices to DECT Messenger. There is a significant difference between the eCAP module and the eESPA module. Therefore, these modules are explained separately in the following subsections.

eCAP

There are four different types of devices that can be connected to the eCAP module using V.24/RS232, as follows:

- Nurse Call systems

  There are many types of Nurse Call systems offering data using V.24/RS232. However, there is no standard protocol.

- Building Management systems

  There are many types of Building Management systems offering data using V.24/RS232. However, there is no standard protocol.

- Paging systems

  There are many types of Paging systems. Almost all offer a V.24/RS232 interface carrying the ESPA protocol. If the paging System supports ESPA 444 protocol, use the eESPA module instead of the eCAP.

- Line Printer Protocols

  Some older Building Management systems offer a line printer protocol over V.24/RS232. This is a simple type of protocol, offering only incoming data. There is no guarding on the protocol, such as ACK/NAK, or timers.

Before using the eCAP module, check which protocol is offered, and check with Avaya, to see if the protocol is supported by DECT Messenger.

If the protocol is supported, install the correct eCAP module. If a Line Printer protocol is required, you can build the protocol yourself.

Remember that the DECT Messenger structure is based on five parameters; see Parameters required to set an alarm on page 96. You must know which parameters are coming in from the external system, and you must specify these parameters in DECT Messenger. For more information, see *Avaya DECT Messenger Installation and Commissioning, NN43120-301*, which describes the supported protocols in detail.

eESPA

The eESPA module supports the ESPA 444 protocol. This is a complex protocol; see *Avaya DECT Messenger Installation and Commissioning, NN43120-301* for more detailed information about the protocol. Read the information provided for the protocol before attempting to set up the eESPA Module.

Using Import/Export menu

You can use eCONFIG to import and export configuration database tables. The menu options are shown in Figure 48: Import/Export menu options on page 144.

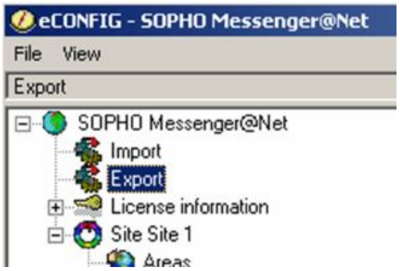
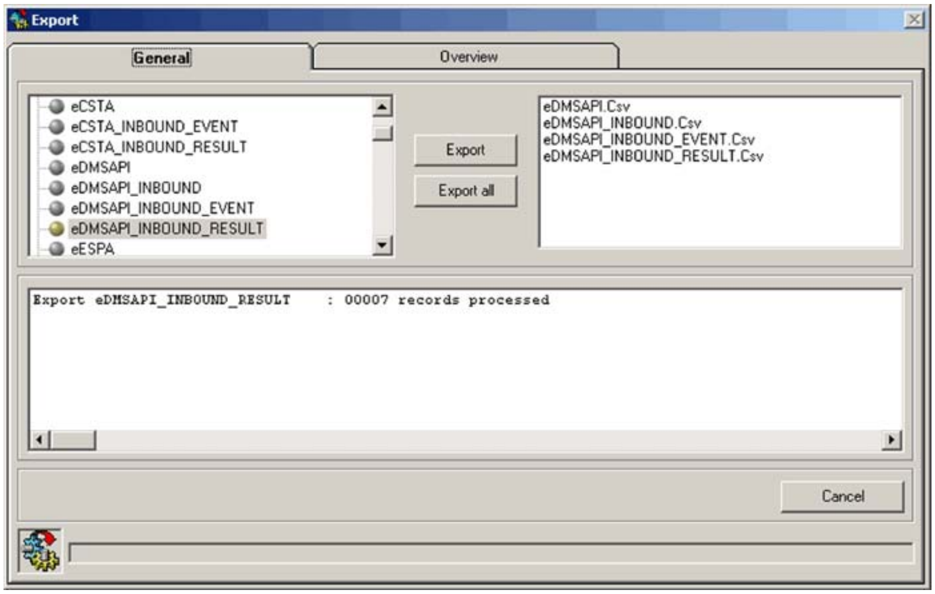


Figure 48: Import/Export menu options

The Import/Export function can only handle files of the type .csv.

Double-click **Export**, to open the following window:



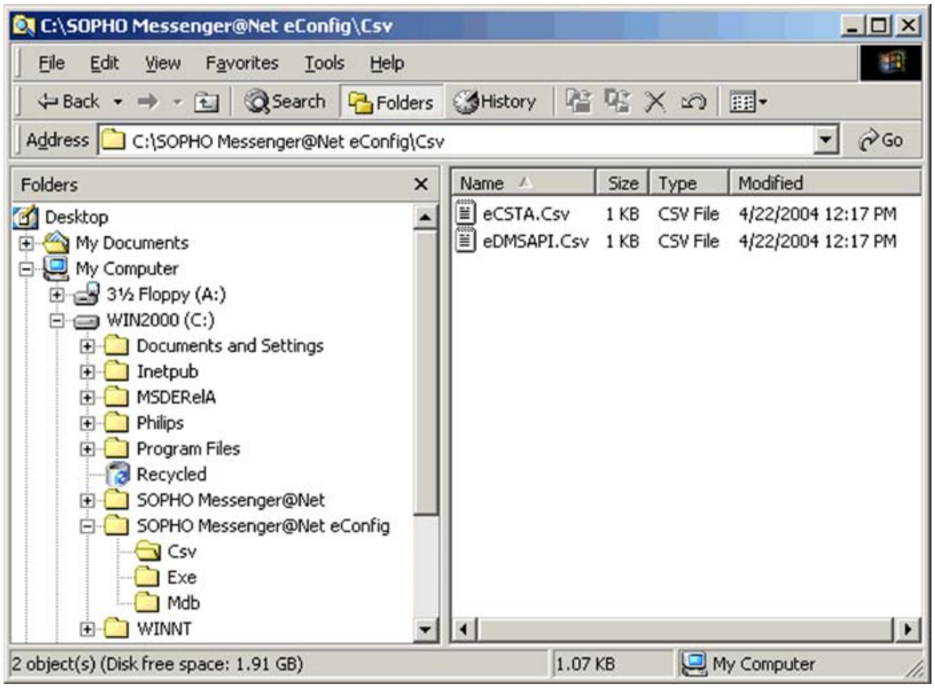
eDMSAPI.Csv
eDMSAPI_INBOUND.Csv
eDMSAPI_INBOUND_EVENT.Csv
eDMSAPI_INBOUND_RESULT.Csv

```
Export eDMSAPI_INBOUND_RESULT    : 00007 records processed
```

Figure 49: The Export window

In the left-top pane, a list of configuration database tables is shown. Select the table that you want to export, and click **Export**. The table is exported immediately as a .csv file.

The files are stored in the following directory: C:\SOPHO Messenger@net eConfig\Csv



Address: C:\SOPHO Messenger@Net eConfig\Csv

Name	Size	Type	Modified
eCSTA.Csv	1 KB	CSV File	4/22/2004 12:17 PM
eDMSAPI.Csv	1 KB	CSV File	4/22/2004 12:17 PM

2 object(s) (Disk free space: 1.91 GB) 1.07 KB My Computer

Figure 50: The configuration file storage directory

You can also import configuration database tables using the Import menu. You must ensure that the format of the .csv file matches the required format. To ensure that the format is correct, you can export the table as an example.

Note:

Ensure that the format and the contents of the .csv files are correct, before you start the import function. An improperly formatted .csv file can corrupt your DECT Messenger system configuration, which can cause unpredictable errors. on page 773/>Ensure that the format and the contents of the .csv files are correct, before you start the import function. An improperly formatted .csv file can corrupt your DECT Messenger system configuration, which can cause unpredictable errors.

eLOG

The eLOG module provides information on how DECT Messenger processes an incoming alarm from the input to the output device. This can be necessary if it is not clear whether a person received a message or not. The eLOG module does not have a user interface and does not provide nice charts. However, it provides three *.csv files with detailed information indicating how the alarm was processed.

Note:

You must have sufficient technical knowledge of DECT Messenger to understand the contents of the files.

The following three files are automatically created and updated:

- INrqs.csv

  This file contains individual records for each alarm that came into the eKERNEL.
- OUTrqs.csv

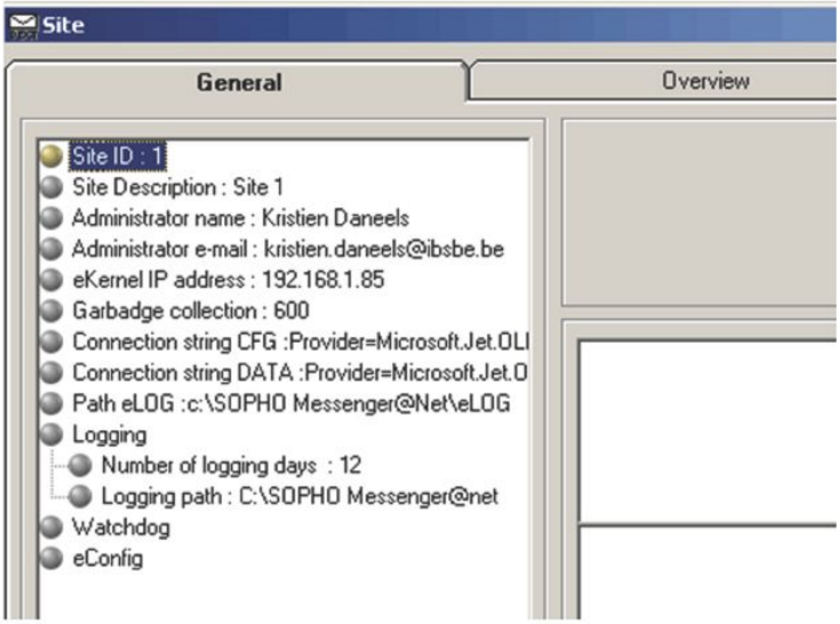
  This file contains individual records for each outgoing alarm from the eKERNEL, for each individual device.
- OUTrpy.csv

  This file contains individual records for the response(s) of each output device on an alarm.

The eLOG module is part of the eKERNEL and is activated if the license for eLOG is present. It automatically stores the three files into the following default directory:

```
C:\Messenger@Net\eLOG
```

You can change this path through the eCONFIG module. Double-click the Site menu option and you see the following window:



- Site ID : 1
- Site Description : Site 1
- Administrator name : Kristien Daneels
- Administrator e-mail : kristien.daneels@ibsbe.be
- eKernel IP address : 192.168.1.85
- Garbadge collection : 600
- Connection string CFG :Provider=Microsoft.Jet.OLI
- Connection string DATA :Provider=Microsoft.Jet.O
- Path eLOG :c:\SOPHO Messenger@Net\eLOG
- Logging
  - Number of logging days : 12
  - Logging path : C:\SOPHO Messenger@net
- Watchdog
- eConfig

Figure 51: eCONFIG module site menu

In the menu option Path eLOG you can enter the path for the eLOG files. The menu option Number of Logging days is NOT applicable for the eLOG files. The eLOG files are never deleted by DECT Messenger. Therefore it can be wise to change the path to another drive on the same PC or to a network drive. This prevents the C drive from becoming overburdened with eLOG files.

The logging information is written to a 1Kb buffer, instead of to the files. The contents of the files is updated as follows:

- After you shut down the eKernel
- After the buffer is full. Remember the buffer is to midnight (after the date changes)
- At midnight (after the date changes) and there is something in the buffer, a new set of files is created and the contents of the buffer is written to the files.
- Manually. If you want to read out recent information from the files, you can force an update manually. Go to the eKernel window and select Refresh Logfile in the pull down menu eKernel. See following window:

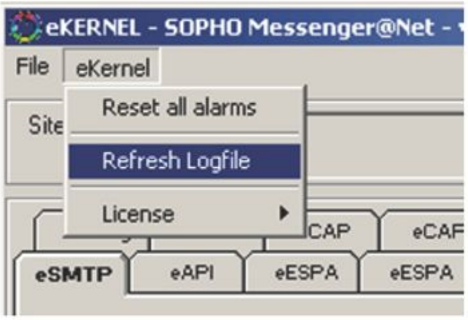


Figure 52: eKERNEL module refresh log file

The contents of these files are related to each other by means of identifiers. You can import the files into a Spreadsheet application or Database Application of your choice, for further analysis.

In the following sections, the contents of these files is explained.

ALARM Remove After GROUP id GROUP Description DEVICE id DEVICE area DEVICE Outpgm eWEB user PINCODE Reason not processed

INrqs.csv

The file INrqs.csv contains detailed information on the incoming alarms. The following columns are available:

- INRQS id

  This is a tag for each input request. This tag is an identifier for each call. After the call is processed, the tag is free again and is used for another incoming alarm. Therefore this tag must always be seen in relation to the incoming alarm time and date. This INRQS id is used in the two other LOG files that specifies the output processing.

- DATE

  Date in format: YYYY-MM-DD

- TIME

  Time in format: HH-MM-ss

- SET or RESET

The incoming request was a request to Set or Reset an alarm.

- TYPE

  Indicates the type of incoming message:

  - msgrqs = Message request or also called incoming alarm
  - incrqs *IC = Incoming Confirmation

- INPGM id

  The Input Program ID. Each input program has its own unique identifier. An Input Program ID is an identifier only, and the digits do not necessarily have a meaning, however, there the common convention is to use the digits as follows:

Table 16: Default Input Program Identification.

Digit	Meaning
1	Site identifier
2	Area identifier
3	Input program identifier - 1 = eCAP or eAPI or eESPA - 4 = eVBVOICE - 5 = eCSTA - 6 = eIO - 7 = eWEB - 8 = eSMTP_server - 9 = eDMSAPI
4 and 5	01-99 Input program sequence number

- INPGM Appl

  Input Program Module Application name. The previously mentioned Input Program ID is always unique, however, this input Program Module Application name is not always unique.

- INPGM Manufacturer

  Description of the manufacturer of the input program. It is a description only. This field is not used in alarm processing at all.

- INPUT DEVICE

  Some input programs generate a specification of where the alarm came from, for example, the eSMTP_server module indicates the Senders E-mail Address. After an alarm comes in through eCSTA or eDMSAPI, and the Calling Line ID is sent over the CSTA connection, you see the CLI of the calling extension.

- MESSAGE

This is the message as it is sent to the output device. Note that this message can differ from the original message. There are two main items that can cause a difference between the original message and this message field:

- Alarm Length as specified in the Alarm ID definitions.

  If the Alarm Length is set to 10 characters, only the first 10 characters of the original message are regarded as relevant and the remaining characters are stripped off.

- Message Format as specified in the eVBVoice Settings of the Alarm ID in eCONFIG.

  The Message Format allows conversion of the original message.

- MESSAGE Original

  This is the original message, as it came from the Input Program.

- ALARM id

  The ALARM id is the unique alarm identifier for processing the input request. This Alarm Identifier, contains parameters on how the alarm must be processed.

- ALARM Prty

  Alarm Priority as specified in the Alarm Record for this Input Request.

- ALARM Description

  Alarm description that is associated with the ALARM id in the Alarm Record for this input. Depending on the Input Program type, it provides either the ALARM id or the description.

- ALARM Remove After

  An Input Program provides the Remove After parameter. It indicates whether the alarm request must stay active until a reset is received from the input program or not.

- GROUP id

  The Group id is the Group Identifier that is provided by the Input Program for an Alarm. In the eKernel, these groups contain one or more Group Members.

- GROUP Description

  The Group Description is a recognizable name for the group, and is associated with the Group id. It is not used for processing the alarm, it is for administrative purposes only.

- DEVICE id

  Not yet implemented.

- DEVICE area

  Not yet implemented.

- DEVICE Outpgm

  Not yet implemented.

- eWEB user

Not yet implemented.

- PINCODE

  After an incoming Confirmation is received, you see the PIN code in this field. (For an Incoming Confirmation, the TYPE filed shows incrqs *IC.)

- Reason not processed

  This field gives you information on why an incoming alarm is not processed. The messages gives you a clear indication of the cause, such as an alarm cannot be processed. Another example of a message is: Called device does not exist in table eCSTA_INBOUND_EVENT.

OUTrqs.csv file

This file contains a record for each outgoing message (request) to a device. The following columns are available:

- OUTRQS id

  This is a tag for each output request. This OUTRQS id is used in the two OUT log files that specifies the output processing. Note that this OUTRQSid is not unique in the logging files. It is used on a call-by-call basis and can therefore be reused for a next call/alarm after the alarm is finished.

- INRQS id

  This is a tag for each input request. This tag is a call-by-call identifier. After the call is processed, the tag is free again and can be used for another incoming alarm. Therefore this tag must always be seen in relation to the incoming alarm time and date. This INRQS id is used in the two other LOG files that specifies the output processing.

- DATE

  Date that the alarm was sent to the output device. Format: YYYY-MM-DD

- TIME

  Time that the alarm was sent to the output device. Format: HH-MM-ss

- DEVICE id

  Device ID of the output device to which the alarm was sent. The Device ID is not necessarily unique. However, the combination of Device ID, Device Area, Device Outpgm and Device Outpgm Facility make the device unique. Therefore you must always consider these fields as a group, to avoid mistakes.

- DEVICE Area

  Area of the output device to which the alarm was sent.

- DEVICE Outpgm

Output Program of the output device to which the alarm was sent.

- DEVICE Outpgm Facility

  Output Program facility of the device to which the alarm was sent. Note that the Facility specifies the device type characteristics.

- DEVICE Member status

  This field indicates the status of the member based on its presence. This status comes from the comparison between the actual time/date and the presence definition on the device as group member. The presence definition is defined through eCONFIG or eWEB after a device is assigned to a Group or after you change the settings of a device in a group.

- MESSAGE

  This is the actual message that is send to the output device. Here you see the same message as in the Message field in the INrqs.csv file.

- ALARM id

  This shows the ALARM id that is used for the outgoing message to the device. According to the structure of DECT Messenger, an Alarm id number or Alarm Description is provided by the Input program for a certain incoming alarm. The Alarm ID and the Description has a fixed relation. In the database, settings are related to this Alarm id that specifies how the incoming alarm must be processed through DECT Messenger. Therefore, you see this Alarm id also in this file for Outgoing message to a device. This Alarm id is the same alarm ID as found in the INrqs.csv for a specific incoming alarm.

- ALARM Description

  Some input programs deliver a character string which is an indication for how the alarm is processed, such as priority and so on, instead of an Alarm id. If the input program delivers such a string, for example eWEB, eCAP, eAPI , and so on, it is always fixed to an Alarm id. This Alarm id describes how the alarm must be processed.

- ALARM Prty

  This indicates the priority for this alarm. A low value means high priority. It comes from the definitions in the Alarm id.

- DIVERTED

  This field indicates that a diversion is active on the output device. This diversion can be a Follow me.

- DIVERTED DEVICE Id

  Diversion destination device.

- DIVERTED DEVICE Area

  Area of the diversion destination device.

- DIVERTED DEVICE Outpgm

Output Program that is used for the diversion destination device.

- DIVERTED DEVICE Outpgm Facility

  Output Program Facility that is used for the diversion destination device.

INrqs.csv

This file contains information about the response(s) (reply) that came from devices on an outgoing alarm/message. The following columns are available:

- OUTRQS id

  This is a tag for each output request. This OUTRQS id is used in the two OUT log files that specifies the output processing. Note that this OUTRQSid is not unique in the logging files. It is used on a call-by-call basis and can therefore be reused for a next call/alarm after the alarm is finished.

- INRQS id

  This is a tag for each input request. This tag is a call-by-call identifier. After the call is processed, the tag is free again and can be used for another incoming alarm. Therefore this tag must always be seen in relation to the incoming alarm time and date. This INRQS id is used in the two other LOG files that specifies the output processing.

- DATE

  Date that the response was received from the output device or from the PBX if the device did not respond itself. Format: YYYY-MM-DD.

- TIME

  Time that the response was received from the output device or from the PBX if the device did not respond itself. Format: HH-MM-ss.

- DEVICE Id

  Device ID of the output device that generated the response. Of course, this is the same as the device to which the alarm was sent. The Device ID is not necessarily unique. However, the combination between the Device ID, the Device Area, Device Outpgm and the Device Outpgm Facility makes the device unique. Therefore you must always take these fields together, to avoid mistakes.

- DEVICE Area

  Area of the output device that generated the response.

- DEVICE Outpgm

  Output Program of the output device that generated the response.

- DEVICE Outpgm Facility

  Output Program facility of the output device that generated the response.

- MESSAGE

  This is the actual message that was send to the output device and for which it generated the response.

- ALARM id

  This shows the ALARM id that was used for the outgoing message, on which the device generated the response.

- ALARM Prty

  This shows the ALARM priority that was used for the outgoing message, on which the device generated the response.

- ALARM Description

  This shows the ALARM Description that was used for the outgoing message, on which the device generated the response.

- REMOVE AFTER

  An Input Program provides the Remove After parameter. It indicates whether the alarm request stays active until a reset is received from the input program or not.

- CONFIRM ACTION

  This shows the setting of the Alarm Confirm Action parameter in the Alarm id. However, this function is not used anymore. Confirm action is specified in the Group Delivery.

- GROUP DELIVERY

  This shows the setting of the Group Delivery parameter in the Alarm id. Values can be *NONE, *ALL or *ANY. In case of *NONE the parameter is ignored and the alarms remain on the device until an incoming Confirmation is received for the device with a PIN code. In case of *ALL, each individual recipient handles messages on individual basis. In case of *ANY, the message must be distributed to at least one group member. After the first user confirms, the message is considered delivered and it removes the message for all group members.

- SILENCE Interval

  This shows the setting of the Silence Interval parameter in the Alarm id. This field defines the number of seconds between repeating the alarm on a device if the device does not respond.

- STATUS

  This is the status of the response. It can be an ACK^, NACK^ or ACK^NACK^.

  - ACK^

    The device has sent an acknowledgement to confirm that the alarm was received by the device. Some devices send such an acknowledgement on receiving the message. Some devices only send an acknowledgement after the message is read by the receiving person.

  - NACK^

    The device has sent a negative-acknowledgement to indicate that the device is unreachable.

  - ACK^NACK^

    The device has sent an acknowledge to confirm that it received the alarm. However, DECT Messenger was waiting for a manual acknowledgement from the device user as well and didn't get it within a certain time period. Therefore an automatic NACK was generated. A manual acknowledgement is always required within 30 seconds after an Urgent message is sent to an LRMS (E2) DECT handset. You can acknowledge the alarm by pressing the OK or the Delete softkey on the DECT handset. In case of a CSTA message to a non-LRMS (E2)-DECT, a NACK is also generated after the user of the device didn't go off hook within the ringing time period.

- CONFIRMED

  This status indicates whether the alarm was confirmed. Confirmed means that a final ACK came from the device or that the confirmation came from another device as Incoming Confirmation with a PIN code through eVBVoice or Calling Line Id. through eCSTA or eDMSAPI.. -1=Confirmed, 0=Not confirmed.

- SET or RESET

  This status indicates the alarm status on the device. As long as an alarm is active on the device, the Alarm Status is Set. After the alarm is reset on a device, the Alarm Status is Reset. Note that after an Alarm is diverted to an Alternative device, the status on the original device goes to Reset and on the alternative device to Set.

- NEXT CALL

  Date and time that the next call are made to the device based on an active alarm on the device. Format: YYYY-MM-DD HH:MM. DECT Messenger makes that call based on the HH:MM:ss instead of crossing the minute boundary.

- SWITCH TO ALTERNATIVE

  This parameter indicates whether the alarm call was diverted to an Alternative Device or not. After an alarm call is diverted, you see a -1 (True) on the original device and on the Alternative device.

  - -1 = Diverted to Alternative device
  - 0 = Not diverted to Alternative device

- ALT DEV Id

  This parameter shows the destination device, in case an alarm call is diverted. Note that a device is not always unique by the Device id parameter on its own. Only in combination with the parameters: ALT DEV Area, ALT DEV Outpgm and ALT DEV Outpgm Facility the device is made unique.

- ALT DEV Area

  Area of the alternative device.

- ALT DEV Outpgm

  Output Program of the alternative device.

- ALT DEV Outpgm Facility

  Output Program Facility of the alternative device.

How to use the Files

The LOG files are used for tracing how an alarm call rolled out. Roughly the procedure is as follows:

Tracing the roll out of an Alarm

1. Make sure that you have all three files.
2. Import these files into a Spreadsheet application.
3. Search for the required incoming alarm in the INrqs.csv file. Then write down the parameters: INRQS id, DATE, TIME and Message.
4. Search a record in the file OUTrqs.csv with the same parameters as you have written down in the previous step. The time can be a few seconds later because of the processing time in the eKERNEL. (The time in the previous step is the eKERNEL received the message/alarm, the time in this step is the time that the eKERNEL has transferred the message/alarm to the output program.
5. Depending on the number of output devices in the Group for this alarm, you have found one or more output records in the file OUTrqs.csv each having an OUTRQS id. Now you know to which devices the alarm/message was sent. You also know the most important parameters that were used to send the alarm/message.
6. Use the identifiers that you used in the previous steps: OUTRQS id, INRQS id, DATE, TIME and Message, to check the reply/response of the devices in the file OUTrpy.csv. This shows you if the device did receive the message, did respond to the message or if the message was diverted to an alternative device.

Checking diagnostics

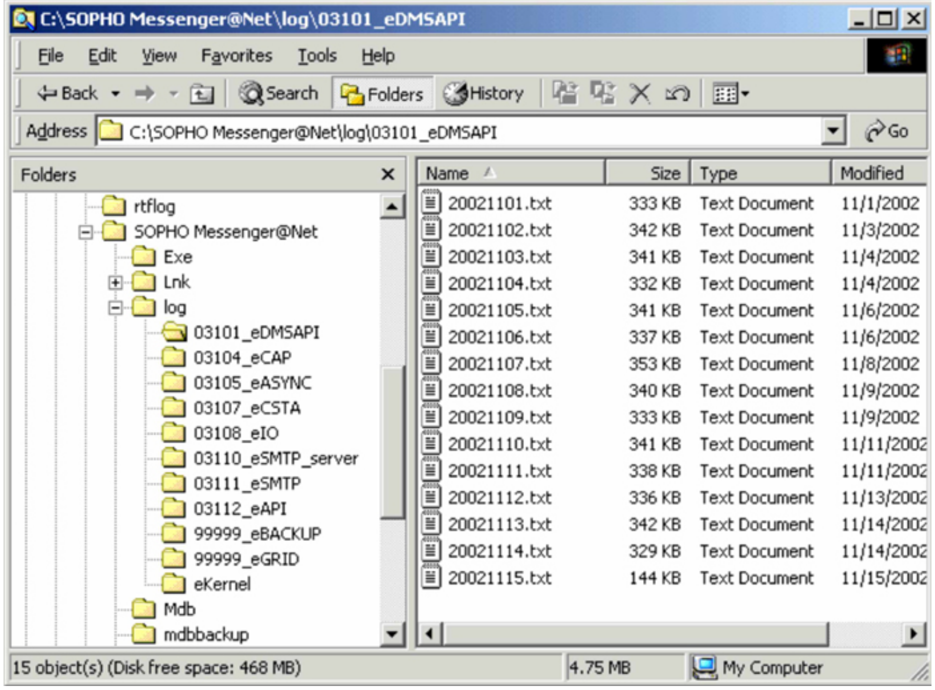
General

The following diagnostics options are discussed in this section:

- Logging on page 156
- Module Window on page 158

Logging

You can use logging to trace history. All the events in each individual module are stored in a log file. Log files are stored in a common directory, as shown in Figure 53: Log file location on page 156.



C:\SOPHO Messenger@Net\log\03101_eDMSAPI

Address C:\SOPHO Messenger@Net\log\03101_eDMSAPI

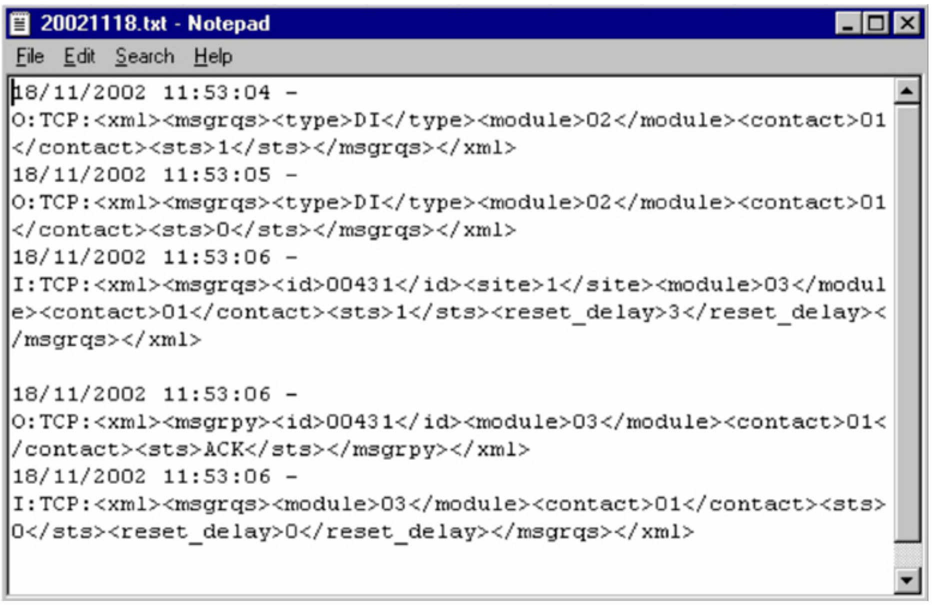
Name	Size	Type	Modified
20021101.txt	333 KB	Text Document	11/1/2002
20021102.txt	342 KB	Text Document	11/3/2002
20021103.txt	341 KB	Text Document	11/4/2002
20021104.txt	332 KB	Text Document	11/4/2002
20021105.txt	341 KB	Text Document	11/6/2002
20021106.txt	337 KB	Text Document	11/6/2002
20021107.txt	353 KB	Text Document	11/8/2002
20021108.txt	340 KB	Text Document	11/9/2002
20021109.txt	333 KB	Text Document	11/9/2002
20021110.txt	341 KB	Text Document	11/11/2002
20021111.txt	338 KB	Text Document	11/11/2002
20021112.txt	336 KB	Text Document	11/13/2002
20021113.txt	342 KB	Text Document	11/14/2002
20021114.txt	329 KB	Text Document	11/14/2002
20021115.txt	144 KB	Text Document	11/15/2002

15 object(s) (Disk free space: 468 MB) 4.75 MB My Computer

Figure 53: Log file location

The Table eKERNEL_SITE defines the directory where the log files are stored, and the number of days that the files are retained.

The information in the log files is stored in XML format, as shown in Figure 54: IO Module log file on page 157.



```
18/11/2002 11:53:04 -
O:TCP:<xml><msgrqs><type>DI</type><module>02</module><contact>01
</contact><sts>1</sts></msgrqs></xml>
18/11/2002 11:53:05 -
O:TCP:<xml><msgrqs><type>DI</type><module>02</module><contact>01
</contact><sts>0</sts></msgrqs></xml>
18/11/2002 11:53:06 -
I:TCP:<xml><msgrqs><id>00431</id><site>1</site><module>03</modul
e><contact>01</contact><sts>1</sts><reset_delay>3</reset_delay><
/msgrqs></xml>

18/11/2002 11:53:06 -
O:TCP:<xml><msgrpy><id>00431</id><module>03</module><contact>01<
/contact><sts>ACK</sts></msgrpy></xml>
18/11/2002 11:53:06 -
I:TCP:<xml><msgrqs><module>03</module><contact>01</contact><sts>
0</sts><reset_delay>0</reset_delay></msgrqs></xml>
```

Figure 54: IO Module log file

Figure 54: IO Module log file on page 157 shows the contents of a log file for the IO module. The subsequent XML strings are the result of pressing a button on the DI module, module 02, contact 01. As result of pressing this button, contact 01 is activated on the Digital Output module 03 for three seconds.

The following is an analysis of the first line in Figure 54: IO Module log file on page 157:

- `18/11/2002 11:53:04 -`

  The date and time

- O:TCP

  This string indicates message direction and protocol. In this case an outgoing XML string using TCP/IP. Outgoing means that the information goes from this module to another module (generally the eKERNEL). If the message is incoming into the module, the following is displayed: I:TCP.

- <xml> ...... </xml>

  These tags enclose xml content. <xml> marks the start, while <xml> marks the end.

- <msgrqs> .... </msgrqs>

  This tag indicates that this is a message request. If the line is <msgrpy> .... </msgrpy>, the xml string is a reply to a previous request.

- <type>DI</type>

  This tag indicates the type of message, which indicates that the message was generated by the Digital Input contact.

- <module>02</module>

This tag specifies from which module the message comes. In Figure 54: IO Module log file on page 157, the message comes from the second module.

- <contact>01</contact>

  This tag indicates the contact on the IO module.

- <sts>1</sts>

  This tag indicates the contact status. 1 means that the contact was activated.

In the file shown in Figure 54: IO Module log file on page 157, the following messages have been exchanged between the eIO module and the eKERNEL for each line:

1. 18/11/2002 11:53:04 - O:TCP:<xml><msgrqs>type>DI</ type><module>02</ module><contact>01</contact><sts>1</sts></msgrqs></xml>

   An outgoing message request from eIO to eKERNEL. Contact 01 on module 02 has been activated. (The input module is type DI.)

2. 18/11/2002 11:53:05 - O:TCP:<xml><msgrqs><type>DI</ type><module>02</ module><contact>01</contact><sts>0</sts></msgrqs></xml>

   An outgoing message request from eIO to eKERNEL. Contact 01 on module 02 has been de-activated. (The input module is type DI.)

3. 18/11/2002 11:53:06 - I:TCP<:xml><msgrqs><id>00431</ id><site>1</ site>module>03</module><contact>01</ contact><sts>1</sts><reset_delay>3</ reset_delay></msgrqs></xml>

   An incoming message request in eIO from eKERNEL. Command to activate contact 01 on module 03 for a time period of 3 seconds. (Message identifier 00431.)

4. 18/11/2002 11:53:06 - O:TCP:<xml><msgrpy><id>00431</ id><module>03</ module><contact>01</contact><sts>ACK</sts></msgrpy></xml>

   An outgoing message reply from eIO to eKERNEL as an acknowledge (ACK) on message request in line 3. (Message identifier 00431.)

5. 18/11/2002 11:53:06 - I:TCP:<xml><msgrqs><module>03</ module><contact>01</contact><sts>0</sts><reset_delay>0</ reset_delay></ msgrqs></xml>

   An incoming message in eIO from eKERNEL to reset the contact 01 in module 03.

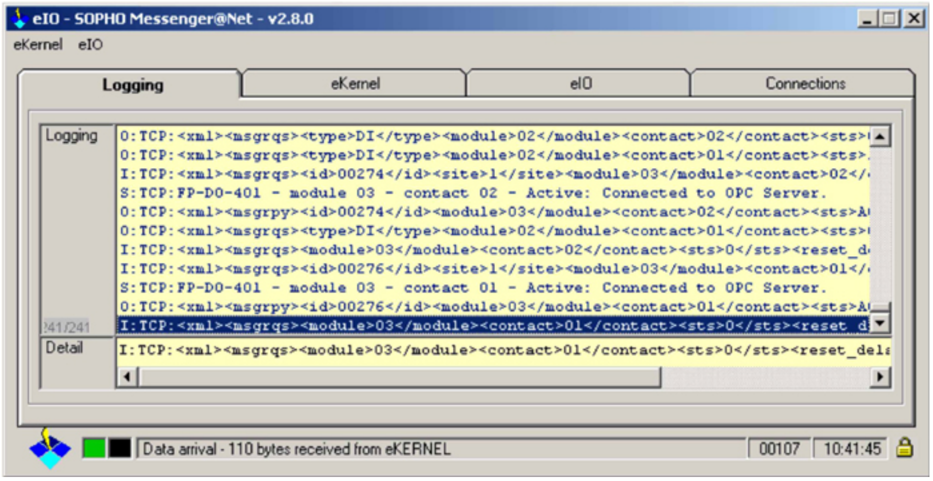
Module Window

Each module runs as an application in the Windows environment, and can be displayed as an open window, or minimized on the Windows Task bar. The module window provides online information about settings, commands/messages/communication. This information is very useful for debugging. The eIO module is shown for the purposes of demonstration; other modules have a similar interface, however, the information displayed is unique in each application.

If the eIO Module window is minimized, maximize it. Four tabs are visible in the window, as follows:

- Logging Tab

  In the logging tab, the online log information is provided.



```
O:TCP:<xml><msgrqs><type>DI</type><module>02</module><contact>02</contact><sts>
O:TCP:<xml><msgrqs><type>DI</type><module>02</module><contact>01</contact><sts>
I:TCP:<xml><msgrqs><id>00274</id><site>1</site><module>03</module><contact>02</
S:TCP:FP-DO-401 - module 03 - contact 02 - Active: Connected to OPC Server.
O:TCP:<xml><msgrpy><id>00274</id><module>03</module><contact>02</contact><sts>A
O:TCP:<xml><msgrqs><type>DI</type><module>02</module><contact>01</contact><sts>
I:TCP:<xml><msgrqs><module>03</module><contact>02</contact><sts>0</sts><reset_d
I:TCP:<xml><msgrqs><id>00276</id><site>1</site><module>03</module><contact>01</
S:TCP:FP-DO-401 - module 03 - contact 01 - Active: Connected to OPC Server.
O:TCP:<xml><msgrpy><id>00276</id><module>03</module><contact>01</contact><sts>A
I:TCP:<xml><msgrqs><module>03</module><contact>01</contact><sts>0</sts><reset_d
```

```
I:TCP:<xml><msgrqs><module>03</module><contact>01</contact><sts>0</sts><reset_del
```

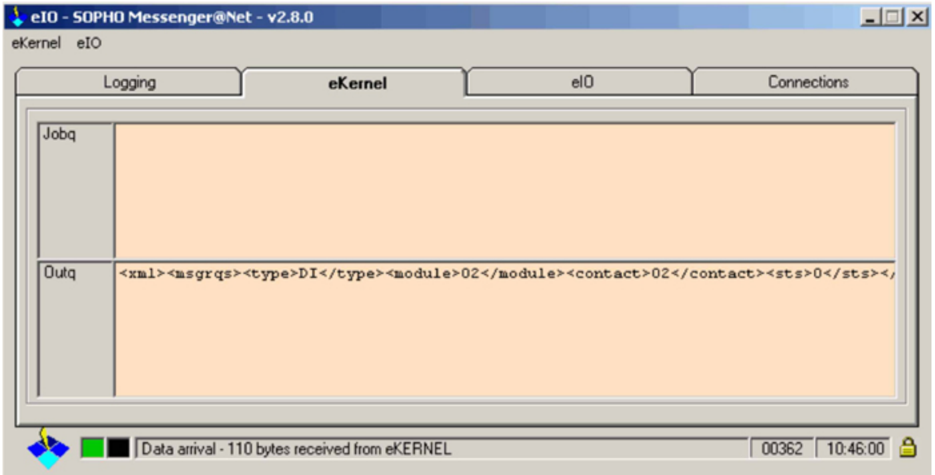
Data arrival - 110 bytes received from eKERNEL

Figure 55: Logging Tab

  There are two logging panes, the upper, called **Logging**, and the lower, called **Detail**. In the **Logging** pane, the XML messages are shown. These are the same as the messages in the log files. However, the lines do not fit in the window. If you need detailed information (the whole line) you can left-lick the line to display it in the Detail pane. There you can scroll from left to right, to see all the information in the line.

- eKERNEL Tab

  The **eKERNEL** tab shows the communication between the module and the eKERNEL.



```
<xml><msgrqs><type>DI</type><module>02</module><contact>02</contact><sts>0</sts></
```

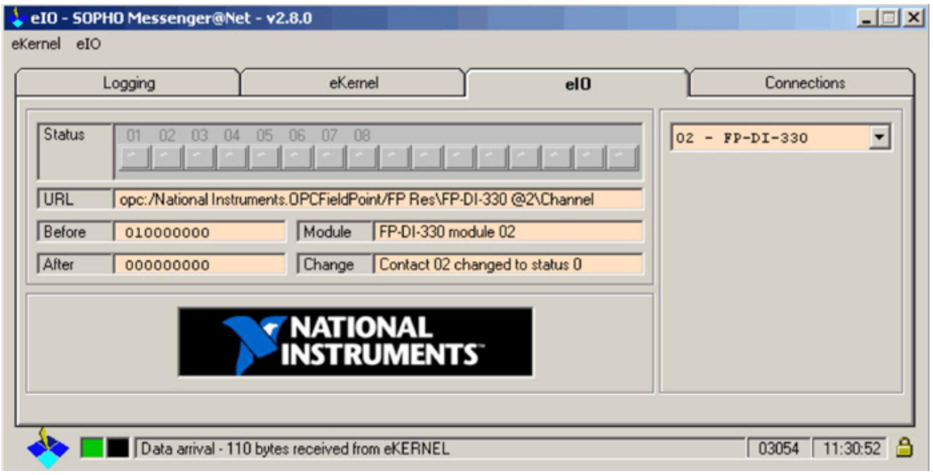
Data arrival - 110 bytes received from eKERNEL | 00362 | 10:46:00

Figure 56: eKERNEL Tab

The **Jobq** pane shows the pending jobs for the module. In the **Outq** pane, the outgoing communication from the module is shown.

- eIO Tab

The **eIO** tab shows IO module specific information.



URL: opc:/National Instruments.OPCFieldPoint/FP Res\FP-DI-330 @2\Channel

Before: 010000000 | Module: FP-DI-330 module 02

After: 000000000 | Change: Contact 02 changed to status 0

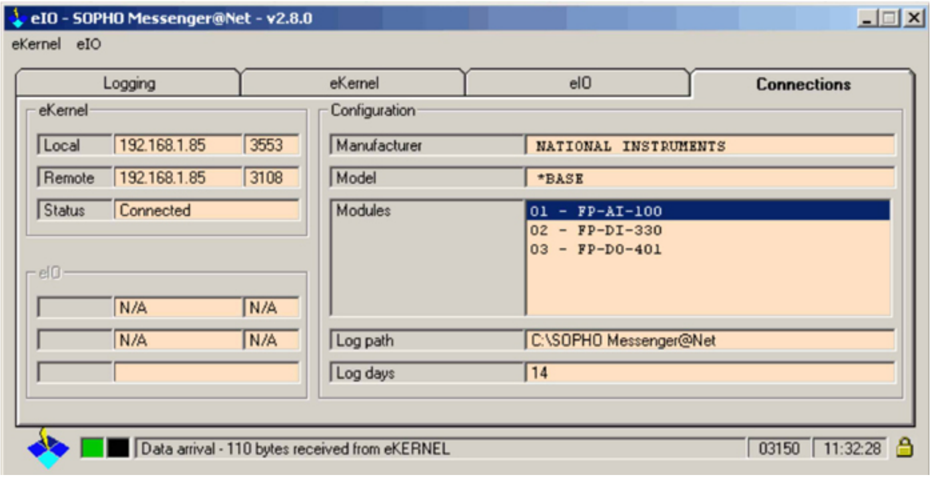
02 - FP-DI-330

Data arrival - 110 bytes received from eKERNEL | 03054 | 11:30:52

Figure 57: eIO Tab

- Connections Tab

The **Connections** tab shows information on the connections between the eIO module and the eKERNEL. This tab also shows information on the connections between the external part and the eIO module itself.



eKernel

Local	192.168.1.85	3553
Remote	192.168.1.85	3108
Status	Connected	

eIO

	N/A	N/A
	N/A	N/A

Configuration

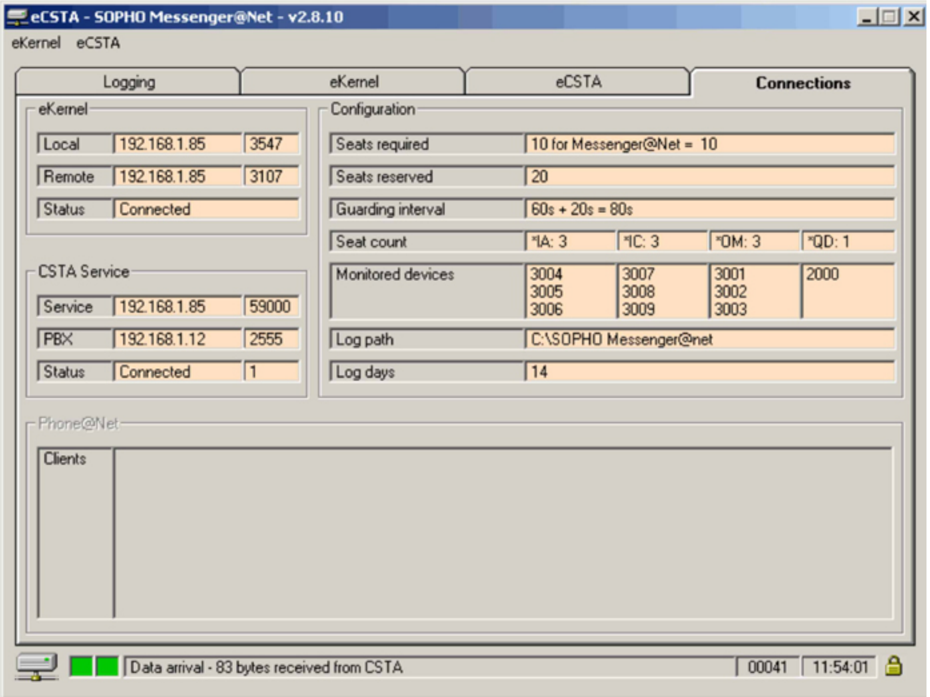
Manufacturer	NATIONAL INSTRUMENTS
Model	*BASE
Modules	01 - FP-AI-100 02 - FP-DI-330 03 - FP-DO-401
Log path	C:\SOPHO Messenger@Net
Log days	14

Data arrival - 110 bytes received from eKERNEL | 03150 | 11:32:28

Figure 58: Connections Tab

The right pane gives information about the external devices that are connected to the eIO Module. The left pane shows information about the TCP/IP connections. The connections between the eKERNEL and the eIO module are shown in the top part of the left pane. The connections between the IO module and (if applicable) an external device are shown in the bottom part of the left pane. The TCP/IP connections that are shown comprise the local and remote IP address with the port number that is used for this socket.

Figure 58: Connections Tab on page 161 shows only one TCP/IP connection between the eIO module and the eKERNEL. If another TCP/IP connection is available, the bottom part of the left pane is filled in.



eKernel

Local	192.168.1.85	3547
Remote	192.168.1.85	3107
Status	Connected	

CSTA Service

Service	192.168.1.85	59000
PBX	192.168.1.12	2555
Status	Connected	1

Configuration

Seats required	10 for Messenger@Net = 10			
Seats reserved	20			
Guarding interval	60s + 20s = 80s			
Seat count	*IA: 3	*IC: 3	*OM: 3	*QD: 1
Monitored devices	3004 3005 3006	3007 3008 3009	3001 3002 3003	2000
Log path	C:\SOPHO Messenger@net			
Log days	14			

Clients

Data arrival - 83 bytes received from CSTA | 00041 | 11:54:01

Figure 59: Status lamps

In the bottom part of the left pane, two lamps are visible, indicating the status of the TCP/IP connection. The left lamp indicates the status of the connection between the IO module and the eKERNEL. The right lamp indicates the TCP/IP status between the IO module and the external device (if applicable). Both are green in Figure 59: Status lamps on page 162. There are three possible colors for these lamps:

- Green

TCP/IP connection (socket) is opened without errors.

- Red

Indicating an error in trying to open the socket (TCP/IP connection).

- Black

Not applicable, because there is no TCP/IP connection specified.

To find out which TCP/IP ports are in use by Windows services, you can display the contents of the services file using an ASCII editor. You can find the services file in the following directory:

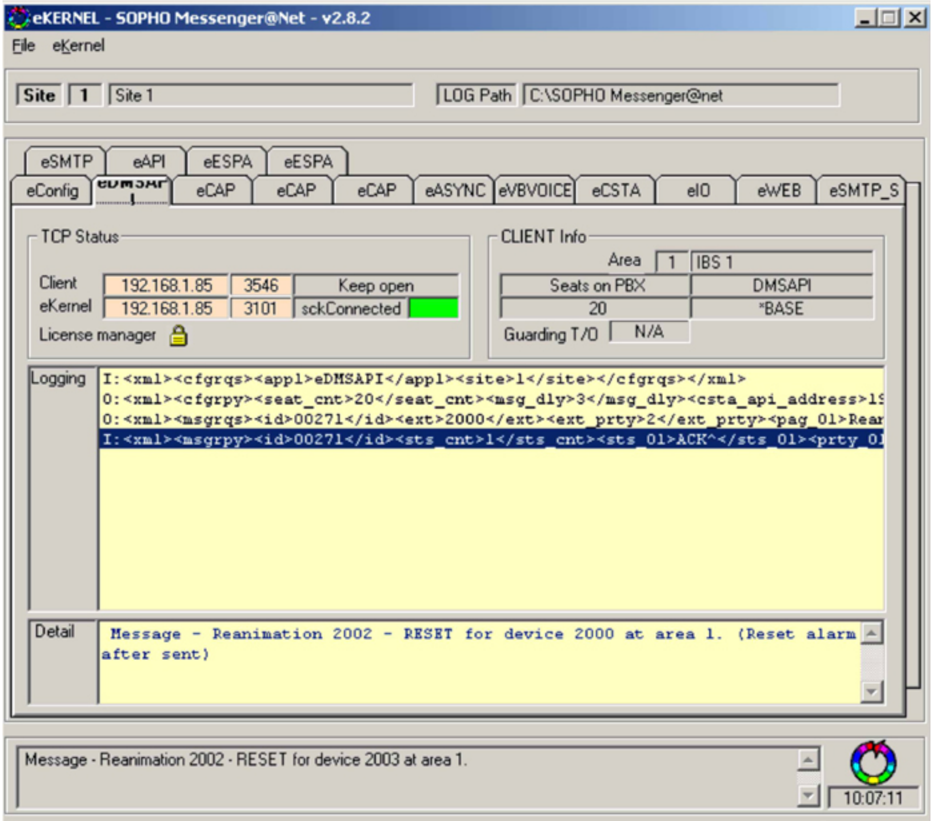
c:\WINNT\system32\drivers\etc\services

Note:

The file does not have a file extension.

eKERNEL Window

The window of the eKERNEL differs from the other modules, and has a tab for each individual module.



Site 1 Site 1 | LOG Path C:\SOPHO Messenger@net

Client	192.168.1.85	3546	Keep open
eKernel	192.168.1.85	3101	sckConnected 🟩
License manager			

Area 1 IBS 1

Seats on PBX	DMSAPI
20	*BASE
Guarding T/O	N/A

```
I:<xml><cfgrqs><appl>eDMSAPI</appl><site>1</site></cfgrqs></xml>
O:<xml><cfgrpy><seat_cnt>20</seat_cnt><msg_dly>3</msg_dly><csta_api_address>19
O:<xml><msgrqs><id>00271</id><ext>2000</ext><ext_prty>2</ext_prty><pag_01>Rean
I:<xml><msgrpy><id>00271</id><sts_cnt>1</sts_cnt><sts_01>ACK^</sts_01><prty_01
```

```
Message - Reanimation 2002 - RESET for device 2000 at area 1. (Reset alarm
after sent)
```

Message - Reanimation 2002 - RESET for device 2003 at area 1.

10:07:11

Figure 60: eKERNEL module window

Select a module tab to see the information for that specific module, as follows:

- TCP status. Shows the connection data for the TCP/IP connection between the eKERNEL and the module.
- Client information Shows information about the module.
- Logging. Shows the logged communication between the eKERNEL and the module.
- Detail. Shows communication. As well, if you left-click a line in the logging pane, you can see the whole line displayed in the Detail window.
- Module tab. At the right side of the logging tab, this lists the jobs that are waiting to be executed.

The bottom of the eKERNEL window shows all the commands going to or coming from the eKERNEL.

Simulation Options in a Module

You can use a simulation menu in modules to simulate an message. The simulation is different for each individual module, because the nature of the modules differ. Figure 61: Accessing Simulate Options on page 164 shows you how to access the simulation menu.

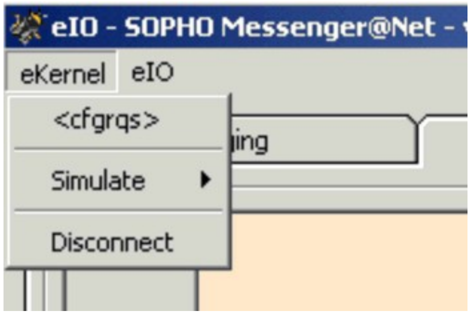


Figure 61: Accessing Simulate Options

eKERNEL Service Options

As shown in Figure 62: Accessing Reset all alarms on page 164, eKERNEL offer the following service options:

- Reset All Alarms

  The menu item **eKERNEL > Reset All Alarms** clears all alarms in DECT Messenger.

- Refresh Logfile

  The menu item **eKERNEL > Refresh Logfile** stores the latest log information in the eKERNEL log file.

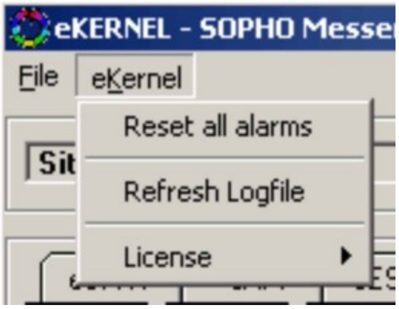


Figure 62: Accessing Reset all alarms

Index