Nortel Communication Server 1000

Nortel Communication Server 1000 Release 4.5

DECT

Description, Planning, Installation, and Operation

Document Number: 553-3001-370
Document Release: Standard 5.00
Date: January 2006

Produced in Canada

Information is subject to change without notice. Nortel Networks reserves the right to make changes in design or components as progress in engineering and manufacturing may warrant.

Revision history

January 2006

Standard 5.00. This document is up-issued to include updated information on external basestation housing, DECT Messenger OS information, and OTM software upgrades.

August 2005

Standard 4.00. This document is up-issued for Communication Server 1000 Release 4.5.

April 2005

Standard 3.00. This document is up-issued for Communication Server 1000 Release 4.0. DECT Messenger documentation added.

September 2004

Standard 2.00. This document is up-issued for Communication Server 1000 Release 4.0.

October 2003

Standard 1.00. This document is a new NTP for Succession 3.0. It was created to support a restructuring of the Documentation Library, which resulted in the merging of multiple legacy NTPs. This new document consolidates information previously contained in the following legacy documents, now retired:

- DECT *Site Planning* (553-3601-101)
- DECT *Provisioning* (553-3601-102)
- DECT *Overview* (553-3601-103)
- DECT *Installation* (553-3601-203)
- DECT *Operation* (553-3601-301)

Contents

System administration 439

List of Figures

List of Procedures

How to get help

This chapter explains how to get help for Nortel products and services.

Getting help from the Nortel web site

The best way to get technical support for Nortel products is from the Nortel Technical Support web site:

www.nortel.com/support

This site provides quick access to software, documentation, bulletins, and tools to address issues with Nortel products. From this site, you can:

- download software, documentation, and product bulletins
- search the Technical Support Web site and the Nortel Knowledge Base for answers to technical issues
- sign up for automatic notification of new software and documentation for Nortel equipment
- open and manage technical support cases

Getting help over the telephone from a Nortel Solutions Center

If you do not find the information you require on the Nortel Technical Support web site, and you have a Nortel support contract, you can also get help over the telephone from a Nortel Solutions Center.

In North America, call 1-800-4NORTEL (1-800-466-7835).

Outside North America, go to the following web site to obtain the telephone number for your region:

www.nortel.com/callus

Getting help from a specialist by using an Express Routing Code

To access some Nortel Technical Solutions Centers, you can use an Express Routing Code (ERC) to quickly route your call to a specialist in your Nortel product or service. To locate the ERC for your product or service, go to:

www.nortel.com/erc

Getting help through a Nortel distributor or reseller

If you purchased a service contract for your Nortel product from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller.

About this document

This document is a global document. Contact your system supplier or your Nortel representative to verify that the hardware and software described are supported in your area.

Subject

This document describes the Nortel Integrated Digital Enhanced Cordless Technologies (DECT) system and explains how to plan, install, and operate DECT.

Note on legacy products and releases

This NTP contains information about systems, components, and features that are compatible with Nortel Communication Server 1000 Release 4.5 software. For more information on legacy products and releases, click the **Technical Documentation** link under **Support** on the Nortel home page:

http://www.nortel.com

Applicable systems

This document applies to the following systems:

- Communication Server 1000S (CS 1000S)
- Communication Server 1000M Chassis (CS 1000M Chassis)
- Communication Server 1000M Cabinet (CS 1000M Cabinet)
- Communication Server 1000M Half Group (CS 1000M HG)
- Communication Server 1000M Single Group (CS 1000M SG)

- Communication Server 1000M Multi Group (CS 1000M MG)
- Communication Server 1000E (CS 1000E)
- Meridian 1 PBX 11C Chassis (Meridian 1 PBX 11C Chassis)
- Meridian 1 PBX 11C Cabinet (Meridian 1 PBX 11C Cabinet)
- Meridian 1 PBX 51C
- Meridian 1 PBX 61C
- Meridian 1 PBX 61C CP PII
- Meridian 1 PBX 81
- Meridian 1 PBX 81C
- Meridian 1 PBX 81C CP PII

Note: When upgrading software, memory upgrades are sometimes required on the Signaling Server, the Call Server, or both.

System migration

When particular Meridian 1 systems are upgraded to run CS 1000 Release 4.0 software and configured to include a Signaling Server, they become CS 1000M systems. Table 1 lists each Meridian 1 system that supports an upgrade path to a CS 1000M system.

Table 1
Meridian 1 systems to CS 1000M systems (Part 1 of 2)

This Meridian 1 system...	Maps to this CS 1000M system
Meridian 1 PBX 11C Chassis	CS 1000M Chassis
Meridian 1 PBX 11C Cabinet	CS 1000M Cabinet
Meridian 1 PBX 51C	CS 1000M Half Group
Meridian 1 PBX 61C	CS 1000M Single Group
Meridian 1 PBX 61C CP PII	CS 1000M Single Group
Meridian 1 PBX 81	CS 1000M Multi Group

Table 1
Meridian 1 systems to CS 1000M systems (Part 2 of 2)

This Meridian 1 system...	Maps to this CS 1000M system
Meridian 1 PBX 81C	CS 1000M Multi Group
Meridian 1 PBX 81C CP PII	CS 1000M Multi Group

For more information, see one or more of the following NTPs:

- *Communication Server 1000M and Meridian 1: Small System Upgrade Procedures* (553-3011-258)
- *Communication Server 1000M and Meridian 1: Large System Upgrade Procedures* (553-3021-258)

Communication Server 1000S: Upgrade Procedures (553-3031-258)

Intended audience

This document is intended for sales representatives, planners, installers, site maintenance personnel, and administrators.

Conventions

Terminology

In this document, the following systems are referred to generically as system:

- Communication Server 1000S (CS 1000S)
- Communication Server 1000M (CS 1000M)
- Communication Server 1000E (CS 1000E)
- Meridian 1

The following systems are referred to generically as Small System:

- Communication Server 1000M Chassis (CS 1000M Chassis)
- Communication Server 1000M Cabinet (CS 1000M Cabinet)

- Meridian 1 PBX 11C Chassis (Meridian 1 PBX 11C Chassis)
- Meridian 1 PBX 11C Cabinet (Meridian 1 PBX 11C Cabinet)

The following systems are referred to generically as Large System:

- Communication Server 1000M Half Group (CS 1000M HG)
- Communication Server 1000M Single Group (CS 1000M SG)
- Communication Server 1000M Multi Group (CS 1000M MG)
- Meridian 1 PBX 51C
- Meridian 1 PBX 61C
- Meridian 1 PBX 61C CP PII
- Meridian 1 PBX 81
- Meridian 1 PBX 81C
- Meridian 1 PBX 81C CP PII

Caution, Danger, Warning tables

These tables are strategically placed in this document to advise the reader of potential hazards. A brief description in provided within each of the following tables.

DANGER — Electric Shock

Advises of the risk of a serious injury or death caused by an electric shock.

DANGER — Electrostatic Sensitive Device

Advises of a procedure that can result in equipment damage due to ElectroStatic Discharge (ESD).

DANGER — Serious Injury

Advises of the risk of a serious injury or death caused by an immediate hazard.

CAUTION — Data Loss

Advises of a procedure that can result in a loss of data.

CAUTION — Equipment Damage

Advises of a procedure that can result in equipment damage.

CAUTION — Service Interruption

Advises of a procedure that can result in an interruption of service.

WARNING — Personal Injury

Advises of the risk of a minor or moderate injury caused by an immediate hazard.

Step Action table

Procedures in this document are contained in Step Action tables. The following example explains how a procedure is arranged in this table format.

Table 2
A Sample Step Action table

Step	Action
1	This portion of the step action table details the required step.
	This portion of the step action table details the action to carry out the above step.
2	This portion of the step action table details the required step.
	This portion of the step action table details the action to carry out the above step.

END

Related information

This section lists information sources that relate to this document.

NTPs

The following NTPs are referenced in this document:

- *Telephony Manager: System Administration* (553-3001-330)
- *Communication Server 1000M and Meridian 1: Small System Installation and Configuration* (553-3011-210)
- *Communication Server 1000M and Meridian 1: Large System Installation and Configuration* (553-3021-210)
- *Communication Server 1000S: Installation and Configuration* (553-3031-210)
- *DECT Programming and Provisioning Record* (553-3601-250)

Online

To access Nortel documentation online, click the **Technical Documentation** link under **Support** on the Nortel home page:

http://www.nortel.com

CD-ROM

To obtain Nortel documentation on CD-ROM, contact your Nortel customer representative.

Product description

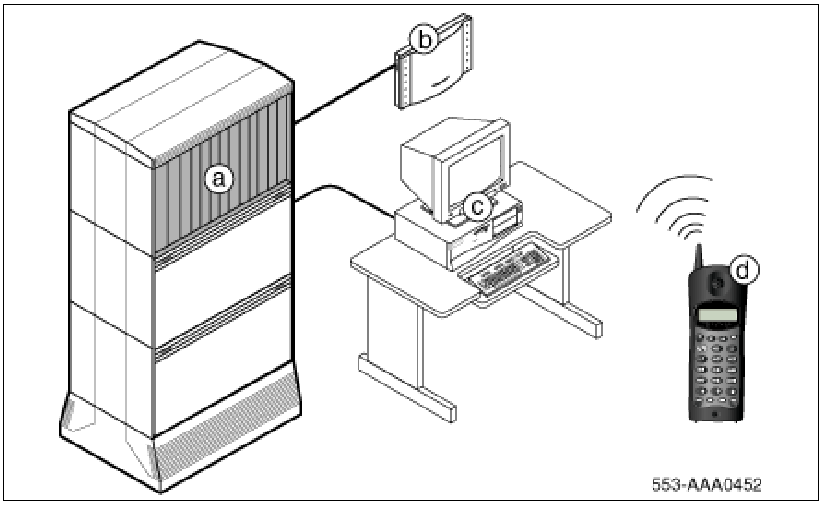
Contents

This section contains information on the following topics:

Overview

Nortel Integrated DECT (DECT) allows users to move freely about their work sites while conducting telephone conversations using wireless handsets. DECT is an acronym for Digital Enhanced Cordless Telecommunications.

Figure 1
Main parts of the DECT system



The DECT system is in a Large System IPE shelf or a Small System cabinet or chassis. DECT has four main components:

- **a** DECT mobility cards
- **b** Basestation
- **c** Handsets
- **d** Optivity Telephony Manager (OTM) with DECT application

Clock requirements

The following clock controller cards are mandatory:

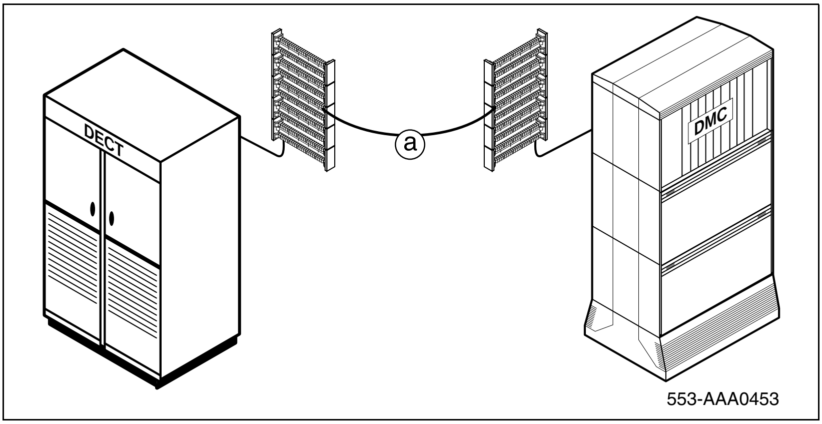
- NTRB53 Clock Controller card for a Large System
- NTAK20BD Clock Controller daughterboard or NTAK79AA card with a built-in clock controller for a Small System

If there is no digital connection to the network, the appropriate clock controller must be installed and operated in free run mode.

Note: On EMC-hardened Cabinet systems, the clock controller must be in one of the first three slots of the CPU cabinet.

Synchronization port

Figure 2
DECT synchronization

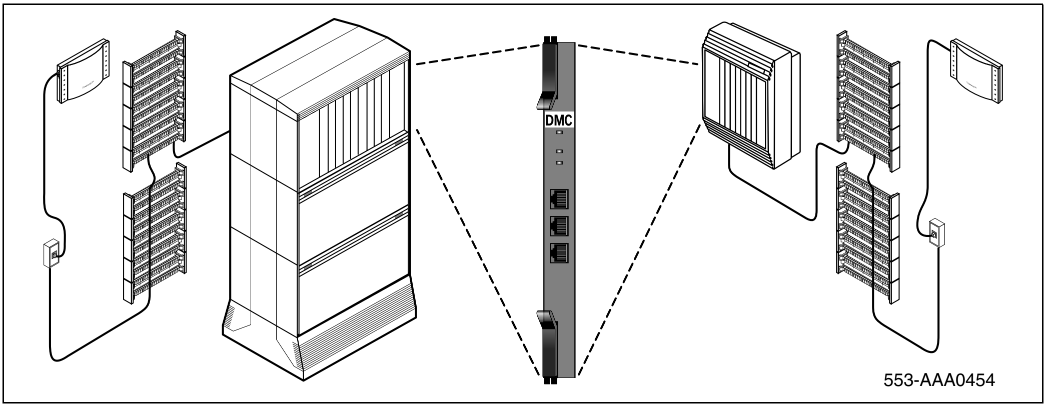


Where multiple DECT systems share the same radio coverage area, the DECT synchronization port must be used. The DECT synchronization port is accessed through a Main Distribution Frame (MDF) connection. Failure to connect the DECT synchronization ports of each system can lead to service interruptions.

Mobility card (DMC8)

The NTCW00xx DMC8 DECT Mobility Card provides an interface between the basestations and the Meridian 1, CS 1000M, or CS 1000S.

Figure 3
DECT Mobility Card



The DECT system supports a mix of DMCs and DMC8s. A DMC8 supports up to eight basestations.

All DMC8s support a Point-to-Point Protocol (PPP) connection to the DECT Manager with an NTCW12DA cable. The DMC8 card requires a NTCW25AA DECT Manager Ethernet (DME) daughterboard installed to support an Ethernet connection.

Each DMC8 is programmed in the database using LD 10.

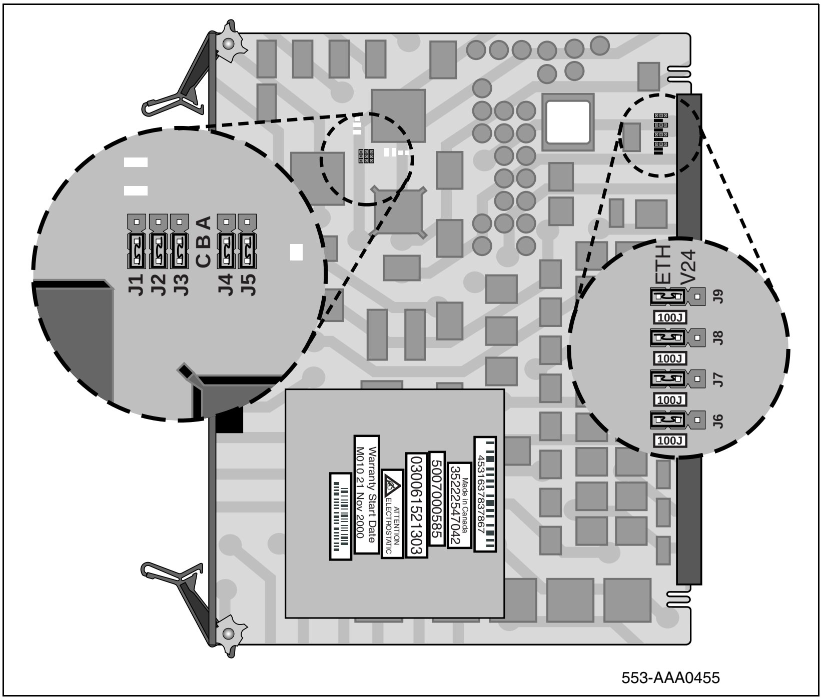
The DMC8s are interconnected by faceplate cables, allowing them to pass information to each other.

DMC8s must be in an IPE shelf or in a cabinet or chassis.

There is no call switching in the DMC8 card. All call switching occurs within the Meridian 1, CS 1000M, or CS 1000S.

DMC8 options

Figure 4
DMC8 options



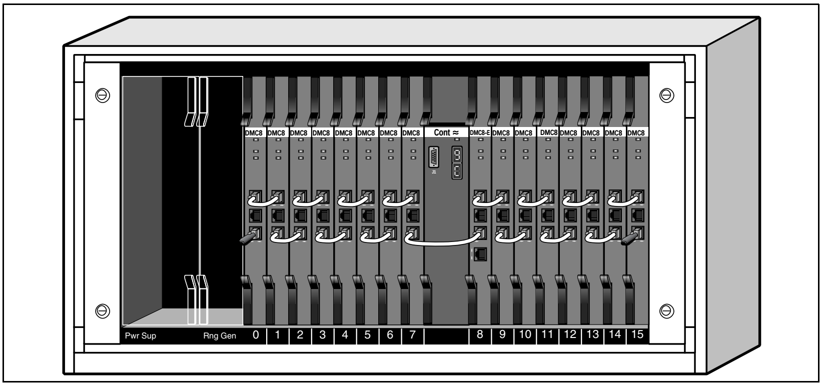
The component side of the DMC8 contains jumpers J1, J2, and J3. The jumpers indicate card status.

DMC8 – Expander (DMC8-E)

The NTCW01xx DMC8-E DECT Mobility Card – Expander provides the same functions as a DMC card.

The DMC8-E has additional circuitry required to regenerate faceplate cable signals when a system contains more than eight DMC8s. The DMC8-E connects two shelves or cabinets in a DECT system.

Figure 5
DECT Mobility Card – Expander



If the DMC8-E is used in an IPE module, and must be located in card slot 8. Do not install a DMC8 in slot 8 of an IPE module.

If the DMC8-E is used in an Small System cabinet or chassis, and must be located in card slot 9, 19 or 29. Do not install a DMC8 in slot 9, 19 or 29 of a Small System cabinet or chassis.

An NTCW25AA DME daughterboard is required to provide Ethernet OTM access. The daughterboard is also required to enable DECT Messaging. The DME daughterboard is not required for serial OTM access. Only one DME daughterboard is required per system.

Faceplate features

Figure 6 on page 97 shows the following DMC8 and DMC8-E faceplate features:

a Red LED (indicates the same status as all IPE cards)

b Yellow LED (indicates DECT sub-system status)

c Green LED (indicates DECT sub-system status)

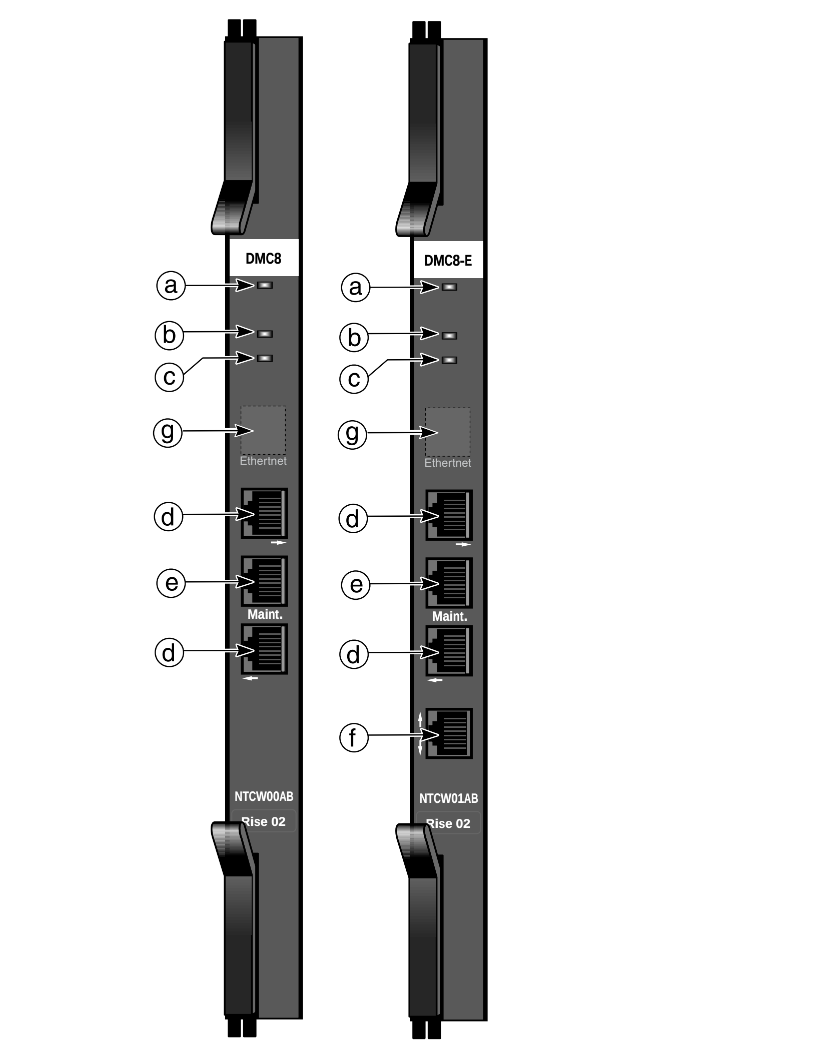
d DMC8 to DMC8 faceplate cable port

e DMC8 bypass faceplate cable port

f DMC8-E to DMC8-E faceplate cable port

g For future use

Figure 6
DMC8 and DMC8-E faceplate features



Faceplate cables

The faceplate cables form the 20 Mb/s bus that connects all DMCs. The faceplate cables meet the standard for Unshielded Twisted-Pair category of performance 5 (UTP Cat 5).

Signalling and PCM are sent to all DMCs over the faceplate cables, allowing a DMC8 to pass a call to another DMC8.

The cables shown in Figure 7 on page 99 are as follows:

a DMC8 to DMC8 faceplate cable

b DMC8 to DMC8-E faceplate cable

c DMC8 faceplate termination

d DMC8 bypass faceplate cable

The DMC8 to DMC8 cable extends the 20Mb/s bus to all DMCs.

The DMC8 to DMC8-E cable extends the 20Mb/s bus past the XPEC card in the IPE shelf.

The DMC8 faceplate termination balances the impedance at either end of the 20Mb/s bus.

The DMC8 bypass faceplate cable bypasses DMC8s to be inserted in or removed from an operational system. The DMC8 bypass faceplate cable is shown in Figure 7 on cards 10 and 12.

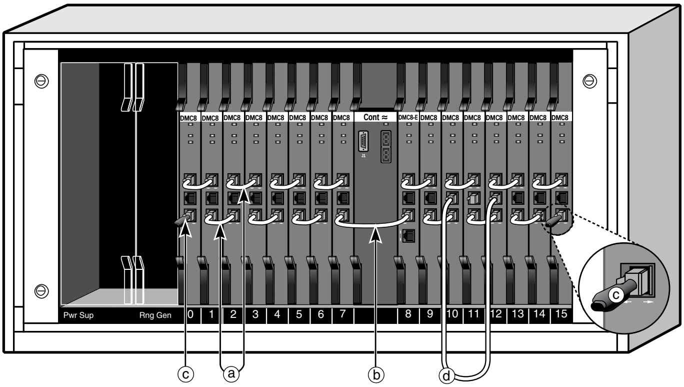
The DMC8-E to DMC8-E faceplate cable connects two shelves or two cabinets. The DMC8-E to DMC8-E faceplate cable is shown in Figure 9 on page 101.

The faceplate cabling layout plan must specify that the DMC8 to DMC8-E cable connects into the ports as shown in Figure 7 on page 99.

CAUTION — Service Interruption

Customers must use UTP Cat 5 faceplate cables supplied by Nortel. Faceplate termination must be used on the DMCs at both ends of the faceplate cabling.

Figure 7
Faceplate cables



Inter-shelf or cabinet faceplate connections

CAUTION — Service Interruption

The DMC8-E to DMC8-E faceplate cable has four sets of movable ferrites. The position of the ferrites on the cable is important. See Figure 8. Each end of the cable must have a group of 20 ferrites. One quarter the distance from each end of the cable must have a group of 10 ferrites. The maximum length of the cable is 1.5 metres, limiting the position of DECT shelves 0 and 1 to adjacent IPE modules or Small System cabinets/chassis.

Figure 8
Cable ferrites

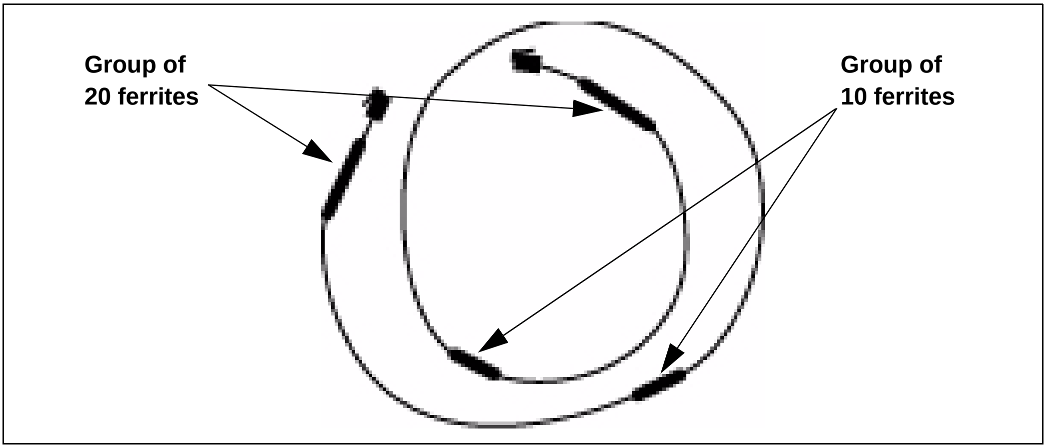


Figure 9 shows the following:

a DECT shelf 0

b DECT shelf 1

c DMC8-E to DMC8-E faceplate cable connection between DMC8-Es on DECT IPE shelves

Figure 9
IPE inter-shelf faceplate connections

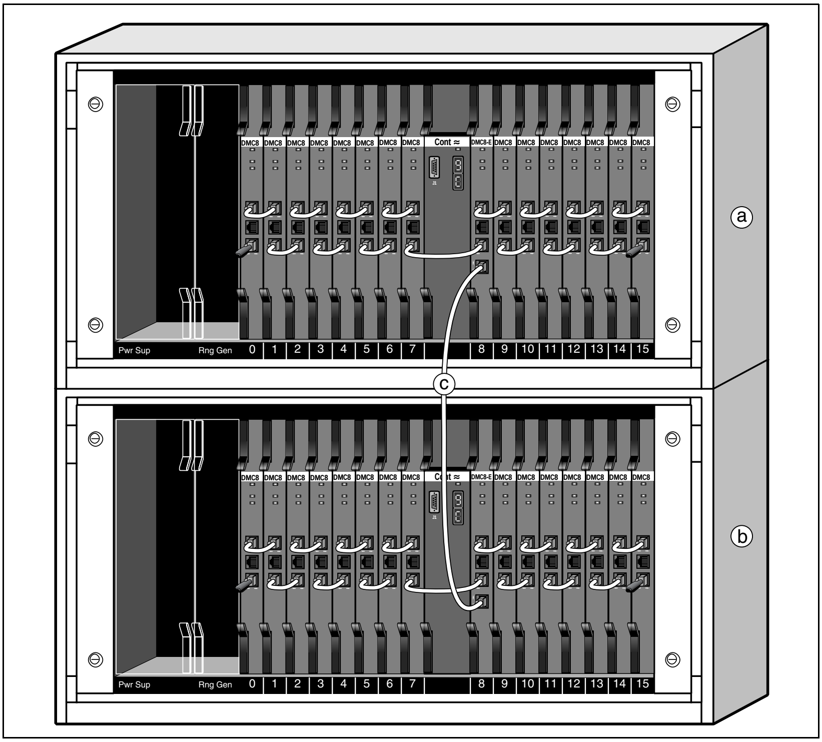
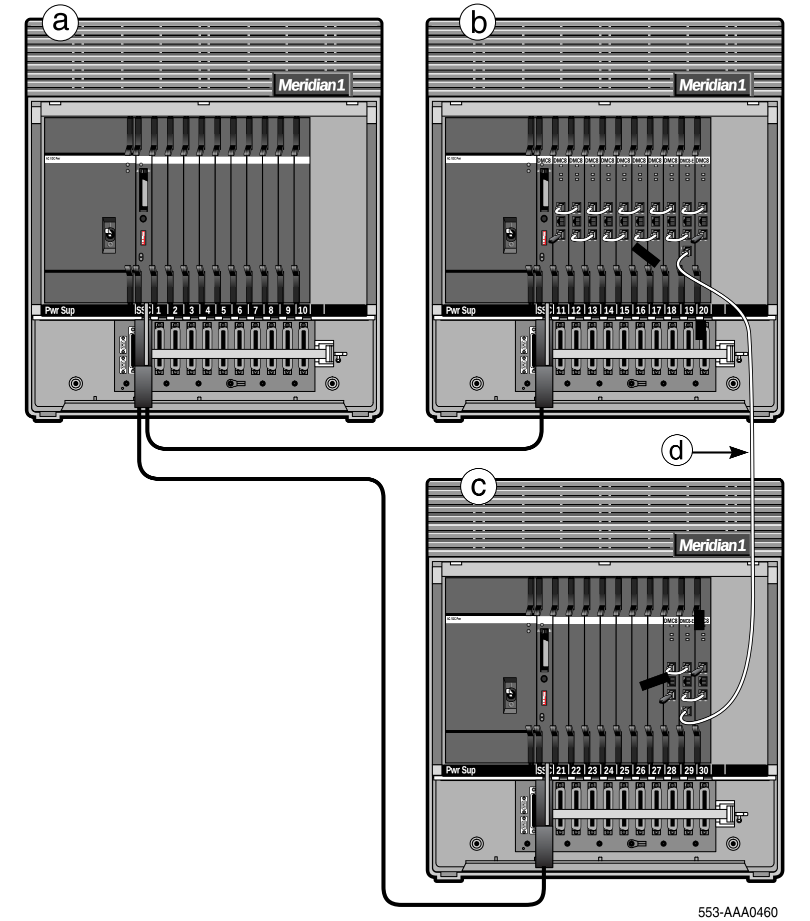


Figure 10 shows the following:

- **a** Main cabinet
- **b** Expansion cabinet
- **c** Second expansion cabinet
- **d** DMC8-E to DMC8-E faceplate cable connection between the DMC8-Es on the first and second cabinets

Figure 10
Inter-cabinet faceplate connections



553-AAA0460

Basestations

There are three basestation models available:

- C4600 – supports six active call radio links
- C4610 – supports 12 active call radio links
- C4610E (with external antenna) – supports 12 active call radio links

Basestations are IP40-compliant wall-mounted transceivers that provide digital radio links to handsets.

> **CAUTION — Service Interruption**
>
> For maximum line length before signal degradation occurs, use UTP Cat 5 cabling between the basestation and the shelf or cabinet. If the line length exceeds 100 ohms for the 4610 basestation, an external power supply must be used. The maximum distance when using external power with UTP Cat 5 cabling is approximately 1.7 km.

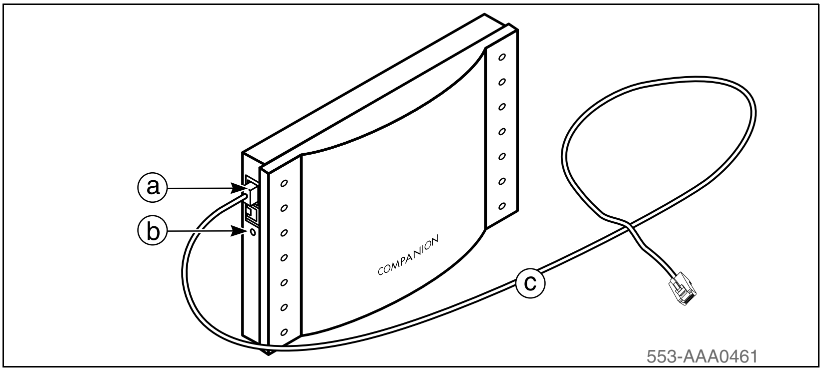
The basestation has the following features:

- RJ45 socket connection to a one meter UTP Cat 5 cable
- RJ45 socket connection to an external or local power supply
- Green LED (C4600) or a yellow LED (C4610), indicates synchronization to its DMC8
- One meter UTP Cat 5 cable connected through an RJ45 Connect Box and MDF to an IPE I/O panel or Small System cabinet I/O panel

Two sources can power the basestation:

- The DMC8 and DMC8-E feeding phantom power over the UTP Cat 5 cable signaling pairs, connected to (a) in Figure 11 on page 104
- A local power supply, connected to (b) in Figure 11 on page 104

Figure 11
Basestation



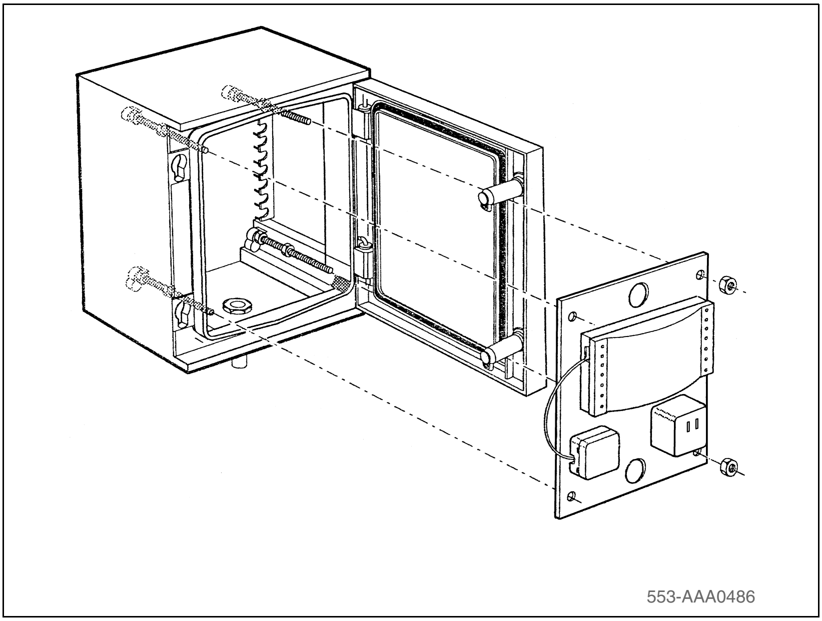
Basestations connected to a DMC8 or DMC8-E card can use phantom power in some conditions, and must use local power in other conditions. An application on the Optivity Telephony Manager (OTM) can enable or disable phantom power.

> ***Note:*** The maximum line length for a twelve-channel basestation using phantom power is 1.0 km. The maximum line length for a six-channel basestation, regardless of power, or a twelve-channel basestation using external power, is 1.7 km.

Basestation housing

The basestation environmental housing is IP66 compliant. The housing must be used indoors if a basestation is subject to conductive pollution, or outdoors if basestations are mounted externally.

Figure 12
Basestation environmental housing

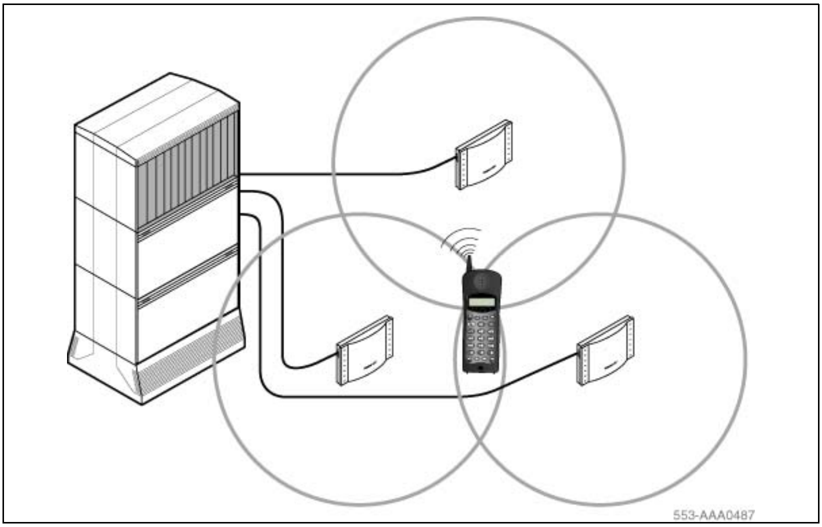


The environmental housing kit includes all of the relevant cables and installation material. The environmental housing mounts to existing walls. Signaling lines provide power to the external basestations.

Basestation cell

A basestation cell is the radio signal area covered by a single basestation. The basestations are positioned so the cells overlap. A DECT handset can make and receive calls when within a basestation cell. When the handset moves from one cell to another, the cell overlap allows the handset to move without interruptions.

Figure 13
Basestation cell



The cell radius varies from 20m to 100m.

The number of basestations required to cover a certain area depends on many factors, such as the following:

- Size of the area of coverage
- Radio propagation characteristics of the buildings
- Materials used for walls, floors, lift shafts, reinforced glass, doors
- Strong magnetic fields from radar, welding equipment, manufacturing equipment, and high energy electronic devices
- Density of telephone users in an area, and amount of telephone traffic

Subscription and de-subscription

Subscription is the process of adding a handset to a DECT system. The handset can then make and receive calls.

A user can subscribe a handset to more than one DECT system. This feature is useful for a company that has multiple DECT sites. See Upgrade a DECT system to an SNMP-managed system, page 394.

De-subscription is the process of removing a handset from a DECT system. The handset user is then prevented from making and receiving calls.

> ***Note:*** Refer to each DECT Handset User Guide for a detailed description of how to use handset and system features.

Optivity Telephony Manager

The Optivity Telephony Manager (OTM), also known as Communication Server 1000 Telephony Manager (TM) from release 3.0 onwards, provides a single point of access and control to manage multiple applications on a Meridian 1, CS 1000M, or CS 1000S system.

OTM provides a DECT application and OTM applications to manage a DECT system.

OTM runs on Windows 2000 Server, Windows 2000 Professional and Windows XP Professional. TM also runs on Windows Server 2003.

> ***Note:*** For an overview of OTM, see *Telephony Manager: System Administration* (553-3001-330).

DECT Application

Features

The DECT Application allows a user to:

- Launch the Application from OTM using Windows and Web navigators
- View DECT provisioning using the DECT Systems window
- View the DMC8 configuration using the Boards window
- View basestation configuration using the Radio Fixed Part window
- View subscription information using the Subscriptions window

- Upgrade firmware using the DECT Systems window
- Subscribe handsets using the Subscription window
- Support DMC8 and DMC (serial only) cards
- Synchronize (update) the DECT Application database to the DECT system configuration when the OTM connects to the DECT system
- Collect performance data using the Performance Collection window
- View On-line Help

OTM Applications

The following DECT management features are provided by OTM Applications:

- Station administration to provision handsets on the PBX system

  Note: For OTM, the application is Windows based, for TM the application is web based.

- OTM Alarm Management provides alarm collection and alarm processing, as well as the following:
  - — a web-based alarm browser to view alarms, past alarms and occurring alarms
  - — a Windows-based alarm browser to view alarms that occur while the browser is open
  - — an Alarm Notification application to notify personnel of an alarm occurrence by pager or e-mail. This application can forward the alarm to an upstream processor
  - — a PC Event log and Viewer to view events and alarms generated from the DECT Application in a report layout
- Backup and restore to create and restore an OTM backup file of the DECT application data
- User profiles to enable configuration of different types of DECT users
- On-line help to provide help for common services features

For more information about the Common Services features, see *Telephony Manager: System Administration* (553-3001-330).

OTM navigators

For information about OTM navigators, refer to *Telephony Manager: System Administration* (553-3001-330).

OTM server connections to DECT

Figure 14 on page 110 shows an overview of an OTM server connected to a DECT system over a V.24 interface.

Web clients access the OTM server over a LAN, WAN and the Public Switched Telephone Network using modems. For the OTM to communicate over PPP with DECT, configure Remote Access Service (RAS) for modem dial out. See “Web-based browser access to the DECT application” on page 443. For more information about OTM access, see *Telephony Manager: System Administration* (553-3001-330).

A client, in this context, is a DECT application that runs on a personal computer or workstation, and depends on an OTM server to perform some operations (for example, a DECT Application client is an application that enables personnel to manage a DECT system).

Figure 15 on page 111 shows an overview of an OTM server connected to a DECT system, over a dedicated LAN interface.

Remote Access Service (RAS)

A computer in a network provides access to remote users through analogue modem or ISDN connections. The computer includes the dial-up protocols and access control (authentication), and can be a regular file server with remote access software or a proprietary system. The modems can be internal or external to the device.

ISDN is an international telecommunications standard for providing a digital service from the customer's premises to the dial-up telephone network.

Figure 14
Local OTM server access to a DECT system by V.24

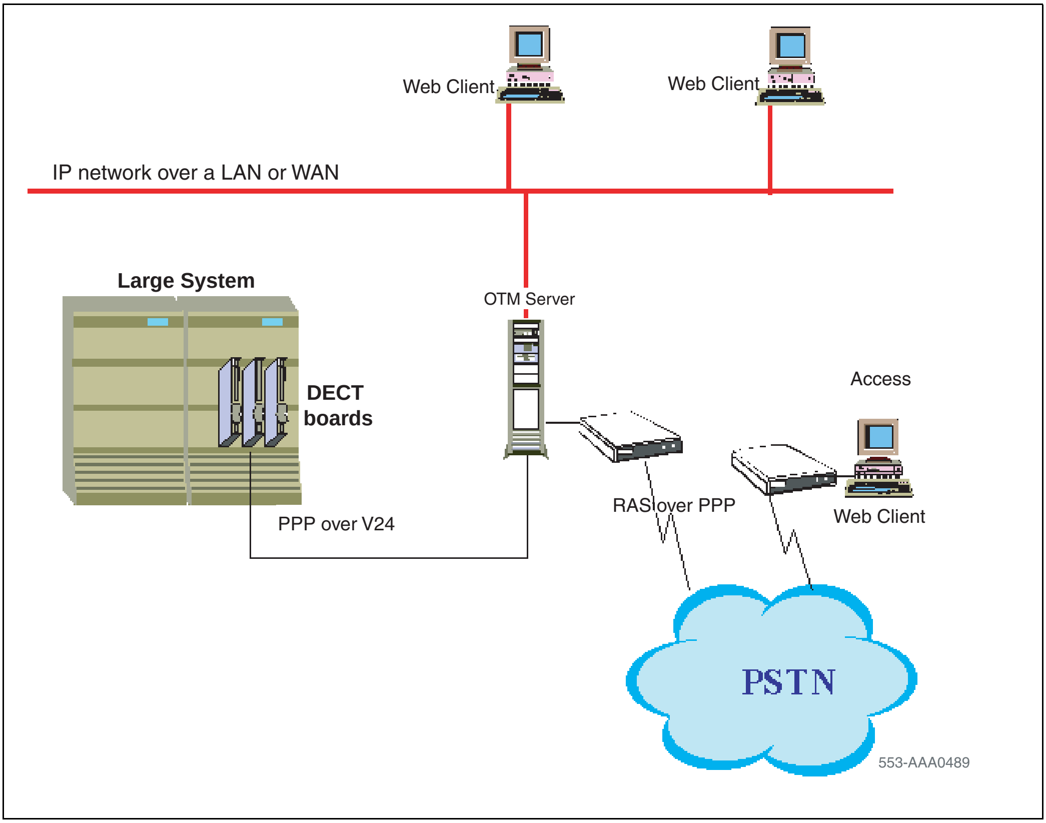
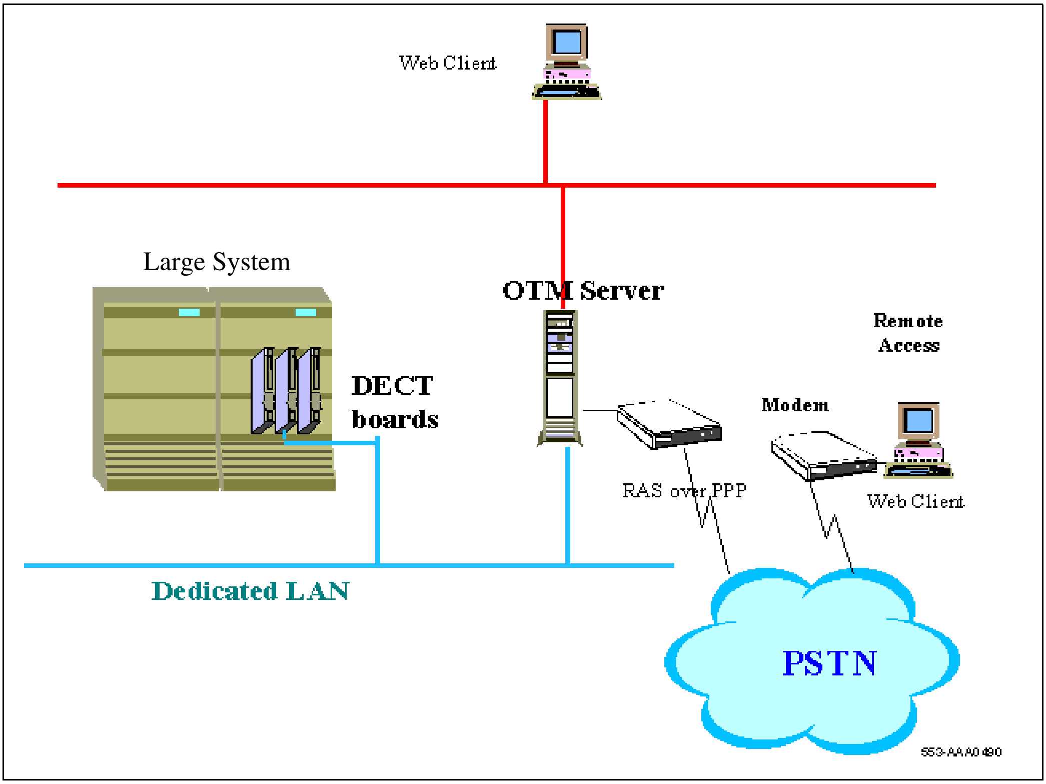


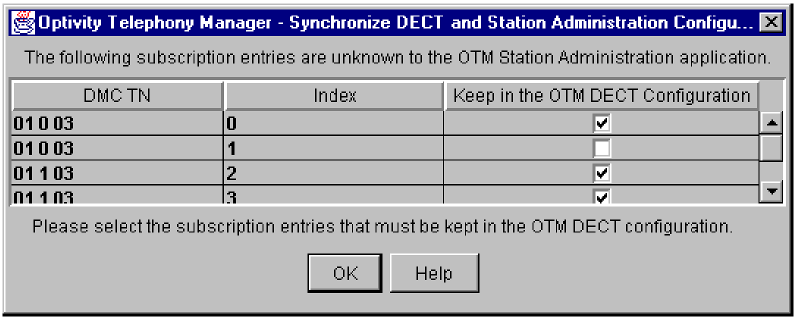
Figure 15
Local OTM server access to a DECT system by dedicated LAN



Synchronize DECT and Station Administration Configuration

The **Synchronize DECT** and **Station Administration Configuration** dialog is selected from the Operations menu (**Retrieve OTM Configuration**) if there is a mismatch. If there is no mismatch, synchronization occurs and Figure 16 on page 112 does not appear.

Figure 16
Synchronize DECT and Station Administration Configuration Mismatch



Optivity Telephony Manager - Synchronize DECT and Station Administration Configu...

The following subscription entries are unknown to the OTM Station Administration application.

DMC TN	Index	Keep in the OTM DECT Configuration
01 0 03	0	☑
01 0 03	1	☐
01 1 03	2	☑
01 1 03	3	☑

Please select the subscription entries that must be kept in the OTM DECT configuration.

DECT systems support configured and subscribed handsets as TNs. The Meridian 1, CS 1000M, or CS 1000S has matching TN handsets configured in LD 10.

PBX to DECT system synchronization

If the PBX configuration data is available through the OTM Station Administration database, then a synchronization facility is available to import the data into the DECT Manager. Synchronization is subject to the following rules:

- A handset not listed in the DECT Manager, but present in the OTM database, is added in the DECT Manager list.
- If the DECT Manager lists a handset, but the OTM database does not, the DECT Manager prompts to either keep or remove the handset.

To add handsets to the DECT manager, select **Configure** from the **Operations** menu. See “Synchronize DECT and Station Administration Configuration” on page 111.

The **Synchronize DECT and Station Administration Mismatch** dialog box highlights DMC TNs in the DECT Manager that are not configured in the OTM Station Administration. Those subscriptions must be kept in the DECT manager so they can be checked. See Figure 16 on page 112.

If there is no mismatch that OTM cannot resolve automatically, the **Synchronize DECT and Station Administration** dialog does not appear.

Two examples of mismatches that OTM cannot resolve automatically are as follows:

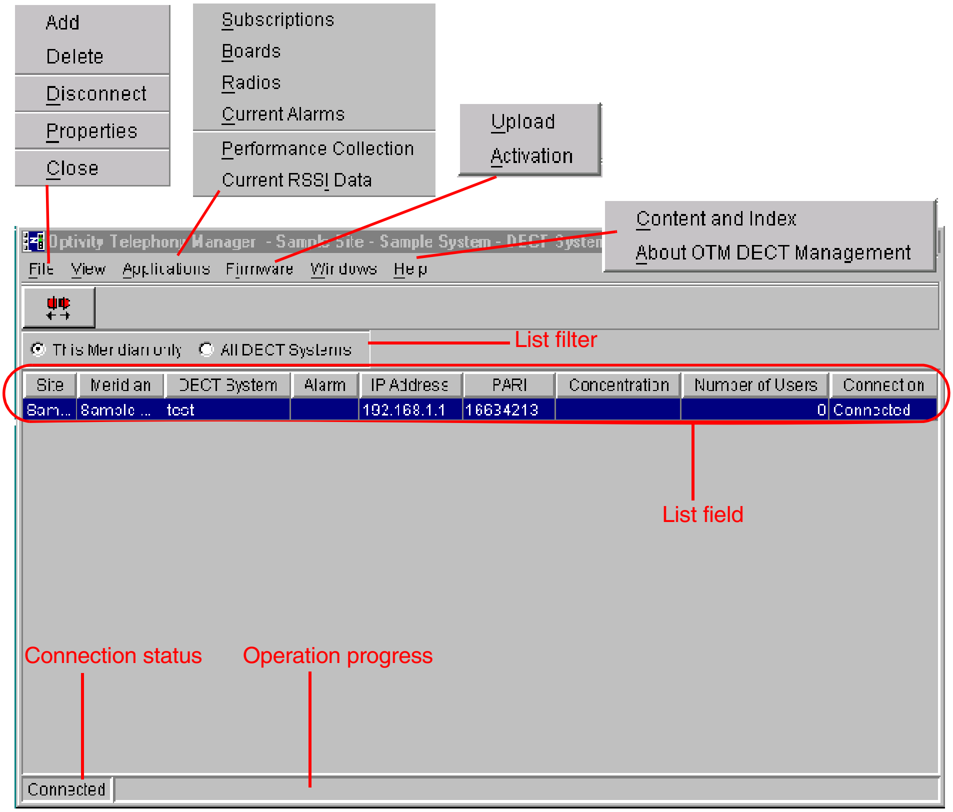
- There are no entries in the Station Administration database, or
- The DECT Manager does not have a DMC configured in a PBX TN location, but an entry exists in the Station Administration database.

Systems window

Use the DECT Systems window to enable the following features:

- Select a DECT system to view database details, or select all DECT systems to view database details.
- Add a DECT system.
- Delete a DECT system.
- Connect to, disconnect from, lock or unlock a connection between the OTM server and a DECT system. See “Connecting to a DECT system” on page 449.
- Open the following windows for the selected DECT systems:
    - Subscriptions
    - DMC Boards
    - Basestation Radio Fixed Parts
    - Active Alarm Snapshot
    - Performance Collection
    - Current RSSI data

Figure 17
DECT Systems window



● This Meridian only ○ All DECT Systems

Site	Meridian	DECT System	Alarm	IP Address	PARI	Concentration	Number of Users	Connection
Sam...	Sample ...	test		192.168.1.1	16634213		0	Connected

Menu

The DECT Systems window displays the following:

- **File** – contains a pull-down menu that allows one of the following to be selected:
  - — Add – creates a new DECT system with default values and opens the DECT System Properties window
  - — Delete – removes a DECT system from the OTM server/OTM client

- Connect / Lock / Disconnect – the same functions as the Connect/ Disconnect tool. See “Connecting to a DECT system” on page 449.
- Properties – opens the DECT System Properties window (Figure 18 to Figure 29)
- Close – closes the client application and all DECT windows opened by that client

- **View** – contains a pull-down menu that allows the following bars to be shown or hidden:
  - Tool bar
  - Status bar
- **Applications** – contains a pull-down menu that allows the following windows to be opened:
  - Subscriptions (Figure 34 on page 131)
  - Boards (DMC) (Figure 47 on page 150)
  - Radios (basestations) (Figure 49 on page 154)
  - Current Alarms
  - Performance Collection (Figure 53 on page 162)
  - Current RSSI data (Figure 55 on page 165)
- **Firmware** – contains a pull-down menu that allows the following windows to be opened:
  - Upload – loads firmware to DMC (Figure 30 on page 128)
  - Activation – makes firmware active
- **Help** – contains a pull-down menu used to select the following:
  - Content and Index
  - About OTM DECT Management application
- **Tool bar icon** – used to click a tool button to do the following:

  Note: While the Connection status is *Connecting* or *Disconnecting*, the Connect/Disconnect tool is disabled. The status bar shows the connection progress.

🟩 →←	Opens a connection to a DECT system selected in the List, when the Connection status shows *Disconnected.* When opened, the icon turns red. See "Connecting to a DECT system" on page 449.
🟨 →←	Locks the connection to a DECT system when the Connection status is *Connected.* This prevents another user from closing the connection.
🟥 ←→	Disconnects from a DECT system when the Connection status is *Connected.*
🟨 ←→	Unlocks the connection from a DECT system when the Connection status is *Connected/Locked.*

- **List filter** – select one of the following:

  — **This Meridian only** – lists the DECT System data selected from the M1 System Window.

  — **All DECT systems** – lists every DECT systems data managed by the OTM server

- **List field** – shows the following for the DECT system or systems selected from the M 1 System Window

  — Site name/location (Figure 18 on page 114)

  — PBX name (Figure 18)

  — DECT system name (Figure 18)

  — Presence of an alarm (Figure 28 on page 126)

  — IP address, for the DECT system (Figure 24 on page 122)

  — Primary Access Rights Identifier (Figure 26 on page 124)

  — Concentration mode (Figure 18)

  — Number of subscribed handsets (Figure 18)

  — Connection status

- **Connection status field** – shows the current state of the connection, where:

  - **Disconnected** – indicates no communication between the OTM server and a DECT system.
  - **Connected** – indicates communication between the OTM server and a DECT system for an operation initiated by a user. The connection disconnects when the operation is finished.

- **Operation progress field** – shows the last received event associated with the connection, such as the following:
  - Disconnecting
  - Connecting
  - Modem Busy
  - Dialling

System Properties dialog

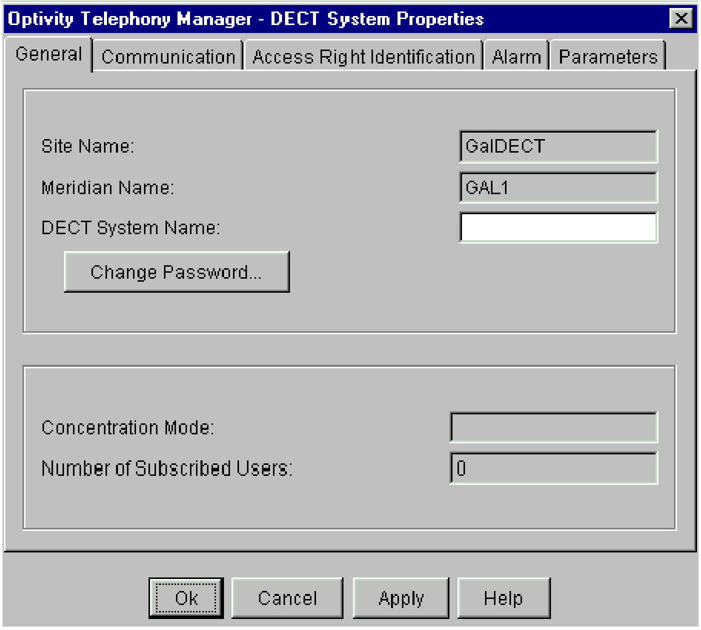
The DECT System Properties dialog is selected from the File menu. The DECT System Properties window has five tabs:

- General
- Communication
- Access Right Identification
- Alarm
- Parameters

See Figure 18 on page 118.

DECT System Properties dialog – General tab

Figure 18
DECT System Properties – General tab


Optivity Telephony Manager - DECT System Properties
General
Communication
Access Right Identification
Alarm
Parameters
Change Password...
Ok
Cancel
Apply
Help

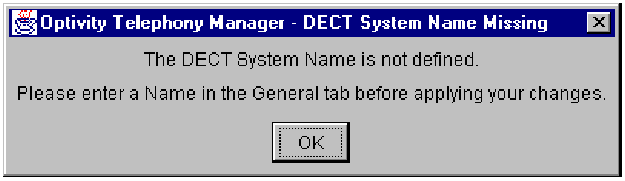
Site Name: GalDECT
Meridian Name: GAL1
DECT System Name:
Concentration Mode:
Number of Subscribed Users: 0

The General tab allows you to:

- View Site Name.
- View Meridian Name.
- View or change the DECT System Name (Figure 19 on page 119 and Figure 20 on page 119).
- Change the password (Figure 21 on page 119).
- View if Concentration Mode is active or not active.
- View Number of Subscribed Users.

The **DECT System Name Missing** window appears when a DECT system name is not entered. See Figure 19.

Figure 19
DECT System Name Missing dialog



Optivity Telephony Manager - DECT System Name Missing

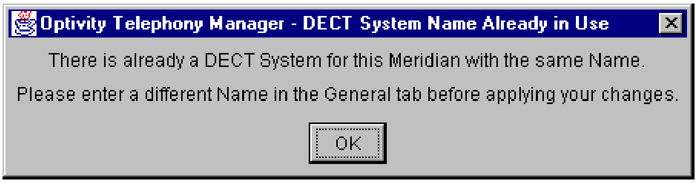
The DECT System Name is not defined.

Please enter a Name in the General tab before applying your changes.

The application does not save a system unless a unique name has been provided.

The **DECT System Name Already in Use** window appears when a DECT system name is the same as the name of another system. See Figure 20.

Figure 20
DECT System Name Already in Use dialog



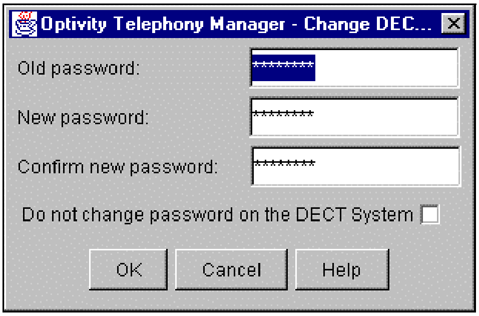
Optivity Telephony Manager - DECT System Name Already in Use

There is already a DECT System for this Meridian with the same Name.

Please enter a different Name in the General tab before applying your changes.

The **Change DECT System Password** window is selected from the **DECT System Properties – General** tab. See Figure 21.

Figure 21
Change DECT System Password dialog



Optivity Telephony Manager - Change DEC...

Old password: ********

New password: ********

Confirm new password: ********

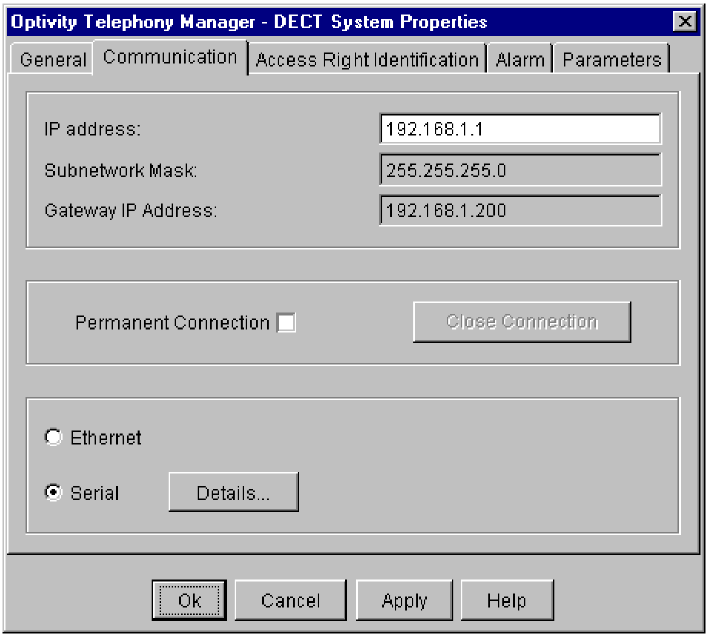
Do not change password on the DECT System □

If the new password does not match the confirmed password, a dialog box opens and warns that the passwords do not match and allows the passwords to be changed.

DECT System Properties dialog – Communication tab

The DECT System Properties dialog is selected from the **File** menu. See Figure 22 on page 120.

Figure 22
DECT System Properties – Communication tab



Optivity Telephony Manager - DECT System Properties

IP address: 192.168.1.1
Subnetwork Mask: 255.255.255.0
Gateway IP Address: 192.168.1.200

Permanent Connection □

○ Ethernet
● Serial

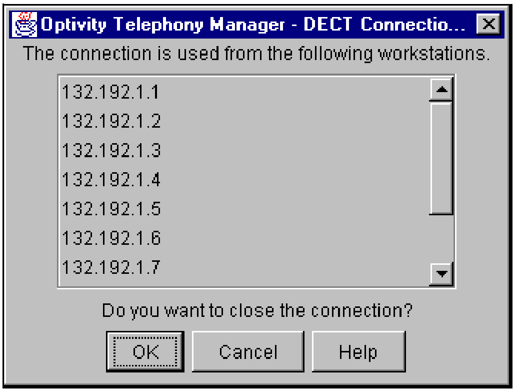
The **Communication** tab allows you to:

- View or change the unique IP address; used if the connection is Serial or Ethernet.
- View the Subnetwork Mask.
- View the Gateway IP address.

- Check a Permanent Connection to keep the connection open and open the connection when the OTM starts.
- Select Close Connection (see Figure 23 on page 121).
- Select Ethernet or Serial connection.
- Select Details for the Serial connection (see Figure 24 on page 122).
- Select a new DECT system definition by pressing the OK button. This causes the manager to try to connect to a new DECT system and write the system name in MIB2, after the following steps are complete:
  - — Enter the new system IP address.
  - — Specify the new system name.

The **Close Connection** dialog opens when the **Close Connection** button on the DECT System Properties – Communication tab is clicked. See Figure 23.

Figure 23
Close Connection dialog



Optivity Telephony Manager - DECT Connectio...

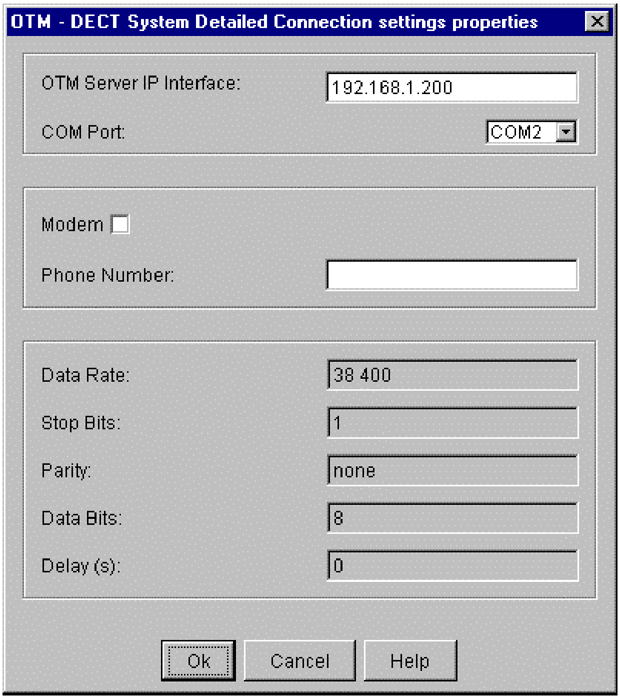
The connection is used from the following workstations.

132.192.1.1
132.192.1.2
132.192.1.3
132.192.1.4
132.192.1.5
132.192.1.6
132.192.1.7

Do you want to close the connection?

DECT System Detailed Connection settings properties is selected from the **Details** button of the **DECT System Properties – Communication** tab. See Figure 24.

Figure 24
DECT System Detailed Connection settings properties



OTM Server IP Interface: 192.168.1.200

COM Port: COM2

Modem □

Phone Number:

Data Rate: 38 400

Stop Bits: 1

Parity: none

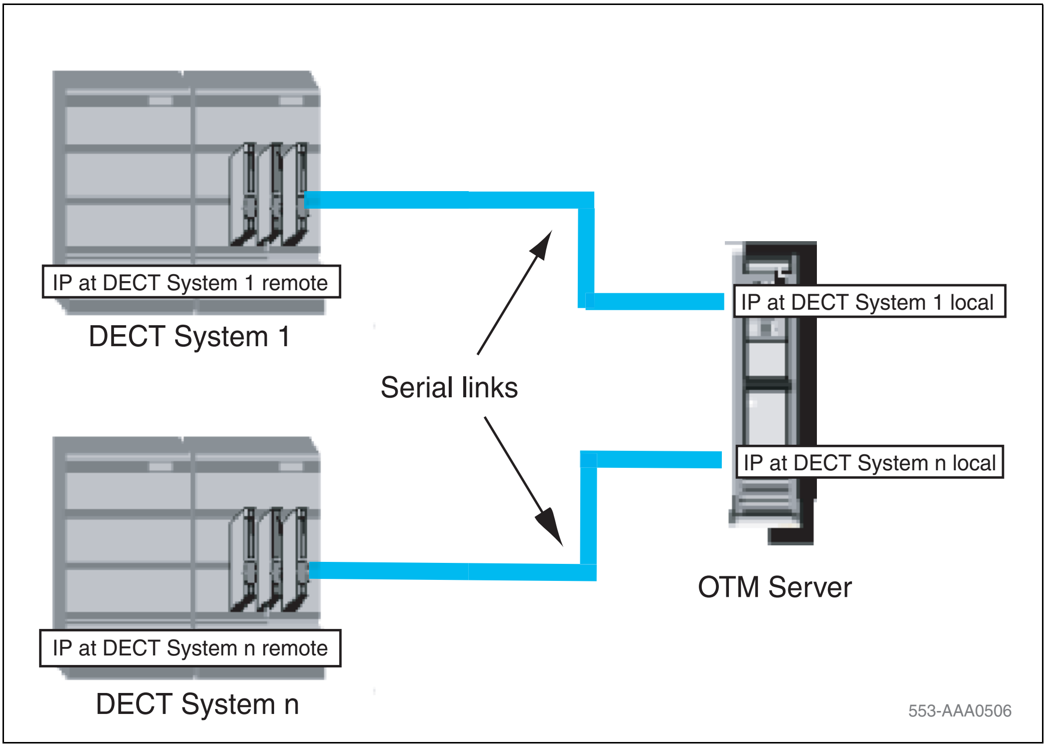
Data Bits: 8

Delay (s): 0

DECT System Detailed Connection settings properties dialog allows you to:

- View or change the OTM Server IP interface assigned to the PC RAS port interface on the same network as DECT.
- View or select the COM Port attached to either DECT or the modem.
- Select a modem mode.
- View or change the Phone Number that dials the modem.

Figure 25
Local and remote IP address for serial connections

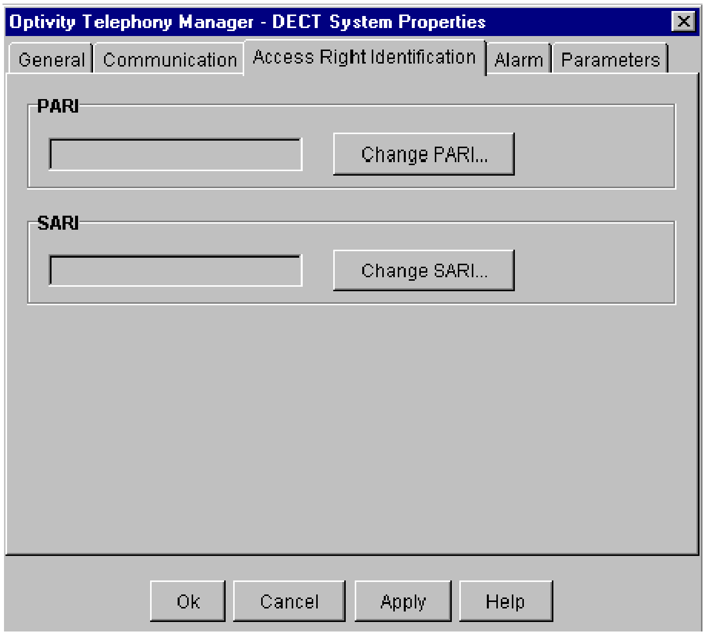

IP at DECT System 1 remote
DECT System 1
Serial links
IP at DECT System 1 local
IP at DECT System n local
OTM Server
IP at DECT System n remote
DECT System n
553-AAA0506

Supply an IP address for local and remote ends of the serial link, so the OTM can route IP traffic to the correct DECT system. See Figure 25.

DECT System Properties dialog – Access Right Identification tab

The **DECT System Properties** dialog is selected from the **File** menu. See Figure 26.

Figure 26
DECT System Properties – Access Right Identification tab

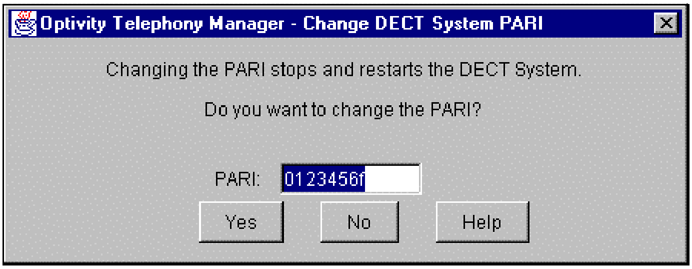


There are two Access Right Identifications, a Primary Access Right Identification (PARI) and a Secondary Access Right Identification (SARI), that identify each DECT system. The Access Right Identification tab allows you to:

- View or change the PARI. See Figure 27 on page 125.
- View or change the SARI. (A SARI dialog box is similar to that shown in Figure 27.)

The **Change DECT System PARI** window appears when the **Change PARI**... button on the **Access Right Identification** tab is pressed. See Figure 27.

Figure 27
Change PARI dialog



Optivity Telephony Manager - Change DECT System PARI

Changing the PARI stops and restarts the DECT System.

Do you want to change the PARI?

PARI: 0123456f

Do not change the PARI or SARI until connected to the DECT system requiring the new PARI or SARI.

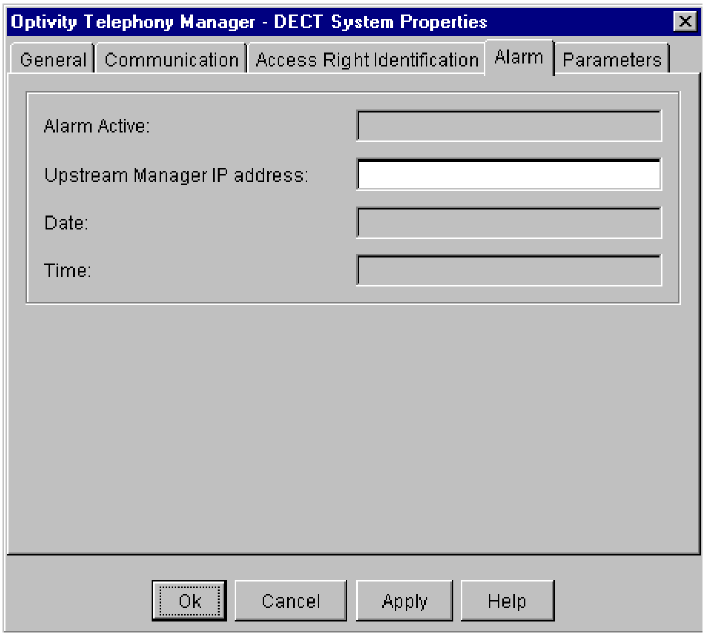
During synchronization, a dialog warns if a DECT system has a different PARI or SARI than the OTM DECT manager.

See “Multi-site Mobility Networking subscriptions” on page 148 for additional information about changing the PARI and SARI.

DECT System Properties dialog – Alarm tab

The **DECT System Properties** dialog is selected from the File menu. See Figure 28.

Figure 28
DECT System Properties – Alarm tab



Optivity Telephony Manager - DECT System Properties

Alarm Active:

Upstream Manager IP address:

Date:

Time:

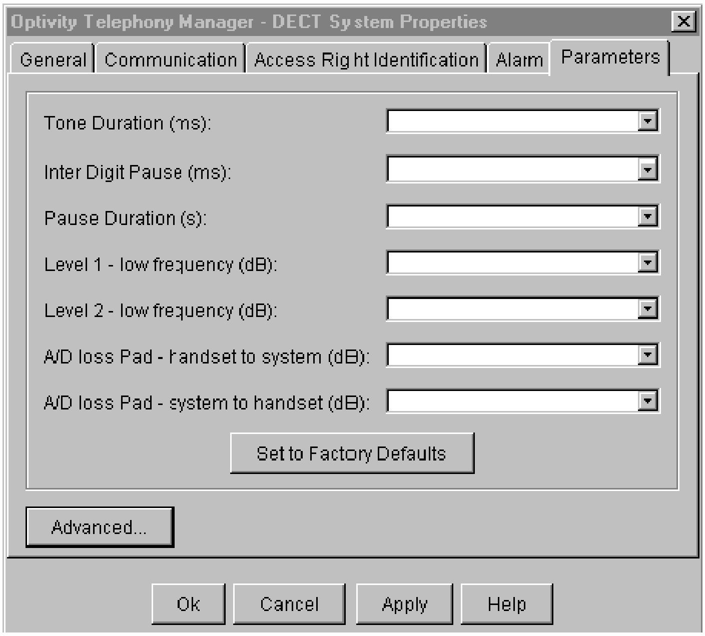
The Alarm tab allows you to:

- View a **Yes** or **No** in the active alarm when the manager is connected to a DECT system with an active alarm.
- View or change the Upstream Manager IP address. The DECT system can send alarms to an upstream manager.
- View or change the Date and Time, used to timestamp alarms. When not connected, the Date and Time fields are blank. When the DECT system is reset, the time and date are not updated.

DECT System Properties dialog – Parameters tab

The **DECT System Properties** dialog is selected from the File menu. See Figure 29.

Figure 29
DECT System Properties – Parameters tab


Optivity Telephony Manager - DECT System Properties
General
Communication
Access Right Identification
Alarm
Parameters
Tone Duration (ms):
Inter Digit Pause (ms):
Pause Duration (s):
Level 1 - low frequency (dB):
Level 2 - low frequency (dB):
A/D loss Pad - handset to system (dB):
A/D loss Pad - system to handset (dB):
Set to Factory Defaults
Advanced...
Ok
Cancel
Apply
Help

The Parameters tab allows you to:

- View or change Tone Duration in milliseconds.
- View or change Inter Digit Pulse width in milliseconds.
- View or change Level 1 – low frequency in decibels.
- View or change Level 2 – low frequency in decibels.
- View or change Analog/Digital loss pad – handset to system in decibels.

- View or change Analog/Digital loss pad – system to handset in decibels.
- Set all parameters to Factory Default values.

WARNING — System Failure

Only change the Advanced button settings under the guidance of a Nortel support representative.

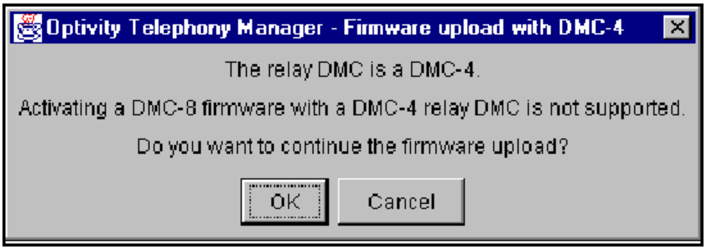
Incorrect settings can cause the system to fail.

The DECT System Properties Parameters are read from DECT on synchronization.

Firmware upload and activation

The Firmware upload dialog is selected from the Firmware menu.

Figure 30
Firmware upload with DMC-4 dialog



Optivity Telephony Manager - Firmware upload with DMC-4

The relay DMC is a DMC-4.

Activating a DMC-8 firmware with a DMC-4 relay DMC is not supported.

Do you want to continue the firmware upload?

The designator DMC is used to differentiate between the NTCW00AA DMC card and the NTCW00xx DMC8 card.

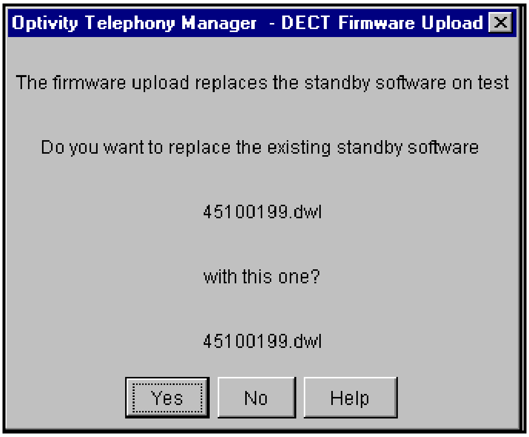
This dialog alerts that a DMC card cannot support a firmware upload. If **OK** is selected, a file chooser allows a firmware file to be selected from the Client or from the OTM server. See Figure 32 on page 129. When **OK** is selected, the existing standby firmware can be replaced with new firmware.

Do one of the following:

- Accept the firmware for DECT.
- Cancel the firmware upload for DECT.

See Figure 30 on page 128.

Figure 31
Firmware upload dialog



Optivity Telephony Manager - DECT Firmware Upload

The firmware upload replaces the standby software on test

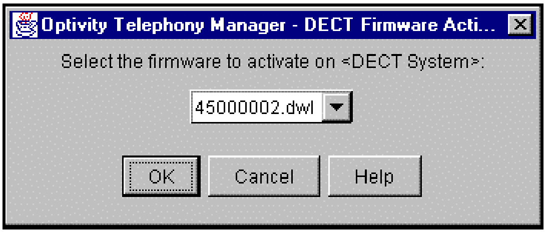
Do you want to replace the existing standby software

45100199.dwl

with this one?

45100199.dwl

Figure 32
Firmware activation dialog

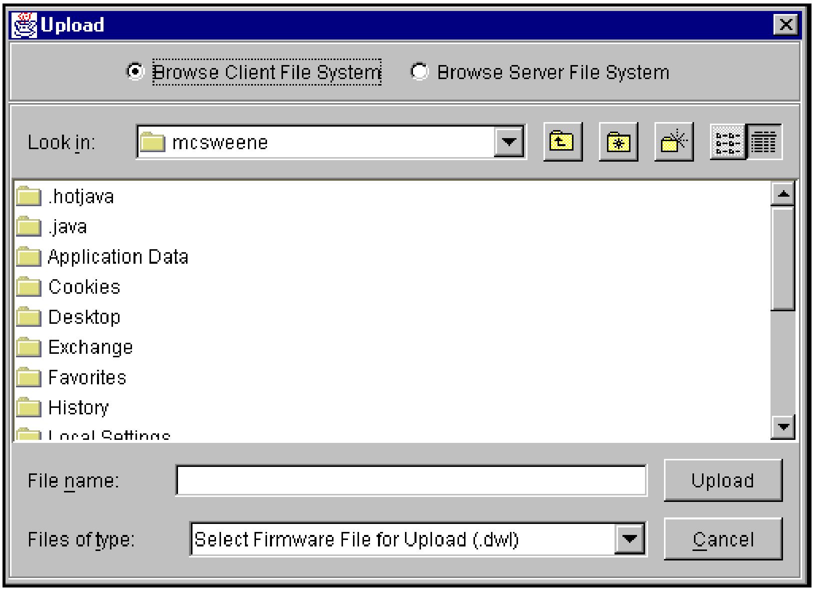


Optivity Telephony Manager - DECT Firmware Acti...

Select the firmware to activate on <DECT System>:

45000002.dwl

Figure 33
Upload file chooser



The **Upload** radio buttons allow you to:

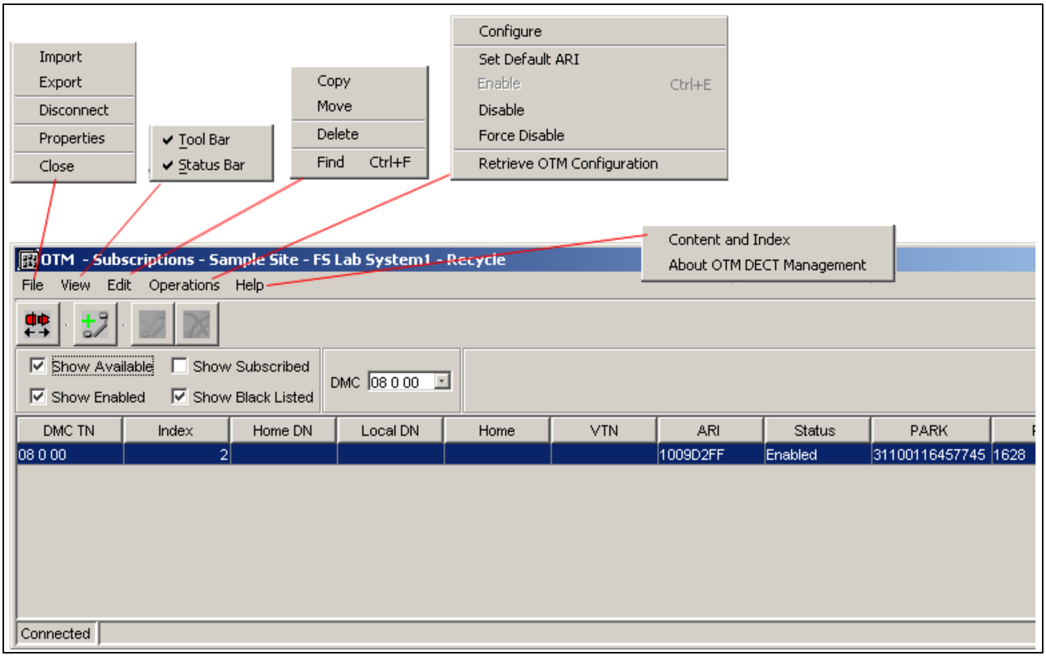
- Browse files on the Client PC.
- Browse files on the OTM Server.

Select a file from either the client or the server to upload to DECT.

Subscriptions window

The Subscriptions window is selected from the DECT Systems window Applications menu. See Figure 34.

Figure 34
Subscriptions window



OTM - Subscriptions - Sample Site - FS Lab System1 - Recycle

☑ Show Available □ Show Subscribed
☑ Show Enabled ☑ Show Black Listed
DMC 08 0 00

DMC TN	Index	Home DN	Local DN	Home	VTN	ARI	Status	PARK	F
08 0 00	2					1009D2FF	Enabled	31100116457745	1628

Connected

Features

The Subscriptions window enables the following:

- Connect to, disconnect from, lock or unlock a connection between the OTM server and a DECT system.
- Choose to show, in any combination, (see Figure 36 on page 137 and Figure 37 on page 138) handsets that are:
  - — Available
  - — Subscribed

  - Enabled
  - Blacklisted
  - Configured on one DMC8 or all DMC8s
- Subscribe (configure) handsets.
- De-subscribe handsets.
- Copy subscription data.
- Move subscription data.
- Delete subscription data.
- Find subscription data.
- Export subscription data.
- Import subscription data.

Note: To use a handset, the handset must first be programmed on the system using LD 10.

Menu

The Subscriptions window displays the following:

- **File** – contains a pull-down menu allowing one of the following to be selected:
  - Import – a subscription from a file (see Figure 40 on page 142)
  - Export – a subscription to a file (see Figure 41 on page 143)
  - Connect – Lock, Unlock, Disconnect
  - Properties – includes data in the subscription list and International Portable User Identifier (IPUI) (see Figure 45 on page 147)
  - Close – close the Subscriptions window
- **View** – contains a pull-down menu that shows or hides the following:
  - Tool bar
  - Status bar
- **Edit** – contains a pull-down menu to open the following dialog boxes:

  - Copy (see Figure 38 on page 139)
  - Delete (see Figure 37 on page 138)
  - Find (see Figure 42 on page 144)
- **Operations** – contains a pull-down menu to open the following windows:
  - Configure – to program a handset on the system. See Figure 35 on page 136.
  - Set Default ARI – enter the default Portable Access Rights Key. See Figure 46 on page 149.)
  - Enable – to subscribe a handset
  - Disable – to de-subscribe a handset from one DECT system (see Figure 43 on page 145) or de-subscribe a handset from all DECT systems, for example, Multi Site Mobility Networking. See the section “Multi-site Mobility Networking subscriptions” on page 148.
  - Force Disable – to return the subscription to the available state, and requests the system to disable the subscription. However, there is no interaction between the system and handset. See Figure 44 on page 146.
  - Retrieve OTM Configuration – to retrieve the handset configuration from the OTM Station Administration database. If there is a mismatch between the Station Administration configuration and the DECT application configuration, see Figure 16 on page 112.
- **Help** – contains a pull-down menu to select the following:
  - Content and Index
  - About DECT application

- **Tool bar** – click the appropriate tool button to do the following:

→←	Connect	Performs same functions as “Systems window” on page 113.
→←	Lock	Performs same functions as “Systems window” on page 113.
←→	Unlock	Performs same functions as “Systems window” on page 113.
←→	Disconnect	Performs same functions as “Systems window” on page 113.
✓	Enable	Subscribes a handset.
✗	Disable	De-subscribes a handset.
+	Configure	Programs a handset.

- **List filter** – to show or hide details of handsets that are:

  — Available (see Figure 36 on page 137 and Figure 37 on page 138)

  — Subscribed (Figure 36 and Figure 37)

  — Enabled (Figure 36 and Figure 37)

  — Black-listed (Figure 36 and Figure 37)

  Note: DMC restricts the list to subscription data for one DMC or lists subscription data for all DMC.

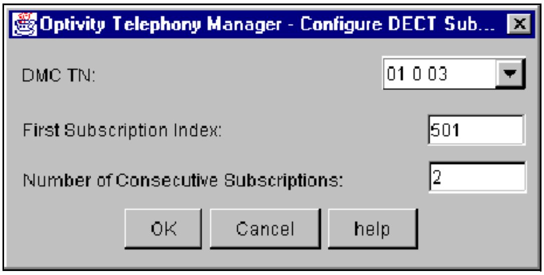
- **List** – to show the following subscription details for handsets assigned to a <sitename>, a <PBX name>, a <DECT system name>. See the Figure 34 title bar on page 131.

  — DMC TN

  - Index – 32 units or 510 virtual units for concentration on a DMC
  - Concentrated handset Home DN
  - Concentrated handset Local DN – different than Home DN for visitor concentrated handset
  - Virtual TN for concentration handsets
  - Subscription ARI
  - Subscription status – updated by SNMP traps from DECT
  - PIN code appears during subscription activation
  - An 80-character comment
- **Pop up menu** – available when at least one subscription is selected. The pop-up menu contains the following items:
  - Configure
  - Enable
  - Disable
  - Copy
  - Move
  - Delete
  - Export
  - Properties
  - Help
- **Status bar** – shows the following:
  - Connection status
  - Operation status
  - Current subscription ARI

Configure and enable subscriptions

Figure 35
Configure DECT Subscription dialog



Optivity Telephony Manager - Configure DECT Sub...

DMC TN: 01 0 03

First Subscription Index: 501

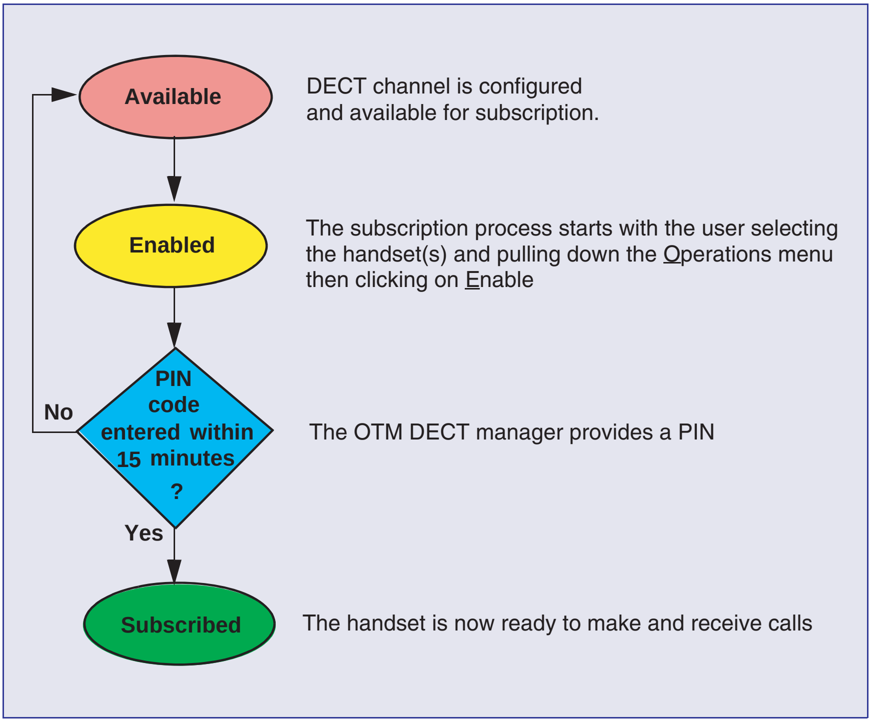
Number of Consecutive Subscriptions: 2

Configure DECT Subscription enables the following:

- Select a DMC TN.
- Enter the first subscription index (unit, as in l s c u).
- Select a number of consecutive subscriptions.

When configured, the subscription becomes available and the subscription can be enabled. During the enable process, the DECT manager generates a PIN code for the subscription. See Figure 36 on page 137.

Figure 36
Enable a subscription

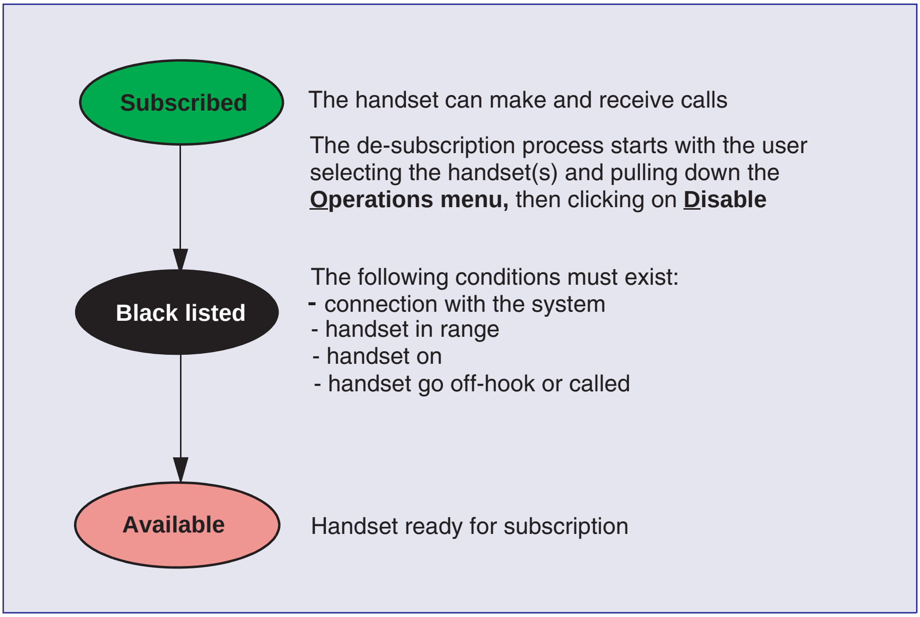

Available
DECT channel is configured and available for subscription.
Enabled
The subscription process starts with the user selecting the handset(s) and pulling down the Operations menu then clicking on Enable
PIN code entered within 15 minutes ?
No
Yes
The OTM DECT manager provides a PIN
Subscribed
The handset is now ready to make and receive calls

Disable subscriptions

A subscription can be de-subscribed in the following ways:

- As a single handset
- In a list of selected handsets
- For all handsets on a DMC

Figure 37
Disable a subscription


Subscribed
The handset can make and receive calls
The de-subscription process starts with the user selecting the handset(s) and pulling down the **Operations menu,** then clicking on **Disable**
Black listed
The following conditions must exist:
- connection with the system
- handset in range
- handset on
- handset go off-hook or called
Available
Handset ready for subscription

Launching an on-air de-subscription requires an open connection to DECT.

When the DECT Manager starts the de-subscription, DECT holds the de-subscription until one of the following occurs:

- The handset makes or receives a call.
- The DECT Manager removes the subscription.

The DECT system notifies the DECT Manager that the handset is de-subscribed.

The DECT Manager can stop a handset from operating on all the DECT systems where the handset is subscribed with a given International Portable User Identifier (IPUI).

To stop a handset from operating, the handset must be within radio range and ready for on-air de-subscription. The process removes handset subscription data from:

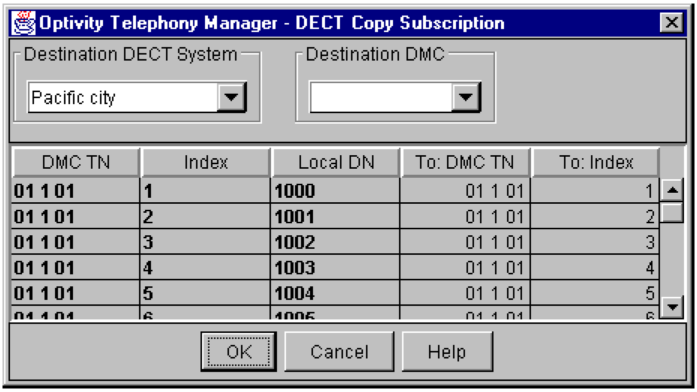
- **a** the DECT system DMCs,
- **b** the handset, and
- **c** the DECT managers handset and DECT system files.

When the handset subscription data is removed, the handset no longer works on any DECT system.

Copy subscriptions

The **DECT Copy Subscription** dialog is selected from the Edit menu.

Figure 38
DECT Copy Subscription dialog



Optivity Telephony Manager - DECT Copy Subscription

Destination DECT System: Pacific city

Destination DMC:

DMC TN	Index	Local DN	To: DMC TN	To: Index
01 1 01	1	1000	01 1 01	1
01 1 01	2	1001	01 1 01	2
01 1 01	3	1002	01 1 01	3
01 1 01	4	1003	01 1 01	4
01 1 01	5	1004	01 1 01	5
01 1 01	6	1005	01 1 01	6

The **DECT Copy Subscription** dialog allows subscriptions to be copied from a DMC on DECT system A and then pasted into a DMC on DECT system B. The subscriptions must have a *Subscribed* status.

Ensure the connection to the destination system is open. Select the Destination DECT system and the Destination DMC from the DECT Copy Subscription dialog.

Subscriptions can be copied from:

a a single handset subscription,

b a list of selected subscriptions, or

c a DMC.

> ***Note:*** Subscriptions cannot be copied within the same DECT system. When a subscription is copied, only DECT data is copied, not the PBX data.

In Figure 38 on page 139, the source subscription data appears in the three left columns: DMC TN, Index, and Local DN. View the source subscription from the Subscription window. The destination subscription data is in columns **To: DMC TN**, and **To: Index**. Index is the Unit on the DMC. When the dialog opens, the source DMCs and destination DMCs are the same.

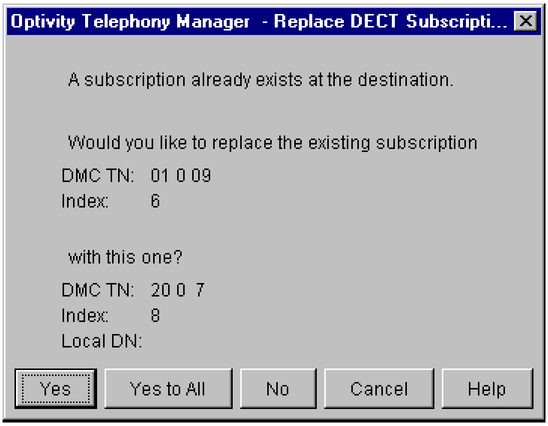
When copying subscription data, ensure a connection exists between the source DECT system and the destination DECT system.

The Copy Subscription feature provides a way to support Multi-site Mobility Networking, by allowing handsets to be subscribed without being on the Distributor Premises.

Replace subscriptions

The **Replace DECT Subscription** dialog allows an action to be confirmed if more than one subscription is overwritten at the destination. See Figure 39.

Figure 39
Replace DECT Subscription dialog



Optivity Telephony Manager - Replace DECT Subscripti...

A subscription already exists at the destination.

Would you like to replace the existing subscription

DMC TN: 01 0 09
Index: 6

with this one?

DMC TN: 20 0 7
Index: 8
Local DN:

Move subscriptions

The **Move Subscriptions** dialog is selected from the **Edit** menu.

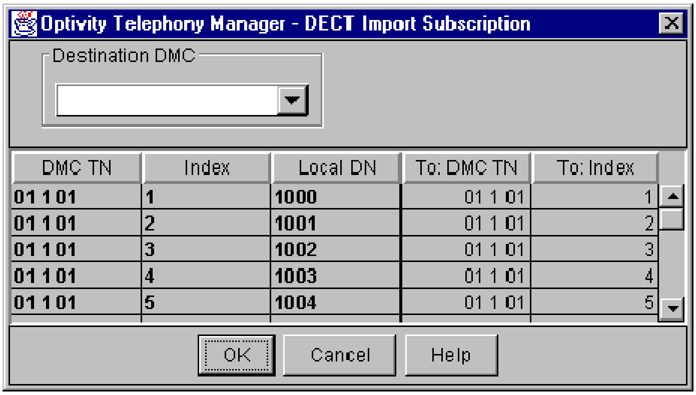
Move Subscriptions is similar to Copy, except for the following. The Move Subscriptions dialog allows subscriptions to be cut/removed from a DMC on DECT system A, and the subscriptions pasted into a DMC on the same DECT system, or on DECT system B.

When using Move, the source DECT system and the destination DECT system must be connected.

Import subscriptions

The **DECT Import Subscriptions** dialog is selected from the File menu. See Figure 40.

Figure 40
DECT Import Subscription dialog



DMC TN	Index	Local DN	To: DMC TN	To: Index
01 1 01	1	1000	01 1 01	1
01 1 01	2	1001	01 1 01	2
01 1 01	3	1002	01 1 01	3
01 1 01	4	1003	01 1 01	4
01 1 01	5	1004	01 1 01	5

Import Subscriptions is similar to Copy, except for the following. The import dialog allows subscriptions to be copied from an import file and the subscriptions pasted into a DMC on a DECT system.

To paste a subscription, ensure a connection to the destination DECT system.

Delete subscriptions

The Delete operation allows handset information to be removed from the manager and the DECT system, but not the handset. The Delete operation does not require the handset to be available for on-air de-subscription. The Delete operation:

a removes DECT handset subscription data,

b retains the handsets subscription data, if the handset had subscription data. (As the handset does not remove its subscription data, it continues operating on all the DECT systems where this subscription is relevant.), and

c removes the DECT manager handsets subscription data including comments and PBX Station Administration data.

The DECT Manager can be used to remove subscription records from:

a a single handset subscription,

b a list of selected subscriptions, or

c a DMC or from all DMCs at once.

The subscription removal requires an open connection to the DECT system.

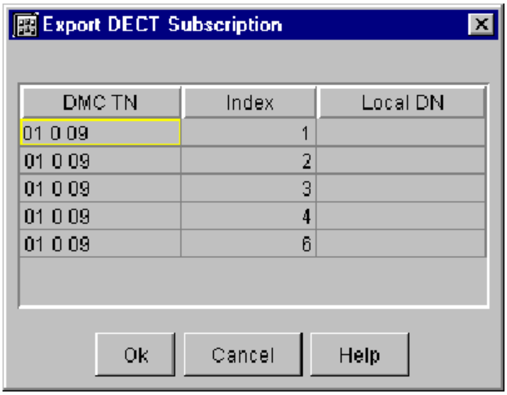
Remove subscription records for the following reasons:

- To clean a Multi Site Mobility Networking DECT system subscriptions on the distributors premises.
- To move a DMC from one DECT system to another.

Export subscriptions

The **Export DECT Subscriptions** dialog is selected from the **File** menu.

Figure 41
Export Subscription dialog



DMC TN	Index	Local DN
01 0 09	1	
01 0 09	2	
01 0 09	3	
01 0 09	4	
01 0 09	6	

Export Subscriptions is similar to Copy, except for the following. The export dialog copies subscriptions from a DECT system and pastes them into a file. See Figure 41.

Note: Import and Export support Multi-site Mobility Networking and Subscription on the Distributor Premises to a DECT system normally managed by OTM B", not OTM A".

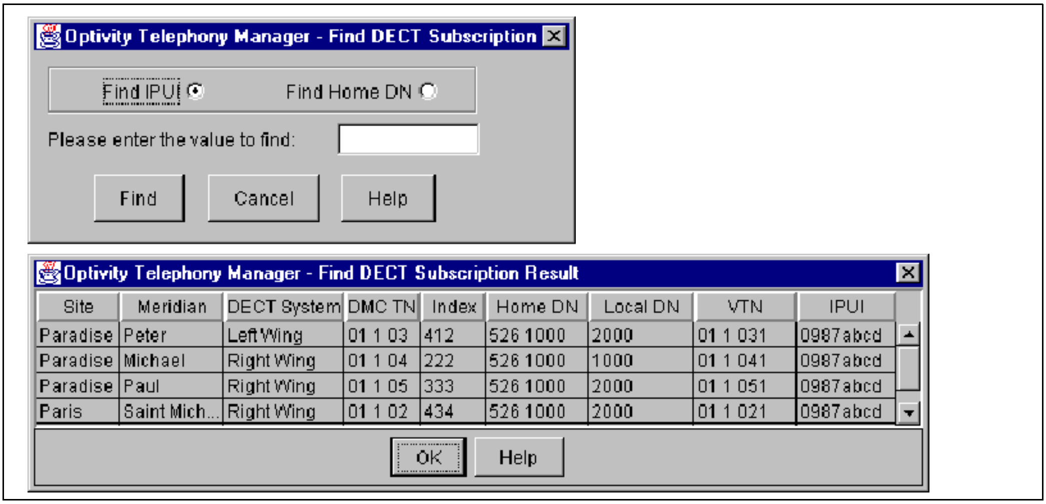
Find subscriptions

The **Find DECT Subscriptions** dialog is selected from the **Edit** menu.

The Find operation allows subscription information to be located by searching for an IPUI or a Home DN, using the Find DECT Subscription dialog. See Figure 42 on page 144.

The Find action displays the subscription information in the **Find DECT Subscription Result** dialog box.

Figure 42
Find Subscription dialog



Optivity Telephony Manager - Find DECT Subscription

Find IPUI ● Find Home DN ○

Please enter the value to find:

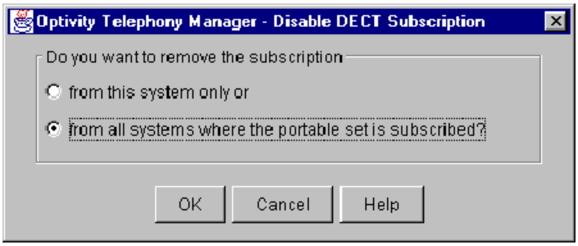
Optivity Telephony Manager - Find DECT Subscription Result

Site	Meridian	DECT System	DMC TN	Index	Home DN	Local DN	VTN	IPUI
Paradise	Peter	Left Wing	01 1 03	412	526 1000	2000	01 1 031	0987abcd
Paradise	Michael	Right Wing	01 1 04	222	526 1000	1000	01 1 041	0987abcd
Paradise	Paul	Right Wing	01 1 05	333	526 1000	2000	01 1 051	0987abcd
Paris	Saint Mich...	Right Wing	01 1 02	434	526 1000	2000	01 1 021	0987abcd

Disable subscriptions

The **Disable DECT Subscriptions** dialog is selected from the Operations menu.

Figure 43
Disable DECT Subscription dialog


Optivity Telephony Manager - Disable DECT Subscription
Do you want to remove the subscription
○ from this system only or
● from all systems where the portable set is subscribed?
OK
Cancel
Help

Use the **Disable DECT Subscriptions** window to disable a handset from all DECT systems used in Multi-site Mobility Networking systems. See Figure 43.

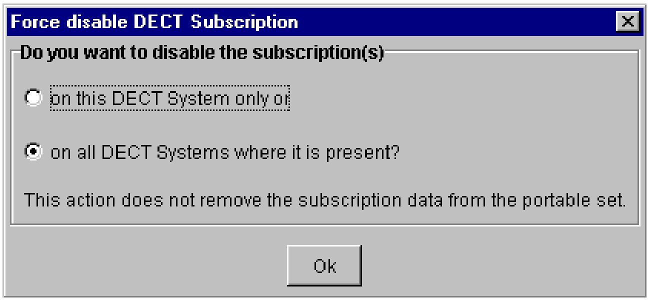
Use **from this system only or** if the handset is on-air on this DECT system. This DECT system contacts the handset. When contact is established, the subscription is removed from the handset. The subscription is removed from both the system database and the OTM server database. The other DECT systems remove subscription data in the background, and the OTM server updates its database for these systems.

If **from all systems where the portable set is subscribed** is used**,** all DECT systems are asked to contact the handset. The first DECT system to contact the handset removes the subscription for that handset from the first DECT system database, and the OTM server database. The other DECT systems remove subscription data in the background and the OTM server updates its database for these systems.

Force disable subscriptions

The **Force disable DECT Subscriptions** dialog is selected from the **Operations** menu.

Figure 44
Force disable DECT Subscription dialog



Force disable DECT Subscription

Do you want to disable the subscription(s)

○ on this DECT System only or

● on all DECT Systems where it is present?

This action does not remove the subscription data from the portable set.

Force disable returns the subscription to the available state and requests the system to disable the subscription. However, there is no interaction between the system and handset.

Force disable can be used when the handset is not in range or on-air.

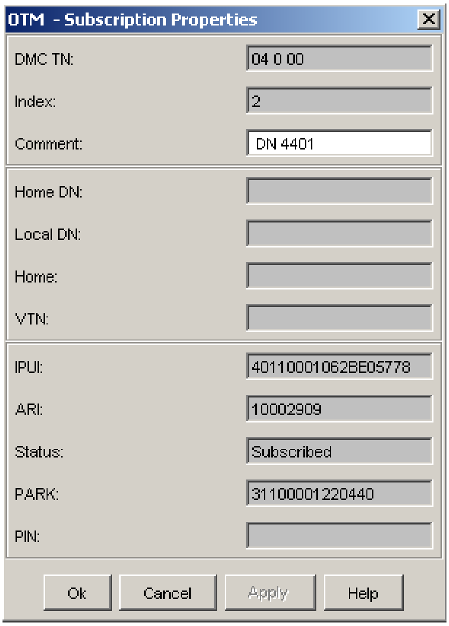
Select **on this DECT System only** or to remove the handset subscription from only this DECT system and remove the handset subscription from all other DECT systems in the background. See Figure 44.

Select **on all DECT Systems where it is present?** to remove the handset subscription from all systems at the same time. See Figure 44.

Subscription Properties

The **DECT Subscription Properties** sheet is selected from the **File** menu. See Figure 45.

Figure 45
DECT Subscription Properties



DMC TN: 04 0 00
Index: 2
Comment: DN 4401
Home DN:
Local DN:
Home:
VTN:
IPUI: 40110001062BE05778
ARI: 10002909
Status: Subscribed
PARK: 31100001220440
PIN:

Features

The DECT Subscription properties sheet allows you to:

- View the DMC Terminal Number.
- View the Index. Index is the TN unit, as programmed in LD 10 in a non-concentrated system, and a virtual TN unit in a concentrated system.
- Change and apply Comments, up to 80 characters.
- View Home DN (where the handset is configured on the PBX as the home location).
- View Local DN.

- View Home handset only.
- View handset Virtual Terminal Number.
- View the International Portable User Identifier (IPUI).
- View the subscription ARI.
- View the Status.
- View the PIN.

DECT Subscription Properties sheet definition

The DECT Subscription Properties sheet displays the same subscription data as the Subscriptions window list items.

Multi-site Mobility Networking subscriptions

In Multi-site Mobility Networking (MSMN), users can take their DECT handsets to other sites in the network, and make and receive calls as if they were at their home location. A handset is subscribed in a given DECT system and can be used in one or many DECT systems.

For information on MSMN feature description, feature interaction, feature packaging, and operating parameters, see “Multi-site Mobility Networking” on page 166. For information on MSMN feature implementation and operation, refer to Upgrade a DECT system to an SNMP-managed system, page 394.

Every handset has a Portable Access Rights Key (PARK). Every DECT system has a Primary Access Rights Identifier (PARI), and can have a Secondary Access Rights Identifier (SARI).

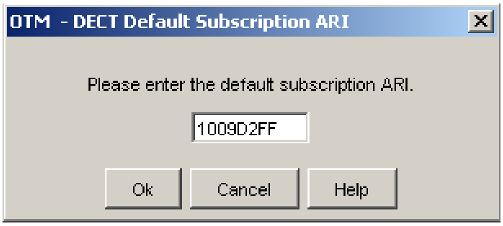
The handset PARK and DECT system PARI and SARI are used by the handset and DECT system to identify each other. The PARK and PARI/SARI match allow the handset to work with a DECT system.

In an MSMN network, for example, DECT system A has a PARI matching a handset PARK while DECT systems B, C, and D have a SARI matching the handset PARK.

The DECT Manager user programs the SARI in the DECT system. The DECT Manager provides the PARK during the on-air subscription, and the PARK is programed into the handset at subscription time. See Figure 26 on page 124 and Figure 27 on page 125.

For example, a handset can be subscribed to a DECT system on the premises of a distributor, where the handset is not to be in operation. Then the subscription data is downloaded to a DECT system where the handset is to be in operation. The PARI, where the handset is subscribed, and the SARI, where the handset is used, are not always the same. The PARK matching the destination DECT system to the handset is provided during the on-air subscription.

Figure 46
DECT Default Subscription ARI dialog



OTM - DECT Default Subscription ARI

Please enter the default subscription ARI.

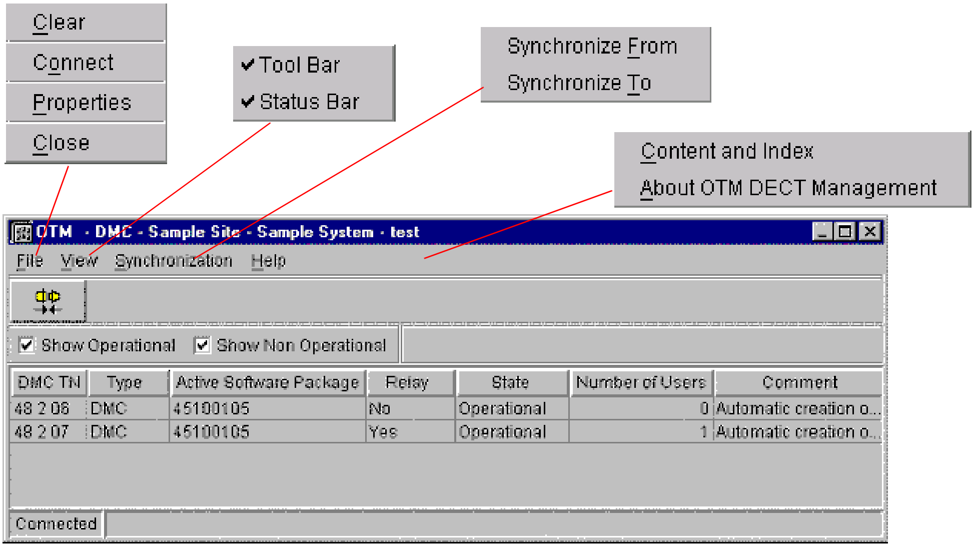
1009D2FF

The DECT Manager provides the ability to specify the ARI given to the handset, to support Multi-site Mobility Networking and Subscription on the distributor premises. See Figure 27 on page 125. The ARI normally defaults to the ARI of the system where the on-air subscription occurs. For MSMN, the default ARI must be equal to the network SARI value for any subscription activity to take place.

DMC boards window

The **DMC Boards** window, seen in Figure 47, is selected from the DECT Systems window **Applications** menu, seen in Figure 17 on page 114.

Figure 47
DMC Boards window



☑ Show Operational ☑ Show Non Operational

DMC TN	Type	Active Software Package	Relay	State	Number of Users	Comment
48 2 06	DMC	45100105	No	Operational	0	Automatic creation o...
48 2 07	DMC	45100105	Yes	Operational	1	Automatic creation o...

Connected

Features

The Boards (DMC) window allows you to:

- Examine DMC details.
- Connect to, disconnect from, lock or unlock a connection between the OTM manager and a DECT system.
- Show Operational DMC, Non-operational DMC, or both.
- Open a properties sheet.

Menu

The Boards window displays the following DMC data:

- **File** – contains a pull-down menu to select one of the following:
  - Clear – erases all subscriptions, sets all basestations to installed status and line powered, allows the DMC to be programmed in a new DECT system.
  - Connect – Lock, Unlock, Disconnect, works the same as the Connect/Disconnect tool.
  - Properties – see Figure 48 on page 153.
  - Close – closes the DMC window.
- **View** – contains a pull-down menu to show or hide the following:
  - Tool bar.
  - Status bar.
- **Synchronization** – contains a pull-down menu to enable the following:
  - Synchronize From – subscription and basestation alarm muting/ power source configuration data from a DMC to the OTM server.
  - Synchronize To – subscription and basestation alarm muting/power source configuration data from the OTM server to a DMC.
- **Help** – contains a pull-down menu to select the following:
  - Content and Index.
  - About DECT application.
- **Tool bar –** used to click a tool button to do the following:

	Connect	Performs same functions as “Menu” on page 151.
	Lock	Performs same functions as “Menu” on page 151.

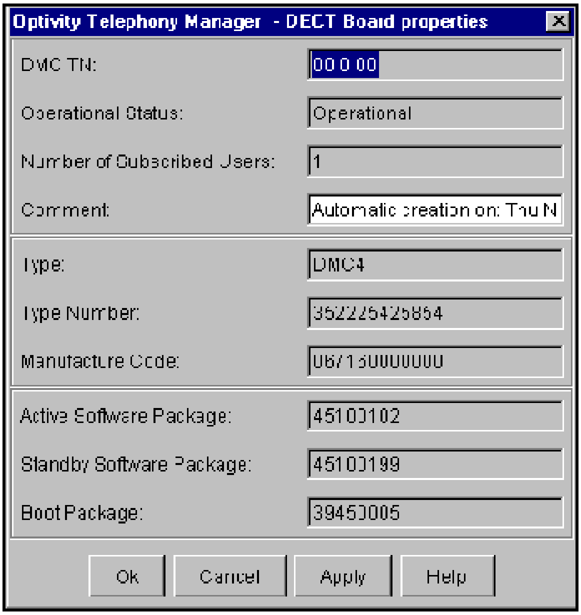
🟨	Unlock	Performs same functions as “Menu” on page 151.
🟥	Disconnect	Performs same functions as “Menu” on page 151.

- **List filter** – to show list details of only the operational DMC or non-operational DMC or both.
- **List** – shows the following DMC details:
  - DMC TN.
  - DMC type.
  - Relay DMC.
  - Operational state – when DMC operational status changes, the OTM server updates the status.
  - Number of handsets on a DMC.
  - An 80-character comment.
- **Pop up menu –** supports the following actions:
  - Synchronize from DMC.
  - Synchronize to DMC.
  - Properties.
  - Help.
- **Properties** – displays additional information about DMC. Only the comment can be modified. See Figure 48 on page 153.

DECT Board properties sheet

The **DECT Board properties** sheet (see Figure 48) is selected from the **File** menu.

Figure 48
Board (DMC) properties sheet



Optivity Telephony Manager - DECT Board properties

DMC TN: 00 0 00

Operational Status: Operational

Number of Subscribed Users: 1

Comment: Automatic creation on: Thu N

Type: DMC4

Type Number: 352225425854

Manufacture Code: 067150000000

Active Software Package: 45100102

Standby Software Package: 45100199

Boot Package: 39450005

Options

The DECT Board properties sheet allows you to:

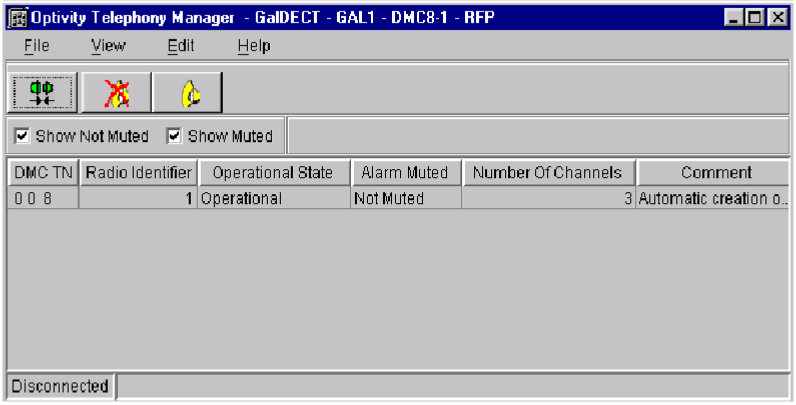
- View DMC details.
- View operational status. When the DMC operational status changes on DECT, the OTM updates the status.
- Change and apply comments, up to 80 characters.
- View DMC Type Number.
- View DMC Manufacture Code.
- View DMC Standby Software Package.

- View DMC Boot Package.
- View DMC Protocol Version.
- Open the help file.
- Close the properties sheet.

Radio Fixed Part (basestation) window

The Radio Fixed Part (**RFP**) window (see Figure 49) is selected from the DECT Systems window **Applications** menu. See Figure 17.

Figure 49
RFP (basestation) window



DMC TN	Radio Identifier	Operational State	Alarm Muted	Number Of Channels	Comment
0 0 8	1	Operational	Not Muted	3	Automatic creation o...

The **RFP** window allows you to:

- Examine basestation details.
- Connect to, disconnect from, lock or unlock a connection between the OTM server and a DECT system.
- Choose to show Muted basestations, or Not Muted basestations, or both.
- Open a properties sheet.

🔕	Mute	Keeps a basestation from generating alarm messages.
🔔	Cancel Mute	Allows a basestation to generate alarm messages.

Menu

The **RFP** window displays the following basestation data:

- **File** – contains a pull-down menu to select one of the following:
  - Connect / Lock / Unlock / Disconnect, works the same as the Connect/Disconnect tool.
  - Properties, opens the Radio Fixed Part properties sheet.
  - Close, closes the Radio Fixed Part window.
- **View** – contains a pull-down menu to show or hide the following:
  - Tool bar.
  - Status bar.
- **Edit** – contains a pull-down menu to do the following:
  - Mute Alarms – keeps a selected basestation from generating alarms.
  - Cancel Mute Alarms – allows a selected basestation to generate alarms.

Note: View alarms on the OTM Alarm browsers (common services) or on the Active Alarm Snapshot window. See Figure 51 on page 158.

- **Help** – contains a pull-down menu to select the following:
  - Content and Index.
  - About DECT application.
- **Tool bar icon** – click the tool button to do the following:

	Connect	Performs same functions as noted in File above.
	Lock	Performs same functions as noted in File above.
	Unlock	Performs same functions as noted in File above.
	Disconnect	Performs same functions as noted in File above.
	Mute	Keeps a selected basestation from generating alarms.
	Cancel	Allows a selected basestation to generate alarms.

- **List filter** – to select a list showing basestations allowed to generate alarms, or basestations not allowed to generate alarms, or both.
- **List** – displays the following:
  - DMC TN – connected to a basestation.
  - Radio Identifier – identifies the basestation (1 to 4) connected to the DMC and the basestation (1 to 8) connected to the DMC8.
  - Operational State – indicates if a basestation is operational or is not operational.
  - Alarm Muted – indicates if a basestation is allowed to generate alarms or not.

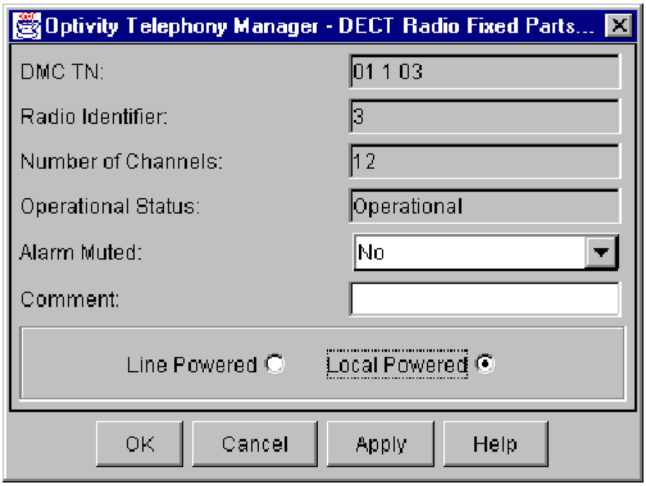
- Number of Channels – identifies the basestation as either a 6-channel or a 12-channel basestation.
- Comment – an 80-character comment field in the DECT application.

- **pop-up menu** – appears when at least one basestation, also known as a Radio Fixed Part (RFP), is selected and right-clicked. Selecting one or more basestations by clicking/double-clicking on a Radio Identifier, or highlighting a row in the list, displays a Properties sheet. See Figure 50 on page 157.
- **Help** – select **Content and Index** or **About** DECT **application.**

DECT Radio Fixed Parts (basestation) properties sheet

The DECT Radio Fixed Parts properties sheet is selected from the pop-up menu.

Figure 50
Radio Fixed Part (basestation) properties sheet



Optivity Telephony Manager - DECT Radio Fixed Parts...

DMC TN: 01 1 03

Radio Identifier: 3

Number of Channels: 12

Operational Status: Operational

Alarm Muted: No

Comment:

Line Powered ○ Local Powered ●

The DECT Radio Fixed Parts properties sheet options

The RFP properties sheet allows you to:

- View basestation details.
- View Operational Status. When the basestation operational status changes, the OTM server updates the status.
- Change and apply Alarm Muting.
- Change and apply comments – up to 80 characters.
- Select Line Power (powered by the DMC card) or Local Powered.
- Open the help file.
- Close the properties sheet.

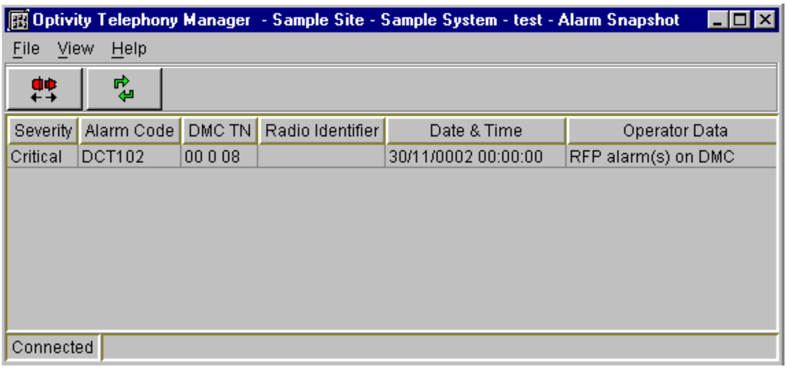
RFP properties sheet definition

The Radio Fixed Part properties sheet displays the same basestation data as the Radio Fixed Part window list items. The properties sheet also shows the power source for the selected basestation.

Active Alarm Snapshot window

The Active Alarm Snapshot window is selected from the DECT Systems window Applications menu.

Figure 51
Active Alarm Snapshot window


Optivity Telephony Manager - Sample Site - Sample System - test - Alarm Snapshot
File
View
Help

Severity	Alarm Code	DMC TN	Radio Identifier	Date & Time	Operator Data
Critical	DCT102	00 0 08		30/11/0002 00:00:00	RFP alarm(s) on DMC

Connected

Features

The Active Alarm Snapshot window allows you to:

- Connect to the Active Alarm Snapshot window.
- Refresh the window.
- Open a properties sheet.

Menu

The Active Alarm Snapshot window displays the alarm data stored in the DMC. The alarm data displayed does not change or update until manually refreshed.

- **File** – contains a pull-down menu to select one of the following:
  - Connect / Lock / Unlock / Disconnect – the same functions as the Connect/Disconnect tool.
  - Properties – opens the Active Alarm Snapshot, Figure 52.
  - Close – closes the Active Alarm Snapshot window.
- **View** – contains a pull-down menu to select the following:
  - Tool bar – to show or hide.
  - Status bar – to show or hide.
  - Refresh – updates the Active Alarm Snapshot window with the latest alarm data from the DECT system selected in the title bar. A separate DMC TN cannot be selected to refresh.
- **Help** – contains a pull-down menu to select the following:
  - Content and Index.
  - About DECT application.

- **Tool bar** – used to click a tool button to do the following:

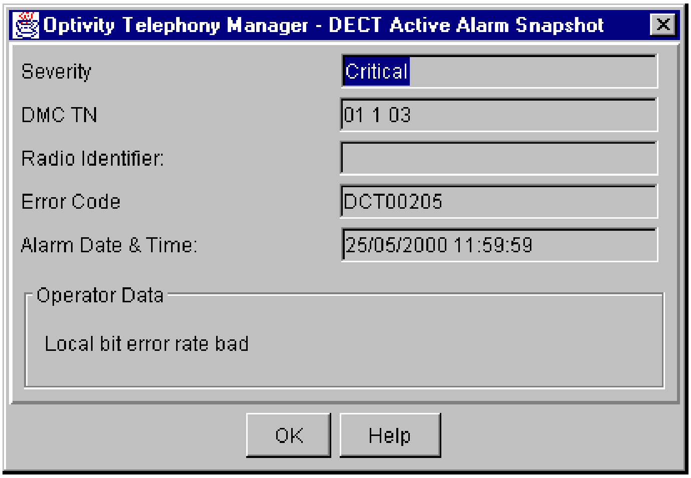
	Connect	Performs same functions as noted in File above.
	Lock	Performs same functions as noted in File above.
	Unlock	Performs same functions as noted in File above.
	Disconnect	Performs same functions as noted in File above.
	Refresh	Updates the Active Alarm Snapshot window with the latest alarm data from the DECT system selected in the title bar. A separate DMC TN cannot be selected to refresh.

- **List** – shows read-only data about the following:
  - Severity – always labeled as Critical.
  - Error Code – a three digit code. Refer to the DECT Operation Administration and Maintenance NTP for the meaning of the Error Codes.
  - DMC TN – indicates the location of the card that originated the alarm.
  - Radio Identifier (basestation identifier) – indicates the basestation that is the source of an alarm.
  - Date and Time – when the alarm occurred.
  - Operator Data – describes the alarm and the faulty component, if applicable.
- **pop-up menu –** appears when at least one RFP (basestation) is selected, and right clicked. The **DECT Active Alarm Snapshot** window opens. See Figure 52.
- **Help** – displays Content and Index, and About DECT application.

DECT Active Alarm Snapshot properties sheet

The **DECT Active Alarm Snapshot** properties sheet, shown in Figure 52, is selected from the pop-up menu. The Active Alarm Snapshot properties sheet displays the same alarm data as the Active Alarm Snapshot window list items.

Figure 52
Active alarm properties sheet



Optivity Telephony Manager - DECT Active Alarm Snapshot

Severity: Critical

DMC TN: 01 1 03

Radio Identifier:

Error Code: DCT00205

Alarm Date & Time: 25/05/2000 11:59:59

Operator Data

Local bit error rate bad

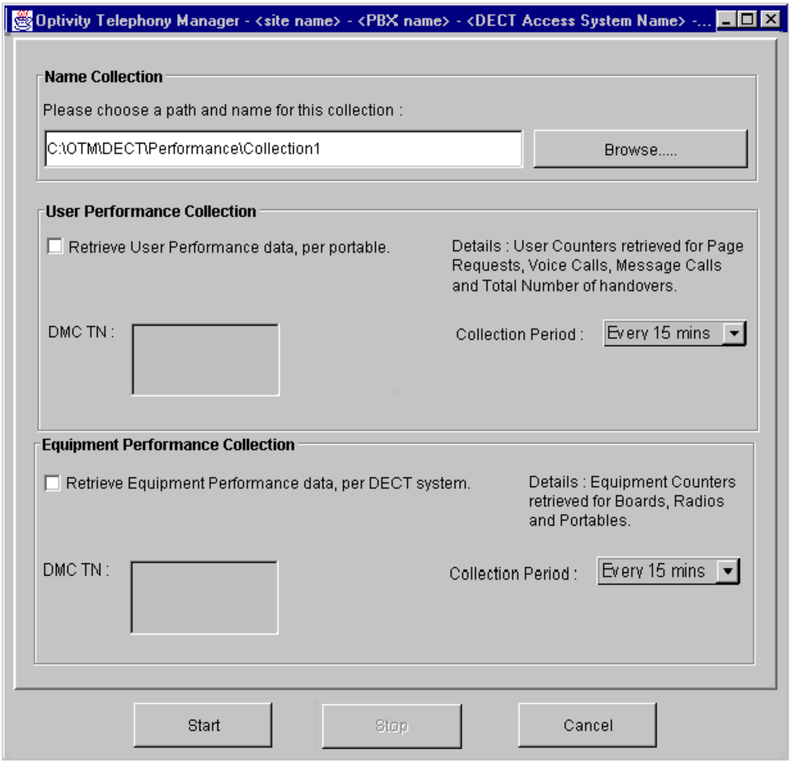
The Active Alarm Snapshot properties sheet properties sheet allows you to:

- View alarm (DECT system message) details.
- Close the properties sheet.
- Open the help file.

Performance Collection window

The Performance Collection window, as seen in Figure 53, is selected from the DECT Systems window Applications menu.

Figure 53
Performance Collection window



Optivity Telephony Manager - <site name> - <PBX name> - <DECT Access System Name> -...

Name Collection

Please choose a path and name for this collection :

C:\OTM\DECT\Performance\Collection1

User Performance Collection

□ Retrieve User Performance data, per portable.

Details : User Counters retrieved for Page Requests, Voice Calls, Message Calls and Total Number of handovers.

DMC TN :

Collection Period : Every 15 mins

Equipment Performance Collection

□ Retrieve Equipment Performance data, per DECT system.

Details : Equipment Counters retrieved for Boards, Radios and Portables.

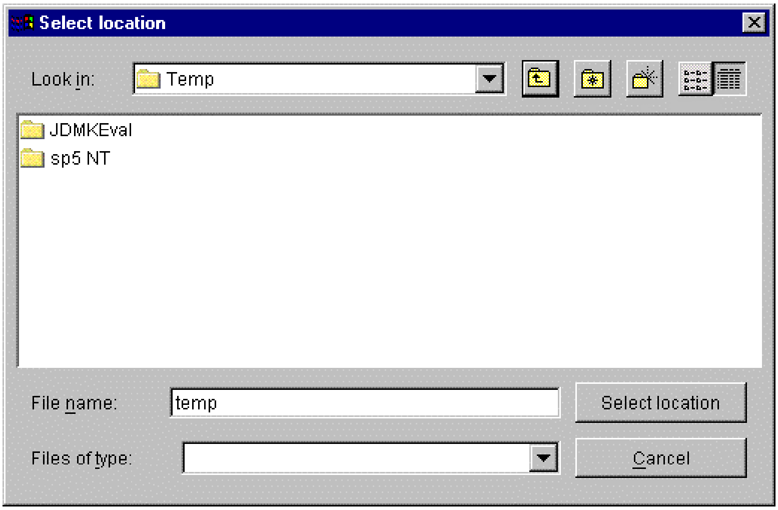
DMC TN :

Collection Period : Every 15 mins

The Performance Collection window displays the following:

- **Name** – to select the directory to store the Performance Collection file.
- **User Performance Collection** – collects counter data on handset user related activities.
- **Equipment Performance Collection** – collects counter data on DMC related activities.

Figure 54
Select location



The Performance Collection window enables the following:

- Start and stop User Performance Collection counters.
- Start and stop Equipment Performance Collection counters.

Performance Collection additional information

The OTM DECT Manager user starts and stops performance counter collection. Performance collection cannot be scheduled. The collection begins when it is manually started, and ceases when manually stopped.

The collection period can be set for 15 minutes, 30 minutes, one hour, or one day. The performance counters are on the DMCs. DMC TNs can be selected.

User (handset) data and Equipment (DECT system) data can be collected separately. User (handset) data and Equipment (DECT system) data collection periods can be set separately.

The OTM DECT Manager stores the performance files. Rebooting the OTM DECT Manager does not destroy the files.

The back up and restore application on the OTM DECT Manager does not back up and restore the performance files.

Retrieve RSSI Snapshot window

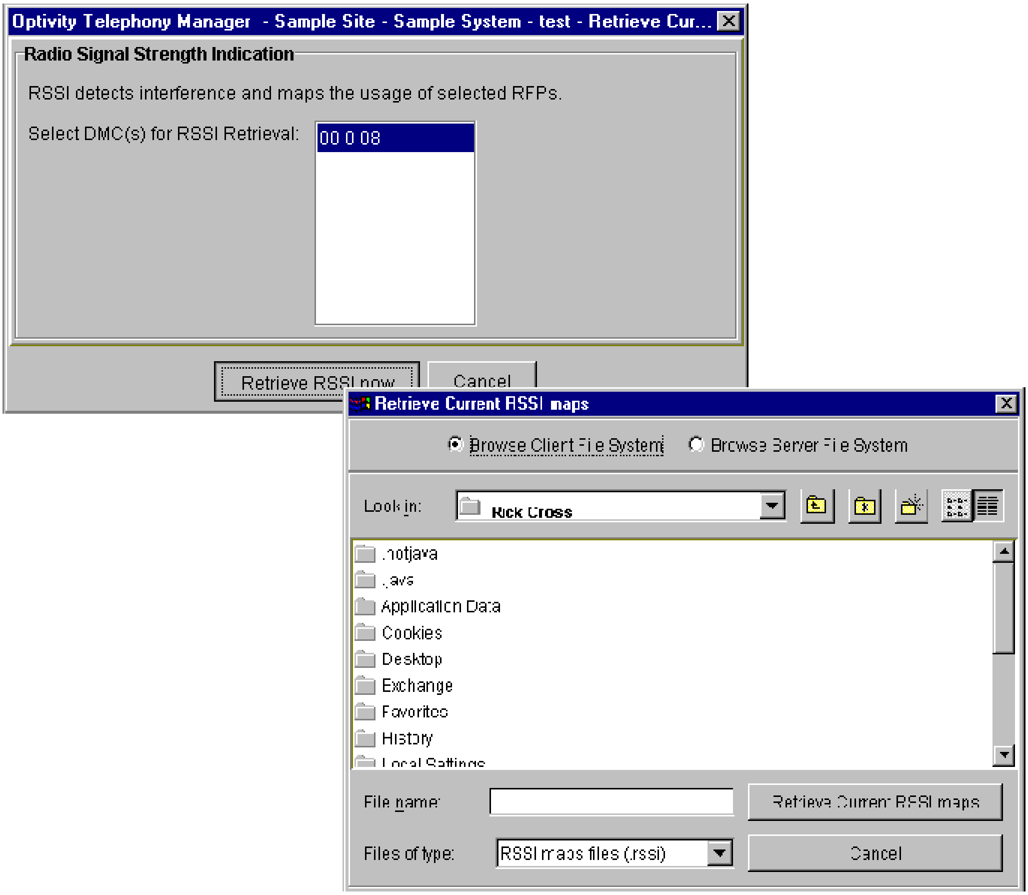
The Retrieve Radio Signal Strength Indication (RSSI) Snapshot window, shown in Figure 55 on page 165, is selected from the DECT Systems window Applications menu.

The Retrieve RSSI window enables the following:

- View Radio Signal Strength Indication details.
- Scroll and select a DMC card for RSSI information retrieval.

The Retrieve RSSI Snapshot window collects, on request, the RSSI for a selected DMC card.

Figure 55
Retrieve RSSI Snapshot window



Optivity Telephony Manager - Sample Site - Sample System - test - Retrieve Cur...

Radio Signal Strength Indication

RSSI detects interference and maps the usage of selected RFPs.

Select DMC(s) for RSSI Retrieval: 00 0 08

Retrieve Current RSSI maps

● Browse Client File System ○ Browse Server File System

Look in: Rick Cross

File name:

Files of type: RSSI maps files (.rssi)

Retrieve RSSI Snapshot attributes

The OTM server collects the RSSI as an ASCII file. The OTM server user must indicate where to store the RSSI file.

Multi-site Mobility Networking

Multi-site Mobility Networking (MSMN) allows a DECT handset user to make and receive calls at any MCDN node. When the handset user visits a MCDN node, the MSMN feature automatically performs the following actions:

- Detects the visiting handset when it is on.
- Forwards calls to the visiting handset from the users home node.

The Call Forward dial tone indicates when MSMN activation was not successful. Turn the handset off and on again to re-activate the MSMN feature.

The MSMN feature requires concentrated DMCs. A concentrated system has each handset configured to a Virtual TN (VTN) on phantom loops. Concentration allows up to 510 handsets to share the DMCs 32 time slots and is a blocking system. See “System concentration traffic” on page 169.

A non-concentrated system has each handset configured to a DMC8 TN. A non-concentrated DMC8 has 32 handset TNs assigned to 32 time slots and is non-blocking.

Separate DECT systems on a PBX can be concentrated or non-concentrated.

Operating parameters

The MSMN feature cannot support a mix of concentrated DMCs and non-concentrated DMCs within the same DECT system.

All DMCs, either new, empty for redundancy, or used for basestation coverage, must have at least one handset configured to ensure system operation.

Feature interactions

Call forward from a MADN handset

A MADN handset at a remote node can activate Call Forward (CFW) at the home node. When the handset shares a DN with another sets, the CFW lamp lights on the shared DN sets. If the handset is not the MARP, the shared DN MARP set can cancel call forward. If the handset is the MARP, the handset overrides any call forward that is set up from other shared DN sets.

Card audit

Card audit does not work with VTNs.

Network Message Service

The MSMN feature does not change the handling of unanswered network calls. The Meridian Mail or CallPilot network mail service does not change with multiple DNs configured against a single mailbox. The visiting DN receives the Message Waiting Indication (MWI) at the visited site.

Feature packaging

The MSMN feature requires the following packages:

- Multi-site Mobility Networking (MSMN) package 370.
- Meridian 1 Companion Option (MCMO) package 240.
- Phantom TN (PHTN) package 254.
- Meridian Companion Enhanced Capacity (MC32) package 350.
- Flexible Feature Codes (FFC) package 139.

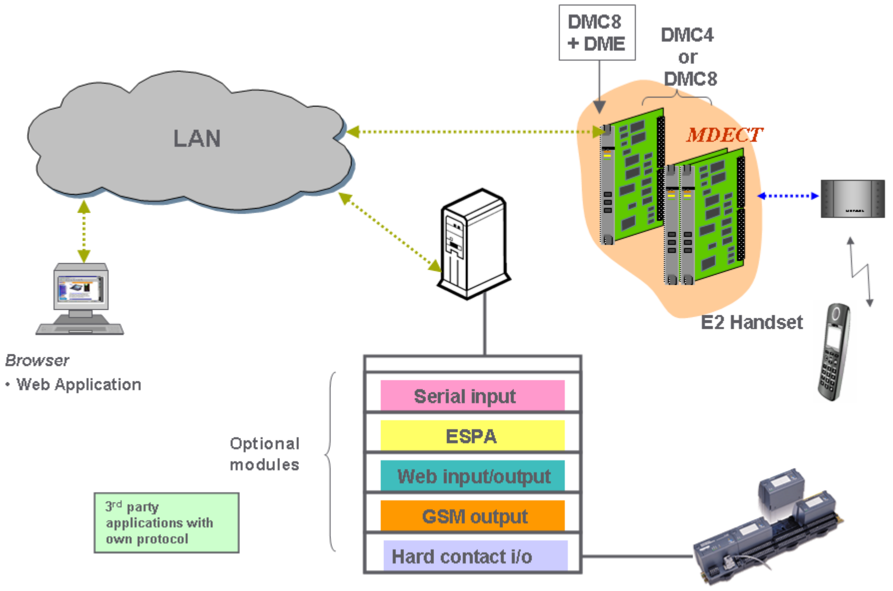
Messaging and Alarms

DECT Messenger provides text messaging from many different sources to various output devices, including DECT handsets. Messages can be sent from the following sources:

- external alarm systems, for example nurse call, building alarms, process control
- a mechanical system
- the web or email
- a DECT handset
- contact panels, door switches etc.

It is possible to send the messages to e-mail, pagers and GSM handsets as well as to DECT handsets, either as escalations if the DECT handset is not available or in parallel.

Figure 56
DECT Messenger connections



Engineering guidelines

Contents

This section contains information on the following topics:

System capabilities and limits

This section examines several issues surrounding DECT capabilities and limits. Information about system hardware and software parameters is also provided.

System concentration traffic

A DECT system without concentration supports a maximum number of 1024 handsets. With the concentration feature, in theory, the handset limit is 510 per DECT Mobility Card x 32 cards = 16320 handsets. However, in practice, traffic limits the number of handsets per card.

Each IPE card slot supports 32 channels of voice and data at the same time through the DS30X interface. Concentration removes the existing fixed ratio of 32 handsets per DMC.

Blocking

Calls in DECT can be blocked at many stages, including the following:

- At the basestation – when all channels (6 or 12) of an basestation are in use, calls through that basestation (both to and from a Portable Part [PP]) are rejected.
- At the Backbone interface – when the basestations of one DMC together have 32 radio connections, calls through those basestations (both to and from a handset) are rejected.
- At the IPE backplane interface – when all 32 speech channels to the DS30X interface on the a DMC8 are occupied, calls to and from handsets that have that specific DMC8 as their home DMC8 are rejected.
- At the Network interface – usually the IPE shelf connectivity is a blocking configuration, where the number of network timeslots provided for a shelf is less than the actual number of terminals configured on that shelf.

Traffic definitions

Busy hour traffic – Busy hour traffic is the hour of the day during which a telephone system carries the most calls, voice or data. The unit for busy hour traffic is the Erlang or Centi Call Second (CCS).

Erlang – One Erlang is equal to the continuous use of a circuit for one hour.

CCS – One hundred Call Seconds (CCS) or 100 seconds of continuous use of a circuit. Normally referred to as CCS per hour. For example, a call on a circuit for one hour is equal to 36 CCS.
(60 minutes x 60 seconds = 3600/100 = 36 CCS)

Blocking – A condition when a telephone call does not complete, and the calling party normally hears a busy signal.

Grade of Service – Grade of Service, given as a decimal fraction, indicates the probability of call blocking. For most applications, acceptable figures for blocking are between 0.01 and 0.03.

Traffic assumptions used for table calculations

The following are traffic assumptions used for table calculations:

- A handset that always has good radio contact with a basestation assumes that the radio deployment is acceptable.
- The Grade of Service used in all calculations is 1%.
- There is little or no overlap between basestations. (In practice, there is overlap, but to apply standard traffic calculations, it is necessary to simplify the calculation). For example, two 6-channel basestations in the same cell deliver a higher traffic flow.
- Ignore radio channels for handover. The traffic calculations allocate a slightly higher traffic capability to a basestation than it can have in practice.
- Blocking occurs at three main areas: the basestations, the backplane, and the network loops. The traffic calculations only use the Erlang values where blocking occurs. For example, if there are three areas each delivering 10 Erlangs, traffic calculations take the total traffic capability as 10 Erlangs, not as 30 Erlangs. Real traffic capacity in this example is possibly more than 10 Erlangs.
- Handset handover continues without interruption.
- Handsets are distributed equally between the system DMC cards.
- All calculations are based on resident handset users. Visiting handset users have a negligible effect on traffic. In unusual circumstances where a site has a large number of visiting handset users, traffic capacity can require adjustments.

System hardware parameters

Tables 3, 4, 5, and 6 detail the minimum and maximum configurations for DECT with the Concentration feature.

Table 3
Minimum configuration

System type	Shelves or cabinets	DMC8	DMC8-E	Basestation	Handset
All systems	1	1	0	1 to 8†	1 to 510†

†Due to number of Virtual TNs available. Subject to engineering rules and constraints.

Table 4
Maximum Large System configuration

System type	Shelves	DMC8	DMC8-E	Basestation	Handset
Large System	2	30	2	256†	16 320†

†Due to number of Virtual TNs available. Subject to engineering rules and constraints.

Table 5
Maximum Option 11 Cabinet configuration

System type	Cabinets	DMC8	DMC8-E	Basestation	Handset
Cabinet system without CPU cabinet	2	18	2	160†	640†
Cabinet system with CPU cabinet	2	17*	2	152†	640†
Chassis system	1**	3*	0	16†	640†
Chassis system (Expansion cabinet)	1**	3*	1	32†	640†

*One of the DMC8 positions in the CPU cabinet is required by the NTAK20 Clock Controller Daughterboard.

**DECT can only exist in one cabinet. The cabinets cannot be joined.

†Due to number of Virtual TNs available. Subject to engineering rules and constraints.

Table 6
Maximum CS 1000S configuration

System type	Cabinets	DMC8	DMC8-E	Basestation	Handset
the first Media Gateway	1***	3	1	32†	640†
all other Media Gateways	1***	4	0	32†	640†

†Due to number of Virtual TNs available. Subject to engineering rules and constraints.
***DECT can only exist in one Media Gateway. The Media Gateways cannot be joined.

If a cabinet or Media Gateway has a 9th slot, the slot must be provisioned with a DMC8-E card. All other cards are DMC8s.

The DECT system components have the following capacities:

- One NTCW00xx DMC8 or one NTCW01xx DMC8-E can support up to 8 basestations.
- One C4600 basestation can support 6 active calls.
- One C4610 basestation can support 12 active calls.
- One C4610E basestation can support 12 active calls.

Multiple DECT systems can co-exist in the same PBX system if they are synchronized to the same clock source. However, from a user perspective, the DECT systems are separate.

System software parameters

The software that operates the DECT system resides as firmware in the DMCs. The firmware consists of an operating program and a system database configuration. The operating program controls basestation and handset functions. The operating program also communicates with the system and the OTM DECT Manager. The system data defines hardware and hardware addressing.

The DMC8/DMC8-E with the ensuing software releases supports the following:

- Release 23 can support basic configuration, CLID and CPND, DECT card addressing within OA&M, and 16 users on each card.
- Release 24.2x can support up to 32 handsets on each card.

Release 25.xx can support up to 510 handsets with Concentration and MSMN.

DMC8 engineering guidelines

This section describes the recommended engineering guidelines for the installation of phantom powered basestations.

The optimum capacity mix of 6-channel and 12-channel basestations is six 6-channel and two 12-channel basestations. Using three or more 12-channel basestations per DMC8 is possible but is not an efficient use of the 32 channels of the DMC8.

Nortel recommends that the 12-channel basestations be distributed over the DMC8s.

Table 7 lists engineering guidelines for various deployments of phantom-powered basestations.

Table 7
DMC8 engineering guidelines for 6-channel RFP (basestation) and 12-channel RFP (basestation) (Part 1 of 2)

System	Number of basestations that can be phantom powered per shelf or cabinet	Total
Large System	eight 6-channel **or** six 6-channel + two 12-channel @ 0.5 km	128
	seven 6-channel **or** five 6-channel + two 12-channel @1.0 km	112
	seven 6-channel @ 1.7 km	112
	new basestations – any mix at 1.7 km	128
Cabinet	seven 6-channel **or** five 6-channel + two 12-channel @ 0.5 km	70
	six 6-channel **or** four 6-channel + two 12-channel @1.0 km	60
	six 6-channel @ 1.7 km	60
	new basestations – any mix at 1.7 km	80
Chassis	eight 6-channel **or** six 6-channel + two 12-channel @ 0.5 km	32
	eight 6-channel **or** six 6-channel + two 12-channel @ 1.0 km	32
	eight 6-channel @ 1.7 km	32
	new basestations – any mix at 1.7 km	32

Table 7
DMC8 engineering guidelines for 6-channel RFP (basestation) and 12-channel RFP (basestation) (Part 2 of 2)

System	Number of basestations that can be phantom powered per shelf or cabinet	Total
CS 1000S	eight 6-channel **or** six 6-channel + two 12-channel @ 0.5 km	32
	eight 6-channel **or** six 6-channel + two 12-channel @ 1.0 km	32
	eight 6-channel @ 1.7 km	32
	new basestations – any mix at 1.7 km	32

Using the maximum of eight basestations on a DMC8 imposes engineering restrictions on the remaining slots, as listed in Table 8.

Table 8
DMC8 Ordering Tool – system slot restrictions for different basestation lengths (Part 1 of 2)

System	Basestation average line length	Required number of unoccupied slots
Large System	0.5 km	no restrictions
	1.0 km	for every 1 – 15 slots, one slot must be unoccupied
	1.7km	for every 1 – 6 slots, one slot must be unoccupied
Cabinet	0.5 km	for every 1 – 9 slots, one slot must be unoccupied
	1.0 km	for every 1 – 8 slots, one slot must be unoccupied
	1.7km	for every 1 – 15 slots, one slot must be unoccupied
Chassis	0.5 km	no restrictions
	1.0 km	no restrictions
	1.7km	no restrictions

Table 8
DMC8 Ordering Tool – system slot restrictions for different basestation lengths (Part 2 of 2)

System	Basestation average line length	Required number of unoccupied slots
CS 1000S	0.5 km	no restrictions
	1.0 km	no restrictions
	1.7km	no restrictions

Netprice Order Tool

The Netprice Order Tool makes certain approximations in provisioning DMC8. This provides a simplified configuration that meets the needs of most sites.

DECT on Large Systems

The Order Tool allows the first 80 basestations to be phantom powered. When more than 80 basestations are requested, the extra basestations are assumed to be local powered. Power adapters are provided as follows:

- C4610 ac adapters
  = (sum of 6-channel and 12-channel basestations) – 80
- Adapters must be purchased separately

Note: Because it is not possible to determine how the cards are spread over the two shelves, it is assumed that there are 80 phantom powered basestations per system.

DECT on Cabinet system

The Order Tool allows the first 40 basestations to be phantom powered. When more than 40 basestations are requested, the extra basestations are assumed to be local powered. Power adapters are provided as follows:

- C4610 ac adapters
  = (sum of 6-channel and 12-channel basestations) – 80
- Adapters must be purchased separately

DECT on Chassis system

All basestations can be powered from the cabinet power supply.

DECT on CS 1000S

All basestations can be powered from the Media Gateway power supply.

Rules with new basestations

With the new basestations, the provisioning rules are relaxed to allow the maximum number of basestations to be provisioned for each shelf, without the requirements.

Basestation combinations for handsets on a DMC8

Low traffic for a 0.1 Erlang capacity

Table 9 shows the 6-channel and 12-channel basestation combinations required to support a maximum number of handsets on a DMC card. The calculations are based on each handset generating 0.1 Erlangs of traffic.

Table 9
Number of handsets for a 0.1 Erlang capacity

		Number of 12-channel basestations								
		0	1	2	3	4	5	6	7	8
Number of 6-channel base stations	0	0	58	117	176	176	220	220	220	220
	1	19	77	136	195	220	220	220	220	
	2	38	97	155	214	220	220	220		
	3	57	116	174	220	220	220			
	4	76	135	194	220	220				
	5	95	154	213	220					
	6	114	173	220						
	7	133	192							
	8	152								

Medium traffic for a 0.15 Erlang capacity

Table 10 shows the 6-channel and 12-channel basestation combinations required to support a maximum number of handsets on a DMC card. The calculations are based on each handset generating 0.15 Erlangs of traffic.

Table 10
Number of handsets for a 0.15 Erlang capacity

		Number of 12-channel basestations								
		0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**
Number of 6-channel base stations	**0**	0	39	78	117	146	146	146	146	146
	1	12	51	91	130	146	146	146	146	
	2	25	64	103	143	146	146	146		
	3	38	77	116	146	146	146			
	4	50	90	129	146	146				
	5	30	102	146	146					
	6	76	115							
	7	89	128							
	8	101								

High traffic for a 0.2 Erlang capacity

Table 11 shows the 6-channel and 12-channel basestation combinations required to support a maximum number of handsets on a DMC card. The calculations are based on each handset generating 0.2 Erlangs of traffic.

Table 11
Number of handsets for a 0.2 Erlang capacity

		Number of 12-channel basestations								
		0	1	2	3	4	5	6	7	8
Number of 6-channel base stations	0	0	29	58	88	110	110	110	110	110
	1	9	38	68	97	110	110	110	110	
	2	19	48	77	107	110	110	110		
	3	28	58	87	110	110	110			
	4	38	67	97	110	110				
	5	47	77	106	110					
	6	57	86	110						
	7	66	96							
	8	76								

Superloop and IPE shelf calculations

Table 12 shows the maximum number of handset users on a DMC8 card for varying traffic levels.

Table 12
Handset capacity/DMC8 for Superloop/IPE

Superloops per IPE shelf	Low traffic 0.1 Erlang	Medium traffic 0.15 Erlang	High traffic 0.2 Erlang
2	138 handsets/DMC	92 handsets/DMC	69 handsets/DMC
1	69 handsets/DMC	46 handsets/DMC	34 handsets/DMC
0.5	34 handsets/DMC	23 handsets/DMC	17 handsets/DMC
Cabinet system	220 handsets/DMC	146 handsets/DMC	110 handsets/DMC

Note: Superloops do not apply to Chassis systems or CS 1000S systems.

Simplified guidelines

Use Table 12 to calculate the superloop capacity.

Low traffic example of one superloop on each IPE shelf

- Sixty-nine (69) handsets per DMC8 card x 16 DMC8 cards per shelf = 1104 (1000)

Medium traffic example of one superloop on each IPE shelf

- Forty-six (46) handsets per DMC8 card x 16 DMC8 cards per shelf = 736 (750)

High traffic example of one superloop on each IPE shelf

- Thirty-four (34) handsets per DMC8 card x 16 DMC8 cards per shelf = 544 (500)

Site planning

Contents

This section contains information on the following topics:

Overview

Site planning starts with a site survey and ends with deployment. The site survey process is an information gathering process. The information received in the site survey determines customer requirements and the number of cells required to support traffic.

Deployment is the process of locating basestations at the site. The module titled “Installing the basestation” on page 283 contains general information about the deployment process. This module includes information about a key piece of deployment equipment, the DECT Radio Deployment Tool. The section titled “Preparing the tool for deployment” on page 218 explains how to prepare equipment for deployment.

Other modules describe in detail the procedures related to deployment. These procedures vary according to site details and user requirements.

Site survey

The site survey begins by researching the customer requirements. The research identifies a variety of information such as contact names, the number of handset users, and building details.

Customer requirements

The customer must provide:

a a site contact name and telephone number;

b site plans;

c building details;

d information on available house cabling;

e radio coverage requirements; and,

f number of users.

On-site contact

The on-site contact provides:

a time and date scheduling;

b access to restricted or locked areas; and,

c additional information when required.

Site plans

A complete set of site plans are required. Dimensions must be clearly stated on the plans.

Building details

System deployment and installation depends upon the following building details.

- Building identification
- Construction materials, such as walls, floors, ceilings
- Type of use, such as an office, hotel, factory, or store
- Dimensions
- Number of floors
- Height of floors
- Partitioning of floors

Position and use of available cabling

Cables that connect the basestation to the DECT system must meet or exceed the UTP Cat 3 standard. Nortel recommends UTP Cat 5, as it provides a greater line length before signal degradation occurs. New cabling is required if the existing cabling does not meet the standard.

Radio coverage

A basestation coverage list is required to indicate:

a areas where radio coverage is required;

b areas excluded from radio coverage due to the proximity of sensitive electronic equipment;

c areas where radio coverage is not required;

d areas where radio coverage is not feasible or requires specific basestations;

e objects inside buildings; and,

f details of furniture, cupboards, and machinery on every floor of the building

Basestation installations can be required to be out of sight. A customer can request basestations to be mounted in unsuitable locations, such as stone columns, air ducts or horizontally on the ceiling. Radio coverage cannot be guaranteed when basestations are mounted in unsuitable locations.

Know in advance where coverage is required. Some examples of coverage areas are:

- elevators
- stairwells
- toilets
- outdoor areas

Number of handset users

The following information must be available.

1. The number of handset users
2. The potential growth of handset users
3. The areas of above average and below average traffic density Number of cells required to support traffic

Traffic requirements are determined for each cell. The deployer calculates system requirements to support user traffic.

Customer review

After the site survey and before the deployment process, the person deploying the site must review coverage requirements with the customer representative. The person deploying the site must explain to the customer representative how the survey is conducted. The customer representative must tell fellow employees that a person deploying the site is taking measurements in their work place.

Site survey example

The site survey process is an information gathering process. The information received in the site survey determines customer requirements and the number of cells required to support traffic.

A normal site survey

The site survey process includes gathering:

1. Survey materials
2. Site contact information
3. Site plans or maps
4. Building information
5. Existing cable information
6. Basestation radio coverage information
7. Handset user information
8. Reviewing the work

Methods and examples for surveying more detailed sites are shown in the Detailed Site Planning section of this guide. Use one or more of the following surveying methods in the site survey:

- Single floor
- Subsequent system installation
- High handset density area
- Multiple systems installation

Site planning example: Able-Studio

This section describes a site survey for Able-Studio, a fictitious company. Follow this example to conduct the site survey.

The facts for Able-Studio

- The contact is Rolf Sundby at 555-0000. A guest lab coat is necessary to be on the site. Get this lab coat from Rolf.

- The sales representative has recommended DECT.
- The location of the user offices (and their wired telephones) often changes within the coverage area.
- Not all users have offices and desk telephones. Some users only have handsets.
- The customer does not need coverage in the toilet facility.
- The telephone switch room is next to the toilet facility.
- The customer has no installation restrictions.

The site survey process for Able-Studio

The technician must gather the following information to conduct a site survey:

1. Gather survey items, page 188
2. Identifying site contacts, page 189
3. Obtaining site plans, page 190
4. Gathering building information, page 191
5. Identifying existing cabling, page 192
6. Assessing radio coverage, page 193
7. Profiling handset use, page 194

Gather survey items

Obtain the following items before beginning the site survey. The items are not customer supplied.

- Pick up the DECT tool kit (consisting of tripod and deployment tool kit).
- Get the appropriate DECT Provisioning Record.
- Gather a pencil, an eraser, a ruler, and coloured pencils.

Identifying site contacts

Gather the following information and enter it into the work-order and the Provisioning records. The installer requires the following information.

Procedure 1
Identifying site contacts (Part 1 of 2)

Step	Action
1	Get the company name.
	Record this information.
2	Get the company address.
	Record this information.
3	Contact name.
	Record this information.
4	Obtain the contact telephone number.
	Record this information.
5	Obtain scheduling times and date.
	Record this information.
6	Access to controlled areas.
	Record this information.
7	Obtain any keys or codes needed for secured site areas where radio coverage is required.
8	Obtain additional contact information, if required.
	Record this information.

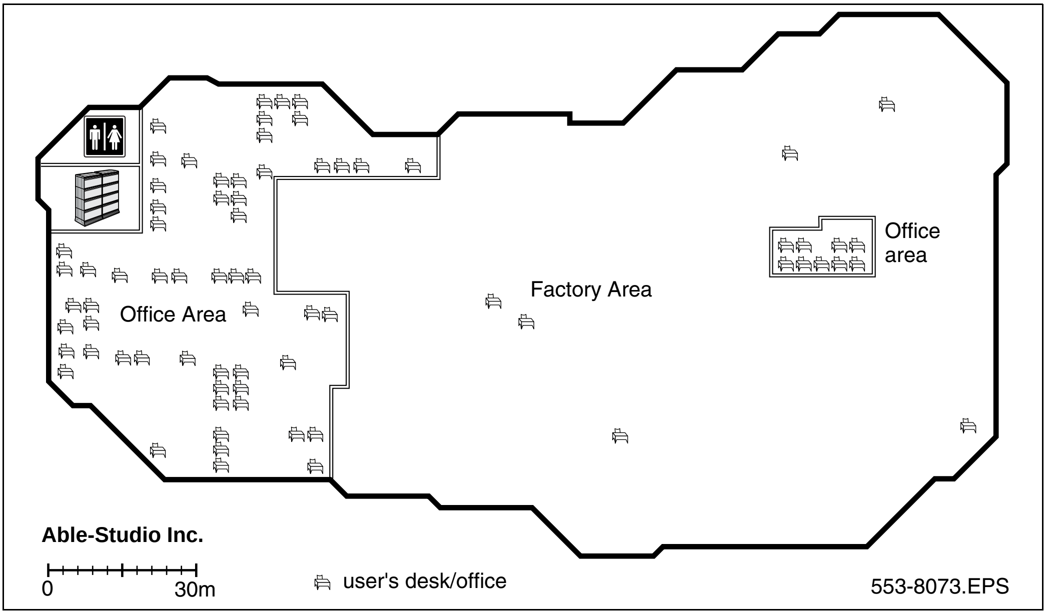
Procedure 1
Identifying site contacts (Part 2 of 2)

Step	Action
9	Obtain any required safety equipment, such as a hard hat or safety glasses.
10	Find out if there is an another DECT system within the radio coverage area.
	Record this information.
	END

Obtaining site plans

Obtain two scaled plans. The scale is required to check wiring distances from the controller to the basestations. The scale is in the form of a measured line so that it remains in proportion to the floor plan through reduction copiers.

Figure 57
Example of a site coverage floor plan



Procedure 2
Obtaining site plans

Step	Action
1	Obtain two site plans/maps, with dimensions marked.
	One working copy to identify critical points, cell centres, and cell boundaries. One clean copy to attach to the site Provisioning Record for the installer, customer, or maintenance.

END

Gathering building information

Gather the following information and enter it into the work-order.

Procedure 3
Gathering building information (Part 1 of 2)

Step	Action
1	Obtain building identification.
	Record this information.
2	Obtain information on construction materials, such as walls, floors, ceilings.
	Record this information.
3	Note the type of use of facilities, such as office, hotel, factory, store.
	Record this information.
4	Find the number of floors.
	Record this information. If the building contains atriums, multiple floors, floors not all the same shape or any unusual conditions, see “Multiple floor deployment” on page 245.
5	Find the height of floors.

Procedure 3
Gathering building information (Part 2 of 2)

Step	Action
	Record this information.
6	Ask about the partitioning of floors.
	Record this information.
7	Discuss the details of furniture, cupboards, and machinery in the interior of buildings on every floor.
	Record this information.
8	Ask about other building details, as necessary.
	Record this information.
	END

Identifying existing cabling

Gather the following information and enter it into the work-order.

Procedure 4
Identifying existing cabling

Step	Action
1	Obtain the location of the telephone switching room.
	Determine the total length of the cable.
2	Ask about the existing cabling for basestation to MDF wiring.
	Wiring from the basestation to the shelf or cabinet must be at least UTP Cat 3. Nortel recommends UTP Cat 5, as it provides greater line length before signal degradation occurs.
3	Review the possibility of new UTP Cat 5 cabling required.
	If the cabling is not at least UTP Cat 3, have UTP Cat 5 installed.
	END

Assessing radio coverage

> ***Note:*** If the customer requires the basestations be installed out of sight, this can reduce the coverage capability of each basestation. It can limit the performance of the system and substantially increase the cost.

Gather the following information and enter it into the work-order.

Procedure 5
Assessing radio coverage (Part 1 of 2)

Step	Action
1	Inquire about areas where radio coverage is required.
	Record this information.
2	Ask about areas where radio coverage is not required.
	Record this information.
3	Ask about external or outdoor radio coverage.
	Record this information.
4	Discuss areas where radio coverage is not feasible or requires specific basestations.
	Record this information.
5	Discuss areas excluded from radio coverage due to the proximity of sensitive electronic equipment.
	Record this information.
6	Ask about objects inside buildings that can affect radio coverage.
	Record this information.
7	Discuss unsuitable basestation locations, such as stone columns, air ducts or horizontally on the ceiling.
8	Discuss what basestations are to be installed out of sight.
	Discuss with the customer. See the preceding note.

Procedure 5
Assessing radio coverage (Part 2 of 2)

Step	Action
9	Inquire about areas of special coverage, such as, elevators, stairwells, toilets.

END

Profiling handset use

Areas of above average traffic density can have a low number of incumbent users but many incoming users. These can include areas such as cafeterias, restaurants, canteens, and meeting room areas where handset users tend to gather.

A further example of above average traffic density is an environment where all occupants of a given area are provided with handsets. This area requires special planning.

Areas of below average traffic density are areas infrequently accessed by users, such as store rooms and maintenance areas.

Obtain the following information and enter it into the work-order.

Procedure 6
Profiling handset users (Part 1 of 2)

Step	Action
1	Document the number of handset users.
	Record this information.
2	Get an estimate of the potential growth of handset users.
	Record this information.
3	Locate areas of above average and below average traffic density.

Procedure 6
Profiling handset users (Part 2 of 2)

Step	Action
	Record this information. See the preceding note.
4	Determine which users have a wired telephone in their office.
	Record this information.
5	Determine the locations of user offices.
	Record this information.
6	Ask about the mobility of the users. For example, do the users move from cell to cell, or is the area of movement restricted, such that the users remain within one cell?
	Record this information.

END

Deployment

A deployment determines the locations of basestations and cells. The deployment process consists of the following steps.

- Identifying initial critical points on the floor plan (page 195).
- Locating cell centres (page 196).
- Determining cell boundaries (page 198).
- Identifying critical points and cell boundaries (page 199).
- Marking the points, centres, and boundaries on the floor plan (page 200).

Identifying initial critical points on the floor plan

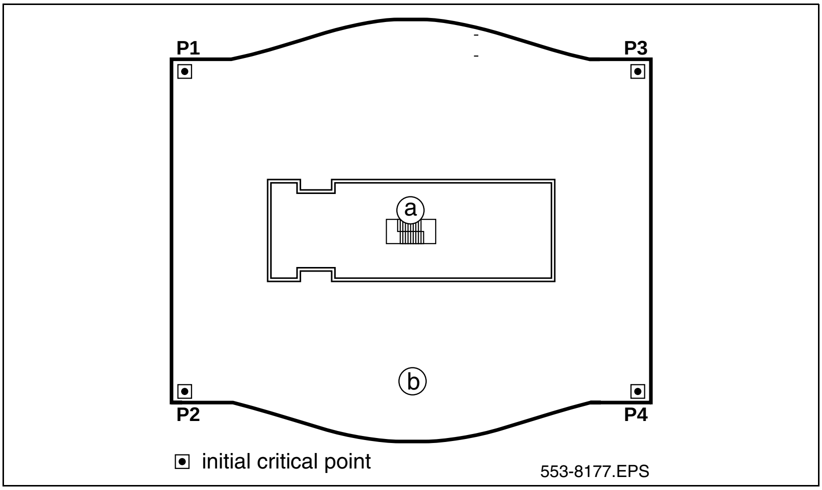
A critical point is a place that can be difficult for the radio signal to reach, such as a corner of a room, lifts and stairwells. Initial critical points are shown in Figure 58 as P1, P2, P3, and P4.

Figure 58 shows the following:

a stairwell

b second floor plan

Figure 58
Critical points



Locating cell centres

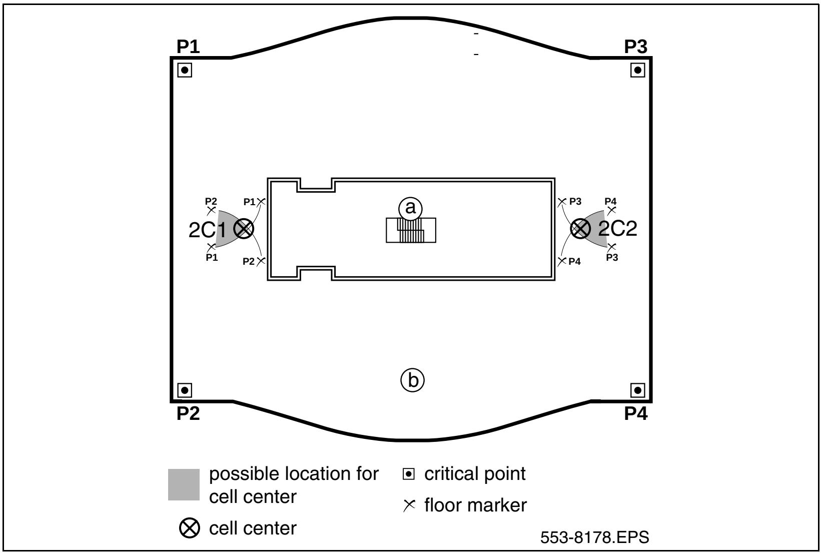
Figure 59 on page 197 shows the following:

a stairwell

b second floor plan

A cell centre is located by placing the deployment tool at one critical point, for example P1, then using the deployment handset to obtain a change in audio quality. The audio quality change determines the cell boundary contour. This process is repeated at an adjacent critical point, for example P2. Where the cell boundaries of both critical points meet is the cell centre. The cell centre position is marked on a floor plan. The cell centre determines the location of a basestation, shown in Figure 59 on page 197, as arc 2C1.

Figure 59
Cell centres



Rules and guidelines for selecting cell centres

Comply with the following when selecting cell centres.

- Ensure that the installation complies with local electrical codes.
- Install basestations indoors where there is no condensation and the temperature remains between 0°C and 50°C.
- Install basestations within 1500 metres of the MDF. Wiring from the basestation to the shelf or cabinet must be at least UTP Cat 3. Nortel recommends UTP Cat 5, as it provides a greater line length before signal degradation occurs.
- Position basestations upright on walls. Basestations must be at least 30 centimeters from the ceiling.
- Position basestations at least 1 m from large concrete or stone columns and from any major building structural members such as support beams or columns.
- Position the basestations high enough to clear obstructions between the basestations and the cell edge close to the ceiling.

- Mount the basestations clear of obstacles such as pipes or ducts.
- Do not install basestations in spaces that transport air, such as ducts or plenums.
- Do not mount basestations on the ceiling.

Determining cell boundaries

A specific RSSI value on the handset defines the cell boundary range. Links can be made outside the cell boundary but the audio quality of the link is poor. The link drops when the handset and the basestation are too far apart.

As shown in Figure 60, the cell boundary is the furthest point from the cell centre where a clear radio signal can be heard.

The range from the cell centre to the cell boundary, or the distance to a potential cell centre from a critical point, is determined by using the cell boundary value and the deployment tool.

Figure 60
Cell boundary terminology

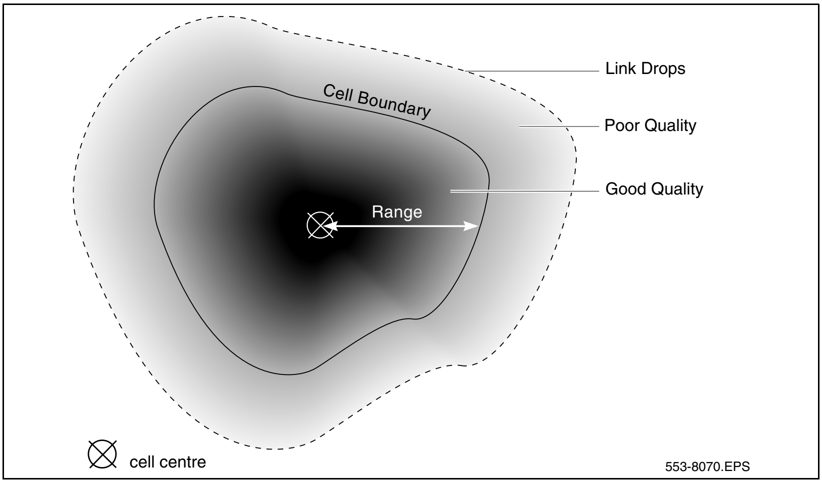
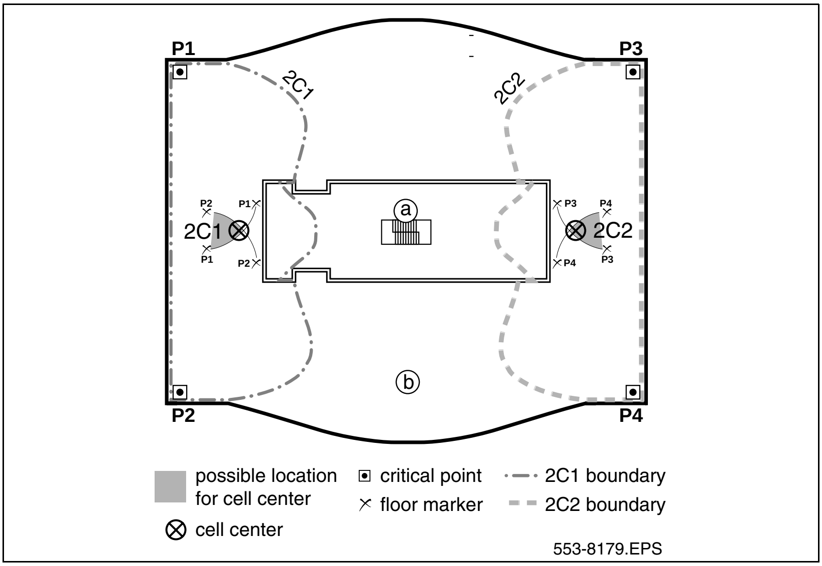


Figure 61 shows the following:

- **a** stairwell
- **b** second floor plan

A cell boundary for the cell centre is determined by placing the deployment tool at the cell centre, for example 2C1, and using the deployment handset to establish the cell boundary. The cell boundary contour is marked on the floor plan, and shown in Figure 61 by a dash-dot line.

Figure 61
Cell boundaries



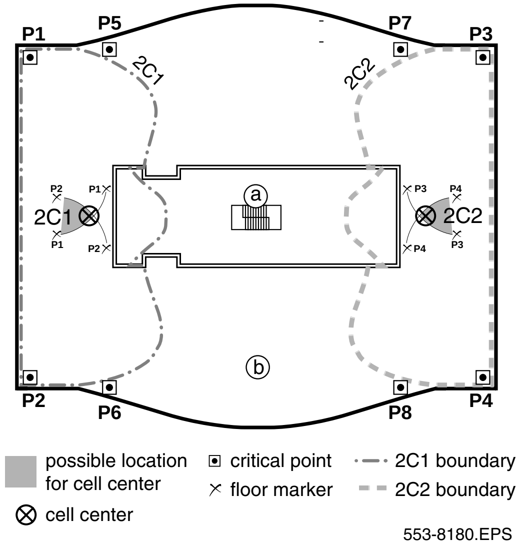
Identifying critical points and cell boundaries

Figure 62 on page 200 shows the following:

- **a** stairwell
- **b** second floor plan

Additional critical points, shown in Figure 62 on page 200 as P5, P6, P7, and P8, are identified to ensure basestation radio coverage for the entire area.

Figure 62
Additional critical points and cell boundaries



Marking the points, centres, and boundaries on the floor plan

This section describes how to label critical points, cell centres, and cell boundaries on the floor plan.

Mark the information clearly on the floor plans during the survey. The customer, the sales group, the installer, and maintenance personnel must read these floor plans.

Use a different colour for each cell. Use the same colour for each cell centre and its corresponding cell boundaries. Indicate the information on the floor plan as follows:

- **critical points** – mark ⊡ on the floor plan.
- **cell centres** – mark ⊗ on the floor plan.

- **cell centre** - label each as xCn where x is the floor and n is the next sequential cell centre.
- **cell boundaries** – mark wide, coloured lines on the floor plan.

For example, label a cell centre on the second floor as 2C3. The 2 before the C indicates that the cell centre is on the second floor. The 3 after the C indicates that this cell is the third cell in sequence in the site planning process.

Table 13
Example cell labels

Floor	Cell label
First floor	2C1, 2C2, 2C3
Ground floor	1C1, 1C2, 1C3
Basement level one	–1C1, –1C2, –1C3
Basement level two	–2C1, –2C2, –2C3

Figure 63
Example cell boundaries

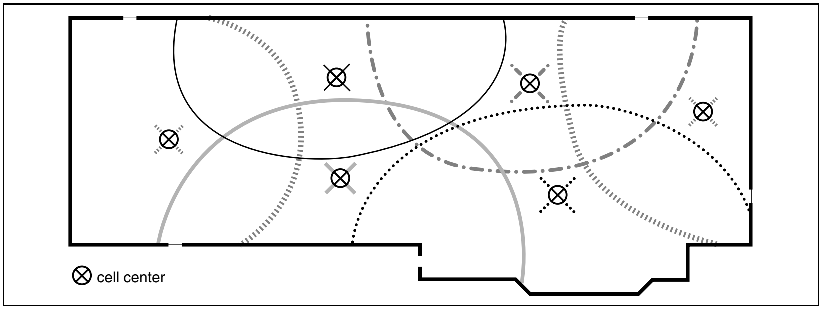


Figure 64
Points, centres, and boundaries on the floor plan

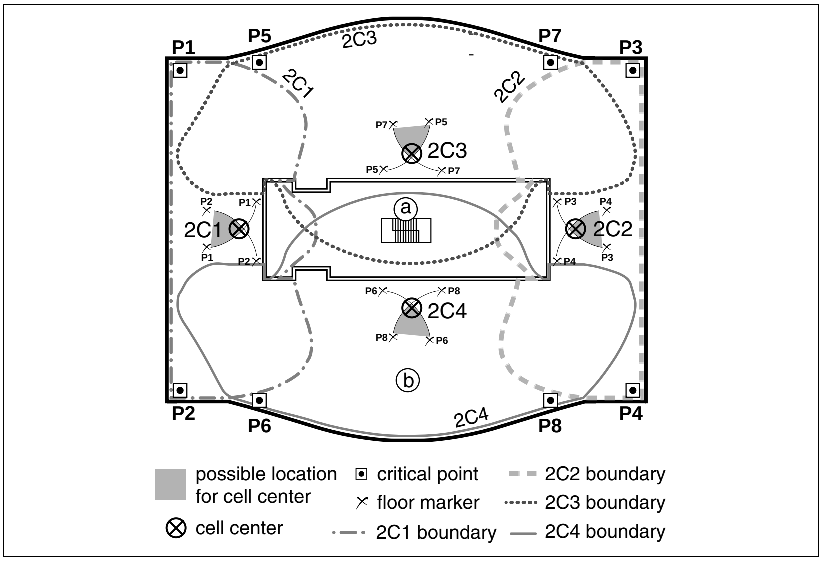


Figure 64 shows a typical floor plan marked-up after determining subsequent cell boundaries. The completed floor plan would appear as follows:

- Initial critical points are shown at P1, P2, P3, and P4.
- Cell centres are located where arcs from P1/P2, P3/P4 intersect.
- 2C1 and 2C2 show cell centres or basestation locations.
- Dashed and dotted lines show cell boundaries.
- Additional critical points are shown at P5 P6 P7 P8.
- 2C3 and 2C4 cell centres provide full coverage of the floor.

Two copies of the floor plan are required. One copy is used during the site planning. The second copy is marked with the information from the site planning copy and attached to Provisioning records, page 277 for the installer.

Deployment illustrations

The illustrations shown in Figures 65 through Figure 79 on page 211 represent the deployment process from start to finish.

Figure 65
Example of initial critical points

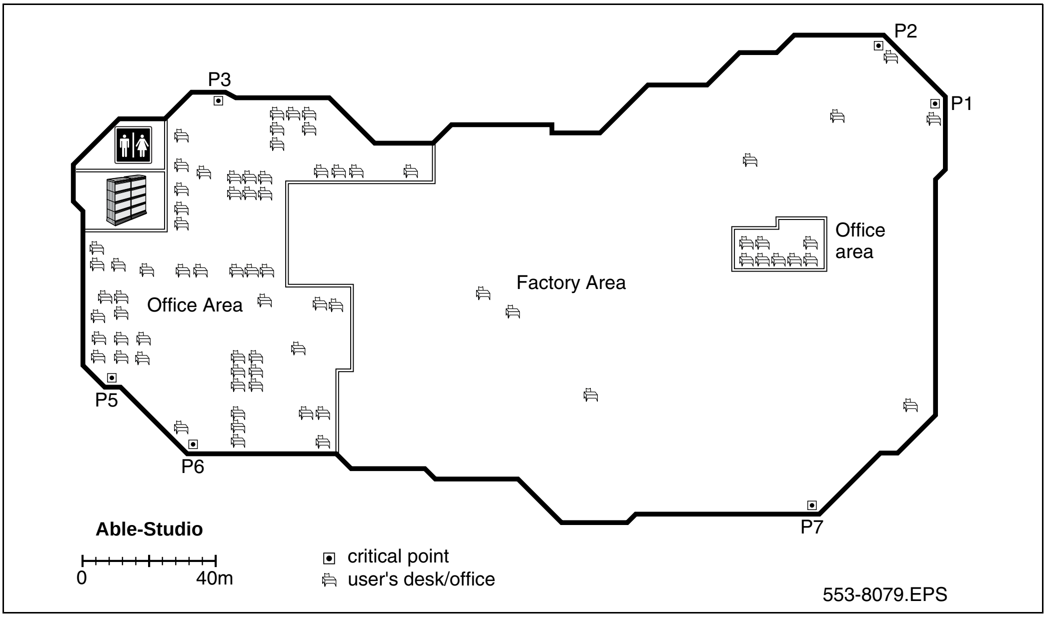


Figure 66
Cell contour of the initial critical point

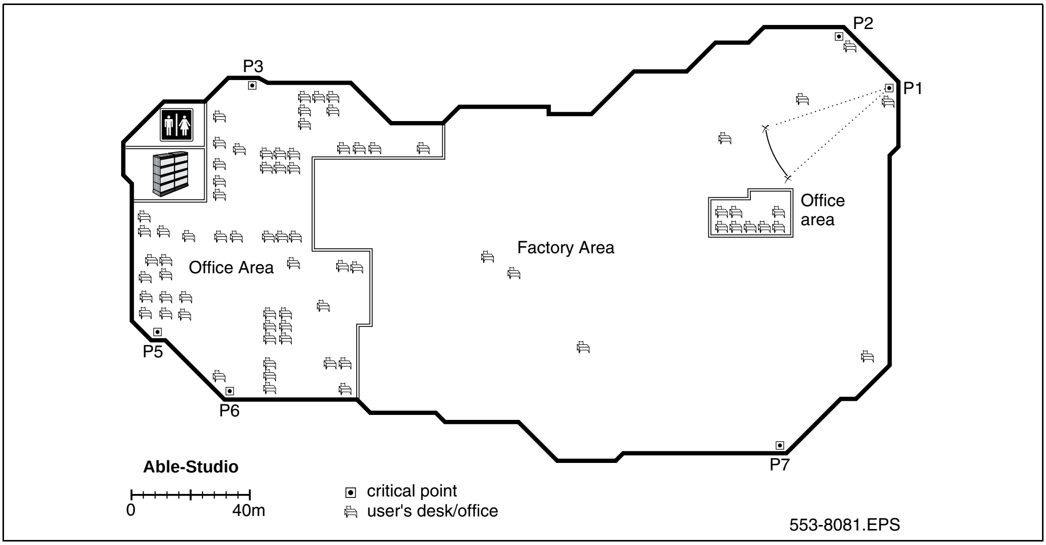


Figure 67
Cell contour of the closest adjacent critical point to the initial critical point

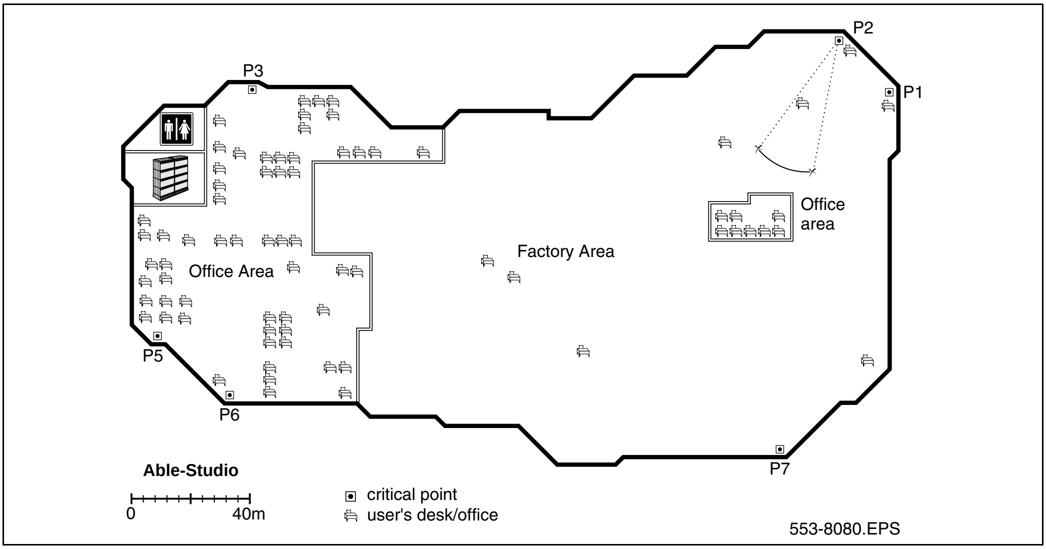


Figure 68
Example of a cell centre

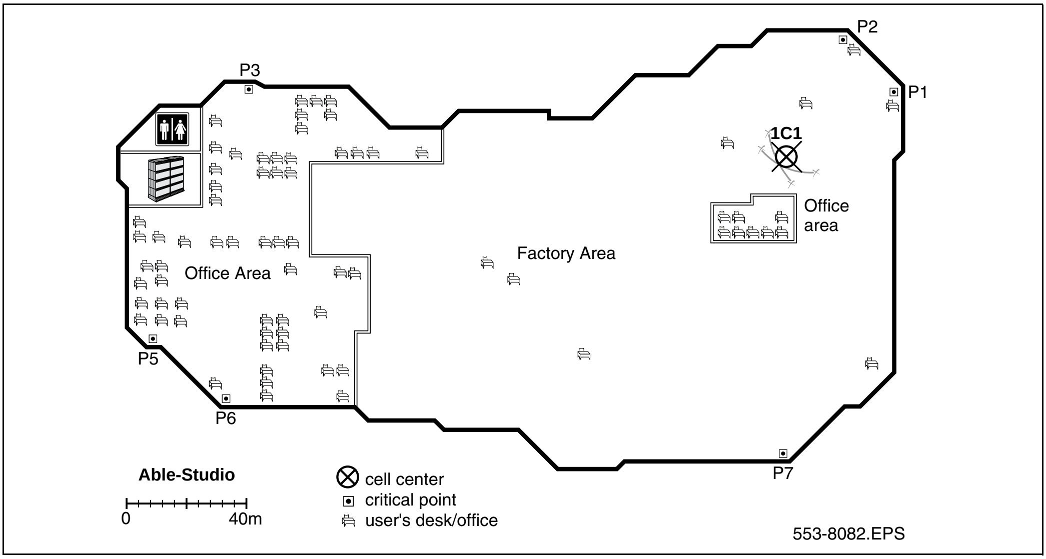


Figure 69
Example of a cell centre boundary

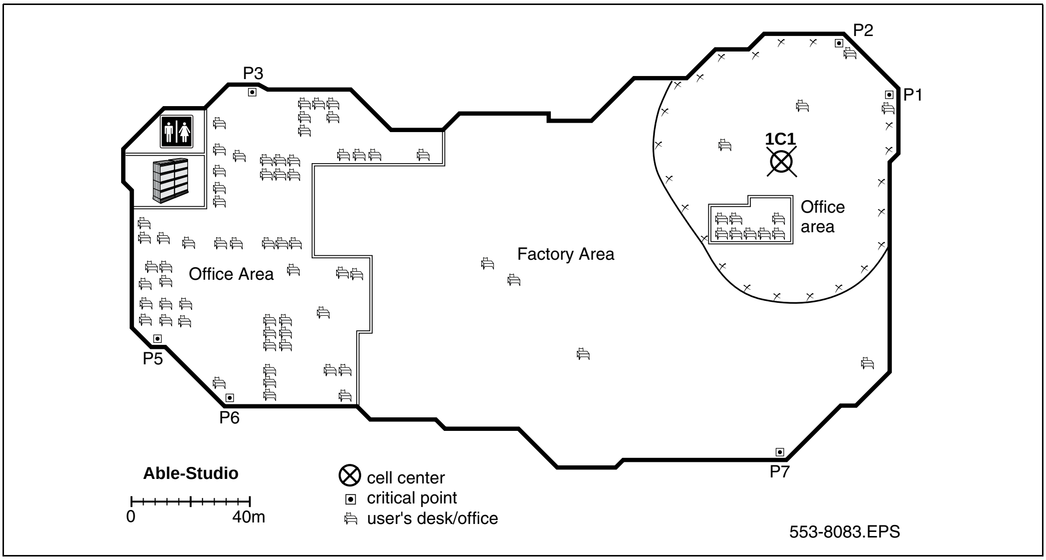


Figure 70
Example of new critical points (P8 and P9)

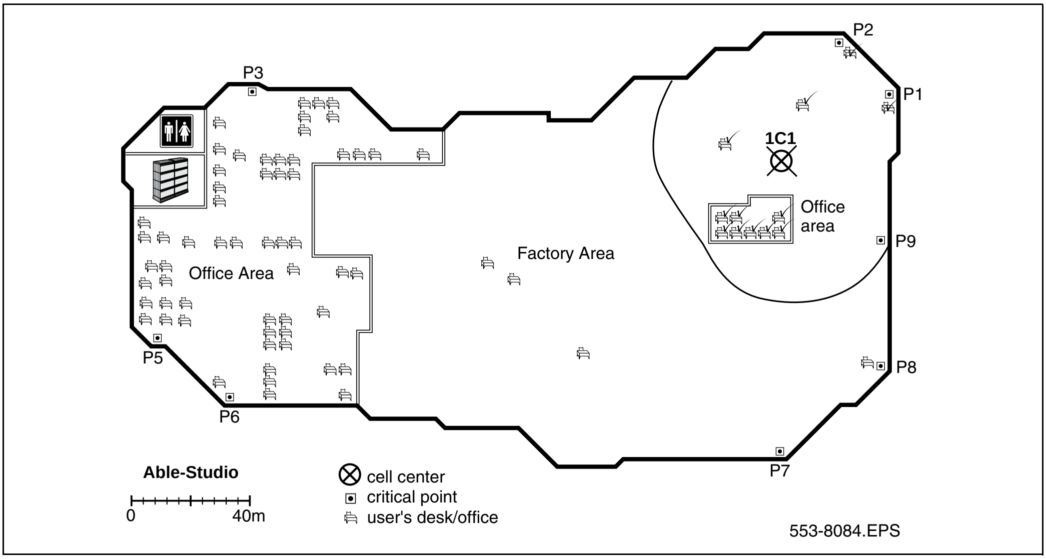


Figure 71
Example of deployment for cell centre 1C2

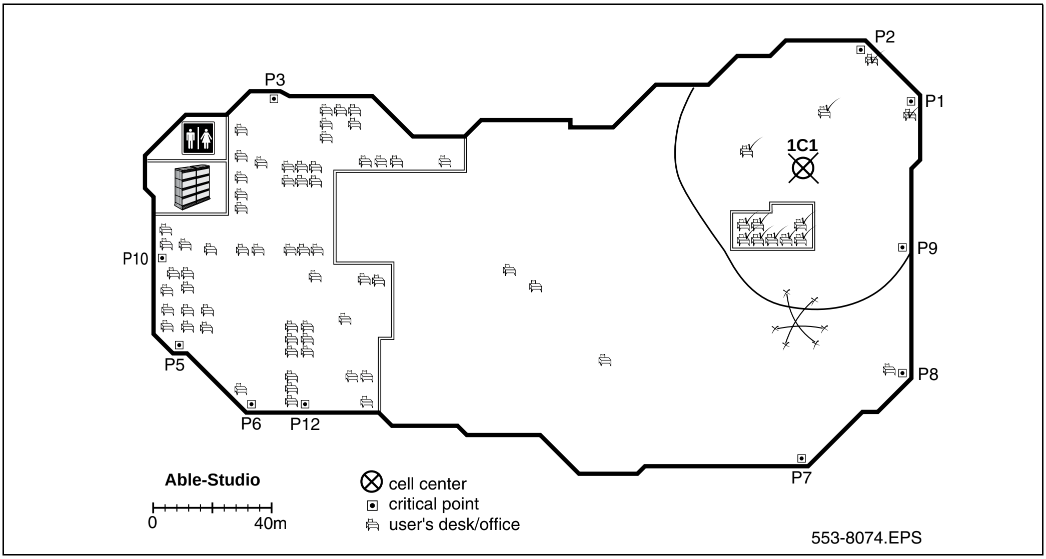


Figure 72
Example of deployment for cells 1C3 and 1C4

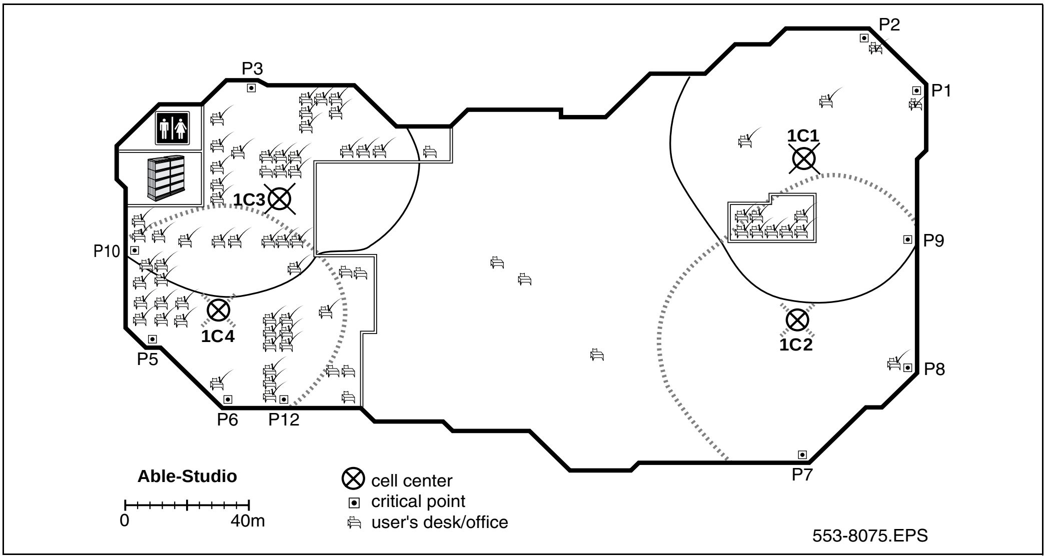


Figure 73
Identify new critical points (P11, P12, P13, P14, P15, P16, P17)

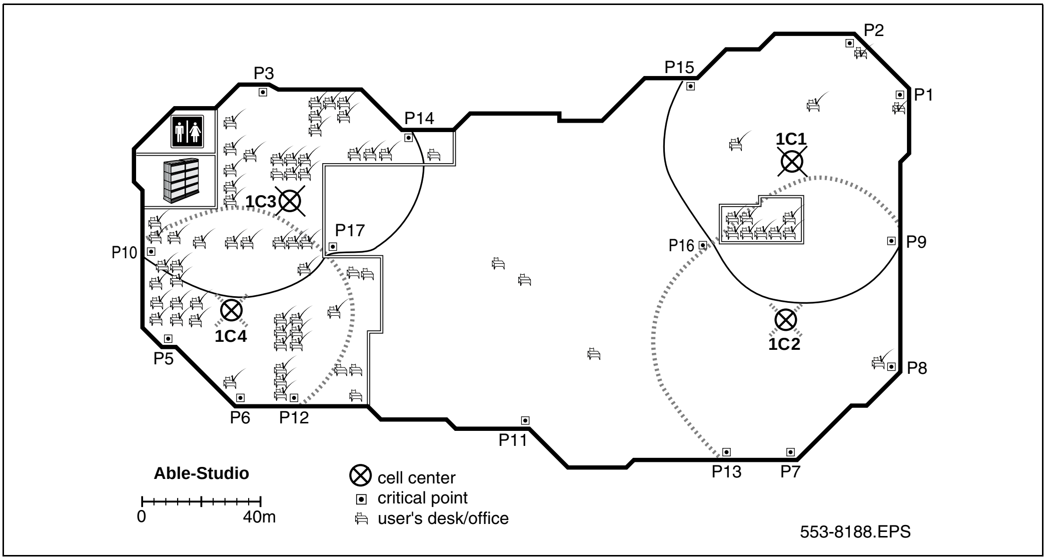


Figure 74
Contours formed by critical points P11, P13 and P16

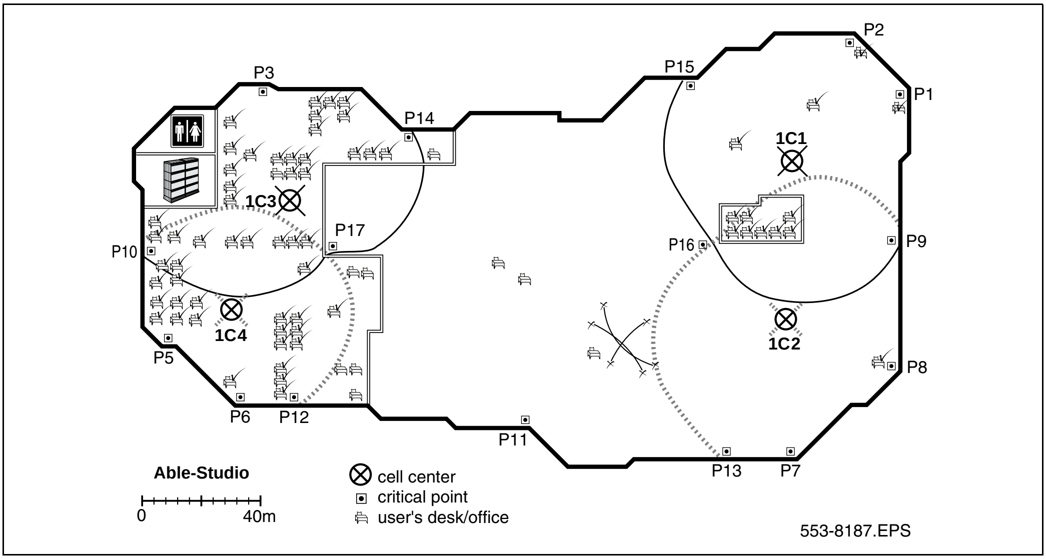


Figure 75
Cell centre 1C5 formed by critical points P11, P13 and P16

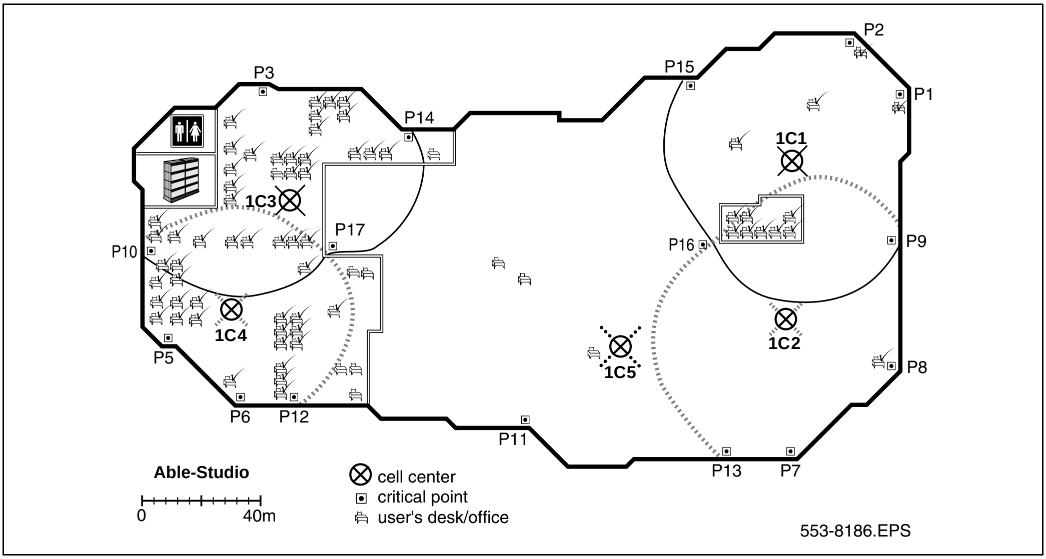


Figure 76
Cell boundary 1C5 formed by critical points P11, P13 and P16

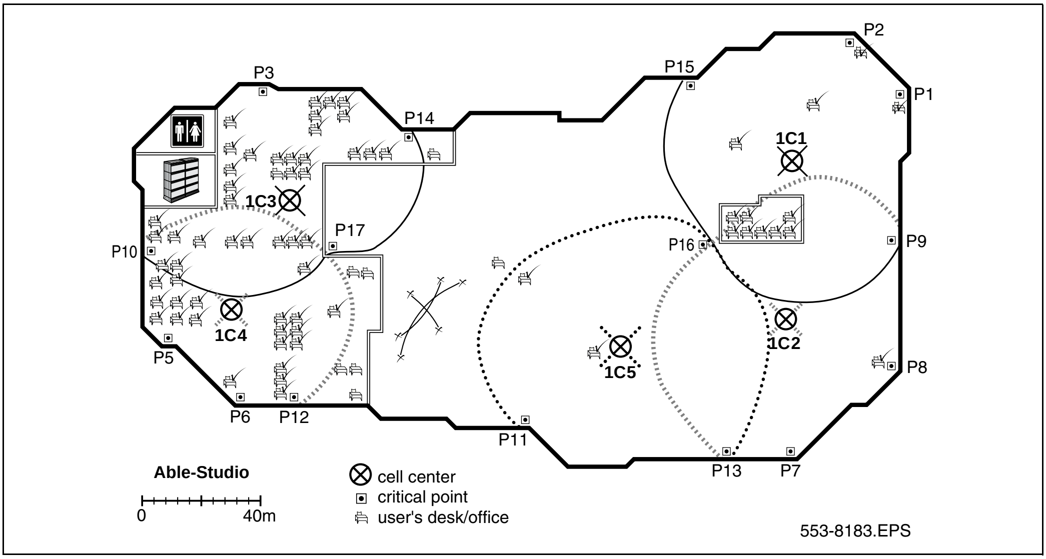


Figure 77
Example of critical point cell boundaries

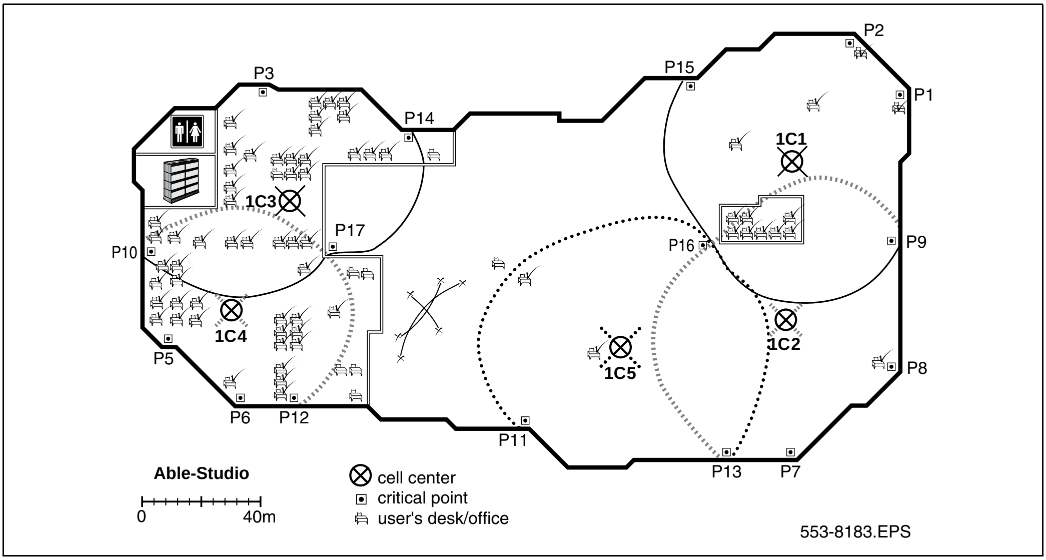


Figure 78
Example of cell centre boundary 1C6

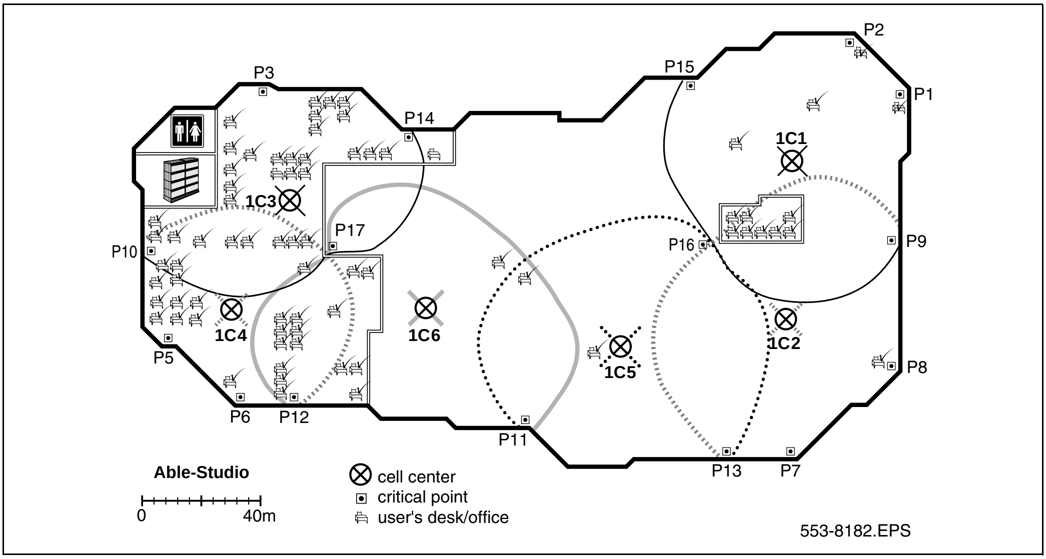
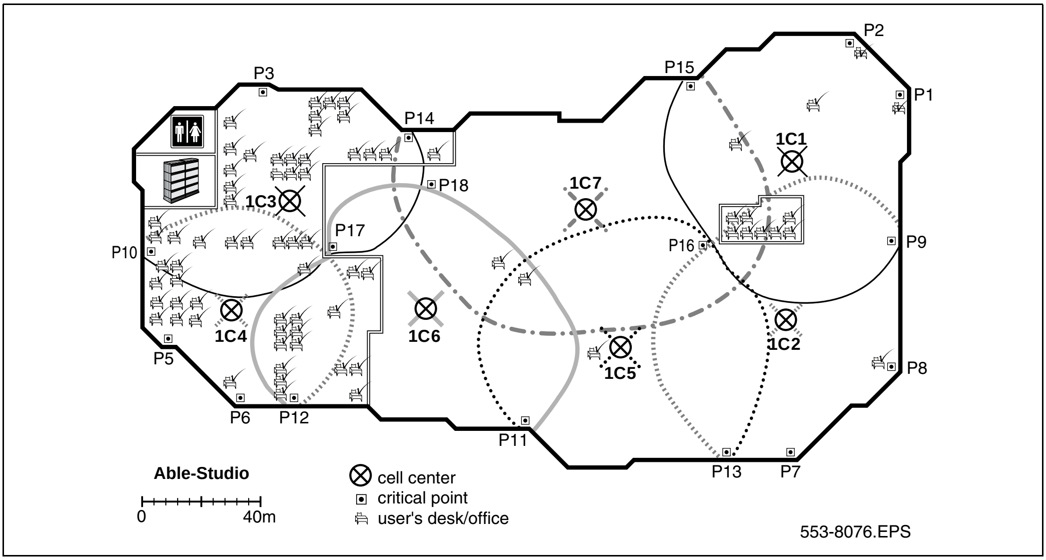


Figure 79
Example of a floor plan showing complete radio coverage



Deployment terms

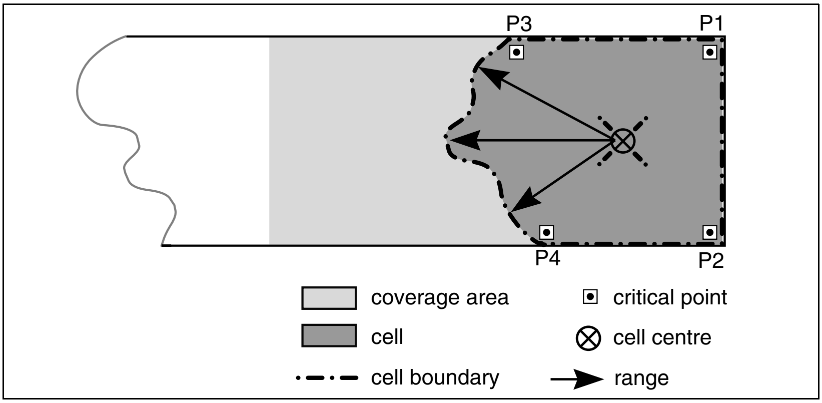
Terms associated with deployment are listed in the following table.

Table 14
Deployment terms

Term	Definition
Coverage area	An area where a handset can be used to make and receive calls.
Cell	The coverage area provided by the basestation antennas.
Cell boundary	The parameter of a cell coverage area.
Critical point	A point or location defined as the extreme corner of a coverage area that can be difficult for the radio signal to reach.
Cell centre	The installation point of the basestation serving the cell.
Range	The distance from a cell centre to its cell boundary.
Traffic table	Traffic tables record site traffic information from the floor plan and the customer. The traffic table helps to determine the required number of basestations for each cell.

The following figure, Figure 80, illustrates these terms.

Figure 80
Example showing deployment terms



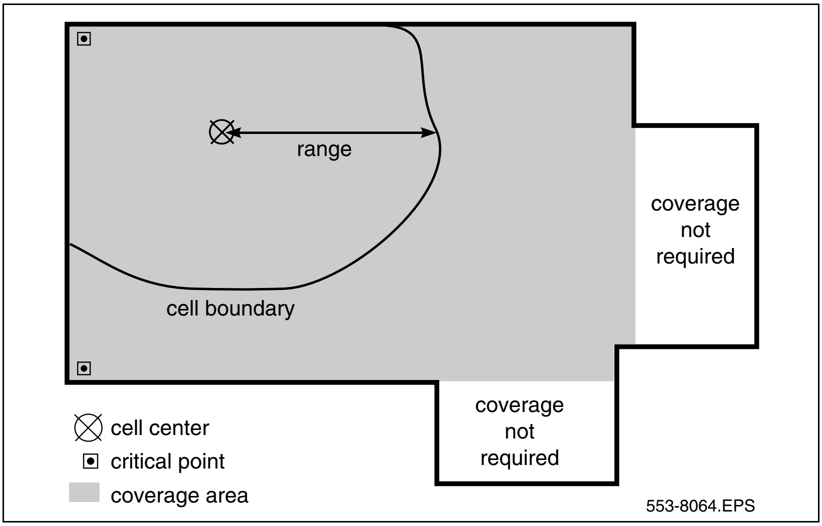
Coverage terms

The terms used in this guide are described in Table 15 and illustrated in Figure 81.

Table 15
Coverage terms

Term	Definition
Estimated number of handsets	The average number of handsets expected in a particular cell.
Cell	The coverage area provided by a basestation.
Cell boundary	The edge of a cell showing the cell coverage area.
Cell centre	The place where all the basestations are installed.
DECT Radio Deployment Tool	The tool used to determine the radio range of a basestation.
Critical point	A point or location defined as an outer corner of a coverage area, or points that can be difficult for the radio signal to reach.
Coverage area	The area defined by the customer in which a handset user can expect to be able to make and receive calls.
Link	When a handset and a basestation are in radio communication with each other.
Range	The distance from a cell centre to the cell boundary.
Office	The location where a handset user spends the majority of their day.
Traffic table	Traffic tables record site traffic information from the floor plan and the customer. The traffic table helps to determine the required number of basestations for each cell.

Figure 81
Coverage terms



Deployment tool

The DECT Deployment Tool (deployment tool) determines cell centres and cell boundaries. See Figure 91 and Figure 92 on page 231.

Figure 82
Deployment tool carrying case and packing details

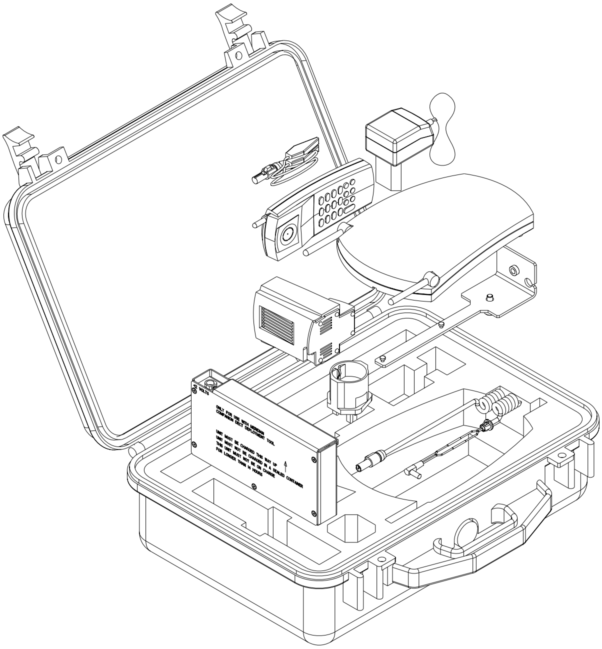
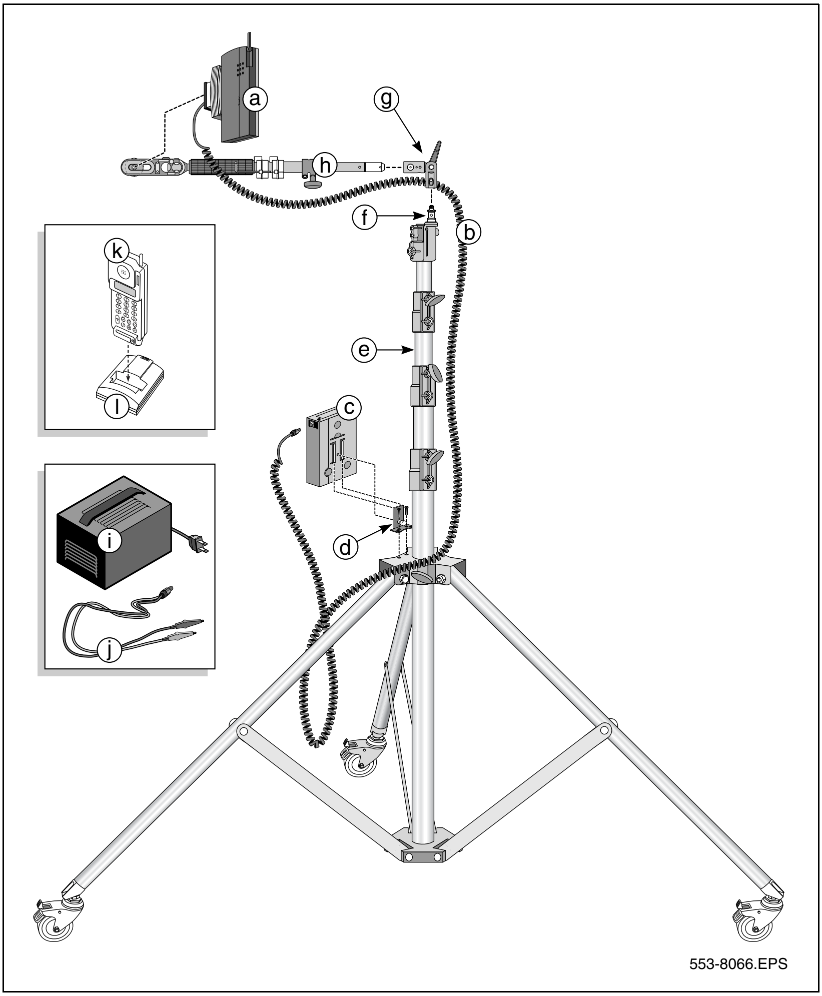

+12 VOLTS
ONLY FOR USE WITH MERIDIAN
COMPANION DECT DEPLOYMENT TOOL
UNIT MUST BE CHARGED THIS WAY UP
UNIT MUST NOT BE CHARGED IN A SEALED CONTAINER
THIS UNIT MUST NOT BE ON CHARGE
FOR LONGER THAN 14 HOURS

Figure 83
Assembled deployment tool



Key

a basestation

b power cord

c battery

d battery mount

e adjustable tripod

f extender arm connector

g extender arm swivel and clamp

h extender arm

i battery charger (separately ordered)

j battery charger cable

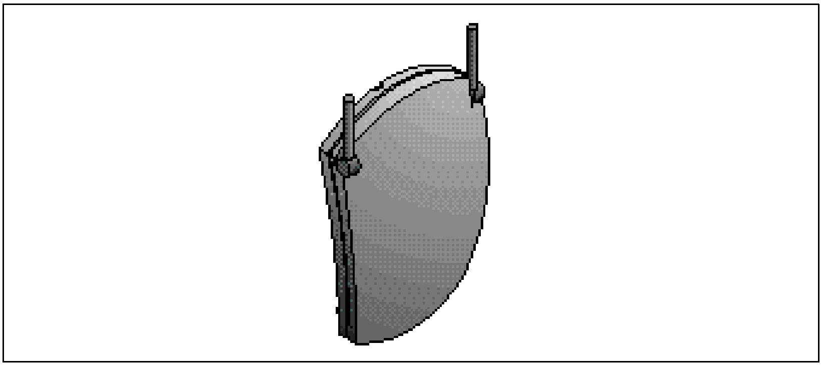
k deployment handset

l deployment handset battery charger

The deployment tool tripod is available in three heights:

- 2.4 meters
- 3.6 meters
- 4.8 meters

Figure 84
Deployment tool basestation



Do not position the deployment tool basestation next to large concrete or stone columns. This affects the contour of the cell boundary. Keep the deployment tool basestation at least 1 m from such columns.

Preparing the tool for deployment

Preparing the tool for deployment involves:

1. "Charging the deployment tool battery" on page 218
2. "Charging the deployment handset battery" on page 220
3. "Assembling the deployment tool" on page 221
4. "Testing the deployment handset" on page 225

Charging the deployment tool battery

Charge the deployment tool battery for at least six hours before using.

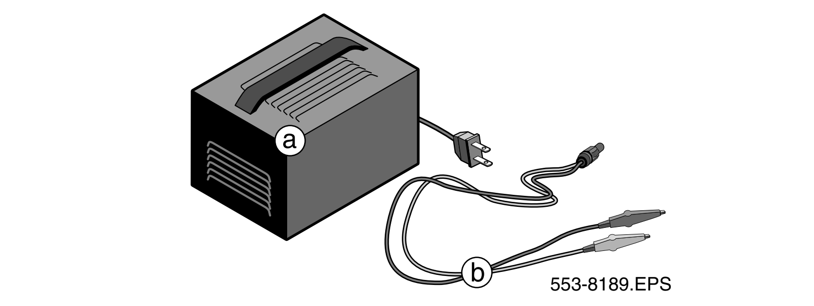
⚠

CAUTION — Equipment Damage

Use the Nortel battery charger. This charger is a separately ordered item. Failure to use an automatic shut-off battery charger can damage the battery.

Do not use the battery supplied with the CT2 deployment tool. The CT2 and DECT batteries are not interchangeable.

Figure 85
Deployment tool battery charger



Key

a battery charger (must be ordered separately)

b battery charger cable

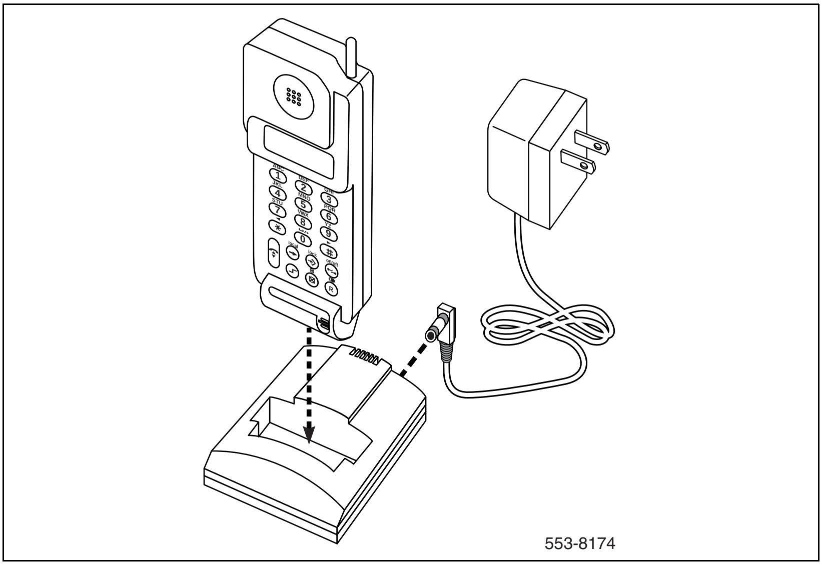
Procedure 7
Charging the deployment tool battery

Step	Action
1	Set up the deployment tool battery charging equipment.
	Remove the deployment tool battery, charger, and charger cord from the yellow case.
2	Charge the deployment tool battery.
	Connect the charger cord plug into the battery. Connect the red alligator clip to the positive lead of the charger, and the black clip to the negative lead of the charger. Connect the battery charger to the ac mains.
3	Remove the deployment tool battery from the charger after it is charged.
	The battery must charge for at least six hours.

END

Charging the deployment handset battery

Figure 86
Deployment handset battery charger



Charging time

Charge the deployment handset battery for at least 12 hours before using the first time. Charge the handset at least six hours before any subsequent use.

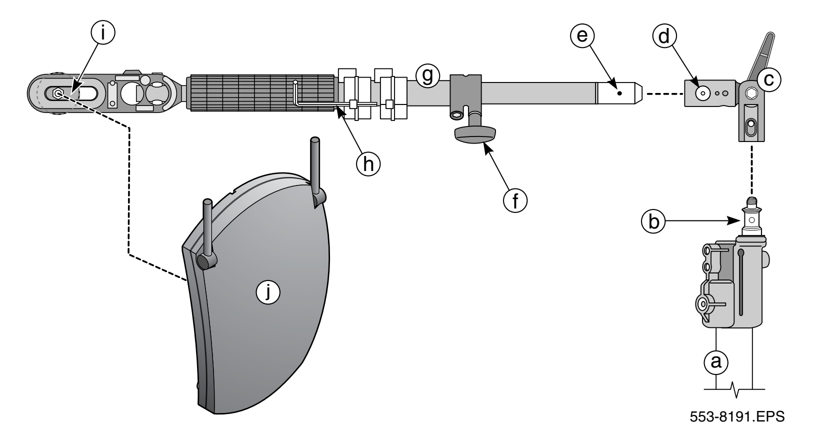
Procedure 8
Charging the deployment handset battery

Step	Action
1	Set up the deployment handset battery charging equipment.
	Remove the deployment handset battery, charger and charger cord from the yellow case.
2	Charge the deployment tool battery.
	Connect the charger cord to the charging stand. Connect the charger cord to the AC mains. Place the handset into the charging stand. The red LED flashes while the handset is charging.
3	Remove the handset from the charger when it is ready for use.

END

Assembling the deployment tool

Figure 87
Deployment tool extension details



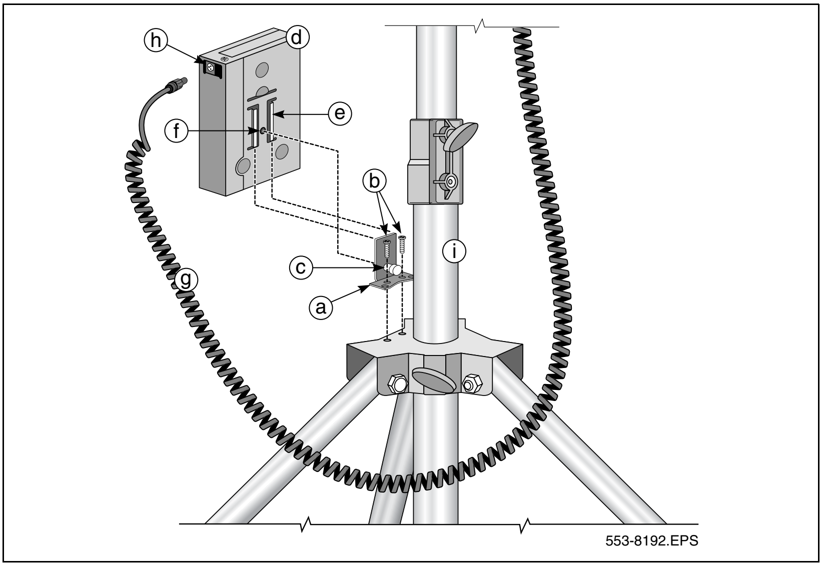
553-8191.EPS

Key

a	adjustable tripod
b	extender arm connector
c	extender arm swivel
d	detente stop
e	detente
f	extension thumb screw
g	telescopic extension
h	allen key
i	basestation attaching thumb screw
j	basestation

Note: The deployment tool battery and the deployment handset battery must be charged for at least six hours before use.

Figure 88
Deployment tool battery details



Key

a	battery mount
b	allen screws
c	thumb screw
d	battery pack
e	guides
f	thumb screw nut
g	power cord
h	power cord receptacle
i	tripod

Procedure 9
Assembling the deployment tool (Part 1 of 2)

Step	Action
1	Set up the tripod.
	Remove the tripod from its carrying case and set upright. Lock the casters.
2	If required, install the extension arm fitting on the tripod. If not required, go to step 4.
	Place the extension arm fitting, shown in Figure 91 on page 229, onto the brass fitting on the top of the tripod.
3	If required, secure the extension arm fitting.
	Use the Allen key attached to the extender arm to secure the extension arm fitting allen screw.
4	Mount the extension arm on the tripod.
	Place the brass end of the extension arm into the fitting, so that the keying hole of the extension arm mates with the retaining thump screw locking device of the tripod fitting. The thumb screw locking device clicks into the keying hole of the extension arm.
5	Position the extension arm.

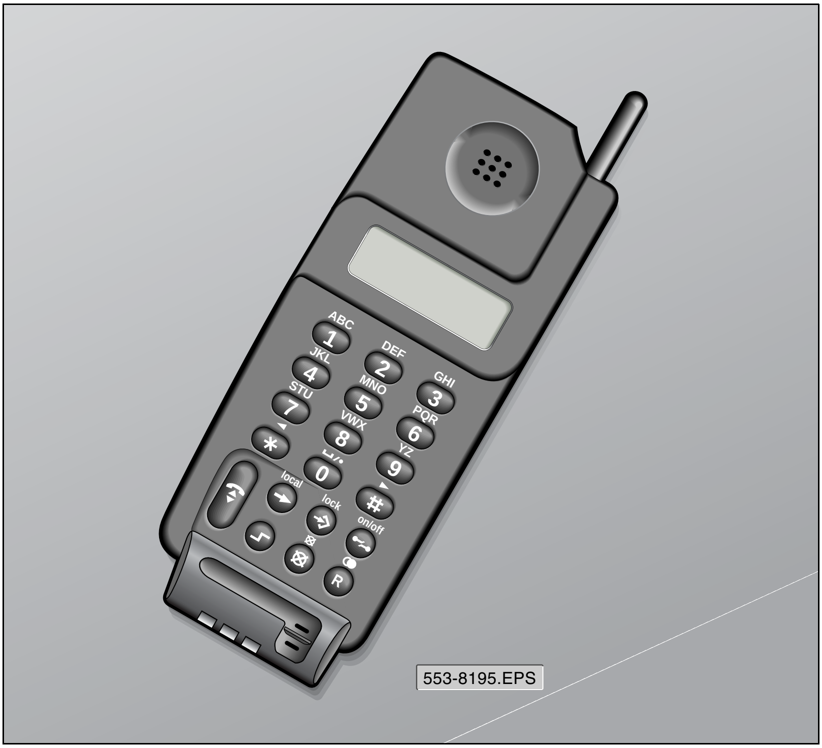
Procedure 9
Assembling the deployment tool (Part 2 of 2)

Step	Action
	Orient the arm into the proper position. Secure the tripod fitting and the extension arm thumb screw.
6	Affix the basestation to the extension arm.
	Remove the basestation from the yellow case. Mount the basestation onto the end of the arm. Screw the brass thumb screw on the arm into the bottom of the basestation and secure it in place with the grey lock thumb screw.
7	Position the antenna.
	Rotate the antenna from its stowed position, against the body of the basestation, to its upright operating position.
8	Position the basestation. The normal position is with the antenna pointing upwards.
	Secure the basestation with the arm thumb screw.
9	Mount the battery fixture on the tripod.
	Remove the battery bracket, shown in Figure 88, from the yellow case. Screw the battery bracket onto the tripod caster brace, with the two machine screws.
10	Mount the battery.
	Pull the release pin on the bracket back and slide the battery grooves on to the bracket. Ensure the bracket pin locks into the battery.
11	Connect the basestation to the battery.
	Plug the basestation power cord connector into the upper right edge of the battery.

END

Testing the deployment handset

Figure 89
Handset display and keypad details



Procedure 10
Testing the deployment tool handset (Part 1 of 2)

Step	Action
1	Start the test and establish a link with the basestation.
	Remove the handset from its charger.

Procedure 10
Testing the deployment tool handset (Part 2 of 2)

Step	Action
2	Turn on the handset.
	Press the shift key and press the ON/OFF button. The handset displays **DECT HANDSET**.
3	Select system mode.
	Press the shift key and press the local key. The handset displays **SYSTEM**.
4	Select the monitor mode.
	Press the star key. The handset displays **MONITOR MODE**.
5	Select the monitor mode code.
	Press the lock button. The handset displays **CODE**.
6	Enter the monitor mode code.
	On the dial pad, enter 2530. Press the lock button.
7	Interpret the handset RSSI display and test tone.
	Follow the explanation in “How the deployment tool works” on page 226 and “How to use the deployment tool” on page 227.

END

How the deployment tool works

The deployment tool basestation and the deployment handset establish a radio link when:

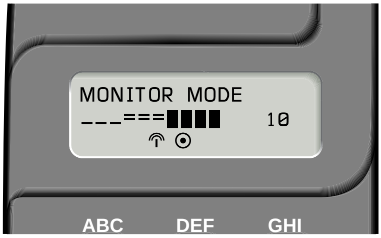
a the handset is in the deployment mode; and,

b the handset and basestation are within range of one another.

The closer the handset is to the basestation the stronger the link. As the handset moves away from the basestation, a point is reached where the signal is no longer reliable for telephone conversations.

When a link is established, the handset emits a continuous 1.4kHz tone and displays a Radio Signal Strength Indication (RSSI).

Figure 90
Deployment handset link display



The display, shown in Figure 90, means as follows:

- A circle and dot indicates a locked signal.
- The antenna symbol indicates a link establishment.
- The number 10 indicates an RSSI value.
- The dash, equal sign and shaded box icons indicate signal strength.

The maximum RSSI is 10. As signal strength diminishes, the number 10 decreases and the icons disappear. For example, at signal strength 7, the three shaded boxes that are on the right side of the display disappear. At signal strength 5, all the shaded boxes and one of the equal sign icons disappear.

The signal strength diminishes as the distance between the handset and the basestation increases. The tone remains unchanged until the handset is out of range of the basestation.

How to use the deployment tool

The deployment tool is assembled as shown in Figure 83 on page 216, with the extension arm parallel to the floor. Position the basestation antenna upwards. Place the basestation as close to the wall as possible and at the height recommended for basestations.

To test the deployment tool, stand in an open area approximately three to five metres away from the deployment tool on its tripod. Establish a link between the basestation and the handset. Keep the deployment tool basestation in plain view. Ensure there are no obstructions (including people).

Walk away from the basestation and observe the deployment handset link display. As the deployment handset moves away from the basestation, the RSSI value changes. When the RSSI value changes from 7 to 6 and the last shaded block disappears, the cell boundary has been reached.

When the cell boundary is reached, stop and listen to the tone. Ensure the tone is clear with no tone changes, tone break-up, modulation, mutes or clicks.

Do not select a cell edge that has an RSSI reading of less than 6. However, keep the following in mind.

- There can be environments that cause poor tone at a RSSI meter reading of between 7 and 10. In this case, contact Nortel support team for assistance.
- The tone stops when the radio link is lost.

Interpreting handset tones

The handset tones indicate how close the handset is to the deployment tool basestation.

- Steady tone – the handset is within the cell boundary, or at the cell boundary edge.
- Tone change, tone break-up, modulation, mute or click – the handset is beyond cell boundary edge.

Rules for outdoor deployment

1. Cover outdoor areas before covering indoor areas. Use the deployment tool to determine outdoor cell centres.
2. Use the deployment handset to determine the outdoor coverage provided by a basestation located indoors.
3. External housings for outdoor basestations must be mounted directly on walls or similar vertical surfaces.

4 When using the deployment tool outdoors, ensure that the deployment tool does not fall over or come in contact with electrical wires and cables.

5 If an outdoor critical point cannot be reached, inform the customer.

6 Do not use the deployment tool on windy days.

7 Do not use the deployment tool in bad weather.

8 Keep all personnel away from the apparatus.

9 Follow all safety requirements.

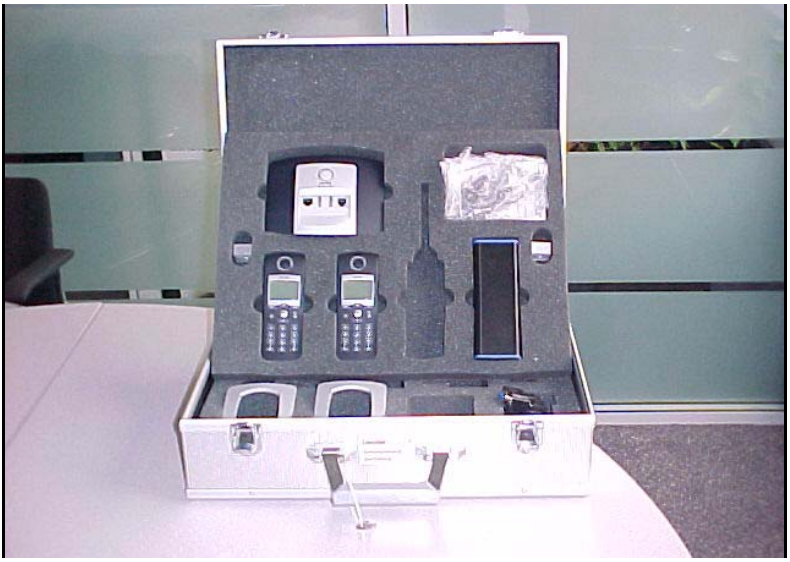
10 Use batteries to power the deployment tool.

11 Charge the batteries indoors.

DECT Deployment Kit 2

The DECT Deployment Kit 2 is shown in Figure 91. Refer to the DeTeWe User Manual that accompanies each kit for additional information.

Figure 91
Deployment Kit 2 and carrying case



The following information can be used in conjunction with the DeTeWe User Manual that accompanies the deployment tool.

1. The two DeTeWe handsets with the kit are subscribed to the basestation and are numbered 13 and 15. Refer to Figure 92 on page 231 to view the assembled basestation and the DeTeWe handsets.
2. The I/R key on the handset is the Off-Hook key.
3. To enter Site Survey Mode on the handset:

   — Press Menu

   — Scroll to System

   — Dial ***76#

   — Scroll to Site Survey

   — Press OK
4. The FE value for the PP is the number of detected Sync/ACRC errors within the last 100 receiving frames (i.e., 1 sec.). For proper deployment, the FE value must not exceed 5.
5. The FE value is for the FP is the number of received Q1/Q2 bit information within the last 100 receiving frames (i.e., 1 sec.). For proper deployment, the FE value must not exceed 5.
6. An RSSI value of -70dBm is used to indicate the cell boundary.
7. Use the following procedure to subscribe a handset that has de-subscribed in error:

   a Long-press the button on the basestation to open the DECT system.

   b On the handset, navigate to **Menu** > **System** > **Subscription** > **New**.

   c Enter the **PARK** number provided at the bottom of the basestation.

   d Enter the authorization code (the last 4 digits of the serial number located at the bottom of the basestation).

   The handset subscribes with the basestation.

Figure 92
Assembled Deployment Kit 2 and DeTeWe handsets

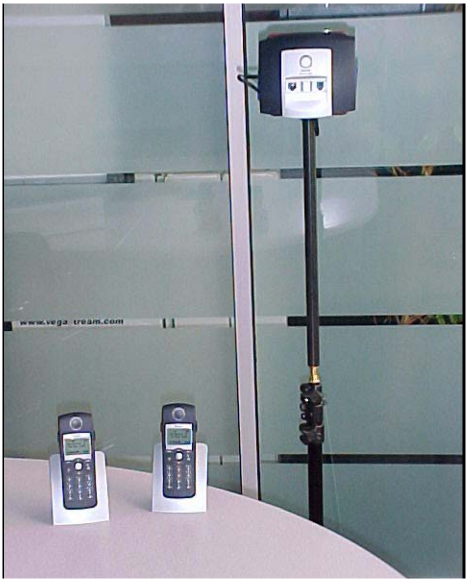
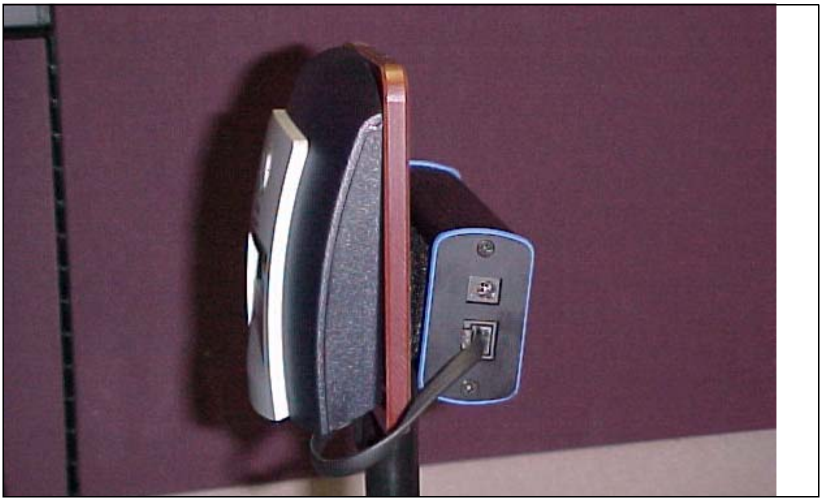


Figure 93
Deployment Kit 2 basestation



Deploying DECT

Follow Procedure 11 to deploy the DECT system.

Procedure 11
Deploying a DECT system (Part 1 of 4)

Step	Action
1	Identify and mark initial critical points.
	Mark critical initial points on the floor plan with the symbol: ⊡. Figure 65 on page 203 shows the initial critical points: P1, P2, P3, P5, P6 and P7.
2	Demarcate the cell contour for the critical point farthest from the centre of the full coverage area.
	To demarcate a cell contour: a Set up the deployment tool basestation. Raise the deployment tool basestation as high as possible, or until it is at the height recommended for basestations. b Establish a link. See “Deployment tool” on page 215 for details. c Measure the range into the coverage area in a few directions to determine where a cell centre can be located and still be within range of the critical point. Listen to the deployment tool handset while moving away from the basestation. When the RSSI value changes from 7 to 6, the cell boundary has been detected. d Mark the cell boundary on the floor plan with a small x. e Repeat steps c and d until there are enough Xs to draw a thin contour arc through the Xs. In Figure 66 on page 204, P1 is the initial critical point.
3	Demarcate the cell contour of the closest adjacent critical point to the first critical point.
	See step 2 for details. In Figure 67 on page 205, P2 is the closest adjacent critical point to the first critical point.

Procedure 11
Deploying a DECT system (Part 2 of 4)

Step	Action
4	Use the cell contours to locate a cell centre.
	Locate the cell centre where the cell contours meet. Choose a position on the floor plan that: • is furthest from the critical points, • still provides good audio quality at the critical point, • complies with the Rules and guidelines for selecting cell centres, page 197, and • is in the coverage area. With a pencil, label the cell centre on the floor plan with the symbol: ⊗ **xCn,** where **x** = the floor and **n** = is the cell number in sequence of the entire plan. In Figure 68 on page 206, IC1 is a cell centre.
5	Demarcate a cell boundary.
	To demarcate a cell boundary: a Set up the deployment tool basestation at the cell centre. b Establish a link. c Refer to the floor plan and check audio quality in user offices within the cell. If a user office is in a zone where audio quality deteriorates, relocate the cell centre closer to the critical point or the office. d Walk into all of the areas (rooms) necessary to demarcate the complete cell boundary. Radio signals travel further in uncluttered areas than in cluttered areas. Record the cell boundary. e Find the cell boundary by measuring the range and marking it on the floor plan with a small x. Repeat steps c and d until there are enough Xs so that a contour arc can be drawn around the cell centre. See Figure 69 on page 206 for an example of a cell boundary.

Procedure 11
Deploying a DECT system (Part 3 of 4)

Step	Action
6	Mark and label the cell boundary on the floor plan
	Follow these steps: a Mark each office within the cell that is isolated from the office area. b Label any subsequent critical point on the floor plan the following symbol: ⊡ c Mark the cell contour on the floor plan. Trace a contour line through the Xs with a marker. d Trace the cell boundaries and cell centres with coloured markers.
7	Identify new critical points.
	Follow these steps: a Identify one new critical point slightly inside of where the cell boundary meets the outside wall. In Figure 70 on page 207, this new critical point is P9. b Identify another new critical point which is adjacent to the first new critical point. Locate this critical point on the opposite side of the cell boundary area. In Figure 70 on page 207, the cell boundary area is IC1 and the new critical point is P8.
8	Mark and label these new critical points on the floor plan with the symbol: ⊡.
	See step 6 on page 234 for details.
9	Using the critical points from step 7, demarcate new cell contours, a new cell centre and a new cell boundary.
	See steps 2 to 5 starting on page 232 for details. **Note:** Cell contour arcs must pass near the cell boundary of adjacent cells. For an example of this, see Figure 71 on page 207.

Procedure 11
Deploying a DECT system (Part 4 of 4)

Step	Action
10	Demarcate additional cell contours, centres and boundaries at the other end of the building.
	Repeat steps 1 to 8 as necessary to demarcate new cell boundaries at the other end of the building. In Figure 72 on page 208, new cells are formed around cell centres IC3 and IC4.
11	Identify new critical points:
	These critical points must be: • adjacent to a critical point and on the opposite side of the cell boundary area. (critical point = P11 in Figure 73 on page 208, where cell boundary area = IC2), • just inside of where the cell boundary meets the outside wall (P12, P13, P14 and P15 in Figure 73 on page 208), and • where cell boundaries meet (P16 and P17 in Figure 73 on page 208).
12	Demarcate additional cell boundaries to cover all areas of the building.
	Repeat steps 1 to 8 as necessary to demarcate new cell boundaries in the middle of the building. Refer to Figures 74, 75, and 76 starting on page 209. Critical points P11, P13 and P16 form: • contours in Figure 74 on page 209 • the cell centre 1C5 in Figure 75 on page 209 • a new cell boundary in Figure 76 on page 210 Refer to Figures 77 and 78 starting on page 210. Critical points P11, P12 and P17 form: • contours in Figure 77 on page 210 • a new boundary based on cell centre 1C6 in Figure 78 on page 211 Figure 74 on page 209 shows a floor plan with complete radio coverage. The floor plan is made complete by cell boundary 1C7.

END

Correcting problems with audio quality

If a user office is near the critical point and the audio quality deteriorates within the user office, then the deployment tool and the cell centre are not properly located.

Procedure 12
Correcting problems with audio quality

Step	Action
1	Move the cell centre closer to the office or work area in question.
2	Repeat the coverage test in that area and ensure that coverage is sufficient.
	This can impact the coverage at other points, and you must ensure that all critical points are still properly covered by the new location.
3	Go into every location where users make and receive calls.
	This includes washrooms, coffee areas, and meeting rooms. Do not speculate where users can make calls.
	END

Deploying an external basestation

Follow Procedure 13 to deploy an external basestation.

Procedure 13
Deploying an external basestation

1 On the site plan, note each of the critical points that are to be reached.

2 Position the deployment tool at the potential location for a cell centre that is closest to the critical point.

3 Check for outdoor coverage to the critical point with the deployment handset.

4 If the critical point is reached, your cell centre is at the position of the deployment tool. Determine the cell boundary. If you cannot reach the critical point, determine and record the cell boundary that you did reach on the site plan.

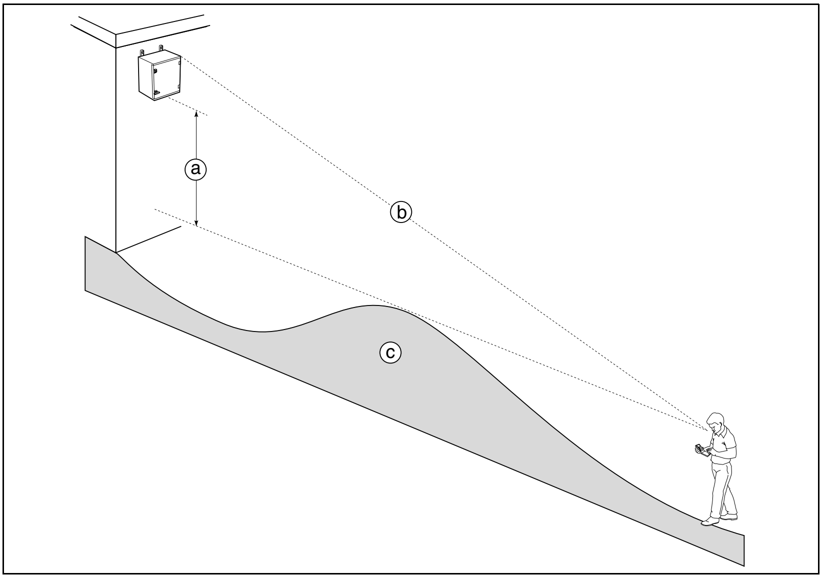
5 For each critical point, determine the potential location of external basestations. The location must be:

a. outdoors,

b. as close as possible to the critical point that you need to reach, and

c. more than 4 m above the highest ground to be covered.

Figure 94
Elevation of external basestation and terrain



Key

a External housing positioned at least 4 m from the ground.

b Clear line of sight to the external housing at the cell boundary.

c The range does not encompass any structures or earth mounds more than 2 m tall and more than 2 m wide.

6 If the critical point cannot be reached, inform the customer to determine if planning must continue.

7 Repeat this procedure until all of the outdoor areas have been completely covered.

End of Procedure

Single and multiple floor deployment

Whether the deployment situation involves a single floor or multiple floors, the deployment process uses basic rules:

1. Deploy the external or outdoor areas first.
2. Deploy from one side of the coverage area, then deploy the opposite side of the coverage area.
3. Finish by deploying the middle of the coverage area.

Follow these rules to prevent cell centres from clustering at one end of the site.

Check the floor plan to be sure that there are no areas where a handset in the required coverage area can be outside the range of a cell centre.

Defining a cell typically takes 25 to 40 minutes.

Single-floor deployment

Deploying a single floor coverage area involves methods that apply to all other applications of coverage. For multi-floor deployment, see page 245.

Use one or all of the following methods of deploying cells.

When determining a cell centre, one or all of the following methods of deploying cells are used:

- **Single cell deployment** – covers the distance between two outside corners at the end of a coverage area with one cell.

- **Double cell deployment** – covers the distance between two outside corners at the end of a coverage area with two cells.
- **Multi cell deployment** – covers the distance between two outside corners at the end of a coverage area with more than two cells.

Always begin with the single-cell method, because the range is not always known; therefore, it is not known how many cells are needed to cover the area between the critical points.

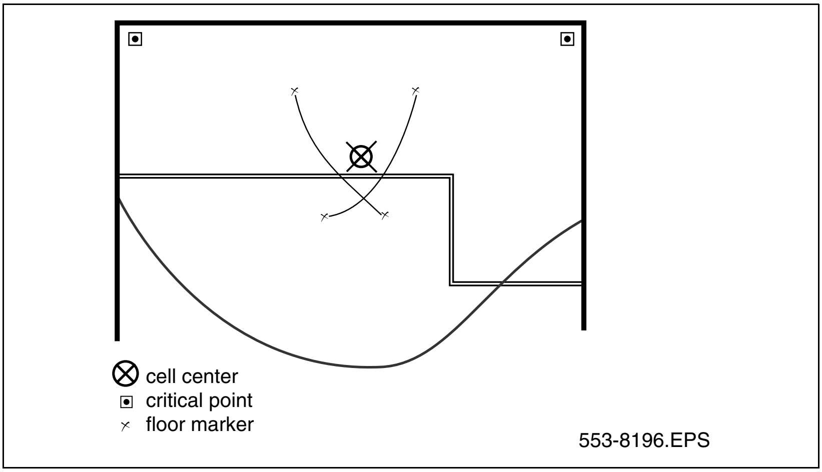
Start at the short side of the coverage area. First cover the corners, then the side between those corners, and finally inward to the centre of the coverage area. Repeat the process for the other end of the coverage area.

By deploying the site using this method, cell centres are distributed throughout the site. If the site is deployed from one end to the other, cell centres can be clustered at one end of the site.

Single cell deployment

Always start with the single-cell technique regardless of the width between the two critical points. using this technique, one cell centre is found that serves two critical points, as shown in Figure 95.

Figure 95
Single cell distance



Procedure 14
Single cell deployment

1 Identify the initial critical points. Mark them on the floor plan with a ⊡. Use different colour pencils for each critical point.

2 Choose the first critical point at the edge of the coverage area furthest away from the centre of the coverage area. Place the deployment tool at this critical point.

3 Establish a link. Refer to “Deployment tool” on page 215 for details.

4 Measure the range into the coverage area in a few directions to determine where a cell centre can be located, and still remain within range of the critical point. Observe the deployment tool handset RSSI value while moving away from the basestation. When the display value changes from 7 to 6, the cell boundary has been detected.

5 Record the cell boundary by marking a small X on the floor plan where the cell boundary value was reached. Use a pencil that is the same colour as the critical point where the deployment tool is located.

6 Repeat step 4 and 5 several times, walking in different directions to determine where the cell centre can be located and still remain within range of the critical point.

7 Draw a thin contour line through the Xs to mark an arc on the floor plan.

8 Choose the other critical point adjacent to the first critical point and repeat steps 3 to 7.

9 If the contour lines do not cross, or cross close to the edge of the coverage area between the two critical points, then see “Double cell deployment” on page 241. Choose a position on the floor plan for the cell centre that:

   a. is furthest from the critical points and still provides good audio quality at the critical point,

   b. complies with the “Rules and guidelines for selecting cell centres” on page 197, and

   c. is in the coverage area.

10 With a pencil, label the cell centre on the floor plan with ⊗ xCn. The x is the floor, and n is the cell number in sequence of the entire plan.

11 Place the deployment tool at each cell centre to locate the cell boundary.

12 Mark the cell boundary on the floor plan.

13 Repeat this task for the remaining coverage area from the extremes of the coverage area toward the centre until the entire floor has been covered.

14 If the cell boundary covers any other critical points, ignore these critical points when proceeding with coverage deployment.

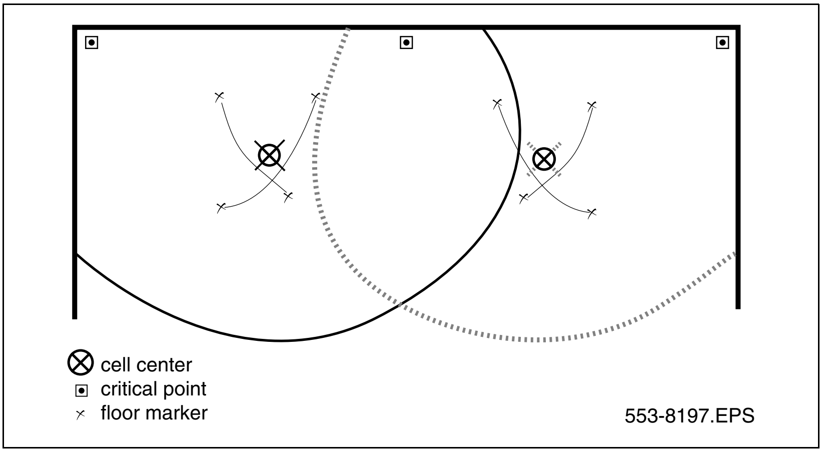
Note: If it is not possible to place the basestation at the exact crossover points of the arcs, place the basestation as close as possible to the crossover.

End of Procedure

Double cell deployment

Use the double cell technique only if referred here from the single-cell technique. Before beginning this technique, there must be two critical points that one cell centre cannot serve. Using the double cell technique, find two locations for cell centres that cover three critical points, as shown in Figure 96.

Figure 96
Double cell distance



Procedure 15
Double cell deployment

1. Mark a third critical point mid-way between the two critical points already identified.
2. Place the deployment tool at this mid-way critical point.
3. Establish a link.
4. Walk briskly into the coverage area within range of either of the first two critical points until the cell boundary is reached.
5. Record the cell boundary by marking a small X on the floor plan where the cell boundary is located.
6. Repeat step 4 and 5 several times, walking in different directions to determine where the cell centre can be located and still be within range of the critical point.
7. Draw a thin contour line through the Xs to mark an arc on the floor plan.
8. Repeat steps 2 through 5 walking into the coverage area of the other of the first two critical points.
9. If the contour lines do not cross, or if the amount of overlap between the cells is less than 1/2 the distance between the cell centre and the cell boundary, then see “Multi cell deployment” on page 243.
10. Choose a position on the floor plan for the cell centre that:

    a. is furthest from the critical points and still provides good audio quality at the critical point,

    b. complies with the “Rules and guidelines for selecting cell centres” on page 197, and

    c. is in the coverage area.
11. Mark each cell centre on the floor plan ⊗ and label them **1C1** and **1C2**.
12. Place the deployment tool at each cell centre to find the cell boundary and mark it on the floor plan.

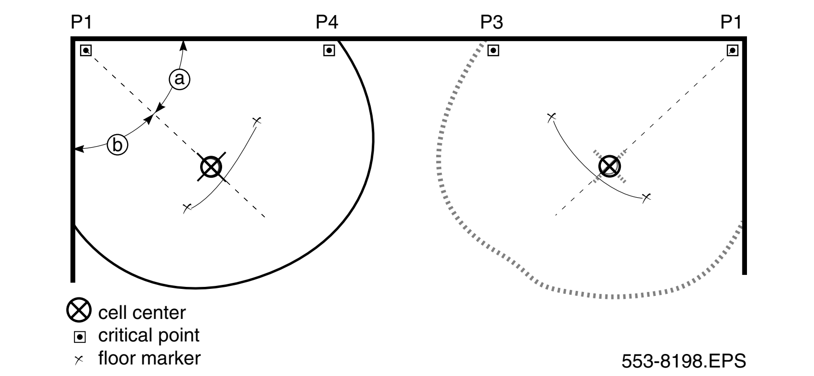
13 Repeat this technique for the remaining coverage area from the outer extremes of the coverage area toward the centre until the entire floor has been covered. If the cell boundary covers any other critical points, ignore these critical points when proceeding with coverage deploying.

End of Procedure

Multi cell deployment

Use the multi cell technique only if referred here from the double cell technique. Before beginning this technique, there must be two critical points that one cell centre cannot serve. Using the multi cell technique, two cell centres, each one serving one of the two critical points, are found, as shown in Figure 97.

Figure 97
Multi-cell distance



Procedure 16
Multi-cell deployment

1 Choose a position on the floor plan for the cell centre that:

a. is furthest from the critical points and still provides good audio quality at the critical point,

b. complies with the “Rules and guidelines for selecting cell centres” on page 197, and

c. is in the coverage area.

2. Place the deployment tool at critical point **P1**.

3. Establish a link.

4. Walk briskly into the coverage area away from the critical point until the cell boundary is reached.

5. Mark a small X on the floor plan where the cell boundary is found.

6. Repeat step 4 and 5 several times, walking in different directions from the critical point to establish an arc. The arc is at the cell boundary and is within range of the critical point.

7. Draw a thin contour line to mark an arc through the Xs on the floor plan.

8. Repeat steps 4 through 7 walking into the coverage area of critical point **P2**.

9. Locate the cell centre on the arc along a line from the critical point that is equal distant from the adjacent walls.

10. Mark each cell centre on the floor plan ⊗ and label them **1C1** and **1C2**.

11. Place the deployment tool at each cell centre.

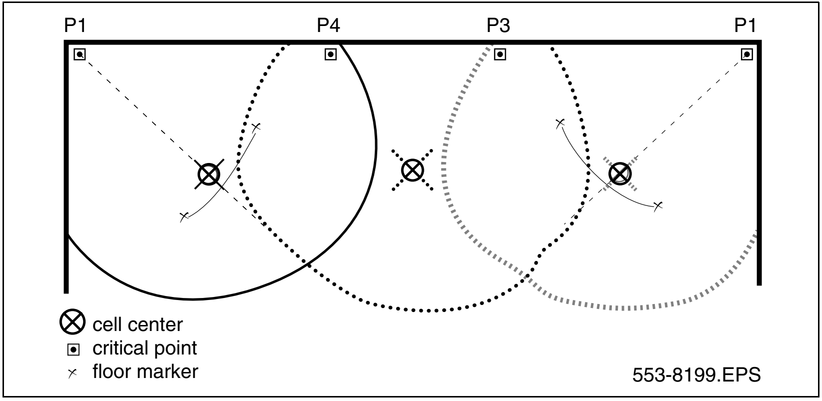
12. Locate the cell boundary and mark it on the floor plan. (Mark the contours in different colours for easy differentiation of cell centres.)

13. Define and mark on the plan any subsequent critical points, where each cell boundary crosses the edge of the coverage area.

14. If the cell boundary covers any other critical points, ignore these critical points when proceeding with coverage deploying.

15. Repeat the multi cell technique for the remaining area to be covered, from the extremes of the coverage area toward the centre, until all of the floor is covered.

Figure 98
Multi cell distance using the single cell technique



16 Use the subsequent critical points to fill in the coverage area between the first two cells using the “Single cell deployment” on page 239. An example of this is shown in Figure 98.

End of Procedure

Multiple floor deployment

This applies to deployment scenarios in the following situations:

- The coverage area is on more than one floor.
- The floors are not adjacent to each other.

Checking for through-the-floor coverage

The first step in covering a multi-floor building is assessing the availability of through-the-floor coverage. In buildings mainly constructed of wood, through-the-floor coverage can be used. However, due to the construction of most modern buildings with raised floors, high metal content, and reinforced concrete, through-the-floor coverage with DECT is limited.

Procedure 17
Checking for through-the-floor coverage

Step	Action
1	Place the deployment tool in a middle floor of the site.
2	Go to the floor above the deployment tool and establish a link with the deployment handset.
	Follow the procedure on Table 10 on page 225.
3	Measure the deployment contour as if the basestation was on this floor, instead of the floor below.
	If only a small area is covered (less than 10 metres radius), then there is effectively no through-the-floor coverage on the floor above an installed basestation.
4	Go to the floor below the deployment tool and repeat the above process.
	If the area that can be covered is small, then there is no through-the-floor coverage below a basestation location.
5	If there is no through-the-floor coverage or coverage is restricted to a small area.
	Deploy each floor using critical points, or if the floors are exactly similar, deploy as multi floors with the same layout.

END

Assess floor layout

The deployment procedure changes according to the similarities and differences of the floors.

All floors have the same layout

To begin a multi-floor deployment when all of the floors have the same layout, deploy one floor and enter the data on the floor plan. Use the data from the deployed floor for other identical floors.

For example, if floor 2 of an office tower is laid out with cubicle style offices with a perimeter of enclosed offices, and floor 3 is designed and laid out in the **exact** same manner, then both floors can have the exact same installation profile for basestations.

All floors do not have the same layout

If there are **any deviations** in the floor plan from floor to floor, use the critical point method to deploy each distinct floor. For more information, see “Preparing the tool for deployment” on page 218.

> ***Note:*** Do not underestimate the importance of changes in floor layout. Simple changes in a room from a meeting room to a storage room can have significant impact on the coverage from a basestation.

Multi-floor coverage situations

The following situations require multi-floor coverage:

1 Atriums (page 247).

2 High rise buildings (page 248).

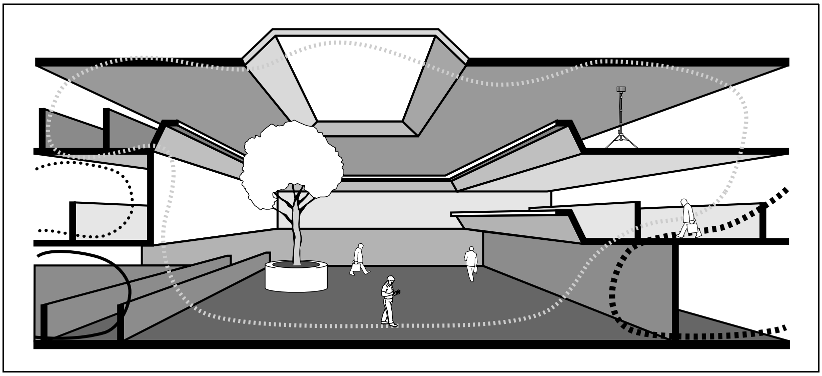
3 Unusual conditions (page 249).

Use Multi-floor coverage procedure, if instructed to do so, from Gathering building information, page 191.

Atriums

Cells in an atrium, as shown in Figure 99 on page 248, are usually larger than the cells of the rest of the building. This section gives guidelines on how to plan an atrium. There are no precise steps to follow when deploying an atrium, however there are points to consider. Also see “Unusual conditions” on page 249.

Figure 99
An atrium



Consider the following when deploying an atrium:

- Plan atriums to their full height.
- Plan an atrium as one full size room, not floor by floor.
- Place cell centres within an atrium only when you intend for them to cover the atrium.
- Do not put cell centres in an atrium if you intend for them to serve adjacent areas.
- To serve adjacent areas, put the cell centres into these areas.
- Deploy the atrium first if the atrium is more than a third the size of the building, or more than one cell in size.
- If cell centres in adjacent dense areas serve one floor of an atrium, check the coverage of the cell on all of the floors that meet with the atrium.

High rise buildings

Deploy high rise buildings as unusual conditions of multi-floor deployment.

Test through-the-floor coverage first. If there is no through-the-floor coverage, then deploy each floor. Repeat as many floors as possible where the floor layout is the exact same as any other, in all other cases deploy floor by floor. A floor with many meeting rooms deploys differently from a building with cubicle style offices.

Unusual conditions

There are no precise steps to follow when deploying for an unusual condition; however, there are points to be considered.

To plan an unusual condition, consider the following situations:

1. Cell centres are too close (page 249)
2. Cell centres are too far apart (page 249)
3. Too many cell centres (page 250)

Cell centres are too close

If cell centres are deployed less than 10 metres apart, the handsets can initiate unnecessary handovers. Unnecessary handovers result in excessive internal messaging and degraded speech quality.

Cell centres are too far apart

If cell centres are deployed too far apart, the edge of a cell does not overlap the coverage from another cell.

Cell centres must be located within the edge of other cell centres to provide satisfactory overlap.

Overlap can be difficult to achieve where coverage is received from the floor above or the floor below. Internal structures can cause overlap deficiencies.

It is not necessary that the cell centre be on the same floor or an adjacent floor of the area that it is covering. It is only necessary to be within the cell boundary, as indicated by the deployment tool.

The installation of basestations in places other than the location shown on the plan can cause coverage problems; for example, if the basestation is mounted on the opposite side of a wall from its planned location.

Consider the following when choosing basestation locations:

- Choose locations only where it is possible to mount basestations.
- Install basestations as close as possible to planned locations.

- Follow safety codes or aesthetic considerations.
- Allow sufficient access for installation of basestations.
- Provide clear installation instructions.
- Test the coverage during post-deployment checks.

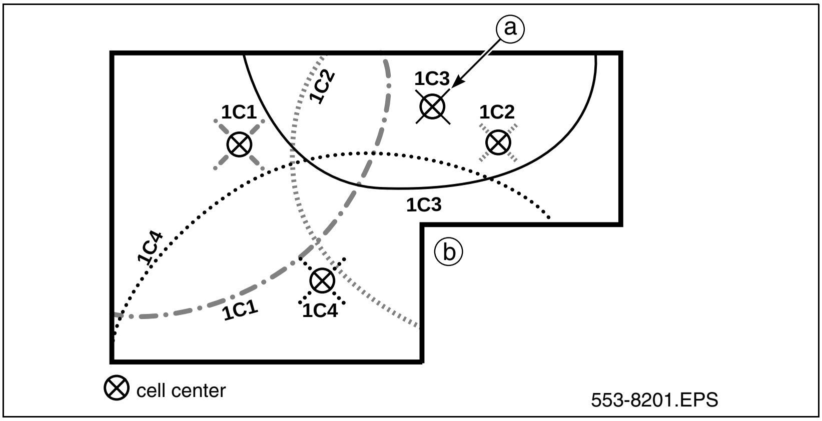
Too many cell centres

The primary concern with deploying too many cell centres is cost. To deploy the correct number of cell centres and reduce cost, do the following:

- Check the coverage and traffic volume before adding additional cells.
- Remove a cell served by other cells unless it is required for high handset density.
- Check the coverage area of each cell.
- Verify that there is at least one area that each cell serves that is not served by another cell.

In the example shown in Figure 100, cell 1C3 is redundant unless required for high handset density.

Figure 100
Locating redundant cells



Cell re-engineering for high traffic areas

To accommodate the demand in high traffic areas, follow the "The cell re-engineering process" on page 251.

Traffic volume

The deployment process ensures coverage throughout the service area. It does not, however, take into account the effect of traffic. In a high traffic area, a shortage of radio channels at the basestation can cause calls to be blocked.

Two options are available to support the volume of telephone calls in cells that carry heavy traffic:

- increase the number of cells deployed
- use 12-channel basestations

The calculation of expected telephone traffic includes an allowance for the user population in a cell, and the roaming user.

About the 12-channel basestation

An optional 12-channel basestation must be used where telephone traffic levels exceed those that can be carried on the standard 6-channel basestation. The radio performance of the 12-channel unit is the same as that of the 6-channel unit so the cell sizes are the same for both units.

Do not connect more than two 12-channel basestations to a DMC card. Two 6-channel basestations can also be attached to a DMC serving two 12-channel units. If loop resistance exceeds 100 ohms, external power must be used.

The cell re-engineering process

The cell re-engineering process involves:

1. "Estimating traffic within a cell" on page 252.
2. "Separating the coverage area and recording the number of offices" on page 253.
3. "Creating an estimate table" on page 254.

4. “Calculating the number of users inside the cell with an office” on page 255.
5. “Calculating the number of users with an office outside the cell who walk into the cell” on page 256.
6. “Calculating the number of users without an office” on page 257.
7. “Totalling the estimate for users in a cell” on page 258.
8. “Calculating the data for all remaining cells” on page 259.
9. “Creating a table to document telephone types in a cell” on page 260.
10. “Determining cell re-engineering” on page 261.

Estimating traffic within a cell

Modify the previous deployment procedure to adjust the estimated number of users. To carry out this procedure:

- Determine the number of handset users with an office within each cell.
- Determine how many of these users have wired sets.
- Determine how many users without an office are normally in each cell.

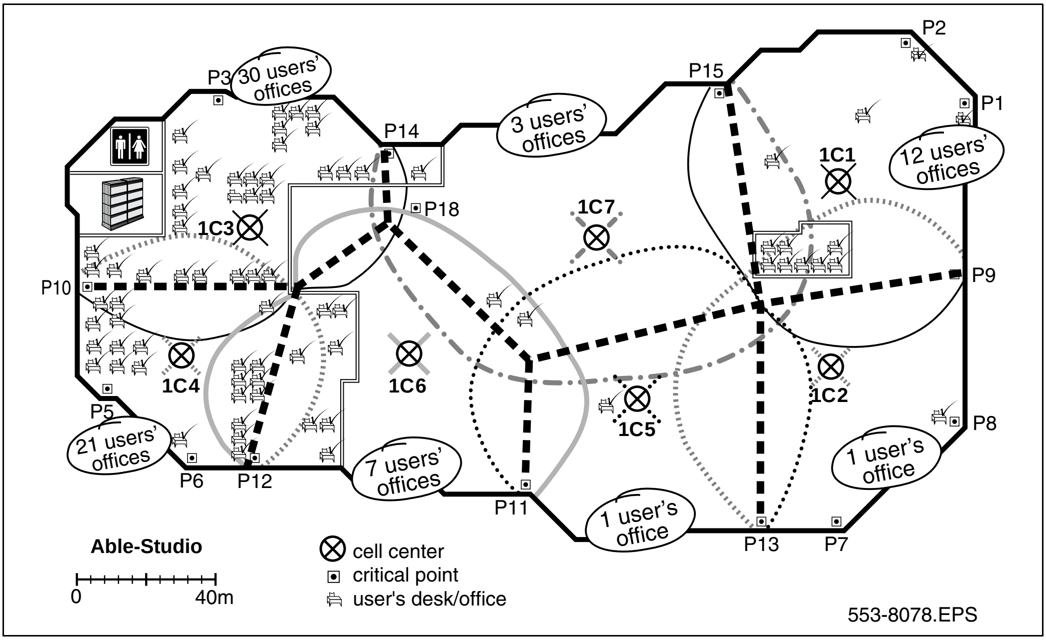
Some users have both wired and handset telephones; other users rely on handsets only.

Re-engineered cells for high traffic areas are represented by an adjusted estimate for the two groups: handset and wireless, and handset only. Use the adjusted estimate to determine whether the cell sizes, indicated by the earlier deployment procedure, can handle the telephone traffic.

If the traffic handling capacity of the cells is not adequate, use 12-channel basestations and subdivide them into smaller cells to ensure the traffic is handled properly in accordance with these instructions.

Separating the coverage area and recording the number of offices

Figure 101
Example of dividing the coverage area and recording offices



Procedure 18
Separating the coverage area and recording the number of offices in each area

Step	Action
1	Divide the floor plan into cell areas.
	Mark the cell areas on the floor plan, one area for each cell, splitting cell overlap areas in half. Shown in Figure 101 as heavy dotted lines.
2	Count the number of user offices in each cell area.
	Record the number of user offices on the floor plan in each cell area.

END

Creating an estimate table

Use this table later to estimate the number of handset users for each cell.

Table 16
Estimate users in a cell

	1C1	1C2	1C3	1Cn
Users inside the cell with an office				
Users with an office outside of a cell who walk into the cell				
Users without an office				
Users in a cell				

Procedure 19
Creating an estimate table

Step	Action
1	Make an estimate table.
	Include as many columns as there are cell centres.
2	Label the rows.
	Example shown in Table 16 on page 254.
3	Label each column heading with the cell centre indicator.
	Use this table to determine how many times to subdivide each cell to carry the handset telephone traffic.

END

Calculating the number of users inside the cell with an office

Table 17
Example of the table first row calculation

	1C1	1C2	1C3	1C4	1C5	1C6	1C7
Users inside the cell with an office	8.4						
Users with an office outside of a cell who walk into the cell							
Users without an office							
Users in a cell							

Procedure 20
Users inside the cell with an office

Step	Action
1	Calculate the estimate for users in the first cell with an office.
	Use the formula: (Users with an office in the cell x 0.7)
2	Enter the result in the row, users inside the cell with an office.
	In the example shown in Figure 101 on page 253, twelve users in cell 1C1 spend 70% of their time in their offices. (12 x 0.7 = 8.4)

END

Note: Traffic engineering has determined that handset users with an office spend seventy percent of their time within their home cell.

Calculating the number of users with an office outside the cell who walk into the cell

Table 18
Example of the table second row calculation

	1C1	1C2	1C3	1C4	1C5	1C6	1C7
Users inside the cell with an office	8.4						
Users with an office outside of a cell who walk into the cell	3.2						
Users without an office							
Users in a cell							

Procedure 21
Users with an office outside the cell who walk into the cell

Step	Action
1	Calculate the estimate for users in the first cell with an office outside of the cell who walk into the cell.
	Use the formula: $\dfrac{(\text{Total users with an office} - \text{Users with an office inside the cell}) \times 0.3}{(\text{Total number of cells} - 1)}$
2	Enter the result in the row, users with an office outside the cell who walk into the cell.”
	For the example shown in Figure 101 on page 253, there are a total of 75 telephone users in Able-Studio, minus the 12 users already in cell 1C1. Therefore, 63 users can walk into cell 1C1. However, the 63 walk in users only spend 30% of their time outside their offices. There are seven cells on the floor plan minus cell 1C1. Accordingly, an estimate of 3.2 walk-in users can be in cell 1C1. $\dfrac{(75 - 12) \times 0.3}{(7 - 1)} = 3.2$

END

Calculating the number of users without an office

Table 19
Example of the table third row calculation

	1C1	1C2	1C3	1C4	1C5	1C6	1C7
Users inside the cell with an office	8.4						
Users with an office outside of a cell who walk into the cell	3.2						
Users without an office	0						
Users in a cell							

Procedure 22
Calculating the number of users without an office

Step	Action
1	Calculate the estimate for users in the first cell without an office.
	Use the formula: $\frac{\text{Total number of users without an office}}{\text{Number of cells}}$
2	Enter the result in the row, users without an office".
	In the example shown in Figure 101 on page 253, there are no users without an office.

END

Totalling the estimate for users in a cell

Table 20
Example of the table first column total

	1C1	1C2	1C3	1C4	1C5	1C6	1C7
Users inside the cell with an office	8.4						
Users with an office outside of a cell who walk into the cell	3.2						
Users without an office	0						
Users in a cell	11.6						

Procedure 23
Totalling the estimate for users in a cell

Step	Action
1	Total the estimate for the number of users in the first cell by adding the three rows in the first column.
2	Enter the result in the bottom row users in a cell".
	For the example shown in Figure 101 on page 253, the 1C1 handset estimate equals 11.6. 8.4 + 3.2 + 0 = 11.6.

END

Calculating the data for all remaining cells

Table 21
Example of a completed estimate table

	1C1	1C2	1C3	1C4	1C5	1C6	1C7
Users inside the cell with an office	8.4	0.7	21.0	14.7	0.7	4.9	2.1
Users with an office outside of a cell who walk into the cell	3.2	3.7	2.3	2.7	3.7	3.4	3.6
Users without an office	0	0	0	0	0	0	0
Users in a cell	11.6	4.4	23.3	17.7	4.4	8.3	5.7

Procedure 24
Calculating the data for all remaining cells

Step	Action
1	Repeat the last four tasks to calculate all the remaining user cell estimates.
2	Enter the result in the estimate table.
	The information contained in Figure 101 on page 253, is shown entered into Table 24. This table is used to note the results of the calculations for cells that require re-engineering.
END	

Creating a table to document telephone types in a cell

Use a table like Table 22 to record the different telephone types in each cell.

Table 22
Telephone types in a cell

	1C1	1C2	1C3	1Cn
User telephone types				

Use the following symbols in each cell to denote the type of telephones in use in the cell:

- **H&W** refer to a cell in which all the users have both wired and handsets (wireless sets).
- **H** refers to a cell in which users have only handsets (wireless sets).
- **M** refers to a mix of H and H&W users.

Procedure 25
Creating a table to document telephone types in a cell

Step	Action
1	Make a Telephone types table.
2	Label the row, User telephone types” and include as many columns as there are cell centres.
3	Label each column heading with the cell centre indicator.
	The information in this table is used to determine the number of cells that require re-engineering.

END

Determining cell re-engineering

Table 23
Example of a completed estimate table

	1C1	1C2	1C3	1C4	1C5	1C6	1C7
Users inside the cell with an office	8.4	0.7	21.0	14.7	0.7	4.9	2.1
Users with an office outside of a cell who walk into the cell	3.2	3.7	2.3	2.7	3.7	3.4	3.6
Users without an office	0	0	0	0	0	0	0
Users in a cell	11.6	4.4	23.3	17.7	4.4	8.3	5.7

Table 24
Example of a completed telephone types table

	1C1	1C2	1C3	1C4	1C5	1C6	1C7
User telephone types	H&W	H&W	M	M	H&W	H&W	H&W

Table 25
Cell re-engineering

Estimate for:		
Users with both a handset and a wired telephone	**Users with only a handset**	**Action**
From 0 up to 20	From 0 up to 12	Keep cell size as deployed.
Greater than 20 but no more than 80	Greater than 12, but no more than 40	Install a 12-channel basestation or sub divide the cell[a].
Greater than 80	Greater than 40	Sub divide the cell[a] to meet the above conditions.

[a] For details on how to subdivide cells, refer to High handset density deployment, page 266. Use a 12-channel basestation in areas of high traffic capacity. Cell subdivision is appropriate when it helps to improve coverage where the loop resistance exceeds 100 ohms or when a DMC cannot support more than two 12-channel units.

Note: Use Table 25 only for user types H&W and H. For user type M" see page 263.

Procedure 26
Determining cell re-engineering

Step	Action
1	Locate the estimate for users in the first cell.
	In the example shown in Table 23 on page 261, the handset estimate is 11.6.
2	Determine the telephone types in the first cell.
	In the example shown in Table 24 on page 261, the telephone type is H&W.
3	Locate the telephone type column in Table 24 on page 261.
	In the example H&W is the users with both a handset and a wired telephone".
4	Find the handset estimate range in Table 25 on page 261.
	In the example, 11.6 falls within the From 0 up to 20" category.
5	Determine if a cell requires division or uses a 12-channel basestation.
	In the example From 0 up to 20", division is not required.
6	Repeat the above steps to determine the required number of cells that need subdivision, except for telephone types M. For M see "A mix of users with and without wired telephones in a cell" on page 263.
7	Transfer the results of Table 26 into the Provisioning records.

END

Cell division requirements in special cases

This section describes how to determine cell division in the following special cases where:

a no office information is available; and,

b there is a mix of handset users with and without wired telephones.

No office information

If it is not known where any of the users offices are, calculate the estimated number of handsets for each cell using this formula:

$$\frac{\text{Number of handsets}}{\text{Number of cells}}$$

The formula assumes that users are located evenly throughout the cells. However, most users offices are clustered in specific areas of a building.

The formula has limitations, as cells can vary in size. The method described starting on page 251 gives more accurate cell division results.

A mix of users with and without wired telephones in a cell

Use this procedure for mixed handset users. This procedure then enables the telephone traffic generated by handset users, to be equated to that of handset and wired users. Combine the two groups for cell size recalculation purposes.

Table 26
Adjustment for users without wired telephones (Part 1 of 3)

Estimated number of handsets for users without wired telephones	Adjusted estimated number of handsets for each cell
0	0
1	2
2	3
3	5
4	7

Table 26
Adjustment for users without wired telephones (Part 2 of 3)

Estimated number of handsets for users without wired telephones	Adjusted estimated number of handsets for each cell
5	9
6	11
7	12
8	14
9	16
10	18
11	20
12	22
13	24
14	25
15	27
16	29
17	31
18	34
19	36
20	38
21	40
22	42
23	44
24	46
25	48
26	49
27	50
28	53

Table 26
Adjustment for users without wired telephones (Part 3 of 3)

Estimated number of handsets for users without wired telephones	Adjusted estimated number of handsets for each cell
29	55
30	57
31	60
32	62
33	64
34	66
35	69
36	71
37	73
38	76
39	78
40	80

Procedure 27
Adjusting for users without wired telephones

Step	Action
1	Count the number of user offices that have handsets and wired telephones (H&W), and record the number.
2	Count the number of user offices that have only wireless handsets, (H).
3	Use Table 26 to determine the equivalent number of H&W users and record this number.
4	Add the numbers received from steps 1 and 3 to determine and adjust the value for the number of users with wired telephones.
5	Use Table 26 to determine the criteria shown in the left column to determine if the cell has to be resized in the same manner described in the section Determine cell re-engineering”.

END

High handset density deployment

The high handset density deployment includes limiting the expected number of handsets for each cell centre.

> ***Note:*** Use the high handset density procedure if instructed to do so from Table 25, “Cell re-engineering,” on page 261. Do not use more than one basestation for each cell centre.

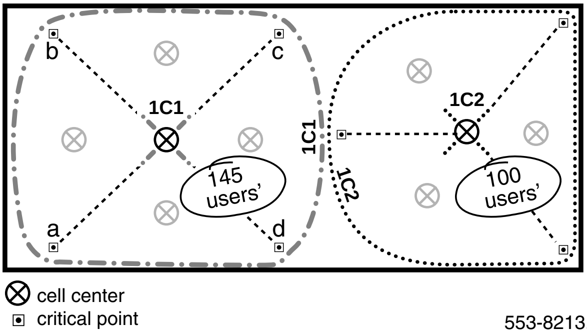
Limiting the anticipated number of handsets

Limit the anticipated number of handsets for each cell centre to the limits shown in Table 25 on page 261. Only subdivide high handset density areas. If a cell falls into the category of a high density area, use the procedure on the following page to subdivide the cell.

Subdividing a cell

To subdivide the area for smaller cells, divide the cell into as many smaller cells as necessary to provide for the number of users in the area.

Figure 102
Example of a subdivided cell



In Figure 102, cell 1C1 has 140 handset users and cell 1C2 has 100 handset users. For example, Table 25 on page 261 indicates the following:

- If the handset users in cell 1C1 are all handset only users, one cell can support 39 handset only users. Therefore, four cells are needed to support 140 users (140÷39 = 3.5 cells).
- If the handset users in cell 1C1 are handset and wired telephone users, and one cell can support 83 users, then two cells are needed to support 140 handset and wired telephone users (140÷83 = 1.6 cells).

Procedure 28
High handset density deployment (Part 1 of 2)

Step	Action
1	Determine the number of handset users in the high handset density cell.
	Count the number of users. Include users served by through-the-floor coverage of this cell.
2	Calculate the cell subdivisions as required.
	Divide the number of users by the appropriate value (12 or 20) shown in Table 25 on page 261. Round up the result to the next whole number. The result equals the number of cells required after subdividing the cell.
3	Divide the cell.
	Draw lines from the cell centre to the critical points on the cell boundary. Shown in Figure 102, the cell 1C1 divides into four sectors and cell 1C2 divides into three sectors.
4	Relocate new cell centres.
	Mark new cell centres within the sectored areas.
5	Check the number of handset users in the new cell areas.
	Count the number of user offices within each smaller sector. Ensure there are fewer user offices within the cell than the traffic limit.
6	Check the locations.

Procedure 28
High handset density deployment (Part 2 of 2)

Step	Action
	Take the deployment tool to the locations that have been calculated on the floor plan. Ensure that there is a location that meets the guidelines on page 197.
7	Check the new cells for complete coverage.
	Use the deployment handset to check coverage.
8	Repeat the anticipated handsets for each cell calculation to ensure that each smaller cell provides appropriate traffic coverage to the users in the area.

END

Deployment review

Review the plan to ensure that the sales group can use it. The plan must be complete for the installer, legible for maintenance purposes, and acceptable to the customer.

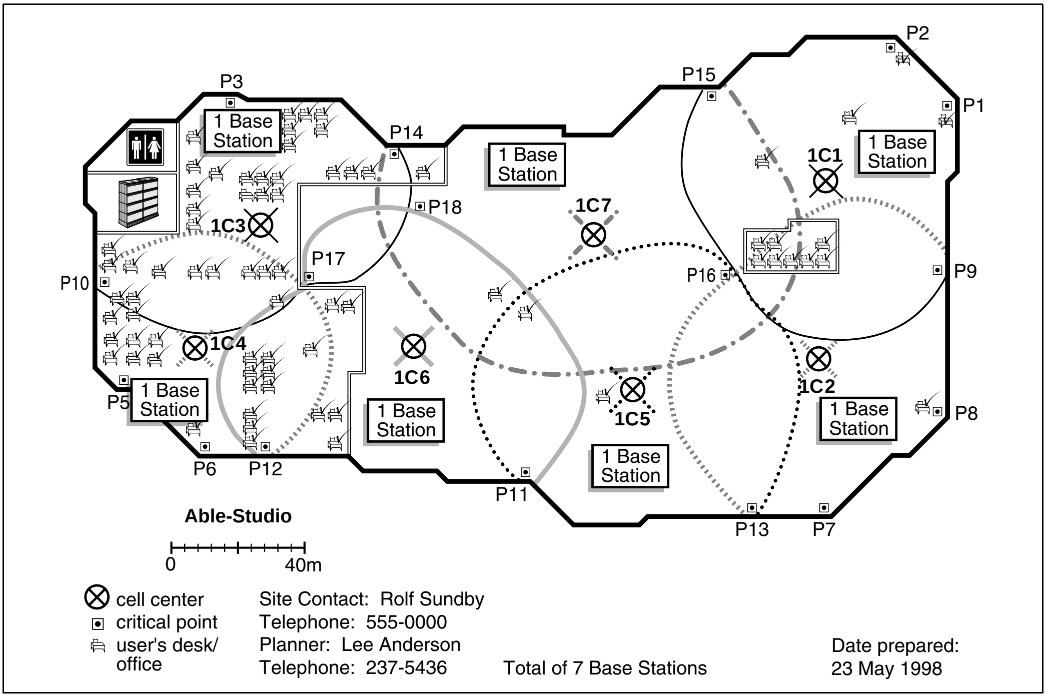
Completing a floor plan

Procedure 29
Completing a floor plan

Step	Action
1	Record the name and telephone number of the planner on the floor plans.
2	Record the name of the customer company on the floor plans.
3	Record the site contact name and telephone number on the floor plans.
4	Record any installation restrictions.
5	Record the details of the installation of an identified cell on the floor plans, recording any 12-channel basestations.
6	Record the positions of user offices on the floor plans.

END

Figure 103
Example of a completed floor plan



Checking system capacity

Procedure 30
Checking system capacity

Step	Action
1	Check that the system does not exceed the DECT system capacity: that is, no more than 512 handsets or 128 basestations for the system with no more than sixty-four 12-channel basestations.
2	Check that there is no cell limit for a DECT system. The limit is the total count of the basestations.
3	Check that the limits on basestations and handsets are independent of each other. Increasing the handset count does not decrease the number of basestations available to install.
4	If more than 128 basestations are deployed, it is necessary to replan the site with multiple systems. See the Detailed Site Planning section.
5	Ensure that the location of the controller is not more than 1500 m (wiring length for Category 5 UTP) from all 6-channel basestations or 1000 m from 12-channel basestations (unless external power is used). If the location is farther than the allowed distance, the customer must examine other installation and equipment configurations with the sales representative and Nortel support personnel.

END

Review with the customer

When the planning is finished, show the customer:

a the final positions of the basestations with a walk-about; and,

b the areas, if any, where the coverage requirements cannot be met.

Record floor plan information

Provide the planning information to the installer or the sales group. It is important that this information be communicated in a clear and accurate way.

Neatly transfer the information from the working copy to the clean copy of the floor plan. Use the coloured markers to mark the cell boundaries and matching cell centres.

Record or attach the following information to the floor plans.

1. All areas needing coverage.
2. The location of the controller.
3. The total number of all basestations.
4. All the named cell centres (for example, 2C5) and their matching cell boundaries.
5. All the critical points that were used.
6. Any installation restrictions.
7. Any notes detailing the installation at a identified cell, recording any 12-channel basestations.
8. The location of any basestation servicing outdoor areas, and the current restrictions on the placing of those basestations.
9. Attach a completed traffic table with the floor plans.

Record provisioning record information

Record the following information on the applicable provisioning record.

1 The date prepared

2 The Customer information

3 The Deployer information (name)

4 The cell numbers

5 The location of the basestations (cell centres)

6 The calculated number of users in each cell

7 Include some notes on the agreed coverage area of the site and any information for the installer

Review the work

At the completion of the site plan, ensure that you have:

a a customer, satisfied with the plan for a DECT system;

b a clean floor plan with all the information, as shown in Figure 103;

c a traffic table; and,

d a completed provisioning record.

Installation and configuration

Contents

This chapter contains information on the following topics:

Before you begin

The following three tasks must be completed before DECT is installed.

1 The site survey

2 The deployment

3 The installation of the house wiring for basestations

After these tasks have been completed, the following information and materials are required before continuing with DECT installation.

- Site work order
- List of equipment to be installed, showing quantities
- A marked-up floor plan
- A volt/ohm meter
- Hand tools and hardware, such as:
  - screwdrivers and pliers
  - spanners and socket wrenches
  - drill and drill bits
  - screws and screw anchors
  - punch-down tools for MDF and RJ45 Connect Box
  - cable continuity checking equipment

Unpacking the equipment

To unpack the equipment, complete the steps in the following table.

Procedure 31
Unpacking and examining the equipment

Step	Action
1	Check the items shipped for discrepancies against the list of equipment required for the installation.
	If any items are missing, take the action that is appropriate for this situation.
2	Carefully unpack and examine the equipment for damage.
	If any items are missing, take the action that is appropriate for this situation.

END

> ***Note:*** Store the equipment containers away from the installation area. Use the containers to return damaged equipment.

Using the Provisioning Records, marked-up floor plans, and the site work order, the installation proceeds in this sequence:

1 Install basestation

2 Install additional IPE shelves or cabinets

3 Install DMC8 cards and faceplate cables

4 Install OTM DECT application

5 Configure DECT on the OTM server

6 Configure handsets and retrieve subscription data

7 Handset subscription

8 Basestation Power and Muting

9 Add a V.24 serial connection

Provisioning records

The DECT Provisioning Records consist of the following:

- System Site Information Record
- Provisioning Information Record
- Installation Record
- System Programming Record
- Handset User Information Record

A copy of these records must be kept at the customer site. Vendors involved in maintaining DECT must also have a copy of these records.

> ***Note:*** Use a pencil to record information that can vary. Make photocopies of the tables as necessary.

System information record

Contacts

Client	
Company name	
Address	
Contact name	
Telephone number	
Billing number	
Date received	

Supplier	
Company name	
Address	
Contact name	
Telephone number	
Invoice number	
Date shipped	

Installer	
Name	
Installation date	

Provisioning information record

Basestation cell

Sheet ______

Cell label	Basestation location	Number of Basestation	Basestation number

Installation record

Basestation connection

Sheet ______

Basestation number	MDF designator or I/O panel label	MDF RJ45 number

TN to DECT TN assignment

Sheet ______

TN	DECT TN	TN	DECT TN

System programming record

System name: ____________________________

PARI licence string: ____________________________

Handset user information record

Sheet__________

username	DN	WRLS TN	MCRD/ MCRA	CLS	CNDD/ CNDA

Installing the basestation

Following the DECT basestation rules, installation involves the following tasks:

- Install C4600 and C4610 basestations:
  - Install basestation wiring to the MDF.
  - Install the C4610 basestation external power supply.
- Install basestation in the external housing.
- Attach the external housing to a wall.
- Connect the external housing wiring to the MDF.

Rules and guidelines

The following rules and guidelines apply to basestation installation.

- For dc-powered systems, an input voltage of at least –48 volts is required for maximum basestation line length.
- One hundred ohms is the maximum line length for a C4610 high traffic basestation. If the line measurement approaches 100 ohms, use an external power supply.
- If the exact location is not accessible, mount the basestation as close as possible to the location in the site survey.
- Mount the basestation in a vertical position, not horizontally, on a ceiling.
- Lead the basestation cable directly away from the basestation. Surplus cable can cause basestation malfunctions.
- Place the basestation where it is unlikely to be damaged. For example, a basestation in a warehouse must be placed where it cannot be damaged by a forklift truck.
- Surrounding objects must not affect the basestation. For example, a basestation in a car park must be placed higher than any vehicle parked next to it.

- The minimum distance between two basestations must be greater than two metres.
- Do not mount basestations on large concrete or stone columns, air ducts or large metal objects.
- The external basestation is powered from the line connection and does not require a mains connection.
- Use the external housing kit to mount any basestation out-of-doors.
- Use the external housing kit for any basestation subject to conductive pollution or dust that can become conductive due to condensation.

Compatibility

The C4600, C4610, and C4610E basestations are compatible with all software releases for DECT, Meridian 1, CS 1000S, and CS 1000M systems. The basestations are backward compatible.

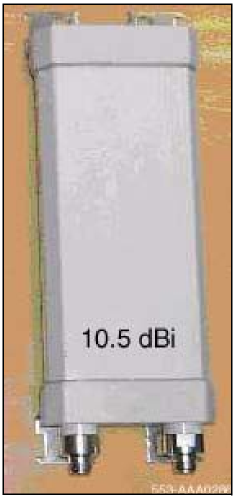
C4610E and external antenna

The C4610E 12-channel basestation has an adaptor to support an external antenna. The external antenna increases the operating distance between the basestation and the DECT handset. Nortel recommends the use of a Hoper & Suhner dual-planar directional antenna. Directional antennas are suitable for use in places such as large halls, outside parking lots, and between buildings. See Figure 104 on page 285.

> ***Note:*** The Huber & Suhner 8.0dBi and 10.5dBi antenna packages were tested with the C4610E basestation. Other third-party directional antenna are available, but have not been tested with this basestation.

For information on installing an external antenna, see “Installing a C4010E basestation in external housing with an external antenna” on page 298.

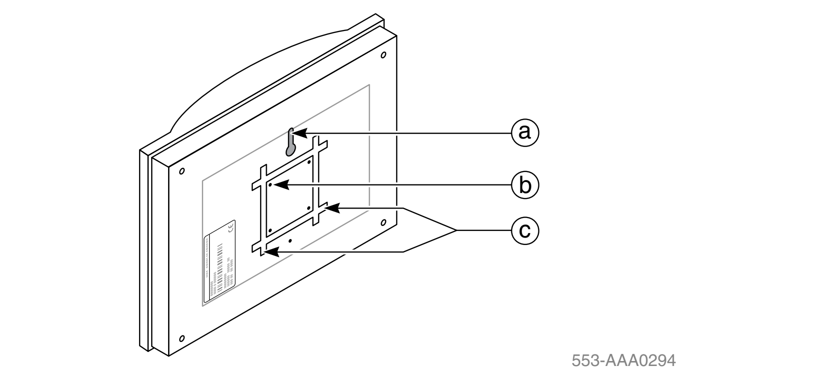
Figure 104
A Huber & Suhner dual-planar directional antenna



Installing C4600, C4610, and C4610E basestations

Consult the work order and marked-up floor plan to determine the position of the basestation, then perform the steps in Table 32 on page 286.

Figure 105
Basestation mounting details



Key

a	screw mounting slot
b	screw and cable tie retaining washer hole
c	cable tie grooves

Procedure 32
Installing C4600, C4610, and C4610E basestation

Step	Action
1	Locate the basestation mounting position.
2	Install the basestation mounting screw.
	If required, drill the holes for a screw anchor and install the anchor.
3	Fasten the basestation on the wall or a building protrusion.
	Hang the basestation on the screw or use cable ties to mount the basestation. Insert the cable ties in the vertical or horizontal grooves on the back of the basestation. Secure the cable ties to the basestation with the retaining washers and screws provided. Fasten the cable ties to the building protrusion.
4	If installing the C4610E basestation, install the external antenna according to the instructions provided by the manufacturer.

END

Installing the wiring to the MDF

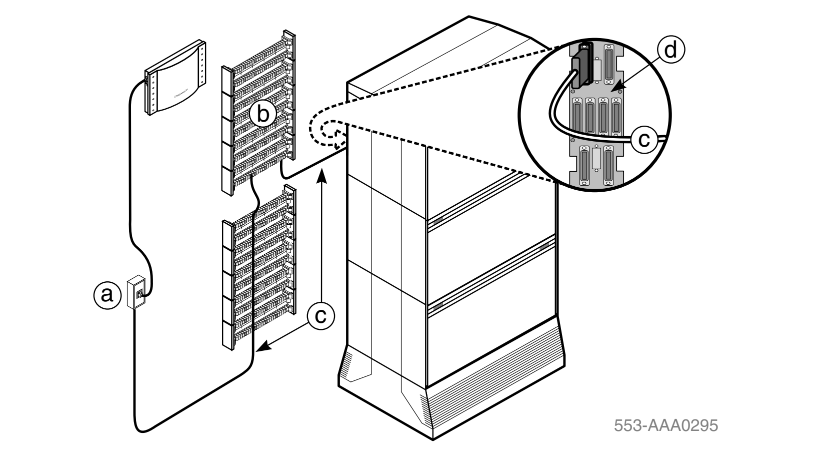
Consult the work order and marked-up floor plan to determine the basestation to MDF connections, then follow the steps in Procedure 33 on page 288.

CAUTION — Service Interruption

For maximum line length before signal degradation occurs, use UTP Cat 5 cabling between the basestation and the shelf or cabinet. If the line length exceeds 100 ohms for the 4610 basestation, an external power supply must be used.

The maximum distance when using external power with UTP Cat 5 cabling is approximately 1.7 km.

Figure 106
Basestation, MDF, and I/O panel details



Key

a RJ45 Connection Box

b MDF

c recommended UTP Cat 5 cable

d IPE shelf I/O connector panel

Procedure 33
Installing basestation wiring to the MDF

Step	Action
1	Connect one end of the NTCW10 cable into the basestation RJ45 jack.
	Use the supplied cable.
2	Install the RJ45 Connection Box.
	Use the NTCW10 cable length to measure the location of the RJ45 Connection Box.
3	See Table 27 on page 289 for connection details.
	Note 1: Ensure that the cable is ***twisted pair*** *from beginning to end*. ***Note 2:*** If there are other twisted pairs available then ensure that the other pairs in the cable are not used for analogue interfaces.
4	Connect the free end of the NTCW10 cable into the RJ45 Connection Box.

END

Note: The BIX tip and ring connections shown in Table 27 on page 289 correspond to standard BIX designation. The first pair are labeled T0 and R0. See *Communication Server 1000M and Meridian 1: Large System Installation and Configuration* (553-3021-210), chapter *Planning and designating the Modular Distribution Frame (MDF)*.

Figure 107
RJ45 Connection Box pin-out

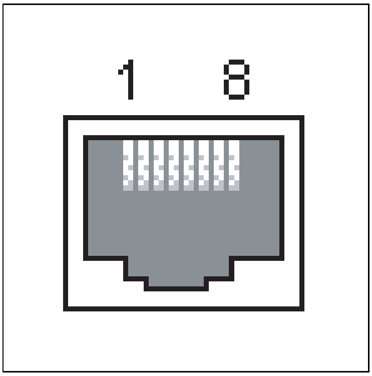


Table 27
Basestation RJ45 to BIX MDF connections (Part 1 of 2)

Basestation number	RJ45 Connection Box	MDF connection
Basestation 1	5 4 6 3	T8 R8 T9 R9
Basestation 2	5 4 6 3	T10 R10 T11 R11

Table 27
Basestation RJ45 to BIX MDF connections (Part 2 of 2)

Basestation number	RJ45 Connection Box	MDF connection
Basestation 3	5	T12
	4	R12
	6	T13
	3	R13
Basestation 4	5	T14
	4	R14
	6	T15
	3	R15
Basestation 5	5	T16
	4	R16
	6	T17
	3	R17
Basestation 6	5	T18
	4	R18
	6	T19
	3	R19
Basestation 7	5	T20
	4	R20
	6	T21
	3	R21
Basestation 8	5	T22
	4	R22
	6	T23
	3	R23

Installing the external power supply

For the C4600, C4610, and C4610E basestations, an external power supply must be installed if the UTP Cat 5 line resistance exceeds 100 ohms.

Figure 108
C4610 basestation external power

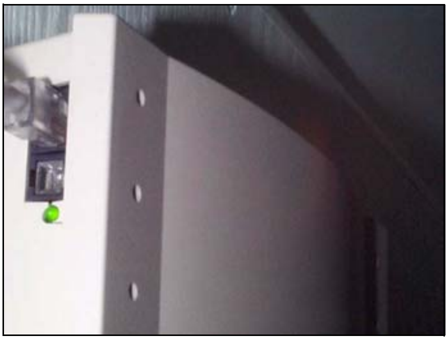
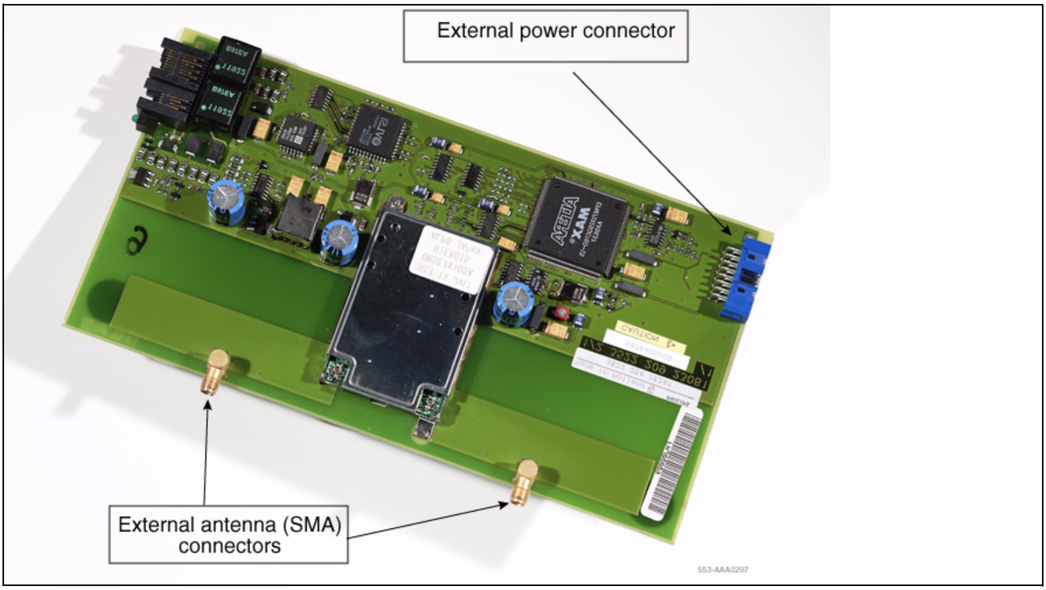


Figure 109
C4610E external power and external antenna connectors



Procedure 34
Installing C4610 basestation external power supply

Step	Action
1	Remove the plastic stopper from the C4610 basestation power socket.
	The power socket is located next to the yellow LED.
2	Plug the external power supply jack into the C4610 basestation power socket.
3	Connect the external power supply to the ac mains outlet.

END

Installing the external housing

Consult the work order, then perform the steps in this section as required.

The section provides the following procedures:

1 "Installing C4600 and C4010 basestations in the external housing" on page 292

2 "Installing a C4010E basestation in external housing with an external antenna" on page 298

3 "Mounting the cabinet" on page 306

Procedure 35
Installing C4600 and C4010 basestations in the external housing

1 Open the cabinet by inserting the cabinet key and turn right.

2 Remove the foam from the cabinet as far as is shown Figure 110 on page 293.

3 Mount the swivel, and lead the incoming cable through it. Make sure that the cable inlet is waterproof. Connect the incoming cable to the connection box that is delivered with the outdoor cabinet. Also connect the CAT5 cable that is inside the outdoor cabinet to the connector box. See pictures below. For connections see Figure 111 on page 294.

Figure 110
External housing: connect cables

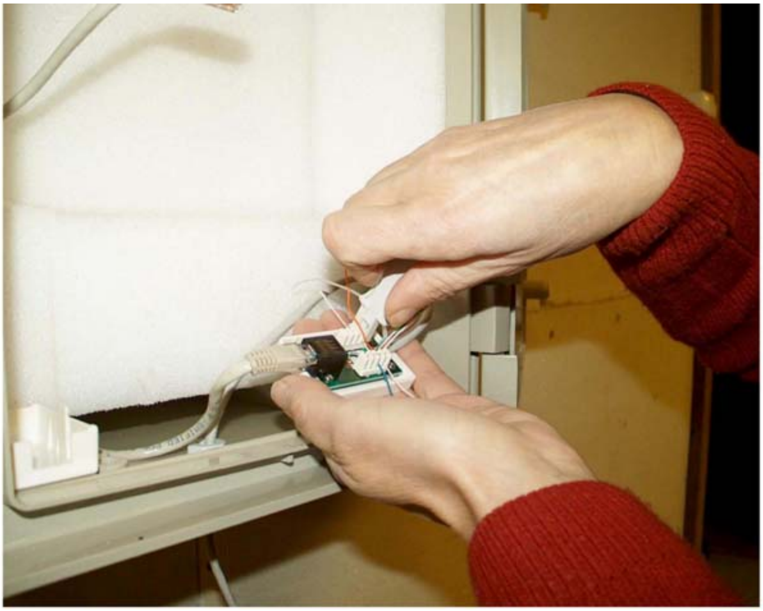
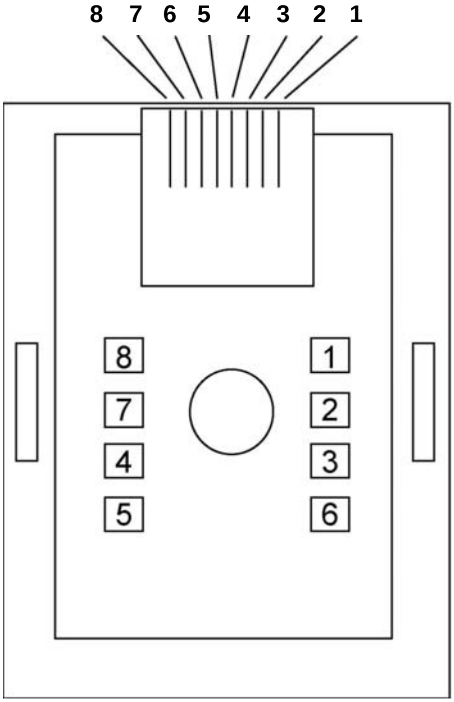
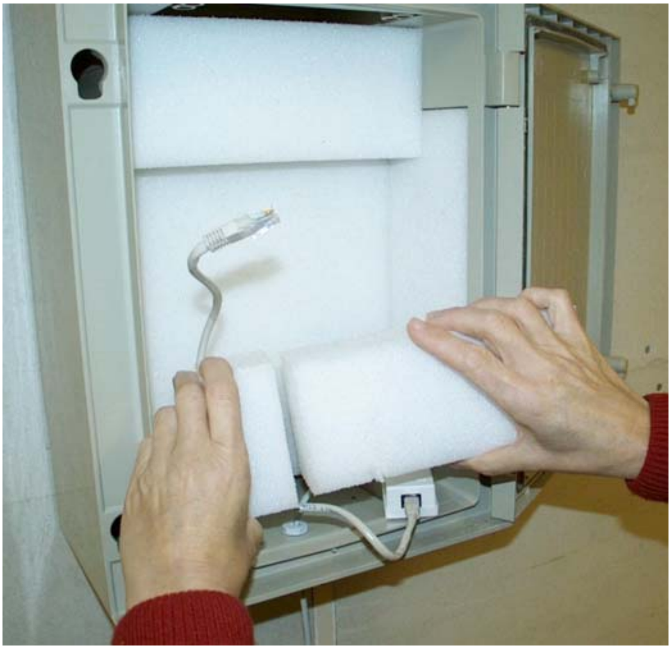


Figure 111
External housing: connector box layout



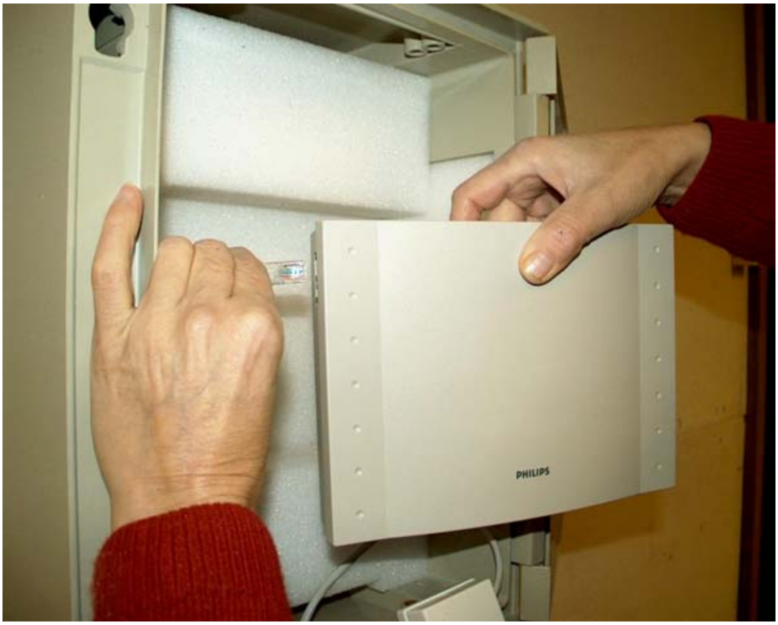
4 Place the foam below the foam blocks as shown Figure 112.

Figure 112
External housing: place foam blocks



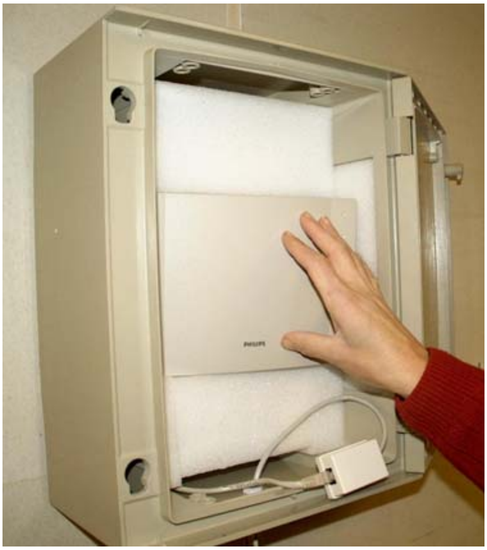
5 Connect the Ethernet CAT5 to the C4600/C4010 basestations as shown in Figure 113.

Figure 113
External housing: connect Ethernet CAT5



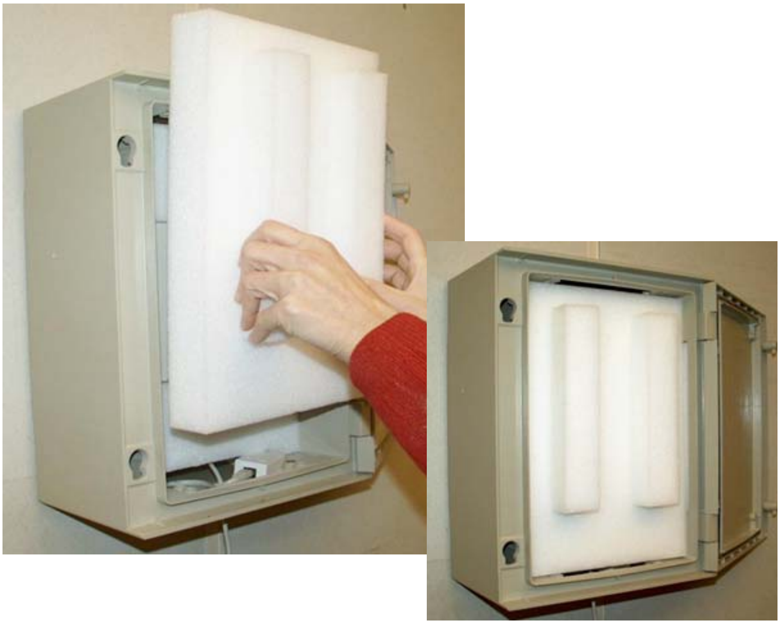
6 Push the C4600/C4010 basestations in the foam as shown in Figure 114.

Figure 114
External housing: basestation in foam



7 Place the cover foam into position as shown in Figure 115.

Figure 115
External housing: place the cover foam



8 Close and lock the cabinet.

End of Procedure

Procedure 36
Installing a C4010E basestation in external housing with an external antenna

1 Unpack the C4010E basestation.

2 Open the cabinet of the C4010E basestation.

To open the cabinet remove the two screws at the rear side of the cabinet. Then separate the cover and the rear side from each other.

Note: The cabinet is closed by four "click" parts, two at each long side of the cabinet. If necessary, use a small screwdriver to carefully open the click parts one-by-one.

3 Drill two holes (10 mm in diameter) in the rear side of the cabinet. See figure 2 for the dimensions.

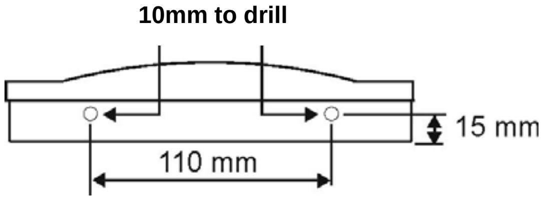
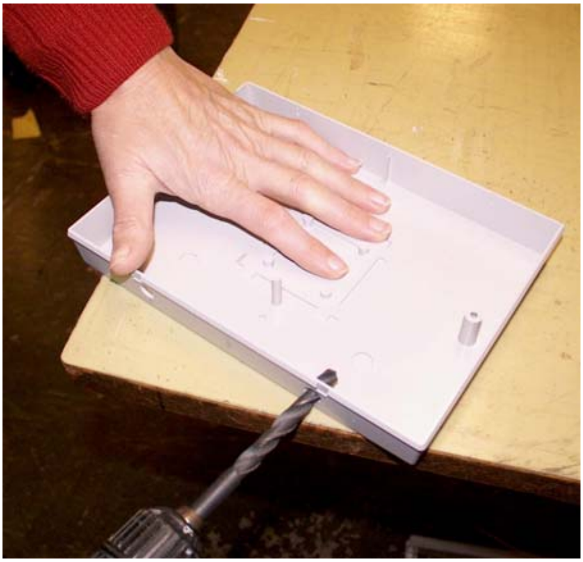
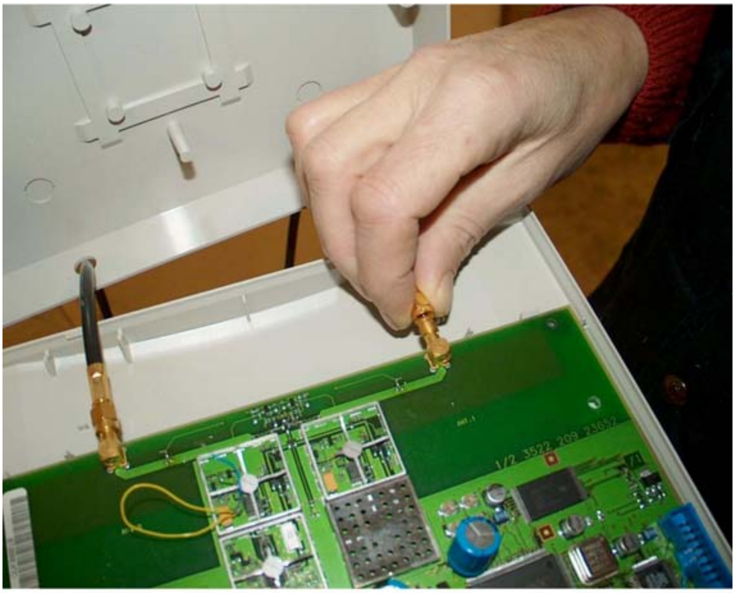


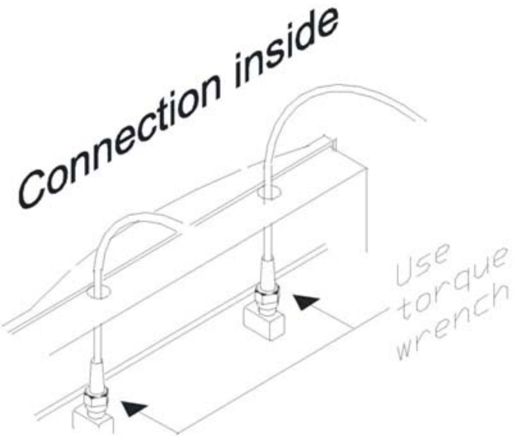
Figure 116
External housing: drill cabinet for external antenna



4 Connect the antenna cables to the connectors on the printed circuit board. Secure the nuts with an SMA Torque Wrench. See Figure 117 on page 300.

Figure 117
External housing: connection inside the C4010E basestation cabinet





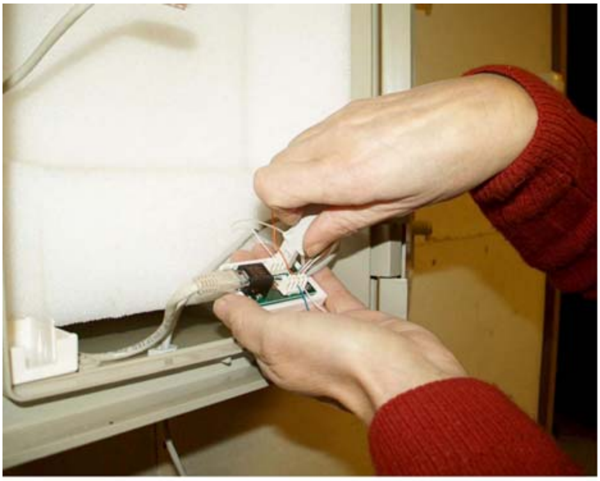
5 Snap the cover of the C4010E basestation to the rear side, to close the C4010E basestation cabinet. Fasten the cabinet by mounting the two screws into the two holes in the rear side of the cabinet.

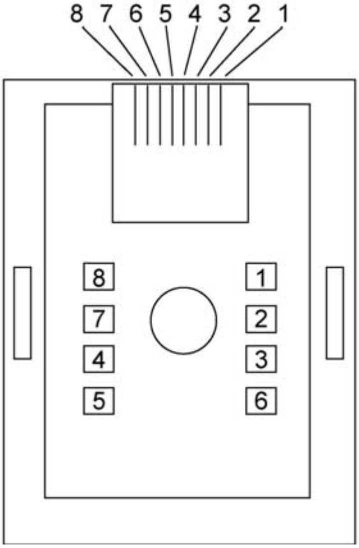
6 Insert the cabinet key and turn right to open the outdoor isolated cabinet.

7 Remove the foam blocks from the cabinet as far as shown in Figure 118 on page 302.

8 Mount the swivel, and lead the incoming cable through it. Make sure that the cable inlet is waterproof. Connect the incoming cable to the connection box that is delivered with the outdoor cabinet. Also connect the CAT5 cable that is inside the outdoor cabinet to the connector box. For connections see Figure 118 on page 302.

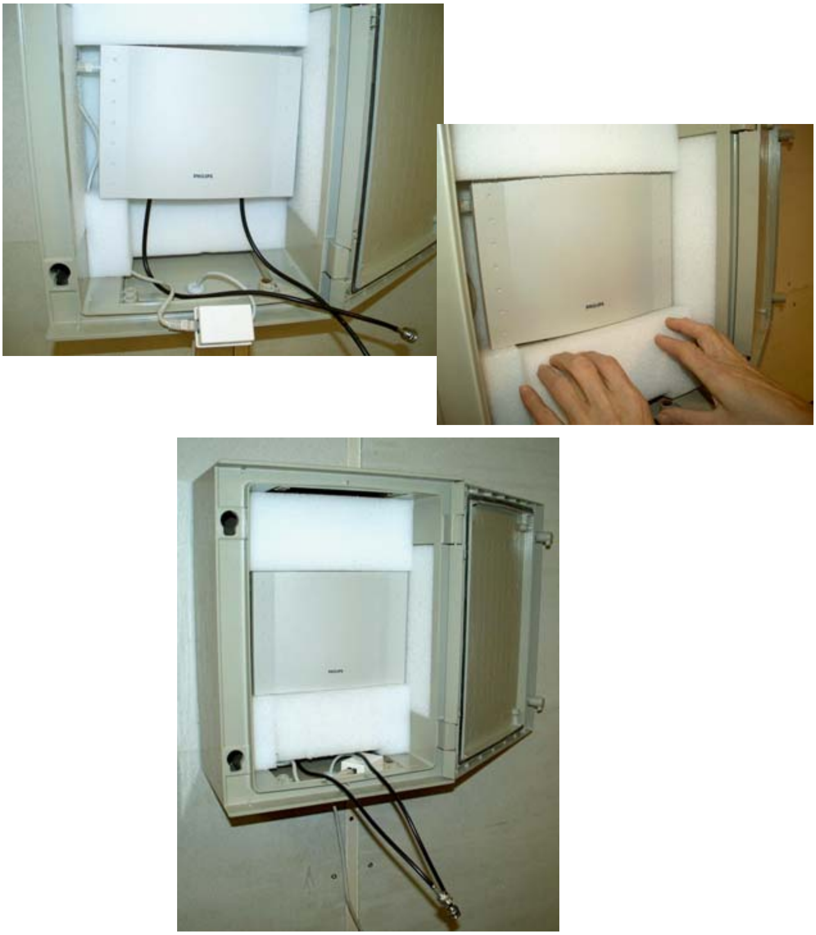
Figure 118
External housing: connections





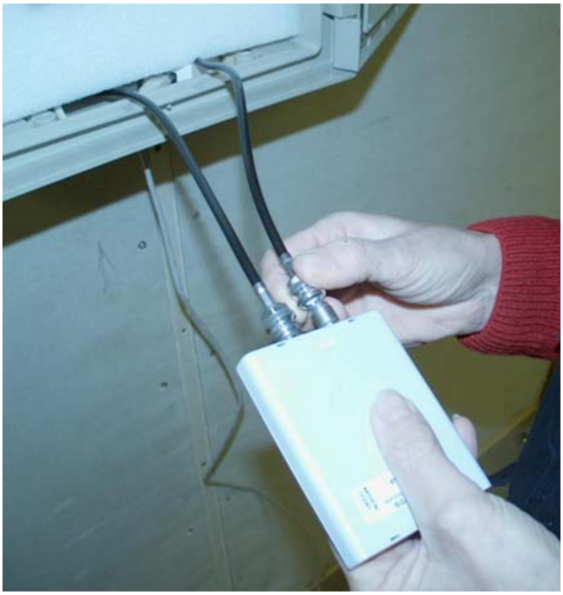
9 Connect the Ethernet CAT5 cable to the C4010E basestation. Place the C4010E basestation in the outdoor cabinet and install the foam. See Figure 119.

Figure 119
External housing: C4010E basestation and foam in place



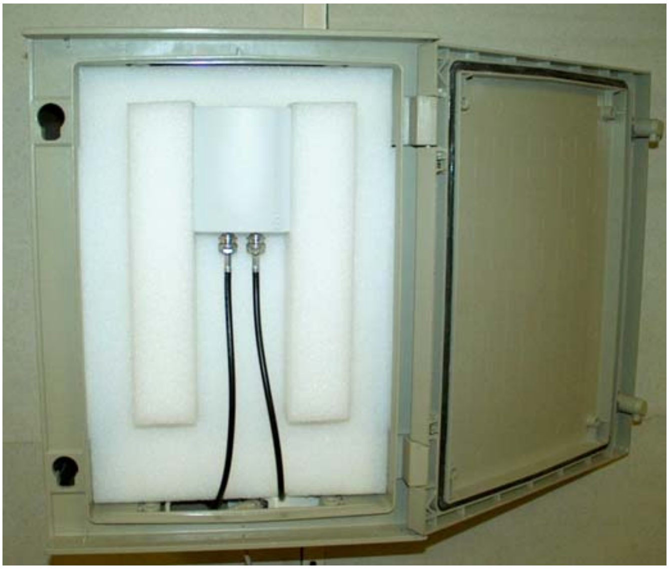
10 Connect the antenna cables to the antenna as shown in Figure 120.

Figure 120
External housing: connect antenna cables



11 Place the cover foam in position then place the antenna in the foam as shown in Figure 121.

Figure 121
External housing: place antenna in foam



12 Close and lock the outdoor cabinet.

IMPORTANT!

Ensure that the C4010E basestation is line powered through the Ethernet cable.

Local power provision is *not* possible in this outdoor cabinet.

End of Procedure

Mounting the cabinet

This section describes the following procedures:

- "Mounting the cabinet to the wall" on page 306
- "Mounting the cabinet to a pole" on page 308

Procedure 37
Mounting the cabinet to the wall

1 Mount the wall mount set on the back of the cabinet.

See Figure 122 on page 307.

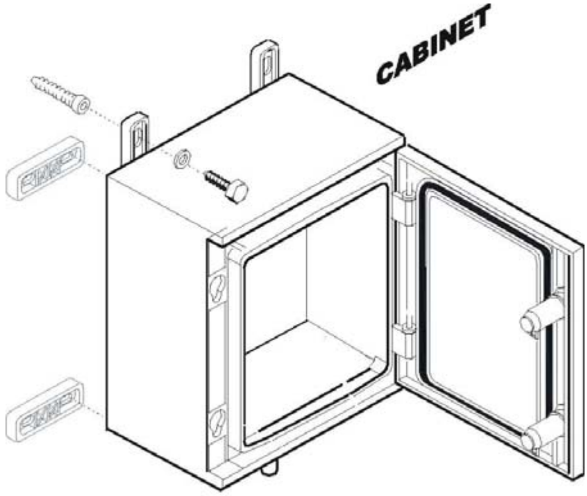
Note: Choose for horizontal or vertical mounting of the wall mount set.

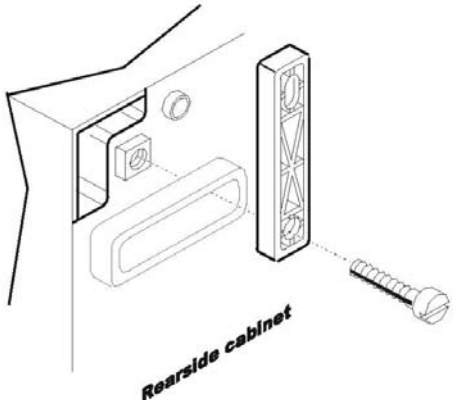
2 Use the drilling jig (suitable for horizontal and vertical configuration) for position of the drill holes.

3 Mount the cabinet to the wall.

End of Procedure

Figure 122
External housing: mounting the cabinet to a wall





Procedure 38
Mounting the cabinet to a pole

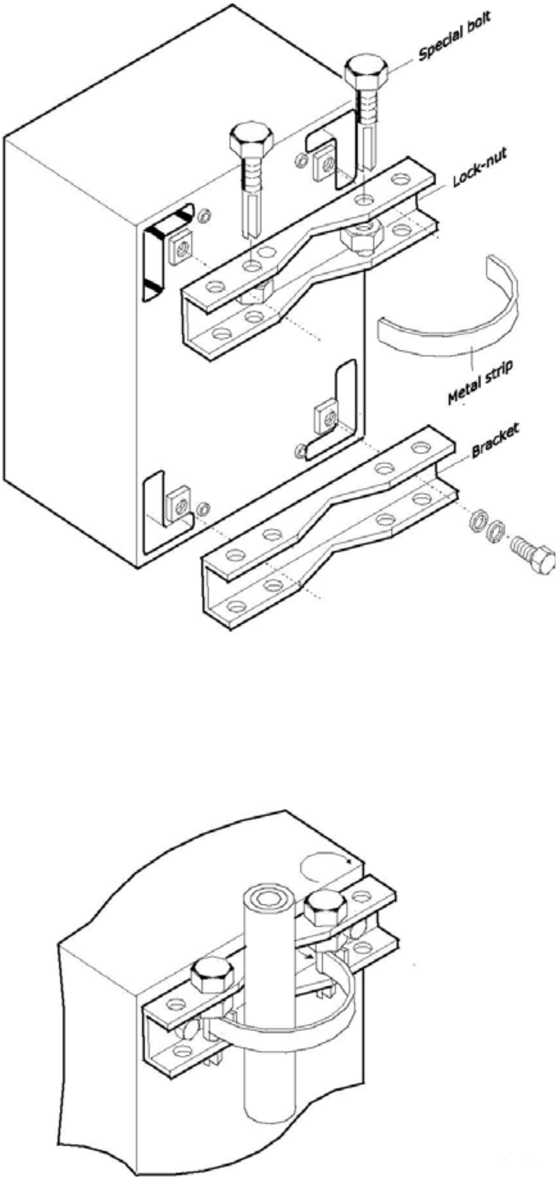
1. Mount the bracket to the back of the cabinet.

   See Figure 123 on page 309.

2. Connect the metal strip with the special bolt to the bracket.
3. Place the cabinet against the pole.
4. Lead the strip around the pole and connect the metal strip to the other side of the bracket (also with a special bolt).
5. Keep the cabinet at the right height and tighten the metal strip around the pole by twisting the special bolt.
6. Secure the metal strip with the lock-nuts.

End of Procedure

Figure 123
External housing: mount cabinet to pole



Installing additional IPE shelves or Small System cabinets

Installing additional IPE shelves or cabinets includes the following tasks:

- Install additional IPE modules.
- Install additional cabinets:
  - — Install IPE module wiring to the MDF.
  - — Install cabinet wiring to the MDF.

Installing additional IPE modules

Consult the work order and marked-up floor plan to determine if additional IPE modules are required, then perform the steps in Procedure 39 on page 310.

> ***Note:*** If unfamiliar with this process, refer to *Communication Server 1000M and Meridian 1: Large System Installation and Configuration* (553-3021-210).

Procedure 39
Installing additional IPE modules (Part 1 of 2)

Step	Action
1	Remove the IPE module front and rear covers.
	Remove the covers from the module on which the DECT module will sit.
2	Remove the air grills.
	Release the air grill tabs or Southco® fasteners and lift the air grill off.
3	Remove the top cap.
	Loosen and remove the three front and rear top cap bolts. Lift off top cap.
4	Unfasten the column LED.
	Remove the LED bracket bolts.
5	Remove the I/O back panel cover.

Procedure 39
Installing additional IPE modules (Part 2 of 2)

Step	Action
	Unlock the four Southco fasteners.
6	Disconnect the column LED.
	Unlock LED wiring connector latches on the module backplane. Detach the LED wiring connector.
7	Disconnect the thermal sensor connector.
	Unlock the sensor connector latches on the 36 pin orange/brown coloured connector, located to the left of the LED connector. Unplug the sensor connector.
8	Remove the EMI perf panel.
	Lift directly up.
9	Place the new module on top of the column.
	Keep hands and fingers out from under the module when placing the module on top of the equipment column.
10	Connect the new module wiring.
	Install the sensor connector of the new module into the vertical connector housing of the module below.
11	Secure the new module.
	Insert the five bolts and lock washers into the base of the new module. Tighten the bolts into the original module.
12	Attach the power cable.
	Connect the ribbon cable of the new module to J2 of the module below.
13	Reinstall the EMI perf panel and the LED.
	Install the LED connector and the sensor connector on the new module.
14	Replace the air grills and covers.
	Reverse the procedure for steps 1 to 4.

END

Installing additional Small System cabinets

Consult the work order and marked-up floor plan to determine if additional Small System cabinets are required, then perform the steps in Table 40.

Note: If you are not familiar with this process, refer to *Communication Server 1000M and Meridian 1: Large System Installation and Configuration* (553-3021-210).

> **DANGER — Electrostatic Sensitive Device**
>
> Wear a properly connected antistatic wrist strap to handle circuit cards. Only touch the edges. Do not touch the contacts or components. Set the cards on a protective antistatic bag. If an antistatic bag is not available, hand-hold the card, or set it in a card cage unseated from the connectors.

Procedure 40
Installing additional Small System cabinets (Part 1 of 3)

Step	Action
1	Mount the expansion cabinet.
	For a wall mount, draw a level line, rest the bottom of mounting bracket on the line, screw the mounting bracket to the wall. Hang the cabinet on the mounting bracket. Fasten the bottom of the cabinet to the wall. For a floor mount, install the cabinet on the pedestal. Position the cabinet according to the equipment layout plan.
2	Remove the drip tray.
	Slide drip tray outward.
3	Install ground wire.
	As a minimum, use #6AWG ground wire. Tag the main ground connection at the ground source to ensure it is not accidently discontinued. Test the ground.
4	Install the power supply.

Procedure 40
Installing additional Small System cabinets (Part 2 of 3)

Step	Action
	Wear the anti-static wrist strap. Turn power supply circuit breaker to OFF. Check the option switches on the power supply.
5	Install the fiber routing guide.
	Mount the guide in the area below the circuit cards and secure with the existing screws.
6	Connect the fiber optic cable or copper cable as applicable.
	For the A0618443 cable, remove the two plugs on the Fiber Receiver card. Connect the cable to the card so the V shaped groove is facing inward. For the glass fiber optic cable, remove the plug on one connector on the card, and the cap on the cable. Insert the connector and secure with a half turn clockwise. Wind the excess cable on the storage device.
7	Insert the circuit cards in the expansion cabinet.
	Refer to Install DMC8-Es Table 45 on page 328 and the work order for card placement.
8	Install or expand the MDF cross-connect terminal.
	Consult the marked-up floor plan for the MDF addition location.
9	Install cables from the cabinet to the MDF cross-connect.
	Consult the marked-up floor plan for the cable location.
10	Install PFTU and SDI cable if required.
	Consult the marked-up floor plan for the cable location.
11	Replace the expansion cabinet drip tray.
	Slide the drip tray inward.
12	Remove the main cabinet cover and drip tray.
	Undo the catches on the main cabinet and slide the drip tray outward.
13	Install a Fiber Routing guide in the main cabinet, if required.
	The Fiber Routing guide is secured to the under side of the bottom card rail and uses the screws to the left of the CPU card label and under the card 2 label.
14	Turn the power supply circuit breaker to OFF.

Procedure 40
Installing additional Small System cabinets (Part 3 of 3)

Step	Action
15	Unseat the NTDK20 SSC card and install a Fiber Expansion daughterboard.
	Connect the Fiber Expansion daughterboard to the connector Fiber 1” if this is the first expansion cabinet, or to Fiber 2” if this is the second expansion cabinet.
16	Connect the fiber optic cable to the Fiber Expansion daughterboard.
	For the A0618443 cable, remove the two plugs on the Fiber Receiver card. Connect the cable to the card so the V shaped groove is facing inward. For the glass fiber optic cable, remove the plug on one connector on the card and the cap on the cable. Insert the connector and secure with a half turn clockwise. Wind the excess cable on the storage device.
17	Re-seat the NTDK20 SCC card.
18	Route the fiber optic cable through the Fiber Routing Guide.
19	Set the circuit breaker in the main cabinet to ON.
	The system reloads. Check time and date using LD 2.
20	Reinstall the drip tray in the main cabinet.
21	Reinstall the main cabinet cover.

END

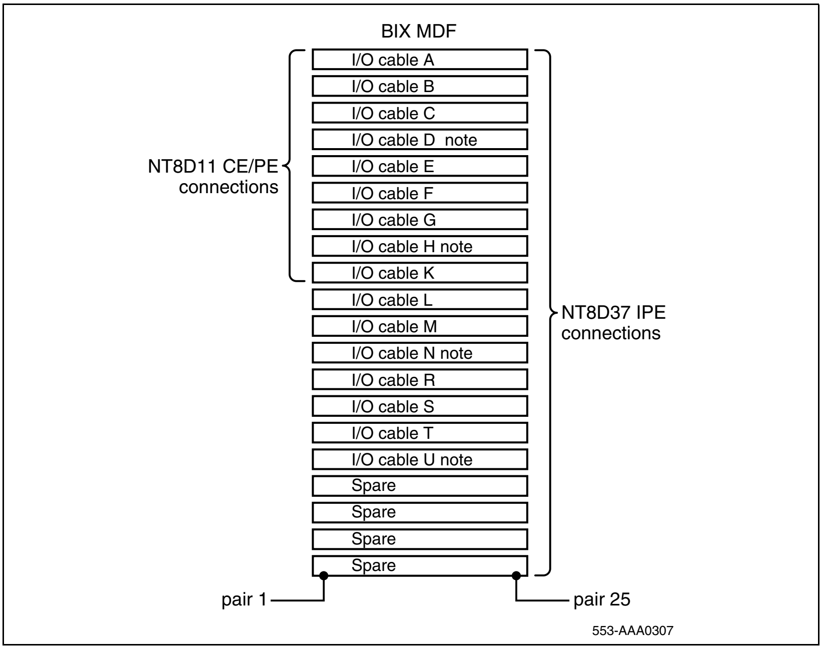
Installing IPE module wiring to the MDF

Consult the work order to determine the layout of the module I/O panel to MDF cabling route, then perform the steps in Table 41 on page 317.

CAUTION — Service Interruption

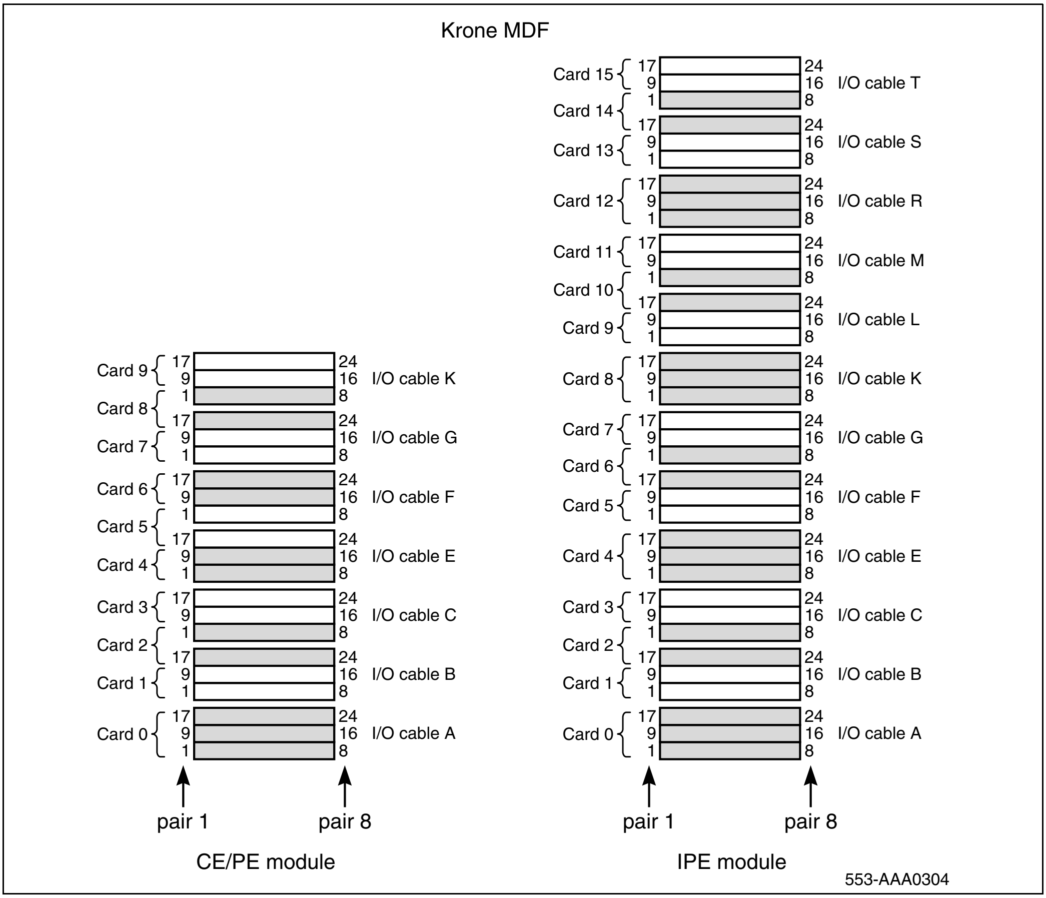
The existing MDF cabling can be used; however, Nortel recommends UTP Cat 5 – NTCW15, NTCW16, or NTCW17 MDF to PBX cabling, as it provides a greater line length before signal degradation occurs.

Figure 124
IPE I/O cable to BIX MDF termination



Note: The BIX connectors shown in Figure 124 are *not* used in NT8D11AC or NT8D11DC CE/PE and NT8D37AC or NT8D37DC IPE modules, but *are* used in the NT8D11BC or NT8D11EC CE/PE and NT8D37BA or NT8D37 EC IPE modules.

Figure 125
IPE I/O cable to Krone MD termination



Procedure 41
Installing IPE module wiring to the MDF

Step	Action
1	Identify the UTP Cat 5 twenty-five pair MDF cable.
	Label both ends of the cable with the IPE module number and the I/O panel letter designation.
2	Connect the IPE or cabinet end of the cable.
	Insert the Amphenol® connector on the cable into the appropriate I/O panel connector. See Table 28.
3	Run the cable to the MDF.
4	Terminate the cable on the MDF.
	For BIX MDF, refer to Figure 124 on page 315 to locate the BIX connectors and Table 28 on page 317 to locate the cable colour code. For Krone MDF, refer to Figure 125 on page 316 to locate the Krone connectors and Table 28 to locate the cable colour code.

END

Table 28
Colour code for 25 pair cable (Part 1 of 2)

Amphenol pin number	Tip	Ring
	Body/Band	**Body/Band**
26/1	White/Blue	Blue/White
27/2	White/Orange	Orange/White
28/3	White/Green	Green/White
29/4	White/Brown	Brown/White
30/5	White/Slate	Slate/White
31/6	Red/Blue	Blue/Red
32/7	Red/Orange	Orange/Red

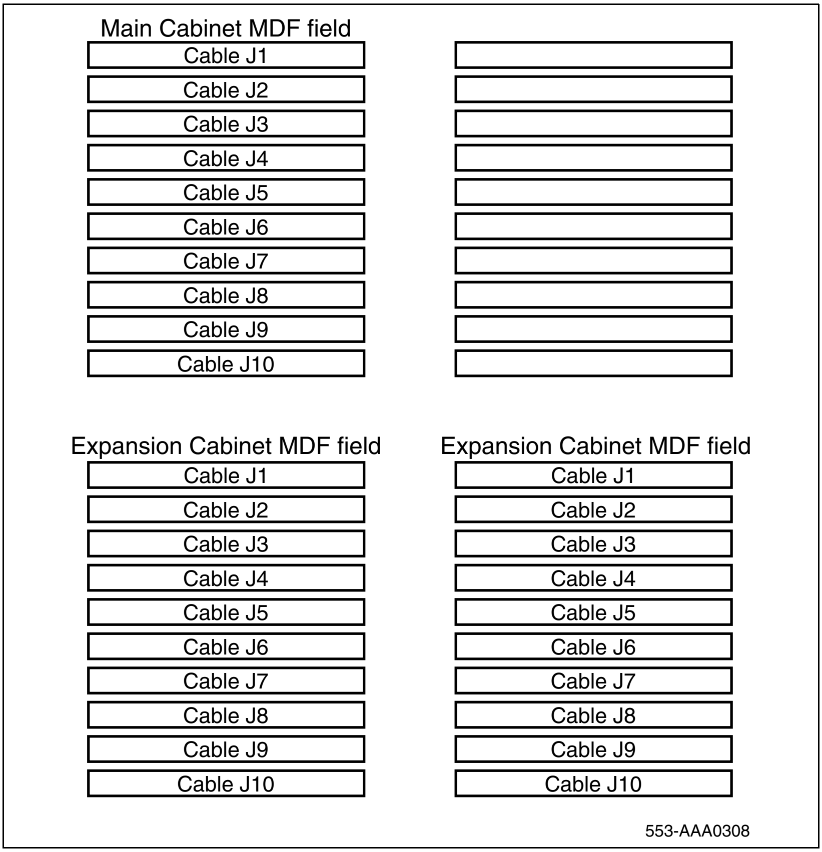
Table 28
Colour code for 25 pair cable (Part 2 of 2)

Amphenol pin number	Tip	Ring
	Body/Band	**Body/Band**
33/8	Red/Green	Green/Red
34/9	Red/Brown	Brown/Red
35/10	Red/Slate	Slate/Red
36/11	Black/Blue	Blue/Black
37/12	Black/Orange	Orange/Black
38/13	Black/Green	Green/Black
39/14	Black/Brown	Brown/Black
40/15	Black/Slate	Slate/Black
41/16	Yellow/Blue	Blue/Yellow
42/17	Yellow/Orange	Orange/Yellow
43/18	Yellow/Green	Green/Yellow
44/19	Yellow/Brown	Brown/Yellow
45/20	Yellow/Slate	Slate/Yellow
46/21	Violet/Blue	Blue/Violet
47/22	Violet/Orange	Orange/Violet
48/23	Violet/Green	Green/Violet
49/24	Violet/Brown	Brown/Violet
50/25	Violet/Slate	Slate/Violet

Installing Small System cabinet wiring to the MDF

Consult the work order to determine the Small System cabinet-to-MDF cabling route, then perform the steps in Table 42 on page 320.

Figure 126
Meridian 1 PBX 11C Cabinet



Procedure 42
Installing Small System cabinet wiring to the MDF

Step	Action
1	Identify the UTP Cat 5 twenty five pair MDF cable.
	Label both ends of the cable with the cabinet jack number.
2	Connect the cabinet end of the cable.
	Insert the Amphenol connector on the cable into the appropriate cabinet connector jack.
3	Run the cable to the MDF.
4	Terminate the cable on the MDF.
	For BIX MDF, refer to Figure 126 on page 319 to locate the BIX connectors and Table 28 on page 317 to locate the cable colour code.

END

Expander installation

For information on installing an Expander, refer to *Communication Server 1000M and Meridian 1: Small System Installation and Configuration* (553-3011-210).

Media Gateway 1000S Expander installation

For information on installing a Media Gateway 1000S Expander (MG 1000S Expander), refer to *Communication Server 1000S: Installation and Configuration* (553-3031-210).

Installing DMC8 and faceplate cables

Installing the DMC8 cards and faceplate cables involves the following tasks:

1. Cross-connect basestations to the DMC8 positions.
2. Cross-connect basestations to the DMC8 Relay card.
3. Install DMC8 and DMC8-E in an IPE shelf.
4. Install DMC8-E in a Cabinet system.
5. Install faceplate cables and inter-shelf/cabinet cable.

Compatibility

The NTCW00xx DMC8 and NTCW01xx DMC8-E are compatible with the following software releases:

- Release 23 and later supports basic configuration, CLID and CPND, DECT card addressing within OA&M, 16 users per card.
- Release 24B and later supports 32 users per card.
- Release 25 and later supports MSMN and Concentration.

Cross-connecting basestations to the DMC8 positions

Consult the work order to determine the cross-connect details and perform the following steps.

CAUTION — Service Interruption

The jumper wire on the MDF must be at least UTP Cat 3. Nortel recommends UTP Cat 5, as it provides a greater line length before signal degradation occurs.

Procedure 43
Cross-connecting basestations to the DMC8 positions

Step	Action
1	Cross-connect from the basestation house side connector to the DMC8 equipment side connector.
	Connect a jumper wire from the tip and ring of the house side connector to the tip and ring of the equipment side connector. Refer to Table 29 on page 322 for the tip and ring designators. For DMC8s type NTCW00xx and NTCW01xx, connect from basestation 1 to basestation 8. **Note:** To support basestations 5, 6, 7, and 8 on NT8D37 (AA and DC) IPE modules, use 24 tip and ring pair backplane to I/O panel connections. To re-cable NT8D37 from 16 pair to 24 pair, see *Communication Server 1000M and Meridian 1: Large System Installation and Configuration* (553-3021-210).
2	Cross-connect the remaining basestations.
	Repeat step one until all basestations are cross-connected.

END

Note: The BIX tip and ring connections shown in Table 29 correspond to standard BIX designation. The first pair are labeled T0 and R0. See *Communication Server 1000M and Meridian 1: Large System Installation and Configuration* (553-3021-210), chapter *Planning and designating the Modular Distribution Frame (MDF).*

Table 29
Basestation tip and ring connections (Part 1 of 3)

Basestation number	Basestation MDF connection	DMC8 MDF connection
Basestation 1	T8	T8
	R8	R8
	T9	T9
	R9	R9

Table 29
Basestation tip and ring connections (Part 2 of 3)

Basestation number	Basestation MDF connection	DMC8 MDF connection
Basestation 2	T10	T10
	R10	R10
	T11	T11
	R11	R11
Basestation 3	T12	T12
	R12	R12
	T13	T13
	R13	R13
Basestation 4	T14	T14
	R14	R14
	T15	T15
	R15	R15
Basestation 5	T16	T16
	R16	R16
	T17	T17
	R17	R17
Basestation 6	T18	T18
	R18	R18
	T19	T19
	R19	R19
Basestation 7	T20	T20
	R20	R20
	T21	T21
	R2	R21

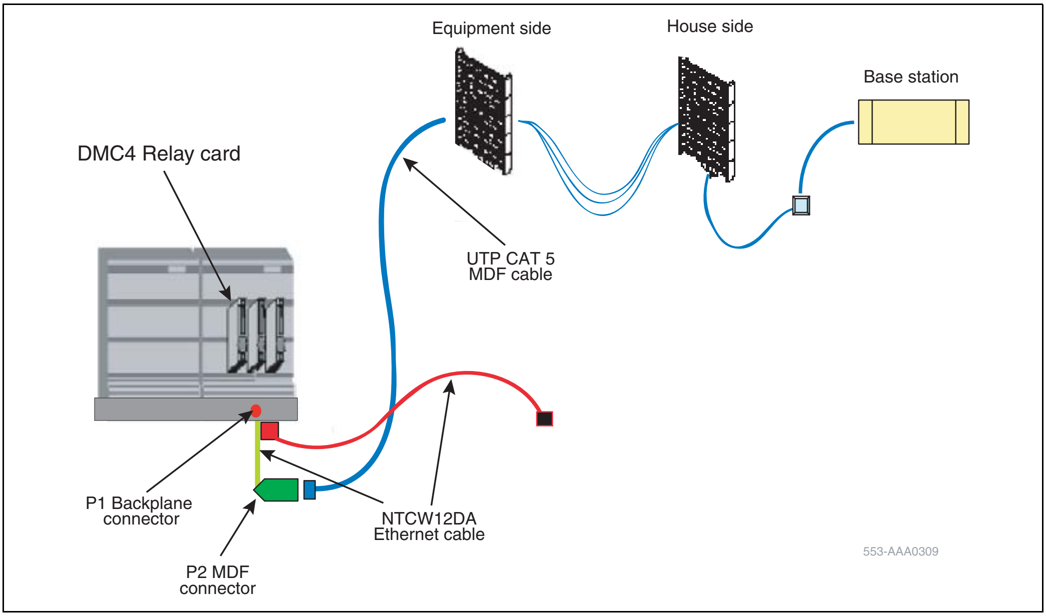
Table 29
Basestation tip and ring connections (Part 3 of 3)

Basestation number	Basestation MDF connection	DMC8 MDF connection
Basestation 8	T22	T22
	R22	R22
	T23	T23
	R23	R23

Cross-connecting basestations to the DMC8 Relay card

Consult the work order to determine the cross-connect details, then perform the steps in Table 44 on page 325.

Figure 127
DMC8 Relay card to basestation connections



Procedure 44
Cross-connecting basestations to the DMC8 positions

Step	Action
1	Connect the NTCW12DA cable to the DMC8 Relay card.
	Insert P1 into the DMC8 Relay card backplane connector located on the PBX shelf/ module or the Cabinet.
2	Connect the MDF cable to the NTCW12DA cable.
	Insert the MDF cable connector into P2.
3	Connect the MDF cable to the equipment side MDF cross-connect terminal block.
	See the chapter in *Communication Server 1000M and Meridian 1: Large System Installation and Configuration* (553-3021-210) that discusses *cabling lines and trunks.* See the chapter in *Communication Server 1000M and Meridian 1: Small System Installation and Configuration* (553-3011-210) that discusses *installing and connecting cross-connect terminal to cabinets.*
4	Cross-connect from the basestation house-side connector to the DMC8 Relay card equipment side connector.
	Connect a jumper wire from the tip and ring of the house-side connector to the tip and ring of the equipment-side connector. Refer to Table 29 on page 322 for the tip and ring designators. For DMC8s, type NTCW00xx and NTCW01xx connect from basestation 1 to basestation 8. To support basestations 5, 6, 7, and 8 on NT8D37 (AA and DC) IPE modules requires 24 tip and ring pair backplane to I/O panel connections. To re-cable NT8D37 from 16 pair to 24 pair, see *Communication Server 1000M and Meridian 1: Large System Installation and Configuration* (553-3021-210).

END

Installing DMC8 and DMC8-E in an IPE shelf

Refer to the work order and marked-up floor plan to determine the position of the DMC8 and DMC8-E, then perform the steps in Table 45 on page 328.

DANGER — Electrostatic Sensitive Device

Wear a properly connected antistatic wrist strap to handle circuit cards. Only touch the edges. Do not touch the contacts or components. Set the cards on a protective antistatic bag, whenever possible. If an antistatic bag is not available, hand-hold the card, or set it in a card cage removed from the connectors.

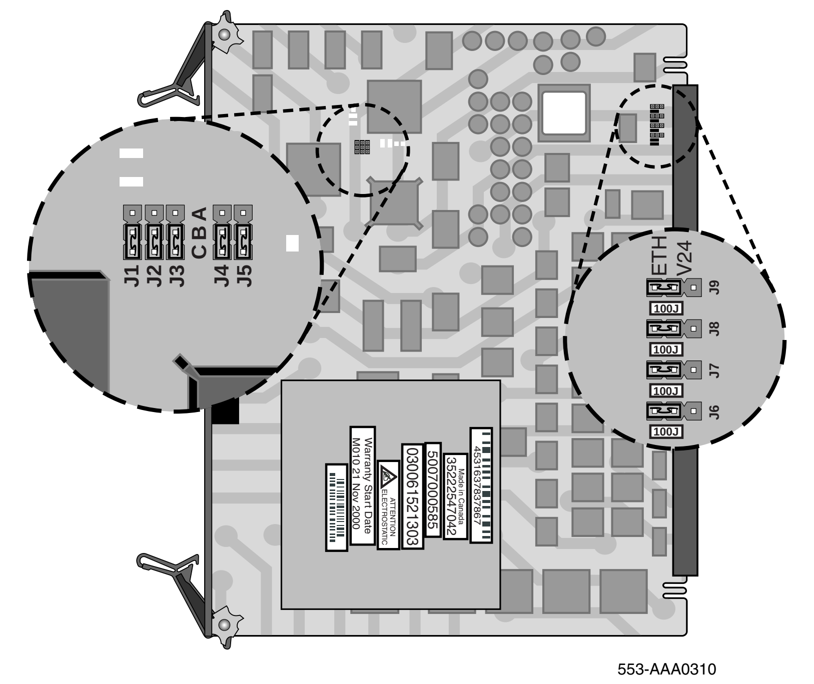
CAUTION — Service Interruption

Only install DMC8-Es in slot 8.

Note 1: Install the DMC8s next to each other so the faceplate cables connect to the ports.

Note 2: See “System software parameters” on page 173 for DMC8 and DMC8-E software package compatibility.

Figure 128
DMC8/DMC8-E jumper details



See Table 45 on page 328 for card jumper settings.

CAUTION — Service Interruption

Ensure that the DMC8/DMC8-E Relay card jumpers J6 to J9 are in the ETH position for operation on a dedicated LAN.

Ensure that the DMC8/DMC8-E Relay card jumpers J6 to J9 are in the V.24 position for operation on a serial connection to the OTM server.

Procedure 45
Installing DMC8 and DMC8-E in an IPE shelf

Step	Action
1	Install J1 jumper straps on the DMC8 and the DMC8-Es for Card ID.
	For pre-Release 23 software, strap A B. For post-Release 23 software, and Multi-Site Mobility Networking, strap B C.
2	Install J2 jumper straps on the DMC8 and the DMC8-Es for the system type.
	Strap A B for IPE shelf.
3	Install J3 jumper straps on the DMC8 and the DMC8-Es for cabinet or IPE shelf number.
	For shelf 0, the lower TN IPE shelf, strap B C. For shelf 1, the higher TN IPE shelf, strap A B.
4	Install J6 to J9 jumper straps on the DMC8 and the DMC8-Es used as the Relay card for either V.24 connection or Ethernet connection.
	For the V.24 connection, strap jumpers J6 to J9 to the V24 position. For the Ethernet connection, strap jumpers J6 to J9 to the ETH position.
5	Insert DMC8-Es, if required.
	Place DMC8-Es in slot 8.
6	Insert DMCs.
	Place DMC8s in the slots as indicated on the work order. Do not place DMC8s in slot 8.

END

Figure 129
Example of a full system housed in two IPE shelves

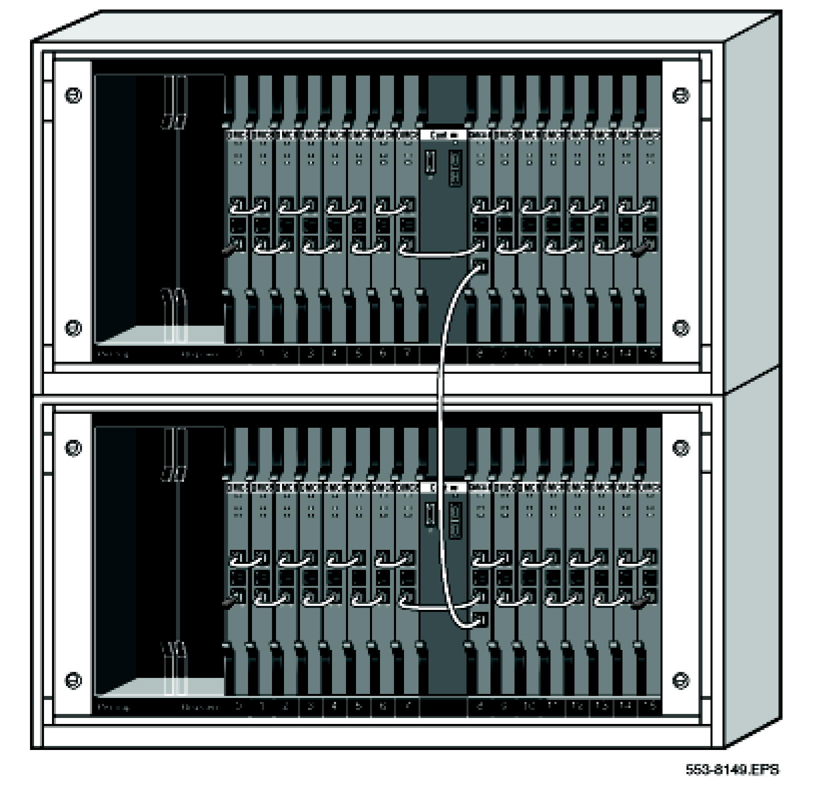


Figure 130
Example of a 16 card system housed in two IPE shelves

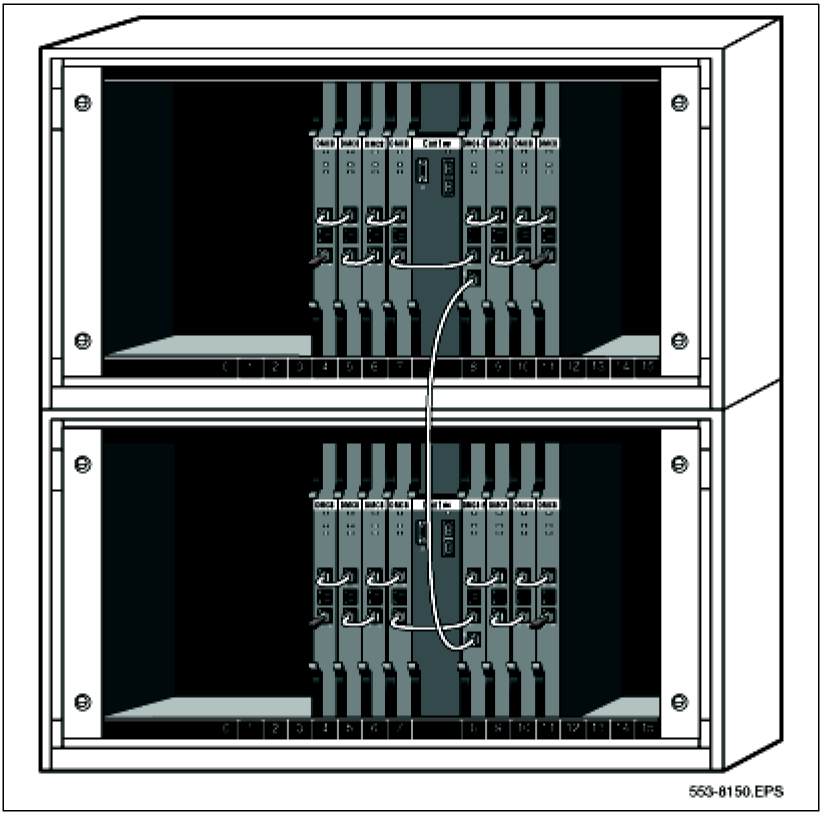


Figure 131
Example of a 17 card system housed in two IPE shelves

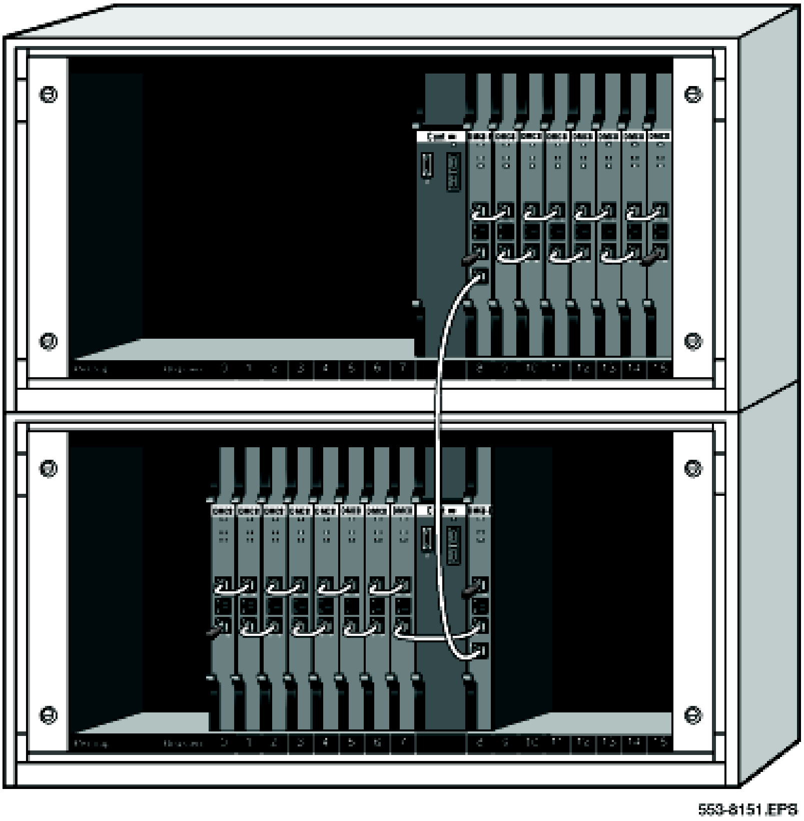
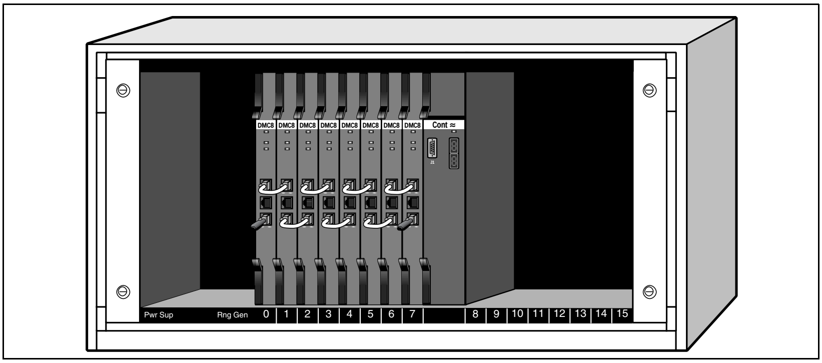


Figure 132
Example of an eight card system housed in one IPE shelf



Installing DMC8-E in a Small System or CS 1000S

Consult the work order and marked-up floor plan to determine the position of the DMC8 and DMC8-Es, then perform the steps in Procedure 46 on page 334.

DANGER — Electrostatic Sensitive Device

Wear a properly connected antistatic wrist strap when handling circuit cards. Handle cards by the edges only. Do not touch the contacts or components. Set the cards on a protective antistatic bag, whenever possible. If an antistatic bag is not available, hand-hold the card, or set it in a card cage unseated from the connectors.

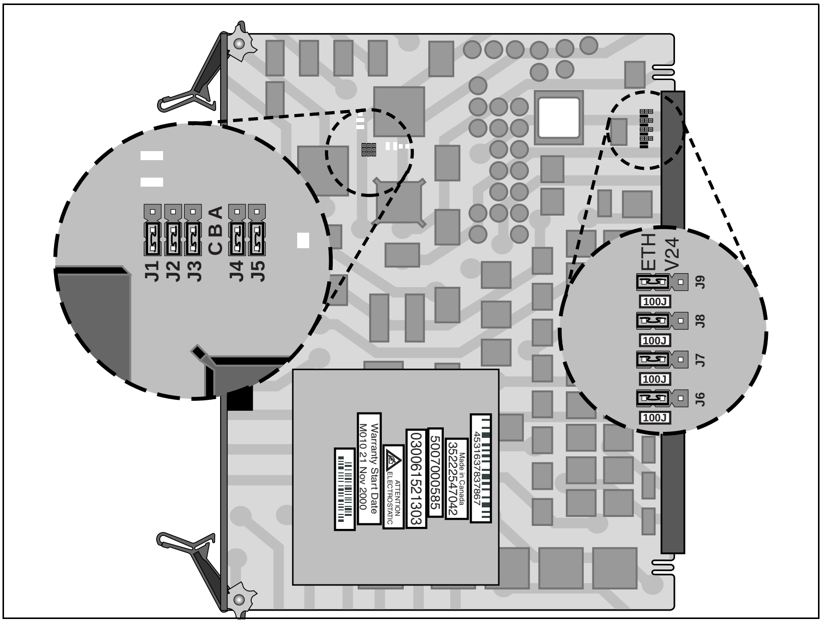
CAUTION — Service Interruption

Do not install DMC8-Es into any slot except slots 9, 19, or 29.

Note 1: The DMC8s must be adjacent to each other so the faceplate cables can be connected to the ports.

Note 2: See System software parameters, page 173 for DMC8 and DMC8-E software package compatibility.

Figure 133
DMC8/DMC8-E jumper details



See Table 45 on page 328 for card jumper settings.

CAUTION — Service Interruption

Ensure that the DMC8/DMC8-E Relay card jumpers J6 to J9 are in the ETH position for operation on a dedicated LAN.

Ensure that the DMC8/DMC8-E Relay card jumpers J6 to J9 are in the V.24 position for operation on a serial connection to the OTM server.

Procedure 46
Installing DMC8-E in a Cabinet or Chassis

Step	Action
1	Install J1 jumper straps on the DMC8 and the DMC8-Es for Card ID.
	For pre Release 23 software strap A B. For post Release 23 software, and Multi-Site Mobility Networking, strap B C.
2	Install J2 jumper straps on the DMC8 and the DMC8-Es for system type.
	Strap B C for Cabinet, Chassis, MG 1000S, or MG 1000S Expander.
3	Install J3 jumper straps on the DMC8 and the DMC8-Es for shelf number.
	For the lower TN cabinet, strap B C. For the higher TN cabinet, strap A B.
4	Insert DMC8-Es, if required.
	Place DMC8-Es in slot 9, slot 19 or slot 29. See examples in Figure 134, Figure 135, Figure 136, and Figure 137.
5	Install J6 to J9 jumper straps on the DMC8 and the DMC8-Es used as the Relay card for either V.24 connection or Ethernet connection.
	For the V.24 connection strap jumpers J6 to J9 to the V24 position. For the Ethernet connection strap jumpers J6 to J9 to the ETH position.
6	Insert DMC8s.
	Place DMC8s in the slots as indicated on the work order. Do not place DMC8s in slot 9, slot 19 or slot 29.

END

Figure 134
Example of full Small System without CPU cabinet

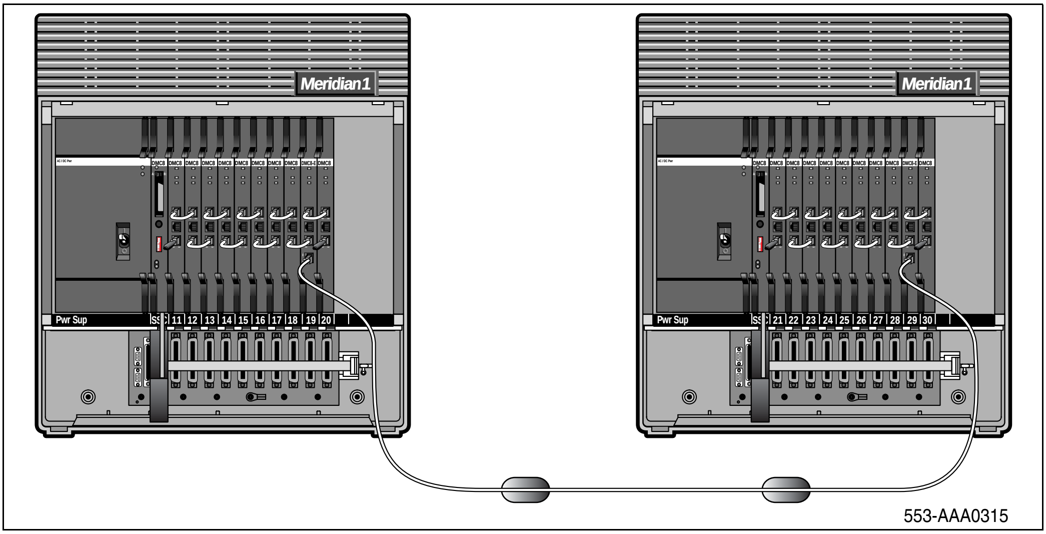


Figure 135
Example of full Small System with CPU cabinet

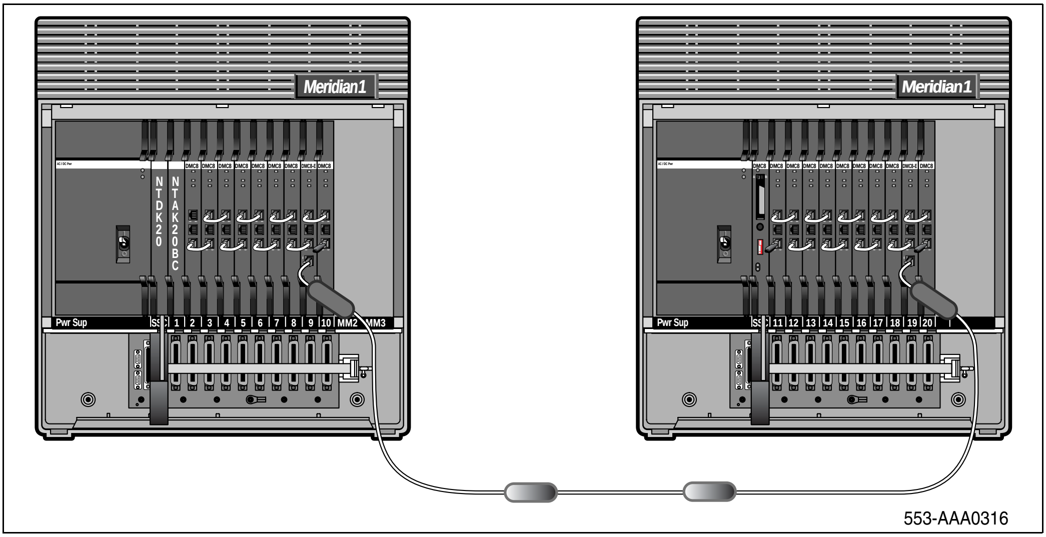


Figure 136
Example of an 8-card system in two Cabinets

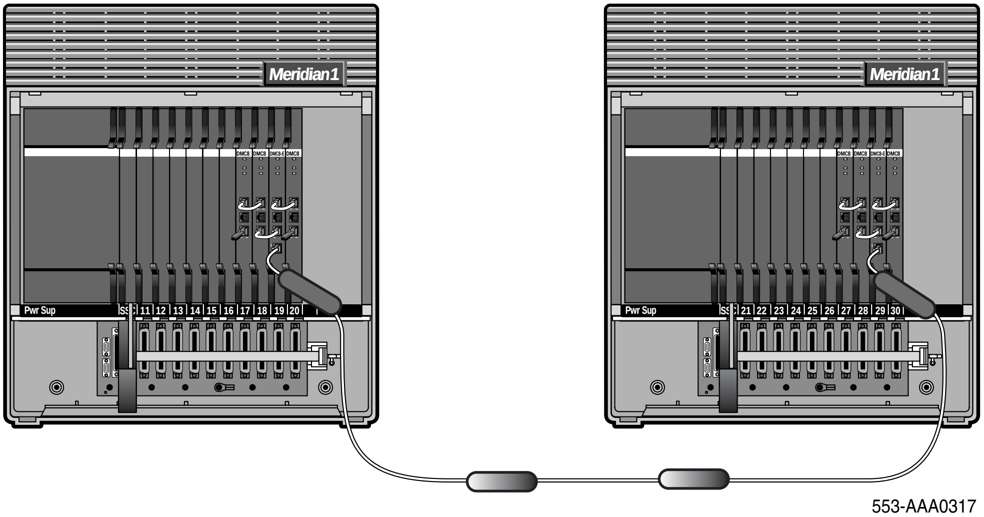
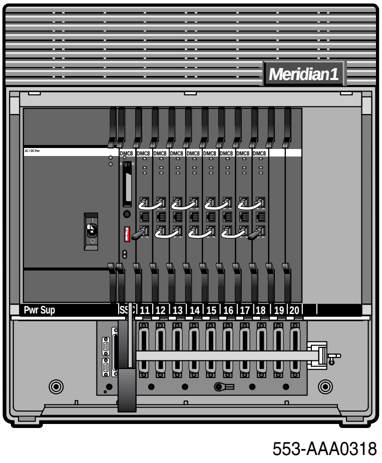


Figure 137
Example of an 8-card system in one Cabinet



Chassis installation

For information on installing circuit cards, refer to *Communication Server 1000M and Meridian 1: Small System Installation and Configuration* (553-3011-210).

Figure 138
Chassis and Expander connected with 2 NTDK95 and CE-MUX/DS-30SX bus cables

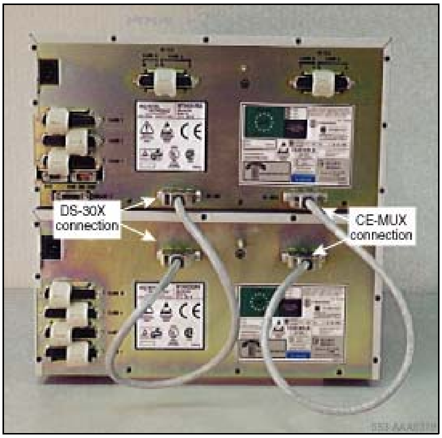
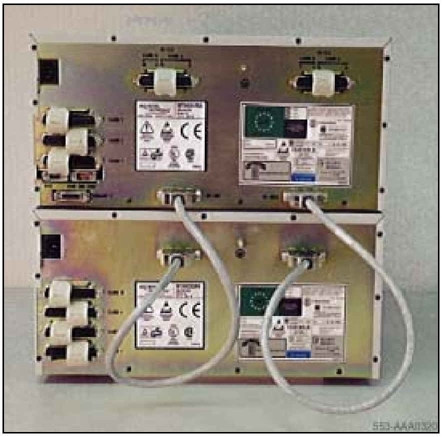


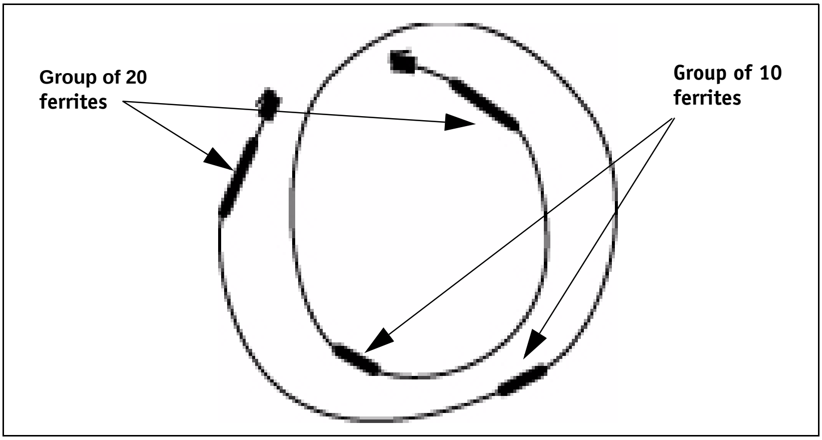
Figure 139
MG 1000S and MG 1000S Expander cabling



Installing faceplate cables and inter-shelf/cabinet cable

Consult the work order to determine the position of the faceplate cable layout and NTCW11EA DMC8-E to DMC8-E inter-shelf cables, then perform the steps in Table 47 on page 339.

Figure 140
NTCW11EA DMC8-E to DMC8-E faceplate cable



CAUTION — Service Interruption

The NTCW11EA DMC8-E to DMC8-E faceplate cable has four sets of movable ferrites. The position of the ferrites on the cable is important.

Each end of the cable must have a group of 20 ferrites. One quarter of the distance from each end of the cable must have a group of 10 ferrites. The maximum length of the cable is 1.5 metres, limiting the position of DECT shelves 0 and 1 to adjacent IPE modules or Small System cabinets.

Consult the work order to determine the position of the terminator plugs, then perform the following steps.

Procedure 47
Installing faceplate and inter-shelf/cabinet cables

Step	Action
1	Connect the DMC8 to DMC8 faceplate cables.
	Arrange the NTCW11AA DMC8 to DMC8 cables so that the DMC8 to DMC8-E cable is connected into the ports shown in Figures 129 to Figure 132.
2	If required, connect the NTCW11BA DMC8 to DMC8-E cable on the IPE shelf. Not required on Option 11C Cabinet.
	Plug the cable into the lower port of the DMC8 in slot 7. Plug the other end of the cable into the arrow pointing left port of the DMC8-E in slot 8. See Figure 129, Figure 130, and Figure 131.
3	Connect the NTCW11EA DMC8-E to DMC8-E inter-IPE shelf or inter-cabinet cable, if required.
	Plug the DMC8-E to DMC8-E cable into each DMC8-E lower port.

END

Installing the OTM DECT application

Installing OTM DECT application involves the following tasks:

- Ensure the DECT application is on the OTM server:
  - — Ensure a Communications Profile is associated with the DECT application.
  - — Add a Communications Profile for the DECT application.
  - — Add an Ethernet profile.

Connecting to a DECT system

When the first connection to a new, installed DECT system is opened, the OTM DECT Application retrieves the DMC configuration from the OTM database. The OTM DECT Application reads the parameters from the DECT system for the manager database.

Perform one of the following actions to open a connection to a DECT system from an OTM DECT Application:

- Check the Permanent Connection box, allowing the connection to open when the OTM server starts. See Figure 22 on page 120.
- Select a DECT system in the list and click the Connect icon.
- Select an action on the menu bar that requires a system connection. For example, when **Firmware** > **Upload** is chosen, the connection opens to carry out the upload and then closes.

  Note: Do not use this type of connection for subscription actions. When using this type of connection, the subscription status is not refreshed when an on-air subscription or de-subscription occurs.

The status bar of the application provides progress feedback while the connection opens.

Synchronizing the DECT Application to a DECT system

When the DECT Manager connects to DECT, synchronization occurs. Synchronization compares the database on the DECT Manager to the DECT system. Database mismatches are flagged by dialogs. The opportunity is then given to change either the system data or manager data.

A number of synchronization steps occur during connection. The Synchronization process flags changes made to a DECT system database by other managers.

Two types of synchronization occur when the connection state goes from **Disconnected** to **Connected**:

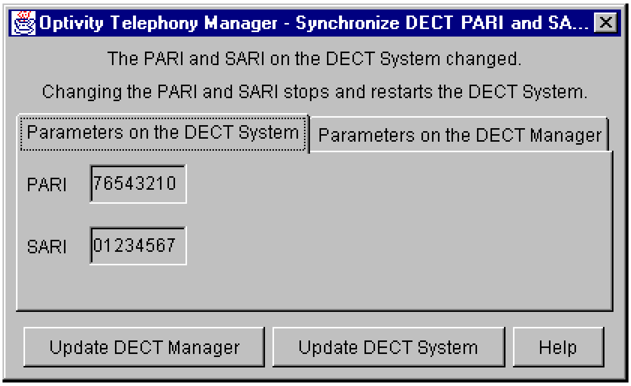
1 When the File menu or tool button is used to connect. The synchronization can be controlled through dialogs.

2 When the OTM re-establishes a permanent connection to DECT. A synchronization report is available in the Event log in the OTM server.

When connecting to a DECT system that has data that does not match the OTM DECT Application data, do one of the following:

- Update the OTM DECT Application database from DECT data.
- Update DECT data with the OTM DECT Application database.

Figure 141
Synchronize DECT PARI and SARI Mismatch dialog



Optivity Telephony Manager - Synchronize DECT PARI and SA...

The PARI and SARI on the DECT System changed.

Changing the PARI and SARI stops and restarts the DECT System.

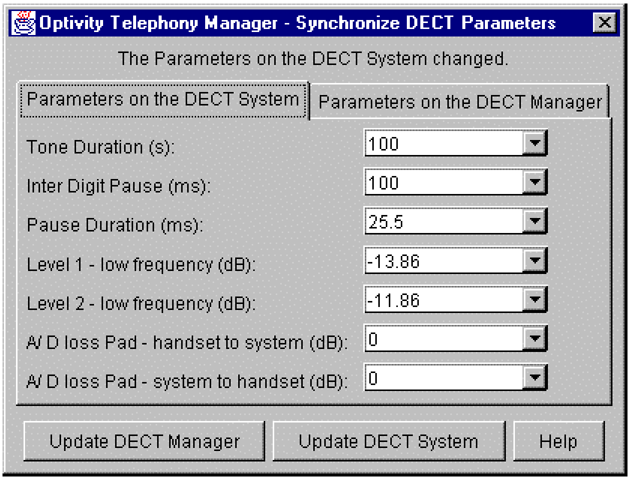
Parameters on the DECT System | Parameters on the DECT Manager

PARI 76543210

SARI 01234567

If there is a PARI or SARI mismatch between the OTM DECT Application database, and the DECT database, the mismatch dialog enables the update of PARI and SARI parameters on both the connected DECT system and the OTM DECT Application. See Figure 141.

Figure 142
Synchronize DECT Parameters Mismatch dialog



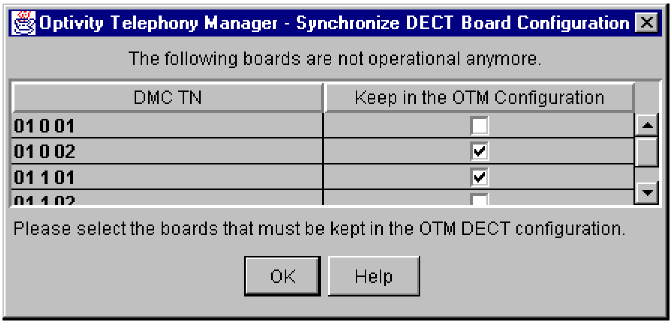
Optivity Telephony Manager - Synchronize DECT Parameters

The Parameters on the DECT System changed.

Tone Duration (s):	100
Inter Digit Pause (ms):	100
Pause Duration (ms):	25.5
Level 1 - low frequency (dB):	-13.86
Level 2 - low frequency (dB):	-11.86
A/ D loss Pad - handset to system (dB):	0
A/ D loss Pad - system to handset (dB):	0

If there is a Parameter mismatch between the OTM DECT Application database, and the DECT system database, the mismatch dialog enables the update of Parameters on both the connected DECT system and the OTM DECT Application. See Figure 142.

Figure 143
Synchronize DECT Board Configuration Mismatch dialog



Optivity Telephony Manager - Synchronize DECT Board Configuration

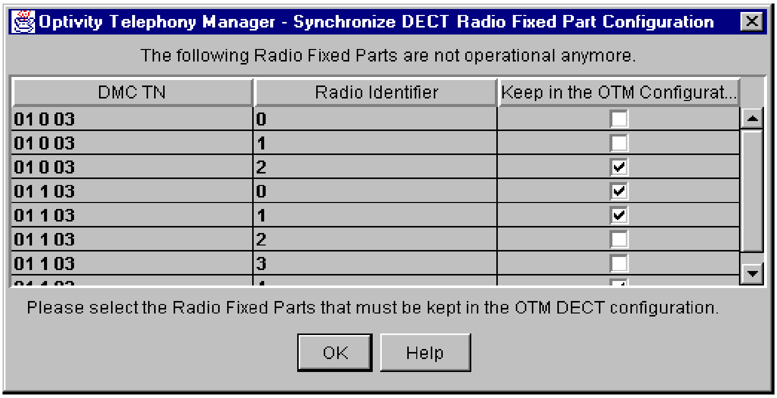
The following boards are not operational anymore.

DMC TN	Keep in the OTM Configuration
01 0 01	☐
01 0 02	☑
01 1 01	☑
01 1 02	☐

Please select the boards that must be kept in the OTM DECT configuration.

Figure 143 shows DMC TNs (Boards) listed in the OTM DECT Application database that are not operational on the DECT system. Delete the check in the check boxes. This allows the DMCs that are no longer required in the OTM DECT Application database to be removed.

Figure 144
Synchronize DECT Radio Fixed Part Configuration Mismatch dialog



Optivity Telephony Manager - Synchronize DECT Radio Fixed Part Configuration

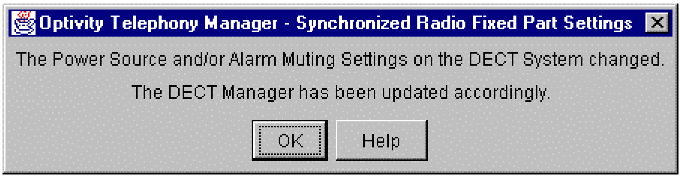
The following Radio Fixed Parts are not operational anymore.

DMC TN	Radio Identifier	Keep in the OTM Configurat...
01 0 03	0	□
01 0 03	1	□
01 0 03	2	☑
01 1 03	0	☑
01 1 03	1	☑
01 1 03	2	□
01 1 03	3	□

Please select the Radio Fixed Parts that must be kept in the OTM DECT configuration.

Figure 144 shows Radio Fixed Parts (basestations) listed in the OTM DECT Application database that are not operational on DECT. Delete the check in the check boxes. This allows the basestations no longer required in the OTM DECT Application database to be removed.

Figure 145
Synchronize Radio Fixed Part Settings Mismatch dialog



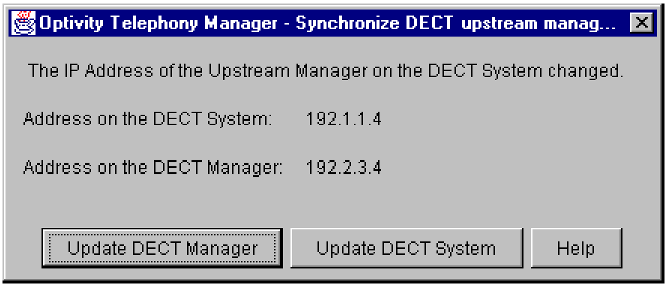
Optivity Telephony Manager - Synchronized Radio Fixed Part Settings

The Power Source and/or Alarm Muting Settings on the DECT System changed.

The DECT Manager has been updated accordingly.

A Power Source/Alarm Muting setting was changed by another manager. Figure 145 says that the OTM DECT Application database automatically updates to match the changed settings.

Figure 146
Synchronize DECT Upstream Manager IP Address Mismatch dialog


Optivity Telephony Manager - Synchronize DECT upstream manag...

The IP Address of the Upstream Manager on the DECT System changed.

Address on the DECT System: 192.1.1.4

Address on the DECT Manager: 192.2.3.4

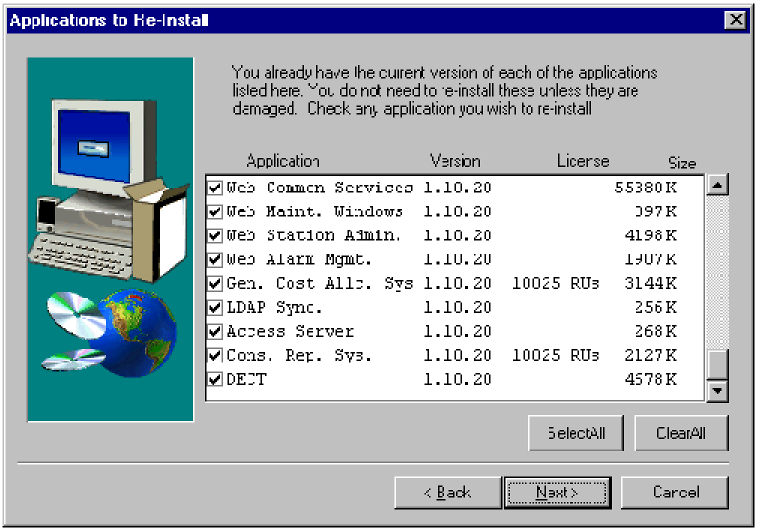
If there is an Upstream Manager IP address mismatch between the OTM DECT Application database and the DECT system database, the mismatch dialog enables an update of the Upstream Manager IP address on both the connected DECT system and the OTM DECT Application. See Figure 146.

Figure 147
DECT Subscription Configuration Mismatch dialog

The dialog warns of a DMC mismatch between DECT and the OTM server database. The manager cannot automatically solve the mismatch. The mismatch must be solved manually.

Ensuring the DECT application is on the OTM server

Figure 148
Applications to Reinstall



Applications to Re-Install

You already have the current version of each of the applications listed here. You do not need to re-install these unless they are damaged. Check any application you wish to re-install

	Application	Version	License	Size
☑	Web Common Services	1.10.20		55380K
☑	Web Maint. Windows	1.10.20		397K
☑	Web Station Admin.	1.10.20		4198K
☑	Web Alarm Mgmt.	1.10.20		1907K
☑	Gen. Cost Allc. Sys	1.10.20	10025 RUs	3144K
☑	LDAP Sync.	1.10.20		256K
☑	Access Server	1.10.20		268K
☑	Cons. Rep. Sys.	1.10.20	10025 RUs	2127K
☑	DECT	1.10.20		4578K

Complete the following steps.

Procedure 48
Ensuring the DECT application is on the OTM server

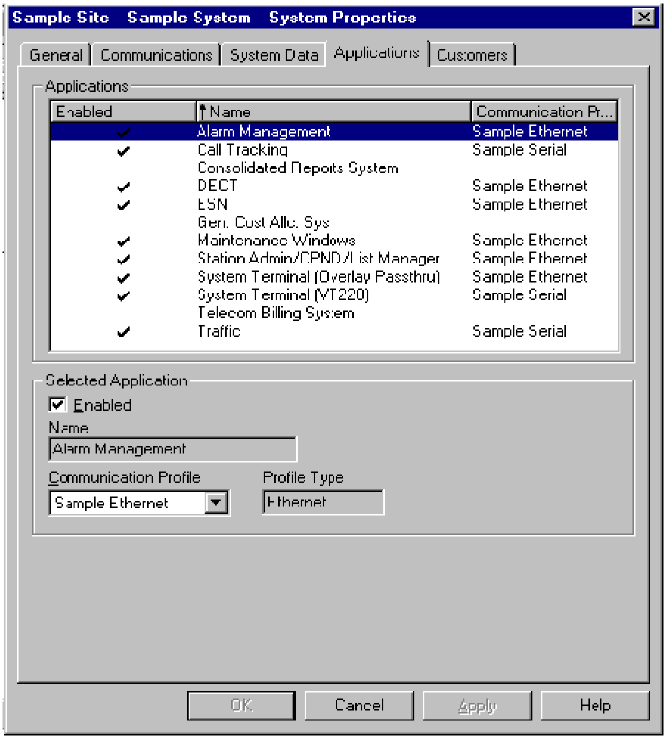
Step	Action
1	If there is a check in the DECT box in the Applications to Reinstall dialog.
	Go to “Configuring DECT on the OTM server” on page 351.
2	If there is no check in the DECT box in the Applications to Reinstall dialog. **Note:** The installation procedure is similar to that for any other application.
	Select the check-box and click the **Next** button.

END

Ensuring a Communications Profile is associated with the DECT application

The DECT application must be associated with a Communications Profile.

Figure 149
Systems Properties – Applications



Applications

Enabled	Name	Communication Pr...
✓	Alarm Management	Sample Ethernet
✓	Call Tracking	Sample Serial
	Consolidated Reports System	
✓	DECT	Sample Ethernet
✓	ESN	Sample Ethernet
	Gen. Cust Allc. Sys	
✓	Maintenance Windows	Sample Ethernet
✓	Station Admin/CPND/List Manager	Sample Ethernet
✓	System Terminal (Overlay Passthru)	Sample Ethernet
✓	System Terminal (VT220)	Sample Serial
	Telecom Billing System	
✓	Traffic	Sample Serial

Selected Application

☑ Enabled

Name: Alarm Management

Communication Profile: Sample Ethernet

Profile Type: Ethernet

The following describes the **OK**, **Cancel**, and **Apply** button actions:

- **OK** adds the changes that were made, then returns to the previous screen.
- **Apply** adds the changes and leaves the properties open so that other information can be added to this properties dialog.
- **Cancel** closes the dialog box without adding the changes.

Complete the following steps.

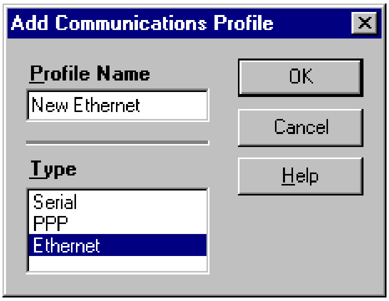
Procedure 49
Associating a Communications Profile with the DECT application

Step	Action
1	Open the Systems Properties sheet.
	Choose **Properties** from the OTM Navigator window **File** menu.
2	Select the Applications tab.
	Click the **Applications** tab.
3	If there is a check in the Enabled column next to DECT in the Name column.
	Go to “Configuring DECT on the OTM server” on page 351.
4	If there is no check in the Enabled column next to DECT in the Name column.
	Highlight DECT in the name column.
5	Select a Communications Profile.
	Choose any entry from the **Communications Profile** drop-down list. **Note:** If there are no entries in the Communications Profile drop-down list, go to “Adding a Communications Profile for the DECT application” on page 348.
6	Accept the changes.
	Click the **OK** button.

END

Adding a Communications Profile for the DECT application

Figure 150
Add Communications Profile



Add Communications Profile

Profile Name: New Ethernet

Type: Serial, PPP, Ethernet (Ethernet selected)

Complete the following steps.

Procedure 50
Adding new PBX Communications Profile (Part 1 of 2)

Step	Action
1	In the Navigator window, select the Sample Site.
	Double-click **Sample Site**.
2	Choose the Properties dialog.
	Click **Properties** from the **File** menu.
3	Open the **Add Communications Profile** dialog.
	Click the **Communications** tab and click **Add**.
4	Select a communication type.
	Highlight **Ethernet** in the **Type** box. **Note:** The DECT application does not use the Communications Profile. Unless there is another application that requires a specific Communications Profile, choosing Ethernet is the least complicated profile to implement.

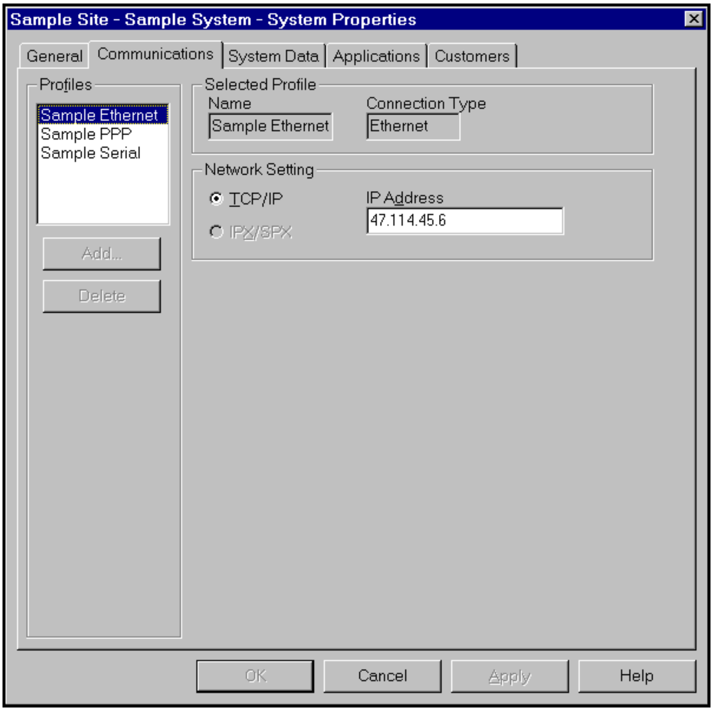
Procedure 50
Adding new PBX Communications Profile (Part 2 of 2)

Step	Action
5	Program the Profile Name.
	Enter a **Profile Name**.
6	Accept the changes.
	Click **OK**.

END

Adding an Ethernet profile

Figure 151
System Properties – Communications



Sample Site - Sample System - System Properties

Selected Profile

Name: Sample Ethernet

Connection Type: Ethernet

Network Setting

● TCP/IP

○ IPX/SPX

IP Address: 47.114.45.6

Complete the following steps.

Procedure 51
Adding the PBX Ethernet profile

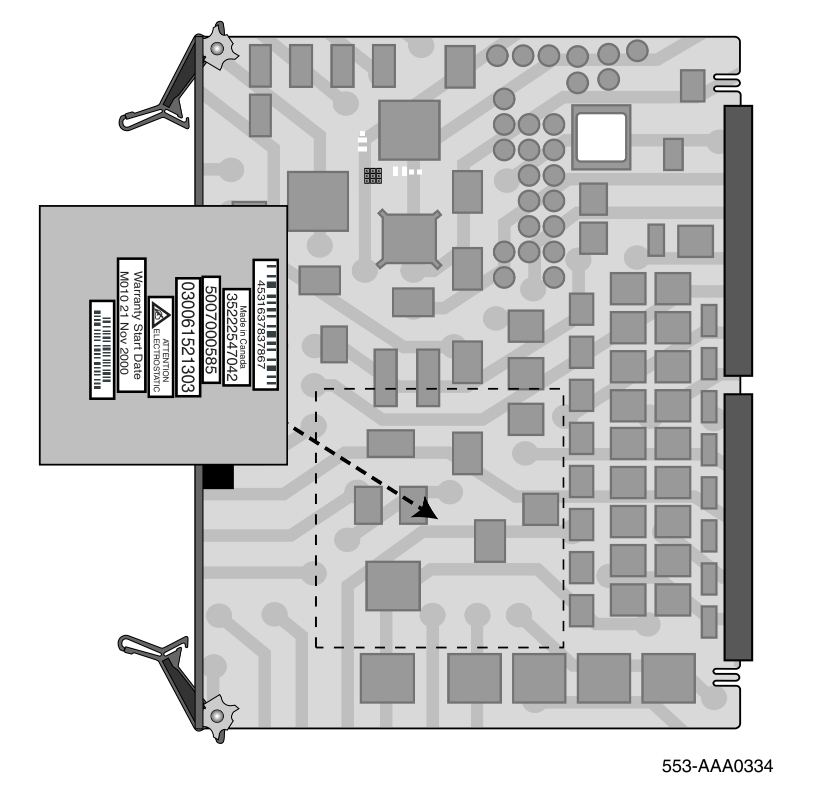
Step	Action
1	Fill in the communication information for the **Ethernet** profile.
	Enter any IP address. **Note:** Unless there is another application that requires a specific IP address, enter a non-existing address.
2	Accept changes.
	Click **Apply**.
3	Return to configuring a Communications Profile.
	Go to “Ensuring a Communications Profile is associated with the DECT application” on page 346.

END

Configuring DECT on the OTM server

Installing the DME on the DMC8 Relay card

Figure 152
NTCW25AA DECT Manager Ethernet (DME) daughterboard location



The NTFZ38AA Ethernet Management Connection package is available, containing the following:

a one NTCW25AA DECT Mobility Ethernet (DME) card, and

b one NTCW12DA DMC8 I/O cable.

Procedure 52
Installing the DME on the DMC8 Relay card

Step	Action
1	Unpack the NTCW25AA DECT Manager Ethernet (DME) daughterboard.
	Remove the packing material.
2	Install the DME.
	Carefully position the daughterboard over the four standoff posts and press onto the DMC8 relay card.

END

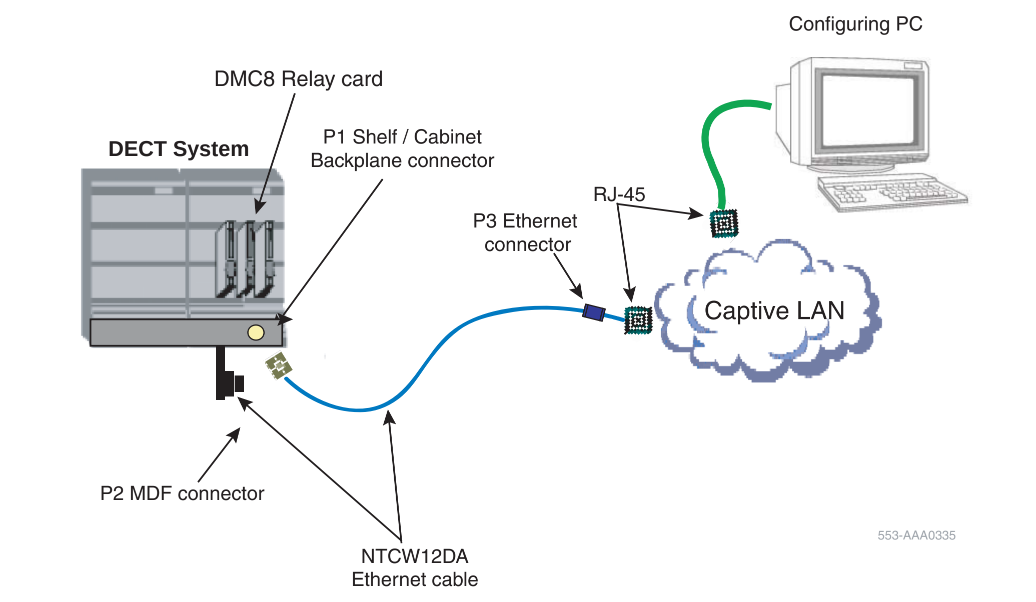
Changing the DMC8 Relay card default IP address

Connecting the DMC8 Relay card to a configuring PC

CAUTION — Service Interruption

The DMC8 is shipped with a default IP address 192.168.1.1. The default address must be changed to conform to the network IP address plan.

Figure 153
NTCW12DA Ethernet cable to configuring PC connections



For information on connecting OTM through a V.24 serial connection, see “Upgrade a DECT system to an SNMP-managed system” on page 394.

> ***Note:*** The configuring PC can be the OTM server or another PC. If the configuring PC is the OTM server, the Captive LAN shown in Figure 153 is the OTM Server Dedicated LAN shown in Figure 127 on page 324.

Consult the work order to determine the DMC8 Relay card location, then perform the steps in Table 53 on page 354.

> ***Note:*** The Relay card can be any of the DMC8 or DMC8-E cards. Usually, the lowest-numbered card is used.

Procedure 53
Connecting the DMC8 Relay card to a configuring PC

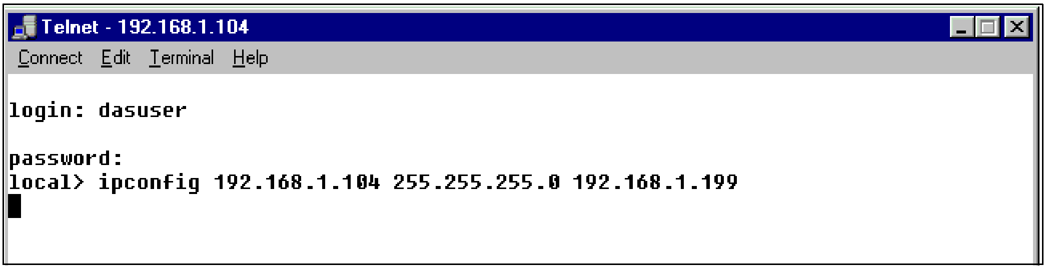
Step	Action
1	Connect the NTCW12DA cable to the connector on the backplane of the DMC8 Relay card.
	Insert P1 into the DMC8 Relay card backplane connector located on the PBX shelf/ module or Cabinet.
2	If the Configuring PC is on a captive LAN, link the DMC8 Relay card to the Configuring PC.
	Insert P3 into the captive LAN RJ45 connector.
3	If the Configuring PC is on the OTM server dedicated LAN,
	Insert P3 into the OTM server dedicated LAN RJ45 connector. See “Connecting the DMC8 Relay card to the OTM server” on page 356.

END

Resetting the DMC8 Relay card default IP address to the LAN IP address

The DMC8 Relay card default IP address 192.168.1.1 must be changed to conform to the server network IP address plan.

Figure 154
Telnet 192.168.1.1



```
login: dasuser

password:
local> ipconfig 192.168.1.104 255.255.255.0 192.168.1.199
```

Complete the following steps.

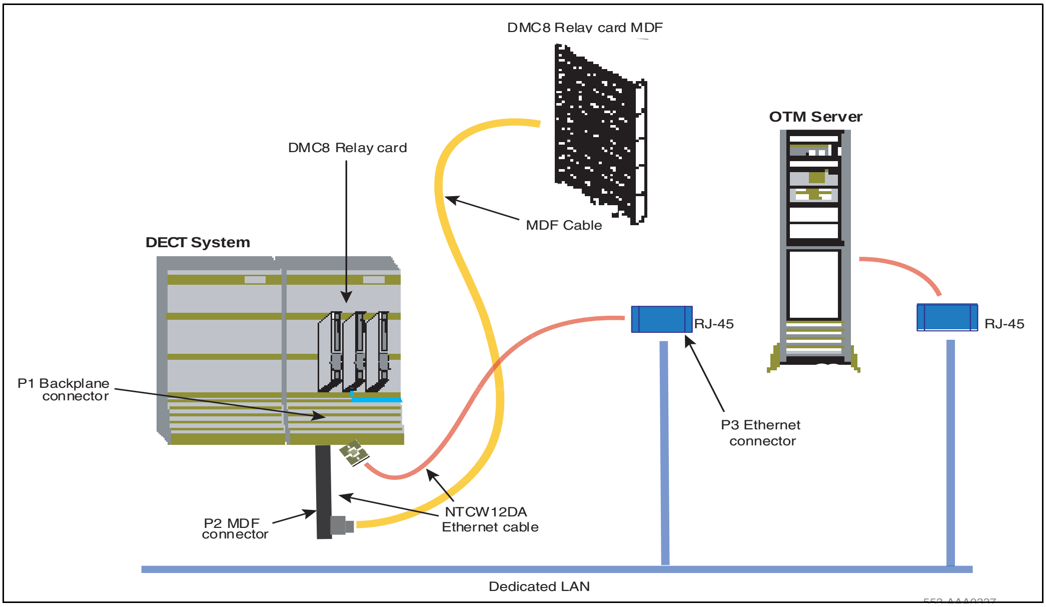
Procedure 54
Resetting the DMC8 Relay card default IP address

Step	Action
1	Open the Telnet dialog.
	Click **Start** on the Windows taskbar and choose **Accessories > Telnet**.
2	Enter username and password.
	Type username **dasuser** and password **dasuser**.
3	When the connection prompt **local** appears, change the DMC8 Relay card address.
	Enter the following command: **ipconfig xxx.xxx.xxx.xxx yyy.yyy.yyy.yyy zzz.zzz.zzz.zzz** **xxx.xxx.xxx.xxx** = new IP address of the DMC8 Relay card. **yyy.yyy.yyy.yyy** = subnet mask, usually **255.255.255.0** **zzz.zzz.zzz.zzz** = IP address if this is the gateway for the network. **Note:** **zzz.zzz.zzz.zzz** must be set to the IP address of the OTM server Ethernet interface. If there are two Ethernet interfaces on the OTM server, **zzz.zzz.zzz.zzz** must be set to the IP address of the interface that is on the same network as the DMC8 Relay card.

END

Connecting the DMC8 Relay card to the OTM server

Figure 155
NTCW12DA Ethernet cable to OTM Server LAN connections



Complete the following steps.

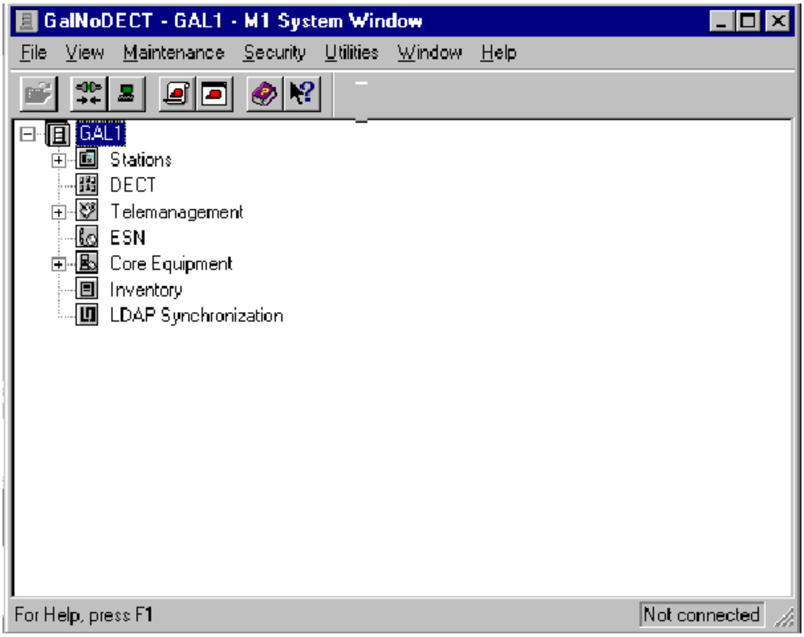
Procedure 55
Connecting the DMC8 Relay card to a Captive LAN

Step	Action
1	If the DMC8 Relay card was configured on a captive LAN, remove the NTCW12DA Ethernet cable from the captive LAN.
	Disconnect P3 from the captive LAN RJ45 connector.
2	Connect the NTCW12DA cable to the OTM Server Dedicated LAN.
	Insert P3 into the Dedicated LAN RJ45 connector.

END

Launching the DECT application

Figure 156
M1 System Window



Complete the following step:

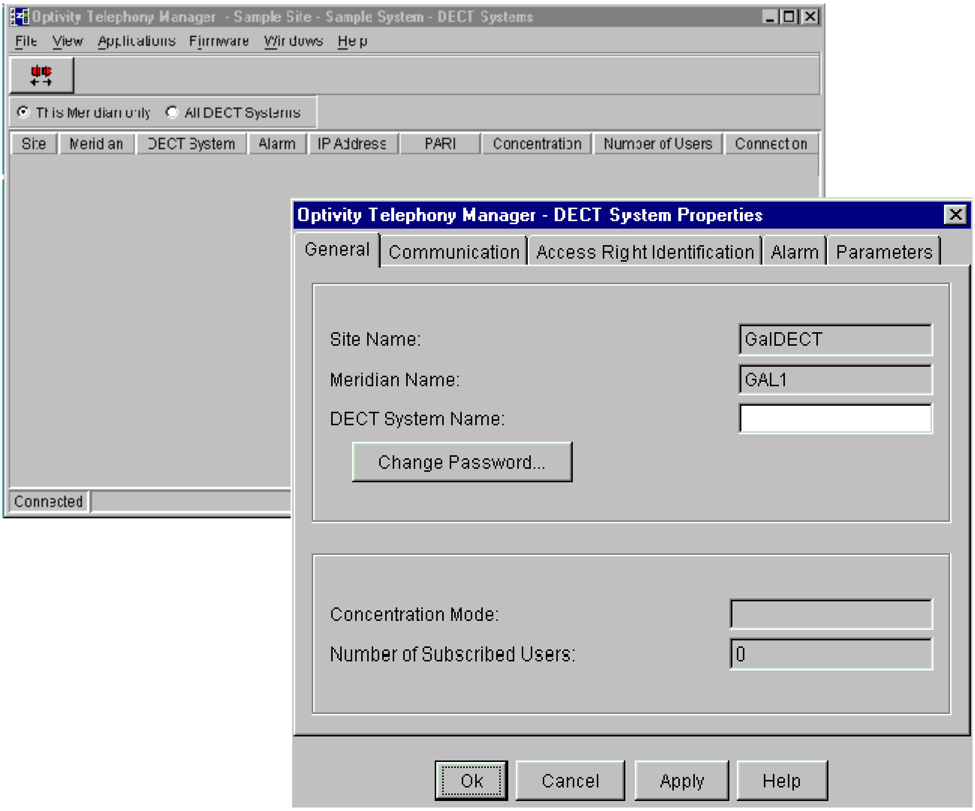
Procedure 56
Launching the DECT application

Step	Action
1	Launch the DECT application.
	Double-click the DECT icon.
	END

Adding DECT

Adding General System Properties

Figure 157
DECT Systems and DECT System Properties windows


Optivity Telephony Manager - Sample Site - Sample System - DECT Systems
File View Applications Firmware Windows Help
Site Meridian DECT System Alarm IP Address PARI Concentration Number of Users Connection
Connected
Optivity Telephony Manager - DECT System Properties
General Communication Access Right Identification Alarm Parameters
Change Password...
Ok Cancel Apply Help

● This Meridian only ○ All DECT Systems

Site Name: GalDECT

Meridian Name: GAL1

DECT System Name:

Concentration Mode:

Number of Subscribed Users: 0

Complete the following steps.

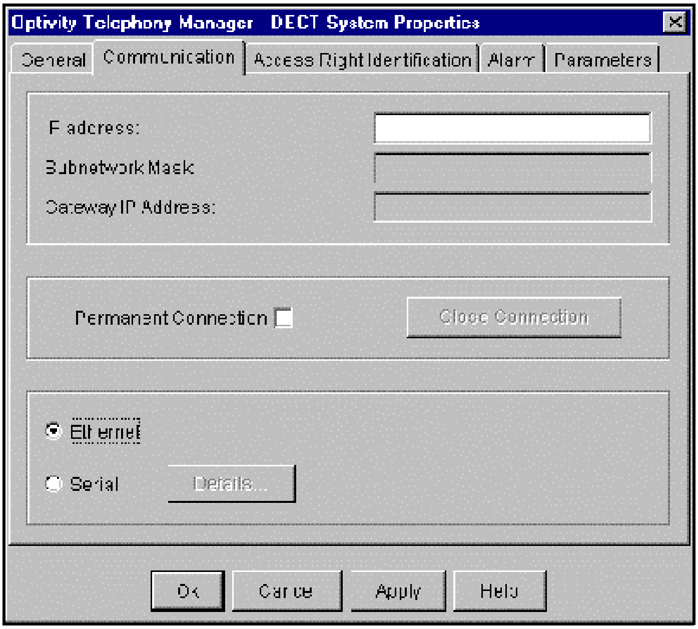
Procedure 57
Adding DECT

Step	Action
1	Open the **DECT System Properties** dialog.
	Pull down **File** > **Properties**.
2	Enter the DECT system name.
	Type the system name in the **DECT System Name** box.
3	Accept the changes.
	Click the **Apply** button.

END

Setting the DECT system IP address to match the DMC8 Relay card

Figure 158
System Properties – Communication



Complete the following steps.

Procedure 58
Setting the IP address of the DMC8 Relay card

Step	Action
1	Open the Communications dialog.
	Click the **Communications** tab.
2	Enter the IP address.

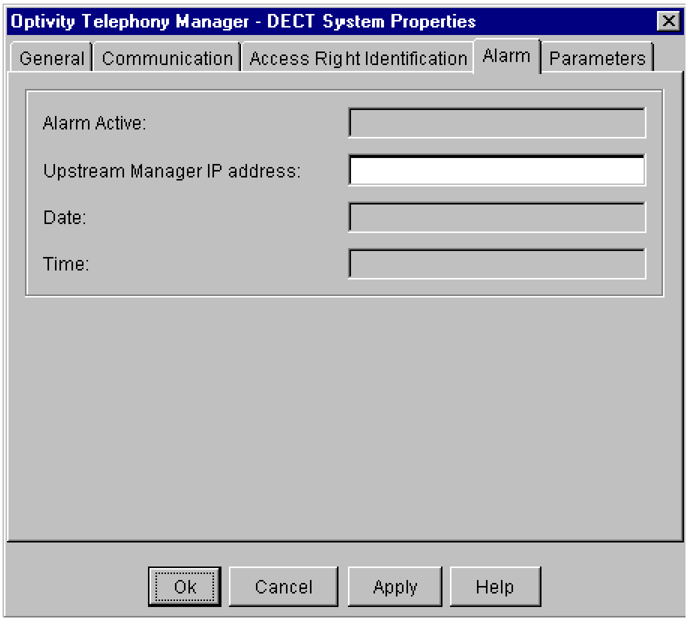
Procedure 58
Setting the IP address of the DMC8 Relay card (Continued)

Step	Action
	Type the IP address that was entered in Table 54 on page 355.
3	If the communication link is Ethernet, select **Ethernet**.
	Click the **Ethernet** radio button.
4	If the communication link is Serial, select **Serial**.
	Click **Serial** radio button, and go to “Upgrade a DECT system to an SNMP-managed system” on page 394.
5	Accept the changes.
	Click the **OK** button. **Note:** When the OK button or Apply button is clicked at this point, the manager attempts to connect to the DECT system to write the MIB2 system name.
6	If required, program an Upstream Manager.
	Go to page 362.
7	If an Upstream Manager is not required.
	Go to “Synchronizing data with DECT” on page 363.

END

Adding the upstream manager IP address, if required

Figure 159
System Properties – Alarm


Optivity Telephony Manager - DECT System Properties
General
Communication
Access Right Identification
Alarm
Parameters
Ok
Cancel
Apply
Help

Alarm Active:

Upstream Manager IP address:

Date:

Time:

Complete the following steps.

Procedure 59
Adding the upstream IP address, if required

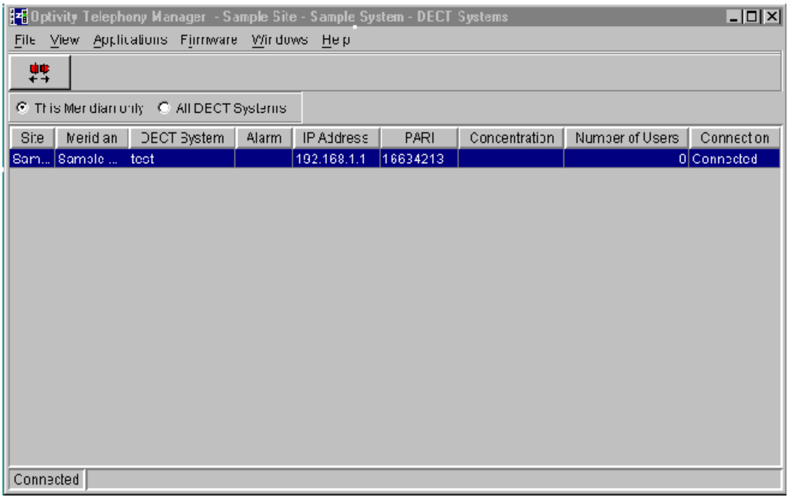
Step	Action
1	Open the **DECT System Properties** dialog.
	Pull down **File** > **Add**.
2	Open the Alarm dialog.
	Click the **Alarm** tab.
3	Enter the IP address.
	Type the Upstream manager IP address.
4	Accept the changes.
	Click the **OK** button.

END

Synchronizing data with DECT

When the DECT manager connects to DECT, synchronization occurs. Synchronization compares the database on the manager to the database of the DECT system. Database mismatches are flagged by dialogs. The opportunity to change either the DECT system data or the manager data is given.

Figure 160
DECT Systems


Optivity Telephony Manager - Sample Site - Sample System - DECT Systems
File
View
Applications
Firmware
Windows
Help

● This Meridian only ○ All DECT Systems

Site	Meridian	DECT System	Alarm	IP Address	PARI	Concentration	Number of Users	Connection
Sam...	Sample ...	test		192.168.1.1	16634213		0	Connected

Connected

Complete the following steps:

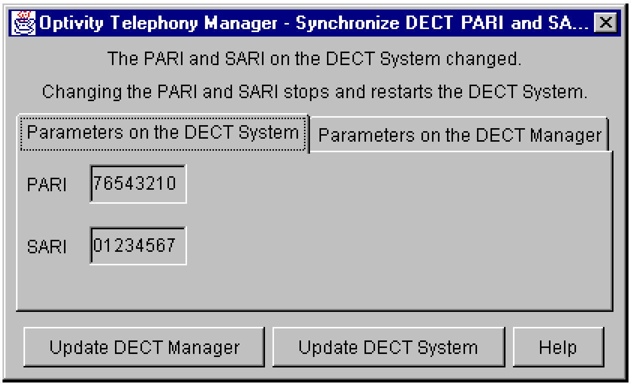
Procedure 60
Synchronizing data with the DECT system

Step	Action
1	If the toolbar icon is **red,** the connection to the DECT system is enabled. Disconnect from the DECT system.
	Double-click the icon, or use **File** > **Disonnect**. Go to “Synchronizing DECT PARI and SARI” on page 365.
2	If the toolbar icon is **green**, re-connect to the DECT system
	Double-click the red icon, or use **File** > **Connect.**

END

Synchronizing DECT PARI and SARI

Figure 161
Synchronize DECT PARI and SARI Mismatch dialog



Optivity Telephony Manager - Synchronize DECT PARI and SA...

The PARI and SARI on the DECT System changed.

Changing the PARI and SARI stops and restarts the DECT System.

PARI 76543210

SARI 01234567

Complete the following step:

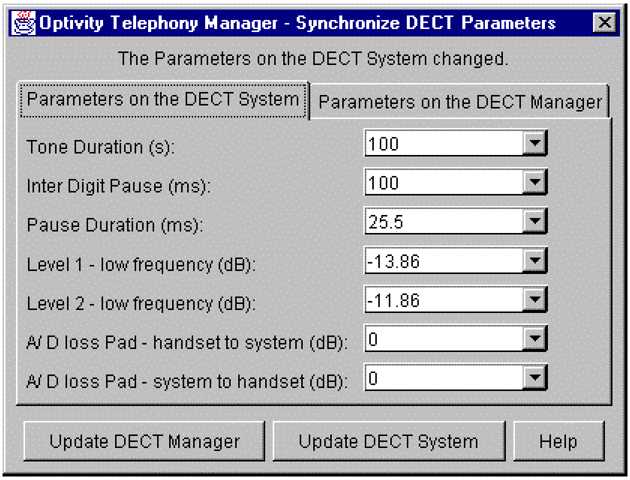
Procedure 61
Synchronizing DECT PARI and SARI

Step	Action
1	Store the DECT system PARI SARI parameters in the OTM Manager database.
	Click the **Update DECT Manager** button.

END

Synchronizing DECT parameters

Figure 162
Synchronize DECT Parameters Mismatch dialog



Optivity Telephony Manager - Synchronize DECT Parameters

The Parameters on the DECT System changed.

Tone Duration (s): 100

Inter Digit Pause (ms): 100

Pause Duration (ms): 25.5

Level 1 - low frequency (dB): -13.86

Level 2 - low frequency (dB): -11.86

A/ D loss Pad - handset to system (dB): 0

A/ D loss Pad - system to handset (dB): 0

Complete the following step:

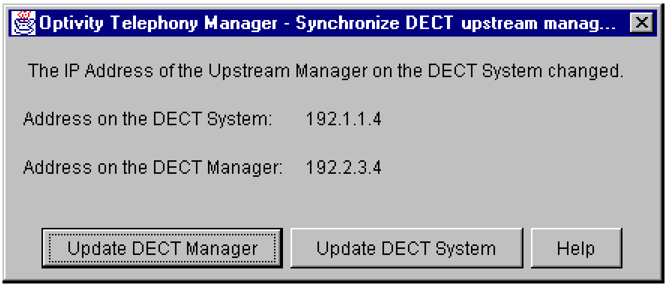
Procedure 62
Synchronizing DECT Parameters

Step	Action
1	Store the DECT system DECT Parameters in the OTM Manager database.
	Click the **Update DECT Manager** button.

END

Synchronizing DECT Upstream Manager IP address

Figure 163
Synchronize DECT Upstream Manager IP address mismatch dialog


Optivity Telephony Manager - Synchronize DECT upstream manag...

The IP Address of the Upstream Manager on the DECT System changed.

Address on the DECT System: 192.1.1.4

Address on the DECT Manager: 192.2.3.4

Complete the following step:

Procedure 63
Synchronizing DECT Upstream Manager IP address

Step	Action
1	Store the DECT system Upstream Manager IP address in the OTM Manager database.
	Click the **Update DECT Manager** button.

END

Removing DECT Manager – Caution

Before removing DECT Manager, read the following information.

⚠ **CAUTION — Service Interruption**

When the OTM DECT Manager software is removed, the Sentinel driver is also removed, even if other applications require the driver. Any attempt to launch other OTM systems or applications generates the message:

“No dongle attached to the PC.”

It is necessary to reinstall the Sentinel driver. Download the driver from the internet. Go to: www.safenet-inc.com/support/tech/sentinel.asp

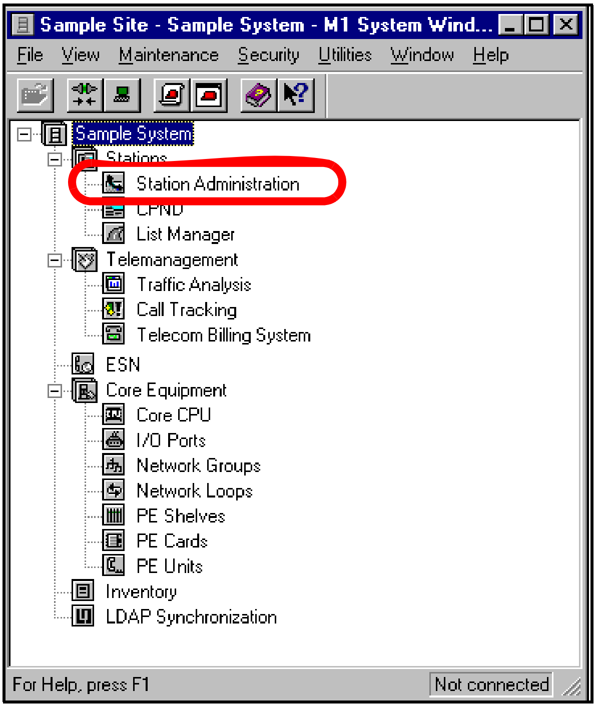
Configuring handsets and retrieve subscription data

Configuring non-concentrated Large System handsets

For information about System Administration, see *Telephony Manager: System Administration* (553-3001-330).

Opening the Station Administration window

Figure 164
System Window



Complete the following step:

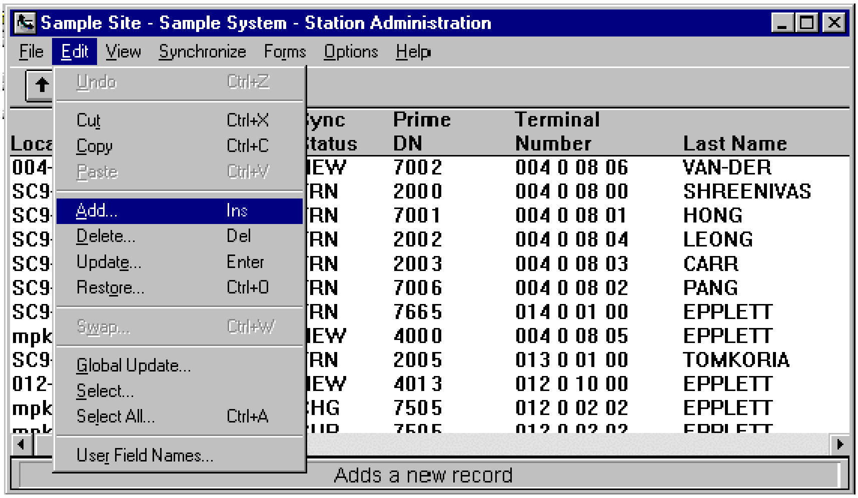
Procedure 64
Opening the Station Administration window

Step	Action
1	Open the Station Administration window.
	Click **Station Administration** in the M1 System Window.

END

Accessing Add Station dialog

Figure 165
Station Administration window



Loca	ync tatus	Prime DN	Terminal Number	Last Name
004-	IEW	7002	004 0 08 06	VAN-DER
SC9	RN	2000	004 0 08 00	SHREENIVAS
SC9	RN	7001	004 0 08 01	HONG
SC9	RN	2002	004 0 08 04	LEONG
SC9	RN	2003	004 0 08 03	CARR
SC9	RN	7006	004 0 08 02	PANG
SC9	RN	7665	014 0 01 00	EPPLETT
mpk	IEW	4000	004 0 08 05	EPPLETT
SC9	RN	2005	013 0 01 00	TOMKORIA
012-	IEW	4013	012 0 10 00	EPPLETT
mpk	HG	7505	012 0 02 02	EPPLETT

Adds a new record

Complete the following step:

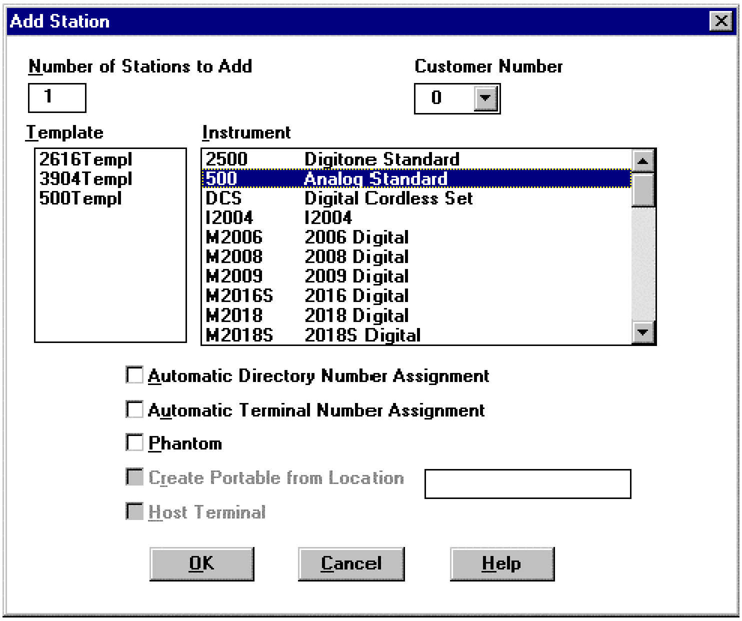
Procedure 65
Accessing Add Station dialog

Step	Action
1	Access Add Station dialog.
	From the **Edit** pull-down menu, click **Add.**

END

Adding 500 analogue standard

Figure 166
Add Station dialog



Add Station

Number of Stations to Add: 1

Customer Number: 0

Template:
2616Templ
3904Templ
500Templ

Instrument:

2500	Digitone Standard
500	Analog Standard
DCS	Digital Cordless Set
I2004	I2004
M2006	2006 Digital
M2008	2008 Digital
M2009	2009 Digital
M2016S	2016 Digital
M2018	2018 Digital
M2018S	2018S Digital

☐ Automatic Directory Number Assignment

☐ Automatic Terminal Number Assignment

☐ Phantom

☐ Create Portable from Location

☐ Host Terminal

Complete the following step:

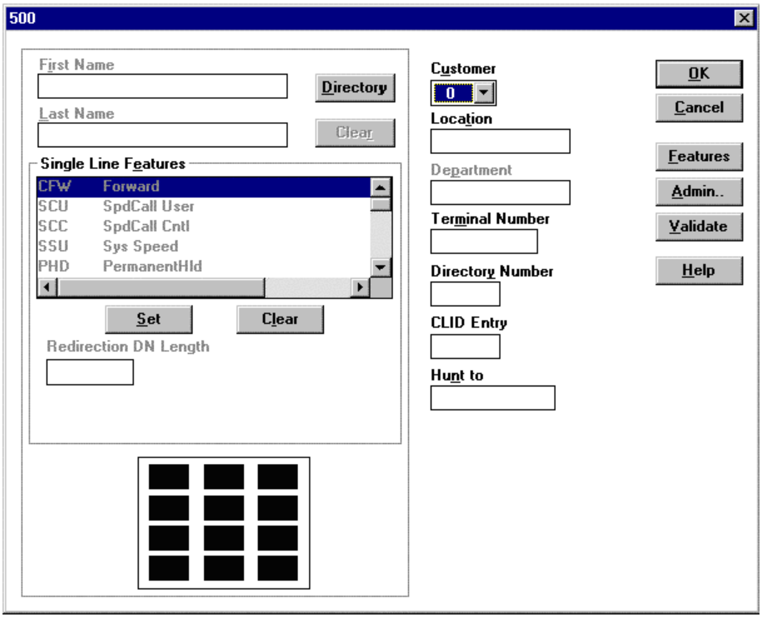
Procedure 66
Adding 500 analogue standard

Step	Action
1	Add 500 analogue standard.
	Highlight **500 Analogue Standard**, and click **OK**.

END

Accessing features

Figure 167
500 dialog



Complete the following step:

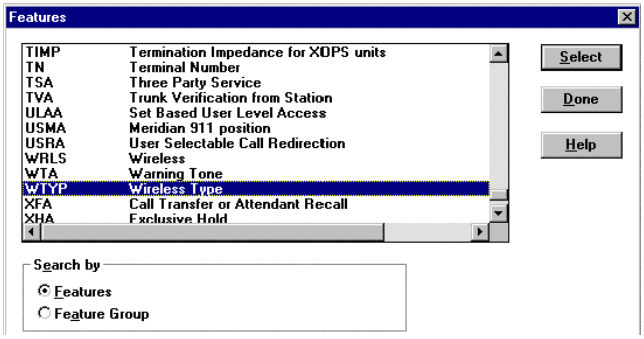
Procedure 67
Accessing features

Step	Action
1	Access the features.
	Click the **Features** button.

END

Accessing wireless type

Figure 168
Features dialog



Features

TIMP	Termination Impedance for XOPS units
TN	Terminal Number
TSA	Three Party Service
TVA	Trunk Verification from Station
ULAA	Set Based User Level Access
USMA	Meridian 911 position
USRA	User Selectable Call Redirection
WRLS	Wireless
WTA	Warning Tone
WTYP	Wireless Type
XFA	Call Transfer or Attendant Recall
XHA	Exclusive Hold

Search by

● Features

○ Feature Group

Complete the following step:

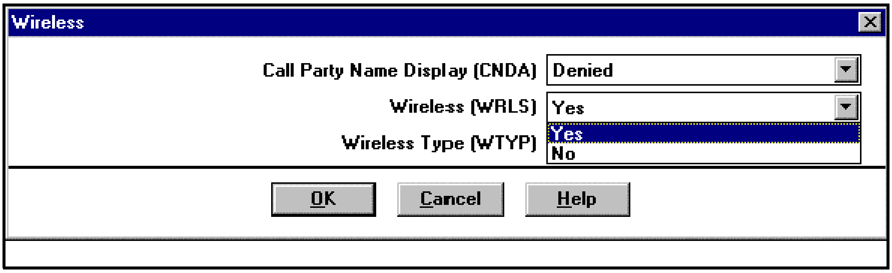
Procedure 68
Accessing wireless type

Step	Action
1	Access wireless type.
	Highlight **Wireless Type**, and click the **Select** button.

END

Selecting wireless type

Figure 169
Wireless dialog



Call Party Name Display (CNDA): Denied
Wireless (WRLS): Yes
Wireless Type (WTYP)

Complete the following step:

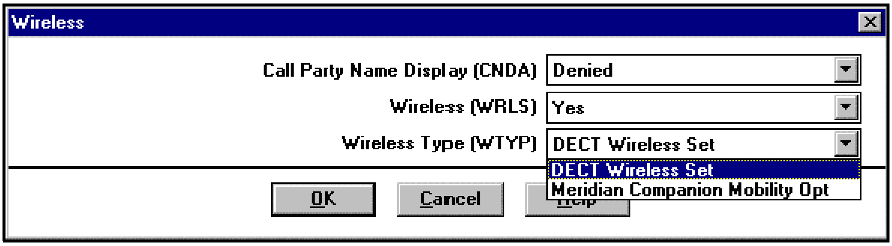
Procedure 69
Selecting wireless type

Step	Action
1	Select wireless type.
	From the **Wireless (WRLS)** pull-down menu select **YES**.

END

Selecting DECT wireless set

Figure 170
Wireless dialog



Call Party Name Display (CNDA): Denied
Wireless (WRLS): Yes
Wireless Type (WTYP): DECT Wireless Set

Complete the following step:

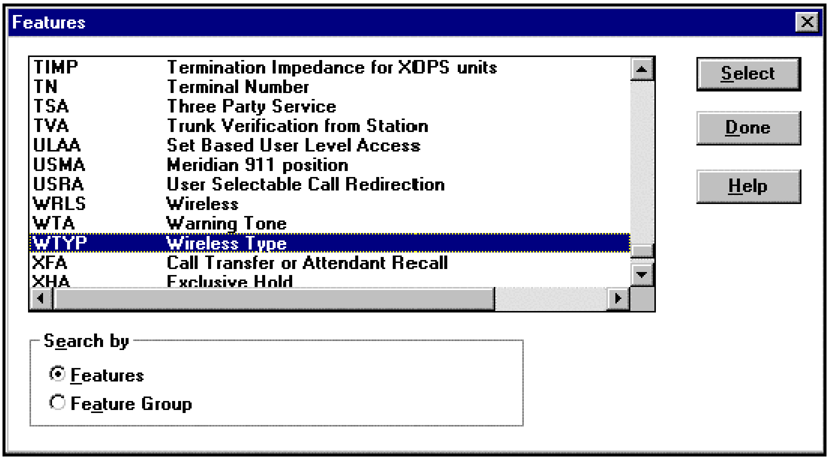
Procedure 70
Selecting DECT wireless set

Step	Action
1	Select a DECT handset.
	From the **Wireless Type (WTYP)** pull-down menu, click **DECT Wireless Set**. Click **OK**.

END

Accepting changes

Figure 171
Features dialog



TIMP	Termination Impedance for XOPS units
TN	Terminal Number
TSA	Three Party Service
TVA	Trunk Verification from Station
ULAA	Set Based User Level Access
USMA	Meridian 911 position
USRA	User Selectable Call Redirection
WRLS	Wireless
WTA	Warning Tone
WTYP	Wireless Type
XFA	Call Transfer or Attendant Recall
XHA	Exclusive Hold

Search by
● Features
○ Feature Group

Complete the following step:

Procedure 71
Accepting changes

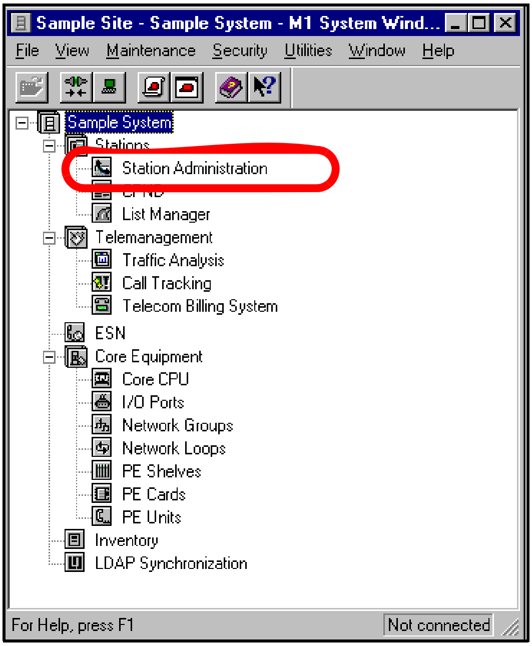
Step	Action
1	Accept changes.
	Click the **Done** button.

END

Configuring concentrated handsets on a Large System

Opening Station Administration window

Figure 172
M1 System Window



Complete the following step.

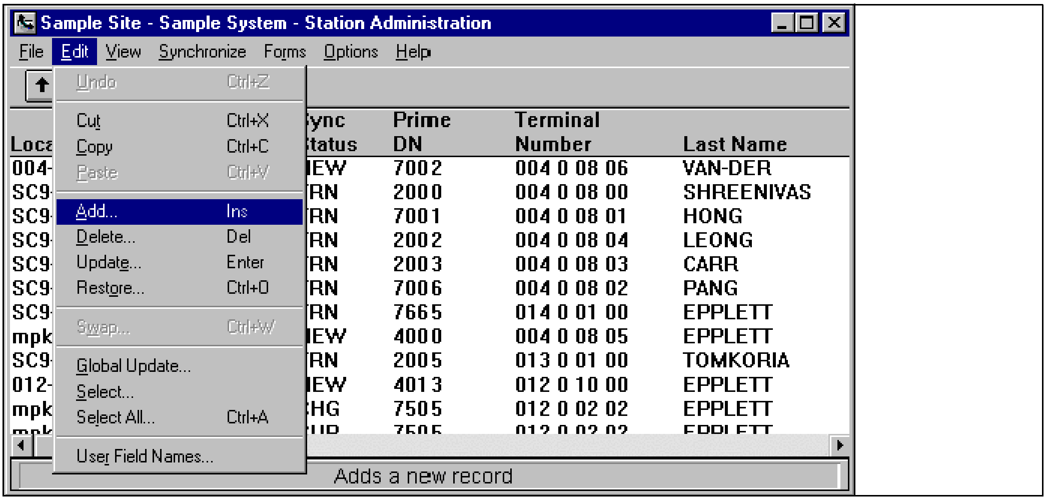
Procedure 72
Opening the Station Administration window

Step	Action
1	Open the Station Administration window.
	Click **Station Administration** in the System Window.

END

Accessing Add Station dialog

Figure 173
Station Administration window



Sample Site - Sample System - Station Administration

Loca	ync tatus	Prime DN	Terminal Number	Last Name
004-	EW	7002	004 0 08 06	VAN-DER
SC9	RN	2000	004 0 08 00	SHREENIVAS
SC9	RN	7001	004 0 08 01	HONG
SC9	RN	2002	004 0 08 04	LEONG
SC9	RN	2003	004 0 08 03	CARR
SC9	RN	7006	004 0 08 02	PANG
SC9	RN	7665	014 0 01 00	EPPLETT
mpk	EW	4000	004 0 08 05	EPPLETT
SC9	RN	2005	013 0 01 00	TOMKORIA
012-	EW	4013	012 0 10 00	EPPLETT
mpk	HG	7505	012 0 02 02	EPPLETT

Adds a new record

Complete the following step:

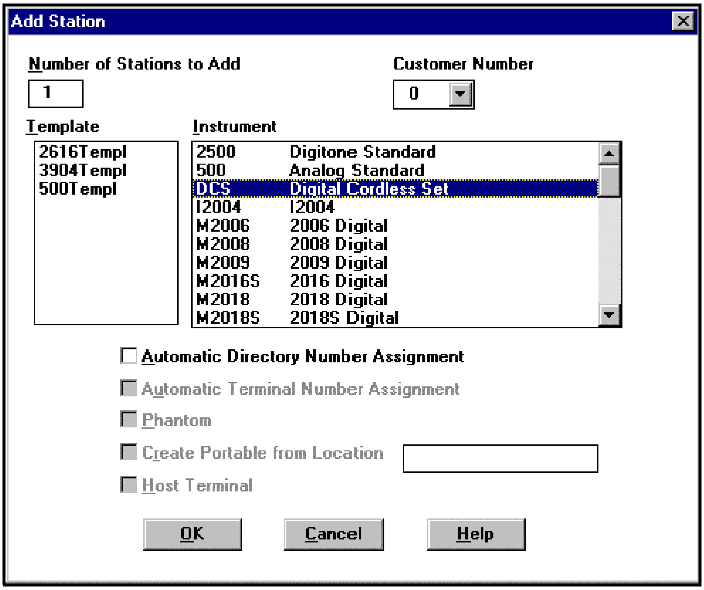
Procedure 73
Accessing Add Station dialog

Step	Action
1	Access Add Station dialog.
	From the **Edit** pull-down menu, click **Add.**

END

Selecting Digital Cordless Set

Figure 174
Add Station dialog



Add Station

Number of Stations to Add: 1

Customer Number: 0

Template
2616Templ
3904Templ
500Templ

Instrument

2500	Digitone Standard
500	Analog Standard
DCS	Digital Cordless Set
I2004	I2004
M2006	2006 Digital
M2008	2008 Digital
M2009	2009 Digital
M2016S	2016 Digital
M2018	2018 Digital
M2018S	2018S Digital

□ Automatic Directory Number Assignment
□ Automatic Terminal Number Assignment
□ Phantom
□ Create Portable from Location
□ Host Terminal

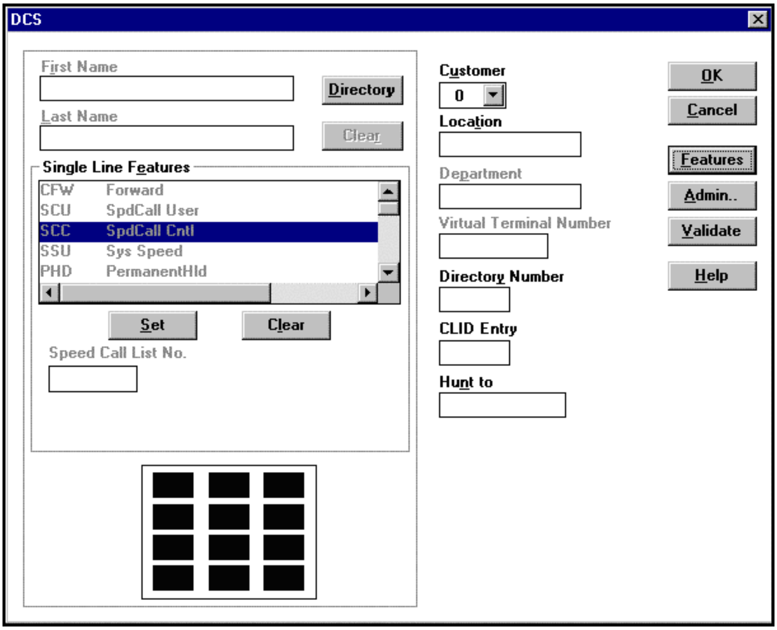
Procedure 74
Selecting Digital Cordless Set

Step	Action
1	Select Digital Cordless Set.
	Highlight **DCS**. Click the **OK** button.

END

Selecting Features

Figure 175
DCS dialog



Customer: 0

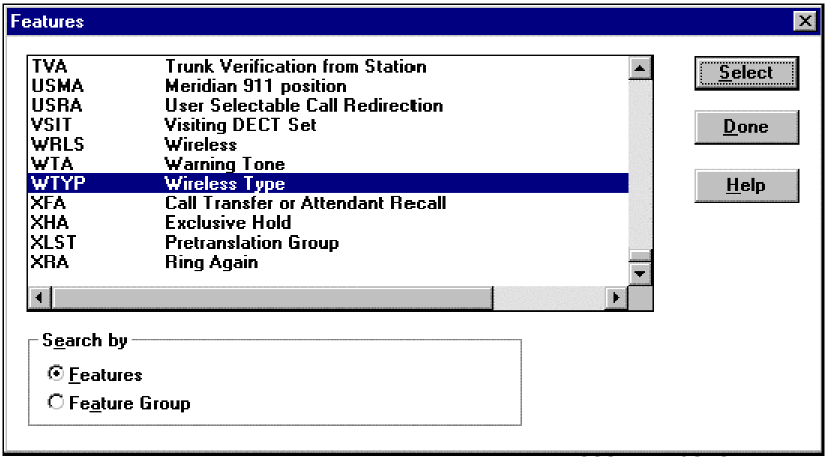
Procedure 75
Selecting Features

Step	Action
1	Select the features.
	Click the **Features** button.

END

Selecting wireless type

Figure 176
Features dialog



TVA	Trunk Verification from Station
USMA	Meridian 911 position
USRA	User Selectable Call Redirection
VSIT	Visiting DECT Set
WRLS	Wireless
WTA	Warning Tone
WTYP	Wireless Type
XFA	Call Transfer or Attendant Recall
XHA	Exclusive Hold
XLST	Pretranslation Group
XRA	Ring Again

Search by
● Features
○ Feature Group

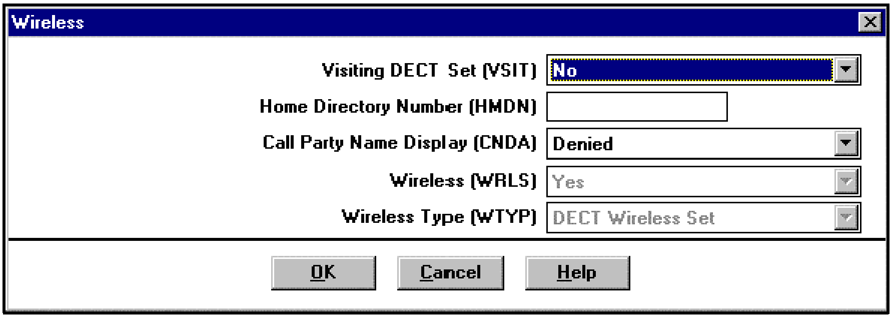
Procedure 76
Selecting wireless type

Step	Action
1	Select wireless type.
	Highlight **WTYP**, and click the **Select** button.

END

Selecting Visiting DECT Set or local calling only

Figure 177
Wireless dialog



Wireless

Visiting DECT Set (VSIT): No

Home Directory Number (HMDN):

Call Party Name Display (CNDA): Denied

Wireless (WRLS): Yes

Wireless Type (WTYP): DECT Wireless Set

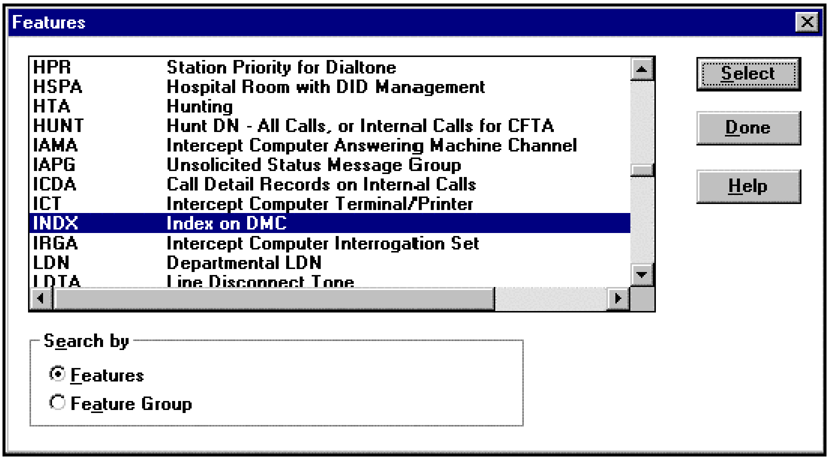
Procedure 77
Selecting Visiting DECT Set or local calling only

Step	Action
1	Select **Visiting DECT Set** as **Yes** if the handset is to visit this PBX. Select **No** if this handset is to be used for local calling only.
	If **Visiting DECT Set** is **Yes**, go to step 2. If this handset is to be used for local calling only, go to step 3.
2	Select a Home DN.
	Enter a DN in the **Home Directory Number (HMDN)** box.
3	If the handset is to be used for local calling only, from the **Visiting DECT Set (VSIT)** list, select **No**.
4	Accept changes.
	Click the **OK** button.

END

Selecting an index

Figure 178
Features dialog



HPR	Station Priority for Dialtone
HSPA	Hospital Room with DID Management
HTA	Hunting
HUNT	Hunt DN - All Calls, or Internal Calls for CFTA
IAMA	Intercept Computer Answering Machine Channel
IAPG	Unsolicited Status Message Group
ICDA	Call Detail Records on Internal Calls
ICT	Intercept Computer Terminal/Printer
INDX	Index on DMC
IRGA	Intercept Computer Interrogation Set
LDN	Departmental LDN
LDTA	Line Disconnect Tone

Search by
● Features
○ Feature Group

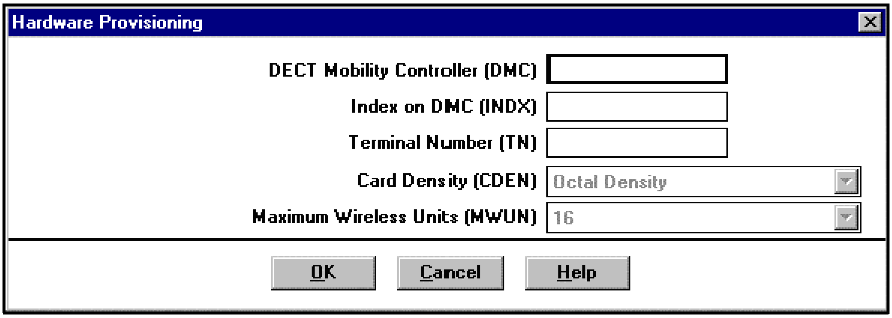
Procedure 78
Selecting an index

Step	Action
1	Select an index.
	Highlight **INDX**, and click the **Select** button.

END

Provisioning hardware

Figure 179
Hardware Provisioning dialog



DECT Mobility Controller (DMC)

Index on DMC (INDX)

Terminal Number (TN)

Card Density (CDEN) Octal Density

Maximum Wireless Units (MWUN) 16

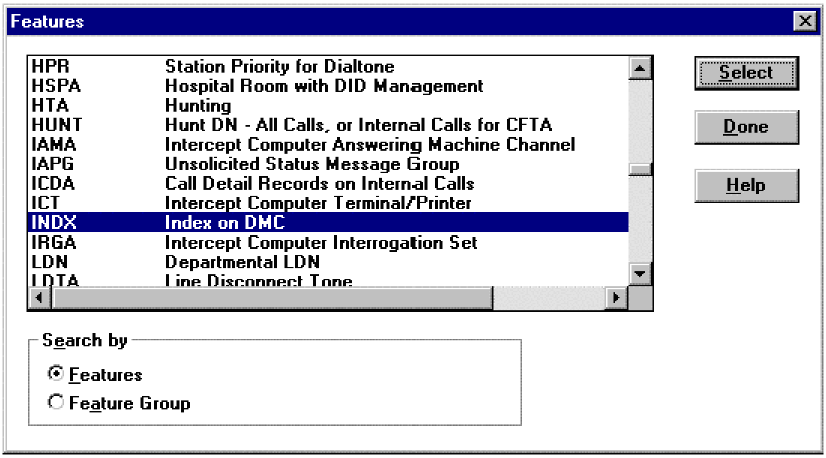
Procedure 79
Provisioning hardware

Step	Action
1	Select a DMC TN.
	Enter a TN in the **DECT Mobility Controller (DMC)** box.
2	Select an index.
	Enter an index in the **Index on DMC (INDX)** box. Index range is 0 to 509. **Note:** The Terminal Number (TN) is a virtual TN and is selected by the system.
3	Accept changes.
	Click the **OK** button.

END

Accepting changes

Figure 180
Features dialog



Features

HPR	Station Priority for Dialtone
HSPA	Hospital Room with DID Management
HTA	Hunting
HUNT	Hunt DN - All Calls, or Internal Calls for CFTA
IAMA	Intercept Computer Answering Machine Channel
IAPG	Unsolicited Status Message Group
ICDA	Call Detail Records on Internal Calls
ICT	Intercept Computer Terminal/Printer
INDX	Index on DMC
IRGA	Intercept Computer Interrogation Set
LDN	Departmental LDN
LDTA	Line Disconnect Tone

Search by

● Features
○ Feature Group

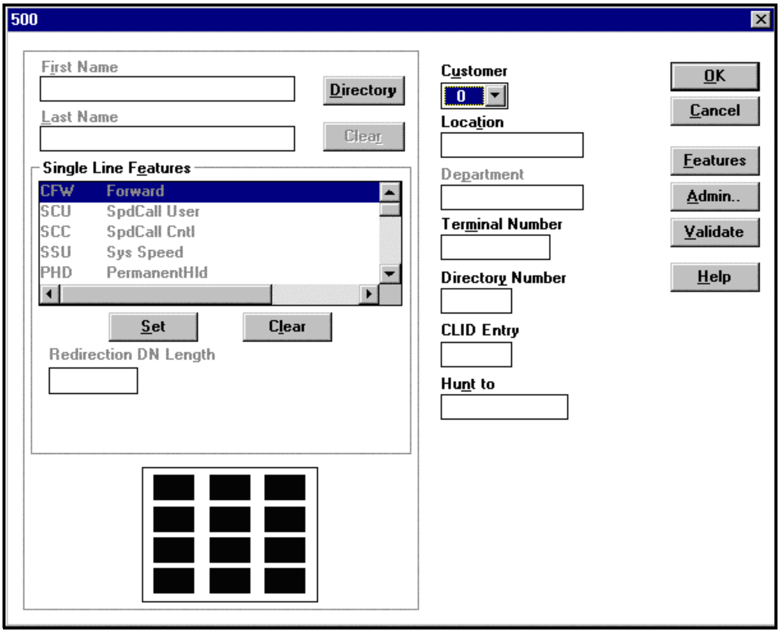
Procedure 80
Accepting changes

Step	Action
1	Accept changes.
	Click the **Done** button.

END

Selecting Single Line Features

Figure 181
500 dialog



CFW	Forward
SCU	SpdCall User
SCC	SpdCall Cntl
SSU	Sys Speed
PHD	PermanentHld

Procedure 81
Selecting Single Line Features
Configure the remaining features on the 500 or DCS set

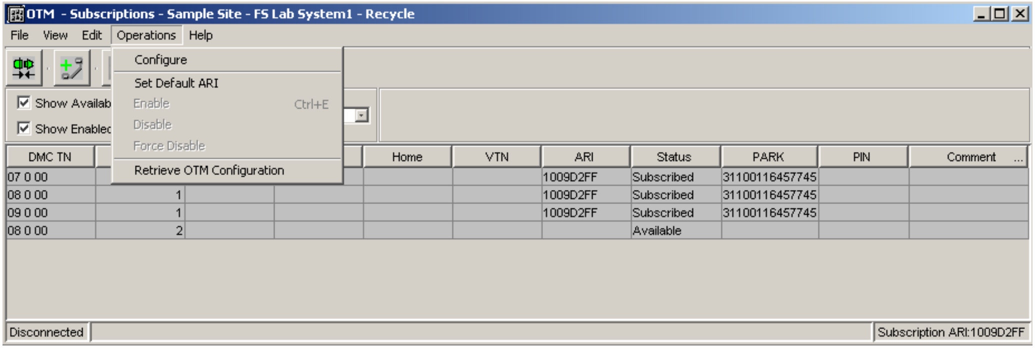
Step	Action
1	For information on other Single Line Features.
	Refer to the OTM Station Administration in *Telephony Manager: System Administration* (553-3001-330).

END

Note: Complete the “System programming record” on page 282 and “Provisioning information record” on page 279.

Retrieving subscription data for handsets

Figure 182
DECT Subscriptions window



DMC TN				Home	VTN	ARI	Status	PARK	PIN	Comment ...
07 0 00						1009D2FF	Subscribed	31100116457745		
08 0 00	1					1009D2FF	Subscribed	31100116457745		
09 0 00	1					1009D2FF	Subscribed	31100116457745		
08 0 00	2						Available			

Complete the following steps.

Procedure 82
Subscribing handsets (Part 1 of 2)

Step	Action
1	Launch the Subscriptions window from the **DECT Systems** window.
	Click the **Applications** pull-down menu, click **Subscriptions**.

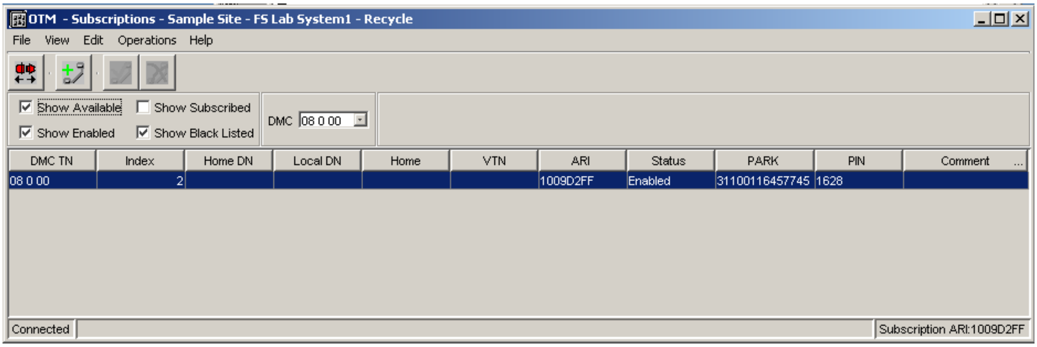
Procedure 82
Subscribing handsets (Part 2 of 2)

Step	Action
2	Retrieve the subscription configuration data from the OTM Station Administration database. **Note:** At this point, no handset data appears in the Subscriptions window.
	In the Subscriptions window, click the **Operations** pull-down menu, click **Retrieve OTM Configuration**.
3	Open the Configure DECT Subscription dialog. **Note:** At this point, all handsets configured on OTM Station Administration are shown in the Subscriptions window
	Click the **File** pull-down menu, click **Add** or click .

END

Enabling subscription

Figure 183
Subscriptions window



OTM - Subscriptions - Sample Site - FS Lab System1 - Recycle

☑ Show Available □ Show Subscribed
☑ Show Enabled ☑ Show Black Listed

DMC 08 0 00

DMC TN	Index	Home DN	Local DN	Home	VTN	ARI	Status	PARK	PIN	Comment
08 0 00	2					1009D2FF	Enabled	31100116457745	1628	

Connected

Subscription ARI:1009D2FF

Complete the following steps for each handset:

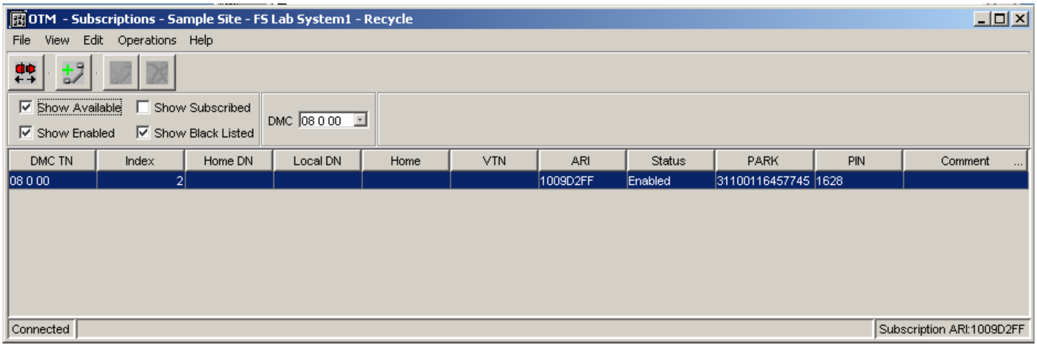
Procedure 83
Configuring handsets

Step	Action
1	**Note:** At this point, there are no PINs shown in the Subscriptions window. Select a handset from the list.
	Click a handset in the list to highlight a row.
2	Enable handsets.
	Click the **Operations** pull-down menu, click **Enable** or click ✓ .

END

Activating the PIN on the handsets

Figure 184
Subscriptions window



OTM - Subscriptions - Sample Site - FS Lab System1 - Recycle

☑ Show Available ☐ Show Subscribed
☑ Show Enabled ☑ Show Black Listed
DMC 08 0 00

DMC TN	Index	Home DN	Local DN	Home	VTN	ARI	Status	PARK	PIN	Comment ...
08 0 00	2					1009D2FF	Enabled	31100116457745	1628	

Connected

Subscription ARI:1009D2FF

Complete the following step:

Procedure 84
Obtaining the PIN

Step	Action
1	**Note:** At this point, in the Subscriptions window, the PINs are shown and the Status is Enabled. Subscribe the DECT handsets.
	See “Handset subscription” on page 390.

END

Note: When a handset is subscribed, the Subscription window shows the Status column as Subscribed and does not show a PIN.

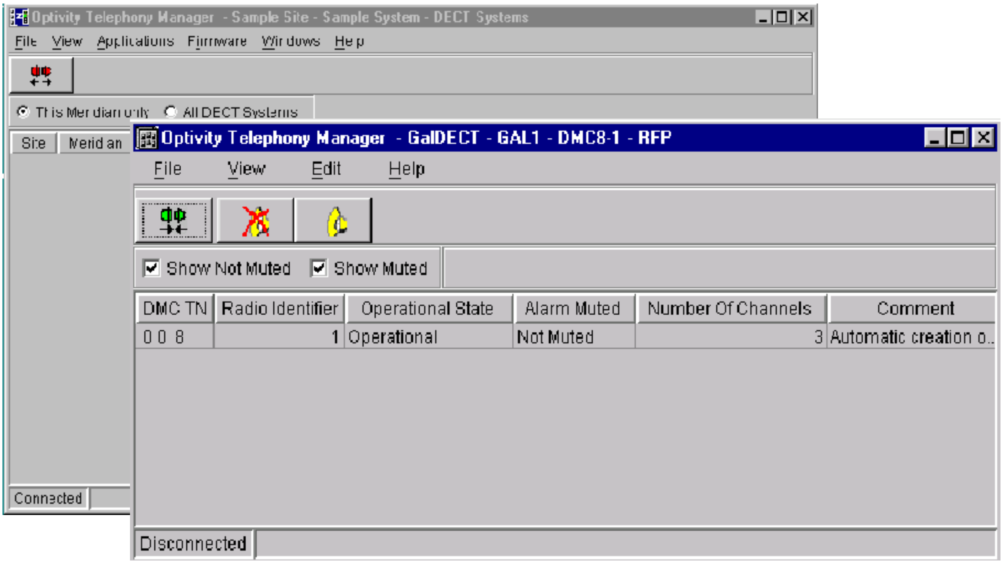
Handset subscription

For detailed information on subscribing a handset, refer to the DECT Handset user guides.

Basestation Powering and Muting

Opening RFP window

Figure 185
DECT Systems main window and RFP window


Optivity Telephony Manager - Sample Site - Sample System - DECT Systems
File View Applications Firmware Windows Help
Site
Meridian
Optivity Telephony Manager - GalDECT - GAL1 - DMC8-1 - RFP
File View Edit Help

● This Meridian only ○ All DECT Systems

Connected

☑ Show Not Muted ☑ Show Muted

DMC TN	Radio Identifier	Operational State	Alarm Muted	Number Of Channels	Comment
0 0 8	1	Operational	Not Muted	3	Automatic creation o..

Disconnected

Complete the following steps:

Procedure 85
Opening RFP window

Step	Action
1	Launch the DECT Systems window.
2	Launch the Boards window.

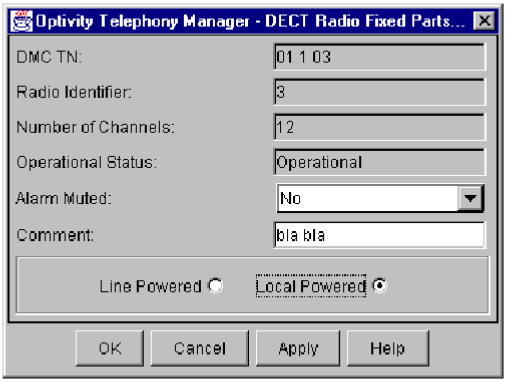
Procedure 85
Opening RFP window

Step	Action
	On the DECT Systems window, click the **Applications** pull-down menu, click **Boards**.
3	Select a basestation from the list.
	Click RFP in the list to highlight a row.
4	Open the Radio Fixed Part properties dialog.
	Click the **File** pull-down menu, click **Properties**.

END

Setting basestation alarm muting, line power, and comments

Figure 186
DECT Radio Fixed Parts



DMC TN: 01 1 03

Radio Identifier: 3

Number of Channels: 12

Operational Status: Operational

Alarm Muted: No

Comment: bla bla

Line Powered ○ Local Powered ●

Complete the following steps:

Procedure 86
Setting alarm muting, line power, and comments

Step	Action
1	Set alarm muting. Select **No** to deny alarm muting or **Yes** to allow alarm muting.
	Click **No** or **Yes**.
2	Enter up to 80 characters for comments.
	Type comments.
3	Select local powered or line powered for the selected basestation.
	Click the **Line Powered** or **Local Powered** radio button.
4	Apply the selections.
	Click the **OK** button.

END

Upgrade a DECT system to an SNMP-managed system

Overview

There are two types of managers for DECT systems:

- Windows Manager
- OTM with DECT application

The Windows Manager, a non-SNMP device, is used to manage the first generation of DECT systems. An OTM with a DECT application manages the present generation of DECT systems.

The following terms are used:

- The DMC (NTCW00AA) and DMC-E (NTCW01AA) are referred to as DMC4 and DMC4-E.
- A DECT system equipped with both DMC4/DMC4-E and DMC8/ DMC8-E is referred to as a Mixed DECT system.

An OTM can manage a DMC4/DMC4-E DECT system or a Mixed DECT system.

In a DMC4/DMC4-E DECT system, or a Mixed DECT system managed by an OTM, the DMC cards must run SNMP software.

A Mixed DECT system must be managed by an OTM. In a Mixed DECT system, a DMC8/DMC8-E must be the relay card.

In a DMC4/DMC4-E DECT system, or a Mixed DECT system managed by OTM, the DMC4 cards must run 45100xxx.dwl software, and the DMC8 cards/ DMC8-E cards must run 47000xxx.dwl software.

Connecting an OTM to a DMC4 relay card using an Ethernet connection is not supported. Only a V.24 connection can be used.

IMPORTANT!

Verify that the correct format of DTN is used before you do the upgrade in the Windows DECT Manager. This avoids major problems after the upgrade to SNMP (OTM).

The DTN format in the Windows DECT Manager must be SCCUU, where S is the shelf, CC is the card, and UU is the unit.

For example, 00210 is shelf 0, card 02, unit 10.

Back up the DMC4 data with Windows DECT Manager

Back up the data on the Windows DECT Manager before proceeding with this upgrade. Follow the steps in Procedure 87 to configure a dial-up network.

Procedure 87
Configuring a dial-up network (Part 1 of 2)

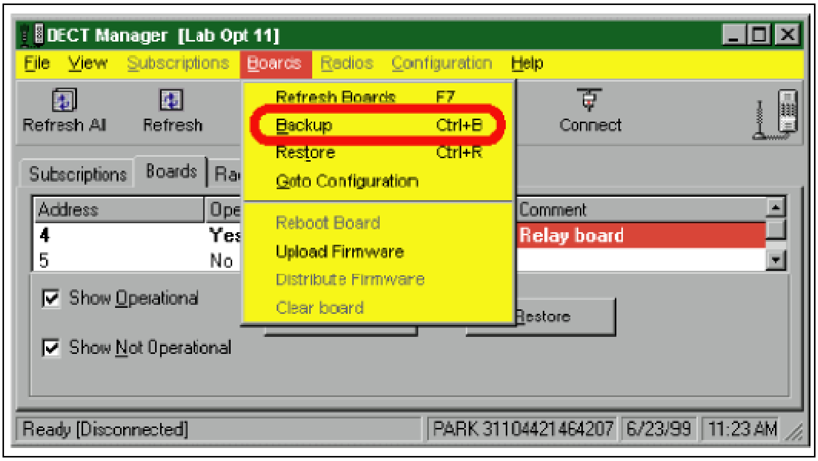
Step	Action
1	Launch the Windows DECT Manager program on the PC.
2	Select **Backup** on the DECT Manager window.
	On the DECT **Manager** window, select **Boards** > **Backup**. See Figure 187 on page 396.
3	Select the DECT system.
	Highlight the system, and click the **OK** button.
4	Click the **Boards** tab.
5	Select all DMC4 cards.

Procedure 87
Configuring a dial-up network (Part 2 of 2)

Step	Action
6	Backup the DMC4 data.
	Click the **Backup** button.
7	Close the connection to the relay card.
	Click the **Connect** icon.

END

Figure 187
DECT Manager window — Boards > Backup



Address	Ope	Comment
4	Yes	Relay board
5	No	

☑ Show Operational

☑ Show Not Operational

Ready [Disconnected] | PARK 31104421464207 | 6/23/99 | 11:23 AM

Uploading OTM supporting firmware to the DMC4 relay card

In a DMC4 DECT system managed by an OTM, the DMC cards must run 45100xxx.dwl software. 45100xxx.dwl software is also required for DECT Messaging.

Connecting an OTM to a DMC4 relay card using an Ethernet connection is not supported. Only a V.24 connection can be used.

Note: Ensure that the DMC relay card is not the first card on the DECT system.

Upload SNMP firmware to the DMC4 relay card

IMPORTANT!

It is very important that the latest non-SNMP firmware (45000405) be loaded before adding SNMP firmware to DMC4 relay cards.

Isolate the DMC4 relay card by disconnecting both faceplate cables connected to the relay card. To upload the OTM supporting firmware to the DMC4 relay card, follow the steps in Table 88.

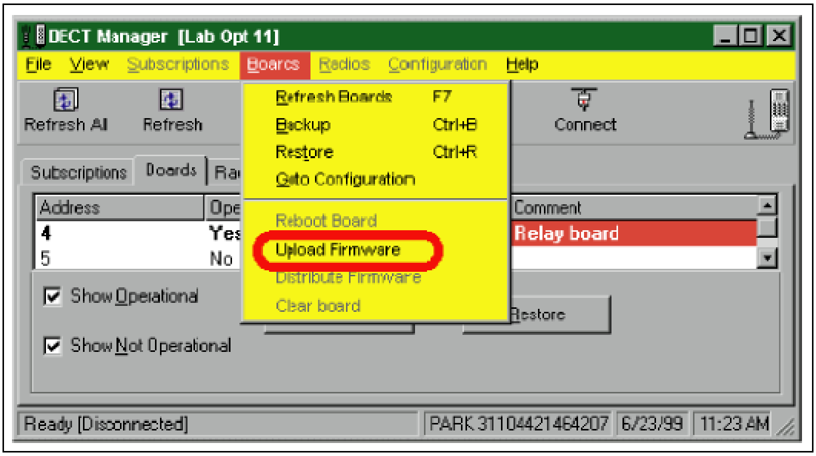
Procedure 88
Uploading SNMP firmware to the DMC4 relay card (Part 1 of 2)

Step	Action
1	Save the SNMP OTM supporting 45100xxx.dwl firmware file to the Windows Manager PC.
2	Select the DECT System on the Windows Manager.
	Highlight the system and click **OK**.
3	Select the **Boards** tab.
	Place the cursor on the tab and click.
4	Select the DMC4 relay board.
	Place the cursor on the DMC4 relay board address and click to highlight it.
5	Upload the new firmware.
	Click the **Boards** drop-down menu and select **Upload Firmware**. See Figure 188 on page 398.

Procedure 88
Uploading SNMP firmware to the DMC4 relay card (Part 2 of 2)

Step	Action
6	Browse and select the new OTM supporting 45100xxx.dwl file.
7	Open the new OTM supporting 45100xxx.dwl file.
	The new software is uploaded to the DMC4 relay card.
	END

Figure 188
DECT Manager window — Boards > Upload Firmware

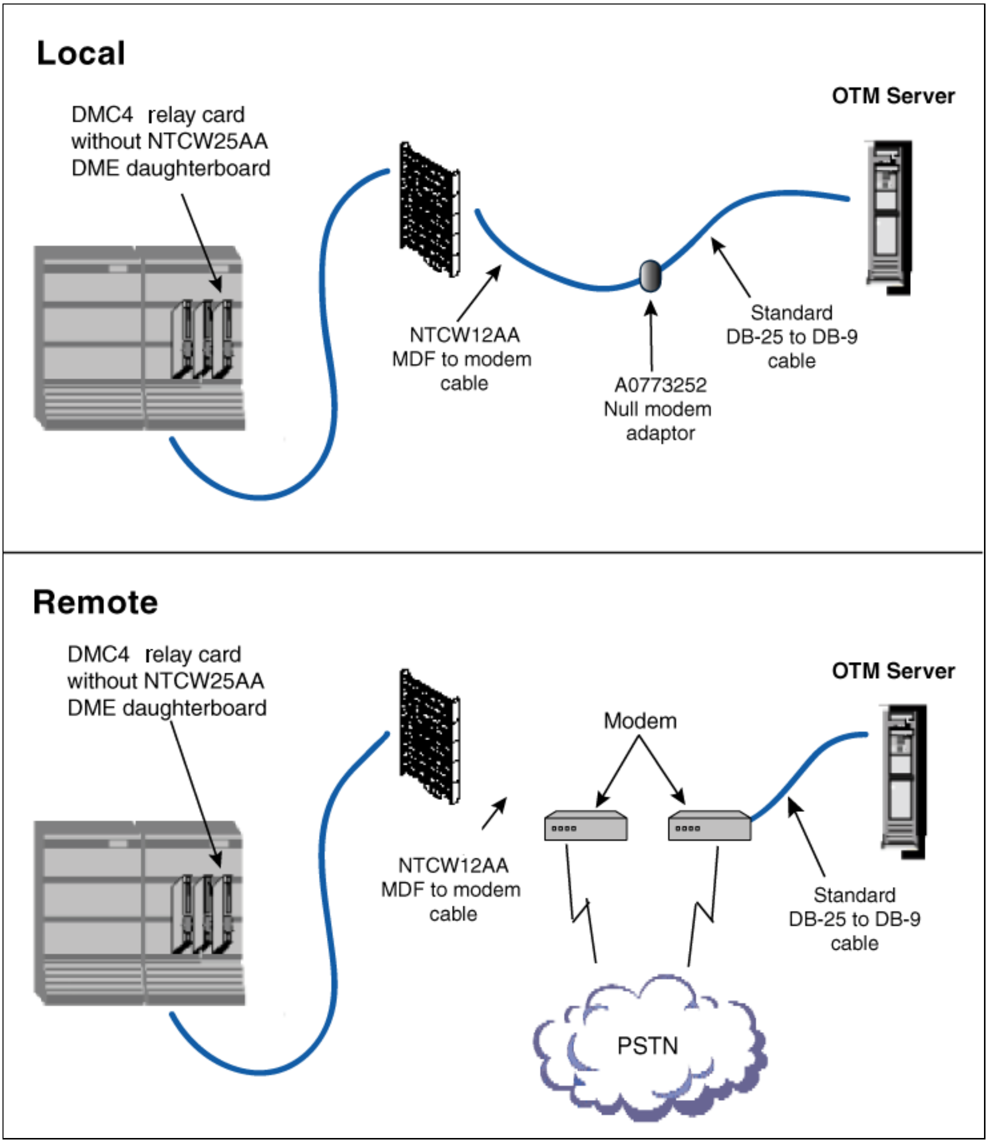


When the new firmware is uploaded, the DMC4 card reboots and the Windows DECT Manager is no longer able to connect to the DECT system.

Connect the DMC relay card to the OTM server

Connect the OTM server to a DMC4 relay card using a V.24 connection. Figure 189 on page 399 shows the OTM server to DMC4 relay card connections.

Figure 189
OTM server to DMC4 relay connections (local and remote)



Configure a local connection

Follow the steps in Procedure 89 to configure a local connection.

Procedure 89
Configuring a local connection

Step	Action
1	Connect the NTCW12AA cable to the DMC4 relay card MDF connector.
2	Choose the OTM Server COM port.
3	Install the null modem plug.
	Connect the DB-25 connector end and the NTCW12AA cable end into the A0773252 null modem adapter.
4	Connect the DB-9 end into the chosen PC COM port.

END

Refer to Table 30 when connecting the NTCW12AA cable to the MDF.

Table 30
NTCW12AA cable to MDF connections

DMC Relay card MDF connection	Cable colour	DB-25 connector pin number	Signal designator
T1	Gray	8	V.24DCD
R2	Yellow	4	V.24RTS
T3	Blue	2	V.24TXD
R3	Red	3	V.24RXD
T4	Pink	7	V.24GND

Note: The BIX tip and ring connections shown in Table 30 on page 400 correspond to standard BIX designation. The first pair is labeled T0 and R0.

Dial-up configuration

For the OTM DECT Manager to communicate over PPP with the DECT system, a RAS service must be configured for dial-out using the appropriate modem.

Note 1: The DECT system can also communicate directly over a modem to a remote OTM DECT Manager.

Note 2: It is also possible to connect to DMC8 relay cards using PPP (serial connect). When connecting to a DMC8 relay board using PPP, Nortel recommends that jumpers J6, J7, J8, and J9 be strapped for V.24 on the DMC.

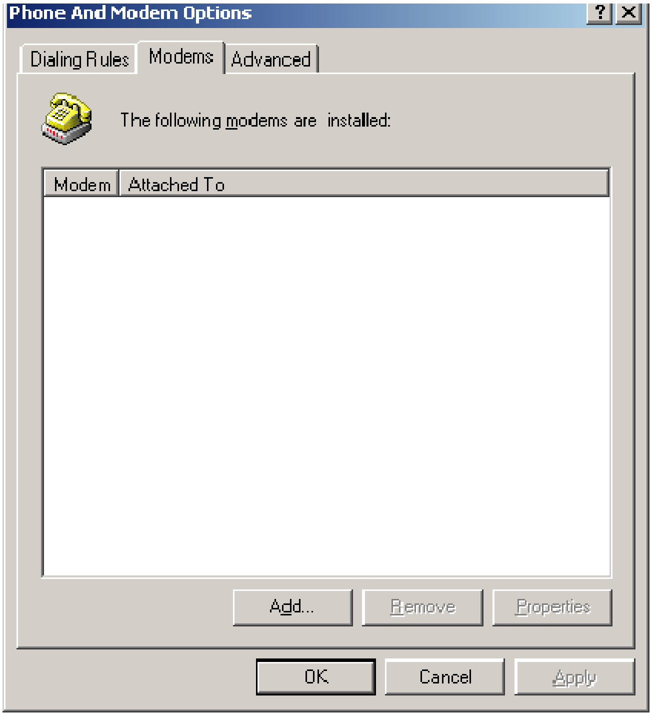
Follow the steps in Procedure 90 on page 402 to configure the dial-up connection.

Procedure 90
Configuring a dial-up connection

To configure a dial-up connection on the PC:

1 Open **Control Panel** > **Phone and Modem Options**. Click the **Modems** tab, if not selected. See Figure 190.

Figure 190
Phone and Modem Options window

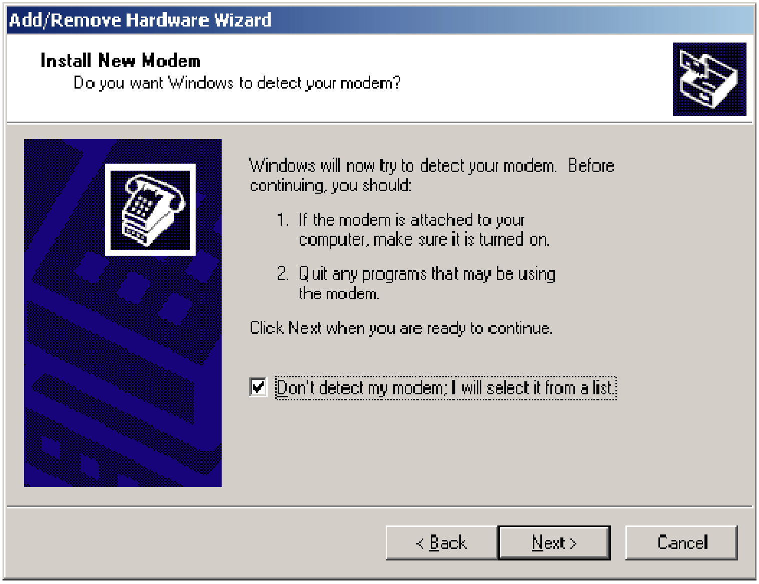


2 Click **Add**.

The **Install New Modem** window opens. See Figure 191 on page 403.

3 Select the **Don’t detect my modem...** check box.

Figure 191
Modem detection



Add/Remove Hardware Wizard

Install New Modem
Do you want Windows to detect your modem?

Windows will now try to detect your modem. Before continuing, you should:

1. If the modem is attached to your computer, make sure it is turned on.
2. Quit any programs that may be using the modem.

Click Next when you are ready to continue.

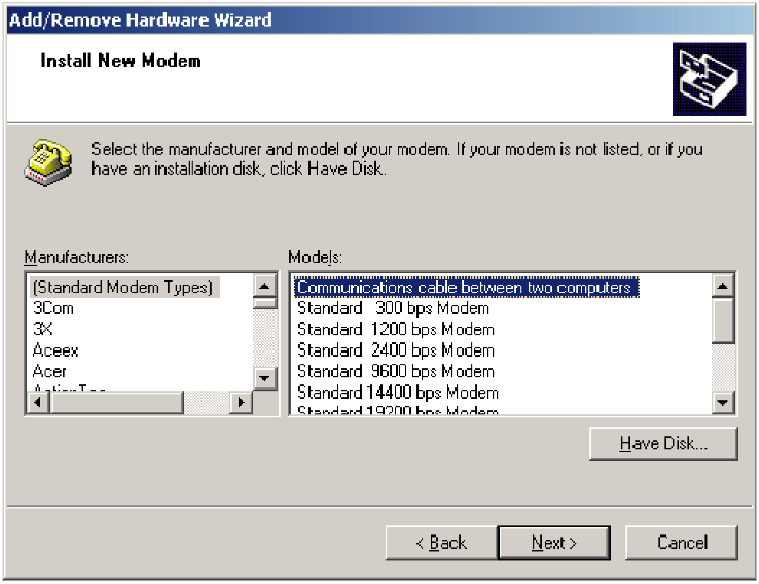
☑ Don't detect my modem; I will select it from a list.

4 Click **Next**.

The Wizard displays a list of modem manufacturers and a list of the corresponding modem models. See Figure 192 on page 404.

5 From the **Manufacturers list:**, select **(Standard Modem Types)**.

Figure 192
Manufacturers and Models lists



Add/Remove Hardware Wizard

Install New Modem

Select the manufacturer and model of your modem. If your modem is not listed, or if you have an installation disk, click Have Disk.

Manufacturers:

- (Standard Modem Types)
- 3Com
- 3X
- Aceex
- Acer

Models:

- Communications cable between two computers
- Standard 300 bps Modem
- Standard 1200 bps Modem
- Standard 2400 bps Modem
- Standard 9600 bps Modem
- Standard 14400 bps Modem

6 From the **Models list:**, select **Communications cable between two computers**.

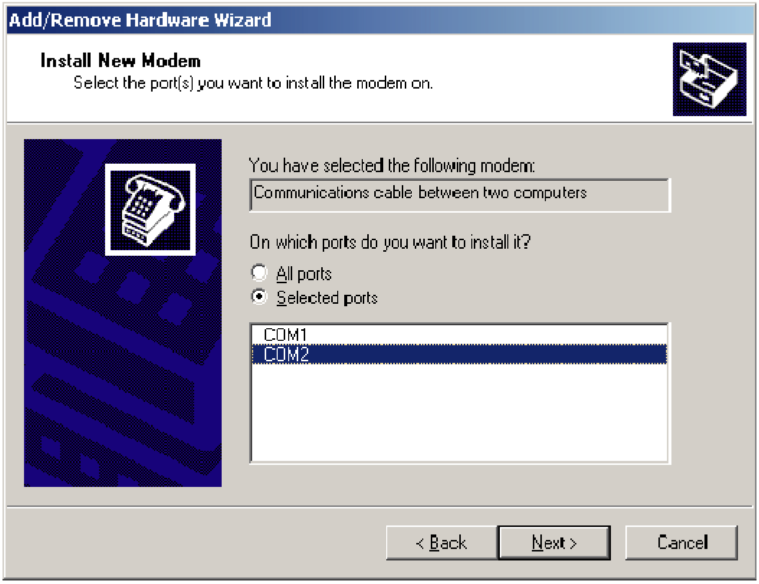
7 Click **Next**.

The Wizard requests information about the ports on which the selected modem is installed. See Figure 193 on page 405.

8 Select a COM port that your PC supports.

Note: Choose the COM port where you made the DB-9 connection.

Figure 193
Port selection



Add/Remove Hardware Wizard

Install New Modem
Select the port(s) you want to install the modem on.

You have selected the following modem:
Communications cable between two computers

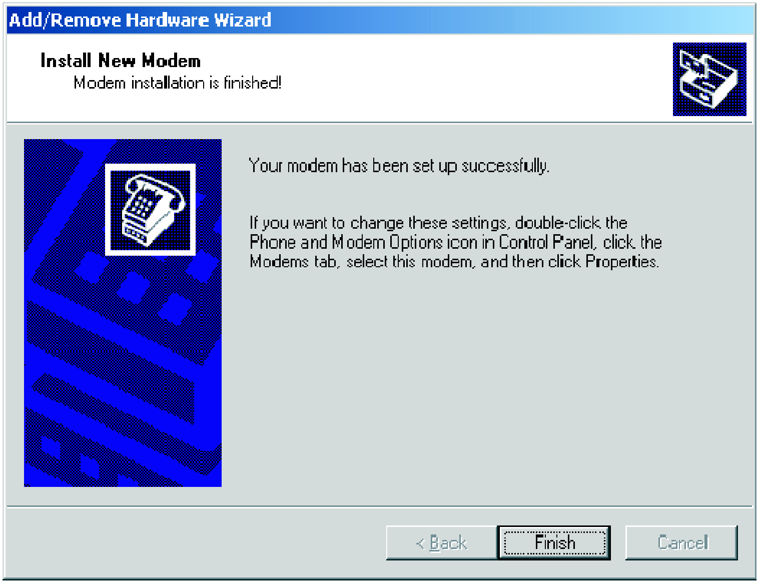
On which ports do you want to install it?
○ All ports
● Selected ports

COM1
COM2

9 Click **Next**.

The Wizard states that modem installation is successful. See Figure 194 on page 406.

Figure 194
Successful modem installation window



Your modem has been set up successfully.

If you want to change these settings, double-click the Phone and Modem Options icon in Control Panel, click the Modems tab, select this modem, and then click Properties.

10 Click **Finish**.

End of Procedure

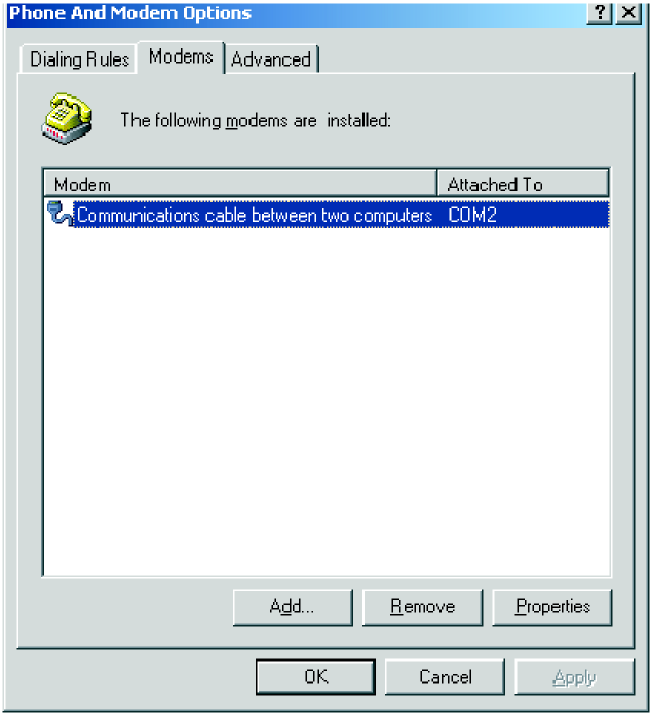
Once installed, the properties of the modem must be configured to communicate serially to the DECT system.

Procedure 91
Configuring the modem

To configure the modem:

1 Open **Control Panel** > **Phone and Modem Options**. Click the **Modems** tab, if not selected. See Figure 195.

Figure 195
Control Panel > Phone and Modem Options > Modems tab



The following modems are installed:

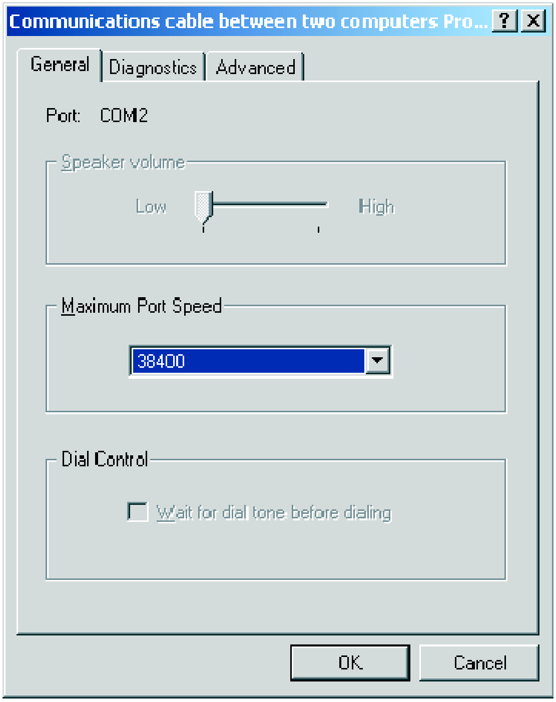
Modem	Attached To
Communications cable between two computers	COM2

2 Select **Communications cable between two computers**.

3 Click **Properties**.

The **Communications cable between two computers Properties** window opens. See Figure 196.

Figure 196
Properties window — General tab



Communications cable between two computers Pro...

General | Diagnostics | Advanced

Port: COM2

Speaker volume

Maximum Port Speed: 38400

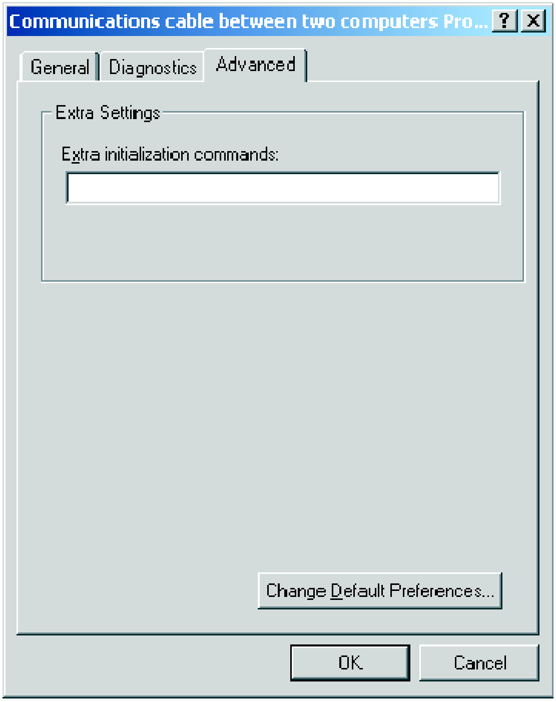
Dial Control

□ Wait for dial tone before dialing

4 Select **38400** from the **Maximum Port Speed** drop-down list.

5 Click the **Advanced** tab to select it. See Figure 197 on page 409.

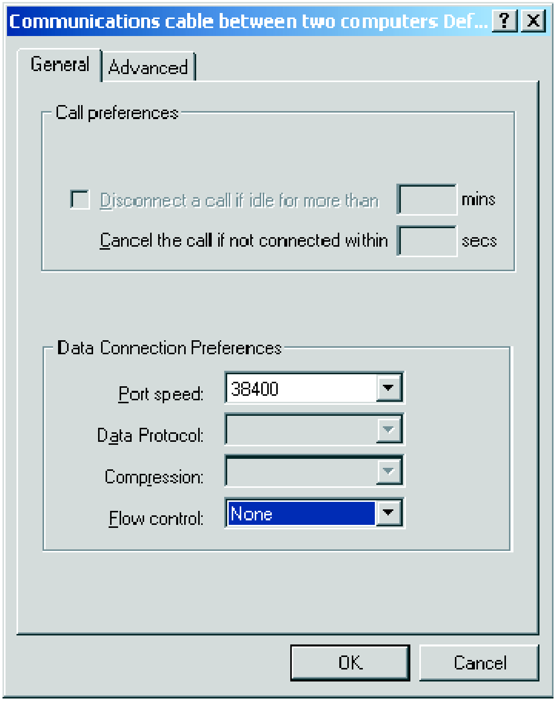
Figure 197
Properties window — Advanced tab


Communications cable between two computers Pro...
?
X
General
Diagnostics
Advanced
Extra Settings
Extra initialization commands:
Change Default Preferences...
OK
Cancel

6 Click **Change Default Preferences**.

The **Communications cable between two computers Default Preferences** window opens. See Figure 198 on page 410.

Figure 198
Change Default Preferences — General tab



Communications cable between two computers Def...

General | Advanced

Call preferences

□ Disconnect a call if idle for more than ____ mins

Cancel the call if not connected within ____ secs

Data Connection Preferences

Port speed: 38400

Data Protocol:

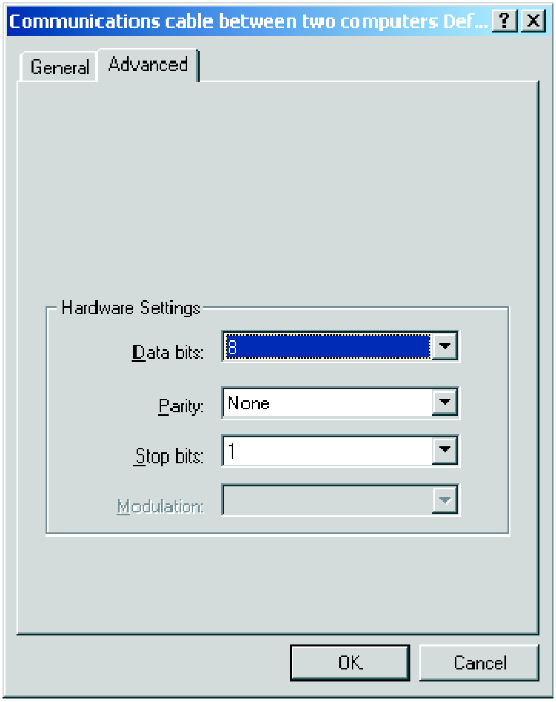
Compression:

Flow control: None

7 Select **None** from the **Flow control:** drop-down list in **Data Connection Preferences**.

8 Click the **Advanced** tab to select it. See Figure 199 on page 411.

Figure 199
Change Default Preferences — Advanced tab



Hardware Settings

Data bits: 8

Parity: None

Stop bits: 1

Modulation:

9 Define **Hardware Settings** on the **Advanced** tab:

a. Set the **Data bits** to **8**.

b. Set the **Parity bits** to **None**.

c. Set the **Stop bits** to **1**.

10 Click **OK**.

The modem configuration windows close.

End of Procedure

Network and dial-up connections configuration

Procedure 92
Configuring the network and dial-up connections

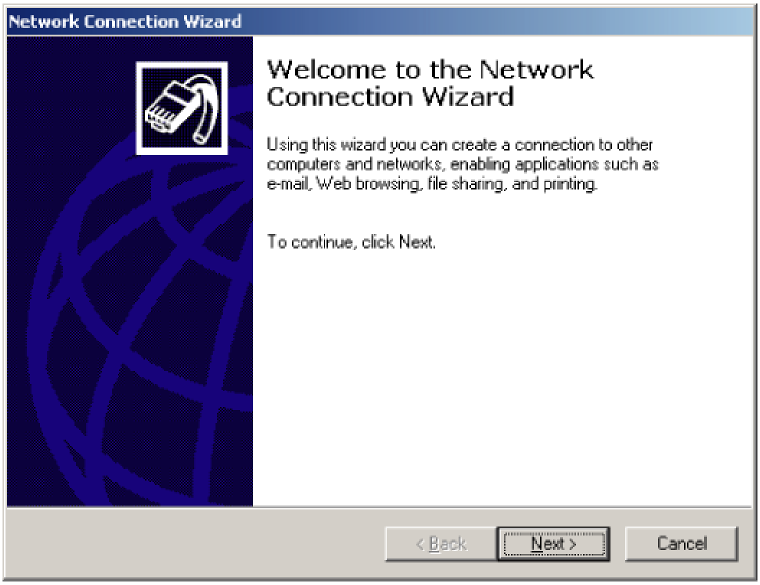
To configure the network and dial-up connections on the PC:

1 Select **Control Panel** > **Network and Dial-up Connections**.

2 Double-click the **Make New Connection** icon.

The Connection Wizard starts. See Figure 200.

Figure 200
Network Connection Wizard



Welcome to the Network Connection Wizard

Using this wizard you can create a connection to other computers and networks, enabling applications such as e-mail, Web browsing, file sharing, and printing.

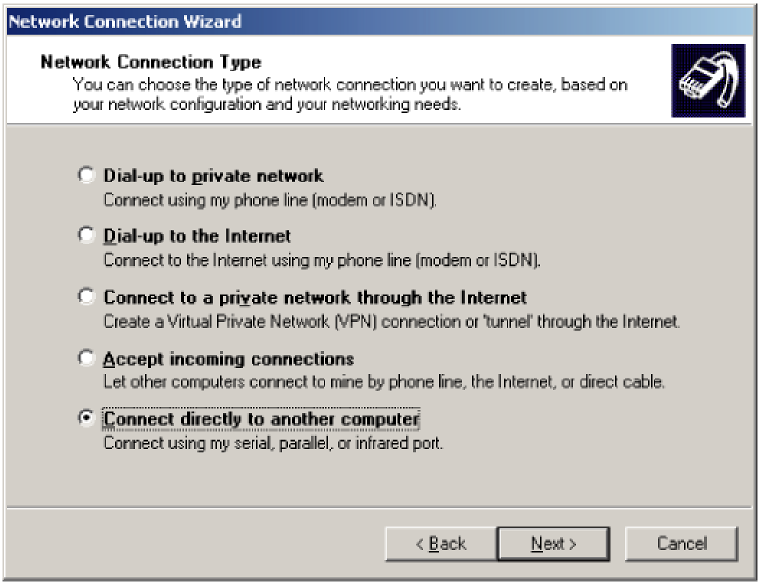
To continue, click Next.

3 Click **Next**.

The **Network Connection Typ**e window opens. See Figure 201.

4 Select the **Connect directly to another computer** radio button.

Figure 201
Network Connection Type window



Network Connection Wizard

Network Connection Type
You can choose the type of network connection you want to create, based on your network configuration and your networking needs.

○ **Dial-up to private network**
Connect using my phone line (modem or ISDN).

○ **Dial-up to the Internet**
Connect to the Internet using my phone line (modem or ISDN).

○ **Connect to a private network through the Internet**
Create a Virtual Private Network (VPN) connection or 'tunnel' through the Internet.

○ **Accept incoming connections**
Let other computers connect to mine by phone line, the Internet, or direct cable.

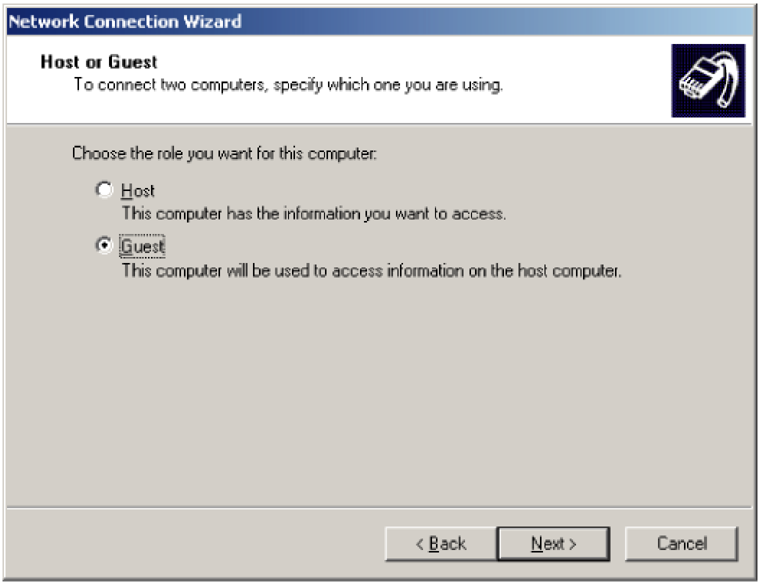
● **Connect directly to another computer**
Connect using my serial, parallel, or infrared port.

5 Click **Next**.

The **Host or Guest** window opens. See Figure 202 on page 414.

6 Select the **Guest** radio button.

Figure 202
Host or Guest window



Network Connection Wizard

Host or Guest

To connect two computers, specify which one you are using.

Choose the role you want for this computer:

○ Host
This computer has the information you want to access.

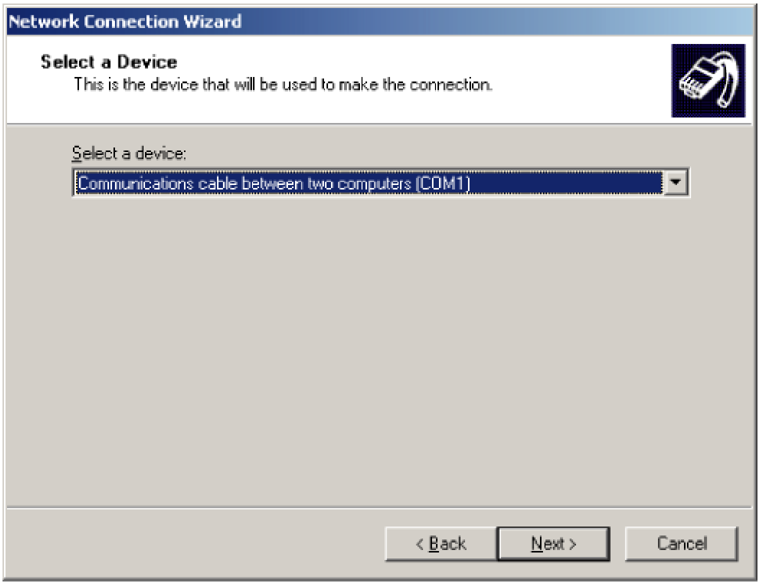
● Guest
This computer will be used to access information on the host computer.

7 Click **Next**.

The **Select a Device** window opens. See Figure 203 on page 415.

8 Select **Communications cable between two computers** from the **Select a device:** drop-down list.

Figure 203
Select a Device window



Network Connection Wizard
Select a Device
This is the device that will be used to make the connection.

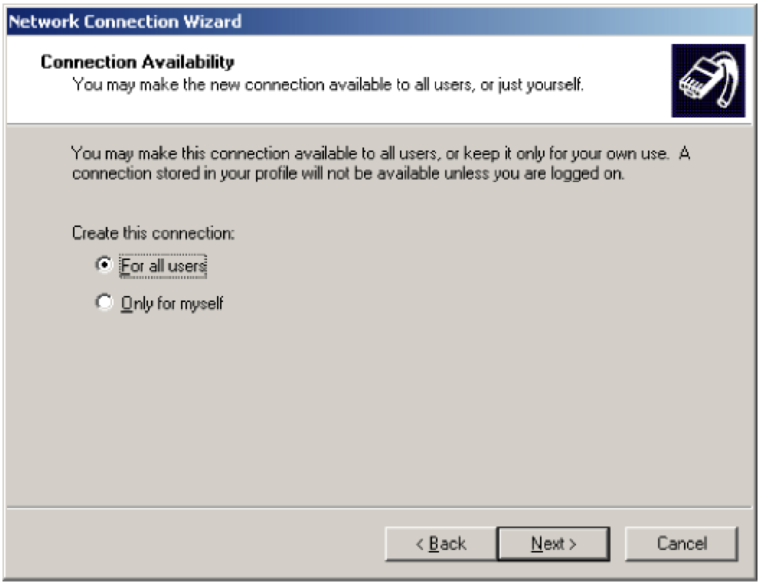
Select a device: Communications cable between two computers (COM1)

9 Click **Next**.

The **Connection Availability** window opens. See Figure 204 on page 416.

10 Select the **For all users** radio button.

Figure 204
Connection Availability window



Connection Availability

You may make the new connection available to all users, or just yourself.

You may make this connection available to all users, or keep it only for your own use. A connection stored in your profile will not be available unless you are logged on.

Create this connection:

● For all users

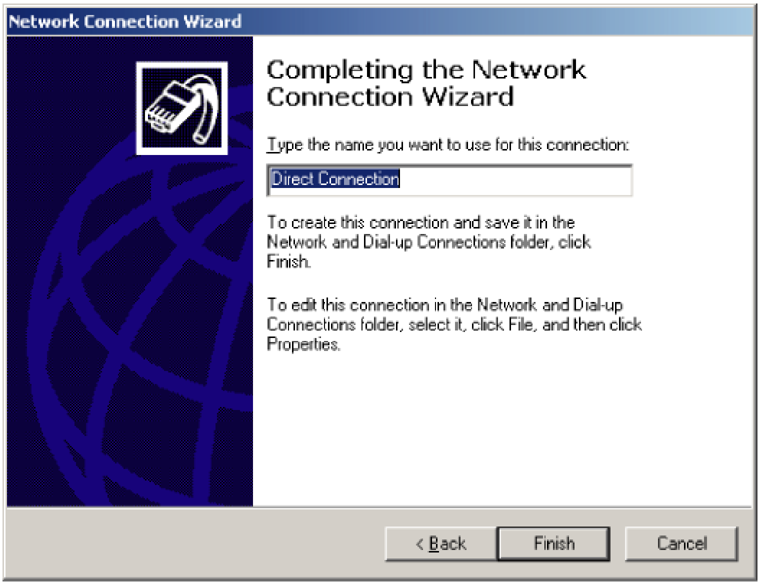
○ Only for myself

11 Click **Next**.

The **Completing the Network Connection Wizard** window opens. See Figure 205 on page 417.

12 Type a name for the connection.

Figure 205
Completing the Network Connection Wizard



Completing the Network Connection Wizard

Type the name you want to use for this connection:

Direct Connection

To create this connection and save it in the Network and Dial-up Connections folder, click Finish.

To edit this connection in the Network and Dial-up Connections folder, select it, click File, and then click Properties.

13 Click **Finish**.

14 Choose a username and password for the connection.

15 Click **Close**.

16 Restart the PC.

End of Procedure

Change the DMC4 relay card default IP address

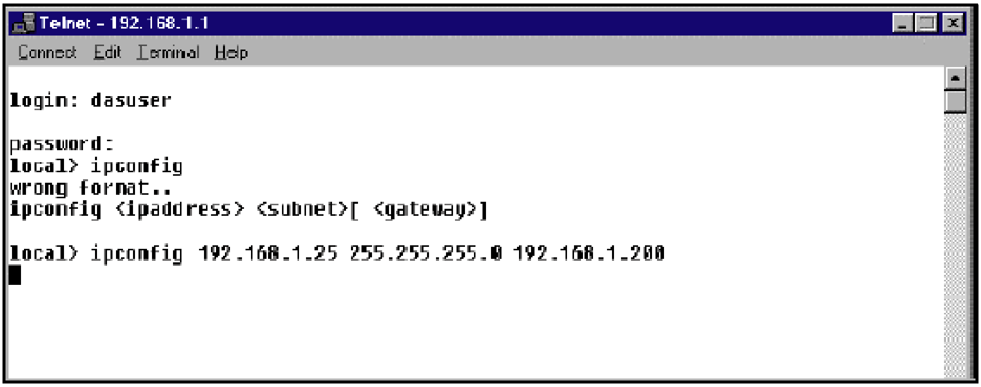
IMPORTANT!

The DMC4 card has a default IP address of 192.168.1.1. This DMC4 address must be changed to conform to the network IP address plan.

Reset the DMC4 relay card to the server IP address

Open Telnet on the PC that is used for configuring. Connect to the default DMC4 IP address (192.168.1.1). Figure 206 shows the Telnet session.

Figure 206
Telnet to 192.168.1.1



```
login: dasuser

password:
local> ipconfig
wrong format..
ipconfig <ipaddress> <subnet>[ <gateway>]

local> ipconfig 192.168.1.25 255.255.255.0 192.168.1.200
```

Follow the steps in Table 93 to reset the DMC4 relay card to the server IP address.

Procedure 93
Resetting the DMC4 relay card to server IP address

Step	Action
1	Open the Telnet dialog.
	Click **Start** on the Windows taskbar and choose **Accessories > Telnet**.
2	Enter the username and password.
	Username: dasuser Password: dasuser
3	Change the relay DMC4 card address when the connection prompt **local** appears.
	Enter the following command: **ipconfig xxx.xxx.xxx.xxx yyy.yyy.yyy.yyy zzz.zzz.zzz.zzz** Where: **xxx.xxx.xxx.xxx** = new IP address of the DMC4 relay card **yyy.yyy.yyy.yyy** = subnet mask (usually 255.255.255.0) **zzz.zzz.zzz.zzz** = IP address if this is the gateway for the network. ***Note:*** Set **zzz.zzz.zzz.zzz** to the IP address of the OTM server Ethernet interface. If there are two Ethernet interfaces on the OTM server, set **zzz.zzz.zzz.zzz** to the IP address of the interface that is on the same network as the DMC4 relay card.

END

Launch the OTM DECT back-end process

The back-end process must be visible to establish a connection. If the back-end is closed in error, OTM DECT does not run.

> **IMPORTANT!**
>
> Always ensure the Windows Registry is backed up before opening the Registry and Registry keys.

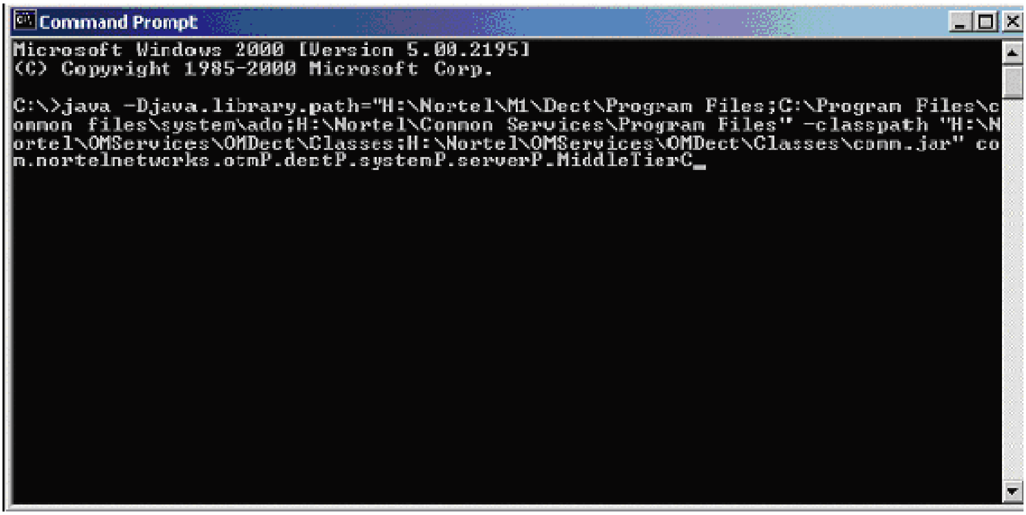
To launch the OTM DECT back-end process, follow the steps in Table 94.

Procedure 94
Launching the OTM DECT back-end process

Step	Action
1	Open the registry window.
	Click **Start** on the Windows taskbar, and select **Run** > **regedit**.
2	Copy the value of the key to the clipboard.
	Highlight **HKEY_LOCAL_MACHINE\SOFTWARE\NorMat\SMP\OTMServices\DECT\Args**, right-click the highlighted text, and select **Copy**.
3	Paste the value of the registry key (that you copied in Step 2) to the **Command Prompt** window.
	Open the **Command Prompt** window. At the command prompt, type **java**, press the space bar once (to enter a space), and then paste the text you copied from the registry. See Figure 207 on page 421.
4	Press **Enter**.
	The OTM DECT back-end is launched.

END

Figure 207
Command Prompt window with registry key value entered



```
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\>java -Djava.library.path="H:\Nortel\M1\Dect\Program Files;C:\Program Files\c
ommon files\system\ado;H:\Nortel\Common Services\Program Files" -classpath "H:\N
ortel\OMServices\OMDect\Classes;H:\Nortel\OMServices\OMDect\Classes\comm.jar" co
m.nortelnetworks.otmP.dectP.systemP.serverP.MiddleTierC_
```

DAS configuration

It is necessary to configure the DECT Access System (DAS). You must first add the DECT system to OTM DECT.

Procedure 95
Adding the DECT system to OTM DECT

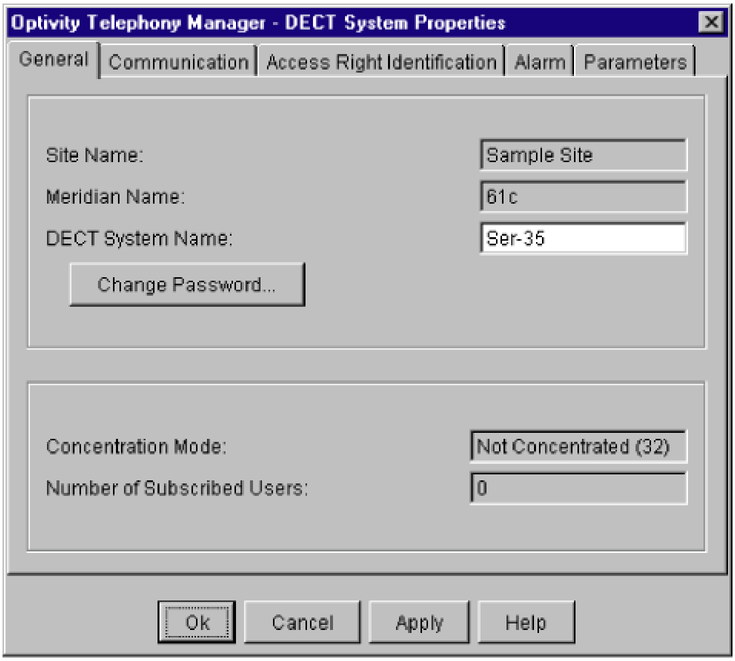
To add the DECT system to OTM DECT:

1 Launch the OTM DECT application.

2 Select **File** > **Add**.

3 Enter the **DECT System Name** on the **General** tab of the **Optivity Telephony Manager – DECT System Properties** window. See Figure 208 on page 422.

Figure 208
Optivity Telephony Manager – DECT System Properties window



Optivity Telephony Manager - DECT System Properties
General
Communication
Access Right Identification
Alarm
Parameters
Change Password...
Ok
Cancel
Apply
Help

Site Name: Sample Site

Meridian Name: 61c

DECT System Name: Ser-35

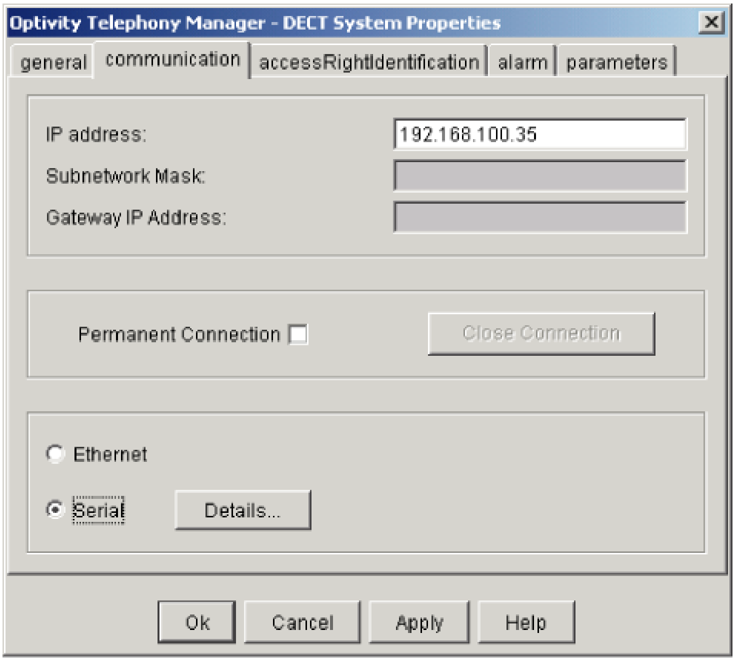
Concentration Mode: Not Concentrated (32)

Number of Subscribed Users: 0

4 Click **Apply**.

5 Click the **Communication** tab to select it. See Figure 209 on page 423.

Figure 209
DECT System Properties — Communication tab



Optivity Telephony Manager - DECT System Properties

IP address: 192.168.100.35

Subnetwork Mask:

Gateway IP Address:

Permanent Connection □

○ Ethernet

● Serial

6 Enter the IP address of this DMC4 card (use the address that you configured in Procedure 93 on page 419).

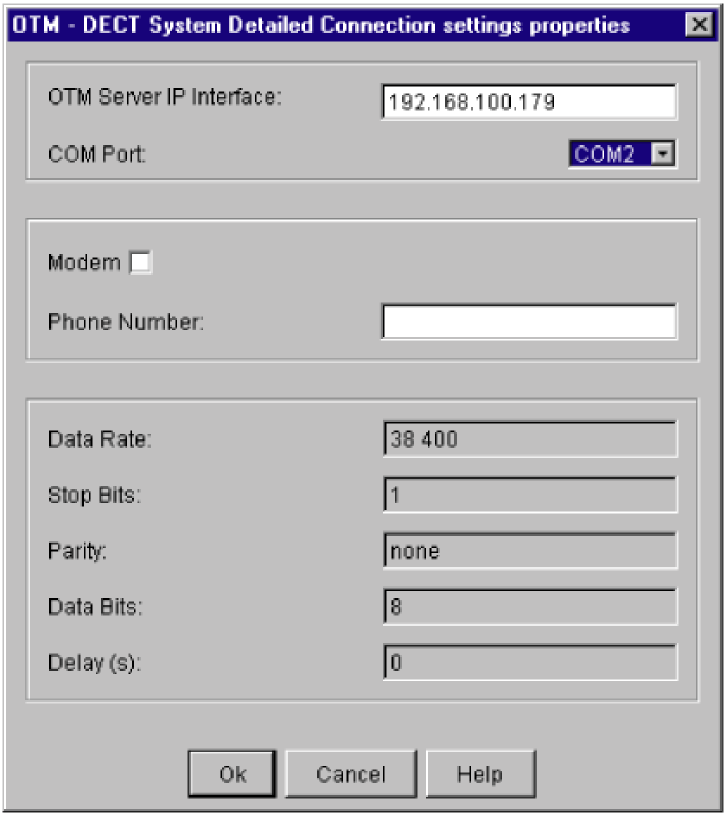
7 Select the **Serial** radio button.

8 Click **Details**.

The **OTM-DECT System Detailed Connection settings properties** window opens.

9 Select the COM port that DAS uses to connect to the PC.

Figure 210
OTM – DECT System Detailed Connection Settings Properties window



OTM - DECT System Detailed Connection settings properties

OTM Server IP Interface: 192.168.100.179

COM Port: COM2

Modem □

Phone Number:

Data Rate: 38 400

Stop Bits: 1

Parity: none

Data Bits: 8

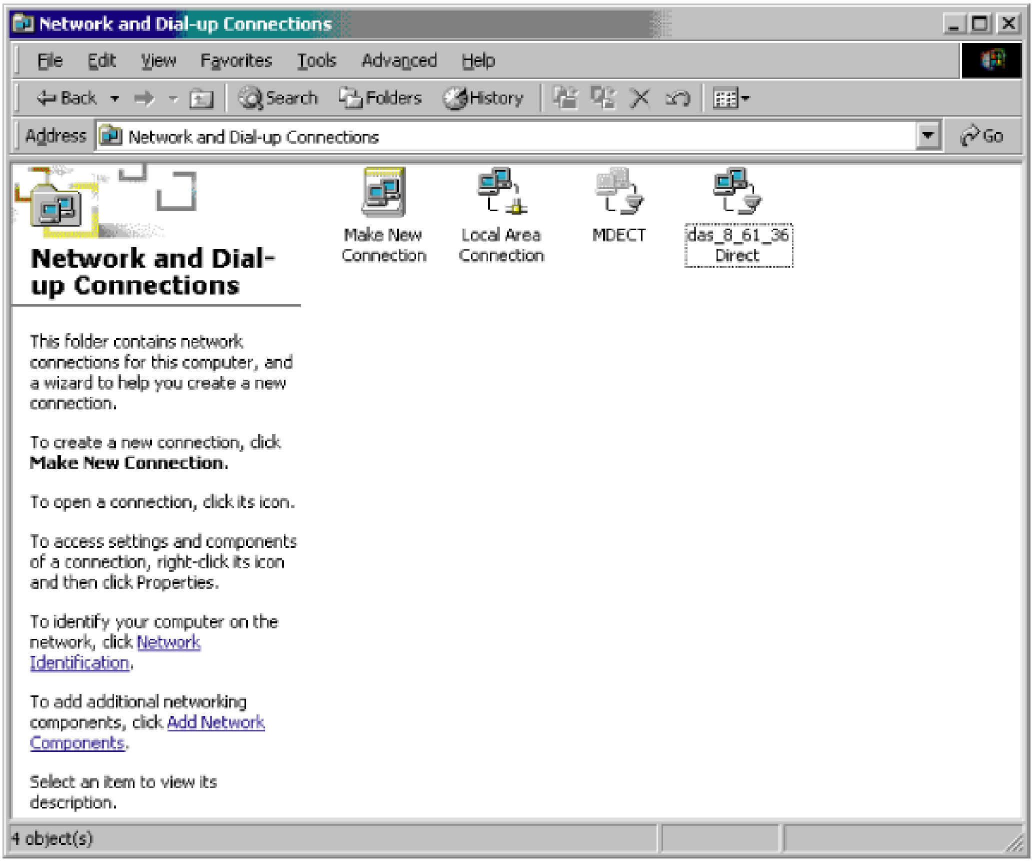
Delay (s): 0

10 Enter the IP address of the OTM Server (for example, 192.168.100.179) in the **OTM Server IP Interface** text box.

End of Procedure

After you have successfully added the DECT system to the OTM DECT, a new icon appears in the **Network and Dial-up Connections** window. Figure 211 shows the new site added to the **Network and Dial-up Connections** window. Note that the icon represents a Direct PC to PC cable connection. If you are connected using a modem, the icon shows a telephone, which represents a dial-up connection.

Figure 211
New connection icon in the Network and Dial-up Connections window



Network and Dial-up Connections
File Edit View Favorites Tools Advanced Help
Back Search Folders History
Address Network and Dial-up Connections
Go
Make New Connection
Local Area Connection
MDECT
das_8_61_36 Direct
4 object(s)

Network and Dial-up Connections

This folder contains network connections for this computer, and a wizard to help you create a new connection.

To create a new connection, click **Make New Connection.**

To open a connection, click its icon.

To access settings and components of a connection, right-click its icon and then click Properties.

To identify your computer on the network, click Network Identification.

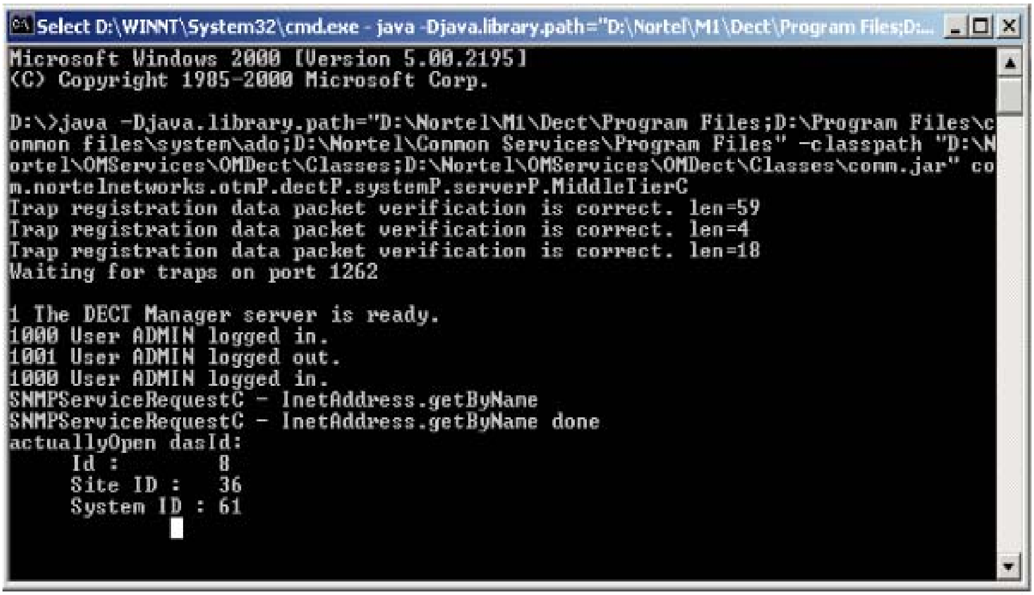
To add additional networking components, click Add Network Components.

Select an item to view its description.

Note: At this stage, disable the LAN. If it is in the enabled state, it can cause an error when attempting to connect to the DECT system using the RAS connection.

Figure 212 is an example of the DOS window running the DECT back-end process after a new DECT site has been added using a serial connection.

Figure 212
DOS window running the back-end process — new DECT site using serial connection


Select D:\WINNT\System32\cmd.exe - java -Djava.library.path="D:\Nortel\M1\Dect\Program Files;D:...

```
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

D:\>java -Djava.library.path="D:\Nortel\M1\Dect\Program Files;D:\Program Files\c
ommon files\system\ado;D:\Nortel\Common Services\Program Files" -classpath "D:\N
ortel\OMServices\OMDect\Classes;D:\Nortel\OMServices\OMDect\Classes\comm.jar" co
m.nortelnetworks.otmP.dectP.systemP.serverP.MiddleTierC
Trap registration data packet verification is correct. len=59
Trap registration data packet verification is correct. len=4
Trap registration data packet verification is correct. len=18
Waiting for traps on port 1262

1 The DECT Manager server is ready.
1000 User ADMIN logged in.
1001 User ADMIN logged out.
1000 User ADMIN logged in.
SNMPServiceRequestC - InetAddress.getByName
SNMPServiceRequestC - InetAddress.getByName done
actuallyOpen dasId:
     Id :       8
     Site ID :   36
     System ID : 61
```

You can now connect to the new DECT system.

When connecting, the following sequence of messages appears at the bottom of the DECT systems window:

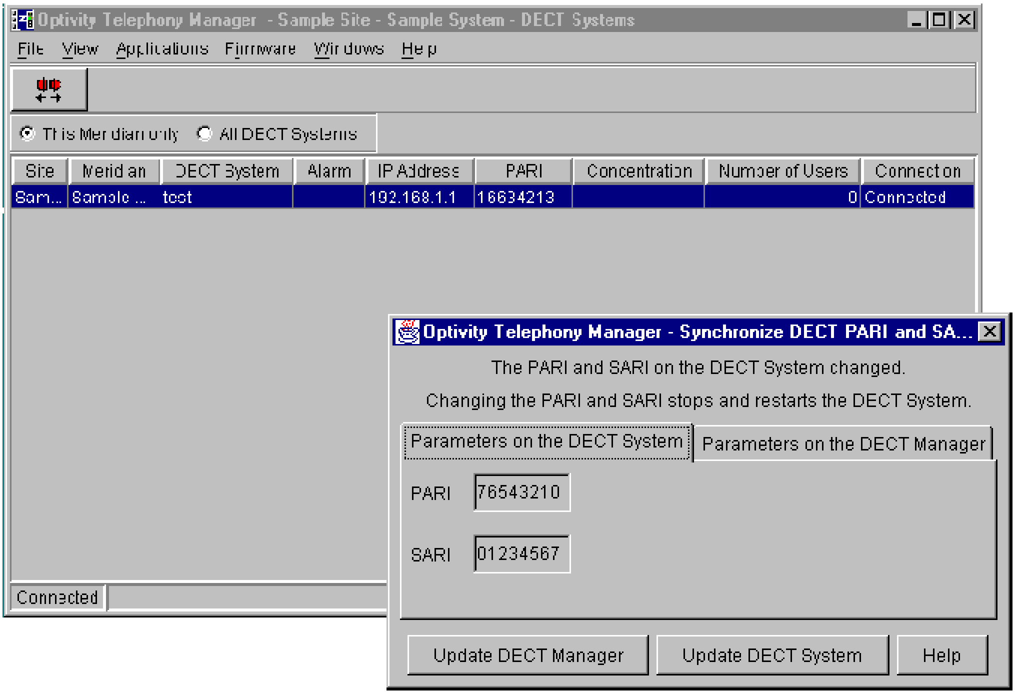
Connecting	The connection to the remote MODEM has been established successfully
Connecting	Authenticating onto the DECT system
Connected	Connections opened
Connected	Synchronization with the DECT System completed

Note: If there is a problem connecting to the system and the error seen on the back-end process window is related to the Authentication process, try resetting the DMC4 relay card password to correct the error.

Synchronize data with the DECT system

When the OTM DECT Manager connects to the DECT system, synchronization occurs. The OTM database can be updated with the DECT system data.

Figure 213
DECT Systems window and a synchronize dialog


Optivity Telephony Manager - Sample Site - Sample System - DECT Systems
File
View
Applications
Firmware
Windows
Help

● This Meridian only ○ All DECT Systems

Site	Meridian	DECT System	Alarm	IP Address	PARI	Concentration	Number of Users	Connection
Sam...	Sample ...	test		192.168.1.1	16634213		0	Connected

Connected

Optivity Telephony Manager - Synchronize DECT PARI and SA...

The PARI and SARI on the DECT System changed.

Changing the PARI and SARI stops and restarts the DECT System.

Parameters on the DECT System
Parameters on the DECT Manager

PARI 76543210

SARI 01234567

Update DECT Manager
Update DECT System
Help

When the DECT system is connected, there is a red icon on the toolbar. See Figure 213.

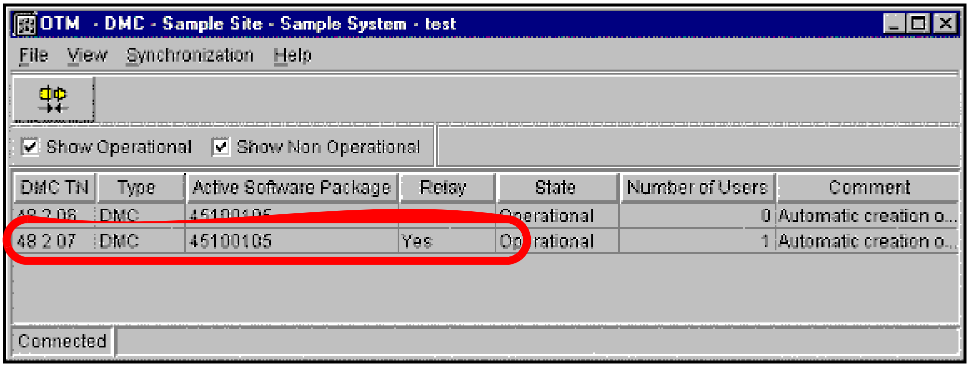
With the OTM DECT Manager connected to the system, store the system data in the OTM Manager database by clicking the **Update DECT Manager** button on all synchronization dialogs.

Activate the firmware on all DMC4 cards

Confirm the active software package on the DMC4 relay card (see Figure 214 on page 428). This must be the same 45100xxx.dwl firmware that was loaded earlier (see Table 88 on page 397).

If it is not the 45100xxx.dwl firmware, you must reload the firmware by selecting **Upload** from the **Firmware** menu on the DECT Systems window (see Figure 215 on page 430). Choose the file you want to upload. The DMC4 card reboots. You must then re-connect to the DECT system.

Figure 214
DMC window and DECT Board properties dialog



☑ Show Operational ☑ Show Non Operational

DMC TN	Type	Active Software Package	Relay	State	Number of Users	Comment
48 2 06	DMC	45100105		Operational	0	Automatic creation o...
48 2 07	DMC	45100105	Yes	Operational	1	Automatic creation o...

Connected

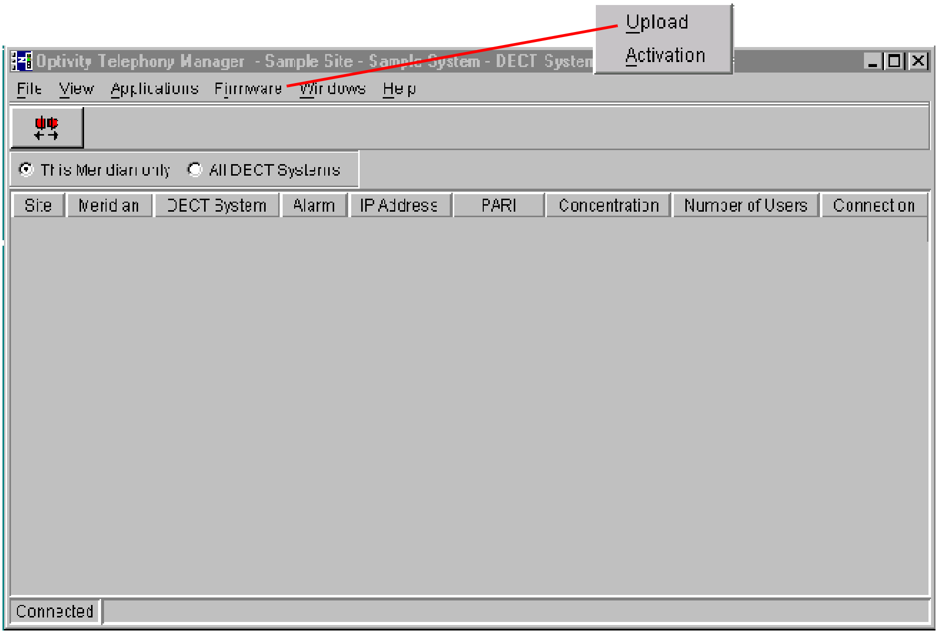
When you have confirmed that the software package on the DMC4 relay card is correct, activate this firmware on all DMC4 cards. To activate the firmware on the DMC4 cards, follow the steps in Table 96.

Procedure 96
Activating the firmware on DMC4 cards

Step	Action
1	Re-connect the faceplate cables from the relay card to the adjoining DMC4 cards.
2	From the **Firmware** menu, select **Activation**.
	After the firmware has been activated, ensure that the Active Software Package on all DMC4 cards corresponds to the 45100xxx.dwl firmware. See Figure 216 on page 430.

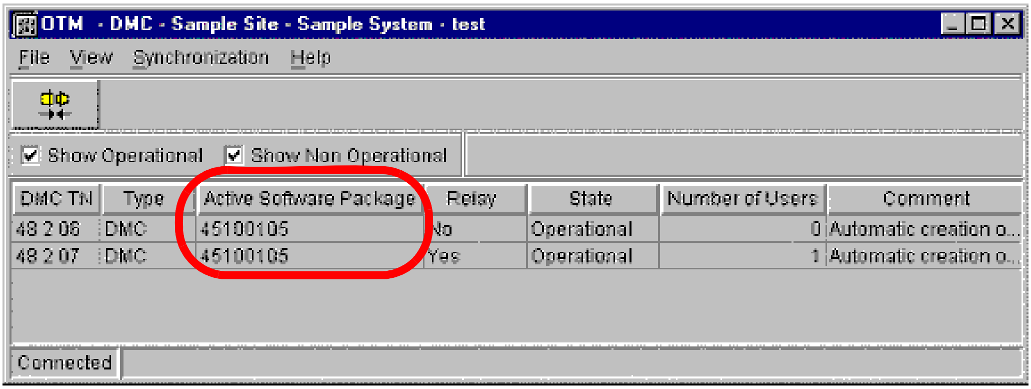
END

Figure 215
DECT Systems window



Site	Meridian	DECT System	Alarm	IP Address	PARI	Concentration	Number of Users	Connection

Figure 216
DMC window



DMC TN	Type	Active Software Package	Relay	State	Number of Users	Comment
48 2 06	DMC	45100105	No	Operational	0	Automatic creation o...
48 2 07	DMC	45100105	Yes	Operational	1	Automatic creation o...

Your DECT system is now complete and fully configured.

Implementing and operating MSMN

Implementing the MSMN feature

The sequence of actions required to configure this feature is as follows:

1 Configure a phantom superloop using LD 97, if required.

2 Create the new DCS sets in LD 10.

3 Configure the RCFW data in LD 57 and LD 15 for handsets assigned as a visitor.

4 Use the DECT manager to configure sets on the DMC8.

5 Pre-subscribe the visiting handset one time at the MCDN node.

Note: Subscription includes both overlay configuration and DECT Manager configuration. For DECT Manager configuration, see "Configuring DECT on the OTM server" on page 351.

LD 10 – Add/Change DCS data block or data blocks (Part 1 of 2)

Prompt	Response	Description
REQ:	NEW NEW 1-255 CHG ECHG	NEW = Add a Digital Cordless Set NEW X = The generation of new DCS units stop when the maximum Index of 509 is reached on a single DMC8 or VTNs on the system run out or WRLS Licence limits reached. All new DCS must be on the same DMC8. CHG = Allows the DCS configuration to change to another DMC8. All new DCS must be on the same DMC8. ECHG = This command can change either the VSIT response or the HMDN response.
TYPE:	DCS	Digital Cordless Set. Differentiates between analogue sets and non-concentrated digital DECT handsets. If TYPE=DCS, the system allocates the next available VTN, and WRLS defaults to YES and WTYP defaults to DECT. If package #350 is included, MWUN defaults to 32. CLS defaults to ERCA, allowing the Enhanced RCFW feature.
TN		Terminal Number
	l s c u	Format for Large System and CS 1000E system, where l = loop, s = shelf, c = card, u = unit
	c u	Format for Small System, CS 1000S system, Media Gateway 1000B, and Media Gateway 1000T, where c = card and u = unit The system provides the Virtual TN for the handset.
CDEN	(4D)	Card Density. Only valid value for IPE is 4D. Normal input is <CR>.
WRLS	YES	WiReLess analogue Set – entry defaults to YES with no user input; value cannot be CHG'ed.

LD 10 – Add/Change DCS data block or data blocks (Part 2 of 2)

Prompt	Response	Description
WTYP	DECT	Wireless TYPe – entry defaults to DECT with no user input; value cannot be CHG’ed.
MWUN	32	Maximum number of Wireless UNits – entry defaults to 32 with no user input – value cannot be CHG’ed. Note: If MWUN = 32, CDEN automatically changes to 8D, and prints as an 8D unit.
DMC8		Location of the actual DMC8. Assigns a TN to a DECT Mobility Card located on an IPE shelf or cabinet.
	l s c	Format for Large System and CS 1000E system, where l = loop, s = shelf, c = card
	c	Format for Small System, CS 1000S system, Media Gateway 1000B, and Media Gateway 1000T, where c = card
INDX	0. 509	DMC8 index to map the Virtual TN to a DMC8 TN. Starting index on DMC8, each unit increments to the next available unit.
VSIT	(NO) YES	ViSITing DECT set. Determines the difference between a local handset and a visiting handset. VSIT available if the MSMN Package is unrestricted. YES = visiting DECT set. NO = local DECT set.
HMDN	x...x	HoMe Directory Number. Sets the DN as a valid MCDN network DN. NMDN available if VSIT = YES.

LD 10 – Copy DCS data block or data blocks

Prompt	Response	Description
REQ:	CPY 1 – 32	CPY n = The generation of new units stops when the following occurs: maximum index of 509 is reached on a single DMC8 or VTNs on the system run out or WRLS Licence limits reached. All DCS must be on the same DMC8.
DMC8	l s c l	Location of the actual DMC8 to copy on an IPE shelf or cabinet.

LD 10 – Remove DCS data block or data blocks

Prompt	Response	Description
REQ:	OUT 1-255	OUT X = Removing units stops when the maximum index of 509 is reached on a single DMC8. All new DCS must be on the same DMC8.
DMC8	l s c l	Location of the actual DMC8 to out on an IPE shelf or cabinet.

LD 10 – Convert handset type 500 to DCS

Prompt	Response	Description
REQ	CDCS	Convert Digital Cordless Set – convert from a non-concentrated to a concentrated system after software upgrade. The conversion routine converts the 500 units to DCS units and moves them from the actual TN to a virtual TN.

> ***Note:*** To convert from concentrated to non-concentrated, OUT all DCS units and re-subscribe the handsets.

The CDCS conversion routine prints each TN as it is moved, in the following format:

```
500 TN l s c 00 = DCS TN L S C Index#.
```

where: L S C = virtual TN
Index# = default of the unit number of the 500 type set.

LD 20 – Print actual DMC8 TN and virtual DMC8 TN list

Prompt	Response	Description
REQ	PRT	Request.
TYPE	DCS	Digital Cordless Set.
TN	l s c	Terminal Number for DMC8 card on IPE shelf or Cabinet
	l	Virtual Terminal Number on an IPE shelf or Cabinet
	l s c u	Format for Large System and CS 1000E system, where l = loop, s = shelf, c = card, u = unit
	c u	Format for Small System, CS 1000S system, Media Gateway 1000B, and Media Gateway 1000T, where c = card and u = unit

The print routine outputs the following format:

```
INDX    Index #    VTN lll s cc uu
```

where: Index # = Index number of virtual TN.
lll s cc uu = Virtual TN of unit.

LD 81 – Print DCS features

Prompt	Response	Description
REQ	LST	Request.

LD 81 – Print DCS features

Prompt	Response	Description
FEAT	VSIT	Feature Request - DECT visitors.
HMDN	Xx / <cr>	HoMe Directory Number. Specify a single HMDN or print all HMDN on system.

The LD 81 output format is as follows:

```
DCS  Cust#  Local DN  TN lll s cc uu  HMDN  Home
DN  Last Activity Date.
```

where:

- Cust# = Customer Number
- Local DN = Local Directory Number of user
- lll s cc uu = TN of unit
- Home DN = Home directory number of user
- Last Activity Date = Last date of service change activity for user

LD 83 – Prints DCS terminal numbers with a unit type of DCS instead of 500.

Operating the MSMN feature

To activate the MSMN feature, perform the following steps.

1 Turn the handset on within the coverage range of a visited DECT system.

2 Enter the coverage range of a visited DECT system from another DECT system with the handset turned on.

To deactivate the MSMN feature, perform the following steps.

1 Turn the handset off within coverage range of the visited DECT system. (The handset must have the DECT Detach feature.)

2 Turn the handset on at the home DECT system. (Any CFW related to the handset is cancelled.)

3 Enter the coverage range of the home DECT system with the handset on. (Any CFW related to the handset is cancelled.)

System administration

Contents

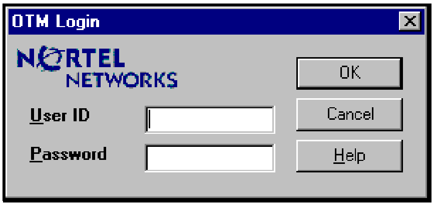
This section contains information on the following topics:

Windows access to the DECT application

For access from a web-based browser, see “Web-based browser access to the DECT application” on page 443.

Logging into the OTM

Figure 217
OTM login dialog box



Complete the following steps.

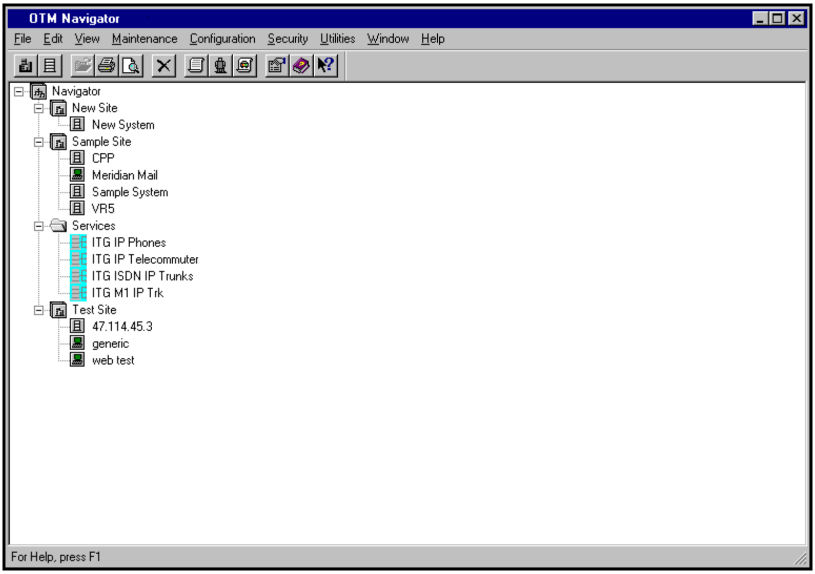
Procedure 97
Login to the OTM

Step	Action
1	Access the OTM Login dialog box.
	Click **Start** on the Windows taskbar and choose **Programs > OTM**.
2	Login.
	Enter **User ID**, **Password**, and click **OK**.

END

Selecting the PBX that supports DECT

Figure 218
OTM Navigator window



Complete the following step.

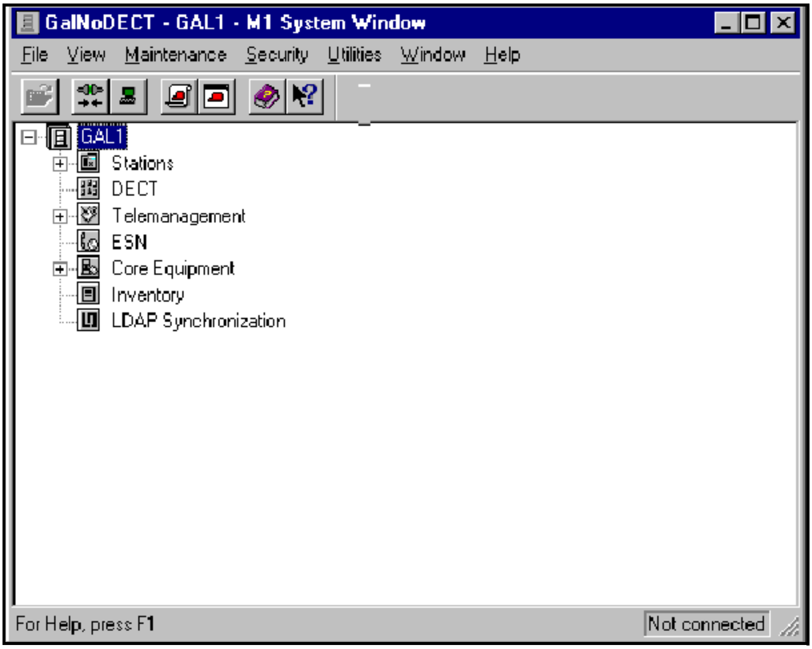
Procedure 98
Selecting the PBX that supports DECT

Step	Action
1	Select the system.
	Double-click on XXX (shown as **Sample System** in Figure 218).

END

Launching the DECT Application

Figure 219
System Window



Complete the following step.

Procedure 99
Launching the DECT application

Step	Action
1	Launch the DECT application.
	Double-click on DECT, or pull-down **File** menu and click DECT.

END

Web-based browser access to the DECT application

For more detailed information on web-based browsers, see *Telephony Manager: System Administration* (553-3001-330).

Opening the Web Administrator Login

Figure 220
Internet Explorer and Netscape Communicator

Complete the following steps.

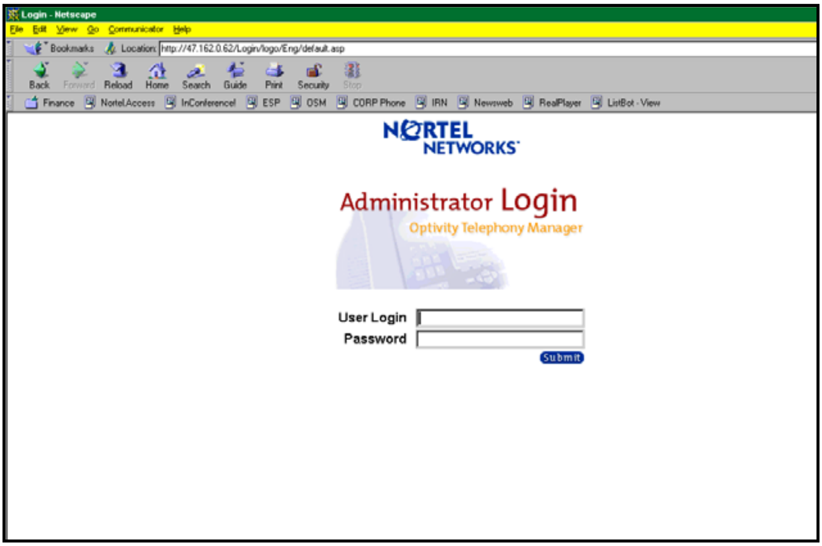
Procedure 100
Opening the Administrator Login

Step	Action
1	Open a Web browser.
	Click on Internet Explorer icon or Netscape Communicator icon.
2	Open the Administrator login screen.
	Enter the URL **http://<**otm_server_name**>/admin** or use the **ip_ address**.

END

Web Administrator Login

Figure 221
OTM web Administrator Login


Login - Netscape
File Edit View Go Communicator Help
Bookmarks Location: http://47.162.0.62/Login/logo/Eng/default.asp
Back Forward Reload Home Search Guide Print Security Stop
Finance NortelAccess InConference! ESP OSM CORP Phone IRN Newsweb RealPlayer ListBot - View
NORTEL NETWORKS
Administrator Login
Optivity Telephony Manager
User Login
Password
Submit

Complete the following steps.

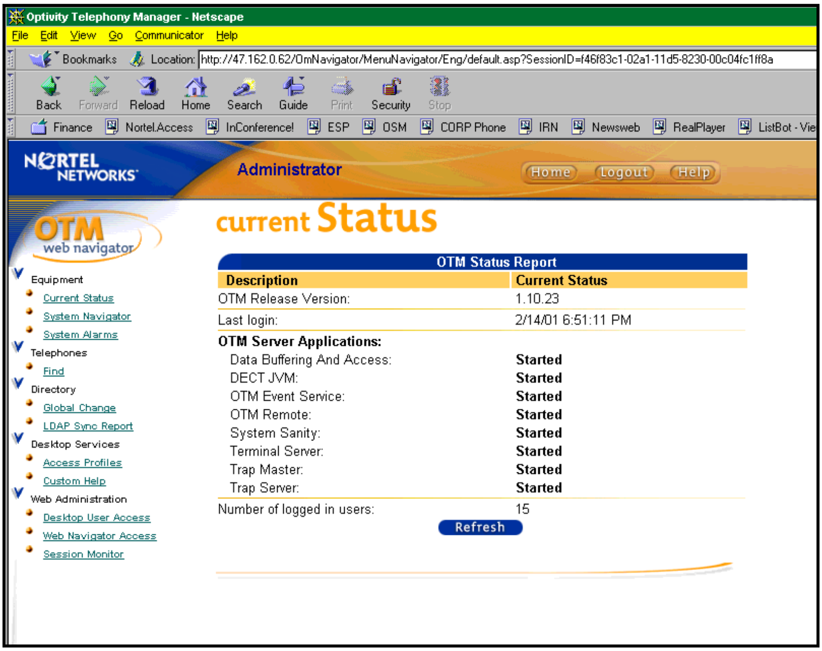
Procedure 101
Opening the OTM web Administrator Login

Step	Action
1	Select the Administrator Login.
	Click on the applet launch logo.
2	Login.
	Enter **User Login**, **Password**, and click **Submit**.

END

Opening the Web current Status

Figure 222
OTM web navigator current Status


Optivity Telephony Manager - Netscape
File Edit View Go Communicator Help
Bookmarks Location: http://47.162.0.62/OmNavigator/MenuNavigator/Eng/default.asp?SessionID=f46f83c1-02a1-11d5-8230-00c04fc1ff8a
Back Forward Reload Home Search Guide Print Security Stop
Finance Nortel.Access InConference! ESP OSM CORP Phone IRN Newsweb RealPlayer ListBot - Vie
NORTEL NETWORKS
Administrator
Home Logout Help
OTM web navigator
Equipment
Current Status
System Navigator
System Alarms
Telephones
Find
Directory
Global Change
LDAP Sync Report
Desktop Services
Access Profiles
Custom Help
Web Administration
Desktop User Access
Web Navigator Access
Session Monitor
current Status
Refresh

OTM Status Report

Description	Current Status
OTM Release Version:	1.10.23
Last login:	2/14/01 6:51:11 PM
OTM Server Applications:	
Data Buffering And Access:	**Started**
DECT JVM:	**Started**
OTM Event Service:	**Started**
OTM Remote:	**Started**
System Sanity:	**Started**
Terminal Server:	**Started**
Trap Master:	**Started**
Trap Server:	**Started**
Number of logged in users:	15

Complete the following step.

Procedure 102
Opening the current Status

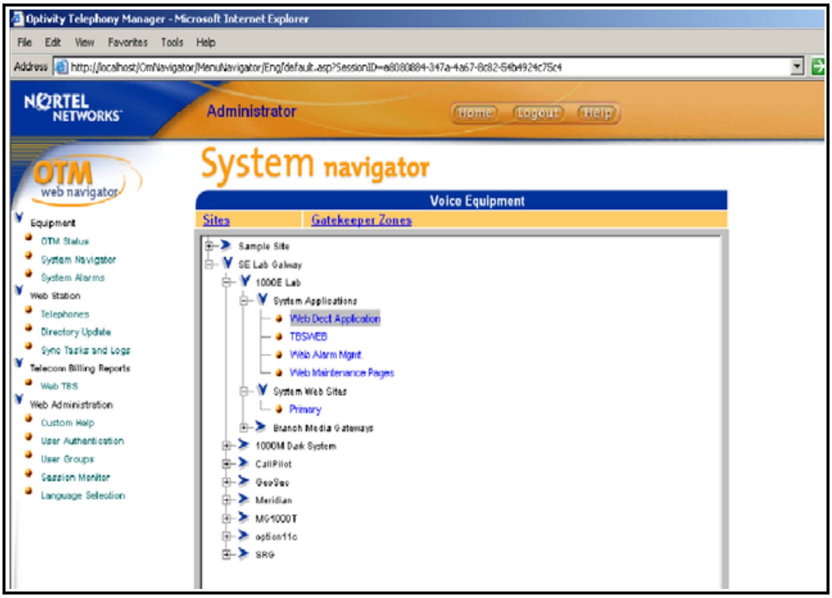
Step	Action
1	Open System Navigator screen.
	Click on **System Navigator** in the **Equipment** list on the left.

END

Opening the web System navigator

The System navigator is selected by clicking on **System Navigator** in the list on the left of the screen shown in Figure 222 on page 445.

Figure 223
OTM web System navigator



Complete the following steps.

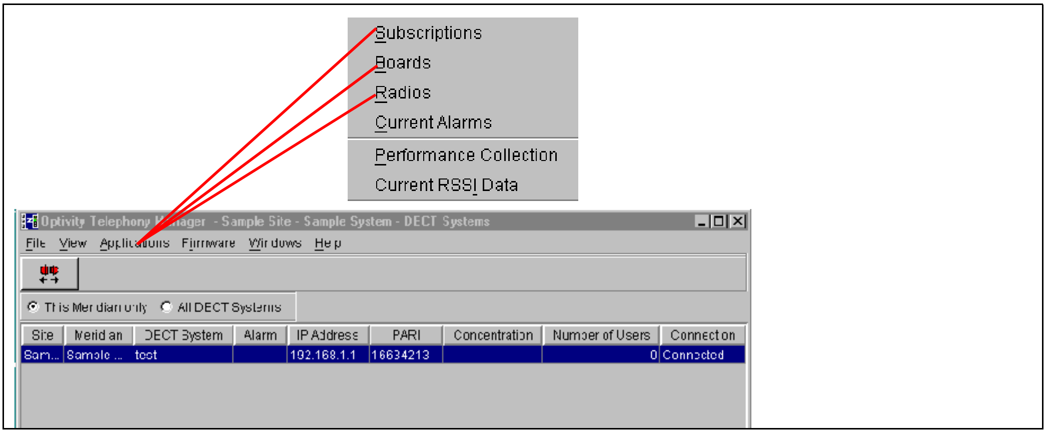
Procedure 103
Opening the web System navigator

Step	Action
1	Select a DECT system.
	Highlight a system in the **Systems** list.
2	Open the DECT systems window.
	Click on **OTM DECT** in the grey box on the left.

END

DECT Systems window

Figure 224
DECT Systems window



Subscriptions
Boards
Radios
Current Alarms
Performance Collection
Current RSSI Data
Optivity Telephony Manager - Sample Site - Sample System - DECT Systems
File View Applications Firmware Windows Help
● This Meridian only ○ All DECT Systems

Site	Meridian	DECT System	Alarm	IP Address	PARI	Concentration	Number of Users	Connection
Sam...	Sample ...	test		192.168.1.1	16634213		0	Connected

Opening Subscriptions, Boards, and RFP windows

Procedure 104
Opening Subscriptions, Boards, and RFP windows

Step	Action
1	Select a DECT system.
	Highlight a system from the list.
2	Open one of the following from the DECT Systems window: • Subscriptions window • Boards (DMC) window • Radios (basestation) window
	Click on the appropriate entry in the **Applications** pull-down menu.

END

Connecting to a DECT system

Complete the following steps.

Procedure 105
Connecting to a DECT system

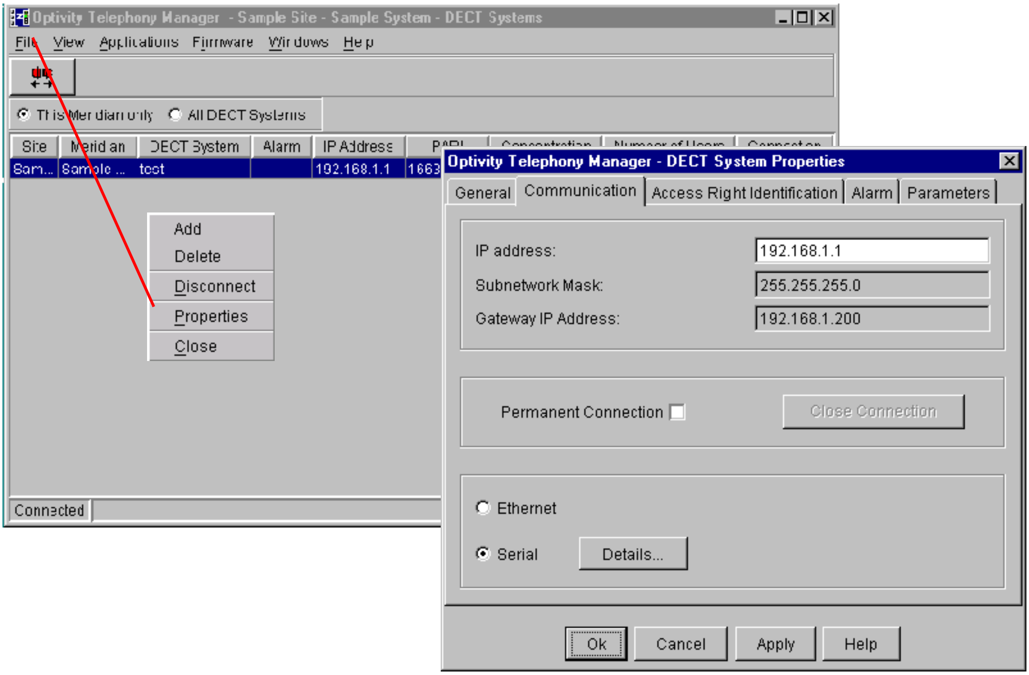
Step	Action
1	Select a DECT system from the DECT Systems window list.
	Highlight a DECT system.
2	Perform one of the following actions from the DECT Systems window: **1** connect to a DECT system **2** disconnect from a DECT system **3** lock a connection to a DECT system **4** unlock a connection from a DECT system
	From the **Applications** pull-down menu click on the following items, or click on the following icon: **1** **Connect** or 🟩 (green) **2** **Disconnect** or 🟨 (yellow) **3** **Lock** or 🟥 (red) **4** **Unlock** or 🟨 (yellow)

END

Note: While the Connection status is **Connecting** or **Disconnecting**, the Connect/Disconnect tool is disabled. The status bar shows the connection progress.

Establishing a permanent connection to a DECT system

Figure 225
DECT Systems window and DECT System Properties window



Optivity Telephony Manager - Sample Site - Sample System - DECT Systems
File View Applications Firmware Windows Help
Add
Delete
Disconnect
Properties
Close
Optivity Telephony Manager - DECT System Properties
General
Communication
Access Right Identification
Alarm
Parameters
Close Connection
Details...
Ok
Cancel
Apply
Help

● This Meridian only ○ All DECT Systems

Site	Meridian	DECT System	Alarm	IP Address	PARI	Concentration	Number of Users	Connection
Sam...	Sample ...	test		192.168.1.1	1663			

Connected

IP address: 192.168.1.1

Subnetwork Mask: 255.255.255.0

Gateway IP Address: 192.168.1.200

Permanent Connection ☐

○ Ethernet

● Serial

Complete the following steps.

Procedure 106
Establishing a permanent connection to a DECT System

Step	Action
1	Select a DECT system from the DECT Systems window list.
	Highlight a DECT system.
2	Connect to a DECT system.
	From the **Applications** pull-down menu, click on **Connect** or click on the (green) icon.
3	Open the Properties dialog.
	From the **File** pull-down menu, click on **Properties**.
4	Select Permanent Connection.
	Check the **Permanent Connection** box.
5	Accept the changes.
	Click on the **OK** button.

END

Adding DECT systems

Adding a DECT system involves:

1 “Adding new site properties” on page 452

2 “Adding the system on the OTM server” on page 454

3 “Adding properties – General tab” on page 455

4 “Adding a Communications Profile for DECT application” on page 456

5 “Adding the System Data Properties” on page 458

6 “Adding the System Applications Properties” on page 460

7 “Adding the Customer Properties” on page 462

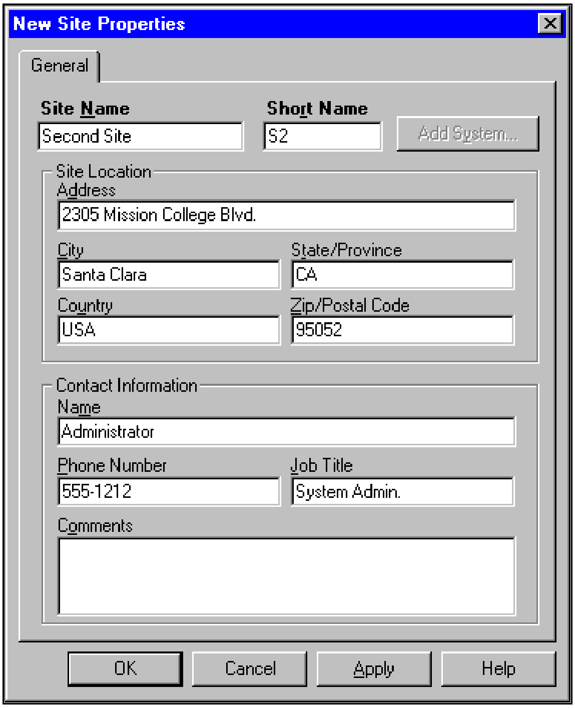
8 "Adding the Customer0 General Properties" on page 464

9 "Adding the Customer0 Features Properties" on page 466

10 "Adding the Customer0 Numbering Plans Properties" on page 468

Adding new site properties

Figure 226
New Site Properties



New Site Properties

General

Site Name: Second Site

Short Name: S2

Site Location

Address: 2305 Mission College Blvd.

City: Santa Clara

State/Province: CA

Country: USA

Zip/Postal Code: 95052

Contact Information

Name: Administrator

Phone Number: 555-1212

Job Title: System Admin.

Comments:

Complete the following steps.

Procedure 107
Adding new site properties

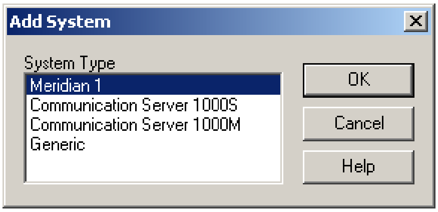
Step	Action
1	Open the New Site Properties window.
	In the OTM Windows Navigator, choose **Add Site** from the **Configuration** menu.
2	The **Site Name** appears in the Navigator tree. The Short Name is an abbreviated site name that displays in the Alarm Banner.
	Enter the **Site Name** and **Short Name**. **Note:** Bold fields in the dialog sheets indicate required information.
3	In the **Site Location** box.
	Enter the **Site Location** information.
4	In the **Contact Information** box.
	Enter the contact name and related information, and click **Apply**.
5	To add a new system to this site.
	Click **Add System**.
6	When the Site information is entered, click one of the following buttons to add the site to the Navigator tree.
	OK adds the site and closes the property sheet. **Apply** adds the site and leaves the property sheet open allowing another system to be added to this site (repeat step 5 to add another system). **Cancel** closes the dialog box without adding the site.

END

Adding the system on the OTM server

As many systems (including non-Nortel systems) as the licence permits can be added to a site. Administrator privileges are required to add a system.

Figure 227
Add System



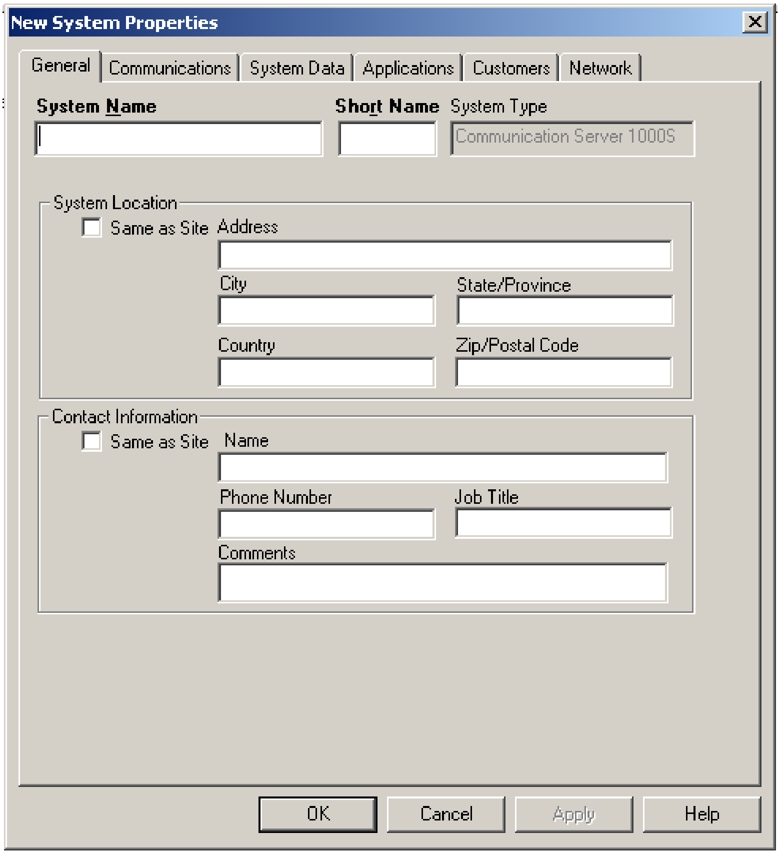
Complete the following steps.

Procedure 108
Adding the PBX on the OTM server

Step	Action
1	In the Navigator window, select the site.
	If adding a new system from within the New Site Properties window, go to step 3 in this procedure.
2	Open the Add System dialog.
	Choose **Add System** from the **Configuration** menu, or right-click and choose it from the button pop-up menu.
3	Program the Add System dialog box.
	It is sometimes necessary to install additional software to enable other system types not listed here. Follow the installation instructions included with the order. • Select the system type, and then click **OK**.
	END

Adding properties – General tab

Figure 228
New System Properties – General tab



System Type: Communication Server 1000S

Complete the following steps.

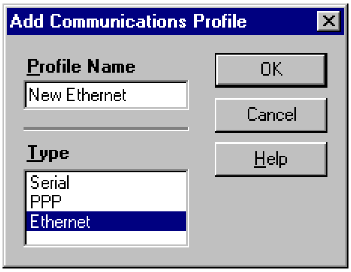
Procedure 109
Adding the properties – General

Step	Action
1	Select the **General** tab.
	Click the **System Properties – General tab**.
2	Program the **System Name** and **Short Name** (required fields), and other information as needed.
	Enter the **System Name** and **Short Name**.
3	**System Location** and **Contact Information** can be the same as site information.
	Click the **Same as Site** checkbox.
4	Accept changes.
	Click the **OK** button.

END

Adding a Communications Profile for DECT application

Figure 229
Add Communications Profile



Add Communications Profile

Profile Name: New Ethernet

Type: Serial, PPP, Ethernet (selected: Ethernet)

Complete the following steps.

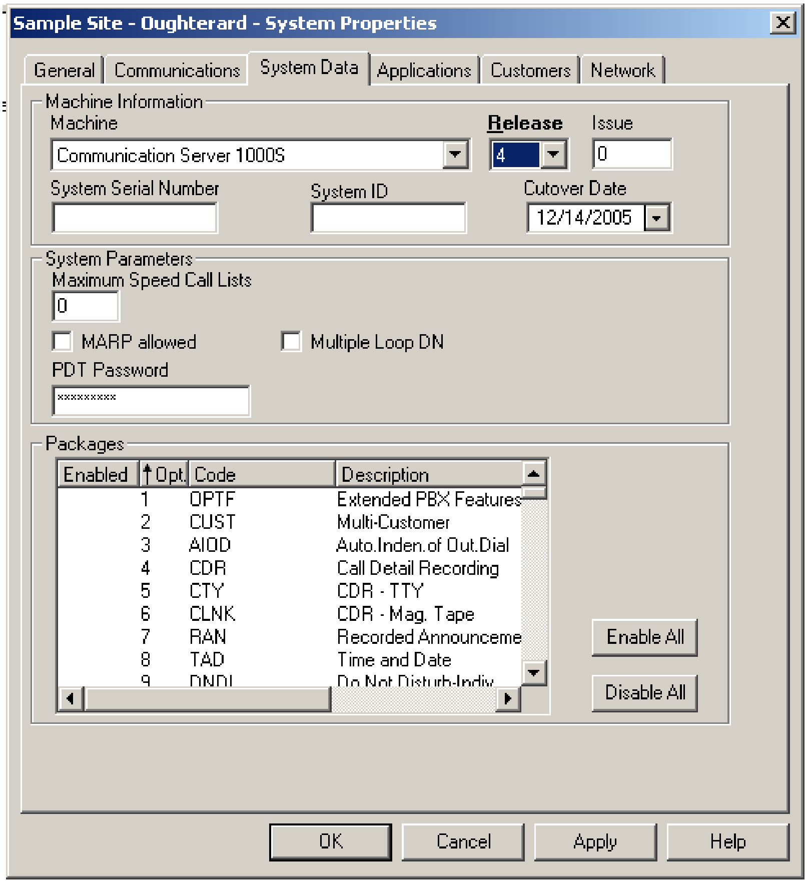
Procedure 110
Adding a new Communications Profile

Step	Action
1	In the Navigator window, select the Sample Site.
	Double-click on **Sample Site**.
2	Choose the Properties dialog.
	Click on **Properties** from the **File** menu.
3	Open the **Add Communications Profile** dialog.
	Click on the **Communications** tab and click **Add**.
4	Select a communication type.
	Highlight **Ethernet** in the **Type** box. ***Note:*** The DECT application does not use the Communications Profile. Unless there is another application that requires a specific Communications Profile, choosing Ethernet is the least complicated profile to implement.
5	Program the Profile Name.
	Enter a **Profile Name**.
6	Accept the changes.
	Click **OK**.

END

Adding the System Data Properties

Figure 230
System Properties – System Data tab



Sample Site - Oughterard - System Properties

Machine Information

Machine: Communication Server 1000S

Release: 4

Issue: 0

System Serial Number:

System ID:

Cutover Date: 12/14/2005

System Parameters

Maximum Speed Call Lists: 0

□ MARP allowed

□ Multiple Loop DN

PDT Password: *********

Packages

Enabled	Opt.	Code	Description
	1	OPTF	Extended PBX Features
	2	CUST	Multi-Customer
	3	AIOD	Auto.Inden.of Out.Dial
	4	CDR	Call Detail Recording
	5	CTY	CDR - TTY
	6	CLNK	CDR - Mag. Tape
	7	RAN	Recorded Announceme
	8	TAD	Time and Date
	9	DNDI	Do Not Disturb-Indiv.

Complete the following steps.

Procedure 111
Adding the System Data Properties

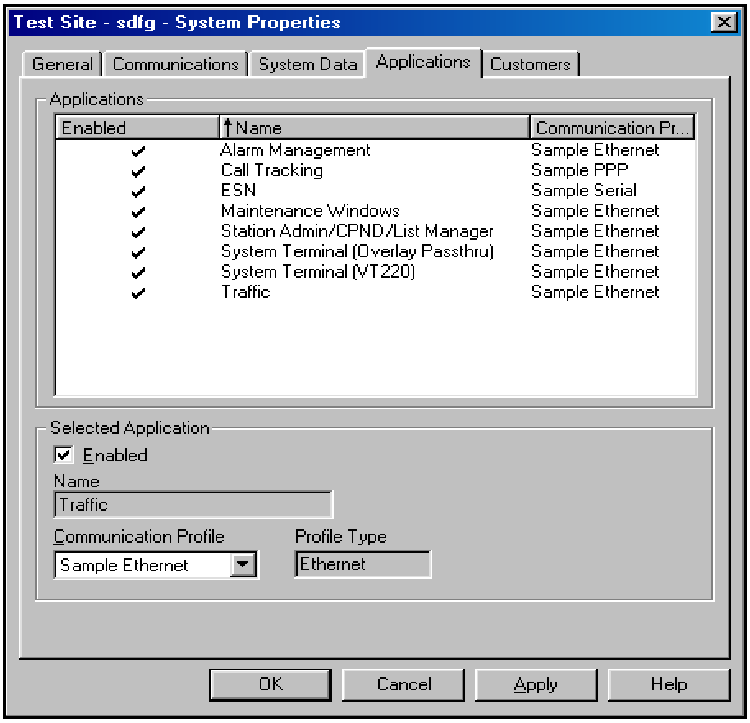
Step	Action
1	Select the System Data tab.
	Click the **System Properties – System Data** tab.
2	Program the Machine Information.
	Enter the **Machine** type and **Release** version for the system. ***Note:*** For example, for a Meridian 1 PBX 61C running Release 25 software, enter **61C** in the Machine field and use the drop down box to select **25** for Release.
3	Program the System Parameters.
	Enter the appropriate values for the system.
4	Program Packages.
	Enable or disable M1 packages as appropriate for the system.
5	***Note:*** This data can be copied directly from an installed switch by scheduling an upload with the **File** menu **Update System Data** command in the System window. **Update System Data** uses the communication profile for Station Administration. However, configure the Release number here first to allow available applications to appear properly in the Applications Tab.

END

Adding the System Applications Properties

This tab defines the OTM applications that appear in the System window and the Communications Profile to be used with each application. An application must be enabled for it to be available in the System window.

Figure 231
System Properties – Applications



Enabled	Name	Communication Pr...
✓	Alarm Management	Sample Ethernet
✓	Call Tracking	Sample PPP
✓	ESN	Sample Serial
✓	Maintenance Windows	Sample Ethernet
✓	Station Admin/CPND/List Manager	Sample Ethernet
✓	System Terminal (Overlay Passthru)	Sample Ethernet
✓	System Terminal (VT220)	Sample Ethernet
✓	Traffic	Sample Ethernet

Selected Application

☑ Enabled

Name: Traffic

Communication Profile: Sample Ethernet

Profile Type: Ethernet

Complete the following steps.

Procedure 112
Adding the System Applications Properties

Step	Action
1	Select the system **Applications** tab.
	Click the **System Properties – Applications Data** tab.
2	To enable an application.
	• Select the application in the **Applications** box. • Select a **Communications Profile** from the drop-down list in the **Selected Application** box. • A checkmark appears next to the application and the **Enabled** box is also checked.
3	To disable an application.
	• Select the application in the **Applications** box. • In the **Selected Application** box, click the **Enabled** checkbox to remove the checkmark.

END

Adding the Customer Properties

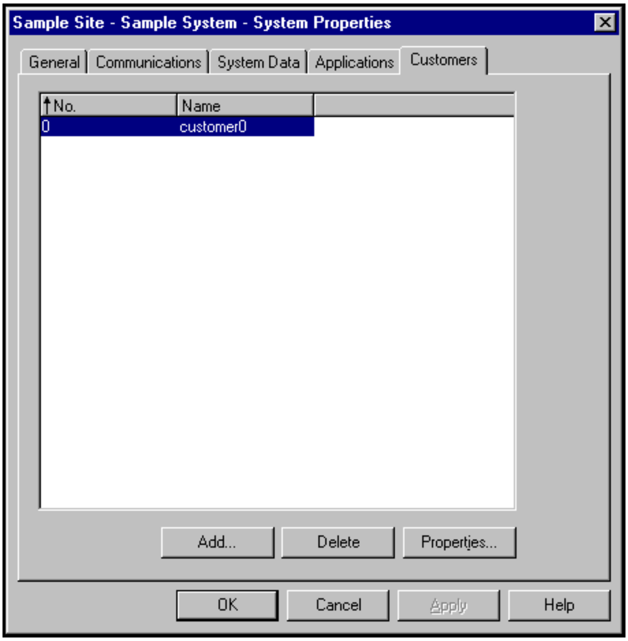
This tab lists the customers currently defined for this system. The following action can be performed:

- add new customers
- delete customers
- review the properties of a selected customer

When a new customer is added, configure the features and numbering plans that are available to the customer. This information is not automatically updated. It must be updated by using LD 15 Customer Data Block.

> ***Note:*** Customer information is required for System Administration/ CPND and ESN applications.

Figure 232
System Properties – Customers



Sample Site - Sample System - System Properties

No.	Name
0	customer0

Complete the following steps.

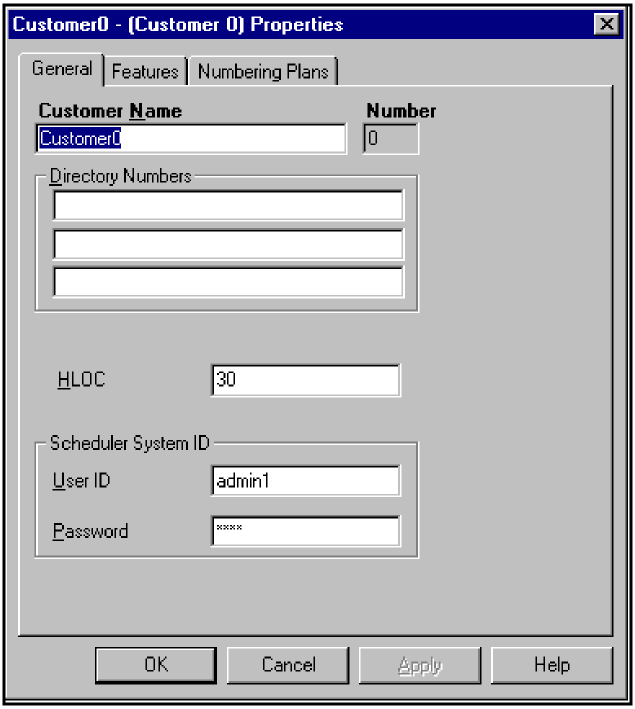
Procedure 113
Adding the customer properties

Step	Action
1	Select the system Customers tab.
	Click the **System Properties – Customers Data** tab.
2	Select a customer number.
	Click **OK**.
3	Update the PBX.
	Use LD 15 Customer Data Block.

END

Adding the Customer0 General Properties

Figure 233
Customer0 Properties – General



Customer0 - (Customer 0) Properties

Customer Name: Customer0

Number: 0

Directory Numbers

HLOC: 30

Scheduler System ID

User ID: admin1

Password: ****

Complete the following steps.

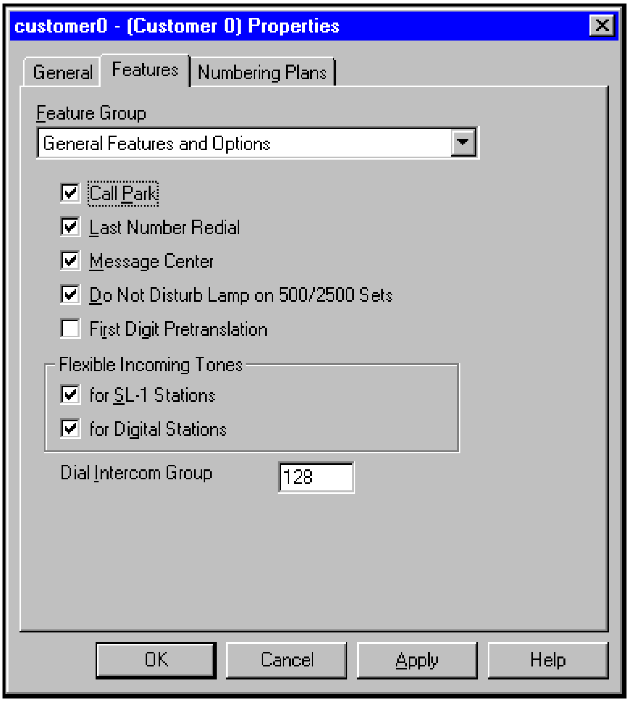
Procedure 114
Adding the Customer0 General Properties

Step	Action
1	Select the General tab.
	Click the **General** tab.
2	Program the Customer Name and Number.
	Enter the **Customer Name** and **Number**.
3	Program the Home Location Code.
	Enter the HLOC as defined in LD 90.
4	Program the **Scheduler System ID**, if using applications with scheduled activities, such as Station Administration/CPND, ESN, and Traffic.
5	Accept changes.
	Click **Apply**.

END

Adding the Customer0 Features Properties

Figure 234
Customer 0 Properties – Features



customer0 - (Customer 0) Properties

Feature Group: General Features and Options

☑ Call Park
☑ Last Number Redial
☑ Message Center
☑ Do Not Disturb Lamp on 500/2500 Sets
☐ First Digit Pretranslation

Flexible Incoming Tones
☑ for SL-1 Stations
☑ for Digital Stations

Dial Intercom Group: 128

Complete the following steps.

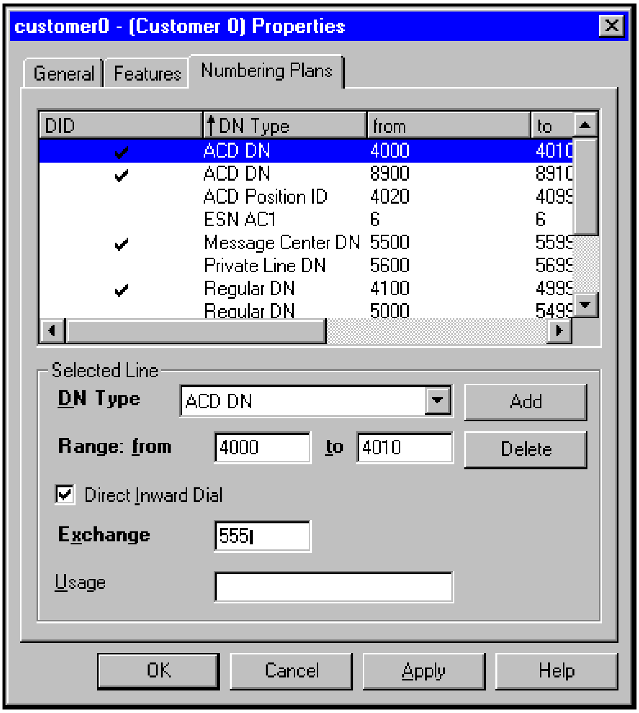
Procedure 115
Adding the Customer0 Features Properties

Step	Action
1	Select the **Features** tab.
	Click the **Features** tab.
2	Program Features Group.
3	Accept changes.
	Click **Apply**.

END

Adding the Customer0 Numbering Plans Properties

Figure 235
Customer Properties – Numbering Plans



DID	DN Type	from	to
✓	ACD DN	4000	4010
✓	ACD DN	8900	8910
	ACD Position ID	4020	4099
	ESN AC1	6	6
✓	Message Center DN	5500	5599
	Private Line DN	5600	5699
✓	Regular DN	4100	4999
	Regular DN	5000	5499

Selected Line

DN Type: ACD DN

Range: from 4000 to 4010

☑ Direct Inward Dial

Exchange: 555

Usage:

Complete the following steps.

Procedure 116
Adding the Customer0 Numbering Plans Properties

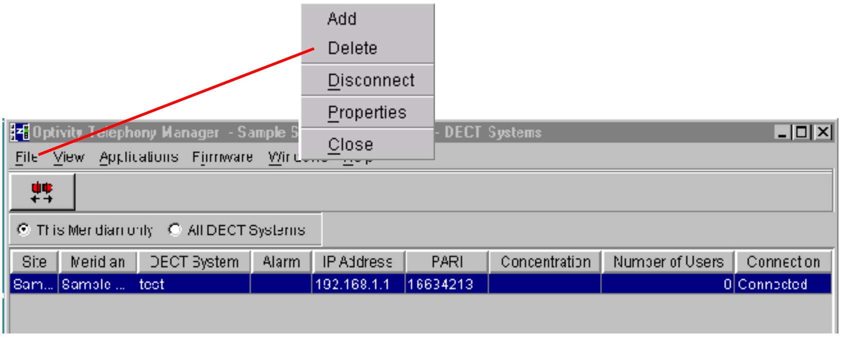
Step	Action
1	Select the **Numbering Plans** tab.
	Click the **Numbering Plans** tab.
2	Program the customer information appropriate for the PBX.
3	Accept changes.
	Click one of the following buttons to save the information: • **OK** adds the customer and returns to the System properties sheet. • **Apply** adds the customer and leaves the Customer properties open so that other information can be added for this customer. • **Cancel** closes the dialog box without adding the customer.

END

Note: At this point the DECT application is installed in the OTM server.

Deleting DECT systems

Figure 236
DECT Systems window



● This Meridian only ○ All DECT Systems

Site	Meridian	DECT System	Alarm	IP Address	PARI	Concentration	Number of Users	Connection
Sam...	Sample ...	test		192.168.1.1	16634213		0	Connected

Complete the following steps.

Procedure 117
Deleting DECT systems

Step	Action
1	Using Windows, log in to OTM. Select the system that supports DECT. Launch the DECT application. Open the DECT Systems window.
	Follow the instructions on page 440 to page 442.
2	Using a web-based navigator, open the Administrator login screen and login. Select the System Navigator. Select the system that supports DECT. Launch the DECT application. Open the DECT Systems window.
	Follow the instructions on page 443 to page 446.
3	Select a DECT system to delete.
	Highlight a DECT system from the list.
4	Delete the DECT system.
	From the **File** pull-down menu, click on **Delete**.

END

Configuring non-concentrated DECT handsets

Configuring non-concentrated DECT handsets involves:

1. “Accessing the Add Station window” on page 473
2. “Adding 500 analogue standard” on page 474
3. “Accessing features” on page 475
4. “Accessing wireless type” on page 476
5. “Selecting wireless type” on page 477
6. “Selecting DECT wireless set” on page 477
7. “Accepting changes” on page 478

If you are using the web-based TM 3.0 to configure DECT handsets, refer to *Telephony Manager: System Administration* (553-3001-330).

Opening Station Administration window

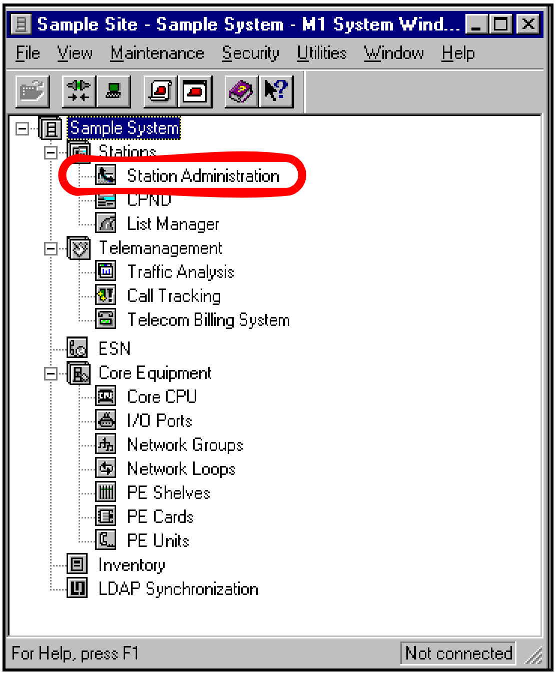


Figure 237
M1 System Window

Complete the following step.

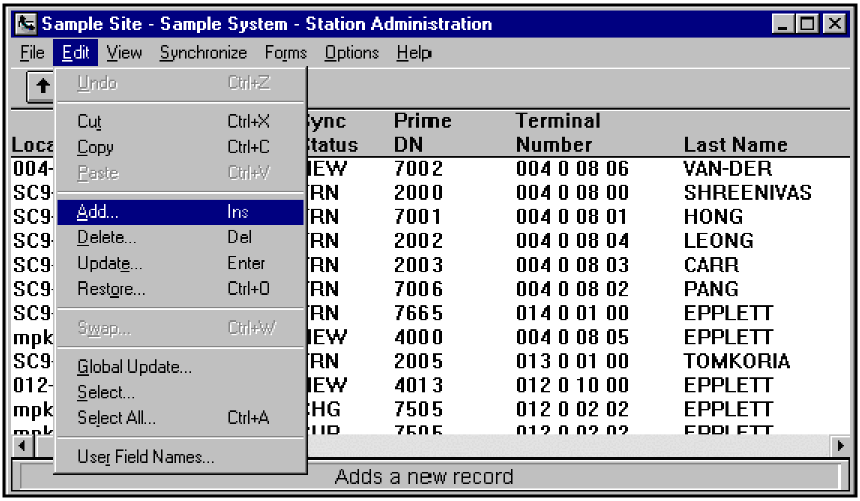
Procedure 118
Opening the Station Administration window

Step	Action
1	Open the Station Administration window.
	Click on **Station Administration** in the M1 System Window.

END

Accessing the Add Station window

Figure 238
Station Administration window



Loca	ync tatus	Prime DN	Terminal Number	Last Name
004-	IEW	7002	004 0 08 06	VAN-DER
SC9	RN	2000	004 0 08 00	SHREENIVAS
SC9	RN	7001	004 0 08 01	HONG
SC9	RN	2002	004 0 08 04	LEONG
SC9	RN	2003	004 0 08 03	CARR
SC9	RN	7006	004 0 08 02	PANG
SC9	RN	7665	014 0 01 00	EPPLETT
mpk	IEW	4000	004 0 08 05	EPPLETT
SC9	RN	2005	013 0 01 00	TOMKORIA
012-	IEW	4013	012 0 10 00	EPPLETT
mpk	HG	7505	012 0 02 02	EPPLETT

Adds a new record

Complete the following steps.

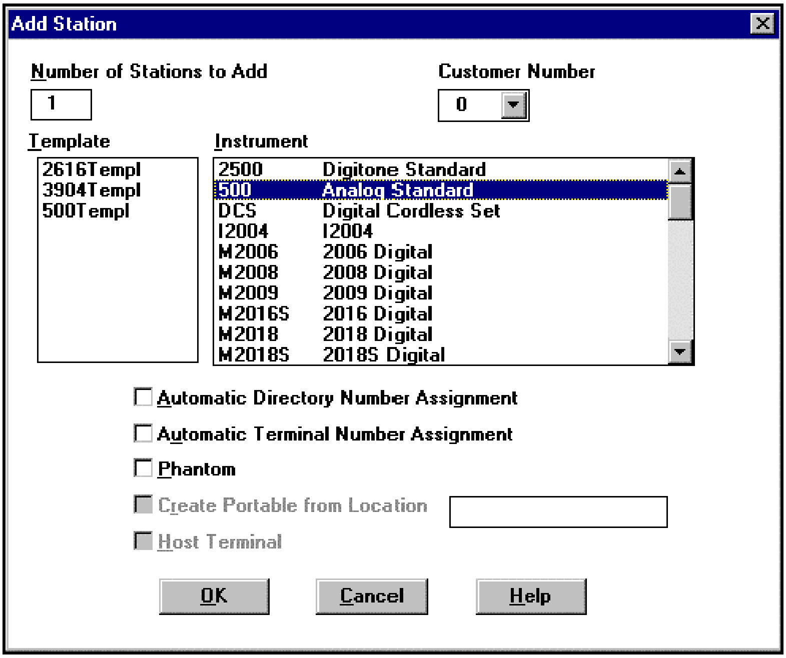
Procedure 119
Accessing Add Station window

Step	Action
1	Access Add Station window.
	From the **Edit** pull-down menu, click on **Add**.

END

Adding 500 analogue standard

Figure 239
Add Station window



Add Station

Number of Stations to Add: 1

Customer Number: 0

Template:
- 2616Templ
- 3904Templ
- 500Templ

Instrument:

2500	Digitone Standard
500	Analog Standard
DCS	Digital Cordless Set
I2004	I2004
M2006	2006 Digital
M2008	2008 Digital
M2009	2009 Digital
M2016S	2016 Digital
M2018	2018 Digital
M2018S	2018S Digital

□ Automatic Directory Number Assignment
□ Automatic Terminal Number Assignment
□ Phantom
□ Create Portable from Location
□ Host Terminal

Complete the following step.

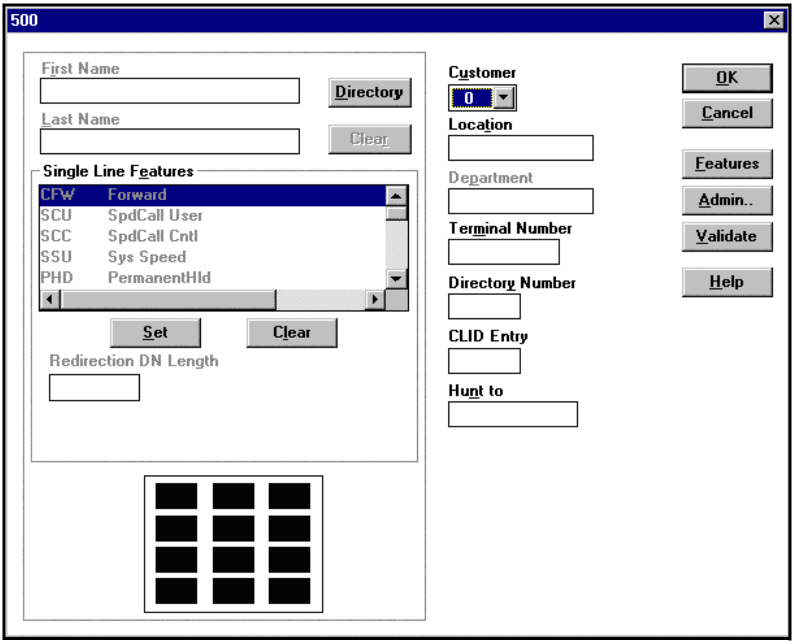
Procedure 120
Adding 500 analogue standard

Step	Action
1	Add 500 analogue standard.
	Highlight **500 Analogue Standard**, and click on the **OK** button.

END

Accessing features

Figure 240
500 dialog



Customer: 0

Single Line Features:

CFW	Forward
SCU	SpdCall User
SCC	SpdCall Cntl
SSU	Sys Speed
PHD	PermanentHld

Complete the following step.

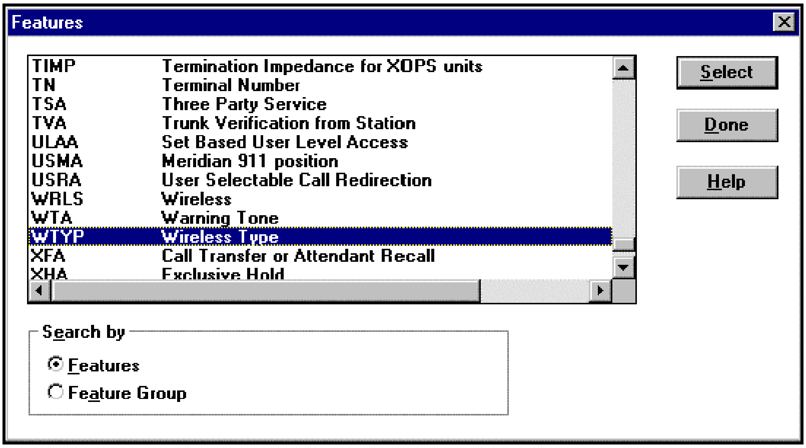
Procedure 121
Accessing features

Step	Action
1	Access features.
	Click on the **Features** button.

END

Accessing wireless type

Figure 241
Features window



TIMP	Termination Impedance for XOPS units
TN	Terminal Number
TSA	Three Party Service
TVA	Trunk Verification from Station
ULAA	Set Based User Level Access
USMA	Meridian 911 position
USRA	User Selectable Call Redirection
WRLS	Wireless
WTA	Warning Tone
WTYP	Wireless Type
XFA	Call Transfer or Attendant Recall
XHA	Exclusive Hold

Search by
● Features
○ Feature Group

Complete the following step.

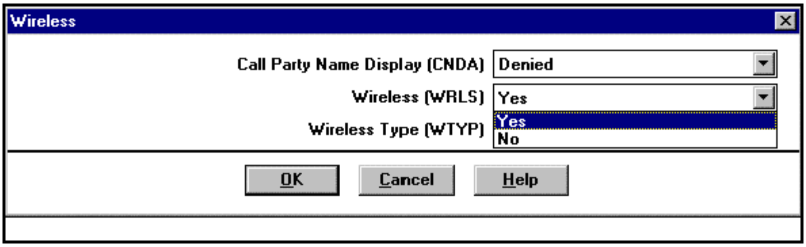
Procedure 122
Accessing wireless type

Step	Action
1	Access wireless type.
	Highlight **Wireless Type**, and click on the **Select** button.

END

Selecting wireless type

Figure 242
Wireless window



Call Party Name Display (CNDA) Denied
Wireless (WRLS) Yes
Wireless Type (WTYP)

Complete the following step.

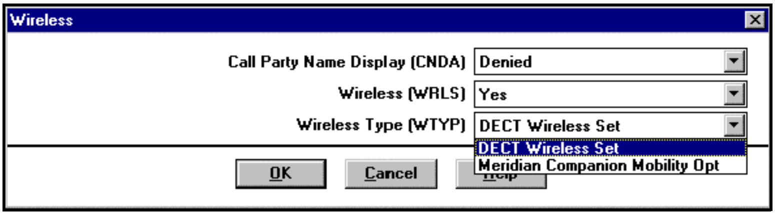
Procedure 123
Selecting wireless type

Step	Action
1	Select wireless type.
	From the **Wireless (WRLS)** pull-down menu, click on **YES**.

END

Selecting DECT wireless set

Figure 243
Wireless window



Call Party Name Display (CNDA) Denied
Wireless (WRLS) Yes
Wireless Type (WTYP) DECT Wireless Set

Complete the following step.

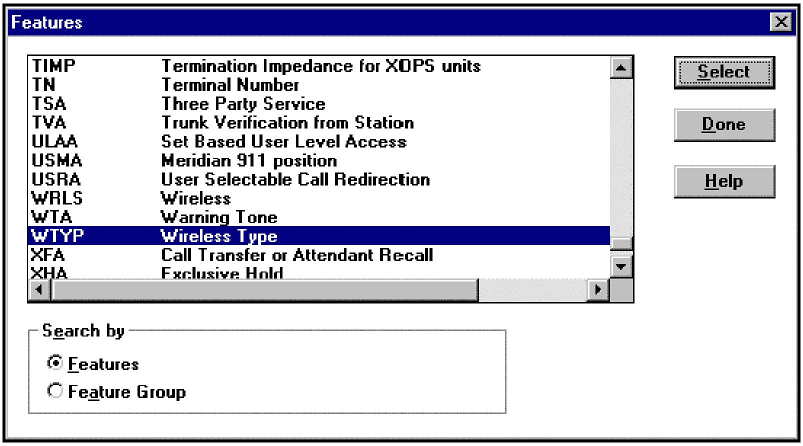
Procedure 124
Selecting DECT wireless set

Step	Action
1	Select a DECT handset.
	From the **Wireless Type (WTYP)** pull-down menu, click on **DECT Wireless Set**, and click on the **OK** button.

END

Accepting changes

Figure 244
Features window



TIMP	Termination Impedance for XOPS units
TN	Terminal Number
TSA	Three Party Service
TVA	Trunk Verification from Station
ULAA	Set Based User Level Access
USMA	Meridian 911 position
USRA	User Selectable Call Redirection
WRLS	Wireless
WTA	Warning Tone
WTYP	Wireless Type
XFA	Call Transfer or Attendant Recall
XHA	Exclusive Hold

Search by
● Features
○ Feature Group

Complete the following step.

Procedure 125
Accepting changes

Step	Action
1	Accept changes.
	Click on the **Done** button.

END

Configuring concentrated DECT handsets on a PBX

If you are using the web-based TM 3.0 to configure DECT handsets, refer to *Telephony Manager: System Administration* (553-3001-330).

Configuring concentrated DECT handsets involves:

1 “Opening the Station Administration window” on page 480

2 “Accessing the Add Station window” on page 481

3 “Selecting Digital Cordless Set” on page 482

4 “Selecting features” on page 483

5 “Selecting wireless type” on page 484

6 “Selecting Visit DECT Set or local calling” on page 485

7 “Selecting an index” on page 486

8 “Provisioning the hardware” on page 487

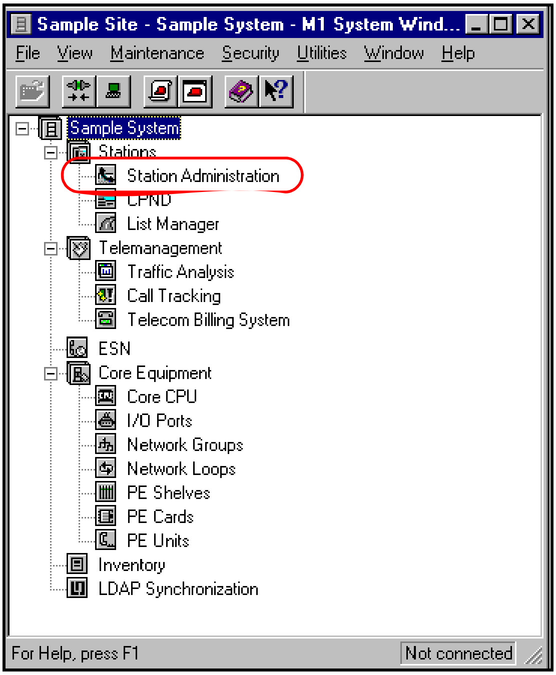
9 “Accepting changes” on page 488

10 “Single line features” on page 489

11 “Opening the Station Administration window” on page 480

Opening the Station Administration window

Figure 245
M1 System Window



Complete the following step.

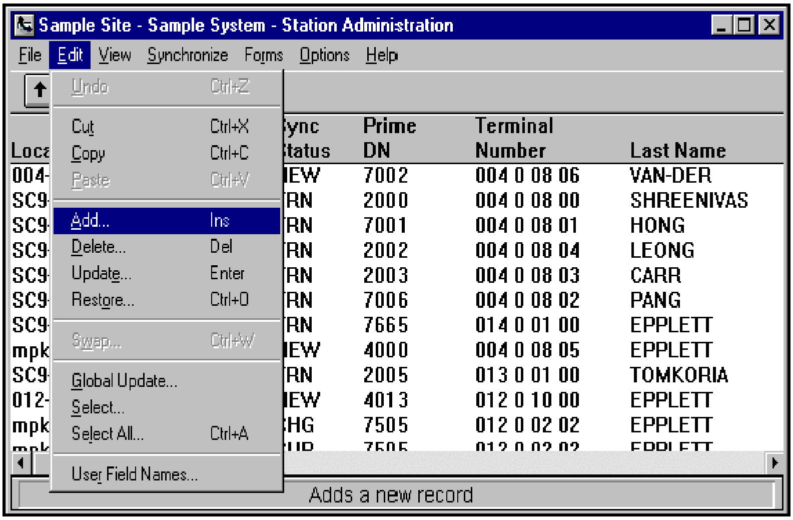
Procedure 126
Opening the Station Administration window

Step	Action
1	Open the Station Administration window.
	Click on **Station Administration** in the System Window.

END

Accessing the Add Station window

Figure 246
Station Administration window



Sample Site - Sample System - Station Administration

Loca	ync tatus	Prime DN	Terminal Number	Last Name
004-	IEW	7002	004 0 08 06	VAN-DER
SC9	RN	2000	004 0 08 00	SHREENIVAS
SC9	RN	7001	004 0 08 01	HONG
SC9	RN	2002	004 0 08 04	LEONG
SC9	RN	2003	004 0 08 03	CARR
SC9	RN	7006	004 0 08 02	PANG
SC9	RN	7665	014 0 01 00	EPPLETT
mpk	IEW	4000	004 0 08 05	EPPLETT
SC9	RN	2005	013 0 01 00	TOMKORIA
012-	IEW	4013	012 0 10 00	EPPLETT
mpk	HG	7505	012 0 02 02	EPPLETT

Adds a new record

Complete the following step.

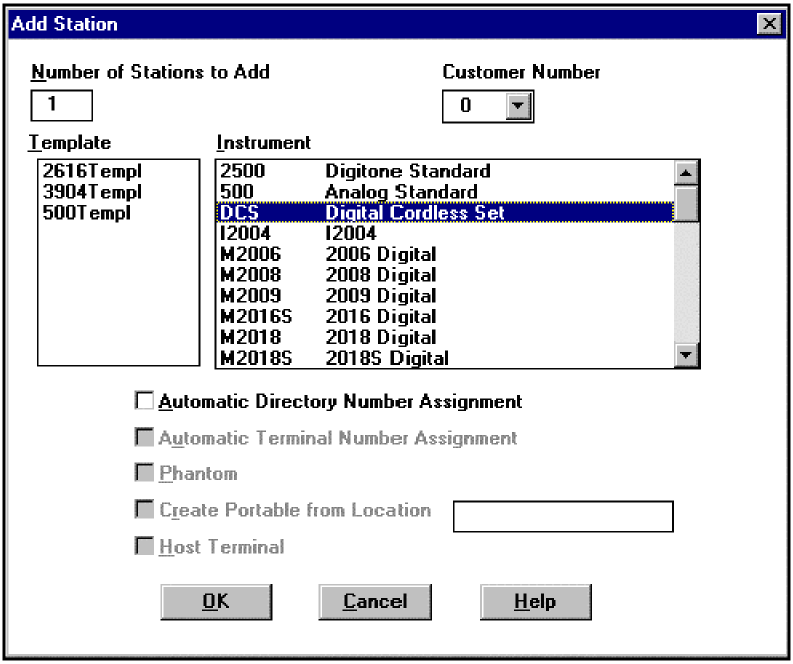
Procedure 127
Accessing Add Station window

Step	Action
1	Access Add Station dialog.
	From the **Edit** pull-down menu, click on **Add**.

END

Selecting Digital Cordless Set

Figure 247
Add Station dialog



Number of Stations to Add: 1

Customer Number: 0

Template
2616Templ
3904Templ
500Templ

Instrument	
2500	Digitone Standard
500	Analog Standard
DCS	Digital Cordless Set
I2004	I2004
M2006	2006 Digital
M2008	2008 Digital
M2009	2009 Digital
M2016S	2016 Digital
M2018	2018 Digital
M2018S	2018S Digital

☐ Automatic Directory Number Assignment

☐ Automatic Terminal Number Assignment

☐ Phantom

☐ Create Portable from Location

☐ Host Terminal

Complete the following step.

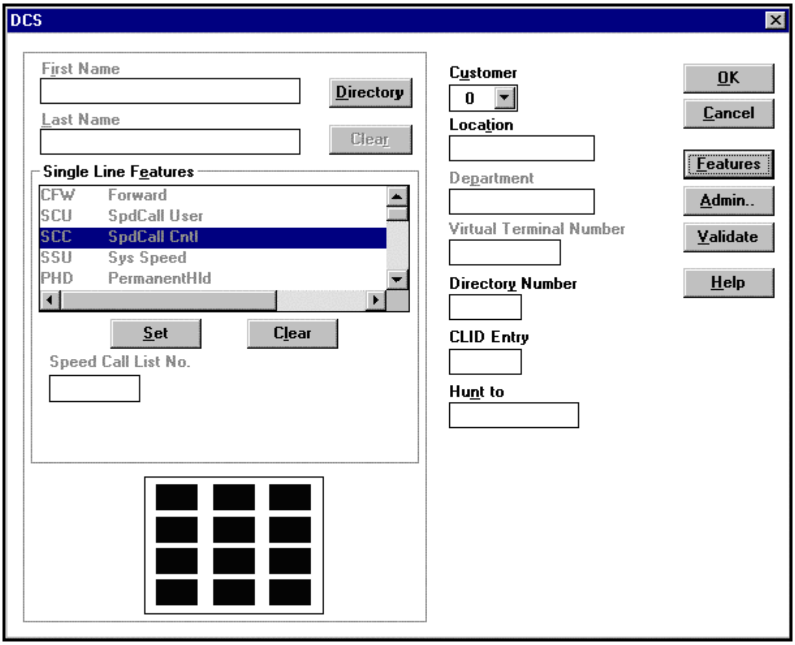
Procedure 128
Selecting Digital Cordless Set

Step	Action
1	Select Digital Cordless Set.
	Highlight **DCS**, and click on the **OK** button.

END

Selecting features

Figure 248
DCS window



Customer: 0

CFW	Forward
SCU	SpdCall User
SCC	SpdCall Cntl
SSU	Sys Speed
PHD	PermanentHld

Complete the following step.

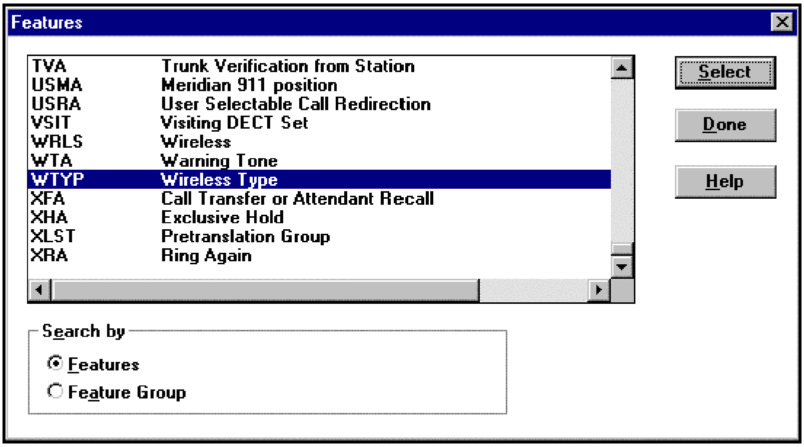
Procedure 129
Selecting features

Step	Action
1	Select features.
	Click on the **Features** button.

END

Selecting wireless type

Figure 249
Features window



TVA	Trunk Verification from Station
USMA	Meridian 911 position
USRA	User Selectable Call Redirection
VSIT	Visiting DECT Set
WRLS	Wireless
WTA	Warning Tone
WTYP	Wireless Type
XFA	Call Transfer or Attendant Recall
XHA	Exclusive Hold
XLST	Pretranslation Group
XRA	Ring Again

Search by

● Features

○ Feature Group

Complete the following step.

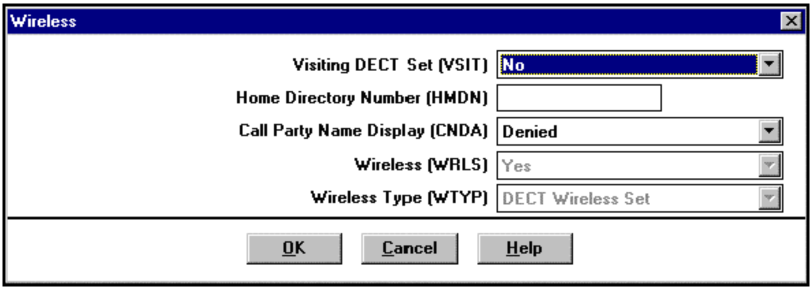
Procedure 130
Selecting wireless type

Step	Action
1	Select wireless type.
	Highlight **WTYP**, and click the **Select** button.

END

Selecting Visit DECT Set or local calling

Figure 250
Wireless Visiting DECT Set



Wireless

Visiting DECT Set (VSIT): No

Home Directory Number (HMDN):

Call Party Name Display (CNDA): Denied

Wireless (WRLS): Yes

Wireless Type (WTYP): DECT Wireless Set

Complete the following steps.

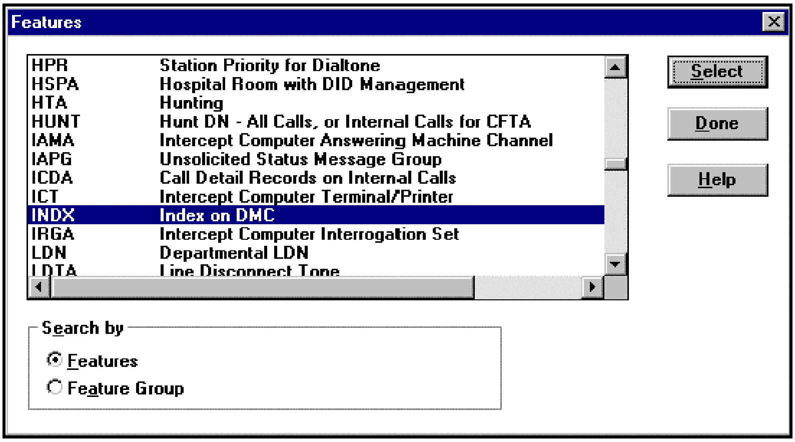
Procedure 131
Selecting Visit or local

Step	Action
1	Select **Visit DECT Set** as **Yes** if this DECT handset is visiting this PBX. Select **No** if this DECT handset is to be configured for local calling only.
	If Visiting DECT Set is Yes, go to step 2. If the DECT handset is configured for local calling only, go to step 4.
2	Select visiting.
	From the **Visiting DECT Set (VSIT)** list, select **Yes**.
3	Select a Home DN.
	Enter a DN in the **Home Directory Number (HMDN)** box.
4	Configure for local calling only.
	From the **Visiting DECT Set (VSIT)** list, select **No**.
5	Accept changes.
	Click on the **OK** button.

END

Selecting an index

Figure 251
Features window



HPR	Station Priority for Dialtone
HSPA	Hospital Room with DID Management
HTA	Hunting
HUNT	Hunt DN - All Calls, or Internal Calls for CFTA
IAMA	Intercept Computer Answering Machine Channel
IAPG	Unsolicited Status Message Group
ICDA	Call Detail Records on Internal Calls
ICT	Intercept Computer Terminal/Printer
INDX	Index on DMC
IRGA	Intercept Computer Interrogation Set
LDN	Departmental LDN
LDTA	Line Disconnect Tone

Search by

● Features

○ Feature Group

Complete the following step.

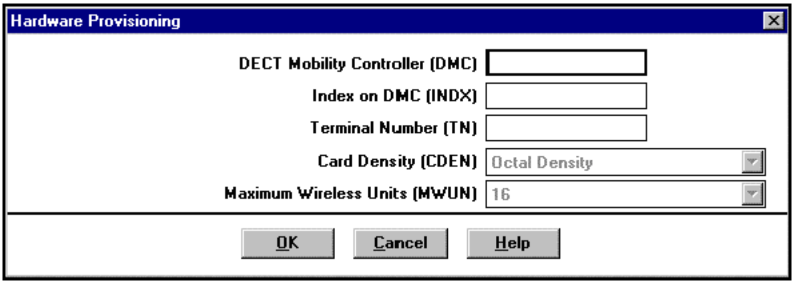
Procedure 132
Selecting an index

Step	Action
1	Select an index.
	Highlight **INDX**, and click on the **Select** button.

END

Provisioning the hardware

Figure 252
Hardware Provisioning window



Hardware Provisioning

DECT Mobility Controller (DMC)

Index on DMC (INDX)

Terminal Number (TN)

Card Density (CDEN) Octal Density

Maximum Wireless Units (MWUN) 16

Complete the following steps.

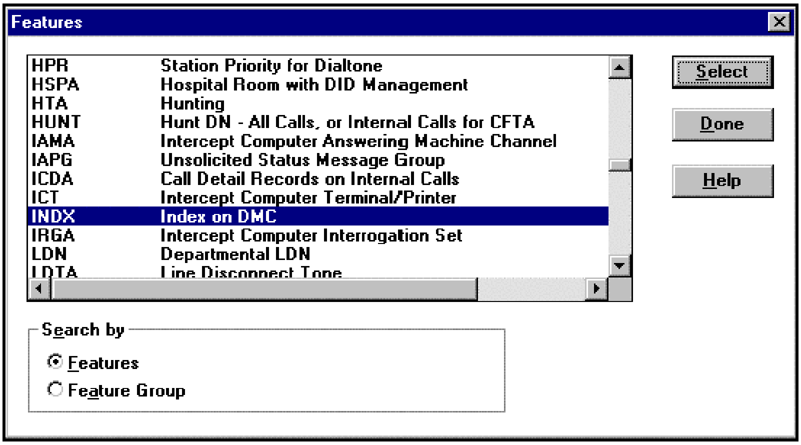
Procedure 133
Provisioning hardware

Step	Action
1	Select a DMC TN.
	Enter a TN in the **DECT Mobility Controller (DMC)** box.
2	Select an index.
	Enter an index in the **Index on DMC (INDX)** box. (Index range is 0 to 509.) ***Note 1:*** The Terminal Number (TN) is a virtual TN and selected by the PBX system. ***Note 2:*** Index 0-509 on PBX is seen as Index 1-510 in OTM.
3	Accept changes.
	Click on the **OK** button.

END

Accepting changes

Figure 253
Features window



HPR	Station Priority for Dialtone
HSPA	Hospital Room with DID Management
HTA	Hunting
HUNT	Hunt DN - All Calls, or Internal Calls for CFTA
IAMA	Intercept Computer Answering Machine Channel
IAPG	Unsolicited Status Message Group
ICDA	Call Detail Records on Internal Calls
ICT	Intercept Computer Terminal/Printer
INDX	Index on DMC
IRGA	Intercept Computer Interrogation Set
LDN	Departmental LDN
LDTA	Line Disconnect Tone

Search by

● Features

○ Feature Group

Complete the following step.

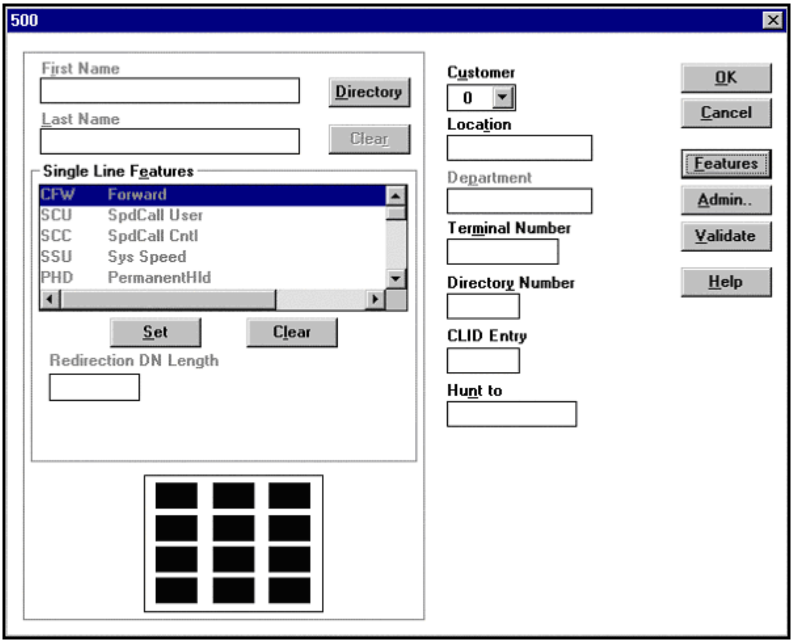
Procedure 134
Accepting changes

Step	Action
1	Accept changes.
	Click on the **Done** button.

END

Single line features

Figure 254
500 window



Customer: 0

CFW	Forward
SCU	SpdCall User
SCC	SpdCall Cntl
SSU	Sys Speed
PHD	PermanentHld

Complete the following step.

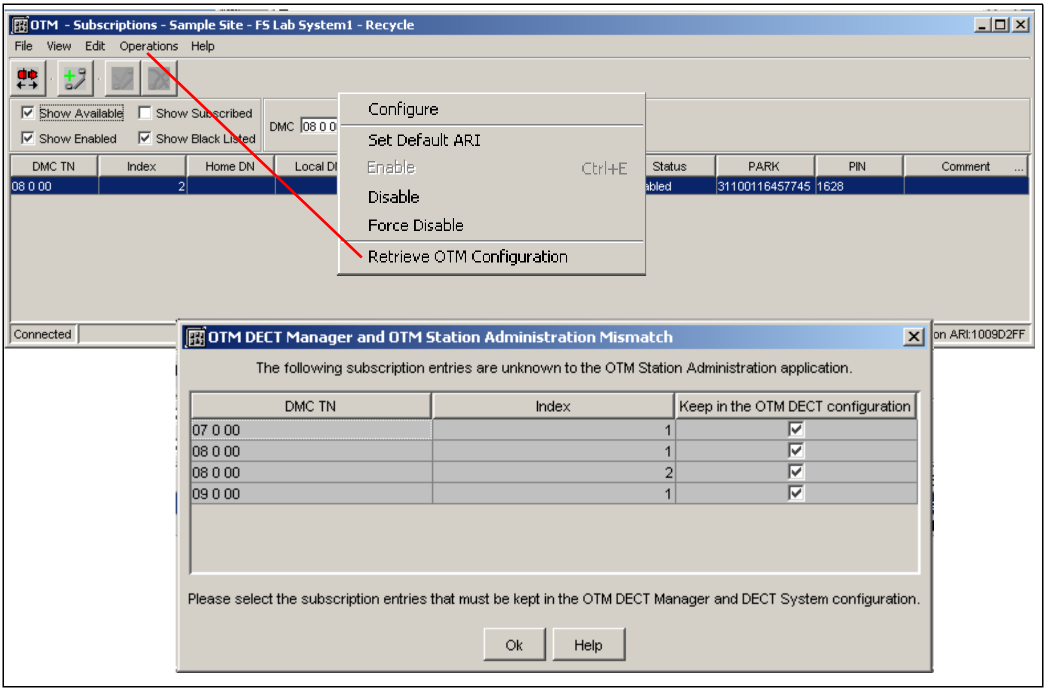
Procedure 135
Single Line Features
Configure the remaining features on the 500 or DCS set

Step	Action
1	For information on other Single Line Features.
	Refer to the OTM Station Administration in *Telephony Manager: System Administration* (553-3001-330).

END

Retrieving subscription data for DECT handsets

Figure 255
DECT Subscriptions window, Synchronize DECT and Administration Config window



The following subscription entries are unknown to the OTM Station Administration application.

DMC TN	Index	Keep in the OTM DECT configuration
07 0 00	1	☑
08 0 00	1	☑
08 0 00	2	☑
09 0 00	1	☑

Please select the subscription entries that must be kept in the OTM DECT Manager and DECT System configuration.

Complete the following steps.

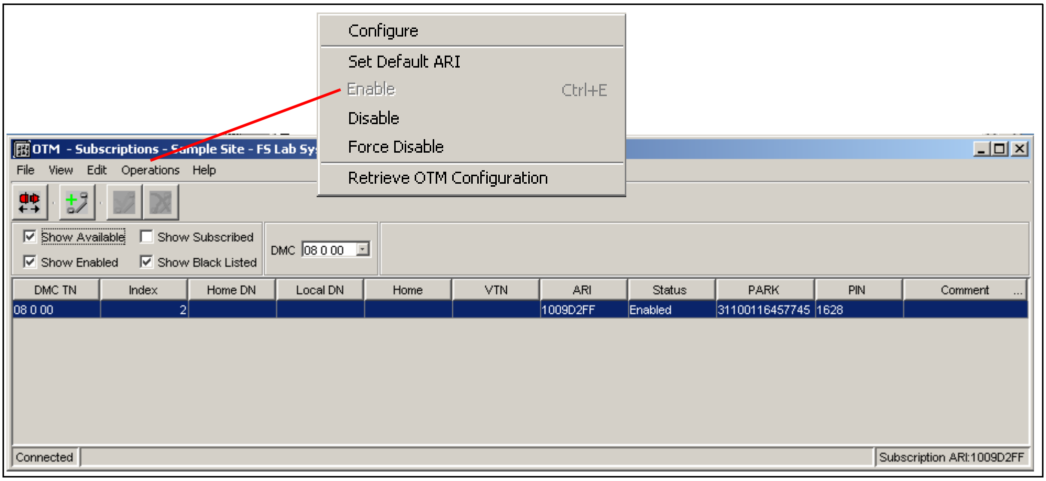
Procedure 136
Retrieving subscription data for DECT handsets

Step	Action
1	Using Windows, login to OTM. Select the system that supports the DECT system. Launch the DECT application. Open the DECT Systems window.
	Follow the instructions on page 440 to page 442.
2	Using a web-based navigator, open the Administrator login screen and login. Select the System Navigator. Select the system that supports the DECT system. Launch the DECT application. Open the DECT Systems window.
	Follow the instructions on page 443 to page 446.
3	Open the Subscriptions window.
	Follow the instructions on page 448.
4	Retrieve the subscription configuration data from the OTM Station Administration database.
	In the Subscriptions window, click on the **Operations** pull-down menu, click on **Retrieve OTM Configuration**.
5	***Note:*** At this point, all DECT handsets configured on OTM Station Administration are shown in the Subscriptions window. Open the Configure DECT Subscription dialog.
	Click the **File** pull-down menu. Click **Add** or + .

END

Enabling subscriptions

Figure 256
Subscriptions window


Configure
Set Default ARI
Enable Ctrl+E
Disable
Force Disable
Retrieve OTM Configuration
OTM - Subscriptions - Sample Site - FS Lab Sy
File View Edit Operations Help

☑ Show Available ☐ Show Subscribed
☑ Show Enabled ☑ Show Black Listed
DMC 08 0 00

DMC TN	Index	Home DN	Local DN	Home	VTN	ARI	Status	PARK	PIN	Comment
08 0 00	2					1009D2FF	Enabled	31100116457745	1628	

Connected | Subscription ARI:1009D2FF

Complete the following steps for each DECT handset:

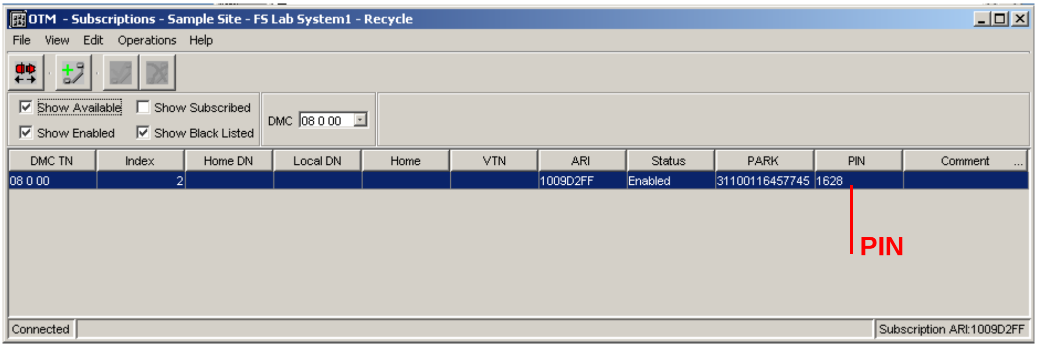
Procedure 137
Enabling DECT handsets

Step	Action
1	***Note:*** At this point, there are no PINs shown in the Subscriptions window. Select a DECT handset from the list.
	Click on one DECT handset in the list to highlight a row.
2	Enable DECT handsets.
	Click on the **Operations** pull-down menu. Click **Enable** or click on ✓ .

END

Activating the PIN on the DECT handsets

Figure 257
Subscriptions window


OTM - Subscriptions - Sample Site - FS Lab System1 - Recycle
File
View
Edit
Operations
Help
PIN

☑ Show Available □ Show Subscribed
☑ Show Enabled ☑ Show Black Listed
DMC 08 0 00

DMC TN	Index	Home DN	Local DN	Home	VTN	ARI	Status	PARK	PIN	Comment
08 0 00	2					1009D2FF	Enabled	31100116457745	1628	

Connected Subscription ARI:1009D2FF

Complete the following step:

Procedure 138
Obtaining the PIN

Step	Action
1	***Note:*** At this point, in the Subscriptions window, the PINs are shown and the Status is Enabled.
	For information on subscribing and provisioning handsets refer to the DECT Handset user guides.

END

Note: When a DECT handset is subscribed, the Subscription window shows the Status column as Subscribed and does not show a PIN.

Working with DECT handset subscriptions

Procedures are available for:

1 “Disabling a DECT handset subscription” on page 494

2 “Copying a DECT handset subscription” on page 496

3 “Moving a DECT handset subscription” on page 498

4 “Finding a DECT handset subscription” on page 500

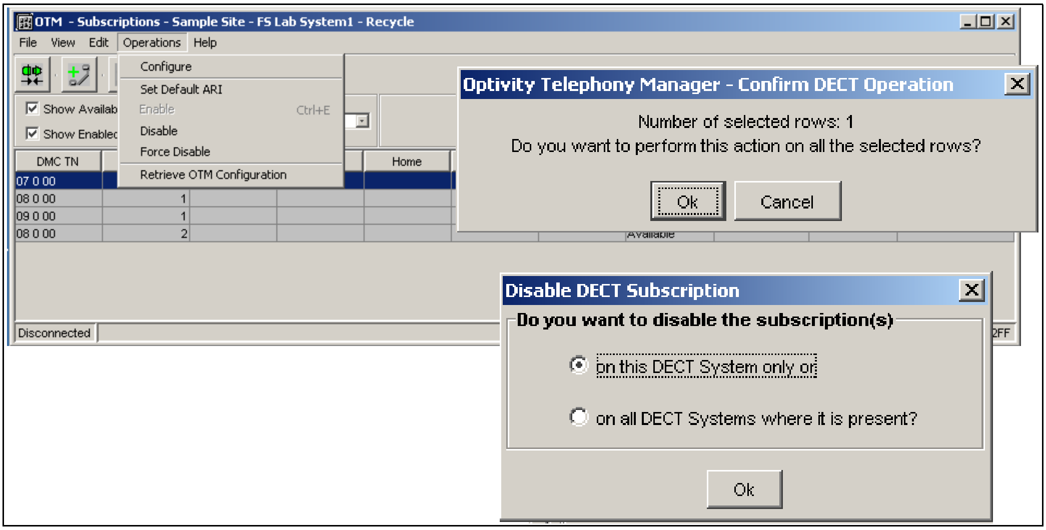
5 “Importing a DECT handset subscription” on page 502

6 “Exporting a DECT handset subscription” on page 504

7 “Force disabling a DECT handset subscription” on page 506

Disabling a DECT handset subscription

Figure 258
DECT Subscriptions window and Disable DECT Subscription window



Optivity Telephony Manager - Confirm DECT Operation

Number of selected rows: 1
Do you want to perform this action on all the selected rows?

Ok Cancel

Disable DECT Subscription

Do you want to disable the subscription(s)

● on this DECT System only or

○ on all DECT Systems where it is present?

Ok

Note: For further information, refer to “Delete subscriptions” on page 142 and “Multi-site Mobility Networking” on page 166.

Complete the following steps.

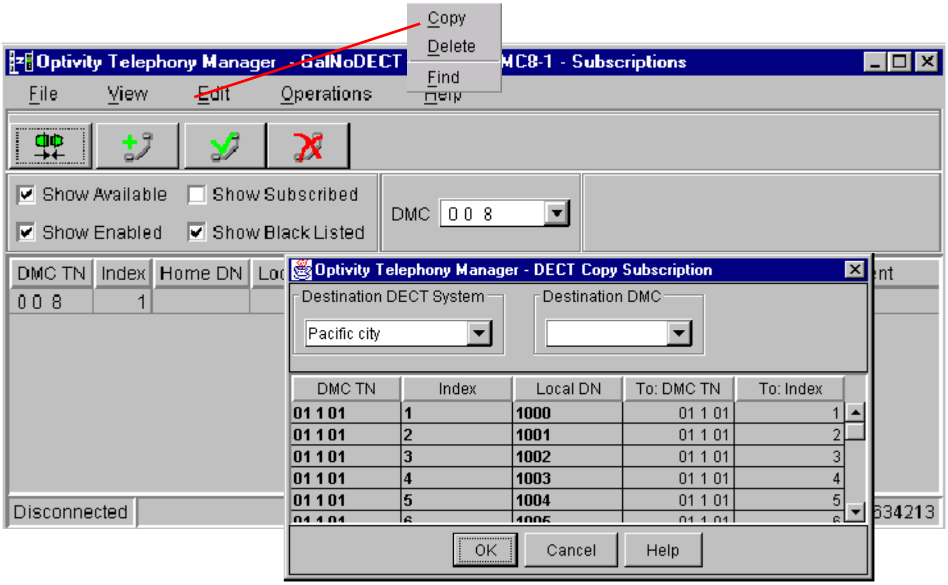
Procedure 139
Disabling DECT handset subscription

Step	Action
1	Using Windows, login to OTM. Select the system that supports the DECT system. Launch the DECT application. Open the DECT Systems window.
	Follow the instructions on page 440 to page 442.
2	Using a web-based navigator, open the Administrator login screen and login. Select the System Navigator. Select the system that supports the DECT system. Launch the DECT application. Open the DECT Systems window.
	Follow the instructions on page 443 to page 446.
3	Open the Subscriptions window.
	Follow the instructions on page 448.
4	Select a DECT handset subscriptions for disabling. ***Note:*** A single DECT handset, a list of DECT handsets, or all DECT handsets on a DMC can be selected.
	Highlight a **DMC TN** and an **Index** (or more than one index) in the list.
5	Disable the DECT handset subscriptions.
	From the **Operations** pull-down menu, click **Disable**.
6	Disable from this system only.
	Click **OK**.
7	Disable from all systems where the portable set is subscribed.
	Click **OK**.

END

Copying a DECT handset subscription

Figure 259
DECT Subscriptions window and DECT Copy Subscription window


Copy
Delete
Find
Optivity Telephony Manager - GalNoDECT ... MC8-1 - Subscriptions
File
View
Edit
Operations
Help
Optivity Telephony Manager - DECT Copy Subscription
OK
Cancel
Help

☑ Show Available □ Show Subscribed
☑ Show Enabled ☑ Show Black Listed

DMC 0 0 8

DMC TN	Index	Home DN	Loc
0 0 8	1		

Disconnected

634213

Destination DECT System: Pacific city

Destination DMC:

DMC TN	Index	Local DN	To: DMC TN	To: Index
01 1 01	1	1000	01 1 01	1
01 1 01	2	1001	01 1 01	2
01 1 01	3	1002	01 1 01	3
01 1 01	4	1003	01 1 01	4
01 1 01	5	1004	01 1 01	5
01 1 01	6	1005	01 1 01	6

Note: For further information, refer to “Copy subscriptions” on page 139.

Complete the following steps.

Procedure 140
Copying a DECT handset subscription (Part 1 of 2)

Step	Action
1	Using Windows, login to OTM. Select the system that supports the DECT system. Launch the DECT application. Open the DECT Systems window.
	Follow the instructions on page 440 to page 442.
2	Using a web-based navigator, open the Administrator login screen and login. Select the System Navigator. Select the system that supports the DECT system. Launch the DECT application. Open the DECT Systems window.
	Follow the instructions on page 443 to page 446.
3	Select the source DECT system to copy the subscription.
	Highlight the DECT system in the DECT Systems window.
4	Open the Subscriptions window.
	Follow the instructions on page 448.
5	Open the DECT Copy Subscription dialog.
	From the **Edit** pull-down menu, click on **Copy**.
6	Select a DECT system where the copied subscription is to be stored
	Pull-down the **Destination DECT System** list and highlight a system name.
7	Select DMC on the DECT system where the copied subscription is to be stored.
	Pull-down the **Destination DMC** list and highlight a DMC.
8	Select a DECT handset subscriptions to copy. ***Note:*** Select a single DECT handset, a list of DECT handsets, or all DECT handsets on a DMC.
	Highlight a **DMC TN** and an **Index** (or more than one index) in the list.

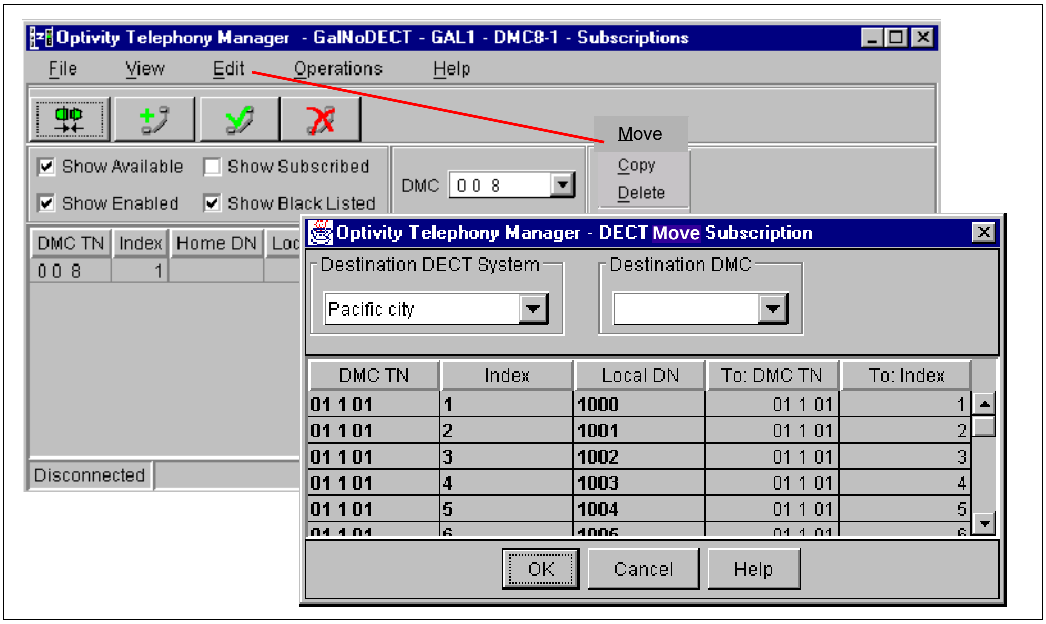
Procedure 140
Copying a DECT handset subscription (Part 2 of 2)

Step	Action
9	Select a DMC or Index for the subscriptions.
	Highlight a **To: DMC TN** or a **To: Index** (or more than one index) in the list.
10	Accept the changes.
	Click on the **OK** button.

END

Moving a DECT handset subscription

Figure 260
DECT Subscriptions window and DECT Move Subscription window


Optivity Telephony Manager - GalNoDECT - GAL1 - DMC8-1 - Subscriptions
File
View
Edit
Operations
Help
Move
Copy
Delete
Optivity Telephony Manager - DECT Move Subscription
OK
Cancel
Help

☑ Show Available ☐ Show Subscribed

☑ Show Enabled ☑ Show Black Listed

DMC 0 0 8

DMC TN	Index	Home DN	Loc
0 0 8	1		

Disconnected

Destination DECT System: Pacific city

Destination DMC:

DMC TN	Index	Local DN	To: DMC TN	To: Index
01 1 01	1	1000	01 1 01	1
01 1 01	2	1001	01 1 01	2
01 1 01	3	1002	01 1 01	3
01 1 01	4	1003	01 1 01	4
01 1 01	5	1004	01 1 01	5
01 1 01	6	1005	01 1 01	6

Note: For further information, refer to “Move subscriptions” on page 141.

Complete the following steps.

Procedure 141
Moving a DECT handset subscription (Part 1 of 2)

Step	Action
1	Using Windows, login to OTM. Select the system that supports the DECT system. Launch the DECT application. Open the DECT Systems window.
	Follow the instructions on page 440 to page 442.
2	Using a web-based navigator, open the Administrator login screen and login. Select the System Navigator. Select the system that supports the DECT system. Launch the DECT application. Open the DECT Systems window.
	Follow the instructions on page 443 to page 446.
3	Open the Subscriptions window.
	Follow the instructions on page 448.
4	Open the DECT Move Subscription dialog.
	From the **Edit** pull-down menu, click on **Move**.
5	Select a DECT system where the moved subscription is to be put.
	Pull-down the **Destination DECT System** list and highlight a system name.
6	Select DMC on the DECT system where the moved subscription is to be put.
	Pull-down the **Destination DMC** list and highlight a DMC.
7	Select DMC on the DECT system the moved subscription is to be put.
	Pull-down the **Destination DMC** list and highlight a DMC.
8	Select a DECT handset subscriptions to move. ***Note:*** Select a single DECT handset, a list of DECT handsets, or all DECT handsets on a DMC.
	Highlight a **DMC TN** and an **Index** (or more than one index) in the list.

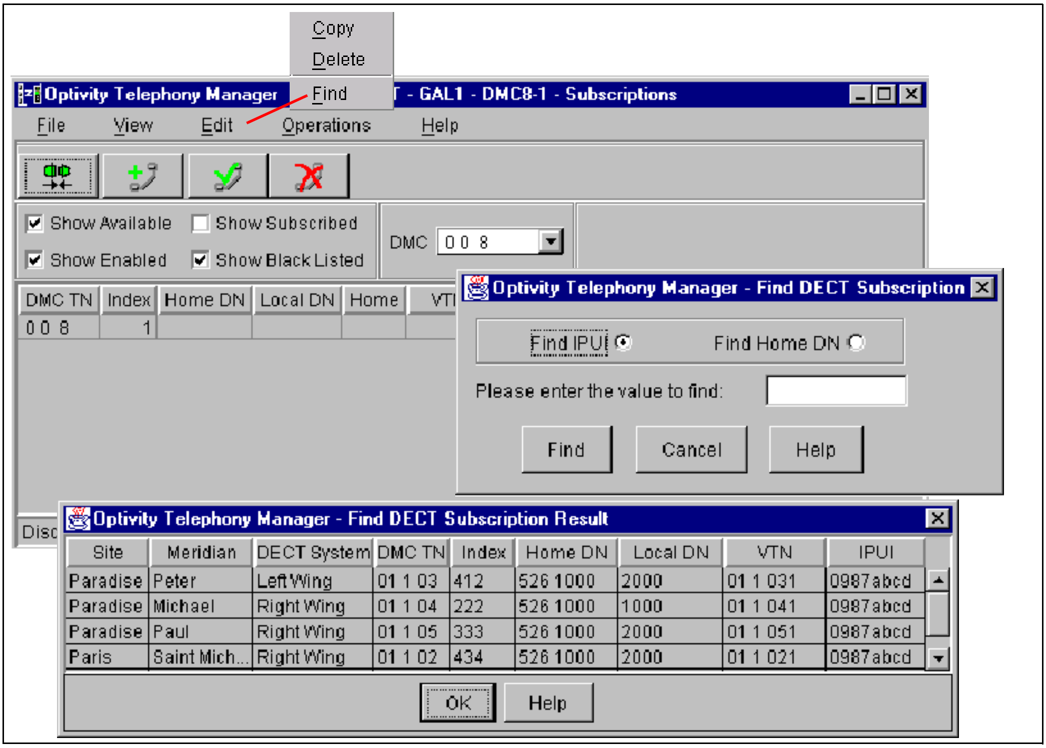
Procedure 141
Moving a DECT handset subscription (Part 2 of 2)

Step	Action
9	Select a DMC or Index for the subscriptions.
	Highlight a **To: DMC TN** or a **To: Index** (or more than one index) in the list.
10	Accept the changes.
	Click **OK**.

END

Finding a DECT handset subscription

Figure 261
DECT Subscriptions window and Find DECT Subscription window



Copy
Delete
Find
Optivity Telephony Manager ... T - GAL1 - DMC8-1 - Subscriptions
File
View
Edit
Operations
Help
Disc
Optivity Telephony Manager - Find DECT Subscription
Find
Cancel
Help
Optivity Telephony Manager - Find DECT Subscription Result
OK
Help

☑ Show Available ☐ Show Subscribed
☑ Show Enabled ☑ Show Black Listed

DMC 0 0 8

DMC TN	Index	Home DN	Local DN	Home	VT
0 0 8	1				

Find IPUI ● Find Home DN ○

Please enter the value to find:

Site	Meridian	DECT System	DMC TN	Index	Home DN	Local DN	VTN	IPUI
Paradise	Peter	Left Wing	01 1 03	412	526 1000	2000	01 1 031	0987abcd
Paradise	Michael	Right Wing	01 1 04	222	526 1000	1000	01 1 041	0987abcd
Paradise	Paul	Right Wing	01 1 05	333	526 1000	2000	01 1 051	0987abcd
Paris	Saint Mich...	Right Wing	01 1 02	434	526 1000	2000	01 1 021	0987abcd

Note: For further information, refer to “Find subscriptions” on page 144.

Complete the following steps.

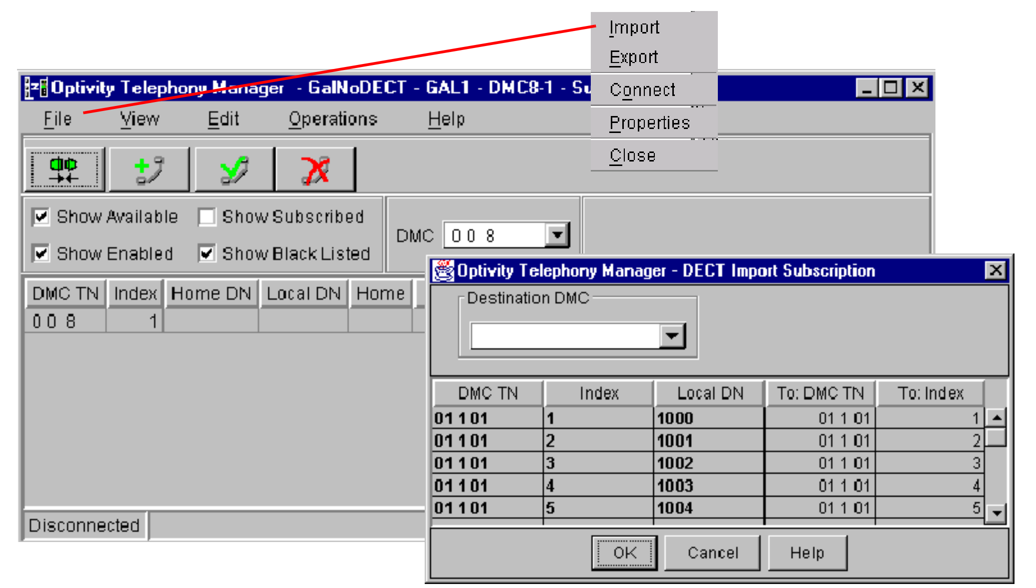
Procedure 142
Finding a DECT handset subscription

Step	Action
1	Using Windows, login to OTM. Select the system that supports the DECT system. Launch the DECT application. Open the DECT Systems window.
	Follow the instructions on page 440 to page 442.
2	Using a web-based navigator, open the Administrator login screen and login. Select the System Navigator. Select the system that supports the DECT system. Launch the DECT application. Open the DECT Systems window.
	Follow the instructions on page 443 to page 446.
3	Open the Subscriptions window.
	Follow the instructions on page 448.
4	Open the Find DECT Subscription dialog.
	From the **Edit** pull-down menu, click on **Find**.
5	Select find criteria.
	Click on **Find IPUI** or **Find Home DN**, enter the value, and click on the **Find** button.
6	View the results.

END

Importing a DECT handset subscription

Figure 262
DECT Subscriptions window and DECT Import Subscription window


Import
Export
Connect
Properties
Close
Optivity Telephony Manager - GalNoDECT - GAL1 - DMC8-1 - Su
File
View
Edit
Operations
Help
Optivity Telephony Manager - DECT Import Subscription
OK
Cancel
Help

☑ Show Available □ Show Subscribed
☑ Show Enabled ☑ Show Black Listed

DMC 0 0 8

DMC TN	Index	Home DN	Local DN	Home
0 0 8	1			

Disconnected

Destination DMC

DMC TN	Index	Local DN	To: DMC TN	To: Index
01 1 01	1	1000	01 1 01	1
01 1 01	2	1001	01 1 01	2
01 1 01	3	1002	01 1 01	3
01 1 01	4	1003	01 1 01	4
01 1 01	5	1004	01 1 01	5

Note: For further information, refer to "Import subscriptions" on page 141.

Complete the following steps.

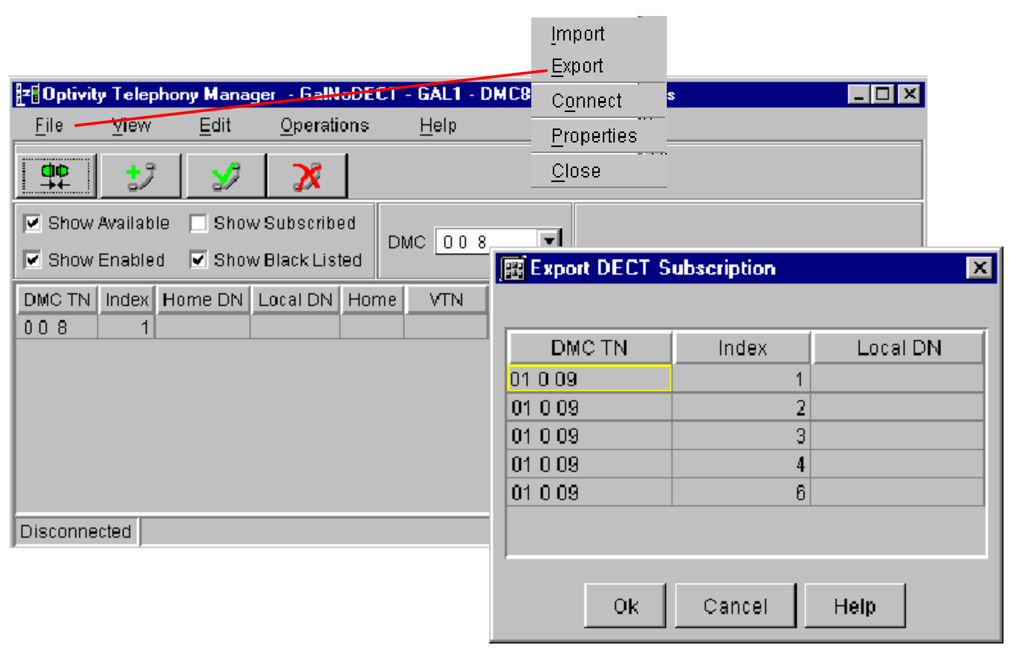
Procedure 143
Importing a DECT handset subscription

Step	Action
1	Access the DECT Application.
	Follow the instructions in “Windows access to the DECT application” on page 440.
2	Using a web-based navigator, open the Administrator login screen and login. Select the System Navigator. Select the system that supports the DECT system. Launch the DECT application. Open the DECT Systems window.
	Follow the instructions on page 443 to page 446.
3	Open the Subscriptions window.
	Follow the instructions on page 448.
4	Open the DECT Import Subscription dialog.
	From the **File** pull-down menu, click on **Import**.
5	Select a DECT system where the imported subscription is to be put.
	Pull-down the **Destination DMC** list and highlight a DMC.
6	Select DMC to be imported.
	Pull-down the **Destination DMC** list and highlight a DMC.
7	Select a DECT handset subscriptions to import. ***Note:*** Select a single DECT handset, a list of DECT handsets, or all DECT handsets on a DMC.
	Highlight a **DMC TN** and an **Index** (or more than one index) in the list.
8	Select a DMC or Index for the subscriptions.
	Highlight a **To: DMC TN** or a **To: Index** (or more than one **To: index**) in the list.
9	Accept the changes.
	Click **OK**.

END

Exporting a DECT handset subscription

Figure 263
DECT Subscriptions window and Export Subscription window



☑ Show Available □ Show Subscribed

☑ Show Enabled ☑ Show Black Listed

DMC 0 0 8

DMC TN	Index	Home DN	Local DN	Home	VTN
0 0 8	1				

DMC TN	Index	Local DN
01 0 09	1	
01 0 09	2	
01 0 09	3	
01 0 09	4	
01 0 09	6	

Note: For further information, refer to “Export subscriptions” on page 143.

Complete the following steps.

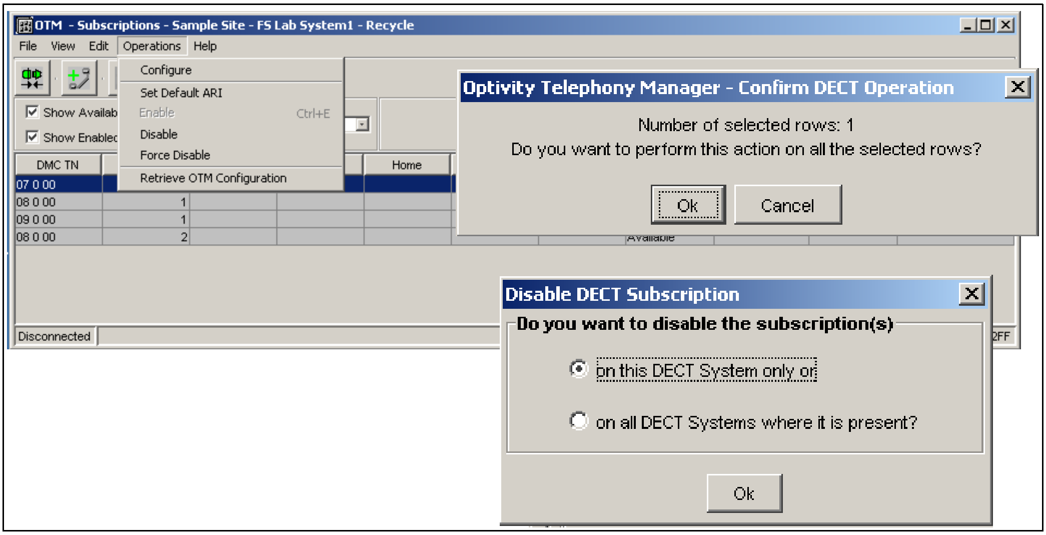
Procedure 144
Exporting a DECT handset subscription

Step	Action
1	Using Windows, login to OTM. Select the system that supports the DECT system. Launch the DECT application. Open the DECT Systems window.
	Follow the instructions on page 440 to page 442.
2	Using a web-based navigator, open the Administrator login screen and login. Select the System Navigator. Select the system that supports the DECT system. Launch the DECT application. Open the DECT Systems window.
	Follow the instructions on page 443 to page 446.
3	Open the Subscriptions window.
	Follow the instructions on page 448.
4	Open the Export DECT Subscription dialog.
	From the **Find** pull-down menu, click on **Export**.
5	Select a DECT handset subscriptions to export. ***Note:*** A single DECT handset, a list of DECT handsets, or all DECT handsets on a DMC can be selected.
	Highlight a **DMC TN** and an **Index** (or more than one **index**) in the list.
6	Select a DMC or Index for the subscriptions.
	Highlight a **To: DMC TN** or a **To: Index** (or more than one **To: indexes**) in the list.
7	Accept the changes.
	Click on the **OK** button.
8	Paste the subscriptions into a file.

END

Force disabling a DECT handset subscription

Figure 264
DECT Subscriptions window and
Force disable DECT Subscription window



Number of selected rows: 1
Do you want to perform this action on all the selected rows?

Do you want to disable the subscription(s)

● on this DECT System only or

○ on all DECT Systems where it is present?

Note: For more information, refer to “Force disable subscriptions” on page 146.

Complete the following steps.

Procedure 145
Force disabling a DECT handset subscription

Step	Action
1	Using Windows, login to OTM. Select the system that supports the DECT system. Launch the DECT application. Open the DECT Systems window.
	Follow the instructions on page 440 to page 442.
2	Using a web-based navigator, open the Administrator login screen and login. Select the System Navigator. Select the system that supports the DECT system. Launch the DECT application. Open the DECT Systems window.
	Follow the instructions on page 443 to page 446.
3	Open the Subscriptions window.
	Follow the instructions on page 448.
4	Open the Force Disable DECT Subscription dialog.
	From the **Operations** pull-down menu, click on **Force Disable**.
5	Select a DECT handset subscriptions for Force Disabling. ***Note:*** Select a single DECT handset, a list of DECT handsets, or all DECT handsets on a DMC.
	Highlight a **DMC TN** and an **Index** (or more than one index) in the list.
6	Disable the DECT handset subscriptions.
	From the **Operations** pull-down menu, click on **Force Disable**.
7	Disable from this system only.
	Click on **OK** button.
8	Disable from all systems where the portable set is subscribed.
	Click **OK**.

END

Deleting TNs that are not on the switch

To remove configured sets (TRN status) that are no longer on the switch, perform the following steps.

Procedure 146
Removing configured sets

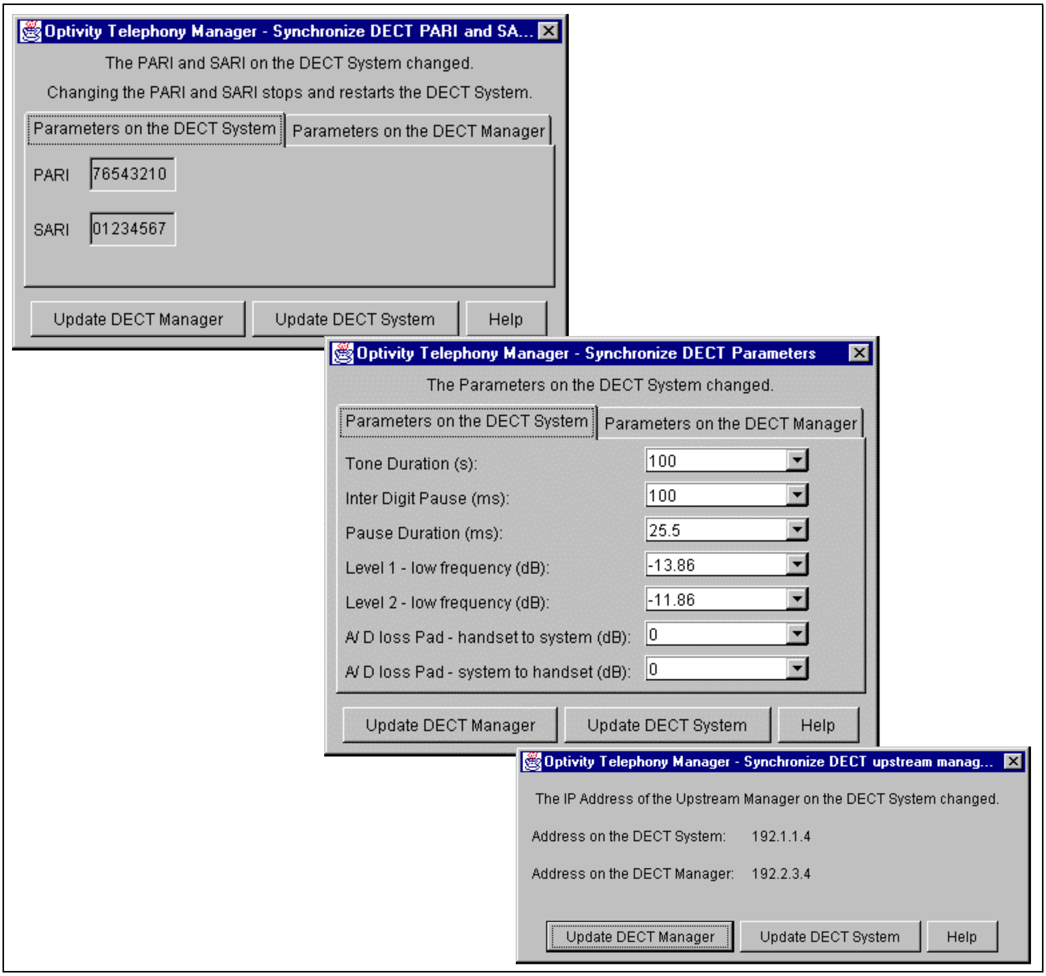
Step	Action
1	Using Windows, log in to OTM. Select the system that supports the DECT system. Launch the DECT application. Open the DECT Systems window.
	Follow the instructions on page 440 to page 442.
2	Use a web-based navigator to open the Administrator login screen and log in. Select the System Navigator. Select the system that supports the DECT system. Launch the DECT application. Open the DECT Systems window.
	Follow the instructions on page 443 to page 446.
3	Open the Subscriptions window.
	Follow the instructions on page 448.
4	Open the DECT Move Subscription dialog.
	From the **Edit** pull-down menu, click **Global update**.
5	Select the sync status **SSTAT**.
	Set **Old value** to the current status. Set **New value** to **NEW**.
6	Delete the TNs from the switch.

END

Note: Perform this procedure after 500 analogue TNs have been converted to concentrated TNs.

Updating data on OTM or updating data on a DECT system

Figure 265
Mismatch dialogs



Optivity Telephony Manager - Synchronize DECT PARI and SA...

The PARI and SARI on the DECT System changed.

Changing the PARI and SARI stops and restarts the DECT System.

PARI 76543210

SARI 01234567

Optivity Telephony Manager - Synchronize DECT Parameters

The Parameters on the DECT System changed.

Tone Duration (s):	100
Inter Digit Pause (ms):	100
Pause Duration (ms):	25.5
Level 1 - low frequency (dB):	-13.86
Level 2 - low frequency (dB):	-11.86
A/ D loss Pad - handset to system (dB):	0
A/ D loss Pad - system to handset (dB):	0

Optivity Telephony Manager - Synchronize DECT upstream manag...

The IP Address of the Upstream Manager on the DECT System changed.

Address on the DECT System: 192.1.1.4

Address on the DECT Manager: 192.2.3.4

When the DECT manager connects to a DECT system, synchronization flags any differences between the DECT manager database and the DECT system database with mismatch dialogs. These dialogs are useful when provisioning DECT systems off-site.

See “Provisioning a DECT system remotely” on page 511 and “Subscribing a DECT system remotely” on page 514.

Complete the following steps.

Procedure 147
Updating data on OTM

Step	Action
1	Using Windows, login to OTM. Select the system that supports the DECT system. Launch the DECT application. Open the DECT Systems window.
	Follow the instructions on page 440 to page 442.
2	Using a web-based navigator, open the Administrator login screen and login. Select the System Navigator. Select the system that supports the DECT system. Launch the DECT application. Open the DECT Systems window.
	Follow the instructions on page 443 to page 446.
3	Select a DECT system.
	Highlight a DECT system from the list.
4	Connect to a DECT system.
	From the **Applications** pull-down menu, click on **Connect** or click on the (green) icon.
5	If any of the dialogs in Figure 266 on page 511 appear, it is necessary to decide to update either the DECT manager or the DECT system.
	Click on either the **Update DECT Manager** button or **Update DECT System** button.

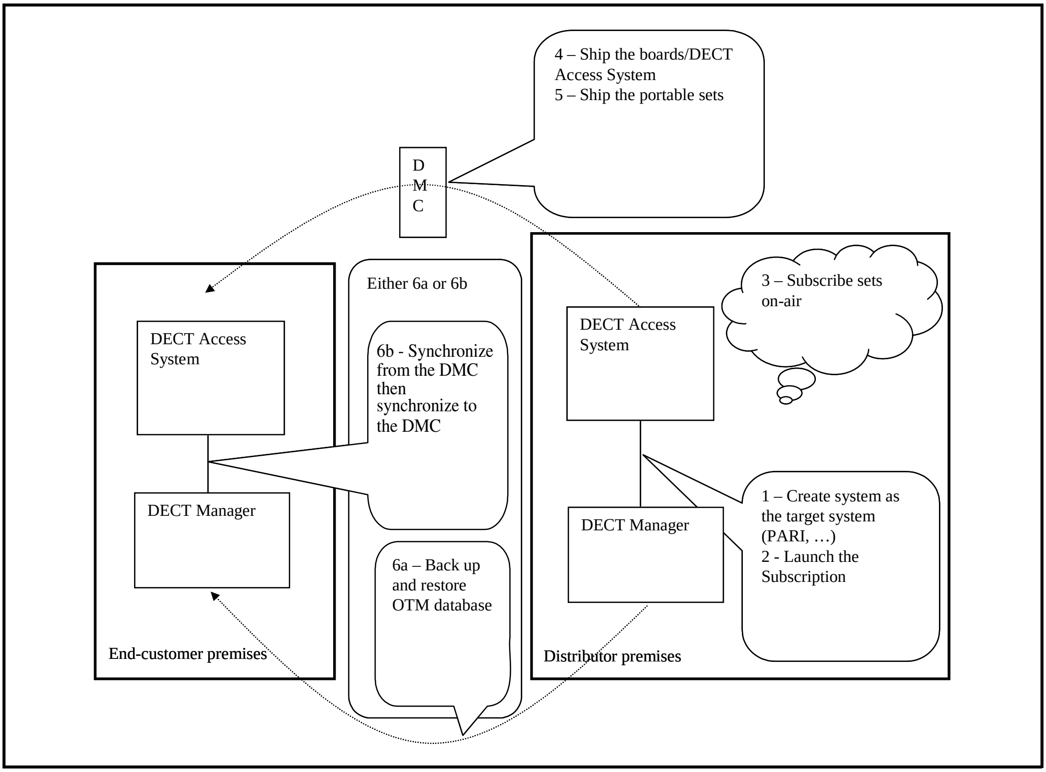
END

Provisioning a DECT system remotely

A distributor can use a DECT system to configure a system and subscribe sets on it. If the DECT Access System and board configuration are the same on both the distributor and the customer DECT systems, and if the DECT handsets are properly programmed on the customer-PBX-side, then the DMCs can be placed in the customer system and the DECT handsets function properly.

Remote DMC8 provisioning where the customer site has a DECT manager

Figure 266
Remote DMC8 provision where the customer site has a DECT manager


4 – Ship the boards/DECT Access System
5 – Ship the portable sets
D M C
Either 6a or 6b
6b - Synchronize from the DMC then synchronize to the DMC
6a – Back up and restore OTM database
3 – Subscribe sets on-air
DECT Access System
DECT Manager
DECT Access System
DECT Manager
1 – Create system as the target system (PARI, …)
2 - Launch the Subscription
End-customer premises
Distributor premises

Complete the following step.

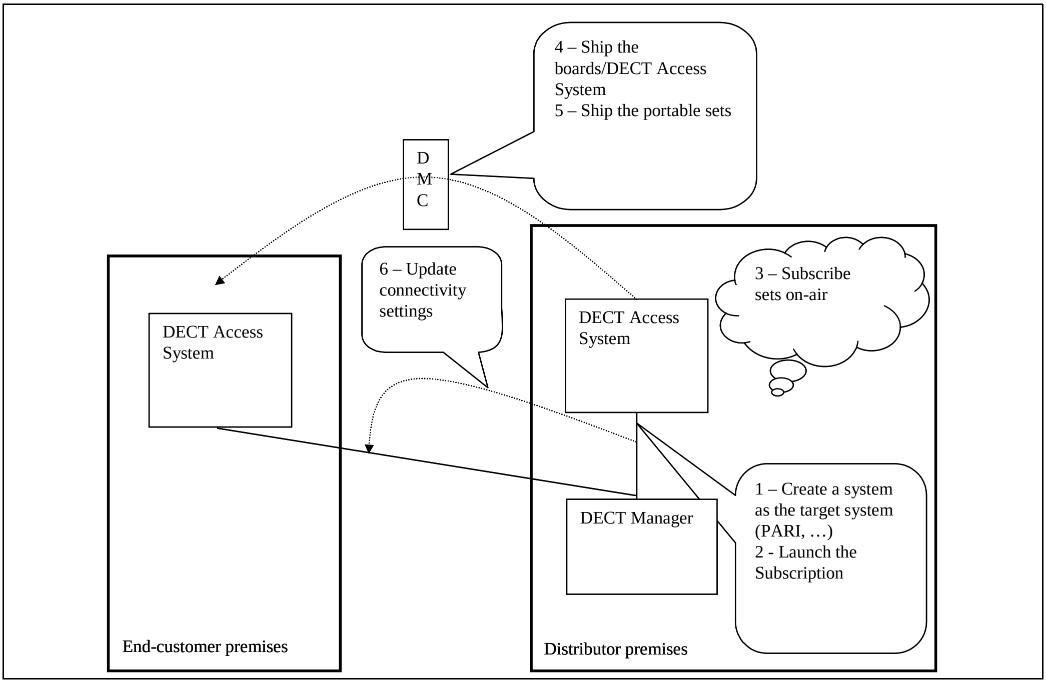
Procedure 148
Provisioning remotely when the customer site has a DECT manager

Step	Action
1	Remotely provision DMC8s for a customer site.
	Follow the steps 1 to 6a/6b shown in Figure 266 on page 511.

END

Remote DMC8 provisioning where the customer site does not have a DECT manager

Figure 267
Remote DMC8 provision where customer site does not have a DECT manager


4 – Ship the boards/DECT Access System
5 – Ship the portable sets
D M C
6 – Update connectivity settings
3 – Subscribe sets on-air
DECT Access System
DECT Access System
DECT Manager
1 – Create a system as the target system (PARI, …)
2 - Launch the Subscription
End-customer premises
Distributor premises

Complete the following step.

Procedure 149
Provisioning remotely when the customer site has no DECT manager

Step	Action
1	Remotely provision a customer site.
	Follow steps 1 to 6 shown in Figure 267 on page 513.

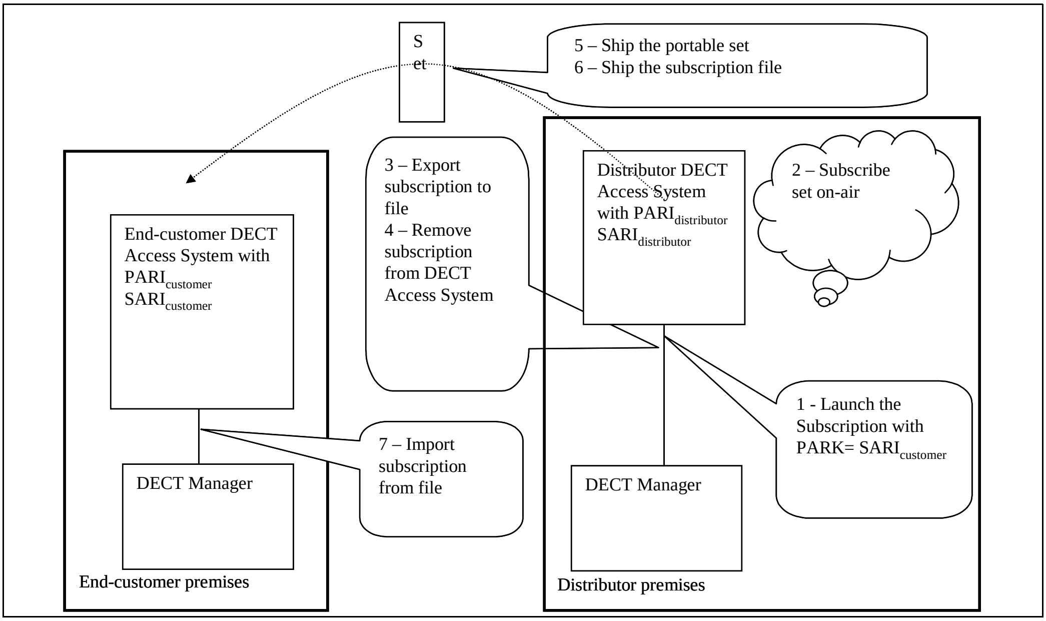
END

Subscribing a DECT system remotely

A DECT handset can subscribe itself to any DECT system, regardless of the DECT system Primary Access Rights Identifier (PARI) and Secondary Access Rights Identifier (SARI). In other words, from the DECT handset itself, the DECT handset can be subscribed to a DECT system where the DECT handset is not necessarily intended to be operational. The customer does not always have a DECT manager on site.

Remote DECT handset subscription where the customer site has a DECT manager

Figure 268
Remote DECT handset subscription where the customer site has a DECT manager


S
et
5 – Ship the portable set
6 – Ship the subscription file
3 – Export subscription to file
4 – Remove subscription from DECT Access System
Distributor DECT Access System with PARI$_{distributor}$ SARI$_{distributor}$
2 – Subscribe set on-air
End-customer DECT Access System with PARI$_{customer}$ SARI$_{customer}$
7 – Import subscription from file
1 - Launch the Subscription with PARK= SARI$_{customer}$
DECT Manager
DECT Manager
End-customer premises
Distributor premises

Complete the following step.

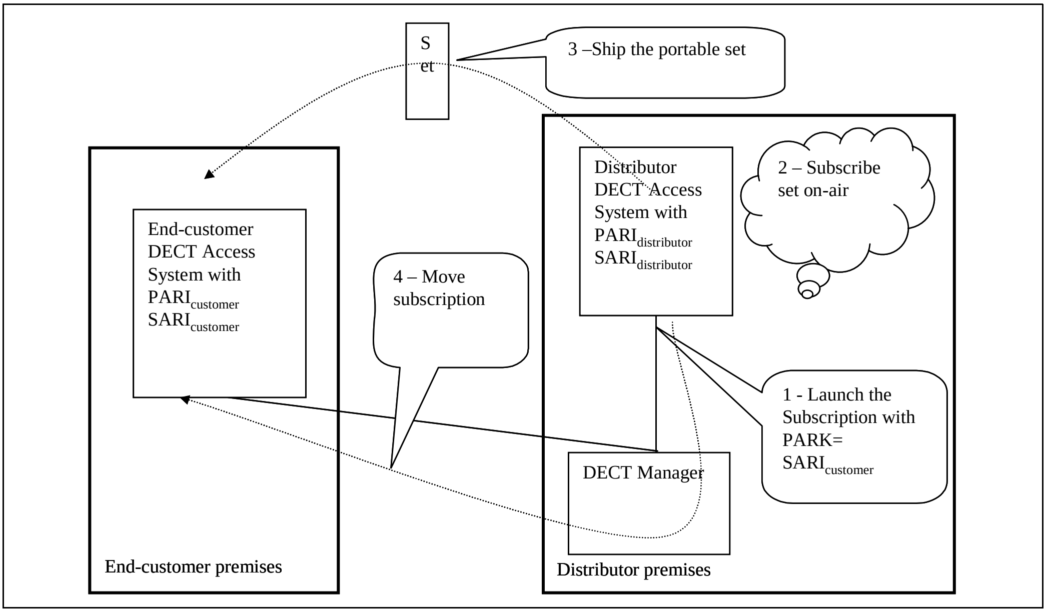
Procedure 150
Updating IP address on OTM

Step	Action
1	Remotely provision a customer site.
	Follow steps 1 to 7 shown in Figure 268.

END

Remote DECT handset subscription where the customer site does not have a DECT manager

Figure 269
Remote DECT handset subscription where customer site does not have a DECT manager


S
et
3 –Ship the portable set
End-customer DECT Access System with PARI$_{customer}$ SARI$_{customer}$
4 – Move subscription
Distributor DECT Access System with PARI$_{distributor}$ SARI$_{distributor}$
2 – Subscribe set on-air
1 - Launch the Subscription with PARK= SARI$_{customer}$
DECT Manager
End-customer premises
Distributor premises

Complete the following step.

Procedure 151
Updating IP address on OTM

Step	Action
1	Remotely provision a customer site.
	Follow steps 1 to 4 shown in Figure 269.

END

Modifying system properties

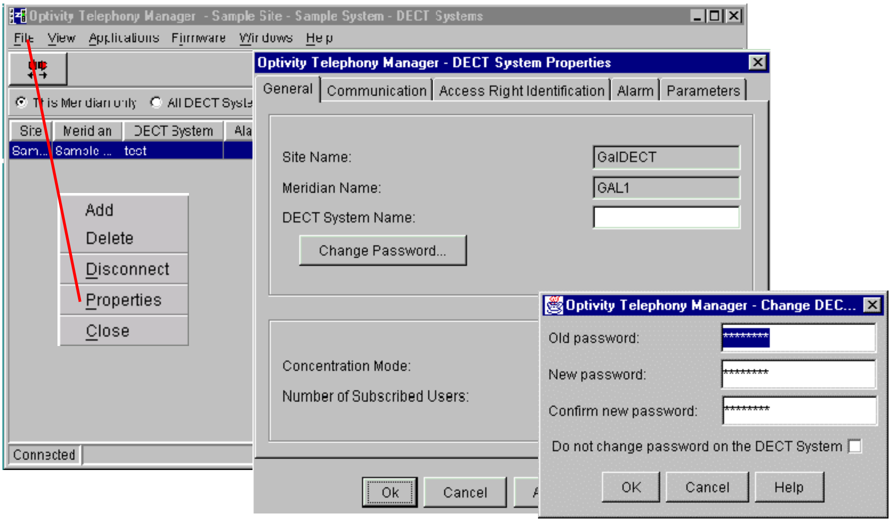
Several system properties can be modified. Procedures are included for:

1. "Changing passwords" on page 518
2. "Changing the DECT system name" on page 520
3. "Changing the IP address on OTM DECT manager" on page 522
4. "Changing the IP address on the DECT system DMC8 Relay card" on page 524
5. "Changing a PARI or SARI" on page 526
6. "Changing the Upstream Manager IP address" on page 528
7. "Changing the time and date" on page 530
8. "Changing parameters" on page 531

Changing passwords

Note: For lost passwords, see "Recovering a password" on page 611.

Figure 270
DECT Systems window and Change DECT Password


Optivity Telephony Manager - Sample Site - Sample System - DECT Systems
File View Applications Firmware Windows Help
This Meridian only
All DECT Syste
Site
Meridian
DECT System
Ala
Sam...
Sample ...
test
Add
Delete
Disconnect
Properties
Close
Connected
Optivity Telephony Manager - DECT System Properties
General
Communication
Access Right Identification
Alarm
Parameters
Change Password...
Concentration Mode:
Number of Subscribed Users:
Ok
Cancel
Optivity Telephony Manager - Change DEC...
OK
Cancel
Help

Site Name: GalDECT

Meridian Name: GAL1

DECT System Name:

Old password: ********

New password: ********

Confirm new password: ********

Do not change password on the DECT System □

Complete the following steps.

Procedure 152
Changing passwords

Step	Action
1	Using Windows, login to OTM. Select the system that supports the DECT system. Launch the DECT application. Open the DECT Systems window.
	Follow the instructions on page 440 to page 442.
2	Using a web-based navigator, open the Administrator login screen and login. Select the System Navigator. Select the system that supports the DECT system. Launch the DECT application. Open the DECT Systems window.

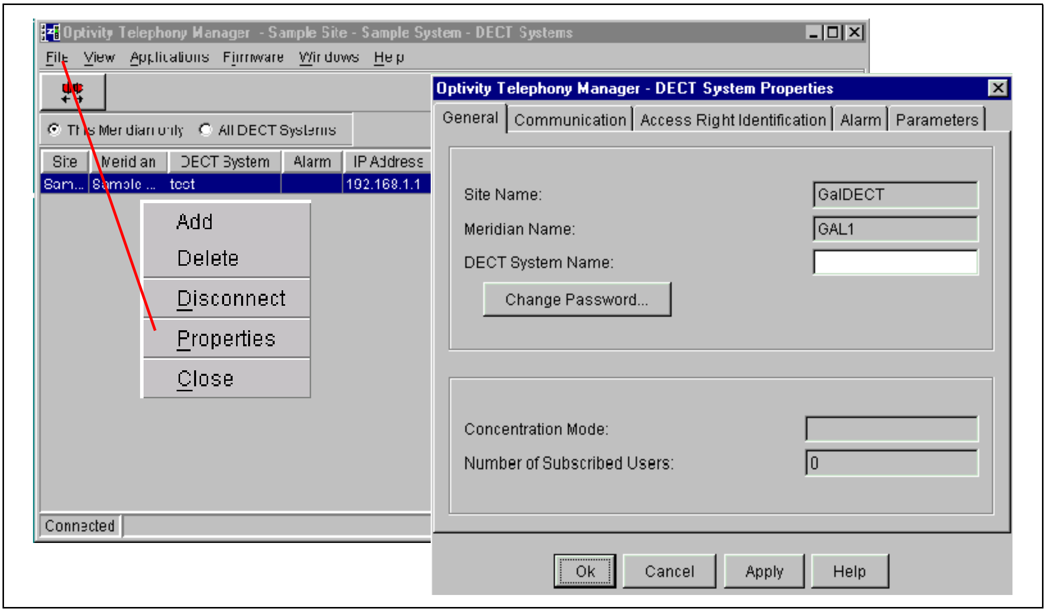
Procedure 152
Changing passwords

Step	Action
	Follow the instructions on page 443 to page 446.
3	Open the DECT Systems Properties dialog.
	From the **File** pull-down menu, click on **Properties**, and click on the **General** tab.
4	Select Change Password.
	Click on the **Change Password** button.
5	Change the password.
	Enter the **Old Password**, enter the **New Password** confirm the **New Password** and click **OK.**

END

Changing the DECT system name

Figure 271
DECT Systems window and DECT System Properties – General tab


Optivity Telephony Manager - Sample Site - Sample System - DECT Systems
File View Applications Firmware Windows Help
This Meridian only
All DECT Systems
Site Meridian DECT System Alarm IP Address
Sam... Sample ... test 192.168.1.1
Add
Delete
Disconnect
Properties
Close
Connected
Optivity Telephony Manager - DECT System Properties
General Communication Access Right Identification Alarm Parameters
Change Password...
Ok Cancel Apply Help

● This Meridian only ○ All DECT Systems

Site	Meridian	DECT System	Alarm	IP Address
Sam...	Sample ...	test		192.168.1.1

Site Name: GalDECT

Meridian Name: GAL1

DECT System Name:

Concentration Mode:

Number of Subscribed Users: 0

Complete the following steps.

Procedure 153
Changing the DECT system name

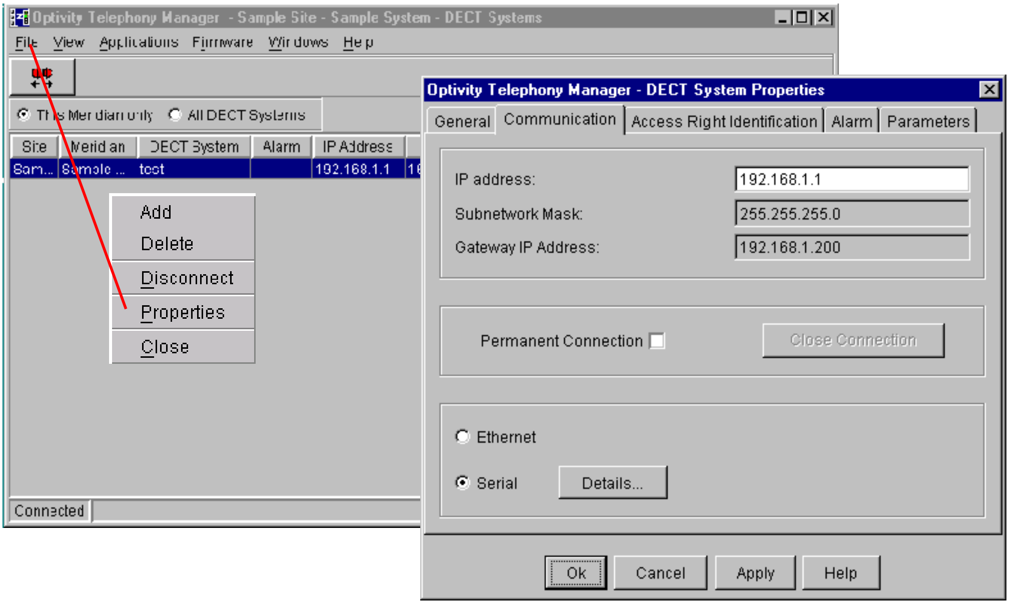
Step	Action
1	Using Windows, login to OTM. Select the system that supports the DECT system. Launch the DECT application. Open the DECT Systems window.
	Follow the instructions on page 440 to page 442.
2	Using a web-based navigator, open the Administrator login screen and login. Select the System Navigator. Select the system that supports the DECT system. Launch the DECT application. Open the DECT Systems window.
	Follow the instructions on page 443 to page 446.
3	Open the DECT Systems Properties dialog.
	From the **File** pull-down menu, click on **Properties**, and click on the **General** tab.
4	Change the DECT system name.
	Enter the new name in the DECT **System Name** box.

END

Changing the IP address on OTM DECT manager

Before changing the IP address on the OTM DECT manager, close the connection. After the change on the DECT system, open the connection as a safety check.

Figure 272
DECT Systems window and DECT System Properties – Communication tab



Optivity Telephony Manager - Sample Site - Sample System - DECT Systems

● This Meridian only ○ All DECT Systems

Site	Meridian	DECT System	Alarm	IP Address
Sam...	Sample ...	test		192.168.1.1

Connected

Optivity Telephony Manager - DECT System Properties

IP address: 192.168.1.1
Subnetwork Mask: 255.255.255.0
Gateway IP Address: 192.168.1.200

Permanent Connection □

○ Ethernet
● Serial

Complete the following steps.

Procedure 154
Changing the IP address on the DECT system

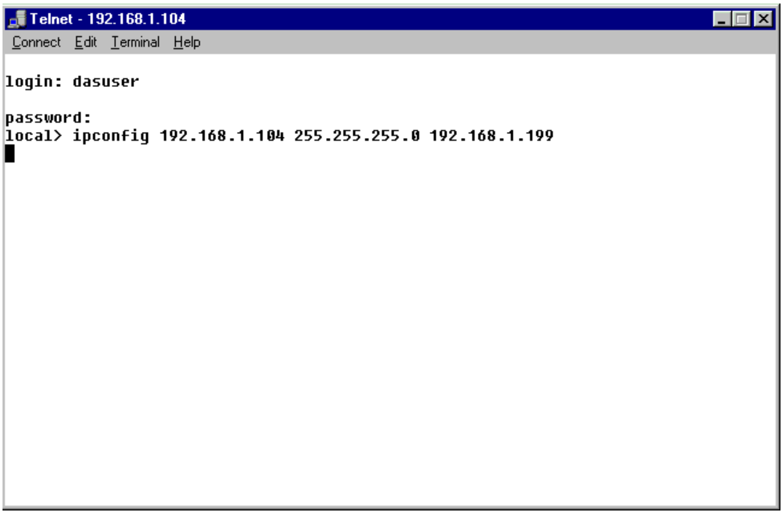
Step	Action
1	Using Windows, login to OTM. Select the system that supports the DECT system. Launch the DECT application. Open the DECT Systems window.
	Follow the instructions on page 440 to page 442.
2	Using a web-based navigator, open the Administrator login screen and login. Select the System Navigator. Select the system that supports the DECT system. Launch the DECT application. Open the DECT Systems window.
	Follow the instructions on page 443 to page 446.
3	Open the DECT Systems Properties dialog.
	From the **File** pull-down menu, click on **Properties**, and click on the **Communication** tab.
4	Select Ethernet.
	Click on the **Ethernet** radio button.
5	Accept the changes.
	Click **OK**.

END

Changing the IP address on the DECT system DMC8 Relay card

Before changing the IP address of the DMC8 Relay card through Telnet, close the connection. After the change on the DECT system, open the connection as a safety check.

Figure 273
Telnet 192.168.1.1



```
login: dasuser

password:
local> ipconfig 192.168.1.104 255.255.255.0 192.168.1.199
```

Complete the following steps.

Procedure 155
Changing IP address on DECT system DMC8 Relay card

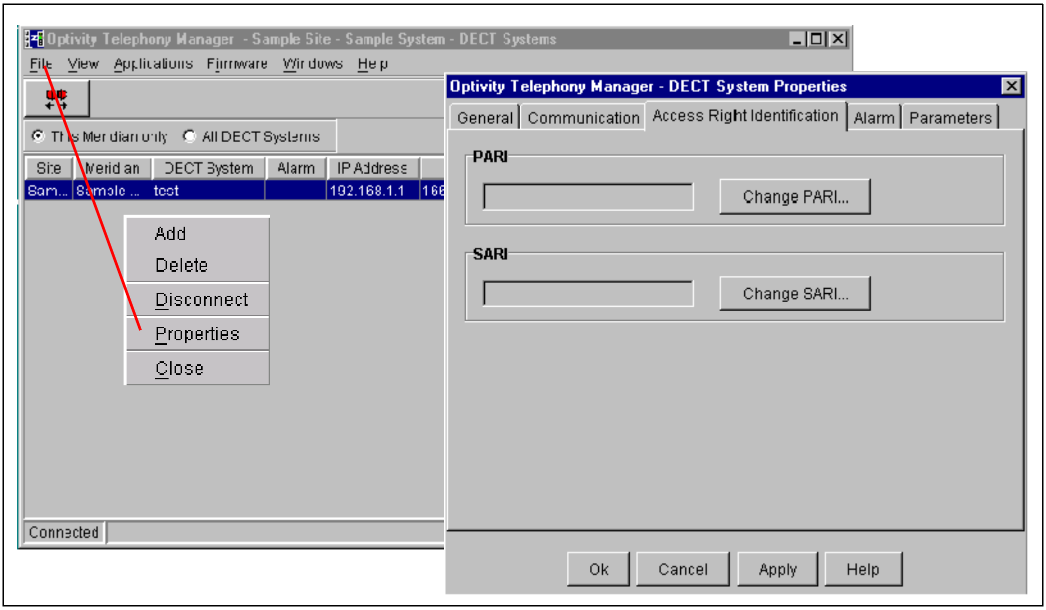
Step	Action
1	Open the Telnet dialog.
	Click **Start** on the Windows taskbar and choose **Accessories > Telnet**.
2	Enter username and password.
	Type username **dasuser** and password **dasuser**.
3	When the connection prompt **local** appears, change the DMC8 Relay card address.
	Enter the following command: **ipconfig xxx.xxx.xxx.xxx yyy.yyy.yyy.yyy zzz.zzz.zzz.zzz** **xxx.xxx.xxx.xxx** = new IP address of the DMC8 Relay card. **yyy.yyy.yyy.yyy** = subnet mask, usually **255.255.255.0** **zzz.zzz.zzz.zzz** = IP address if this is the gateway for the network. ***Note:*** Set **zzz.zzz.zzz.zzz** to the IP address of the OTM server Ethernet interface. If there are two Ethernet interfaces on the OTM server, set **zzz.zzz.zzz.zzz** to the IP address of the interface, which is on the same network as the DMC8 Relay card.

END

Changing a PARI or SARI

Note: When the PARI or SARI changes, the DECT system resets and the connection closes. If the connection is permanent, the OTM manager attempts to open in the background.

Figure 274
DECT Systems window and DECT System Properties – Access tab



Complete the following steps.

Procedure 156
Changing a PARI or SARI

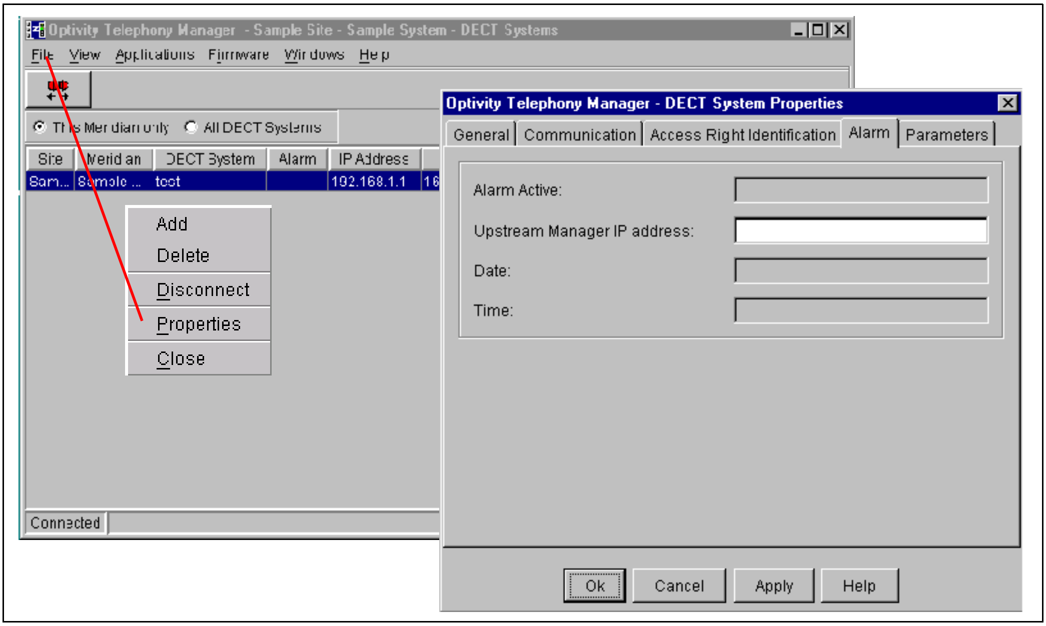
Step	Action
1	Using Windows, login to OTM. Select the system that supports the DECT system. Launch the DECT application. Open the DECT Systems window.
	Follow the instructions on page 440 to page 442.
2	Using a web-based navigator, open the Administrator login screen and login. Select the System Navigator. Select the system that supports the DECT system. Launch the DECT application. Open the DECT Systems window.
	Follow the instructions on page 443 to page 446.
3	Open the DECT Systems Properties dialog.
	From the **File** pull-down menu, click on **Properties**, and click on the **Access Right Identification** tab.
4	Change the PARI or SARI.
	Enter the **PARI** or **SARI**.
5	Accept the changes.
	Click on the **OK** button.

END

Changing the Upstream Manager IP address

Note: An upstream manager IP address can only be programmed on the DMC8 Relay card.

Figure 275
DECT Systems window and DECT System Properties – Alarm tab



Optivity Telephony Manager - Sample Site - Sample System - DECT Systems
File View Applications Firmware Windows Help
● This Meridian only ○ All DECT Systems
Site Meridian DECT System Alarm IP Address
Sam... Sample ... test 192.168.1.1 16
Add
Delete
Disconnect
Properties
Close
Connected
Optivity Telephony Manager - DECT System Properties
General Communication Access Right Identification Alarm Parameters
Alarm Active:
Upstream Manager IP address:
Date:
Time:
Ok Cancel Apply Help

Complete the following steps.

Procedure 157
Changing the Upstream Manager IP address

Step	Action
1	Using Windows, login to OTM. Select the system that supports the DECT system. Launch the DECT application. Open the DECT Systems window.
	Follow the instructions on page 440 to page 442.
2	Using a web-based navigator, open the Administrator login screen and login. Select the System Navigator. Select the system that supports the DECT system. Launch the DECT application. Open the DECT Systems window.
	Follow the instructions on page 443 to page 446.
3	Open the DECT Systems Properties dialog.
	From the **File** pull-down menu, click on **Properties**. Click the **Alarm** tab.
4	Change the Upstream Manager IP address.
	Enter the **Upstream Manager IP address**.
5	Accept the changes.
	Click on the **OK** button.

END

Changing the time and date

The time and date is used to time stamp the alarms.

> ***Note:*** The time and date must be changed when the DECT system reboots or a DMC resets.

Complete the following steps.

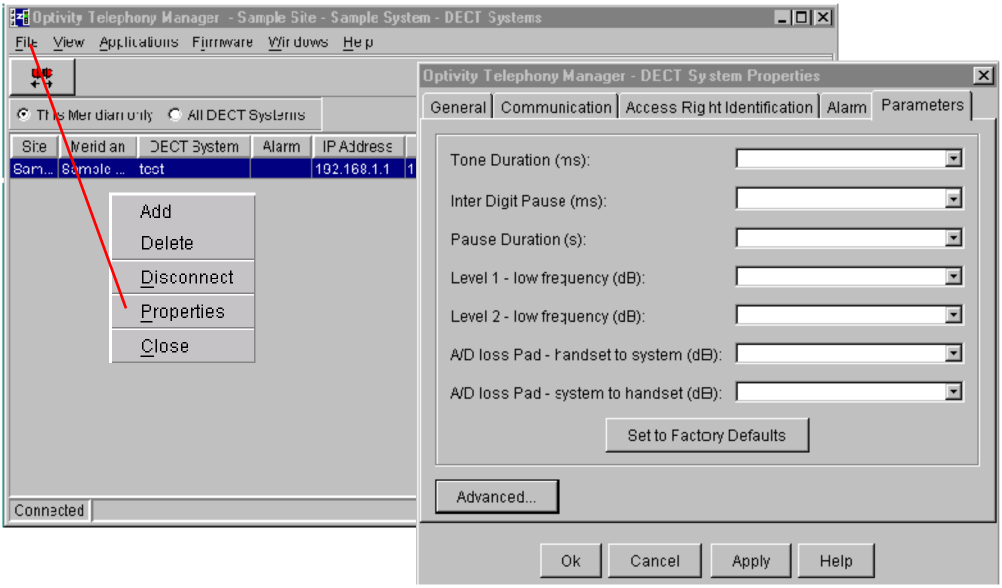
Procedure 158
Changing time and date

Step	Action
1	Using Windows, login to OTM. Select the system that supports the DECT system. Launch the DECT application. Open the DECT Systems window.
	Follow the instructions on, page 440 to page 442.
2	Using a web-based navigator, open the Administrator login screen and login. Select the System Navigator. Select the system that supports the DECT system. Launch the DECT application. Open the DECT Systems window.
	Follow the instructions on page 443 to page 446.
3	Connect to a DECT system.
	From the **Applications** pull-down menu click on **Connect** or 🟩 (green).
4	Open the DECT Systems Properties dialog.
	From the **File** pull-down menu, click on **Properties**. Click the **Alarm** tab as shown in Figure 275 on page 528.
5	Change the time and date.
	Enter the **Date** and **Time**.
6	Accept the changes.
	Click the **OK** button.

END

Changing parameters

Figure 276
DECT Systems window and DECT System Properties – Parameters tab


Optivity Telephony Manager - Sample Site - Sample System - DECT Systems
File View Applications Firmware Windows Help
This Meridian only
All DECT Systems
Site
Meridian
DECT System
Alarm
IP Address
Sam...
Sample ...
test
192.168.1.1
1
Add
Delete
Disconnect
Properties
Close
Connected
Optivity Telephony Manager - DECT System Properties
General
Communication
Access Right Identification
Alarm
Parameters
Tone Duration (ms):
Inter Digit Pause (ms):
Pause Duration (s):
Level 1 - low frequency (dB):
Level 2 - low frequency (dB):
A/D loss Pad - handset to system (dB):
A/D loss Pad - system to handset (dB):
Set to Factory Defaults
Advanced...
Ok
Cancel
Apply
Help

Complete the following steps.

Procedure 159
Changing parameters

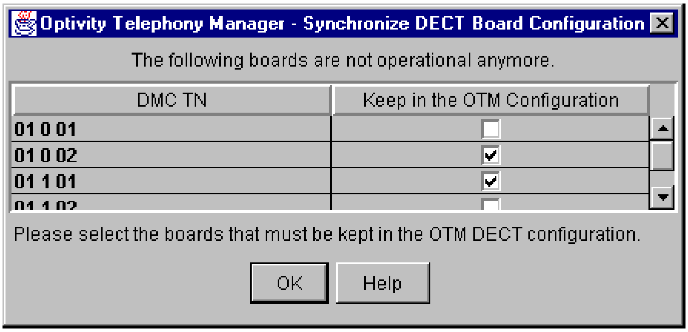
Step	Action
1	Using Windows, log in to OTM. Select the system that supports the DECT system. Launch the DECT application. Open the DECT Systems window.
	Follow the instructions on, page 440 to page 442.
2	Using a web-based navigator, open the Administrator login screen and login. Select the System Navigator. Select the system that supports the DECT system. Launch the DECT application. Open the DECT Systems window.
	Follow the instructions on page 443 to page 446.
3	Open the DECT System Properties dialog.
	From the **File** pull-down menu, click on **Properties**. Click the **Parameters** tab.
4	Change the parameters.
	From the appropriate pull-down menus, highlight the parameter time/level.
5	Accept the changes.
	Click the **OK** button.

END

Keeping or removing non-operational DMC8 cards from OTM

Note: Figure 277 on page 533 only appears when a connection is established and there is a mismatch. If there is a permanent connection and the DECT system configuration changes, the OTM DECT manager is updated automatically. The change is noted in the OTM event log.

Figure 277
Synchronize DECT Board Configuration window



Optivity Telephony Manager - Synchronize DECT Board Configuration

The following boards are not operational anymore.

DMC TN	Keep in the OTM Configuration
01 0 01	□
01 0 02	☑
01 1 01	☑
01 1 02	□

Please select the boards that must be kept in the OTM DECT configuration.

Complete the following steps.

Procedure 160
Managing non-operational DMC8 cards from OTM

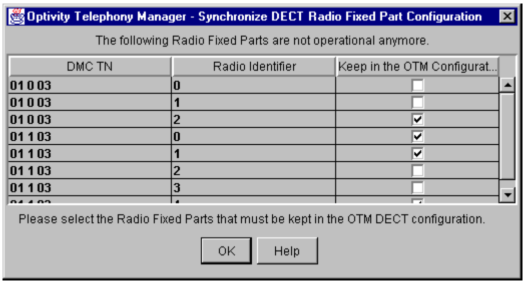
Step	Action
1	To keep DMC8 cards,
	Delete the check mark from the appropriate box.
2	To remove DMC8 cards,
	Put a check mark in the appropriate box.
3	Accept the changes.
	Click the **OK** button.

END

Keeping or removing non-operational basestations from OTM

> ***Note:*** Figure 278 only appears when a connection is established and there is a mismatch. If there is a permanent connection and the DECT system configuration changes, the OTM DECT manager is updated automatically and the change is noted in the OTM event log.

Figure 278
Synchronize DECT Radio Fixed Part Configuration window



Optivity Telephony Manager - Synchronize DECT Radio Fixed Part Configuration

The following Radio Fixed Parts are not operational anymore.

DMC TN	Radio Identifier	Keep in the OTM Configurat...
01 0 03	0	□
01 0 03	1	□
01 0 03	2	☑
01 1 03	0	☑
01 1 03	1	☑
01 1 03	2	□
01 1 03	3	□

Please select the Radio Fixed Parts that must be kept in the OTM DECT configuration.

Complete the following steps.

Procedure 161
Managing non-operational basestations from OTM

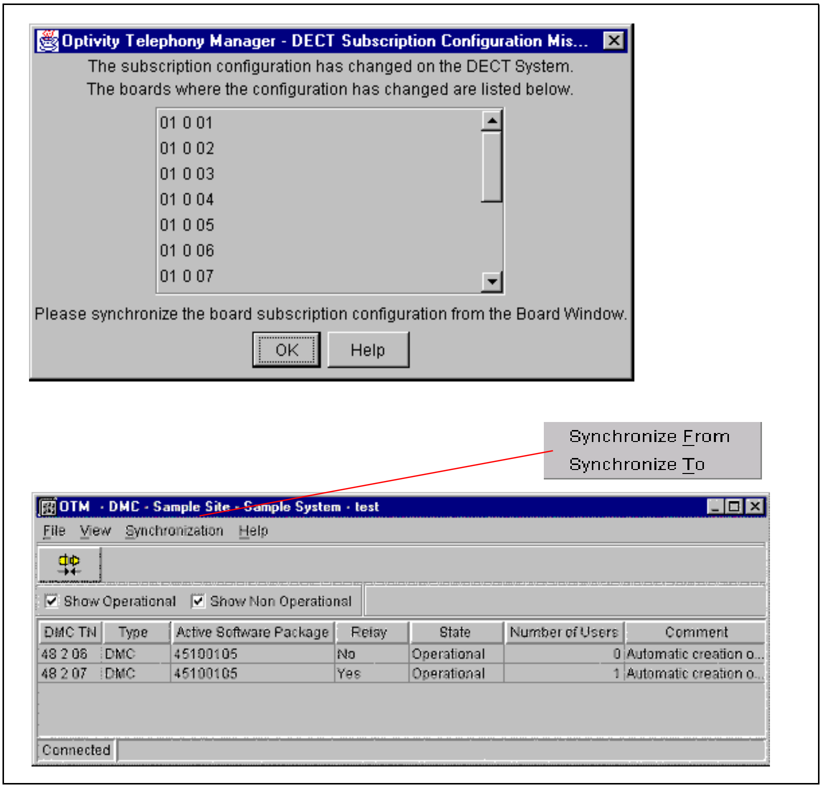
Step	Action
1	To keep basestations,
	Delete the check mark from the appropriate box.
2	To remove basestations,
	Put a check mark in the appropriate box.
3	Accept the changes.
	Click the **OK** button.

END

Resolving a subscription configuration mismatch

> *Note:* The window shown in Figure 279 opens when subscriptions are enabled with the Subscriptions window Operation pull-down menu and clicking on Configure.

Figure 279
DECT Subscriptions Configuration Mismatch window and DMC window



Optivity Telephony Manager - DECT Subscription Configuration Mis...

The subscription configuration has changed on the DECT System.
The boards where the configuration has changed are listed below.

01 0 01
01 0 02
01 0 03
01 0 04
01 0 05
01 0 06
01 0 07

Please synchronize the board subscription configuration from the Board Window.

OK
Help
Synchronize From
Synchronize To
OTM - DMC - Sample Site - Sample System - test
File
View
Synchronization
Help

☑ Show Operational ☑ Show Non Operational

DMC TN	Type	Active Software Package	Relay	State	Number of Users	Comment
48 2 06	DMC	45100105	No	Operational	0	Automatic creation o...
48 2 07	DMC	45100105	Yes	Operational	1	Automatic creation o...

Connected

Complete the following steps.

Procedure 162
Selecting login options

Step	Action
1	Using Windows, login to OTM. Select the system that supports the DECT system. Launch the DECT application. Open the DECT Systems window.
	Follow the instructions on page 440 to page 442.
2	Using a web-based navigator, open the Administrator login screen and login. Select the System Navigator. Select the system that supports the DECT system. Launch the DECT application. Open the DECT Systems window.
	Follow the instructions on page 443 to page 446.
3	Open the DMC window.
	Follow the instructions on page 448.
4	Store DMC changes from the DECT system in the OTM server,
	In the **Synchronization** pull-down menu, click on **Synchronize From**.
5	Make OTM server changes to the DMCs in the DECT system,
	In the **Synchronization** pull-down menu, click on **Synchronize To**.

END

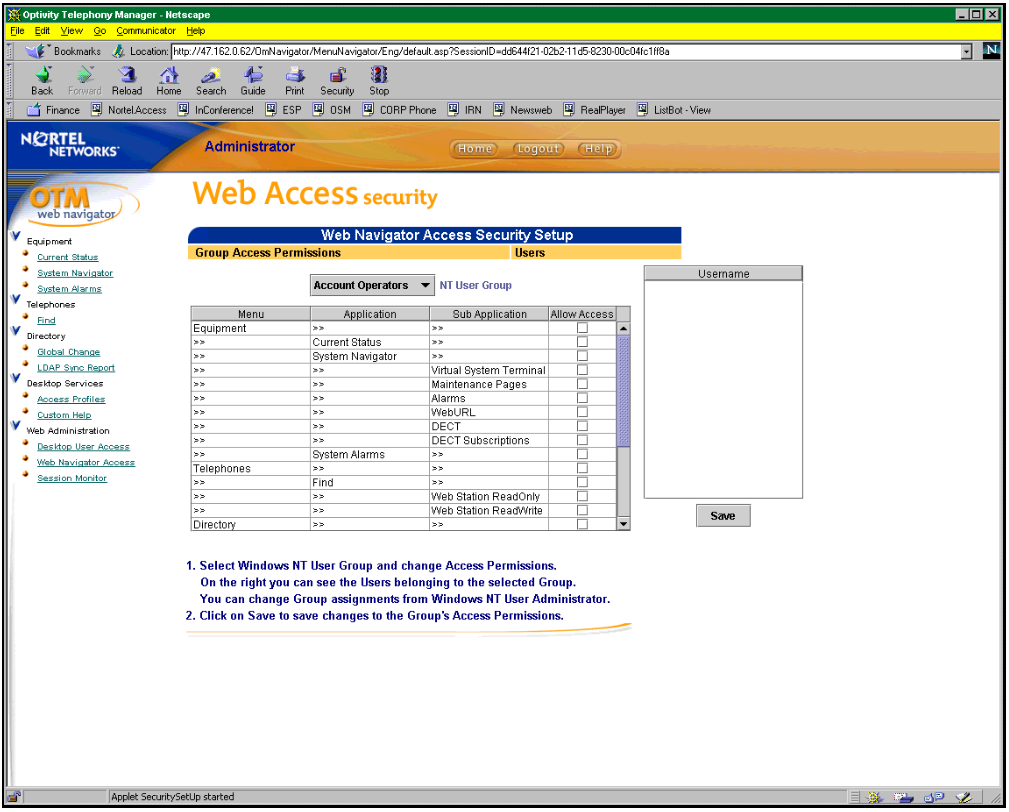
User Access security

Security can be accessed either through a web-based navigator or through Windows.

Web-based navigator Access security

Group access to DECT OA&M features or DECT handset subscriptions can be allowed or denied with the Web Access security window.

Figure 280
OTM Web Access security


Optivity Telephony Manager - Netscape
File Edit View Go Communicator Help
Bookmarks Location: http://47.162.0.62/OmNavigator/MenuNavigator/Eng/default.asp?SessionID=dd644f21-02b2-11d5-8230-00c04fc1ff8a
Back Forward Reload Home Search Guide Print Security Stop
Finance NortelAccess InConference! ESP OSM CORP Phone IRN Newsweb RealPlayer ListBot - View
NORTEL NETWORKS
Administrator
Home Logout Help
OTM web navigator
Equipment
Current Status
System Navigator
System Alarms
Telephones
Find
Directory
Global Change
LDAP Sync Report
Desktop Services
Access Profiles
Custom Help
Web Administration
Desktop User Access
Web Navigator Access
Session Monitor
Applet SecuritySetUp started

Web Access security

Web Navigator Access Security Setup

Group Access Permissions | Users

Account Operators ▼ NT User Group

Menu	Application	Sub Application	Allow Access
Equipment	>>	>>	□
>>	Current Status	>>	□
>>	System Navigator	>>	□
>>	>>	Virtual System Terminal	□
>>	>>	Maintenance Pages	□
>>	>>	Alarms	□
>>	>>	WebURL	□
>>	>>	DECT	□
>>	>>	DECT Subscriptions	□
>>	System Alarms	>>	□
Telephones	>>	>>	□
>>	Find	>>	□
>>	>>	Web Station ReadOnly	□
>>	>>	Web Station ReadWrite	□
Directory	>>	>>	□

Username

Save

1. Select Windows NT User Group and change Access Permissions.
   On the right you can see the Users belonging to the selected Group.
   You can change Group assignments from Windows NT User Administrator.
2. Click on Save to save changes to the Group's Access Permissions.

Complete the following steps.

Procedure 163
Accessing security – web-based navigator

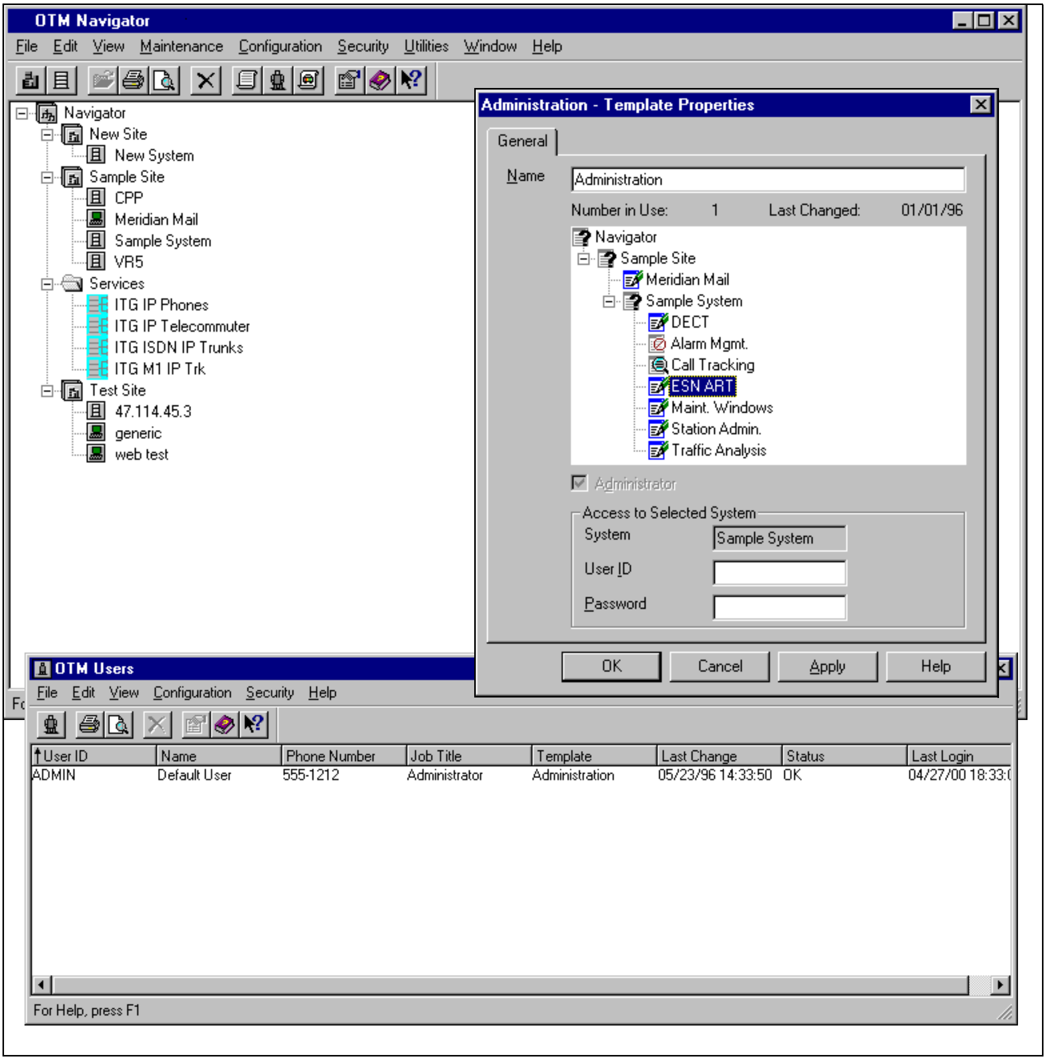
Step	Action
1	Using Windows, login to OTM. Select the system that supports DECT. Launch the DECT application. Open the DECT Systems window.
	Follow the instructions on page 443 to page 446.
2	Select Web Navigator Access.
	Click on **Web Navigator Access**.
3	Follow the on-screen instructions.
	A check in the Allow Access column boxes permits access for the selected users group. No check in the boxes denies access to the selected users group.

END

Windows Access security

Allow or deny Group access to DECT OA&M features with the Windows Administration – Template Properties dialog.

Figure 281
OTM Navigator, OTM Users, and Template Properties



Name: Administration

Number in Use: 1 Last Changed: 01/01/96

☑ Administrator

Access to Selected System

System: Sample System

User ID:

Password:

User ID	Name	Phone Number	Job Title	Template	Last Change	Status	Last Login
ADMIN	Default User	555-1212	Administrator	Administration	05/23/96 14:33:50	OK	04/27/00 18:33:(

Complete the following steps.

Procedure 164
Accessing security – Windows

Step	Action
1	Using Windows, login to OTM to open the OTM Navigator window.
	See “Logging into the OTM” on page 440.
2	Open the OTM Users window.
	From the **Security** pull-down menu, click on **OTM Users**.
3	Open the Template Properties.
	From the **Configuration** pull-down menu, click on **User Templates**.
4	Select the appropriate access level for the user group.
	Left-click on the icon to change the access, as follows: ✎ – Read and write access 🔍 – Read only access* ⊘ – No access ***Note:*** * Choosing read only access allows read and write access.

END

Troubleshooting

This section provides information to help solve common problems.

Disconnecting

The passwords on a DMC8 Relay card and a system on the OTM DECT must match.

The default password for both a DMC8 Relay card and an OTM DECT system is **Arsenal**.

If the password on a DMC8 Relay card is not the same as the OTM DECT password, OTM is not able to connect to the relay card. If the DMC8 Relay card is rebooted, the mismatched password is accepted for only five minutes. Then the card disconnects again.

To solve the problem, ensure the password on the system in OTM DECT and the password on the DMC8 Relay card are the same.

Nortel recommends that the passwords be reset to the default **Arsenal**.

To change the OTM DECT password, see “Changing passwords” on page 518.

> ***Note:*** Select the option Do not change password on the DECT system.

To change the password on the DMC8 relay card, see “Recovering a password” on page 611.

> ***Note:*** Do **not** select the option Do not change password on the DECT system.

System maintenance

Contents

This section contains information on the following topics:

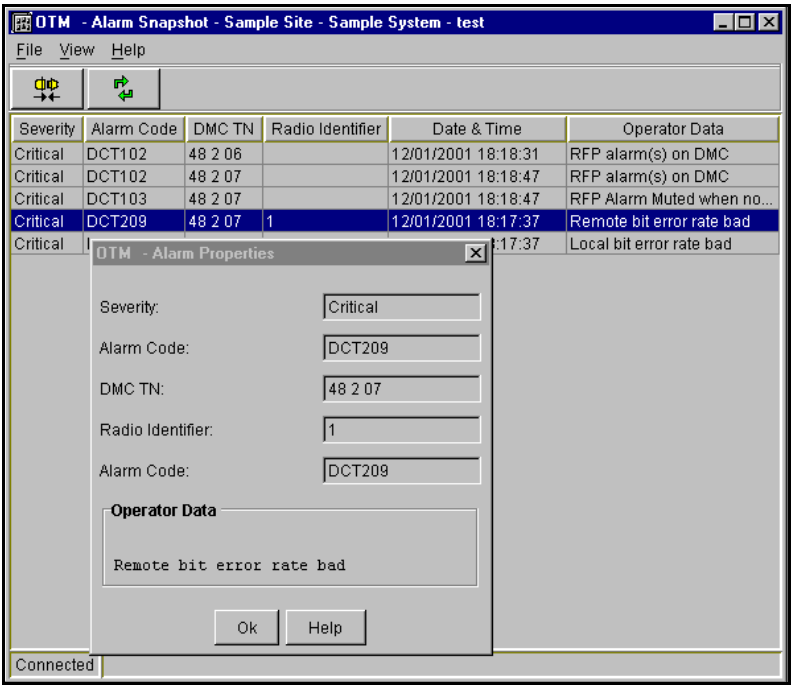
Alarm Code maintenance actions

Alarm Codes can be viewed with one of the following:

- “Windows Alarm Snapshot” on page 544
- “Web Alarm browser” on page 552
- “Windows Alarm Notification” on page 554

Windows Alarm Snapshot

Figure 282
Alarm Snapshot window and Alarm Properties window



Severity	Alarm Code	DMC TN	Radio Identifier	Date & Time	Operator Data
Critical	DCT102	48 2 06		12/01/2001 18:18:31	RFP alarm(s) on DMC
Critical	DCT102	48 2 07		12/01/2001 18:18:47	RFP alarm(s) on DMC
Critical	DCT103	48 2 07		12/01/2001 18:18:47	RFP Alarm Muted when no...
Critical	DCT209	48 2 07	1	12/01/2001 18:17:37	Remote bit error rate bad
Critical				:17:37	Local bit error rate bad

Severity:	Critical
Alarm Code:	DCT209
DMC TN:	48 2 07
Radio Identifier:	1
Alarm Code:	DCT209

Operator Data

```
Remote bit error rate bad
```

Note: The Alarm Snapshot window is a static display. The Alarm Snapshot window only shows the alarms present at the time the window was opened. The window must be refreshed for an up-to-date display. The web-based alarm browser displays alarm history and occurring alarms.

Complete the following steps.

Procedure 165
Alarm Code maintenance actions

Step	Action
1	Using Windows, and login to OTM. Select the system that supports the DECT system. Launch the DECT application. Open the DECT Systems window. Open the Current Alarms window.
	Follow the instructions on page 440 to page 449.
2	Refresh the Alarm Snapshot window.
	Click on the ⟳ icon.
3	Examine the alarm code, and take the appropriate maintenance action.
	See Table 166 on page 553.

END

Note: The Windows Alarm Notification browser (page 554) only displays alarms that have occurred since the window was opened. The Web Alarm browser (page 552) has a circular log that provides information on a limited history of alarms. The Web Alarm browser records alarms at all times.

Table 31
Alarms (Part 1 of 6)

Alarm code	Alarm description	Maintenance action
DMC8 operational state Synthesis		
DCT001	All DMC8 cards are operational. (DCT001 only displayed in the Alarm browsers. DCT001 does not show in the Alarm Snapshot list.)	Information only, no action needed.
DCT002	At least one DMC8 card is not operational. (DCT002 only displayed in the Alarm browsers. DCT002 does not show in the Alarm Snapshot list.)	Remove the DMC8 and insert the DMC8 again to reboot. If the reboot fails, replace the DMC8.
Note: When at least one DMC8 card becomes inoperable, DCT002 appears in the alarm browser history. When all the DMC8 cards become operational again, DCT001 appears in the browser history.		
Presence of an alarm		
DCT101	No alarms. (DCT101 only displayed in the Alarm browsers).	Information only, no action needed.
DCT102	**1** DCT102 displayed in the Alarm browsers is an alarm on a DMC8. **2** DCT102 displayed in the Alarm Snapshot is an alarm on a basestation.	**1** Open the Alarm Snapshot window for alarm details and perform the corresponding maintenance actions. **2** Look for one or more DCT202 to DCT215 alarms in the Alarm Snapshot window, and perform the corresponding maintenance actions.
DCT103	Basestation alarm muted when no alarms. Look for one or more DCT501 alarms for details.(DCT103 only displayed in the Alarm Snapshot window.)	Configure the basestation using the OTM, or disconnect the basestation.

Table 31
Alarms (Part 2 of 6)

Alarm code	Alarm description	Maintenance action
DCT104	Faceplate cable alarms on DMC8. Look for one or more DCT302 to DCT307 alarms for details.(DCT104 only displayed in the Alarm Snapshot window.)	Perform the DCT302 to DCT307 maintenance action.
DCT105	Software alarms on DMC8. Look for one or more DCT401 to DCT403 alarms for details. (**DCT105** only displayed in the Alarm Snapshot window.)	Perform the DCT402 to DCT407 maintenance action.
Basestation alarms		
DCT201	No basestation alarm. (DCT201 only displayed in the Alarm browsers.)	Information only, no action needed.
DCT202	Local receiver signal missing (basestation disconnected). If a re-connection does not solve the problem, check: **1** the basestation **2** the DMC8 cards in the basestation **3** for a cable problem between the basestation and a DMC8 card.	Disconnect the basestation for 30 seconds. **1** Replace the basestation. **2** Replace the DMC8 cards in the basestation. **3** Check the faceplate cabling.
DCT203	Local loss of receiver slot synchronization.	Perform the DCT202 maintenance action.
DCT204	Local loss of receiver frame synchronization.	Perform the DCT202 maintenance action.
DCT205	Local bit error rate bad.	Perform the DCT202 maintenance action.
DCT206	Remote receiver signal missing.	Perform the DCT202 maintenance action.

Table 31
Alarms (Part 3 of 6)

Alarm code	Alarm description	Maintenance action
DCT207	Remote loss of receiver slot synchronization.	Perform the DCT202 maintenance action.
DCT208	Remote loss of receiver frame synchronization.	Perform the DCT202 maintenance action.
DCT209	Remote bit error rate bad.	Perform the DCT202 maintenance action.
DCT210	Synthesizer out of synchronization.	Perform the DCT202 maintenance action.
DCT211	Power amp out of order.	Perform the DCT202 maintenance action.
DCT212	Round-trip delay changed.	Perform the DCT202 maintenance action.
DCT213	RFP synthesizer type changed.	Perform the DCT202 maintenance action.
DCT214	LFC out of synchronization with BMC.	Disconnect and reinsert the DMC8.
DCT215	Error due to synchronization-port mutation.	Can affect the interpretation of the alarm snapshot or alarm browser applications; however, the alarm must clear automatically within 200 seconds.
Faceplate cable alarms		
DCT301	No faceplate cable alarm. (DCT301 only displayed in the Alarm browsers.	Information only, no action needed.
DCT302	The DMC8card is working; however, there is a loss of faceplate cable synchronization.	Remove all the DMC8s. Check the strap setting on the DMC8s. Check the faceplate cabling. Reinsert all the DMC8 cards. If the above procedure does not solve the problem, try to find which DMC8 card gives the error condition by inserting the DMC8 cards one at a time with a minute in between insertions. If needed, replace the defective DMC8 card or the defect faceplate cables.

Table 31
Alarms (Part 4 of 6)

Alarm code	Alarm description	Maintenance action
DCT303	No faceplate cable synchronization found. The DMC8 card responsible for this alarm cannot pass the alarm on to the DMC8 Relay card.	Perform the DCT302 maintenance action.
DCT304	The DMC8 card is working; however, a user connected a faceplate cable section to the DMC8, causing a counter difference.	Do not connect faceplate cables to a DMC8 on an active DECT system.
DCT305	The DMC8 card is working; however, there is a timing signal loss within the DMC8.	Perform the DCT302 maintenance action.
DCT306	The DMC8 card is working; however, the input of the faceplate cable controller is locked.	Perform the DCT302 maintenance action.
DCT307	The DMC8 card is working; however, the processor is overloaded with too many faceplate cable messages, causing an I/O transmit overflow.	Perform the DCT302 maintenance action. If the DCT302 action does not solve the problem, try provisioning an additional DMC8.
Software alarms		
DCT401	The DMC8 card is working; however, there is a subscription database corruption.	In the Boards window, **Synchronize From** the DMC8, then **Synchronize To** the DMC8.

Table 31
Alarms (Part 5 of 6)

Alarm code	Alarm description	Maintenance action
DCT402	The DMC8 card is located in a card slot position that does not match the DMC8 card subscription data card slot address. The mismatch is due to one of the following: • the DMC8 card is placed in the wrong card slot position • the DMC8 card does not come into service	Perform the DCT401 maintenance action.
DCT403	Duplicate subscription in the system. A subscription is moved from a source DMC8 card to a destination DMC8 card; however, the original subscription is still present on the source DMC8 card. The DCT403 alarm must always come from both the source and destination DMC8 cards.	Perform the DCT401 maintenance action. If the problem does not clear, look for duplicated subscription IPUI in the Subscription Property dialog. Delete the unnecessary subscription from the source DMC8.
DCT404	(DCT404 only displayed in the Alarm browsers.) One of the following events occurred: • the power was turned on • the DMC8 was inserted into the shelf backplane • a software exception restarted the DMC8	If this alarm was caused by a software exception, examine the alarm browsers for details.

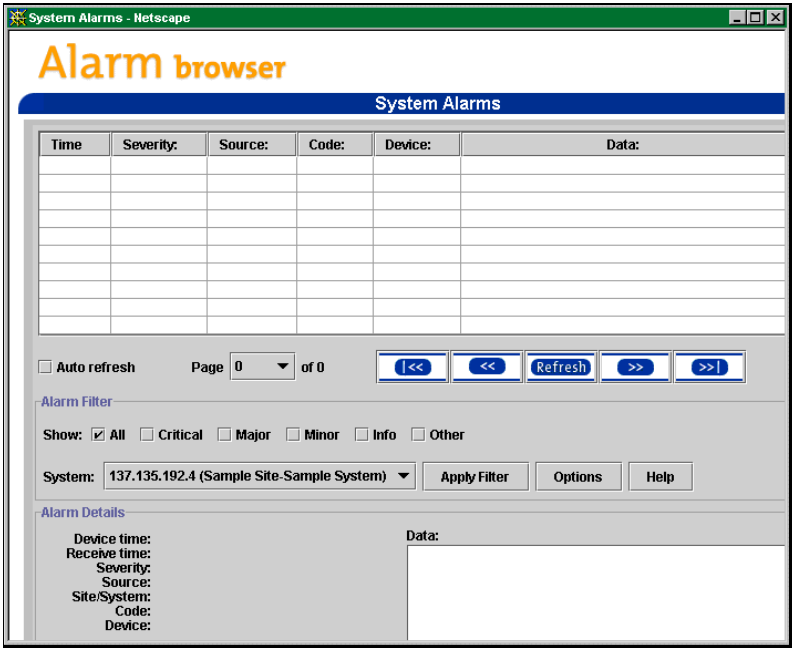
Table 31
Alarms (Part 6 of 6)

Alarm code	Alarm description	Maintenance action
Radio Fixed Part alarm muted		
DCT501	Alarms are muted in the RFP window, however the basestation does not have any intrinsic alarms.	Use the RFP window to **Cancel Mute Alarms**.
Backplane controller unit		
DCT601	This alarm is used by Nortel designers.	Information only, no action needed.

Web Alarm browser

The web Alarm browser has a circular log that provides information on a limited history of alarms. The Web Alarm browser records alarms at all times.

Figure 283
OTM web System Alarm browser



Time	Severity:	Source:	Code:	Device:	Data:

□ Auto refresh Page 0 of 0

Alarm Filter

Show: ☑ All □ Critical □ Major □ Minor □ Info □ Other

System: 137.135.192.4 (Sample Site-Sample System)

Alarm Details

Device time:
Receive time:
Severity:
Source:
Site/System:
Code:
Device:

Data:

Complete the following steps.

Procedure 166
Alarm Code maintenance actions

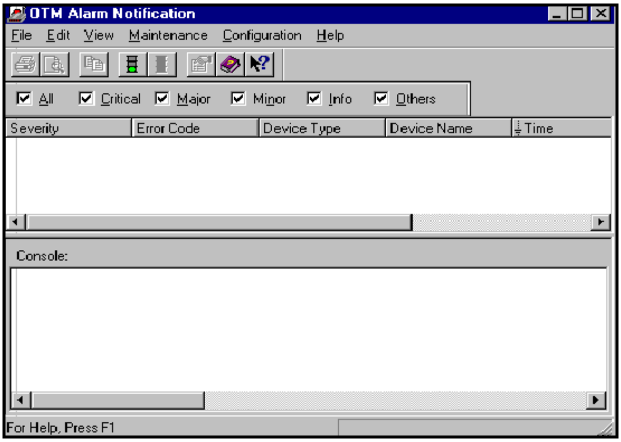
Step	Action
1	Using a web-based navigator, open the login screen and log in. Select the System Navigator. Select the system that supports the DECT system. Select Alarms.
	Follow the instructions on page 443 to page 446.
2	Examine the code, and take the appropriate maintenance action.
	See Table 31 on page 546.

END

Windows Alarm Notification

Alarm Notification provides an alert by pagers, e-mail, and forwards SNMP traps to an upstream processor. For more information about the Alarm Notification, see *Telephony Manager: System Administration* (553-3001-330).

Figure 284
Alarm Notification


OTM Alarm Notification
File Edit View Maintenance Configuration Help
☑ All ☑ Critical ☑ Major ☑ Minor ☑ Info ☑ Others
Severity
Error Code
Device Type
Device Name
Time
Console:
For Help, Press F1

Complete the following steps.

Procedure 167
Alarm Notification

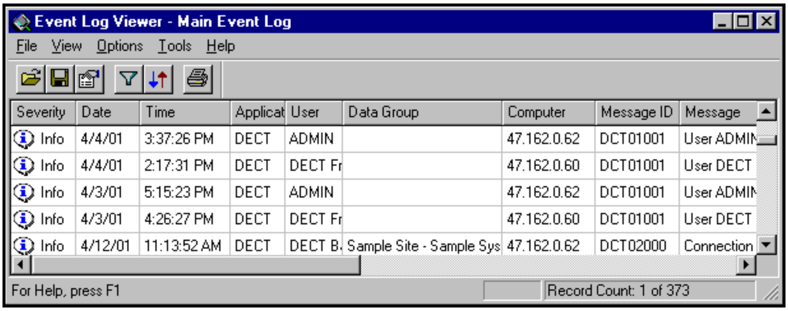
Step	Action
1	Using Windows, open the login screen, login, select the Alarm Notification from the Utilities menu of the OTM Windows Navigator.
	Follow the instructions on, page 443 to page 446.
2	Examine the Message ID, and take the appropriate maintenance action.
	See Table 31 on page 546.

END

Event Monitor window

The Event Monitor window displays the system's Event Log, allowing all recent system events stored in the history file to be viewed. For more information about the Alarm management, see *Telephony Manager: System Administration* (553-3001-330).

Figure 285
Event Log



Severity	Date	Time	Applicat	User	Data Group	Computer	Message ID	Message
Info	4/4/01	3:37:26 PM	DECT	ADMIN		47.162.0.62	DCT01001	User ADMIN
Info	4/4/01	2:17:31 PM	DECT	DECT Fr		47.162.0.60	DCT01001	User DECT
Info	4/3/01	5:15:23 PM	DECT	ADMIN		47.162.0.62	DCT01001	User ADMIN
Info	4/3/01	4:26:27 PM	DECT	DECT Fr		47.162.0.60	DCT01001	User DECT
Info	4/12/01	11:13:52 AM	DECT	DECT B.	Sample Site - Sample Sys	47.162.0.62	DCT02000	Connection

For Help, press F1

Record Count: 1 of 373

Complete the following steps.

Procedure 168
Event Log

Step	Action
1	Using Windows, login to OTM. Select the Event Log Viewer from the Maintenance menu of OTM Windows Navigator.
	Follow the instructions on page 443 to page 446.
2	Examine the Application column.
	DECT indicates a DECT event.
3	Examine the Data Group column.
	Gives the Site name, PBX name, DECT name.

Procedure 168
Event Log

Step	Action
4	Examine the Message ID column.
	Non-error logs range from 1 to 9999. Error logs range from 10000 to 19999.
5	Examine the Message column.
	Messages are the explanation of Message ID number codes.

END

LED status for DMC8/DMC8-E and basestation

The system LED status indicates the functioning of the DMC8/DMC8-E, basestation power and card subsystem operation.

Table 32
DMC8/DMC8-E red LED status

Red LED State	Description	Action
On	The card is in one of the following states: **1** not programmed **2** disabled **3** has faults	**1** Program the card. See page 535. **2** Re-enable the card. Use LD 32 ENLC l s c. **3** Replace the card. See page 559.
Flashes three times	Card is doing a self test.	Wait.
Off	**1** The card is in service if the yellow LED is off and the green LED is on. **2** The card has no power if all LEDs are off.	**1** No action. **2** Restore power.

Table 33
DMC8/DMC8-E yellow/green LED status (Part 1 of 2)

Yellow LED Status	Green LED Status	Description	Action
Off	Off	Power down.	Restore power.
On	Off	Hardware testing by boot program.	Wait.
On	On	Wait for download command by the boot program.	Wait.
On	Loop‡	No valid main program found by the boot program. Card is continuously restarting.	Start firmware distribution with the DECT Manager.
Slow flash†	On	Faults caused by one of the following: • software download in progress • software distribution in progress • subscription or configuration data is saving to the flash ROM	Wait. Do not remove the card, removal corrupts the flashROM data.
Off	Fast flash††	Card is synchronizing to the faceplate cable bus.	Wait.

Legend for LED action:
† Slow flash = 2 seconds On and 2 seconds Off
††Fast flash = 1 second On and 1 second Off
‡ Loop for no program = 3 seconds On and 0.25 seconds Off
‡ Loop for corrupted program = 12 seconds On and 0.25 seconds Off

Table 33
DMC8/DMC8-E yellow/green LED status (Part 2 of 2)

Yellow LED Status	Green LED Status	Description	Action
Off	Slow flash†	**1** Card has no PARI, or has an incomplete PARI. **2** Card has detected an error.	**1** Contact the technical support group. **2** Replace the card. See page 559.
Off	On	Card is in service.	No action required.
Slow flash†	Slow flash†	Simultaneous occurrence of: • card has no PARI, or incomplete PARI and • either software distribution is in progress or subscription or configuration data is saving to the flashROM	Contact the technical support group.
Legend for LED action: **† Slow flash = 2 seconds On and 2 seconds Off** **††Fast flash = 1 second On and 1 second Off** **‡ Loop for no program = 3 seconds On and 0.25 seconds Off** **‡ Loop for corrupted program = 12 seconds On and 0.25 seconds Off**			

Table 34
Basestation LED status

Green	Description	Action
Off	No power.	Check DMC8 to basestation cables.
Flashes	Input power present but no output power.	Check DMC8 LED Status and Alarm Reports. Check DMC8 to basestation cables.
On	Power present and communication with DMC8 established.	No action required.

Removing and inserting a DMC8 for maintenance

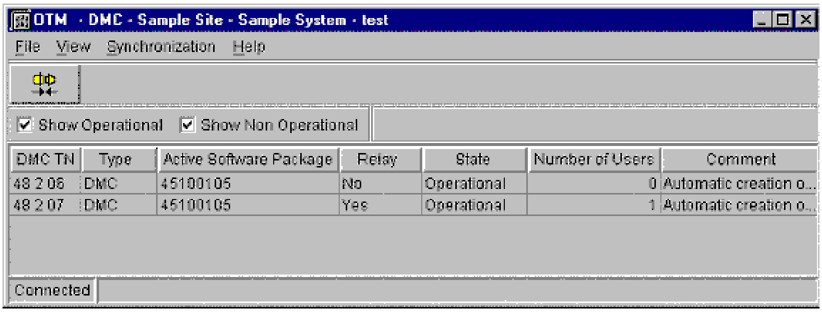
> **CAUTION — Service Interruption**
>
> Do not bypass the DMC8-E or the DMC8 immediately to the left of the DMC8-E. A bypassed DMC8-E cannot regenerate the faceplate bus signals in the left half of the shelf.
>
> Although the separated left half of the shelf remains in synchronization, system performance decreases as follows:
>
> - Any calls passing through the separated part of the faceplate bus are dropped.
> - Handsets configured on a DMC in the separated half cannot make or receive calls through a basestation in the other half.

To remove, re-seat, or insert DMC8 card, perform the following actions:

- Backup the data from the DMC8 card to be removed.
- Remove the faulty DMC8 card.
- Insert a working DMC8 card.
- Restore the data to the DMC8 card that was replaced.

Backing up a DMC8 card configuration and subscription information

Figure 286
DMC window


OTM - DMC - Sample Site - Sample System - test
File View Synchronization Help
☑ Show Operational ☑ Show Non Operational

DMC TN	Type	Active Software Package	Relay	State	Number of Users	Comment
48 2 06	DMC	45100105	No	Operational	0	Automatic creation o...
48 2 07	DMC	45100105	Yes	Operational	1	Automatic creation o...

Connected

Complete the following steps.

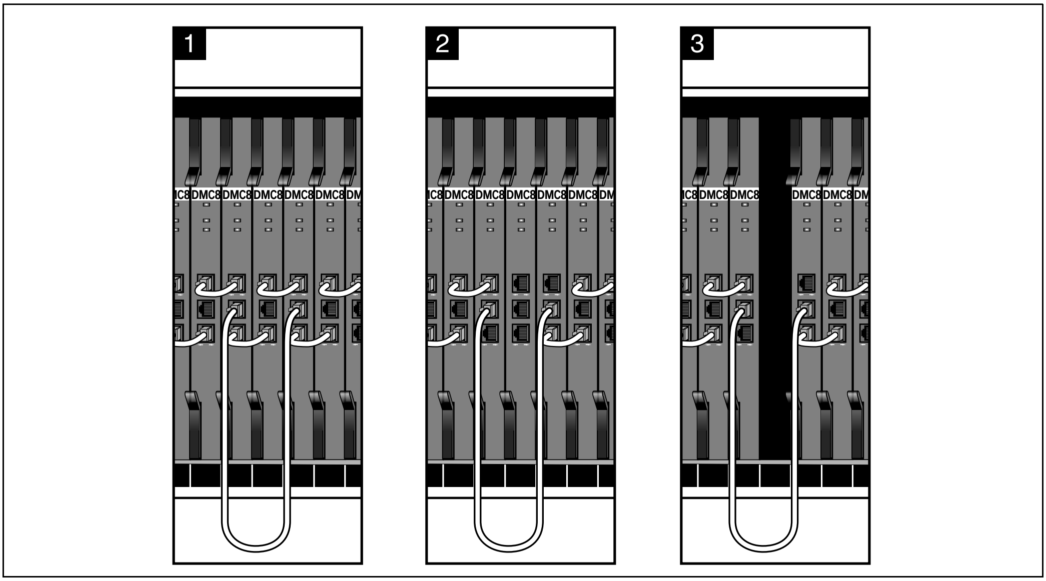
Procedure 169
Backing up a DMC8 card information

Step	Action
1	Using Windows, login to OTM. Select the system that supports the DECT system. Launch the DECT application. Open the DECT Systems window. Open the Boards window.
	Follow the instructions on page 440 to page 449.
2	Select the DMC8 card.
	Highlight the DMC8 card in the list.
3	Save the DMC8 data on the OTM.
	From the **Synchronization** pull-down menu, click on **Synchronize From**.

END

Removing a faulty DMC8 card

Figure 287
DMC8 card removal



Complete the following steps.

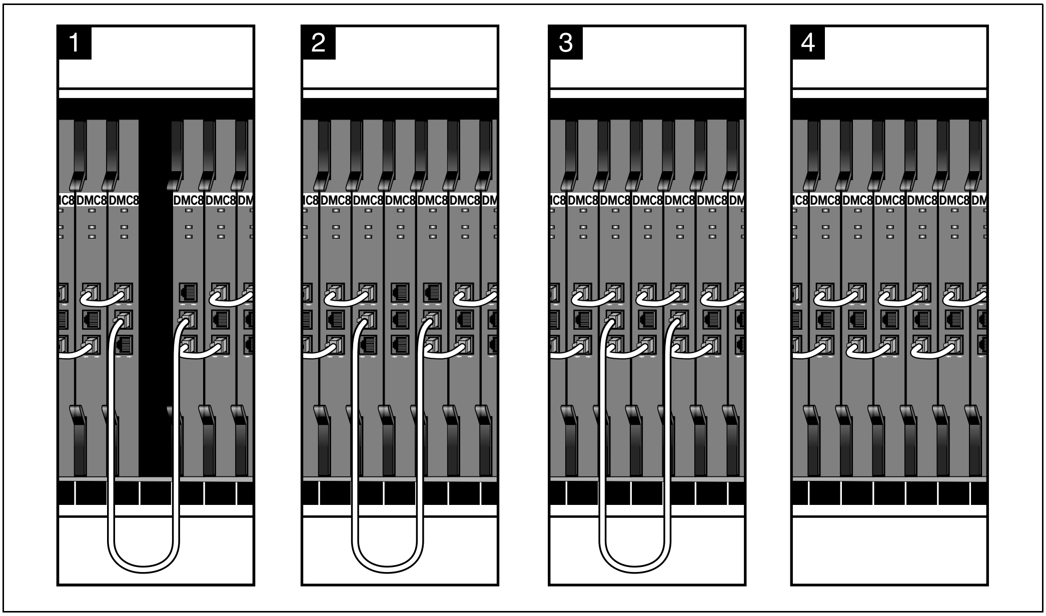
Procedure 170
Removing a faulty DMC8 card

Step	Action
1	Connect the maintenance bypass cable.
	Plug the maintenance bypass cable into the **Maint** port of the DMC8 cards on either side of the DMC8card to be removed.
2	Disconnect the faceplate cables.
	Detach the faceplate cables from the DMC8 card to be removed and from the cards on either side of it.
3	Remove the DMC8.
	Release the card locking devices and lever the card out of the shelf backplane.

END

Inserting a serviceable DMC8 card

Figure 288
DMC8 card insertion



Complete the following steps.

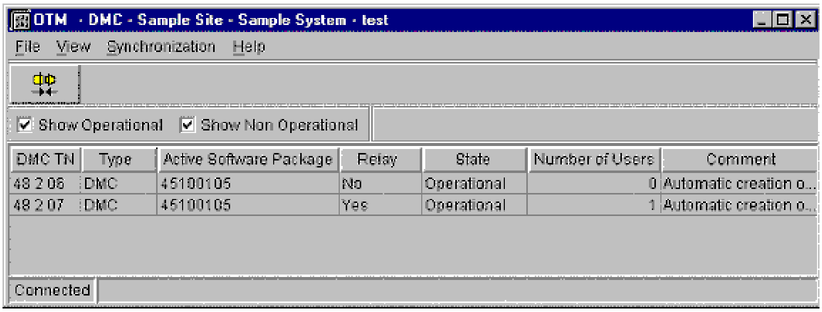
Procedure 171
Inserting a serviceable DMC8 card

Step	Action
1	Insert the DMC8 card.
	Lever the card into the shelf backplane and latch the card locking devices.
2	Connect the faceplate cables.
	Insert the faceplate cables into the DMC8 card, and into the cards on either side of it.
3	Disconnect the maintenance bypass cable.
	Remove the maintenance bypass cable from the **Maint** port of the DMC8 cards on either side of the replaced DMC8 card.

END

Restoring subscription data to the serviceable DMC8 card

Figure 289
DMC window



☑ Show Operational ☑ Show Non Operational

DMC TN	Type	Active Software Package	Relay	State	Number of Users	Comment
48 2 06	DMC	45100105	No	Operational	0	Automatic creation o...
48 2 07	DMC	45100105	Yes	Operational	1	Automatic creation o...

Connected

Complete the following steps.

Procedure 172
Restoring subscription data to the DMC8 card

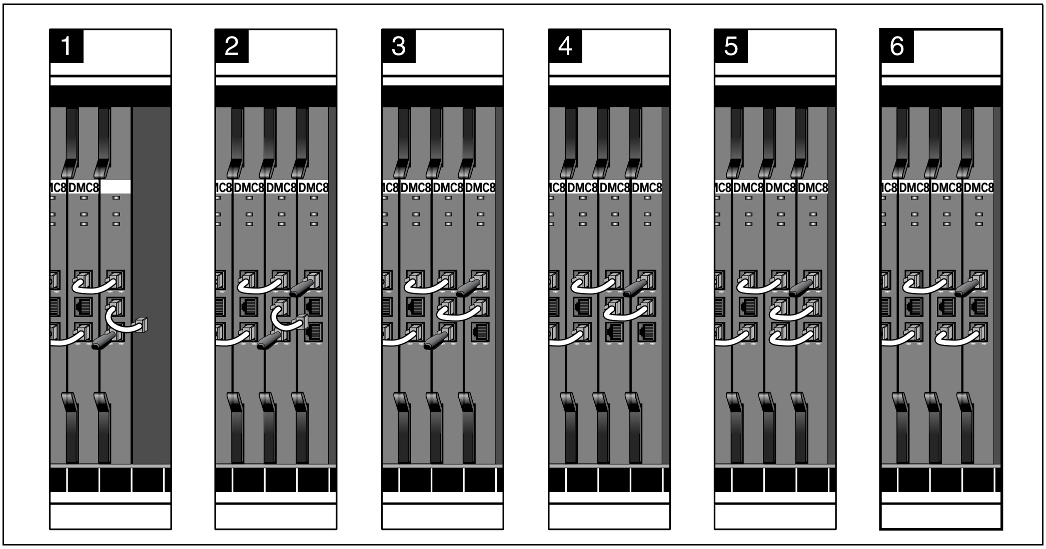
Step	Action
1	Using Windows, login to OTM. Select the system that supports the DECT system. Launch the DECT application. Open the DECT Systems window, and open the Boards window.
	Follow the instructions on page 440 to page 449.
2	Select the DMC8.
	Highlight the DMC8 in the list.
	Save the DMC8 data on the OTM.
	From the **Synchronization** pull-down menu, click on **Synchronize To**.

END

Note: Restore only one DMC (Board) at a time.

Adding a DMC8 card to a DECT system

Figure 290
Add a DMC8 card to the system



Complete the following steps.

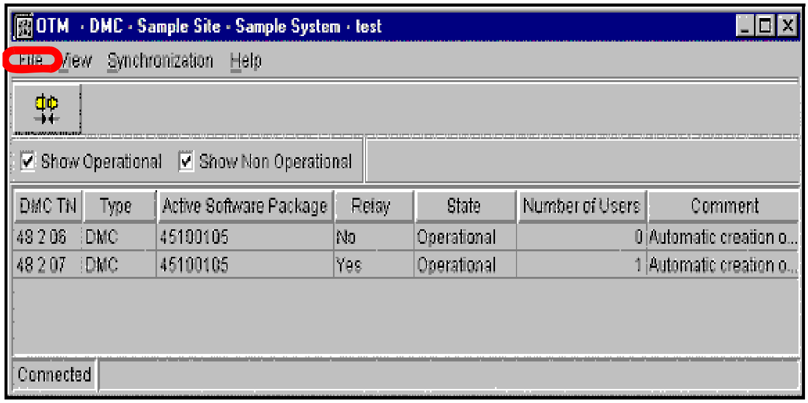
Procedure 173
Adding a DMC8 card to a DECT system

Step	Action
1	Connect the bypass cable.
	Plug the bypass cable into the **Maint** port of the existing DMC8.
2	Insert the DMC8 card, with a terminating plug installed, into the top ◄► port.
	Lever the card into the shelf backplane and latch the card locking devices.
3	Connect the bypass cable to the added DMC8 card.
	Plug the bypass cable into the **Maint** port of the added DMC8 card.
4	Remove the terminating plug from the existing card.
	Remove the terminating plug from the bottom ◄► port of the existing DMC8 card.
5	Connect the faceplate cable.
	Insert the faceplate cables into the bottom ◄► port of the existing DMC8 card and the added DMC8 card.
6	Disconnect the bypass cable.
	Remove the maintenance bypass cable from the **Maint** port of the existing DMC8 card and the added DMC8 card.
7	Add the DMC8 card to the database.
	Use the procedure on page 565.

END

Reusing a DMC8 card in another DECT system

Figure 291
DMC window



☑ Show Operational ☑ Show Non Operational

DMC TN	Type	Active Software Package	Relay	State	Number of Users	Comment
48 2 06	DMC	45100105	No	Operational	0	Automatic creation o...
48 2 07	DMC	45100105	Yes	Operational	1	Automatic creation o...

Connected

Complete the following steps.

Procedure 174
Reusing a DMC8 card in another DECT system

Step	Action
1	Select the DMC8 card to be reused.
	Highlight the DMC8 in the list.
2	Delete the subscriptions from the DMC8 card memory.
	From the **File** pull-down menu, click on **Clear**.

END

Removing and reinstalling a basestation for maintenance

Removing and reinstalling a basestation for maintenance involves:

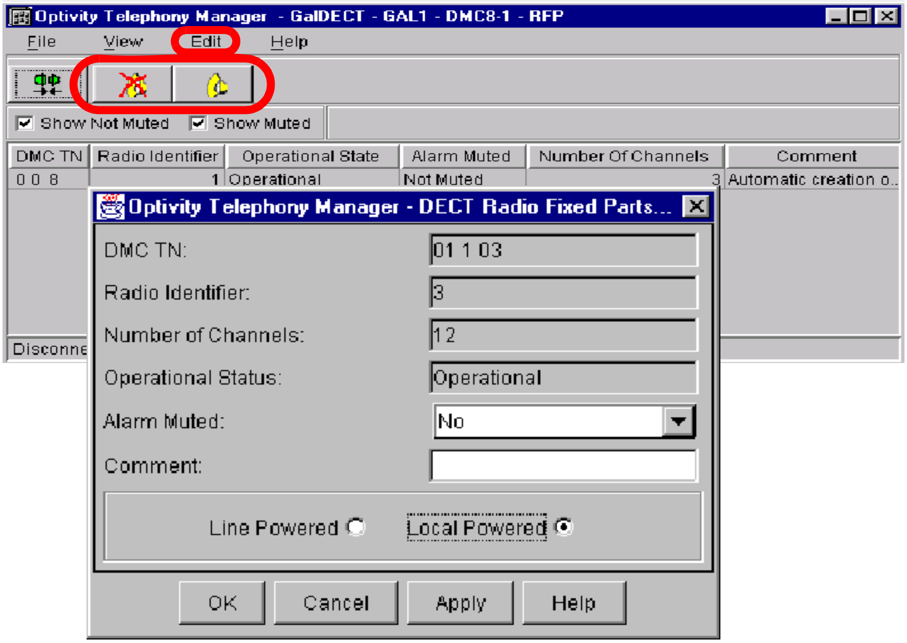
1 “Muting alarms on a basestation” on page 570

2 “Canceling mute alarms on a basestation” on page 572

3 “Disconnecting and reinstalling a basestation” on page 573

Muting alarms on a basestation

Figure 292
RFP window and DECT Radio Fixed Parts properties window


Optivity Telephony Manager - GalDECT - GAL1 - DMC8-1 - RFP
File
View
Edit
Help
Optivity Telephony Manager - DECT Radio Fixed Parts...
OK
Cancel
Apply
Help

☑ Show Not Muted ☑ Show Muted

DMC TN	Radio Identifier	Operational State	Alarm Muted	Number Of Channels	Comment
0 0 8	1	Operational	Not Muted	3	Automatic creation o..

Disconne

DMC TN: 01 1 03

Radio Identifier: 3

Number of Channels: 12

Operational Status: Operational

Alarm Muted: No

Comment:

Line Powered ○ Local Powered ●

Complete the following steps.

Procedure 175
Muting alarms on a basestation

Step	Action
1	Using Windows, login to OTM. Select the system that supports the DECT system. Launch the DECT application. Open the DECT Systems window, and open the RFP window.
	Follow the instructions on page 440 to page 449.
2	Select the DMC8 to mute.
	Highlight the DMC8 in the list.
3	Mute the alarms.
	From the **File** pull-down menu, click on **Mute Alarms**, or click on the icon.

END

Canceling mute alarms on a basestation

Complete the following steps.

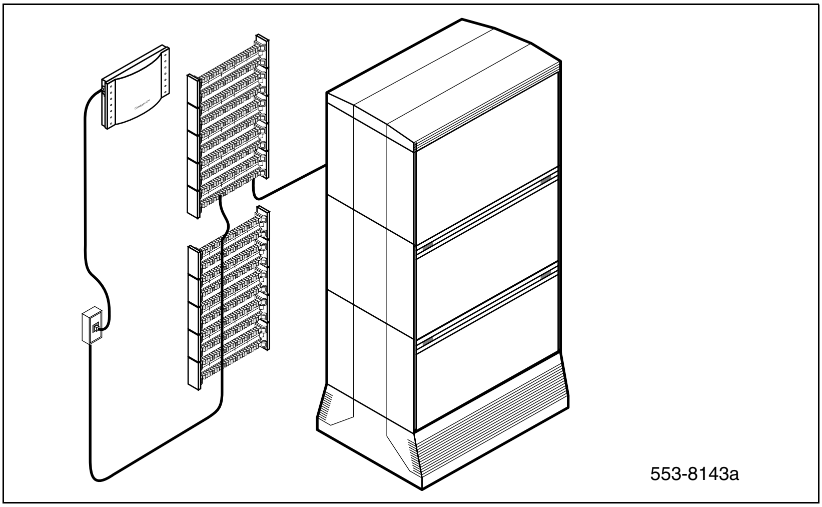
Procedure 176
Canceling mute alarms on a basestation

Step	Action
1	Using Windows, login to OTM. Select the system that supports the DECT system. Launch the DECT application. Open the DECT Systems window, and open the RFP window.
	Follow the instructions on page 440 to page 449.
2	Select the DMC8 to cancel mute alarms.
	Highlight the DMC8 in the list.
3	Cancel mute alarms.
	From the **File** pull-down menu, click on **Cancel Mute Alarms**, or click on the 🔔 icon.

END

Disconnecting and reinstalling a basestation

Figure 293
Disconnect/reinstall the basestation



> ***Note:*** After disconnecting the cable to the basestation, wait for 60 seconds before reconnecting another basestation.

Complete the following steps.

Procedure 177
Disconnecting/reinstalling a basestation (Part 1 of 2)

Step	Action
1	Disconnect the RJ45 cable, MDF side.
	Unplug the RJ45 cable from the wall socket of the RJ45 Connection Box.
2	Disconnect the RJ45 cable, basestation side.

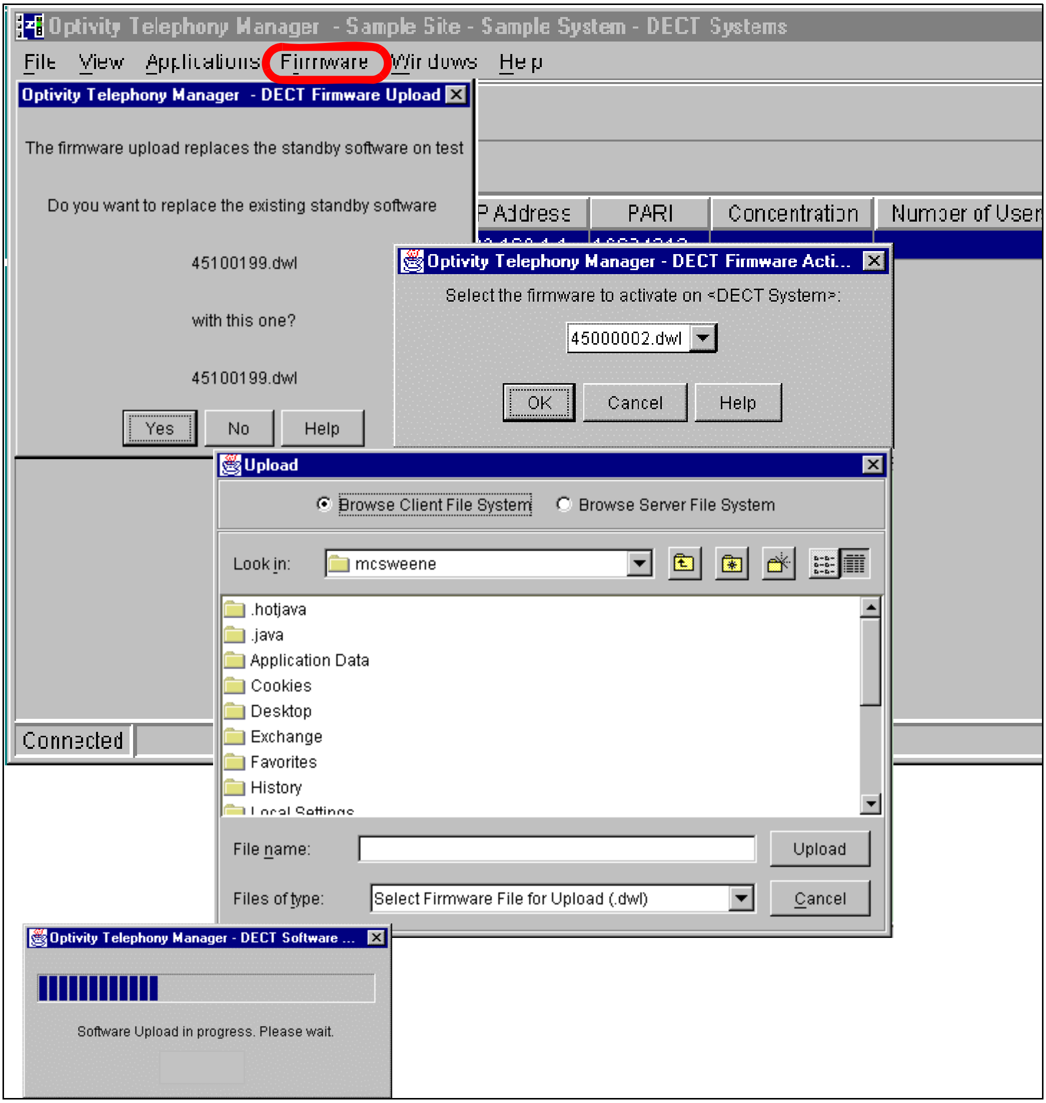
Procedure 177
Disconnecting/reinstalling a basestation (Part 2 of 2)

Step	Action
3	Remove the unserviceable basestation from the mounting plate.
4	Reinstall a serviceable basestation on the mounting plate.
5	Re-connect the RJ45 cable to the basestation.
6	Re-connect the RJ45 cable, MDF side.

END

Uploading and activating firmware

Figure 294
DECT systems, DECT Firmware Upload, DECT Firmware Activation, Upload



Optity Telephony Manager - Sample Site - Sample System - DECT Systems

Optivity Telephony Manager - DECT Firmware Upload

The firmware upload replaces the standby software on test

Do you want to replace the existing standby software

45100199.dwl

with this one?

45100199.dwl

Optivity Telephony Manager - DECT Firmware Acti...

Select the firmware to activate on <DECT System>:

45000002.dwl

Upload

● Browse Client File System ○ Browse Server File System

Look in: mcsweene

.hotjava
.java
Application Data
Cookies
Desktop
Exchange
Favorites
History
Local Settings

File name:

Files of type: Select Firmware File for Upload (.dwl)

Optivity Telephony Manager - DECT Software ...

Software Upload in progress. Please wait.

Connected

Complete the following steps.

Procedure 178
Uploading and activating firmware

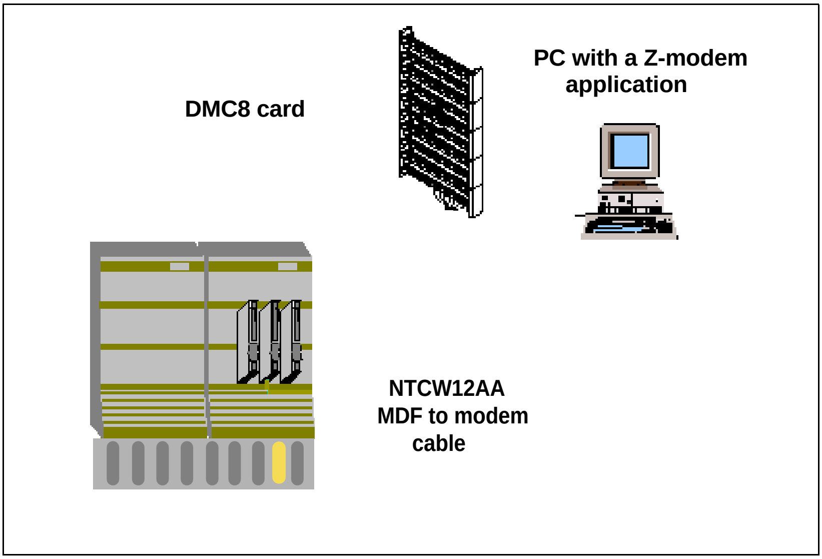
Step	Action
1	Using Windows, login to OTM. Select the system that supports the DECT system. Launch the DECT application. Open the DECT Systems window.
	Follow the instructions on page 440 to page 449.
2	Open the Firmware upload dialog.
	Select the **Firmware** pull-down menu, and click on **Upload**.

END

Recovering from a firmware upload failure

It is possible to upload DMC firmware with the V.24 port of a DMC8 card using a PC equipped with Z-modem protocol. During the upload, the DMC8 card deletes the active and standby firmware, and stores the uploaded firmware as the active firmware. When the upload completes, the boot program starts the uploaded firmware.

Figure 295
Recovery upload to a DMC8 card



Complete the following steps.

Procedure 179
Recovering from a firmware upload failure

Step	Action
1	Configure the COM port settings.
	baud rate = 19200 data bits = 8 parity = no parity stop bit = no flow control
2	Connect the NTCW12AA cable to the DMC8 card to be uploaded.
	Refer to Table 35 on page 579 for the NTCW12AA cable tip and ring connections.
3	Locate the OTM server COM port.
	Connect the NTCW12AA cable connector into the PC COM port.
4	Unseat the DMC8 card.
	Disconnect the DMC8 card from the shelf backplane.
5	Access Z-modem application; for example, Windows HyperTerminal.
	Click **Start** on the Windows taskbar and choose **Programs > Accessories > HyperTerminal**.
6	Initiate the file transfer.
	Start the Z-modem application on the PC.
7	Activate the boot program.
	Insert the DMC8 card into the shelf backplane.

END

Note: The BIX tip and ring connections shown in Table 35 on page 579 correspond to standard BIX designation. The first pair are labeled T0 and R0. See the section in *Communication Server 1000M and Meridian 1: Large System Installation and Configuration* (553-3021-210) that deals with planning and designating the MDF.

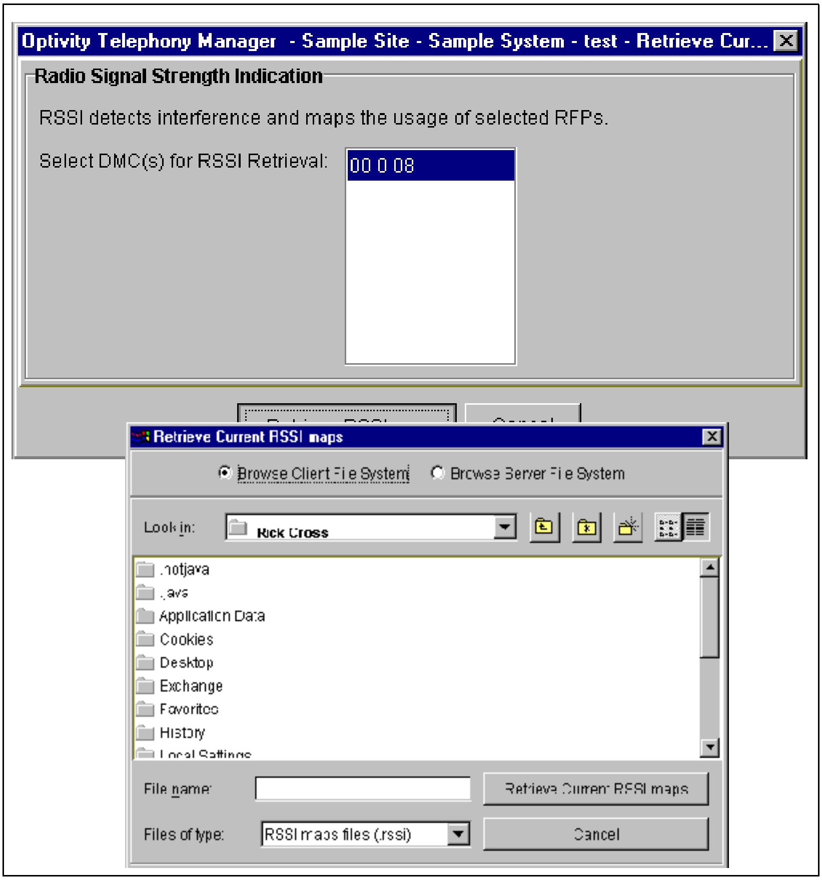
Table 35
NTCW12AA cable to MDF connections

DMC8 Relay card MDF connection	Cable color	DB25 connector pin number	Signal designator
T1	Grey	8	V.24DCD
R2	Yellow	4	V.24RTS
T3	Blue	2	V.24TXD
R3	Red	3	V.24RXD
T4	Pink	7	V.24GND

Retrieving current RSSI data

The Radio Signal Strength Indication (RSSI) shows interference and usage by a certain basestation. A snapshot of the RSSI data is retrieved and stored in a file when the user requests it. If the file already existed, the new snapshot data is appended to the last snapshot data in the file.

Figure 296
Retrieve Current RSSI window and
Retrieve Current RSSI maps window



Optivity Telephony Manager - Sample Site - Sample System - test - Retrieve Cur...

Radio Signal Strength Indication

RSSI detects interference and maps the usage of selected RFPs.

Select DMC(s) for RSSI Retrieval: 00 0 08

Retrieve Current RSSI maps

● Browse Client File System ○ Browse Server File System

Look in: Rick Cross

- .hotjava
- .avs
- Application Data
- Cookies
- Desktop
- Exchange
- Favorites
- History
- Local Settings

File name:

Files of type: RSSI maps files (.rssi)

Complete the following steps.

Procedure 180
Retrieving current RSSI data

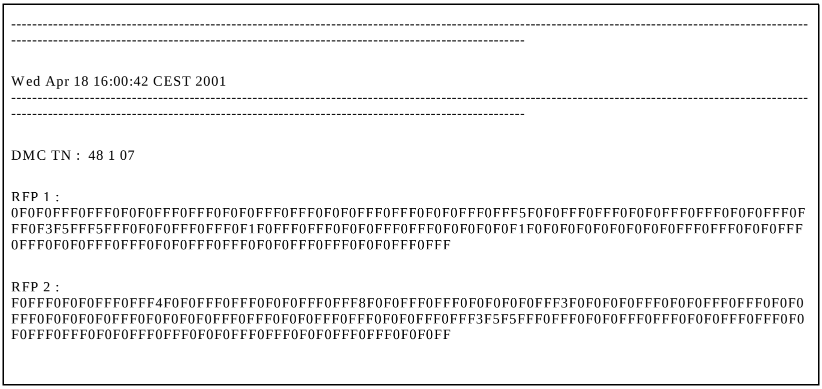
Step	Action
1	Using Windows, login to OTM. Select the system that supports the DECT system. Launch the DECT application. Open the DECT Systems window, and open the Current RSSI Data window.
	Follow the instructions on page 440 to page 449.
2	Select a DMC8 card or cards for RSSI information retrieval.
	Scroll and highlight a TN in the **Select DMCs for RSSI Retrieval:** box.
3	Retrieve the RSSI data.
	Click on the **Retrieve RSSI now** button.
4	Store the RSSI data.
	Select a file location.

END

RSSI file format

The data for each RFP is a nibble for indication of the RSSI value for each slot (24) for each carrier (10). This results in 10 (number of carriers) times 24 (number of slots) nibbles equal to 240 nibbles (120 octets).

Figure 297
RSSI file format



```
---------------------------------------------------------------------------------------------------------------------------------------
----------------------------------------------------------------------------------------

Wed Apr 18 16:00:42 CEST 2001
---------------------------------------------------------------------------------------------------------------------------------------
----------------------------------------------------------------------------------------

DMC TN :  48 1 07

RFP 1 :
0F0F0FFF0FFF0F0F0FFF0FFF0F0F0FFF0FFF0F0F0FFF0FFF0F0F0FFF0FFF5F0F0FFF0FFF0F0F0FFF0FFF0F0F0FFF0F
FF0F3F5FFF5FFF0F0F0FFF0FFF0F1F0FFF0FFF0F0F0FFF0FFF0F0F0F0F0F1F0F0F0F0F0F0F0F0F0FFF0FFF0F0F0FFF
0FFF0F0F0FFF0FFF0F0F0FFF0FFF0F0F0FFF0FFF0F0F0FFF0FFF

RFP 2 :
F0FFF0F0F0FFF0FFF4F0F0FFF0FFF0F0F0FFF0FFF8F0F0FFF0FFF0F0F0F0F0FFF3F0F0F0F0FFF0F0F0FFF0FFF0F0F0
FFF0F0F0F0F0FFF0F0F0F0F0FFF0FFF0F0F0FFF0FFF0F0F0FFF0FFF3F5F5FFF0FFF0F0F0FFF0FFF0F0F0FFF0FFF0F0
F0FFF0FFF0F0F0FFF0FFF0F0F0FFF0FFF0F0F0FFF0FFF0F0F0FF
```

Performance Collection

Overview

The DECT Performance Manager is an application developed specifically to help with investigations in the following areas:

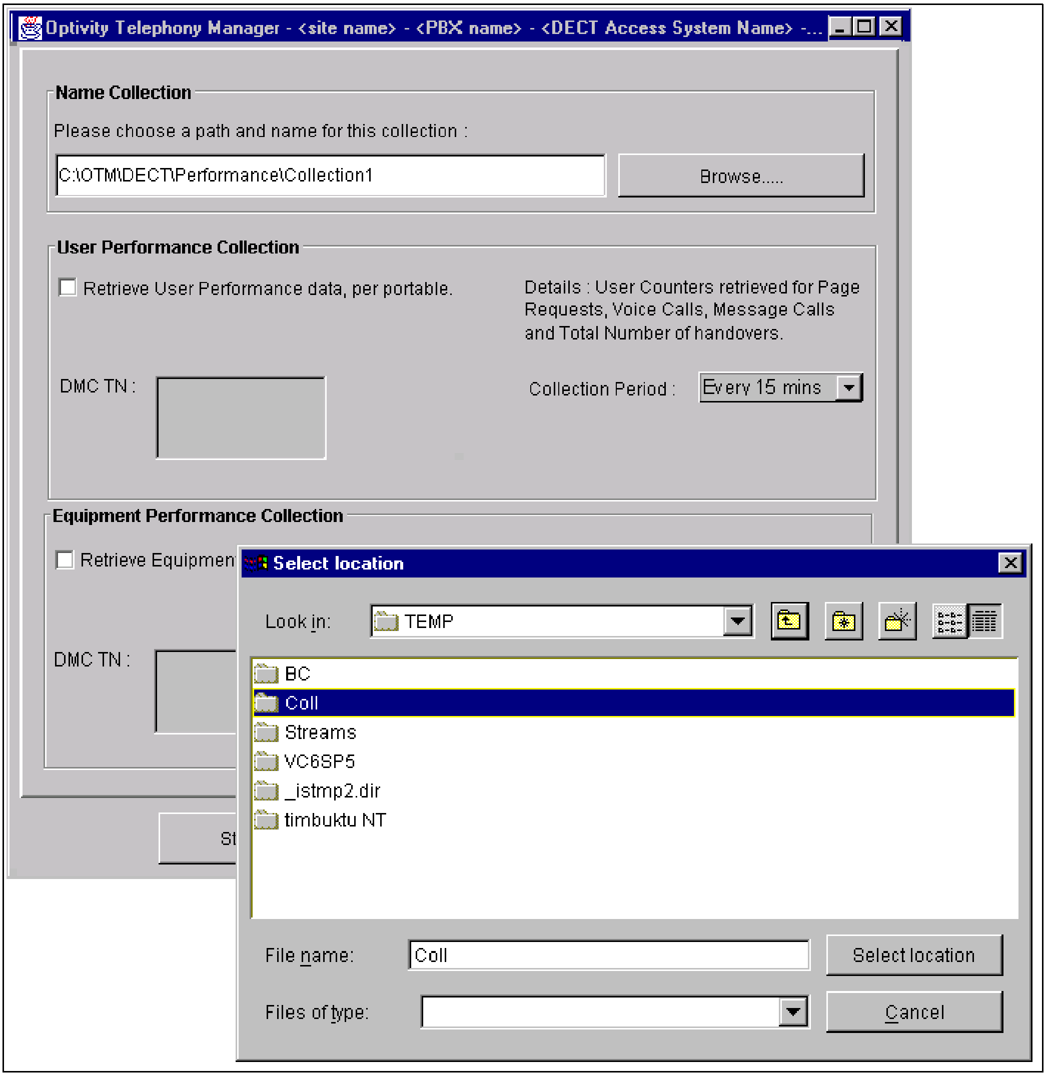
- deployment
- engineering
- configuration
- traffic
- call and non-call associated issues

The DECT Performance Manager does not work on non-SNMP firmware. Users of the Performance Manager must have a basic understanding of the DECT product.

Every DMC board has two performance files, the Equipment Performance Management (epm) file and the User Performance Management (upm) file. The epm file contains the counters and timers for DMC board and RFP information. The upm files contain the counters and timers for PP information.

The DECT Performance Manager uses a database created from upm and epm files retrieved from the DMC boards on the DECT system. Using the database, the DECT Performance Manager can generate Reports and Trends. The upm and epm files are collected from the boards on the DECT system using the Performance collection application on OTM DECT. See Figure 298 on page 584.

Figure 298
Performance Collection window and Select location dialog



Optivity Telephony Manager - <site name> - <PBX name> - <DECT Access System Name> -...

Name Collection

Please choose a path and name for this collection :

C:\OTM\DECT\Performance\Collection1

User Performance Collection

□ Retrieve User Performance data, per portable.

Details : User Counters retrieved for Page Requests, Voice Calls, Message Calls and Total Number of handovers.

DMC TN :

Collection Period : Every 15 mins

Equipment Performance Collection

□ Retrieve Equipmen

DMC TN :

Select location

Look in: TEMP

File name: Coll

Files of type:

The DECT Performance Manager is capable of generating Reports and Trends for the following:

- B-channel occupation
- S-channel occupation
- basestation (RFP) channel occupation
- board statistics
- portable statistics
- basestation statistics

For more information on the Reports, see “DECT Performance Manager data” on page 601.

Complete the following steps in sequence:

1. “DECT Performance Manager installation” on page 586
2. “Set date and time on OTM DECT Manager” on page 588
3. “Retrieve upm and epm files” on page 589
4. “Creating a new directory structure” on page 592
5. “Rename upm and epm files” on page 594
6. “Creating a database” on page 596
7. “Using the database” on page 598
8. “DECT Performance Manager data” on page 601

> ***Note:*** Omit the steps in “Creating a new directory structure” on page 592 and “Rename upm and epm files” on page 594 if you are using OTM 2.2 (the directory structure and file names are correct).

CAUTION — Service Interruption

Check to ensure the Performance Collection is not using all the OTM server storage space.

DECT Performance Manager installation

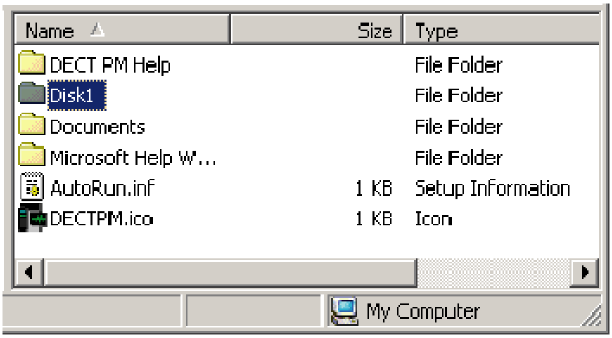
You must have Windows Internet Explorer™ 6.x installed to run the DECT Performance Manager. The application software zip file is 14.5 Mbits. The extracted file is 54 Mbits.

Procedure 181
Installing DECT Performance Manager

Step	Action
1	Download the DECT Performance Manager application software.
	The software file is located on the TSC server in a zip file format: **http://imola.europe.nortel.com:8081/TSC_EUROPE/**
2	Extract the application software.
	Use the application installed on your computer for extracting files and directories from a zip file.
3	Open the folder labeled Disk 1. See Figure 299 on page 587.
	Double-click the folder labeled Disk 1.
4	Run Setup.exe.
	Double-click the Setup.exe icon. See Figure 300 on page 587.
5	Follow the Install Wizard.
	After installation is complete, open the DECT Performance Manager by double-clicking the DECT Performance Manager icon located in the Programs folder (accessed through the **Start** menu).

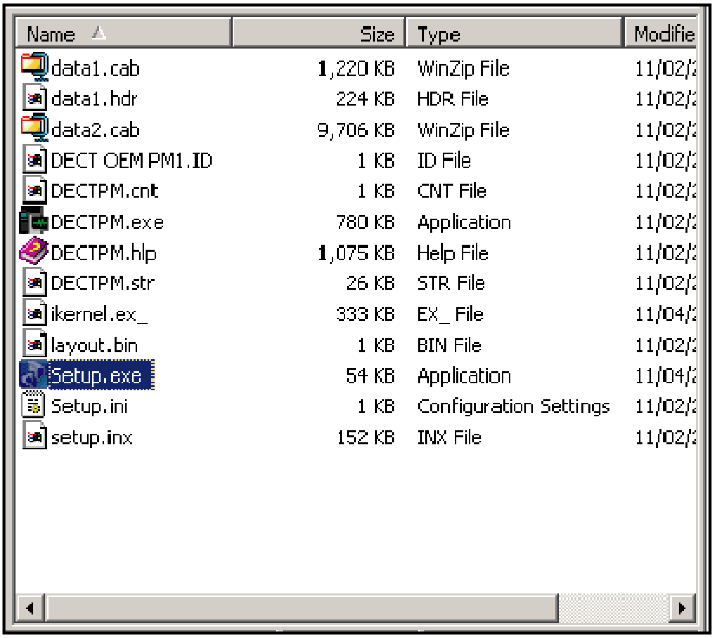
END

Figure 299
DECT Performance Manager application software



Name	Size	Type
DECT PM Help		File Folder
Disk1		File Folder
Documents		File Folder
Microsoft Help W...		File Folder
AutoRun.inf	1 KB	Setup Information
DECTPM.ico	1 KB	Icon

Figure 300
DECT Performance Manager installation file



Name	Size	Type	Modifie
data1.cab	1,220 KB	WinZip File	11/02/
data1.hdr	224 KB	HDR File	11/02/
data2.cab	9,706 KB	WinZip File	11/02/
DECT OEM PM1.ID	1 KB	ID File	11/02/
DECTPM.cnt	1 KB	CNT File	11/02/
DECTPM.exe	780 KB	Application	11/02/
DECTPM.hlp	1,075 KB	Help File	11/02/
DECTPM.str	26 KB	STR File	11/02/
ikernel.ex_	333 KB	EX_ File	11/04/
layout.bin	1 KB	BIN File	11/02/
Setup.exe	54 KB	Application	11/04/
Setup.ini	1 KB	Configuration Settings	11/02/
setup.inx	152 KB	INX File	11/02/

Set date and time on OTM DECT Manager

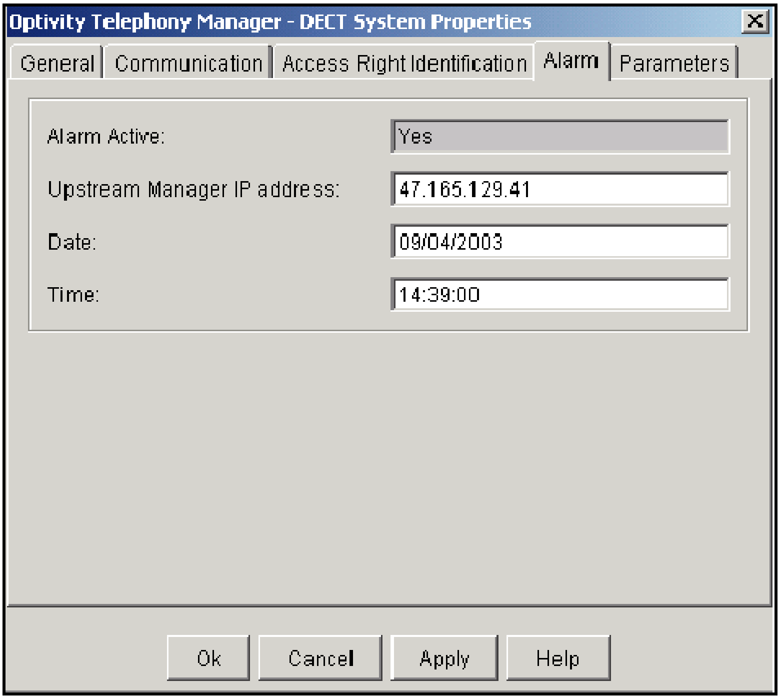
You must set the date and time on the OTM DECT Manager before retrieving upm and epm files from the DECT system. This ensures a more accurate Report or Trend when using the DECT Performance Manager.

Procedure 182
Setting date and time on the OTM DECT Manager

Step	Action
1	Connect to the DECT system.
2	Select **File > Properties**.
	Select **File** on the toolbar, and select **Properties** from the **File** menu. The **Properties** window opens. See Figure 301 on page 589.
3	Click the **Alarm** tab.
4	Change the date and time.
5	Save changes.
	Click the **Apply** button, then click **OK**.

END

Figure 301
OTM-DECT System Properties window — Alarm tab


Optivity Telephony Manager - DECT System Properties
General
Communication
Access Right Identification
Alarm
Parameters
Ok
Cancel
Apply
Help

Alarm Active: Yes

Upstream Manager IP address: 47.165.129.41

Date: 09/04/2003

Time: 14:39:00

Retrieve upm and epm files

Use the Performance Collection application on OTM DECT to retrieve upm and epm files.

Note: The Performance Collection application (used with OTM up to and including Release 2.0) allows files to be collected from a single board only at one time. However, it is possible to collect from multiple boards on the DECT system if the OTM patch 20050su1 is installed. The patch is available on the MPL.

Procedure 183
Retrieving upm and epm files (Part 1 of 2)

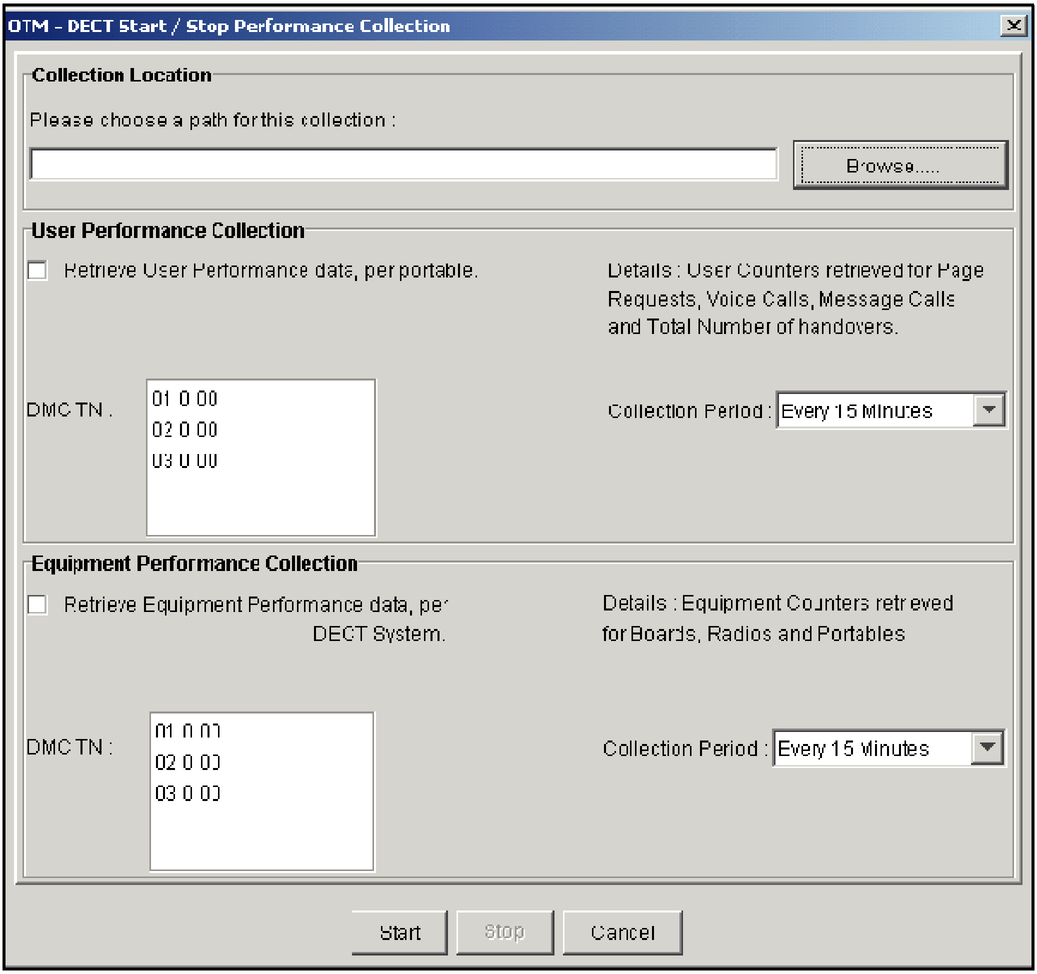
Step	Action
1	Create a folder to be the Collection Location.
	Use this folder to store the retrieved upm and epm files.
2	Connect to the DECT system.
	Follow the instructions on page 440 to page 449.
3	Select **Applications > Performance Collection**.
	Select **Applications** on the toolbar, and select **Performance Collection** from the **Applications** menu.
4	Browse for the folder in which to store the upm and epm files.
	Click the **Browse** button under **Collection Location** and navigate to the folder you created in Step 1.
5	Select the **Retrieve User Performance Collection data, per portable** and **Retrieve Equipment Performance Collection data, per DECT System** check boxes.
6	Select the board or boards from which to collect the upm and epm files.
	Enter the DMC TNs of the boards.
7	Select the collection period from the **Collection Period:** drop-down list.
	Use a 15-minute collection period for the most detailed results. For less detailed results, use a longer collection period. A minimum of two files is required for the Performance Manager to work.

Procedure 183
Retrieving upm and epm files (Part 2 of 2)

Step	Action
8	Click the **Start** button.
	When the Performance Collection starts, upm and epm files are stored in the Collection Location at intervals specified in the **Collection Period**. To close the **Performance Collection** window, click the **Cancel** button. (The Performance Collection continues while the window is closed.)
9	Click the **Stop** button to stop the Performance Collection.

END

Figure 302
OTM DECT Start/Stop Performance Collection window



OTM - DECT Start / Stop Performance Collection
Collection Location
Browse.....
User Performance Collection
Equipment Performance Collection
Start
Stop
Cancel

Please choose a path for this collection :

□ Retrieve User Performance data, per portable.

Details : User Counters retrieved for Page Requests, Voice Calls, Message Calls and Total Number of handovers.

DMC TN :

01 0 00
02 0 00
03 0 00

Collection Period : Every 15 Minutes

□ Retrieve Equipment Performance data, pe DECT System.

Details : Equipment Counters retrieved for Boards, Radios and Portables

DMC TN :

01 0 00
02 0 00
03 0 00

Collection Period : Every 15 Minutes

Creating a new directory structure

A database must be created before using the DECT Performance Manager. To create the database, the upm and epm files must be located in a defined directory format (see Figure 303 on page 593).

Figure 303
Directory structure

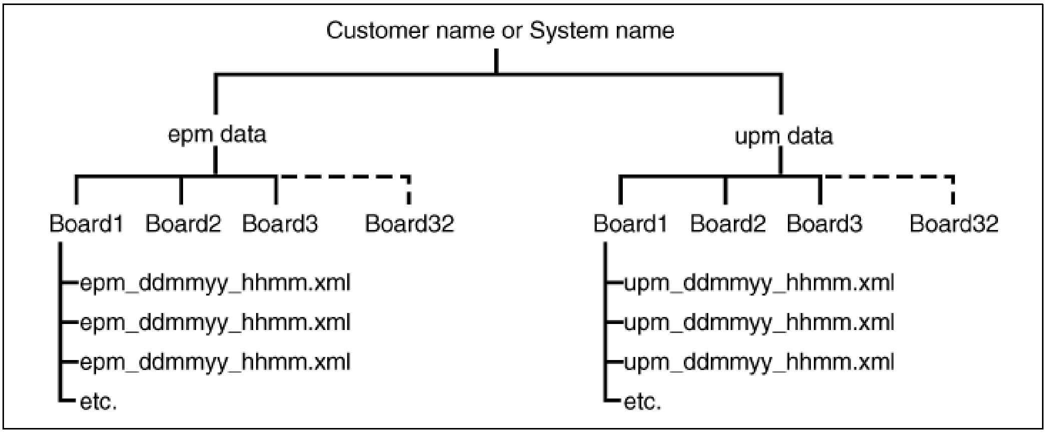
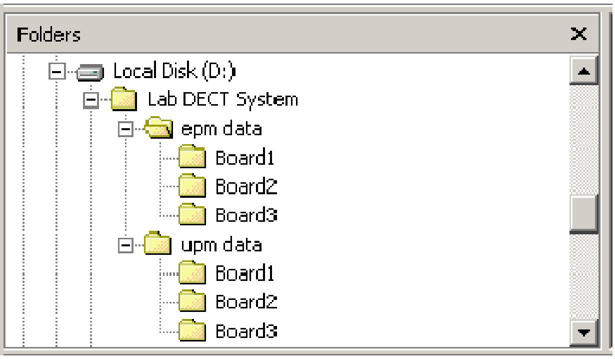


Figure 304 is an example of a directory.

Figure 304
Directory example



Rename upm and epm files

With some versions of OTM, the upm and epm files exist in a format that is not compatible with the Performance Manager. Therefore, all upm and epm files collected must be renamed before either a database can be created, or Reports and Trends can be generated. All the files must be renamed correctly, using the proper format, to create a database for the generation of Reports.

IMPORTANT!

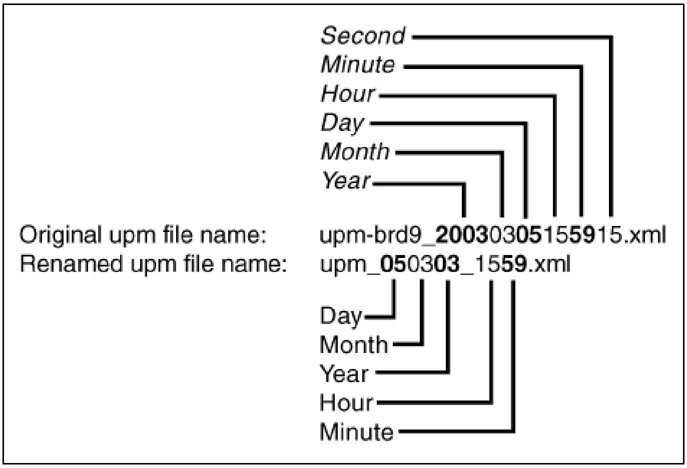
Place all the upm and epm files in the new directory structure before renaming takes place.

The upm file name format is upm_ddmmyy_hhmm.xml, where:

- ddmmyy=PC date the performance data was requested (day, month, year)
- hhmm=PC time the performance data was requested (hour, minute)

Figure 305 shows an original upm file name and the file renamed.

Figure 305
Upm file renamed

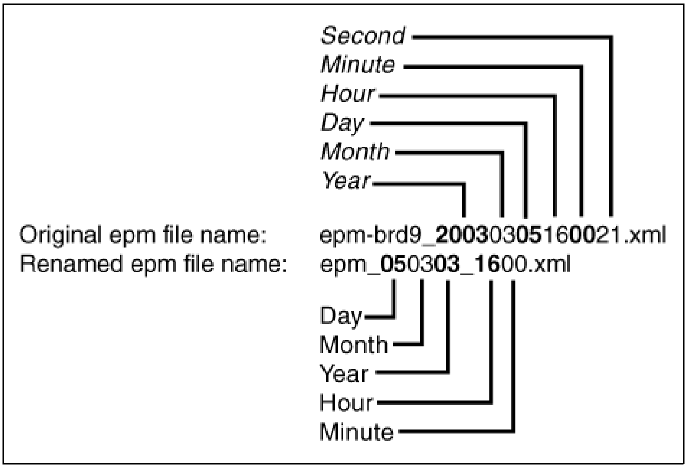


The epm file name format is epm_ddmmyy_hhmm.xml, where:

- ddmmyy=PC date the performance data was requested (day, month, year)
- hhmm=PC time the performance data was requested (hour, minute)

Figure 306 shows an original epm file name and the file renamed.

Figure 306
Epm file renamed



Creating a database

You must first create a database as part of the process to generate Reports and Trends. Create the database using the DECT Performance Manager.

Procedure 184
Retrieving upm and epm files (Part 1 of 2)

Step	Action
1	Open the Performance Manager application.
	Double-click the DECT Performance Manager icon located in the Programs folder.
2	Select **Database > New Database**.
	Select **Database** on the toolbar, and select **New Database** from the **Database** menu.
3	Enter a description for the database. See Figure 307 on page 597.
	Enter the Customer or System name.
4	Click the **OK** button.
5	Select a location in which to store the database.
6	Name the database.
	Enter the Customer or System name as the database name.
7	Click the **Save** button.
8	Select **File > Import**.
	Select **File** from the toolbar, and select **Import from files** from the **File** menu.
9	Select the folder where the upm and epm files are located.
	The upm and epm file folders are at the top of the directory structure. Ensure that both the epm data and upm data check boxes are selected. See Figure 308 on page 597 (DMC is in slot 9).

Procedure 184
Retrieving upm and epm files (Part 2 of 2)

Step	Action
10	Click the **Import** Button.
11	Click the **Done** button.
	The database is created with the name entered in Step 3. The database has a .mbd extension, and is now ready to use for generating Reports and Trends.

END

Figure 307
New DECT Performance Manager Database description dialog

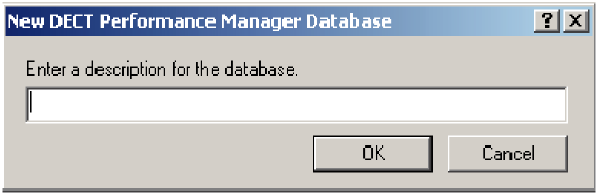
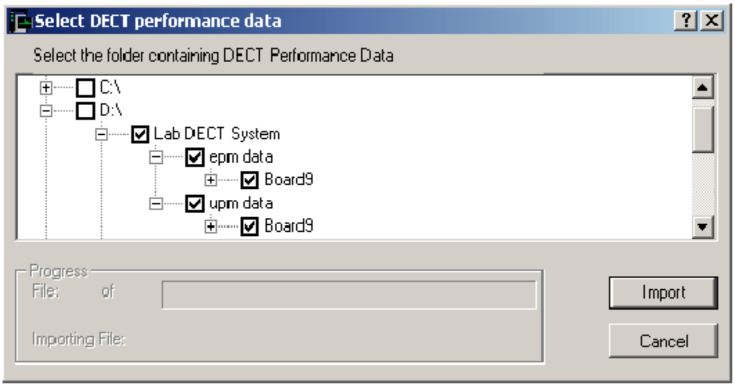

New DECT Performance Manager Database
?
X
Enter a description for the database.
OK
Cancel

Figure 308
Select DECT performance data window



Using the database

You can generate Reports and Trends after the database is created.

The DECT information in the database is detailed and can be complex. The Help files included with the DECT Performance Manager application are comprehensive, and explain in detail all aspects of this tool.

Procedure 185
Generating Reports or Trends

To generate Reports or Trends:

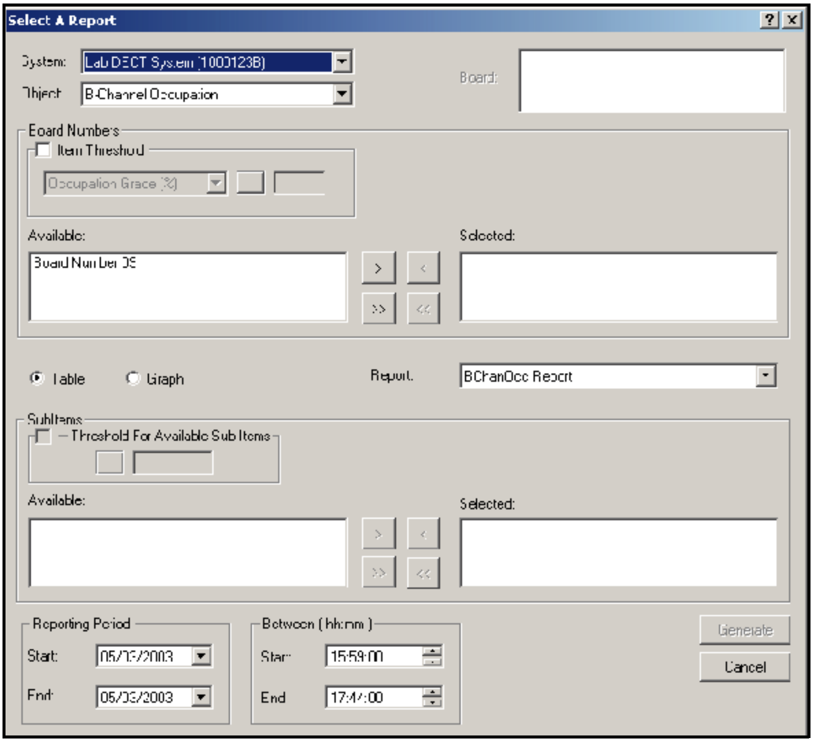
1 Select **Reports** on the toolbar of the DECT Performance Manger application.

2 Select **Reports or Trends** from the **Reports** menu.

The **Select A Report** window opens (see Figure 309 on page 599). You can now generate Reports and Trends.

End of Procedure

Figure 309
Select A Report window



System: Lab DECT System (1000123B)

Object: B-Channel Occupation

□ Item Threshold: Occupation Grace (%)

Available: Board Number 09

● Table ○ Graph

Report: BChanOcc Report

□ Threshold For Available Sub Items

Reporting Period: Start: 05/03/2003 End: 05/03/2003

Between (hh:mm): Start 15:59:00 End 17:47:00

Previously created databases

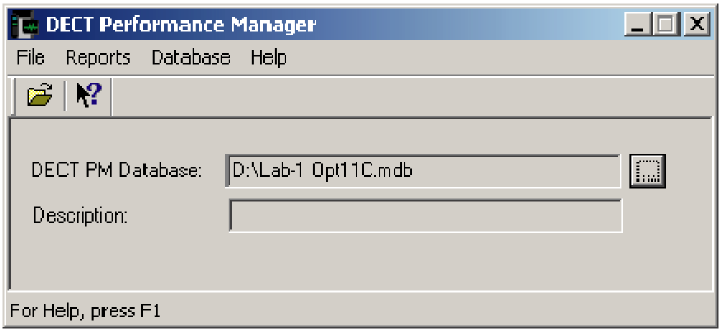
It is also possible to use databases previously created to generate Reports and Trends.

Procedure 186
Retrieving upm and epm files

Step	Action
1	Open the Performance Manager application.
	Double-click the DECT Performance Manager icon located in the Programs folder.
2	Select a database.
	Click the button to the right of the **DECT PM Database:** field, or select **Database** on the toolbar, and then **Select Database** from the **Database** menu. See Figure 310.
3	Open a database.
	Click on a database to select it, and click the **Open** button.
4	Select **Reports > Reports or Trends**.
	Select **Reports** on the toolbar, and select **Reports or Trends** from the **Reports** menu. You can now generate Reports and Trends.

END

Figure 310
Select an existing database



DECT PM Database: D:\Lab-1 Opt11C.mdb
Description:
For Help, press F1

DECT Performance Manager data

This section describes the most relevant performance data. The data is collected during operation of a DECT system. The performance data is statistical and can be used to identify potential problems. The performance data consists of counters that represent a number of events.

The DECT manager retrieves the data from the DECT system within a defined interval period. During this interval, the Performance Manager measures objects by retrieving events (counters).

IMPORTANT!

Counters represent a number of events. For example, the “voice call” counter increments when a PP successfully sets up a voice call. During the voice call, the PP does not increment the counter. If a voice call (in progress) extends beyond the performance data retrieval period, the voice call is not marked in the new retrieval period. It is only marked in the period in which it began. In the new retrieval period, a dropped call can appear, but the continuing voice call is not identified. Nortel recommends making the retrieval period long enough to allow most voice calls to finish within one retrieval period (minimum value is 15 minutes).

The following events are the most relevant performance data:

- paging
- dropped voice call
- dropped message
- handover
- RFP-channel occupation
- S-channel occupation
- B-channel occupation
- degradation of service
- grade of page failures

- grade of page retries
- grade of page rejects

Paging

Paging is the process of broadcasting a message from an RFP to one or more PPs. Paging messages are used to alert a PP (a call setup attempt). The paging message contains the system information and the identifier of a PP. A PP enters the alert phase when it recognizes its own identifier.

The following events (performance data) are associated with paging messages:

- Request: number of call setup attempts
- Retries: number of call setup attempts after the PP did not respond on a page request
- Failure: after a number of page retries (default is two attempts), the call setup attempt is aborted (that is, the paging procedure failed)
- Reject: the PP responds to the request, but rejects the call setup attempt

Dropped voice call

A dropped voice call occurs when the PP loses the connection with the RFP. The PP is no longer able to make or receive a call.

A dropped call can occur during either of the following phases:

- Active phase: the PP loses the synchronization with the RFP with a call in progress
- Call setup phase: the PP loses the synchronization with the RFP, but there is no call in progress

Dropped message

A dropped message occurs when the PP loses the connection with the RFP. The PP is no longer able to receive messages from the RFP.

Handover

Handover is the process of switching a call in progress from one physical channel to another physical channel.

There are two types of handover:

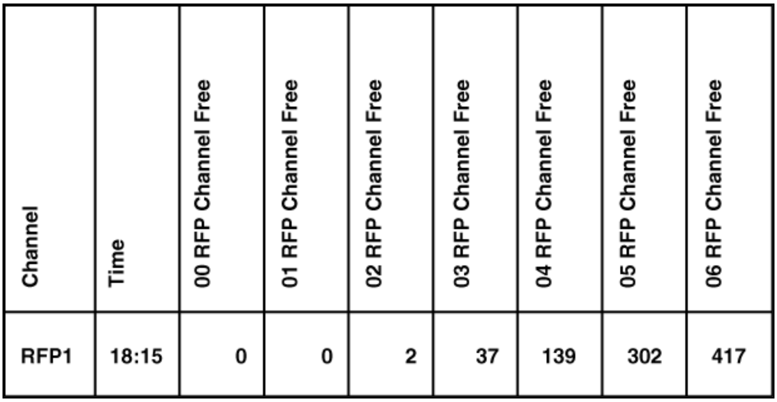
- Inter-cell: A call in progress switches from one RFP to another RFP. This type of handover generally occurs because the user is roaming.
- Intra-cell: A handover that is completely internal to one RFP. This type of handover is generally caused by interference on the carrier frequency to which the call is locked.

RFP-channel occupation

The RFP-channel occupation report indicates how many RFPs are installed and can be helpful when determining if enough RFPs are installed.

The RFP-channel occupation report contains tables that show the number of seconds that RFP channels are free. Figure 311 shows an example of an RFP-channel occupation report from a 6-channel RFP. The performance retrieval period is 15 minutes (900 seconds).

Figure 311
RFP channel occupation report — 6-channel RFP



Channel	Time	00 RFP Channel Free	01 RFP Channel Free	02 RFP Channel Free	03 RFP Channel Free	04 RFP Channel Free	05 RFP Channel Free	06 RFP Channel Free
RFP1	18:15	0	0	2	37	139	302	417

The report indicates the following:

- 6 channels were free for 417 seconds. Therefore, at least 1 channel was occupied for 483 seconds (900 - 417 = 483 seconds).
- 5 channels were free for 302 seconds. Therefore, at least 2 channels were occupied for 181 seconds (483 - 302 = 181 seconds).
- 4 channels were free for 139 seconds. Therefore, at least 3 channels were occupied for 42 seconds (181 - 139 = 42 seconds).
- 3 channels were free for 37 seconds. Therefore, at least 4 channels were occupied for 5 seconds (42 - 37 = 5 seconds).
- 2 channels were free for 2 seconds. Therefore, at least 5 channels were occupied for 3 seconds (5 - 2 = 3 seconds).
- 1 channel was free for 0 seconds. Therefore, at least 1 channel was free at any moment.

S-channel occupation

The backbone bus of a DECT system is the interface between the DMC boards. The DMC boards communicate through the bus for the re-routing of calls.

A PP can be synchronized with an RFP that is not connected to the DMC board that contains the subscription information for this PP. The DMC board to which this RFP is connected is called the visitor DMC. The DMC board that contains the subscription information is called the home DMC. The (visitor) DMC board to which the PP is locked (or synchronized) re-routes the PP to the home DMC board.

The DMC board has 32 internal channels between the PRI block and the RFP interfaces. These channels are named S-channels (see Figure 312 on page 605). The S-channel occupation report contains tables that show the number of seconds that S-channels are free.

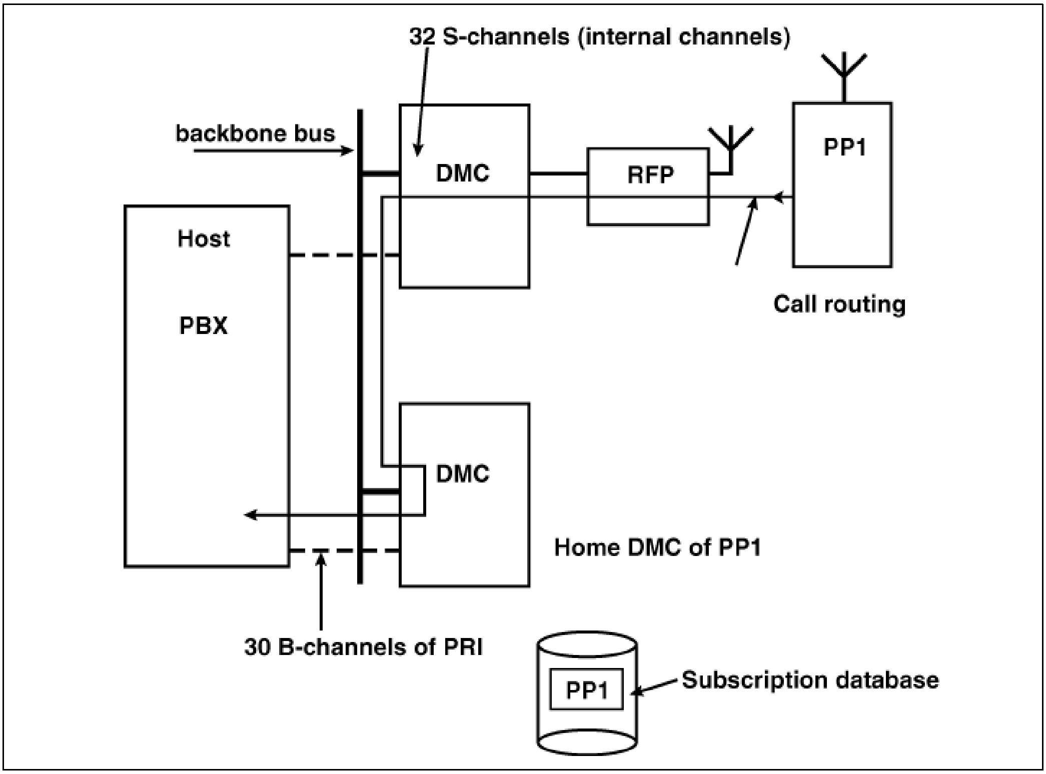
The S-channel occupation report mimics the RFP-channel occupation report. Refer to“RFP-channel occupation” on page 603 for an explanation of how to read the channel occupation reports.

B-channel occupation

There are 32 channels that connect the DMC board to a switching network circuit (Host PBX). These 32 channels are named B-channels or speech-channels. See Figure 312 on page 605.

The B-channel occupation report mimics the RFP-channel occupation report. Refer to“RFP-channel occupation” on page 603 for an explanation of how to read the channel occupation reports.

Figure 312
Channels within the system



Degradation of service

The degradation of service report shows the relation between the number of dropped active calls and the number of successful calls.

Grade of page failures

The grade of page failures report shows the relation between the number of page failures and the number of successful calls and messages.

Grade of page retries

The grade of page retries report shows the relation between the number of page retries and the number of successful calls and messages.

Grade of page rejects

The grade of page rejects report shows the relation between the number of page rejects and the number of successful calls and messages

Top-down analysis

Importing performance files to a database can be a time-consuming process. The time the import process consumes depends on the number of files, the number of installed RFPs, the number of subscribed DNRs, the number of boards, and the performance of the PC. The following example demonstrates how many performance files can be generated in a single week.

Example

Company ABC has 10 DMC boards installed on a DECT system. The performance of this DECT system is measured 10 hours a day for one work week (5 days). The Performance Collection application on OTM DECT retrieves the upm and epm files every hour.

The Performance Manager retrieves 2 files from each of the 10 boards every hour (20 files every hour). Therefore, 200 files are collected each day (20 files/hour x 10 hours). This is 1000 performance files each week (200 files/ day x 5 days).

Company ABC imports these performance files to a database.

Top-down analysis explanation

The top-down analysis is a troubleshooting strategy that helps you to more efficiently generate a performance file database.

Begin the top-down analysis by generating a database that contains only the first and the last performance data files of the week. Limiting the number of performance data files that are generated helps you to determine which board, RFP, or PP causes problems during the week.

You can also limit the number of files imported to the database. Copy the directory structure that contains all performance files to create the database. Delete the performance files that are not needed by clicking **Start** on the Windows taskbar and choosing **Search** > **For Files or Folders** on the taskbar of Windows 2000™. Use the time and date stamps on files to find the performance files that must be deleted. Press <CRTL + A> to select the files, and press the **Delete** key.

If you cannot determine what components of the system cause problems, try generating a new database with one data file each day. If you still cannot solve the problem, add more detail, but generate a new database each time. Generating databases with more details (that is, more performance files) substantially increases the duration of the import process. Always consider if there is enough value added in generating more details to compensate for the extra time this takes.

Select the following items for generating a more detailed performance database:

- one board only
- upm files (contain PP information)
- epm files (contain board and RFP information)
- a combination of the above selection criteria

If you cannot verify exactly which board, RFP, or PP causes the problem, import only the data files that contain the relevant information for your problem. For example, if an RFP on a specific board causes the problem, import the epm files of only that board (epm files contain board and RFP counters and timers). You can now efficiently generate a new, detailed database that contains only the relevant information.

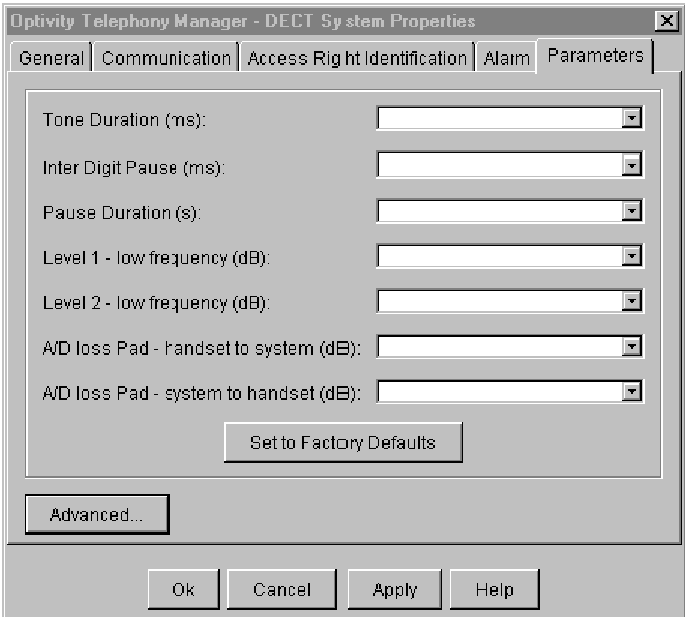
Statistical Performance Data

Table 36
Statistical Performance Data

Counter	Description
1	Indicators, not used
2	Number of page failures
3	Number of page retries
4	Number of page requests
5	Number of page rejects
6	Number of voice calls
7	Number of message calls
8	Number of voice calls, dropped in passive state
9	Number of voice calls, dropped in active state
10	Number of message calls, dropped in passive state
11	Number of message calls, dropped in active state
12	Number of hand overs
13	Number of failed hand overs
14	Number of aborted hand overs
15	Number of delayed hand overs
16	Current Circuit Number (0xFF, if none)

Setting parameters

Figure 313
DECT System Properties – Parameters tab


Optivity Telephony Manager - DECT System Properties
General
Communication
Access Right Identification
Alarm
Parameters
Tone Duration (ms):
Inter Digit Pause (ms):
Pause Duration (s):
Level 1 - low frequency (dB):
Level 2 - low frequency (dB):
A/D loss Pad - handset to system (dB):
A/D loss Pad - system to handset (dB):
Set to Factory Defaults
Advanced...
Ok
Cancel
Apply
Help

Complete the following steps.

Procedure 187
Setting parameters

Step	Action
1	Using Windows, login to OTM. Select the system that supports the DECT system, Launch the DECT application. Open the DECT Systems window. Open the Properties dialog, and click on the Parameters tab.
	Follow the instructions on page 440 to page 449.
2	Select the parameter.
	Select a pull-down menu item, and click **Apply**.

END

Recovering a password

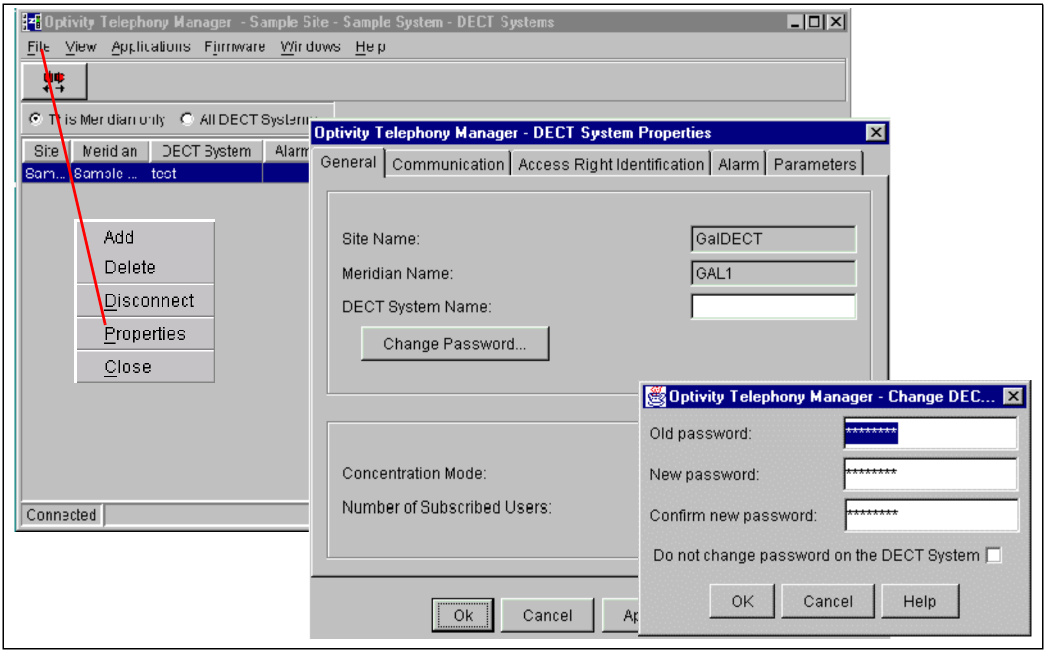
Passwords recovery is needed in several instances:

- If the DECT system password is changed by a customer, the distributor managing the system can be left without knowledge of the new password.
- The password can be damaged in the OTM database by a disk crash.
- The password can be forgotten.

Passwords cannot be accessed from the OTM.

The OTM provides a mechanism allowing the password to be reset to the factory password. The password can be changed in the DECT system and the OTM DECT database, or in the OTM DECT database only.

Figure 314
DECT Systems window, DECT Systems Properties, Change DECT Password


Optivity Telephony Manager - Sample Site - Sample System - DECT Systems
File View Applications Firmware Windows Help
This Meridian only
All DECT Systems
Site Meridian DECT System Alarm
Sam... Sample ... test
Add
Delete
Disconnect
Properties
Close
Connected
Optivity Telephony Manager - DECT System Properties
General Communication Access Right Identification Alarm Parameters
Change Password...
Concentration Mode:
Number of Subscribed Users:
Ok Cancel Ap
Optivity Telephony Manager - Change DEC...
OK Cancel Help

Site Name: GalDECT

Meridian Name: GAL1

DECT System Name:

Old password: ********

New password: ********

Confirm new password: ********

Do not change password on the DECT System □

Complete the following steps.

Procedure 188
Recovering a password

Step	Action
1	Using Windows, login to OTM. Select the system that supports DECT. Launch the DECT application. Open the DECT Systems window. Open the Properties dialog, and click on the General tab.
	Follow the instructions on page 440 to page 442.
2	Select password change.
	Click on **Change Password**.
3	Change to the factory default password. ***Note:*** The default is case-sensitive.
	Type **Arsenal** in the **New password** box.
4	Confirm the password.
	Type **Arsenal** in the **Confirm new password** box.
5	Set up for a password change the on the DECT system.
	Remove the DMC8 Relay card, and reinsert the DMC8 Relay card.
6	Connect to the DECT system ***within five minutes***.
	From the **Applications** pull-down menu click on **Connect** or the (green) icon.

END

Nortel DECT Messenger Contents

Release 3.0.0 - build 2004.08.02

This online documentation is shipped in Adobe Portable Document Format (PDF). You must install Adobe Acrobat Reader to view the documents.
"Acrobat® Reader Copyright © 1987-1999 Adobe Systems Incorporated. All rights reserved. Adobe is trademark of Adobe Systems Incorporated."

General - Install PC	
Step 2 - Nortel DECT Messenger	“Install PC – Step 2 – Nortel DECT Messenger” on page 873
Step 3 - National Instruments	“Install PC – Step 3 – National Instruments” on page 889
Step 4 - WebServer	“Install PC – Step 4 – Web Server” on page 949
Step 5 - SMTP Server	“Install PC – Step 5 – eSMTP_Server” on page 995
Step 6 - Configuration	“Install PC – Step 6 – eCONFIG” on page 1013
Reinstalling DECT Messenger	“Install PC – Reinstalling Nortel DECT Messenger” on page 1045

Modules	
eAPI	“Module eAPI” on page 1049
	“Module – eAPI sample” on page 1057
eASYNC	“Module – eASYNC” on page 1071
eBACKUP	“Module – eBACKUP” on page 1081
eCAP	“Module – eCAP” on page 1091
eESPA	“Module – eESPA” on page 1115
	“Module – eESPA – sample” on page 1125
eDMSAPI	“Module – eDMSAPI” on page 1127
eGRID	“Module – eGRID” on page 1141
eIO	“Module – eIO” on page 1149
eKERNEL	“Module – eKERNEL” on page 1163
eSMTP	“Module – eSMTP” on page 1173
eSMTP_server	“Module – eSMTP_server” on page 1189
eTM	“Module – eTM” on page 1205

Modules	
eTM_HA	“Module – eTM_HA” on page 1225
eWEB	“Module – eWEB” on page 1265

Tables (Part 1 of 2)	
eASYNC	“Table: eASYNC ” on page 1301
eBACKUP	“Table: eBACKUP” on page 1309
eCAP	“Table: eCAP_generic” on page 1315
eDMSAPI	“Table: eDMSAPI” on page 1327
	“Table: eDMSAPI_INBOUND” on page 1335
	“Table: eDMSAPI_INBOUND_EVENT” on page 1339
	“Table: eDMSAPI_INBOUND_RESULT” on page 1343
eESPA	“Table: eESPA” on page 1347
	“Table: eESPA_OUTBOUND_CFG” on page 1363
eIO	“Table: eIO_MODULE” on page 1367
	“Table: eIO_AI” on page 1371
	“Table: eIO_DI” on page 1381
	“Table: eIO_DO” on page 1387
eKERNEL	“Table: eKERNEL_AREA” on page 1391
	“Table: eKERNEL_ALARM” on page 1393
	“Table: eKERNEL_DEVICE” on page 1407
	“Table: eKERNEL_DEVICE_ALT” on page 1415
	“Table: eKERNEL_DEVICE_FORMAT” on page 1419
	“Table: eKERNEL_GROUP” on page 1425
	“Table: eKERNEL_GROUP_AUTH” on page 1429

Tables (Part 2 of 2)

Nortel DECT Messenger Administrator Guide

This chapter contains information on the following topics:

Preface

This chapter is the Administrator Guide for the DECT Messenger and provides an overview of Nortel DECT Messenger. The chapter also provides important information about the structure of eCONFIG, and offers information on creating, deleting, and making changes to Users, Devices, and Groups.

This chapter does not cover all 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 more information about the menu parameters in the eCONFIG module, refer to:

- "eCONFIG basic concepts" on page 623
- "eCONFIG" on page 629
- "Using eCONFIG" on page 725
- "Install PC – Step 6 – eCONFIG" on page 1013

For detailed information on any of the other modules, see the appropriate chapters in this document.

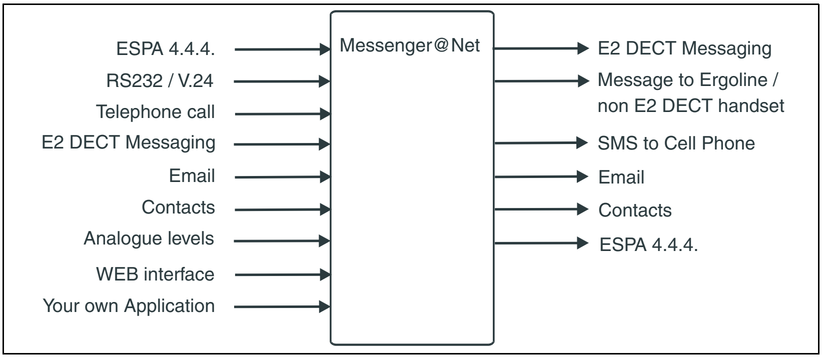
DECT Messenger overview

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

What is Nortel DECT Messenger

The DECT Messenger is a software platform that allows message generation, message routing, and message protocol conversion. Figure 315 shows the inputs and outputs of DECT Messenger.

Figure 315
Nortel 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 the 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 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 the DECT Messenger: the DECT Messenger provides a port on TCP/IP that is open to receive input data from this type of unique program.

Message output

The DECT Messenger supports the following output:

- DECT E2 messages (up to 160 characters)

  Although the 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 when a call is connected

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

- SMS messages to cell phones

  The 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

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

Modules overview

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

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

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

Kernel modules

There are two main modules that are used for the core software:

- eKERNEL

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

- 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.

Incoming and outgoing modules

There are nine modules (incoming and outgoing) that communicate with the eKERNEL module. Incoming modules receive messages and outgoing modules send messages. Each module has a specific incoming function, outgoing function, or both. Table 37 on page 621 provides an overview of the modules.

Table 37
Incoming and outgoing Modules (Part 1 of 2)

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	-

Table 37
Incoming and outgoing Modules (Part 2 of 2)

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

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 automatically detects when another DECT Messenger module is down and restarts it.

eCONFIG basic concepts

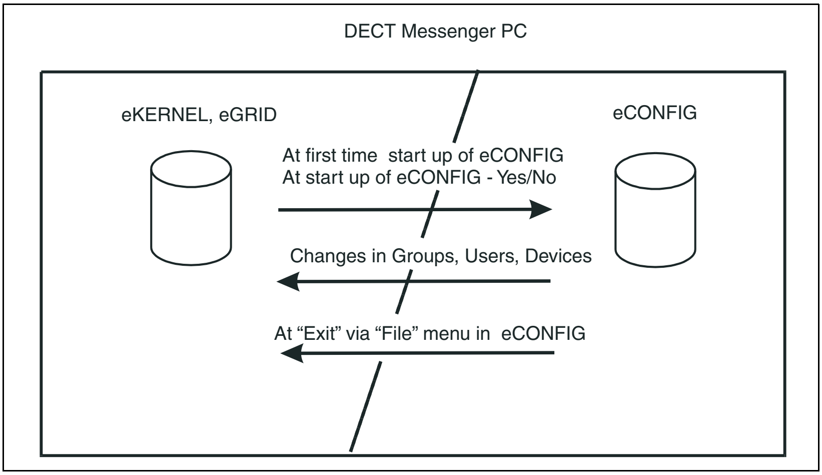
The system configuration is stored in a database. You use the eCONFIG module to make changes to the configuration. This section explains how the eCONFIG module uses the database.

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

When the eCONFIG is installed on the DECT Messenger server PC, the database is handled as shown in Figure 316.

Figure 316
Database handling when eCONFIG is on local 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

When you open the eCONFIG for the first time, the eCONFIG makes a copy of the operational configuration database in the DECT Messenger. This copy is stored in the eCONFIG. When you make configuration changes using the eCONFIG, these changes are stored in the 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. When you restart the modules that you closed down, the new configuration becomes active.

When 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 1: When you make changes in the database copy that resides in eCONFIG, ensure that no one else is making changes in the operational database. If there are other pending changes, an error can occur when you shut down the eCONFIG and try to write the database into the DECT Messenger directory.

Note 2: When 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 have made are lost (except for the changes in Users, Groups, and Devices).

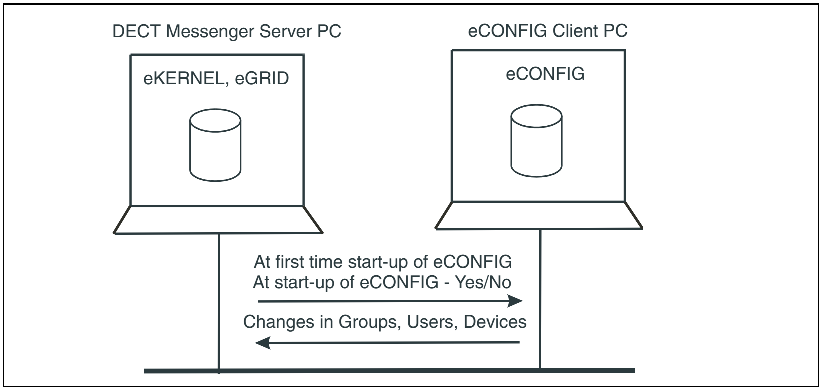
Restarting the eCONFIG

When you restart the program, eCONFIG finds a database in its directory. The eCONFIG asks you whether you want to continue with this database, or retrieve a fresh copy from the operational database. Nortel recommends that you make a fresh copy of the operational database to ensure that there is no database inconsistency.

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

When 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 317.

Figure 317
Database handling when eCONFIG is installed on a remote PC


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

When you open the eCONFIG for the first time at the remote PC, a copy is made of the configuration database of the 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.

When 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 1:*** If there is more than one eCONFIG active at the same time, on different PCs, the individual eCONFIG databases are not updated/ synchronized when 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 2:*** The database is never saved to the server PC when you work on a remote PC.

Restarting the eCONFIG

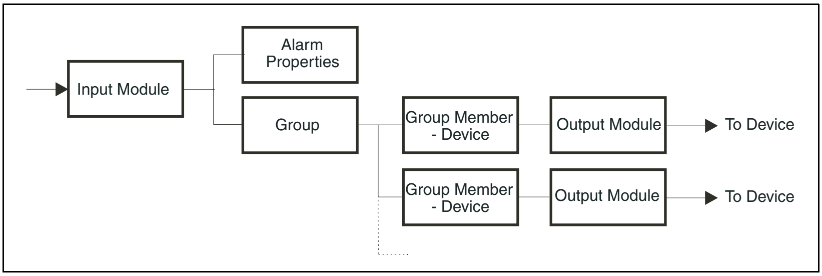
When you restart the program, eCONFIG finds a database in its directory. The eCONFIG asks you whether you want to continue with this database, or retrieve a fresh copy from the operational database. Nortel recommends that you make a fresh copy of the operational database to ensure that there is no database inconsistency. Database inconsistency can occur when other users make changes in the database from another PC or at the server PC.

DECT Messenger concepts

The 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 318 on page 627 shows the relation among the modules and how messages are processed.

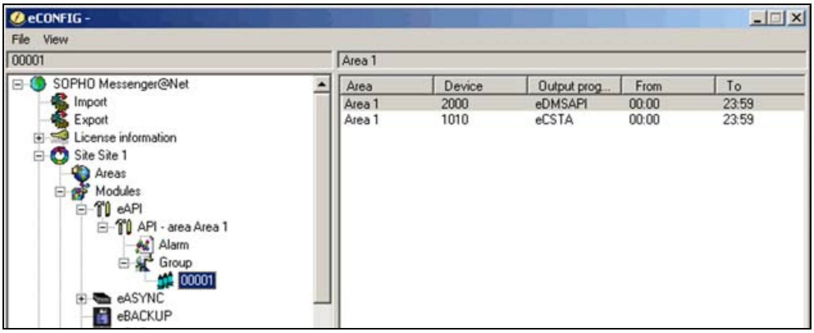
Figure 318
Alarm processing structure



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 319 on page 628 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 IBS 1**). Each input module displays different properties.

Figure 319
eCONFIG



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

The following explanations relate to the blocks in Figure 319 on page 628:

- **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 633). 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.

- **Group**

  The group identifier that originates at the input module determines the group to which the alarm must be sent. In Figure 319, 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 319 on page 628, 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.

The following sections contain instructions for creating, deleting, and changing parameters in Groups, Users, and Devices:

- “Managing devices” on page 635
- “Managing groups” on page 646
- “Managing group members” on page 655
- “Managing users” on page 664

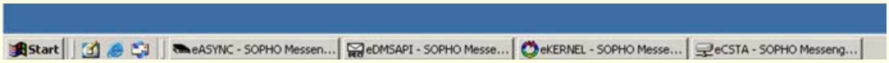
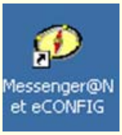
eCONFIG

This section contains the following topics related to the eCONFIG:

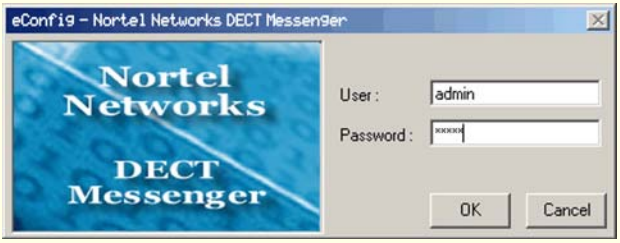
- “Opening the eCONFIG” on page 630
- “eCONFIG main window” on page 633

Opening the eCONFIG

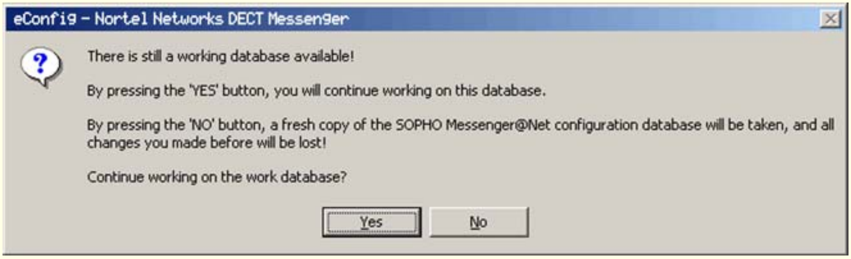
Procedure 189
Opening the eCONFIG (Part 1 of 3)

Step	Action
1	Ensure that the 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, the Windows taskbar indicates that the eKERNEL is running by displaying the corresponding icon.  Start eASYNC - SOPHO Messen... eDMSAPI - SOPHO Messe... eKERNEL - SOPHO Messe... eCSTA - SOPHO Messeng... If other modules are also running, an icon is displayed for each (for example, the eDMSAPI).
3	Start up the eCONFIG.
	Double-click the eCONFIG icon on the PC desktop. 

Procedure 189
Opening the eCONFIG (Part 2 of 3)

Step	Action
4	Enter your login information.
	The Signon dialog box opens:  eConfig – Nortel Networks DECT Messenger Nortel Networks DECT Messenger OK Cancel User : admin Password : ***** 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).

Procedure 189
Opening the eCONFIG (Part 3 of 3)

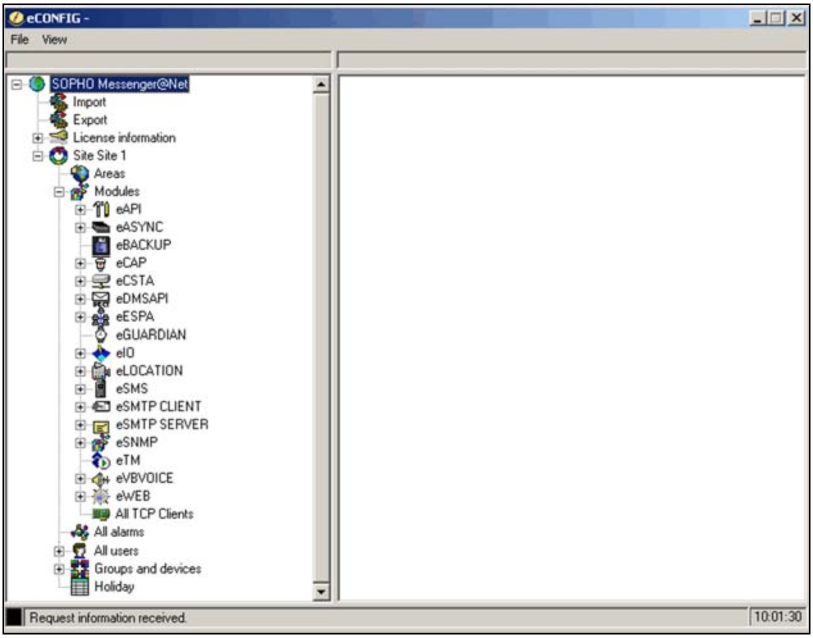
Step	Action
5	Select the database.
	The following message box opens:  eConfig - Nortel Networks DECT Messenger There is still a working database available! By pressing the 'YES' button, you will continue working on this database. By pressing the 'NO' button, a fresh copy of the SOPHO Messenger@Net configuration database will be taken, and all changes you made before will be lost! Continue working on the work database? ***Note:*** The eCONFIG asks you which database you want to use. Ensure that you have read the information on database handling in “eCONFIG basic concepts” on page 623 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. Nortel recommends that you choose this option. It ensures that you have a copy of the actual operational database. When working on a remote PC, you must select this option to avoid conflicts with changes made from other locations by other users.
6	The eCONFIG main window opens.
	Detailed information about the **eCONFIG** main window is provided in “eCONFIG main window” on page 633.

END

eCONFIG main window

The main eCONFIG window is shown in Figure 320.

Figure 320
eCONFIG main window



Request information received.

10:01:30

Note: The contents of the eCONFIG window are different per user or per system configuration. Figure 320 shows all the menu items that are possible.

Explanations of the menu items are as follows:

- 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.
- Licence information: provides information about the current licences that are active in your DECT Messenger. You cannot make licence 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 DMC with DECT. For each connection from your DECT Messenger to a DMC system, you must specify a different area. Use a number to identify the area. The area number is used in the various modules in the 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 1: The list of modules can differ per user. The list of modules is displayed only if you have view/edit rights.

  Note 2: 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 explains the following DECT Messenger tasks:

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

The following are examples of devices in DECT Messenger:

- DNR in the DMC
- e-mail address
- cell phone number (for SMS)
- relay contacts

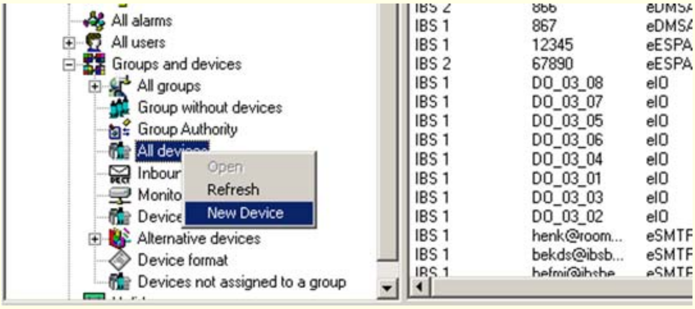
Because of the device type variety, you must know the properties for each device in the equipment where the device exists (that is, the properties in the DMC, in the Mail Server, and so on).

> ***Note:*** Task procedures are in 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

Procedure 190 describes how to create a new device.

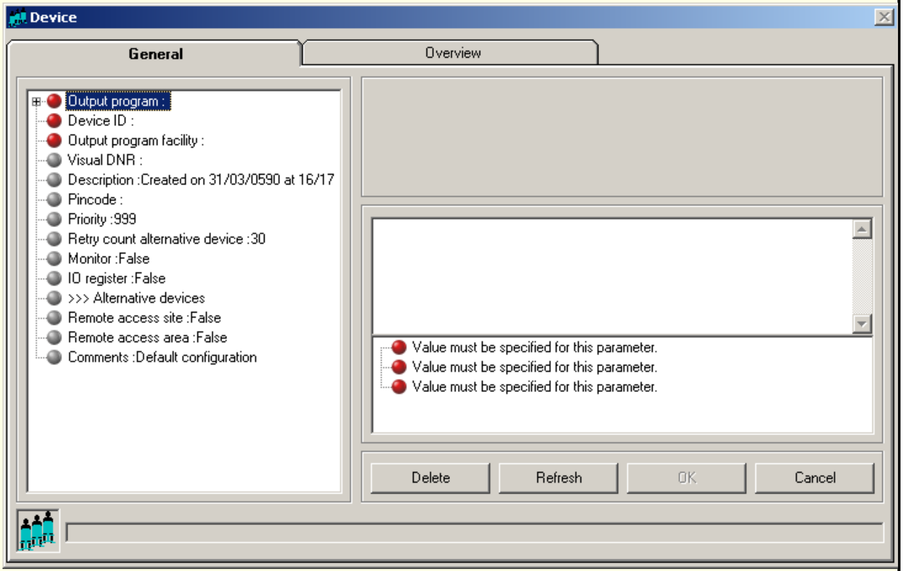
Procedure 190
Creating a new device (Part 1 of 3)

Step	Action
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	eDMSA
IBS 1	867	eDMSA
IBS 1	12345	eESPA
IBS 2	67890	eESPA
IBS 1	DO_03_08	el0
IBS 1	DO_03_07	el0
IBS 1	DO_03_05	el0
IBS 1	DO_03_06	el0
IBS 1	DO_03_04	el0
IBS 1	DO_03_01	el0
IBS 1	DO_03_03	el0
IBS 1	DO_03_02	el0
IBS 1	henk@room...	eSMTF
IBS 1	bekds@ibsb...	eSMTF
IBS 1	hefmi@ibsbe	eSMTF

Procedure 190
Creating a new device (Part 2 of 3)

Step	Action
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. • Nortel 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 641.

Procedure 190
Creating a new device (Part 3 of 3)

Step	Action
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.
	END

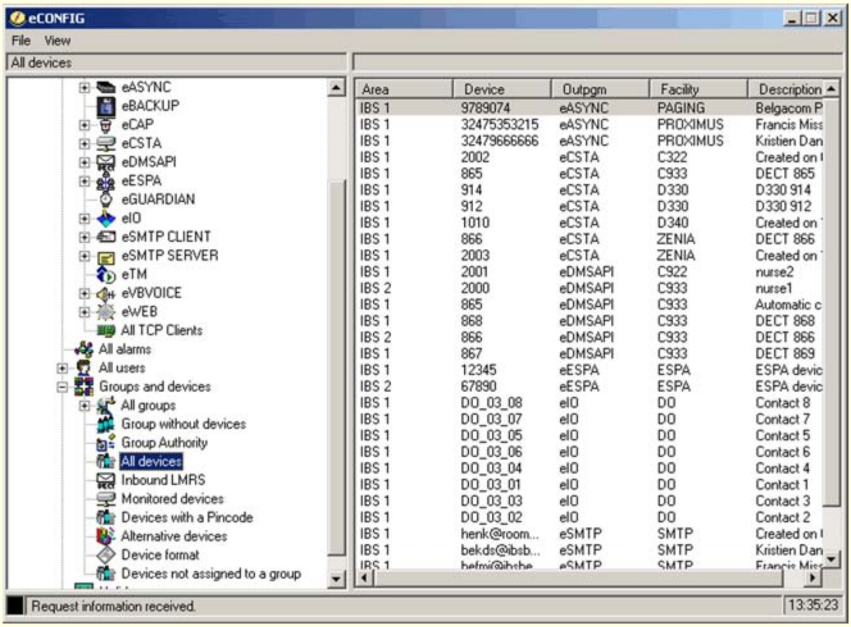
Changing device parameters

Procedure 191 describes how to change device parameters.

Procedure 191
Changing device parameters (Part 1 of 4)

Step	Action
1	Access the eCONFIG **Groups and Devices** menu.
	• Open eCONFIG. • Expand the **Groups and Devices** menu by clicking the **+** to the left of it.

Procedure 191
Changing device parameters (Part 2 of 4)

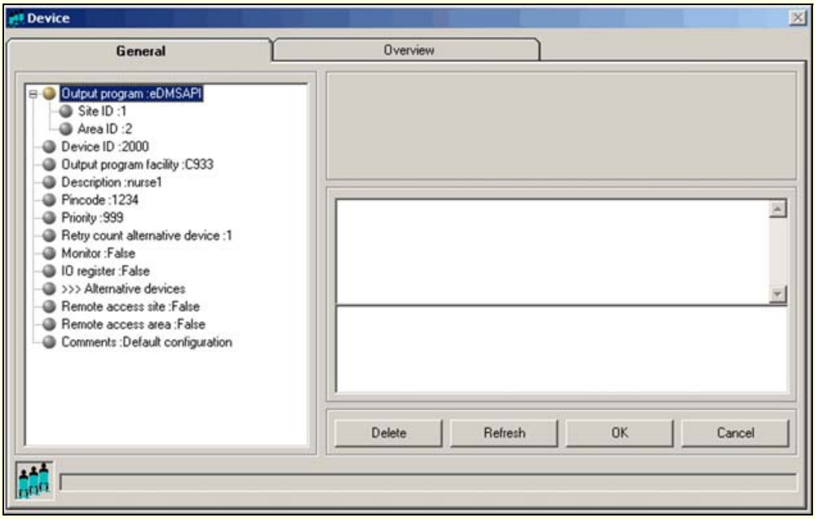
Step	Action
2	Open the **All Devices** information window.
	Left-click the **All Devices** parameter. The following window opens (example): 

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

Procedure 191
Changing device parameters (Part 3 of 4)

Step	Action
3	Select the device of your choice.
	• In the right panel, browse in the list of devices in the 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

Procedure 191
Changing device parameters (Part 4 of 4)

Step	Action
4	Change the parameters.
	Click the name of the property you want to change. When editing the parameters, note the following: • You cannot change the **Output Program**, the **Site ID**, the **Area ID**, or the **Device ID**. • Nortel 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 641.
5	Confirm your choices.
	Click **OK** and follow the instructions on the screen, if applicable.
	END

Deleting a device

To delete a device, follow the procedure for changing the device parameters (see section “Changing device parameters” on page 638). At Step 4 of Table 191 on page 638, click the **Delete** button to delete the device. The DECT Messenger asks you to confirm the action. When you confirm the action, the device is deleted immediately.

Device parameters

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

- Output Program

  This field specifies the output program that processes a request. Note that a device can be defined for 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).

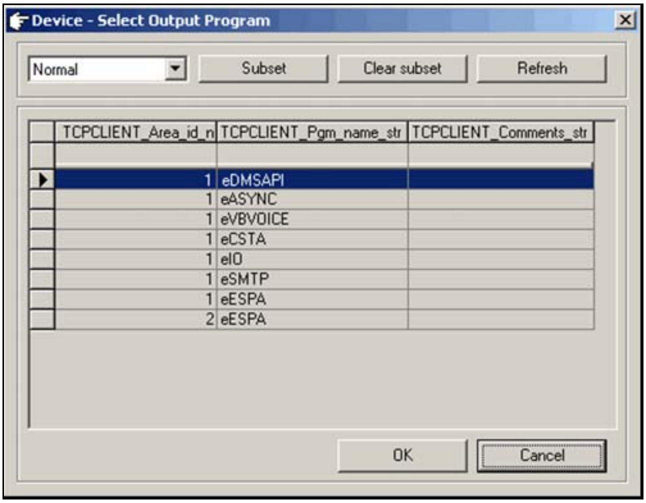
— eIO for enabling/disabling discrete output contacts.

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

Note 1: 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 2: Selecting the output program is only possible when you create a new device. Always use the **Browse** button to select the output program. Figure 321 on page 642 shows the browser window.

Figure 321
Select Output Program 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	

- Device ID

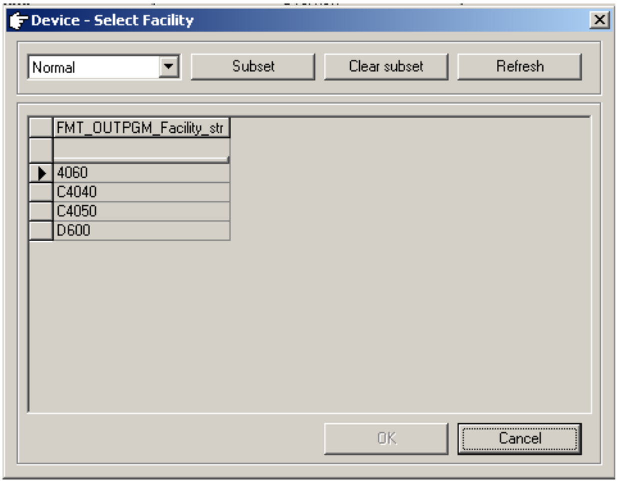
  The device ID is the actual identifier of the device in the output equipment. For instance, if the device is a DECT handset, this field specifies the board number#index number (for example 04#01). When an e-mail destination is defined, the field contains an e-mail address (for example, henk@company1.org).

- 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, the 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 322 on page 643 shows the selection window for the eDMSAPI.

Figure 322
Device Select Facility



FMT_OUTPGM_Facility_str
4060
C4040
C4050
D600

- 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. When a device sends an E2 message, the message always goes to the DECT Messenger directly (and not to the destination number). Messages sent to the DECT Messenger are processed by the 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. When 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

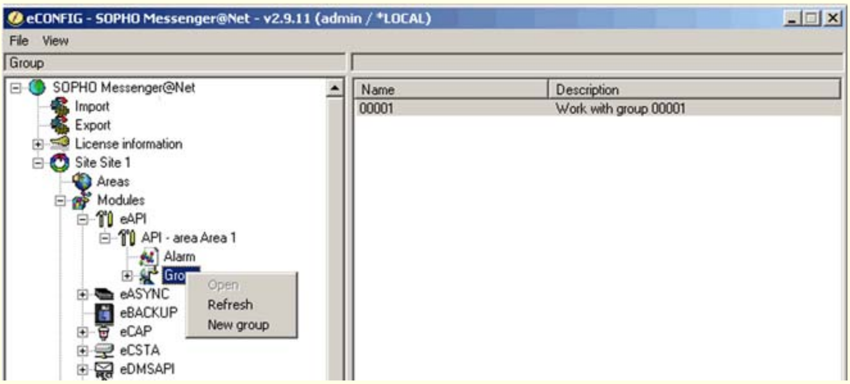
Creating a new group

Procedure 192 describes how to create a new group.

Procedure 192
Creating a new group (Part 1 of 4)

Step	Action
1	Open eCONFIG.

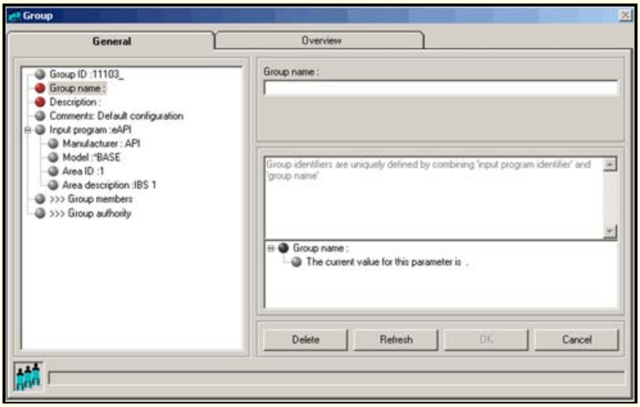
Procedure 192
Creating a new group (Part 2 of 4)

Step	Action
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.  eCONFIG - SOPHO Messenger@Net - v2.9.11 (admin / *LOCAL) Name: 00001 — Description: Work with group 00001 File View Group SOPHO Messenger@Net Import Export License information Site Site 1 Areas Modules eAPI API - area Area 1 Alarm Gro Open Refresh New group eASYNC eBACKUP eCAP eCSTA eDMSAPI Name Description - 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.

Procedure 192
Creating a new group (Part 3 of 4)

Step	Action
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 .

When 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.
- Nortel recommends that you use the **Browse** option, when present, to define a location, rather than typing an entry.

Note 1: 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 2: 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 652.

Procedure 192
Creating a new group (Part 4 of 4)

Step	Action
4	Confirm your choices.
	Click **OK** and follow the instructions on the screen, if applicable.
	END

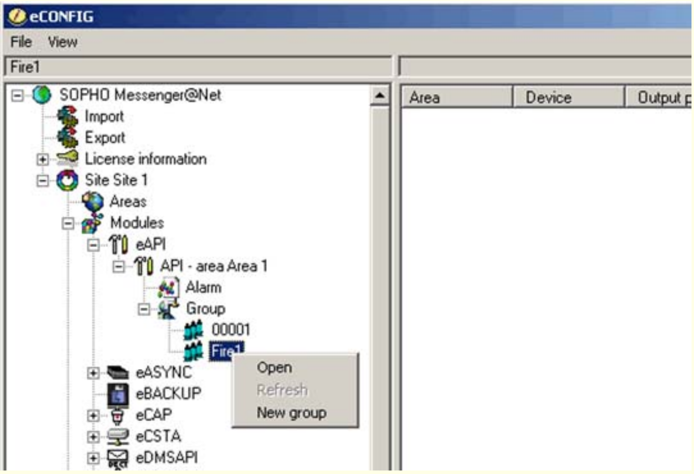
Changing group parameters

Procedure 193 describes how to change group parameters.

Procedure 193
Changing group parameters (Part 1 of 3)

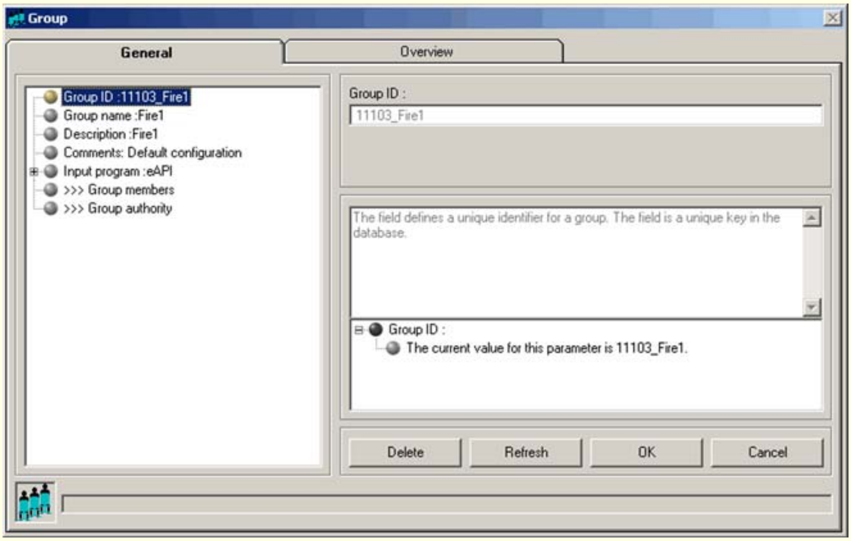
Step	Action
1	Open eCONFIG.
2	Select the input module for which you want to change the group parameters.
	Select the input module for which you want to change group parameters from the **Modules** menu. ***Note:*** A group is always associated with an input module. However, to change group parameters, you can also select a group from the **Groups and Devices** menu.

Procedure 193
Changing group parameters (Part 2 of 3)

Step	Action
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.  eCONFIG File View Fire1 SOPHO Messenger@Net Import Export License information Site Site 1 Areas Modules eAPI API - area Area 1 Alarm Group 00001 Fire1 eASYNC eBACKUP eCAP eCSTA eDMSAPI Open Refresh New group Area Device Output p • Select **Open.** The **Group Properties/Parameters** window opens.

Procedure 193
Changing group parameters (Part 3 of 3)

Step	Action
4	Change group parameters.

	The parameters are described in section “Group parameters” on page 652.
	
	 Group
	General
	Overview
	Delete
	Refresh
	OK
	Cancel
	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.

END

Deleting a group

To delete a group, follow the procedure for changing the group parameters (see “Changing group parameters” on page 649). At Step 4 of Procedure 193 on page 649, click the **Delete** button to delete the group. The DECT Messenger asks you to confirm the action. When 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 when 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: It is possible to use the same group name for more than one input program. This is possible 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 when you create the group. However, you can change the group name later. The Group ID remains the same.

- Description

  The **Description** field contains descriptive text that allows administrators to easily recognize the group (for example, Intensive Care).

- Comments

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

- Input program

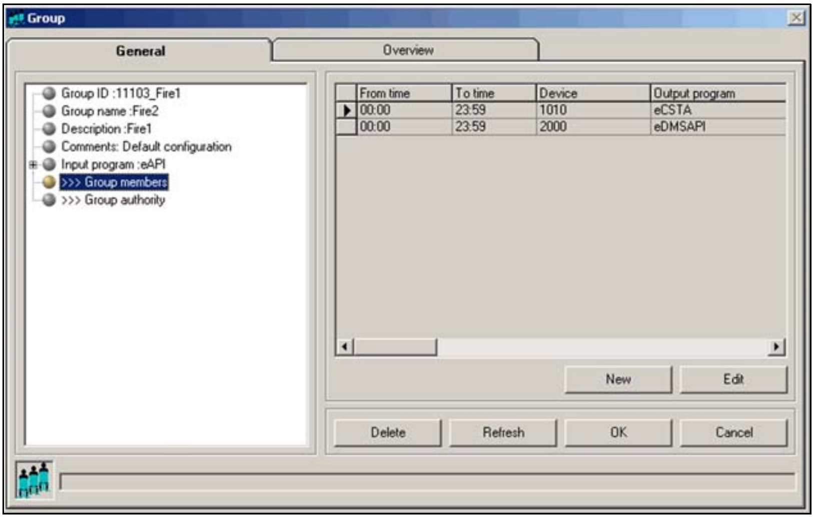
  The **Input program** parameter provides information about the input program. You cannot change this parameter. When you create a new group for an input program, these parameters are assigned automatically.

- Group members

  Use the **Group members** parameter to assign group members to the group (assign devices to the group from the list of devices). Once assigned, these devices become group members. If the device (for example, an extension) that you want to assign is not in the list, then you must create that device first according to the procedures “Creating a new device” on page 636.

  Use the **Group members** menu to open the window shown in Figure 323.

Figure 323
Group members window



- 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

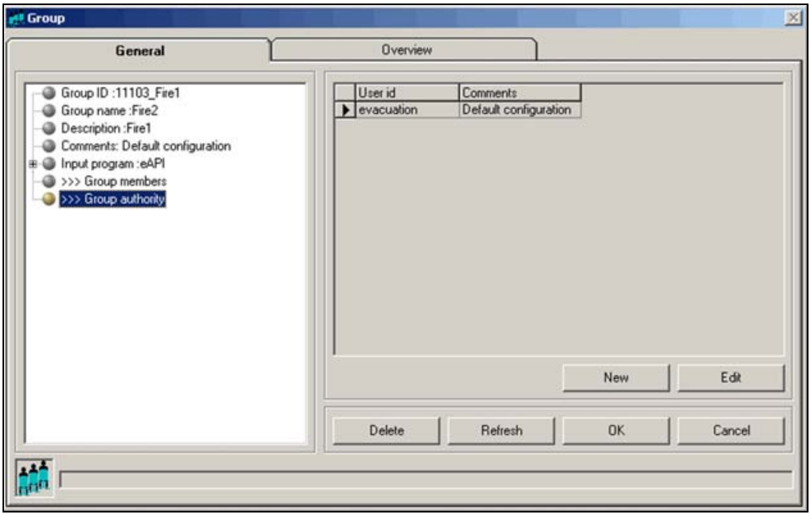
The section “Changing group member parameters” on page 660, provides information on assigning new members, editing members, and deleting members.

- 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. A special value ***ALL** can be implemented. If you specify this value, 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 324.

Figure 324
Group authority



- 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

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 324 on page 655, 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 656
- "Changing group member parameters" on page 660

- "Removing a group member" on page 661
- "Member parameters" on page 661

Assigning a new member to a group

Procedure 194 describes how to assign a new member to a group.

Procedure 194
Assigning a new member to a group (Part 1 of 4)

Step	Action
1	Open eCONFIG.
	Ensure that the member that you want to assign to the group is already in the 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 636.

Procedure 194
Assigning a new member to a group (Part 2 of 4)

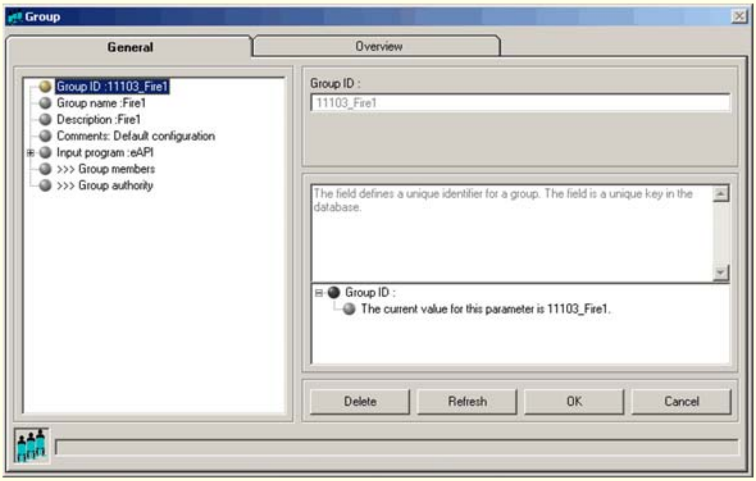
Step	Action
2	Access the **Group Properties** window.

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.**



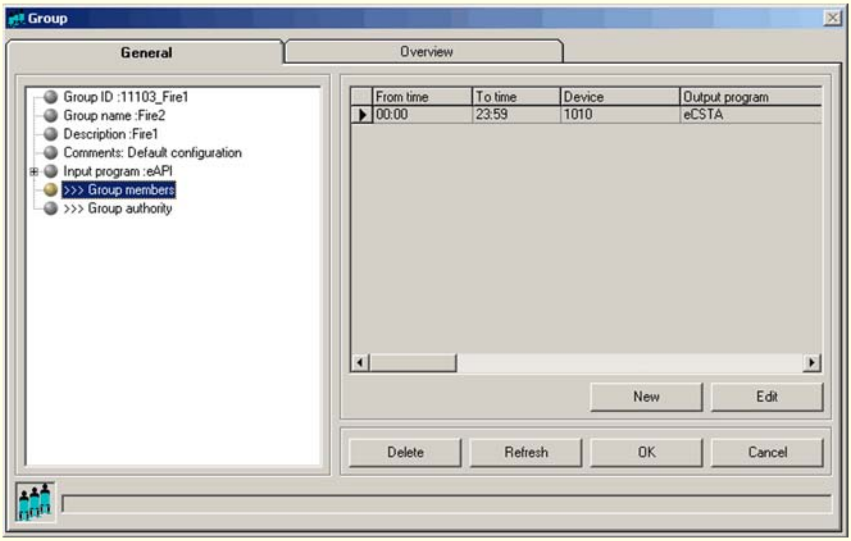
Group ID :11103_Fire1
Group name :Fire1
Description :Fire1
Comments: Default configuration
Input program :eAPI
>>> Group members
>>> Group authority

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.

Procedure 194
Assigning a new member to a group (Part 3 of 4)

Step	Action
3	Open the **Group members** window.
	Click the **>>>Group members** item.  A list of group members displays (the example shows only one group member: device 1010).

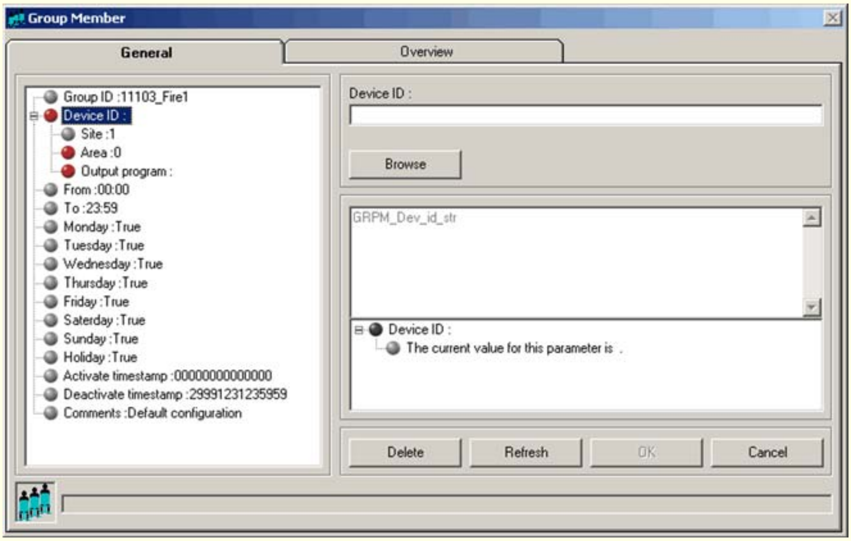
Group

General | Overview

- 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

Procedure 194
Assigning a new member to a group (Part 4 of 4)

Step	Action
4	Add a new member.
	- Click **New**. The following window opens.  Group Member General Overview Browse Delete Refresh OK Cancel 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 on 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:*** When you select a device, the area and output program are defined automatically for the member. See “Member parameters” on page 661 for more information on the parameters.
5	Confirm your choices.
	Click **OK** and follow the instructions on the screen, if applicable.
	END

Changing group member parameters

Procedure 195 describes how to change the parameters for a group member.

Procedure 195
Changing group member parameters

Step	Action
1	Open the **Group members** window.
	Follow Steps 1, 2, and 3 in “Assigning a new member to a group” on page 656.
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 Table 194 on page 656, opens, however all parameters are entered. • Click on 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.

END

Removing a group member

Procedure 196 describes how to remove a member from a group.

Procedure 196
Removing a group member

Step	Action
1	Open the **Group members** window.
	Follow Steps 1, 2, and 3 in “Assigning a new member to a group” on page 656.
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 Table 194 on page 656, 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.

END

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 when 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 when 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 when you click on this menu item.

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

- 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 above). 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. When set to **True**, the member is active on that day.

- Holiday

  This value is a Boolean value: True or False. When 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 when 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 when 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. This functionality allows you 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

The 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.

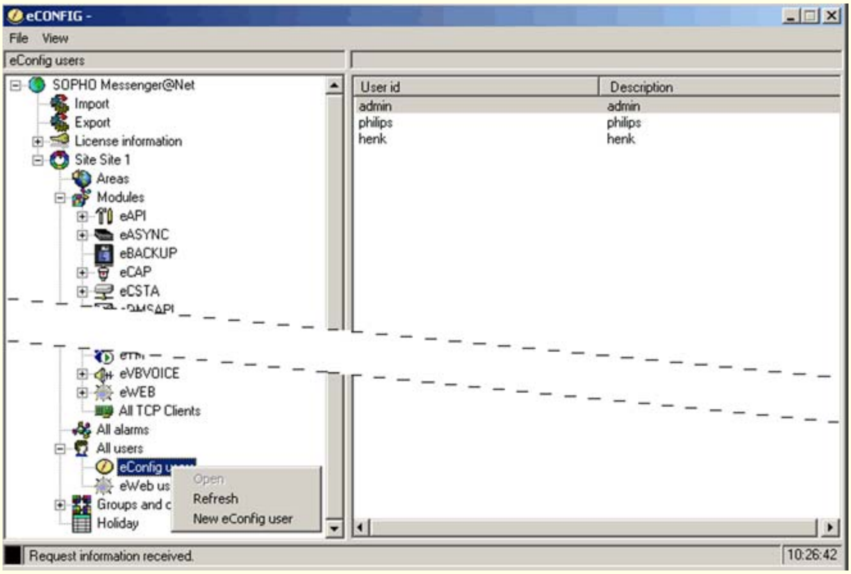
Creating a new user

Procedure 197 describes how to create a new user.

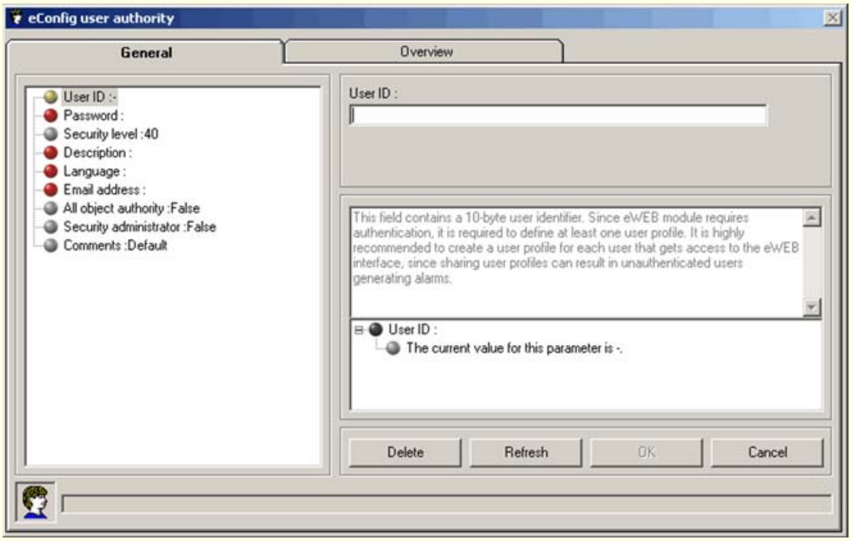
Procedure 197
Create a new user (Part 1 of 3)

Step	Action
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.

Procedure 197
Create a new user (Part 2 of 3)

Step	Action
3	Access the pop-up menu.
	In the **All users** menu, right-click either eCONFIG or eWEB.  eCONFIG - File View eConfig users SOPHO Messenger@Net Import Export License information Site Site 1 Areas Modules eAPI eASYNC eBACKUP eCAP eCSTA eDMSAPI eTM eVBVOICE eWEB All TCP Clients All alarms All users eConfig u eWeb us Groups and c Holiday Open Refresh New eConfig user User id Description admin admin philips philips henk henk Request information received. 10:26:42
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**

Procedure 197
Create a new user (Part 3 of 3)

Step	Action
5	Enter the parameters for the new user.
	Select each item in the left panel and enter parameters.  eConfig user authority General Overview Delete Refresh OK Cancel 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 669.
6	Confirm your choices.
	Click **OK** and follow the instructions on the screen, if applicable.

END

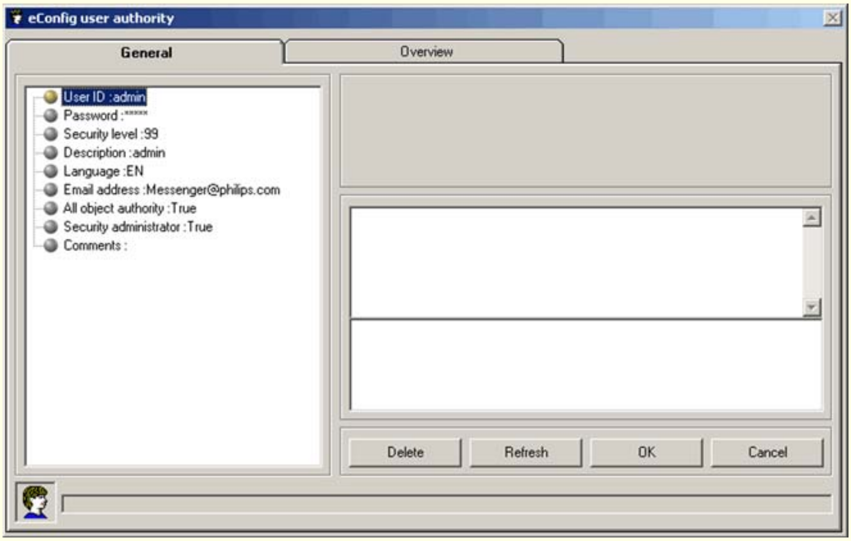
Changing user properties

Procedure 198 describes how to create a new user.

Procedure 198
Changing user properties (Part 1 of 2)

Step	Action
1	Open the Group Members window.
2	Expand the All Users menu.
	Two sub-menu items are listed: 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 sub-menu item that contains the user you want to edit.
	Select either eCONFIG or eWEB, dependent 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.

Procedure 198
Changing user properties (Part 2 of 2)

Step	Action
5	Change the parameters.
	Change the parameters by clicking the item and changing the field contents.  eConfig user authority General Overview Delete Refresh OK Cancel 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 669.
6	Confirm your choices.
	Click **OK** and follow the instructions on the screen, if applicable.

END

Deleting a user

Procedure 199 describes how to delete a user.

Procedure 199
Deleting a user

Step	Action
1	Open the User Properties window.
	Follow Steps 1, 2, 3, and 4 of the procedure in “Changing user properties” on page 667.
2	Delete the user.
	Click the **Delete** button.
3	Confirm your choices.
	Click **OK** and follow the instructions on the screen, if applicable.

END

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. Nortel 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, Nortel 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**

  The **security level** parameter allows you 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 could be assigned to top-level administrators. The value 00 is the lowest possible value. Nortel 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. When 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 **All object authority** parameter allows the user to maintain all groups in the DECT Messenger. Remember that a user can be assigned to a group. When 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 the 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

  When 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.

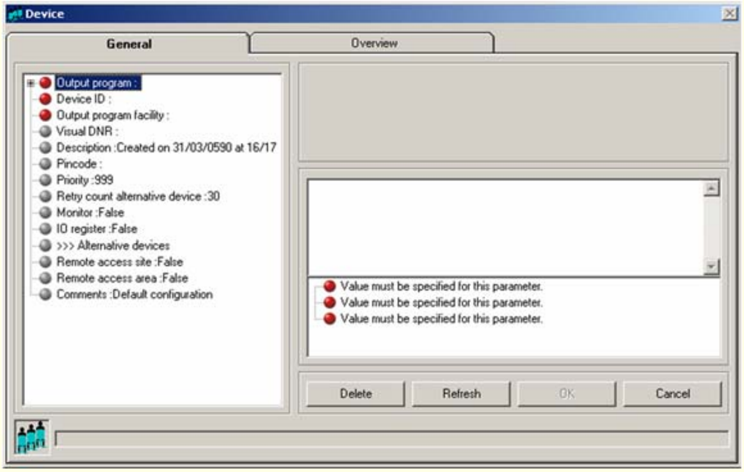
Adding a DECT device to the Messenger system

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

Procedure 200
Adding a DECT device to the Messenger system (Part 1 of 6)

Step	Action
1	Configure a device format.
	Ensure that you have a Device Format for this type of DECT handset. See “Table: eKERNEL_DEVICE” on page 1407, and “Table: eKERNEL_DEVICE_FORMAT” on page 1419, for more information on defining device facilities. 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.

Procedure 200
Adding a DECT device to the Messenger system (Part 2 of 6)

Step	Action
2	Add new Device.
	Within **Groups and Devices** right click on **All Devices**, and choose **New Device.**  Device General Overview Delete Refresh OK Cancel ● 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.

Procedure 200
Adding a DECT device to the Messenger system (Part 3 of 6)

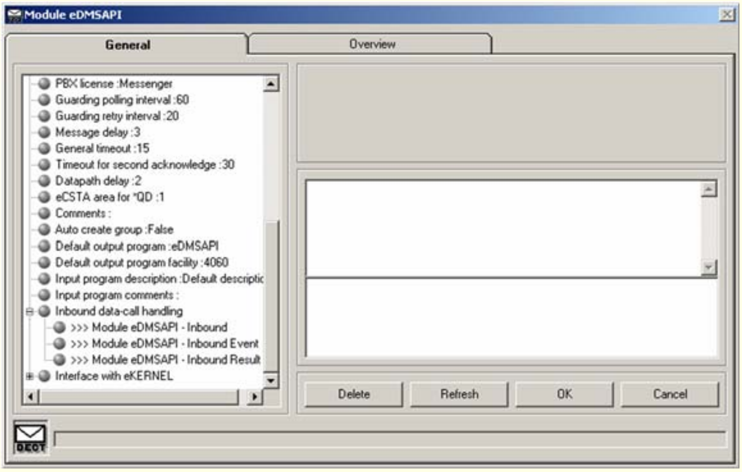
Step	Action
3	Configure the new device.
	Make the following configuration changes: • Select **eDMSAPI** as the Output program. • Device ID Board_Number#Index_Number Example: For a DMC Card in Slot 4 of an Option 11c Cabinet, and a DECT handset subscribed to **index 2, 04#02** • Configure the Output Program Facility according to the type of DECT handset you have. Example: **C4050** • Visual DNR The 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 drop-down-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, and the sub-items **Alarm** and **Group** are visible. Click on **Alarm**. • Ensure that you have at least two Alarms, as follows: — E2_MSG_N — E2_MSG_U

Procedure 200
Adding a DECT device to the Messenger system (Part 4 of 6)

Step	Action
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, and the sub-items **Alarm** and **Group** are visible. • Right-click on **Group**, and select **New Group** in the pop-up menu. (Refer to page 636 - Creating a Group)
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 on **New**. Browse under Device_ID for the device you created in Step 2. • Group Authority. Click on **New**. Under User_ID browse for ***ALL**

Procedure 200
Adding a DECT device to the Messenger system (Part 5 of 6)

Step	Action
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 on 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 sub-menus are displayed:
	— Inbound
	— Inbound Event
	— Inbound Result
	
	Module eDMSAPI
	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
	 General
	Overview
	Delete
	Refresh
	OK
	Cancel
	DECT

Procedure 200
Adding a DECT device to the Messenger system (Part 6 of 6)

Step	Action
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]

END

DECT Messenger Customer Engineer Manual

This chapter contains information on the following topics:

- “V.24 - RS232 connections (eCAP, eESPA)” on page 790
- “Using Import/Export menu” on page 792
- “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 793
- “Checking diagnostics” on page 794

Preface

This chapter is for Nortel DECT Messenger, and is designed to be used in addition to the DECT Messenger documentation found in other chapters. This chapter describes the steps necessary to configure and begin using the system, and also describes how various modules work. For details on the modules, consult later chapters.

The process for installing the DECT Messenger is described in “Install PC – Step 2 – Nortel DECT Messenger” on page 873.

> ***Note:*** No legal rights can be obtained from the information in this manual.

About the manual

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

The modules and related database tables are described in detail in later chapters as follows:

- Tables: pages 1301 through 1515.
- Modules: pages 1049 through 1265.

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 need to 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 Nortel 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 Nortel 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 when 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, when 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. Nortel applications can use a range of ports and access types. Contact Nortel 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 Nortel 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 when 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 re-naming 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:

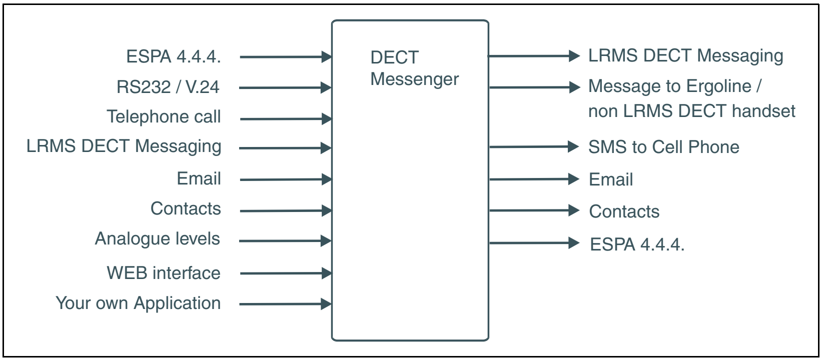
- "Nortel DECT Messenger functional description" on page 683
- "Modules overview" on page 686
- "Linking modules" on page 689

Nortel DECT Messenger functional description

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

Figure 325 on page 684 shows the various inputs and outputs of the DECT Messenger.

Figure 325
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 to the DECT Messenger server PC: send a message by e-mail to a telephone set, or SMS to cell phone, or any other output on the 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 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 the DECT Messenger: the DECT Messenger provides a port on TCP/IP that is open to receive input data from this type of unique program.

Message output

The DECT Messenger supports the following output:

- DECT E2 messages (up to 160 characters)

  Although the 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 when 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 per device type. Messages that are too long to be displayed are broken into sections suitable for the display devices.

- SMS messages to cell phones

  The 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

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

Modules overview

The 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 located 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 are nine modules (incoming and outgoing) that communicate with the eKERNEL module. Incoming modules receive messages, and outgoing modules send messages. Table 38 provides an overview of the modules.

Table 38
Incoming and outgoing modules (Part 1 of 2)

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	-

Table 38
Incoming and outgoing modules (Part 2 of 2)

Module Name	Function	Incoming	Outgoing
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 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

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.

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 located anywhere in a TCP/IP network. Figure 326 shows logical links between the modules. Figure 327 on page 691 shows a practical example of module linking.

Figure 326
Example of logical representation of module links

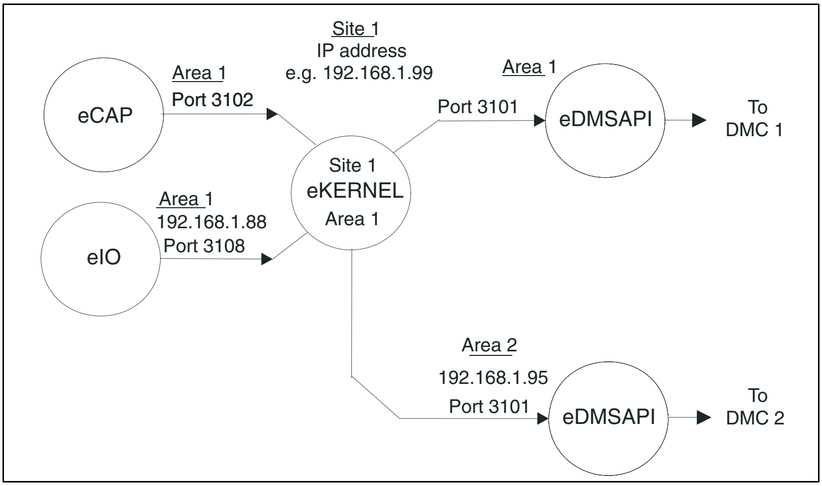
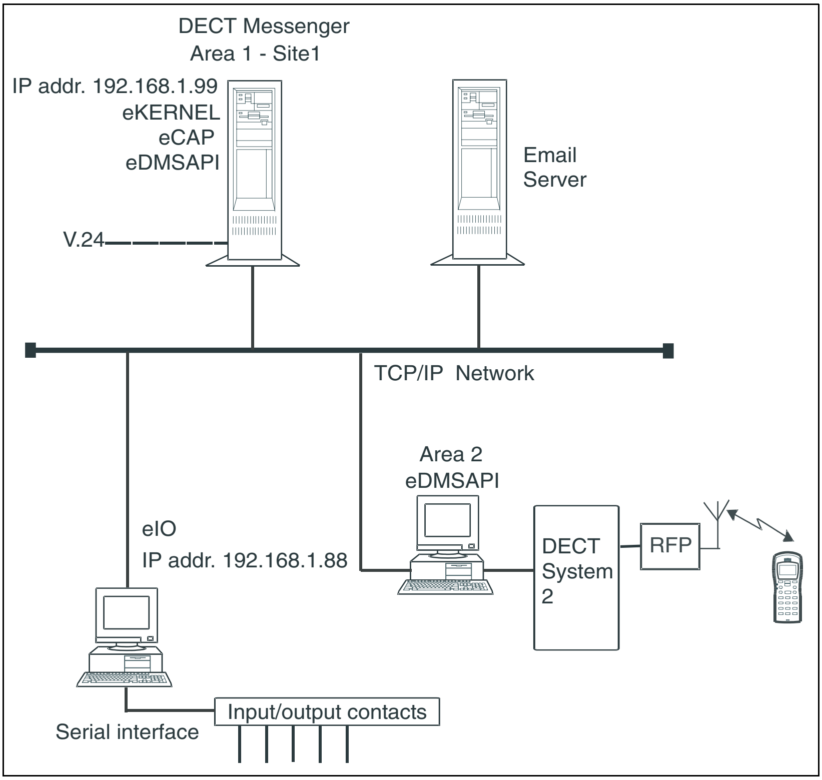


Figure 327
Example of module links (practical)



In Figure 326, 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 326. 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. When 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 per 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. This allows you to set up a second eKERNEL (that is, a second site) offline. Once the configuration is set, you can shut down the first site, and start the second one.

  Table 39 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 39
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 326 on page 690 and Figure 327 on page 691, the site and area structure is shown in Table 40.

Table 40
Site and Area structure

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

This modular structure allows you 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 the DECT Messenger

DECT Messenger in a MAN or WAN network

The DECT Messenger can be used in a multiunit MAN (IMP network), or in a multinode WAN (DPNSS network). If the DECT Messenger is installed in a multiunit DMC network (MAN), you can send LRMS (E2) messages to DECT handsets in units other than that in which the DECT Messenger is connected. The IMP links support LRMS (E2) messaging, but this generates a heavy load on the interunit links. Therefore, Nortel 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, Nortel recommends that you make a direct DECT Messenger connection to those other units, as well. Figure 328 on page 694 shows a configuration in which the 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 328
DECT Messenger in a multiunit or multinode environment

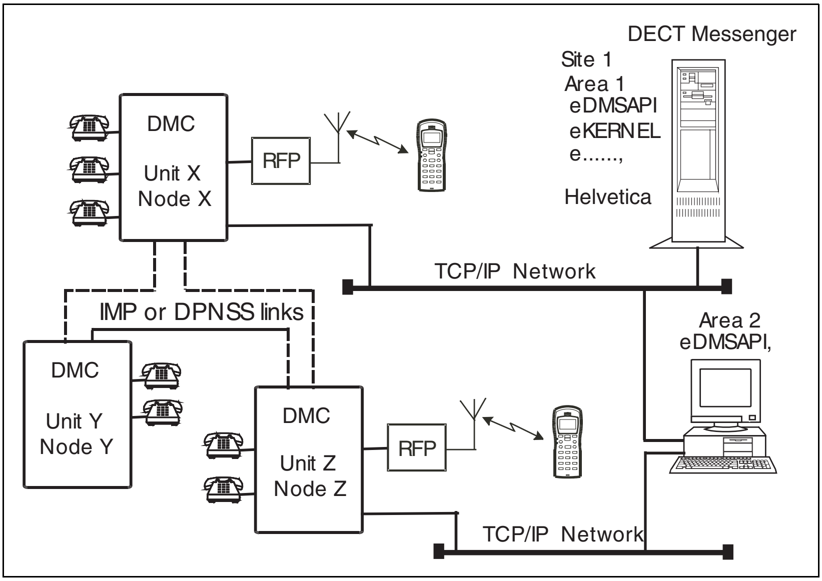


Figure 328 shows a multiunit or multinode network. The DECT Messenger must be able to send messages to DECT handsets in Unit X/Node X and Unit Z/Node Z. On the DECT Messenger computer (Area 1), the eKERNEL is running with other modules and an eDMSAPI to send messages to Unit X/Node X. The second computer (Area 2) provides messaging to Unit Z/Node Z. The 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.

Licencing

Licencing is done using the following:

- DECT Messenger Licence Manager
- DECT Messenger CTI Licences (for each DECT system)

The licences are described in the following:

- "CSTA connection (link) licence" on page 695
- "SOPHO CTI module Licence Manager licences" on page 698

CSTA connection (link) licence

Each application connected to the DMC through CSTA is licenced through one or more application licence and seat licence. For Nortel DECT Messenger, the number of application licences depends on the configuration.

For each DECT Messenger link to a DMC, one application licence 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 licences, you must have seat licences. For DMS, the total number of seat licences 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 the DECT Messenger

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

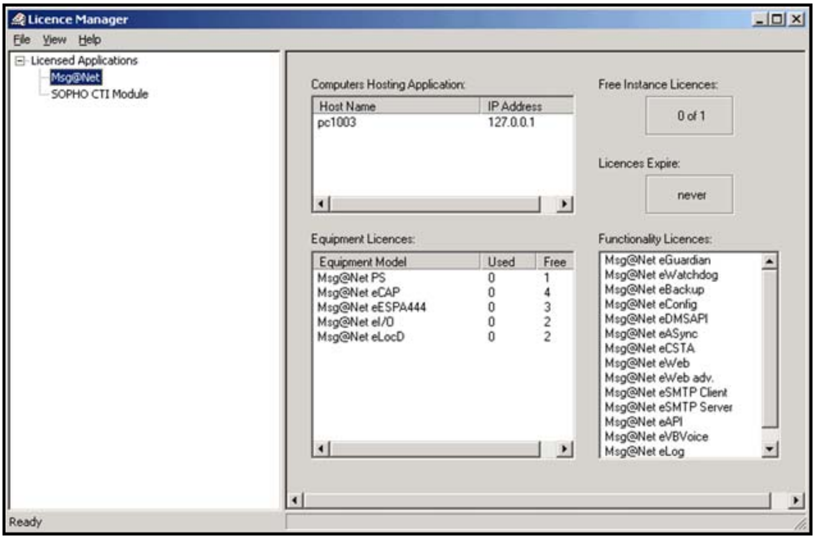
At startup, DECT Messenger immediately reserves the licences needed, although there is no call yet. If the number of seat licences in the DMC is less than the number of seat licences specified in the DECT Messenger, the DECT Messenger cannot reserve the licences and, therefore, cannot make a call.

DECT Messenger Licence Manager licences

The DECT Messenger Licence Manager is the Nortel Licence Manager. This licence manager uses a dongle (using either a parallel connection or USB) and a licence file.

Table 329 shows the Licence Manager.

Figure 329
DECT Messenger Licence 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

> ***Note:*** Figure 329 also shows the CTI application as a licenced application. You require this CTI application licence only if a connection exists to the DECT system.

The following licences are available through the Licence Manager:

- Application module licences

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

The following licences are available:

- Basic Package
- Full Package

Note: The application module licence is shown under the equipment licences in the Licence Manager.

- Equipment licences

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

  Equipment for which you can acquire licences is as follows:

  - DECT Messenger eI/O
  - DECT Messenger eCAP
  - DECT Messenger ESPA444

- Functionality licences

  These licences allow you to implement certain functionality. The functionality licences are submitted to the PC application module licences. If the PC application licences 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

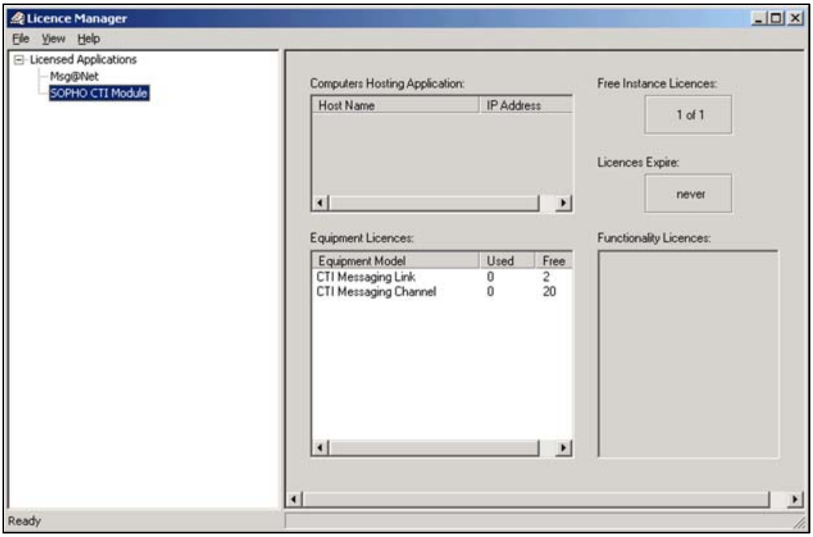
— DECT Messenger eAPI

— DECT Messenger eLog

SOPHO CTI module Licence Manager licences

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

Figure 330
SOPHO CTI Module Licence Manager



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:

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

The number of CTI message channel licences 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 are able to send LRMS messages to the DECT Messenger.

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

Detailed module descriptions

This section provides detailed information for the following modules:

- "eKERNEL" on page 700
- "eDMSAPI" on page 700
- "eIO" on page 700
- "eSMTP" on page 701
- "eSMTP_Server" on page 701
- "eAPI" on page 702
- "eWEB" on page 702
- "eCONFIG" on page 704
- "eGRID" on page 704
- "eTM" on page 704
- "eCAP" on page 705
- "eESPA" on page 705

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. When a confirmation is required, the eKERNEL sends the message repeatedly until a confirmation is received. A maximum of 20 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), or multiple units in a DMC DPNSS network (WAN). (For more information on using the DECT Messenger in a multiunit environment, see "eDMSAPI".)

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 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. When the DECT handsets are located 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.

eIO

The eIO module is an input and output module that requires specific additional hardware from National Instruments. When there is no available COM port in the PC, a multi-IO board is required. The additional hardware uses an RS-232 connection. The eIO module connects external hardware to the Nortel 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 the 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 component that is automatically installed with Windows 2000 Server. In Windows 2000 Professional and Windows 2003 Server, 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 the DECT Messenger

When you send an e-mail message to the 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. When 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. When 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. The eAPI allows you to write your own program to send data to the eKERNEL to generate an alarm. 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” on page 1049. Also included in the chapters are examples of programming code you can use to write your own eAPI program in Visual Basic. There is also a sample program that ships with the software, which is 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, the eAPI allows you to create your own interface for the 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 the 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 be able 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. When sending messages directly to a single device (LRMS [E2] compatible DECT handsets and e-mail addresses), there is no control mechanism 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.)

When 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. When the module is used on the local PC, almost all parameters in the system can be changed, and new items can be added. When 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 the DECT Messenger. eTM is not a scheduler, but serves as a monitor to ensure that the modules in the DECT Messenger are running. If a module stops, the Task Manager restarts the module within two seconds. When the Task Manager is running, Windows cannot be shut down.

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, check see “Module – eCAP” on page 1091, or check the most recent commercial documentation. The eCAP_Generic module allows you 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 Nortel 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.

What is required to run DECT Messenger

Hardware Requirements

The hardware requirements for the 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 for more info.
- V.24 multi port card.

Software Requirements

The DECT Messenger works with the following required and optional software:

- Required software
  - Windows 2000/XP Professional, Windows 2000 Server, or Windows 2003 Server Standard Edition.
  - If you decide to use MS SQL Server as the database engine, you must have Windows 2000 Server or Windows 2003 Server. Windows 2000/XP Professional is not supported for SQL Server. (MSDE is supported under Windows 2000/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. 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

General

On the Nortel DECT Mobility Card (DMC) you must have firmware that supports CTI DASGIF Version 1.2. This version of DASGIF interface supports connection to DECT Messenger.

Examples of versions of DMC firmware that support this interface are:

- DMC-4 Firmware: 45000301.dwl
- DMC-8 Firmware: 47000301.dwl

Connection to the 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 the DECT Messenger to the DMC.

The DECT Messenger uses a CTI port to send and receive LRMS messages, requiring one CTI Messaging Link per 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
- Secure Session
- CSTA_Service (runs in the system tray)
- DECT Messenger eDMSAPI

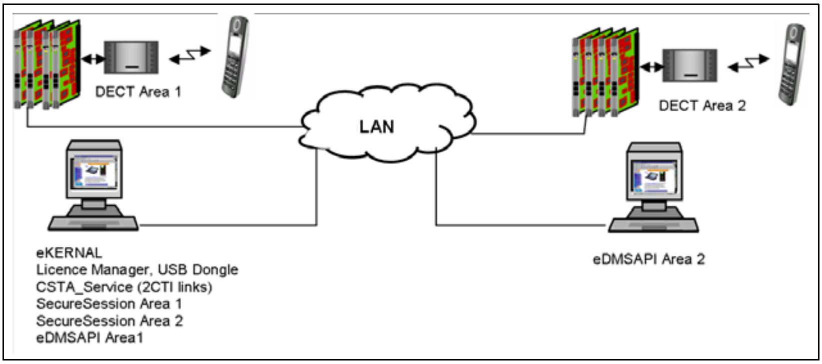
The CSTA_Service provides the CTI link to the DMC.

Connecting to Multiple DECT Systems

To connect to more than one DECT system you must have a CTI link for each DECT system. Check your licence 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 331.

Figure 331
Connecting to two DECT systems



The connection to each DECT system requires its own Secure Session.

Example: Connecting to Two DECT systems.

eKERNEL and eCONFIG are located on PC One, as shown in both Figure 331 and Table 41. 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 41
Example: connecting to two DECT systems

PC 1:	PC 2:
Licence, Dongle, Licence Manager eKERNEL eCONFIG	eDMSAPI module - Area 2

Table 41
Example: connecting to two DECT systems

PC 1:	PC 2:
Secure Session - Area 1	
CSTA_Service (With at least 2 CTI links)	
eDMSAPI module - Area 1	
Secure Session - Area 2	

Databases in DECT Messenger

Supported Database types

The 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.

When 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, there is no user interface, and the maximum number of concurrent users is five. This is not a problem for the DECT Messenger because you do not need database maintenance on the DECT Messenger database. To install the database under MSDE, there is a Batch file 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” on page 949.

— 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 licenced product. Consult the Microsoft WEB Site for more information on the licence structure. The MS SQL Server also requires MS Windows 2000 Server or Windows 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” on page 949.

How to set up the Databases

Setting up the databases is described in “Installing and getting started” on page 711. 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/XP Professional, because for SQL Server you must have Windows 2000 Server or Windows 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.

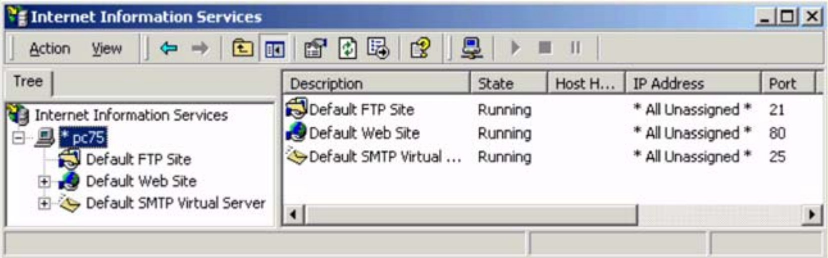
Switch the Default WEB access in IIS **off** to avoid conflicts with the Apache WEB server in the DECT Messenger

Stopping IIS WEB Services

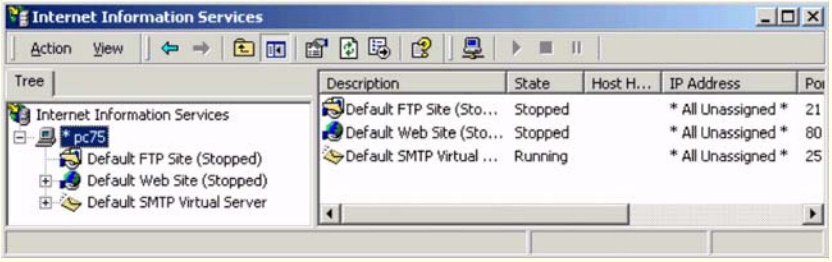
> ***Note:*** This section is only applicable if Internet Information Services (IIS) is installed in your Windows configuration, and the Apache Server is installed for DECT Messenger WEB access.

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 Procedure 201.

Procedure 201
Stopping WEB Services IIS for DECT Messenger (Part 1 of 2)

<table>
<tr><th>Step</th><th>Action</th></tr>
<tr><td></td><td></td></tr>
<tr><td><b>1</b></td><td>Open the Internet Information Services (IIS) window.</td></tr>
<tr><td></td><td>Open IIS by clicking <b>Start</b> on the Windows taskbar, and choosing <b>Settings Control Panel</b> &gt; <b>Administrative Tools</b> &gt; <b>Internet Services Manager</b>.

Internet Information Services
Action
View
Tree
Internet Information Services
* pc75
Default FTP Site
Default Web Site
Default SMTP Virtual Server
<table>
<tr><th>Description</th><th>State</th><th>Host H...</th><th>IP Address</th><th>Port</th></tr>
<tr><td>Default FTP Site</td><td>Running</td><td></td><td>* All Unassigned *</td><td>21</td></tr>
<tr><td>Default Web Site</td><td>Running</td><td></td><td>* All Unassigned *</td><td>80</td></tr>
<tr><td>Default SMTP Virtual ...</td><td>Running</td><td></td><td>* All Unassigned *</td><td>25</td></tr>
</table></td></tr>
<tr><td><b>2</b></td><td>Expand the PC name.</td></tr>
<tr><td></td><td>If the PC name is not expanded, click the <b>+</b> sign next to the name to expand the sub-list to access the FTP, WEB, and SMTP services.</td></tr>
</table>

Procedure 201
Stopping WEB Services IIS for DECT Messenger (Part 2 of 2)

<table>
<tr><th>Step</th><th>Action</th></tr>
<tr><td>3</td><td>Stop the Default Web Site.</td></tr>
<tr><td></td><td>Right-click <b>Default Web Site</b> to access the pop-up menu. Select <b>Stop</b> in this menu.
<b><i>Note:</i></b> 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.</td></tr>
<tr><td>4</td><td>Verify that the service is stopped.</td></tr>
<tr><td></td><td>Ensure that the State column indicates <b>(Stopped)</b> next to <b>Default Web Site</b>.

Internet Information Services
Action View
Tree
Internet Information Services
* pc75
Default FTP Site (Stopped)
Default Web Site (Stopped)
Default SMTP Virtual Server
<table>
<tr><th>Description</th><th>State</th><th>Host H...</th><th>IP Address</th><th>Po</th></tr>
<tr><td>Default FTP Site (Sto...</td><td>Stopped</td><td></td><td>* All Unassigned *</td><td>21</td></tr>
<tr><td>Default Web Site (Sto...</td><td>Stopped</td><td></td><td>* All Unassigned *</td><td>80</td></tr>
<tr><td>Default SMTP Virtual ...</td><td>Running</td><td></td><td>* All Unassigned *</td><td>25</td></tr>
</table>
IIS no longer starts the Web services.</td></tr>
<tr><td colspan="2">END</td></tr>
</table>

Installing DECT Messenger

The software installation process is described in “General – Install PC” on page 805.

Procedure 202
Installation of DECT Messenger Software

Step	Action
1	Verify that the licences and Options are set correctly in the DMC.
2	Verify that the CSTA link to the DMC is installed and operational.
	• Execute a ping command to the IP address of the DMC. • Execute the OM command exping with the IP address of the DECT Messenger PC from the OM terminal.
3	Verify licence availability.
	Ensure that you have a DECT Messenger application licence available, and that you have sufficient Seat licences for the DECT Messenger. ***Note:*** When DECT Messenger starts, the eDMSAPI module reserves the number of licences 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.
	Follow the installation procedure described in “General – Install PC” on page 805.

END

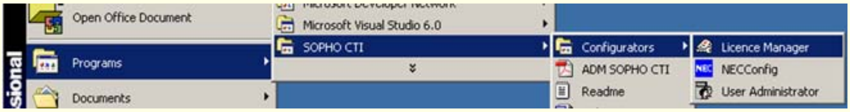
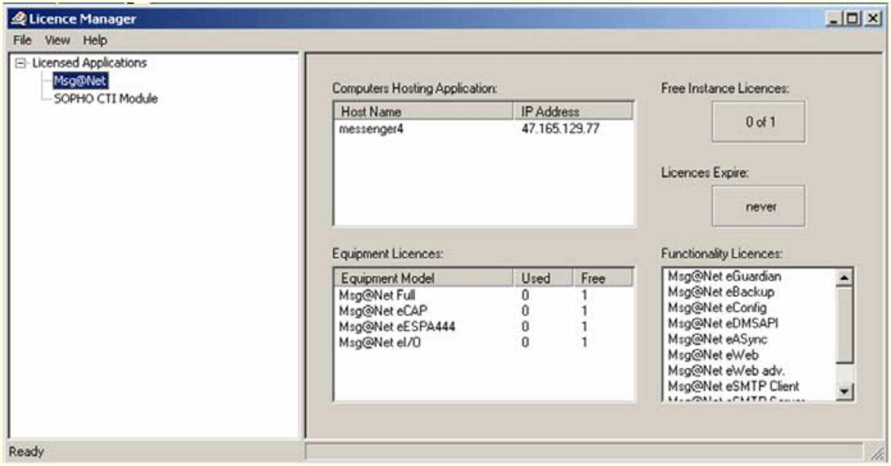
After the installation of the DECT Messenger, carry out the next procedure, “Stopping IIS WEB Services” on page 711.

Getting Started

After installation, you can start up DECT Messenger by restarting the PC. Table 203 on page 715 provides the procedure to start using the system.

Note: To load your licence file you must first acquire the Licence file licxxxx.lic and the DECT Messaging USB Dongle.

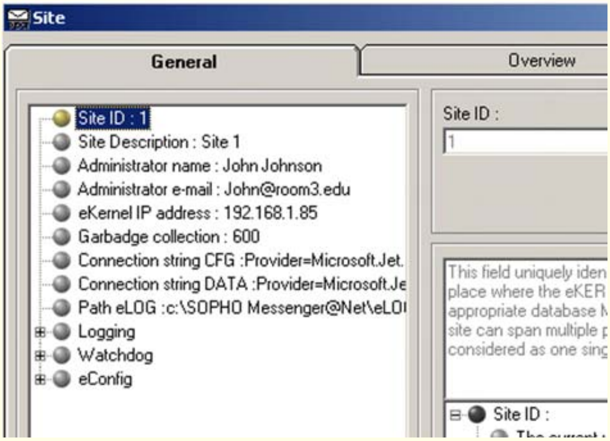
Procedure 203
Getting Started (Part 1 of 10)

Step	Action
1	Install the dongle and start the Licence Manager.
	- Click **Start** on the Windows taskbar and choose **Programs > SOPHO CTI > Configurators > Licence Manager**:  sional Open Office Document Programs Documents Microsoft Developer Network Microsoft Visual Studio 6.0 SOPHO CTI Configurators ADM SOPHO CTI Readme Licence Manager NECConfig User Administrator - The Licence Manager window opens, and a dialog opens requesting a license file.
2	Select the licence file.
	- Browse to the location where your licence file is located, and click **Open**.  Licensed Applications Msg@Net SOPHO CTI Module 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 Ready - Close the Licence Manager.

Procedure 203
Getting Started (Part 2 of 10)

Step	Action
3	Install a preconfigured database, if you have one.
	The 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, than edit the following tables: • eKERNEL_AREA • eKERNEL_SITE • eDMSAPI • eKERNEL_DEVICE • eWEB Use the help information to fill in the tables.

Procedure 203
Getting Started (Part 3 of 10)

Step	Action
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 taskbar, 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 N site can span multiple p considered as one sinc 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**.

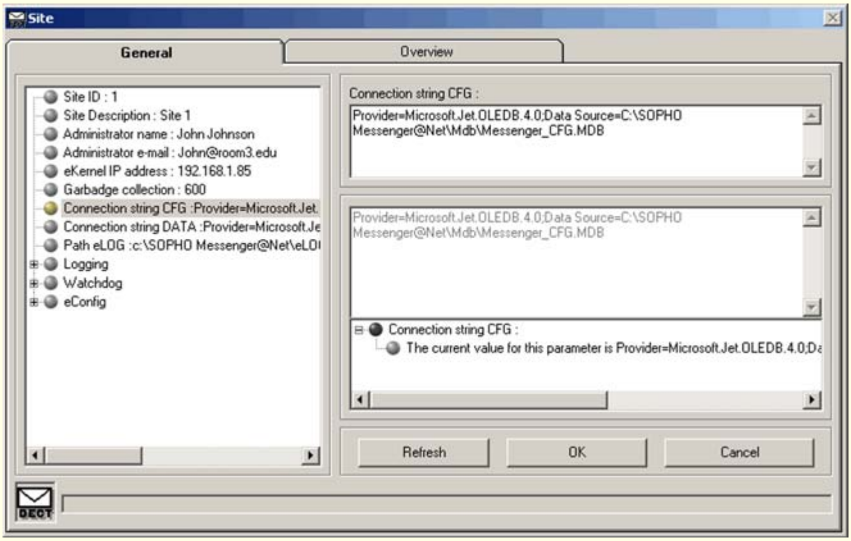
Procedure 203
Getting Started (Part 4 of 10)

Step	Action
7	Check 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.
- Check 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

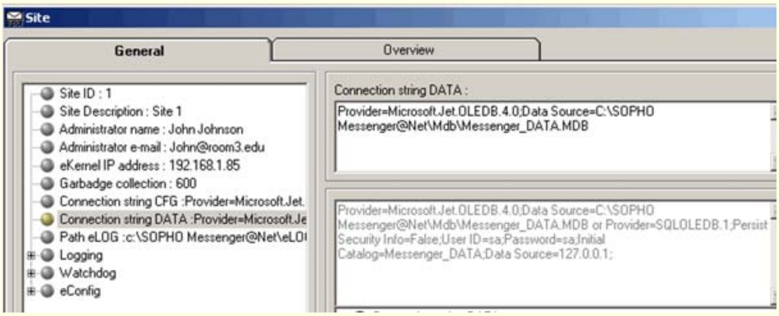
Connection string CFG :
The current value for this parameter is Provider=Microsoft.Jet.OLEDB.4.0;Da

Procedure 203
Getting Started (Part 5 of 10)

Step	Action
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 “Install PC – Step 1f – SQL Server” on page 843.
- 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\eL0
- Logging
- Watchdog
- eConfig

Connection string DATA :

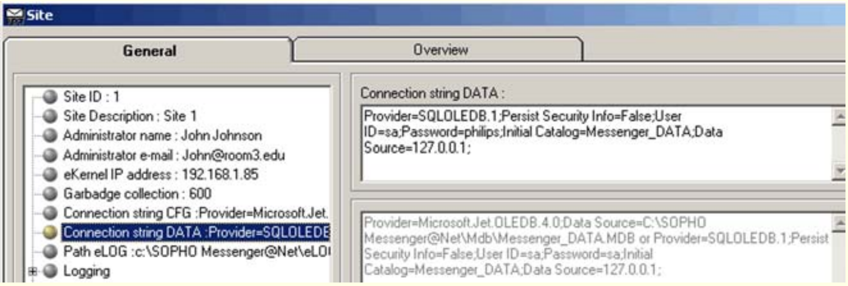
Provider=Microsoft.Jet.OLEDB.4.0;Data Source=C:\SOPHO Messenger@Net\Mdb\Messenger_DATA.MDB

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;

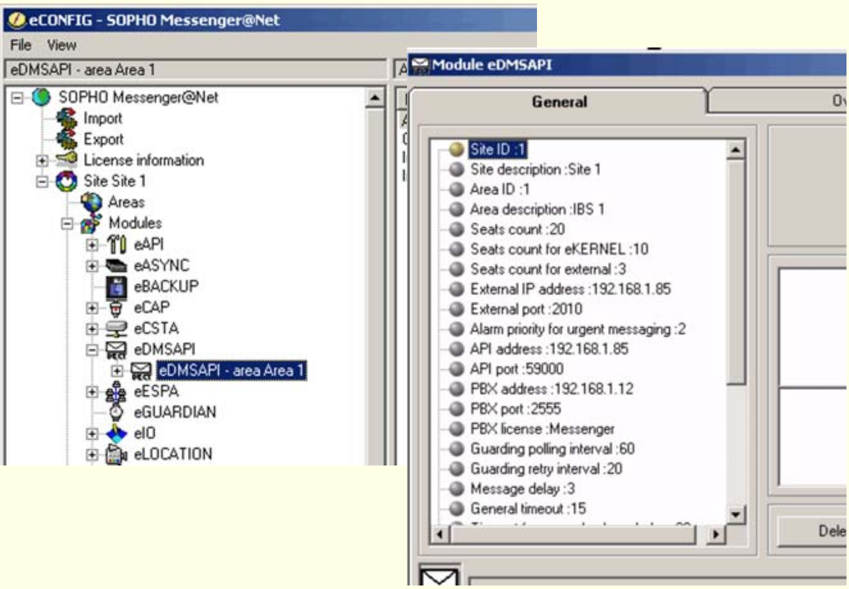
- Set the path for the **MSDE** or **SQL** Server database:
  The path setting for the **MSDE** or **SQL** Server database must point to the ODBC link that you created when you installed the eWEB module.

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

Procedure 203
Getting Started (Part 6 of 10)

Step	Action
	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. When 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.

Procedure 203
Getting Started (Part 7 of 10)

Step	Action
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.  eCONFIG - SOPHO Messenger@Net File View eDMSAPI - area Area 1 SOPHO Messenger@Net Import Export License information Site Site 1 Areas Modules eAPI eASYNC eBACKUP eCAP eCSTA eDMSAPI eDMSAPI - area Area 1 eESPA eGUARDIAN eIO eLOCATION Module eDMSAPI General Dele 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

Procedure 203
Getting Started (Part 8 of 10)

Step	Action
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 - **Nortel** PBX Licence - Always **Messenger** ***Note:*** Only specify the number of seats you anticipate requiring, (not the total number of seats allowed by your licence), as it will take longer for seats to register. Ensure that you do not exceed the number of seats (CTI Messaging Channels) as specified in your licence Manager. If the number of seats is not sufficient in the Licence, you cannot make an LRMS (E2) message call.
12	Add a DECT Device.
	Refer to “Adding a DECT device to the Messenger system” on page 673.

Procedure 203
Getting Started (Part 9 of 10)

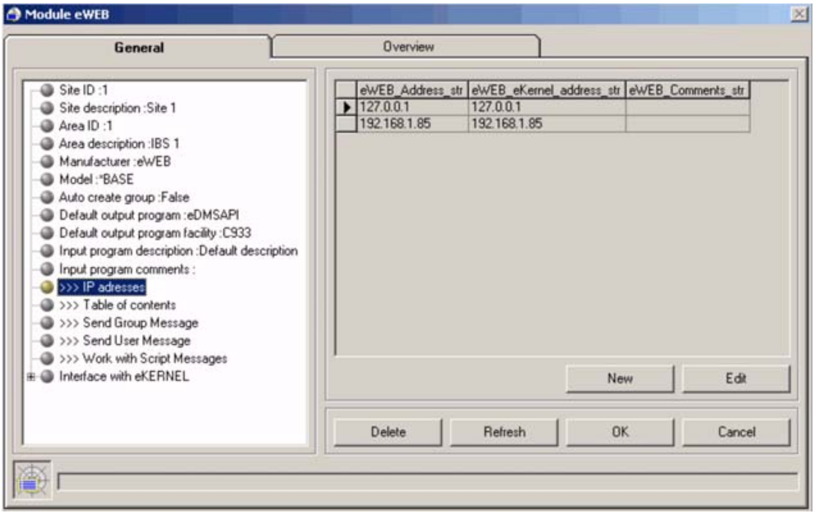
Step	Action
13	Configure eWEB module.
	• Expand the item **Modules > eWEB Module**. One instance of the eWEB module: eWEB - area <x> is shown. • Double-click the eWEB instance to open the parameters/properties. Click **IP addresses**, as shown in Figure 332 on page 725. The first line in the right pane 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 contained 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.

Procedure 203
Getting Started (Part 10 of 10)

Step	Action
14	Verify the operation of the DECT Messenger.
	• Start up the eKERNEL from the shortcut in the Windows **Start** menu. • Open the Secure Session application. • Start up the CSTA_Service. This appears in the system tray. • Start up 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.

END

Figure 332
eWEB Properties



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	

Using eCONFIG

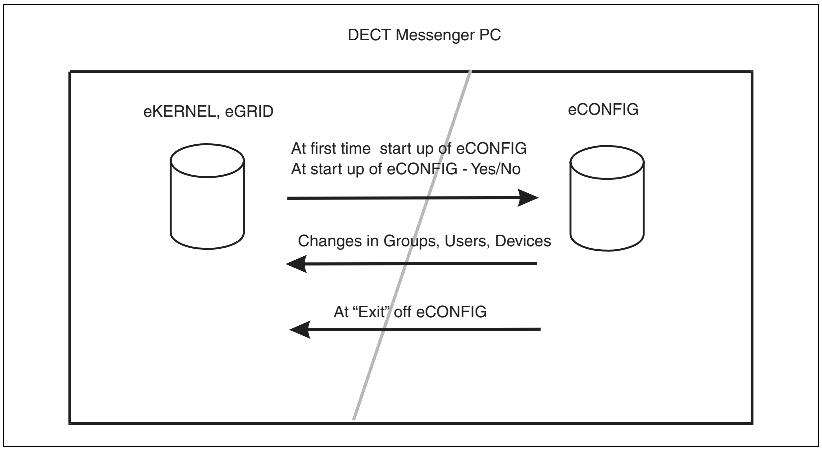
The eCONFIG Module is the tool most commonly used for making changes in the configuration. The configuration is stored in a Database. Be cautious when editing the database, because incorrect or invalid entries can interfere with the operation of DECT Messenger.

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

When the eCONFIG is installed on the DECT Messenger server PC the database is handled as shown in Figure 333 on page 726.

Figure 333
Database handling with eCONFIG on DECT Messenger Server PC (Local)


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

When you start the eCONFIG for the first time, a copy is made of the configuration database of the 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. When 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:

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 1: When 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 2: When 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).

When 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.

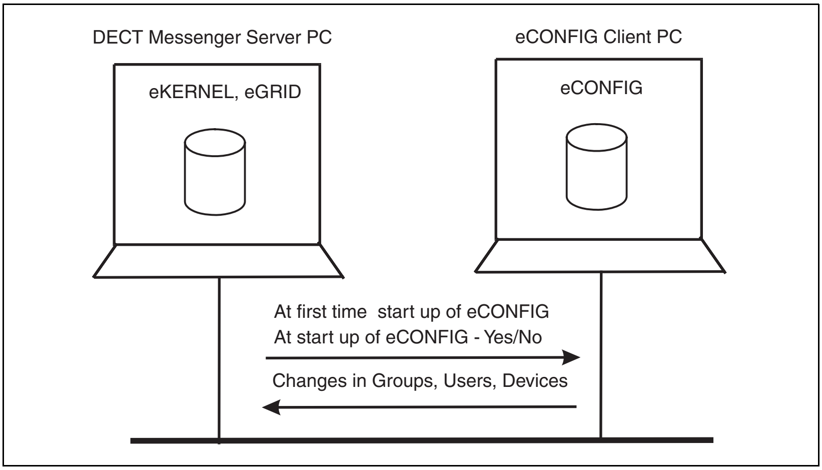
- **Starting up the eCONFIG again**

  When 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. Nortel recommends that you make a fresh copy of the operational database, because then you are sure that there is no database inconsistency.

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

When the eCONFIG is installed on the DECT Messenger server PC the database is handled as shown in Figure 334 on page 728.

Figure 334
eCONFIG database handling when used on a remote PC (client PC)


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

When you start up the eCONFIG for the first time on the remote PC, a copy is made of the configuration database of the 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

When 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 there is more than one eCONFIG active at the same time on different PCs, the individual eCONFIG databases are not updated or synchronized when 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**

  When 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. Nortel recommends that you make a fresh copy of the operational database, because then you are sure that there is no database inconsistency.

Using eTM

The eTM is the Task Manager in the DECT Messenger. The eTM opens in the Windows system tray, and monitors the modules of the 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 up, 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 when 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 1:*** On these PCs you must also have eTM running if you want to use the Task Manager.
>
> ***Note 2:*** 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, just 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 the DECT Messenger. The message is delivered to the 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 the DECT Messenger, this message is not sent to the intended destination directly; DECT Messenger decides what to do with the message. The 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 the DECT Messenger, with a Group-to-Group Member-to-Device structure.

Figure 335
Incoming message (IA) in eDMSAPI

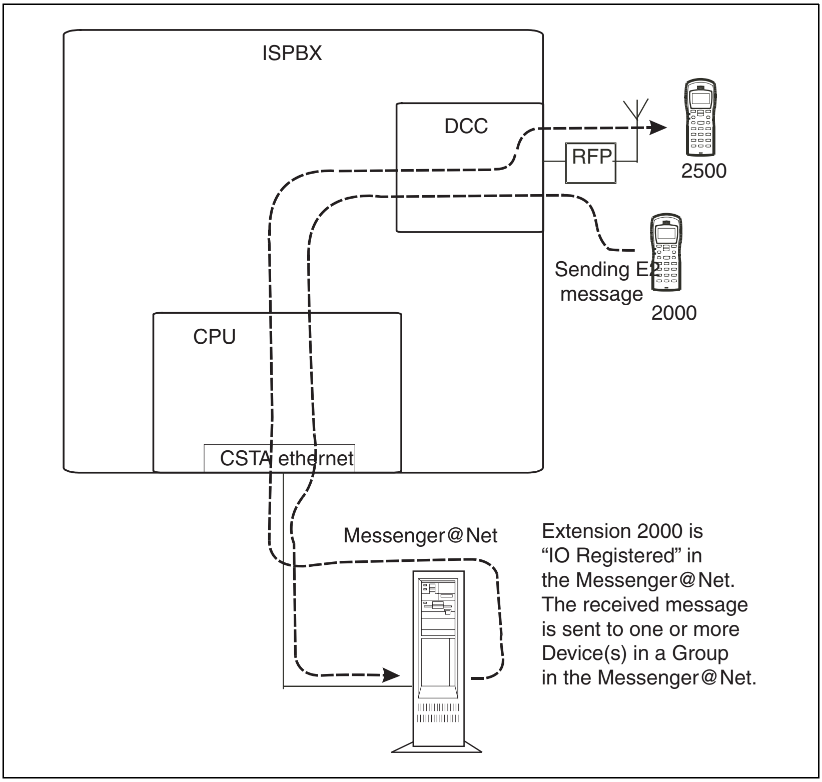


Figure 335 illustrates the handling of an incoming message (IA) in the eDMSAPI module, as follows:

- 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 the DECT Messenger.
- The DECT Messenger checks the intended destination of the message. If that destination is in the Inbound configuration in the eDMSAPI module, then 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 the 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 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 the 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.

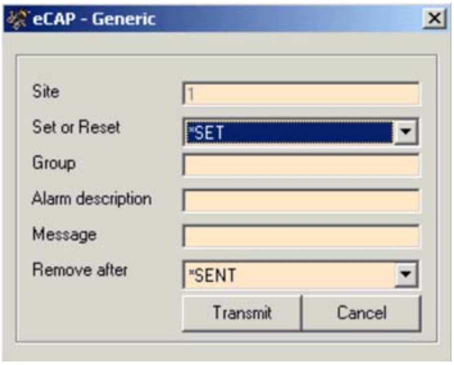
The extension number to which the message is sent for IC can be a hardware-less DN in the DMC.

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

Parameters required to set an alarm

The structure of the 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 shows that these parameters are required. Figure 336 shows the Sending Message option of the eCAP generic, and shows the parameters.

Figure 336
eCAP Sending Message option



eCAP - Generic

Site: 1
Set or Reset: *SET
Group:
Alarm description:
Message:
Remove after: *SENT

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 739.

- 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 have been defined in the 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

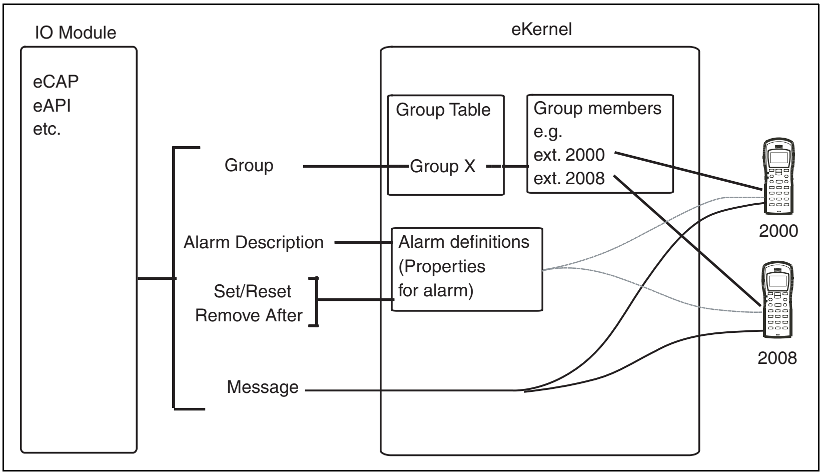
  This is the actual message that is transferred to the device.

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

  This is described in “SET/RESET structure” on page 739.

Alarm handling is shown in Figure 337, which illustrates an input program that provides the input parameters.

Figure 337
Alarm handling



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

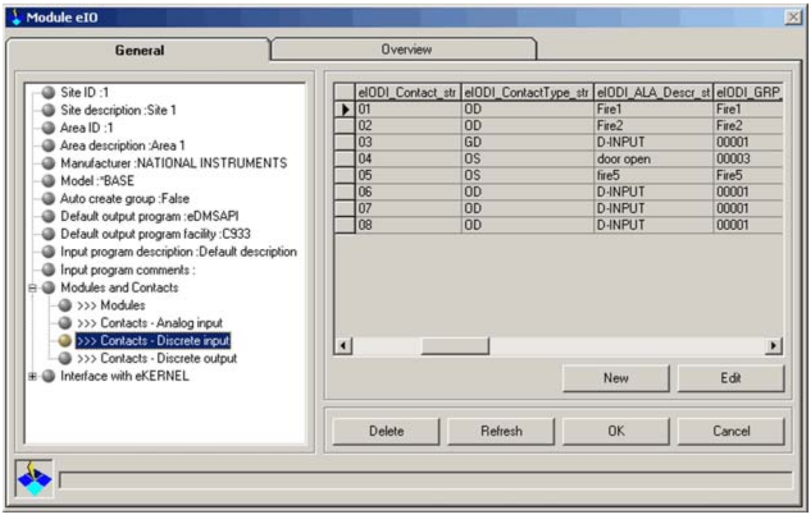
Detailed explanation of the five parameters

- Group

  The input program provides a Group name to which the alarm must be sent. This Group name must have been 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 when you use the eCONFIG module for configuration.

  Figure 338 shows an example of the relation between the input program and the output devices, and uses the eIO Module as input module.

Figure 338
Input/output relationships



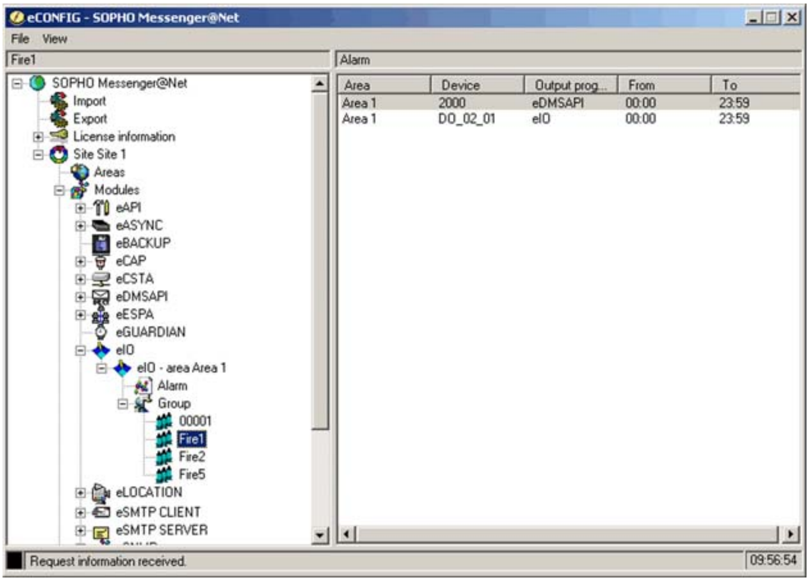
- Site ID :1
- Site description :Site 1
- Area ID :1
- Area description :Area 1
- Manufacturer :NATIONAL INSTRUMENTS
- Model :*BASE
- Auto create group :False
- Default output program :eDMSAPI
- Default output program facility :C933
- Input program description :Default description
- Input program comments :
- 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 338 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. (Note that only eIODI_Group_ is shown in Figure 338.)

Under the eIO Module in the eCONFIG, two submenus are displayed: 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 339.

Figure 339
Groups in an input module



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.

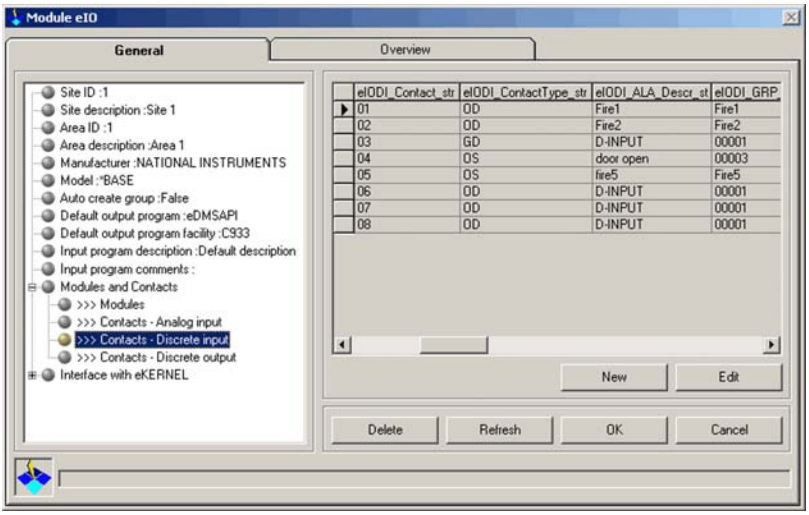
A Group name must match a Group name that comes from the input module. In this example, the Group name (Fire1) must match the Group name that is assigned to the input contact (01) in Figure 339. Under the Group name Fire1, two Members are listed, which are actual output Devices (Device 2000 and Device 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 there is a group 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).

Figure 340
Input "contact 01"

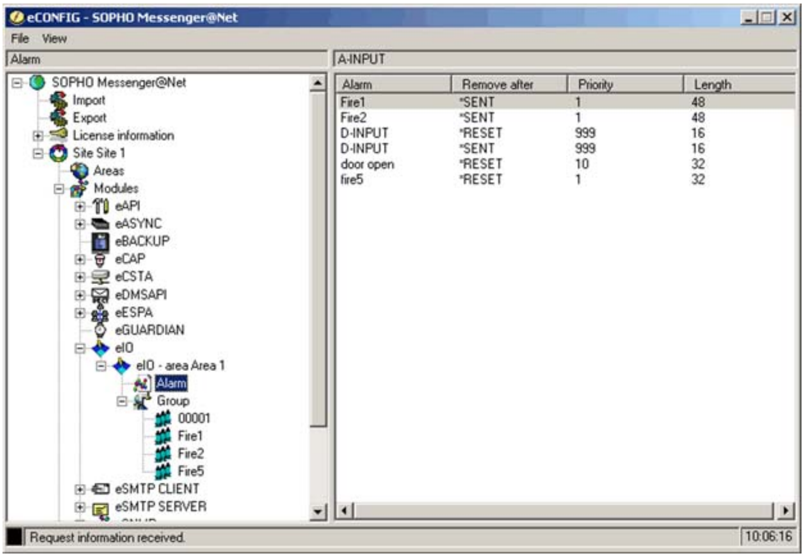


Site ID :1
Site description :Site 1
Area ID :1
Area description :Area 1
Manufacturer :NATIONAL INSTRUMENTS
Model :*BASE
Auto create group :False
Default output program :eDMSAPI
Default output program facility :C933
Input program description :Default description
Input program comments :
Modules and Contacts
>>> 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 340 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).

Figure 341
Alarm identifier



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.

The Alarm Identifier, illustrated in Figure 341, 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 de-activated. See “SET/RESET structure” on page 739.

- **Remove After**

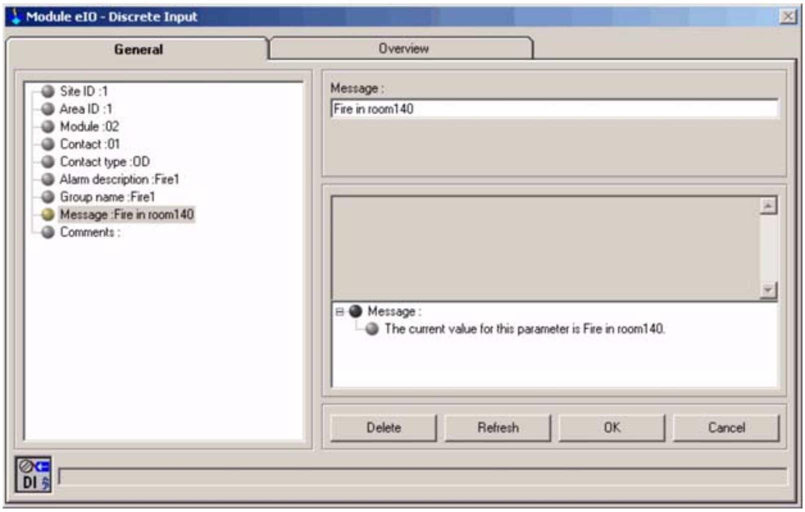
  Remove After specifies what is to be done with the alarm after the eKERNEL has received the alarm. Valid settings are as follows: Remove after sent, Remove after Reset or Remove after Calculate. This is discussed in “SET/RESET structure” on page 739.

- **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, when 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 342 shows the message assigned to a button.

Figure 342
Message assigned to a button



Site ID :1
Area ID :1
Module :02
Contact :01
Contact type :OD
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.

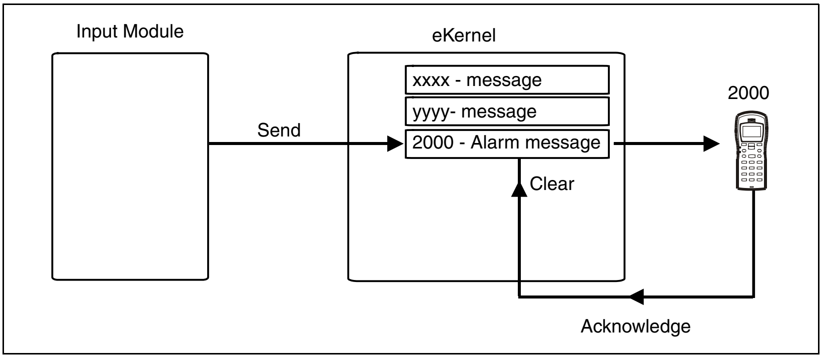
SET/RESET structure

The SET/RESET structure of alarms is complex; you can Set an Alarm and wait for a Reset, or you can just 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 343 shows the structure.

Figure 343
Sent Alarm structure

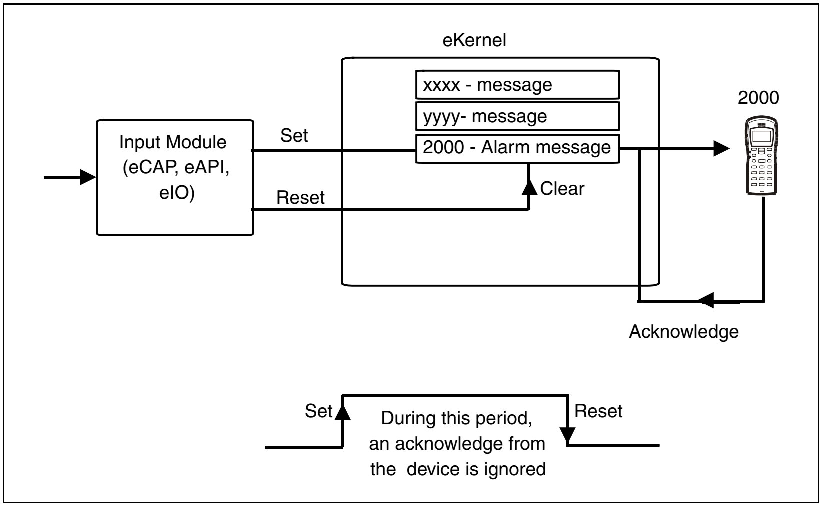


In this figure, there is an input module that generates an alarm as a sent. Therefore, the alarm is sent to the eKERNEL, and stored in an alarm database (data table). Immediately after sending, the input module withdraws the alarm, so the alarm condition is only present in the database table, with a 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 per device type. If the device is an LRMS (E2) DECT handset, and the alarm was sent as a normal message, then 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 346 on page 743.

- SET/RESET

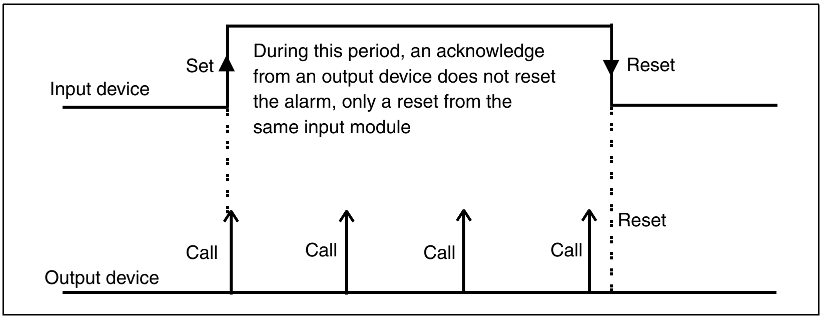
  An alarm can also be generated, based on a set command. This command must always be followed by a reset from the same input module, when the alarm condition is no longer active. Figure 344 on page 741 illustrates the SET/REST alarm structure.

Figure 344
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.

Figure 345
Alarm processing

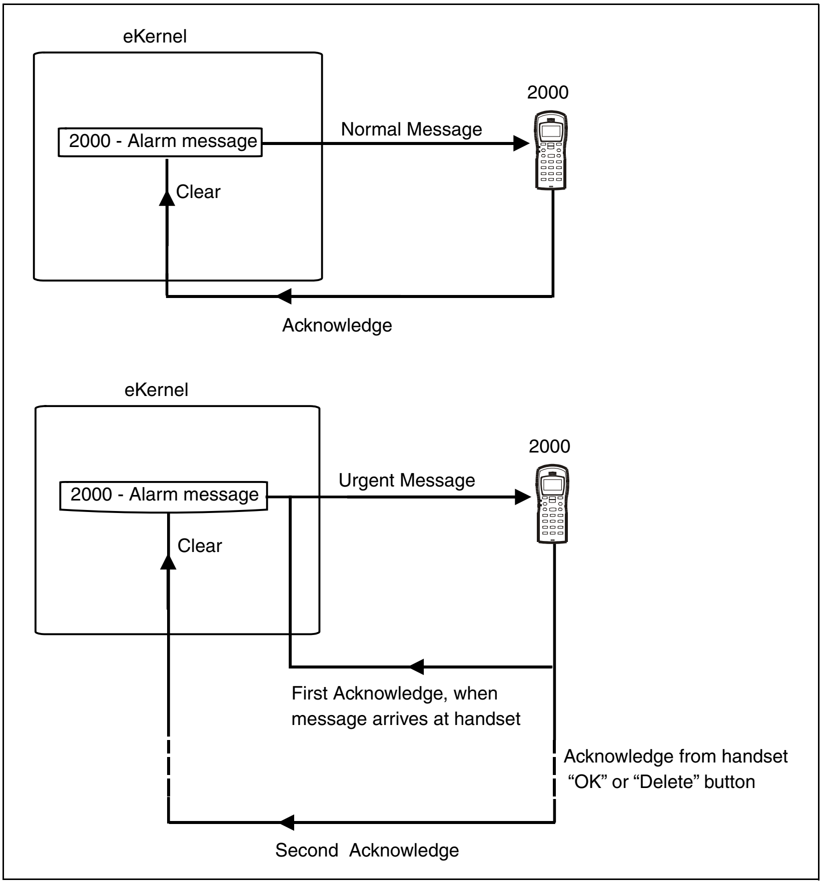

Input device
Set
During this period, an acknowledge
from an output device does not reset
the alarm, only a reset from the
same input module
Reset
Output device
Call
Call
Call
Call
Reset

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 345 on page 741.

- **ACK / NAK**

  A message can be sent to an LRMS (E2) DECT handset as a Normal message, or as an Urgent message. When 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 when the second Acknowledge arrives. When the user presses the **Delete** or **OK** key on the handset, the message call is acknowledged.

Figure 346
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 when 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.
- The I/O allows you to set an alarm using a push button. This is issued when 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 when 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 the 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 the **OK** or **Delete** button 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.
- When you receive an alarm through eAPI, the options shown in Table 42 apply to alarm handling:

Table 42
Options for alarm handling

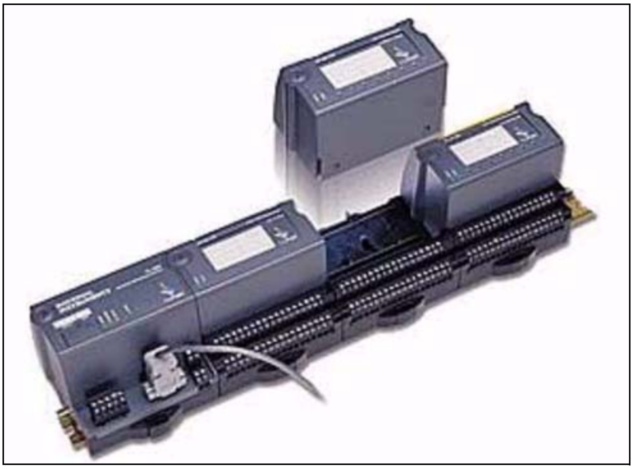
Field: set or reset	Field: Remove after	DECT Messenger action
*set	*sent	Alarm processed as sent alarm.
*set	*reset	Alarm set and waits for a reset.
*set	*calc	System sets the alarm. The system searches in the eKERNEL_ALARM table for a Remove_after SENT for that Input Module with the same Alarm Description. 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.

Connecting National Instruments modules

General

The Digital Input, Digital Output, and Analogue Input options are achieved using FieldPoint modules of National Instruments. Figure 347 shows the National Instruments IO modules on a rail.

Figure 347
Rail with National Instruments FieldPoint IO Modules



The various types of IO modules that are supported for the DECT Messenger can be classified as control modules or I/O Modules. Table 43 and Table 44 give an overview of these modules.

Table 43
Overview of supported control modules

Module Type	Description	Additional info
FP-1000	Control Module with V.24 interface to the DECT Messenger	This module is as interface module between the I/O modules and the 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 44
Overview of supported I/O modules (Part 1 of 2)

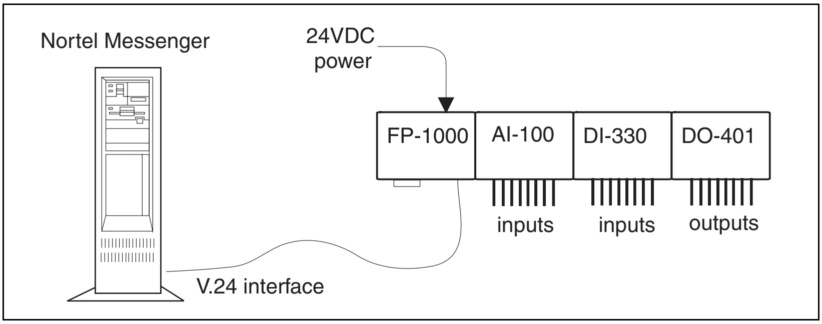
Module Type	Description	Additional info
AI-100	Analogue input Module	8 Analogue inputs, each can be set to one of the following ranges: 30V, 15V, 5V, 1V, 0-30V, 0-15V, 0-5V, 0-1V, 20mA, 0-20mA, 4-20mA.
DI-300	Digital Input	8 discrete input channels. These inputs are sinking inputs for 24VDC.
DI-301	Digital 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.

Table 44
Overview of supported I/O modules (Part 2 of 2)

Module Type	Description	Additional info
DO-400	Digital output	8 discrete output channels. Max. 2A per output, max 8A per module. Maximum voltage 30VDC.
DO-401	Digital output	16 discrete output channels. Max. 2A per output, max 8A per module. Maximum voltage 30VDC.
For each I/O module, one Terminal Base is required - TB-1		

Figure 348 on page 748 shows how one rail with National Instruments I/O modules is connected to the DECT Messenger. On this rail there can be various types of I/O Modules. The maximum number of modules per rail is eight. The modules shown in Figure 348 are examples only.

Figure 348
National Instruments rail connected to DECT Messenger

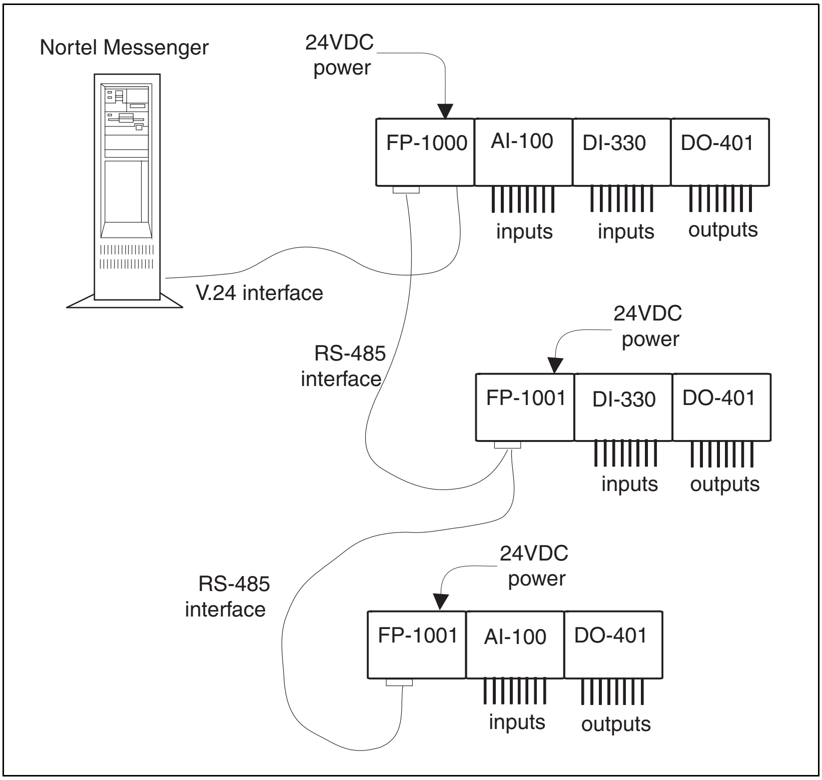


> ***Note:*** The maximum number of contacts per eIO Module in the DECT Messenger is 128.

Figure 349 on page 749 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 349
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 the 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.

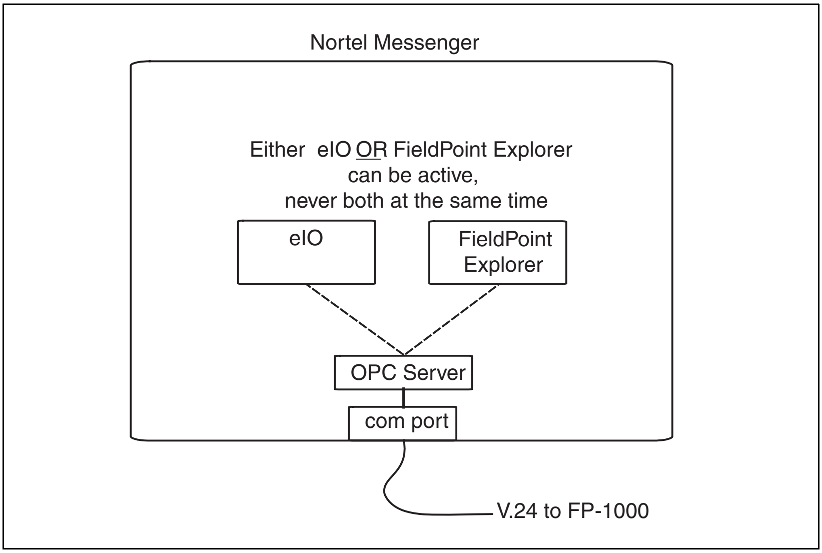
The software for the I/O modules is based on the industry standard OPC (OLE for Process Control) Server software. When you have installed the software for the National Instruments modules, according to the installation procedure in “Install PC – Step 3 – National Instruments” on page 889, this OPC software 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 350 on page 751 shows how these modules are related.

Figure 350
Software Parts for the I/O modules


Nortel Messenger
Either eIO OR FieldPoint Explorer can be active, never both at the same time
eIO
FieldPoint Explorer
OPC Server
com port
V.24 to FP-1000

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

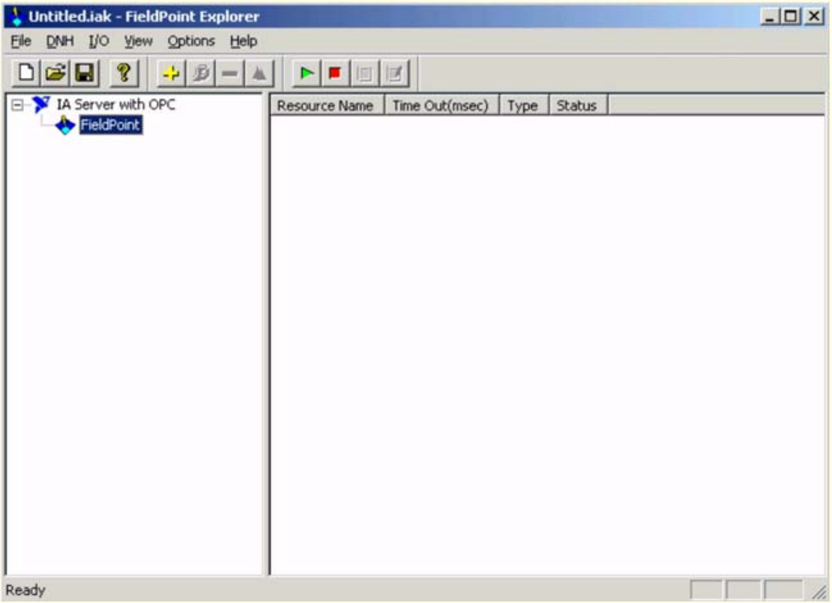
> ***Note:*** Do not forget to close down the FieldPoint Explorer before you start up the eIO module. Conversely, do not forget to close down the eIO Module before starting up the FieldPoint Explorer.

Table 204 on page 752 describes the steps needed to use the FieldPoint Explorer software:

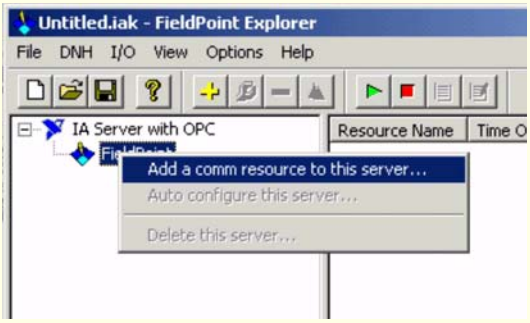
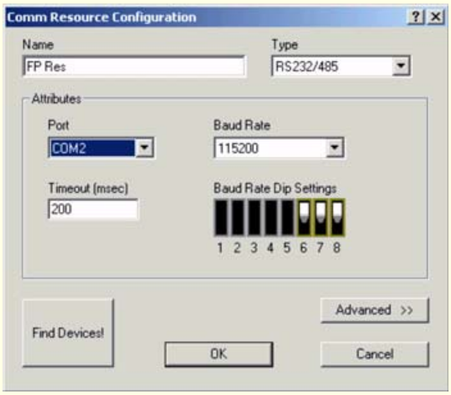
Procedure 204
Using the National Instruments FieldPoint Explorer software (Part 1 of 6)

Step	Action
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.

Procedure 204
Using the National Instruments FieldPoint Explorer software (Part 2 of 6)

Step	Action
2	Open the FieldPoint Explorer.
	Click **Start** on the Windows taskbar, and choose **Programs > National Instruments FieldPoint 2.0 > FieldPoint Explorer**.  Untitled.iak - FieldPoint Explorer File DNH I/O View Options Help IA Server with OPC FieldPoint Resource Name Time Out(msec) Type Status Ready

Procedure 204
Using the National Instruments FieldPoint Explorer software (Part 3 of 6)

Step	Action
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:  Comm Resource Configuration Name: FP Res Type: RS232/485 Attributes Port: COM2 Baud Rate: 115200 Timeout (msec): 200 Baud Rate Dip Settings 1 2 3 4 5 6 7 8 Find Devices! Advanced >> OK Cancel

Procedure 204
Using the National Instruments FieldPoint Explorer software (Part 4 of 6)

Step	Action
4	Configure the comm resource

In the Comm Resources Configuration window, set the following:

- **Name**

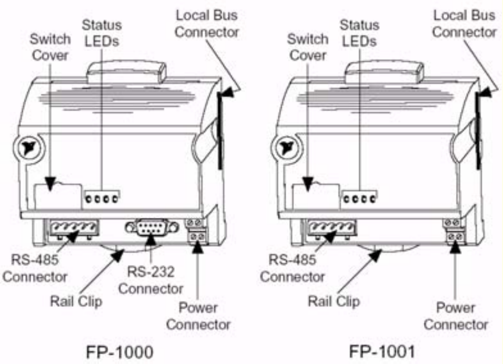
Accept the default name (FP Res).

- **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 located under a small cover on the top of the FP-1000 module.

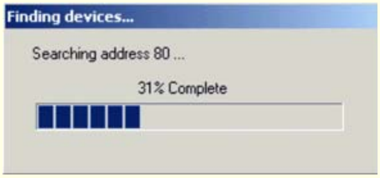
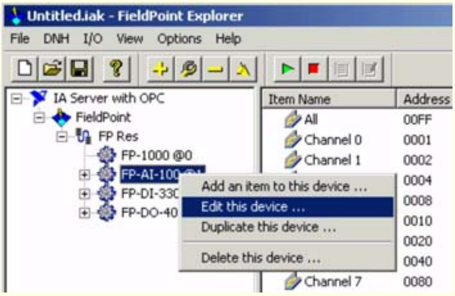


- **Time-out** (msec.)

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.

Procedure 204
Using the National Instruments FieldPoint Explorer software (Part 5 of 6)

Step	Action
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...**  Untitled.iak - FieldPoint Explorer File DNH I/O View Options Help IA Server with OPC FieldPoint FP Res FP-1000 @0 FP-AI-100 @1 FP-DI-330 FP-DO-40 Add an item to this device ... Edit this device ... Duplicate this device ... Delete this device ... Item Name Address All 00FF Channel 0 0001 Channel 1 0002 0004 0008 0010 0020 0040 Channel 7 0080

Procedure 204
Using the National Instruments FieldPoint Explorer software (Part 6 of 6)

Step	Action
8	Set channel configuration values.
	Click the button: **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, then the eIO Module does not receive information from the FieldPoint modules. ***Note:*** Setting up the eIO Modules is described in “Module – eIO” on page 1149.

END

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:

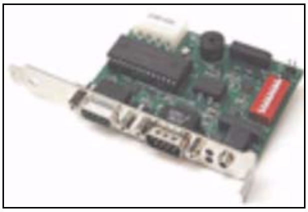
- The input program you expect input from at regular intervals
- The time of day when you expect input
- The days in the week when you expect input
- The Alarm Group and Alarm Description the alarm must be sent with (if there is a time out)
- The Expected time interval between inputs
- The Message to 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 the DECT Messenger the Internal Serial PC Watchdog from Berkshire Products is supported. Figure 351 on page 759 shows this card.

Figure 351
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, 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. When 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 initialisation sequence.

The standard Watchdog package contains the following items:

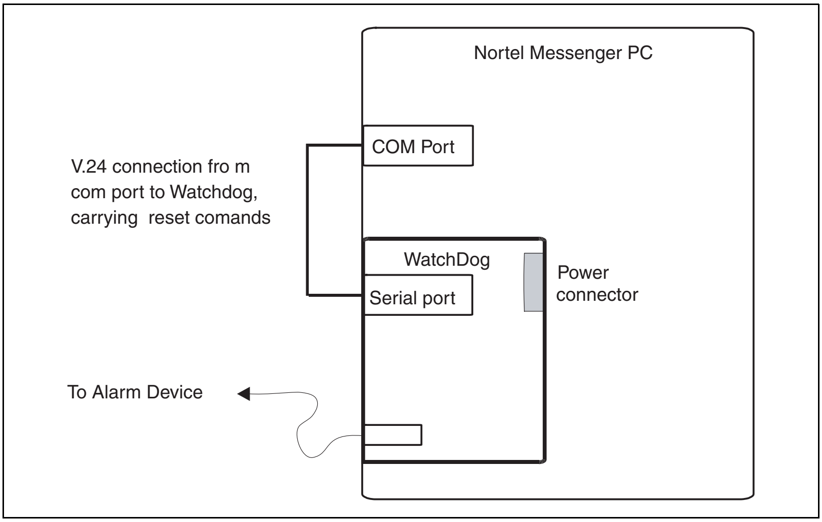
- The Berkshire Watchdog manual on diskette as a PDF file
- The Watchdog timer on a standard PC I/O bracket
- A disk drive Y style power cable to power the board
- A DB-9 to DB-9 serial cable
- A 3.5" program diskette
- A reset cable

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 352 on page 760 shows how the Watchdog is used in the 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 when an application sends the correct commands to the card using V.24 (RS232). The DECT Messenger cannot send such commands to the Watchdog.

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

Figure 352
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.

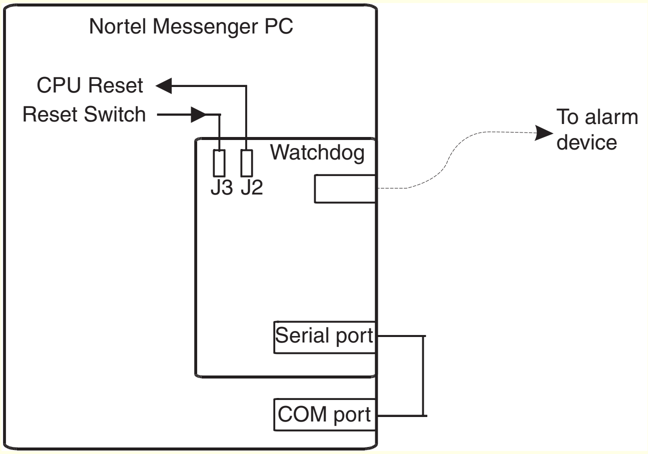
Watchdog Installation

The following procedure describes how to install the Watchdog.

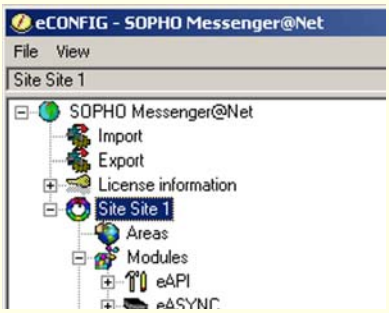
Procedure 205
Installing and connecting the Watchdog (Part 1 of 5)

<table>
<tr><th>Step</th><th>Action</th></tr>
<tr><td></td><td></td></tr>
<tr><td><b>1</b></td><td>Set DIP switches.</td></tr>
<tr><td></td><td>To enable command mode and set the timer (in this example, to 30 seconds), make the following dipswitch settings on the Watchdog card:
<table>
<tr><th>SW1</th><th>SW2</th><th>SW3</th><th>SW4</th><th>SW5</th><th>SW6</th><th>SW7</th><th>SW8</th></tr>
<tr><td>OFF</td><td>ON</td><td>OFF</td><td>OFF</td><td>OFF</td><td>OFF</td><td>ON</td><td>OFF</td></tr>
</table>
<b><i>Note:</i></b> 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.</td></tr>
</table>

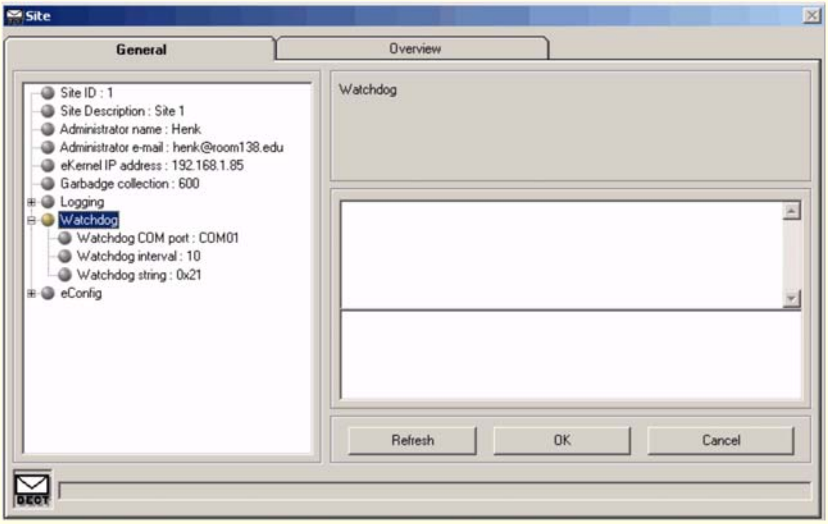
Procedure 205
Installing and connecting the Watchdog (Part 2 of 5)

Step	Action
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:  Nortel Messenger PC CPU Reset Reset Switch Watchdog J3 J2 To alarm device Serial port COM port
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.

Procedure 205
Installing and connecting the Watchdog (Part 3 of 5)

Step	Action
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 up the PC, and start the eCONFIG. In eCONFIG double-click the **Site** menu:  eCONFIG - SOPHO Messenger@Net File View Site Site 1 SOPHO Messenger@Net Import Export License information Site Site 1 Areas Modules eAPI eASYNC

Procedure 205
Installing and connecting the Watchdog (Part 4 of 5)

Step	Action
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 Site General Overview Watchdog Refresh OK Cancel DECT ***Note 1:*** 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 2:*** When selecting the COM port, keep in mind that other Modules use COM ports as well, such as eCAP, eESPA, eIO.

Procedure 205
Installing and connecting the Watchdog (Part 5 of 5)

Step	Action
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. When 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”, for additional information about the Watchdog card.

END

Watchdog settings and indicators

- LEDs

Table 45
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.
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 46
Bottom LED Indications

Bottom LED Indication	Meaning
Steady on.	Alarm condition. The timer in the Watchdog has been 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 Table 205 on page 761. If you want to use another delay time, change the delay time using switches 6,7, and 8. See Table 47 for the settings.

  Note: Also adapt the eKERNEL_SITE table in the DECT Messenger.

Table 47
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 the DECT Messenger.

Automatic Watchdog Start-up

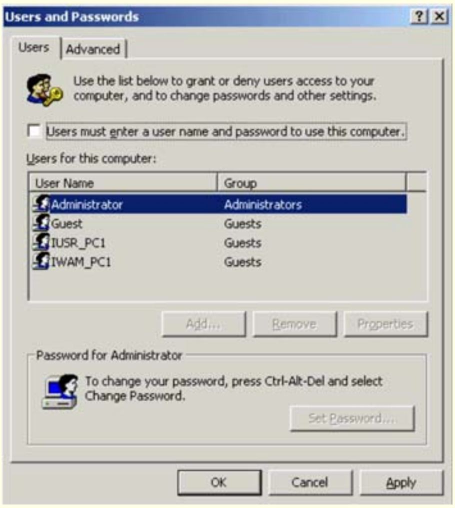
The Watchdog is connected to the reset button of the PC. Watchdog automatically restarts the PC if Watchdog detects that the software is no longer running.

> ***Note:*** Automatic start-up 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.

Procedure 206
Automatic start-up with login in Windows 2000 Professional (Part 1 of 2)

Step	Action
1	Open the Users and Passwords window.
	Click **Start** on the Windows taskbar, and choose **Settings > Control Panel > Users and Passwords**.

Procedure 206
Automatic start-up with login in Windows 2000 Professional (Part 2 of 2)

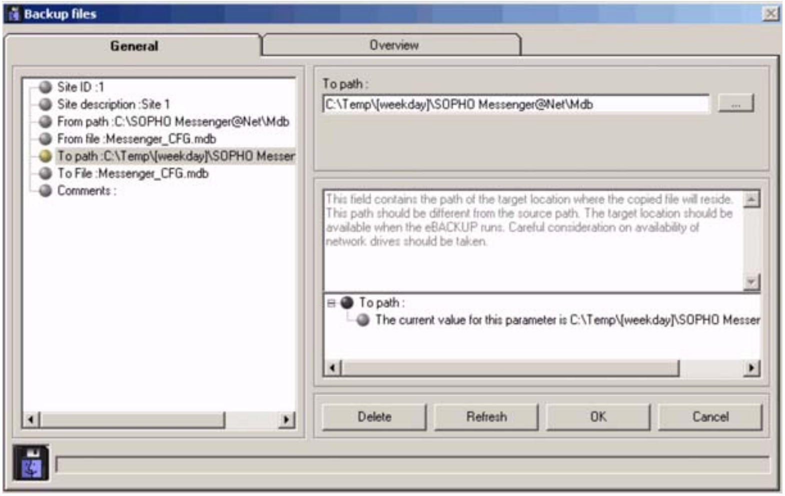
Step	Action
2	Disable login.
	- Uncheck the box **Users must enter a user name and password to use this computer** as shown in the illustration. - Click **Apply**, and, and then **OK**.  Users and Passwords Use the list below to grant or deny users access to your computer, and to change passwords and 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. Users Advanced Add... Remove Properties Set Password... OK Cancel Apply

END

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.

Figure 353
The Backup window



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

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

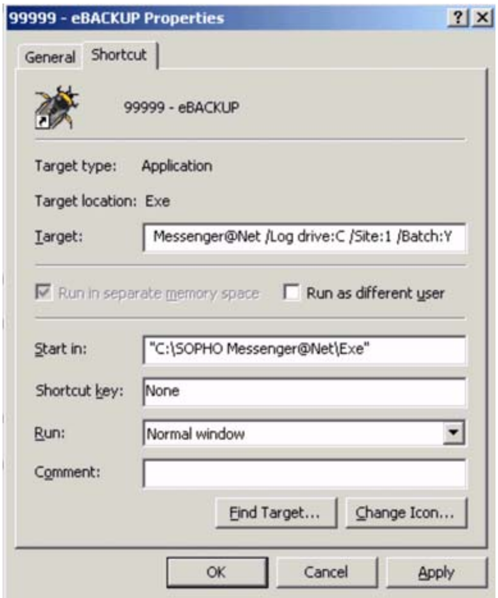
  When you double-click the eBACKUP program shortcut, the program does one of the following:

  — 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 354 on page 770. If there is specified Batch:N, eBACKUP opens the Site selection window. If there is specified Batch:Y, eBACKUP generates a backup immediately.

Figure 354
Shortcut definition to 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:

Note: Figure 354 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

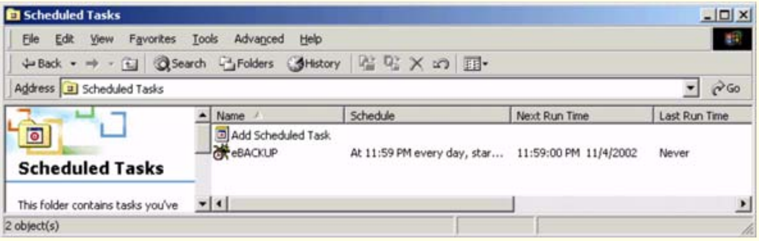
  When you want automatically created backups of files, you must use the Scheduler in Windows to start the Backup module. When activated from the Scheduler, eBACKUP makes a copy of the files that you have specified in the eBACKUP configuration tables, in the directories that you have specified.

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.

Procedure 207
How to set up a Scheduled task for eBACKUP (Part 1 of 3)

Step	Action
1	Open the Scheduled Tasks wizard.
	Click **Start** on the Windows taskbar, 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 username 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**.

Procedure 207
How to set up a Scheduled task for eBACKUP (Part 2 of 3)

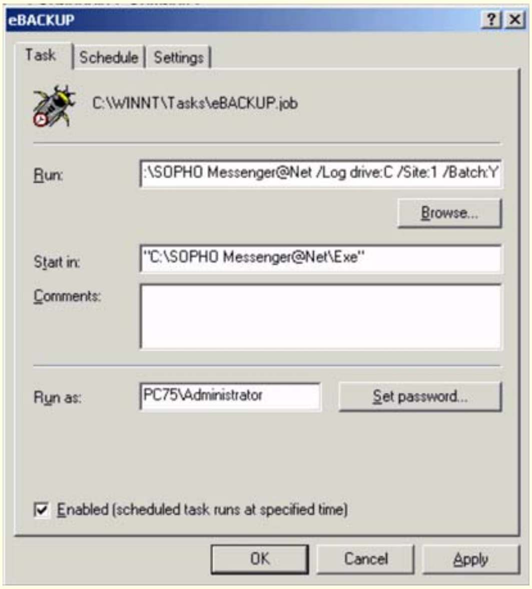
Step	Action
6	Open the eBACKUP Properties.
	Right-click the **eBACKUP** line in the window. In the pop-up menu, select **Properties**. 

Scheduled Tasks
File Edit View Favorites Tools Advanced Help
Back
Search
Folders
History
Address
Go
Scheduled Tasks
This folder contains tasks you've
2 object(s)

Address: Scheduled Tasks

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

Procedure 207
How to set up a Scheduled task for eBACKUP (Part 3 of 3)

Step	Action
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.  eBACKUP 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) Task Schedule Settings Browse... Set password... OK Cancel Apply
8	Select the file to back up.
	In the eCONFIG, module eBACKUP, select which file you want to back up.
	END

Setting up e-mail integration (eSMTP-Server/eSMTP)

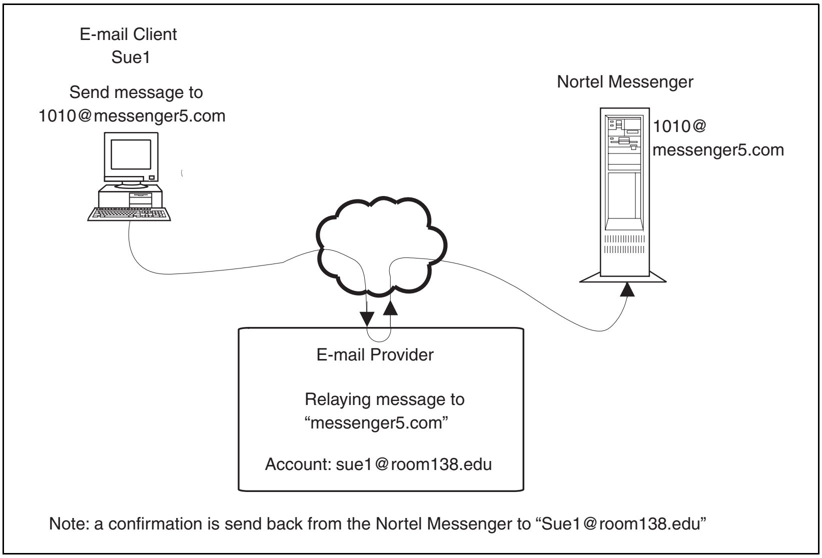
General

The 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 355 shows the path of an e-mail message from client to DECT Messenger.

Figure 355
Sending e-mail from client to DECT Messenger



In the 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.

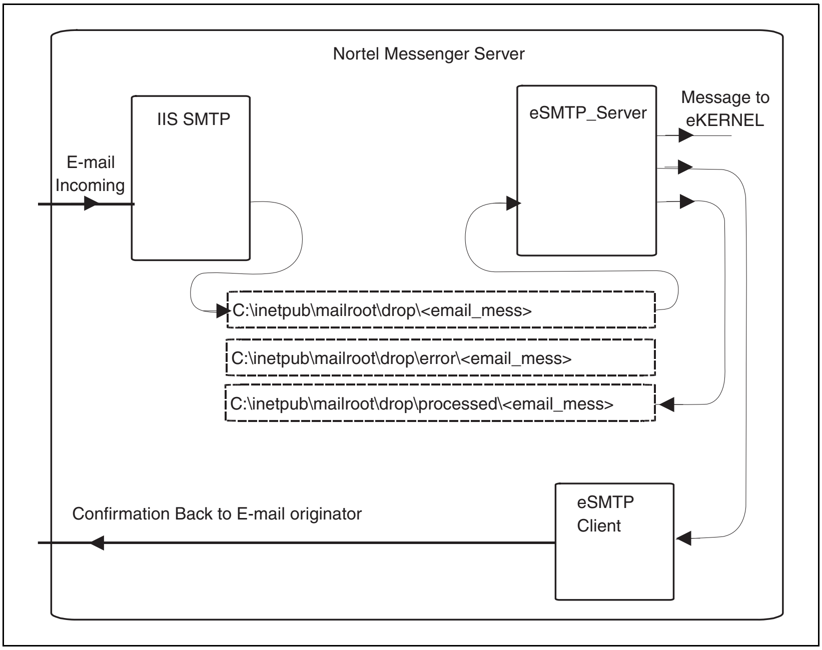
  If a Lotus Notes Domino server is installed on the system, there must also be a Lotus Notes SMTP server that is capable of receiving SMTP messages from the DECT Messenger. You cannot send an e-mail message from the DECT Messenger directly to a Domino server.

Using eSMTP Server

How eSMTP Works

The eSMTP_Server handles incoming e-mail messages, working in cooperation with IIS. In Figure 356 on page 776 the structure of the e-mail path is depicted.

Figure 356
e-mail handling in the DECT Messenger


Nortel 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

When an e-mail is sent from the e-mail client to the DECT Messenger, the e-mail generally goes through an e-mail provider (through a server). In this e-mail Server, relaying must have been switched on, otherwise the e-mail is not transferred to the 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 have been 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.

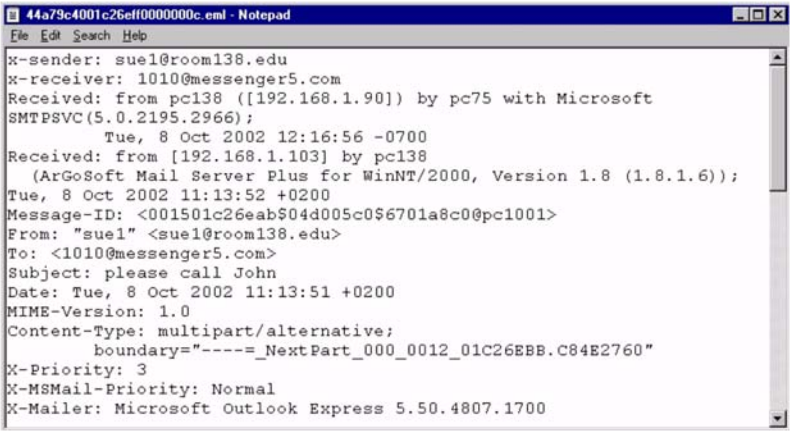
When an e-mail is sent to the DECT Messenger, the message arrives at the IIS SMTP server. The IIS SMTP Server stores the mail message as a file in a specified directory on the hard disk. This directory is the interface between IIS and the eSMTP_Server software. The eSMTP_Server checks the contents of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

- The e-mail address on the 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. When 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.

Figure 357
Example of e-mail message



```
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
```

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, then 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, then 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 the 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/Windows 2003 Server, you must install IIS separately, and then configure IIS. Installing IIS is described in “Installing IIS” on page 779. Configuring IIS is described in “Configuring IIS For DECT Messenger” on page 780.

In the eCONFIG you must set up the configuration for the eSMTP_Server. See “Install PC – Step 5 – eSMTP_Server” on page 995 for further information on setting up the eSMTP_Server.

Installing IIS

The following procedure guides you through the IIS installation process.

Note 1: You must have the Windows CD-ROM on hand to complete this procedure.

Note 2: In Windows 2000/XP Professional and Windows 2003 Server, IIS is not installed by default. In Windows 2000 Server, IIS is installed by default,

Procedure 208
Install IIS

Step	Action
1	Open Add/Remove Programs.
	• Click **Start** on the Windows taskbar, 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 when the system asks for it.

END

Note: After installing IIS on Windows 2000 Pro, 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:

1. Assuming the 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.

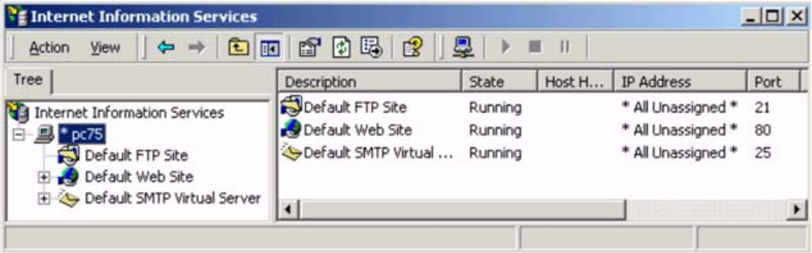
Procedure 209
Configure IIS for DECT Messenger (Part 1 of 6)

Step	Action
1	Open the Internet Services Manager (IIS).
	Click **Start** on the Windows taskbar, and choose **Settings Control Panel > Administrative Tools > Internet Services Manager.**

Procedure 209
Configure IIS for DECT Messenger (Part 2 of 6)

Step	Action
2	Disable the default ftp/web sites.

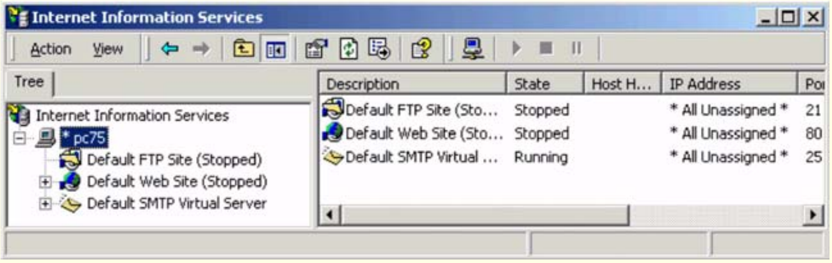
- Expand the PC name to access the FTP, WEB, and SMTP services under it.
- Right-click the **Default FTP Site**, and select **Stop** in the pop-up menu.


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.

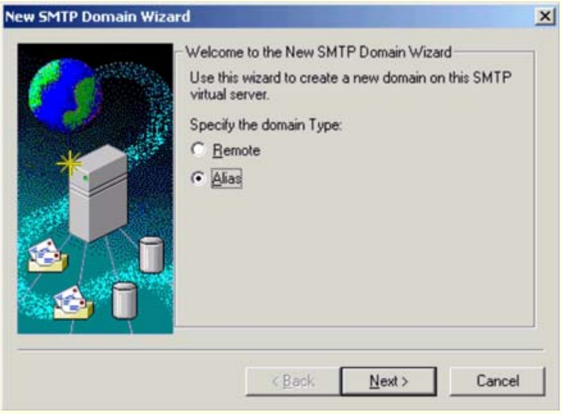
Note: If the Default Web Site is already stopped, IIS has detected that your Apache Web server is running. You can have only one web server running on port 80, which is the reason why IIS web server must be stopped. Check to ensure the State column changes to read Stopped, as shown in the following image:


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

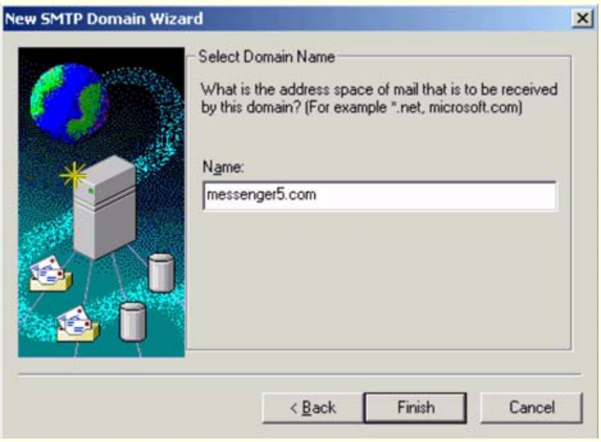
Description	State	Host H...	IP Address	Poi
Default FTP Site (Sto...	Stopped		* All Unassigned *	21
Default Web Site (Sto...	Stopped		* All Unassigned *	80
Default SMTP Virtual ...	Running		* All Unassigned *	25

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

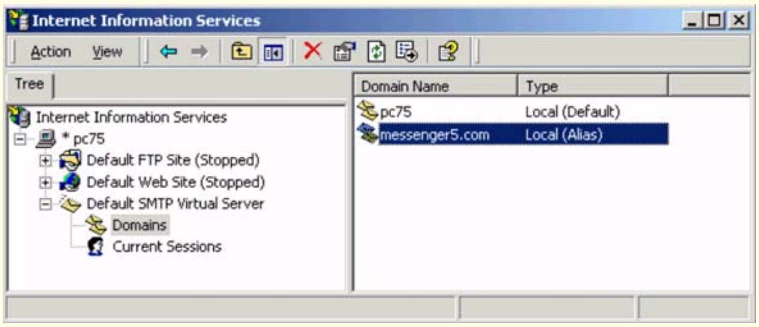
Procedure 209
Configure IIS for DECT Messenger (Part 3 of 6)

Step	Action
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

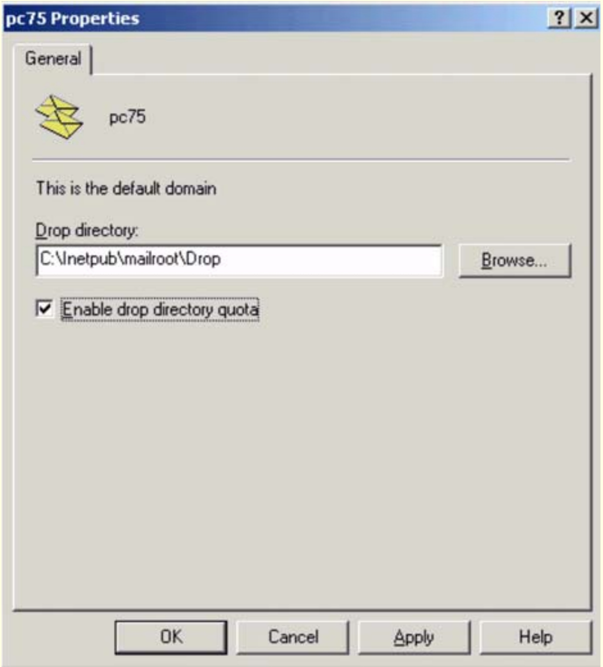
Procedure 209
Configure IIS for DECT Messenger (Part 4 of 6)

Step	Action
5	Set the domain name.
	Enter the domain name. If necessary, contact your system administrator to verify the domain name. This name must have been 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 the 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.  New SMTP Domain Wizard Select Domain Name What is the address space of mail that is to be received by this domain? (For example *.net, microsoft.com) Name: messenger5.com

Procedure 209
Configure IIS for DECT Messenger (Part 5 of 6)

Step	Action
6	Verify the Domain Name list.
	After entering the Alias, the IIS window must look like the following example:  Internet Information Services Tree: Internet Information Services / * pc75 / Default FTP Site (Stopped) / Default Web Site (Stopped) / Default SMTP Virtual Server / Domains / Current Sessions Domain Name: pc75 — Type: Local (Default) Domain Name: messenger5.com — Type: Local (Alias) ***Note:*** The name Alias in this window is an example. In your configuration a different name appears.

Procedure 209
Configure IIS for DECT Messenger (Part 6 of 6)

Step	Action
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:  pc75 Properties General pc75 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**.

END

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:

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.

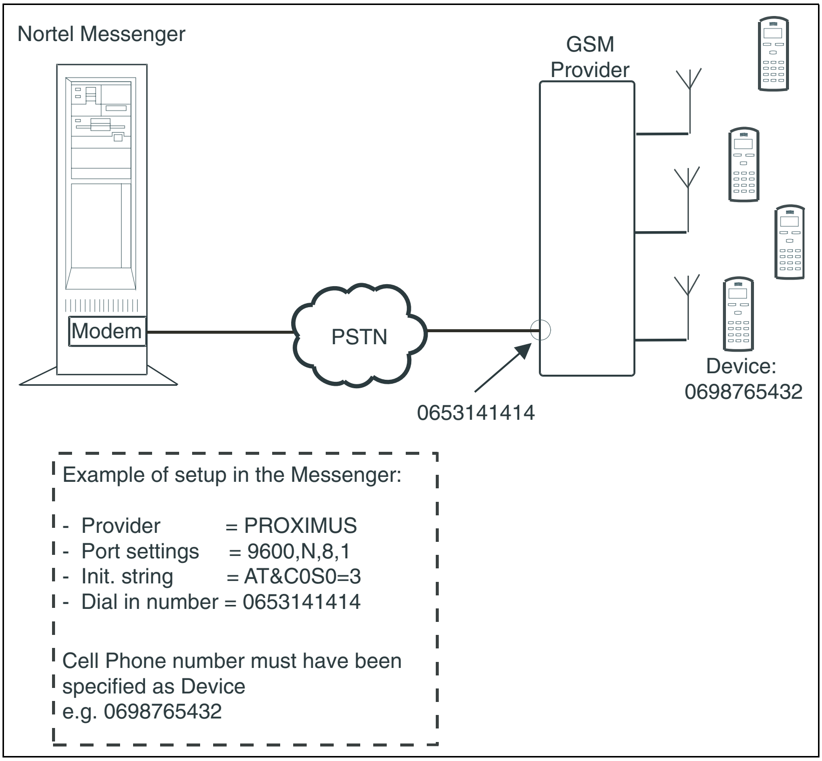
3 Set the number of retries for the DECT device = 2.

If the 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 358 shows the configuration.

Figure 358
Setup for sending SMS Messages (or Wide Area Paging messages)



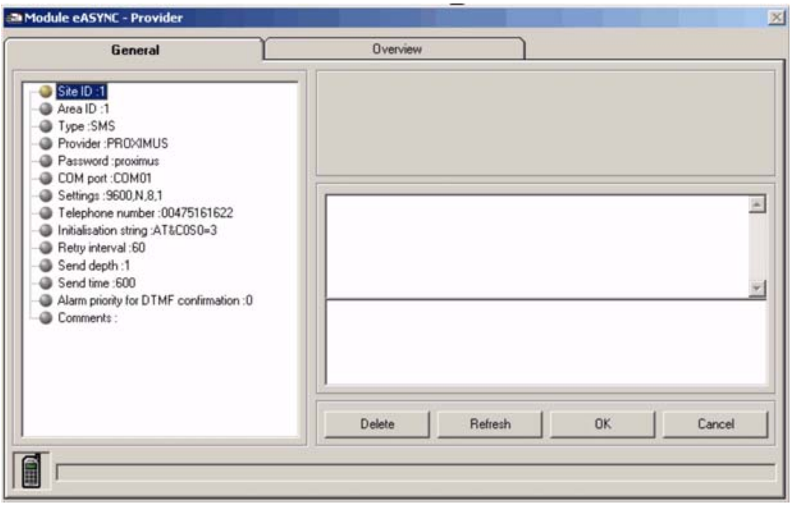
Example of setup in the Messenger:

- 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

The connection between DECT Messenger and the GSM SMS provider is made through a modem connection using the PSTN. In the 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 359 on page 788 opens.

Figure 359
eASYNC settings



- 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 :

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 UCP (Universal Computer Protocol) 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 initialisation string for modem initialisation. The string depends on the type of modem that you use. A generic modem initialisation 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

  The 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. When 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 the DECT Messenger waiting for a long period, you can specify a Send Time. Once 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 the 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 Nortel, to see if the protocol is supported by the 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 732. You must know which parameters are coming in from the external system, and you must specify these parameters in the DECT Messenger. For more information, see the chapter “Module – eCAP” on page 1091, which describes the supported protocols in detail.

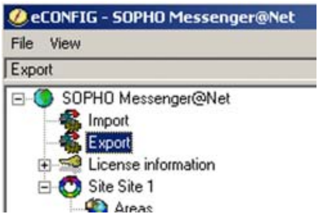
eESPA

The eESPA module supports the ESPA 444 protocol. This is a complex protocol; see “Module – eESPA” on page 1115 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

eCONFIG allows you to import and export configuration database tables. The menu options are shown in Figure 360 on page 792.

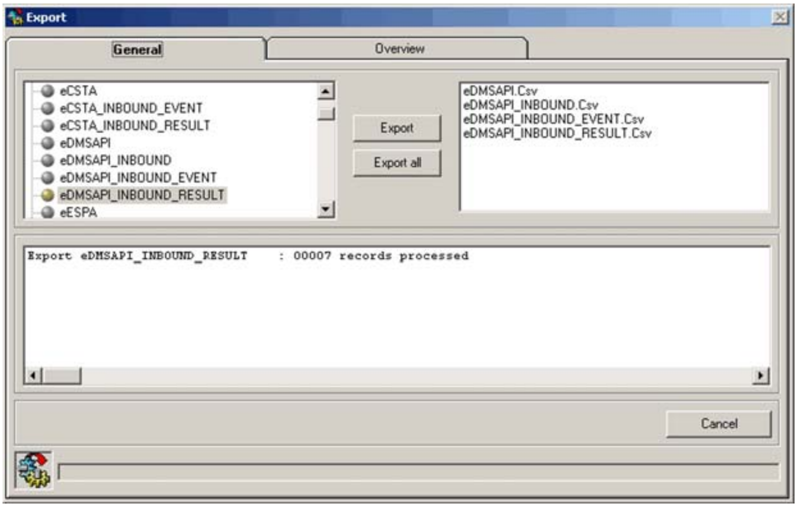
Figure 360
Import/Export menu options



The Import/Export function can only handle files of the type .CSV.

Double-click **Export**, to open the following window:

Figure 361
The Export window

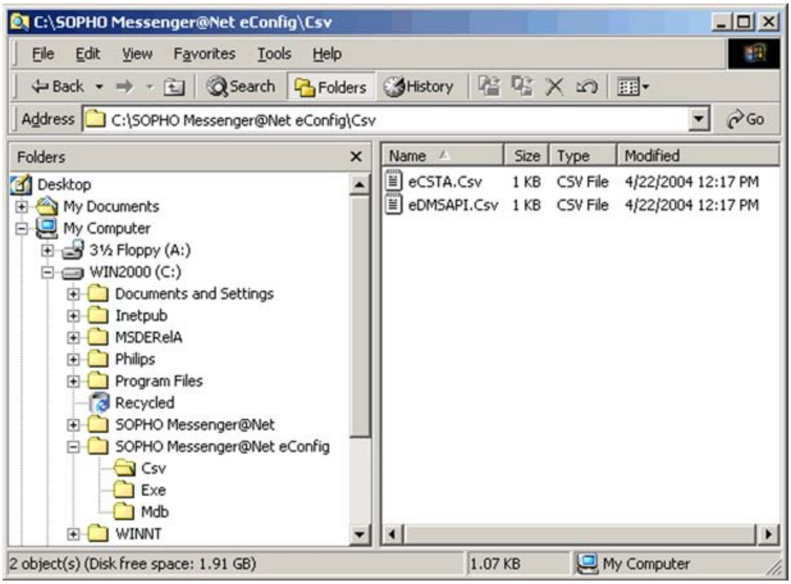


```
Export eDMSAPI_INBOUND_RESULT    : 00007 records processed
```

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

Figure 362
The configuration file storage directory



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

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.

Checking diagnostics

General

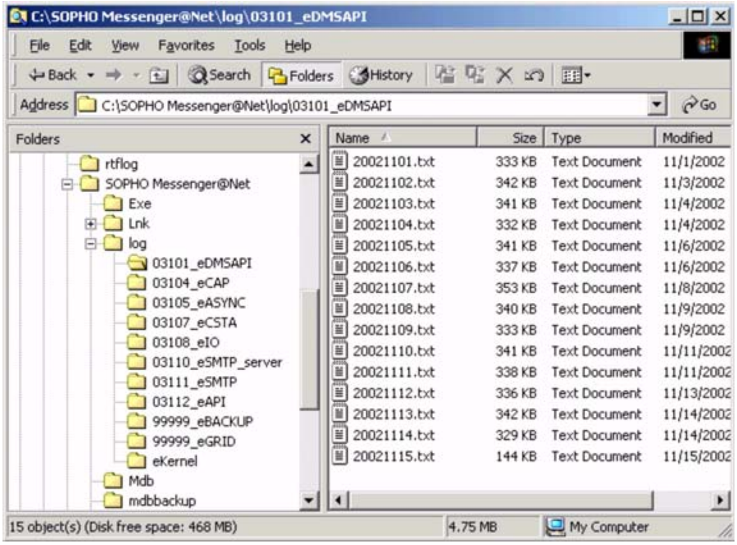
The following diagnostics options are discussed in this section:

- “Logging” on page 794
- “Module Window” on page 797

Logging

Logging allows you 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 363.

Figure 363
Log file location



Address: C:\SOPHO Messenger@Net\log\03101_eDMSAPI

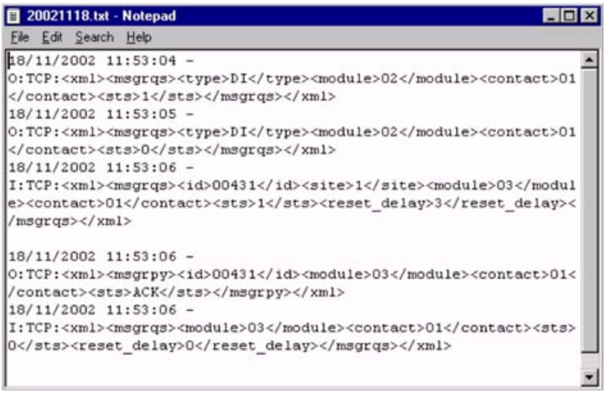
Name	Size	Type	Modified
20021101.txt	333 KB	Text Document	11/1/2002
20021102.txt	342 KB	Text Document	11/3/2002
20021103.txt	341 KB	Text Document	11/4/2002
20021104.txt	332 KB	Text Document	11/4/2002
20021105.txt	341 KB	Text Document	11/6/2002
20021106.txt	337 KB	Text Document	11/6/2002
20021107.txt	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

The “Table: eKERNEL_SITE” on page 1459 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 364 on page 795.

Figure 364
IO Module log file



```
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 364 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 364:

- `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 364 on page 795, 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 364, the following messages have been exchanged between the eIO module and the eKERNEL per 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

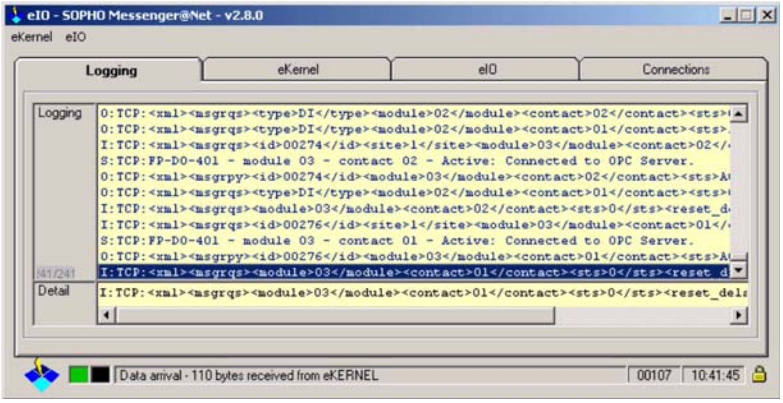
Each module runs as an application in the Windows environment, and can be displayed as an open window, or minimised on the Windows Taskbar. The module window provides online information about settings, commands/messages/communication. This information is very useful for debugging. The eIO module is shown 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 minimised, maximize it. Four tabs are visible in the window, as follows:

- Logging Tab

  In the logging tab, the online log information is provided.

Figure 365
Logging Tab



```
0:TCP:<xml><msgrqs><type>DI</type><module>02</module><contact>02</contact><sts>
0: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-D0-401 - module 03 - contact 02 - Active: Connected to OPC Server.
0:TCP:<xml><msgrpy><id>00274</id><module>03</module><contact>02</contact><sts>A
0: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-D0-401 - module 03 - contact 01 - Active: Connected to OPC Server.
0: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
```

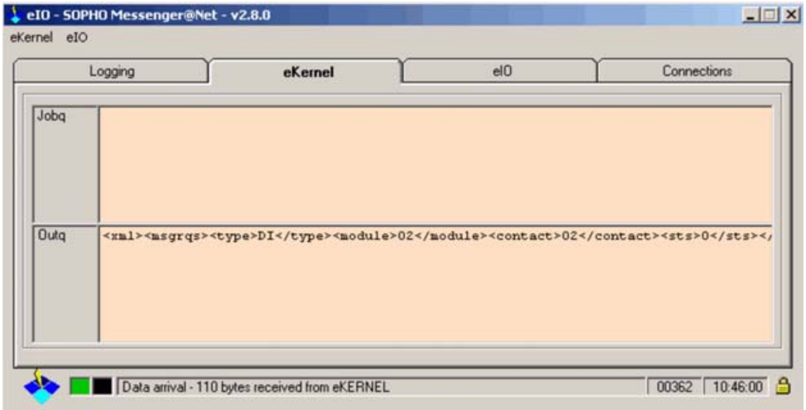
Data arrival - 110 bytes received from eKERNEL 00107 10:41:45

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, see “Logging” on page 794. 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.

Figure 366
eKERNEL Tab



Outq: `<xml><msgrqs><type>DI</type><module>02</module><contact>02</contact><sts>0</sts></`

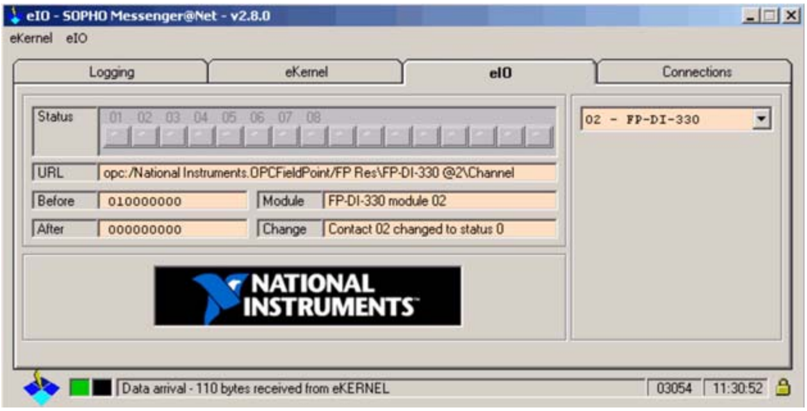
Data arrival - 110 bytes received from eKERNEL | 00362 | 10:46:00

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.

Figure 367
eIO Tab



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

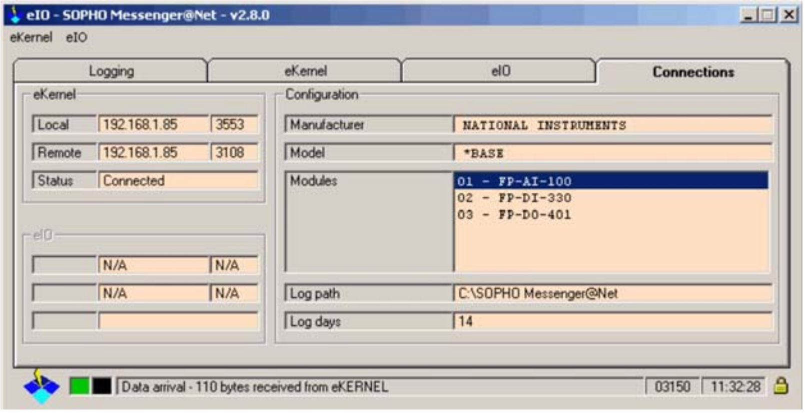
02 - FP-DI-330

Data arrival - 110 bytes received from eKERNEL | 03054 | 11:30:52

- 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.

Figure 368
Connections Tab



eKernel
Local 192.168.1.85 3553
Remote 192.168.1.85 3108
Status Connected

eIO
N/A N/A
N/A N/A

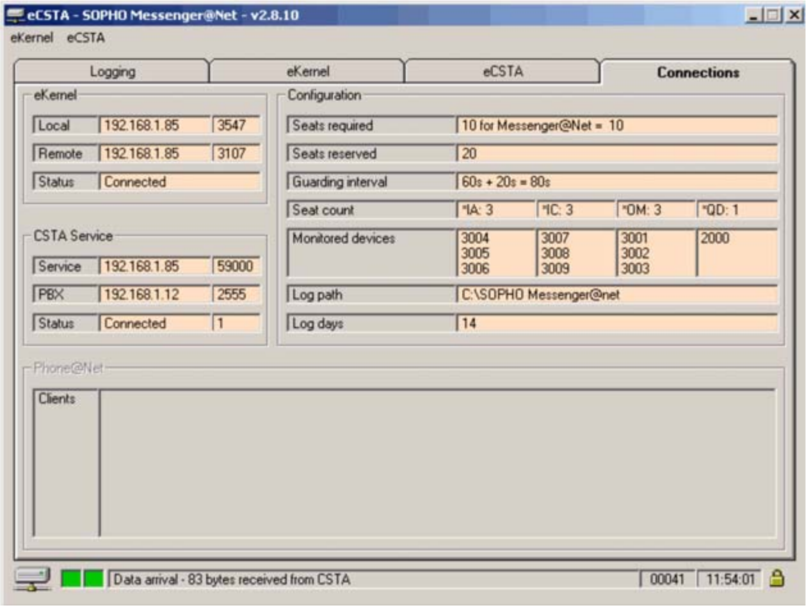
Configuration
Manufacturer NATIONAL INSTRUMENTS
Model *BASE
Modules 01 - FP-AI-100
02 - FP-DI-330
03 - FP-DO-401
Log path C:\SOPHO Messenger@Net
Log days 14

Data arrival - 110 bytes received from eKERNEL 03150 11:32:28

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 368 shows only one TCP/IP connection between the eIO module and the eKERNEL. If another TCP/IP connection was available, the bottom part of the left pane would be filled in.

Figure 369
Status lamps



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			

Phone@Net

Clients	

🟩🟩 Data arrival - 83 bytes received from CSTA | 00041 | 11:54:01

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 369. There are three possible colours 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:

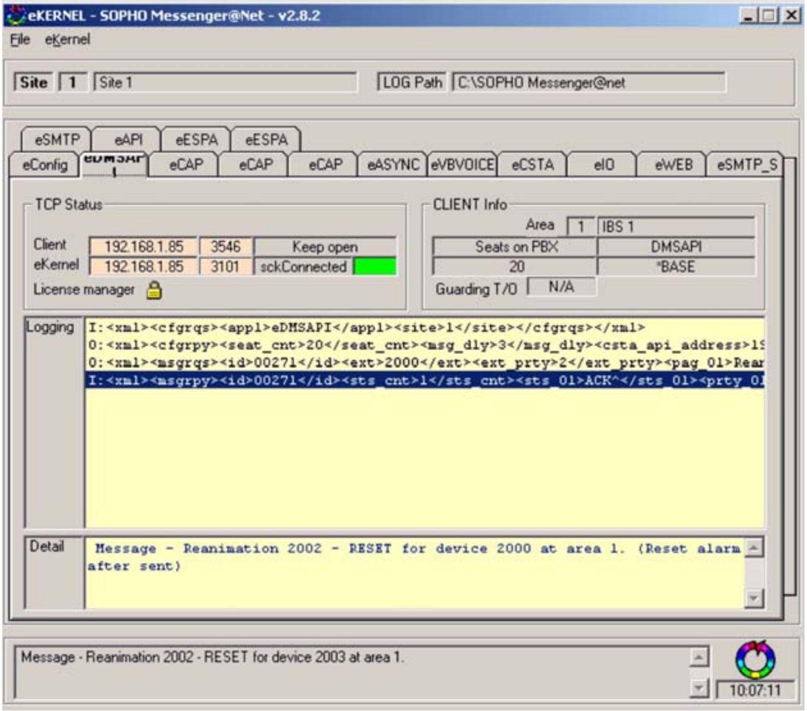
c:\WINNT\system32\drivers\etc\services

> ***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.

Figure 370
eKERNEL module window



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>1S
O:<xml><msgrqs><id>00271</id><ext>2000</ext><ext_prty>2</ext_prty><pag_01>Rear
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

Select a module tab to see the information for that specific module, as follows:

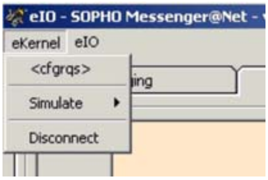
- TCP status. Shows the connection data for the TCP/IP connection between the eKERNEL and the module.
- Client info. Shows information about the module.
- Logging. Shows the logged communication between the eKERNEL and the module.
- Detail. Shows communication. As well, if you left-click a line in the 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

Modules have a simulation menu, which allows you to simulate an message. The simulation is different for each individual module, because the nature of the modules differ. Figure 371 shows you how to access the simulation menu.

Figure 371
Accessing Simulate Options



eKERNEL Service Options

As shown in Figure 372 on page 804, eKERNEL offer the following service options:

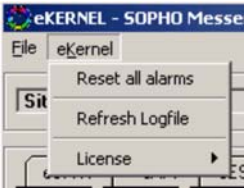
- Reset All Alarms

  The menu item **eKERNEL** > **Reset All Alarms** clears all alarms in the DECT Messenger.

- Refresh Logfile

  The menu item **eKERNEL** > **Refresh Logfile** stores the latest log information in the eKERNEL log file.

Figure 372
Accessing Reset all alarms



General – Install PC

This chapter provides information on “Installing DECT Messenger components” on page 806.

Before you begin

Before installing the Nortel DECT Messenger components, verify that your PC is ready by performing the following:

1 Install and configure the operating system on the PC. Supported Operating Systems are: Windows 2000 Professional, Windows XP Professional, Windows 2000 Server, and Windows 2003 Server Standard Edition.

Note: Nortel recommends that you use the computer name WMS. If a different name is used, some configuration changes are required in Apache Web Server configuration.

2 Configure TCP/IP and verify the network connection with the PBX.

3 Verify the international settings while configuring your Windows operating system. If your system is preloaded, verify the Regional Options in the Control Panel (Locale, and so on).

4 Proceed with the installation steps discussed in Table 210 on page 806.

Installing DECT Messenger components

Procedure 210
Install PC components (Part 1 of 4)

Step	Action
1a	Install Adobe Acrobat Reader.
	Refer to “Install PC – Step 1a – Adobe Acrobat Reader” on page 811 for more information on how to install this product. This step is required if you plan to use eGRID module, eWEB module, or if you plan on consulting available online help documentation.
1b	Install the latest service pack on the Windows operating system.
	Note: Perform the Windows Update after installation, and regularly thereafter ensure that the latest available patches are installed.
1c	Install the latest Microsoft Data Access Components (MDAC).
	Refer to “Install PC – Step 1b – Microsoft Data Access Components (MDAC)” on page 817 for more information.
1d	Install WinZip (optional).
	Refer to “Install PC – Step 1c – WinZip” on page 823 for more information. It is useful to install compression software on the system, for example to compress log files for problem analysis. For your convenience, WinZip is shipped with DECT Messenger. ***Note:*** You are free to choose another compression tool, such as WinRar. Windows XP also features support for Zip-compression.
1e	Install the TCP Monitor.
	Refer to “Install PC – Step 1d – TCP Monitor” on page 835 for more information. ***Note:*** This step is optional, but Nortel recommends it for troubleshooting if you are using the eDMSAPI module.

Procedure 210
Install PC components (Part 2 of 4)

Step	Action
1f	Install the Nortel Licence Manager.
	Refer to “Install PC – Step 1e – Licence Manager” on page 839 for more information. Be sure to install the latest release of this software. Contact Nortel if you need help, or are unsure what release is installed. You also need a valid licence key for your installation.
1g	Install the SQL Server.
	Refer to “Install PC – Step 1f – SQL Server” on page 843 for more information. This is required if you plan to use the SQL Server or MSDE engine for DECT Messenger. This step is not required if you pan to use the MS Access database engine.
1h	Install Secure Session.
	Refer to “Install PC – Step 1g – Secure Session” on page 865 for more information.
2	Install the Nortel DECT Messenger.
	Refer to “Install PC – Step 2 – Nortel DECT Messenger” on page 873 for more information.
3	Install National Instruments software.
	Refer to “Install PC – Step 3 – National Instruments” on page 889 for more information on how to configure the components FieldPoint Explorer and DataSocket OPC Server. Both steps are required if you plan to use eIO module.
4	Install Web Server.

Procedure 210
Install PC components (Part 3 of 4)

Step	Action
	Refer to “Install PC – Step 4 – Web Server” on page 949 for more information on how to configure the ODBC based access used within the eWEB module. The same document describes the steps involving installing and configuring Apache and PHP. These steps are required if you plan to use eWEB module.
5	Install SMTP Server.
	Refer to “Install PC – Step 5 – eSMTP_Server” on page 995 for more information on how to configure the SMTP Server. This step is required if the module eSMTP_server (inbound e-mail support) is used.
6	Install configuration tool.
	Choose one of the following: • Refer to “Install PC – Step 6 – eCONFIG” on page 1013 for more information on how to install the eCONFIG module. Nortel recommends that you use the eCONFIG module as a central configuration tool. • If you prefer manual configuration through the eGRID module, you must locate and manually modify the appropriate shortcuts that reside in **C:\SOPHO Messenger@Net\Lnk**. You can use the eTM Task Manager module to launch the configured modules at start-up. If you do not use the eTM module, move all shortcuts to the **Startup** group, so that the application launches when the PC reboots. Refer to the relevant documents for more information on configuration issues. For further documentation of table values, refer to the Readme.html index of documentation. Refer to “Module – eWEB” on page 1265 for more information on eWEB. If eWEB is activated, you can also consult the online documentation through the eWEB interface.

Procedure 210
Install PC components (Part 4 of 4)

Step	Action
7	Install Updates.
	Due to ongoing development on the DECT Messenger product suite, enhancements of software modules are distributed from time to time. These enhancements can also introduce new functionality. Nortel recommends that you install any updates found in the directory **\Step 8 - Updates.**
8	DECT Messenger add-on modules.
	The development team of DECT Messenger also provides add-on modules for DECT Messenger. These modules are usually deployed on a project-by-project basis, and are to be installed separately. The current distribution provides the modules eNET and eLICENCE.

END

Install PC – Step 1a – Adobe Acrobat Reader

This chapter provides information on "Installing Adobe Acrobat Reader" on page 812.

The documentation of Nortel DECT Messenger is shipped in .PDF format. To read these documents, you must install "Adobe Acrobat Reader" on your PC.

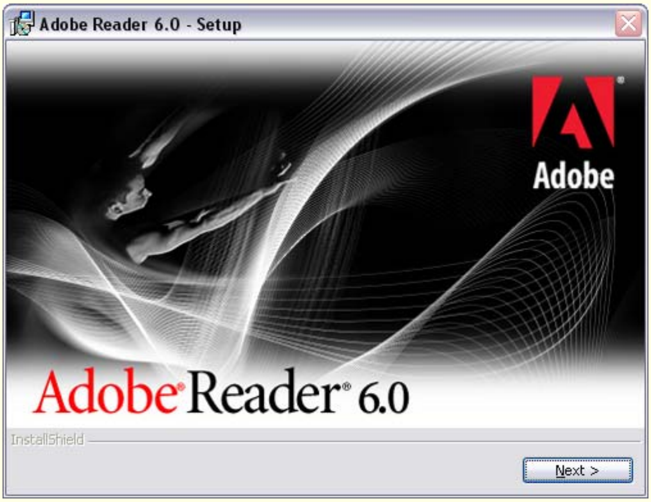
> ***Note:*** If you offer access to the DECT Messenger documentation through a Web Server, users must also install the reader to view these documents.

The Adobe Acrobat Reader can be downloaded from the Internet. For your convenience, a copy of the installation program is shipped on the DECT Messenger CD-ROM. The Adobe Acrobat Reader Installation package is located in the directory Step 1 – Prerequisites > Step 1a - Adobe Acrobat Reader > 6.0 > English. Only the English version is provided; other languages can be downloaded from the Internet.

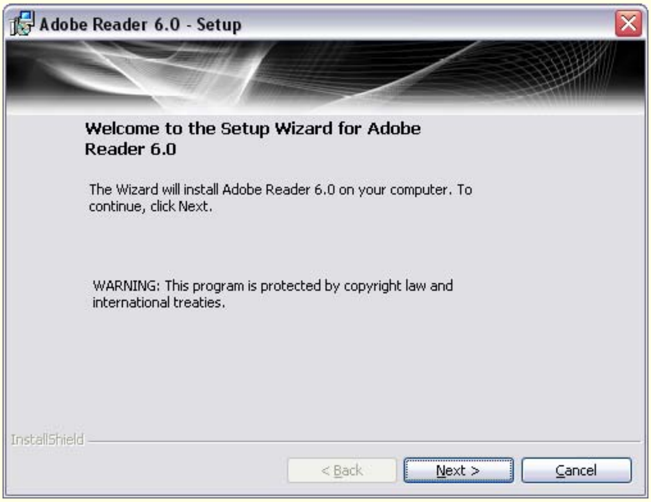
Table 211 on page 812 describes the installation procedure for the English version.

Installing Adobe Acrobat Reader

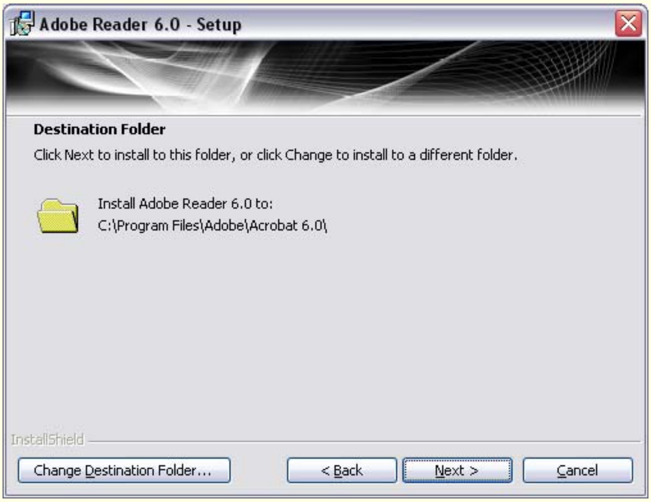
Procedure 211
Installing Adobe Acrobat Reader (Part 1 of 5)

Step	Action
1	Start the installation wizard for Adobe Acrobat Reader 6.0.
	Double-click the file AdbeRdr60_enu_full.exe. A progress window opens, followed by the dialog box shown in step 2.
2	Acknowledge the Adobe splash screen.
	Click **Next** to continue.  Adobe Reader 6.0 - Setup Adobe Adobe Reader 6.0 InstallShield Next >

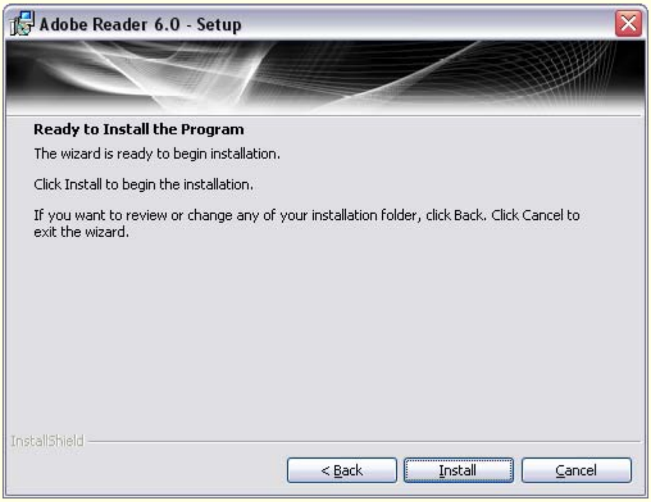
Procedure 211
Installing Adobe Acrobat Reader (Part 2 of 5)

Step	Action
3	Acknowledge the warning, and start the installation process.
	Click **Next** to continue.  Adobe Reader 6.0 - Setup **Welcome to the Setup Wizard for Adobe Reader 6.0** The Wizard will install Adobe Reader 6.0 on your computer. To continue, click Next. WARNING: This program is protected by copyright law and international treaties.

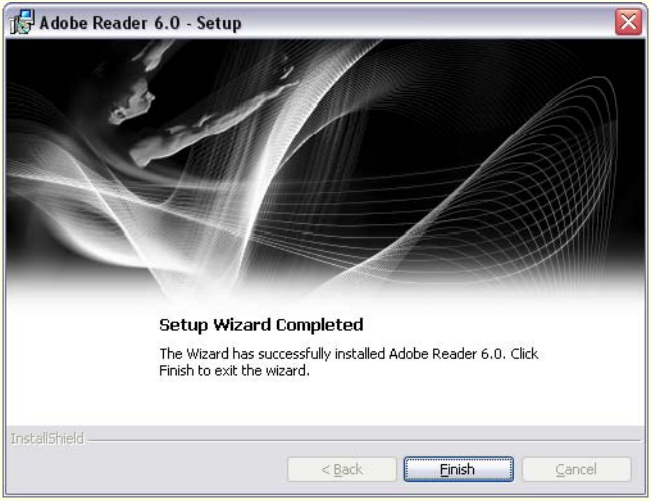
Procedure 211
Installing Adobe Acrobat Reader (Part 3 of 5)

Step	Action
4	Verify the install location.
	Click **Next** to accept the default location.  Adobe Reader 6.0 - Setup **Destination Folder** Click Next to install to this folder, or click Change to install to a different folder. Install Adobe Reader 6.0 to: C:\Program Files\Adobe\Acrobat 6.0\ InstallShield Change Destination Folder... < Back Next > Cancel

Procedure 211
Installing Adobe Acrobat Reader (Part 4 of 5)

Step	Action
5	Verify that you are ready to install the software.
	Click **Install** to start installation.  Adobe Reader 6.0 - Setup **Ready to Install the Program** The wizard is ready to begin installation. Click Install to begin the installation. If you want to review or change any of your installation folder, click Back. Click Cancel to exit the wizard.

Procedure 211
Installing Adobe Acrobat Reader (Part 5 of 5)

Step	Action
6	Acknowledge completion of the installation.
	When installation is complete, the following window opens. Click **Finish**.  **Setup Wizard Completed** The Wizard has successfully installed Adobe Reader 6.0. Click Finish to exit the wizard.
7	(Optional) Remove the Acrobat Reader 6.0 icon that appears on the desktop.
	An Acrobat Reader 6.0 icon is installed on the desktop as part of the installation procedure; you can remove this if you wish. If you double-click files with the .PDF extension, Adobe Acrobat Reader is launched automatically.

END

Install PC – Step 1b – Microsoft Data Access Components (MDAC)

This chapter provides information on "Installing MDAC" on page 818.

Consult the Microsoft web site (www.microsoft.com), and the Microsoft Universal Database Access Download Page, for more information.

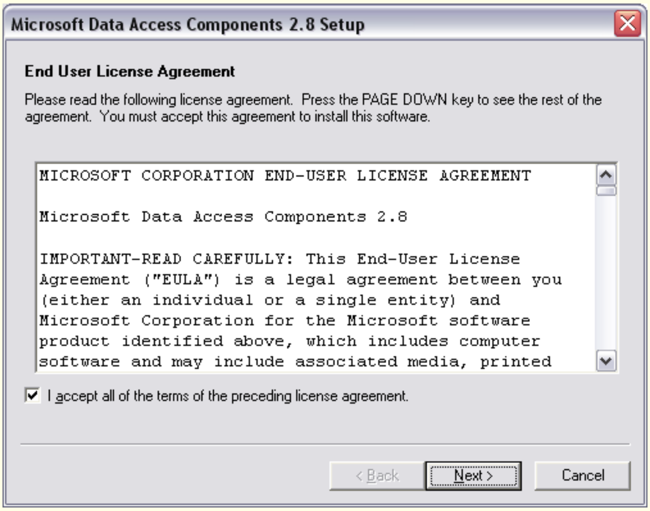
Microsoft Data Access Components (MDAC) 2.8 contain core Data Access components, such as the Microsoft SQL Server™ OLE DB provider and ODBC driver.

This release does not include Microsoft Jet, the Microsoft Jet OLE DB Provider or ODBC driver, the Desktop Database ODBC Drivers, or the Visual FoxPro ODBC Driver.

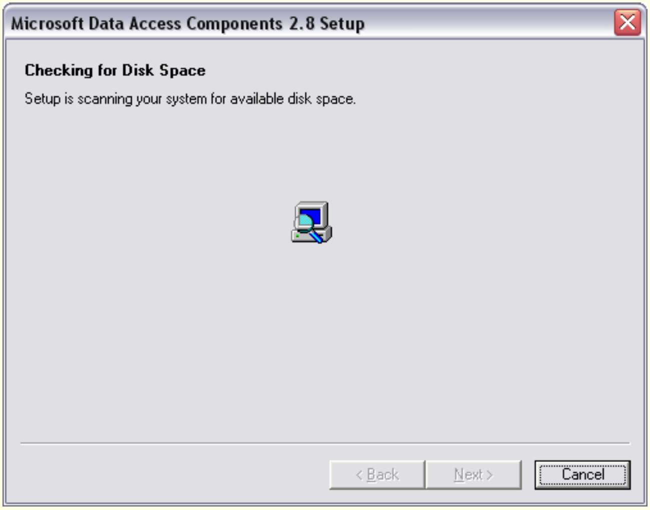
For your convenience, a recent English version of Microsoft Data Access Components 2.8 is shipped on the CD-ROM and is located in \Step 1 – Prerequisites > Step 1c – MDAC > MDAC 2.8. If you require another language, you can download the appropriate version from the Microsoft web site.

Installing MDAC

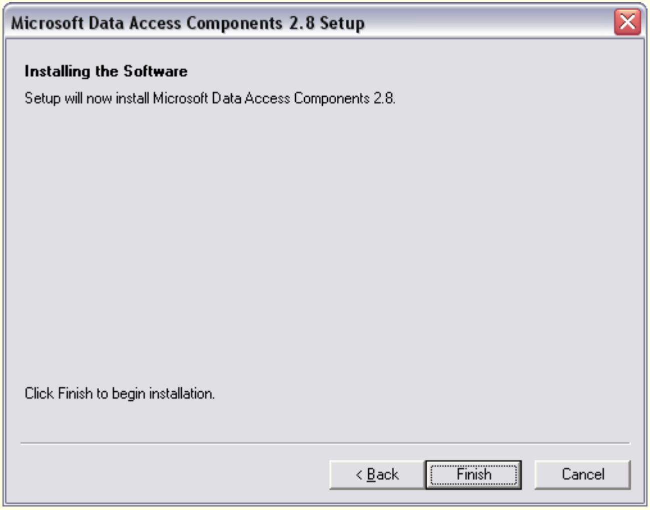
Procedure 212
Install MDAC (Part 1 of 4)

Step	Action
1	Start MDAC installation.
	Double-click the MDAC_TYP.exe file to launch the Microsoft Data Access Components 2.8 Setup. A message box with a progress indicator opens.
2	Accept the Licence Agreement.
	Click **Next**.  Microsoft Data Access Components 2.8 Setup **End User License Agreement** Please read the following license agreement. Press the PAGE DOWN key to see the rest of the agreement. You must accept this agreement to install this software. MICROSOFT CORPORATION END-USER LICENSE AGREEMENT Microsoft Data Access Components 2.8 IMPORTANT-READ CAREFULLY: This End-User License Agreement ("EULA") is a legal agreement between you (either an individual or a single entity) and Microsoft Corporation for the Microsoft software product identified above, which includes computer software and may include associated media, printed ☑ I accept all of the terms of the preceding license agreement.

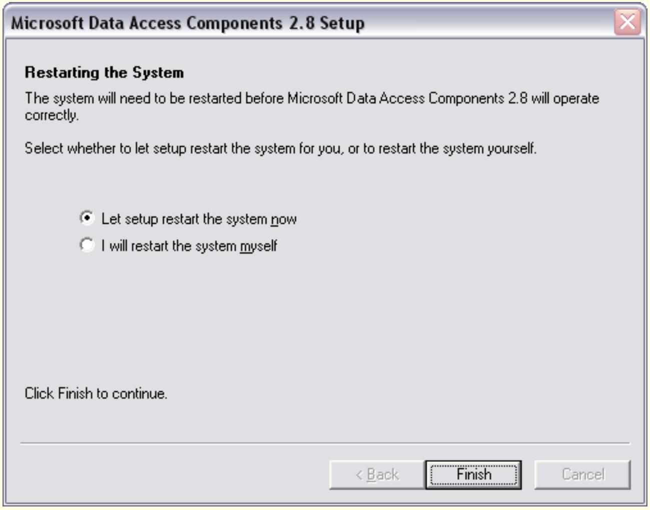
Procedure 212
Install MDAC (Part 2 of 4)

Step	Action
3	Wait while intermediate windows are displayed.
	An intermediate window is shown while the program checks disk space and shared resources. Wait until this step has finished (do not click **Cancel**).  Microsoft Data Access Components 2.8 Setup **Checking for Disk Space** Setup is scanning your system for available disk space. An additional intermediate window is sometimes shown indicating shutdown of server components if they share resources that are updated during the installation of MDAC_TYP.exe.

Procedure 212
Install MDAC (Part 3 of 4)

Step	Action
4	Begin the installation.
	Click **Finish** to begin the installation.  Microsoft Data Access Components 2.8 Setup **Installing the Software** Setup will now install Microsoft Data Access Components 2.8. Click Finish to begin installation. A number of windows open during installation, displaying progress indicators.

Procedure 212
Install MDAC (Part 4 of 4)

Step	Action
5	Restart the system.
	When installation is finished, you must restart the system. Shut down any other applications you are using, to prevent data loss. When all applications are stopped, the following dialog box opens. Click **Finish**.  Microsoft Data Access Components 2.8 Setup **Restarting the System** The system will need to be restarted before Microsoft Data Access Components 2.8 will operate correctly. Select whether to let setup restart the system for you, or to restart the system yourself. ● Let setup restart the system now ○ I will restart the system myself Click Finish to continue. < Back Finish Cancel

END

Install PC – Step 1c – WinZip

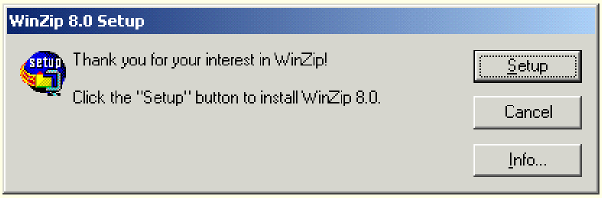
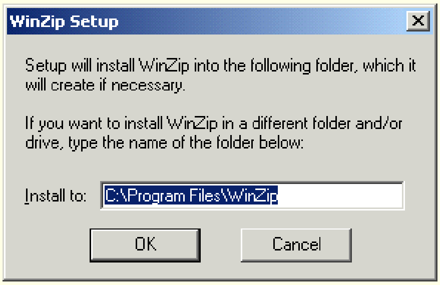
This chapter provides information on “Installing WinZip” on page 824.

Many files are shipped in .ZIP format. An application to extract these files (for example WinZip) can be downloaded from the Internet.

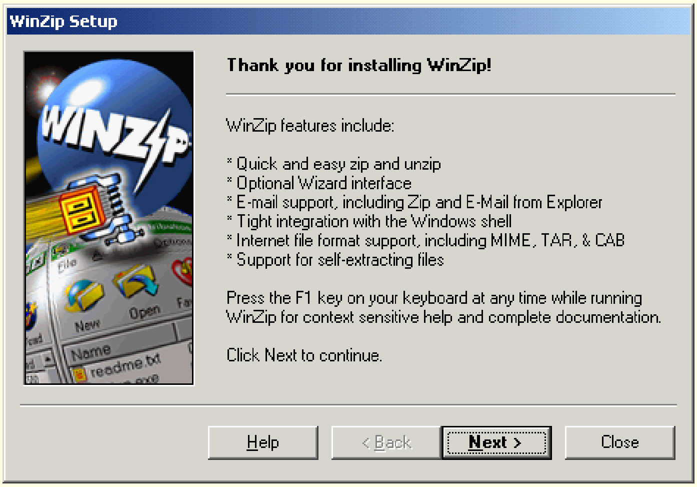
For your convenience, a distribution of WinZip 8.0 evaluation version is shipped on the CD-ROM. You can find the program in the directory \Step 1 – Prerequisites > Step 1d – WinZip > WinZip 8.0.

Installing WinZip

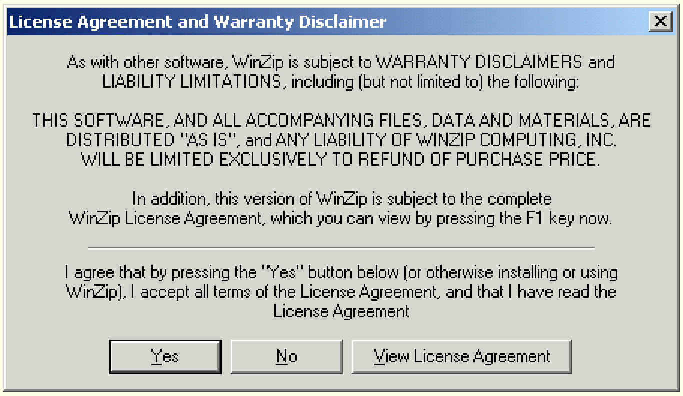
Procedure 213
Install WinZip (Part 1 of 10)

Step	Action
1	Start WinZip installation.
	• Double-click **winzip80.exe**. • Click **Setup**.  WinZip 8.0 Setup Thank you for your interest in WinZip! Click the "Setup" button to install WinZip 8.0.
2	Select the location in which to install the software.
	Accept the default location and click **OK**.  WinZip Setup Setup will install WinZip into the following folder, which it will create if necessary. If you want to install WinZip in a different folder and/or drive, type the name of the folder below: Install to: C:\Program Files\WinZip

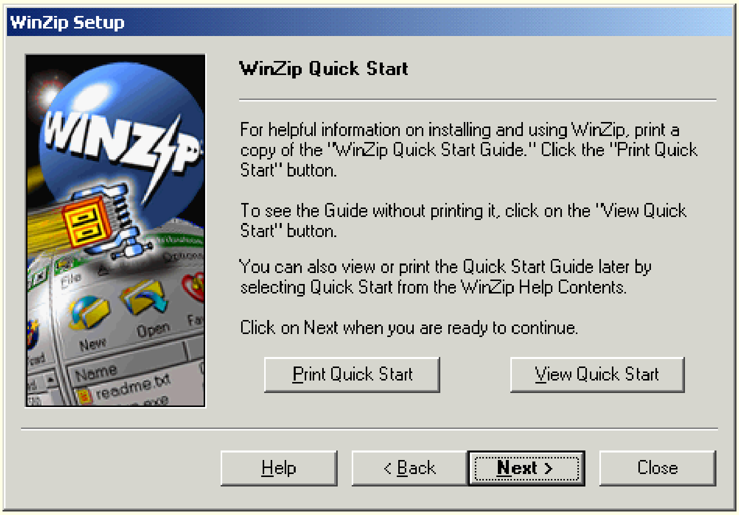
Procedure 213
Install WinZip (Part 2 of 10)

Step	Action
3	Continue with the installation.
	Click **Next** to continue.  WinZip Setup **Thank you for installing WinZip!** WinZip features include: * Quick and easy zip and unzip * Optional Wizard interface * E-mail support, including Zip and E-Mail from Explorer * Tight integration with the Windows shell * Internet file format support, including MIME, TAR, & CAB * Support for self-extracting files Press the F1 key on your keyboard at any time while running WinZip for context sensitive help and complete documentation. Click Next to continue.

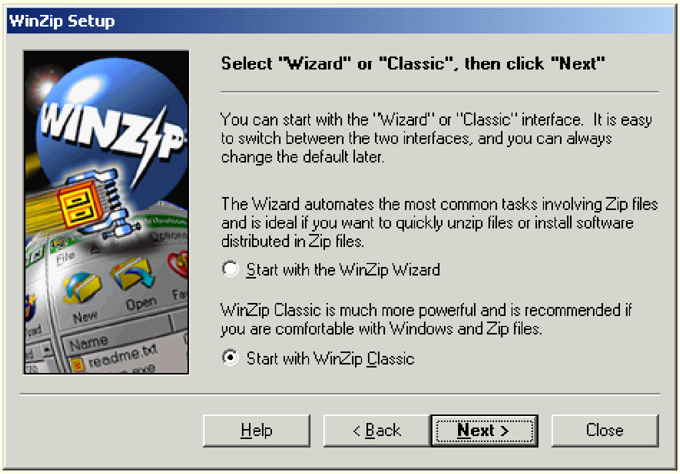
Procedure 213
Install WinZip (Part 3 of 10)

Step	Action
4	Accept the Licence Agreement.
	Review the Licence Agreement. When you are ready, accept the Licence Agreement and warranty disclaimer by clicking **Yes**.  License Agreement and Warranty Disclaimer As with other software, WinZip is subject to WARRANTY DISCLAIMERS and LIABILITY LIMITATIONS, including (but not limited to) the following: THIS SOFTWARE, AND ALL ACCOMPANYING FILES, DATA AND MATERIALS, ARE DISTRIBUTED "AS IS", and ANY LIABILITY OF WINZIP COMPUTING, INC. WILL BE LIMITED EXCLUSIVELY TO REFUND OF PURCHASE PRICE. In addition, this version of WinZip is subject to the complete WinZip License Agreement, which you can view by pressing the F1 key now. I agree that by pressing the "Yes" button below (or otherwise installing or using WinZip), I accept all terms of the License Agreement, and that I have read the License Agreement

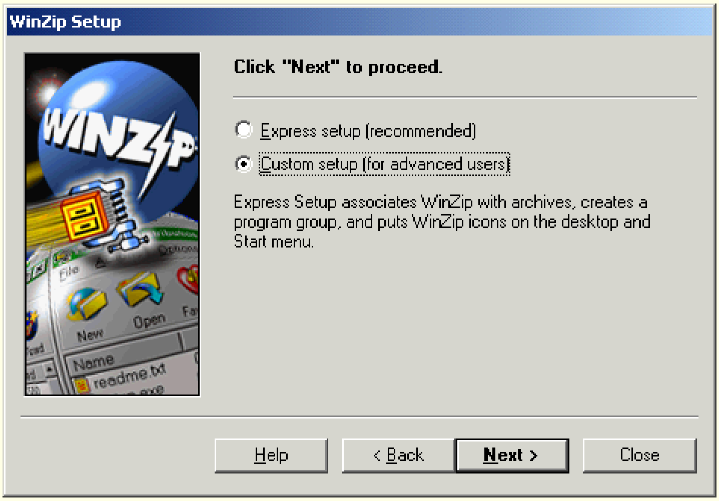
Procedure 213
Install WinZip (Part 4 of 10)

Step	Action
5	Proceed with the installation.
	Review the information provided, and click **Next** to continue.  WinZip Setup WinZip Quick Start For helpful information on installing and using WinZip, print a copy of the "WinZip Quick Start Guide." Click the "Print Quick Start" button. To see the Guide without printing it, click on the "View Quick Start" button. You can also view or print the Quick Start Guide later by selecting Quick Start from the WinZip Help Contents. Click on Next when you are ready to continue. Print Quick Start View Quick Start Help < Back Next > Close

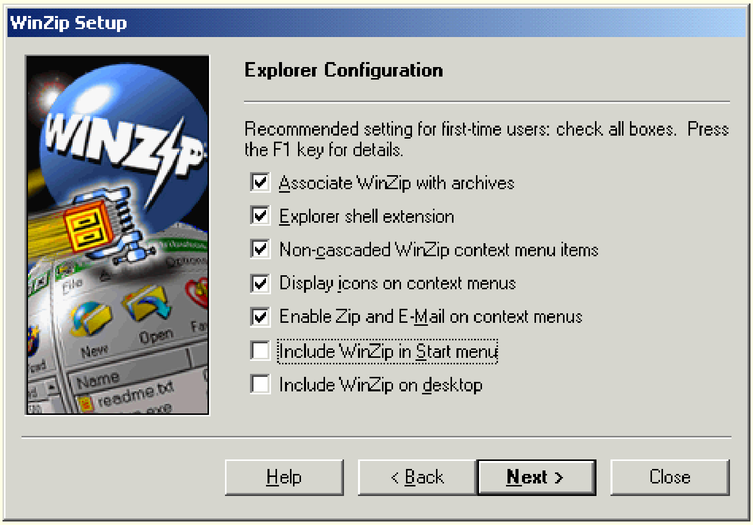
Procedure 213
Install WinZip (Part 5 of 10)

Step	Action
6	Select the interface to use.
	Select the **Start with WinZip Classic** option and click **Next** to continue.  WinZip Setup **Select "Wizard" or "Classic", then click "Next"** You can start with the "Wizard" or "Classic" interface. It is easy to switch between the two interfaces, and you can always change the default later. The Wizard automates the most common tasks involving Zip files and is ideal if you want to quickly unzip files or install software distributed in Zip files. ○ Start with the WinZip Wizard WinZip Classic is much more powerful and is recommended if you are comfortable with Windows and Zip files. ● Start with WinZip Classic

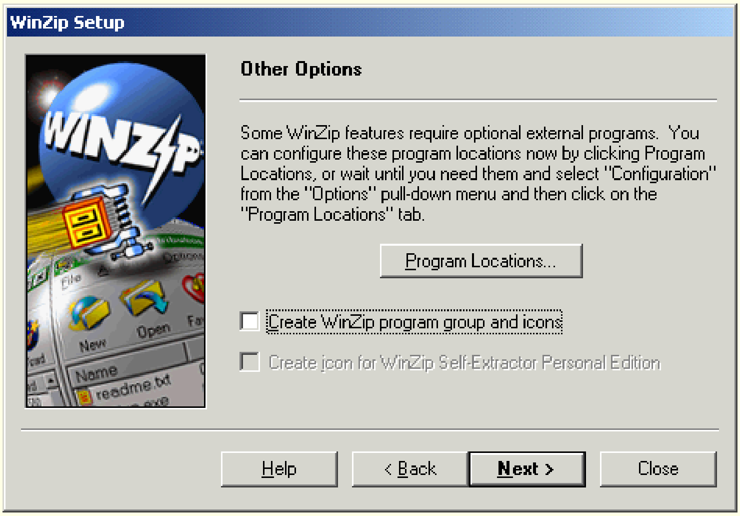
Procedure 213
Install WinZip (Part 6 of 10)

Step	Action
7	Choose a setup option.
	Select the **Custom setup** option (recommended), and click **Next** to continue.  WinZip Setup **Click "Next" to proceed.** ○ Express setup (recommended) ● Custom setup (for advanced users) Express Setup associates WinZip with archives, creates a program group, and puts WinZip icons on the desktop and Start menu.

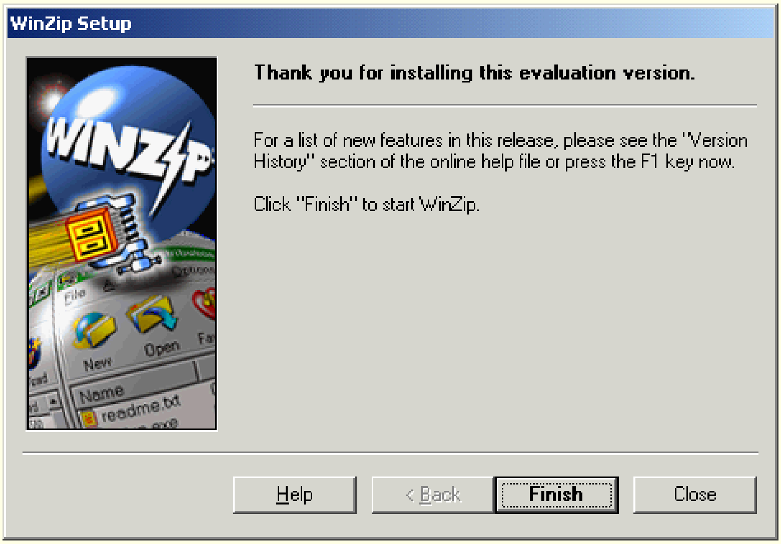
Procedure 213
Install WinZip (Part 7 of 10)

Step	Action
8	Set **Custom setup** options (if you chose **Express setup**, skip to step 9).
	If you want, clear unneeded configuration settings, as shown in the following window.  WinZip Setup **Explorer Configuration** Recommended setting for first-time users: check all boxes. Press the F1 key for details. ☑ Associate WinZip with archives ☑ Explorer shell extension ☑ Non-cascaded WinZip context menu items ☑ Display icons on context menus ☑ Enable Zip and E-Mail on context menus ☐ Include WinZip in Start menu ☐ Include WinZip on desktop

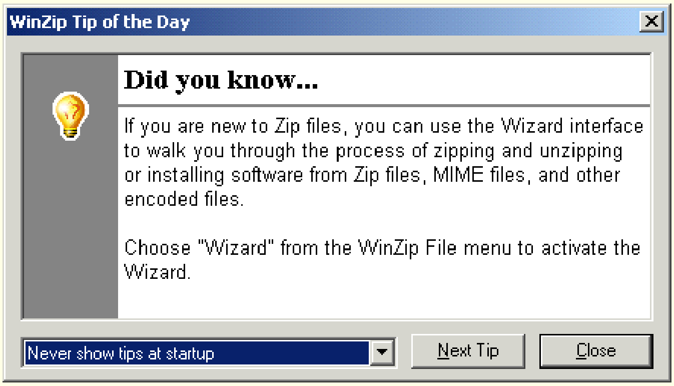
Procedure 213
Install WinZip (Part 8 of 10)

Step	Action
9	Choose whether you want a program group and icons.
	• If you so choose, clear the option to create a program group and icons. • Click **Next** to continue.  WinZip Setup **Other Options** Some WinZip features require optional external programs. You can configure these program locations now by clicking Program Locations, or wait until you need them and select "Configuration" from the "Options" pull-down menu and then click on the "Program Locations" tab. Program Locations... ☐ Create WinZip program group and icons ☐ Create icon for WinZip Self-Extractor Personal Edition

Procedure 213
Install WinZip (Part 9 of 10)

Step	Action
10	Acknowledge completion of the installation.
	Click **Finish** to complete the install procedure.  WinZip Setup **Thank you for installing this evaluation version.** For a list of new features in this release, please see the "Version History" section of the online help file or press the F1 key now. Click "Finish" to start WinZip.

Procedure 213
Install WinZip (Part 10 of 10)

Step	Action
11	Disable Tip of the Day (optional).
	The program is launched once installation is complete. If you want, disable the function that shows Tip of the Day at each start-up. Choose **Never show tips at startup** from the drop-down list, as shown in the following window, and click **Close**.  WinZip Tip of the Day Did you know... If you are new to Zip files, you can use the Wizard interface to walk you through the process of zipping and unzipping or installing software from Zip files, MIME files, and other encoded files. Choose "Wizard" from the WinZip File menu to activate the Wizard. Never show tips at startup

END

Install PC – Step 1d – TCP Monitor

This chapter provides information on copying TCP Monitor to the hard disk.

Install the TCP Monitor program if you want to troubleshoot eDMSAPI module. Installation of this program is optional, but highly recommended.

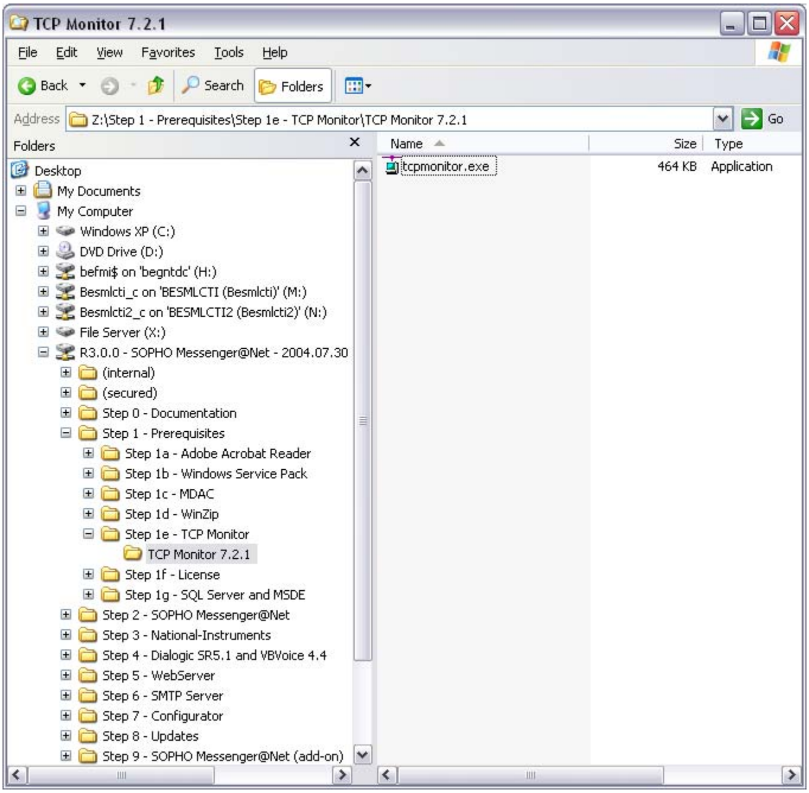
Copying TCP Monitor to the hard disk

> ***Note:*** If hard disk space is limited, you can run the program from the CD.

Copy the program from the CD-ROM image directory **/Step 1 – Prerequisites/Step 1e - TCP Monitor/** to the hard disk of the DECT Messenger PC. See Figure 373 on page 836.

By default, TCP Monitor is installed in **C:\Program Files\TCP Monitor**. See Figure 374 on page 837. You can install the software in any directory you choose.

Figure 373
Source directory

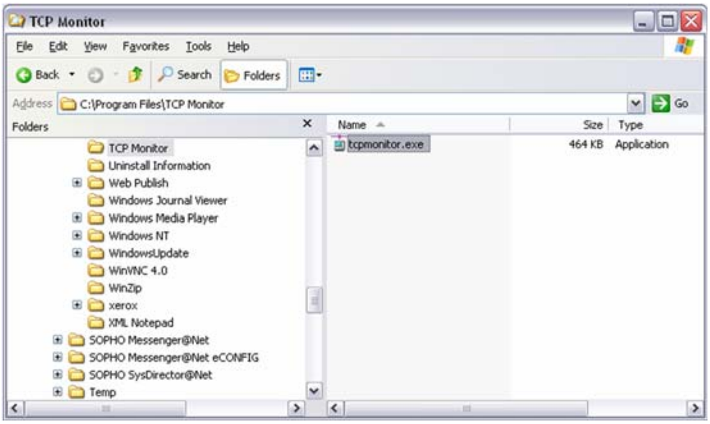


Address: Z:\Step 1 - Prerequisites\Step 1e - TCP Monitor\TCP Monitor 7.2.1

Name	Size	Type
tcpmonitor.exe	464 KB	Application

```
Desktop
  My Documents
  My Computer
    Windows XP (C:)
    DVD Drive (D:)
    befmi$ on 'begntdc' (H:)
    Besmlcti_c on 'BESMLCTI (Besmlcti)' (M:)
    Besmlcti2_c on 'BESMLCTI2 (Besmlcti2)' (N:)
    File Server (X:)
    R3.0.0 - SOPHO Messenger@Net - 2004.07.30
      (internal)
      (secured)
      Step 0 - Documentation
      Step 1 - Prerequisites
        Step 1a - Adobe Acrobat Reader
        Step 1b - Windows Service Pack
        Step 1c - MDAC
        Step 1d - WinZip
        Step 1e - TCP Monitor
          TCP Monitor 7.2.1
        Step 1f - License
        Step 1g - SQL Server and MSDE
      Step 2 - SOPHO Messenger@Net
      Step 3 - National-Instruments
      Step 4 - Dialogic SR5.1 and VBVoice 4.4
      Step 5 - WebServer
      Step 6 - SMTP Server
      Step 7 - Configurator
      Step 8 - Updates
      Step 9 - SOPHO Messenger@Net (add-on)
```

Figure 374
Destination directory



Name	Size	Type
tcpmonitor.exe	464 KB	Application

Install PC – Step 1e – Licence Manager

This chapter provides information on installing Nortel Licence Manager.

The Nortel Licence Manager is a required component. Check to ensure that you are installing the latest release of this software, and contact Nortel if required.

You need an appropriate licence key to install Nortel Licence Manager.

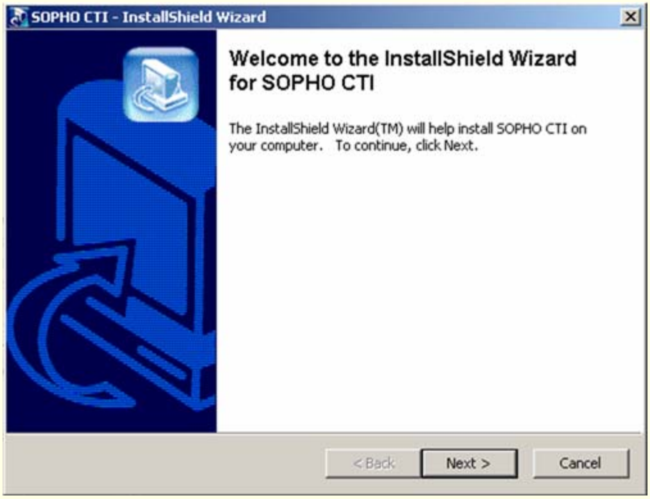
For your convenience a copy of the software is available on CD-ROM1 in the folder \Step 1f - Licence; for more information, see the readme.txt document located in the same directory.

Installing Nortel Licence Manager

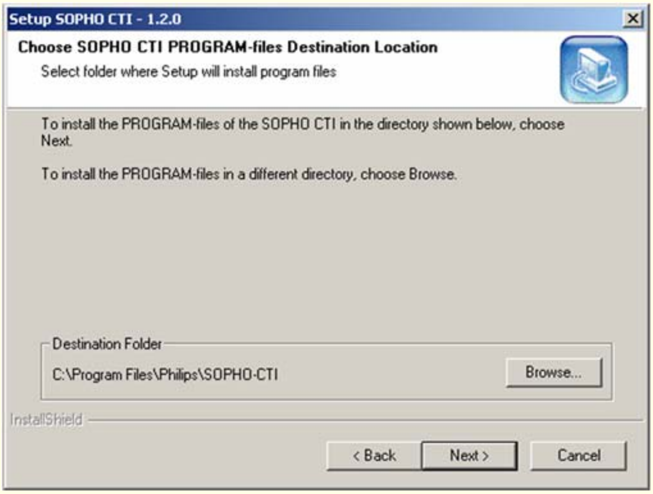
Procedure 214
Install Nortel Licence Manager (Part 1 of 4)

Step	Action
1	Start the Installation wizard.
	• Browse to the following folder on CD-ROM1: \Step 1f - Licence • Double-click the install application SOPHOCTI_1_2_0.exe.

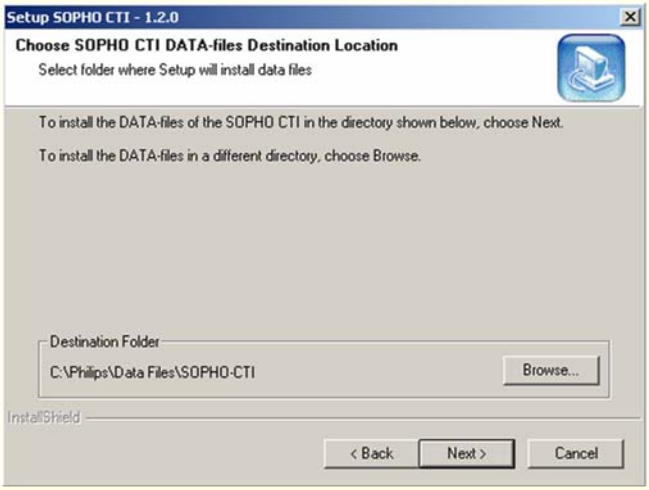
Procedure 214
Install Nortel Licence Manager (Part 2 of 4)

Step	Action
2	Begin the installation procedure.
	Click **Next** to begin the installation.  SOPHO CTI - InstallShield Wizard Welcome to the InstallShield Wizard for SOPHO CTI The InstallShield Wizard(TM) will help install SOPHO CTI on your computer. To continue, click Next.

Procedure 214
Install Nortel Licence Manager (Part 3 of 4)

Step	Action
3	Select the PROGRAM-files destination directory.
	Click **Next** to continue.  Setup SOPHO CTI - 1.2.0 **Choose SOPHO CTI PROGRAM-files Destination Location** Select folder where Setup will install program files To install the PROGRAM-files of the SOPHO CTI in the directory shown below, choose Next. To install the PROGRAM-files in a different directory, choose Browse. Destination Folder C:\Program Files\Philips\SOPHO-CTI

Procedure 214
Install Nortel Licence Manager (Part 4 of 4)

Step	Action
4	Select the DATA-files destination directory.
	Click **Next** to continue.  Setup SOPHO CTI - 1.2.0 **Choose SOPHO CTI DATA-files Destination Location** Select folder where Setup will install data files To install the DATA-files of the SOPHO CTI in the directory shown below, choose Next. To install the DATA-files in a different directory, choose Browse. Destination Folder C:\Philips\Data Files\SOPHO-CTI
5	Complete the installation.
	Click **Finish** to complete the installation procedure.
	END

Install PC – Step 1f – SQL Server

Nortel DECT Messenger currently supports three database engines for the Messenger_DATA database. Choose one of the following:

- "Microsoft Access 2000"
- "MSDE 2000 A"
- "Microsoft SQL Server 2000" on page 851

Microsoft Access 2000

The Microsoft Access 2000 database (Messenger_DATA.mdb) is installed automatically, so you can skip this chapter.

MSDE 2000 A

MSDE 2000 A (English) is shipped with DECT Messenger, in the directory Step 1 – Prerequisites > Step 1g - SQL Server and MSDE > 1. MSDE 2000 A.

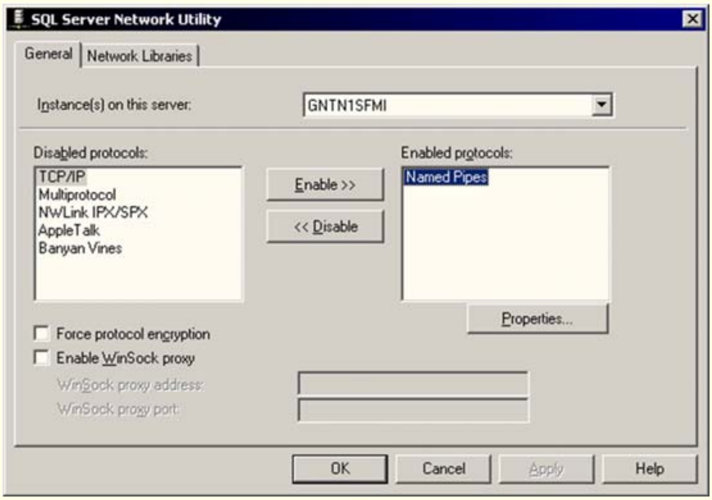
You must choose a password for the system administrator (username sa); the examples in this chapter use the password BEFMI@A31. This password is needed later to configure the DECT Messenger product, for example, when defining the ADO connection string for the Messenger_DATA database in the table eKERNEL_SITE.

Follow Procedure 215 if you plan to use the MSDE 2000 A.

Procedure 215
Setting up MSDE 2000 A (Part 1 of 6)

Step	Action
1	Open a command window.
	Click the **Start** button, and choose **Run > cmd**.
2	Change directory.
	Change the directory to the folder on the CD where the MSDE 2000 A setup is found. Enter the command as follows (substituting your CD-ROM drive letter instead of the example D): `cd “D:\Step 1 - Prerequisites\Step 1g - SQL Server and MSDE\1. MSDE 2000 A”`
3	Enter the setup command.
	Enter the setup command as follows (enter the password you prefer instead of the example **BEFMI@A31**): `setup SAPWD="BEFMI@A31" SECURITYMODE=SQL TARGETDIR="C:\Program Files\MSDE" /L*v C:/MSDELog.log` ***Note 1:*** If you plan to use the example password, you can skip this step, and instead, double-click the install.bat located on the CD-ROM folder \Step 1 – Prerequisites > Step 1g - SQL Server and MSDE > 1. MSDE 2000 A ***Note 2:*** If you experience problems, review the log file MSDELog.log that is created in the C:\ directory. Delete the log file after successful installation.
4	Wait while the install proceeds.
	A series of information windows is displayed while the installation proceeds. ***Note:*** The directories C:\Program Files\MSDEMSSQL and C:\Program Files\Microsoft SQL Server are created as part of the installation procedure.

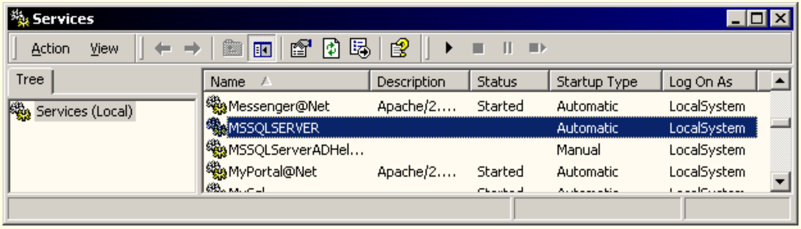
Procedure 215
Setting up MSDE 2000 A (Part 2 of 6)

Step	Action
5	Enable Named Pipes.
	- Start the program SVRNETCN.exe in directory C:\Program Files\Microsoft SQL Server\80\Tools\Binn and enable the protocol **Named Pipes** as shown:  SQL Server Network Utility Instance(s) on this server: GNTN1SFMI Disabled protocols: TCP/IP, Multiprotocol, NWLink IPX/SPX, AppleTalk, Banyan Vines Enabled protocols: Named Pipes □ Force protocol encryption □ Enable WinSock proxy WinSock proxy address: WinSock proxy port: General Network Libraries Enable >> << Disable Properties... OK Cancel Apply Help - Press **OK** and close the network utility.
6	Open the Services application.
	Click the **Start** button on the Windows taskbar and choose: **Settings > Control Panel > Administrative Tools > Services**.

Procedure 215
Setting up MSDE 2000 A (Part 3 of 6)

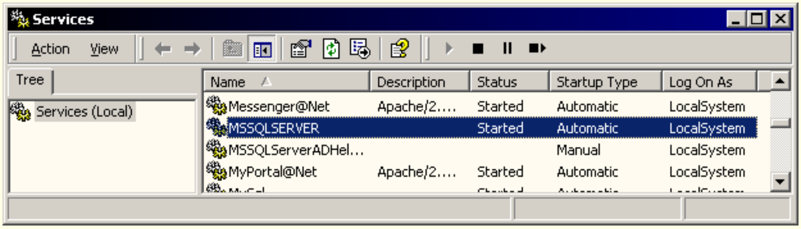
<table>
<tr><th>Step</th><th>Action</th></tr>
<tr><td>7</td><td>Start MSSQLSERVER.</td></tr>
<tr><td></td><td>

- Select **MSSQLSERVER** by left-clicking:



<table>
<tr><th>Name</th><th>Description</th><th>Status</th><th>Startup Type</th><th>Log On As</th></tr>
<tr><td>Messenger@Net</td><td>Apache/2....</td><td>Started</td><td>Automatic</td><td>LocalSystem</td></tr>
<tr><td>MSSQLSERVER</td><td></td><td></td><td>Automatic</td><td>LocalSystem</td></tr>
<tr><td>MSSQLServerADHel...</td><td></td><td></td><td>Manual</td><td>LocalSystem</td></tr>
<tr><td>MyPortal@Net</td><td>Apache/2....</td><td>Started</td><td>Automatic</td><td>LocalSystem</td></tr>
</table>

- Choose **Action > Start** in the menu. The Status column changes to read Started.



<table>
<tr><th>Name</th><th>Description</th><th>Status</th><th>Startup Type</th><th>Log On As</th></tr>
<tr><td>Messenger@Net</td><td>Apache/2....</td><td>Started</td><td>Automatic</td><td>LocalSystem</td></tr>
<tr><td>MSSQLSERVER</td><td></td><td>Started</td><td>Automatic</td><td>LocalSystem</td></tr>
<tr><td>MSSQLServerADHel...</td><td></td><td></td><td>Manual</td><td>LocalSystem</td></tr>
<tr><td>MyPortal@Net</td><td>Apache/2....</td><td>Started</td><td>Automatic</td><td>LocalSystem</td></tr>
</table>

</td></tr>
<tr><td>8</td><td>In the command window, change directory.</td></tr>
<tr><td></td><td>

Enter the command as follows:

```
cd C:\Program Files\Microsoft SQL Server\80\Tools\Binn
```

</td></tr>
</table>

Procedure 215
Setting up MSDE 2000 A (Part 4 of 6)

Step	Action
9	Check for your server in the server list.

Enter the following command to list the available SQL Servers and MSDE servers.

```
osql -L
```

Look for your (local) server in the list.

```
C:\Program Files\Microsoft SQL Server\80\Tools\Binn>osql -L

Servers:
     (local)
     BEBRXPROXY
     BEBRXTIVTMR
     GNTINDMES
     GNTINDPDL
     GNTINDPDL\NetSDK
     GNTINDPLC
     GNTN1SCCM
     GNTN1SCHP
     GNTN1SKDS
     IBSBI
     SRV1
```

Procedure 215
Setting up MSDE 2000 A (Part 5 of 6)

<table>
<tr><th>Step</th><th>Action</th></tr>
<tr><td>10</td><td>Verify that MSDE engine is running.</td></tr>
<tr><td></td><td>

- Enter the command **osql –U sa** and press the **Enter** key.
- Enter the password – for example **BEFMI@A31** – when prompted.
- Enter **select @@version** on line 1.
- Enter **go** on line 2.

The version is displayed, as shown in the following illustration:

```
C:\Program Files\Microsoft SQL Server\80\Tools\Binn>osql -U sa
Password:
1> select @@version
2> go



------------------------------------------------------------
------------------------------------------------------------
------------------------------------------------------------
Microsoft SQL Server  2000 - 8.00.760 (Intel X86)
        Dec 17 2002 14:22:05
        Copy
        right (c) 1988-2003 Microsoft Corporation
        Desktop Engine on Windows NT
        5.0 (Build 2195: Service Pack 4)


(1 row affected)
```

- Enter **quit** to exit the command-line utility.

</td></tr>
</table>

Procedure 215
Setting up MSDE 2000 A (Part 6 of 6)

Step	Action
11	Restore the Messenger_DATA database.

Perform either of the following:

- Double-click the install.bat file located in \Step 1 – Prerequisites\Step 1g - SQL Server and MSDE\3. Messenger_DATA. The install.bat processes the SQL script file Messenger_DATA.sql. If a previous version of Messenger_DATA exists, this replaces the existing file with a new one. The install.bat script prompts you for the password of the SQL Server when needed.
- Manually restore the database from the backup image available on the CD-ROM-image, by copying the file Messenger_DATA.backup from the directory \Step 1 – Prerequisites\Step 1g - SQL Server and MSDE\3. Messenger_DATA to the directory C:\SOPHO Messenger@Net\Sql\.

```
osql -S (local) -Q "RESTORE DATABASE Messenger_DATA FROM
DISK='D:\Step 1 - Prerequisites\Step 1g - SQL Server and MS-
DE\3. Messenger_DATA\ C:\SOPHO Messen-
ger@Net\Sql\Messenger_DATA.backup' WITH REPLACE" -U sa
Password: xxxxxxx (for example, BEFMI@A31)

Processed 248 pages for database 'Messenger_DATA', file
'Messenger_DATA' on
file 1.
Processed 1 pages for database 'Messenger_DATA', file
'Messenger_Log' on file
1.
RESTORE DATABASE successfully processed 249 pages in 0.665
seconds (3.058
MB/sec).

C:\Program Files\Microsoft SQL Server\80\Tools\Binn>
```

END

Transaction log maintenance

The transaction log file grows progressively larger over time, consuming system resources. You can reduce the amount of space the log requires by following the steps in Procedure 216.

Procedure 216
Reducing transaction log size (Part 1 of 2)

Step	Action
1	Clean up the transaction log.

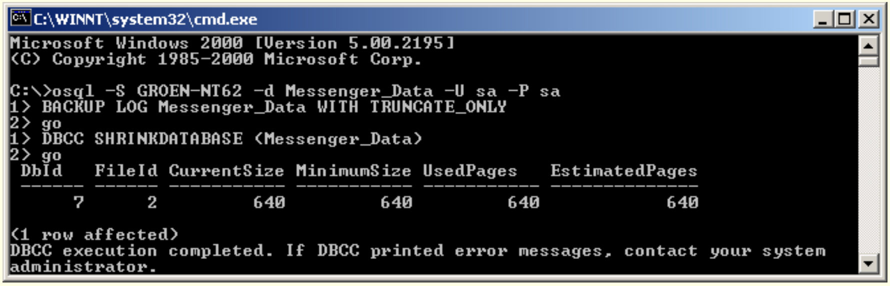
Open the osql command line utility as follows:

```
osql -S (local) -d Messenger_Data -U sa
```

- Enter **BACKUP LOG Messenger_Data WITH THRUNCATE_ONLY**.
- Enter **go**.
- Enter **DBCC SHRINKDATABASE (Messenger_Data)**.
- Enter **go**.
- Enter **exit**.

```
1>BACKUP LOG Messenger_Data WITH THRUNCATE_ONLY
2>go
1>DBCC SHRINKDATABASE (Messenger_Data)
2>go
3>exit
```

The output is displayed as follows:



```
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\>osql -S GROEN-NT62 -d Messenger_Data -U sa -P sa
1> BACKUP LOG Messenger_Data WITH TRUNCATE_ONLY
2> go
1> DBCC SHRINKDATABASE (Messenger_Data)
2> go
 DbId   FileId CurrentSize MinimumSize UsedPages   EstimatedPages
 ------ ------ ----------- ----------- ----------- --------------
      7      2         640         640         640            640

(1 row affected)
DBCC execution completed. If DBCC printed error messages, contact your system
administrator.
```

Procedure 216
Reducing transaction log size (Part 2 of 2)

Step	Action
2	Change database model to **simple** (to disable the transaction log).

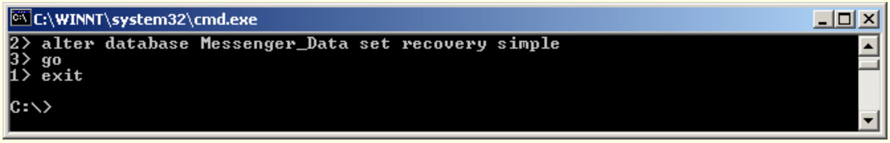
Open the osql command line utility.

```
Osql -S (local) -d Messenger_Data -U sa
```

- Enter **alter database Messenger_Data set recovery simple**.
- Enter **go**.
- Enter **exit**.

```
1>alter database Messenger_Data set recovery simple
2>go
3>exit
```

The output is displayed as follows:



```
2> alter database Messenger_Data set recovery simple
3> go
1> exit

C:\>
```

END

Microsoft SQL Server 2000

Before you start

Before you proceed with the installation of Microsoft SQL Server 2000, restore the SQL Server 2000 engine and install the Enterprise Manager utility as part of the SQL Server 2000 engine.

Nortel recommends that you install the latest SQL Server service pack prior to continuing. For your convenience, the software install package is provided on the CD-ROM in \Step 1 – Prerequisites > Step 1g - SQL Server and MSDE > 2. SQL Server 2000 > SQL Server SP3a. Refer to the Microsoft web site (www.microsoft.com) for more information on the SQL Server service pack.

Before you continue, acquire the following information:

- User ID, for example, sa.
- Password associated with that user ID, for example, sa.
- Service instance name, for example (local), GNTN1SFMI, and so on.

  Note: In many cases, there is one service instance only for SQL Server, such as (local) – and you can address this default instance by means of the "127.0.0.1;" reference.

Setting up Microsoft SQL Server 2000

Verify that SQL Server Enterprise Manager is available on either the SQL Server, or on a networked administration PC.

Procedure 217
Setting up Microsoft SQL Server 2000 (Part 1 of 9)

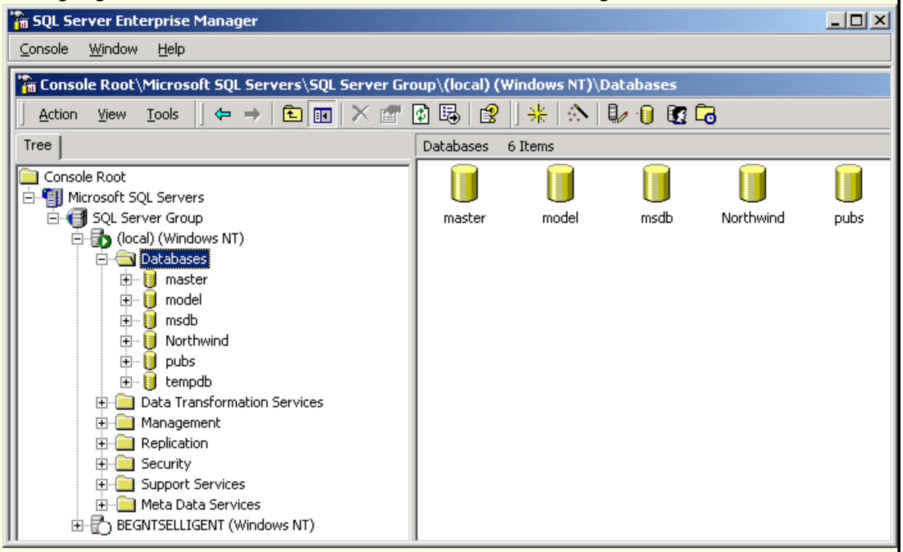
Step	Action
1	Start the SQL Server Enterprise Manager.
	Click **Start** and navigate to the SQL Server Enterprise Manager shortcut.
2	Add a server registration if you are working from an external platform (optional).
	If you are maintaining the SQL Server from an external platform, you can add a server registration by performing the following steps: • Highlight the **SQL Server Group**. • Right-click to open the pop-up menu. • Select the option **New SQL Server Registration**.

Procedure 217
Setting up Microsoft SQL Server 2000 (Part 2 of 9)

Step	Action
3	Create a new database.

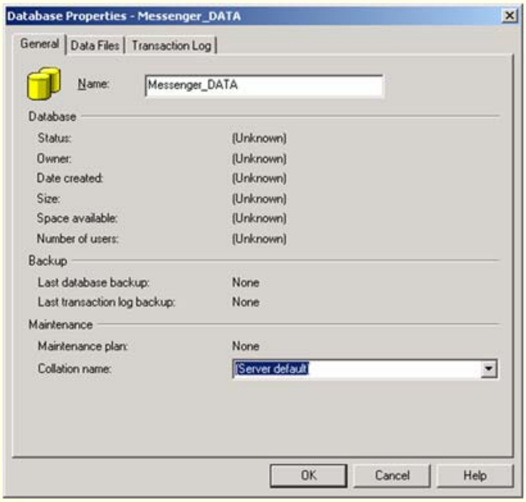
To create a new database, perform the following steps:

- Highlight the **Database** node as shown in the following illustration:

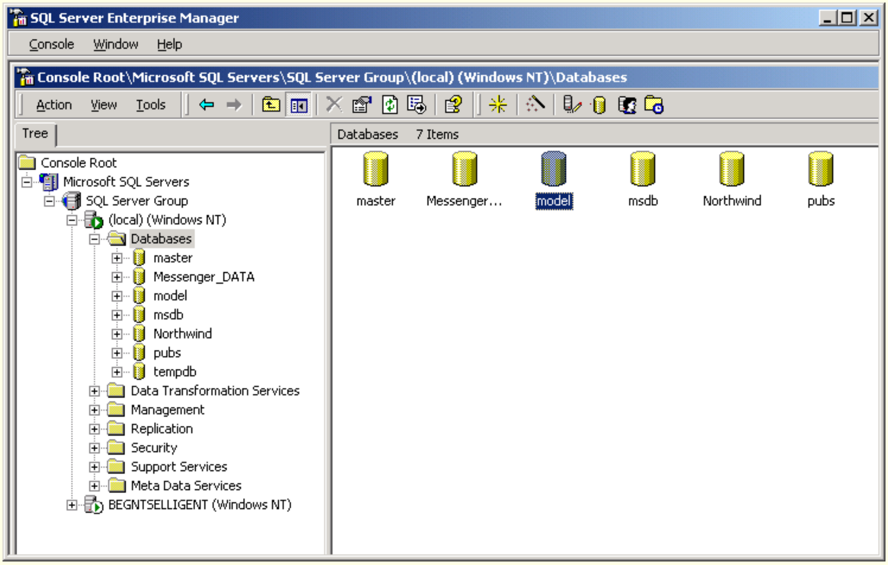


- Right-click to open the pop-up menu.
- Select **New database**.

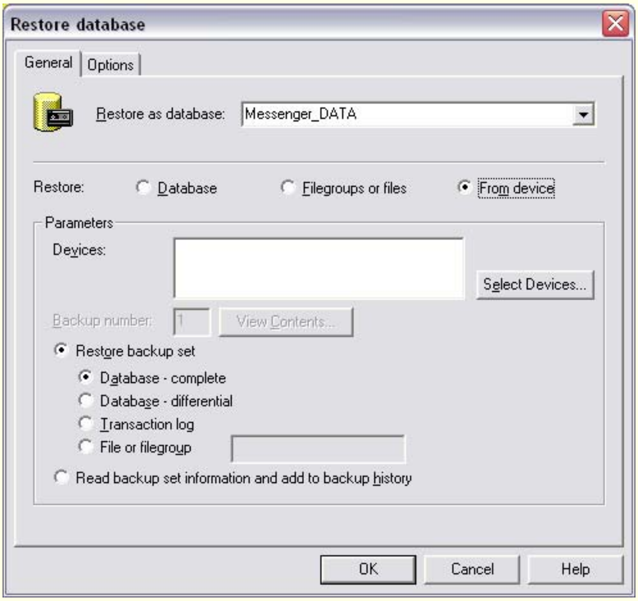
Procedure 217
Setting up Microsoft SQL Server 2000 (Part 3 of 9)

Step	Action
4	Enter the database name.
	Enter the database name **Messenger_DATA** as shown in the following illustration, and click **OK**.  Database Properties - Messenger_DATA Name: Messenger_DATA Database Status: (Unknown) Owner: (Unknown) Date created: (Unknown) Size: (Unknown) Space available: (Unknown) Number of users: (Unknown) Backup Last database backup: None Last transaction log backup: None Maintenance Maintenance plan: None Collation name: (Server default)

Procedure 217
Setting up Microsoft SQL Server 2000 (Part 4 of 9)

Step	Action
5	Restore database.
	To restore the database, perform the following steps: • Highlight the **Database** node, as shown in the following illustration:  • Right-click to open the pop-up menu. • Select the menu-option **All tasks > Restore database**.

Procedure 217
Setting up Microsoft SQL Server 2000 (Part 5 of 9)

Step	Action
6	Access the Choose Restore Device window.
	• Choose **From Device**. • Click **Select Devices**. 

Restore database

Restore as database: Messenger_DATA

Restore: ○ Database ○ Filegroups or files ● From device

Parameters

Devices:

Backup number: 1

● Restore backup set

● Database - complete

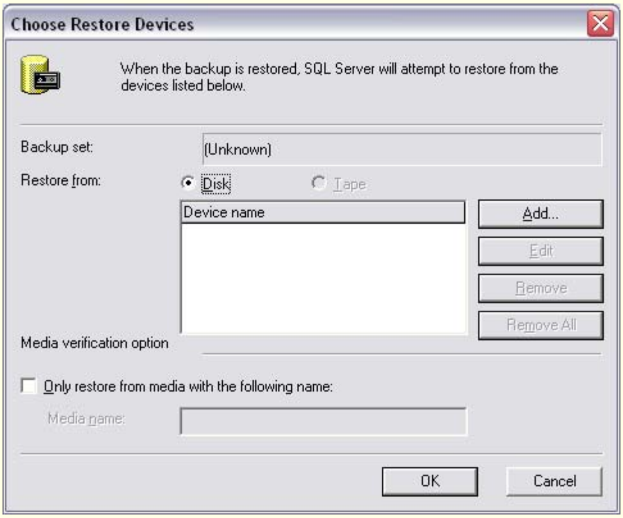
○ Database - differential

○ Transaction log

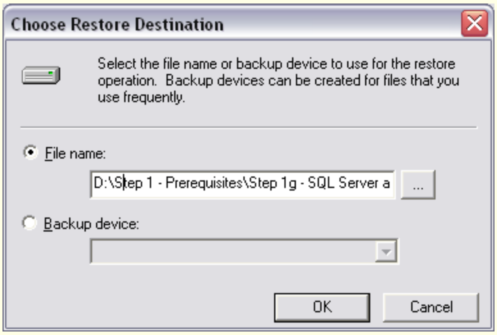
○ File or filegroup

○ Read backup set information and add to backup history

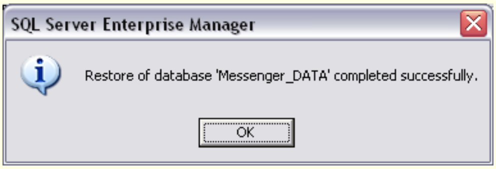
Procedure 217
Setting up Microsoft SQL Server 2000 (Part 6 of 9)

Step	Action
7	Add a restore path.
	Click the **Add** button.  Choose Restore Devices When the backup is restored, SQL Server will attempt to restore from the devices listed below. Backup set: (Unknown) Restore from: ● Disk ○ Tape Device name Media verification option □ Only restore from media with the following name: Media name:

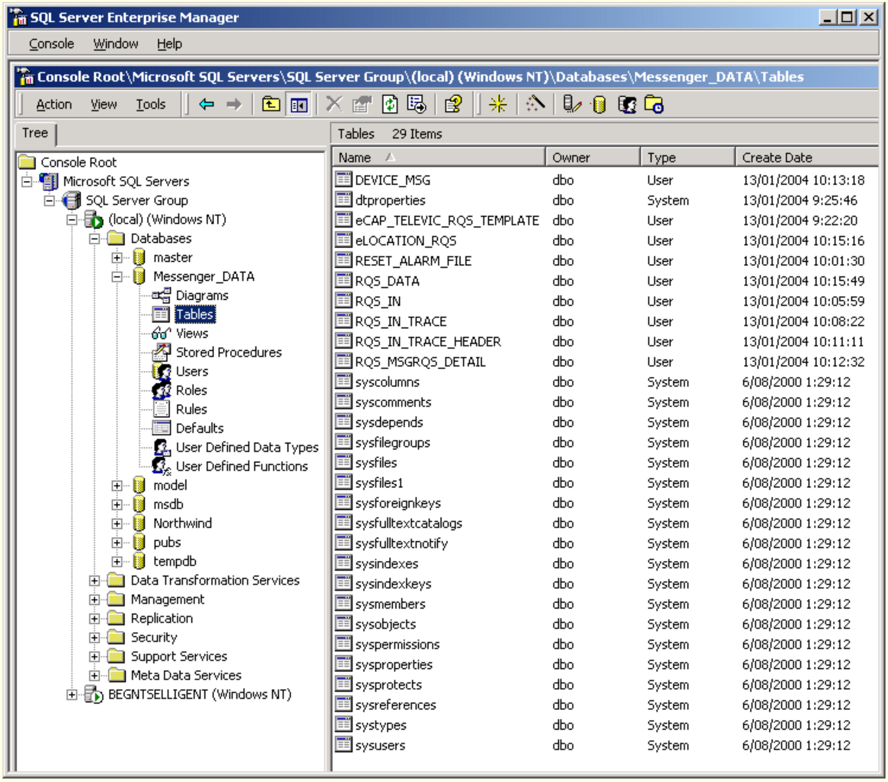
Procedure 217
Setting up Microsoft SQL Server 2000 (Part 7 of 9)

Step	Action
8	Set the path to the device from which you want to restore the database.
	• Click the **...** button to choose the restore location. • Navigate to \Step 1 – Prerequisites\Step 1g - SQL Server and MSDE\3. Messenger_DATA • Select the file Messenger_DATA.backup. • Choose **OK** and the database is restored. Choose Restore Destination Select the file name or backup device to use for the restore operation. Backup devices can be created for files that you use frequently. ● File name: D:\Step 1 - Prerequisites\Step 1g - SQL Server a ○ Backup device:

Procedure 217
Setting up Microsoft SQL Server 2000 (Part 8 of 9)

Step	Action
9	Acknowledge the completion of the database restore operation.
	Click **OK**.  SQL Server Enterprise Manager Restore of database 'Messenger_DATA' completed successfully.

Procedure 217
Setting up Microsoft SQL Server 2000 (Part 9 of 9)

Step	Action
10	Verify the restore procedure.
	As a result of the restore procedure, new entries appear in the Tables list of the Messenger_DATA database, as shown in the following illustration: 

SQL Server Enterprise Manager

Console Root\Microsoft SQL Servers\SQL Server Group\(local) (Windows NT)\Databases\Messenger_DATA\Tables

Tables 29 Items

Name	Owner	Type	Create Date
DEVICE_MSG	dbo	User	13/01/2004 10:13:18
dtproperties	dbo	System	13/01/2004 9:25:46
eCAP_TELEVIC_RQS_TEMPLATE	dbo	User	13/01/2004 9:22:20
eLOCATION_RQS	dbo	User	13/01/2004 10:15:16
RESET_ALARM_FILE	dbo	User	13/01/2004 10:01:30
RQS_DATA	dbo	User	13/01/2004 10:15:49
RQS_IN	dbo	User	13/01/2004 10:05:59
RQS_IN_TRACE	dbo	User	13/01/2004 10:08:22
RQS_IN_TRACE_HEADER	dbo	User	13/01/2004 10:11:11
RQS_MSGRQS_DETAIL	dbo	User	13/01/2004 10:12:32
syscolumns	dbo	System	6/08/2000 1:29:12
syscomments	dbo	System	6/08/2000 1:29:12
sysdepends	dbo	System	6/08/2000 1:29:12
sysfilegroups	dbo	System	6/08/2000 1:29:12
sysfiles	dbo	System	6/08/2000 1:29:12
sysfiles1	dbo	System	6/08/2000 1:29:12
sysforeignkeys	dbo	System	6/08/2000 1:29:12
sysfulltextcatalogs	dbo	System	6/08/2000 1:29:12
sysfulltextnotify	dbo	System	6/08/2000 1:29:12
sysindexes	dbo	System	6/08/2000 1:29:12
sysindexkeys	dbo	System	6/08/2000 1:29:12
sysmembers	dbo	System	6/08/2000 1:29:12
sysobjects	dbo	System	6/08/2000 1:29:12
syspermissions	dbo	System	6/08/2000 1:29:12
sysproperties	dbo	System	6/08/2000 1:29:12
sysprotects	dbo	System	6/08/2000 1:29:12
sysreferences	dbo	System	6/08/2000 1:29:12
systypes	dbo	System	6/08/2000 1:29:12
sysusers	dbo	System	6/08/2000 1:29:12

END

Transaction log maintenance

As the transaction log file grows, system resources are consumed. To correct this, follow the steps in Procedure 218.

Procedure 218
Reducing transaction log resource consumption (Part 1 of 2)

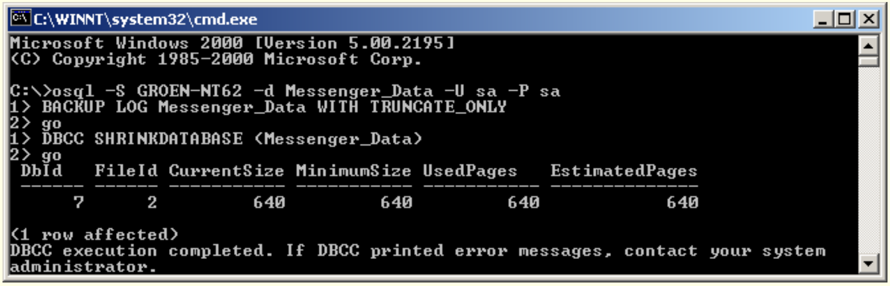
<table>
<tr><th>Step</th><th>Action</th></tr>
<tr><td></td><td></td></tr>
<tr><td>1</td><td>Clean up the transaction log.</td></tr>
<tr><td></td><td>
Open the osql command line utility.

```
osql -S (local) -d Messenger_Data -U sa
```

- Enter **BACKUP LOG Messenger_Data WITH THRUNCATE_ONLY**.
- Enter **go**.
- Enter **DBCC SHRINKDATABASE (Messenger_Data)**.
- Enter **go**.
- Enter **exit**.

```
3>BACKUP LOG Messenger_Data WITH THRUNCATE_ONLY
4>go
4>DBCC SHRINKDATABASE (Messenger_Data)
5>go
6>exit
```

The output is displayed as follows:



```
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\>osql -S GROEN-NT62 -d Messenger_Data -U sa -P sa
1> BACKUP LOG Messenger_Data WITH TRUNCATE_ONLY
2> go
1> DBCC SHRINKDATABASE (Messenger_Data)
2> go
 DbId   FileId CurrentSize MinimumSize UsedPages   EstimatedPages
 ------ ------ ----------- ----------- ----------- --------------
      7      2         640         640         640            640

(1 row affected)
DBCC execution completed. If DBCC printed error messages, contact your system
administrator.
```
</td></tr>
<tr><td></td><td></td></tr>
</table>

Procedure 218
Reducing transaction log resource consumption (Part 2 of 2)

Step	Action
2	Change database model to simple (no use of transaction log).

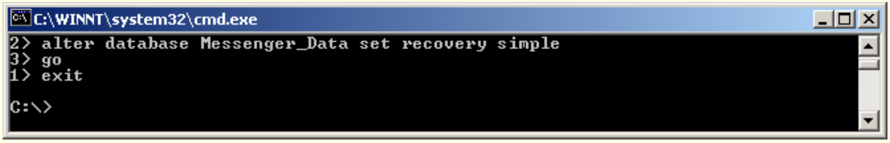
Open the osql command line utility

```
Osql -S (local) -d Messenger_Data -U sa
```

- Enter **alter database Messenger_Data set recovery simple**.
- Enter **go**.
- Enter **exit**.

```
4>alter database Messenger_Data set recovery simple
5>go
6>exit
```

The output is displayed as follows:



```
2> alter database Messenger_Data set recovery simple
3> go
1> exit

C:\>
```

END

Changing the database location

To adjust the location of the Messenger_DATA database repository, use the eCONFIG configuration tool, by defining a connection string for the Messenger_DATA database on site configuration level.

If DECT Messenger is not yet installed (“Installing the DECT Messenger” on page 873), you can perform this step later on. If DECT Messenger is already installed, you can alter the definition of the repository in the Messenger_CFG database, by editing the field CFG_Connectionstring_DATA_str in the table eKERNEL_SITE. If you prefer to work without eCONFIG, you can use eGRID module or another database maintenance tool to maintain this table.

The following shows sample configuration settings, indicating the database is located on server “127.0.0.1;”, and can be accessed with user sa and password sa, and uses the catalog Messenger_DATA.

Adjust these settings according to your environment.

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

When using eWEB_Advanced, configure the ODBC as well. If you change database engine of related configuration parameters, you must also alter the ODBC connections, as described in “Install PC – Step 4 – Web Server” on page 949.

Install PC – Step 1g – Secure Session

This chapter provides information on the following topics:

- "Installing Secure Session"
- "Configuring Secure Session" on page 869

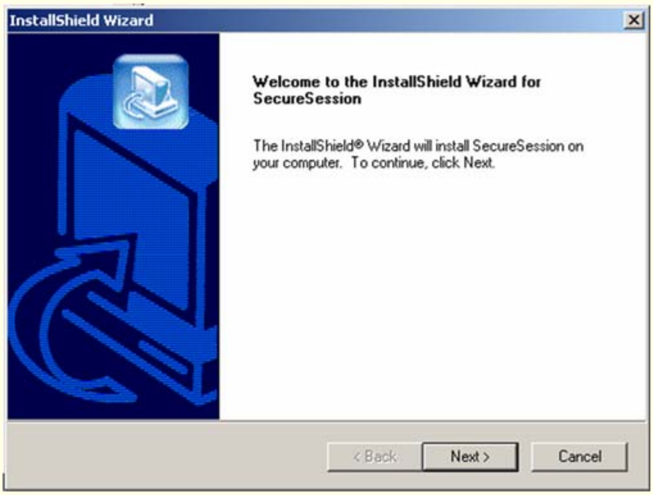
Secure Session is an application used to create a secure link between the DECT Messaging Server and the DECT system. Secure Session provides SNMP Authentication with the DMC card. Installation files are located on the CD-ROM1 in the directory \Step 1h\SNMP Secure Session.

Installing Secure Session

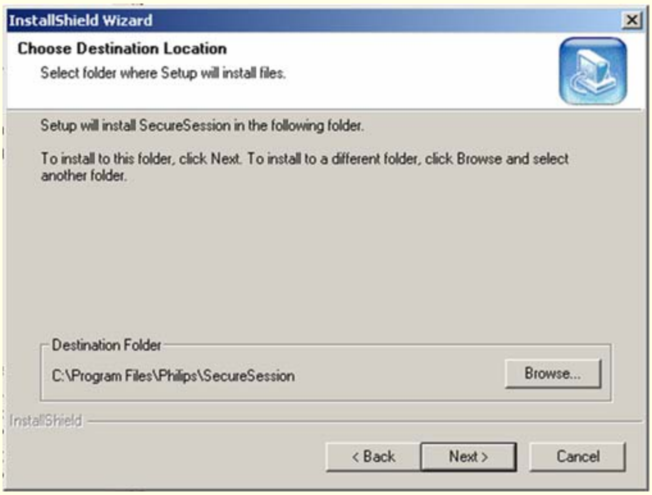
Procedure 219
Install Secure Session (Part 1 of 4)

Step	Action
1	Launch the Setup wizard.
	Launch the InstallShield Setup wizard: • Browse to the folder \Step 1h\SNMP Secure Session on the CD-ROM. • Double-click **Setup.exe**.

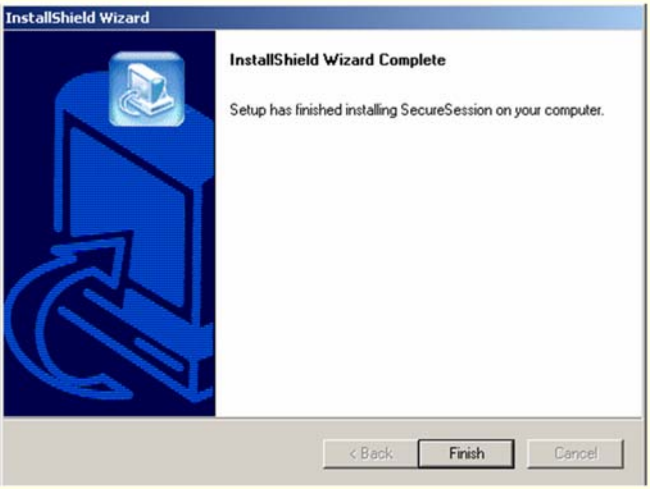
Procedure 219
Install Secure Session (Part 2 of 4)

Step	Action
2	Begin the installation.
	Click **Next** to continue.  **Welcome to the InstallShield Wizard for SecureSession** The InstallShield® Wizard will install SecureSession on your computer. To continue, click Next.

Procedure 219
Install Secure Session (Part 3 of 4)

Step	Action
3	Choose an installation folder.
	- Click **Browse** to select a folder, or use the default. - Click **Next** to continue.  InstallShield Wizard **Choose Destination Location** Select folder where Setup will install files. Setup will install SecureSession in the following folder. To install to this folder, click Next. To install to a different folder, click Browse and select another folder. Destination Folder C:\Program Files\Philips\SecureSession

Procedure 219
Install Secure Session (Part 4 of 4)

Step	Action
4	Acknowledge completion of the installation procedure.
	Click **Finish**.  **InstallShield Wizard Complete** Setup has finished installing SecureSession on your computer.

END

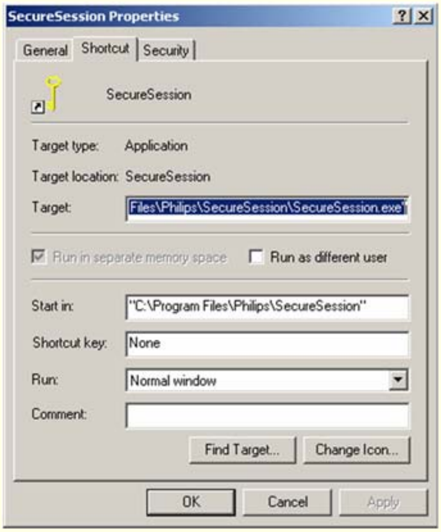
Configuring Secure Session

Once you complete the installation of Secure Session, follow the steps in Procedure 220 to configure Secure Session to work with your DECT system. This is performed by adding command line parameters to the Secure Session application shortcut.

Procedure 220
Configure Secure Session (Part 1 of 3)

Step	Action
1	Open the **Properties** window for the Secure Session shortcut.
	• Click the **Start** button on the Windows taskbar and choose **Programs > Secure Session**. • Right-click the **Secure Session** application. • Choose **Properties** from the pop-up menu.

Procedure 220
Configure Secure Session (Part 2 of 3)

Step	Action
2	Identify the Target field.
	Examine the **Properties** window to find the Target field, which contains the default string: C:\Program Files\Philips\SecureSession\SecureSession.exe  SecureSession Properties SecureSession Target type: Application Target location: SecureSession Target: Files\Philips\SecureSession\SecureSession.exe" ☑ Run in separate memory space □ Run as different user Start in: "C:\Program Files\Philips\SecureSession" Shortcut key: None Run: Normal window Comment: General Shortcut Security Find Target... Change Icon... OK Cancel Apply

Procedure 220
Configure Secure Session (Part 3 of 3)

Step	Action
3	Add parameters to the Target string.

Add the following parameters:

Parameter	Meaning	Example setting
/addr <addr>	IP address of the SNMP agent (DMC Relay Card)	192.124.48.2
/readcom <com>	The reading community	DAS_ro
/writecom <com>	The writing community	DAS_rw
/key <key>	The encryption key	Arsenal

Example:

```
C:\Program Files\Philips\SecureSession\SecureSession.exe /
addr 192.124.48.2 /readcom DAS_ro /writecom DAS_rw /
key Arsenal
```

Note 1: Remember to change the IP address to that of the DMC Relay card to which you want to connect your DECT Messenger.

Note 2: Ensure that you include all spaces shown in the example.

Step	Action
4	Save your changes.

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

END

Install PC – Step 2 – Nortel DECT Messenger

This chapter provides information on the following topics:

- "Installing the DECT Messenger" on page 873
- "Installing template shortcuts (optional procedure)" on page 883

Before you start

Before installing DECT Messenger, complete all the prerequisite actions that are described in "General – Install PC" on page 805.

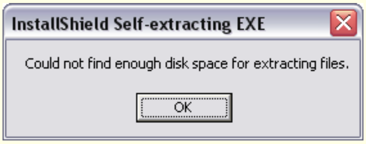
> ***Note:*** DECT Messenger and all associated modules require the Nortel Licence Manager to be installed, and require a valid licence key for the dongle to unlock the functionality. Refer to "Install PC – Step 1e – Licence Manager" on page 839 for the licence manager installation procedure, and for more information, check the readme.txt file in the same directory.

Installing the DECT Messenger

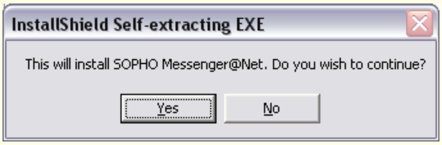
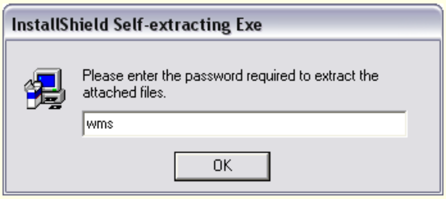
Installation files are located on the CD-ROM in directory **Step 2 - Nortel DECT Messenger**.

Note: The installation procedure is designed to install from a CD-ROM or DVD image or drive. This means the \Step 2 - Nortel DECT Messenger folder must reside in the root of the drive (usually drive D:). Installation from a subdirectory or a network drive is not supported, and can result in messages such as "Could not find enough disk space for extracting files." If you must install from a network resource, share the directory, and map the shared directory to a network drive, so the \Step 2 - Nortel DECT Messenger resides in the root of the shared network drive.

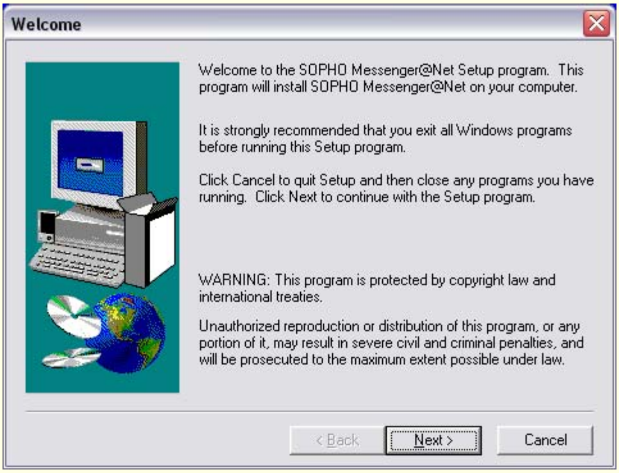
Procedure 221
Install Nortel DECT Messenger (Part 1 of 9)

Step	Action
1	Start the Setup Wizard.
	• Open the directory \Step 2 - Nortel DECT Messenger on the CD-ROM. • Double-click the file: Nortel DECT Messenger_R3.0.0_build_2004.06.27.exe. ***Note 1:*** The name of the .EXE files varies depending on the release version. The file name can include a release level and build data. If more than one copy of the program is located in the directory, install the most recent version, unless instructed otherwise. ***Note 2:*** If you are not installing from a CD-ROM, DVD image, or shared drive, the InstallShield sometimes detects a path name that is too long, and the following warning is shown. Refer to the Note at the top of this page for information on how to avoid this unsupported environment. You can ignore the warning when there is at least 500MB free space on drive C:  InstallShield Self-extracting EXE Could not find enough disk space for extracting files.

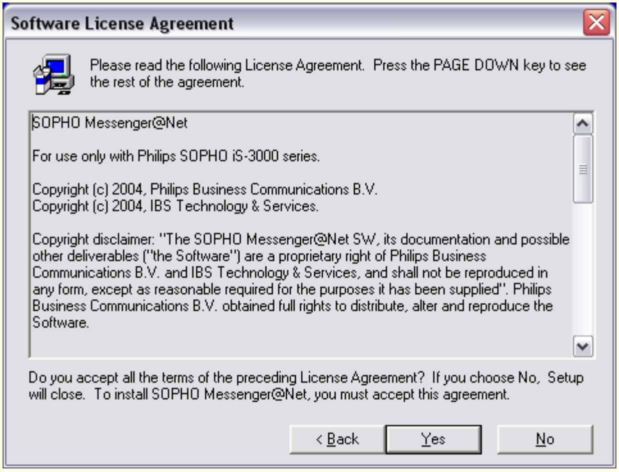
Procedure 221
Install Nortel DECT Messenger (Part 2 of 9)

Step	Action
2	Confirm that you wish to install Nortel DECT Messenger.
	Press **Yes** to continue.  InstallShield Self-extracting EXE This will install SOPHO Messenger@Net. Do you wish to continue?
3	Enter the password to unlock the installer.
	Enter wms.  InstallShield Self-extracting Exe Please enter the password required to extract the attached files. wms ***Note:*** The password is case-sensitive (the default password is entirely in lowercase).

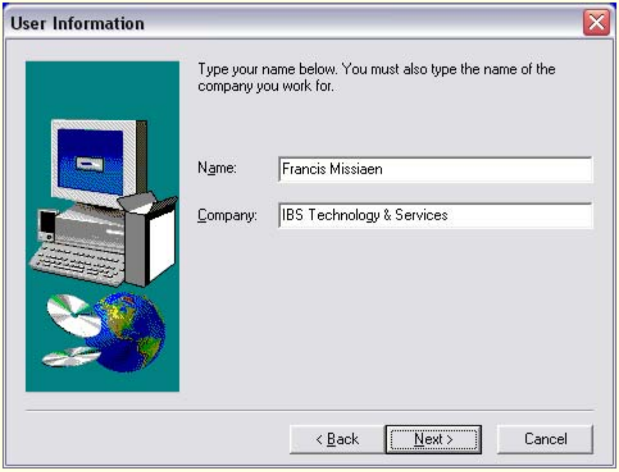
Procedure 221
Install Nortel DECT Messenger (Part 3 of 9)

Step	Action
4	Read the warnings, and begin the installation.
	An **InstallShield** progress bar is displayed, followed by a **Welcome** window. Click **Next** to continue.  Welcome Welcome to the SOPHO Messenger@Net Setup program. This program will install SOPHO Messenger@Net on your computer. It is strongly recommended that you exit all Windows programs before running this Setup program. Click Cancel to quit Setup and then close any programs you have running. Click Next to continue with the Setup program. WARNING: This program is protected by copyright law and international treaties. Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under law.

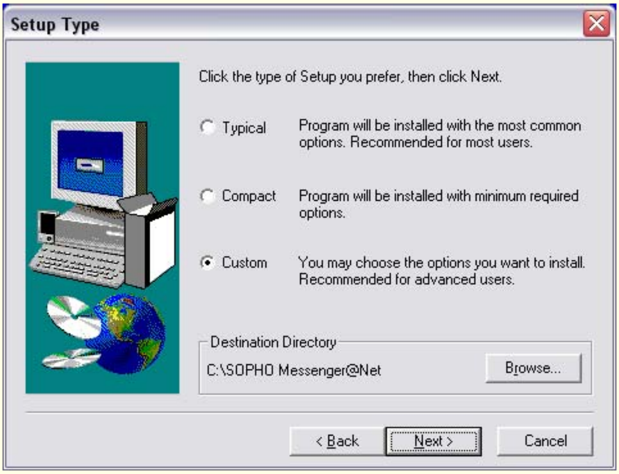
Procedure 221
Install Nortel DECT Messenger (Part 4 of 9)

Step	Action
5	Accept the Software Licence Agreement.
	The Software Licence Agreement window is shown. Click **Yes** to accept the terms. If you do not want to accept the Licence Agreement, click **No** to cancel installation.  Please read the following License Agreement. Press the PAGE DOWN key to see the rest of the agreement. SOPHO Messenger@Net For use only with Philips SOPHO iS-3000 series. Copyright (c) 2004, Philips Business Communications B.V. Copyright (c) 2004, IBS Technology & Services. Copyright disclaimer: "The SOPHO Messenger@Net SW, its documentation and possible other deliverables ("the Software") are a proprietary right of Philips Business Communications B.V. and IBS Technology & Services, and shall not be reproduced in any form, except as reasonable required for the purposes it has been supplied". Philips Business Communications B.V. obtained full rights to distribute, alter and reproduce the Software. Do you accept all the terms of the preceding License Agreement? If you choose No, Setup will close. To install SOPHO Messenger@Net, you must accept this agreement.

Procedure 221
Install Nortel DECT Messenger (Part 5 of 9)

Step	Action
6	Verify the user information.
	Verify the user information and press **Next** to continue.  User Information Type your name below. You must also type the name of the company you work for. Name: Francis Missiaen Company: IBS Technology & Services

Procedure 221
Install Nortel DECT Messenger (Part 6 of 9)

Step	Action
7	Select **Setup Type**.
	On the **Setup Type** window, select one of: **Typical**, **Compact** or **Custom** setup. Nortel recommends **Custom**. Do not alter the destination directory. Installing in a location other than the default C:\Nortel DECT Messenger is technically possible, but is not supported or documented.  Setup Type Click the type of Setup you prefer, then click Next. ○ Typical — Program will be installed with the most common options. Recommended for most users. ○ Compact — Program will be installed with minimum required options. ● Custom — You may choose the options you want to install. Recommended for advanced users. Destination Directory: C:\SOPHO Messenger@Net

Procedure 221
Install Nortel DECT Messenger (Part 7 of 9)

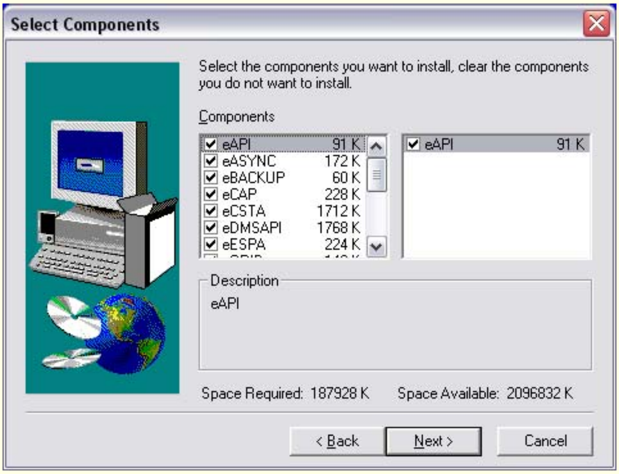
Step	Action
8	Review component choices (optional).

If you chose **Custom** Setup, you can select the components you want to install. Most modules consist of one part only (for example, eAPI, eASYNC, eDMSAPI, eCAP, eESPA, eGRID, eIO, eSMTP, eSMTP_server, and so on), and are either installed or not installed. Other modules (for example, eKERNEL, eWEB, and so on), consist of multiple parts.

Note: The ability to choose not to install some parts of eKERNEL, and eWEB, does not imply that you can skip any of these parts. In most cases, the decision to define different parts of a module is related to the fact that the components are installed in a different target location. Nortel recommends that you not omit any part of a module, because that can limit the functionality of DECT Messenger.

If you chose the **Typical** all available components are installed: eAPI, eASYNC, eCAP, eDMSAPI, eESPA, eGRID, eIO, eKERNEL, eSMTP, eSMTP_server, eWEB, and eTM_HA.

If you chose the **Compact** setup type, the following components are installed: eBACKUP, eCAP, eDMSAPI, eGRID, eKERNEL, and eTM.



Select Components

Select the components you want to install, clear the components you do not want to install.

Components

☑	eAPI	91 K
☑	eASYNC	172 K
☑	eBACKUP	60 K
☑	eCAP	228 K
☑	eCSTA	1712 K
☑	eDMSAPI	1768 K
☑	eESPA	224 K

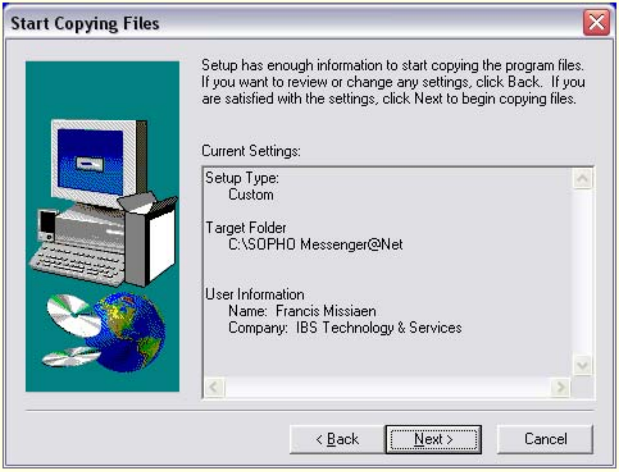
☑	eAPI	91 K

Description
eAPI

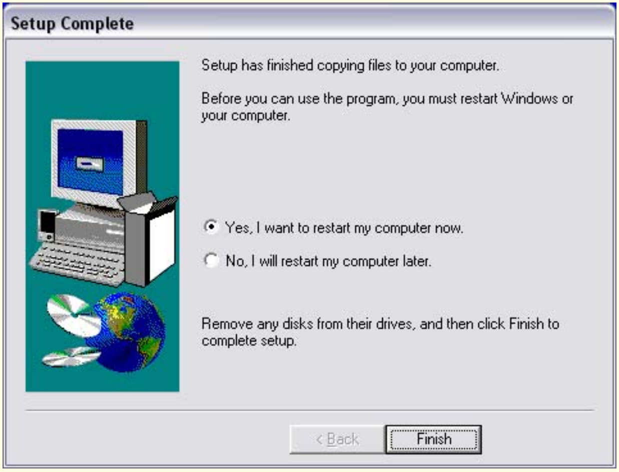
Space Required: 187928 K Space Available: 2096832 K

Click **Next** to continue.

Procedure 221
Install Nortel DECT Messenger (Part 8 of 9)

Step	Action
9	Confirm your choices, and begin copying files.
	Review the Current Settings, and click **Next** to initiate the installation procedure.  Start Copying Files Setup has enough information to start copying the program files. If you want to review or change any settings, click Back. If you are satisfied with the settings, click Next to begin copying files. Current Settings: Setup Type: Custom Target Folder C:\SOPHO Messenger@Net User Information Name: Francis Missiaen Company: IBS Technology & Services

Procedure 221
Install Nortel DECT Messenger (Part 9 of 9)

Step	Action
10	Restart the computer.
	- When installation is complete, the message in the following illustration is shown:  Setup Complete Setup has finished copying files to your computer. Before you can use the program, you must restart Windows or your computer. ● Yes, I want to restart my computer now. ○ No, I will restart my computer later. Remove any disks from their drives, and then click Finish to complete setup. Follow the instructions to restart the computer.

END

Additional configuration

Once you complete all the steps in Procedure 221 on page 874, DECT Messenger is installed. However, there are other steps that you must complete before you use the product. Return to “General – Install PC” on page 805, and complete the remaining steps. For example, additional components must be installed if you plan to use eIO, SMTP_Server, eWEB, and so on.

As a result of the installation procedure described in this document, a directory C:\SOPHO Messenger@Net is created, with a number of subdirectories and files. Additionally, some run-time files, such as OCX and DLL files, are installed and registered.

Note: Nortel recommends that you use eCONFIG as your configuration tool. Configure eTM to start automatically when the PC boots up, which subsequently launches the different modules. Return to “General – Install PC” on page 805, for instructions on setting up eCONFIG and eTM.

The following information is provided for reference, and for backwards compatibility with older systems that run without eCONFIG and eTM.

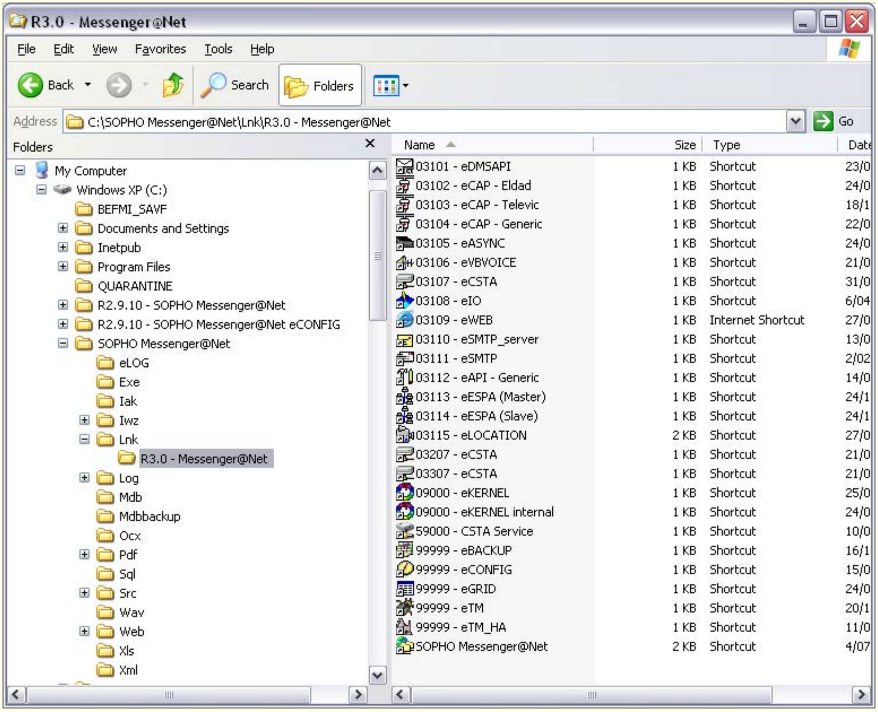
Installing template shortcuts (optional procedure)

To assist in the configuration process, a number of templates are shipped with DECT Messenger, providing database configuration and shortcuts for sample configurations. To install shortcuts to these templates, follow the steps in Procedure 222 on page 884.

Procedure 222
Installing shortcuts to templates (Part 1 of 2)

Step	Action
1	Locate the source and destinations folders.

- Open Windows Explorer.
- Locate the source files in C:\Nortel DECT Messenger\Lnk\, as shown:



C:\SOPHO Messenger@Net\Lnk\R3.0 - Messenger@Net

- My Computer
  - Windows XP (C:)
    - BEFMI_SAVF
    - Documents and Settings
    - Inetpub
    - Program Files
    - QUARANTINE
    - R2.9.10 - SOPHO Messenger@Net
    - R2.9.10 - SOPHO Messenger@Net eCONFIG
    - SOPHO Messenger@Net
      - eLOG
      - Exe
      - Iak
      - Iwz
      - Lnk
        - R3.0 - Messenger@Net
      - Log
      - Mdb
      - Mdbbackup
      - Ocx
      - Pdf
      - Sql
      - Src
      - Wav
      - Web
      - Xls
      - Xml

Name	Size	Type	Date
03101 - eDMSAPI	1 KB	Shortcut	23/0
03102 - eCAP - Eldad	1 KB	Shortcut	24/0
03103 - eCAP - Televic	1 KB	Shortcut	18/1
03104 - eCAP - Generic	1 KB	Shortcut	22/0
03105 - eASYNC	1 KB	Shortcut	24/0
03106 - eVBVOICE	1 KB	Shortcut	21/0
03107 - eCSTA	1 KB	Shortcut	31/0
03108 - eIO	1 KB	Shortcut	6/04
03109 - eWEB	1 KB	Internet Shortcut	27/0
03110 - eSMTP_server	1 KB	Shortcut	13/0
03111 - eSMTP	1 KB	Shortcut	2/02
03112 - eAPI - Generic	1 KB	Shortcut	14/0
03113 - eESPA (Master)	1 KB	Shortcut	24/1
03114 - eESPA (Slave)	1 KB	Shortcut	24/1
03115 - eLOCATION	2 KB	Shortcut	27/0
03207 - eCSTA	1 KB	Shortcut	21/0
03307 - eCSTA	1 KB	Shortcut	21/0
09000 - eKERNEL	1 KB	Shortcut	25/0
09000 - eKERNEL internal	1 KB	Shortcut	24/0
59000 - CSTA Service	1 KB	Shortcut	10/0
99999 - eBACKUP	1 KB	Shortcut	16/1
99999 - eCONFIG	1 KB	Shortcut	15/0
99999 - eGRID	1 KB	Shortcut	24/0
99999 - eTM	1 KB	Shortcut	20/1
99999 - eTM_HA	1 KB	Shortcut	11/0
SOPHO Messenger@Net	2 KB	Shortcut	4/07

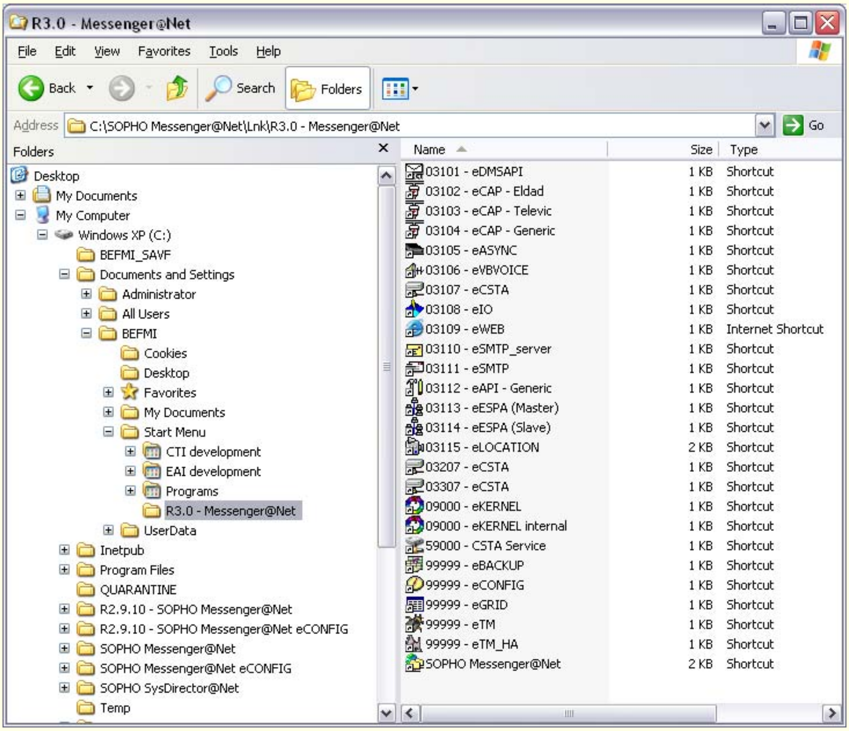
- Use Windows Explorer to locate the All Users \ Startup folder; this is the destination folder. An example of a valid destination folder is C:\Documents and Settings\All Users\Start Menu\Programs\Startup\.

Procedure 222
Installing shortcuts to templates (Part 2 of 2)

Step	Action
2	Copy the files.

- Drag the contents of sub-directory C:\Nortel DECT Messenger\Lnk\ to the Startup group of All Users.

This results in a number of sample shortcuts being created in the **Start** menu, as shown:



Address: C:\SOPHO Messenger@Net\Lnk\R3.0 - Messenger@Net

Name	Size	Type
03101 - eDMSAPI	1 KB	Shortcut
03102 - eCAP - Eldad	1 KB	Shortcut
03103 - eCAP - Televic	1 KB	Shortcut
03104 - eCAP - Generic	1 KB	Shortcut
03105 - eASYNC	1 KB	Shortcut
03106 - eVBVOICE	1 KB	Shortcut
03107 - eCSTA	1 KB	Shortcut
03108 - eIO	1 KB	Shortcut
03109 - eWEB	1 KB	Internet Shortcut
03110 - eSMTP_server	1 KB	Shortcut
03111 - eSMTP	1 KB	Shortcut
03112 - eAPI - Generic	1 KB	Shortcut
03113 - eESPA (Master)	1 KB	Shortcut
03114 - eESPA (Slave)	1 KB	Shortcut
03115 - eLOCATION	2 KB	Shortcut
03207 - eCSTA	1 KB	Shortcut
03307 - eCSTA	1 KB	Shortcut
09000 - eKERNEL	1 KB	Shortcut
09000 - eKERNEL internal	1 KB	Shortcut
59000 - CSTA Service	1 KB	Shortcut
99999 - eBACKUP	1 KB	Shortcut
99999 - eCONFIG	1 KB	Shortcut
99999 - eGRID	1 KB	Shortcut
99999 - eTM	1 KB	Shortcut
99999 - eTM_HA	1 KB	Shortcut
SOPHO Messenger@Net	2 KB	Shortcut

END

Refer to the documentation of each module later in this document for more information on building shortcuts.

For your reference, a number of sample shortcuts are shown in the following illustration. The shortcuts refer to a sample environment with one site, and all modules running on one single local PC. There are 3 eCAP modules, 1 eIO module, 1 eWEB module, one eSMTP_server module, three eDMSAPI module, one eGRID module, 1 eKERNEL module and 1 eBACKUP module:

```
"C:\Nortel DECT Messenger\Exe\eCAP.exe" /Site:1 /eKernel
port:3102 /eKernel address:*LOCAL /Log drive:C

"C:\Nortel DECT Messenger\Exe\eCAP.exe" /Site:1 /eKernel
port:3103 /eKernel address:*LOCAL /Log drive:C

"C:\Nortel DECT Messenger\Exe\eCAP.exe" /Site:1 /eKernel
port:3104 /eKernel address:*LOCAL /Log drive:C

"C:\Nortel DECT Messenger\Exe\eIO.exe" /Site:1 /eKernel
address:*LOCAL /eKernel port:3106 /Log drive:C

http://127.0.0.1/eWeb_index.php

"C:\Nortel DECT Messenger\Exe\eSMTP_server.exe" /Site:1
eKernel address:*LOCAL /eKernel port:3110 /Log drive:C

"C:\Nortel DECT Messenger\Exe\eDMSAPI.exe" /Site:1 /eKer
port:3111 /eKernel address:*LOCAL /DMS-API port:2010 /
DMS-API address:*LOCAL /Log drive:C

"C:\Nortel DECT Messenger\Exe\eASYNC.exe" /Site:1 /eKern
address:*LOCAL /eKernel port:3112 /Log drive:C

"C:\SOPHO Messenger@Net\Exe\eSMTP.exe" /Site:1 /eKernel
address:*LOCAL /eKernel port:3113/Log drive:C

"C:\SOPHO Messenger@Net\Exe\eKERNEL.exe" /Site:1

"C:\SOPHO Messenger@Net\Exe\eBACKUP.exe" /Path:C:\SOPHO
Messenger@Net /Log drive:C /Site:1 /Batch:N

"C:\SOPHO Messenger@Net\Exe\eGRID.exe" /Path:C:\SOPHO
Messenger@Net /Log drive:C
```

Refer to “Module – eTM” on page 1205 for more information on the Task Manager module. Use this module, in conjunction with the eCONFIG or eGrid module, to automatically configure shortcuts and to automatically start and monitor all processes.

IMPORTANT!

Ensure the eGRID module is not made available for unauthorized access. Remove the shortcut where applicable.

The eGRID module provides direct access to the tables in the database. There is no password protection on this module.

Return to “General – Install PC” on page 805 to continue.

IMPORTANT!

If you need to reinstall DECT Messenger for any reason, refer to “Install PC – Reinstalling Nortel DECT Messenger” on page 1045.

Install PC – Step 3 – National Instruments

This chapter provides information on the following topics:

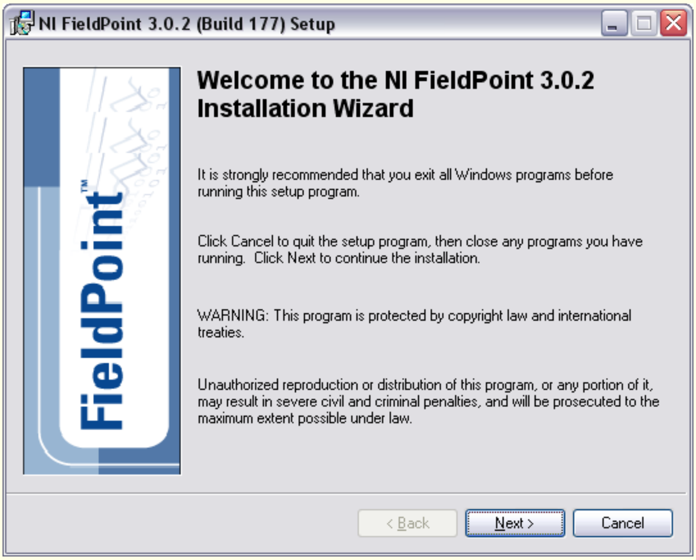
This chapter describes the installation procedure of modules that are related to the eIO component of Nortel DECT Messenger. You can skip this chapter if you plan not to use the eIO module.

> ***Note:*** This release of DECT Messenger provides the latest versions available for FieldPoint Software Firmware and OPC Server. If you are upgrading an existing configuration, Nortel recommends first removing the previous versions.

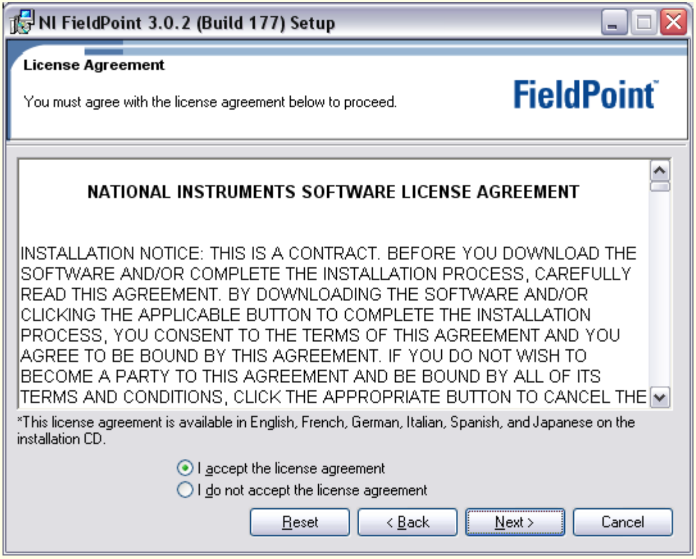
Installing the FieldPoint Explorer software

The FieldPoint Explorer is a program provided by National Instruments, which is required to detect and configure the connected distributed I/O modules.

Procedure 223
FieldPoint Explorer Software 3.0.2 (Build 177) (Part 1 of 9)

Step	Action
1	Launch the Autorun.exe.
	The software is located in the CD-ROM directory Step 3 - National-Instruments\Step 3a - FieldPoint Explorer 3.0.2 (Build 177)\nifp302\. Double-click the Autorun.exe file to start installing.
2	Review the Welcome message, and continue with the installation.
	Click **Next** to continue.  **Welcome to the NI FieldPoint 3.0.2 Installation Wizard** It is strongly recommended that you exit all Windows programs before running this setup program. Click Cancel to quit the setup program, then close any programs you have running. Click Next to continue the installation. WARNING: This program is protected by copyright law and international treaties. Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under law.

Procedure 223
FieldPoint Explorer Software 3.0.2 (Build 177) (Part 2 of 9)

Step	Action
3	Accept the Licence Agreement.
	Read the Licence Agreement and click **Next** to continue. 

NI FieldPoint 3.0.2 (Build 177) Setup

License Agreement

You must agree with the license agreement below to proceed.

FieldPoint

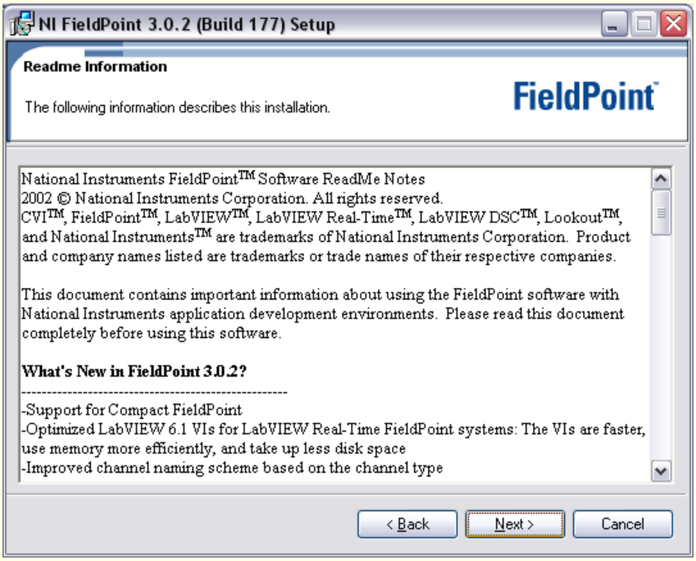
NATIONAL INSTRUMENTS SOFTWARE LICENSE AGREEMENT

INSTALLATION NOTICE: THIS IS A CONTRACT. BEFORE YOU DOWNLOAD THE SOFTWARE AND/OR COMPLETE THE INSTALLATION PROCESS, CAREFULLY READ THIS AGREEMENT. BY DOWNLOADING THE SOFTWARE AND/OR CLICKING THE APPLICABLE BUTTON TO COMPLETE THE INSTALLATION PROCESS, YOU CONSENT TO THE TERMS OF THIS AGREEMENT AND YOU AGREE TO BE BOUND BY THIS AGREEMENT. IF YOU DO NOT WISH TO BECOME A PARTY TO THIS AGREEMENT AND BE BOUND BY ALL OF ITS TERMS AND CONDITIONS, CLICK THE APPROPRIATE BUTTON TO CANCEL THE

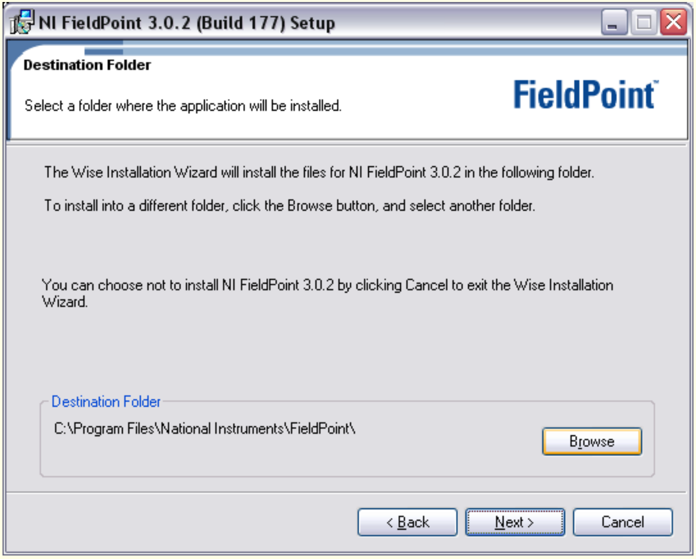
*This license agreement is available in English, French, German, Italian, Spanish, and Japanese on the installation CD.

● I accept the license agreement
○ I do not accept the license agreement

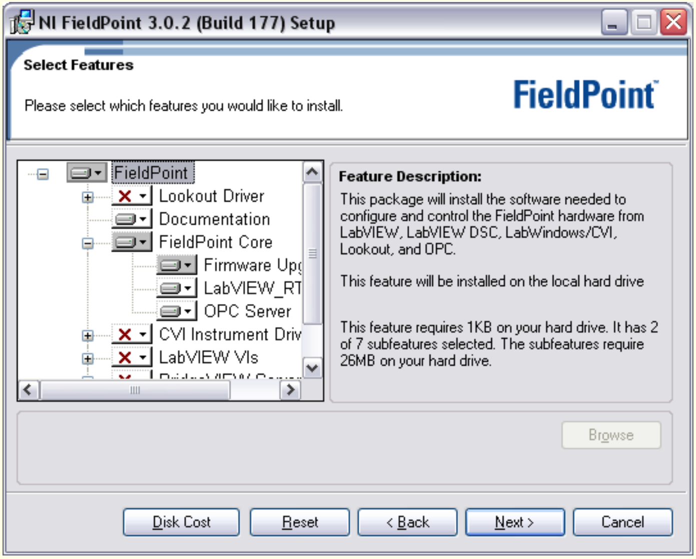
Procedure 223
FieldPoint Explorer Software 3.0.2 (Build 177) (Part 3 of 9)

Step	Action
4	Review the Information provided, and continue with the installation.
	Click **Next** to continue.  NI FieldPoint 3.0.2 (Build 177) Setup **Readme Information** The following information describes this installation. National Instruments FieldPoint™ Software ReadMe Notes 2002 © National Instruments Corporation. All rights reserved. CVI™, FieldPoint™, LabVIEW™, LabVIEW Real-Time™, LabVIEW DSC™, Lookout™, and National Instruments™ are trademarks of National Instruments Corporation. Product and company names listed are trademarks or trade names of their respective companies. This document contains important information about using the FieldPoint software with National Instruments application development environments. Please read this document completely before using this software. **What's New in FieldPoint 3.0.2?** -- -Support for Compact FieldPoint -Optimized LabVIEW 6.1 VIs for LabVIEW Real-Time FieldPoint systems: The VIs are faster, use memory more efficiently, and take up less disk space -Improved channel naming scheme based on the channel type

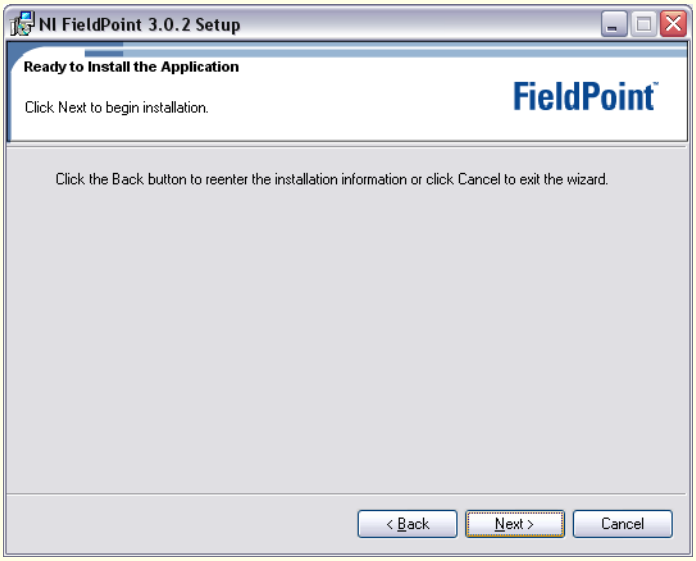
Procedure 223
FieldPoint Explorer Software 3.0.2 (Build 177) (Part 4 of 9)

Step	Action
5	Select the install location.
	Click **Next** to accept the default settings and continue with the installation.  NI FieldPoint 3.0.2 (Build 177) Setup **Destination Folder** Select a folder where the application will be installed. The Wise Installation Wizard will install the files for NI FieldPoint 3.0.2 in the following folder. To install into a different folder, click the Browse button, and select another folder. You can choose not to install NI FieldPoint 3.0.2 by clicking Cancel to exit the Wise Installation Wizard. Destination Folder C:\Program Files\National Instruments\FieldPoint\

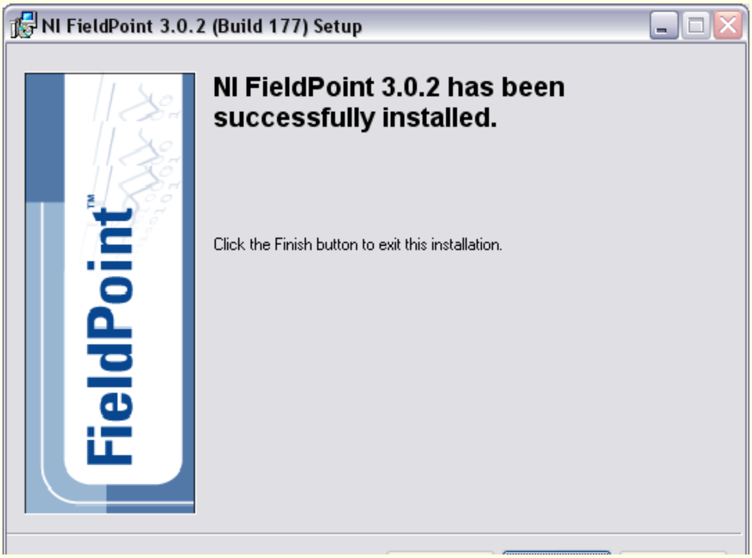
Procedure 223
FieldPoint Explorer Software 3.0.2 (Build 177) (Part 5 of 9)

Step	Action
6	Select the components to install.
	Click **Next** to accept the default settings and continue with the installation.  NI FieldPoint 3.0.2 (Build 177) Setup **Select Features** Please select which features you would like to install. **Feature Description:** This package will install the software needed to configure and control the FieldPoint hardware from LabVIEW, LabVIEW DSC, LabWindows/CVI, Lookout, and OPC. This feature will be installed on the local hard drive This feature requires 1KB on your hard drive. It has 2 of 7 subfeatures selected. The subfeatures require 26MB on your hard drive. FieldPoint FieldPoint Lookout Driver Documentation FieldPoint Core Firmware Upg LabVIEW_RT OPC Server CVI Instrument Driv LabVIEW VIs Browse Disk Cost Reset < Back Next > Cancel

Procedure 223
FieldPoint Explorer Software 3.0.2 (Build 177) (Part 6 of 9)

Step	Action
7	Begin copying files.
	Click **Next** to install the software.  NI FieldPoint 3.0.2 Setup **Ready to Install the Application** Click Next to begin installation. Click the Back button to reenter the installation information or click Cancel to exit the wizard.

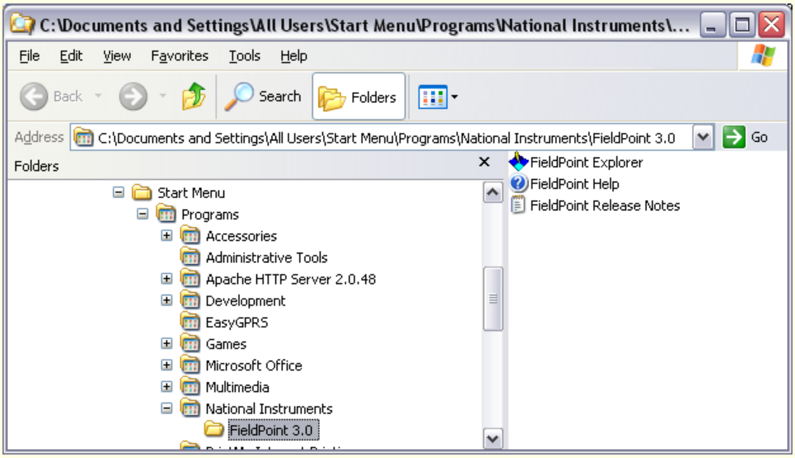
Procedure 223
FieldPoint Explorer Software 3.0.2 (Build 177) (Part 7 of 9)

Step	Action
8	Acknowledge the completion of the installation.
	Click **Finish**.  NI FieldPoint 3.0.2 (Build 177) Setup **NI FieldPoint 3.0.2 has been successfully installed.** Click the Finish button to exit this installation.

Procedure 223
FieldPoint Explorer Software 3.0.2 (Build 177) (Part 8 of 9)

<table>
<tr><th>Step</th><th>Action</th></tr>
<tr><td>9</td><td>Open the FieldPoint Explorer folder.</td></tr>
<tr><td></td><td>

Find the shortcut FieldPoint 3.0 in the National Instruments group of the Program Files, as shown:

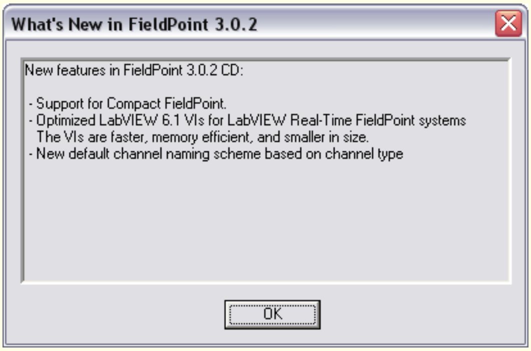
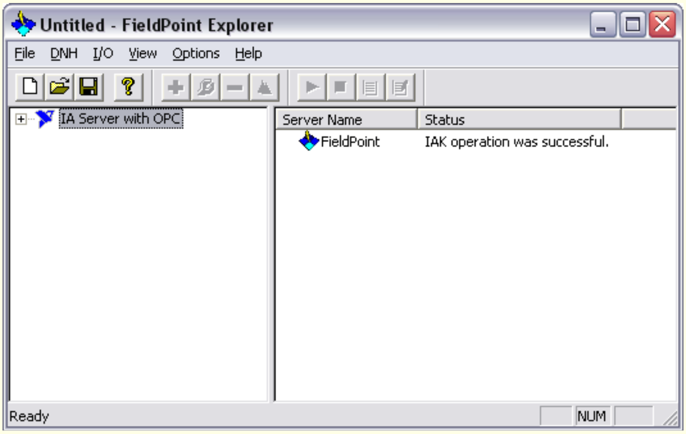


C:\Documents and Settings\All Users\Start Menu\Programs\National Instruments\...

Address C:\Documents and Settings\All Users\Start Menu\Programs\National Instruments\FieldPoint 3.0

</td></tr>
</table>

Procedure 223
FieldPoint Explorer Software 3.0.2 (Build 177) (Part 9 of 9)

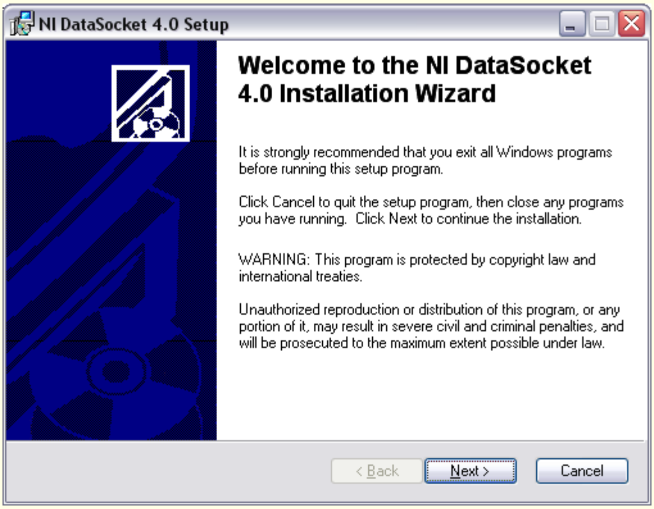
Step	Action
10	Launch FieldPoint Explorer.
	Double-click on the FieldPoint Explorer icon. The **What's New** message box opens, as follows. Click **OK**.  What's New in FieldPoint 3.0.2 New features in FieldPoint 3.0.2 CD: - Support for Compact FieldPoint. - Optimized LabVIEW 6.1 VIs for LabVIEW Real-Time FieldPoint systems The VIs are faster, memory efficient, and smaller in size. - New default channel naming scheme based on channel type The FieldPoint Explorer window opens.  Untitled - FieldPoint Explorer IA Server with OPC Server Name | Status FieldPoint | IAK operation was successful. Ready

END

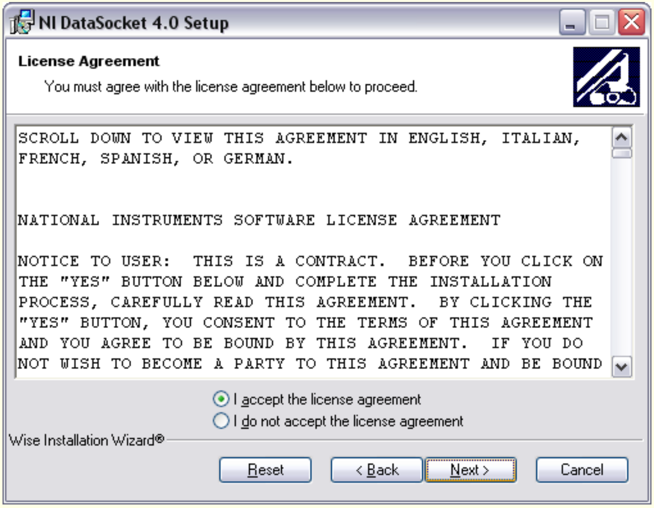
Installing DataSocket 4.0

This is a program that is required to communicate between the eIO module of DECT Messenger and the connected National Instruments distributed I/O modules.

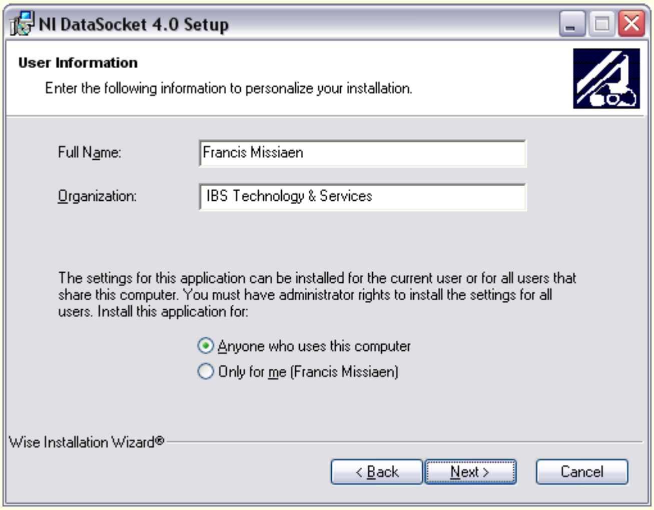
Procedure 224
Install DataSocket 4.0 (Part 1 of 8)

Step	Action
1	Begin installation.
	The software is located on the CD-ROM in the directory Step 3 - National-Instruments\Step 3b – DataSocket 4.0. Double-click the Setup.exe file to start installing.
2	Read the Welcome information, and continue with the installation.
	Click **Next** to continue.  **Welcome to the NI DataSocket 4.0 Installation Wizard** It is strongly recommended that you exit all Windows programs before running this setup program. Click Cancel to quit the setup program, then close any programs you have running. Click Next to continue the installation. WARNING: This program is protected by copyright law and international treaties. Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under law.

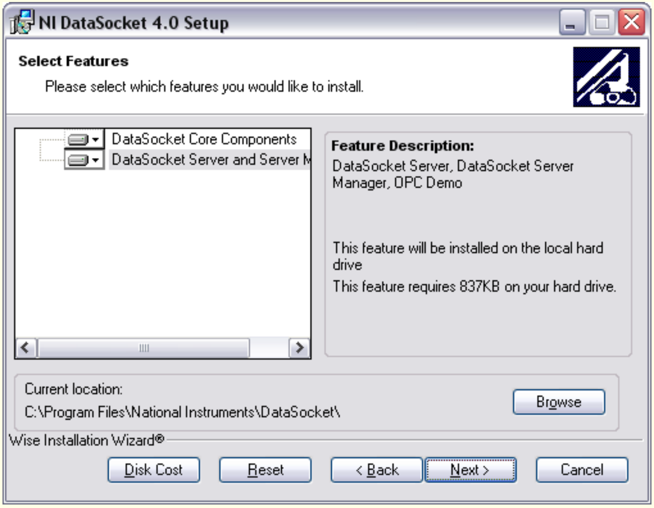
Procedure 224
Install DataSocket 4.0 (Part 2 of 8)

Step	Action
3	Read and accept the Licence Agreement.
	Read the Licence Agreement, and click **Next** to continue.  NI DataSocket 4.0 Setup **License Agreement** You must agree with the license agreement below to proceed. SCROLL DOWN TO VIEW THIS AGREEMENT IN ENGLISH, ITALIAN, FRENCH, SPANISH, OR GERMAN. NATIONAL INSTRUMENTS SOFTWARE LICENSE AGREEMENT NOTICE TO USER: THIS IS A CONTRACT. BEFORE YOU CLICK ON THE "YES" BUTTON BELOW AND COMPLETE THE INSTALLATION PROCESS, CAREFULLY READ THIS AGREEMENT. BY CLICKING THE "YES" BUTTON, YOU CONSENT TO THE TERMS OF THIS AGREEMENT AND YOU AGREE TO BE BOUND BY THIS AGREEMENT. IF YOU DO NOT WISH TO BECOME A PARTY TO THIS AGREEMENT AND BE BOUND ● I accept the license agreement ○ I do not accept the license agreement Wise Installation Wizard® Reset < Back Next > Cancel

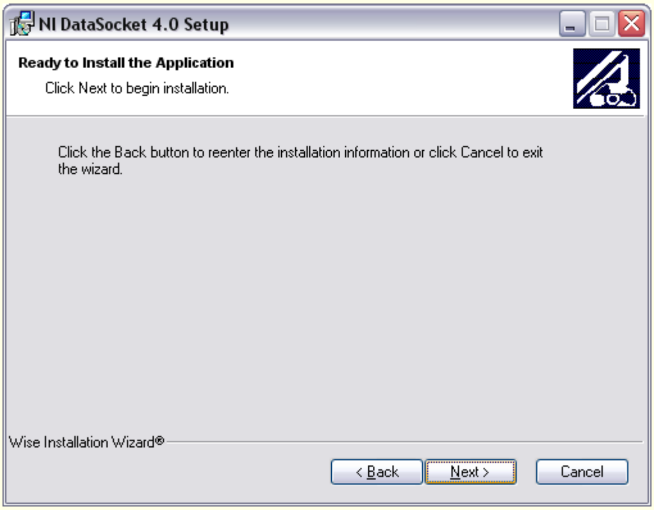
Procedure 224
Install DataSocket 4.0 (Part 3 of 8)

Step	Action
4	Enter user information.
	Enter the user information, and click **Next**.  NI DataSocket 4.0 Setup **User Information** Enter the following information to personalize your installation. Full Name: Francis Missiaen Organization: IBS Technology & Services The settings for this application can be installed for the current user or for all users that share this computer. You must have administrator rights to install the settings for all users. Install this application for: ● Anyone who uses this computer ○ Only for me (Francis Missiaen) Wise Installation Wizard®

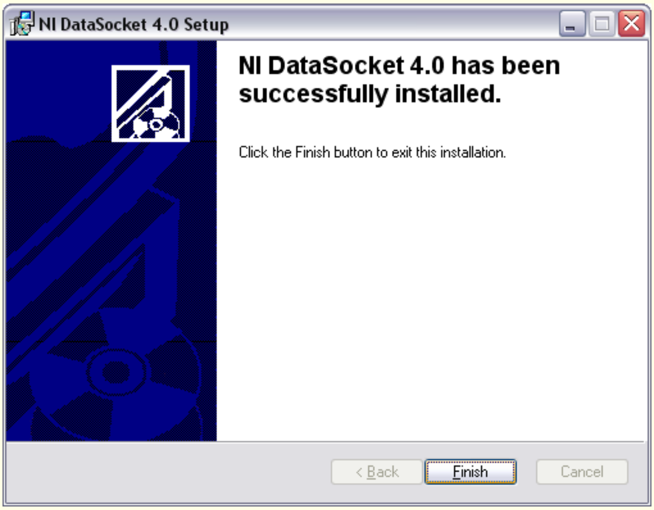
Procedure 224
Install DataSocket 4.0 (Part 4 of 8)

Step	Action
5	Select Features.
	Click **Next** to accept the default settings and continue with the installation.  NI DataSocket 4.0 Setup **Select Features** Please select which features you would like to install. DataSocket Core Components DataSocket Server and Server M **Feature Description:** DataSocket Server, DataSocket Server Manager, OPC Demo This feature will be installed on the local hard drive This feature requires 837KB on your hard drive. Current location: C:\Program Files\National Instruments\DataSocket\ Browse Wise Installation Wizard® Disk Cost Reset < Back Next > Cancel

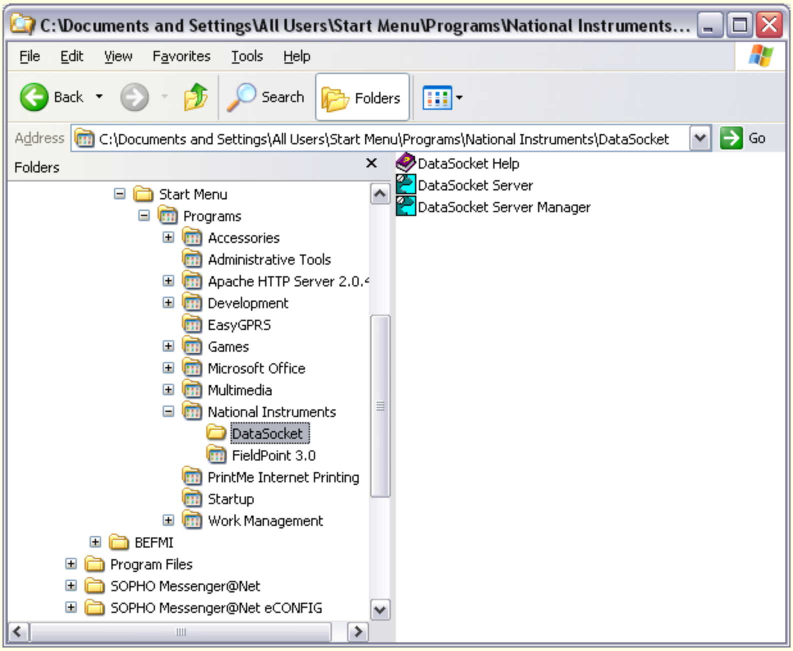
Procedure 224
Install DataSocket 4.0 (Part 5 of 8)

Step	Action
6	Begin copying files.
	Click **Next** to install the software.  NI DataSocket 4.0 Setup **Ready to Install the Application** Click Next to begin installation. Click the Back button to reenter the installation information or click Cancel to exit the wizard. Wise Installation Wizard®

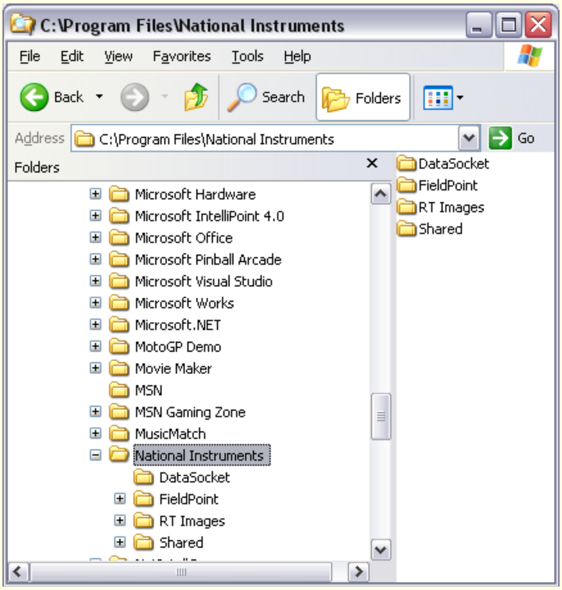
Procedure 224
Install DataSocket 4.0 (Part 6 of 8)

Step	Action
7	Acknowledge the completion of the installation.
	Click **Finish**.  NI DataSocket 4.0 Setup **NI DataSocket 4.0 has been successfully installed.** Click the Finish button to exit this installation.

Procedure 224
Install DataSocket 4.0 (Part 7 of 8)

Step	Action
8	Verify the shortcuts.
	Check the **Start** menu to ensure that DataSocket shortcuts are now available, as shown:  C:\Documents and Settings\All Users\Start Menu\Programs\National Instruments... Address: C:\Documents and Settings\All Users\Start Menu\Programs\National Instruments\DataSocket File Edit View Favorites Tools Help Back Search Folders Go Folders Start Menu Programs Accessories Administrative Tools Apache HTTP Server 2.0.4 Development EasyGPRS Games Microsoft Office Multimedia National Instruments DataSocket FieldPoint 3.0 PrintMe Internet Printing Startup Work Management BEFMI Program Files SOPHO Messenger@Net SOPHO Messenger@Net eCONFIG DataSocket Help DataSocket Server DataSocket Server Manager

Procedure 224
Install DataSocket 4.0 (Part 8 of 8)

Step	Action
9	Verify the Program installation.
	You can access the DataSocket shortcuts in the National Instruments group of the Program Files, as shown.  C:\Program Files\National Instruments File Edit View Favorites Tools Help Back Search Folders Address C:\Program Files\National Instruments Go Folders Microsoft Hardware Microsoft IntelliPoint 4.0 Microsoft Office Microsoft Pinball Arcade Microsoft Visual Studio Microsoft Works Microsoft.NET MotoGP Demo Movie Maker MSN MSN Gaming Zone MusicMatch National Instruments DataSocket FieldPoint RT Images Shared DataSocket FieldPoint RT Images Shared

END

Launching FieldPoint Explorer

Connect the hardware modules.

Important notes

Note that DECT Messenger has the following limitations:

- A single eIO instance can handle communications through either a FP-1000 module (RS-232) or a FP-1600 module (Ethernet). So for each FP-1000 or FP-1600, you need an instance of an eIO module.
- DECT Messenger supports the connection of only one eIO module. While some environments are known to be stable with more than one eIO module attached to a DECT Messenger, this is not officially supported by the authors of the eIO module. Contact Nortel product support before attaching more than one eIO.
- The eIO instance that handles an FP-1000 or FP-1600 can connect to other modules, such as FP-1001 and FP-1601, to build a tree-structure. The string can attach FP-AI-100, DP-DI-300, FP-DI-301, FP-DI-330, and FP-DO-401 modules.

  Note: DECT Messenger eIO is designed to support a maximum of eight modules attached to an eIO instance. Connecting more that eight modules is possible; however, because eIO can only handle eight modules, the remaining modules are nonoperational from the perspective of DECT Messenger.

At this stage, you must decide whether to use FP-1000 or FP-1600 to connect the eIO instance. The following sections provide examples of environments using FP-1000 and FP-1600, as follows:

- “Example 1: sample environment using FP-1000 module” on page 907
- “Example 2: sample environment using FP-1600 module” on page 923

Example 1: sample environment using FP-1000 module

Note: Consult the National Instruments web site at www.ni.com to obtain more information on installing and configuring the distributed I/O modules.

The following four tables provide configuration examples for a sample environment using FP-1000 module, as follows:

- Table 48: "Example 1a – FP-1000 module – Connect hardware modules" on page 908
- Table 49: "Example 1b – FP-1000 module – Adjust module configuration" on page 912
- Table 50: "Example 1c – FP-1000 module – Adjust contact configuration" on page 919
- Table 51: "Example 1d – FP-1000 module – Save configuration" on page 923

Table 48
Example 1a – FP-1000 module – Connect hardware modules (Part 1 of 4)

Step	Action
1	Attach the modules and power supply.
	• Attach the available modules (FP-AI-100, DP-DI-300, FP-DI-301, FP-DI-330, FP-DO-401) to the FP-1000 controller. • Attach the power supply to the FP-1000 module. If connected correctly, the power and ready lights on all modules show a green LED.
2	Connect the serial cable.
	• Look for an available COM port on the PC, and determine the resource name. This example uses COM01 port. • Connect the DB-9 serial cable to the selected COM port. ***Note:*** Refer to the FP-1000 documentation for more information on setting baud rate and address on the module. In this example, the factory default settings are used.

Table 48
Example 1a – FP-1000 module – Connect hardware modules (Part 2 of 4)

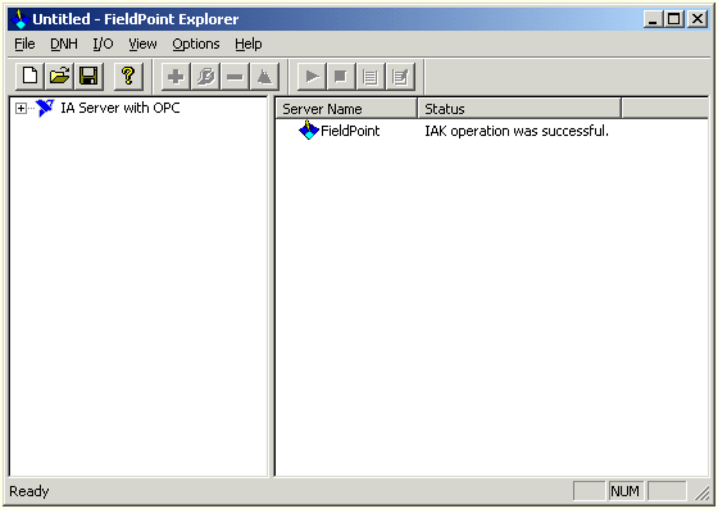
Step	Action
3	Launch the FieldPoint Explorer.
	Click **Start** and choose **Programs > National-Instruments > FieldPoint 3.0 > FieldPoint Explorer**.  Untitled - FieldPoint Explorer File DNH I/O View Options Help NUM IA Server with OPC Server Name: FieldPoint — Status: IAK operation was successful. Ready

Table 48
Example 1a – FP-1000 module – Connect hardware modules (Part 3 of 4)

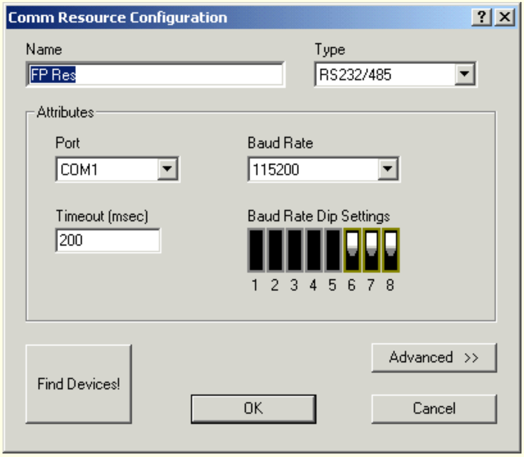
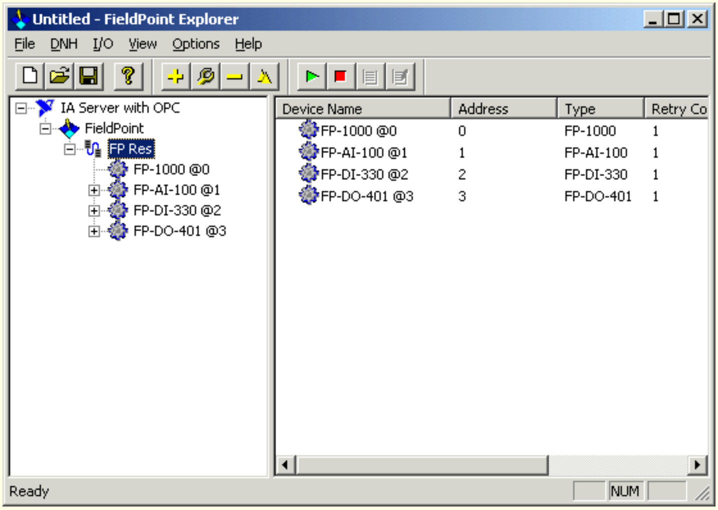
Step	Action
4	Add a comm resource.
	- Expand the **IA Server with OPC** item, and click **FieldPoint** to highlight the section. - Right-click and select the option **Add a com resource to this server...** from the pop-up menu. The following window opens:  Comm Resource Configuration Name: FP Res Type: RS232/485 Attributes Port: COM1 Baud Rate: 115200 Timeout (msec): 200 Baud Rate Dip Settings 1 2 3 4 5 6 7 8 Find Devices! Advanced >> OK Cancel

Table 48
Example 1a – FP-1000 module – Connect hardware modules (Part 4 of 4)

<table>
<tr><th>Step</th><th>Action</th></tr>
<tr><td>5</td><td>Configure the comm resource.</td></tr>
<tr><td></td><td>Adjust (if necessary) the <b>Port</b> (COM1) and <b>Baud Rate</b> parameter, according to your specific environment.
Refer to the FP-1000 module documentation for more information on the dip switch settings of the module.
In the <b>Advanced >></b> section, you can leave the default values for the <b>timeout value</b> (200 msec) and the <b>read interval</b> (100 msec) unchanged, in most environments.</td></tr>
<tr><td>6</td><td>Check for attached modules.</td></tr>
<tr><td></td><td>Click the <b>Find Devices!</b> button to search for attached peripherals. An intermediate window appears while the program searches for devices.
When the process is finished, the attached modules are automatically configured. This is shown in the following window:

Untitled - FieldPoint Explorer

IA Server with OPC
FieldPoint
FP Res
FP-1000 @0
FP-AI-100 @1
FP-DI-330 @2
FP-DO-401 @3
<table>
<tr><th>Device Name</th><th>Address</th><th>Type</th><th>Retry Co</th></tr>
<tr><td>FP-1000 @0</td><td>0</td><td>FP-1000</td><td>1</td></tr>
<tr><td>FP-AI-100 @1</td><td>1</td><td>FP-AI-100</td><td>1</td></tr>
<tr><td>FP-DI-330 @2</td><td>2</td><td>FP-DI-330</td><td>1</td></tr>
<tr><td>FP-DO-401 @3</td><td>3</td><td>FP-DO-401</td><td>1</td></tr>
</table>
Ready
 </td></tr>
</table>

END

.

Table 49
Example 1b – FP-1000 module – Adjust module configuration (Part 1 of 7)

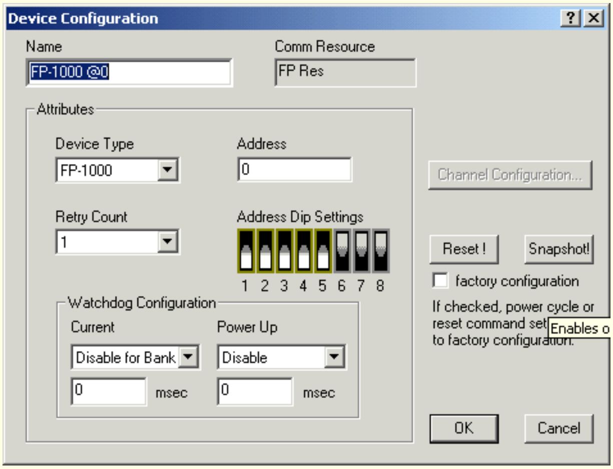
Step	Action
1	Open the Device Configuration window for FP-1000.
	- Highlight **FP-1000**. - Right-click to access a pop-up menu. - Choose **Device Configuration**.  Device Configuration Name: FP-1000 @0 Comm Resource: FP Res Attributes Device Type: FP-1000 Address: 0 Retry Count: 1 Address Dip Settings Watchdog Configuration Current: Disable for Bank, 0 msec Power Up: Disable, 0 msec ☐ factory configuration If checked, power cycle or reset command set to factory configuration. ? 1 2 3 4 5 6 7 8 Channel Configuration... Reset ! Snapshot! Enables o OK Cancel ***Note:*** You can highlight any module, and right-click the pop-up window to edit it.

Table 49
Example 1b – FP-1000 module – Adjust module configuration (Part 2 of 7)

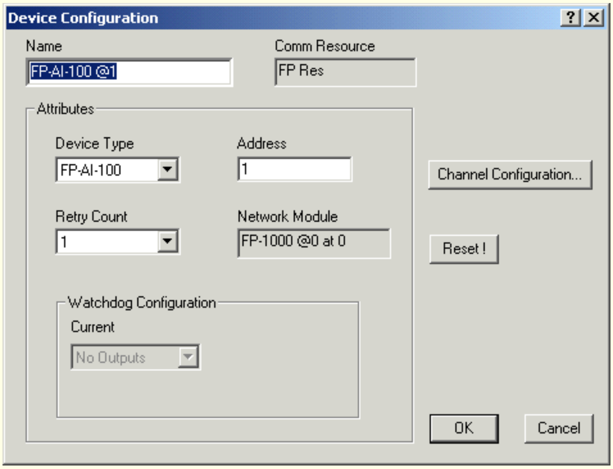
Step	Action
2	Open the Device Configuration window for FP-AI-1000.
	• Highlight **FP-AI-100**. • Right-click to access a pop-up menu. • Choose **Device Configuration**.  Device Configuration Name: FP-AI-100 @1 Comm Resource: FP Res Attributes Device Type: FP-AI-100 Address: 1 Retry Count: 1 Network Module: FP-1000 @0 at 0 Watchdog Configuration Current: No Outputs

Table 49
Example 1b – FP-1000 module – Adjust module configuration (Part 3 of 7)

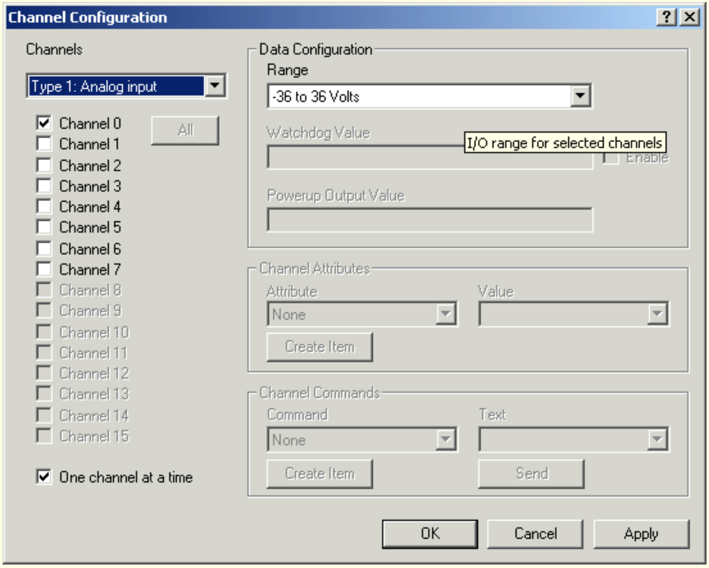
Step	Action
3	Adjust the range of analogue input on contact level for FP-AI-100.
	Click **Channel Configuration...** to open the Channel Configuration window.  Channel Configuration Channels: Type 1: Analog input ☑ Channel 0 □ Channel 1 □ Channel 2 □ Channel 3 □ Channel 4 □ Channel 5 □ Channel 6 □ Channel 7 □ Channel 8 □ Channel 9 □ Channel 10 □ Channel 11 □ Channel 12 □ Channel 13 □ Channel 14 □ Channel 15 ☑ One channel at a time Data Configuration Range: -36 to 36 Volts I/O range for selected channels Watchdog Value: □ Enable Powerup Output Value: Channel Attributes Attribute: None Value: Channel Commands Command: None Text:

Table 49
Example 1b – FP-1000 module – Adjust module configuration (Part 4 of 7)

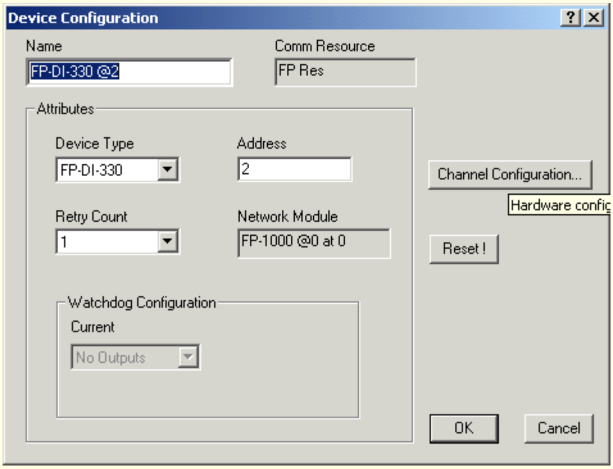
Step	Action
4	Open the Device Configuration window for FP-DI-330.
	• Highlight **FP-DI-330**. • Right-click to access a pop-up menu. • Choose **Device Configuration**.  Device Configuration Name: FP-DI-330 @2 Comm Resource: FP Res Attributes Device Type: FP-DI-330 Address: 2 Retry Count: 1 Network Module: FP-1000 @0 at 0 Watchdog Configuration Current: No Outputs Channel Configuration... Hardware config Reset ! OK Cancel

Table 49
Example 1b – FP-1000 module – Adjust module configuration (Part 5 of 7)

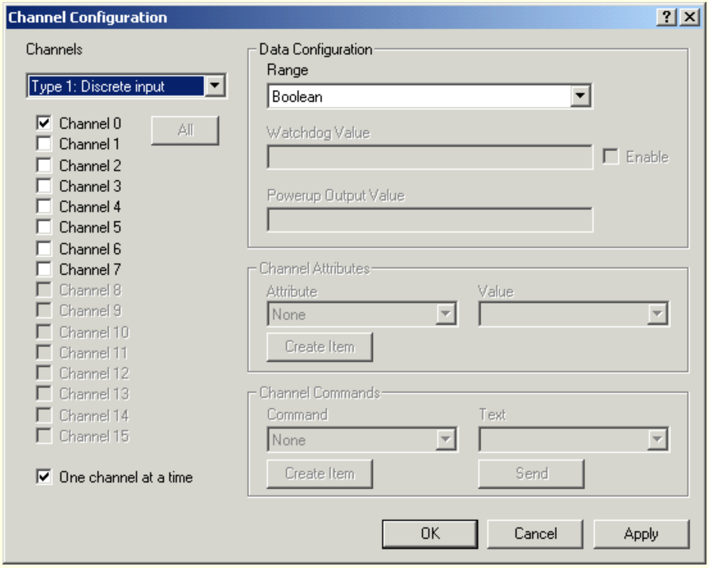
Step	Action
5	Adjust the range of discrete input on contact level for FP-DI-330.
	Click **Channel Configuration...** to open the Channel Configuration window.  Channel Configuration Channels: Type 1: Discrete input ☑ Channel 0 □ Channel 1 □ Channel 2 □ Channel 3 □ Channel 4 □ Channel 5 □ Channel 6 □ Channel 7 □ Channel 8 □ Channel 9 □ Channel 10 □ Channel 11 □ Channel 12 □ Channel 13 □ Channel 14 □ Channel 15 ☑ One channel at a time Data Configuration Range: Boolean Watchdog Value: □ Enable Powerup Output Value: Channel Attributes Attribute: None Value: Channel Commands Command: None Text:

Table 49
Example 1b – FP-1000 module – Adjust module configuration (Part 6 of 7)

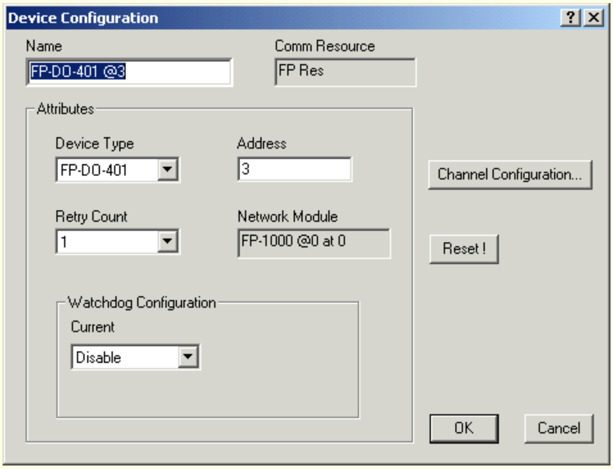
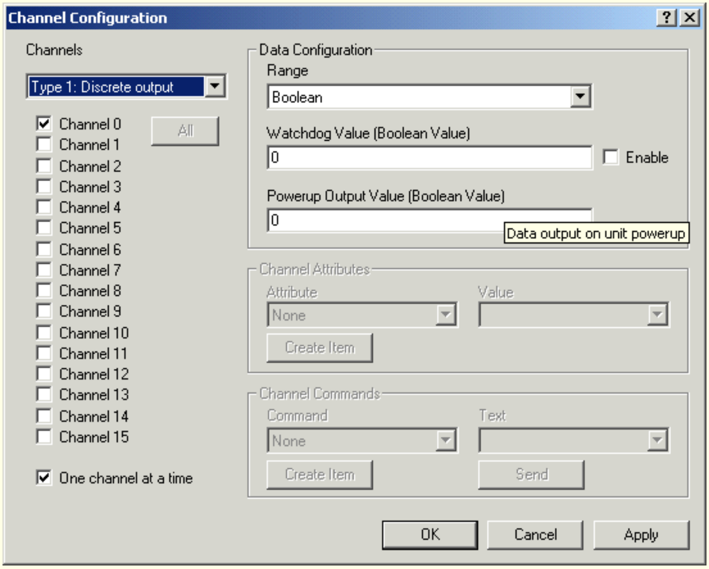
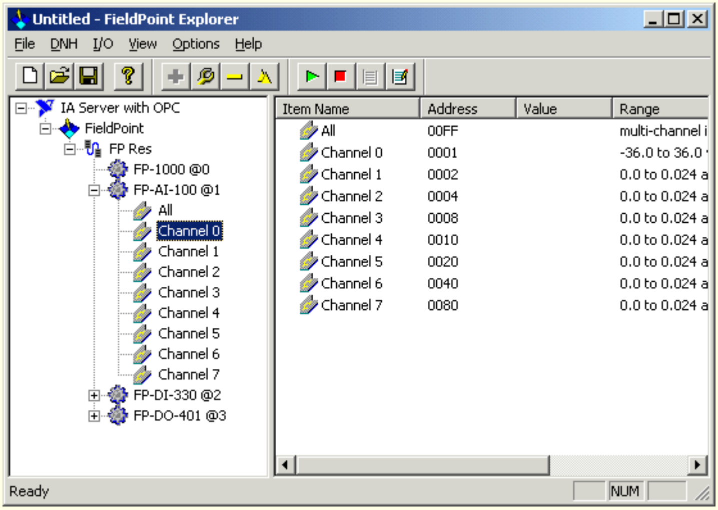
Step	Action
6	Adjust the range of analogue input on contact level for FP-DO-401.
	- Highlight **FP-DO-401.** - Right-click to access a pop-up menu. - Choose **Device Configuration**.  Device Configuration Name: FP-DO-401 @3 Comm Resource: FP Res Attributes Device Type: FP-DO-401 Address: 3 Retry Count: 1 Network Module: FP-1000 @0 at 0 Watchdog Configuration Current: Disable

Table 49
Example 1b – FP-1000 module – Adjust module configuration (Part 7 of 7)

Step	Action
7	Adjust the range of digital input on contact level for FP-DO-401.
	Click **Channel Configuration...** to open the **Channel Configuration** window.  Channel Configuration Channels Type 1: Discrete output ☑ Channel 0 ☐ Channel 1 ☐ Channel 2 ☐ Channel 3 ☐ Channel 4 ☐ Channel 5 ☐ Channel 6 ☐ Channel 7 ☐ Channel 8 ☐ Channel 9 ☐ Channel 10 ☐ Channel 11 ☐ Channel 12 ☐ Channel 13 ☐ Channel 14 ☐ Channel 15 All ☑ One channel at a time Data Configuration Range: Boolean Watchdog Value (Boolean Value): 0 ☐ Enable Powerup Output Value (Boolean Value): 0 Data output on unit powerup Channel Attributes Attribute: None Value: Create Item Channel Commands Command: None Text: Create Item Send OK Cancel Apply

END

Table 50
Example 1c – FP-1000 module – Adjust contact configuration (Part 1 of 4)

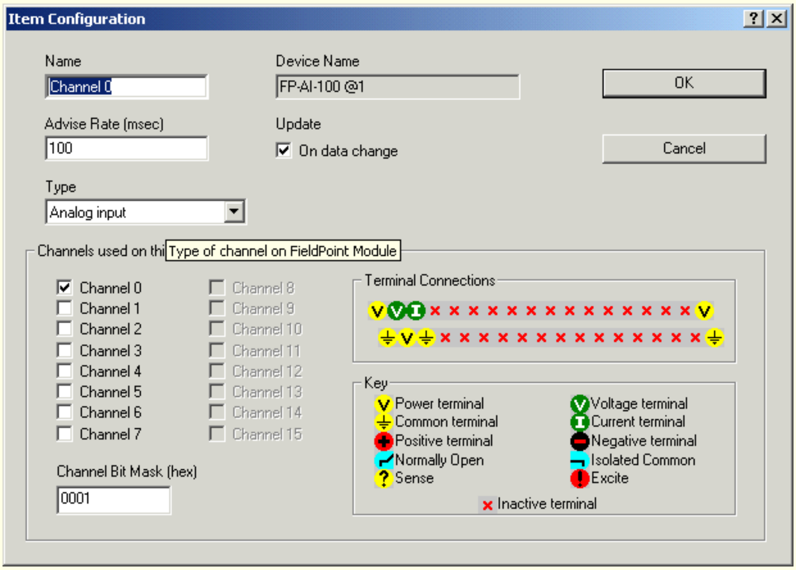
Step	Action
1	Editing an individual contact.
	- Highlight an individual contact. - Right-click to open the pop-up window and edit the individual item. 

Untitled - FieldPoint Explorer
File DNH I/O View Options Help
Ready
NUM

IA Server with OPC
- FieldPoint
  - FP Res
    - FP-1000 @0
    - FP-AI-100 @1
      - All
      - Channel 0
      - Channel 1
      - Channel 2
      - Channel 3
      - Channel 4
      - Channel 5
      - Channel 6
      - Channel 7
    - FP-DI-330 @2
    - FP-DO-401 @3

Item Name	Address	Value	Range
All	00FF		multi-channel i
Channel 0	0001		-36.0 to 36.0 '
Channel 1	0002		0.0 to 0.024 a
Channel 2	0004		0.0 to 0.024 a
Channel 3	0008		0.0 to 0.024 a
Channel 4	0010		0.0 to 0.024 a
Channel 5	0020		0.0 to 0.024 a
Channel 6	0040		0.0 to 0.024 a
Channel 7	0080		0.0 to 0.024 a

Table 50
Example 1c – FP-1000 module – Adjust contact configuration (Part 2 of 4)

Step	Action
2	Edit an Analogue **Input** contact on a FP-AI-100 module.
	

Item Configuration

Name: Channel 0

Device Name: FP-AI-100 @1

Advise Rate (msec): 100

Update
☑ On data change

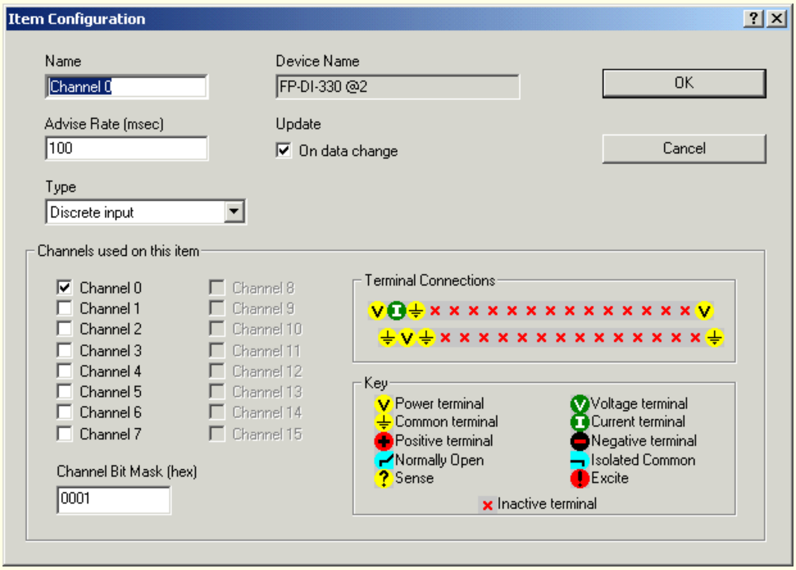
Type: Analog input

Channels used on thi Type of channel on FieldPoint Module

☑ Channel 0
□ Channel 1
□ Channel 2
□ Channel 3
□ Channel 4
□ Channel 5
□ Channel 6
□ Channel 7
□ Channel 8
□ Channel 9
□ Channel 10
□ Channel 11
□ Channel 12
□ Channel 13
□ Channel 14
□ Channel 15

Channel Bit Mask (hex): 0001

Table 50
Example 1c – FP-1000 module – Adjust contact configuration (Part 3 of 4)

Step	Action
3	Edit a Digital Input contact on a FP-DI-330 module.
	

Item Configuration

Name: Channel 0

Device Name: FP-DI-330 @2

Advise Rate (msec): 100

Update: ☑ On data change

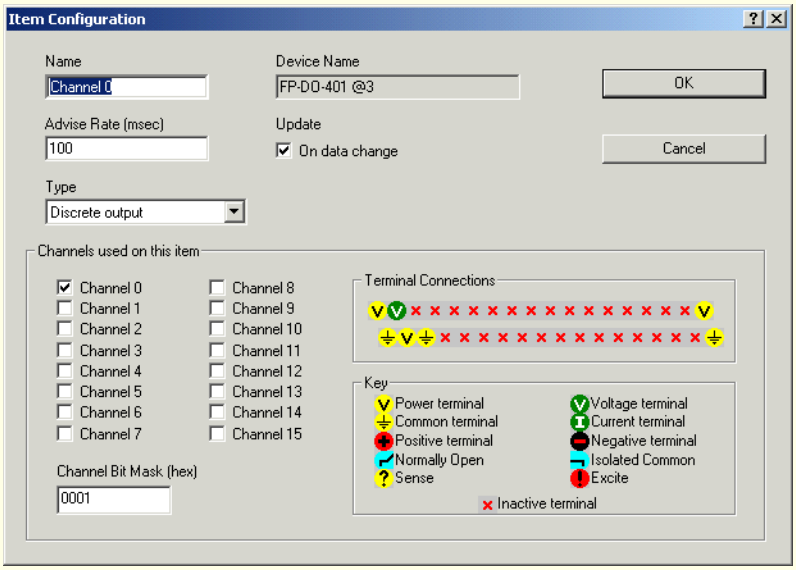
Type: Discrete input

Channels used on this item

☑ Channel 0
□ Channel 1
□ Channel 2
□ Channel 3
□ Channel 4
□ Channel 5
□ Channel 6
□ Channel 7
□ Channel 8
□ Channel 9
□ Channel 10
□ Channel 11
□ Channel 12
□ Channel 13
□ Channel 14
□ Channel 15

Channel Bit Mask (hex): 0001

Table 50
Example 1c – FP-1000 module – Adjust contact configuration (Part 4 of 4)

Step	Action
4	Edit a Digital Output contact on a FP-DO-401 module
	
	END

Item Configuration

Name: Channel 0

Device Name: FP-DO-401 @3

Advise Rate (msec): 100

Update: ☑ On data change

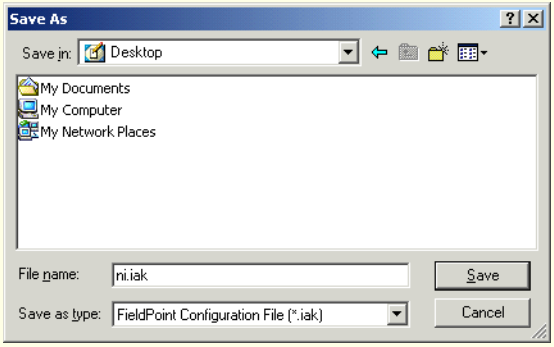
Type: Discrete output

Channels used on this item

☑ Channel 0
☐ Channel 1
☐ Channel 2
☐ Channel 3
☐ Channel 4
☐ Channel 5
☐ Channel 6
☐ Channel 7
☐ Channel 8
☐ Channel 9
☐ Channel 10
☐ Channel 11
☐ Channel 12
☐ Channel 13
☐ Channel 14
☐ Channel 15

Channel Bit Mask (hex): 0001

Table 51
Example 1d – FP-1000 module – Save configuration

Step	Action
1	Save the configuration.
	Choose **File > Save As**. Nortel recommends using the name ni.iak and locating the file on the desktop.  Save in: Desktop File name: ni.iak Save as type: FieldPoint Configuration File (*.iak) Save As My Documents My Computer My Network Places Save Cancel
	END

Example 2: sample environment using FP-1600 module

Note: National Instruments FieldPoint distributed I/O modules are documented extensively on the National Instruments web site www.ni.com. Consult the web site to obtain more information on installing and configuring the modules.

See Table 52 for configuration procedures for a sample environment using FP-1600 module.

Table 52
Example 2 - FP-1600 module (Part 1 of 7)

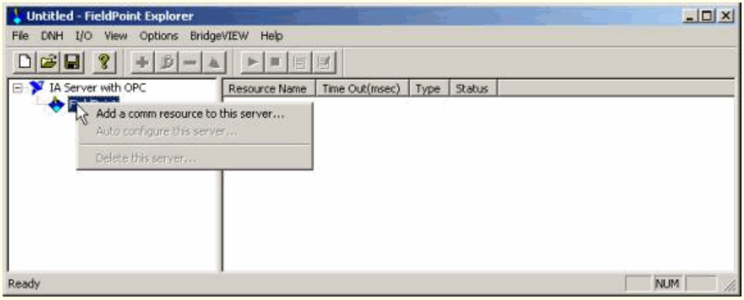
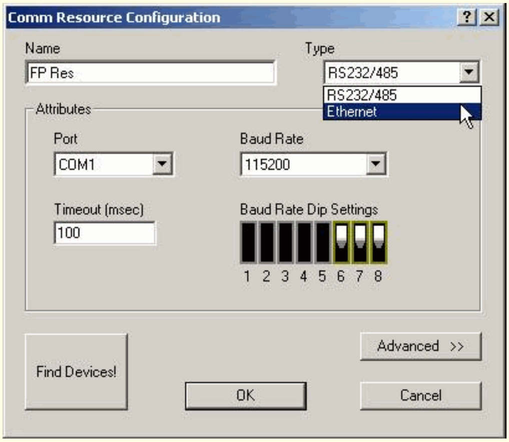
Step	Action
1	Launch FieldPoint Explorer, and create a new project.
	Launch FieldPoint Explorer and select **File > New** to start a new FieldPoint project. ***Note:*** All FieldPoint Explorer projects are saved as *.iak files.
2	Add a comm resource.
	• Double-click **IA Server with OPC**. • Highlight the **FieldPoint** resource. • Right-click and select **Add a comm resource to this server**, as shown:  Untitled - FieldPoint Explorer File DNH I/O View Options BridgeVIEW Help IA Server with OPC Add a comm resource to this server... Auto configure this server... Delete this server... Resource Name Time Out(msec) Type Status Ready NUM

Table 52
Example 2 - FP-1600 module (Part 2 of 7)

<table>
<tr><th>Step</th><th>Action</th></tr>
<tr><td>3</td><td>Configure the comm resource.</td></tr>
<tr><td></td><td>

- Select **Ethernet** as the communication type in the **Comm Resource Configuration** Window:



Comm Resource Configuration

Name: FP Res

Type: RS232/485 (list: RS232/485, Ethernet)

Attributes

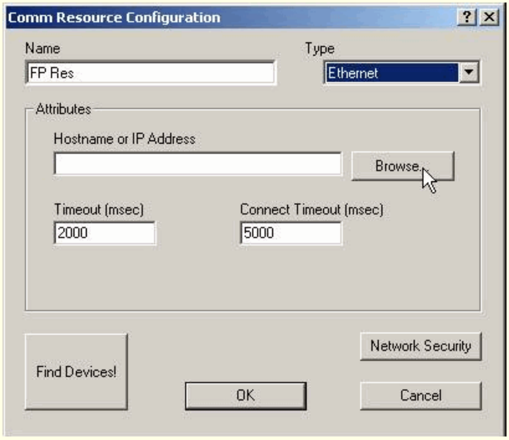
Port: COM1

Baud Rate: 115200

Timeout (msec): 100

Baud Rate Dip Settings: 1 2 3 4 5 6 7 8

The window changes to the following:



Comm Resource Configuration

Name: FP Res

Type: Ethernet

Attributes

Hostname or IP Address:

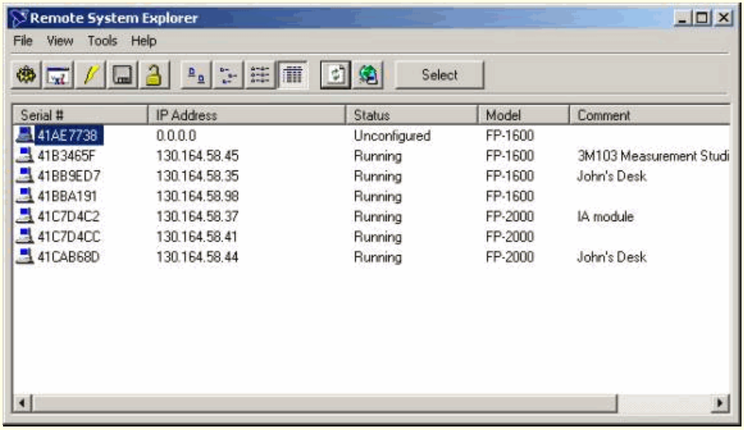
Timeout (msec): 2000

Connect Timeout (msec): 5000

- Click **Browse**.

</td></tr>
<tr><td></td><td></td></tr>
</table>

Table 52
Example 2 - FP-1600 module (Part 3 of 7)

<table>
<tr><th>Step</th><th>Action</th></tr>
<tr><td>4</td><td>Find your Ethernet network module in the Remote System Explorer list.</td></tr>
<tr><td></td><td>
If your Ethernet network module does not appear in the list of Network Devices, then refer to Troubleshooting Communication Problems with FieldPoint Ethernet Network Modules on the www.ni.com web site.
Note: The Ethernet network module is shipped from the factory, without any configuration. If you previously configured the module, then reset the module before proceeding.


<table>
<tr><th>Serial #</th><th>IP Address</th><th>Status</th><th>Model</th><th>Comment</th></tr>
<tr><td>41AE7738</td><td>0.0.0.0</td><td>Unconfigured</td><td>FP-1600</td><td></td></tr>
<tr><td>41B3465F</td><td>130.164.58.45</td><td>Running</td><td>FP-1600</td><td>3M103 Measurement Studi</td></tr>
<tr><td>41BB9ED7</td><td>130.164.58.35</td><td>Running</td><td>FP-1600</td><td>John's Desk</td></tr>
<tr><td>41BBA191</td><td>130.164.58.98</td><td>Running</td><td>FP-1600</td><td></td></tr>
<tr><td>41C7D4C2</td><td>130.164.58.37</td><td>Running</td><td>FP-2000</td><td>IA module</td></tr>
<tr><td>41C7D4CC</td><td>130.164.58.41</td><td>Running</td><td>FP-2000</td><td></td></tr>
<tr><td>41CAB68D</td><td>130.164.58.44</td><td>Running</td><td>FP-2000</td><td>John's Desk</td></tr>
</table>
</td></tr>
</table>

Table 52
Example 2 - FP-1600 module (Part 4 of 7)

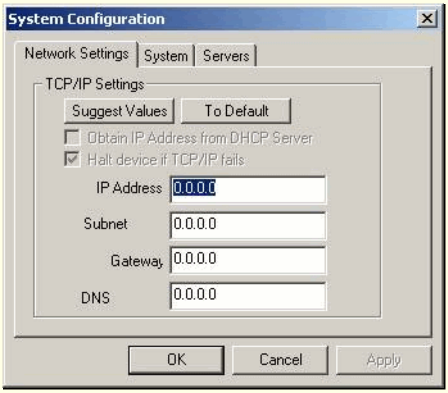
Step	Action
5	Open the **System Configuration** window for your Ethernet network module.
	• Select your Ethernet network module. • Double-click its serial number. The following window opens:  System Configuration Network Settings System Servers TCP/IP Settings Suggest Values To Default OK Cancel Apply ☐ Obtain IP Address from DHCP Server ☑ Halt device if TCP/IP fails IP Address 0.0.0.0 Subnet 0.0.0.0 Gateway 0.0.0.0 DNS 0.0.0.0

Table 52
Example 2 - FP-1600 module (Part 5 of 7)

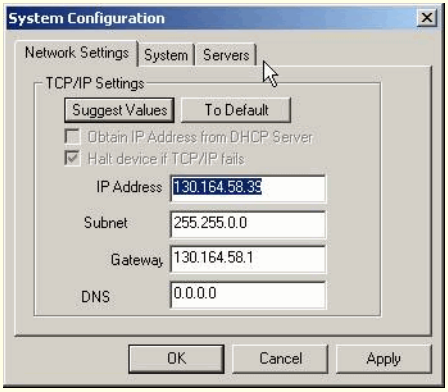
Step	Action
6	Configure the network settings.
	Enter values for: • IP address • Subnet mask • Time Server IP The IP address is the address of your Ethernet network module on the network, the Subnet mask is the mask that the device uses to find other devices on the Ethernet network (255.255.255.0 is the most common), and the Time server IP is the address of the host computer connected to your Ethernet network module.  System Configuration Network Settings | System | Servers TCP/IP Settings Suggest Values To Default ☐ Obtain IP Address from DHCP Server ☑ Halt device if TCP/IP fails IP Address 130.164.58.39 Subnet 255.255.0.0 Gateway 130.164.58.1 DNS 0.0.0.0 OK Cancel Apply ***Note 1:*** This illustration shows a typical configuration. You can press **Suggest Values** for the FieldPoint Explorer to suggest values. ***Note 2:*** If you are using a network, ask the network administrator to assign a unique IP address to your Ethernet network module.

Table 52
Example 2 - FP-1600 module (Part 6 of 7)

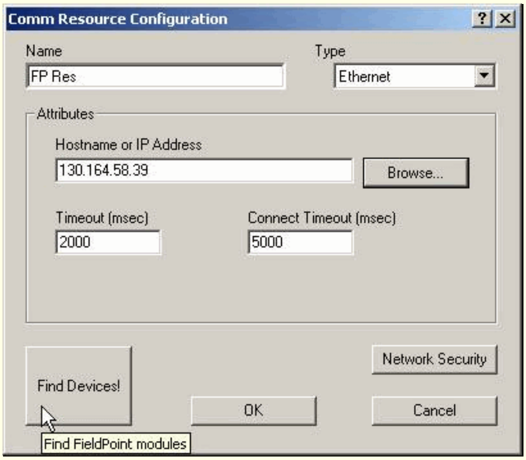
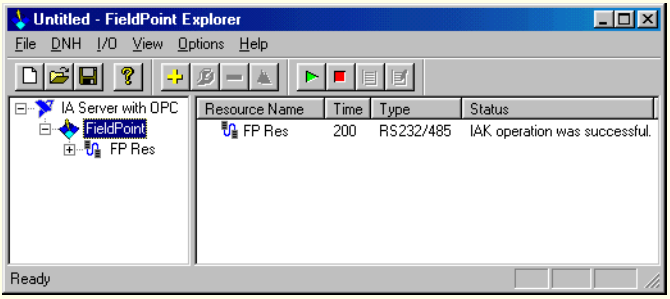
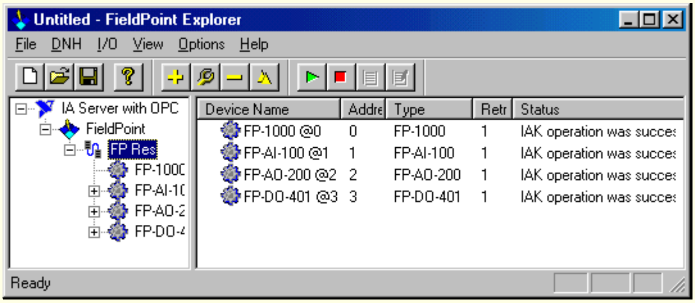
Step	Action
7	Apply your changes.
	Click **Apply**, then **OK** in each of the successive windows until you return to the window shown:  Comm Resource Configuration Name: FP Res Type: Ethernet Attributes Hostname or IP Address: 130.164.58.39 Timeout (msec): 2000 Connect Timeout (msec): 5000 Browse... Find Devices! Network Security OK Cancel Find FieldPoint modules

Table 52
Example 2 - FP-1600 module (Part 7 of 7)

Step	Action
8	Find connected modules.
	Press the **Find Devices!** button to cause FieldPoint Explorer to detect your FP Modules:  Untitled - FieldPoint Explorer File DNH I/O View Options Help IA Server with OPC FieldPoint FP Res Resource Name | Time | Type | Status FP Res | 200 | RS232/485 | IAK operation was successful. Ready ***Note:*** If you receive the message **No Modules were found.**, then go to Troubleshooting Communication Problems with FieldPoint Ethernet Network Modules on the www.ni.com web site.
9	Review the list of devices.
	Left-click **FP Res**, and the devices appear in the left panel of the window.  Untitled - FieldPoint Explorer File DNH I/O View Options Help IA Server with OPC FieldPoint FP Res FP-100C FP-AI-1C FP-AO-2 FP-DO-4 Device Name | Addre | Type | Retr | Status FP-1000 @0 | 0 | FP-1000 | 1 | IAK operation was succes FP-AI-100 @1 | 1 | FP-AI-100 | 1 | IAK operation was succes FP-AO-200 @2 | 2 | FP-AO-200 | 1 | IAK operation was succes FP-DO-401 @3 | 3 | FP-DO-401 | 1 | IAK operation was succes Ready
10	Save configuration.
	Select **File > Save** to save your configuration settings.
	END

Installing latest firmware

Nortel recommends that you use the latest available firmware on the FieldPoint FP-1000, FP-1001, FP-1600, and FP-1601 modules. Check the www.ni.com web site to determine what firmware revision is available.

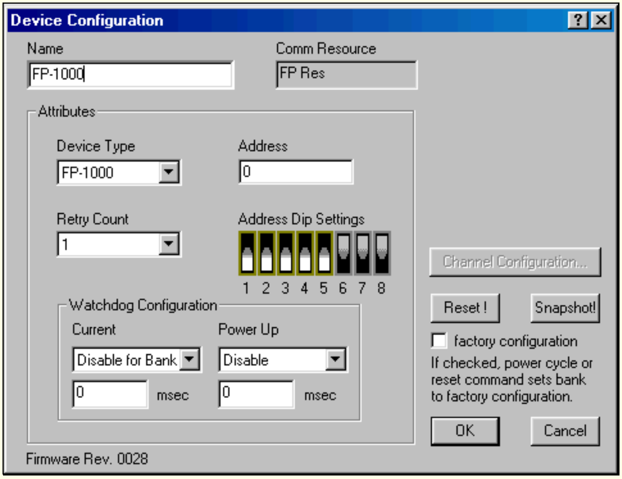
For your convenience, Firmware Revision 30 for FP-100x and Revision 417 for FP-160x are shipped in the CD-ROM in the folder the Step 3 - National-Instruments\Step 3c - Firmware Revisions directory structure.

Use the steps in Procedure 225 to determine your current firmware revision.

Procedure 225
Check which firmware you are currently using (Part 1 of 3)

Step	Action
1	Open the **Device Configuration** dialog box.
	• Launch FieldPoint Explorer. • Click the **+** next to IA Server with OPC Server. • Continue expanding the tree until you find your network module. • Right-click your network module and select **Edit this device in the pop-up menu.**

Procedure 225
Check which firmware you are currently using (Part 2 of 3)

Step	Action
2	Read the firmware version.
	In the **Device Configuration** dialog box, the firmware revision normally appears in the lower left corner in the form of Firmware Rev. xxxx, where xxxx represents the firmware revision number as is shown in the following dialog box.  Device Configuration Name: FP-1000 Comm Resource: FP Res Attributes Device Type: FP-1000 Address: 0 Retry Count: 1 Address Dip Settings: 1 2 3 4 5 6 7 8 Watchdog Configuration Current: Disable for Bank, 0 msec Power Up: Disable, 0 msec ☐ factory configuration If checked, power cycle or reset command sets bank to factory configuration. Firmware Rev. 0028 ? Channel Configuration... Reset ! Snapshot! OK Cancel If the firmware revision ***does not*** appear in the lower left corner of the dialog box: • Continue to step 3. If the firmware revisions ***does*** appear: • Click **Cancel** to exit. • Continue to Procedure 226 on page 935.

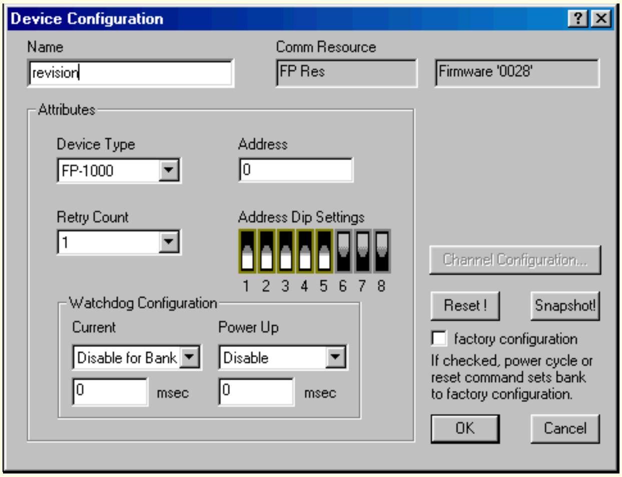
Procedure 225
Check which firmware you are currently using (Part 3 of 3)

Step	Action
3	Check firmware revision if it is not displayed in Step 2.

- If the firmware revision does not appear in the lower left corner, as shown in the previous dialog box, enter **revision** in the Name field.

The firmware revision appears in the upper-right corner as shown in the following dialog box.

- Click **Cancel** to exit.



Device Configuration

Name: revision

Comm Resource: FP Res

Firmware '0028'

Attributes

Device Type: FP-1000

Address: 0

Retry Count: 1

Watchdog Configuration

Current: Disable for Bank, 0 msec

Power Up: Disable, 0 msec

□ factory configuration

If checked, power cycle or reset command sets bank to factory configuration.

Note: Do ***not*** press **Enter** or click **OK**. Doing so renames the module revision, resulting in undesired changes. Click **Cancel** to exit from the **Device Configuration** dialog box.

END

Procedure 226
Determining which firmware you need

Step	Action
1	Check to determine what firmware version you need.
	Check Table 53 to determine the minimum firmware revision required for each of the FieldPoint I/O modules. Use the table to compare the minimum firmware requirement to your current firmware revisions that you found in the previous section, Procedure 225 on page 932.

END

Table 53
Minimum firmware revision required for each of the FieldPoint I/O modules (Part 1 of 3)

Network Modules	Minimum FP-1000/1001 Firmware	Minimum FP-1600 Firmware	Minimum FP-2000/2010 Firmware	Minimum FP-3000 Firmware
FP-1000	14	—	—	—
FP-1001	14	—	—	—
FP-1600	—	0100	—	—
FP-2000	—	—	1.0.21	—
FP-2010	—	—	1.0.21	—
FP-3000	—	—	—	1.0
Analogue Modules	—	—	—	—
FP-AI-100	14	0100	1.0.21	1.0
FP-AI-110	14	0100	1.0.21	1.0
FP-AI-111	14	0100	1.0.21	1.0

Table 53
Minimum firmware revision required for each of the FieldPoint I/O modules (Part 2 of 3)

FP-AO-200	14	0100	1.0.21	1.0
FP-AO-210	14	0100	1.0.21	—
FP-RTD-122	14	0100	1.0.21	1.0
FP-TC-120	20	0100	1.0.21	1.0
Discrete Modules	—	—	—	—
FP-CTR-500	30	0100	1.0.21	—
FP-CTR-502	30	0100	1.0.21	—
FP-DI-300	14	0100	1.0.21	1.0
FP-DI-301	14	0100	1.0.21	1.0
FP-DI-330	14	0100	1.0.21	1.0
FP-DO-400	14	0100	1.0.21	1.0
FP-DO-401	14	0100	1.0.21	1.0
FP-DO-403	14	0100	1.0.21	2.3.5
FP-DO-410	24	0100	1.0.21	2.3.5
Pulse Modules	—	—	—	—
FP-PG-522	24	0200	1.0.21	—
FP-PWM-520	24	0100	1.0.21	1.0
Relay Modules	—	—	—	—
FP-RLY-420	14	0100	1.0.21	1.0
FP-RLY-422	14	0100	1.0.21	2.3.5
Quadrature Input Module	—	—	—	—
FP-QUAD-510	25	0200	1.0.21	—

Table 53
Minimum firmware revision required for each of the FieldPoint I/O modules (Part 3 of 3)

Dual Channel Modules	—	—	—	—
FP-TB-10	28	0320	1.0.21	—

If the firmware revision you are using does not meet the needs of your I/O modules, you must upgrade your firmware. Continue to one of the following sections, depending on which network module is installed:

- Procedure 227 “Downloading firmware for the FP-1000/1001” on page 938”
- Procedure 228 “Downloading firmware for the FP-1600” on page 940”

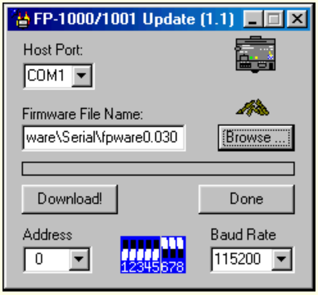
Note: Nortel recommends the Firmware Revision 30 or later for FP-100x, and Revision 417 or later for FP-160x. These versions are shipped on the CD-ROM, or you can download them from the web site as described in Procedure 227 on page 938.

WARNING
To protect your FieldPoint system when downloading firmware for the FP-1001, isolate your FP-1001 and your computer from the rest of your FieldPoint system.

Procedure 227
Downloading firmware for the FP-1000/1001 (Part 1 of 2)

Step	Action
1	Go to the NL Software Library web page.
	• Launch your web browser. • Go to the Driver and Firmware download page on www.ni.com **(Support > Product Reference > Drivers and Updates > All Software Versions > Distributed I/O - Fieldpoint)**.
2	Download the firmware update utility.
	Browse in the list titled Firmware, and: • Click **FP-1000/1001 Firmware Revision 30 for Windows 95/98/NT/2000/ME**. • Click **continue the download process**. • If are not already logged in, log in to the web site as prompted. • Download FPupdate.zip. • Unzip the archive into your FieldPoint directory.

Procedure 227
Downloading firmware for the FP-1000/1001 (Part 2 of 2)

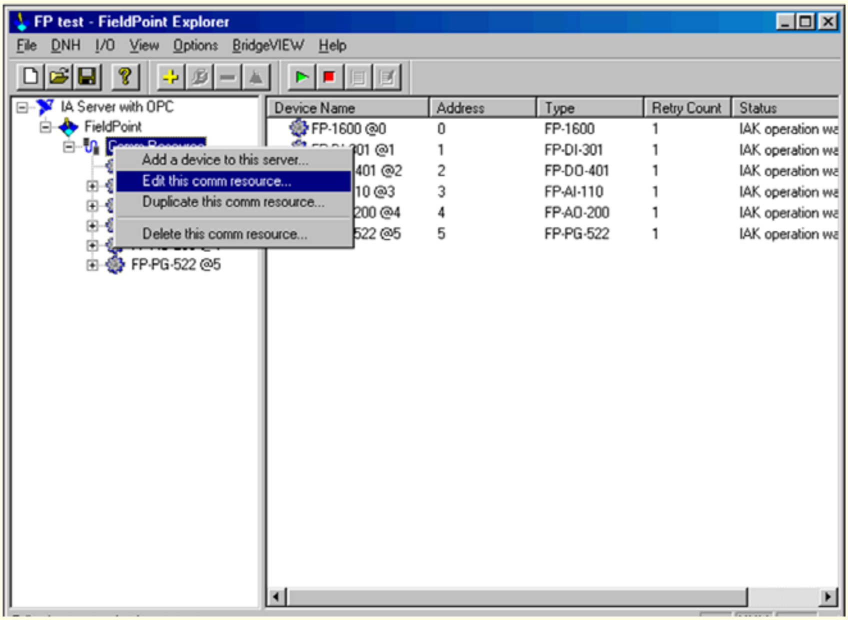
Step	Action
3	Run FPUpdate to update the firmware.
	Close FieldPoint Explorer. In your FieldPoint directory, navigate to the file, **FPUpdate**. Double-click **FPUpdate,** which brings up the **FP-1000/1001 Update** dialog box as shown in the following window.  FP-1000/1001 Update (1.1) Host Port: COM1 Firmware File Name: ware\Serial\fpware0.030 Address: 0 Baud Rate: 115200 **WARNING** Do not interrupt the download.
4	Choose the firmware version you need.
	• Click **Browse** and navigate to the firmware to which you are upgrading. In this example, the firmware is fpware0.030. • Set the address and baud rate to correspond with the settings on your FP-1000/1001. • Click **Download**.
5	Verify that the firmware upgrade is complete.
	Follow the steps in Procedure 225 on page 932.
	END

Use the following instructions if you use FieldPoint Explorer 3.0.0 or higher. The steps are slightly different if you are using an older version.

Procedure 228
Downloading firmware for the FP-1600 (Part 1 of 3)

Step	Action
1	Go to the NL Software Library web site.
	• Launch your internet browser. • Go to the Driver and Firmware download page on www.ni.com **(Support > Product Reference > Drivers and Updates > All Software Versions > Distributed I/O - Fieldpoint)**.
2	Download the firmware.
	Browse in the list titled Firmware, and: • Click **FP-1600 Firmware Revision 417 for Windows**. • Click **continue the download process**. • If you are not already logged in, log in to the Web site as prompted. • Download the firmware file. • Unzip the archive.

Procedure 228
Downloading firmware for the FP-1600 (Part 2 of 3)

Step	Action
3	Open the **Comm Resource Configuration** dialog box.
	Launch FieldPoint Explorer. Right-click the comm resource of your FP-1600 and select **Edit this device**. 
4	Open the **Remote System Explorer** dialog box.
	In the **Comm Resource Configuration** dialog box, click **Browse**.
5	Select Install/Upgrade Software.
	In the **Remote System Explorer** dialog box, right-click your FP-1600 and select **Install/Upgrade Software**.

FP test - FieldPoint Explorer
File DNH I/O View Options BridgeVIEW Help
IA Server with OPC
FieldPoint
Comm Resource
FP-PG-522 @5
Add a device to this server...
Edit this comm resource...
Duplicate this comm resource...
Delete this comm resource...

Device Name	Address	Type	Retry Count	Status
FP-1600 @0	0	FP-1600	1	IAK operation wa
FP-DI-301 @1	1	FP-DI-301	1	IAK operation wa
401 @2	2	FP-DO-401	1	IAK operation wa
10 @3	3	FP-AI-110	1	IAK operation wa
200 @4	4	FP-AO-200	1	IAK operation wa
522 @5	5	FP-PG-522	1	IAK operation wa

Procedure 228
Downloading firmware for the FP-1600 (Part 3 of 3)

Step	Action
6	Select the firmware update file to install.
	• In the Upgrade Firmware dialog box, click **Browse**. • Navigate to the firmware upgrade file you downloaded from the NI web page in Step 2. • Click **Update.** **WARNING** Do not interrupt the download.
7	Confirm the upgrade.
	Confirm that the firmware upgrade is complete by following the steps in Procedure 225 on page 932.

END

Using the eIO module

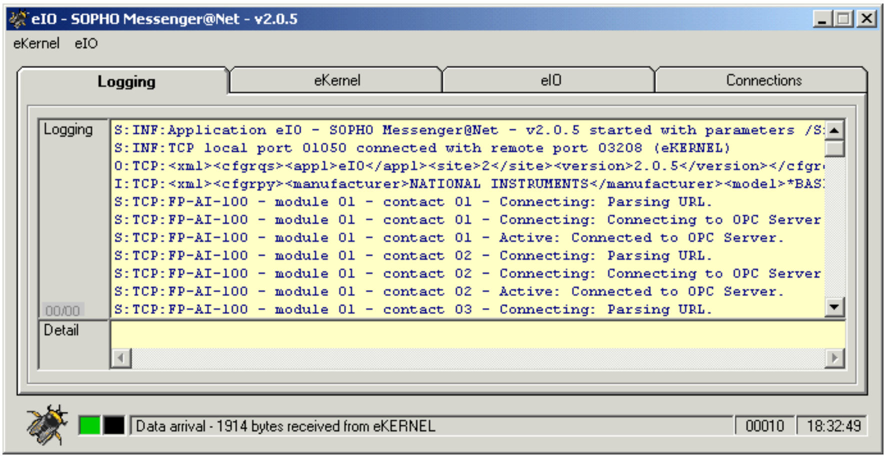
WARNING
Close the FieldPoint Explorer application when you want to activate the eIO module. Both applications attempt to allocate the distributed I/O resources, and therefore cannot run concurrently. If one application is active, the other one cannot run simultaneously.

You must adjust the configuration of each module and contact prior to using eIO. You can use the built-in functions of the FieldPoint Explorer to monitor the status and measured levels on attached peripherals. For analogue input, be careful to select the correct input range and unit of measurement. For discrete output, pay close attention to the start-up value.

To determine the configuration values needed to correctly configure the eIO_MODULE, eIO_AI, eIO_DI and eIO_DO configuration tables, use the

FieldPoint Explorer software. You must configure the DECT Messenger database before you launch the eIO module. When everything is correctly configured, the eIO window shows information similar to the illustrations in Figures 375 and Figure 376, and in Figure 377 on page 944 through Figure 379 on page 945.

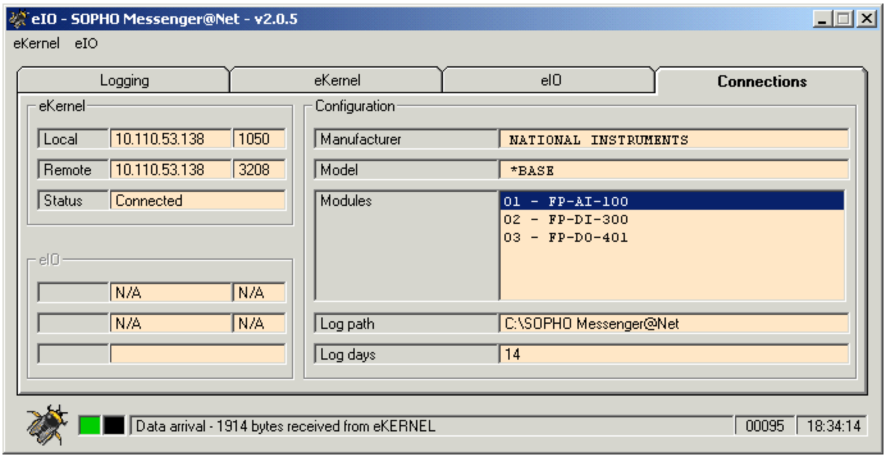
Figure 375
eIO module



```
S:INF:Application eIO - SOPHO Messenger@Net - v2.0.5 started with parameters /S:
S:INF:TCP local port 01050 connected with remote port 03208 (eKERNEL)
O:TCP:<xml><cfgrqs><appl>eIO</appl><site>2</site><version>2.0.5</version></cfgr
I:TCP:<xml><cfgrpy><manufacturer>NATIONAL INSTRUMENTS</manufacturer><model>*BAS
S:TCP:FP-AI-100 - module 01 - contact 01 - Connecting: Parsing URL.
S:TCP:FP-AI-100 - module 01 - contact 01 - Connecting: Connecting to OPC Server
S:TCP:FP-AI-100 - module 01 - contact 01 - Active: Connected to OPC Server.
S:TCP:FP-AI-100 - module 01 - contact 02 - Connecting: Parsing URL.
S:TCP:FP-AI-100 - module 01 - contact 02 - Connecting: Connecting to OPC Server
S:TCP:FP-AI-100 - module 01 - contact 02 - Active: Connected to OPC Server.
S:TCP:FP-AI-100 - module 01 - contact 03 - Connecting: Parsing URL.
```

Data arrival - 1914 bytes received from eKERNEL | 00010 | 18:32:49

Figure 376
eIO connections



eKernel

Local	10.110.53.138	1050
Remote	10.110.53.138	3208
Status	Connected	

eIO

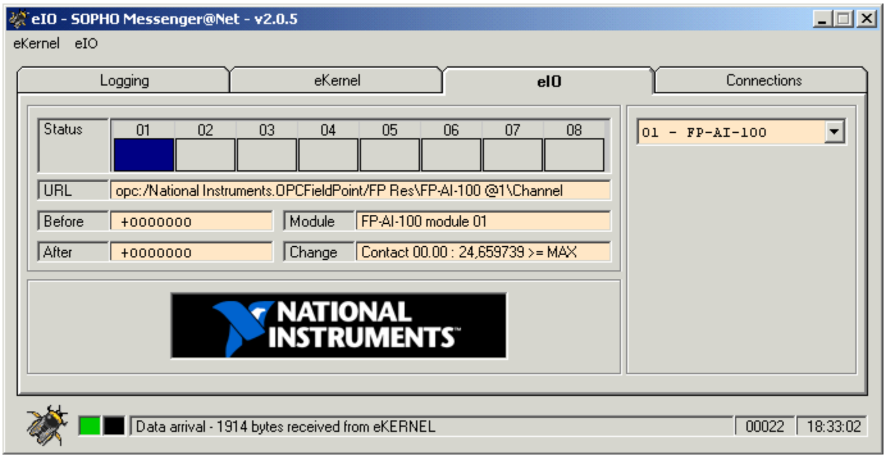
	N/A	N/A
	N/A	N/A

Configuration

Manufacturer	NATIONAL INSTRUMENTS
Model	*BASE
Modules	01 - FP-AI-100 02 - FP-DI-300 03 - FP-DO-401
Log path	C:\SOPHO Messenger@Net
Log days	14

Data arrival - 1914 bytes received from eKERNEL | 00095 | 18:34:14

Figure 377
Analogue input module



URL: opc:/National Instruments.OPCFieldPoint/FP Res\FP-AI-100 @1\Channel

Before: +0000000

Module: FP-AI-100 module 01

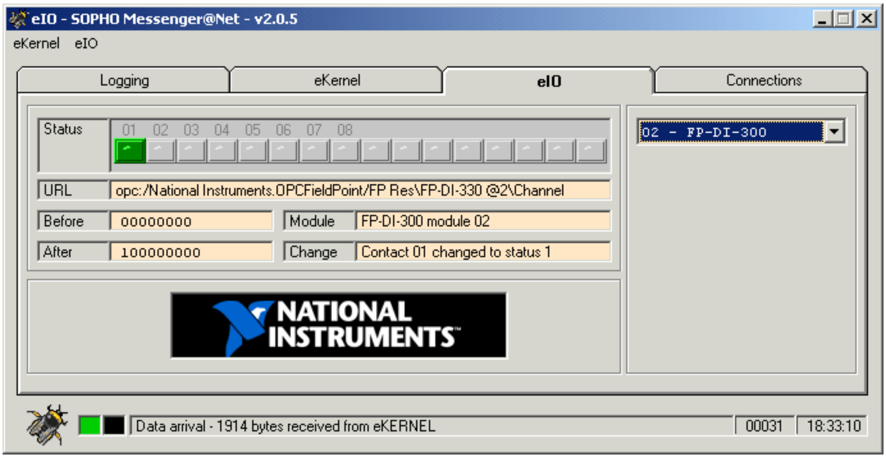
After: +0000000

Change: Contact 00.00 : 24,659739 >= MAX

01 - FP-AI-100

Data arrival - 1914 bytes received from eKERNEL 00022 18:33:02

Figure 378
Digital input module



URL: opc:/National Instruments.OPCFieldPoint/FP Res\FP-DI-330 @2\Channel

Before: 00000000

Module: FP-DI-300 module 02

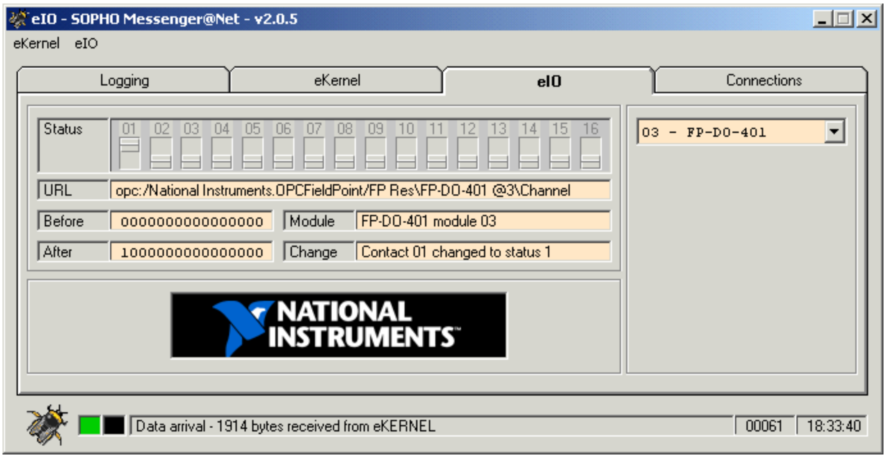
After: 100000000

Change: Contact 01 changed to status 1

02 - FP-DI-300

Data arrival - 1914 bytes received from eKERNEL 00031 18:33:10

Figure 379
Digital output module



URL: opc:/National Instruments.OPCFieldPoint/FP Res\FP-DO-401 @3\Channel

Before: 0000000000000000

Module: FP-DO-401 module 03

After: 1000000000000000

Change: Contact 01 changed to status 1

03 - FP-DO-401

Data arrival - 1914 bytes received from eKERNEL | 00061 | 18:33:40

Accessing troubleshooting resources

In case of problems, you can consult the www.ni.com for more information. The content of two documents from this repository are provided in:

- “Why Does the FP-1600/2000/2010 Have Problems Configuring in Computers with 2 Ethernet Ports?”
- Minimizing and Suppressing Noise (EMI) In the FieldPoint FP-1600/ 2000/2010 Ethernet Cable (p. 948)

Why Does the FP-1600/2000/2010 Have Problems Configuring in Computers with 2 Ethernet Ports?

Product Group: FieldPoint Hardware

Product Name: FP-1600

Version/Revision: N/A

Problem: In computers that use two Ethernet cards, attempts to configure an FP-1600/2000/2010 sometimes results in the message, “no response from module.” I am trying to assign an IP address to my FieldPoint 1600 module.

It shows up as Unconfigured, but when I try to assign the IP address, I see the message "Module not responding." What is wrong?

Solution: This can be caused by a variety of factors. First, in a two Ethernet port system, both ports must be configured with mutually exclusive subnets. There can be no overlap in the subnet addresses of the two ports; however, even when this is properly configured, there are frequently problems with configuring the FP-1600/2000/2010.

This is due to a limitation with the Microsoft TCP/IP stack (as tested under Windows 98 and Windows NT4 SP5). A typical message contains source, destination, and data information. When sending out broadcast messages, the Microsoft TCP/IP stack places the same source address in the messages going out both ports (that is, the address of the first port in the stack is used), rather than using the appropriate source address for each port. Thus, an FP-1600/2000/2010 trying to respond to the message is trying to respond to the wrong port, because that is the address received. This happens only with broadcast messages. FieldPoint uses broadcast messages while configuring a module. When the module is configured, point-to-point messages are used to communicate with the module.

There are several ways to work around the broadcast limitation while configuring the module.

- Workaround 1: Place the module on the other Ethernet card for configuration.
- Workaround: 2: Use a computer that has only one Ethernet card for configuration.
- Workaround 3: Remove the Ethernet drivers for both cards, then reinstall the drivers with the board that talks to the FP-1600 being installed first.
- Workaround 4: If your system uses two plug-in Ethernet cards (not integrated on the computer motherboard), then swap the positions of the two cards.

Note 1: Broadcast messages pass through both ports simultaneously, whereas point-to-point messages go out a single port, based on the address information.

Note 2: This affects only the configuration of the IP settings of an FP-1600/2000/2010, but does not affect normal communications.

After configuration, you can use two Ethernet cards on a single computer to communicate to a FieldPoint network module, but only if the cards are configured with mutually exclusive subnets. This is because point-to-point communications are transmitted out single ports based on the subnet masks for the network cards. During configuration the FieldPoint network modules are not assigned IP addresses, so broadcast messaging is used through both ports.

Related Links:
Developer Zone Tutorial: Troubleshooting Communication Problems with the FP-1600 at zone.ni.com/zone/jsp/zone.jsp.

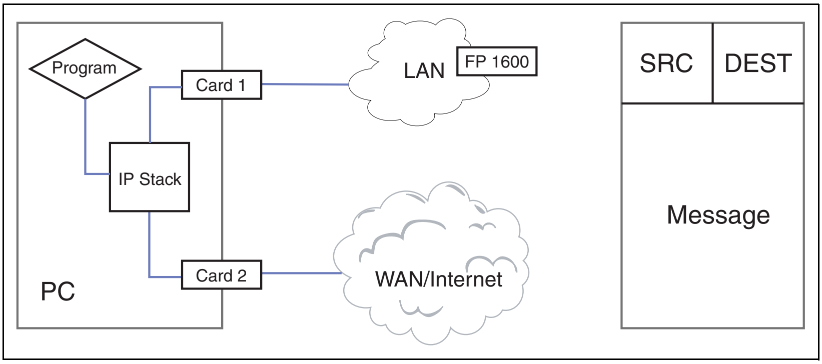
Fixed Version:

Report Date: 09/06/2000

Last Updated: 30/09/2002

Document ID: 1Y8CJDEB

Attachments:



Minimizing and Suppressing Noise (EMI) In the FieldPoint FP-1600/2000/2010 Ethernet Cable

Product Group: FieldPoint Hardware

Product Name: FP-1600, FP-2000, FP-2010

Version/Revision: N/A

Problem: Noise from a nearby fluorescent light or machine is interfering with the communication of my FieldPoint Ethernet network module. How do I suppress this noise?

Solution:

1 Place a snap-on ferrite noise suppressor on the Ethernet cable. Install the suppressor, using one half-turn (one pass-through) and place the suppressor within 10 cm of the network module. You can purchase a ferrite EMI suppressor from Fair-Rite Products (manufacturer part number: 0443164251, available through the web site www.fair-rite.com).

2 Install the entire FieldPoint bank in an EMC-rated enclosure or in an earth-grounded cabinet. Shield all other I/O and control lines connected to your FieldPoint Ethernet network module with EMC rated cable raceway or metal conduit.

Related Links:
Fair-Rite Products web site at www.fair-rite.com

Fixed Version:

Report Date: 14/06/2001

Last Updated: 20/11/2003

Document ID: 2ADF2T8T

For more information go to the National Instruments web site at www.ni.com.

Install PC – Step 4 – Web Server

This chapter provides information on the following topics:

This section is required only if you install the eWEB module.

Installing ODBC

Nortel DECT Messenger requires *two* ODBC System DSN configurations; one to access the Messenger_CFG database and one to access the Messenger_DATA database.

IMPORTANT!

> The Messenger_CFG database is supported only through Microsoft Access Driver. The Messenger_DATA database is supported through Microsoft Access Driver and through SQL Server driver. You must determine whether you plan to use Microsoft Access or SQL Server prior to continuing. This setting must match the definitions in Messenger_CFG table eKERNEL_Site, as follows:

- Example of Microsoft Access

  Provider=Microsoft.Jet.OLEDB.4.0;Data Source=C:\Nortel DECT Messenger\Mdb\Messenger_DATA.MDB

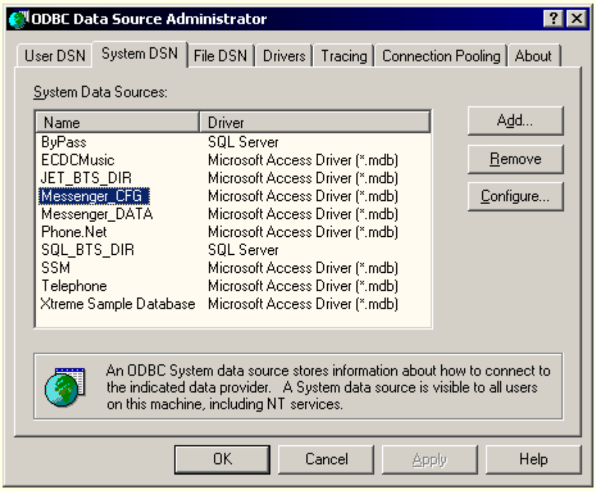
- Example of SQL Server

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

Procedure 229
Configuring Messenger CFG database (Part 1 of 4)

Step	Action
1	Launch the Open Database Connectivity (OBDC) Administrator tool.
	Click the **Start** button on the Windows taskbar, and choose **Settings > Control Panel > Administrative Tools > Data Sources (ODBC)**.

Procedure 229
Configuring Messenger CFG database (Part 2 of 4)

Step	Action
2	Open the **OBDC Setup** window for Messenger_CFG.
	• Click the **System DSN** tab. • Click **Add**. 

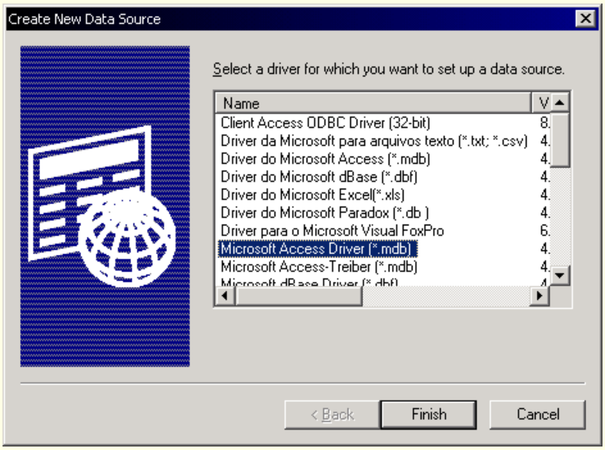
ODBC Data Source Administrator

System Data Sources:

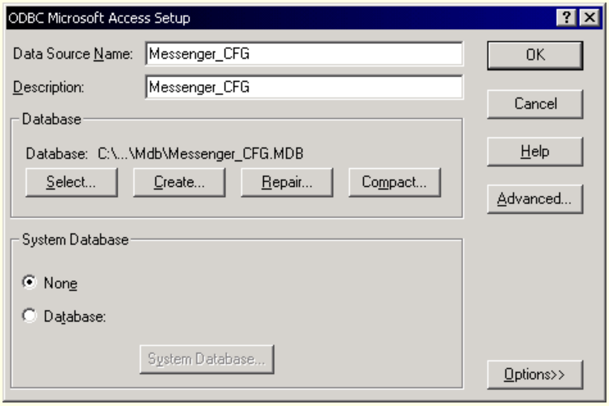
Name	Driver
ByPass	SQL Server
ECDCMusic	Microsoft Access Driver (*.mdb)
JET_BTS_DIR	Microsoft Access Driver (*.mdb)
Messenger_CFG	Microsoft Access Driver (*.mdb)
Messenger_DATA	Microsoft Access Driver (*.mdb)
Phone.Net	Microsoft Access Driver (*.mdb)
SQL_BTS_DIR	SQL Server
SSM	Microsoft Access Driver (*.mdb)
Telephone	Microsoft Access Driver (*.mdb)
Xtreme Sample Database	Microsoft Access Driver (*.mdb)

An ODBC System data source stores information about how to connect to the indicated data provider. A System data source is visible to all users on this machine, including NT services.

Procedure 229
Configuring Messenger CFG database (Part 3 of 4)

Step	Action
3	Select the driver.
	• Choose **Microsoft Access Driver (*.mdb)** from the list. • Click **Finish**.  Create New Data Source Select a driver for which you want to set up a data source. Name — V Client Access ODBC Driver (32-bit) — 8. Driver da Microsoft para arquivos texto (*.txt; *.csv) — 4. Driver do Microsoft Access (*.mdb) — 4. Driver do Microsoft dBase (*.dbf) — 4. Driver do Microsoft Excel(*.xls) — 4. Driver do Microsoft Paradox (*.db) — 4. Driver para o Microsoft Visual FoxPro — 6. Microsoft Access Driver (*.mdb) — 4. Microsoft Access-Treiber (*.mdb) — 4. Microsoft dBase Driver (*.dbf) — 4

Procedure 229
Configuring Messenger CFG database (Part 4 of 4)

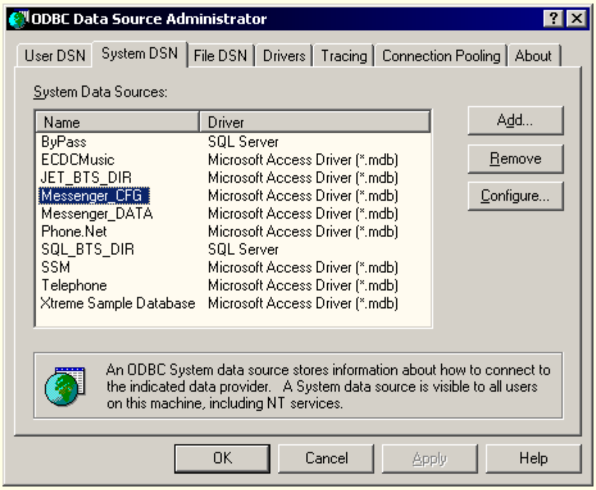
Step	Action
4	Enter parameters and set the database path
	- Enter the parameters as specified in the following dialog box:  ODBC Microsoft Access Setup Data Source Name: Messenger_CFG Description: Messenger_CFG Database Database: C:\...\Mdb\Messenger_CFG.MDB System Database ● None ○ Database: OK Cancel Help Advanced... Select... Create... Repair... Compact... System Database... Options>> - Click **Select** and specify the appropriate configuration database: C:\SOPHO Messenger@Net\Mdb\Messenger_CFG.Mdb.

END

IMPORTANT!

Remember to define the second DSN.

Procedure 230
Configuring Messenger DATA database using Microsoft Access Driver (Part 1 of 3)

Step	Action
1	Launch the Open Database Connectivity (OBDC) Administrator tool.
	Click the **Start** button on the Windows taskbar, and choose **Settings > Control Panel > Administrative Tools > Data Sources (ODBC)**.
2	Open the OBDC Setup window for Messenger_DATA.
	• Click the **System DSN** tab. • Click **Add**. 

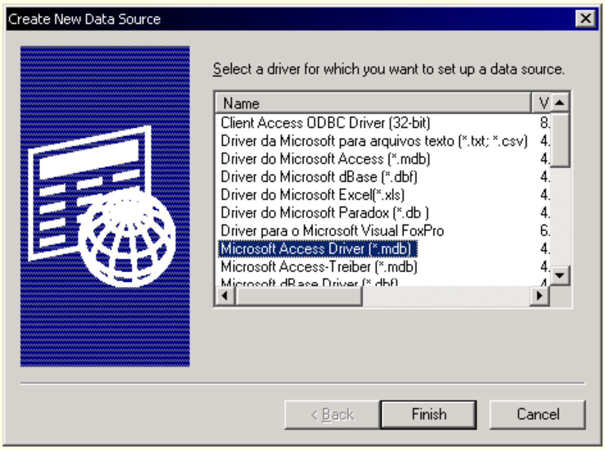
ODBC Data Source Administrator

System Data Sources:

Name	Driver
ByPass	SQL Server
ECDCMusic	Microsoft Access Driver (*.mdb)
JET_BTS_DIR	Microsoft Access Driver (*.mdb)
Messenger_CFG	Microsoft Access Driver (*.mdb)
Messenger_DATA	Microsoft Access Driver (*.mdb)
Phone.Net	Microsoft Access Driver (*.mdb)
SQL_BTS_DIR	SQL Server
SSM	Microsoft Access Driver (*.mdb)
Telephone	Microsoft Access Driver (*.mdb)
Xtreme Sample Database	Microsoft Access Driver (*.mdb)

An ODBC System data source stores information about how to connect to the indicated data provider. A System data source is visible to all users on this machine, including NT services.

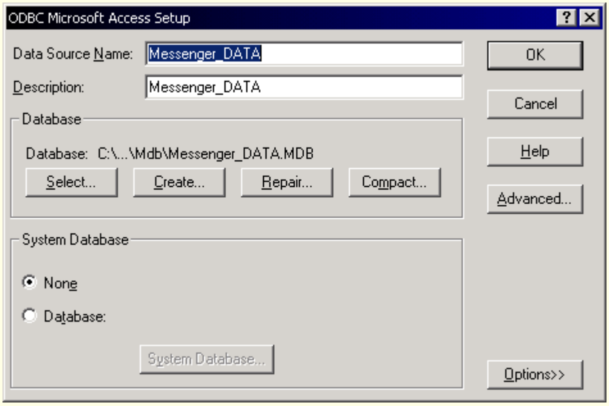
Procedure 230
Configuring Messenger DATA database using Microsoft Access Driver (Part 2 of 3)

Step	Action
3	Select the driver.
	• Choose Microsoft Access Driver (*.mdb) from the list. • Click **Finish**. 

Select a driver for which you want to set up a data source.

Name	V
Client Access ODBC Driver (32-bit)	8.
Driver da Microsoft para arquivos texto (*.txt; *.csv)	4.
Driver do Microsoft Access (*.mdb)	4.
Driver do Microsoft dBase (*.dbf)	4.
Driver do Microsoft Excel(*.xls)	4.
Driver do Microsoft Paradox (*.db)	4.
Driver para o Microsoft Visual FoxPro	6.
Microsoft Access Driver (*.mdb)	4.
Microsoft Access-Treiber (*.mdb)	4.
Microsoft dBase Driver (*.dbf)	4.

Procedure 230
Configuring Messenger DATA database using Microsoft Access Driver (Part 3 of 3)

Step	Action
4	Enter parameters and set the database path.
	- Enter the parameters as specified in the following dialog box:  ODBC Microsoft Access Setup OK Cancel Help Advanced... Database Select... Create... Repair... Compact... System Database System Database... Options>> Data Source Name: Messenger_DATA Description: Messenger_DATA Database: C:\...\Mdb\Messenger_DATA.MDB ● None ○ Database: - Click **Select** and specify the appropriate configuration database: C:\SOPHO Messenger@Net\Mdb\Messenger_DATA.mdb

END

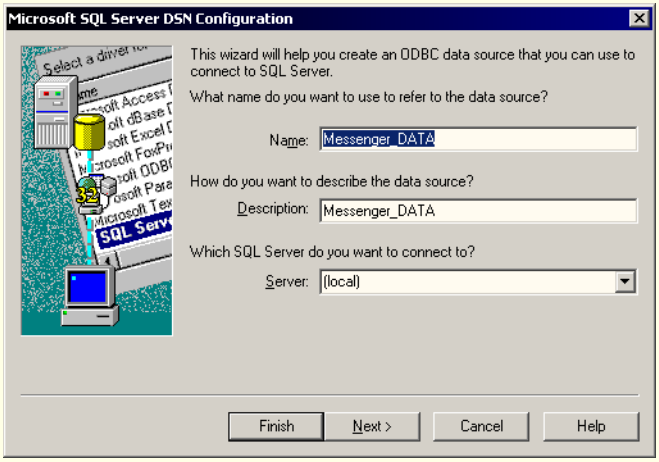
If you plan to use SQL Server

Before you can configure the SQL Server, you must determine the user and password to access the SQL Server to ensure they match the settings described in the connection string as follows:

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

In the foregoing example, user =sa and password = sa. Nortel recommends that you select a new password during the setup of SQL Server.

Procedure 231
Configuring Messenger DATA database using SQL Server (Part 1 of 7)

Step	Action
1	Start the Configuration wizard.
	Start the SQL Server DSN Configuration wizard.
2	Set the data source name and description.
	• Fill in the **Name** and **Description** fields. • Click **Next** to continue. 

Microsoft SQL Server DSN Configuration

This wizard will help you create an ODBC data source that you can use to connect to SQL Server.

What name do you want to use to refer to the data source?

Name: Messenger_DATA

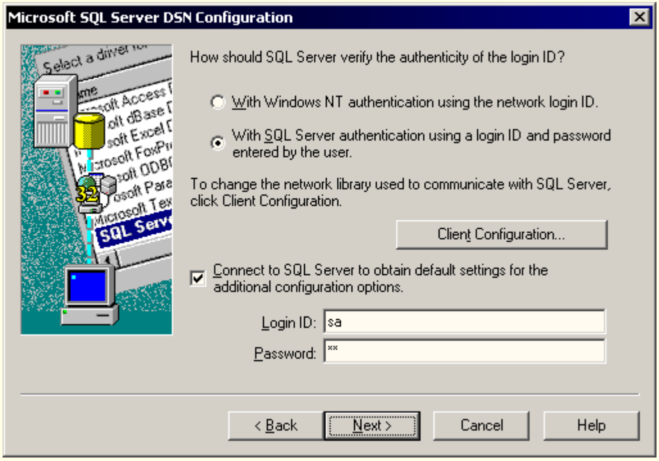
How do you want to describe the data source?

Description: Messenger_DATA

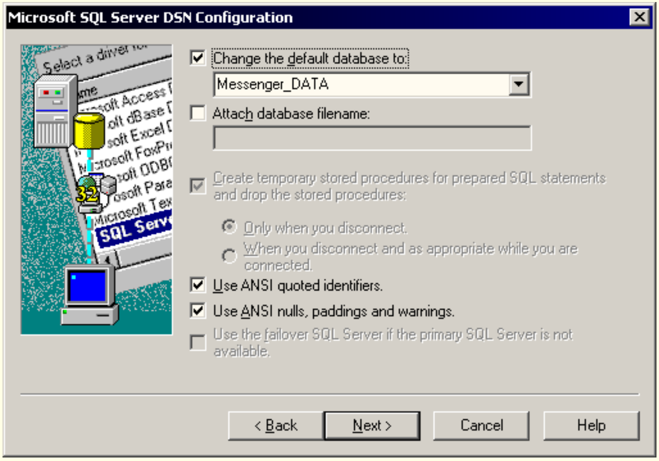
Which SQL Server do you want to connect to?

Server: (local)

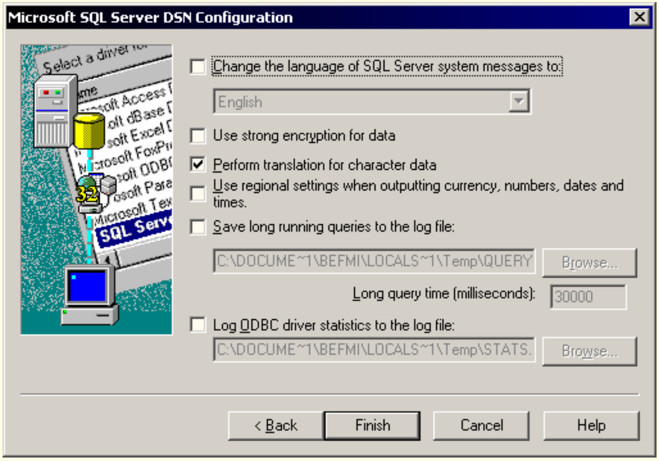
Procedure 231
Configuring Messenger DATA database using SQL Server (Part 2 of 7)

Step	Action
3	Choose the login verification method and configuration options.
	- Choose options as shown in the following dialog box:  Microsoft SQL Server DSN Configuration How should SQL Server verify the authenticity of the login ID? ○ With Windows NT authentication using the network login ID. ● With SQL Server authentication using a login ID and password entered by the user. To change the network library used to communicate with SQL Server, click Client Configuration. ☑ Connect to SQL Server to obtain default settings for the additional configuration options. Login ID: sa Password: ** Client Configuration... < Back Next > Cancel Help - Click **Next** to continue.

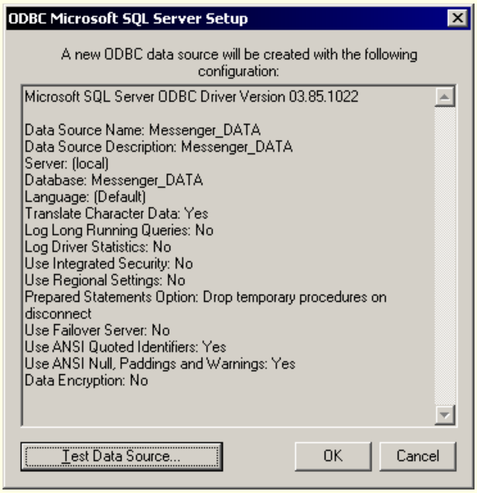
Procedure 231
Configuring Messenger DATA database using SQL Server (Part 3 of 7)

Step	Action
4	Set the default database.
	- Choose options as shown in the following dialog box:  Microsoft SQL Server DSN Configuration ☑ Change the default database to: Messenger_DATA ☐ Attach database filename: ☑ Create temporary stored procedures for prepared SQL statements and drop the stored procedures: ● Only when you disconnect. ○ When you disconnect and as appropriate while you are connected. ☑ Use ANSI quoted identifiers. ☑ Use ANSI nulls, paddings and warnings. ☐ Use the failover SQL Server if the primary SQL Server is not available. - Click **Next** to continue.

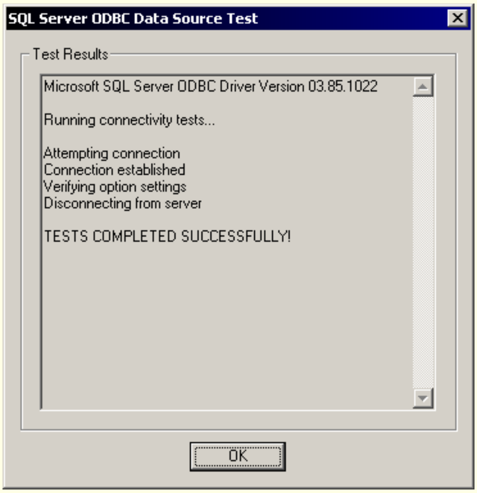
Procedure 231
Configuring Messenger DATA database using SQL Server (Part 4 of 7)

Step	Action
5	Set regional and language options.
	- Choose options as shown in the following dialog box: Microsoft SQL Server DSN Configuration □ Change the language of SQL Server system messages to: English □ Use strong encryption for data ☑ Perform translation for character data □ Use regional settings when outputting currency, numbers, dates and times. □ Save long running queries to the log file: C:\DOCUME~1\BEFMI\LOCALS~1\Temp\QUERY Long query time (milliseconds): 30000 □ Log ODBC driver statistics to the log file: C:\DOCUME~1\BEFMI\LOCALS~1\Temp\STATS. Browse... Browse... < Back Finish Cancel Help - Click **Finish** to complete the configuration.

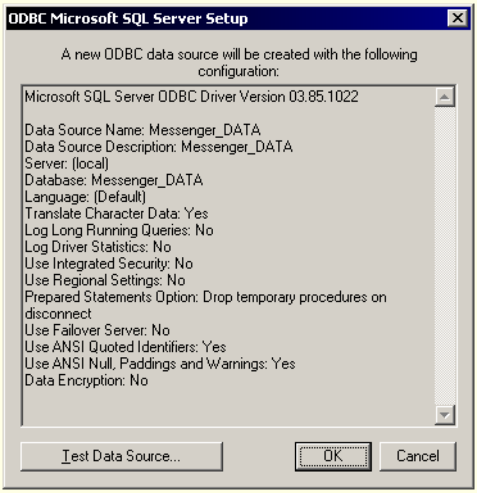
Procedure 231
Configuring Messenger DATA database using SQL Server (Part 5 of 7)

Step	Action
6	Test the connection to the data source.
	Click **Test Data Source**.  ODBC Microsoft SQL Server Setup A new ODBC data source will be created with the following configuration: Microsoft SQL Server ODBC Driver Version 03.85.1022 Data Source Name: Messenger_DATA Data Source Description: Messenger_DATA Server: (local) Database: Messenger_DATA Language: (Default) Translate Character Data: Yes Log Long Running Queries: No Log Driver Statistics: No Use Integrated Security: No Use Regional Settings: No Prepared Statements Option: Drop temporary procedures on disconnect Use Failover Server: No Use ANSI Quoted Identifiers: Yes Use ANSI Null, Paddings and Warnings: Yes Data Encryption: No

Procedure 231
Configuring Messenger DATA database using SQL Server (Part 6 of 7)

Step	Action
7	Review test results.
	If SQL Server is set up correctly, the test results resemble those shown in the following dialog box: - Click **OK**.  Microsoft SQL Server ODBC Driver Version 03.85.1022 Running connectivity tests... Attempting connection Connection established Verifying option settings Disconnecting from server TESTS COMPLETED SUCCESSFULLY!

Procedure 231
Configuring Messenger DATA database using SQL Server (Part 7 of 7)

Step	Action
8	Review the configuration settings.
	Click **OK**.  ODBC Microsoft SQL Server Setup A new ODBC data source will be created with the following configuration: Microsoft SQL Server ODBC Driver Version 03.85.1022 Data Source Name: Messenger_DATA Data Source Description: Messenger_DATA Server: (local) Database: Messenger_DATA Language: (Default) Translate Character Data: Yes Log Long Running Queries: No Log Driver Statistics: No Use Integrated Security: No Use Regional Settings: No Prepared Statements Option: Drop temporary procedures on disconnect Use Failover Server: No Use ANSI Quoted Identifiers: Yes Use ANSI Null, Paddings and Warnings: Yes Data Encryption: No
	END

Installing Apache Web Server 2.0.50

If installing Apache Web Server on a Windows 2000 Server operating system, STOP the default web server before installing Apache, as follows:

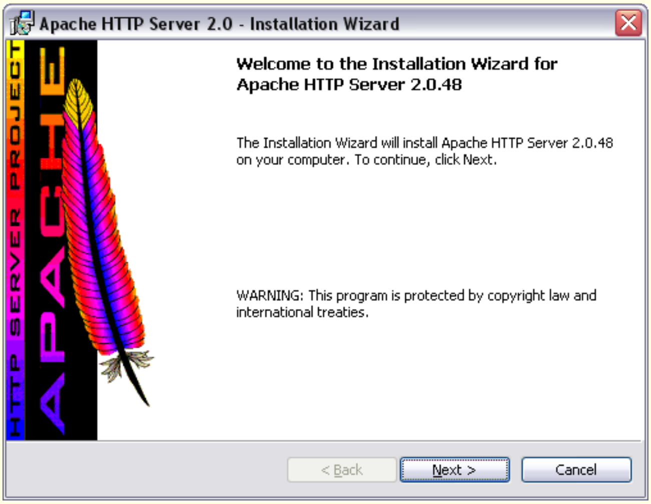
1 Click **Start** on the Windows taskbar, and choose **Settings** > **Control Panel** > **Administrative Tools** > **Internet Services Manager**

2 Right-click **Default Web Site** and choose **Stop**.

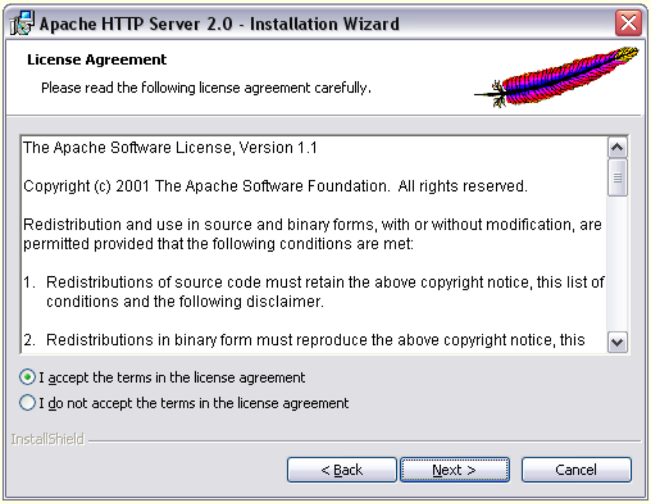
Procedure 232
Install Apache Web Server (Part 1 of 9)

Step	Action
1	Start the installation wizard.
	• On the CD-ROM, open the folder: \Step 5 – Web Server > Step 5a - Apache > Apache Web Server 2.0.50. • Double-click the file apache_2.0.50-win32-x86-no_ssl.msi.

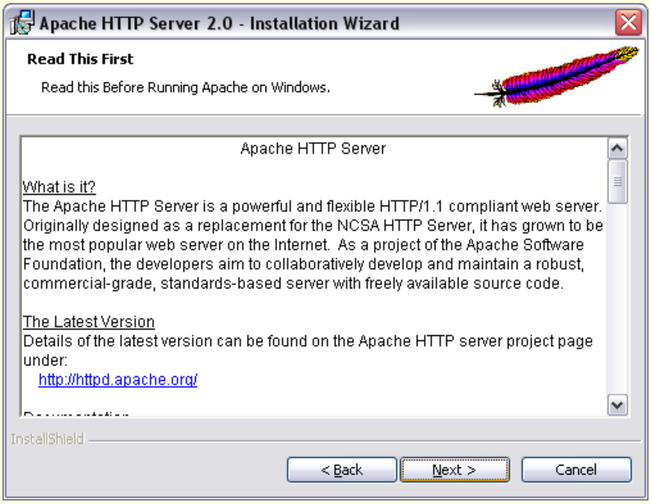
Procedure 232
Install Apache Web Server (Part 2 of 9)

Step	Action
2	Begin the installation.
	Click **Next**.  Apache HTTP Server 2.0 - Installation Wizard **Welcome to the Installation Wizard for Apache HTTP Server 2.0.48** The Installation Wizard will install Apache HTTP Server 2.0.48 on your computer. To continue, click Next. WARNING: This program is protected by copyright law and international treaties.

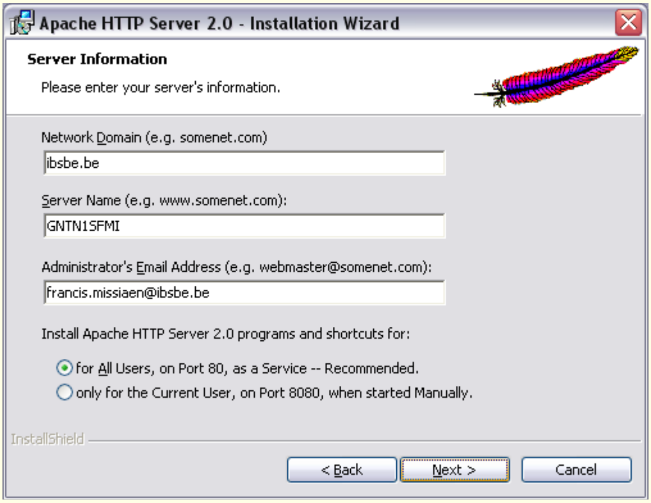
Procedure 232
Install Apache Web Server (Part 3 of 9)

Step	Action
3	Accept the Licence Agreement.
	Click **Next**.  Apache HTTP Server 2.0 - Installation Wizard **License Agreement** Please read the following license agreement carefully. The Apache Software License, Version 1.1 Copyright (c) 2001 The Apache Software Foundation. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met: 1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer. 2. Redistributions in binary form must reproduce the above copyright notice, this ● I accept the terms in the license agreement ○ I do not accept the terms in the license agreement

Procedure 232
Install Apache Web Server (Part 4 of 9)

Step	Action
4	Review the Apache information.
	Read the information provided and click **Next**.  Apache HTTP Server 2.0 - Installation Wizard **Read This First** Read this Before Running Apache on Windows. Apache HTTP Server What is it? The Apache HTTP Server is a powerful and flexible HTTP/1.1 compliant web server. Originally designed as a replacement for the NCSA HTTP Server, it has grown to be the most popular web server on the Internet. As a project of the Apache Software Foundation, the developers aim to collaboratively develop and maintain a robust, commercial-grade, standards-based server with freely available source code. The Latest Version Details of the latest version can be found on the Apache HTTP server project page under: http://httpd.apache.org/

Procedure 232
Install Apache Web Server (Part 5 of 9)

Step	Action
5	Enter Server Information.
	Enter the domain name, server name and e-mail address. In most cases you can accept the default settings, which are retrieved from the current Windows settings. These values are appropriate for most installations. If your network administrator chooses tighter integration of DECT Messenger in the existing network, you must adapt your settings to those provided by the network administrator. In the following dialog box, the system is defined to be a member of a domain (in this example, ibsbe.be), and is assigned the identifier GNTN1SFMI with indication to append the DNS-suffix ibsbe.be. To find out your network identification and domain name settings, click **Start**, and choose **Settings > Control Panel > System > Network Identification**. 

Apache HTTP Server 2.0 - Installation Wizard

Server Information

Please enter your server's information.

Network Domain (e.g. somenet.com)
ibsbe.be

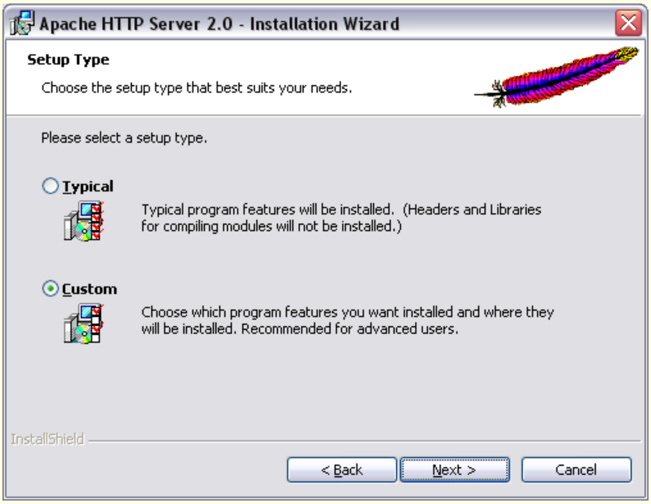
Server Name (e.g. www.somenet.com):
GNTN1SFMI

Administrator's Email Address (e.g. webmaster@somenet.com):
francis.missiaen@ibsbe.be

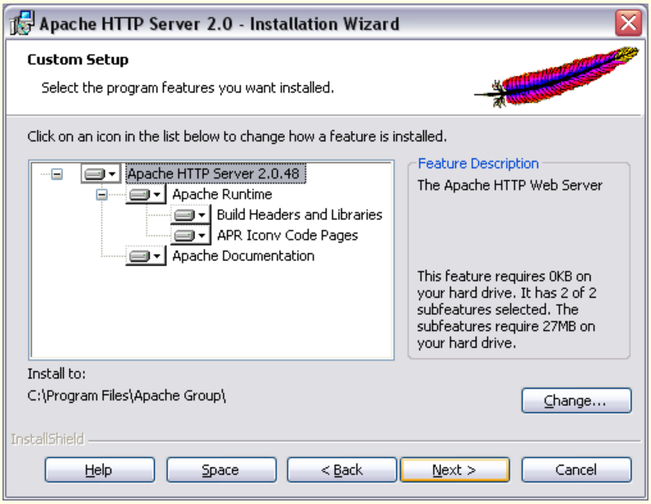
Install Apache HTTP Server 2.0 programs and shortcuts for:

● for All Users, on Port 80, as a Service -- Recommended.
○ only for the Current User, on Port 8080, when started Manually.

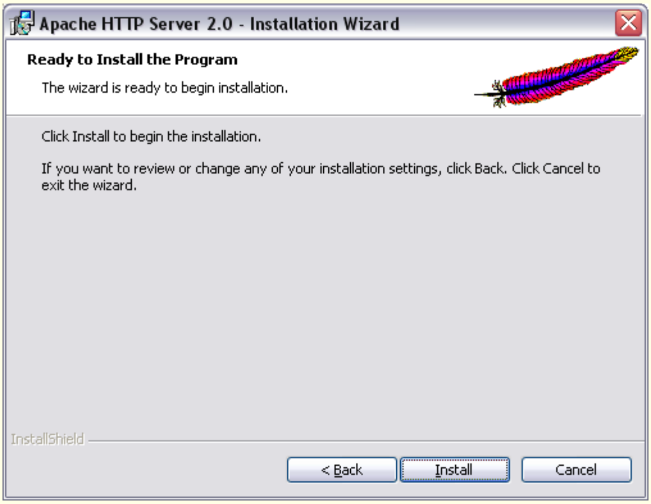
Procedure 232
Install Apache Web Server (Part 6 of 9)

Step	Action
6	Choose Setup Type.
	Select **Custom** and click **Next**.  Apache HTTP Server 2.0 - Installation Wizard **Setup Type** Choose the setup type that best suits your needs. Please select a setup type. ○ **Typical** Typical program features will be installed. (Headers and Libraries for compiling modules will not be installed.) ● **Custom** Choose which program features you want installed and where they will be installed. Recommended for advanced users. InstallShield < Back | Next > | Cancel

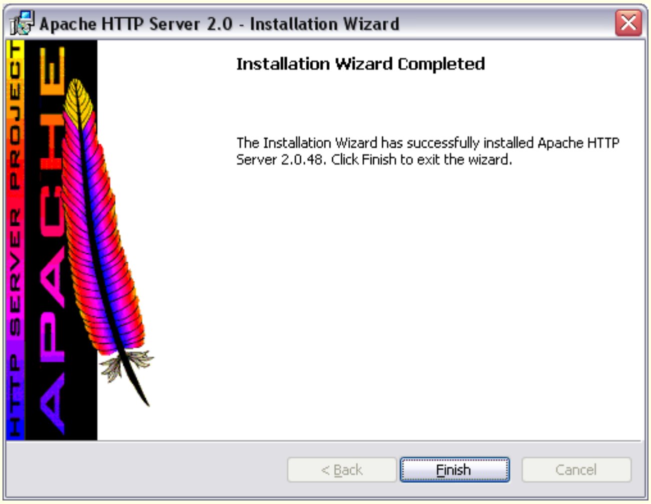
Procedure 232
Install Apache Web Server (Part 7 of 9)

Step	Action
7	Select the features you want to install.
	Click **Next** to continue.  Apache HTTP Server 2.0 - Installation Wizard **Custom Setup** Select the program features you want installed. Click on an icon in the list below to change how a feature is installed. Apache HTTP Server 2.0.48 Apache Runtime Build Headers and Libraries APR Iconv Code Pages Apache Documentation Feature Description The Apache HTTP Web Server This feature requires 0KB on your hard drive. It has 2 of 2 subfeatures selected. The subfeatures require 27MB on your hard drive. Install to: C:\Program Files\Apache Group\ Change... InstallShield Help Space < Back Next > Cancel

Procedure 232
Install Apache Web Server (Part 8 of 9)

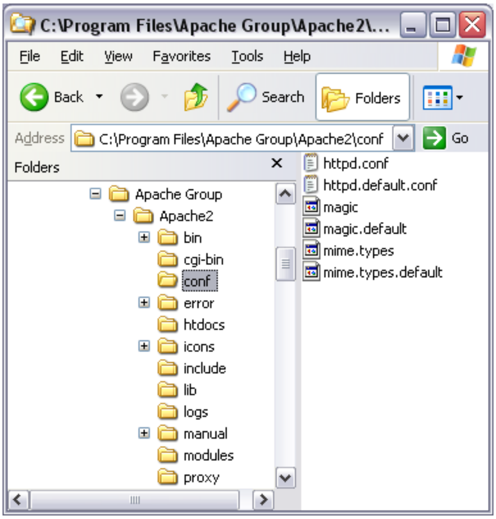
Step	Action
8	Begin copying files.
	Click **Install** to continue.  Apache HTTP Server 2.0 - Installation Wizard Ready to Install the Program The wizard is ready to begin installation. Click Install to begin the installation. If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.

Procedure 232
Install Apache Web Server (Part 9 of 9)

Step	Action
9	Acknowledge the completion of the installation.
	Click **Finish**.  Apache HTTP Server 2.0 - Installation Wizard **Installation Wizard Completed** The Installation Wizard has successfully installed Apache HTTP Server 2.0.48. Click Finish to exit the wizard.
	END

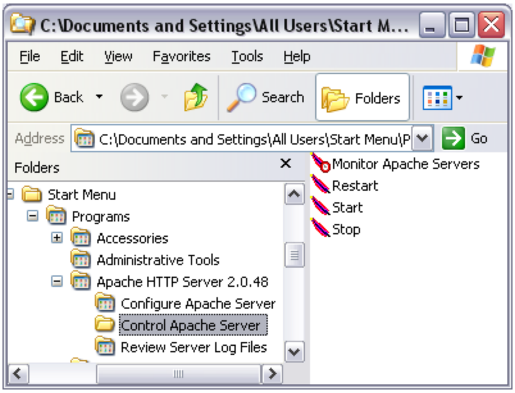
As part of the installation procedure, a number of resources are installed in C:\Program Files\Apache Group\Apache2, as shown in Figure 380 on page 973.

Figure 380
Resources installed with Apache 2.0



The start-up group contains a number of shortcuts, as shown in Figure 381 on page 973, among which **Monitor Apache Servers** is the most important one. This process is also shown as an icon in the system tray of your desktop.

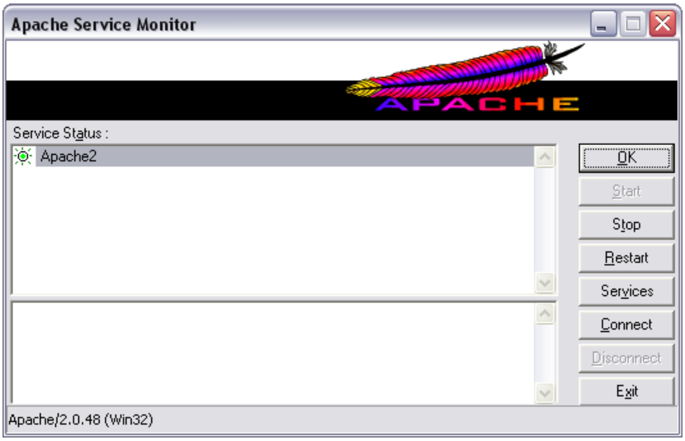
Figure 381
Start-up items added by Apache 2.0



If you accidentally close the Apache Monitor in the system tray, the path of the Apache Monitor (see Figure 382) is as follows:

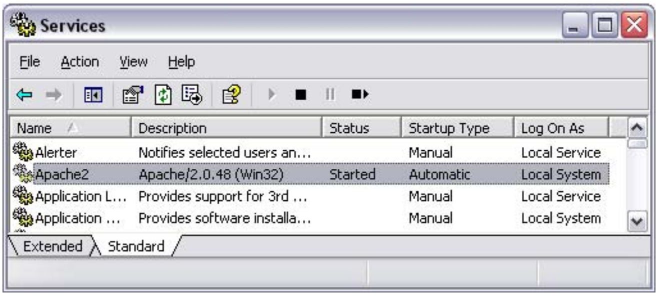
C:\Program Files\Apache Group\Apache2\bin\ApacheMonitor.exe

Figure 382
Apache Service Monitor



Note: The procedure in Table 232 on page 964 installs Apache as a service, with server instance name Apache2 as shown in Figure 383 on page 975.

Figure 383
Apache server instance name



Name	Description	Status	Startup Type	Log On As
Alerter	Notifies selected users an...		Manual	Local Service
Apache2	Apache/2.0.48 (Win32)	Started	Automatic	Local System
Application L...	Provides support for 3rd ...		Manual	Local Service
Application ...	Provides software installa...		Manual	Local System

IMPORTANT!

To preserve a dedicated Apache Web Server environment for DECT Messenger, you must perform the steps described in Table 233 on page 976. Do not skip any of these installation instructions.

Preserving a dedicated Apache Web Server environment

During installation of Apache web server, a new server instance called Apache2 is installed. To verify this, open the Apache Monitor that runs in the system tray:

```
C:\Program Files\Apache
Group\Apache2\bin\ApacheMonitor.exe
```

Next, you must configure a new web server instance called Messenger@Net to work with the Nortel Messenger.

Procedure 233
Preserving a dedicated Apache Web Server environment for DECT Messenger (Part 1 of 2)

Step	Action
1	Stop the default Apache2 server instance.
	• Click on the Apache Service Monitor in the system tray; the following options are listed: — **Start** — **Stop** — **Restart** • Choose **Stop**.
2	Remove the default Apache2 server instance.
	• Browse to the following folder on the Installation CD2: \Step 4 - WebServer\Step 4a - Apache\Config files • Double-click the file Remove Apache2 Server Instance. To verify if the action was successful, check the Apache Service Monitor. If the instance was removed successfully, no server instance is shown.
3	Create a new server instance configuration.
	• Browse to the following folder on the installation CD2: \Step 4 - WebServer\Step 4a - Apache\Config files • Copy the file httpd_Messenger@Net.conf • Paste the file into C:\Program Files\Apache Group\Apache2\conf\

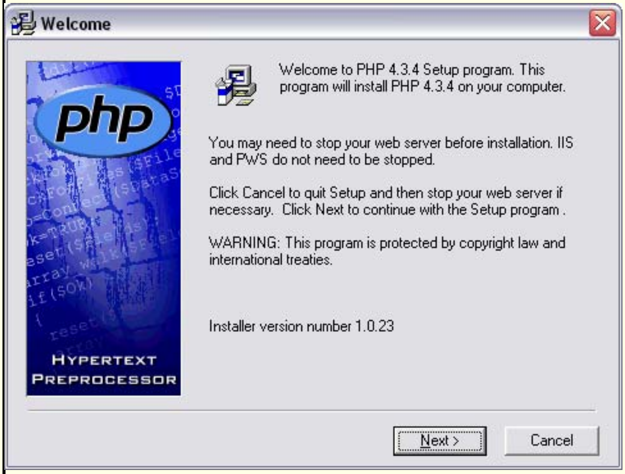
Procedure 233
Preserving a dedicated Apache Web Server environment for DECT Messenger (Part 2 of 2)

Step	Action
4	Install the server instance.
	• Browse to the following folder on the Installation CD2: \Step 5 – WebServer\Step 5a – Apache\Config files • Double-click the file Install Messenger@Net Server Instance. To verify if the action was successful, check the Apache Service Monitor. If the installation was successful, a Messenger@Net server instance is shown.
5	Start the DECT Messenger server instance.
	• Browse to the following folder on the Installation CD2: \Step 4 - WebServer\Step 4a - Apache\Config files • Double-click the file Start Messenger@Net Server Instance. To verify if the action was successful, check the Apache Service Monitor. If the server instance started successfully, a Messenger@Net server instance is shown with the status Started.
	END

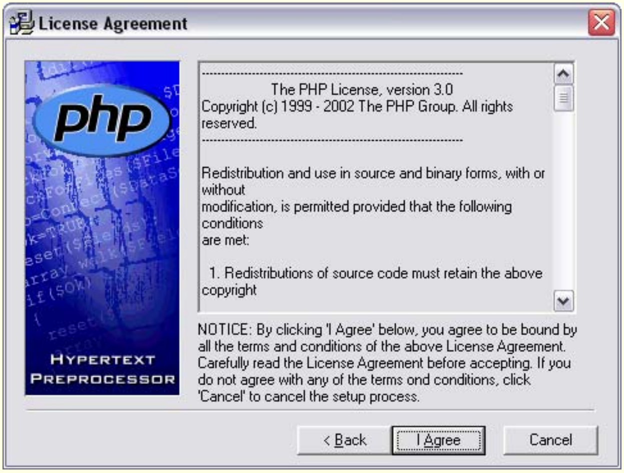
Installing PHP

The PHP engine must be installed separately, as follows.

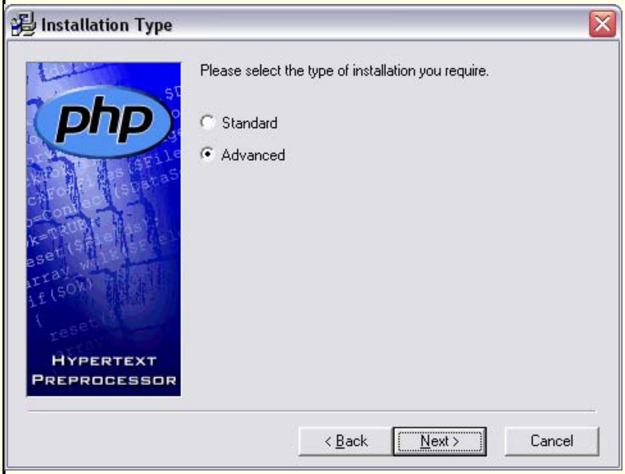
Procedure 234
Install PHP (Part 1 of 13)

Step	Action
1	Start the PHP installer.
	• Browse to the following folder on the CD-ROM: Step 5 - Web Server/Step 5b – PHP/PHP 4.3.8 • Double-click php-4.3.8-installer.exe.
2	Begin the installation.
	Click **Next** to continue.  Welcome to PHP 4.3.4 Setup program. This program will install PHP 4.3.4 on your computer. You may need to stop your web server before installation. IIS and PWS do not need to be stopped. Click Cancel to quit Setup and then stop your web server if necessary. Click Next to continue with the Setup program . WARNING: This program is protected by copyright law and international treaties. Installer version number 1.0.23

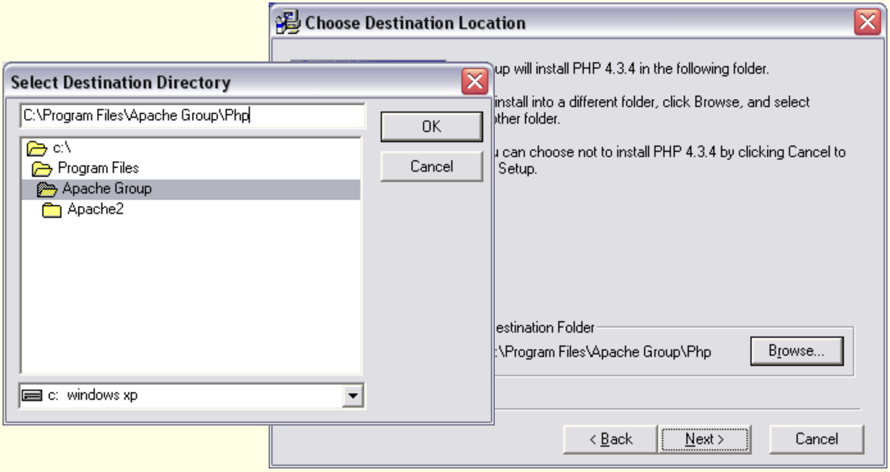
Procedure 234
Install PHP (Part 2 of 13)

Step	Action
3	Accept the Licence Agreement.
4	Click **I Agree**.  License Agreement --- The PHP License, version 3.0 Copyright (c) 1999 - 2002 The PHP Group. All rights reserved. --- Redistribution and use in source and binary forms, with or without modification, is permitted provided that the following conditions are met: 1. Redistributions of source code must retain the above copyright NOTICE: By clicking 'I Agree' below, you agree to be bound by all the terms and conditions of the above License Agreement. Carefully read the License Agreement before accepting. If you do not agree with any of the terms ond conditions, click 'Cancel' to cancel the setup process. php HYPERTEXT PREPROCESSOR < Back I Agree Cancel

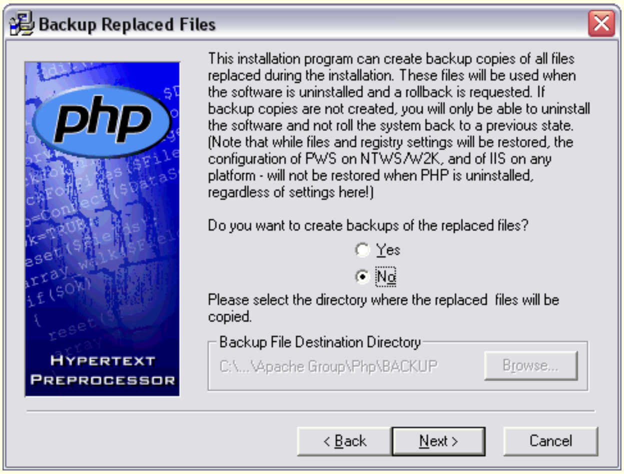
Procedure 234
Install PHP (Part 3 of 13)

Step	Action
5	Choose the Installation type.
	Select **Advanced** and click **Next** to continue.  Installation Type Please select the type of installation you require. ○ Standard ● Advanced

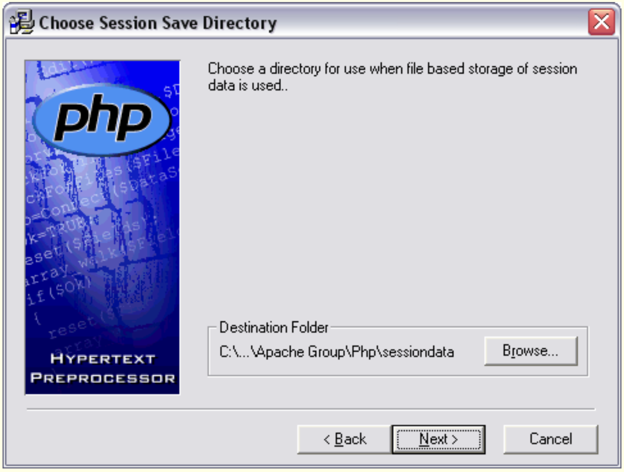
Procedure 234
Install PHP (Part 4 of 13)

Step	Action
6	Select an install location.
	IMPORTANT! Do not accept the default location C:\PHP. - Click **Browse**. - Select the path C:\Program Files\Apache Group\Php as shown in the following dialog boxes:  Choose Destination Location up will install PHP 4.3.4 in the following folder. install into a different folder, click Browse, and select ther folder. u can choose not to install PHP 4.3.4 by clicking Cancel to Setup. estination Folder :\Program Files\Apache Group\Php Select Destination Directory C:\Program Files\Apache Group\Php c:\ Program Files Apache Group Apache2 c: windows xp - This creates a new folder called **Php**.

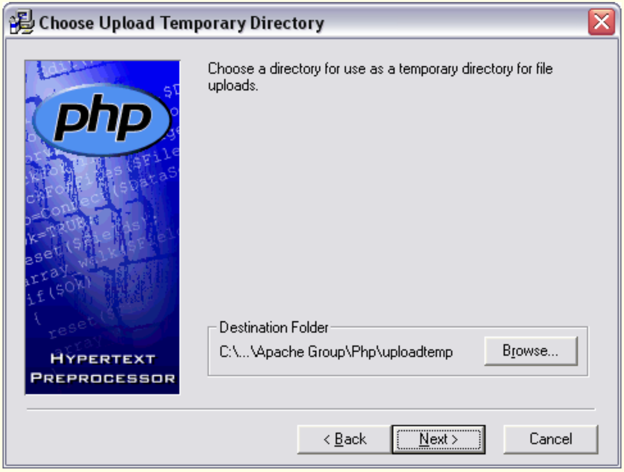
Procedure 234
Install PHP (Part 5 of 13)

Step	Action
7	Choose Backup options.
	Check **No** and Click **Next** to continue.  Backup Replaced Files This installation program can create backup copies of all files replaced during the installation. These files will be used when the software is uninstalled and a rollback is requested. If backup copies are not created, you will only be able to uninstall the software and not roll the system back to a previous state. (Note that while files and registry settings will be restored, the configuration of PWS on NTWS/W2K, and of IIS on any platform - will not be restored when PHP is uninstalled, regardless of settings here!) Do you want to create backups of the replaced files? ○ Yes ● No Please select the directory where the replaced files will be copied. Backup File Destination Directory C:\...\Apache Group\Php\BACKUP Browse... < Back Next > Cancel

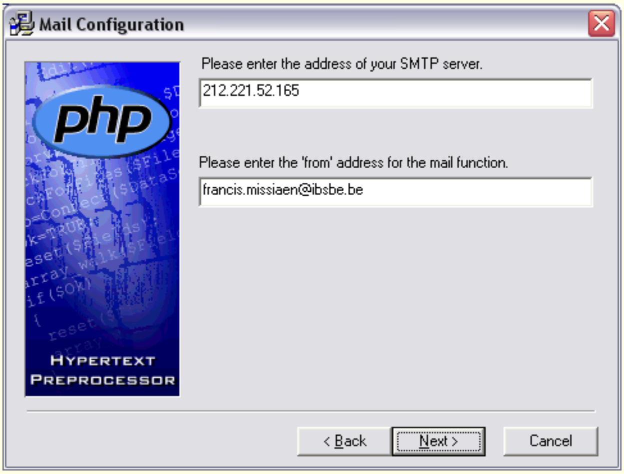
Procedure 234
Install PHP (Part 6 of 13)

Step	Action
8	Choose a directory to store session data.
	Use the **Browse** button to specify a directory, and the click **Next** to continue.  Choose Session Save Directory Choose a directory for use when file based storage of session data is used.. Destination Folder C:\...\Apache Group\Php\sessiondata

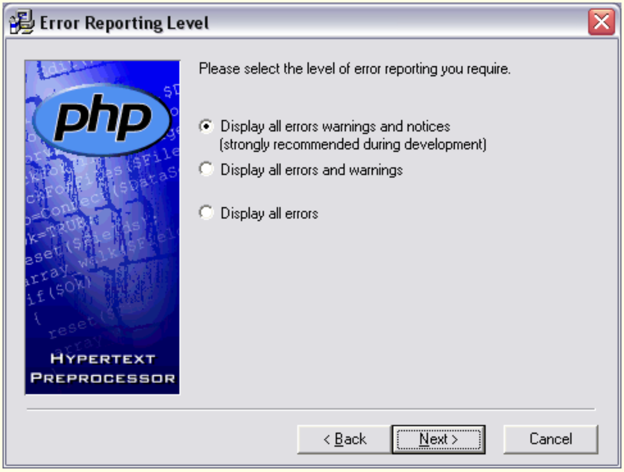
Procedure 234
Install PHP (Part 7 of 13)

Step	Action
9	Specify a temporary directory.
	Use the **Browse** button to specify a directory, and the click **Next** to continue.  Choose Upload Temporary Directory Choose a directory for use as a temporary directory for file uploads. Destination Folder C:\...\Apache Group\Php\uploadtemp php Hypertext Preprocessor Browse... < Back Next > Cancel

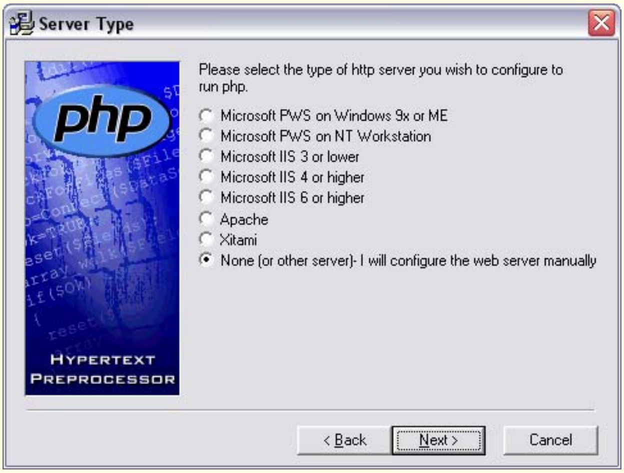
Procedure 234
Install PHP (Part 8 of 13)

Step	Action
10	Enter mail information.
	Enter the IP address and the mail address of the system administrator. You can accept default values, or choose a dummy value if these parameters are not available.  Mail Configuration Please enter the address of your SMTP server. 212.221.52.165 Please enter the 'from' address for the mail function. francis.missiaen@ibsbe.be

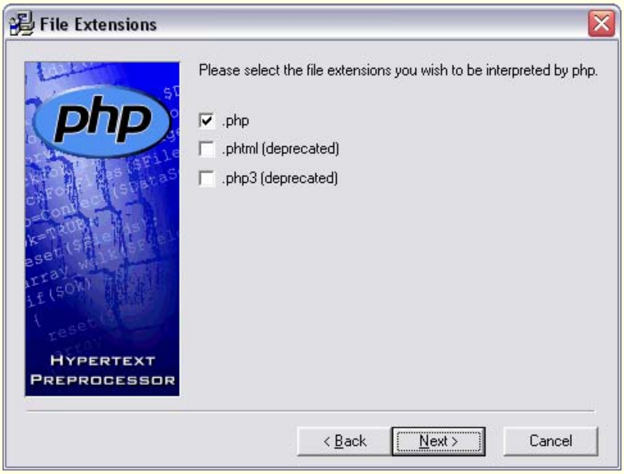
Procedure 234
Install PHP (Part 9 of 13)

Step	Action
11	Configure error reporting.
	Check the level of error reporting you prefer, and click **Next** to continue.  Error Reporting Level Please select the level of error reporting you require. ● Display all errors warnings and notices (strongly recommended during development) ○ Display all errors and warnings ○ Display all errors

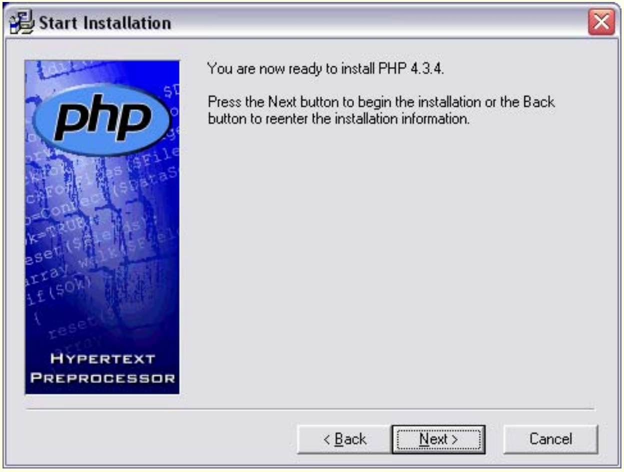
Procedure 234
Install PHP (Part 10 of 13)

Step	Action
12	Select the type of http server you want to run PHP.
	Check **None** and click **Next** to continue.  Server Type Please select the type of http server you wish to configure to run php. ○ Microsoft PWS on Windows 9x or ME ○ Microsoft PWS on NT Workstation ○ Microsoft IIS 3 or lower ○ Microsoft IIS 4 or higher ○ Microsoft IIS 6 or higher ○ Apache ○ Xitami ● None (or other server)- I will configure the web server manually

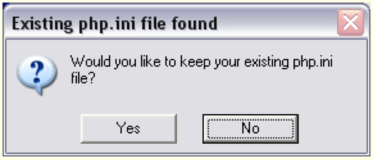
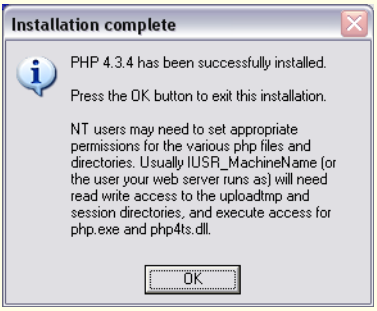
Procedure 234
Install PHP (Part 11 of 13)

Step	Action
13	Select file extensions.
	Select the file extensions you want to associate with PHP, and click **Next** to continue.  Please select the file extensions you wish to be interpreted by php. ☑ .php □ .phtml (deprecated) □ .php3 (deprecated) File Extensions php Hypertext Preprocessor < Back Next > Cancel

Procedure 234
Install PHP (Part 12 of 13)

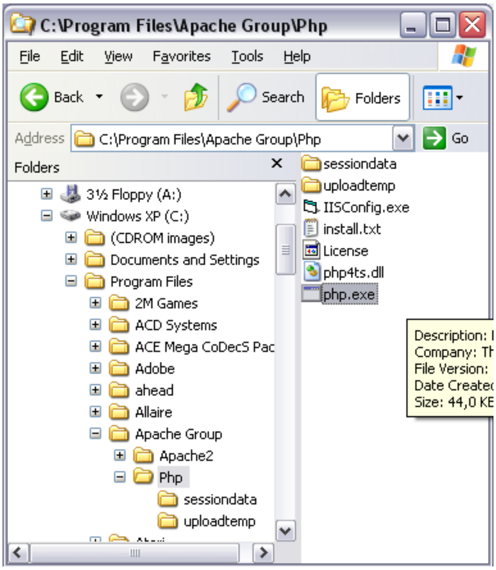
Step	Action
14	Begin copying files.
	Click **Next** to confirm your choices and begin copying files.  Start Installation You are now ready to install PHP 4.3.4. Press the Next button to begin the installation or the Back button to reenter the installation information.

Procedure 234
Install PHP (Part 13 of 13)

Step	Action
15	Discard old configuration data.
	The following error message opens if a previous version of PHP is installed:  Existing php.ini file found Would you like to keep your existing php.ini file? - Choose **No** to prevent using old configuration data.
16	Acknowledge completion of the installation.
	Click **OK** to continue.  Installation complete PHP 4.3.4 has been successfully installed. Press the OK button to exit this installation. NT users may need to set appropriate permissions for the various php files and directories. Usually IUSR_MachineName (or the user your web server runs as) will need read write access to the uploadtmp and session directories, and execute access for php.exe and php4ts.dll.
	END

The PHP install process also creates a number of resources in C:\Program Files\Apache\Php as shown in Figure 384 on page 991.

Figure 384
Resources installed by PHP



Configuring PHP

A configuration file named php.ini is also created in the Windows directory, usually C:\Windows.

Note: In the configuration file, the semicolon (;) denotes a comment.

Procedure 235
Configuring PHP to support DECT Messenger

Step	Action
1	Rename the PHP.ini file.
	• Locate the PHP.ini configuration file, which is located in the Windows directory, (for instance C:\WINNT). • Rename the PHP.ini file to PHP_original.ini.
2	Copy the new PHP.ini file from the CD.
	• Browse to the following folder on CD2: \Step 4 - WebServer\Step 4a - Apache\Config files • Copy the file PHP.ini • Paste the file into the Windows directory (for instance, C:\WINNT).

END

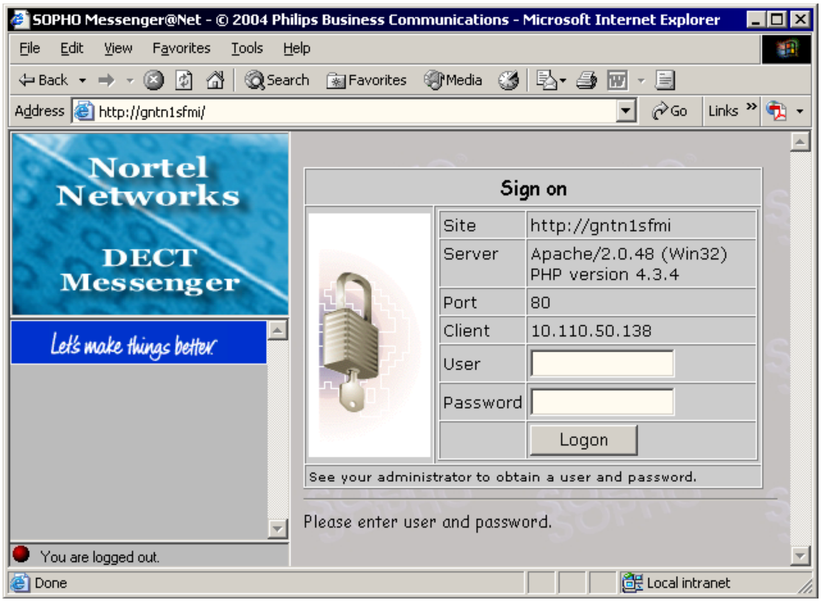
The Apache Web Server and PHP are installed and started.

If you have configured the DECT Messenger database, you can now test the eWEB application. This requires configuration of the eWEB-related tables: eWEB, eWEB_TOC, eWEB_USER_AUTH, and others.

Verifying that the web server is running

You can verify that the web server is running by starting Internet Explorer and typing the URL http://127.0.0.1. If the web server is working correctly, the window shown in Figure 385 on page 993 opens.

Figure 385
Verifying that the web server is running


SOPHO Messenger@Net - © 2004 Philips Business Communications - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://gntn1sfmi/
Go Links
Nortel Networks
DECT Messenger
Let's make things better
Done
Local intranet

Sign on

Site	http://gntn1sfmi
Server	Apache/2.0.48 (Win32) PHP version 4.3.4
Port	80
Client	10.110.50.138
User	
Password	
	Logon

See your administrator to obtain a user and password.

Please enter user and password.

You are logged out.

If the error **No Branding in eWeb** is displayed, your web server is installed correctly, but you still need to configure the Nortel branding within the eCONFIG module under eWeb. See “Module – eWEB” on page 1265 for help configuring the eWeb module.

You can now return to the remaining steps described in “General – Install PC” on page 805.

Install PC – Step 5 – eSMTP_Server

This chapter provides information on the following topics:

- "Installing the Microsoft SMTP service component" on page 995
- "Configuring the Microsoft SMTP service" on page 998

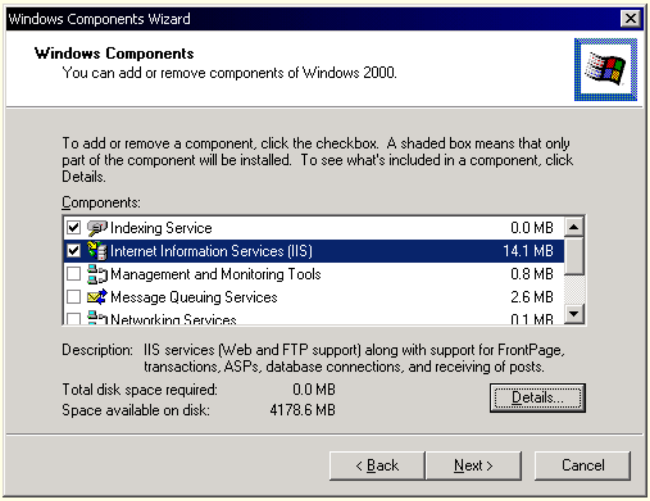
Installing the Microsoft SMTP service component

The SMTP Service component is shipped with Windows. The SMTP server is part of the Windows component Internet Information Server. Check to see if the SMTP Service is already installed by following the steps, and install the service if necessary:

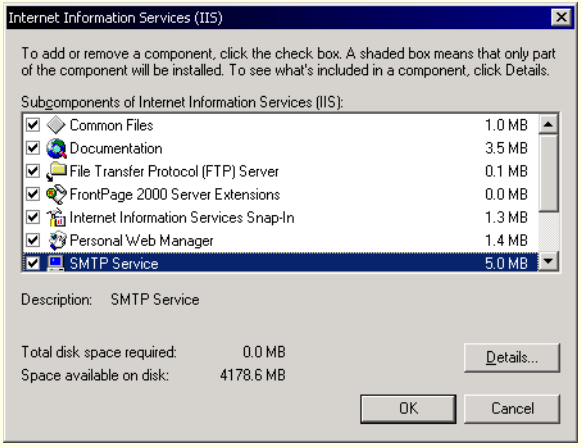
Procedure 236
Installing the SMTP Service (Part 1 of 4)

Step	Action
1	Open Add/Remove Programs.
	Click **Start** and choose **Settings > Control Panel > Add/Remove programs**.
2	Open the **Add/Remove Windows Components** window.
	Click **Add/Remove Windows Components**.

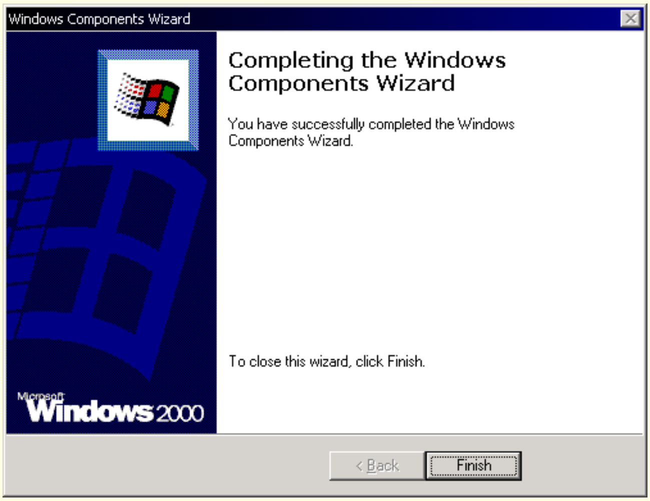
Procedure 236
Installing the SMTP Service (Part 2 of 4)

Step	Action
3	Select **Internet Information Service (IIS)** and open the **Details** window.
	- Click the **Internet Information Service (IIS)** check box to indicate you need this component. - Click the **Details** button.  Windows Components Wizard **Windows Components** You can add or remove components of Windows 2000. To add or remove a component, click the checkbox. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details. Components: ☑ Indexing Service 0.0 MB ☑ Internet Information Services (IIS) 14.1 MB ☐ Management and Monitoring Tools 0.8 MB ☐ Message Queuing Services 2.6 MB ☐ Networking Services 0.1 MB Description: IIS services (Web and FTP support) along with support for FrontPage, transactions, ASPs, database connections, and receiving of posts. Total disk space required: 0.0 MB Space available on disk: 4178.6 MB Details... < Back Next > Cancel

Procedure 236
Installing the SMTP Service (Part 3 of 4)

Step	Action
4	Select SMTP Service
	Choose one of the following: • If SMTP Service is not already checked, check the corresponding box to select the SMTP Service. • If the box is already checked, the SMTP service is already installed, and you can proceed to “Configuring the Microsoft SMTP service” on page 998. ***Note:*** In the following illustration of the IIS window, other components (such as File Transfer Protocol (FTP) server, and so on) are shown but are *not* required for the DECT Messenger eSMTP_server module.  Internet Information Services (IIS) To add or remove a component, click the check box. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details. Subcomponents of Internet Information Services (IIS): ☑ Common Files 1.0 MB ☑ Documentation 3.5 MB ☑ File Transfer Protocol (FTP) Server 0.1 MB ☑ FrontPage 2000 Server Extensions 0.0 MB ☑ Internet Information Services Snap-In 1.3 MB ☑ Personal Web Manager 1.4 MB ☑ SMTP Service 5.0 MB Description: SMTP Service Total disk space required: 0.0 MB Space available on disk: 4178.6 MB

Procedure 236
Installing the SMTP Service (Part 4 of 4)

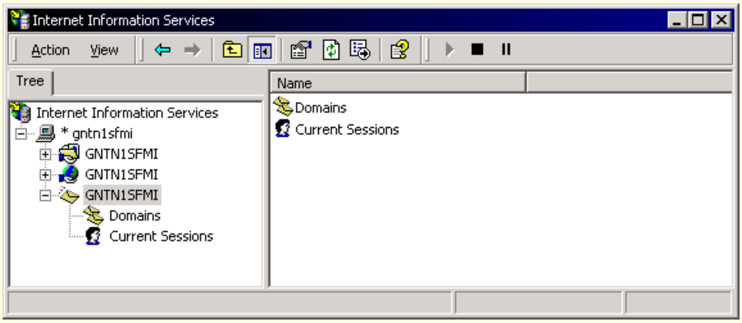
Step	Action
5	Begin copying files.
	Click **OK** and then **Next** to confirm your selections and begin copying files.
6	Acknowledge the completion of the installation.
	Click **Finish**.  Windows Components Wizard Completing the Windows Components Wizard You have successfully completed the Windows Components Wizard. To close this wizard, click Finish.

END

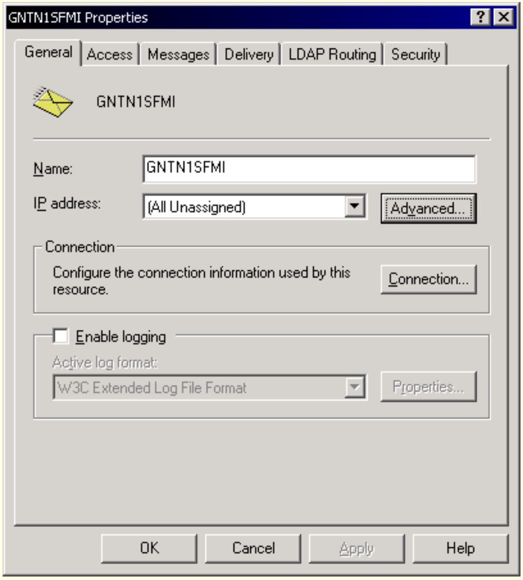
Configuring the Microsoft SMTP service

Once the SMTP service is installed, you can tailor the parameters to your own preferences. Table 237 on page 999 illustrates some of the configuration settings that can be defined. For more information on these settings, check the Microsoft web site at www.microsoft.com.

Procedure 237
Configuring the SMTP Service (Part 1 of 14)

Step	Action
1	Open the **IIS** window.
	Click **Start** and choose **Settings > Control Panel > Administrative Tools > Internet Service Manager**.
2	Review the information provided in the **IIS** window.
	Note: In the following illustrations, the name GNTN1SFMI is the name of the PC used to capture the illustration. Your system shows the name of your own PC. One or more services are shown, depending on the installed components: — the folder icon refers to the FTP service (if installed). — the globe icon refers to the web server (if installed). — the letter icon refers to the SMTP service.  Internet Information Services Action View Tree Name Internet Information Services * gntn1sfmi GNTN1SFMI GNTN1SFMI GNTN1SFMI Domains Current Sessions Domains Current Sessions
3	Open the **Properties** window for the SMTP Service.
	• Highlight the SMTP Service, indicated with the letter icon, and right-click. • Select **Properties** from the pop-up menu.

Procedure 237
Configuring the SMTP Service (Part 2 of 14)

Step	Action
4	Set parameters on the General tab.
	Use the **General** tab to maintain general parameters. For example, use the following steps to disable logging by clearing the **Enable logging** check box. Enter the following: • SMTP virtual server • IP address • connection type By default, the SMTP virtual server can respond to connection requests for all IP addresses configured on the computer. 

GNTN1SFMI Properties

GNTN1SFMI

Name: GNTN1SFMI

IP address: (All Unassigned)

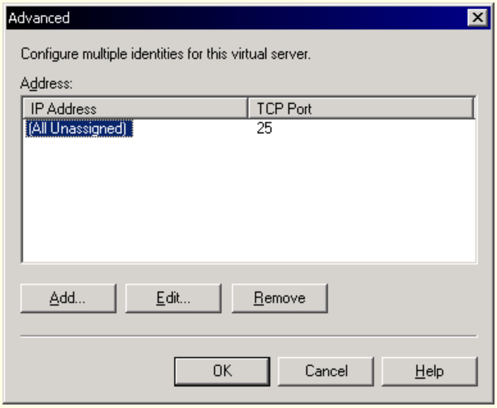
Connection

Configure the connection information used by this resource.

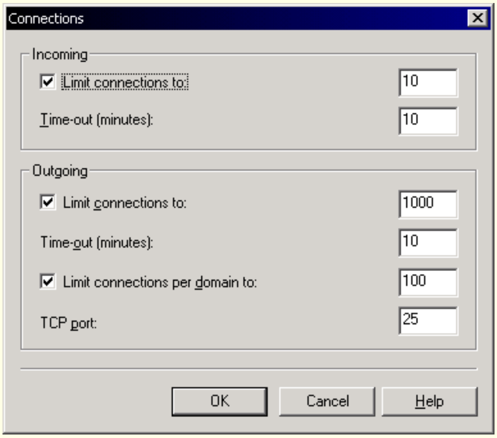
☐ Enable logging

Active log format: W3C Extended Log File Format

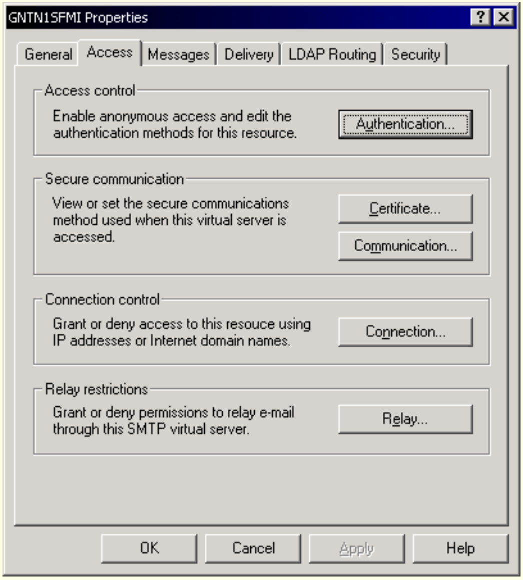
Procedure 237
Configuring the SMTP Service (Part 3 of 14)

Step	Action
5	Access **Advanced** settings.
	Click the **Advanced** button to specify the port the SMTP service listens to (leave this value at the default (25) for most environments).  Advanced Configure multiple identities for this virtual server. Address: IP Address: (All Unassigned) — TCP Port: 25

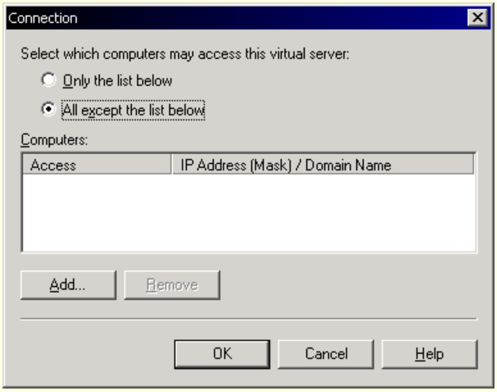
Procedure 237
Configuring the SMTP Service (Part 4 of 14)

Step	Action
6	Access the **Connections** window.
	Click **Connection...** to configure incoming and outgoing connections on this SMTP virtual server. Set the following: • Limit connections • Time-out • Limit connections per domain • TCP port  Connections Incoming ☑ Limit connections to: 10 Time-out (minutes): 10 Outgoing ☑ Limit connections to: 1000 Time-out (minutes): 10 ☑ Limit connections per domain to: 100 TCP port: 25

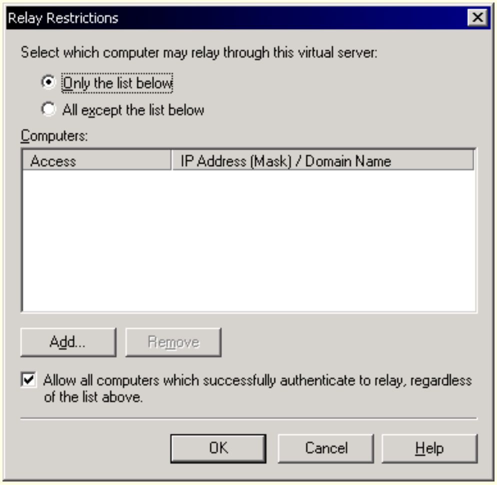
Procedure 237
Configuring the SMTP Service (Part 5 of 14)

Step	Action
7	Set options on the Access tab.
	Use the **Access** tab to configure client access to the SMTP virtual server and to establish transmission security. • Use **Access control** to configure Microsoft SMTP Service to allow anonymous access or to prompt users for a username and password. • Use **Secure communication** to set security for the virtual server once access has been granted. • Use **Connection control** to grant or deny use of the virtual server to specific users or groups. • Use **Relay restrictions** to block relay access to the virtual server, thus preventing processing of unwanted mail.  GNTN1SFMI Properties Access control: Enable anonymous access and edit the authentication methods for this resource. Secure communication: View or set the secure communications method used when this virtual server is accessed. Connection control: Grant or deny access to this resouce using IP addresses or Internet domain names. Relay restrictions: Grant or deny permissions to relay e-mail through this SMTP virtual server. General Access Messages Delivery LDAP Routing Security Authentication... Certificate... Communication... Connection... Relay... OK Cancel Apply Help

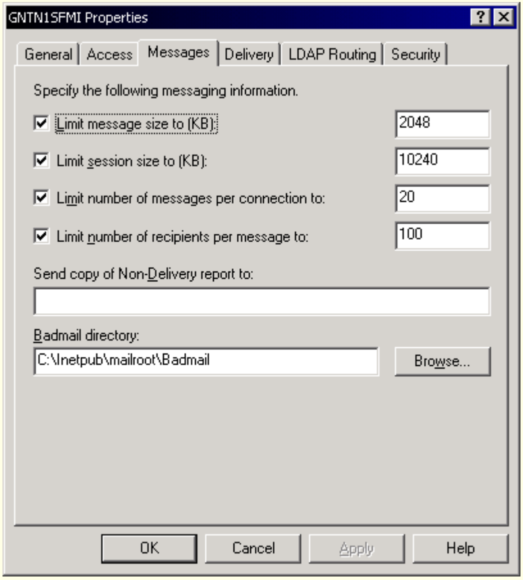
Procedure 237
Configuring the SMTP Service (Part 6 of 14)

Step	Action
8	Set Connection control options.
	Use these options to limit access to the SMTP virtual server by client IP address or domain name. You can grant access to all computers, and then make exceptions to this rule by denying access to specific computers. Alternatively, if you deny access to all computers, you still can grant access to specific computers.  Connection Select which computers may access this virtual server: ○ Only the list below ● All except the list below Computers: Access — IP Address (Mask) / Domain Name

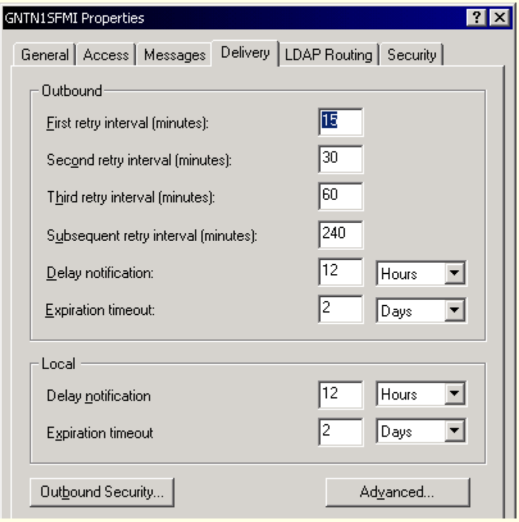
Procedure 237
Configuring the SMTP Service (Part 7 of 14)

Step	Action
9	Set Relay restrictions.
	Use these options to limit by client IP address or domain name those computers allowed to relay mail through this virtual server. You can grant relaying to all computers and then make exceptions to this rule by denying relay access to specific computers. Alternatively, if you deny relay access to all computers, you still can grant relay access to specific computers.  Relay Restrictions Select which computer may relay through this virtual server: ● Only the list below ○ All except the list below Computers: Access / IP Address (Mask) / Domain Name ☑ Allow all computers which successfully authenticate to relay, regardless of the list above. ***Note:*** If your virtual server is on the Internet, Nortel does not recommend relaying, as the virtual server can end up propagating unsolicited commercial e-mail.

Procedure 237
Configuring the SMTP Service (Part 8 of 14)

Step	Action
10	Set options on the Messages tab.
	When a connection is open, and the receiving server is ready to receive data, messages can be transmitted for delivery. Use the **Messages** tab to determine transmission requirements and limits: • limit message size • limit session size • limit number of messages per connection • limit number of recipients per message • send a copy of Non-Delivery report • locate Badmail directory.  GNTN1SFMI Properties Specify the following messaging information. ☑ Limit message size to (KB): 2048 ☑ Limit session size to (KB): 10240 ☑ Limit number of messages per connection to: 20 ☑ Limit number of recipients per message to: 100 Send copy of Non-Delivery report to: Badmail directory: C:\Inetpub\mailroot\Badmail General Access Messages Delivery LDAP Routing Security Browse... OK Cancel Apply Help

Procedure 237
Configuring the SMTP Service (Part 9 of 14)

Step	Action
11	Set options on the Delivery tab.
	When a connection is open, and the receiving server has is ready to receive data, messages can be transmitted for delivery. Use the **Delivery** tab to set all delivery and routing options. This includes: • setting retry intervals for delivering messages, • limiting the number of hops to servers during delivery, • identifying a masquerade domain name to display in the From line instead of the sender's original domain name, • first retry interval, second retry interval, third retry interval, • subsequent retry interval, • delay notification, • expiration timeout, • other options available through **Outbound Security** and **Advanced**. 

GNTN1SFMI Properties

Outbound

First retry interval (minutes): 15

Second retry interval (minutes): 30

Third retry interval (minutes): 60

Subsequent retry interval (minutes): 240

Delay notification: 12 Hours

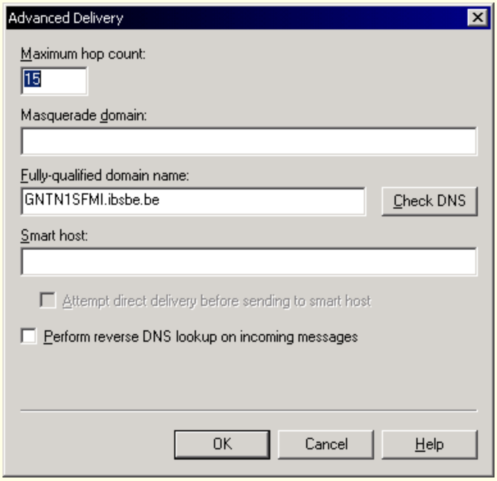
Expiration timeout: 2 Days

Local

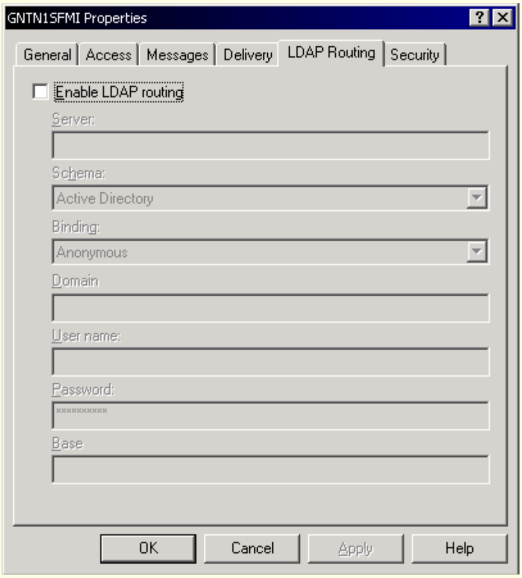
Delay notification 12 Hours

Expiration timeout 2 Days

Procedure 237
Configuring the SMTP Service (Part 10 of 14)

Step	Action
12	Set Advanced Delivery options.
	Click **Advanced** to open the Advanced Delivery dialog box. Use this window to set routing options on your SMTP virtual server: • maximum hop count, • masquerade domain, • fully-qualified domain name, • smart host, • attempt direct delivery before sending to smart host, • perform reverse DNS lookup on incoming messages.  Advanced Delivery Maximum hop count: 15 Masquerade domain: Fully-qualified domain name: GNTN1SFMI.ibsbe.be Smart host: ☐ Attempt direct delivery before sending to smart host ☐ Perform reverse DNS lookup on incoming messages

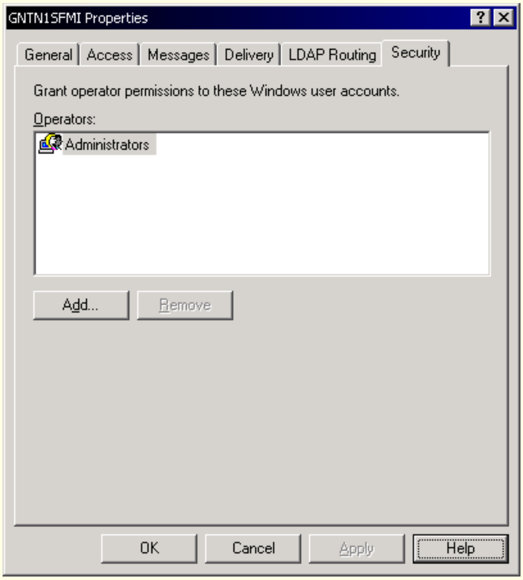
Procedure 237
Configuring the SMTP Service (Part 11 of 14)

Step	Action
13	Set directory services server properties on the LDAP Routing tab.
	Use the **LDAP Routing** tab to specify the identity and properties of the directory services server used for this SMTP virtual server. The directory services store information about mail clients and their mailboxes. The SMTP virtual server uses Lightweight Directory Access Protocol (LDAP) to communicate with the directory services. You can configure Microsoft SMTP Service to consult an LDAP server to resolve senders and recipients. For example, you can use the Windows 2000 Active Directory as an LDAP server, and use Active Directory Users and Computers to create a group mailing list that is automatically expanded on the SMTP virtual server. • To activate LDAP Routing, select the Enable LDAP routing check box. • Configure the following fields: server, schema, binding, domain, username, password, and base.  GNTN1SFMI Properties ☐ Enable LDAP routing Server: Schema: Active Directory Binding: Anonymous Domain User name: Password: ********** Base ? X General Access Messages Delivery LDAP Routing Security OK Cancel Apply Help

Procedure 237
Configuring the SMTP Service (Part 12 of 14)

<table>
<tr><th>Step</th><th>Action</th></tr>
<tr><td><b>14</b></td><td>Give users or groups operator status.</td></tr>
<tr><td></td><td>

Use the **Security** tab to add Microsoft Windows accounts and groups to the list of SMTP virtual server operators.



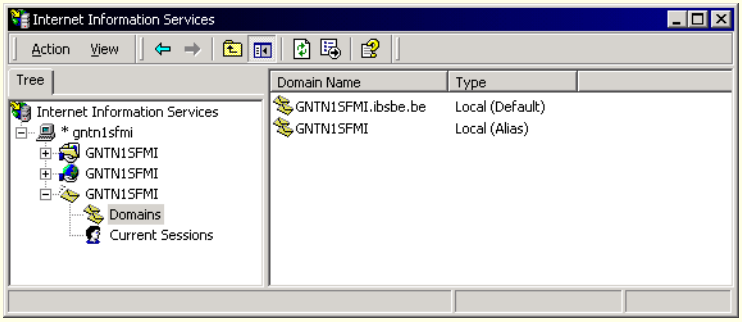
Grant operator permissions to these Windows user accounts.

Operators:

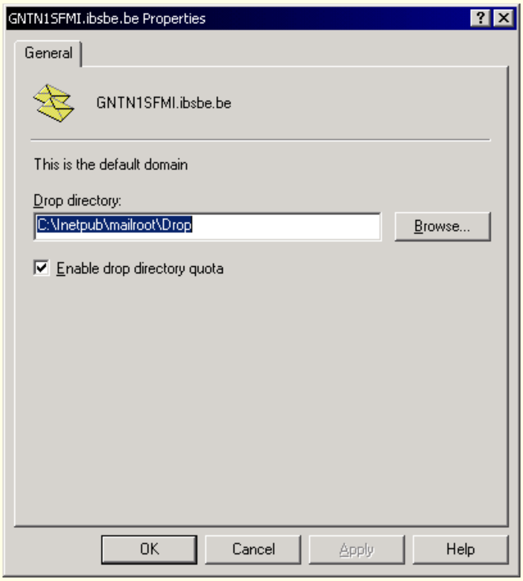
Administrators

</td></tr>
<tr><td></td><td></td></tr>
</table>

Procedure 237
Configuring the SMTP Service (Part 13 of 14)

Step	Action
15	Access domain configuration options.
	The SMTP virtual server has at least one domain: the Local (default) domain. - Highlight the domain name and right-click to open the pop-menu. Choose **Properties** to open the **Properties** window.  Internet Information Services Action View Tree Internet Information Services * gntn1sfmi GNTN1SFMI GNTN1SFMI GNTN1SFMI Domains Current Sessions Domain Name Type GNTN1SFMI.ibsbe.be Local (Default) GNTN1SFMI Local (Alias) You can add more domains and configure them as local or remote. You can delete any domain that you create, but you cannot delete the default domain. Domain configuration options depend on whether the domain is a Local Domain or a Remote Domain.

Procedure 237
Configuring the SMTP Service (Part 14 of 14)

Step	Action
16	Set drop directory for Local Domains.
	For local default domains, you can set the **drop directory**. - Click **Browse** and choose the location where you wish set the drop directory. The drop directory is used in the DECT Messenger configuration of the eSMTP_SERVER table. In most cases, the default value **C:\Inetpub\mailroot\Drop** is used.  GNTN1SFMI.ibsbe.be Properties GNTN1SFMI.ibsbe.be This is the default domain Drop directory: C:\Inetpub\mailroot\Drop ☑ Enable drop directory quota

END

Install PC – Step 6 – eCONFIG

This chapter provides information on the following topics:

- “Installing eCONFIG” on page 1014
- “Using eCONFIG” on page 1019
- “Editing eCONFGI.ini” on page 1022

Before you begin

Prior to installing the Nortel DECT Messenger eCONFIG, you must:

1. Complete the steps in “General – Install PC” on page 805.
2. Install DECT Messenger and all the prerequisite actions that are described in the document “Install PC – Step 2 – Nortel DECT Messenger” on page 873.
3. Configure the eKERNEL module to provide an online TCP/IP socket connection between the eCONFIG module and eKERNEL.

IMPORTANT!

DECT Messenger and all associated modules require the Nortel Licence Manager to be installed, and require a valid licence key for the dongle to unlock the functionality of the software. Refer to “Install PC – Step 1e – Licence Manager” on page 839 for the licence manager installation procedure; the readme.txt file in that same directory contains more information.

IMPORTANT!

The installation procedure assumes you are installing from a CD-ROM, or a DVD image of the product. This means the \Step 6 – Configurator folder must reside in the root of the drive (usually drive D:). Installation from a subdirectory or a network drive is not supported, and can result in the error “Could not find enough disk space for extracting files.” If you must install from a network resource, share the directory, and map the shared directory to a network drive, so that the folder \Step 6 – Configurator resides in the root of the network drive.

Installing eCONFIG

Installation files are located on the CD-ROM in directory \Step7 – Configurator.

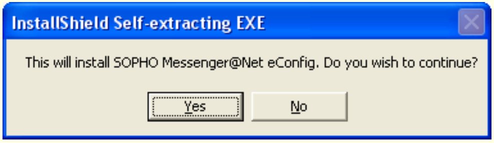
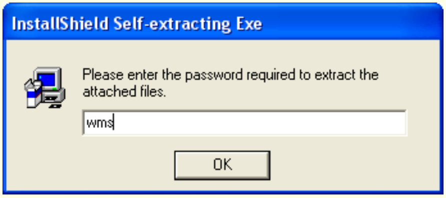
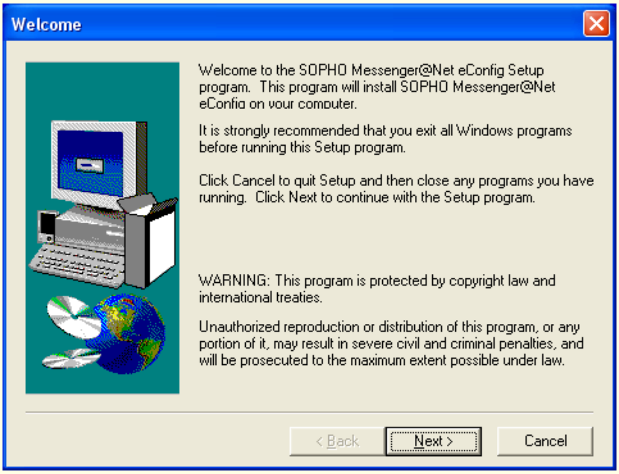
IMPORTANT! Branding notice

Two versions of the installation program are available. If you are running in a Nortel environment, the Nortel version must be used.

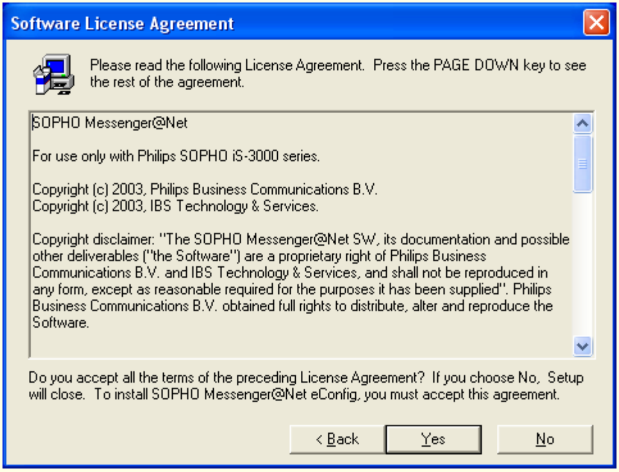
Procedure 238
Installing eCONFIG (Part 1 of 6)

Step	Action
1	Launch the installation program.
	Navigate to the CD-ROM folder \Step7 – Configurator and double-click eCONFIG_NORTEL_R3.0.0_2004.06.27.exe. ***Note:*** The filename contains the release level and the build date. If more than one version is available, install the latest version, unless instructed otherwise.

Procedure 238
Installing eCONFIG (Part 2 of 6)

Step	Action
2	Start the installation.
	Click **Yes** to begin.  InstallShield Self-extracting EXE This will install SOPHO Messenger@Net eConfig. Do you wish to continue?
3	Enter the password.
	Enter **wms** in the password field (all lowercase).  InstallShield Self-extracting Exe Please enter the password required to extract the attached files. wms
4	Review Welcome information.
	Review the Welcome window information and click **Next** to continue.  Welcome Welcome to the SOPHO Messenger@Net eConfig Setup program. This program will install SOPHO Messenger@Net eConfig on your computer. It is strongly recommended that you exit all Windows programs before running this Setup program. Click Cancel to quit Setup and then close any programs you have running. Click Next to continue with the Setup program. WARNING: This program is protected by copyright law and international treaties. Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under law.

Procedure 238
Installing eCONFIG (Part 3 of 6)

Step	Action
5	Accept the Licence Agreement.
	Review the Licence Agreement, and click **Yes** to continue. 

Software License Agreement

Please read the following License Agreement. Press the PAGE DOWN key to see the rest of the agreement.

SOPHO Messenger@Net

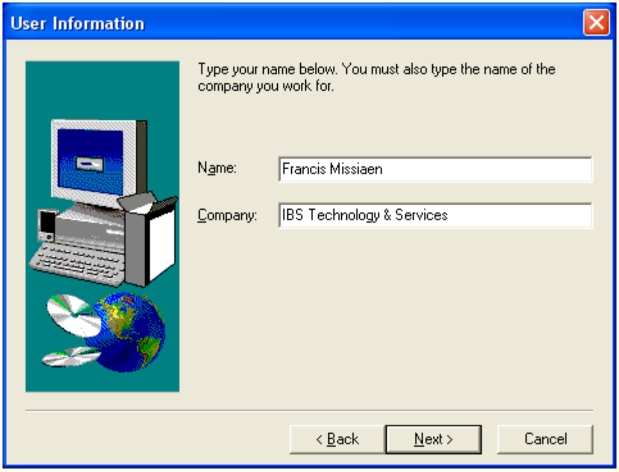
For use only with Philips SOPHO iS-3000 series.

Copyright (c) 2003, Philips Business Communications B.V.
Copyright (c) 2003, IBS Technology & Services.

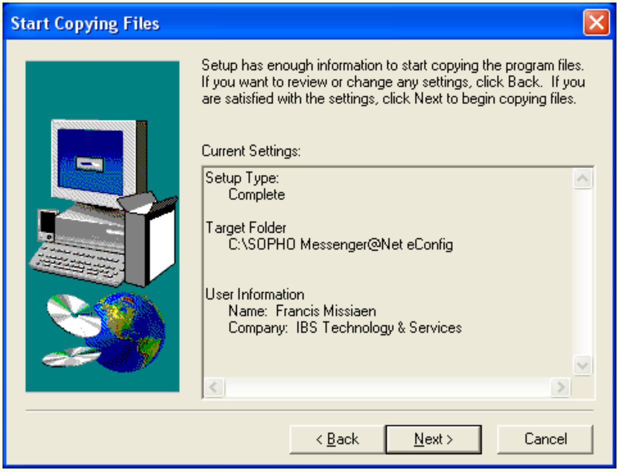
Copyright disclaimer: "The SOPHO Messenger@Net SW, its documentation and possible other deliverables ("the Software") are a proprietary right of Philips Business Communications B.V. and IBS Technology & Services, and shall not be reproduced in any form, except as reasonable required for the purposes it has been supplied". Philips Business Communications B.V. obtained full rights to distribute, alter and reproduce the Software.

Do you accept all the terms of the preceding License Agreement? If you choose No, Setup will close. To install SOPHO Messenger@Net eConfig, you must accept this agreement.

Procedure 238
Installing eCONFIG (Part 4 of 6)

Step	Action
6	Enter name and company information.
	Enter name and company information, and click **Next** to continue.  User Information Type your name below. You must also type the name of the company you work for. Name: Francis Missiaen Company: IBS Technology & Services

Procedure 238
Installing eCONFIG (Part 5 of 6)

Step	Action
7	Start copying files.
	Click **Next** to verify your selections and start copying files. 

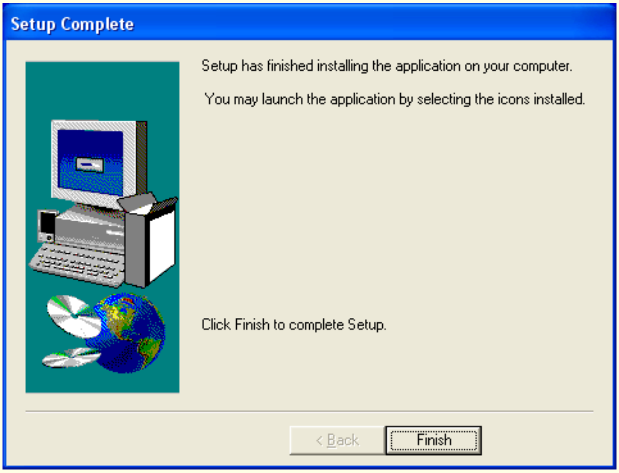
Start Copying Files

Setup has enough information to start copying the program files. If you want to review or change any settings, click Back. If you are satisfied with the settings, click Next to begin copying files.

Current Settings:

```
Setup Type:
     Complete

Target Folder
     C:\SOPHO Messenger@Net eConfig


User Information
     Name:  Francis Missiaen
     Company:  IBS Technology & Services
```

Procedure 238
Installing eCONFIG (Part 6 of 6)

Step	Action
8	Acknowledge completion of the installation, and reboot your machine if requested.
	When the installation is complete, review the information provided, and choose one of the following: • If the **Setup Complete** window advises you to reboot your PC, do so. • If no reboot is required, click **Finish** to complete the installation.  Setup Complete Setup has finished installing the application on your computer. You may launch the application by selecting the icons installed. Click Finish to complete Setup.

END

Using eCONFIG

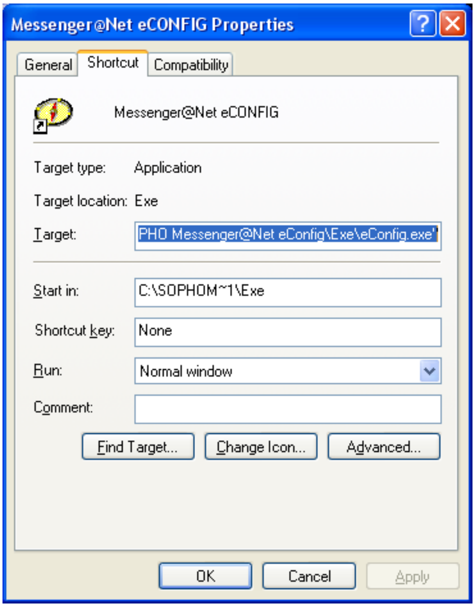
After you complete the preceding steps, a shortcut appears on your desktop, as shown in Figure 386 on page 1020.

Figure 386
The Messenger shortcut

1 Select the Messenger shortcut icon, and right-click.

2 Choose **Properties** from the pop-up menu to access the Properties window for this shortcut, as shown in Figure 387.

Figure 387
Messenger icon properties



Messenger@Net eCONFIG

Target type: Application

Target location: Exe

Target: PHO Messenger@Net eConfig\Exe\eConfig.exe"

Start in: C:\SOPHOM~1\Exe

Shortcut key: None

Run: Normal window

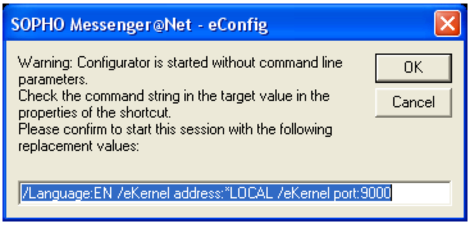
Comment:

The Target field points to C:\SOPHO Messenger@Net eCONFIG\Exe\eConfig.exe.

Editing start-up parameters

If you start the software with this default setting, you are prompted at start-up to enter a number of missing parameters, as shown in Figure 388 on page 1021.

Figure 388
Missing parameters prompt



SOPHO Messenger@Net - eConfig

Warning: Configurator is started without command line parameters.
Check the command string in the target value in the properties of the shortcut.
Please confirm to start this session with the following replacement values:

/Language:EN /eKernel address:*LOCAL /eKernel port:9000

eCONFIG is requesting the following parameters:

- eKernel address: the default setting *LOCAL refers to the 127.0.0.1 address, and directs eCONFIG to contact the eKERNEL module on the local system. This default setting is appropriate only for local maintenance. When eCONFIG is used for distributed maintenance, the IP address of the DECT Messenger system that runs eKERNEL must be specified.
- eKernel port: the default value 9000 is the port number that is typically used in eKERNEL_SITE table as the administration port, which is used in the sockets connection between eCONFIG and eKERNEL.

  Note: The language keyword pictured in Figure 388 is no longer used, because the language of the user is retrieved from the configuration automatically.

When the eCONFIG is installed on a local PC (that is, the same system that runs the eKERNEL module of DECT Messenger), you can update the shortcut with the missing parameters. To do so, edit the **target** parameter of the shortcut to match the following.

```
C:\SOPHO Messenger@Net eCONFIG\Exe\eConfig.exe"
/eKernel address:*LOCAL /eKernel port:9000
```

When you make this change, eCONFIG no longer prompts for the parameters at start-up.

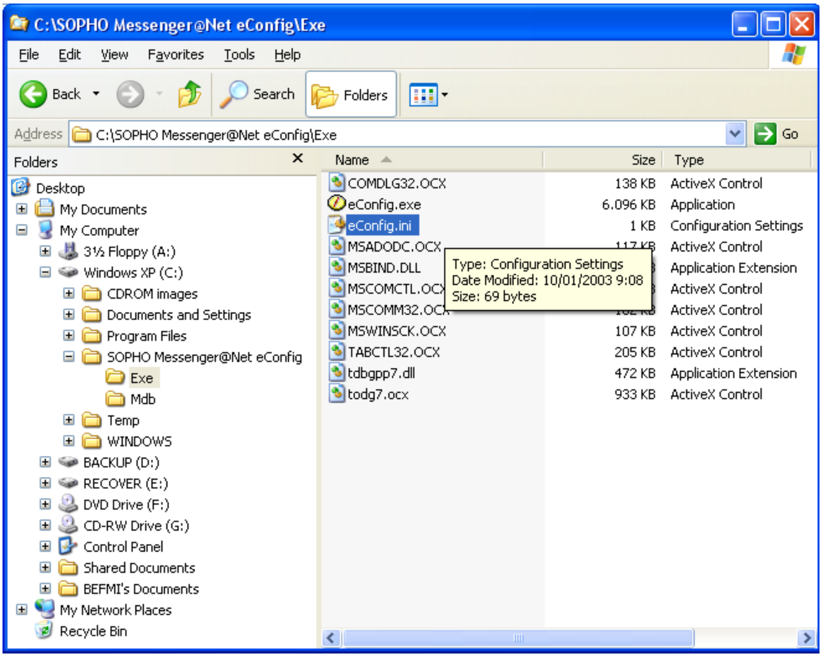
When the eCONFIG is installed on a distributed PC, Nortel strongly recommends updating the shortcut with the IP address of the eKERNEL. For example, if eKERNEL runs on a system with IP address 10.110.50.138, you must update the shortcut of all distributed PC systems as follows:

```
C:\SOPHO Messenger@Net eCONFIG\Exe\eConfig.exe"
/eKernel address:10.110.50.138 /eKernel port:9000
```

Editing eCONFGI.ini

Another important configuration setting is defined in the eCONFIG.INI file, located in the path **C:\SOPHO Messenger@Net eCONFIG\Exe**, as shown in Figure 389.

Figure 389
Accessing the eCONFIG.ini


C:\SOPHO Messenger@Net eConfig\Exe
File Edit View Favorites Tools Help
Back
Search
Folders
Address
Go
Folders

Address: C:\SOPHO Messenger@Net eConfig\Exe

- Desktop
  - My Documents
  - My Computer
    - 3½ Floppy (A:)
    - Windows XP (C:)
      - CDROM images
      - Documents and Settings
      - Program Files
      - SOPHO Messenger@Net eConfig
        - Exe
        - Mdb
      - Temp
      - WINDOWS
    - BACKUP (D:)
    - RECOVER (E:)
    - DVD Drive (F:)
    - CD-RW Drive (G:)
    - Control Panel
    - Shared Documents
    - BEFMI's Documents
  - My Network Places
  - Recycle Bin

Name	Size	Type
COMDLG32.OCX	138 KB	ActiveX Control
eConfig.exe	6.096 KB	Application
eConfig.ini	1 KB	Configuration Settings
MSADODC.OCX	117 KB	ActiveX Control
MSBIND.DLL		Application Extension
MSCOMCTL.OCX		ActiveX Control
MSCOMM32.OCX		ActiveX Control
MSWINSCK.OCX	107 KB	ActiveX Control
TABCTL32.OCX	205 KB	ActiveX Control
tdbgpp7.dll	472 KB	Application Extension
todg7.ocx	933 KB	ActiveX Control

Type: Configuration Settings
Date Modified: 10/01/2003 9:08
Size: 69 bytes

To edit the eCONFIG.ini:

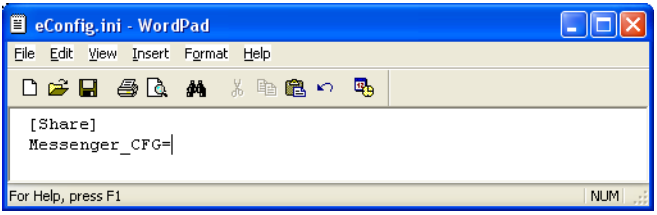
1 Open Windows Explorer.

2 Navigate to the file.

3 Double-click to open the file in your default text editor, usually Notepad.

During installation, eCONFIG uses the default eCONFIG.INI file, as shown in Figure 390.

Figure 390
eCONFIG.ini default



```
[Share]
Messenger_CFG=
```

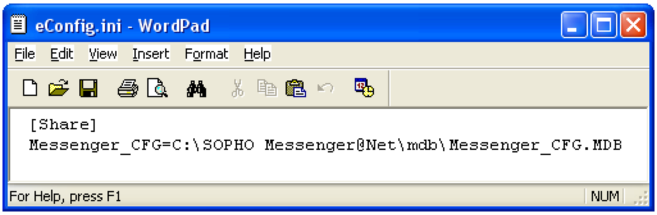
In this case, the parameter Messenger_CFG is not defined, and the user is prompted to select the Messenger_CFG database on the PC that runs eKERNEL. This is usually found in the path **C:\SOPHO Messenger\Mdb,** on the system that runs eKERNEL. To prevent the software from prompting for a database file at start-up, set the path and filename in the eCONFIG.INI file.

IMPORTANT! Branding notice

To support both SOPHO and NORTEL environment, additional tags are available in the eCONFIG.INI file. These tags provide internal steering parameters for the user interface of the eCONFIG instance. Do not alter or remove these statements. Tampering with branding related information can violate copyright regulations.

- When your run eCONFIG on a local machine, your can enter the path C:\SOPHO Messenger@Net\Mdb\Messenger_CFG.MDB manually, as shown in Figure 391 on page 1024.

Figure 391
eCONFIG.ini for local machine



```
[Share]
Messenger_CFG=C:\SOPHO Messenger@Net\mdb\Messenger_CFG.MDB
```

- When you run eCONFIG on a distributed machine, you can enter the path that refers to the location of the Messenger_CFG database file on the machine that runs eKERNEL. This means the directory where the file resides must be shared, so that remote machines can access the shared database. For example, if the drive is shared as MDB on eKERNEL system 10.110.50.138, the values can be specified as follows:

```
“Messenger_CFG=\\10.110.50.138\MDB\Messenger_CFG.MDB”
```

  In this case, you can skip the process of manually editing the eCONFIG.INI file. Once the correct file is selected, eCONFIG allows the user to navigate on the network.

- On a local machine, navigate to the local path C:\SOPHO Messenger@Net\Mdb\Messenger_CFG.MDB

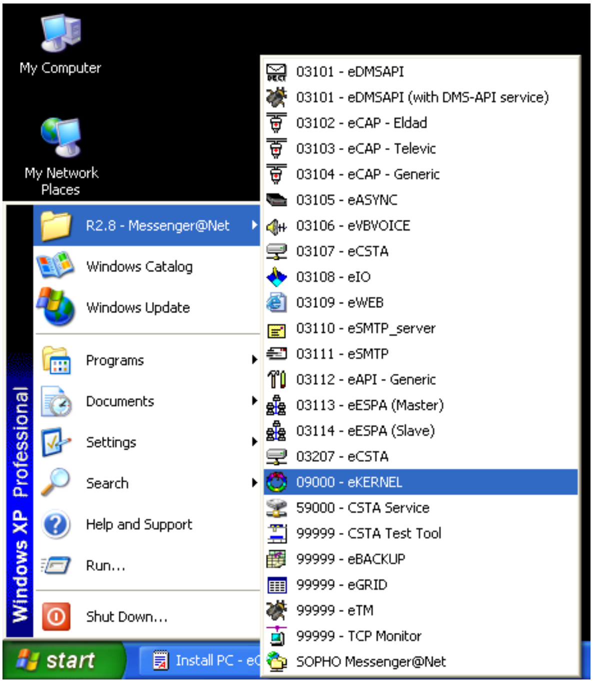
- On a distributed machine, navigate to the appropriate machine, and select the Messenger_CFG.MDB file in the shared directory.

Start eKERNEL prior to launching the eCONFIG module:

- If you are setting up a new installation, eKERNEL can be started by clicking **Start** on the Windows taskbar, and choosing **R2.8 – DECT Messenger** > **09000 – eKERNEL**, as shown in Figure 392 on page 1025.

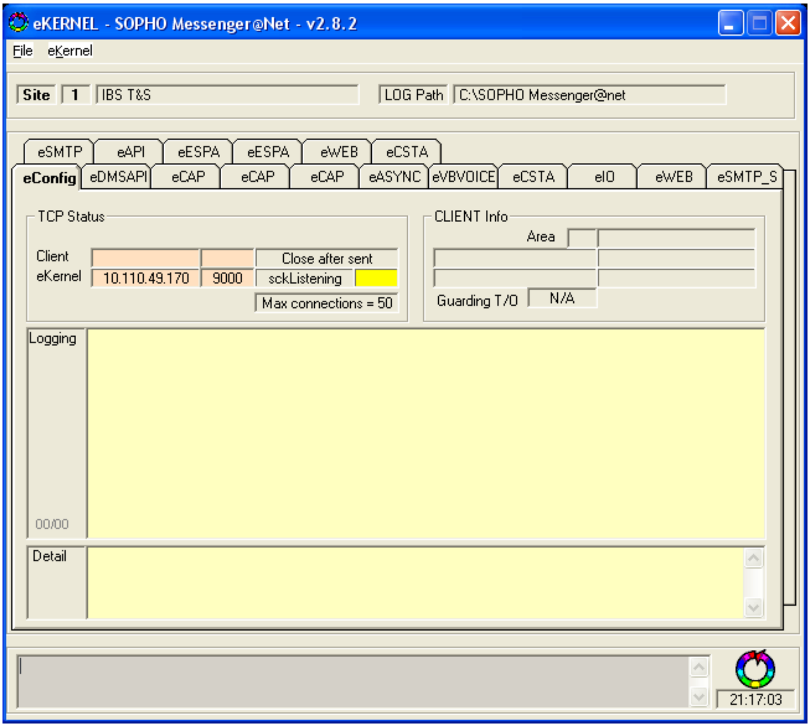
- If the system is already operational, the eKERNEL process is already running (either with or without control of eTM module).

Figure 392
Starting eKERNEL



When eKERNEL is started, the first tab shows the eCONFIG module. In Figure 393 on page 1026, eKERNEL is shown with IP address 10.110.49.170 port 9000.

Figure 393
eKERNEL interface



Site 1 IBS T&S

LOG Path C:\SOPHO Messenger@net

Client

eKernel 10.110.49.170 9000 sckListening

Close after sent

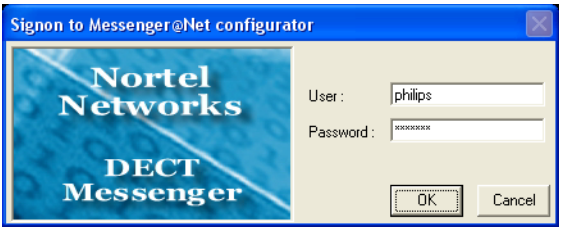
Max connections = 50

Guarding T/O N/A

21:17:03

When the eCONFIG task is started, an authentication check is performed, which requires you to enter a valid user and password as shown in Figure 394 on page 1027. This information is checked against the eCONFIG_USER table in Messenger_CFG.MDB.

Figure 394
eCONFIG Signon



Signon to Messenger@Net configurator

User : philips

Password : *******

The default installation provides two Users:

User = admin, Password = admin

User = phillips, Password = philips

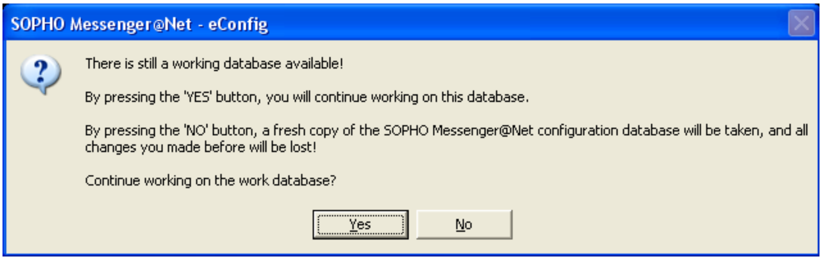
An operational environment usually features other users as well, each of them with an associated password and security level.

> ***Note:*** Nortel strongly recommends assigning a secret password to default users.

> ***Note:*** It is possible to keep the changes of eCONFIG suspended, so that you can resume the configuration later. As a result, the changes are not applied immediately, and the workspace of temporary changes is stored online. eCONFIG checks for such a previous workspace at start-up.

If a workspace is still available, the user is prompted whether to resume the previous session, or to ignore the changes made so far and start with a new copy, as shown in Figure 395 on page 1028. If the last eCONFIG session has been applied (made into production), the user does not see this message.

Figure 395
eCONFIG database already exists


SOPHO Messenger@Net - eConfig

There is still a working database available!

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

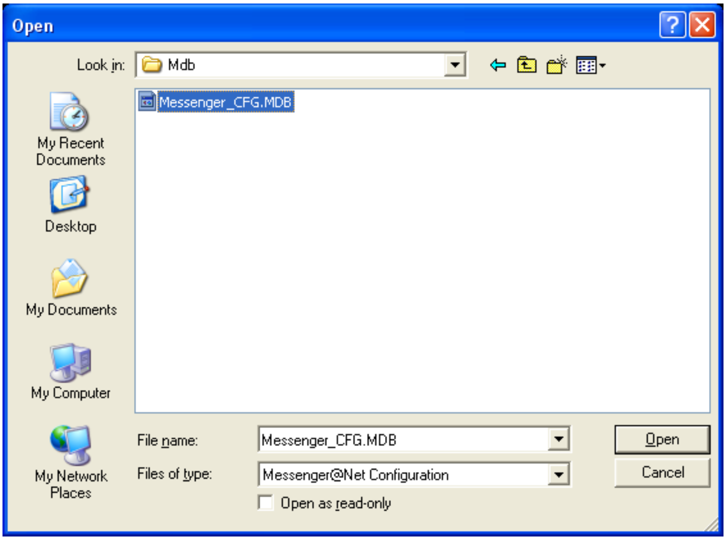
By pressing the 'NO' button, a fresh copy of the SOPHO Messenger@Net configuration database will be taken, and all changes you made before will be lost!

Continue working on the work database?

When you start eCONFIG for the first time (both locally and distributed) the eCONFIG.INI has no path on which the MESSENGER_CFG database is stored. Once the CONFIG.INI file is updated manually to provide a valid path, the system no longer prompts for the location.

If eCONFIG.INI does not yet contain a path, the dialog box in Figure 396 is shown.

Figure 396
Select the correct path


Look in: Mdb

Messenger_CFG.MDB

File name: Messenger_CFG.MDB

Files of type: Messenger@Net Configuration

□ Open as read-only

In the dialog box shown in Figure 396 on page 1028:

1. Navigate to the folder where MESSENGER_CFG resides.
2. Select the MESSENGER_CFG file.
3. Press **OK.**

   The eCONFIG.INI is updated automatically with the selected path.

The most common location for local users to find MESSENGER.CFG is as follows:

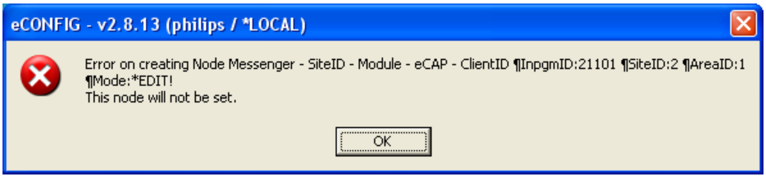
C:\SOPHO Messenger@Net\Mdb\Messenger_CFG_MDB

When distributed users are given access to eCONFIG, you must make the directory path of the MESSENGER.CFG available to the network, which is usually performed by sharing the path. The distributed users can then navigate through the Network Neighborhood to select the appropriate file. Contact the system administration regarding security, and network questions related to access priveledges.

> ***Note:*** In some environments, distributed maintenance can lead to redesign of the network topology, especially in cases where DECT Messenger is initially installed in a separate network.

If a number of message windows open, such as in the example shown in Figure 397, there are inconsistencies in the original database. This is sometimes caused when the administrator creates a corrupt configuration using eGRID or MS Access. For example, a record is defined in eKERNEL_INPGM or eKERNEL_TCPCLIENT without an associated area, and so on.

Figure 397
Start-up error message



eCONFIG - v2.8.13 (philips / *LOCAL)

Error on creating Node Messenger - SiteID - Module - eCAP - ClientID ¶InpgmID:21101 ¶SiteID:2 ¶AreaID:1 ¶Mode:*EDIT!
This node will not be set.

eCONFIG is designed to preserve data integrity during data entry only, which means automatic cleanup does not take place. If messages such as the one in Figure 397 on page 1029 open, perform the following:

1 Check data consistency using eGRID interface.

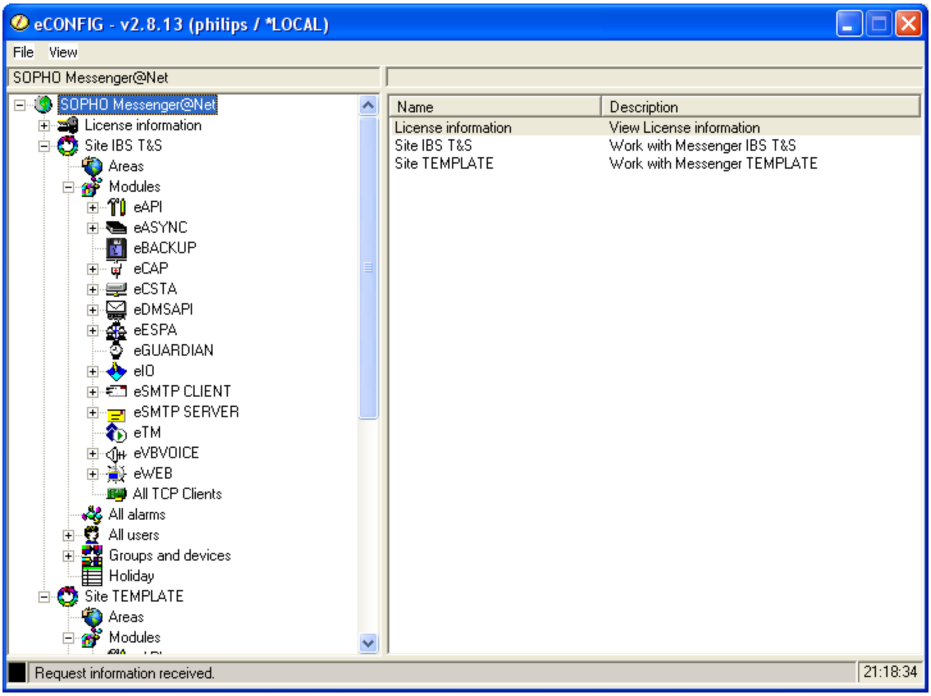
2 If possible, resolve any issues prior to using eCONFIG.

New configurations entered immediately through eCONFIG do not expose this phenomenon.

Figure 397 on page 1029 shows an example of such a warning, indicating a problem in site 2, area 1, input program 21101, type eCAP. This can be caused by a bad configuration in eKERNEL_TCPLCIENT or eKERNEL_INPGM or eKERNEL_SITE or eKERNEL_AREA.

The eCONFIG features an interface as shown in Figure 398 on page 1031. Contact Nortel for more information on training sessions for the DECT Messenger.

Figure 398
The eCONFIG interface



Name	Description
License information	View License information
Site IBS T&S	Work with Messenger IBS T&S
Site TEMPLATE	Work with Messenger TEMPLATE

Request information received.

To make any configuration change, left-click a node in the left panel of the window.

- Right-click the node to access a pop-up a menu, with menu options depending on the selected environment.
- Double-click the node to perform maintenance of the current selection, depending on the selected node.

Double-click Site1 to access the Site window as shown in Figure 399 on page 1032.

- Click on any of the nodes to reveal more details in the right panel of the window. Depending on the selected item, this affects some or all of the following:

— Label

— Text box

— Drop-down list

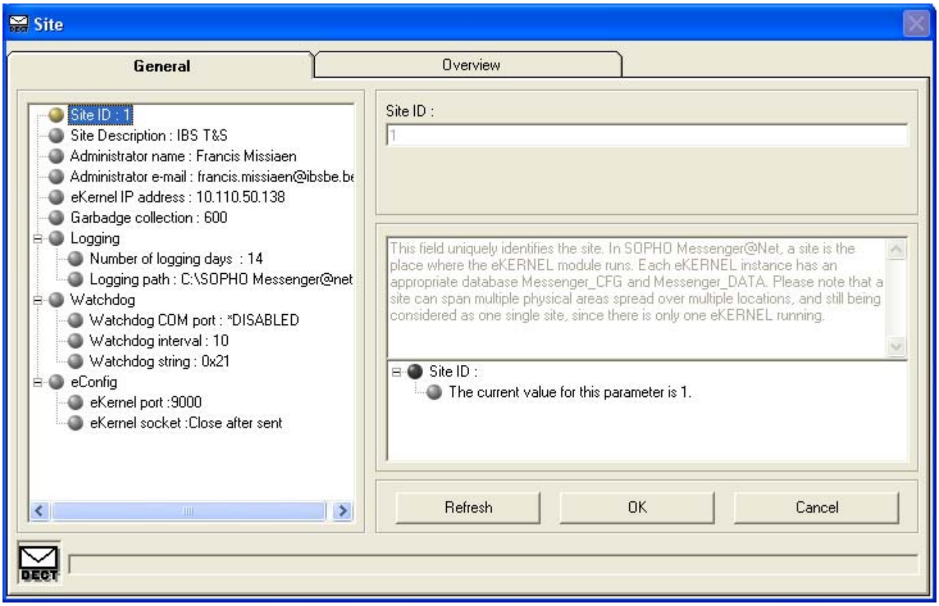
— Grid

— Label with Browse button

— Date picker

— Time picker

Figure 399
Site configuration window



- Site ID : 1
- Site Description : IBS T&S
- Administrator name : Francis Missiaen
- Administrator e-mail : francis.missiaen@ibsbe.be
- eKernel IP address : 10.110.50.138
- Garbadge collection : 600
- Logging
  - Number of logging days : 14
  - Logging path : C:\SOPHO Messenger@net
- Watchdog
  - Watchdog COM port : *DISABLED
  - Watchdog interval : 10
  - Watchdog string : 0x21
- eConfig
  - eKernel port :9000
  - eKernel socket :Close after sent

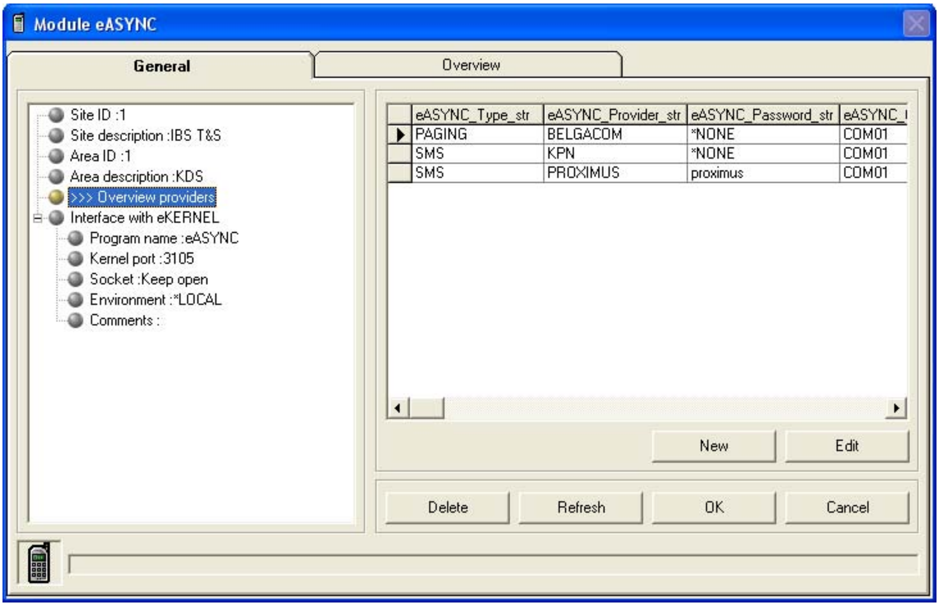
Site ID :
1

This field uniquely identifies the site. In SOPHO Messenger@Net, a site is the place where the eKERNEL module runs. Each eKERNEL instance has an appropriate database Messenger_CFG and Messenger_DATA. Please note that a site can span multiple physical areas spread over multiple locations, and still being considered as one single site, since there is only one eKERNEL running.

- Site ID :
  - The current value for this parameter is 1.

An example of a Grid view is shown in Figure 400 on page 1033. In most cases, these nodes are indicated with >>> symbol, indicating the one-to-many relationship that is common with these nodes. For example, a single eASYNC instance (site 1 – area 1) can have definitions for multiple providers, each of them with a separate set of parameters.

Figure 400
GRID view



- Site ID :1
- Site description :IBS T&S
- Area ID :1
- Area description :KDS
- >>> Overview providers
- Interface with eKERNEL
  - Program name :eASYNC
  - Kernel port :3105
  - Socket :Keep open
  - Environment :*LOCAL
  - Comments :

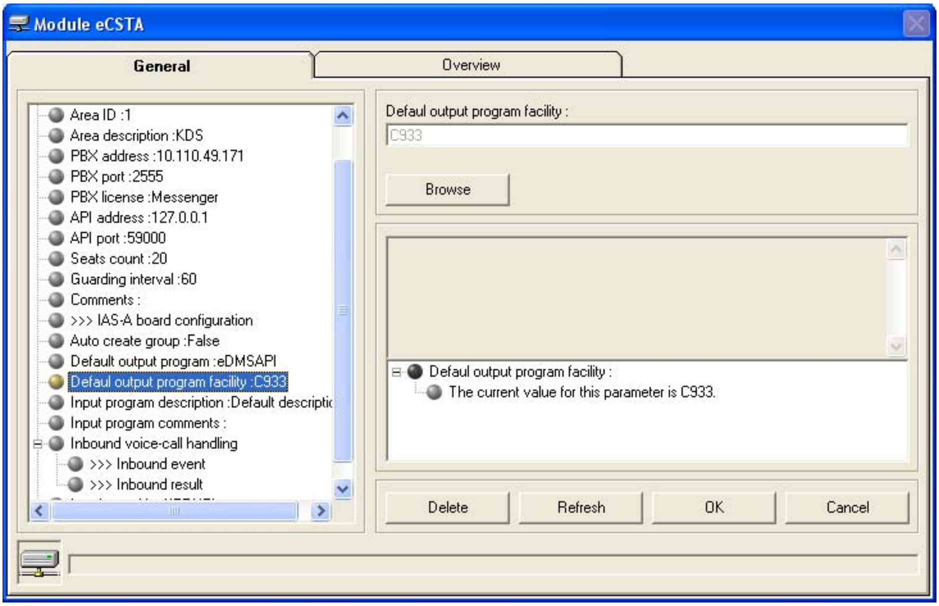
	eASYNC_Type_str	eASYNC_Provider_str	eASYNC_Password_str	eASYNC_I
▶	PAGING	BELGACOM	*NONE	COM01
	SMS	KPN	*NONE	COM01
	SMS	PROXIMUS	proximus	COM01

Detailed records on the Grid can be edited by selecting the record in the left-hand area of the grid (indicated with an arrow) and clicking **Edit**. New records can be added by clicking **New**.

Records can be deleted by first clicking **Edit**, and then clicking **Delete**.

Figure 401 on page 1034 illustrates the Browsing option. The current value is shown in a Label; use the **Browse** button to select a new value.

Figure 401
Browsing option



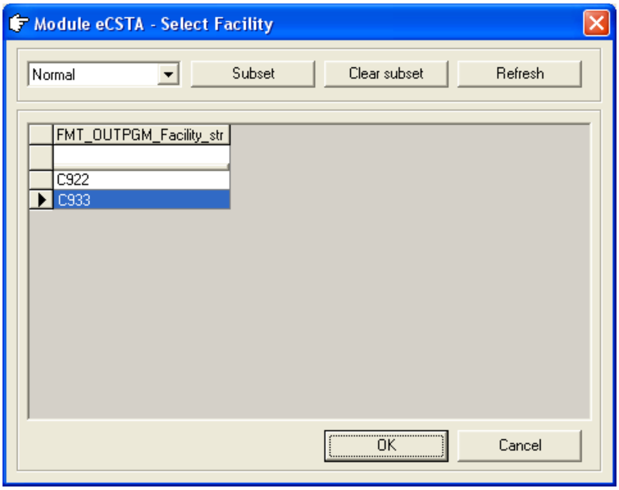
Area ID :1
Area description :KDS
PBX address :10.110.49.171
PBX port :2555
PBX license :Messenger
API address :127.0.0.1
API port :59000
Seats count :20
Guarding interval :60
Comments :
>>> IAS-A board configuration
Auto create group :False
Default output program :eDMSAPI
Defaul output program facility :C933
Input program description :Default descriptic
Input program comments :
Inbound voice-call handling
>>> Inbound event
>>> Inbound result

Defaul output program facility :
C933

Defaul output program facility :
The current value for this parameter is C933.

Click on **Defaul output program facility** to view information for it. Click **Browse** to open the Select Facility window as shown in Figure 402 on page 1035. In this interface a record can be selected with the left-hand section of the Grid interfaces. When a record is selected, the **OK** button is enabled. When **Cancel** is pressed, the original value is maintained.

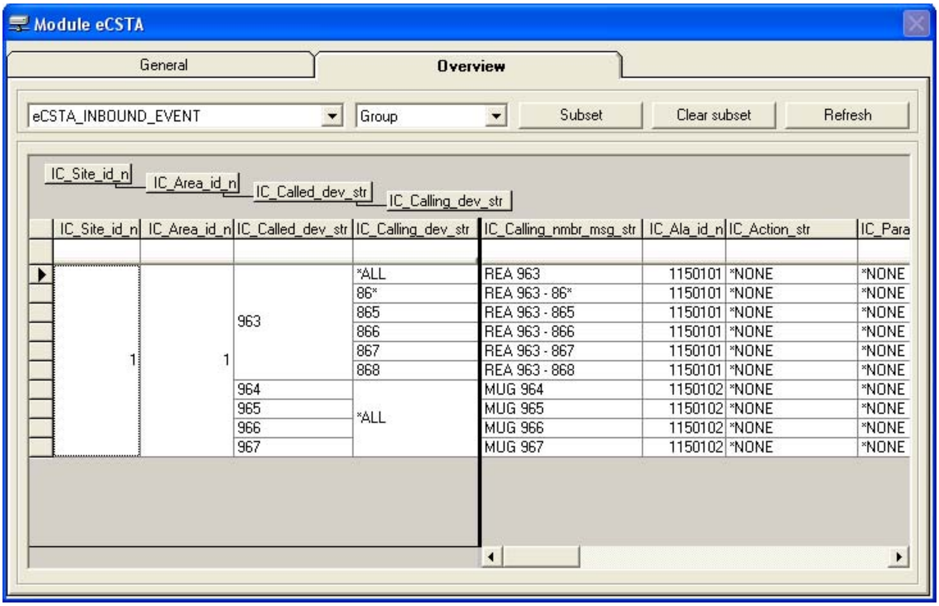
Figure 402
Browsing an output program



FMT_OUTPGM_Facility_str
C922
C933

An advanced grid interface is available in many situations, as shown in Figure 403 on page 1036. As well, many module-related windows include an Overview tab, which provides access to only those tables that are relevant. A table selector is shown on the left. Use the drop-down list to choose the function from the following options: **Normal**, **Inverted**, or **Group**. The **Group** function provides access to a drag-and-drop interface, where you can arrange column headers to create groups of records in a hierarchical order, as shown Figure 403 on page 1036.

Figure 403
Advanced GRID interface

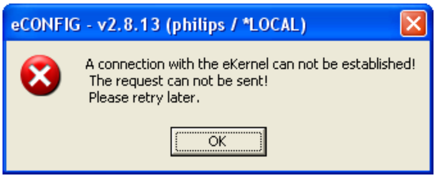


eCSTA_INBOUND_EVENT
Group

IC_Site_id_n	IC_Area_id_n	IC_Called_dev_str	IC_Calling_dev_str	IC_Calling_nmbr_msg_str	IC_Ala_id_n	IC_Action_str	IC_Para
1	1	963	*ALL	REA 963	1150101	*NONE	*NONE
			86*	REA 963 - 86*	1150101	*NONE	*NONE
			865	REA 963 - 865	1150101	*NONE	*NONE
			866	REA 963 - 866	1150101	*NONE	*NONE
			867	REA 963 - 867	1150101	*NONE	*NONE
			868	REA 963 - 868	1150101	*NONE	*NONE
		964	*ALL	MUG 964	1150102	*NONE	*NONE
		965		MUG 965	1150102	*NONE	*NONE
		966		MUG 966	1150102	*NONE	*NONE
		967		MUG 967	1150102	*NONE	*NONE

The message shown in Figure 404 appears when the link with eKERNEL cannot be established or is no longer available. During initial local configuration, this can indicate that the eKERNEL is not started. When you use eCONFIG on a remote PC, you cannot make system changes. However, any changes you make to groups, devices, and users are implemented immediately on the Messenger PC database.

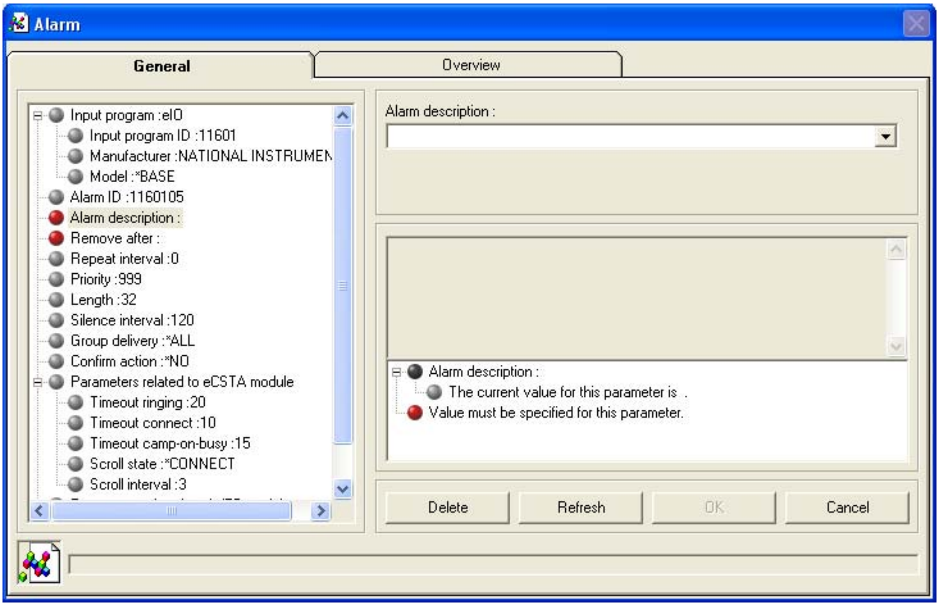
Figure 404
eKERNEL error: connection cannot be established



A connection with the eKernel can not be established!
The request can not be sent!
Please retry later.

On the maintenance windows, there is an extensive consistency check on data validation of several parameters. These nodes are indicated in red. For example, on the Alarm window shown in Figure 405, two parameters are in error. The selected error is explained on the right-hand panel of the window, in a statement such as “Value must be specified for this parameter.”

Figure 405
Alarms



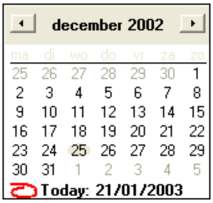
- Input program :eI0
  - Input program ID :11601
  - Manufacturer :NATIONAL INSTRUMEN
  - Model :*BASE
- Alarm ID :1160105
- Alarm description :
- Remove after :
- Repeat interval :0
- Priority :999
- Length :32
- Silence interval :120
- Group delivery :*ALL
- Confirm action :*NO
- Parameters related to eCSTA module
  - Timeout ringing :20
  - Timeout connect :10
  - Timeout camp-on-busy :15
  - Scroll state :*CONNECT
  - Scroll interval :3

Alarm description :

- Alarm description :
  - The current value for this parameter is .
- Value must be specified for this parameter.

The guarding maintenance window features a date selector, as shown in Figure 406. Use this to select a date.

Figure 406
Date selector



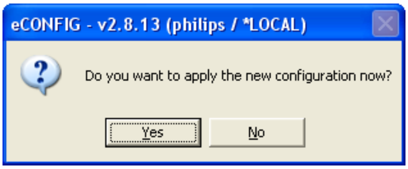
december 2002

ma	di	wo	do	vr	za	zo
25	26	27	28	29	30	1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30	31	1	2	3	4	5

Today: 21/01/2003

If you want to abort the configuration process, you can use the Exit menu. A confirmation requester appears, as shown in Figure 407.

Figure 407
Confirm Applying configuration



eCONFIG - v2.8.13 (philips / *LOCAL)

Do you want to apply the new configuration now?

Choose one of the following:

- If you answer **No**, the changes you made are stored online on the hard disk, and the can resume the configuration process later. Note that maintenance of groups, devices, and users are always applied immediately, and are not part of this resume procedure.
- If you answer **Yes,** the apply process is initiated.

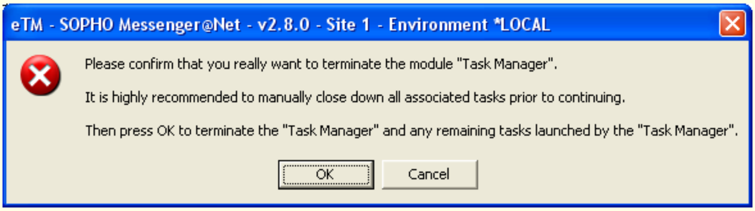
  If you answer **Yes**, follow the steps discussed in “Applying a new configuration” on page 1038.

Applying a new configuration

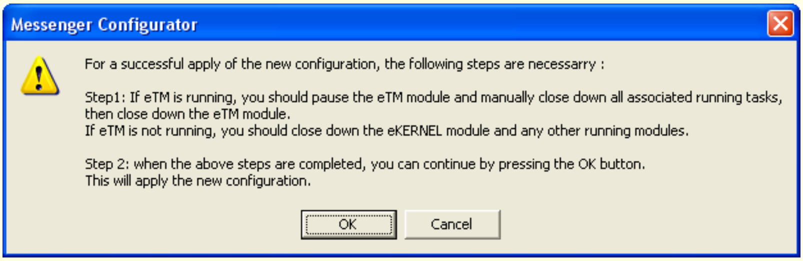
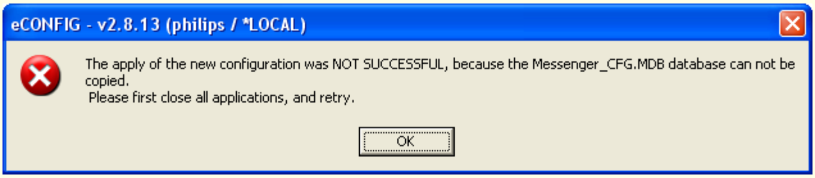
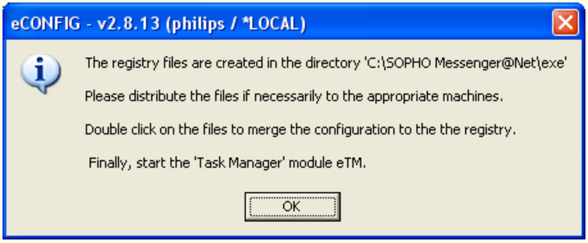
Before the new configuration can be applied, you must free all locks to the current database. This means the DECT Messenger environment must be stopped, so eKERNEL and all associated modules must be stopped. Before stopping eKERNEL, take into consideration that all pending alarms are cleared at restart. Also, while eKERNEL and associated modules are down, no input and output is performed, and alarm input and distribution is suspended. Thus, an apply procedure requires careful planning.

- When eTM is not operational, you can close down every application manually. All modules, including eKERNEL, can usually be stopped by clicking the close control box in the right top of each window. Note that any program that has locks Messenger_CFG.MDB must be closed, for example, eGRID, Microsoft Access, and so on. You can stop the Apache web server as well.
- When eTM is operational, refer to the special instructions under the heading "Module – eTM" on page 1205. Because eTM is monitoring jobs, this includes the following steps:

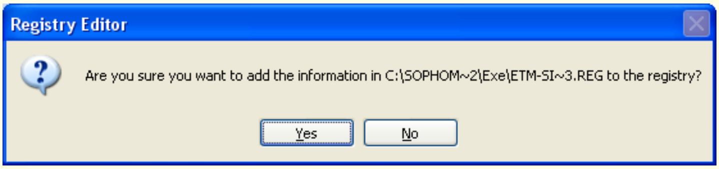
Procedure 239
Apply a new configuration (Part 1 of 4)

Step	Action
1	Shut down eTM.
	• Select the **Stop** menu option. • Close all modules. • Selecting the **Exit** menu option.
2	Confirm your choice to shut down eTM.
	Click **OK**.  eTM - SOPHO Messenger@Net - v2.8.0 - Site 1 - Environment *LOCAL Please confirm that you really want to terminate the module "Task Manager". It is highly recommended to manually close down all associated tasks prior to continuing. Then press OK to terminate the "Task Manager" and any remaining tasks launched by the "Task Manager".

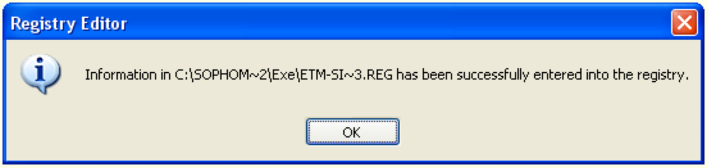
Procedure 239
Apply a new configuration (Part 2 of 4)

Step	Action
3	Apply the new configuration.
	Click OK.  Messenger Configurator For a successful apply of the new configuration, the following steps are necessarry : Step1: If eTM is running, you should pause the eTM module and manually close down all associated running tasks, then close down the eTM module. If eTM is not running, you should close down the eKERNEL module and any other running modules. Step 2: when the above steps are completed, you can continue by pressing the OK button. This will apply the new configuration.
4	Troubleshoot (if necessary).
	If the following dialog box opens, the apply process failed. This usually occurs when some modules remain active, for example, when eGRID or eKERNEL are still running. Identify the reason for the failure and retry, or postpone the apply to a later time.  eCONFIG - v2.8.13 (philips / *LOCAL) The apply of the new configuration was NOT SUCCESSFUL, because the Messenger_CFG.MDB database can not be copied. Please first close all applications, and retry. - Click **OK**.
5	Acknowledge successful application of the new configuration files.
	If the apply process was successful, the following dialog box appears. Click **OK**.  eCONFIG - v2.8.13 (philips / *LOCAL) The registry files are created in the directory 'C:\SOPHO Messenger@Net\exe' Please distribute the files if necessarily to the appropriate machines. Double click on the files to merge the configuration to the the registry. Finally, start the 'Task Manager' module eTM.

Procedure 239
Apply a new configuration (Part 3 of 4)

Step	Action
6	Remove old registry keys.
	Nortel recommends using REGDIT to manually remove the old registry keys in the following section: `[HKEY_CURRENT_USER\Software\Philips\SOPHO Messenger@Net]`
7	Locate the new registry file.
	As part of the registration process, one or more registry export files are created in the path **C:\SOPHO Messenger@Net\Exe**. eTM - Site 1 - Environment LOCAL.reg ***Note:*** When more than one registry file is available, check the contents and filename to identify the local file and remote files. Depending on the environment parameter of each module, one or more registry files are created. ***Note:*** Registry files for distributed PC environments (for example, an instance of eIO resides on a remote networked PC) must be manually distributed to the target machine and applied there, after stopping eTM and associated processes.
8	Merge the registry file.
	• Double-click the registry file to merge the contents into the registry repository. • Click **OK**.  Registry Editor Are you sure you want to add the information in C:\SOPHOM~2\Exe\ETM-SI~3.REG to the registry?

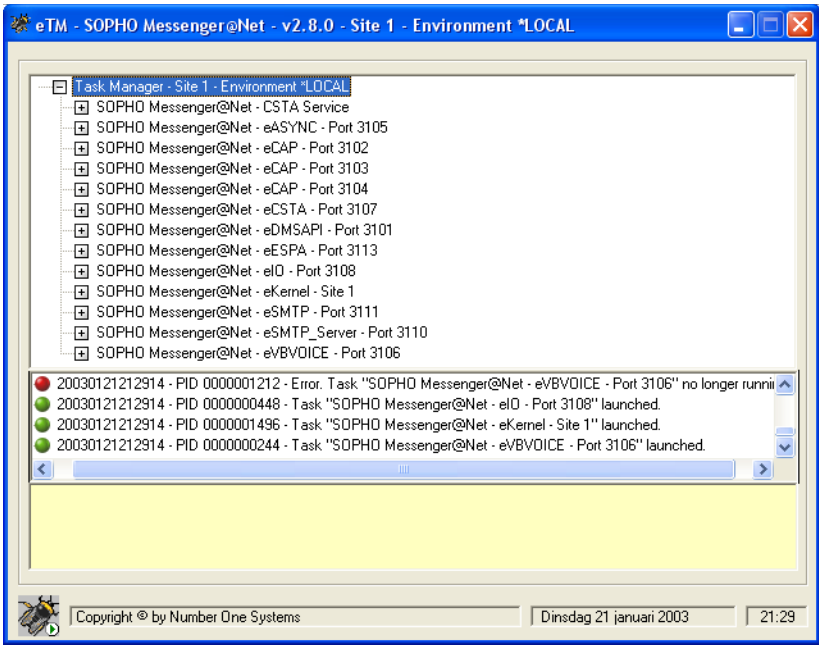
Procedure 239
Apply a new configuration (Part 4 of 4)

Step	Action
9	Acknowledge the completion of the merge operation.
	After merging the data, the following message box opens.  Information in C:\SOPHOM~2\Exe\ETM-SI~3.REG has been successfully entered into the registry.
10	Restart the environment.
	Choose either of the following: • If you use eTM, the Task Manager retrieves the new configuration from the local registry repository, and activates the configured modules. This is shown in Figure 408 on page 1043. Refer to the documentation of the “Module – eTM” on page 1205 for additional information on the Task Manager. • If you prefer to work in the traditional way by means of shortcuts in the start-up group, you must verify the configuration settings to determine the parameters needed for the appropriate shortcuts. Nortel recommends using the eTM module in R2.8 and later.

END

The eTM module interface is shown in Figure 408 on page 1043.

Figure 408
eTM module interface



eTM - SOPHO Messenger@Net - v2.8.0 - Site 1 - Environment *LOCAL

```
⊟ Task Manager - Site 1 - Environment *LOCAL
   ⊞ SOPHO Messenger@Net - CSTA Service
   ⊞ SOPHO Messenger@Net - eASYNC - Port 3105
   ⊞ SOPHO Messenger@Net - eCAP - Port 3102
   ⊞ SOPHO Messenger@Net - eCAP - Port 3103
   ⊞ SOPHO Messenger@Net - eCAP - Port 3104
   ⊞ SOPHO Messenger@Net - eCSTA - Port 3107
   ⊞ SOPHO Messenger@Net - eDMSAPI - Port 3101
   ⊞ SOPHO Messenger@Net - eESPA - Port 3113
   ⊞ SOPHO Messenger@Net - eIO - Port 3108
   ⊞ SOPHO Messenger@Net - eKernel - Site 1
   ⊞ SOPHO Messenger@Net - eSMTP - Port 3111
   ⊞ SOPHO Messenger@Net - eSMTP_Server - Port 3110
   ⊞ SOPHO Messenger@Net - eVBVOICE - Port 3106
```

```
● 20030121212914 - PID 0000001212 - Error. Task "SOPHO Messenger@Net - eVBVOICE - Port 3106" no longer runnii
● 20030121212914 - PID 0000000448 - Task "SOPHO Messenger@Net - eIO - Port 3108" launched.
● 20030121212914 - PID 0000001496 - Task "SOPHO Messenger@Net - eKernel - Site 1" launched.
● 20030121212914 - PID 0000000244 - Task "SOPHO Messenger@Net - eVBVOICE - Port 3106" launched.
```

Copyright © by Number One Systems | Dinsdag 21 januari 2003 | 21:29

Install PC – Reinstalling Nortel DECT Messenger

This chapter provides instructions to help you upgrade DECT Messenger within the same Major release.

Follow the steps in Procedure 240 to reinstall DECT Messenger.

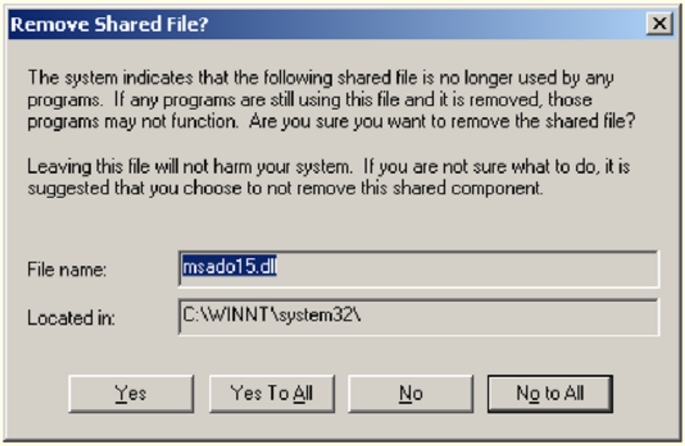
Procedure 240
Upgrading DECT Messenger

Step	Action
1	Stop **DECT Messenger**.
	End all activity of **DECT Messenger by** closing all running modules and (if available) task manager.
2	Create Backups.
	Make a backup of the current environment, by storing the following directories, (a ZIP file is recommended): C:\SOPHO Messenger@Net and C:\SOPHO Messenger@Net eCONFIG.

Procedure 240
Upgrading DECT Messenger

Step	Action
3	Back up configuration and log files.
	• Make a backup copy of the file Messenger_CFG.MDB, which is found in C:\SOPHO Messenger@Net\Mdb. It is important that you have this file available when you reinstall DECT Messenger, because it contains your full configuration. • If you want to preserve logging data, make backups of the following folders: C:\SOPHO Messenger@Net\Log and C:\SOPHO Messenger@Net\eLOG (if available).
4	Uninstall prerequisites (optional).
	If any of the prerequisite software you are using must be upgraded, it is recommended to uninstall this software now. You must install this software again during the installation of the Messenger.

Procedure 240
Upgrading DECT Messenger

Step	Action
5	Uninstall the Messenger.
	• Click on the **Start** button in the Windows taskbar, and choose **Control Panel > Add or Remove Programs**. • Select **DECT Messenger** from the list. • Click **Remove**. • When the following dialog box opens, click **No to All**.  Remove Shared File? The system indicates that the following shared file is no longer used by any programs. If any programs are still using this file and it is removed, those programs may not function. Are you sure you want to remove the shared file? Leaving this file will not harm your system. If you are not sure what to do, it is suggested that you choose to not remove this shared component. File name: msado15.dll Located in: C:\WINNT\system32\ **IMPORTANT!** In the **Remove Shard File?** dialog box, do not choose any option other than **No to All**, because doing so removes critical files, causing the reinstallation to fail. • Uninstall eConfig. • Uninstall eCONFIG instances installed on other systems in the network. • Remove the following directories: C:\SOPHO Messenger@Net, and C:\SOPHO Messenger@Net eConfig.

Procedure 240
Upgrading DECT Messenger

Step	Action
6	Install DECT Messenger.
	Install DECT Messenger from the latest CDROM or DVD image, using the steps described in “General – Install PC” on page 805. **IMPORTANT!** After completing the steps in “Install PC – Step 2 – Nortel DECT Messenger” on page 873, you must restore the file Messenger_CFG.MDB, which you backed up Step 3 of this procedure, to the folder: C:\SOPHO Messenger@Net\Mdb. If you saved \Log or \eLOG you can restore that data as well. **IMPORTANT!** Never reuse or apply an old configuration generated with eCONFIG prior to the Messenger version you are using. Therefore, when eCONFIG opens a dialog informing you that a working database is available, you must answer **No**.

END

Module eAPI

Introduction

The module eAPI is not a real module, but rather a description of a public Application Program Interface (API) for third-party developers who want to communicate with DECT Messenger. This chapter is intended for developers who want to build an interface to the eKERNEL module.

The objective of this document is to describe how developers can integrate applications with DECT Messenger. Note that the eAPI interface has limited capabilities. An alternative to developing your own program is to contact Nortel and request the development of an integrated solution.

Limitations

Input program functionality only

The functionality implemented in the eAPI interface is limited to the sending of message requests to the eKERNEL module. This process is carried out through so-called message request (msgrqs) transactions. Therefore, third-party application programs that are created using eAPI technology are limited to input program functionality only.

No central configuration

A second limitation in eAPI is that there currently is no support for configuration request messages. In all other modules, there is a central configuration database, where all relevant parameters are centrally administered. This process is normally carried out through configuration requests (cfgrqs) from the module to eKERNEL and configuration replies (cfgrpy) from eKERNEL to the module. As a result, third-party developers must provide their own configuration techniques (through registry, .INI files, database, command line parameters, and so on) to control the behaviour of their applications.

Basic architecture

The architecture of eAPI is embedded in the eKERNEL module. The eAPI interface refers to the ability of eKERNEL to provide a TCP server, which listens to a specified port, and receives TCP sockets packages that contain message requests.

Therefore, when building an eAPI-based third-party product, you require an application that acts as TCP client and establishes a sockets connection to the eKERNEL module, which acts as TCP server.

Depending on the eKERNEL settings, the sockets connections are kept open or are closed after reception of a request. When the socket is kept open, the port remains allocated to the connected client. This is suitable for implementations where a dedicated connection is required. If multiple clients must address the same eKERNEL port, Nortel recommends that you close the socket after each ad hoc request. With this approach, a single port can serve to accept message requests from multiple input sources.

Message format

Message requests to eKERNEL must be formatted according to specific rules. A sample request is illustrated in Figure 409.

Figure 409
Sample message request

```
<xml><msgrqs><set_or_reset>*SET</
set_or_reset><group>1</group><alarmdescr>2</
alarmdescr><msg>3</msg><remove_after>*SENT</
remove_after></msgrqs></xml>
```

The following rules apply:

- The string must start with <xml><msgrqs> and end with </msgrs></xml> tags
- At the end of the string, a carriage return (ASCII 13) and line feed (ASCII 10) must be appended
- The message request must contain 5 parameters
    - The parameter set_or_reset must start with <set_or_reset> tag and end with the </set_or_reset> tag
    - The parameter group must start with <group> tag and end with the </group> tag
    - The parameter alarmdescr must start with <alarmdescr> and end with the </alarmdescr> tag
    - The parameter msg must start with <msg> tag and end with the </msg> tag
    - The parameter remove_after must start with <remove_after> tag and end with the </remove_after> tag
- The parameter set_or_reset can supports the following values: *SET or *RESET
- The parameter group refers to a configured group defined in the eKERNEL_GROUP table
- The parameter alarm_descry refers to a configured alarm description, defined in the eKERNEL_ALARM table
- The parameter remove_after supports the following values: *SENT, *RESET or *CALC

Refer to the appropriate chapters of this document for more information on the tables.

Introduction to a sockets client

Refer to the documentation of your development environment for more information on sockets programming.

The code sample shown in Figure 410 on page 1054 describes an introduction for beginner programmers on how to build a very simple Visual Basic program that contacts the DECT Messenger eKERNEL module and delivers a message request. Note that the source code is provided for illustration only, and does not include error recovery.

Creating a basic sockets client using Visual Basic

1 Start Visual Basic, and open a new project of Standard .EXE type. In the menu, choose **Project** > **Components** and add the Microsoft Winsock Control component to the project. This component usually refers to C:\WINNT\system32\MSWINSCK.OCX.

2 Drag a **CommandButton** control to the form. The default name Command1 can be used.

3 Drag a **Winsock** control to the form. The default name `Winsock1` can be used.

4 Add the code shown in Figure 410 on page 1054 in the **Private Sub Command1_Click**.

5 Specify the correct IP address (the IP address of the system where eKERNEL runs) and port number (the configured port for eAPI, as defined in eKERNEL_TCPCLIENT table).

6 Run the program. If you click the Command1 button, a message request is sent to eKERNEL.

7 You can alter the code shown in Figure 410 on page 1054 to specify the correct parameters for the parameters group (use one of the values specified in the eKERNEL_GROUP table), alarm description (use one of the values specified in the eKERNEL_ALARM table), and so on.

Note: The code shown in Figure 410 on page 1054 is not intended to represent a reliable TCP client, and is meant only to illustrate how to start programming with eAPI using minimal code entry. A real-life program must take all necessary action to handle all error conditions.

The following issues usually require improvement:

- The sample code shown in Figure 410 on page 1054 does not respond on the asynchronous connection attempt by means of the Winsock1_Connect() event. The code assumes that the connect succeeds after doing a DoEvents(). Note that the Winsock1.State must be 7 before a SendData can be requested.

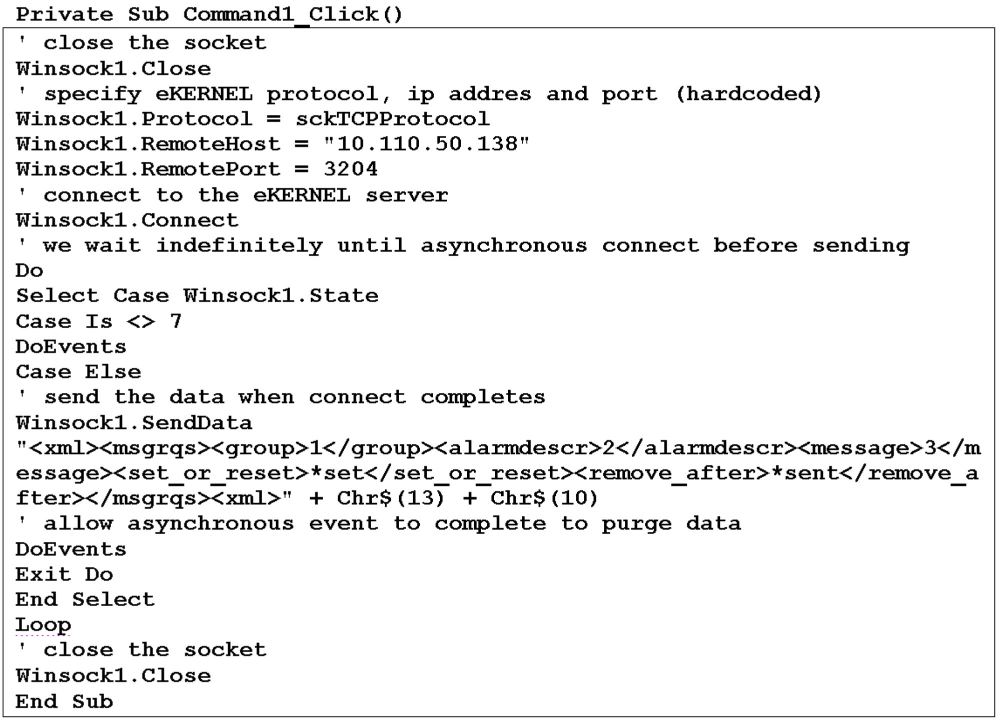
- The sample code shown in Figure 410 on page 1054 includes appropriate error recovery, but does not respond to failed connection attempts.

- The sample code shown in Figure 410 on page 1054 assumes the data is actually transmitted with the SendData, and does not check for instance on the Winsock1_SendComplete() event.

- The values for IP address and port are hard-coded, and users must be able to set them as parameters in a real-word program.

- The values in the message request are hard-coded, and must be filled with actual alarm information and appropriate configured values, as defined in the configuration database.

Figure 410
Sample socket client code



```
Private Sub Command1_Click()
' close the socket
Winsock1.Close
' specify eKERNEL protocol, ip addres and port (hardcoded)
Winsock1.Protocol = sckTCPProtocol
Winsock1.RemoteHost = "10.110.50.138"
Winsock1.RemotePort = 3204
' connect to the eKERNEL server
Winsock1.Connect
' we wait indefinitely until asynchronous connect before sending
Do
Select Case Winsock1.State
Case Is <> 7
DoEvents
Case Else
' send the data when connect completes
Winsock1.SendData
"<xml><msgrqs><group>1</group><alarmdescr>2</alarmdescr><message>3</m
essage><set_or_reset>*set</set_or_reset><remove_after>*sent</remove_a
fter></msgrqs><xml>" + Chr$(13) + Chr$(10)
' allow asynchronous event to complete to purge data
DoEvents
Exit Do
End Select
Loop
' close the socket
Winsock1.Close
End Sub
```

More extended program

Refer to “Module – eAPI sample” on page 1057 for a detailed source code listing of a more complete implementation of a Visual Basic program that implements eAPI functionality. The compiled program eAPI.exe and the source code eAPI.zip (zipped) are shipped with the DECT Messenger and the .exe is installed when you select eAPI module during custom install.

Note that this code is provided on as-is basis, and is not intended to be used without modification. Usage of the code is the responsibility of the third-party developer, as all aspects needed to make the code reliable are not implemented.

The eAPI program is designed to provide the same look and feel as is found in other DECT Messenger modules.

Some typical features include:

- Ability to specify certain run-time parameters of the program by means of the command line parameters in the shortcut, such as: /Site:2 /eKernel address:*LOCAL /eKernel port:3209 /Log drive:C
- Queuing mechanism that allows the module to handle situations in which eKERNEL is temporarily unavailable. This is carried out by means of list boxes.
- Logging facilities on-screen, with the option to left-click a log entry to see details.
- Logging facilities to disk, in the same directory structure mechanism as used for all other modules.

Real-world examples

Using eAPI, you can write external applications in your language of choice (Visual Basic, C++, Java, and so on). These applications can collect alarm information from external systems, for example by means of asynchronous communications or a network connection.

It is important however to realize that the scope of the eAPI interface to eKERNEL is limited, and there is for instance no ability to give feedback to eAPI (and the alarm system) upon successful or failed message delivery within DECT Messenger.

Nortel recommends investigating alternatives, such as re-using an existing module of DECT Messenger (for example, eCAP generic) or contacting Nortel to request the development of a new integrated module. There is a road-map procedure within the Nortel group that keeps track of all new requirements.

Module – eAPI sample

```
eAPI_form - 1
Option Explicit
' ---------------------------------------
' This program requires a valid command$
' ---------------------------------------
' /Site:1
' /eKernel address:*LOCAL or value xxx.xxx.xxx.xxx
' /eKernel port:2001
' /Log drive:C
' ---------------------------------------
Private Function parse_cmd_line(keyword As String) As String
' This routine isolates the value of a keyword from the command$
Dim lcl_cmd As String
Dim lcl_str As Integer
Dim lcl_end As Integer
On Error Resume Next
Err = 0
lcl_cmd = g_command
lcl_str = InStr(1, UCase(lcl_cmd), "/" & UCase(keyword) & ":")
If lcl_str = 0 Then
parse_cmd_line = "N/A"
log "S", "INF", "Warning : parameter '" & keyword & "' not available in
'" & lcl_cmd & "'
"
Else
lcl_end = InStr(lcl_str + 1, UCase(lcl_cmd) + " /", "/")
parse_cmd_line = Mid$(g_command + Space$(5), lcl_str + 2 + Len(keyword),
lcl_end - lcl_st
r - Len(keyword) - 3)
End If
If Err Then
MsgBox (Err.Description & " - Unexpected error in parse_cmd_line() func-
tion")
```

```
log "E", "ERR", Err.Description & " - Unexpected error in parse_cmd_line()
function"
End If
On Error GoTo 0
End Function
Private Function parse_xml(keyword As String, xml As String) As String
' Isolates the 'value' for a 'keyword' from a 'xml' string
' When no value is found, 'N/A' is returned
On Error Resume Next: Err = 0
Dim lcl_start As Integer
Dim lcl_end As Integer
Dim lcl_from As String
Dim lcl_to As String
Dim lcl_value As String
lcl_from = LCase$("<" & keyword & ">")
lcl_to = LCase$("</" & keyword & ">")
lcl_start = InStr(1, LCase$(xml), lcl_from)
lcl_end = InStr(lcl_start + Len(lcl_from), LCase$(xml), lcl_to)
lcl_value = Mid$(xml, lcl_start + Len(lcl_from), 1 + lcl_end - lcl_start
- Len(lcl_to))
If Err Then
parse_xml = "N/A"
log "S", "INF", "Warning : parameter '" & keyword & "' not available in
'" & xml & "'
"
Else
parse_xml = lcl_value
End If
On Error GoTo 0
End Function
Private Sub lab_message_Click()
End Sub
Private Sub cmd_transmit_Click()
Dim lcl_xml As String
' Validate
If Trim$(txt_group) = "" Then
lab_msg = " Error. Group must be entered."
txt_group.SetFocus
Exit Sub
End If
If Trim$(txt_alarmdescr) = "" Then
lab_msg = " Error. Alarm description must be entered."
txt_alarmdescr.SetFocus
```

```
eAPI_form - 2
Exit Sub
End If
If Trim$(txt_msg) = "" Then
lab_msg = " Error. Message must be entered."
txt_msg.SetFocus
Exit Sub
End If
' Build XML string
lcl_xml = "<xml><msgrqs>" '<site>" & g_site & "</site>"
lcl_xml = lcl_xml + "<set_or_reset>" & cbo_set_or_reset & "</
set_or_reset>"
lcl_xml = lcl_xml + "<group>" & Trim$(txt_group) & "</group>"
lcl_xml = lcl_xml + "<alarmdescr>" & Trim$(txt_alarmdescr) & "</alarmde-
scr>"
lcl_xml = lcl_xml + "<msg>" & Trim$(txt_msg) & "</msg>"
lcl_xml = lcl_xml + "<remove_after>" & cbo_remove_after & "</
remove_after>"
lcl_xml = lcl_xml + "</msgrqs></xml>"
' Submit request
eAPI_form.lst_ekernel_outq.AddItem lcl_xml
' Inform user
lab_msg = " Message submitted to eKERNEL."
End Sub
Private Sub Form_QueryUnload(Cancel As Integer, UnloadMode As Integer)
Dim lcl_o As String
' Submit <pgmsts> shutdown request to ekernel if connected
On Error Resume Next: Err = 0
If ip_ekernel.State = 7 Then
lcl_o = "<xml><pgmsts><value>Shutdown</value></pgmsts></xml>"
ip_ekernel.SendData lcl_o + Chr$(13) + Chr$(10)
If Err Then
lab_msg = " Error " & Err & " - " & Err.Description
log "E", "ERR", "TCP senddata error " & Err & " - " & Err.Description & "
- " & l
cl_o & " could not be sent to eKERNEL"
Else
lst_ekernel_outq.RemoveItem 0
log "O", "TCP", lcl_o
End If
On Error GoTo 0
End If
DoEvents
```

```
' log
log "S", "INF", "Application ended"
' end
End
End Sub
Private Sub lst_log_DblClick()
' show details
On Error Resume Next: Err = 0
txt_log.Text = lst_log.List(lst_log.ListIndex)
On Error GoTo 0
show_pages
End Sub
Private Sub Form_KeyDown(KeyCode As Integer, Shift As Integer)
'F3=Exit
If KeyCode = 114 Then
Unload Me
'End
End If
End Sub
Private Sub Form_Load()
Dim lcl_rc As String
Dim lcl_o
Dim lcl_version
Dim Lcl_Msg As String
Dim lcl_h As Integer
' Set application title
Me.Caption = "eAPI - SOPHO Messenger@Net - v" & App.Major & "." & App.Minor
& "." & App.R
evision
' Startup values required to enable logging
g_log_path = "D:\SOPHO Messenger@Net"
g_log_days = 14
lab_log_path = " " & g_log_path
lab_log_days = " " & g_log_days
' Default command line parameters
eAPI_form - 3
' /Site:1 /eKernel address:*LOCAL /eKernel port:3209 /Log drive:C
g_command = Command$
If g_command = "" Then
Lcl_Msg = "Warning: eAPI is started without command line parameters." +
Chr$(10) + Ch
r$(10)
Lcl_Msg = Lcl_Msg + "Check the command string in the target value in the
```

```
properties o
f the shortcut." + Chr$(10) + Chr$(10)
Lcl_Msg = Lcl_Msg + "Please confirm to start this session with the fol-
lowing replacem
ent values:" + Chr(10) + Chr$(10)
g_command = "/Site:2 /eKernel address:*LOCAL /eKernel port:3209 /Log
drive:C"
lcl_rc = InputBox(Lcl_Msg, Me.Caption, g_command)
If lcl_rc = "" Then
End
Else
g_command = lcl_rc
End If
End If
' Initialise screen labels
lab_ekernel_remote_address = " N/A"
lab_ekernel_remote_port = " N/A"
lab_ekernel_local_address = " N/A"
lab_ekernel_local_port = " N/A"
' Get command line parameter
g_site = parse_cmd_line("Site")
g_ekernel_remote_address = parse_cmd_line("eKernel address")
g_ekernel_remote_port = parse_cmd_line("eKernel port")
g_log_drive = parse_cmd_line("Log drive")
' Handle special values
If g_ekernel_remote_address = "*LOCAL" Then g_ekernel_remote_address =
ip_ekernel.LocalIP
' Start
log "S", "INF", "Application " & Me.Caption & " started with parameters "
& g_command
' Terminate if undefined values
If g_site = "N/A" Then
lcl_rc = MsgBox("eAPI could not start. Parameter '/Site:xxx' missing in
command strin
g.", vbCritical, "eAPI - SOPHO Messenger@Net")
Unload Me
End If
If g_ekernel_remote_address = "N/A" Then
lcl_rc = MsgBox("eAPI could not start. Parameter '/eKernel ad-
dress:xxx.xxx.xxx.xxx' m
issing in command string.", vbCritical, "eAPI - SOPHO Messenger@Net")
Unload Me
End If
```

```
If g_ekernel_remote_port = "N/A" Then
lcl_rc = MsgBox("eAPI could not start. Parameter '/eKernel port:xxxxx'
missing in com
mand string.", vbCritical, "eAPI - SOPHO Messenger@Net")
Unload Me
End If
If g_log_drive = "N/A" Then
lcl_rc = MsgBox("eAPI could not start. Parameter '/Log drive:x' missing
in command st
ring.", vbCritical, "eAPI - SOPHO Messenger@Net")
Unload Me
End If
If Len(g_log_drive) <> 1 Then
lcl_rc = MsgBox("eAPI could not start. Parameter '/Log drive:x' is invalid
in command
string.", vbCritical, "eAPI - SOPHO Messenger@Net")
Unload Me
End If
' Update screen labels
lab_ekernel_remote_address = " " & g_ekernel_remote_address
lab_ekernel_remote_port = " " & g_ekernel_remote_port
' Initialise eAPI screen fields
With cbo_set_or_reset
.Clear
.AddItem "*SET"
.AddItem "*RESET"
.ListIndex = 0
End With
With cbo_remove_after
.Clear
.AddItem "*SENT"
.AddItem "*RESET"
.AddItem "*CALC"
eAPI_form - 4
.ListIndex = 0
End With
' Set socket state indicator to defaults
lab_ekernel_state.BackColor = RGB(0, 0, 0)
' Show copyright
lab_msg = " " & App.LegalCopyright
' Initialise CFGRQS variables
g_log_path = g_log_drive + ":\SOPHO Messenger@Net"
g_log_days = 14
```

```
lab_log_path = " " & g_log_path
lab_log_days = " " & g_log_days
' Ininitialise guarding
g_guarding = Timer
' Enable timer for eKernel
tim.Interval = 100
tim.Enabled = True
End Sub
Private Sub ip_ekernel_Connect()
Dim lcl_version As String
Dim lcl_o As String
' Update screen
g_ekernel_local_address = ip_ekernel.LocalIP
lab_ekernel_local_address = " " & g_ekernel_local_address
g_ekernel_local_port = ip_ekernel.LocalPort
lab_ekernel_local_port = " " & g_ekernel_local_port
' log "S", "INF", "TCP local port " & Format$(g_ekernel_local_port,
"00000") & " connected
with remote port " & Format$(g_ekernel_remote_port, "00000") & " (eKER-
NEL)"
End Sub
Private Sub ip_ekernel_DataArrival(ByVal bytesTotal As Long)
' ip data received
lab_msg = " Data arrival - " & bytesTotal & " bytes received from eKERNEL"
Dim lcl_i As String
ip_ekernel.GetData lcl_i, vbString
' Append to buffer, and isolate a valid <xml>xxxx</xml> sockets data stream
g_ekernel_buffer = g_ekernel_buffer + lcl_i
Dim lcl_str_xml As Integer
Dim lcl_end_xml As Integer
Dim lcl_dta_xml As String
' Begin Loop
Do
' Check if <xml> string occurs
lcl_str_xml = InStr(g_ekernel_buffer, "<xml>")
' Incomplete block without <xml> is not yet processed
If lcl_str_xml = 0 Then Exit Do
' Check if </xml> string occurs
lcl_end_xml = InStr(lcl_str_xml, g_ekernel_buffer, "</xml>" + Chr$(13) +
Chr$(10)
)
' Incomplete block without </xml> is not yet processed
If lcl_end_xml = 0 Then Exit Do
```

```
' Both <xml> and </xml> tags are found, isolate this data stream
lcl_dta_xml = Mid$(g_ekernel_buffer, lcl_str_xml, (lcl_end_xml -
lcl_str_xml) + 8
)
' Keep remainder of this data stream (if any is available)
g_ekernel_buffer = Mid$(g_ekernel_buffer, lcl_str_xml + Len(lcl_dta_xml))
' Add to listbox
log "I", "TCP", lcl_dta_xml
' Submit request to ekernel jobqueue
lst_ekernel_jobq.AddItem lcl_dta_xml
' End loop
Loop
End Sub
Private Sub ip_ekernel_Error(ByVal number As Integer, Description As
String, ByVal Scode As L
ong, ByVal Source As String, ByVal HelpFile As String, ByVal HelpContext
As Long, CancelDispl
ay As Boolean)
lab_msg = " Error " & number & " - " & Description
log "E", "ERR", "TCP error " & number & " - " & Description & " (eKERNEL)"
End Sub
Private Sub mnu_ekernel_disconnect_Click()
ip_ekernel.Close
lab_ekernel_state.BackColor = RGB(0, 0, 0)
g_ekernel_local_address = "N/A"
g_ekernel_local_port = "N/A"
eAPI_form - 5
lab_ekernel_local_port = " " & g_ekernel_local_port
lab_ekernel_local_address = " " & g_ekernel_local_address
End Sub
Private Sub process_ekernel()
Dim lcl_o As String
Dim lcl_version As String
' Handle sockets status - continuously attempt to stay connected
Dim lcl_ekernel_cur_state As Integer
lcl_ekernel_cur_state = ip_ekernel.State
If lcl_ekernel_cur_state <> g_ekernel_prv_state Then
g_ekernel_prv_state = lcl_ekernel_cur_state
Select Case lcl_ekernel_cur_state
Case 0
lab_ekernel_msg = " Closed"
lab_ekernel_state.BackColor = RGB(0, 0, 0)
Case 1
```

```
lab_ekernel_msg = " Open"
lab_ekernel_state.BackColor = RGB(200, 130, 0)
Case 2
lab_ekernel_msg = " Listening"
lab_ekernel_state.BackColor = RGB(255, 255, 0)
Case 3
lab_ekernel_msg = " Connection pending"
lab_ekernel_state.BackColor = RGB(200, 130, 0)
Case 4
lab_ekernel_msg = " Resolving host"
lab_ekernel_state.BackColor = RGB(200, 130, 0)
Case 5
lab_ekernel_msg = " Host resolved"
lab_ekernel_state.BackColor = RGB(200, 130, 0)
Case 6
lab_ekernel_msg = " Connecting"
lab_ekernel_state.BackColor = RGB(200, 130, 0)
Case 7
lab_ekernel_msg = " Connected"
lab_ekernel_state.BackColor = RGB(0, 200, 0)
Case 8
lab_ekernel_msg = " Closing"
lab_ekernel_state.BackColor = RGB(200, 130, 0)
Case 9
lab_ekernel_msg = " Error"
lab_ekernel_state.BackColor = RGB(128, 0, 0)
Case Else
End Select
End If
' Only process if ekernel_outq is populated
If lst_ekernel_outq.ListCount = 0 Then Exit Sub
' Not yet connected
If ip_ekernel.State <> 7 Then
On Error Resume Next
Err = 0
If ip_ekernel.State <> sckClosed Then ip_ekernel.Close
g_ekernel_local_address = "N/A"
g_ekernel_local_port = "N/A"
lab_ekernel_local_address = " " & g_ekernel_local_address
lab_ekernel_local_port = " " & g_ekernel_local_port
ip_ekernel.RemoteHost = g_ekernel_remote_address
ip_ekernel.RemotePort = g_ekernel_remote_port
ip_ekernel.Connect
```

```
DoEvents
Exit Sub
On Error GoTo 0
End If
' Connected
g_ekernel_local_address = ip_ekernel.LocalIP
g_ekernel_local_port = ip_ekernel.LocalPort
lab_ekernel_local_address = " " & g_ekernel_local_address
lab_ekernel_local_port = " " & g_ekernel_local_port
'
------------------------------------------------------------------------
--
' Handle requests in ekernel jobqueue
'
------------------------------------------------------------------------
--
While lst_ekernel_jobq.ListCount > 0
process_ekernel_jobq lst_ekernel_jobq.List(0)
lst_ekernel_jobq.RemoveItem 0
eAPI_form - 6
Wend
'
------------------------------------------------------------------------
--
' Handle requests in ekernel outq
'
------------------------------------------------------------------------
--
On Error Resume Next: Err = 0
Do While lst_ekernel_outq.ListCount > 0
lcl_o = lst_ekernel_outq.List(0)
ip_ekernel.SendData lcl_o + Chr$(13) + Chr$(10)
If Err Then
lab_msg = " Error " & Err & " - " & Err.Description
log "E", "ERR", "Error " & Err & " - " & Err.Description & " during SendData
" & lcl_
o & " to eKERNEL"
Exit Do
Else
lst_ekernel_outq.RemoveItem 0
log "O", "TCP", lcl_o
End If
Loop
```

```
On Error GoTo 0
'
-----------------------------------------------------------------------
-----
' Close socket after send
'
-----------------------------------------------------------------------
-----
DoEvents
ip_ekernel.Close
' Set socket state indicator to defaults
lab_ekernel_state.BackColor = RGB(0, 0, 0)
' Update screen
g_ekernel_local_address = ip_ekernel.LocalIP
lab_ekernel_local_address = " " & g_ekernel_local_address
g_ekernel_local_port = ip_ekernel.LocalPort
lab_ekernel_local_port = " " & g_ekernel_local_port
'----------------------------------------------------------------------
-----
End Sub
Private Sub process_ekernel_jobq(cmd As String)
Dim lcl_rc As Integer
' <xxxxxx>
If Left$(cmd + Space$(13), 13) = "<xml><xxxxxx>" Then
' TODO - you could add code here
End If
' <yyyyyy>
If Left$(cmd + Space$(13), 13) = "<xml><yyyyyy>" Then
' TODO : you could add code here
End If
End Sub
Sub show_pages()
lab_log = Format$(lst_log.ListIndex + 1, "00") & "/" & For-
mat$(lst_log.ListCount, "00")
End Sub
Private Sub tim_Timer()
Dim lcl_guarding As Variant
' Disable timer to prevent recursive calls
tim.Enabled = False
' Update clock
lab_clock = " " & Format$(Now, "hh:nn:ss")
' Update guarding
lcl_guarding = Timer - g_guarding
```

```
If lcl_guarding < 0 Then lcl_guarding = lcl_guarding + 86400
If (lab_guarding <> Format$(lcl_guarding, "00000")) Then
lab_guarding = Format$(lcl_guarding, "00000")
End If
' Process ekernel
process_ekernel
' Enable timer to resume processing
tim.Enabled = True
End Sub
Private Sub txt_log_GotFocus()
lst_log.SetFocus
End Sub
Sub log(log_type As String, log_sts As String, log_dta As String)
Dim lcl_rc As Integer
' Check log_type
Select Case log_type
eAPI_form - 7
Case "I"
Case "O"
Case "S"
Case "E"
Case Else
lcl_rc = MsgBox("Invalid log type " & log_type)
Exit Sub
End Select
' Check log_sts
Select Case log_sts
Case "TCP"
Case "COM"
Case "INF"
Case "ERR"
Case Else
lcl_rc = MsgBox("Invalid log status " & log_sts)
Exit Sub
End Select
' Add log data to listbox
lst_log.AddItem log_type & ":" & log_sts & ":" & log_dta
Do While lst_log.ListCount > 99
lst_log.RemoveItem 0
Loop
lst_log.ListIndex = lst_log.ListCount - 1
'------------------------------------------------------------------------
---------
```

```
' Add log data to logfile
'
------------------------------------------------------------------------
--------
' do not log is g_log_days=0
If g_ekernel_remote_port = "" Then Exit Sub
' build directory and file
Dim lcl_path As String
Dim lcl_file As String
' start error recovery
On Error Resume Next: Err = 0
' if specified drive is valid, try to toggle between C: drive and D: drive
Err = 0
Dim lcl_chk As Integer
lcl_chk = Len(Dir$(g_log_path, vbDirectory))
lcl_path = g_log_path
If Len(Dir$(lcl_path, vbDirectory)) = 0 Then
MkDir lcl_path
End If
lcl_chk = Len(Dir$(g_log_path, vbDirectory))
If ((Err = 52) Or (lcl_chk = 0)) Then
Select Case Left$(g_log_path, 3)
Case "C:\"
g_log_path = "D:\" + Mid$(g_log_path, 4)
lab_log_path = " " & g_log_path
Case "D:\"
g_log_path = "C:\" + Mid$(g_log_path, 4)
lab_log_path = " " & g_log_path
Case Else
g_log_path = "C:\" + Mid$(g_log_path, 4)
lab_log_path = " " & g_log_path
End Select
End If
Err = 0
' make "D:\SOPHO Messenger@Net"
lcl_path = g_log_path
If Len(Dir$(lcl_path, vbDirectory)) = 0 Then
MkDir lcl_path
End If
' make "D:\SOPHO Messenger@Net\log"
lcl_path = lcl_path + "\log"
If Len(Dir$(lcl_path, vbDirectory)) = 0 Then
MkDir lcl_path
```

```
End If
' make "D:\SOPHO messenger@Net\log\02001_eAPI"
lcl_path = lcl_path + "\" + Format$(g_ekernel_remote_port, "00000") +
"_eAPI"
If Len(Dir$(lcl_path, vbDirectory)) = 0 Then
MkDir lcl_path
End If
' Kill log-files older then x days if g_LastLogFile not today
If Mid$(g_LastLogFile, 1, 8) <> Format$(Now, "yyyymmdd") Then
eAPI_form - 8
KILL_OLD_LOGFILES lcl_path
End If
' make "20001030.txt"
lcl_file = Format$(Now, "yyyymmdd") & ".txt"
g_LastLogFile = lcl_file
' open file "D:\SOPHO messenger@Net\log\02001_eAPI\20001030txt"
Open lcl_path & "\" & lcl_file For Append As 1
' write log record
Print #1, Format$(Now, "dd/mm/yyyy hh:mm:ss") & " - " & log_type & ":" &
log_sts & ":" &
log_dta
' close log file
Close 1
' disable error recovery
On Error GoTo 0
End Sub
```

Module – eASYNC

The module eASYNC consists of one program eASYNC.exe, written in Visual Basic.

Overview

eASYNC.exe

The eASYNC.exe is the Visual Basic component of the eASYNC module. The program communicates with two processes: the eKERNEL.exe and the asynchronous modem attached to a COM port. The eKERNEL.exe is the central engine that centralises all database access and communication with input and output capable modules.

The eASYNC.exe communicates with eKERNEL.exe by means of TCP sockets. In this communication, eASYNC.exe is a TCP client software that connects to the other component, acting as TCP server software.

At start-up, eASYNC.exe contacts the eKERNEL.exe by means of a socket connection. Start-up parameters are required to identify eASYNC.exe, and locate the eKERNEL.exe program. These parameters are set in the Properties section of the shortcut that initiates eASYNC.exe. This shortcut is usually located in the Windows Startup group (click **Start**, and choose **Programs** > **Startup**).

Figure 411
Typical parameters in the shortcut

```
"C:\SOPHO Messenger@Net\Exe\eASYNC.exe"
/Site:1
/eKernel port:3105
/eKernel address:*LOCAL
/Log drive:C
```

In the example in Figure 411, the eASYNC.exe identifies itself as belonging to Site 1, and specifies the location of eKERNEL through IP address *LOCAL and port 3105. The special value *LOCAL refers to the assigned IP address of the first NIC adapter found in the PC, as can be found in the IPCONFIG.exe command or in the appropriate sections of the Windows network settings. The keyword Log drive refers to the drive in which the logging data must be stored; usually this is the C:-drive, referring to C:\SOPHO Messenger@Net\Log\ structure.

At start-up, the eASYNC.exe sends an XML string to eKERNEL.exe requesting a configuration. This step is needed for each module that interacts with eKERNEL.exe, because this approach allows central administration using a single database, even if some client modules are located on a distributed machine.

Figure 412
A typical <cfgrqs> configuration request and reply

```
<xml>
<cfgrqs>
<appl>eASYNC</appl>
<site>1</site>
</cfgrqs>
</xml>
```

```
<xml>
<cfgrpy><interface_cnt>2</interface_cnt>
<com_port_01>COM02</com_port_01>
<settings_01>9600,N,8,1</settings_01>
<type_01>PAGING</type_01>
<provider_01>BELGACOM</provider_01>
<password>*NONE</password>
<number_01>00452500001</number_01>
<init_01>AT&C0S0=3</init_01>
<rty_intv_01>60</rty_intv_01>
<rty_cnt_01>1</rty_cnt_01>
<snd_depth_01>1</snd_depth_01>
<snd_time_01>600</snd_time_01>
<com_port_02>COM02</com_port_02>
<settings_02>9600,N,8,1</settings_02>
<type_02>SMS</type_02>
<provider_02>PROXIMUS</provider_02>
<password>proximus</password>
<number_02>00475161622</number_02>
<init_02>AT&C0S0=3</init_02>
<rty_intv_02>60</rty_intv_02>
<rty_cnt_02>2</rty_cnt_02>
<snd_depth_02>1</snd_depth_02>
<snd_time_02>600</snd_time_02>
<log_path>C:\SOPHO Messenger@net</log_path>
<log_days>1</log_days>
</cfgrpy>
</xml>
```

Refer to the appropriate sections on the database tables that define the received parameters for more information on each value. The information in this document is provided for informational purposes; detailed description of these internal inter-process communications is beyond the scope of this document.

If the <cfgrpy> shown in Figure 412 on page 1073 is received, a licence for eASYNC is valid.

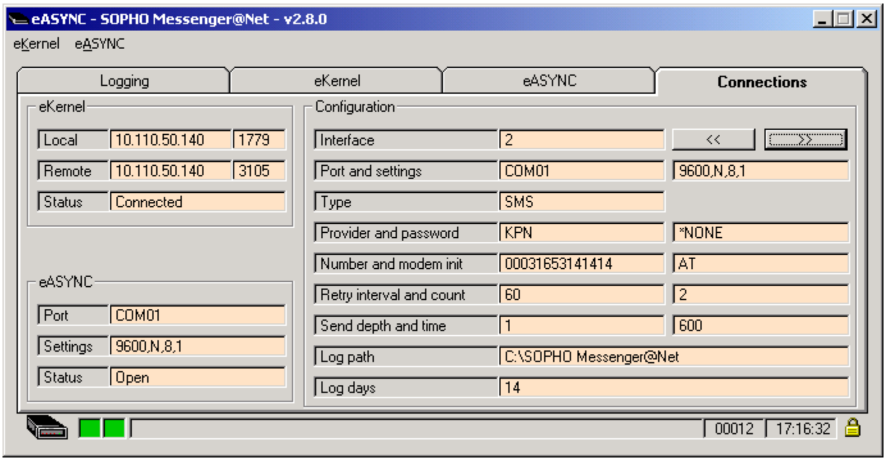
If the <cfgrpy> shown in Figure 413 is received, no licence is available, and the eASYNC module cannot connect to the eKernel module anymore.

Figure 413
eASYNC module receives this cfgrpy from the eKernel if no licence is available for eASYNC

```
<xml>
<cfgrpy>
<licence>No licence available></licence>
</cfgrpy>
</xml>
```

The eASYNC Connections tab is shown in Figure 414.

Figure 414
eASYNC Connections tab



eKernel

Local	10.110.50.140	1779
Remote	10.110.50.140	3105
Status	Connected	

eASYNC

Port	COM01
Settings	9600,N,8,1
Status	Open

Configuration

Interface	2	
Port and settings	COM01	9600,N,8,1
Type	SMS	
Provider and password	KPN	*NONE
Number and modem init	00031653141414	AT
Retry interval and count	60	2
Send depth and time	1	600
Log path	C:\SOPHO Messenger@Net	
Log days	14	

00012 17:16:32

The eASYNC module receives message requests from eKERNEL. After processing, feedback is sent from eASYNC to eKERNEL. Figure 415 on page 1075 shows an example of a message request and the feedback generated by eASYNC.

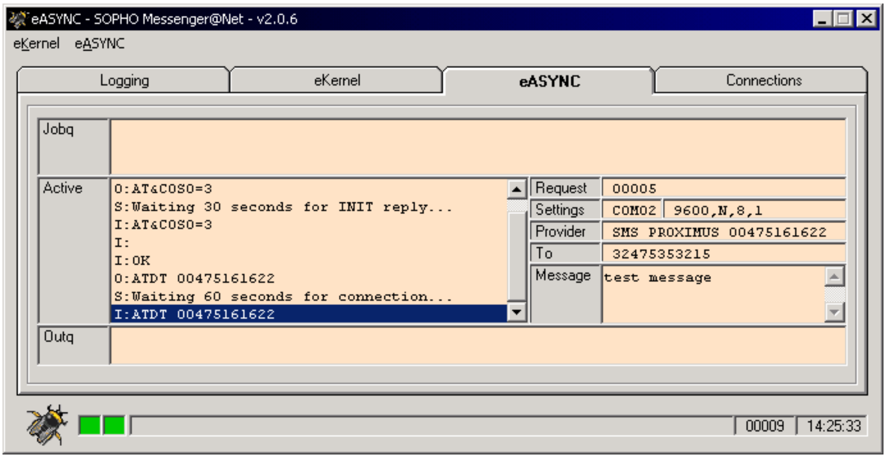
Figure 415
Sample eKERNEL message request and eASYNC feedback

```
<xml>
<msgrqs><id>00005</id>
<type>SMS</type>
<provider>PROXIMUS</provider>
<password>proximus</password>
<to>32475353215</to>
<pag_01>test message</pag_01>
<pag_more>N</pag_more>
</msgrqs>
</xml>
```

```
<xml>
<msgrpy>
<id>00005</id>
<sts>NACK - No carrier while waiting for connection^</sts>
</msgrpy>
</xml>
```

During communications, eASYNC contacts the provider and handle the dialog that is required to deliver the message. The transactions are processed on a first-in first-out basis. However, there can be configuration settings active that request a wait time or a queue depth that must be reached prior to initiating the communication process. This is especially relevant for SMS messaging to PROXIMUS or KPN, because these providers support the ability to deliver more than one SMS message during one single dial-up connection.

Figure 416
eASYNC tab



```
O:AT&COSO=3
S:Waiting 30 seconds for INIT reply...
I:AT&COSO=3
I:
I:OK
O:ATDT 00475161622
S:Waiting 60 seconds for connection...
I:ATDT 00475161622
```

Request: 00005
Settings: COM02 9600,N,8,1
Provider: SMS PROXIMUS 00475161622
To: 32475353215
Message: test message

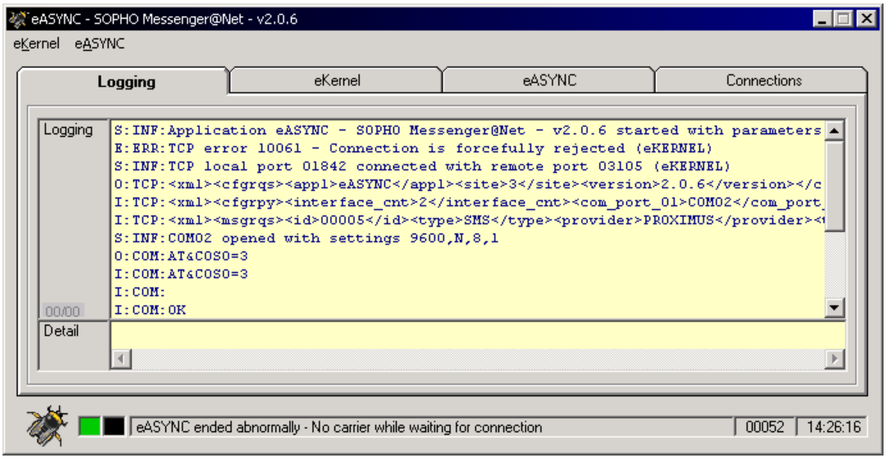
00009 14:25:33

Logging

Logging information is available both on-screen and in logging files.

The on-screen logging can be visualized through the Logging tab.

Figure 417
eASYNC Logging tab



```
S:INF:Application eASYNC - SOPHO Messenger@Net - v2.0.6 started with parameters
E:ERR:TCP error 10061 - Connection is forcefully rejected (eKERNEL)
S:INF:TCP local port 01842 connected with remote port 03105 (eKERNEL)
O:TCP:<xml><cfgrqs><appl>eASYNC</appl><site>3</site><version>2.0.6</version></c
I:TCP:<xml><cfgrpy><interface_cnt>2</interface_cnt><com_port_01>COM02</com_port_
I:TCP:<xml><msgrqs><id>00005</id><type>SMS</type><provider>PROXIMUS</provider><t
S:INF:COM02 opened with settings 9600,N,8,1
O:COM:AT&COSO=3
I:COM:AT&COSO=3
I:COM:
I:COM:OK
```

eASYNC ended abnormally - No carrier while waiting for connection 00052 14:26:16

Figure 418
Sample logging data for SMS to PROXIMUS

```
19/03/2001 10:57:25 - S:INF:COM02 opened with settings 9600,N,8,1
19/03/2001 10:57:26 - O:COM:AT&C0S0=3
19/03/2001 10:57:26 - O:COM:ATDT 00475161622
19/03/2001 10:57:27 - I:COM:AT&C0S0=3
19/03/2001 10:57:27 - I:COM:
19/03/2001 10:57:27 - I:COM:OK
19/03/2001 10:57:27 - I:COM:ATDT 00475161622
19/03/2001 10:57:49 - I:COM:
19/03/2001 10:57:49 - I:COM:CONNECT 33600 V42bis
19/03/2001 10:57:50 - O:COM:_01/00121/O/01/32475353215//proximus/3/
534D5320746F2050726F78696D7573207769746820534F50484F204D657373656E67657
2404E6574/A3_
19/03/2001 10:57:54 - I:COM:connected
19/03/2001 10:57:54 - I:COM:_01/00019/R/01/A//69_
19/03/2001 10:57:55 - S:INF:Port closed
19/03/2001 10:57:55 - O:TCP:<xml><msgrpy><id>00002</id><sts>ACK^</
sts></msgrpy></xml>
```

Figure 419
Sample logging data for SMS to KPN

```
S:INF:COM03 opened with settings 9600,N,8,1
02-05-2002 13:57:37 - O:COM:AT
02-05-2002 13:57:38 - I:COM:AT
02-05-2002 13:57:38 - I:COM:
02-05-2002 13:57:38 - I:COM:OK
02-05-2002 13:57:39 - O:COM:ATDT 00653141414
02-05-2002 13:57:43 - I:COM:ATDT 00653141414
02-05-2002 13:58:16 - I:COM:
02-05-2002 13:58:16 - I:COM:CONNECT 33600 V42bis
02-05-2002 13:58:17 - O:COM:_01/00084/O/01/0620032328///3/
456D657267656E637920534F5320312045766163756174696F6E/E2_
02-05-2002 13:58:33 - S:INF:Port closed
02-05-2002 13:58:33 - O:TCP:<xml><msgrpy><id>00142</id><sts>ACK^</
sts></msgrpy></xml>
```

Figure 420
Sample logging data for PAGING to BELGACOM

```
19/03/2001 15:56:08 - S:INF:COM02 opened with settings 9600,N,8,1
19/03/2001 15:56:09 - O:COM:AT&C0S0=3
19/03/2001 15:56:10 - I:COM:AT&C0S0=3
19/03/2001 15:56:10 - I:COM:
19/03/2001 15:56:10 - I:COM:OK
19/03/2001 15:56:09 - O:COM:ATDT 00452500001
19/03/2001 15:56:10 - I:COM:OK
19/03/2001 15:56:10 - I:COM:ATDT 00452500001
19/03/2001 15:56:34 - I:COM:
19/03/2001 15:56:34 - I:COM:CONNECT 14400 V42bis
19/03/2001 15:56:40 - I:COM:_
19/03/2001 15:56:40 - I:COM:WELCOME TO THE BELGACOM PAGING SERVICE.
19/03/2001 15:56:40 - I:COM:-------------------------------------
19/03/2001 15:56:40 - I:COM:You can call numbers in the range:
19/03/2001 15:56:40 - I:COM:2xxxxxx, 3xxxxxx, 8xxxxxx, 9xxxxxx
19/03/2001 15:56:40 - I:COM:Correction with backspace, delete or @
19/03/2001 15:56:40 - I:COM:Terminate each input with "RETURN-KEY"
19/03/2001 15:56:40 - I:COM:Disconnect with "ctrl-D"
19/03/2001 15:56:40 - I:COM:_
19/03/2001 15:56:40 - I:COM:****IMPORTANT INFORMATION****      +98+
19/03/2001 15:56:40 - I:COM:NEW  "Email Notification for paging"
19/03/2001 15:56:40 - I:COM:Interested: Send a mail to : Email.paging@belgacom.be
19/03/2001 15:56:41 - I:COM:or Contact 02/5406161(NL) - 02/5406302(FR)
19/03/2001 15:56:42 - I:COM:www.belgacom.be/cgi-bin/echannel/web/index.jsp?LANGUAGE=EN&DIVISION=RES
19/03/2001 15:56:42 - I:COM:Select:
19/03/2001 15:56:42 - I:COM:Catalog/Mobiles Solutions/Pagers   +99+
19/03/2001 15:56:42 - I:COM:_
19/03/2001 15:56:42 - I:COM:Type the 7 digits of the
19/03/2001 15:56:42 - I:COM:wanted pager-number:               +01+
19/03/2001 15:56:43 - O:COM:9789074
19/03/2001 15:56:44 - I:COM:.......
19/03/2001 15:56:44 - I:COM:9789074
19/03/2001 15:56:44 - I:COM:
19/03/2001 15:56:44 - I:COM:Type your alpha-numeric message.   +30+
19/03/2001 15:56:45 - O:COM:Test paging to Belgacom with SOPHO Messenger@Net
```

continued on next page...

Sample logging data for PAGING to BELGACOM (continued)

```
19/03/2001 15:56:46 -
I:COM:_[?7h.............................................................
.........................................................................
.............................
19/03/2001 15:56:46 - I:COM:_[A_[ATest paging to Belgacom with SOPHO Mes-
senger@Net
19/03/2001 15:56:47 - I:COM:
19/03/2001 15:56:47 - I:COM:CALL ACCEPTED.                     +80+
19/03/2001 15:56:48 - S:INF:Port closed
19/03/2001 15:56:48 - O:TCP:<xml><msgrpy><id>00001</id><sts>ACK^</
sts></msgrpy></xml>
```

Module – eBACKUP

The eBACKUP module allows you to make a backup of a predefined list of files.

Refer to “Table: eBACKUP” on page 1309 for more information on configuration issues.

The eBACKUP.exe must be started from a shortcut, which provides a number of command line parameters. Figure 421 shows an example of a shortcut with the required command line parameters:

Figure 421
eBACKUP shortcut with required line parameters

```
"C:\SOPHO Messenger@Net\Exe\eBACKUP.exe"
/Path:C:\SOPHO Messenger@Net
/Log drive:C
/Site:1
/Batch:N
```

The following keywords are available:

- Path specifies the default path where the MDB subdirectory resides in.
- Log drive specifies the letter of the drive in which logging information resides.
- Site specifies the site identifier to be saved.
- Batch specifies whether the application runs in interactively or in batch. In batch mode you need not click the Backup site **Close** button to close the program after execution. Batch is typically used in environments in which automated backup is scheduled at set intervals.

You can use the eBACKUP application to back up the files that are configured in the BACKUP table of the configuration database.

Table 54 shows sample data. Refer to "Table: eBACKUP" on page 1309 for more information.

Table 54
eBACKUP sample data (Part 1 of 2)

Site	From path	From file	To path	To file
3	C:\Php	php.ini	C:\Temp\[weekday]\php	php.ini
3	C:\Program Files\Apache group\Apache\conf	httpd.conf	C:\Temp\[weekday]\Program Files\Apache Group\Apache\conf	httpd.conf
3	C:\SOPHO Messenger@Net\Exe	csta.dll	C:\Temp\[weekday]\SOPHO Messenger@Net\Exe	csta.dll
3	C:\SOPHO Messenger@Net\Exe	CSTA_Service.exe	C:\Temp\[weekday]\SOPHO Messenger@Net\Exe	CSTA_Service.exe
3	C:\SOPHO Messenger@Net\Exe	eAPI.exe	C:\Temp\[weekday]\SOPHO Messenger@Net\Exe	eAPI.exe
3	C:\SOPHO Messenger@Net\Exe	eASYNC.exe	C:\Temp\[weekday]\SOPHO Messenger@Net\Exe	eASYNC.exe
3	C:\SOPHO Messenger@Net\Exe	eBACKUP.exe	C:\Temp\[weekday]\SOPHO Messenger@Net\Exe	eBACKUP.exe
3	C:\SOPHO Messenger@Net\Exe	eCAP.exe	C:\Temp\[weekday]\SOPHO Messenger@Net\Exe	eCAP.exe
3	C:\SOPHO Messenger@Net\Exe	eDMSAPI.exe	C:\Temp\[weekday]\SOPHO Messenger@Net\Exe	eDMSAPI.exe
3	C:\SOPHO Messenger@Net\Exe	eGRID.exe	C:\Temp\[weekday]\SOPHO Messenger@Net\Exe	eGRID.exe

Table 54
eBACKUP sample data (Part 2 of 2)

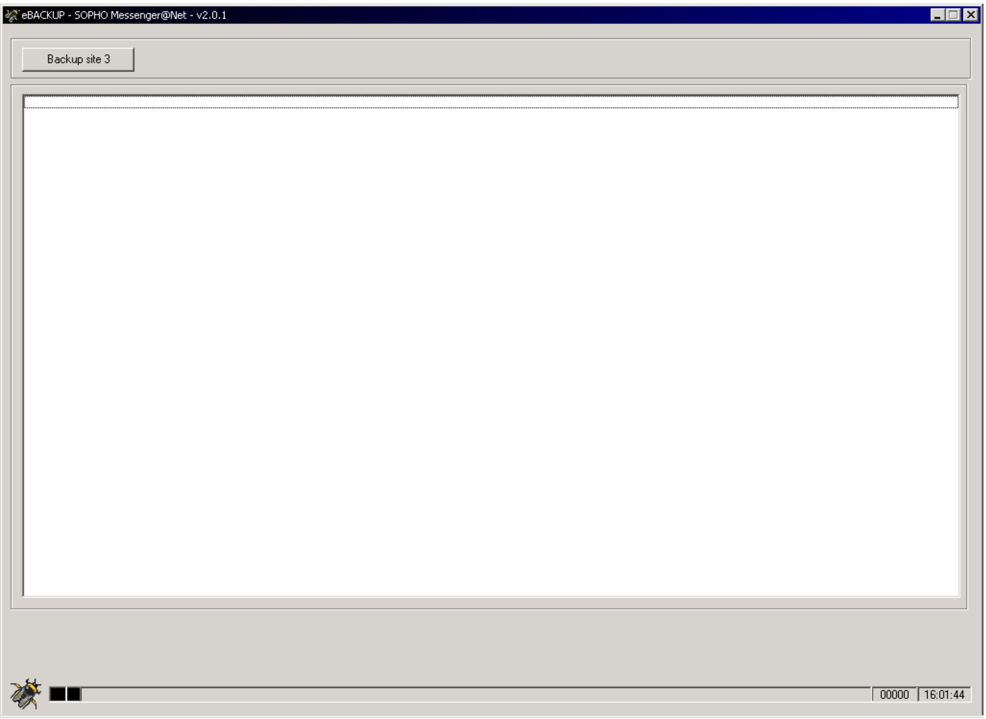
3	C:\SOPHO Messenger@Net\Exe	eIO.exe	C:\Temp\[weekday]\SOPHO Messenger@Net\Exe	eIO.exe
3	C:\SOPHO Messenger@Net\Exe	eKERNEL.exe	C:\Temp\[weekday]\SOPHO Messenger@Net\Exe	eKERNEL.exe
3	C:\SOPHO Messenger@Net\Exe	eSMTP.exe	C:\Temp\[weekday]\SOPHO Messenger@Net\Exe	eSMTP.exe
3	C:\SOPHO Messenger@Net\Exe	eSMTP_server.exe	C:\Temp\[weekday]\SOPHO Messenger@Net\Exe	eSMTP_server.exe
3	C:\SOPHO Messenger@Net\Exe	omnithread_rt.dll	C:\Temp\[weekday]\SOPHO Messenger@Net\Exe	omnithread_rt.dll
3	C:\SOPHO Messenger@Net\Mdb	Messenger_CFG.mdb	C:\Temp\[weekday]\SOPHO Messenger@Net\Mdb	Messenger_CFG.mdb
3	C:\SOPHO Messenger@Net\Mdb	Messenger_Data.mdb	C:\Temp\[weekday]\SOPHO Messenger@Net\Mdb	Messenger_Data.mdb

Refer to “Table: eBACKUP” on page 1309 for more information on the use of [weekday], [weekdayname], and [timestamp] special replacement values.

From_path and From_file specify the path and the name of the file that are copied to the To_path and To_file.

When eBACKUP is started, a blank window with one button is shown, for example, Backup site 3.

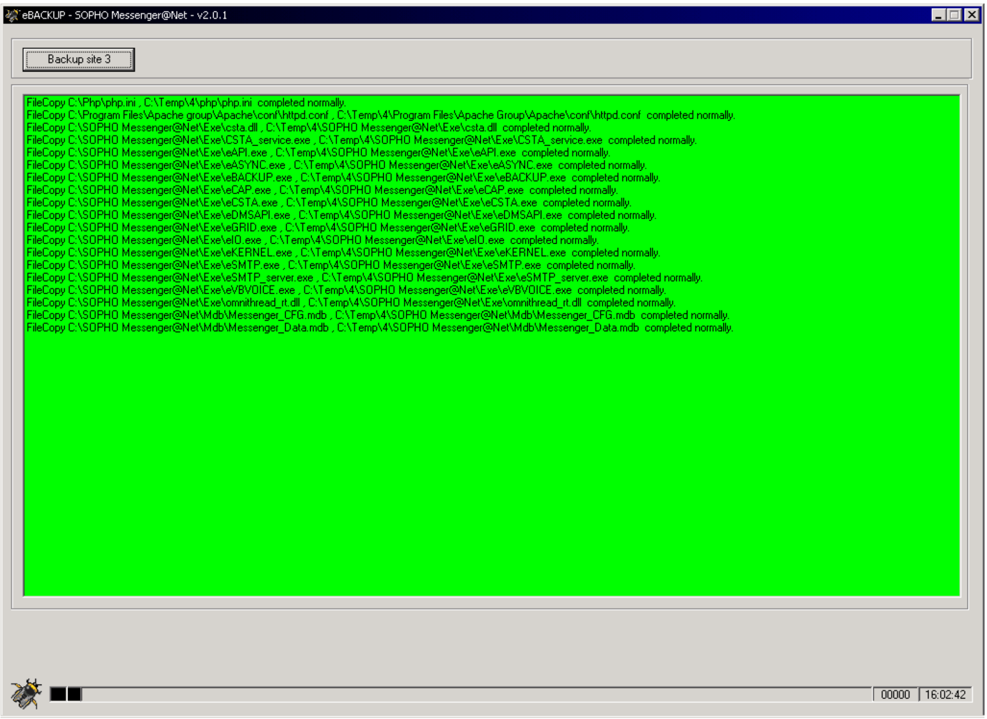
Figure 422
Backup start window



Click on the Backup button to begin the backup procedure.

When all the files are successfully copied, the window becomes green.

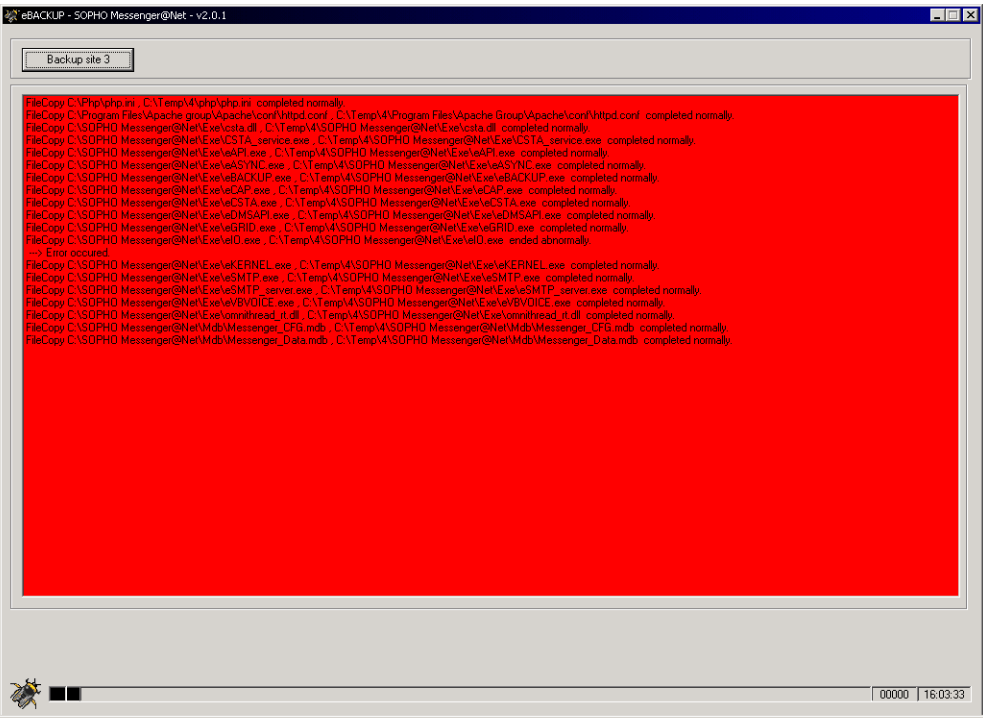
Figure 423
Backup successful



```
FileCopy C:\Php\php.ini , C:\Temp\4\php\php.ini  completed normally.
FileCopy C:\Program Files\Apache group\Apache\conf\httpd.conf , C:\Temp\4\Program Files\Apache Group\Apache\conf\httpd.conf  completed normally.
FileCopy C:\SOPHO Messenger@Net\Exe\csta.dll , C:\Temp\4\SOPHO Messenger@Net\Exe\csta.dll  completed normally.
FileCopy C:\SOPHO Messenger@Net\Exe\CSTA_service.exe , C:\Temp\4\SOPHO Messenger@Net\Exe\CSTA_service.exe  completed normally.
FileCopy C:\SOPHO Messenger@Net\Exe\eAPI.exe , C:\Temp\4\SOPHO Messenger@Net\Exe\eAPI.exe  completed normally.
FileCopy C:\SOPHO Messenger@Net\Exe\eASYNC.exe , C:\Temp\4\SOPHO Messenger@Net\Exe\eASYNC.exe  completed normally.
FileCopy C:\SOPHO Messenger@Net\Exe\eBACKUP.exe , C:\Temp\4\SOPHO Messenger@Net\Exe\eBACKUP.exe  completed normally.
FileCopy C:\SOPHO Messenger@Net\Exe\eCAP.exe , C:\Temp\4\SOPHO Messenger@Net\Exe\eCAP.exe  completed normally.
FileCopy C:\SOPHO Messenger@Net\Exe\eCSTA.exe , C:\Temp\4\SOPHO Messenger@Net\Exe\eCSTA.exe  completed normally.
FileCopy C:\SOPHO Messenger@Net\Exe\eDMSAPI.exe , C:\Temp\4\SOPHO Messenger@Net\Exe\eDMSAPI.exe  completed normally.
FileCopy C:\SOPHO Messenger@Net\Exe\eGRID.exe , C:\Temp\4\SOPHO Messenger@Net\Exe\eGRID.exe  completed normally.
FileCopy C:\SOPHO Messenger@Net\Exe\eIO.exe , C:\Temp\4\SOPHO Messenger@Net\Exe\eIO.exe  completed normally.
FileCopy C:\SOPHO Messenger@Net\Exe\eKERNEL.exe , C:\Temp\4\SOPHO Messenger@Net\Exe\eKERNEL.exe  completed normally.
FileCopy C:\SOPHO Messenger@Net\Exe\eSMTP.exe , C:\Temp\4\SOPHO Messenger@Net\Exe\eSMTP.exe  completed normally.
FileCopy C:\SOPHO Messenger@Net\Exe\eSMTP_server.exe , C:\Temp\4\SOPHO Messenger@Net\Exe\eSMTP_server.exe  completed normally.
FileCopy C:\SOPHO Messenger@Net\Exe\eVBVOICE.exe , C:\Temp\4\SOPHO Messenger@Net\Exe\eVBVOICE.exe  completed normally.
FileCopy C:\SOPHO Messenger@Net\Exe\omnithread_rt.dll , C:\Temp\4\SOPHO Messenger@Net\Exe\omnithread_rt.dll  completed normally.
FileCopy C:\SOPHO Messenger@Net\Mdb\Messenger_CFG.mdb , C:\Temp\4\SOPHO Messenger@Net\Mdb\Messenger_CFG.mdb  completed normally.
FileCopy C:\SOPHO Messenger@Net\Mdb\Messenger_Data.mdb , C:\Temp\4\SOPHO Messenger@Net\Mdb\Messenger_Data.mdb  completed normally.
```

If one or more files are not copied, the window becomes red.

Figure 424
Backup error window



```
FileCopy C:\Php\php.ini , C:\Temp\4\php\php.ini  completed normally.
FileCopy C:\Program Files\Apache group\Apache\conf\httpd.conf , C:\Temp\4\Program Files\Apache Group\Apache\conf\httpd.conf  completed normally.
FileCopy C:\SOPHO Messenger@Net\Exe\csta.dll , C:\Temp\4\SOPHO Messenger@Net\Exe\csta.dll  completed normally.
FileCopy C:\SOPHO Messenger@Net\Exe\CSTA_service.exe , C:\Temp\4\SOPHO Messenger@Net\Exe\CSTA_service.exe  completed normally.
FileCopy C:\SOPHO Messenger@Net\Exe\eAPI.exe , C:\Temp\4\SOPHO Messenger@Net\Exe\eAPI.exe  completed normally.
FileCopy C:\SOPHO Messenger@Net\Exe\eASYNC.exe , C:\Temp\4\SOPHO Messenger@Net\Exe\eASYNC.exe  completed normally.
FileCopy C:\SOPHO Messenger@Net\Exe\eBACKUP.exe , C:\Temp\4\SOPHO Messenger@Net\Exe\eBACKUP.exe  completed normally.
FileCopy C:\SOPHO Messenger@Net\Exe\eCAP.exe , C:\Temp\4\SOPHO Messenger@Net\Exe\eCAP.exe  completed normally.
FileCopy C:\SOPHO Messenger@Net\Exe\eCSTA.exe , C:\Temp\4\SOPHO Messenger@Net\Exe\eCSTA.exe  completed normally.
FileCopy C:\SOPHO Messenger@Net\Exe\eDMSAPI.exe , C:\Temp\4\SOPHO Messenger@Net\Exe\eDMSAPI.exe  completed normally.
FileCopy C:\SOPHO Messenger@Net\Exe\eGRID.exe , C:\Temp\4\SOPHO Messenger@Net\Exe\eGRID.exe  completed normally.
FileCopy C:\SOPHO Messenger@Net\Exe\eIO.exe , C:\Temp\4\SOPHO Messenger@Net\Exe\eIO.exe  ended abnormally.
 ---> Error occured.
FileCopy C:\SOPHO Messenger@Net\Exe\eKERNEL.exe , C:\Temp\4\SOPHO Messenger@Net\Exe\eKERNEL.exe  completed normally.
FileCopy C:\SOPHO Messenger@Net\Exe\eSMTP.exe , C:\Temp\4\SOPHO Messenger@Net\Exe\eSMTP.exe  completed normally.
FileCopy C:\SOPHO Messenger@Net\Exe\eSMTP_server.exe , C:\Temp\4\SOPHO Messenger@Net\Exe\eSMTP_server.exe  completed normally.
FileCopy C:\SOPHO Messenger@Net\Exe\eVBVOICE.exe , C:\Temp\4\SOPHO Messenger@Net\Exe\eVBVOICE.exe  completed normally.
FileCopy C:\SOPHO Messenger@Net\Exe\omnithread_rt.dll , C:\Temp\4\SOPHO Messenger@Net\Exe\omnithread_rt.dll  completed normally.
FileCopy C:\SOPHO Messenger@Net\Mdb\Messenger_CFG.mdb , C:\Temp\4\SOPHO Messenger@Net\Mdb\Messenger_CFG.mdb  completed normally.
FileCopy C:\SOPHO Messenger@Net\Mdb\Messenger_Data.mdb , C:\Temp\4\SOPHO Messenger@Net\Mdb\Messenger_Data.mdb  completed normally.
```

During backup, logging information is written to the hard disk, an example of which is shown in Figure 425 on page 1087. Note that in the example, the file eIO.exe was not saved.

Figure 425
Sample backup log

```
25/10/2001 16:06:20 - S:INF:Application eBACKUP - SOPHO Messenger@Net -
v2.0.1 started with parameters /Path:C:\SOPHO Messenger@Net /Log drive:C
/Site:3 /Batch:N
25/10/2001 16:06:22 - S:INF:FileCopy C:\Php\php.ini ,
C:\Temp\4\php\php.ini  completed normally.
25/10/2001 16:06:22 - S:INF:FileCopy C:\Program Files\Apache
group\Apache\conf\httpd.conf , C:\Temp\4\Program Files\Apache
Group\Apache\conf\httpd.conf  completed normally.
25/10/2001 16:06:22 - S:INF:FileCopy C:\SOPHO Messenger@Net\Exe\csta.dll
, C:\Temp\4\SOPHO Messenger@Net\Exe\csta.dll  completed normally.
25/10/2001 16:06:22 - S:INF:FileCopy C:\SOPHO Messen-
ger@Net\Exe\CSTA_service.exe , C:\Temp\4\SOPHO Messen-
ger@Net\Exe\CSTA_service.exe  completed normally.
25/10/2001 16:06:22 - S:INF:FileCopy C:\SOPHO Messenger@Net\Exe\eAPI.exe
, C:\Temp\4\SOPHO Messenger@Net\Exe\eAPI.exe  completed normally.
25/10/2001 16:06:22 - S:INF:FileCopy C:\SOPHO Messen-
ger@Net\Exe\eASYNC.exe , C:\Temp\4\SOPHO Messenger@Net\Exe\eASYNC.exe
completed normally.
25/10/2001 16:06:22 - S:INF:FileCopy C:\SOPHO Messenger@Net\Exe\eBACK-
UP.exe , C:\Temp\4\SOPHO Messenger@Net\Exe\eBACKUP.exe  completed nor-
mally.
25/10/2001 16:06:22 - S:INF:FileCopy C:\SOPHO Messenger@Net\Exe\eCAP.exe
, C:\Temp\4\SOPHO Messenger@Net\Exe\eCAP.exe  completed normally.

25/10/2001 16:06:22 - S:INF:FileCopy C:\SOPHO Messenger@Net\Exe\eDMSA-
PI.exe , C:\Temp\4\SOPHO Messenger@Net\Exe\eDMSAPI.exe  completed nor-
mally.
25/10/2001 16:06:23 - S:INF:FileCopy C:\SOPHO Messen-
ger@Net\Exe\eGRID.exe , C:\Temp\4\SOPHO Messenger@Net\Exe\eGRID.exe
completed normally.
25/10/2001 16:06:23 - S:INF:FileCopy C:\SOPHO Messenger@Net\Exe\eIO.exe
, C:\Temp\4\SOPHO Messenger@Net\Exe\eIO.exe  ended abnormally.
25/10/2001 16:06:23 - S:INF: ---> Error occured.
25/10/2001 16:06:23 - S:INF:FileCopy C:\SOPHO Messenger@Net\Exe\eKER-
NEL.exe , C:\Temp\4\SOPHO Messenger@Net\Exe\eKERNEL.exe  completed nor-
mally.
```

continued on next page...

Sample backup log (continued)

```
25/10/2001 16:06:23 - S:INF:FileCopy C:\SOPHO Messenger@Net\Exe\eS-
MTP.exe , C:\Temp\4\SOPHO Messenger@Net\Exe\eSMTP.exe  completed normal-
ly.
25/10/2001 16:06:23 - S:INF:FileCopy C:\SOPHO Messen-
ger@Net\Exe\eSMTP_server.exe , C:\Temp\4\SOPHO Messen-
ger@Net\Exe\eSMTP_server.exe  completed normally.
25/10/2001 16:06:23 - S:INF:FileCopy C:\SOPHO Messen-
ger@Net\Exe\omnithread_rt.dll , C:\Temp\4\SOPHO Messen-
ger@Net\Exe\omnithread_rt.dll  completed normally.
25/10/2001 16:06:23 - S:INF:FileCopy C:\SOPHO Messen-
ger@Net\Mdb\Messenger_CFG.mdb , C:\Temp\4\SOPHO Messen-
ger@Net\Mdb\Messenger_CFG.mdb  completed normally.
25/10/2001 16:06:25 - S:INF:FileCopy C:\SOPHO Messen-
ger@Net\Mdb\Messenger_Data.mdb , C:\Temp\4\SOPHO Messen-
ger@Net\Mdb\Messenger_Data.mdb  completed normally.
25/10/2001 16:06:30 - S:INF:Application ended
```

Nortel recommends that you close all the DECT Messenger applications before starting the backup procedure. In release 2, the file copy procedure is implemented by means of a Windows API-call, as shown with the code excerpt in Figure 426:

Figure 426
File copy example

```
:
Declare Function apiCopyFile Lib "kernel32" Alias "CopyFileA" (ByVal
lpExistingFileName As String, ByVal lpNewFileName As String, ByVal bFail-
IfExists As Long) As Long
:
Result = apiCopyFile(SourceFile, DestFile, False)
:
```

IMPORTANT!

To ensure a complete and consistent image, you must close all applications before backup.

The code shown in Figure 426 on page 1088 can back up files, even if they are open, so the eBACKUP can be initiated while, for instance, eKERNEL is active and the Messenger_CFG.mdb database is open. Although the eBACKUP allows you to save the open files, Nortel does not guarantee that the copied file is a complete image or a consistent database image. During activity of eKERNEL, parts of the Access 2000 database are sometimes in use and transactions are pending. Saving open files is not officially supported.

For more information, visit the Microsoft web site at:
http://support.microsoft.com/support/kb/articles/Q207/7/03.asp

Module – eCAP

The module eCAP consists of the program eCAP.exe, written in Visual Basic. In general, DECT Messenger programs reside in the default directory C:\SOPHO Messenger@Net\Exe, unless otherwise implemented in your environment.

Overview

eCAP.exe

The eCAP.exe is a Visual Basic component of the eCAP module. The program communicates with two processes: the eKERNEL.exe and an external alarm interface. The eKERNEL.exe is the central engine that centralises all database access and communication with input and output capable modules.

The eCAP.exe communicates with eKERNEL.exe by means of TCP sockets. In this communication, eCAP.exe is a TCP client software that connects to the eKERNEL component, acting as TCP server software.

At start-up, eCAP.exe contacts the eKERNEL.exe by means of a socket connection. Start-up parameters identify eCAP.exe, and locate the eKERNEL.exe program. These parameters are set in the Properties section of the shortcut that initiates eCAP.exe. This shortcut is usually located in the Windows Startup group (click **Start** on the Windows toolbar, and choose **Programs > Startup**).

Figure 427
Typical parameters in the shortcut

```
"C:\SOPHO Messenger@Net\Exe\eCAP.exe"
/Site:1
/eKernel address:*LOCAL
/eKernel port:3102
/Log drive:C
```

In the example shown in Figure 427 on page 1092, the eCAP.exe identifies itself as belonging to site 1, and specifies the location of eKERNEL through IP address *LOCAL and port 3102. The special value *LOCAL refers to the assigned IP address of the first NIC adapter found in the PC, as can be found in the IPCONFIG.exe command or in the appropriate sections of the Windows network settings. The keyword Log drive refers to the drive where the logging data must be stored. Usually this is C:\SOPHO Messenger@Net\Log\.

At start-up, the eCAP.exe sends an XML string to eKERNEL.exe requesting a configuration. This step is needed for each module that interacts with eKERNEL.exe, because this approach allows central administration using a single database, even if some client modules are located on a distributed machine.

Figure 428
A typical <cfgrqs> configuration request and its received <cfgrpy> configuration reply

```
<xml>
<cfgrqs>
<appl>eCAP</appl>
<site>1</site>
</cfgrqs>
</xml>
```

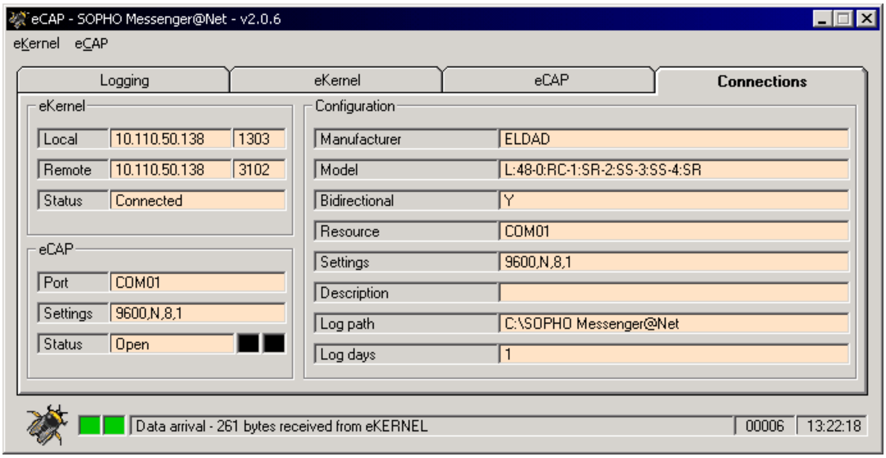
```
<xml>
<cfgrpy>
<manufacturer>ELDAD</manufacturer>
<model>L:48-0:RC-1:SR-2:SS-3:SS-4:SR </model>
<bidir>N</bidir>
<link_type>RS232</link_type>
<resource>COM01</resource>
<settings>9600,N,8,1</settings>
<descr>Eldad DP6000</descr>
<log_path>c:\SOPHO Messenger@net</log_path>
<log_days>30</log_days>
</cfgrpy></xml>
```

> ***Note:*** The generic eCAP configuration sends extra keywords and values, as defined in the eCAP_generic table.

Refer to the chapters of this document that describe the database tables for more information on each value. Detailed descriptions of these internal inter-process communications is beyond the scope of this chapter.

When the configuration is received, the **Connection** tab displays information similar to what is pictured in Figure 429 on page 1094.

Figure 429
eCAP Connection tab



eKernel

Local	10.110.50.138	1303
Remote	10.110.50.138	3102
Status	Connected	

eCAP

Port	COM01
Settings	9600,N,8,1
Status	Open

Configuration

Manufacturer	ELDAD
Model	L:48-0:RC-1:SR-2:SS-3:SS-4:SR
Bidirectional	Y
Resource	COM01
Settings	9600,N,8,1
Description	
Log path	C:\SOPHO Messenger@Net
Log days	1

Data arrival - 261 bytes received from eKERNEL 00006 13:22:18

Because the eCAP is designed to handle asynchronous serial communications with a number of alarm systems, the eCAP requires configuration settings to start processing. These values are returned through the <cfgrpy> reply that is sent on return of the <cfgrqs> request. Some parameters refer to asynchronous communication settings (for example, port number, baud rate, data bits, parity bits, stop bits, and so on); others refer to general information settings (for example, logging parameters); the rest are parameters that actually determine the alarm system (for example, manufacturer, model, bidirectional, and so on).

> ***Note:*** The values shown in Figure 429 on page 1094 are received from the DECT Messenger database: from the eKERNEL_INPGM table, eCAP_generic table, and the eKERNEL_SITE table.

At start-up, the eCAP.exe opens the specified COM port with the specified settings. The COM port specified must be available, be set to use a valid baud rate, and so on. A physical connection must exist between the specified COM port and the external alarm system through a properly wired serial cable. In many cases, alarm systems support a limited number of control signals (for example, ground and send), so check with the alarm system vendor on cable specifications. In most cases, a standard null-modem cable can be used. If no more COM ports are available, extra hardware (such as DigiBoard PC/4e or

DigiBoard PC/8e) is needed to provide extra serial ports. Check compatibility issues (supported by operating system, driver available, and so on) and hardware requirements (memory, available slots, IRQ conflicts, and so on) before ordering or configuring a system.

In many cases the distance between the DECT Messenger and the external-alarm system is relatively small, so no extra hardware is needed. In some conditions hardware is needed, such as, when RS-232-C limitations apply (for example, at 9600 baud maximum limit of 9 metres). In some cases galvanic isolation is requested, or base-band modems, SOPHO LAM, CISCO equipment, and so on are needed to bridge the distance between the DECT Messenger and the alarm system.

One a link is established between eCAP and the alarm system, the eCAP handles further communications and informs eKERNEL when relevant information is to be exchanged.

Functional description

In general, eCAP is designed to provide eKERNEL with alarm information. This is carried out using a <msgrqs> message request. For some interfaces eKERNEL must send feedback to the alarm system, a process that is handled through <msgrpy> message reply request.

IMPORTANT!

The eCAP module is compatible with a number of alarm system installations. However, many of the supported vendors offer a broad variety of hardware and software environments, all of which are not necessarily compatible with eCAP. For example, the fact that one NIRA serial protocol is implemented does not mean that every version of serial input from NIRA is compatible.
Ensure that a specific alarm-system model is supported by DECT Messenger before purchasing or installing it. In most cases manufacturers are not using the same standard for all of their equipment, so obtain information on protocols and specifications. Nortel recommends pre-sales consultation. If necessary, a modification of the current release of eCAP can be made to embed new protocols.

The most typical protocols are listed in Table 55 and described in more detail in the pages following the table. Refer to the protocol specifications of each vendor for more information, as detailed protocol issues are beyond the scope of this document. The information in Table 55 provides a list of supported manufacturers and models. This information is provided on an as-is basis, to illustrate the eCAP module.

Table 55
Supported manufacturer/model protocols

	Manufacturer	Model
eCAP	ARITECH	*BASE
eCAP	BEMAC	DIANA 1
eCAP	BEMAC	DIANA 2
eCAP	ELDAD	L:48-0:RC-1:SR-2:SS-3:SS-4:SR
eCAP	GENERIC	*BASE
eCAP	NIRA	*BASE
eCAP	TELEVIC	PROTOCOL CONVERTOR – L:03
eCAP	VSK	DE LICHTERVELDE
eCAP	VSK	OLV VAN VREDE
eCAP	VSK	ST-JOZEF
eCAP	WORMALD	*BASE
eCAP	WORMALD	L:01

ARITECH

Valid manufacturer is ARITECH, valid model is *BASE.

Aritech is based upon installation Floreal Nieuwpoort.

Figure 430
Sample Aritech protocol data

```
19980218 08:49:41 ----------------------------------------
19980218 08:49:41 Fout     :1      Gebeu. :1258 Aktief
19980218 08:49:41 Poort    :SER1   Printer afgekoppeld
19980218 08:49:41                  18/02/98  08:19:31 P:1
19980218 08:49:41 ----------------------------------------
19980218 08:49:41 Actie    :4      Gebeu. :1259 Gelogd
19980218 08:49:41                  Stop Zoemer
19980218 08:49:41                  18/02/98  08:19:35 P:1
19980218 08:49:42 ----------------------------------------
19980218 08:49:42 Fout     :2      Gebeu. :1260 Gelogd
19980218 08:49:42                  Deur contact
19980218 08:49:43                  18/02/98  08:19:47 P:1
19980218 08:49:43 ----------------------------------------
19980218 08:49:43 Actie    :5      Gebeu. :1261 Gelogd
19980218 08:49:43                  Stop Zoemer
19980218 08:49:43                  18/02/98  08:19:48 P:1
19980218 08:49:43 ----------------------------------------
19980218 08:49:43 Actie    :6      Gebeu. :1262 Gelogd
19980218 08:49:43                  Deurcontact gesloten
19980218 08:49:43                  18/02/98  08:21:09 P:1
19980218 08:49:43 ----------------------------------------
19980218 08:49:43 Fout     :2      Gebeu. :1263 Gelogd
19980218 08:49:43                  Deur contact
19980218 08:49:43                  18/02/98  08:21:11 P:1
19980218 08:49:43 ----------------------------------------
19980218 08:49:43 Actie    :7      Gebeu. :1264 Gelogd
19980218 08:49:43                  HERSTEL
19980218 08:49:43                  18/02/98  08:22:35 P:1
19980218 14:28:29 ----------------------------------------
19980218 14:28:29 Alarm    :1      Gebeu. :1509 Aktief
19980218 14:28:30 Zone     :2      Gebied :0
19980218 14:28:30 Adres    :3/4    Brand
19980218 14:28:30 DKKV             18/02/98  14:24:05 P:1
19980218 14:28:30 C TELEFOONCENTRALE
19980218 14:28:46 ----------------------------------------
19980218 14:28:46 Actie    :3      Gebeu. :1510 Gelogd
19980218 14:28:46                  Stop Zoemer
19980218 14:28:46                  18/02/98  14:24:23 P:1
```

Aritech alarms are always sent to group ARITECH, because no pager information is available in the datastream. Messages are sent with alarm description ARITECH. An alarm is set only when Gebeur occurs in the datastream. When BRAND occurs the message is BRAND; in other cases the message is ARITECH. When HERSTEL occurs a general reset of all ARITECH alarms is issued.

> ***Note:*** Use of this protocol usually requires consulting services and customization.

BEMAC

Valid manufacturer is BEMAC, valid model is DIANA 1 and DIANA 2.

Bemac is based upon installation Clinique St-Vincent Rocourt.

Figure 431
Sample Bemac protocol data

```
20000913 15:07:09 I:<866/LOC 101B/0>
20000913 15:09:09 I:<861/LOC 222B/0>
20000913 15:09:31 I:<861/LOC 333B/0>
20000913 15:10:47 I:<861/LOC 444B/0>
20000913 15:11:34 I:<999/RESET/0>
20000913 15:12:04 I:<999/RESET/0>
20000913 15:12:39 I:<999/RESET/0>
```

Bemac alarms contain three fields, a pager number, a message and a tone code. Alarms are sent with group equal to the first parameter (for example, 866). The message is retrieved from the second parameter (for example, LOC 101B). When the third parameter is 0 the message is reset. When the message is RESET all messages for all groups are reset; in other cases only the specific message for the specified group is reset. When the third parameter is a value other than 0, the message is set. During set the alarm description is BEMAC_x, where x is the specified tone code (for example, tone code 3 sets message with alarm description BEMAC_3.

ELDAD

Valid manufacturer is ELDAD, valid model is specified through a special syntax, for example, L:48-0:RC-1:SR-2:SS-3:SS-4SR. Note that the model is built upon components having syntax A:BB and separated with a hyphen (-).

- L:xx denotes that the length of an alpha-message is xx bytes. For example, L:48 means that alpha-messages are 48 bytes long, L:24 denotes alpha-messages are 24 bytes long.
- 0:xx specifies behaviour of tone code 0, 1:xx specified behaviour of tone code 1, 2:xx specifies behaviour of tone code 2, and so on.

For each tone code, the syntax ends on two characters. The first character can be S or R. S denotes set of alarm, R denotes reset of alarm. The second character can be S or R or C. The value S refers to remove after *SENT, the value R refers to remove after *RESET, the C refers to remove after *CALC.

For example, L:48-0:RC-1:SR-2:SS-3:SS-4SR means the alpha-messages are 48 bytes long, tone code 0 denotes *RESET alarm remove after *CALC, tone code 1 and 4 denote *SET alarm remove after *RESET, and tone code 2 and 3 denote *SET alarm remove after *SENT.

Bemac is based upon installation Sint-Franciskus-Ziekenhuis Heusden-Zolder.

The syntax is

```
‘STX’ + "XXXXTZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZYYYYYP" +
‘LF’ + ‘CR’
```

where:

XXXX = pager number

T = Tone-code

ZZ.. = Alpha-message (usually 24 or 48 bytes)

YYYYY= 5-digit information (= message if ZZ.. are all "…")

P = present flag

Figure 432
Sample Eldad protocol data

```
20000419 00:00:45 I:_01241NUR A203                00000P
20000419 00:00:45 O: _(ACK)
20000419 00:01:35 I:_01640NUR A203                00000P
20000419 00:01:35 O: _(ACK)
20000419 00:03:38 I:_01244ASS A203                00000P
20000419 00:03:38 O: _(ACK)
20000419 00:03:50 I:_01244ASS A203                00000P
20000419 00:03:50 O: _(ACK)
20000419 00:07:09 I:_01142TECHNISCH               00000P
20000419 00:07:09 O: _(ACK)
20000419 00:11:41 I:_01643BRAND                   00000P
20000419 00:11:41 O: _(ACK)
```

Eldad messages are either *SET or *RESET based upon tone code and model configuration. The group is located from the datastream (4-byte pager number). The message is retrieved from the alpha-message, but if the alpha-message is a string of period (.) characters then 5-byte digit information is used instead. The alarm description is the tone code (for example, 1 or 2 or 3 and so on).

STEAFA

Note: The Landis-Steafa interface was not ordered nor implemented and protocol information is provided on an as-is basis. Contact your software vendor for implementation.

Figure 433
Sample Steafa protocol data

```
19970403000053 COM    03/04/97  Prio 1 CONTROLLER 00   SYSTEM STAEFA
test alarm
19970403000054 COM    00:05:00      COM. NICO-RS MODU(U)L(EN) NORMAAL
UIT
19970403000054 COM                                                  00
COS   2000
19970403000154 COM ____
19970403000154 COM    03/04/97  Prio 1 CONTROLLER 00   SYSTEM STAEFA
test alarm
19970403000154 COM      00:06:01        GEEN COMMUNICATIE NICO-RS
MODU(U)L(EN)   IN
19970403000154 COM                                                  00
COS   2000
19970403000252 COM ____
19970403000253 COM    03/04/97  Prio 1 CONTROLLER 00   SYSTEM STAEFA
test alarm
19970403000253 COM    00:07:00      COM. NICO-RS MODU(U)L(EN) NORMAAL
UIT
19970403000253 COM                                                  00
COS   2000
19970403000354 COM ____
```

NIRA

Valid manufacturer is NIRA, valid model is *BASE.

Nira is based upon installation Eeuwfeestkliniek Antwerpen.

Figure 434
Sample Nira protocol data

```
20010110 00:00:02 I: 22:37 | 0781 | 10 |    | 6  |          |  -  | 416-C
20010110 00:00:12 I: 22:37 | 0784 | 10 |    | 6  |          |  -  | 419-C
20010110 00:00:12 I: Tuesday
9-JANUARY-2001
20010110 00:00:12 I:
20010110 00:00:12 I: TIME    ADDR. LINK S/P CODE CALL-INFO ID    MESSAGE
20010110 00:00:12
I:-------+------+----+---+----+--------+-----+----------------------
20010110 00:00:12 I: 22:37 | 0777 | 08 |   | 5  |        |  -  | 336-C----A
20010110 00:00:33 I: 22:38 | 0777 | 08 |   | 5  |        |  -  | 336-C----A
20010110 00:00:33 I: 22:38 | 0781 | 10 |    | 6  |          |  -  | 416-C
20010110 02:02:17 I: 00:39 | 0777 | 08 |   | 5  |        |  -  | 336-C----A
20010110 02:02:18 I: 00:39 | 0784 | 10 |    | 7  |          |  -  | 520-A
20010110 02:02:38 I: 00:40 | 0777 | 08 |   | 5  |        |  -  | 336-C----A
20010110 02:02:59 I: 00:40 | 0777 | 08 |   | 5  |        |  -  | 336-C----A
```

Alarms are always *SET, and repeat mechanisms are to be configured to know whether an alarm is no longer active (logical *RESET based upon no longer repeating). Therefore alarm repeat interval must be specified to, for example, 30 seconds. The room number is retrieved from the datastream (for example, 416, 419, 336 and so on) and used as group. The message is 4 bytes long and consists of room number, followed by either an C or an A indication. Datastreams in format XXX-C and XXX----A are considered as C, datastreams in format XXX-A and XXX---AA and XXX—AAA are considered A type alarms. Therefore, the message text is 416C or 520A. Alarm description is NIRA_C for messages that end with C and NIRA_A for alarms that end with A. All messages are remove after *SENT.

> ***Note:*** Use of this protocol usually requires consulting services and customization.

TELEVIC

Valid manufacturer is TELEVIC.

Valid model is PROTOCOL CONVERTOR – L:xx, with xx between 01 and 99.

Note: The extension – L:xx is new in release 2, and must be specified. The functionality is introduced to obtain more flexibility in message handling. The following string handling is performed:

- Remove leading spaces of the message

  NUR K100 -> NUR K100

- Append a trailing space to the result

  BEERPUT -> BEERPUT

- Look up the occurrence of the first space character

  NUR K100 -> 4

  BEERPUT -> 8

- Keep the leading non-blank characters

  NUR K100 and 4 -> „NUR

  BEERPUT and 8 -> BEERPUT

- Keep the leading characters only, with length specified in L:xx

  NUR and L:03 -> NUR

  BEERPUT and L:03 -> BEE

Table 56
Televic Example (Part 1 of 2)

Length	Original message	Resulting alarm type	Length
L:01	"NUR K100"	"N"	1
	"WC 120"	"W"	1
	"BEERPUT"	"B"	1
L:02	"NUR K100"	"NU"	2
	"WC 120"	"WC"	2

Table 56
Televic Example (Part 2 of 2)

	"BEERPUT"	"BE"	2
L:03	"NUR K100"	"NUR"	3
	"WC 120"	"WC"	2
	"BEERPUT"	"BEE"	3
L:04	"NUR K100"	"NUR"	3
	"WC 120"	"WC"	2
	"BEERPUT"	"BEER"	4
L:05	"NUR K100"	"NUR"	3
	"WC 120"	"WC"	2
	"BEERPUT"	"BEERP"	5

Refer to the official specifications on Televic Protocol Convertor. These specifications can be obtained from the manufacturer, or through Nortel sales support. Detailed information is beyond the scope of this document.

Televic is based upon installation CAZK campus Groeninghe Kortrijk.

Figure 435
Sample Televic protocol data

```
07/01/2001 00:02:15 - I:COM:_O0103224210          8POORT100Y4C_
07/01/2001 00:02:15 - O:COM:_A0103Y1A_
07/01/2001 00:02:22 - O:COM:_T010312421052_
07/01/2001 00:02:23 - I:COM:_A0103Y1A_
07/01/2001 00:02:24 - O:COM:_T010312421052_
07/01/2001 00:02:25 - I:COM:_A0103Y1A_
07/01/2001 00:11:17 - I:COM:_O0104225091          1NUR PALIY52_
07/01/2001 00:11:17 - O:COM:_A0104Y1D_
07/01/2001 00:11:23 - O:COM:_T01041250915F_
07/01/2001 00:11:24 - I:COM:_A0104Y1D_
07/01/2001 00:11:25 - O:COM:_T01041250915F_
07/01/2001 00:11:26 - I:COM:_A0104Y1D_
07/01/2001 00:16:39 - I:COM:_O0105225091          1NUR PALIY53_
07/01/2001 00:16:39 - O:COM:_A0105Y1C_
```

Televic is an extended two-direction protocol, which provides a number of protocol rules to keep the communication secure; for example, through sequencing each packet, requesting acknowledge string, handshake through clear-string, return of feedback on message delivery through what is called terugmelding string, error detection through checksum, and so on. Refer to the protocol specifications for details on Televic protocol.

Regarding configuration, the following details are important:

The datastream contains a pager indication. This pager indication is used as a group indication.

Alarms can either be sent as type 1 (*SET of an alarm that has a *RESET type 0), type 0 (*RESET of an alarm that was previously *SET through code 1) and finally a type 2 (*SET of an alarm that does receive a *RESET). As a result, messages can be *SET or *RESET with remove after *SENT or remove after *RESET.

The DECT Messenger implements three distinct alarm descriptions.

1. The highest priority is assigned to alarm types that are configured through the specified length L:xx of the alarm text (For example, L:03 : NUR, ASS, SAN, REA, MUG, and so on). If this definition is found, the alarm attributes are fetched there.
2. When the first definition is unavailable, alarm types are fetched equal to the tone code (0, 1, 2, 3, 4, 5, 6, 7, 8, 9). If this definition is found, the alarm attributes are fetched there.
3. As the last option, the alarm types are fetched through *OTHER special value. If this definition is found, alarm attributes are fetched there. In absence of any of the three definitions, the alarms are ignored.

The alarm message is retrieved from the datastream (NUR PAL, POORT 100, and so on).

VSK

Valid manufacturer is VSK.

Valid models are:

- DE LICHTERVELDE
- OLV VAN VREDE
- ST-JOZEF

VSK is based upon the three installations defined in the model, with a different implementation for each, as illustrated in Figure 436 on page 1107, Figure 437 on page 1108, and Figure 438 on page 1109.

Figure 436
Sample DE LICHTERVELDE protocol data

```
19990329 11:58:29 R:-----------------------
19990329 11:58:29 R:D:HOOFDBORD+CENTR.L707
19990329 11:58:29 R:Z:043 D:0945
19990329 11:58:29 R:29-03-99 11:59 DET.FOUT
19990329 11:59:47 R:-----------------------
19990329 11:59:47 R:S:GENERAL RESET
19990329 11:59:47 R:S:9130
19990329 11:59:47 R:29-03-99 12:00 SYS.FOUT
19990329 12:08:27 R:-----------------------
19990329 12:08:27 R:S:GENERAL RESET
19990329 12:08:27 R:S:9130
19990329 12:08:27 R:29-03-99 12:09 SYS.FOUT
19990329 12:08:34 R:-----------------------
19990329 12:08:34 R:S:GEEN PAPIER MEER !
19990329 12:08:34 R:S:9098
19990329 12:08:34 R:29-03-99 12:09 SYS.FOUT
19990329 12:08:59 R:-----------------------
19990329 12:08:59 R:S:BUZZER RESET
19990329 12:08:59 R:S:9131
19990329 12:08:59 R:29-03-99 12:09 SYS.FOUT
19990329 12:21:06 R:-----------------------
19990329 12:21:06 R:D:GANG            G710
19990329 12:21:06 R:Z:043 D:0931
19990329 12:21:06 R:29-03-99 12:21 DET.FOUT
19990329 12:21:35 R:-----------------------
```

Figure 437
Sample OLV VAN VREDE protocol data

```
19981117 00:14:30 R:S:GENERAL RESET
19981117 00:14:30 R:S:9130
19981117 00:14:30 R:17-11-98 00:11 SYS.FOUT
19981117 00:14:53 R:-----------------------
19981117 00:14:53 R:D:BEZOEKZAAL       303
19981117 00:14:53 R:Z:003 D:0193
19981117 00:14:53 R:17-11-98 00:11 DET.FOUT
19981117 00:16:03 R:-----------------------
19981117 00:16:03 R:D:BEZOEKZAAL       303
19981117 00:16:03 R:Z:003 D:0193
19981117 00:16:03 R:17-11-98 00:13 DET.FOUT
19981117 00:21:41 R:-----------------------
19981117 00:21:41 R:S:BUZZER RESET
19981117 00:21:41 R:S:9131
19981117 00:21:41 R:17-11-98 00:18 SYS.FOUT
19981117 05:47:14 R:-----------------------
19981117 05:47:14 R:S:NACHTBEL       POORT
19981117 05:47:14 R:S:9176      GP01
19981117 05:47:14 R:17-11-98 05:44 SYS.FOUT
19981117 05:47:51 R:-----------------------
19981117 05:47:51 R:S:BUZZER RESET
19981117 05:47:51 R:S:9131
19981117 05:47:51 R:17-11-98 05:44 SYS.FOUT
19981117 06:32:10 R:-----------------------
19981117 06:32:10 R:S:NACHTBEL       POORT
19981117 06:32:10 R:S:9176      GP01
19981117 06:32:10 R:17-11-98 06:29 SYS.FOUT
19981117 06:40:25 R:-----------------------
```

Figure 438
Sample ST-JOZEF protocol data

```
19980318 11:30:44 -----------------------
19980318 11:30:44 D:KAMER 1
19980318 11:30:45 ZONE #00
19980318 11:30:45 Z:000 D:0001
19980318 11:30:46 26-01-98 04:13 BRAND
19980318 11:40:54 S:VERWIJDER CFG. STRAP
19980318 11:40:54 S:9146
19980318 11:40:55 26-01-98 04:12 SYS.FOUT
19980318 11:40:57 D:KAMER 56
19980318 11:40:57 Z:001 D:0056
19980318 11:40:58 26-01-98 04:12 ISOLATIE
19980318 11:40:58 -----------------------
19980318 11:40:59 D:KAMER 1
19980318 11:40:59 ZONE #00
19980318 11:41:00 Z:000 D:0001
19980318 11:41:00 26-01-98 04:13 BRAND
19980318 11:42:48 S:VERWIJDER CFG. STRAP
19980318 11:42:49 S:9146
19980318 11:42:49 26-01-98 04:12 SYS.FOUT
19980318 11:44:00 D:KAMER 56
19980318 11:44:01 Z:001 D:0056
19980318 11:44:01 26-01-98 04:12 ISOLATIE
19980318 11:44:02 -----------------------
19980318 11:44:02 D:KAMER 1
19980318 11:44:03 ZONE #00
19980318 11:44:03 Z:000 D:0001
19980318 11:44:04 26-01-98 04:13 BRAND
19980318 11:44:23 -----------------------
19980318 11:44:24 S:NETONDERBREKING
19980318 11:44:24 S:9048      L1.0
19980318 11:44:25 26-01-98 04:13 SYS.FOUT
19980318 11:44:37 -----------------------
19980318 11:44:38 D:KAMER 49
19980318 11:44:38 Z:001 D:0049
19980318 11:44:39 26-01-98 04:14 DET.FOUT
19980318 11:46:14 -----------------------
19980318 11:46:14 S:VERWIJDER CFG. STRAP
```

continued on next page...

Sample ST-JOZEF protocol data (continued)

```
19980318 11:46:15 S:9146
19980318 11:46:15 26-01-98 04:17 SYS.FOUT
19980318 11:46:29 S:VERWIJDER CFG. STRAP
19980318 11:46:29 S:9146
19980318 11:46:30 26-01-98 04:12 SYS.FOUT
19980318 11:46:34 D:KAMER 56
19980318 11:46:34 Z:001 D:0056
19980318 11:46:35 26-01-98 04:12 ISOLATIE
19980318 11:46:35 -----------------------
```

Fire alarms are sent to group VSK_F (fire alarm) with alarm description VSK_F, system errors are sent to group VSK_S (system errors) with alarm description VSK_S, detector errors are sent to group VSK_D (detector errors) with alarm description VSK_D.

All alarms are *SET with remove after *RESET. When GENERAL RESET occurs in the datastream, all active alarms for the VSK input program are reset for all groups.

Small differences between the three models are found, for example, in the level of detail in the messages that are sent (for example, FOUT BRANDCENTRALE in DE LICHTERVELDE, VSKFOUT in ST JOZEF and all details in OLV VAN VREDER). Also, fire alarm messages are formatted slightly differently between the models (BRAND or BR*xxxxx where xxxxx denotes a location).

> ***Note:*** Use of this protocol usually requires consulting services and customization.

WORMALD

Valid manufacturer is WORMALD, valid model is *BASE or L:xx (new in release 2.9.11).

Wormald is based upon installation Alexianen Bouchout and RUCA Antwerpen and is compatible with both versions through automatic-protocol-recognition programming.

The model L:xx defines the group. The model *BASE, identifies the group WORMALD_F or WORMALD_P depending on the type of alarm (see the examples “Alexianen” and “RUCA” on page 1112).

If the model = L:xx, the first xx characters of the message define the group.

If the group is not defined in the Messenger_CFG.mdb database, the eKernel application sends the request to the group identified with a question mark (?), if one is defined in the table eKERNEL_GROUP (field GRP_Descr_str). This feature is supported for eCAP WORMALD only when model = L:xx.

Examples:

Alexianen

```
27/04/99 15:30:23
 ALARM 001-084 DK
 8000 REV EVACUA
```

This datastream results in *SET of alarm with alarm description WORMALD_F and message F8000 REV EVACUA, remove after *RESET.

The group varies depending on the model.

Table 57
F8000 REV EVACUA groups

Model	Group
*BASE	WORMALD_F.
L:01	8 ((group description: field GRP_Descr_str from table eKERNEL_GROUP)
L:02	80
L:03	800
L:04	8000

```
27/04/99 19:55:52
  VOORALARM 0001-024 ION
  9003 KEU EETPL
```

This datastream results in *SET of alarm with alarm description WORMALD_P and message P9003 KEU EETPL, remove after *RESET.

The group varies depending on the model.

Table 58
P9003 KEU EETPL groups

Model	Group
*BASE	WORMALD_P.
L:01	9
L:02	90
L:03	900
L:04	9003

```
 27/04/99 19:56:12
   Reset
```

This datastream results in a *RESET of alarm description *ALL for group *ALL and message *ALL.

RUCA

```
0000. Brand                 MG 099  MLD 009              01:01:00 01.01.97
      Boodschap
```

This datastream results in a *SET of alarm description WORMALD_F , with message Boodschap and remove after *RESET.

The group varies depending on the model.

Table 59
F8000 REV EVACUA groups

Model	Group
*BASE	WORMALD_F.
L:01	B
L:02	Bo
L:03	Boo
L:04	Bood

```
0001. Reset
```

This datastream results in *RESET of alarm description *ALL for group WORMALD_F with message *ALL and remove after *RESET.

> ***Note:*** Use of this protocol usually requires consulting services and customization.

Generic

Valid manufacturer is GENERIC, valid model is *BASE.

This new manufacturer and model combination is implemented in release 2, to handle fixed-formatted serial inputs that are built upon single lines and separated with a fixed character.

There are many parameters available to define the interpretation of the datastreams that are received through the generic eCAP implementation. These parameters define criteria for retrieval of group, message, alarm description, set_or_reset and remove_after parameters. There are also default values available if some parameters are missing. Another set of parameters describes record separators, field separators, and so on.

Refer to “Table: eCAP_generic” on page 1315 for detailed information on the configuration of the interface, including descriptions of the usage of each parameter.

Module – eESPA

The module eESPA consists of one program. The program is eESPA.exe and is written in Visual Basic (v6.0).

In general, the programs reside in the default directory C:\SOPHO Messenger@Net\Exe, unless otherwise implemented in your environment.

Overview

eESPA.exe

The eESPA.exe is a Visual Basic component of the eESPA module. The program communicates with two processes: the eKERNEL.exe and external paging equipment. The eKERNEL.exe is the central engine that centralises all database access and communication with input and output capable modules.

The eESPA.exe communicates with eKERNEL.exe by means of TCP sockets. In this communication, eESPA.exe is a TCP client software that connects to the eKERNEL component, acting as TCP server software.

At start-up, eESPA.exe contacts the eKERNEL.exe by means of a socket connection. eESPA.exe requires at start-up a few parameters, so that eESPA can identify itself and locate the eKERNEL.exe program. This is carried out by means of parameters in the properties section of the shortcut that initiates eESPA.exe. This shortcut is usually located in the Windows Startup group.

Figure 439
Typical parameters in the shortcut

```
"C:\SOPHO Messenger@Net\Exe\eESPA.exe"
/Site:1
/eKernel address:*LOCAL
/eKernel port:3114
/Log drive:C
/SleepBeforeAnswer:0
```

In the example shown in Figure 439, the eESPA.exe identifies itself as belonging to site 1, and specifies the location of eKERNEL through IP address *LOCAL and port 3114. The special value *LOCAL refers to the assigned IP address of the first NIC adapter found in the PC, as can be found in the IPCONFIG.exe command or in the appropriate sections of the Windows network settings. The keyword Log drive refers to the drive where the logging data must be stored. Usually this is C:\SOPHO Messenger@Net\Log\.

The keyword SleepBeforeAnswer refers to the number of milliseconds the system waits before sending an answer to the linked station. Some systems block the answer if the answer is sent immediately (less than 6 milliseconds after receipt). Use this parameter to set a delay of x milliseconds before the output is sent.

> ***Note:*** The maximum supported value is 150 milliseconds

Set this value as low as possible, because during the delay time, the application is inactive, so high values can disrupt the operation of the system.

At start-up, the eESPA.exe sends an XML string to eKERNEL.exe requesting a configuration. This step is needed for each module that interacts with eKERNEL.exe, because this approach allows central administration from a single database, even if some client modules are located on a distributed machine.

Figure 440
Typical <cfgrqs> configuration request and its received <cfgrpy> configuration reply

```
<xml>
<cfgrqs>
<appl>eESPA</appl>
<site>1</site>
</cfgrqs>
</xml>
```

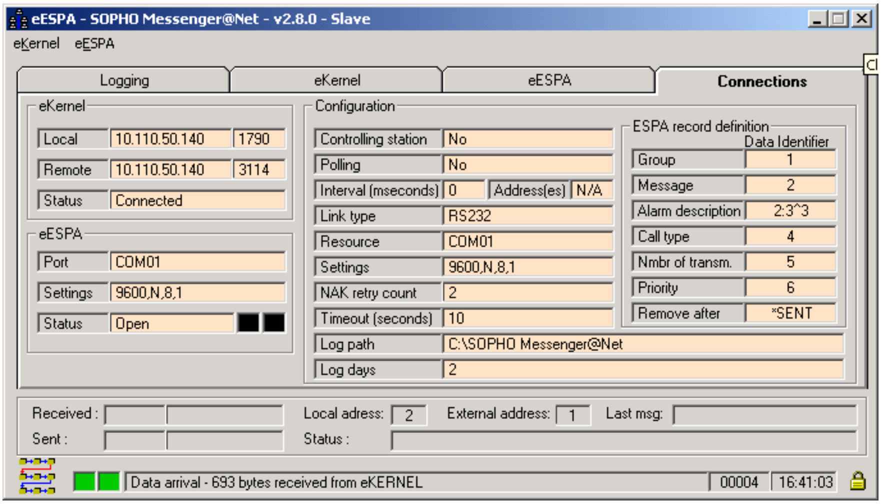
```
<xml>
<cfgrpy>
<resource>COM01</resource>
<settings>9600,N,8,1</settings>
<link_type>RS232</link_type>
<ControlStation>Y</ControlStation>
<polling_intv>300</polling_intv>
<Polling_address_list>2</Polling_address_list>
<localAddress>1</localAddress>
<externalAddress>2</externalAddress>
<dataId_Group>1</dataId_Group>
<group_default>eESPA</group_default>
<dataId_Msg>2</dataId_Msg>
<msg_default>Default ESPA msg</msg_default>
<dataId_Ala_descr>3</dataId_Ala_descr>
<ala_descr_default>1</ala_descr_default>
<remove_after>*RESET</remove_after>
<nak_retry_cnt>2</nak_retry_cnt>
<timeout>600</timeout>
<handshaking>0</handshaking>
<log_path>C:\SOPHO Messenger@net</log_path>
<log_days>14</log_days>
</cfgrpy>
</xml>
```

Refer to the appropriate sections on the database tables that define the received parameters for more information on each value. The information in this document is provided for informational purposes only; a detailed description of these internal inter-process communications is beyond the scope of this document.

If no valid licence is available to run an eESPA module, the eKernel sends a reply <xml><pgmsts>NO LICENCE AVAILABLE</pgmsts></xml> and close its port. If you receive this message upon connection to the eKernel, check Nortel Licence Manager for available licences.

When the configuration is received, the **Connection** tab displays information similar to what is pictured in Figure 441.

Figure 441
eESPA Connection tab showing a valid configuration



eKernel

Local	10.110.50.140	1790
Remote	10.110.50.140	3114
Status	Connected	

eESPA

Port	COM01
Settings	9600,N,8,1
Status	Open ■ ■

Configuration

Controlling station	No		
Polling	No		
Interval (mseconds)	0	Address(es)	N/A
Link type	RS232		
Resource	COM01		
Settings	9600,N,8,1		
NAK retry count	2		
Timeout (seconds)	10		
Log path	C:\SOPHO Messenger@Net		
Log days	2		

ESPA record definition

	Data Identifier
Group	1
Message	2
Alarm description	2:3^3
Call type	4
Nmbr of transm.	5
Priority	6
Remove after	*SENT

Received :
Sent :
Local adress: 2
External address: 1
Last msg:
Status :

Data arrival - 693 bytes received from eKERNEL | 00004 | 16:41:03

Because the eESPA is designed to handle serial data communications with a number of paging systems, the eESPA must be configured before use. These values are returned through the <cfgrpy> reply that is sent on return of the <cfgrqs> request.

> ***Note:*** The values shown in Figure 441 are retrieved from the DECT Messenger database; from the KERNEL_INPGM table, and from the eESPA, eESPA_OUTBOUND_CFG, and the eKERNEL_SITE tables.

At start-up, the eESPA.exe opens the specified COM port with the specified settings.

Note: The COM port you identify must be available, and you must specify a valid baud rate, and so on.

As well, a physical connection between the specified COM port and the external paging system must be available, which requires a serial cable. In most cases, a standard null-modem cable can be used. However, in some cases, alarm systems support a limited number of control signals (for example, ground, send and receive), so check with the alarm system vendor for cable specifications.

If no COM ports are available, extra hardware (such as DigiBoard PC/4e and DigiBoard PC/8e) is required to provide extra serial ports. Investigate compatibility issues (operating system support, driver available, and so on) and hardware requirements (memory, available slots, IRQ conflicts, and so on) before purchasing equipment, or configuring the system.

In some cases, additional hardware is needed, for example, when RS-232-C limitations apply (for example, at 9600 baud maximum limit of 9 metres). In some cases galvanic isolation is requested, or base-band modems, SOPHO LAM, CISCO equipment, and so on are needed to bridge the distance between the DECT Messenger and the alarm system. In many cases the distance between the DECT Messenger and the external-paging system is relatively small, so no extra hardware is needed.

Once a link is established between eESPA and the paging system, the eESPA handles further communications and informs eKERNEL when relevant information is to be exchanged.

For a detailed description of the ESPA4.4.4 protocol, refer to the proposal for serial data interface for paging equipment (Nov. 1984), reference JMJ182/NB/12B, and ISO1745 Information processing, basic mode control procedures for data communication systems.

Functional description

In general, eESPA is designed to provide eKERNEL with paging information. This is carried out using a <msgrqs> message request. For some interfaces eKERNEL must send feedback to the paging system, a process that is handled through <msgrpy> message reply request.

Figure 442
<msgrqs> message request

```
<xml><msgrqs>
<id>00786</id>
<group>1234</group>
<call_type>3</call_type>
<transmission_nmbr>1</transmission_nmbr>
<alarm_cnt>1</alarm_cnt>
<message_01>NURSE ROOM45</message_01>
<beep_code_01>1</beep_code_01>
<priority_01>2</priority_01>
</msgrqs></xml>
```

Every <msgrqs> message belongs to a group and has a specific group ID. A group contains one or more requests. For every message request in a group, a data block is created. A data block consists of a header, record separators, unit separators, and data that is retrieved from the message request. Every data block also contains a specifically calculated checksum (block check character ISO 1155). After sending the data over the serial line, the receiving side uses the block check character (BCC) to check whether data has arrived properly or not. In the event of a successful delivery, the receiving side answers with an ACK.

Figure 443
<msgrpy> message ACK

```
<xml><msgrpy>
<id>00786</id>
<sts_cnt>1</sts_cnt>
<sts_01>ACK^</sts_01>
</msgrpy></xml>
```

If an incorrect BCC is found, delivery fails, and the receiving side sends a NACK, which is prefixed with error code 1 (“Transmission error, corrupt characters or corrupt BCC received by the station”).

eESPA handles only data blocks of type 1, Call to Pager data blocks. If another type of data block comes in, eESPA reacts by sending an ACK, but the data block is not processed.

Delivery can also fail if a timeout occurs while sending the data block. The temporary master station, which is always the sending side, expects to receive an ACK within a timeout of eESPA_Timeout_n seconds. In the event of a timeout on sending a data block, the sending side tries to re-send the data block. This retry is attempted x times (where x is the defined value of the field eESPA_NAK_retry_cnt_n in the eESPA table). After retrying x times and not receiving an ACK, the temporary master station decides that the transaction is unsuccessful.

Figure 444
<msgrpy> message NACK

```
<xml><msgrpy>
<id>00786</id>
<sts_cnt>1</sts_cnt>
<sts_01>NACK^</sts_01>
</msgrpy></xml>
```

Data flow

The ESPA4.4.4 protocol prescribes a controlling station that polls devices on the communication line. Polling means sending out requests for data. The polling device, which is also called controlling station or master, sends out requests to the other devices available on the communication line. Every device on the line has a specific address. The characters 0 to 9 are available as addresses. Nortel recommends that you assign the character 1 to the controlling station. In the field eESPA_Polling_address_list_str of the table eESPA you can define multiple addresses of slave devices. At least one address (that represents a slave) is required in this field. Multiple addresses are separated by ^.

For example: the value 2^4^5 in eESPA_Polling_address_list_str defines three slaves that are polled by the controlling station.

Define a control station by placing eESPA_ControlStation_b in the eESPA table on True. eESPA_LocalAddress_n and eESPA_ExternalAddress_n must be filled up respectively with the local address of the module (a controlling station prefers a local address 1), and the address of an external eESPA module or device, with which the module communicates.

The controlling station polls every address with an enquiry. To extend the example, the controlling station sends 2ENQ, 4ENQ, and 5ENQ. The field eESPA_Polling_intv_n in the eESPA table defines the time between sequencing polls.

A slave whose address is polled reacts by replying with either a nothing-to-transmit (EOT), or an enquiry (<master address>ENQ) that tells the controlling station that this slave wants to transmit some data. If a slave receives data that is not assigned to the slave address, the slave ignores the data. If a slave does not respond to an enquiry within eESPA_Timeout_n seconds, the controlling station places this slave in a special offline list. When polling, the controlling station checks the offline list to determine if a slave is online or not, before sending an enquiry. After 60 seconds, the slave is removed from the offline list, and polling to the IP address of the slave is restarted. If the slave does not react, the slave is put back in the offline list. By using an offline list (also known as a black list) the polling interval is not disturbed by repeated timeouts of some slaves.

The controlling station stops polling when data is waiting to be sent to one of the slaves, or when a slave has indicated that data is ready to send.

The controlling station stops polling when a message request is received from the eKERNEL. The controlling station then creates a data block and sends this to the appropriate slave address. A slave station sends data in the same fashion, but with one difference: the slave first has to wait to be polled to tell the controlling station that data is ready to send. When a slave is polled and has data to send, the slave tells the controlling station to stop polling. The controlling station accepts this request by sending an ACK to the slave that wants to send data. When it receives an ACK from the controlling station, the slave becomes temporarily master station. Only a master station is able to send data blocks. A master station always sends data; a slave always receives. In this scenario, the controlling station becomes (temporarily) a slave.

Every eESPA module has a status bar with some additional information about the actual communication situation.

- The label Receiving shows the timestamp and the latest incoming databits. Values that can appear on this label are as follows: ACK, NAK, EOT, address + ENQ, SOH (start of data), and data.

- The label Sent shows the timestamp and the databit that was last sent. Values that can appear on this label are as follows: ACK, NAK, EOT, address + ENQ, SOH (start of data), and data.

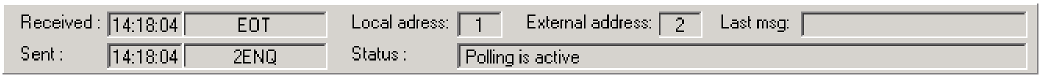
- The Local address field shows the defined value of eESPA_LocalAddress_n in the eESPA table. Nortel recommends that you set the controlling station local address to 1. The field eESPA_ControlStation_b in the eESPA table defines whether this module is a controlling station or not.

  In the DECT Messenger model, a module always communicates with one other module (master to slave or point to point). The address of the other station is defined in the eESPA_ExternalAddress_n field in the eESPA table. In the case of a non-controlling module (defined by setting eESPA_ControlStation_b on No in the database), for example, a local address of 2 and an external address of 1 can be used. In this case, the module communicates directly with the controlling station.

- The label Status shows log information to allow users to see special actions.

Figure 445 shows an example of the eESPA status bar.

Figure 445
Status of master/slave



Received : 14:18:04 EOT
Sent : 14:18:04 2ENQ
Local adress: 1
External address: 2
Last msg:
Status : Polling is active

Logging

In the **Logging** tab, only basic (default) logging is shown.

Basic logging: incoming and outgoing data on the communication port (I:COM and O:COM), incoming and outgoing data on the socket communication with the eKernel (I:TCP and O:TCP), and warning information.

To show and log additional information, choose the menu item **eESPA** > **Logging** > **Detailed**. The additional information is set in bold in Figure 446.

Figure 446
Detailed logging information

```
I:INF:--> Created datablock is: _1_156789-2eAPI Koekoek-51-63_O
O:COM:_1_156789-2eAPI Koekoek-51-63_O
I:INF:--> ACK received on sending datablock
O:COM:EOT
I:INF:--> Concluded transaction with sending an EOT
I:COM:ACK
I:COM:EOT
I:INF:--> Received EOT character after sending messages.
O:COM:EOT
O:TCP:<xml><msgrpy><id>00124</id><sts_cnt>1</sts_cnt>
<sts_01>ACK^</sts_01></msgrpy></xml>
```

The label Last msg shows the last sent or received message.

Module – eESPA – sample

Table 60
eESPA sample (Part 1 of 2)

MASTER (address 1)		SLAVE (address 2)
No data to be transferred		
2ENQ	✍	
	✍	EOT
Master has data to be transferred		
1ENQ (I want to send something)	✍	
2ENQ (Destination address)	✍	
	✍	ACK (I am ready to receive data)
Data Block1	✍	
	✍	1NAK
Data Block1	✍	
	✍	ACK
EOT	✍	
	✍	EOT
2ENQ (polling)	✍	
Master has data to be transferred (Slave is not ready to receive data)		
1ENQ (I want to send something)	✍	

Table 60
eESPA sample (Part 2 of 2)

2ENQ (Destination address)	✍	
	✍	1NAK (Transmission error)
EOT	✍	
1ENQ	✍	
2ENQ	✍	
	✍	1NAK
EOT	✍	
Slave has data to be transferred		
2ENQ	✍	
	✍	1ENQ (I have data for address 1)
ACK (I am ready to receive data)	✍	
	✍	DATA Block1
ACK	✍	
	✍	DATA Block2
1NAK (Transmission error)	✍	
	✍	DATA Block2
ACK	✍	
	✍	EOT
2ENQ (Polling)	✍	
	✍	EOT
2ENQ	✍	
	✍	EOT
...		

Module – eDMSAPI

The module eDMSAPI consists of two separate programs. One program is eDMSAPI and is written in Visual Basic. The other program is called CSTA_Service.exe and is written in C++.

In general, both programs reside in the default directory C:\SOPHO Messenger@Net\Exe, unless otherwise implemented in your environment.

Overview

eDMSAPI.exe

The eDMSAPI is the Visual Basic component of the eDMSAPI module. The program communicates with two processes: the eKERNEL and the CSTA Service. The eKERNEL is the central engine that centralises all database access and communication with input and output capable modules.

The eDMSAPI communicates with both eKERNEL and CSTA_Service.exe by means of TCP sockets. In both communications, eDMSAPI is a TCP client software that connects to the two other components, acting as TCP server software.

For external clients (eWEB), the eDMSAPI acts as a multiple socket server.

At start-up, eDMSAPI contacts the eKERNEL by means of a socket connection. For the eDMSAPI module to locate the eKERNEL, the eDMSAPI must start up with parameters that identify the eDMSAPI module and locate the eKERNEL program. These parameters are provided to eDMSAPI in the Properties section of the shortcut that initiates eDMSAPI.

This shortcut is usually located in the Windows Startup group (click **Start** on the Windows taskbar and choose **Programs** > **Startup)**.

Figure 447
Typical parameters in the shortcut

```
"C:\SOPHO Messenger@Net\Exe\eDMSAPI.exe"
/Site:1
/eKernel port:3101
/eKernel address:*LOCAL
/Log drive:C
```

In the example shown in Figure 447, eDMSAPI identifies itself as belonging to Site 1, and specifies the location of eKERNEL through IP address *LOCAL and port 3101. The special value *LOCAL refers to the assigned IP address of the first NIC adapter found in the PC, as can be found in the IPCONFIG.exe command or in the appropriate sections of the Windows network settings. The keyword Log drive refers to the drive where the logging data must be stored; usually this is C:\SOPHO Messenger@Net\Log\.

At start-up, the eDMSAPI sends an XML string to eKERNEL requesting a configuration. This step is needed for each module that interacts with eKERNEL, because this approach allows central administration using a single database, even if some client modules are located on a distributed machine.

Figure 448
A typical <cfgrqs> configuration request and its received <cfgrpy> configuration reply

```
<xml>
<cfgrqs>
<appl>eDMSAPI</appl>
<site>1</site>
</cfgrqs>
</xml>
```

```
<xml>
<cfgrpy>
<seat_cnt>20</seat_cnt>
<msg_dly>3</msg_dly>
<csta_api_address>10.110.50.140</csta_api_address>
<csta_api_port>59000</csta_api_port>
<external_seat_cnt>3</external_seat_cnt>
<external_port>2010</external_port>
<csta_pbx_address>10.110.49.171</csta_pbx_address>
<csta_pbx_port>2555</csta_pbx_port>
<csta_licence>Messenger</csta_licence>
<guarding_intv>60</guarding_intv>
<guarding_Retry_intv>20</guarding_Retry_intv>
<eKernel_Seat_cnt>10</eKernel_Seat_cnt>
<GeneralTimeOut>15</GeneralTimeOut>
<Ack2TimeOut>30</Ack2TimeOut>
<DataPathDelay>2</DataPathDelay>
<network>ETHERNET_DMC</network>(new in Msg@Net R3.0)
<pbxtype>DMC</pbxtype>(new in Msg@Net R3.0)
<IoReg_cnt>3</IoReg_cnt>
<IoReg_0001>863</IoReg_0001>
<IoReg_0002>123</IoReg_0002>
<IoReg_0003>914</IoReg_0003>
><keepalive>60</keepalive>
<log_path>C:\SOPHO Messenger@net</log_path>
<log_days>14</log_days>
</cfgrpy>
</xml>
```

Table 61
Possible values for the network and pbxtype tags

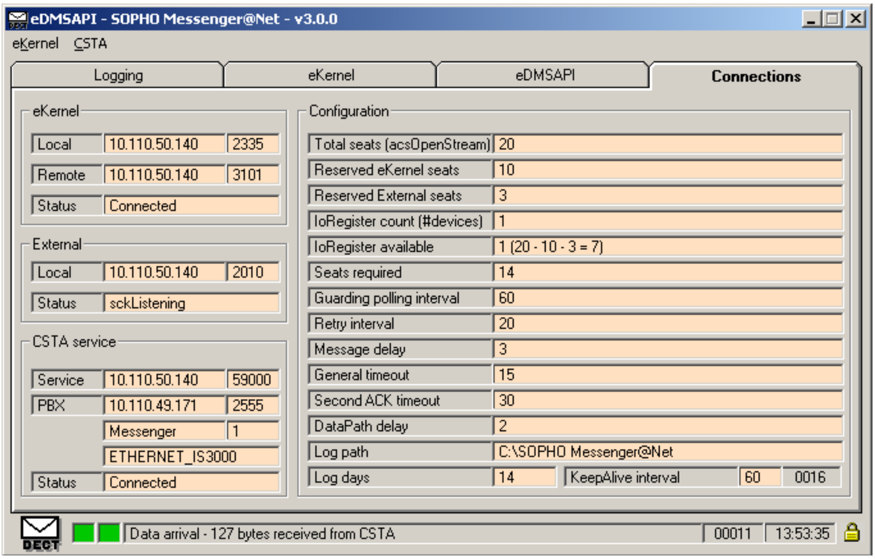
eDMSAPI_PBX_type_str(eDMSAPI	<pbxtype>	<network>
DAP controller	DAP Controller	dasgif
DMC	DMC	ETHERNET_DMC
NORTEL	NORTEL	Dasgif

Refer to the chapters of this document that deal with the database tables for more information on each value. A detailed description of these internal inter-process communications is beyond the scope of this document.

The parameter <IoReg_cnt> specifies how much DECT extension is IoRegistered (can send data messages to the DECT Messenger application).

The parameter <IoReg_xxxx> (where xxxx starts with 0001 till IoReg_cnt) specifies the DECT extensions that must be IoRegistered.

Figure 449
eDMSAPI Connections



eKernel

Local	10.110.50.140	2335
Remote	10.110.50.140	3101
Status	Connected	

External

Local	10.110.50.140	2010
Status	sckListening	

CSTA service

Service	10.110.50.140	59000
PBX	10.110.49.171	2555
	Messenger	1
	ETHERNET_IS3000	
Status	Connected	

Configuration

Total seats (acsOpenStream)	20			
Reserved eKernel seats	10			
Reserved External seats	3			
IoRegister count (#devices)	1			
IoRegister available	1 (20 - 10 - 3 = 7)			
Seats required	14			
Guarding polling interval	60			
Retry interval	20			
Message delay	3			
General timeout	15			
Second ACK timeout	30			
DataPath delay	2			
Log path	C:\SOPHO Messenger@Net			
Log days	14	KeepAlive interval	60	0016

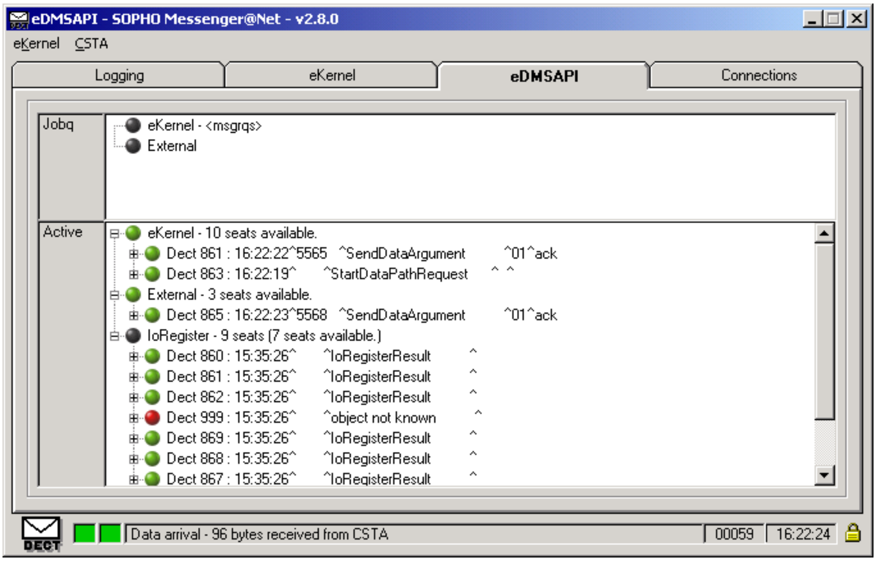
🟩 🟩 Data arrival - 127 bytes received from CSTA | 00011 | 13:53:35

In the left panel of the window shown in Figure 449, the configuration and state of the different socket connections is shown.

On the right side, the configuration parameters received (<cfgrpy>) from the eKernel are shown.

> ***Note:*** When the eDMSAPI functionality is not licenced, the eKernel sends the following configuration reply: <xml><cfgrpy><licence>NO LICENCE AVAILABLE</licence></cfgrpy></xml>. After sending this reply to eDMSAPI, the port through which the eDMSAPI is communicating is closed on the eKernel side.

Figure 450
eDMSAPI tab



```
Jobq
  eKernel - <msgrqs>
  External

Active
  eKernel - 10 seats available.
    Dect 861 : 16:22:22^5565  ^SendDataArgument      ^01^ack
    Dect 863 : 16:22:19^      ^StartDataPathRequest  ^ ^
  External - 3 seats available.
    Dect 865 : 16:22:23^5568  ^SendDataArgument      ^01^ack
  IoRegister - 9 seats (7 seats available.)
    Dect 860 : 15:35:26^      ^IoRegisterResult    ^
    Dect 861 : 15:35:26^      ^IoRegisterResult    ^
    Dect 862 : 15:35:26^      ^IoRegisterResult    ^
    Dect 999 : 15:35:26^      ^object not known    ^
    Dect 869 : 15:35:26^      ^IoRegisterResult    ^
    Dect 868 : 15:35:26^      ^IoRegisterResult    ^
    Dect 867 : 15:35:26^      ^IoRegisterResult    ^

Data arrival - 96 bytes received from CSTA    00059    16:22:24
```

Note that during call handling, the eDMSAPI tab shows an overview of current call states of each device. The window consists of two sections:

- The Jobq section contains two job queues. One jobq is for the request from eKernel, and the other is for requests from external clients.

  This area is used to temporarily store requests that are waiting to be executed. For instance, when all the data paths are in use, new requests must wait until resources are available.

  Requests can come from the eKernel (<msgrqs>) or from an external client (SNDNMSG|ID|DNR|MESSAGE<cr><lf> or SNDUMSG|ID|DNR|MESSAGE<cr><lf>)

  The functionality to receive requests from external clients is supported only for the DECT Messenger application (internal use only).

- The Active section contains active jobs. This area is used to handle currently active requests. There are three different sections in this area: the eKernel, the External and the IoRegister.

  The eKERNEL and External areas show the active extensions. Active requests wait for acknowledge from the CSTA Service. A normal message receives an ACK or NAK (StopDataPathRequest) reply. An urgent message receives an initial ACK or NAK. Urgent messages that receive ACK wait <Ack2TimeOut> seconds for a second ACK or a NAK.

CSTA_Service.exe

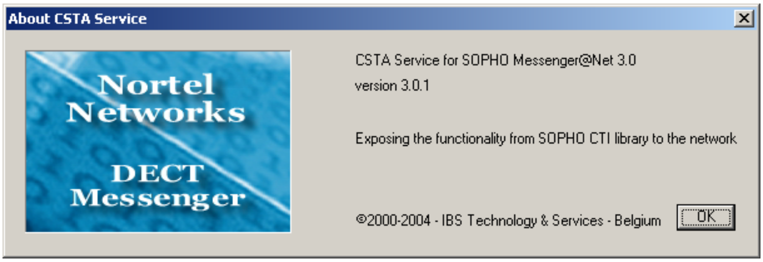
The CSTA_Service.exe communicates through CSTA.DLL with the SOPHO iS-3000 switch. The CSTA_Service.exe acts as TCP server for eDMSAPI. Communications to SOPHO iS-3000 is performed through CSTA.DLL, based upon Ethernet iS-Link CSTA interface on Ethernet. Details on these communications are beyond the scope of this document.

The CSTA_Service.exe has no user interface, but is visible as an icon in the system tray. Right-click on the icon to open a pop-up menu with the following three options:

- About CSTA Service

  Choose this menu item to display a message box with copyright information similar to the one shown in Figure 451.

Figure 451
Copyright information



About CSTA Service

CSTA Service for SOPHO Messenger@Net 3.0

version 3.0.1

Exposing the functionality from SOPHO CTI library to the network

©2000-2004 - IBS Technology & Services - Belgium

- Kill all clients

  Choose this menu item to disconnect all TCP connections, for example, the TCP/IP connection to eDMSAPI. This function must normally not be performed, unless instructed to do so by service support.

- End CSTA Service

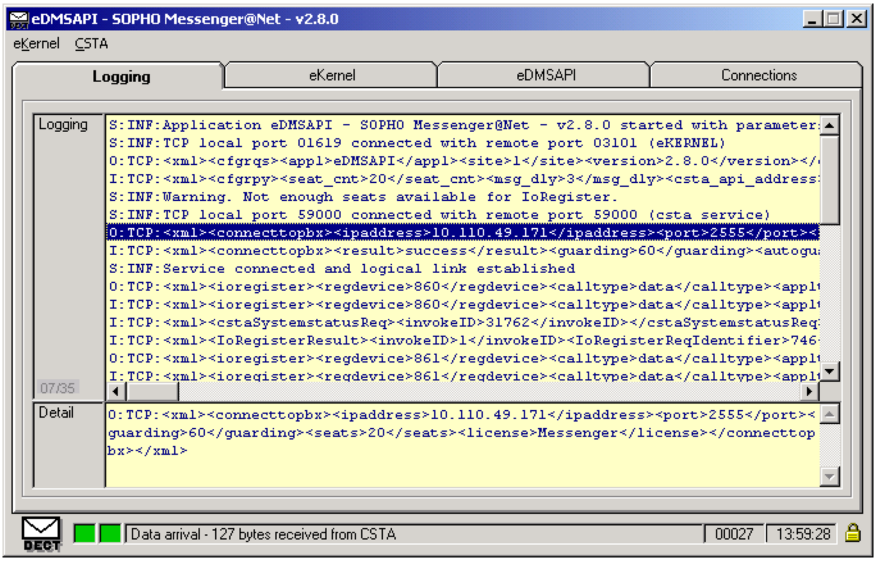
  Choose this menu item to close the CSTA_Service.exe program.

Logging

The eDMSAPI application provides logging to both the window and to logging files on disk.

You can view the on-screen log through the Logging tab:

Figure 452
Logging information



```
S:INF:Application eDMSAPI - SOPHO Messenger@Net - v2.8.0 started with parameter:
S:INF:TCP local port 01619 connected with remote port 03101 (eKERNEL)
O:TCP:<xml><cfgrqs><appl>eDMSAPI</appl><site>1</site><version>2.8.0</version></
I:TCP:<xml><cfgrpy><seat_cnt>20</seat_cnt><msg_dly>3</msg_dly><csta_api_address
S:INF:Warning. Not enough seats available for IoRegister.
S:INF:TCP local port 59000 connected with remote port 59000 (csta service)
O:TCP:<xml><connecttopbx><ipaddress>10.110.49.171</ipaddress><port>2555</port><
I:TCP:<xml><connecttopbx><result>success</result><guarding>60</guarding><autogu
S:INF:Service connected and logical link established
O:TCP:<xml><ioregister><regdevice>860</regdevice><calltype>data</calltype><appl
I:TCP:<xml><ioregister><regdevice>860</regdevice><calltype>data</calltype><appl
I:TCP:<xml><cstaSystemstatusReq><invokeID>31762</invokeID></cstaSystemstatusReq
I:TCP:<xml><IoRegisterResult><invokeID>1</invokeID><IoRegisterReqIdentifier>746
O:TCP:<xml><ioregister><regdevice>861</regdevice><calltype>data</calltype><appl
I:TCP:<xml><ioregister><regdevice>861</regdevice><calltype>data</calltype><appl
```

```
O:TCP:<xml><connecttopbx><ipaddress>10.110.49.171</ipaddress><port>2555</port><
guarding>60</guarding><seats>20</seats><license>Messenger</license></connecttop
bx></xml>
```

```
Data arrival - 127 bytes received from CSTA
```

Sample logging data is shown in Figure 453 on page 1135 and Figure 454 on page 1138.

Figure 453
Log example: Initialisation procedure

```
03/10/2002 13:58:52 - S:INF:Application eDMSAPI - SOPHO Messenger@Net -
v2.8.0 started with parameters /Site:1 /eKernel address:*LOCAL /eKernel
port:3101 /Log drive:C

03/10/2002 13:58:53 - S:INF:TCP local port 01619 connected with remote
port 03101 (eKERNEL)

03/10/2002 13:58:53 - O:TCP:<xml><cfgrqs><appl>eDMSAPI</appl><site>1</
site><version>2.8.0</version></cfgrqs></xml>

PBX type:DMC
28/06/2004 13:58:55 - I:TCP:<xml><cfgrpy><seat_cnt>20</
seat_cnt><msg_dly>3</msg_dly><csta_api_address>10.110.50.140</
csta_api_address><csta_api_port>59000</
csta_api_port><external_seat_cnt>3</
external_seat_cnt><external_port>2010</
external_port><csta_pbx_address>10.110.49.171</
csta_pbx_address><csta_pbx_port>2555</csta_pbx_port><csta_licence>Mes-
senger</csta_licence><guarding_intv>60</
guarding_intv><guarding_Retry_intv>20</
guarding_Retry_intv><eKernel_Seat_cnt>10</eKernel_Seat_cnt><GeneralTim-
eOut>15</GeneralTimeOut><Ack2TimeOut>30</Ack2TimeOut><DataPathDelay>2</
DataPathDelay><network>ETHERNET_DMC</network><pbxtype>DMC</pbx-
type><IoReg_cnt>9</IoReg_cnt><IoReg_0001>860</
IoReg_0001><IoReg_0002>861</IoReg_0002><IoReg_0003>862</
IoReg_0003><IoReg_0004>999</IoReg_0004><IoReg_0005>869</
IoReg_0005><IoReg_0006>868</IoReg_0006><IoReg_0007>867</
IoReg_0007><IoReg_0008>866</IoReg_0008><IoReg_0009>865</
IoReg_0009><log_path>C:\SOPHO Messenger@net</log_path><log_days>14</
log_days></cfgrpy></xml>

PBX type:DAP controller
28/06/2004 13:58:55 - I:TCP:<xml><cfgrpy><seat_cnt>20</
seat_cnt><msg_dly>3</msg_dly><csta_api_address>10.110.50.140</
csta_api_address><csta_api_port>59000</
csta_api_port><external_seat_cnt>3</
external_seat_cnt><external_port>2010</
external_port><csta_pbx_address>10.110.49.171</
```

continued on next page...

Log example: Initialisation procedure (continued)

```
csta_pbx_address><csta_pbx_port>28001</csta_pbx_port><csta_licence>Mes-
senger</csta_licence><guarding_intv>60</
guarding_intv><guarding_Retry_intv>20</
guarding_Retry_intv><eKernel_Seat_cnt>10</eKernel_Seat_cnt><GeneralTim-
eOut>15</GeneralTimeOut><Ack2TimeOut>30</Ack2TimeOut><DataPathDelay>2</
DataPathDelay><network> dasgif</network><pbxtype> DAP Controller</pbx-
type><IoReg_cnt>9</IoReg_cnt><IoReg_0001>860</
IoReg_0001><IoReg_0002>861</IoReg_0002><IoReg_0003>862</
IoReg_0003><IoReg_0004>999</IoReg_0004><IoReg_0005>869</
IoReg_0005><IoReg_0006>868</IoReg_0006><IoReg_0007>867</
IoReg_0007><IoReg_0008>866</IoReg_0008><IoReg_0009>865</
IoReg_0009><log_path>C:\SOPHO Messenger@net</log_path><log_days>14</
log_days></cfgrpy></xml>

PBX type:NORTEL
28/06/2004 13:58:55 - I:TCP:<xml><cfgrpy><seat_cnt>20</
seat_cnt><msg_dly>3</msg_dly><csta_api_address>10.110.50.140</
csta_api_address><csta_api_port>59000</
csta_api_port><external_seat_cnt>3</
external_seat_cnt><external_port>2010</
external_port><csta_pbx_address>10.110.49.171</
csta_pbx_address><csta_pbx_port>28001</csta_pbx_port><csta_licence>Mes-
senger</csta_licence><guarding_intv>60</
guarding_intv><guarding_Retry_intv>20</
guarding_Retry_intv><eKernel_Seat_cnt>10</eKernel_Seat_cnt><GeneralTim-
eOut>15</GeneralTimeOut><Ack2TimeOut>30</Ack2TimeOut><DataPathDelay>2</
DataPathDelay><network> dasgif</network><pbxtype>NORTEL</pbx-
type><IoReg_cnt>9</IoReg_cnt><IoReg_0001>860</
IoReg_0001><IoReg_0002>861</IoReg_0002><IoReg_0003>862</
IoReg_0003><IoReg_0004>999</IoReg_0004><IoReg_0005>869</
IoReg_0005><IoReg_0006>868</IoReg_0006><IoReg_0007>867</
IoReg_0007><IoReg_0008>866</IoReg_0008><IoReg_0009>865</
IoReg_0009><log_path>C:\SOPHO Messenger@net</log_path><log_days>14</
log_days></cfgrpy></xml>


03/10/2002 13:58:55 - S:INF:Warning. Not enough seats available for
IoRegister.
```

continued on next page...

Log example: Initialisation procedure (continued)

```
03/10/2002 13:59:00 - S:INF:TCP local port 59000 connected with remote
port 59000 (csta service)

PBX type:DMC
03/10/2002 13:59:00 - O:TCP:<xml><connecttopbx><ipad-
dress>10.110.49.171</ipaddress><port>2555</port><guarding>60</guard-
ing><seats>20</seats><licence>Messenger</licence>
<network>ETHERNET_DMC</network></connecttopbx></xml>

PBX type:DAP controller
03/10/2002 13:59:00 - O:TCP:<xml><connecttopbx><ipad-
dress>10.110.49.171</ipaddress><port>28001</port><guarding>60</guard-
ing><seats>20</seats><licence>Messenger</licence><network>dasgif</
network></connecttopbx></xml>

PBX type:NORTEL
03/10/2002 13:59:00 - O:TCP:<xml><connecttopbx><ipad-
dress>10.110.49.171</ipaddress><port>28001</port><guarding>60</guard-
ing><seats>20</seats><licence>Messenger</licence><network>dasgif</
network></connecttopbx></xml>


03/10/2002 13:59:00 - I:TCP:<xml><connecttopbx><result>success</re-
sult><guarding>60</guarding><autoguarding>1</autoguarding></connecttop-
bx></xml>

03/10/2002 13:59:00 - S:INF:Service connected and logical link estab-
lished

03/10/2002 13:59:00 - O:TCP:<xml><ioregister><regdevice>860</regde-
vice><calltype>data</calltype><appltype>messaging</appltype></ioregis-
ter></xml>

03/10/2002 13:59:00 - I:TCP:<xml><IoRegisterResult><invokeID>1</in-
vokeID><IoRegisterReqIdentifier>746</IoRegisterReqIdentifier></IORegis-
terResult></xml>
03/10/2002 13:59:00 - I:TCP:<xml><cstaSystemstatusReq><invokeID>31762</
invokeID></cstaSystemstatusReq></xml> (Guarding)
>
</xml>
```

Figure 454
Log example: Message handling

```
03/10/2002 12:08:57 - I:TCP:<xml><msgrqs><id>00774</id> <ext>861</ext>
<ext_prty>6</ext_prty><pag_01>Guarding AM TELEVIC             </
pag_01><prty_01>N</prty_01><pag_more>N</pag_more><format>16^16^0^5^2</
format>
</msgrqs></xml>

PBX type: DMC and DAP controller: NORMAL and/or URGENT messages
03/10/2002 12:08:57 - O:TCP:<xml><startdatapathdevice><deviceID>861</de-
viceID><pathtype>text</pathtype>
<dirtype>bi</dirtype><homelocationnumber>1<homelocationnumber> </start-
datapathdevice></xml>

PBX type: NORTEL: NORMAL and/or URGENT messages
03/10/2002 12:08:57 - O:TCP:<xml><startdatapathdevice><deviceID>861</de-
viceID><pathtype>text</pathtype>
<dirtype>bi</dirtype><homelocationnumber>0<homelocationnumber> </start-
datapathdevice></xml>

PBX type: DMC and DAP controller: also Emergency messages
03/10/2002 12:08:57 - O:TCP:<xml><startdatapathdevice><deviceID>861</de-
viceID><pathtype>text</pathtype>
<dirtype>bi</dirtype><callcategory>emergency</callcategory> <homeloca-
tionnumber>1<homelocationnumber></startdatapathdevice></xml>

PBX type: NORTEL: Emergency messages
03/10/2002 12:08:57 - O:TCP:<xml><startdatapathdevice><deviceID>861</de-
viceID><pathtype>text</pathtype>
<dirtype>bi</dirtype><callcategory>emergency</callcategory><homeloca-
tionnumber> 0<homelocationnumber></startdatapathdevice></xml>

03/10/2002 12:08:58 - I:TCP:<xml><StartDataPathResult><IoCrossRefIdenti-
fier>5697</IoCrossRefIdentifier>
<invokeID>58</invokeID></StartDataPathResult></xml>

03/10/2002 12:08:58 - O:TCP:<xml><senddata><iocrossrefid>5697</iocross-
refid>
<Text>Guarding AM TELEVIC            01/01</Text><originator>pbx</orig-
inator>
```

continued on next page...

Log example: Message handling (continued)

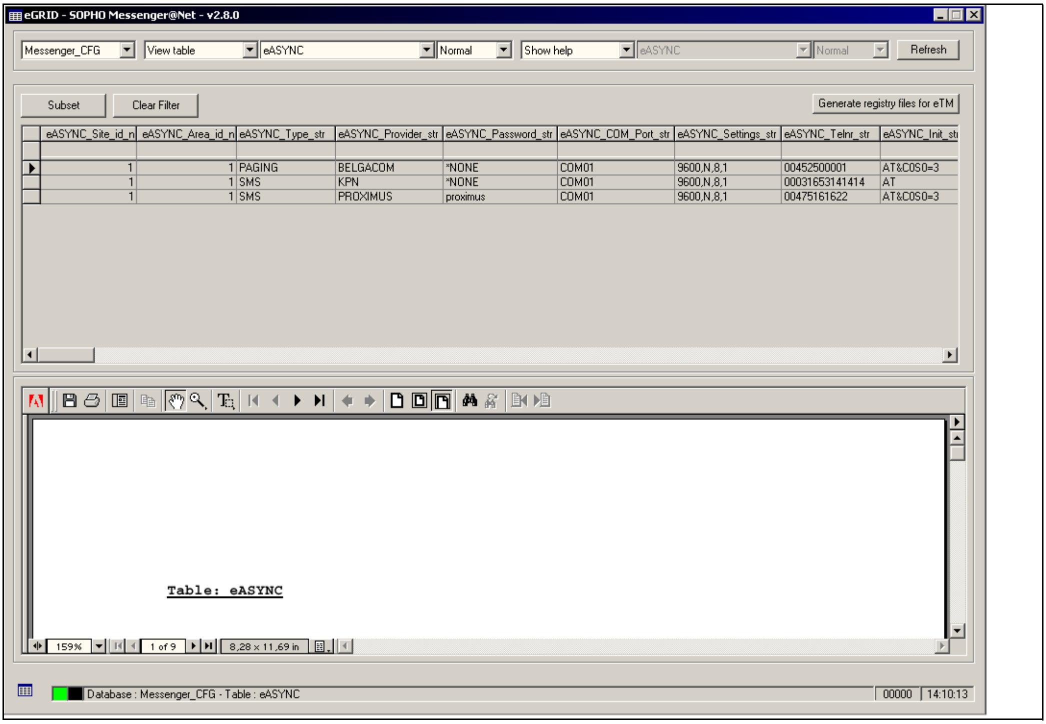
```
<msgtype>normal</msgtype><direction>outbound</direction></senddata></
xml>

03/10/2002 12:08:58 - I:TCP:<xml><SendDataResult><invokeID>59</in-
vokeID></SendDataResult></xml>

03/10/2002 12:09:00 - I:TCP:<xml><SendDataArgument><invokeID>31206</in-
vokeID>
<ioCrossRefIdentifier>5697</ioCrossRefIdentifier><Provider>1</Provider>
<Text><ack></Text></SendDataArgument></xml>

03/10/2002 12:09:00 - O:TCP:<xml><senddataresult><invokeID>31206</in-
vokeID></senddataresult></xml>

03/10/2002 12:09:00 - O:TCP:<xml><stopdatapath><iocrossrefid>5697</
iocrossrefid>
<originator>pbx</originator></stopdatapath></xml>

03/10/2002 12:09:00 - I:TCP:<xml><stopdatapath><iocrossrefid>5697</
iocrossrefid>
<originator>pbx</originator></stopdatapath><invokeID>61</invokeID></
xml>

03/10/2002 12:09:06 - I:TCP:<xml><StopDataPathResult><InvokeID>61</In-
vokeID>nodata
</StopDataPathResult></xml>
```

Module – eGRID

The eGRID application gives you a view of the different tables in the databases.

The eGRID.exe application can be started without command line parameters. At start-up, the window in Figure 455 is shown:

Figure 455
eGRID start-up window



eASYNC_Site_id_n	eASYNC_Area_id_n	eASYNC_Type_str	eASYNC_Provider_str	eASYNC_Password_str	eASYNC_COM_Port_str	eASYNC_Settings_str	eASYNC_Telnr_str	eASYNC_Init_str
1	1	PAGING	BELGACOM	*NONE	COM01	9600,N,8,1	00452500001	AT&C0S0=3
1	1	SMS	KPN	*NONE	COM01	9600,N,8,1	00031653141414	AT
1	1	SMS	PROXIMUS	proximus	COM01	9600,N,8,1	00475161622	AT&C0S0=3

Database : Messenger_CFG - Table : eASYNC 00000 14:10:13

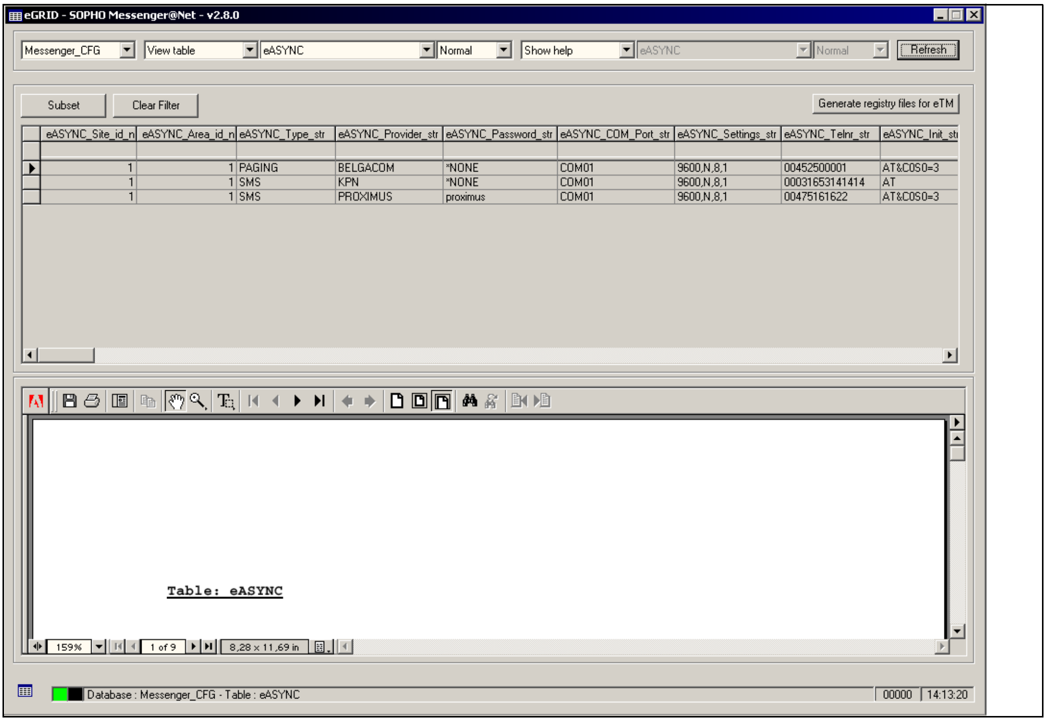
Seven drop-down lists are available at the top of the window. From left to right, the functions of these drop-down lists are as follows:

- Use the first drop-down list, on the far left, to select the Messenger_CFG database or the Messenger_DATA database.
- Use the second drop-down list to select one of the following:
  - — View table allows you to perform inquiry functions
  - — Edit table allows you to perform maintenance
  - — Export to CSV allows you to export a table to a comma separated file
  - — Export to HTML allows you to export to an HTML file

- Use the third drop-down list to select a table. The available tables are retrieved automatically from the database object.
- Use the fourth drop-down list to control the GRID view as follows:
  - Normal uses default view
  - Inverted uses a rotated view
  - Group allows grouping records through drag and drop
- The fifth drop-down list offers the following choices:
  - None uses a full-screen interface for one table
  - Show help splits the window interface in two halves: the top half is used to access the table, the bottom half is used to show the related PDF-file help information
  - View another table allows you to select a second table, and splits the window in two; the upper half is used to access the first table, the lower half is used to access the second table
- The sixth drop-down list is available only if a View another table is specified. Use this list to select the second table.
- Use the seventh drop-down list, on the far right, to modify the view of the second table.
  - Normal uses default view
  - Inverted uses a rotated view
  - Group allows grouping records through drag and drop

The example in Figure 456 on page 1144 shows the Show help mode:

Figure 456
eGRID with Show help mode

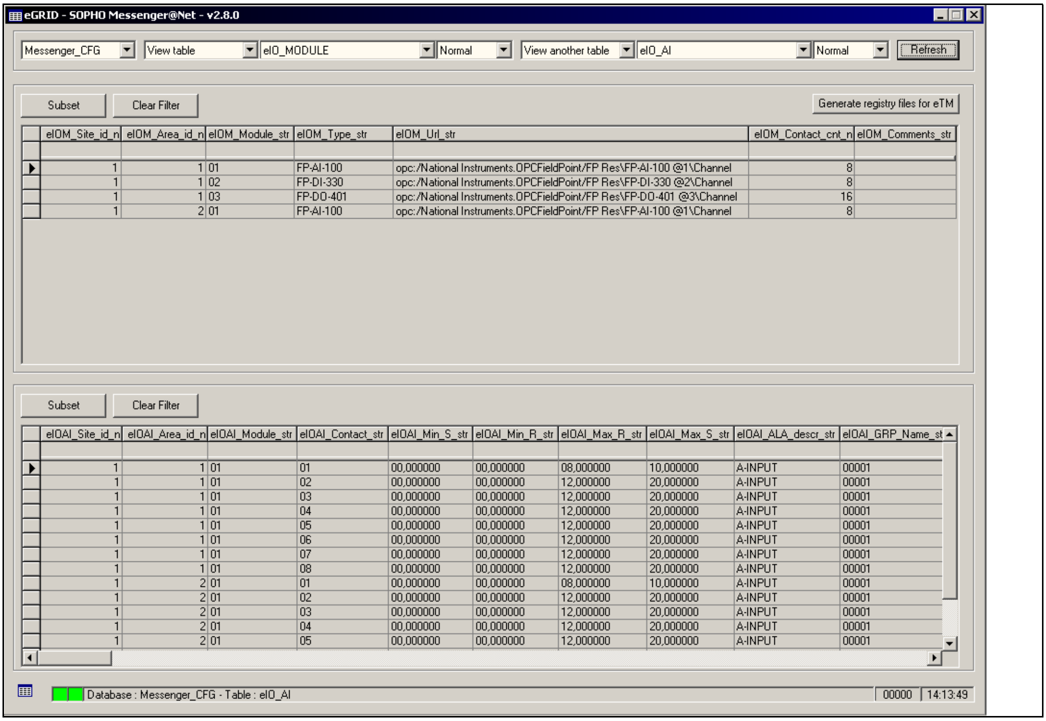


eASYNC_Site_id_n	eASYNC_Area_id_n	eASYNC_Type_str	eASYNC_Provider_str	eASYNC_Password_str	eASYNC_COM_Port_str	eASYNC_Settings_str	eASYNC_Telnr_str	eASYNC_Init_str
1	1	PAGING	BELGACOM	*NONE	COM01	9600,N,8,1	00452500001	AT&C0S0=3
1	1	SMS	KPN	*NONE	COM01	9600,N,8,1	00031653141414	AT
1	1	SMS	PROXIMUS	proximus	COM01	9600,N,8,1	00475161622	AT&C0S0=3

Table: eASYNC

Database : Messenger_CFG - Table : eASYNC 00000 14:13:20

Figure 457
eGRID with View another table mode



eGRID - SOPHO Messenger@Net - v2.8.0

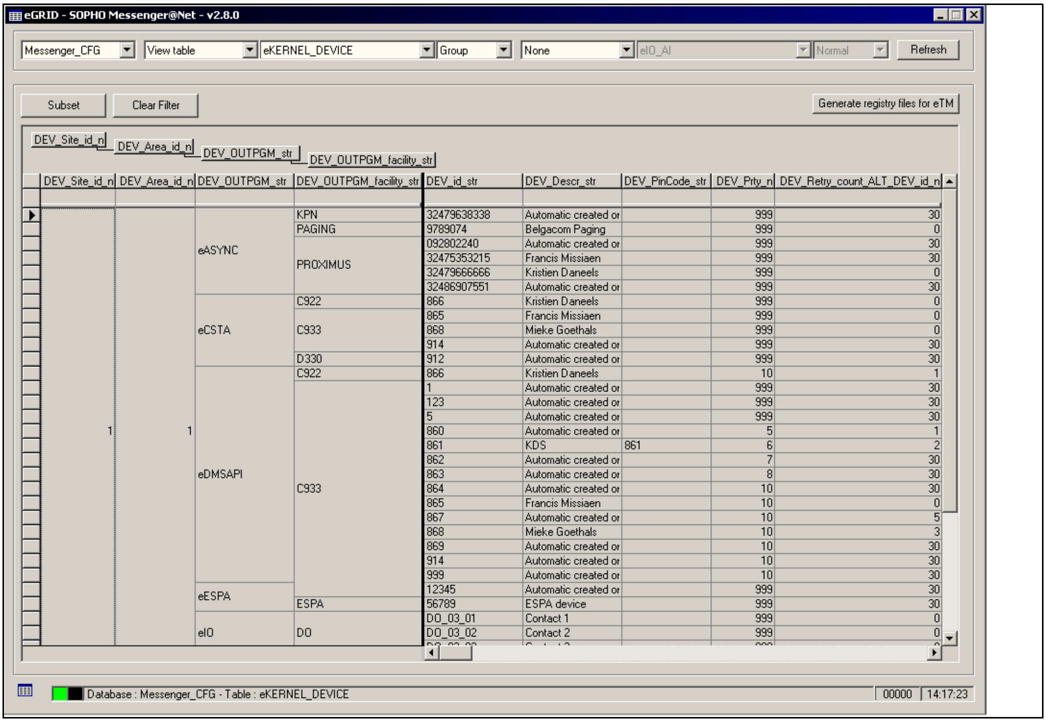
Messenger_CFG | View table | eIO_MODULE | Normal | View another table | eIO_AI | Normal | Refresh

eIOM_Site_id_n	eIOM_Area_id_n	eIOM_Module_str	eIOM_Type_str	eIOM_Url_str	eIOM_Contact_cnt_n	eIOM_Comments_str
1	1	01	FP-AI-100	opc:/National Instruments.OPCFieldPoint/FP Res\FP-AI-100 @1\Channel	8	
1	1	02	FP-DI-330	opc:/National Instruments.OPCFieldPoint/FP Res\FP-DI-330 @2\Channel	8	
1	1	03	FP-DO-401	opc:/National Instruments.OPCFieldPoint/FP Res\FP-DO-401 @3\Channel	16	
1	2	01	FP-AI-100	opc:/National Instruments.OPCFieldPoint/FP Res\FP-AI-100 @1\Channel	8	

eIOAI_Site_id_n	eIOAI_Area_id_n	eIOAI_Module_str	eIOAI_Contact_str	eIOAI_Min_S_str	eIOAI_Min_R_str	eIOAI_Max_R_str	eIOAI_Max_S_str	eIOAI_ALA_descr_str	eIOAI_GRP_Name_st
1	1	01	01	00,000000	00,000000	08,000000	10,000000	A-INPUT	00001
1	1	01	02	00,000000	00,000000	12,000000	20,000000	A-INPUT	00001
1	1	01	03	00,000000	00,000000	12,000000	20,000000	A-INPUT	00001
1	1	01	04	00,000000	00,000000	12,000000	20,000000	A-INPUT	00001
1	1	01	05	00,000000	00,000000	12,000000	20,000000	A-INPUT	00001
1	1	01	06	00,000000	00,000000	12,000000	20,000000	A-INPUT	00001
1	1	01	07	00,000000	00,000000	12,000000	20,000000	A-INPUT	00001
1	1	01	08	00,000000	00,000000	12,000000	20,000000	A-INPUT	00001
1	2	01	01	00,000000	00,000000	08,000000	10,000000	A-INPUT	00001
1	2	01	02	00,000000	00,000000	12,000000	20,000000	A-INPUT	00001
1	2	01	03	00,000000	00,000000	12,000000	20,000000	A-INPUT	00001
1	2	01	04	00,000000	00,000000	12,000000	20,000000	A-INPUT	00001
1	2	01	05	00,000000	00,000000	12,000000	20,000000	A-INPUT	00001

Database : Messenger_CFG - Table : eIO_AI | 00000 | 14:13:49

Figure 458
eGRID grouping functions



eGRID - SOPHO Messenger@Net - v2.8.0

Messenger_CFG | View table | eKERNEL_DEVICE | Group | None | eIO_AI | Normal | Refresh

DEV_Site_id_n	DEV_Area_id_n	DEV_OUTPGM_str	DEV_OUTPGM_facility_str	DEV_id_str	DEV_Descr_str	DEV_PinCode_str	DEV_Prty_n	DEV_Retry_count_ALT_DEV_id_n
1	1	eASYNC	KPN	32479638338	Automatic created or		999	30
			PAGING	9789074	Belgacom Paging		999	0
			PROXIMUS	092802240	Automatic created or		999	30
				32475353215	Francis Missiaen		999	30
				32479666666	Kristien Daneels		999	0
				32486907551	Automatic created or		999	30
		eCSTA	C922	866	Kristien Daneels		999	0
			C933	865	Francis Missiaen		999	0
				868	Mieke Goethals		999	0
				914	Automatic created or		999	30
			D330	912	Automatic created or		999	30
		eDMSAPI	C922	866	Kristien Daneels		10	1
			C933	1	Automatic created or		999	30
				123	Automatic created or		999	30
				5	Automatic created or		999	30
				860	Automatic created or		5	1
				861	KDS	861	6	2
				862	Automatic created or		7	30
				863	Automatic created or		8	30
				864	Automatic created or		10	30
				865	Francis Missiaen		10	0
				867	Automatic created or		10	5
				868	Mieke Goethals		10	3
				869	Automatic created or		10	30
				914	Automatic created or		10	30
				999	Automatic created or		10	30
		eESPA		12345	Automatic created or		999	30
			ESPA	56789	ESPA device		999	30
		eIO	DO	DO_03_01	Contact 1		999	0
				DO_03_02	Contact 2		999	0

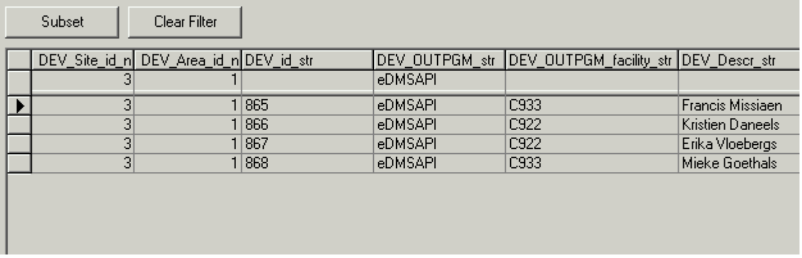
Database : Messenger_CFG - Table : eKERNEL_DEVICE | 00000 | 14:17:23

Because eGRID is the preferred access method for maintenance, an extra functionality is implemented to optimize flexibility. This functionality is referred to as Data Filtering and is handled through the command buttons Subset, Clear filter, and an entry field between the column heading and the first row.

Figure 459 illustrates the usage of Data Filtering. This example shows a subset of the devices of site 3, area 1a, and output program eDMSAPI in the table eKERNEL_DEVICE. You can clear the subset criteria with the Clear Filter button, by selecting another table, or by selecting Refresh.

> ***Note:*** Incomplete information is displayed when you use Data Filtering, because only the records with matching criteria are shown.

Figure 459
eGRID Data Filtering



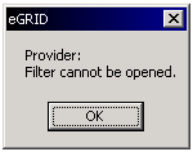
DEV_Site_id_n	DEV_Area_id_n	DEV_id_str	DEV_OUTPGM_str	DEV_OUTPGM_facility_str	DEV_Descr_str
3	1		eDMSAPI		
3	1	865	eDMSAPI	C933	Francis Missiaen
3	1	866	eDMSAPI	C922	Kristien Daneels
3	1	867	eDMSAPI	C922	Erika Vloebergs
3	1	868	eDMSAPI	C933	Mieke Goethals

Look at the column header to find out what data type the field has. Because the filtering function is based upon SQL instructions, you must specify subset data that results in valid SQL grammar:

- Selecting partial data (omitting training characters) is valid only for string fields with the extension _str. For example DEV_OUTPGM_str can be part of a subset with e, eD, eDM, and so on. Boolean fields with extension _b and numeric fields with extension _n cannot be part of a subset with partial values and must be fully qualified.
- You must not specify special characters that can be interpreted by the SQL processor.
- String values can also be subset with syntax %EN, which select *SEND. Specify % to accept generic leading characters.

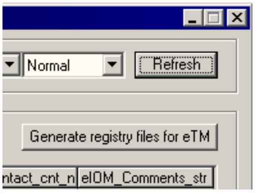
Specifying invalid filter criteria can result in errors such as the one shown in Figure 460.

Figure 460
Invalid filter criteria error



Provider:
Filter cannot be opened.

Figure 461
Accessing Generate registry files for eTM



Click **Generate registry files for eTM** to export the configuration for the module eTM, also referred to as Task Manager. Refer to “Module – eTM” on page 1205 for more information on this procedure.

IMPORTANT!

Ensure the eGRID module is not made available for unauthorized access. Remove the shortcut where applicable.

The eGRID module provides direct access to the tables in the database. There is no password protection on this module.

Module – eIO

Overview

The eIO module is a stand-alone application that communicates with eKERNEL. The module is capable of controlling and measuring Distributed I/O peripherals of National Instruments. eIO offers support for analogue input, digital input and digital output.

See “Install PC – Step 3 – National Instruments” on page 889 for a detailed explanation of installation and configurations issues of the modules, and the supporting Measurement Studio components (FieldPoint Explorer and OPC Server).

Prior to starting eIO, Nortel recommends that you review the documentation “Table: eIO_MODULE” on page 1367, “Table: eIO_AI” on page 1371, “Table: eIO_DI” on page 1381, and “Table: eIO_DO” on page 1387.

All these documents contain important information that is required to understand and configure the eIO module. To avoid duplicate information, the concepts are not repeated in this chapter.

Start-up

You must start the eIO application by means of a shortcut that uses the syntax described in Figure 462 on page 1150.

Figure 462
Parameters in the shortcut for eIO

```
"C:\SOPHO Messenger@Net\Exe\eIO.exe"
/Site:3
/eKernel address:*LOCAL
/eKernel port:3108
/Log drive:C
```

The following parameters are required:

- **Site**

  Defines the site identifier and is used by eKERNEL to verify the identifier with the eKERNEL_TCPCLIENT and eKERNEL_INPGM settings. This identifier is also required so that eKERNEL can respond with the appropriate configuration settings.

- **eKernel address**

  Defines the IP address of eKERNEL. The special value *LOCAL can be specified to refer to the same address as the system where eIO resides. In a single-computer environment the *LOCAL value is usually specified, because eKERNEL and eIO both share the same network adapter. When eIO is running on a different computer, the IP address of the eKERNEL must be specified.

- **eKernel port**

  Refers to the port number eKERNEL listens to for that specific eIO instance. This port is defined in the eKERNEL_TCPCLIENT table.

- **Log drive**

  Specifies the drive letter where logging files must be stored.

When all parameters are correctly specified, the eIO contacts the eKERNEL application, producing the log information shown in Figure 463 on page 1151.

Figure 463
Logging information for eIO

```
25/10/2001 10:41:35 -
S:INF:Application eIO - SOPHO Messenger@Net - v2.0.6 started with param-
eters /Site:3 /eKernel address:*LOCAL /eKernel port:3108 /Log drive:C

25/10/2001 10:41:36 -
S:INF:TCP local port 01183 connected with remote port 03108 (eKERNEL)
25/10/2001 10:41:36 -
```

Once connected to eKERNEL, the eIO module requests its configuration. This is performed through a configuration request. The eKERNEL fetches the configuration from the IO_MODULE, eIO_AI, eIO_DI and eIO_DO tables and responds with all relevant parameters that are needed for eIO to continue processing. Figure 464 on page 1152 shows the configuration request and the response eKERNEL sends back.

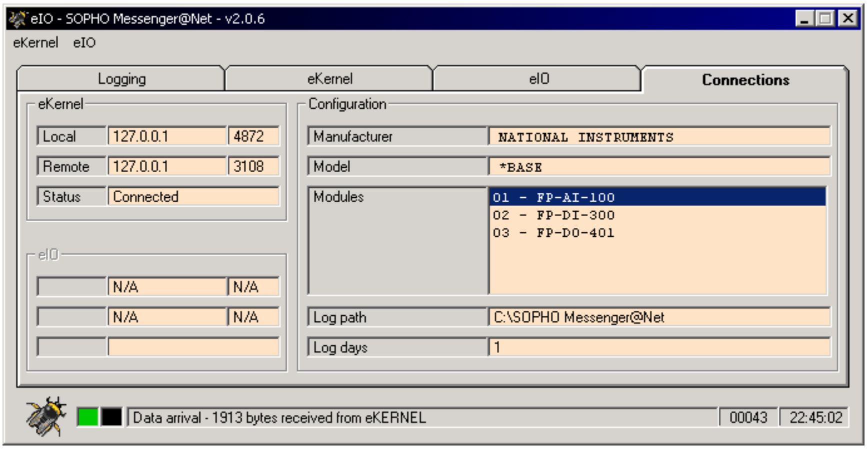
Figure 464
eIO configuration request and response

```
<xml>
<cfgrqs>
<appl>eIO</appl>
<site>3</site>
</cfgrqs>
</xml>
```

```
<xml>
<cfgrpy>
<manufacturer>NATIONAL INSTRUMENTS</manufacturer>
<model>*BASE</model>
<mod_cnt>3</mod_cnt>
<mod_01>FP-AI-100</mod_01>
<url_01>opc:/National Instruments.OPCFieldPoint/FP Res\FP-AI-100
@1\Channel</url_01>
<cnt_01>8</cnt_01>
<mod_02>FP-DI-300</mod_02>
<url_02>opc:/National Instruments.OPCFieldPoint/FP Res\FP-DI-330
@2\Channel</url_02>
<cnt_02>8</cnt_02>
<mod_03>FP-DO-401</mod_03>
<url_03>opc:/National Instruments.OPCFieldPoint/FP Res\FP-DO-401
@3\Channel</url_03>
<cnt_03>16</cnt_03>
<ai_01_01_min_s>00,000000</ai_01_01_min_s>
<ai_01_01_min_r>00,000000</ai_01_01_min_r>
<ai_01_01_max_r>12,000000</ai_01_01_max_r>
<ai_01_01_max_s>20,000000</ai_01_01_max_s>
:
:
<ai_01_08_min_s>00,000000</ai_01_08_min_s>
<ai_01_08_min_r>00,000000</ai_01_08_min_r>
<ai_01_08_max_r>12,000000</ai_01_08_max_r>
<ai_01_08_max_s>20,000000</ai_01_08_max_s>
<log_path>C:\SOPHO Messenger@net</log_path>
<log_days>1</log_days>
</cfgrpy>
</xml>
```

When the configuration is received, the eIO updates the configuration information on the **Connections** tab, as shown in Figure 465. During this time, the eIO is temporarily less responsive to user input. This is due to the large number of OPC Server connections that take place at start-up time.

Figure 465
eIO Connections update



eKernel

Local 127.0.0.1 4872
Remote 127.0.0.1 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-300
03 - FP-DO-401
Log path C:\SOPHO Messenger@Net
Log days 1

Data arrival - 1913 bytes received from eKERNEL 00043 22:45:02

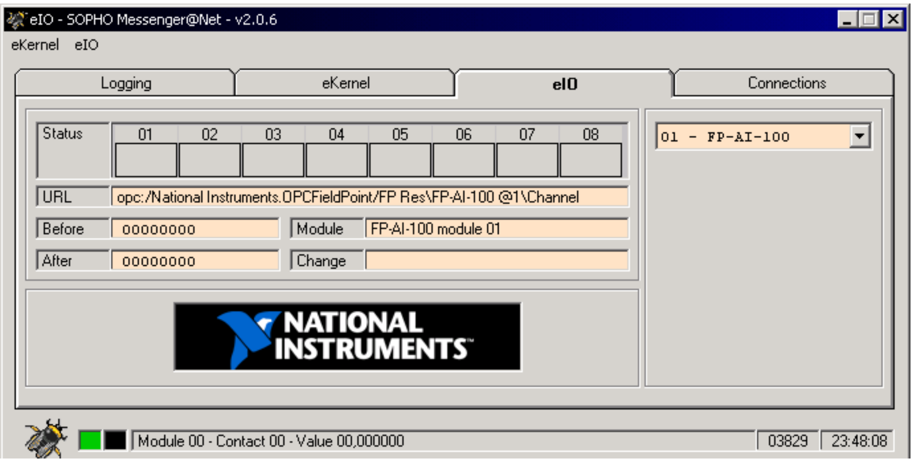
eIO Modules

Select the eIO tab to see a panel with details of the available modules and contacts. Use the drop-down list at the right-hand side of the window to select the module to view.

Analogue input

When you select an analogue input module (FP-AI-100), a window similar to the one in Figure 466 is shown. For each module a graphical display shows the available contacts. The analogue input also shows the analogue levels.

Figure 466
eIO analogue input modules



URL: opc:/National Instruments.OPCFieldPoint/FP Res\FP-AI-100 @1\Channel

Before: 00000000

Module: FP-AI-100 module 01

After: 00000000

Change:

01 - FP-AI-100

Module 00 - Contact 00 - Value 00,000000 | 03829 | 23:48:08

For each module, the URL is shown, and the module identifier. When you hold the mouse pointer over the status area of a contact, detailed information is shown. An example of the information provided is as follows:

```
Min (set: 02,000000 - reset: 08,000000)
Max (reset: 14,000000 - set: 20,000000)
```

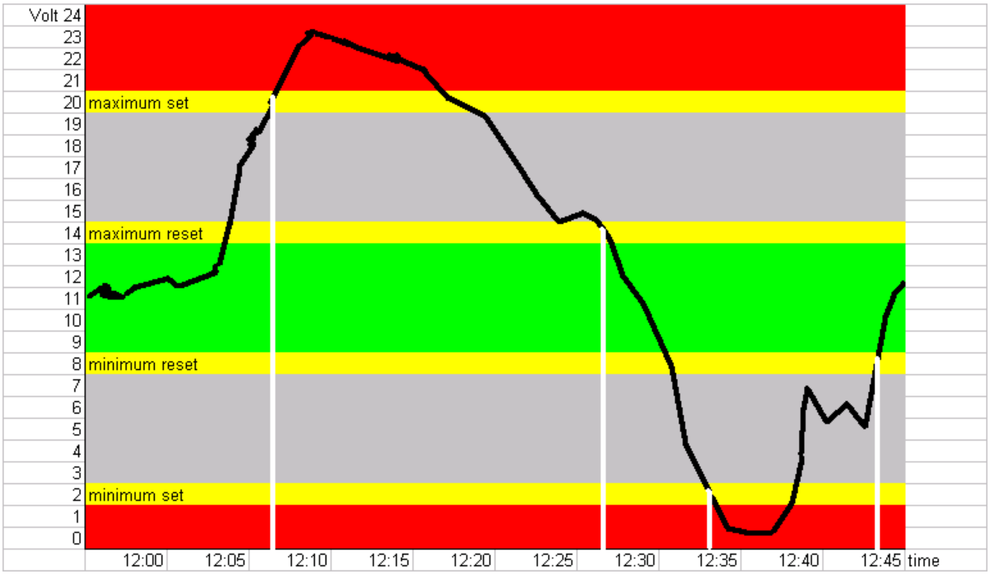
The chart shown in Figure 467 on page 1155 explains the behaviour of these settings. The chart shows the voltage levels between 0 and 24 V on the Y-axis, and the time between 12:00 and 12:45 on the X-axis. There are four different configuration values, which are indicated in yellow. These values are retrieved from the eIO_AI table and match the environment in FieldPoint Explorer.

On the chart, the analogue measured values are shown in black. The green area is the idle zone, the red areas are alarm zones, and the grey areas are transition zones.

- When the measured value reaches 20,00000 V, a MAX ALARM condition is set. This is shown in the chart on 12:07.
- When the measured value drops to 14,00000 B, the MAX ALARM condition is reset. This is shown in the chart on 12:27.

- When the measured value drops to 02,00000 B, the MIN ALARM condition is reset. This is shown in the chart on 12:37.
- When the measured value reaches 08,00000 V, a MIN ALARM condition is set. This is shown in the chart on 12:45.

Figure 467
Analogue input ranges



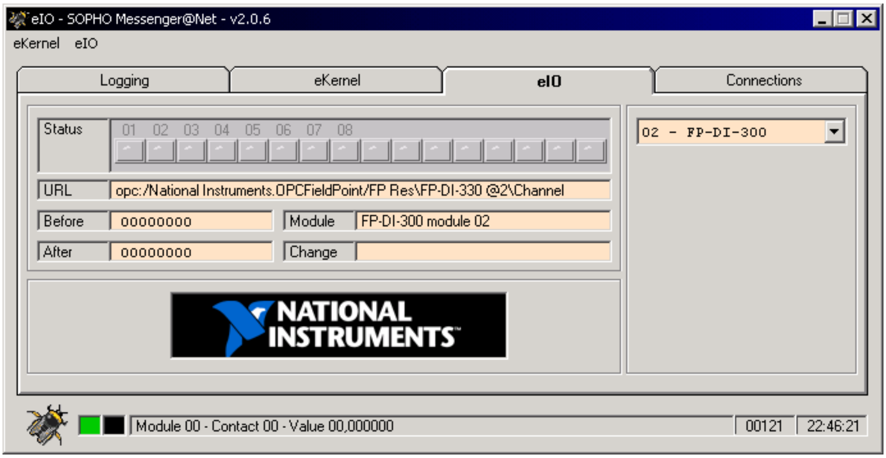
Note: Alarm values are given in pairs. Both maximum and minimum alarms are set and reset with different values. This was implemented to prevent continuous switching between set and reset when measured values are in the neighbourhood of alarm values.

- Left-click in the status zone of an analogue contact to display the currently measured value.
- If a measured value generates a maximum (+) or minimum (-) alarm boundary, the Change area of the interface is updated.

Digital input (discrete input)

When you select a digital input module (FP-DI-300, FP-DI-301 or FP-DI-330), a window opens similar to the one shown in Figure 468. For each module a graphical display shows the available contacts. A grey rectangle indicates a discrete input value is Off, a green rectangle indicates a discrete input value is On.

Figure 468
Digital Input module information



Status: 01 02 03 04 05 06 07 08

URL: opc:/National Instruments.OPCFieldPoint/FP Res\FP-DI-330 @2\Channel

Before: 00000000

Module: FP-DI-300 module 02

After: 00000000

Change:

02 – FP-DI-300

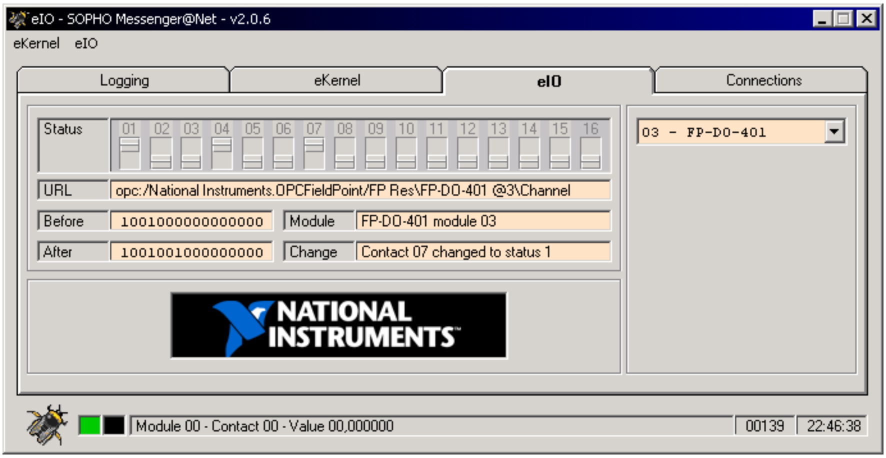
Module 00 - Contact 00 - Value 00,000000 | 00121 | 22:46:21

Note: When the value of a contact changes from Off to On or from On to Off, the Before and After fields are updated with the status of the contact before the change occurred and the status of the contact after the change occurred. The Change field is also updated with the new value.

Digital output (discrete output)

When you select a digital output module (FP-DO-401), a window opens similar to the one shown in Figure 469 on page 1157. For each module a graphical display shows the available output contacts. A grey switch directed to the bottom indicates a discrete output value is Off; a grey switch directed to the upwards position indicates a discrete output value is On. In Figure 469, contacts 01 and 04 and 07 are On; all others are Off.

Figure 469
Digital Output module information



URL: opc:/National Instruments.OPCFieldPoint/FP Res\FP-DO-401 @3\Channel

Before: 1001000000000000

Module: FP-DO-401 module 03

After: 1001001000000000

Change: Contact 07 changed to status 1

03 - FP-DO-401

Module 00 - Contact 00 - Value 00,000000 | 00139 | 22:46:38

Note 1: When the value of a contact changes from Off to On or from On to Off, the Before and After fields are updated with the status of the contact before the change occurred and the status of the contact after the change occurred. The Change field is also updated with the new value.

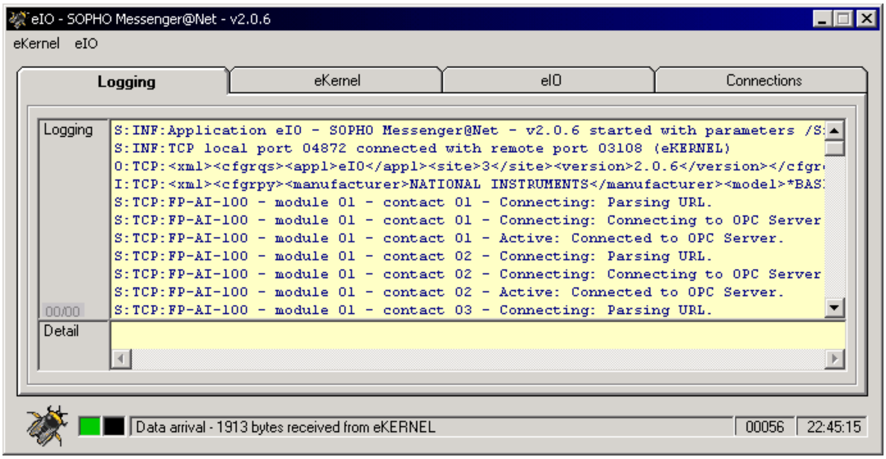
Note 2: You can also change the status of the contacts to On or Off by using the mouse to drag the switch to the On or Off position. This must be carried out only while installing or testing. In most environments, the eKERNEL application is responsible to activate or deactivate the alarm condition of the discrete outputs. You can however manually reset a status of a contact, for example, if manual intervention is required.

Logging

The eIO module provides logging facilities, both on-screen and on log files on disk.

The on-screen logs are visible through the Logging tab, as shown in Figure 470 on page 1158.

Figure 470
eIO logging



```
S:INF:Application eIO - SOPHO Messenger@Net - v2.0.6 started with parameters /S:
S:INF:TCP local port 04872 connected with remote port 03108 (eKERNEL)
O:TCP:<xml><cfgrqs><appl>eIO</appl><site>3</site><version>2.0.6</version></cfgr
I:TCP:<xml><cfgrpy><manufacturer>NATIONAL INSTRUMENTS</manufacturer><model>*BAS
S:TCP:FP-AI-100 - module 01 - contact 01 - Connecting: Parsing URL.
S:TCP:FP-AI-100 - module 01 - contact 01 - Connecting: Connecting to OPC Server
S:TCP:FP-AI-100 - module 01 - contact 01 - Active: Connected to OPC Server.
S:TCP:FP-AI-100 - module 01 - contact 02 - Connecting: Parsing URL.
S:TCP:FP-AI-100 - module 01 - contact 02 - Connecting: Connecting to OPC Server
S:TCP:FP-AI-100 - module 01 - contact 02 - Active: Connected to OPC Server.
S:TCP:FP-AI-100 - module 01 - contact 03 - Connecting: Parsing URL.
```

Data arrival - 1913 bytes received from eKERNEL

The log files on disk contain the same information as shown on-screen. On the next few pages, Figure 470 through Figure 475 show examples of log information saved on disk during different steps of eIO setup and use.

Figure 471
Log example: initialisation procedure

```
25/10/2001 10:41:35 -
S:INF:Application eIO - SOPHO Messenger@Net - v2.0.6 started with param-
eters /Site:3 /eKernel address:*LOCAL /eKernel port:3108 /Log drive:C

25/10/2001 10:41:36 -
S:INF:TCP local port 01183 connected with remote port 03108 (eKERNEL)
25/10/2001 10:41:36 -
```

Figure 472
Log example: Configuration procedure

```
O:TCP:<xml><cfgrqs><appl>eIO</appl><site>3</site><version>2.0.6</ver-
sion></cfgrqs></xml>

25/10/2001 10:41:37 -
I:TCP:<xml><cfgrpy><manufacturer>NATIONAL INSTRUMENTS</manufacturer>
<model>*BASE</model><mod_cnt>3</mod_cnt><mod_01>FP-AI-100</mod_01>
<url_01>opc:/National Instruments.OPCFieldPoint/FP Res\FP-AI-100
@1\Channel</url_01><cnt_01>8</cnt_01><mod_02>FP-DI-300</mod_02>
<url_02>opc:/National Instruments.OPCFieldPoint/FP Res\FP-DI-330
@2\Channel</url_02><cnt_02>8</cnt_02><mod_03>FP-DO-401</mod_03>
<url_03>opc:/National Instruments.OPCFieldPoint/FP Res\FP-DO-401
@3\Channel</url_03><cnt_03>16</cnt_03><ai_01_01_min_s>00,000000</
ai_01_01_min_s><ai_01_01_min_r>00,000000</
ai_01_01_min_r><ai_01_01_max_r>12,000000</
ai_01_01_max_r><ai_01_01_max_s>20,000000</
ai_01_01_max_s><ai_01_02_min_s>00,000000</
ai_01_02_min_s><ai_01_02_min_r>00,000000</
ai_01_02_min_r><ai_01_02_max_r>12,000000</
ai_01_02_max_r><ai_01_02_max_s>20,000000</
ai_01_02_max_s><ai_01_03_min_s>00,000000</
ai_01_03_min_s><ai_01_03_min_r>00,000000</
ai_01_03_min_r><ai_01_03_max_r>12,000000</
ai_01_03_max_r><ai_01_03_max_s>20,000000</
ai_01_03_max_s><ai_01_04_min_s>00,000000</
ai_01_04_min_s><ai_01_04_min_r>00,000000</
ai_01_04_min_r><ai_01_04_max_r>12,000000</
ai_01_04_max_r><ai_01_04_max_s>20,000000</
ai_01_04_max_s><ai_01_05_min_s>00,000000</
ai_01_05_min_s><ai_01_05_min_r>00,000000</
ai_01_05_min_r><ai_01_05_max_r>12,000000</
ai_01_05_max_r><ai_01_05_max_s>20,000000</
ai_01_05_max_s><ai_01_06_min_s>00,000000</
ai_01_06_min_s><ai_01_06_min_r>00,000000</
ai_01_06_min_r><ai_01_06_max_r>12,000000</
ai_01_06_max_r><ai_01_06_max_s>20,000000</
ai_01_06_max_s><ai_01_07_min_s>00,000000</
ai_01_07_min_s><ai_01_07_min_r>00,000000</
ai_01_07_min_r><ai_01_07_max_r>12,000000</
ai_01_07_max_r><ai_01_07_max_s>20,000000</
```

Log example: Configuration procedure (continued)

```
ai_01_07_max_s><ai_01_08_min_s>00,000000</
ai_01_08_min_s><ai_01_08_min_r>00,000000</
ai_01_08_min_r><ai_01_08_max_r>12,000000</
ai_01_08_max_r><ai_01_08_max_s>20,000000</
ai_01_08_max_s><log_path>C:\SOPHO Messenger@net
</log_path><log_days>1</log_days></cfgrpy></xml>
```

Figure 473
Log example: Binding to OPC Servers

```
25/10/2001 10:41:37 -
S:TCP:FP-AI-100 - module 01 - contact 01 - Connecting: Parsing URL.

25/10/2001 10:41:37 -
S:TCP:FP-AI-100 - module 01 - contact 01 - Connecting: Connecting to OPC
Server.

25/10/2001 10:41:38 -
S:TCP:FP-AI-100 - module 01 - contact 01 - Active: Connected to OPC Serv-
er.

:
:
:

25/10/2001 10:41:39 -
S:TCP:FP-DI-300 - module 02 - contact 01 - Connecting: Parsing URL.

25/10/2001 10:41:39 -
S:TCP:FP-DI-300 - module 02 - contact 01 - Connecting: Connecting to OPC
Server.

25/10/2001 10:41:39 -
S:TCP:FP-DI-300 - module 02 - contact 01 - Active: Connected to OPC Serv-
er.
:
:
:
25/10/2001 10:41:39 -
S:TCP:FP-DO-401 - module 03 - contact 01 - Connecting: Parsing URL.

25/10/2001 10:41:39 -
S:TCP:FP-DO-401 - module 03 - contact 01 - Connecting: Connecting to OPC
Server.

25/10/2001 10:41:39 -
S:TCP:FP-DO-401 - module 03 - contact 01 - Active: Connected to OPC Serv-
er.
```

Figure 474
Log example: Message Request

```
25/10/2001 10:42:47 - O:TCP:<xml><msgrqs><type>DI</type><module>02</mod-
ule><contact>01</contact><sts>1</sts></msgrqs></xml>
```

Figure 475
Log example: Termination

```
25/10/2001 10:41:59 -
O:TCP:<xml><pgmsts><value>Shutdown</value></pgmsts></xml>

25/10/2001 10:41:59 -
S:INF:Application ended
```

Module – eKERNEL

General

eKERNEL is the core engine of the DECT Messenger, and is in the basic implementation the only module that accesses the database.

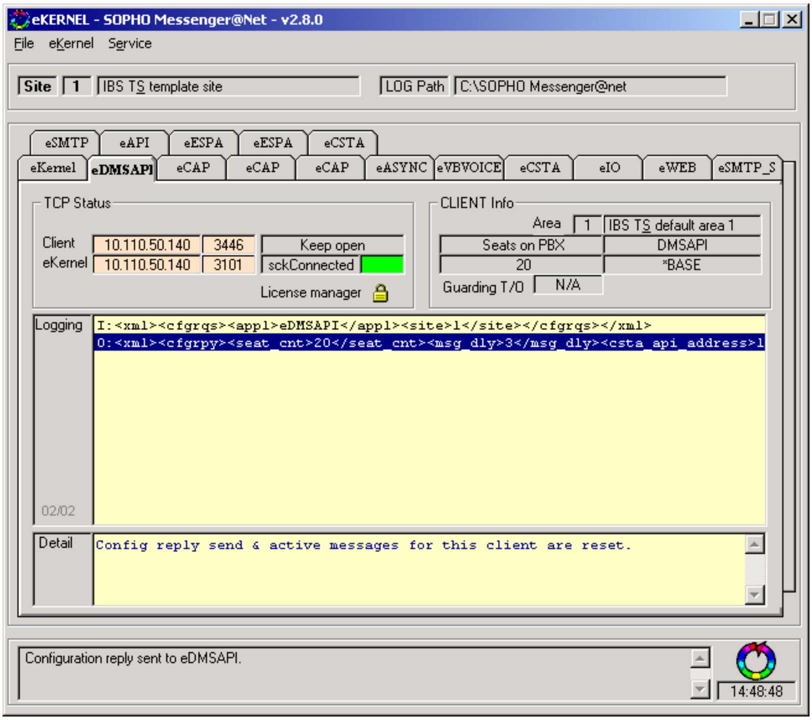
The eKERNEL receives information from various input sources, and exchanges information with various output sources.

Communication with eKERNEL is performed through TCP/IP stream sockets, where the eKERNEL acts as a server. The other modules that communicate to the eKERNEL act as clients.

All data streams are formatted in XML format, and are delimited with an <xml> start tag and an </xml> end tag, followed by CHR$(13) and CHR$(10). Within these tags, a number of keywords are embedded with their appropriated values.

In short, the eKERNEL is the central engine of the DECT Messenger, and controls the functioning of all the other modules. Figure 476 on page 1164 shows the eKERNEL interface.

Figure 476
eKERNEL interface



Site 1 IBS TS template site
LOG Path C:\SOPHO Messenger@net

Client	10.110.50.140	3446	Keep open
eKernel	10.110.50.140	3101	sckConnected 🟩

License manager 🔒

Area 1 IBS TS default area 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>1
```

```
Config reply send & active messages for this client are reset.
```

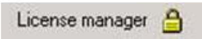
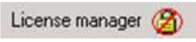
Configuration reply sent to eDMSAPI.

Licence Manager

The DECT Messenger package is secured by a licensing system, to prevent abuse of certain modules/clients. To properly install the licensing system and make Licence Manager available to DECT Messenger, refer to “General – Install PC” on page 805.

At start-up, the eKERNEL checks whether a valid licence is available or not. If there is no valid licence (because, for instance, the licence expired or licensing system not installed), the eKERNEL program aborts. To check if the installed licensing system is valid, use the Nortel Licence Manager. If this component is not yet installed, refer to “Install PC – Step 1e – Licence Manager” on page 839.

If a valid application is bound, all Tabs of the eKERNEL program show a crossed-through key icon, while the eKERNEL Tab shows a clear key icon.

- Clear key icon: [licence bound]  License manager
- Crossed-through key icon: [licence unbound]  License manager

Equipment versus Functionality modules

The licensing system distinguishes between *equipment* modules and *functionality* modules.

- The following modules are assigned as equipment:

  eCAPs, eESPAs, and eIOs.

- The following modules are assigned as functionality:

  Watchdog, eBACKUP, eCONFIG, eDMSAPI, eASYNC, eCSTA, eWEB, SMTP client, SMTP server, eAPI.

A key difference between equipment and functionality modules is the count of available licences, as illustrated in Table 62. Equipment modules have only a specified number of available licences, while functionality modules have an unlimited number of available licences.

Table 62
Licence examples

Module	total licences	used	free
ECAP [equipment]	3	2	1
EESPA [equipment]	2	2	0
DMSAPI [functionality]	unlimited	N/A	N/A

Whenever a client connects to the eKERNEL through a configuration request, the eKERNEL checks to determine if the client is an equipment or functionality module.

- Equipment module

  If the client is defined as equipment, the eKERNEL tries to bind this equipment to the licence. Success depends on the availability of a free licence. To verify how many licences are available on the system, check the Nortel Licence Manager. This program gives an overview of bound licences. If an equipment module disconnects, its licence is unbound and the total of free equipment licences is increased. On the other hand, if an equipment module connects, the total of free equipment licences is decreased (and the total of used equipment licences increased). A bound equipment module receives a valid configuration reply. If the equipment module cannot be bound, a status message is sent as follows: **<pgmsts>NO LICENCE AVAILABLE</pgmsts>**.

- Functionality module

  If a client is a functionality module, the eKERNEL checks if the given functionality is available in the licence system, and if so, sends a valid configuration reply. If the requested functionality is not available in the licence, then a status message is sent as follows: <pgmsts>NO LICENCE AVAILABLE</pgmsts>.

When a client (equipment or functionality module) is licenced, eKERNEL also provides a configuration reply, and the specific eKERNEL tab-page is updated with a clear key icon. If the licence cannot be bound or no correct functionality is available, then the eKERNEL tab-page is not updated, and the crossed-through key icon remains.

eAPI and eWEB

eAPI and eWEB do not send configuration requests. To ensure that eAPI and eWEB are licenced properly, eKERNEL checks these two functionality modules individually. If eAPI and eWEB are found in the Licence system, the TCP/IP ports for any clients of this kind are opened. If no eAPI or eWeb functionality is available in the licence system, then the ports are not opened and the eAPI or eWeb clients are not able to connect.

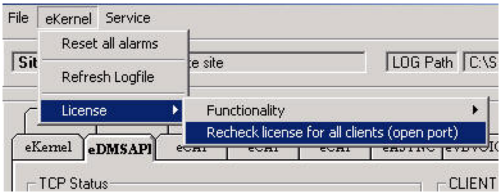
Licence maintenance

Every 24 hours, at midnight, each client that is connected to the eKERNEL is checked to determine whether the licence is still valid. If the Application licence (eKERNEL program) is expired, then eKERNEL sends a message to all of its clients and closes all of its ports, so no client is able to reconnect. After checking the Application licence, equipment and functionality modules are checked for validation.

When installing a new licence with more available equipment modules or adding one of the functionality modules eWeb or eAPI, the eKERNEL must explicitly be told about the new licence. To tell eKERNEL about a new licence, use the menu command: **eKERNEL > Licence > Recheck licence of all clients (open port)** as shown in Figure 477.

> ***Note:*** eKERNEL makes this same check automatically at midnight. Note that rechecking all licensing is a time-consuming process.

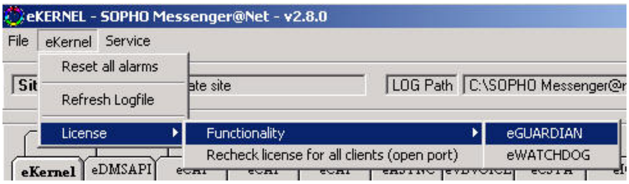
Figure 477
Rechecking licences



When installing a new licence with new available functionality (eGuardian or eWatchdog), the eKERNEL must be told about the new licence. To tell eKERNEL about a new licence, use the menu command: **eKERNEL** > **Licence** > **functionality** as shown in Figure 478 on page 1167.

> ***Note:*** eKERNEL makes this same check automatically at midnight. Note that rechecking all licensing can take a little time.

Figure 478
Adding licence functionality



If a licence is installed with fewer equipment licences than there are clients that need them, then the clients that are no longer licenced continue to function until the licence is rechecked. When the licence is rechecked, unlicenced clients receive a status message <pgmsts>NO LICENCE AVAILABLE</pgmsts>, and their TCP/IP port is closed. This same principle applies to functionality modules such eWEB and eAPI.

External interfaces

There are a number of external interfaces that can be attached to the eKERNEL. These interfaces can act as input source, output source, or play both roles.

An eKERNEL without any external modules is unable to perform work. A minimum configuration requires at least one input source (for example, eCAP for capturing a TELEVIC PROTOCOL CONVERTOR signalling system), and one output source (for example, eDMSAPI for sending E2-data messages to cordless DECT handsets).

Additional input sources can be attached to the product and are currently available, for example, eCAP for other signalling systems, eIO for unpowered contact detection, eSMTP for receiving MAIL, eWEB for receiving messages from the Internet.

Additional output sources can be attached to the product and are currently available or can be implemented in the future, for example, eSMTP for sending electronic mail, eASYNC for sending short messages to GSM and Pagers, eFAX for sending facsimile messages, and so on.

Note: In the current release there is a limitation of 21 external interfaces.

Database

The eKERNEL application is the only application that communicates directly with the databases. Every external application receives its configuration from eKERNEL.

There are two databases. One is named Messenger_CFG.mdb, and another is named Messenger_data.mdb. Both databases are in Microsoft Access 2000 format, and are processed through applications written in Microsoft Visual Studio 6.0 (Visual Basic and C++).

The Messenger_CFG.mdb contains about 39 tables, and defines the configuration of the DECT Messenger software. These tables determine the behaviour of the product.

The Messenger_data.mdb usually contains eight tables, which are an internal work space of the DECT Messenger. Some modules – such as eKERNEL – access this database heavily. Nortel recommends that you avoid using the data database, except for problem determination and recovery services.

TCP Connections

The eKERNEL acts as a TCP Server, and typically listens to several ports.

The configuration of the TCP clients can be performed in the configuration database.

The status of each connection is visible in the interface of the eKERNEL application. In normal operation, an active connection is indicated with green colour. A client that is not connected is indicated with yellow colour. Other colours indicate an intermediate state or an error condition.

Logging

Every event is logged, and can be accessed both in log files on disk and on-screen. The on-screen buffer is limited to 100 records, and details can be seen by double-clicking on the log records. The log files are commonly stored in the directory specified in the CFG_Log_path_str field of the eKERNEL_site table.

If CFG_Log_path_str = C:\SOPHO Messenger@net, then all log files are stored in the C:\SOPHO Messenger@Net\log\eKERNEL directory. Each day a new log file is created at midnight.

Menu options

- **File > Exit**

  This option closes the eKERNEL application.

- **eKERNEL > Reset all alarms**

  This option clears all active alarms in the data database.

- **eKERNEL >Refresh logfiles**

  This option closes and reopens the log file of the eKERNEL application. Perform this action before opening the log file for the current day, so all data that is still in memory is copied to the log file.

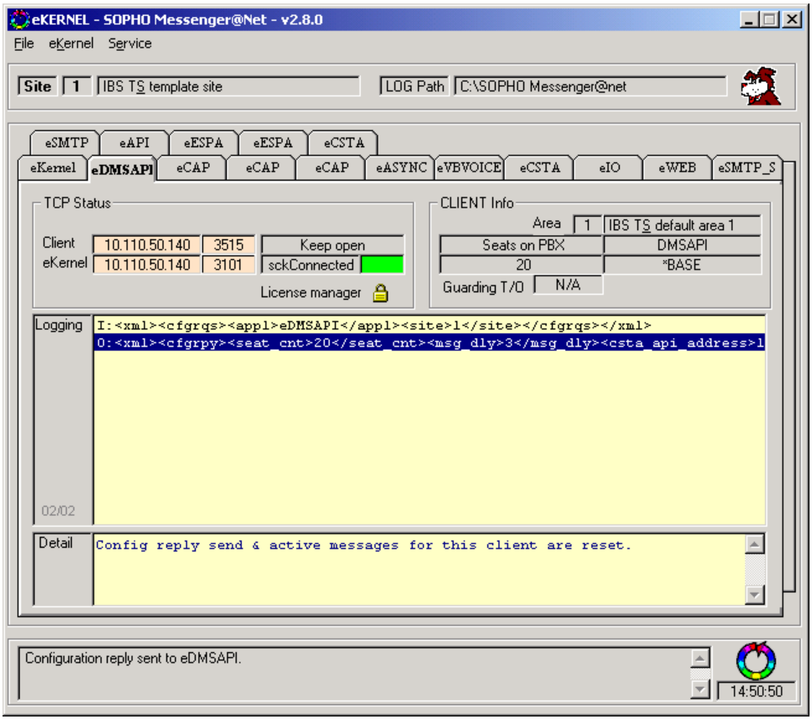
- **Service > Delete all data records**

  This function deletes all the records of the selected table.
  Perform this action to be sure you start with a clean data database at the customer.

Watchdog

When the Watchdog facility is enabled (see "Table: eKERNEL_SITE" on page 1459), an icon of a dog is visible at the right top of the window, as shown in " Watchdog enabled" on page 1171. When active, Watchdog sends the command string entered in the CFG_Watchdog_cmd_str field of the eKERNEL_SITE table to the connected com port. The command string is sent every CFG_Watchdog_interval_n seconds.

Figure 479
Watchdog enabled



Site: 1 IBS TS template site
LOG Path: C:\SOPHO Messenger@net

Client: 10.110.50.140 3515 Keep open
eKernel: 10.110.50.140 3101 sckConnected 🟩

Area: 1 IBS TS default area 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>1
```

Detail: Config reply send & active messages for this client are reset.

Configuration reply sent to eDMSAPI.

14:50:50

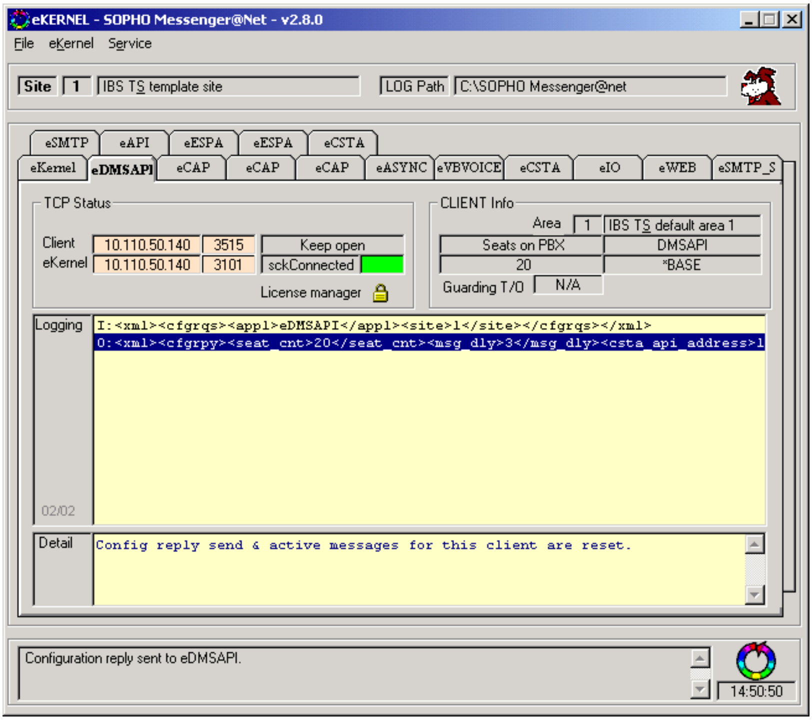
Guarding

For every input program, the administrator can configure a guarding facility, as shown in Figure 480 on page 1172.

If guarding is activated for a specific input program, an indication is given in the Client information frame for every TCP/IP client.

The Guarding T/O field specifies the timeout that is defined in the eKERNEL_guarding table (see “Table: eKERNEL_GUARDING” on page 1439), and the last event field text box shows the number of seconds that have passed since the last request was received from the TCP/IP client. Once the Last event value exceeds the guarding timeout value, a guarding alarm is generated.

Figure 480
Guarding information



Site 1 IBS TS template site

LOG Path C:\SOPHO Messenger@net

Client 10.110.50.140 3515 Keep open

eKernel 10.110.50.140 3101 sckConnected 🟩

Area 1 IBS TS default area 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>1
```

02/02

Config reply send & active messages for this client are reset.

Configuration reply sent to eDMSAPI.

14:50:50

Module – eSMTP

The eSMTP module is an output program that receives message requests from the eKERNEL module. The eSMTP connects to an SMTP server, and delivers mail requests to the mail server according to the RFC821 specifications. This involves a sockets connection between eSMTP and the SMTP server of choice. For such a connection, eSMTP is TCP client and the SMTP server is TCP server, listening on port 25.

Initialisation

The eSMTP module is started by means of a shortcut. Figure 481 shows an example of the required keywords:

Figure 481
Example of required keywords

```
"C:\SOPHO Messenger@Net\Exe\eSMTP.exe"
/Site:3
/eKernel address:*LOCAL
/eKernel port:3111
/Log drive:C
```

The following keywords are used:

- **Site**

  The Site keyword denotes the site that is assigned to the eSMTP module.

- **eKERNEL address**

  The eKERNEL address keyword denotes the IP address that is assigned to the eKERNEL module. The eSMTP contacts this IP address to connect to the eKERNEL.

- **eKERNEL port**

  The eKERNEL port keyword denotes the port number that is assigned in the configuration for the eSMTP client instance.

On start-up, the eSMTP application attempts to connect to the eKERNEL. This is performed based upon the address and port information obtained from the shortcut.

At connection, the eSMTP requests the eKERNEL to provide additional configuration settings. This is known as a configuration request. The eKERNEL in turn authenticates the client and responds with a configuration reply.

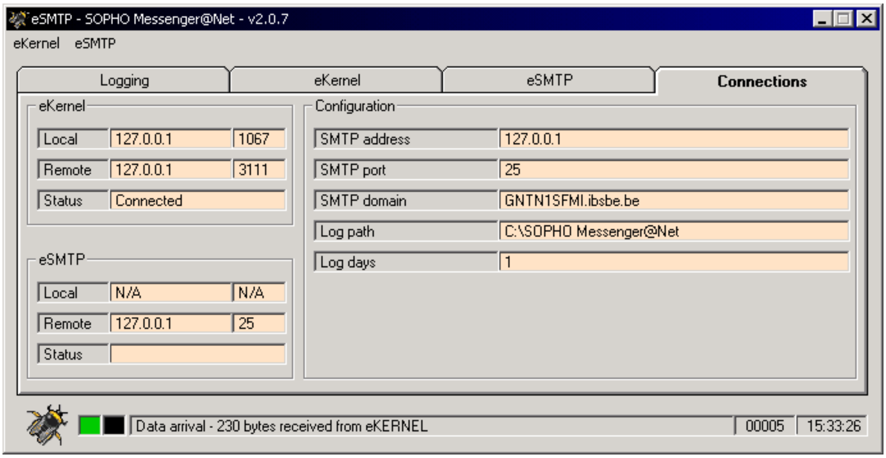
Figure 482 on page 1175 shows the configuration request.

Figure 482
eSMTP configuration request

```
28/10/2001 15:28:39 - S:INF:
Application eSMTP - SOPHO Messenger@Net - v2.0.7 started with parameters
/Site:3 /eKernel address:*LOCAL /eKernel port:3111 /Log drive:C

28/10/2001 15:28:40 - S:INF:
TCP local port 01065 connected with remote port 03111 (eKERNEL)

28/10/2001 15:28:40 - O:TCP:
<xml>
<cfgrqs>
<appl>eSMTP</appl>
<site>3</site>
</cfgrqs></xml>

28/10/2001 15:28:40 - I:TCP:
<xml>
<cfgrpy>
<smtp_address>127.0.0.1</smtp_address>
<smtp_port>25</smtp_port>
<smtp_domain>GNTN1SFMI.ibsbe.be</smtp_domain>
<email_from>Messenger@Net</email_from>
<format>32^0^0^0^0</format>
<log_path>C:\SOPHO Messenger@net</log_path>
<log_days>1</log_days>
</cfgrpy>
</xml>
```

When the configuration is received, a window similar to the one shown Figure 483 on page 1176 opens. The configuration can be viewed in the Connections tab.

Figure 483
Configuration information



eKernel

Local	127.0.0.1	1067
Remote	127.0.0.1	3111
Status	Connected	

eSMTP

Local	N/A	N/A
Remote	127.0.0.1	25
Status		

Configuration

SMTP address	127.0.0.1
SMTP port	25
SMTP domain	GNTN1SFMI.ibsbe.be
Log path	C:\SOPHO Messenger@Net
Log days	1

Data arrival - 230 bytes received from eKERNEL | 00005 | 15:33:26

Output program activity

The eSMTP module is now ready to receive message requests from eKERNEL. These requests are handled on a first-in first-out basis.

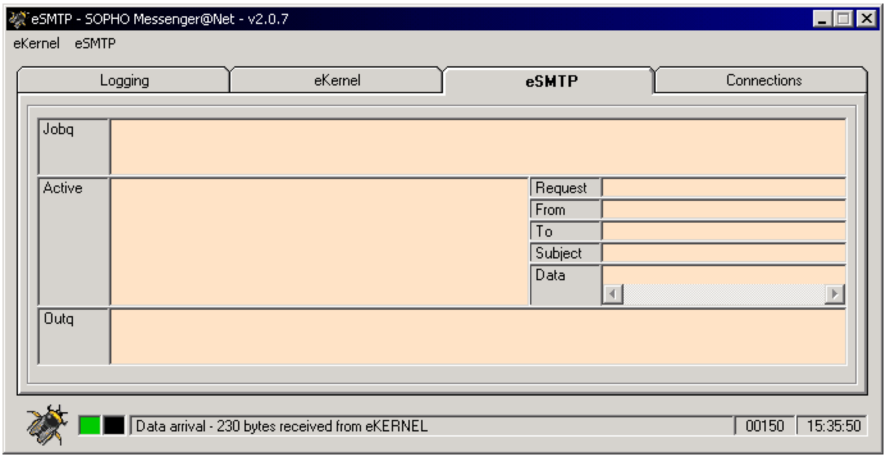
The requests are received in the format shown in Figure 484.

Figure 484
Message request format

```
<xml>
<msgrqs>
<id>00251</id>
<to>befmi@1s.be</to>
<pag_01>Test to eSMTP</pag_01>
<pag_more>N</pag_more>
</msgrqs>
</xml>
```

The message requests are executed one at a time, by means of a TCP sockets connection to the SMTP server of choice. The actual dialog with the SMTP server can be monitored through the eSMTP tab, as shown in Figure 485 on page 1177.

Figure 485
eSMTP tab



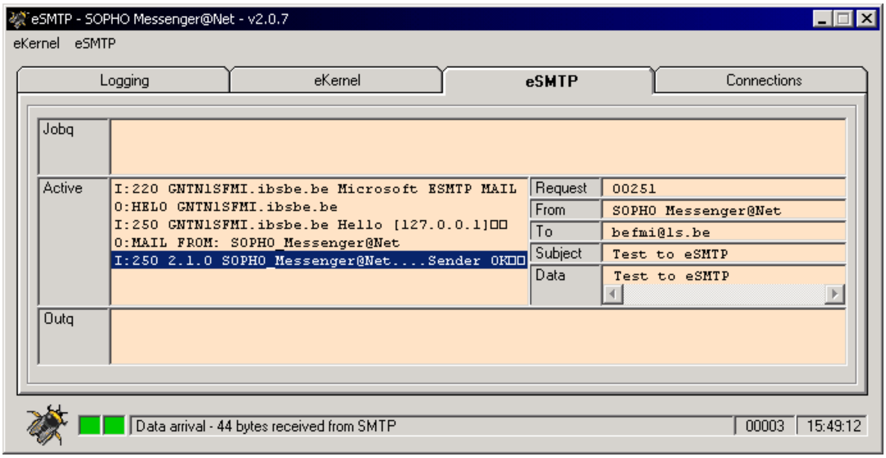
Data arrival - 230 bytes received from eKERNEL | 00150 | 15:35:50

The eSMTP tab provides an overview of the requests that are waiting to be processed. This is visible in the top area (referred to as the job queue). Requests are handled as follows:

1 The request is analysed, and the required keywords are extracted and shown to the right.

The left-hand site of the window shows the actual dialog with the SMTP server. See Figure 486 on page 1178 for an example of an active message.

Figure 486
Request queue with extracted keywords



```
I:220 GNTN1SFMI.ibsbe.be Microsoft ESMTP MAIL
O:HELO GNTN1SFMI.ibsbe.be
I:250 GNTN1SFMI.ibsbe.be Hello [127.0.0.1]□□
O:MAIL FROM: SOPHO_Messenger@Net
I:250 2.1.0 SOPHO_Messenger@Net....Sender OK□□
```

Request	00251
From	SOPHO Messenger@Net
To	befmi@ls.be
Subject	Test to eSMTP
Data	Test to eSMTP

Data arrival - 44 bytes received from SMTP | 00003 | 15:49:12

2 The eSMTP module sends the status of the request back to the eKERNEL. This status can either indicate a positive acknowledge or a negative acknowledge.

The format of the message reply is shown in Figure 487.

Figure 487
Message reply format

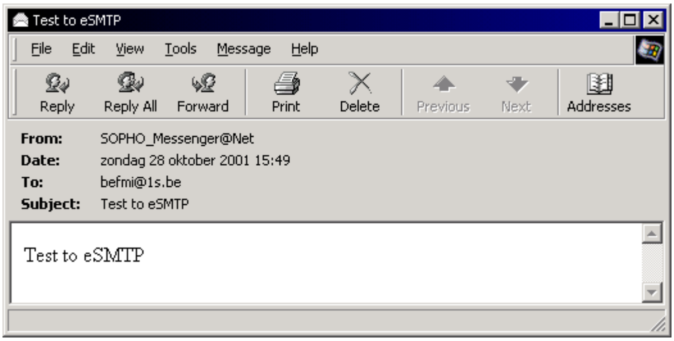
```
<xml>
<msgrpy>
<id>00251</id>
<sts>ACK^</sts>
</msgrpy>
</xml>
```

3 The e-mail message is delivered to the mailbox of the destination user.

Note that intermediate processing on the external SMTP server or servers is responsible for message delivery. This process is completely out of the control of the eSMTP application.

Figure 488 shows an example of the mail that is produced by the eSMTP module, when viewed using Microsoft Outlook Express.

Figure 488
Example of mail produced by eSMTP module

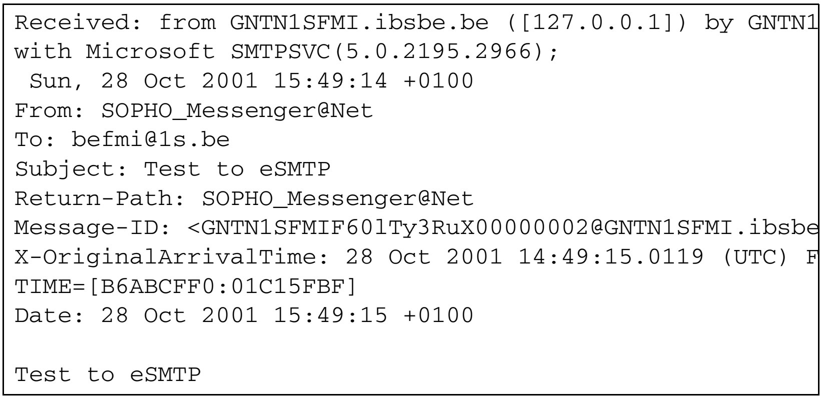


From: SOPHO_Messenger@Net
Date: zondag 28 oktober 2001 15:49
To: befmi@1s.be
Subject: Test to eSMTP

Test to eSMTP

Figure 488 shows an example of the raw data of the mail that is produced by the eSMTP module.

Figure 489
Raw data of mail produced by eSMTP module



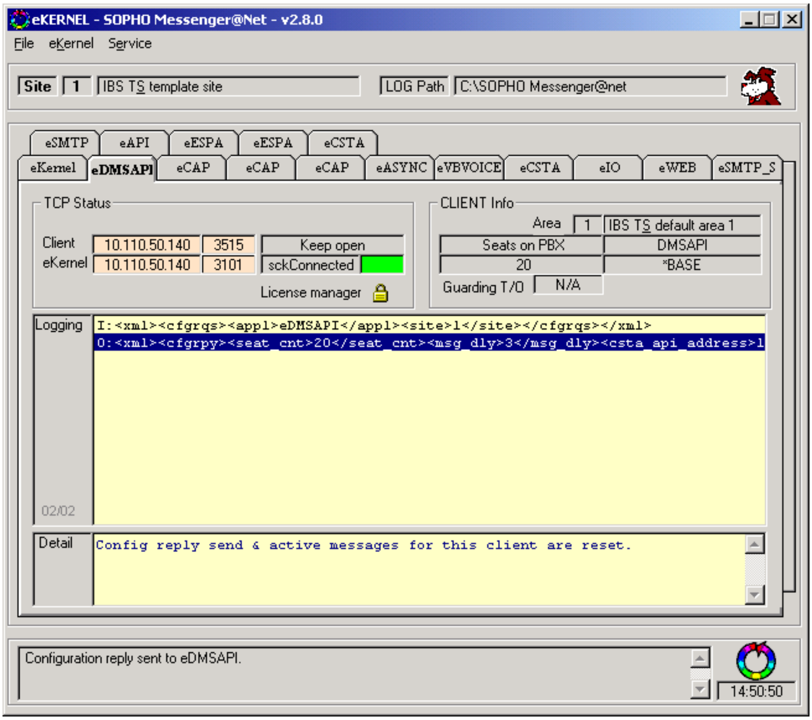
```
Received: from GNTN1SFMI.ibsbe.be ([127.0.0.1]) by GNTN1
with Microsoft SMTPSVC(5.0.2195.2966);
 Sun, 28 Oct 2001 15:49:14 +0100
From: SOPHO_Messenger@Net
To: befmi@1s.be
Subject: Test to eSMTP
Return-Path: SOPHO_Messenger@Net
Message-ID: <GNTN1SFMIF60lTy3RuX00000002@GNTN1SFMI.ibsbe
X-OriginalArrivalTime: 28 Oct 2001 14:49:15.0119 (UTC) F
TIME=[B6ABCFF0:01C15FBF]
Date: 28 Oct 2001 15:49:15 +0100

Test to eSMTP
```

Logging

The eSMTP application provides logging both on-screen and on disk.

Figure 490 shows the on-screen logging, displayed on the Logging tab.

Figure 490
eSMTP on-screen logging



Site 1 IBS TS template site

LOG Path C:\SOPHO Messenger@net

Client 10.110.50.140 3515 Keep open

eKernel 10.110.50.140 3101 sckConnected 🟩

Area 1 IBS TS default area 1

Seats on PBX	DMSAPI
20	*BASE

Guarding T/O N/A

Logging

```
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>1
```

02/02

Detail

```
Config reply send & active messages for this client are reset.
```

Configuration reply sent to eDMSAPI.

14:50:50

Figure 491 shows an example of a log file on disk, as viewed with a text editor.

Figure 491
Log files on hard disk

```
28/10/2001 14:46:32 - I:TCP:
221 2.0.0 GNTN1SFMI.ibsbe.be Service closing transmission channel

28/10/2001 14:46:33 - O:TCP:
<xml><msgrpy><id>00001</id><sts>NACK - 550 5.7.1 Unable to relay for
francis.missiaen@1s.be^</sts></msgrpy></xml>

28/10/2001 14:51:10 - S:INF:
TCP local port 01063 connected with remote port 00025 (eDMSAPI)

28/10/2001 14:51:10 - I:TCP:
220 GNTN1SFMI.ibsbe.be Microsoft ESMTP MAIL Service, Version:
5.0.2195.2966 ready at  Sun, 28 Oct 2001 14:51:10 +0100

28/10/2001 14:51:11 - O:TCP:
HELO GNTN1SFMI.ibsbe.be

28/10/2001 14:51:11 - I:TCP:
250 GNTN1SFMI.ibsbe.be Hello [127.0.0.1]

28/10/2001 14:51:12 - O:TCP:
MAIL FROM: SOPHO.Messenger@Net
28/10/2001 14:51:12 - I:TCP:
250 2.1.0 SOPHO.Messenger@Net....Sender OK

28/10/2001 14:51:13 - O:TCP:
RCPT TO: francis.missiaen@1s.be

28/10/2001 14:51:13 - I:TCP:250 2.1.5 francis.missiaen@1s.be

28/10/2001 14:51:14 - O:TCP:
DATA

28/10/2001 14:51:14 - I:TCP:
354 Start mail input; end with <CRLF>.<CRLF>

28/10/2001 14:51:15 - O:TCP:
From: SOPHO.Messenger@Net

continued on next page...
```

Log files on hard disk (continued)

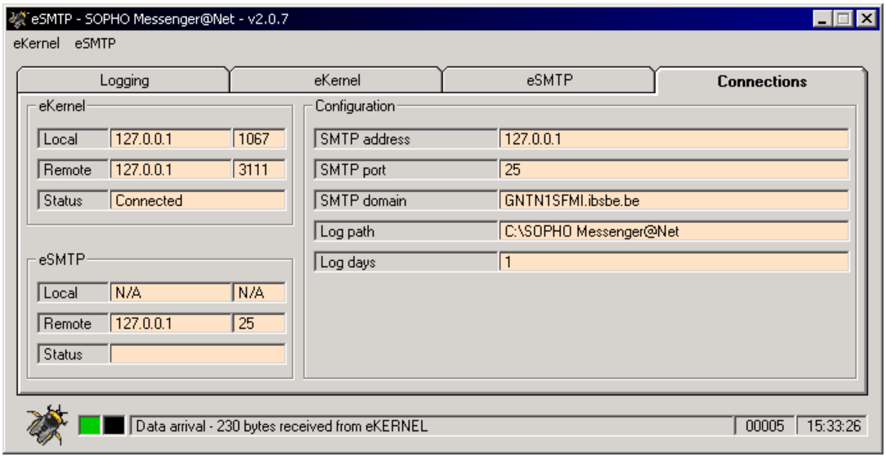
```
28/10/2001 14:51:15 - O:TCP:
To: francis.missiaen@1s.be

28/10/2001 14:51:15 - O:TCP:
Subject: REA K100

28/10/2001 14:51:15 - O:TCP:

28/10/2001 14:51:15 - O:TCP:
REA K100

28/10/2001 14:51:15 - O:TCP:
.

28/10/2001 14:51:15 - I:TCP:
250 2.6.0 <GNTN1SFMIrywNUG0Vy100000001@GNTN1SFMI.ibsbe.be> Queued mail
for delivery

28/10/2001 14:51:16 - O:TCP:
quit

28/10/2001 14:51:16 - I:TCP:
221 2.0.0 GNTN1SFMI.ibsbe.be Service closing transmission channel

28/10/2001 14:51:17 - O:TCP:
<xml><msgrpy><id>00001</id><sts>ACK^</sts></msgrpy></xml>
```

Relaying and Routing

IMPORTANT!

A common configuration error, related to relaying and routing settings, occurs when eSMTP tries to deliver a message to a mail destination user that is not residing in the same domain, as shown in Figure 492 on page 1183.

Figure 492
Relaying and Routing error on-screen



eKernel
Local 127.0.0.1 1067
Remote 127.0.0.1 3111
Status Connected

eSMTP
Local N/A N/A
Remote 127.0.0.1 25
Status

Configuration
SMTP address 127.0.0.1
SMTP port 25
SMTP domain GNTN1SFMI.ibsbe.be
Log path C:\SOPHO Messenger@Net
Log days 1

Data arrival - 230 bytes received from eKERNEL 00005 15:33:26

The error is usually recorded in the log files with a message similar to the one shown in Figure 493.

Figure 493
Relaying error log (relay failed)

```
:

28/10/2001 14:46:31 - O:TCP:
RCPT TO: francis.missiaen@1s.be

28/10/2001 14:46:31 - I:TCP:
550 5.7.1 Unable to relay for francis.missiaen@1s.be

:
```

Other messages can be shown instead, for example, 550 - prohibited, 550 - Unable to relay, and so on.

To correct this issue, consult with the system administrator regarding the rights granted for routing and relaying in the module. Nortel recommends that the IP address of eSMTP be defined in the SMTP server of the mail platform, so that eSMTP is allowed to send mail to destinations that are not in the local domain.

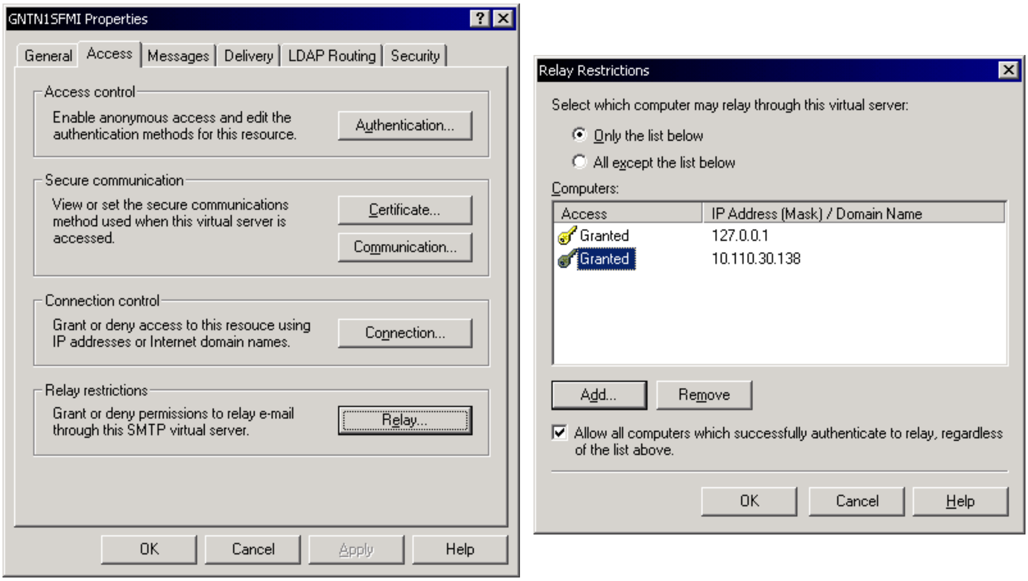
The related configuration issues are beyond the scope of this document. In the following pages, configuration information is shown for illustration only. Look for a more detailed discussion of relaying and routing issues in the official documentation for your SMTP server (Windows 2000, Exchange, Domino, iSeries 400, and so on).

Windows SMTP server

In Windows SMTP Server (part of the Internet Information Server), you can for instance grant access by clicking **Start** on the Windows taskbar, and choosing **Settings** > **Control Panel** > **Administrative Tools** > **Properties** > **Internet Service Manager.**

Figure 494 on page 1185 illustrates the settings needed to grant the SMTP server access to relay from both 127.0.0.1 and 10.110.50.138. These addresses are the addresses where eSMTP modules reside.

Figure 494
Setting SMTP relay



GNTN1SFMI Properties

Access control

Enable anonymous access and edit the authentication methods for this resource.

Secure communication

View or set the secure communications method used when this virtual server is accessed.

Connection control

Grant or deny access to this resouce using IP addresses or Internet domain names.

Relay restrictions

Grant or deny permissions to relay e-mail through this SMTP virtual server.

Relay Restrictions

Select which computer may relay through this virtual server:

● Only the list below

○ All except the list below

Computers:

Access	IP Address (Mask) / Domain Name
Granted	127.0.0.1
Granted	10.110.30.138

☑ Allow all computers which successfully authenticate to relay, regardless of the list above.

eSMTP can send mail to users that do not reside in the local domain. This is indicated in the log as shown in Figure 495.

Figure 495
Relaying successful

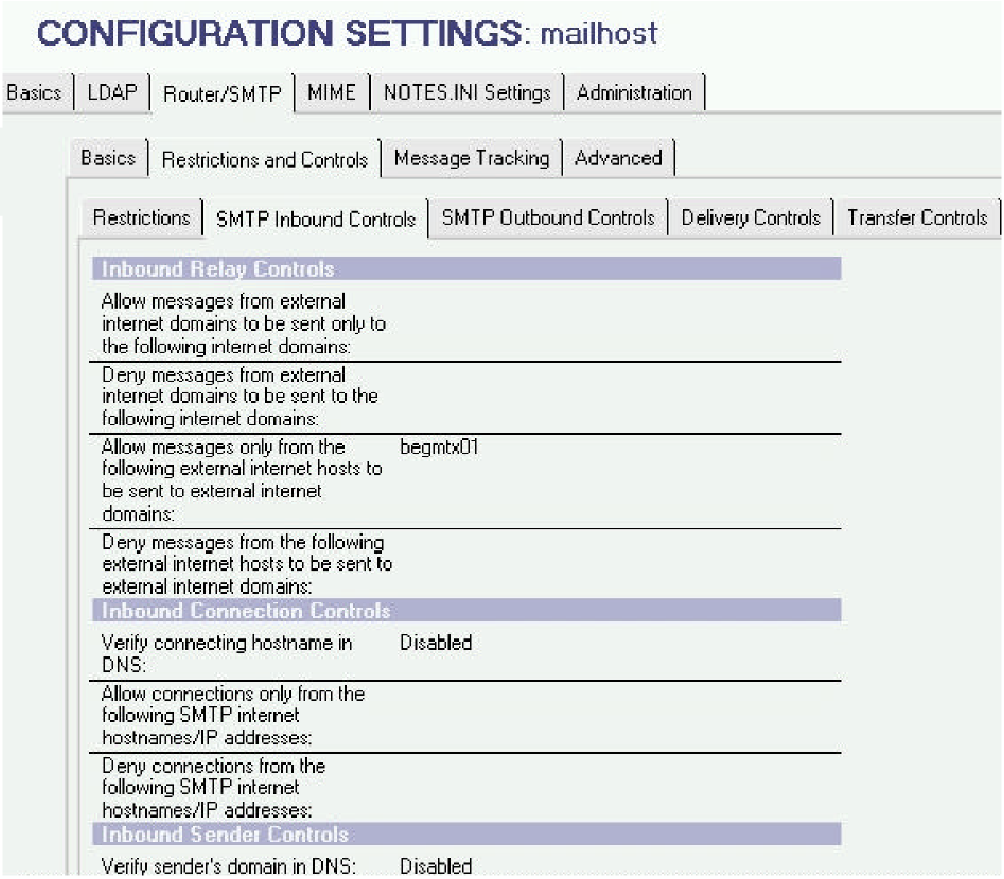
```
:
:
28/10/2001 14:51:13 - O:TCP:
RCPT TO: francis.missiaen@1s.be

28/10/2001 14:51:13 - I:TCP:
250 2.1.5 francis.missiaen@1s.be
:
:
```

Domino (Lotus Notes)

The same techniques discussed for "Windows SMTP server" on page 1184 can be implemented on other SMTP servers. For example, in Domino (Lotus Notes), you can allow inbound SMTP requests from other parties (eSMTP).

To configure inbound SMTP options, click **Router/SMTP > Restrictions and Controls > SMTP Inbound Controls > Allows messages only from …** Figure 496 on page 1187 illustrates the settings needed to allow messages from external hosts to be sent to external Internet domains.

Figure 496
Enable messages from external hosts to be sent to external Internet domains



CONFIGURATION SETTINGS: mailhost

Inbound Relay Controls

Allow messages from external internet domains to be sent only to the following internet domains:	
Deny messages from external internet domains to be sent to the following internet domains:	
Allow messages only from the following external internet hosts to be sent to external internet domains:	begmtx01
Deny messages from the following external internet hosts to be sent to external internet domains:	

Inbound Connection Controls

Verify connecting hostname in DNS:	Disabled
Allow connections only from the following SMTP internet hostnames/IP addresses:	
Deny connections from the following SMTP internet hostnames/IP addresses:	

Inbound Sender Controls

Verify sender's domain in DNS:	Disabled

Consult with your network administrator for more information on configuration aspects and network design.

Module – eSMTP_server

The eSMTP_server module is a member of the input program family. Therefore, the eSMTP_server is capable of generating alarms to eKERNEL.

The name eSMTP_server can be rather confusing. In fact, there is no SMTP server functionality implemented in the module. This means the application is not acting as an SMTP server, and is not listening on port 25 for inbound SMTP requests.

The module eSMTP_server must always be seen in conjunction with the SMTP Server component that is shipped with Windows, as part of the Internet Information Server software. Refer to “Module – eSMTP_server” on page 1189 for more information.

The actual role of SMTP server (handling inbound sockets connections on port 25) is played by the Microsoft component. This component stores inbound mails in a directory structure, as specified during configuration of the Microsoft component.

A typical configuration sends inbound mails to the directory c:\inetpub\mailroot\drop.

These e-mail files are in fact readable text-files that can be opened with a text editor, such as Notepad. Figure 497 on page 1190 shown an example of an inbound e-mail:

Figure 497
Example of inbound e-mail

```
x-sender: francis.missiaen@1s.be
x-receiver: kristien.daneels@1s.be
Received: from gntn1sfmi ([10.110.49.102]) by GNTN1SFMI.ibsbe.be with Mi-
crosoft SMTPSVC(5.0.2195.2966);
 Wed, 27 Jun 2001 14:50:25 +0200
From: beibsbru@ibsbe.be
To: kristien.daneels@1s.be
Subject: Reanimation
MIME-Version:1.0
Content-Type: multipart/mixed; bound-
ary="--_=_NextPart_000_01C07713.6DAD45D0"
Content-Disposition: inline
Return-Path: beibsbru@ibsbe.be
Message-ID: <GNTN1SFMIfznRukVykX00000004@GNTN1SFMI.ibsbe.be>
X-OriginalArrivalTime: 27 Jun 2001 12:50:25.0293 (UTC) FILE-
TIME=[BC2773D0:01C0FF07]
Date: 27 Jun 2001 14:50:25 +0200

----_=_NextPart_000_01C07713.6DAD45D0
Content-type: text/html
Content-transfer-encoding: binary

<html>
<body bgcolor='#FFFFFF' link='#336699' alink='#336699'>
:
:
:
</body></html>

----_=_NextPart_000_01C07713.6DAD45D0
Content-type: text/plain; charset=iso-8859-1
Content-Disposition: attachment; filename="Attach_0.txt"
Content-transfer-encoding: binary

:
:
:
----_=_NextPart_000_01C07713.6DAD45D0--
```

IMPORTANT!

There are many competing specifications for mail formatting. A basic implementation is specified in RFC821. Many other specifications were added, for example, RFC1251 described the MIME format. The current release of eSMTP_server is not designed to be fully compatible with all available functionality embedded in e-mail messages. Future releases of the eSMTP_server can be enhanced with, for instance, functionality that is capable of detaching media streams (for example, BASE64 encoded audio/wave contents).

Keyword processing

For the purpose of illustration, examples in this chapter ignore all mail contents, and process only the following keywords:

- x-sender. The value of the x-sender tag is stored
- x-receiver. The value of the x-receiver tag is stored
- Subject. The value of the Subject: tag is stored

Because the x-sender and x-receiver tags are Microsoft proprietary, the module eSMTP_server also looks for From and To keywords, if the x-sender and x-receiver tags are missing. Although not officially supported, it is possible to use the eSMTP_server in environments that work with other SMTP Servers than the one officially supported (Microsoft Internet Information Server).

The information in Figure 498 is stored for further processing.

Figure 498
Keyword processing of selected e-mail tags

```
<from>francis.Missiaen@1s.be</from>
<to>kristien.daneels@1s.be</to>
<subject>Reanimation</subject>
```

Initialisation

The eSMTP_server is started by means of a shortcut. This shortcut contains required parameters illustrated in Figure 499 on page 1192.

Figure 499
Shortcut parameters

```
"C:\SOPHO Messenger@Net\Exe\eSMTP_server.exe"
/Site:3
/eKernel address:*LOCAL
/eKernel port:3110
/Log drive:C
```

The following keywords are used:

- **Site**

  The Site keyword denotes the site that is assigned to the eSMTP_server module.

- **eKERNEL**

  The eKernel address keyword denotes the IP address that is assigned to the eKERNEL module. The eSMTP_server contacts this IP address to connect to the eKERNEL.

- **eKERNEL Port**

  The eKernel Port keyword denotes the port number that is assigned in the configuration for the eSMTP_server instance.

On start-up, the eSMTP_server application attempts to connect to the eKERNEL, as shown in Figure 500. This is performed based upon the address and port information obtained from the Shortcut.

Figure 500
eKERNEL connection attempt

```
28/10/2001 16:08:07 - S:INF:
Application eSMTP_server - SOPHO Messenger@Net - v2.0.7 started with pa-
rameters /Site:3 /eKernel address:*LOCAL /eKernel port:3110 /Log drive:C

28/10/2001 16:08:08 - S:INF:
TCP local port 01127 connected with remote port 03110 (eKERNEL)
```

At connection, the eSMTP_server requests the eKERNEL to provide additional configuration settings, as shown in Figure 501. The eKERNEL authenticates the client and responds with a configuration reply, as shown in Figure 502 on page 1194.

Figure 501
Configuration request

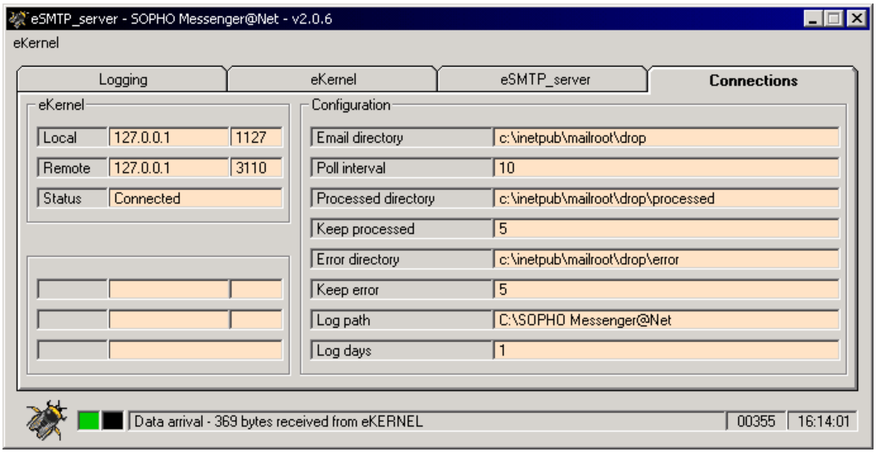
```
228/10/2001 16:08:08 - O:TCP:
<xml><cfgrqs><appl>eSMTP_server</appl><site>3</site></cfgrqs></xml>

28/10/2001 16:08:08 - I:TCP:<xml>
<cfgrpy><email_dir>c:\inetpub\mailroot\drop</email_dir><poll_intv>10</
poll_intv><email_dir_processed>c:\inetpub\mailroot\drop\processed</
email_dir_processed><keep_processed>5</
keep_processed><email_dir_error>c:\inetpub\mailroot\drop\error</
email_dir_error><keep_error>5</keep_error><log_path>C:\SOPHO Messen-
ger@net</log_path><log_days>1</log_days> </cfgrpy></xml>
```

Figure 502
Configuration reply

```
<xml>
<cfgrpy>
<email_dir>c:\inetpub\mailroot\drop</email_dir>
<poll_intv>10</poll_intv>
<email_dir_processed>c:\inetpub\mailroot\drop\processed</
email_dir_processed>
<keep_processed>5</keep_processed>
<email_dir_error>c:\inetpub\mailroot\drop\error</email_dir_error>
<keep_error>5</keep_error>
<log_path>C:\SOPHO Messenger@net</log_path>
<log_days>1</log_days>
</cfgrpy>
</xml>
```

When the configuration is received, the Connections tab of the eSMTP_server module is updated with information similar to what is shown the panel shown in Figure 503.

Figure 503
Updated eSMTP Connection information



eSMTP_server - SOPHO Messenger@Net - v2.0.6

eKernel

Local	127.0.0.1	1127
Remote	127.0.0.1	3110
Status	Connected	

Configuration

Email directory	c:\inetpub\mailroot\drop
Poll interval	10
Processed directory	c:\inetpub\mailroot\drop\processed
Keep processed	5
Error directory	c:\inetpub\mailroot\drop\error
Keep error	5
Log path	C:\SOPHO Messenger@Net
Log days	1

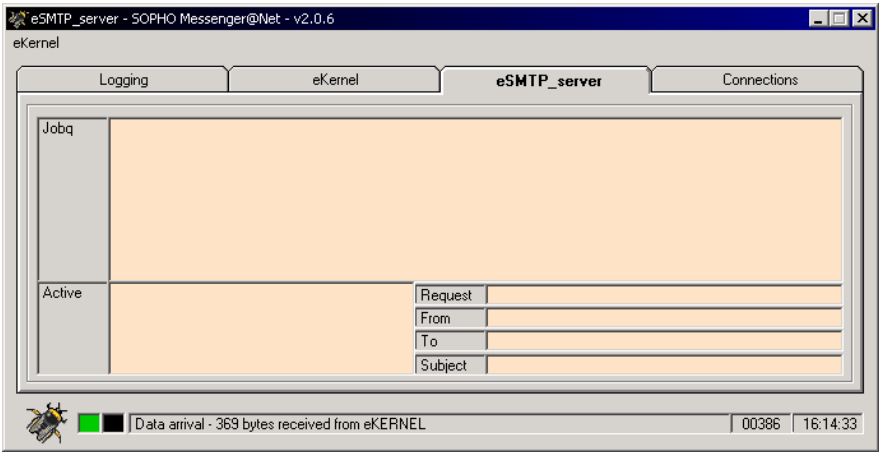
Data arrival - 369 bytes received from eKERNEL | 00355 | 16:14:01

Activity of eSMTP_server

The eSMTP_server module is now ready to send message requests to eKERNEL. These requests are sent on a first-in first-out basis.

Click the eSMTP_server tab to view request processing, as shown in Figure 504.

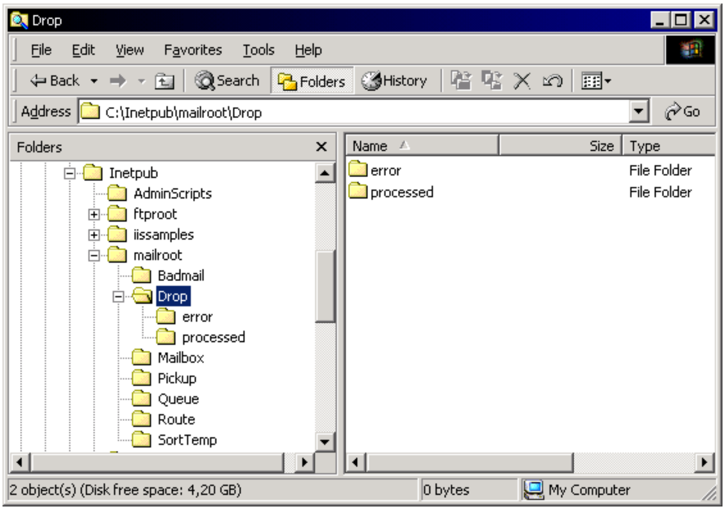
Figure 504
Request processing shown on the eSMTP_server tab



Data arrival - 369 bytes received from eKERNEL | 00386 | 16:14:33

As specified in the configuration reply, the eSMTP_server polls the specified directory for new inbound mail messages at fixed intervals. This interval is usually 10 seconds. The default directory is C:\Inetpub\mailroot\Drop, as shown in Figure 505 on page 1196.

Figure 505
Default inbound mail (drop) directory



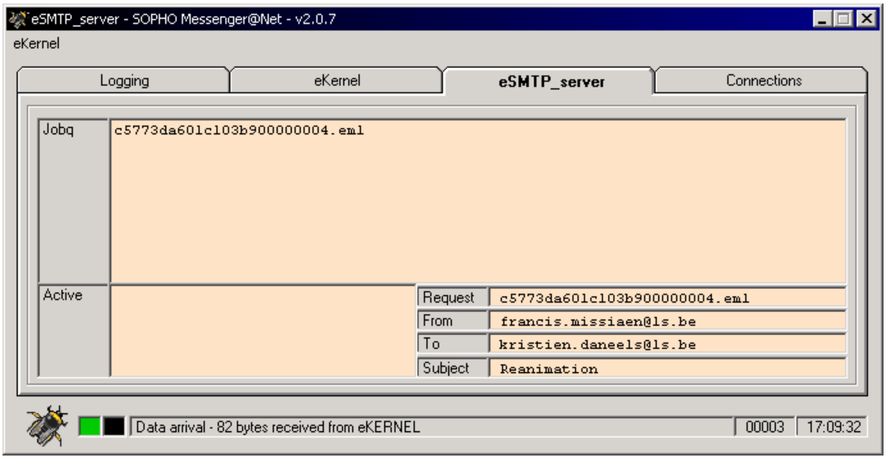
Address: C:\Inetpub\mailroot\Drop

Name	Size	Type
error		File Folder
processed		File Folder

2 object(s) (Disk free space: 4,20 GB) | 0 bytes

Inbound mail messages are processed one by one. During processing, a window opens similar to the one shown in Figure 506.

Figure 506
Mail processing



Jobq: c5773da601c103b900000004.eml

Active:

Request: c5773da601c103b900000004.eml
From: francis.missiaen@ls.be
To: kristien.daneels@ls.be
Subject: Reanimation

Data arrival - 82 bytes received from eKERNEL | 00003 | 17:09:32

The Mail processing window shows:

- **Request identifier**

  This is a long filename and refers to the filename of the e-mail message that is being processed. These names were generated by the Microsoft SMTP Server component.

- **From** field

  Isolated from the <x-receiver> tag.

- **To** field

  Isolated from the <x-sender> tag.

- **Subject** field

  Isolated from the Subject: tag.

With these values, the eSMTP_server produces a message request for eKERNEL, as shown in Figure 507.

Figure 507
eSMTP message request for eKERNEL

```
<xml>
<msgrqs>
<id>bc6c51d001c0ff0700000004.eml</id>
<from>francis.missiaen@1s.be</from>
<to>kristien.daneels@1s.be</to>
<subject>Reanimation</subject>
</msgrqs>
</xml>
```

The eKERNEL then validates the message request, and either accepts or refuses the request. During the validation process, the eSMTP_server is considered as an input program, so all configuration settings must be defined correctly. One major criterion is whether for this input program the auto-create group is activated. Without auto creation of groups, both **From** and **To** must be known in the database.

- **Message Accepted**

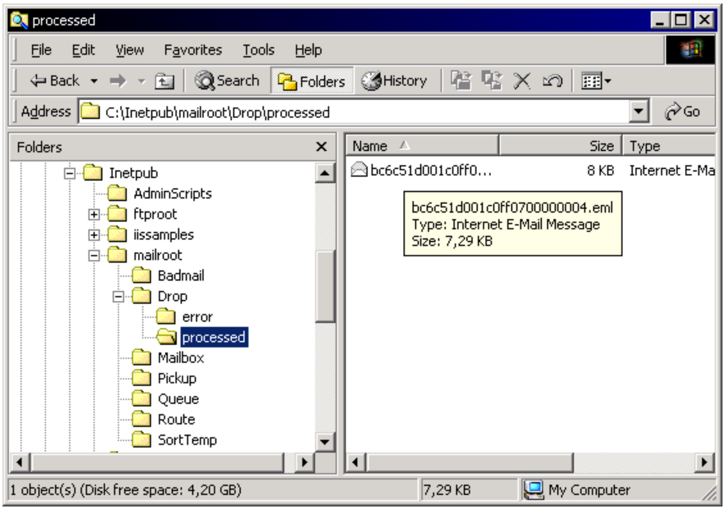
  If the message is accepted, a reply is sent, as shown in Figure 508.

Figure 508
Message reply: accepted

```
<xml>
<msgrpy>
<id>bc6c51d001c0ff0700000004.eml</id>
<sts>ACK^</sts>
</msgrpy>
</xml>
```

Upon receiving this acknowledgement, the eSMTP_server moves the original mail message to a processed location, unless the target directory is set to a value of *NONE. Figure 509 shows the target folder for accepted messages.

Figure 509
Specifying the location to file accepted messages



Address C:\Inetpub\mailroot\Drop\processed

Name	Size	Type
bc6c51d001c0ff0...	8 KB	Internet E-Ma

bc6c51d001c0ff0700000004.eml
Type: Internet E-Mail Message
Size: 7,29 KB

1 object(s) (Disk free space: 4,20 GB) 7,29 KB

- **Message Rejected**

If the message is not accepted in eKERNEL, a negative reply is sent, as shown in Figure 510.

Figure 510
Message reply: rejected

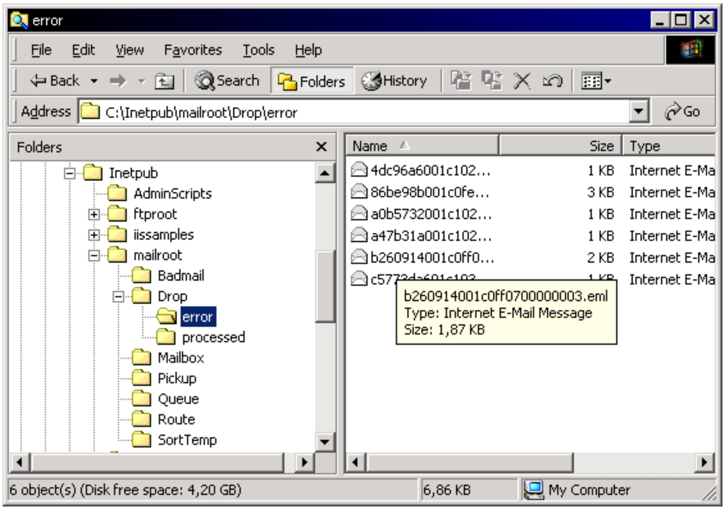
```
<xml>
<msgrpy>
<id>bc6c51d001c0ff0700000004.eml</id>
<sts>NACK^</sts>
</msgrpy>
</xml>
```

Refer to the log files of eKERNEL (see the **eKERNEL > Logging** tab) to find out why the message was not accepted. Following is an example of the informational message that is shown:

```
S: Alarm not processed. Unknown group in eKERNEL_GROUP table! Auto create
group for eSMTP_server is set to False.
```

Upon reception of this negative acknowledge (NACK), the eSMTP_server moves the original mail message to an error location, unless the target directory is set to a value of *NONE. Figure 511 on page 1200 shows the target folder for rejected messages.

Figure 511
Specifying the error target directory



Address: C:\Inetpub\mailroot\Drop\error

Name	Size	Type
4dc96a6001c102...	1 KB	Internet E-Ma
86be98b001c0fe...	3 KB	Internet E-Ma
a0b5732001c102...	1 KB	Internet E-Ma
a47b31a001c102...	1 KB	Internet E-Ma
b260914001c0ff0...	2 KB	Internet E-Ma
c577[illegible]	[illegible]	Internet E-Ma

b260914001c0ff0700000003.eml
Type: Internet E-Mail Message
Size: 1,87 KB

6 object(s) (Disk free space: 4,20 GB) | 6,86 KB | My Computer

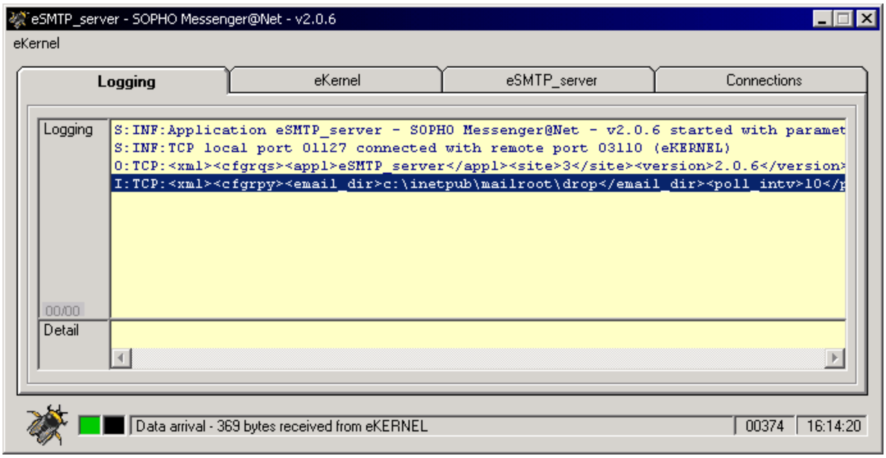
> ***Note:*** Because these rejected inbound mail messages are still available online, you can let the administrator determine the cause of the problem, and if necessary adjust the configuration settings. In many cases the problems are related to wrong configuration, or processing of unexpected mail messages (spawn mail, hackers, and so on). After the configuration s fixed, the messages in error can be either deleted or moved back to the Dropped directory for reprocessing.

Logging

The eSMTP_server application provides logging both on-screen and on disk.

Figure 512 on page 1201 shows the on-screen logging that can be found in the Logging tab.

Figure 512
On-screen logging



```
S:INF:Application eSMTP_server - SOPHO Messenger@Net - v2.0.6 started with paramet
S:INF:TCP local port 01127 connected with remote port 03110 (eKERNEL)
O:TCP:<xml><cfgrqs><appl>eSMTP_server</appl><site>3</site><version>2.0.6</version>
I:TCP:<xml><cfgrpy><email_dir>c:\inetpub\mailroot\drop</email_dir><poll_intv>10</p
```

Data arrival - 369 bytes received from eKERNEL | 00374 | 16:14:20

Figure 513 on page 1202 shows the log file stored on disk.

Figure 513
Log file on disk

```
28/10/2001 16:08:07 - S:INF:Application eSMTP_server - SOPHO Messen-
ger@Net - v2.0.6 started with parameters /Site:3 /eKernel address:*LOCAL
/eKernel port:3110 /Log drive:C
28/10/2001 16:08:08 - S:INF:TCP local port 01127 connected with remote
port 03110 (eKERNEL)
28/10/2001 16:08:08 - O:TCP:<xml><cfgrqs><appl>eSMTP_server</ap-
pl><site>3</site><version>2.0.6</version></cfgrqs></xml>
28/10/2001 16:08:08 - I:TCP:<xml><cfgrpy><email_dir>c:\inetpub\mail-
root\drop</email_dir><poll_intv>10</
poll_intv><email_dir_processed>c:\inetpub\mailroot\drop\processed</
email_dir_processed><keep_processed>5</
keep_processed><email_dir_error>c:\inetpub\mailroot\drop\error</
email_dir_error><keep_error>5</keep_error><log_path>C:\SOPHO Messen-
ger@net</log_path><log_days>1</log_days></cfgrpy></xml>

28/10/2001 16:20:02 - O:TCP:<xml><pgmsts><value>Shutdown</value></
pgmsts></xml>
28/10/2001 16:20:02 - S:INF:Application ended
28/10/2001 16:22:18 - S:INF:Application eSMTP_server - SOPHO Messen-
ger@Net - v2.0.7 started with parameters /Site:3 /eKernel address:*LOCAL
/eKernel port:3110 /Log drive:C
28/10/2001 16:22:19 - S:INF:TCP local port 01128 connected with remote
port 03110 (eKERNEL)
28/10/2001 16:22:19 - O:TCP:<xml><cfgrqs><appl>eSMTP_server</ap-
pl><site>3</site></cfgrqs></xml>
28/10/2001 16:22:20 - I:TCP:<xml><cfgrpy><email_dir>c:\inetpub\mail-
root\drop</email_dir><poll_intv>10</
poll_intv><email_dir_processed>c:\inetpub\mailroot\drop\processed</
email_dir_processed><keep_processed>5</
keep_processed><email_dir_error>c:\inetpub\mailroot\drop\error</
email_dir_error><keep_error>5</keep_error><log_path>C:\SOPHO Messen-
ger@net</log_path><log_days>1</log_days></cfgrpy></xml>

28/10/2001 16:53:21 - O:TCP:<xml><ms-
grqs><id>bc6c51d001c0ff0700000004.eml</id><from>beibsbru@ibsbe.be</
from><to>befmi@gntn1sfmi.ibsbe.be</to><subject>Subject goes here</sub-
ject></msgrqs></xml>
```

continued on the next page...

Log file on disk (continued)

```
28/10/2001 16:53:21 - I:TCP:<xml><ms-
grpy><id>bc6c51d001c0ff0700000004.eml</id><sts>NACK^</sts></msgrpy></
xml>

28/10/2001 17:00:10 - O:TCP:<xml><ms-
grqs><id>c5773da601c103b900000004.eml</id><from>francis.missi-
aen@1s.be</from><to>kristien.daneels@1s.be</to><subject>Reanimation</
subject></msgrqs></xml>
28/10/2001 17:00:11 - I:TCP:<xml><ms-
grpy><id>c5773da601c103b900000004.eml</id><sts>NACK^</sts></msgrpy></
xml>

28/10/2001 17:03:25 - O:TCP:<xml><ms-
grqs><id>c5773da601c103b900000004.eml</id><from>francis.missi-
aen@1s.be</from><to>kristien.daneels@1s.be</to><subject>Reanimation</
subject></msgrqs></xml>
28/10/2001 17:03:26 - I:TCP:<xml><ms-
grpy><id>c5773da601c103b900000004.eml</id><sts>NACK^</sts></msgrpy></
xml>

28/10/2001 17:07:00 - O:TCP:<xml><ms-
grqs><id>c5773da601c103b900000004.eml</id><from>francis.missi-
aen@1s.be</from><to>kristien.daneels@1s.be</to><subject>Reanimation</
subject></msgrqs></xml>
28/10/2001 17:07:00 - I:TCP:<xml><ms-
grpy><id>c5773da601c103b900000004.eml</id><sts>NACK^</sts></msgrpy></
xml>

28/10/2001 17:07:39 - O:TCP:<xml><pgmsts><value>Shutdown</value></
pgmsts></xml>
28/10/2001 17:07:39 - S:INF:Application ended
28/10/2001 17:09:06 - S:INF:Application eSMTP_server - SOPHO Messen-
ger@Net - v2.0.7 started with parameters /Site:3 /eKernel address:*LOCAL
/eKernel port:3110 /Log drive:C
28/10/2001 17:09:08 - S:INF:TCP local port 01129 connected with remote
port 03110 (eKERNEL)
28/10/2001 17:09:08 - O:TCP:<xml><cfgrqs><appl>eSMTP_server</ap-
pl><site>3</site></cfgrqs></xml>
```

continued on the next page...

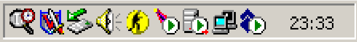
Log file on disk (continued)

```
28/10/2001 17:09:08 - I:TCP:<xml><cfgrpy><email_dir>c:\inetpub\mail-
root\drop</email_dir><poll_intv>10</
poll_intv><email_dir_processed>c:\inetpub\mailroot\drop\processed</
email_dir_processed><keep_processed>5</
keep_processed><email_dir_error>c:\inetpub\mailroot\drop\error</
email_dir_error><keep_error>5</keep_error><log_path>C:\SOPHO Messen-
ger@net</log_path><log_days>1</log_days></cfgrpy></xml>

28/10/2001 17:09:29 - O:TCP:<xml><ms-
grqs><id>c5773da601c103b900000004.eml</id><from>francis.missi-
aen@1s.be</from><to>kristien.daneels@1s.be</to><subject>Reanimation</
subject></msgrqs></xml>
28/10/2001 17:09:29 - I:TCP:<xml><ms-
grpy><id>c5773da601c103b900000004.eml</id><sts>ACK^</sts></msgrpy></
xml>
```

Module – eTM

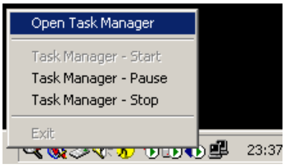
The module eTM is an application that is represented as a small icon in the system tray on the bottom right-hand side of the desktop. This tray is usually populated with other applications, as shown in Figure 514, where the eTM icon is shown to the immediate left of the clock.

Figure 514
System Tray



When the mouse is moved over the icon in the system tray, right-click to open the menu shown in Figure 515.

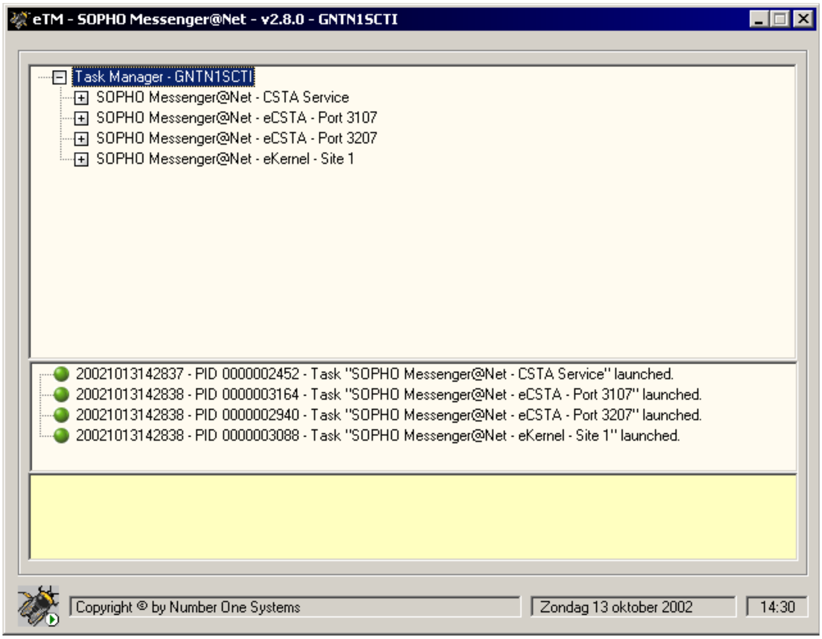
Figure 515
Open Task Manager



The menu option **Open Task Manager** restores the main menu, and can be opened to monitor the tasks in detail. This menu also provides options to **Start**, **Stop**, or **Pause** processing. Use the **Exit** menu option to terminate the eTM module and all associated tasks.

Select the **Open Task Manager** menu option in the pop-up menu, to open the Task Manager, as shown in Figure 516 on page 1206.

Figure 516
eTM Task Manager



eTM - SOPHO Messenger@Net - v2.8.0 - GNTN1SCTI

- ⊟ Task Manager - GNTN1SCTI
  - ⊞ SOPHO Messenger@Net - CSTA Service
  - ⊞ SOPHO Messenger@Net - eCSTA - Port 3107
  - ⊞ SOPHO Messenger@Net - eCSTA - Port 3207
  - ⊞ SOPHO Messenger@Net - eKernel - Site 1

```
● 20021013142837 - PID 0000002452 - Task "SOPHO Messenger@Net - CSTA Service" launched.
● 20021013142838 - PID 0000003164 - Task "SOPHO Messenger@Net - eCSTA - Port 3107" launched.
● 20021013142838 - PID 0000002940 - Task "SOPHO Messenger@Net - eCSTA - Port 3207" launched.
● 20021013142838 - PID 0000003088 - Task "SOPHO Messenger@Net - eKernel - Site 1" launched.
```

Copyright © by Number One Systems | Zondag 13 oktober 2002 | 14:30

> ***Note:*** The window contents vary according to your configuration settings.

The window is composed of the following sections:

- The upper section presents a tree-view of the environment, and contains a hierarchical overview of all configured tasks. Every task has the following keywords and values:
  - — The keyword PID denotes the process identifier of the task. This identifier is formatted as a 10-digit numeric value. The PID is the value that is also shown when the system supplied Task Manager of Microsoft is used to represent the processes. A special value 0000000000 is shown when the task is not running.

- — The keyword Window style denotes the style of the window of the task. Supported values are described in Table 63.

Table 63
Supported window styles

Value	Description
0	Window is hidden and focus is passed to the hidden window.
1	Window has focus and is restored to its original size and position.
2	Window is displayed as an icon with focus.
3	Window is maximized with focus.
4	Window is restored to its most recent size and position. The currently active window remains active.
6	Window is displayed as an icon. The currently active window remains active.

- — The keyword Shortcut denotes the command line parameter that is used to launch the process.

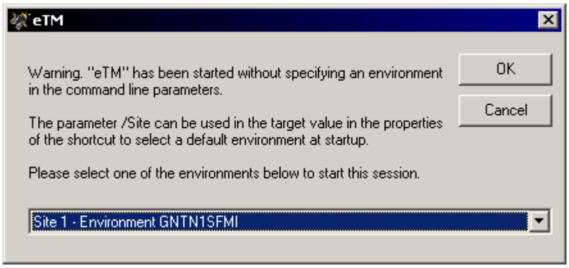
- The second section shows a log of the changes in the state of the tasks.
- The third section shows some additional logging information, and is updated when, for instance, a task is terminated from within the eTM application.
- The bottom section shows on the left a small icon that denotes the current state of the eTM. This application can be started, paused or stopped.

The eTM is launched by means of the following command:

```
C:\SOPHO Messenger@Net\Exe\eTM.exe
```

In most cases there is only one environment configured, and the eTM uses this default configuration. When there is more than one environment configured, a selection window opens that allows you to specify the environment that must be started, as shown in Figure 517 on page 1208.

Figure 517
Specify the eTM environment (when more than one is configured)


eTM

Warning. "eTM" has been started without specifying an environment in the command line parameters.

The parameter /Site can be used in the target value in the properties of the shortcut to select a default environment at startup.

Please select one of the environments below to start this session.

Site 1 - Environment GNTN1SFMI

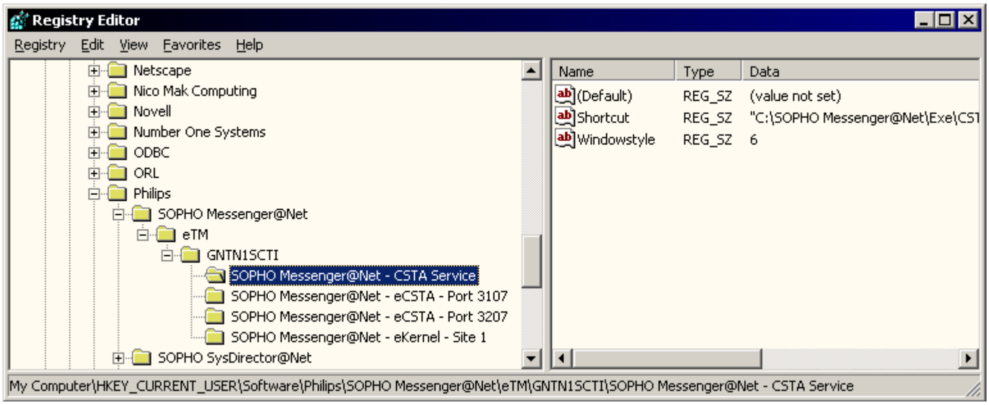
If there is more than one environment configured, you can choose to automatically select a start-up environment. This can be accomplished by extending the launch command with the keyword /Site:xxxxx, where xxxxx is to be replaced by the configured environment name. For example, the following command automatically launches the eTM for environment GNTN1SFMI.

```
C:\SOPHO Messenger@Net\Exe\eTM.exe /Site:GNTN1SFMI
```

The Windows Registry Editor (regedit or regedt32) can be used to maintain the configuration of the eTM.

Figure 518 on page 1209 shows a sample configuration, as represented in the system registry as a result of the configuration process.

Figure 518
Sample eTM configuration registry entry



```
Netscape
Nico Mak Computing
Novell
Number One Systems
ODBC
ORL
Philips
    SOPHO Messenger@Net
        eTM
            GNTN1SCTI
                SOPHO Messenger@Net - CSTA Service
                SOPHO Messenger@Net - eCSTA - Port 3107
                SOPHO Messenger@Net - eCSTA - Port 3207
                SOPHO Messenger@Net - eKernel - Site 1
    SOPHO SysDirector@Net
```

Name	Type	Data
(Default)	REG_SZ	(value not set)
Shortcut	REG_SZ	"C:\SOPHO Messenger@Net\Exe\CST
Windowstyle	REG_SZ	6

My Computer\HKEY_CURRENT_USER\Software\Philips\SOPHO Messenger@Net\eTM\GNTN1SCTI\SOPHO Messenger@Net - CSTA Service

Figure 519 on page 1210 shows a sample configuration for the eTM module that defines the following:

- One instance of CSTA_Service.exe
- One instance of eKERNEL.exe

The text file represented in Figure 519 on page 1210 has a filename with extension .reg and can be created with a text editor (for example, Notepad).

Figure 519
Sample eTM configuration

```
Windows Registry Editor Version 5.00

[HKEY_CURRENT_USER\Software\Philips\SOPHO Messenger@Net]

[HKEY_CURRENT_USER\Software\Philips\SOPHO Messenger@Net\eTM]

[HKEY_CURRENT_USER\Software\Philips\SOPHO Messenger@Net\eTM\GNTN1SCTI]

[HKEY_CURRENT_USER\Software\Philips\SOPHO Messen-
ger@Net\eTM\GNTN1SCTI\SOPHO Messenger@Net - CSTA Service]
"Shortcut"="\"C:\\SOPHO Messenger@Net\\Exe\\CSTA_service.exe\""
"Windowstyle"="6"

[HKEY_CURRENT_USER\Software\Philips\SOPHO Messen-
ger@Net\eTM\GNTN1SCTI\SOPHO Messenger@Net - eKernel - Site 1]
"Shortcut"="\"C:\\SOPHO Messenger@Net\\Exe\\eKERNEL.exe\" /Site:1"
"Windowstyle"="6"
```

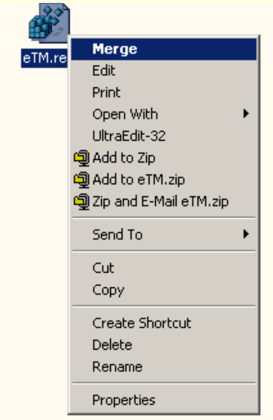
Files with .reg extension can be merged to the registry.

Procedure 241
Merging .reg files (Part 1 of 2)

<table>
<tr><th>Step</th><th>Action</th></tr>
<tr><td></td><td></td></tr>
<tr><td>1</td><td>Select the Merge command.</td></tr>
<tr><td></td><td>

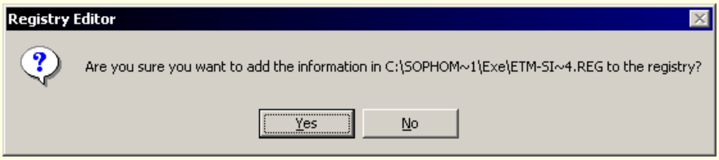
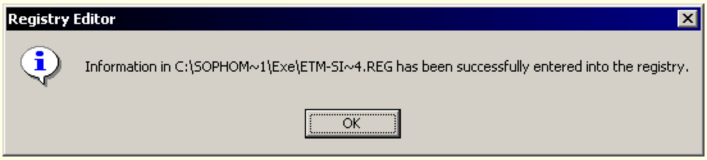
In Windows Explorer:

- Locate the file you want to merge.
- Right-click the file.
- Choose **Merge** from the pop-up menu, as follows**:**



</td></tr>
<tr><td></td><td></td></tr>
</table>

Procedure 241
Merging .reg files (Part 2 of 2)

Step	Action
2	Confirm that you wish to merge the registry.
	Click **Yes** to continue.  Registry Editor Are you sure you want to add the information in C:\SOPHOM~1\Exe\ETM-SI~4.REG to the registry?
3	Confirm completion of the registry merge.
	Click **OK**.  Registry Editor Information in C:\SOPHOM~1\Exe\ETM-SI~4.REG has been successfully entered into the registry.
	END

The command RegEdit or RegEdt32 can be used to verify the configuration, or to apply changes to an existing configuration.

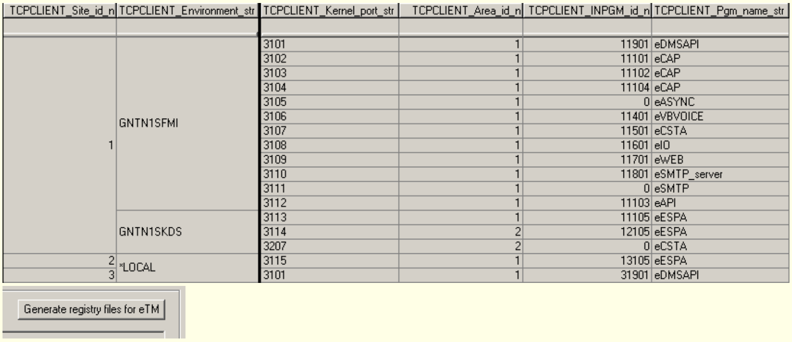
A future release of DECT Messenger will provide automatic procedures for configuring the Task Manager from the Configurator module.

In current release the eGRID module features a command button **Generate registry files for eTM**. Click this button to read the eKERNEL_TCPCLIENT table and automatically generate the required shortcuts for each site and environment, as shown in Figure 242.

Procedure 242
Generate shortcuts

Step	Action
1	Use eGRID to generate registry files for eTM.

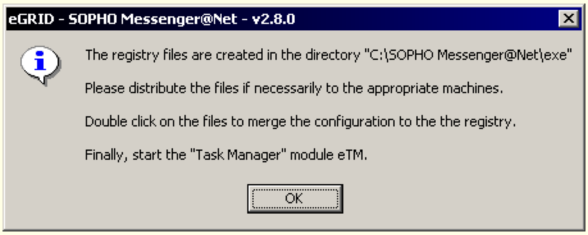
Launch eGRID and click **Generate registry files for eTM**.



TCPCLIENT_Site_id_n	TCPCLIENT_Environment_str	TCPCLIENT_Kernel_port_str	TCPCLIENT_Area_id_n	TCPCLIENT_INPGM_id_n	TCPCLIENT_Pgm_name_str
1	GNTN1SFMI	3101	1	11901	eDMSAPI
		3102	1	11101	eCAP
		3103	1	11102	eCAP
		3104	1	11104	eCAP
		3105	1	0	eASYNC
		3106	1	11401	eVBVOICE
		3107	1	11501	eCSTA
		3108	1	11601	eIO
		3109	1	11701	eWEB
		3110	1	11801	eSMTP_server
		3111	1	0	eSMTP
		3112	1	11103	eAPI
	GNTN1SKDS	3113	1	11105	eESPA
		3114	2	12105	eESPA
		3207	2	0	eCSTA
2	*LOCAL	3115	1	13105	eESPA
3		3101	1	31901	eDMSAPI

Step	Action
2	Review the information provided, and acknowledge completion of the process.

Click **OK** to continue.



eGRID - SOPHO Messenger@Net - v2.8.0

The registry files are created in the directory "C:\SOPHO Messenger@Net\exe"

Please distribute the files if necessarily to the appropriate machines.

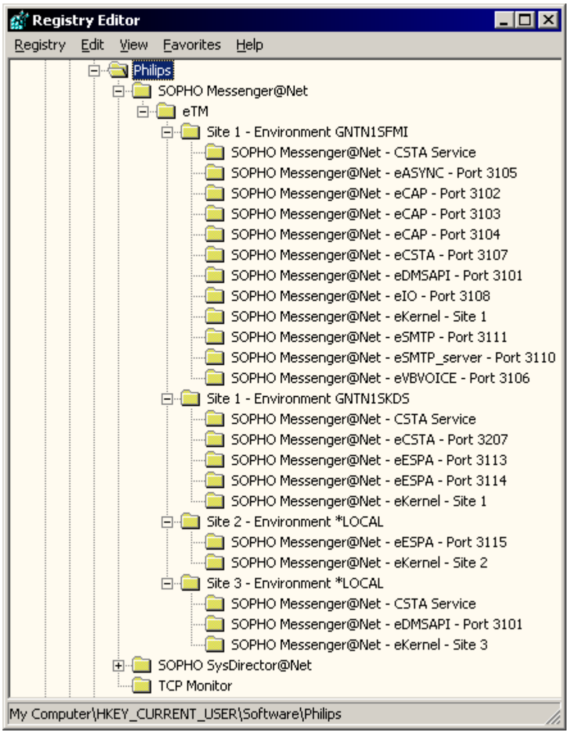
Double click on the files to merge the configuration to the the registry.

Finally, start the "Task Manager" module eTM.

END

Figure 520 on page 1214 shows a configuration of four environments.

Figure 520
Example of configuration of four environments



```
Philips
  SOPHO Messenger@Net
    eTM
      Site 1 - Environment GNTN1SFMI
        SOPHO Messenger@Net - CSTA Service
        SOPHO Messenger@Net - eASYNC - Port 3105
        SOPHO Messenger@Net - eCAP - Port 3102
        SOPHO Messenger@Net - eCAP - Port 3103
        SOPHO Messenger@Net - eCAP - Port 3104
        SOPHO Messenger@Net - eCSTA - Port 3107
        SOPHO Messenger@Net - eDMSAPI - Port 3101
        SOPHO Messenger@Net - eIO - Port 3108
        SOPHO Messenger@Net - eKernel - Site 1
        SOPHO Messenger@Net - eSMTP - Port 3111
        SOPHO Messenger@Net - eSMTP_server - Port 3110
        SOPHO Messenger@Net - eVBVOICE - Port 3106
      Site 1 - Environment GNTN1SKDS
        SOPHO Messenger@Net - CSTA Service
        SOPHO Messenger@Net - eCSTA - Port 3207
        SOPHO Messenger@Net - eESPA - Port 3113
        SOPHO Messenger@Net - eESPA - Port 3114
        SOPHO Messenger@Net - eKernel - Site 1
      Site 2 - Environment *LOCAL
        SOPHO Messenger@Net - eESPA - Port 3115
        SOPHO Messenger@Net - eKernel - Site 2
      Site 3 - Environment *LOCAL
        SOPHO Messenger@Net - CSTA Service
        SOPHO Messenger@Net - eDMSAPI - Port 3101
        SOPHO Messenger@Net - eKernel - Site 3
  SOPHO SysDirector@Net
  TCP Monitor
```

My Computer\HKEY_CURRENT_USER\Software\Philips

- Site 1
  - — Environment GNTN1SFMI
  - — Environment GNTN1SKDS
- Site 2
  - — Environment *LOCAL
- Site 3
  - — Environment *LOCAL

The first two environments reside on site 1, the other environments reside on other sites. In this example, the modules of site 1 are distributed across two environments (two separate PC platforms). The PC with environment

GNTN1SFMI contains a full-featured installation with one or more instances of each module; the second environment GNTN1SKDS contains a subset of the modules only. Figure 521 on page 1216 shows the registry file corresponding to the foregoing example.

Figure 521
eTM - Site 1 - Environment GNTN1SFMI.reg

```
Windows Registry Editor Version 5.00

[HKEY_CURRENT_USER\Software\Philips\SOPHO Messenger@Net]

[HKEY_CURRENT_USER\Software\Philips\SOPHO Messenger@Net\eTM]

[HKEY_CURRENT_USER\Software\Philips\SOPHO Messenger@Net\eTM\Site 1 -
Environment GNTN1SFMI]

[HKEY_CURRENT_USER\Software\Philips\SOPHO Messenger@Net\eTM\Site 1 -
Environment GNTN1SFMI\SOPHO Messenger@Net - eKernel - Site 1]
"Shortcut"="\"C:\\SOPHO Messenger@Net\\Exe\\eKERNEL.exe\" /Site:1"
"Windowstyle"="6"

[HKEY_CURRENT_USER\Software\Philips\SOPHO Messenger@Net\eTM\Site 1 -
Environment GNTN1SFMI\SOPHO Messenger@Net - eSMTP_server - Port 3110]
"Shortcut"="\"C:\\SOPHO Messenger@Net\\Exe\\eSMTP_server.exe\" /Site:1
/eKernel address:GNTN1SFMI /eKernel port:3110 /Log drive:C"
"Windowstyle"="6"

[HKEY_CURRENT_USER\Software\Philips\SOPHO Messenger@Net\eTM\Site 1 -
Environment GNTN1SFMI\SOPHO Messenger@Net - eCAP - Port 3102]
"Shortcut"="\"C:\\SOPHO Messenger@Net\\Exe\\eCAP.exe\" /Site:1 /eKernel
address:GNTN1SFMI /eKernel port:3102 /Log drive:C"
"Windowstyle"="6"

[HKEY_CURRENT_USER\Software\Philips\SOPHO Messenger@Net\eTM\Site 1 -
Environment GNTN1SFMI\SOPHO Messenger@Net - eCAP - Port 3103]
"Shortcut"="\"C:\\SOPHO Messenger@Net\\Exe\\eCAP.exe\" /Site:1 /eKernel
address:GNTN1SFMI /eKernel port:3103 /Log drive:C"
"Windowstyle"="6"

[HKEY_CURRENT_USER\Software\Philips\SOPHO Messenger@Net\eTM\Site 1 -
Environment GNTN1SFMI\SOPHO Messenger@Net - eCAP - Port 3104]
"Shortcut"="\"C:\\SOPHO Messenger@Net\\Exe\\eCAP.exe\" /Site:1 /eKernel
address:GNTN1SFMI /eKernel port:3104 /Log drive:C"
"Windowstyle"="6"
```

continued on next page...

eTM - Site 1 - Environment GNTN1SFMI.reg (continued)

```
[HKEY_CURRENT_USER\Software\Philips\SOPHO Messenger@Net\eTM\Site 1 -
Environment GNTN1SFMI\SOPHO Messenger@Net - eASYNC - Port 3105]
"Shortcut"="\"C:\\SOPHO Messenger@Net\\Exe\\eASYNC.exe\" /Site:1 /eKer-
nel address:GNTN1SFMI /eKernel port:3105 /Log drive:C"
"Windowstyle"="6"

[HKEY_CURRENT_USER\Software\Philips\SOPHO Messenger@Net\eTM\Site 1 -
Environment GNTN1SFMI\SOPHO Messenger@Net - CSTA Service]
"Shortcut"="\"C:\\SOPHO Messenger@Net\\Exe\\CSTA_Service.exe\""
"Windowstyle"="6"

[HKEY_CURRENT_USER\Software\Philips\SOPHO Messenger@Net\eTM\Site 1 -
Environment GNTN1SFMI\SOPHO Messenger@Net - eDMSAPI - Port 3101]
"Shortcut"="\"C:\\SOPHO Messenger@Net\\Exe\\eDMSAPI.exe\" /Site:1 /eK-
ernel address:GNTN1SFMI /eKernel port:3101 /Log drive:C"
"Windowstyle"="6"

[HKEY_CURRENT_USER\Software\Philips\SOPHO Messenger@Net\eTM\Site 1 -
Environment GNTN1SFMI\SOPHO Messenger@Net - eSMTP - Port 3111]
"Shortcut"="\"C:\\SOPHO Messenger@Net\\Exe\\eSMTP.exe\" /Site:1 /eKer-
nel address:GNTN1SFMI /eKernel port:3111 /Log drive:C"
"Windowstyle"="6"

[HKEY_CURRENT_USER\Software\Philips\SOPHO Messenger@Net\eTM\Site 1 -
Environment GNTN1SFMI\SOPHO Messenger@Net - eIO - Port 3108]
"Shortcut"="\"C:\\SOPHO Messenger@Net\\Exe\\eIO.exe\" /Site:1 /eKernel
address:GNTN1SFMI /eKernel port:3108 /Log drive:C"
"Windowstyle"="6"
```

Figure 522
eTM - Site 1 - Environment GNTN1SKDS.reg

```
Windows Registry Editor Version 5.00

[HKEY_CURRENT_USER\Software\Philips\SOPHO Messenger@Net]

[HKEY_CURRENT_USER\Software\Philips\SOPHO Messenger@Net\eTM]

[HKEY_CURRENT_USER\Software\Philips\SOPHO Messenger@Net\eTM\Site 1 - Environment
GNTN1SKDS]

[HKEY_CURRENT_USER\Software\Philips\SOPHO Messenger@Net\eTM\Site 1 - Environment
GNTN1SKDS\SOPHO Messenger@Net - eKernel - Site 1]
"Shortcut"="\"C:\\SOPHO Messenger@Net\\Exe\\eKERNEL.exe\" /Site:1"
"Windowstyle"="6"

[HKEY_CURRENT_USER\Software\Philips\SOPHO Messenger@Net\eTM\Site 1 - Environment
GNTN1SKDS\SOPHO Messenger@Net - eESPA - Port 3113]
"Shortcut"="\"C:\\SOPHO Messenger@Net\\Exe\\eESPA.exe\" /Site:1 /eKernel address:GNTN1SKDS /
eKernel port:3113 /Log drive:C"
"Windowstyle"="6"

[HKEY_CURRENT_USER\Software\Philips\SOPHO Messenger@Net\eTM\Site 1 - Environment
GNTN1SKDS\SOPHO Messenger@Net - eESPA - Port 3114]
"Shortcut"="\"C:\\SOPHO Messenger@Net\\Exe\\eESPA.exe\" /Site:1 /eKernel address:GNTN1SKDS /
eKernel port:3114 /Log drive:C"
"Windowstyle"="6"

[HKEY_CURRENT_USER\Software\Philips\SOPHO Messenger@Net\eTM\Site 1 - Environment
GNTN1SKDS\SOPHO Messenger@Net - CSTA Service]
"Shortcut"="\"C:\\SOPHO Messenger@Net\\Exe\\CSTA_Service.exe\""
"Windowstyle"="6"
```

Figure 523
eTM - Site 2 - Environment LOCAL.reg

```
Windows Registry Editor Version 5.00

[HKEY_CURRENT_USER\Software\Philips\SOPHO Messenger@Net]

[HKEY_CURRENT_USER\Software\Philips\SOPHO Messenger@Net\eTM]

[HKEY_CURRENT_USER\Software\Philips\SOPHO Messenger@Net\eTM\Site 2 - Environment *LOCAL]

[HKEY_CURRENT_USER\Software\Philips\SOPHO Messenger@Net\eTM\Site 2 - Environment *LOCAL\SOPHO Messenger@Net - eKernel - Site 2]
"Shortcut"="\"C:\\SOPHO Messenger@Net\\Exe\\eKERNEL.exe\" /Site:2"
"Windowstyle"="6"

[HKEY_CURRENT_USER\Software\Philips\SOPHO Messenger@Net\eTM\Site 2 - Environment *LOCAL\SOPHO Messenger@Net - eESPA - Port 3115]
"Shortcut"="\"C:\\SOPHO Messenger@Net\\Exe\\eESPA.exe\" /Site:2 /eKernel address:*LOCAL /eKernel port:3115 /Log drive:C"
"Windowstyle"="6"
```

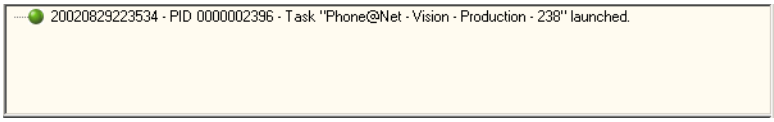
Figure 524
eTM - Site 3 - Environment LOCAL.reg

```
Windows Registry Editor Version 5.00

[HKEY_CURRENT_USER\Software\Philips\SOPHO Messenger@Net]

[HKEY_CURRENT_USER\Software\Philips\SOPHO Messenger@Net\eTM]

[HKEY_CURRENT_USER\Software\Philips\SOPHO Messenger@Net\eTM\Site 3 - Environment *LOCAL]

[HKEY_CURRENT_USER\Software\Philips\SOPHO Messenger@Net\eTM\Site 3 - Environment *LOCAL\SOPHO Messenger@Net - eKernel - Site 3]
"Shortcut"="\"C:\\SOPHO Messenger@Net\\Exe\\eKERNEL.exe\" /Site:3"
"Windowstyle"="6"

[HKEY_CURRENT_USER\Software\Philips\SOPHO Messenger@Net\eTM\Site 3 - Environment *LOCAL\SOPHO Messenger@Net - eDMSAPI - Port 3101]
"Shortcut"="\"C:\\SOPHO Messenger@Net\\Exe\\eDMSAPI.exe\" /Site:3 /eKernel address:*LOCAL /eKernel port:3101 /Log drive:C"
"Windowstyle"="6"

[HKEY_CURRENT_USER\Software\Philips\SOPHO Messenger@Net\eTM\Site 3 - Environment *LOCAL\SOPHO Messenger@Net - CSTA Service]
"Shortcut"="\"C:\\SOPHO Messenger@Net\\Exe\\CSTA_Service.exe\""
"Windowstyle"="6"
```

At start-up, the eTM retrieves the configuration, and launches all tasks that are defined in the environment according to the configuration. As shown in the example in Figure 524, the environment GNTN1SCTI launches the DECT Messenger modules CSTA Server, and the module eKERNEL.

When a task is successfully launched, the logging section features a green icon indicating a normal condition, as shown in Figure 525 on page 1220.

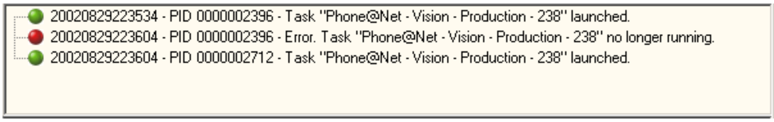
Figure 525
Green icon indicates Normal Condition



● 20020829223534 - PID 0000002396 - Task "Phone@Net - Vision - Production - 238" launched.

When the task is ended — for example, by means of the Alt-F4 keystroke combination — the eTM detects this and relaunches the missing task. This is indicated in the log as shown in Figure 526.

Figure 526
Red icon indicates a task that is no longer running

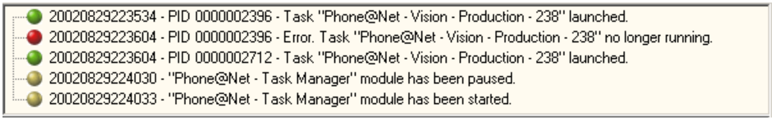


```
🟢 20020829223534 - PID 0000002396 - Task "Phone@Net - Vision - Production - 238" launched.
🔴 20020829223604 - PID 0000002396 - Error. Task "Phone@Net - Vision - Production - 238" no longer running.
🟢 20020829223604 - PID 0000002712 - Task "Phone@Net - Vision - Production - 238" launched.
```

eTM checks every five seconds to ensure that each task is still running. When the eTM is paused or stopped, the routine that verifies and restarts the process is temporarily interrupted.

This interruption usually occurs during maintenance of one of more of the programs that are guarded by the eTM. Such a temporary condition is shown in the log as illustrated in Figure 527.

Figure 527
Yellow icon indicates a task that is paused



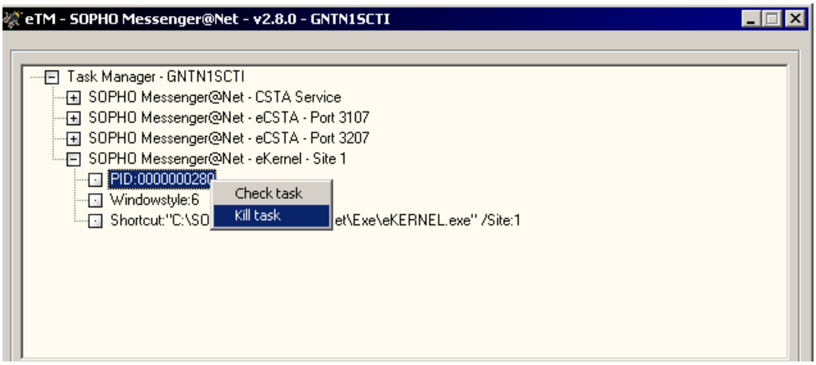
```
🟢 20020829223534 - PID 0000002396 - Task "Phone@Net - Vision - Production - 238" launched.
🔴 20020829223604 - PID 0000002396 - Error. Task "Phone@Net - Vision - Production - 238" no longer running.
🟢 20020829223604 - PID 0000002712 - Task "Phone@Net - Vision - Production - 238" launched.
🟡 20020829224030 - "Phone@Net - Task Manager" module has been paused.
🟡 20020829224033 - "Phone@Net - Task Manager" module has been started.
```

A system administrator can also terminate a task from within the eTM_HA environment using a **Terminate process** API-call.

> ***Note:*** Using the **Terminate process** API-call can cause data loss, as this does not provide any graceful cleanup or shutdown of the associated program.

To terminate a process, use the menu **Kill task** option, as shown in Figure 528 on page 1222. The **Kill task** option is available only when the tree-view is expanded and the mouse is right-clicked on the PID:xxxxxxxxxx line.

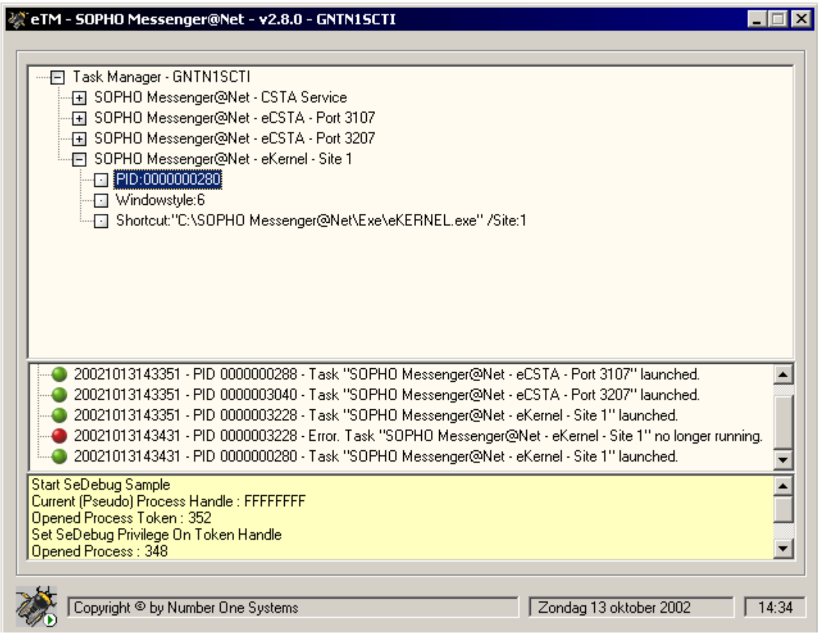
Figure 528
Kill Task



```
⊟ Task Manager - GNTN1SCTI
   ⊞ SOPHO Messenger@Net - CSTA Service
   ⊞ SOPHO Messenger@Net - eCSTA - Port 3107
   ⊞ SOPHO Messenger@Net - eCSTA - Port 3207
   ⊟ SOPHO Messenger@Net - eKernel - Site 1
      · PID:0000000280
      · Windowstyle:6
      · Shortcut:"C:\SO            et\Exe\eKERNEL.exe" /Site:1
```

When **Kill task** is clicked, the running task is terminated, as shown in Figure 529.

Figure 529
A task is terminated



```
⊟ Task Manager - GNTN1SCTI
   ⊞ SOPHO Messenger@Net - CSTA Service
   ⊞ SOPHO Messenger@Net - eCSTA - Port 3107
   ⊞ SOPHO Messenger@Net - eCSTA - Port 3207
   ⊟ SOPHO Messenger@Net - eKernel - Site 1
      · PID:0000000280
      · Windowstyle:6
      · Shortcut:"C:\SOPHO Messenger@Net\Exe\eKERNEL.exe" /Site:1
```

```
● 20021013143351 - PID 0000000288 - Task "SOPHO Messenger@Net - eCSTA - Port 3107" launched.
● 20021013143351 - PID 0000003040 - Task "SOPHO Messenger@Net - eCSTA - Port 3207" launched.
● 20021013143351 - PID 0000003228 - Task "SOPHO Messenger@Net - eKernel - Site 1" launched.
● 20021013143431 - PID 0000003228 - Error. Task "SOPHO Messenger@Net - eKernel - Site 1" no longer running.
● 20021013143431 - PID 0000000280 - Task "SOPHO Messenger@Net - eKernel - Site 1" launched.
```

```
Start SeDebug Sample
Current (Pseudo) Process Handle : FFFFFFFF
Opened Process Token : 352
Set SeDebug Privilege On Token Handle
Opened Process : 348
```

Copyright © by Number One Systems | Zondag 13 oktober 2002 | 14:34

> ***Note:*** When the eTM is running, the system re-launches the terminated tasks within 10 seconds.

When the eTM form is closed through the control box on the right top of the form, the application does not shut down, but is instead minimised to an icon in the system tray. This function is designed to prevent the user from accidentally closing the eTM and associated tasks. This approach is similar to monitoring applications of other vendors, such as the Apache Monitor or the SQL Server Service Manager.

Shutting down eTM_HA

The eTM can be shut down by opening the pop-up menu shown in Figure 515 on page 1205, and choosing the **Exit** menu option.

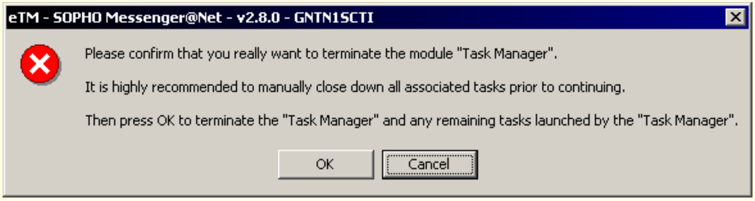
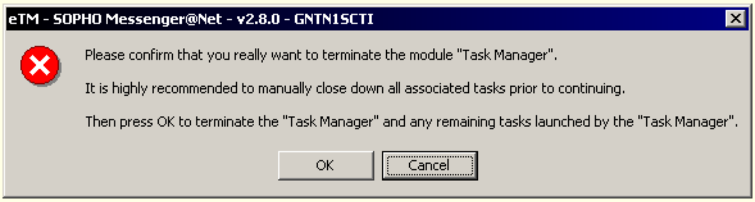
IMPORTANT!

Nortel recommends that you close applications using shut down or exit/close options in the applications themselves, to ensure a clean shutdown. This helps to protect volatile data, properly close down serial and sockets communications, free resources, clean up garbage, and so on. To stop processes gracefully, follow the steps described in Procedure 243.

Procedure 243
Shutting down eTM (Part 1 of 2)

Step	Action
1	Open the eTM_HA pop-up menu.
	Right-click the eTM_HA icon in the system tray.

Procedure 243
Shutting down eTM (Part 2 of 2)

Step	Action
2	Stop the eTM_HA.
	- Choose the menu item **Task Manager - Stop**. - Choose the menu item **Exit**. The following confirmation prompt is shown; do not click **OK** or **Cancel** yet:  eTM - SOPHO Messenger@Net - v2.8.0 - GNTN1SCTI Please confirm that you really want to terminate the module "Task Manager". It is highly recommended to manually close down all associated tasks prior to continuing. Then press OK to terminate the "Task Manager" and any remaining tasks launched by the "Task Manager". ***Note:*** The application also responds to a system Log off or Shut down event.
3	Shut down the applications.
	Close down all programs using the program specific instructions. In most cases this means closing the main form of each application by clicking the Close box on the top right of each form. However, some applications require specific shutdown procedures.
4	Confirm the eTM termination warning dialog.
	Click **OK**.  eTM - SOPHO Messenger@Net - v2.8.0 - GNTN1SCTI Please confirm that you really want to terminate the module "Task Manager". It is highly recommended to manually close down all associated tasks prior to continuing. Then press OK to terminate the "Task Manager" and any remaining tasks launched by the "Task Manager". Because all associated tasks were already manually ended gracefully, no more processing is involved. Any associated tasks still running are terminated through a **Terminate process** API-call for each task that is launched from within the eTM and finally shuts down the eTM module too.

END

Module – eTM_HA

IMPORTANT!

Setting up the eTM_HA module in a networked environment is a complex task, and requires training to set up, maintain, and use in the DECT Messenger environment. Read the following documentation closely, and refer to the training session on eTM_HA for more details.

Overview

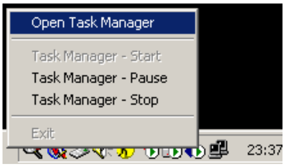
The module eTM_HA is the high-availability implementation of the eTM module. If you wish to migrate your system from eTM to eTM_HA, you must must update the system registry.

The module eTM_HA is an application that is represented as a small icon in the system tray on the bottom right-hand side of the desktop. This tray is usually populated with other applications, as shown in Figure 530, where the eTM_HA icon is shown to the immediate left of the clock.

Figure 530
Windows System Tray

Move the mouse over the icon in the system tray, then right-click to open the menu shown in Figure 531 on page 1226.

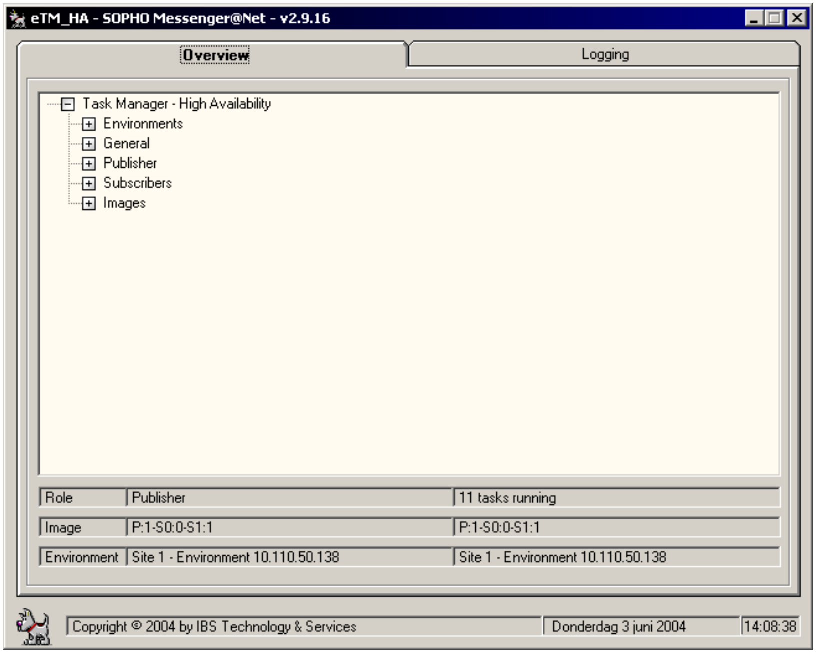
Figure 531
Open Task Manager



The menu option **Open Task Manager** restores the main menu, and can be opened to monitor the tasks in detail. This menu also provides options to **Start**, **Stop**, or **Pause** processing. Use the **Exit** menu option to terminate the eTM_HA module and all associated tasks.

When the **Open Task Manager** menu option of the pop-up menu is selected, a window similar to Figure 532 on page 1227 opens. The **Overview** tab shows the configuration, which is fetched from the registry.

Figure 532
eTM-HA Task Manager - Overview tab

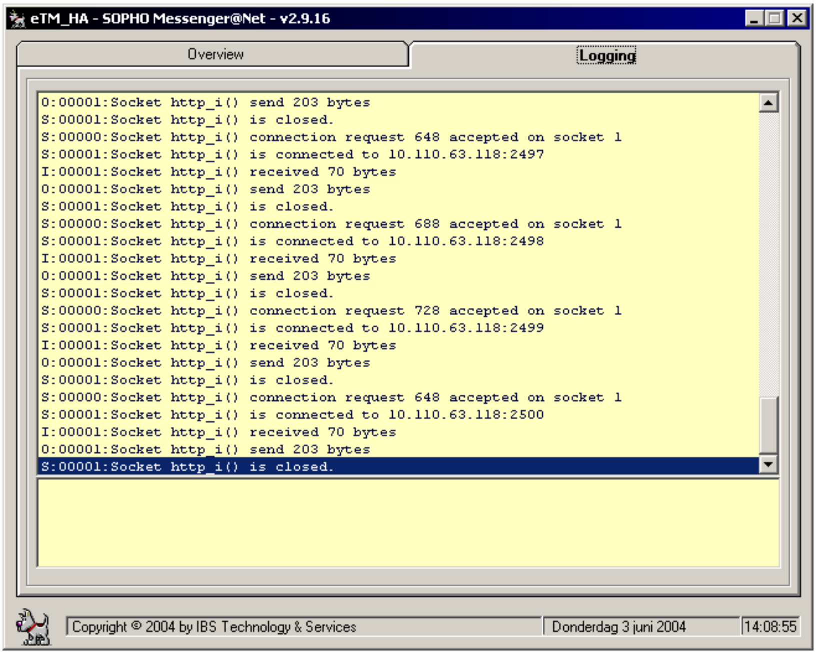

eTM_HA - SOPHO Messenger@Net - v2.9.16
Overview
Logging
Task Manager - High Availability
Environments
General
Publisher
Subscribers
Images

Role	Publisher	11 tasks running
Image	P:1-S0:0-S1:1	P:1-S0:0-S1:1
Environment	Site 1 - Environment 10.110.50.138	Site 1 - Environment 10.110.50.138

Copyright © 2004 by IBS Technology & Services | Donderdag 3 juni 2004 | 14:08:38

The **Logging** tab provides data as shown in Figure 533 on page 1228.

Figure 533
eTM-HA Logging tab



```
O:00001:Socket http_i() send 203 bytes
S:00001:Socket http_i() is closed.
S:00000:Socket http_i() connection request 648 accepted on socket 1
S:00001:Socket http_i() is connected to 10.110.63.118:2497
I:00001:Socket http_i() received 70 bytes
O:00001:Socket http_i() send 203 bytes
S:00001:Socket http_i() is closed.
S:00000:Socket http_i() connection request 688 accepted on socket 1
S:00001:Socket http_i() is connected to 10.110.63.118:2498
I:00001:Socket http_i() received 70 bytes
O:00001:Socket http_i() send 203 bytes
S:00001:Socket http_i() is closed.
S:00000:Socket http_i() connection request 728 accepted on socket 1
S:00001:Socket http_i() is connected to 10.110.63.118:2499
I:00001:Socket http_i() received 70 bytes
O:00001:Socket http_i() send 203 bytes
S:00001:Socket http_i() is closed.
S:00000:Socket http_i() connection request 648 accepted on socket 1
S:00001:Socket http_i() is connected to 10.110.63.118:2500
I:00001:Socket http_i() received 70 bytes
O:00001:Socket http_i() send 203 bytes
S:00001:Socket http_i() is closed.
```

Copyright © 2004 by IBS Technology & Services | Donderdag 3 juni 2004 | 14:08:55

> ***Note:*** The information shown in Figure 531 is intended as an example. The exact information for your system differs according to your configuration settings.

Publisher and Subscriber

A typical eTM_HA environment involves one system configured be Publisher, and one or more system configured as Subscribers. Although eTM_HA can run stand-alone (just one publisher), there is no value in activating an eTM_HA when there are no Subscribers. If there are no Subscribers, use eTM instead of eTM_HA.

In the Publisher and Subscriber model, the Publisher is the site where the Messenger_CFG configuration database is centralised. This is often called the main site. All configuration must reside on this centralised database only, so eCONFIG maintenance and eKERNEL must all reside on this same site.

The eTM_HA software can also be installed on distributed systems, intended to launch tasks on the distributed system. These systems launch, for instance, eCAP and eDMSAPI modules, all of them referring to the central eKERNEL residing on the Publisher site.

The eTM_HA software must be installed on both the Publisher and the Subscriber site. Based upon configuration settings in the registry, the instance behaves as Publisher or as Subscriber.

The following functionality is available:

- eTM functionality
  - Launch tasks associated with an environment
  - Keep track of running processes of an environment
  - Restart tasks that are missing
- eTM_HA specific functionality on Publisher
  - TCP server, listening on an admin port (default 7000)
  - Handling KeepAlive requests from Subscriber
  - Handling GetImage requests from Subscriber
  - Keeping track of state of Publisher and Subscriber
  - Changing the environment depending on the Publisher and Subscriber states
- eTM_HA specific functionality on Subscriber
  - TCP client, connecting to Publisher admin port
  - Sending KeepAlive requests to Publisher
  - Sending GetImage requests to Publisher
  - Keeping track of state of Publisher and Subscriber
  - Changing the environment depending on the Publisher and Subscriber states

During a change of environment, all running tasks of a previous environment are ended, and new tasks of the new environment are launched. During such an event, the Subscriber applies the last database image received from the Publisher and optionally applies changes defined in an SQL Script.

Registry settings eTM

The configuration of environments and tasks is stored in the following section:

```
[HKEY_CURRENT_USER\Software\Philips\SOPHO
        Messenger@Net\eTM]
```

This section contains definitions of environments and tasks, as described in the documentation of module eTM, “Module – eTM” on page 1205. These settings can be entered manually of can be generated by the eCONFIG or eGRID modules.

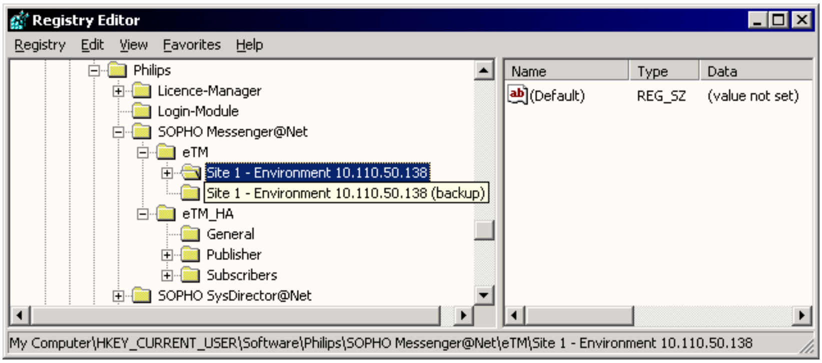
IMPORTANT!

If the environment names for eTM_HA are not defined with a name containing the local IP address, rename the registry structure generated by eGRID or eCONFIG, so that the IP address is available in the name.

The eTM structure can contain one or multiple environments. If you launch the eTM_HA.exe without additional parameters, the program analyses the available environments of the registry, and prompt for an initial environment at start-up.

Figure 534 on page 1231 shows an example, with two environments defined. One environment is called Site 1 – Environment 10.110.50.138, the other is called Site 1 – Environment 10.110050.138 (backup).

Figure 534
Example of two environments



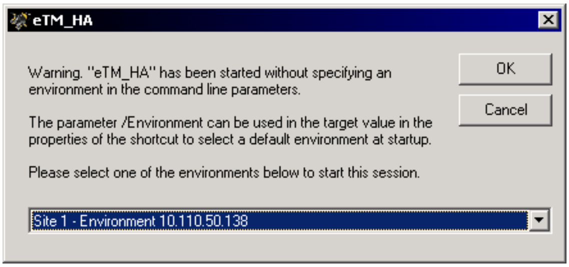
Name	Type	Data
(Default)	REG_SZ	(value not set)

My Computer\HKEY_CURRENT_USER\Software\Philips\SOPHO Messenger@Net\eTM\Site 1 - Environment 10.110.50.138

If eTM_HA.exe is launched without additional parameters on a system with local IP address 10.110.50.138, then a prompt appears as follows:

```
"C:\SOPHO Messenger@Net\Exe\eTM_HA.exe"
```

Figure 535
Selecting an environment when more than one is defined



Warning. "eTM_HA" has been started without specifying an environment in the command line parameters.

The parameter /Environment can be used in the target value in the properties of the shortcut to select a default environment at startup.

Please select one of the environments below to start this session.

Site 1 - Environment 10.110.50.138

Note: Because the objective of this module is to provide high availability, Nortel recommends that you suppress this prompt. This can be accomplished by adding a parameter on the command line of the shortcut, specifying the initial environment to select. This is performed by means of the optional keyword */Environment*.

Create a shortcut for eTM_HA in the start-up group specifying the initial environment, as follows:

```
"C:\SOPHO Messenger@Net\Exe\eTM_HA.exe" /
       Environment:Site 1 - Environment 10.110.50.138
```

Note: In eTM.exe a similar function existed, but the keyword was called */Site:*. In eTM_HA the keyword is renamed to */Environment*.

eTM registry entries accept the following parameters:

- PID

  The keyword PID denotes the process identifier of the task. This identifier is formatted as a 10-digit numeric value. The PID is also shown when Microsoft Task Manager is used to represent the processes. A special value 0000000000 is shown when the task is not running.

- Windowstyle

  The keyword Windowstyle denotes the style of the window of the task. The supported values are shown in Table 64.

Table 64
Supported window styles

Value	Description
0	Window is hidden and focus is passed to the hidden window.
1	Window has focus and is restored to its original size and position.
2	Window is displayed as an icon with focus.
3	Window is maximised with focus.
4	Window is restored to its most recent size and position. The currently active window remains active.
6	Window is displayed as an icon. The currently active window remains active.

- **Shortcut**

  The keyword Shortcut denotes the command line parameter that is used to launch the process.

Figure 536 on page 1234 shows a sample (exported) registry file of the eTM section, and refers to a Publisher site, usually containing an eKERNEL reference.

Figure 536
Sample registry file of the eTM, illustrating a Publisher site

```
Windows Registry Editor Version 5.00


[HKEY_CURRENT_USER\Software\Philips\SOPHO Messenger@Net\eTM\Site 1 -
       Environment 147.93.76.255]


[HKEY_CURRENT_USER\Software\Philips\SOPHO Messenger@Net\eTM\Site 1 -
       Environment 147.93.76.255\SOPHO Messenger@Net - CSTA Service]
"Shortcut"="\"C:\\SOPHO Messenger@Net\\Exe\\CSTA_Service.exe\""
"Windowstyle"="1"


[HKEY_CURRENT_USER\Software\Philips\SOPHO Messenger@Net\eTM\Site 1 -
       Environment 147.93.76.255\SOPHO Messenger@Net - eAPI - Port 3212]
"Shortcut"="\"C:\\SOPHO Messenger@Net\\Exe\\eAPI.exe\" /Site:1 /eKernel
       port:3212 /eKernel address:147.93.76.255 /Log drive:C"
"Windowstyle"="1"


[HKEY_CURRENT_USER\Software\Philips\SOPHO Messenger@Net\eTM\Site 1 -
       Environment 147.93.76.255\SOPHO Messenger@Net - eCAP - Port 3202]
"Shortcut"="\"C:\\SOPHO Messenger@Net\\Exe\\eCAP.exe\" /Site:1 /eKernel
       address:147.93.76.255 /eKernel port:3202 /Log drive:C"
"Windowstyle"="1"


[HKEY_CURRENT_USER\Software\Philips\SOPHO Messenger@Net\eTM\Site 1 -
       Environment 147.93.76.255\SOPHO Messenger@Net - eDMSAPI - Port
       3201]
"Shortcut"="\"C:\\SOPHO Messenger@Net\\Exe\\eDMSAPI.exe\" /Site:1 /
       eKernel address:147.93.76.255 /eKernel port:3201 /Log drive:C"
"Windowstyle"="1"
```

continued on next page...

Sample registry file of the eTM (continued)

```
[HKEY_CURRENT_USER\Software\Philips\SOPHO Messenger@Net\eTM\Site 1 -
       Environment 147.93.76.255\SOPHO Messenger@Net - eKernel - Site 1]
"Shortcut"="\"C:\\SOPHO Messenger@Net\\Exe\\eKERNEL.exe\" /Site:1 /
       licence:*NONE /keepalive:60"
"Windowstyle"="6"


[HKEY_CURRENT_USER\Software\Philips\SOPHO Messenger@Net\eTM\Site 1 -
       Environment 147.93.76.255\SOPHO Messenger@Net - eSMTP - Port 3211]
"Shortcut"="\"C:\\SOPHO Messenger@Net\\Exe\\eSMTP.exe\" /Site:1 /
       eKernel address:147.93.76.255 /eKernel port:3211 /Log drive:C"
"Windowstyle"="1"
```

Figure 537 on page 1236 shows another example, illustrating a Subscriber section in production mode. There is no eKERNEL reference in this example, as all modules refer to the eKERNEL on the publisher system.

Figure 537
Sample registry file, illustrating a Subscriber section in production mode

```
Windows Registry Editor Version 5.00

[HKEY_CURRENT_USER\Software\Philips\SOPHO Messenger@Net\eTM\Site 1 -
       Environment 147.93.169.130]

[HKEY_CURRENT_USER\Software\Philips\SOPHO Messenger@Net\eTM\Site 1 -
       Environment 147.93.169.130\SOPHO Messenger@Net - CSTA Service]
"Shortcut"="\"C:\\SOPHO Messenger@Net\\Exe\\CSTA_Service.exe\""
"Windowstyle"="1"

[HKEY_CURRENT_USER\Software\Philips\SOPHO Messenger@Net\eTM\Site 1 -
       Environment 147.93.169.130\SOPHO Messenger@Net - eCAP - Port 3403]
"Shortcut"="\"C:\\SOPHO Messenger@Net\\Exe\\eCAP.exe\" /Site:1 /eKernel
       address:147.93.76.255 /eKernel port:3403 /Log drive:C"
"Windowstyle"="1"

[HKEY_CURRENT_USER\Software\Philips\SOPHO Messenger@Net\eTM\Site 1 -
       Environment 147.93.169.130\SOPHO Messenger@Net - eDMSAPI - Port
       3401]
"Shortcut"="\"C:\\SOPHO Messenger@Net\\Exe\\eDMSAPI.exe\" /Site:1 /
       eKernel address:147.93.76.255 /eKernel port:3401 /Log drive:C"
"Windowstyle"="1"
```

Figure 538 on page 1237 shows another example, illustrating a Subscriber section in backup mode. Here an eKERNEL reference is shown, as the environment runs when the publisher is unavailable. All modules refer to the local eKERNEL on the subscriber system.

Figure 538
Sample registry file, illustrating a Subscriber section in backup mode

```
Windows Registry Editor Version 5.00


[HKEY_CURRENT_USER\Software\Philips\SOPHO Messenger@Net\eTM\Site 1 -
       Environment 147.93.169.130 (backup)\SOPHO Messenger@Net - eKernel
       - Site 1]
"Shortcut"="\"C:\\SOPHO Messenger@Net\\Exe\\eKERNEL.exe\" /Site:1 /
       licence:*NONE /keepalive:60"
"Windowstyle"="6"


[HKEY_CURRENT_USER\Software\Philips\SOPHO Messenger@Net\eTM\Site 1 -
       Environment 147.93.169.130 (backup)]


[HKEY_CURRENT_USER\Software\Philips\SOPHO Messenger@Net\eTM\Site 1 -
       Environment 147.93.169.130 (backup)\SOPHO Messenger@Net - CSTA
       Service]
"Shortcut"="\"C:\\SOPHO Messenger@Net\\Exe\\CSTA_Service.exe\""
"Windowstyle"="1"


[HKEY_CURRENT_USER\Software\Philips\SOPHO Messenger@Net\eTM\Site 1 -
       Environment 147.93.169.130 (backup)\SOPHO Messenger@Net - eCAP -
       Port 3403]
"Shortcut"="\"C:\\SOPHO Messenger@Net\\Exe\\eCAP.exe\" /Site:1 /eKernel
       address:147.93.169.130 /eKernel port:3403 /Log drive:C"
"Windowstyle"="1"


[HKEY_CURRENT_USER\Software\Philips\SOPHO Messenger@Net\eTM\Site 1 -
       Environment 147.93.169.130 (backup)\SOPHO Messenger@Net - eDMSAPI
       - Port 3401]
"Shortcut"="\"C:\\SOPHO Messenger@Net\\Exe\\eDMSAPI.exe\" /Site:1 /
       eKernel address:147.93.169.130 /eKernel port:3401 /Log drive:C"
"Windowstyle"="1"
```

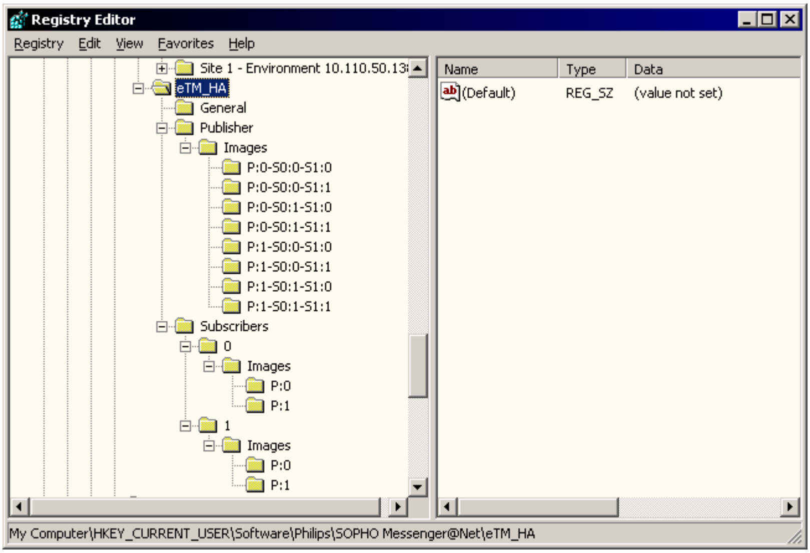
Registry settings eTM_HA

The configuration of environments and tasks is stored in the following section:

```
[HKEY_CURRENT_USER\Software\Philips\SOPHO
        Messenger@Net\eTM_HA]
```

This section contains additional configuration settings that are needed for configuring the high-availability functionality that is added in eTM_HA.

Figure 539
Registry settings: General section



Name	Type	Data
(Default)	REG_SZ	(value not set)

My Computer\HKEY_CURRENT_USER\Software\Philips\SOPHO Messenger@Net\eTM_HA

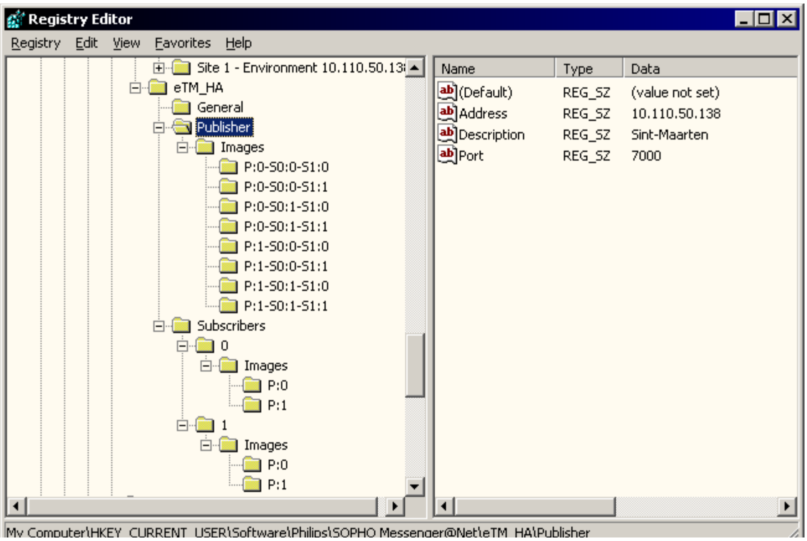
The General section defines the following parameters:

- Interval CheckAvailability
- Interval CheckTasks
- Interval KeepAlive
- Interval GetImage
- Timeout KeepAlive

- Timeout GetImage
- Timeout Task
- Log days
- Publisher database
- Subscriber database
- Subscriber workspace
- Subscriber image

The Publisher section contains a structure as shown Figure 540:

Figure 540
Registry settings: Publisher section



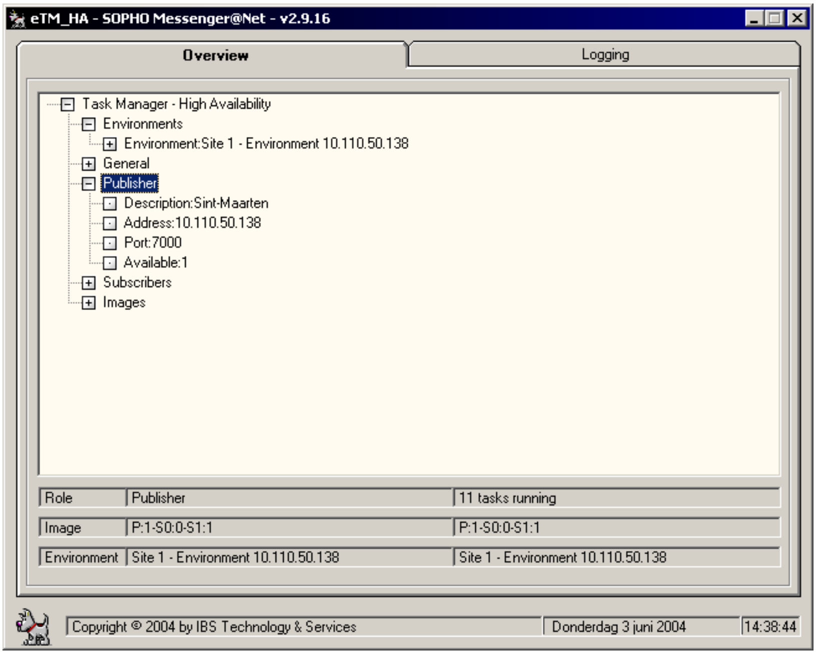
```
Site 1 - Environment 10.110.50.13
eTM_HA
    General
    Publisher
        Images
            P:0-S0:0-S1:0
            P:0-S0:0-S1:1
            P:0-S0:1-S1:0
            P:0-S0:1-S1:1
            P:1-S0:0-S1:0
            P:1-S0:0-S1:1
            P:1-S0:1-S1:0
            P:1-S0:1-S1:1
    Subscribers
        0
            Images
                P:0
                P:1
        1
            Images
                P:0
                P:1
```

Name	Type	Data
(Default)	REG_SZ	(value not set)
Address	REG_SZ	10.110.50.138
Description	REG_SZ	Sint-Maarten
Port	REG_SZ	7000

My Computer\HKEY_CURRENT_USER\Software\Philips\SOPHO Messenger@Net\eTM_HA\Publisher

The same information is represented in the eTM_HA Overview tab, as illustrated in Figure 541 on page 1240.

Figure 541
Registry settings: Publisher overview in eTM_HA



eTM_HA - SOPHO Messenger@Net - v2.9.16

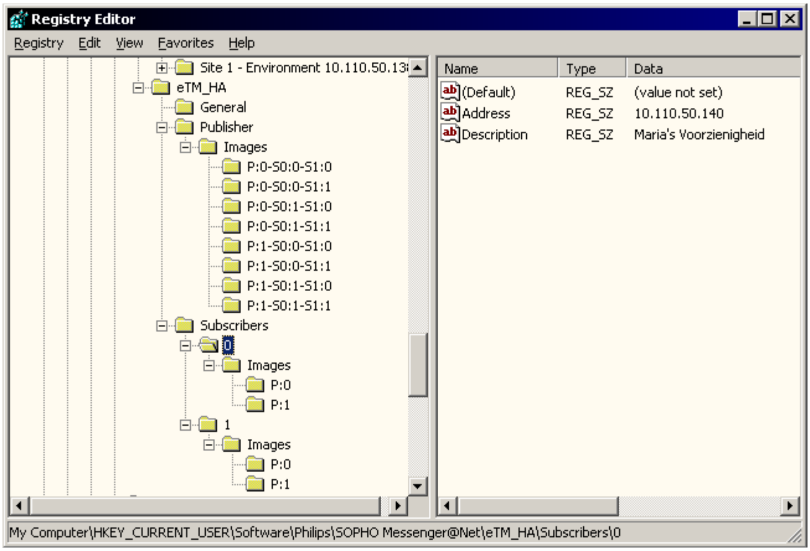
```
⊟ Task Manager - High Availability
    ⊟ Environments
        ⊞ Environment:Site 1 - Environment 10.110.50.138
    ⊞ General
    ⊟ Publisher
        ⊡ Description:Sint-Maarten
        ⊡ Address:10.110.50.138
        ⊡ Port:7000
        ⊡ Available:1
    ⊞ Subscribers
    ⊞ Images
```

Role	Publisher	11 tasks running
Image	P:1-S0:0-S1:1	P:1-S0:0-S1:1
Environment	Site 1 - Environment 10.110.50.138	Site 1 - Environment 10.110.50.138

Copyright © 2004 by IBS Technology & Services | Donderdag 3 juni 2004 | 14:38:44

The Subscribers section contains a structure as illustrated in Figure 542 on page 1241 and Figure 543 on page 1241.

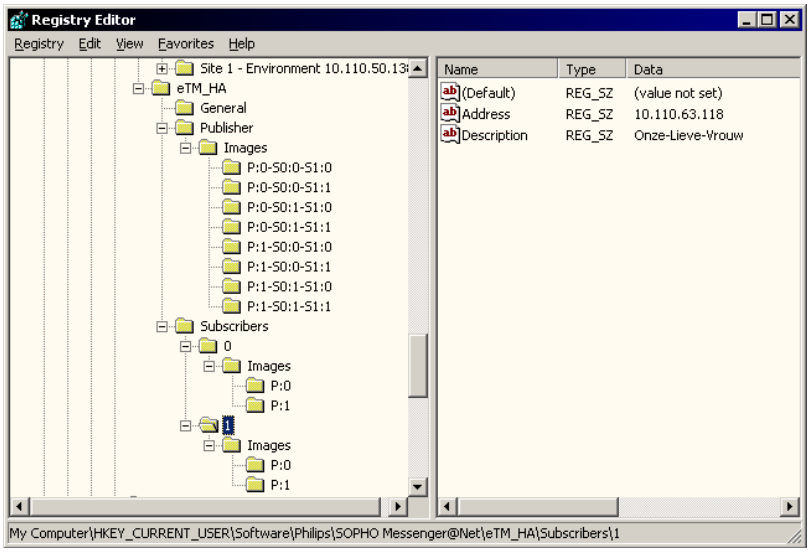
Figure 542
Registry settings: Subscribers (0) section



Name	Type	Data
(Default)	REG_SZ	(value not set)
Address	REG_SZ	10.110.50.140
Description	REG_SZ	Maria's Voorzienigheid

My Computer\HKEY_CURRENT_USER\Software\Philips\SOPHO Messenger@Net\eTM_HA\Subscribers\0

Figure 543
Registry settings: Subscribers (1) section

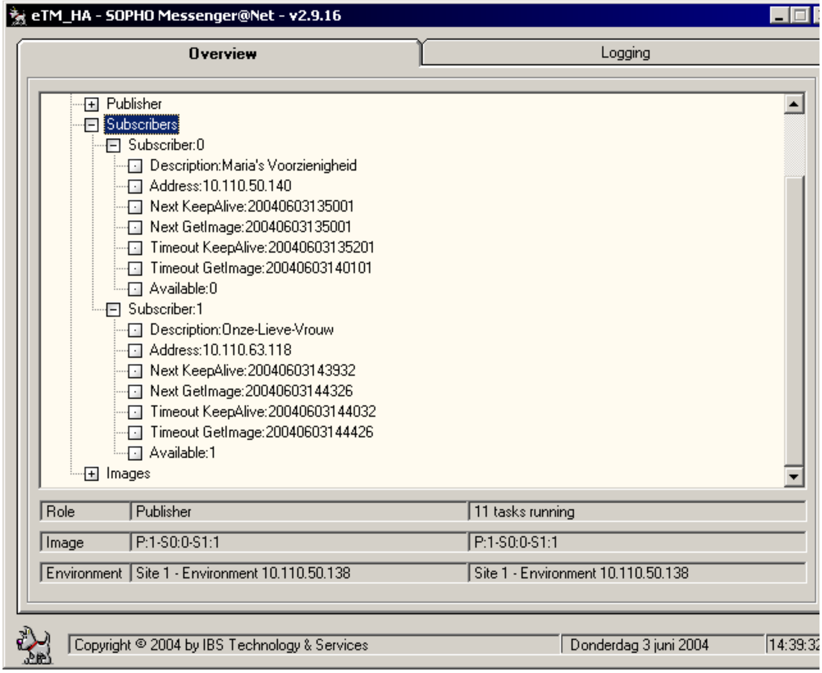


Name	Type	Data
(Default)	REG_SZ	(value not set)
Address	REG_SZ	10.110.63.118
Description	REG_SZ	Onze-Lieve-Vrouw

My Computer\HKEY_CURRENT_USER\Software\Philips\SOPHO Messenger@Net\eTM_HA\Subscribers\1

The same information is represented in the eTM_HA Overview tab, as illustrated in Figure 544.

Figure 544
Registry settings: Subscribers overview in eTM_HA



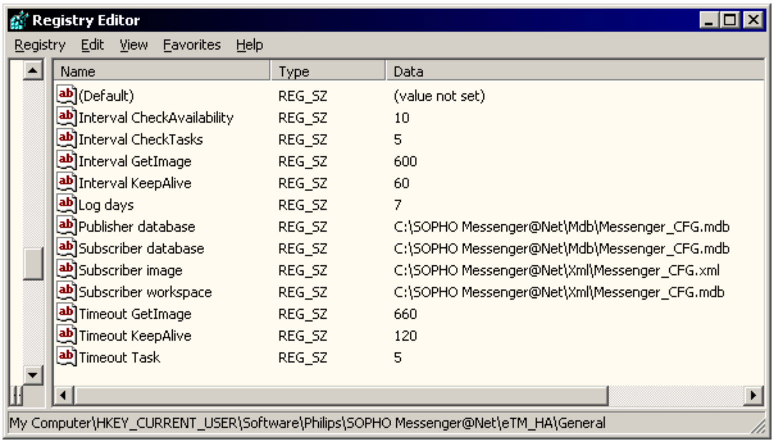
```
⊞ Publisher
⊟ Subscribers
    ⊟ Subscriber:0
        □ Description:Maria's Voorzienigheid
        □ Address:10.110.50.140
        □ Next KeepAlive:20040603135001
        □ Next GetImage:20040603135001
        □ Timeout KeepAlive:20040603135201
        □ Timeout GetImage:20040603140101
        □ Available:0
    ⊟ Subscriber:1
        □ Description:Onze-Lieve-Vrouw
        □ Address:10.110.63.118
        □ Next KeepAlive:20040603143932
        □ Next GetImage:20040603144326
        □ Timeout KeepAlive:20040603144032
        □ Timeout GetImage:20040603144426
        □ Available:1
⊞ Images
```

Role	Publisher	11 tasks running
Image	P:1-S0:0-S1:1	P:1-S0:0-S1:1
Environment	Site 1 - Environment 10.110.50.138	Site 1 - Environment 10.110.50.138

Copyright © 2004 by IBS Technology & Services | Donderdag 3 juni 2004 | 14:39:3

The General section contains a structure as illustrated in Figure 545 on page 1243.

Figure 545
Registry settings: General

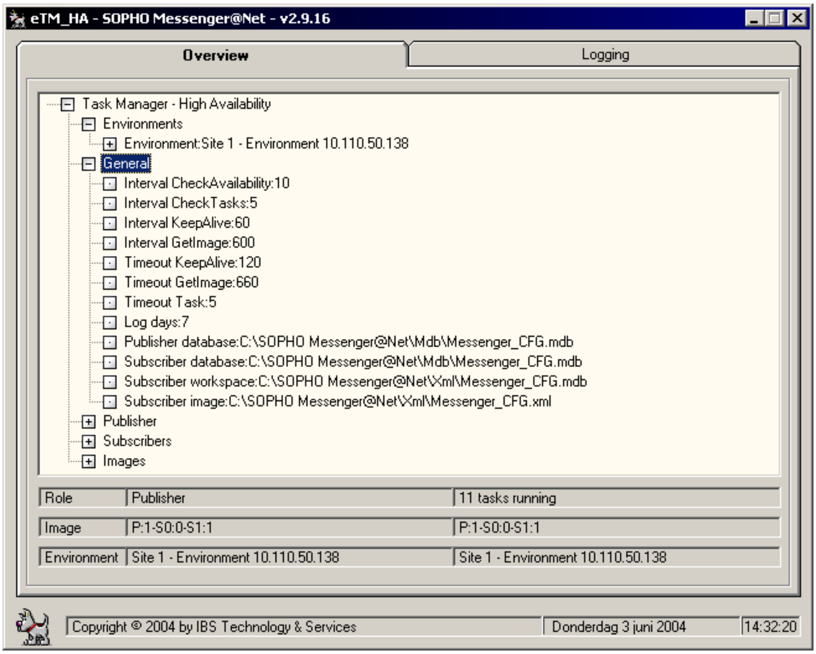


Name	Type	Data
(Default)	REG_SZ	(value not set)
Interval CheckAvailability	REG_SZ	10
Interval CheckTasks	REG_SZ	5
Interval GetImage	REG_SZ	600
Interval KeepAlive	REG_SZ	60
Log days	REG_SZ	7
Publisher database	REG_SZ	C:\SOPHO Messenger@Net\Mdb\Messenger_CFG.mdb
Subscriber database	REG_SZ	C:\SOPHO Messenger@Net\Mdb\Messenger_CFG.mdb
Subscriber image	REG_SZ	C:\SOPHO Messenger@Net\Xml\Messenger_CFG.xml
Subscriber workspace	REG_SZ	C:\SOPHO Messenger@Net\Xml\Messenger_CFG.mdb
Timeout GetImage	REG_SZ	660
Timeout KeepAlive	REG_SZ	120
Timeout Task	REG_SZ	5

My Computer\HKEY_CURRENT_USER\Software\Philips\SOPHO Messenger@Net\eTM_HA\General

The same information is shown in the eTM_HA Overview tab, as shown in Figure 546 on page 1244.

Figure 546
Registry settings: General in eTM_HA



eTM_HA - SOPHO Messenger@Net - v2.9.16

```
⊟ Task Manager - High Availability
   ⊟ Environments
      ⊞ Environment:Site 1 - Environment 10.110.50.138
   ⊟ General
      ⊡ Interval CheckAvailability:10
      ⊡ Interval CheckTasks:5
      ⊡ Interval KeepAlive:60
      ⊡ Interval GetImage:600
      ⊡ Timeout KeepAlive:120
      ⊡ Timeout GetImage:660
      ⊡ Timeout Task:5
      ⊡ Log days:7
      ⊡ Publisher database:C:\SOPHO Messenger@Net\Mdb\Messenger_CFG.mdb
      ⊡ Subscriber database:C:\SOPHO Messenger@Net\Mdb\Messenger_CFG.mdb
      ⊡ Subscriber workspace:C:\SOPHO Messenger@Net\Xml\Messenger_CFG.mdb
      ⊡ Subscriber image:C:\SOPHO Messenger@Net\Xml\Messenger_CFG.xml
   ⊞ Publisher
   ⊞ Subscribers
   ⊞ Images
```

Role	Publisher	11 tasks running
Image	P:1-S0:0-S1:1	P:1-S0:0-S1:1
Environment	Site 1 - Environment 10.110.50.138	Site 1 - Environment 10.110.50.138

Copyright © 2004 by IBS Technology & Services | Donderdag 3 juni 2004 | 14:32:20

Merging registry files

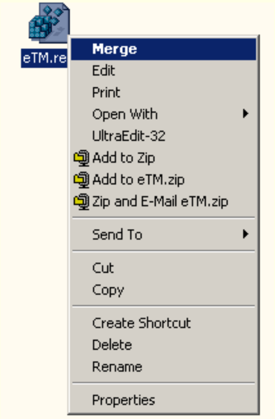
Use the steps in Procedure 244 to merge registry files.

Procedure 244
Merging .reg files (Part 1 of 2)

<table>
<tr><th>Step</th><th>Action</th></tr>
<tr><td></td><td></td></tr>
<tr><td>1</td><td>Select the Merge command.</td></tr>
<tr><td></td><td>

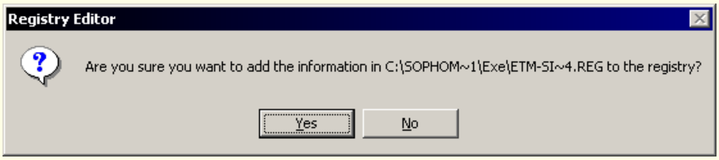
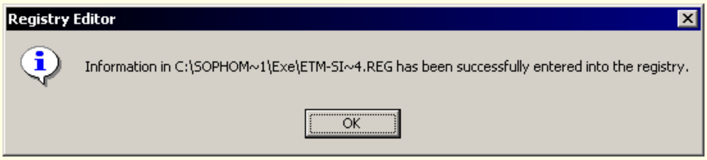
In Windows Explorer:

- Locate the file you want to merge.
- Right-click the file.
- choose **Merge** from the pop-up menu, as follows:



</td></tr>
</table>

Procedure 244
Merging .reg files (Part 2 of 2)

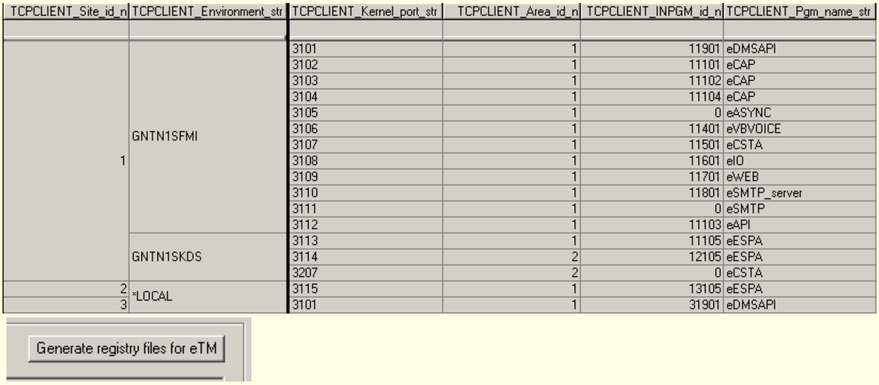
Step	Action
2	Confirm that you wish to merge the registry.
	Choose **Yes** to continue.  Registry Editor Are you sure you want to add the information in C:\SOPHOM~1\Exe\ETM-SI~4.REG to the registry?
3	Confirm completion of the registry merge.
	Click **OK**.  Registry Editor Information in C:\SOPHOM~1\Exe\ETM-SI~4.REG has been successfully entered into the registry.
	END

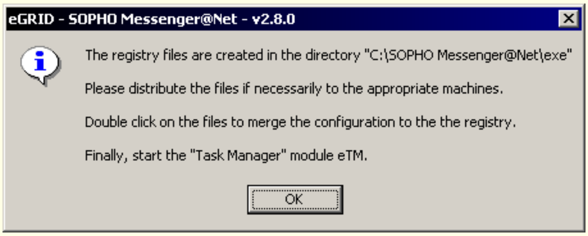
The command RegEdit or RegEdt32 can be used to verify the configuration, or to apply changes to an existing configuration.

Future releases of DECT Messenger will provide automatic procedures for configuring the Task Manager from the Configurator module.

The eGRID module features a command button **Generate registry files for eTM**. Click this button to read the eKERNEL_TCPCLIENT table and automatically generate the required shortcuts for each site and environment, as shown in Figure 245.

Procedure 245
Generate shortcuts

<table>
<tr><th>Step</th><th>Action</th></tr>
<tr><td></td><td></td></tr>
<tr><td>1</td><td>Use eGRID to generate registry files for eTM.</td></tr>
<tr><td></td><td>Launch eGRID and click <b>Generate registry files for eTM</b>.

<table>
<tr><th>TCPCLIENT_Site_id_n</th><th>TCPCLIENT_Environment_str</th><th>TCPCLIENT_Kernel_port_str</th><th>TCPCLIENT_Area_id_n</th><th>TCPCLIENT_INPGM_id_n</th><th>TCPCLIENT_Pgm_name_str</th></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>1</td><td>GNTN1SFMI</td><td>3101</td><td>1</td><td>11901</td><td>eDMSAPI</td></tr>
<tr><td></td><td></td><td>3102</td><td>1</td><td>11101</td><td>eCAP</td></tr>
<tr><td></td><td></td><td>3103</td><td>1</td><td>11102</td><td>eCAP</td></tr>
<tr><td></td><td></td><td>3104</td><td>1</td><td>11104</td><td>eCAP</td></tr>
<tr><td></td><td></td><td>3105</td><td>1</td><td>0</td><td>eASYNC</td></tr>
<tr><td></td><td></td><td>3106</td><td>1</td><td>11401</td><td>eVBVOICE</td></tr>
<tr><td></td><td></td><td>3107</td><td>1</td><td>11501</td><td>eCSTA</td></tr>
<tr><td></td><td></td><td>3108</td><td>1</td><td>11601</td><td>eIO</td></tr>
<tr><td></td><td></td><td>3109</td><td>1</td><td>11701</td><td>eWEB</td></tr>
<tr><td></td><td></td><td>3110</td><td>1</td><td>11801</td><td>eSMTP_server</td></tr>
<tr><td></td><td></td><td>3111</td><td>1</td><td>0</td><td>eSMTP</td></tr>
<tr><td></td><td></td><td>3112</td><td>1</td><td>11103</td><td>eAPI</td></tr>
<tr><td></td><td>GNTN1SKDS</td><td>3113</td><td>1</td><td>11105</td><td>eESPA</td></tr>
<tr><td></td><td></td><td>3114</td><td>2</td><td>12105</td><td>eESPA</td></tr>
<tr><td></td><td></td><td>3207</td><td>2</td><td>0</td><td>eCSTA</td></tr>
<tr><td>2</td><td>*LOCAL</td><td>3115</td><td>1</td><td>13105</td><td>eESPA</td></tr>
<tr><td>3</td><td></td><td>3101</td><td>1</td><td>31901</td><td>eDMSAPI</td></tr>
</table>

</td></tr>
<tr><td>2</td><td>Review the information provided, and acknowledge completion of the process.</td></tr>
<tr><td></td><td>Click <b>OK</b> to continue.


The registry files are created in the directory "C:\SOPHO Messenger@Net\exe"
Please distribute the files if necessarily to the appropriate machines.
Double click on the files to merge the configuration to the the registry.
Finally, start the "Task Manager" module eTM.

</td></tr>
</table>

END

> ***Note:*** Do not forget to verify that the names of the environments in the eTM registry keys contain the IP address; if not, rename the key to include the IP address. Nortel recommends that you use the following naming conventions in the registry: Site n - Environment x.x.x.x and Site n - Environment x.x.x.x - backup

Check tasks

The program verifies all tasks with a time interval specified in the registry (usually 5 seconds).

When the eTM_HA is paused or stopped, the routine that verifies and restarts the process is temporarily interrupted.

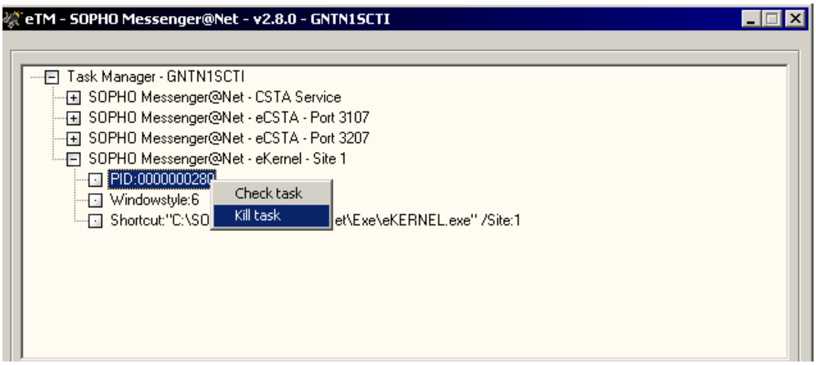
This usually occurs during maintenance of one of more of the programs that are guarded by the eTM_HA. This temporary condition is shown in the logging.

A system administrator can also terminate a task from within the eTM_HA environment using a **Terminate process** API-call.

> ***Note:*** Using the **Terminate process** API-call can cause data loss, as this does not provide any graceful cleanup or shutdown of the associated program.

To terminate a process in the Task Manager, use the **Kill task menu** option as shown in Figure 547 on page 1249. The **Kill task** option is available only when the tree-view is expanded and the mouse is right-clicked on the PID:xxxxxxxxxx line.

Figure 547
Kill Task



eTM - SOPHO Messenger@Net - v2.8.0 - GNTN1SCTI

```
⊟ Task Manager - GNTN1SCTI
   ⊞ SOPHO Messenger@Net - CSTA Service
   ⊞ SOPHO Messenger@Net - eCSTA - Port 3107
   ⊞ SOPHO Messenger@Net - eCSTA - Port 3207
   ⊟ SOPHO Messenger@Net - eKernel - Site 1
      ⊡ PID:000000028
      ⊡ Windowstyle:6
      ⊡ Shortcut:"C:\SO                et\Exe\eKERNEL.exe" /Site:1
```

> ***Note:*** When the eTM is running, the system relaunches the terminated tasks within 10 seconds.

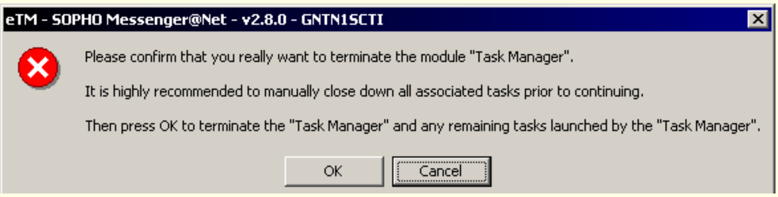
When the eTM form is closed through the control box on the right top of the form, the application does not shut down, but is instead minimised to an icon in the system tray. This function is designed to prevent the user from accidentally closing the eTM and associated tasks. This approach is similar to monitoring applications of other vendors, such as the Apache Monitor or the SQL Server Service Manager.

Shutting down eTM_HA

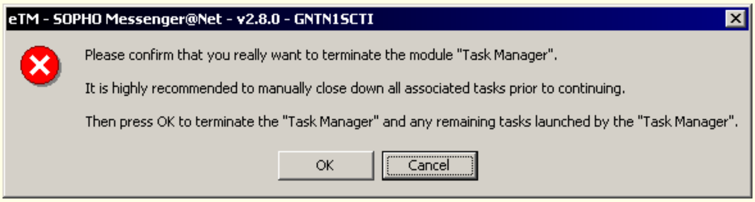
The eTM can be shut down by means of the pop-up menu shown in Figure 531 on page 1226, using the **Exit** menu option.

> **IMPORTANT!**
>
> Nortel recommends that you close applications using shut down or exit/close options in the applications themselves, to ensure a clean shutdown. This helps to protect volatile data, properly close down serial and sockets communications, free resources, clean up garbage, and so on. To stop the processes gracefully, follow the steps in Procedure 246

Procedure 246
Shutting down eTM_HA (Part 1 of 2)

Step	Action
1	Open the eTM_HA pop-up menu.
	Right-click the eTM_HA icon in the system tray.
1	Stop the eTM_HA.
	• Choose the menu item **Task Manager - Stop**. • Choose the menu item **Exit**. The following confirmation prompt is shown; do not click **OK** or **Cancel** yet:  eTM - SOPHO Messenger@Net - v2.8.0 - GNTN1SCTI Please confirm that you really want to terminate the module "Task Manager". It is highly recommended to manually close down all associated tasks prior to continuing. Then press OK to terminate the "Task Manager" and any remaining tasks launched by the "Task Manager". ***Note:*** The application also responds to a system Log off or Shut down event.

Procedure 246
Shutting down eTM_HA (Part 2 of 2)

Step	Action
2	Shut down the applications.
	Close down all programs using the program specific instructions. In most cases this means closing the main form of each application by clicking the close box on the top right of each form. However, some applications require specific shutdown procedures.
3	Confirm the eTM termination warning dialog.
	Click **OK**.  eTM - SOPHO Messenger@Net - v2.8.0 - GNTN1SCTI Please confirm that you really want to terminate the module "Task Manager". It is highly recommended to manually close down all associated tasks prior to continuing. Then press OK to terminate the "Task Manager" and any remaining tasks launched by the "Task Manager". Because all associated tasks were already manually ended gracefully, no more processing is involved. Any associated tasks still running are terminated through a **Terminate process** API-call for each task that is launched from within the eTM and finally shuts down the eTM module as well.

END

Publisher

The publisher instance of eTM_HA features a TCP Server listing on a port specified in the registry. Typically, port 7000 is used as the default port. The TCP Server is a multiple-accept model, so multiple clients can connect at the same time. The number of simultaneous connections is also defined in the registry. Specify a number at least as great as the number of subscribers. Nortel recommends specifying a value that equals the number of subscribers multiplied by three, to provide room for recovery in case of bad connection attempts.

The netstat command can be used on the Publisher to verify that the TCP Server is listening (sample data is shown in Figure 548).

Figure 548
Sample netstat command and returned data

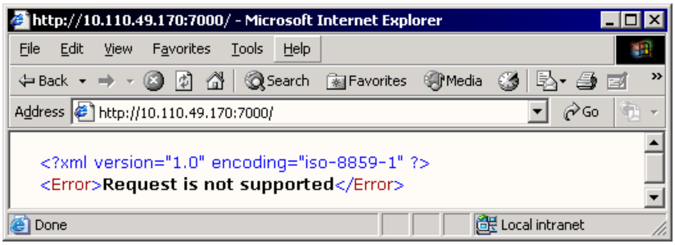
```
C:\>netstat -a -n

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:21             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:25             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:80             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:90             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:443            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:7000           0.0.0.0:0              LISTENING
:
```

IMPORTANT!

The TCP Server is used for internal processing only. Do not attempt to access the server unless instructed to do so.

The TCP Server is to be accessed from the Subscribers only. You can test this connection (from the subscriber PCs only) with Internet Explorer. An HTTP request to port 7000 must reply with the error code shown in Figure 549 on page 1253.

Figure 549
TCP Server Error response



http://10.110.49.170:7000/ - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://10.110.49.170:7000/
Go
Done
Local intranet

```
<?xml version="1.0" encoding="iso-8859-1" ?>
<Error>Request is not supported</Error>
```

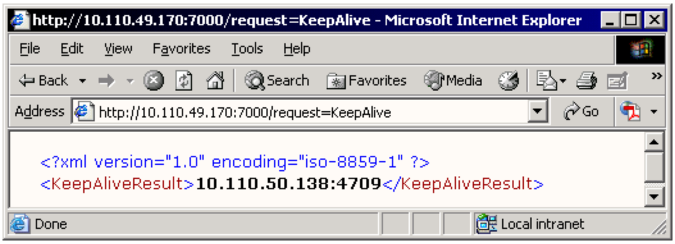
In an operational environment, the eTM_HA instances of the Subscribers send these two requests to the publisher on a regular basis: KeepAlive, and GetImage.

- **KeepAlive**

  A KeepAlive request is exchanged between subscriber and publisher, and allows both parties to verify the presence of the other. Interval and timeout between attempts are defined in the registry.

  Figure 550 shows an example of what is sent during this exchange. To test this response, Nortel recommends using Internet Explorer on the Subscriber.

Figure 550
TCP Server Keep Alive response



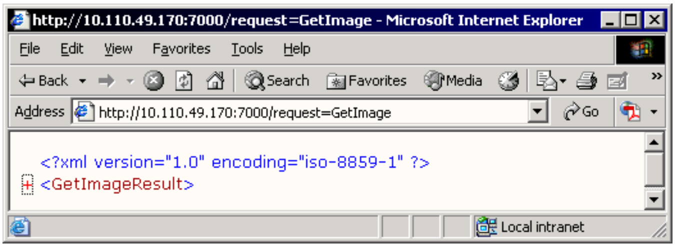
http://10.110.49.170:7000/request=KeepAlive - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://10.110.49.170:7000/request=KeepAlive
Go
Done
Local intranet

```
<?xml version="1.0" encoding="iso-8859-1" ?>
<KeepAliveResult>10.110.50.138:4709</KeepAliveResult>
```

- **GetImage**

  The GetImage request is sent from each Subscriber to the Publisher on a regular time interval, as specified in the registry. The publishing system responds to such a request with an XML image of the Messenger_CFG database. Figure 551 shows an example.

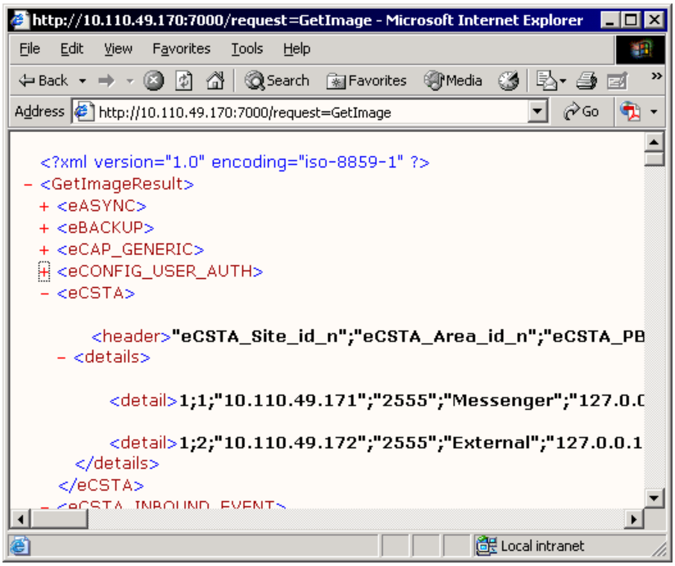
Figure 551
TCP Server Get Image response


http://10.110.49.170:7000/request=GetImage - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://10.110.49.170:7000/request=GetImage
Go
Local intranet

```
  <?xml version="1.0" encoding="iso-8859-1" ?>
+ <GetImageResult>
```

The XML image file provided by the GetImage request can be expanded and collapsed with the plus (+) and minus (-) signs, as shown in Figure 552. For more information on the XML image, see “XML image” on page 1260.

Figure 552
Expanded information


http://10.110.49.170:7000/request=GetImage - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://10.110.49.170:7000/request=GetImage
Go
Local intranet

```
  <?xml version="1.0" encoding="iso-8859-1" ?>
- <GetImageResult>
  + <eASYNC>
  + <eBACKUP>
  + <eCAP_GENERIC>
  + <eCONFIG_USER_AUTH>
  - <eCSTA>

       <header>"eCSTA_Site_id_n";"eCSTA_Area_id_n";"eCSTA_PB
    - <details>

         <detail>1;1;"10.110.49.171";"2555";"Messenger";"127.0.0

         <detail>1;2;"10.110.49.172";"2555";"External";"127.0.0.1
      </details>
    </eCSTA>
  - <eCSTA_INBOUND_EVENT>
```

Note 1: Messenger_CFG contains sensitive data, and is exchanged as plain text in XML format. To prevent security exposure, HTTP requests from external systems are rejected with an authentication error. This test is performed based upon the IP address of the requester.

Note 2: In a WAN environment, a test with a Browser can lead to rejection, even from the subscriber system. The most common cause is a proxy server that masks the IP address of the subscriber. During tests with Internet Explorer, you must disable the proxy server for local addresses or specify the IP address of the publisher in the bypass list.

Keeping track of states

Both publisher and subscriber keep track of the state of the other party. This leads to a so-called “image” of Boolean settings of publisher and subscriber.

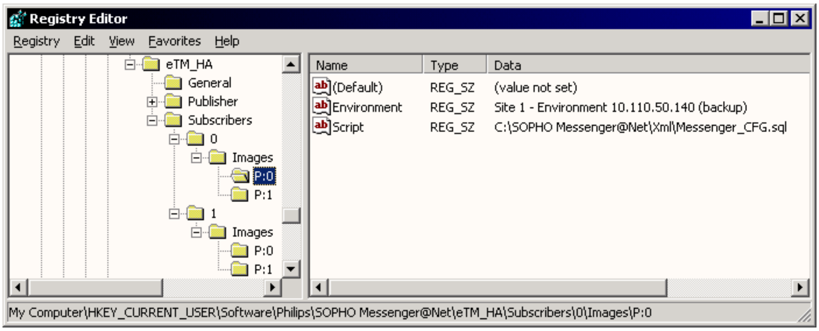
Subscriber

On the subscriber level, there is a state represented by P:0 and P:1, indicating whether the publisher can be reached. P:1 denotes the publisher is available, P:0 denotes the publisher is unavailable.

Appropriate registry settings associate an environment to each image. Optionally an SQL script can be defined to run during switching environments.

The registry definitions are shown in Figure 553 on page 1256.

Figure 553
Registry definitions



Name	Type	Data
(Default)	REG_SZ	(value not set)
Environment	REG_SZ	Site 1 - Environment 10.110.50.140 (backup)
Script	REG_SZ	C:\SOPHO Messenger@Net\Xml\Messenger_CFG.sql

My Computer\HKEY_CURRENT_USER\Software\Philips\SOPHO Messenger@Net\eTM_HA\Subscribers\0\Images\P:0

In Figure 553, an example is shown with one Publisher and two Subscribers; Subscriber 0 has an image for handling P:0 and P:1. This example shows the settings when the subscriber cannot connect to the publisher. The environment Site 1 – Environment 10.110.50.140 (backup) is associated and SQL script Messenger_CFG_sql is defined.

Publisher

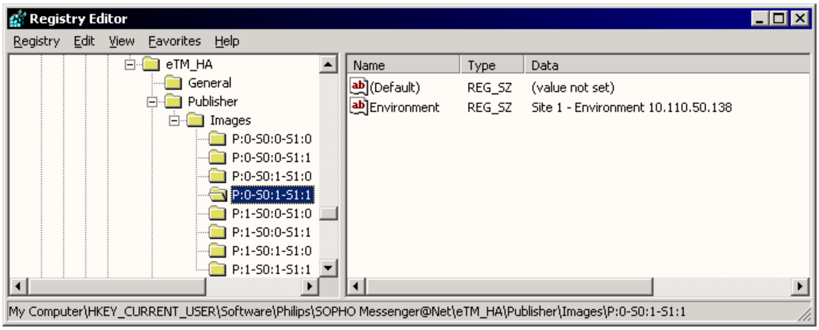
On the publisher level, a similar registry image is used. However, as a Publisher is often in contact with multiple subscribers, the available images grow exponentially, as the state of publisher and every subscriber forms a number of combinations for each Boolean state.

Figure 554 on page 1257 shows a network where one Publisher and two Subscribers lead to eight images, and depend on each Boolean state of available (1) or unavailable (0).

The syntax for images on publisher level are similar to P:1:S0:1-S1:1. Each section is separated by a minus sign (-).

- The P:1 or P:0 denotes the state of the publisher
- The S0:1 or S0:1 denotes the state of first subscriber
- The S1:1 or S1:1 denotes the state of second subscriber

Figure 554
Example of an image at the publisher level



eTM_HA
General
Publisher
Images
P:0-S0:0-S1:0
P:0-S0:0-S1:1
P:0-S0:1-S1:0
P:0-S0:1-S1:1
P:1-S0:0-S1:0
P:1-S0:0-S1:1
P:1-S0:1-S1:0
P:1-S0:1-S1:1

Name	Type	Data
(Default)	REG_SZ	(value not set)
Environment	REG_SZ	Site 1 - Environment 10.110.50.138

My Computer\HKEY_CURRENT_USER\Software\Philips\SOPHO Messenger@Net\eTM_HA\Publisher\Images\P:0-S0:1-S1:1

The registry keys are to be entered manually.

Recommendation

Nortel recommends that you begin with a definition on the Publisher level that refers to the same environment for each image, and with a definition on the Subscriber level that refers to the same environment for each image.

In this initial setup no environment changes occur, and initial testing can take place.

In a later stage you can modify environments. A copy of the production environment is usually made at the Subscriber sites, for example, Site 1 – Environment 10.110.50.140 and Site 1 – Environment 10.110.50.140 (backup). In this backup environment, the tasks can be altered, for example, an eKERNEL instance can be added, and eKERNEL_address refers to a local instance of eKERNEL.

Figure 555
Example: Site 1 - Environment 147.93.169.130

```
Windows Registry Editor Version 5.00


[HKEY_CURRENT_USER\Software\Philips\SOPHO Messenger@Net\eTM\Site 1 -
       Environment 147.93.169.130]


[HKEY_CURRENT_USER\Software\Philips\SOPHO Messenger@Net\eTM\Site 1 -
       Environment 147.93.169.130\SOPHO Messenger@Net - CSTA Service]
"Shortcut"="\"C:\\SOPHO Messenger@Net\\Exe\\CSTA_Service.exe\""
"Windowstyle"="1"


[HKEY_CURRENT_USER\Software\Philips\SOPHO Messenger@Net\eTM\Site 1 -
       Environment 147.93.169.130\SOPHO Messenger@Net - eCAP - Port 3403]
"Shortcut"="\"C:\\SOPHO Messenger@Net\\Exe\\eCAP.exe\" /Site:1 /eKernel
       address:147.93.76.255 /eKernel port:3403 /Log drive:C"
"Windowstyle"="1"


[HKEY_CURRENT_USER\Software\Philips\SOPHO Messenger@Net\eTM\Site 1 -
       Environment 147.93.169.130\SOPHO Messenger@Net - eDMSAPI - Port
       3401]
"Shortcut"="\"C:\\SOPHO Messenger@Net\\Exe\\eDMSAPI.exe\" /Site:1 /
       eKernel address:147.93.76.255 /eKernel port:3401 /Log drive:C"
"Windowstyle"="1"
```

Figure 556
Example: "Site 1 - Environment 147.93.169.130 (backup)"

```
Windows Registry Editor Version 5.00


[HKEY_CURRENT_USER\Software\Philips\SOPHO Messenger@Net\eTM\Site 1 -
       Environment 147.93.169.130 (backup)\SOPHO Messenger@Net - eKernel
       - Site 1]
"Shortcut"="\"C:\\SOPHO Messenger@Net\\Exe\\eKERNEL.exe\" /Site:1 /
       licence:*NONE /keepalive:60"
"Windowstyle"="6"


[HKEY_CURRENT_USER\Software\Philips\SOPHO Messenger@Net\eTM\Site 1 -
       Environment 147.93.169.130 (backup)]


[HKEY_CURRENT_USER\Software\Philips\SOPHO Messenger@Net\eTM\Site 1 -
       Environment 147.93.169.130 (backup)\SOPHO Messenger@Net - CSTA
       Service]
"Shortcut"="\"C:\\SOPHO Messenger@Net\\Exe\\CSTA_Service.exe\""
"Windowstyle"="1"


[HKEY_CURRENT_USER\Software\Philips\SOPHO Messenger@Net\eTM\Site 1 -
       Environment 147.93.169.130 (backup)\SOPHO Messenger@Net - eCAP -
       Port 3403]
"Shortcut"="\"C:\\SOPHO Messenger@Net\\Exe\\eCAP.exe\" /Site:1 /eKernel
       address:147.93.169.130 /eKernel port:3403 /Log drive:C"
"Windowstyle"="1"


[HKEY_CURRENT_USER\Software\Philips\SOPHO Messenger@Net\eTM\Site 1 -
       Environment 147.93.169.130 (backup)\SOPHO Messenger@Net - eDMSAPI
       - Port 3401]
"Shortcut"="\"C:\\SOPHO Messenger@Net\\Exe\\eDMSAPI.exe\" /Site:1 /
       eKernel address:147.93.169.130 /eKernel port:3401 /Log drive:C"
"Windowstyle"="1"
```

XML image

The Subscriber receives the result of the GetImage in a flat-file repository, located in the following directory:

```
C:\SOPHO Messenger@Net\Xml
```

IMPORTANT!

This directory must be created manually on Subscriber systems. Also a copy of the Messenger_CFG.mdb with the exact layout of the database of the publisher must be created in this directory. If the database is missing or has incorrect layout, system malfunction results. An update of eKERNEL on the Publisher site must always be synchronized with the same update on subscribers systems, and the eKERNEL can automatically add changes to the database at startup. Therefore, after applying a new version of eKERNEL, you must first start eKERNEL, and then copy the Messenger_CFG.mdb database.

If you install new versions of eKERNEL, you must synchronize the eKERNEL modules on all systems. Also the latest layout of Messenger_CFG of publisher (after automatic upgrade changes at first run) must be manually placed in the directory of the Subscribers.

GetImage puts a file Messenger_CFG.xml in the same directory, and replaces this file on receipt of a GetImage result.

If you want to review this file, make a copy in another location before doing so, for example, C:\Temp. You can, for example, launch the Internet Explorer and associate XML files to this program, as Internet Explorer has built-in functionality to parse XML documents.

WARNING
Do not open the file in the C:\SOPHO Messenger@Net\Xml, because the file can be allocated by the viewer, and must be replaced when the next KeepAlive result is received.

SQL script

When a Subscriber detects a change between P:1and P:0:

1 The Subscriber ends all running tasks associated with the current environment.

At this time, Messenger functionality is disrupted, and pending and new alarms can be lost.

2 The SQL image in C:\SOPHO Messenger@Net\Xml repository Messenger_CFG.xml is imported to the workspace C:\SOPHO Messenger@Net\Xml access database Messenger_CFG.mdb. For this reason, the Messenger_CFG.mdb on Publisher and Subscriber sites must always use the same layout.

Thus the following repositories exist:

- (original database on publisher)

```
C:\SOPHO Messenger@Net\Mdb\Messenger_CFG.mdbat publisher
```

- (transferred as XML images through HTTP)

```
C:\SOPHO Messenger@Net\Xml\Messenger_CFG.xmlat
      subscriber
```

- (converted into MDB on subscriber)

```
C:\SOPHO Messenger@Net\Xml\Messenger_CFG.mdbat
      subscriber
```

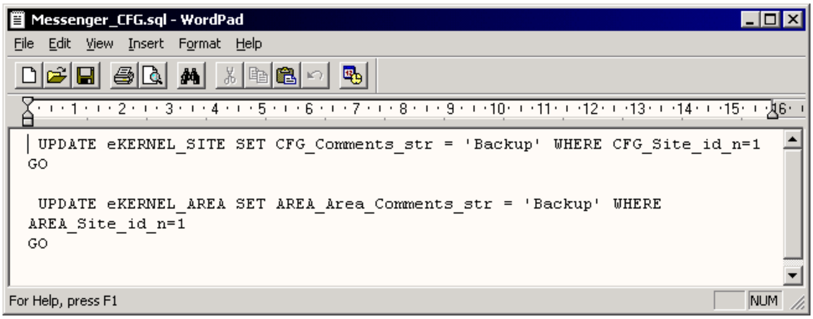
- (processed through optional SQL script, described in Figure 557 on page 1262)

```
C:\SOPHO Messenger@Net\Xml\Messenger_CFG.mdbat
      subscriber
```

- (activated on subscriber)

```
C:\SOPHO Messenger@Net\Mdb\Messenger_CFG.mdbat
      subscriber
```

Figure 557
Sample SQL script



Messenger_CFG.sql - WordPad
File Edit View Insert Format Help
For Help, press F1
NUM

```
UPDATE eKERNEL_SITE SET CFG_Comments_str = 'Backup' WHERE CFG_Site_id_n=1
GO

 UPDATE eKERNEL_AREA SET AREA_Area_Comments_str = 'Backup' WHERE
AREA_Site_id_n=1
GO
```

Use this (optional) SQL script to modify the contents of the database, as arrived from the operational publisher system. In some environments no changes are required; in more demanding customer environments complex scenarios can be set up to allow applying changes to the database. This can include changing .COM ports, IP address, group members, and so on. Review your SQL changes carefully.

Switch back

When Publisher or Subscribers detect a change in the availability image, a switch to another environment – or switch-back to the original environment – can be appropriate.

Conclusion

Careful planning and testing is required. Nortel recommends you simulate every configured scenario, and analyse in detail the possible impact of every scenario. An off-site testing procedure in a lab environment is usually appropriate, to prevent loss of alarms (during change in image, eKERNEL and other modules are stopped and all alarms can be lost).

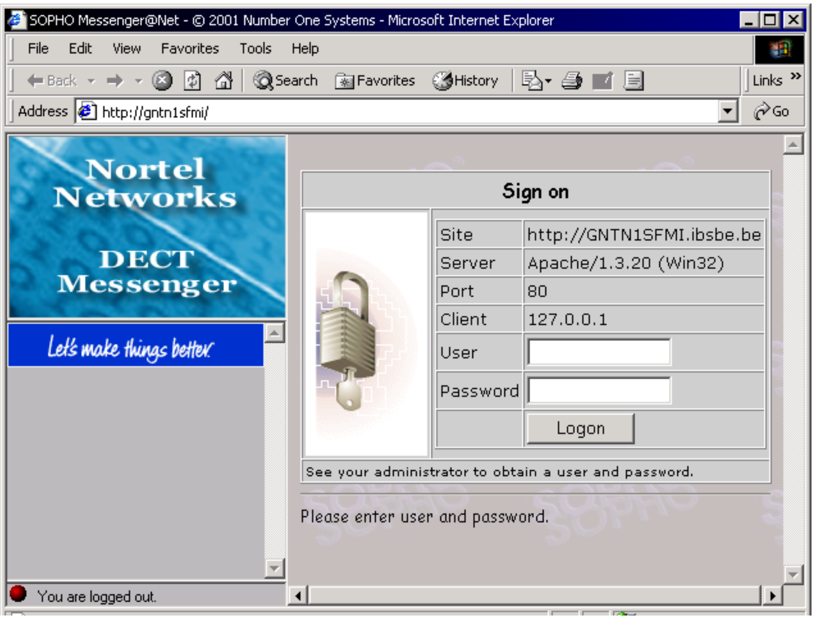
Also, take into account that having a high-availability solution in place affects change management. Changes applied to eKERNEL must be synchronized, and (automatic) database upgrade changes to Messenger_CFG.MDB must be handled manually by the system administrator.

Finally, note that configuration changes with eCONFIG, eGRID, eWEB, or another configuration tool can affect the total environment. For example, a divert to another device does not work in a backup environment if the destination device in not available, or the module is unavailable. Therefore, due to the nature of such an architecture, and maintenance issues and customer specific factors that are beyond our control, the authors of eTH_HA cannot accept responsibility for malfunction of the software.

Module – eWEB

When you start your web browser application and navigate to the DECT Messenger system that has the eWEB module operational, a window opens similar to the one shown in Figure 558. Contact the system administrator to obtain the URL address assigned to the system.

Figure 558
eWEB module Sign-on



SOPHO Messenger@Net - © 2001 Number One Systems - Microsoft Internet Explorer

Address: http://gntn1sfmi/

Sign on

Site	http://GNTN1SFMI.ibsbe.be
Server	Apache/1.3.20 (Win32)
Port	80
Client	127.0.0.1
User	
Password	

See your administrator to obtain a user and password.

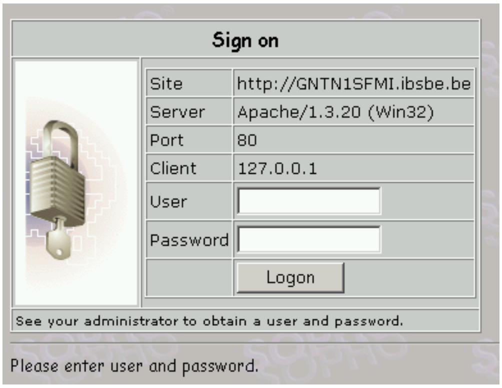
Please enter user and password.

You are logged out.

Sign-on procedure

A sign-on is required; because you are not yet authenticated to the application, this window is presented in English.

Figure 559
Sign on information



Sign on

Site	http://GNTN1SFMI.ibsbe.be
Server	Apache/1.3.20 (Win32)
Port	80
Client	127.0.0.1
User	
Password	

See your administrator to obtain a user and password.

Please enter user and password.

On the lower left-hand side of the window, user status is displayed, indicating that you are not logged in at this time, similar to the following:

● You are logged out.

To start working, you must log in with a valid user and password combination. The password is displayed as a series of asterisks (*) during entry.

The user and password is checked against the eWEB_USER_AUTH table. Refer to the documentation for “Table: eWEB_USER_AUTH” on page 1515 for more information.

When a valid user and password is found, you can continue working in the eWEB module.

It is important to know that during the sign on procedure, two additional parameters are fetched: the language code and the security level.

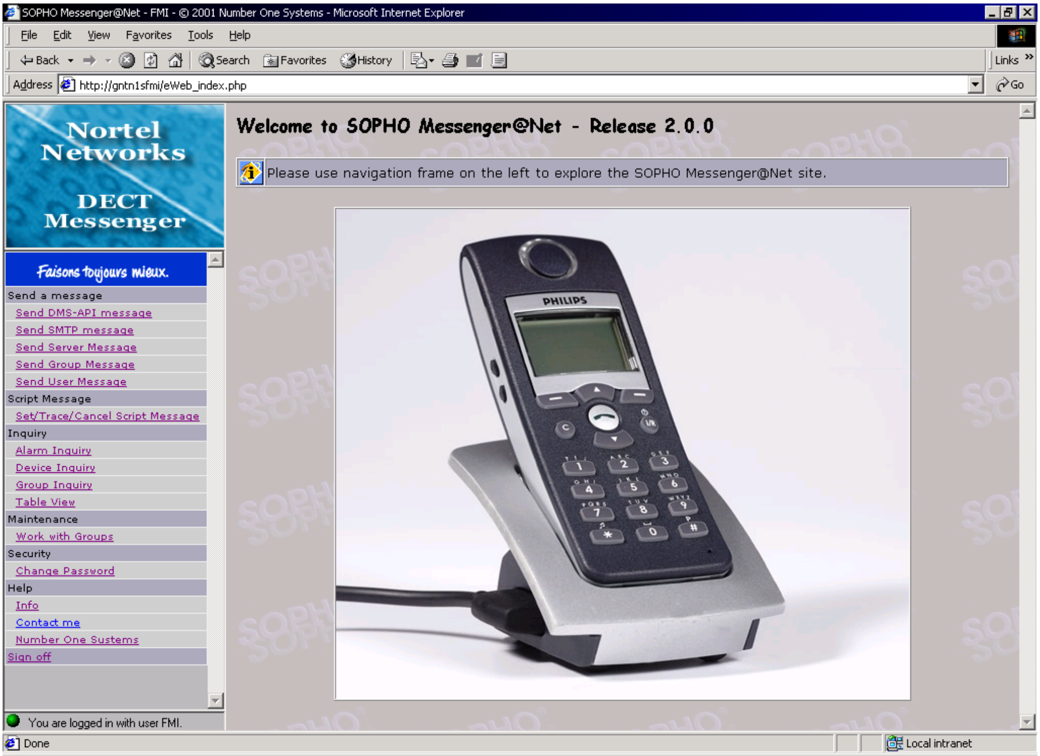
The language code determines the language of the forms that are presented to the user. If for example the language code is 2909 – Belgian English, the panels are in English. If the language code is 2963 – Belgian Dutch, the panels are in Dutch.

The security level determines the table-of-contents options that are presented to the user. A user with a limited security level has only a small number of options available, whereas a user with a high security level has many options available. Refer to the documentation of "Table: eWEB_TOC" on page 1507 for more information on the table-of-contents mechanism.

In the illustrations on the following pages, the user shown has a language code that refers to English forms, and a security level that gives access to all available options. The information displayed varies depending on your security level and language code.

When you sign on, a window similar to the one shown in Figure 560 on page 1268 is displayed.

Figure 560
eWEB main window



SOPHO Messenger@Net - FMI - © 2001 Number One Systems - Microsoft Internet Explorer

Address http://gntn1sfmi/eWeb_index.php

Welcome to SOPHO Messenger@Net - Release 2.0.0

Please use navigation frame on the left to explore the SOPHO Messenger@Net site.

You are logged in with user FMI.

Done

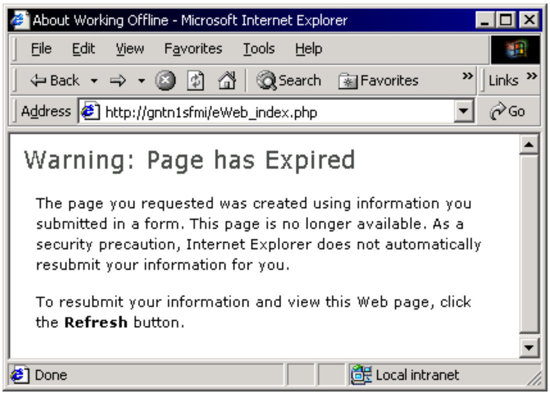
Sign-off procedure

To log off, choose the last option in the list on the left side of the window, Sign off. You are also automatically logged off when either of the following occurs:

- Twelve hours elapse after initial sign-on.
- You leave the eWEB web site, for instance by selecting another URL in the address field of your browser or selecting another web site through Favorites, Home, Back, and so on.

Figure 561 on page 1269 shows an expired state, requiring a new logon.

Figure 561
Expired login



About Working Offline - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Links
Address http://gntn1sfmi/eWeb_index.php Go

Warning: Page has Expired

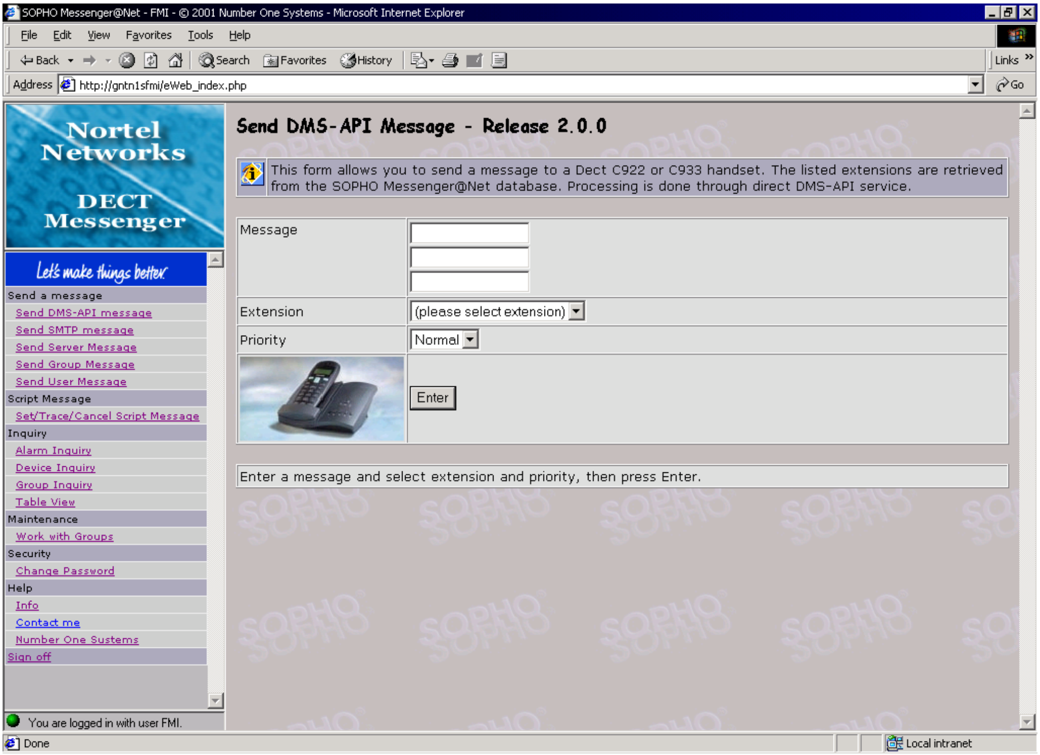
The page you requested was created using information you submitted in a form. This page is no longer available. As a security precaution, Internet Explorer does not automatically resubmit your information for you.

To resubmit your information and view this Web page, click the **Refresh** button.

Send DMS-API Message

The Send DMS-API Message window is shown in Figure 562.

Figure 562
Send DMS-API Message



Send DMS-API Message - Release 2.0.0

This form allows you to send a message to a Dect C922 or C933 handset. The listed extensions are retrieved from the SOPHO Messenger@Net database. Processing is done through direct DMS-API service.

Message	
Extension	(please select extension)
Priority	Normal

Enter a message and select extension and priority, then press Enter.

You are logged in with user FMI.

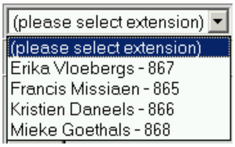
This function allows you to send an E2-data message to a peripheral that is capable of receiving messages through this technology. The web interface presents all DECT extensions that are defined in the eKERNEL_DEVICE table for the local site and area and the output program eDMSAPI.

IMPORTANT!

The eWEB application is configured in the eWEB table, and identifies its site and area based upon the IP address of the Apache Web Server. Therefore, it lists only those devices that are defined for that same site and area. In a multi-area environment, you can access the devices that belong to another area. You can assign these remote area devices on device level in the eKERNEL_DEVICE table, where the DEV_Ras_Area_b value must be set to **True**.

Figure 563 shows the list of extensions that all reside locally on the same site and area.

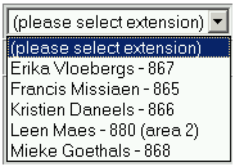
Figure 563
Local extensions



(please select extension)
(please select extension)
Erika Vloebergs - 867
Francis Missiaen - 865
Kristien Daneels - 866
Mieke Goethals - 868

Figure 564 shows the list of extensions that all reside locally on the same site and area, but also displays an extension that resides on another area, which is made available through the DEC_Ras_Area_b value in the eKERNEL_DEVICE table.

Figure 564
Local and remote extensions



(please select extension)
(please select extension)
Erika Vloebergs - 867
Francis Missiaen - 865
Kristien Daneels - 866
Leen Maes - 880 (area 2)
Mieke Goethals - 868

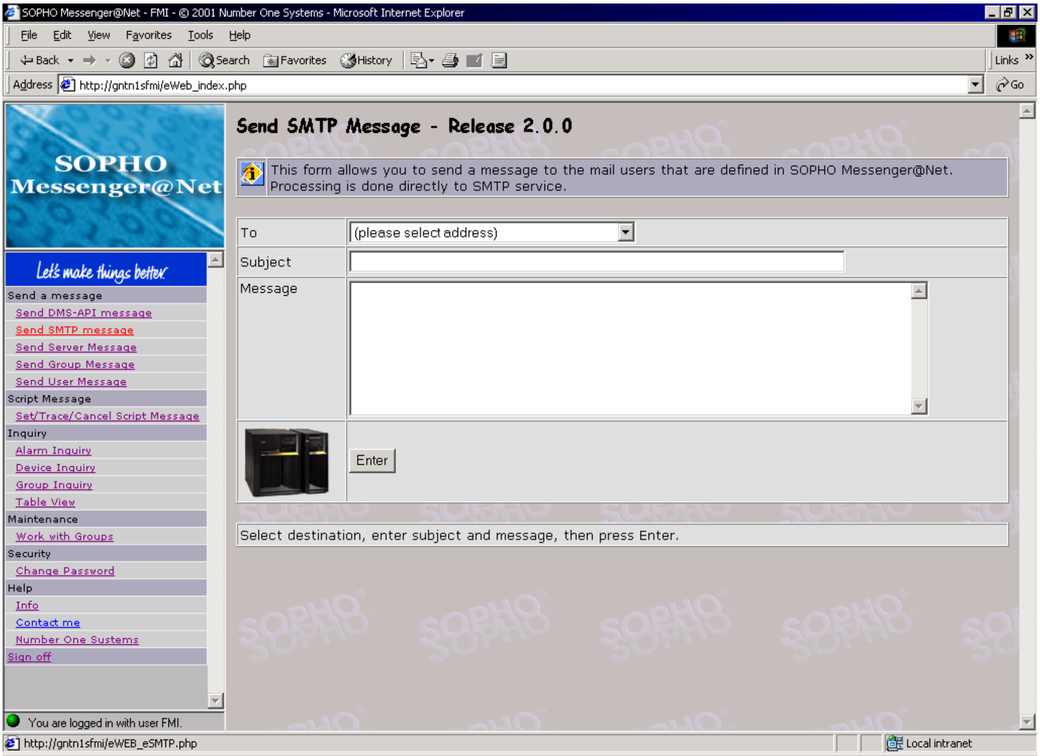
> ***Note:*** The Send DMS-API Message form always contacts that local DMS-API Service of the same site and area as the Apache Web Server. In a multi-area environment, where there are possible multiple eDMSAPI applications defined, the local DMS-API service contacts all peripherals.

The user can enter a message and the message type (normal or urgent) and click **Enter** to transmit the message. The application waits for message delivery or failure. In the case of urgent messages, this delay can sometimes be quite long because the application waits for the user to acknowledge receipt of the message by pressing **OK** on the DECT handset.

Send SMTP Message

The Send SMTP Message window is shown in Figure 565.

Figure 565
Send SMTP Message



Send SMTP Message - Release 2.0.0

This form allows you to send a message to the mail users that are defined in SOPHO Messenger@Net. Processing is done directly to SMTP service.

To	(please select address)
Subject	
Message	

Select destination, enter subject and message, then press Enter.

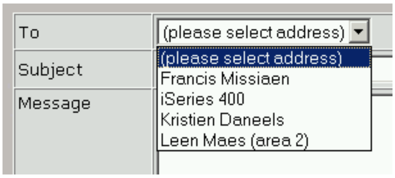
You are logged in with user FMI.

This function allows the user to send a message to a mail address destination, by means of an SMTP connection between the Apache Web Server and the SMTP server of the mail server. In this process, no eKERNEL activity takes place, because the transaction is executed directly.

The list of available addresses is limited to the devices that are defined in eKERNEL_DEVICE table, and defined for the same site and area as the eWEB application, and with output program eSMTP.

You can also make devices that are allocated to a remote area available through the DEV_Ras_Area_b value in the eKERNEL_DEVICE table. An example is shown in Figure 566:

Figure 566
Sending messages to remote addresses



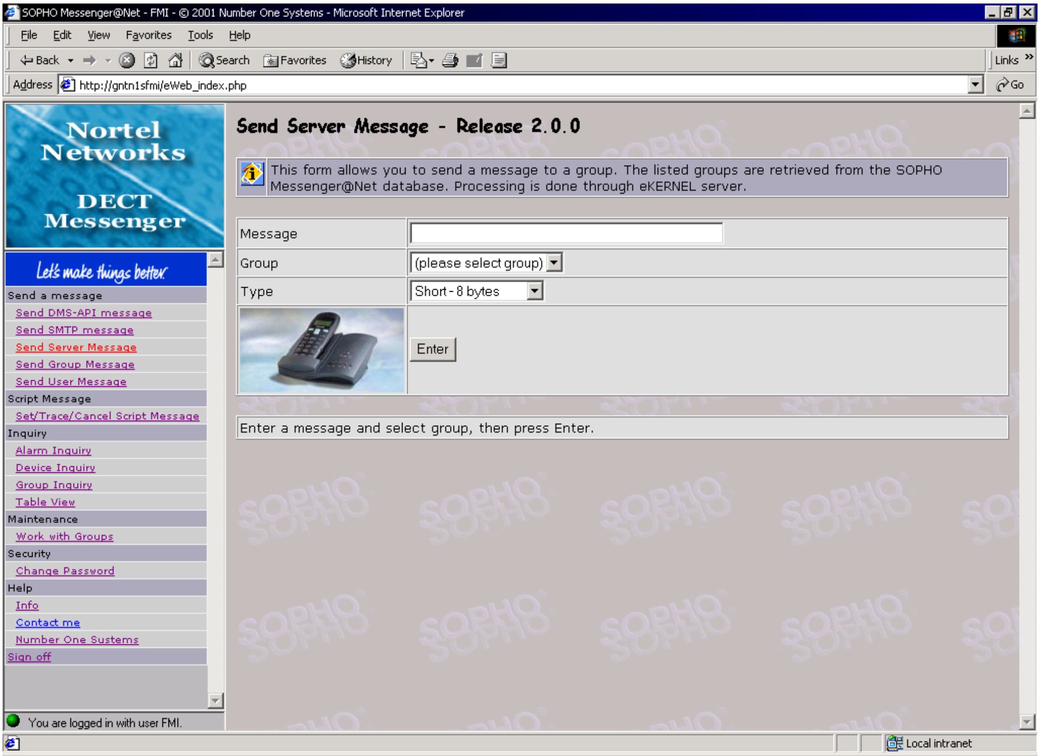
As a result, the SMTP server is contacted, and a message is sent. The IP address and port number is retrieved for the server defined in the eSMTP_CLIENT table, with a matching site and area as used by the Apache Web Server.

The mail is sent following the specs of RFC821. In the composed mail, the MAIL FROM: keyword is automatically retrieved from the definition in the eWEB_USER_AUTH table. As a result, when the destination user replies to the mail, the reply arrives in the correct mailbox of the sender.

Send Server Message

The Send Server Message window is shown in Figure 567.

Figure 567
Send Server Message



SOPHO Messenger@Net - FMI - © 2001 Number One Systems - Microsoft Internet Explorer

http://gntn1sfmi/eWeb_index.php

Send Server Message - Release 2.0.0

This form allows you to send a message to a group. The listed groups are retrieved from the SOPHO Messenger@Net database. Processing is done through eKERNEL server.

Message	
Group	(please select group)
Type	Short - 8 bytes

Enter a message and select group, then press Enter.

You are logged in with user FMI.

Send Server Message is a function that communicates to the eKERNEL module.

This is the opposite of the Send DMS-API Message and Send SMTP Message, both of which directly access the underlying services and ignore the eKERNEL module for processing. A major advantage of using Send Server Message is that it utilizes more product features, including: logging, sending to a group of users, assigning alarm types, priorities, addressing any kind of peripherals, implementing confirmation procedures, implementing alternatives devices, and so on.

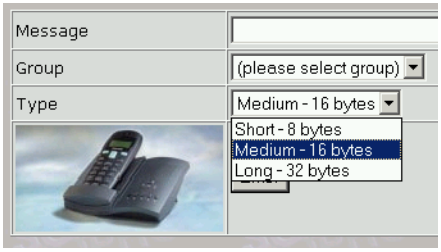
Because Send Server Message communicates with eKERNEL, a number of configuration actions are required. One of them is specifying alarm identifiers in the eKERNEL_ALARM tabl, for the input program that is assigned to the eWEB instance. At this time, you can define for instance alarm types with different lengths (for example, short messages of 8 bytes, medium messages of 16 bytes and long messages of 32 bytes).

IMPORTANT!

Because the Send Server Message is designed only to set a message, and cannot reset a message, you must always specify remove after *SENT in the eKERNEL_ALARM table, otherwise the message remains active forever.

In the example shown in Figure 568, you can choose between three alarm types, which are defined in the eKERNEL_ALARM table.

Figure 568
Alarm types



Message	
Group	(please select group)
Type	Medium - 16 bytes

IMPORTANT!

You can only access alarm types in the eKERNEL_ALARM table with field ALA_Trace_b equal to False. While assigning alarm types, always make a distinction between alarms for Send Server Message (False) and Send Script Message (True).

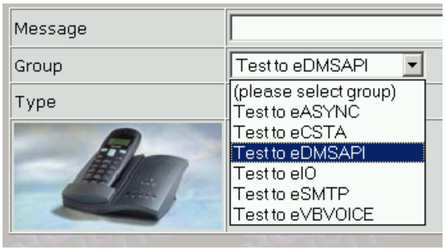
The destination of the message is also defined in the database. The eWEB module has an input program identifier, and one or more alarm definitions. For the same input program, you also must predefine the group, group members and group authorities in the corresponding tables eKERNEL_GROUP, eKERNEL_GROUP_MEMBER and eKERNEL_GROUP_AUTH.

The web user is able only to select from the list of groups that are configured for that input program.

> ***Note:*** The web user can *submit* a message to the eKERNEL, but is not able to verify that the message actually arrives at the destination address. One potential issue is that a message can be sent to a group that is empty (it has no peripherals defined as group members). Another issue can arise if a group is configured in such way that, due to the definitions in eKERNEL_GROUP_MEMBER, no one is active in the group, based upon hour, day, holiday and activation interval issues. eWEB users must be aware of these possibilities.

In the sample shown in Figure 569, six groups are defined (it is advisable to use more descriptive group names than those shown in the example).

Figure 569
Group list



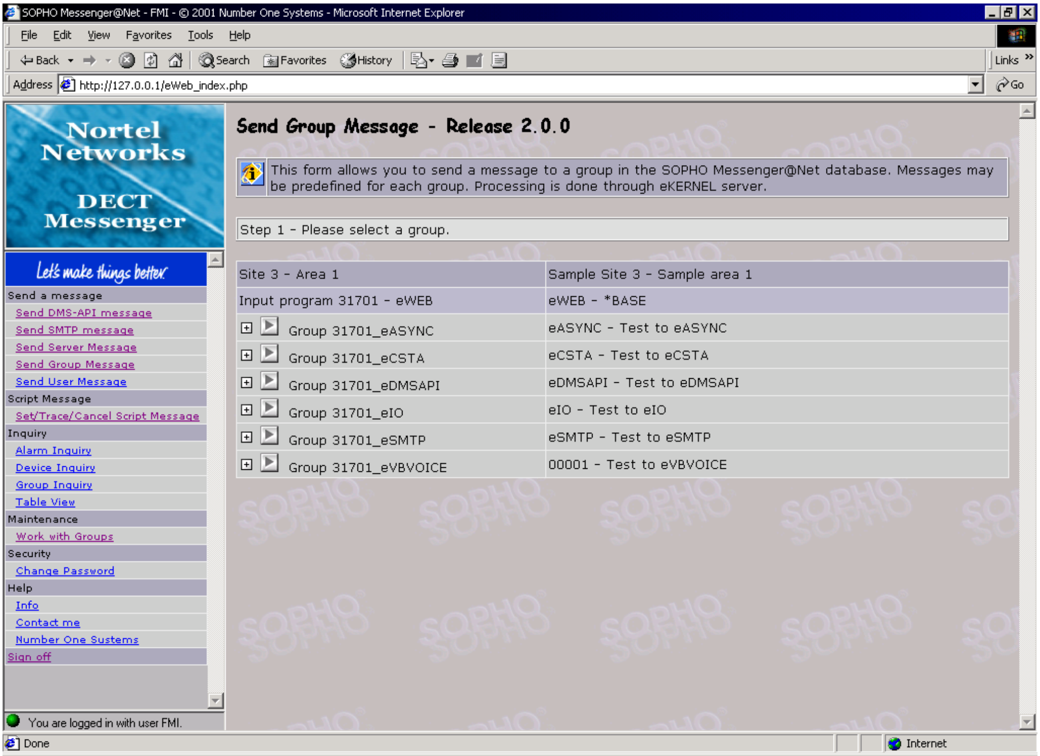
Message	
Group	Test to eDMSAPI
Type	

(please select group)
Test to eASYNC
Test to eCSTA
Test to eDMSAPI
Test to eIO
Test to eSMTP
Test to eVBVOICE

Send Group Message

The Send Group Message window is shown in Figure 570:

Figure 570
Send Group Message



Send Group Message - Release 2.0.0

This form allows you to send a message to a group in the SOPHO Messenger@Net database. Messages may be predefined for each group. Processing is done through eKERNEL server.

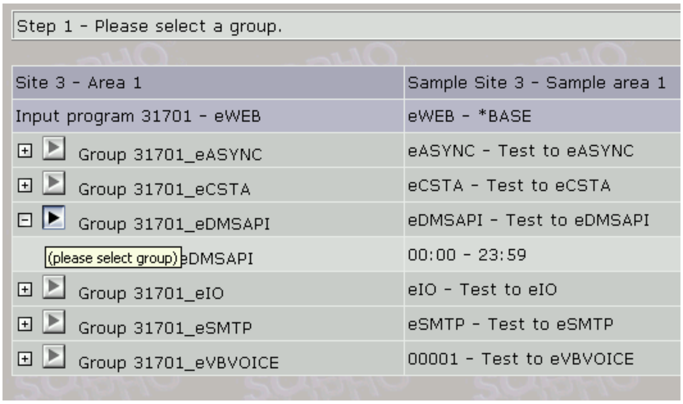
Step 1 - Please select a group.

Site 3 - Area 1	Sample Site 3 - Sample area 1
Input program 31701 - eWEB	eWEB - *BASE
⊞ ▷ Group 31701_eASYNC	eASYNC - Test to eASYNC
⊞ ▷ Group 31701_eCSTA	eCSTA - Test to eCSTA
⊞ ▷ Group 31701_eDMSAPI	eDMSAPI - Test to eDMSAPI
⊞ ▷ Group 31701_eIO	eIO - Test to eIO
⊞ ▷ Group 31701_eSMTP	eSMTP - Test to eSMTP
⊞ ▷ Group 31701_eVBVOICE	00001 - Test to eVBVOICE

In step 1, shown in Figure 571 on page 1280, you can choose from a list of groups. These groups are retrieved from the eKERNEL_GROUP and eKERNEL_GROUP_MEMBER tables. All the groups that use a matching input program with the appropriate eWEB module (site/area) are shown to the user. Collapse or expand the group to see the group members.

Click the arrow to select the group.

Figure 571
Select a group



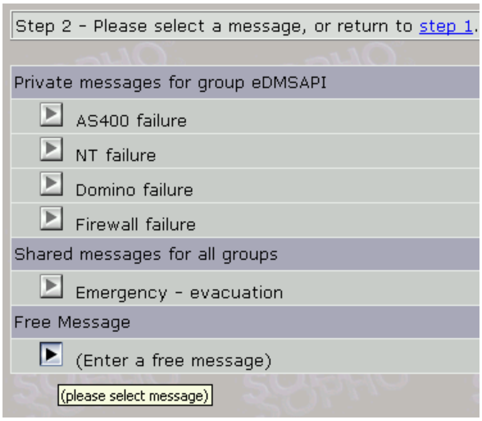
Step 1 - Please select a group.

Site 3 - Area 1	Sample Site 3 - Sample area 1
Input program 31701 - eWEB	eWEB - *BASE
⊞ ▷ Group 31701_eASYNC	eASYNC - Test to eASYNC
⊞ ▷ Group 31701_eCSTA	eCSTA - Test to eCSTA
⊟ ▶ Group 31701_eDMSAPI	eDMSAPI - Test to eDMSAPI
(please select group) eDMSAPI	00:00 - 23:59
⊞ ▷ Group 31701_eIO	eIO - Test to eIO
⊞ ▷ Group 31701_eSMTP	eSMTP - Test to eSMTP
⊞ ▷ Group 31701_eVBVOICE	00001 - Test to eVBVOICE

The next step offers an overview of the group messages that are preconfigured for the selected group. As shown in Figure 572, the eWEB_SNDGRPMSG table can define private messages per group, shared messages for all groups and also user messages.

In the example shown in Figure 572, the administrator has configured four private messages, one fixed message and one user-specified message:

Figure 572
Select a message



Step 2 - Please select a message, or return to step 1.

Private messages for group eDMSAPI

▷ AS400 failure

▷ NT failure

▷ Domino failure

▷ Firewall failure

Shared messages for all groups

▷ Emergency - evacuation

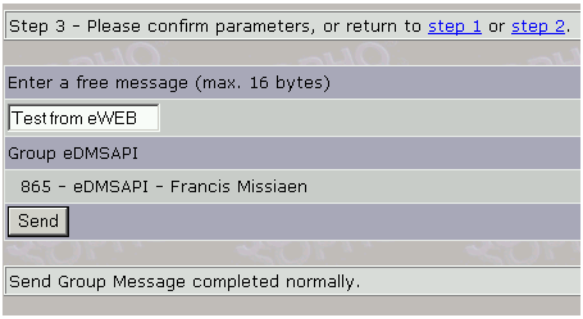
Free Message

▶ (Enter a free message)

(please select message)

Finally, you can send the request to eKERNEL and submit the request for further processing. The example shown in Figure 573 shows a situation in which a user-defined message has been selected, so you must enter the message text manually.

Figure 573
Confirm and send message



Step 3 - Please confirm parameters, or return to step 1 or step 2.

Enter a free message (max. 16 bytes)

Test from eWEB

Group eDMSAPI

865 - eDMSAPI - Francis Missiaen

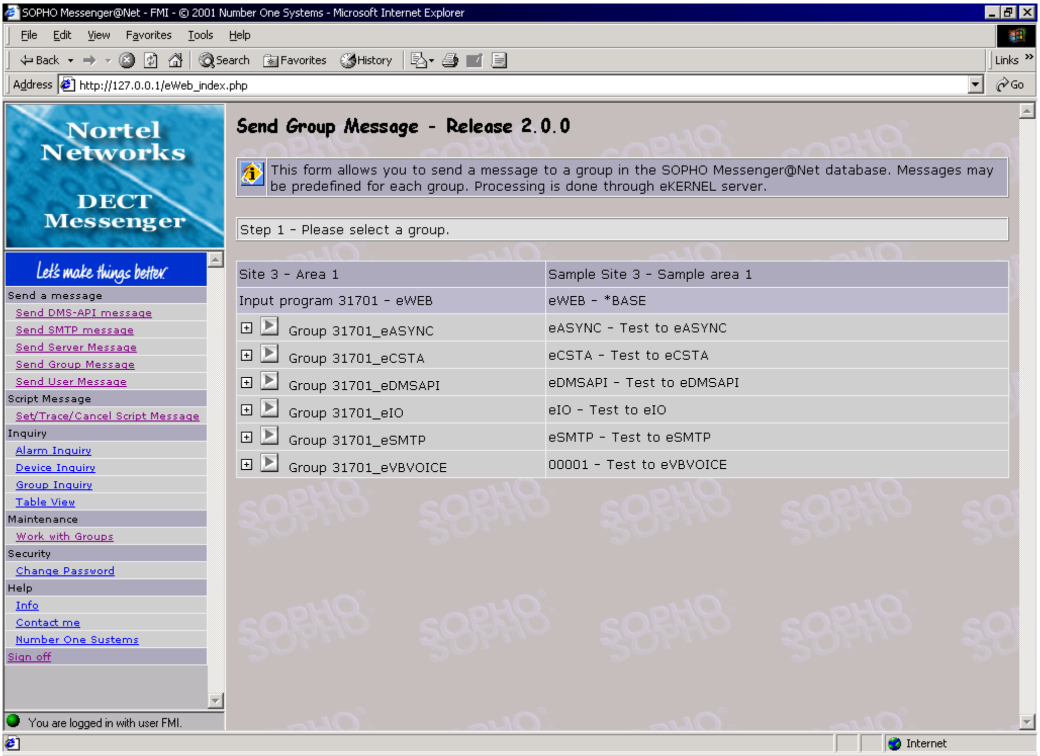
Send Group Message completed normally.

The Send Group Message completed normally message indicates the message has been submitted to eKERNEL. Final message delivery depends on a number of factors and are beyond control of the eWEB user.

Send User Message

The Send User Message window is shown in Figure 574.

Figure 574
Send user message



Send Group Message - Release 2.0.0

This form allows you to send a message to a group in the SOPHO Messenger@Net database. Messages may be predefined for each group. Processing is done through eKERNEL server.

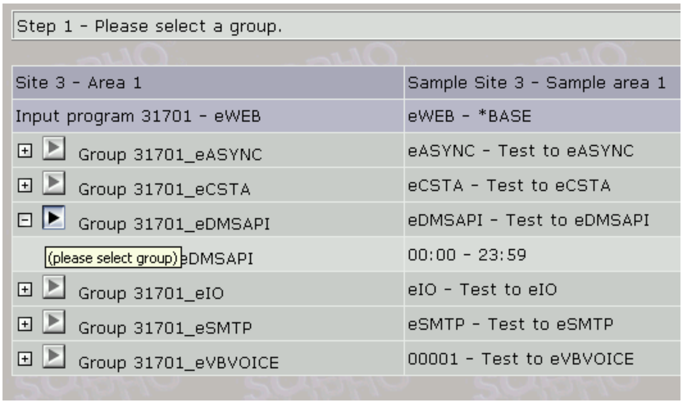
Step 1 - Please select a group.

Site 3 - Area 1	Sample Site 3 - Sample area 1
Input program 31701 - eWEB	eWEB - *BASE
⊞ ▷ Group 31701_eASYNC	eASYNC - Test to eASYNC
⊞ ▷ Group 31701_eCSTA	eCSTA - Test to eCSTA
⊞ ▷ Group 31701_eDMSAPI	eDMSAPI - Test to eDMSAPI
⊞ ▷ Group 31701_eIO	eIO - Test to eIO
⊞ ▷ Group 31701_eSMTP	eSMTP - Test to eSMTP
⊞ ▷ Group 31701_eVBVOICE	00001 - Test to eVBVOICE

In step 1, a list of groups is presented, as shown in Figure 575 on page 1283. These groups are retrieved from the eKERNEL_GROUP and eKERNEL_GROUP_MEMBER tables. All the groups that use a matching input program with the appropriate eWEB module (site/area) are shown to the user. Collapse or expand the group to see the group members.

Click the arrow to select the group.

Figure 575
Select the group



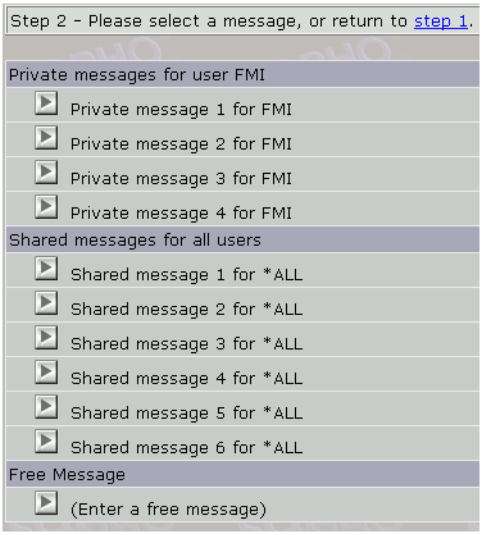
Step 1 - Please select a group.

Site 3 - Area 1	Sample Site 3 - Sample area 1
Input program 31701 - eWEB	eWEB - *BASE
⊞ ▷ Group 31701_eASYNC	eASYNC - Test to eASYNC
⊞ ▷ Group 31701_eCSTA	eCSTA - Test to eCSTA
⊟ ▶ Group 31701_eDMSAPI	eDMSAPI - Test to eDMSAPI
(please select group) eDMSAPI	00:00 - 23:59
⊞ ▷ Group 31701_eIO	eIO - Test to eIO
⊞ ▷ Group 31701_eSMTP	eSMTP - Test to eSMTP
⊞ ▷ Group 31701_eVBVOICE	00001 - Test to eVBVOICE

Step 2 provides an overview of the user messages that are preconfigured for your current user profiles, which is used during the login procedure in the initial window of eWEB. As shown in Figure 576 on page 1284, the eWEB_SNDUSRMSG table can define private messages per user, shared messages for all users, or user-defined entered messages.

In the example shown in Figure 576 on page 1284, the administrator has configured four private messages, six fixed messages, and a user-defined message.

Figure 576
Select a message



Step 2 - Please select a message, or return to step 1.

Private messages for user FMI

- ▶ Private message 1 for FMI
- ▶ Private message 2 for FMI
- ▶ Private message 3 for FMI
- ▶ Private message 4 for FMI

Shared messages for all users

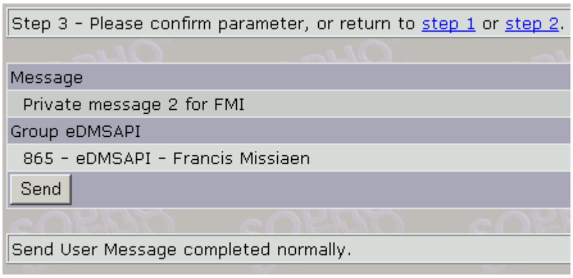
- ▶ Shared message 1 for *ALL
- ▶ Shared message 2 for *ALL
- ▶ Shared message 3 for *ALL
- ▶ Shared message 4 for *ALL
- ▶ Shared message 5 for *ALL
- ▶ Shared message 6 for *ALL

Free Message

- ▶ (Enter a free message)

Finally you can send the request to eKERNEL and submit the request for further processing. Note that the example in Figure 577 shows a fixed message and therefore message text need not be entered.

Figure 577
Confirm your choices



Step 3 - Please confirm parameter, or return to step 1 or step 2.

Message

Private message 2 for FMI

Group eDMSAPI

865 - eDMSAPI - Francis Missiaen

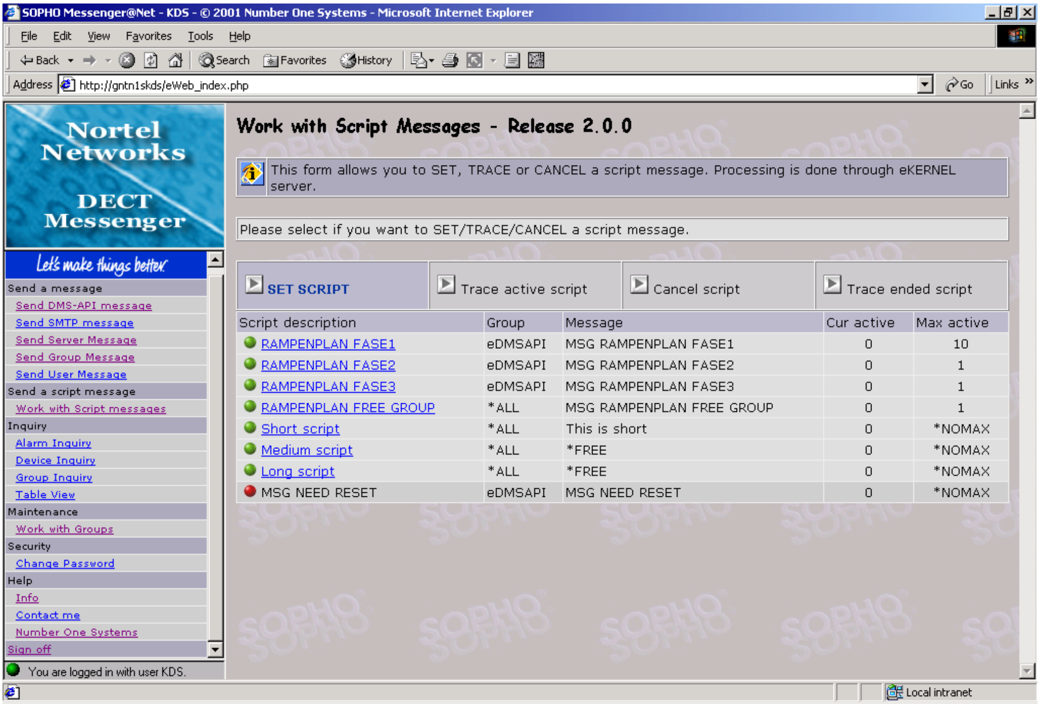
Send User Message completed normally.

When the message is submitted to eKERNEL, the message “Send User Message completed normally” is displayed. Final message delivery depends on a number of factors and are beyond control of the eWEB user.

Send Script Message

The Work with Script Messages window is shown in Figure 578.

Figure 578
Send script message



Work with Script Messages - Release 2.0.0

This form allows you to SET, TRACE or CANCEL a script message. Processing is done through eKERNEL server.

Please select if you want to SET/TRACE/CANCEL a script message.

Script description	Group	Message	Cur active	Max active
● RAMPENPLAN FASE1	eDMSAPI	MSG RAMPENPLAN FASE1	0	10
● RAMPENPLAN FASE2	eDMSAPI	MSG RAMPENPLAN FASE2	0	1
● RAMPENPLAN FASE3	eDMSAPI	MSG RAMPENPLAN FASE3	0	1
● RAMPENPLAN FREE GROUP	*ALL	MSG RAMPENPLAN FREE GROUP	0	1
● Short script	*ALL	This is short	0	*NOMAX
● Medium script	*ALL	*FREE	0	*NOMAX
● Long script	*ALL	*FREE	0	*NOMAX
● MSG NEED RESET	eDMSAPI	MSG NEED RESET	0	*NOMAX

You are logged in with user KDS.

You can choose from the following sub-functions:

- **Set Script** is used to activate a script. The scripts are defined the eWEB_SCRIPT table.
- **Trace Active Script** is used to see an overview of activated scripts. These scripts are still running.
- **Cancel Script** is used to abort a script that has been activated.

- **Trace ended Script** is used to see an overview of these scripts that are completed.

For more information, refer to:

- “Table: eWEB_SCRIPT” on page 1489
- “Table: eWEB_SCRIPT_SET_AUTH” on page 1493
- “Table: eWEB_SCRIPT_TRACE_AUTH” on page 1495
- “Table: eWEB_SCRIPT_CANCEL_AUTH” on page 1497

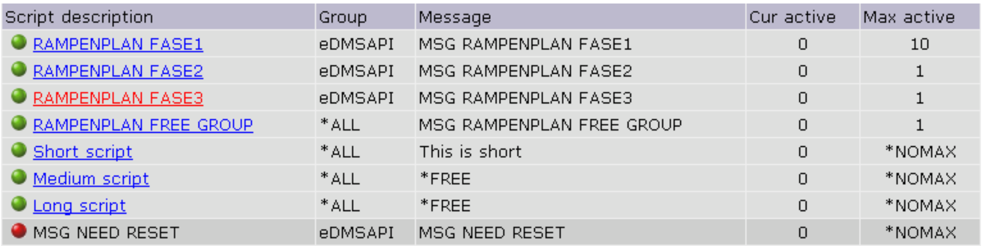
Set Script

Choose Set Script to browse an overview of defined scripts, as shown in Figure 579. A green or red icon indicates if the eWEB user is authorised to activate the script. The window also shows additional information; as follows:

- The identifier of the group.
- The message that is sent to the group members.
- The current number of instances of the script currently active.
- The maximum number of instances of the script that can be active.

The illustration in Figure 579 shows that the current user is authorised to set the first seven scripts, but not authorised for the last script. No script is currently active.

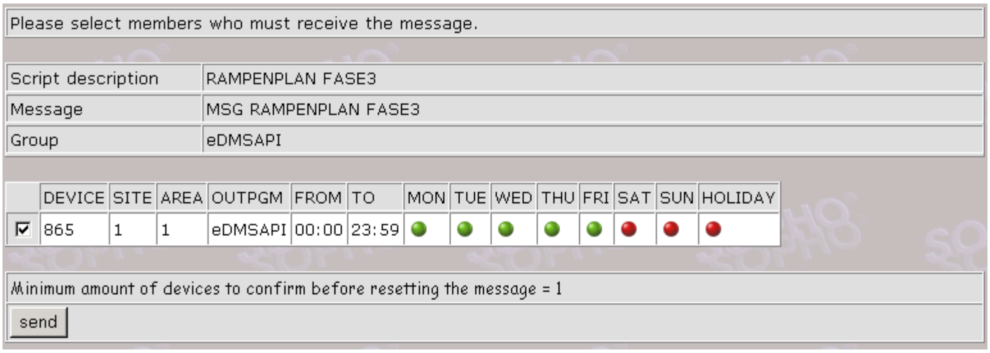
Figure 579
Overview of defined scripts



Script description	Group	Message	Cur active	Max active
🟢 RAMPENPLAN FASE1	eDMSAPI	MSG RAMPENPLAN FASE1	0	10
🟢 RAMPENPLAN FASE2	eDMSAPI	MSG RAMPENPLAN FASE2	0	1
🟢 RAMPENPLAN FASE3	eDMSAPI	MSG RAMPENPLAN FASE3	0	1
🟢 RAMPENPLAN FREE GROUP	*ALL	MSG RAMPENPLAN FREE GROUP	0	1
🟢 Short script	*ALL	This is short	0	*NOMAX
🟢 Medium script	*ALL	*FREE	0	*NOMAX
🟢 Long script	*ALL	*FREE	0	*NOMAX
🔴 MSG NEED RESET	eDMSAPI	MSG NEED RESET	0	*NOMAX

In Figure 580, the third script has been activated, and more detailed information on the script is provided (only one such script can be activated at a time). The window shows us that one device is a member of the group, and the device is configured to be available 24/24 hours and 7/7 days. A minimum of one device must confirm the alarm, therefore you must not clear the device selection.

Figure 580
Script details



Please select members who must receive the message.

Script description	RAMPENPLAN FASE3
Message	MSG RAMPENPLAN FASE3
Group	eDMSAPI

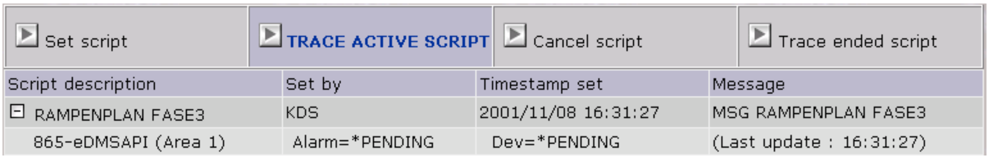
	DEVICE	SITE	AREA	OUTPGM	FROM	TO	MON	TUE	WED	THU	FRI	SAT	SUN	HOLIDAY
☑	865	1	1	eDMSAPI	00:00	23:59	🟢	🟢	🟢	🟢	🟢	🔴	🔴	🔴

Minimum amount of devices to confirm before resetting the message = 1

Trace Active Script

Use Trace Active Script, shown in Figure 581, to monitor the event handling of scripts that are active.

Figure 581
Trace active script

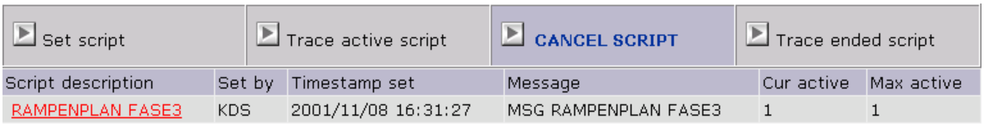


Script description	Set by	Timestamp set	Message
⊟ RAMPENPLAN FASE3	KDS	2001/11/08 16:31:27	MSG RAMPENPLAN FASE3
865-eDMSAPI (Area 1)	Alarm=*PENDING	Dev=*PENDING	(Last update : 16:31:27)

Cancel Script

Use Cancel Script to abort an active script. Figure 582 on page 1288 shows one active script.

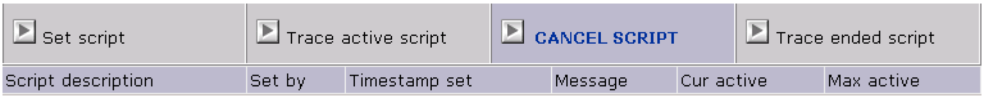
Figure 582
Cancel script



Script description	Set by	Timestamp set	Message	Cur active	Max active
RAMPENPLAN FASE3	KDS	2001/11/08 16:31:27	MSG RAMPENPLAN FASE3	1	1

Cancelled scripts are removed from the list, as shown in Figure 583.

Figure 583
Cancelled script removed from the list

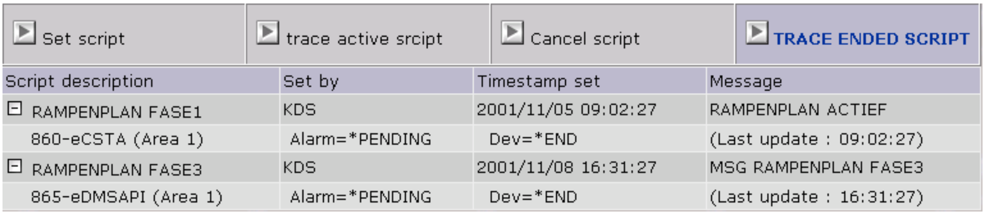


Script description	Set by	Timestamp set	Message	Cur active	Max active

Trace Ended Script

Trace Ended Script, shown in Figure 584, allows you to monitor the event handling of scripts that are finished.

Figure 584
Trace Ended Script



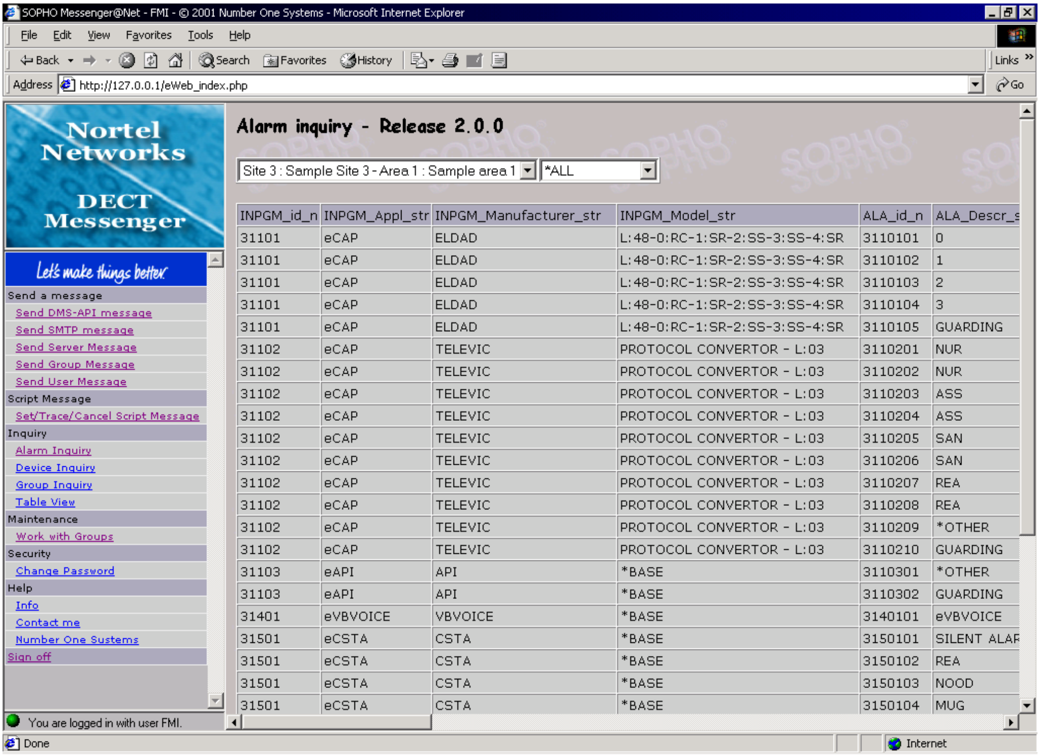
Script description	Set by	Timestamp set	Message
⊟ RAMPENPLAN FASE1	KDS	2001/11/05 09:02:27	RAMPENPLAN ACTIEF
860-eCSTA (Area 1)	Alarm=*PENDING	Dev=*END	(Last update : 09:02:27)
⊟ RAMPENPLAN FASE3	KDS	2001/11/08 16:31:27	MSG RAMPENPLAN FASE3
865-eDMSAPI (Area 1)	Alarm=*PENDING	Dev=*END	(Last update : 16:31:27)

Alarm Inquiry

Alarm Inquiry allows you to see all relevant parameters for the eKERNEL_ALARM file as shown in Figure 585 on page 1289. Only those records are shown that refer to the site where the current eWEB instance resides.

The information is retrieved from two tables: eKERNEL_ALARM and eKERNEL_INPGM. You can either display data for all input programs (by specifying *ALL) or select one input program.

Figure 585
Alarm inquiry



Alarm inquiry - Release 2.0.0

Site 3 : Sample Site 3 - Area 1 : Sample area 1

*ALL

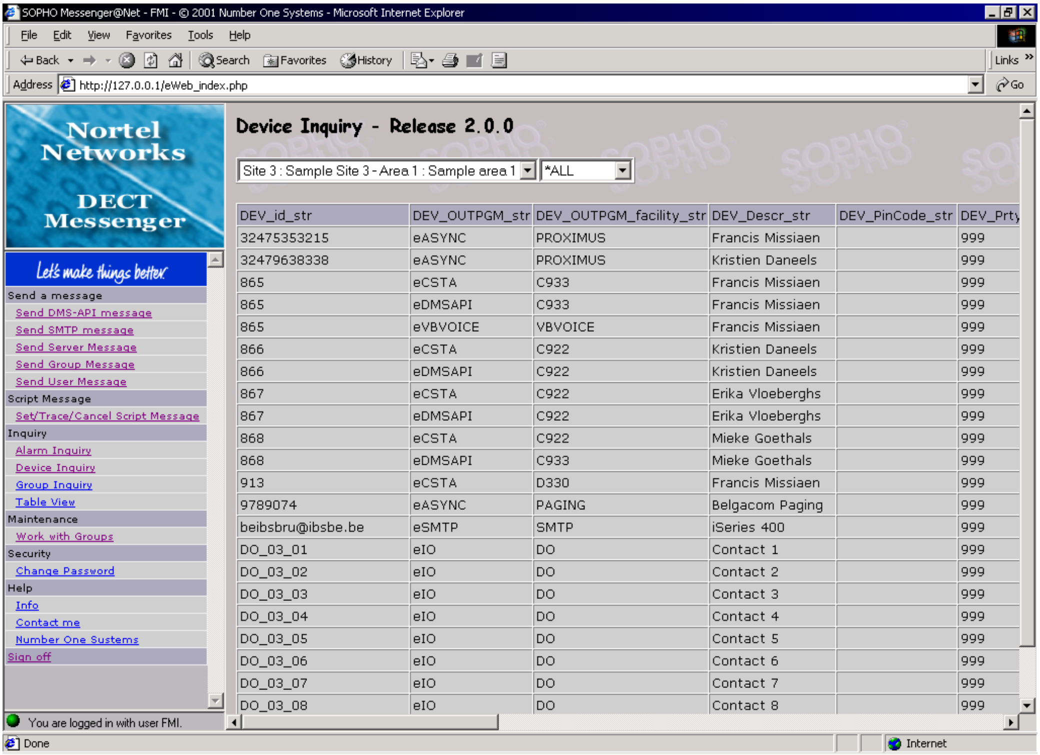
INPGM_id_n	INPGM_Appl_str	INPGM_Manufacturer_str	INPGM_Model_str	ALA_id_n	ALA_Descr_s
31101	eCAP	ELDAD	L:48-0:RC-1:SR-2:SS-3:SS-4:SR	3110101	0
31101	eCAP	ELDAD	L:48-0:RC-1:SR-2:SS-3:SS-4:SR	3110102	1
31101	eCAP	ELDAD	L:48-0:RC-1:SR-2:SS-3:SS-4:SR	3110103	2
31101	eCAP	ELDAD	L:48-0:RC-1:SR-2:SS-3:SS-4:SR	3110104	3
31101	eCAP	ELDAD	L:48-0:RC-1:SR-2:SS-3:SS-4:SR	3110105	GUARDING
31102	eCAP	TELEVIC	PROTOCOL CONVERTOR - L:03	3110201	NUR
31102	eCAP	TELEVIC	PROTOCOL CONVERTOR - L:03	3110202	NUR
31102	eCAP	TELEVIC	PROTOCOL CONVERTOR - L:03	3110203	ASS
31102	eCAP	TELEVIC	PROTOCOL CONVERTOR - L:03	3110204	ASS
31102	eCAP	TELEVIC	PROTOCOL CONVERTOR - L:03	3110205	SAN
31102	eCAP	TELEVIC	PROTOCOL CONVERTOR - L:03	3110206	SAN
31102	eCAP	TELEVIC	PROTOCOL CONVERTOR - L:03	3110207	REA
31102	eCAP	TELEVIC	PROTOCOL CONVERTOR - L:03	3110208	REA
31102	eCAP	TELEVIC	PROTOCOL CONVERTOR - L:03	3110209	*OTHER
31102	eCAP	TELEVIC	PROTOCOL CONVERTOR - L:03	3110210	GUARDING
31103	eAPI	API	*BASE	3110301	*OTHER
31103	eAPI	API	*BASE	3110302	GUARDING
31401	eVBVOICE	VBVOICE	*BASE	3140101	eVBVOICE
31501	eCSTA	CSTA	*BASE	3150101	SILENT ALAR
31501	eCSTA	CSTA	*BASE	3150102	REA
31501	eCSTA	CSTA	*BASE	3150103	NOOD
31501	eCSTA	CSTA	*BASE	3150104	MUG

Device Inquiry

The device inquiry allows you to see all relevant parameters for the eKERNEL_DEVICE file, as shown in Figure 586 on page 1290. Only those records are shown that refer to the site where the current eWEB instance resides.

The information is retrieved from one table: eKERNEL_DEVICE. You can either display data for all output programs (by specifying *ALL) or select one output program.

Figure 586
Device inquiry



Device Inquiry - Release 2.0.0

Site 3 : Sample Site 3 - Area 1 : Sample area 1 | *ALL

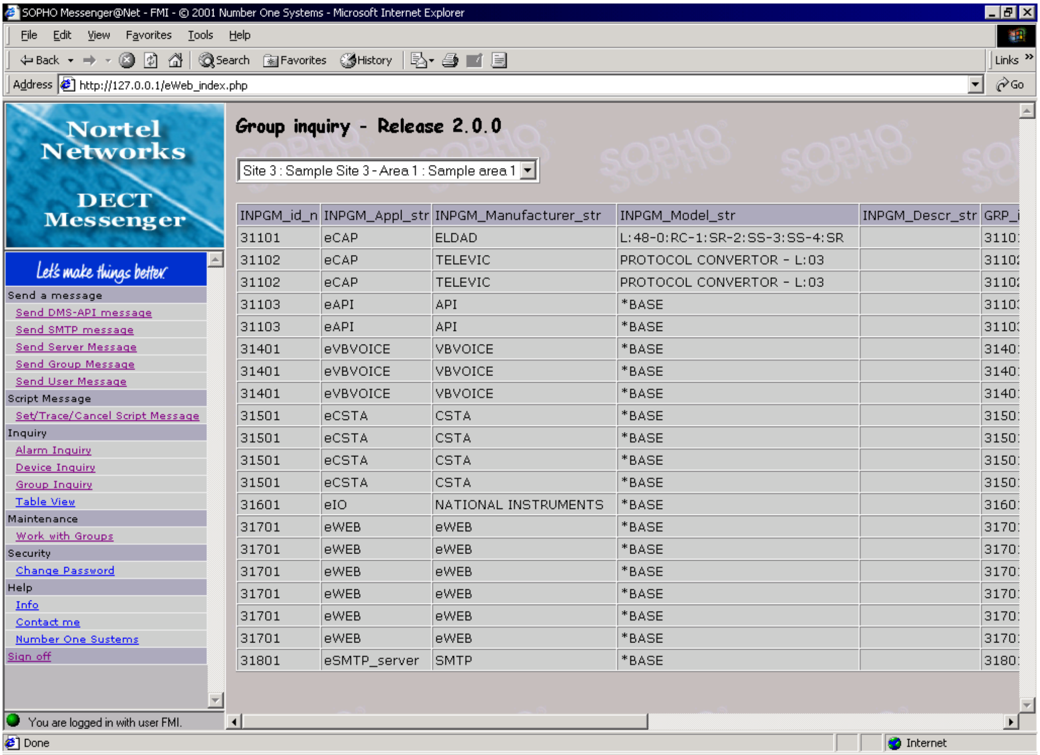
DEV_id_str	DEV_OUTPGM_str	DEV_OUTPGM_facility_str	DEV_Descr_str	DEV_PinCode_str	DEV_Prty
32475353215	eASYNC	PROXIMUS	Francis Missiaen		999
32479638338	eASYNC	PROXIMUS	Kristien Daneels		999
865	eCSTA	C933	Francis Missiaen		999
865	eDMSAPI	C933	Francis Missiaen		999
865	eVBVOICE	VBVOICE	Francis Missiaen		999
866	eCSTA	C922	Kristien Daneels		999
866	eDMSAPI	C922	Kristien Daneels		999
867	eCSTA	C922	Erika Vloeberghs		999
867	eDMSAPI	C922	Erika Vloeberghs		999
868	eCSTA	C922	Mieke Goethals		999
868	eDMSAPI	C933	Mieke Goethals		999
913	eCSTA	D330	Francis Missiaen		999
9789074	eASYNC	PAGING	Belgacom Paging		999
beibsbru@ibsbe.be	eSMTP	SMTP	iSeries 400		999
DO_03_01	eIO	DO	Contact 1		999
DO_03_02	eIO	DO	Contact 2		999
DO_03_03	eIO	DO	Contact 3		999
DO_03_04	eIO	DO	Contact 4		999
DO_03_05	eIO	DO	Contact 5		999
DO_03_06	eIO	DO	Contact 6		999
DO_03_07	eIO	DO	Contact 7		999
DO_03_08	eIO	DO	Contact 8		999

Group Inquiry

The group inquiry allows you to see all relevant parameters for the eKERNEL_GROUP and eKERNEL_GROUP_MEMBER files, as shown in Figure 587 on page 1291. Only those records are shown that refer to the site where the current eWEB instance resides.

The information is retrieved from multiple tables: eKERNEL_GROUP, eKERNEL_GROUP_MEMBER, eKERNEL_INPGM, eKERNEL_DEVICE, eKERNEL_SITE and eKERNEL_AREA. You can select the data for each area.

Figure 587
Group Inquiry



Group inquiry - Release 2.0.0

Site 3 : Sample Site 3 - Area 1 : Sample area 1

INPGM_id_n	INPGM_Appl_str	INPGM_Manufacturer_str	INPGM_Model_str	INPGM_Descr_str	GRP_i
31101	eCAP	ELDAD	L:48-0:RC-1:SR-2:SS-3:SS-4:SR		3110
31102	eCAP	TELEVIC	PROTOCOL CONVERTOR - L:03		3110
31102	eCAP	TELEVIC	PROTOCOL CONVERTOR - L:03		3110
31103	eAPI	API	*BASE		3110
31103	eAPI	API	*BASE		3110
31401	eVBVOICE	VBVOICE	*BASE		3140
31401	eVBVOICE	VBVOICE	*BASE		3140
31401	eVBVOICE	VBVOICE	*BASE		3140
31501	eCSTA	CSTA	*BASE		3150
31501	eCSTA	CSTA	*BASE		3150
31501	eCSTA	CSTA	*BASE		3150
31501	eCSTA	CSTA	*BASE		3150
31601	eIO	NATIONAL INSTRUMENTS	*BASE		3160
31701	eWEB	eWEB	*BASE		3170
31701	eWEB	eWEB	*BASE		3170
31701	eWEB	eWEB	*BASE		3170
31701	eWEB	eWEB	*BASE		3170
31701	eWEB	eWEB	*BASE		3170
31701	eWEB	eWEB	*BASE		3170
31801	eSMTP_server	SMTP	*BASE		3180

Table View

The Table View function allows you to perform inquiry functions of all tables available in Messenger_CFG database. Only users with security administrator special authority rights can access the eWEB_USER_AUTH file. Users who lack security administrator special authority rights cannot access this table, which contains sensitive information such as passwords. An example of a table is shown in Figure 588 on page 1292.

Figure 588
Table View

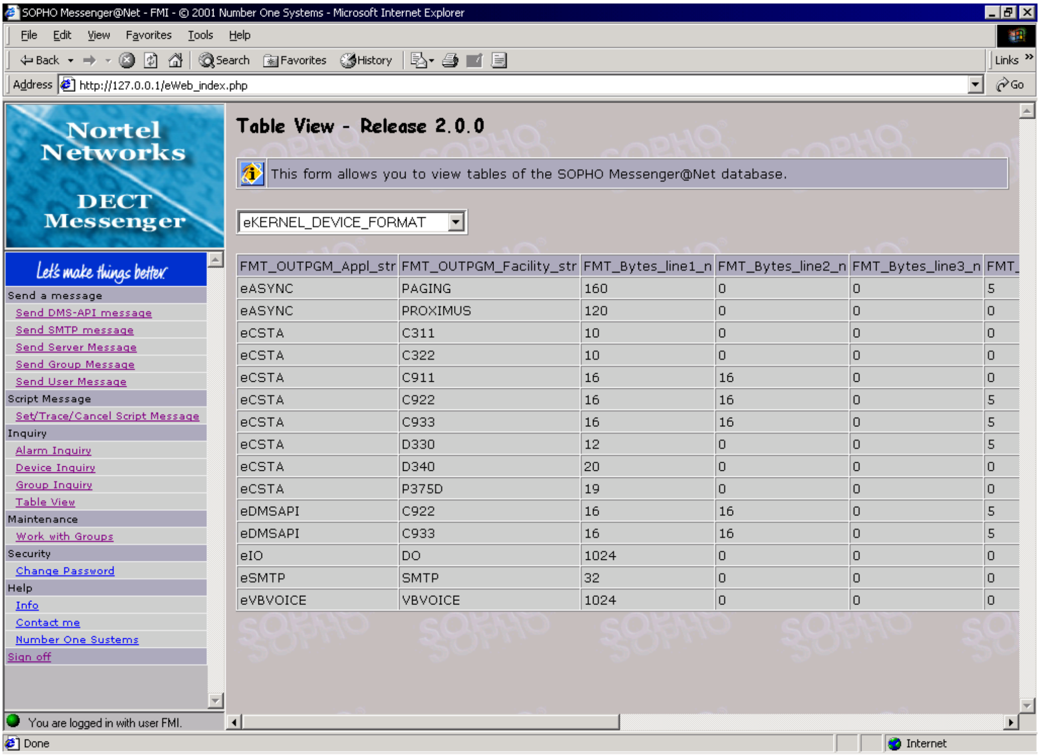


Table View - Release 2.0.0

This form allows you to view tables of the SOPHO Messenger@Net database.

eKERNEL_DEVICE_FORMAT

FMT_OUTPGM_Appl_str	FMT_OUTPGM_Facility_str	FMT_Bytes_line1_n	FMT_Bytes_line2_n	FMT_Bytes_line3_n	FMT_
eASYNC	PAGING	160	0	0	5
eASYNC	PROXIMUS	120	0	0	0
eCSTA	C311	10	0	0	0
eCSTA	C322	10	0	0	0
eCSTA	C911	16	16	0	0
eCSTA	C922	16	16	0	5
eCSTA	C933	16	16	0	5
eCSTA	D330	12	0	0	5
eCSTA	D340	20	0	0	0
eCSTA	P375D	19	0	0	0
eDMSAPI	C922	16	16	0	5
eDMSAPI	C933	16	16	0	5
eIO	DO	1024	0	0	0
eSMTP	SMTP	32	0	0	0
eVBVOICE	VBVOICE	1024	0	0	0

You are logged in with user FMI.

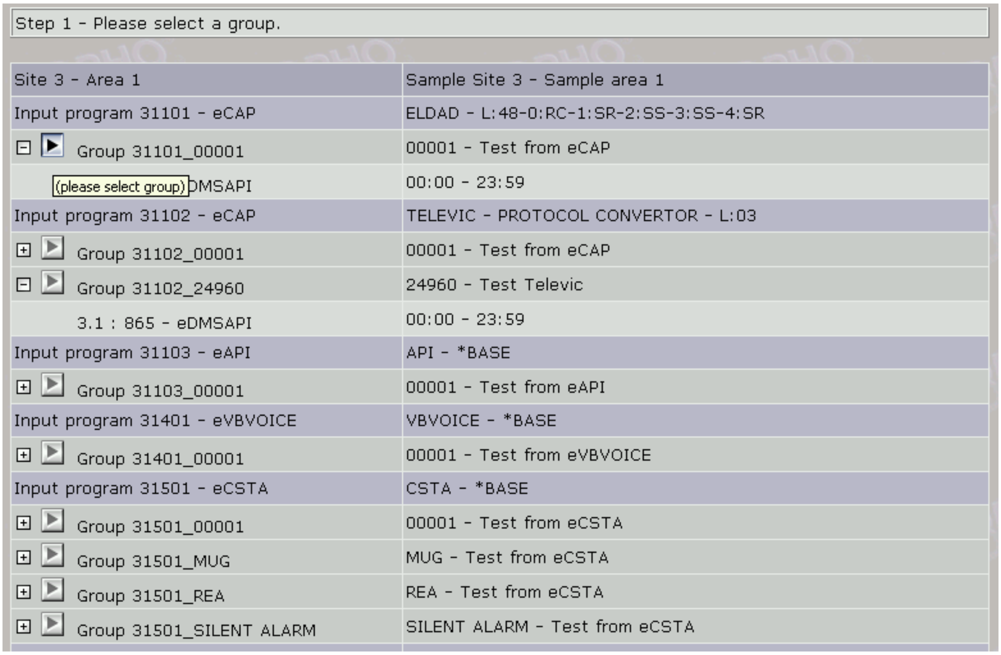
Work with Groups

Click **Work with Groups** to access group maintenance functions. Users with all object special authority can access all groups, while users without these rights can access only groups specified in eKERNEL_GROUP_AUTH.

> ***Note:*** If no groups are shown, the user has no all object special authority, or no access to any group. You must grant if necessary access to one or more groups through the eKERNEL_GROUP_AUTH table.

In step 1, shown in Figure 589 on page 1293, select a group. You can collapse or expand a group to preview the group member information.

Figure 589
Select a group

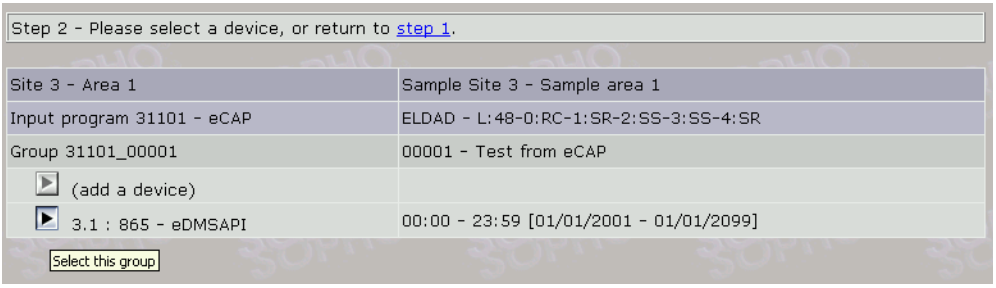


Step 1 - Please select a group.

Site 3 - Area 1	Sample Site 3 - Sample area 1
Input program 31101 - eCAP	ELDAD - L:48-0:RC-1:SR-2:SS-3:SS-4:SR
⊟ ▶ Group 31101_00001	00001 - Test from eCAP
(please select group)DMSAPI	00:00 - 23:59
Input program 31102 - eCAP	TELEVIC - PROTOCOL CONVERTOR - L:03
⊞ ▷ Group 31102_00001	00001 - Test from eCAP
⊟ ▷ Group 31102_24960	24960 - Test Televic
3.1 : 865 - eDMSAPI	00:00 - 23:59
Input program 31103 - eAPI	API - *BASE
⊞ ▷ Group 31103_00001	00001 - Test from eAPI
Input program 31401 - eVBVOICE	VBVOICE - *BASE
⊞ ▷ Group 31401_00001	00001 - Test from eVBVOICE
Input program 31501 - eCSTA	CSTA - *BASE
⊞ ▷ Group 31501_00001	00001 - Test from eCSTA
⊞ ▷ Group 31501_MUG	MUG - Test from eCSTA
⊞ ▷ Group 31501_REA	REA - Test from eCSTA
⊞ ▷ Group 31501_SILENT ALARM	SILENT ALARM - Test from eCSTA

Next, you can either maintain an existing device or add a new device. The example shown in Figure 590 demonstrates selecting an existing device for maintenance (update or delete).

Figure 590
Select a device



Step 2 - Please select a device, or return to step 1.

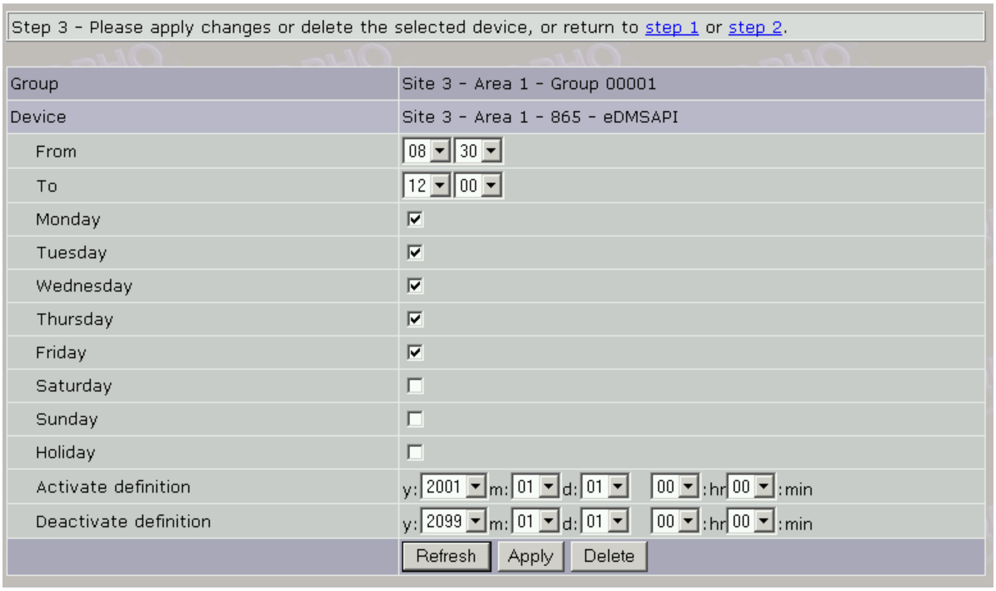
Site 3 - Area 1	Sample Site 3 - Sample area 1
Input program 31101 - eCAP	ELDAD - L:48-0:RC-1:SR-2:SS-3:SS-4:SR
Group 31101_00001	00001 - Test from eCAP
▷ (add a device)	
▶ 3.1 : 865 - eDMSAPI	00:00 - 23:59 [01/01/2001 - 01/01/2099]

The values displayed when you choose Work with Groups refer to the fields in the eKERNEL_GROUP_MEMBER table. Refer to “Table: eKERNEL_GROUP_MEMBER” on page 1431 for details. The example shown in Figure 591 defines the extension 865 to be available on working days only between 8:30 and 12:00. Note that the record is disabled on Saturdays, Sundays and holidays.

IMPORTANT!

The last two fields (Activate definition and Deactivate definition) allow you to specify an interval during which the record is active. In the example shown in Figure 591, the record is active from January 1, 2001 at 00:00 until December 31, 23:59. This functionality allows administrators and power users with group maintenance rights to predefine schedules that are activated and deactivated automatically. This functionality can add flexibility in your group maintenance in handling holiday planning, staff schedules, and so on.

Figure 591
Confirm changes

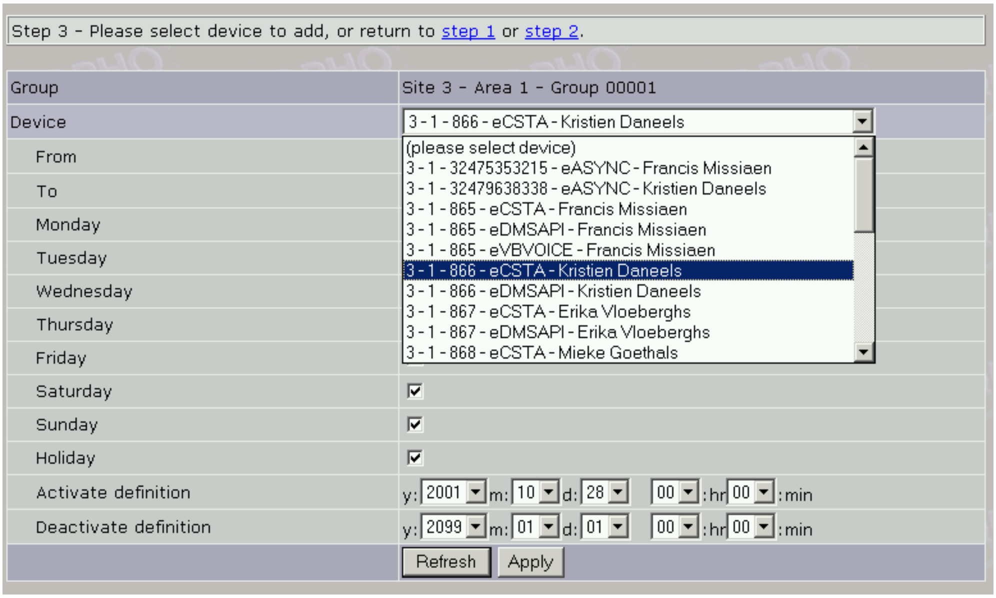


Step 3 - Please apply changes or delete the selected device, or return to step 1 or step 2.

Group	Site 3 - Area 1 - Group 00001
Device	Site 3 - Area 1 - 865 - eDMSAPI
From	08 30
To	12 00
Monday	☑
Tuesday	☑
Wednesday	☑
Thursday	☑
Friday	☑
Saturday	□
Sunday	□
Holiday	□
Activate definition	y: 2001 m: 01 d: 01 00 :hr 00 :min
Deactivate definition	y: 2099 m: 01 d: 01 00 :hr 00 :min

If you select to add a new device, a window similar to the one in Figure 592 is shown. Select one of the configured devices and specify the additional parameters prior to adding the device.

Figure 592
Select new device



Step 3 - Please select device to add, or return to step 1 or step 2.

Group	Site 3 - Area 1 - Group 00001
Device	3 - 1 - 866 - eCSTA - Kristien Daneels
From	
To	
Monday	
Tuesday	
Wednesday	
Thursday	
Friday	
Saturday	☑
Sunday	☑
Holiday	☑
Activate definition	y: 2001 m: 10 d: 28 00 :hr 00 :min
Deactivate definition	y: 2099 m: 01 d: 01 00 :hr 00 :min

(please select device)
3 - 1 - 32475353215 - eASYNC - Francis Missiaen
3 - 1 - 32479638338 - eASYNC - Kristien Daneels
3 - 1 - 865 - eCSTA - Francis Missiaen
3 - 1 - 865 - eDMSAPI - Francis Missiaen
3 - 1 - 865 - eVBVOICE - Francis Missiaen
3 - 1 - 866 - eCSTA - Kristien Daneels
3 - 1 - 866 - eDMSAPI - Kristien Daneels
3 - 1 - 867 - eCSTA - Erika Vloeberghs
3 - 1 - 867 - eDMSAPI - Erika Vloeberghs
3 - 1 - 868 - eCSTA - Mieke Goethals
Refresh
Apply

Note: You can access only the devices that belong to the same site as used by the eWEB module. Figure 592 shows devices of site 3 because, in this example, eWEB is running in site 3 – area 1.

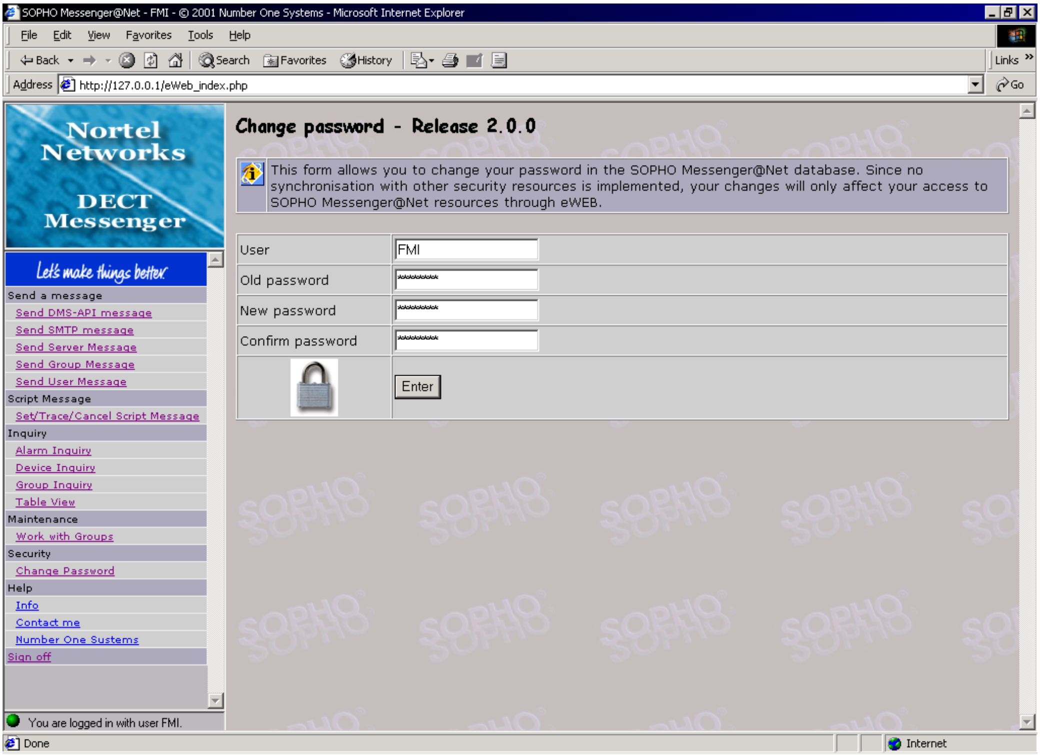
Change Password

Change Password allows you to enter a new password. You must enter:

- your User ID
- your old password
- your new password
- your new password (for verification)

This option eliminates the need for an eGRID-based administration of passwords of existing user profiles.

Figure 593
Change password



Address: http://127.0.0.1/eWeb_index.php

Change password - Release 2.0.0

This form allows you to change your password in the SOPHO Messenger@Net database. Since no synchronisation with other security resources is implemented, your changes will only affect your access to SOPHO Messenger@Net resources through eWEB.

User	FMI
Old password	*********
New password	*********
Confirm password	*********
	Enter

You are logged in with user FMI.

Note: More advanced security settings or resetting passwords of users that forgot their password, still must be performed through eGRID in the eWEB_USER_AUTH table. Some additional tables (with extension _AUTH) are available for more detailed security implementation.

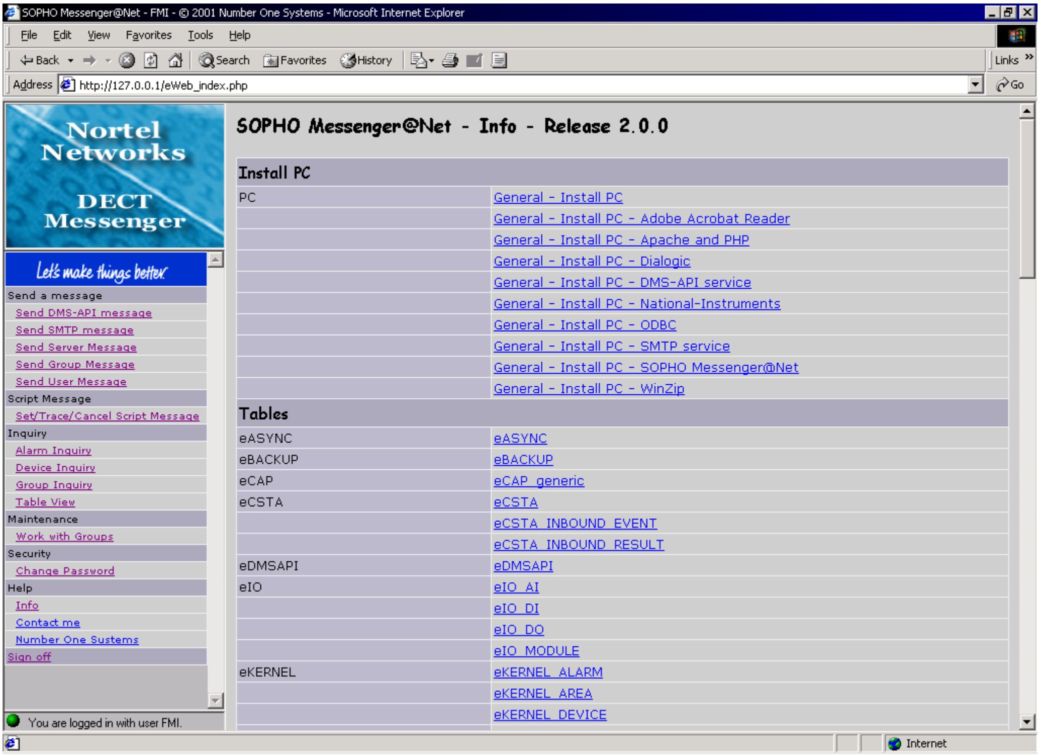
Info

The Info page provides web-based access to Adobe Portable Document Format (.PDF) files. The eWEB user must install on their desktop PC a suitable Adobe Acrobat Reader to open the .PDF files.

A .PDF reader is shipped on the CD-ROM, but if you can access the Internet, Nortel recommends you download the software from the Adobe web site.

There are .PDF files that handle installation issues, others that provide information on table configuration issues, and others that are more module functional.

Figure 594
Info: more documentation



You are logged in with user FMI.

SOPHO Messenger@Net - Info - Release 2.0.0

Install PC	
PC	General - Install PC
	General - Install PC - Adobe Acrobat Reader
	General - Install PC - Apache and PHP
	General - Install PC - Dialogic
	General - Install PC - DMS-API service
	General - Install PC - National-Instruments
	General - Install PC - ODBC
	General - Install PC - SMTP service
	General - Install PC - SOPHO Messenger@Net
	General - Install PC - WinZip
Tables	
eASYNC	eASYNC
eBACKUP	eBACKUP
eCAP	eCAP_generic
eCSTA	eCSTA
	eCSTA_INBOUND_EVENT
	eCSTA_INBOUND_RESULT
eDMSAPI	eDMSAPI
eIO	eIO_AI
	eIO_DI
	eIO_DO
	eIO_MODULE
eKERNEL	eKERNEL_ALARM
	eKERNEL_AREA
	eKERNEL_DEVICE

Contact me

The table of contents can contain definitions similar to those shown in Table 65.

Table 65
Contact me

3	7	2	2909	Contact me	mailto:francis.missiaen@1s.be	40
3	7	2	2963	Kontakteer mij	mailto:francis.missiaen@1s.be	40

Such definitions use the syntax mailto:user@domain. You can add more internal contacts, for instance the names and e-mail address of the ICT department, and the system administrator.

Sign off

The sign-off link logs you out of the system. You must always sign off if you leave your browser unattended, to prevent other users from accessing eWEB functions.

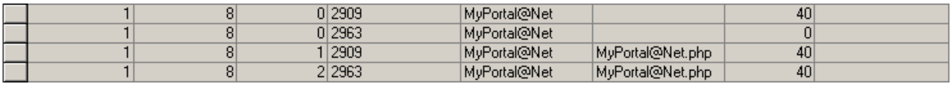
IMPORTANT!

Due to the users' ability to activate disaster scenarios, evacuation scenarios, and others, you must clearly inform all users of the risk they run by leaving their browser unattended. In many situations, users who leave their browser unattended can be held personally responsible for actions that are taken with their authenticated session.

Plug-in Support

The DECT Messenger eWEB module allows embedding plug-in modules that add additional functionality to the web interface. The plug-in modules can be integrated easily through the standard eWEB_TOC table. This is illustrated in Figure 595 on page 1299, where additional table-of-contents entries are added for the plug-in MyPortal@Net.

Figure 595
Plug-ins added to eWEB

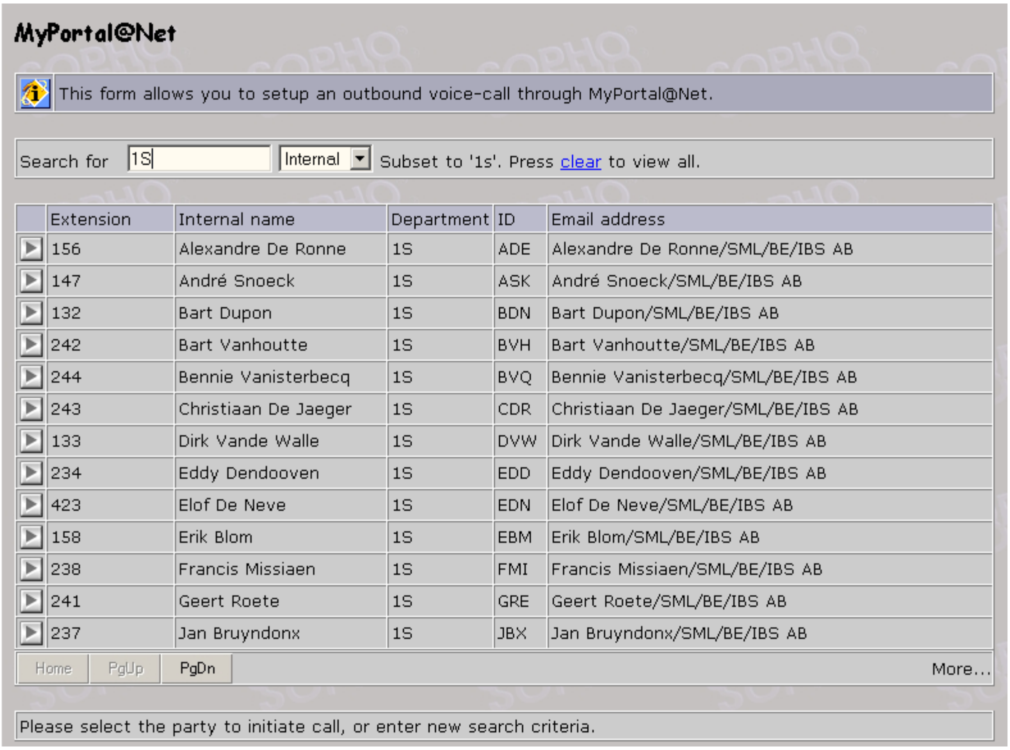


	1	8	0	2909	MyPortal@Net		40	
	1	8	0	2963	MyPortal@Net		0	
	1	8	1	2909	MyPortal@Net	MyPortal@Net.php	40	
	1	8	2	2963	MyPortal@Net	MyPortal@Net.php	40	

Plug-in module MyPortal@Net

An example of a plug-in module is MyPortal@Net. The interface is shown in Figure 596 on page 1300. This module is *not* part of the base product, and is sold separately. The application provides a web interface for outbound voice-calls integrated in the eWEB module. This allows data retrieval from any data repository, including Sigma PhoneWare BTS_DIR directory. Other databases can be accessed as well through OLE/DB, ADO or sockets.

Figure 596
MyPortal@Net plug-in



MyPortal@Net

This form allows you to setup an outbound voice-call through MyPortal@Net.

Search for 1S Internal Subset to '1s'. Press clear to view all.

	Extension	Internal name	Department	ID	Email address
▶	156	Alexandre De Ronne	1S	ADE	Alexandre De Ronne/SML/BE/IBS AB
▶	147	André Snoeck	1S	ASK	André Snoeck/SML/BE/IBS AB
▶	132	Bart Dupon	1S	BDN	Bart Dupon/SML/BE/IBS AB
▶	242	Bart Vanhoutte	1S	BVH	Bart Vanhoutte/SML/BE/IBS AB
▶	244	Bennie Vanisterbecq	1S	BVQ	Bennie Vanisterbecq/SML/BE/IBS AB
▶	243	Christiaan De Jaeger	1S	CDR	Christiaan De Jaeger/SML/BE/IBS AB
▶	133	Dirk Vande Walle	1S	DVW	Dirk Vande Walle/SML/BE/IBS AB
▶	234	Eddy Dendooven	1S	EDD	Eddy Dendooven/SML/BE/IBS AB
▶	423	Elof De Neve	1S	EDN	Elof De Neve/SML/BE/IBS AB
▶	158	Erik Blom	1S	EBM	Erik Blom/SML/BE/IBS AB
▶	238	Francis Missiaen	1S	FMI	Francis Missiaen/SML/BE/IBS AB
▶	241	Geert Roete	1S	GRE	Geert Roete/SML/BE/IBS AB
▶	237	Jan Bruyndonx	1S	JBX	Jan Bruyndonx/SML/BE/IBS AB

Please select the party to initiate call, or enter new search criteria.

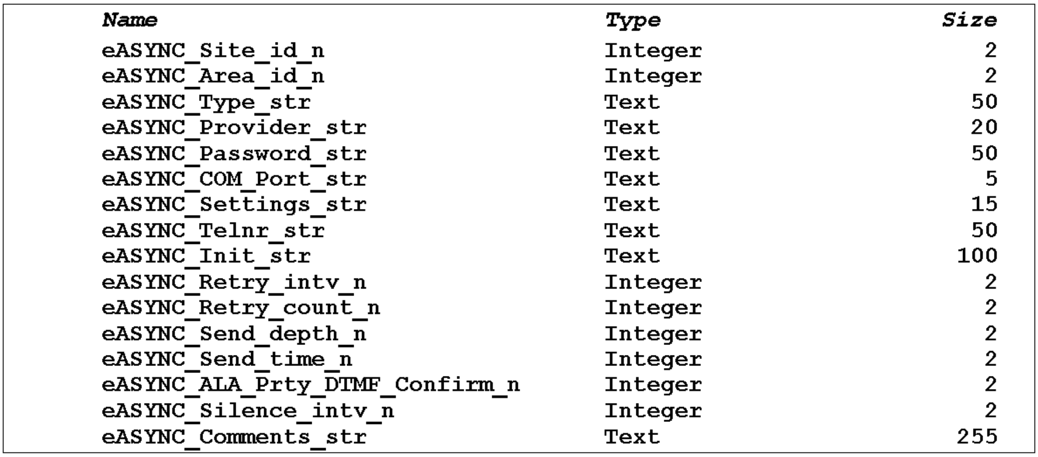
The module uses native CSTA.DLL interfacing to handle voice-calls.

More information can be obtained through the following contact:

IBS Technology & Services
Francis Missiaen
X. De Cocklaan 70
B-9830 Sint-Martens-Latem
Tel. ++32 9 280 22 38
Fax. ++32 9 280 22 49
Email:: francis.missiaen@1s.be
www: http://www.ibsts.be

Table: eASYNC

Figure 597
eASYNC parameters



Name	*Type*	*Size*
eASYNC_Site_id_n	Integer	2
eASYNC_Area_id_n	Integer	2
eASYNC_Type_str	Text	50
eASYNC_Provider_str	Text	20
eASYNC_Password_str	Text	50
eASYNC_COM_Port_str	Text	5
eASYNC_Settings_str	Text	15
eASYNC_Telnr_str	Text	50
eASYNC_Init_str	Text	100
eASYNC_Retry_intv_n	Integer	2
eASYNC_Retry_count_n	Integer	2
eASYNC_Send_depth_n	Integer	2
eASYNC_Send_time_n	Integer	2
eASYNC_ALA_Prty_DTMF_Confirm_n	Integer	2
eASYNC_Silence_intv_n	Integer	2
eASYNC_Comments_str	Text	255

eASYNC_Site_id_n

This field specifies the site, as defined in eKERNEL_SITE table. In most cases the value is 1.

An example of an entry typically found in this field is as follows: 1

eAsync_Area_id_n

This field specifies the area, as defined in eKERNEL_AREA table. In most cases the value is 1.

An example of an entry typically found in this field is as follows: 1

eASYNC_Type_str

This field specifies the provider type, which can be either PAGING or SMS. Currently there is support for PAGING with provider BELGACOM, and SMS with provider PROXIMUS or KPN. Support for other providers and types can be added in future releases, or can be built on request.

For example:

- PAGING (requires the field eASYNC_Provider_str to equal BELGACOM)
- SMS (requires the field eASYNC_Provider_str to equal PROXIMUS)
- SMS (requires the field eASYNC_Provider_str to equal KPN)

eASYNC_Provider_str

This field specifies the provider, which is related to the type specified in the eASYNC_Type_str field, which can be either PAGING or SMS. Currently there is support for PAGING with provider BELGACOM and SMS with provider PROXIMUS and KPN. Support for other providers and types can be added in future releases, or can be built on request.

For example:

- BELGACOM (required when eASYNC_Type_str is PAGING)
- PROXIMUS or KPN (required when eASYNC_Type_str is SMS)

eASYNC_Password_str

This field specifies the password to access the service provider. This field is only relevant when eASYNC_Type_str is SMS.

For the provider PROXIMUS, you must enter a password (proximus) in the initialisation string. In this field, you can enter the password.

For KPN, no password is required (eASYNC_Password_str = *NONE).

The default value is *NONE, and means that no password is required.

Note: Password is case-sensitive.

Example of initialisation string for provider PROXIMUS, password proximus:

01/00121/O/01/32475353215//proximus/3/
534D5320746F2050726F78696D

7573207769746820534F50484F204D657373656E676572404E6574/A3

Example of initialisation string for provider KPN:

01/00084/O/01/0620032328///3/
456D657267656E637920534F5320312045766163756174696F6E/E2

An example of an entry typically found in this field is as follows: *NONE

eASYNC_COM_Port_str

This field specifies the COM port that handles the asynchronous communication. Usually an asynchronous modem is attached to port COM02. In this case, specify COM02.

IMPORTANT!

Verify that the resource is available, and that the modem is attached to the correct resource. There are environments where many COM ports are available, which can lead to confusion during configuration. As well, resources such as National Instruments or Watchdog adapters, can also occupy a COM port.

For example: COM02

eASYNC_Settings_str

This value specifies a valid setting string, defining baud rate, parity, data bits and stop bits. Valid values are modem- and provider-specific.

IMPORTANT!

The eASYNC module performs some handshaking during the initialisation phase. The eASYNC module expects an OK response to these initialisation steps. Some modems do not reply with OK in these steps, when the initial baud rate is set to a different value than 9600,N,8,1.

Therefore, Nortel recommends that you specify 9600,N,8,1 for PAGING/ BELGACOM, SMS/PROXIMUS and SMS/KPN, and not to specify the 14400,N,8,1 value that BELGACOM suggests for their paging application. The baud rate is negotiated during the CONNECT phase, so that is when the modems synchronize.

An example of an entry typically found in this field is as follows: 9600,N,8,1

eASYNC_Telnr_str

This field specifies the dial-in number of the service provider (currently limited to PROXIMUS, KPN, and BELGACOM). Contact your service provider to get the correct number, and enter the number in this field. Check whether leading 0 or other PSTN access digits are required in your environment.

Table 66
eASYNC_Telnr_str

Type	Provider	Password	Settings	Telnr
PAGING	BELGACOM	*NONE	9600,N,8,1	00452500001
SMS	KPN	*NONE	9600,N,8,1	00653141414
SMS	PROXIMUS	proximus	9600,N,8,1	00475161622

Note: Nortel recommends that you specify 9600,N,8,1 for PAGING/ BELGACOM service provider.

An example of an entry typically found in this field is as follows: 00475161622

eASYNC_Init_str

This field allows you to specify a modem initialisation string command. This is useful in situations where a clean start is required. Refer to the instructions of your modem for valid AT-commands that must be specified in your environment. An OK reply is expected on this initialisation string, which can require a specific baud rate with some modems.

You can start with the setting AT&C0S0=3. Refer to your modem manual for more information on AT-commands that are supported for your specific modem type.

An example of an entry typically found in this field is as follows: AT&C0S0=3

eASYNC_Retry_intv_n

This value specifies, in combination with eASYNC_retry_count_n, the interval in seconds between retries if a failure occurs in message delivery. Time can be lost while waiting for recovery (for example, 3 x 1 minutes = 3 minutes lost time). The value is processed in eKERNEL.

An example of an entry typically found in this field is as follows: 60

eASYNC_Retry_count_n

This value specifies, in combination with eASYNC_retry_intv_n, the number of times recovery is performed if a message cannot be delivered to the provider. Note that valuable time can be spent while waiting for recovery (for example, 3 times 1 minutes leads to 3 minutes lost time). The value is processed in eKERNEL.

An example of an entry typically found in this field is as follows: 1

eASYNC_Send_depth_n

This value specifies – in combination with eASYNC_Send_time_n – when eASYNC starts processing. A value of 1 denotes immediate processing; a larger value specifies the number of messages that must be in the queue before processing starts. This value is supported only for PROXIMUS – SMS and KPN – SMS. This is the only provider that allows the delivery of more than one message in a single dial-out request, thus potentially reducing communication costs at the expense of speed. Nortel recommends a value of 1 for most environments, because processing is usually executed as soon as possible, and any related call setup costs are therefore less important.

An example of an entry typically found in this field is as follows: 1

eASYNC_Send_time_n

This value specifies (in seconds and in combination with eASYNC_Send_Depth_n) the moment when actual message delivery is triggered in eASYNC module. When 1 is specified, immediate processing is triggered when a message request is received from eKERNEL. A larger value causes the system to wait until the specified number of messages is queued before processing begins. Note that processing starts due to either Send Depth or Send time, whichever occurs first. Time can be lost if values larger than 1 are specified.

An example of an entry typically found in this field is as follows: 1

eASYNC_ALA_Prty_DTMF_Confirm_n

This field specifies the priority of the alarm, as defined in ALARM table. Alarms distributed to eASYNC with priority higher than the defined value are automatically considered acknowledged, when the provider receives the message. This is usually acceptable; however, eASYNC typically delivers messages to devices (such as Pagers, GSM, and so on) that cannot respond with a confirmation. In some circumstances, the message must be active until a manual confirmation takes place. This can be performed through eASYNC (dial-in and confirm using CLID).

If the priority of the alarm is lower than or equal to the eASYNC_ALA_Prty_DTMF_Confirm_n priority, the message reply (<msgrpy>) sent by the eASYNC module to the eKERNEL is treated as a NACK reply (even if an ACK was sent).

As a result, when alarms that require confirmation are sent using eASYNC and successfully delivered (status = ACK), they continue to behave as if the status is NACK. The alarm is repeated every eASYNC_Silence_intv_n seconds until confirmation is received. If the alarm is not confirmed within DEV_Retry_count_ALT_DEV_id_n (eKERNEL_device) retries, it is sent to the alternative devices (if configured).

An example of an entry typically found in this field is as follows: 2

eASYNC_Silence_intv_n

This value specifies how frequently users are informed of remaining active messages. The default value is 600 seconds, which reduces unnecessary calling traffic to the provider.

Note that a similar value is implemented in eKERNEL_ALARM table. The value here overrides the value in the eKERNEL_ALARM table due to bandwidth constraints.

An example of an entry typically found in this field is as follows: 600 (seconds)

eASYNC_Comments_str

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

Table: eBACKUP

Table 67
eBACKUP parameters

Name	*Type*	*Size*
BU_Site_id_n	Integer	2
BU_From_Path_str	Text	255
BU_From_File_str	Text	255
BU_To_Path_str	Text	255
BU_To_File_str	Text	255
BU_Comments_str	Text	255

BU_Site_id_n

This field specifies the site identifier, as defined in the eKERNEL_SITE table. Usually, there is only one site defined, and the value 1 is used.

An example of an entry typically found in this field is as follows: 1

BU_From_Path_str

This field specifies the path of the file that must be saved.

An example of an entry typically found in this field is as follows: C:\SOPHO Messenger@Net\Mdb

BU_From_File_str

This field specifies the filename of the file that must be saved.

An example of an entry typically found in this field is as follows: Messenger_CFG.mdb

BU_To_Path_str

This field specifies the target path in which to store the copied file. This path must be different from the source path. The target location must also be available when the eBACKUP runs.

You do not need to manually build the directory tree structure, as the nested directory path is built automatically step-by-step during the backup procedure.

In most cases, Nortel recommends that you not overwrite a previous backup. System administrators typically want to make a copy of the environment both before and after making maintenance updates, and in some cases want to store a history online.

To establish flexibility in the backup approach, a number of special values are supported in the eCAB module. These special values are valid only in the BU_To_Path_str field

- The special value [timestamp] is used at the beginning of the backup to calculate the current time stamp, formatted in a 14-character string containing both date and time indication (YYYYMMDDHHNNSS). The path is dynamically recalculated, and provides a new unique directory path:
  - — C:\Temp\[timestamp]\SOPHO Messenger@Net\Mdb becomes C:\Temp\20011009190312\SOPHO Messenger@Net\Mdb
- The special value [weekday] is used at the beginning of the backup to calculate the current time stamp, formatted in a one-character string containing the day of week indication (1=Monday, 2=Tuesday, 3=Wednesday, and so on. The path is dynamically recalculated, and provides a new unique directory path:
  - — C:\Temp\[weekday]\SOPHO Messenger@Net\Mdb becomes C:\Temp\3\SOPHO Messenger@Net\Mdb

- The special value [weekdayname] is used at the beginning of the backup to calculate the current time stamp, formatted in a character string containing the name of the day of week (Monday, Tuesday, Wednesday, and so on). The path is dynamically recalculated, and provides a new unique directory path. The day of week is in the language identified in the regional settings of the Windows environment:
  - — C:\Temp\[weekdayname]\SOPHO Messenger@Net\Mdb becomes C:\Temp\Wednesday\SOPHO Messenger@Net\Mdb

An example of an entry typically found in this field is as follows: C:\Temp\[weekday]\SOPHO Messenger@Net\Mdb

BU_To_File_str

This field specifies the file name of the destination file, which is, in most cases, the same as the source file. Therefore, Nortel recommends that you specify the same value as in BY_From_File field.

An example of an entry typically found in this field is as follows: Messenger_CFG.mdb

BU_Comments_str

This field can be filled with reminder information for an administrator, for example the usage of the file. You can leave the field blank.

An example of an entry typically found in this field is as follows: Configuration Database

Sample Data

Table 68
Sample data

Site	From path	From file	To path	To file
3	C:\Php	php.ini	C:\Temp\[weekday]\php	php.ini

Table 68
Sample data

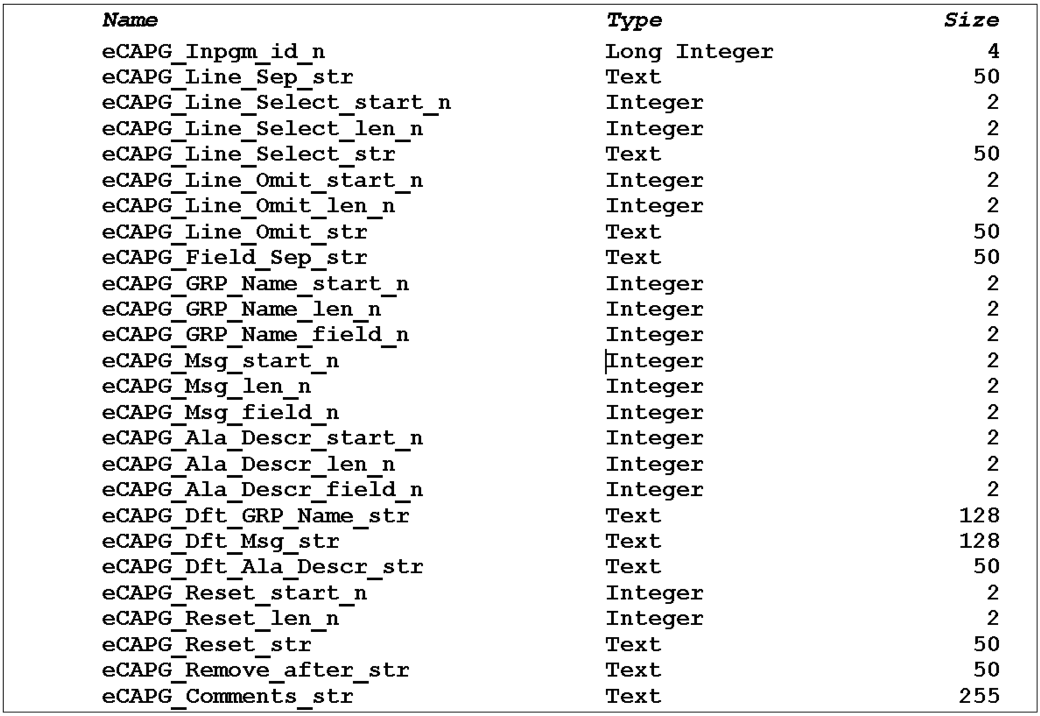
3	C:\Program Files\Apache group\Apache\conf	httpd.conf	C:\Temp\[weekday]\Program Files\Apache Group\Apache\conf	httpd.conf
3	C:\SOPHO Messenger@Net\Exe	eAPI.exe	C:\Temp\[weekday]\SOPHO Messenger@Net\Exe	eAPI.exe
3	C:\SOPHO Messenger@Net\Exe	CSTA_service.exe	C:\Temp\[weekday]\SOPHO Messenger@Net\Exe	CSTA_service.exe
3	C:\SOPHO Messenger@Net\Exe	eASYNC.exe	C:\Temp\[weekday]\SOPHO Messenger@Net\Exe	eASYNC.exe
3	C:\SOPHO Messenger@Net\Exe	eBACKUP.exe	C:\Temp\[weekday]\SOPHO Messenger@Net\Exe	eBACKUP.exe
3	C:\SOPHO Messenger@Net\Exe	eCAP.exe	C:\Temp\[weekday]\SOPHO Messenger@Net\Exe	eCAP.exe
3	C:\SOPHO Messenger@Net\Exe	eDMSAPI.exe	C:\Temp\[weekday]\SOPHO Messenger@Net\Exe	eDMSAPI.exe
3	C:\SOPHO Messenger@Net\Exe	eGRID.exe	C:\Temp\[weekday]\SOPHO Messenger@Net\Exe	eGRID.exe
3	C:\SOPHO Messenger@Net\Exe	eIO.exe	C:\Temp\[weekday]\SOPHO Messenger@Net\Exe	eIO.exe
3	C:\SOPHO Messenger@Net\Exe	eKERNEL.exe	C:\Temp\[weekday]\SOPHO Messenger@Net\Exe	eKERNEL.exe
3	C:\SOPHO Messenger@Net\Exe	eSMTP.exe	C:\Temp\[weekday]\SOPHO Messenger@Net\Exe	eSMTP.exe
3	C:\SOPHO Messenger@Net\Exe	eSMTP_server.exe	C:\Temp\[weekday]\SOPHO Messenger@Net\Exe	eSMTP_server.exe
3	C:\SOPHO Messenger@Net\Exe	omnithread_rt.dll	C:\Temp\[weekday]\SOPHO Messenger@Net\Exe	omnithread_rt.dll

Table 68
Sample data

3	C:\SOPHO Messenger@Net\Mdb	Messenger_CFG.mdb	C:\Temp\[weekday]\SOPHO Messenger@Net\Mdb	Messenger_CFG.mdb
3	C:\SOPHO Messenger@Net\Mdb	Messenger_Data.mdb	C:\Temp\[weekday]\SOPHO Messenger@Net\Mdb	Messenger_Data.mdb

Table: eCAP_generic

Table 69
eCAP_generic



Name	*Type*	*Size*
eCAPG_Inpgm_id_n	Long Integer	4
eCAPG_Line_Sep_str	Text	50
eCAPG_Line_Select_start_n	Integer	2
eCAPG_Line_Select_len_n	Integer	2
eCAPG_Line_Select_str	Text	50
eCAPG_Line_Omit_start_n	Integer	2
eCAPG_Line_Omit_len_n	Integer	2
eCAPG_Line_Omit_str	Text	50
eCAPG_Field_Sep_str	Text	50
eCAPG_GRP_Name_start_n	Integer	2
eCAPG_GRP_Name_len_n	Integer	2
eCAPG_GRP_Name_field_n	Integer	2
eCAPG_Msg_start_n	Integer	2
eCAPG_Msg_len_n	Integer	2
eCAPG_Msg_field_n	Integer	2
eCAPG_Ala_Descr_start_n	Integer	2
eCAPG_Ala_Descr_len_n	Integer	2
eCAPG_Ala_Descr_field_n	Integer	2
eCAPG_Dft_GRP_Name_str	Text	128
eCAPG_Dft_Msg_str	Text	128
eCAPG_Dft_Ala_Descr_str	Text	50
eCAPG_Reset_start_n	Integer	2
eCAPG_Reset_len_n	Integer	2
eCAPG_Reset_str	Text	50
eCAPG_Remove_after_str	Text	50
eCAPG_Comments_str	Text	255

eCAPG_Inpgm_id_n

This field refers to the input program identifier, as defined in eKERNEL_INPGM table.

An example of an entry typically found in this field is as follows: 11101

eCAPG_Line_Sep_str

This field specifies the character sequence that is used to separate input lines that are processed through the generic eCAP interface. This value must be formatted using one or more 2-byte hexadecimal ASCII values. For example, the carriage return (with ASCII 13 value) is represented by 0D, because 0D is the hexadecimal value of decimal 13. Usually, this field specifies the value 0D0A, which places one carriage return, and one line feed between individual lines. Note that the indicated value must be 2-bytes or a multiple of 2-bytes; therefore the leading 0 or trailing 0 must not be omitted.

Although the separator us used to isolate logical blocks, a number of hard-coded routines are active within eCAP module. 0A0D and 0C0D blocks are always ignored.

An example of an entry typically found in this field is as follows: 0D0A

eCAPG_Line_Select_start_n

This value, together with eCAPG_Line_Select_len_n and eCAPG_Line_Select_str, is used to optionally define selection criteria, which are used to select only those records in a asynchronous datastream that are defined.

The value 0 denotes the select capabilities are not in use. As a result, the corresponding values are ignored, and all records are processed. In this case, the field eCAP_Line_Select_len_n must be 0, and the field eCAP_Line_Select_str must be N/A.

A value larger than 0 indicates select capabilities are used. The value refers to the start position of the select pattern. In this case, the field eCAP_Line_Select_len_n must be larger than 0, and the field eCAP_Line_Select_str must contain the select character or characters.

An example of an entry typically found in this field is as follows: 5

eCAPG_Line_Select_len_n

This value, together with eCAPG_Line_Select_start_n and eCAPG_Line_Select_str, are used to optionally define selection criteria, which are used to select only those records in an asynchronous datastream that are defined.

This value must be 0 if no select functionality is in use, which is specified through eCAPG_Line_Select_start_n equal to 0.

A value larger than 0 denotes select criteria are active, and the field defines the character length of the selection characters defined in eCAPG_Line_Select_str.

An example of an entry typically found in this field is as follows: 1

eCAPG_Line_Select_str

This value, together with eCAPG_Line_Select_start_n and eCAPG_Line_Select_len_n, is used to optionally define selection criteria, which are used to select only those records in a asynchronous datastream that are defined.

This value N/A must be used if the select functionality is not used, indicated by eCAPG_Line_Select_start_n and eCAPG_Line_Select_len_n equal to 0.

The field contains the characters that are used in the select pattern test, which must be a string with length equal to the length defined in eCAPG_Line_Select_len_n.

An example of an entry typically found in this field is as follows: colon (:)

eCAPG_Line_Omit_start_n

This value, together with eCAPG_Line_Omit_len_n and eCAPG_Line_Omit_str, are used to optionally define omit criteria, which are used to omit specific records in a asynchronous datastream.

The value 0 denotes the omit capabilities are not in use. As a result, the corresponding values are ignored, and no records are omitted. In this case, the field eCAP_Line_Omit_len_n must be 0 and the field eCAPG_Line_Omit_str must be N/A.

A value larger than 0 indicates select capabilities are used. The value refers to the start position of the select pattern. In this case, the field eCAP_Line_Select_len_n must be larger than 0 and the field eCAP_Line_Select_str must contain the select character or characters.

An example of an entry typically found in this field is as follows: 12

eCAPG_Line_Omit_len_n

This value, together with eCAPG_Line_Omit_start_n and eCAPG_Line_Omit_str, is used to optionally define omit criteria, which are used to omit specific records in a asynchronous datastream.

This value must be 0 if no omit functionality is in use, which is specified through eCAPG_Line_Omit_start_n equal to 0.

A value larger than 0 denotes omit criteria are active, and the field defines the character length of the omit characters defined in eCAPG_Line_Omit_str.

An example of an entry typically found in this field is as follows: 1

eCAPG_Line_Omit_str

This value, together with eCAPG_Line_Omit_start_n and eCAPG_Line_Omit_len_n, is used to optionally define omit criteria, which are used to omit specific records in a asynchronous datastream.

This value N/A must be used if the omit functionality is not used, indicated by eCAPG_Line_Omit_start_n and eCAPG_Line_Omit_len_n equal to 0.

This field specifies the characters that are used in the omit pattern test, which must be a string with length equal to the length defined in eCAPG_Line_Omit_len_n.

An example of an entry typically found in this field is as follows: /

eCAPG_Field_Sep_str

This field can optionally define field separators. Field separators can be used when no fixed format of datastreams is available, and individual fields are to be retrieved from a variable-length datastream.

In most cases, this field is not used, and the special value **N/A** is specified. The generic eCAP module is targeted to handle only datastreams that use a fixed format layout (for example, printer ports typically produce such formatted data).

When a different value is specified, the characters specified are used as a field delimiter. For example, the value / can be used to define a datastream 001/02/ABC. The field separator can later be used to identify field numbers. In this example, field number 1 is 001, field number 2 is 02, and field number 3 is ABC.

Note that support for such field-separated datastreams is somewhat limited in current release, and does not support offsets. For example, <001/02/ABC> with field separators / fails to handle the < and > characters, and generates field 1 as <001, field 2 as 02 and field 3 as ABC>.

An example of an entry typically found in this field is as follows: /

eCAPG_GRP_Name_start_n

This value, together with eCAPG_GRP_Name_len_n and eCAPG_GRP_Name_field_n, defines the criteria to isolate the group name parameter in the datastream.

This field refers to the definitions of eKERNEL_GROUP table.

The value 0 denotes this field is not available in the datastream. The remaining values in field eCAPG_GRP_Name_str must be set to 0 and eCAPG_GRP_NAME_Field_n to 0. In this case, the field eCAPG_Dft_GRP_Name_str must be used to define a default group.

A group indication can be defined based either upon string position (through eCAPG_GRP_Name_start_n and eCAPG_GRP_Name_len_n) or based upon field occurrence (through eCAPG_GRP_Name_field_n).

A positive value in eCAPG_GRP_Name_start_n indicates a positional definition is available, and denotes the start position of the group name.

An example of an entry typically found in this field is as follows: 1

eCAPG_GRP_Name_len_n

This field specifies the length of the group name description.

If the field eCAPG_GRP_Name_start_n equals 0, the eCAPG_GRP_Name_len_n must be 0 as well.

If the field eCAPG_GRP_Name_start_n is not set to 0, the eCAPG_GRP_Name_len_n must be non-0 as well, and define the length of the group name.

An example of an entry typically found in this field is as follows: 4

eCAPG_GRP_Name_field_n

This field specifies the occurrence number of the field that denotes group name, and only applies when a field separator is defined. In this case, no positional definition is active.

The field must be 0 when no such definition is active.

A positive value indicates the field number. For example, when the field separator is / and the datastream is 001/02/ABC, the value of 1 returns 001 as group name, a value 2 would return 02 as group name, and 3 would return ABC as group name.

An example of an entry typically found in this field is as follows: 0

eCAPG_Msg_start_n

This value, together with eCAPG_Msg_len_n and eCAPG_Msg_field_n, refers to the message contents in the datastream.

This field refers to the definitions of eKERNEL_ALARM table, and must be appropriately configured (for example, message length).

As explained for the group name, the field can be either defined on position (through eCAPG_Msg_start_n and eCAPG_Msg_len_n) or occurrence (through eCAPG_Msg_field_n).

The value 0 denotes this field is not available in the datastream. The remaining values in field eCAPG_Msg_len_n must be set to 0 and eCAPG_Msg_field_n to 0. In this case, the field eCAPG_Dft_Msg_str must be used to define a default message.

A message indication can be defined based either upon string position (through eCAPG_Msg_start_n and eCAPG_Msg_len_n) or based upon field occurrence (through eCAPG_Msg_field_n).

A positive value in eCAPG_Msg_start_n indicates a positional definition is available, and denotes the start position of the message.

An example of an entry typically found in this field is as follows: 6

eCAPG_Msg_len_n

This field specifies the length of the message.

If the field eCAPG_Msg_start_n equals 0, the eCAPG_Msg_len_n must be 0. If the field eCAPG_Msg_start_n is non-0, the eCAPG_Msg_len_n must be non-0, and define the length of the message.

Note the length specified in eKERNEL_ALARM table.

An example of an entry typically found in this field is as follows: 16

eCAPG_Msg_field_n

This field specifies the occurrence number of the field that denotes message, and only applies when a field separator is defined. In this case, no positional definition is active.

The field must be 0 when no such definition is active.

A positive value indicates the field number. For example, when the field separator is / and the datastream is 001/02/ABC, the value of 1 returns 001 as message, a value 2 would return 02 as message, and 3 would return ABC as message.

An example of an entry typically found in this field is as follows: 0

eCAPG_Ala_Descr_start_n

This value specifies, together with eCAPG_Ala_Descr_len_n and eCAPG_Ala_Descr_field_n, the alarm description contents in the datastream.

The alarm description refers to the definitions in the eKERNEL_ALARM table.

The value 0 denotes this field is not available in the datastream. The remaining values in field eCAPG_Ala_Descr_str must be set to 0 and eCAPG_Ala_Descr_Field_n to 0. In this case, the field eCAPG_Dft_Ala__Descr_str must be used to define a default alarm description.

An alarm description indication can be defined based either upon string position (through eCAPG_Ala_Descr_start_n and eCAPG_Ala_Descr_len_n) or based upon field occurrence (through eCAPG_Ala_Descr_field_n).

A positive value in eCAPG_Ala_Descr_start_n indicates a positional definition is available, and denotes the start position of the alarm description.

An example of an entry typically found in this field is as follows: 20

eCAPG_Ala_Descr_len_n

This field specifies the length of the alarm description.

If the field eCAPG_Ala_Descr_start_n equals 0, the eCAPG_Ala_Descr_len_n must be 0 as well.

If the field eCAPG_Ala_Descr_start_n is non-0, the eCAPG_Ala_Descr_len_n must be non-0 as well.

An example of an entry typically found in this field is as follows: 1

eCAPG_Ala_Descr_field_n

This field specifies the occurrence number of the field that denotes alarm description, and only applies when a field separator is defined. In this case, no positional definition is active.

The field must be 0 when no such definition is active.

A positive value indicates the field number. For example, when the field separator is / and the datastream is 001/02/ABC, the value of 1 returns 001 as alarm description, a value 2 would return 02 as alarm description and 3 would return ABC as alarm description.

An example of an entry typically found in this field is as follows: 0

eCAPG_Dft_GRP_Name_str

This field is used to provide a default group name, in the event that no value can be retrieved from the available datastream. In this case, the same value is used for all alarms generated through this eCAP generic interface instance.

The value N/A must be specified if this field is not used.

An example of an entry typically found in this field is as follows: N/A

eCAPG_Dft_Msg_str

This field is used to provide a default message, in the event that no value can be retrieved from the available datastream. In this case, the same value is used for all alarms generated through this eCAP generic interface instance.

The value N/A must be specified if this field is not used.

An example of an entry typically found in this field is as follows: N/A

eCAPG_Dft_Ala_Descr_str

This field is used to provide a default alarm description, in the event that no value can be retrieved from the available datastream. In this case, the same value is used for all alarms generated through this eCAP generic interface instance.

The value N/A must be specified if this field is not used.

An example of an entry typically found in this field is as follows: N/A

eCAPG_Reset_start_n

This value, together with eCAPG_Reset_len_n and eCAPG_Reset_str, refers to the optional reset functionality that can be deployed in the eCAP generic module.

In most cases, a eCAP generic is implemented in environments, where alarms are detected through an asynchronous serial interface, such as a printer port.

The eCAP generic is targeted to environments, where each alarm indication results in sending an alarm request to the eKERNEL interface. Due to the nature of such requests, and the scope of the current eCAP implementation, these alarms results in setting an alarm, a so-called <msgrqs>-transaction that contains a *set request. In most cases you define these alarm types in eKERNEL_ALARM table as alarms that are removed after *sent. Therefore, the parameter eCAPG_Remove_after_str is, in most cases, set to *set.

In such environments, the default value 0 must be used for both the fields eCAPG_Reset_start_n and eCAPG_Reset_len_n, and the default value N/A must be used for the parameter eCAPG_Reset_str.

In some environments, all alarms must remain active in eKERNEL, unless a specific reset signal is encountered. This reset indication typically indicates a complete reset of all alarms of this interface (for example, resetting a fire detection infrastructure after some warning alarms).

In this case, the field eCAPG_Reset_start_n must be set to the start position of the reset character pattern.

An example of an entry typically found in this field is as follows: 35

eCAPG_Reset_len_n

This parameter is related to the eCAPG_Reset_start_n parameter. If the reset functionality is not used, both parameters are set to 0.

If an eCAPG_Reset_start_n value is specified (for example, 35), the parameter eCAPG_Reset_len_n and eCAPG_Reset_str are to be defined.

The eCAPG_Reset_len_n indicates the length of the string that must be compared to activate a reset condition. If, for example, the text GENERAL RESET must be encountered in position 35, then eCAP_Reset_len_n must be set to 13 (the length of the string) and eCAP_Reset_str must be set to the text GENERAL RESET

An example of an entry typically found in this field is as follows: 13

eCAPG_Reset_str

This parameter also refers to the optional reset capabilities, and contains the string that must be found in the starting position eCAP_Reset_start_n with length eCAP_Reset_len_n.

In most cases the reset functionality is not used, and the default value **N/A** is defined.

An example of an entry typically found in this field is as follows: GENERAL RESET

eCAPG_Remove_after_str

This parameter accepts the value *SENT or *RESET.

In most cases the eCAP generic interfaces is used to capture alarms from an asynchronous serial line (for example, printer port), and received data contains alarm information. In this situation, messages are transmitted to eKERNEL immediately upon arrival, and these alarms are processed within DECT Messenger.

In most environments, the remote peripherals cannot indicate that all pending alarms are reset, and therefore the eKERNEL handles the alarms. Use this field to configure the eKERNEL_ALARM table handling of alarm requests, and prevent endless-loop conditions. Alarms are typically *set with the option remove after sent. The eCAPG_Remove_after_str must then be set to *SENT.

In some exceptional environments, the attached peripherals are capable of sending a general reset to clear all pending alarms. This is performed through the eCAPG_Reset_start_n, eCAPG_Reset_len_n and eCAPG_Reset_str parameters. In such case, alarms must be set using the remove after *RESET value, indicating all pending alarms remain in the eKERNEL database unless the reset condition is met.

Due to the scope of the eCAP generic implementation, no granular method of resetting individual alarms is currently available, and reset functionality must only be activated when the required prerequisite conditions are met.

An example of an entry typically found in this field is as follows: *RESET

eCAPG_Commentrs_str

Use this field to store comments or remarks pertaining to the configuration record.

An example of an entry typically found in this field is as follows: Serial link to the fire detection system.

Table: eDMSAPI

Table 70
eDMSAPI parameters

Name	*Type*	*Size*
eDMSAPI_Site_id_n	Integer	2
eDMSAPI_Area_id_n	Integer	2
eDMSAPI_Seats_count_n	Integer	2
eDMSAPI_eKernel_Seats_count_n	Integer	2
eDMSAPI_External_Seats_count_n	Integer	2
eDMSAPI_External_Address_str	Text	15
eDMSAPI_External_Port_str	Text	5
eDMSAPI_ALA_Prty_UMSG_n	Integer	2
eDMSAPI_ALA_Prty_EMSG_n	Integer	2
eDMSAPI_api_address_str	Text	15
eDMSAPI_api_port_str	Text	5
eDMSAPI_PBX_address_str	Text	15
eDMSAPI_PBX_port_str	Text	5
eDMSAPI_PBX_type_str	Text	50
eDMSAPI_PBX_license_str	Text	50
eDMSAPI_Guarding_Polling_intv_n	Integer	2
eDMSAPI_Guarding_Retry_intv_n	Integer	2
eDMSAPI_Msg_dly_n	Integer	2
eDMSAPI_GeneralTimeOut_n	Integer	2
eDMSAPI_Ack2TimeOut_n	Integer	2
eDMSAPI_DataPathDelay_n	Integer	2
eDMSAPI_QD_eCSTA_Area_n	Integer	2
eDMSAPI_Comments_str	Text	255

eDMSAPI_site_id_n

This field specifies the site identifier, as defined in eKERNEL_SITE table. This value is set to 1 in most environments.

An example of an entry typically found in this field is as follows: 1

eDMSAPI_Area_id_n

This field specifies the area identifier, as defined in eKERNEL_AREA table. This value is set to 1 in most environments.

An example of an entry typically found in this field is as follows: 1

eDMSAPI_Seats_count_n

This field specifies the total number of seats available for E2 messaging (aCsOpenStream).

Sending an E2 message to a DECT extension consumes one seat (one seat is allocated between the StartDataPath and the StopDatPath).

For receiving E2 messages (generation of an alarm), DECT extensions that are configured to generate alarms (table eKERNEL_DEVICE field DEV_IoRegister_b) must be IoRegistered.

The number of possible IoRegisters is related to the number of seats available.

If eDMSAPI is configured with a larger value than available, too many simultaneous E2-data requests are initiated simultaneously, which leads to a large number of failed requests.

An example of an entry typically found in this field is as follows: 30

eDMSAPI_eKERNEL_Seats_count_n

This field specifies the number of seats reserved for message requests (<msgrqs>) from eKERNEL.

An example of an entry typically found in this field is as follows: 5

eDMSAPI_External_Seats_count_n

This field specifies the number of seats reserved for applications with direct access to the eDMSAPI. For example, the eWeb module. The number of seats specified in the field is part of the number of seats defined in the eDMSAPI_Seats_count_n field.

An example of an entry typically found in this field is as follows: 2

eDMSAPI_External_Address_str

This field specifies the IP address of the PC where the eDMSAPI module runs.

This value is necessary for external clients such as eWeb, which directly access the eDMAPI module.

When sending a normal message, the following format is used:
SNDNMSG|ID|DNR|Message<cr><lf>

When sending an urgent message, the following format is used:
SNDUMSG|ID|DNR|Message<cr><lf>.

An example of an entry typically found in this field is as follows:
10.110.50.138

eDMSAPI_External_Port_str

This field specifies the port reserved for requests from the External clients.

This port can accept eDMSAPI_External_Seats_count_n simultaneously requests.

The only valid format of the requests are:

SNDNMSG|ID|DNR|message<CR><LF>

SNDUMSG|ID|DNR|message<CR><LF>

An example of an entry typically found in this field is as follows: 2010

eDMSAPI_ALA_Prty_UMSG_n

This field specifies the priority an alarm message must have, to be handled as an urgent message. The priority refers to the alarm priority as defined in the eKERNEL_ALARM table. Alarms that do not meet the requirement of being urgent are treated as normal messages. Refer to the DMS-API related documentation for more information.

If, for example, 2 is specified, alarms with alarm priority of 1 and 2 are handled as urgent messages, whereas alarms with priority of 3, 4, and so on are handled as normal messages. Nortel recommends that you carefully evaluate the consequences of changes to this field, for two reasons:

- Emergency messages impact the DECT C4060 user (different tone, user intervention required for acknowledge).
- Emergency messages impact throughput, because normal message allocates a datapath a few seconds, while urgent messages can allocate more than 30 seconds, depending on the timeout value specified for user confirmation.

An example of an entry typically found in this field is as follows: 2

eDMSAPI_ALA_Prty_EMSG_n

This field specifies the required priority of an alarm message to be handled as an emergency message. Introduced in R3.0, this field refers to the support of C4060 handsets that allow emergency message levels. The priority refers to the alarm priority as defined in the eKERNEL_ALARM table. Alarms that do not meet the requirement of being urgent are treated as urgent or normal message. Refer to the DMS-API related documentation for more information.

For example, if 1 is specified, alarms with alarm priority of 1 are handled as emergency messages, whereas alarms with priority of 2, 3, 4, and so on are handled as urgent or normal messages. Nortel recommends that you carefully evaluate the consequences of changes to this field, for two reasons:

- Emergency messages impact the DECT C4060 user (different tone, user intervention required for acknowledge).
- Emergency messages impact throughput, because normal message allocates a datapath a few seconds, while urgent messages can allocate more than 30 seconds, depending on the timeout value specified for user confirmation.

An example of an entry typically found in this field is as follows: 1

eDMSAPI_api_address_str

This field specifies the IP address of the CSTA Service.exe module. In most cases this is the same value as the local IP address of eKERNEL, and can be obtained with IPCONFIG.exe.

An example of an entry typically found in this field is as follows:
10.110.50.138

eDMSAPI _API_port_str

This field specifies the port to which CSTA Service.exe listens, and (in the current release) must always be set to 59000.

An example of an entry typically found in this field is as follows: 59000

eDMSAPI _PBX_address_str

This field specifies the IP address of the PBX. The information is distributed to CSTA Service.exe, which handles the sockets connection between DECT Messenger and the PBX. Contact the switch administrator to obtain the IP address of the switch. If a different addressing scheme or subnet mask is in use, appropriate TCP/IP network configuration must be performed on both platforms (default gateway, additional interface, and so on).

An example of an entry typically found in this field is as follows:
10.110.49.171

eDMSAPI_PBX_port_str

This field specifies the port to which the PBX listens, and depends on the PBX type. In previous releases, the recommended value was 2555, which is the default port to which a SOPHO DMC listens. Starting from R3.0, there is also support for DAP controller and Nortel. The recommended default value for DMC is still 2555, and the recommended default value for DAP controller and Nortel is 28001; however, depending on the configuration settings, other values (for example, 2001) are appropriate.

An example of an entry typically found in this field is as follows: 2555

eDMSAPI_PBX_type_str

This field specifies the PBX type used to handle the DMSAPI functionality. The value is introduced in R3.0. Supported values are DMC, DAP, and Nortel. Note that the eDMSAPI_PBX_port_str must also be set according to the recommendations of the PBX type.

An example of an entry typically found in this field is as follows: DMC

eDMSAPI_PBX_licence_str

This keyword specifies the Licence that is used to connect to the PBS. For DECT Messenger, the licence = Messenger (Licence number = 61) is used.

Note that you can also use the external licence (external licence number).

An example of an entry typically found in this field is as follows: Messenger

eDMSAPI_Guarding_Polling_intv_n

This field specifies the polling interval for testing the iSLink in seconds.

The PBX sends a System Status request, with a frequency equal to eDMSAPI_Guarding_Polling_intv_n seconds.

The guarding process in the eDMSAPI module, which continuously checks the iSLink connection, automatically re-establishes the connection when the eDMSAPI_Guarding_Polling_intv_n + eDMSAPI_Guarding_Retry_intv_n Time is the value in this field.

An example of an entry typically found in this field is as follows: 60

eDMSAPI_Guarding_Retry_intv_n

This field specifies the time to wait in seconds, before retrying to establish an iSLink after a failed link setup is detected.

An example of an entry typically found in this field is as follows: 20

eDMSAPI_Msg_dly_n

This field specifies the delay in seconds between sending the individual requests: send normal message and send urgent message.

An example of an entry typically found in this field is as follows: 3

eDMSAPI_GeneralTimeOut_n

This field specifies the Time, in seconds, the eDMSAPI program waits for an event from the CSTA service. This value is by default 10 seconds, and must be greater than 5.

When no event is received within this time, a negative acknowledge is sent to the eKERNEL application or External clients for outbound calls.

An example of an entry typically found in this field is as follows: 10

eDMSAPI_Ack2TimeOut_n

Time in seconds the eDMSAPI program waits for an ACK message request from the iSPBS, signaling that an URGENT message has been read by the DECT user (outbound calls).

An example of an entry typically found in this field is as follows: 30

eDMSAPI_DataPathDelay_n

This keyword specifies the time in seconds to wait between receiving a StopDataResult event form a device and before sending a new StartDataPathRequest for the same device.

The default value is 2 seconds.

This parameter is implemented because the eDMSAPI module receives Universal failure events (reason = INVALID_CALLING_DEVICE) when sending a StartDataPathRequest directly after receiving a StopDataResult for the same device.

An example of an entry typically found in this field is as follows: 2

eDMSAPI_Comments_str

This field contains remarks from the administrator and is informational only.

Table: eDMSAPI_INBOUND

Table 71
eDMSAPI_inbound parameters

Name	*Type*	*Size*
eDMSAPII_Site_id_n	Integer	2
eDMSAPII_Area_id_n	Integer	2
eDMSAPII_Called_dev_str	Text	6
eDMSAPII_Type_str	Text	5
eDMSAPII_Comments_str	Text	255

eDMSAPII_Site_id_n

This field specifies the site identifier, as defined in eKERNEL_SITE table. In most environments, this value is 1.

An example of an entry typically found in this field is as follows: 1

eDMSAPII_Area_id_n

This field specifies the area identifier, as defined in eKERNEL_AREA table. In most environments, this value is 1.

An example of an entry typically found in this field is as follows: 1

eDMSAPII_Called_dev_str

This field identifies the called device. This is the number of the extension to which the message was sent.

An example of an entry typically found in this field is as follows: 999

eDMSAPII_Type_str

This value can be *IC or *IA.

These values are interpreted by eKERNEL module of DECT Messenger.

*IC When a call is made, the calling line identifier of the calling party (also known as CLID) is used to confirm outstanding messages for those devices in DEVICE table with the DEV_Pincode_str equal to the CLID. This technique is known as incoming confirmation, and is typically used in environments where urgent messages must be confirmed when sent to devices such as SMS, PAGING, and SMTP, without implicit bidirectional confirmation techniques embedded. A callback from a predefined number (for example, GSM, home subscriber, and so on) can be used to call-off and confirm messages.

An incoming confirmation is only valid if the called device is defined in the eDMSAPI_INBOUND table with eDMSAPI_Type_str = *IC. Therefore, the calling device receives a ÷ indication before the message to confirm the called device is valid, and an X for an invalid destination.

*IA When a E2 message is sent by an extension that is IoRegistered (field DEV_IoRegister_b in table eKERNEL_DEVICE is true), an incoming alarm action is triggered, providing eKERNEL with four pieces of information: the calling device, called device, message, and priority.

When the eKERNEL application receives a request, the request is valid when the called device is defined in the eDMSAPI_INBOUND table with Type = *IA, and if the called and calling device is defined in the eDMSAPI_INBOUND_EVENT table. Therefore, valid requests are indicated with a ÷ symbol before the message sent, invalid requests with a X indication.

An example of an entry typically found in this field is as follows: *IA

eDMSAPII_Comments_str

This field can optionally be used by an administrator to store reminder information, describing, for example, usage of the extension.

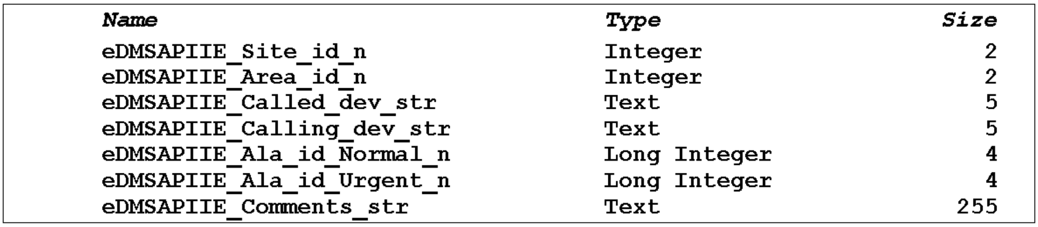
An example of an entry typically found in this field is as follows: “this port is used for outbound user-to-user messaging”.

Table 72
Sample data

eDMSAPII _Site_id_n	eDMSAPII_ Area_id_n	eDMSAPII_ Called_dev_str	eDMSAPII _ Type_str	eDMSAPII_Comments_str
1	1	12345	*IC	TEST Incoming confirmation
1	1	222	*IA	TEST Incoming alarm
1	1	333	*IC	Incoming confirmation
1	1	56789	*IA	TEST
1	1	860	*IA	REA
1	1	861	*IA	User to User message
1	1	865	*IA	User to User message
1	1	888	*IA	NOOD
1	1	999	*IA	REA

Table: eDMSAPI_INBOUND_EVENT

Table 73
eDMSAPI_inbound_event parameters



Name	*Type*	*Size*
eDMSAPIIE_Site_id_n	Integer	2
eDMSAPIIE_Area_id_n	Integer	2
eDMSAPIIE_Called_dev_str	Text	5
eDMSAPIIE_Calling_dev_str	Text	5
eDMSAPIIE_Ala_id_Normal_n	Long Integer	4
eDMSAPIIE_Ala_id_Urgent_n	Long Integer	4
eDMSAPIIE_Comments_str	Text	255

eDMSAPIIE_Site_id_n

This field specifies the site, as defined in eKERNEL_SITE table. Is most environments, the value is 1.

An example of an entry typically found in this field is as follows: 1

eDMSAPIIE_Area_id_n

This field specifies the area, as defined in eKERNEL_AREA table. Is most environments the value is 1.

An example of an entry typically found in this field is as follows: 1

eDMSAPIIE_Called_dev_str

This field specifies the Called device in an incoming call alarm generation situation, handled by eDMSAPI. This field specifies the number to which the message was sent.

An example of an entry typically found in this field is as follows: 999

eDMSAPIIE_Calling_dev_str

This field specifies the Calling device in an incoming call alarm generation situation, handled by eDMSAPI.

The Calling device specified here defines those extensions that can generate an alarm by sending a message to the related called device.

1. Define an extension by number, for example, 866.
2. Define a generic value *ALL.
3. Define a generic number starting with some characters 85*.

An example of an entry typically found in this field is as follows: *ALL

eDMSAPIIE_Ala_id_Normal_n

This field defines (based upon appropriate record selection through CLID detection) the alarm characteristics of the alarm that are initiated as a result of the incoming message process with a priority = Normal.

The alarm identifier must match a definition in eKERNEL_ALARM table, and defines properties such as alarm priority, length, and so on.

The remainder of the action is defined in the eDMSAPI_INBOUND_RESULT table, where a message is defined, and a destination group is assigned, based on calling and called device.

An example of an entry typically found in this field is as follows: 1190101

eDMSAPIIE_Ala_id_Urgent_n

This field defines (based upon appropriate record selection through CLID detection) the alarm characteristics of the alarm that are initiated as a result of the incoming message process with a priority = Urgent.

The alarm identifier must match a definition in eKERNEL_ALARM table, and defines properties such as alarm priority, length, and so on.

The remainder of the action is defined in the eDMSAPI_INBOUND_RESULT table, where a message is defined, and a destination group is assigned, based on calling and called device.

An example of an entry typically found in this field is as follows: 1190102

eDMSAPIIE_Comments_str

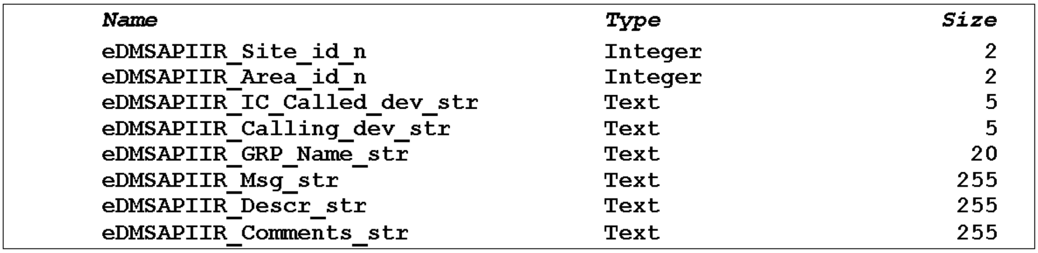
This field can contain remarks from the administrator and is informational only.

Table 74
Sample Data

Site	Area	Called device	Calling device	Alarm ID Normal	Alarm ID Urgent	Comments
1	1	222	8*	1190105	1190106	TEST
1	1	333	*ALL			
1	1	56789	850	1190105	1190106	TEST
1	1	56789	851	1190105	1190106	TEST
1	1	56789	852	1190105	1190106	TEST
1	1	56789	853	1190105	1190106	TEST
1	1	56789	86*	1190105	1190106	TEST
1	1	860	85*	1190104	1190104	REA
1	1	861	*ALL	1190101	1190102	User to User msg allowed for device 861
1	1	865	*ALL	1190101	1190102	User to User msg allowed for device 865
1	1	888	*ALL	1190103	1190103	NOODOPROEP
1	1	999	*ALL	1190104	1190104	REANIMATIE

Table: eDMSAPI_INBOUND_RESULT

Table 75
eDMSAPI _inbound_result parameters



Name	*Type*	*Size*
eDMSAPIIR_Site_id_n	Integer	2
eDMSAPIIR_Area_id_n	Integer	2
eDMSAPIIR_IC_Called_dev_str	Text	5
eDMSAPIIR_Calling_dev_str	Text	5
eDMSAPIIR_GRP_Name_str	Text	20
eDMSAPIIR_Msg_str	Text	255
eDMSAPIIR_Descr_str	Text	255
eDMSAPIIR_Comments_str	Text	255

eDMSAPIIR_Site_id_n

This field specifies the site, as defined in eKERNEL_SITE table. In most environments, this value is 1.

An example of an entry typically found in this field is as follows: 1

eDMSAPIIR_Area_id_n

This field specifies the site, as defined in eKERNEL_AREA table. In most environments, this value is 1.

An example of an entry typically found in this field is as follows: 1

eDMSAPIIR_IC_Called_dev_str

This field specified a descriptor of the called device.

When a message is sent to a device that is defined in eDMSAPI_INBOUND table as type *IA, the resulting action depends on the called and calling devices.

The value must be the extension number of the device where the message is sent. In most situations each device defined in eDMSAPI_INBOUND table as *IA has at least one record in this table.

An example of an entry typically found in this field is as follows: 999

eDMSAPIIR_Calling_dev_str

This field specified a descriptor of the calling device. As described in eDMSAPI documentation section, incoming E2 messages are notified within eDMSAPI through calling device and called device. When an incoming message (to a device that is defined in eDMSAPI_INBOUND table as type *IA – incoming call alarm generation) is detected by eDMSAPI, the result action depends on the Called and Calling device.

The value must be the extension number to which the message was sent.

Possible values are:

Define an extension by number, for example, 866.

Define a generic value *ALL.

Define a generic number starting with some characters 85.

An example of an entry typically found in this field is as follows: *ALL

eDMSAPIIR_GRP_Name_str

This field specifies the group of users that is notified as a result of the *IA (incoming alarm generation) process through eDMSAPI. The group must be defined in eKERNEL_GROUP and eKERNEL_GROUP_MEMBER. A message is created for that group, with alarm identification (and attributes) specified in eDMSAPI_INBOUND_EVENT table. The corresponding attributes are defined in eKERNEL_ALARM table.

An example of an entry typically found in this field is as follows: REA

eDMSAPIIR_Msg_str

This field specifies the message that is sent as a result of the *IA (incoming alarm generation) process through eDMSAPI. The group receives a message defined in this field, with alarm attributes specified in eDMSAPI_INBOUND_EVENT table and eDMSAPI_INBOUND_RESULT table.

Refer to the sample data in Table 76 on page 1346 for examples of message definitions. As illustrated in the examples in Table 76 on page 1346, messages are built based upon fixed characters, plus the following:

- [Calling number], [
- Called number],
- [msg] special value,
- some combination of the three preceding values, which are replaced by the actual value of the request.

A format REA [Calling number] translates into REA 865 when the calling number is 865.

In release 3.0 and later, you can use a visual DNR to a device in the Messenger (new field DEV_Visual_dnr_str in table eKERNEL_DEVICE). Now when the system configuration configures a device with a visual DNR, this DNR is used to format a message when the message contains [Calling number]. The end user is confronted with the visual DNR instead of the device id.

An example of an entry typically found in this field is as follows: (see Figure 76 on page 1346)

eDMSAPIIR_Descr_str

This field is informational only.

eDMSAPIIR_Comments_str

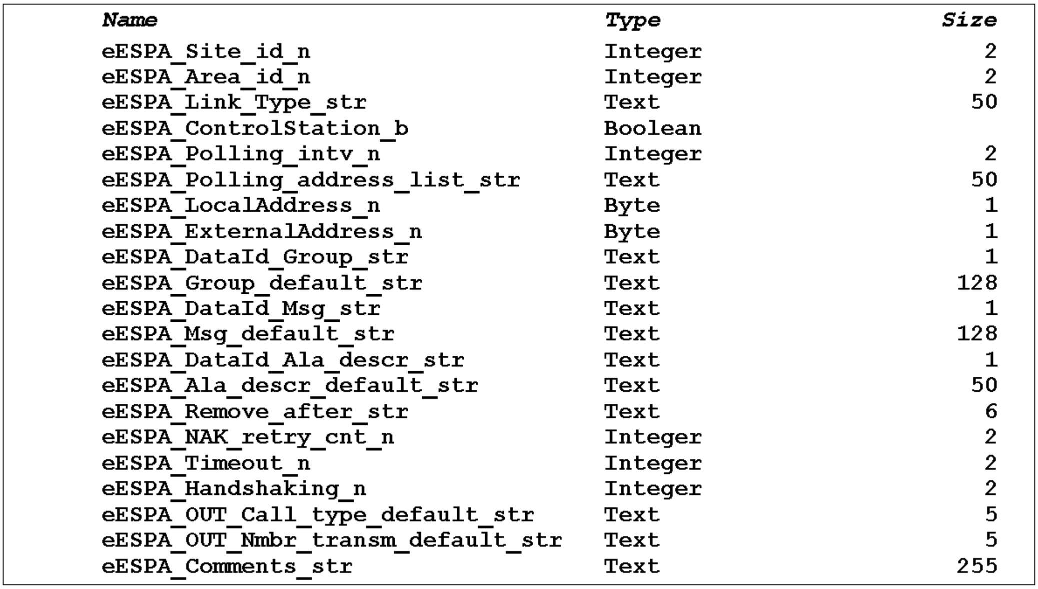
This field is used by administrators to add some remarks. The value is informational only.

Table 76
Sample Data

Site	Area	Called device	Calling device	Group	Message
1	1	222	8*	E2TESTGRP	TEST : [msg] from [Calling number] to [Called number].
1	1	56789	86*	E2TESTGRP	TEST 86* [msg]
1	1	56789	861	E2TESTGRP	TEST 861 [msg]
1	1	56789	865	E2TESTGRP	TEST 865 [msg]
1	1	56789	866	E2TESTGRP	TEST 866 [msg]
1	1	860	86*	REA	REA : [msg] from [Calling number] to [Called number].
1	1	860	865	REA	REA [msg] from [Calling number] to [Called number].
1	1	860	866	REA	REA [msg] from [Calling number] to [Called number].
1	1	860	867	REA	REA [msg] from [Calling number] to [Called number].
1	1	860	868	REA	REA [msg] from [Calling number] to [Called number].
1	1	861	*ALL	861	[msg]
1	1	865	*ALL	865	[msg]
1	1	888	*ALL	NOOD	NOOD [msg] from [Calling number] to [Called number].
1	1	999	*ALL	REA	REA [msg] from [Calling number] to [Called number].

Table: eESPA

Table 77
eESPA parameters



Name	*Type*	*Size*
eESPA_Site_id_n	Integer	2
eESPA_Area_id_n	Integer	2
eESPA_Link_Type_str	Text	50
eESPA_ControlStation_b	Boolean	
eESPA_Polling_intv_n	Integer	2
eESPA_Polling_address_list_str	Text	50
eESPA_LocalAddress_n	Byte	1
eESPA_ExternalAddress_n	Byte	1
eESPA_DataId_Group_str	Text	1
eESPA_Group_default_str	Text	128
eESPA_DataId_Msg_str	Text	1
eESPA_Msg_default_str	Text	128
eESPA_DataId_Ala_descr_str	Text	1
eESPA_Ala_descr_default_str	Text	50
eESPA_Remove_after_str	Text	6
eESPA_NAK_retry_cnt_n	Integer	2
eESPA_Timeout_n	Integer	2
eESPA_Handshaking_n	Integer	2
eESPA_OUT_Call_type_default_str	Text	5
eESPA_OUT_Nmbr_transm_default_str	Text	5
eESPA_Comments_str	Text	255

eESPA_Site_id_n

This field specifies the site identifier, as defined in eKERNEL_SITE. This value is, in most environments, equal to 1.

An example of an entry typically found in this field is as follows: 1

eESPA_Area_id_n

This field specifies the area identifier, as defined in eKERNEL_AREA. This value is, in most environments, equal to 1.

An example of an entry typically found in this field is as follows: 1

eESPA_Link_Type_str

This field specifies the type of physical link between the controlling and the controlled system.

The only supported value that can be entered in this field is RS232.

An example of an entry typically found in this field is as follows: RS232

eESPA_ControlStation_b

This value specifies whether the station is a control (master) station, or a slave. The protocol used conforms to International Standard ISO 1745 Information processing – Basic mode control procedures for data communication systems. It is a multidrop protocol utilizing a Control Station.

Because the physical interface is only RS232, it can only support a point to point interface to the external espa infrastructure. If more than one system must be integrated, multiple eESPA modules must be configured on multiple areas.

There is on each RS-232 interface only one system that can act as Control Station.

If the eESPA module for this site and area must act as Control Station (master), the value must be True or -1, otherwise, the value must be False or 0 (slave).

An example of an entry typically found in this field is as follows: False

eESPA_Polling_intv_n

This field specifies the polling interval in milliseconds, and is only relevant if eESPA_ControlStation_b is set to True (only the Control Station is polling).

An example of an entry typically found in this field is as follows: 150

eESPA_Polling_address_list_str

This field is only relevant if the module acts as Control Station (eESPA_ControlStation_b is set to True).

The Control Station must poll a device or devices on the communication line with the sequence <address> ENQ.

The characters 0 to 9 can be specified as addresses.

If more than one address must be polled, the addresses must be separated with a ^ sign. In this release, only a point to point link is supported, so only one address can be specified.

An example of an entry typically found in this field is as follows: 2

eESPA_LocalAddress_n

This field specifies the address of the local espa interface.

An example of an entry typically found in this field is as follows: 1

eESPA_ExternalAddress_n

This field specifies the address of the remote station.

One eESPA interface is linked with one area, so is linked to only one remote station. If more than one station can receive are sent espa alarms, more areas must be configured in the configuration database.

An example of an entry typically found in this field is as follows: 2

eESPA_DataId_Group_str

Use this field to set the relationship between the DECT Messenger Device or Group and the data identifier of the espa record that specifies the call address if eESPA acts as input program, so only relevant if eESPA receives external data from the espa infrastructure.

If the eESPA module acts as input program:

The eESPA module receives espa records. Each espa record received must be translated to a valid message request, and sent to the eKERNEL application.

The eESPA_DataId_Group_str field specifies the Data Identifier (normally 1) of the espa record that specifies the group. This group refers to the field GRP_Descr_str of eKERNEL_GROUP table.

In the following example, data identifier 1 (call address) is defined as eESPA_DataId_Group_str.

Table 78
Espa record: SOH1STX**1US12345**RS2USThe messageRS3US9RS4US3RS6US3ETXBCC

(SOH)	Start of header
STX	Start of text
ETX	End of text
US	Unit separator
RS	Record separator
BCC	Checksum

The incoming alarm/message, must be translated to a valid message request and sent to the eKERNEL, as shown in Figure 598.

Figure 598
Example: eESPA module acts as input program

```
<msgrqs>:

<xml><msgrqs><set_or_reset>*SET</set_or_reset>

<msg>The message</msg>

<alarmdescr>9</alarmdescr>

<group>12345</group>

<remove_after>*SENT</remove_after>

</msgrqs></xml>
```

If the specified data identifier is not present in the available datastream record, than the field eESPA_Group_default_str must be used to define a group in the message request.

If this eESPA module acts as an output program:

In the current release, the data identifiers for the espa records are fixed. Therefore, when a message request is sent by the eKERNEL to the eESPA module, the data in the <group> tag is put in data identifier 1 (call address).

In the following example, the data in the <group> tag from the message request, must be translated to data identifier 1 (call address) in the espa record.

Figure 599
Example: eESPA module acts as output program

```
Input: <msgrqs>:

<xml><msgrqs>

<id>00851</id>

<group>12345</group>

<call_type>3</call_type<transmission_nmbr>1</
transmission_nmbr>

<alarm_cnt>1</alarm_cnt>

<message_01>MESSAGE</message_01>

<beep_code_01>3</beep_code_01>

<priority_01>1</priority_01></msgrqs></xml>

Output: espa record :

SOH1STX1US12345RS2USMESSAGERS3US3RS4US3RS5US1RS6Us1ETXB
CC
```

> ***Note:*** An eESPA module can act as input and output program simultaneously, so can receive alarms from the espa infrastructure and sends a message request to the eKERNEL, and can receive on message requests from the eKERNEL and sends the alarms to the espa infrastructure.

An example of an entry typically found in this field is as follows: 1

eESPA_Group_default_str

This field is used to provide a default group name, in the event that no value can be retrieved from the available espa datastream. In this case, the same value is used for all alarms generated through this eESPA interface instance.

This group refers to the definitions of eKERNEL_GROUP table.

This parameter is only relevant if eESPA acts as an input program (so receives external data from the espa infrastructure).

An example of an entry typically found in this field is as follows: ESPA GROUP

eESPA_DataId_Msg_str

This field specifies the Data Identifier of the espa record that specifies the message. Mostly this values is 2.

This parameter is only relevant if eESPA acts as an input program (so receives external data from the espa infrastructure.

If the specified data identifier is not present in the available datastream record, than the field eESPA_Msg_default_str must be used to define a default message.

If the eESPA module acts as input program:

The received espa record must be translated to a valid message request, and sent to the eKERNEL application.

This field specifies the Data Identifier (normally 2) of the espa record that specifies the message.

In this example, data identifier 2 (display message) is defined as eESPA_DataId_Msg_str.

Table 79
Espa record: SOH1STX1US12345RS**2USThe message**RS3US9RS4US3RS6US3ETXBCC

(SOH)	Start of header
STX	Start of text
ETX	End of text
US	Unit separator
RS	Record separator
BCC	Checksum

The incoming alarm/message, must be translated to a valid message request and sent to the eKERNEL:

Figure 600
Example: eESPA module acts as input program

```
<msgrqs>:

<xml><msgrqs><set_or_reset>*SET</set_or_reset>

<msg>The message</msg>

<alarmdescr>9</alarmdescr>

<group>12345</group>

<remove_after>*SENT</remove_after>

</msgrqs></xml>
```

If this eESPA module acts as an output program:

in the current release, the data identifiers for the espa records are fixed. Therefore, when a message request is sent by the eKERNEL to the eESPA module, the data in the <message_xx> tag is put in data identifier 2 (display message).

In the following example, the data in the <message_xx> tag from the message request, must be translated to data identifier 2 (display message) in the espa record.

Figure 601
Example: eESPA module acts as output program

```
Input: <msgrqs>:

<xml><msgrqs>

<id>00851</id>

<group>12345</group>

<call_type>3</call_type>

<transmission_nmbr>1</transmission_nmbr>

<alarm_cnt>1</alarm_cnt>

<message_01>MESSAGE</message_01>

<beep_code_01>3</beep_code_01>

<priority_01>1</priority_01></msgrqs></xml>

Output: espa record :

SOH1STX1US12345RS2USMESSAGERS3US3RS4US3RS5US1RS6Us1ETXB
CC
```

An example of an entry typically found in this field is as follows: 2

eESPA_Msg_default_str

This field is used to provide a default message, in the event that no value can be retrieved from the available datastream. In this case, the same value is used for all alarms generated through this eESPA interface instance.

This parameter is only relevant if eESPA acts as an input program (so receives external data from the espa infrastructure.

An example of an entry typically found in this field is as follows: ESPA alarm

eESPA_DataId_Ala_descr_str

This field specifies the Data Identifier of the espa record that specifies the alarm description.

This parameter is only relevant if eESPA acts as an input program (so receives external data from the espa infrastructure.

This field refers to the definitions of eKERNEL_ALARM table, and must be appropriately configured (for example, message length, and so on).

If the specified data identifier is not present in the available datastream record, than the field eESPA_Ala_descr_default_str must be used to define a default message.

This field can also be a combination of more than one data identifier.

Than the data identifiers must be separated by a ^ sign. If for instance the beep code (data identifier 3) in combination with the priority (data identifier 6) must result in the alarm description, this value must be 3^6.

If the display message (data identifier 2) is a part of the alarm description, you can specify the first x characters of the message as the alarm description. For example the value 2:3, results in an alarm description equal to the first 3 characters of the display message (data identifier 2). If the message is, for example, NURSE CALL ROOM 02, the alarm description is NUR, so the alarm NUR must be configured in the eKERNEL_ALARM table.

If this eESPA module acts as an input program:

In this example, data identifier 3 (beep coding) is defined as eESPA_DataId_Ala_descr_str.

Table 80
Espa record: SOH1STX1US12345RS2USThe messageRS**3US9**RS4US3RS6US3ETXBCC

(SOH)	Start of header
STX	Start of text
ETX	End of text

Table 80
Espa record: SOH1STX1US12345RS2USThe messageRS**3US9**RS4US3RS6US3ETXBCC

US	Unit separator
RS	Record separator
BCC	Checksum

The incoming alarm/message must be translated to a valid message request and sent to the eKERNEL:

Figure 602
Example: eESPA module acts as input program

```
<msgrqs>:

<xml><msgrqs><set_or_reset>*SET</set_or_reset>

<msg>The message</msg>

<alarmdescr>9</alarmdescr>

<group>12345</group>

<remove_after>*SENT</remove_after>

</msgrqs></xml>
```

If this eESPA module acts as an output program:

In the current release, the data identifiers for the espa records are fixed. Therefore, when a message request is sent by the eKERNEL to the eESPA module, the data in the <beep_code_xx> tag is put in data identifier 3 (beep coding).

In the following example, the data in the <beep_code_xx> tag from the message request, must be translated to data identifier 3 (beep coding) in the espa record.

Figure 603
Example: eESPA module acts as output program

```
Input: <msgrqs>:

<xml><msgrqs>

<id>00851</id>

<group>12345</group>

<call_type>3</call_type>

<transmission_nmbr>1</transmission_nmbr>

<alarm_cnt>1</alarm_cnt>

<message_01>MESSAGE</message_01>

<beep_code_01>3</beep_code_01>

<priority_01>1</priority_01></msgrqs></xml>

Output: espa record :

SOH1STX1US12345RS2USMESSAGERS3US3RS4US3RS5US1RS6Us1ETXB
CC
```

An example of an entry typically found in this field is as follows: 2:3^3. This indicates that the first 3 characters of the display message, a ^ and the values of data identifier 3 is equal to the alarm description. The value NUR^1, NUR^2, SAN^1, and so on, must be configured in the eKERNEL_ALARM table.)

eESPA_Ala_descr_default_str

This field is used to provide a default alarm description, in the event that no value can be retrieved from the available datastream. In this case, the same value is used for all alarms generated through this eESPA interface instance. This alarm description refers to the definitions of eKERNEL_ALARM table.

This parameter is only relevant if eESPA acts as an input program (so receives external data from the espa infrastructure.

An example of an entry typically found in this field is as follows: ESPA

eESPA_Remove_after_str

This parameter accepts values *SENT, *RESET, or *CALC.

This parameter is only relevant if eESPA acts as an input program (so it receives external data from the espa infrastructure).

In most cases the eESPA interfaces is used to capture alarms and received data contains alarm information (acts as input program). In this situation messages are transmitted to eKERNEL immediately upon arrival and these alarms are processed within DECT Messenger.

In some environments, the remote peripherals cannot indicate that pending alarms are reset, and therefore the eKERNEL must handle the alarms. Use this field to configure eKERNEL_ALARM table to correctly handle the alarm requests and refrain from endless-loop conditions. As such alarms are typically *set with the option remove after sent. The eESPA_Remove_after_str are then set to *SENT.

In some environments, the attached peripherals are capable of sending a reset to clear all pending alarms. In such case, alarms must be set using the remove after *RESET value, indicating all pending alarms remain in the eKERNEL database unless the reset condition is met.

This parameter refers to all alarms, so that means that every alarm must receive a reset (a reset occurs if data identifier 4 (call type) is equal to value 1).

If the value *CALC is specified, some alarms receive a reset, and other alarms not. Therefore the eKERNEL application checks to determine if the alarm description with remove after *SENT exists. If so, this alarm type is processed, otherwise the alarm is processed as if remove after *RESET is specified.

If the alarm description is not configured in the eKERNEL_ALARM table, the alarm is not processed.

An example of an entry typically found in this field is as follows: *SENT

eESPA_NAK_retry_cnt_n

This field specifies the number of retries to re-transmit a message after receiving a NAK.

A device that has control of the communication line can transfer data to the other devices. When unable to accept the message, the receiving device sends a negative acknowledge with a (1 or 2 or 3) NAK sequence, and the sending device can then retransmit the block. If, after eESPA_NAK_retry_cnt_n attempts, the transmission still fails, and the sending device terminates transmission with the EOT character.

An example of an entry typically found in this field is as follows: 2

eESPA_Timeout_n

This values specifies in seconds how long the station waits, if no valid transactions are detect on the communication line, before sending a EOT and terminate the communication and regain control.

An example of an entry typically found in this field is as follows: 10

eESPA_Handshaking_n

This field sets and returns the hardware handshaking protocol.

The possible values are:

No handshaking. (comNone)

XOn/XOff handshaking. (ComXonXoff)

Request-to-send/clear-to-send handshaking (comRTS)

Both request-to-send and XOn/XOff handshaking. (comRTSXonXoff)

The default value is 0.

An example of an entry typically found in this field is as follows: 0

eESPA_OUT_Call_type_default_str

This field is only relevant if the eESPA module acts as output program, so for message sent from the eKERNEL to the eESPA interface.

A <msgrqs> request from the eKERNEL to the espa interface, contains a tag <call_type> that defines the value for data identifier 4 (call type). If *NONE is specified, data identifier 4 is not a part of the espa record.

The possible values are: 0, 1, 2, 3, *NONE

In the following example, the data in the <call_type> tag from the message request, must be translated to data identifier 4 (call type) in the espa record.

Figure 604
Example: eESPA module acts as output program

```
Input: <msgrqs>:

<xml><msgrqs>

<id>00851</id>

<group>12345</group>

<call_type>3</call_type>

<transmission_nmbr>1</transmission_nmbr>

<alarm_cnt>1</alarm_cnt>

<message_01>MESSAGE</message_01>

<beep_code_01>3</beep_code_01>

<priority_01>1</priority_01></msgrqs></xml>

Output: espa record :

SOH1STX1US12345RS2USMESSAGERS3US3RS4US3RS5US1RS6Us1ETXB
CC
```

An example of an entry typically found in this field is as follows: 3

eESPA_OUT_Nmbr_transm_default_str

This field is only relevant if the eEPSA module acts as an output program, so for message sent from the eKERNEL to the eESPA interface.

A <msgrqs> request from the eKERNEL to the espa interface, contains a tag <transmission_nmbr> that defines the value for data identifier 5 (transmission number). If *NONE is specified, data identifier 5 is not a part of the espa record.

In the following example, the data in the <transmission_nmbr> tag from the message request, must be translated to data identifier 5 (number of transmissions) in the espa record.

Figure 605
Example: eESPA module acts as output program

```
Input: <msgrqs>:

<xml><msgrqs>

<id>00851</id>

<group>12345</group>

<call_type>3</call_type>

<transmission_nmbr>1</transmission_nmbr>

<alarm_cnt>1</alarm_cnt>

<message_01>MESSAGE</message_01>

<beep_code_01>3</beep_code_01>

<priority_01>1</priority_01></msgrqs></xml>

Output: espa record :

SOH1STX1US12345RS2USMESSAGERS3US3RS4US3RS5US1RS6Us1ETXB
CC
```

An example of an entry typically found in this field is as follows: 1

eESPA_Comments_str

This field can be filled with comments, to allow administrators to add some remarks to the configuration record.

Table: eESPA_OUTBOUND_CFG

Table 81
eESPA_outbond_cfg parameters

Name	*Type*	*Size*
eESPAO_Site_id_n	Integer	2
eESPAO_Area_id_n	Integer	2
eESPAO_ALA_Prty_from_n	Integer	2
eESPAO_ALA_Prty_to_n	Integer	2
eESPAO_BeepCode_str	Text	5
eESPAO_Priority_str	Text	5
eESPAO_Comments_str	Text	255

eESPAO_Site_id

This field specifies the site identifier, as defined in eKERNEL_SITE. This value is, in most environments, equal to 1.

An example of an entry typically found in this field is as follows: 1

eESPAO_Area_id_n

This field specifies the site identifier, as defined in eKERNEL_AREA. This value is, in most environments, equal to 1.

An example of an entry typically found in this field is as follows: 1

eESPAO_ALA_Prty_from_n

This field refers to the ALA_Prty_n field of the table eKERNEL_ALARM, and defines the priority of an alarm.

A low value indicates an important alarm, a high value a less important alarm.

With the fields eESPAO_ALA_Prty_from_n and eESPAO_ALA_Prty_to_n you can specify a range of alarm priorities and set a relationship to the beepcode record type and the priority record type of the espa datablock.

The Data identifier for the beepcode record type is 3.

The Data identifier for the priority record type is 6.

Table 82
Example eESPAO_ALA_Prty_from/to_n values

Site	Area	Alarm from	Alarm to	Beepcode	Priority
1	1	0	2	1	2
1	1	3	5	3	1
1	1	6	999	9	3

When a <msgrqs> is sent to the eESPA with an alarm priority equal to 2 for pager 4567, a datablock is created with a beepcode 1 (data identifier 3) and a priority 2 (High) (data identifier 6). Therefore, all alarms with a priority between 0 and 2 have these specifications.

Example datablock:

(RS: record separator, US: Unit separator

* Alarm priority equal to or between 0 and 2

```
1US4567RS2USExampleRS3US1RS6US2
```

* Alarm priority equal to or between 3 and 5

```
1US4567RS2USExampleRS3US3RS6US1
```

* Alarm priority equal to or between 6 and 999 (highest possible value)

```
1US4567RS2USExampleRS3US9RS6US3
```

An example of an entry typically found in this field is as follows: 0

eESPAO_ALA_Prty_to_n

See eESPAO_ALA_Prty_from_n

An example of an entry typically found in this field is as follows: 999

eESPAO_BeepCode_str

This field specifies the data that must be entered in the espa datablock for record type beepcode (data identifier 3).

An example of an entry typically found in this field is as follows: 1

eESPAO_Priority_str

This field specifies the data that must be entered in de espa datablock for record type priority (data identifier 6).

An example of an entry typically found in this field is as follows: 3

eESPAO_Comments_str

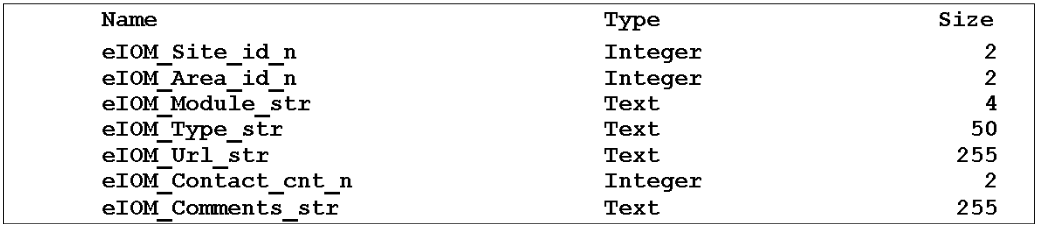
This field can be used to store comments, enabling administrators to add remarks to the configuration record. See Table 83 for example eESPAO_Comments_str values.

Table 83
Sample eESPAO_Comments_str values

Site	Area	Alarm from	Alarm to	Beepcode	Priority
1	1	0	2	1	2
1	1	3	5	3	1
1	1	6	999	9	3
1	2	0	5	1	3
1	2	6	999	*NONE	3
1	3	0	999	1	*NONE

Table: eIO_MODULE

Table 84
eIO_modules parameters



Name	Type	Size
eIOM_Site_id_n	Integer	2
eIOM_Area_id_n	Integer	2
eIOM_Module_str	Text	4
eIOM_Type_str	Text	50
eIOM_Url_str	Text	255
eIOM_Contact_cnt_n	Integer	2
eIOM_Comments_str	Text	255

eIOM_Site_id_n

This field specifies the site identifier, as defined in eKERNEL_SITE table. In most environments, this value is 1.

An example of an entry typically found in this field is as follows: 1

eIOM_Area_id_n

This field specifies the area identifier, as defined in eKERNEL_AREA table. In most environments, this value is 1.

An example of an entry typically found in this field is as follows: 1

eIOM_Module_str

This value refers to the 2-byte module identifier, specified in the FieldPoint Explorer and in eIO_MODULE table. A typical value is between 01 and 08. Ensure that the table eIO_DO defines only digital output-contacts (those with a matching digital output module). The current release supports up to eight modules per eIO instance, including one FP-1000 controlling module, and can refer to FP-AI-100, DP-DI-300, FP-DI-301, FP-DI-330 and FP-DO-401.

The current implementation of eIO is limited to configurations of up to eight modules attached to one FP-1000 controller module. Nortel recommends starting the first module with number 01 and incrementing by 1 for the other modules.

> ***Note:*** Specify the leading 0 in the numbering (enter the value 01, not 1).

An example of an entry typically found in this field is as follows: 01

eIOM_Type_str

The current release supports the following modules:

Table 85
eIOM supported modules

FP-AI-100	Analogue input	8 contacts
FP-DI-300	Digital input	8 contacts
FP-DI-301	Digital input	16 contacts
FP-DI-330	Digital input	8 contacts
FP-DI-401	Digital output	8 contacts

Refer to the corresponding chapter in this document for technical specifications on the modules.

An example of an entry typically found in this field is as follows: FP-DI-330

eIOM_Url_str

This field denotes the URL string associated with the module. Refer to the FieldPoint Explorer and other National Instrument distributed I/O documentation resources for more information on the URL defined OPC server binding mechanism.

The FieldPoint Explorer is a recommended way to determine naming conventions. Take note of the ending characters specified in Table 86 on page 1370. Using an incorrect URL prevents binding contacts to the OPC Server, resulting in system malfunction.

An example of an entry typically found in this field is as follows: opc:/ National Instruments.OPCFieldPoint/FP Res\FP-AI-100 @1\Channel

eIOM_Contact_cnt_n

The field defines the number of contacts that are associated to the module.This field can specify a smaller number than the maximum number of physical available contacts on a module, in which case the remaining contacts are not bound to the OPC Server and remain non-operational.

An example of an entry typically found in this field is as follows: 8

eIOM_Comments_str

This field can be entered with remarks from an administrator, and is informational only. You can use this filed to document the physical connection here too, to ease later configuraion.

An example of an entry typically found in this field is as follows: OR 004 – fire detection.

Table 86 on page 1370 provides sample eIO module table data.

Table 86
eIO_module sample data

Site	Area	Module	Type	URL	Count
1	1	01	FP-DI-300	opc:/National Instruments.OPCFieldPoint/FP Res\FP-DI-330 @2\Channel	16
2	1	01	FP-AI-100	opc:/National Instruments.OPCFieldPoint/FP Res\FP-AI-100 @1\Channel	8
2	1	02	FP-DI-300	opc:/National Instruments.OPCFieldPoint/FP Res\FP-DI-330 @2\Channel	8
2	1	03	FP-DO-401	opc:/National Instruments.OPCFieldPoint/FP Res\FP-DO-401 @3\Channel	16
2	2	01	FP-AI-100	opc:/National Instruments.OPCFieldPoint/FP Res\FP-AI-100 @1\Channel	8
2	2	02	FP-DI-300	opc:/National Instruments.OPCFieldPoint/FP Res\FP-DI-330 @2\Channel	8
2	2	03	FP-DO-401	opc:/National Instruments.OPCFieldPoint/FP Res\FP-DO-401 @3\Channel	16
2	3	02	FP-DI-300	opc:/National Instruments.OPCFieldPoint/FP Res\FP-DI-330 @2\Channel	8

Table: eIO_AI

Table 87
eIO_AI parameters

Name	*Type*	*Size*
eIOAI_Site_id_n	Integer	2
eIOAI_Area_id_n	Integer	2
eIOAI_Module_str	Text	4
eIOAI_Contact_str	Text	2
eIOAI_Min_S_str	Text	10
eIOAI_Min_R_str	Text	10
eIOAI_Max_R_str	Text	10
eIOAI_Max_S_str	Text	10
eIOAI_ALA_descr_str	Text	50
eIOAI_GRP_Name_str	Text	20
eIOAI_MSG_str	Text	255
eIOAI_Comments_str	Text	255

eIOAI_Site_id_n

This field refers to the site identifier, as defined in the eKERNEL_SITE table. In most environments, this value is 1.

An example of an entry typically found in this field is as follows: 1

eIOAI_Area_id_n

This field refers to the area identifier, as defined in the eKERNEL_AREA table. In most environments, this value is 1.

An example of an entry typically found in this field is as follows: 1

eIOAI_Module_str

This value refers to the 2-byte module identifier, specified in the FieldPoint Explorer and in eIO_MODULE table. A typical value is between 01 and 08. Verify that the table eIO_AI only defines analogue input-contacts (the contacts with a matching analogue input module). Current release supports FP-AI-100 modules.

Current implementation of eIO is limited to configurations of up to 8 modules attached to one FP-1000 controller module. Nortel recommends starting the first module with number 01 and incrementing by one for the other modules. Specify the leading 0 in the numbering (do not specify 1, but specify instead 01).

An example of an entry typically found in this field is as follows: 01

eIOAI_Contact_str

This value refers to each individual contact, and is specified in the FieldPoint Explorer. Valid values are in the range between 01 and 08 for the currently supported FP-AI-100. Note that contact numbers start with 01 and are incremented by one. You must specify the leading 0 in the numbering (do not specify 1, but specify instead 01). Note that some peripherals of National Instruments include labels and documentations where contacts start numbering at 0 up to 7, whereas eIO starts at 01 up to 08.

An example of an entry typically found in this field is as follows: 01

eIOAI_Min_S_str

The value specifies the analogue level measured on a contact to set a minus-level alarm. If minus-level alarms are to be disabled a 00,000000 value can be specified.

> ***Note:*** All values must be specified in format 00,000000 with 2 digits before the decimal separator and 6 digits after the decimal separator. The decimal separator must be set according to the operating system regional settings.

Refer to the FieldPoint Explorer documentation on how to configure the FP-AI-100 module. Each channel can individually be set according to the attached input, and allow specifying the unit of measurement en the measured input range. Nortel recommends that you first test the peripherals with the FieldPoint Explorer prior to configuring and taking eIO into production.

> ***Note:*** Check your operating system settings to find out which decimal separator is in use. Nortel recommends that you set the operating system to the country specific values, thus the locale Belgium (Dutch) in Belgium, even when an English operating system is installed. These regional settings result in internal usage of decimal separator symbols in the form of period (.) or comma (,). If your system is set up with comma (,) as decimal separator, a comma (,) must also be specified when values are entered in the database.

An example of an entry typically found in this field is as follows: 03,000000

eIOAI_Min_R_str

The value specifies the analogue level measured on a contact to reset a minus-level alarm. If minus-level alarms are to be disabled a 00,000000 value can be specified.

> ***Note:*** All values must be specified in format 00,000000 with 2 digits before the decimal separator and 6 digits after the decimal separator. The decimal separator must be set according to the operating system regional settings.

Refer to the FieldPoint Explorer documentation for more information the configuration of the FP-AI-100 module. Each channel can individually be set according to the attached input, and allow to specify the unit of measurement en the measured input range. Nortel recommends that you first test the peripherals with the FieldPoint Explorer prior to configuring and taking eIO into production.

> ***Note:*** Check your operating system settings to find out which decimal separator is in use. Nortel recommends that you set the operating system to the country-specific values, thus the locale Belgium (Dutch) in Belgium, even when an English operating system is installed. These regional settings result in internal usage of decimal separator symbols in the form of period (.) or comma (,). If your system is set up with comma (,) as decimal separator, a comma (,) must also be specified when values are entered in the database.

An example of an entry typically found in this field is as follows: 06,000000

eIOAI_Max_R_str

The value specifies the analogue level measured on a contact to set a plus-level alarm.

If plus-level alarms are to be disabled a 99,999999 value can be specified.

> ***Note:*** All values must be specified in format 00,000000 with 2 digits before the decimal separator and 6 digits after the decimal separator. The decimal separator must be set according to the operating system regional settings.

Refer to the FieldPoint Explorer documentation for more information on the configuration of the FP-AI-100 module. Each channel can individually be set according to the attached input, and allow specifying the unit of measurement en the measured input range. Nortel recommends that you first test the peripherals with the FieldPoint Explorer prior to configuring and taking eIO into production.

> ***Note:*** Check your operating system settings to find out which decimal separator is in use. Nortel recommends that you set the operating system to the country specific values, thus the locale Belgium (Dutch) in Belgium, even when an English operating system is installed. These regional settings result in internal usage of decimal separator symbols in the form of period (.) or comma (,). If your system is set up with comma (,) as decimal separator, a comma (,) must also be specified when values are entered in the database.

An example of an entry typically found in this field is as follows: 20,000000

eIOAI_Max_S_str

The value specifies the analogue level measured on a contact to reset a plus-level alarm.

If plus-level alarms are to be disabled a 99,999999 value can be specified.

> ***Note:*** All values must be specified in format 00,000000 with 2 digits before the decimal separator and 6 digits after the decimal separator. The decimal separator must be set according to the operating system regional settings.

Refer to the FieldPoint Explorer documentation for more information on the configuration of the FP-AI-100 module. Each channel can individually be set according to the attached input, and allow specifying the unit of measurement en the measured input range. Nortel recommends that you first test the peripherals with the FieldPoint Explorer prior to configuring and taking eIO into production.

> ***Note:*** Check your operating system settings to find out which decimal separator is in use. Nortel recommends that you set the operating system to the country specific values, thus the locale Belgium (Dutch) in Belgium, even when an English operating system is installed. These regional settings result in internal usage of decimal separator symbols in the form of period (.) or comma (,). If your system is set up with comma (,) as decimal separator, a comma (,) must also be specified when values are entered in the database.

When values are entered in the database.

An example of an entry typically found in this field is as follows:15,000000

eIOAI_ALA_Descr_str

The alarm description field is a description defined in the eKERNEL_ALARM table for the associated eIO module. In the example shown in Table 88, an alarm description A-INPUT is defined with matching records in the eKERNEL_ALARM table.

Table 88
eIOAS_ALA_Descr_str example

ALA_id_n	ALA_INPGM_id	ALA_Descr_str	ALA_Remove_	ALA_Prty_n
1160101	11601	A-INPUT	*SENT	5
1160102	11601	A-INPUT	*RESET	5

An example of an entry typically found in this field is as follows: A-INPUT

eIOAI_GRP_Name_str

The group name describes what group is informed on the error condition, and refers to a group defined in eKERNEL_GROUP and eKERNEL_GROUP_MEMBER tables.

An example of an entry typically found in this field is as follows: 00003

eIOAI_MSG_str

This field describes the message that is sent to the group members. Nortel recommends that you enter descriptive text that provides the recipient sufficient information to handle the alarm condition. Mobile users often lack immediate access to other information resources such as plans, technical specs, and so on. Nortel recommends that you select an appropriate message that is short and descriptive enough, and keep text length less than, or equal to, the maximum length defined in the associated eKERNEL_ALARM table.

An example of an entry typically found in this field is as follows: TEMPERATURE OR 002

eIOAI_Comments_str

This field is available for an administrator to enter some descriptive text that allows location and identification of the attached input device and its usage.

Table 89 provides sample eIO_AI module table data.

Table 89
eIO_AI sample data (Part 1 of 4)

SITe	AREa	Mod	Cont	Min_S	Min_R	Max_R	Max_S	ALA_descr	Group	MSG
1	1	01	01	00,000000	00,000000	00,000400	00,000400	A-INPUT	AI	Analog Input 01
1	1	01	02	00,000000	00,000000	12,000000	20,000000	A-INPUT	AI	Analog Input 02
1	1	01	03	00,000000	00,000000	12,000000	20,000000	A-INPUT	AI	Analog Input 03

Table 89
eIO_AI sample data (Part 2 of 4)

1	1	01	04	00,000000	00,000000	12,000000	20,000000	A-INPUT	AI	Analog Input 04
1	1	01	05	00,000000	00,000000	12,000000	20,000000	A-INPUT	AI	Analog Input 05
1	1	01	06	00,000000	00,000000	12,000000	20,000000	A-INPUT	AI	Analog Input 06
1	1	01	07	00,000000	00,000000	12,000000	20,000000	A-INPUT	AI	Analog Input 07
1	1	01	08	00,000000	00,000000	12,000000	20,000000	A-INPUT	AI	Analog Input 08
2	1	01	01	00,000000	00,000000	12,000000	20,000000	A-INPUT	AI	Analog Input 01
2	1	01	02	00,000000	00,000000	12,000000	20,000000	A-INPUT	AI	Analog Input 02
2	1	01	03	00,000000	00,000000	12,000000	20,000000	A-INPUT	AI	Analog Input 03
2	1	01	04	00,000000	00,000000	12,000000	20,000000	A-INPUT	AI	Analog Input 04
2	1	01	05	00,000000	00,000000	12,000000	20,000000	A-INPUT	AI	Analog Input 05

Table 89
eIO_AI sample data (Part 3 of 4)

2	1	01	06	00,000000	00,000000	12,000000	20,000000	A-INPUT	AI	Analog Input 06
2	1	01	07	00,000000	00,000000	12,000000	20,000000	A-INPUT	AI	Analog Input 07
2	1	01	08	00,000000	00,000000	12,000000	20,000000	A-INPUT	AI	Analog Input 08
2	2	01	01	00,000000	00,000000	12,000000	20,000000	A-INPUT	00001	Analog Input 01
2	2	01	02	00,000000	00,000000	12,000000	20,000000	A-INPUT	00001	Analog Input 02
2	2	01	03	00,000000	00,000000	12,000000	20,000000	A-INPUT	00001	Analog Input 03
2	2	01	04	00,000000	00,000000	12,000000	20,000000	A-INPUT	00001	Analog Input 04
2	2	01	05	00,000000	00,000000	12,000000	20,000000	A-INPUT	00001	Analog Input 05
2	2	01	06	00,000000	00,000000	12,000000	20,000000	A-INPUT	00001	Analog Input 06

Table 89
eIO_AI sample data (Part 4 of 4)

2	2	01	07	00,000000	00,000000	12,000000	20,000000	A-INPUT	00001	Analog Input 07
2	2	01	08	00,000000	00,000000	12,000000	20,000000	A-INPUT	00001	Analog Input 08

Table: eIO_DI

Table 90
eIO_DI parameters

Name	*Type*	*Size*
eIODI_Site_id_n	Integer	2
eIODI_Area_id_n	Integer	2
eIODI_Module_str	Text	4
eIODI_Contact_str	Text	2
eIODI_ContactType_str	Text	2
eIODI_ALA_Descr_str	Text	50
eIODI_GRP_Name_str	Text	20
eIODI_MSG_str	Text	255
eIODI_Comments_str	Text	255

eIODI_Site_id_n

This field refers to the site identifier, as defined in the eKERNEL_SITE table. In most environments, this value is 1.

An example of an entry typically found in this field is as follows: 1

eIODI_Area_id_n

This field refers to the area identifier, as defined in the eKERNEL_AREA table. In most environments, this value is 1.

An example of an entry typically found in this field is as follows: 1

eIODI_Module_str

This value refers to the 2-byte module identifier, specified in the FieldPoint Explorer and in eIO_MODULE table. A typical value is between 01 and 08. Ensure that the table eIO_DI only defines digital input-contacts, thus only the contacts with a matching digital input module. Current release supports FP-DI-300, FP-DI-301 and FP-DI-330.

Current implementation of eIO is limited to configurations of up to eight modules attached to one FP-1000 controller module. Nortel recommends starting the first module with number 01 and incrementing by one for the other modules. Specify the leading 0 in the numbering (do not specify 1, but specify instead 01).

An example of an entry typically found in this field is as follows: 02

eIODI_Contact_str

Valid values are in the range between 01 and 08 for the modules with 8 contacts and between 01 and 16 for the modules with 16 contacts. Note contact numbers start with 01 and are incremented by one. You must specify the leading 0 in the numbering (do not specify 1, but specify instead 01). Note that some peripherals of National Instruments include labels and documentations where contacts start numbering at 0 up to 7 (or 0 up to 15), whereas eIO starts at 01 up to 08 (or 01 up tot 16).

This value refers to each individual contact, and is specified in the FieldPoint Explorer. Range of values are 01 to 16 for FP-DI-301 module and 01 to 08 for the other digital input modules.

An example of an entry typically found in this field is as follows: 01

eIODI_ContactType_str

This parameter accepts the following values:

OS (in Dutch open schakelaar – open switch) meaning the contact is, in the base state, open and can be switched on at set and remains on until switched off at reset

OD (in Dutch open drukknop – open push button) meaning the contact is in base state open and can be switched on for a very short time and immediately fall back to the base state. Typically used for push buttons that generate alarm.

GS (in Dutch gesloten schakelaar – closed switch) meaning the contact is in base state closed and can be switched off at set and remains off until switched back on at reset.

GD (in Dutch gesloten drukknop – closed push button) meaning the contact is in base state closed and can be switched off for a very short time and immediately fall back to the base state.

An example of an entry typically found in this field is as follows: GD

eIODI_ALA_Descr_str

The alarm description field is a description defined in the eKERNEL_ALARM table for the associated eIO module. In the example shown in Table 91, an alarm description D-INPUT is defined with matching records in the ALARM table, as shown in Table 91.

Table 91
eIO alarm description

Alarm ID	Input program	Alarm description	Remove after	Priority
1160101	11601	D-INPUT	*SENT	5
1160101	11601	D-INPUT	*RESET	5

An example of an entry typically found in this field is as follows: D-INPUT

eIODI_GRP_Name_str

The group name describes what group is informed on the error condition, and refers to a group defined in eKERNEL_GROUP and eKERNEL_GROUP_MEMBER table.

An example of an entry typically found in this field is as follows: 00003

eIODI_MSG_str

This field describes the message that is sent to the group members. Nortel recommends that you enter descriptive text that provides the recipient sufficient information to handle the alarm condition. When selecting a message, Nortel recommends that you take into account that mobile users often lack immediate access to other information resources, such as a site map or technical specs, and keep the message length less than, or equal to, the maximum length defined in the associated eKERNEL_ALARM table.

An example of an entry typically found in this field is as follows: FIRE IN ELEVATOR

eIODI_Comments_str

This field is available for an administrator to enter some descriptive text that allows location and identification of the attached input device and its usage.

Table 92 provides sample eIO_DI module table data.

Table 92
eIO_DI sample data (Part 1 of 2)

Site	ARea	Mod	Contact	Type	ALA_Descr	GRP_ Name	Message
1	1	01	01	OD	D-INPUT	DI	Digital Input 01
1	1	01	02	OS	D-INPUT	DI	Digital Input 02
1	1	01	03	GS	D-INPUT	DI	Digital Input 03
1	1	01	04	GD	D-INPUT	DI	Digital Input 04
1	1	01	05	OD	D-INPUT	DI	Digital Input 05
1	1	01	06	OD	D-INPUT	DI	Digital Input 06
1	1	01	07	OD	D-INPUT	DI	Digital Input 07
1	1	01	08	OS	D-INPUT	DI	Digital Input 08
1	1	01	09	OD	D-INPUT	DI	Digital Input 09
1	1	01	10	OS	D-INPUT	DI	Digital Input 10
1	1	01	11	GS	D-INPUT	DI	Digital Input 11
1	1	01	12	GD	D-INPUT	DI	Digital Input 12
1	1	01	13	OD	D-INPUT	DI	Digital Input 13
1	1	01	14	OD	D-INPUT	DI	Digital Input 14

Table 92
eIO_DI sample data (Part 2 of 2)

1	1	01	15	OD	D-INPUT	DI	Digital Input 15
1	1	01	16	OS	D-INPUT	DI	Digital Input 16

Table: eIO_DO

Table 93
eIO_DO parameters

Name	*Type*	*Size*
eIODO_Site_id_n	Integer	2
eIODO_Area_id_n	Integer	2
eIODO_Module_str	Text	2
eIODO_Contact_str	Text	2
eIODO_Seconds_n	Integer	2
eIODO_Comments_str	Text	255

eIODO_Site_id_n

This field specifies the site identifier, as defined in the eKERNEL_SITE table. In most environments, this field has value 1.

An example of an entry typically found in this field is as follows: 1

eIODO_Area_id_n

This field specifies the area identifier, as defined in the eKERNEL_AREA table. In most environments, this field has value 1.

An example of an entry typically found in this field is as follows: 1

eIODO_Module_str

This value refers to the two-byte module identifier, specified in the FieldPoint Explorer and in eIO_MODULE table. A typical value is between 01 and 08. Ensure that the table eIO_DO only defines digital output-contacts, thus only the contacts with a matching digital output module. Current release supports FP-DO-401 modules.

Current implementation of eIO is limited to configurations of up to 8 modules attached to one FP-1000 controller module. Nortel recommends starting the first module with number 01 and incrementing by one for the other modules. Specify the leading 0 in the numbering (do not specify 1, but specify instead 01).

An example of an entry typically found in this field is as follows: 01

eIODO_Contact_str

This value refers to each individual contact, and is specified in the FieldPoint Explorer. Valid values are in the range between 01 and 16 for the currently supported FP-DO-401. Note contact numbers start with 01 and are incremented by one. You must specify the leading 0 in the numbering (do not specify 1, but specify instead 01). Note that some peripherals of National Instruments include labels and documentations where contacts start numbering at 0 up to 15, whereas eIO starts at 01 up to 16.

An example of an entry typically found in this field is as follows: 01

eIODO_Seconds_n

The implementation of digital output consists of two different models.

- In the first model, the eKERNEL changes the state of the contact at alarm activation, and changed the contact back to the original state at alarm deactivation. In this model both set and reset are controlled by eKERNEL, and requires off-course alarm conditions where there is a discrete set and reset condition.
- In the second model, the eKERNEL only changes the state of the contact at alarm activation. This is a one-time signal, and here is no further request that resets the alarm condition. In this model, eIO automatically resets the alarm condition when an specified amount of time elapsed.

The value eIODO_Seconds_n refers to the second model, and specifies the number of seconds a digital output is activated, in the event that the alarms are not reset from eKERNEL.

The value must be set to 0 when the contact is used for the first model. In this case, eKERNEL deactivates the alarm.

An example of an entry typically found in this field is as follows: 30

eIODO_Comments_str

This field can contain remarks from the administrator. The value is informational only, and does not affect processing.

Table 94 provides sample eIO_DO module table data.

Table 94
eIO_DO sample data (Part 1 of 2)

Site	Area	Module	Contact	Seconds	Comments
1	1	03	01	5	
1	1	03	02	5	
1	1	03	03	5	
1	1	03	04	5	
1	1	03	05	5	
1	1	03	06	5	
1	1	03	07	5	
1	1	03	08	5	
2	1	03	01	5	
2	1	03	02	5	
2	1	03	03	5	
2	1	03	04	5	
2	1	03	05	5	
2	1	03	06	5	
2	1	03	07	5	
2	1	03	08	5	
2	2	03	01	5	
2	2	03	02	5	

Table 94
eIO_DO sample data (Part 2 of 2)

2	2	03	03	5	
2	2	03	04	5	
2	2	03	05	5	
2	2	03	06	5	
2	2	03	07	5	
2	2	03	08	5	

Table: eKERNEL_AREA

Table 95
eKERNEL_area parameters

Name	*Type*	*Size*
AREA_Site_id_n	Integer	2
AREA_Area_id_n	Integer	2
AREA_Area_Descr_str	Text	50
AREA_Area_Comments_str	Text	255

AREA_Site_id_n

This field refers to the site identifier, as defined in the eKERNEL_SITE table. In most cases only one site is configured. A typical value is 1.

An example of an entry typically found in this field is as follows: 1

AREA_Area_id_n

This field indicates the area identifier. The combination site and area must be unique in the database.

In most cases the configuration consists of 1 site and 1 area. As explained in the eKERNEL_SITE table, the term site is referred to an environment that is handled by one single eKERNEL instance.

The concept of area is introduced in DECT Messenger in release 2. Prior to this release, there were a number of constraints, for example there could only be one instance be defined for several modules. This limitation affected both input programs and output programs.

With the introduction of the area concept, a site can now cover several divisions. These divisions can be geographically distributed to multiple locations, or they can all be in the same location.

One advantage of the area concept is that some configuration limitations are no longer active. For instance, you can now define multiple instances of both input programs and output programs. For example, an immediate result is the ability to support two or more eIO modules, with the immediate advantage that analogue input and discrete input modules can now be installed in a distributed location (near the contacts).

The most significant focus is however on output program level. With the area concept, you can now configure, for example, more than one instance of eDMSAPI. This is most useful in larger environments (for example, 3 high-range iS-3090 switches covering 3 locations in an IMP network), where you can now install one eDMSAPI per area (location). Because communication to the central eKERNEL (one per site) is now on sockets basis on the WAN, this dramatically reduces IMP network traffic, because calls can be processed locally on each location.

As a result of this design, the area field is found in many other tables. Peripherals (better known as devices) are now identified by site, area, output program and device.

An example of an entry typically found in this field is as follows: 1

AREA_Area_Descr_str

This field allows you to enter a small description of the area. This description is for instance visualized on several windows on the eWEB interface.

An example of an entry typically found in this field is as follows: Campus Sint-Jan

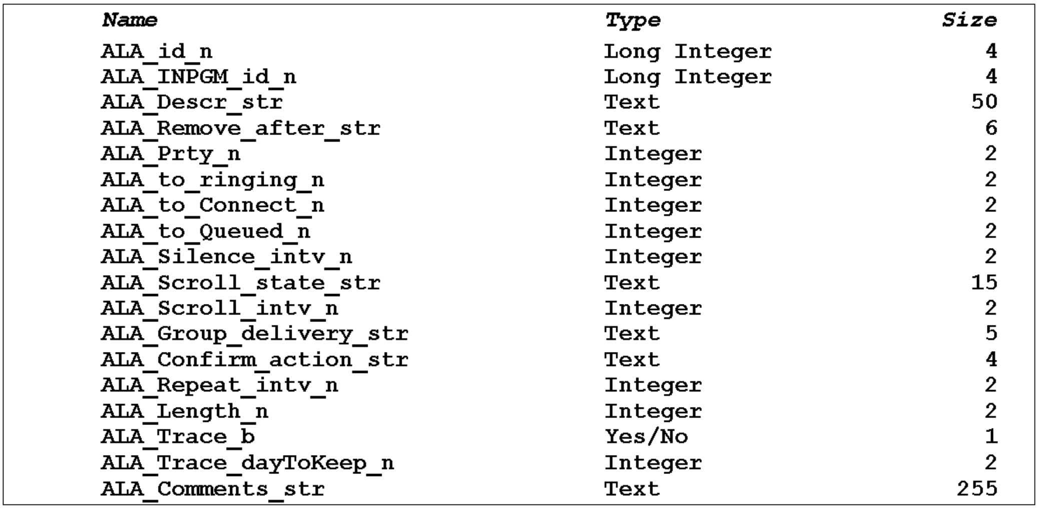
AREA_Area_Comments_str

This field can be used to add some additional comments and is informational only.

An example of an entry typically found in this field is as follows: Main area with iS-3090 switch

Table: eKERNEL_ALARM

Table 96
eKERNEL_alarm parameters



Name	*Type*	*Size*
ALA_id_n	Long Integer	4
ALA_INPGM_id_n	Long Integer	4
ALA_Descr_str	Text	50
ALA_Remove_after_str	Text	6
ALA_Prty_n	Integer	2
ALA_to_ringing_n	Integer	2
ALA_to_Connect_n	Integer	2
ALA_to_Queued_n	Integer	2
ALA_Silence_intv_n	Integer	2
ALA_Scroll_state_str	Text	15
ALA_Scroll_intv_n	Integer	2
ALA_Group_delivery_str	Text	5
ALA_Confirm_action_str	Text	4
ALA_Repeat_intv_n	Integer	2
ALA_Length_n	Integer	2
ALA_Trace_b	Yes/No	1
ALA_Trace_dayToKeep_n	Integer	2
ALA_Comments_str	Text	255

ALA_id_n

This field specifies the unique identifier of the alarm. Although you can to enter a numeric value of choice, Nortel recommends developing a logical naming convention for alarms.

A common approach is to base the numbering scheme upon input program identifier (that in turn is built upon site and area of the input program and a input program sequence number). A two-byte sequence number is the appended. This brings the length to seven bytes.

Table 97
Alarm identifiers

Byte 1	Site identifier		
Byte 2	Area identifier		
Byte 3-5	Input program identifier		
	Byte 3	1	eCAP or eAPI or eESPA
		6	eIO
		7	eWEB
		8	eSMTP_server
		9	eDMSAPI
	Byte 4-5	01-99	Input program sequence number
Byte 6-7	Alarm sequence number		

As shown in Figure 97, the first bytes denote the site identifier. The second byte denotes the area identifier. The third byte denotes the input application type. The fourth and fifth byte indicates a sequence number. These five first bytes refer to the input-program identifier.

The two remaining bytes (byte 6 and 7) are a sequence number that specified the alarm for that input program.

The first five digits match the value of the field ALA_INPGM_id_n. This helps to keep track of alarms in the complex definitions that occur in some configurations.

An example of an entry typically found in this field is as follows: 1110101 (denotes site 1, area 1, eCAP 01, alarm 01)

ALA_INPGM_id_n

This field specifies the unique identifier of the input program.

Note that this identifier is defined in the eKERNEL_TCPCLIENT table (field TCPCLIENT_INPGM_id_n). Refer to the section of eKERNEL_TCPCLIENT on how to set up these input programs.

Nortel recommends that you develop a naming convention to assign values for these identifiers.

Table 98
Alarm input program identifiers

Byte 1	Site identifier				
Byte 2	Area identifier				
Byte 3-5	Input program identifier				
	Byte 3	1	eCAP or eAPI or eESPA		
		6	eIO		
		7	eWEB		
		8	eSMTP_server		
		9	eDMSAPI		
	Byte 4-5	01-9 9	Input program sequence number		

Nortel recommends using five digits to uniquely identify an input program. With the guidelines above, the identifier implies the site, area, input program application and sequence number.

The ALA_id_n and ALA_INPGM_id_n both form a unique key, thus one input program with ALA_INPGM_id_n value 11101 cannot have two records with the same ALA_id_n value 1110101.

An example of an entry typically found in this field is as follows: 11101

ALA_Descr_str

This field is a very important parameter in the DECT Messenger alarm handling.

IMPORTANT!

Do not confuse this value with the ALA_Comments_str field for giving a description to the alarm.

The ALA_Descr_str contains a string of one or more characters. The eCAP alarm capture programs use these characters to find an appropriate alarm definition for a received alarm string.

The proper usage of this field is highly depending on the proprietary protocol implementation in eCAP and other input programs, such as eWEB. In many cases, some rules are defined for handling alarms from external systems.

The alarm generates some kind of string with information, and DECT Messenger must find out how to handle the string. The retrieval of the alarm definition from the eKERNEL_ALARM table is performed using the ALA_Descr_str field.

A special value *OTHER can be defined. If specified, the *OTHER description is used to handle alarms that were not identified by a qualified description.

Alarms with descriptions that do not either match a qualified description or the value *OTHER, are ignored.

Refer to other reference material for detailed instructions for each alarm system. The following examples are provided to clarify the usage:

Example 1: ELDAD

If the alarm is described as ELDAD, alarms are sent where behaviour depends on a tone code. Alarms with tone code 1, 2, 3 and 4 each have different characteristics, and need different alarm handling. In the case of ELDAD define the ALA_Descr_str values 1, 2, 3 and 4 for the 4 corresponding records.

Example 2: TELEVIC

TELEVIC sends alarms where behaviour depends on tone code or message contents.

If the alarm is described as TELEVIC, the system looks first for a string pattern (first blank or first xx characters as specified in the L:xx description of the INPGM_Model_str field of the eKERNEL_INPGM table (PROTOCOL CONVERTOR – L:03). If no length (L:xx) is specified, the default value is 3. Characters of message or search until first blank character: NUR, SAN, ASS, REA, MUG, and so on.

See documentation Table eKERNEL_inpgm.pdf.

If no such definition is found; the system looks for a matching tone code pattern (for example, 0, 1, 2, 3, 4, 5, 6, 7, 8, 9 or 0).

If again no definition is found, the system looks for an *OTHER definition.

Example 3 - National Instruments

The National Instruments distributed I/O modules FP-DI-300, FP-DI-301 and FP-DI-330 generate discrete input alarms, the I/O module FP-AI-100 generates analogue input alarms. Both modules are configured in eIO_MODULE, eIO_AI and eIO_DI tables. In the latter two files the alarm type can be defined, default is D-INPUT and A-INPUT. If these defaults are used, ALA_Descr_id_str must have records for D-INPUT and A-INPUT.

Example 4 – Guarding

A special feature in the eCAP input program consists of a method to verify the amount of time between two requests. If a specific type has elapsed, this can be caused by a failure in the external alarm system or the physical interface. In such case, GUARDING can be implemented. This is configured in the eKERNEL_GUARDING table. The link between eKERNEL_GUARDING and eKERNEL_ALARM is performed through an alarm identifier, but Nortel recommends specifying GUARDING in the alarm description field.

An example of an entry typically found in this field is as follows:
GUARDING

ALA_Remove_after_str

This field can have the value *SENT or *RESET.

If the field value is ***SENT**, the message is removed after successfully sending the message.

If the field value is ***RESET**, the message remains in the database until an explicit reset signal is received from the alarm system.

Again, this value is generally depending of the proprietary implementation of the alarm system and the attached peripherals. Some devices can send a SET and RESET indication (for example, a switch button van be set to on or off); others cannot generate a RESET (for example, a push button can only generate a push signal while pressing the contact).

In some cases you can have difficulty determining whether alarms have reset or not. In fact, some third-party alarm system vendors are not aware of the signals provided. In these cases, you must specify *SENT, to prevent alarms that do not receive a *RESET from remaining active in the system.

An example of an entry typically found in this field is as follows: *SENT

ALA_Prty_n

This field specifies the priority of an alarm. A low value indicates an important alarm, a high value a less important alarm. Nortel recommends that you exercise caution when assigning priorities to alarms. For some output devices, high-important alarms are shown first and low-priority alarms are shown last.

Other output programs (such as eSMTP and eASYNC) allow you to automatically confirm arrival of messages when distributed, while others require confirmation procedures based upon a call back procedure.

Nortel recommends that you begin by assigning all alarms to default priority 5 (for example, nurse calls, and so on) and assigning more important alarms to a lower value (1 for MUG, 2 for REA, 3 for ASS, and so on) and less important alarms to a higher value (6 for SAN, and so on). In most cases, alarm priorities are subject to discussion with those in authority on-site.

An example of an entry typically found in this field is as follows: 5

ALA_to_ringing_n

This field specifies the number of seconds a peripheral is kept in ringing state before taking further action. This parameter is ignored for most peripherals.

An example of an entry typically found in this field is as follows: 20

ALA_to_Connect_n

This field specifies the number of seconds a peripheral is kept in connect state before taking further action. This parameter is ignored for all peripherals and is provided for backwards compatibility issues.

An example of an entry typically found in this field is as follows: 10

ALA_to_Queued_n

This field specifies the number of seconds a peripheral is kept in camp-on-busy state before taking further action. This parameter is ignored for all peripherals and is provided for backwards compatibility issues.

An example of an entry typically found in this field is as follows: 15

ALA_Silence_intv_n

This field specifies the number of seconds a peripheral is left quiet (idle) before repeating any outstanding messages (also referred to as pace interval).

In many cases DECT users want to have a pace interval greater than zero, so that repeated messages do not pose an interruption. Therefore the DECT Messenger keeps track of all active alarms, stores them in an internal database, and distributes them as the image of active alarms for a device is changing.

When no changes occur, the remaining alarms are repeated every ALA_Silence_intv_n specified number of seconds.

When a new alarm is generated and the image changes, the user is informed immediately.

On the other hand, when no changes occur, the outstanding messages are repeated at the specified interval.

An example of an entry typically found in this field is as follows: 120 (denotes 2 minutes)

ALA_Scroll_state_str

This field specifies the state in which a device must be to receive messages. Valid values are *CONNECT and *RINGING.

Scrolling starts at connect event when *CONNECT is specified, and starts at ringing event when *RINGING is specified.

This parameter is however, due to architectural reasons, currently ignored for most peripherals.

An example of an entry typically found in this field is as follows: *CONNECT

ALA_Scroll_intv_n

This field specifies the number of seconds that is used as scroll interval, when peripherals allow scrolling. This parameter is, due to architectural reasons, ignored for most peripherals and is provided for backwards compatibility issues.

An example of an entry typically found in this field is as follows: 3

ALA_Group_delivery_str

This value defines the degree of message delivery that is required on delivery of a message to a group. Values can be *ALL or *ANY and is only relevant if the field ALA_Remove_after_str is set to *SENT.

If the field ALA_Repeat_intv_n is set (value is greater than 0), than this field is only relevant if ALA_Confirm_action_str is set to *YES.

If the field value is *ALL, each individual recipient handles their messages on individual basis.

If the field value is *ANY, the message is only distributed to (at least) one group member. When the first user confirms, the message is considered delivered. This can result in removal of the message for all group members. This can mean some group members do not see the message at all.

An example of an entry typically found in this field is as follows: *ALL

ALA_Confirm_action_str

This value defines the confirm action. Valid entries are YES or NO.

If *NO is specified, message delivery confirmation is not required.

If of *YES, message delivery confirmation is mandatory.

This parameter is related to the ALA_Group_delivery_str parameter specified above.

Note that confirm delivery depends on a number of criteria, for example, alarm priority can have impact in defining whether an alarm required confirmation or not. Some other peripherals provide intrinsic message delivery (sending a normal E2 message through DMS-API) while others require use intervention (sending an urgent E2 message through DMS-API required user acknowledge). In some circumstances, special procedures apply to the confirmation action. This is defined in the corresponding eASYNC table and eSMTP table.

An example of an entry typically found in this field is as follows: *NO

ALA_Repeat_intv_n

This value defines the number of seconds between repeating alarm. Be careful not to confuse this entry with ALA_Silence_intv_n discussed above.

The ALA_Repeat_intv_n is in most cases 0, meaning the alarm system does not repeat active alarms. ALA_Repeat_intv_n is kept to 0 in situations where the alarm systems can set a SET and RESET, or when the alarm system sends an alarm once at SET.

The ALA_Repeat_intv_n is set to a value larger than 0 if the alarm system is incapable of sending a RESET indication, and repeats active alarms on frequent basis. When the appropriate alarms are no longer repeated, the situation is interpreted as a RESET condition. You can use this option to provide a steady repeat interval (for example, active alarms are repeated every 20 seconds) and a continuously repetition (repeat is not stopped after 10 repeats). When repeat interval is known, you can add a small safety factor (for example, add 5 to 10 seconds) and define the ALA_Repeat_intv_n as such.

An example of an entry typically found in this field is as follows: 0

ALA_Length_n

This field specifies the length of the alarm that is considered as relevant. Nortel recommends that you set the length to correspond to the length of the received alarm signal, although this is not always necessary. You can just as easily change messages in the alarm systems, so the length fits your environment and peripherals.

For instance, if you keep message length to 16 bytes or less, the messages fit on a single line on a DECT C4040 or DECT C4050 extension. This demand can result is instructions to the alarm vendor to properly align relevant information in the received alarm messages, so all needed text is left-adjusted and processed in DECT Messenger.

In some environments, longer messages are relevant. In such cases, you can specify, for example, message lengths of 100 bytes, if input comes from, for example, WEB interface and output goes to peripherals that are capable of handling long messages (eSMTP, eASYNC, and so on).

An example of an entry typically found in this field is as follows: 16

ALA_Trace_b

This parameter is a Boolean value and can be either True (-1) or False (0).

Specify the value True only for those alarms that are related to eWEB input program and generated using the Send Script Message function. These alarms are defined in the eWEB_SCRIPT table.

For all other alarms, set this value to False.

An example of an entry typically found in this field is as follows: False (-1)

ALA_Trace_dayToKeep_n

This value also refers to the trace function described in the ALA_Trace_b field.

Set this value to 0, unless the value ALA_Trace_b is set to True (-1). In this case, tracing is activated for the alarm, and the number of days to keep the trace data must be entered. A typical value is 14 days.

For all other alarms, set this value to 0.

An example of an entry typically found in this field is as follows: 0

ALA_Comments_str

This field can optionally be used by an administrator to store reminder information, describing, for example, the usage of the alarm.

An example of an entry typically found in this field is as follows: Reanimation through TELEVIC.

Table 99 on page 1404 provides sample eKERNEL_alarm module table data.

Table 99
eKERNEL_alarm sample data (Part 1 of 3)

Alarm	Inpgm	Descr	Remove after	Priority	...
1110101	11101	0	*SENT	3	...
1110102	11101	1	*SENT	1	...
1110103	11101	2	*RESET	2	...
1110104	11101	3	*SENT	3	...
1110105	11101	GUARDING	*SENT	10	...
1110201	11102	NUR	*SENT	10	...
1110202	11102	NUR	*RESET	10	...
1110203	11102	ASS	*SENT	7	...
1110204	11102	ASS	*RESET	7	...
1110205	11102	SAN	*SENT	10	...
1110206	11102	SAN	*RESET	10	...
1110207	11102	REA	*SENT	1	...
1110208	11102	REA	*RESET	1	...
1110209	11102	1	*RESET	10	...
1110210	11102	1	*SENT	10	...
1110211	11102	*OTHER	*RESET	20	...
1110212	11102	*OTHER	*SENT	20	...
1110213	11102	GUARDING	*SENT	10	...
1110301	11103	API SENT	*SENT	10	...
1110302	11103	API RESET	*RESET	10	...
1110401	11104	GENERIC	*SENT	10	...
1110501	11105	1	*SENT	10	...

Table 99
eKERNEL_alarm sample data (Part 2 of 3)

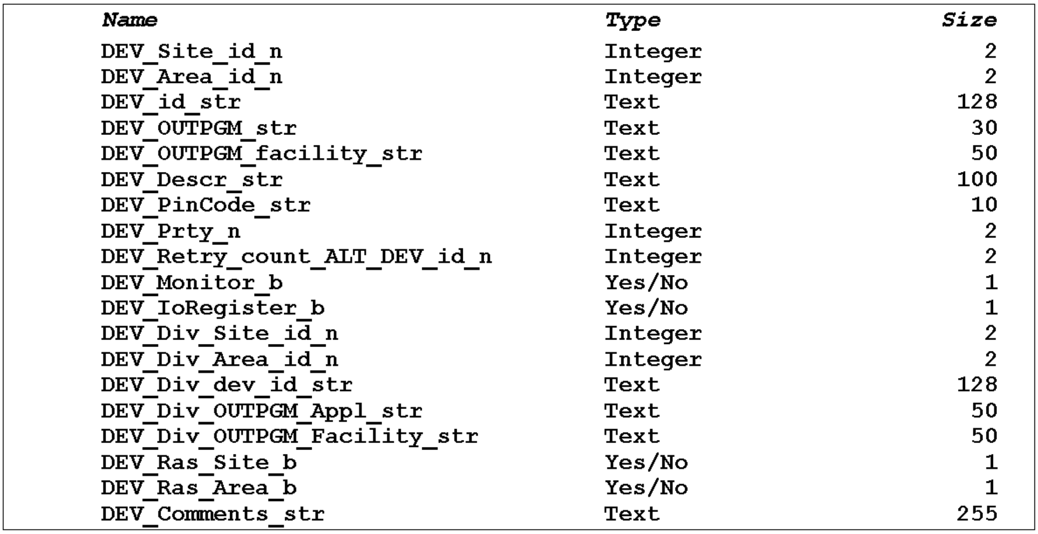
1110502	11105	2	*SENT	2	...
1140101	11401	EVACUATION	*RESET	2	...
1140102	11401	FIRE	*SENT	5	...
1140103	11401	TEST	*SENT	20	...
1150101	11501	REA	*SENT	999	...
1150102	11501	MUG	*SENT	999	...
1160101	11601	A-INPUT	*RESET	999	...
1160102	11601	A-INPUT	*SENT	999	...
1160103	11601	D-INPUT	*RESET	999	...
1160104	11601	D-INPUT	*SENT	999	...
1170101	11701	Short	*SENT	1	...
1170102	11701	Medium	*SENT	999	...
1170103	11701	Long	*SENT	999	...
1170104	11701	SCRIPT Message	*SENT	1	...
1170105	11701	SCRIPT Message	*RESET	1	...
1170106	11701	Short script	*SENT	10	...
1170107	11701	Medium script	*SENT	10	...
1170108	11701	Long script	*SENT	10	...
1180101	11801	SMTP	*SENT	10	...
1190101	11901	E2_MSG_N	*SENT	10	...
1190102	11901	E2_MSG_U	*SENT	2	...
1190103	11901	E2_NOODOPROEP	*SENT	1	...
1190104	11901	E2_REANIMATIE	*SENT	1	...

Table 99
eKERNEL_alarm sample data (Part 3 of 3)

1190105	11901	E2_TEST_N	*SENT	5	...
1190106	11901	E2_TEST_U	*SENT	2	...
1210501	12105	1	*SENT	10	...
1210502	12105	2	*SENT	999	...
1210503	12105	3	*SENT	5	...
1310501	13105	1	*SENT	999	...
1310502	13105	2^9	*RESET	2	...
1310503	13105	NUR	*SENT	10	...
1310504	13105	NUR	*RESET	10	...

Table: eKERNEL_DEVICE

eKERNEL_DEVICE parameters



Name	*Type*	*Size*
DEV_Site_id_n	Integer	2
DEV_Area_id_n	Integer	2
DEV_id_str	Text	128
DEV_OUTPGM_str	Text	30
DEV_OUTPGM_facility_str	Text	50
DEV_Descr_str	Text	100
DEV_PinCode_str	Text	10
DEV_Prty_n	Integer	2
DEV_Retry_count_ALT_DEV_id_n	Integer	2
DEV_Monitor_b	Yes/No	1
DEV_IoRegister_b	Yes/No	1
DEV_Div_Site_id_n	Integer	2
DEV_Div_Area_id_n	Integer	2
DEV_Div_dev_id_str	Text	128
DEV_Div_OUTPGM_Appl_str	Text	50
DEV_Div_OUTPGM_Facility_str	Text	50
DEV_Ras_Site_b	Yes/No	1
DEV_Ras_Area_b	Yes/No	1
DEV_Comments_str	Text	255

DEV_site_id_n

This field refers to the site as specified in eKERNEL_SITE table. Usually this field has value 1. In most environments, this value is 1.

An example of an entry typically found in this field is as follows: 1

DEV_Area_id_n

This field refers to the area identifier, as defined in the eKERNEL_AREA table. In most environments, this value is 1.

An example of an entry typically found in this field is as follows: 1

DEV_id_str

This field contains a reference to the destination device as known in our internal infrastructure. When a device is, for instance, a DECT extension, this field specifies the extension number (for example, 865). When a mail destination is defined, this field contains a mail address (for example, francis.missiaen@1s.be). As such the next field GRP_OUTPGM_Appl_str further identifies the device for a specific site and area.

GRP_Dev_id_str, GRP_OUTPGM_Appl_str, DEV_Site_id_n and DEV_Area_id_n must be handled to uniquely identify a device.

An example of an entry typically found in this field is as follows: 1 – 1 – 865 – eDMSAPI or 1 – 2 – francis.missiaen@1s.be - eSMTP

DEV_OUTPGM_str

This field identifies the application that processes the request.

A device can be defined more than once. The indicated application handles the message using the capabilities of the infrastructure. eDMSAPI can for instance send E2 data profile messages (non-voice-call to extensions such as DECT C4040 and C4050). The supported values are currently:

- eASYNC

  for sending SMS to PROXIMUS or KPN and PAGING to BELGACOM

- eDMSAPI

  for sending E2 messages

- eESPA

  for sending messages to ESPA 4.4.4 interface

- eIO

  for enabling/disabling discrete output contacts

- eSMTP

  for sending mail to SMTP-compliant infrastructure

- eESPA

  for sending messages to ESPA infrastructure

DEV_OUTPGM_facility_str

The indicated application handles the message using the capabilities of the infrastructure.

The supported values are specified in the field FMT_OUTPGM_Facility_str of the eKERNEL_DEVICE_FORMAT table for the corresponding output program.

An example of an entry typically found in this field is as follows: C4050 for eDMSAPI

DEV_Descr_str

This field can be used to enter a description of the device.

This description is used to shown information of devices in the eWeb module.

An example of an entry typically found in this field is as follows: DECT: Kristien Daneels

DEV_PinCode_str

The pincode is used when messages sent to, for example, a GSM or a pager must be confirmed. for example, 12345.

DEV_Prty_n

This field is currently not implemented, but is foreseen for future enhancements.

DEV_Retry_count_ALT_DEV_id_n

This field is implemented in a different fashion after eKERNEL version 2.10:

- Before eKERNEL Version 2.1.0:

  The number of retries before switching to an alternative device, if device (site + area + device + output program is unique) is defined in the eKERNEL_device_alt table.

  The default value is 30, which means that if an alarm has a silence interval of for instance 120 seconds; the alarm is removed for this device after one hour (and set for the alternative device if defined).

  For example, 1 => after the second retry, the alternative devices is set.

- eKERNEL Version 2.1.1 and later:

  This keyword defines how many times the application tries to deliver the message before switching to an alternative device if defined in the eKERNEL_device_alt table.

  The default value is 30, which means that if an alarm has a silence interval of for instance 120 seconds; the alarm is removed for this device after one hour (and set for the alternative device if defined).

  The value = 0 means 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 (ALA_Silence_intv_n in eKERNEL_Alarm) until the alarm is reset by, for example, the input program.

  The value = 1 means that after 1 try, the application clears the message for this device, and sends the message to the alternative device if defined in the eKERNEL_Device_alt table.

IMPORTANT!

In this case, the switch to the alternative device is immediate, which means that there is no silence interval between those two calls. Therefore, be very careful that there are no loop conditions defined in the eKERNEL_device_alt table.

The value = 2 means that after the second try, the alternative device is contacted.

For example, 2 => after 2 times trying to send the message, the alternative devices is set.

DEV_Monitor_b

An example of an entry typically found in this field is as follows: False (-1).

DEV_IoRegister_b

All the devices with value equal to True (-1) are sent to the eDMSAPI application and are able to send messages from the device to EDP (DECT Messenger).

The eDMSAPI module requests registration (IoRegisterRequest) of this devices.

This parameter is only relevant when the field DEV_OUTPGM_str is equal to eDMSAPI.

When a DECT that is IoRegistered sends a message, the message is no longer sent to the PBX but to the EDP.

Messages sent to EDP are not forwarded to the specified destination device by the eDMSAPI module, but are sent to the eKERNEL application. If the destination must receive the message, the destination device must be specified in the eKERNEL_group (field GRP_Descr_str) and defined as a member in the eKERNEL_group_member table.

An example of an entry typically found in this field is as follows: -1

DEV_Div_Site_id_n

This field specifies the site of the diverted device.

When a device is diverted to another device, the system ignores the divert in cases where the destination device is not configured in the eKERNEL_DEVICE table. When more than one device is defined the eDMSAPI device type is selected, and the corresponding site is entered in this field. If no eDMSAPI capable device is defined, the first available matching device is used, and the corresponding site is entered in this field.

An example of an entry typically found in this field is as follows: 1

DEV_Div_Area_id_n

This field specifies the area of the diverted device.

See DEV_Div_Site_id_n

An example of an entry typically found in this field is as follows: 1

DEV_Div_OUTPGM_Appl_str

This field specifies the output program of the diverted device.

See DEV_Div_Site_id_n

An example of an entry typically found in this field is as follows: 1

DEV_Div_OUTPGM_Facility_str

This field specifies the output program of the diverted device.

See DEV_Div_Site_id_n

An example of an entry typically found in this field is as follows: eDMSAPI

DEV_Ras_Site_b

This field is currently not implemented, but is reserved for future enhancements when multisite facilities are implemented.

In future versions, eKERNEL-to-eKERNEL communications will be implemented, so alarms for devices located on another site can be sent to the remote eKenel.

An example of an entry typically found in this field is as follows: False (0)

DEV_Ras_Area_b

This field specifies the behaviour of the eWEB-based function Send DMS-API Message. The Send DMS-API message default only presents those devices that are defined in the eKERNEL_DEVICE table, and have output program eDMSAPI and reside on the same site and area as the eWEB input program. For example, if the eWEB application is defined on site 1 and area 1, the Send DMS-API Message presents the eDMSAPI devices of site 1 area 1.

Some multi-area environments require that you present devices that are configured for a remote area. You can select for each device whether the remote device is available to the local eWEB area or not.

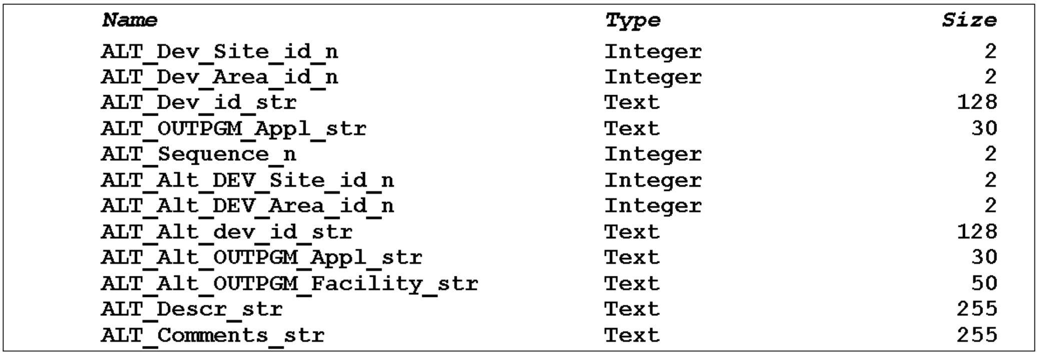
An example of an entry typically found in this field is as follows: False (0)

DEV_Comments_str

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

Table: eKERNEL_DEVICE_ALT

Table 100
eKERNEL_DEVICE_ALT parameters



Name	*Type*	*Size*
ALT_Dev_Site_id_n	Integer	2
ALT_Dev_Area_id_n	Integer	2
ALT_Dev_id_str	Text	128
ALT_OUTPGM_Appl_str	Text	30
ALT_Sequence_n	Integer	2
ALT_Alt_DEV_Site_id_n	Integer	2
ALT_Alt_DEV_Area_id_n	Integer	2
ALT_Alt_dev_id_str	Text	128
ALT_Alt_OUTPGM_Appl_str	Text	30
ALT_Alt_OUTPGM_Facility_str	Text	50
ALT_Descr_str	Text	255
ALT_Comments_str	Text	255

ALT_Dev_Site_id_n

This field refers to the site as specified in eKERNEL_SITE table. Usually this field has value 1. In most environments, this value is 1.

An example of an entry typically found in this field is as follows: 1

ALT_Dev_Area_id_n

This field refers to the area identifier, as defined in the eKERNEL_AREA table. In most environments, this value is 1.

An example of an entry typically found in this field is as follows: 1

ALT_Dev_id_str

This field defines – in combination with ALT_Dev_Site_id_n, ALT_Dev_Area_id_n and ALT_OUTPGM_Appl_str – a device in the system. The record specifies one or more alternate devices that are to be used in case an unrecoverable error occurs when sending a message to a specified device. In case of a failure, a list of alternate devices can be processed upon successful message delivery.

Define the device (site, area, device and outpgm) as a valid device in eKERNEL_DEVICE table.

An example of an entry typically found in this field is as follows: 865

ALT_OUTPGM_Appl_str

The field is associated with the previous field and defines the device.

An example of an entry typically found in this field is as follows: eDMSAPI

ALT_Sequence_n

This field is a sequence number to make a record definitions in eKERNEL_DEVICE_ALT unique. Nortel recommends starting with a value of 1 and incrementing by 1s.

An example of an entry typically found in this field is as follows: 1

ALT_Alt_DEV_Site_id_n

This field defines, in combination with ALT_Alt_DEV_area_id_, ALT_Alt_dev_id_str, ALT_Alt_OUTPGM_Appl_str and ALT_Alt_OUTPGM_Facility_str the alternate device.

An example of an entry typically found in this field is as follows: 1

ALT_Alt_DEV_area_id_n

This field defines, in combination with ALT_Alt_DEV_site_id_, ALT_Alt_dev_id_str, ALT_Alt_OUTPGM_Appl_str and ALT_Alt_OUTPGM_Facility_str the alternate device.

An example of an entry typically found in this field is as follows: 1

ALT_Alt_dev_id_str

This field defines, in combination with ALT_Alt_DEV_Site_id_n, ALT_Alt_DEV_area_id_, ALT_Alt_OUTPGM_Appl_str and ALT_Alt_OUTPGM_Facility_str the alternate device.

Check for possible loop conditions when setting up this table.

An example of an entry typically found in this field is as follows: 865

ALT_Alt_OUTPGM_Appl_str

This field defines, in combination with ALT_Alt_DEV_Site_id_n, ALT_Alt_DEV_area_id_, ALT_Alt_dev_id_str and ALT_Alt_OUTPGM_Facility_str the alternate device.

Check for possible loop conditions when setting up this table.

An example of an entry typically found in this field is as follows: eDMSAPI

ALT_Alt_OUTPGM_Facility_str

This field defines, in combination with ALT_Alt_DEV_Site_id_n, ALT_Alt_DEV_area_id_, ALT_Alt_dev_id_str and ALT_Alt_OUTPGM_Appl_str the alternate device.

Check for possible loop conditions when setting up this table.

An example of an entry typically found in this field is as follows: C4050

ALT_descr_str

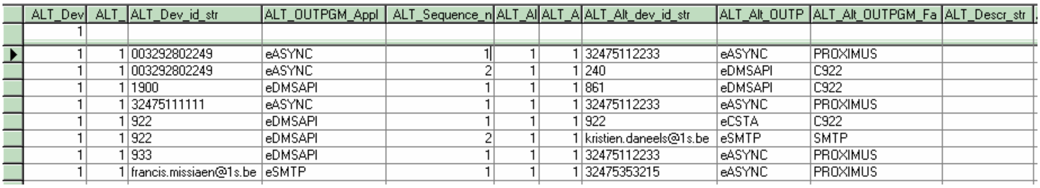
This informational field can contain some remarks (informational only)

ALT_Comments_str

This field is used for an administrator to add remarks and is used informational only.

Table 101 on page 1418 provides sample eKERNEL_DEVICE_ALT table data.

Table 101
eKERNEL_DEVICE_ALT parameters



ALT_Dev	ALT_	ALT_Dev_id_str	ALT_OUTPGM_Appl	ALT_Sequence_n	ALT_Al	ALT_A	ALT_Alt_dev_id_str	ALT_Alt_OUTP	ALT_Alt_OUTPGM_Fa	ALT_Descr_str
1										
1	1	003292802249	eASYNC	1	1	1	32475112233	eASYNC	PROXIMUS	
1	1	003292802249	eASYNC	2	1	1	240	eDMSAPI	C922	
1	1	1900	eDMSAPI	1	1	1	861	eDMSAPI	C922	
1	1	32475111111	eASYNC	1	1	1	32475112233	eASYNC	PROXIMUS	
1	1	922	eDMSAPI	1	1	1	922	eCSTA	C922	
1	1	922	eDMSAPI	2	1	1	kristien.daneels@1s.be	eSMTP	SMTP	
1	1	933	eDMSAPI	1	1	1	32475112233	eASYNC	PROXIMUS	
1	1	francis.missiaen@1s.be	eSMTP	1	1	1	32475353215	eASYNC	PROXIMUS	

Table: eKERNEL_DEVICE_FORMAT

Table 102
eKERNEL_DEVICE_FORMAT parameters

Name	Type	Size
FMT_OUTPGM_Appl_str	Text	30
FMT_OUTPGM_Facility_str	Text	50
FMT_Bytes_line1_n	Integer	2
FMT_Bytes_line2_n	Integer	2
FMT_Bytes_line3_n	Integer	2
FMT_Page_ind_n	Integer	2
FMT_Page_more_ind_n	Integer	2
FMT_Concatination_b	Yes/No	1
FMT_Scroll_depth_n	Integer	2
FMT_AllowEmergency_b	Yes/No	1
FMT_Descr_str	Text	250
FMT_Comments_str	Text	255

FMT_OUTPGM_Appl_str

This field identifies the output program. The following options are supported: eASYNC, eDMSAPI, eIO, eSMTP.

An example of an entry typically found in this field is as follows: eDMSAPI

FMT_OUTPGM_Facility_str

This field specifies the supported facility or facilities for a specified output program. See Table 103 for supported entries. The administrator can create new facilities.

Table 103
Application-Facility associations (Part 1 of 2)

Application	Facility
eASYNC	PAGING

Table 103
Application-Facility associations (Part 2 of 2)

eASYNC	PROXIMUS
eDMSAPI	C4040
eDMSAPI	C4050
eIO	DO
eSMTP	SMTP
eESPA	ESPA

FMT_Bytes_line1_n

This field specifies the number of bytes available on the first line. In general, the maximum length is to be used. Refer to the sample data in Table 106 on page 1423 for examples.

An example of an entry typically found in this field is as follows: 16

FMT_Bytes_line2_n

This field specifies the number of bytes available on the second line. In general, this value is 0 for devices with no second line and the maximum length, in case a second line is available. If only two lines are available, a smaller number of bytes is appropriate to reserve room for page indication and so on. Refer to the sample data in Table 106 on page 1423 for examples.

An example of an entry typically found in this field is as follows: 16

FMT_Bytes_line3_n

This field specifies the number of bytes available on the third line. In general, the value is smaller than the actual available size to reserve room for page indication and more indication.

When a customer has infrastructure with extensions capable of displaying three lines of 16 bytes, alarm lengths up to 48 bytes can be displayed (without page indication and more indication). In most cases, Nortel recommends that you reserve the third line for page indication and more indication, thus specifying 0 for the third line.

An example of an entry typically found in this field is as follows: 0

FMT_Page_ind_n

This field specifies the number of bytes reserved for page indication. Recommended value is five bytes, which allows the XX/XX syntax. A lower number of characters can be used if space is limited. See Table 104 for example values.

Table 104
Page identification syntax

0	(no page indication)
1	+
2	+
3	X/X
4	X/X
5	XX/XX
6	XX/XX

Note: This value is only implemented on the eDMSAPI output program.

An example of an entry typically found in this field is as follows: 5

FMT_Page_more_ind_n

This field specifies the number of bytes reserved for more indication. Recommended value is 2 bytes, which allows a + syntax. A lower number of characters can be used in space is limited. See Table 105 for example values.

Table 105
More indication syntax

0	(no more indication)
1	+
2	+

Note: This value is only implemented on eDMSAPI output program.

An example of an entry typically found in this field is as follows: 2

FMT_Concatination_b

This field defines whether small messages that fit on one display are merged to one page. If, for example, a DECT C4050 extension is defined as 16/16/0/5/2 and messages are a maximum 16 bytes, you can show two messages on a single page.

Note: This value is only implemented on eDMSAPI output program.

An example of an entry typically found in this field is as follows: –1 (true)

FMT_Scroll_depth_n

This field specifies the maximum number of pages that is shown to a user. If scroll depth is 4 and there are seven pages available, the user is only informed on the first four pages. A **more** indication is shown to indicate more pages, unless this is suppressed.

An example of an entry typically found in this field is as follows: 4

FMT_AllowEmergency_b

This field is introduced in R3.0 and defines whether the peripheral supports Emergency LRMS Messaging. Example, DECT C4060 devices. Sending an emergency message through eDMSAPI module to a peripheral that does not support this feature, resulting in a system malfunction. Administrators must carefully assign the device facility that enables emergency calls only to peripherals that support it. To prevent problems, the default equals false, so enabling emergency calls on supported devices is performed only on demand.

An example of an entry typically found in this field is as follows: 0 (false)

FMT_Descr_str

An administrator can enter a description of the template in this field. This value is informational only.

An example of an entry typically found in this field is as follows: template for C4050 extensions for nurse-calls

FMT_Comments_str

An administrator can enter remarks in this field. This value is informational only.

An example of an entry typically found in this field is as follows: two lines and indicators.

Table 106 provides sample eKERNEL_DEVICE_FORMAT table data.

Table 106
eKERNEL_DEVICE_FORMAT sample data

Application	Facility	Line 1	Line 2	Line 3	Page	More	Concat	Scroll depth
eASYNC	PAGING	160	0	0	5	2	0	999
eASYNC	PROXIMUS	120	0	0	0	0	0	999
eDMSAPI	C4040	16	16	0	5	2	-1	999
eDMSAPI	C4050	16	16	0	5	2	-1	999
eIO	DO	1024	0	0	0	0	0	999
eSMTP	SMTP	32	0	0	0	0	0	999
eESPA	ESPA	128	0	0	0	0	0	999

Table: eKERNEL_GROUP

Table 107
eKERNEL_GROUP parameters

Name	*Type*	*Size*
GRP_id_str	Text	128
GRP_InPGM_id_n	Long Integer	4
GRP_Name_str	Text	128
GRP_Descr_str	Text	50
GRP_Comments_str	Text	255

GRP_id_str

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

Nortel recommends defining group identifiers using the following naming convention:

Table 108
Recommended Group identifier naming convention (Part 1 of 2)

Byte 1-5	**Input program**	
	Byte 1	Site of input program
	Byte 2	Area of input program
	Byte 3	Input program type
		1 - eCAP or eAPI or eESPA
		6 - eIO

Table 108
Recommended Group identifier naming convention (Part 2 of 2)

		7 - eWEB
		8 - eSMTP_server
	Byte 4-5	Input program sequence number
Byte 6	(Underscore character)	
Byte 7-...	Group name	

Example: 31101_00001 denotes site 3, area 1, input program type eCAP or eAPI, input program sequence 01, group name 00001.

For each defined group, one or more group member must be defined in the eKERNEL_GROUP_MEMBER table.

You can assign authority to the groups by means of the eKERNEL_GROUP_AUTH table.

An example of an entry typically found in this field is as follows:
31101_00001

GRP_InPGM_id_n

As described above, group identifiers are uniquely defined by combining input program identifier and group name.

The input program is the value specified in the eKERNEL_INPGM table.

Nortel recommends following the naming convention set out in Table 109.

Table 109
Recommended Group identifier naming convention (Part 1 of 2)

Byte 1-5	**Input program**	
	Byte 1	Site of input program

Table 109
Recommended Group identifier naming convention (Part 2 of 2)

	Byte 2	Area of input program
	Byte 3	Input program type
		1 - eCAP or eAPI or eESPA
		6 - eIO
		7 - eWEB
		8 - eSMTP_server

Example: 31101 denotes site 3, area 1, input program type eCAP or eAPI and input program sequence 01.

An example of an entry typically found in this field is as follows: 31101

GRP_Name_str

As described above, group identifiers are uniquely defined by combining input program identifier and group name.

The input program is the value specified in the eKERNEL_INPGM table.

The group name field is the group indication that is typically received from the external alarm system. In many environments, alarm systems are capable of sending some kind of destination information in the alarm string. This can, for example, be referred to with terms such as paging number, group, or destination.

Note that the above-described design allows sharing the same group name between multiple input programs. A first eCAP instance can have a different understanding for group 00001 than a second eCAP instance. In most cases the group names are determined by third-party vendors, and in many environments cannot be changed.

With this approach, you can logically link any group name and assign our internally known group members (peripherals) to them.

An example of an entry typically found in this field is as follows: 00001

GRP_Descr_str

This field can have a descriptive text, to allow administrators to easily recognize the group.

An example of an entry typically found in this field is as follows: Intensive Care

GRP_Comments_str

This field can also contain additional information.

An example of an entry typically found in this field is as follows: “Warning: minimum 3 DECT extensions required”

Table 110 provides sample eKERNEL_GROUP table data.

Table 110
eKERNEL_GROUP sample data

Group id	Input program	Group name	Description	Comments
31101_00001	31101	00001	Test from eCAP	
31102_00001	31102	00001	Test from eCAP	
31102_24960	31102	24960	Test Televic	
31103_00001	31103	00001	Test from eAPI	
31601_00001	31601	00001	Test from eIO	
31701_eASYNC	31701	eASYNC	Test to eASYNC	
31701_eDMSAPI	31701	eDMSAPI	Test to eDMSAPI	
31701_eIO	31701	eIO	Test to eIO	
31701_eSMTP	31701	eSMTP	Test to eSMTP	
31801_00001	31801	00001	Test from eSMTP	

Table: eKERNEL_GROUP_AUTH

Table 111
eKERNEL_GROUP_AUTH parameters

Name	*Type*	*Size*
GRPA_GRP_id_str	Text	128
GRPA_UserID_str	Text	10
GRPA_Comments_str	Text	255

GRPA_GRP_id_str

This field refers to the unique group identifier, as described in the eKERNEL_GROUP table. Each group identifier must be defined in the eKERNEL_GROUP table. The member of each group identifier must be defined in the eKERNEL_GROUP_MEMBER table. At least one group member per group identifier must be defined, because empty groups result in loss of alarms.

The table eKERNEL_GROUP_AUTH allows an administrator to grant access to eWEB users. In eWEB, there is a group maintenance function: Work with Groups. User without all object authority in their eWEB_USER_AUTH table definition can see only those groups that are defined in the eKERNEL_GROUP_AUTH table.

A typical example is a hospital, where the person responsible for a department is allowed to maintain only their own departmental groups, and not the groups of other departments.

An example of an entry typically found in this field is as follows:
31101_00001

GRPA_UserID_str

This field specifies the username that is granted access to the group. This value must match the definition of the users in eWEB_USER_AUTH table.

A special value *ALL is implemented. If you specify this special value, all users have access to this group. With *ALL you do not need to enter all individual users, but as a result you have no granular authority definition because all users are granted access.

Note that eWEB only allows maintenance of the groups that are assigned to input programs of the same site as the eWEB. This means a eWEB instance of site 1 only allows maintenance of groups of site 1.

An example of an entry typically found in this field is as follows: FMI

GRPA_Comments_str

This field can contain remarks of an administrator, and is informational only.

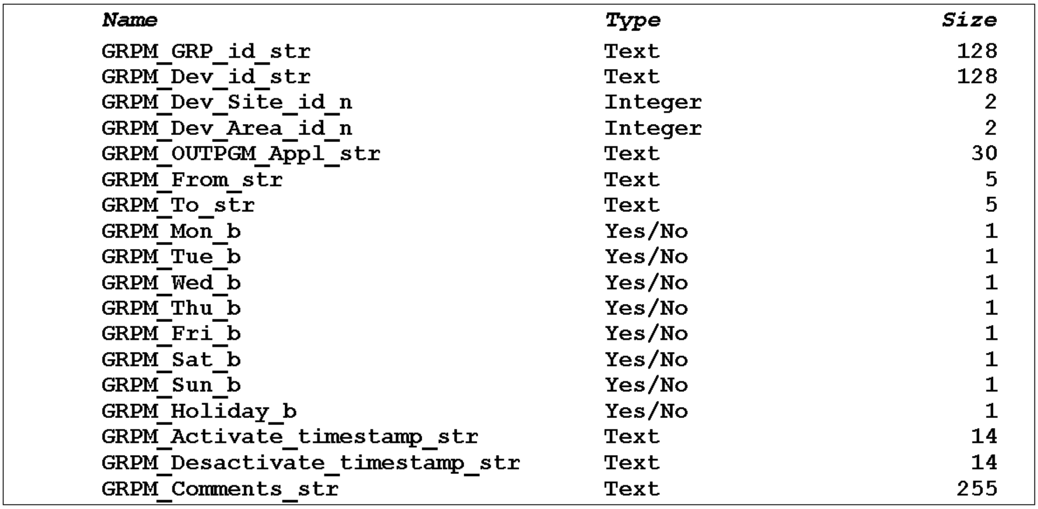
Table 111 provides sample eKERNEL_GROUP_AUTH table data.

Table 112
eKERNEL_GROUP_AUTH sample data

Group id	User id	Comments
31101_00001	FMI	
31102_00001	KDS	
31102_24960	*ALL	

Table: eKERNEL_GROUP_MEMBER

Table 113
eKERNEL_GROUP_MEMBER parameters



Name	*Type*	*Size*
GRPM_GRP_id_str	Text	128
GRPM_Dev_id_str	Text	128
GRPM_Dev_Site_id_n	Integer	2
GRPM_Dev_Area_id_n	Integer	2
GRPM_OUTPGM_Appl_str	Text	30
GRPM_From_str	Text	5
GRPM_To_str	Text	5
GRPM_Mon_b	Yes/No	1
GRPM_Tue_b	Yes/No	1
GRPM_Wed_b	Yes/No	1
GRPM_Thu_b	Yes/No	1
GRPM_Fri_b	Yes/No	1
GRPM_Sat_b	Yes/No	1
GRPM_Sun_b	Yes/No	1
GRPM_Holiday_b	Yes/No	1
GRPM_Activate_timestamp_str	Text	14
GRPM_Desactivate_timestamp_str	Text	14
GRPM_Comments_str	Text	255

GRPM_GRP_id_str

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

Nortel recommends defining group identifiers using the following naming convention:

Table 114
Recommended Group identifier naming convention

Byte 1-5	Input program	
	Byte 1	Site of input program
	Byte 2	Area of input program
	Byte 3	Input program type
		1 - eCAP or eAPI or eESPA
		6 - eIO
		7 - eWEB
		8 - eSMTP_server
		9 - eDMSAPI
	Byte 4-5	Input program sequence number
Byte 6	(Underscore character)	
Byte 7-…	Group name	

Example: 31101_00001 denotes site 3, area 1, input program type eCAP or eAPI, input program sequence 01, group name 00001.

Each group must be defined in the eKERNEL_GROUP table.

For each defined group, one or more group member must be defined in the eKERNEL_GROUP_MEMBER table.

You can assign authority to the groups by means of the eKERNEL_GROUP_AUTH table. See documentation Table_eKERNEL_GROUP_AUTH.pdf.

An example of an entry typically found in this field is as follows:
31101_00001

GRPM_Dev_id_str

This field contains a reference to the destination peripheral as it is known in the internal infrastructure. The site, area, output program application, and device identifier identify peripherals. These four values define a peripheral unambiguously.

A number of sample records are shown in Table 115.

Table 115
GRPM_Dev_id_str sample records (Part 1 of 2)

Site	Area	Device	Output program	Facility
1	1	32479638338	eASYNC	PROXIM US
1	1	865	eDMSAPI	C4050
1	1	9789074	eASYNC	PAGING
1	1	475353215	eASYNC	PROXIM US
1	1	bekds@1s.be	eSMTP	SMTP
1	1	DO_03_01	eIO	DO
1	1	DO_03_02	eIO	DO
1	1	DO_03_03	eIO	DO
1	1	DO_03_04	eIO	DO
1	1	DO_03_05	eIO	DO
1	1	DO_03_06	eIO	DO
1	1	DO_03_07	eIO	DO
1	1	DO_03_08	eIO	DO

Table 115
GRPM_Dev_id_str sample records (Part 2 of 2)

1	1	francis.missiaen@1s.be	eSMTP	SMTP
1	1	kristien.daneels@1s.be	eSMTP	SMTP

GRPM_Dev_Site_id_n

This value refers to the site identifier of the input program that is associated with the group. Refer to "Table: eKERNEL_SITE" on page 1459 for more details on the site parameter.

An example of an entry typically found in this field is as follows: 1

GRPM_Dev_Area_id_n

This value refers to the area identifier of the input program that is associated with the group. Refer to "Table: eKERNEL_AREA" on page 1391 for more details on the site parameter.

An example of an entry typically found in this field is as follows: 1

GRP_OUTPGM_Appl_str

This field provides the output program application identifier of the application that processes the request.

A device can be used more than once depending of the used output program. For example, a DECT extension 865 can be defined for two or more modules.

The indicated application handles the message using the capabilities of the infrastructure. For example, the eDMSAPI module can send E2 data profile messages (non-voice call-based) to extensions, such as DECT C4040 and C4050. The supported values are shown in Figure 116:

Table 116
Supported output applications

eASYNC	for sending SMS to PROXIMUS/KPN and PAGING to BELGACOM
eCSTA	for sending voice-call related user-to-user messages
eDMSAPI	for sending E2 data messages to DECT C922 and C933 sets
eESPA	for sending messages t ESPA 4.4.4 infrastructure
eIO	for enabling/disabling discrete output contacts
eSMTP	for sending mail to SMTP compliant infrastructure
eVBVOICE	for sending wave files through voice-calls

GRP_From_str

This value specifies an hour and time in the format xx:xx. The valid range is 00:00 to 23:59; values outside this range produce unpredictable results. GRP_From_str denotes the start of the time interval where the defined device is an active member of the specified group GRP_Name_str. For example, 00:00 indicates the group-member is active at midnight, and 12:00 indicates the group-member starts at noon. The active period ends at the time specified in GRP_To_str.

An example of an entry typically found in this field is as follows: 00:00

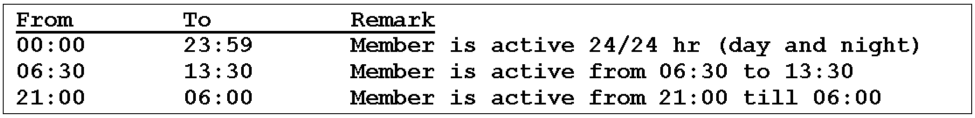
GRP_To_str

This value specifies an hour and time in the format xx:xx. The valid range is 00:00 to 23:59; values outside this range produce unpredictable results. GRP_To_str denotes time when the defined device ceases to be an active member of the specified group GRP_Name_str. For example, 23:59 indicates the group-membership expires at midnight, and 12:00 indicates that the group-membership expires at noon. The active time period begins at the time specified in GRP_From_str.

> ***Note 1:*** GRP_From_str can be larger than GRP_To_str: In this case, a job can start at 21:00 and end at 06:00 (night-shift).
>
> ***Note 2:*** A device can be active from for more than one period of time on a given day. For example: 08:00-12:00 and 13:15-17:30; in this case, two group members must be defined, one of 08:00-12:00 and another with 13:15-17:30.

To clarify the possible values, examples are shown in Figure 117.

Table 117
Group member schedule examples:



From	To	Remark
00:00	23:59	Member is active 24/24 hr (day and night)
06:30	13:30	Member is active from 06:30 to 13:30
21:00	06:00	Member is active from 21:00 till 06:00

GRP_Mon_b

This value specifies whether the group-member record is active on Mondays. Accepted values are True (-1) or False (0). When -1 is specified, the group-member record is active on Mondays. When 0 is specified, the record is not active on this day.

An example of an entry typically found in this field is as follows:-1

GRP_Tue_b

This value specifies whether the group-member record is active on Tuesdays. Accepted values are True (-1) or False (0). When -1 is specified, the group-member record is active on Tuesdays. When 0 is specified, the record is not active on this day.

An example of an entry typically found in this field is as follows:-1

GRP_Wed_b

This value specifies whether the group-member record is active on Wednesdays. Accepted values are True (-1) or False (0). When -1 is specified, the group-member record is active on Wednesdays. When 0 is specified, the record is not active on this day.

An example of an entry typically found in this field is as follows:-1

GRP_Thu_b

This value specifies whether the group-member record is active on Thursdays. Accepted values are True (-1) or False (0). When -1 is specified, the group-member record is active on Thursdays. When 0 is specified, the record is not active on this day.

An example of an entry typically found in this field is as follows:-1

GRP_Fri_b

This value specifies whether the group-member record is active on Fridays. Accepted values are True (-1) or False (0). When -1 is specified, the group-member record is active on Fridays. When 0 is specified, the record is not active on this day.

An example of an entry typically found in this field is as follows:-1

GRP_Sat_b

This value specifies whether the group-member record is active on Saturdays. Accepted values are True (-1) or False (0). When -1 is specified, the group-member record is active on Saturdays. When 0 is specified, the record is not active on this day.

An example of an entry typically found in this field is as follows:-1

GRP_Sun_b

This value specifies whether the group-member record is active on Sundays. Accepted values are True (-1) or False (0).When -1 is specified, the group-member record is active on Sundays. When 0 is specified, the record is not active on this day.

An example of an entry typically found in this field is as follows:-1

GRP_Holiday_b

This value specifies whether the group-member record is active on holidays. Accepted values are True (-1) or False (0). When -1 is specified, the group-member record is active on holidays. When 0 is specified, the record is not active on this day.

> ***Note:*** The term Holiday refers to the dates defined in the eKERNEL_HOLIDAY table. At installation time, a few dates are defined. The tables must be maintained by an administrator. You can use this calendar for other purposes, such as indicating official closing days, if this is suitable to your working environment.

An example of an entry typically found in this field is as follows:-1

GRPM_Activate_timestamp_str

This field specifies the timestamp when the record becomes activated. The format is YYYYMMDDHHMMSS.

The GRPM_Activate_timestamp_str and GRPM_Desactivate_timestamp_str fields can be used to define a time interval, where records are active. This functionality allows to anticipate on future changes in availability of staff, and is typically used in environments where planning is needed for staff, regimes, changing schedules, holiday period, and so on.

An example of an entry typically found in this field is as follows: 20010101000000

GRPM_Desactivate_timestamp_str

This field specifies the timestamp when the record becomes deactivated. The format is YYYYMMDDHHMMSS.

The GRPM_Activate_timestamp_str and GRPM_Desactivate_timestamp_str fields can be used to define a time interval, where records are active. This functionality allows to anticipate on future changes in availability of staff, and is typically used in environments where there is need for on-front planning of staff, regimes, changing schedules, holiday period, and so on.

An example of an entry typically found in this field is as follows: 20991231235959

GRP_Comments_str

This field can optionally be used by an administrator to store reminder information, describing, for example, a description of the file usage.

An example of an entry typically found in this field is as follows: Backup of regular anesthetist during holidays

Table: eKERNEL_GUARDING

Table 118
eKERNEL_GUARDING parameters

GUA_INPPGM_id_n	long	4
GUA_From_str	Text	5
GUA_To_str	Text	5
GUA_Mon_b	Yes/No	1
GUA_Tue_b	Yes/No	1
GUA_Wed_b	Yes/No	1
GUA_Thu_b	Yes/No	1
GUA_Fri_b	Yes/No	1
GUA_Sat_b	Yes/No	1
GUA_Sun_b	Yes/No	1
GUA_Timeout_n	Integer	2
GUA_msg_str	Text	255
GUA_GRP_Name_str	Text	50
GUA_ALA_id_n	long	4
GUA_Comments_str	Text	255

GUA_INPPGM_id_n

This field specifies the unique identifier of the input program. Note that this identifier is defined in the eKERNEL_TCPCLIENT table (field TCPCLIENT_INPGM_id_n). Refer to “Table: eKERNEL_TCPCLIENT” on page 1469 for more information on how to set up these input programs.

An example of an entry typically found in this field is as follows: 11101

GUA_From_str

This value specifies an hour and time in the format xx:xx. The valid range is 00:00 to 23:59; values outside this range produce unpredictable results. GUA_From_str denotes the start of the time interval during which the guarding facility is active. If the eKERNEL module does not receive any requests (message request, configuration request, and so on) from the input program during the GUA_Timeout_n interval, a guarding alarm is activated.

An example of an entry typically found in this field is as follows: "00:00"

GUA_To_str

This value specifies an hour and time in the format xx:xx. The valid range is 00:00 to 23:59; values outside this range produce unpredictable results. The value denotes the end of the time period during which the guarding facility is active.

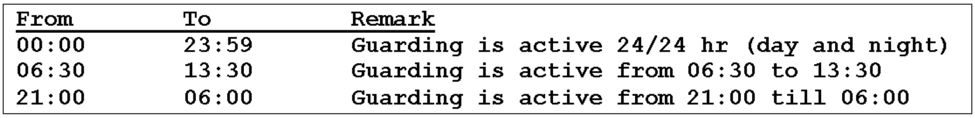
The active time period begins at the time specified in GUA_From_str.

> ***Note 1:*** GUA_From_str can be larger than GUA_To_str, resulting, for example, in a job that starts at 21:00 and ends at 06:00.
>
> ***Note 2:*** A device can be active from for more than one period of time on a given day. For example: 08:00-12:00 and 13:15-17:30; in this case, two group members must be defined, one of 08:00-12:00 and another with 13:15-17:30.

If the same time is specified in more than one case, only the first record is processed.

Table 119 shows examples of Guarding schedules.

Table 119
Guarding schedule examples



From	To	Remark
00:00	23:59	Guarding is active 24/24 hr (day and night)
06:30	13:30	Guarding is active from 06:30 to 13:30
21:00	06:00	Guarding is active from 21:00 till 06:00

GUA_Mon_b

This value specifies whether the group-member record is active on Mondays. Accepted values are True (-1) or False (0). When -1 is specified, the group-member record is active on Mondays. When 0 is specified, the record is not active on this day.

An example of an entry typically found in this field is as follows:-1

GUA_Tue_b

This value specifies whether the group-member record is active on Tuesdays. Accepted values are True (-1) or False (0). When -1 is specified, the group-member record is active on Tuesdays. When 0 is specified, the record is not active on this day.

An example of an entry typically found in this field is as follows:-1

GUA_Wed_b

This value specifies whether the group-member record is active on Wednesdays. Accepted values are True (-1) or False (0). When -1 is specified, the group-member record is active on Wednesdays. When 0 is specified, the record is not active on this day.

An example of an entry typically found in this field is as follows:-1

GUA_Thu_b

This value specifies whether the group-member record is active on Thursdays. Accepted values are True (-1) or False (0). When -1 is specified, the group-member record is active on Thursdays. When 0 is specified, the record is not active on this day.

An example of an entry typically found in this field is as follows:-1

GUA_Fri_b

This value specifies whether the group-member record is active on Fridays. Accepted values are True (-1) or False (0). When -1 is specified, the group-member record is active on Fridays. When 0 is specified, the record is not active on this day.

An example of an entry typically found in this field is as follows:-1

GUA_Sat_b

This value specifies whether the group-member record is active on Saturdays. Accepted values are True (-1) or False (0). When -1 is specified, the group-member record is active on Saturdays. When 0 is specified, the record is not active on this day.

An example of an entry typically found in this field is as follows:-1

GUA_Sun_b

This value specifies whether the group-member record is active on Sundays. Accepted values are True (-1) or False (0). When -1 is specified, the group-member record is active on Sundays. When 0 is specified, the record is not active on this day.

An example of an entry typically found in this field is as follows:-1

GUA_Timeout_n

This field specifies the timeout in seconds, before the defined guarding alarm is activated if no request (configuration request, message request, and so on) of the input program is received by the eKERNEL.

If for instance a timeout of 900 seconds is defined, a guarding alarm is generated if the input program (eCAP, eAPI, and so on) does not send any request within fifteen minutes.

Note that some manufacturers (for example, Honeywell) have the possibility to send with a fix interval a Still alive request to the eCap program. The absence of this request can result in a guarding alarm.

An example of an entry typically found in this field is as follows: 900

GUA_msg_str

This field describes the message that is sent to the group members. Nortel recommends that you enter descriptive text that provides the recipient sufficient information to handle the alarm condition. Mobile users often lack immediate access to other information resources, such as a site map or technical specification. Nortel recommends that you keep the message length less than, or equal to, the maximum length defined in the associated eKERNEL_ALARM table.

An example of an entry typically found in this field is as follows:
HONYWELL NOT ACTIVE

GUA_GRP_Name_str

The group name describes who receives the guarding alarm, and refers to a group defined in eKERNEL_GROUP and eKERNEL_GROUP_MEMBER table.

An example of an entry typically found in this field is as follows: GUARDING

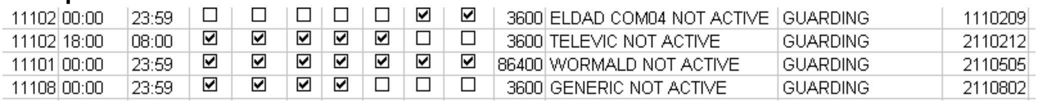
GUA_ALA_id_n

This field refers to the unique alarm identifiers as specified in the eKERNEL_ALARM table. See “Table: eKERNEL_ALARM” on page 1393 for more information on alarm identifies. In a typical environment, input programs (for example, 11101) have a number of alarm identifiers (for example, 1110101 up to 1110107) each of them defining characteristics (alarm priority, length, and so on).

Refer to “Table: eKERNEL_ALARM” on page 1393 for more information on naming conventions.

An example of an entry typically found in this field is as follows: 11101. Refer to Table 120 for more examples.

Table 120
Examples of alarm characteristics



11102	00:00	23:59	□	□	□	□	□	☑	☑	3600	ELDAD COM04 NOT ACTIVE	GUARDING	1110209
11102	18:00	08:00	☑	☑	☑	☑	☑	□	□	3600	TELEVIC NOT ACTIVE	GUARDING	2110212
11101	00:00	23:59	☑	☑	☑	☑	☑	☑	☑	86400	WORMALD NOT ACTIVE	GUARDING	2110505
11108	00:00	23:59	☑	☑	☑	☑	□	□	□	3600	GENERIC NOT ACTIVE	GUARDING	2110802

GUA_Comments_str

This field can optionally be used by an administrator to store reminder information, describing, for example, the usage of the file.

Table: eKERNEL_HOLIDAY

Table 121
eKERNEL_HOLIDAY parameters

Name	*Type*	*Size*
Holiday_str	Text	8
Holiday_Comments_str	Text	255

Holiday_str

This field defines a date that is to be considered as a holiday. Days that are entered here as holidays are important when eKERNEL processes the group members that are defined in the eKERNEL_GROUP_MEMBER table.

Holidays must always be formatted as 8 bytes numeric values in format YYYYMMDD; for example, Christmas 2001 is defined as 20011225. Do not use any formatting symbols, such as spaces, slashes, and so on.

Note the days must be entered manually, a process that must be repeated on regular basis. Nortel recommends that you specify one person in the organization who is responsible for maintaining the holiday information, and for notifying the administrator.

In the excerpt of the eKERNEL_GROUP_MEMBER definition given in Table 122, extension 865 of group 00001 is not processed on holidays; the remaining members are processed on holidays.

Table 122
Holiday definition examples (Part 1 of 2)

GRP_Name_str	GRP_Holiday	GRP	GRP_Holiday_b
00001	1	865	0
00001	2	866	-1

Table 122
Holiday definition examples (Part 2 of 2)

GRP_Name_str	GRP_Holiday	GRP	GRP_Holiday_b
00001	3	867	-1
00001	4	868	-1

An example of an entry typically found in this field is as follows: 20050815 (denotes a fictional national holiday, August 15th, 2005).

Holiday_Comments_str

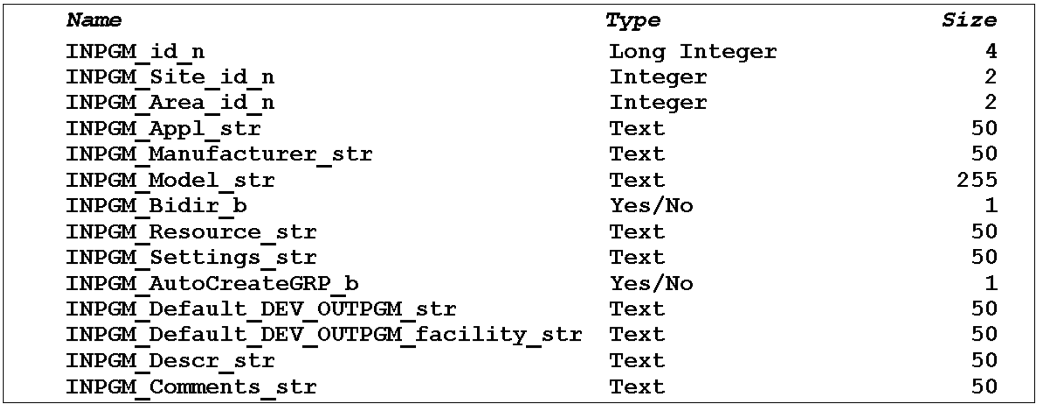
This field can contain remarks from an administrator and is used only for informational purpose. Refer to Table 123 for examples of Holiday comments values.

Table 123
Holiday comments examples

Holiday_str	Holiday_Comments_str
20050101	
20050501	
20050721	
20050815	National Holiday

Table: eKERNEL_INPGM

Table 124
eKERNEL_INPGM parameters



Name	Type	Size
INPGM_id_n	Long Integer	4
INPGM_Site_id_n	Integer	2
INPGM_Area_id_n	Integer	2
INPGM_Appl_str	Text	50
INPGM_Manufacturer_str	Text	50
INPGM_Model_str	Text	255
INPGM_Bidir_b	Yes/No	1
INPGM_Resource_str	Text	50
INPGM_Settings_str	Text	50
INPGM_AutoCreateGRP_b	Yes/No	1
INPGM_Default_DEV_OUTPGM_str	Text	50
INPGM_Default_DEV_OUTPGM_facility_str	Text	50
INPGM_Descr_str	Text	50
INPGM_Comments_str	Text	50

INPGM_id_n

This field specifies the unique identifier of an input capable program.

For each input program, a record must be entered in the eKERNEL_INPGM table. You must also define a matching record in the eKERNEL_TCPCLIENT table (field TCPCLIENT_INPGM_id_n).

Nortel recommends that you develop a naming strategy in assigning values for this identifier. Nortel recommends the following naming convention:

Table 125
Recommended naming strategy for input programs

Byte 1	Site identifier				
Byte 2	Area identifier				
Byte 3-5	Input program identifier				
	Byte 3	1	eCAP or eAPI or eESPA		
		6	eIO		
		7	eWEB		
		8	eSMTP_server		
		9	eDMSAPI		
	Byte 4-5	01-9 9	Input program sequence number		

Nortel recommends using five digits to uniquely identify an input program. Using this method, the identifier indicates the site, area, input program application, and sequence number.

An example of an entry typically found in this field is as follows: 11101

INPGM_Site_id_n

This field specifies the number of the site, as defined in eKERNEL_SITE table. In most cases this is 1.

An example of an entry typically found in this field is as follows: 1

INPGM_Area_id_n

This field specifies the number of the area, as defined in eKERNEL_AREA table. In most cases this is 1.

An example of an entry typically found in this field is as follows: 1

INPGM_Appl_str

This field indicates the specification of the input program. There is a predefined list of supported values; each of them refers to a module.

In the current release only the following values are supported: eAPI, eCAP, eIO, eWEB and eSMTP_server. Other modules can be added to the list in future releases.

The recommended naming convention dictates the use of an appropriate value for the field INPGM_id_n. The eCAP and eAPI input programs have identifies, such as xx1xx, and so on.

An example of an entry typically found in this field is as follows: eAPI

INPGM_Manufacturer_str

The behaviour of different input program modules depends to the external alarm system, and is therefore manufacturer-related. You must always enter a valid value in this field. Refer to Table 126 for a complete list of valid values in current release.

An example of an entry typically found in this field is as follows: *BASE

INPGM_Model_str

The behaviour of different modules depends to the alarm system and manufacturer, and is in most cased model related. You must enter a valid value in this field. Refer to Table 126 for an overview of valid values in current release.

Table 126
Valid model values (Part 1 of 2)

Application	Manufacturer	Model
eAPI	API	*BASE
eCAP	ARITECH	*BASE
eCAP	BEMAC	DIANA 1
eCAP	BEMAC	DIANA 2

Table 126
Valid model values (Part 2 of 2)

eCAP	ELDAD	L:48-0:RC-1:SR-2:SS-3:SS-4:SR
eCAP	GENERIC	*BASE
eCAP	NIRA	*BASE
eCAP	TELEVIC	PROTOCOL CONVERTOR – L:03
eCAP	VSK	DE LICHTERVELDE
eCAP	VSK	OLV VAN VREDE
eCAP	VSK	ST-JOZEF
eCAP	WORMALD	*BASE
eCAP	WORMALD	L:01
eESPA	ESPA	*BASE
eIO	NATIONAL-INSTRUMENTS	BASE
eSMTP_server	SMTP	BASE
eDMSAPI	DMSAPI	BASE
eWEB	eWEB	BASE

INPGM_Bidir_b

This field defines when the protocol is bidirectional to eKERNEL or not. In all cases, the value is 0 (False), only eCAP of TELEVIC model PROTOCOL CONVERTOR – L:03 is –1 (True).

The flag that indicates bidirectional behaviour defines whether external alarm system must be informed on successful or failed message delivery. Currently, there is only one implementation of such a bidirectional protocol. Refer to “Module – eCAP” on page 1091 for more information.

An example of an entry typically found in this field is as follows: 0

INPGM_Resource_str

This value must be set to blanks for the modules eAPI, IO, SMTP_server, and WEB.

The value must be set to the COMxx for the module eCAP. The indication COMxx must specify an available and valid COM port (that is not in use for other resources, is exclusively reserved, and is connected to the alarm system).

An example of an entry typically found in this field is as follows: COM01

INPGM_Settings_str

This value must be set to blanks for the modules eAPI, IO, SMTP_server, and eWEB.

The value must be set to the so-called COM-setting for the module eCAP (RS-232 interfaces). The settings must be a supported combination of baud-rate, parity, data-bits, and stop bits. The value must off-course match the settings of the attached alarm system.

An example of an entry typically found in this field is as follows: 9600,N,8,1

INPGM_AutoCreateGRP_b

This value is an important value for relation to eKERNEL_GROUP and eKERNEL_GROUP_MEMBER and eKERNEL_DEVICE.

This value defines whether alarms from the defined system must automatically create a group in eKERNEL_GROUP table and a group member in the eKERNEL_GROUP_MEMBER table and a device in eKERNEL_DEVICE table. In most cases, the alarm system is unaware of the range of groups and devices and need manual configuration. In this case, the value is 0 (False).

In some cases, external parties can provide a valid DECT number in alarm datastreams. This can be because the external parties are aware of the infrastructure and number scheme of the DECT extension, or have administrative tools available in the alarm systems that allow them to adjust the alarm information according to the DECT Messenger number scheme.

When the alarm system provides valid device names in the alarm string, you can choose to eliminate the need of defining the infrastructure over again in the eKERNEL_GROUP, eKERNEL_GROUP_MEMBER and eKERNEL_DEVICE tables.

IMPORTANT!

Carefully evaluate whether you trust the external parties in ALWAYS providing valid information. If you do, set the value to **1** (True), indicating automatic creation of groups, group members, and devices.

If you activate this function, you must indicate in the fields INPGM_Default_DEV_OUTPGM_str and INPGM_Default_DEV_OUTPGM_facility_str the additional parameters that are needed for the auto-configuration process.

An example of an entry typically found in this field is as follows: 0

INPGM_Default_DEV_OUTPGM_str

The field INPGM_AutoCreateGRP_b allows you to indicate whether auto-create is enabled or disabled.

If O is specified, the value INPGM_Default_DEV_OUTPGM_str is ignored.

If -1 is specified, the value INPGM_Default_DEV_OUTPGM_str is used to indicate the output program that is associated with the device that is created automatically in the eKERNEL_DEVICE. A typical value is eDMSAPI, which assumes that all devices that are automatically created for this input program are to be processed by the eDMSAPI application.

See the eKERNEL_DEVICE information for a list of supported output programs.

An example of an entry typically found in this field is as follows: eDMSAPI

INPGM_Default_DEV_OUTPGM_facility_str

The field INPGM_AutoCreateGRP_b allows you to indicate whether auto-create is enabled or disabled.

If O was specified, the INPGM_Default_DEV_OUTPGM_facility_str is ignored.

If -1 was specified, the INPGM_Default_DEV_OUTPGM_facility_str is used to indicate the facility that is associated with the device that is created automatically in the eKERNEL_DEVICE table. A typical value is C4050, which assumes that all devices that are automatically created for this input program are sharing the same facility C4050. As a result, auto-creation is typically reserved for environments where the peripherals are somewhat standardized.

See “Table: eKERNEL_DEVICE” on page 1407, and “Table: eKERNEL_DEVICE_FORMAT” on page 1419, for more information on defining device facilities.

An example of an entry typically found in this field is as follows: C4050

INPGM_Descr_str

This field allows you to enter descriptive text, which is visible in the eKERNEL module, in the associated input program and in some web-based functions.

An example of an entry typically found in this field is as follows: Televic Protocol Convertor

INPGM_Comments_str

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

Table: eKERNEL_MESSAGE_FORMAT

Table 127
eKERNEL_MESSAGE_FORMAT parameters

Name	*Type*	*Size*
Msg_Ala_id_n	Long Integer	4
Msg_Msg_str	Text	50
Msg_VBVoice_phrase_str	Text	50
Msg_Descr_str	Text	255
Msg_Comments_str	Text	255

Msg_Ala_id_n

This field refers to the unique alarm identifiers as specified in the eKERNEL_ALARM table. See “Table: eKERNEL_ALARM” on page 1393 for more information on alarm identifies. In a typical environment, input programs (for example, 11101) have a number of alarm identifiers (for example, 1110101 up to 1110107) each of them defining characteristics (alarm priority, length, and so on).

Refer to “Table: eKERNEL_ALARM” on page 1393 for more information on naming conventions.

Table 128
Alarm identifiers (Part 1 of 2)

Byte 1	Site identifier				
Byte 2	Area identifier				
Byte 3-5	Input program identifier				
	Byte 3	1	eCAP or eAPI or eESPA		
		6	eIO		

Table 128
Alarm identifiers (Part 2 of 2)

		7	eWEB		
		8	eSMTP_server		
		9	eDMSAPI		
	Byte 4-5	01-99	Input program sequence number		
Byte 6-7	Alarm sequence number				

An example of an entry typically found in this field is as follows: 1110101

Msg_Msg_str

This field describes the format of the result message after internal processing through eKERNEL. When no records are specified, received messages are transmitted as is to the destination party. When definitions are found in the MESSAGE_FORMAT table, an internal preprocessing can reformat the message, either completely replacing the message or manipulating the message by means of a prefix and suffix.

Refer to Table 129 on page 1457 for examples on message formats. Messages are built based upon fixed characters and the [message] special value, which is replaced by the original message text, as follows:

- A format AA [message] translates Hello world into AA Hello world.
- A format FIRE ALARM translates Hello world into FIRE ALARM.

An example of an entry typically found in this field is as follows: see Table 129 on page 1457.

Msg_VBVoice_phrase_str

This field can be left blank.

Msg_descr_str

This describes the conversion process. This field is informational only.

Msg_Comments_str

This field can be updated with remarks of the system administrator. The value is informational only.

Table 129 shows examples of data found in the eKERNEL_MESSAGE_FORMAT table.

Table 129
eKERNEL_MESSAGE_FORMAT sample data

Msg_Ala_id_n	Msg_msg_str	Msg_VBVoice_phrase_str
1110101	AA [message]	
1110102	AI [message]	
1110103	AC [message]	
1110104	CC [message]	
1120105	BRANDALARM	Fire.wav
1110201	BEMAC [message]	
1110202	BEMAC [message]	
1110203	BRAND [message]	Wormald_fire.wav
1110203	TECHN [message]	Wormald_technical.wav

Table: eKERNEL_SITE

Table 130
eKERNEL_SITE parameters

Name	*Type*	*Size*
CFG_Site_id_n	Integer	2
CFG_Site_Descr_str	Text	50
CFG_Site_Admin_name_str	Text	50
CFG_Site_Admin_email_str	Text	128
CFG_Site_eKernel_ip_str	Text	15
CFG_Site_eKernel_port_str	Text	5
CFG_Site_eKernel_socket_str	Text	50
CFG_Connectionstring_DATA_str	Text	255
CFG_eLOG_Path_str	Text	255
CFG_eLOG_nmbr_days_n	Integer	2
CFG_Connectionstring_CFG_str	Text	255
CFG_Log_nmbr_days_n	Integer	2
CFG_Log_path_str	Text	50
CFG_GarbadgeCollection	Integer	2
CFG_Watchdog_com_port_str	Text	9
CFG_Watchdog_interval_n	Integer	2
CFG_Watchdog_cmd_str	Text	4
CFG_INRQS_id_n	Integer	2
CFG_OUTRQS_id_n	Integer	2
CFG_Comments_str	Text	255

CFG_site_id_n

This field specifies the site ID. In DECT Messenger, a site is the place where the eKERNEL module runs. Each eKERNEL instance has an appropriate database Messenger_CFG and Messenger_DATA. Note that a site can span multiple physical areas spread over multiple locations, and still being considered as one single site, because there is only one eKERNEL running.

Note: The field is numeric. Nortel recommends using site 1 for the first site, and increase the value by one for other sites that are added in time. If two sites have neither communications nor any interference, both sites can in theory use the same number. However, if integration is planned, give different sites different numbers.

Current release does not foresee eKERNEL to eKERNEL communication. The concept of inter-eKERNEL communications can however be implemented in a future release, adding advanced functionality such as database-synchronization, database-replication, load-balancing, high-availability, and so on.

An example of an entry typically found in this field is as follows: 1

CFG_Site_Descr_str

This field specifies a brief description of the site; usually the name of the institution or the name of the city is entered here. You can also enter, for example, your Nortel customer number.

An example of an entry typically found in this field is as follows: Number One Systems

CFG_Site_Admin_name_str

This field specifies the name of the system administrator who is responsible within the institution for the installation. This is usually the name of the help desk, the IT department or the person responsible of the PBX infrastructure. The name is displayed in some user interfaces as the person to contact to request more information.

An example of an entry typically found in this field is as follows: Francis Missiaen

CFG_Site_Admin_email_str

This field specifies a valid e-mail address of the person or department specified in CFG_Site_Admin_name_str. In the current release, the field is informational only. If you install the eWEB module, Nortel recommends that you enter the e-mail address while configuring the Apache Web Server 3.1.20.

An example of an entry typically found in this field is as follows: francis.missiaen@1s.be

CFG_Site_eKERNEL_ip_str

This field specifies the local IP address of the system.

> ***Note:*** It is required to assign a fixed IP address for the DECT Messenger.

You can determine the IP address of the system with the IPCONFIG command (Click **Start** on the Windows taskbar, and choose **Run >cmd.** Enter the command **IPCONFIG**). You must – prior to connecting the system to the network – contact the network administrator and request a valid IP address. If DHCP server is in place, check for an IP address that is not within the range of the DHCP server. Although there are techniques to extend the lease period to a high value, obtaining an IP address from a DHCP server is not supported and can result in system malfunction.

An example of an entry typically found in this field is as follows: 10.110.50.138

CFG_Site_eKERNEL_port_str

This field specifies a port number. Valid port numbers are in the range between 0 and 65535. However, Nortel recommends that you avoid using ports in the range of 0 and 1024, as these ports are likely to used by other applications.

> ***Note:*** You can use the NETSTAT command to find out what ports are in use. When all required service is installed (for example, DMSAPI-service, CSTA_service, PC Anywhere, Web Server, SMTP Server, and so on), you can find out what ports are currently in use. Click **Start** in the Windows taskbar and choose **Run** > **cmd.** Enter the command **NETSTAT /A** to display an overview of TCP/IP ports is use.

The default value 9000 is usually acceptable. Although current release does not implement eKERNEL-to-eKERNEL communication, the eKERNEL always binds a socket to the port that is reserved for eKERNEL to eKERNEL traffic in a multisite configuration. In single site configurations, you still must enter this value. The eKERNEL module always makes this sockets connection active, even in single site configurations.

An example of an entry typically found in this field is as follows: 9000

CFG_Site_eKERNEL_socket_str

This value specifies the behaviour of the socket connection reserved for eKERNEL-to-eKERNEL communication. You must always specify the value `Close after send` here. Other preserved values are `Keep socket open` and `Close after receive`, but are currently unsupported.

An example of an entry typically found in this field is as follows: Close after sent

CFG_Connectionstring_DATA_str

This field specifies the connection string, which contains information used for establishing a connection to the Messenger_DATA database. A complete connection string contains all the information needed to establish a connection. The connection string is a series of keyword/value pairs separated by semicolon.

The Provider keyword identifies the OLE DB provider to be used.

The Persist Security Info property specifies whether the data source can persist sensitive authentication information such as a password.

The keyword Data source is the name or network address of the instance of the database to which to connect.

The username is the SQL Server login account, and the password is the password for the SQL Server account logging on.

The Initial Catalog property specifies the name of the initial default catalog to use when connecting to a data source.

There are two possible connection strings supported for the DECT Messenger application:

1 for Ms Access: the keyword are:

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

2 for SQL server or the MSDN engine:

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

CFG_eLOG_Path_str

This field specifies the path where the daily log files are stored, in a comma separated format.

This field is only relevant if the eLOG licence is available.

If the value *NONE is set, the logging functionality is disabled.

An example of an entry typically found in this field is as follows: C:\SOPHO Messenger\eLOG

CFG_eLOG_nmbr_days_n

This field specifies the number of days the eLOG-files are kept online available. Nortel recommends specifying at least 30 days. The parameter is introduced in R3.0 and refers to the eLOG functionality that generates in eKERNEL comma separated files located in C:\SOPHO Messenger@Net\eLOG. These files must not be confused with logging files located in the directory C:\SOPHO Messenger@Net\Log, and contain logging of eKERNEL and other modules.

Special value 0 indicates no clean-up occurs. This means eLOG files remain on the system until manual clean-up takes place.

Note: On systems with a high workload the eLOG-files can consume a lot of disk space. To correct this, specify a small value for this parameter.

An example of an entry typically found in this field is as follows: 30

CFG_Connectionstring_CFG_str

This field is reserved for future releases and is not implemented yet.

CFG_log_nmbr_days_n

This field specifies the number of days the log-files are kept online available. This value is always used by eKERNEL. The other modules start with a hard-coded value of 14 days, and contact eKERNEL to request the configuration. Once the configuration is received, the modules continue work with the specified number of days. Note the modules other that eKERNEL only purge old log files at midnight. Nortel recommends specifying at least 14 days for this parameter.

Special value 0 indicates no clean-up occurs. This means log files remain on the system until manual clean-up takes place.

> ***Note:*** On systems with a high workload the eLOG-files can consume a lot of disk space. To correct this, specify a small value for this parameter.

An example of an entry typically found in this field is as follows: 14

CFG_log_path_str

This field specifies the logging path for eKERNEL only. Other modules use the drive specified in the command-line parameters of the shortcut (for example, /Log drive:C) in combination with a hard-coded path (C:\SOPHO Messenger@Net\Log).

An example of an entry typically found in this field is as follows: C:\SOPHO Messenger@Net\Log

CFG_GarbageCollection

This field specifies the rate of garbage collection (internal use only). CFG_GarbageCollection refers to the number of seconds when alarms are considered expired when a <msgrqs> does not receive a <msgrpy>. This helps establishing internal recovery for non-responding devices and peripherals. Nortel recommends that you specify 600 for this value.

An example of an entry typically found in this field is as follows: 600

CFG_Watchdog_com_port_str

This field specifies the usage of an optional watchdog configuration.

The default value is *DISABLED, indicating no watchdog function is available. If a Watchdog board is installed, you must specify the COM port here (for example, COM03). If a watchdog is operational, the system signals error conditions using a watchdog board configured on the specified COM-resource. An attached relay contact can generate an audible or visible alarm notification to signal the error condition.

An example of an entry typically found in this field is as follows: COM03

CFG_Watchdog_interval_n

This field specifies, in combination with CFG_Watchdog_com_port_n, the behaviour of a Watchdog board.

- If *DISABLED was specified, the value must be set to 0.
- If a COM port was specified to activate the card, an interval can be specified. The value indicates the frequency eKERNEL sends a control signal to the card.

When eKERNEL fails to send the signal at the specified interval (for example, because of a hardware failure, operating system failure, eKERNEL failure, eKERNEL stopped, and so on.) the card detects the error condition and triggers an alarm, if the Watchdog is configured correctly. A typical value is between 10 and 60 seconds, but must match the card configuration. Large values can slow down alarm notification, while very small values unnecessarily consume system resources.

An example of an entry typically found in this field is as follows: 10

CFG_Watchdog_cmd_str

This field specifies the signal that is sending to the COM port is a 5-byte packet that includes a checksum:
[0x01][0x57][0x84][CFG_Watchdog_cmd_str][checksum].

The default value is 0x21.

For more information, see the user manual of the internal serial watchdog page 9 till 13.

An example of an entry typically found in this field is as follows: 0x21

CFG_INRQS_id_n

This field specifies a value that is used internally by eKERNEL, and *you must not change the value* unless explicitly instructed to do so. The value stored in CFG_INRQS_id_n is used to generate unique numbers to incoming message requests. Manipulation of this value can result in system malfunction. The value is used to generate unique keys in the Messenger_DATA database table RQS_IN. Resetting the value without cleaning up RQS_IN can result in system failure and is unsupported.

IMPORTANT!

Because table values are, for performance reasons, retrieved at start-up of eKERNEL, and committed at close down of eKERNEL, never stop the eKERNEL using any method other than gracefully shutting down the application with the close button. Abnormal shutdown can result in problems when the system is started. Nortel recommends the use of a UPS. Problems due to system power failure are unsupported.

An example of an entry typically found in this field is as follows: 2392 (never change the current value manually)

CFG_OUTRQS_id_n

This field specifies a value that is used internally by eKERNEL and *you must not change the value* unless explicitly instructed to do so. The value stored in CFG_OUTRQs_id_n is a number that is used to generate unique numbers to outgoing message requests. Manipulation with this value can result in system malfunction. The value is used to generate unique keys in the

Messenger_DATA database. Resetting the value without cleaning up the appropriate database can result in system failure and is unsupported.

IMPORTANT!

Because table values are, for performance reasons, retrieved at start-up of eKERNEL, and committed at close down of eKERNEL, never stop the eKERNEL using any method other than gracefully shutting down the application with the close button. Abnormal shutdown can result in problems when the system is started. Nortel recommends the use of a UPS. Problems due to system power failure are unsupported.

An example of an entry typically found in this field is as follows: 4 (never change the current value manually)

CFG_Comments_str

This field provides space for the administrator to enter comments, such as reminder information, describing, for example, the full name of the site.

An example of an entry typically found in this field is as follows: “Development site of Number One System”.

Table 131 shows examples of data found in the eKERNEL_SITE table (example data is split to improve readability).

Table 131
eKERNEL_SITE sample data

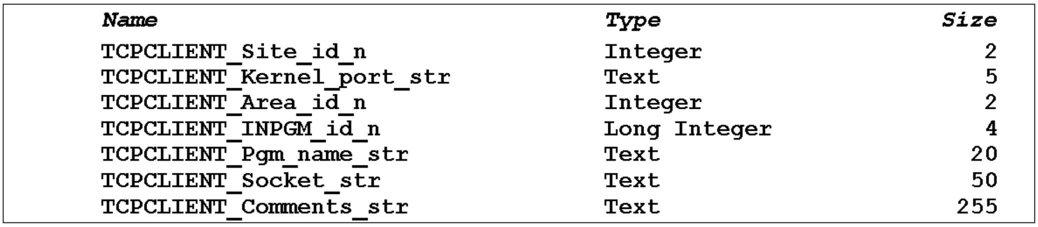
Site	Description	Admin	Mail	Address	Port	Socket	...
3	Sample Site 3	Francis Missiaen	francis.missiaen@1s.be	10.110.50.138	9000	Close after send	…

eKERNEL_SITE sample data (continued)

…	Log days	Log path	Garbage	Watch dog	Intv	Cmd	InRqs	OuRqs	Comments
…	1	C:\SOPHO Messenger@net	600	*DISABLED	10	0x21	58	4	

Table: eKERNEL_TCPCLIENT

Table 132
eKERNEL-TCPCLIENT parameters



Name	*Type*	*Size*
TCPCLIENT_Site_id_n	Integer	2
TCPCLIENT_Kernel_port_str	Text	5
TCPCLIENT_Area_id_n	Integer	2
TCPCLIENT_INPGM_id_n	Long Integer	4
TCPCLIENT_Pgm_name_str	Text	20
TCPCLIENT_Socket_str	Text	50
TCPCLIENT_Comments_str	Text	255

TCPCLIENT_site_id_n

This field refers to the site ID specified in the eKERNEL_SITE table. Usually this field has value 1.

An example of an entry typically found in this field is as follows: 1

TCPCLIENT_kernel_port_str

This field specifies the port that is reserved for the specified module.

A client/server connection is established between eKERNEL and all adjacent modules. In this client/server model, the eKERNEL is TCP server and the remaining modules are TCP client.

At startup the eKERNEL must initiate a number of socket connections, and must listen on a specific port until an inbound socket connection is received from the client module.

The eKERNEL_TCPCLIENT table described this list of adjacent modules, and, for each instance of the module, indicates the specific port number.

> ***Note:*** The adjacent modules also must know what port is reserved for them. This is implemented for most modules through a command line parameter string that is defined in the shortcut of the modules. The administrator must carefully assign the port numbers and use the matching port number in the creation of the shortcut.

Each module must have a dedicated TCP/IP port. Through this port, a socket connection is established between the module and the eKERNEL. The eKERNEL_TCPCLIENT table defines for the eKERNEL module an overview of all defined modules, and starts a socket server for each module. In theory, the modules can have any valid value between 0 and 65535, however Nortel recommends against using the following:

- port 0 (which results in a random port generation, and so is unsuitable for a server)
- a common port (21, 23, 25, 80, and so on)

Nortel recommends using the range 3000 to 3999 for assigning ports to modules, and using the Area number as the second digit of the port number. This means the range 31xx is used for modules of area 1, 32xx for modules of area 2, and so one. The last two digits can be a number starting at 01 and incrementing by one for the additional modules. See the sample data for more information.

An example of an entry typically found in this field is as follows: 3101 (for the first module on area 1)

TCPCLIENT_Area_id_n

This field refers to the area a specified in eKERNEL_AREA table. Usually this field has value 1

An example of an entry typically found in this field is as follows: 1

TCPCLIENT_INPGM_id_n

When an output-only module is specified (for example, eASYNC, eDMSAPI, eSMTP, and so on), the value must always be set to 0. This indicates the module is not capable of generating alarms, and is not familiar to the concept of input programs.

When an input-capable module is specified (for example, eAPI, eCAP, eSMTP_server, eWEB, and so on), a value other than 0 must be specified.

This field specifies the unique identifier of the input program.

As specified in the eKERNEL_INPGM and eKERNEL_ALARM table related section, Nortel recommends establishing a naming convention for script messages.

Table 133
Recommended input program identifiers naming convention

Byte 1	Site identifier				
Byte 2	Area identifier				
Byte 3-5	Input program identifier				
	Byte 3	1	eCAP or eAPI or eESPA		
		6	eIO		
		7	eWEB		
		8	eSMTP_server		
		9	eDMSAPI		
	Byte 4-5	01-9 9	Input program sequence number		

Nortel recommends using five digits to uniquely identify an input program. With the guidelines above, the identifier implies the site, area, input program application, and sequence number.

This value is refers to the unique identifier defined in the eKERNEML_INPGM table. This unique identifier is also found in the eKERNEL_ALARM table, where available alarm types are defined for each input program.

An example of an entry typically found in this field is as follows: 11101

TCPCLIENT_pgm_name_str

This field refers to any of the list of available modules that can be attached to eKERNEL. This list includes modules that are input only, output only, or capable of both input and output.

This list of supported modules currently includes: eAPI, eASYNC, eCAP, eESPA, eDMSAPI, eIO, eSMTP, eSMTP_server, and eWEB. Other modules can be included in the future.

IMPORTANT!

An additional module is also available for the IBM iSeries or IBM AS/400 platform. This module must be seen as API for the iSeries 400 or AS/400 platform. The module provides an interface to access the DECT Messenger functionality from an iSeries 400 or AS/400 platform. If you have such a host system, you must contact the authors of DECT Messenger for more information.

Contact Number One Systems, Francis Missiaen, Xavier De Cocklaan 72, B-9730 Sint-Martens-Latem, phone ++ 32 9 280 22 22, e-mail: francis.missiaen@1s.be for more information on this plug-in module. All functionality, for example, sending messages to DECT, SMTP, GSM, triggering discrete output on Distributed I/O peripherals, and so on, are accessible to your existing iSeries 400 or AS/400 legacy applications.

An example of an entry typically found in this field is as follows: eCAP

TCPCLIENT_socket_str

This field defines what happens to an inbound socket connection, when eKERNEL receives data. The following values are supported: Keep socket open, Close sockets after send, or Close sockets after receive.

As the values imply, you can choose to keep the link open, close the link after receiving data, or close the link after sending data.

The majority of modules must be defined with Keep socket open. This means a permanent socket connection remains active. Nortel recommends using Keep socket open for all modules, unless specified otherwise.

Note 1: For the eWEB module the value Close after receive must be specified if no script messages are used. If the Send Script Message functionality is implemented in eWEB, the value Close after send must be specified. This is a major issue, because closing a connection too soon can prevent eKERNEL from sending a feedback to the eWEB module.

Note 2: When eAPI is used, you have the choice to specify any value. The correct value depends on a number of factors, one of them is the question whether the port is dedicated for one eAPI-based interface or shared between multiple instances of eAPI-based interface. Nortel recommends that you define Keep socket open. This requires a dedicated port for each eAPI. However, if external applications access the system through ad hoc requests to eKERNEL, you must specify the value Close after receive to free the resources for other inbound requests.

An example of an entry typically found in this field is as follows: **Keep socket open** (required for all modules, except eWEB or eAPI).

TCPCLIENT_Comments_str

This field can be used by an administrator to enter reminder information, describing, for example, usage of the module.

An example of an entry typically found in this field is as follows: This module handles input of ELDAD.

Table 134 shows examples of data found in the eKERNEL_TCPClient table.

Table 134
eKERNEL_TCPClient sample data

Site	Port	Area	Input program	Application	Socket
3	3101	1	31901	eDMSAPI	Keep open
3	3102	1	31101	eCAP	Keep open
3	3103	1	31102	eCAP	Keep open
3	3104	1	31103	eAPI	Close after receive
3	3105	1	0	eASYNC	Keep open

Table 134
eKERNEL_TCPClient sample data

3	3108	1	31601	eIO	Keep open
3	3109	1	31701	eWEB	Close after sent
3	3110	1	31801	eSMTP_server	Keep open
3	3111	1	0	eSMTP	Keep open
3	3112	1	31105	eESPA	Keep open

Table: eSMTP_CLIENT

Table 135
eSMTP_CLIENT parameters

Name	*Type*	*Size*
eSMTP_Site_id_n	Integer	2
eSMTP_Area_id_n	Integer	2
eSMTP_Srv_ip_str	Text	15
eSMTP_Srv_port_str	Text	5
eSMTP_Srv_domain_str	Text	128
eSMTP_ALA_Prty_DTMF_Confirm_n	Integer	2
eSMTP_Silence_intv_n	Integer	2
eSMTP_From_address_str	Text	50
eSMTP_Comments_str	Text	255

eSMTP_Site_id_n

This field specifies the site identifier, as defined in eKERNEL_SITE table. In most environments, the value is 1.

An example of an entry typically found in this field is as follows: 1

eSMTP_Area_id_n

This field specifies the area identifier, as defined in eKERNEL_AREA table. In most environments, the value is 1.

An example of an entry typically found in this field is as follows: 1

eSMTP_srv_ip_str

This field specifies the IP address of the SMTP server that is used to handle outbound SMTP messages. This is typically an SMTP compatible system, for example, Lotus Notes, Lotus Domino, Microsoft Exchange, AS400 SMTP Server, iSeries400 SMTP server, Windows 2000 SMTP server, and so on.

The SMTP server must be properly configured to allow inbound SMTP requests from the DECT Messenger applications (relaying, and so on).

An example of an entry typically found in this field is as follows: 10.110.17.6

eSMTP_srv_port_str

This field specifies the port number used for SMTP access. In most environments, this is value 25.

An example of an entry typically found in this field is as follows: 25

eSMTP_srv_domain_str

This field refers to the domain name used in the SMTP connection. Refer to the RFC821 specifications on the process involved in message delivery through SMTP. The domain parameter is associated to the HELO command in the SMTP dialog.

An example of an entry typically found in this field is as follows: ibsbe.be

eSMTP_ALA_Prty_DTMF_Confirm_n

This field specifies what alarm priority levels require a confirmation. Alarm priority is defined in the eKERNEL_ALARM table.

Alarms that do not meet the requirements are automatically confirmed when the DECT Messenger SMTP client sends a message to an external SMTP server. The message is considered sent when it reaches the server. However, at this stage, there is no guaranteed message delivery, because there is no read indication. This situation is similar to eASYNC, where SMS and PAGING as well do not foresee end user confirmation. An SMTP mail can be pending between intermediate server (for example, in an internet environment) or remain unread in the mailbox for a large amount of time.

Confirmation techniques can be appropriate to force mail destinations to respond to the alarm request. This can be accomplished by calling back to a predefined DID number. In eKERNEL release 2.9.18 and later, the functionality is implemented that if the priority of the alarm is lower than or equal to this value (so has an higher importance), the message reply (<msgrpy>) sent by the eSMTP module to the eKERNEL is treated as a NAK reply (even if a ACK was sent). Therefore, alarms that are sent using eSMTP (and are successfully delivered (so status = ACK)), and that need a confirmation, have the same behaviour as alarms with status NAK.

This results in the alarm repeating every eSMTP_Silence_intv_n seconds until confirmation. If the alarm is not confirmed within the DEV_Retry_count_ALT_DEV_id_n (eKERNEL_device) retries, the alarm is sent to the alternative devices (if configured).

A value of, for example, 2 indicates alarms with priority 0,1 and 2 are considered to be confirmed using this callback procedure.

An example of an entry typically found in this field is as follows: 2

eSMTP_Silence_intv_n

This field specifies the silence interval, the time between repeating outstanding messages that need confirmation. The parameter corresponds with the parameter available in the eKERNEL_ALARM table, but overrules the latter value. Due to bandwidth restrictions, a larger value than specified in eKERNEL_ALARM table is suitable. For example, repeating unconfirmed alarms every two minutes in a mail destination environment is not desirable. A typical value is ten minutes. The value must be expressed in seconds.

An example of an entry typically found in this field is as follows: 600

eSMTP_From_address_str

This field specifies the e-mail address of the sender of both eSMTP module and eWEB module (form Send SMTP Message). The specified value is used in the MAIL FROM tag of the mail composition process, as spec RFC821 and RFC1521.

> ***Note:*** In R3.0, there is now ability to specify a friendly name as well. The module eSMTP and eWEB now support any of the following three syntax:

francis.missiaen@ibsbe.be
<francis.missiaen@ibsbe.be>
Francis Missiaen <francis.missiaen@ibsbe.be>

An example of an entry typically found in this field is as follows: francis.missiaen@ibsbe.be

eSMTP_Comments_str

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

Table 136 shows examples of data found in the eSMTP_CLIENT table.

Table 136
eSMTP_CLIENT sample data

Site	Area	Address	Port	Domain	Confirm	Interval	Comments
1	1	10.110.17.6	25	1s.be	1	600	

Table: eSMTP_SERVER

Table 137
eSMTP_SERVER parameters

Name	*Type*	*Size*
eSMTPS_Site_id_n	Integer	2
eSMTPS_Area_id_n	Integer	2
eSMTPS_Email_dir_str	Text	255
eSMTPS_Poll_intv_n	Integer	2
eSMTPS_Email_dir_processed_str	Text	255
eSMTPS_Email_keep_processed_n	Integer	2
eSMTPS_Email_dir_error_str	Text	255
eSMTPS_Email_keep_error_n	Integer	2
eSMTPS_Delivery_text_str	Text	255
eSMTPS_NonDelivery_text_str	Text	255
eSMTPS_ALA_id_n	Long Integer	4
eSMTPS_Comments	Text	255

eSMTP_Site_id_n

This field denotes the site identifier, as defined in eKERNEL_SITE table. In most environments, this field has a value of 1.

An example of an entry typically found in this field is as follows: 1

eSMTPS_Area_id_n

This field denotes the area identifier, as defined in eKERNEL_AREA table. In most environments, this field has a value of 1.

An example of an entry typically found in this field is as follows: 1

eSMTPS_Email_dir_str

This field specifies the directory that is polled upon arrival of incoming e-mail. In the Windows 2000 environment with the Internet Information Server component SMTP server activated, this is typically c:\inetpub\mailroot\drop. The specified directory is the directory where the Windows shipped SMTP server drops incoming mail.

This directory contains e-mail files (with the extension .EML) that are processed by DECT Messenger eSMPT_server module, which analyses the inbound e-mail files and handles them as alarm input.

An example of an entry typically found in this field is as follows:
c:\inetpub\mailroot\drop

eSMTPS_Poll_intv_n

This parameter defines the interval between individual poll operations the eSMTP_server module handles to look for inbound mail. The value is expressed in seconds, and typically has a value of 10 seconds.

Specifying a smaller value requires additional system resources, and can speed up the detection process of inbound e-mail based alarm generation. Note however that e-mail processing is as such a technology that is not designed to guarantee lightning-speed response, and therefore a very small interval does not lead to substantial benefit. Only in very special environments with internal LAN-only mail exchange and dedicated resources are time-critical intervals suitable.

An example of an entry typically found in this field is as follows: 10

eSMTPS_Email_dir_processed

Once an inbound e-mail is detected, the eSMTP_server module moves the processed e-mail message an archive storage location.

A special value *NONE can be defined here, indicating the processed e-mail messages are not be kept online, and are removed from the hard disk. Although some kind of logging information is often still available, the originating mail message is destroyed.

In most cases, a directory name is specified, and defines the location where the processed e-mail messages are temporarily archived. This archive allows system administrators to perform more detailed problem analysis.

Warning: the value specified must be different from the value specified in the eSMTPS_Email_dir_str parameter, or otherwise infinite looping condition occurs. The eSMTP_server module attempts to create the hierarchical directory structure if the path does not exist.

An example of an entry typically found in this field is as follows: c:\inetpub\mailroot\drop\processed.

eSMTPS_Email_keep_processed_n

This field specifies the number of days the archive of processed e-mail messages is kept on the hard disk. The value is expressed in days, and has typically a value of 5 days.

Adjust this value to accommodate for the number of inbound e-mail messages, the requested archive period, and the available disk space.

An example of an entry typically found in this field is as follows: 5

eSMTPS_Email_dir_error_str

Once an inbound e-mail is detected, the eSMTP_server module moves the processed e-mail message to some kind of archive storage location. This location is defined in eSMTPS_Email_dir_processed_str. Mail that cannot be processed is moved to a separate location, defined in eSMTPS_Email_dir_error_str.

A special value *NONE can be defined here, indicating the e-mail messages in error are not kept online, and are removed from the hard disk. Although some kind of logging information is often still available, the originating mail message is destroyed.

In most cases, a directory name is specified, and defines the location where the e-mail messages in error are temporarily archived. This archive allows system administrators to perform more detailed problem analysis.

Warning: the value specified must be different from the value specified in the eSMTPS_Email_dir_str parameter, or otherwise infinite looping condition occurs. The eSMTP_server module attempts to create the hierarchical directory structure if the path does not exist.

An example of an entry typically found in this field is as follows: c:\inetpub\mailroot\drop\error

eSMTPS_Email_keep_error_n

This field specifies the number of days the archive of e-mail messages in error is kept on the hard disk. The value is expressed in days, and has typically a value of 5 days.

Adjust this value to accommodate the number of inbound e-mail messages, the requested archive period, and the available disk space.

An example of an entry typically found in this field is as follows: 5

eSMTPS_Delivery_text_str

When an inbound e-mail message is accepted by eKERNEL, the sender receives a delivery report. This delivery report is sent through eSMTP client. (The eSMTP module is a prerequisite.)

The message text for the delivery messages is defined in the eSMTPS_Delivery_text_str field.

An example of an entry typically found in this field is as follows: MESSAGE SUCESSUFULLY DELIVERED

eSMTPS_NonDelivery_text_str

When an inbound e-mail message is rejected by eKERNEL, the sender receives a non-delivery report. This non-delivery report is sent through eSMTP client. (The eSMTP module is a prerequisite.)

The message text for the non-delivery messages is defined in the eSMTPS_NonDelivery_text_str field.

An example of an entry typically found in this field is as follows: MESSAGE COULD NOT BE DELIVERED

eSMTPS_ALA_id_n

When an inbound e-mail message is accepted or rejected by eKERNEL, the sender receives a delivery or non-delivery report. This report is sent from eKERNEL to eSMTP client. (The eSMTP module is a prerequisite.)

To produce such outbound message, eKERNEL must known the alarm identifier that is used to produce the message for eSMTP. This value must match the value specified in eKERNEL_ALARM table. Verify the length of the delivery and non-delivery messages specified in eSMTPS_Delivery_text_str and eSMTPS_NonDelivery_text_str.

An example of an entry typically found in this field is as follows: 1180101

eSMTPS_Comments

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

Table: eWEB

Table 138
eWEB parameters

Name	*Type*	*Size*
eWEB_Address_str	Text	15
eWEB_Site_id_n	Integer	2
eWEB_Area_id_n	Integer	2
eWEB_eKernel_address_str	Text	15
eWEB_Branding_str	Text	50
eWEB_Comments_str	Text	50

eWEB_Address_str

This field specifies the IP address of the system where the Apache Web Server is running.

You can obtain the address with the IPCONFIG command. The eWEB module uses this address to obtain its site, area number, and the address of the eKERNEL (based upon eWEB table) and to obtain the port number at which eKERNEL listens (based upon eKERNEL_TCPCLIENT table).

This process is carried out in the PHP-scripts that run on the Apache Web Server. As a result, the Web Server can use its own IP address to retrieve the configuration data from the database. The values are needed in eWEB to set up a proper socket connection to eKERNEL module, and to give the user access to the correct site and area-related data. You can define multiple addresses for the same eWEB module.

An example of an entry typically found in this field is as follows:
10.100.50.138

eWEB_Site_id_n

This field specifies the site number associated to the eWEB instance obtained by the IP address of the Web Server. In most cases this value is 1, as defined in eKERNEL_SITE.

An example of an entry typically found in this field is as follows: 1

eWEB_Area_id_n

This field specifies the area number associated to the eWEB instance obtained by the IP address of the Web Server. In most cases this value is 1, as defined in eKERNEL_AREA.

An example of an entry typically found in this field is as follows: 1

eWEB_eKERNEL_address_str

This field specifies the IP address of the eKERNEL. In the current release, this value is the same as the eWEB_Address_str field. Therefore, eKERNEL and the Apache Web Server must reside on the same computer. Future releases can implement the architecture of distributed web servers that reside on another system (for example, located in a DMZ).

An example of an entry typically found in this field is as follows: 10.100.50.138

eWEB_Branding_str

This field is introduced in R3.0 and defines the branding information shown in eWEB user interface.

Note that tampering with branding information without permission is a copyright violation.

An example of an entry typically found in this field is as follows: NORTEL

eWEB_Comments_str

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

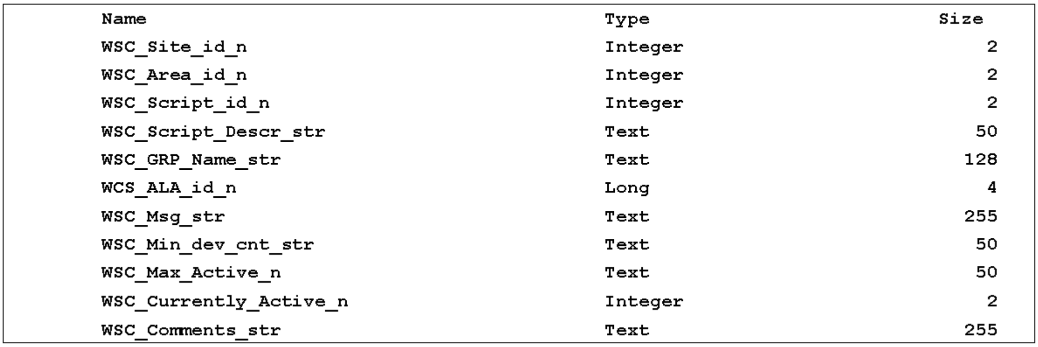
Table 139 shows examples of data found in the eWEB table.

Table 139
eWEB sample data

Address	Site	Area	Kernel address	Comments
10.110.50.138	1	1	10.110.50.138	
10.110.53.138	1	1	10.110.53.138	
127.0.0.1	1	1	127.0.0.1	

Table: eWEB_SCRIPT

Table 140
eWEB parameters



Name	Type	Size
WSC_Site_id_n	Integer	2
WSC_Area_id_n	Integer	2
WSC_Script_id_n	Integer	2
WSC_Script_Descr_str	Text	50
WSC_GRP_Name_str	Text	128
WCS_ALA_id_n	Long	4
WSC_Msg_str	Text	255
WSC_Min_dev_cnt_str	Text	50
WSC_Max_Active_n	Text	50
WSC_Currently_Active_n	Integer	2
WSC_Comments_str	Text	255

WSC_Site_id_n

This field specifies the site, as defined in eKERNEL_SITE table. In most environments, the value is 1.

An example of an entry typically found in this field is as follows: 1

WSC_Area_id_n

This field specifies the area, as defined in eKERNEL_AREA table. In most cases the value is 1.

An example of an entry typically found in this field is as follows: 1

WSC_Script_id_n

This field specifies the unique identifier of the script message within one site.

Script messages are a special type of message requests with the unique feature of being traceable.

Although you are free to enter a numeric value of choice, Nortel recommends establishing a naming convention for script messages.

In the field ALA_Trace_b of the eKernel_alarm table, the administrator can activate this field (note that this feature is supported only for script messages in the current release), which means that the whole call flow is logged in the data database.

An example of an entry typically found in this field is as follows: 1

WSC_Script_Descr_str

This field is a description of the script message.

In the eWeb module, the visualization of the script message is performed with the description of the script message, and never with the script ID.

An example of an entry typically found in this field is as follows: EMERGENCY

WSC_GRP_Name_str

This parameter specifies the name of the group as defined in the field GRP_Name_str in the eKernel_group table or another valid text is *ALL.

If this field is equal to *ALL, the user can select a group, otherwise the group (the message destinations) are fixed.

The groups are presented as message destinations.

If the group name defined does not match a group name in the eKernel_group table, no devices are shown, so the alarm is not processed.

An example of an entry typically found in this field is as follows: EVACUATION

WCS_ALA_id_n

This field must have a value that corresponds with any of the definitions in the eKernel_alarm table for input program related to eWEB. For example, if eWEB is input program 11701 and eKernel_alarm table contains alarm identifiers 1170101 and 1170102, one of these defined values must be used. In most cases, a number of alarm identifiers are defined to handle different message lengths and different message priorities.

An example of an entry typically found in this field is as follows: 1170101

WSC_Msg_str

This field describes the message that is sent to the group members. Nortel recommends that you add a descriptive message that allows the recipient sufficient information to handle the alarm condition. Mobile users often lack immediate access to other information resources, such as a site map or technical specification. Nortel recommends that you keep the message length less than or equal to the maximum length defined in the associated eKERNEL_ALARM table.

*FREE is the only other valid entry. This keyword enables the end user to enter a message.

An example of an entry typically found in this field is as follows: EVACUATION is active

WSC_Min_dev_cnt_str

This field specifies the minimum number of devices that must be selected from the group by the end user, before a script message can be activated. The only other valid entry in the current release is *ALL; therefore, all devices from the group receive the message, so the end user does not have the opportunity to select devices.

Warning: you must not specify a value larger then the number of devices present in the group.

> ***Note:*** In the current release, this parameter has nothing to do with the number of devices that must receive the message before clearing the message for all other devices from the group.

An example of an entry typically found in this field is as follows: *ALL

WSC_Max_Active_n

This field specifies the maximum number of times this script message can be active. The keyword *NOMAX can be used to indicate there is no limit.

An example of an entry typically found in this field is as follows: 1 (for EVACUATION) or *NOMAX (for informative messages)

WSC_Currently_Active_n

This field specifies the number of script messages currently active.

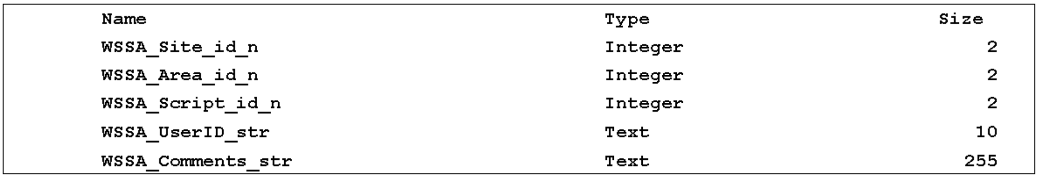
This field is used by the eKernel application, and has nothing to do with configuration of the database.

WSCA_Comments_str

This field can be used by an administrator to enter remarks. The field is informational only.

Table: eWEB_SCRIPT_SET_AUTH

Table 141
eWEB_SCRIPT_SET_AUTH parameters



Name	Type	Size
WSSA_Site_id_n	Integer	2
WSSA_Area_id_n	Integer	2
WSSA_Script_id_n	Integer	2
WSSA_UserID_str	Text	10
WSSA_Comments_str	Text	255

WSSA_Site_id_n

This field specifies the site, as defined in eKERNEL_SITE table. In most environments, the value is 1.

An example of an entry typically found in this field is as follows: 1

WSSA_Area_id_n

This field specifies the area, as defined in eKERNEL_AREA table. In most cases the value is 1.

An example of an entry typically found in this field is as follows: 1

WSSA_Script_id_n

This field must have a value that corresponds with any of the definitions in eWEB_script table for the eWEB interface.

An example of an entry typically found in this field is as follows: 1

WSSA_UserID_str

This field must have a username that corresponds with the USERA_UserID_str field of the eWeb_user_auth table or can be the keyword *ALL.

If the value *ALL is entered, any user can set this script message. If one or more users are defined, only those users can set the related script message.

If nothing configured in this table for a specific script message, no one can activate this script message.

An example of an entry typically found in this field is as follows: KDS

WSSA_Comments_str

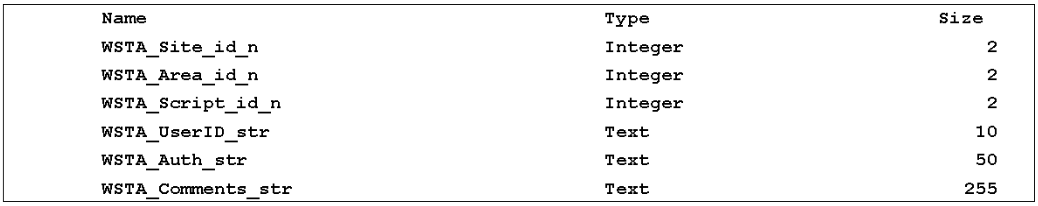
This field can be used by an administrator to enter remarks. The field is informational only.

Table: eWEB_SCRIPT_TRACE_AUTH

Note 1: Note: An alarm is only traceable for script message if the ALA_Trace_b alarm ID related to the script message has the field ALA_Trace_b in the eKERNEL_ALARM table set to True.

Note 2: In the current release, traceable alarms are only supported for script messages.

Table 142
eWEB_SCRIPT_TRACE_AUTH parameters



Name	Type	Size
WSTA_Site_id_n	Integer	2
WSTA_Area_id_n	Integer	2
WSTA_Script_id_n	Integer	2
WSTA_UserID_str	Text	10
WSTA_Auth_str	Text	50
WSTA_Comments_str	Text	255

WSTA_Site_id_n

This field specifies the site, as defined in eKERNEL_SITE table. In most environments, the value is 1.

An example of an entry typically found in this field is as follows: 1

WSTA_Area_id_n

This field specifies the area, as defined in eKERNEL_AREA table. In most cases the value is 1.

An example of an entry typically found in this field is as follows: 1

WSTA_Script_id_n

This field must have a value that corresponds with any of the definitions in eWEB_script table for the eWEB interface.

An example of an entry typically found in this field is as follows: 1

WSTA_UserID_str

This field must have a username that corresponds with the USERA_UserID_str field of the eWeb_user_auth table or can be the keyword *ALL.

If the value *ALL is entered, any user can trace this script message. If one or more users are defined, only those users can trace the related script message.

If nothing configured in this table for a specific script message, no one can trace this script message.

An example of an entry typically found in this field is as follows: KDS

WSTA_Auth_str

This field is provided for security enhancements in future releases.

Only the value *VIEW and *EXCLUDE are supported in the current release.

If the end user must have the authority to trace a script message, this field must be *VIEW. *EXCLUDE is similar to not entering a record.

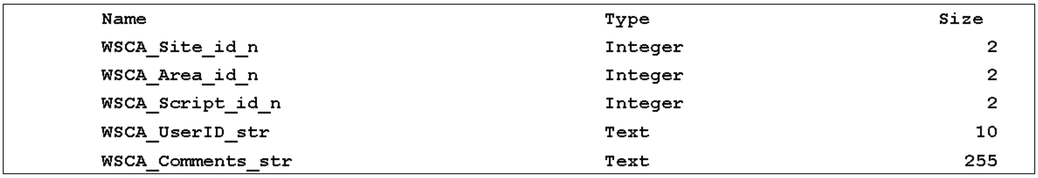
An example of an entry typically found in this field is as follows: *VIEW

WSTA_Comments_str

This field can be used by an administrator to enter remarks. The field is informational only.

Table: eWEB_SCRIPT_CANCEL_AUTH

Table 143
eWEB_SCRIPT_CANCEL_AUTH parameters



Name	Type	Size
WSCA_Site_id_n	Integer	2
WSCA_Area_id_n	Integer	2
WSCA_Script_id_n	Integer	2
WSCA_UserID_str	Text	10
WSCA_Comments_str	Text	255

WSCA_Site_id_n

This field specifies the site, as defined in eKERNEL_SITE table. In most environments, the value is 1.

An example of an entry typically found in this field is as follows: 1

WSCA_Area_id_n

This field specifies the area, as defined in eKERNEL_AREA table. In most cases, the value is 1.

An example of an entry typically found in this field is as follows: 1

WSCA_Script_id_n

This field must have a value that corresponds with any of the definitions in eWEB_script table for the eWEB interface.

An example of an entry typically found in this field is as follows: 1

WSCA_UserID_str

This field must have a username that corresponds with the USERA_UserID_str field of the eWeb_user_auth table or can be the keyword *ALL.

If the value *ALL is entered, any user can cancel this script message. If one or more users are defined, only those users can cancel the related script message.

If nothing configured in this table for a specific script message, no one can cancel this script message.

An example of an entry typically found in this field is as follows: Admin

WSCA_Comments_str

This field can be used by an administrator to enter remarks. The field is informational only.

Table: eWEB_SNDGRPMSG

Table 144
eWEB_SNDGRPMSG parameters

Name	*Type*	*Size*
WGM_Site_id_n	Integer	2
WGM_Area_id_n	Integer	2
WGM_GRP_Name_str	Text	128
WGM_Sequence_n	Integer	2
WGM_Message_str	Text	80
WGM_AlA_id_n	Long Integer	4
WGM_Comments_str	Text	255

WGM_Site_id_n

This field specifies the site identifier, as described in table eKERNEL_SITE. In most cases this value is 1.

An example of an entry typically found in this field is as follows: 1

WGM_Area_id_n

This field specifies the area identifier, as described in table eKERNEL_AREA. In most cases this value is 1.

An example of an entry typically found in this field is as follows: 1

WGM_GRP_Name_str

This field specifies the group, as defined in eKERNEL_GROUP table. The Send Group Message function in eWEB allows sending a predefined message to a group. The table eWEB_SNDGRPMSG allows a system administrator to predefine a number of messages that are automatically presented to a web user in the web-based Send Group Message functionality.

The field can either contain a qualified group name or can have the generic special value *ALL. This special value *ALL means the message is automatically defined for all groups. You must use this value only when appropriate, as sharing messages affects all groups.

When entering a value in this field, ensure that the specified group name exists in the eKERNEL_GROUP table, and that the eKERNEL_GROUP_MEMBER contains at least one member.

An example of an entry typically found in this field is as follows: 00001 (qualified group) or *ALL (generic group)

WGM_Sequence_n

This field is a sequence number and makes the records unique in the database. The field allows you to define the sequence used to present the data in the Send Group Message function. Nortel recommends that you start with a value of 1 and increase by one for subsequent messages.

An example of an entry typically found in this field is as follows: 1

WGM_Message_str

This field specifies the message that is shown to the eWEB user in the Send Group Message functionality, and is finally sent to the destination users.

Note the length of the message must be smaller than or equal to the maximum length associated with the WGM_AlA_id_n definition in eKERNEL_ALARM table. For example, when an alarm identifier defines maximum length in eKERNEL_ALARM table of 48 bytes, the specified message must not be longer that 48 bytes. A special value *FREE can be defined, enabling the end user to enter a message.

An example of an entry typically found in this field is as follows: Evacuation (qualified) or *FREE (user-defined message)

WGM_AlA_id_n

This field must have a value that corresponds with any of the definitions in eKERNEL_ALARM table for the eWEB interface. For example, if eWEB is input program 11701 and ALARM table contains alarm identifiers 1170101 and 1170102 and 1170103, one of these defined values must be used. In most cases, a number of alarm identifiers are defined to handle different message lengths and different message priorities.

An example of an entry typically found in this field is as follows: 1170101

WGM_Comments_str

This field can be used by and administrator to enter some remarks. The field is informational only.

Table 145 shows examples of data found in the eWEB_SNDGRPMSG table.

Table 145
eWEB_SNDGRPMSG sample data (Part 1 of 2)

Site	Area	Group	Sequence	Message	Alarm id	Comments
3	1	*ALL	1	Emergency - evacuation	3170103	
3	1	*ALL	2	*FREE	3170102	
3	1	1	1	AS400 failure	3170102	
3	1	1	2	NT failure	3170102	
3	1	1	3	Domino failure	3170102	
3	1	1	4	Firewall failure	3170102	
3	1	2	1	Check invoice	3170102	
3	1	2	2	Check mailbox	3170102	
3	1	2	3	Check quotations	3170102	
3	1	2	4	Check received goods	3170102	
3	1	EMERGENCY	1	Fase 1 - start	3170102	
3	1	EMERGENCY	2	Fase 2 - start	3170102	
3	1	EMERGENCY	3	Fase 3 - start	3170102	

Table 145
eWEB_SNDGRPMSG sample data (Part 2 of 2)

3	1	EMERGENCY	4	Fase 1 - end	3170102	
3	1	EMERGENCY	5	Fase 2 - end	3170102	
3	1	EMERGENCY	6	Fase 3 - end	3170102	
3	1	VSK_F	1	Brand - gelijkvloers	3170102	
3	1	VSK_F	2	Brand - verdieping 1	3170102	
3	1	VSK_F	3	Brand - verdieping 2	3170102	

Table: eWEB_SNDUSRMSG

Table 146
eWEB_SNDUSRMSG parameters

Name	*Type*	*Size*
WUM_User_id_str	Text	10
WUM_Sequence_n	Integer	2
WUM_Message_str	Text	80
WUM_AlA_id_n	Long Integer	4
WUM_Comments_str	Text	255

WUM_User_id_str

This field specifies the user, as defined in eWEB_USER_AUTH table. The user is defined at the login process, where the web user enters a valid user and password. This user name is stored in the Web browser and reused as needed when authentication is needed for Web requests. The table eWEB_SNDUSRMSG allows a system administrator to predefine a number of messages that are automatically presented to a web user in the web-based Send User Message functionality.

The field can either contain a qualified username or can have the generic special value *ALL. This special value *ALL means the message is defined for all users.

An example of an entry typically found in this field is as follows: 00001 (qualified user) or *ALL (generic user)

WUM_Sequence_n

This field is sequence number and makes the WUM_User_id_str and WUM_Sequence_n a unique key. Use WUM_Sequence_n to define the sort sequence of the available predefined messages. Nortel recommends that you start with a value of 1 and increase by one for subsequent messages.

An example of an entry typically found in this field is as follows: 1

WUM_Message_str

This field specifies the message that is shown to the eWEB user in the Send User Message functionality, and finally is sent to the destination users. Note the length of the message must be smaller than or equal to the maximal length associated with the WUM_AlA_id_n definition in eKERNEL_ALARM table. For example, when an alarm identifier defines maximum length in eKERNEL_ALARM table of 48 bytes, the specified message must not be longer that 48 bytes. A special value *FREE can be defined, enabling the end user to enter a message.

An example of an entry typically found in this field is as follows: Evacuation (qualified) or *FREE (user-defined message)

WUM_AlA_id_n

This field must have a value that corresponds with any of the definitions in ALARM table for the eWEB interface. For example, if eWEB is input program 11701 and eKERNEL_ALARM table contains alarm identifiers 1170101 and 1170102 and 1170103, one of these defined values must be used. In most cases, a number of alarm identifiers are defined to handle different message lengths and different message priorities.

An example of an entry typically found in this field is as follows: 1170101

WGM_Comments_str

This field can be used by and administrator to enter some remarks. The field is informational only.

Table 147 shows examples of data found in the eWEB_SNDUSRMSG table.

Table 147
eWEB_SNDUSRMSG sample data (Part 1 of 2)

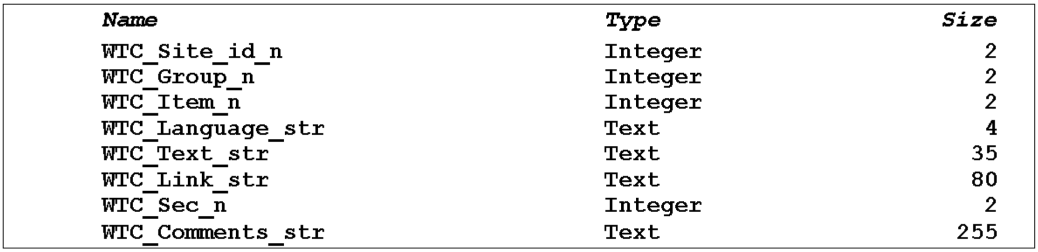
User	Sequence	Message	Alarm id	Comments
*ALL	1	Normal message 1 for *ALL	3170101	
*ALL	2	Shared message 2 for *ALL	3170101	

Table 147
eWEB_SNDUSRMSG sample data (Part 2 of 2)

*ALL	3	Shared message 3 for *ALL	3170101	
*ALL	4	Shared message 4 for *ALL	3170101	
*ALL	5	Shared message 5 for *ALL	3170101	
*ALL	6	Shared message 6 for *ALL	3170101	
*ALL	7	*FREE	3170101	
FMI	1	Private message 1 for FMI	3170103	
FMI	2	Private message 2 for FMI	3170103	
FMI	3	Private message 3 for FMI	3170103	
FMI	4	Private message 4 for FMI	3170103	
KDS	1	Private message 1 (Medium)	3170102	
KDS	2	Private message 2 (Short)	3170101	
KDS	3	Private message 3 (Long)	3170103	

Table: eWEB_TOC

Table 148
eWEB_TOC parameters



Name	*Type*	*Size*
WTC_Site_id_n	Integer	2
WTC_Group_n	Integer	2
WTC_Item_n	Integer	2
WTC_Language_str	Text	4
WTC_Text_str	Text	35
WTC_Link_str	Text	80
WTC_Sec_n	Integer	2
WTC_Comments_str	Text	255

WTC_Site_id_n

This field specifies the site identifier, as defined in eKERNEL_SITE table. The site is in most cases equal to 1.

The Web Server determines its site and area based upon its own IP address, as defined in the eWEB table.

An example of an entry typically found in this field is as follows: 1.

WTC_Group_n

This field contains a numeric sequence number, which is combined with WTC_Item_n and WTC_Language_str to generate a key. The key is unique within the site. WTC_Group_n is used to logically sort the table of contents in groups and items. Nortel recommends starting the first group at 1 and incrementing by 1.

An example of an entry typically found in this field is as follows: 1.

WTC_Item_n

This field contains a numeric sequence number, which is combined with WTC_Group_n, and WTC_Language_str to generate a key. The key is unique within the site. WTC_Item_n is used to logically sort table of contents in groups and items. Nortel recommends starting the first item in a group at 1 and incrementing by 1.

An example of an entry typically found in this field is as follows: 1.

WTC_Language_str

This field contains a 4-byte language code. Refer to the documentation of the “Table: eWEB_USER_AUTH” on page 1515 for a list of language codes. This field contains a number, and when combined with WTC_Group_n, and WTC_Item_n, results in a key, which is not duplicated within a site.

This field specifies the language used in the field WTC_Text_str, and in the PHP script of HTML documents defined in WTC_Link_str.

This field allows the table of contents to be multilingual. With the correct definition, English users see the table of contents in English, Dutch users in Dutch, and so on.

To implement a new language:

1 Define the appropriate language code in the eWEB_USER_AUTH table.

2 Translate the descriptions of the links in the eWEB_TOC table.

3 Edit the eWeb_mri.php file that is located in C:\SOPHO Messenger@Net\Web\htdocs.

4 Provide an additional section for the new language.
The eWeb_mri.php is provided in English (2909), and Dutch (2963).

An example of an entry typically found in this field is as follows: 2909.

WTC_Text_str

This field specifies the text that the web user sees in the table of contents. Nortel recommends using the same language as specified in the field WTC_Language_str.

An example of an entry typically found in this field is as follows: Welcome (in English - 2909) or Welkom (in Dutch - 2963).

WTC_Link_str

This field specifies the hyperlink associated with the table of contents. If blank, the hyperlink is inactive. This is typically used to logically group menu options in different sections, and define such empty link for the header of each section. See the sample in Table 149 for more information.

In most cases, this field contains a valid filename of a PHP-script, a HTML-filename of another valid string understood by a browser (for example, mailto:francis.missiaen@1s.be).

Table 149 provides a list of valid links that can be used. The files are shipped with eWEB module and are located in C:\SOPHO Messenger@Net\Web\htdocs.

Table 149
Valid WTC_Link_str values

eWEB_alarm_inquiry.php
eWEB_chgpwd.php
eWEB_device_inquiry.php
eWEB_eDMSAPI.php
eWEB_eSMTP.php
eWEB_group_inquiry.php
eWEB_script.php
eWEB_sndgrpmsg_1.php
eWEB_sndsrvmsg.php
eWEB_sndusrmsg_1.php
eWEB_table_view.php
eWeb_wrkgrp_1.php
info.html
mailto:francis.missiaen@1s.be
1s/launch.htm

An example of an entry typically found in this field is as follows: eWEB_eDMSAPI.php

WTC_Sec_n

This field specifies whether a user can see table of contents items. For example, a user with security level 20 defined in the eWEB_USER_AUTH table sees only the table of contents items defined in the eWEB_TOC table with a WTC_Sec_n value lower than or equal to 20. WTC_Sec_n provides a method to restrict access to some functionality to a subset of users.

An example of an entry typically found in this field is as follows: 20

WTC_Comments_str

This fields can be used by an administrator to enter remarks. The field is informational only.

Table 150 shows examples of data found in the eWEB_TOC table. Figure 606 shows an example of the eWEB_TOC result for language 2909 and language 2963.

Table 150
eWEB_TOC sample configuration (Part 1 of 3)

Site	Group	Item	Language	Text	Link	Level
3	2	0	2909	Send a message		10
3	2	0	2963	Zend een boodschap		10
3	2	1	2909	Send DMS-API message	eWEB_eDMSAPI.php	10
3	2	1	2963	Zend DMS-API boodschap	eWEB_eDMSAPI.php	10
3	2	2	2909	Send SMTP message	eWEB_eSMTP.php	10
3	2	2	2963	Zend SMTP boodschap	eWEB_eSMTP.php	10
3	2	3	2909	Send Server Message	eWEB_sndsrvmsg.php	10

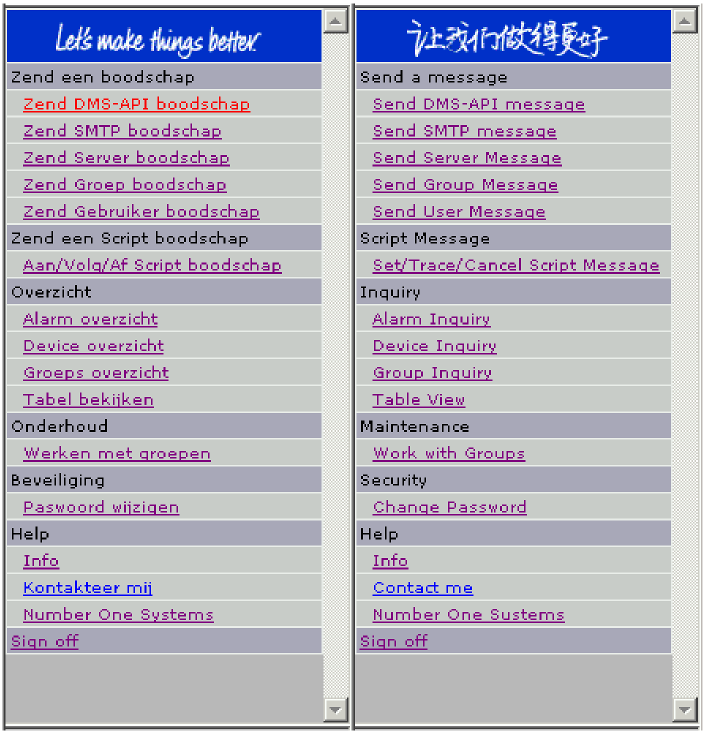
Table 150
eWEB_TOC sample configuration (Part 2 of 3)

3	2	3	2963	Zend Server boodschap	eWEB_sndsrvmsg.php	10
3	2	4	2909	Send Group Message	eWEB_sndgrpmsg_1.php	10
3	2	4	2963	Zend Groep boodschap	eWEB_sndgrpmsg_1.php	10
3	2	5	2909	Send User Message	eWEB_sndusrmsg_1.php	10
3	2	5	2963	Zend Gebruiker boodschap	eWEB_sndusrmsg_1.php	10
3	3	0	2909	Send a script message		40
3	3	0	2963	Zend een script boodschap		40
3	3	1	2909	Work with Script messages	eWEB_script.php	40
3	3	1	2963	Werken met Script boodschappen	eWEB_script.php	40
3	4	0	2909	Inquiry		20
3	4	0	2963	Overzicht		20
3	4	1	2909	Alarm Inquiry	eWEB_alarm_inquiry.php	20
3	4	1	2963	Alarm overzicht	eWEB_alarm_inquiry.php	20
3	4	2	2909	Device Inquiry	eWEB_device_inquiry.php	20
3	4	2	2963	Device overzicht	eWEB_device_inquiry.php	20
3	4	3	2909	Group Inquiry	eWEB_group_inquiry.php	20
3	4	3	2963	Groeps overzicht	eWEB_group_inquiry.php	20
3	4	4	2909	Table View	eWEB_table_view.php	20
3	4	4	2963	Tabel bekijken	eWEB_table_view.php	20
3	5	0	2909	Maintenance		30
3	5	0	2963	Onderhoud		30
3	5	1	2909	Work with Groups	eWeb_wrkgrp_1.php	30

Table 150
eWEB_TOC sample configuration (Part 3 of 3)

3	5	1	2963	Werken met groepen	eWeb_wrkgrp_1.php	30
3	6	0	2909	Security		10
3	6	0	2963	Beveiliging		10
3	6	1	2909	Change Password	eWEB_chgpwd.php	10
3	6	1	2963	Paswoord wijzigen	eWEB_chgpwd.php	10
3	7	0	2909	Help		40
3	7	0	2963	Help		40
3	7	1	2909	Info	info.html	40
3	7	1	2963	Info	info.html	40
3	7	2	2909	Contact me	mailto:francis.missiaen@1s.be	40
3	7	2	2963	Kontakteer mij	mailto:francis.missiaen@1s.be	40
3	7	3	2909	Number One Systems	1s/launch.htm	40
3	7	3	2963	Number One Systems	1s/launch.htm	40

Figure 606
eWEB_TOC sample result (language 2909 and language 2963)



Zend een boodschap
- Zend DMS-API boodschap
- Zend SMTP boodschap
- Zend Server boodschap
- Zend Groep boodschap
- Zend Gebruiker boodschap

Zend een Script boodschap
- Aan/Volg/Af Script boodschap

Overzicht
- Alarm overzicht
- Device overzicht
- Groeps overzicht
- Tabel bekijken

Onderhoud
- Werken met groepen

Beveiliging
- Paswoord wijzigen

Help
- Info
- Kontakteer mij
- Number One Systems

Sign off

Send a message
- Send DMS-API message
- Send SMTP message
- Send Server Message
- Send Group Message
- Send User Message

Script Message
- Set/Trace/Cancel Script Message

Inquiry
- Alarm Inquiry
- Device Inquiry
- Group Inquiry
- Table View

Maintenance
- Work with Groups

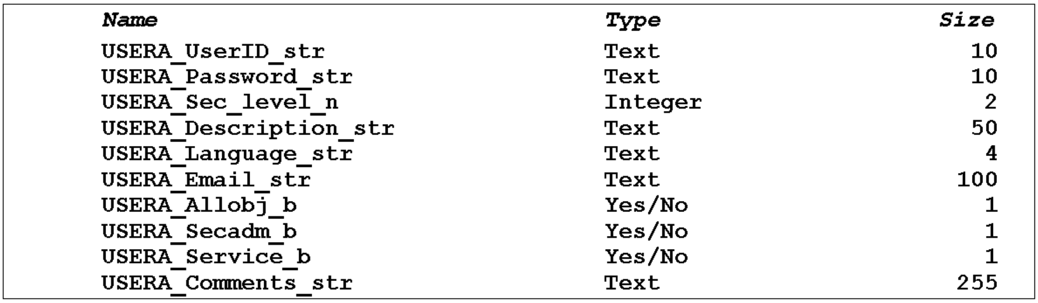
Security
- Change Password

Help
- Info
- Contact me
- Number One Sustems

Sign off

Table: eWEB_USER_AUTH

Table 151
EWEB_USER_AUTH parameters



Name	*Type*	*Size*
USERA_UserID_str	Text	10
USERA_Password_str	Text	10
USERA_Sec_level_n	Integer	2
USERA_Description_str	Text	50
USERA_Language_str	Text	4
USERA_Email_str	Text	100
USERA_Allobj_b	Yes/No	1
USERA_Secadm_b	Yes/No	1
USERA_Service_b	Yes/No	1
USERA_Comments_str	Text	255

USERA_UserID_str

This field contains a User ID. The eWEB module must define at least one user profile for authentication purposes. Nortel recommends that you create a user profile for each user that has access to the eWEB interface, to avoid alarms generated by unauthenticated users.

> ***Note 1:*** In many environments, other computer infrastructure is in use, such as iSeries 400, Windows NT, Lotus Notes, and so on, and users often desire to use the same username on every platform. In this case, Nortel recommends that you ask the ICT manager for a list of existing user profiles, so that DECT Messenger can use the same User IDs. On iSeries 400 the OS/400, command WRKUSRPRF can be used to determine defined users.
>
> ***Note 2:*** The USERA_UserID_str field is restricted to a length of 10 bytes.

An example of an entry typically found in this field is as follows: FMI.

USERA_Password_str

This field contains a 10-byte password. The eWEB interface allows users to change their own password. Therefore you can create new users with default passwords (for example, the same as the User ID), and ask users to change their password when they log in for the first time.

> ***Note:*** eWEB stores passwords without encryption in the Access 2000 database, and are therefore available to anyone who can access the DECT Messenger system. Depending on your configuration, table information is accessible through eWEB. Because the security mechanism is limited, Nortel recommends that users *not* use the same password used on other systems that contain secured information, as that poses a serious security risk. Inform all users of this important issue.

An example of an entry typically found in this field is as follows: SOPHO.

USERA_Sec_level_n

The security level is a number between 00 and 99. The higher the number, the more authority a user has. The value 99 is the highest level, and gives full access to all functionality. The value 00 is the lowest possible value. Nortel recommends that you initially assign values in 2 or 3 levels and handle increment by 10. For instance, start with the following values: 20 for low-end users, 40 for power users, and 60 for administrators.

> ***Note:*** The security level is related to the values specified in the eWEB_TOC table, where the field WTC_Sec_n level specifies the minimum required user security level that is needed for a specified function. For example, a user with level 20 can execute all the functions in WTC_Sec_n with level 00–20.

An example of an entry typically found in this field is as follows: 40.

USERA_Description_str

This field contains a description of the user, which usually consists of the first and last name of the User ID. This field is informational only.

An example of an entry typically found in this field is as follows: Francis Missiaen.

USERA_Email_str

This field specifies the e-mail address of the user. This field is important when eWEB module is activated, and the Send SMTP Message function is available to the users. When a user sends an e-mail message through the Send SMTP Message script, the system checks the username of the eWEB user, as specified during the login procedure. The e-mail address of the user is retrieved based on the User ID, and is used in the MAIL FROM tag of the mail composition process, as defined in the RFC821 specifications.

An example of an entry typically found in this field is as follows: francis.missiaen@1s.be.

USERA_Allobj_b

This field specifies whether a user has the authority to access all objects. In most cases the value False (0) is used. This means the user does not have authority to access all objects. Instead, the user only has access to maintain the groups he or she has been granted access to, as defined in the eKERNEL_GROUP_AUTH table.

If your environment requires it, you can create users with administrator privileges, who are allowed to maintain any existing group through the eWEB based Work with Groups. To do so, set this field to True (-1) to grant the all object special authority to these users. Users with all object special authority do not need to be granted authority in the eKERNEL_GROUP_AUTH table.

Nortel recommends giving this special authority only to system administrators and service staff.

An example of an entry typically found in this field is as follows: 0 (denotes False).

USERA_Secadm_b

This field specifies whether a user has security administrator special authority. If this value is set to False (0), the user has access to all tables in the Table View within eWEB, except eWEB_USER_AUTH, which shows usernames and passwords in plain text.

If your environment requires it, you can create users with administrator privileges, who are allowed to maintain any user profile in eWEB. For those users, set this field to True (-1) to allow those users to consult the table eWEB_USER_AUTH, and see the user and password information.

> ***Note:*** The web interface only supports inquiry to the tables. Maintenance of the tables must be performed using the eGRID interface.

An example of an entry typically found in this field is as follows: 0 (denotes False).

USERA_Service_b

This value is not implemented in the current release. Nortel recommends using the value False (0). This feature will be used in future releases to grant access to service functions that can be implemented in eWEB at a later stage.

An example of an entry typically found in this field is as follows: 0 (denotes False).

USERA_Language_str

This field contains a 4-byte identifier that denotes the language used for eWEB-access and eGRID-access. Enter one of the valid language codes provided in Table 152. The codes are in the range 2900–2999. A small number of languages are currently supported, but additional languages can be implemented if needed.

Table 152 shows the codes for currently supported languages, while Table 153 on page 1519 shows codes reserved for future language support.

Table 152
Currently supported language values in eWEB

Code	Language
2909	Belgian English
2963	Belgian Dutch
2966	Belgian French

Table 153
Language values reserved for future implementation (Part 1 of 3)

Code	Language
2902	Estonian
2903	Lithuanian
2904	Latvian
2905	Vietnamese
2906	Lao
2911	Slovenian
2912	Croatian
2913	Macedonian
2914	Serbian Cyrillic
2922	Portuguese
2923	Dutch Netherlands
2924	English
2925	Finnish
2926	Danish
2928	French
2929	German
2931	Spanish
2932	Italian
2933	Norwegian
2937	Swedish
2938	English Uppercase Support for Double-Byte Character Set (DBCS)

Table 153
Language values reserved for future implementation (Part 2 of 3)

Code	Language
2939	German Multinational Character Set
2940	French Multinational Character Set
2942	Italian Multinational Character Set
2950	English Uppercase
2954	Arabic
2956	Turkish
2957	Greek
2958	Icelandic
2961	Hebrew
2962	Japanese Double-Byte Character Set (DBCS)
2972	Thai
2974	Bulgarian
2975	Czech
2976	Hungarian
2978	Polish
2979	Russian
2980	Brazilian Portuguese
2981	Canadian French
2984	English Uppercase and Lowercase Support for Double-Byte Character Set (DBCS)
2986	Korean Double-Byte Character Set (DBCS)
2987	Traditional Chinese Double-Byte

Table 153
Language values reserved for future implementation (Part 3 of 3)

Code	Language
	Character Set (DBCS)
2989	Simplified Chinese Double-Byte Character Set (DBCS) (PRC)
2992	Romanian
2994	Slovakian
2995	Albanian
2996	Portuguese Multinational Character Set
2998	Farsi

> ***Note:*** The language-code corresponds with an entry in eGRID that provides a directory where the language dependent files are stored. This path is usually C:\SOPHO Messenger@Net\pdf\mri29xx. The concept of multi-lingual support in the eWEB module is implemented in the file eWeb_mri.php that is located in C:\SOPHO Messenger@Net\Web\htdocs.

An example of an entry typically found in this field is as follows: 2909.

USERA_Comments_str

Use this field to record remarks about the user.

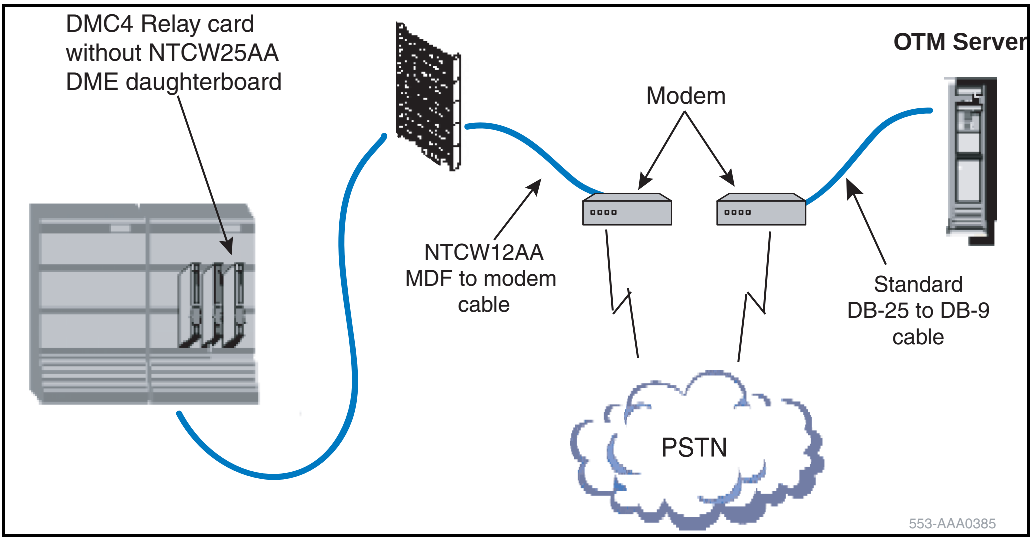
An example of an entry typically found in this field is as follows: Technical manager.

Appendix A: Connecting to OTM DECT using remote modems

Cable setup

It is possible to manage a DECT system remotely with the OTM DECT manager using two modems connected to the Public Switched Telephone Network (PSTN). This works for SNMP DECT systems with a DMC8 or DMC4 relay card. Figure 607 on page 1523 shows the DMC8 relay card connected to a remote OTM server.

Figure 607
DMC8 relay card connection to a remote OTM server



DECT relay board to remote modem

Refer to Table 154 when connecting the NTCW12AA cable to the MDF.

Table 154
NTCW12AA cable to MDF connections

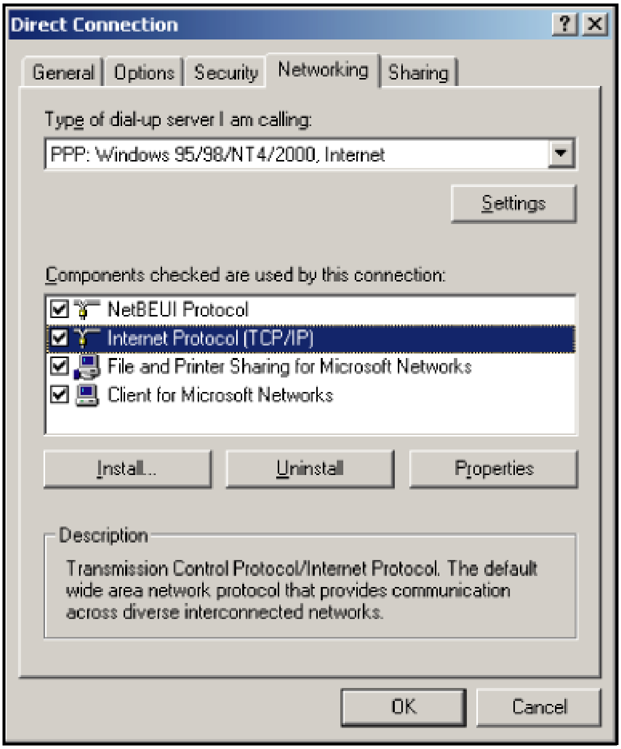
DMC Relay card MDF connection	Cable colour	DB-25 connector pin number	Signal designator
T1	Gray	8	V.24DCD
R2	Yellow	4	V.24RTS
T3	Blue	2	V.24TXD
R3	Red	3	V.24RXD
T4	Pink	7	V.24GND

Note: The BIX tip and ring connections shown in Table 154 on page 1524 correspond to standard BIX designation. The first pair is labeled T0 and R0. See *System Installation Procedures (553-3001-210)*, “Planning and Designating the MDF” section, for more information.

Configuring NetBEUI Protocol

You must first install NetBEUI Protocol if it is not already installed on the OTM Server PC.

Figure 608
Networking tab of the Local Area Connection Properties



Type of dial-up server I am calling:
PPP: Windows 95/98/NT4/2000, Internet

Components checked are used by this connection:

- ☑ NetBEUI Protocol
- ☑ Internet Protocol (TCP/IP)
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ Client for Microsoft Networks

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

Complete the steps in Procedure 247 to configure NetBEUI Protocol:

Procedure 247
Configuring NetBEUI Protocol

Step	Action
1	Open the **Network and Dial-up Connections** dialog.
	Select **My Network Places**, right-click it, and select **Properties**.
2	Open the **Properties** dialog for **Local Area Connection**.
	Select **Local Area Connection**, right-click it, and select **Properties**. If the NetBEUI Interface Service is already installed, it appears in the **Local Area Connection Properties** dialog (see Figure 608 on page 1525). If NetBEUI Protocol does not appear in the **Local Area Connection Properties** dialog, continue with Steps 3 – 6.
3	Click the **Install** button.
4	Open the **Select Network Protocol** dialog.
	Select Protocol in the **Select Network Component Type** dialog, and click **Add**.
5	Add NetBEUI Protocol.
	Select **NetBEUI Protocol**, and click **OK**. The PC must be rebooted after installing NetBEUI Protocol.

END

Configuring a dial-up network on the OTM server

Complete the steps in Procedure 248 to configure a dial-up network:

Procedure 248
Configuring a dial-up network (Part 1 of 2)

Step	Action
1	Click the **Start** button on the PC taskbar.
2	Select **Settings**.
3	Select **Control Panel**.
4	Double-click **Network and Dial-up Connections**.
5	Double-click **Make New Connection**.
6	Click **Next**.
7	Select the network connection type.
	Select the **Connect directly to another computer** radio button, and click **Next**.
8	Identify your computer as a Guest machine.
	Select the **Guest** radio button, and click **Next**.
9	Select the device to make the connection.
	Select **Communications Port (COM x)** from the **Select a device:** drop-down list, and click **Next**.

Procedure 248
Configuring a dial-up network (Part 2 of 2)

Step	Action
10	Identify the connection availability.
	Select the **For all users** radio button, and click **Next**.
11	Identify the network connection.
	Enter a name for this connection, and click **Finish**.
	END

Setting the properties of the new connection

Complete the steps in Procedure 249 to set the properties of the new connection:

Procedure 249
Configuring connection properties (Part 1 of 3)

Step	Action
1	Click the **Properties** button.
2	Click the **General** tab.
3	Select **Communications Port (COM x)** from the **Select a device:** drop-down list.
4	Click the **Configure** button.
5	Choose **38400** from the **Maximum speed (bps)** drop-down list.

Procedure 249
Configuring connection properties (Part 2 of 3)

Step	Action
6	Verify the modem configuration settings.
	Ensure that all the **Hardware features** check boxes are clear, and click **OK**.
7	Click the **Security** tab.
8	Select the **Security** options.
	Click **Typical** and choose **Allow unsecured password** in the **Security** options.
9	Click the **Networking** tab.
10	Select the dial-up server type.
	Select **PPP: Windows 95/98/NT4/2000, Internet**
11	Configure settings for the dial-up server.
	Click **Settings**, select the three check boxes in the **PPP settings** window, and click **OK**.
12	Click **Internet Protocol (TCP/IP)** and **Client for Microsoft Networks**.
13	Open the **Properties** dialog for Internet Protocol.
	Highlight **Internet Protocol (TCP/IP)** and click **Properties**.
14	Select the **Use the following IP address** radio button.

Procedure 249
Configuring connection properties (Part 3 of 3)

Step	Action
15	Set the IP address.
	Enter an IP address for this connection, and click **OK**. **Note:** The IP address must be unique and in the same range as the IP address of the DECT system. This becomes the Client IP address.
16	Click **OK**.

END

Modem setup

Install the local modem on the PC, then configure the modem.

Modem requirements

The modem requirements are:

- 56 Kbits/s
- Baud rate 38 400 Kbits/s fixed.

When using a US Robotics modem, use factory defaults.

Connect the modem to the required COM port on the PC using a standard DB-25 to DB-9 cable.

Procedure 250
Configuring the local modem

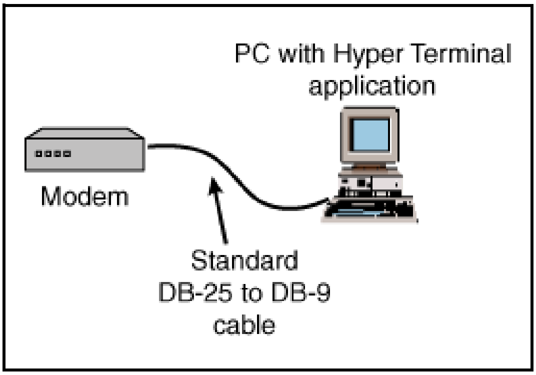
Step	Action
1	Click the **Start** button on the PC taskbar.
2	Select **Settings**.
3	Select **Control panel**.
4	Double-click **Phone and Modems Options**.
5	Click the **Modems** tab.
6	Click the **Add** button.
7	Follow the Wizard.

END

Setting the modems to factory defaults

Connect to the local modem using Hyper Terminal. See Figure 609 on page 1532. Set the remote modem to the factory defaults.

Figure 609
Local modem connected using Hyper Terminal


PC with Hyper Terminal application
Modem
Standard DB-25 to DB-9 cable

Use the initialisation commands in Table 155 to configure the modems.

Table 155
Initialisation commands

Initialisation commands	Meaning
US Robotics:	
AT	
AT&F	Set to factory default
AT&W0	Write setting into non-volatile memory 0
ATY0	At power up, start modem with settings in non-volatile memory 0
Dynalink modem:	
AT	
AT&F	Set to factory default
AT&K0	Flow control disabled
AT&W0	Write setting into non-volatile memory 0
ATY0	At power up, start modem with settings in non-volatile memory 0

Adding a new DECT system to OTM DECT

Before adding the DECT system to OTM DECT, the DECT relay card must be added to the network.

> ***Note:*** When connecting to the DMC8 relay board using modems, jumpers J6, J7, J8, and J9 must be strapped for V.24 on the DMC.

Open the OTM DECT System window. Complete the steps in Procedure 251.

Procedure 251
Adding a new DECT system (Part 1 of 2)

Step	Action
1	Click **File**.
2	Click **Add**.
3	Click the **General** tab.
4	Identify the DECT system name.
	Enter a DECT **System Name**, and click the **Apply** button.
5	Click the **Communication** tab.
6	Enter the **IP Address** of the DECT relay board.
7	Click **Serial**.
8	Click the **Details** button.

Procedure 251
Adding a new DECT system (Part 2 of 2)

Step	Action
9	Enter the **OTM Server IP Interface**.
	This is the IP address entered as the Client IP address in Table 249 on page 1528, Step 15.
10	Choose the COM Port to which the local modem is connected.
11	Enter the **Phone Number** of the remote modem.
12	Click **OK**.
13	Enter values in the **Access Right Identification** and **Parameters** tabs according to normal operating procedures.
14	Click the **Alarm** tab.
15	Define the OTM Server IP Interface IP address.
	Enter the OTM Server IP Interface IP address in the **Upstream Manager IP address** field.
16	Click the **Apply** button
17	Click the **OK** button.
	The DECT system is now added to OTM DECT. All the OTM DECT features and functions continue to operate normally. ***Note:*** The modem connection can slow the completion time for some operations.

END

Changing an existing DECT system on OTM DECT from an Ethernet connection to a modem connection

It is possible to manage a DECT system, which was previously managed using an Ethernet connection, using modems.

To change an Ethernet connection to a modem connection, you must first install the modem (see “Cable setup” on page 1523 and “DECT relay board to remote modem” on page 1524), and complete all the steps in “Configuring NetBEUI Protocol” on page 1524. Then complete the steps in Procedure 252.

> ***Note:*** When connecting to the DECT relay board using modems, jumpers J6, J7, J8, and J9 must be strapped for V.24 on the DMC.

Complete the following steps to change an Ethernet connection to a modem connection:

Procedure 252
Changing an Ethernet connection to a modem connection (Part 1 of 2)

Step	Action
1	Select the DECT system that you want to change from an Ethernet connection to a modem connection.
	Open the OTM DECT System window, and select the DECT system to be changed.
2	Select **File** > **Properties**.
	Select **File** on the toolbar, and select **Properties** from the **File** menu. The **Properties** window opens.
3	Click the **Communication** tab.
4	Select the **Serial** radio button.
5	Click the **Details** button.

Procedure 252
Changing an Ethernet connection to a modem connection (Part 2 of 2)

Step	Action
6	Enter the **OTM Server IP Interface**.
	This is the IP address entered as the Client IP address in Table 249 on page 1528, Step 15.
7	Choose the COM port to which the local modem is connected.
8	Enter the **Phone Number** of the remote modem.
9	Click **OK**.
10	Enter values in the **Access Right Identification** and **Parameters** tabs according to normal operating procedures.
11	Click the **Alarm** tab.
12	Enter the OTM Server IP Interface IP address in the **Upstream Manager IP address** text box.
13	Click the **Apply** button.
14	Click **OK**.
	It is now possible to manage the DECT system using the modem connection. All the OTM DECT features and functions continue to operate normally. ***Note:*** The modem connection can slow the completion time for some operations.

END

Appendix B: Adding a DMC8 to a non-SNMP DECT system

Overview

It is possible to add DMC8 cards to a DECT system that previously contained only DMC4 cards. The system becomes an SNMP system. Therefore, OTM DECT is used for management.

> ***Note 1:*** If the DMC8 is not new, ensure that the card has no subscriptions, or PARI/SARI, and has a known IP address. (Default IP address is 192.168.1.1.)
>
> ***Note 2:*** Nortel recommends that you avoid having the relay card (DMC8) as the lowest card in the system. Additional DMC8 cards can be positioned in lower slots.

IMPORTANT!

It is very important that all the DMC4 cards in the system have the latest non-SNMP firmware (45000405) before adding a DMC8 to a non-SNMP DECT system.

Procedure 253
Adding a DMC8 (Part 1 of 2)

Step	Action
1	Connect the DMC8 to the OTM DECT manager.
	Caution: Do not connect the faceplate connectors between the DMC4 and DMC8 at this time.
2	Create a new DECT system.
	Use the OTM DECT standard procedure to create a new DECT system. **Note:** The DMC8 is the only board visible on OTM DECT at this time. **Caution:** Ensure that the System Parameters on the DMC8 are the same as the existing DECT system. The System Parameters on the DMC8 become the System Parameters for the complete system.
3	Upload the DMC4 SNMP software (45100xxx).
4	Replace the terminators in their new location.
5	Connect the faceplate connectors.
	Note: DMC4 cards can reboot at this point — this is normal. The DMC8 continues to be the only board visible on OTM DECT until the SNMP firmware is activated on all DMC4 cards.

Procedure 253
Adding a DMC8 (Part 2 of 2)

Step	Action
6	Activate the DMC4 SNMP firmware.
	Note 1: If you receive system notifications on OTM DECT (this can occur because the DMC4 cards are rebooting), disconnect from the DECT system and close down OTM DECT. Reconnect to the DECT system and activate the firmware again. **Note 2:** During activation, OTM DECT loses the connection to the DECT system. After activation is complete and the boards reboot a number of times, the green LEDs become solid (stop flashing). Reconnect OTM DECT to the DECT system. You can now see all the DMC4 cards on the DECT system.
7	Synchronize all boards.
	When prompted to synchronize, select all boards and synchronize from DMC. The DECT system is now upgraded. **Caution:** The DMC8 can reboot frequently if there is not at least one handset subscribed to the system.

END

Appendix C: DMC8 debug port

Overview

The ability to monitor messages on the DMC8 card is an important aid to resolving problems on DECT. Monitoring messages is an important part of the Serviceability program for DECT.

Use the information in this Appendix to identify how far messages are travelling, and where they are getting lost in the system.

For example, an investigation of a DMC card lockup problem shows that messages are leaving the PBX through LD 77, coming into the DMC card through the DS30 monitor, and being sent to the Cordless Controller Unit (CCU) through the IPC monitor. It is verified that there is a problem on the CCU because there are no responses from the CCU, although the "Hello messaging" is ok.

DMC card

The DMC is divided into the following sections:

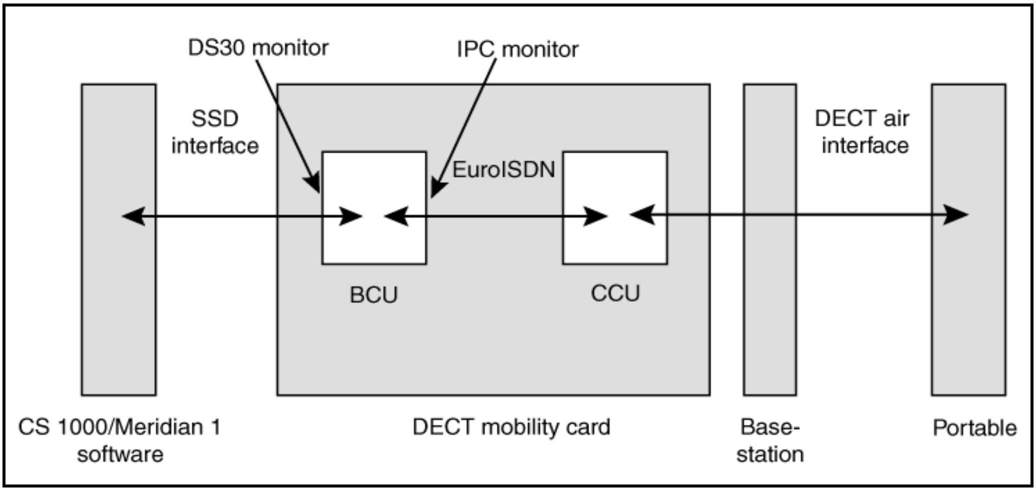
- CCU section that is primarily derived from the existing Philips DAS CCC hardware
- Backplane Conversion Unit (BCU) section that connects to the CCU

The BCU section of the DMC includes software to connect the Philips system to the PBX backplane. It effectively makes the CCU look like an Intelligent Peripheral card to the system. In fact, the DMC emulates an analogue line card with 32 handsets attached.

The CCU (Philips part) is connected to the BCU (Nortel part) through a 2Mbit EuroISDN link.

Figure 610 shows the components of the DECT interface. For the purposes of this Appendix, the BCU is the key component. For preliminary investigations, the DS30 monitor and Inter Processor Communications (IPC) monitor are the most important points to monitor from the DMC card.

Figure 610
DECT interface



Items to monitor

The DS30 driver and IPC driver tasks are the most informative for preliminary investigation. They track message passing through the debug task. The DS30 driver and IPC driver tasks provide detail on:

- Messages received and sent through the DS30 driver task from/to the PBX, and from/to the BCU software.
- Messages received and sent through the IPC driver task from/to the BCU software, and from/to the EuroISDN link (inter processor link).

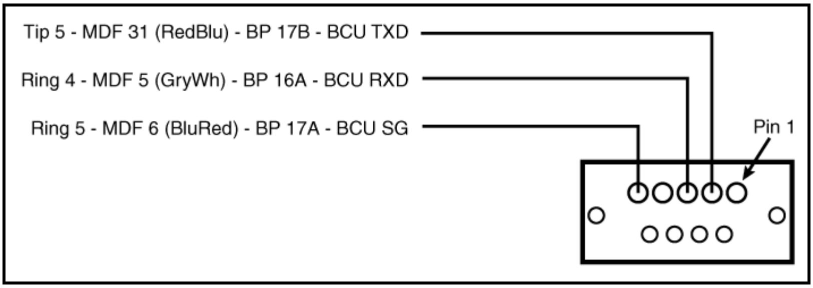
Monitor port physical connection

The DMC8 debug port connections allow the DMC8 to be connected as Data Communications Equipment (DCE) to a COM port of a PC (the Data Terminal Equipment [DTE]).

DMC8 debug port

The debug port of the DMC8 is connected directly from the MDF BIX block.

Figure 611
DMC8 debug port connections


Tip 5 - MDF 31 (RedBlu) - BP 17B - BCU TXD
Ring 4 - MDF 5 (GryWh) - BP 16A - BCU RXD
Ring 5 - MDF 6 (BluRed) - BP 17A - BCU SG
Pin 1

Connecting a modem

Figure 611 shows the DMC connected to a PC as DCE. To connect to a modem, the DMC has to act as DTE (because the modem is DCE). This is achieved in one of two ways:

1. Cross the TX and RX of the connections shown in Figure 611 (that is, swap pins 2 and 3 of the DB-9 cable).
2. Use a modem eliminator (null modem).

Before connecting to the DMC, the modem must be configured as follows using Hyper Terminal or similar (19200 baud):

1. ats0=1: s0 (zero) = 1, which enables auto answer after one ringing cycle.
2. at&d0: DTR override; the modem ignores DTR.
3. at&w0: Save settings.

Figure 612 is an example of the settings from a 3COM US Robotics modem. The most important settings are highlighted in bold.

Figure 612
3COM US Robotics modem settings

```
ati4

U.S. Robotics 56K Voice EXT Settings...

   B0  E1  F1  L2  M1  Q0  V1  X4  Y0
   SPEED=19200  PARITY=N  WORDLEN=8
   DIAL=TONE      OFFLINE

   &A1  &B0  &C1  &D0  &H0  &I0  &K1
   &M4  &N0  &R1  &S0  &T4  &U0  &Y1

   S00=001  S01=000  S02=043  S03=013  S04=010  S05=008  S06=004
   S07=060  S08=002  S09=006  S10=014  S11=070  S12=050  S13=000
   S15=000  S16=000  S18=000  S19=000  S21=010  S22=017  S23=019
   S25=005  S27=001  S28=008  S29=020  S30=000  S31=128  S32=002
   S33=000  S34=000  S35=000  S36=014  S38=000  S39=011  S40=000
   S41=004  S42=000

   LAST DIALLED #:

OK
```

Terminal configuration

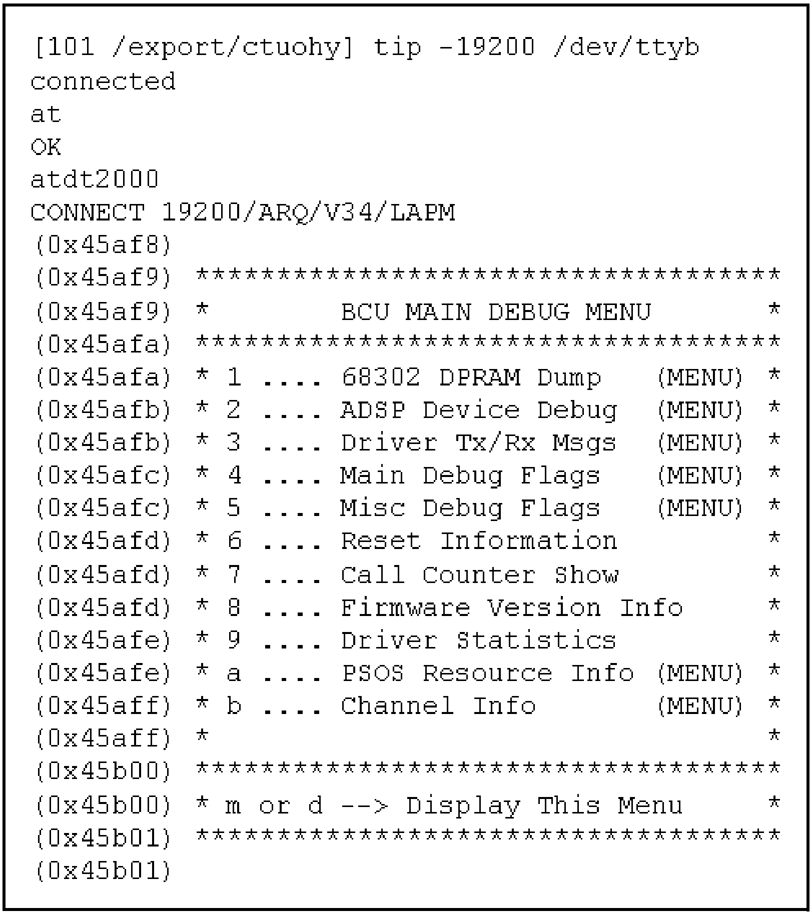
Whether connected to the DMC directly, or through modems, terminal configuration is the following:

- 19200 baud
- 8 bits
- no parity
- 1 stop bit UART

Successful connection

When you have successfully connected to the DMC, press **d** or **m** to display the main debug menu.

Figure 613
BCU Main Debug Menu



```
[101 /export/ctuohy] tip -19200 /dev/ttyb
connected
at
OK
atdt2000
CONNECT 19200/ARQ/V34/LAPM
(0x45af8)
(0x45af9) ************************************
(0x45af9) *        BCU MAIN DEBUG MENU       *
(0x45afa) ************************************
(0x45afa) * 1 .... 68302 DPRAM Dump   (MENU) *
(0x45afb) * 2 .... ADSP Device Debug  (MENU) *
(0x45afb) * 3 .... Driver Tx/Rx Msgs  (MENU) *
(0x45afc) * 4 .... Main Debug Flags   (MENU) *
(0x45afc) * 5 .... Misc Debug Flags   (MENU) *
(0x45afd) * 6 .... Reset Information         *
(0x45afd) * 7 .... Call Counter Show         *
(0x45afd) * 8 .... Firmware Version Info     *
(0x45afe) * 9 .... Driver Statistics         *
(0x45afe) * a .... PSOS Resource Info (MENU) *
(0x45aff) * b .... Channel Info       (MENU) *
(0x45aff) *                                  *
(0x45b00) ************************************
(0x45b00) * m or d --> Display This Menu     *
(0x45b01) ************************************
(0x45b01)
```

Information collection

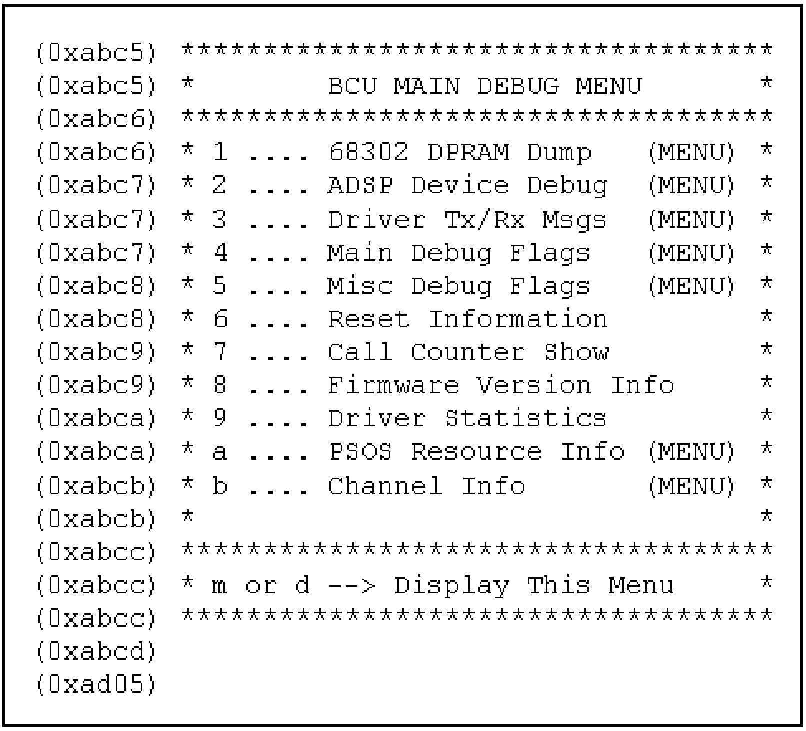
Record the following information (see "Switching on DS30 and IPC monitors" on page 1546) with a capture file using HyperTerminal or equivalent before you start monitoring.

Procedure 254
Switching on DS30 and IPC monitors

To switch on the DS30 and IPC monitors:

1 Press **m** or **d** to open the main menu. See Figure 614.

Figure 614
BCU main menu

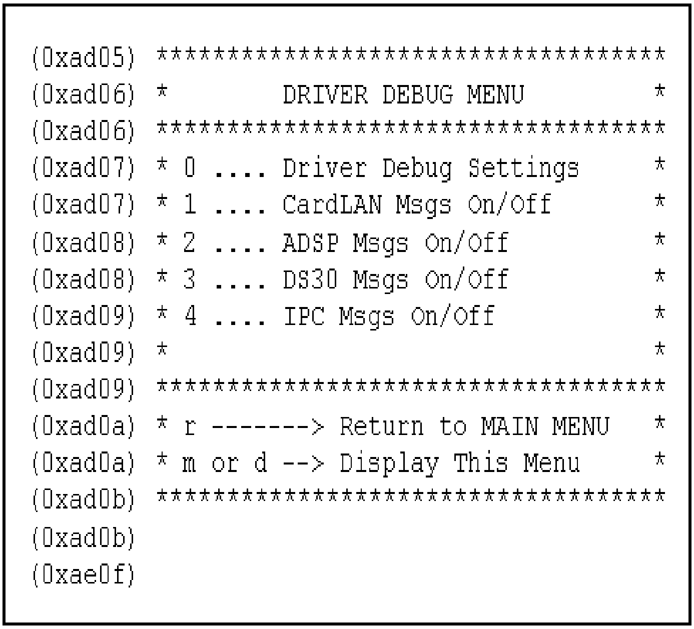


```
(0xabc5) *************************************
(0xabc5) *        BCU MAIN DEBUG MENU        *
(0xabc6) *************************************
(0xabc6) * 1 .... 68302 DPRAM Dump    (MENU) *
(0xabc7) * 2 .... ADSP Device Debug   (MENU) *
(0xabc7) * 3 .... Driver Tx/Rx Msgs   (MENU) *
(0xabc7) * 4 .... Main Debug Flags    (MENU) *
(0xabc8) * 5 .... Misc Debug Flags    (MENU) *
(0xabc8) * 6 .... Reset Information          *
(0xabc9) * 7 .... Call Counter Show          *
(0xabc9) * 8 .... Firmware Version Info      *
(0xabca) * 9 .... Driver Statistics          *
(0xabca) * a .... PSOS Resource Info  (MENU) *
(0xabcb) * b .... Channel Info        (MENU) *
(0xabcb) *                                   *
(0xabcc) *************************************
(0xabcc) * m or d --> Display This Menu      *
(0xabcc) *************************************
(0xabcd)
(0xad05)
```

2 Press **3** from the main menu.

The Driver Debug Menu displays. See Figure 615.

Figure 615
Current debug settings

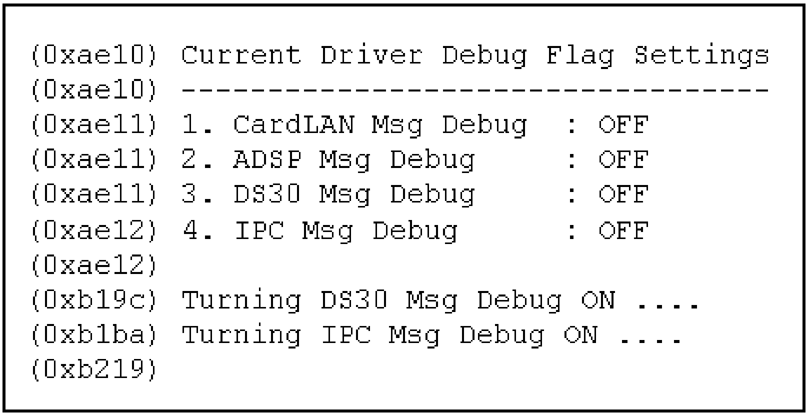


```
(0xad05) *************************************
(0xad06) *        DRIVER DEBUG MENU          *
(0xad06) *************************************
(0xad07) * 0 .... Driver Debug Settings      *
(0xad07) * 1 .... CardLAN Msgs On/Off        *
(0xad08) * 2 .... ADSP Msgs On/Off           *
(0xad08) * 3 .... DS30 Msgs On/Off           *
(0xad09) * 4 .... IPC Msgs On/Off            *
(0xad09) *                                   *
(0xad09) *************************************
(0xad0a) * r -------> Return to MAIN MENU    *
(0xad0a) * m or d --> Display This Menu      *
(0xad0b) *************************************
(0xad0b)
(0xae0f)
```

3 Press **0** (zero) to display the current debug settings.

4 Press **3** and **4** to switch on the monitors. See Figure 616 on page 1548.

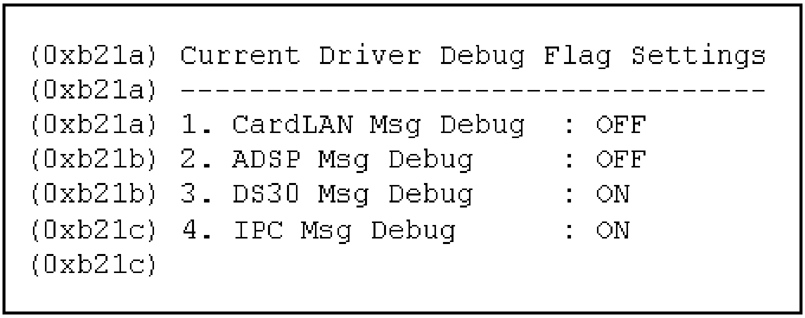
Figure 616
Current Driver Debug Flag Settings menu



```
(0xae10) Current Driver Debug Flag Settings
(0xae10) ----------------------------------
(0xae11) 1. CardLAN Msg Debug  : OFF
(0xae11) 2. ADSP Msg Debug     : OFF
(0xae11) 3. DS30 Msg Debug     : OFF
(0xae12) 4. IPC Msg Debug      : OFF
(0xae12)
(0xb19c) Turning DS30 Msg Debug ON ....
(0xb1ba) Turning IPC Msg Debug ON ....
(0xb219)
```

5 Press **0** (zero) to display the debug settings again. See Figure 617.

Figure 617
DS30 and IPC monitors ON



```
(0xb21a) Current Driver Debug Flag Settings
(0xb21a) ----------------------------------
(0xb21a) 1. CardLAN Msg Debug  : OFF
(0xb21b) 2. ADSP Msg Debug     : OFF
(0xb21b) 3. DS30 Msg Debug     : ON
(0xb21c) 4. IPC Msg Debug      : ON
(0xb21c)
```

End of Procedure

Messages on an idle system

IPC interface

After switching on the monitors, it is normal to see ping/pong (Hello messaging) messages on the IPC monitor between the BCU and CCU.

Hello messaging is used to detect errors on the BCU to CCU communication interface. The BCU and CCU are not synchronized with one another. They send Hello messages asynchronously, and there is no acknowledge. On receipt of a Hello message, the receiving unit resets the timer for the receipt of the next Hello message. On sending a Hello message, the sending unit resets the timer for sending the next Hello message. If the timeout for receiving a Hello message is exceeded, the receiving unit resets the DMC.

Table 156 shows the timeout values.

Table 156
Timeout values for Hello messaging

Item	Time-out duration
Timeout for sending new Hello	15 seconds for BCU
	16 seconds for CCU
Timeout for receiving a Hello message	40 seconds

The timeout values for sending differ for the BCU and the CCU to create an asynchronous exchange of the Hello messages.

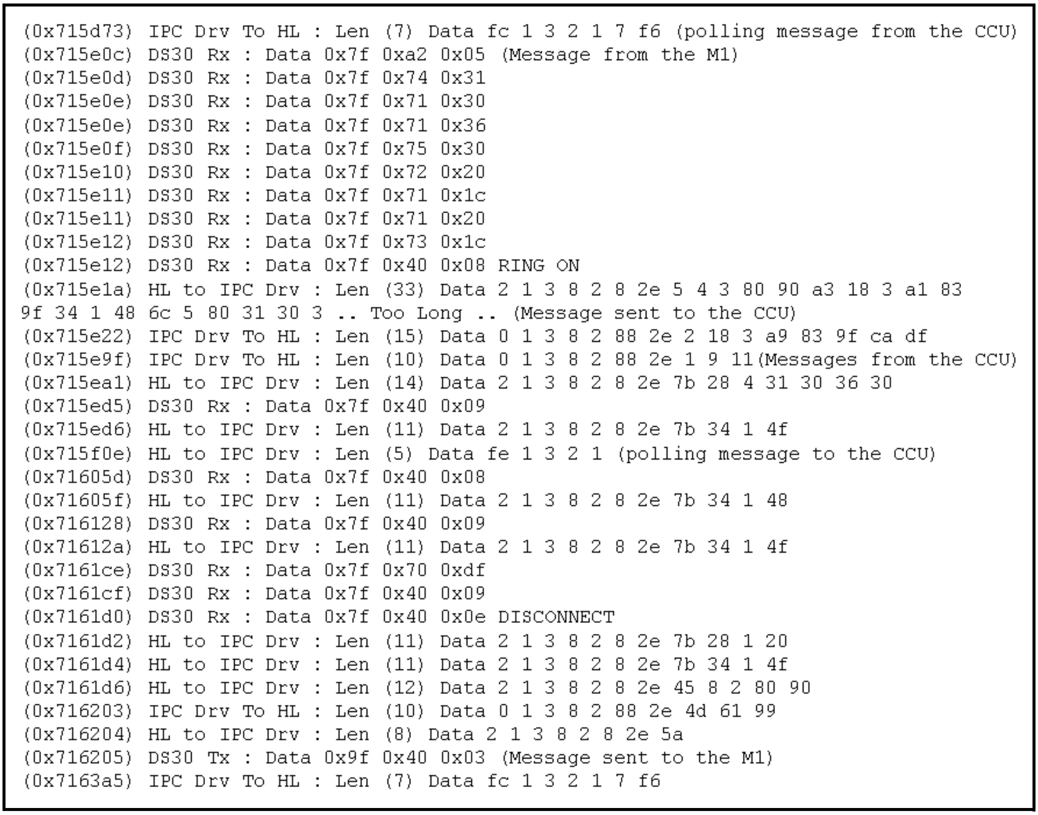
DS30 interface

Audit messages come from the PBX interface every few minutes for audit purposes. You can also view the audit messages using the SSD monitor on the PBX through LD 77.

Message examples

Figure 618 on page 1550 shows typical messages that can be seen during call processing on the DS30 and IPC link. This type of monitoring can impact call processing on a busy site because all 32 channels are monitored together.

Figure 618
Error message example



```
(0x715d73) IPC Drv To HL : Len (7) Data fc 1 3 2 1 7 f6 (polling message from the CCU)
(0x715e0c) DS30 Rx : Data 0x7f 0xa2 0x05 (Message from the M1)
(0x715e0d) DS30 Rx : Data 0x7f 0x74 0x31
(0x715e0e) DS30 Rx : Data 0x7f 0x71 0x30
(0x715e0e) DS30 Rx : Data 0x7f 0x71 0x36
(0x715e0f) DS30 Rx : Data 0x7f 0x75 0x30
(0x715e10) DS30 Rx : Data 0x7f 0x72 0x20
(0x715e11) DS30 Rx : Data 0x7f 0x71 0x1c
(0x715e11) DS30 Rx : Data 0x7f 0x71 0x20
(0x715e12) DS30 Rx : Data 0x7f 0x73 0x1c
(0x715e12) DS30 Rx : Data 0x7f 0x40 0x08 RING ON
(0x715e1a) HL to IPC Drv : Len (33) Data 2 1 3 8 2 8 2e 5 4 3 80 90 a3 18 3 a1 83
9f 34 1 48 6c 5 80 31 30 3 .. Too Long .. (Message sent to the CCU)
(0x715e22) IPC Drv To HL : Len (15) Data 0 1 3 8 2 88 2e 2 18 3 a9 83 9f ca df
(0x715e9f) IPC Drv To HL : Len (10) Data 0 1 3 8 2 88 2e 1 9 11(Messages from the CCU)
(0x715ea1) HL to IPC Drv : Len (14) Data 2 1 3 8 2 8 2e 7b 28 4 31 30 36 30
(0x715ed5) DS30 Rx : Data 0x7f 0x40 0x09
(0x715ed6) HL to IPC Drv : Len (11) Data 2 1 3 8 2 8 2e 7b 34 1 4f
(0x715f0e) HL to IPC Drv : Len (5) Data fe 1 3 2 1 (polling message to the CCU)
(0x71605d) DS30 Rx : Data 0x7f 0x40 0x08
(0x71605f) HL to IPC Drv : Len (11) Data 2 1 3 8 2 8 2e 7b 34 1 48
(0x716128) DS30 Rx : Data 0x7f 0x40 0x09
(0x71612a) HL to IPC Drv : Len (11) Data 2 1 3 8 2 8 2e 7b 34 1 4f
(0x7161ce) DS30 Rx : Data 0x7f 0x70 0xdf
(0x7161cf) DS30 Rx : Data 0x7f 0x40 0x09
(0x7161d0) DS30 Rx : Data 0x7f 0x40 0x0e DISCONNECT
(0x7161d2) HL to IPC Drv : Len (11) Data 2 1 3 8 2 8 2e 7b 28 1 20
(0x7161d4) HL to IPC Drv : Len (11) Data 2 1 3 8 2 8 2e 7b 34 1 4f
(0x7161d6) HL to IPC Drv : Len (12) Data 2 1 3 8 2 8 2e 45 8 2 80 90
(0x716203) IPC Drv To HL : Len (10) Data 0 1 3 8 2 88 2e 4d 61 99
(0x716204) HL to IPC Drv : Len (8) Data 2 1 3 8 2 8 2e 5a
(0x716205) DS30 Tx : Data 0x9f 0x40 0x03 (Message sent to the M1)
(0x7163a5) IPC Drv To HL : Len (7) Data fc 1 3 2 1 7 f6
```

Appendix D: Performance Collection file samples

Equipment Performance Collection file sample

```
<?xml version="1.0"?>
<file>
<header>
<systeminfo PARI="44446666"/>
<boardinfo boardnumber="24"/>
<package package_id="45100105"/>
</header>
<data>
<boardstat>
<dateandtime>2001,1,12,18,17,37,0</dateandtime>
<counters>0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0</counters>
</boardstat>
<rfpinfo>
<rfpstat rfp="1">
<dateandtime>2001,1,24,19,50,9,0</dateandtime>
<counters>1,0,0,0,8,420,0,1,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,0,0,0,0,0,0</counters>
</rfpstat>
<rfpstat rfp="2">
<dateandtime>2001,1,24,19,50,13,0</dateandtime>
<counters>1,0,0,0,8,420,0,1,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,0,0,0,0,0,0</counters>
</rfpstat>
<rfpstat rfp="3">
<dateandtime>2001,1,24,19,50,13,0</dateandtime>
```

```
<counters>0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0</counters>
</rfpstat>
<rfpstat rfp="4">
<dateandtime>2001,1,24,19,50,19,0</dateandtime>
<counters>0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0</counters>
</rfpstat>
</rfpinfo>
<rfpchanocc>
<rfpchocc rfp="1">
<dateandtime>2001,1,12,18,17,37,0</dateandtime>
<choc>0,0,0,0,0,0,0,0,0,0,0,0,0</choc>
</rfpchocc>
<rfpchocc rfp="2">
<dateandtime>2001,1,12,18,17,37,0</dateandtime>
<choc>0,0,0,0,0,0,0,0,0,0,0,0,0</choc>
</rfpchocc>
<rfpchocc rfp="3">
<dateandtime>2001,1,24,19,50,6,0</dateandtime>
<choc>0,0,0,0,0,0,0,0,0,0,0,0,0</choc>
</rfpchocc>
<rfpchocc rfp="4">
<dateandtime>2001,1,24,19,50,6,0</dateandtime>
<choc>0,0,0,0,0,0,0,0,0,0,0,0,0</choc>
</rfpchocc>
</rfpchanocc>
<bschanocc>
<bchanocc>
<dateandtime>2001,1,24,19,50,6,0</dateandtime>
<choc>0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,434</choc>
</bchanocc>
<schanocc>
<dateandtime>2001,1,24,19,50,6,0</dateandtime>
<choc>0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,434</choc>
</schanocc>
</bschanocc>
```

```
</data>
</file>
```

User Performance Collection file sample

```
<?xml version="1.0"?>
<file>
<header>
<systeminfo PARI="44446666"/>
<boardinfo boardnumber="24"/>
<package package_id="45100105"/>
</header>
<data>
<ppstat RecNum="2">
<dateandtime>2001,1,12,18,17,37,0</dateandtime>
<ipui>40110000E5A97B7F84</ipui>
<dnr>20801</dnr>
<counters>0,0,0,0,0,0,0,0,0,0,0,0,0,0,255</counters>
</ppstat>
</data>
</file>
```

Nortel Communication Server 1000

DECT

Description, Planning, Installation, and Operation

Information is subject to change without notice.
Nortel Networks reserves the right to make changes in design or components as progress in engineering and manufacturing may warrant.

Nortel, Nortel (Logo), the Globemark, This is the Way, This is Nortel (Design mark), SL-1, Meridian 1, and Succession are trademarks of Nortel Networks.

Publication number: 553-3001-370
Document release: Standard 5.00
Date: January 2006
Produced in Canada

NORTEL

>THIS IS THE WAY

>THIS IS NORTEL™