

# CPDM3

INSTALLATION AND OPERATION MANUAL



## NOTICE

The information contained in this document is believed to be accurate in all respects but is not warranted by Mitel Networks™ Corporation (MITEL®). Mitel makes no warranty of any kind with regards to this material, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. The information is subject to change without notice and should not be construed in any way as a commitment by Mitel or any of its affiliates or subsidiaries. Mitel and its affiliates and subsidiaries assume no responsibility for any errors or omissions in this document. Revisions of this document or new editions of it may be issued to incorporate such changes.

No part of this document can be reproduced or transmitted in any form or by any means - electronic or mechanical - for any purpose without written permission from Mitel Networks Corporation.

## TRADEMARKS

The trademarks, service marks, logos and graphics (collectively "Trademarks") appearing on Mitel's Internet sites or in its publications are registered and unregistered trademarks of Mitel Networks Corporation (MNC) or its subsidiaries (collectively "Mitel") or others. Use of the Trademarks is prohibited without the express consent from Mitel. Please contact our legal department at [legal@mitel.com](mailto:legal@mitel.com) for additional information. For a list of the worldwide Mitel Networks Corporation registered trademarks, please refer to the website: <http://www.mitel.com/trademarks>.

© Copyright 2017, Mitel Networks Corporation  
All rights reserved

## Contents

|  |           |
|--|-----------|
| <b>Introduction.....</b>                             | <b>1</b>  |
| 1.1 About the Product.....                           | 1         |
| 1.2 Products for CPDM3.....                          | 1         |
| 1.3 Abbreviations and Glossary.....                  | 1         |
| 1.4 How to Use this Document .....                   | 3         |
| 1.5 Included in the delivery.....                    | 4         |
| 1.6 Technical Solution .....                         | 5         |
| 1.7 Requirements.....                                | 5         |
| <b>2. Installation and Configuration Steps .....</b> | <b>6</b>  |
| 2.1 Information required for the Setup.....          | 6         |
| 2.2 Accessing the CPDM3.....                         | 6         |
| 2.3 Basic Configuration Steps.....                   | 7         |
| 2.4 Manage Central Phonebook Entries .....           | 7         |
| 2.5 Optional Settings .....                          | 9         |
| 2.6 Multiple CPDM3.....                              | 10        |
| <b>3. General.....</b>                               | <b>11</b> |
| 3.1 Graphical User Interfaces (GUI's).....           | 11        |
| 3.2 Authentication Levels and Default Password ..... | 14        |
| 3.3 Password Settings .....                          | 15        |
| 3.4 System Security Settings .....                   | 16        |
| 3.5 Proxy Settings.....                              | 19        |
| 3.6 Demonstration Mode .....                         | 20        |
| <b>4. Basic Configuration .....</b>                  | <b>21</b> |
| 4.1 Manage Central Phonebook Entries .....           | 21        |
| 4.2 Create Messaging Groups.....                     | 23        |
| 4.3 Select Messaging Destination.....                | 24        |
| 4.4 Input/Output Setup .....                         | 24        |
| 4.5 Alarm Handling .....                             | 26        |
| 4.6 Status .....                                     | 33        |
| 4.7 Module Redundancy .....                          | 40        |
| 4.8 Back up the Configuration.....                   | 46        |
| 4.9 Restore the Configuration .....                  | 47        |
| <b>5. Central Phonebook Configuration .....</b>      | <b>48</b> |
| 5.1 Technical Specification .....                    | 48        |
| 5.2 Change the Phonebook Address.....                | 48        |
| 5.3 Customize the Search Result Text .....           | 49        |
| 5.4 Select Central Phonebook Database .....          | 49        |

|            |  |            |
|------------|--|------------|
| 5.5        | LDAP Parameter Setup.....  | 49         |
| 5.6        | CMG Parameter Setup.....   | 52         |
| 5.7        | Digit Manipulation in Central Phonebook .....                    | 53         |
| <b>6.</b>  | <b>Serial Interface.....</b>                                     | <b>57</b>  |
| 6.1        | Serial Protocol Settings.....                                    | 57         |
| <b>7.</b>  | <b>Device Manager .....</b>                                      | <b>62</b>  |
| 7.1        | Description.....   | 62         |
| 7.2        | Logging On to the Device Manager.....                            | 67         |
| 7.3        | Templates .....  | 67         |
| 7.4        | Numbers .....  | 71         |
| 7.5        | Devices .....  | 77         |
| 7.6        | File management.....   | 81         |
| 7.7        | Import/Export Numbers and Templates .....                        | 88         |
| 7.8        | Other Settings.....  | 89         |
| <b>8.</b>  | <b>Device.....</b>   | <b>91</b>  |
| 8.1        | Device Management Setup .....                                    | 91         |
| 8.2        | Allow IP-DECT Handsets/Chargers to log in to Device Manager..... | 92         |
| 8.3        | Device Relogin Time.....   | 92         |
| 8.4        | Service Discovery.....   | 94         |
| <b>9.</b>  | <b>Additional System Settings.....</b>                           | <b>96</b>  |
| 9.1        | Unite Name Server (UNS) .....                                    | 96         |
| 9.2        | Logging .....  | 98         |
| 9.3        | Time Settings .....  | 98         |
| 9.4        | Network Settings .....   | 100        |
| 9.5        | Setting the License Number .....                                 | 101        |
| <b>10.</b> | <b>Remote Management.....</b>                                    | <b>102</b> |
| 10.1       | Serial IP Server Protocol.....                                   | 103        |
| <b>11.</b> | <b>Absence Handling.....</b>                                     | <b>105</b> |
| 11.1       | Absence Handling in DECT .....                                   | 105        |
| 11.2       | Absence Handling in the VoWiFi System .....                      | 105        |
| <b>12.</b> | <b>Base Station Conversion .....</b>                             | <b>107</b> |
| 12.1       | Background .....   | 107        |
| 12.2       | Configuration.....   | 107        |
| <b>13.</b> | <b>Open Access Protocol (OAP) .....</b>                          | <b>108</b> |
| 13.1       | Configuration.....   | 108        |
| 13.2       | Importing a new OA-XML file .....                                | 108        |
| <b>14.</b> | <b>DECT Interface.....</b>                                       | <b>110</b> |
| 14.1       | DECT Phone Systems .....   | 110        |

|                    |   |            |
|--------------------|---|------------|
| 14.2               | Mixed DECT Systems .....                                    | 111        |
| 14.3               | DECT Interface Settings .....                               | 113        |
| <b>15.</b>         | <b>WLAN Interface .....</b>                                 | <b>117</b> |
| 15.1               | Handset Registration .....                                  | 117        |
| 15.2               | WLAN System .....   | 117        |
| 15.3               | WLAN Message Distribution .....                             | 118        |
| 15.4               | User Server .....   | 118        |
| <b>16.</b>         | <b>System 900 .....</b>                                     | <b>119</b> |
| 16.1               | System 900 Interface.....                                   | 119        |
| 16.2               | System 900 Message Distribution.....                        | 120        |
| <b>17.</b>         | <b>Messaging Operation.....</b>                             | <b>121</b> |
| 17.1               | Create and Send Messages via NetPage.....                   | 121        |
| 17.2               | Predefined Messages.....                                    | 121        |
| 17.3               | Message History Status .....                                | 122        |
| 17.4               | Predefined Groups.....                                      | 123        |
| 17.5               | NetPage Configuration .....                                 | 123        |
| <b>18.</b>         | <b>Administration of Language and User Interfaces .....</b> | <b>127</b> |
| 18.1               | Customize the Language.....                                 | 127        |
| 18.2               | Customize the User Interface (GUI).....                     | 131        |
| 18.3               | Test the New User Interface .....                           | 141        |
| 18.4               | Update the User Interface after a new Release .....         | 141        |
| <b>19.</b>         | <b>Software Administration .....</b>                        | <b>142</b> |
| 19.1               | Add Device Software to the Device Manager.....              | 142        |
| 19.2               | Upgrade the Boot Software .....                             | 142        |
| 19.3               | Software Information .....                                  | 142        |
| 19.4               | Switch Software.....  | 142        |
| 19.5               | Install New Software .....                                  | 143        |
| <b>20.</b>         | <b>Troubleshooting.....</b>                                 | <b>144</b> |
| 20.1               | General Troubleshooting .....                               | 144        |
| 20.2               | NetPage Troubleshooting .....                               | 145        |
| 20.3               | Troubleshooting Guide .....                                 | 145        |
| 20.4               | Built-in tools.....   | 151        |
| 20.5               | Advanced Troubleshooting.....                               | 153        |
| 20.6               | What to consider when replacing a module.....               | 153        |
| 20.7               | Technical Support.....                                      | 153        |
| <b>21.</b>         | <b>Related Documents .....</b>                              | <b>154</b> |
| <b>Appendix A.</b> | <b>Used IP Ports.....</b>                                   | <b>155</b> |
| <b>Appendix B.</b> | <b>RS232 Connections .....</b>                              | <b>157</b> |
| <b>Appendix C.</b> | <b>System 900 Connections .....</b>                         | <b>159</b> |

**Appendix D. Alarm Action Configuration Examples ..... 160**

**Appendix E. Protocol Limitations ..... 166**

**Appendix F. Device Manager Keyboard Shortcuts..... 169**

**Appendix G. File types ..... 170**

**Appendix H. Multiple CPDM3 Configuration Examples ..... 171**

**Appendix I. Network Monitoring in a Redundancy System ..... 178**

# 1. INTRODUCTION

## 1.1 ABOUT THE PRODUCT

Centralized Portable Device Manager (CPDM3) is a gateway. In combination with IP-DECT or WiFi systems it offers typical wireless services such as access to central phonebook and centralized device management. It also offers basic messaging services as web messaging, messaging handset to handset (SMS) and messaging protocols.

## 1.2 PRODUCTS FOR CPDM3

- KDU 137 610 /3 ( FE3-EHBBAC) – CPDM3 Basic included in CPDM3 hardware, power supply, software and license with Device Management, 1 000 devices, 2 500 numbers

### **Additional Licenses for CPDM3**

- 86L00009AAA-A (FE3-EHBLAA) – License for messaging and alarm handling (Basic)
- 86L00010AAA-A (FE3-EHBLAP1) – License for ESPA 4.4.4 Messaging protocol, Ascum Line Protocol, URL Messaging Protocol, TAP 1.8
- 86L00008AAA-A (FE3-EHBLAP3) – License for OAP, Open Access Protocol for sending messages and receiving alarms.

## 1.3 ABBREVIATIONS AND GLOSSARY

|                     |   |
|---------------------|---|
| Ascum Line Protocol | A simple alternative to ESPA 4.4.4 with all basic features of paging call available but with a very limited status report.                                      |
| BAM                 | Basic Alarm Manager:<br>In CPDM3, this tool is referred to as Alarm Handling.   |
| Central Phonebook   | A Phonebook stored in a database in the control module or reached from the control module.  |
| Charger             | Can be a desktop charger or a charging rack   |
| CMG                 | Mitel Contact Management system used for telephony which includes telephone directory services.   |
| Company Phonebook   | A Phonebook that is uploaded to a handset from the Device Manager. The entries are locked for editing in the handset.   |
| Contacts            | The name of the phonebook in a handset.   |
| CPDM3               | Centralized Portable Device Manager<br>An application suite running on a CPDM3 hardware. The CPDM3 enables wireless services to and from handsets and chargers. |

|                           |  |
|---------------------------|--|
| CSV file                  | Comma Separated Value:<br>A file with data, where values in each row are separated by a delimiter, which can be a comma, a semicolon or a tab.   |
| DECT                      | Digital Enhanced Cordless Telecommunications:<br>A global standard for cordless telephony.   |
| Device                    | Can be a handset, a charger or a fixed IP-DECT device developed to work together with CPDM3 and the Device Manager application. Device is used as a general term in this document.   |
| DHCP                      | Dynamic Host Configuration Protocol  |
| ESPA 4.4.4                | A message-based serial protocol intended for communication with external equipment. Built upon the ISO1745 transport specification.  |
| FTP                       | File Transfer Protocol   |
| GUI                       | Graphical User Interface   |
| IPBS                      | IP-DECT Base Station   |
| IPDI                      | International Portable DAM Identity<br>DAM (DECT Authentication Module)<br>See IPEI for more information.  |
| IPEI                      | International Portable Equipment Identity:<br>IPEI/IPDI is needed to enable network subscription of the handset. At delivery of the handset, IPEI and IPDI are the same and either can be used for network subscription. If the IPEI and the IPDI differ, the IPDI shall be used for network subscription. |
| Language file             | Language file for portable devices on CPDM3.<br>Language file for CPDM3 uses XML (eXtensible Markup Language.).  |
| LDAP                      | Lightweight Directory Access Protocol  |
| NetPage                   | Tool for generating messages from a web browser.   |
| Number                    | Settings for the complete set of parameters of a single device, tied to a specific identity.   |
| OAP                       | Open Access Protocol:<br>Ascom defined XML based messaging and alarm protocol.   |
| OA-XML                    | The Open Access-XML protocol defines messages in XML format. CPDM3 contains a OAP interface for sending and receiving messages defined by the OA-XML protocol.   |
| OTA                       | Over the Air   |
| Parameter definition file | Defines the parameters for a portable device model, for example a handset, alarm transmitter etc.  |
| PDM                       | Portable Device Manager  |
| PKCS#12                   | A cryptography standard, defining a file format used to store keys and certificates.   |
| TAP                       | Telocator Alphanumeric Protocol:<br>An industry standard protocol for the input of paging requests.  |
| TFTP                      | Trivial File Transfer Protocol, a simple protocol to transfer files  |



|              |  |
|--------------|--|
| Unite system | Unite is the Ascom name for the Ascom Professional Messaging system.<br>The Unite communication protocol is used for communication between CPDM3s in systems with more than one CPDM3.   |
| UNS          | Unite Name Server:<br>Unite module component that holds the Unite number plan and Unite destinations   |
| VoWiFi       | Voice over Wireless Fidelity:<br>is a wireless version of VoIP and refers to IEEE 802.11a, 802.11b, 802.11g, or 802.11n network.   |
| WiFi         | WiFi is a term developed by the Wi-Fi Alliance® to describe wireless local area network (WLAN) products that are based on the Institute of Electrical and Electronics Engineers' (IEEE) 802.11 standards. Today, most people use WiFi as a reference to wireless connectivity. |
| WLAN         | Wireless LAN   |

## 1.4 HOW TO USE THIS DOCUMENT

This sub chapter includes references to other chapters/documents with more detailed information regarding following activities:

- Installation and basic configuration
- Extended configuration
- Installation of chargers
- Central Phonebook administration
- Daily operation

### References for Installation and Basic Configuration

- For installation and basic configuration, see the following chapters:
  - [2. Installation and Configuration Steps](#) on page 12
  - [3. General](#) on page 17

### References for Extended Configuration

Some extended configuration is included in the basic license, other requires an additional license, see below:

- For settings included in the FE3-EHBBAC license:  
Refer to chapters:
  - [4. Basic Configuration](#) on page 27
  - [10. Remote Management](#) on page 108
  - [11. Absence Handling](#) on page 111
  - [12. Base Station Conversion](#) on page 113

- For settings included in the FE3-EHBLAA license option:  
Refer to chapters:
  - [4.2 Create Messaging Groups](#) on page 29
  - [4.5 Alarm Handling](#) on page 32
  - [17. Messaging Operation](#) on page 127
- For settings included in the FE3-EHBLAP1 license option:  
Refer to chapters:
  - [6. Serial Interface](#) on page 63
- For settings included in the FE3-EHBLAP3 license option:  
Refer to chapters:
  - [13. Open Access Protocol \(OAP\)](#) on page 114.  
See also Function Description, Open Access Protocol (OAP), TD 93016EN.

NOTE: The installation of Chargers is described in the manual for the charger.

#### **Central Phonebook Administration**

- For administration of the central phonebook, refer to chapter [4.1 Manage Central Phonebook Entries](#) on page 27.

#### **Daily Operation**

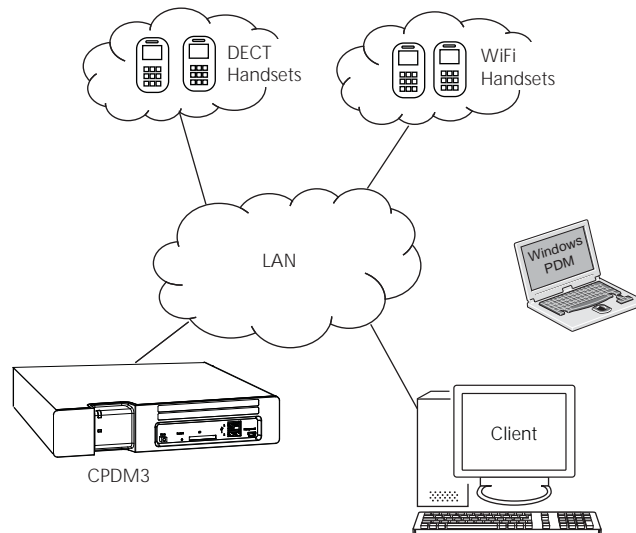
- For the daily operation, that is, creating and sending messages, see chapter [17. Messaging Operation](#) on page 127.

## **1.5 INCLUDED IN THE DELIVERY**

- CPDM3 hardware including a 230 V power cable
- Getting started document

## 1.6 TECHNICAL SOLUTION

Figure 1. CPDM3 in a system.



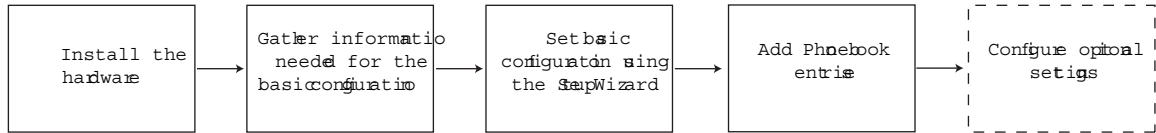
The CPDM3 runs on the hardware and is configured via a web interface using a computer (client) connected to the Local Area Network (LAN).

## 1.7 REQUIREMENTS

Refer to the Data Sheet for CPDM3.

## 2. INSTALLATION AND CONFIGURATION STEPS

Figure 2. Initial installation and configuration.



NOTE: The installation of the products hardware is described in the Installation Guide for CPDM3.

After installing the hardware, the basic configuration is easily made using the Setup Wizard. The setup wizard includes all basic settings needed to get the CPDM3 up and running.

### 2.1 INFORMATION REQUIRED FOR THE SETUP

Make sure the following information is available:

- MAC address – found on a label on the CPDM3's rear side and in the application's GUI in the Setup Wizard.
- The module key – found on the license certificate or on the CPDM3's rear side
- Network parameters – ask your network administrator
- License number – found on the license certificate
- Type of connected wireless phone system
- Single or Multiple IP-DECT Masters if connected to an IP-DECT Systems
- IP address to connected system (if connected via IP)
- Other messaging systems to send messages to (optional)
- LDAP/CMG properties, if an LDAP/CMG server is used for Central Phonebook requests (optional)

### 2.2 ACCESSING THE CPDM3

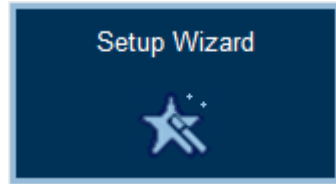
#### 2.2.1 GETTING STARTED

When accessing the CPDM3 the first time, follow the instructions in the Getting Started and safety Leaflet PM000033, or the Installation Guide for CPDM3

NOTE: The IP address must not change during operation because renew of IP address via DHCP is not handled. Other equipment connected to this product also expects a fixed IP address in some cases. If the IP plan is changed, this product must be restarted to update the IP address. Otherwise the system will not function properly.

## 2.3 BASIC CONFIGURATION STEPS

Figure 3. The Setup Wizard.



As long as the CPDM3 is not configured, the Setup Wizard will start automatically when logging on from a web browser.

The content of the wizard is depending on the license. It means that all configuration is not shown for all licenses.

- 1 Enter the address to the CPDM3 in a web browser.
- 2 Click "Setup Wizard" on the Start Page.
- 3 Enter the appropriate login credentials.

|           |          |          |
|-----------|----------|----------|
| User ID:  | admin    | sysadmin |
| Password: | changeme | setmeup  |

The default passwords can be changed later on.

The setup wizard will open and help you with the basic configuration. The setup wizard includes the following settings:

- Network setup – can be set manually or via DHCP
- License number – the type of license determines the functionality
- Type of connected wireless phone system – the exchange used by the handsets in the system.
- IP address to the connected DECT phone system (if connected via IP)
- Serial Interface – select which serial interface to use (using ESPA, Ascom Line protocol or TAP)
- Default messaging destination
- Date and time properties/settings – for time stamps on activities
- Central Phonebook properties – database to use when searching (local phonebook on the module, LDAP server, or CMG).
- LDAP/CMG properties – (only visible if LDAP/CMG is selected in the Central Phonebook properties)
- Digit Manipulation Properties – information on how to convert telephone numbers (only visible if LDAP is used as database)
- Passwords – change from default to site specific passwords

## 2.4 MANAGE CENTRAL PHONEBOOK ENTRIES

NOTE: This section is only applicable if a local database was selected in the Setup Wizard.

The phonebook entries can be added manually or by importing a CSV file. If the local database Local - 2000 View only is to be used, the CSV file is required to add the entries.

### 2.4.1 ADD ENTRIES TO THE CENTRAL PHONEBOOK

The central phonebook supports entries with character encoding UTF-8 (for example Russian characters and Swedish characters).

- 1 Click "Phonebook" on the start page.
- 2 Select Phonebook > Edit on the Configuration page.
- 3 Click "Add".

#### Edit Central Phonebook

| Last Name            | First Name           | Number               |
|----------------------|----------------------|----------------------|
| <input type="text"/> | <input type="text"/> | <input type="text"/> |

- 1 Enter the following settings in the text fields:

| Setting     | Description            |
|-------------|------------------------|
| Last Name:  | The family name        |
| First Name: | The first (given) name |
| Number:     | The telephone number   |

- 2 To add additional rows click "Add" again.
- 3 Click "Save".

### 2.4.2 IMPORT ENTRIES FROM CSV FILE

The CSV file to be imported to the phonebook should have the following format with either ";" or "," as delimiter (as in the example below) or TAB:

First name 1;Last name 1;Phone number 1

First name 2,Last name 2,Phone number 2

NOTE: When importing a Central phonebook file in CSV format, existing entries are deleted.

- 1 Click "Phonebook" on the start page.
- 2 Select Phonebook > Import/Export in the menu on the Configuration page.

**Import**

Character encoding

Separator character

Import file

- 3 Select the character encoding of the file in the Character encoding drop-down list.  
NOTE: It is important that you select the same character encoding that the file is saved as. If not, the entries will be corrupted after the file has been imported.
- 4 Select separator for the CSV file.  
Different separators may be used in a delimiter-separated file. Currently, the module supports import of files with the separators semicolon, comma or TAB.
- 5 Click "Browse" to locate the CSV file in the system.
- 6 Click "Import".

## 2.5 OPTIONAL SETTINGS

Some of the optional settings in the module are included in the basic license, other requires an additional license.

- Alarm Handling – alarm actions can be set (type of trigger and what action to take). Refer to chapter [4.5 Alarm Handling](#) on page 32.
- Status – information about the site and information about supervised modules and equipment can be exported for troubleshooting purposes. Refer to chapter [4.6 Status](#) on page 39.
- Set Language – it is possible to translate the user interface language, refer to chapter [18.1 Customize the Language](#) on page 133.
- Input/Output setup – makes it possible to define inputs (for example a switch or button) and outputs (for example to turn on a siren or to close a door). Inputs can be used as trigger conditions and outputs can be used as actions. Refer to chapter [4.4 Input/Output Setup](#) on page 30.
- Customize the Start page and NetPage GUI – the Start page and the NetPage user interface can be customized to suit the individual customer requirements concerning functionality. Refer to chapter [18.2 Customize the User Interface \(GUI\)](#) on page 137.
- Remote Connection – makes it possible to establish a remote connection to a customer site. This makes it possible to configure and maintain sites, independent of distance. Refer to chapter [10. Remote Management](#) on page 108.
- Open Access Protocol (OAP) – makes it possible to communicate with other systems that is connected to the module. Refer to chapter [13. Open Access Protocol \(OAP\)](#) on page 114.
- Digit Manipulation – makes it possible to set the way telephone numbers are converted in telephone number lists. See [5.7 Digit Manipulation in Central Phonebook](#) on page 59.
- Redundancy – makes it possible to set up a pair of CPDM3s for redundancy. Refer to chapter [4.7 Module Redundancy](#) on page 46.

## 2.6 MULTIPLE CPDM3

In some situations there is a need for more than one CPDM3 in a system. More than one module is required in following cases:

- in systems with centralized management for more than 1000 devices, see [H.1 More than 1000 devices](#) on page 176.
- with high messaging traffic
- when it is preferred to split functionality on different CPDM3 modules, such as:
  - device management
  - central phonebook
  - messaging
  - This can be due to:
    - security reasons
    - geographical reasons
    - administrative reasons

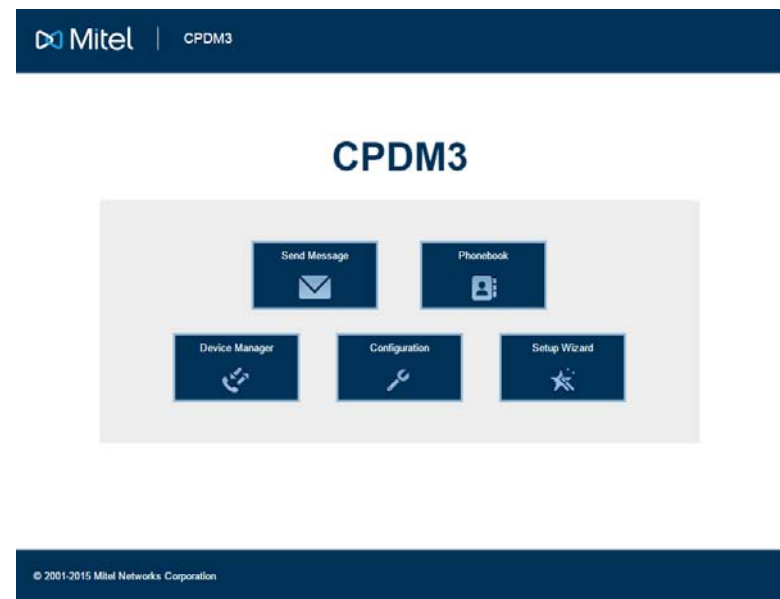


### 3. GENERAL

#### 3.1 GRAPHICAL USER INTERFACES (GUI'S)

##### 3.1.1 START PAGE

Figure 4. The Start Page



The start page has entrances to different applications. The number and type of applications is license dependent. Different applications also requires different authentication levels as shown in [table 1](#) on page 17.

Table 1.

| Applications  | Authentication levels<br>(user name/password)        |
|---|--|
| Send Message, see <a href="#">17. Messaging Operation</a> on page 127.  | No logon required                                    |
| Phonebook, see <a href="#">4.1 Manage Central Phonebook Entries</a> on page 27.<br>Describes how to handle phonebook entries. | user/password<br>admin/changeme<br>sysadmin/setmetup |
| Device Manager, see <a href="#">7. Device Manager</a> on page 68.<br>Describes device management.                             | user/password<br>admin/changeme<br>sysadmin/setmetup |
| Configuration, see <a href="#">3.1.3 Configuration Page</a> on page 19.<br>Setup page for the module settings.                | admin/changeme<br>sysadmin/setmetup                  |

Setup Wizard, see [2.3 Basic Configuration Steps](#) admin/changeme  
on page 13. sysadmin/setmetup

The first time and as long as the module is not  
configured, the Setup wizard will start  
automatically.

The default authentication levels and passwords can be changed, see [3.2 Authentication Levels and Default Password](#) on page 20.

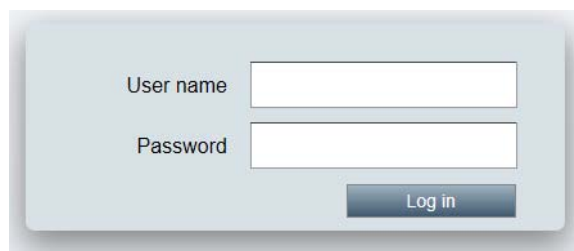
### 3.1.2 LOGIN PAGE

When clicking an application that requires login credentials, the CPDM3 redirects you to a Login page. Once logged in, you will remain logged in until you close the web browser or by clicking "Log out" in the CPDM3's web interface.

If you are logged in to an application and then navigate to another application requiring a higher authentication level than the prior application, you will be prompted to log in again.

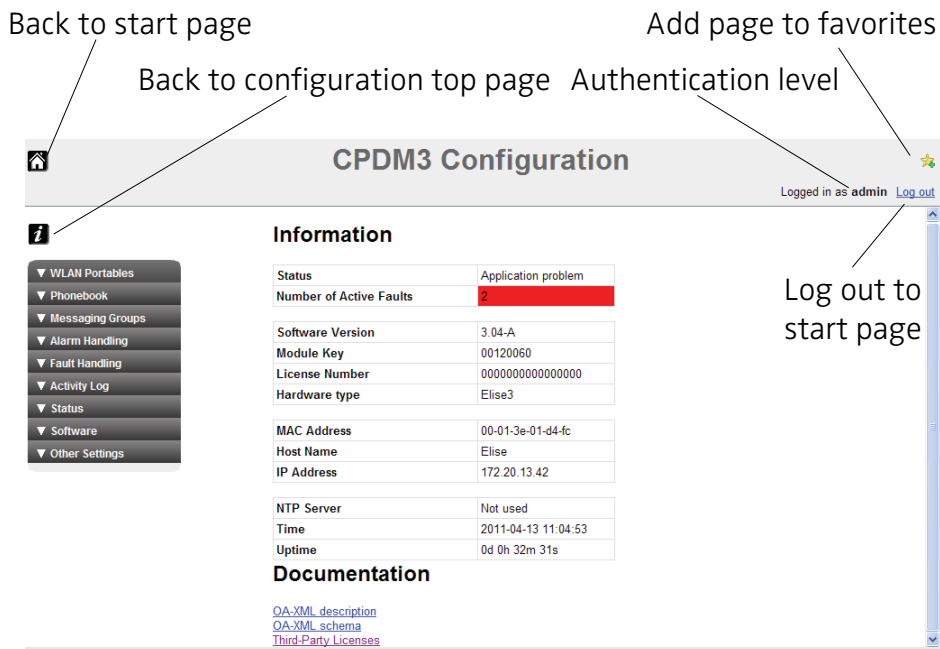
For example; you log in to the Phonebook application as user, and then navigate to the Setup Wizard. In this case, you will be prompted to log in again due to a higher authentication level (admin or sysadmin) is required for that application.

Figure 5. Login page in the CPDM3


The image shows a login form with a light blue background and a subtle drop shadow. It contains two input fields: "User name" and "Password". The "User name" field is a white rectangle with a thin border. The "Password" field is a white rectangle with a thin border. Below the "Password" field is a blue button with the text "Log in" in white. The form is centered on the page.

### 3.1.3 CONFIGURATION PAGE

Figure 6. The Configuration page



With system administrator or administrator rights you will be able to access the complete configuration page from the Configuration- and Phonebook buttons on the start page. Links to documentation are also found on the Configuration page.

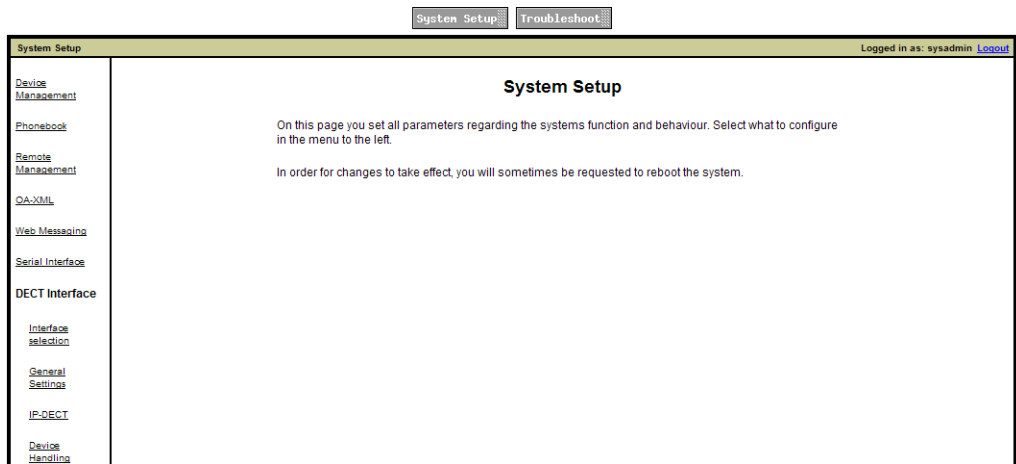
Use the  symbol if you want to return to the start page without logging out. Using the "Log out" link will also send you back to the start page but you will be logged out as well.

System information is shown on the Configuration top page, for example host name, IP address and MAC Address.

### 3.1.4 ADVANCED CONFIGURATION PAGE

The Advanced Configuration page is reached from the Configuration page (under Other Settings).

Figure 7. The Advanced Configuration Page



3.2 AUTHENTICATION LEVELS AND DEFAULT PASSWORD

The product has five different authentication levels:

- Using the Send Message function, i.e. creating and sending messages, can be done by any user in the system and it normally does not require a password.
- User rights are required for the administration of the phonebook. Default user name and password are “user” and “password”.
- Administrator rights are required for the setup, the configuration and administration, simple troubleshooting and changing passwords (except for the sysadmin password). Default user name and password are “admin” and “changeme”.
- System Administrator rights is used for advanced troubleshooting. It gives access to all administration pages and the permission to change all passwords. Default user name and password are “sysadmin” and “setmeup”.
- Auditor rights gives basically the same access as Administrator rights, but without permission to alter values. There is no access to the setup wizard or the Device Manager. Default user name and password is “auditor” and “readonly”.

Different levels of password policy can be set in, see [3.3.2 Set Password Policy](#) on page 21.

Functionality matrix

The following matrix shows which functionality that can be used by the different authentication levels.

|                             | anonymous | user | admin | sysadmin | auditor |
|-----------------------------|-----------|------|-------|----------|---------|
| Send messages               | Yes       | Yes  | Yes   | Yes      | Yes     |
| Phonebook administration    | No        | Yes  | Yes   | Yes      | No      |
| NetPage login               |           |      |       |          |         |
| View configuration settings | No        | No   | Yes   | Yes      | Yes     |

|                               |    |     |                  |     |    |
|-------------------------------|----|-----|------------------|-----|----|
| Configuration                 | No | No  | Yes              | Yes | No |
| Access to the setup wizard    |    |     |                  |     |    |
| Access to the Device Manager. | No | Yes | Yes              | Yes | No |
| Change passwords              | No | No  | Yes <sup>a</sup> | Yes | No |

a.Admin cannot change password for sysadmin.

## 3.3 PASSWORD SETTINGS

The default passwords for the different type of users; sysadmin, admin etc., can be changed and it is also possible to specify the password complexity, such as length and number of character types. Passwords can be changed in both the Setup Wizard and on the Advanced Configuration page, but the password complexity (password policy) can only be changed on the Advanced Configuration page.

### 3.3.1 CHANGE PASSWORDS

Different passwords can be set for different users.

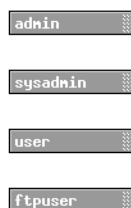
- 1 Click "Configuration" on the start page.
- 2 Select Other Settings > Advanced Configuration in the menu in the on the Configuration page.
- 3 Under Security, click "Change Passwords" in the menu on the Advanced Configuration page.

#### Passwords

On this page you can change the passwords for the users admin and sysadmin, restricting access to the Administration page. The admin user can only change the admin password, while the sysadmin user can change both sysadmin and the admin password.

You can also change the password for the users user and ftpuser.

Select user:



The image shows a vertical list of four buttons, each representing a user. The buttons are labeled 'admin', 'sysadmin', 'user', and 'ftpuser' from top to bottom. Each button has a small grid icon on its right side.

- 4 Click the user to change password for.
- 5 Enter your user name and password. Enter the new password and confirm the password.
- 6 Click "Ch. Passwd".

### 3.3.2 SET PASSWORD POLICY

The required password complexity can be set.

- 1 Click "Configuration" on the start page.
- 2 Select Other Settings > Advanced Configuration in the menu in the on the Configuration page.

- 3 Select "Password Policy" under Security in the menu on the Advanced Configuration page.

The screenshot shows the "Password Policy" configuration window. It contains five settings, each with a help icon (question mark in a square) and a dropdown menu:

- Minimum length: 5
- Number of character types: 1
- Number of previous passwords not allowed: 0
- Repeated characters: Allowed
- Sequential characters: Allowed

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

- 4 Select password policy.
- 5 Click "Activate".

It is also possible to select previous or factory default settings.

## 3.4 SYSTEM SECURITY SETTINGS

Security settings, such as not allowing HTTP and FTP access, disabling NETBIOS and increasing the security by using Certificates might be needed if required by the customer.

### 3.4.1 WEB ACCESS SECURITY SETTINGS

You can determine if the CPDM3 only should be accessed via HTTPS and FTPES to establish a secure connection between your client and the CPDM3. Information sent between the client and the CPDM3 cannot be seen by any third-party. The HTTPS and FTPES require a certificate.

- 1 Click "Configuration" on the start page.
- 2 Select Other Settings > Advanced Configuration in the menu in the on the Configuration page.
- 3 Select "Web Access" under Security in the menu on the Advanced Configuration page.

The screenshot shows the "Web Access Security" configuration window. It contains one setting with a help icon (question mark in a square) and a dropdown menu:

- Secure Mode: Disabled

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

- 4 Select if Secure Mode shall be enabled or not.
- 5 Click "Activate"

It is also possible to select previous or factory default settings.

### 3.4.2 NETBIOS PORT

You can determine if the NETBIOS port (UDP 137) shall be open or closed. The NETBIOS makes it possible to access the CPDM3 with the NetBIOS name “elise-XXXXXXX”, where XXXXXXXX is the module key number. If the port is closed, only the CPDM3’s IP address can be used to access the CPDM3.

The NetBIOS port is default enabled but can be disabled if needed for security reasons.

- 6 Click “Configuration” on the start page.
- 7 Select Other Settings > Advanced Configuration in the menu on the Configuration page.
- 8 Select “IP Ports” under Security in the menu on the Advanced Configuration page.

**IP Ports**

|  |   |            |
|--|---|------------|
| NetBIOS (UDP Port 137)                   | ? | Enabled ▼  |
| Fragmented TCP packets (Caution advised) | ? | Disabled ▼ |
| FTP (TCP Port 21)                        | ? | Enabled ▼  |

Previous Factory

Activate Cancel

- 9 Select if the port should be closed (disabled) or open (enabled) in the NetBIOS (UDP Port 137) drop-down list.
- 10 Click “Activate”.

### 3.4.3 FRAGMENTED TCP PACKETS

You can determine if the module shall allow that IP packets is broken into several smaller packets, which then can be transmitted an reassembled at the final destination.

If the IP network only allows packets with 1500 bytes, the packets will be dropped if not fragmenting is allowed. If fragmentation is allowed in the IP network, the parameter needs to be enabled in module.

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

**IP Ports**

|  |   |            |
|--|---|------------|
| NetBIOS (UDP Port 137)                   | ? | Enabled ▼  |
| Fragmented TCP packets (Caution advised) | ? | Disabled ▼ |
| FTP (TCP Port 21)                        | ? | Enabled ▼  |

Previous Factory

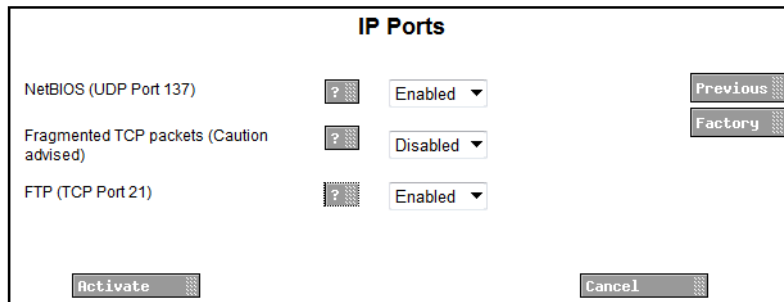
Activate Cancel

- 4 Select “Enabled” in the Fragmented TCP packets (Caution advised) drop down list.
- 5 Click “Activate”.

### 3.4.4 FTP PORT

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

- 1 Click "Configuration" on the start page.
- 2 Select Other Settings > Advanced Configuration. Select "IP Ports" under Security in the menu on the Advanced Configuration page.



The screenshot shows the "IP Ports" configuration page. It has a title bar "IP Ports". Below the title, there are three rows of settings, each with a help icon (?), a dropdown menu, and a button. The first row is "NetBIOS (UDP Port 137)" with a dropdown set to "Enabled" and a "Previous" button. The second row is "Fragmented TCP packets (Caution advised)" with a dropdown set to "Disabled" and a "Factory" button. The third row is "FTP (TCP Port 21)" with a dropdown set to "Enabled". At the bottom of the page, there are "Activate" and "Cancel" buttons.

- 3 Select if the FTP port shall be open (enabled) or not (disabled) in the FTP (TCP Port 21) drop-down list.
- 4 Click "Activate".

### 3.4.5 CERTIFICATES

Certificates are used to increase security by encryption. A self-signed digital certificate is created during the first start-up. This certificate is issued for the module's MAC address. A certificate can also be imported or created in the module.

NOTE: Certificates can be used to control if VoWiFi handsets are authorized to access a WLAN network, see [7.4.4 Certificate Handling for VoWiFi Handset](#) on page 78

#### Import certificates

Certificates can be imported to the CPDM3. These certificates may be created by a system administrator with IT security responsibility. The CPDM3 uses PKCS#12 files, which include keys and certificates. Consult your IT responsible to obtain the PKCS#12 file.

- 1 Click "Configuration" on the start page.
- 2 Select Other Settings > Advanced Configuration in the menu in the on the Configuration page.
- 3 Click "Import" under Certificates in the menu.



The screenshot shows the "Certificates Import" page. It has a title bar "Certificates Import". Below the title bar, there is a section titled "Import PKCS#12 file". Below this section, there is a text box with the text "Import a PKCS#12 file received from the IT security responsible. Please note that the web server will be restarted automatically." Below the text box, there are two input fields: "File name" and "Password". Each input field has a help icon (?) and a "Browse..." button. At the bottom of the page, there are "Import file" and "Close" buttons.




- 4 In the Certificates Import window, you can locate a certificate file. Enter file name and a valid password. The certificate is tied to a specific password which should be delivered with the file.
- 5 Click "Import file". The file is imported to the module.
- 6 Click "Close".

When starting, there may be a warning about the security certificate. This warning can be ignored.

### Create certificate

It is possible to create certificates in the module. For instructions on how to create a PKCS#12 file, follow this instruction:

- 1 Click "Configuration" on the start page.
- 2 Select Other Settings > Advanced Configuration in the menu in the on the Configuration page.
- 3 Click "Create" under Certificates in the menu.

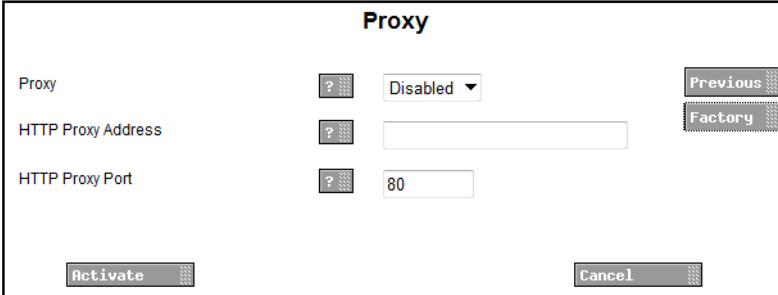


- 4 Enter valid parameters for your certificate file in the Create Self Signed Certificate window. "Validity" and "Common name" are mandatory.  
Due to security reasons, some characters in the ASCII-table are not allowed to use in the fields "Common Name", "Organization Unit", "Organization", "Locality", "State or Province" and "Country" when creating a certificate.  
Among these are: [ , ] , ( , ) , { , } , \$ , & , \ , | , \* , " , ' , ? , ~ , > , < , ^ , \n , \r.
- 5 Click "Create Certificate".

## 3.5 PROXY SETTINGS

If your corporate network is using a proxy server, the CPDM3 must send all outgoing requests through the proxy server to be able to send the requests outside the corporate network.

- 1 Click "Configuration" on the start page.
- 2 Select Other Settings > Advanced Configuration.
- 3 Select "Proxy" under Security in the menu on the Advanced Configuration page.



The image shows a 'Proxy' configuration dialog box. It has a title bar 'Proxy'. Inside, there are three rows of settings: 'Proxy' with a dropdown menu set to 'Disabled', 'HTTP Proxy Address' with an empty text field, and 'HTTP Proxy Port' with a text field containing '80'. To the right of these settings are two buttons: 'Previous' and 'Factory'. At the bottom of the dialog are two buttons: 'Activate' and 'Cancel'. Each setting field has a small help icon (a square with a question mark) to its left.

- 4 Enter/Select the following:
- |                     |  |
|---------------------|--|
| Proxy:              | Determines if the proxy settings below is to be used |
| HTTP Proxy Address: | The address to the proxy server                      |
| HTTP Proxy Port:    | The port the proxy server is listening at            |

## 3.6 DEMONSTRATION MODE

Demonstration Mode makes it possible to run the product for two hours with almost full functionality of the application.

The Demonstration Mode can be set from the application's Configuration page or manually by using the Mode button. The module will automatically return to previous license and parameters (without restart) after 2 hours.

Demonstration Mode is indicated by the Status LED with yellow slow flashing light. If any application encounters problems during Demonstration Mode, the Status LED will however show red slow flashing light instead. The Mode button LED shows blue fixed light.

### From the application's Configuration page:

- 1 Click "Configuration" on the start page.
- 2 Select Other Settings > Demonstration Mode in the menu on the Configuration page.
- 3 Click "Activate".
- 4 Exiting before the 2 hours have passed, is done by clicking "Deactivate".

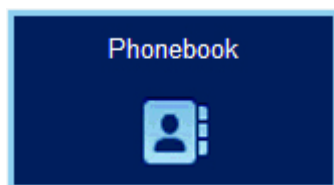
### Using the Mode button:

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

## 4. BASIC CONFIGURATION

The basic configuration requires system administrator or administrator rights. With user rights you will only be able to access and configure the Central Phonebook. Refer to [3.2 Authentication Levels and Default Password](#) on page 20.

### 4.1 MANAGE CENTRAL PHONEBOOK ENTRIES



The central phonebook makes it possible for users to search and find phonebook entries from a handset in the system. The entries can be added manually ([4.1.1 Add Entries to the Central Phonebook](#) on page 27) or by importing a file containing the entries ([4.1.3 Import Entries to the Central Phonebook from a CSV File](#) on page 28).

#### 4.1.1 ADD ENTRIES TO THE CENTRAL PHONEBOOK

The entries in the central phonebook can be filled in manually. The central phonebook supports entries with character encoding UTF-8 (for example Russian characters and Swedish characters).

- 1 Click "Phonebook" on the start page.
- 2 Select Phonebook > Edit on the Configuration page.
- 3 Click "Add" and enter the information needed in the text fields as described below.

#### Edit Central Phonebook

| Last Name            | First Name           | Number               |
|----------------------|----------------------|----------------------|
| <input type="text"/> | <input type="text"/> | <input type="text"/> |

- 1 Enter the following settings in the text fields:

| Setting     | Description            |
|-------------|------------------------|
| Last Name:  | The family name        |
| First Name: | The first (given) name |
| Number:     | The telephone number   |

- 2 To add several rows click "Add" again.
- 3 Click "Save".


### Sorting Entries in the Central Phonebook

The entries in the Central phonebook can be sorted on Last Name, First Name or Number by clicking the arrows in the list's title bar.



#### 4.1.2 DELETE ENTRIES

- 1 Click "Phonebook" on the start page.
- 2 Select Phonebook > Edit in the menu on the Configuration page.

##### A) Delete a single Entry:

- 1 Locate the entry to be deleted and click the  button in the same row.
- 2 Click "Save". The entry is deleted.

##### B) Delete several Entries:

- 1 Click "Delete All".  
All entries in the list will be crossed over and the  icon will be displayed to the right of each entry. If you want to keep an entry just click the  icon and the changes will be discarded for that entry.
- 2 Click "Save". All entries marked with a blue arrow are deleted.

#### 4.1.3 IMPORT ENTRIES TO THE CENTRAL PHONEBOOK FROM A CSV FILE

The CSV file to be imported to the Central phonebook shall have the following format:

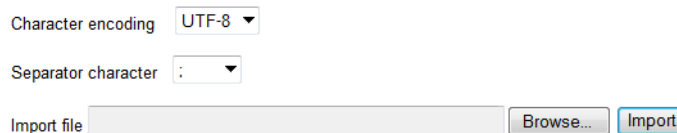
First name;Last name 1;Telephone number

Different separators may be used, see below:

NOTE: When importing a Central phonebook file in CSV format, existing entries are deleted.

- 1 Click "Phonebook" on the start page.
- 2 Select Phonebook > Import/Export in the menu on the Configuration page.

##### Import



- 3 Select the character encoding of the file in the Character encoding drop-down list.  
NOTE: It is important that you select the same character encoding that the file is saved as. If not, the entries will be corrupted after the file has been imported.
- 4 Select separator for the CSV file.  
Different separators may be used in a delimiter-separated file. Currently, the module supports import of files with the separators semicolon, comma or TAB.
- 5 Click "Browse" to locate the CSV file in the system.
- 6 Click "Import".

#### 4.1.4 EXPORT THE CENTRAL PHONEBOOK TO A CSV FILE

The complete Central phonebook can be exported to a CSV file for backup reasons. The exported file will be saved with the character encoding UTF-8.

- 1 Click "Phonebook" on the start page.
- 2 Select Phonebook > Import/Export in the menu on the Configuration page.
- 3 Click "Export".
- 4 Click "Save" in the window that opens.
- 5 Enter a name of the file, and select in which folder the file should be saved.
- 6 Click "Save".

## 4.2 CREATE MESSAGING GROUPS

Messaging Groups in the CPDM3 makes it possible to send one message to several handsets. 30 groups with 15 handsets in each group, and one group with 50 handsets can be created. Messaging Groups can also be used to send Push-to-talk (PTT) messages to a group of handsets. In this case, PTT parameters must also be set in the handset that shall initiate the PTT message. Refer to the handset's Configuration Manual for more information about the parameters.

Each group is given an address, either a name or a number, and a description. Then the addresses of the handsets, that should be included in the group, are added.

- 1 Click "Configuration" on the Start page.
- 2 Select Messaging Groups > Edit in the menu on the Configuration page.

**Groups**

|        |   |   |
|--------|---|---|
| Groups | ? | <a href="#">EMPTY LARGE GROUP</a><br><a href="#">EMPTY</a><br><a href="#">EMPTY</a><br><a href="#">EMPTY</a><br><a href="#">EMPTY</a><br><a href="#">EMPTY</a><br><a href="#">EMPTY</a><br><a href="#">EMPTY</a><br><a href="#">EMPTY</a><br><a href="#">EMPTY</a><br><a href="#">EMPTY</a> |
|--------|---|---|

**Group configuration**

|                   |   |  |   |
|-------------------|---|--|---|
| Group address     | ? | <input style="width: 90%;" type="text"/>   | <input type="button" value="Previous"/> |
| Group description | ? | <input style="width: 90%;" type="text"/>   | <input type="button" value="Factory"/>  |
| Members           | ? | <input style="width: 90%;" type="text"/><br><input style="width: 90%;" type="text"/><br><input style="width: 90%;" type="text"/><br><input style="width: 90%;" type="text"/><br><input style="width: 90%;" type="text"/><br><input style="width: 90%;" type="text"/> |   |

- 4 Enter the following settings:

| Setting  | Description  |
|--|--|
| Group address:   | ID for the group, can be a name <sup>a</sup> or a number |
| Group description:   | Description of the group.                                |
| Members:   | Add members/handsets to the group                        |
| a.If it should be possible to send messages from a handset in the Cordless Telephone System or from the System 900 A-bus to the group address, the address has to be a number. |  |

- 5 Click "Activate".

## 4.3 SELECT MESSAGING DESTINATION

Messaging Groups can be used for one messaging interface at a time (DECT System Interface or WLAN Messaging Interface), or both simultaneously, dependent on selection of Default Messaging Destination in the setup wizard. If "WLAN and DECT" is selected, a message is first sent to WLAN and if there is no reply, it is sent to DECT.

- 1 Select "Setup Wizard" on the start page.
- 2 Click "Next" until you reach the Default Messaging Destination page.
- 3 Select which interface to use.

## 4.4 INPUT/OUTPUT SETUP

The CPDM3 hardware has 2 input ports and 2 output ports. Inputs are used to trigger conditions and outputs are used as actions. Example of input is a switch or a button connected to the CPDM3, and example of outputs is a siren or a lamp connected to the CPDM3.

### 4.4.1 DEFINE OUTPUT

- 1 Click "Configuration" on the Start page.
- 2 Select Other Settings > Input/Output.

#### Outputs

| ID | Output Name          | Module Address                         | Output               | Inactive/Initial State  |
|----|----------------------|--|----------------------|---|
| 1  | Internal Output 1    | 127.0.0.1                              | Internal             | 1 High (open-collector) <input type="button" value="Reset"/>  |
| 2  | Internal Output 2    | 127.0.0.1                              | Internal             | 2 High (open-collector) <input type="button" value="Reset"/>  |
| 3  | <input type="text"/> | <input type="text" value="127.0.0.1"/> | <input type="text"/> | <input type="text" value="Low"/> <input type="button" value="Save"/> <input type="button" value="X"/> |

- 3 Click "Define new output".
- 4 Enter a unique Output Name.

- 5 Enter one of the following:
  - If the output ports on this CPDM3 are to be extended by connecting an Output Module, enter the localhost IP address (e.g 127.0.0.1) of the CPDM3.
  - If the output ports are to be used on another CPDM3 or an Output Module is connected to another CPDM3, enter the IP address to that CPDM3.
- 6 If an Output Module is connected, enter the A-bus address of the Output Module.
- 7 Enter one of the following:
  - If the Output ports on another CPDM3 are to be used, enter the output port (e.g 1 or 2) to be used on that CPDM3.
  - If an Output Module is connected to CPDM3, enter the output port to be used on that Output Module (e.g. 1 - 16).
- 8 Select initial state.  
The state is set to the opposite of the initial state when activated. For example, if output 2 is set to "low" in initial state, the output will automatically be set to "high" when activated.
- 9 Click "Save".

#### 4.4.2 DEFINE INPUTS

The hardware has two inputs that can be used. These inputs are predefined at delivery. The states that can be detected are open and close.

| ID | Input Name       | Module Address | Input | Activation | Activation Time |   |
|----|------------------|----------------|-------|------------|-----------------|---|
| 1  | Internal Input 1 | Internal       | 1     | On Opening |                 |   |
| 2  | Internal Input 2 | Internal       | 2     | On Opening |                 |   |
| 7  | MyInput          | Internal       | 2     | On Opening | 4               | ✗ |
| 8  | Test1            | 1              | 1     | On Closing |                 | ✗ |
| 9  | Test2            | 1              | 1     | On Closing | 10              | ✗ |
| 10 | Test3            | 1              | 1     | On Closing | 20              | ✗ |

|    |  |                                   |  |            |  |        |
|----|--|-----------------------------------|--|------------|--|--------|
| 11 |  | <input type="checkbox"/> Internal |  | On Opening |  | Save ✗ |
|----|--|-----------------------------------|--|------------|--|--------|

Save Cancel

- 1 Click "Configuration" on the Start page.
- 2 Select Other Settings > Input/Output.
- 3 Click "Define new input".
- 4 Enter a unique Input Name.
- 5 Enter "IP address" of the module connected to the A-bus.  
Normally localhost, but if the A-bus is connected to another CPDM3 its IP address is set here.
- 6 Enter the Alarm Module's "module address" on the A-bus or select "Internal" depending on if the input is connected via A-bus module or directly to the CPDM3.  
  
If you want to trigger on both opening and closing or using different "Activation time" you can define multiple inputs for the same physical input. This can for example be used if you at a door (by using a microswitch) want an activation on both opening and closing the door. Please see [Appendix D. Alarm Action Configuration Examples](#) on page 165 for other examples.

- 7 Enter "Input number".  
Note: If you have selected the internal check box in the previous step, enter the number of the internal input (1 or 2).
- 8 Select Activation condition.
- 9 Enter Activation Time. By default a notification will be sent immediately. If you enter activation time, the input has to be active for the set time before a notification is sent.
- 10 Click "Save".

#### 4.4.3 ALARM MODULE INPUTS

The number of inputs that can be used on the CPDM3 can be extended by using an Alarm Module connected to the A-bus. The input on the Alarm Module is defined by a name, the module address<sup>1</sup> on the A-bus, and the input number. The states that can be detected are open and close.

See also Installation Guide for T941AM32 Alarm Module, TD 90854GB, and Installation Guide for T941AM8 Alarm Module, TD 90858GB.

#### 4.4.4 OUTPUT MODULE OUTPUTS

The number of outputs that can be used on the CPDM3 can be extended by using an Output Module connected to the A-bus. The output on the Output Module is defined by a name, the module address<sup>1</sup> on the A-bus, and the output number. The initial state can be set to high or low.

See also Installation Guide for T941OM Output Module, TD 90859GB.

### 4.5 ALARM HANDLING

This functionality requires an additional license.

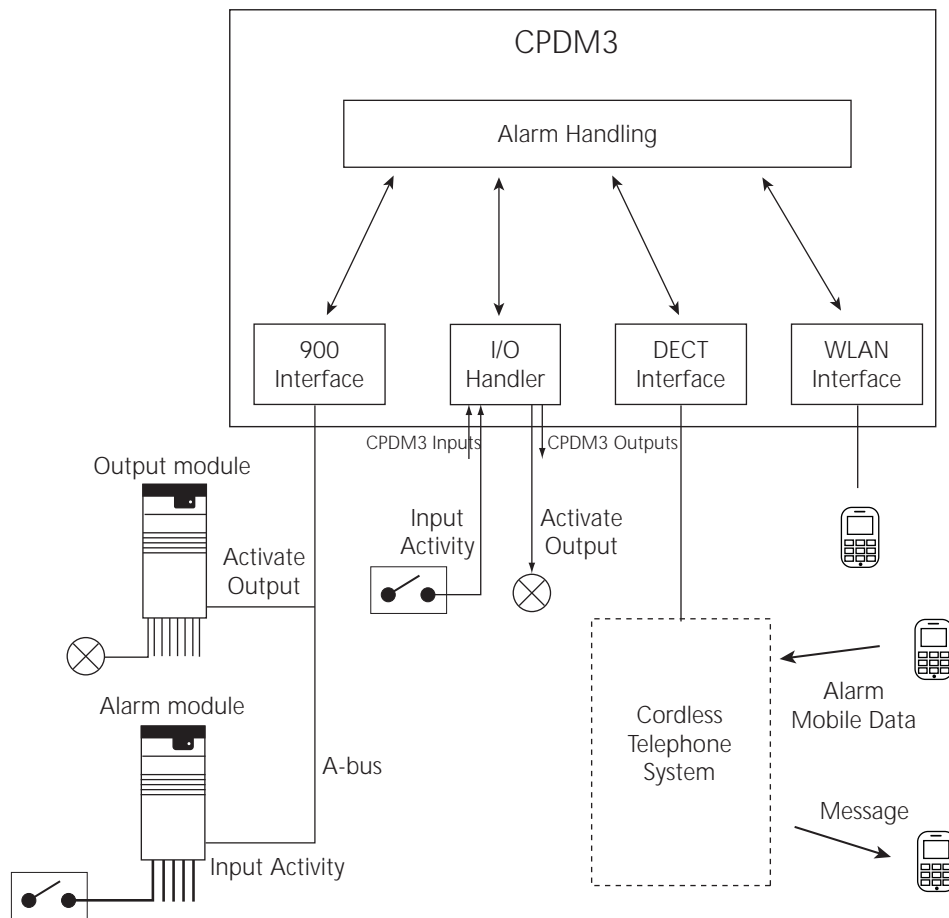
The alarm handling included in CPDM3 makes it possible to trigger on alarms and data from handsets in the Cordless Telephone System. Activated inputs on CPDM3 or a module connected to the A-bus, can also be used as a trigger. As a reaction to the incoming information, messages can be sent to handsets and it is also possible to activate outputs on the CPDM3 or modules connected to the A-bus.

---

<sup>1</sup>.Every module that is connected to the A-bus has a two digit hexadecimal address.



Figure 8. Communication flow for the Alarm Handling and external systems.



For instructions on how to set up Alarm Actions, see [4.5.2 Add Alarm Actions](#).

For examples of how to set up Alarm Actions, see [Appendix D. Alarm Action Configuration Examples](#) on page 165.

### 4.5.1 NOMENCLATURE

|              |  |
|--------------|--|
| Alarm action | An alarm action consists of trigger conditions that leads to an action i.e. sending a message to a handset in the system and/or activating an output. One alarm action can consist of several triggers and lead to several actions. The actions can be repeated at a regular time interval as long as an input is active.                  |
| Input        | An input on the CPDM3 or an input on an Alarm Module connected to the System 900 A-bus.  |
| Output       | An output on the CPDM3 or an output on an Output Module connected to the A-bus.  |
| Trigger      | <p>A trigger is a set of conditions that have to be fulfilled, for example that an input has to be open for a certain time period or that an alarm has been sent from a handset.</p> <p>Several triggers of the same type can be defined for each alarm action. The actions will be carried out when any of the triggers is fulfilled.</p> |
| Action       | Sending a message to a handset or activating an output.  |

Figure 9. Alarm Action view

**Alarm Action**

Name

Notes

Triggers

Select trigger type and click "Add". Several triggers of the same type can be added.

Alarm trigger Add

Actions




Select type of action and click "Add". Several actions can be added.




Message action Add

Save Cancel

### Alarm Handling Icons

On the Alarm Handling pages the following icons can be shown:

-  Reply to sender (Message symbol)
-  Add Call ID
-  Add Alarm Type











-  Add location information
-  Add Input Description
-  Delete

4.5.2 ADD ALARM ACTIONS

- 1 Click “Configuration” on the Start page.
- 2 Select Alarm Handling > Alarm Actions in the menu on the Configuration page.

Alarm Actions

Number of triggers: 6 (250)

| Name                                   | Notes | Triggers   |   |   |
|--|-------|--|---|---|
| Push-button alarm from 1440            |       | Alarm Type: Push-button double press, Number: 1440                     |    |    |
| Alarm cancellation                     |       | Data: 7274   |    |    |
| Cold-storage room closed               |       | Input: Cold-storage, door closed                                       |    |    |
| Cold-storage room open                 |       | Input: Cold-storage, door open<br>Input: Cold-storage, door still open |   |   |
| Cold-storage room, door open very long |       | Input: Cold-storage, door open very long                               |  |  |

Add

- 3 Click “Add”.
- 4 In the Name text field, enter a descriptive name for the alarm action
- 5 In the Notes text field, enter a short description/useful information.

Define Trigger

- 1 In the Triggers drop-down list, select type of trigger.
- 2 Click “Add”.

Several triggers of the same type can be added to the same action.

Triggers

Select trigger type and click “Add”. Several triggers of the same type can be added.

Alarm trigger

Alarm trigger

Input trigger

Data trigger

Add

- Alarm Trigger

- 1 In the Alarm Type drop-down list, select alarm type.

Select trigger type and click "Add". Several triggers of the same type can be added.

**Alarm Trigger**

|                   |               |
|-------------------|---------------|
| <b>Alarm Type</b> | <b>Number</b> |
| Any alarm ▼       |               |

✗

- Any alarm – Trigger on any alarm types
  - Push-button double press (Push-button alarm 1 and 2) – Trigger when a handset sends a Push-button alarm 1 or a Push-button alarm 2.
  - Push-button long press (Test alarm) – Trigger when a handset sends a Test alarm.
  - No-movement/Man-down alarm – Trigger when a handset sends a No-movement alarm or a Man-down alarm.
  - Pull-cord alarm – Trigger when a handset sends a Pull-cord alarm.
- 2 In the Number text field, enter the handset number if the alarm is to be sent from a specific handset. Leave empty if any handset shall be able to trigger the alarm.
  - 3 Click "Add"
- Input Trigger
- 1 In the Input drop-down list, select input trigger. Only inputs defined in the I/O Setup are available. Refer to [4.4 Input/Output Setup](#) on page 30.

### Triggers

Select trigger type and click "Add". Several triggers of the same type can be added.

**Input Trigger**

|  |                            |                               |
|--|----------------------------|-------------------------------|
| <b>Input</b>   | <b>Repetition Time (s)</b> | <b>Max No. of Repetitions</b> |
| <div style="display: flex; align-items: center;"> <div style="border: 1px solid black; padding: 2px; margin-right: 5px;">No selection ▼</div> <div style="border: 1px solid black; padding: 2px;"> No selection<br/>Internal Input 1<br/>Internal Input 2<br/>Prod line 2 problem<br/>Prod line 2 OK </div> </div> | 60                         | 0                             |

✗

- 2 In the Repetition Time text field, enter the interval (in seconds) between repetitions  
Note that this field must be set to min.10 seconds even if no repetitions shall be made.
  - 3 In the Max. No. of Repetitions text field, enter how many times the trigger shall be repeated. For no repetitions, enter '0'.
  - 4 Click "Add".
- Data Trigger

- 1 In the Data text field, enter the data value that shall be used as a trigger. Only exact match is valid, wildcard is not supported.

#### Triggers

Select trigger type and click "Add". Several triggers of the same type can be added.

- 2 In the Number text field, enter handset number if the data is to be sent from a specific handset. Leave empty if any handset shall be able to send the data.

#### Select Type of Action

- 1 In the Actions drop-down list, select type of action.

#### Actions

Select type of action and click "Add". Several actions can be added.


- 2 Click "Add".  
Several actions can be added.

#### • Message Action

The following figure is an example.

#### Actions

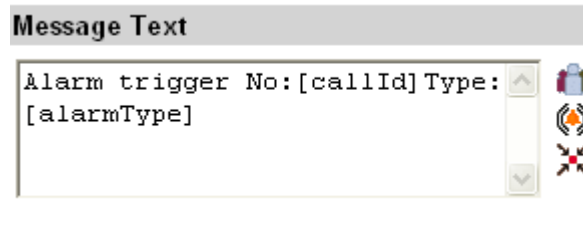
Select type of action and click "Add". Several actions can be added.

- 1 Do one of the following:
  - In the Call ID text field, enter the Call ID that shall receive the message.
  - Click , to the right of the Call ID text field, if the message is to be sent as a reply to the sender of the alarm or data.

- 2 Enter the message text in the Message Text field. By clicking the icons to the right of the text field, you can add valuable information to the message, such as Call ID of the sender, type of alarm and the location<sup>1</sup>.

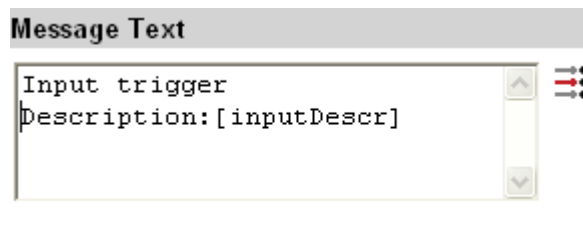
If an input is activated the description of the input can be added.

Figure 10. Available information for the alarm trigger



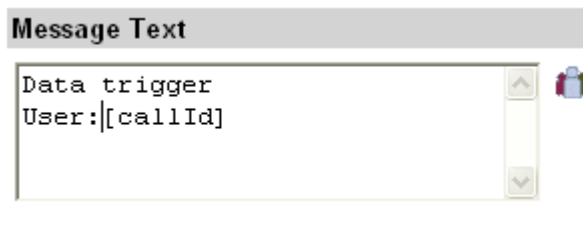
The screenshot shows a text input field titled "Message Text". Inside the field, the text "Alarm trigger No:[callId] Type:[alarmType]" is entered. To the right of the text field, there are three icons: a person icon, a fire alarm icon, and a location pin icon.

Figure 11. Available information for the input trigger



The screenshot shows a text input field titled "Message Text". Inside the field, the text "Input trigger Description:[inputDescr]" is entered. To the right of the text field, there are three icons: a person icon, a fire alarm icon, and a location pin icon.

Figure 12. Available information for the data trigger



The screenshot shows a text input field titled "Message Text". Inside the field, the text "Data trigger User:[callId]" is entered. To the right of the text field, there are three icons: a person icon, a fire alarm icon, and a location pin icon.

- 3 In the Beep Code drop-down list, select number of beeps
- 4 In the Priority drop-down list, select message priority.
- Output Action
- 1 In the Output drop-down list, select which output to activate. Only outputs defined in the I/O Setup are available. Refer to [4.4 Input/Output Setup](#) on page 30.

---

<sup>1</sup>.The location is the ID of the Base Station with the highest signal strength.

**Actions**

Select type of action and click "Add". Several actions can be added.

Output action

Add

---

**Activate Output**

|              |              |
|--------------|--------------|
| Output       | Duration (s) |
| No selection |              |

**Send Message**

|         |              |           |          |
|---------|--------------|-----------|----------|
| Call ID | Message Text | Beep Code | Priority |
|         |              | 2 beeps   | Normal   |

Save Cancel

- In the Duration text field, enter (in seconds) how long the output shall be activated Allowed value is 1 - 3600 seconds.

### 4.5.3 ADD LOCATIONS

- Select Alarm Handling > Locations and click "Add".
- Enter the code for the location in the Code text field.  
TIP: To get the code for the location: 1) select alarm trigger, 2) create a message action, 3) click "Reply to sender" icon to send the message to the sender of the alarm, 4) insert [location] in the message text, 5) trigger an alarm. You will receive the code in the display.
- Enter a short description of the location in the Description text field. Click "Save". When setting up the alarm action this description can be included in the message text.

## 4.6 STATUS

On these pages, information on active faults or stored faults can be shown.

### 4.6.1 ACTIVE FAULTS

Active Faults page is where the last 100 received active persistent fault logs are listed. For more information about the fault log, refer to [4.6.4 Fault Log](#) on page 41.

- Click "Configuration" on the Start page.
- Select Status > Active Faults, in the menu on the Configuration page.

The following information is shown for each fault:

- Time when the fault occurred
- Level of the fault:
  - Critical error

- Error
- Warning
- Description of the fault, as defined in the module
- Type of module
- IP address and host name of the module that generated the fault

By expanding the fault in the list, additional information about the fault is shown containing:

- Fault ID
- This is used to reference a persistent fault when it later is reset
- Fault code
- Description of the fault code
- Extended address information showing the system, bus type and module address
- In the figure below the system is 00, the bus type is 1 and the module address is 0A.

#### Active Faults

Active Faults: 1 - 3

[Collapse all entries](#)

| Time                                      | Level | Description | Module | Address       |   |
|---|-------|-------------|--------|---------------|---|
| 2010-12-13 17:34:44                       | Error | Supervision | CPDM   | 10.30.4.29    | ✗ |
|   |       |             |        |               |   |
| ID: 1C8      3-4-1      Lost link to DECT |       |             |        |               |   |
| No link to DECT (DECT System Interface)   |       |             |        |               |   |
| 2008-10-21 13:54:37                       | Error | Supervision | CPDM   | 172.20.15.200 | ✗ |
|   |       |             |        |               |   |
| ID: 1C8      3-4-1      Lost link to DECT |       |             |        |               |   |
| No link to DECT (DECT System Interface)   |       |             |        |               |   |
| 2008-10-21 13:05:27                       | Error | Supervision | CPDM   | 172.20.10.254 | ✗ |
|   |       |             |        |               |   |
| ID: 1C8      3-4-1      Lost link to DECT |       |             |        |               |   |
| No link to DECT (DECT System Interface)   |       |             |        |               |   |

Persistent faults will remain in the list until the module sends a status message confirming that the module is working properly again. It is also possible to delete the fault in the list by clicking the icon ✗.

NOTE: If the IP address or license is changed in the module, the faults reported for the previous IP address/license will remain since no confirmation can be received. These faults must be manually deleted.

The active faults list page has to be manually updated by clicking the “Update Page” link uppermost on the page.

## 4.6.2 RESET THE ERROR RELAY

The error relay can be reset manually from the Active Faults page.

- 1 Click “Configuration” on the start page.
- 2 Select Status > Active Faults in the menu on the Configuration page.
- 3 Click “Reset” button.



### 4.6.3 LEVEL OF SERIOUSNESS FOR DIFFERENT FAULT TYPES (MODULE FAULT LIST)

A module fault list exists which shows codes and statuses etc. for each module in the system. The level of seriousness can be changed for different fault types in the logs.

- 1 Click "Configuration" on the Start page.
- 2 Select Other Settings > Advanced Configuration, in the menu on the Configuration page.
- 3 Click the "Troubleshoot" button and select "Module Fault List" in the menu.

| Module Supervisor |                                   |            |                    |
|-------------------|-----------------------------------|------------|--------------------|
| Code              | Status                            | Persistent | Seriousness        |
| 7-3-16            | Start of module                   | No         | Information (Defe) |
| 3-3-7             | Reoccurring application failure   | Yes        | Critical (Default) |
| 3-3-8             | Application restarted             | No         | Error (Default)    |
| 10-3-10           | Module key failure                | Yes        | Critical (Default) |
| 12-3-21           | Module running in unlicensed mode | Yes        | Warning (Default)  |
| 12-3-22           | All applications stopped          | Yes        | Critical (Default) |
| 11-3-28           | Module restart                    | No         | Information (Defe) |

| Unite Name Server |                    |            |                    |
|-------------------|--------------------|------------|--------------------|
| Code              | Status             | Persistent | Seriousness        |
| 7-3-15            | Start of component | No         | No Error (Default) |

- 4 Select level of seriousness in the drop-down list for the code(s) for which you want to change level.

### 4.6.4 FAULT LOG

The fault log is a centralized log file and shows a complete log of the faults in the system. Every time a fault message is generated in the system, information about the fault is written to the log file. The maximum number of entries in the log file is 1050. When the log file is full, the 50 oldest entries are removed.

- 1 Click "Configuration" on the Start page.

- 2 Select Status > Fault Log in the menu on the Configuration page.  
The first 25 log entries are shown. To get the following 25 log entries, click the “Next” link.

The following fault levels exist in the log:








- Information
- Individual reset
- All OK
- Critical error
- Error
- Warning

### Fault Log




Entry 1 - 25 (51)

1 .. 25 26 .. 50 51 .. 51 [Next](#)

[Expand all entries](#)

| Time                | Level            | Description   | Module | Address               |
|---------------------|------------------|---|--------|-----------------------|
| 2011-04-13 13:21:00 | Error            |  Supervision<br>Lost link to DECT                  | CPDM3  | 172.20.13.42<br>Elise |
| 2011-04-13 13:20:08 | Information      |  License<br>Module running in demonstration mode   | CPDM3  | 172.20.13.42<br>Elise |
| 2011-04-13 13:20:08 | Individual Reset |  No error  | CPDM3  | 172.20.13.42<br>Elise |
| 2011-04-13 13:20:08 | Information      |  Start of module/component<br>Start of component  | CPDM3  | 172.20.13.42<br>Elise |
| 2011-04-13 13:20:07 | All OK           |  Start of module/component<br>Start of component | CPDM3  | 172.20.13.42<br>Elise |
| 2011-04-13 13:20:06 | All OK           |  Start of module/component<br>Start of component | CPDM3  | 172.20.13.42<br>Elise |
| 2011-04-13 13:20:06 | All OK           |  No error  | CPDM3  | 172.20.13.42<br>Elise |

### Symbols used in the Fault Log

| Symbol  | Description                            |
|---|--|
|  | Active persistent fault                |
|  | Persistent fault that has been handled |
|  | Reset message, no fault exists         |

To get more detailed information about the events, the log entries can be expanded by clicking the “Expand all entries” link. Single log entries can be expanded by clicking the individual “+” icon.

## 4.6.5 ADMINISTER THE FAULT LOG

The Fault log can be exported in a CSV (Comma Separated Values) file format. The log can be cleared from non-active faults and a timeout can also be set to block repeated faults, that is, the fault will be discarded and no actions will be executed.

- 1 Click “Configuration” on the Start page.
- 2 Select select Other Settings > Administer Fault Log, in the menu on the Configuration page.

#### Export the Fault Log in CSV format

- 1 Click "Export".
- 2 Click "Save" in the dialog window and enter the file name (default name statuslog.csv) and the file path.

#### Remove all non-active faults from the Fault Log

- 1 Click "Clear".
- 2 Click "Yes" in the dialog window to remove all non-active faults from the status log file.

#### Set a Timeout to block the Fault log from repeated faults

- 1 Enter the timeout in minutes (0-1000 minutes), the default value is 10 minutes.  
If no Status Logs should be blocked, set the timeout to 0.
- 2 Click "Set timeout" to save the setting.  
An incoming fault will now be handled the first time it is received and then blocked during the set timeout.

### 4.6.6 WLAN HANDSETS

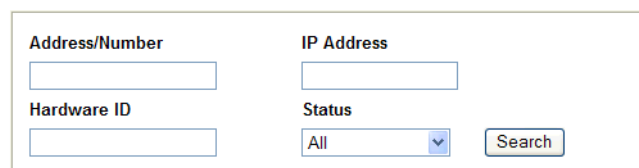
Handset Administration gives you the possibility to list all handsets that are registered in the system, search for a specific handset, or a range of handsets. This is intended to facilitate troubleshooting.

The pages can be customized by changing the number of handsets shown on the search result list.

#### Show all Registered VoWiFi Handsets

- 1 Select "Configuration" on the Start page.
- 2 Click "WLAN Handsets" in the menu on the Configuration page.
- 3 Do one of the following:
  - Click "Search" to search for registered VoWiFi handsets based on different search criterias. For example Address/Number, IP address, Hardware ID (often the MAC address) or the Status of the handset. The Search page opens.

#### Search








|                                       |                                      |
|---------------------------------------|--------------------------------------|
| Address/Number                        | IP Address                           |
| <input type="text"/>                  | <input type="text"/>                 |
| Hardware ID                           | Status                               |
| <input type="text"/>                  | All <input type="button" value="v"/> |
| <input type="button" value="Search"/> |                                      |

- Click "List all" to show all registered VoWiFi handsets.
- 4 The search result can be sorted by address/number, IP address, status or last login. Click the name of the column to be sorted.

Figure 13. Search Result for Registered VoWiFi Handsets

**List All**

5 portables were found

| <input type="checkbox"/> | Address/Number | IP Address    | Status    | Last login          |   |
|--------------------------|----------------|---------------|-----------|---------------------|---|
| <input type="checkbox"/> | 2605           | 172.20.15.183 | Available | 2008-05-09 13:31:41 |  |
| <input type="checkbox"/> | 2606           | Not logged in | Available | 2008-05-08 13:26:37 |  |
| <input type="checkbox"/> | 2607           | Not logged in | Available | 2008-05-08 13:27:08 |  |
| <input type="checkbox"/> | 2619           | Not logged in | Available | 2008-05-08 13:30:50 |  |
| <input type="checkbox"/> | 6374           | 172.20.13.188 | Available | 2008-05-09 13:31:42 |  |

- Address/Number – shows the number of a handset
- IP Address – shows the IP address of a handset that is logged in to CPDM3.
- Status – shows if a handset is available or absent.
- Last login – shows the time of the latest received keep-alive (i.e “relogin”) message sent from a handset. How often the handset sends this message determines by the relogin time configured in CPDM3.

NOTE: This time should not be mixed up with the Last login time shown in the Device Manager. The time in the WLAN Portable GUI is updated each time a keep-alive message is received, but the time in the Device Manager is only updated if the handset is restarted, or if the handset relogs due to lost connection to CPDM3.

### Save a list with all Registered VoWiFi Handsets

The search result list can be exported to a comma separated file.

- 1 Click the “Export Result” button.
- 2 Select “Save”. Enter a file name and the location where the file shall be stored, and click “Save”.

### Remove IP Address, Force a Relogin, or Delete a VoWiFi Handset

- 1 Select the handset(s) check box in the search result list.
- 2 Click “Remove IP Address”, “Force Relogin” or “Delete Selected”.
  - Remove IP Address  
Used for refreshing the address of a handset.
  - Force Relogin  
Used for checking the connection with a handset.
  - Delete Selected  
Used for removing numbers not in use.

### Show Handset Details

Click the icon  in the search result list. All details of the chosen handset are viewed.

## Details

Remove IP

Force Relogin

Delete

|                |                     |   |
|----------------|---------------------|---|
| Address/Number | IP Address          | Current status                          |
| 2302           | 172.20.13.176       | Available                               |
| Hardware ID    | Last login          | Manual Absent                           |
| 00013E1103D0   | 2010-04-16 14:18:21 | Off <input type="button" value="Save"/> |

### 4.6.7 CHANGE THE HANDSET ABSENT STATUS

It is possible to change the Manual Absent status of the VoWiFi handsets.

- 1 View all handsets, refer to [Show all Registered VoWiFi Handsets](#) on page 43.
- 2 Click the icon to view handset details, see [Show Handset Details](#) above.
- 3 In the Manual Absent drop-down list, select “On” or “Off”.

### 4.6.8 EXPORT ACTIVITY LOGS TO A SYSLOG SERVER

Activities in the module are logged and can be exported to a Syslog Server where the logs can be managed and analyzed. Messages are sent to the syslog server every time an activity occur in the module. Example of activities are: An SMS has been sent to a handset, an alarm has been received from a handset, an error has occurred in the module etc. Syslog is a simple protocol (SYStem LOG protocol) for transmitting event messages and alerts text across an IP network. The activities are sent as text messages from the module to the Syslog Server. The IP address to the Syslog Server must be set in the module. The activities can be exported to 5 syslog servers in parallel.

- 1 Click “Configuration” on the Start page.
- 2 Select Activity Log > Log Export in the menu on the Configuration page.
- 3 Select “Enable” in the drop-down list.
- 4 Click the “Add Syslog entry” button.
- 5 Enter the Syslog Server’s IP address in the text field.
- 6 Click “Save”.

#### Administer Activity Log

##### Realtime export

Export

Enable

Syslog server

Server address

## 4.7 MODULE REDUNDANCY

A redundant system consists of an active module and a standby module. When setting up the redundancy in the system, the primary CPDM3 will act as an active module, and the secondary CPDM3 will act as a standby module. If the active module goes down, the system will automatically switch to the standby module that becomes an active module. The modules will indicate that the system no longer is redundant since no data synchronization between the modules can be done.

**IMPORTANT:** A redundant system does not replace a backup of a CPDM3.

### Prerequisites

In order to set up module redundancy in the CPDM3, the following requirements must be fulfilled:

- The installed software version (3.51 or higher) must be identical on both modules.
- The CPDM3 must use the same type of SD memory card. Refer to the CPDM3's Data Sheet for more information on which SD cards that currently are supported.
- The primary CPDM3 must support module redundancy (license dependent feature).
- The secondary CPDM3 must be an empty CPDM3 Basic without any licenses or settings.
- RS232 Data Splitter. Only required if you want to connect equipment via serial interface (for example external equipment via TAP, ESPA or Line protocol)
- Three static IP addresses. Ask your network administrator to obtain the IP addresses.

TIP: See also [Prepare IP addresses](#).

### Prepare IP addresses

**NOTE:** It is assumed that your system already have one CPDM3 installed and that an additional CPDM3 will be installed in order to set up a redundant system.

The three static IP addresses will be used as follows;

- two IP addresses will be used by the primary- and secondary CPDM3.
- the third IP address will be used by the equipment (for example Access Points) to communicate with the active CPDM3 when the system has become redundant. In this document, the third IP address will be called "virtual IP address".

**NOTE:** If a firewall is used between a redundant CPDM3 and an application/system connected to that CPDM3, the IP port 3217 (UDP) has to be open for communication for the primary-, secondary- and virtual IP addresses.

The equipment that communicates with CPDM3 must have the CPDM3's IP address configured. To avoid changing the CPDM3's IP address in the equipment, follow the instructions below:

#### Network without DHCP Server

- 1 Replace the IP address in the origin CPDM3 with the static IP address to be used by the primary CPDM3. The replaced IP address can now be used as virtual IP address by the external equipment.
- 2 Make sure the other CPDM3 to be used as secondary module has been assigned correct IP address.

#### Network with DHCP Server

- 1 Make sure that the origin IP address of the CPDM3 no longer is reserved to the CPDM3's MAC address. Note that the IP address still must be available but not reserved to a specific MAC address. If needed, consult your network administrator. This IP address will be used as virtual IP address later on.
- 2 Ask your network administrator to reserve a new static IP address to the origin CPDM3 that later on will be used for the primary module. The IP address must be reserved to the module's MAC address.
- 3 Ask your network administrator to reserve a static IP address for the CPDM3 to be used for the secondary module. The IP address must be reserved to the module's MAC address.

#### 4.7.1 CONFIGURE MODULE REDUNDANCY

Do the following on the CPDM3 to be used as primary module:

- 1 Click "Configuration" on the start page.
- 2 Select Other > Redundancy on the Configuration page.

### Redundancy

#### Configuration

Configuration of module redundancy

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

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

- 3 In the Virtual IP address text field, enter the virtual IP address.
- 4 In the Virtual netmask text field, enter the netmask of virtual IP address.
- 5 In the Secondary IP address text field, enter the IP address of the secondary CPDM3.
- 6 In the Network monitor IP address text field, enter the IP address of the equipment to be used as network reference. The CPDM3 will check that it has connection to the network by sending ICMP (Internet Control Message Protocol) ping inquiries to this equipment every second. If you do not want you use a network reference, set the IP address to 127.0.0.1.

NOTE: It is highly recommended to use network monitoring when the modules are connected to different switches to avoid "split brain" behavior. See [Appendix I. Network Monitoring in a Redundancy System](#) on page 183.

- 7 Click "Activate".

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

8 Click "Reboot" or "reboot later".

The CPDM3 will now reboot and copy data from its internal flash memory to the SD memory during the start up sequence. This can take up to 3 minutes. The GUI will not be updated automatically when the reboot is done. Update the GUI by clicking the "F5" button on your keyboard. Note that Primary will be stated in the GUI's upper left corner when the module is up and running again.

IMPORTANT: When the module redundancy has been activated, you must not remove the SD memory cards since the modules will use these as data storage instead of the internal flash memory. The CPDM3 will continue to use the SD memory card as data storage even if the redundancy is deactivated.

When the data has been copied, the primary CPDM3 sends configuration settings to the secondary CPDM3 that in turn reboots to apply the settings. After the reboot, the data will be synchronized with the secondary CPDM3's SD memory card. It can take up to one hour to synchronize all data to a SD memory card with 1 GB capacity the first time. During this time, the primary CPDM3 is fully operational.

The LEDs on each CPDM3 indicate the status of the synchronization.

Figure 14. LEDs showing the status of synchronization

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

It is also possible to view the synchronization status via the GUI. Use the virtual IP address to access the active module and the secondary IP address to access the standby module. In the GUI of the primary CPDM3, Primary is shown in the upper left corner. In the GUI of the standby module, Secondary is shown in the upper left corner.

Additionally, information such as synchronization status is also shown.

- Synchronizing - The synchronizing is in progress. Additionally, the amount of data (in percentage) that has been synchronized is also shown.
- Data in sync - The data in both CPDM3 are identical. The system is redundant when this status is shown.
- Data out of sync - The modules are not synchronized. This is shown for example if the connection to the other module is lost.

When the system has become redundant, the virtual IP address will be used by the CPDM3 that currently is active. Note that no configuration can be done on a CPDM3 that is in standby mode.



#### 4.7.2 CONNECTION OF EXTERNAL EQUIPMENT VIA RS232 AND S900 INTERFACE

Connection of external equipment using RS232 serial interface or S900 interface must be connected physically to both CPDM3s. See [Appendix B. RS232 Connections](#) on page 163, or [C.1 System 900/A-bus Connections in a Redundancy System](#) on page 164 for more information.

#### 4.7.3 REDUNDANCY TEST

- 1 Unplug the active module's power cord from the power source.

The standby module will now start up to become an active module which takes up to 60 seconds before all applications are up and running.

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

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

- 2 Enter the secondary module using the virtual IP address. Note that Secondary is stated in the upper left corner indicating that this module currently is the active module.
- 3 Select Status > Active Faults on the Configuration page. The log shows for example that the secondary module is active and that the primary module has failed. Other faults might also be shown.
- 4 Perform an action to ensure that the active module works properly. For example send a message to a handset to check if it receives the message.
- 5 Connect the primary module and check if the secondary module starts to synchronize with the primary module. A completed synchronization is indicated as follows;
  - On the secondary module; the Status LED and the Power LED will be steady blue as long the module acts as an active module.
  - On the primary module; the Status LED is turned off and the Power LED will still flash blue as long the module acts as a standby module.
  - The synchronization status on both modules will be changed to Data in sync when the data is synchronized.

After the test, it is recommended to switch back to the primary module again. See [4.7.5 Fallback to the Primary CPDM3](#) on page 50.

NOTE: When switching between primary- and secondary CPDM3, it might take a while before devices appear in the Device Manager. The parameter Device relogin time determines the maximum time the devices have to re-login to the Device Manager. See [8. Device](#) on page 97.

#### 4.7.4 RESTRICTIONS ON AN ACTIVE SECONDARY MODULE

A secondary module that has become active, has redistricted functionality as follows:

- The secondary module can only be up and running as active module for 30 days without a repaired primary module connected. Note: If you for example shut down the secondary module day 10, it can still use the remaining twenty days when it is started again. If the repaired primary module is not connected within 30 days, the

secondary module will fallback as a standby module meaning that no modules will be up and running.

- It is not possible to disable the module redundancy
- It is not possible to perform a backup restore
- It is not possible to add a license
- It is not possible to run the Wizard
- It is not possible to activate the Demonstration Mode

#### 4.7.5 FALLBACK TO THE PRIMARY CPDM3

When a secondary CPDM3 has become an active one, it will switch back to the primary CPDM3 when the secondary one goes down. It is possible to manually switch back to the primary CPDM3 when it is in standby mode after repair.

NOTE: The network monitoring setting might affect the fallback behavior, see [1.1 Fallback behavior when network monitoring is not used](#) on page 184.

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

On the secondary module, do as follows:

- 1 Click "Configuration" on the start page.
- 2 Select Other > Redundancy on the Configuration page.
- 3 Click the "Fallback to primary module" button.

NOTE: It is only possible to press the button if the data has been synchronized with the primary module.

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

NOTE: When switching between primary- and secondary CPDM3, it might take a while before devices appear in the Device Manager. The parameter Device relogin time determines the maximum time the devices have to relogin to the Device Manager. See [8. Device](#) on page 97.

#### 4.7.6 ACCESS TROUBLESHOOTING PAGES

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

##### **Troubleshooting page on active module**

- 1 Click "Configuration" on the start page.
- 2 Select Other > Advanced Configuration on the Configuration page.
- 3 Click the "Troubleshoot" button on the Advanced Configuration page.
- 4 Click "View Info Log" or "View Complete Log".

##### **Troubleshooting page on standby module**

Click the "Troubleshoot" link on the Standby page.

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

#### 4.7.7 DEACTIVATE REDUNDANCY

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

- 1 Click "Configuration" on the start page.
- 2 Select Other > Redundancy on the Configuration page.
- 3 Click the "Deactivate" button.
- 4 Select one of the following:
  - Click "Cancel deactivate" to undo the deactivation.
  - Click "Really deactivate" to perform the deactivation. Both CPDM3s will now reboot immediately. The GUI will not be updated automatically when the reboot is done. Update the GUI by clicking the "F5" button on your keyboard.
- 5 Do one of the following:
  - If the IP address was changed in the modules: Change the IP address in the former primary CPDM3 to its origin IP address. NOTE: If DHCP server is used, ask your network administrator to reserve the IP address to the module's MAC address.
  - If the IP address was changed in the equipment with configured CPDM3 IP address, change to the origin IP address.

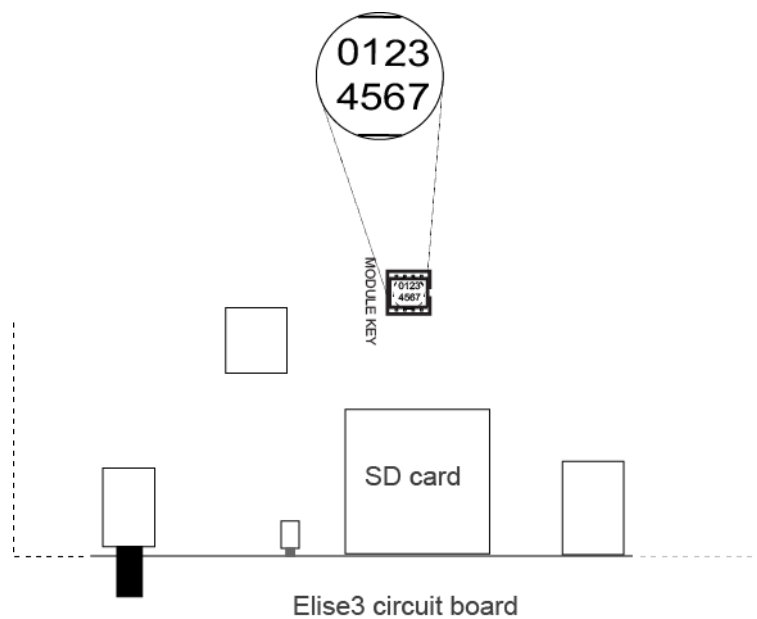
IMPORTANT: Do not remove the SD memory card from the CPDM3 that acted as primary module. The SD memory card on that module will still be used as storage even when the module redundancy has been deactivated.

#### 4.7.8 REPLACEMENT OF BROKEN CPDM3 IN A REDUNDANT SYSTEM

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

The broken primary module:

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



The replacement module:

- 5 Untighten the four screws on the backside of the module by using a torx (T-10) screwdriver.
- 6 Open the housing by pulling top cover towards the backside of the module.
- 7 Replace the module key with the one from the broken module.
- 8 Connect the power source and other cable connections to the primary module.
- 9 Insert a SD card into the module. NOTE: The vendor and capacity must be identical as the SD card inserted in the secondary module.
- 10 Run the Setup Wizard to configure network settings and license settings.
- 11 Configure the module redundancy, see [4.7.1 Configure Module Redundancy](#).

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

## 4.8 BACK UP THE CONFIGURATION

This instruction is used to backup the Device Manager database and the configuration of the CPDM3. The backup file is saved in a proprietary file format and cannot be edited. Save it in a place where you can easily find it for a restore.

- 1 Click “Configuration” on the start page.
- 2 Select Other Settings > Backup/Restore, on the Configuration page.

### Backup/Restore

Backup parameters

---

Restore parameters

- 3 Click “Backup”.

A backup of the current configuration is created and the File Download window opens.

- 4 Click "Save". The Save As window opens.
- 5 Select a location, enter a file name, and save the file.

## 4.9 RESTORE THE CONFIGURATION

When restoring the configuration, all applications and services are terminated until the CPDM3 is up and running after a restart. When CPDM3 is restored, all changes made since the last backup is discarded.

NOTE: A backup of a newer software should not be restored on an older software because the configuration of the new software might not be compatible with the old software. However, a backup of an old software can be restored on a newer software.

- 1 Click "Configuration" on the start page.
- 2 Select Other Settings > Backup/Restore, on the Configuration page.
- 3 Click "Browse" and select the backup file.
- 4 Click "Restore". The text "Backup successfully restored!" will be displayed and inform you when the restore is ready.
- 5 Click "Restart Now" to reboot, else click "Restart Later". If the IP address has been changed, the module needs to be restarted for the settings to take effect.

A restart will take a couple of minutes and during that time the module cannot be reached.

### **Backup successfully restored!**

It is recommended to restart the module after a restore.  
If any passwords or language settings have been changed you must restart your browser for these changes to take effect.

Restart Now

Restart Later

## 5. CENTRAL PHONEBOOK CONFIGURATION

The Central Phonebook makes it possible for users to search and find phonebook entries in a local database or in an LDAP/CMG server, from a handset in the system.

For information about entering phonebook entries, see [4.1 Manage Central Phonebook Entries](#) on page 27.

NOTE: If an LDAP connection to a central phonebook is used, all settings needed are done in the setup wizard but can also be done from the Advanced Configuration page.

### 5.1 TECHNICAL SPECIFICATION

The local database has defined limitations while most of the limitations for the LDA/CMGP server depends on the LDAP server used, see table below.

|   | Local Database           | LDAP/CMG Server  |
|---|--------------------------|------------------|
| Max. No. of phonebook entries:          | 500/2000                 | Server dependent |
| Max. No. of characters in family name:  | 20                       | Server dependent |
| Max. No. of characters in first name:   | 20                       | Server dependent |
| Max. No. of digits in telephone number: | 20                       | Server dependent |
| Max. No. of returned entries / request: | 25                       | 25               |
| Handsets that can access the phonebook: | Depends on handset type. |                  |

### 5.2 CHANGE THE PHONEBOOK ADDRESS

The default Call ID for accessing the phonebook is "999999".

When the Unite Name Server (UNS) is set to forwarding mode, the phonebook Call ID must exist in the module that the requests are sent to. Any change of the Call ID and/or IP address must be made in that module. If the default address is used, no changes are needed.

When the UNS is set to stand-alone mode, do as follows to change the address:

- 1 Click "Configuration" on the Start page.
- 2 Select Other Settings > Advanced Configuration in the menu on the Configuration page.
- 3 Select "Phonebook" in the menu on the Advanced Configuration page.
- 4 Click "Call ID Setting".
- 5 Enter the new Call ID for the phonebook, that is, the Call ID the handsets are using to access the Central phonebook. Check that the Call ID does not conflict with any of the handsets in the system.
- 6 If the phonebook is located on another module, enter the IP address to that module.

## 5.3 CUSTOMIZE THE SEARCH RESULT TEXT

When a request is sent to the central phonebook, a text is included in the response sent to the handset. These texts can be customized, for example translated.

The central phonebook supports search texts with character encoding UTF-8.

NOTE: These settings are not applicable for all handsets.

- 1 Click "Configuration" on the Start page.
- 2 Select Other Settings > Advanced Configuration in the menu on the Configuration page.
- 3 Select "Phonebook" in the menu on the Advanced Configuration page.
- 4 Enter the texts that should be included in the search result, see table below for more information about the different texts and when they are used.

| Default text             | Description  |
|--------------------------|--|
| Search result            | Included in a successful request before the entries that matched the request |
| Sorry, no match          | Sent when there were no match for the sent request.                          |
| Unable to reach database | Sent when connection to the Central Phonebook is lost                        |

## 5.4 SELECT CENTRAL PHONEBOOK DATABASE

Select which database to use for telephone numbers; "Local - 500 Editable", "Local - 2000 View only", or "LDAP", or "CMG".

- If the default local database is selected the entries must be added, either manually or imported from a CSV file, see chapters 4.1.3 on page 27 or 4.1.4 on page 28.
- If LDAP server is selected, continue in chapter [5.5 LDAP Parameter Setup](#) on page 55.
- If CMG is selected, continue in [5.6 CMG Parameter Setup](#) on page 58.

To set database to use for the Central phonebook, do as follows:

- 1 Click "Configuration" on the Start page.
- 2 Select Other Settings > Advanced Configuration in the menu on the Configuration page.
- 3 Select "Phonebook" in the menu on the Advanced Configuration page.
- 4 In the Database for lookups field, choose between "Local - 500 Editable", "Local - 2000 View only", or "LDAP", or "CMG".

If "Local - 2000 View only" is chosen, the "Add" and "Delete all" buttons are not visible in the Edit Phonebook pages.

## 5.5 LDAP PARAMETER SETUP

The Lightweight Directory Access Protocol (LDAP) is an application protocol for querying and modifying directory services running over TCP/IP. The CPDM3 starts an

LDAP session by connecting to an LDAP server. Then it sends operation requests to the server, and the server sends responses in return.

An LDAP directory is a tree of directory entries and follows the structure below:

- An entry consists of a set of attributes.
- An attribute has a name and one or more values.

Each entry has a unique name; the distinguished name (DN). DN consists of its relative distinguished name (RDN) constructed from some attribute(s) in the entry, followed by the parent entry's DN. Think of the DN as a full filename and the RDN as a relative filename in a folder.

An entry can look like this:

```
dn: cn=John Ericson,dc=company,dc=com
cn: John Ericson
givenName: John
sn: Ericson
telephoneNumber: +1 888 555 6789
mail: john@company.com
```

dn is the name of the entry; it is not an attribute nor part of the entry. "cn=John Ericson" is the entry's RDN, and "dc=company, dc=com" is the DN of the parent entry. The other lines show the attributes in the entry. Attribute names are typically mnemonic strings, like "cn" for common name, "dc" for domain component, "mail" for e-mail address and "sn" for surname. See [5.5.1 Examples of Settings](#) on page 57.

- 1 Click the LDAP settings link.

The screenshot shows a 'Phonebook' configuration window. It contains several input fields and dropdown menus for LDAP settings. The fields are: 'LDAP Server or Proxy Address', 'Port Number', 'LDAP Connection Security' (set to 'No encryption'), 'Authentication Method' (set to 'Anonymous'), 'User name', 'Password', 'Search Base DN', 'Number Attribute', 'Type of Name Attribute(s)' (set to 'One containing both first and last name'), and 'Name Attribute(s)' (set to 'cn'). There are 'Previous' and 'Factory' buttons on the right, and 'Activate' and 'Cancel' buttons at the bottom.

- 2 In the LDAP Server or Proxy Address field, enter the IP address or DNS address to the LDAP server.



- 3 In the Port Number field, enter the port number used by the LDAP server. If the field is left empty, port 389 will be used for non-encrypted connection, and port 636 will be used for encrypted connection (LDAP over SSL, called LDAPS).
- 4 In the LDAP Connection Security drop-down list, select if the connection to the LDAP database is to be encrypted.
- 5 In the Authentication Method drop down list, select how to authenticate to the LDAP server.

NOTE: If the authentication method SASL/DIGEST-MD5 is selected, the IP address for primary DNS server must be entered in the DNS server field on the Network setup page. Otherwise it is not possible to authenticate with the LDAP directory Microsoft Active Directory 2003.

- 6 In the User name field, enter the user name used for logging on to the LDAP server. It is a good idea to create a new user in the domain with access for the LDAP server.
- 7 In the Password field, enter the password used for logging on to the LDAP server.
- 8 In the Search Base DN field, enter the user entries' parent DN.  
(The distinguished name for all users common entry.)
- 9 In the Number attribute field, enter the name of the attribute that holds the telephone numbers.
- 10 In the Type of Name Attribute(s) drop down list, select the appropriate option.  
The option depends on if the name is stored in a single attribute or if it is split into two different attributes.
- 11 In the Name Attribute(s) field, enter name(s) of the attribute(s) containing first name and family name. If two attributes are used, enter the first name on the first line and the family name on the second line.
- 12 In the Error message field, enter an error message to be sent as an answer to a phonebook query that was unsuccessful, due to no answer from the server.

### 5.5.1 EXAMPLES OF SETTINGS

- Active directory 2003

Figure 15. Settings for Active directory 2003

Phonebook

LDAP Server or Proxy Address

172.20.9.219

Previous

Port Number

389

Factory

Authentication Method

Simple

User name

ldap-user

Password

•••••

Search Base DN

cn=Users,dc=smallbusiness,c

Number Attribute

telephoneNumber

Type of Name Attribute(s)

Separate attributes for first and last name

Name Attribute(s)

givenName

sn

Error message

Unable to reach LDAP database

Activate

Cancel

5.6 CMG PARAMETER SETUP

The CMG is a central management server used for administration and it includes telephone directory services which can be used by the CPDM3.

Phonebook

CMG Server Address

Previous

Port Number

Factory

User name

Password

Activate

Cancel

- 1 Enter the IP address or host name to the server in the CMG Server Address text field.
- 2 Enter the port number to be used by the CMG server in the Port Number text field.
- 3 Enter user name and password for logging in to the CMG server, in the User name and Password text fields.
- 4 Click “Activate”.

## 5.7 DIGIT MANIPULATION IN CENTRAL PHONEBOOK

When importing telephone numbers it is sometimes necessary to automatically change the way a number is written according to preset conditions.

Depending on where a number is situated, the module can alter the number that is returned in a phonebook query. If, for example, the queried number is situated within the same local exchange, the telephone number is considered to be an internal number and the number is stripped from superfluous international prefixes, etc.

### Telephone number standards

There are several standardized ways of writing telephone numbers.

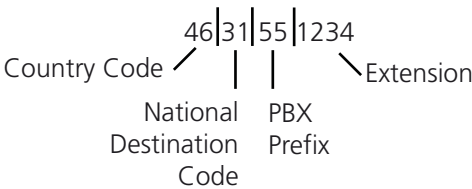
The following formats are currently supported:

| Format         | Comment  |
|----------------|--|
| +4631559300    | E.164 international standard, and E.123  |
| (031)-559300   | E.123 local number   |
| +46(031)559300 | National prefix + national destination code in parentheses   |
| +46(0)31559300 | National prefix in parentheses   |
| +46(31)559300  | Canonical address format   |
| 4631551234     | Digits only. Conversion is controlled by setting maximum lengths of internal and national numbers. |

### Examples

The following figure shows the elements of a telephone number, +46(31)551234 (in canonical format), used in the parameter descriptions below.

Figure 16.



Example of how a telephone number is built up from different prefixes and extensions.

Figure 17. Example of Digit Manipulation Settings

| Phonebook   |   |
|---|---|
| Digit Manipulation  | <input type="button" value="Help"/> Yes |
| Digit Manipulation Enabled  | <input type="button" value="Help"/> Yes |
| Country Code  | <input type="button" value="Help"/> 46  |
| National Destination Code   | <input type="button" value="Help"/> 31  |
| International Prefix  | <input type="button" value="Help"/> 00  |
| National Prefix   | <input type="button" value="Help"/> 0   |
| External Line Prefix  | <input type="button" value="Help"/> 00  |
| PBX First Prefix  | <input type="button" value="Help"/> 55  |
| PBX Second Prefix   | <input type="button" value="Help"/> 56  |
| Maximum size of internal phone numbers  | <input type="button" value="Help"/> 4   |
| Minimum size of global phone numbers  | <input type="button" value="Help"/> 11  |
| <input type="button" value="Activate"/> <input type="button" value="Cancel"/> |   |

The following examples illustrate how digit manipulation works in different queries. The queries are considered to be done from within +463155xxxx (local exchange), see also figure above.

- Example 1: The query is within the same local exchange.  
Queried number: 551234  
Digit manipulation identifies 55 as the local exchange prefix and strips 55 from the number.  
Resulting number: 1234
- Example 2: The query is within the same city (area code), but outside the local exchange.  
Queried number: 031612500  
Digit manipulation identifies 0 as National Prefix and 31 as National Destination Code, strips 031 from the number and adds 00 for external line.  
Resulting number: 00612500
- Example 3: The query is within the same country, but not in the same city.  
Queried number: 035158115  
Digit manipulation identifies 0 as National Prefix and 35 as National Destination Code and adds 00 for external line.  
Resulting number: 00035158115
- Example 4: The query is within another country.  
Queried number: +4781530555  
Digit manipulation identifies "+47" as an international call, skips the "+", and adds 00 for external line prefix and 00 for international prefix.  
Resulting number: 00004781530555

- Example 5: Size of internal number.  
Queried number: 1234  
Digit manipulation identifies that the number of digits in the telephone number is equal to the number of digits entered as "maximum size of internal phone numbers".  
Resulting number: 1234
- Example 6: Size of global number.  
Queried number: 47815305555  
Digit manipulation identifies that the number of digits in the telephone number is equal to the number of digits entered as "minimum size of global phone numbers", then adds 00 for external line prefix and 00 for international prefix.  
Resulting number: 000047815305555

### Digit Manipulation Settings

The parameters for digit manipulation can be set via the Configuration page.

- 1 Click "Configuration" on the Start page.
- 2 Select Other Settings > Advanced Configuration in the menu on the Configuration page.
- 3 Select "Phonebook" in the menu on the Advanced Configuration page.
- 4 Click "Digit Manipulation Settings".

The following parameters can be configured for digit manipulation:

- Digit Manipulation Enabled  
The digit manipulation function can be enabled and disabled. If the function is enabled, the parameters below apply, otherwise they do not apply.
- Country Code  
The Country Code is the prefix to be used when dialling to a particular country from another country. The country code is what follows after the + in a telephone number. The value is used to identify the country code in the number and remove it when it is not needed.
- National Destination Code  
The National Destination Code (NDC) is what follows after the country code in a telephone number.  
The value is used to identify the NDC in the telephone number and remove it when it is not needed.
- International Prefix  
The International Prefix is used to dial a call from a particular country to another country. This is followed by the country code for the destination country.  
This value is used to replace the + character when an international call is made.
- National Prefix  
National Prefix is used to make a call within a country from one city to another. The national prefix is followed by the national destination code for the destination of the call.  
This value is used for two purposes:
  - To identify the national prefix in the number and remove it when it is not needed.
  - To change a number when the destination is another city.
- External Line Prefix  
External Line Prefix is what needs to be dialled before the number to reach the public network.  
The value is used to change the telephone number if it is identified as an external number.

- **PBX First Prefix**  
PBX First Prefix is what precedes an internal number to create an external number. This value is used to compare with the phonebook number to decide whether the number is internal or external.
- **PBX Second Prefix**  
Points out an additional prefix to be handled in the same way as "PBX First prefix".
- **Maximum size of internal telephone numbers**  
Used for numbers that starts with a digit instead of "+" or "(". If the number is longer than this value, it is considered to be an external number.
- **Minimum size of global telephone numbers**  
Used for numbers that starts with a digit instead of "+" or "(". If the number is equal to or longer than this value, it is considered to be a global number.

## 6. SERIAL INTERFACE

This feature requires an additional license, see [1.2 Products for CPDM3](#) on page 7.

The serial interface included in the CPDM3 makes it possible to receive pagers from external equipment and send them to handsets in the system.

The serial interface supports the ESPA 4.4.4 protocol and two ESPA dialects; the Ascom dialect and Ericsson paging dialect with some limitations. The serial interface also supports the TAP 1.8 protocol and a simplified protocol called the Ascom Line protocol.

TAP (Telocator Alphanumeric Protocol) is a paging protocol used to transmit up to a thousand 7-bit characters to an alphanumeric pager. Developed in the early 1980s by the Telocator Paging Association, which later became the Personal Communications Industry Association (PCIA), TAP was also known as IXO and PET. TAP is widely used in the U.S. and throughout Europe.

For limitations in these protocols, see [Appendix E. Protocol Limitations](#) on page 171

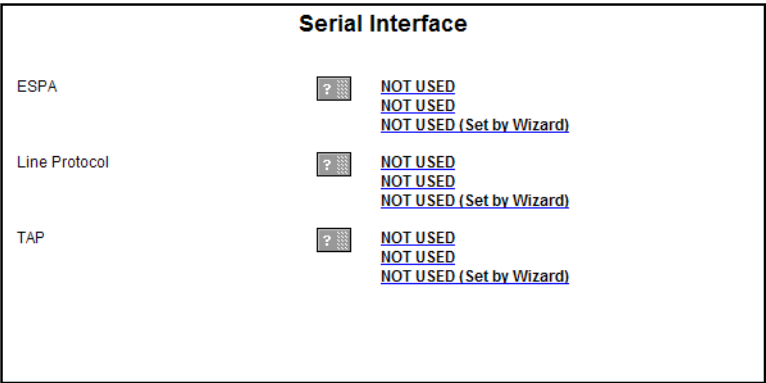
A detailed description of the two ESPA dialects and the Ascom Line protocol can be found in the Protocol, Serial Data Interface S942SI document.

A description of cables for the connections is found in [Appendix B. RS232 Connections](#) on page 163.

### 6.1 SERIAL PROTOCOL SETTINGS

Basic protocol settings are configured in the setup wizard. Detailed and more advanced settings can be configured from the Advanced Configuration page.

- 1 Click "Configuration" on the start page.
- 2 Select Other Settings > Advanced Configuration in the menu on the Configuration page.
- 3 Select "Serial Interface" in the menu on the Advanced Configuration page.



- 4 Click a link for the protocol you want to use (ESPA, Line protocol or TAP).
- 5 Continue in [6.1.1 ESPA Protocol](#), [6.1.2 Line Protocol](#) or [6.1.3 TAP Protocol](#).

### 6.1.1 ESPA PROTOCOL

- 1 The following settings can be selected/changed:

| Settings                              | Description  |
|---------------------------------------|--|
| Enabled:                              | Yes/No selection. Default: No  |
| Name:                                 | Description of the channel   |
| Serial port:                          | Port selection (1,2,3)<br>Default: None<br>Port 3 will be selected when set from the setup wizard, but all three ports can be configured here. |
| Bit rate:                             | Select bit rate. Default: 9600 bits/s.   |
| Mode:                                 | Select mode. Default: 8 Data bits, Even parity   |
| Flow control:                         | Used for handshaking control. Default: None  |
| ESPA dialect:                         | Select dialect, with or without an extra Carriage Return (CR).<br>Default: TeleCourier extensions (i.e. Ascom dialect)                         |
| Control station selection:            | Determines which module shall act as control station. Default: External equipment.   |
| Address of external equipment:        | Enter address (0 - 9). Default: 1  |
| Address of this module:               | Enter address (0 - 9). Default: 2  |
| Default Call ID:                      | Number to call if not specified in the external equipment. Default:000   |
| Default display message:              | Message to display if not specified in the external equipment. Default: BLANK  |
| Default message priority:             | Priority if not specified in the external equipment. Default: 7 (Normal)   |
| Default beep code:                    | Beep code if not specified in the external equipment. Default: 2 beeps.  |
| Default method for ack.:              | Select how the paging shall be acknowledged if not specified by the external equipment. Default: No Ack.                                       |
| Default urgency:                      | Urgency if not specified in the external equipment. Default: Normal.   |
| Transmission delay (x10 ms):          | How long to wait before transmission to external equipment. Default: 30 milliseconds   |
| Identical pagings treatment:          | How to handle identical pagings. Default: Not accepted.  |
| Running number to external equipment: | If running number shall be sent or not. Default: No  |
| Timeout mode:                         | Determines when to start timeout mode i.e. remove paging from queue. Default: after "Call Terminated" call status.                             |



|   |  |
|---|--|
| Timeout mode TTL (seconds):                   | Determines the time for timeout mode i.e. during this time the paging remains in the queue after the "Timeout mode" has started. Default: 5 seconds.   |
| Manual Ack type:                              | Dependent on if the external equipment supports negative acknowledge. Default: Positive and Negative manual acknowledge.   |
| Manual Ack TTL (minutes):                     | How long a paging with manual acknowledge remains in the queue after transmission of Call Terminated call status. Default: 5 minutes.  |
| Message Ref. ID TTL (minutes):                | How long a Message Reference ID remains in queue. Only valid for Ascom dialect. Default: 5 minutes.  |
| Return Status Information:                    | Defines if status information for ongoing pagings shall be sent back to external equipment. Set to "No" if external equipment have problems in handling status information. Default: Yes.          |
| Supervision time for communication (seconds): | Defines the time before lost communication with external equipment will be considered as a fault and sent as a Status log. If set to "0" no supervision is done.<br>Max 3600 seconds<br>Default: 0 |
| ASCII conversion table:                       | Makes it possible to convert display message characters.   |

- 2 Click "Activate".

### 6.1.2 LINE PROTOCOL

- 1 The following settings can be selected/changed:

| Settings                  | Description  |
|---------------------------|--|
| Enabled:                  | Yes/No selection. Default: No  |
| Name:                     | Description of the channel   |
| Serial port:              | Port selection (1,2,3)<br>Default: None<br>Port 3 will be selected when set from the setup wizard, but all three ports can be configured here. Note that only one at the time can be used. |
| Bit rate:                 | Select bit rate. Default: 9600 bits/s  |
| Mode:                     | Select mode. Default: 8 Data bits, Even parity   |
| Flow control:             | Used for handshaking control. Default: None  |
| Default Call ID:          | Number to call if not specified in the external equipment. Default: 000  |
| Default display message:  | Message to display if not specified in the external equipment. Default BLANK   |
| Default message priority: | Priority if not specified in the external equipment. Default: 7 (Normal)   |

|                              |   |
|------------------------------|---|
| Default beep code:           | Beep code if not specified in the external equipment.<br>Default: 2 beeps                           |
| Transmission delay (x10 ms): | How long to wait before transmission to external equipment. Default: 30 milliseconds                |
| Status to ext equipment:     | If status characters ACK/NAK shall be sent on protocol level to external equipment.<br>Default: Yes |
| Start character:             | Start character for the message.<br>Default: < (3C Hex)   |
| End character:               | End character for the message.<br>Default: > (3E Hex)   |
| Record separator character:  | Record separator character for the message.<br>Default: / (2F Hex)                                  |
| ACK character:               | Character for positive acknowledge of the message. Default: A (41 Hex)                              |
| NAK character:               | Character for negative acknowledge of the message. Default: N (4E Hex)                              |
| ASCII conversion table:      | Makes it possible to convert display message characters.  |

- 2 Click "Activate".

### 6.1.3 TAP PROTOCOL

- 1 The following settings can be selected/changed:

| Settings                  | Description   |
|---------------------------|---|
| Enabled:                  | Yes/No selection. Default: No   |
| Name:                     | Description of the channel  |
| Serial port:              | Port selection (1,2,3)<br>Default: None<br>Port 3 will be selected when set from the setup wizard, but all three ports can be configured here.<br>Note that only one at the time can be used. |
| Bit rate:                 | Select bit rate.<br>Default: 9600 bits/s  |
| Mode:                     | Select mode.<br>Default: 8 Data bits, Even parity   |
| Flow control:             | Used for handshaking control. Default: None   |
| Default Call ID:          | Number to call if not specified in the external equipment. Default: 000   |
| Default display message:  | Message to display if not specified in the external equipment. Default: BLANK   |
| Default message priority: | Priority if not specified in the external equipment.<br>Default: 7 (Normal)   |

|  |  |
|--|--|
| Default beep code:                                     | Beep code if not specified in the external equipment.<br>Default: 2 beeps  |
| Default urgency:                                       | If set to High "Stand-by" mode in receiver is broken through.<br>Default: Normal.  |
| Transmission delay (x10 ms):<br>(Advanced)             | How long to wait before transmission to receiver.<br>Default: 30 milliseconds  |
| Enable checksum validation:<br>(Advanced)              | Set to "No" if, for example, external equipment uses an algorithm that differ from the 7-bit value used in TAP.<br>Default: Yes        |
| Delay time before log on timeout occurs:<br>(Advanced) | How long to wait before disconnecting the external equipment.<br>Valid values: 0-127 where 0 means 'Not enabled'.<br>Default 8 seconds |
| Delay time before block timeout occurs:<br>(Advanced)  | How long this module shall wait before hanging up.<br>Valid values: 0-127 where 0 means 'Not enabled'.<br>Default 4 seconds.           |
| Numbers of allowed times to log on:<br>(Advanced)      | How many logon attempt from external equipment shall be permitted.<br>Valid values: 1-127.<br>Default 3 tries.                         |
| Numbers of allowed checksum failures:<br>(Advanced)    | How many checksum failures from external equipment shall be permitted.<br>Valid values: 1-127.<br>Default 3 tries.                     |
| Numbers of allowed timeouts:                           | How many timeouts shall be permitted.<br>Valid values: 1-127.<br>Default 3 timeouts.   |
| ASCII conversion table:                                | Makes it possible to convert display message characters.   |

- 2 Click "Activate".

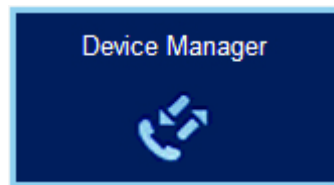
## 7. DEVICE MANAGER

NOTE: Make sure that the Device Manager is configured to communicate with the interface (for example IP-DECT) the devices are connected to. If not, the devices will not appear in the Device Manager. See [8.1 Device Management Setup](#) on page 97.

The Device Manager can manage large sets of devices and contains a solution for:

- Centralized software upgrade on a set of devices and configuration of devices
- Central database storage for all device settings

In the Device Manager, much of the work is done with Devices, Numbers and Templates.



### 7.1 DESCRIPTION

This section gives a description of the Device Manager application in the CPDM3 and how it is intended to be used.

#### 7.1.1 DEVICE MANAGER TERMINOLOGY

This section gives a brief description of the basic terminology in the Device Manager.

|                           |   |
|---------------------------|---|
| Device                    | Can be a charger, a handset, or a fixed device (such as IP-DECT base station) that can be connected to the module.                  |
| Number <sup>a</sup>       | The complete settings for a single device.  |
| Template <sup>a</sup>     | General settings for a specific device type. A template can be applied to several Numbers of the same device type.                  |
| Tabs                      | In the Device Manager there are different views, or tabs. In these tabs, the information for devices, Numbers, templates are shown. |
| Parameter definition file | A file including all possible settings for a certain device type. Templates are created from parameter definition files.            |
| Software                  | The software used in devices. The device software can be updated via the module.  |
| Version                   | Parameter definition files and device software are indicated by versions.   |
| Package file              | A file that can contain other files, such as parameter definition files, software files and template files.                         |

|                        |   |
|------------------------|---|
| Importing              | Different types of files can be imported. Note that if a software file should be imported, it may have been delivered in a package file.  |
| Associate <sup>a</sup> | Before being able to synchronize parameters between the CPDM3 and devices, it is necessary to associate a Number with the device. Association includes all parameters. If it exists on that device type, it also includes Contacts. |
| Assign <sup>a</sup>    | It is possible to assign a Number to a device that has not yet been assigned a Number in the Device Manager. Assign includes only the parameters defining the Number.   |

a.Not applicable for fixed devices.

7.1.2 HOW TO USE THE DEVICE MANAGER

The following list is a short description to give a basic understanding on how to use the Device Manager with devices. It is not intended to be used as a work flow description.

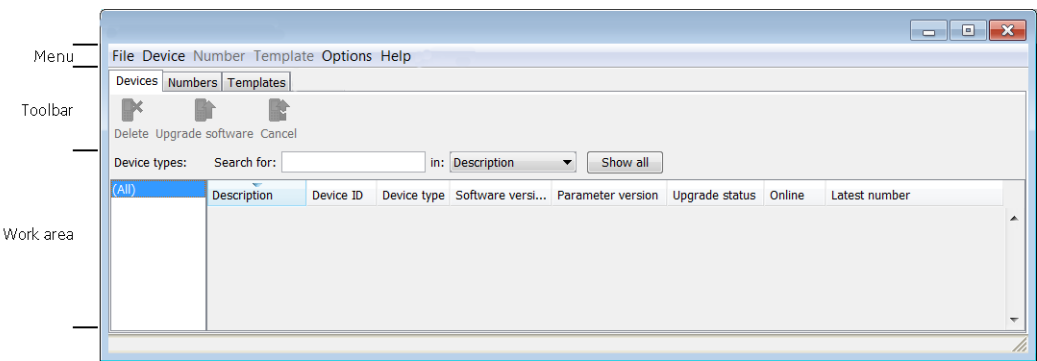
- Import a parameter definition file of the corresponding device type to Device Manager.
- Create a template from the parameter definition file.<sup>1</sup>
- Add a device to the Device Manager.<sup>1</sup>
- Create a new Number for the corresponding device type.<sup>1</sup>
- Upgrade the software of a device
- Associate the Number with the device.<sup>1</sup>

Refer to applicable manual for a description of the work flow.

7.1.3 DEVICE MANAGER GUI

The Device Manager window has a menu bar, a toolbar and a work area. The toolbar has different tabs and when a tab is selected the available device types will be shown in the left hand pane of the work area. The right pane shows devices, numbers, templates, or licenses already configured.

Figure 18. Device Manager Window



1.Not applicable for fixed devices.

The upper part of the work area has search fields with different search criterias for each tab.

### Sort and Filter the Lists

By default, the lists are sorted as follows:

- Devices tab – sorted by Device ID
- Numbers tab – sorted by Number
- Templates tab – sorted by Name

To sort the list by any other column, click the appropriate column heading. To reverse the sort order, click the column heading again. The sorting order is indicated by an up or down arrow in the column heading.

By default, the list in each tab shows all available Devices, Numbers or Templates, but it is possible to filter the list by selecting the desired device type in the left hand pane of the work area.

## 7.1.4 COLOR CODED INFORMATION

### Color coding for lists in tabs

- If the version number is shown in red, the Device Manager has found no parameter definition files supporting that device type.
- If the version number is shown in dark red, the parameter definition file is compatible, but does not have exactly the same version as the device.

### Color coding for parameter and template editing

In the parameter and template editing windows, the following color coding is used:

| Color     | Context                             | Description  |
|-----------|-------------------------------------|--|
| Black     | General                             | Normal   |
| Dark blue | For templates and parameter editing | Parameter has been edited during the current session |
| Purple    | For templates                       | The parameter is included in the template (checked)  |
| Red       | For templates and parameter editing | Value not valid                                      |
| Turquoise | For templates and parameter editing | The value differs from the default value             |

## 7.1.5 NAVIGATION

For keyboard short-cuts, see [Appendix F. Device Manager Keyboard Shortcuts](#) on page 174.

## 7.1.6 TABS


The Device manager has different views, or tabs:

- Devices tab
- Numbers tab
- Templates tab

Each tab shows information about devices, Numbers, or templates. Some information overlaps, for example Device ID, which is tied to both a specific device and to a specific Number. Different menus are accessible in the different tabs.





### Devices Tab

The Devices tab shows all devices configured at the site in a detailed list. The following information can be displayed (see also [figure 18](#) on page 69):

- Description – optional information of a Number that can be added by the user. For example, the user of the device.
- Device ID – the unique identifier of the device.
- Device type – the device model.
- Software version – shows the version of the software in the device.
- Parameter version – shows the version of the parameters in the Number.
- Upgrade status – might show one of the symbols shown in table 2 below.
- Online – shows if the device is connected to the Device Manager. The symbol  indicates a connected device.
- Latest Number – shows the latest known Number for a device.

The columns order can be changed and the application will keep the changes.

Table 2. Upgrade status symbols


- |   |   |
|---|---|
|    | – software upgrade in progress.<br>It is also possible to see a progress bar when the device is being upgraded. |
|  | – software upgrade Pending, Request sent, or Accepted (a green arrow).  |
|  | – software upgrade Scheduled or Retrying.   |
|  | – the last upgrade Failed or Aborted (a red broken arrow).  |
|   | – “Completed”, no symbol is shown   |

NOTE: A software upgrade should be done on one device to start with. If successful, the remaining devices can be updated in one operation.

- IP address - shows the IP address of the latest logged in device (e.g VoWiFi handset or IP-DECT Master). In the case a IP-DECT handset logs in Over the Air (OTA), the IP address of the IP-DECT Master where the handset is registered is shown.
- Serial number - shows the serial number of the latest logged in device.

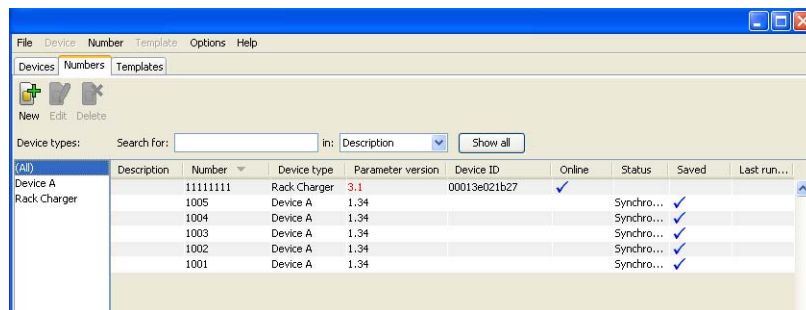
### Numbers Tab

The Numbers tab shows all Numbers configured at the site in a detailed list. Following columns are displayed:

- Description – optional information of a Number that can be added by the Device Manager user. For example, the user of the number.
- Number – the unique identifier of the Number. The identifier is unique for that device type.
- Device type – the device model the Number is intended for
- Parameter version – shows the version of the parameters in the Number
- Device ID – the unique identifier of the device that the Number is associated to
- Online – shows if the device the Number is associated to is online. The  symbol indicates an online device

- **Status** – shows the parameter synchronization status. A Number can also be queued for synchronization. Several different indications are used, for example Synchronizing, Sync queued, Save queued, Synchronized, etc. When the Number is offline, the database status is shown; Synchronized or Not synched.
  - **Saved** – shows if the Number's parameters have been stored in the database. The ✓ symbol indicates that the parameters have been stored
  - **Last login** – shows the date and time the device was last online in the Device Manager/logged in to Device Manager.
  - **Last applied template** – indicates which template that was last applied for that Number
- The columns order can be changed and the application will keep the changes.

Figure 19. The Numbers tab showing a list of Numbers in a system.



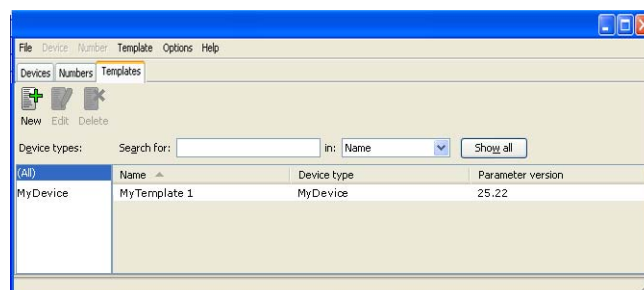
## Templates Tab

NOTE: This tab is not applicable for fixed devices.

The Templates tab shows all templates in a detailed list. The following columns are displayed:

- **Name** – the name of the template
- **Device type** – the device model the template is intended for
- **Parameter Version** – shows the parameter version

Figure 20. The Templates tab in the Device Manager





## 7.2 LOGGING ON TO THE DEVICE MANAGER

NOTE: When an attempt is made to start the Device Manager, a dialog window is displayed with a warning that the program's digital signature cannot be verified. The text is displayed in the language used in the computer's operating system. Click "Run" (or the equivalent term in the operating system language).

NOTE: Ten clients can be logged in at the same time, but to avoid conflicts make sure that only one at a time is updating Numbers.

- 1 Log on to the module.
- 1 Enter User name and Password and click "OK".
- 2 Click "Device Manager" on the start page.

### 7.2.1 CLOSING THE DEVICE MANAGER

In the File menu, click "Exit". The Device Manager shuts down.

## 7.3 TEMPLATES

NOTE: Templates are not applicable for fixed devices.

By using a template, the same configuration can easily be applied to many devices simultaneously. Templates are also an efficient way to give good control over which changes that are applied to each device.

Templates enable configuration of all aspects of a handset from sound volume to keypad shortcuts.

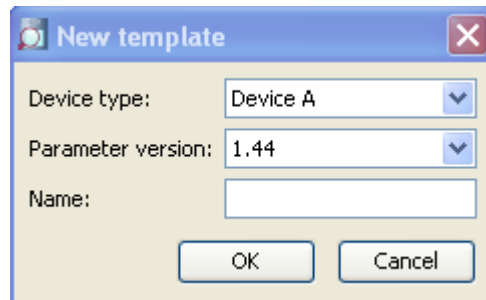
Your supplier can provide example templates for different PBXs. The handset will have full functionality towards the PBX even without such a template. By using such a template, though, the handset will be customized for that PBX with menu options for PBX specific functions such as Callback.

NOTE: The device settings are unexchangeable between device types. For example, a template for device type Device A can only be used on that device type, and not on a different device type (e.g. Device B), and vice versa.

### 7.3.1 CREATE A PARAMETER TEMPLATE

It is usually desirable to create a customized parameter template that can be applied to all devices of a certain device type.

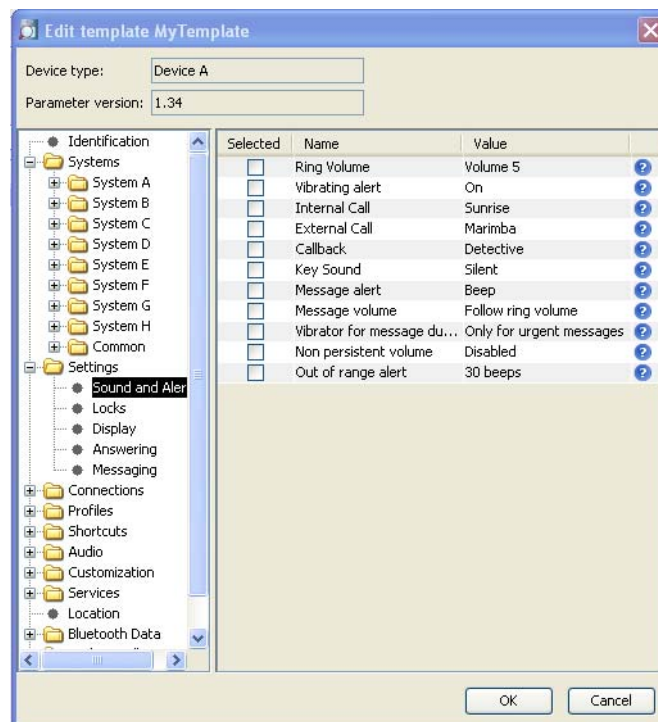
- 1 Select the “Templates” tab and click “New”. The Create template dialog opens.



- 2 Select device type and parameter version, type in a name for the template, and click “OK”. The view switches to the Edit Template parameter view.

NOTE: If you cannot find your device type and/or parameter version in the list, the Device Manager needs to be updated with new parameter definition files, see [7.6.3 Import Parameter Definition Files](#) on page 88.

Figure 21. Edit Template parameter view.



- 3 Select the parameters you want to be saved in the template by selecting the check box to the left of each parameter.
- 4 Change the parameters to the desired values.
- 5 Click “OK”.

### 7.3.2 SAVE A DEVICE CONFIGURATION AS A TEMPLATE

It is possible to use an already configured device and save it as a template. The template will contain configuration data and will not include contacts and other personal data if it is a handset.

This template can be used as a backup if you later want to restore the configuration of the device, or as a template to be applied on a number of devices.

- 1 Some parameters are user specific. If it is decided to apply this type of template to several handsets, it is recommended to exclude the following parameters:
  - Owner ID - A text string specified in standby mode. The parameter is located directly under “Settings”.
  - Phone lock PIN code - The security code used to unlock the keypad. The parameter is located under Settings > Locks.
- 2 Open the Device Manager.
- 3 Select the Numbers tab and select the handset you want to save as a template.
- 4 Right-click and select “Use as a template...”. Enter a descriptive name for the template.
- 5 The Edit template window is opened. By default, all parameters are selected and are saved when clicking “OK”.  
  
If one or more parameters should be excluded, remove them by clearing the check box next to the parameter.
- 6 Click “OK”.

NOTE: When the Edit template window is opened from the “Use as template” command, an extra drop-down list is shown in the bottom left corner. This setting decides which parameters that shall be copied from the Number. If “All parameters” is selected, the synchronization time will be longer.

It is also possible to create a template from a handset that is online but not stored in the database. The template will contain all parameters for the device except for those that are Number specific.

### 7.3.3 RENAME A TEMPLATE

- 1 Select the “Templates” tab.
- 2 Select the template you want to rename. The selected row is highlighted.
- 3 In the Template menu, select “Rename...” or right-click and select “Rename...”. The Rename template dialog opens.
- 4 In the Rename template dialog, enter a new name in the New name text field.
- 5 Click “OK”. The dialog window closes and the new name appears in the list.

### 7.3.4 COPY A TEMPLATE

- 1 Select the “Templates” tab.
- 2 Select the template you want to copy. The selected row is highlighted.
- 3 In the Template menu, select “Copy...” or right-click and select “Copy...”. The Copy template dialog opens.
- 4 In the dialog window, enter a new name in the New name text field.
- 5 Click “OK”. The dialog window closes and the new template appears in the list.

### 7.3.5 EDIT A TEMPLATE

- 1 Select the “Templates” tab.
- 2 Select the template you want to edit. The selected row is highlighted.

- 3 In the Template menu, select “Edit...” or right-click and select “Edit...”. The Edit template window opens.
- 4 In the Edit template window, edit the parameters that shall be edited.
- 5 Click “OK”.

### 7.3.6 DELETE A TEMPLATE

- 1 Select the “Templates” tab.
- 2 Select the template you want to delete. The selected row is highlighted.
- 3 In the Template menu, select “Delete”, or right-click and select “Delete”, or press the Delete button. The Delete template dialog opens.
- 4 Click “Yes”. The dialog window closes and the template is deleted.

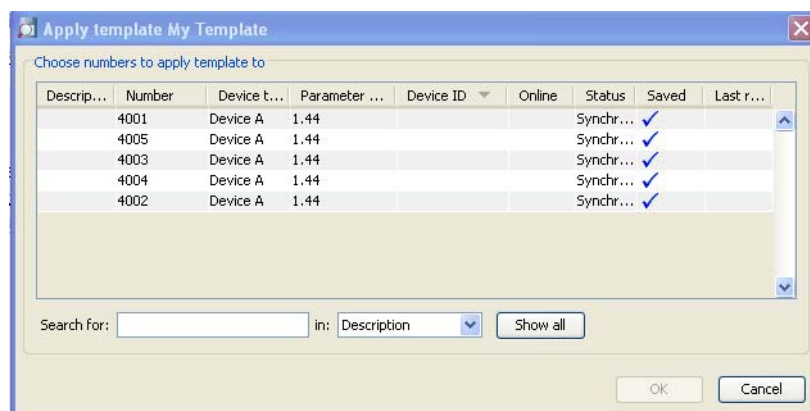
### 7.3.7 UPGRADE A TEMPLATE

NOTE: In order to upgrade a template, the new parameter version must have the same major version as the old parameter version. For example, upgrading from 25.8 to 25.9 works, but not upgrading from 25.8 to 26.x.

- 1 Select the “Templates” tab.
- 2 Select the template you want to upgrade. The selected row is highlighted.
- 3 In the Template menu, select “Upgrade...” or right-click and select “Upgrade...”. The Upgrade template dialog opens.
- 4 Select the parameter version to upgrade to.
- 5 Click “OK”. The template is upgraded and the dialog window closes

### 7.3.8 APPLY A TEMPLATE

- 1 Select the “Templates” tab.
- 2 Select the template you want to use. The selected row is highlighted.
- 3 In the Template menu, select “Apply to...” or right-click and select “Apply to...”. The Apply template window opens.



- 4 If needed, select search parameters or click “Show all”.
- 5 Select Number(s) to apply the template on.
- 6 Click “OK”. The template is applied and the dialog window closes.

## 7.4 NUMBERS

NOTE: The device settings are unexchangeable between device types. For example, a number for device type Device A can only be used on that device type, and not on a different device type (e.g. Device B), and vice versa.

NOTE: Templates are not applicable for fixed devices.

### 7.4.1 CREATE NEW NUMBERS

- 1 Select the "Numbers" tab.
- 2 In the Number menu, select "New...". Alternatively, right-click in the Numbers list and select "New...".
- 3 In the Device type drop-down list, select device type.
- 4 In the Parameter version drop-down list, select the parameter version.
- 5 In the Template drop-down list, select template to run on the Number. This is optional and therefore "None" can be selected.
- 6 In the Prefix field, enter the Number's prefix (if needed).
- 7 Select one of the following options:
  - To create a single Number, select the Single option and enter the call number. Click "OK".
  - To create a range of Numbers, select the Range option. Enter the start call number, end call number, and click "OK".

Note: The maximum range that can be added at a time is 100 Numbers.

### 7.4.2 SAVE A NUMBER TO DATABASE

An online device can be saved to the database.

- 1 Select the "Numbers" tab.
- 2 Select the Number.
- 3 In the Number menu, select "Save". Alternatively, right-click the Number and select "Save"

**Tip:** An online device can automatically be enabled and saved (default), see [7.8.1 Automatically enable new Devices Settings](#) on page 95 for more information.

### 7.4.3 ENTER/EDIT DESCRIPTION OF A NUMBER

It is possible to enter information about a Number. For example, the user of the number or the location of the device.

- 1 Select the "Numbers" tab.
- 2 Select the Number.
- 3 In the Number menu, select "Enter description". Alternatively, right-click the Number and select "Enter description".
- 4 Enter an appropriate description and click "OK" to save the setting.

## 7.4.4 CERTIFICATE HANDLING FOR VOWIFI HANDSET

NOTE: This function is applicable for some VoWiFi handsets only.

Certificate(s) is used for authorizing a VoWiFi handset to access a WLAN system using Extensible Authentication Protocol (EAP).

There are two types of certificates: Root certificate and client certificate.

The VoWiFi handset uses the root certificate to control if the WLAN system is trusted. If the system is trusted, the handset send its client certificate to show that it is authorized to access and log on to the system.

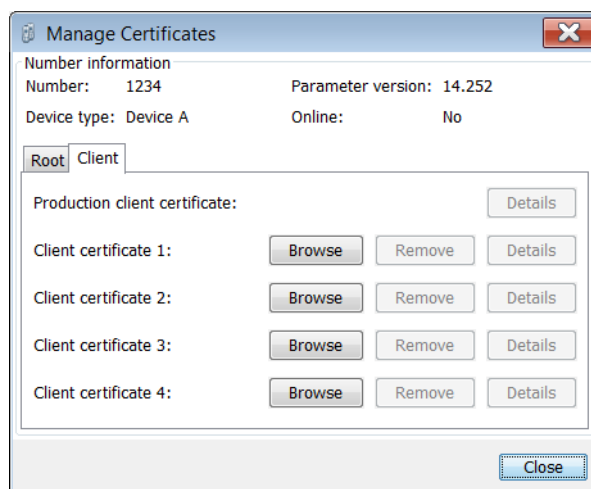
The root- and the client certificate contain a public key, but the client certificate also contains a private key.

The following must be done to be able to use certificates:

- Import certificates to handset
- Select which client certificate to use by setting an EAP client certificate parameter, see the Configuration Manual for the VoWiFi handset.

### Import Certificate

- 1 Select the “Numbers” tab.
- 2 In the Number menu, select “Manage certificates”. Alternatively, right-click the handset in the Numbers list and select “Manage certificates”.



- 3 Click the Root- or the Client certificate tab depending on which certificate to be managed.
- 4 Click “Browse” and locate the certificate file to be imported.
- 5 If the certificate is passport protected, an Enter Password dialog opens. Enter the password and then click “OK”.

A Confirm Certificate window opens showing the details of the certificate.

- 6 Import the certificate to the handset by clicking “Yes”.

If needed, repeat step 3 - 5 for importing additional certificates.

### View Certificate Details

- 1 Select the “Numbers” tab.

- 2 In the Number menu, select "Manage certificates". Alternatively, right-click the handset in the Numbers list and select "Manage certificates".
  - 3 Click the "Root" tab or the "Client" tab depending on which certificated to be viewed.
  - 4 Select the certificate to view by clicking the corresponding "Details" button.
- A Certificate details window appears showing the details of the certificate.

#### **Remove Certificate**

- 1 Select the "Numbers" tab.
- 2 In the Number menu, select "Manage certificates". Alternatively, right-click in the handset in the Numbers list and select "Manage certificates".
- 3 Click the "Root" tab or the "Client" tab depending on which certificated to be removed.
- 4 Select the certificate to remove by clicking the corresponding "Remove" button.
- 5 Click "Yes" to confirm the deletion.


The certificate is now removed from the handset.

### **7.4.5 PARAMETER TRANSFER BETWEEN A DEVICE AND THE DEVICE MANAGER**

When a device is connected, it is synchronized with the associated Number in the Device Manager, see [7.5.2 Synchronize a Device](#) on page 84.

NOTE: When parameters have been edited and the device is synchronized, only the edited parameters will be sent to the device.

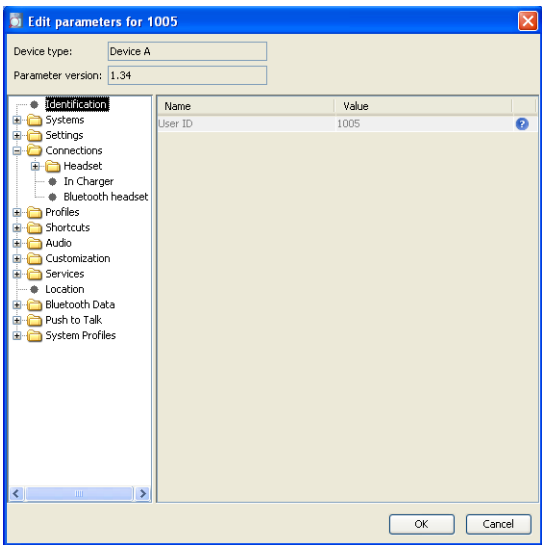
### **7.4.6 EDIT PARAMETERS FOR A NUMBER**

The Edit parameters window shows the set of parameters relevant to the Number that is being edited. The parameter groups are organized in a tree structure in the left pane, with the parameters in the current node in the right pane. The parameter list has one column with the parameter name, and another column shows the parameter value. This can be for example a numerical value, a boolean value, or text. Clicking the  icon will give a short description of the selected parameter.

- 1 Select the "Numbers" tab. The Number view opens.
- 2 Select the Number. The selected row is highlighted.
- 3 Click "Edit" in the Number menu. Alternatively, right-click and choose "Edit", or double-click the Number.

The Edit Parameters for <Number> window opens, where <Number> is the ID of the current Number.

Figure 22. Editing parameters



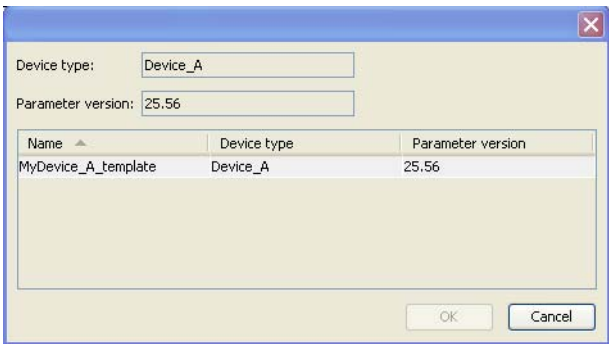
- 4 In the left pane, select parameter.
- 5 On the Value row, make the changes.  
When a parameter has been edited, the name of the node to which the parameter belongs changes to a blue color.  
(Click "Cancel" if you want to undo all parameters edited since your last save and return to the main window.)
- 6 Click "OK" to save the changes.

NOTE: When you save the parameters, they are automatically sent to the device if it is online.

7.4.7 APPLY TEMPLATE TO NUMBERS

If a template has been created for a device type, it can be used to set the parameter values for a range of devices, or a single device.

- 1 Select the "Numbers" tab. The Number view opens.
- 2 Select the Number(s) you wish to apply the template on.
- 3 In the Number menu, click "Apply template...". Alternatively, right-click the Number in the Number list and select "Apply template..." from the menu that opens.





- 4 Select a template from the Template list.
- 5 Click “OK”.

If the parameters in the database have been edited but not yet sent to the device it is indicated with “Not synched” or “Update queued”.

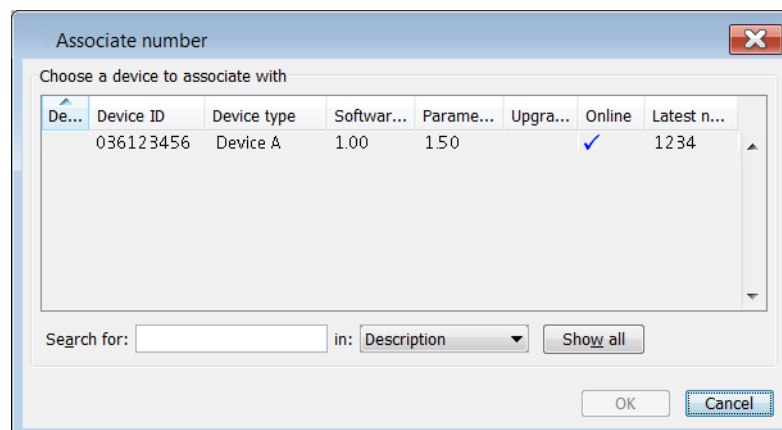
If the Number has not been associated with a device, it is now possible to do so. Connect a device and associate it with a Number in the database. The parameters will automatically be sent from the Device Manager to the device. See chapter [7.4.8 Associate a Number with a Device](#) .

## 7.4.8 ASSOCIATE A NUMBER WITH A DEVICE

Before being able to synchronize parameters between the Device Manager and a device, it is necessary to associate a Number with the device. It is possible to enter several Device IDs in advance and to associate them with a Number at a later moment.

See also [7.5.6 Assign a Number to a device](#) on page 85 and [7.5.5 Add a new Device](#) on page 84.

- 1 Select the “Numbers” tab.
- 2 In the Number menu, select “Associate with device...”. The Associate Number dialog opens.



- 3 Select the device you want to associate with in the list.
- 4 Click “OK”.

If the selected device is online, it will immediately be updated with the selected Number. If the selected device is not online, it will be updated the next time it is online.

It is possible to associate several Numbers with several devices simultaneously.

## 7.4.9 DELETE A NUMBER IN THE SITE DATABASE

- 1 Select the “Numbers” tab.
- 2 Select the Number you want to delete. The selected row is highlighted.
- 3 In the Number menu, select “Delete” or right-click and select “Delete”.
- 4 Click “Yes” in the Delete Number dialog.

The dialog window closes and the Number is deleted from the list.

#### 7.4.10 RENAME A NUMBER

- 1 Select the “Numbers” tab.
- 2 Select the Number you want to rename. The selected row is highlighted.
- 3 In the Number menu, select “Rename...” or right-click and select “Rename...”. The Rename number dialog opens.
- 4 In the “New prefix” field, enter a new prefix (if needed)
- 5 In the “New number” field, enter a new Number.
- 6 Click “OK”. The dialog window closes and the new Number appears in the list in the Numbers tab.

#### 7.4.11 COPY A NUMBER

When a Number is copied, the parameter settings and device type for that Number will be copied to a new specified Number.

- 1 Select the “Numbers” tab.
- 2 Select the Number you want to copy. The selected row is highlighted.
- 3 In the Number menu, select “Copy...”, or right-click and select “Copy...”. The Copy Number dialog opens.
- 4 In the “New prefix” field, enter a new prefix (if needed).
- 5 In the “New number” field, enter a new Number.
- 6 Click “OK”. The dialog window closes and the new Number appears in the list in the Numbers tab.

#### 7.4.12 IMPORT CONTACTS

NOTE: The number for the handset must be saved, see [7.4.2 Save a Number to Database](#) on page 77.

##### **Import Contacts From File**

A file containing contacts can be imported to Device Manager and synchronized with a device. This can for example be useful when you want to transfer contacts from legacy devices to newer devices.

NOTE: When importing the file, the entries (if any) in the device will be replaced by the entries in the file. Additionally, the import works only if the receiving device can store all entries included in the file.

- 1 In the Device Manager, select the Numbers tab.
- 2 Select a number.
- 3 In the Number menu, select Import contacts > From file. Alternatively, right-click the device and select Import contacts > From file from the menu that opens.
- 4 Find and select a file containing contacts ( .txt or .csv. Click “Open”.

The contacts in the imported file are synchronized with the handsets.

##### **Import Contacts From Number**

You can make a copy of a device’s contact list and paste it to another device’s contact list directly. This means that you do not need to save the contact list temporarily on for example your computer.

NOTE: The import works only if the receiving device can store the entire contact list of the device you are importing from. Additionally, the Company phonebook contacts included in the Call contact list are not transferred to the other handset using this feature. To upload the Company phonebook, see [7.6.8 Upload Company Phonebook](#) on page 91.

- 1 In Device Manager, select the Numbers tab.
- 2 Select a number.
- 3 In the Number menu, select "Import contacts" > "From number". Alternatively, right-click the Number in the Number list and select "Import contacts"> "From number" from the menu that opens.
- 4 Select a number.
- 5 Click "OK". The contacts are now imported to the handset.

### 7.4.13 EXPORT CONTACTS TO A FILE

Contacts can be exported from a handset to a csv-file. The contacts can then be transferred to another handset by importing the file, as described in chapter [7.4.12 Import Contacts](#) on page 82.

- 1 In the Numbers tab, select the handset whose contacts you want to export.
- 2 In the Number menu, select "Export contacts". Alternatively, right-click the handset and select "Export contacts" from the menu that appears.  
An Export contacts window opens.
- 3 Enter a descriptive file name and click "Save".

## 7.5 DEVICES

A device can be a handset, a charger, or a fixed device (such as IP-DECT base station) developed to work together with the Device Manager. See the manual for respective device.

All work with devices is performed from the Devices view.

- Devices can be added by connecting the device to the system, or use the "Add device" function.
- The information for a Number from one device can be transferred to a new device.
- Devices can be reset to factory settings.
- Devices can be updated with new software.

### 7.5.1 ADD DEVICES

NOTE: Before connecting a device to the Device Manager, make sure the connection is set up according to the instructions in the device's User Manual.

If a range of new devices are to be added, the easiest way is to:

- 1 Create a template with all common parameter settings. See [7.3.1 Create a Parameter Template](#) on page 73.
- 2 Add a range of Numbers and run the template. See [7.4.1 Create New Numbers](#) on page 77 and [7.4.7 Apply Template to Numbers](#).

- 3 Edit the parameters and change individual settings. See [7.4.6 Edit Parameters for a Number](#) on page 79.
- 4 Connect the devices and associate them with the Numbers in the database. See [7.4.8 Associate a Number with a Device](#) on page 81.

A single device can be added in the same way.

## 7.5.2 SYNCHRONIZE A DEVICE

NOTE: This feature is not applicable for fixed devices.

When parameters have been changed in a device, the device is synchronized with the Number saved in the database. During the synchronization, changed parameters in the device are uploaded to the Device Manager, and parameters changed in the Device Manager are sent to the device.

If a parameter has been changed in both the device and the Device Manager, the setting made in the Device Manager will take precedence.

- 1 When a device is connected to the system running the Device Manager, and if the Number is saved, and it has a parameter definition, the device is automatically synchronized.

While synchronizing, a progress bar and a text is shown in the Numbers view.

## 7.5.3 DELETE A DEVICE

- 1 Select the “Devices” tab.
- 2 Select the device you want to delete. The selected row is highlighted.
- 3 In the Devices menu, select “Delete” or right-click and select “Delete”.
- 4 Click “Yes” in the Delete Device dialog.

The dialog closes and the device is deleted from the list.

NOTE: A device that is online cannot be deleted.

## 7.5.4 REPLACE A DEVICE

NOTE: This feature is not applicable for fixed devices.

If a device shall be replaced with a new device, it is possible to transfer its associated Number including settings to the new device. The new device must be of the same device type as the old one.

- 1 If the device to be replaced is still working, make sure that it is synchronized.
- 2 Shut off the old device or make a factory reset.
- 3 Connect the new device to the Device Manager.
- 4 Associate the new device to the Number associated to the old device according to the instructions in [7.4.8 Associate a Number with a Device](#) on page 81. The Number will no longer be associated with the old device.

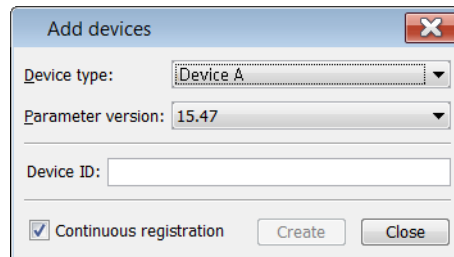
## 7.5.5 ADD A NEW DEVICE

NOTE: This feature is not applicable for fixed devices.

It is possible to enter several new Device IDs in advance into the Device Manager for later association.

In order to simplify input when handling many devices a bar code reader can be used. The bar code reader should send a carriage return after each item, but it is not necessary. If carriage return is not sent, it is necessary to click "Create" after each read item.

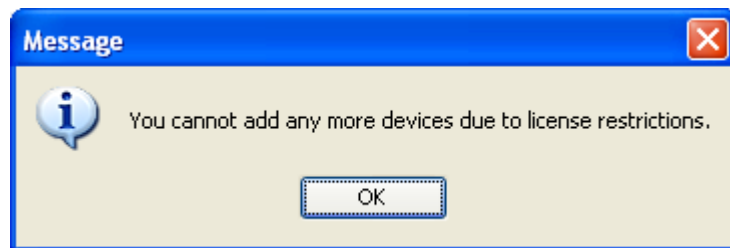
- 1 Select the "Devices" tab.
- 2 In the Device menu, select "Add device". The Create devices dialog opens.



- 3 Select Device type and Parameter Version.
- 4 Enter a Device ID for the device, manually or by using a bar code reader.
- 5 The "Continuous registration" box can be used to select whether the "Create devices" dialog shall close after clicking "Create" or if it shall still be open.
- 6 If the bar code reader does not send carriage return, click "Create".

NOTE: If you try to add more devices than allowed the following dialog window opens, see below.

Figure 23. License restrictions



- 7 Repeat 4 to 6 if more devices are to be created, otherwise click "Close".

### 7.5.6 ASSIGN A NUMBER TO A DEVICE

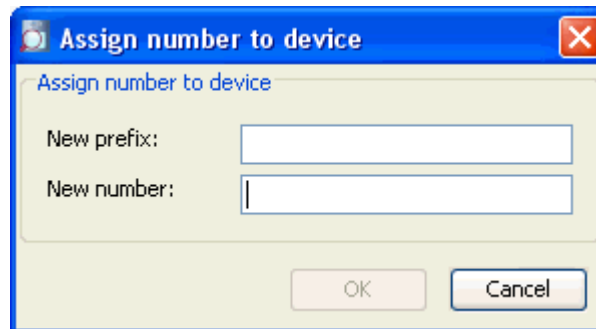
NOTE: This feature is not applicable for fixed devices.

It is possible to assign a Number to a device that has not yet been assigned a Number in the Device Manager. This feature can be used if parameters have been changed on the device prior to connection to the Device Manager.

NOTE: Assign shall not be done on a device that already has a Number.

- 1 Select the "Devices" tab.
- 2 Select the device you want to assign a Number for.

- 3 Select Device >Assign number in the menu. A new window opens.



- 4 Enter a new number in the New number field. New prefix is optional. Click "OK".  
The new Number appears in the list in the Numbers tab.

NOTE: Some devices need to be restarted for the new numbers to be shown.

### 7.5.7 ENTER/EDIT DESCRIPTION OF A DEVICE

It is possible to enter information of a device. For example, the description can be used to describe a location of a device.

- 1 Select the "Device" tab.
- 2 Select the device.
- 3 In the Device menu, select "Enter description". Alternatively, right-click the device and select "Enter description".
- 4 Enter an appropriate description and click "OK" to save the setting.

### 7.5.8 RESTART OF DEVICES

If supported by the devices, they can be restarted when they are online in the Device Manager. This feature, for example, can be used if you want to perform a controlled restart of several devices simultaneously.

- 1 Select the "Devices" tab.
- 2 Select the devices you want to restart.
- 3 Select Device > Restart device...
- 4 Select when the restart request should be sent to the devices.
  - Immediately — the request is sent to the devices directly
  - Later (server time zone) — the request is sent to the devices on a specified date and time.

NOTE: If the time zone at your current location differs from the time zone used by the module, select date and time that follows the time zone in the module.

For example:

The current date and time at your current location are 20 May 2014 12:00 (GMT) and the current date and time in the module are 20 May 2014 10:00 (GMT -02:00). The upgrade should be performed 20 May 2014 20:00 (GMT) meaning that "20 May 2014 18:00" (GMT -02:00) should be selected in this case.

- 5 Select when request should be activated, that is, when the devices should be restarted.
  - Immediately — the devices are restarted directly
  - When idle — the devices are restarted when the devices are in idle mode.
  - When idle in charger — the devices are restarted when they are put in a charger and are in idle mode.
- 6 Click "OK".

### 7.5.9 FACTORY RESET

NOTE: This feature is not applicable for fixed devices.

Factory reset means that the device parameters will be reset to factory settings. The Number in the database that is associated with the device will not be affected.

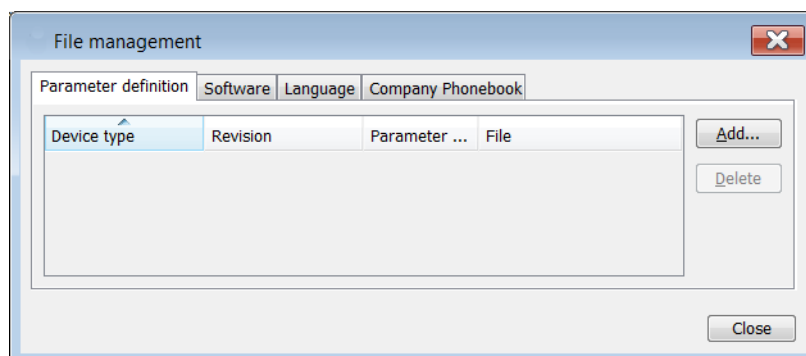
NOTE: The device must be online.

- 1 Select the "Devices" tab.
- 2 Select the device(s) to be reset.
- 3 Click "Factory reset" in the Device menu. Alternatively, right-click on the device and select "Factory reset".
- 4 A message saying "Do you want to reset the selected device(s) to factory defaults?" will appear.
- 5 Click "Yes".

## 7.6 FILE MANAGEMENT

This chapter covers file management for parameter definition files, software files, language files and company phonebook files.

Figure 24. The File Management Window



Import and export of templates and Numbers is described in [7.7 Import/Export Numbers and Templates](#) on page 94. Import of translation files is described in [18.1.4 Import Language File](#) on page 136.

The parameter definition file holds the definitions of all parameters for a specific version of a Number's parameter set. Updated software and new parameter definition files for devices and Numbers can be added to the Device Manager, see [7.6.3 Import Parameter Definition Files](#) on page 88 and [7.6.4 Import new Software for Devices](#) on page 89.

If there is a naming conflict when importing, a warning message is displayed.

### 7.6.1 DEFINITION FILE VERSION – PARAMETER VERSION

Both definition files and device software include parameters and are indicated by a version number.

NOTE: The version of the definition file matches the version of the device software.

If a device is updated with a new parameter version it does not always demand a new definition file. An old definition file can often be used but if new parameters have been added in the new parameter version, these parameters will not be editable. The release note will tell you if a new definition file is needed to match the new parameters.

#### Example

If a parameter version for a Number is 2.5, then a parameter definition file with a version between 2.0 and 2.5 is required.

### 7.6.2 IMPORT A PACKAGE FILE

A package file may include different types of files, such as software files, parameter definition files and/or template files. If the package does not include a certain file, it can be imported separately. See [7.6.3 Import Parameter Definition Files](#) on page 88, [7.6.4 Import new Software for Devices](#) on page 89, and/or [7.7.2 Import Templates](#) on page 94.

- 1 In the File menu, select "File management".
- 2 Select the Parameter definition tab or Software tab and click "Add".
- 3 Select the package file (.pkg) to be imported and click "Open".

The files included in the package are now imported. If needed, select the Parameter definition tab or Software tab to view the corresponding imported files (if any).

If template(s) has been imported, it can be viewed by clicking "Close" and then selecting the Template tab.

- 4 Click "Close".

### 7.6.3 IMPORT PARAMETER DEFINITION FILES

Updated parameter definition files are distributed by your supplier.

NOTE: Parameter definition files (.def) are mainly included in package files (.pkg) distributed by your supplier, see [7.6.2 Import a Package File](#).

- 1 In the File menu, click "File management". The File management window opens.
- 2 Click the Parameter definition tab.
- 3 Click "Add". The Import files window opens.



- 4 Select the definition files to be imported.  
Only files with a corresponding extension are shown, such as .def and .pkg.
- 5 Click “Open”.
- 6 Check that the newly imported definition files appear in the list.
- 7 Click “Close”.

If a definition file for a certain device type already exists in the database and an attempt is made to import a definition file with the same parameter version but with a lower revision, the file will not be imported. But if a new definition file with the same parameter version with a higher revision is imported, the old file will be replaced with the new imported file.

For each update of a parameter definition file, the revision is increased. An update does not necessarily affect the parameter version.

The following columns are displayed:

- Device type – the device model.
- Revision – the revision number of the definition file. Used to determine which definition file is the most recent.
- Parameter version – shows the version of the parameters in the definition file. Used to determine compatibility with device software.
- File – the name of the imported definition file.

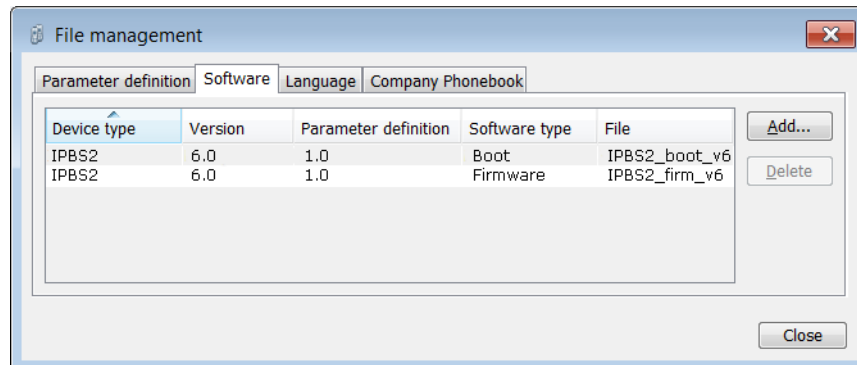
#### 7.6.4 IMPORT NEW SOFTWARE FOR DEVICES

Updated software files are distributed by your supplier.

NOTE: Software files (.bin) are mainly included in package files (.pkg) distributed by your supplier, see [7.6.2 Import a Package File](#) on page 88.

- 1 In the File menu, click “File management”. The File management window opens.

- 2 Click the “Software” tab.



The following columns are displayed:

- Device type – the device model.
- Version – the version number of the software file. Used to determine which software file is the most recent.
- Parameter version – shows the version of the parameters in the definition file. Used to determine compatibility with device software.
- Software type – shows if the software type is a boot software<sup>1</sup> or a firmware.
- File – the name of the imported software file.

- 3 Click “Add”. The Import files window opens.
- 4 Select the software files to be imported.  
Only files with a corresponding extension are shown, such as .bin and .pkg.
- 5 Click “Open”.
- 6 Check that the newly imported software files appear in the list.
- 7 Click “Close”.

### 7.6.5 IMPORT LANGUAGE FILES FOR DEVICES

For adding a new language to a device, a language file (.lng) distributed by your supplier must be imported to the Device Manager and then uploaded to the device.

- 1 In the File menu, click “File management”. The File management window opens.
- 2 Click the “Language” tab.
- 3 Click “Add”. The Import files dialog opens.
- 4 Select the language files to be imported.
- 5 Click “Open”.
- 6 Check that the newly imported language files appear in the list.
- 7 Click “Close”.

To apply the language for a device, see [7.6.7 Upload a Language to a Device](#) on page 91.

### 7.6.6 IMPORT COMPANY PHONEBOOK FILES

It is possible to import a phonebook file for later use.

---

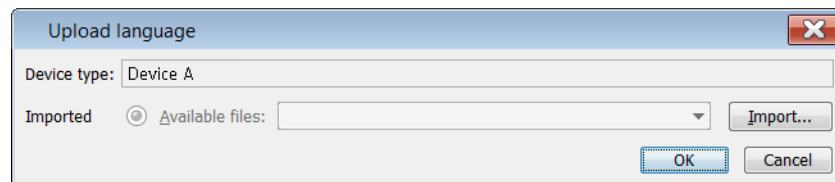
<sup>1</sup>.Currently, boot software is only applicable for fixed devices.

- 1 Select File > File management, in the menu. A new window opens.
- 2 Click the “Company Phonebook” tab.
- 3 Click “Add”. The Import files dialog opens.
- 4 Select the company phonebook files to be imported.
- 5 Click “Open”.
- 6 Check that the newly imported company phonebook files appear in the list.
- 7 Click “Close”.

### 7.6.7 UPLOAD A LANGUAGE TO A DEVICE

A language can be uploaded to portable devices that support Language Upload. Note that upload of languages is not available in demonstration mode.

- 1 Select the “Devices” tab.
- 2 Select the device(s) to upload a language to. It is possible to select several devices, but only devices of the same Device Type can be selected.
- 3 Select Device > Upload Language, in the menu. A new window opens.



- 4 Do one of the following:
  - If needed; import the language file (.lng) to be used by clicking “Import...”, locate the file, and click “OK”. In the Available files: drop-down list, select which language to upload.
  - Enter the URL where the language file is located.
- 5 Click “OK”. The language is uploaded to the device.

### 7.6.8 UPLOAD COMPANY PHONEBOOK

It is possible to upload a company phonebook to portable devices that support Company Phonebook Upload.

Upload of Company Phonebook is not available in Demonstration mode.

- 1 Select the “Devices” tab.
- 2 Select the handsets to upload a company phonebook to. It is possible to select several devices, but only devices of the same Device Type can be selected.
- 3 Select Device > Upload company phonebook, in the menu. A new window opens.



- 4 Select which company phonebook to upload.
- 5 Click “OK”. The company phonebook is uploaded to the device.

### 7.6.9 UPGRADE A DEVICE WITH NEW SOFTWARE

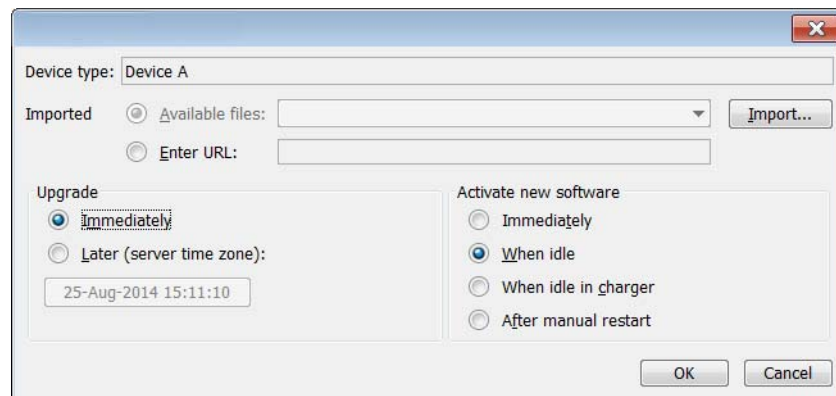
Devices can be upgraded with new software. Note that upgrade of device software is not available in demonstration mode.

- 1 Connect a device to the system.
- 2 Select the “Devices” tab.
- 3 Select device(s) to upgrade in the list. A selected row is highlighted. It is possible to select several devices, but only devices of the same Device Type can be selected.

**NOTE:** A software upgrade should be done on one device to start with. If successful, the remaining devices can be updated in one operation.

**Tip:** By using Ctrl and/or Shift several devices can be selected simultaneously.

- 4 Select Device > Upgrade software, in the menu. Alternatively, right-click and choose “Upgrade”, double-click the desired device, or click the “Upgrade” button in the toolbar. The Upgrade software window opens.



- 5 In the Upgrade software window the following fields are shown:
  - Device type – shows the model of your device.
  - Imported area:
    - Available files contains previously imported software files (see [7.6.4 Import new Software for Devices](#) on page 89); the latest used software file is selected by default.
    - Enter URL text field gives you a possibility to enter a path to a URL.
    - Import... is used to import new software.

**NOTE:** When upgrading devices with imported software, up to 10 devices can be upgraded simultaneously. When upgrading devices with software obtained via URL, up to 20 devices can be upgraded simultaneously.

- Upgrade area:
  - Immediately will start upgrade immediately
  - Later (server time zone) will start a scheduled upgrade on the specified date and time

**NOTE:** If the time zone at your current location differs from the time zone used by the module, select date and time that follows the time zone in the module.

For example:

The current date and time at your current location are 20 May 2014 12:00 (GMT) and the current date and time in the module are 20 May 2014 10:00

(GMT -02:00). The upgrade should be performed 20 May 2014 20:00 (GMT) meaning that "20 May 2014 18:00" (GMT -02:00) should be selected in this case.

- Activate new software area:
    - different selections depending on when the new software shall be activated (Immediately, When idle, When idle in charger or After manual restart).
- 6 If the software to be used for software upgrade is not available, it needs to be imported. If so, click "Import...". The Import software dialog opens. Locate the file and click "Open". The file is imported to the Device Manager.
- It is recommended to use Enter URL:<sup>1</sup> if the software is stored on an external server and should not be imported to the Device Manager.
- 7 Select software to be used in the upgrade in the Available files text box.
- 8 Click "OK". The Upgrade software window closes.
- The software will be downloaded to the device. For some device types, a progress bar in the Status column for the device shows the progress of the download.
- To cancel the upgrade, click "Cancel upgrade" in the Device menu. Alternatively, right-click the device in the device list and select "Cancel upgrade".
- The device will restart automatically after a successful download.

NOTE: A switched off device is upgraded when restarted.

#### 7.6.10 DELETE PARAMETER DEFINITION FILES

- 1 In the File menu, click "File management". The File management window opens.
- 2 Click the Parameter definition tab.
- 3 Select the definition files to be deleted.
- 4 Click "Delete".
- 5 In the Delete files dialog, click "Yes".
- 6 Click "Close".

#### 7.6.11 DELETE SOFTWARE

- 1 In the File menu, click "File management". The File management window opens.
- 2 Click the Software tab.
- 3 Select the software to be deleted.
- 4 Click "Delete".
- 5 In the Delete files dialog, click "Yes".
- 6 Click "Close".

#### 7.6.12 DELETE LANGUAGE FILE FOR DEVICES

- 1 In the File menu, click "File management". The File management window opens.
- 2 Click the Language tab.

---

<sup>1</sup>It is recommended to open a web browser and enter the URL (for example [http://myserver/kathy\\_v1.5.7.bin](http://myserver/kathy_v1.5.7.bin)). Make sure that the web browser asks you to save or open the correct file. Copy the URL and paste it in the Upgrade software dialog.

- 3 Select the language to be deleted.
- 4 Click "Delete".
- 5 In the Delete files dialog, click "Yes".
- 6 Click "Close".

### 7.6.13 DELETE COMPANY PHONEBOOK FILE

- 1 In the File menu, click "File management". The File management window opens.
- 2 Click the Company Phonebook tab.
- 3 Select the company phonebook to be deleted.
- 4 Click "Delete".
- 5 In the Delete files dialog, click "Yes".
- 6 Click "Close".

## 7.7 IMPORT/EXPORT NUMBERS AND TEMPLATES

This section describes import and export of Numbers and templates.

The purpose of importing and exporting Numbers and Templates is to be able to move Numbers and Templates to another site or to use at a later time. It is also possible to move between PDM Windows Version and Device Manager.

The parameter configuration in Numbers can be exported to a file. This file can be used by the supplier to pre-program devices before delivery to the customer.

If there is a naming conflict when importing a template, the new template is imported and the old template is deleted. If there is a Number conflict when importing Numbers, an error message is displayed.

**NOTE:** The device settings are unexchangeable between device types. For example, a number or template exported from device type Device A can only be used on that device type (i.e. Device A), and not on a different device type (e.g. Device B), and vice versa.

### 7.7.1 IMPORT NUMBERS

- 1 In the File menu, click "Import > Numbers...". An Import numbers window opens.
- 2 Select the Number files (\*.xcp) to be imported.
- 3 Click "Open".
- 4 The number(s) will be imported.

### 7.7.2 IMPORT TEMPLATES

A template may be imported from another system. Updated Template files may be distributed by your supplier.

- 1 In the File menu, click "Import > Templates...". An Import templates window opens.
- 2 Select the Template files (\*.tpl) to be imported.
- 3 Click "Open".

- 4 The template(s) will be imported.

### 7.7.3 EXPORT NUMBERS TO A FILE

It is possible to configure Numbers for a site and export the settings to a file. One or several Numbers can be selected.

The exported file can then be used when producing new devices for the customer.

- 1 Select the “Numbers” tab. The Numbers view opens.
- 2 Select the Number(s) to be exported.
- 3 In the Number menu, click “Export”.  
The “Export Numbers” window opens. By default the file will be saved in the My documents folder with the name EliseSite.xcp. You can select another name and folder.
- 4 Click “Save”.

### 7.7.4 EXPORT TEMPLATES TO A FILE

It is possible to export templates to a file. One or several templates can be selected.

- 1 Select the “Templates” tab. The Templates view opens.
- 2 Select the template(s) to be exported.
- 3 In the Template menu, click “Export”.  
The Export templates window opens. By default the file will be saved in the My documents folder with the name Templates.tpl. You can select another name and folder.
- 4 Click “Save”.

## 7.8 OTHER SETTINGS

### 7.8.1 AUTOMATICALLY ENABLE NEW DEVICES SETTINGS

By default, when a new device logs in, it is automatically enabled and saved in the CPDM3's database.

**NOTE:** The CPDM3 license determines the number of devices that can be enabled simultaneously in the Device Manager. If logging in more devices than allowed, they will be disabled in the Device Manager. The devices must be enabled in order to configure them.

When a single CPDM3 is used, the Automatically enable new devices function should normally be enabled. But if Device Management is distributed over multiple CPDM3s in a system, the function shall be disabled; if the function is enabled, devices will be enabled and saved on all CPDM3s running device management. This will cause synchronization problems and the logged in devices will consume license positions on each CPDM3. See also [2.6 Multiple CPDM3](#) on page 16.

To disable automatic enabling of new devices, do as follows:

- 1 Select Options > Preferences, in the menu. A new window opens.
- 2 Uncheck the “Automatically enable new devices” check box.

- 3 Click "OK".

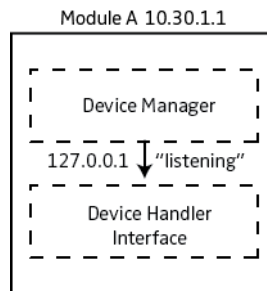


## 8. DEVICE

### 8.1 DEVICE MANAGEMENT SETUP

This setting determines which Device Handler interface the Device Manager should listening to. When a device logs in to the interface, the device appears in the Device Manager GUI.

#### 8.1.1 EXAMPLE 1: ALL DEVICES LOG IN A SINGLE CPDM3



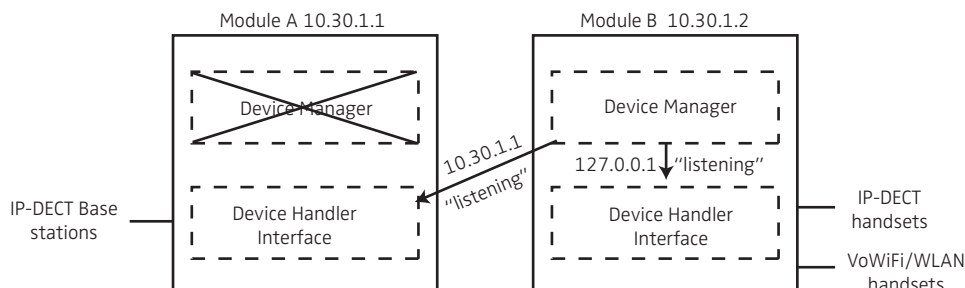
The CPDM3 has a Device Manager enabled. All devices that log in to the local Device Handler interface should appear in the CPDM3's local Device Manager.

In this case the CPDM3 points at its local Device Handler interface. The Device Manager is listening to the interface for logged in devices, that will appear in the Device Manager GUI.

##### Configuration in Example 1

- 1 From the Start page, click **Configuration**.
- 2 Select **Other Settings > Advanced Configuration**.
- 3 Click **Device Management**.
- 4 In the CPDM3, enter the following:
  - For IP-DECT handsets, enter **127.0.0.1/DECT**
  - For IP-DECT Base Stations, enter **127.0.0.1/IPDECT**
  - For WLAN handsets, enter **127.0.0.1/WLAN**
- 5 Click **Activate**.

#### 8.1.2 EXAMPLE 2: DEVICES LOG IN TO DIFFERENT CPDM3



The Device Manager in CPDM3 A is disabled, but enabled in CPDM3 B. The devices that logs in to CPDM3 A and the devices that log in to CPDM3 B should appear in the Device Manager of CPDM3 B. In this case, the CPDM3 B should point at its local Device Handler and also point at the Device Handler of CPDM3 A.

The Device Manager is listening to the interfaces for logged in devices, that will appear in the Device Manager GUI.

#### Configuration in Example 2

- 1 From the Start page, click **Configuration**.
- 2 Select **Other Settings > Advanced Configuration**.
- 3 Click **Device Management**.
- 4 In the CPDM3 B, enter the following:
  - For IP-DECT handsets, enter **127.0.0.1/DECT**
  - For IP-DECT Base Stations, enter **10.30.1.1/IPDECT**
  - For WLAN handsets, enter **127.0.0.1/WLAN**

NOTE: The Device Management fields in CPDM3 A should be left empty.

- 5 Click **Activate**.

## 8.2 ALLOW IP-DECT HANDSETS/CHARGERS TO LOG IN TO DEVICE MANAGER

If your system having multiple Device Managers, you can configure which Device Manager the handsets and chargers shall log on to. For example, this gives the possibility to only allow handsets to log in to one Device Manager and chargers to log in to another Device Manager.

- 1 Click "Configuration" on the start page.
- 2 Select Other Settings > Advanced Configuration on the Configuration page.
- 3 Under DECT Interface, click "Device Handling" in the menu on the Advanced Configuration page.
- 4 Click the device type to change settings for.
- 5 In the Allow devices to log in? drop-down list, select whether if the device type shall be able to log in or not.
- 6 Click "Activate".

## 8.3 DEVICE RELOGIN TIME

All devices send keep alive messages to CPDM3 to remain logged in. How often the devices should send the messages can be configured. E.g. if the relogin time is set to 10 minutes, the devices should send a keep alive message every tenth minute.

If a device does not send a keep alive message before the relogin time expires, the device will be considered as logged out.

NOTE: A short device relogin time implies a higher security but it also loads the system.

### 8.3.1 RELOGIN TIME FOR CHARGERS

- 1 Click "Configuration" on the Start page.
- 2 Select Other Settings > Advanced Configuration on the Configuration page.
- 3 Under DECT Interface, click "Device Handling" on the Advanced Configuration page.
- 4 Click the device type (i.e. desktop charger or charging rack) to change settings for.
- 5 Enter how often (in minutes) the device should send a keep alive message in the Device relogin time field. Minimum legal time is 10 minutes.
- 6 Click "Activate".

### 8.3.2 DELAY TIME FOR CHARGING RACKS

To move a charging rack without being logged out, it is also possible to set a delay time. If the charging rack has not logged in again within the Device relogin time, the delay timer starts. If the device does not log in within that delay time, a status report is sent to the Fault Log.

- 1 Click "Configuration" on the Start page.
- 2 Select Other Settings > Advanced Configuration on the Configuration page.
- 3 Under DECT Interface, click "Device Handling" on the Advanced Configuration page.
- 4 Click "Charging Racks".
- 5 Enter the delay time (in minutes) in Status Log Delay Time field.
- 6 Click "Activate".

### 8.3.3 RELOGIN TIME FOR DECT/IP-DECT HANDSETS PUT IN CHARGER

- 1 Click "Configuration" on the start page.
- 2 Select Other Settings > Advanced Configuration on the Configuration page.
- 3 Under DECT Interface, click "Device Handling" in the menu on the Advanced Configuration page.
- 4 Click "DECT Handsets".
- 5 Enter how often (in minutes) the device should send a keep alive message in the Device relogin time for devices put in charger field. Minimum legal time is 10 minutes.
- 6 Click "Activate".

### 8.3.4 RELOGIN TIME FOR FIXED IP-DECT DEVICES

- 1 Click "Configuration" on the start page.
- 2 Select Other Settings > Advanced Configuration on the Configuration page.
- 3 Under IP-DECT Interface, click "Device Handling" in the menu on the Advanced Configuration page.
- 4 Enter how often (in minutes) the device should send a keep alive message in the Device relogin time field. Legal values: 10 - 1440.
- 5 Click "Activate".

### 8.3.5 RELOGIN TIME FOR VOWIFI HANDSETS

- 1 Click "Configuration" on the Start page.
- 2 Select Other Settings > Advanced Configuration in the menu in the on the Configuration page.
- 3 Click "WLAN System" under WLAN Interface on the Advanced Configuration page.
- 4 Enter how often (in minutes) the device should send a keep alive message in the Device relogin time field. Legal values: 10 - 1440.
- 5 Click "Activate".

## 8.4 SERVICE DISCOVERY

### 8.4.1 SERVICE DISCOVERY DOMAIN ID

Service Discovery allows automatic detection of CPDM3s, devices and services on a network without prior configuration. CPDM3s, services and devices that shall belong to a certain CPDM3 must be set to the same domain ID.

- 1 Click "Configuration" on the start page.
- 2 Select Other Settings > Advanced Configuration on the Configuration page.
- 3 Under Other, click "Service Discovery" in the menu on the Advanced Configuration page.
- 4 In the Domain ID field, enter the Service Discovery Domain ID.
- 5 Click "Activate".

The screenshot shows a 'Module settings' window. It contains a 'Domain ID' label, a text input field with a question mark icon to its left, and a 'Previous' button to its right. Below the input field is a 'Factory' button. At the bottom left is an 'Activate' button, and at the bottom right is a 'Cancel' button.

### 8.4.2 ENABLE/DISABLE SERVICE DISCOVERY FOR FIXED IP-DECT DEVICES

This setting determines if the devices can log in to the Device Manager using Service Discovery. Service Discovery allows automatic detection of devices and services on a network without prior configuration. CPDM3 and the devices, that shall belong to that CPDM3 have to be set to the same Domain ID.

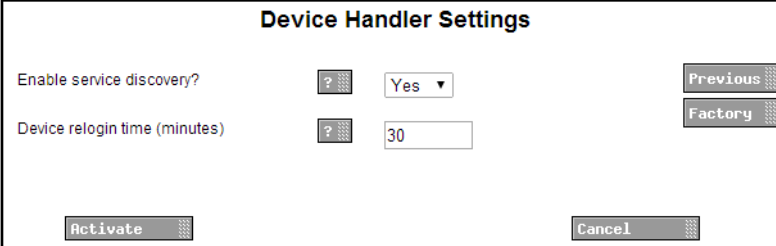
If your system having multiple Device Managers, it is possible to set which Device Manager the IP-DECT base station (IPBS) should logon to. This can be used to logon the IPBS to one Device Manager while another Device Manager for example can be used for handsets.

The IPBS can use either the CPDM3's IP address or the Service Discovery Domain ID to logon to the wanted Device Manager. This chapter is only applicable when Service Discovery Domain ID is to be used.

For example:

In the IPBS, the Service Discovery is enabled with Domain ID set to "Module\_A", and the Domain ID in your Unite module is also set to "Module\_B" (see [8.4 Service Discovery](#) on page 100). In this case, enable the service discovery in the CPDM3 in order to logon the IPBS to the Device Manager that matches the Domain ID.

- 1 Click "Configuration" on the start page.
- 2 Select Other Settings > Advanced Configuration on the Configuration page.
- 3 Under IP-DECT Interface, click "Device Handling" in the menu on the Advanced Configuration page



- 4 In the Enable service discovery? drop-down list, select "Yes" if the IP-DECT base station uses service discovery to find the Device Manager.
- 5 Click "Activate".

#### 8.4.3 ENABLE/DISABLE SERVICE DISCOVERY FOR VOWIFI HANDSETS

This setting determines if the devices can log in to the Device Manager using Service Discovery. Service Discovery allows automatic detection of devices and services on a network without prior configuration. CPDM3 and the devices, that shall belong to that CPDM3 have to be set to the same Domain ID.

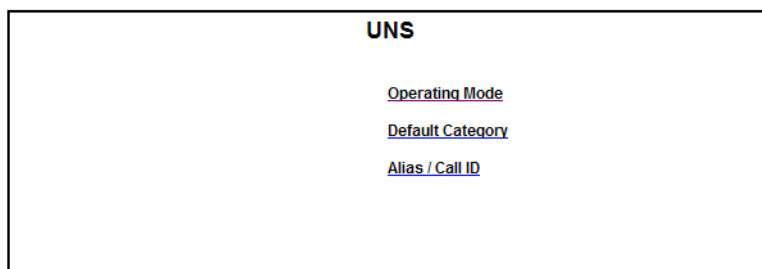
- 1 Click "Configuration" on the start page.
- 2 Select Other Settings > Advanced Configuration in the menu in the on the Configuration page.
- 3 Click "WLAN System" under WLAN Interface on the Advanced Configuration page.
- 4 In the Enable service discovery? drop-down list, select "Yes" if the handsets use service discovery to find the Device Manager.
- 5 Click "Activate".

## 9. ADDITIONAL SYSTEM SETTINGS

### 9.1 UNITE NAME SERVER (UNS)

The UNS in the CPDM3 is used to resolve addresses into complete destinations. The module can be configured to send all requests to the local UNS (stand-alone mode) or to forward all requests to a centralized UNS (forwarding mode). In forwarding mode, the local UNS will only be used if the centralized UNS cannot resolve the address.

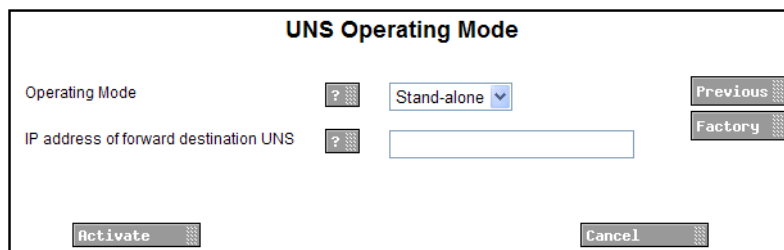
- 1 Click “Configuration” on the start page.
- 2 Select Other Settings > Advanced Configuration on the Configuration page.
- 3 Under Other, click “UNS” in the menu on the Advanced Configuration page.



#### 9.1.1 UNS OPERATING MODE

Operating mode is changed in systems with a Unite CM only.

- 1 To set Operating mode, click “Operating mode”.



- 2 In a system with a Unite CM, set operating mode to Forwarding and enter the Unite CM IP address.
- 3 Click “Activate”.

#### 9.1.2 DEFAULT CATEGORY

The UNS Default Category is used to decide where messages from the CPDM3 should be sent. The messaging handler is default set to localhost (127.0.0.1) which is the internal message group handler in the module. This can be changed if you want to use a messaging handler in another module. This parameter is changed for example if your system is connected to another CPDM3.

- 1 Click “Default Category”.

- 2 Enter values for Messaging handler IP address and Messaging handler service name. Default service name is DGH, which also is required if Messaging Groups should be used in theCPDM3
- 3 Click “Activate”.

### 9.1.3 ALIAS / CALL ID

Alias can be used when there are numbers that do not belong to the default category.

- 1 To set Alias, click “Alias / Call ID”.

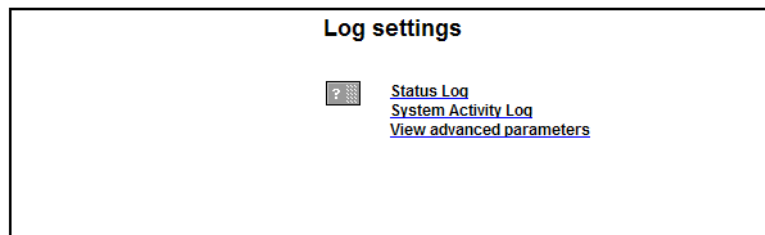
- 2 Click one of the links.

- 3 Enter settings for UNS Alias / Call ID.  
In this example, a message that is addressed to “MyAlias” will be sent to the handset with extension 1234 in the DECT system that is connected to the CPDM3 with the address 192.168.0.1.
- 4 Click “Activate”.

## 9.2 LOGGING

Status information can be stored locally, but can also be sent to a central log. The System Activity Log can store “activities” such as messages, alarms, faults etc. Activity logging is useful for troubleshooting. Default the Status- and System Activity logs are stored locally but they can also be sent to another CPDM3.

- 1 Click “Configuration” on the start page.
- 2 Select Other Settings > Advanced Configuration on the Configuration page.
- 3 Under Other, click “Logging” in the menu on the Advanced Configuration page.



- 4 Click “Status Log”, “System Activity Log” or “View Advanced parameters”.
- 5 In the selected log page, enter settings. Click “Activate”.

## 9.3 TIME SETTINGS

It is possible to select where to fetch the time from, such as a web browser or a time server.

- 1 Click “Configuration” on the start page.
- 2 Select Other Settings > Advanced Configuration on the Configuration page.
- 3 Under Time, click “Settings” in the menu on the Advanced Configuration page.



**Time settings**

Time source ? Web browser

Time server address (\*) ? 0.0.0.0

Fault log (\*) ? Yes

Time zone ? ((GMT+01:00) Amsterdam, Berlin, Rome, Stockholm)

Auto DST adjust ? Yes

Date format ? YYYY MM DD

Date separator ? -

Time Format ? HH:MM:SS

Time push time (HH:MM) ? 00:00

\* = Only valid when 'Time server' is selected

Previous

Factory

Activate

Cancel

4 The following parameters can be set (some of these parameters can also be set in the setup wizard):

- Time source – Where to fetch the time, web browser or NTP server
- Time server address – IP address to NTP server
- Fault log – Create fault log for time server faults
- Time zone – Current time zone
- Auto DST adjust – Automatic adjustment for daylight saving time
- Date format – Which date format to use
- Date separator – Which character to use to separate the date fields
- Time Format – Which time format to use
- Time push time – When to update all interfaces within the module

5 Click “Activate”.

For additional information, see also the Installation Guide for your product.

### 9.3.1 MANUAL TIME SETTING (IF WEB BROWSER IS TIME SOURCE)

If Web browser has been selected as time source, the time must be set manually. Otherwise this setting shall not be done. The setting can also be done in the setup wizard.

1 Under Time, click “Set time”

Set Date and Time

Current date is: 2010-05-06  
Current time is: 12:15:09 [\(reload\)](#)

Please Note! The time cannot be set from here unless the "Time source" parameter in Time Settings is set to "Web Browser".

Local PC Date

2010-05-06

?

Local PC Time

12:15:22

?

Submit Time

Close

- 2

Enter date and time.
- 3

Click "Submit time".
- Date and time can also be set in the setup wizard.

9.4 NETWORK SETTINGS

- 1

Click "Configuration" on the start page.
- 2

Select Other Settings > Advanced Configuration on the Configuration page.
- 1

Under Common, click "Network" in the menu on the Advanced Configuration page.

Network

Require network connection

?

Yes

Previous

DHCP

?

Enabled

Factory

IP address

?

172.20.13.5

Default gateway

?

172.20.8.1

Subnet mask

?

255.255.248.0

Host name

?

Modermodemet

Domain name

?

ascom-ws.com

Primary DNS

?

172.20.8.145

Secondary DNS

?

0.0.0.0

WINS Server

?

172.20.8.145

Activate

Cancel

- 2 The following parameters can be set (some of these parameters can also be set in the setup wizard):
  - Require network connection – Controls if the module needs a connection to the network to start up. This can be useful if you want configure the module before connecting it to a network.
  - DHCP – Controls whether static or dynamic IP address shall be assigned to this hardware. If DHCP is enabled, only the host name below is applicable.
  - IP address – Sets the IP address for the module
  - Default gateway – Sets the IP address to a Gateway on the LAN
  - Subnet mask – sets the network mask that is to be used. If this parameter is set to 0.0.0.0 it means that the Gateway never will be used.
  - Host name
  - Domain name – Sets the desired domain name for the module
  - DNS Server – Sets the IP address to a DNS if one exists. If no DNS Server is present on the network, set this parameter to 0.0.0.0.
  - WINS Server – sets the IP address to a Primary WINS Server if one exists.
  - If no WINS Server is present on the network, set this parameter to 0.0.0.0.

For additional information, see also the Installation Guide for your product.

- 3 Click “Activate”.

## 9.5 SETTING THE LICENSE NUMBER

The license number is normally set in the setup wizard but it can also be set on the Advanced Configuration page.

- 1 Click “Configuration” on the start page.
- 2 Select Other Settings > Advanced Configuration on the Configuration page.
- 3 Under Common, click “License” in the menu on the Advanced Configuration page
- 4 Enter the license number and click “Activate”.

### 9.5.1 REBOOT

The module can be rebooted on the Advanced Configuration page.

- 1 Click “Configuration” on the start page.
- 2 Select Other Settings > Advanced Configuration on the Configuration page.
- 3 Under Common, click “Reboot” in the menu on the Advanced Configuration page
- 4 Click the “Reboot” button.

NOTE: If the Reboot page is reloaded, this will trigger another reboot.

## 10. REMOTE MANAGEMENT

A remote connection to a customer site can be established through the CPDM3. This makes it possible to configure and maintain sites, independent of distance.

To be able to connect remotely, the remote management server in the module has to be configured. The help text buttons in the GUI will give more information about each parameter settings.

- 1 Click “Configuration” on the start page.
- 2 Select Other Settings > Advanced Configuration on the Configuration page.
- 3 Click “Remote Management” in the menu on the Advanced Configuration page

The screenshot shows the 'Remote Management Server' configuration page. It contains three rows of settings, each with a help icon (question mark in a square) and an 'Edit' button. The first row is 'Remote connection' with an 'Edit' button. The second row is 'Open ports' with an 'Edit' button. The third row is 'Serial port channel' with a 'NOT USED' button. Below the 'Serial port channel' row, there are three more 'NOT USED' buttons stacked vertically.

### Remote connection

- 1 Click “Edit” for Remote Connection, to set up the connection parameters.

The screenshot shows the 'Connection parameters' configuration page. It contains five rows of settings, each with a help icon (question mark in a square) and a text input field. The first row is 'Password' with a text input field containing 'password'. The second row is 'Require user identification' with a dropdown menu set to 'No'. The third row is 'Serial port' with a dropdown menu set to '-- None --'. The fourth row is 'PPP server address' with a text input field containing '192.168.0.1'. The fifth row is 'PPP client address' with a text input field containing '192.168.0.2'. At the bottom of the page, there are two buttons: 'Activate' and 'Cancel'. On the right side of the page, there are two buttons: 'Previous' and 'Factory'.

- 2 Set up the connection parameters.
- 3 Click “Activate”.

### Open ports

- 1 Click “Edit” for Open Ports to open any additional ports that are needed for configuration tools. This is a secured setting and before it can be activated it must manually be confirmed by pressing the mode button on the module.

Port

To be able to change this setting the Confirmation Mode on the module must be activated

Open ports

10101

Previous

Factory

Activate

Cancel

For TCP and RS232, port 10101 has to be open.

- 2 Set up the port parameters.
- 3 Click “Activate”.  
You will be prompt to confirm the change by pressing the mode button.
- 4 Press the mode button on the module.
- 5 Click “Activate” to save the changes.
- 6 Click the mode button to return to normal mode immediately or wait 10 minutes for the module to return automatically. Any secured setting can be activated within the 10 minutes period.

The module needs to be restarted for the changes to take effect.

**Serial port channel**

- 1 Click one of the “NOT USED” links for Serial port channel to set up a new channel.

Serial port channel

Name

IP address

Remote Serial port

Baud rate

Parity

Notes

Previous

Factory

Activate

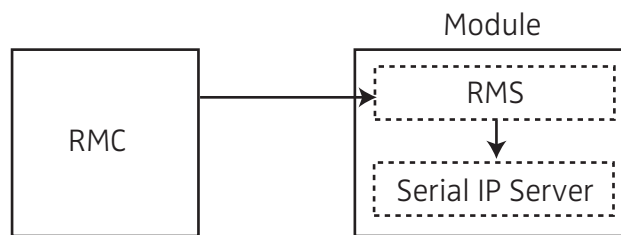
Cancel

One serial port channel for each tool, for example WinBK for System 900 configuration, has to be set up. Web based configuration tools do not require serial port channels.

- 2 Set up the channel and click “Activate”.

10.1 SERIAL IP SERVER PROTOCOL

This parameter determines the version of Serial IP Server protocol to be used to establish a serial port channel from the RMC to the Serial IP Server. The Serial IP Server is a service that communicates with the CPDM3's COM-ports.



RMS = Remote Management Server

RMC = Remote Management Client

- 1 Click "Configuration" on the start page.
- 2 Select Other > Advanced Configuration in the menu on the Configuration page.
- 3 Select "Remote Management" in the menu on the Advanced Configuration page.

The screenshot shows the 'Serial-IP Server' configuration window. At the top, the title 'Serial-IP Server' is centered. Below the title, on the left, is the label 'Protocol Version'. To its right is a drop-down menu currently showing '2.0' with a question mark icon to its left. Further right are two buttons: 'Previous' and 'Factory'. At the bottom left is an 'Activate' button, and at the bottom right is a 'Cancel' button.

- 4 In the Protocol Version drop-down list, select one of the following:
  - Select protocol version 1.0 if a legacy RMC is connected, or if a RMC is not connected through a VPN tunnel.
  - Select protocol version 2.0 if a RMC is connected through a VPN tunnel. In this case RMC version 1.32 or later must be used.

## 11. ABSENCE HANDLING

Absence handling in the CPDM3 is handled differently for DECT and VoWiFi.

### 11.1 ABSENCE HANDLING IN DECT

The module keeps track of handsets that have reported absence status. When a message is sent to an absent handset, the sending device can receive information from the CPDM3 that the handset is absent.

#### 11.1.1 ABSENCE LIST

The absence list indicates which handsets that have reported absence status.

- 1 Click "Configuration" on the start page.
- 2 Select Other Settings > Advanced Configuration on the Configuration page.
- 3 Under DECT Interface, click "View Absence List" in the menu on the Advanced Configuration page

The handset identity and absence type, for example "Manual absent" or "In storage rack", are reported in the list.

A handset can be removed manually from the absent list by clicking on the corresponding "Remove" link.

#### 11.1.2 CLEAR ABSENCE LIST

The absence list in the module can be cleared. This has to be done, for example, when the module is reinstalled in a system since the absence list then will be out of date. This should only be used as a last resort if there is a permanent mismatch in the system.

- 1 Click "Configuration" on the start page.
- 2 Select Other Settings > Advanced Configuration on the Configuration page.
- 3 Under DECT Interface, click "Clear Absence List" in the menu on the Advanced Configuration page.
- 4 Click "Clear".

NOTE: When the absence list is cleared, the module will consider handsets that currently are placed in a charger, or manually set to absent, as present.

### 11.2 ABSENCE HANDLING IN THE VOWIFI SYSTEM

These features requires that your CPDM3 has a valid license.

See also [4.6.6 WLAN Handsets](#) on page 43.

#### 11.2.1 SORT ON HANDSET STATUS

A list with all handsets can be created.

- 1 Click "Configuration" on the start page.

- 2 Select WLAN Handsets > List All on the Configuration page.
- 3 Click the name of the column (in this case, "Status") to sort the list on handset status.

### 11.2.2 SEARCH ON HANDSET STATUS

It is possible to search for handsets with selected status.

- 1 Click "Configuration" on the start page.
- 2 Select WLAN Handsets > Search in the menu on the Configuration page.
- 3 Enter the optional search parameters Address/Number, IP Address, Hardware ID and Status. To view absent portables, select "All absent" or "Manual Absent".



## 12. BASE STATION CONVERSION

The base station IDs that are received together with personal alarms can be converted to another ID before it is sent to the system.

### 12.1 BACKGROUND

In some systems, the base station IDs might alter when the Cordless Telephone System is upgraded. In the alarm handling the base station IDs are used for location determination of an alarming handset. Normally the ID is converted to a text string that describes the location. The ID can also be used in trigger conditions, for example to decide which guards that should be informed about an alarm. To avoid having to update the base station IDs in many different places in the configuration of the alarm handling, the CPDM3 can convert the base station IDs before it is sent to the alarm system.

This can be convenient regardless of how the Cordless Telephone System handles an upgrade as the base station IDs normally consists of about ten characters. The base station conversion can then be used to shorten the IDs before it is sent to the alarm system. It is also possible to convert the ID to a descriptive text.

### 12.2 CONFIGURATION

The Base Station Conversion can be reached from the menu on the Advanced Configuration page. Requires “admin” or “sysadmin” password, refer to [3.2 Authentication Levels and Default Password](#) on page 20.

- 1 Click “Configuration” on the start page.
- 2 Select Other Settings > Advanced Configuration on the Configuration page.
- 3 Under DECT Interface, click “Base Station Conversion” in the menu on the Advanced Configuration page
- 4 Enter the file name or click “Browse” and select the file.
- 5 Click “Import file”.

The conversion table is imported as a CSV file, with the base station ID in the first column and the new ID in the second. The new ID is a string of maximum 50 characters. IDs that are not included in the table will be sent to the alarm system without any conversion.

## 13. OPEN ACCESS PROTOCOL (OAP)

This feature requires a specific license, see [1.2 Products for CPDM3](#) on page 7. This function makes it possible for customer applications to communicate with other connected systems, for example the Cordless Telephone System. The protocol that is used for communication is called Open Access Protocol (OAP).

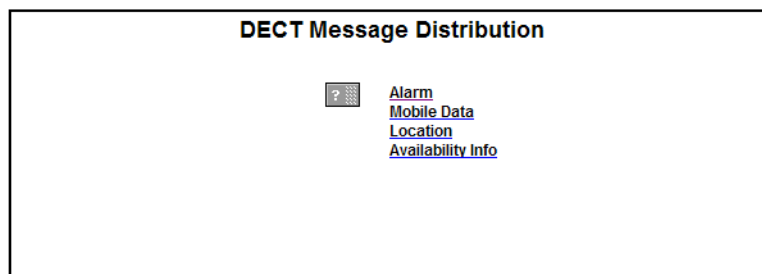
Refer to the Function Description for Open Access Protocol (OAP) for more information about the protocol and when it can be used.

### 13.1 CONFIGURATION

The Message Distribution lists for the different interfaces have to be configured to send the information to the OAP Server, in order to give the client access to the information. The address of the OAP Server is xxx.xxx.xxx.xxx/OAP.

#### Configuration Example

- 1 The DECT or WLAN Interface should be configured to send User Data to the OAP Server. Click “Configuration” on the start page.
- 2 Select Other Settings > Advanced Configuration in the menu on the Configuration page.
- 3 Under respectively interface (DECT and WLAN), click “Message Distribution” in the menu on the Advanced Configuration page.
- 4 Select “Alarm”.

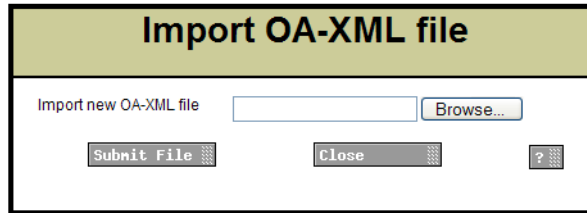


- 5 Enter the address xxx.xxx.xxx.xxx/OAP in one of the address fields.
- 6 Click “Activate”.

### 13.2 IMPORTING A NEW OA-XML FILE

It is possible to import new services, and update existing services, by importing a new OA-XML file to the module. The OA-XML description and OA-XML schema documents will also be updated when a new file is imported.

- 1 Select "OA-XML" in the menu on the System Setup page. The Import OA-XML file opens.



The screenshot shows a dialog box titled "Import OA-XML file" with a light green header. Below the header, the text "Import new OA-XML file" is followed by a text input field and a "Browse..." button. At the bottom of the dialog, there are three buttons: "Submit File", "Close", and a help icon (a question mark inside a square).

- 2 Click "Browse" and locate the file.
- 3 Click "Submit File".

New services are added to the OAP list on the System Information page. The Protocol version in the list shows the currently installed OA-XML version.

**NOTE:** The new service will only be shown in System Information if there is a valid license for the service.

## 14. DECT INTERFACE

It is recommended to configure the carrier system interfaces from the Wizard, but it can also be done from the Advanced Configuration page.

This chapter describes configuration from the Advanced Configuration page, for some carrier systems. It does not include all supported carrier systems.

The CPDM3 can be connected to one carrier system (see [14.1 DECT Phone Systems](#)) or to several carrier systems simultaneously, see [14.2 Mixed DECT Systems](#) on page 117.

### 14.1 DECT PHONE SYSTEMS

#### 14.1.1 MIVOICE MX-ONE

CPDM3 can communicate with the MX-ONE over a LAN. For configuration of the MX-ONE, See the MX-ONE installation documentation.

#### 14.1.2 IP-DECT

Figure 25. Communication with the IP-DECT system is done over a LAN



For configuration of the IP-DECT system refer to Installation and Operation Manual for your IP-DECT system.

It is possible to set an address to a secondary IP-DECT master which is used as a redundancy backup. The secondary IP Address is used if the connection to the primary IP Address is lost. If the secondary IP Address is lost, the module will try to use the primary IP Address.

- 1 Click "Configuration" on the start page.
- 2 Select Other Settings > Advanced Configuration in the menu on the Configuration page.
- 3 Select "IP-DECT" in the menu on the Advanced Configuration page.
- 4 Continue in A) IP-DECT system with a Single Master or B) IP-DECT system with Multiple Masters below.
- 5 Enter the IP address to the DECT system
- 6 Enter a secondary IP address if two DECT system are used for redundancy purposes, enter the IP address to the secondary DECT system in the Secondary DECT IP Address text field.

##### A) IP-DECT system with a Single Master

- 1 Enter the IP address to the DECT system
- 2 Enter a secondary IP address if two DECT system are used for redundancy purposes, enter the IP address to the secondary DECT system in the Secondary DECT IP Address text field.

### B) IP-DECT system with Multiple Masters

Multiple DECT interfaces are used for connections to an IP-DECT multi-master system with a common PBX number plan.

NOTE: All numbers in the system must be unique, i.e. a number for a user in one system cannot be the same as a number for a user in another system.

- 1 If not already set via the wizard, click the Multiple Locations link, select "Yes" and reboot the module.
- 2 Select IP-DECT in the menu and click a "NOT USED" link.
- 3 Enter a name for the DECT interface.
- 4 Enter the Master IP address.
- 5 Enter the Standby Master IP address if a secondary Master is used as a backup.
- 6 Configure desired number of interfaces. Up to 20 DECT interfaces can be set up. The relative order when entering the IP-DECT Masters makes no difference.
- 7 If data shall be encrypted for multiple IP-DECT locations, click the Encrypt data link and select "Yes".

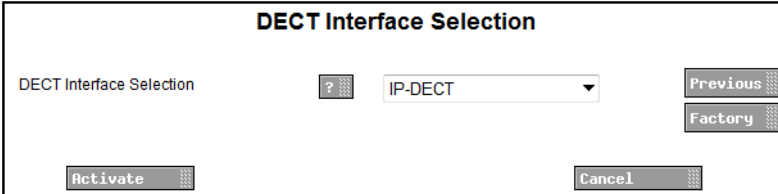
Every configured connection is supervised every 60 seconds. If the supervision fails the connection is handled as lost and a persistent fault is generated. After solving a problem with a lost connection, it can take up to one minute before the connection over the DECT interface is restored. During that time the connection is considered lost and no messages will be sent to that specific connection.

## 14.2 MIXED DECT SYSTEMS

It is possible to connect different kinds of DECT systems to a CPDM3. The systems that can be connected are MX-ONE and IP-DECT. This feature is useful when you want to connect only one CPDM3 to different DECT systems.

NOTE: Configuration of mixed DECT systems cannot be done via the Wizard.

- 1 Click "Configuration" on the start page.
- 2 Select Other > Advanced Configuration in the menu on the Configuration page.
- 3 Select "Interface Selection" under DECT Interface on the Advanced Configuration page.



The screenshot shows a dialog box titled "DECT Interface Selection". Inside the dialog, there is a label "DECT Interface Selection" followed by a question mark icon and a dropdown menu currently showing "IP-DECT". To the right of the dropdown are two buttons: "Previous" and "Factory". At the bottom of the dialog are two buttons: "Activate" and "Cancel".

- 4 In the DECT Interface Selection drop-down list, select "IP-DECT"
- 5 Click "Activate".
- 6 The CPDM3 must reboot to apply the setting. Click the link "Click here to reboot" and then click "Reboot".

- 7 When the CPDM3 has been rebooted, select "IP-DECT" under DECT Interface on the Advanced Configuration page.

IP-DECT

DECT interfaces

?

NOT USED

NOT USED

NOT USED

NOT USED

NOT USED

NOT USED

NOT USED

NOT USED

NOT USED

NOT USED

Multiple IP-DECT masters

Data encryption for multiple IP-DECT masters

- 8 Click "Multiple IP-DECT masters".

Module settings

Multiple IP-DECT masters

?

Yes

Previous

Factory

Activate

Cancel

- 9 In the Multiple IP-DECT masters drop-down list, select "Yes".
- 10 Click "Activate".
- 11 The CPDM3 must reboot to apply the setting. Click the link "Click here to reboot" and then click "Reboot".
- 12 When the CPDM3 has been rebooted, select "IP-DECT" under DECT Interface on the Advanced Configuration page.
- 13 Configure the DECT interface to be connected to the CPDM3 by clicking on a "NOT USED" link.

### DECT Interface IP address

|                           |   |  |          |
|---------------------------|---|--|----------|
| Name                      | ? | <input style="width: 95%;" type="text"/>   | Previous |
| Master IP address         | ? | <input style="width: 95%;" type="text"/>   | Factory  |
| Standby Master IP address | ? | <input style="width: 95%;" type="text"/>   |          |
| DECT Interface Selection  | ? | <div style="border: 1px solid black; padding: 2px; display: inline-block;">IP-DECT ▼</div> |          |

Activate
Cancel

- 14 Enter the following:
 

|                           |   |
|---------------------------|---|
| Name:                     | Description to identify the DECT interface. The description will appear in the DECT interface list.         |
| Master IP address:        | The IP address to primary DECT system. That is, the IP address of IP-DECT Master or IP address of MX-ONE.   |
| Standby IP address:       | The IP address to the secondary DECT system used as backup if the primary DECT system goes down. (Optional) |
| DECT Interface Selection: | The DECT interface to be used.  |
- 15 Click "Activate".
- 16 Repeat steps 13 - 14 to add additional DECT systems.

## 14.3 DECT INTERFACE SETTINGS

The DECT Interface controls the messaging flow between the Cordless Telephone System and the CPDM3.

### 14.3.1 GENERAL SETTINGS

- 1 Click "Configuration" on the start page.
- 2 Select Other Settings > Advanced Configuration in the menu in the on the Configuration page.
- 3 Select "General Settings" in the menu on the Advanced Configuration page.
  - Call Diversion Display Text  
When this parameter is enabled, the text specified is added to the display message when a call diversion takes place. The original Call ID can be included in the parameter text by writing a % character where the Call ID shall be inserted.

Advanced parameters include:

- **Broadcast**  
Specifies whether broadcast messaging is allowed or not. Only IP-DECT systems can handle broadcast, all other systems will ignore the parameter.
- **Set time in DECT?**  
N/A
- **DECT Interface**  
This parameter makes it possible to disable the DECT Interface on the CPDM3. When the DECT interface is disabled, messaging is not supported and lost link to DECT system will not be indicated.
- **IM update status handling**  
Only valid in combination with Ascom messaging system.
- **No of included 9dLD locations**  
Only valid in combination with Ascom messaging system.

### 14.3.2 SYSTEM DEPENDENT SETTINGS

Which parameters that can be changed is dependent on the connected Cordless Telephone System.

To find IP-DECT settings, see [14.3.1 General Settings](#) on page 119.

#### **MiVoice MX-ONE**

- **IP address**  
Since the IP-DECT Master is connected over the LAN, the IP address to MX-ONE has to be entered.
- **Port Numbers**  
Port 1814 is used for communication with the MX-ONE. This port has to be defined in the MX-ONE as well. The MX-ONE must be configured to use port 1815 when communicating with the CPDM3. The MX-ONE must be configured to use port 1817 when communicating with a CPDM3 configured with a mixed DECT system that uses encryption.

NOTE: If the CPDM3 replaces a 9dMMS, check that no other port numbers than the ones above are used for communication between the 9dMMS and the MX-ONE.

#### **For a single IP-DECT interface**

- **DECT IP address**  
Enter the IP address to the IP-DECT Master.
- **Secondary DECT IP address**  
If two DECT systems are used for redundancy purposes, enter the IP address to the secondary DECT system.

#### **For multiple IP-DECT interfaces**

- **Name**  
Enter a name for the IP-DECT interface. The name will be shown in the DECT interface list.
- **Master IP address**  
Enter the IP address to the primary Master
- **Standby Master IP address**  
Enter the IP address to the secondary Master if a secondary Master is used as a backup.



### 14.3.3 DECT MESSAGE DISTRIBUTION

The DECT Interface has distribution lists that define where incoming data from handsets, for example alarms and user data, should be sent.

- 1 Click "Configuration" on the Start page.
- 2 Select Other Settings > Advanced Configuration in the menu on the Configuration page.
- 3 Select "Message Distribution" under DECT Interface in the menu on the Advanced Configuration page.

The following information is supported:

- Alarm
  - Personal alarm with location information from handsets in the Cordless Telephone System.
- Mobile Data
  - .Not used
- Location
  - Special Location<sup>1</sup> information from handsets in the Cordless Telephone System. This information can be used to track the route of a handset in a building.
- Availability info
  - Includes absence information, that is, if a handset is placed in Charging/Storage Rack.

The addressing of the receivers is described in the Installation Guide for your product.

### 14.3.4 SMS CHARACTER SET

This setting determines which characters that can be displayed in the handsets when they receive messages. Additionally, the setting also determines which characters that can be entered in the handsets when the users write messages.

NOTE: The number of characters that can be entered in the handset when writing a message depends on which SMS character set that is used.

- 1 Click "Configuration" on the Start page.
- 2 Select Other Settings > Advanced Configuration in the menu on the Configuration page.
- 3 Select "SMS Character Set" under DECT Interface in the menu on the Advanced Configuration page.
- 4 Select one of the following:

|  |  |
|--|--|
| - Standard SMS<br>(Compatibility Mode) | Standard SMS works with all handsets but some special characters may not be correct. |
| - Latin-1                              | Used for later generation of handsets.   |

---

<sup>1</sup>.A Special Location can be sent every time a handset gets a new location code from a location device in the system. This feature can only be used in combination with Ascom messaging system and also require configuration both in the handset and in the location device. Also called "Immediate Alarm Transmission".

- UTF-8

Used for later generation of handsets. Use UTF-8 to include characters that is not included in the Latin-1 character set.

5 Click "Activate".

## 15. WLAN INTERFACE

### 15.1 HANDSET REGISTRATION

To be able to register, each VoWiFi handset must be programmed with the IP address of the CPDM3 used, refer to the Configuration Manual for respective VoWiFi handset.

### 15.2 WLAN SYSTEM

WLAN system handles the VoWiFi handset relogin time and authentication. A handset is considered to be logged out if it has not made a relogin within a certain time. Call diversion display text, Extended activity logging are also enabled in this view.

To find settings for WLAN System, do as follows:

- 1 Click "Configuration" on the start page.
  - 2 Select Other Settings > Advanced Configuration in the menu in the on the Configuration page.
  - 3 Select "WLAN System" under WLAN Interface in the menu in the on the Advanced Configuration page.
- Device relogin time (minutes)  
The time before a handset must relogin is set in minutes and when this time is exceeded the handset will be considered unreachable. This is the maximum time it takes for a handset to reconnect after installing a new or updating the CPDM3. Note that a short relogin time implies a higher service/security but it also loads the system.
  - Call Diversion Display Text  
Text specified in the "Call Diversion Display Text" text field is, if enabled, added to the display text when a call diversion takes place. By entering the character "%", the original call ID will be included in the display text on the place where the character is entered. Note that some characters are special characters that are not visible.
  - Enable Extended Activity Log  
Enable Extended Activity Log for intermediate logs, for more information see the Function Description, Activity logging in Unite document.
  - Authentication Method  
The very first time a VoWiFi handset logs in, it must authenticate itself with a password. The password is then stored in the handset for future authentication. The CPDM3 has three authentication alternatives; "Common password", "User server" and "Number as password".
  - Common Password  
A common password can be specified in the CPDM3, and this password is then used for all VoWiFi handsets in the system. If the common password field is left empty, the handset must send an empty password for authentication.
  - Allow Forced Login?

NOTE: The function is only valid when the authentication method is set to “Common password” or to “Number as password”. See • [Authentication Method](#) on page 123.

Forced login allows a user to login with a call number that already is in use. The handset that already is logged in will then be unregistered.

IP address is specified, EventHandler will be used as a default service.

## 15.3 WLAN MESSAGE DISTRIBUTION

The WLAN Interface has distribution lists that define where incoming data from handsets, for example alarms and user data, should be sent.

To find settings for WLAN Message Distribution, do as follows:

- 1 Click “Configuration” on the Start page.
- 2 Select Other Settings > Advanced Configuration in the menu on the Configuration page.
- 3 Select “Message Distribution” under WLAN Interface in the menu on the Advanced Configuration page.

The following information is supported:

- Alarm
  - Personal alarm from VoWiFi handsets.
- Mobile Data
  - User data sent from VoWiFi handsets.
- Availability Info
  - Change of status of the VoWiFi handsets.  
(The status can also be changed from the VoWiFi handset).

The addressing of the receivers is described in Installation Guide, Elise3, TD 92232GB.

## 15.4 USER SERVER

CPDM3 can set a user server for authentication of handsets, see [15.2 WLAN System](#) on page 123.

- 1 Click “Configuration” on the Start page.
- 2 Select Other Settings > Advanced Configuration in the menu on the Configuration page.
- 3 Select “User Server” under Other in the menu on the Advanced Configuration page.
- 4 Enter the IP address of the User Server and click “Activate”.

## 16. SYSTEM 900

This chapter handles settings for the connection to the System 900 A-bus. If the A-bus is not connected, the bus operating mode should be set to 'No A-bus'. All other parameters only need to be set when the CPDM3 is connected to a Central Unit in the System 900, or controlling the communication on the A-bus in systems without a Central Unit. See [16.1 System 900 Interface](#) for more information about the parameters.

### 16.1 SYSTEM 900 INTERFACE

- 1 Click "Configuration" on the Start page.
- 1 Select Other Settings > Advanced Configuration in the menu on the Configuration page.
- 2 Select 900 Interface > System 900 in the menu on the Advanced Configuration page. The following parameters can be set:
  - Bus operating mode
    - A-bus with Central Unit: the module is connected to a system with a Central Unit
    - A-bus without Central Unit: the module controls the communication on the A-bus.
    - No A-bus connected: The A-bus connection is not used.
  - Module address

This is the A-bus module address used when the module is connected to a system with a Central Unit.
  - Module priority

This is the module's priority on the A-bus. This parameter is only used when it is connected to an A-bus with Central Unit. Permitted values: 1-9.

    - 1 = Highest priority (Alarm Modules)
    - 3 = Normal priority (Other modules), Default: Normal priority
    - 9 = Lowest priority (Data Modem)
  - Default number of transmissions

This is how many times a paging is transmitted in the System 900. This parameter is only used when the module is connected to an A-bus with Central Unit.
  - Automatic or Manual configuration of prefix and call number

When the module is connected to an A-bus with Central Unit, the parameters in the Central Unit can be used and this parameter can be set to "Automatic". If the module is controlling the communication on the A-bus, the parameters have to be configured manually.
  - Number of digits in call number
  - This is the number of digits in the Portable Device addresses in the system. If the module is controlling the communication on the A-bus, this parameter has to be set manually.

Prefix and call number range

This is the prefix that is used in the system. The prefix has to be the same as for the other modules in the system. If the module is controlling the communication on the A-bus, this parameter has to be set manually.
  - Send module status from A-bus to Unite

When this parameter is enabled, the module sends module status to Unite as a status log.

- **Call Diversion Display Text**  
When this parameter is enabled, the text specified is added to the display message when a call diversion takes place. The original Call ID can be included in the parameter text by writing a % character where the Call ID shall be inserted.

## 16.2 SYSTEM 900 MESSAGE DISTRIBUTION

The 900 Interface in CPDM3 has distribution lists that define where incoming data from the handsets in the System 900 and the System 900 modules should be sent. The receivers are addressed in the same way as for the DECT Interface that is described in Installation Guide, CPDM3, TD 93040EN.

- 1 Click "Configuration" on the Start page.
- 1 Select Other Settings > Advanced Configuration in the menu on the Configuration page.
- 2 Select Message Distribution under 900 Interface in the menu on the Advanced Configuration page. The following parameters can be set:
  - **Alarm**  
Personal alarms with location information from handsets.
  - **Mobile Data**  
Data sent from handsets.
  - **Input activity**  
An input on an Alarm Module has been activated.
  - **Location**  
Special Location<sup>1</sup> information from handsets.
  - **Availability Info**  
Includes absence information, that is, if a handset is placed in Charging/Storage Rack.

Pagings that are received from the A-bus will be transmitted to the destination that corresponds to the address in the UNS.

---

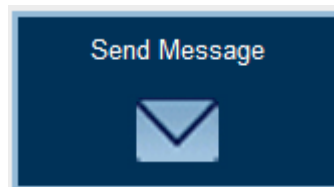
1. The Special Location can be sent every time a cordless phone gets a new location from a locator in the system. This requires configuration both in the handset and in the locator. Also called "Immediate Alarm Transmission".

## 17. MESSAGING OPERATION

Creating and sending messages via the Messaging Tool requires no password and can be done by any user in the system.

Depending on license, different tools for messaging are displayed:

- Messaging Tool - included if the license does not include NetPage

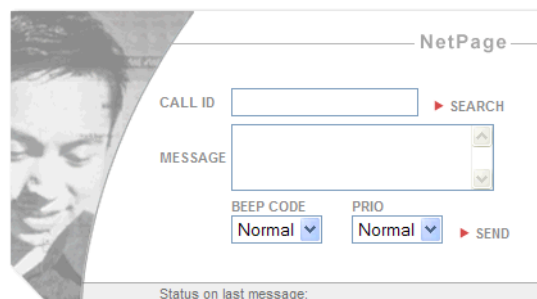


### 17.1 CREATE AND SEND MESSAGES VIA NETPAGE

NetPage supports messages with character encoding UTF-8 (for example Russian characters and Swedish characters).

- 1 Click "Send Message" on the start page. Netpage opens.

Figure 26. The Netpage window



- 2 Click either the "Search" button to search a number from the number list, or enter a number in the Call ID field. It is possible to write several Call IDs separated by a semicolon.
- 3 Enter message text in the Message text field.
- 4 Select Beep Code and Priority.
- 5 Click "Send".

### 17.2 PREDEFINED MESSAGES

NOTE: This feature can only be reached from index4.

The predefined messages feature includes message text, beep characteristics, priority and message type. There are two types of messages: "Common Messages" and "My Messages".

NOTE: The maximum message length differs depending on which system or handset the message is sent to and the amount of special characters included in the message.

### Common Messages

Common Messages can be used by all NetPage users. Up to 30 "Common Messages" can be created. These messages are stored on the module and can only be changed by authorized persons.

### My Messages

Up to 30 predefined "My Messages" with 120 characters per message can be created. It is also possible to have fewer "My Messages" containing more characters. These messages are stored locally and can only be accessed or changed from that PC.

## 17.2.1 CREATE A PREDEFINED MESSAGE

- 1 Click the "Common Messages" or "My Messages" button in NetPage. For "Common Messages" enter the user name "user" and the password "password".
- 2 Click "Add message".
- 3 Enter the name of the message and add a message text of maximum 250 characters.
- 4 Set the message type, beep code and priority.
- 5 Click "Save".
- 6 Click "Close" to exit the administration.

## 17.2.2 EDIT A PREDEFINED MESSAGE

- 1 Click the "Common Messages" or "My Messages" button in NetPage. For "Common Messages" enter the user name "user" and the password "password".
- 2 Select the message that shall be changed and the administration field will open.
- 3 Make the changes and click "Save".
- 4 Click "Close" to exit the administration.

## 17.3 MESSAGE HISTORY STATUS

Status on the last sent message:

| Status            | Description   |
|-------------------|---|
| Message accepted  | The message is accepted by NetPage and will be transmitted.         |
| Message completed | The Messaging System has completed the transmission of the message. |

In the user interface (index4), other "message history statuses" can appear such as:

- Absence
- Call Diversion
- Manual Acknowledge
- Delivery Receipt



## 17.4 PREDEFINED GROUPS

NOTE: This functionality is only accessible from index4, see [figure 35](#) on page 143.

### My Groups

“My Groups” are stored locally and can only be accessed or changed from the PC where they are stored.

### Common Groups

“Common Groups” can be used by all NetPage users. It is possible to create up to 30 predefined “Common Groups” with up to 50 Call IDs in each. These groups are stored on the FTP area.

There is a limited storage area. This means that, for groups with approximately 20 characters (name and Call ID), the following applies:

| Amount of Groups | Group Members |
|------------------|---------------|
| 10               | 19            |
| 15               | 7             |
| 20               | 2             |

### 17.4.1 CREATE A GROUP

- 1 Click the “Common Groups” or “My Groups” button in NetPage. For “Common Groups” enter the user name “user” and the password “password”.
- 2 Click “Add group”.
- 3 Enter a name for the group in the Name text field.
- 4 Click the “To” button and select users (from the phonebook) to be members of this group or enter number in the Call ID text field and click “Add”.
- 5 Click “Save”.
- 6 Click “Close” to exit the administration.

### 17.4.2 EDIT A GROUP

- 1 Click the “Common Groups” or “My Groups” button in NetPage. For “Common Groups” enter the user name “user” and the password “password”.
- 2 Select the group that should be changed and the administration field will open.
- 3 Make changes and click “Save”.
- 4 Click “Close” to exit the administration.

## 17.5 NETPAGE CONFIGURATION

### Set Messaging Properties

Besides the settings for NetPage web messaging it is also possible to select which GUI to use as default for NetPage.

- 1 Click “Configuration” on the start page.
- 2 Select Other Settings > Advanced Configuration on the Configuration page.
- 3 Click “Web Messaging” in the menu on the Advanced Configuration page.

**Message**

Message max length ? 160 Previous

Call ID range - Lower limit ? Factory

Call ID range - Upper limit ?

User login required ? No

Automatic logout when idle (minutes) ?

Messaging rights ? Call ID range

Number list source ? Local

Default GUI ? Custom

Activate Cancel

4 Enter values for messaging.

5 Click “Activate”.

The following parameter can be set:

- **Message max length.**  
Sets the maximum number of characters that can be forwarded to a unit. Messages longer than the set value are truncated.
- **Call ID range - Lower limit**  
Sets the lower limit of a Call ID range. Messages sent to Call IDs out of this range are cancelled. An empty field means no lower limit.
- **Call ID range - Upper limit**  
Sets the upper limit of a Call ID range. Messages sent to Call IDs out of this range are cancelled. An empty field means no upper limit.
- **User login required**  
Sets whether a login is required for NetPage. This parameter shall be set to No for the default GUI (index3). If index4 is used, the Message History section must be included. Refer to [18.2 Customize the User Interface \(GUI\)](#) on page 137.
- **Automatic logout when idle (minutes)**  
Sets how long a user can be idle before being logged out. To prevent automatic logout, leave this field empty. If the parameter “User login required” is set to “No”, leave this field empty.
- **Messaging rights.** Choose between Call ID range and User rights to determine how NetPage shall verify Call IDs.  
“Call ID range” means that Call IDs are verified according to the Call ID range limit settings. This requires that the parameter “User login required” is set to “Yes”.
- **Number list source.** Choose between Local and Unite CM users.  
This is the Number list that is used in NetPage. In systems without an Unite CM, this parameter shall always be set to “Local”.
- **Default GUI.** Select which GUI to use as start page for NetPage. Choose between Custom, Index 1, Index 2, Index 3, Index 4. See [18.2 Customize the User Interface \(GUI\)](#) on page 137 for more information about the different GUI's.

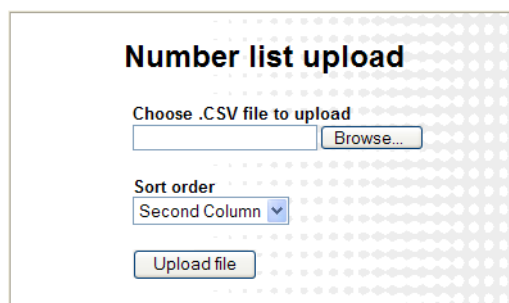
### Creating or Updating the Number list

In the NetPage default GUI (index.html), a number list can be accessed by clicking the “Search” button. Before the number list can be used, the entries have to be added.

The number list entries can be created from any CSV file, using Microsoft Excel or any leading spreadsheet or relational database application. It is possible to import maximum 3000 entries via the CSV file.

The CSV file is uploaded/pasted with the “Number list upload” program (included in NetPage) as described below.

- 1 Create a CSV file with the following format:  
First name 1;Surname 1;Telephone number 1  
First name 2;Surname 2;Telephone number 2
- 2 Open the page: <http://xxx.xxx.xxx.xxx/admin/user/uploadnrlist.html>.  
Log on with “user”. The default password is “password”



- 3 Browse to find the CSV file. Choose the sort order. Click “Upload file”.

When the CSV file is uploaded, it will be converted and saved as “uploadednrlist.js”. The file is a text file with the following format:

```
nr_array=[["First name 1","Surname 1","Telephone number 1"],["First name 2","Surname 2","Telephone number 2"]];
```

If you later want to edit the number list, the “uploadednrlist.js” file is accessible with the FTP client and can also be modified manually.

- 4 Test that the number list works as desired.

NOTE: When the phonebook has been updated, be sure to clear the cache memory on the web browser.

### 17.5.1 BACKUP AND RESTORE NETPAGE FILES

It is recommended to make a backup of all NetPage files, the phonebook and predefined groups and messages, if for example, you want to move a customized GUI to another module.

#### NetPage Files

NetPage files are the number list, the GUI files including image files and the Common Groups and the Common Messages files.

#### Backup

Copy and save modified files in the NetPage FTP area, see [18.2.2 Files for Translation/Editing](#) on page 138.

#### Restore

- 1 Put copies of the backup files in the NetPage FTP area, see [18.2.2 Files for Translation/Editing](#) on page 138.

- 2 Test that NetPage is functioning properly, see [18.3 Test the New User Interface](#) on page 147.

#### **Backup of Predefined Groups and Messages**

NOTE: Default user name is “user” and password is “password”, but this can have been changed in your system.

#### **Backup**

- 1 Open NetPage. In the Administrate field, select the “My Groups” button. Click the “Backup/ Restore” button. The “Backup/ Restore” view is opened. Click “Backup” > “Save”. Choose the file name and save.
- 2 Repeat the same process as above in point 1) but for “My Messages”

Common messages are included in the ordinary backup for the module. To backup common messages separately, repeat the same process as above in point 1) but for “Common Messages”. (Log in with “user” and password “password”).

#### **Restore**

- 1 Open NetPage. In the Administrate field select the “My Groups” button. Click the “Backup/ Restore” button. In the “Backup/ Restore” view click “Browse...” and browse to the once backed-up file. Click Open > Restore.
- 2 Repeat the same process as above in point 1) but for “My Messages”
- 3 If not already done, repeat the same process as above in point 1) but for “Common Messages”. (Log on with “user” and password “password”).
- 4 Test that NetPage is functioning properly, see [18.3 Test the New User Interface](#) on page 147.

## 18. ADMINISTRATION OF LANGUAGE AND USER INTERFACES

All text shown in the user interface is default in English, but a copy of the language can be translated and imported to the module. Several languages can be added. The default English language is not possible to edit or remove. The supplied user interface can also be modified to suit the individual customer requirements concerning functionality.

Basic changes that can be made are:

- Translate or adapt text (refer to [18.1.2 Translate/Edit the Language](#) on page 134)
- Hide unused functionality (refer to [18.2.5 Change the NetPage User Interface Functionality](#) on page 141)
- Modify the user interface to suit the customer's image (refer to [18.2 Customize the User Interface \(GUI\)](#) on page 137)
  - Limit the number of characters included in the message text.
  - Add company logo and/or modify the GUI to suit the customer's image

NOTE: The user interface only supports the Latin-1 character set.

### For the best screen appearance

Windows standard screen settings, using normal font size, are recommended. The recommended screen resolution is 1024 x 768.

### How to edit

The code is thoroughly commented to make it easy to understand, and can be edited with a simple text or HTML editor. Basic HTML, Java Script, and CSS knowledge is recommended.

NOTE: Do not use an intelligent html editor like Frontpage or Dreamweaver, as it might corrupt the html code.

## 18.1 CUSTOMIZE THE LANGUAGE

### 18.1.1 EXPORT A LANGUAGE FOR TRANSLATION/EDITING

- 1 Click "Configuration" on the start page.
- 2 Select Other Settings > Set language in the menu in the on the Configuration page.
- 3 Click the "Import/Export Language" button. The Translation page opens.

## Translation

Existing languages:

[English](#)

*Each language can be exported as an XML file. To create a new language or update an existing, click a language link above to download the file. If a new language should be created, change the language indication in the "language" tag. Translate/Update the text within "translation" and "helptext" tags and save the file. Import the XML file.*

Import language file:

Enable translation mode: ☐

*In "Translation mode" all text will be exchanged with the identification in the language file. This can be used to identify where a text is displayed in the GUI.*

- 4 Click an existing language link to create or update languages. An XML file is generated and the File Download window opens.
- 5 Save the file for translation or editing purposes. The file can be saved in any name during the translation.

### 18.1.2 TRANSLATE/EDIT THE LANGUAGE

In the downloaded language file, there are numerous tags but only the translation of two tags and one attribute are mandatory:

- `<language id="English">`  
The "id" attribute is the text that appears in the drop-down list. Change "English" to the name of your translated language here.
- `<translation>`  
Text displayed in menus, on buttons, tabs etc. Translated text can be added inside the tags.
- `<helptext>`  
On-line help text. Translated text can be added inside the tags.

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

Figure 27.

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<translations>
  <language id="English" type="complete">
    <app id="Alarm Manager">
      <text id="ACTION_TYPE_SELECTOR">
        <translation>Action Type</translation>
        <helptext>Select which type of action to take.</helptext>
      </text>
      <text id="ACTIVATE_EHCONF_OK">
        <translation>Activation of configuration OK.</translation>
      </text>
      <text id="ALARM_TYPE_SELECTOR">
        <translation>Alarm Type</translation>
        <helptext>The alarm type that should be triggered. </helptext>
      </text>
    </app>
  </language>
</translations>
```

079

Example of a language file (.xml).

### 18.1.3 SHOW PAGES IN TRANSLATION MODE

All texts, buttons, menus etc. are identified with labels (for example TEXT\_TRANSLATION\_TITLE). With the translation mode function it is possible to view the label for each button, menu etc. This can be helpful when translating the language file. For not losing one's bearings during the translation it is a help to open two windows and view one of them in translation mode and the other in normal mode.

- 1 Select the "Enable translation mode" check box in the Import/Export Language page, and click "Apply".

Figure 28.

## Translation

Existing languages:

[English](#)

*Each language can be exported as an XML file. To create a new language or update an existing, click a language link above to download the file. If a new language should be created, change the language indication in the "language" tag. Translate/Update the text within "translation" and "helptext" tags and save the file. Import the XML file.*

Import language file:

Enable translation mode: ☒

*In "Translation mode" all text will be exchanged with the identification in the language file. This can be used to identify where a text is displayed in the GUI.*

### Translation page in normal view

All the labels on the pages are shown, see example below.

Figure 29.

## TEXT\_TRANSLATION\_TITLE

TEXT\_TRANSLATION\_LANGUAGE\_TEXT

[English](#)

TEXT\_TRANSLATION\_EXPORT\_TEXT

TEXT\_IMPORT\_LANGUAGE

TEXT\_TRANSLATION\_CHECKBOX\_CAPTION

☒ OPTION\_DESIGN\_MODE

TEXT\_TRANSLATION\_SAVE\_TEXT

### Translation page in translation mode

To return to standard view:

- 1 Clear the OPTION\_DESIGN\_MODE box.
- 2 Click "BUTTON\_SAVE".

#### 18.1.4 IMPORT LANGUAGE FILE


When the file is translated, it must be imported to the module.

- 1 Click "Configuration" on the start page.



- 2 Select Other Settings > Set language in the menu in the on the Configuration page.
  - 3 Click the “Import/Export Language” button. The Translation page opens
  - 4 Click “Browse” to locate the translated file, and then click the “Import” button.
- The name of the translated language (the language “id” attribute) will appear as a link in the Existing Language list and can be downloaded for editing purposes.

#### 18.1.5 DELETE LANGUAGE FILE

On the Translation page, click the  icon to the right of the language you want to remove. Note that it is not possible to remove the default language.

[Swedish](#) 


[English](#)

#### 18.1.6 SELECT LANGUAGE

Translated languages (the language “id” attribute) are shown together with the default language “English” in the language drop-down list in the Language page.

- 1 Click “Configuration” on the start page.
- 2 Select Other Settings > Set language in the menu in the on the Configuration page.

##### Set language

English  Temporary Permanent

---

Import/Export Language

- 3 Select language in the drop-down list and click “Permanent”.  
To change language for this session only, that is, for this browser window until closed, click “Temporary”.

## 18.2 CUSTOMIZE THE USER INTERFACE (GUI)

The module has an FTP area with default 50 MB disk space. The disk space can be set in the interval 5 MB up to 150 MB.

The free space can be used for storing files and folders, for example, a customized user interface for sending messages.

### 18.2.1 CHANGE THE SIZE OF THE FTP AREA

This is a secured setting and before it can be activated it must manually be confirmed by pressing the mode button on the module.

- 1 Click "Configuration" on the start page.
- 2 Select Other Settings > Advanced Configuration in the menu on the Configuration page.
- 3 Under Common, click "FTP area" in the menu on the Advanced Configuration page.
- 4 Fill in required size between 5 – 150 MB and click "Activate".  
You will be prompt to confirm the change by pressing the mode button.
- 5 Press the mode button on the module.
- 6 Click "Activate" to save the changes.
- 7 Click the mode button to return to normal mode immediately or wait 10 minutes for the module to return automatically. Any secured setting can be activated within the 10 minutes period.

The module needs to be restarted for the changes to take effect.

### 18.2.2 FILES FOR TRANSLATION/EDITING

- 1 Log on to the module via an FTP client. Note that how to log on can differ between different FTP clients.<sup>1</sup>

Default username is "ftpuser" and default password is "changemetoo".  
xxx.xxx.xxx.xxx is the host name.

Examples:

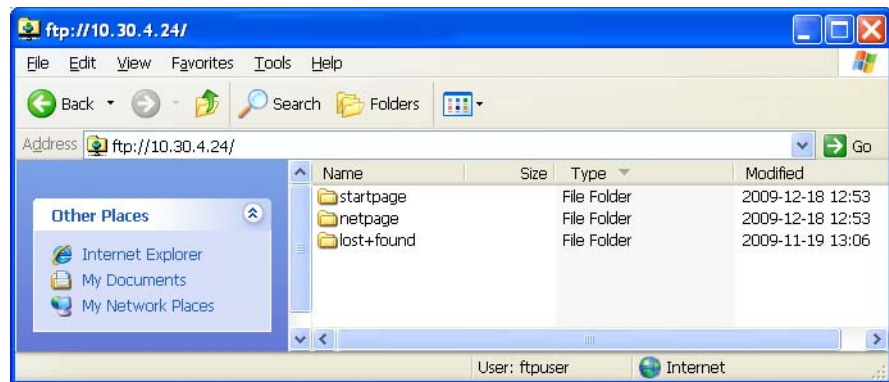
- Windows Explorer: fill in "ftp://username:password@xxx.xxx.xxx.xxx" in the address field.
- Firefox: fill in "ftp://xxx.xxx.xxx.xxx" in the address field and log on with "username" and "password".

NOTE: When secure mode is enabled, only secure access via HTTPS and FTPES are allowed. HTTP is automatically redirected to HTTPS, and FTP access is not allowed. The FileZilla Client freeware (not included) supports FTPES. See [3.4.1 Web Access Security Settings](#) on page 22.

The files located in the Start page and Netpage folders, including GIFs and CSS, can be downloaded/copied to a folder on your hard disc.

---

<sup>1</sup>.Internet Explorer is not an FTP client. It can be used for viewing but not for transferring files.



When restoring NetPage files, the files shall be placed in the same folder.

### 18.2.3 DEFAULT START PAGE GUI

Figure 30. Start page default user interface (index\_template)

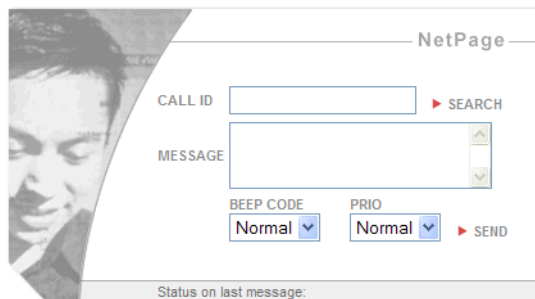


A copy of the default Start page is stored in the start page folder on the module's FTP area. The start page copy `index_template`, is an html file that can be copied and edited. The start page can also be replaced with a completely new user interface.

When the edited or new html file is saved as `index.html` and placed in the Start page folder on the module's FTP area, it will replace the default start page.

## 18.2.4 DEFAULT SEND MESSAGE GUI

Figure 31. NetPage default user interface (index3).



The screenshot shows the NetPage default user interface. It features a header bar with the title 'NetPage'. Below the header, there is a 'CALL ID' text input field followed by a red 'SEARCH' button. Underneath is a 'MESSAGE' text area with a vertical scrollbar. Below the message area are two dropdown menus: 'BEEP CODE' and 'PRIO', both currently set to 'Normal'. To the right of these dropdowns is a red 'SEND' button. At the bottom of the interface, there is a status bar labeled 'Status on last message:'.

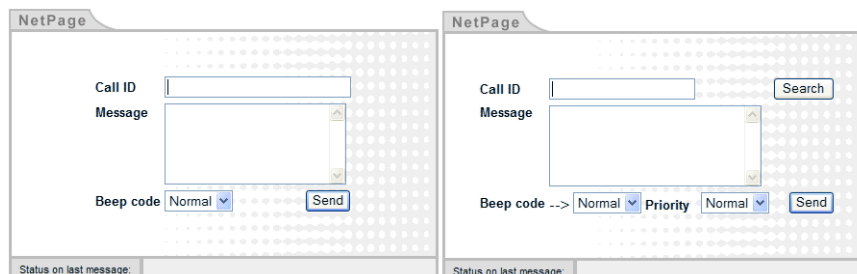
By clicking “Send Message” on the start page, the default NetPage user interface index3.html is opened.

In the NetPage folder on the module’s FTP area, there are four examples of the NetPage user interface; index1, index2, index3 and index4. index3 is a copy of the default NetPage user interface.

All NetPage functionality is included in the default user interface, but all parameters that can be configured in the example user interfaces index1, index2 and index3, are not shown. The necessary code for viewing and configuring the hidden parameters is included, but they are marked as comments to prevent the browser from interpreting them, see [18.2.5 Change the NetPage User Interface Functionality](#) on page 141.

The default user interface can be exchanged with one of the example user interfaces, shown in [figure 32](#), by saving the html file as index.html and replacing the existing index.html file. index4 is shown in [Example GUI index4](#) on page 143.

Figure 32. NetPage user interface examples; index1 and index2



The figure displays two side-by-side screenshots of NetPage user interfaces. The left screenshot (index1) shows a 'Call ID' input field, a 'Message' text area, a 'Beep code' dropdown menu set to 'Normal', and a 'Send' button. The right screenshot (index2) shows a similar layout but includes an additional 'Priority' dropdown menu set to 'Normal' next to the 'Beep code' dropdown. Both interfaces have a 'Status on last message:' bar at the bottom.

**NOTE:** The Java Script code in the HTML files is used for interpreting and displaying responses from the messaging system. It is recommended that this code is used unmodified, otherwise, the Message history functionality may be lost. Also, the Java Applets must be left unchanged to preserve the functionality.

**NOTE:** No server side scripts are allowed in the FTP area.

## Priority and Beep Codes in the default NetPage User Interface

| GUI Description    | Priority Code |
|--------------------|---------------|
| Low                | 9             |
| Normal             | 7             |
| High               | 3             |
| Alarm <sup>a</sup> | 1             |

a. Marked as hidden in the html page.

| GUI Description | Beep Code |
|-----------------|-----------|
| Silent          | 0         |
| 1 beep          | 1         |
| 2 beeps         | 2         |
| 3 beeps         | 3         |
| 4 beeps         | 4         |
| 5 beeps         | 5         |
| 10 beeps        | 6         |
| Siren           | 7         |

### 18.2.5 CHANGE THE NETPAGE USER INTERFACE FUNCTIONALITY

As a help for locating comments/hidden text in the html code, the comment marks “<!--” and “-->” are used, see the example in [figure 33](#). The comment marks are also used to hide functionality in the user interface. Text written, or functionality, framed by the comment marks is not interpreted by the web browser.

Figure 33. Example of how to mark html text as comments, that is,. hide it.

```
<TD valign="top" style="height:25">
  <!-- This is the button that opens the NetPage phonebook.
  If the phonebook is not used, remove the complete script and
  the &nbsp;&nbsp;  line (mark it as comments to be able to
  include it again later on) -->
```

For comments included in the Java Script code, the comment mark “//” is used, see figure [figure 34](#). Text written after the comment mark (in the same line) is not interpreted by the web browser.

Figure 34. Example on comments in a Java Script.

```
function sendform() {
    addCallNo(document.testform.callno.value, '');
    // If the user forgot to press 'add'
    tmp1list = document.testform.callnolist;
```

Buttons, for example the “To” button that opens the phonebook, can also be hidden directly in the code. To do this, insert “hidden” (double quotation marks both before and after “hidden”) as input type as follows:

```
document.write('<input type="button" value="...  
will become  
document.write('<input type="hidden" value="...
```

NOTE: To change the user interface (index4) it is necessary to open and change one or more of the files: “send.html”, “receive.html” and “admin.html”.

NOTE: If changes to the phonebook access (“To” button), beep codes or priority settings are made, it is also necessary to change the files “editpagtext.html” and “leditpagtext.html”, to get a consistent user interface.

In order to be able to restore the default GUI, make a backup before changes. See [18. Administration of Language and User Interfaces](#) on page 133.

## 18.2.6 TRANSLATION OF THE USER INTERFACES

The texts presented in the user interfaces can be translated. The translation is entered differently depending on the example user interface that is used. The HTML files index\_template and index1, index2 and index3 are translated in the HTML code. The NetPage user interface (index4) on the other hand is translated in the “language.js” and “receive.html” file, where receive.html includes the NetPage message history applet. See [figure](#) on page 143 for an overview of where the different files are used.

### Start Page

- 1 Download/copy the file and included image from the FTP area, refer to [18.2.2 Files for Translation/Editing](#) on page 138.
- 2 Open the file in a text or HTML editor and translate all words.
- 3 Save the file.
- 4 Upload/paste the file to the FTP area, refer to [18.2.7 Upload the Files to the module's FTP Area](#) on page 144.
- 5 Check that the user interface looks all right.

### Example User Interfaces index1, index2 or index3

- 1 Download/copy the file and included images from the FTP area, refer to [18.2.2 Files for Translation/Editing](#) on page 138.
- 2 Open the file in a text or HTML editor and translate all words and “immediate status” texts. For existing “immediate status” texts, see table below.
- 3 Save the file.
- 4 Upload/paste the file to the FTP area, refer to [18.2.7 Upload the Files to the module's FTP Area](#) on page 144.
- 5 Check that the user interface looks all right.

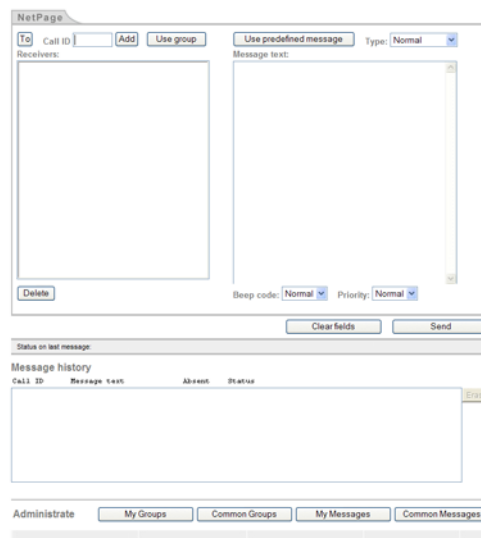
The following “immediate status” texts must be translated. Exchange the English text with your translation. Keep the code (20, 30 etc.) unchanged.

|     |                                   |
|-----|-----------------------------------|
| 20  | Message accepted                  |
| 30  | Memory full in message service    |
| 31  | Message deleted due to time-out   |
| 40  | Message not sent, invalid Call ID |
| nst | Message not sent                  |
| nlc | Message cancelled, no license     |

|     |                                      |
|-----|--------------------------------------|
| sto | Status time-out from message service |
| sns | Can't receive status                 |
| nan | Message cancelled, no Call ID        |
| oor | Call ID(s) out of number range       |
|     | Unknown returncode, confused!        |

#### Example GUI index4

Figure 35.



Files used for translation of the user interface (index4).

Text which needs to be translated, is found in two different files. Translation of texts in the user interface (including text in Administration pages, but excluding text in the Java Applet) are found in the "language.js" file. Translation of the Java Applet (Message history field) is found in the "receive.html" file.

- 1 Download/copy the files "language.js" and "receive.html" from the FTP area, refer to [18.2.2 Files for Translation/Editing](#) on page 138.
- 2 Open the "language.js" file in a text editor, for example Wordpad. Add the translation inside the quotation marks after the English text, see example below:  
"Add Group", " " will become "Add Group", "Your translation".  
Save the file.
- 3 Open the "receive.html" file in a text editor, for example Wordpad. Add the translation inside the quotation marks after the English text, see example below:  
PARAM NAME="English text" VALUE="Your translation".  
Save the file.
- 4 Upload/paste the files to the FTP area, refer to [18.2.7 Upload the Files to the module's FTP Area](#) on page 144.
- 5 Refresh the page and check the result. All buttons except the Administration buttons will expand/decrease when the text is translated. The width of the Administration buttons is fixed but can be altered in the HTML file "admin.html".

### 18.2.7 UPLOAD THE FILES TO THE MODULE'S FTP AREA

Upload/paste all updated files (including GIFs and CSS) to the FTP area.

NOTE: When secure mode is enabled, see [3.4.1 Web Access Security Settings](#) on page 22, only secure access via HTTPS and FTPES are allowed. HTTP is automatically redirected to HTTPS, and FTP access is not allowed. The FileZilla Client freeware (not included) supports FTPES.

- 1 Log on with an FTP client. Note that how to log on can differ between different FTP clients.<sup>1</sup>

Default username is "ftpuser" and default password is "changemetoo".  
xxx.xxx.xxx.xxx is the host name.

Examples:

- Windows Explorer: fill in "ftp://username:password@xxx.xxx.xxx.xxx" in the address field.
- Firefox: fill in "ftp://xxx.xxx.xxx.xxx" in the address field and log on with "username" and "password".

- 2 Copy the files and paste them into the FTP area.

### 18.2.8 INSERTING A COMPANY LOGOTYPE

In the default GUI, a company logotype can be inserted, for example, in a separate table above the NetPage application.

In the examples index1, index2 and index3, the company logotype can be inserted in any of the empty table cells of the NetPage application.

### 18.2.9 CREATING A URL CALL

It is also possible to send messages with hypertext links. This is useful in two ways. It makes it possible to open NetPage with some fields already filled in and to create buttons on another web page. For example, a hotel guest can then use a button on a PC screen to send a message to room service. In this case, NetPage is never shown to the user since the URL string contains all relevant data such as Call ID and message.

A CGI script on the NetPage web server is called with a set of parameters which are separated by the character "&". The "immediate status" (shown after the text "Status on last message:") can be presented on a separate web page by enclosing the URL to that web page. If no URL parameter is specified, the "immediate status" is always sent to the same web page as the message was generated from, and then that page has to handle the status. It is possible to use Common Groups when creating URL calls, Common Messages, My Groups and My Messages can not be used.

NOTE: The "immediate status" texts are shown in [18.2.6 Translation of the User Interfaces](#) on page 142.

NOTE: It is not possible to remote erase or receive "message history status" when using the URL call function.

---

<sup>1</sup>.Internet Explorer is not an FTP client. It can be used for viewing but not for transferring files.



### Parameters

The following parameters can be set for a URL message:

| Description   | Name | Value range   | Default value      |
|---------------|------|---|--------------------|
| Call ID       | no   | -   | -                  |
| Message text  | msg  | -   | -                  |
| Message type  | ack  | 0 no delivery receipt<br>1 delivery receipt<br>2 manual acknowledge | 0                  |
| Beep code     | bp   | 0-7   | 3                  |
| Priority      | pri  | 1-9   | 7                  |
| Return page   | url  | -   | Page you sent from |
| Message ID    | id   | see below   | Set by NetPage     |
| Erase message | del  | see below   | -                  |
| UTF8 encoded  | utf8 | see below   | -                  |

The wildcard (\*) is allowed in the Call ID, for example Call IDs 9370-9379 can be written as 937\*

NOTE: Wildcards are not supported by all systems.

### Message ID

The Message ID is used to refer to previously sent messages, for example, to make the cordless phone beep at each transmission of the message or to erase a previously sent message. The same Message ID as when the message originally was sent has to be used.

The Message ID can be set manually by the user or automatically by NetPage. NetPage sets the Message ID automatically if the parameter "id" is set to 0 or not specified. If the number is generated manually, it should be kept in the range 1 to 2147483647.

NOTE: NetPage does not check for conflicting manually set message IDs, therefore manually set message IDs must be kept unique. Conflicting message IDs will result in erroneous status reports among other problems.

### Erase message

A previously sent message can be erased with a new URL call. Call ID, Message ID and the parameter "del" should be included in the URL call. This brings that the Message ID has to be set manually if a message should be able to erase later on. The parameter "del" has to be given a value but the value has no meaning, i.e. it can have any value.

The URL will look as follows:

`http://xxx.xxx.xxx.xxx/cgi-bin/npcgi?no=1234&id=23&del=1`

### UTF8 encoded

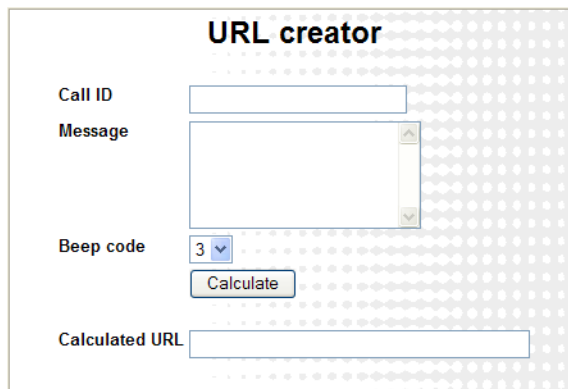
When NetPage is accessed from a cordless unit that uses WAP version earlier than 2.0, the message that is sent will be UTF8 encoded. The parameter “utf8” then has to be included to indicate this for the CGI script in NetPage. The parameter “utf8” has to be given a value but the value has no meaning, i.e. it can be any value.

NOTE: This parameter should not be used for HTML based NetPage applications.

### Creating the URL

When creating the URL message, special characters, for example space and question mark, have to be converted to hex code. For this purpose, a special conversion program called “URL Creator” is included in NetPage as described below.

- 1 Open “URL Creator”: <http://xxx.xxx.xxx.xxx/netpage/urlcreator.html>.

The image shows a web form titled "URL creator" with a light blue background and a dotted pattern. It contains four input fields: "Call ID" (a text box), "Message" (a larger text area), "Beep code" (a dropdown menu showing "3"), and "Calculated URL" (a text box). A "Calculate" button is located between the "Beep code" and "Calculated URL" fields.

- 2 Enter the Call ID and the message. Press “Calculate”. The URL string with special characters in hex is shown in the “Calculated URL” field.

### Creating a Quick Button with a URL Call

Example:

The link “<http://xxx.xxx.xxx.xxx/cgi-bin/npcgi?no=1234&bp=3&pri=7&msg=Hi%21>” will send a message to a cordless phone with number 1234 with the message Hi!, the priority 7, and the beep code 3.

NOTE: Priority can’t be set in the URL creator, but this part of the URL message can be written manually in the web browser address field, see the example above “&pri=7”.

- 3 Create a button. When the button is pressed, the following link should be opened: <http://xxx.xxx.xxx.xxx/cgi-bin/npcgi?<parameters>>. For information about parameters see [Parameters](#) on page 145.
- 4 If the “immediate status” should be shown on the page, it has to be handled. It is also possible to state a URL for the return page in order to show the “immediate status” on another web page.
- 5 Store the web page either locally or in the NetPage ftp area, see [18.2.2 Files for Translation/Editing](#) on page 138.

### Opening NetPage with Fields Automatically filled in

Example:

The link "http://xxx.xxx.xxx.xxx/netpage/?no=1234&msg=Hi%21" will open NetPage with the Call ID 1234 entered in the number field and the message Hi! in the message field.

- 1 Create a link or button that opens the following link when the button is pressed: <http://xxx.xxx.xxx.xxx/netpage/?<parameters>>.  
For information about parameters see [Parameters](#) on page 145.
- 2 If the "immediate status" should be shown on the page, it has to be handled. It is also possible to state a URL for the return page in order to show the "immediate status" on another web page. If index1, index2 or index3 is used, this is handled automatically.
- 3 Store the web page either locally or on the NetPage ftp area, see [18.2.2 Files for Translation/Editing](#) on page 138.

NOTE: This is not applicable when index4 example is used as default GUI.

## 18.3 TEST THE NEW USER INTERFACE

It is recommended to test the customized user interface as follows, for example:

- If a company logotype is added, check that it looks all right and that the module opens quickly. If it opens slowly, minimize the picture file size and save it as "interlaced" to decrease wait time for the image.
- Check that all text is correctly translated.
- Check that the phonebook opens and that the entries are correct.
- Send a message.
- Check that the "message history status" is received and displayed.

## 18.4 UPDATE THE USER INTERFACE AFTER A NEW RELEASE

When a new version of the module's software is released, there might be changes in the user interface that need to be translated.

- 1 Import your old translated file to the module that has been updated with new software. New text and buttons in the user interface are shown in English.
- 2 Click the language file link and save it.
- 3 Open the file. All tags that are not translated are marked with the comment:  
<!-- The text identifier below couldn't be translated -->
- 4 Translate the new text and import the translated file again.

## 19. SOFTWARE ADMINISTRATION

Besides the software administration via the CPDM3's Configuration page, it is also possible to administer the software via the module's Boot Mode GUI. This is described in the Installation Guide for CPDM3. The Boot Mode GUI is typically used if no software is installed on the module or if it is not possible to access the software.

Adding software for devices is done from the Device Manager application.

### 19.1 ADD DEVICE SOFTWARE TO THE DEVICE MANAGER

- 1 Click "Device Manager" on the start page.
- 2 Upload definition files. The definition files are usually included in a package file. See [7.6.3 Import Parameter Definition Files](#) on page 88 for more information. The package files may also contain software for the devices (.bin) and templates (.tpl). You may have to contact your supplier for the latest updates.

How to work with Numbers is described in chapter [7.4 Numbers](#) on page 77.

### 19.2 UPGRADE THE BOOT SOFTWARE

For instruction on how to upgrade the CPDM3 hardware with new Boot software (autoupdate.bin) refer to the Installation Guide for CPDM3.

### 19.3 SOFTWARE INFORMATION

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

- 1 Click "Configuration" on the start page.
- 2 Select Software > Information in the menu on the Configuration page.  
The software name, versions, the date they were installed and also which version that currently is running are shown.

### 19.4 SWITCH SOFTWARE

If two software versions are installed on the CPDM3 you can switch between them. When switching to another software, the CPDM3 takes a backup of the current running software. That backup is used if you want to go back to the previously run software later on and keep the previous settings.

- 1 Click "Configuration" on the start page.
- 2 Select Software > Switch in the menu on the Configuration page.
- 3 Under Select settings, select one of the following:
  - Keep previous settings – uses the last configuration of the software you want to switch to. This option is only available if that software has been used before.
  - Copy Current settings – copies the configuration of the current software to the software you want to switch to. This option is only available if both software

are of the same type.

NOTE: If switching to an older software version of the same type, this option should not be selected because the configuration of the current software might not be compatible with the older software.

- Use factory default settings – restores to factory configuration in the software you want to switch to.

IMPORTANT: All configurations and files will be replaced by the ones made/installed in the factory, except the current network configuration.

- 4 Click "Switch".

## 19.5 INSTALL NEW SOFTWARE

It is recommended to always perform a backup before installing new software, see [19.5.1 Create a Software Backup](#). After the software installation see also [18.4 Update the User Interface after a new Release](#) on page 147.

Make sure that no Device Manager client is open and it is also important that no ftp client is logged in to the module.

The information stored in the database will not be overwritten when new software is installed. Files in the netpage folder in the ftp area that are new or changed are kept when updating.

NOTE: It is not recommended to use the module's Management port when installing software.

- 1 Click "Configuration" on the start page.
- 2 Select Software > Installation in the menu on the Configuration page.
- 3 Select software (.pkg) to upload. The software will replace the not running software.
- 4 Select "Switch immediately" if you want to run the new software.
- 5 Select "Copy current settings" if you want the new software to inherit the settings currently used. This selection will have no effect if the software type is different than the currently used software. The module will always start up using factory settings if the software type differs.
- 6 Click the "Start Installation" button.

### 19.5.1 CREATE A SOFTWARE BACKUP

The complete configuration of the current software on the module and the files on the FTP-area are included in the backup.

- 1 Click "Configuration" on the start page.
- 2 Select Software > Installation in the menu on the Configuration page.
- 3 Click the "Backup" button.

Note that the backup will contain configuration for the running software only.

## 20. TROUBLESHOOTING

### 20.1 GENERAL TROUBLESHOOTING

#### 20.1.1 LOG FILES

When troubleshooting it is always a good idea to examine the log files, since they provide additional information that may prove useful. The first log to examine is the Fault log found under Status on the Configuration page, but when reporting an error to your supplier more advanced logs might be needed. Always include the appropriate log file.

**To find Info log and Error log:**

- 4 Click "Configuration" on the start page.
- 5 Select Other Settings > Advanced Configuration in the menu on the Configuration page.
- 6 Click the "Troubleshoot" button on the Advanced Configuration page.
- 7 Click "View Info Log" or "View Error Log".

#### 20.1.2 THE MODULE DOES NOT START

To use the module's GUI, the computer must confirm to the requirements listed in [1.7 Requirements](#) on page 11. If you do not have the correct software versions installed, contact your system administrator.

#### 20.1.3 FIREWALL ISSUES, OR NO INDICATION OF CONNECTED DEVICE

If there is a firewall between the module and any devices, the firewall may need some configuration to allow communication. See [Appendix A. Used IP Ports](#) on page 161 for a description of used ports.

#### 20.1.4 UNABLE TO ACCESS FTP AREA

Make sure the client is set in active mode.

Example for Internet Explorer:

In the menu, select Tools -> Internet Options... -> Advanced. Under "Browsing", uncheck the "Use Passive FTP (for firewall and DSL modem compatibility)" check box.

When secure mode is enabled, see [3.4.1 Web Access Security Settings](#) on page 22, only secure access via HTTPS and FTPES is allowed. HTTP is automatically redirected to HTTPS and FTP access is not allowed. The FileZilla Client freeware (not included) supports FTPES.

## 20.2 NETPAGE TROUBLESHOOTING

| Fault  | Probable cause  | Action or comment  |
|--|---|--|
| <ul style="list-style-type: none"> <li>• My Groups and My Messages do not work.</li> </ul>   | <ul style="list-style-type: none"> <li>– Cookies are not allowed in your web browser.</li> </ul>  | <p>Check that cookies are enabled in your web browser.</p>   |
| <ul style="list-style-type: none"> <li>• Number list or Common Messages are unsatisfactorily updated</li> </ul>  | <ul style="list-style-type: none"> <li>---</li> </ul>   | <p>Refresh the cache memory on the web browser. If they still are unsatisfactory, refresh catching proxy (if any). In, for example Microsoft Internet Explorer, this can be achieved by pressing CTRL+F5.</p>  |
| <ul style="list-style-type: none"> <li>• Entire Message history including column headings doesn't appear</li> </ul>  | <ul style="list-style-type: none"> <li>– The Java Virtual Machine may be missing on your computer.</li> </ul>   | <p>Contact your IT department for assistance.</p>  |
| <ul style="list-style-type: none"> <li>• Message history is not running, although messages are sent and column headings are visible.</li> </ul>              | <ul style="list-style-type: none"> <li>– There might be a firewall preventing you from receiving data from the NetPage server.</li> </ul>   | <p>Contact your IT department to open port number 5891 in the fire wall, in the direction from the web client to the NetPage server.</p>   |
| <ul style="list-style-type: none"> <li>• Translation into language with character encoding UTF-8 is not displayed correctly in the NetPage's GUI.</li> </ul> | <ul style="list-style-type: none"> <li>– The software has been upgraded. The newer software has inherit the older software's settings (for example by using the "Copy current settings" option).</li> </ul> | <p>Open the html files used by Netpage (located on the FTP area) in WordPad or similar text editor.</p> <p>Change the character encoding in the files to this:</p> <pre>&lt;meta http equiv= "Content-Type" content="text/html; charset=utf-8"&gt;</pre> |

## 20.3 TROUBLESHOOTING GUIDE

This section lists a number of possible faults, probable causes and suggested actions.

### 20.3.1 TROUBLESHOOTING FOR THE DEVICE MANAGER

| Fault   | Probable cause  | Action or comment   |
|---|---|---|
| <ul style="list-style-type: none"> <li>It is not possible to edit any parameters after logging on to the system.</li> </ul> | The user is logged on as auditor.   | Close the browser session and re-log on as admin or sysadmin.   |
| <ul style="list-style-type: none"> <li>The system does not have the correct time.</li> </ul>                                | <ul style="list-style-type: none"> <li>Configuration error, no time server configured.</li> <li>The time server is configured but is offline.</li> <li>The web browser is selected as time source but the time has not been set by the user.</li> </ul> | <p>Configure the system to connect to a time server.</p> <p>Restore connection to time server.</p> <p>Set the time via the advanced configuration.</p>  |
| Device does not show up in the Device Manager   | -The connected interface (for example DECT) is not up and running   | <p>Check the status of the interface. Starting up mode is indicated during start of applications. If an application has lost connection to a required resource it is indicated as application problem mode. An Application problem is always shown as a persistent fault in the Status log (see <a href="#">9.2 Logging</a> on page 104).</p> <p>NOTE: If the information on the Configuration page shows Normal mode, it is not necessary to check the System information.</p> <ol style="list-style-type: none"> <li>Click "Configuration" on the start page.</li> <li>Select Other Settings &gt; Advanced Configuration in the menu on the Configuration page.</li> <li>Click "Troubleshoot" button on the Advanced Configuration page.</li> <li>Select "System information" in the menu.</li> </ol> |



| Fault   | Probable cause   | Action or comment   |
|---|--|---|
| <ul style="list-style-type: none"> <li>An advanced charger does not come online in the Device Manager in a system with "Service discovery" enabled.</li> </ul>                                | <ul style="list-style-type: none"> <li>The charger parameters for Service Discovery are not set.</li> </ul>  | Use PDM to set the parameter in the charger and in the Device Manager so that they match.   |
|   | <ul style="list-style-type: none"> <li>The service discovery parameter "Domain Name" is not unique in the IP network domain.</li> </ul>  | Use PDM to reconfigure the advanced charger. Make sure that there is only one Device Manager with the used "Domain Name".   |
|   | <ul style="list-style-type: none"> <li>The advanced charger and the Device Manager are located in two separate IP networks that prevents the service discovery request.</li> </ul>   | Use PDM to disable service discovery in the advanced charger and to set the IP Address to the Device Manager.   |
| <ul style="list-style-type: none"> <li>The charger logs out immediately after login and does not come online again. The charger is configured in another Device Manager or in PDM.</li> </ul> | The charger is already saved in the Device Manager that the administrator wants it to use. The Advanced Charger parameter in the desired Device Manager is pointing to another Device Manager (service discovery or IP address) which causes the charger to log out and connect to another Device Manager after completed synchronisation. | <ul style="list-style-type: none"> <li>Before connecting the advanced charger to the LAN, make sure that if the advanced charger is saved in the desired Device Manager it has parameters that points to the correct Device Manager.</li> <li>Delete the saved charger from the Device Manager before connecting the charger to the LAN.</li> </ul> |
| <ul style="list-style-type: none"> <li>Some devices report device busy in the Device Manager when the user is trying to change device parameters.</li> </ul>                                  | The device is occupied with some action that the device cannot combine with parameter synchronisation.   | No action needed. The Device Manager will synchronize the changes when possible.  |
| <ul style="list-style-type: none"> <li>Software download is stuck in pending.</li> </ul>  | <ul style="list-style-type: none"> <li>The device is not online. Software download will start when device gets online.</li> </ul>  | Connect the handset to the Device Manager either via a advanced charger or via a DECT system supporting OTA.  |
|   | <ul style="list-style-type: none"> <li>Multiple devices are currently being updated.</li> </ul>  | There is a limitation in the Device Manager on the number of simultaneous software downloads. All devices are placed in a queue and will be upgraded in time. No action needed. Download will start in time.  |

| Fault   | Probable cause  | Action or comment  |
|---|---|--|
| • File downloads retrying.  | The device is currently unavailable (device out of range, network problem)  | No action needed. The download will start when the device comes in range again.  |
| • Software downloads rejected.                                      | The device is already updated with a new software but not yet restarted on the new software. This is due to selected activation time in previous software update i.e. "When idle in charger" or "After manual restart". | Restart the device manually and restart the download.  |
| Software in Device Not Recognized/<br>Synchronization Fails         | The parameter definition file is not compatible with the device.  | In the Devices tab, check the parameter version for the device. If the parameter version is highlighted with red, a package file (.pkg) including the software file and definition file with that parameter version, must be imported to the module. |
| • Software downloads are aborted.                                   | Wrong file selected for download to devices (External web server).  | – Make sure that the URL to the desired software is correct and retry.<br><br>– Make sure that the file is intended for that device.   |
| • Low software download performance to handset inserted in charger. | The charger is not connected to the Device Manager (not online in the Device Manager). The handset is online only via OTA.  | Configure the advanced charger so that it connects and logs on to the correct Device Manager.  |
| • Communication failure to device.                                  | The device did not respond in an expected way. The reason could be temporary communication problems caused by coverage problems or network problems.  | Repeat the action after a while to see if it is possible to communicate with the device.   |

| Fault  | Probable cause  | Action or comment   |
|--|---|---|
| <ul style="list-style-type: none"> <li>• No connection available for the Device Manager GUI.</li> </ul>  | – Max number of Device Manager GUI's has been reached.                                      | Close the other Device Manager GUI to open new. A maximum of three Device Manager GUIs can be connected.                              |
|  | – The Device Manager server side is restarted due to reconfiguration.                       | No Action, the server will be up within a few minutes.  |
|  | – The Device Manager is temporarily unavailable due to restore of database.                 | No Action, the server will be up soon.  |
|  | – The network is preventing the GUI from connecting to the server.                          | No action.  |
| <ul style="list-style-type: none"> <li>• All devices log out after restore of a backup.</li> </ul>   | The backup is older than the devices' "Device relogin time".                                | No action. All devices will re-login within "device relogin time" (see device handling).  |
| <ul style="list-style-type: none"> <li>• The parameter version is displayed in bright red in the Device Manager GUI.</li> </ul>  | There are no compatible .pkg files imported to the system.                                  | Import a .pkg file suitable for the device. The .pkg file is provided by the supplier.  |
| <ul style="list-style-type: none"> <li>• The parameter version is displayed in dark red in the Device Manager GUI.</li> </ul>  | The version of the imported .pkg files are not 100% compatible with the device.             | Import a .pkg file suitable for the device. The .pkg file is provided by the supplier.  |
| <ul style="list-style-type: none"> <li>• The parameter version of the Number in the Numbers tab is higher than in the parameter version of the device in the Devices tab.</li> </ul> | The device has been downgraded to a previous software version with lower parameter version. | No action needed. This is not an error. The parameter version will be the same after a software upgrade has been performed on device. |
| <ul style="list-style-type: none"> <li>• No numbers are visible of the selected device type in the Number tab.</li> </ul>  | The search field is red. Current search returns no hit.                                     | Alter search or use "show all" to reset search to default.  |
| <ul style="list-style-type: none"> <li>• "Go to device" is dimmed out for a device in the device view.</li> </ul>  | The selected device has no number associated to it.   | – Assign a new number to the device.  |
|  |   | – Associate a new or existing number to the current device  |
| <ul style="list-style-type: none"> <li>• The handset is not visible in the Number tab.</li> </ul>  | – The handset has no number associated.   | Assign or associate a number to the device.   |
|  | – The device is offline and not saved as number.  | Bring the device online. Save the number in order to make it possible to edit the number when it is offline.                          |

| Fault   | Probable cause   | Action or comment   |
|---|--|---|
| <ul style="list-style-type: none"> <li>• Number creation of desired device type is not possible.</li> <li>• It is not possible to apply a template at creation of new number.</li> <li>• A handset logs out when placed in an advanced charger</li> </ul> | <p>The .pkg file for the desired device type is not imported to the Device Manager.</p> <p>No compatible template for the desired device exists.</p> <p>The device manager configurations in the IPBS and the advanced charger are not the same.</p> | <p>Import the .pkg file for the desired device type. The file is provided by the supplier.</p> <p>Create a new template or upgrade an existing template and retry.</p> <p>Delete the saved instance of the advanced charger in the Device Manager. Use PDM to reconfigure the advanced charger so that it will log on to the correct device manager. Connect the advanced charger to the LAN.</p> |
| <ul style="list-style-type: none"> <li>• The handset does not log on to the device manager OTA.</li> </ul>  | <p>– The Domain ID is not set correctly in the IPBS.</p> <p>– The system does not support service discovery.</p>   | <p>Reconfigure it to match the device manager Service Discovery parameter Domain ID.</p> <p>Erase the Domain ID in the IPBS and set the IP address to the Device Manager under Advanced Settings &gt; Device Management.</p>  |
| <p>Fault message Device Manager: Running-application problem (Error relay: Database init in progress) is shown after software upgrade of the CPDM3.</p>   | <p>You have upgraded the CPDM3 with a software that uses another database structure for the Device Manager than the previous installed software version.</p>   | <p>The CPDM3 needs to re-configure the database used by the Device Manager after the upgrade.</p> <p>The time it takes to re-configure the database depends on number of parameters, devices, phonebook entries, and numbers saved in the database.</p> <p>It can take up to several hours.</p>   |

### 20.3.2 GENERAL TROUBLESHOOTING FOR THE CPDM3

This part of the Troubleshooting Guide lists possible faults that are not connected to the Device Manager

| Fault  | Probable cause   | Action or comment   |
|--|--|---|
| • It is not possible to edit the Central Phonebook.  | – The phonebook is configured to be read-only.                   | Edit the external phonebook file and re-import it to the Central Phonebook.   |
|  | – The phonebook is configured to use a LDAP server               | Access the LDAP server and alter the desired entry. After “commit”, the new data will be available for the Central Phonebook. |
| • Import of language to the configuration GUI fails.   | The language file has the wrong format.                          | Export the default language to set the format and edit the language file.   |
| • Set language fails.  | – The language file might be faulty.                             | Export the language files and compare them. Make sure that the <language id= tag is unique for each file.                     |
| • The log files are flooded with log entries.  | The log settings are set to a detailed level.                    | Change the log settings in Advanced configuration > Troubleshoot > System information.  |
| • Several functions of the system does not start.  | – There is not a valid license.                                  | Enter a valid license and restart the module.   |
| • Some IP-DECT Base Stations have no contact with the Unite module system after a migration from a multiple system to a single CPDM3 system. | – The IP address to CPDM3 has not been set in all base stations. | Enter the correct CPDM3 IP address in the base stations.  |

## 20.4 BUILT-IN TOOLS

The hardware has different LEDs to indicate the status and besides that the possibility to show active faults and logging the faults via the GUI. Flashing patterns

| Tools | Description  |
|-------|--|
| LEDs  | The LEDs show different colors to determine type of information and have different flashing frequency for showing the priority |



#### colors

|        |                       |
|--------|-----------------------|
| Red    | Fault indication      |
| Yellow | Mode indication       |
| Blue   | Normal operation (OK) |

#### Flashing frequency

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

| Status LED                                    |        |  |          |
|---|--------|--|----------|
| Status OK                                     | Blue   |  |          |
| Starting up/shutting down                     | Blue   |  |          |
| Feedback (1 sec.)                             | Blue   |  |          |
| Error/fault                                   | Red    |  |          |
| Warning                                       | Red    |  |          |
| Boot mode                                     | Yellow |  | Mode LED |
| Demonstration mode                            | Yellow |  | Blue     |
| Active module during synchronization          | Red    |  |          |
| Active module synchronized                    | Blue   |  | Blue     |
| Standby module during synchronization         | Yellow |  | Blue     |
| Standby module synchronized                   |        |  | Blue     |
| Waiting for automatic startup (1 min.)        | Yellow |  |          |
| Troubleshoot mode and during firmware upgrade | Yellow |  |          |
| Mass storage mode                             |        |  | Blue     |

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

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

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

#### Demonstration Mode:

Demonstration Mode is activated by pressing the Mode button for 10 seconds. The module will then run with full functionality for 2 hours, it then returns to the configured license! If it works in Demonstration Mode and not in normal operation you probably have a license problem.

#### Active faults:

Refer to [4.6.1 Active Faults](#) on page 39.

#### Fault logging:

Refer to [4.6.4 Fault Log](#) on page 41 and [4.6.5 Administer the Fault Log](#) on page 42.

#### System Information:

See [20.5 Advanced Troubleshooting](#) below.

## 20.5 ADVANCED TROUBLESHOOTING

The Advanced Configuration page (requires system administrator rights) includes advanced troubleshooting. Snapshots of selected logs or a complete log can be viewed.

- 1 Click "Configuration" on the start page.
- 2 Select Other Settings > Advanced Configuration in the menu on the Configuration page.
- 3 Click the "Troubleshoot" button on the Advanced Configuration page.
- 4 In the left menu on the Troubleshoot page you can view logs and find detailed information about the system.

- Specify Information to Log

Standard debug is set by default but this can be extended and show more details.

- 1 Click "System Information" in the left menu.
- 2 Enable desired logs and click "Activate".

- Send Test Message

The Troubleshoot page also includes the possibility to send test messages.

- 1 Click "Send Test Message" in the left menu.
- 2 Enter Call ID and click "Send Message".

## 20.6 WHAT TO CONSIDER WHEN REPLACING A MODULE

- IP Address
- License
- Module key
- Remember where cables were connected

## 20.7 TECHNICAL SUPPORT

For technical support please contact your local representative.

## 21. RELATED DOCUMENTS

|  |                    |
|--|--------------------|
| Installation and operation manual, WinPDM          | 12/1531-ANF 901 43 |
| DT4x3 Configuration Manual                         | 27/1531-ANF 901 43 |
| DT390 and DT690 Configuration Manual               | 23/1531-ANF901 43  |
| Rack PDM Charger Installation and Operation Manual | 21/1531-ANF 901 43 |
| Battery Pack Rack Charger Installation Guide       | 22/1531-ANF 901 43 |
| T941OM Output Module, Installation Guide           | 55/1531-ANF 901 43 |
| T941AM8 Alarm Module, Installation Guide           | 58/1531-ANF 901 43 |
| T941AM32 Alarm Module, Installation Guide          | 59/1531-ANF 901 43 |
| T930PS1 Power Module, Description                  | 60/1551-ANF 901 43 |
| ESPA 4.4.4, Description                            | 56/1551-ANF 901 43 |
| Serial Data Interface S942SI, Protocol             | 53/1551-ANF 901 43 |
| Telocator Alphanumeric Protocol, TAP               | 57/1551-ANF 901 43 |
| Function Description, Open Access Protocol (OAP)   | 52/1551-ANF 901 43 |
| Mitel 5613 Configuration Manual                    | LZT103080          |
| Mitel 5614 Configuration Manual                    | LZT103081          |



## Appendix A. Used IP Ports

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

NOTE: If a firewall is used, the well-known port (fixed) must be available for communication in the network.

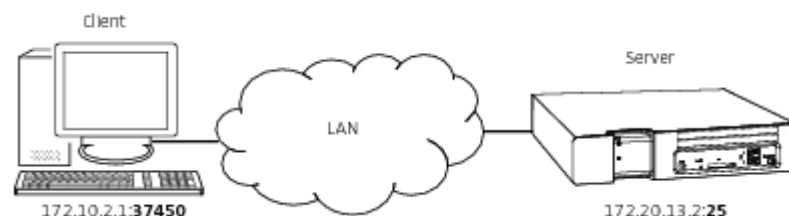
The table below describes the well-known port used by the application/unit acting as server.

### Example 1:

In this example the FTP area on the CPDM3 should be accessed. An FTP client installed on a computer is used to access the FTP area. In this case, the CPDM3 acting as a server and the computer acting as a client.

Port 21 is a well-known one for FTP requests and port 37450 is a temporary one assigned to the client.

Figure 36. CPDM3 acting as a server



### Example 2:

In this example, the CPDM3 should obtain time and date from an external source acting as a NTP server. In this case, the CPDM3 is acting as a client since it initiates the connection to the NTP server.

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

Figure 37. CPDM3 acting as a client

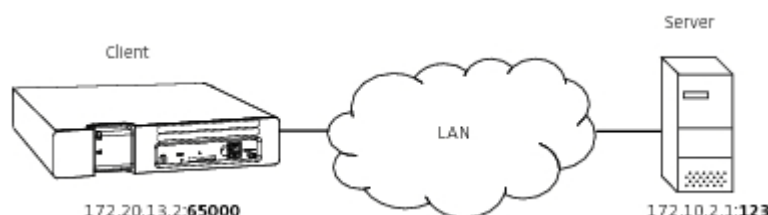


Table 3. IP ports used by applications/units acting as server

| Port        | Application or unit          | Transport protocol |
|-------------|------------------------------|--------------------|
| 20–21       | FTP                          | TCP                |
| 53          | Domain Name Server (DNS)     | UDP                |
| 68          | DHCP                         | UDP                |
| 80          | Web traffic (HTTP)           | TCP                |
| 113         | Authentication               | TCP                |
| 123         | Network Time Protocol (NTP)  | UDP                |
| 443         | HTTPS                        | TCP                |
| 514         | Syslog<br>Syslog messages    | UDP                |
| 1321–1322   | OAP Server                   | TCP                |
| 1814–1817   | MX-ONE/IP-DECT               | TCP                |
| 3217        | Unite traffic                | UDP                |
| 5891        | NetPage                      | TCP                |
| 8080        | HTTP                         | TCP                |
| 10147       | DECT Charger Communication   | TCP                |
| 10153       | Device Manager Communication | TCP                |
| 33000–33001 | VoWiFi handset Communication | TCP                |

## Appendix B. RS232 Connections

### B.1 Cables for the ESPA-, the Ascom Line- and the TAP protocol

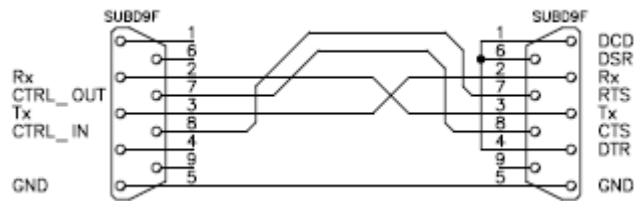
Figure 38.



Connection to external equipment

A cable with RS232 and D-SUB connectors is required to be able to receive pagings from external equipment. By default the cable shall be connected to the COM2 port on CPDM3 for ESPA in, Ascom Line protocol and TAP in and also for ESPA out and TAP out.

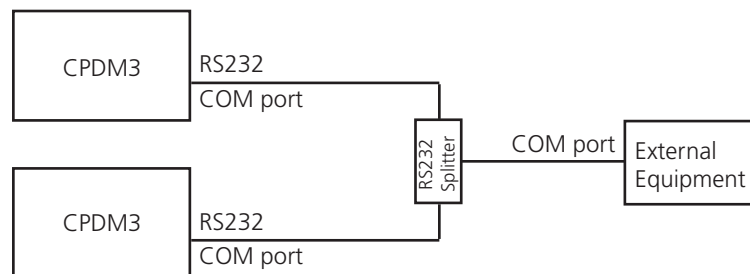
Figure 39.



Cable wiring for the ESPA -, the Ascom Line- and the TAP protocol

### B.2 R232 Cable Connections in a Redundancy System

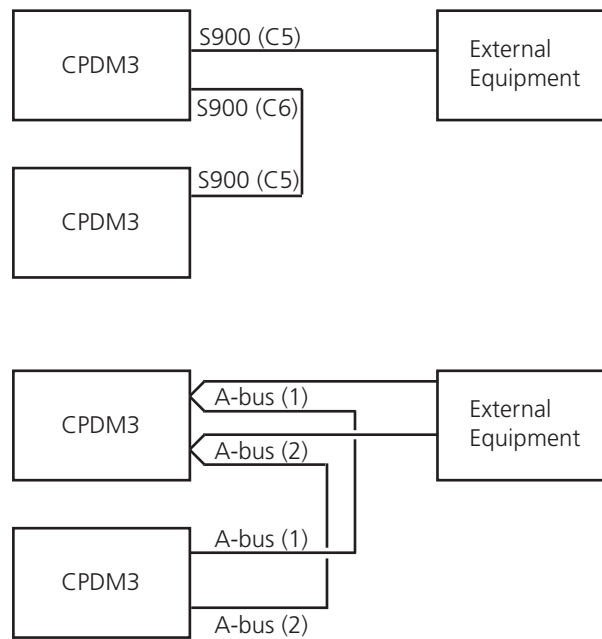
In a redundancy system, having equipment connected via serial interface, must the R232 cable be attached to both the primary CPDM3 and the secondary CPDM3. By using a RS232 data splitter the cable can be branched to both modules.



## Appendix C. System 900 Connections

The external equipment can be connected to the A-bus in two different ways depending on the connector used.

### C.1 System 900/A-bus Connections in a Redundancy System



## Appendix D. Alarm Action Configuration Examples

This appendix presents examples on how alarm actions can be configured.

### D.1 System Setup for Examples

In this section, first the included system components are presented, then which inputs and outputs that need to be setup.

#### D.1.1 System Components

##### One Alarm Module

4 inputs have been defined in the Input/Output Setup.

- Cold-storage, door open
- Cold-storage, door still open
- Cold-storage, door open very long
- Cold-storage, door closed

##### One CPDM3

2 outputs have been defined in the Input/Output Setup.

- Cold-storage lamp
- Siren

##### 4 handsets with push-button alarms

Handset numbers: 1440, 1441, 1442, and 1443.

##### Input/Output Setup

In these examples, the outputs and inputs are set according to the following figure.

Figure 40. I/O setup.

#### I/O Setup

##### Outputs

| ID | Output Name       | Module Address | Output   | Inactive/Initial State |  |
|----|-------------------|----------------|----------|------------------------|--|
| 1  | Internal Output 1 | 127.0.0.1      | Internal | 1                      | High (open-collector) <input type="button" value="Reset"/> |
| 2  | Internal Output 2 | 127.0.0.1      | Internal | 2                      | High (open-collector) <input type="button" value="Reset"/> |

##### Inputs

| ID | Input Name                 | Module Address | Input    | Activation | Activation Time |                                      |
|----|----------------------------|----------------|----------|------------|-----------------|--------------------------------------|
| 1  | Internal Input 1           | 127.0.0.1      | Internal | 1          | On Opening      |                                      |
| 2  | Internal Input 2           | 127.0.0.1      | Internal | 2          | On Opening      |                                      |
| 3  | Cold storage, door open    | 127.0.0.1      | 02       | 1          | On Opening      | 120 <input type="button" value="X"/> |
| 6  | Cold storage, door still c | 127.0.0.1      | 02       | 1          | On Opening      | 600 <input type="button" value="X"/> |
| 7  | Cold storage, door open    | 127.0.0.1      | 02       | 1          | On Opening      | 900 <input type="button" value="X"/> |
| 8  | Cold storage, door close   | 127.0.0.1      | 02       | 1          | On Closing      | <input type="button" value="X"/>     |

D.2 Example 1: Alarm from Handset

A push-button alarm (double press) is received from 1440. A message is sent to the other handsets and a siren starts to sound. The alarm is cancelled by sending the data 1440 and then the siren stops.

Two alarm actions are created. One that handles the push-button alarm called “Push-button alarm from 1440” and one that handles the cancellation called “Alarm cancellation”.

Push-button alarm from 1440

Select Alarm handling, Alarm Actions and set Alarm Trigger “Push-button double press (Push-button alarm 1 and 2)”

Figure 41. Alarm trigger setup.

Alarm Action

Name

Notes

Triggers

Select trigger type and click "Add". Several triggers of the same type can be added.

Alarm Trigger

| Alarm Type               | Number |
|--------------------------|--------|
| Push-button double press | 1440   |

Add

Activate Actions

Activate which actions to be activated when an alarm is received. Two different actions are setup, a siren and messages sent to other handsets.

Figure 42. Activate Output Action and Send Message Actions.

Actions

Select type of action and click "Add". Several actions can be added.

Message action

Add

Activate Output

| Output | Duration (s) |
|--------|--------------|
| Siren  | 3600         |

Send Message

| Call ID | Message Text        | Beep Code | Priority |
|---------|---------------------|-----------|----------|
| 1441    | Alarm from [callId] | 2 beeps   | Normal   |
| 1442    | Alarm from [callId] | 2 beeps   | Normal   |
| 1443    | Alarm from [callId] | 2 beeps   | Normal   |

Save

Cancel

For Output Action Siren, the value is set to max value 3600.

### Alarm cancellation

For handset 1440, Alarm cancellation is setup with a Data Trigger with an Alarm with duration of 1 second.

Figure 43. Activating an Action for Alarm Cancellation.

**Alarm Action**

**Name**

Alarm cancellation

**Notes**

**Triggers**

Select trigger type and click "Add". Several triggers of the same type can be added.

**Data Trigger**

| Data | Number |
|------|--------|
| 1440 | 1      |

Add

**Actions**

Select type of action and click "Add". Several actions can be added.

Message action Add

**Activate Output**

| Output | Duration (s) |
|--------|--------------|
| Siren  | 1            |

Save Cancel

It does not matter which handset that sends the data so the trigger is general when it comes to handset numbers.

The output is set to the initial state again (after 1 second).

## D.3 Example 2: Alarm from Cold-storage Room

When the door to one of the cold-storage rooms is opened, the input from Cold-storage room is activated. If the door is open longer than 2 minutes a message is sent and a lamp above the door is lit.

If the door still is open after 10 minutes another message is sent. After 15 minutes another message is sent and the siren starts to sound. When the door is closed the siren and lamp are turned off.

Three alarm actions are created. One that handles the alarm called "Cold-storage room open", one called "Cold-storage room open very long" and one called "Cold-storage room closed".

When the door to one of the cold-storage rooms is opened, the input from Cold-storage room is activated. If the door is open longer than 120 seconds, a message is sent and a lamp above the door is lit.

**Cold-storage room 1, door open**

Input Triggers: “Cold-storage door open” and “Cold-storage door still open”

When the door has been open for 2 minutes (120 seconds), the action is started. The action shall not be repeated so the “Repetition time” is not stated, and the value in the “Max. No. of Repetitions” field has no meaning.

When the door has been open for 10 minutes (600 seconds), another message is sent as a reminder. A separate Alarm Action is required if a different beep-code is desired.

**Actions Activate Output Action and Send Message Actions**

Figure 44. Alarm Action, Cold-storage room open.

**Alarm Action**

Name  
Cold-storage room open

Notes

Triggers

Select trigger type and click "Add". Several triggers of the same type can be added.

| Input                         | Repetition Time (s) | Max No. of Repetitions |
|-------------------------------|---------------------|------------------------|
| Cold-storage, door open       | 60                  | 0                      |
| Cold-storage, door still open | 60                  | 0                      |

Actions

Select type of action and click "Add". Several actions can be added.

Output action

Activate Output

| Output            | Duration (s) |
|-------------------|--------------|
| Cold-storage lamp | 3600         |

Send Message

| Call ID | Message Text  | Beep Code | Priority |
|---------|---------------|-----------|----------|
| 1440    | {inputDevice} | 2 beeps   | Normal   |

Save Cancel

For Activate Output Action, the duration is here set to max value 3600.

**Cold-storage room 1, door open very long**

The Input Trigger “Cold-storage room, door open very long” is used.



Figure 45. Cold-storage room 1, door open very long.

Alarm Action

Name

Cold-storage room, door open very long

Notes

Triggers

Select trigger type and click "Add". Several triggers of the same type can be added.

Input Trigger

| Input                            | Repetition Time (s) | Max No. of Repetitions |
|----------------------------------|---------------------|------------------------|
| Cold-storage door open very long | 60                  | 0                      |

Add

Actions

Select type of action and click "Add". Several actions can be added.

Message action

Add

Activate Output

| Output | Duration (s) |
|--------|--------------|
| Siren  | 3600         |

Send Message

| Call ID | Message Text   | Beep Code | Priority |
|---------|----------------|-----------|----------|
| 1440    | [input device] | 10 beeps  | High     |
| 1441    | [input device] | 4 beeps   | Normal   |
| 1442    | [input device] | 4 beeps   | Normal   |
| 1443    | [input device] | 4 beeps   | Normal   |

Save Cancel

When the door has been open for 15 minutes (900 seconds), the message is sent to all Portable Devices and the siren starts to sound.

The duration is set to max value 3600 and will sound until expired or another action is started with shorter expire time, for example “Cold-storage room closed”.

Cold-storage room door closed

Figure 46. Cold-storage room door closed.

Alarm Action

Name

Cold-storage room closed

Notes

Triggers

Select trigger type and click "Add". Several triggers of the same type can be added.

Input Trigger

| Input                     | Repetition Time (s) | Max No. of Repetitions |
|---------------------------|---------------------|------------------------|
| Cold-storage, door closed | 60                  | 0                      |

Add

Actions

Select type of action and click "Add". Several actions can be added.

Output action

Add

Activate Output

| Output            | Duration (s) |
|-------------------|--------------|
| Siren             | 1            |
| Cold-storage lamp | 1            |

SaveCancel

For Input Trigger “Cold-storage, door closed”: When the door closes the actions are started. The output is set to the initial state again (after 1 second).

Summary of alarm actions

This figure shows a list of the Alarm Action setup in the examples.

Figure 47. Summary of Alarm Actions

Alarm Actions

Number of triggers: 6 (250)

| Name                             | Notes | Triggers   |  |   |
|----------------------------------|-------|--|--|---|
| Push-button Alarm from 1440      |       | Alarm Type: Push-button double press, Number: 1440 |  | ✗ |
| Alarm cancellation               |       | Data: 1440   |  | ✗ |
| Cold-storage room closed         |       | Input: Cold-storage, door closed                   |  | ✗ |
| Cold-storage room open very long |       | Input: Cold-storage, door open very long           |  | ✗ |
| Cold-storage room open           |       | Input: Cold-storage, door open                     |  | ✗ |
|                                  |       | Input: Cold-storage, door still open               |  | ✗ |

Add

## Appendix E. Protocol Limitations

This appendix describes a number of protocol specific limitations. The serial interface included in the module is a successor to the system 900 module S942SI Serial Interface and the supported protocols are described in the Protocol, Serial Data Interface S942SI document. To be able to fully understand the limitations it is recommended to have this document available.

### E.1 ESPA 4.4.4

The implementation only supports point-to-point connection. Dial-up connection or multiprop connection are not supported.

#### E.1.1 Functionality

The protocol consists of **blocks** which consist of **records** which consist of **data**.

#### E.1.2 Limitations

##### Protocol Blocks

The original ESPA 4.4.4 specification has 4 different blocks and an additional 5'th block for equipment manufacturer specified functionality. The 5'th block is not used by Ascom and Ericsson paging dialect, instead two additional blocks 7 and 9 are specified for the dialects.

|   |   |
|---|---|
| Request for license<br>(Block 7, Ascom and Ericsson paging dialect):    | This block is not supported. The block is NAK:ed if received. |
| Request for module key number<br>(Block 9, Ascom and Ericsson dialect): | This block is not supported. The block is NAK:ed if received. |

#### E.1.3 Protocol Records

|   |  |
|---|--|
| Call type: Speech call (Record 4.2):  | Speech paging is not supported. This record is handled as a standard paging (Record 4.3)                     |
| Call type: Remote ack of old paging in mobile unit (Record 4.5, Ascom dialect): | This record not supported and is NAK:ed.   |
| Call type: Erase of old paging (Record 4.6, Ascom dialect):                     | If neither "ID" (Record 9) or "Running Number" (Record D) is included in the message, the message is NAK:ed. |
| Call type: Cordless phone, undefined type (Record 4.7, Ascom dialect):          | Sent as standard paging (Record 4.3).  |
| Call type: Cordless phone, internal type (Record 4.8, Ascom dialect):           | Sent as standard paging (Record 4.3).  |
| Call type: Cordless phone, external type (Record 4.9, Ascom dialect):           | Sent as standard paging (Record 4.3).  |

|  |   |
|--|---|
| Number of transmissions<br>(Record 5, standard ESPA):  | This record is accepted but ignored since it is not applicable in DECT or VoWiFi systems. |
| Mailbox number<br>(Record A, Ericsson paging dialect): | This record is accepted but ignored.  |
| Infopage<br>(Record C, Ascom dialect):                 | This record is accepted but ignored.  |

#### E.1.4 Advanced parameters

|                          |  |
|--------------------------|--|
| Bleep each transmission: | Not applicable.  |
| Flow control XON/XOFF:   | Not supported since there are some issues with the control characters. If the block check character becomes any of the two control characters XON or XOFF, the flow control fails, therefore we decided to not support this. |

### E.2 Ascom Line Protocol

#### E.2.1 Functionality

A line protocol message consists of the following records and separators:

<Addr/Message/Beepcode/PagFunc/NoOfTransm/Prio/Infopage>

All characters are writeable by hand using an ordinary terminal program such as hyper terminal etc. Not all records needs to be given, for instance <> is a valid message that delivers default message to default paging address.

#### E.2.2 Limitations

The following limitations apply:

|             |   |
|-------------|---|
| PagFunc:    | The Line protocol only supports call type 3 (plain paging) and 4 (alarm). All others are handled as plain paging. |
| NoOfTransm: | Not applicable.   |
| InfoPage:   | Not applicable.   |

### E.3 TAP Protocol

#### E.3.1 Functionality

- <ESC>PG1<CR> Default logon string
- First field of the TAP transaction block is assumed to contain the paging address. The address is treated as a decimal address, valid digits is 0-9. Any leading spaces will be ignored.
- Field(s) after the first field is assumed to contain the paging text. If the TAP transaction block is containing more than 2 fields, fields 3,4,5.. will be concatenated to the paging text to be sent. (the separating <CR>:s will be treated as a part of the paging text. The paging text is set as 'Body' in the Unite paging. The 'Subject' will be empty.

- There is no restriction on how many blocks that can be sent during one logon session.

### E.3.2 Limitations

The following limitations apply:

|  |   |
|--|---|
| Using <US> or <ETB> as block terminators:                              | Not supported.  |
| Sending <SUB> as control character:                                    | Not supported.  |
| Maximum session timeout:   | Not implemented, however an inactivity timeout will occur after 8 seconds when waiting for logon string and 4 seconds when waiting for block data after a <STX> has been received. After 3 successive timeouts, an automatic disconnect sequence will be initiated. These values can be changed through parameters. |
| Timeout between blocks:  | There will be no timeout between blocks.<br>After a logon has been received and after each paging block, the Serial Interface is put into sleep mode. Three actions can wake it up: A logoff request, a new logon request or a new paging block.  |
| Messages longer than 128 characters:                                   | Will be accepted but truncated.   |
| Message sequences:   | Not used by the Serial Interface.   |
| Software flow control of the serial port:                              | Not supported.  |
| Characters in the paging text below 0x20 (except for carriage return): | Will be converted to something above 0x7F (by adding the 8'th bit).   |

## Appendix F. Device Manager Keyboard Shortcuts

The following table shows the shortcuts that can be used in the Device Manager.

### F.1 General

| Short-cut  | Description                     |
|------------|---------------------------------|
| Ctrl + H   | Open the File management window |
| Ctrl + Tab | Switch tab                      |
| Alt + F4   | Close the application           |

### F.2 Devices

| Shortcut     | Description  |
|--------------|--|
| Ctrl + N     | Add a new device                                   |
| Enter        | Upgrade the selected device(s)                     |
| Delete       | Delete the selected device(s)                      |
| Ctrl + F     | Find a device                                      |
| Ctrl + Enter | Open the Properties window for the selected device |

### F.3 Numbers

| Shortcut | Description                                  |
|----------|--|
| Ctrl + N | Add a new Number                             |
| Enter    | Edit the selected Number                     |
| Ctrl + C | Copy the selected Number                     |
| F2       | Rename the selected Number                   |
| Ctrl + S | Save the selected Number to the database     |
| Delete   | Delete the selected Number from the database |
| Ctrl + F | Find a Number                                |

### F.4 Templates

| Shortcut | Description                  |
|----------|------------------------------|
| Ctrl + N | Add a new template           |
| Enter    | Edit the selected template   |
| Ctrl + C | Copy the selected template   |
| F2       | Rename the selected template |
| Delete   | Delete the selected template |
| Ctrl + F | Find a template              |

## Appendix G. File types

In this appendix, the different file extensions that are used in the module are explained. System files are not described.

| File type                 | Extension   | Description   |
|---------------------------|-------------|---|
| Software file             | bin         | Software for devices  |
| Company Phonebook file    | cpb         | Company Phonebook file for handsets.  |
| Parameter Definition file | def         | Including all possible settings for a certain device type for a certain version.  |
| Language file             | lng, or xml | Language file for handsets or the CPDM3. Language file for the module uses XML (eXtensible Markup Language.).                             |
| Package file              | pkg         | Archive that can include different file types such as parameter definition files (.def), software files (.bin) and template files (.tpl). |
| Template file             | tpl         | Contains one or more exported templates.  |
| Number file               | xcp         | Exported Numbers.   |

## Appendix H. Multiple CPDM3 Configuration Examples

This chapter presents configuration examples for multiple modules.

### H.1 More than 1000 devices

Up to 1000 devices can be configured on each CPDM3 module. If more than 1000 devices shall be configured, one possible solution is to use two modules and to register all handsets on one module and the chargers on another module

NOTE: All WiFi412 handsets must be configured to use a specific CPDM3. Therefore, during reconfiguration of the system, the VoWiFi handsets must be assigned to a corresponding CPDM3 using the PDM Windows Version.

### H.2 High messaging load in DECT

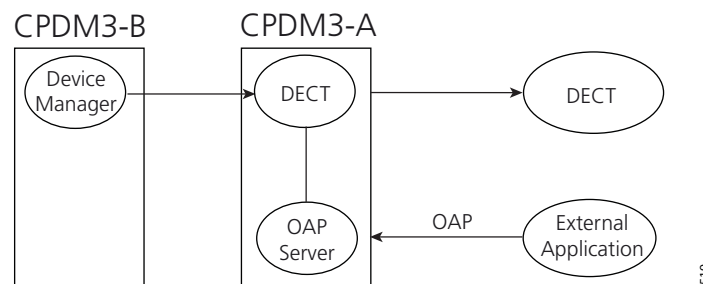
This solution applies to:

- systems with high messaging load
- systems with high requirements on maximum message burst throughput

When the messaging load is too high, a single CPDM3 cannot handle both messaging and device management effectively. Typically, this occurs when the messaging load is more than 4 000 messages per hour (or an equivalent amount of central phonebook enquires).

A solution to this situation can be achieved by running the messaging on one module and to handle Device Management on another module, see figure below.

Figure 48.



Example of paging in a multiple solution with OAP and DECT.

#### H.2.1 Configuration for the setup

The basic configuration for this setup is described below.

- CPDM3-A  
Disable Device Management in Configuration > Other Settings > Advanced Configuration > Device Management:
  - Remove IP addresses.
  - Click "Activate".

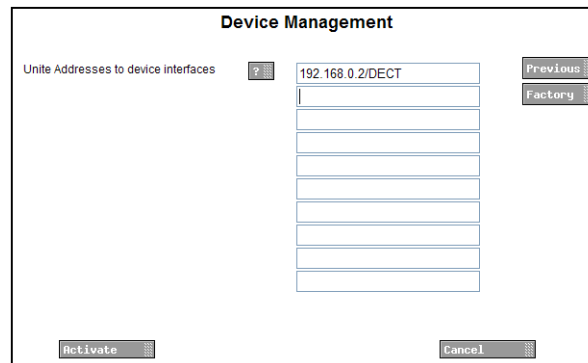


- CPDM3-B  
Disable the DECT interface in Configuration > Other Settings > Advanced Configuration > General Settings > View advanced parameters:
  - Set "DECT Interface" to Disabled.

Enable Device Management for the DECT system in Configuration > Other Settings > Advanced Configuration > Device Management:

- Replace the address "127.0.0.1/DECT" with the IP address of CPDM3-A plus "/DECT", that is, if CPDM3-A has the IP address 192.168.0.2, change to "192.168.0.2/DECT".
- Click "Activate".  
See figure below.

Figure 49.



Device Management enabled for the DECT system in CPDM3-B

## H.2.2 Migration example to a double CPDM3 solution

This example assumes that the original system uses one CPDM3module. Basically, the system setup is the same, but the original system with a single module has to be configured for a higher level of messaging traffic.

Change the following settings in the originalmodule:

- CPDM3-A  
Disable Device Management in Configuration > Other Settings > Advanced Configuration > Device Management:
  - Remove the address "127.0.0.1/DECT".
  - Click "Activate".

Export all device management data from CPDM3-A in Device Manager > Numbers:

- Select all Numbers.
- In the menu, select Number > Export.
- In Device Manager > Templates:
- Select all templates.
- In the menu, select Template > Export

Do the following settings in the added module:

- CPDM3-B

Disable the DECT interface in Configuration > Other Settings > Advanced Configuration > General Settings > View advanced parameters:

- Set "DECT Interface" to Disabled.

Enable Device Management for the DECT system in Configuration > Other Settings > Advanced Configuration > Device Management:

- Replace the address "127.0.0.1/DECT" with the IP address of CPDM3-A plus "/DECT", that is, if CPDM3-A has the IP address 192.168.0.2, change to "192.168.0.2/DECT".
- Click "Activate".

Import all device management data to CPDM3-B:

In Device Manager:

- In the menu, select File > Import > Numbers...
- In the menu, select File > Import > Templates...

### H.3 High Messaging load in VoWiFi

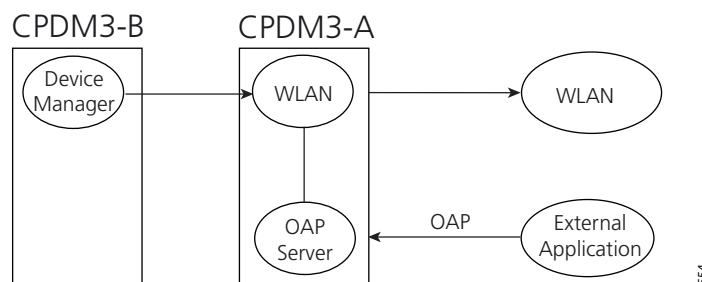
This solution applies to:

- systems with high messaging load
- systems with high requirements on maximum message burst throughput
- when requiring maximum shared phone performance in a system

When the messaging load is too high, a single CPDM3 cannot handle both messaging and device management effectively. Typically, this occurs when the messaging load is more than 4 000 messages per hour (or an equivalent amount of central phonebook enquires).

A solution to this situation can be achieved by running the messaging on one module and to handle Device Management on another module, as shown in the figure below.

Figure 50.



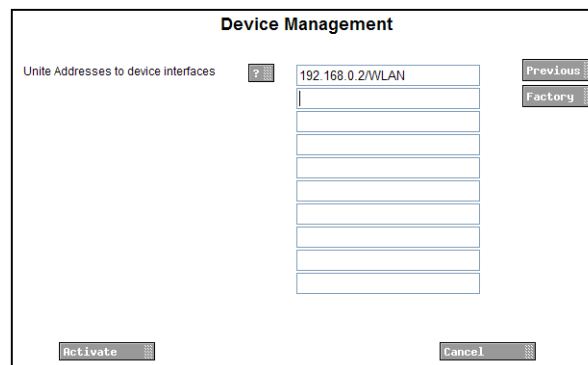
Example of paging in a multiple solution with OAP and WLAN.

#### H.3.1 Configuration for the setup

The basic configuration for this setup is described below.

- CPDM3-A  
In Configuration > Other Settings > Advanced Configuration > Device Management:
  - Remove IP addresses.
  - Click “Activate”.
- CPDM3-B  
Change IP address in Configuration > Other Settings > Advanced Configuration > Device Management:
  - Replace the address “127.0.0.1/WLAN” with the IP address of CPDM3-A plus “/WLAN”, that is, if CPDM3-A has the IP address 192.168.0.2, change to “192.168.0.2/WLAN”.
  - Click “Activate”.See figure below.

Figure 51.



Setting the IP address.

### H.3.2 Migration example to a double CPDM3 solution

This example assumes that the original system uses one CPDM3 module. Basically, the system setup is the same, but the original system with a single module has to be configured for a higher level of messaging traffic.

Change the following settings in the original module:

- CPDM3-A  
Change IP address in Configuration > Other Settings > Advanced Configuration > Device Management:
  - Remove the address “127.0.0.1/WLAN”.
  - Click “Activate”.

Export all device management data from CPDM3-A:

In Device Manager > Numbers:

- Select all Numbers.
- Number > Export.

In Device Manager > Templates:

- Select all templates.
- Template > Export

For settings in the added module:

See section [H.3.1 Configuration for the setup](#) on page 178.

- CPDM3-B  
Import all device management data to CPDM3-B in Device Manager:
  - File > Import > Numbers.
  - File > Import > Templates...

## H.4 Functionality distributed on three CPDM3 modules

This solution may be preferred due to security reasons, geographical reasons or administrative reasons.

Examples of functionality that can be distributed on different CPDM3 modules are Device Management, Central Phonebook and NetPage messaging.

A system configuration with three CPDM3s can be used when it is preferred to have Device Management on a separate CPDM3.

### H.4.1 Configuration for the setup

The basic configuration for this setup is described below.

- CPDM3-A
  - Disable the DECT interface  
In Configuration > Other Settings > Advanced Configuration > General Settings > View advanced parameters:
    - Set “DECT Interface” to Disabled.
  - Change IP address:  
In Configuration > Other Settings > Advanced Configuration > Device Management:  
Replace the address “127.0.0.1/DECT” with the IP address of CPDM3-C plus “/DECT”,  
that is, if CPDM3-C has the address 192.168.0.3, change to “192.168.0.3/DECT”.
  - Change UNS operating mode in order to get Basic Message Tool to work:  
In Configuration > Other Settings > Advanced Configuration > Other > UNS > Operating mode:
    - “Operating Mode” shall be set to Forwarding.
    - “IP address of forward destination UNS” shall be set to the IP address of the CPDM3  
with the DECT connection (here CPDM3-C).
- CPDM3-B
  - Disable the DECT interface  
In Configuration > Other Settings > Advanced Configuration > General Settings > View advanced parameters:
    - Set “DECT Interface” to Disabled.
  - Remove subscription of managed devices:  
In Configuration > Other Settings > Advanced Configuration > Device Management:
    - Remove all IP addresses.
  - Change UNS operating mode in order to get NetPage to work:  
In Configuration > Other Settings > Advanced Configuration > Other > UNS > Operating mode:
    - “Operating Mode” shall be set to Forwarding.

- “IP address of forward destination UNS” shall be set to the IP address of the CPDM3 with the DECT connection (here CPDM3-C).
- CPDM3-C
  - The DECT connection is configured in the Setup Wizard.
  - Remove IP addresses:  
In Configuration > Other Settings > Advanced Configuration > Device Management:
    - Remove all IP addresses.
  - Set name server address:  
In Configuration > Other Settings > Advanced Configuration > Other > UNS > “Alias / Call ID” > 999999:
    - In the “UNITE Address” field, enter the IP address of CPDM3-B plus “/ Phonebook”, that is, if CPDM3-B has the address 192.168.0.2, enter “192.168.0.2/Phonebook”.

#### H.4.2 Migration example to a triple CPDM3 solution

This example assumes that the original system uses two CPDM3s. CPDM3-A handles Device Management. CPDM3-B handles NetPage and the connection to DECT. An additional module shall now be added to the system.

One reason for this migration is to configure the external application which here is considered to be the most business critical application on one CPDM3 and the less critical applications NetPage, Phonebook and Device Management on the another two CPDM3s.

Change the following settings in the original CPDM3s:

- CPDM3-A:
  - Disable the DECT interface  
In Configuration > Other Settings > Advanced Configuration > General Settings > View advanced parameters:
    - Set “DECT Interface” to Disabled.
  - Set operating mode for UNS:  
In Configuration > Other Settings > Advanced Configuration > Other > UNS > Operating mode:
    - Set “Operating Mode” to Forwarding.
    - Set “IP address of forward destination UNS” to the IP address of the CPDM3 with the DECT connection (here CPDM3-C).
- CPDM3-B:
  - Disable the DECT interface  
In Configuration > Other Settings > Advanced Configuration > General Settings > View advanced parameters:
    - Set “DECT Interface” to Disabled.
  - Remove IP addresses for DECT:  
In Configuration > Other Settings > Advanced Configuration > DECT Interface > IP-DECT:
    - Click “Factory” to remove IP addresses and click “Activate”.
  - Set operating mode for UNS:  
In Configuration > Other Settings > Advanced Configuration > Other > UNS > Operating mode:
    - Set “Operating Mode” to Forwarding.

- Set "IP address of forward destination UNS" to the IP address of the CPDM3 with the DECT connection (here CPDM3-C).
- Remove IP addresses:  
In Configuration > Other Settings > Advanced Configuration > Device Management:
  - Remove all IP addresses.

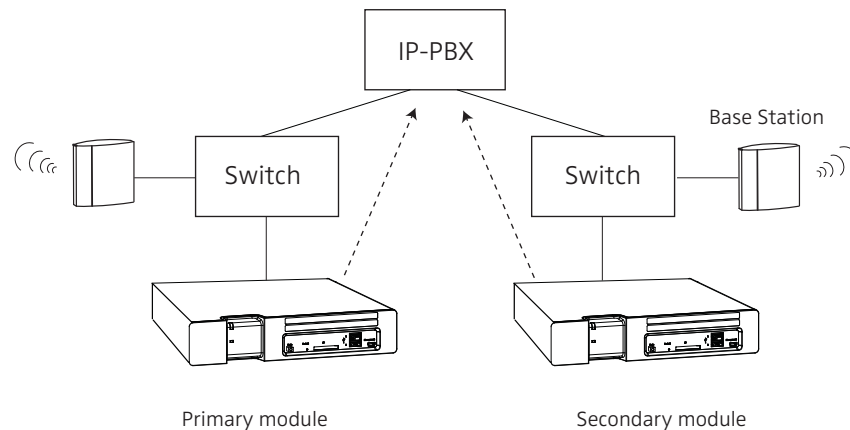
For settings in the added CPDM3, see above.

## Appendix I. Network Monitoring in a Redundancy System

In a redundant system, both the primary CPDM3 and the secondary CPDM3 can check if they have connection to the network by sending ICMP inquiries to an optional equipment in the same network. It is recommended to use the equipment that is centrally installed in the network, for example an IP-PBX. See the example below for more information.

If the active CPDM3 loses the connection to the network, the standby CPDM3 will become active instead.

Figure 52. Illustration of using a centralized equipment as network reference



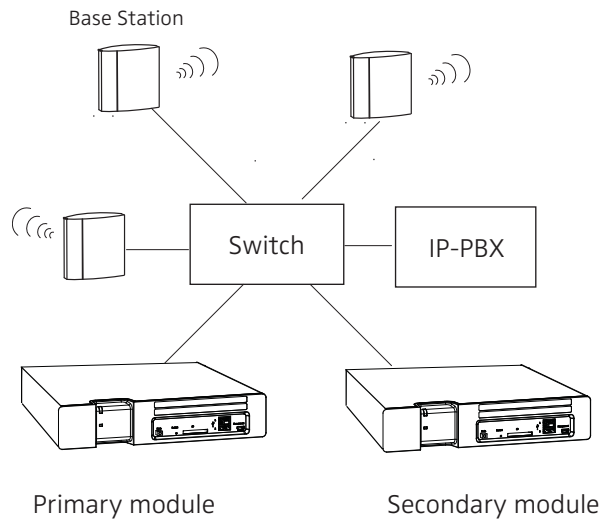
In [figure 52](#), both the primary CPDM3 module and the secondary CPDM3 are using the IP-PBX as network reference since it is centrally installed in the network.

**NOTE:** The use of the network monitor function is optional<sup>1</sup>, but it is strongly recommended to use when the modules are connected to different switches. If the function is disabled and the modules cannot communicate with each other, both modules might become active since they consider that the other module has failed. The result is that the one part of the system will write data to the primary CPDM3, and the other part will write data to the secondary CPDM3. This behavior is called “split brain behavior”.

---

<sup>1</sup>.By setting the Network monitor IP address to 127.0.0.1 disables the function.

Figure 53. Illustration of a network where no network monitoring is required.



If the primary CPDM3 and secondary CPDM3 are connected to the same switch (see [figure 53](#)), no equipment (for example an IP-PBX) is needed as network reference. If the secondary CPDM3 do not receive any response from the primary CPDM3, the primary CPDM3 has actually failed and the secondary CPDM3 becomes active.

### I.1 Fallback behavior when network monitoring is not used

If the primary CPDM3 loses the connection to the LAN (the power source is still connected), the secondary CPDM3 takes over as an active one. When the primary CPDM3 is reconnected to the LAN, the system switches back to the primary CPDM3 immediately.

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