

# Mitel WSM3\_Installation and Operation



### **About this document**

This document is used for installation and configuration of the product. It is also used for administration, maintenance and troubleshooting. These activities require good knowledge about functionality and limitations, both on module and system level, and also knowledge about how systems, modules and parameters interact.

## Table of Contents

About this document .....	2
<b>1. Introduction .....</b>	<b>1</b>
1.1 About the Product .....	1
1.2 Variants of the WSM3 Product .....	1
Art.no. Description .....	1
Optional licenses for WSM3 .....	1
Art.no. Description .....	1
1.3 Abbreviations and Glossary .....	1
1.4 How to Use this Document .....	3
References for Installation and Basic Configuration .....	3
References for Extended Configuration .....	3
Central Phonebook Administration .....	4
Daily Operation .....	4
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 WSM3 .....	6
2.2.1 Getting Started .....	6
2.3 Basic Configuration Steps .....	7
2.4 Manage Central Phonebook Entries .....	7
2.4.1 Add Entries to the Central Phonebook .....	8
Setting Description .....	8
2.4.2 Import entries from CSV file .....	8
2.5 Optional Settings .....	9
2.6 Multiple WSM3 .....	9
2.7 Expansion with Ascom Unite .....	10
<b>3. General .....</b>	<b>11</b>
3.1 Graphical User Interfaces (GUI's) .....	11
3.1.1 Start Page .....	11
Applications Authentication levels .....	11
(user name/password) .....	11
3.1.2 Login Page .....	12
3.1.3 Configuration Page .....	13
3.1.4 Advanced Configuration page .....	13

3.2	Authentication Levels and Default Password.....	14
3.3	Password Settings .....	15
3.3.1	Change Passwords .....	15
3.3.2	Set Password Policy .....	15
3.3.3	Set Programmatic Password Policy.....	16
3.4	System Security Settings.....	16
3.4.1	Web Access Security Settings .....	16
3.4.2	Access Logging .....	17
3.4.3	Module Shared Key .....	17
3.4.4	NetBIOS Port .....	17
3.4.5	Fragmented TCP Packets .....	18
3.4.6	FTP Port .....	19
3.4.7	Certificates .....	19
	Create a certificate signing request.....	19
	Export a certificate signing request .....	20
	Import certificate .....	21
	Create a self-signed certificate .....	21
	View Server Certificate .....	22
	View Trusted Certificates .....	22
	Import Trusted Certificates .....	22
	Delete a Trusted Certificate .....	23
3.5	Proxy Settings.....	23
3.6	Demonstration Mode .....	24
	From the application's Configuration page: .....	24
	Using the Mode button: .....	24
<b>4.</b>	<b>Basic Configuration.....</b>	<b>25</b>
4.1	Manage Central Phonebook Entries.....	25
4.1.1	Add Entries to the Central Phonebook .....	25
	Setting Description .....	25
	Sorting Entries in the Central Phonebook .....	25
4.1.2	Delete Entries .....	26
A)	Delete a single Entry: .....	26
B)	Delete several Entries:.....	26
4.1.3	Import Entries to the Central Phonebook from a CSV File .....	26
4.1.4	Export the Central Phonebook to a CSV File .....	26

4.2	Create Messaging Groups.....	27
Setting	Description .....	27
4.3	Select Messaging Destination.....	28
4.4	Input/Output Setup.....	28
4.4.1	Define Outputs.....	28
4.4.2	Define Inputs.....	28
4.5	Alarm Handling .....	29
4.5.1	Nomenclature.....	30
	Alarm Handling Icons .....	30
4.5.2	Add Alarm Actions .....	31
	Define Trigger.....	31
	Select Type of Action .....	33
4.5.3	Add Locations .....	35
4.6	Status.....	35
4.6.1	Active Faults .....	35
4.6.2	Reset the Error Relay .....	36
4.6.3	Level of Seriousness for different Fault Types (Module Fault List).....	36
4.6.4	Fault Log.....	37
	Symbols used in the Fault Log.....	38
	Symbol Description .....	38
4.6.5	Administer the Fault Log.....	38
	Export the Fault Log in CSV format.....	38
	Remove all non-active faults from the Fault Log .....	38
	Set a Timeout to block the Fault log from repeated faults.....	38
4.6.6	Module Performance Overview.....	38
	View graph details .....	39
4.6.7	WLAN Handsets .....	40
	Show all Registered VoWiFi Handsets.....	40
	Save a list with all Registered VoWiFi Handsets .....	41
	Remove IP Address or Delete a VoWiFi Handset .....	41
	Show Handset Details.....	41
4.6.8	Change the Handset Absent Status .....	42
4.6.9	Export Activity Logs to a Syslog Server .....	42
4.7	Module Redundancy .....	43
	Prerequisites .....	43

Licensing for Module Redundancy .....	43
Prepare IP addresses .....	45
4.7.1 Configure Module Redundancy.....	46
4.7.2 Redundancy Test.....	47
4.7.3 Restrictions on an Active Secondary Module.....	48
4.7.4 Fallback to the Primary WSM3 .....	49
4.7.5 Access Troubleshooting Pages.....	49
Troubleshooting page on active module .....	49
Troubleshooting page on standby module .....	49
4.7.6 Deactivate Redundancy .....	49
4.7.7 Replacement of Broken WSM3 in a Redundant System .....	50
4.8 Back up the Configuration.....	51
4.9 Restore the Configuration.....	51
<b>5. Central Phonebook Configuration .....</b>	<b>53</b>
5.1 Technical Specification .....	53
5.2 Change the Phonebook Address.....	53
5.3 Customize the Search Result Text .....	53
Default text      Description .....	54
5.4 Select Central Phonebook Database.....	54
5.5 LDAP Parameter Setup.....	54
5.5.1 Examples of Settings .....	56
5.6 Digit Manipulation in Central Phonebook.....	58
Telephone number standards.....	58
Format      Comment.....	58
Examples .....	58
Digit Manipulation Settings .....	60
<b>6. Serial Interface.....</b>	<b>62</b>
6.1 Serial Protocol Settings.....	62
6.1.1 ESPA Protocol .....	62
Settings      Description .....	62
6.1.2 Line Protocol .....	64
Settings      Description .....	64
6.1.3 TAP Protocol.....	65
Settings      Description .....	65
<b>7. Device Manager .....</b>	<b>67</b>
7.1 Start Device Manager in Java Runtime Environment.....	67

Device Manager in Oracle Java Runtime Environment.....	67
Device Manager in Eclipse Adoptium Environment .....	67
Install Eclipse Temurin .....	67
Download the IcedTea-Web plugin.....	67
Start Device Manager in the Eclipse Adoptium environment .....	68
<b>8. Device Configuration .....</b>	<b>69</b>
8.1 Device Management Setup.....	69
8.1.1 Example 1: All devices log in a single WSM3 .....	69
Configuration in Example 1 .....	69
8.1.2 Example 2: Devices log in to different WSM3 .....	69
Configuration in Example 2 .....	70
8.2 Inactivity Timeout .....	70
8.3 License Server Communication .....	70
8.4 Allow IP-DECT Handsets/Chargers to log in to Device Manager.....	70
8.5 Device Relogin Time .....	71
8.5.1 Relogin Time for Chargers .....	71
8.5.2 Delay Time for Charging Racks.....	71
8.5.3 Relogin Time for DECT/IP-DECT Handsets Put in Charger.....	71
8.5.4 Relogin Time for Fixed IP-DECT Devices .....	71
8.5.5 Relogin Time for VoWiFi Handsets .....	72
8.6 Service Discovery.....	72
8.6.1 Service Discovery Domain ID.....	72
8.6.2 Enable/Disable Service Discovery for Fixed IP-DECT Devices .....	72
8.6.3 Enable/Disable Service Discovery for VoWiFi Handsets.....	73
<b>9. Additional System Settings .....</b>	<b>74</b>
9.1 Unite Name Server (UNS).....	74
9.1.1 UNS Operating Mode .....	74
9.1.2 Default Category .....	74
9.1.3 Alias / Call ID.....	75
9.2 Logging .....	76
9.3 Time Settings.....	76
9.3.1 Manual Time Setting (if Web browser is Time Source) .....	77
9.4 Network Settings.....	78
9.4.1 Hostname Mapping.....	79
9.5 Setting the License Number .....	80
9.6 Reboot .....	80

<b>10. Remote Management .....</b>	<b>82</b>
Remote connection .....	82
Open ports .....	82
Serial port channel .....	83
10.1 Serial IP Server Protocol .....	83
<b>11. Absence Handling.....</b>	<b>85</b>
11.1 Absence Handling in DECT .....	85
11.1.1 Absence List.....	85
11.1.2 Clear Absence List .....	85
11.2 Absence Handling in the VoWiFi System.....	85
11.2.1 Sort on Handset Status.....	85
11.2.2 Search on Handset Status .....	85
<b>12. Base Station Conversion .....</b>	<b>87</b>
12.1 Background.....	87
12.2 Configuration .....	87
<b>13. Open Access Protocol (OAP) .....</b>	<b>88</b>
13.1 Configuration .....	88
OAP Server settings .....	88
OAP encryption parameters .....	88
Configuration Example .....	89
13.2 Importing a new OA-XML file .....	89
<b>14. DECT Interface .....</b>	<b>90</b>
14.1 DECT Phone Systems .....	90
14.1.1 IP-DECT .....	90
A) IP-DECT system with a Single Master.....	90
B) IP-DECT system with Multiple Masters .....	90
14.2 DECT Interface Settings.....	91
14.2.1 General Settings.....	91
14.2.2 System Dependent Settings .....	92
For a single IP-DECT interface .....	92
For multiple IP-DECT interfaces .....	92
14.2.3 DECT Message Distribution .....	92
14.2.4 SMS Character set.....	93
14.2.5 DECT WebSocket Connectivity .....	93
General Settings .....	93
Authentication Settings .....	94

14.2.6	IP-DECT Device Handling .....	94
<b>15.</b>	<b>WLAN Interface .....</b>	<b>96</b>
15.1	Handset Registration.....	96
15.2	Shared Phones .....	96
15.3	WLAN System.....	96
15.4	WLAN Message Distribution .....	98
15.5	User Server .....	98
15.6	WLAN Websocket Connectivity .....	98
	General Settings .....	98
	Authentication Settings .....	99
	Temporary authentication credentials .....	100
	Example.....	101
<b>16.</b>	<b>Messaging Operation .....</b>	<b>102</b>
16.1	Create and Send Messages via the Messaging Tool .....	102
16.2	Create and Send Messages via NetPage.....	102
16.3	Predefined Messages .....	103
	Common Messages .....	103
	My Messages.....	103
16.3.1	Create a Predefined Message .....	103
16.3.2	Edit a Predefined Message .....	104
16.4	Message History Status .....	104
	Status Description .....	104
16.5	Predefined Groups.....	104
	My Groups.....	104
	Common Groups .....	104
16.5.1	Create a Group.....	104
16.5.2	Edit a Group.....	105
16.6	Messaging Tool Configuration.....	105
16.7	NetPage Configuration .....	105
	Set Messaging Properties .....	105
	Creating or Updating the Number list .....	106
16.7.1	Colored messaging.....	107
16.7.2	Backup and Restore NetPage files .....	108
	NetPage Files .....	108
	Backup.....	108
	Restore .....	108
	Backup of Predefined Groups and Messages .....	108

Backup.....	108
Restore .....	109
<b>17. Administration of Language and User Interfaces .....</b>	<b>110</b>
For the best screen appearance .....	110
How to edit .....	110
17.1 Customize the Language .....	110
17.1.1 Export a Language for Translation/Editing.....	110
17.1.2 Translate/Edit the Language .....	111
17.1.3 Show Pages in Translation Mode.....	112
17.1.4 Import Language File .....	113
17.1.5 Delete Language File .....	114
17.1.6 Select Language.....	114
17.2 Customize User Login Message .....	114
17.3 Customize the User Interface (GUI).....	115
17.3.1 Change the Size of the FTP Area.....	115
17.3.2 Files for Translation/Editing.....	116
17.3.3 Default Start Page GUI .....	117
17.3.4 Default Send Message GUI.....	117
Priority and Beep Codes in the default NetPage User Interface GUI Description	Priority
Code	119
17.3.5 Change the NetPage User Interface Functionality.....	119
17.3.6 Translation of the User Interfaces .....	120
Start Page .....	120
Example User Interfaces index1, index2 or index3 .....	120
Example GUI index4 .....	121
17.3.7 Upload the Files to the module's FTP Area .....	122
17.3.8 Inserting a Company Logotype .....	122
17.3.9 Creating a URL Call .....	122
Parameters .....	123
Message ID.....	123
Erase message.....	123
UTF8 encoded .....	123
Creating the URL.....	124
Creating a Quick Button with a URL Call .....	124

Opening NetPage with Fields Automatically filled in.....	124
17.4 Test the New User Interface .....	125
17.5 Update the User Interface after a new Release .....	125
<b>18. Software Administration.....</b>	<b>126</b>
18.1 Upgrade the Boot Software.....	126
18.2 Software Information.....	126
18.3 Switch Software .....	126
18.3.1 Switch software in a non-redundant system .....	126
18.3.2 Switch software in a redundant system .....	127
18.4 Install New Software.....	127
18.4.1 Create a Software Backup .....	127
<b>19. Troubleshooting .....</b>	<b>128</b>
19.1 General Troubleshooting.....	128
19.1.1 Log files.....	128
To find Info log and Error log: .....	128
19.1.2 The Module does not Start.....	128
19.1.3 Firewall Issues, or No Indication of Connected Device.....	128
19.1.4 Unable to Access FTP Area .....	128
19.2 NetPage Troubleshooting .....	129
Fault Probable cause Action or comment.....	129
19.3 Troubleshooting Guide.....	129
19.3.1 Troubleshooting for the Device Manager.....	130
Fault Probable cause Action or comment.....	130
Fault Probable cause Action or comment.....	131
Fault Probable cause Action or comment.....	132
Fault Probable cause Action or comment.....	133
Fault Probable cause Action or comment.....	134
19.3.2 General Troubleshooting for the WSM3 .....	134
Fault Probable cause Action or comment.....	134
Fault Probable cause Action or comment.....	135
19.4 Built-in tools .....	135
Tools Description .....	135
colors.....	135
Flashing frequency .....	135
Flashing patterns.....	136
19.5 Advanced Troubleshooting .....	136

19.6	What to consider when replacing a module .....	137
19.7	Technical Support .....	137
20.	<b>Related Documents .....</b>	<b>138</b>
	<b>Appendix A. Used IP Ports .....</b>	<b>139</b>
	Example 1: .....	139
	Example 2: .....	139
	<b>Appendix B. RS232 Connections .....</b>	<b>141</b>
	<b>Appendix C. Alarm Action Configuration Examples .....</b>	<b>142</b>
C.1.1	System Components One WSM3 .....	142
	4 handsets with push-button alarms .....	142
	Input/Output Setup .....	142
	Push-button alarm from 1440 .....	142
	Activate Actions .....	143
	Alarm cancellation .....	143
	Cold-storage room 1, door open .....	144
	Actions Activate Output Action and Send Message Actions .....	145
	Cold-storage room door closed .....	146
	Summary of alarm actions .....	146
	<b>Appendix D. Protocol Limitations .....</b>	<b>147</b>
D.1.1	Functionality .....	147
D.1.2	Limitations Protocol Blocks .....	147
D.1.3	Protocol Records .....	147
D.1.4	Advanced parameters .....	148
D.2.1	Functionality .....	148
D.2.2	Limitations .....	148
D.3.1	Functionality .....	148
D.3.2	Limitations .....	148
	<b>Appendix E. File types .....</b>	<b>150</b>
	<b>Appendix F. Multiple WSM3 Configuration Examples .....</b>	<b>151</b>
F.1.1	Configuration for the setup .....	151
	Example: Migration to a double WSM3 solution .....	151
F.2.1	Configuration for the setup .....	153
F.2.2	Migration example to a double WSM3 solution .....	154
F.3.1	Configuration for the setup .....	155

F.3.2	Migration example to a double WSM3 solution .....	156
F.4.1	Configuration for the setup.....	157
Call ID	Number/Address -> Category .....	157
F.4.2	Migration example to a Multimaster IP-DECT solution.....	158
<b>Appendix G. Network Monitoring in a Redundancy System .....</b>		<b>159</b>
G.I	Fallback behavior when network monitoring is not used.....	160

## 1. Introduction

### 1.1 About the Product

Wireless Service Messaging (WSM3) is a web-based tool designed as an all-in-one solution. 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 Variants of the WSM3 Product

Art.no.	Description
FE3-EFDBAC	WSM3 Basic including hardware module, software and license with Device Management (100 Devices) and Module Redundancy.

NOTE: If Module Redundancy is to be used, the license provided with this variant may only be installed on the WSM Basic to be used as primary module. The secondary WSM3 Basic must be an empty module without any licenses and settings. See [4.7 Module Redundancy](#) on page 43 for more information.

#### Optional licenses for WSM3

When ordering licenses for the product, the licenses are only valid for that product's hardware. For example, if you order a license for a product with module key 001234, the license will only work for that hardware.

Art.no.	Description
FE3-EGDLB	Upgrade license to WSM3 Standard. Device Management for 2,500 Devices.
FE3-EGDLAP3	Upgrade license with OAP. Requires also FE3-EGDLB WSM3 Standard
FE3-EGDLRB	Upgrade license with Module Redundancy for WSM3 Standard. Requires also FE3-EGDLB WSM3 Standard.

NOTE: This license may only be installed on the WSM3 Standard to be used as primary module. The secondary module must be an empty WSM3 Basic without any licenses and settings. See [4.7 Module Redundancy](#) on page 43 for more information.

### 1.3 Abbreviations and Glossary

Ascom 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: In WSM3, this tool is referred to as Alarm Handling.
CA	Certification Authority: An entity that issues digital certificates.
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
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.
CSR	Certificate Signing Request: A message from an applicant to a certificate authority in order to apply for a digital certificate.
CSV file	Comma Separated Value: 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: A global standard for cordless telephony.
Device	Can be a DECT or VoWiFi handset, or a charger developed to work together with WSM3 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 DAM (DECT Authentication Module) See IPEI for more information.
IPEI	International Portable Equipment Identity: 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 handset on WSM3. Language file for WSM3 uses XML (eXtensible Markup Language.).
LDAP	Lightweight Directory Access Protocol
License file	A file containing license keys for devices. The file can be exported from the license web and imported to the Device Manager in the WSM3.
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: Ascom defined XML based messaging and alarm protocol.
OA-XML	The Open Access-XML protocol defines messages in XML format. WSM3 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: 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. The Unite communication protocol is used for communication between WSM3s in systems with more than one WSM3.
UNS	Unite Name Server: Unite module component that holds the Unite number plan and Unite destinations
VoWiFi	Voice over Wireless Fidelity: 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
WSM3	Wireless Service Messaging An application suite that enables wireless services to and from handsets and chargers.

## 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 6
  - [3. General](#) on page 11

### References for Extended Configuration

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

- For settings included in the FE3-EFDBAC WSM Basic variant.  
See chapters:
  - [4.2 Create Messaging Groups](#) on page 27
  - [4. Basic Configuration](#) on page 25
  - [4.1 Manage Central Phonebook Entries](#) on page 25
  - [10. Remote Management](#) on page 82
  - [11. Absence Handling](#) on page 85
  - [12. Base Station Conversion](#) on page 87
  - [7. Device Manager](#) on page 67
  - [4.7 Module Redundancy](#) on page 43
- For settings included in the upgrade license FE3-EGDLB WSM3 Standard.  
See chapters:
  - [5.5 LDAP Parameter Setup](#) on page 54
  - [4.2 Create Messaging Groups](#) on page 27
  - [4.5 Alarm Handling](#) on page 29
  - [16. Messaging Operation](#) on page 102
  - [17.3.9 Creating a URL Call](#) on page 122
  - [6. Serial Interface](#) on page 62
- For settings included in the upgrade license FE3-EGDLRB Module Redundancy for WSM3 Standard.  
See chapter:
  - [4.7 Module Redundancy](#) on page 43
- For settings included in the FE3-EGDLAP3 OAP license.  
See chapter:
  - [13. Open Access Protocol \(OAP\)](#) on page 88

See also *Function Description, Open Access Protocol (OAP)*, TD 925/4GB.

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 25.

#### Daily Operation

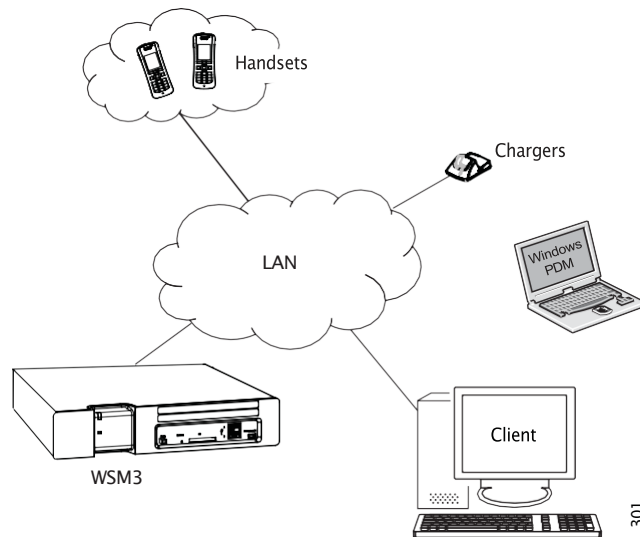
- For the daily operation, that is, creating and sending messages, see chapter [16. Messaging Operation](#) on page 102.

### 1.5 Included in the delivery

- WSM3 hardware including a 230 V power cable
- Getting started document

## 1.6 Technical Solution

Figure 1. WSM3 in a system.



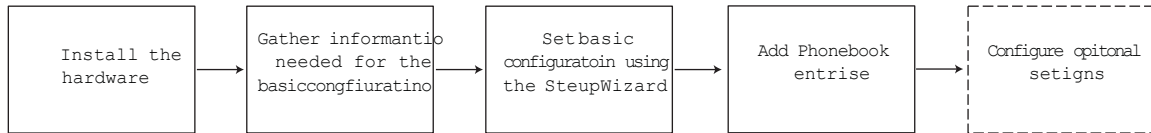
The WSM3 runs on the hardware and is configured via a web interface using a computer (client) connected to the Local Area Network (LAN).

## 1.7 Requirements

Refer to the Data Sheet for WSM3.

## 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 WSM3.

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 WSM3 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 WSM3's rear side and in the application's GUI in the Setup Wizard.
- The module key – found on the license certificate or on the WSM3's rear side
- Network parameters – ask your network administrator
- License number – found on the license certificate
- Type of connected wireless phone system
- IP address to connected system (if connected via IP)
- Other messaging systems to send messages to (optional)
- LDAP properties, if an LDAP server is used for Central Phonebook requests (optional)

### 2.2 Accessing the WSM3

#### 2.2.1 Getting Started

When accessing the WSM3 the first time, follow the instructions in the Getting Started and safety Leaflet PM000033, or the Installation Guide for WSM3

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 WSM3 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 WSM3 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, or LDAP server).
- LDAP properties – (only visible if LDAP is selected in the Central Phonebook properties)
- Passwords – all default passwords must be changed according to the password policy.

### 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/Export Central Phonebook Entries

#### Export

Export phonebook

#### Import

Mitel 3300 format ☒

Import file

- 3 If the file to be imported is of Mitel 3300 format, mark the *Mitel 3300* check box.

- 4 Click “Browse” to locate the CSV file in the system.
- 5 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 29.
- 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 35.
- Set Language – it is possible to translate the user interface language, refer to chapter [17.1 Customize the Language](#) on page 110.
- 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 28.
- 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 [17.3 Customize the User Interface \(GUI\)](#) on page 115.
- 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 82.
- 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 88.
- Digit Manipulation – makes it possible to set the way telephone numbers are converted in telephone number lists. See [5.6 Digit Manipulation in Central Phonebook](#) on page 58.
- Redundancy – makes it possible to set up a pair of WSM3s for redundancy. Refer to chapter [4.7 Module Redundancy](#) on page 43.

## 2.6 Multiple WSM3

In some situations there is a need for more than one WSM3 in a system. More than one module is required in following cases:

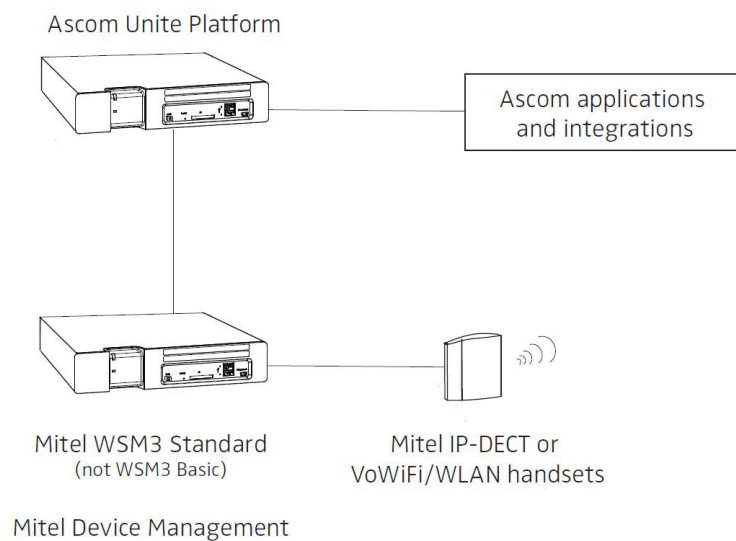
- in systems with centralized management for more than 2500 devices, see [F.1 More than 2500 devices](#) on page 157.
- in DECT systems with centralized management in combination with a traffic load expected to be more than 4 000 messages per hour (or an equivalent amount of central phonebook enquires), see [F.2 High messaging load in DECT](#) on page 158.
- in VoWiFi systems with centralized management in combination with a traffic load expected to be more than 8 000 messages per hour (or an equivalent amount of central phonebook enquires), see [F.3 High Messaging load in VoWiFi](#) on page 160.
- in multi-master IP-DECT systems in combination with a traffic load expected to be more than 12000 messages per hour (or an equivalent amount of central phonebook enquires) (one WSM3 per IP-DECT master, in combination with number planning). see [F.4 Multi-master IP-DECT systems and Multiple DECT systems](#) on page 162.
- in a multiple DECT systems (one WSM3 per DECT system, in combination with number planning). see [F.4 Multi-master IP-DECT systems and Multiple DECT systems](#) on page 162.

## 2.7 Expansion with Ascom Unite

For Ascom Unite functionality, WSM3 can be expanded with the Ascom Unite Platform. In this configuration, WSM3 acts as a DECT and/or WLAN interface in the Ascom Unite system and provides device management. The Ascom Unite platform enables various integrations and applications.

If WSM3 is expanded with Ascom Unite, the following steps must be performed:

- Make sure you have the WSM3 Standard license. The Basic license is not supported.
- Enable the forwarding operating mode. See [9.1 Unite Name Server \(UNS\)](#) on page 74.
- Configure the Ascom Unite system IP address for Status Log and System Activity Log. See [9.2 Logging](#) on page 76.
- Check network settings and update hosting settings, if necessary. [9.4 Network Settings](#) on page 78.



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 11.

Table 1.

Applications	Authentication levels (user name/password)
Send Message, see <a href="#">16. Messaging Operation</a> on page 102.	No logon required
Phonebook, see <a href="#">4.1 Manage Central Phonebook Entries</a> on page 25. Describes how to handle phonebook entries.	user/password admin/changeme sysadmin/setmetup
Device Manager, see <a href="#">7. Device Manager</a> on page 67. Describes device management.	user/password admin/changeme sysadmin/setmetup
Configuration, see <a href="#">3.1.3 Configuration Page</a> on page 13. Setup page for the module settings.	admin/changeme sysadmin/setmetup

Setup Wizard, see [2.3 Basic Configuration Steps](#) on page 7.      admin/changeme  
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 14.

### 3.1.2 Login Page

When clicking an application that requires login credentials, the WSM3 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 WSM3'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 WSM3



The image shows a login form with a light blue background. It contains two text input fields: the first is labeled 'User name' and the second is labeled 'Password'. Below these fields is a blue button with the text 'Log in' in white.

**NOTE:** A custom login message can be defined by a system administrator to appear on the login page. Follow the instructions in the [17.2 Customize User Login Message](#) on page 114 to set up the login message.

### 3.1.3 Configuration Page

Figure 6. The Configuration page

Back to start page

Add page to favorites

Back to configuration top page Authentication level

**WSM3 Configuration**

Logged in as admin [Log out](#)

**Information**

Status	Application problem
Number of Active Faults	2

Software Version	3.04-A
Module Key	00120080
License Number	0000000000000000
Hardware type	Elise3

MAC Address	00-01-3e-01-d4-fc
Host Name	Elise
IP Address	172.20.13.42

NTP Server	Not used
Time	2011-04-27 12:48:44
Uptime	8d 19h 57m 28s

**Documentation**

[OA-XML description](#)  
[OA-XML schema](#)  
[Third-Party Licenses](#)

Log out to start 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.

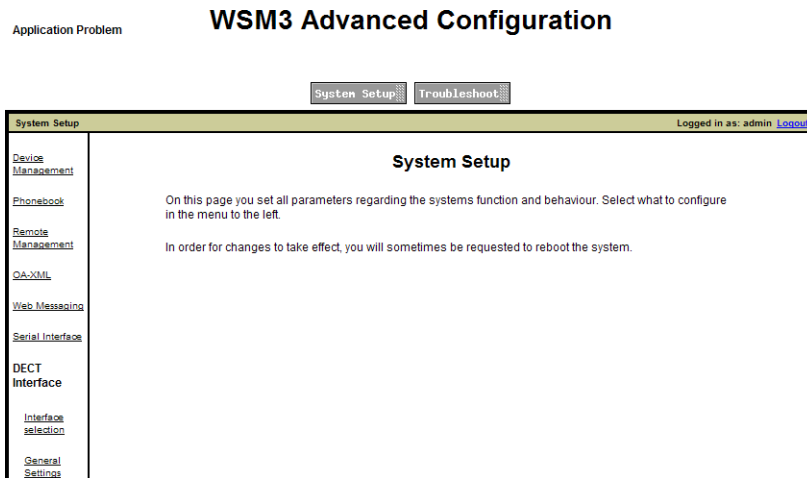
Use the symbol if you want to return to the start page without logging out. Using the “Log out” link will also send you back to the start page but you will be logged out as well.

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 is “user”.
- *Administrator* rights are required for the setup, the configuration and administration, simple troubleshooting and changing passwords (except for the sysadmin password). Default user name is “admin”.
- *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 is “sysadmin”.
- *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 is “auditor”.

Different levels of password policy can be set in, see [3.3.2 Set Password Policy](#) on page 15.

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., must 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:

admin

sysadmin

user

ftpuser

- 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 on the *Configuration* page.
- 3 Select "Password Policy" under Security in the menu on the *Advanced Configuration* page.
- 4 Set password policy.
- 5 Click "Activate".

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

### 3.3.3 Set Programmatic Password Policy

The programmatic password complexity is applied to passwords used by IP DECT and VoWiFi devices if the Secure web socket mode is enabled, see [14.3.6 DECT WebSocket Connectivity](#) on page 205 and [15.6 WLAN WebSocket Connectivity](#) on page 98.

- 1 Click "Configuration" on the start page.
- 2 Select Other Settings > Advanced Configuration in the menu in the on the *Configuration* page.
- 3 Select "Programmatic Password Policy" under Security in the menu on the *Advanced Configuration* page.
- 4 Set 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 WSM3 only should be accessed via HTTPS and FTPS to establish a secure connection between your client and the WSM3. Information sent between the client and the WSM3 cannot be seen by any third-party. The HTTPS and FTPS require a certificate.

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

Select "Web Access" under Security in the menu on the *Advanced Configuration* page.

- 3 In the "Secure Mode" drop-down list, select whether WSM3 can be accessed via HTTP/FTP and/or HTTPS/FTPS:
  - Enabled - Only HTTPS/FTPS is allowed.
  - Disabled - Both HTTP/FTP and HTTPS/FTPS are allowed.
- 4 In the "TLS Protocol Version" drop-down list, select which protocol that must be used to allow access to the WSM3 via HTTPS/FTPS.
- 5 In the "Check client certificate" drop-down list, select whether the WSM3 shall ask for the client certificate when accessing the module via HTTPS/FTPS.
  - Enabled – The WSM3 asks for the client certificate. Additionally, the WSM3 also controls if the client certificate is trusted by a Certification Authority (CA).

NOTE: If enabled, the certificate has to be imported to the WSM3, see [3.4.7 Certificates](#) on page 19.

- Disabled – The WSM3 will not ask for the client certificate.
- 6 In the "Inactivity Timeout" field, enter the number of minutes of inactivity that should be allowed before the session expires and the user must log in again. (Allowed values 10-60 minutes, default 10 minutes). If the field is left empty the session will not expire.
  - 7 Click "Activate".

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

#### 3.4.2 Access Logging

This parameter determines which login attempts that should be collected in the Activity Log.

- 1 Click "Configuration" on the start page.
- 2 Select Other Settings > Advanced Configuration in the menu in the on the Configuration page.
- 3 Select "Access Logging" under Security in the menu on the Advanced Configuration page.
- 4 In the drop-down list, select under which conditions an activity log should be created.
  - None – No activity log will be created (default).
  - Failed attempts only – An activity will be logged if a user tries to log in to the Configuration page with the wrong user name and/or password.
  - All attempts – An activity will be logged as soon as a user logs in or out on the Configuration page.
- 5 Click "Activate".

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

#### 3.4.3 Module Shared Key

To enable AES encryption for secure connection between multiple WSM3 servers, configure a shared key.

NOTE: The same shared key must be configured on all WSM3 servers.

- 1 Click "Configuration" on the start page.
- 2 Select Other Settings > Advanced Configuration. Select "Module Shared Key" under Security in the menu on the *Advanced Configuration* page.
- 3 In the "Shared Key" field, enter a 32-character long shared key. The key can include the following characters: A-Z, a-z, 0-9, and special characters.  
If the "Shared Key" field is empty, the default XTEA encryption is used.
- 4 Click "Activate".

#### 3.4.4 NetBIOS Port

You can determine if the NETBIOS port (UDP 137) shall be open or closed. The NETBIOS makes it possible to access the WSM3 with the NetBIOS name "elise-XXXXXXX", where XXXXXXXX is the module key number. If the port is closed, only the WSM3's IP address can be used to access the WSM3.

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

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

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

#### 3.4.5 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.

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

### 3.4.6 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.

- 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”.

### 3.4.7 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 *User Manual, Device Manager, TD 93028EN*.

#### Create a certificate signing request

Before a certificate is signed by a Certification Authority, a certificate signing request (CSR) must be created.

Due to security reasons, some characters in the ASCII-table are not allowed to use in the fields for a CSR, for example: [ , ] , ( , ) , { , } , \$ , & , \ , | , \* , " , ' , ? , ~ , > , < , ^ , \n , \r .

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

- 3 Click “Create CSR” under Certificates in the menu.

- 4 In the “Key” field, select the length of the private certificate key.
- 5 In the “Signature” field, select the algorithm to encode the certificate signature.
- 6 In the “Common name” field, enter an identifier of the WSM3 module. The maximum length of the identifier is 64 characters.  
Usually, the domain name of the WSM3 module is entered in the “Common name” field.
- 7 Optionally, complete the “Organizational Unit” and the “Organization” fields. The maximum length for each field is 64 characters.
- 8 Optionally, complete the “Locality” and the “State or Province” fields. The maximum length for each field is 128 characters.
- 9 Optionally, complete the “Country” field with a two-character country code, for example, UK.
- 10 Click “Create CSR”.

Creating a CSR takes some time. The status of CSR creation is shown in a pop-up window. If the CSR has been created successfully, export the CSR.

#### Export a certificate signing request

After a CSR has been created, it can be exported and sent to a Certification Authority for generating a signed certificate.

- 1 Click “Configuration” on the start page.
- 2 Select Other Settings > Advanced Configuration in the menu on the *Configuration* page.
- 3 Click “Export CSR” under Certificates in the menu
- 4 Click “Export file”.
- 5 Send the file to a Certificate Authority to generate a PEM encoded certificate.

NOTE: Only PEM encoded certificates are supported. The certificate file can have the following extensions: .pem, .crt, .cer.


IMPORTANT: After a CSR is created and sent to a Certification Authority, no new CSR should be created. If a new CSR is created, a certificate generated from a previous CSR will be invalid.

After a certificate is generated and signed by the Certification Authority, import the certificate.

### Import certificate

Certificates can be imported to the WSM3. These certificates may be created by a system administrator with IT security responsibility. The WSM3 uses a PKCS#12 .p12 or .pfx file, which includes keys and certificates, or a .pem, .crt, or .cer file, which includes a PEM encoded certificate signed by a Certification Authority.

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



The screenshot shows a dialog box titled "Import" with a subtitle "Import certificate file". It contains the following text:

The following certificate can be imported:

- Single certificate - a server certificate generated from a Certificate Signing Request (created on this server using the Create CSR option in the menu) and signed by a Certification Authority. The certificate must be PEM encoded and the file shall have one of the following extensions: .crt, .cer, .pem. No password is needed to import this certificate.
- A PKCS#12 bundle that contains a private key, a server certificate and, optionally, the CA certificate that was used to sign the server certificate. The certificate file shall have one of the following extensions: .p12, .pfx. The PKCS#12 file is always supplied with a password.

Note: After a certificate is successfully imported, the web server restarts and forces connected web browsers to reload open pages of the administrative portal.

Below the text, there are two input fields: "File name" and "Password". The "File name" field has a "Choose File" button and the text "No file chosen". The "Password" field has a question mark icon and a text input box. At the bottom, there are two buttons: "Import file" and "Close".

- 4 In the "File Name" field, click "Browse" and locate a certificate file.
- 5 For the PKCS#12 file, in the "Password" field, enter a password delivered with the file.
- 6 Click "Import file". The file is imported to the module.
- 7 Click "Close".

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

### Create a self-signed certificate

To create a self-signed certificates in the module, perform the following steps:

- 1 Click "Configuration" on the start page.
- 2 Select Other Settings > Advanced Configuration in the menu 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.  
The following characters are not allowed: [ , ] , ( , ) , { , } , \$ , & , \ , | , \* , " , ' , ? , ~ , > , < , ^ , \n , \r .

- 5 Click “Create Certificate”.

A self-signed certificate is created and can be downloaded as a PKCS#12 file.

#### View Server Certificate

To view the server certificate, imported on the WSM3, perform the following steps:

- 1 Click “Configuration” on the start page.
- 2 Select Other Settings > Advanced Configuration in the menu on the *Configuration* page.
- 3 Click “View server certificate” under Certificates in the menu.

#### View Trusted Certificates

The trusted certificates repository can contain up to 10 certificates including:

- The CA certificate that was imported from a PKCS#12 bundle with the server certificate (if any).
- Imported certificates of the client devices the server shall trust.

To view trusted certificates, imported on the WSM3, perform the following steps:

- 1 Click “Configuration” on the start page.
- 2 Select Other Settings > Advanced Configuration in the menu on the *Configuration* page.
- 3 Click “Trusted Certificates Repository” under Certificates in the menu.
- 4 Click “View” to see the required imported certificate.

#### Import Trusted Certificates

When the WSM3 establishes a secure connection with a client device, the client certificate is verified. The client certificate is considered as trusted if it has been imported to the repository on the WSM3. PEM encoded certificates are supported only. The certificate file

shall have one of the following extensions: .crt, .cer, .pem. Up to 10 certificates can be imported on the WSM3.

To import a certificate of a client device, perform the following steps:

- 1 Click "Configuration" on the start page.
- 2 Select Other Settings > Advanced Configuration in the menu on the *Configuration* page.
- 3 Click "Trusted Certificates Repository" under Certificates in the menu.
- 4 Click "Import file".
- 5 In the "File Name" field, click "Browse" and locate a certificate file.
- 6 Click "Import file".
- 7 Click "Close" in the certificate import confirmation window.

#### Delete a Trusted Certificate

To delete a certificate that was imported to the trusted certificates repository, perform the following steps:

- 1 Click "Configuration" on the start page.
- 2 Select Other Settings > Advanced Configuration in the menu on the *Configuration* page.
- 3 Click "Trusted Certificates Repository" under Certificates in the menu.
- 4 Find the required certificate and click "Delete".
- 5 Click "Close" in the certificate import confirmation window.

### 3.5 Proxy Settings

If your corporate network is using a proxy server, the WSM3 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.

- 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 14.

### 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 25) or by importing a file containing the entries ([4.1.3 Import Entries to the Central Phonebook from a CSV File](#) on page 26).

#### 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/Export Central Phonebook Entries

##### Export

Export phonebook

##### Import

Mitel 3300 format ☒

Import file

- 3 If the file to be imported is of Mitel 3300 format, mark the *Mitel 3300* check box.
- 4 Click "Browse" to locate the CSV file in the system.
- 5 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.

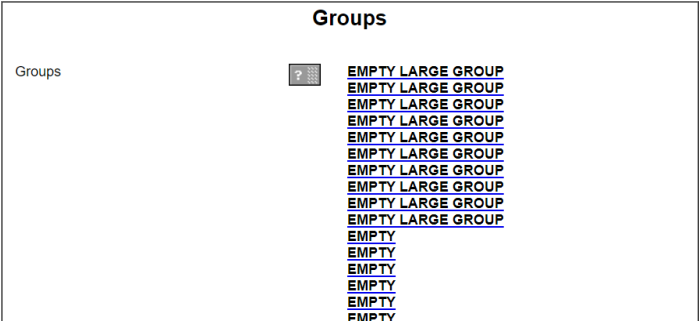
- 6
- Click “Save”.

4.2 Create Messaging Groups

Messaging Groups in the WSM3 makes it possible to send one message to several handsets. 60 small groups with 15 handsets in each group, and 10 large groups with 100 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.



- 3
- Open the group to be configured by clicking on its name (default EMPTY).

Group configuration

Group address

?

Previous

Group description

?

Factory

Members

?

- 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, 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 WSM3 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 WSM3, and example of outputs is a siren or a lamp connected to the WSM3.

#### 4.4.1 Define Outputs

You can change the output name and the initial state of the output ports.

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

##### Outputs

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

- 3 In the Output Name field, change the description of the Output port.
- 4 In the Initial State drop-down list, select the initial state to be used. To revert to default setting (i.e. High), click "Reset".
- 5 Click "Save".

#### 4.4.2 Define Inputs

You can change the input name, the activate state and activation time of the input ports.

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

##### Inputs

ID	Input Name	Module Address	Input	Activation	Activation Time
1	<input type="text" value="Internal Input 1"/>	127.0.0.1	Internal	1 <input type="text" value="On Opening"/>	<input type="text" value=""/>
2	<input type="text" value="Internal Input 2"/>	127.0.0.1	Internal	2 <input type="text" value="On Opening"/>	<input type="text" value=""/>

- 3 In the Input Name field, change the description of the Input port.

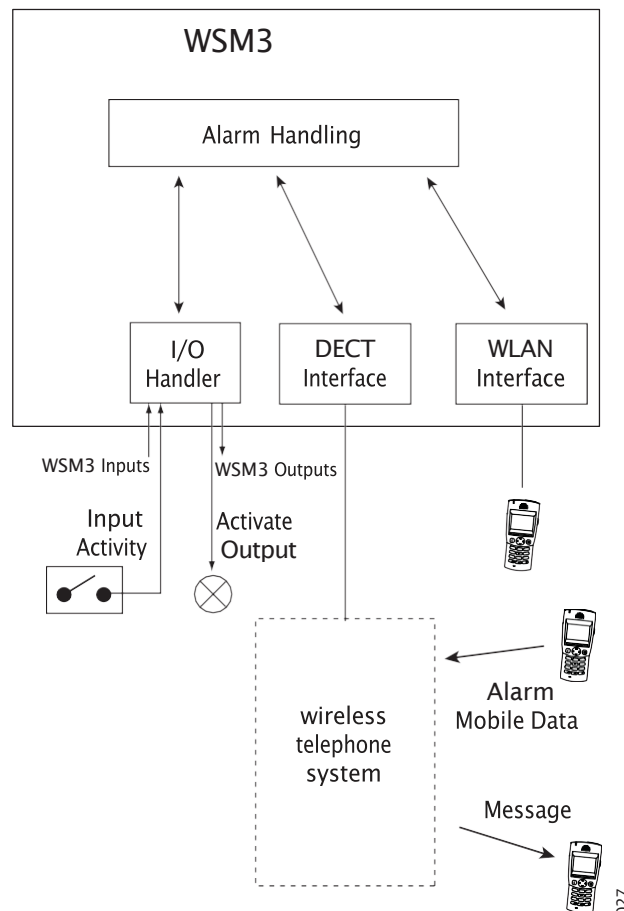
- 4 In the Activation drop-down list, select the activation state to be used.
  - On opening - if the port should be activated when a connected switch/button is released.
  - On closing - if the port should be activated when a connected switch/button is pressed.
- 5 By default a notification will be sent immediately. If you enter activation time, the input has to be active for the set time before a notification is sent. Legal values: 1 - 36000.

## 4.5 Alarm Handling

This functionality requires an additional license.

The alarm handling included in WSM3 makes it possible to trigger on alarms and data from handsets in the Cordless Telephone System. Activated inputs on WSM3 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 WSM3.

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 C. Alarm Action Configuration Examples](#) on page 148.

### 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 WSM3.
Output	An output on the WSM3.
Trigger	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. 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.
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: 1 (250)

Name	Notes	Triggers		
MyAlarmAction		Alarm Type: Push-button double press, Number: 123456		

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**

Alarm Type	Number
Any alarm ▼	<input style="width: 80%;" type="text"/> <span style="color: red; font-weight: bold;">✗</span>
<input style="width: 50px;" type="button" value="Add"/>	

- 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 28.

### 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
<div style="border: 1px solid black; padding: 2px;"> <div style="background-color: #fff; padding: 2px;">No selection ▼</div> <div style="background-color: #fff; padding: 2px;">No selection</div> <div style="background-color: #fff; padding: 2px;">Internal Input 1</div> <div style="background-color: #fff; padding: 2px;">Internal Input 2</div> <div style="background-color: #fff; padding: 2px;">Prod line 2 problem</div> <div style="background-color: #fff; padding: 2px;">Prod line 2 OK</div> </div>	<input style="width: 80%;" type="text" value="60"/>	<input style="width: 80%;" type="text" value="0"/> <span style="color: red; font-weight: bold;">✗</span>

- 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

- I 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

- I 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.

- I 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

Figure 11. Available information for the input trigger

Figure 12. Available information for the data trigger

- 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 28.

<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

- 2 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

- 1 Select Alarm Handling > Locations and click "Add".
- 2 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.
- 3 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 37.

- 1 Click "Configuration" on the Start page.
- 2 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 - 2

[Expand all entries](#)

Time	Level	Description	Module	Address
2011-04-27 15:18:43	Error	License	WSM3	172.20.13.42 
		All applications stopped		Elise
2011-04-27 13:19:50	Error	Supervision	WSM3	172.20.13.42 
		Lost link to DECT		Elise

Error Relay

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 Fault List				
Module Supervisor				
Code	Status	Persistent	Seriousness	
7-3-16	Start of module	No	Information (Defe	<a href="#">Previous</a>
3-3-7	Reoccurring application failure	Yes	Critical (Default)	<a href="#">Factory</a>
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 (110)

1 .. 25 [26](#) .. [50](#) [51](#) .. [75](#) [76](#) .. [100](#) [101](#) .. [110](#) [Next](#)

[Expand all entries](#)

Time	Level	Description	Module	Address
2011-04-27 15:18:43	Error	License All applications stopped	WSM3	172.20.13.42 Elise
2011-04-27 15:18:43	Individual Reset	No error	WSM3	172.20.13.42 Elise
2011-04-27 13:19:50	Error	Supervision Lost link to DECT	WSM3	172.20.13.42 Elise
2011-04-27 13:18:59	Information	License Module running in demonstration mode	WSM3	172.20.13.42 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

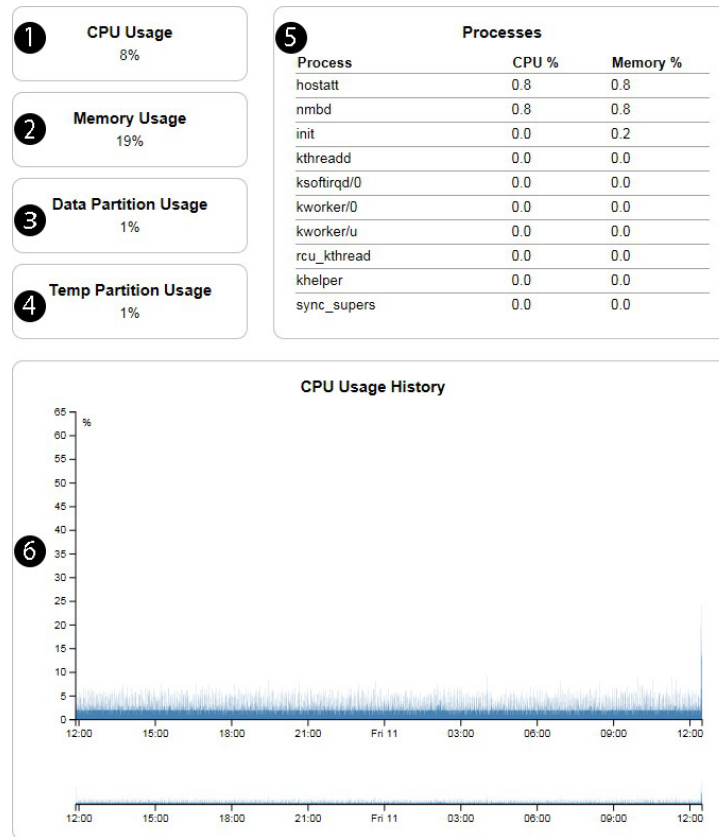
- 1 Enter the timeout in minutes (0-1000 minutes), the default value is 10 minutes.  
If no Status Logs should be blocked, set the timeout to 0.
- 2 Click “Set timeout” to save the setting.  
An incoming fault will now be handled the first time it is received and then blocked during the set timeout.

#### 4.6.6 Module Performance Overview

Information about the module’s CPU usage and memory usage can be shown. This information can for example be used for the following purposes:

- View history of CPU usage the latest 24 hours (approximately)
- Test module performance in a new installation at a site
- Troubleshooting (for example to view why the module is running slow)

- 1 Click “Configuration” on the start page.
- 2 Select Status > Module Performance.



- (1) Shows the average usage of CPU.
- (2) Shows the current RAM usage.
- (3) Shows the current usage of non-volatile memory (internal memory or SD card).
- (4) Shows the current usage of the disk partition where the applications on Unite CM temporarily store files.
- (5) Shows the CPU usage and memory usage currently used by each process. The ten processes that use most CPU are shown the list sorted by CPU usage (descending order).
- (6) Shows history of CPU usage. The upper graph is a detailed view of the lower graph.

NOTE: The graph is not supported by Internet Explorer 8 or lower.

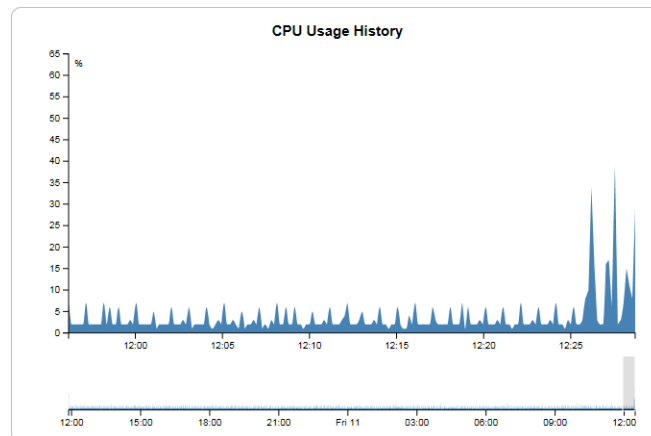
NOTE: The usage information is not refreshed automatically. However, the information is refreshed each time the page is visited.

#### View graph details

The details in the lower graph can be shown by marking a part in the lower graph as follows:

Hover the cursor over the lower graph until the cursor changes to **+** and then mark the part of the graph to be viewed. The marked part in the graph is indicated by a gray square.

Figure 13. Example of part of graph that is marked



Approximate 24 hours of CPU usage history can be shown.

#### 4.6.7 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 <input type="text"/>	IP Address <input type="text"/>
Hardware ID <input type="text"/>	Status 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 14. Search Result for Registered VoWiFi Handsets

## WLAN Portables

4 portables were found

<div>Remove IP</div>		<div>Delete Selected</div>		<div>Export Result</div>	
<input type="checkbox"/>	<div><div>Address/Number</div><div></div></div>	<div>IP Address</div>	<div>Status</div>	<div>Last login</div>	
<input type="checkbox"/>	4323	10.111.118.63	Available	2016-06-21 09:28:16	<div></div>
<input type="checkbox"/>	4324	10.111.118.64	Available	2016-06-21 09:31:38	<div></div>
<input type="checkbox"/>	4325	10.111.118.65	Available	2016-06-21 09:33:37	<div></div>
<input type="checkbox"/>	4330	Not logged in	Available	2016-06-20 18:51:21	<div></div>

- Address/Number – shows the number of a handset
- IP Address – shows the IP address of a handset that is logged in to WSM3.
- 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 WSM3.

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 in due to lost connection to WSM3.

### 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 or Delete a VoWiFi Handset

- 1 Select the handset(s) check box in the search result list.
- 2 Click “Remove IP Address” or “Delete Selected”.
  - Remove IP Address  
Used for refreshing the address of 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
Delete

Address/Number	IP Address	Current status
4325	10.111.118.65	Available
<div style="display: flex; justify-content: space-between;"> <div> <b>Hardware ID</b> 00013E19186F         </div> <div> <b>Last login</b> 2016-06-21 09:33:37         </div> <div> <b>Manual Absent</b> Off <span>▼</span> </div> </div>		
		<span>Save</span>

### 4.6.8 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 40.
- 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”.

### 4.6.9 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.

For log encryption, first import the CA certificate that was used for signing the Syslog server certificate. See [Import Trusted Certificates](#) on page 22.

- 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 To enable log encryption, select Enable in the “Encryption” field and select the CA certificate that was used for signing the Syslog server certificate.
- 5 Click the “Add Syslog entry” button.
- 6 Enter the Syslog Server’s IP address in the text field.
- 7 Click “Save”.

## 4.7 Module Redundancy

### Administer Activity Log

Realtime export

A redundant system consists of an active module and a standby module. When setting up the redundancy in the system, the primary WSM3 will act as an active module, and the secondary WSM3 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 WSM3.

### Prerequisites

In order to set up module redundancy in the WSM3, the following requirements must be fulfilled:

- The installed software version (3.52 or higher) must be identical on both modules.
- The WSM3 must use the same type of SD memory card.
- The primary WSM3 must support module redundancy (license dependent feature).
- The secondary WSM3 must be an empty WSM3 Basic module without any licenses and 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](#).

### Licensing for Module Redundancy

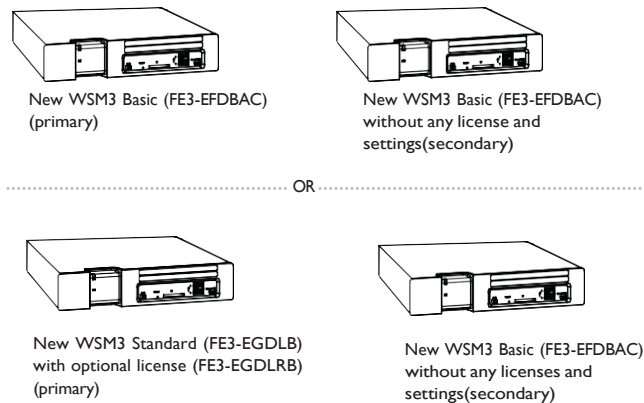
The following licenses can be used for module redundancy:

*Scenario 1:*

**Prerequisites:** Your current system has no WSM3 modules and you would like to add two modules to make your system redundant.

Depending on wanted functionality, the following modules can be combined in a redundant system.

Figure 15. Redundancy with two new modules.

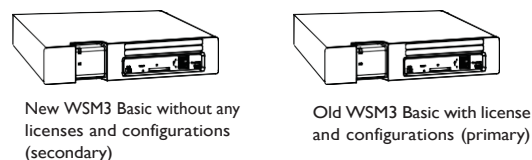


- If only WSM3 Basic modules are to be used. Install a primary WSM3 Basic (FE3-EFDBAC) and a secondary WSM3 Basic (FE3-EFDBAC) without any licenses and configurations.
- If a WSM3 Standard is to be used as primary module, add a WSM3 Basic (FE3-EFDBAC) and then upgrade it with the following licenses to obtain a WSM3 Standard with module redundancy: FE3-EGDLRB and FE3-EGDLB. Add then another WSM3 Basic (FE3-EFDBAC) to be used as secondary module. The latter module must not have any licenses and configurations.

#### Scenario 2:

Prerequisites: Your current system has one WSM3 Basic (FE3-EFDBAC) and you would like to add an additional module to make your system redundant.

Figure 16. Redundancy with WSM3 Basic modules.

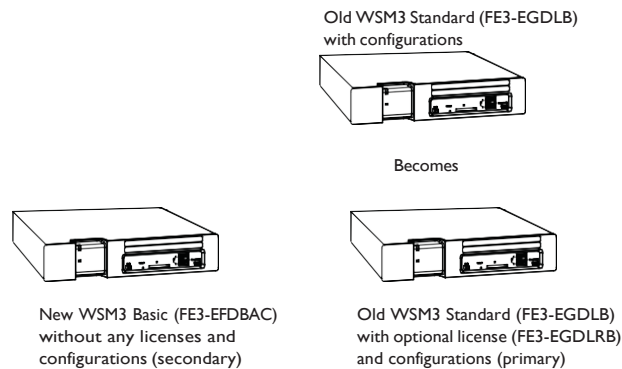


- 1 Order one new WSM3 Basic (FE3-EFDBAC).
  - 2 Add the new WSM3 Basic, but do not install any licenses or configure this module.
- The modules are now prepared to be used as primary- and secondary modules. Continue with additional configuration that are described below.

#### Scenario 3:

Prerequisites: Your current system has one WSM3 Standard and you would like to add an additional module to be used as secondary module.

Figure 17. Redundancy with WSM3 Basic and WSM3 Standard modules.



- 1 Make the WSM3 Standard module as primary module by adding the FE3-EGDLRB license.
- 2 Add a WSM3 Basic (FE3-EFDBAC) module to be used as secondary module. This module must not have any licenses and configurations.

The modules are now prepared to be used as primary- and secondary modules. Continue with additional configuration that are described below.

#### Prepare IP addresses

**NOTE:** It is assumed that your system already have one WSM3 installed and that an additional WSM3 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 WSM3.
- the third IP address will be used by the equipment (for example Access Points) to communicate with the active WSM3 when the system has become redundant. In this document, the third IP address will be called "virtual IP address".

**NOTE:** The primary-, secondary- and virtual IP addresses must be on the same subnet. Otherwise, the communication between the modules will not work properly.

**NOTE:** If a firewall is used between a redundant WSM3 and an application/system connected to that WSM3, the IP port 3217 (UDP) has to be open for communication for the primary-, secondary- and virtual IP addresses.

The equipment that communicates with WSM3 must have the WSM3's IP address configured. To avoid changing the WSM3's IP address in the equipment, follow the instructions below:

#### Network without DHCP Server

- 1 Replace the IP address in the origin WSM3 with the static IP address to be used by the primary WSM3. The replaced IP address can now be used as virtual IP address by the external equipment.
- 2 Make sure the other WSM3 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 WSM3 no longer is reserved to the WSM3'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 WSM3 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 WSM3 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 WSM3 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:** If this is the very first time module redundancy shall be activated, make sure that both SD memory cards are fully formatted (FAT32) before inserting them in the modules. If this is a re-activation, make sure that the SD memory card of the secondary module is fully formatted (FAT32) before inserting it in the secondary module.

- 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 WSM3.
- 6 In the *Network monitor IP address* text field, enter the IP address of the equipment to be used as network reference. The WSM3 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 G. Network Monitoring in a Redundancy System](#) on page 165.

- 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 WSM3 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 primary WSM3 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 WSM3 sends configuration settings to the secondary WSM3 that in turn reboots to apply the settings. After the reboot, the data will be synchronized with the secondary WSM3'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 WSM3 is fully operational.

The LEDs on each WSM3 indicate the status of the synchronization.

Figure 18. 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 WSM3, *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 WSM3 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 WSM3 that currently is active. Note that no configuration can be done on a WSM3 that is in standby mode.

#### 4.7.2 Redundancy Test

- I 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 [4.7.4 Fallback to the Primary WSM3](#) on page 49.

NOTE: When switching between primary- and secondary WSM3, 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 Configuration](#) on page 69.

#### 4.7.3 Restrictions on an Active Secondary Module

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

- The secondary module can only be up and running as active module for 30 days without a repaired primary module connected. It is strongly recommended to switch back to the primary one as soon as possible due to restrictions apply on the secondary one.  
For example; if the secondary module is shut down day 10, it can still use the remaining twenty days when it is started again.

IMPORTANT: If the repaired primary module is not connected within 30 days, the secondary module will become a standby module which means that no module is active.

- 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

#### 4.7.4 Fallback to the Primary WSM3

When a secondary WSM3 has become an active one, it will switch back to the primary WSM3 when the secondary one goes down. It is possible to manually switch back to the primary WSM3 when it is in standby mode after repair.

NOTE: The network monitoring setting might affect the fallback behavior, see [G.1 Fallback behavior when network monitoring is not used](#) on page 166.

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 WSM3, 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 Configuration](#) on page 69.

#### 4.7.5 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.

#### 4.7.6 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 deactive" to perform the deactivation. Both WSM3s 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 WSM3 to its origin IP address. NOTE: If DCHP server is used, ask your network administrator to reserve the IP address to the module's MAC address.
  - If the IP address was changed in the equipment with configured WSM3 IP address, change to the origin IP address.

**IMPORTANT:** Do not remove the SD memory card from the WSM3 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.

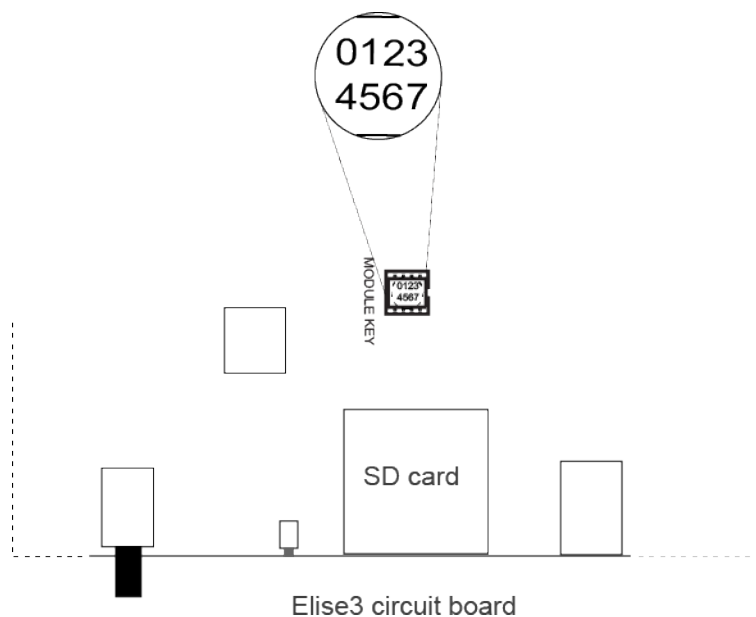
**IMPORTANT:** The secondary WSM3 module will revert back to factory settings and use internal flash as storage after redundancy has been deactivated.

#### 4.7.7 Replacement of Broken WSM3 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](#).

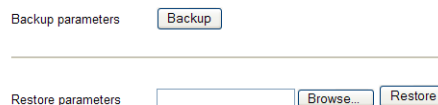
When the primary module is up and running, it will synchronize with the secondary module, that currently is the active one.

#### 4.8 Back up the Configuration

This instruction is used to backup the Device Manager database and the configuration of the WSM3. 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 WSM3 is up and running after a restart. When WSM3 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 server, from a handset in the system.

For information about entering phonebook entries, see [4.1 Manage Central Phonebook Entries](#) on page 25.

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 LDAP server depends on the LDAP server used, see table below.

	Local Database	LDAP 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.

#### 5.4 Select Central Phonebook Database

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

- 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 25 or 4.1.4 on page 26.
- If LDAP server is selected, continue in chapter 5.5 *LDAP Parameter Setup* on page 54.

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”.

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 WSM3 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 56.

- 1 Click the *LDAP settings* link.

The screenshot shows a 'Phonebook' configuration window with the following fields and controls:

- LDAP Server or Proxy Address:** Text field containing '0.0.0.0'. To its right are 'Previous' and 'Factory' buttons.
- Port Number:** Text field.
- LDAP Connection Security:** Dropdown menu set to 'No encryption'.
- Authentication Method:** Dropdown menu set to 'Anonymous'.
- User name:** Text field.
- Password:** Text field.
- Search Base DN:** Text field.
- Number Attribute:** Text field.
- Type of Name Attribute(s):** Dropdown menu set to 'One containing both first and family name'.
- Name Attribute(s):** Text field containing 'cn'.
- LDAP Search Timeout:** Text field containing '15'.
- Error message:** Text field containing 'Unable to reach LDAP database'.
- Buttons:** '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 leaved 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 *LDAP Search Timeout* field, enter the maximum time WSM3 can process search results received from LDAP. The minimum value is 15 seconds, the maximum value is 60 seconds.
- 13 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

- LDAP directory in VoIP Gateway

Figure 19. Settings for LDAP Directory in the VoIP Gateway

Phonebook		
LDAP Server or Proxy Address	<input type="text" value="172.20.9.219"/>	<a href="#">Previous</a>
Port Number	<input type="text" value="389"/>	<a href="#">Factory</a>
Authentication Method	<input type="text" value="Simple"/>	
User name	<input type="text" value="ldap-guest"/>	
Password	<input type="password" value="•••••"/>	
Search Base DN	<input type="text" value="cn=PBX0"/>	
Number Attribute	<input type="text" value="e164"/>	
Type of Name Attribute(s)	<input type="text" value="One containing both first and last name"/>	
Name Attribute(s)	<input type="text" value="cn"/>	
Error message	<input type="text" value="Unable to reach LDAP database"/>	
<a href="#">Activate</a>		<a href="#">Cancel</a>

- Active directory 2003

Figure 20. Settings for Active directory 2003

Phonebook		
LDAP Server or Proxy Address	<input type="text" value="172.20.9.219"/>	<a href="#">Previous</a>
Port Number	<input type="text" value="389"/>	<a href="#">Factory</a>
Authentication Method	<input type="text" value="Simple"/>	
User name	<input type="text" value="ldap-user"/>	
Password	<input type="password" value="•••••"/>	
Search Base DN	<input type="text" value="cn=Users,dc=smallbusiness,c"/>	
Number Attribute	<input type="text" value="telephoneNumber"/>	
Type of Name Attribute(s)	<input type="text" value="Separate attributes for first and last name"/>	
Name Attribute(s)	<input type="text" value="givenName"/> <input type="text" value="sn"/>	
Error message	<input type="text" value="Unable to reach LDAP database"/>	
<a href="#">Activate</a>		<a href="#">Cancel</a>

5.6 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.

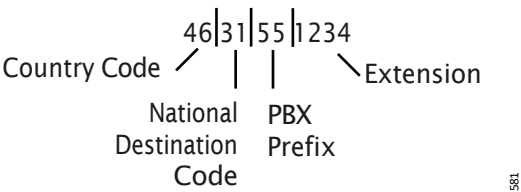
The following formats are currently supported:

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 21.



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

Figure 22. Example of Digit Manipulation Settings

The screenshot shows a 'Phonebook' configuration window. It contains several settings for digit manipulation, each with a help icon (a question mark in a square) and a text input field. The settings are:

- Digit Manipulation:** A checkbox that is currently checked.
- Digit Manipulation Enabled:** A dropdown menu set to 'Yes'.
- Country Code:** A text input field containing '46'.
- National Destination Code:** A text input field containing '31'.
- International Prefix:** A text input field containing '00'.
- National Prefix:** A text input field containing '0'.
- External Line Prefix:** A text input field containing '00'.
- PBX First Prefix:** A text input field containing '55'.
- PBX Second Prefix:** A text input field containing '56'.
- Maximum size of internal phone numbers:** A text input field containing '4'.
- Minimum size of global phone numbers:** A text input field containing '11'.

At the top right of the window are two buttons: 'Previous' and 'Factory'. At the bottom are two buttons: 'Activate' and '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 require a WSM3 Standard license, see [1.2 Variants of the WSM3 Product](#) on page 1. [1.3 Items for AIWS2](#) on page 3.

The serial interface included in the WSM3 makes it possible to receive pagings 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 D. Protocol Limitations](#) on page 153

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 147.

6.1 Serial Protocol Settings

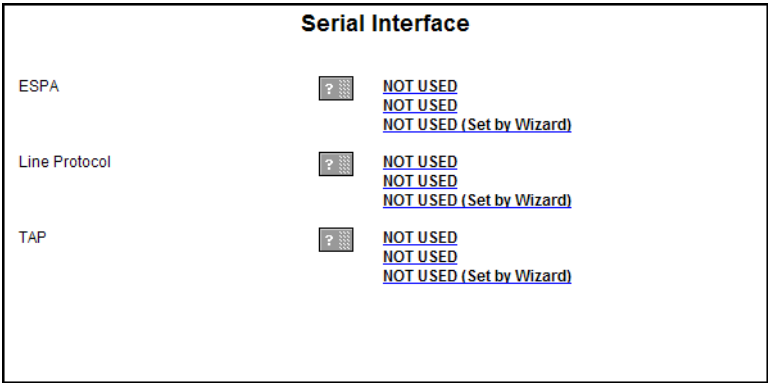
Basic protocol settings are configured in the setup wizard. Detailed and more advanced settings can be configured from the *Advanced Configuration* page.

- 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) Default: None 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). 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 <i>Call Terminated call status</i> . 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. Max 3600 seconds Default: 0
ASCII conversion table:	Makes it possible to convert display message characters.

- 2 Click "Activate".

### 6.1.2 Line Protocol

- I 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) Default: None 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. 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. Default: Yes
Start character:	Start character for the message. Default: < (3C Hex)

End character:	End character for the message. Default: > (3E Hex)
Record separator character:	Record separator character for the message. 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) Default: None 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. Default: 2 beeps
Default urgency:	If set to High "Stand-by" mode in receiver is broken through. Default: Normal.
Transmission delay (x10 ms): (Advanced)	How long to wait before transmission to receiver. Default: 30 milliseconds
Enable checksum validation: (Advanced)	Set to "No" if, for example, external equipment. uses an algorithm that differ from the 7-bit value used in TAP. Default: Yes

Delay time before log on timeout occurs: (Advanced)	How long to wait before disconnecting the external equipment. Valid values: 0-127 where 0 means 'Not enabled'. Default 8 seconds
Delay time before block timeout occurs: (Advanced)	How long this module shall wait before hanging up. Valid values: 0-127 where 0 means 'Not enabled'. Default 4 seconds.
Numbers of allowed times to log on: (Advanced)	How many logon attempt from external equipment shall be permitted. Valid values: 1-127. Default 3 tries.
Numbers of allowed checksum failures: (Advanced)	How many checksum failures from external equipment shall be permitted. Valid values: 1-127. Default 3 tries.
Numbers of allowed timeouts: (Advanced)	How many timeouts shall be permitted. Valid values: 1-127. 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 69.

Figure 23. Device Manager in WSM3



- 1 Click "Device Manager" on the start page. A Login window opens.
- 2 Enter User ID and Password. Click "OK".

### 7.1 Start Device Manager in Java Runtime Environment

Device Manager must be started on a machine with a Microsoft Windows operating system in Java Runtime Environment. Device Manager supports Oracle Java Runtime Environment (subscription needed) and the free open source licensed Eclipse Temurin from Adoptium.

#### Device Manager in Oracle Java Runtime Environment

To start Device Manager in Oracle Runtime Environment:

- 1 Ensure Oracle JRE is installed on the machine.
- 2 Log in on the Unite start page and click **Device Manager**.
- 3 Click **Open** to start Device Manager.

#### Device Manager in Eclipse Adoptium Environment

NOTE: The procedures below describe installing Eclipse Temurin and the IcedTea-Web plugin on a machine with the Microsoft Windows 10 operating system.

##### Install Eclipse Temurin

- 1 Download version 8 of Eclipse Temurin JDK at <https://adoptium.net/temurin/releases/?version=8>.
- 2 Install **OpenJDK 8 + HotSpot**. Choose default settings + installed feature set JAVA\_HOME variable.

##### Download the IcedTea-Web plugin

The IcedTea-Web plugin is required to start Device Manager from a browser.

- 1 Download IcedTea (x86\_64) from <https://adoptopenjdk.net/icedtea-web.html> and move to **C:\Program Files\Eclipse Adoptium**.

NOTE: The MSI installation file is not supported.

- 2 Add **C:\Program Files\Eclipse Adoptium\jdk-x.x.xxx.xx-hotspot\bin** (where x.x.xxx.xx is the JDK version installed on your computer) to the **PATH** environmental variable (System variables).

- 3 Associate the file type .jnlp with javaws.exe in **C:\Program Files\Eclipse Adoptium\icedtea-web-image\bin\**.

**Start Device Manager in the Eclipse Adoptium environment**

- 1 Log in on the Unite start page and right-click **Device Manager**.
- 2 Select **Save as** and save the file on the machine.
- 3 Right-click the saved file and select **Open with**.
- 4 Select the **Always use this app to open .jnlp files** checkbox.
- 5 Click **More apps**.
- 6 Scroll down to click the **Look for another app on this PC** option.
- 7 Navigate to **C:\Program Files\Eclipse Adoptium\bin** and select **javaws.exe**.
- 8 Click **Yes** in the Security warning window.

Device Manager will start.

To start Device Manager next time, on the Unite start page click **Device Manager** and click **Open** to allow the browser to use the Eclipse Adoptium software automatically.

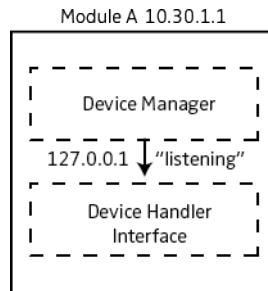
A description of the Device Manager, and how it is intended to be used, is found in a separate document. See *User Manual, Device Manager, TD 93028EN*

## 8. Device Configuration

### 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 WSM3



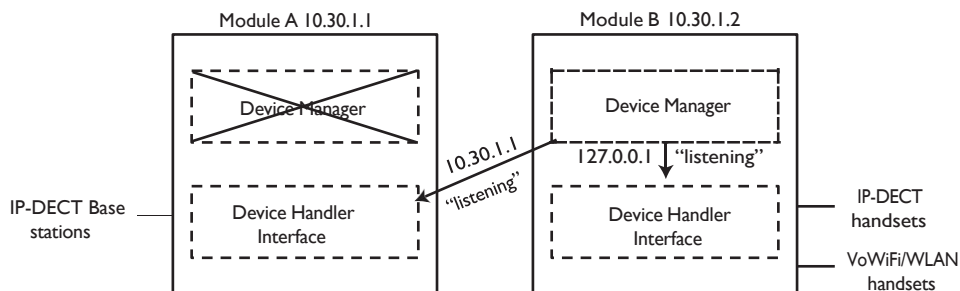
The WSM3 has a Device Manager enabled. All devices that log in to the local Device Handler interface should appear in the WSM3's local Device Manager.

In this case the WSM3 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 WSM3, 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 WSM3



The Device Manager in WSM3 A is disabled, but enabled in WSM3 B. The devices that logs in to WSM3 A and the devices that log in to WSM3 B should appear in the Device Manager of WSM3 B. In this case, the WSM3 B should point at its local Device Handler and also point at the Device Handler of WSM3 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 WSM3 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 WSM3 A should be left empty.

- 5 Click **Activate**.

### 8.2 Inactivity Timeout

In the **Inactivity Timeout** field it is possible to enter the number of minutes of inactivity that should be allowed before the session expires and the user must log in again. (Allowed values are 10-60 minutes; default is 10 minutes). If the field is left empty the session will not expire.

### 8.3 License Server Communication

This setting determines if the Device Manager should be able to contact the License server to retrieve licenses bought on the License web.

- 1 From the Start page, click **Configuration**.
- 2 Select **Other Settings > Advanced Configuration**.
- 3 Click **Device Management**.
- 4 In the **Enable communication with license server** drop-list, select whether if the communication should be enabled or not.
- 5 Click **Activate**.

### 8.4 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".

## 8.5 Device Relogin Time

All devices send keep alive messages to WSM3 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.

### 8.5.1 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".

### 8.5.2 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".

### 8.5.3 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".

### 8.5.4 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".

#### 8.5.5 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".

### 8.6 Service Discovery

#### 8.6.1 Service Discovery Domain ID

Service Discovery allows automatic detection of WSM3s, devices and services on a network without prior configuration. WSM3s, services and devices that shall belong to a certain WSM3 must be set to the same domain ID.

NOTE: The Service Discovery Domain feature is not available if Secure websocket mode is enabled.

- 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".

#### 8.6.2 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. WSM3 and the devices, that shall belong to that WSM3 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 WSM3'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 [8.6 Service Discovery](#) on page 72). In this case, enable the service discovery in the WSM3 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

The screenshot shows a 'Device Handler Settings' window. It has two main configuration options: 'Enable service discovery?' which is a dropdown menu currently showing 'Yes', and 'Device relogin time (minutes)' which is a text input field containing the number '30'. To the right of these settings are two buttons: 'Previous' and 'Factory'. At the bottom of the window are two buttons: 'Activate' on the left and 'Cancel' on the right.

- 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".

### 8.6.3 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. WSM3 and the devices, that shall belong to that WSM3 have to be set to the same Domain ID.

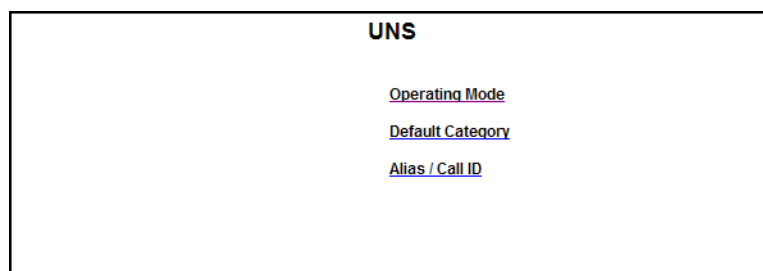
- 1 Click "Configuration" on the start page.
- 2 Select Other Settings > Advanced Configuration in the menu in the on the *Configuration* page.
- 3 Click "WLAN System" under WLAN Interface on the *Advanced Configuration* page.
- 4 In the *Enable service discovery?* drop-down list, select "Yes" if the 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 WSM3 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.

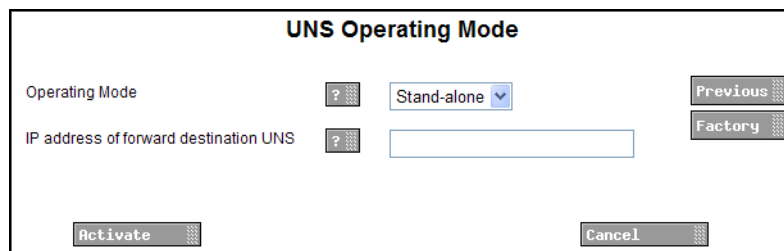
- 1 Click “Configuration” on the start page.
- 2 Select Other Settings > Advanced Configuration on the *Configuration* page.
- 3 Under Other, click “UNS” in the menu on the *Advanced Configuration* page.



#### 9.1.1 UNS Operating Mode

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

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



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

#### 9.1.2 Default Category

The UNS Default Category is used to decide where messages from the WSM3 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 WSM3.

- 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 the WSM3
- 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”.

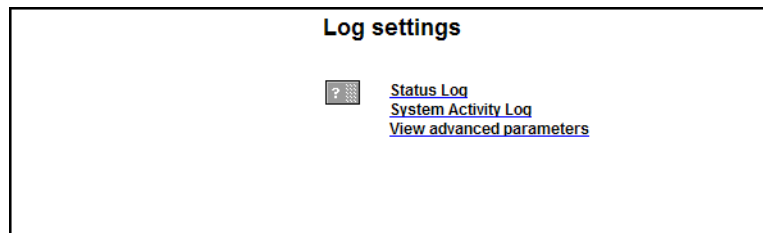
- 2 Click one of the links.

- 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 WSM3 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 WSM3.

- 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.

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.

I Under Time, click “Set time”

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.

3 Under Common, click “Network” in the menu on the *Advanced Configuration* page.

- 4 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.
  - Configure hosts.

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

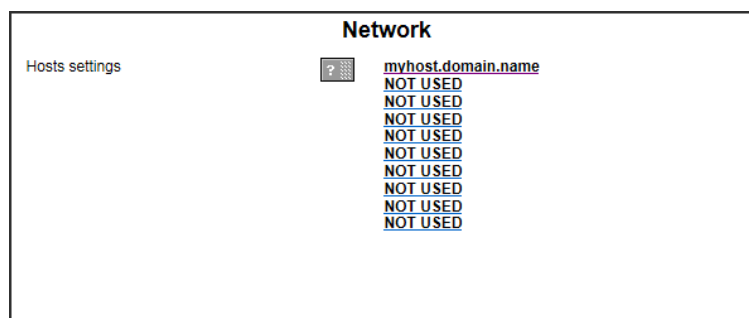
- 5 Click "Activate".

#### 9.4.1 Hostname Mapping

The Unite module has a hostname list that can be used for mapping up to ten hostnames to their IP addresses. The Unite module looks first in the hostname list, and if a matching hostname is found, the IP address mapped to that hostname is used to establish a connection. If no matching hostname is found in the list, the Unite module sends a request to the DNS server (if any).

The hostname list can be used if no DNS is available, or if the DNS server cannot resolve certain hostnames for some reason.

- 1 Click "Configuration" on the start page.
- 2 Select Other Settings > Advanced Configuration on the *Configuration* page.
- 3 Click "Network" under Common on the Advanced Configuration page.
- 4 Click "Map hostnames to IP address".
- 5 Click "NOT USED" to add a new hostname to the list. If you want edit a hostname, click the link labelled as the hostname.



- 6 In the "Hostname" field, enter the hostname to be resolved, e.g. "www.mycompany.com".
- 7 In the "IP address" field, enter the IP address that shall be mapped to the hostname.

**Host entry**

Hostname  Previous

IP address  Factory

Activate Cancel

- 8 Click "Activate".

The Unite module must reboot to apply the setting. Click the link "Click here to reboot" and then click "Reboot". 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.

**Host entry**

**The following changes have been made.**

You must reboot to activate the changes.  
[Click here to reboot.](#)

Hostname

IP address

NOTE: Reboot can be done once after all hosts configured.

## 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".

## 9.6 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.

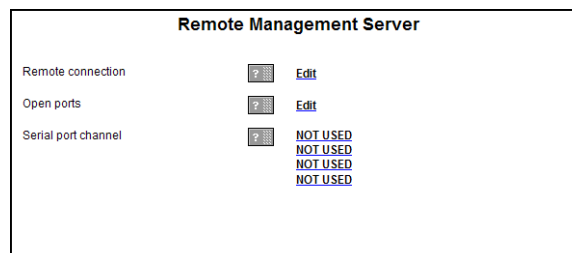
NOTE: If the Reboot page is reloaded, this will trigger another reboot.

## 10. Remote Management

A remote connection to a customer site can be established through the WSM3. This makes it possible to configure and maintain sites, independent of distance.

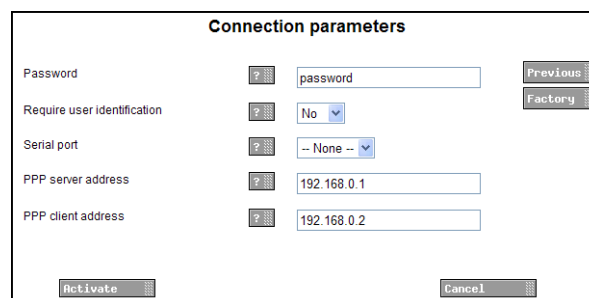
To be able to connect remotely, the remote management server in the module has to be configured. The help text buttons in the GUI will give more information about each parameter settings.

- 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



### Remote connection

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



- 2 Set up the connection parameters.

NOTE: The default password is "password".

- 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.

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.

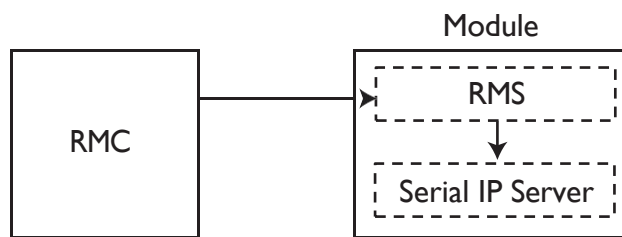
One serial port channel for each tool has to be set up. Web based configuration tools do not require serial port channels.

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

The configuration of the remote management server is described in detail in the document **Function Description, Remote Management**.

### 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 WSM3’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.

**Serial-IP Server**

Protocol Version: ? 2.0

Buttons: Previous, Factory, Activate, Cancel

- 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

### 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 WSM3 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 WSM3 has a valid license.

See also [4.6.7 WLAN Handsets](#) on page 40.

#### 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 WSM3 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 14.

- 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 WSM3 OAP license.

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.

#### OAP Server settings

- 1 Click "Configuration" on the start page.
- 2 Select Other Settings > Advanced Configuration in the menu on the *Configuration* page.
- 3 Click "OAP".
- 4 In the "Delivery response policy" field, select:
  - "Completion only" if no delivery confirmation from the handset is required.
  - "Completion + delivery receipt" if the OAP server requires delivery confirmation from the handset.
- 5 In the "Include user of device in OAP messages" field, select whether the first and last names of a user logged in to a handset should be sent to the OAP client.
- 6 In the "OA protocol version" field, select what protocol of OAP is supported. This parameter determines what TCP ports are enabled for OAP messages.

**IMPORTANT:** If this parameter is changed, the OAP server will restart and clients will be disconnected. This may result in messages being lost.

- 7 Select "Activate".

#### OAP encryption parameters

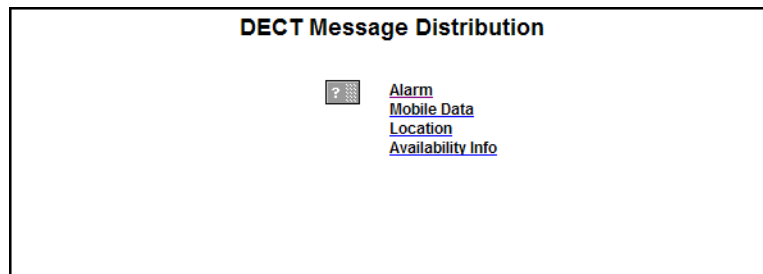
The OAP server can support either secure only or both secure and unsecure connections. For secure connections, AES-256 encryption is used.

- 1 Click "Configuration" on the start page.
- 2 Select Other Settings > Advanced Configuration in the menu on the *Configuration* page.
- 3 Click "OAP".
- 4 Click "OAP encryption parameters".
- 5 In the "Communication policy" field, select:
  - "Secure" to enable secured connections only.
  - "Both secure and unsecure communicated allowed" to enable any connections.
- 6 To add a device or a service that requires secured connection to the OAP server, click "NOT USED".
- 7 In the "Name". field, enter a device or service identifier that is used in the OAP message header according to the OAP protocol. The maximum length of the identifier is 128 characters. The name can include the following characters A-Z, a-z, 0-9.

- 8 In the “Pre-shared key” field, enter a 32-character long shared key. The key can include the following characters: A-Z, a-z, 0-9.
- 9 Select “Activate”.
- 10 Repeat steps 6-9 to add more devices or services with secured connection if needed.
- 11 Select “Activate”.

#### 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”.

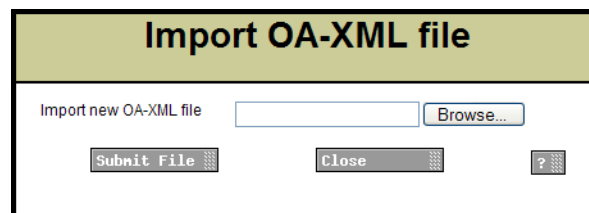


- 5 Enter the address xxx.xxx.xxx.xxx/OAP in one of the address fields.
- 6 Click “Activate”.

### 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.



- 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.

### 14.1 DECT Phone Systems

#### 14.1.1 IP-DECT

Figure 24. 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 DECT Interface Settings

The DECT Interface controls the messaging flow between the Cordless Telephone System and the WSM3.

### 14.2.1 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:

- Extended Activity Log  
In addition to when a Unite block is delivered to a handset, activity log information is also sent to Log Viewer in the Unite Connectivity Manager (Unite CM) when the block is received by the DECT interface. The extra information can only be displayed in Log Viewers that are updated continuously, and if activity logs are configured in the Unite CM. This function should be used with care as it generates heavier network load. For more information about extended activity logs.
- 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
- Priority Conversion  
Used to convert messaging priorities; Alarm, High, Normal and Low. This conversion is normally only used for compatibility with some PWT handsets and should never be enabled unless you are absolutely sure.
- DECT Interface  
This parameter makes it possible to disable the DECT Interface on the WSM3. 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.

#### 14.2.2 System Dependent Settings

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

To find IP-DECT settings, see [14.2.1 General Settings](#) on page 91.

##### 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.

#### 14.2.3 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
- 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.

---

<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".

#### 14.2.4 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:
 

<ul style="list-style-type: none"> <li>- Standard SMS (Compatibility Mode)</li> <li>- Latin-I</li> <li>- UTF-8</li> </ul>	<p>Standard SMS works with all handsets but some special characters may not be correct.</p> <p>Used for later generation of handsets.</p> <p>Used for later generation of handsets. Use UTF-8 to include characters that is not included in the Latin-I character set.</p>
---	--
- 5 Click "Activate".

#### 14.2.5 DECT WebSocket Connectivity

These settings determine how IP-DECT systems communicate with the AIWS2.

##### General Settings

To configure general settings that apply to all configured IP-DECT systems, perform the following steps:

- 1 Click "Configuration" on the Start page.
- 2 Select Other Settings > Advanced Configuration in the menu on the *Configuration* page.
- 3 Select "WebSocket Connectivity" under DECT Interface in the menu on the *Advanced Configuration* page.
- 4 In the "General settings" field, click "Edit".
- 5 In "Secure websocket mode", select:
  - "Enabled", if only secure access via WS channel is allowed for IP-DECT devices.
  - "Disabled", if any connection via WS channel is allowed.

NOTE: When the "Secure websocket mode" setting is changed, the WebSocket Connectivity service and SMS Center service are rebooted.

- 6 In the "High priority supervision timeout (seconds)" field, enter how often a supervision request should be sent to the devices that request high priority supervision timeout. By default, it is set to 60 seconds. The range of values is from 30 to 1000 seconds.
- 7 In the "Medium priority supervision timeout (minutes)" field, enter how often a supervision request should be sent to the devices that request medium priority

supervision timeout. By default, it is set to 5 minutes. The range of values is from 5 to 60 minutes.

- 8 In the “Low priority supervision timeout (minutes)” field, enter how often a supervision request should be sent to the devices that request low priority supervision timeout. By default, it is set to 60 minutes. The range of values is from 30 to 1000 minutes.
- 9 Click “Activate”.

### Authentication Settings

If the Secure WebSocket mode is enabled, configure authentication settings individually for each IP-DECT system:

- 1 Click “Configuration” on the Start page.
- 2 Select Other Settings > Advanced Configuration in the menu on the *Configuration* page.
- 3 Select “WebSocket Connectivity” under DECT Interface in the menu on the *Advanced Configuration* page.
- 4 To add authentication settings for a new IP-DECT system, click “NOT USED”.
- 5 In the “Description” field, enter a name of IP DECT system.
- 6 In the “Authentication user ID” field, enter the user ID that IP-DECT base station uses to log in. Each IP-DECT system in the list shall use unique user ID.

NOTE: The corresponding user ID must also be configured on the device.

- 7 In the “Authentication password” field, enter the password that IP-DECT base station uses to log in. The password must match the programmatic password policy, see [3.3.3 Set Programmatic Password Policy](#) on page 38.

NOTE: The corresponding password must also be configured on the IP-DECT base station.

- 8 Click “Activate”.

#### 14.2.6 IP-DECT Device Handling

This setting determines if 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. AIWS2 and the devices that shall belong to that AIWS2 have to be set to the same Domain ID.

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

The IPBS can use either the AIWS2’s IP address or the Service Discovery Domain ID to log on to the wanted Device Manager. This chapter is only applicable when Service Discovery Domain ID is to be used.

NOTE: The Service Discovery Domain feature is not available if Secure websocket mode is enabled.

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 [8.6 Service Discovery](#) on page 72). In this case, enable the service discovery in the AIWS2 in order to log on the IPBS to the Device Manager that matches the Domain ID.

All devices send keep alive messages to AIWS2 to remain logged in. How often the devices should send the messages can be configured. For example, 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.

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

**Device Handler Settings**

Enable service discovery? ? Yes ▼

Device relogin time (minutes) ? 30

Previous  
Factory

Activate Cancel

station uses service discovery to find the Device Manager.

- 5 Enter how often (in minutes) the device should send a keep alive message in the Device relogin time field. Legal values: 10 - 1440.
- 6 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 WSM3 used, refer to the Configuration Manual for respective VoWiFi handset.

### 15.2 Shared Phones

When using shared phones all VoWiFi handsets authenticates with passwords. The password can be a common password for all users or the call number. Individual passwords are supported by the User Server in Unite CM. Unite CM is available from Ascom.

In order to work, all shared phones in a system need to have the same “major” version in the software version.

If a User Server is used the operating mode for the UNS must be set to “forwarding” and the User Server must be specified as the forwarding destination.

### 15.3 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 WSM3.  
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 WSM3 has three authentication alternatives; “Common password”, “User server” and “Number as password”.
- **Common Password**  
A common password can be specified in the WSM3, 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.  
The password can only consist of numeric characters (0-9).  
If individual passwords are needed, for example for shared phones, passwords can either be specified in a User Server or the individual call numbers can be used, refer to chapter [15.2 Shared Phones](#) on page 96.
- **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 97.

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.

#### 15.4 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.

#### 15.5 User Server

WSM3 can set a user server for authentication of handsets, see [15.3 WLAN System](#) on page 96.

- 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”.

#### 15.6 WLAN Websocket Connectivity

These settings determine how handsets communicate with the WSM3.

##### General Settings

To configure general settings that apply to all handsets using the WLAN interface, perform the following steps:

- 1 Click “Configuration” on the Start page.
- 2 Select Other Settings > Advanced Configuration in the menu on the *Configuration* page.

- 3 Select “WebSocket Connectivity” under WLAN Interface in the menu on the Advanced Configuration page.
- 4 In the “General settings” field, click “Edit”.
- 5 In “Secure websocket mode”, select:
  - “Disabled”, if the secure websocket mode is not required.
  - “Enabled - allow legacy”, if only secure access via the websocket channel is allowed but devices that are already connected in insecure mode are still reachable. This option is preferable if you change the mode from Disabled.
  - “Enabled - secure only”, if only secure access via websocket channel is allowed for handsets.

NOTE: When the “Secure websocket mode” setting is changed, the WebSocket Connectivity service is rebooted.

- 6 In the “High priority supervision timeout (seconds)” field, enter how often a supervision request should be sent to the devices that request high priority supervision timeout. By default, it is set to 60 seconds. The range of values is from 30 to 1000 seconds.
- 7 In the “Low priority supervision timeout (minutes)” field, enter how often a supervision request should be sent to the devices that request low priority supervision timeout. By default, it is set to 60 minutes. The range of values is from 30 to 1000 minutes.
- 8 In the “Client certificate validation” drop-down list, select whether the server refuses connection from devices without a certificate signed with an appropriate CA certificate. The CA certificate must be uploaded to the server first, otherwise, the parameter cannot be enabled. When the parameter is changed, currently connected clients must connect again.
- 9 Click “Activate”.

### Authentication Settings

To log in the handsets to the WSM3, they have to authenticate themselves with shared key common for all handsets. The shared key to be entered in the handsets is configured in the WSM3.

There are two types of authentication settings that can be configured in WSM3:

- Temporary authentication credentials
- Permanent authentication credentials

If the Secure WebSocket mode is enabled, configure authentication settings individually for each group of handsets:

- 1 Click “Configuration” on the Start page.
- 2 Select Other Settings > Advanced Configuration in the menu on the Configuration page.
- 3 Select “WebSocket Connectivity” under WLAN Interface in the menu on the Advanced Configuration page.
- 4 To add authentication settings for a group, click “NOT USED”.
- 5 In the “Description” field, enter a name of the group.
- 6 In the “Authentication user ID” field, enter the user ID that handsets in the group use to log in. Each group in the list shall use unique user ID.

NOTE: The corresponding user ID must also be configured on the handset.

- 7 In the “Authentication password” field, enter the password that the handsets of the group use to log in.

NOTE: The corresponding password must also be configured on the handset.

- 8 Click “Activate”.

#### Temporary authentication credentials

NOTE: If the WSM3 is rebooted, the temporary authentication credentials will be restored to the default credentials.

NOTE: The Temporary authentication credentials functionality is not available if any of the following conditions is met:

- The “Client certificate validation” parameter is enabled. See [General Settings](#) on page 98.
- The “Check client certificate” parameter is enabled. See [3.4.1 Web Access Security Settings](#) on page 16.

- 1 Click “Configuration” on the Start page.
- 2 Select Other Settings > Advanced Configuration in the menu on the Configuration page.
- 3 Select “WebSocket Connectivity” under WLAN Interface in the menu on the Advanced Configuration page.
- 4 Click “Temporary Authentication”.

#### Temporary Authentication

##### Authentication shared key

Enter the shared key required for the handsets to log in to Unite CM.

##### Timeout

Enter how long time the temporary authentication should be enabled. When the time elapsed, the temporary authentication is disabled. Legal values: 1 - 1440 minutes.

##### Start temporary authentication

To enable temporary authentication with the above given shared key and time out, click the “Start” button. To disable temporary authentication, click the “Stop” button.

- 5 Enter the shared key required for the handsets to log in to WSM3 in the “Authentication shared key” text field.
- 6 Enter the time handsets can use the temporary authentication credentials in the “Timeout” text field. Allowed values: 1 - 254 minutes.
- 7 To allow handsets using the temporary authentication credentials, click the “Start” button. These credentials can now be used until the timeout time has elapsed. If you want to disallow handsets to use these credentials before the timeout time elapsed, click the “Stop” button.

NOTE: If the WSM3 is rebooted, the temporary authentication credentials will be restored to the default credentials.

### Example

A site has handsets that already have logged in to WSM3 by using the permanent authentication credentials configured by an administrator. New handsets with factory settings should also log in, but instead of changing the credentials in each new handset you can allow them to log in by using the credentials configured in the factory. This is made by configuring temporary authentication credentials, that match the ones configured in the new handsets.

By doing this the administrator does not need to change the permanent authentication credentials used by already logged in handsets. The advantage is that already logged in handsets can keep their credentials and new handsets can log in with temporary credentials.

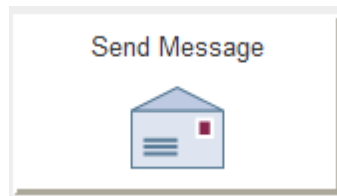
To configure the new handsets to use the permanent authentication credentials after the very first log in, that credentials can be configured for each handset in the Device Manager. When the handsets synchronize with the Device Manager, the temporary authentication credentials are replaced by the permanent ones.

## 16. 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:

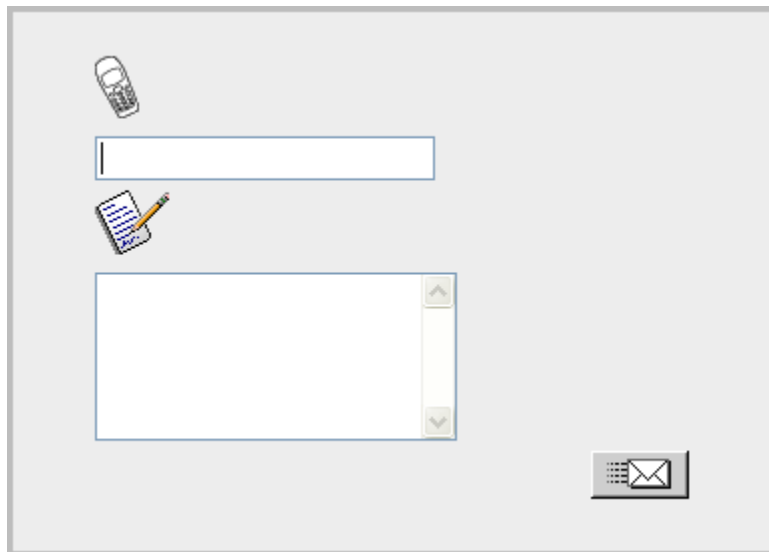
- Messaging Tool - included if the license does not include NetPage
- NetPage - requires the WSM3 Standard license




### 16.1 Create and Send Messages via the Messaging Tool

The Messaging Tool GUI is displayed without additional license.

*Figure 25. Messaging Tool GUI.*



- 1 Click "Send Message" on the start page. The Message Tool opens.
- 2 Enter Call ID in the upper text field.
- 3 Enter message in the bottom text field.
- 4 Click . The message is sent to the receiver.

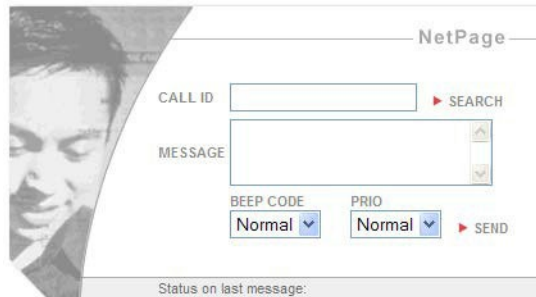
### 16.2 Create and Send Messages via NetPage

NOTE: Requires a variant that includes 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”.

### 16.3 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.

#### 16.3.1 Create a Predefined Message

- 1 Click the “Common Messages” or “My Messages” button in *NetPage*. For “Common Messages” enter the “user” credentials.
- 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.

### 16.3.2 Edit a Predefined Message

- 1 Click the “Common Messages” or “My Messages” button in *NetPage*. For “Common Messages” enter the “user” credentials.
- 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.

## 16.4 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

## 16.5 Predefined Groups

NOTE: This functionality is only accessible from index4, see [figure 35](#) on page 121.

### 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

### 16.5.1 Create a Group

- 1 Click the “Common Groups” or “My Groups” button in *NetPage*. For “Common Groups” enter the “user” credentials.
- 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.

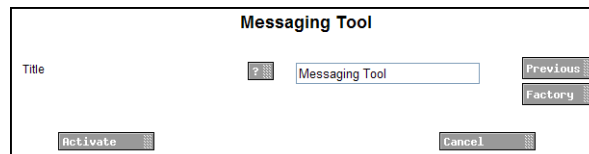
#### 16.5.2 Edit a Group

- 1 Click the “Common Groups” or “My Groups” button in NetPage. For “Common Groups” enter the “user” credentials.
- 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.

### 16.6 Messaging Tool Configuration

It is possible to change the title of the Messaging Tool web page.

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

The screenshot shows a dialog box titled "Messaging Tool". It has a "Title" label on the left, followed by a small icon of a speech bubble with a question mark, and then a text input field containing the text "Messaging Tool". To the right of the input field are two buttons: "Previous" and "Factory". At the bottom of the dialog box are two buttons: "Activate" on the left and "Cancel" on the right.

- 4 Enter text to be shown as title. Click “Activate”.

### 16.7 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

Call ID range - Lower limit:

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

Previous Factory

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 user login is required for NetPage.
- **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, Index1, Index2, Index3, Index4, or Index5. If the default GUI parameter is set to "Custom", then the index.html page from the module's FTP area is used as start page for NetPage. See [17.3 Customize the User Interface \(GUI\)](#) on page 115 for more information.

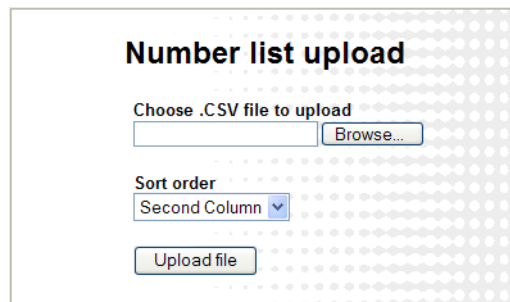
### Creating or Updating the Number list

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 the “user” account. 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.

#### 16.7.1 Colored messaging

It is possible to add color information in messages sent to handsets. The beep code in a message is mapped to a color. When this feature is enabled, color information will be added to all transmitted messages.

NOTE: All handset types do not support colored messaging. See the handset’s Data Sheet for more information.

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

The image shows a 'Parameter setup' dialog box with the following settings:

Setting	Value
Coloured Messaging enabled	Yes
Silent	None
1 beep	None
2 beeps	None
3 beeps	None
4 beeps	None
5 beeps	None
10 beeps	Blue
Siren	Red

Buttons: Previous, Factory, Activate, Cancel.

- 4 In the Colored Messaging enabled drop-down list, select to “Yes” if color information shall be added to messages according to the settings in step 5.
- 5 Map which colors that shall correspond to the different beep codes. These colors are displayed with messages in the handsets.
- 6 Click “Activate”.

#### 16.7.2 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 [17.3.2 Files for Translation/Editing](#) on page 116.

##### Restore

- 1 Put copies of the backup files in the NetPage FTP area, see [17.3.2 Files for Translation/Editing](#) on page 116.
- 2 Test that NetPage is functioning properly, see [17.4 Test the New User Interface](#) on page 125.

##### Backup of Predefined Groups and Messages

NOTE: The default user account is “user” 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 the “user” account.)

### 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 the “user” account.)
- 4 Test that NetPage is functioning properly, see [17.4 Test the New User Interface](#) on page 125.

## 17. 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 [17.1.2 Translate/Edit the Language](#) on page 111)
- Hide unused functionality (refer to [17.3.5 Change the NetPage User Interface Functionality](#) on page 119)
- Modify the user interface to suit the customer's image (refer to [17.3 Customize the User Interface \(GUI\)](#) on page 115)
  - Limit the number of characters included in the message text.
  - Add company logo and/or modify the GUI to suit the customer's image.
  - Define a custom message to appear on the login page.

NOTE: The user interface only supports the Latin-I 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.

## 17.1 Customize the Language

### 17.1.1 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.

### 17.1.2 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).

### 17.1.3 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.

- I 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".

#### 17.1.4 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.

#### 17.1.5 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](#)

#### 17.1.6 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 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”.

#### 17.2 Customize User Login Message

You can set a custom message to appear on the Login page.



- 1 Click "Configuration" on the start page.
- 2 Select Other Settings > Advanced Configuration in the menu on the *Configuration* page.
- 3 Under the "Common" section, click "Login message".
- 4 In the "Login message text" field, enter the message to appear on the login page.
- 5 Click "Activate" to save the changes.

The user login message text is shown on the login page on the next login.

### 17.3 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.

#### 17.3.1 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.

### 17.3.2 Files for Translation/Editing

- I Log on to the module via an FTP client. Note that how to log on can differ between different FTP clients.<sup>1</sup>

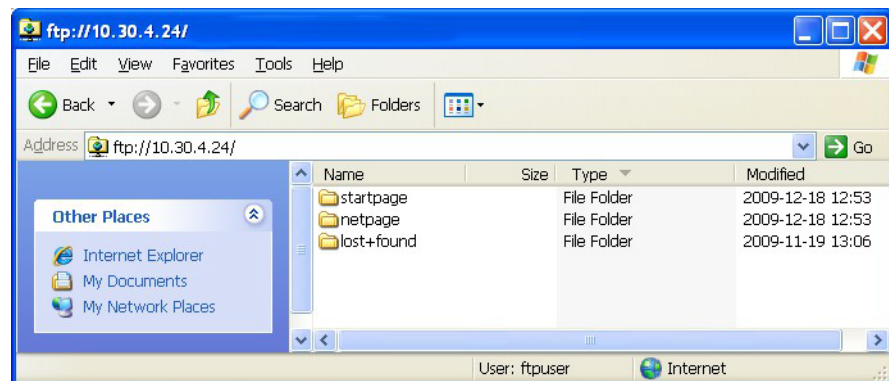
Default username is “ftpuser” and default password is “changemetoo”.  
xxx.xxx.xxx.xxx is the host name.

*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 FTPS are allowed. HTTP is automatically redirected to HTTPS, and FTP access is not allowed. The FileZilla Client freeware (not included) supports FTPS. See [3.4.1 Web Access Security Settings](#) on page 16.

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.

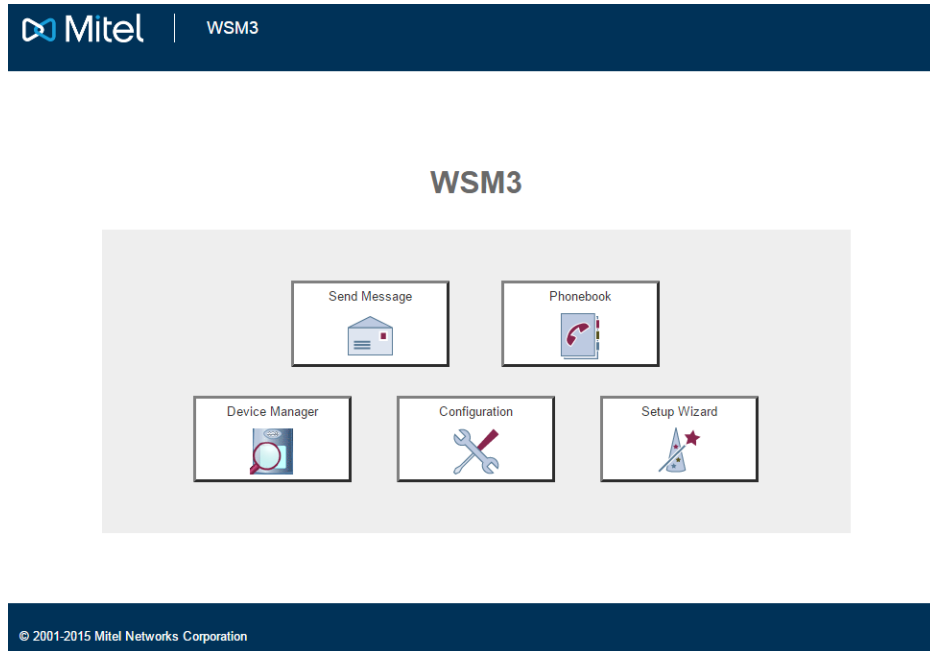


When restoring NetPage files, the files shall be placed in the same folder.

<sup>1</sup>Internet Explorer is not an FTP client. It can be used for viewing but not for transferring files.

### 17.3.3 Default Start Page GUI

Figure 30. Start page default user interface (index\_template)

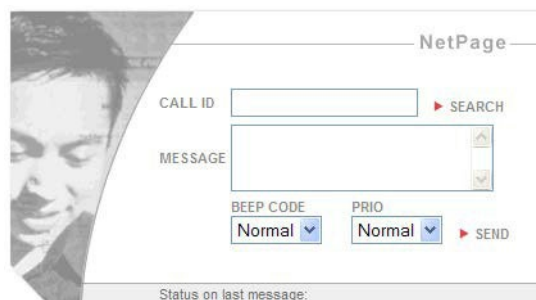


A copy of the default Start page is stored in the start page folder on the module's FTP area. The start page copy *index\_template*, is an html file that can be copied and edited. The start page can also be replaced with a completely new user interface.

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.

### 17.3.4 Default Send Message GUI

Figure 31. NetPage default user interface (index3).



By clicking "Send Message" on the start page, the default NetPage user interface *index3.html* is opened.

A customized NetPage user interface can be used. Set the Default GUI parameter to 'Custom' on the NetPage Configuration (refer to [16.7 NetPage Configuration](#) on page 105), and the *index.html* page from the module's FTP area will be used as the start page for NetPage.

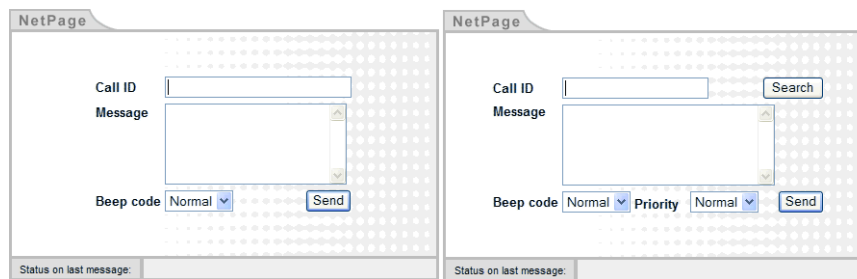
In the NetPage folder on the module's FTP area, there are four examples of the NetPage user interface: *index\_example1*, *index\_example2*, *index\_example3* and *index\_example4*. Initially, the *index.html* is a copy of the default NetPage user interface (Index3).

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 [17.3.5 Change the NetPage User Interface Functionality](#) on page 119.

The index4 page message history area, which runs as a Java Applet, requires Java Runtime Environment and the Internet Explorer browser. The Index5 page message history area does not require Java Runtime Environment and can be run in any browser except for Internet Explorer.

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 121.

Figure 32. NetPage user interface examples: index1 and index2



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, on the Index 4 page, 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

### 17.3.5 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) -->
```

088

For comments included in the Java Script code, the comment mark “//” is used, see [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'
  tmp1ist = document.testform.callnolist;
```

089

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 default user interface (index4) it is necessary to open and change one or more of the files: “send.html”, “receive.html” and “admin.html”. To change index 5, it is necessary to open and change one or more of the files: “send.html”, “receivesse.html” and “adminsse.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 [17. Administration of Language and User Interfaces](#) on page 110.

### 17.3.6 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. Netpage user interface on the *index5* page is translated in the “language.js” file. See [figure](#) on page 121 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 [17.3.2 Files for Translation/Editing](#) on page 116.
- 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 [17.3.7 Upload the Files to the module's FTP Area](#) on page 122.
- 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 [17.3.2 Files for Translation/Editing](#) on page 116.
- 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 [17.3.7 Upload the Files to the module's FTP Area](#) on page 122.
- 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 Administrate 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 [17.3.2 Files for Translation/Editing](#) on page 116.
- 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 [17.3.7 Upload the Files to the module's FTP Area](#) on page 122.
- 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”.

### 17.3.7 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 16, only secure access via HTTPS and FTPS are allowed. HTTP is automatically redirected to HTTPS, and FTP access is not allowed. The FileZilla Client freeware (not included) supports FTPS.

- 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.

### 17.3.8 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.

### 17.3.9 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 [17.3.6 Translation of the User Interfaces](#) on page 120.

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 1 delivery receipt 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>.

- 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 123.
- 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 [17.3.2 Files for Translation/Editing](#) on page 116.

### 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 123.
- 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 [17.3.2 Files for Translation/Editing](#) on page 116.

NOTE: This is not applicable when index4 example is used as default GUI.

#### 17.4 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.

#### 17.5 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.

## 18. Software Administration

Besides the software administration via the WSM3'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 WSM3. 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.

### 18.1 Upgrade the Boot Software

For instruction on how to upgrade the WSM3 hardware with new Boot software (autoupdate.bin) refer to the Installation Guide for WSM3.

### 18.2 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.

### 18.3 Switch Software

If two software versions are installed on the WSM3 you can switch between them. When switching to another software, the WSM3 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.

#### 18.3.1 Switch software in a non-redundant system

This section describes how to switch software when module redundancy is disabled.

- 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".

### 18.3.2 Switch software in a redundant system

This section describes how to switch software when module redundancy is enabled.

You can only switch software when both Software 1 is identical and Software 2 is identical on the both WSM3. Additionally, both WSM3 must be also be synchronized.

NOTE: If you switch software from a secondary WSM3 that is active, the primary one becomes active and the secondary one enters standby mode when the system is up and running after the reboot.

- 1 Click “Configuration” on the start page.
- 2 Select Other Settings > Redundancy in the menu on the *Configuration* page.
- 3 Click “Switch software”.

## 18.4 Install New Software

It is recommended to always perform a backup before installing new software, see [18.4.1 Create a Software Backup](#). After the software installation see also [17.5 Update the User Interface after a new Release](#) on page 125.

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.

### 18.4.1 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.

## 19. Troubleshooting

### 19.1 General Troubleshooting

#### 19.1.1 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:

- 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 Click "View Info Log" or "View Error Log".

#### 19.1.2 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 5. If you do not have the correct software versions installed, contact your system administrator.

#### 19.1.3 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 145 for a description of used ports.

#### 19.1.4 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 16, only secure access via HTTPS and FTPS is allowed. HTTP is automatically redirected to HTTPS and FTP access is not allowed. The FileZilla Client freeware (not included) supports FTPS.

## 19.2 NetPage Troubleshooting

Fault	Probable cause	Action or comment
• My Groups and My Messages do not work.	– Cookies are not allowed in your web browser.	Check that cookies are enabled in your web browser.
• Number list or Common Messages are unsatisfactorily updated	---	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.
• Entire Message history including column headings doesn't appear	– The Java Virtual Machine may be missing on your computer.	– Install Java on the computer, See the data sheet WSM3 for more information about supported Java versions.
• Message history is not running, although messages are sent and column headings are visible.	– There might be a firewall preventing you from receiving data from the NetPage server.	Contact your IT department to open port number 5891 in the fire wall, in the direction from the web client to the NetPage server.
• Translation into language with character encoding UTF-8 is not displayed correctly in the NetPage's GUI.	– The software has been upgraded. The newer software has inherit the older software's settings (for example by using the "Copy current settings" option).	Open the html files used by Netpage (located on the FTP area) in WordPad or similar text editor.  Change the character encoding in the files to this:  <meta http equiv= "Content-Type" content="text/html; charset=utf-8">

## 19.3 Troubleshooting Guide

This section lists a number of possible faults, probable causes and suggested actions.

### 19.3.1 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> </ul>	Configure the system to connect to a time server.
	<ul style="list-style-type: none"> <li>The time server is configured but is offline.</li> </ul>	Restore connection to time server.
	<ul style="list-style-type: none"> <li>The web browser is selected as time source but the time has not been set by the user.</li> </ul>	Set the time via the advanced configuration.
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 76).</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. Multiple devices are currently being updated.</li> </ul>	Connect the handset to the Device Manager either via a advanced charger or via a DECT system supporting OTA. 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.
<ul style="list-style-type: none"> <li>File downloads retrying.</li> </ul>	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.

Fault	Probable cause	Action or comment
<ul style="list-style-type: none"> <li>• Software downloads rejected.</li> </ul>	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/ 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.
<ul style="list-style-type: none"> <li>• Software downloads are aborted.</li> </ul>	Wrong file selected for download to devices (External web server).	<ul style="list-style-type: none"> <li>– Make sure that the URL to the desired software is correct and retry.</li> <li>– Make sure that the file is intended for that device.</li> </ul>
<ul style="list-style-type: none"> <li>• Low software download performance to handset inserted in charger.</li> </ul>	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.
<ul style="list-style-type: none"> <li>• Communication failure to device.</li> </ul>	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.
<ul style="list-style-type: none"> <li>• No connection available for the Device Manager GUI.</li> </ul>	<ul style="list-style-type: none"> <li>– Max number of Device Manager GUI's has been reached.</li> <li>– The Device Manager server side is restarted due to reconfiguration.</li> <li>– The Device Manager is temporarily unavailable due to restore of database.</li> <li>– The network is preventing the GUI from connecting to the server.</li> </ul>	<ul style="list-style-type: none"> <li>Close the other Device Manager GUI to open new. A maximum of three Device Manager GUIs can be connected.</li> <li>No Action, the server will be up within a few minutes.</li> <li>No Action, the server will be up soon.</li> <li>No action.</li> </ul>

Fault	Probable cause	Action or comment
<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.	<ul style="list-style-type: none"> <li>– Assign a new number to the device.</li> <li>– Associate a new or existing number to the current device</li> </ul>
<ul style="list-style-type: none"> <li>• The handset is not visible in the Number tab.</li> </ul>	<ul style="list-style-type: none"> <li>– The handset has no number associated.</li> <li>– The device is offline and not saved as number.</li> </ul>	<ul style="list-style-type: none"> <li>Assign or associate a number to the device.</li> <li>Bring the device online. Save the number in order to make it possible to edit the number when it is offline.</li> </ul>
<ul style="list-style-type: none"> <li>• Number creation of desired device type is not possible.</li> </ul>	The .pkg file for the desired device type is not imported to the Device Manager.	Import the .pkg file for the desired device type. The file is provided by the supplier.
<ul style="list-style-type: none"> <li>• It is not possible to apply a template at creation of new number.</li> </ul>	No compatible template for the desired device exists.	Create a new template or upgrade an existing template and retry.
<ul style="list-style-type: none"> <li>• A handset logs out when placed in an advanced charger</li> </ul>	The device manager configurations in the IPBS and the advanced charger are not the same.	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.

Fault	Probable cause	Action or comment
<ul style="list-style-type: none"> <li>The handset does not log on to the device manager OTA.</li> </ul>	– The Domain ID is not set correctly in the IPBS.	Reconfigure it to match the device manager Service Discovery parameter Domain ID.
	– The system does not support service discovery.	Erase the Domain ID in the IPBS and set the IP address to the Device Manager under Advanced Settings > Device Management.
Fault message <i>Device Manager: Running-application problem (Error relay: Database init in progress)</i> is shown after software upgrade of the WSM3.	You have upgraded the WSM3 with a software that uses another database structure for the Device Manager than the previous installed software version.	The WSM3 needs to re-configure the database used by the Device Manager after the upgrade.
		The time it takes to re-configure the database depends on number of parameters, devices, phonebook entries, and numbers saved in the database.  It can take up to several hours.

### 19.3.2 General Troubleshooting for the WSM3


This part of the Troubleshooting Guide lists possible faults that are not connected to the Device Manager

Fault	Probable cause	Action or comment
<ul style="list-style-type: none"> <li>It is not possible to edit the Central Phonebook.</li> </ul>	– 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.
<ul style="list-style-type: none"> <li>Import of language to the configuration GUI fails.</li> </ul>	The language file has the wrong format.	Export the default language to set the format and edit the language file.
<ul style="list-style-type: none"> <li>Set language fails.</li> </ul>	– 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.




















Fault	Probable cause	Action or comment
• 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 WSM3 system.	– The IP address to WSM3 has not been set in all base stations.	Enter the correct WSM3 IP address in the base stations.
• Module key and MAC address are not shown in the System Information on the Troubleshooting page on a standby module of a redundant system.	The standby module in a module redundant system cannot display this information in the System Information on the Troubleshooting page.	Known limitation in a module redundant system. To see module key and MAC address, go to the main page on the standby module.




#### 19.4 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.

Tools	Description
LEDs	The LEDs show different colors to determine type of information and have different flashing frequency for showing the priority
	<b>colors</b>
	Red                      Fault indication
	Yellow                  Mode indication
	Blue                     Normal operation (OK)
	<b>Flashing frequency</b>
	Fixed light              indicates normal state
	Slow flashing light    indicates medium attention
	Quick flashing light   indicates high attention

## Flashing patterns

		Status LED				Mode LED				Power LED		
Status OK	Blue											
Starting up/shutting down	Blue											
Feedback (1 sec.)	Blue											
Error/fault	Red											
Warning	Red											
Boot mode	Yellow			Blue								
Demonstration mode	Yellow			Blue								
Active module during synchronization	Red							Blue				
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 35.

**Fault logging:** Refer to [4.6.4 Fault Log](#) on page 37 and [4.6.5 Administer the Fault Log](#) on page 38.

**System Information:** See [19.5 Advanced Troubleshooting](#) below.

## 19.5 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”.

## 19.6 What to consider when replacing a module

- IP Address
- License
- Module key
- Remember where cables were connected

## 19.7 Technical Support

For technical support please contact your local representative.

## 20. Related Documents

- *13/1531-ANF90114 Mitel IP-DECT\_System (12.1.5) Installation and Operation.pdf*
- *32/1531-ANF90143 Mitel Base Station & IPBL, Installation Guide.pdf*
- *51/1551-ANF90114 Mitel IP-DECT\_System Planning.pdf*
- *52/1551-ANF90114 Mitel IP-DECT\_System Description.pdf*
- *15/1531-ANF90114 Mitel WSM3\_Installation and Operation.pdf*

## 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.

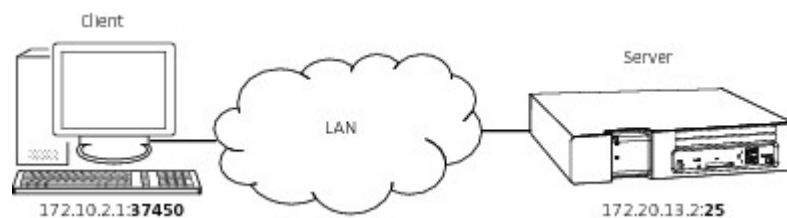
The table below describes the well-known port used by the application/unit acting as server.

### Example 1:

In this example the FTP area on the WSM3 should be accessed. An FTP client installed on a computer is used to access the FTP area. In this case, the WSM3 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. WSM3 acting as a server

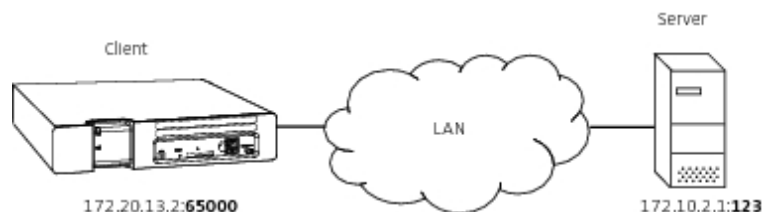


### Example 2:

In this example, the WSM3 should obtain time and date from an external source acting as a NTP server. In this case, the WSM3 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. WSM3 acting as a client



*Table 2. IP ports used by applications/units acting as server*

Port	Application or unit	Transport protocol
20–21	FTP	TCP
53	Domain Name Server (DNS) License Web Server communication	UDP
68	DHCP	UDP
80	Web traffic (HTTP) License Web Server communication	TCP
113	Authentication	TCP
123	Network Time Protocol (NTP)	UDP
443	HTTPS License Web Server communication	TCP
514	Syslog Syslog messages	UDP
1321–1322	OAP Server	TCP
5891	NetPage	TCP
8080	HTTP	TCP
10089	Ascotel I6	UDP
10101	Remote connection - TCP and RS232 conversion	TCP
10103	Remote connection - Communication between Remote Access Client and Remote Access Server	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

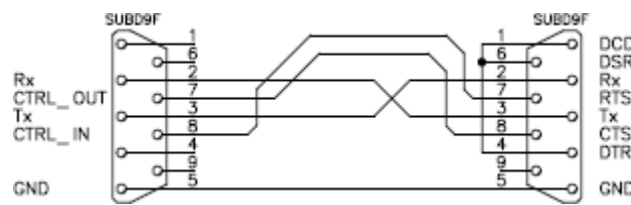
Figure 38.



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 WSM3 for ESPA in, Ascom Line protocol and TAP in and also for ESPA out and TAP out.

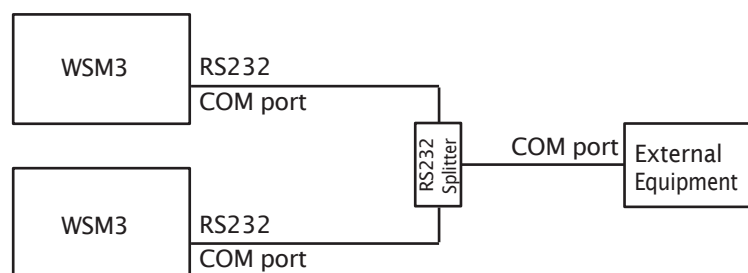
Figure 39.



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 WSM3 and the secondary WSM3. By using a RS232 data splitter the cable can be branched to both modules.



## Appendix C. Alarm Action Configuration Examples

This appendix presents examples on how alarm actions can be configured.

### C.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.

#### C.1.1 System Components

##### One WSM3

2 inputs have been defined in the Input/Output Setup.

- Cold-storage, door open
- Cold-storage, door closed

2 outputs have been defines 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.

##### Outputs

ID	Output Name	Module Address	Output Initial State	
1	Cold-storage lamp	127.0.0.1	Internal 1	High (open-collector) ▼ Reset
2	Siren	127.0.0.1	Internal 2	High (open-collector) ▼ Reset

##### Inputs

ID	Input Name	Module Address	Input	Activation	Activation Time
1	Cold-storage, door open	127.0.0.1	Internal 1	On Opening ▼	120
2	Cold-storage, door closed	127.0.0.1	Internal 2	On Opening ▼	

Save Cancel

### C.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

Push-button Alarm from 1440

Notes

Triggers

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

Alarm Trigger

Alarm Type

Push-button double press

Number

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

Siren

Duration (s)

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	

SaveCancel

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	

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).

### C.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 120 seconds, a message is sent and a lamp above the door is lit.

Two alarm actions are created. One that handles the alarm called "Cold-storage room open" and one called "Cold-storage room closed"

#### Cold-storage room 1, door open

Input Triggers: "Cold-storage door 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.

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 Trigger

Input	Repetition Time (s)	Max No. of Repetitions
Cold-storage, door open	60	0

Add

Actions

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

Output action

Add

Activate Output

Output	Duration (s)
Cold-storage lamp	3600

Send Message

Call ID	Message Text	Beep Code	Priority
1440	[inputDescr]	2 beeps	Normal

SaveCancel

For Activate Output Action, the duration is here set to max value 3600.

Cold-storage room door closed

Figure 45. 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 46. Summary of Alarm Actions

Alarm Actions

Number of triggers: 4 (250)

Name	Notes	Triggers		
Push-button alarm from 1440		Alarm Type: Push-button double press (Push-button alarm 1 and 2), Number: 1440		
Alarm cancellation		Data: 1440		
Cold-storage room closed		Input: Cold-storage, door closed		
Cold-storage room open		Input: Cold-storage, door open		

## Appendix D. Protocol Limitations

This appendix describes a number of protocol specific limitations.

### D.1 ESPA 4.4.4

The implementation only supports point-to-point connection. Dial-up connection or multiprop connection are not supported.

#### D.1.1 Functionality

The protocol consists of **blocks** which consist of **records** which consist of **data**.

#### D.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*

(Block 7, Ascom and Ericsson paging dialect):

This block is not supported. The block is NAK:ed if received.

*Request for module key number*

(Block 9, Ascom and Ericsson dialect):

This block is not supported. The block is NAK:ed if received.

#### D.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*

(Record 5, standard ESPA):

This record is accepted but ignored since it is not applicable in DECT or VoWiFi systems.

*Mailbox number*

(Record A, Ericsson paging dialect):

This record is accepted but ignored.

*Infopage*

(Record C, Ascom dialect):

This record is accepted but ignored.

#### D.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.

### D.2 Ascom Line Protocol

#### D.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.

#### D.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.

### D.3 TAP Protocol

#### D.3.1 Functionality

- <ESC>PGI<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.

#### D.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. 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.
Maximum message length:	A TAP transaction block can contain up to 256 characters that includes paging address, paging text, control bits and checksum. 8 characters are allocated for control bits and checksum, and 248 characters are allocated for paging address and paging text (e.g 248 = paging address + paging text).
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 E. 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 WSM3. 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.
Product Information file	xml	A file containing information needed for licensing and upgrade of a handsets.
License file	xml	A file containing license keys for handsets.

## Appendix F. Multiple WSM3 Configuration Examples

This chapter presents configuration examples for multiple modules.

### F.1 More than 2500 devices

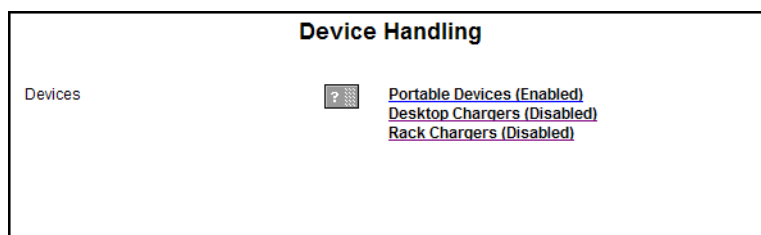
Up to 2500 devices can be configured on each WSM3 module. If more than 2500 devices shall be configured, one possible solution is to use two modules and to register all handsets on one module and the chargers on another module

#### F.1.1 Configuration for the setup

The basic configuration for this setup is described below. In this configuration, only the WSM3-A module has a DECT connection and the DECT interface in WSM3-A is disabled.

- WSM3-A  
Set the Device Manager to handle portable devices only in Configuration > Other Settings > DECT Interface > Device Handling:
  - Portable Devices: Set “Device support” to Enabled
  - Desktop Chargers: Set “Device support” to Disabled
  - Rack Chargers: Set “Device support” to Disabled

Figure 47.



Setting handsets on WSM3-A.

- WSM3-B  
Disable the DECT interface in Configuration > Other Settings > Advanced Configuration > General Settings > View advanced parameters:
  - Set “DECT Interface” to Disabled.

Set the Device Manager to handle chargers only in Configuration > Other Settings > DECT Interface > Device Handling:

- Portable Devices: Set “Device support” to Disabled
- Desktop Chargers: Set “Device support” to Enabled
- Rack Chargers: Set “Device support” to Enabled

#### Example: Migration to a double WSM3 solution

- This example assumes that the original system has all device management on one module. The reason for a migration to a double WSM3 solution is that the number of registered devices will increase to more than 2500, but the number of handsets is expected to remain under 1000. The device management of the chargers will be moved to the new module. In this example, the DECT interface in WSM3-B is disabled.

Change the following settings in the original module:

- WSM3-A  
Set the Device Manager to handle only portable devices in Configuration > Other Settings > DECT Interface > Device Handling:
  - Portable Devices: Set “Device support” to Enabled
  - Desktop Chargers: Set “Device support” to Disabled
  - Rack Chargers: Set “Device support” to Disabled

Do the following settings in the added module:

- WSM3-B  
Disable the DECT interface in Configuration > Other Settings > Advanced Configuration > General Settings > View advanced parameters:
  - Set “DECT Interface” to Disabled.

Set the Device Manager to handle only chargers in Configuration > Other Settings > DECT Interface > Device Handling

- Portable Devices: Set “Device support” to Disabled
- Desktop Chargers: Set “Device support” to Enabled
- Rack Chargers: Set “Device support” to Enabled

To move the device management of the chargers from WSM3-A to WSM3-B:

- Move the templates for the chargers from WSM3-A to WSM3-B (or create new templates on WSM3-B). This can be done by using the Export Template and Import Template function in the Device Manager.
- WSM3-B:  
The chargers will automatically log in to the module. It may take several hours.
- WSM3-A:  
Delete the chargers in the Device Manager.
- If any new devices (portables or chargers) shall be added to the system at this point, it can be done as a normal installation using the Add device feature in the Device Manager.

## F.2 High messaging load in DECT

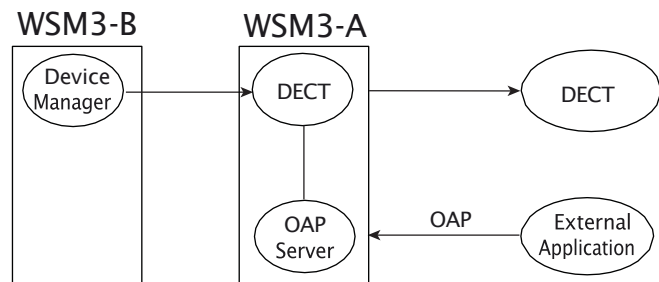
This solution applies to:

- systems with high messaging load
- systems with high requirements on maximum message burst throughput

When the messaging load is too high, a single WSM3 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.

### F.2.1 Configuration for the setup

The basic configuration for this setup is described below.

- WSM3-A  
Disable Device Management in Configuration > Other Settings > Advanced Configuration > Device Management:  
- Remove IP addresses.  
- Click “Activate”.
- WSM3-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 WSM3-A plus “/DECT”, that is, if WSM3-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 WSM3-B

### F.2.2 Migration example to a double WSM3 solution

This example assumes that the original system uses one WSM3 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:

- WSM3-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 WSM3-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:

- WSM3-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 WSM3-A plus "/DECT", that is, if WSM3-A has the IP address 192.168.0.2, change to "192.168.0.2/DECT".
- Click "Activate".

Import all device management data to WSM3-B:

In Device Manager:

- In the menu, select File > Import > Numbers...
- In the menu, select File > Import > Templates...

### F.3 High Messaging load in VoWiFi

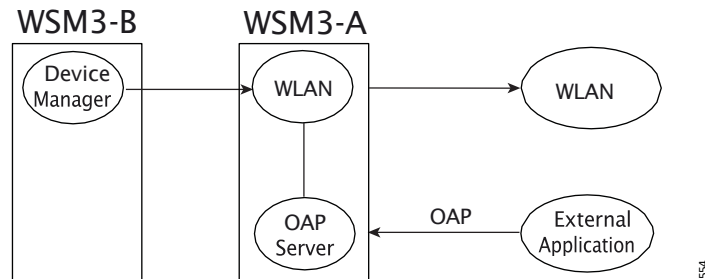
This solution applies to:

- 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 WSM3 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.

### F.3.1 Configuration for the setup

The basic configuration for this setup is described below.

- WSM3-A  
In Configuration > Other Settings > Advanced Configuration > Device Management:
  - Remove IP addresses.
  - Click “Activate”.
- WSM3-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 WSM3-A plus “/WLAN”, that is, if WSM3-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.

### F.3.2 Migration example to a double WSM3 solution

This example assumes that the original system uses one WSM3 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:

- WSM3-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 WSM3-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:

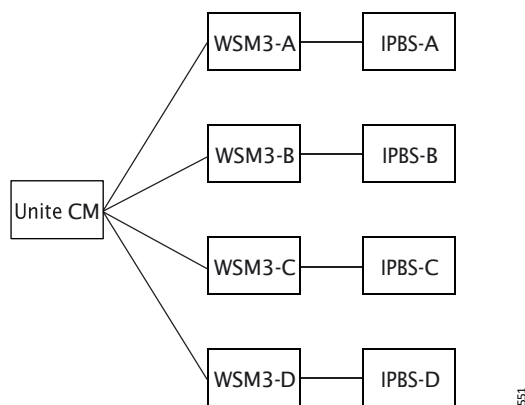
See section [F.3.1 Configuration for the setup](#) on page 161.

- WSM3-B
  - Import all device management data to WSM3-B in Device Manager:
    - File > Import > Numbers.
    - File > Import > Templates...

### F.4 Multi-master IP-DECT systems and Multiple DECT systems

This solution applies to multi-master IP-DECT systems and multiple DECT systems, in combination with a central number plan that is set up in an Ascom Unite Connectivity Manager (Unite CM) module.

Figure 52.



Example of a system with one Unite CM and several DECT/IP-DECT systems

#### F.4.1 Configuration for the setup

The basic configuration for this setup is described below.

- Unite CM setup:  
See *Configuration Manual, Unite Connectivity Manager, TD 92735EN* for details.
- For each DECT or IP-DECT system, configure a “category” for the DECT or IP-DECT system, for example:

Category description	IP address	Service
IPDECT-A	172.20.10.11	DECT
IPDECT-B	172.20.10.12	DECT
IPDECT-C	172.20.10.13	DECT
IPDECT-D	172.20.10.14	DECT

- For each handset, set up a Call ID and add it to the number plan. It can be done for individual handsets or for ranges, for example:

Call ID	Number/Address -> Category
1000	1000 -> IPDECT-A
1001	1001 -> IPDECT-A
2000	2000 -> IPDECT-B
2001	2001 -> IPDECT-B
3001	3001 -> IPDECT-C
4001	4001 -> IPDECT-D

- Set all WSM3s to use the number plan in Unite CM.

Figure 53. 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 Unite Connectivity Manager (here 192.168.0.20).

Click “Activate”. The WSM3 now uses the Unite Connectivity Manager number plan

Setting UNS in WSM3 (in this example the Unite Connectivity Manager uses the IP address 192.168.0.20).

#### F.4.2 Migration example to a Multimaster IP-DECT solution

This example assumes that the original system is a single IP-DECT system with one WSM3 and no Unite CM.

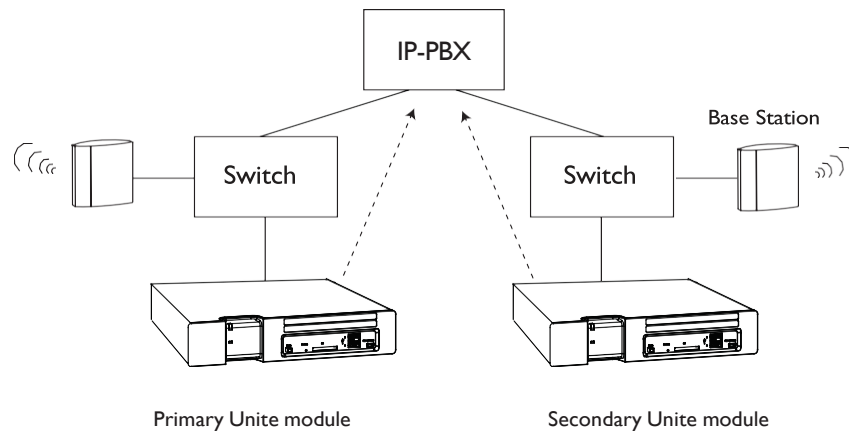
- Configure the Unite CM. For the specific settings for multiple WSM3 modules, see Unite CM setup in [F.4.1 Configuration for the setup](#) on page 163. See *Configuration Manual, Unite Connectivity Manager, TD 92735EN* for details.
- Configure the existing WSM3 to use the number plan in the Unite CM, see [F.4.1 Configuration for the setup](#) on page 163.
- Set up the added IP-DECT system.

## Appendix G. Network Monitoring in a Redundancy System

In a redundant system, both the primary WSM3 and the secondary WSM3 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 WSM3 loses the connection to the network, the standby WSM3 will become active instead.

Figure 54. Illustration of using a centralized equipment as network reference



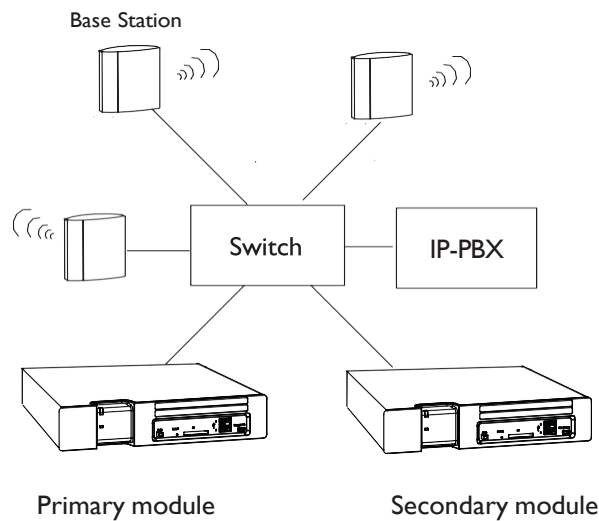
In [figure 54](#), both the primary WSM3 module and the secondary WSM3 are using the IP-PBX as network reference since it is centrally installed in the network.

NOTE: The primary-, secondary- and virtual IP addresses must be on the same subnet. Otherwise, the communication between the modules will not work properly.

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 WSM3, and the other part will write data to the secondary WSM3. This behavior is called “split brain behavior”.

<sup>1</sup>By setting the Network monitor IP address to 127.0.0.1, the function is disabled.

Figure 55. Illustration of a network where no network monitoring is required.



If the primary WSM3 and secondary WSM3 are connected to the same switch (see [figure 55](#)), no equipment (for example an IP-PBX) is needed as network reference. If the secondary WSM3 do not receive any response from the primary WSM3, the primary WSM3 has actually failed and the secondary WSM3 becomes active.

### G.1 Fallback behavior when network monitoring is not used

If the primary WSM3 loses the connection to the LAN (the power source is still connected), the secondary WSM3 takes over as an active one. When the primary WSM3 is reconnected to the LAN, the system switches back to the primary WSM3 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.