

# SIP-DECT OM System Manual

Installation, Administration, and  
Maintenance  
Release 3.0

Document ID: depl-1230

Version: 0.2

Aastra Deutschland GmbH    Zeughofstr. 1  
10997 Berlin, Germany

© 2012 - All Rights Reserved

*No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or information storage and retrieval system, for any purpose without the express written permission of Aastra.*

## Table of Contents

<b>1</b>	<b>OVERVIEW</b>	<b>7</b>
1.1	THE SIP-DECT SOLUTION	7
1.2	ABOUT THE RADIO FIXED PARTS (RFPs)	8
1.2.1	RFP Families	8
1.2.1.1	Former RFP Types (Till SIP-DECT Release 2.1)	8
1.2.1.2	New RFP Types (Since SIP-DECT Release 3.0)	10
1.2.2	RFP only Mode	11
1.2.3	OpenMobility Manager (OMM) Mode	11
1.3	ABOUT THE OPENMOBILITY MANAGER	12
1.3.1	OMM Tasks	12
1.3.2	SIP-DECT Special Features and Capacities	13
1.3.3	OMM Capacities and Features	14
1.4	ABOUT THE PORTABLE PARTS	15
<b>2</b>	<b>GETTING STARTED</b>	<b>17</b>
2.1	SETTING UP DHCP / TFTP	17
2.2	INITIAL SETUP	22
<b>3</b>	<b>ENHANCED FEATURE OVERVIEW</b>	<b>26</b>
<b>4</b>	<b>NAMING CONVENTION</b>	<b>32</b>
<b>5</b>	<b>LOGIN AND PASSWORDS</b>	<b>33</b>
<b>6</b>	<b>LICENSING</b>	<b>34</b>
6.1	LICENSING MODEL	34
6.1.1	Latency Timer	35
6.1.2	License Violations and Restrictions	36
6.1.3	G. 729 License Violations	36
6.2	UPLOADING AN ACTIVATION OR LICENSE FILE	37
6.3	DEMONSTRATION MODE	37
6.4	LICENSE MODES	38
6.4.1	Small System	38
6.4.2	Medium System	38
6.4.3	Large System	39
<b>7</b>	<b>OMM WEB SERVICE</b>	<b>41</b>
7.1	LOGIN	41
7.2	LOGOUT	42
7.3	"STATUS" MENU	42
7.4	"SYSTEM" MENU	43
7.4.1	"System settings" Menu	43
7.4.1.1	Restarting the OMM	46
7.4.1.2	Updating the OMM	47
7.4.2	"SIP" Menu	47
7.4.3	"User administration" Menu	51
7.4.4	"Time zones" Menu	53
7.4.4.1	Changing Time Zones	53
7.4.4.2	Resetting Time Zones	54
7.4.5	"SNMP" Menu	54
7.4.6	"DB management" Menu	55
7.4.6.1	Manual Database Import	56
7.4.6.2	Automatic Database Import	56
7.4.6.3	Manual Database Export	58
7.4.6.4	Automatic Database Export	58
7.4.7	"Event log" Menu	60
7.5	"SITES" MENU	60
7.5.1	Creating a New Site	61
7.5.2	Editing a Site	61
7.5.3	Deleting a Site	61
7.6	"RADIO FIXED PARTS" MENU	62
7.6.1	States of an RFP	63

7.6.2	OMM / RFP SW Version Check .....	64
7.6.3	Creating and Changing RFPs.....	64
7.6.4	Importing RFP Configuration Files .....	67
7.6.5	Capturing RFPs .....	68
7.6.6	Deleting RFPs.....	69
7.7	“PORTABLE PARTS” MENU.....	69
7.7.1	Creating and Changing PPs.....	70
7.7.2	Importing PP Configuration Files.....	72
7.7.3	Subscribing PPs .....	74
7.7.3.1	Subscription with Configured IPEI .....	76
7.7.3.2	Wildcard Subscription.....	76
7.7.4	Deleting PPs.....	76
7.7.5	Searching within the PP List.....	76
7.8	“WLAN” MENU.....	78
7.8.1	“WLAN profiles” Menu .....	78
7.8.1.1	Creating and Changing WLAN Profiles .....	79
7.8.1.2	Deleting WLAN Profiles.....	85
7.8.1.3	Exporting WLAN Profiles.....	86
7.8.2	“WLAN clients” Menu.....	86
7.9	“SYSTEM FEATURES” MENU .....	86
7.9.1	“Digit treatment” Menu.....	87
7.9.1.1	Creating and Changing “Digit treatment” Entries.....	88
7.9.1.2	Deleting “Digit treatment” Entries .....	89
7.9.2	“Directory” Menu.....	89
7.9.2.1	Creating and Changing LDAP Servers.....	90
7.9.2.2	Deleting LDAP Entries.....	91
7.9.3	“Feature access codes” Menu .....	91
7.10	“LICENSES” MENU .....	92
7.11	“INFO” MENU .....	93
<b>8</b>	<b>OM MANAGEMENT PORTAL (OMP) .....</b>	<b>94</b>
8.1	LOGIN .....	94
8.2	LOGOUT .....	95
8.3	OMP MAIN WINDOW .....	95
8.4	“STATUS” MENU .....	97
8.5	“SYSTEM” MENU.....	98
8.5.1	“System settings” Menu.....	98
8.5.2	“Statistics” Menu.....	99
8.5.3	“SIP” Menu.....	101
8.5.4	“User administration” Menu .....	103
8.5.4.1	Creating New User Accounts .....	104
8.5.4.2	Changing a User Account .....	105
8.5.4.3	Viewing User Account Details .....	105
8.5.4.4	Deleting User Accounts.....	106
8.5.5	“Data management” Menu.....	106
8.5.5.1	“Automatic DB import” Tab.....	106
8.5.5.2	“Automatic DB export” Tab.....	108
8.5.5.3	“User data import” Tab .....	109
8.5.5.4	“Manual DB import” Tab.....	110
8.5.5.5	“Manual DB export” Tab.....	111
8.5.5.6	“Maintenance” Tab .....	112
8.6	“SITES” MENU .....	113
8.7	“RADIO FIXED PARTS” MENU.....	114
8.7.1	“Device list” Menu.....	114
8.7.1.1	RFP Detail Panel.....	116
8.7.1.2	Adding New RFPs.....	118
8.7.1.3	Changing RFPs.....	120
8.7.1.4	Viewing RFP Details.....	120
8.7.1.5	Deleting RFPs.....	120
8.7.1.6	Showing Synchronization Relations .....	120
8.7.1.7	Selecting Columns .....	121
8.7.1.8	Filtering RFP Table .....	121
8.7.2	“Paging areas” Menu .....	122
8.7.3	“Enrolment” Menu.....	123

8.7.4	“Export” Menu .....	124
8.7.5	“Sync view” Menu .....	125
8.7.6	“Statistics” Menu .....	127
	8.7.6.1 RFP Statistics Overview .....	127
	8.7.6.2 RFP Statistics Group Panels .....	128
8.8	“PORTABLE PARTS” MENU .....	129
8.8.1	Overview” Menu .....	129
8.8.2	“Users” Menu .....	132
8.8.3	“Devices” Menu .....	133
8.8.4	PP Detail Panel .....	134
8.8.5	Creating PP Datasets .....	138
8.8.6	Configuring PP Datasets .....	138
8.8.7	Subscribing PP Datasets .....	138
8.8.8	Deleting PP Datasets .....	139
8.8.9	Selecting Columns.....	139
8.8.10	Filtering PP Table .....	139
8.8.11	Enabling / Disabling PP Event Log.....	140
8.9	“SYSTEM FEATURES” MENU .....	140
8.9.1	“General settings” Menu .....	141
8.9.2	“Feature access codes” Menu .....	141
8.9.3	“Alarm triggers” Menu .....	142
	8.9.3.1 Creating “Alarm triggers” .....	143
	8.9.3.2 Configuring “Alarm triggers” .....	144
	8.9.3.3 Deleting “Alarm triggers” .....	144
	8.9.3.4 View “Alarm trigger” Details.....	144
8.9.4	“Digit treatment” Menu .....	144
8.9.5	“Directory” Menu .....	146
8.9.6	“XML applications” Menu .....	146
	8.9.6.1 Creating a New XML Hook.....	148
	8.9.6.2 Changing an XML Hook .....	148
	8.9.6.3 Viewing XML Hook Details .....	149
	8.9.6.4 Deleting XML Hooks.....	149
8.10	“LICENSE” MENU .....	150
8.11	“GENERAL” MENU .....	150
8.12	“HELP” MENU .....	152
<b>9</b>	<b>CONFIGURATION UND ADMINISTRATION ASPECTS .....</b>	<b>153</b>
9.1	IP SIGNALING AND MEDIA STREAM .....	153
9.2	RFP SYNCHRONIZATION .....	155
	9.2.1 Initial Synchronization Procedure .....	156
	9.2.2 Checking the Synchronization of a Network.....	157
9.3	RFP CHANNEL CAPACITY .....	157
9.4	NETWORK INFRASTRUCTURE PREREQUISITES .....	158
9.5	SIP-DECT STARTUP .....	158
	9.5.1 TFTP and DHCP Server Requirements .....	159
	9.5.2 Booting Steps .....	159
	9.5.3 Booter Startup .....	160
	9.5.3.1 DHCP Client.....	160
	9.5.3.1.1 DHCP Request.....	161
	9.5.3.1.2 DHCP Offer .....	161
	9.5.3.1.3 Retries .....	161
	9.5.3.2 TFTP Client.....	161
	9.5.3.3 Booter Update .....	162
	9.5.4 Application Startup .....	162
	9.5.4.1 DHCP Client.....	162
	9.5.4.2 Configuration using DHCP .....	164
	9.5.4.3 Selecting the Right DHCP Server.....	165
	9.5.5 RFP LED Status .....	165
	9.5.5.1 Booter LED Status.....	166
	9.5.5.2 Application LED Status.....	167
9.6	STATE GRAPH OF THE START-UP PHASES.....	170
9.7	STATIC LOCAL CONFIGURATION OF AN RFP (OM CONFIGURATOR).....	171
9.8	RFP CONFIGURATION FILES .....	178
9.9	RFP (L) 35/36/37 IP / RFP (L) 43 WLAN SOFTWARE UPDATE .....	181

9.10	802.1Q SUPPORT .....	182
9.10.1	Boot Phase of IP RFPs (DHCP) .....	183
9.10.2	Boot Phase of IP RFPs (Local Configuration) .....	183
9.11	INSTALLING OMM IN HOST MODE .....	183
9.11.1	System Requirements .....	184
9.11.2	Installing the OMM Software .....	184
9.11.3	Configuring the Start Parameters .....	186
9.11.4	Specific Commands – Troubleshooting .....	186
9.11.5	Upgrade from OMM Version 2.x to 3.x in Host Mode .....	187
9.12	UPDATING THE OMM .....	187
9.12.1	Updating a Single OMM Installation .....	187
9.12.2	Updating a Standby OMM Installation .....	188
9.13	OMM STANDBY .....	189
9.13.1	Configuring OMM Standby .....	190
9.13.2	Fail Over Situations .....	190
9.13.3	Fail Over Failure Situations .....	190
9.13.4	Specific Standby Situations .....	192
9.13.4.1	How A Standby OMM Becomes Active .....	192
9.13.4.2	Handling When Both OMMs Are Not Synchronized .....	192
9.13.4.3	Two DECT Air Interfaces .....	192
9.14	MANAGING ACCOUNT DATA FOR SYSTEM ACCESS .....	193
9.14.1	Account Types .....	193
9.14.2	Potential Pitfalls .....	194
9.15	WLAN CONFIGURATION (RFP (L) 42 WLAN / RFP (L) 43 WLAN ONLY) .....	194
9.15.1	WLAN configuration steps .....	194
9.15.2	Optimizing the WLAN .....	195
9.15.3	Securing the WLAN .....	197
9.16	SNMP CONFIGURATION .....	197
9.17	DOWNLOAD OVER AIR .....	198
9.17.1	How “Download Over Air” Works .....	198
9.17.2	How to configure “Download Over Air” .....	199
<b>10</b>	<b>MAINTENANCE .....</b>	<b>202</b>
10.1	SITE SURVEY MEASUREMENT EQUIPMENT .....	202
10.2	CHECKING THE AASTRA DECT 142 / AASTRA 142D HANDSET FIRMWARE VERSION .....	202
10.3	DIAGNOSTIC .....	202
10.3.1	Aastra DECT 142 / Aastra 142d Site Survey Mode .....	202
10.3.2	Aastra DECT 142 / Aastra 142d Auto Call Test Mode .....	203
10.3.3	Aastra DECT 142 / Aastra 142d Auto Answer Test Mode .....	203
10.3.4	Syslog .....	204
10.3.5	SSH user shell .....	205
10.3.5.1	Login .....	205
10.3.5.2	Command Overview .....	206
10.3.5.3	OMM Console On Linux Server .....	206
10.3.5.4	RFP Console Commands .....	207
10.3.5.5	OMM Console Commands .....	208
10.3.6	Core File Capturing .....	209
10.3.7	DECT Monitor .....	210
<b>11</b>	<b>APPENDIX .....</b>	<b>214</b>
11.1	DECLARATION OF CONFORMITY .....	214
11.2	COMMUNICATIONS REGULATION INFORMATION FOR AASTRA 142D, AASTRA 600D .....	214
11.2.1	FCC Notices (U.S. Only) .....	214
11.2.2	Industry Canada (Canada only, not for Aastra 600d) .....	215
11.3	COMMUNICATIONS REGULATION INFORMATION FOR RFP 32, RFP 34, RFP 35 AND RFP 36 .....	215
11.3.1	FCC Notices (U.S. Only) .....	215
11.3.2	Industry Canada (Canada only) .....	216
11.4	ABBREVIATIONS .....	217
11.5	DEFINITIONS .....	217
11.6	REFERENCES .....	219
11.7	PRE-CONFIGURATION FILE RULES .....	220
11.7.1	PP Configuration File (OMM Database) .....	221
11.7.1.1	Supported Instructions .....	221

11.7.1.2	Data Section Fields .....	221
11.7.1.3	Example .....	222
11.7.2	RFP Configuration File / Central (OMM Database).....	223
11.7.2.1	Supported Instructions .....	224
11.7.2.2	Data Section Fields .....	224
11.7.2.3	Example .....	225
11.7.3	RFP Configuration File / Local (OM Configurator) .....	227
11.7.3.1	Supported Instructions .....	227
11.7.3.2	Data Section Fields .....	227
11.7.3.3	Example .....	228
11.8	RFP EXPORT FILE FORMAT .....	230
11.9	PROTOCOLS AND PORTS .....	232
<b>12</b>	<b>INDEX.....</b>	<b>234</b>

# 1 Overview

This document describes the installation / configuration, administration, and maintenance of the SIP-DECT solution.

## Other valid documentation

Please observe also the information to other parts of your SIP-DECT installation given in the documents listed in the section entitled References starting on page 219.

## Reference

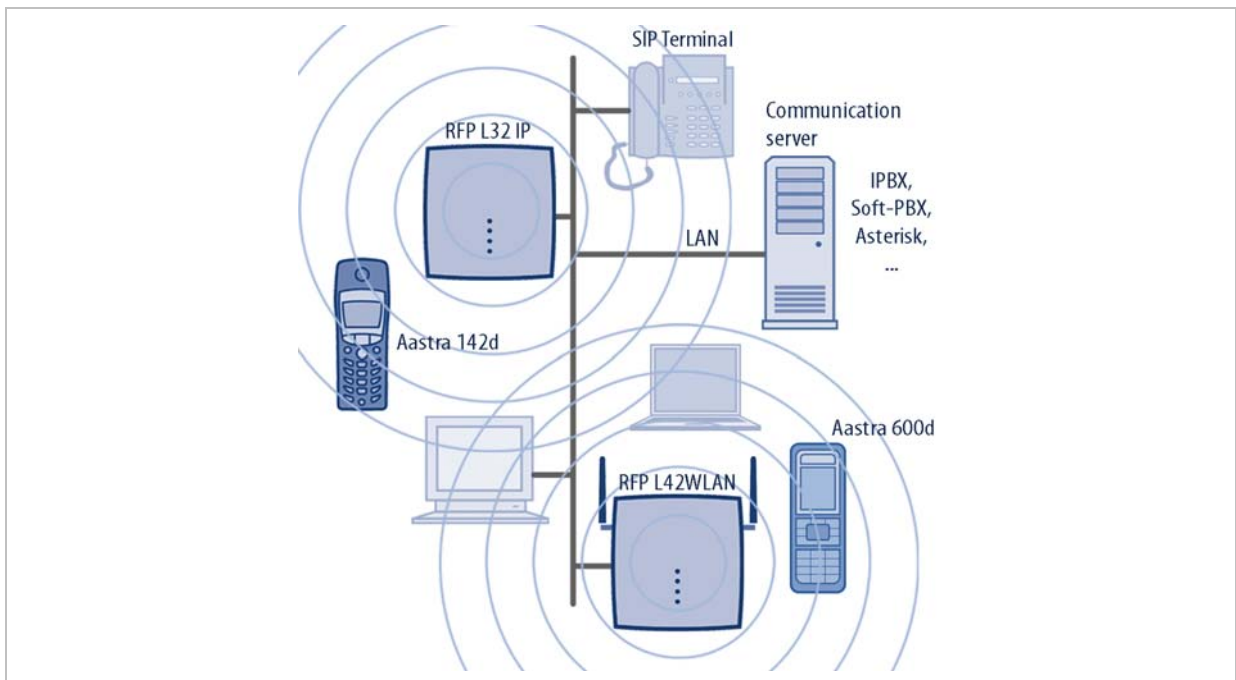
For a list of abbreviations and definitions valid for this manual please refer to the appropriate chapters in the Appendix starting on page 214.

## 1.1 The SIP-DECT Solution

The SIP-DECT solution comprises the following main components:

- Aastra SIP-DECT base stations or Radio Fixed Parts (RFPs) being distributed over an IP network and offering DECT and IP interfaces.
- Portable DECT devices known as handsets, Portable Parts (PP) or just device e.g. Aastra 620d.
- OpenMobility Manager (OMM): Management and signaling SW for the SIP-DECT solution, which runs on one of the Radio Fixed Parts or on a dedicated Linux PC (for large installations). In addition, a standby OMM can be configured to ensure the OMM function in case of failure or loss of network connection.
- A SIP Call Manager/IP PBX/Media Server platform e.g. Asterisk.

The following figure gives a graphical overview of the architecture of the SIP-DECT wireless solution:

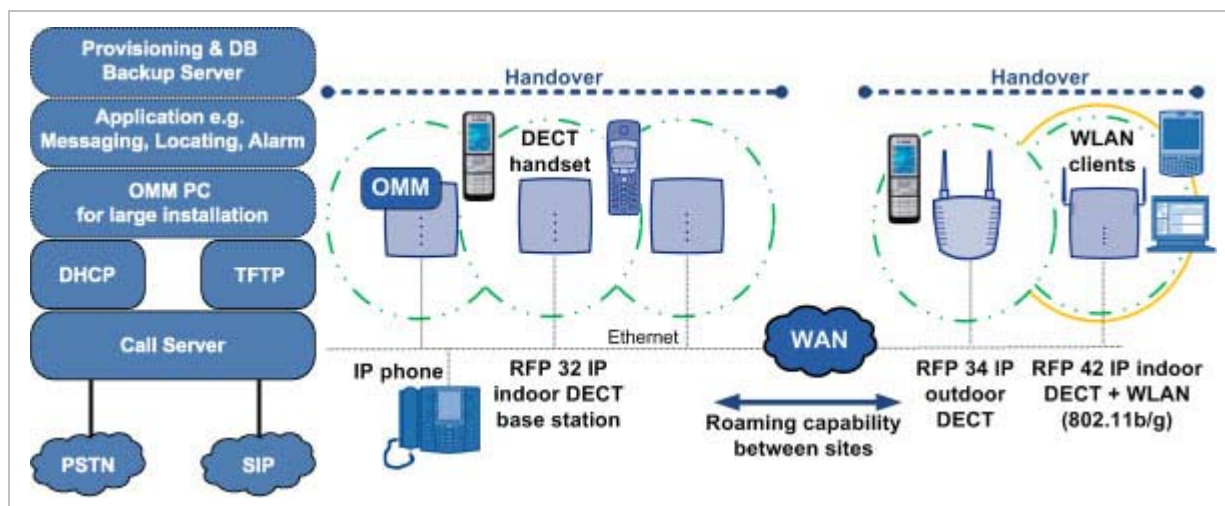


The IP PBX/media server/media gateway, OMM and the RFPs communicate through the IP infrastructure. The RFPs and the Portable Parts communicate over the air, where the DECT GAP protocol or DECT GAP with proprietary enhancements is used.

The SIP-DECT solution supports seamless handover between RFPs which are in a group of synchronized RFPs (cluster) and roaming between RFPs on remote sites.

Additional components are:

- LDAP server to facilitate a central corporate directory;
- Provisioning server to provide RFP configuration or user data files;
- Data backup server to automatically backup an OMM database on the server or to automatically import an OMM database into the OMM;
- OM Locating server and clients to run the Aastra SIP-DECT locating solution;
- 3<sup>rd</sup> party messaging or alarm server to integrate the SIP-DECT text messaging into a unified messaging or alarm environment;
- Computer for administration and maintenance tools: Web browser, OM Management Portal (OMP), DECT Monitor.



## 1.2 About the Radio Fixed Parts (RFPs)

### 1.2.1 RFP Families

#### 1.2.1.1 Former RFP Types (Till SIP-DECT Release 2.1)

Aastra provides 3 types of RFPs for the SIP-DECT solution:

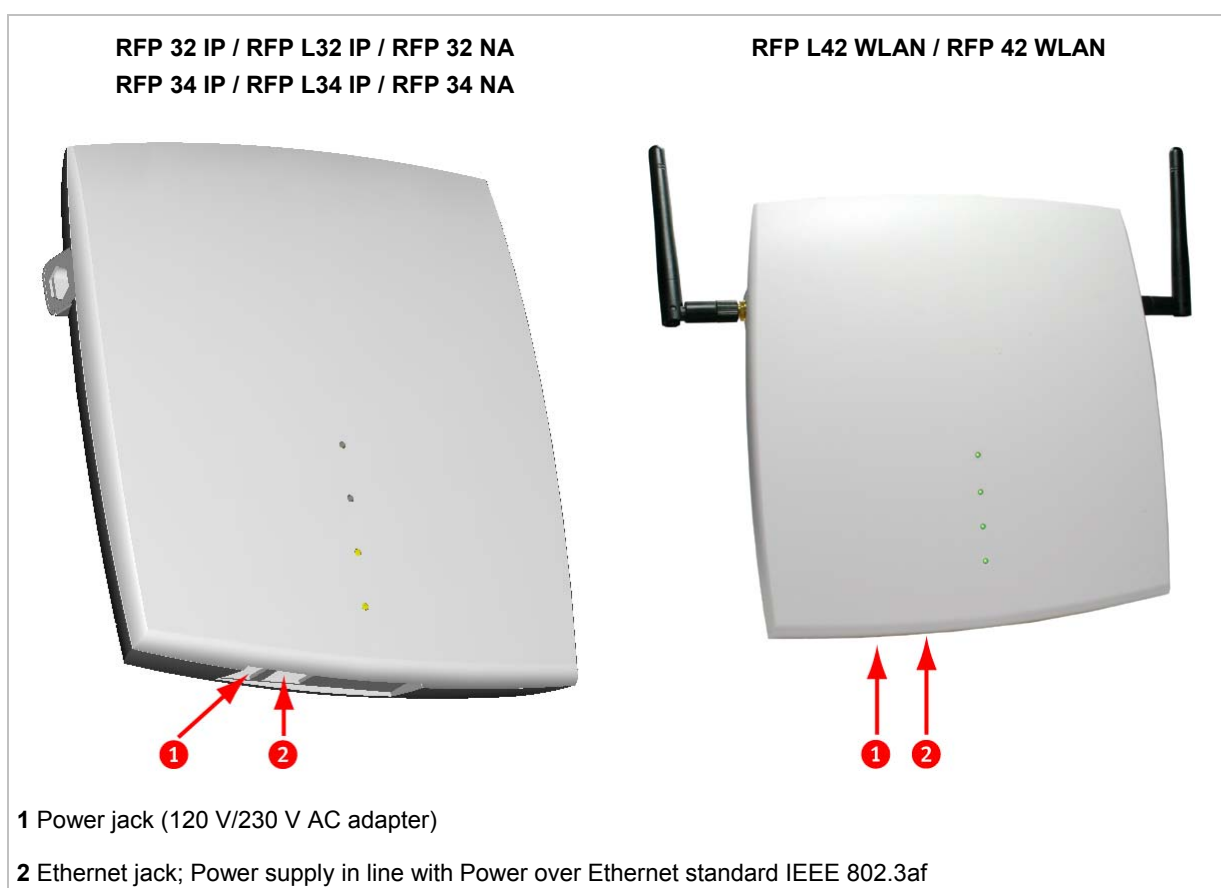
- RFP 32 IP / RFP L32 IP  
DECT RFP as indoor model
- RFP 34 IP / RFP L34 IP  
DECT RFP as outdoor model
- RFP 42 WLAN / RFP L42 WLAN  
DECT RFP + WLAN Access Point as indoor model



In general the RFP 32 and RFP 34 have the same hardware and software capabilities. Please be aware of the regulatory differences between North America and all other areas of the world. These differences lead to different RFP 32/34 variants which use specific frequency bands and field strengths:

- RFP 32 NA or RFP 34 NA (NA)
  - Frequency Band 1920 to 1930 MHz
  - 5 carrier frequencies
  - Transmit Power 20 dBm
- RFP L32 IP or RFP L34 IP (EMEA)
  - Frequency Band 1880 to 1900 MHz
  - 10 carrier frequencies
  - Transmit Power 24 dBm

The RFP L42 WLAN is only available for the EMEA region.



The difference between L-RFPs (L32 IP / L34 IP / L42 WLAN) and non-L-RFPs (32 IP / 34 IP / 42 WLAN) is that the “L” variants have a built-in license, please see chapter Licensing for details.

**Note:** Since SIP-DECT the previous RFP family (RFP (L) 32/34 IP and RFP (L) 42 WLAN) cannot longer house the Open Mobility Manager (see also chapter 1.3). The SW package for this RFP family has a tftp extension e.g. “SIP-DECT\_3.0.tftp”.

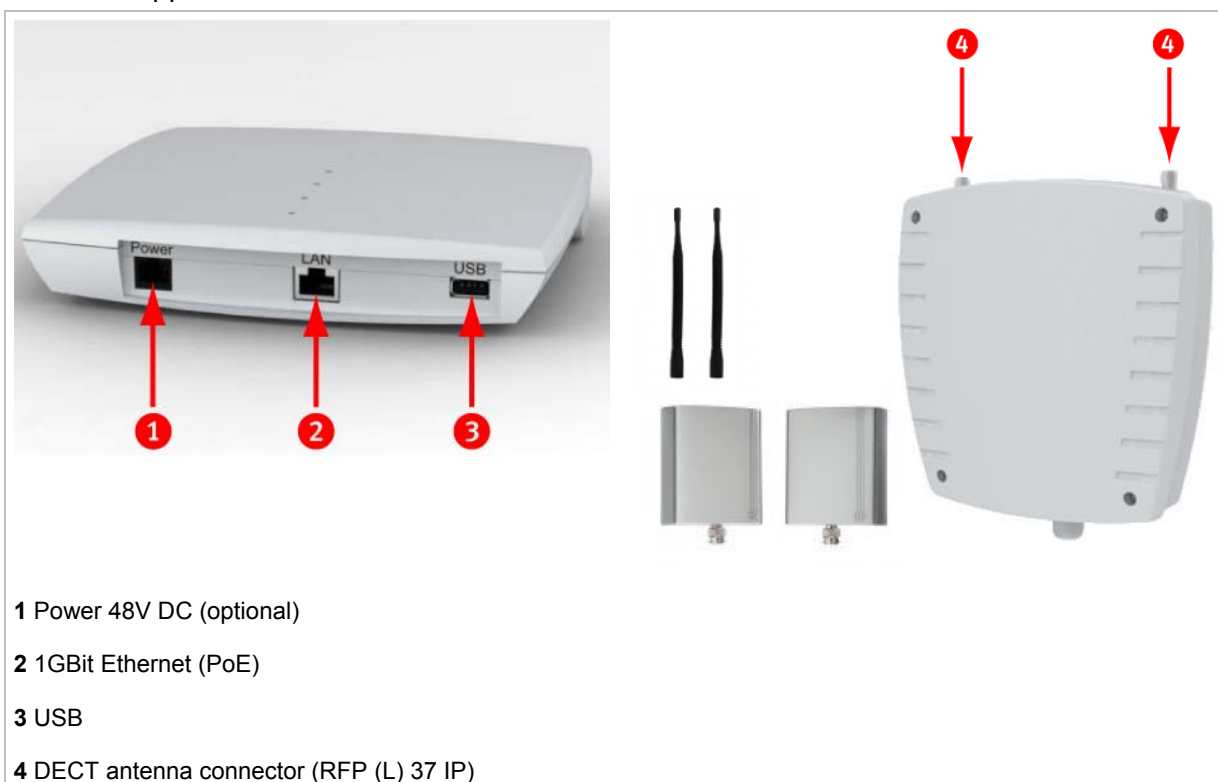
### 1.2.1.2 New RFP Types (Since SIP-DECT Release 3.0)

With SIP-DECT release 3.0 Aastra provides 3 new types of RFPs for the SIP-DECT solution:

- RFP 35 IP / RFP L35 IP  
DECT RFP as indoor model
- RFP 36 IP / RFP L36 IP  
DECT RFP as outdoor model with built-in dipole antennas
- RFP 37 IP / RFP L37 IP  
DECT RFP as outdoor model with connectors for external directional antennas
- RFP 43 WLAN / RFP L43 WLAN  
DECT RFP + WLAN Access Point as indoor model with internal antennas for DECT and WLAN

The difference between L-RFPs (L35 IP / L36 IP / L37 IP / L43 WLAN) and non-L-RFPs (35 IP / 36 IP / 37 IP / 43 WLAN) is that the “L” variants have built-in licenses, please see chapter Licensing for details.

In general the RFP 35 / 36 / 37 IP have the same hardware and software capabilities. RFP 43 supports WLAN in addition to DECT.



The hardware of all the new RFPs complies with the different regulatory areas of the world. There are no specific hardware variants required to use specific frequency bands and field strengths. Transmit Power, frequency band and carrier frequencies are controlled by software.

Other differences compared to the previous RFP family (RFP (L) 32/34 IP and RFP (L) 42 WLAN) are:

- Boot from internal flash memory instead of net-boot; there is already a SIP-DECT software on board
- software update via TFTP, FTP(S), HTTP(S) supported

- supports 1Gbit Ethernet
- supports CAT-iq 1.0 level high definition voice for the new Aastra 650c handset family
- hardware is ready to support Secure SIP and SRTP with a SIP-DECT 3.0 follow-up release
- uses an external 48V DC Power Supply (if no PoE available) which fulfils the latest environmental requirements, i.e. EOP step 2 level 5
- The RFP 43 WLAN supports the 802.11n standard.
- The RFP 43 WLAN can house the OMM.
- The indoor RFPs have a USB 2.0 interface to connect external hardware for future applications e.g. video camera

### 1.2.2 RFP only Mode

Within this mode the RFP converts IP protocol to DECT protocol and then transmits the traffic to and from the handsets over a DECT time slot. On air the RFP has 12 available time slots, 8 can have associated DSP resources for media streams. All DECT time slots are used for control signaling, software download over air, messaging and bearer handover independent of associated DSP resources.

2 control signaling channels are also used to carry bearer signals that signal the handset to start the handover process. If the radio signal of another RFP is stronger than that of the current RFP, then the handset starts the handover process to the RFP that has the stronger signal as the user moves around the site.

#### Clusters

Groups of RFPs can be built which are named clusters. Within a cluster RFPs are synchronized to enable a seamless handover when an user crosses from one RFP's area of coverage to another. For synchronization it is not necessary for an RFP to see directly all other RFPs in the system. Each RFP only needs to be able to see the next RFP in the chain. But it is preferable for an RFP to see more than one RFP to guarantee synchronization in the event that one of the RFPs fails.

### 1.2.3 OpenMobility Manager (OMM) Mode

If the OMM shall not run on a dedicated Linux PC then one RFP within a SIP-DECT installation must be declared to operate as the OpenMobility Manager (OMM). The RFP acting as the OMM may also act as a regular RFP as well if it is included into a DECT cluster.

In OMM mode an RFP functions as a regular RFP. Additionally it is responsible for SIP signaling between the SIP-DECT system and the IP PBX/media server. Further on it takes over the management part of the SIP-DECT solution. You designate an RFP as the OMM by assigning an IP address to the RFP within the DHCP scope (see chapter 9.5) or by setting the data via the OM Configurator (see 9.6). After an RFP is designated as the OMM, it starts the extra services on board (for example, the web service that supports the management interface). All RFPs download the same firmware from a TFTP server but only one RFP activates the OMM services.

**Note:** It is possible to deactivate the DECT part of an RFP. If the DECT interface is deactivated then all resources (CPU and memory) are available for the OMM.

When you decide to run an RFP-based OMM, you should be sure that the maximum number concurrent calls will not exceed  $\leq 100$  in your DECT network.

## 1.3 About the OpenMobility Manager

With SIP-DECT 3.0 the OpenMobility Manager (OMM) requires to run on one of the new RFP types (RFP (L) 35/36/37 IP resp. RFP (L) 43 WLAN) or on a dedicated Linux x86 server.

There is only one active OpenMobility Manager (OMM) in the system.

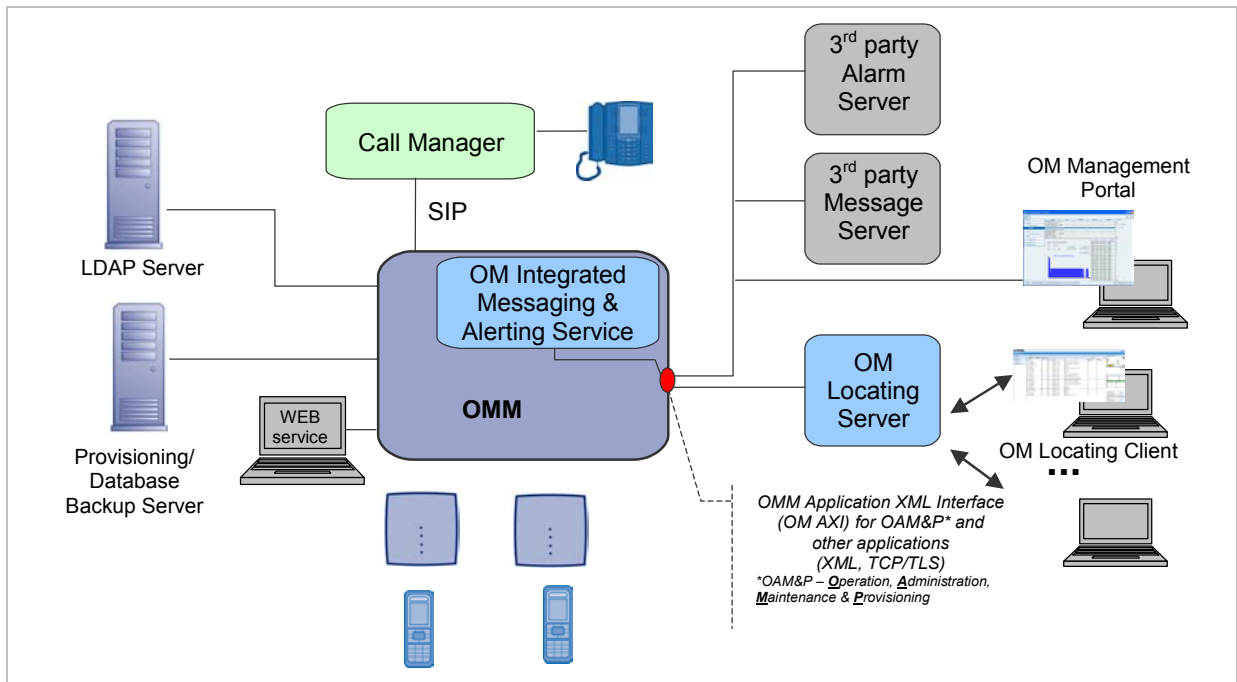
- If the OMM runs on an RFP, a 100 Mbit network link is required.
- If the OMM runs on on a dedicated Linux PC, a 1 Gbit network link is required (see also chapter 9.11.1).

In addition, a standby OMM can be configured to ensure the OMM function in case of failure or loss of network connection. For more information on the standby OMM see chapter 9.13.

### 1.3.1 OMM Tasks

The OMM performs the following tasks:

- Signaling gateway (SIP <-> DECT)
- Media stream management
- Managing sync-over-air functions between RFPs
- Provides a Web service for system configuration
- Provides additional services e.g.
  - LDAP based central corporate directory
  - OM Application XML interface (OM AXI) for OAM&P, messaging, alerting service and locating
  - Integrated Messaging and Alerting Service (OM IMA)
  - Data backup and provisioning services
  - SIP-DECT XML terminal interface. This interface adapts the “XML API for Aastra SIP Phones“ for SIP-DECT handsets. The Aastra 600d handset family (firmware release 4.00 required) and the Aastra 650c handset are supported.



Additional information on the following topics are available with separate documents.

- Locating: please see the SIP-DECT; OM Locating Application; Installation, Administration & User Guide /25/.
- Integrated Messaging and Alerting Service: please see the SIP-DECT; OM Integrated Messaging & Alerting Application; Installation, Administration & User Guide /26/ and the SIP-DECT; Aastra 610d, 620d, 630d; Messaging & Alerting Applications; User Guide /28/.
- Integration of SIP-DECT in unified messaging and alarm environments: please see /28/ and the OM Application XML Interface (OM AXI) specification /28/.
- User data provisioning: please see the SIP-DECT; OM Handset Sharing & Provisioning; User Guide /27/.
- Administration and Monitoring by 3rd party applications: please see the OM Application XML Interface (OM AXI) specification /28/.
- SIP-DECT XML terminal interface: please see the SIP-DECT XML terminal interface specification /34/.

### 1.3.2 SIP-DECT Special Features and Capacities

Special features and capacities of the SIP-DECT 3.0 solution are:

Feature/Handset	GAP	142d	600d <sup>1</sup>	650c
Large DECT Systems (XXL)	No connection handover beyond 256 RFPs	yes	yes	yes
Messaging & Alerting	no	no	yes	yes
Initiate Alarm Trigger	*, # procedure no sensor alarm	*, # procedure no sensor alarm	yes	yes

Feature/Handset	GAP	142d	600d <sup>1</sup>	650c
Locating	yes	yes	yes enhanced locating features	yes enhanced locating features
DECT XQ	no	no	yes	yes
UTF-8 and alphanumeric dialing support <sup>2</sup>	no	no	yes	yes
SIP-DECT XML terminal API <sup>2</sup>	no	no	yes	yes
CAT-iq 1.0 / Aastra Hi-Q™ audio technology <sup>2</sup>	no	no	no	yes

<sup>1</sup> requires Aastra 600d firmware release 4.00 or higher

<sup>2</sup> new with SIP-DECT 3.0

### 1.3.3 OMM Capacities and Features

The OMM capacities are:

Feature/SW Release	Release 1.8		Release 2.1		Release 3.0 or later	
	RFP OMM	Linux x86 server OMM	RFP OMM	Linux x86 server OMM	RFP OMM	Linux x86 server OMM
L-RFP: RFP L32/34IP & RFP L42WLAN	256	-	20	-	20 <sup>1</sup>	-
Standard RFP: RFP 32/34IP & RFP 42WLAN	-	-	256 <sup>2</sup>	2048 <sup>2</sup>	256 <sup>1,2</sup>	2048 <sup>2</sup>
L-RFP: RFP L35/36/37IP & RFP L43WLAN	-	-	-	-	20	-
Standard RFP: RFP 35/36/37IP & RFP 43WLAN	-	-	-	-	256 <sup>2</sup>	2048 <sup>2</sup>
Handsets / users	512	-	512	4500	512	4500
Message / Alarm receive	-	-	yes / yes <sup>2</sup>	yes / yes <sup>2</sup>	yes / yes <sup>2</sup>	yes / yes <sup>2</sup>
Message send	-	-	yes <sup>3</sup>	yes <sup>3</sup>	yes <sup>3</sup>	yes <sup>3</sup>
Locating	-	-	yes <sup>2</sup>	yes <sup>2</sup>	yes <sup>2</sup>	yes <sup>2</sup>
DECT XQ	-	-	yes	yes	yes	yes
UTF-8 and alphanumeric dialing support	-	-	-	-	yes	yes
SIP-DECT XML terminal API	-	-	-	-	yes	yes

Feature/SW Release	Release 1.8		Release 2.1		Release 3.0 or later	
	RFP OMM	Linux x86 server OMM	RFP OMM	Linux x86 server OMM	RFP OMM	Linux x86 server OMM
CAT-iq 1.0 / Aastra Hi-Q™ audio technology	-	-	-	-	yes	yes

<sup>1</sup> There must be at least one RFP L35/36/37 IP or RFP L43 WLAN to host the OMM (2nd RFP for OMM standby).

<sup>2</sup> The feature requires a license and is not available for L-RFP installations which are using built-in licenses.

<sup>3</sup> This feature requires a license for standard RFP installations. There is a built-in license for L-RFP installation.

## 1.4 About the Portable Parts

Portable Part (PP) is DECT standard terminology and in the context of the SIP-DECT solution is interchangeable with handset. Aastra provides the following handsets: Aastra 142d, Aastra 610d / Aastra 620d / Aastra 630d, and (since SIP-DECT 3.0) Aastra 650c.



### Notes on the Aastra 142d handset

Please be aware of differences in regulatory requirements between North America and all other areas of the world. These differences lead to different Aastra 142d variants which use specific frequency bands and field strengths:

Aastra DECT 142 (NA)	Aastra 142d (global, all other countries)
Frequency Band 1920 to 1930 MHz (UPCS)	Frequency Band 1880 to 1900 MHz
60 duplex channels	120 duplex channels
100 mW (maximum output per active channel)	250 mW (maximum output per active channel)
5 mW (average output per active channel)	10 mW (average output per active channel)

In addition to the Aastra DECT 142 / Aastra 142d, standard 3rd party DECT GAP phones may operate on the SIP-DECT solution. But the functionality may be limited by the characteristics of the 3rd party DECT phone.

### **Notes on the Aastra 600d and Aastra 650c handsets**

The Aastra 610d / 620d / 630d supports both the NA and EMEA regulatory requirements.

The new Aastra 600d firmware release 4.0 has to be used with Aastra 610d / Aastra 620d / Aastra 630d to support the SIP-DECT release 3.0 features. SIP-DECT release 3.0 still supports the previous Aastra 600d firmware release 3.03 but with limitation. The Aastra 600d firmware release 3.03 is incompatible with new SIP-DECT release 3.0 features like UTF-8.

The Aastra 600d firmware release 4.0 has the following characteristics:

- New user interface e.g. new dial editor with alphanumerical and always en-bloc dialing
- Support of UTF-8 in over the air signaling with the OMM
- Digit and alphanumeric dialing
- Support of SIP-DECT XML terminal interface
- Support of microSD-Card to save subscription data and the most important local device data (Aastra 620d / Aastra 630d)
- Additional subscription options
- Additional alarm melodies
- Profile indication in idle display

For more details please see /28/and /29/.

The Aastra 650c handset has the same feature set as the current Aastra 600d handsets. In addition to the Aastra 600d firmware release 4.0x feature set, the new Aastra 650c handset supports CAT-iq 1.0 and is thus capable to run G.722 (wideband) voice connections. For the full experience of wideband audio the handset hardware e.g. speakers, microphone, processor, have been improved.



## 2 Getting Started

This chapter describes how to set up a small SIP-DECT system using two RFP devices, useable as a small stand-alone DECT telephony system or for evaluation purposes.

**Note:** The DHCP/TFTP configuration described here can be used to operate current RFPs 35/36/37/43 together with older RFPs 32/34/42. However, a more straightforward setup using the Java-based OpenMobility Configurator tool is described in the SIP-DECT: Installation & Administration Compendium document (see /24/).

### Prerequisites

Some hardware and software prerequisites are to be met to follow this quick start guide:

- at least two licensed RFP devices (e.g. RFP L35 IP),
- a PC to run a browser or start java programs,
- a PC-based server for setting up DHCP/TFTP,
- two or more DECT handsets (preferably two Aastra 610d/620d/630d/650c),
- OMM-SIP installation medium with software, such as the “iprfp3g.dnld” file,
- optional: a VoIP communications system that provides SIP accounts.

You can use any operating system for the PC-based server system that provides a DHCP and TFTP server. However, the following description details on a Linux system. For testing and evaluation, you may download and install virtualization software for your workstation, such as “VmWare Player” or “VirtualBox”. Within a virtual machine, you are able to operate a Linux system, for example the CentOS, Debian or Ubuntu “Live-CD” ISO files that are downloadable for free on the respective Linux vendor web sites.

**Note:** The PC-OMM (OMM in host mode, see also chapter 9.11) is not supported on virtual machines.

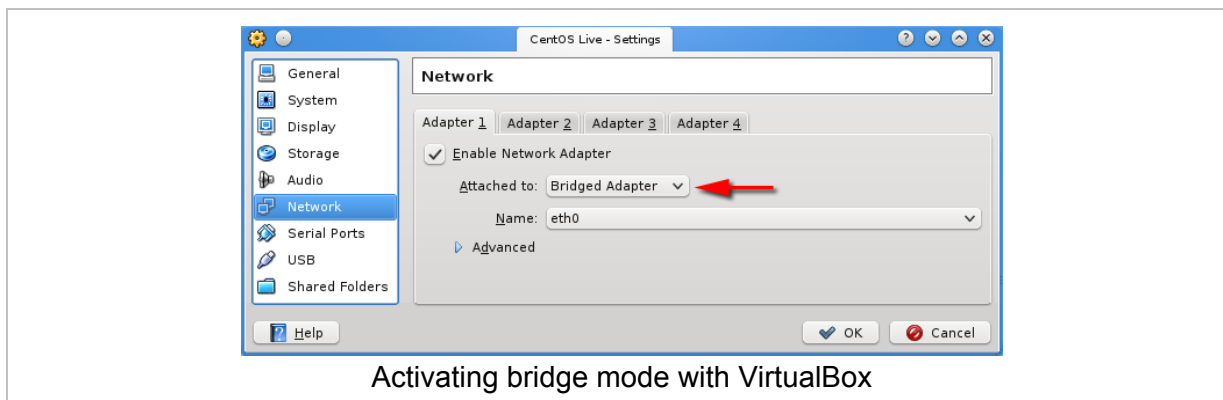
### 2.1 Setting up DHCP / TFTP

An RFP in the factory default configuration will request the address configuration via DHCP. While it is possible to configure a fixed (non-DHCP) address for the RFPs (see chapter 9.6), this description starts with setting up a DHCP server that will answer the DHCP requests. The DHCP server will be limited to answer only DHCP requests from Aastra RFPs (sorted out by MAC address), so the new DHCP server will not disturb the operation of possibly other DHCP servers in your LAN.

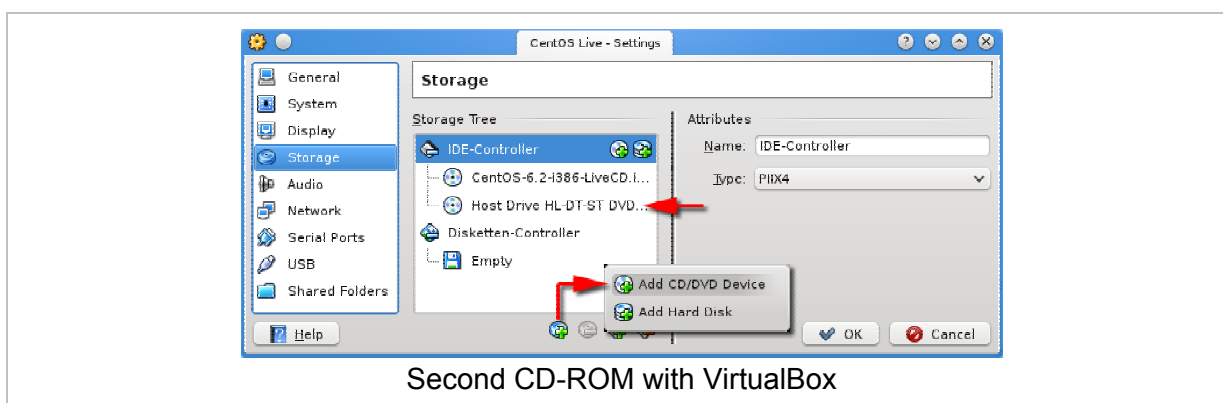
Also you need a TFTP server that offers the software file for the RFPs. For current RFPs 35/36/37/43, the TFTP server provides the software file for updates (“iprfp3g.dnld”). For older RFPs 32/34/42, the TFTP server provides the software file loaded during RFP startup (“iprfp2g.tftp”). The IP address and the software file download location is part of the DHCP answer, the RFP receives during start-up. By using this DHCP-provided configuration, the RFP downloads the software file and starts the program that is included in the software file.

As stated earlier, the PC server system described here is operated by a Linux system. If you run Linux in a virtual machine, the virtual machine’s network adapter should be configured for

the “Bridged Mode” which allows the virtual machine to receive/answer DHCP broadcasts on the physical Ethernet adapter.

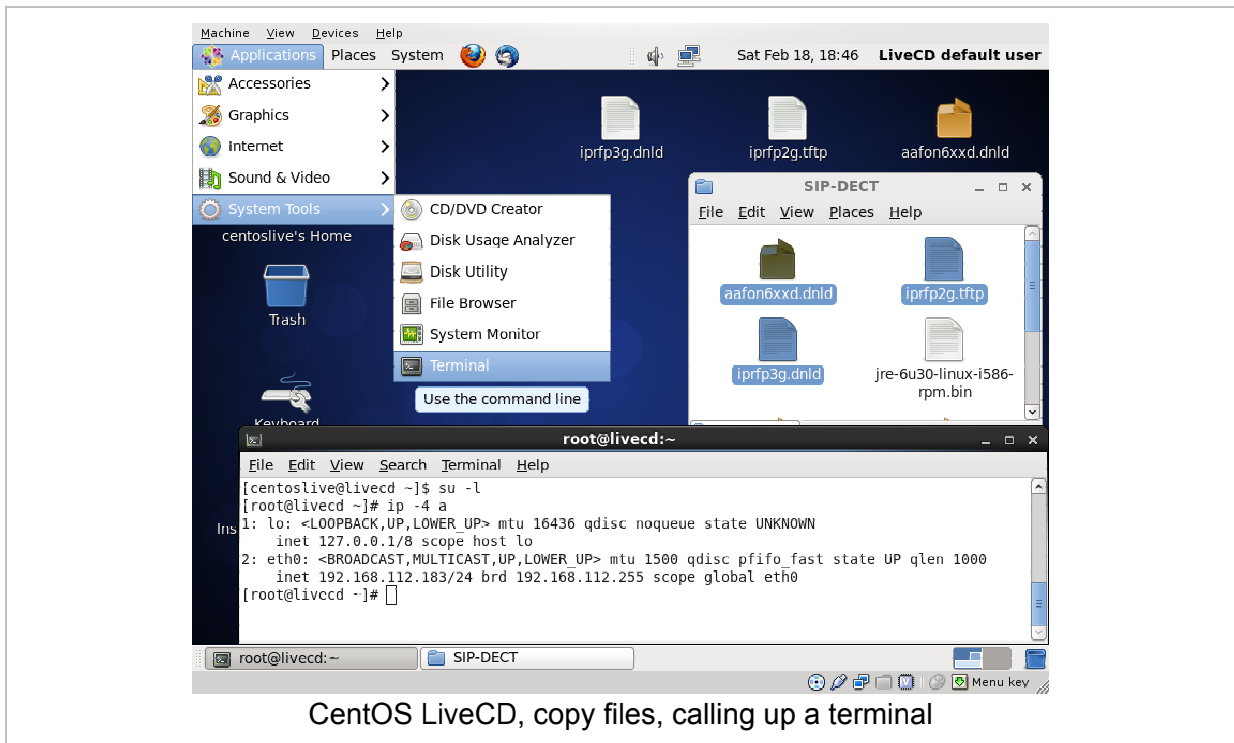


Also, you need the firmware file for the RFP inside the virtual machine. You can copy via network e.g. by using SCP, FTP, SMB etc. To keep things simple, the virtual machine used in this example has a second CD-ROM that points to the hardware CD-ROM drive that in turn has the OMM-SIP installation medium inserted.



The following steps will start the virtual machine where you can configure and run the DHCP/TFTP server program.

- 1 Start the virtual machine. The Linux desktop should be displayed after start-up. The following screenshot depicts the situation if you start VirtualBox with a Live CD Linux (CentOS 6.2 to be precise).



- 2 On the virtual machine's desktop, double click the OMM-SIP CD-ROM. Use drag & drop to copy the "iprpf3g.dnld", "iprpf2g.tftp", and "aafon6xxd.dnld" files to the Linux desktop.
- 3 Start a terminal program. With Gnome desktop, select the **Applications: Accessories: Terminal** menu command.
- 4 In the terminal program, you need to enter the following commands to switch off the firewall and to start the SSH service:

<code>su -l</code>	Starts a super user ("root") shell.
<code>ip -4 a</code>	Shows the current network configuration. The "eth0" adapter should show an IP address allocated by a DHCP server in your LAN.
<code>ip a add 192.168.1.1/24 dev eth0 ip l set dev eth0 up</code>	Optional: if the "eth0" adapter has no IP address, you can assign the address manually.
<code>/etc/init.d/sshd start</code>	Starts the SSH service.
<code>passwd centoslive</code>	Set a (simple) password for the "centoslive" user.
<code>iptables -F INPUT echo 0 &gt; /selinux/enforce</code>	Flush (clear) the INPUT firewall. Disable SELINUX that prevents TFTP downloads.

- 5 Leave the virtual machine. With VirtualBox press and release the right [Ctrl] key. With VmWare Player press and release both the left [Ctrl] key and the left [Alt] key. You may iconize the virtual machines window now.
- 6 From your home desktop, start a remote terminal via SSH. Use your favorite SSH program (e.g. the PuTTY program for Windows) and connect to the IP address of the virtual machine. Log in as "centos" user with the password entered previously. Note, that it

is now possible to use the clipboard to enter new commands and configuration file statements.

**7** Enter the following commands to configure and start the DHCP/TFTP service:

<code>su -l</code>	Starts a super user (“root”) shell.
<code>yum install dhcp tftp-server</code>	Installs a DHCP and a TFTP server.
<code>yum install nano</code>	Installs the “nano” text editor.
<code>cd /var/lib/tftpboot</code>	Change the current directory.
<code>cp -v /home/centoslive/Desktop/* .</code>	Copy files here. (“iprfp3g.dnld”, “iprfp2g.tftp”, and “aafon6xdd.dnld” from the CD ROM). Mind the trailing dot in the command.
<code>nano /etc/dhcp/dhcpd.conf</code>	Start the “nano” text editor to change the “/etc/dhcp/dhcpd.conf” configuration file for the ISC DHCP daemon. Adapt and paste the example configuration from below. Press [Ctrl-X] to end the text editor and confirm saving the file with the [Y] and [Return] keys.
<code>/etc/init.d/dhcpd restart</code>	Start the DHCP server.
<code>chkconfig tftp on</code> <code>/etc/init.d/xinetd restart</code>	Enable the TFTP server that is started from xinetd. Start the xinetd daemon after this.
<code>tail -f /var/log/messages</code>	View the system log for DHCP messages.

**8** Connect the desired RFPs to your LAN. Establish their power supply, either by PoE or by plugging in the external power adapters. During the RFP start-up, the SSH console windows should display DHCP messages that indicate the RFP DHCP queries.

### DnsMasq Configuration File (/etc/dhcp/dhcpd.conf)

The following configuration example needs to be adapted to your network and RFPs. Change all lines with “192.168.112.” to match your LAN. Also change the MAC address (here: 00:30:42:0d:10:2e) to the value printed on the backside label of the RFP that is designated as OMM.

```
#####
# dhcpd.conf sample configuration for SIP-DECT #
#####

ddns-update-style interim;
ignore client-updates;
default-lease-time 86400;
max-lease-time 86400;

### Define SIP-DECT options (incl. structure of option 43) ###

option space SIPDECT;
option SIPDECT.omm-ip          code 10 = ip-address;
option SIPDECT.omm-syslog      code 14 = ip-address;
option SIPDECT.omm-syslog-port code 15 = unsigned integer 16;
option SIPDECT.country         code 17 = unsigned integer 16;
option SIPDECT.ntpsrvname      code 18 = text;
option SIPDECT.omm-ip2         code 19 = ip-address;
```

```
option SIPDECT.importurl      code 24 = text;

option magic_str              code 224 = text;
option tftp-list              code 150 = array of ip-address;
option vlanid                 code 132 = unsigned integer 16;

### class definition ###

# RFP (L) 31,32,33,34,41,42
class "SIP-DECT2G" {
    match if option vendor-class-identifier = "OpenMobility";
}

# RFP (L) 35,36,37,43, since firmware 3.0RC3
class "SIP-DECT3G" {
    match if option vendor-class-identifier = "OpenMobility3G";
}

### subnet definition ###

shared-network SIP-DECT
{
    subnet 192.168.112.0 netmask 255.255.255.0
    {
        pool {
            range 192.168.112.52 192.168.112.55;
            allow members of "SIP-DECT2G";
            allow members of "SIP-DECT3G";

            option routers 192.168.112.1;
            option subnet-mask 255.255.255.0;
            option ntp-servers 192.168.112.109;
            option domain-name-servers 192.168.112.1,8.8.8.8;

            next-server 192.168.112.183;
            vendor-option-space SIPDECT;
            option magic_str = "OpenMobilitySIP-DECT";
            option SIPDECT.omm-ip 192.168.112.43;
            # option SIPDECT.omm-ip2 192.168.112.52;
            # option SIPDECT.country 1;
            # option SIPDECT.omm-syslog 192.168.112.1;

            if option vendor-class-identifier = "OpenMobility" {
                filename "/iprfrp2g.tftp";
            }

            if option vendor-class-identifier = "OpenMobility3G" {
                filename "/iprfrp3g.dnld";
            }

            # option tftp-server-name "tftp://192.168.112.183/subdir";

            host OMM {
```

```
        hardware ethernet 00:30:42:12:6E:3B;
        fixed-address 192.168.112.43;
    }
} # end of pool
} # end of subnet
}
```

### OMM selection

One RFP of a set needs to function as OpenMobility Manager (OMM). The configuration suggested above will select a specific RFP for this role with the “DHCP option 43”. The OMM is generally selected

- via the DHCP request (see chapter 9.5.3.1),
- within the static local configuration of an RFP (see chapter 9.6),
- within the RFP configuration file of a PC-based OMM (see chapter 9.8).

The RFP which has the same IP address as the dedicated OMM IP address will be the RFP which the OMM application runs on. If two OMM IP addresses are configured, the OMM application is started on both dedicated RFPs. One OMM becomes the active OMM and the other the standby OMM. For more details about the standby feature, see chapter 9.13.

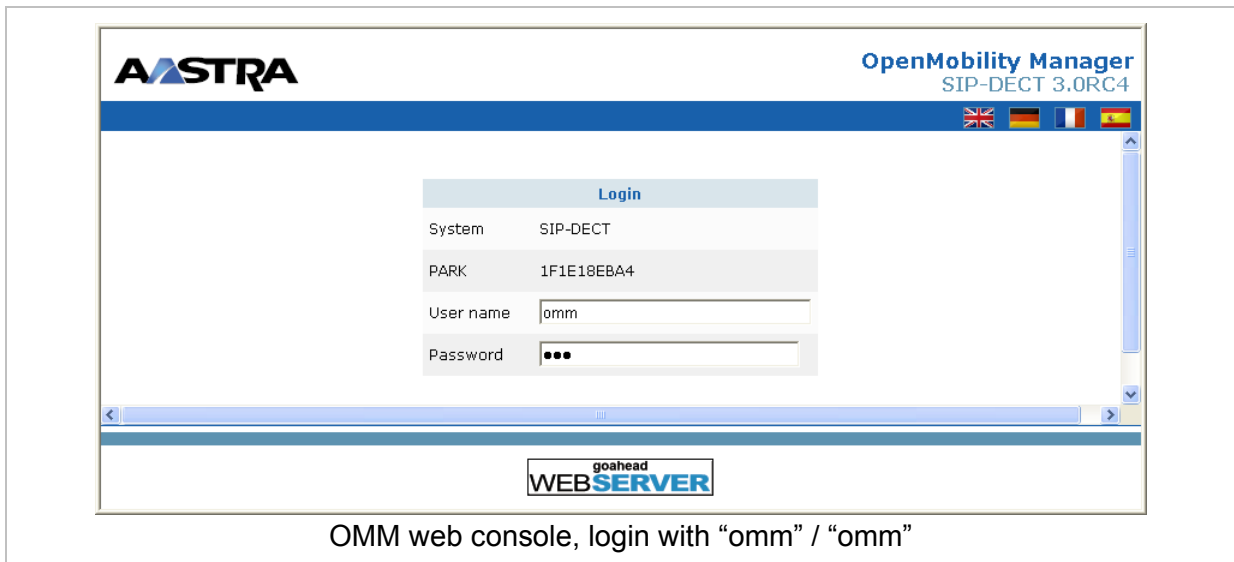
## 2.2 Initial Setup

After bringing up the DHCP/TFTP server and starting the RFPs, you can start a web browser and call up the web-based user interface of the OMM. Alternatively, the Java-based OpenMobility Manager (“OMP.jar”) may be used. The following step-by-step description emphasizes on the OMM’s web console.

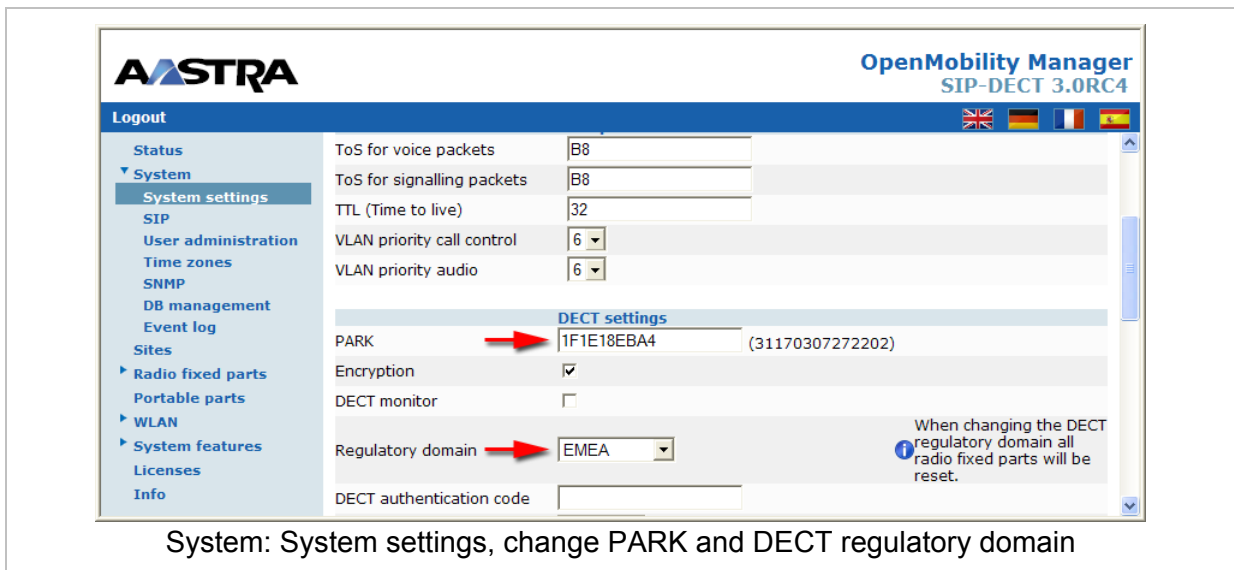
- 1 Start a web browser and navigate to the IP address that you have configured for the OMM in the DHCP option 43. This will display the OMM’s login page.

**Note:** The browser’s communication with the OMM’s web console is secured by the HTTPS protocol. However, since you cannot validate a numeric intranet address with a certificate chain, you need to ignore / overwrite the web browser’s warning about invalid certificates.

- 2 Enter “omm” in the **User name** input field. Also enter “omm” in the **Password** input field. Click the **OK** button to log in. In the factory default configuration, the OMM now displays the **Info: End-user license agreement** page. Read the agreement and confirm by clicking the **Accept** button.

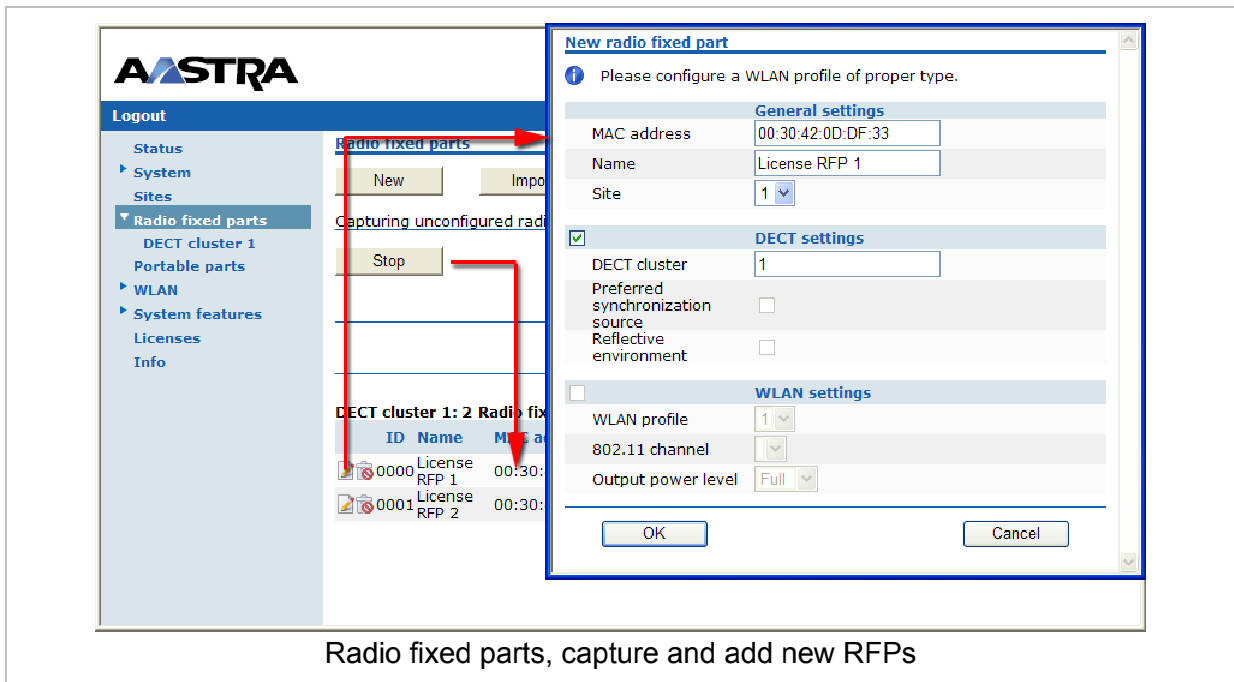



- 3 On the next two pages that are displayed automatically, you need to enter new passwords for two administrative user accounts. The first account is the “omm” user that can change the configuration. The second account can be used to call up the OMM’s command line shell via SSH. Enter passwords that contain at least lower case letters, capital letters, and digits. After changing the passwords, the web console shows the **Status** page.
- 4 Navigate to the **System: System settings** page. Change the **PARK** setting to the PARK code that is printed on the installation CD-ROM. Also change the **Regulatory domain** to match your region. Confirm with **OK**.

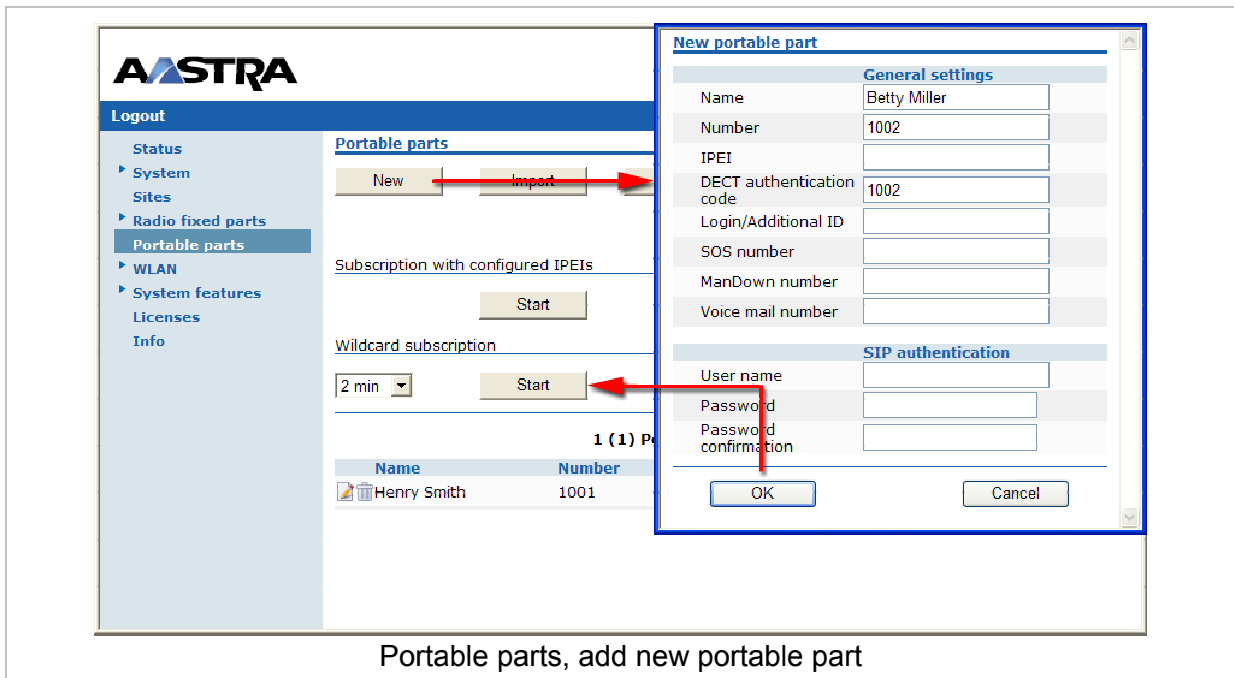


**Note:** The RFP L35 IP / RFP L36 IP / RFP L37 IP / RFP L43 WLAN and RFP L32 IP / RFP L34 IP / RFP L42 WLAN devices provide a build in license as described here. If you have purchased another license type and e.g. RFP L35 IP / RFP L36 IP devices, you need to upload the license file on the **Licenses** page now (see chapter 4).

- 5 Navigate to the **Radio fixed parts** page. Click the **Start** button to start capturing. Wait 10 seconds. Click the **Radio fixed parts** menu entry to refresh the display. If all expected RFPs are listed, click **Stop** to end capturing.



- 6 Click the  icon next to the desired entry to add a new RFP to the OMM. The **New radio fixed part** dialog opens. Enter a **Name**. Enable the **DECT settings** checkbox that assigns the RFP to **DECT cluster "1"**. Confirm with **OK**. Repeat this step for the second RFP.
- 7 Navigate to the **Portable parts** page. Click on the **New** button. The **New portable part** dialog opens. Enter a **Name**, a **Number** and a **DECT authentication code**. Confirm with **OK**. Repeat this step for a second DECT portable part with a different **DECT authentication code**.



- 8 Click on the **Start** button below the **Wildcard subscription** heading. This will activate subscription without known handset IPEIs for the next two minutes. During this period, subscribe two of your DECT handsets. Enter the configured DECT authentication code on



the DECT handset during the subscription procedure (see chapter 7). After subscribing two DECT handsets make a test call from one DECT handset to the other.

- Navigate to the **System: SIP** page to connect the OMM to your PBX. Enter the IP address of your PBX in the **Proxy server** and **Registrar server** fields. In the following screen shot, an Aastra 800 PBX with address 192.168.112.91 is used to provide the SIP PBX functions.

The screenshot displays the Aastra 800 web interface. The top window shows the 'SIP phones' table with the following data:

Ph.No.	Licence	IP address	Port	Expiration time
1001	✓	192.168.112.43	5060	18.01.12 08:33
1002	✓	192.168.112.43	5060	18.01.12 08:33
1003	✓	192.168.112.43	5060	18.01.12 08:33
1004	✓	192.168.112.43	5060	18.01.12 08:33


The bottom window shows the 'SIP' settings page with the following fields:

Field	Value
Proxy server	192.168.112.91
Proxy port	5060
Registrar server	192.168.112.91
Registrar port	5060
Registrar user	Betty Miller
Registration period	3600

The 'Configure portable part' dialog shows the following fields:

Field	Value
Name	Betty Miller
Number	1002
IPEI	03586 0017017 7
DECT authentication code	1002
Login/Additional ID	
Delete subscription	<input type="checkbox"/>
SOS number	
ManDown number	
Voice mail number	
User name	om-1002
Password	.....
Password confirmation	.....

SIP: System, connect to PBX & change portable part SIP configuration

- Navigate back to the **Portable parts** page. Click the  icon next to the desired portable part entry to open the respective **Configure portable part** dialog. Change to **User name** and **Password** fields under the **SIP authentication** heading to the SIP account credentials configured on the PBX (see chapter 7.4.2 and chapter 7.7.1). Note, that the entered **User name** is sent to the PBX as "authorization username" within the SIP "REGISTER" message.

Verify the SIP registration, for example on a status display of your PBX as shown above. Place a test call from the DECT portable part to another phone attached to the PBX.

The next steps depend on your requirements and would typically include setting up a standby OMM (see chapter 9.13) or setting up the Download over Air software-update for Aastra 610d/620d/630d/650c portable parts (see chapter 9.17).

### 3 Enhanced Feature Overview

An SIP-DECT system scale from a single licensed RFP up to a larger SIP-DECT system that may include hundreds of RFPs. Some of the more advanced features target larger DECT systems. You may browse the following list of features in order to get an overview and to decide if it's relevant for your requirements. You find in-depth explanations in the referenced chapters.

**Please note:** Be aware that the majority of the new enhanced features require at least the following handset firmware releases

- 600d: firmware release 4.00
- 650c: firmware release 1.00

It is assumed that SIP-DECT installations are configured to perform an automatic firmware update over the air.

#### Download over Air

The Aastra 600d handset family and the Aastra 650c handset are able to download and upgrade its firmware via DECT over the air.

For the OMM running on an RFP the handset firmware packages are delivered in the package file “aafon6xxd.dnld” for the Aastra 600d handset family and the Aastra 650c handset. This package file must be put on the same server and path where the RFP gets a software image file for update purposes (e.g. SIP-DECT\_3.0.dnld).

The handset firmware packages are included in the OMM installation package for Red Hat® Linux for the Linux x86 server version of the OMM (e.g. SIP-DECT\_3.0.bin).

#### Wideband (CAT-iq 1.0 / Aastra Hi-Q™ audio technology)

Together with the new RFP (L)35/36/37 IP and RFP (L) 43 WLAN, the Aastra 650c offers the possibility to act as Aastra Hi-Q audio terminal. This feature is realized using wideband speech according to CAT-iq.

Each Hi-Q connection uses, compared to conventional narrowband, the double capacity on the DECT air interface. Due to this fact, 4 Hi-Q connections (instead of 8) can be established via one RFP.

Aastra Hi-Q audio technology must be enabled or disabled per site (see chapters 7.5 and 8.6). This functionality must be homogeneously available among synchronous RFPs (members of the same cluster). Each site with enabled Hi-Q audio must exclusively contain new RFP (L)35/36/37 IP or RFP (L) 43 WLAN.

Typically one site is identical with one cluster, i.e. all RFPs belonging to a specific site belonging to a specific cluster. However a site can have more than one cluster. The OMM does not refuse to configure one cluster which contains multiple sites. Such configuration could annul the rule that Hi-Q audio must be homogeneously available among synchronous RFPs.

**Please note:** It is strongly recommended not to setup systems with multiple sites within one cluster.

### RFP mixed installations

In sites (or whole systems) with disabled Hi-Q audio, an arbitrary mixture of RFP (L) 32/34 IP / RFP (L) 42 WLAN and RFP (L)35/36/37 IP / RFP (L) 43 WLAN is allowed. No further restrictions appear for mixed installations.

### DECT XQ

The DECT radio communication generally suffers from attenuation and radio wave reflection. Especially if a building's walls and ceilings contain a higher portion of metal-based material or if larger metal surfaces are present, the DECT XQ improves the radio communication between an RFP and an Aastra 600d / Aastra 650c portable part at the expense of DECT channel capacity (see 9.3). Enable this feature for some or all of your RFPs (see chapter 7.6.3, "DECT settings" or chapter 8.7.1.2, "DECT tab").

It is not possible to have DECT XQ audio combined with Hi-Q audio within the same connection.

Three operating modes regarding audio quality are selectable at the Aastra 650c handset: standard audio, Hi-Q audio and automatic.

- In case that an Aastra 650c operates in Hi-Q audio mode, it will exclusively establish wideband connections and not switch to narrowband later on. An Aastra 650c in this mode will ignore the XQ capability of the RFP.
- In case that an Aastra 650c operates in standard audio mode, it will exclusively establish narrowband connections and not switch to wideband later on. An Aastra 650c in this mode will switch to DECT XQ and back as necessary.
- In case that an Aastra 650c operates in automatic mode, the connection establishment depends on whether the current base provides DECT XQ or not. If DECT XQ is available, a narrowband connection will be established. Otherwise a wideband connection will be established.

### UTF-8

The UTF-8 support allows the presentation of a wider range of language specific characters e.g. umlauts and eases the internationalization/localization. Since SIP-DECT 2.1 the OMM and the Aastra 600d handset family support UTF-8 for text messaging.

With the SIP-DECT 3.0 the OMM and the Aastra 600d/650c handsets support an extended character set for

- User parameter (configurable via WEB, OMP or external user configuration files)
  - System name
  - User name
  - Number
- SIP "display names" und SIP "user id's" of incoming and outgoing calls
- Call logs
- LDAP directory access
- XML terminal interface objects

Be aware that this feature needs at least following handset firmware releases:

- Aastra 600d: firmware release 4.00 or later
- Aastra 650c: firmware release 1.00 or later

For 3-party GAP handsets, Aastra 142d or Aastra 600d/650c with older firmware releases, the UTF-8 character set is not supported. If possible, the OMM maps UTF-8 character to LATIN-1.

**Please note:** The actually available set of characters is defined by the handset. Please see /29/. Characters not supported by the 600d/650c e.g. “用” are replaced by “□”. User configuration files must be encoded in UTF-8.

### Alphanumeric dialing

The SIP-DECT release 3.0 supports together with the new handset firmware releases Aastra 600d 4.00 and Aastra 650c 1.00 the dialing of alphanumeric characters. This allows in advance to the classical dialing of digits the dialing of names (e.g. “Heinrich.Mueller”).

If SIP URI dialing like “name@domain” shall be used please use an (outbound) proxy which supports the interpretation of SIP user names including domain names.

### Digit treatment and UTF-8/alphanumeric dialing

The feature “Digit treatment” is designated to handle dialed digit strings only. It cannot be applied with SIP-DECT release 3.0 to UTF-8/alphanumeric dialing.

### Voice mail number

A system wide voice mail number can be configured within the system setting section. This number is used by the Aastra 600d/650c handset family if a voice box call is initiated.

The system wide voice mail number can be overruled by a user specific voice mail number.

If there is no voice mail number configured or another type of handset is used; then the voice mail number must be configured locally in the handset.

**Please note:** The voice mail number is supported by the external user data configuration files. The parameter UD\_VoiceMailNumber can be set in the user\_common.cfg and/or “user.cfg” or “LoginID.cfg” e.g. “UD\_VoiceMailNumber=222”. For details please refer to: SIP-DECT; OM Handset Sharing & Provisioning; User Guide.

### OMM standby

The OMM is the central management entity in a SIP-DECT system and forms thereby single point of failure. It is possible to automatically transfer the OMM function to a second RFP device in case of failure or loss of network connection (see chapter 9.13).

### RFP synchronization / radio coverage planning

To ensure a seamless communication experience, the SIP-DECT system switches an ongoing DECT phone call from one RFP to another if the radio communication quality drops below a certain threshold. The seamless handover is possible only if the participating RFPs are synchronized. RFP synchronization is performed via radio communication between RFPs, which in turn requires a decent radio coverage planning (see chapter 9.2).

### Clustering / paging areas

Your SIP-DECT system may include different locations, where the distances between the locations prevent the RFPs from performing the over-the-air synchronization. In this case, you need to split your network into clusters (or “synchronization domains”). Assign RFPs to cluster numbers for this (see chapter 7.6.3, “DECT settings” or chapter 8.7.1.2, “DECT tab”).

If your SIP-DECT system consists of a very large number of RFPs, you should configure the paging area size to optimize the signaling necessary for paging a DECT portable part in throughout the SIP-DECT system (see 8.7.2).

### Isolated sites

A separate cluster number is also required, e.g. for a single RFP servicing an office abroad. Also, if the VPN network connection to the isolated site’s RFP cannot transport DHCP, you may use static IP address configuration for the single RFP (see chapter 9.6).

### Wireless LAN (WLAN)

If you purchased a number of WLAN RFPs (RFP L42 WLAN or RFP 42 WLAN), the SIP-DECT system also provides access to your company LAN via Wireless LAN. The WLAN configuration of a group of WLAN RFPs is managed by WLAN profiles (see chapter 7.8).

### PC-based OMM installation

A very large number of RFPs or a large number of DECT portable parts may exceed the storage capacity or processing power of the embedded RFP device. For this reason, it is also possible to operate the OMM on a standard PC under the Linux operating system (see chapter 9.10).

SIP-DECT release 3.0 is tested and released for Red Hat© Enterprise Linux 6 for x86 server.

### Locating application

You can set up a system to locate and track DECT portable parts in your DECT system. This includes a separate Web user interface, which for example can be operated by service personnel to locate a DECT portable part that has triggered an alarm. Refer to the “OpenMobility Location Application” user guide for details, see /25/.

### Extended messaging

You can set up an extended messaging and alarms system, e.g. to provide automated reactions on alarms triggered by DECT portable parts or on alert messages. The extended messaging system may also provide message confirmations, message based services, and may also be integrated with external computer systems. Refer to the “OpenMobility Integrated Messaging & Alerting” user guide for details, see /26/.

### OpenMobility provisioning

While some users in the SIP-DECT system will use their “personal handset”, it is also possible to operate shared handsets. The OpenMobility SIP-DECT solution provides an enhanced DECT Handset Sharing and Provisioning concept that enables to comfortably manage a large amount of DECT handsets and which provides a flexible subscribing model. With this, the SIP-DECT system supports new features such as logging in and out with a personalized user account on different DECT handsets, import of user data from an external

provisioning server, automatically subscribe new DECT handsets or control subscription specific system functions from DECT handsets. Refer also to the “OpenMobility Provisioning” user guide for details see /27/.

### SIP-DECT XML terminal interface



The SIP-DECT XML terminal interface allows external applications to provide content for the user on the DECT handsets display and much more. The list of potential applications is endless. The interface is derived from the XML API for Aastra SIP Phones and coexists with the OM AXI features e.g. text messaging.

Partners can get access to the interface specification /34/ by registering at the A2P2 program.

To call a certain URI there are a number of hooks available for the Aastra 600d/650c handsets which can be put on a programmable key or can be called from a menu.

The following hooks are available:

Hook	Description	Programmable Key	Menu entry
Call log	To replace the local call log	yes	yes
Redial list	To replace the local redial list	yes	yes
Server Menu	Hook to reach a server menu	yes	yes <sup>1</sup>
Presence	Hook to reach a presence application	yes	yes
Applications	List of 10 hooks; each of them can be freely defined (App1 – App10)	yes	yes
App1 – App10	10 hooks which can be freely defined	yes	no
Event Actions	URI to be called in case of user/device events	no <sup>2</sup>	no <sup>2</sup>

<sup>1</sup> The server menu is integrated in the OMM system menu. The (OMM) system menu is available as a menu entry in the local main menu of the handset (soft key ) or directly available by a long press of the soft key . If no user is assigned to the handset, then the server menu is the only available XML application hook.

<sup>2</sup> The URI to be called is configured in the OMM via OMP. Content can be pushed towards the handset via SIP notify. For more information please see /34/.

### SNMP integration / External configuration files

To integrate the SIP-DECT system into external management systems, each RFP runs an SNMP agent that can be queried by SNMP management software (see 9.16). To integrate to external configuration management systems, the DECT system’s configuration is available by means of ASCII-based configuration files. For example, you can configure automatic import or export of configuration files from/to an external server (refer also to the “OpenMobility Provisioning” user guide for details see /27/).

### System configuration tools

You can configure and maintain the SIP-DECT system with two different applications:

- a web-based service (OMM Web service, see chapter 7) and
- a java-based tool (OM Management Portal, OMP, see chapter 8).

Both applications support the essential configuration and administration settings required for smaller SIP-DECT systems. However, for larger SIP-DECT systems using enhanced features, some settings are not available in both applications. To help you to decide which application to use, the following table lists the features and settings that are available in one of the applications:

<b>Feature</b>	<b>Web</b>	<b>OMP</b>
Time zone settings	Yes	No
SNMP configuration	Yes	No
DB management: User data import	No	Yes
Configuration and start of a system dump	No	Yes
Event information display (Event log)	Yes	No
WLAN profile configuration	Yes	No
Dynamic PP subscriptions (OpenMobility provisioning)	No	Yes
Locating settings for PP	No	Yes
Paging areas	No	Yes
Alarm Triggers	No	Yes
RFP sync. View	No	Yes
RFP statistics	No	Yes
RFP data export	No	Yes
Configuration of XMI applications (SIP-DECT XML terminal interface)	No	Yes

## 4 Naming Convention

The naming convention used with SIP-DECT 2.1 or earlier for software deliverable is unified with SIP-DECT 3.0. This applies for the software packaged for the RFPs as well as for the Red Hat® Linux x86 server packages.

SW package	Old	New	Recommended standard name in SIP-DECT installations
SW image for RFP (L) 32/34 IP / RFP (L) 42 WLAN	omm_ffsip.tftp	SIPDECT_<version>.tftp	iprfp2g.tftp
SW image for RFP (L) 35/36/37 IP / RFP (L) 43 WLAN	-	SIPDECT_<version>.dnld	iprfp3g.dnld
OMM software for Linux Red Hat® x86 server (selfextracting executable)	omm_ffsip_install.bin	SIPDECT_<version>.bin	-
SIP-DECT OMM SW rpm	omm_ffsip-OMM-<ommversion>.i586.rpm	SIP-DECT-OMM-<version>.i586.rpm	-
SIP-DECT handset firmware rpm	omm_ffsip-6xxd-<handsetversion>.i586.rpm	SIP-DECTHANDSET-<version>.i586.rpm	-



## 5 Login and Passwords

Interface/Tool	OMM	RFP (L) 32/34 IP / RFP (L) 42 WLAN	RFP (L) 35/36/37 IP / RFP (L) 43 WLAN
Initial configuration via OM Configurator login / password (no previous connection with the OMM)	n.a.	No login required	"omm" / "omm"
Initial OMM configuration via Web or OMP standard full-access account login / password	"omm" / "omm"	n.a.	n.a.
OMM access via Web or OMP (after initial OMM configuration)	Read-only or full-access accounts as configured	n.a.	n.a.
Configuration via OM Configurator after connection with OMM login / password (system wide set by OMM)	n.a.	OMM standard full-access account login / password	OMM standard full-access account login / password
ssh (no previous connection with the OMM)	n.a.	User shell: "omm" / "omm"  Root shell: "root" / "22222"	User shell: "omm" / "omm"  Root shell: "root" / "22222"
ssh (with previous connection with the OMM) (system wide set by OMM)	n.a.	User shell: OMM standard full-access account login / password  Root shell: as configured	User shell: OMM standard full-access account login / password  Root shell: as configured

## 6 Licensing

### 6.1 Licensing Model

Starting with SIP-DECT release 2.1 several features of the Open Mobility system are licensed:

- the system size concerning the number of configured RFPs,
- the software version running the OMM,
- the messaging application, and
- the locating application.

For information on the messaging and locating application please refer to the appropriate documents listed in the section 11.6 References.

Starting with SIP-DECT release 3.0 the G.729 codec is a licensed feature. If G.729 shall be used, an appropriate license is required. This applies to all types of SIP-DECT installations independent from the RFP type.

The G.729 license contains the number of G.729 channel licensed. A SIP-DECT installation does not maintain more G.729 channel than licensed. As soon the number of licensed G.729 connections has been reached, the OMM does not offer this codec in further SIP codec negotiations. If the number of G.729 calls exceeds the license, syslog and health state warnings occur.

<b>System</b>			
Number of radio fixed parts	10	<input type="text"/>	OM System License XXX
Software version	3.0.x	currently running SIP-DECT 3.0RC4	
License key	JLX1A-WZ67G-4DFHS-44A4X-R3ZQX		
<b>Messaging</b>			
Number of users allowed to send messages	10	<input type="text"/>	OM Messaging License XXX
Receiving text messages	✓	OM Messaging & Alerting System License	
License key	L2QEA-187G3-Q7H9T-NJENS-GK68C		
<b>Locating</b>			
Number of users allowed to be located	10	<input type="text"/>	OM Locating License XXX
External locating application	✓	OM Locating Server License	
License key	1Z3UH-WHWFV-FKRW9-8ZGKU-VFUPL		
<b>G.729</b>			
Number of G.729 channels	10	<input type="text"/>	OM G.729 License XXX
License key	UFFGZ-CXG39-W5V25-9K74B-ZDG84		

OM Web service: [Licenses](#) page

There are different license modes available for the user depending on the desired system size:

- Built-in license for activated L-RFP installations
  - Activated L-RFP installation with 1 or 2 RFPs (small system)
  - Activated L-RFP installation with 3 and up to 20 RFPs (medium system)
- Standard license
  - Standard RFP installation with 1 or 2 RFPs (small system)
  - Standard RFP installation with 3 and up to 2048 RFPs (large system; the actual number of RFPs is part of the license)

Additionally the OMM can operate in a demonstration mode.

### Update License


Updates from release 2.1 to 3.0 need an update license. A free update license can be received up to one year after the initial SIP-DECT 2.1 license activation. After this time an update license is required.

## 6.1.1 Latency Timer

The OMM identifies medium and large systems using the unique PARK as well as the MAC addresses of up to three RFPs (called validation RFPs here).


The number of three RFPs guarantees a redundancy when a hardware or network error occurs. On the other hand, an odd number does not allow system duplication with splitting the system into two separate parts.

When the 1<sup>st</sup> validation RFP is disconnected the OMM generates just a warning. This warning will be displayed on the **Status** page of the OM Web service, see also chapter 7.3.


General	
Status	⚠ Not all of the RFPs selected for licensing are currently connected to the OpenMobility Manager. If the next RFP fails the license becomes invalid. Please reconnect the missing RFP, let it repair or obtain a new license with other RFPs.
License type	Standard license
Latency period	71:30 (charging ...) 
PARK	1F1018732C (31100303462609)
MAC address 1	00:30:42:0D:22:42 ✓
MAC address 2	00:30:42:0D:20:80 ✗
MAC address 3	00:30:42:0C:BE:99 ✓

OM Web service: **Status** page

But when the 2<sup>nd</sup> validation RFP is disconnected, the OMM considers a license violation. In this case a latency timer of up to 72 hours starts to decrement. When the timer expires, the OMM restricts all licensed features.

General	
Status	⊘ Please ensure that the RFPs selected for licensing are connected to the OpenMobility Manager.
License type	Standard license
Latency period	72:00 (discharging ...) 
PARK	1F1018732C (31100303462609)
MAC address 1	00:30:42:0D:22:42 ✓
MAC address 2	00:30:42:0D:20:80 ✗
MAC address 3	00:30:42:0C:BE:99 ✗

When the validation RFPs are reconnected to the OMM, the latency timer is incremented until it reaches its maximum of 72 hours. In other words the latency timer must be recharged the same time as the violation last to gain the full redundancy time.

General	
Status	✓
License type	Standard license
Latency period	71:57 (charging ...) 
PARK	1F1018732C (31100303462609)
MAC address 1	00:30:42:0D:22:42 ✓
MAC address 2	00:30:42:0D:20:80 ✓
MAC address 3	00:30:42:0C:BE:99 ✓

## 6.1.2 License Violations and Restrictions

A license can be violated in three ways:

- The number of configured items exceeds the number of licensed items. In this case the associated feature is restricted:
  - the audio stream of calls is dropped after 30 seconds when the number of connected RFPs exceeds the licensed number,
  - the messaging application limits the type of messages to “info”,
  - the locating feature is stopped.
- The software version coded into the activation or license file does not cover the software version running on the OMM.

All of the restrictions above will be activated until either the OMM is restarted with the correct version or the license is replaced covering the correct software version.

- The OMM has no connection to at least 2 of the validation RFPs and the latency timer has expired.

All of the restrictions above will be activated until at least 2 validation RFPs are reconnected to the OMM.

## 6.1.3 G. 729 License Violations

After the grace period of 72h for the violation of common licenses (like activation or installation/system license) telephone calls are limited to 30 seconds for each call. If G.729 was previously licensed, the G.729 codec can still be used for the number of licensed channels for such limited calls.

If all G.729 licenses have been consumed, the remaining licenses are not affected in form of a new license violation:

- No license grace period timer will be started.
- The remaining licenses are not influenced.
- Telephony using other codecs is not influenced.


If all G.729 licenses have been consumed, G.729 will not be offered in the SIP codec negotiation anymore. A dynamic codec change to G.729 will terminate the call with the following actions:

- The reason of the call termination will be displayed on the handset screen and sent as a text message to the handset.
- An event log and a syslog entry are generated.

A system health state for G.729 licenses will be changed to the state ‘Warning’ as long as no G.729 resources are temporarily free (condition: number of G.729 licenses >0 (built-in or license file)).

There is a new predefined alarm trigger “G729ABORT” which is initiated if a call fails:

- a) The remote site offers G.729 but the OMM does not and the setup fails because of no overlap of codec (incl. re-invite and update).
- b) No license can be allocated at the point in time of dynamic codec change.

The G.729 license state will be displayed with a yellow exclamation mark  (Warning: insufficient G.729 licenses) in the OMM configuration user interfaces as long as no G.729

resources are temporarily free (condition: number of G.729 licenses >0 (built-in or license file)).

## 6.2 Uploading an Activation or License File





An activation or a license file must be purchased from the Aastra license server. The license confirmation you received contains detailed information how to generate an activation / license file. The file can be uploaded into the OMM either via Web service (see chapter 7.10) or via the OMP (see chapter 8.9.6).

An activation file as well as a license file contain a PARK for system identification. If the newly imported PARK differs from the current PARK, the OMM will perform a reset.

**Note:** The file can be opened with a text editor to view the license or activation parameter.

## 6.3 Demonstration Mode

When an OMM comes up for the first time, it considers itself as working in demonstration mode. In this mode all of the OMM features can be evaluated without any license for 72 hours starting with the 1<sup>st</sup> RFP being connected to the OMM. In demonstration mode, the audio stream of calls is dropped after 30 seconds.

<b>General</b>	
Status	 Please configure a valid license or activation key to ensure the correct operation of the OpenMobility Manager!
License type	Demonstration mode
Latency period	72:00 (discharging ...) 
PARK	1F100CF0A6 (31100147412304)
<b>System</b>	
Number of radio fixed parts	4096 <input type="text"/> OM System License XXX
Software version	2.1.x currently running private patch based on 2.1.0 Build 10
<b>Messaging</b>	
Users allowed to send text messages	4500 <input type="text"/> OM Messaging License XXX
Receiving text messages	 OM Messaging & Alerting System License
<b>Locating</b>	
Number of locatable users	4500 <input type="text"/> OM Locating License XXX
External locating application	 OM Locating Server License

Display of demonstration mode in the OM Web service

After 72 hours the OMM restricts all features as described in section 6.1.2.

The OMM stays in demonstration mode as long as the default built-in PARK is not changed. The PARK can be changed either on the **System settings** page as described in section 7.4.1. This leads to a small system using the built-in license. Another way to change the PARK is to upload an activation or license file purchased from the Aastra license server (see chapter 6.1.1). This leads to a medium system or large system respectively.

### Notes on demonstration mode

- Multiple OMMs running the Demo license at the same location can influence each other because of the same PARK!
- G.729 is not available if the OMM operates in a demonstration mode.

## 6.4 License Modes

### 6.4.1 Small System

When changing the PARK on the **System settings** page of the OM Web service, the OMM uses the built-in license resp. the standard license for a small system.

The built-in license for a small system features:

- up to two L-RFPs
  - messaging restricted to type “Info”, “Low”, “Normal” and “High” for all user (no “Emergency” and “Locating Alert”), and
  - no locating.

The standard license for a small system features:

- up to two “normal” RFPs
  - no messaging (except prio Info) and
  - no locating.

On a small system it is prohibited to exceed the limits of license due configuration. Since there is no activation or license file present, the software version is not checked. As the system is not validated via RFPs and hence the latency timer does not play any role there are no license violations possible at all.

General	
License type	Build in license for up to 2 radio base stations
PARK	1F1018732C (31100303462609)
System	
Number of radio fixed parts	2 <input type="text"/> OM System License XXX
Software version	2.1.x currently running private patch based on 2.1.0 Build 10
Messaging	
Users allowed to send text messages	4500 <input type="text"/> OM Messaging License XXX
Receiving text messages	<input checked="" type="checkbox"/> OM Messaging & Alerting System License
Locating	
Number of locatable users	- OM Locating License XXX
External locating application	<input checked="" type="checkbox"/> OM Locating Server License

When there are more than 2 RFPs configured while the PARK is changed only the first two RFPs will stay in the configuration database. All other RFPs will be dropped silently.

### 6.4.2 Medium System

When the PARK is changed via the upload of an activation file, the built-in license is activated and the OMM enters the activated system state. In this state the OMM uses the following license features:

- 3 and up to 20 L-RFPs,
- messaging restricted to type “Info”, “Low”, “Normal” and “High” for all user (no “Emergency” and “Locating Alert”), and
- no locating.

The OMM extracts the software version from the activation file and checks this against its own software version. A lower software version within the activation file leads to a license violation.

The OMM prevents a license violation due misconfiguration e.g. it is not possible to configure a 21<sup>st</sup> RFP in the system.

To obtain an activation file from the Aastra license server the MAC address of 3 RFPs must be entered. These 3 validation RFPs are used to validate the activation.

General	
Status	✓
License type	Activated built-in license for up to 20 radio base stations
Latency period	00:36 (charging ...) <input type="text"/>
PARK	1F1018732C (31100303462609)
MAC address 1	00:30:42:0D:22:42 ✓
MAC address 2	00:30:42:0D:20:80 ✓
MAC address 3	00:30:42:0C:BE:99 ✓
System	
Number of radio fixed parts	20 <input type="text"/> OM System License XXX
Software version	2.1.x currently running private patch based on 2.1.0 Build 10
License key	9HDKD-18G78-1L6U7-12QLS-64VK4
Messaging	
Users allowed to send text messages	4500 <input type="text"/> OM Messaging License XXX
Receiving text messages	✓ OM Messaging & Alerting System License
Locating	
Number of locatable users	- OM Locating License XXX
External locating application	✗ OM Locating Server License

While obtaining an activation file from the Aastra license server it is possible to enter the PARK used for a small system installation. This prevents the need to re-subscribe all handsets.

When there are more than 20 RFPs configured (in demonstration mode) while an activation file is uploaded, only the first 20 RFPs will stay in the configuration database. All other RFPs will be dropped silently.

**Note:** Note: When once changed via activation file upload, the PARK cannot be changed any more on the **System settings** page of the OM Web service.

### 6.4.3 Large System

When the PARK is changed via the upload of a license file, the OMM enters the large system state. In this state the OMM uses the following license features coded into the license file.

- System license:
  - 3 and up to 2048 RFPs (L-RFPs or normal RFPs),
  - software version of the OMM allowed to be executed.
- Messaging license:
  - number of messaging clients allowed to send messages,
  - whether clients are allowed to receive messages.
- Locating license:
  - number of locatable handsets,
  - whether the locating application is allowed to execute.

During purchase of a license file from the Aastra license server, the MAC address of 3 RFPs must be entered. These 3 validation RFPs are used to operate the latency timer as described in section 6.1.1.

General			
Status	✓		
License type	Standard license		
Latency period	00:28 (charging ...)	<input type="text"/>	
PARK	1F1018732C	(31100303462609)	
MAC address 1	00:30:42:0D:22:42	✓	
MAC address 2	00:30:42:0D:20:80	✓	
MAC address 3	00:30:42:0C:BE:99	✓	
System			
Number of radio fixed parts	1000	<input type="text"/>	OM System License XXX
Software version	2.1.x	currently running private patch based on 2.1.0 Build 10	
License key	99BRD-EBW12-83W7P-9ZFXJ-HCNM		
Messaging			
Users allowed to send text messages	200	<input type="text"/>	OM Messaging License XXX
Receiving text messages	✓		OM Messaging & Alerting System License
License key	4VJGQ-8T66T-8WTPZ-5LBPC-2XR,RS		
Locating			
Number of locatable users	100	<input type="text"/>	OM Locating License XXX
External locating application	✓		OM Locating Server License
License key	H6DSF-86S6X-3EWWF-SXE9-FNMWK		

When obtaining the license file from the Aastra license server, it is possible to use the PARK used for a small or medium system installation. This prevents the need to re-subscribe all handsets.

**Note:** Note: When once changed via activation file upload, the PARK cannot be changed any more on the **System settings** page of the OM Web service.



## 7 OMM Web Service

The OMM acts as an HTTP/HTTPS server. The HTTP server binds to port 80 and HTTPS binds to port 443 by default. A HTTP request on port 80 will be redirected to HTTPS on port 443. The service access is restricted to one active session at a time and is password protected.

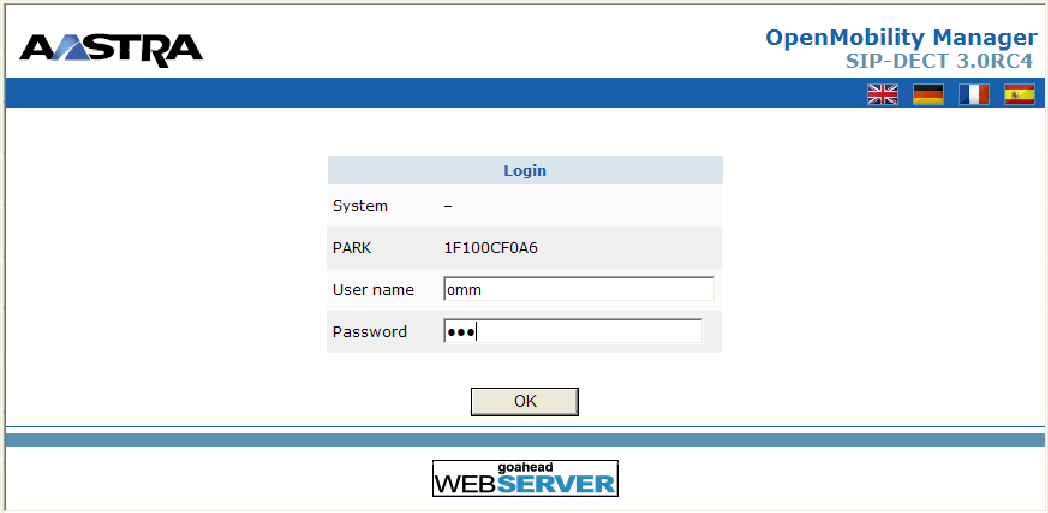
The browser used for service access has to be at least Microsoft Internet Explorer 6.0 or Mozilla Firefox 1.5 and must have frame support, JavaScript and cookies enabled.

**Note:** The service access is restricted to one active session at a time and is password protected.

### 7.1 Login

The OMM allows only one user at a time to configure the system. A user must authenticate with a user name and a password. Both strings are checked case sensitive.

With initial installation or after discarding all settings, the OMM Web service is accessible via a default built-in user account with user “omm” and password “omm”.



With the first login into a new SIP-DECT SW version the user has to accept the End User License Agreement (EULA), see chapter 7.11.

If the default built-in user account is active, the administrator has to change the default account data (passwords) of the “Full access” and “root” account. Refer Initial Setup (see chapter 2.2). The meaning of the different account types is described in section 9.14.1.

**Please note:** The OMM will force to alter the default account data. As long as the passwords are unchanged, the OMM will not allow any other configuration.

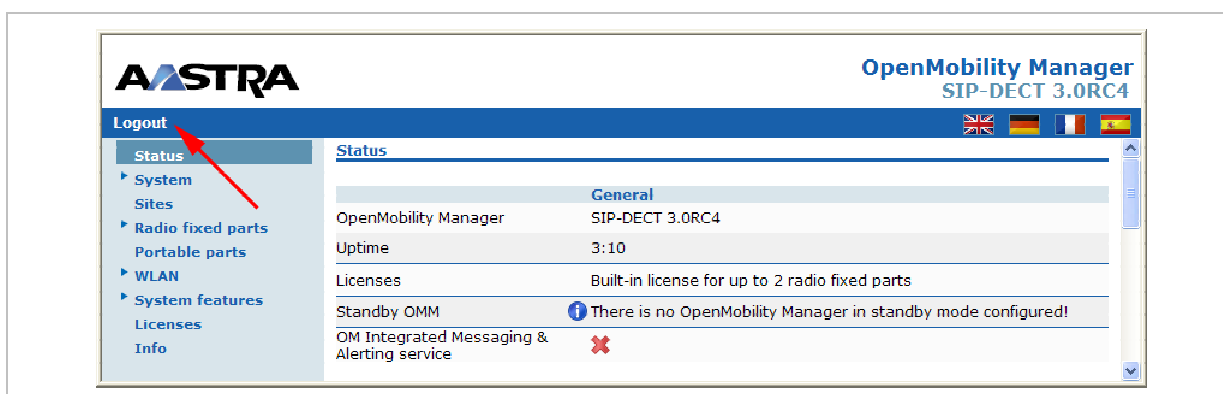
After login in, the following menus are available:

- **Status** menu:  
displays the system status, see chapter 7.3;
- **System** menu:  
allows configuration of general SIP-DECT system parameters, see chapter 7.4;

- **Sites** menu:  
allows to group RFPs into different sites, see chapter 7.5;
- **Radio fixed parts** menu:  
allows configuration and administration of the attached RFPs, see chapter 7.6;
- **Portable parts** menu:  
allows administration of the PPs, see chapter 7.7;
- **WLAN** menu:  
allows configuration of WLAN parameters, see chapter 7.8;
- **System features** menu:  
allows administration of system features like digit treatment and directory, see chapter 7.9;
- **Licenses** menu:  
allows administration of licenses, see chapter 7.10.
- **Info** menu:  
displays the End User License Agreement (EULA), see chapter 7.11.

## 7.2 Logout

If no user action takes place, the OMM automatically logs out the user after 5 minutes. To log out from the system click the **Logout** button on the upper left of the OM Web service screen.



**Note:** If the browser is closed without logging out first, the service access will be blocked for other clients for 5 minutes.

## 7.3 “Status” Menu

The Status page provides information on the SIP-DECT system status. In case of system errors, system warning messages are also displayed on this page.

The screenshot shows the OpenMobility Manager (OMM) web interface. The top header includes the Aastra logo and the text "OpenMobility Manager SIP-DECT 3.0RC4". Below the header is a navigation menu with "Logout" and a language selection bar. The main content area is titled "Status" and is divided into several sections:

- General:**
  - OpenMobility Manager: SIP-DECT 3.0RC4
  - Uptime: 0:08
  - Licenses: Please import a valid license file to ensure the correct operation of the OpenMobility Manager!
  - Grace period: 72:00
  - Standby OMM: There is no OpenMobility Manager in standby mode configured!
  - OM Integrated Messaging & Alerting service:
- Radio fixed parts:**
  - Total number: 0
- Portable parts:**
  - Total number: 0
  - Subscription allowed:
  - Downloading new firmware to portable parts:
  - Loading firmware from: tftp://192.168.112.109/aafon6xxd.dnld
  - State: Delayed during startup phase

## 7.4 “System” Menu

The System menu comprises general parameters to configure and administrate the system parameters of the SIP-DECT solution.

### 7.4.1 “System settings” Menu

The system settings cover global settings for the OpenMobility Manager. The following tasks can be performed:

- configuring the global settings (see the following description in this section),
- updating the OMM (see chapter 7.4.1.2),
- restarting the OMM (see chapter 7.4.1.1).

**AASTRA** OpenMobility Manager SIP-DECT 3.0RC4

Logout

**System settings**

**Status**  
 ⚠ Please check the status page.  
 ⓘ Changing these settings may cause the OpenMobility Manager to be reset.  
 [OK] [Cancel] [Update] [Restart]

**General settings**

System name: SIP Gate  
 Remote access:

**Net parameters**

ToS for voice packets: B8  
 ToS for signalling packets: B8  
 TTL (Time to live): 32  
 VLAN priority call control: 6  
 VLAN priority audio: 6

**DECT settings**

PARK: 1F1E18EBA4 (31170307272202)  
 Encryption:   
 DECT monitor:   
 Regulatory domain: EMEA **Currently used PARK** ⓘ When changing the DECT regulatory domain all radio fixed parts will be reset.  
 DECT authentication code:   
 Portable part user login type: Number

**Downloading new firmware to portable parts**

Active:

**Voice mail**

Voice mail number:

**OM Integrated Messaging & Alerting service**

Active:   
 URL:

**Syslog**

Active:   
 IP address:   
 Port: 0 [Default]

**WLAN settings**

Regulatory domain: DE ⓘ When changing the WLAN regulatory domain all access points will be deactivated.

**Date and time**

Time zone: Central European (CET UTC+1 DST)

The following parameters can be set:

### General settings

- **System Name:** Enter the system name.
- **Remote Access:** Switches on/off the SSH access to all RFPs of the DECT system. For more information on the SSH access see chapter 10.3.5.

### Net parameters

To allow the prioritization of Voice Packets and/or Signaling Packets (SIP) inside the used network the IP parameter ToS (Type of Service) should be configured.

- **ToS for voice packets:** Determines the type of service (ToS resp. DiffServ) byte of the IP packet header for all packets that transport RTP voice streams.
- **ToS for signalling packets:** Determines the type of service (ToS resp. DiffServ) byte of the IP packet header for all packets related to VoIP signaling.
- **TTL (Time to live):** Determines the maximum hop count for all IP packets.
- **VLAN priority call control:** Determines the VLAN priority tag for VoIP-signaling packets.
- **VLAN priority audio:** Determines the VLAN priority tag for RTP packets.

#### DECT settings

- **PARK:** This setting depends on the licensing mode:  
Demo mode: shows the default PARK.  
L-RFP systems: Enter the PARK key as labeled on the OpenMobility CD.  
License file: shows the PARK included in the license file.
- **Encryption:** Activate this option, if you want to enable DECT encryption for the whole system.

**Please note:** Make sure that all deployed 3rd party handsets support DECT encryption. If not, encryption can be disabled per device (see 8.8.4).

- **DECT monitor:** For monitoring the DECT system behavior of the OpenMobility Manager the separate DECT monitor application exists. This tool needs an access to the OpenMobility Manager which is disabled by default and can be enabled here. Because of security, the DECT monitor flag is not stored permanently in the internal flash memory of the OMM/RFP. After a reset the DECT monitor flag is ever disabled.
- **Regulatory domain:** To define where the IP DECT is used the parameter regulatory domain has to be configured. Existing installations are updated to the default value **EMEA**.  
To setup a North American FCC compliant installation the value has to be set to **US (FCC/CI)**. In a North American US (FCC/CI) deployment, ETSI compliant RFPs are made inactive and can not be activated if the regulatory domain is set to **US (FCC/CI)**. Vice-versa is also true.
- **DECT authentication code:** The authentication code is used during initial PP subscription as a security option (see chapter 7.7.1). A code entered here provides a default DECT authentication code for each new created PP. It is optional.
- **Portable part user login type:** Portable part user login type: Two kinds of login types are supported. During the login the user can either be determined by the telephone number (**Number**) or by the unique user login ID (**Login ID**). Both elements are part of each user data set. The **Portable part user login type** setting specifies the system wide login variant.

**Note:** Changing this setting forces an automatic logout of all logged in DECT handsets.

#### Downloading new firmware to portable parts

If the **Active** checkbox is enabled, the “Download over Air” feature is activated. The OMM is acting as a download server which provides the firmware for downloads. For more information on this feature please refer to section 9.17.

## Voice mail

**Voice mail number:** You can configure a system wide voice mail number. This number is used by the Aastra 600d / Aastra 650c handset family if the voice box is called.

## OM Integrated Messaging and Alerting Service

The OpenMobility Manager provides a integrated message and alarm server, which could be activated/deactivated and configured here. For a detailed description see /26/.

## Syslog

The OMM and the RFPs are capable of propagating syslog messages. Enable the **Active** checkbox if you want to use this feature. Enter the **IP address** and the **Port** of the host which should collect these messages.

## WLAN settings

This setting applies to RFPs of the type L42 WLAN. In the **Regulatory domain** field specify the regulatory domain of the WLAN network. This setting depends on the country and is prescribed by the laws of that country. Only the setting prescribed for that country must be used. For more information on the WLAN settings please refer to the sections 7.8 and 9.15.

This settings apply to (L-)42 WLAN and (L-)43 WLAN RFPs. The country and therefore the regulatory domain of the WLAN network are specified in the **Regulatory domain** field. Only the correct country code prescribed for that country must be used. Please use ISO 3166-1 alpha-2 codes which are two-letter country codes defined in ISO 3166-1.

**Please note:** If you upgrade a system to release 3.0, you must configure the appropriate regulatory domain.

## Date and time

If an SNTP is configured the date and time of the configured time zone can by synchronized with the DECT 142 / Aastra 142d and 6xxd handsets. The date and time will be provided by the OMM to these handsets if they initiate a DECT location registration. The rules for a time zone, which is shown on this web page, can be configured in the **Time zones** menu (see chapter 7.4.4). Select the desired zone in the **Time Zone** field.

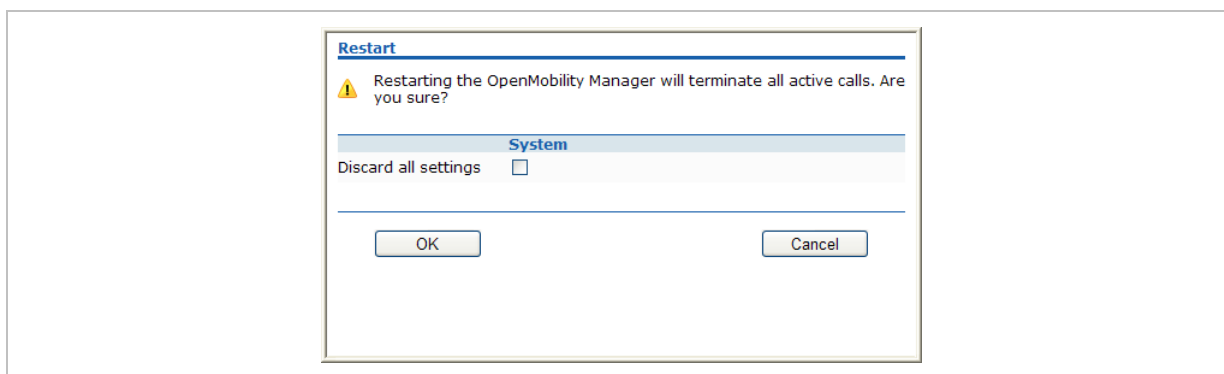
## Notes on System Wide SOS And ManDown Numbers

System wide SOS and ManDown numbers for SOS (142d, 620d, 630d) and sensor initiated calls (630d) can be configured within the SOS and ManDown alarm trigger settings. Please see section 8.9.3.

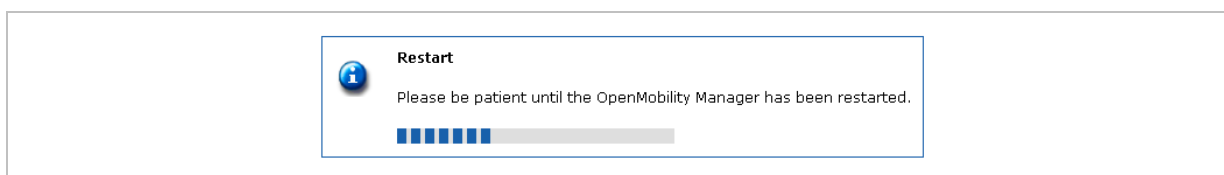
These numbers are used for SOS and ManDown calls if no user specific number is set.

### 7.4.1.1 Restarting the OMM

To restart the OMM call up the **System settings** web page and press **Restart**. There is also the option to reset the configuration data. To do so, activate the **Discard all settings** checkbox.



A reset web page is loaded then displaying a progress bar and the login web page is loaded automatically if the OMM is reachable again.




### 7.4.1.2 Updating the OMM

If the OMM is running on an RFP, the **Update** button is available on the **System settings** web page. After pressing the **Update** button, the RFP residing the OMM checks whether a new boot image file is available on the TFTP server or not. For more details about updating the OMM see the section 9.12.


## 7.4.2 “SIP” Menu

The SIP settings cover all global settings matching the SIP signaling and the RTP voice streams.



**OpenMobility Manager**  
 SIP-DECT 3.0RC4

Logout



- Status
- System
  - System settings
  - SIP
  - User administration
  - Time zones
  - SNMP
  - DB management
  - Event log
  - Sites
  - Radio fixed parts
  - Portable parts
  - WLAN
  - System features
  - Licenses
  - Info

### SIP

**Status**

⚠ Please check the status page.

i Changing these settings may cause the OpenMobility Manager to be reset.

Basic settings	
Proxy server	sipgate.de
Proxy port	5060
Registrar server	sipgate.de
Registrar port	5060
Registration period	3600 sec

Advanced settings	
Outbound proxy server	sipgate.de
Outbound proxy port	5060
Explicit MWI subscription	<input type="checkbox"/>
User agent info	<input checked="" type="checkbox"/>
Dial terminator	#
Registration retry timer	1200 sec
Transaction timer	4000 msec
Blacklist time out	5 min
Determine remote party by	P-Asserted-Identity header
Multiple 180 Ringing	<input checked="" type="checkbox"/>

RTP settings	
RTP port base	16320
Preferred codec 1	G.711 u-law
Preferred codec 2	G.711 A-law
Preferred codec 3	G.729 A
Preferred codec 4	G.722
Preferred packet time	20 msec
Silence suppression	<input type="checkbox"/>
Receiver precedence on CODEC negotiation	<input type="checkbox"/>
Eliminate comfort noise packets	<input type="checkbox"/>

DTMF settings	
Out-of-band	<input checked="" type="checkbox"/>
Method	RTP(RFC 2833)
Payload type	101

Registration traffic shaping	
Active	<input checked="" type="checkbox"/>
Simultaneous Registrations	4
Waiting time	0 msec

Supplementary Services	
Call forwarding / Diversion	<input checked="" type="checkbox"/>
Local line handling	<input checked="" type="checkbox"/>

i When switched off, all R key events (Hook flash) in a call active state will be sent via SIP INFO as DTMF.

The following parameters can be set:

### Basic settings

- **Proxy server:** IP address or name of the SIP proxy server. If a host name and domain are used for the proxy server parameter, ensure that a DNS server and a domain are specified for your SIP-DECT system via DHCP or the OM Configurator tool.
- **Proxy port:** SIP proxy server's port number. Default is 5060. To enable DNS SRV support for proxy lookups, use a value of "0" for the proxy port.



- **Registrar server:** IP address or name of the SIP registrar. Enables the PPs to be registered with a Registrar. If a host name and domain are used for the proxy server parameter, ensure that a DNS server and a domain are specified for your SIP-DECT system via DHCP or the OM Configurator tool.
- **Registrar port:** SIP Registrar's port number. Default is 5060. To enable DNS SRV support for registrar lookups, use a value of 0 for the registrar port.
- **Registration period:** The requested registration period, in seconds, from the registrar. Default is 3600.

### Advanced settings

- **Outbound proxy server:** This setting is optional. You can enter the address of the outbound proxy server in this field. All SIP messages originating from the OMM are sent to this server. For example, if you have a Session Border Controller in your network, then you would normally set its address here.
- **Outbound proxy port:** The proxy port on the proxy server to which the OMM sends all SIP messages. This setting is optional.
- **Explicit MWI subscription:** Some Media Server such as the Asterisk support Message Waiting Indication (MWI) based on /20/. An MWI icon will be presented on an Aastra DECT 142 Handset / Aastra 142d if the user has received a voice message on his voice box which is supported by the Media Server. If **Explicit MWI subscription** is enabled, the OMM sends explicit for each PP an MWI subscription message to the Proxy or Outbound Proxy Server.
- **User agent info:** If this option enabled, the OMM sends information on his version inside the SIP headers *User-Agent/Server*.
- **Dial terminator:** The dial terminator is configurable (up to 2 characters; "0" – "9", "+", "# or empty). The default dial terminator is "#". A dial terminator is necessary if digit treatment shall be applied on outgoing calls and overlapped sending is used.
- **Registration retry timer:** Specifies the time, in seconds, that the OMM waits between registration attempts when the registration is rejected by the registrar.
- **Transaction timer:** The amount of time in milliseconds that the OMM allows a call server (proxy/registrar) to respond to SIP messages that it sends. If the OMM does not receive a response in the amount of time designated for this parameter, the OMM assumes the message as timed out. In this case the call server is recorded to the blacklist. Valid values are 4000 to 64000. Default is 4000.
- **Blacklist time out:** The amount of time in minutes an unreachable call server stays in the blacklist. Valid values are 0 to 1440. Default is 5.
- **Determine remote party by ... header:** The SIP header can be selected from which the remote party information (user id and display name) should be determined. If **P-Asserted-Identity** (default value) is selected, but no such header is received a fallback to the mandatory **From / To** header will be done. This feature can be configured by choosing one of the two values.
  - **Multiple 180 Ringing:** If this feature is deactivated, the OMM sends out only one 180 Ringing response for an incoming call if PRACK is not supported. If this feature is activated, the OMM retransmits multiple times the 180 Ringing response for an incoming call if PRACK is not supported. This ensures that the calling side receives a 180 response in case of packet losses on the network. By default this feature is active.

### RTP settings

- **RTP port base:** Each RFP needs a continuous port area of 68 UDP ports for RTP voice streaming. The RTP port base is the start port number of that area. Default is 16320.
- **Preferred codec 1 – 4:** Specifies a customized codec preference list which allows you to use the preferred codecs. The *Codec 1* has the highest and *Codec 4* the lowest priority.

**Note:** With SIP-DECT Release 3.0 the voice codecs G.722 (wideband), G.711 u-law, G.711 A-law and G.729 A are supported. The previously supported codec G.723 is not available anymore.  
The SIP-DECT license model includes a license for the G.729 codec. The **Licenses** Web page (see also chapter 7.10) provides information about how many G.729 channels are licensed and how many licenses are temporarily in use.

- **Preferred packet time** (10, 20 or 30 msec): Determines the length of voice samples collected before sending out a new RTP packet. A small setting improves voice quality at the expense of data transmission overhead.
- **Silence suppression:** Enables automatic silence detection in the RTP voice data stream to optimize the data transfer volume.
- **Receiver precedence on CODEC negotiation:**
  - The ON (option is enabled) setting means:  
The CODEC selection for incoming SDP offers based on the own preference order list. The first entry in the OMM preferred codec list matching an entry in the incoming SDP offer will be selected.
  - The OFF (option is disabled) setting means:  
The CODEC selection based on the preference order list of incoming SDP offer. The first entry in the incoming order list matching an entry of OMM preferred codec list will be selected. This is the default and is as recommended in RFC 3264.
- **Eliminate comfort noise packets:** If this feature is activated then comfort noise packets are removed from the RTP media stream which causes gaps in the sequence numbers. This can be used if comfort noise packets e.g. in G.711 media streams disturb voice calls in certain installations.

### DTMF settings

- **Out-of-band:** Used to configure whether DTMF Out-of-band is preferred or not.
- **Method:** The OMM supports the following DTMF Out-of-band methods:
  - RTP (RFC 2833)  
Transmit DTMF as RTP events according to RFC 2833 (/14/) after the payload type negotiation via SIP/SDP. If the payload type is not negotiated, "in band" will be used automatically.
  - INFO  
The SIP INFO method is used to transmit DTMF tones as telephone events (application/dtmf-relay). This setting should be used if RFC 2833 is not supported.
  - BOTH  
DTMF telephones events are send according to RFC 2833 and as well as SIP INFO method. **Note:** Possibly, the other party recognizes events twice.
- **Payload type:** If the **Out-of-band** option is enabled, this setting specifies the payload type which is used for sending DTMF events based on section 1.3 reference /14/.

### Registration traffic shaping

Allows to limit the number of simultaneous SIP registrations at startup/fail over of the OMM. If activated, it prevents bursts of SIP registration during startup/fail over of the OMM.

- **Active:** The registration traffic shaping mechanism can be switched off/on herewith.
- **Simultaneous Registrations:** The maximum number of simultaneously started registrations.
- **Waiting time:** The waiting time between a registration finish and starting the next registration in ms (0-1000ms).

**Supplementary ServicesCall forwarding / Diversion:** The handset user can (de)activate call forwarding/diversion in the OMM via menu. In some installations the implemented call forwarding/diversion feature in the IPBX system is in conflict with the OMM based call forwarding/diversion. Thus, the OMM based call forwarding/diversion can be deactivated to let menu on the handset disappear. This setting becomes active on handsets with the next DECT “Locating Registration” process (Can be forced by switching the handset off and on again). An already activated call forwarding is ignored if the call forwarding feature is deactivated.

**Local line handling:** In some installations the implemented multiple line support in the IPBX system is in conflict with the OMM based multiple line support. Thus, the OMM based multiple line support can be deactivated. Note, that the OMM based multiple line support is active by default.

A deactivation of the “Local line handling” flag results in the following implications:

- Only one line is handled for each user (exceptional SOS call <sup>1</sup>)
- If a user presses the “R” key or hook-off key in a call active state a DTMF event is send to the IPBX via SIP INFO including signal 16 (hook-flash). All Hook-flash events are send in every case via SIP INFO independently from the configured or negotiated DTMF method during call setup. All other key events are send via configured or negotiated DTMF method.
- The OMM based call features “Call waiting”, “Call Transfer”, “Brokering” and “Hold” are not any longer supported.
- This setting becomes active on handsets with the next DECT “Locating Registration” process (Can be forced by switching the handset off and on again).

### 7.4.3 “User administration” Menu

After initial installation or after removing the configuration file, the OMM Web service is accessible via a built-in user account with user “omm” and password “omm”.

If the default built-in user account is active, the administrator has to change the default account data of the “Full access” and “Root (SSH only)” account. The meaning of the different account types is described in section 9.14.1.

**Please note:** The OMM will force to alter the default account data. As long as the passwords are unchanged, the OMM will not allow any other configuration.

These settings which are case sensitive can be changed on the **User administration** web page.

The screenshot shows the 'User administration' page in the OpenMobility Manager (SIP-DECT 3.0RC4) interface. The left sidebar contains a navigation menu with 'User administration' highlighted. The main content area is titled 'User administration' and includes a 'Status' section with a warning icon and the text 'Please check the status page.' Below this are 'OK' and 'Cancel' buttons. The 'Local user account' section contains the following fields:

Local user account	
Account type	Full access
Active	<input checked="" type="checkbox"/>
User name	omm
Old password	.....
Password	.....
Password confirmation	.....
Password aging	None

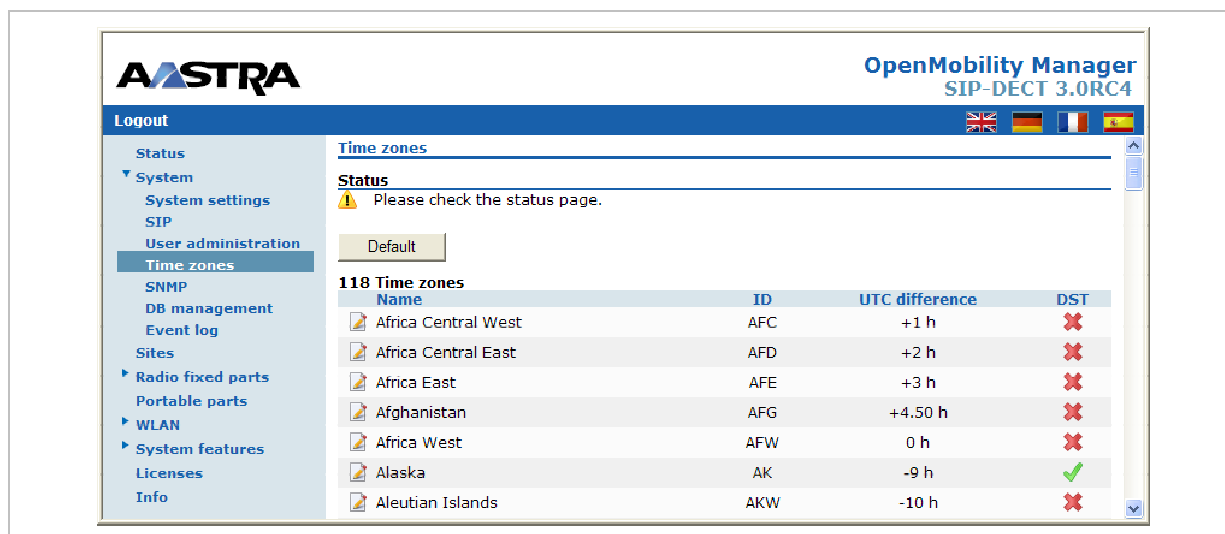
- 1 **Account type:** Select the account type you wish to change.
- 2 **Active:** This setting applies to the **Read-only access** account. Using this account, a user is not allowed to configure any item of the OMM installation. The account can be deactivated.
- 3 **User name:** If desired, enter a new user name.
- 4 **Old password:** To change the password the old password must typed in again.
- 5 **Password, Password confirmation:** Enter the appropriate data in these fields.  
The OMM has several rules to check the complexity of the new password, hence a new password will not be accepted when any of this rules are violated:
  - the new password is not 5 or more characters long,
  - the new password does not contain characters from at least 3 of the following groups: lower case, upper case, digits or other characters,
  - the new password has 50% or more of the same character ('World11111' or 'W1o1r1l1d1'), or
  - the new password contains one of the following items (either upper or lower case as well as forward or backward):
    - account name,
    - host name (IP address),
    - old password, or
    - some adjoining keystrokes (e.g. 'qwert').
- 6 **Password aging:** A timeout for the password can be set. Select the duration, the password should be valid.

---

<sup>1</sup> The OM SOS call feature is unchanged. The initiation of a SOS call in call active state result in the creation of a new line which handles the SOS call.

## 7.4.4 “Time zones” Menu

On the **Time zones** page, the OMM provides all available time zones. They are set with their known daylight savings time rules adjusted to the Universal Coordinated Time (UTC) per default. The difference to the UTC time is shown in the **UTC difference** column. In case of a configured daylight savings time rule (**DST** column) this is also marked for each time zone.



The screenshot shows the OpenMobility Manager SIP-DECT 3.0RC4 web interface. The left sidebar contains a navigation menu with options like Status, System, System settings, SIP, User administration, Time zones (selected), SNMP, DB management, Event log, Sites, Radio fixed parts, Portable parts, WLAN, System features, Licenses, and Info. The main content area is titled 'Time zones' and shows a status message: 'Please check the status page.' Below this is a 'Default' button and a table of 118 time zones. The table has columns for Name, ID, UTC difference, and DST. The DST column contains red 'X' marks for most zones and a green checkmark for Alaska (AK).

Name	ID	UTC difference	DST
Africa Central West	AFC	+1 h	✗
Africa Central East	AFD	+2 h	✗
Africa East	AFE	+3 h	✗
Afghanistan	AFG	+4.50 h	✗
Africa West	AFW	0 h	✗
Alaska	AK	-9 h	✓
Aleutian Islands	AKW	-10 h	✗

The date and time will be provided by the OMM to the Aastra DECT 142 / Aastra 142d and 6xxd handsets if the handset initiates a DECT location registration. This will be done in the following cases:


- subscribing at the OMM,
- entering the network again after the DECT signal was lost,
- power on,
- silent charging feature is active at the phone and the phone is taken out of the charger,
- after a specific time to update date and time.

The following tasks can be performed on the **Time zones** page:

- changing the time zones (see chapter 7.4.4.1),
- resetting time zones (see chapter 7.4.4.2).

### 7.4.4.1 Changing Time Zones

It is possible to change the time zone rules for maximal five time zones. Changed rules are marked with a bold time zone name in the table. The changes are saved in the configuration file and are restored after each OpenMobility Manager startup.

- 1 To change the settings of a time zone, click on the  icon left behind the time zone entry. The **Configure time zone** dialog opens.
- 2 You can change the standard time and the daylight savings time (DST) of a time zone. If the time zone has no DST, only the UTC difference can be configured. For the DST both points of time (begin of standard time and begin of daylight savings time) have to be specified exactly. Therefore a certain day in the month or a certain week day in a month can be used. See the following screenshot as an example:

**Configure time zone**

Time zone	
Name	Africa Central West
ID	AFC
<b>Standard Time</b>	
UTC difference	<input type="text" value="60"/> min
Month	<input type="text" value="0"/> (0 = Not used)
Day	<input type="text" value="0"/> (0 = Not used)
Day of week	<input type="text" value="0"/> (0 = Not used 1 = Sunday 7 = Saturday)
Week	<input type="text" value="0"/> (0 = Not used, 1 = First, 5 = Last)
Hour	<input type="text" value="0"/>
Minute	<input type="text" value="0"/>
<b>Daylight savings time</b>	
Standard time difference	<input type="text" value="0"/> min
Month	<input type="text" value="0"/> (0 = Not used)
Day	<input type="text" value="0"/> (0 = Not used)
Day of week	<input type="text" value="0"/> (0 = Not used 1 = Sunday 7 = Saturday)
Week	<input type="text" value="0"/> (0 = Not used, 1 = First, 5 = Last)
Hour	<input type="text" value="0"/>
Minute	<input type="text" value="0"/>

### 7.4.4.2 Resetting Time Zones

To reset individual time zone settings, press the **Default** button on the **Time zone** web page. This sets all time zones back to the default values and deletes the changed time zone rules in the configuration file.

### 7.4.5 “SNMP” Menu

To manage a larger RFP network, an SNMP agent is provided for each RFP. This will give alarm information and allow an SNMP management system (such as “HP Open View”) to manage this network. On the **SNMP** page of the OMM Web service you configure the SNMP service settings.

**OpenMobility Manager**  
SIP-DECT 3.0RC4

**Logout**

- Status
- System
  - System settings
  - SIP
  - User administration
  - Time zones
  - SNMP**
  - DB management
  - Event log
- Sites
  - Radio fixed parts
  - Portable parts
  - WLAN
  - System features
  - Licenses
  - Info

**SNMP**

**Status**

Please check the status page.

**General settings**

Read-only community	<input type="text" value="public"/>
System contact	<input type="text" value="Charles Brown"/>

**Trap handling**

Trap community	<input type="text" value="trap-secret"/>
Trap host IP address	<input type="text" value="192.168.112.51"/>

The following parameters can be configured using the OMM web service:

### General settings

- **Read-only community:** The SNMP community strings forms a password that is sent by the SNMP management system when querying devices. The query is answered only if the SNMP community string matches. You may use “public” as a default keyword for read-only access.
- **System contact:** Enter a descriptive text that typically is displayed in the SNMP management software.

### Trap handling

Activate the checkbox behind the **Trap handling** section to enable this feature.

- **Trap community:** This community string is used if the SNMP agent informs the SNMP management system about events (Traps).
- **Trap host IP address:** Enter the IP Address that the SNMP agent uses to send traps.

### Further notes

- The RFP needs an initial (one-time) OMM connection to receive its SNMP configuration. In case of a reset, this configuration does not change. Changing the SNMP configuration on the OMM forces all agents to be reconfigured.
- The agent does not support MIB-II write access, SNMPv2-MIB read/write access, NET-SNMP-MIB read/write access, NET-SNMP-AGENT-MIB read/write access and SNMPv3.
- For background information on using SNMP with the SIP-DECT system please refer to section 9.16.

## 7.4.6 “DB management” Menu

The database management (DB management) allows a flexible backup and restore management of the OMM database. The OMM database contains all configuration settings which are configurable via the OMM Web service interface.

The OMM database can be

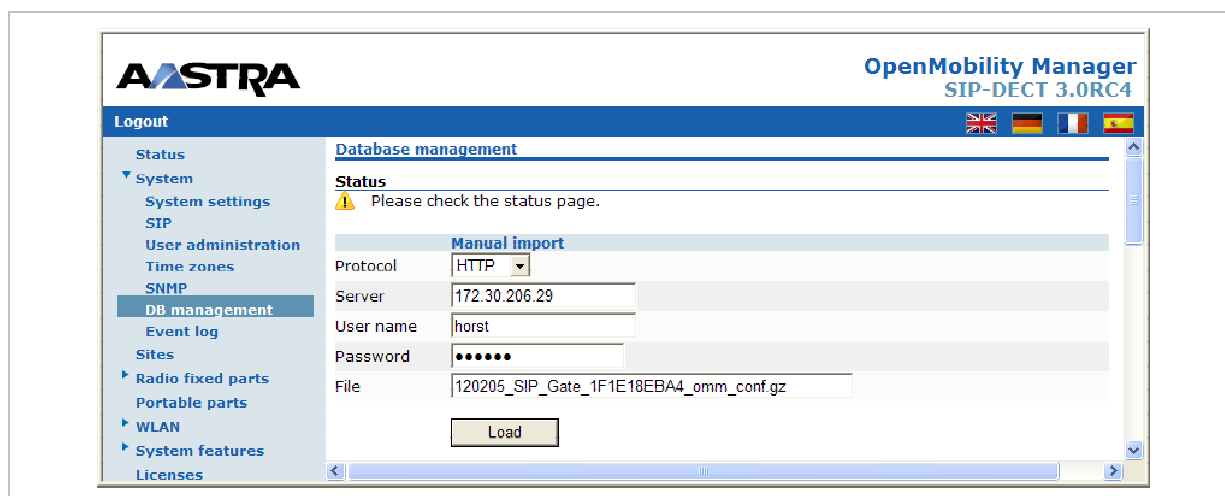
- manually imported from the Web browser’s file system or from an external server (see chapter 7.4.6.1),
- automatically imported from an external server (see chapter 7.4.6.2),
- manually exported to the Web browser’s file system or to an external server (see chapter 7.4.6.3),
- automatically exported to an external server when configuration modifications are done (see chapter 7.4.6.4).

**Note:** The OMM database will be saved in a compressed file in a proprietary format. Any modification of this file outside the OMM is not allowed.

The following protocols for the transport to or from an external server are supported: FTP, TFTP, FTPS, HTTP, HTTPS.

## 7.4.6.1 Manual Database Import

**Please note:** A manual import of a database leads to a reset of the OMM to take effect.



In the **Manual import** section of the **DB management** page enter the following:

**1 Protocol:**

- To import a database from the Web browser's file system the protocol **FILE** has to be selected.
- To import a database from an external server select the preferred protocol (e.g. HTTP).

**2 Server:** Enter the IP address or the name of the external server.

**3 User name, Password** (in case of import from an external server): If necessary, enter the account data of the server.

**4 File:** Enter the path and file name which include the OMM database. If you have selected the **FILE** protocol, the **Browse** button is displayed and you can select the file from the file system.

**5** Press the **Load** button.

Before the OMM accepts the database, a validation check is performed. If the database is verified as valid, the OMM will be reset to activate the new database.

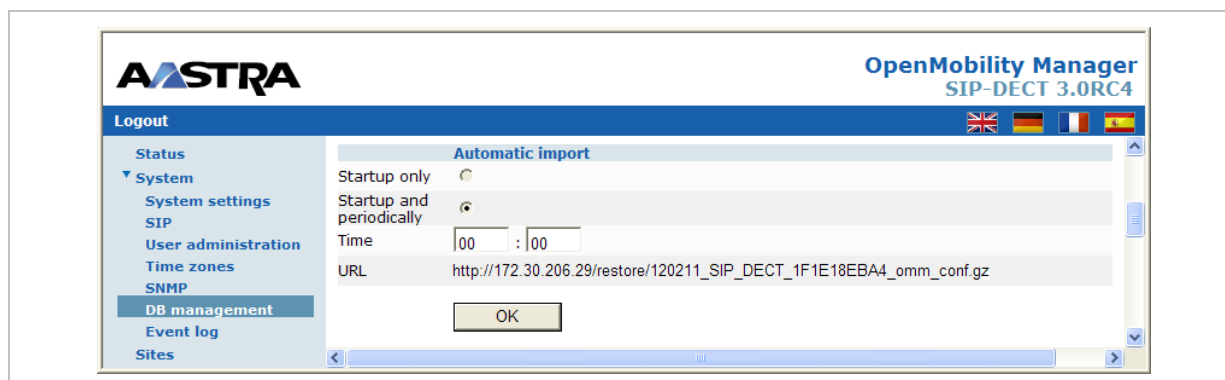
**Note:** After the reset all configurations of the restored database are taken effect but not the user account settings. The user account settings can be only modified locally via the OMM Web service (see chapter 7.4.3) and will never be restored by an database import.

## 7.4.6.2 Automatic Database Import

The automatic database import feature makes it easier to restore a prepared OMM database into an OMM for an initial configuration or for update reasons.

**Please note:** An automatic import of a database leads to a reset of the OMM to take effect.





In the **Automatic import** section of the **DB management** page enter the following:

- 1 **Startup only**: Activate this option if the import should be started for an initial configuration.
- 2 **Startup and periodically**: If this option is activated, the OMM tries to import the configured database file during startup and at the configured time of day.
- 3 **Time**: Enter the time, the import should be started.

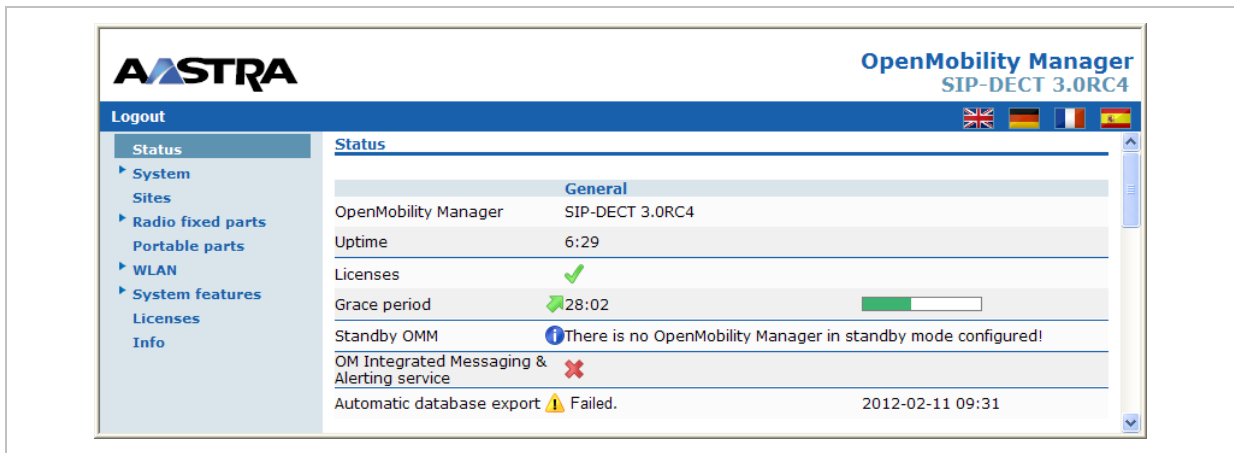
**Please note:** An automatic database import at a configured time recommends the time synchronization with an NTP server. For NTP server configuration see chapter 9.5.4 and chapter 9.6.

- 1 **URL**: The database file for an automatic import has to be configured in an URL format like {ftp|ftps|http|https}://[[user:password@]server]/[directory/]file or tftp://server/[directory/]file. To be available at OMM startup time and to allow an initial configuration via automatic import, this URL has to be specified via DHCP (option 24, see chapter 9.5.4) or OM Configurator (see chapter 9.6). If such a URL is given by DHCP or OM Configurator, the OMM tries to import a configured database file automatically during the OMM startup. The file URL configured via DHCP or OM Configurator is always displayed.
- 2 Click **OK** to confirm the settings for the automatic import.

Before a database is accepted and replaced by automatic import process, the OMM performs the following checks:

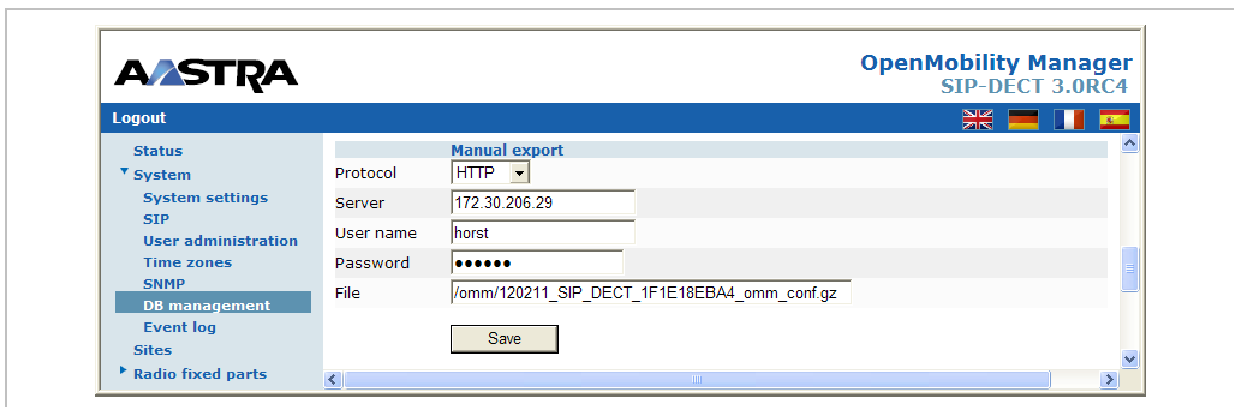
- The integrity of the file must be OK.
- To avoid the import of the same file multiple times, the checksum of the new database file and the checksum of the last database import file (stored in the flash) must be different.
- For authorization/authentication reasons:  
The PARK of the new database file must be the same to the PARK of the current configuration.
- The admin/full access account (see also chapter 9.14.1) of the new database file must be the same to the one of the current configuration. Only if all of these checks are successful the database file is accepted.

If the database file is not accepted or was not found, an error message is displayed on the **Status** page of the OMM Web service.



The automatic OMM database import allows to change all configuration settings but not the account settings and the PARK. There is only one exception: changing the default user account and the PARK for an initial configuration is possible. After the initial configuration, the user account settings and PARK can only be changed via the Web service on the target OMM itself.

### 7.4.6.3 Manual Database Export



In the **Manual export** section of the **DB management** page enter the following:

- 1 **Protocol**: Select the preferred protocol. If you want to export the database to the Web browser's file system, select the **FILE** setting.
- 2 **Server**: Enter the IP address or the name of the server.
- 3 **User name**, **Password**: If necessary, enter the account data of the server.
- 4 **File**: Enter the path and filename where the database is to be saved.
- 5 Press the **Save** button.

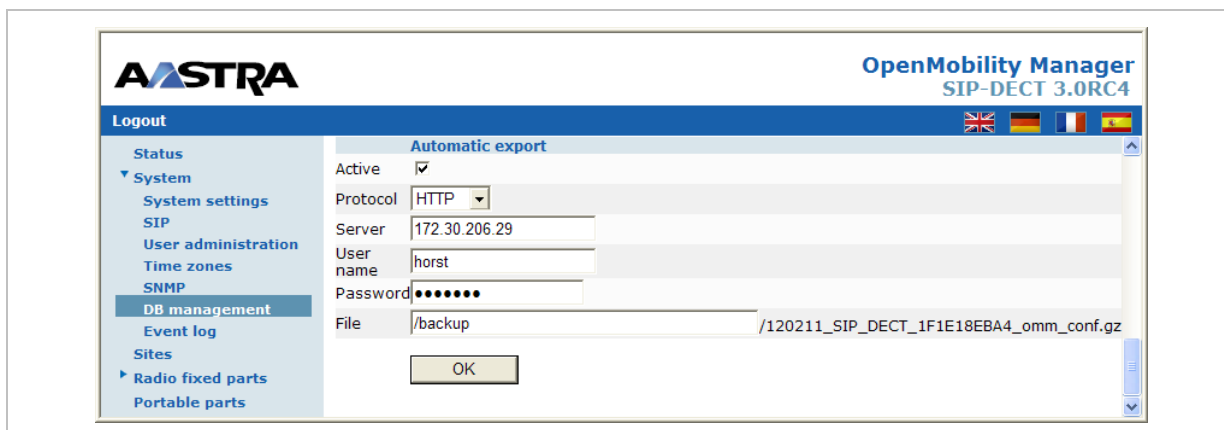
### 7.4.6.4 Automatic Database Export

The automatic database export feature allows an automatic database backup to an external server for each configuration modification.

If this feature is activated, the OMM transfers a backup file to a configured external server any time configuration changes occur, e.g. handset subscription. If there is no configuration

change, then no backup will be done. A backup file will be overwritten during a day if there is more than one modification. A new file will be created when this first change occurs at the day.

**Please note:** For an automatic database export a time synchronization with an NTP server is mandatory. For NTP server configuration see chapter 9.5.4 and chapter 9.6.



In the **Automatic export** section of the **DB management** page enter the following:

- 1 **Active:** Activate this option to enable the automatic export feature.
- 2 **Protocol:** Select the preferred protocol.
- 3 **Server:** Enter the IP address or the name of the server.
- 4 **User name, Password:** If necessary, enter the account data of the server.
- 5 **File:** Enter the path and filename where the database is to be saved.

The OMM writes the database into a file on the external server with following name convention:

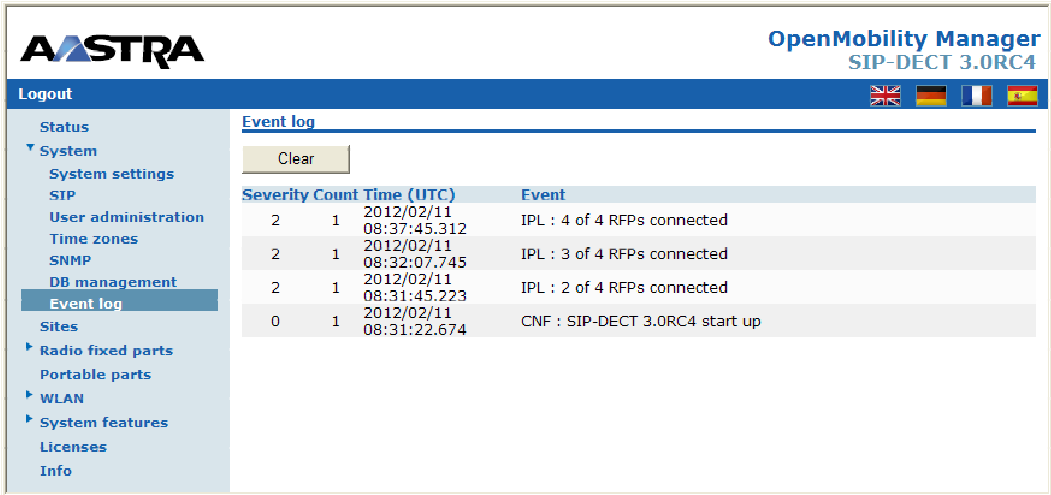
<yymmdd>\_<system\_name>\_<PARK>\_omm\_conf.gz

If the system name contains non-standard ASCII character then these character are replaced by “\_”.

- 6 Press the **OK** button.

## 7.4.7 “Event log” Menu

The **Event log** page displays important event information on OMM system functions, e.g. security aspects. A more detailed system log can be obtained by configuring the **Syslog** function in the **System settings** menu, see chapter 7.4.1.



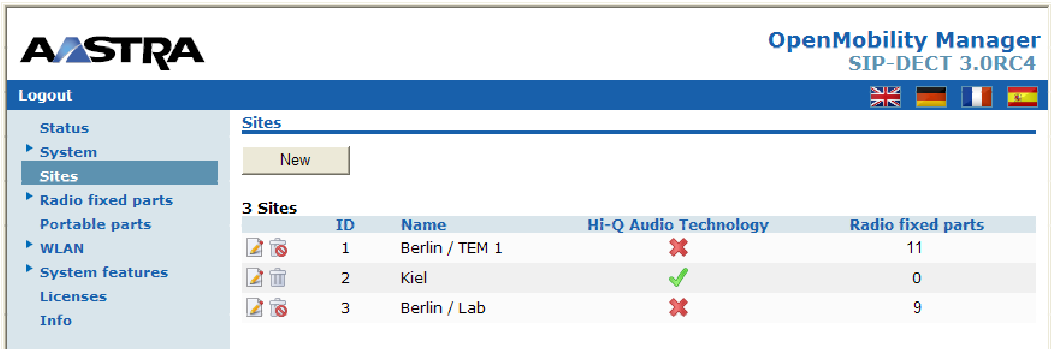
Severity	Count	Time (UTC)	Event
2	1	2012/02/11 08:37:45.312	IPL : 4 of 4 RFPs connected
2	1	2012/02/11 08:32:07.745	IPL : 3 of 4 RFPs connected
2	1	2012/02/11 08:31:45.223	IPL : 2 of 4 RFPs connected
0	1	2012/02/11 08:31:22.674	CNF : SIP-DECT 3.0RC4 start up

To clear the display, press the **Clear** button.

## 7.5 “Sites” Menu

RFPs can be grouped into different sites. A site consists of the following parameters:

- **ID**: Identification number of the site.
- **Name**: The name of the site.
- **Radio fixed parts**: The number of RFPs which are assigned to this site.



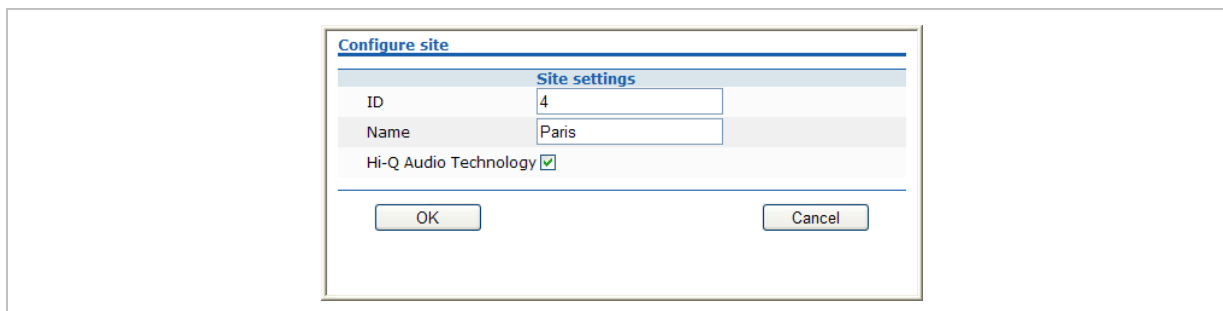
ID	Name	Hi-Q Audio Technology	Radio fixed parts
1	Berlin / TEM 1	✗	11
2	Kiel	✓	0
3	Berlin / Lab	✗	9

The following tasks can be performed:

- creating a new site (see chapter 7.5.1),
- editing a site (see chapter 7.5.2),
- deleting a site (see chapter 7.5.3).

## 7.5.1 Creating a New Site

- 1 On the **Sites** page press the **New** button.  
The **Configure site** dialog opens.




Site settings	
ID	4
Name	Paris
Hi-Q Audio Technology	<input checked="" type="checkbox"/>

- 2 **ID**: Enter the identification number of the site. A value between 1 and 250 is possible. If no value is given, the OMM selects the next free ID.
- 3 **Name**: Enter the name of the site.
- 4 **Hi-Q Technology**: The capability Hi-Q™ audio technology must be enabled or disabled for each site specifically.
  - In sites, which are configured to provide this functionality, exclusively RFP 35/36/37 and RFP 43 WLAN are applicable.
  - In sites without this capability, it is allowed to mix these new RFP types with former RFP 32/34 and RFP 42 WLAN.
- 5 Press the **OK** button.

## 7.5.2 Editing a Site


You can change the name of an existing site:

- 1 On the **Sites** page click on the  icon left behind the site entry.  
The **Configure site** dialog opens.
- 2 Change the site name.
- 3 Press the **OK** button.

## 7.5.3 Deleting a Site

**Note:** Only sites without assigned RFPs can be deleted.

To delete an existing site:

- 1 On the **Sites** web page click on the  icon left behind the site entry.  
The **Delete site** dialog opens.
- 2 Press the **Delete** button.

## 7.6 “Radio fixed parts” Menu

On the **Radio fixed parts** page, all configured RFPs are listed in tables. The RFPs are sorted by their Ethernet (MAC) addresses.

The screenshot shows the 'Radio fixed parts' page in the OpenMobility Manager. The page title is 'Radio fixed parts' and it is sorted by 'DECT clusters'. There are 'New' and 'Import' buttons at the top. Below the buttons, there is a 'Stop' button and a 'Capture allowed: ✓' indicator. The main content area displays a table of 4 Radio fixed parts, categorized into two DECT clusters.

4 Radio fixed parts										
DECT cluster 1: 3 Radio fixed parts										
ID	Name	MAC address	IP address	HW type	Site	RPN	Reflective environment	Connected	Active	
0000	License RFP 3	00:30:42:0D:DF:33	192.168.112.53	RFP L32	1	01	✗	✓	✓	
0001	License RFP 2	00:30:42:0D:10:2E	192.168.112.54	RFP L32	1	02	✗	✓	✓	
0002	License RFP 1	00:30:42:12:6E:3B	192.168.112.43	RFP L43	1	00	✗	✓	✓	
DECT cluster 2: 1 Radio fixed part										
ID	Name	MAC address	IP address	HW type	Site	RPN	Reflective environment	Connected	Active	
0003	-	00:30:42:0D:20:9C	192.168.112.55	RFP 42	1	03	✗	✓	✓	

You can select a sorting criterion for the RFP table. In the **Sorted by** field, select the criterion:

- **DECT clusters:** The RFPs are sorted by clusters. All used clusters are displayed in the navigation bar on the left side. The OMM RFP of each cluster is marked with a bold font.
- **WLAN profiles:** The RFPs are sorted by WLAN profile (see chapter 7.8).
- **Sites:** The RFPs are sorted by sites (see chapter 7.5). All used sites are displayed in the navigation bar on the left side. The OMM RFP of each site is marked with a bold font.

The table provides information on all configured RFPs and their status in several columns:

- **ID:** An internal number that is used to manage the RFP.
- **Name:** Indicates the RFP's name (see chapter 7.6.3).
- **MAC address:** Indicates the RFP's MAC address (see chapter 7.6.3).
- **IP address:** Shows the current IP address of the RFP. The IP address may change over time by using dynamic IP assignment on the DHCP server.
- **HW type:** When the RFPs are connecting the OMM they, submit their HW type. This type is displayed on the RFP list web page. If an error message is indicated in this column, there is a mismatch between the RFP and the OMM SW version (see chapter 7.6.2).
- **Site:** Indicates the site the RFP is assigned to (see chapter 7.5).
- **RPN:** Shows the Radio Fixed Part Number that is currently used by the RFP.
- **Reflective environment:** Indicates if this RFP is operated in a reflective environment (see chapter 7.6.3).
- **Connected:** Indicates if the RFP is connected to the OMM (see chapter 7.6.1).
- **Active:** Indicates if the RFP is active (see chapter 7.6.1).

The following tasks can be performed on the **Radio fixed parts** page:






- creating and changing RFPs (see chapter 7.6.3),

- importing RFP configuration files (see chapter 7.6.4),
- capturing RFPs (see chapter 7.6.5),
- deleting RFPs (see chapter 7.6.6).

## 7.6.1 States of an RFP






For each RFP the state of the DECT subsystem is displayed. These states are:

### Synchronous

ID	Name	MAC address	IP address	HW type	Site	RPN	Reflective environment	Connected	Active
 	0000 License RFP 3	00:30:42:0D:DF:33	192.168.112.53	RFP L32	1	01			





The RFP is up and running. The RFP recognizes and is recognized by other RFPs in its cluster through its air interface and delivers a synchronous clock signal to the PPs.

### Asynchronous

ID	Name	MAC address	IP address	HW type	Site	RPN	Reflective environment	Connected	Active
 	0000 License RFP 3	00:30:42:0D:DF:33	192.168.112.53	RFP L32	1	01			




The RFP has not been able to synchronize to its neighbors yet. No DECT communication is possible. But nevertheless the RFP has already been able to connect to the OMM. This phase should usually last only for a few seconds after starting up the RFP or the OMM. If this state lasts longer this is an indication for a hardware or network failure.

### Searching

ID	Name	MAC address	IP address	HW type	Site	RPN	Reflective environment	Connected	Active
 	0000 License RFP 3	00:30:42:0D:DF:33	192.168.112.53	RFP L32	1	01			

The RFP has lost synchronization to its neighbors. No DECT communication is possible. This phase should usually last only for a few seconds after starting up the RFP or the OMM. If this state lasts longer or is re-entered after being in a synchronous state this is an indication for a bad location of the RFP.

### Inactive

ID	Name	MAC address	IP address	HW type	Site	RPN	Reflective environment	Connected	Active
 	0000 License RFP 3	00:30:42:0D:DF:33	192.168.112.53	RFP L32	1	-	-		-





The RFP has connected to the OMM but the air interface has not been switched on yet. For any RFP with activated DECT functionality this phase should last only for a few seconds after starting up the RFP. If this state lasts longer this may indicate a hardware failure.

### Not connected

ID	Name	MAC address	IP address	HW type	Site	RPN	Reflective environment	Connected	Active
 	0000 License RFP 3	00:30:42:0D:DF:33	-	RFP L32	1	-	-		-

The RFP was configured but has not connected to the OMM yet. Therefore the IP address column is empty.

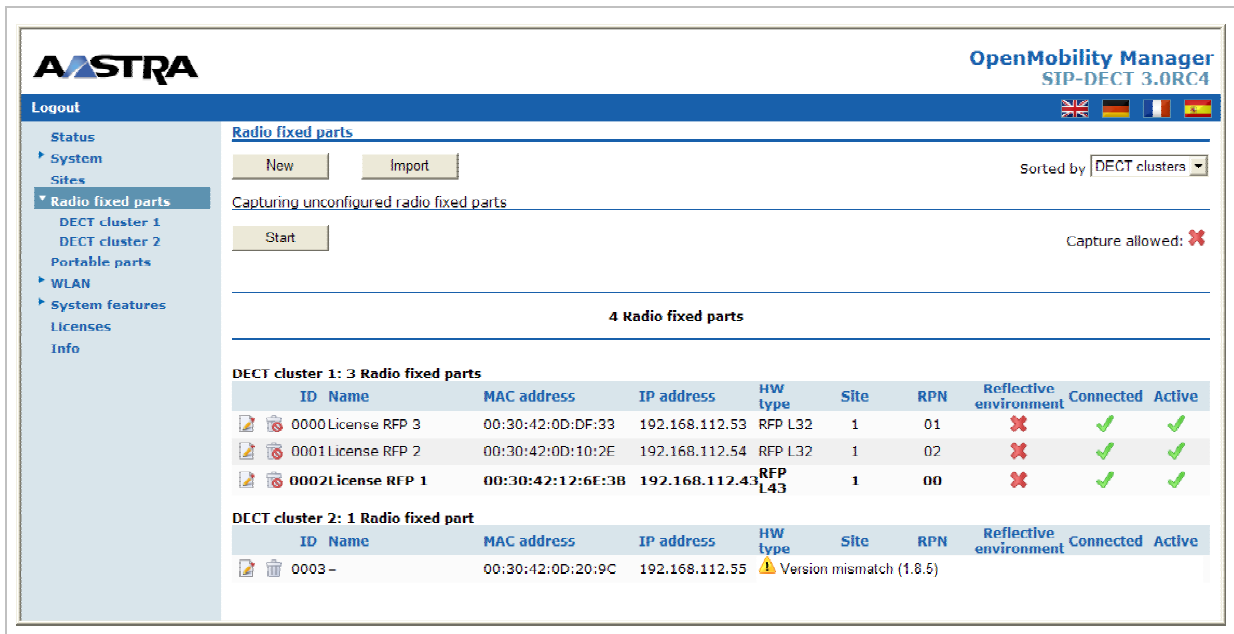
### SW Update available

ID	Name	MAC address	IP address	HW type	Site	RPN	Reflective environment	Connected	Active
 	0000 License RFP 3	00:30:42:0D:DF:33	192.168.112.53	RFP L32	1	01			

The RFP is connected to the OMM. On the TFTP server has found a new software. The RFP is waiting that the OMM initiates a reboot. In the meantime is the RFP full operational.

## 7.6.2 OMM / RFP SW Version Check

When the RFPs are connecting the OMM they submit their SW version. If this version differs from the OMM SW version and the versions are incompatible the RFP connection attempt is rejected. This could happen when using several TFTP servers with different OpenMobility SW versions. In this case the RFP is marked with an error message. Moreover a global error message is displayed on the RFP list web page if at least one version mismatch has been found.



**OpenMobility Manager**  
SIP-DECT 3.0RC4

Logout UK DE FR ES

Status

System

Sites

Radio fixed parts

DECT cluster 1

DECT cluster 2

Portable parts

WLAN

System features

Licenses

Info


**Radio fixed parts**

New Import

Sorted by DECT clusters
















Capturing unconfigured radio fixed parts

Start




Capture allowed: 

4 Radio fixed parts

DECT cluster 1: 3 Radio fixed parts

ID	Name	MAC address	IP address	HW type	Site	RPN	Reflective environment	Connected	Active
 	0000 License RFP 3	00:30:42:0D:DF:33	192.168.112.53	RFP L32	1	01			
 	0001 License RFP 2	00:30:42:0D:10:2E	192.168.112.54	RFP L32	1	02			
 	0002 license RFP 1	00:30:42:12:6E:3B	192.168.112.43	RFP L43	1	00			

DECT cluster 2: 1 Radio fixed part

ID	Name	MAC address	IP address	HW type	Site	RPN	Reflective environment	Connected	Active
 	0003 -	00:30:42:0D:20:9C	192.168.112.55	 Version mismatch (1.8.5)					

## 7.6.3 Creating and Changing RFPs

- To configure a new RFP press the **New** button on the **Radio fixed parts** page.  
To change the configuration of an existing RFP click on the  icon left behind the RFP entry.  
The **New radio fixed part** resp. the **Configure radio fixed part** dialog opens.



Configure radio fixed part	
<b>General settings</b>	
MAC address	00:30:42:0D:20:9C
Name	Lab1
Site	1
<input checked="" type="checkbox"/> <b>DECT settings</b>	
DECT cluster	1
Preferred synchronization source	<input type="checkbox"/>
Reflective environment	<input type="checkbox"/>
<input checked="" type="checkbox"/> <b>WLAN settings</b>	
WLAN profile	2
Antenna diversity	<input type="checkbox"/>
Antenna	1
802.11 channel	6
Output power level	Full
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

RFP 42 configuration

Configure radio fixed part	
<b>General settings</b>	
MAC address	00:30:42:12:6E:3B
Name	License RFP 1
Site	1
<input checked="" type="checkbox"/> <b>DECT settings</b>	
DECT cluster	1
Preferred synchronization source	<input type="checkbox"/>
Reflective environment	<input type="checkbox"/>
<input checked="" type="checkbox"/> <b>WLAN settings</b>	
WLAN profile	1
802.11 channel	1
Output power level	Full
HT40	<input type="checkbox"/>
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

RFP 43 configuration

2 Configure the RFP, see parameter description below.

3 Press the **OK** button.

The following parameters can be set in the **New radio fixed part** resp. the **Configure radio fixed part** dialog:

#### General settings

- **MAC address:** Each RFP is identified by its unique MAC address (6 bytes hex format, colon separated). Enter the MAC address, it can be found on the back of the chassis.
- **Name:** For easier administration each RFP can be associated with a location string. The location string can hold up to 20 characters.
- **Site:** If several sites exist (see chapter 7.5), select the site the RFP is assigned to.

## DECT settings

The DECT functionality for each RFP can be switched on/off.

- **DECT cluster:** If DECT is active the RFP can be assigned to a cluster.
- **Preferred synchronization source:** Activate this checkbox if the RFP should be used as synchronization source for the other RFPs in the cluster. For background information on RFP synchronization please refer to chapter 9.2.
- **Reflective environment:** Within areas containing lot of reflective surfaces (e.g. metal or metal coated glass) in an open space environment the voice quality of a DECT call can be disturbed because of signal reflections which arrive on the handset or RFP using multipath propagation. Calls may have permanent drop outs while moving and high error rates on the RFPs and handsets.

For such environment Aastra has developed the DECT XQ enhancement into the RFP base stations and the Aastra 600d handsets family. Using this enhancement by switching the **Reflective environment** flag on might reduce drop outs and cracking noise.

As soon as **Reflective environment** is switched on, the number of calls on an RFP is reduced to 4 calls at the same time.

**Please note:** The RFPs and handsets use more bandwidth on the Air Interfaces if the “Reflective environment“ is switched on. Therefore this shall only be used when problems sourced by metal reflections are detected.

## WLAN settings

The WLAN section applies to RFPs of the type “RFP 42 WLAN” and “RFP L42 WLAN” only. For details about WLAN configurations please see chapter 9.15.

RFP 42 WLAN and RFP 43 WLAN have different WLAN parameters, which are configurable in the RFP configuration dialog.

- Activation check box: Enables or disables the WLAN function for this RFP.
- **WLAN profile:** Select the desired profile from the list. This applies all settings made in the respective WLAN profile to the current RFP. For information on configuring WLAN profiles see chapter 7.8.1.

**Please note:** WLAN settings are only configurable, if the RFP has been connected at least once to detect the HW type and a proper WLAN profile is configured (see also chapter 7.8.1. WLAN can not be enabled in the “New radio fixed part” dialog if the HW type is unknown.

The following settings are not applied by the WLAN profile. Configure these settings for each RFP individually.

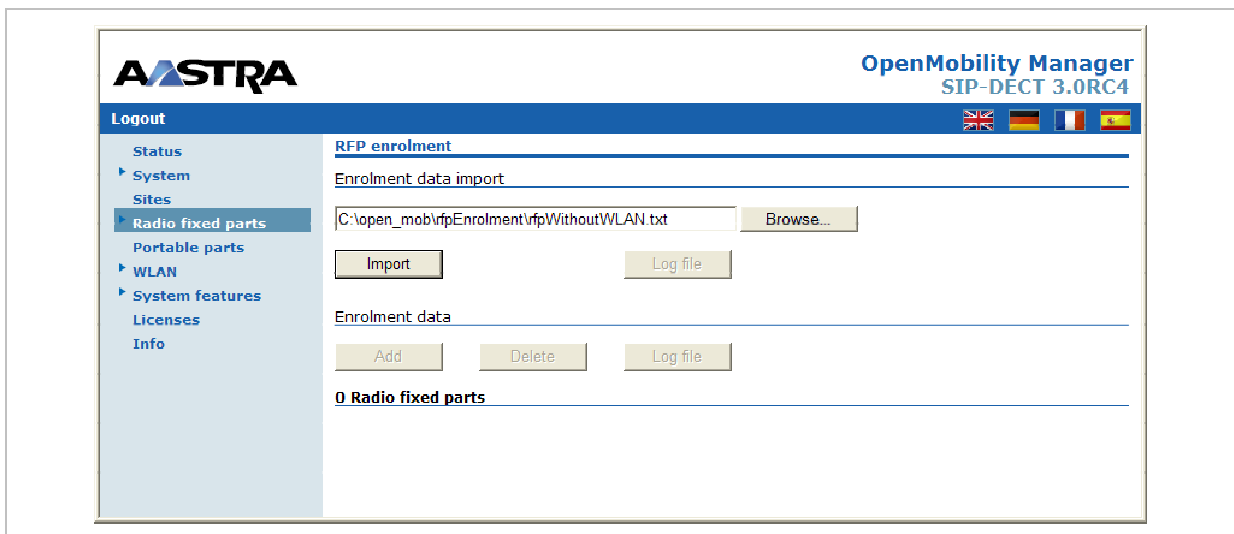
- **Antenna diversity** (RFP 42 WLAN only): This option should generally be activated so that the AP (Access Point) can automatically select the antenna with the best transmission and reception characteristics.
- **Antenna** (RFP 42 WLAN only): If **Antenna diversity** is switched off, this setting determines the antenna that is used for transmitting or receiving WLAN data.
- **802.11 channel:** Determines the WLAN channel used by the current RFP. The channel numbers available are determined by the WLAN **Regulatory domain** setting on the **System settings** page (see 7.4.1).

- **Output power level** (default: “Full”): Determines the signal power level used by the RFP to send WLAN data. You may limit the power level to minimize interferences with other WLAN devices. The actual power level is also capped by the WLAN **Regulatory domain** setting on the **System settings** page.
- **HT40** (RFP 43 WLAN only): High throughput mode with 40 MHz bandwidth increases data rate up to 300 Mbit/s.

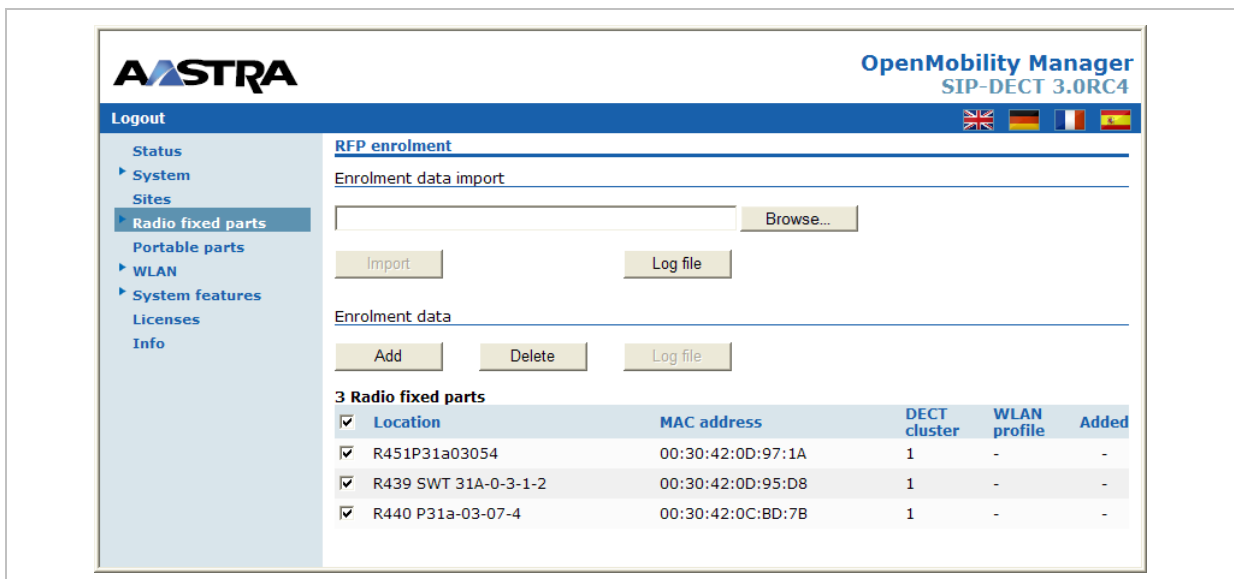
## 7.6.4 Importing RFP Configuration Files

A set of RFPs can also be configured in a semiautomatic manner by import of a configuration file.

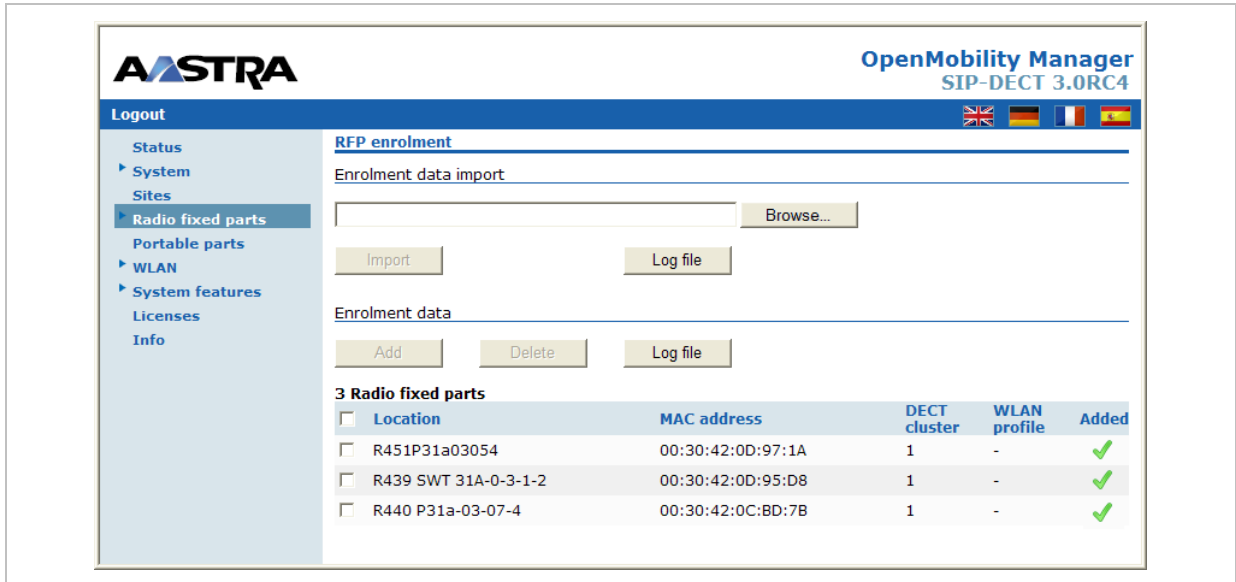
- 1 On the **Radio fixed parts** page press the **Import** button.  
The **RFP enrolment** page opens.



- 2 Select your configuration file and press the **Import** button. For information on the file layout see chapter 11.7.2.
- 3 A parsing protocol can be read, if you press the referring **Log file** button. All successfully imported data records are presented in a list:



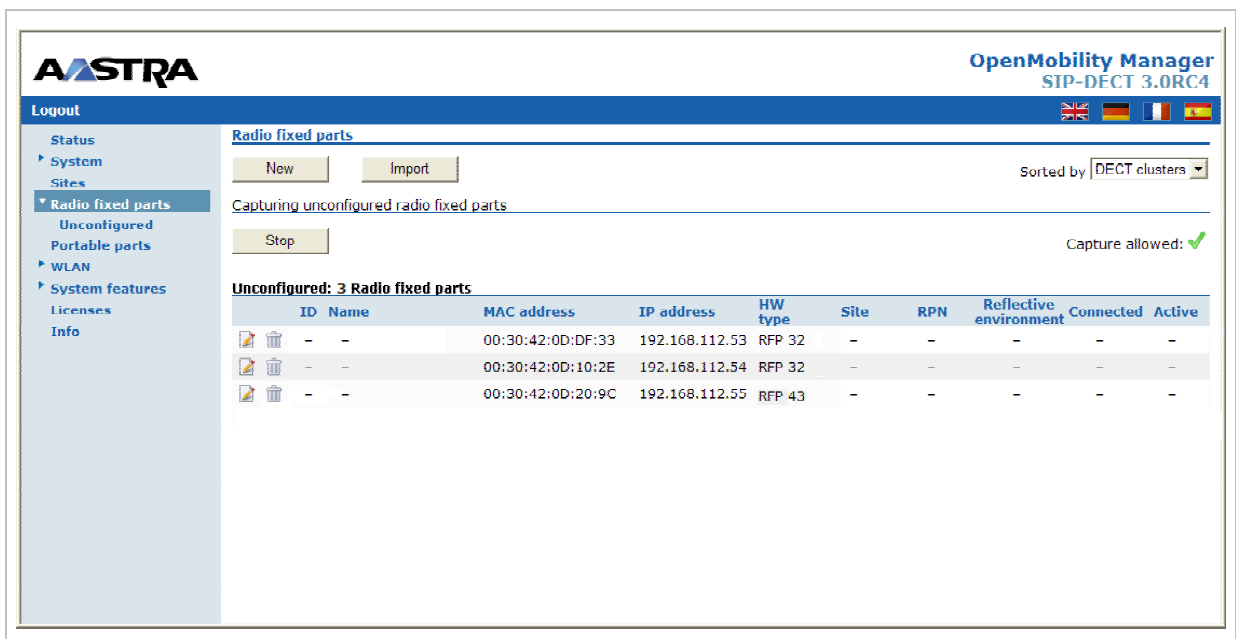
- 4 Select the RFPs you want to add to the OMM database by selecting the appropriate checkboxes.
- 5 Press **Add**.  
All successfully stored records are marked green in the **Added** column.  
Failed records are marked with a red star.



- 6 To read error hints in the referring log file, press the **Log file** button. Error hints can also be read in a syslog trace (see chapter 7.4.1).
- 7 To remove imported data entries, activate the check box next to the desired entries. Press **Delete** to remove the selected entries.


## 7.6.5 Capturing RFPs

RFPs, which are assigned to the OMM by DHCP options or OM Configurator settings, may plug to the system.




- 1 On the **Radio fixed parts** page press the **Start** button.  
After a while the list page is filled by the MAC addresses of those RFPs which tried to register to the OMM (unregistered RFPs).


**Note:** Please note that these entries are not really stored (they are lost after reset).

- 2 By pressing the customize icon  of the appropriate RFP, you can add further data and store the RFP (see chapter 7.6.3).

## 7.6.6 Deleting RFPs

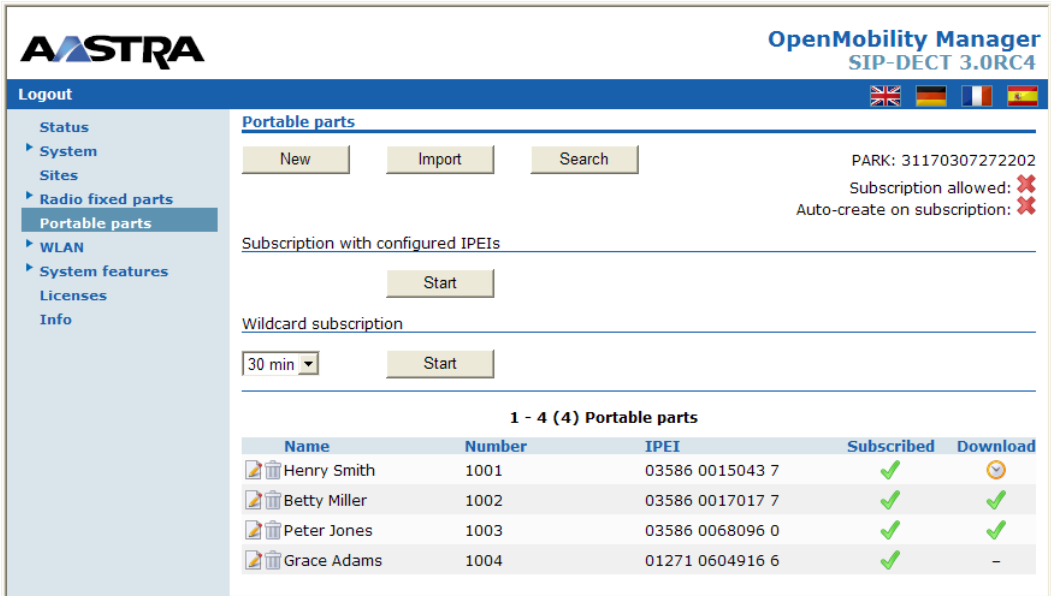
To delete an existing RFP:

- 1 On the **Radio fixed parts** page click on the  icon left behind the RFP entry.  
The **Delete radio fixed part?** dialog opens showing the current configuration of this RFP.
- 2 Press the **Delete** button.






**Please note:** The RFPs bound to a license (License RFPs) can not be deleted. The License RFPs are displayed in the RFP list with a license icon  instead of the trash icon. For further information on licenses see chapter 4).

## 7.7 “Portable parts” Menu

The **Portable parts** web page provides an overview of all configured DECT handsets (Portable Parts) sorted by their number. To keep the list concise, the complete list is split up into sub lists containing up to 100 handsets. The user can move back and forth in steps of 100 handsets.





The screenshot shows the OpenMobility Manager SIP-DECT 3.0RC4 web interface. The left sidebar contains a navigation menu with options: Status, System, Sites, Radio fixed parts, Portable parts (selected), WLAN, System features, Licenses, and Info. The main content area is titled 'Portable parts' and includes buttons for 'New', 'Import', and 'Search'. Below these buttons, there are sections for 'Subscription with configured IPEIs' and 'Wildcard subscription', each with a 'Start' button. A table titled '1 - 4 (4) Portable parts' displays the following data:

Name	Number	IPEI	Subscribed	Download
 Henry Smith	1001	03586 0015043 7	✓	
 Betty Miller	1002	03586 0017017 7	✓	✓
 Peter Jones	1003	03586 0068096 0	✓	✓
 Grace Adams	1004	01271 0604916 6	✓	-

The table provides information on the PPs and their status in several columns:

- **Name:** Indicates the PP name.
- **Number:** Indicates the internal call number of the PP.


- **IPEI**: Indicates the PP' IPEI.
- **Subscribed**: Indicates if the PP subscribed to the system.
- **Download**: This column is only presented if the “Download over Air” feature is started successfully and gives information about the download status of the handset SW (see chapter 9.17).

**Note:** All PP data that are configured as unbound (split into device and user data) are also listed at the OM Web service when user are logged in at the device, but they can not be deleted or changed. This is indicated by the  and  icons.

The following tasks can be performed on the **Portable parts** page:

- creating and changing PPs (see chapter 7.7.1),
- importing PP configuration files (see chapter 7.7.2),
- subscribing PPs (see chapter 7),
- deleting PPs (see chapter 7.7.4),
- searching within the PP list (see chapter 7.7.5).

## 7.7.1 Creating and Changing PPs

- 1 To configure a new PP press the **New** button on the **Portable parts** page. To change the configuration of an existing PP click on the  icon left behind the PP entry. The **New portable part** resp. the **Configure portable part** dialog opens.

**New portable part**

General settings	
Name	Tony
Number	5147
IPEI	0358600083186
DECT authentication code	1234
Login/Additional ID	101
SOS number	911
ManDown number	912
Voice mail number	400

SIP authentication	
User name	
Password	••••
Password confirmation	••••

**Configure portable part**

i Changing Number and/or IPEI requires the PP to be subscribed again.

General settings	
Name	Henry Smith
Number	1001
IPEI	03586 0015043 7
DECT authentication code	1001
Login/Additional ID	
Delete subscription	<input type="checkbox"/>
SOS number	
ManDown number	
Voice mail number	

SIP authentication	
User name	om-1001
Password	●●●●●●●●●●
Password confirmation	●●●●●●●●●●

2 Configure the PP, see parameter description below.

3 Press the **OK** button.

The following parameters can be set in the **New portable part** resp. the **Configure portable part** dialog:

#### General settings

- **Name:** The name parameter represents the SIP Display Name field. This parameter is optional but recommended.
- **Number:** The number is the SIP account number or extension for the PP.
- **IPEI:** The IPEI is the DECT handset IPEI number. On an Aastra 142d handset, the IPEI can be found via the following path of the device menu **Main menu > Phone settings > System**. On an Aastra 600d / 650c handset, the IPEI can be found in the **System** device menu. Consult the handset's user guide for further information.
- **DECT authentication code:** The DECT authentication code is used during initial DECT subscription as an security option and can be set here for each PP separately. If a global DECT authentication code is given on the **System settings** page (see chapter 7.4.1), this value is filled in here as default. This parameter is optional.
- **Login/Additional ID:** The additional ID can be used as a mean for data search within wildcard subscription (because of the IPEI is not configured which selects the data otherwise).

**Note:** The authentication code and additional ID can only be changed if the PP is not subscribed.

- **Delete subscription:** This option is only available when configuring an existing PP (in the **Configure portable part** dialog). If this option is selected, the PP will be unsubscribed.

- **SOS number, ManDown number:** SOS and ManDown are calling numbers which will be automatically called as soon as an SOS or ManDown event happens. If no individual SOS or ManDown number is configured for a handset the number of the appropriate alarm trigger will be used as calling number in case of a SOS or ManDown event. Please see chapter 8.9.3 and /28/ for details.
- **Voice mail number:** The voice mail number is the number which will be automatically called as soon as a voice mail call is initiated on the Aastra 600d / Aastra 650c handset. If there is no individual voice mail number configured in this field, then the system wide voice mail number is used (see also the **System setting** menu, chapter 7.4.1). If there is no voice mail number configured (neither the individual nor the system wide) or another handset type is used, then the voice mail number must be configured locally in the handset.

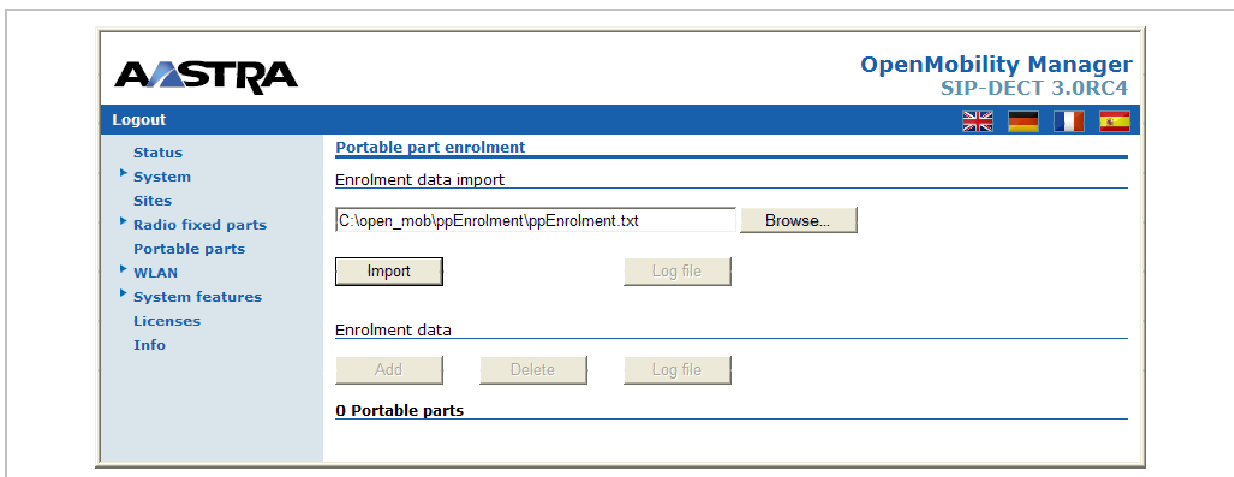
### SIP authentication

- **User name:** The SIP Authentication user name is optional but recommended. It represents the name which will be used during SIP registration and authentication. If no name is given the number will be used by default.
- **Password, Password confirmation:** The password will be used during SIP registration and authentication. Enter the appropriate data in these fields.

## 7.7.2 Importing PP Configuration Files

A set of PPs can also be configured in a semiautomatic manner by import of a configuration file.

- 1 On the **Portable parts** page press the **Import** button.  
The **Portable part enrolment** page opens.



- 2 Select your configuration file and press the **Import** button. For information on the file layout see chapter 11.7.1.
- 3 A parsing protocol can be read, if you press the referring **Log file** button. All successfully imported data records are presented in a list:



**Aastra** OpenMobility Manager  
SIP-DECT 3.0RC4

Logout

- Status
- System
- Sites
- Radio fixed parts
- Portable parts
- WLAN
- System features
- Licenses
- Info

**Portable part enrolment**

Enrolment data import

Enrolment data

**12 Portable parts**

<input checked="" type="checkbox"/> Name	Number	IPEI	DECT authentication code	Additional ID	Added
<input checked="" type="checkbox"/> PP 1	101	0081008625768	1001	101	-
<input checked="" type="checkbox"/> PP 4	104	0007701154842	1002	104	-
<input checked="" type="checkbox"/> Kiel Phone1	5401	0127105395099	1003	5401	-
<input checked="" type="checkbox"/> Karl May	5402	-	1004	5402	-
<input checked="" type="checkbox"/> Karl Valentin	5403	-	1005	5403	-
<input checked="" type="checkbox"/> Karl Heinz	5404	-	1006	5404	-
<input checked="" type="checkbox"/> Radi Radenkowicz	5405	-	1007	5405	-
<input checked="" type="checkbox"/> Radi Rettich	5406	-	1008	5406	-
<input checked="" type="checkbox"/> Wadi Wade	5407	-	1009	5407	-
<input checked="" type="checkbox"/> -	5408	-	1010	5408	-
<input checked="" type="checkbox"/> -	5409	-	1011	5409	-
<input checked="" type="checkbox"/> -	5410	-	1012	5410	-

- Select the PPs you want to add to the OMM database by selecting the appropriate checkboxes.
- Press **Add**.

**AASTR** OpenMobility Manager SIP-DECT 3.0RC4

Logout

Portable part enrolment

Enrolment data import

Import Log file

Enrolment data

Add Delete Log file

**12 Portable parts**

<input type="checkbox"/> Name	Number	IPEI	DECT authentication code	Additional ID	Added
<input type="checkbox"/> PP 1	101	0081008625768	1001	101	✓
<input type="checkbox"/> PP 4	104	0007701154842	1002	104	✓
<input type="checkbox"/> Kiel Phone1	5401	0127105395099	1003	5401	✓
<input type="checkbox"/> Karl May	5402	-	1004	5402	✓
<input type="checkbox"/> Karl Valentin	5403	-	1005	5403	✓
<input type="checkbox"/> Karl Heinz	5404	-	1006	5404	✓
<input type="checkbox"/> Radi Radenkowicz	5405	-	1007	5405	✓
<input type="checkbox"/> Radi Rettich	5406	-	1008	5406	✓
<input type="checkbox"/> Wadi Wade	5407	-	1009	5407	✓
<input type="checkbox"/> -	5408	-	1010	5408	✓
<input type="checkbox"/> -	5409	-	1011	5409	✓
<input type="checkbox"/> -	5410	-	1012	5410	✓

All successfully stored records are marked green in the **Added** column.

Failed records are marked with a red star.

- 6 To read error hints in the referring log file, press the **Log file** button. Error hints can also be read in a syslog trace (see chapter 7.4.1).
- 7 To remove imported data entries, activate the check box next to the desired entries. Press **Delete** to remove the selected entries.

### 7.7.3 Subscribing PPs

#### Preparation by OMM Web service

After adding a PP configuration to the OMM, the PP must be subscribed. The OMM must first be enabled to allow subscriptions to be take place from PP handsets. This is done by pressing the following buttons on the Portable Parts OMM web page.

- **Start** button of the **Subscription with configured IPEIs** section (see chapter 7.7.3.1). This button enables the subscription for the next 24 hours.
- or
- **Start** button and time interval of the **Wildcard Subscription** section (see chapter 7.7.3.2). This button enables the “wildcard subscription” for the selected time. After expiry the “subscription with configured IPEIs” is still enabled for 24 hours.

**Note:** To ease the first installation of a DECT system, the subscription is enabled permanently while at least one PP (with IPEI) is set up within the database and no PP is subscribed. After successful subscription of the first PP the subscription will still be enabled for 24 hours.

**OpenMobility Manager**  
SIP-DECT 3.0RC4

Logout

Portable parts

New Import Search

PARK: 31170307272202  
Subscription allowed: X  
Auto-create on subscription: X

Subscription with configured IPEIs

Start

Wildcard subscription

30 min Start

1 - 4 (4) Portable parts

Name	Number	IPEI	Subscribed	Download
Henry Smith	1001	03586 0015043 7	✓	📄
Betty Miller	1002	03586 0017017 7	✓	✓
Peter Jones	1003	03586 0068096 0	✓	✓
Grace Adams	1004	01271 0604916 6	✓	-

**Note:** To allow an unbound device subscription, the **Auto-create on subscription** flag must be set with the help of the OM Management Portal (OMP). Please see chapter 8.5.1 for details.

### Subscription steps, done by PP

After the PP configuration is complete on the OMM and the OMM is allowing new subscriptions, each PP must subscribe to the system.

On each PP handset, the administrator or user must subscribe to the SIP-DECT system through the System/Subscriptions menu. The specific PArk code for the SIP-DECT system should be entered in order to subscribe to the system.

**Please note:** The PArk code in numeric format can be found at the top-right corner of the Portable Parts OMM web page. Each SIP-DECT deployment will have a unique PArk code that was provided with the OMM Activation kit.

If the administrator configured a global or individual Portable Part DECT authentication code, the administrator/user must enter in the code before the PP will subscribe to the system.

In case of “wildcard subscription”, please note that an additional ID may be configured (see sub section Wildcard Subscription), which has to be typed then.

If administrators/users have any difficulties subscribing to the SIP-DECT system, it is recommended that they power-off the PP handset and reattempt subscription again. This completes the subscription process for a PP on the SIP-DECT system.

### 7.7.3.1 Subscription with Configured IPEI

The PP data to be assigned to the subscribing PP are identified by the IPEI. Furthermore the IPEI leads to a further guarantee not to receive none authorized subscriptions even if AC is not set as a mean to achieve security.

To enable subscriptions, press the **Start** button of the section **Subscription with configured IPEIs** on the **Portable parts** page.

The OMM will allow a subscription of configured but not subscribed PPs during the next hour only. The administrator must press the **Subscribe** button again to permit more PP handsets to subscribe to the SIP-DECT system.

### 7.7.3.2 Wildcard Subscription

To minimize administration effort, subscription is also possible, if the IPEI is not configured. But because of the loss of further security by IPEI check, this kind of subscription is only allowed within a short default time interval of 2 minutes.

To enable subscriptions, press the **Start** button of the section **Wildcard subscription** on the **Portable parts** page. If necessary, increase the time interval (or refresh subscription permission in time).

The OMM will allow a wildcard subscription during the set time interval. In case of timeout the permission is lost. Only subscription with IPEI remains allowed within the fixed limit of one hour (see chapter before).


To achieve a selection of data during subscription (e.g. the user name being assigned to the PP), the field "additional ID" can be set in OMM data. If the OMM receives a valid "additional ID" during subscription, the referring data are assigned to the PP.

If the additional ID is requested for a data record, the PP user has to type it. "Additional ID" can be set within the authentication code menu. Please type the R-Key and type the additional ID.

**Please note:** The input of the additional ID is only possible with Aastra DECT 142 / Aastra 142d and 6xxd. There is no possibility to type that value on third party GAP phones. If GAP phones are going to subscribe wildcard, the first free PP data record without any additional ID will be selected and assigned.

### 7.7.4 Deleting PPs

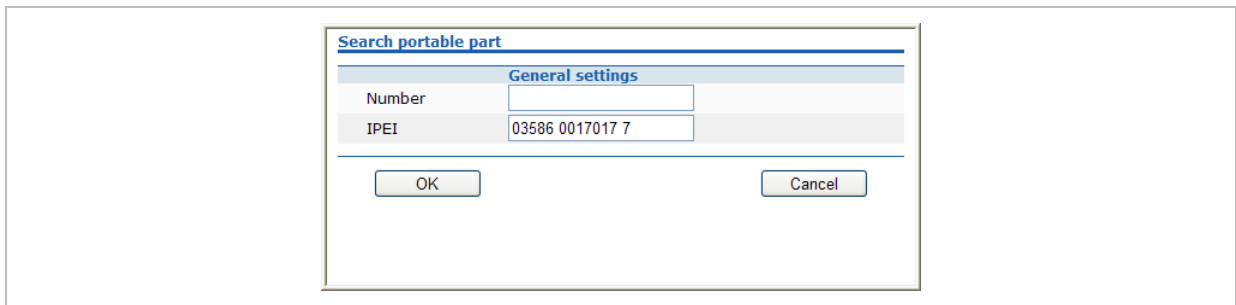
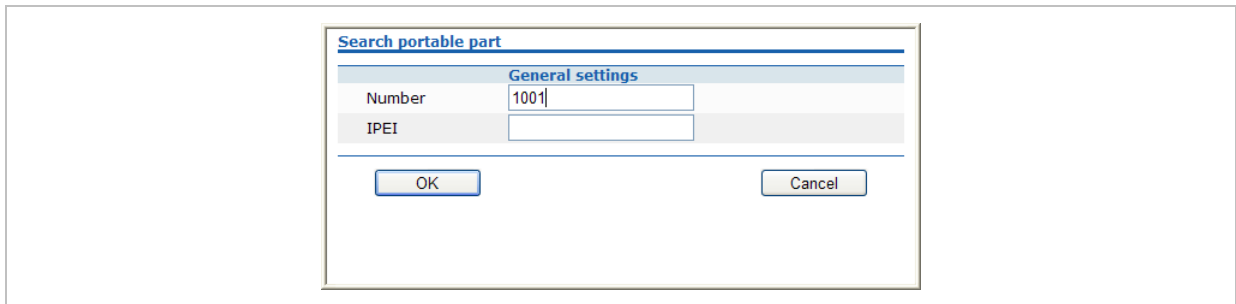
To delete an existing RFP:

- 1 On the **Portable parts** page click on the  icon left behind the PP entry.  
The **Delete portable part?** dialog opens showing the current configuration of this PP.
- 2 Press the **Delete** button.

### 7.7.5 Searching within the PP List

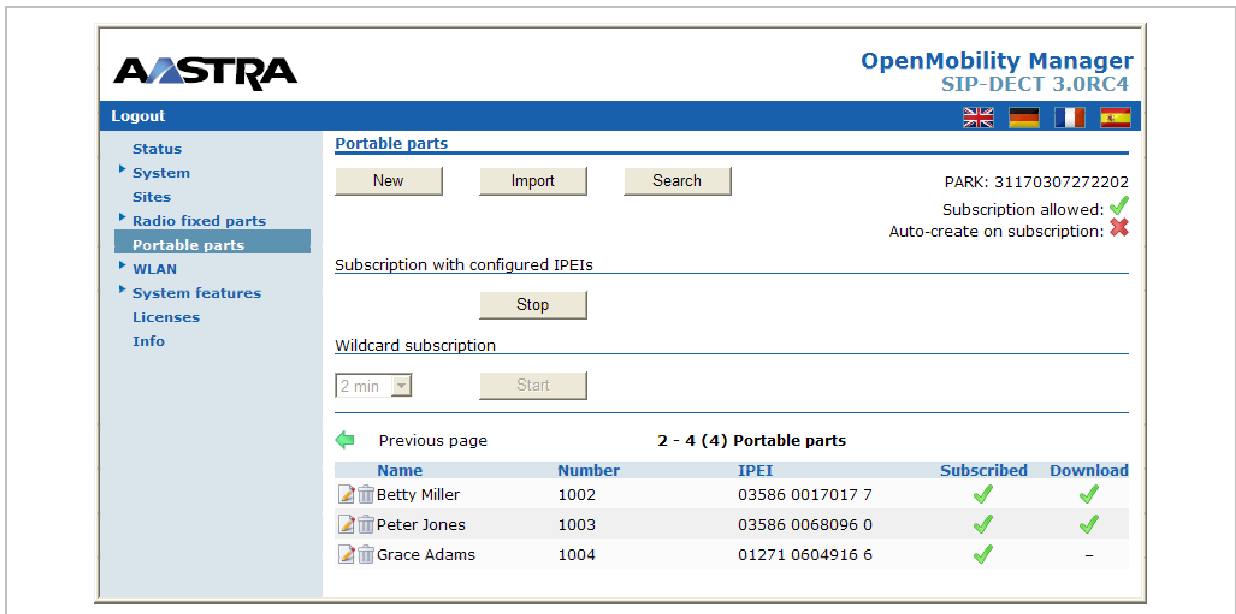
To search for a certain handset in the PP list, the search function can be used which allows to find a handset by a given number or IPEI.

- 1 On the **Portable parts** page click on the **Search** button.  
The **Search portable parts** dialog opens.



- 2 Enter the handset’s number or IPEI. At least one parameter has to be set. The entered number or IPEI has to match exactly with a handset’s number or IPEI. If number **and** IPEI are given then a handset has to exist in the OMM’s database whose number and IPEI match both otherwise the search fails.

If a handset with the specified number and/or IPEI was found, a list is displayed which has this handset as the first entry. The search function can also be used to get to the right sub list in one step.



## 7.8 “WLAN” Menu

The **WLAN** menu allows you to manage the wireless LAN function of all WLAN capable RFPs that are connected to the OMM. You can view and change wireless parameters and security settings to adapt the WLAN configuration to suit your needs. You can also check how many and which wireless clients are currently connected. Nevertheless, the WLAN function is only available for devices of the type RFP L42 WLAN and RFP L43 WLAN. Note also, that you cannot activate the WLAN function for the OMM, even if the OMM device is an RFP L42 WLAN or RFP L43 WLAN.

For a detailed description on WLAN configuration please refer to the section 9.15.

### 7.8.1 “WLAN profiles” Menu

WLAN settings are grouped in WLAN profiles. You need at least one WLAN profile that can be assigned to one or more WLAN-RFPs. Of course, you can define more than one WLAN profile. You can manage / change the desired WLAN settings for a group of WLAN-RFPs by changing their assigned WLAN profiles. Moreover, you can manage different settings, for example separate WLAN profiles for different buildings, a special WLAN profile for temporary use, or WLAN profile for RFPs only useable by guests.

Please take attention to the different WLAN profile types:

RFP type	WLAN profile type
RFP 42 WLAN / RFP L42 WLAN	RFP42
RFP 43 WLAN / RFP L43 WLAN	RFP43

The screenshot shows the 'WLAN profiles' configuration page in the OpenMobility Manager (SIP-DECT 3.0RC4) web interface. The page includes a navigation menu on the left with options like Status, System, Sites, Radio fixed parts, Portable parts, WLAN, WLAN profiles (selected), WLAN clients, System features, Licenses, and Info. The main content area displays two sections for WLAN profiles:

- Type RFP43: 1 WLAN profile**

Profile ID	SSID	SSID2	SSID3	SSID4	Security	Radio fixed parts
1	aastraguest	aastradtw	ptamobile	-	WPA	2
- Type RFP42: 1 WLAN profile**

Profile ID	SSID	SSID2	SSID3	SSID4	Security	Radio fixed parts
2	aastradtw	aastradtw	ptamobile	-	WPA Radius	4


The **WLAN profiles** menu allows to configure and administrate these WLAN profiles. The following tasks can be performed:

- Creating and changing WLAN profiles (see chapter 7.8.1.1),
- Deleting WLAN profiles (see chapter 7.8.1.2),
- Exporting WLAN profiles (see chapter 7.8.1.3).


The defined WLAN profiles are then assigned to one or more WLAN RFPs (see chapter 7.8.2). Note, that some device-specific WLAN settings are not part of a WLAN profile, such as the channel and the antenna configuration. These settings are defined separately for each RFP (see chapter 7.6.3).

### 7.8.1.1 Creating and Changing WLAN Profiles


You need at least one active WLAN profile in order to operate the WLAN function for an RFP (L)42 WLAN or RFP (L)43 WLAN device.

- 1 Navigate to the **WLAN profiles** page. This page shows the number of existing WLAN profiles and a list of available WLAN profiles.
- 2 If you create a new WLAN profile, configure the RFP type first to get the correct input fields. Select the appropriate profile (**RFP42** or **RFP43**) from the **WLAN profile type** selection list.
- 3 To add a new WLAN profile, press the **New** button. To change an existing WLAN profile, click on the  icon available on the left of the WLAN profile entry.

The **New WLAN profile** page resp. the **WLAN profile [Number]** page shows the WLAN profile configuration.



**OpenMobility Manager**  
SIP-DECT 3.0RC4



Logout

New WLAN profile

WLAN profile type: RFP42

SSID1	SSID2	SSID3	SSID4	MAC access filters
<b>General settings</b>				
<input checked="" type="checkbox"/> Profile active				
SSID				
<input type="checkbox"/> VLAN tag	[1 .. 4094]			
Beacon period	100	msec [50 .. 65535]		
DTIM period	5	Beacon(s) [1 .. 255]		
RTS threshold	2346	Byte(s) [0 .. 4096]		
Fragmentation threshold	2346	Byte(s) [0 .. 4096]		
Maximum rate	54	Mbps		
802.11 mode	Mixed			
Hidden SSID mode	<input type="checkbox"/>			
Interference avoidance	<input type="checkbox"/>			
<b>Security settings</b>				
<input type="radio"/> Open system				
<input type="radio"/> Wired equivalent privacy (WEP)				
Privacy <input type="checkbox"/>				
Number of tx keys	1	as	Text	
Default tx key	1			
Key #1				Generate
Key #2				Generate
Key #3				Generate
Key #4				Generate
<input checked="" type="radio"/> WiFi protected access (WPA)				
Type	WPA any			
<input checked="" type="radio"/> 802.1x (Radius)				
Pre-shared key <input type="radio"/>				
Value				Generate
<input type="radio"/> 802.1x (Radius)				
<input type="checkbox"/> BSS isolation				
<b>Key settings</b>				
Cipher length	64 Bits			
Distribution interval	120	sec [1 .. 65535]		
<b>Radius settings</b>				
IP address	0.0.0.0			
Port	0	Default		
Secret				
<b>QoS settings</b>				
<input type="checkbox"/> WME	VLAN			

RFP 42 WLAN profile configuration



**AASTR** OpenMobility Manager SIP-DECT 3.0RC4

Logout

System  
Sites  
Radio fixed parts  
Portable parts  
WLAN  
WLAN profiles  
WLAN clients  
System features  
Licenses  
Info

**New WLAN profile**

OK Cancel WLAN profile type: RFP43

SSID1	SSID2	SSID3	SSID4	MAC access filters
-------	-------	-------	-------	--------------------

**General settings**

Profile active

VLAN tag [1 .. 4094]

Beacon period 100 msec [40 .. 65535]

DTIM period 5 Beacon(s) [1 .. 255]

RTS threshold 2347 Byte(s) [0 .. 2347]

Fragmentation threshold 2346 Byte(s) [256 .. 2346]

802.11 mode 802.11bg

Hidden SSID mode

**Security settings**

Open system

Wired equivalent privacy (WEP)

Privacy

Number of tx keys 1 as Text

Default tx key 1

Key #1 Generate

Key #2 Generate

Key #3 Generate

Key #4 Generate

WiFi protected access (WPA)

Type WPA any

802.1x (Radius)

Pre-shared key

Value as Text Generate

MAC access filter

BSS isolation

**Key settings**

Cipher length 64 Bits

Distribution interval 600 sec [60 .. 86400]

**Radius settings**

IP address 0.0.0.0

Port 0 Default

Secret

**QoS settings**

WME

RFP 43 WLAN profile configuration

- 4 Change the desired settings of the WLAN profile. You need at least to define the ESSID setting. The different settings are explained in detail in the sections below.
- 5 Activate the **Profile active** setting, otherwise the WLAN profile is inactive which deactivates the WLAN function for RFPs that are assigned to this WLAN profile.
- 6 Press the **OK** button to apply the settings. If you created a new WLAN profile, you can proceed by assigning the WLAN profile to the desired RFPs (see chapter 7.6.3). If you changed an existing WLAN profile, the settings are applied to the assigned RFPs automatically.

The following description details the different parameters that are available on the **New WLAN profile** page resp. on the **WLAN profile [Number]** page.

### General settings

- **Profile active**: Activate this checkbox to activate the profile. This in turn activates the WLAN function for all RFPs that are assigned to the WLAN profile.
- **SSID**: Enter a descriptive character string to identify the WLAN network (e.g. "OurCompany"). The service set identifier is broadcasted by the RFP within "WLAN beacons" in a regularly interval. The SSID identifies the WLAN network and is visible by all WLAN clients. This is typically used with a scan function, e.g. from a WLAN client that tries to establish a connection. The SSID should not exceed 32 characters and it is advisable not to use unusual characters that may trigger WLAN client software bugs.
- **VLAN tag** (number, 1..4094, default: off): You can separate VoIP and client data traffic (transferred via WLAN) by using different virtual LANs, e.g. to prevent bulk data transfers to interfere with VoIP. To use a separate VLAN for the client data traffic, activate the check box and enter the desired VLAN number (see chapters 9.15 and 9.10).
- **Beacon period** (milliseconds, 50..65535, default: 100 ms): Determines the WLAN beacon interval. A higher value can save some WLAN airtime that can be used for data transfers.
- **DTIM period** (number, 1..255, default: 5): Determines the number of beacons between DTIM messages. These messages manage the WLAN wakeup/sleep function e.g. that is critical for battery powered WLAN clients.
- **RTS threshold** (bytes, 0..4096, default: 2346): If a WLAN packet exceeds this threshold, it will be transferred with RTS/CTS handshake. This may improve transfer reliability if several WLANs share the same channel. The default of 2346 byte switches off this function because the IP-MTU is typically only 1500 byte.
- **Fragmentation threshold** (bytes, 0..4096, default: 2346): If a WLAN packet exceeds this threshold, it will be transferred in chunks. This may improve transfer reliability for a weak connection. The default of 2346 bytes switches off this function because the IP-MTU is typically only 1500 byte.
- **Maximum rate** (list of rates in Mbps, 1..54, default: 54): Determines the maximum transfer rate used by the RFP. You can limit the rate to increase the WLAN range, e.g. to prevent WLAN clients in the vicinity of the RFP to disturb distant WLAN clients.
- **802.11 mode** (RFP 42 (L) WLAN selection list: Mixed / 802.11b-only / 802.11g-only, default: Mixed): Both the older and long-ranged B-Mode and the newer and faster G-Mode are typically supported by WLAN clients. You can change this setting to prevent problems with very old WLAN clients.  
(RFP 43 (L) WLAN selection list: 802.11bg /802.11b-only / 802.11g-only / 802.11abg /802.11n, default: 802.11bg): On the new RFP43 profiles you can choose additional 802.11 modes 802.11abg and 802.11n.

Mode	802.11abg	802.11n
Open	yes	yes
WEP	yes	no
Radius (802.1x WEP)	yes	no
WPA v.1 (802.1x + PSK)	yes	no
WPA v.2 (802.1x + PSK)	yes	yes

- **Hidden SSID mode** (on / off, default: off): If switched on, the transmission of the SSID within beacons is suppressed. This in turn requires a more elaborate and manual connection procedure for WLAN clients.

- **Interference avoidance** (on / off, default: off): Enables a WLAN procedure to enhance radio interference avoidance. This setting applies to RFP (L)42 WLAN only.

### Security settings

These settings determine the encryption used for the WLAN connection. Select one of the four modes (Open, WEP, WPA, or Radius). This will activate / gray-out the necessary additional input fields that specify further security settings on the **WLAN profile** page.

- **Open system**: Enable this option to deactivate authentication and encryption (“Hotel mode”). Note, that all data is transferred un-encrypted in this mode, which can be easily eavesdropped with any WLAN equipment.
- **Wired equivalent privacy (WEP)**: Enable this option to use the older WEP encryption mode. This mode may be useful, e.g. if your WLAN should support older WLAN clients that do not implement the recommended WPA encryption.
  - **Privacy** (on / off, default: off): De-activate this setting to use no authentication (“Open System”) with standard WEP encryption. Activate this setting to use an additional shared key authentication between the RFP and the WLAN client.
  - **Number of tx keys** (number, 1..4, default: 1): The WEP encryption can use a single shared key or multiple shared keys (“key rotation”). Select the number of shared keys, select how to enter a shared key (by default as **Text** or as **Hex value**), and select the **Cipher length** (see **Key settings** below).
  - **Default tx key** (number, 1..4, default: 1): If more than one shared keys is used, you can select the default shared key. You need to configure the same default key on the WLAN client.
  - **Key #1 – Key #4**: Enter one or more shared key. The **Cipher length** setting (see **Key settings** below) determines the length of the required input. If you selected to enter as **Text** (see above), input a password with 5, 13, or 29 characters that matches a 64, 128, or 256 bit cipher. If you selected to enter as **Hex value**, you can input a hexadecimal number with 10, 26, or 58 characters (0-9, a-f). Press the **Generate** button to generate a random shared key that matches the current settings.
- **WiFi protected access (WPA)**: Enable this option to use the recommended WPA encryption mode.
  - **Type** (selection, WPA any / WPA v.1 / WPA v.2, default: WPA any): Select the WPA version required for WLAN clients. The **WPA any** setting allows WPA v.1 and WPA v.2 to be used concurrently. The **WPA v.1** setting enforces the use of the older RC4-based encryption. The **WPA v.2** setting enforce the use of the stronger AES encryption. You can also change the distribution interval (see **Key settings** below).
  - **802.1x (Radius)**: Select this option if your WLAN should use a RADIUS server for WLAN client authentication (“Enterprise WPA” with different username/password combinations per client). You also need to specify the **Radius settings** (see below). For details about the RADIUS authentication procedure, using the public keys, and importing certificates to the WLAN clients refer to the documentation of your RADIUS server product.
  - **Pre-shared key**: Select this option to use a single shared key for all WLAN clients (**Value** setting below). A WLAN client user needs to enter the shared key in order to connect.

- **Value:** You can enter a shared key as **Text**. Use a longer text sequence with alphanumeric characters and special characters to enhance the shared key strength. A text shared key is case sensitive. Alternatively, the shared key can be entered as **Hex value** (hexadecimal number, 0-9, a-f). Press the **Generate** button to generate a random shared key that matches the current settings.
- **802.1x (Radius):** This setting applies to RFP (L)42 WLAN only. Enable this option to use the RADIUS authentication without the stronger WPA encryption. You also need to specify the **Radius settings** and you may adapt the **Key settings** (see below).
- **MAC access filters** (on / off, default: off): This setting applies to RFP (L)43 WLAN only. You can limit WLAN access for WLAN clients with specified MAC addresses. Note, that without encryption this should not be used for security reasons. You can configure a list of MAC addresses that are allowed to connect via the **MAC access filters** tab on the WLAN profile page.
- **BSS isolation** (on / off, default: off): In a standard WLAN setup, each WLAN client can contact other WLAN clients. For special purposes (e.g. "Internet café setup"), you may switch on this options to protect WLAN clients from eavesdropping on other WLAN clients.

### Key settings

- **Cipher length** (selection, 64 Bits / 128 Bits / 256 Bits, default: 64 Bits): Determines the key length used for the WEP encryption. Larger bit sequences provide better security but may be unsupported by very old WLAN clients.
- **Distribution interval** (seconds, 1..65535, default: 20): Determines how often the WEP encryption is re-negotiated.

### Radius settings

The parameters in this section can only be configured if the **802.1x (Radius)** option has been selected.

- **IP address:** Enter the IP address of the RADIUS server.
- **Port:** Enter the port number used to connect to the RADIUS server. Press the **Default** button to change to the standard port.
- **Secret:** Enter the character string that is used by the RFP to secure the communication with the RADIUS server.

### QoS settings

- **WME with:** (on / off, VLAN or DiffServ, default: off/VLAN): You can enable the Wireless Media Extensions to prioritize WLAN traffic. The WLAN traffic priority is determined by **VLAN** number or by examining the **DiffServ** data field of IP packets.

### SSID2 – SSID4 Tabs

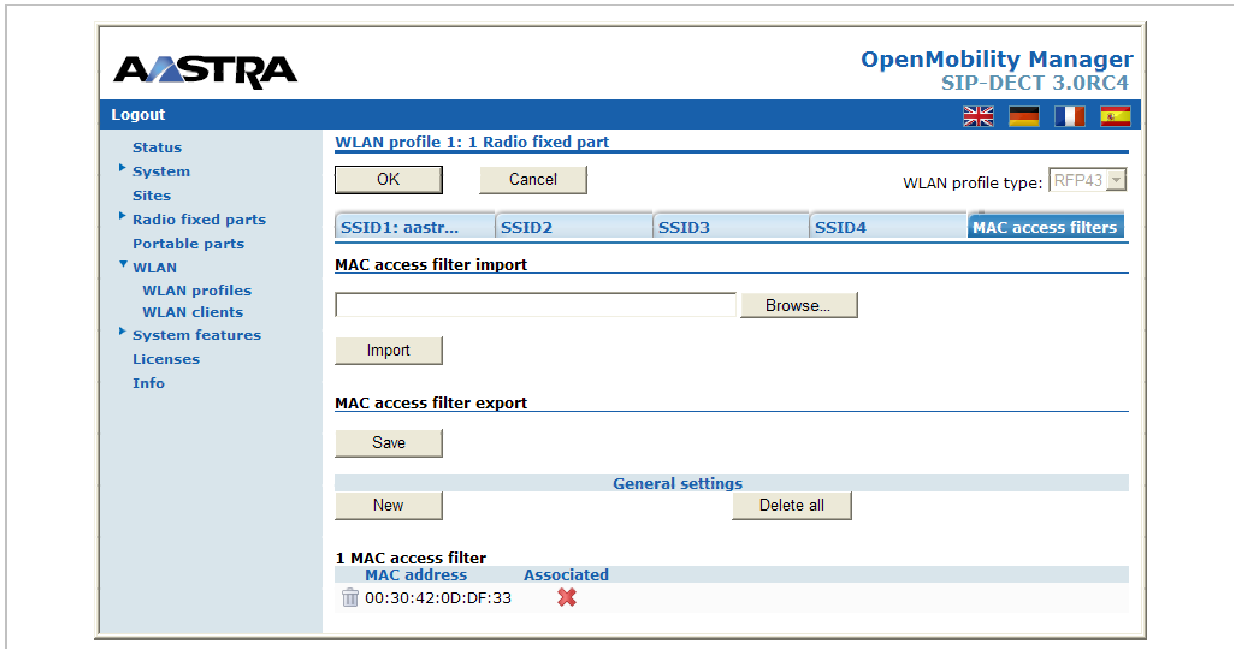
You can enable up to three additional virtual WLAN networks that are managed by their SSID. This can be used for example to provide WLAN access for guests that is separated from the company WLAN by means of VLAN tags and encryption settings. To activate this feature proceed as follows:


- 1 Switch to the appropriate **SSID** tab, e.g. SSID2. Activate the **Active** check box to enable the additional virtual WLAN. The tab provides separate configuration items for the selected SSID.
- 2 Enter at least a new **SSID**. Also enter a currently unused **VLAN tag** number.

- 3 You can specify different authentication/encryption settings for each SSID section. For example, you can use **WPA / Pre-shared key** with different passwords.

Note, that some configuration combinations are incompatible with multiple SSIDs. For example, the wireless hardware only manages a single WEP encryption key. Also, some features apply to all defined SSIDs, this includes the **MAC access filters** list.

You can edit the **MAC access filters** list via the **MAC access filters** tab on the WLAN profile page.




- You can import a prepared list of MAC addresses (\*.txt. file, one line per MAC address) Use the **Browse** button to select the file from the file system. Afterwards press the **Import** button.
- To configure single MAC addresses, use the **New** button in the **General settings** section. Enter the address in the following **New MAC access filter** dialog.
- To delete a single MAC address, click on the  icon left behind the address entry. Use the **Delete all** button to delete the entire list.
- Using the **Save** button you can export the MAC address filter list.


The **Associate** column indicates for each MAC address if the respective WLAN client is currently connected to the WLAN.

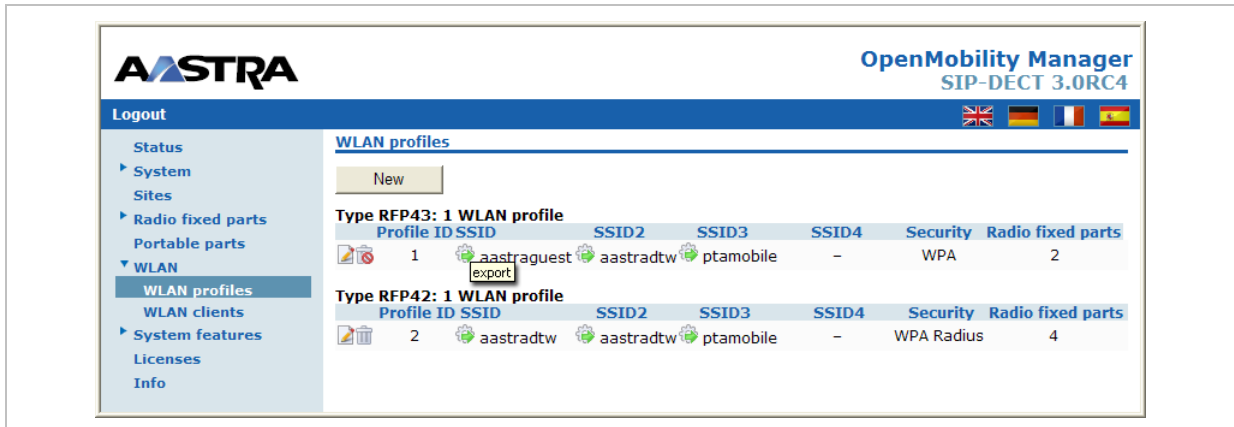
### 7.8.1.2 Deleting WLAN Profiles

To delete an existing WLAN profile:

- 1 You cannot remove WLAN profile that is in use. To remove a currently used WLAN profile, you need to select another WLAN profile for all assigned RFPs first (see chapter 7.6.3).
- 2 On the **WLAN profiles** page click on the  icon next to the profile entry. The **Delete WLAN profile?** dialog opens showing a summary of the WLAN profile's configuration.
- 3 Press the **Delete** button.

### 7.8.1.3 Exporting WLAN Profiles

To help simplify the configuration of wireless devices, you can export SSID configuration to a XML WLAN profile file. To export the configuration, please click on the  icon.



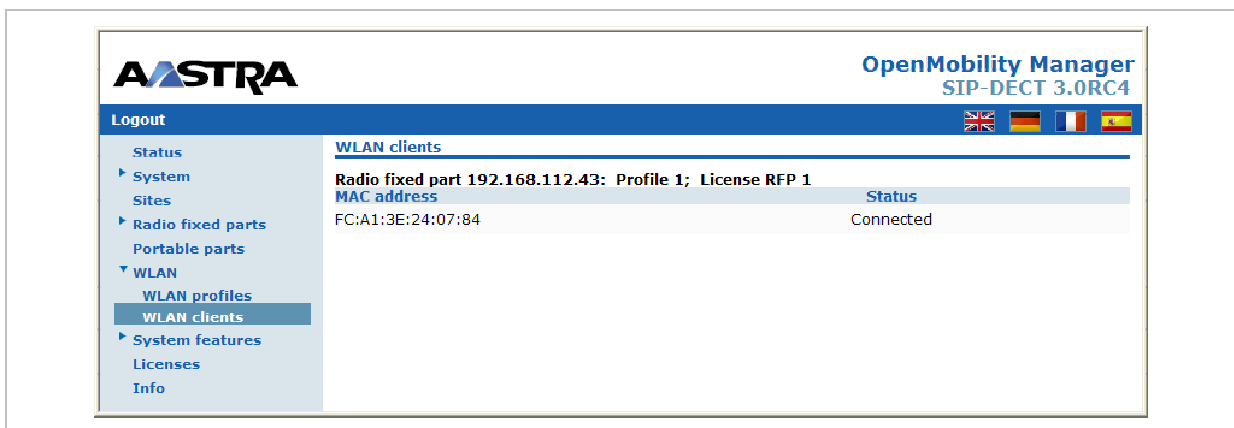
The screenshot shows the 'WLAN profiles' page in the OpenMobility Manager interface. It features a sidebar menu with options like Status, System, Sites, Radio fixed parts, Portable parts, WLAN (with sub-items WLAN profiles, WLAN clients, System features, Licenses, Info), and Logout. The main content area shows two WLAN profiles:

Type	RFP43: 1 WLAN profile	RFP42: 1 WLAN profile
Profile ID	1	2
SSID	aastraguest	aastradtw
SSID2	aastradtw	aastradtw
SSID3	ptamobile	ptamobile
SSID4	-	-
Security	WPA	WPA Radius
Radio fixed parts	2	4

On Windows 7 you can use the command “netsh wlan add profile filename=xxx” to import a WLAN configuration. Many other tools to import WLAN configuration files are available for Windows Vista / Windows XP systems (for example wlan.exe from Microsoft).

### 7.8.2 “WLAN clients” Menu

The **WLAN clients** page shows the status of all WLAN clients currently connected to the WLAN. This can be used for example for troubleshooting purposes. The display shows the total number of connected WLAN clients and a list of RFPs that are part of the WLAN. For each RFP, the WLAN client connected to the RFP are listed. You can view the **MAC address** and the current **Status** of each WLAN client.



The screenshot shows the 'WLAN clients' page in the OpenMobility Manager interface. The sidebar menu is similar to the previous screenshot, but 'WLAN clients' is selected. The main content area shows the following information:

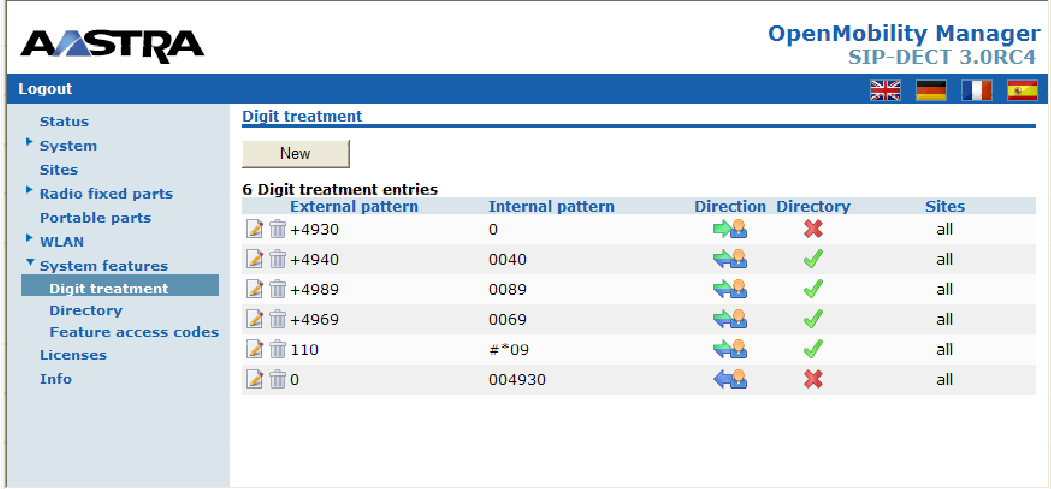
Radio fixed part	MAC address	Status
192.168.112.43: Profile 1; License RFP 1	FC:A1:3E:24:07:84	Connected

### 7.9 “System features” Menu

The **System features** menu allows administration of system features concerning call number handling and directory access.

## 7.9.1 “Digit treatment” Menu

A number manipulation is provided by the digit treatment feature for LDAP corporate directories, that handles both incoming and outgoing calls (see chapter 7.9.2).



The screenshot shows the Aastra OpenMobility Manager SIP-DECT 3.0RC4 web interface. The left sidebar contains a navigation menu with options like Status, System, Sites, Radio fixed parts, Portable parts, WLAN, System features, Digit treatment (selected), Directory, Feature access codes, Licenses, and Info. The main content area is titled 'Digit treatment' and includes a 'New' button and a table of 6 digit treatment entries.

6 Digit treatment entries					
External pattern	Internal pattern	Direction	Directory	Sites	
+4930	0	→	✗	all	
+4940	0040	←	✓	all	
+4989	0089	←	✓	all	
+4969	0069	←	✓	all	
110	#*09	←	✓	all	
0	004930	←	✗	all	

### LDAP

A chosen number from a LDAP entry is checked against the external prefix pattern and if a pattern matches it is replaced by the configured internal prefix pattern. Only the best matching rule will be applied.

Before a rule is applied the following character are automatically removed from the LDAP entry: '%', space, '(' and ')'. The result of the conversion is sent to the handset to be displayed e.g. directory entry details and entered in the redial list.

**Note:** A conversion performed for a LDAP entry can be reversed if the rule is also activated for an outgoing call.

### Incoming Call

The calling party number of an incoming call is checked against the configured external prefix pattern and if a pattern matches it will be replaced by the internal prefix pattern. Only the best matching rule will be applied.

The result of the conversion is sent to the handset to be displayed and entered in the call log<sup>1</sup>.

### Outgoing Call

A dialled number of an outgoing call is checked against the configured internal prefix pattern and if a pattern matches it will be replaced by the external prefix pattern. This applies to on-bloc dialled numbers and to overlap sending as long as the SIP session has not been initiated.

<sup>1</sup> For Incoming Call/Calling Party Number; Depending on the capabilities of the handset and the level of integration.


**Note:** To support digit treatment and overlap sending, it is necessary to have a dial terminator configured.

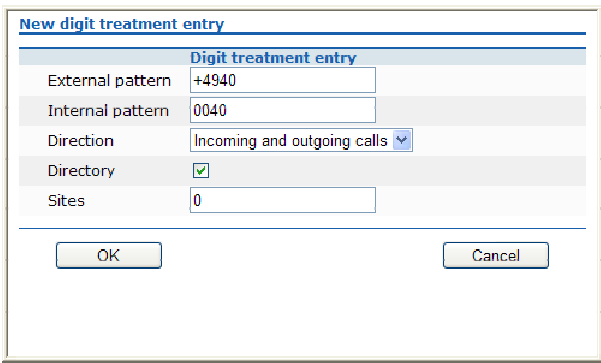
The result of the conversion is not sent to the handset to be displayed or entered in the call log<sup>1</sup>.

The following tasks can be performed on the **Digit treatment** page:

- creating and changing “Digit treatment” entries (see chapter 7.9.1.1),
- deleting “Digit treatment” entries(see chapter 7.9.1.2).

### 7.9.1.1 Creating and Changing “Digit treatment” Entries

- 1 To configure a new entry press the **New** button on the **Digit treatment** page. To change the configuration of an existing entry click on the  icon left behind the entry. The **New digit treatment entry** resp. the **Configure digit treatment entry** dialog opens.



- 2 **External pattern:** enter an external prefix pattern with up to 32 characters that matches an incoming call number or a number received via LDAP. The prefix to be substituted for calling party numbers has the same character set as the user telephone number (e.g.:”+\*~#;,;\_-!\$%&/()=?09aAZZ”).
- 3 **Internal pattern:** enter an internal prefix pattern with up to 32 character that replaces the external pattern for LDAP / incoming calls or vice versa for outgoing calls. An internal prefix pattern can be composed of:characters “\*”, “#” and “0” – “9”.

**Please note:** The plus character (“+”) can not be dialled from a handset and can not be transferred to a call log.

- 4 **Direction:** select one of the following options:
  - “Incoming calls”: Rule applies on incoming calls.
  - “Outgoing calls”: Rule applies on outgoing calls.
  - “Incoming and outgoing calls”: Rule applies on incoming and outgoing calls.
  - “Apply on directory only”: Rule applies on LDAP only.
- 5 **Directory:** Activate this option if the rule applies to LDAP directories (see chapter 7.9.2).


<sup>1</sup> For Outgoing Call/Called Number; If the user would dial the number from the redial list again the same procedure will be applied as for the initial dialling.



- 6 **Sites:** Specifies the sites for which a rule shall be applied e.g. "1,2" (see chapter 7.5). If set to "0" the rule applies to all sites i.e. the rule will be applied to all calls or corporate directory requests.
- 7 Press the **OK** button.

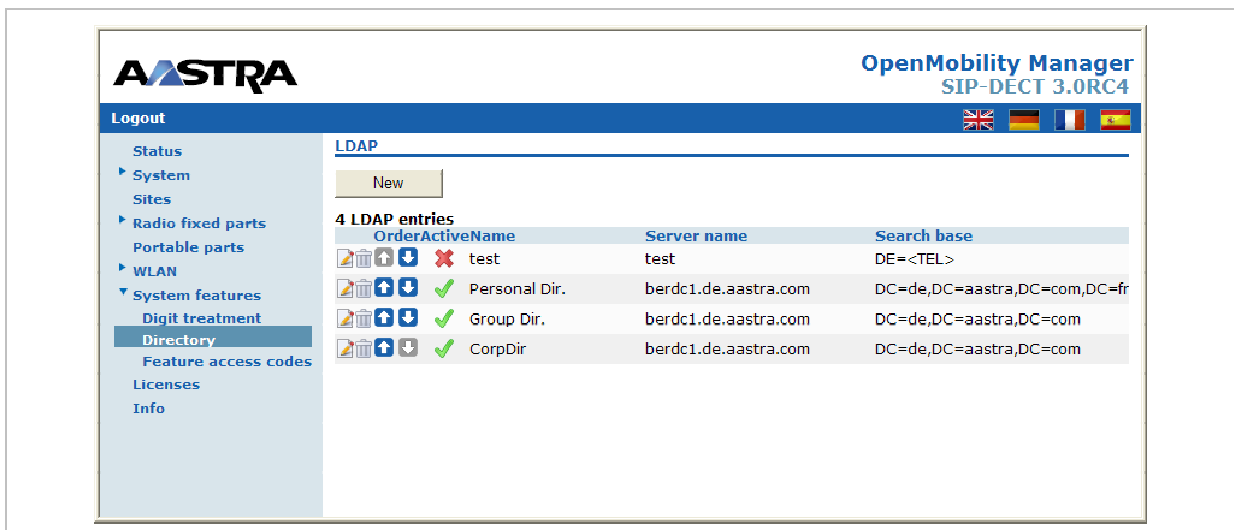
### 7.9.1.2 Deleting "Digit treatment" Entries

To delete an existing entry:

- 1 On the **Digit treatment** page click on the  icon left behind the entry.  
The **Delete digit treatment entry?** dialog opens showing the current configuration of this entry.
- 2 Press the **Delete** button.

### 7.9.2 "Directory" Menu

The **System features** menu allows you to manage connections to one or more LDAP servers that in turn facilitate central corporate directories. The OMM supports multiple LDAP servers with specific parameter settings to support different types of directories e.g. global corporate directory, group specific directory, personal directory.



If there is more than one LDAP server configured then the multiple options are offered to the user as a list. The list is presented to the user if the central directory is called e.g. via soft key or selecting central directory from the menu. The user can choose one of the entries in the list. The name of an entry shown in the list is configured in the OMM when creating the LDAP server entry. (Latin-1 character set is supported).

- If there is only one LDAP server configured then the directory function is directly started when pressing the soft key or selecting central directory from the menu.
- The name configured in the OMM is not relevant and ignored if there is only one LDAP server configured.
- There are up to 5 LDAP directories configurable.

The OMM determines the display order of the directories in the handset menu by the order specified by the administrator.