

SIP-DECT OM System Manual

ADMINISTRATION GUIDE

Release 8.0



NOTICE

The information contained in this document is believed to be accurate in all respects but is not warranted by Mitel Networks™ Corporation (MITEL®). The information is subject to change without notice and should not be construed in any way as a commitment by Mitel or any of its affiliates or subsidiaries. Mitel and its affiliates and subsidiaries assume no responsibility for any errors or omissions in this document. Revisions of this document or new editions of it may be issued to incorporate such changes.

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

TRADEMARKS

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

Mitel's Power Over Ethernet (PoE) Powered Device (PD) products are covered by one or more of the U.S. patents (and any foreign patent counterparts thereto) identified at Mitel's website: www.mitel.com/patents.

For more information on the PD patents that are licensed, please refer to www.cmspatents.com.

SIP-DECT OM System Manual
Administration Guide
Release 8.0 - September 2018

®,™ Trademark of Mitel Networks Corporation
© Copyright 2018 Mitel Networks Corporation
All rights reserved

CONTENTS

1	Overview	10
1.1	The SIP-DECT Solution	10
1.2	About DECT Base Stations	11
1.2.1	DECT Base Station Families	11
1.2.2	OpenMobility Manager (OMM) Mode	16
1.3	About the OpenMobility Manager	16
1.3.1	OMM Tasks	16
1.3.2	SIP-DECT Special Features and Capabilities	17
1.3.3	OMM Capacities and Features	18
1.3.4	OMM Capacities and RFP Support	18
1.4	About DECT Phones	19
1.5	File naming conventions	19
1.6	Login and passwords	20
2	Enhanced Feature Overview	21
2.1	PC-based OMM installation	21
2.2	DECT XQ	21
2.3	Wideband (CAT-iq 1.0 / Mitel Hi-Q™ audio technology)	22
2.4	DECT enhanced security	22
2.5	VoIP encryption	23
2.6	Mixed DECT base station installations	23
2.7	Wireless LAN (WLAN)	23
2.7.1	802.11i: WPA2-Enterprise Pre-Authentication for fast Roaming	23
2.7.2	Channel Configuration Feedback for HT40 and tx Power	24
2.7.3	Channel Configuration Feedback for HT80	24
2.8	DECT base station synchronization	24
2.8.1	Clustering and paging areas	24
2.9	DECT base station Reset to Factory Settings	25
2.9.1	RFP4G reset to factory defaults	25
2.10	System redundancy	26
2.10.1	OMM standby	26
2.10.2	Backup SIP proxy/registrar	26
2.10.3	Configurable User Account for Standby Check	26
2.10.4	User data synchronization (MiVoice 5000 dual homing support)	26
2.10.5	Multi-OMM Manager for OMM-centralized management	27
2.11	Simplified licensing	27
2.12	Extended regulatory domain support	27
2.13	DECT phone functionality	28
2.13.1	DECT Phone Download over Air	28
2.13.2	Central DECT Phone Configuration Over Air (CoA)	29
2.13.3	OMM DECT phone provisioning	30
2.13.4	Mitel 600 DECT Phone Dial Editor Mode	30
2.13.5	Mitel 602 DECT Phone Customizable Boot Texts	30
2.13.6	OMM-Centralized call logs	30
2.13.7	User individual DECT Phone PIN Key Lock	30
2.14	Hot Desking	31
2.15	Conferencing	31
2.15.1	Conferencing audio notification	32
2.15.2	Centralized conferencing with MiVoice Business	32
2.15.3	N-WAY CONFERENCING	32
2.16	SIP over UDP/TCP/TLS	33
2.17	SIP multiport	33
2.18	UTF-8 encoding	34
2.19	Alphanumeric dialing	34
2.20	Voice mail number	35
2.21	Call handling	35
2.21.1	Diversion indication	35
2.21.2	Call completed elsewhere	36

2.21.3	Semi-Attended Transfer	36
2.21.4	Third Line Handling for Mitel 142d and 600 DECT Phones	36
2.21.5	Call Transfer Enhancements for Mitel 142d DECT phones	37
2.22	Truncating SIP User Name in SIP URI	38
2.23	OM Locating application	38
2.24	Extended messaging	38
2.25	Video support	38
2.25.1	USB Video Devices	39
2.25.2	Terminal Video	39
2.26	User monitoring	40
2.27	Corporate directory integration	41
2.28	Integration into external management systems	41
2.29	System configuration tools	41
2.30	SIP enhancements	42
2.30.1	Globally Routable User-Agent URIs (GRUUs)	42
2.30.2	Session timer	42
2.30.3	SIP Contact matching	42
2.30.4	Configurable Call reject state codes	43
2.30.5	Call release timers	43
2.30.6	Incoming call timeout	43
2.30.7	Call reject on silent charging	43
2.30.8	route header	43
2.30.9	MWI SUBSCRIPTION period	43
2.31	Auto answer, intercom calls and audio settings	44
2.31.1	Intercom Calls	44
2.31.2	Auto answer audio settings	45
2.32	SIP-DECT XML terminal interface	45
2.32.1	Feature Access Codes Translation	45
2.32.2	Ring Tone Selection for (Alarm) Messages	46
2.33	Software Update Dispersion	46
3	Licensing	47
3.1	Licensing Model	47
3.1.1	System Licenses	47
3.1.2	About G.729 Channels	48
3.1.3	PARK Service	48
3.1.4	Upgrade License	49
3.1.5	Grace Period	49
3.1.6	License Violations and Restrictions	50
3.2	Uploading a License File	50
3.3	License Models	51
3.3.1	Small System (Unlicensed)	51
3.3.2	Medium or Large System	51
4	Getting Started	53
4.1	Base Station Startup Configuration	53
4.2	System Configuration	53
4.3	System Settings	54
4.4	Base Stations	54
4.5	SIP settings	55
4.6	DECT Phones	56
4.6.1	DECT Phone and SIP state verification	57
5	OMM Web Service	59
5.1	Login	59
5.2	Logout	60
5.3	"Status" Menu	60
5.4	"System" Menu	61
5.4.1	"System Settings" Menu	61
5.4.2	"Provisioning" Menu	68
5.4.3	"SIP" Menu	71

5.4.4	“User administration” Menu	79
5.4.5	“Time zones” Menu	81
5.4.6	“SNMP” Menu	82
5.4.7	“DB management” Menu	83
5.4.8	“Event log” Menu	85
5.5	“Sites” Menu	86
5.5.1	Creating a New Site	86
5.5.2	Editing a Site	87
5.5.3	Deleting a Site	87
5.6	“Base Stations” Menu	87
5.6.1	Base Station States	89
5.6.2	OMM / RFP Software Version Check	90
5.6.3	Creating and Changing Base Stations	90
5.6.4	Capturing DECT Base Stations	92
5.6.5	Deleting DECT Base Stations	92
5.6.6	Find my SIP-DECT Base Station	92
5.7	“DECT Phones” Menu	94
5.7.1	Creating and Changing DECT Phones	95
5.7.2	Importing DECT phone Configuration Files	96
5.7.3	Subscribing DECT Phones	97
5.7.4	Deleting DECT phones	98
5.7.5	Searching the DECT phone List	99
5.7.6	Displaying User and DECT Phone Data	99
5.8	“WLAN” Menu	103
5.8.1	“WLAN profiles” Menu	103
5.8.2	“WLAN clients” Menu	108
5.9	“System features” Menu	108
5.9.1	“Digit treatment” Menu	109
5.9.2	“Directory” Menu	110
5.9.3	“Directory (comp. mode)” menu	112
5.9.4	“Feature Access Codes” Menu	113
5.9.5	“XML Applications” Menu	115
5.10	“Licenses” Menu	117
5.11	“Info” Menu	117
6	OM Management Portal (OMP).....	118
6.1	Login	118
6.2	Logout	119
6.3	OMP Main Window	119
6.4	“Status” Menu	120
6.4.1	Overview	121
6.4.2	DECT base stations	122
6.4.3	Users	123
6.4.4	Devices	124
6.4.5	Sites	125
6.4.6	Conference	126
6.4.7	Video Devices	126
6.5	“System” Menu	127
6.5.1	“Basic settings” Menu	127
6.5.2	“Advanced settings” Menu	130
6.5.3	“Statistics” Menu (Monitoring Mode Only)	138
6.5.4	“SIP” Menu	139
6.5.5	“Provisioning” Menu	143
6.5.6	“User administration” Menu	145
6.5.7	“Data management” Menu	149
6.5.8	“Event Log” Menu	151
6.6	“Sites” Menu	153
6.7	“DECT Base Stations” Menu	154
6.7.1	“Device list” Menu	154
6.7.2	“Paging areas” Menu	160
6.7.3	“Capturing” Menu	161

6.7.4	“Enrolment” Menu	162
6.7.5	“Export” Menu	162
6.7.6	“Sync view” Menu	163
6.7.7	“Statistics” Menu	164
6.7.8	“Quality” Menu	166
6.8	“WLAN” Menu	168
6.8.1	Profiles	168
6.9	“Video devices” Menu	172
6.9.1	Changing Video Devices	172
6.9.2	Viewing Video Device Details	173
6.9.3	Deleting Video Devices	173
6.9.4	Filtering Video Device Table	173
6.10	“DECT Phones” Menu	173
6.10.1	“Overview” Menu	174
6.10.2	“Users” Menu	176
6.10.3	“Devices” Menu	176
6.10.4	Device Detail Panel	177
6.10.5	Creating DECT phone Datasets	184
6.10.6	Configuring DECT phone Datasets	185
6.10.7	Subscribing DECT phone Datasets	185
6.10.8	Deleting DECT phone Datasets	185
6.10.9	Selecting Columns	186
6.10.10	Filtering DECT phone Table	186
6.10.11	Changing the Relation Type	186
6.10.12	Enabling / Disabling DECT phone Event Log	187
6.10.13	User Monitoring	187
6.11	“Conference rooms” Menu	188
6.11.1	Creating Conference Rooms	188
6.11.2	Configuring Conference Rooms	189
6.11.3	Deleting Conference Rooms	189
6.11.4	Viewing Conference Room Details	190
6.12	“ALARM TRIGGERS” MENU “System features” Menu	190
6.12.1	“General settings” Menu	190
6.12.2	“Feature access codes” Menu	191
6.12.3	“Alarm triggers” Menu	191
6.12.4	“Digit treatment” Menu	193
6.12.5	“Directory” Menu	194
6.12.6	Easy migration from corporate Directory (comp. mode) to new corporate Directory structure	196
6.12.7	“Directory (comp. mode)” Menu	197
6.12.8	“XML applications” Menu	199
6.12.9	“CoA Profiles” Menu	203
6.13	“Licenses” Menu	204
6.14	“General” Menu	205
6.15	“Help” Menu	206
7	DECT Phone	208
7.1	Key lock with PIN	208
7.1.1	Maintain the PIN	208
7.1.2	Unlock a locked Mitel 600 DECT phone	208
7.1.3	Setup automatic key lock with PIN	210
8	Configuration and Administration	211
8.1	IP Signaling and Media Stream	211
8.2	DECT Base Station Synchronization	213
8.2.1	Initial Synchronization Procedure	214
8.2.2	Checking the Synchronization of a Network	215
8.3	DECT Base Station Channel Capacity	215
8.4	Network Infrastructure Prerequisites	216
8.5	SIP-DECT Startup	216
8.5.1	TFTP and DHCP Server Requirements	217
8.5.2	Bootting Steps	217

8.5.3	Booter Startup	218
8.5.4	Application Startup	220
8.5.5	RFP LEDs	224
8.6	State Graph of the Start-up Phases	228
8.7	Local DECT Base Station Configuration (OM Configurator)	231
8.7.1	Selecting the Network Interface	232
8.7.2	Adding DECT Base Stations for configuration	232
8.7.3	Scanning for DECT Base Stations	232
8.7.4	Adding DECT Base Stations manually	233
8.7.5	Loading DECT Base Station data from File	233
8.7.6	Editing DECT Base Station configuration data	233
8.7.7	Applying Configuration Changes	236
8.7.8	Factory Reset	236
8.7.9	Saving and Loading a DECT Base Station List	236
8.7.10	Removing DECT Base Station Entries	237
8.7.11	Compatibility with Older SIP-DECT Releases	237
8.8	OMM Configuration and Resource Files	237
8.8.1	Configuration File URL	238
8.8.2	Specific Configuration URLs	240
8.8.3	ReLoad of Configuration and Resource files	240
8.8.4	AXI Commands in Configuration Files	241
8.8.5	User Configuration Files	243
8.8.6	Digest Authentication and Certificate Validation	245
8.8.7	DECT base station software Image from RFP OMM	246
8.8.8	Redirection and Configuration Service (RCS)	246
8.8.9	Customer Logo on OMM Web Service	247
8.9	DECT Base Station Configuration Files	247
8.9.2	Standard IP settings	248
8.9.3	Configuration file source	248
8.9.4	Parameter settings priority	249
8.9.5	Software update settings for 3 rd generation DECT base stations	249
8.9.6	SOFTWARE UPDATE SETTINGS FOR 4 th GENERATION DECT BASE STATIONS	249
8.9.7	Times when RFP configuration times are read	249
8.9.8	RFP configuration file update check	250
8.9.9	Handling of parameter changes	251
8.9.10	Configuration file syntax	251
8.10	Consolidated Certificate management	253
8.10.1	SIP over TLS certificates	253
8.10.2	OMM Certificate (Web service / AXI)	253
8.10.3	Provisioning certificates	253
8.10.4	Certificate validation	254
8.11	3 rd and 4 th Generation RFP Software Update	254
8.12	802.1Q Support	254
8.12.1	Boot Phase of IP RFPs (DHCP)	255
8.12.2	Boot Phase of IP RFPs (Local Configuration)	256
8.13	Installing OMM in Host Mode	256
8.13.1	System Requirements	256
8.13.2	Installing the OMM Software	256
8.13.3	Configuring the Start Parameters	257
8.13.4	Specific Commands – Troubleshooting	258
8.14	Updating the OMM	258
8.14.1	Updating a Single OMM Installation	259
8.14.2	Updating a Standby OMM Installation	259
8.15	OMM Standby	261
8.15.1	Configuring OMM Standby	261
8.15.2	Fail Over Situations	261
8.15.3	Failover Failure Situations	262
8.15.4	Specific standby situations	263
8.16	User data synchronization (MiVoice 5000 dual homing support)	264
8.16.1	Roaming	265
8.16.2	Setting up user data synchronization	266

8.16.3	User data synchronization modes	267
8.17	Managing Account Data for System Access	269
8.17.1	Account Types	269
8.17.2	Potential Pitfalls	270
8.18	WLAN Configuration	270
8.18.1	WLAN configuration steps (RFP 42 WLAN / RFP 43 WLAN only)	270
8.18.2	WLAN configuration steps (RFP 48 WLAN)	271
8.18.3	Optimizing the WLAN	273
8.18.4	Securing the WLAN	275
8.19	SNMP Configuration	275
8.20	Backup SIP Proxy/Registrar	276
8.20.1	REGISTER Redirect	276
8.20.2	DNS SRV	277
8.20.3	Backup SIP Servers	278
8.20.4	Keep Alive Mechanism	280
8.20.5	Prioritized Registration	280
8.20.6	Monitoring the SIP Registration Status	281
8.20.7	Configurable User Account for Standby Check	281
8.20.8	OMM Standby Enhancement	281
8.21	Conferencing	282
8.21.1	Centralized Conferencing	283
8.21.2	Integrated Conference Server (ICS)	283
8.21.3	Configure conference rooms	285
8.22	Download Over Air	288
8.22.1	How "Download Over Air" Works	288
8.22.2	How to configure "Download Over Air"	289
8.23	Central DECT Phone Configuration Over Air (CoA)	291
8.23.1	Configuration files	291
8.23.2	Configuration file download to DECT phones	292
8.23.3	CoA Configuration using OMP	293
8.23.4	Configuration using usr_common.cfg/<user>/cfg Files	293
8.23.5	Variable lists	294
8.24	Extended DECT Phone Interface	299
8.25	OMM/DECT Phone Lock with Branding ID	301
8.25.1	Subscribing the DECT Phone	301
8.26	Device Placement	301
8.26.1	"Placement" View	301
8.26.2	"DECT Base Stations" View	302
8.26.3	"Image management" View	303
8.27	Monitoring with USB Video Devices	305
8.27.1	Configuration of a video user account	305
8.27.2	Configuration of USB video devices	306
8.27.3	Monitoring with USB video devices	306
8.28	Terminal Video	306
8.28.1	Technical Details	307
8.28.2	OMP Configuration Steps	307
8.28.3	Camera Selection via DECT phone Menu	307
8.29	User Monitoring	307
8.29.1	Overview	308
8.29.2	Status Attributes and Validation Mechanisms	309
8.29.3	Escalation	312
8.29.4	Alarm Triggers	312
8.29.5	OM Locating Application	313
8.29.6	Licensing and System Capacities	313
8.29.7	Configuration	313
8.29.8	Start and Failover	315
8.29.9	Supported DECT phones	316
8.29.10	Restrictions	317
8.30	SRTP	317
8.31	SIP over TLS	318
8.31.2	Certificates	319

8.31.3	Private Key	320
8.31.4	TLS Transport Mode	320
8.31.5	Verification of Remote Certificates	321
8.31.6	Additional Security Considerations	321
8.32	DECT Enhanced Security	322
8.33	Migration of RFP SL35 IP from SIP-DECT Lite 3.1 to SIP-DECT 6.1	322
8.34	802.1x Certificate Based Authentication	323
8.34.1	802.1x Configuration	324
8.34.2	Prerequisites Referring to 802.1x Topology	325
8.34.3	802.1x Feature Description	325
8.35	802.1x Certificate Server Configuration	330
8.36	Initiate 802.1x by DHCP Options or OM_Configurator	331
8.36.1	DHCP Options	331
8.36.2	OM_Configurator	331
9	Maintenance	332
9.1	Site Survey Measurement Equipment	332
9.2	Checking the Mitel Handset Firmware Version	332
9.3	Diagnostic	332
9.3.1	Mitel DECT Phone Site Survey Mode	332
9.3.2	Mitel Handset Auto Call Test Mode	333
9.3.3	Mitel Handset Auto Answer Test Mode	333
9.3.4	Syslog	334
9.3.5	SSH user shell	335
9.3.6	Core File Capturing	339
9.3.7	DECT Monitor	340
10	Regulatory Compliance and Safety Information (4th Generation Dect Base Stations)	344
11	Safety Information (3rd Generation Dect Base Stations)	345
11.1	CE Marking	345
11.2	Communications Regulation Information	345
11.2.1	FCC Notices (U.S. Only)	345
11.3	Health and Safety	346
11.3.1	Exposure to Radio Frequency (RF) Signals:	346
11.3.2	Industry Canada (Canada only)	346
11.4	Informations réglementaires en matière de communications	346
11.4.1	Notes FCC (USA uniquement)	347
12	Appendix	348
12.1	Pre-Configuration File Rules	348
12.2	DECT phone Configuration File (OMM Database)	348
12.2.1	Supported Instructions	348
12.2.2	Data Section Fields	349
12.2.3	Example	350
12.3	RFP Configuration File / Central (OMM Database)	353
12.3.2	RFP Configuration File / Local (OM Configurator)	356
12.4	RFP Export File Format	360
12.5	CoA Configuration Parameters	362
12.5.1	Configuration of Variable Lists	362
12.5.2	Extended COA Examples	363
12.5.3	Example 1	363
12.5.4	Example 2	363
12.5.5	Example 3	367
12.5.6	Example 4	367
12.5.7	Example 5	369
12.5.8	Supported COA Parameters	370
12.6	Protocols and Ports	398
12.7	Abbreviations	400
12.8	Definitions	401
12.9	References	403

1 OVERVIEW

This document describes the installation / configuration, administration, and maintenance of the SIP-DECT solutions. Please also see the documents listed in the References section (section [12.9](#)) for additional details on different aspects of the SIP-DECT system.

For a list of abbreviations and definitions, see the appropriate sections in the Safety Information.

1.1 THE SIP-DECT SOLUTION

The SIP-DECT solution includes the following main components:

- SIP-DECT base stations that are distributed over an IP network and offer DECT, WLAN, and IP interfaces
- DECT phones (portable DECT devices)
- OpenMobility Manager (OMM): Management and signaling software for the SIP-DECT solution, which runs on one of the DECT base stations or on a dedicated Linux server (for large installations). In addition, a standby OMM can be configured to ensure OMM function in case of failure or loss of network connection.
- A SIP Call Manager/IP PBX/Media Server platform (e.g. Asterisk) 001-omm-arch.psd/.

The IP PBX/media server/media gateway, OMM and the RFPs communicate through the IP infrastructure. The RFPs and the DECT phones 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 include:

- 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 from the server
- OM Locating server and clients to run the SIP-DECT locating solution
- 3rd 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

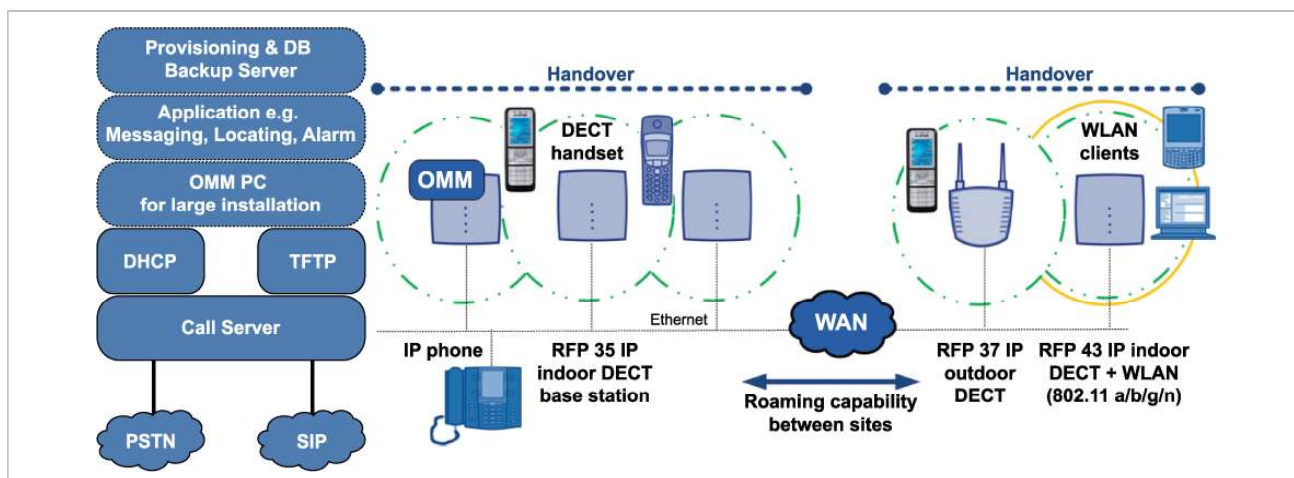


Figure 1 Architectural Overview of the SIP-DECT Infrastructure and Features

1.2 ABOUT DECT BASE STATIONS

DECT base stations are also referred to as Radio Fixed Parts (RFPs) in this document.

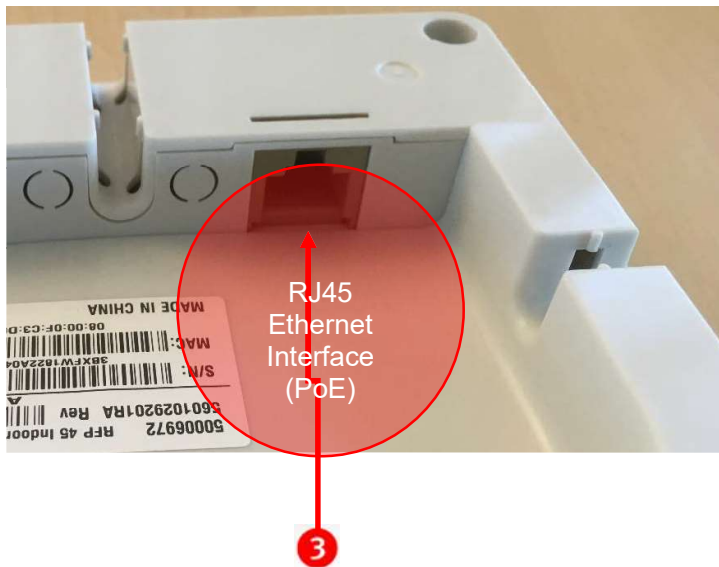
1.2.1 DECT BASE STATION FAMILIES

1.2.1.1 RFP 4G DECT Base Station family

As of SIP-DECT 8.0, SIP-DECT supports the 4th base station generation (RFP 4G). This 4th RFP generation comprises of:

- RFP 44
DECT RFP as indoor model with 4 narrow band voice channels and internal antennas.
- RFP 45
DECT RFP as indoor model with 8 narrow band voice channels and internal antennas.
- RFP 47 (Indoor Unit)
DECT RFP as indoor model with 8 narrow band voice channels and 2 SMA connectors for external directional antennas.
- RFP 47 DRC (Outdoor Unit)
RFP 47 pre-installed with directional antennas and 3m cable in an outdoor enclosure.
- RFP 48
DECT RFP with 8 narrow band voice channels + WLAN Access Point as indoor model with internal antennas for DECT and WLAN.

The hardware of all the RFPs complies with the different regulatory domains. 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.



- 1 RFP 44/45/47/48 (1 LED)
- 2 Configuration Button
- 3 100Mbit/s Ethernet Interface, PoE (RFP 44, 45, 47)
- 4 1Gbit/s Ethernet Interface, PoE (RFP 48)

Differences compared to the previous 3rd RFP family (RFP 35, 36, 37 IP and RFP 43 WLAN) are:

- RFP 48 supports 5GHz WLAN according to 802.11ac and 3x3 MIMO
- Configuration button
 - switch to SIP-DECT with Cloud-ID mode
 - reset RFP to factory defaults
- Separate outdoor enclosure available for outdoor usage
- No external power supply (PoE only)
- No USB interface
- RFP 44/45/ support 100MBit/s Ethernet only, The RFP 48 supports 1 GBit/s
- Boots from internal flash memory instead of net-boot (SIP-DECT software is already on board)
- Software update via TFTP, FTP(S), HTTP(S), SFTP supported
- Hardware can support Secure SIP and SRTP (with SIP-DECT 5.0 or later)
- Supports CAT-iq 1.0 level high definition voice for the Mitel 650 DECT phone

There are no differences regarding the SW update process compared with the 3rd RFP generation, except a SW update through USB is not possible; because, the RFP 4G does not come with a USB interface.

The RFP 47 RF output is provided through 50 ohm SMA–type connectors. These are electrically compliant with old external antennas, although might not fit mechanically to some antenna cabling. It is the responsibility of installers to propose connecting solutions according to the installations. For that, a 50 ohm / 3Ghz coaxial adapter is required, which will link the RF output connectors of RFP47 to the existing DECT antenna infrastructure.

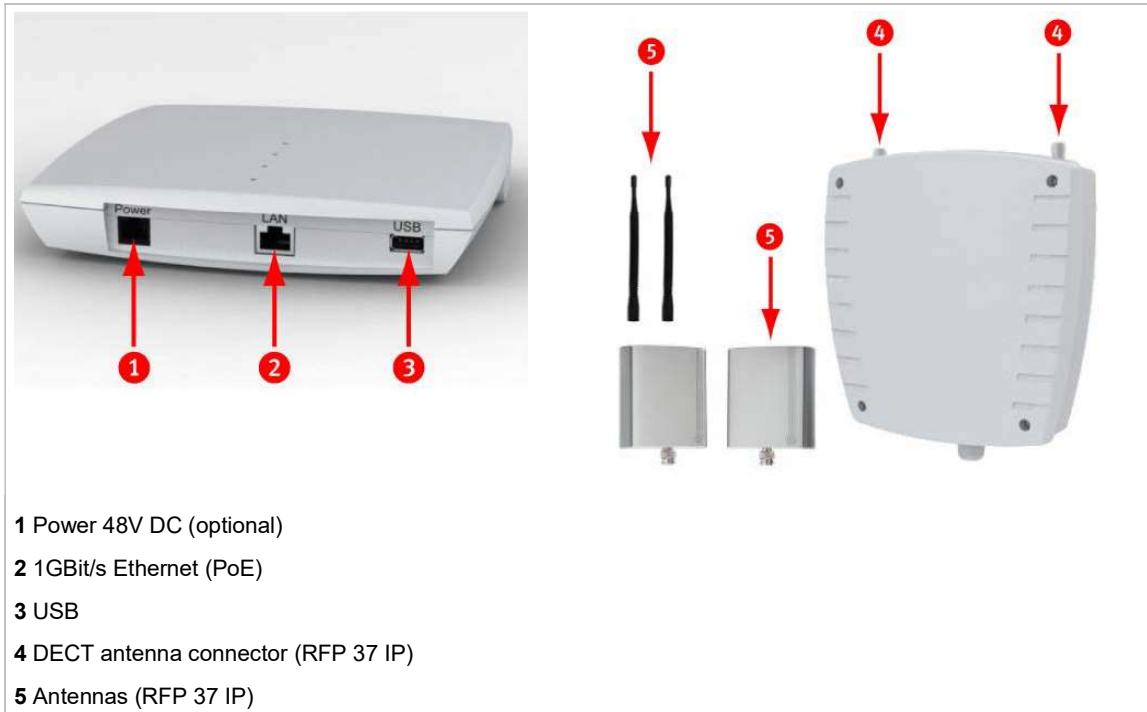
1.2.1.2 RFP 3G DECT Base Station Types

Mitel offers four types of RFP 3G DECT base stations for the SIP-DECT solution:

- RFP 35 IP
DECT RFP as indoor model
- RFP 36 IP
DECT RFP as outdoor model with built-in dipole antennas
- RFP 37 IP
DECT RFP as outdoor model with connectors for external directional antennas
- RFP 37 DRC (Set)
DECT RFP, preinstalled with directional antennas and 3m cable in an outdoor enclosure
- RFP 43 WLAN
DECT RFP + WLAN Access Point as indoor model with internal antennas for DECT and WLAN

As of SIP-DECT 6.0, there is no distinction between DECT base station soft brands (that is, L-RFPs and non-L-RFPs). See section [3.3.2](#) for more information.

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



The hardware of all the new RFPs complies with the different regulatory domains. 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 32/34 IP and RFP 42 WLAN):

- Boots from internal flash memory instead of net-boot (SIP-DECT software is already on board)
- Supports software update through TFTP, FTP(S), HTTP(S), SFTP
- Supports 1Gbit/s Ethernet
- Supports CAT-iq 1.0 level high definition voice for the Mitel 650 DECT phone
- Hardware can support Secure SIP and SRTP (with SIP-DECT 5.0 or later)
- Uses an external 48V DC Power Supply (if no PoE available) which meets the latest environmental requirements (RFP 37: PoE only)
- RFP 43 WLAN supports the 802.11a/b/g/n standards
- Indoor RFPs have a USB 2.0 interface to connect external hardware for future applications (for example, Video Camera)

1.2.1.3 Older RFP Types

Older RFP models supported by the SIP-DECT solution include:

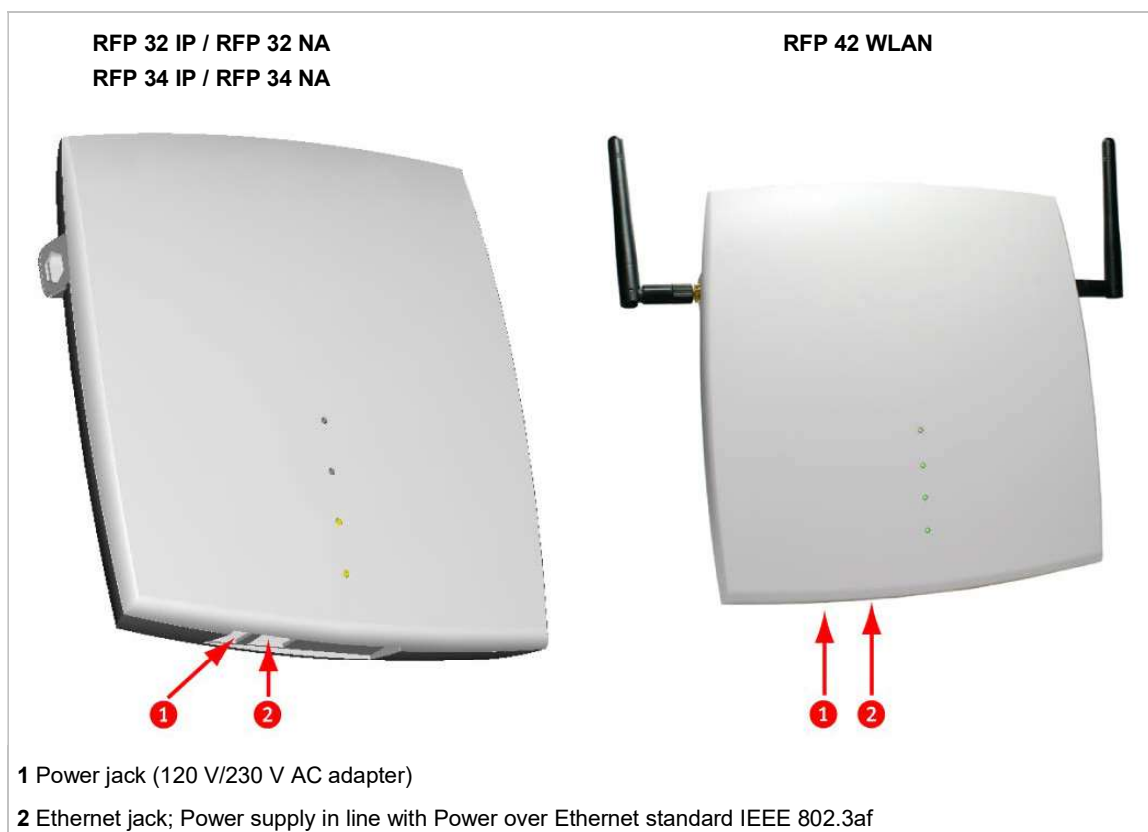
- RFP 32 IP
DECT RFP as indoor model
- RFP 34 IP
DECT RFP as outdoor model

- RFP 42 WLAN
DECT RFP + WLAN Access Point as indoor model

The RFP 32 and RFP 34 have the same hardware and software capabilities. Please note the regulatory differences between North America and 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 32 IP or RFP 34 IP (EMEA)
 - Frequency Band 1880 to 1900 MHz
 - 10 carrier frequencies
 - Transmit Power 24 dBm

The RFP 42 WLAN is only available for the EMEA region.



As of SIP-DECT 6.0, there is no distinction between RFP soft brands (i.e., L-RFPs and non-L-RFPs). With SIP-DECT 5.0 and older releases, the “L” variants have built-in licenses. See section [3.3.2](#) (Licensing) for more information.

Note: The software package for previous RFPs has a tftp extension e.g. “iprpf2G.tftp”. With SIP-DECT 3.0 or higher, you need a 3G RFP to run the Open Mobility Manager.

1.2.2 OPENMOBILITY MANAGER (OMM) MODE

If the OMM is not running on a dedicated Linux server, 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 if it is part of 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/SIP 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 section [8.5](#)) or by setting the data via the OM Configurator (see section [8.7](#)). 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 (for their RFP type), but only one RFP (or two, in standby implementations) activates the OMM services.

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

This might be necessary, for example, in configurations where a mix of OpenMobility Manager, G.729/Conferencing and WLAN is provided by the same RFP.

1.3 ABOUT THE OPENMOBILITY MANAGER

The OpenMobility Manager (OMM) requires an RFP 35/36/37 IP resp. RFP 43 WLAN, or a dedicated Linux server.

There is only one OpenMobility Manager (OMM) active in the system at a given time.

- If the OMM runs on a DECT base station, a 100 Mbit/s network link is required.
- If the OMM runs on a dedicated Linux server, a 1 GBit/s network link is required (see also section [8.13.1](#)).

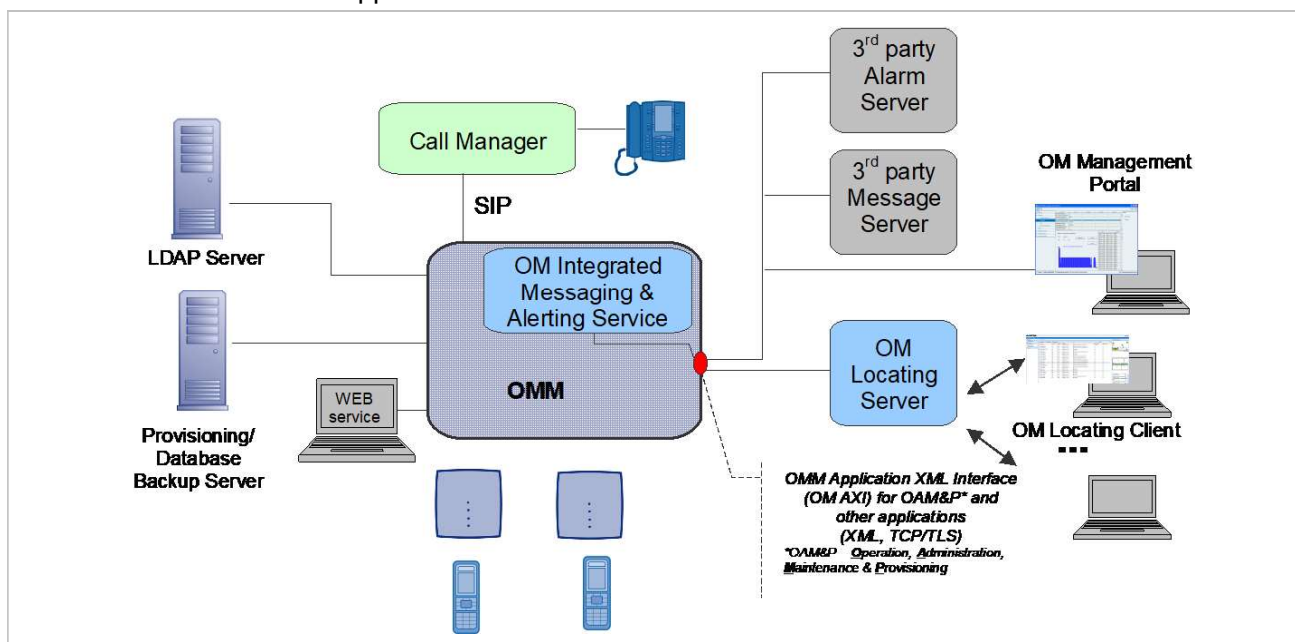
In addition, a standby OMM can be configured to ensure the OMM function in case of failure or loss of network connection. For more information on the standby OMM see section [8.15](#).

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 such as
 - 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 SIP Phones” to SIP-DECT phones. The Mitel 600 DECT phone family is supported.



Additional information on the following functionality is available in separate documents.

- **Locating:** See the SIP-DECT OM Locating Application Administration Guide.
- **Integrated Messaging and Alerting Service:** See the SIP-DECT OM Integrated Messaging and Alerting Application Guide and the SIP-DECT Mitel 600 Messaging and Alerting Applications Guide.
- **User data provisioning:** See the SIP-DECT OM Handset Sharing and Provisioning Guide.
- Administration and monitoring by third party applications: See the OM Application XML Interface Specification.
- SIP-DECT XML terminal interface: See the SIP-DECT XML Terminal Interface Specification.

1.3.2 SIP-DECT SPECIAL FEATURES AND CAPABILITIES

Feature	GAP	142d	600
Large DECT Systems (XXL)	No connection handover beyond 256 RFPs	yes	yes
Messaging & Alerting	no	no	yes
Initiate Alarm Trigger	*, # feature access code procedure, no sensor alarm	*, # feature access code procedure, no sensor alarm	yes
Locating	yes	yes	yes
DECT XQ	no	no	yes

Feature	GAP	142d	600
UTF-8 and alphanumeric dialing support	no	no	yes
SIP-DECT XML terminal API	no	no	yes
CAT-iq 1.0 / Hi-Q™ audio technology	no	no	yes (650 only)

1.3.3 OMM CAPACITIES AND FEATURES

The following table summarizes OMM capabilities:

Feature	Release 3.0 or later		Release 6.0 or later	
	RFP OMM	Linux server OMM	RFP OMM	Linux server OMM
RFP 32/34/35/36/37/44/45/47 IP and RFP 42/43/48 WLAN	256 ¹	2048 ¹	256 ¹	4096 ¹
Handsets / users	512	4500	512/1024 ³	10000
Message / Alarm receive	yes / yes ¹	yes / yes ¹	yes / yes ¹	yes / yes ¹
Message send	yes	yes	yes	yes
Locating	yes ¹	yes ¹	yes ¹	yes ¹
DECT XQ	yes	yes	yes	yes
UTF-8 and alphanumeric dialing support	yes	yes	yes	yes
SIP-DECT XML terminal API	yes	yes	yes	yes
CAT-iq 1.0 / Hi-Q™ audio technology	yes ²	yes ²	yes ²	yes ²

¹ The feature requires a license.

² The feature is available with the RFP 35/36/37/44/45/47 IP and RFP 43/48 WLAN and the Mitel 650 DECT phone (or other CAT-iq-capable devices). The feature is enabled per site and requires that the RFPs are configured in the same site and cluster.

³ Release 8.0 or later: If RFP 4G runs as OMM, 1024 users/handsets are supported.

1.3.4 OMM CAPACITIES AND RFP SUPPORT

The following table summarizes OMM and RFP support capabilities:

Feature	As of SIP-DECT 6.0		As of SIP-DECT 8.0	
	RFP OMM	Linux server OMM	RFP OMM	Linux server OMM
RFP 32/34 IP and RFP 42 WLAN	256	4096	256	4096
RFP 35/36/37 IP and RFP 43 WLAN	256	4096	256	4096
RFP 44/45/47 IP and RFP 48 WLAN	Not applicable	Not applicable	256	4096

Feature	As of SIP-DECT 6.0		As of SIP-DECT 8.0	
	RFP OMM	Linux server OMM	RFP OMM	Linux server OMM
DECT phones / users	512	10000	1024 (RFP 4G OMM) 512 (RFP 3G OMM)	10000

1.4 ABOUT DECT PHONES

DECT Phones (formerly referred to as Portable Parts) are an integral part of the SIP-DECT solution.

Mitel provides the following DECT phones:

- Mitel 142 DECT Phone
- Mitel 600 DECT Phone series
 - Mitel 612 DECT Phone
 - Mitel 622 DECT Phone
 - Mitel 632 DECT Phone
 - Mitel 650 DECT Phone

Notes on the Mitel 600 DECT Phones

The Mitel 600 DECT phones support both the NA and EMEA regulatory requirements.

The latest Mitel 600 firmware release 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 (not supported by Mitel 600 DECT phones)
- Additional subscription options
- Additional alarm melodies
- Profile indication in idle display

For more details please see /31/and /32/.

In addition to the existing Mitel 600 DECT phone set, the new Mitel 650 DECT phone supports CAT-ig 1.0 and thus supports G.722 (wideband) voice connections. For the full experience of wideband audio, the DECT phone hardware (e.g., speakers, microphone, and processor) has been improved.

The Mitel 600 DECT phone also supports DECT enhanced security.

1.5 FILE NAMING CONVENTIONS

The following table lists the file names for SIP-DECT software deliverables.

Software package	As of SIP-DECT 7.1	As of SIP-DECT 8.0
Software image for RFP 32/34 IP / RFP 42 WLAN	omm_ffsip.tftp	iprfp2G.tftp
Software image for RFP 35/36/37 IP / RFP 43 WLAN	iprfp3G.dnld	iprfp3G.dnld
Software image for RFP 44/45/47 IP / RFP 48 WLAN	Not applicable	lprfp4G.dnld
OMM software for Linux Red Hat server (self-extracting executable)	SIP-DECT_<version>.bin	SIP-DECT_<version>.bin
OMM software rpm	SIP-DECT-OMM- <version>.i686.rpm	SIP-DECT-OMM- <version>.i686.rpm
DECT phone software rpm	SIP-DECT-HANDSET- <version>.i686.rpm	SIP-DECT-HANDSET- <version>.i686.rpm
SIP-DECT OMM/MOM OVA	SIP-DECT-<version>.ova	SIP-DECT-<version>.ova

1.6 LOGIN AND PASSWORDS

The following table summarizes the default login and passwords for SIP-DECT system components.

Interface/Tool	SIP-DECT OMM SDC OMM	RFP 32/34 IP / RFP 42 WLAN	RFP 35/36/37 IP / RFP 43 WLAN RFP 44/45/47 IP / RFP 48 WLAN
Initial configuration through OM Configurator login / password (no previous connection with the OMM)	n/a	No login required	"omm" / "omm"
Initial OMM configuration through Web or OMP standard full-access account login / password	"omm" / "omm" "omm" / "omm"	n/a	n/a
OMM access through Web or OMP (after initial OMM configuration)	Read-only or full-access accounts as configured	n/a	n/a
Configuration through 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

2 ENHANCED FEATURE OVERVIEW

A SIP-DECT system can scale from a small system of five or less DECT base stations to a larger SIP-DECT system that may include hundreds of DECT base stations. 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 sections.

Please note: Be aware that the majority of the new enhanced features require the current DECT phone firmware release. It is assumed that SIP-DECT installations are configured to perform an automatic firmware update over the air.

2.1 PC-BASED OMM INSTALLATION

A very large number of DECT base stations or a large number of DECT phones may exceed the storage capacity or processing power of the embedded DECT base station. For this reason, it is also possible to operate the OMM on a standard PC under the Linux operating system (see section [8.13](#)).

As of SIP-DECT 5.0, CentOS 6 and virtualized environments (VMware vSphere ESXi 5 and 6) are also supported. SIP-DECT 6.1 is tested with CentOS 6.x.

As of SIP-DECT 7.1, CentOS 7 is required. An OVA-File is distributed together with the software for usage within virtualized environments (VMware vSphere 6.5). The verification is executed with VMware vSphere 6.0 and 6.5. For further information, see document */47/ SIP-DECT_LinuxServerInstallation*.

2.2 DECT XQ

The DECT radio communication generally suffers from attenuation and radio wave reflection. In particular, 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 a DECT base station and a Mitel 600 DECT phone at the expense of DECT channel capacity (see [8.3](#)). Enable this feature for some or all of your DECT base stations (see section 5.6.3, "DECT settings" or section 6.7.1.2, "DECT tab").

DECT XQ audio cannot be combined with Hi-Q audio within the same connection.

There are three operating modes related to audio quality available on the Mitel 650 DECT phone: standard audio, Hi-Q audio and automatic.

- In Hi-Q audio mode, a Mitel 650 DECT phone exclusively establishes wideband connections and does not switch to narrowband later. A Mitel 650 in this mode ignores the XQ capability of the RFP.
- In standard audio mode, a Mitel 650 DECT phone exclusively establishes narrowband connections and does not switch to wideband later. A Mitel 650 in this mode will switch to DECT XQ and back as necessary.
- 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.

2.3 WIDEBAND (CAT-IQ 1.0 / MITEL HI-Q™ AUDIO TECHNOLOGY)

In conjunction with the RFP 35/36/37/44/45/47 IP and RFP 43/48 WLAN, the Mitel 650 DECT phone can act as a Mitel Hi-Q audio terminal. This feature is realized using wideband speech according to CAT-iq. Each Hi-Q connection uses twice the capacity on the DECT air interface, as compared to conventional narrowband. Therefore, four Hi-Q connections can be established via one RFP, instead of eight narrowband calls.

Mitel Hi-Q audio technology must be enabled or disabled per site (see section 5.5). 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 35/36/37/44/45/47 IP or RFP 43/48 WLAN.

Typically one site is identical with one cluster, i.e. all RFPs belonging to a specific site belong to a specific cluster. However a site can have more than one cluster. The OMM allows configuration of a cluster that 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.

2.4 DECT ENHANCED SECURITY

In response to market concerns, the DECT standard has introduced improvements to security. Many security features, which were specified in the DECT standard (respectively GAP) were left optional for the DECT phones. These mechanisms became mandatory with CAT-iq. Almost all of this functionality was present and used within SIP-DECT right from the start.

Furthermore, some new features have been added to GAP:

- Encryption of all calls (not only voice calls)
- Re-keying during a call
- Early encryption

Each feature provides an additional security guarantee and is therefore an integral part of the SIP-DECT solution.

The feature set can be enabled or disabled per site, because enhanced security is available with 3rd or 4th generation RFPs. Roaming between sites where enhanced security is enabled and disabled respectively should be avoided.

With SIP-DECT 5.0 and later, when DECT enhanced security is enabled, every connection is encrypted – not only voice calls, but also service calls (e.g. list access) or messaging.

Additionally, the cipher key used for encryption during an ongoing call is changed every 60 seconds.

Finally, every connection is encrypted immediately upon establishment to protect the early stages of the signaling such as dialing or CLIP information.

DECT enhanced security is only supported with Mitel 602 DECT phones. Older terminals (e.g. 6x0d or 142d) or GAP phones still operate as normal, but do not support the new security mechanisms.

2.5 VOIP ENCRYPTION

To allow secured call connections over unsecured IP infrastructures (e.g. internet), SIP-DECT supports SRTP to encrypt the RTP voice streams and TLS to encrypt the SIP signaling.

These security mechanisms, together with a secured IPBX infrastructure, allow protected call services and ensure:

- Authentication
- Integrity
- Confidentiality
- Privacy

When a Mitel 600 DECT phone user is involved in a SRTP call, a key icon in the call display indicates that the media path to the next hop is ciphered.

The key icon is only displayed when the connection uses SIP over TLS, SRTP (for 3G RFPs only) and DECT encryption together for a secure key exchange and a secure media transport.

2.6 MIXED DECT BASE STATION INSTALLATIONS

In sites (or whole systems) with Hi-Q audio disabled, any combination of RFP 32/34 IP / RFP 42 WLAN and RFP 35/36/37 IP / RFP 43/48 WLAN is allowed. Note, however, that some security features are not supported for all DECT base stations (that is, SRTP and enhanced security are supported on 3rd and 4th generation RFPs only).

RFP SL35 IP support

SIP-DECT supports the RFP SL35 IP after applying the unlock file and the standard SIP-DECT software to the DECT base station.

Before the standard SIP-DECT software can be installed on the RFP SL35 IP, the unlock.xml file must be available for the DECT base station on the USB. After applying the unlock.xml file the DECT base station accepts the standard SIP-DECT software.

In terms of licensing, the OMM manages the RFP SL35 IP with the unlock file and the standard SIP-DECT software like an RFP 35 IP.

For a detailed description see section [8.30](#).

2.7 WIRELESS LAN (WLAN)

If you have a number of WLAN DECT base stations (RFP 42/43/48 WLAN), the SIP-DECT system also provides access to your company LAN through Wireless LAN. The RFP 43/48 WLAN support 802.11n. The RFP 48 WLAN also supports 802.11ac. The WLAN configuration of a group of WLAN RFPs is managed by WLAN profiles (see section 5.8).

2.7.1 802.11i: WPA2-ENTERPRISE PRE-AUTHENTICATION FOR FAST ROAMING

WLAN stations (e.g. laptop) which decide to roam to another WLAN access point (AP) must perform the full authentication process with the new AP. In 802.1x (RADIUS) networks this can take a long time resulting in network dropouts during the roam.

The AP share authentication information with other APs, so the station can authenticate faster (pre-auth) when roaming to a new AP. This method reduces network dropouts significantly.

The RFP 43 and RFP 48 automatically enables pre-authentication for WPA-Enterprise enabled WLANs. The RFP 42 does not support this feature.

2.7.2 CHANNEL CONFIGURATION FEEDBACK FOR HT40 AND TX POWER

The HT40 channel configuration in 802.11n enabled networks may not always become active because of other access points that use channels that would overlap. In this case, the RFP 43 and RFP 48 fall back to HT20.

From SIP-DECT 5.0 on, the effective channel configuration and the transmit power are reported to the OpenMobility Manager.

You can view these parameters in the OMM Web service and the OMP (**DECT base stations > Device list** -> **Show details** – **WLAN** tab) and change the channel to a frequency without overlapping APs.

2.7.3 CHANNEL CONFIGURATION FEEDBACK FOR HT80

HT80 includes the HT40/HT20 bandwidth setting. A channel with a bandwidth of 80 MHz occupies 4 WLAN channels with a bandwidth of 20 MHz. If the WLAN profile options HT80/ HT40 MHz have been activated, the necessary center channel will be automatically selected in the corresponding areas by configuration itself.

HT80 is independent from 256 QAM / 3x3 MIMO. The ac standard is the first WLAN standard with 256 QAM modulation and the bandwidth HT80. The n standard supports 3x3 MIMO too, but the RFP43 has only 2 antennas (for 2x2 MIMO) and the RFP48 has 3 antennas.

2.8 DECT BASE STATION SYNCHRONIZATION

To ensure a seamless communication experience, the SIP-DECT system switches an ongoing DECT phone call from one DECT base station to another if the radio communication quality drops below a certain threshold. The seamless handover is possible only if the participating DECT base stations are synchronized. DECT base station synchronization is performed via radio communication between DECT base stations, which in turn requires a decent radio coverage planning (see section [8.2](#)).

2.8.1 CLUSTERING AND 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 must split your network into clusters (or “synchronization domains”). You assign DECT base stations to cluster numbers for this purpose (see section 5.6.3 “DECT settings” or section 6.7.1.2, “DECT tab”). Note that overlap between different clusters on one campus or site must be avoided.

If your SIP-DECT system consists of a very large number of DECT base stations, you should configure the paging area size to optimize the signaling necessary for paging a DECT phone in throughout the SIP-DECT system (see 6.7.2).

A separate cluster number is also required for a remote site (e.g., for a single DECT base station servicing an office abroad). Also, if the VPN network connection to the isolated site’s DECT base station cannot transport DHCP, you may use static IP address configuration for the single DECT base station (see section [8.7.6](#)).

2.9 DECT BASE STATION RESET TO FACTORY SETTINGS

A DECT base station can be reset to factory settings using a USB flash drive with a file on it named “factoryReset”. When the USB flash drive is plugged into the DECT base station, the DECT base station is reset to factory settings automatically. The file is automatically removed from the USB flash drive during this process.

You can also reset the base station to default settings using the OM Configurator or the OMM Web service (see section [8.7.8](#)).

2.9.1 RFP4G RESET TO FACTORY DEFAULTS

To reset to factory defaults, do the following:

1. Use the configuration button to reset the RFP to factory defaults. After the reset to factory defaults, the RFP operates in the standard SIP-DECT mode.
2. Press the Configuration button to start the configuration process. The LED starts flashing green which indicates that the button is pressed.
3. Keep the button pressed until it starts flashing red (10 sec < t < 15 sec).



4. Release the button while the LED is flashing red to reset the RFP to factory defaults.
5. The RFP performs a reset to factory defaults and reboots. After reboot the RFP is started in the standard SIP-DECT mode.

Note: If the button is pressed until it is flashing green, then the button has no effect.

2.10 SYSTEM REDUNDANCY

The SIP-DECT solution offers a number of features to support system robustness and redundancy.

2.10.1 OMM STANDBY

The OMM is the central management entity in a SIP-DECT system and therefore constitutes a single point of failure. It is possible to automatically transfer the OMM function to a second DECT base station in case of failure or loss of network connection (see section [8.15](#)).

In an OMM standby implementation, it could happen in rare cases that both OMMs become temporarily active. In such a situation, all SIP-DECT users are SIP registered from to the configured PBX both OMMs. This can cause problems if the PBX accepts only one registration per user (non-forking proxy).

To prevent this scenario, SIP-DECT has a mechanism to detect situations with two active OMMs. When such a situation is detected, the remaining active OMM will SIP re-register all users to the PBX.

This mechanism can be enabled/disabled through the “SIP reRegister after 2 active OMM failover” parameter in the OMP **System -> SIP-> Supplementary Services** menu (see section 5.4.3.6)

2.10.2 BACKUP SIP PROXY/REGISTRAR

To increase the operational availability of the system in critical environments like hospitals, the OMM offers a new failover mechanism for the SIP server. Therefore, in addition to the primary proxy, outbound proxy and registrar server, it is possible to configure two additional levels of backup servers named “secondary” and “tertiary” servers (see section [8.20.3](#)).

In addition, a keep-alive mechanism implemented in the OMM allows the automatic failover to secondary/tertiary servers or automatic coming back to primary servers (see section [8.20.4](#)).

2.10.3 CONFIGURABLE USER ACCOUNT FOR STANDBY CHECK

The “Standby OMM” feature of SIP-DECT allows configuration of the user account to be used to check the availability of the iPBX. An availability check starts automatically in fail over situations.

The OMM starts a SIP registration for a specific DECT phone user and sends an OPTIONS request to the configured SIP proxy. If there is an answer, the SIP proxy/registrar is considered reachable and the standby OMM becomes active.

With previous SIP-DECT releases, the OMM used the user account with the lowest phone number for the check procedure. To select a specific user account for this purpose, enable the “Used for visibility checks” flag in the user settings (see section [6.10.4.2](#)).

Please note: The “Used for visibility checks” flag can only be set for one user. The number for visibility checks is shown under OMP **Status -> Users -> Number** menu. If the flag is not set for a specific user, the OMM uses the user account with the lowest phone number.

2.10.4 USER DATA SYNCHRONIZATION (MIVOICE 5000 DUAL HOMING SUPPORT)

With SIP-DECT 6.1 and later, SIP-DECT supports MiVoice 5000 dual homing, to ensure that SIP-DECT telephony services survive if the network connection to the OMM goes down. Dual homing is achieved through user data synchronization across all OMMs in the system. Every peripheral OMM propagates changes in user, device, Configuration over Air (CoA) profiles or SARI configuration to a central OMM.

Every OMM in the installation (including the central OMM) can use a standby OMM. AXI is used to distribute configuration changes between the central and peripheral OMMs.

For more information on this feature, see section [8.16](#).

2.10.5 MULTI-OMM MANAGER FOR OMM-CENTRALIZED MANAGEMENT

With SIP-DECT 7.0 and later, SIP-DECT supports centralized management through the Multi-OMM Manager (MOM).

The Multi-OMM Manager (MOM) is a server application that provides centralized provisioning and user/device data synchronization across multiple SIP-DECT sites within a SIP-DECT system. Additionally, the MOM supports system-wide messaging.

Instead of deploying one OMM with DECT base stations installed at different sites, or deploying DECT base stations and a dedicated OMM at each site, you can create a multi-site SIP-DECT system with local survivability and centralized management capabilities. You deploy OMMs and DECT base stations as a standalone system at each site, but manage the entire SIP-DECT system through the MOM interface.

For more information on this feature, see the *Multi-OMM Manager Configuration and Administration Guide*.

2.11 SIMPLIFIED LICENSING

With SIP-DECT 6.0 or later, the licensing model is simplified. The system no longer distinguishes between different DECT base station “soft-brands”, and some licenses are deprecated. See section [3.3.2](#) for more information.

Please note: New license files are not compatible with SIP-DECT 4.0 (or older) systems.

2.12 EXTENDED REGULATORY DOMAIN SUPPORT

SIP-DECT 6.1 enables operation of the SIP-DECT solution in more countries. The SIP-DECT system can be operated in all countries that allow operation of DECT devices with frequency bands and transmit power settings supported by the current SIP DECT phones and base stations. In most cases, this requires different frequency channel and transmit power settings.

This feature is intended mainly for installations on cruise liners, where the SIP-DECT system requires a switch of regulatory domain depending on the actual location of the ship. Such systems are planned and installed based on a site survey with 100mW transmit power. The lower transmit power value is used at all times, independent from the regulatory domain.

A new regulatory domain, 1910-1927MHz_250mW, has been added for South America. You can configure this regulatory domain via the OMP (**System** -> **Basic settings** -> **DECT** tab); see section 6.5.1.2 for configuration details.

In addition, a new parameter is introduced to limit the DECT base station transmit power to 100mW, independent of the active regulatory domain. The active transmit power is sent to the DECT phone when it registers its location with the OMM. The DECT phone adjusts its transmit power to the value received from the OMM.

2.13 DECT PHONE FUNCTIONALITY

2.13.1 DECT PHONE DOWNLOAD OVER AIR

The Mitel 600 series DECT Phones can download and upgrade their firmware via DECT over the air. As of SIP-DECT 6.0, the DECT base station software images (iprfp3G.dnld and iprfp4G.dnld) contains the Mitel 600 DECT phone software. The 3rd generation RFPs can house the SIP-DECT 8.0 OMM as in previous releases. The OMM supports the 2nd, 3rd and 4th generation RFPs. If the DECT base station houses the OMM, the OMM uses this software to update the DECT phones. The DECT base station OMM no longer automatically attempts to load a DECT phone software image from a DECT base station software URL when provided via DHCP or local configuration.

For specific maintenance purposes only, SIP-DECT allows configuration of a URL via the OMM Web service or OMP to use an alternative DECT phone software image (see section [5.4.1.8](#)). The Mitel 600 DECT phone firmware packages are delivered in the “600.dnld” file for the OMM running on a DECT base station.

For large installations using a Linux Server-hosted OMM, a DECT base station software images (iprfp3G.dnld and iprfp4G.dnld) without Mitel 600 DECT phone software is available to reduce network traffic in update scenarios.

The DECT phone firmware packages are included in the OMM installation package for Red Hat Enterprise Linux (RHEL) and CentOS for the Linux server version of the OMM.

Please note: An DECT base station upgrade from SIP-DECT 3.0 to 6.0 or later is not supported due to the extended DECT base station software image. The 3.0 software does not accept the extended software image.

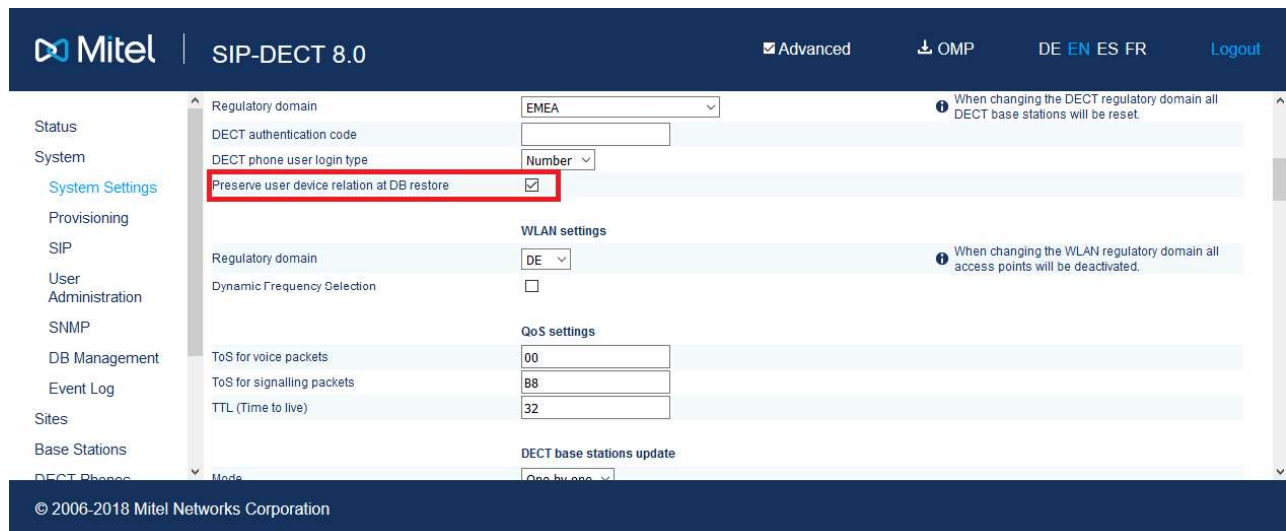
For large installations using a Linux Server OMM, the DECT base station software images (iprfp3G.dnld and iprfp4G.dnld) without Mitel 600 DECT phone software can be used. This software image supports a direct RFP upgrade from SIP-DECT 3.0 to 6.1.

2.13.1.1 4th Generation RFP houses the OMM

The 4th generation RFPs come with more hardware resources in terms of CPU speed and memory. It is recommended to operate the OMM on a 4G RFP.

Please note: If you move the OMM and you want to keep the existing dynamic user phone relation which is stored in the OMM DB backup file, then activate the option **Preserve user device relation at DB restore** in the new OMM. The new OMM restores the relation between the user and the DECT phone during DB import.

If this option is not set, then all dynamic user gets logged out from their DECT phones when importing the OMM DB into the new OMM.



If the OMM is operated on 4G RFP, then 1024 DECT users and phones are supported. (512 DECT users and phones if the OMM is operated on a 3G RFP).

The 4G RFP comes with the configuration button, which allows to switch to the SIP-DECT with Cloud-ID (SDC) mode. As of SIP-DECT 8.0, a 4G RFP is required to run an SDC OMM.

2.13.2 CENTRAL DECT PHONE CONFIGURATION OVER AIR (COA)

SIP-DECT 6.0 and later supports centralized DECT phone configuration over the air (CoA) for Mitel 602 DECT phones. DECT phone CoA is useful for deployment of special configuration to a single DECT phone or a large number of DECT phones. No local access to the DECT phone is required.

DECT phone CoA is implemented by providing additional configuration information to the well-known configuration files or providing profiles via OMP. Configuration can be changed at the device level (DECT subscription) or the user level (based on login).

Configuration of all DECT phones with a predefined default profile is also supported. Up to 20 possible DECT phone profiles make it easy to adapt to different usage scenarios for heterogeneous user groups (e.g., nurses and doctors in hospital environments). See section [8.23](#) for more information on this feature.

2.13.2.1 CoA enhancements

The Mitel 602 DECT phone 6.1 firmware (bundled with SIP-DECT release 6.1) includes new features which are configurable via Configuration over Air (CoA).

New configuration commands allow you to overwrite local key programming on the Mitel 602 DECT phones. SIP-DECT 6.1 also supports configuration of the new XML application hooks introduced for the XML terminal interface via CoA (see section [2.32](#)).

In addition, the Mitel 602 DECT phone 6.1 firmware introduces variable lists. A variable list includes a number of items, each of which corresponds to an action to be performed on the DECT phone. For more information, see section [8.23.5](#).

2.13.3 OMM DECT PHONE PROVISIONING

While some users in the SIP-DECT system use a dedicated DECT phone, it is also possible to operate shared DECT phones. The SIP-DECT solution provides an enhanced DECT phone sharing and provisioning concept that enables the management of a large number of DECT phones and provides a flexible subscription model.

The SIP-DECT system allows logging into and out of different DECT phones with a personalized user account, import of user data from an external provisioning server, automatic subscription of new DECT phones, and control of subscription-specific system functions from DECT phones.

See the *SIP-DECT DECT Phone Sharing and Provisioning Guide* for details on this feature.

2.13.4 MITEL 600 DECT PHONE DIAL EDITOR MODE

It is assumed that most customers use digits only in their dialing plan, and that it is more convenient if dial editors support only the digits 0 to 9, * and #. The **Dial editor supports digits only** flag (on the OMP (**System** -> **Advanced settings** -> **DECT Phones** tab) enables this mode. In this mode, the * has the meaning of a digit to be merely dialed, even if it short-pressed.

If the mode is not set to digits only, the short pressed * will change the editor mode to alphanumeric.

2.13.5 MITEL 602 DECT PHONE CUSTOMIZABLE BOOT TEXTS

By default, the text shown on the Mitel 600 DECT phone at start up is Mitel-specific (branded in the firmware). Customers can also define their own text (on the OMP (**System** -> **Advanced settings** -> **DECT Phones** tab).

2.13.6 OMM-CENTRALIZED CALL LOGS

SIP-DECT 7.0 introduces support for OMM-centralized call logs for SIP-DECT systems using the Mitel MX-ONE call server.

The OMM-centralized call log features the OMM manager caller and redial list entries pushed by the MX-ONE call server for all DECT phones in the system. When this feature is enabled, DECT phone users can access the OMM-centralized call log on their DECT phones using the existing XML hooks for caller list and redial list.

The OMM also handles the “missed call” notifications for the DECT phone. If the number of missed calls changes, the OMM sends the information to the DECT phone.

The OMM sorts the call log entries according to the most recent entry. Call log entries from the same day are listed with the time stamp and older entries are listed with the date stamp.

For information on how to enable OMM-centralized call logs, see section 5.9.5.2 (Modifying an XML Hook via the OMM web service) or section [6.12.8.2](#) (Modifying an XML Hook via the OMP).

2.13.7 USER INDIVIDUAL DECT PHONE PIN KEY LOCK

2.13.7.1 OMM Key Lock with PIN Management

The Mitel 600d DECT phone family Mitel 612d, 622d, 632d, 650c offers a new PIN management to protect the DECT Phone. As of SIP-DECT 8.0 and the DECT phone SW 7.2, the key lock PIN is managed by the OMM to improve the shift worker support and the roaming between OMMs in a MOM setup.

If the DECT phone is subscribed to a SIP-DECT system, the local DECT phone key lock PIN settings are suppressed and the OMM managed PIN is used. Although PIN key lock settings may be suppressed the user can change his PIN.

The key lock with PIN can be managed through Web, OMP, OMM configuration files and by the user through the DECT phone UI in System menu/Administration/Key lock.

Note that this is not possible for external users, that is, users who are provisioned through `user.cfg` file. If user data are provisioned through `user.cfg` files, then the provisioning platform is the data master and there is no option to update data towards the provisioning platform when changed in the SIP-DECT system. Therefore, data changes in the SIP-DECT system are prevented.

For information on how to activate the feature, see section [6.10.4.12](#) “**Key lock**” tab.

2.13.7.2 Resetting DECT Phone PIN

If a user has forgotten his PIN to unlock the DECT phone, the administrator can setup a new PIN through OMP, if the phone is reachable by the system; see section [6.10.4.12](#) “**Key lock**” tab.

If the DECT phone is not reachable by the system, the phone may be master-reset by a procedure described in the *Mitel 600 DECT Phone User Guide*.

2.14 HOT DESKING

With SIP-DECT 6.2 and later, hot desking functionality, as provided by the MiVoice Business platform, is supported.

Users with hot desking permissions are configured in the OMM system without a bound device, and the hot desking capability flag set to enabled.

The hot desking capability allows a user to use the same extension on multiple devices. For example, a user who has a hot desk extension can log into the DECT phone and be automatically logged out of the desk phone (and vice versa).

The user can initiate a log out from the DECT phone via the **Administration** menu on the device.

2.15 CONFERENCING

To improve the integration with different SIP servers, SIP-DECT includes support for centralized and internal three-way conferencing.

The centralized conferencing feature is based on RFC 4579 and supports the use of external third party conference servers (e.g. Broadsoft or Sylanro servers), which are RFC 4579-compliant.

SIP-DECT also includes an integrated conference server implementation based on RFC 4579. The integrated conference server offers three-way conferencing to SIP-DECT users who are hosted on SIP servers without their own conference solution.

The centralized as well as the integrated conferencing feature allows users to:

- merge two active calls together into a conference call
- transfer another party into the conference when on an active conference call

- disconnect from an active conference call while allowing the other participants to remain connected

Regardless whether the centralized or the integrated conferencing is used, conferences can be initiated from the Mitel 600 and Mitel 142d DECT phones.

For a detailed description of conferencing functionality, see section [8.21](#).

2.15.1 CONFERENCING AUDIO NOTIFICATION

The SIP-DECT Integrated Conference Server (ICS) notifies all conference participants when someone is joining or leaving the conference. The notification is a specific tone for joining and a specific tone for leaving the conference.

2.15.2 CENTRALIZED CONFERENCING WITH MIVOICE BUSINESS

SIP-DECT 6.1 introduces support for centralized conferences hosted by the MiVoice Business platform. The SIP signaling implemented by the MiVoice Business platform require that the SIP-DECT implementation initiate a conference via blind transfer. The conference mode (External – blind transfer) can be configured globally for all SIP-DECT users (via the OMP **System** -> **SIP** -> **Conference** tab) or configured individually for SIP-DECT users (via the OMP **DECT Phones** -> **Users** -> **Conference** tab). SIP-DECT 6.1 also introduces a new Feature Access Code. The new “Blind transfer” Feature Access Code allows a user to initiate a SIP blind transfer from the Mitel 600 DECT phone. You can configure the FAC via the OMM web service (see section 5.9.4) or the OMP (see section [6.12.2](#)).

Please note: Overlap sending is not supported for FAC. The blind transfer FAC and the following transfer target number must be entered en-bloc. The blind transfer FAC cannot be triggered manually from the dial editor.

To support the integration of SIP-DECT with the MiVoice Business platform, SIP-DECT 6.1 extends the XML terminal interface for the Mitel 600 DECT phone to include new predefined XML application hooks. These additional functions can be applied to the DECT phone's programmable keys or accessed from a menu.

You must configure the appropriate hooks in the OM via the OMM Web service or OMP (**System Features** -> **XML Applications**) to make the applications available on the Mitel 600 DECT phones.

2.15.3 N-WAY CONFERENCING

SIP-DECT introduces off release 7.1 support of n-way conferencing in conjunction with third party conference servers which are compliant with RFC4579 (for example, Broadsoft).

This functionality allows to easily extend an already established 3-way conference by adding further participants.

The creator of the conference has to execute the following steps to accomplish this:

- make an inquiry call to the next participant.
- if the called party accepts the call, then enter the options menu.
- select entry "conference".
- the called party is added to the conference.

2.16 SIP OVER UDP/TCP/TLS

In addition to UDP, SIP-DECT also supports TCP and TLS as transport protocols for SIP signaling. The OMM provides the following transport protocol modes:

- **UDP:** All SIP messages are sent/received via UDP
- **TCP:** All SIP messages are sent/received via TCP
- **UDP/TCP:** All outgoing connections are always set up via TCP, but incoming SIP messages are also accepted when sent over UDP
- **TLS:** All SIP messages are sent/received via TLS connections
- **Persistent TLS:** All SIP messages are sent/received over TLS connections. The OMM tries to keep the connection to the SIP server open permanently.

2.17 SIP MULTIPOINT

Some call server platforms (e.g. Cisco CUCM) and internet telephony provider environments (SBCs) do not accept SIP registration from different users who have the same IP address and port, but require a unique source signaling port for every SIP extension. By default, the OMM uses one source port for all extensions, but does allow the configuration of individual local signaling ports for users and conference rooms.

The port range is set per protocol (i.e., UDP/TCP and TLS), and must not overlap with other ports in use.

The following parameters can be configured or read per user (see section 6.10.4) and conference room:

- **Fixed port:** Port used explicitly for SIP signaling. If set to 0, an automatically calculated port is used for this user or conference room. The default is 0.
- **Calculated port:** A read-only parameter whose calculation is based on the internal user or conference room ID and a configurable port range, in a way that all users or conference rooms are spread over the range.

The calculation is based on the following rules:

$$\begin{aligned} \text{UserPortCount} &= \text{UserPortRangeStart} - \text{UserPortRangeEnd} + 1 \\ \text{UserPort} &= ((\text{UserID} - 1) \% \text{UserPortCount}) + \text{UserPortRangeStart} \end{aligned}$$

$$\begin{aligned} \text{ConfRoomPortCount} &= \text{ConfRoomPortRangeStart} - \text{ConfRoomPortRangeEnd} + 1 \\ \text{ConfRoomPort} &= (\text{ConfRoomID} \% \text{ConfRoomPortCount}) + \text{ConfRoomPortRangeStart} \end{aligned}$$

The “Calculated port” is first updated with the SIP registration of the user or conference room.

Depending on the “Register Traffic Shaping” settings and the number of users/conference rooms, the update may take some time.

The port ranges used for the port calculation can be configured globally for all SIP DECT users and conference rooms via the OMP (see section 6.5.4.1).

Please note: To provide each user and/or conference room with a unique port using the port calculation, the port range must be greater than or equal to the number of users or conference rooms.

Configuration Rules for Port Ranges

Please note the following configuration rules for configuration of the UDP/TCP and TLS port ranges:

- Port ranges for users and conference rooms may not overlap.
- A port range configured outside the defaults (5060, 5061, 4060, 4061) can be within the range 17000 – 32767.
- Port ranges may not overlap with the ports of other OMM services. See section [12.6](#) for a list of all protocols and ports.
- If the OMM is running on a DECT base station, the ranges may not include ports used by other DECT base station protocols. See section 10.4 for a list of all ports and protocols.
- The port range for conference rooms is limited to 100 ports.
- The port range for users is limited to the following:
RFP OMM: Maximum 512 ports (1024 ports if OMM runs on RFP 4G).
Linux Server OMM: Maximum 10,000 ports.

2.18 UTF-8 ENCODING

The UTF-8 support allows the display of a wider range of language specific characters (e.g., umlauts) and facilitates localization for different markets. The OMM and the Mitel 600 DECT phone family support UTF-8 for text messaging.

In addition, the OMM and the Mitel 600 DECT phones support an extended character set for

- User parameters (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

For third-party GAP DECT phones, Mitel DECT 142 / Mitel 142d or Mitel 600 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 available set of characters is defined by the DECT phone. Please see /31/. User configuration files must be encoded in UTF-8.

2.19 ALPHANUMERIC DIALING

SIP-DECT supports the dialing of alphanumeric characters. This allows a user to dial names (e.g. “Heinrich.Mueller”) as well as digits.

If SIP URI dialing such as “name@domain” is used, you must use an (outbound) proxy that supports the interpretation of SIP user names, including domain names.

Please note: The “Digit treatment” feature handles dialed digit strings only. It cannot be applied with UTF-8/alphanumeric dialing.

2.20 VOICE MAIL NUMBER

You can configure a system-wide voice mail number. This number is used by the Mitel 600 DECT phone 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 DECT phone is used, the voice mail number must be configured locally on the DECT phone.

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, see the *SIP-DECT DECT Phone Sharing and Provisioning Guide*.

2.21 CALL HANDLING

SIP-DECT supports a number of features for enhanced call handling.

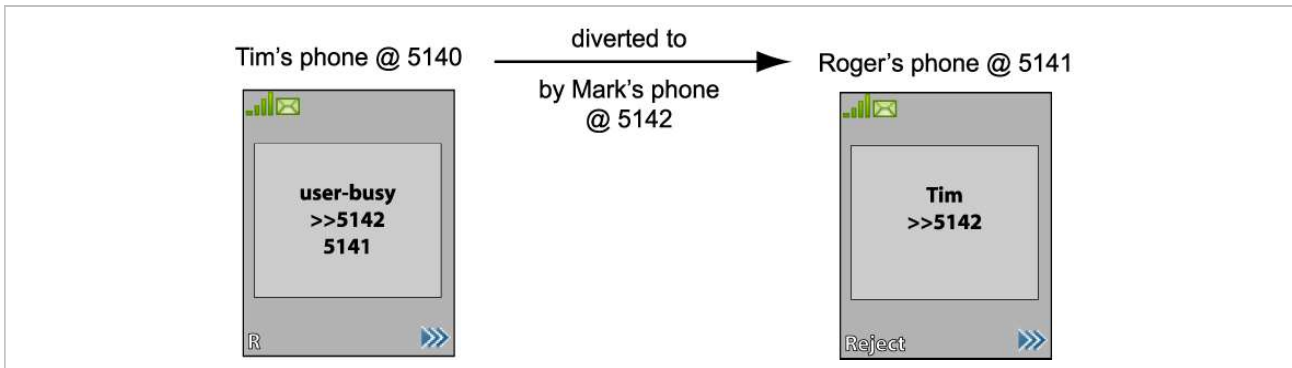
2.21.1 DIVERSION INDICATION

The OMM supports the displaying of diversion indications for Mitel 142d and Mitel 600 DECT phones based on the SIP Diversion Header defined in RFC 5806. This feature is only available with iPBXs generating such Diversion Headers.

When an outgoing call from a Mitel 142d / Mitel 600 phone is being diverted to another destination (i.e. via call forward), the phone displays the Caller ID (phone number and/or caller name) of the new destination and the reason for the call diversion (if delivered from IPBX). Similarly, at the new destination, the Caller ID of the original call destination is displayed.

Example:

- 1 Tim calls Mark at 5142.
- 2 Mark’s phone is busy and diverts the incoming call to Roger at 5141.
- 3 Tim’s phone displays the extensions where the call is being diverted to and the reason for diverting the call.
- 4 Roger’s phone starts ringing and displays the name and number of the phone the incoming call (Tim) and the original called destination (5142).



2.21.2 CALL COMPLETED ELSEWHERE

SIP-DECT supports the SIP “Reason” header field defined in RFC 3326. When SIP-DECT receives a CANCEL request including a “Reason” header field with “cause=200”, the incoming call will be marked as accepted in the local incoming call logs of the Mitel 600 and Mitel 142d phones.

2.21.3 SEMI-ATTENDED TRANSFER

The SIP message sequence for a “Semi-Attended Transfer” allows the transferor to start the transfer while the target phone is still ringing. SIP-DECT supports different behaviors for semi-attended transfers. This can be configured on the OMP SIP -> **Advanced settings** tab (see section 6.5.4.2).

The supported modes are:

Semi-attended transfer mode	Refer-to with replaces	Behavior
Blind	No	The semi-attended transfer is handled as a blind transfer. The phone sends CANCEL before REFER for semi-attended transfer.
Blind	Yes	The semi-attended transfer is handled as a blind transfer. The phone sends REFER with Replaces for semi-attended transfer and no CANCEL. This behavior is not SIP compliant but necessary for some iPBX platforms.
Attended	-	The semi-attended transfer is handled as an attended transfer. Both lines of the transferor remain active until the transfer succeeds. This behavior is compliant to RFC 5589.

Please note: The mode “Semi-attended transfer mode: Blind” with “Refer-to with replaces: yes” is not SIP compliant and should only be used on iPBX platforms that require that signaling.

2.21.4 THIRD LINE HANDLING FOR MITEL 142D AND 600 DECT PHONES

In earlier implementations of SIP-DECT user call control, a waiting call forces the user to react to that call (accept or reject), before he can use other supplementary services like call transfer, conference or inquiry call options.

In the new implementation, a third line is reserved for call waiting purposes. The waiting call is kept in the background, even if the receiving user decides to finish supplementary services first (see rule at the end of this subsection). It is also kept, if two lines are already used for brokering (in the former implementation, the incoming call was answered with busy state). After one of those lines is released, the waiting call can be accessed by the known means (by R-Key or the referring menu options).

Please note: The Third Line Handling is available for Mitel 142d and Mitel 600 DECT phones, but not for third party GAP phones.

Third Line Handling follows the existing MMI philosophy of the DECT phones. If the user wants to continue supplementary services when a call comes in:

- R-Key will accept the incoming call. All supplementary services will involve that incoming call directly or indirectly.
- Selecting “Transfer” or “Brokering” offers the possibility to keep the waiting call and continue supplementary services with the former line only. The waiting call is not involved but can be accepted later.

Please note: The Third Line Handling feature offers the option to receive a further incoming call only. A user cannot open a third line as the active part (e.g. to open a further third line for an inquiry call in a brokering situation, where two lines are already involved).

2.21.5 CALL TRANSFER ENHANCEMENTS FOR MITEL 142D DECT PHONES

The blind transfer has been slightly simplified. The second confirmation after selection of the transfer targets number by the “start” button is removed. So the steps are reduced to:

- Press I-Key within a basic call
- Select “Transfer”
- Select editor or phonebooks
- Edit or select destination and press “OK”

In earlier OMM releases (SIP-DECT 4.0 and earlier), call transfer had to be initiated via menu. Pressing the hook key led to the release of the active line and a callback menu popped up.

The OMM now allows the use of the hook key for call transfer, as it is already known from Mitel 600 DECT phones. To enable this feature, the administrator must enable the “Call Transfer by Hook” feature in the OMP **System -> SIP -> Supplementary Services** menu.

To initiate a transfer via the hook key, do the following:

- initiate an inquiry call and dial
- wait for completed connection (optional)
- press the hook key

You can still initiate a transfer via the menu.

If the “transfer by hook” capability is set, the release of the active line in brokering state must be done via the menu option “Release”:

- Press I-Key within an inquiry call or brokering state

- Select “Release”

2.22 TRUNCATING SIP USER NAME IN SIP URI

If user name info in SIP to-/from-/contact headers or p-asserted-identity is extended by a suffix, which is separated by a semicolon, this suffix is truncated before the username is printed to call displays or DECT phone internal call logs.

Example: If the DECT phone receives

Contact: "Dominique B." sip:5405;openSipsTestproxy@testlab.mitel.randd.com

only 5405 will be extracted as user name to be printed. The display name “Dominique B.” will also be shown, but the extension “openSipsTestproxy” will be removed.

To enable this feature, the administrator must set the “Truncate Caller Identification” parameter in the OMP **System -> SIP -> Supplementary Services** menu.

2.23 OM LOCATING APPLICATION

You can set up a system to locate and track DECT phones in your DECT system. This includes a separate Web user interface, which for example can be operated by service personnel to locate a DECT phone that has triggered an alarm. See the *OpenMobility Locating Application User Guide* for details (see /27/).

The OM Locating application can display small maps showing the placement of a DECT base station. In earlier SIP-DECT releases, these graphic maps had to be generated manually by using a graphic editing program.

The OM Management Portal (OMP) can be used to generate the graphic map images needed by the OM Locating application.

Images showing the floor plan of the buildings belonging to the OM system can be imported into the OMP. In a next step the RFPs of the SIP-DECT system can be placed on these images with drag and drop. Finally for each of the RFPs, the graphic map images will be generated in the format and size as required by the OM Locating application.

The process and the OMP functionality for this feature are described in detail in section [8.26](#).

2.24 EXTENDED MESSAGING

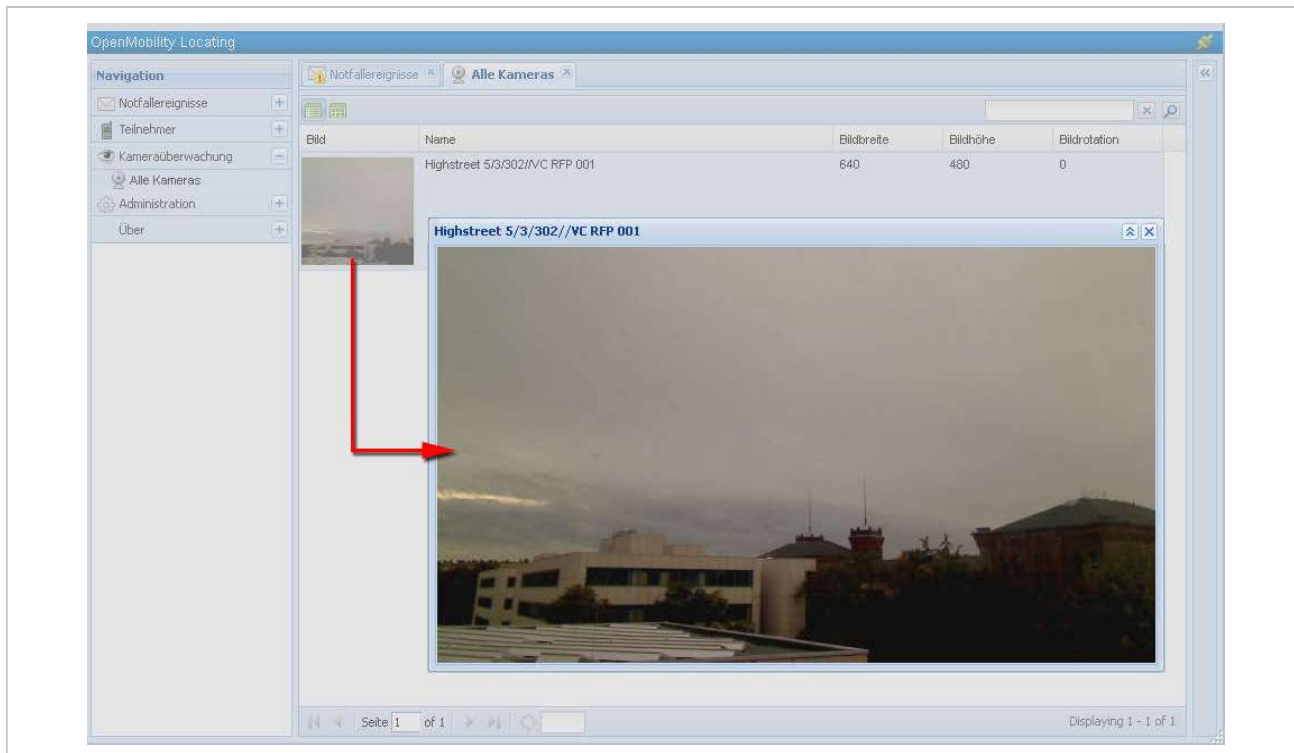
You can set up an extended messaging and alarms system (e.g. to provide automated reactions on alarms triggered by DECT phones or on alert messages). The extended messaging system may also provide message-based services, and may also be integrated with external computer systems. See the *OpenMobility Integrated Messaging & Alerting User Guide* for details.

2.25 VIDEO SUPPORT

The SIP-DECT solution supports snapshot images and video streaming via USB video devices connected to DECT base stations.

2.25.1 USB VIDEO DEVICES

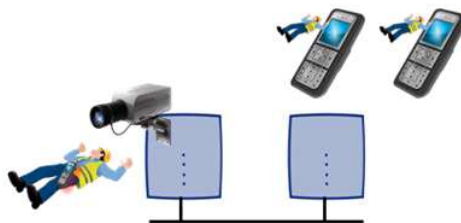
You can configure and use USB video devices that are fully supported by the UVC video class device driver. The USB video device is connected to the USB port of a SIP-DECT RFP 35. In conjunction with the “Surveillance” feature of the OM Locating application, the USB video devices generate snapshot images and video streams.



One USB camera (only the types Logitech HD Webcam C615 or Logitech HD Pro Webcam C920) can directly be connected to a SIP-DECT RFP 35/43. Such cameras are used as well with the OM Locating Application as with the Terminal Video feature. For a detailed description see section [8.27](#).

2.25.2 TERMINAL VIDEO

With SIP-DECT 5.0 and later, the Mitel 602 DECT phones support video streams from cameras connected to SIP-DECT base stations RFP 35/43. When a user has the video stream permission, he can choose in the system menu from a list of cameras to connect.



Video Streaming is only available when the DECT phone is connected to a 3rd or 4th generation RFP and the permission is set for the site and the DECT phone.

Video streams are treated like a call by the DECT phone, and require two (of eight) air channels on the RFP for each stream. The DECT phone can also perform handover between DECT base stations with an active video connection.

A video connection is automatically terminated by the system in case that any related capability (e.g. video stream permission) is changed.

The maximum number of simultaneous terminal video streams per camera is restricted to 10.

Connection and configuration of cameras is similar to the steps for the locating application. Special steps necessary for terminal video are:

- Enable all sites that have the technical capability (only 3rd or 4th generation RFPs) via OMP for terminal video.
- Enable the additional service “Video stream permission” via OMP (**DECT Phones -> Users**) for those users who are allowed to use this feature.

Please note: It is strongly recommended to set the radio fixed parts attributes building, floor and room, if you configure a huge system with a large number of cameras. This will ease the selection of cameras on the DECT phone menu.

A video camera must be configured in OMP before it can be offered to applications and the Mitel 602 DECT phones.

The selection of the menu “Cameras” is offered in the Mitel 602 DECT phone “System menu” (e.g. long press on Menu >>>), if

- at least one camera is plugged and activated by the enable flag
- the DECT phone user has the permission to select cameras
- the DECT phone is located within a site, which allows terminal video

Navigation within the camera menu will be done by OK (and ESC) keys. To establish a video stream, press “hook off” if the name of your camera is selected.

If the number of cameras exceeds the visible lines of the DECT phones display, the presentation is arranged hierarchically. In this case, at least one sublevel must be selected before camera names are offered. The hierarchy of the referenced DECT base station (site, building, etc) is inherited for that purpose.

The destination of a video call is added to the DECT phone internal redial list.

Please note: Audio calls or any system service activities are not possible during an established video link. Any kind of auto callback (initiated by a message or pushed by XML notification to direct dial) is not supported for video calls.

2.26 USER MONITORING

The OMM monitors the status of the user’s DECT phone to verify the user’s availability to receive calls or messages. By default, passive and active user monitoring is disabled.

In addition to the standard request, response and notification messages, the OMM generates alarm triggers if a user becomes unavailable. The alarm triggers can be consumed by the OM IMA, the OM Locating application, or another application using OM AXI. If a user becomes available again, the OMM sends an additional alarm trigger to indicate the change in status.

User status information is available via OM AXI and OMP.

For a detailed description of the “User monitoring” feature, see section [8.29](#).

2.27 CORPORATE DIRECTORY INTEGRATION

The SIP-DECT solution supports integration of up to five directory servers. The configured directories are displayed in a list on the Mitel 600 DECT phone when the user invokes the central directory function, and search by name to retrieve phone or mobile numbers (as well as email addresses for SIP-DECT messaging applications). Note that users can only access one directory at a time.

SIP-DECT supports LDAP and XML directories, and as of SIP-DECT 6.2, Broadsoft XSI-based directories are also supported. XML-based directory services can be implemented using the XML terminal interface.

The SIP user name and SIP authentication credentials can be used for directory access, or can be specified separately. If different from the SIP user name and authentication credentials, the user name and credentials must be explicitly configured for each user.

For configuration information see section 6.12.5.

2.28 INTEGRATION INTO EXTERNAL MANAGEMENT SYSTEMS

You can use the following features to integrate the SIP-DECT system into external management systems:

- Each DECT base station may run an SNMP agent that can be queried by SNMP management software (see [8.19](#)).
- To further integrate into external configuration management systems, the DECT system’s configuration is available by means of ASCII-based configuration files. You can configure automatic import of configuration files from an external server. For more information, see section [8.8](#).
- The OM AXI software application interface can also be used for integration into external systems. See the OM Application XML Interface (OM AXI) specification, see /31/.

2.29 SYSTEM CONFIGURATION TOOLS

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

- the Web-based OMM Web service (see section 5)
- the Java-based OM Management Portal (OMP, see section 6)

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 only available in the OMP application.

The following table lists the features and settings that are available in each configuration tool:

Feature	Web	OMP
---------	-----	-----

SNMP configuration	Yes	Yes
DB management: User data import	No	Yes
Configuration and start of a system dump	Yes	Yes
Download system dump to PC	No	Yes
Event information display (Event log)	Yes	Yes
WLAN profile configuration	Yes	Yes
Dynamic DECT phone subscriptions (OpenMobility provisioning)	No	Yes
Locating settings for DECT phone	No	Yes
Paging areas	No	Yes
Alarm Triggers	No	Yes
DECT base station sync. View	No	Yes
DECT base station statistics	No	Yes
DECT base station data export	No	Yes
Capturing unconfigured DECT base stations	Yes	Yes
Configuration of XML applications (SIP-DECT XML terminal interface)	Yes	Yes
Configuration of SIP backup servers	No	Yes
User monitoring	No	Yes

2.30 SIP ENHANCEMENTS

With SIP-DECT 6.0 and later, the SIP-DECT solution provides several enhancements to the SIP protocol implementation.

2.30.1 GLOBALLY ROUTABLE USER-AGENT URIS (GRUUS)

Globally Routable User-Agent URIs (GRUUs) provide a way for anyone on the Internet to route a call to a specific instance of a SIP User-Agent. IP-DECT provides GRUU support according to RFC 5627.

A “sip.instance” is added to all non-GRUU contacts. You can enable or disable this support via OMP or Web service (**System -> SIP -> Basic Settings**).

2.30.2 SESSION TIMER

SIP-DECT supports RFC4028 “Session Timers in the Session Initiation Protocol (SIP)” to keep call sessions alive and to determine whether established call sessions are still alive.

You can configure the session refresh period via OMP or Web service (**System -> SIP -> Advanced Settings**).

2.30.3 SIP CONTACT MATCHING

In special Network Address Translation (NAT) environments, the Contact URI in a SIP response to a REGISTER request may not match the URI originally sent out.

In such cases, SIP-DECT offers the “SIP contact matching” configuration parameter. You can enable this parameter via OMP or Web service (**System -> SIP -> Advanced Settings**).

2.30.4 CONFIGURABLE CALL REJECT STATE CODES

The SIP status codes for user-rejected calls and device-unreachable calls are configurable via OMP and Web service (**System -> SIP -> Advanced Settings**).

2.30.5 CALL RELEASE TIMERS

SIP-DECT 6.0 or later allows changing certain system default timers. These timers determine the DECT phone call behavior when calls are released by the B party.

You can configure the “Call release timeout”, “Hold call release timeout”, and “Failed call release timeout” parameters via OMP or Web service (**System -> SIP -> Supplementary Services**).

2.30.6 INCOMING CALL TIMEOUT

Incoming calls are automatically rejected when the user does not answer the call within 180 seconds. This time period is too short for special customer use cases.

You can configure this interval through the “Incoming call timeout” parameter through OMP or Web service (**System>SIP>Advanced Settings**).

2.30.7 CALL REJECT ON SILENT CHARGING

If the following 2 conditions are fulfilled, all Mitel 600 DECT phones reject incoming calls:

- If the flag “Call reject on silent charging” is set.
- If the phones are in charging mode and “silent charging” is activated in the phone.

If the flag is set by OMP or WEB service. The parameter is grouped under **System>SIP>Supplementary Services**.

2.30.8 ROUTE HEADER

In some special environments, SIP outbound proxies do not support SIP Route header.

For such cases, SIP-DECT offers the `Remove route` configuration parameter. If this parameter is enabled, SIP Route headers are not added to SIP messages sent to outbound proxies.

You can enable this parameter through OMP or through Web service (**System>SIP>Advanced Settings>General**).

2.30.9 MWI SUBSCRIPTION PERIOD

SIP-DECT supports MWI subscription based on /21/. The configuration parameter `Explicit MWI subscription period` enables configuring the requested duration in seconds, which is the interval at which SIP-DECT re-subscribes to MWI before the MWI subscription times out. You can enable this parameter through OMP or through Web service (**System>SIP>Advanced Settings>General**).

2.31 AUTO ANSWER, INTERCOM CALLS AND AUDIO SETTINGS

Certain call features force the DECT phone to call a specified SIP user automatically and, as an option, to establish a speech path immediately without any intervention by the DECT phone user.

SIP-DECT allows control of the following audio settings on the DECT phone to prevent unauthorized parties from hearing the call:

- Speech path can be initially set to be muted
- A warning tone may be generated

SIP-DECT also supports intercom calls. This means that the originating party can force the called party's phone to establish a speech path immediately. Control of the same audio settings applies.

2.31.1 INTERCOM CALLS

A DECT phone can be forced to answer an incoming SIP call automatically if certain information is included in the SIP header. A DECT phone user can also initiate an intercom call, which automatically triggers the destination to talk.

Intercom calls can interrupt active calls ("barge in"). If it is an established basic call, the active call is put on hold. In more complex call situations, a "barge in" always supercedes existing active calls, unless the active call is a "SOS" call.

The call is identified as an intercom call if the SIP INVITE header includes:

- a "Call-Info" header containing "answer-after=0"
- an "Alert-Info" header containing "info=alert-autoanswer"

Please note: This feature is only available for Mitel 600 DECT Phones, version 4.0 or higher.

2.31.1.1 Barge-in of incoming intercom call

If a "barge in" action on an existing call is necessary, note the following rules about the treatment of existing active calls:

- If the user is in a basic call (one line already active) or is brokering (two lines are used), the active line is placed on hold and kept in the background. No line is released.
- Incoming ringing calls which are not yet connected are converted to waiting calls.
- If a third line is open due to a waiting call, that call is released and the line is replaced by the intercom call.
- Outgoing calls that have not yet been answered and are in a dialing state, are released.
- If a call is on hold by the B party, the call is released. An on-hold by the B party is difficult to maintain while another line has an active audio stream.

Normally, the user should be able to resume the interrupted calls again when the intercom call is finished. However, the calls may fail if several maintained lines collide with call exceptions (e.g., a failed call transfer that was maintained in the background).

Please note: Barge-in is rejected if the DECT phone is part of a SOS/alarm call.

2.31.1.2 Outgoing intercom calls

A DECT phone can initiate an intercom call. The user must dial the configured access code, followed by the destination's user id / number.

If a DECT phone generates an intercom call, an Alert-Info header is added to the SIP INVITE:

- the "Alert-Info" header contains "<http://x>info=alert-autoanswer"

2.31.2 AUTO ANSWER AUDIO SETTINGS

You can configure global auto-answer settings through the OMM Web service or the OMP. Global settings are valid for all DECT phone users in the system, except users who have individual settings.

Incoming call settings:

- Auto answer allowed (default: true)
- Microphone mute (default: true)
- Warning tone (default: true). A short ringtone is played if there are no active calls. If there is an active call in a "barge in" situation, the ringing will be in-band.
- Allow barge in (default: true)

Outgoing call setting:

- Dial prefix (default: string is empty). Empty string means that an intercom call cannot be initiated by a DECT phone.

2.31.2.1 User-specific incoming call setting

You can set user-specific settings via OMP, but not the OMM Web Service. Default values for all parameters are inherited from global settings.

2.32 SIP-DECT XML TERMINAL INTERFACE

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

Partners can get access to the interface specification /37/ by registering for the A2P2 program.

To call a certain URI, there are a number of hooks available for the Mitel 600 DECT phones which can be put on a programmable key or can be called from a menu. You can activate the predefined XML hooks via the OMM Web service (see section 5.9.5) or the OMP (see section [6.12.8](#)).

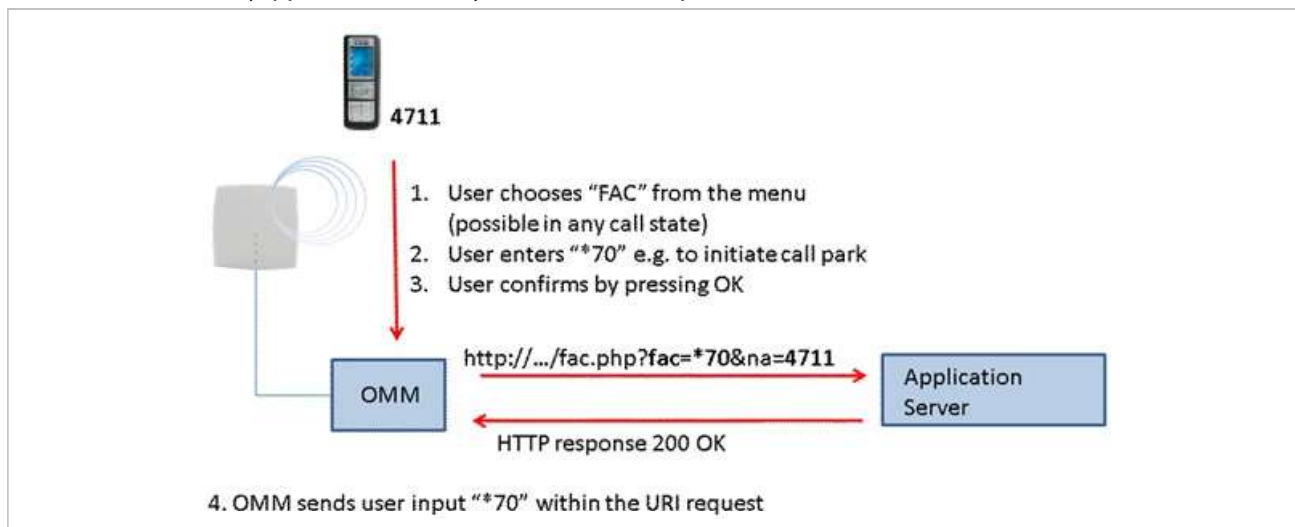
You can also activate the XML hooks through the Configuration over Air (CoA) feature, see section [8.23](#) for more information.

Please note: From SIP-DECT release 3.1 on, behavior for XML objects has been added or changed (see SIP-DECT XML terminal interface specifications for more details).

2.32.1 FEATURE ACCESS CODES TRANSLATION

Many PBXs allow the control of PBX supplementary services by dialing specific numbers called feature access codes (FAC). SIP-DECT supports the "Feature Access Codes Translation" XML application to avoid conflicts between SIP-DECT feature access codes or digit treatment rules and PBX feature access codes. If "Feature Access Codes Translation" is activated, SIP-DECT users can chose "FAC" menu on

the Mitel 600 or Mitel 142d DECT phones in any call state and enter the feature code en-bloc. The input is sent to the PBX (Application server) within a URI request.



This feature can be configured using OMP on the **XML applications** page (see section [6.12.8](#)).

2.32.2 RING TONE SELECTION FOR (ALARM) MESSAGES

This feature extends the capability to set ringer tones to provide an acoustic signal to the receiver of a message and is related to messaging configuration and management function described in the *OM Application XML Interface Specification*.

In previous SIP-DECT releases, the "melody" field offered ten tones, selected by an identifier. In the current release, the "explicitToneSelection" field allows the user to select a tone, which does not have to belong to the set of "melody" tones, by the name string. If both are set, the explicitToneSelection value takes precedence.

IMPORTANT : Depending on the DECT phone, not all strings may work. The string value is not checked for correctness. Invalid or unknown string values are ignored.

Please note: The OM Message & Alerting License is required to use these features.

2.33 SOFTWARE UPDATE DISPERSION

SIP-DECT supports following 2 features to control and manage the update process in SIP-DECT system:

- Time-controlled Daily automatic reload of configuration and firmware files
- Time-controlled RFP software update

A new configuration parameter `Maximum delay` allows a randomly spread over the given delay, when a reload or an update starts. The additional new configuration parameter `Autonomous SW update check by OMM` allows to disable the default behaviour of the RFP-OMMs to check for a new software image, whenever a RFP re-configuration (DHCP renew, OM Configurator, `ipdect.cfg`, `<MAC>.cfg`) happens.

3 LICENSING

3.1 LICENSING MODEL

Licenses are required based on the SIP-DECT system size and feature set. Licensed features include:

- the number of configured DECT base stations
- the Messaging application
- the Locating application

For information on the messaging and locating applications see the appropriate documents listed in the References section (section 10.8).

Note: A license to upgrade the SIP-DECT software to a SIP-DECT 6.0 or later is no longer required.

The **License settings** page in the OMM Web Service provides a summary of the SIP-DECT licenses installed.

License settings	
Status	Installation ID: 270943175
System	License file import: <input type="button" value="Choose file"/> No file chosen <input type="button" value="Import"/>
Base Stations	
DECT Phones	
WLAN	
Licenses	
Info	
General	
Status	<input checked="" type="checkbox"/>
License type	Standard license
Grace period	720:00 <input type="text"/>
PARK	1F102643C7 (31100462074346)
MAC address 1	00:30:42:18:1D:BD <input checked="" type="checkbox"/>
MAC address 2	-
MAC address 3	-
System	
Number of DECT base stations	256 <input type="text"/> <i>Mitel SIP-DECT System License XXX</i>
License key	U3TUK-74SBC-W5FGR-2E243-38SDM
Messaging	
Receiving text messages (Emergency, Locating alert) and enhanced messaging features	<input checked="" type="checkbox"/> <i>Mitel SIP-DECT Messaging & Alerting License Enterprise</i>
License key	TNC3K-DX1ZK-T4MUM-XERW6-WDM83
Locating	
Number of users allowed to be located	10000 <input type="text"/> <i>Mitel SIP-DECT Locating User License XXX</i>
OM Locating application	<input checked="" type="checkbox"/> <i>Mitel SIP-DECT Locating Server License</i>
License key	PZMVX-HTTPK-RH9GR-CM2L3-UUG7B

3.1.1 SYSTEM LICENSES

To properly address small, medium and large installations, the SIP-DECT offering is split into the following categories, according to system size.

Note: As of SIP-DECT 6.0, no distinction is made between DECT base station brands. License and feature rules apply equally to all DECT base station types (standard RFP, L-RFP). Only the DECT base station hardware determines available functionality.

Small systems – 1 .. 5 DECT base stations

- No license required
- Telephony and basic messaging only
- No locating or enhanced messaging functionality
- PARK code for up to 256 DECT base stations required for operation (provided by the online PARK service)

Note: Existing SIP-DECT systems with up to five L-RFPs are automatically migrated to the integrated license model. Larger systems still require a valid license file.

Medium systems – up to 256 DECT base stations (minimum 3 DECT base stations)

- OM System License required for the number of DECT base stations (10, 20, 50, 100, etc)
- Licenses for Messaging and Locating can be added
- PARK code for 256 DECT base stations included in license file

Large systems – up to 4,096 DECT base stations

- OM System License required for the number of DECT base stations
- OpenMobility Manager (core software) resides on one or two Linux-based PCs
- Licenses for Enhanced Messaging and Locating can be added
- PARK code for 4096 DECT base stations included

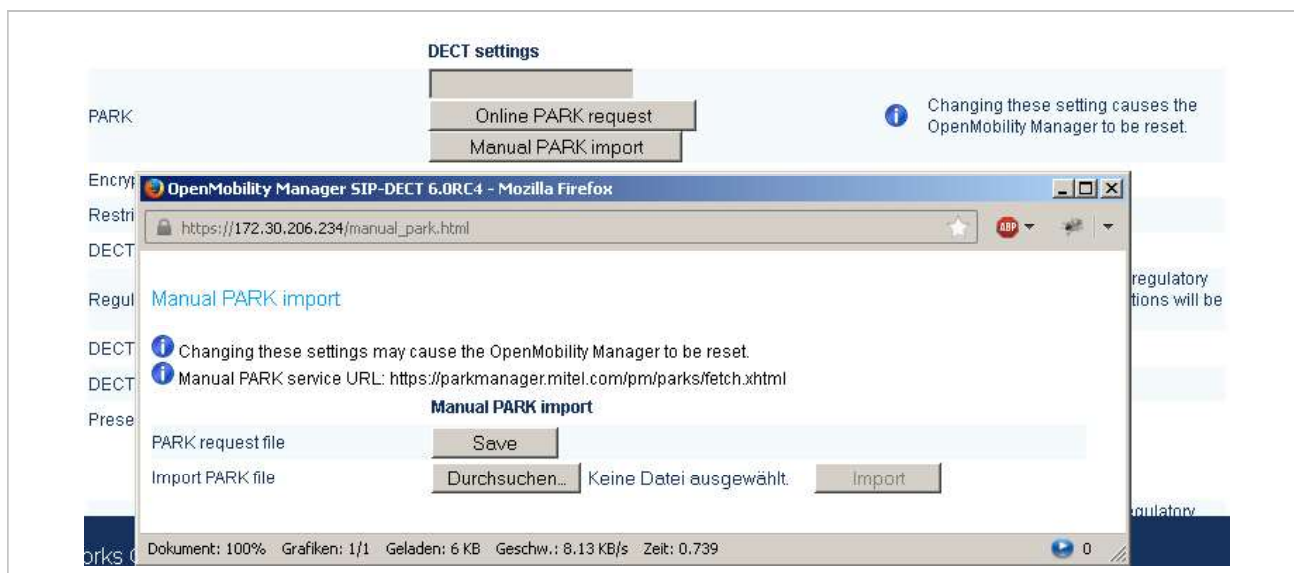
Note: With SIP-DECT Release 6.0 or later, there is no longer a demonstration mode for the OMM.

3.1.2 ABOUT G.729 CHANNELS

With SIP-DECT Release 6.0 or later, the number of G.729 channels is no longer limited to a specific fixed number or license. The number of G.729 channels depends only on the resources available (i.e., DECT base station capacity and number of base stations).

3.1.3 PARK SERVICE

A Portable Access Rights Key (PARK) is required to operate a SIP-DECT system with up to five DECT base stations. (For systems with more than five DECT base stations, the generated license file contains the PARK code). With SIP-DECT 6.0 or later, the PARK code is provided via a centralized Web service; you do not need to enter the code manually (as in earlier SIP-DECT releases). A PARK for up to 256 DECT base stations is available upon request from the OMM Web service.



You must have an internet connection to access the online PArk service. If no internet connection is available, you can download a PArk request file from the OMM (PArk service URL is <https://parkmanager.mitel.com/pm/parks/fetch.xhtml>) and upload it to the PArk server from a computer that is connected to the Internet. You can then import the file into the OMM.

If you have a valid license file that includes a PArk, this mechanism is not necessary.

3.1.4 UPGRADE LICENSE

With SIP-DECT Release 6.0 or later, you do not require a license to upgrade to a newer release.

Older systems with an OM Activation License for L-RFPs (3..20 RFP-L) require a license upgrade, which is available from the License server at no cost. Note that you must already have three MAC addresses registered on the license server for the license upgrade.

3.1.5 GRACE PERIOD

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

Three DECT base stations guarantee redundancy when a hardware or network error occurs. An odd number of DECT base stations prevents system duplication by splitting the system into two separate parts.

When the first validation DECT base station is disconnected, the OMM generates a warning and displays the message on the **Status** page of the OM Web service (see also section 5.3).

If the second validation DECT base station is disconnected, the OMM treats it as a license violation, and starts the timer on a 30-day grace period. When the timer expires, the OMM restricts all licensed features.

When the validation DECT base stations are reconnected to the OMM, the grace period is incremented until it reaches its maximum of 30 days.

3.1.6 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 DECT base stations exceeds the licensed number
 - the messaging application limits the type of messages to “info”, “low”, “normal” and “high”
 - the locating feature is stopped
- For SIP-DECT 5.0 (or older) systems, the software version in the license file does not match the software version running on the OMM.
- The OMM has no connection to at least two of the validation DECT base stations and the grace period has expired.

The restrictions above are in place until at least two validation DECT base stations are reconnected to the OMM.

3.2 UPLOADING A LICENSE FILE

A license file must be generated on the Mitel license server. The license confirmation provided when you order your system contains detailed information on how to generate the license file. The file can be uploaded into the OMM either via Web service (see section 5.10) or via the OMP (see section 6.13).

A license file contains a PARK for system identification. If the newly imported PARK differs from the current PARK, the OMM performs a restart. In this case, all existing DECT phone subscriptions will be deleted.

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

The license file includes an installation ID. This ID prevents the administrator from loading the wrong license file with a different PARK (resulting in all DECT phones being unsubscribed). The download page for the license file displays the installation ID. If no Installation ID is configured (value 0, which is the default), the ID is automatically set while loading the license file. If the ID does not fit to the license file, the license file import will fail. The installation ID does not change when you load a new license file from the license server, unless the PARK has changed.

The screenshot displays the 'License file' tab in the OMM web interface. At the top, there are navigation tabs: 'Status', 'License file', 'System', 'Messaging', and 'Locating'. Below these, the 'Server' section is visible, containing a 'General' sub-section with an 'Installation ID' field set to '270943175'. There are 'OK' and 'Cancel' buttons below this field. The 'License file import' section is also visible, featuring a 'File' button with a document icon, a text input field, and an 'Import' button. A small information icon (i) is next to the 'Import' button, with a note: 'Importing a license file may cause the OpenMobility Manager to be reset.'

The SIP-DECT license file format prepares the system for receiving licenses from Mitel PBXs or to act as a license key server for other Mitel products in future releases.

Please note: New license files (as of SIP-DECT 5.0) are not compatible with previous versions of SIP-DECT systems (SIP –DECT 2.1 – 4.0).

3.3 LICENSE MODELS

3.3.1 SMALL SYSTEM (UNLICENSED)

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 small system features:

- up to five DECT base stations
 - standard telephony
 - sending messages from DECT phones for all users
 - no locating
- Messaging features are generally restricted to type “Info”, “Low”, “Normal” and “High” for all users (no “Emergency” and no “Locating Alert”).

When there are more than five DECT base stations configured, only the first five base stations stay in the configuration database. All other base stations are dropped silently.

3.3.2 MEDIUM OR LARGE SYSTEM

When the PARK is set through the upload of a license file, the OMM enters the licensed state. In this state the OMM uses the following license features coded into the license file.

- System license (Medium):
 - Three and up to 256 base stations
- System license (Large):
 - Three and up to 4096 base stations
 - Software version of the OMM allowed to be executed
 - Messaging license:
 - Whether clients are allowed to receive alarm messages or have enhanced messaging options
- Locating license:
 - Number of locatable DECT phones
 - Whether the locating application is allowed to execute

When you generate a license file from the license server, you must enter the MAC address of three base stations. These three validation base stations are used to operate the grace period as described in section [3.1.5](#).

When obtaining the license file from the 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 DECT phones.

Note: As of SIP-DECT 6.0, the PARK can no longer be changed manually on the **System settings** page of the OM Web service.

4 GETTING STARTED

The following example describes the steps required for a minimal SIP-DECT configuration.

4.1 BASE STATION STARTUP CONFIGURATION

Start up information for each DECT base station needs to be provided by DHCP or OM Configurator. To use DHCP, specific vendor options must be configured in the DHCP Server for SIP-DECT (see section [8.5.4.1](#)).

In this example, the OM Configurator is used to provide a static IP Configuration to the RFPs.

- 1 Connect the DECT base station(s) to your LAN and power up the units.
- 2 Open the OM Configurator and select your network interface via the **General** -> **Options** menu.
- 3 Click **Scan** to find the base stations connected to your LAN (enter user name and password: "omm" / "omm" for initial configuration until start-up)
- 4 Select a base station entry and double-click for configuration.
- 5 Enter the configuration parameters for the base station. For configuration details, see section [8.7](#).
- 6 Click **OK** when you have entered configuration parameters.
- 7 Click **Send Configuration** to apply the configuration to the DECT base station.
- 8 To configure the next unit, select another base station entry from the table, set the appropriate parameters (and confirm with **OK**), and click **Send Configuration**.

Note: The OM Configurator requires the Java Runtime Environment version 1.7 or higher.

4.2 SYSTEM CONFIGURATION

As soon as the OMM starts up, open a browser and connect (https://<IP_address>). Login with the user: omm and password: omm for the initial configuration.

The OMM forces you to change the login, which then also applies to the OM Configurator.

The OMM Web service provides basic parameters to setup the system, which is sufficient for this example scenario. To configure the OMM in detail, use the OM Management Portal (OMP). This application requires a current Java 1.7 to run and supports detailed OMM configuration and monitoring. The OMM Web service provides a link to run the OMP application via Java Web start.

4.3 SYSTEM SETTINGS

The OMM System settings menu provides the basic settings to operate the SIP-DECT system.

General settings	
System name	Customer
Remote access	<input checked="" type="checkbox"/>
Tone scheme	US ▼
DECT settings	
PARK	1F102643C7
DECT power limit 100mW	<input type="checkbox"/>
Encryption	<input type="checkbox"/>
Restrict subscription duration	<input type="checkbox"/>
DECT monitor	<input type="checkbox"/>
Regulatory domain	US (FCC/IC) ▼
DECT authentication code	2222
DECT phone user login type	Number ▼
Preserve user device relation at DB restore	<input type="checkbox"/>
Voice mail	
Voice mail number	25711

System name: Customer Name

Remote access: Allow SSH access

Tone Scheme: Scheme to simulate call control tones (country-dependent).

PARK: The system needs a PARK code to operate. Use the Online PARK service to obtain a PARK code (see section [3.1.3](#)) (five or more RFP systems).

Regulatory domain: DECT regulatory domain applicable to your local region.

DECT authentication code: Define as template for the subscription of new DECT phones.

Voice mail number: Your system voicemail number. A Mitel 600 phone will then offer the voice box in the Handset menu.


4.4 BASE STATIONS

Configure all base stations (formerly referred to as Radio Fixed Parts) from the **Base Stations** menu (including the OMM DECT base stations).

When you click on the **Start** button below the “Capturing unconfigured DECT base stations” caption, the OMM lists all DECT base stations trying to connect.

Click on **New** to configure a new base station.

New base station

 Please configure a WLAN profile of proper type.





General settings	
MAC address	<input type="text"/>
Name	<input type="text"/>
Site	1 ▼
DECT settings	
DECT Cluster	1
Preferred synchronization source	<input type="checkbox"/>
Reflective environment	<input type="checkbox"/>
WLAN settings	
WLAN profile	1 ▼
802.11 channel	▼
Output power level	Full ▼

OK Cancel

The base station configuration requires:

- base station MAC address
- Name e.g. location
- Site (default: 1)
- DECT active
- DECT cluster (default: 1)

The Status for each DECT base station is shown in the **Base Stations** section.

- **Active:** DECT Radio State (Active , Searching , Off , disabled  / -)
- **Connected:** DECT base station is connected to the OMM, DECT base station must be configured first.

4.5 SIP SETTINGS

Configure the SIP connection to the call server that the OMM must connect to in the OMM **System** -> **SIP** menu. Make sure the **Advanced** checkbox in the top bar is enabled.

The SIP user account (SIP-ID, Auth, and password) configuration is part of the DECT Phones configuration.

The default SIP signaling port for SIP-DECT is 5060 / UDP. Change if this is required by the SIP Server.

SIP

OK Cancel

Basic settings	
Proxy server	10.37.44.99
Proxy port	5060
Registrar server	10.37.44.99
Registrar port	5060
Registration period	300 sec
Globally Routable User-Agent URL	<input checked="" type="checkbox"/>
Outbound proxy server	
Outbound proxy port	5060
Transport protocol	UDP
Local UDP/TCP port range	5060 - 5060
Local TLS port range	5061 - 5061

Enter values for the following:

- **Proxy Server:** PBX IP or DNS Name
- **Proxy Port:** 5060
- **Registration Server:** PBX IP or DNS Name
- **Registration Port:** 5060

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	10 msec
Silence suppression	<input type="checkbox"/>
Receiver precedence on codec negotiation	<input type="checkbox"/>
Eliminate comfort noise packets	<input type="checkbox"/>
Single codec reply in SDP	<input type="checkbox"/>

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

Use the default RTP settings unless your installation requires a different configuration.

Use the default DTMF settings unless your installation requires a different configuration.

4.6 DECT PHONES

SIP-DECT allows multiple configuration and provisioning methods for DECT phones. In this example we use fixed DECT phones. A SIP-extension must be configured for each DECT phone (user) on the SIP call server.

To add a new DECT phone, go to the **DECT Phones** menu (ensure the **Advanced** option in the top bar is enabled) and click **New**.

New DECT phone

General settings	
Display name	<input type="text"/>
Number/SIP user name	<input type="text"/>
IPEI	<input type="text"/>
DECT authentication code	<input type="text" value="2222"/>
Login/Additional ID	<input type="text"/>
SOS number	<input type="text"/>
ManDown number	<input type="text"/>
Voice mail number	<input type="text"/>
Number used for visibility checks	<input type="checkbox"/>
SIP authentication	
Authentication user name	<input type="text"/>
Password	<input type="text"/>
Password confirmation	<input type="text"/>

OK Cancel

Subscription with configured IPEIs

Start

Wildcard subscription

2 min ▼

Start

Enter values for the following:

Display name: Extension Name

Number/SIP user name: SIP-ID e.g. terminal phone number

IPEI: Handset hardware identifier (optional)

DECT authentication code: Code for Handset subscription. If this field is left empty, the system-wide DECT authentication code is used (see section [4.3](#)).

Authentication user name: SIP user name

Password: SIP Extension password

To subscribe new DECT phones, subscriptions must be permitted by the OMM.

Use **Wildcard subscription** if no IPEI is set.

To subscribe new Mitel 600 DECT phones, open the DECT phone **System > Subscriptions** menu. Select **New system** and enter the Authentication code provided in your System Settings (e.g. 123456). The DECT phone prompts you to enter a PARK or to proceed with the subscription without a PARK. Set the PARK if several DECT systems are around, otherwise the DECT phone tries to subscribe to the first available DECT system.

4.6.1 DECT PHONE AND SIP STATE VERIFICATION

You can check the DECT phone state and SIP registration status from the **DECT Phones** page.

Click on the magnifying glass icon beside the entry for the DECT phone you just created to view details on the SIP registration status.

User/device status & configuration

User status:

Registered:	Yes
Registrar server type:	Primary
Registrar server:	10.37.44.99
Registrar port:	5060
Calculated local port:	5060
Silent charging:	No
CoA data loaded:	No

User configuration data:

User ID:	2
User rel. type:	Fixed
Name:	x25053 622d
Number:	25053
Description 1:	
Description 2:	
User lang.:	English
SOS number:	
MD number:	
VM number:	
SIP auth. user name:	25053
SIP auth. password:	*****
Fixed local port:	

Login/Add ID:

PIN:	*****
External:	No
VIP:	Yes
Visibility checks:	No
Sending messages:	No
Sending vCards:	No
Receiving vCards:	No
Video stream perm.:	No

Switch the DECT phone off / on to force SIP user registrations.

5 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.

5.1 LOGIN

The OMM allows more than one user at a time to configure the system. A user must authenticate with a user name and a password. Both strings are 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 to a new SIP-DECT software version, the user must accept the End User License Agreement (EULA) (see section 5.11).

If the default built-in user account is active, the administrator must change the default account data (passwords) of the “Full access” and “root” account. The meaning of the different account types is described in section [8.17.1](#).

Please note: The OMM forces a change to 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 (with the **Advanced** option enabled in the top bar):

- **Status** menu: Displays the system status (see section 5.3).
- **System** menu: Allows configuration of general SIP-DECT system parameters (see section 5.4).
- **Sites** menu: Allows grouping of DECT base stations into different sites (see section 5.5).
- **Base Stations** menu: Allows configuration and administration of the attached base stations (see section 5.6).
- **DECT Phones** menu: Allows administration of the DECT phones (see section 5.7).
- **WLAN** menu: Allows configuration of WLAN parameters (see section 5.8).

- **System Features** menu: Allows administration of system features like digit treatment and directory (see section 5.9).
- **Licenses** menu: Allows administration of licenses (see section 5.10).
- **Info** menu: Displays the End User License Agreement (EULA) (see section 5.11).

5.2 LOGOUT

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



5.3 “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.

Status	General
System	OpenMobility Manager SIP-DECT 6.0RC4 Build 2
Sites	Uptime 20:32
Base Stations	Licenses ✔
DECT Phones	Grace period 720:00 <div style="width: 100%; height: 10px; background-color: green;"></div>
WLAN	Standby OMM ✔
System Features	IP address 10.37.18.31
Licenses	Number used for visibility checks 26052
Info	OM Integrated Messaging & Alerting service ✔
	Base Stations
	Total number 12
	Connected 2 <div style="width: 16.6%; height: 10px; background-color: blue;"></div>
	DECT activated 12
	DECT currently active 2 <div style="width: 16.6%; height: 10px; background-color: blue;"></div>
	DECT clusters 2
	WLAN activated 0
	DECT Phones
	Total number 84
	Subscribed 4 <div style="width: 4.76%; height: 10px; background-color: blue;"></div>
	Subscription allowed ✘
	Activate firmware update ✔
	Loading firmware from: ftp://10.37.18.35/600.dnid
	Firmware version [600: 5.00.SP5.RC1] - [600,602: 6.0.RC8]
	Number of known downloadable DECT phones 4

5.4 “SYSTEM” MENU

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

5.4.1 “SYSTEM SETTINGS” MENU

The System settings cover global settings for the OpenMobility Manager. You can perform the following tasks from the System Settings menu:

- configure global settings (see the following sub-sections)
- restart the OMM (see section [5.4.1.17](#))
- update the OMM (see section [5.4.1.18](#))

The following sections describe the parameters that can be set.

Note: The following information describes all parameters visible when the **Advanced** option (in the top bar) is enabled.

5.4.1.1 General settings

- **System Name:** Enter the system name.
- **Remote Access:** Switches on/off the SSH access to all DECT base stations of the DECT system. For more information on the SSH access see section [9.3.5](#).
- **Tone scheme:** Select the country in which the OMM resides. This enables country specific tones (busy tone, dial tone, etc).

5.4.1.2 DECT settings

- **PARK:** This setting depends on the licensing mode. Small systems: Enter the PARK code obtained from the PARK service (see section [3.1.3](#)). License file: Shows the PARK included in the license file.
- **DECT power limit 100mW:** Limits the DECT base station transmit power to 100mW, independent of the selected regulatory domain. Enable for SIP-DECT installations that are mobile (e.g., on cruise liners that travel between countries). See section [2.12](#) for more information on this feature.
- **Encryption:** Activate this option if you want to enable DECT encryption for the whole system.

Please note: Make sure that all deployed third party DECT phones support DECT encryption. If not, encryption can be disabled per DECT phone (see 6.10.4).

- **Restrict subscription duration:** Activate this option if you want to restrict the duration for DECT phone subscriptions to 2 minutes after subscription activation. This option is not useful in case that you want to subscribe more than one DECT phone at a time or together with auto-create on subscription. It should be activated exclusively in case that there is a special need.
- **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/DECT base station. After a reset, the DECT monitor flag is ever disabled.
- **Regulatory domain:** Specifies where the IP DECT is used. Supported regulatory domains are:
 - EMEA
 - US (FCC/IC)
 - Brazil
 - Taiwan
 - South America (Radio 1910-1927Mhz 250mW)

Note that 3rd and 4th generation DECT base stations support different DECT frequencies. These devices can operate in different regulatory domains provided that the **Regulatory domain** setting is configured accordingly.

For older 2nd generation DECT base stations, there are different DECT base station models to meet different regulatory domain demands. To setup a North American FCC compliant DECT base station, the value must be set to **US (FCC/IC)**. In a North American US (FCC/IC) deployment, ETSI compliant DECT base stations are made inactive and cannot be activated if the regulatory domain is set to **US (FCC/IC)**. The reverse is also true.

WARNING: Note that selecting the incorrect regulatory domain may result in a violation of applicable laws in your country.

Note: Whenever you modify the regulatory domain, a warning is displayed. You must confirm it first to apply the changed setting.

- **DECT authentication code:** The authentication code is used during initial DECT phone subscription as a security option. A code entered here provides a system-wide DECT authentication code for each DECT phone subscription. Alternatively, a DECT phone-specific authentication code can be set (see section 5.7.1).
- **DECT phone user login type:** Specifies the system-wide variant for DECT phone login method. Two kinds of login types are supported: 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.

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

In case, the OMM works within a system along with MOM or UDS, this will happen in all OMMs of this system.

- **Preserve user device relation at DB restore:** Enables the preservation of the user – DECT phone association with an OMM database restore. This option is only applicable for database snapshots from SIP-DECT 6.0 or later.

Note: If you want to restore the association, enable this option BEFORE uploading a database for an OMM restore. The current OMM value is used, not the setting in the database being uploaded.

5.4.1.3 WLAN settings

This setting applies to RFP 42/43/48 WLAN base stations.

- **Regulatory domain:** Select 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 see the sections 5.8 and [8.18](#).

WARNING: Please note that selecting the incorrect regulatory domain may result in a violation of applicable law in your country!

Note: Whenever you modify the regulatory domain, a warning is displayed. You must confirm it first to apply the changed setting.

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

5.4.1.4 DECT base stations update

- **Mode:** DECT base station update mode – “One by one” (every single DECT base stations is updated separately) or “All at once” (all DECT base stations are updated in one step).

- **Trigger:** When this option is selected, the DECT base station update is time-controlled.
- **Time:** Time for time controlled updates.

5.4.1.5 Maximum delay

This parameter specifies the maximum time (in minutes) and the OMM waits past the schedule time before starting the update process.

5.4.1.6 Calculated time of delay

The calculated time for scheduled update (24h time format). This parameter is read-only and is calculated by the OMM based on given “Time of Day” and “Maximum Delay”.

5.4.1.7 OMP web start

- **Configure specific source:** Enables the specific URL to an external file server for retrieving the OMP jar file.
- **Protocol:** Specifies the protocol used to retrieve the OMP file.
- **Server:** Specifies the IP address or name of the external file server.
- **Port:** Specifies the port of the external file server.
- **Path:** Specifies the location of the OMP jar file on the external file server.

5.4.1.8 DECT phone’s firmware update

With SIP-DECT 6.0 or later, the DECT base station software images (iprfp3G.dnld and iprfp4G.dnld) contains the Mitel 600 DECT phone software. For specific maintenance purposes only, you can configure a URL to use an alternative DECT phone software image. The Mitel 600 DECT phone firmware packages are delivered in the “600.dnld” file for the OMM running on a DECT base station.

- **Activate firmware update:** Enables or disables the “Download over Air” feature. The OMM provides a DECT phone firmware update over the air when this feature is activated. For more information on, see section [8.22](#).
- **Configure specific source:** Enables the specific URL to an external file server for retrieving the DECT phone firmware file.
- **Protocol:** Specifies the protocol used to retrieve the firmware file from the external server.
- **Server:** Specifies the IP address or name of the external file server.
- **Port:** Specifies the port of the external file server.
- **User name:** Specifies the user name to authenticate on the external file server.
- **Password:** Specifies the password to authenticate on the external file server.
- **Password confirmation:** Confirms the password to authenticate on the external file server.
- **Path:** Specifies the location of the firmware file on the external file server.

- **Use common certificate configuration:** Enables the use of the system-wide certificate validation settings for this URL, as configured on the **System -> Provisioning -> Certificates page** (see section 5.4.2).

5.4.1.9 Voice mail

- **Voice mail number:** Specifies a system-wide voice mail number. This number is used by the Mitel 600 DECT phone family if the voice box is called.

5.4.1.10 OM Integrated Messaging & Alerting service

The OpenMobility Manager provides an integrated message and alarm service. The Internal message routing (DECT phone <> DECT phone) can be activated/deactivated. For a detailed description, see /28/.

- **Internal message routing (phone <> phone):** Enables or disables internal messaging between DECT phones.
- **Configure specific destination:** Enables the specific URL to an external file server for retrieving the IMA configuration file.
- **Protocol:** Specifies the protocol used to retrieve the IMA configuration file from the external server.
- **Server:** Specifies the IP address or name of the external file server.
- **Port:** Specifies the port of the external file server.
- **User name:** Specifies the user name to authenticate on the external file server.
- **Password:** Specifies the password to authenticate on the external file server.
- **Password confirmation:** Confirms the password to authenticate on the external file server.
- **Path & filename:** Specifies the location and file name of the IMA configuration file on the external file server.
- **Use common certificate configuration:** Enables the use of the system-wide certificate validation settings for this URL, as configured on the System -> Provisioning -> Certificates page (see section 5.4.2).

5.4.1.11 Syslog

The OMM and the DECT base stations are capable of propagating syslog messages.

- **Active:** Enables or disables collection of syslog messages.
- **IP address:** Address of the host that should collect the syslog messages.
- **Port:** Port of the host that should collect the syslog messages.
- **Forward OMM Messages to syslog:** (Visible only on a PC-hosted OMM system) Enables/disables forwarding of syslog messages from the PC-hosted OMM.

5.4.1.12 Software update URL

With SIP-DECT 6.0 or later, DECT base stations in small SIP-DECT systems (~10 RFPs) can obtain their software image from the DECT base station hosting the OMM, if they have no valid URL from which to load their software (see section [8.9.3](#) for information on URL syntax). If the OMM is running on a DECT base station, the OMM DECT base station delivers the software to the connected DECT base stations.

The new software image for the OMM DECT base station can be provided as an iprpf3G.dnld and iprpf4G.dnld file on an external file server. You configure the URL for the software image in this section.

- **Configure specific source:** Enables the specific URL for downloading the iprpf3G.dnld file (as opposed to the ConfigURL, which points to an external file server for all configuration and resource files).
- **Protocol:** Specifies the protocol used to fetch the software image file.
- **Port:** Specifies the port of the external file server.
- **Server:** Specifies the IP address or name of the external file server.
- **User name:** Specifies the user name to authenticate on the external file server.
- **Password:** Specifies the password to authenticate on the external file server.
- **Password confirmation:** Confirms the password to authenticate on the external file server.
- **Path:** Specifies the location of the software image file on the external file server.
- **Use common certificate configuration:** Enables the use of the system-wide certificate validation settings for this URL, as configured on the **System -> Provisioning -> Certificates page** (see section 5.4.2).

5.4.1.13 System dump

A system dump is a file that holds information about the OpenMobility Manager and all connected DECT base stations. With the Remote System Dump feature, a system dump is transferred to a remote server. You can configure a specific destination, otherwise the system ConfigURL is used. The system dump is generated manually by pressing the **Dump** button or automatically at the specified time.

Please ensure that the fileserver used allows writing or creation of system dumps.

- **Trigger:** Enables the automatic generation of a system dump time every day at the time specified in the **Time** field.
- **Time:** The time of day the system automatically generates a system dump file (only activated if the **Trigger** checkbox is enabled).
- **Dump:** Immediately triggers the generation of a system dump file.
- **Configure specific source:** Enables the specific URL for transferring the system dump file (as opposed to the ConfigURL, which points to an external file server for all configuration and resource files).
- **Protocol:** Specifies the protocol used to transfer the system dump file.
- **Port:** Specifies the port of the external file server.
- **Server:** Specifies the IP address or name of the external file server.
- **User name:** Specifies the user name to authenticate on the external file server.

- **Password:** Specifies the password to authenticate on the external file server.
- **Password confirmation:** Confirms the password to authenticate on the external file server.
- **Path:** Specifies where the system dump file is stored on the external file server.
- **Use common certificate configuration:** Enables the use of the system-wide certificate validation settings for this URL, as configured on the **System -> Provisioning -> Certificates page** (see section 5.4.2).

5.4.1.14 Core dump URL

Fatal software problems may result in memory dumps, in core files. The DECT base station can transfer the core files to a remote fileserver. With SIP-DECT 6.0 or later, you can configure a specific URL to an external file server where core dump files should be transferred and stored. The Core dump URL is used by each DECT base station connected to the OMM.

Without a configured Core dump URL, whether and where core files are transferred is dependent on specific DECT base station settings. Without any special configuration, the files are transferred to the server that is used to retrieve the system software (i.e., the directory of the boot image).

- **Configure specific destination:** Enables the specific URL to an external file server for transferring and storing core files.
- **Protocol:** Specifies the protocol used to transfer the core files.
- **Server:** Specifies the IP address or name of the external file server.
- **Port:** Specifies the port of the external file server.
- **Path:** Specifies the location of the core files on the external file server.

5.4.1.15 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.

5.4.1.16 Date and time

If OMM DECT base stations start an SNTP client, the date and time of the configured time zone is synchronized with the Mitel DECT 142 / Mitel 142d and Mitel 600 DECT phones. The date and time will be provided by the OMM to these DECT phones if they initiate a DECT location registration. The rules for a time zone can be configured in the **Time zones** menu (see section 5.4.5).

- **NTP server:** The NTP servers used for time synchronization.

- **Time zone:** Specifies the time zone in which the OMM is operating. This feature is exclusively available on the OMM DECT base station. On PC-OMM configurations, the PC time and time zone is used.

5.4.1.17 Restarting the OMM

You can restart the OMM by clicking on the **Restart** button in the top right corner of the **System Settings** page.

- 1 Click on the **Restart** button.

The **Restart** dialog window opens.

- 2 In the **Restart** dialog window, set the following options:

- **Discard OMM DB and configuration files:** Specifies whether OMM database and configuration data is removed from the DECT base station, including the data retrieved from RCS. Local IP configuration remains unaffected. This parameter is only available on an OMM DECT base station.
- **Reset OMM RFP(s) to factory defaults:** Specifies whether all data is removed from the DECT BASE STATION including the OMM database, configuration files and local IP configuration.

Note: Both options also affect the standby OMM.

- 3 Click **OK**.

A Restart web page opens and displays a progress bar. The login page is loaded automatically if the OMM is reachable again.

5.4.1.18 Updating the OMM

An **Update** button is available on the **System settings** web page. Pressing the **Update** button forces the DECT base stations to check for new software and initiates the software update. For more details about updating the OMM, see the section [8.14](#).

5.4.2 "PROVISIONING" MENU

SIP-DECT supports provisioning through external configuration files. With SIP-DECT 6.0 or later, you can configure a URL for an external file server, from which all configuration files can be downloaded. The configured provisioning server URL is used for secure connections to the file server to retrieve configuration or firmware files. For more information on this feature, see section [8.8.1](#).

The **Provisioning** menu allows you to set parameters for the external provisioning server.

5.4.2.1 Current configuration file URL

- **Current configuration file URL:** URL for the configuration file that is currently loaded.

5.4.2.2 System credentials

System credentials are used to retrieve configuration and resource files from the configured provisioning server for protocols supporting authentication or servers requesting authentication. For HTTP/HTTPS, basic and digest authentication are supported. System credentials can also be inherited for specific URLs, where no user credentials are specified.

- **User name:** Specifies the user name for authentication against the provisioning server.
- **Password:** Specifies the password for authentication against the provisioning server
- **Password confirmation:** Confirms the password for authentication against the provisioning server.

5.4.2.3 Configuration file URL

- **Active:** Enables or disables the configuration file URL feature.
- **Protocol:** Specifies the protocol to be used to fetch the configuration files.
- **Server:** Specifies the IP address or name of the provisioning server.
- **Port:** Specifies the provisioning server's port number.
- **Path:** Specifies the path to the configuration and resource files on the provisioning server.

5.4.2.4 Daily automatic reload of configuration and firmware files

- **Active:** Enables automatic reload of the configuration and resource files on a daily basis, at the specified time.
- **Time of day:** Time for scheduled reload of configuration and firmware files.

5.4.2.5 Autonomous SW update check by OMM

When this is activated, the RFP-OMMs (active, standby) checks autonomously for a new software, whenever a RFP re-configuration (DHCP renew, OM Configurator, ipdect.cfg, <MAC>.cfg) happens.

5.4.2.6 Maximum delay

This parameter specifies the maximum time (in minutes) and the OMM waits past the schedule time before starting the reload of configuration and firmware files. The Maximum Delay has only an effect, when “Daily automatic reload of configuration and firmware files” is activated.

5.4.2.7 Calculated time of delay

The calculated time for scheduled reload of configuration and firmware files (24h time format). This parameter is read-only and is calculated by the OMM based on given “Time of Day” and “Maximum Delay”.

5.4.2.8 Certificates

The OMM uses a trusted certificate chain to validate the server. This is required if the server has no certificate derived from a trusted CA root certificate, where the OMM uses the Mozilla CA Certificate List. You can specify the validation methods to be used.

- **Trusted certificate(s):** Read-only; specifies the number of trusted certificates deployed on the OMM.
- **Local certificate chain:** Read-only; specifies the number of local certificate chains deployed on the OMM.
- **Private key:** Read-only; specifies whether a private key file is deployed on the OMM.
- **Private key password:** Specifies a password for the private key file.
- **Password confirmation:** Confirms the password for the private key file.
- **Delete certificates/key:** Allows the user to delete existing certificates and private key files from the OMM.
- **SSL version:** The SSL protocol version to use for the configuration file server connection. Available options are: TLS1.0, TLS1.1, TLS1.2 or AUTO, where AUTO accepts all protocol versions.
- **Validate certificates:** Enables or disables certificate validation. If enabled, the server certificate is validated against trusted CA's (signed by a CA from the Mozilla CA certificate list) and the configured trusted certificates.

- **Validate expires:** Enables or disables the validation of certificate expiry. When this parameter is enabled, the client verifies whether or not a certificate has expired prior to accepting the certificate.
- **Validate host name:** Enables or disables the validation of hostnames on the OMM.
- **Allow unconfigured trusted certificates:** If enabled, this parameter disables any server certificate validation as long as no trusted certificate was imported into the OMM. AXI commands in a received configuration file may import such trusted certificates into the OMM.
- **Import certificates with first connection:** If enabled (in conjunction with the Allow unconfigured trusted certificates parameter), the trusted certificate will be imported from the cert chain delivered in the server response without any validation, as long as no trusted certificate was imported previously into the OMM.

5.4.2.9 Manual import

You can overwrite the hard coded OMM certificate by importing trusted certificates, a local certificate chain and a private key file.

- **Import PEM file with:** Specifies the type of file to be imported (trusted certificate, local certificate, or private key).
- **Import PEM file:** Specifies the location of the file to be imported.

5.4.3 "SIP" MENU

The SIP settings cover all global settings matching the SIP signaling and the RTP voice streams. Parameters are grouped under the tabs described below.

Category	Setting	Value
Basic settings	Proxy server	10.103.35.11
	Proxy port	5060
	Registrar server	10.103.35.11
	Registrar port	5060
	Registration period	3600 sec
	Globally Routable User-Agent URL	<input checked="" type="checkbox"/>
	Outbound proxy server	
	Outbound proxy port	5060
	Transport protocol	UDP
	Local UDP/TCP port range	5060 - 5060
Advanced	Local TLS port range	5061 - 5061
	Explicit MWI subscription	<input type="checkbox"/>
	User agent info	<input checked="" type="checkbox"/>
	User agent info - compatibility mode	<input checked="" type="checkbox"/>

5.4.3.1 Basic settings

You can set basic SIP settings for the system on the Basic settings menu.

- **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. In case that TLS is used, the value shall be changed to "5061".
- **Registrar server:** IP address or name of the SIP registrar. Enables the DECT phones 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. In case that TLS is used, the value shall be changed to "5061".
- **Registration period:** The requested registration period, in seconds, from the registrar. Default is "3600".
- **Globally Routable User Agent (URL):** Enables support for Globally Routable User-Agent URIs (GRUUs). GRUUs provide a way for anyone on the Internet to route a call to a specific instance of a SIP User-Agent.
- **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. Default is "5060". In case that TLS is used, the value shall be changed to "5061".
- **Transport protocol:** The protocol used by the OMM to send/receive SIP signaling. Default is "UDP".
- **Local UDP/TCP port range:** The port range to be used for DECT users when UDP/TCP is used as the transport protocol. The default is 5060 – 5060.
- **Local TLS port range:** The port range to be used for DECT users when TLS is used as the transport protocol. The default is 5061 – 5061.

There are certain rules to note when configuring port ranges; see section [2.17](#) for more information.

5.4.3.2 Advanced settings

You can set more advanced SIP settings for the system on the Advanced settings menu.

- **Explicit MWI subscription:** Some SIP Call Managers such as the Asterisk support Message Waiting Indication (MWI) based on /21/. An MWI icon is displayed on a DECT phone (Mitel DECT 142 / Mitel 142d, Mitel 600) if the user has received a voice message on his voice box which is supported by the SIP Call Manager. If **Explicit MWI subscription** is enabled, the OMM sends explicit for each DECT phone an MWI subscription message to the Proxy or Outbound Proxy Server.
- **Explicit MWI subscription period:** The requested duration in seconds, before the MWI subscription times out. SIP-DECT re-subscribes to MWI before the subscription period ends.

- **User agent info:** If this option is 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 failed retry timer:** Specifies the time, in seconds, that the OMM waits between registration attempts when the registration is rejected by the registrar. Default is “1200” seconds.
- **Registration timeout retry timer:** Specifies the time that the OMM waits between registration attempts when the registration timed out. Default is “180” seconds.
- **Session timer:** The interval, in seconds, between re-INVITE requests sent from the OMM to keep a SIP session alive. The minimum session timer is 90 seconds and the maximum is 86400 seconds. The default is 0 (i.e., feature is disabled).
- **Transaction timer:** The time period 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 time period 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” milliseconds.
- **Blacklist time out:** The time period in minutes an unreachable call server stays in the blacklist. Valid values are “0” to “1440”. Default is “5” minutes.
- **Incoming call timeout:** The time, in seconds, that the OMM waits for a user to accept an incoming call before rejecting the call automatically. The minimum time is 30 seconds and the maximum is 300 seconds. The default is 180 seconds.
- **Determine remote party by:** You can select the SIP header 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.

Note: When SIP-DECT receives a SIP header **P-Asserted-Identity** in ringing state during an outgoing call, the included identity information (e.g. SIP display name and user-id) will be displayed on Mitel 600 and Mitel 142d phones as new call target. In addition, the outgoing call log of the Mitel 600 and Mitel 142d phones will be updated with the new given identity.

- **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 Ringing response in case of packet losses on the network. By default this feature is active.

- **Semi-attended transfer mode and Refer-to with replaces:**

Semi-attended transfer mode	Refer-to with replaces	Behavior
Blind	No	The semi-attended transfer is handled as a blind transfer. The phone sends CANCEL before REFER for semi-attended transfer.
Blind	Yes	The semi-attended transfer is handled as a blind transfer. The phone sends REFER with Replaces for semi-attended transfer and no CANCEL. This behavior is not SIP compliant but necessary for some iPBX platforms.
Attended	-	The semi-attended transfer is handled as an attended transfer. Both lines of the transferor remain active until the transfer succeeds. This behavior is compliant to RFC 5589.

Please note: The mode “Semi-attended transfer mode: Blind” with “Refer-to with replaces: yes” is not SIP compliant and should only be used on iPBX platforms that require this type of signaling.

- **Remove route:** Enables or disables the addition of the Route header in a SIP packet. Enable this parameter for outbound proxies that do not support Route headers.

Please note: When enabled, this breaks all support for SIP routing. So, if some other devices in the network attempts to add itself to the route, it fails.

- **SIP contact matching:** Specifies the method used by the OMM to match the Contact header in a SIP response to a REGISTER request. Available options are:
 - **URI** – Match user username, domain name, phone IP and port and transport
 - **IP only** – Match the IP address of the phone only
 - **Username only** – Match the username only
 - **IP and user name** – Match the IP address of the phone and the username

The default is **URI**.

- **Call reject state code (user reject):** Specifies the SIP state code sent as response when the user rejects an incoming call by pressing the “Reject” option. Valid values are “400” to “699”. The default is “486”
- **Out of range state code (device unreachable):** Specifies the SIP state code sent as **response** when the incoming call is rejected because the DECT phone is unreachable (e.g., the DECT phone is out of range or out of battery power). Valid values are “400” to “699”. The default is 486.

5.4.3.3 RTP settings

You can set RTP parameters in the RTP settings section.

- **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 or higher 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 no longer available.
- **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. Default is “20” milliseconds.
- **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.
- **Single codec reply in SDP:** If this feature is activated, the OMM answers to SDP offers (included in the SIP signaling) with a single codec in the SDP answer.

5.4.3.4 DTMF settings

You can set DTMF parameters in the DTMF section.

- **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)
Transmits 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 [4.5](#), reference /14/.

5.4.3.5 Registration traffic shaping

Registration traffic shaping parameters allow you to limit the number of simultaneous SIP registrations at startup/fail over of the OMM. This feature is always activated because disabling it may overload the OMM or the call server.

Some providers use a keep-alive mechanism based on SIP registration renewals for remote endpoints that are behind a Network Address Translator (NAT), as in an IP-Centrex solution. The keep-alive mechanism keeps the pinhole open and ensures communication between the remote endpoint and the Session Border Controller (SBC).

The OMM feature that spreads the registration renewals to prevent bottlenecks in large systems is not compatible with the keep-alive mechanism. With SIP-DECT 6.0 or later, you can disable the spread mechanism and configure a registration renewal timer to allow support for the NAT feature.

- **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).
- **Spread registration renewals:** If set to ON, the OMM distributes all DECT phone registration renewals automatically, between half-way through the registration period and 30 seconds before expiry. This prevents registration renewal bottlenecks. Default is ON.
- **Renewal timer:** The time, in seconds, during which the OMM renews DECT phone registrations before expiry (if "Spread registration renewals" is set OFF). The DECT phone automatically sends registration renewals half-way through the registration period, unless the half-way point is greater than the threshold value. For example, if the threshold value is set to 60 seconds and the registration period is 600 seconds, the phone sends the renewal REGISTER message 60 seconds prior to the expiration of the registration period. If the registration period is 100 seconds, the renewal is sent at the half-way point as $(100/2) < 60$. Valid values are 0 to 2147483647. Default is 15.

5.4.3.6 Supplementary Services

The Supplementary Services section contains various parameters related to call control.

- **Call forwarding / Diversion:** The DECT phone user can (de)activate call forwarding/diversion in the OMM via DECT phone 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 the menu on the DECT phone disappear. This setting becomes active on DECT phones with the next DECT "Locating Registration" process (can be forced by switching the DECT phone off and on again). Call forwarding that is already activated 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 (except for an SOS call 0F0F1)
- 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 sent in every case via SIP INFO, independent of the configured or negotiated DTMF method during call setup. All other key events are sent via the configured or negotiated DTMF method.
- The OMM-based call features “Call waiting”, “Call Transfer”, “Brokering” and “Hold” are no longer supported.
- This setting becomes active on DECT phones with the next DECT “Locating Registration” process (can be forced by switching the DECT phone off and on again).
- **Automatic ringback on hold call:** Enables or disables a ringback on the loudspeaker if the B party of the active line releases the call. The ringing begins after the call release timeout interval (see description below).
- **Call transfer by hook on (Mitel 600):** Enables call transfer via the hook key on a Mitel 600 DECT phone (in addition to call transfer via menu).
- **Call transfer by hook on (Mitel 142):** Enables call transfer via the hook key on a Mitel 142 DECT phone (in addition to call transfer via menu).
- **Truncate Caller Indication after ‘;’:** If the user name info in SIP to-/from-/contact headers or p-asserted-identity is extended by a suffix, which is separated by a semicolon, this suffix is truncated before the username is printed to call displays or DECT phone internal call logs.
- **SIP reRegister after 2 active OMM failover:** Enables SIP re-registration of all users from the active OMM when the system detects two active OMMs (in a failover scenario).
- **Call release timeout:** Specifies the time, in seconds, after which an active line is released if the DECT phone user has not gone on-hook after the B party on an active call releases the call.
- **Hold call release timeout:** Specifies the time, in seconds, after which the active line is released if the DECT phone user has not switched to a held line (when the B party on a held call releases the call).
- **Failed call release timeout:** Specifies the time, in seconds, after which an active line is released if the called party is busy, or the call is rejected for any reason.

¹ The OM SOS call feature is unchanged. The initiation of a SOS call in call active state results in the creation of a new line which handles the SOS call.

5.4.3.7 Intercom Push-to-talk-Outgoing calls/Incoming calls

You can set global auto-answer settings in the Intercom Push-to-talk section. For more information on this feature, see section [2.31](#).

Outgoing calls

- **Initialization prefix for Push-to-talk:** String to be entered when initiating an intercom call. An empty string indicates that the DECT phone cannot initiate an intercom call.

Incoming calls

- **Auto answer:** Enables or disables auto-answer on incoming calls.
- **Microphone mute:** Enables or disables microphone muting when incoming calls are automatically answered.
- **Warning tone:** Enables or disables warning tone on incoming call. A short ringtone is played if there are no active calls. If there is an active call in a “barge in” situation, the ringing will be in-band.
- **Allow barge in:** Allows/disallows “barge-in” on existing calls.

5.4.3.8 Security

You can set security-specific settings in the Security section.

- **Persistent TLS keep alive timer active:** When enabled and “Persistent TLS” is selected as transport protocol, the OMM sends out keep alive messages periodically to keep the TLS connection open.
- **Persistent TLS keep alive timer timeout:** Specifies the time pattern, in seconds, in which the OMM sends out keep-alive messages. Valid values are “10” to “3600”. Default is “30” seconds.
- **Send SIPS over TLS active:** When enabled, and “TLS” or “Persistent TLS” is selected as transport protocol, the OMM uses SIPS URIs in the SIP signaling. Default is “ON”.
- **TLS-Authentication:** When enabled and “TLS” or “Persistent TLS” is selected as transport protocol, the OMM validates the authenticity of the remote peer via exchanged certificates and the configured “Trusted certificates”. Default is “ON”.
- **TLS-Common-Name-Validation:** When enabled and “TLS authentication” is selected, the OMM validates the “Alternative Name” and “Common Name” of the remote peer certificate against the configured proxy, registrar and outbound proxy settings. If there is no match, an established TLS connection will be closed immediately.
- **Trusted certificate(s):** The number of imported trusted certificates (read-only).
- **Local certification chain:** Indicates the number of imported certificates in the local certificate chain (read-only).
- **Private key:** Indicates whether the OMM has a private key file (read-only).
- **Delete certificates/key:** Allows deletion of all certificates and the local key.

5.4.3.9 Certificate server

Set the parameters on the Certificate server tab to automatically import Trusted, Local Certificates and a Private Key files from an external server for SIP signaling.

- **Active:** Enables the feature.
- **Protocol:** Specifies the preferred protocol (FTP, TFTP, FTPS, HTTP, HTTPS, SFTP)
- **Server:** Specifies the name or IP address of the external file server.
- **User name:** Specifies the user name to authenticate against the external file server.
- **Password:** Specifies the password to authenticate against the external file server.
- **Password confirmation:** Confirms the password to authenticate against the external file server.
- **Path:** Specifies the path on the file server to the certificate files.
- **Trusted certificate file:** Specifies the name of the PEM file on the specified server, including the trusted certificates.
- **Local certificate file:** Specifies the name of the PEM file on the external server including the local certificate or a certificate chain.
- **Private key file:** Specifies the name of the PEM file on the external server including the local key.
- **Port:** Specifies the certificate server's port number.
- **Use default port:** If selected, the default port associated with the selected protocol is used.
- **Use common certificate configuration:** Enables the use of the system-wide certificate validation settings, as configured on the **System -> Provisioning -> Certificates page** (see section 5.4.2.8).

5.4.3.10 Manual import

Set the parameters for manual import of certificate keys.

- **Import PEM file with:** Allows selection of the kind of certificate/key to be imported.
- **Import PEM file:** Specifies the file to be imported.
- **Import:** Triggers an import of the file.

5.4.4 “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 must 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 [8.17.1](#).

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

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

Status	User Administration	
System	<input type="button" value="OK"/> <input type="button" value="Cancel"/>	
System Settings		
Provisioning		
SIP		
User Administration	Local user account	
Time Zones	Account type	<input type="text" value="Full access"/>
SNMP	Active	<input checked="" type="checkbox"/>
DB Management	User name	<input type="text" value="omm"/>
Event Log	Old password	<input type="text"/>
Sites	Password	<input type="text"/>
Base Stations	Password confirmation	<input type="text"/>
DECT Phones	Password aging	<input type="text" value="None"/>
WLAN		
System Features		
Licenses		
Info		

- **Account type:** Select the account type you wish to change.
- **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.
- **User name:** If desired, enter a new user name.
- **Old password:** Related to the “Full Access Account”, to change the password the old password must be typed in again.
- **Password, Password confirmation:** Enter the appropriate data in these fields.

The OMM has several rules to check the complexity of the new password. A new password will not be accepted if:

- the new password is not five or more characters long
- the new password does not contain characters from at least three 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')
- 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
 - some adjoining keystrokes (e.g. 'qwert')
- **Password aging:** A timeout for the password can be set. Select the duration, the password should be valid.

5.4.5 “TIME ZONES” MENU

Note: This menu is only available if the OMM resides on a DECT base station.

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.

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	✗
Armenian Standard Time	ARM	+4 h	✓
Asia UTC+4	AS4	+4 h	✗
Asia UTC+5	AS5	+5 h	✗
Asia UTC+6	AS6	+6 h	✗
Asia UTC+7	AS7	+7 h	✗
Asia UTC+8	AS8	+8 h	✗
Asia UTC+9	AS9	+9 h	✗
Atlantic	ATL	-4 h	✓
Australia East	AUE	+10 h	✓

The date and time are provided by the OMM to the Mitel 142 and Mitel 600 DECT phones if the DECT phone initiates a DECT location registration. This will be done in the following cases:


- Subscribing to 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 section 5.4.5.1)
- Resetting time zones (see section 5.4.5.2)

5.4.5.1 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.

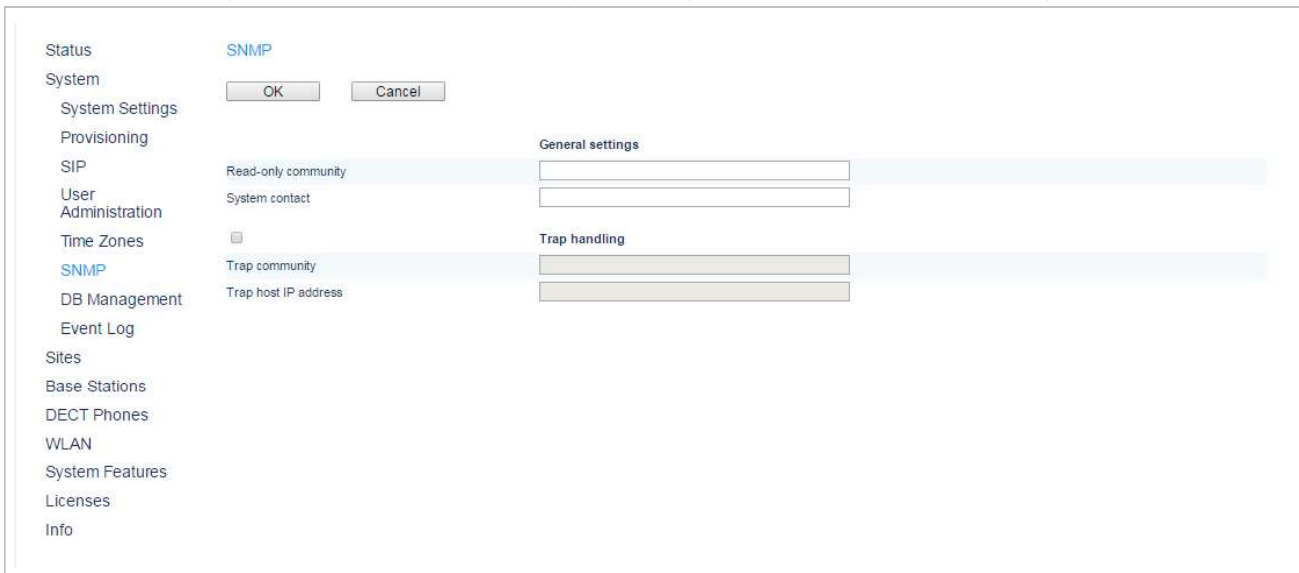
For the DST both points of time (begin of standard time and begin of daylight savings time) must be specified exactly. Therefore a certain day in the month or a certain week day in a month can be used.

5.4.5.2 Resetting Time Zones

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

5.4.6 “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.



You can configure the following SNMP parameters using the OMM web service:

General settings

- **Read-only community:** The SNMP community string 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, see section [8.19](#).

5.4.7 “DB MANAGEMENT” MENU

The database management (DB) menu allows 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 section 5.4.7.1),
- manually exported to the Web browser's file system or to an external server (see section 5.4.7.2),
- automatically exported to an external server when configuration modifications are done (see section 5.4.7.3).

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

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

5.4.7.1 Manual Database Import

Please note: A manual import of a database results in a reset of the OMM.

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

1 Protocol:

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

2 Server: 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: Path and file name which include the OMM database. If you have selected the **FILE** protocol, the **Browse** button is displayed and you can to select the file from the file system.

5 Use common certificate configuration: Enables the use of the system-wide certificate validation settings, as configured on the **System -> Provisioning -> Certificates** page (see section 5.4.2.8).

6 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.

Please note: After the reset, all configuration in the restored database takes effect with the exception of the user account settings. The user account settings can be only modified locally via the OMM Web service and are never restored by a database import.

5.4.7.2 Manual Database Export

In the **Manual export** section of the **Database 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 **Use common certificate configuration:** Enables the use of the system-wide certificate validation settings, as configured on the **System -> Provisioning -> Certificates** page (see section 5.4.2.8).
- 6 Press the **Save** button.

5.4.7.3 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. DECT phone subscription). The backup file overwrites any existing backup files.

Please note: Synchronization with an NTP server is mandatory for an automatic database export. For NTP server configuration, see section [8.5.4](#) and section [8.6](#).

In the **Automatic export** section of the **Database 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 **Port:** Enter the port of the server.
- 5 **User name, Password:** If necessary, enter the account data of the server.
- 6 **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 “_”.
- 7 **Use common certificate configuration:** Enables the use of the system-wide certificate validation settings, as configured on the **System -> Provisioning -> Certificates** page (see section 5.4.2.8).
- 8 Press the **OK** button.

5.4.8 “EVENT LOG” MENU

The **Event log** page displays important event information on OMM system functions, e.g. security aspects. A more detailed system log is available by configuring the **Syslog** function in the **System settings** menu (see section [5.4.1.11](#)).

Status [Event Log](#)

System

System Settings

Provisioning

	Severity	Count	Time (UTC)	Event
SIP	3	1	2016/09/25 19:31:57.579	AXI : [211/omm] client information: Setting 'SUBSCRIPTION' in OMM while MOM is connected and does not handle subscription can force unwanted results
User Administration	3	1	2016/09/25 19:31:57.577	AXI : [211/omm] client information: MOM request sent: 'DECTSubscriptionMode' --> OFF
Time Zones	3	1	2016/09/25 19:31:54.367	AXI : [211/omm] client information: MOM request sent: 'DECTSubscriptionMode' --> WILDCARD (timeout=60 minutes)
SNMP	3	1	2016/09/25 19:31:51.041	AXI : [211/omm] client information: MOM request sent: 'DECTSubscriptionMode' --> ON
DB Management	2	1	2016/09/23 07:04:13.153	AXI : [213/omm] Disconnect client (10.103.35.100) because of elapsed client inactivity timer
Event Log	2	1	2016/09/23 06:55:04.715	AXI : [213/omm] Permission 'Alerting' disabled: No License
Sites	2	1	2016/09/23 06:55:04.715	AXI : [213/omm] Permission 'LocatingAlert' disabled: No License
Base Stations	2	1	2016/09/23 06:55:04.635	AXI : [213] New secure connection from 10.103.35.100:50303
DECT Phones	3	2	2016/09/23 02:17:25.442	AXI : [211/omm] client information: MOM: moved to MOM: device not located at this OMM
WLAN	2	1	2016/09/22 22:02:20.627	IPL : 3 of 3 RFPs connected
System Features	3	1	2016/09/22 22:02:19.348	AXI : [211/omm] client information: MOM: moved to MOM: device not located at this OMM
Licenses	3	1	2016/09/22 22:02:16.576	AXI : [211/omm] client information: MOM request sent: 'DECTSubscriptionMode' --> OFF
Info	2	1	2016/09/22 22:02:16.557	AXI : [211/omm] Permission 'Alerting' disabled: No License
	2	1	2016/09/22 22:02:16.557	AXI : [211/omm] Permission 'LocatingAlert' disabled: No License

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




5.5 “SITES” MENU

DECT base stations 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.
- **Hi-Q Audio Technology, SRTP, Enhanced DECT Security:** Indicates whether (one of) these features are enabled for the site.
- **Base stations:** The number of base stations assigned to the site.

[Sites](#)

2 Sites

	ID	Name	Hi-Q audio technology	SRTP	Enhanced DECT security	Base Stations
 	1	default				10
 	3	Real RFP				2

You can perform the following tasks:

- create a new site (see section 5.5.1)
- edit a site (see section 5.5.2)
- delete a site (see section 5.5.3)


5.5.1 CREATING A NEW SITE

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

- 2 In the Configure site window, specify values for the following parameters:
 - **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.
 - **Name:** Enter the name of the site.
 - **Hi-Q audio technology, SRTP, Enhanced DECT security:** Enable or disable these capabilities.
 - Only 3rd and 4th generation RFPs are supported where these features are enabled.
 - You can mix new RFP types with older RFP 32/34 and RFP 42 WLAN base stations where these features are disabled.
- 3 Press the **OK** button to save your changes.

5.5.2 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.

5.5.3 DELETING A SITE

Note: Only sites without assigned base stations can be deleted. At least one site must remain, so the last site cannot 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.

5.6 “BASE STATIONS” MENU

All configured base stations are listed on the **Base stations** page. The base stations are sorted by their Ethernet (MAC) addresses.

Base Stations

New

Sorted by: DECT clusters

Capturing unconfigured DECT base stations

Start

Capture allowed: ✘

12 Base Stations

DECT Cluster 1: 2 Base Stations

ID	Name	MAC address	IP address	HW type	Site	RPN	Reflective environment	Connected	Active
0000	SVE RFP1	00:30:42:18:1D:BD	10.37.18.31	RFP 35	3	00	✔	✔	✔
0001	SVE RFP2	00:30:42:18:20:A2	10.37.18.32	RFP 35	3	01	✔	✔	✔

DECT Cluster 5: 10 Base Stations

ID	Name	MAC address	IP address	HW type	Site	RPN	Reflective environment	Connected	Active
0002	simu	01:02:03:04:05:06	-	RFP 32	1	02	✘	✘	-
0003	simu	01:02:03:04:05:07	-	RFP 32	1	03	✘	✘	-
0004	simu	01:02:03:04:05:08	-	RFP 32	1	04	✘	✘	-
0005	simu	01:02:03:04:05:09	-	RFP 32	1	05	✘	✘	-

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

- **DECT clusters:** The base stations are sorted by clusters. All used clusters are displayed in the navigation bar on the left side. The OMM base station is marked with a bold font.
- **WLAN profiles:** The base stations are sorted by WLAN profile (see section 5.8).
- **Sites:** The base stations are sorted by sites (see section 5.5). All used sites are displayed in the navigation bar on the left side. The OMM base station is marked with a bold font.

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

- **ID:** An internal number that is used to manage the base station.
- **Name:** Indicates the base station's name (see section 5.6.3).
- **MAC address:** Indicates the base station's MAC address (see section 5.6.3).
- **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 base stations connect to the OMM, they submit their hardware type. The hardware type is displayed in this column. If an error message is indicated in this column, there is a mismatch between the base station and the OMM software version (see section 5.6.2).
- **Site:** Indicates the site the base station is assigned to (see section 5.5).
- **RPN:** Shows the Radio Fixed Part Number that is currently used by the RFP.
- **Reflective environment:** Indicates if the base station is operated in a reflective environment (see section 5.6.3).
- **Connected:** Indicates if the base station is connected to the OMM (see section 5.6.1).
- **Active:** Indicates if the base station is active (see section 5.6.1).

The following tasks can be performed on the **Base stations** page:

- Create and change base stations (see section 5.6.3).

- Capture base stations (see section 5.6.4).
- Delete base stations (see section 5.6.5).
- Find my SIP-DECT base station (see section 5.6.6).

5.6.1 BASE STATION STATES

For each base station 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 DECT phones.

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.

Software 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. The OMM has found new software on the TFTP server. The RFP is waiting for the OMM to initiate a reboot. In the meantime is the RFP fully operational.

5.6.2 OMM / RFP SOFTWARE VERSION CHECK

When the DECT base stations connect to the OMM, they submit their software version. If this version differs from the OMM software version and the versions are incompatible, the RFP connection attempt is rejected. This could happen when using several TFTP servers with different OpenMobility software 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.

5.6.3 CREATING AND CHANGING BASE STATIONS

- 1 To configure a new RFP, click the **New** button on the **Base Stations** page.
To change the configuration of an existing RFP click on the  icon left beside the base station entry.
The **New base station** (or the **Configure base station**) dialog opens.
- 2 Configure the base station (see parameter descriptions below).
- 3 Click **OK**.

Please note: DECT regulatory domain, WLAN regulatory domain and WLAN profile must be configured first. Otherwise DECT and/or WLAN cannot be enabled.

The following parameters can be set in the **New base station** and the **Configure base station** dialogs:

General settings

- **MAC address:** Each RFP is identified by its unique MAC address (6 bytes hex format, colon separated). Enter the MAC address (as it appears on the back of the base station 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 section 5.5), 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 see section [8.2](#).

- **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 DECT phone or RFP using multipath propagation. Calls may have permanent drop outs while moving and high error rates on the RFPs and DECT phones.

For such environment, Mitel has developed the DECT XQ enhancement into the RFP base stations and the Mitel 600 DECT phones 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 DECT phones use more bandwidth on the Air Interfaces if the “Reflective environment“ attribute is switched on. Therefore this is used when problems caused by metal reflections are detected.

WLAN settings

The WLAN section applies to RFPs of the type “RFP 42 WLAN”, “RFP 43 WLAN” and “RFP 48 WLAN” only. For details about WLAN configurations please see section [8.18](#).

The WLAN RFPs 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 section 5.8.1.

Please note: WLAN settings are only configurable if the RFP has been connected at least once to detect the hardware type and a proper WLAN profile is configured (see also section 5.8.1). WLAN cannot be enabled in the **New DECT base station** dialog if the hardware type is unknown.

The following settings are not applied by the WLAN profile. Configure these settings for each DECT base station 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.
- **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.

- **RFP 43:** 300 MBit/s (n) 2x2 MIMO
- **RFP 48:** 450 MBit/s (n) or 600 MBit/s (ac) 3x3 MIMO


5.6.4 CAPTURING DECT BASE STATIONS

Base stations that are assigned to the OMM by DHCP options or OM Configurator settings may connect to the system.

- 1 On the **Base Stations** page, press the **Start** button below the “Capturing unconfigured DECT base stations” caption.


The page is updated with the MAC addresses of those base stations that attempted to register with the OMM (unregistered RFPs).


Note: These entries are not actually stored, and are lost after an OMM reset.

- 2 By clicking on the edit icon  of the appropriate base station, you can add further data and store the base station (see section 5.6.3).

5.6.5 DELETING DECT BASE STATIONS

To delete an existing DECT base station:

- 1 On the **Base Stations** page, click on the  icon left beside the RFP entry.
The **Delete base station?** dialog opens showing the current configuration of this RFP.
- 2 Click the **Delete** button.

Please note: The RFPs bound to a license (License RFPs) cannot be deleted. The License RFPs are displayed in the list with a license icon  instead of the trash icon. For further information on licenses, see section [3.3.2](#).

5.6.6 FIND MY SIP-DECT BASE STATION

This is a new web page and currently located at <http://www.teqdomain.de/RFPsearch/> (to be changed), which is used to scan the local customer network for RFPs running a SIP-DECT 8.0 SW or higher. This helps to determine the IP addresses of the base stations assigned by DHCP.

The IP address of the client PC is determined automatically if it is supported by the browser. The search IP range is initialized automatically. Otherwise, the customer needs to enter the IP range.

My IP address: 10 . 103 . 35 . 126

Base station's IP address range: 10 . 103 . 35 . 1 - 10 . 103 . 35 . 254

Your browser searches for SIP-DECT base station's in the base station's IP address range using HTTP on port 8080.

Search

Progress: [Show details](#)

Result	MAC address	IP address	Go to Web service
	08:00:0F:C3:DC:50	10.103.35.107	Open
	00:30:42:1C:37:83	10.103.35.109	Open
	00:30:42:0D:95:CE	10.103.35.128	Open
	00:30:42:0D:D4:CD	10.103.35.129	Open
	00:30:42:12:33:16	10.103.35.144	Open
	00:30:42:1D:DE:D3	10.103.35.145	Open
	08:00:0F:C3:DC:41	10.103.35.146	Open
	08:00:0F:C3:DC:07	10.103.35.147	Open
	00:30:42:17:88:11	10.103.35.149	Open

© 2018 Mitel Networks Corporation

The results get listed with the base station MAC address, IP address and optionally the RFP generation and configuration state. The configuration web GUI of the OMM running on the base station or the base station that is assigned to, can be opened by clicking the **Open** button of the listed data record.

My IP address: 10 . 103 . 35 . 126

Base station's IP address range: 10 . 103 . 35 . 1 - 10 . 103 . 35 . 254

Your browser searches for SIP-DECT base station's in the base station's IP address range using HTTP on port 8080.

Search

Progress:

Result	MAC address	IP address	RFP Generation	OMM	Go to Web service
	08:00:0F:C3:DC:50	10.103.35.107	4th (RFP45 family)	OMM	Open
	00:30:42:1C:37:83	10.103.35.109	3rd (RFP35 family)	OMM	Open
	00:30:42:0D:95:CE	10.103.35.128	2nd (RFP32 family)	Configured	Open
	00:30:42:0D:D4:CD	10.103.35.129	2nd (RFP32 family)	Configured	Open
	00:30:42:12:33:16	10.103.35.144	2nd (RFP32 family)	Configured	Open
	00:30:42:1D:DE:D3	10.103.35.145	3rd (RFP35 family)	Configured	Open
	08:00:0F:C3:DC:41	10.103.35.146	4th (RFP45 family)	OMM	Open
	08:00:0F:C3:DC:07	10.103.35.147	4th (RFP45 family)	Configured	Open
	00:30:42:17:88:11	10.103.35.149	3rd (RFP35 family)	Configured	Open

© 2018 Mitel Networks Corporation

For Microsoft Edge, the Internet Properties needs to be changed. In the **Security** tab, for the 'Local intranet' in the Advanced view of the Sites configuration, an entry 'http://*.teqdomain.de' (to be changed) needs to be added.

5.7 “DECT PHONES” MENU

The **DECT Phones** page provides an overview of all configured DECT phones sorted by their number. To keep the list concise, the complete list is split up into sub lists containing up to 100 DECT phones. You can move back and forth in increments of 100 DECT phones.

Display name	Number/SIP user name	IPEI	Subscribed	Download
Jürgen Wedemeyer	2075	03586 0677930 4	✓	-
Jürgen Wedemeyer	8241	03586 0677865 *	✓	-

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


- **Display name:** Indicates the DECT phone name.
- **Number/SIP user name:** Indicates the internal call number of the DECT phone.
- **IPEI:** Indicates the DECT phone IPEI.
- **Subscribed:** Indicates if the DECT phone is subscribed to the system.
- **Download:** This column is only displayed if the “Download over Air” feature is started successfully and provides information about the download status of the DECT phone software (see section [8.22](#)).

Note: All DECT phone data that are configured as unbound (split into DECT phone and user data) are also listed at the OM Web service when a user is logged in at the DECT phone, but they cannot be deleted or changed. This is indicated by the and icons. Unbound DECT phones where no user is logged in are not displayed on the **DECT phones** page.

The following tasks can be performed on the **DECT Phones** page:

- create and change DECT phones (see section 5.7.1)
- import DECT phone configuration files (see section 5.7.2),
- subscribe DECT phones (see section 5.7.3)
- delete DECT phones (see section 5.7.4)
- search within the DECT phone list (see section 5.7.5)

5.7.1 CREATING AND CHANGING DECT PHONES

- 1 To configure a new DECT phone, click the **New** button on the **DECT phones** page.
To change the configuration of an existing DECT phone click on the  icon left beside the DECT phones entry.

The **New DECT phone** or the **Configure DECT phone** dialog opens.

- 2 Configure the DECT phone (see parameter descriptions below).
- 3 Press the **OK** button.

The following parameters can be set in the **New DECT phone** and the **Configure DECT phone** dialog:

General settings

- **Display name:** The name parameter represents the SIP Display Name field. This parameter is optional but recommended.
- **Number/SIP user name:** The number is the SIP account number or extension for the DECT phone.
- **IPEI:** This optional setting is the DECT phone IPEI number. On a Mitel DECT 142 / Mitel 142d DECT phone, the IPEI can be found via the following path of the DECT phone menu: **Main menu > Phone settings > System**. On a Mitel 600 DECT phone, the IPEI can be found in the **System** DECT phone menu. Consult the DECT phone's user guide for further information.
- **DECT authentication code:** The DECT authentication code is used during initial DECT subscription as a security option and can be set here for each DECT phone separately (DECT phone-specific DECT authentication code). This parameter is optional. If no DECT phone-specific DECT authentication code is set, the system-wide DECT authentication code is used.
- **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).
- **Delete subscription:** This option is only available when configuring an existing DECT phone (in the **Configure DECT phone** dialog). If this option is selected, the DECT phone 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 DECT phone, the number of the appropriate alarm trigger will be used as a system-wide calling number in case of a SOS or ManDown event. Please see /31/ 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 Mitel 600 DECT phone. 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, section [5.4.1.9](#)). If there is no voice mail number configured (neither the individual nor the system-wide) or another DECT phone type is used, then the voice mail number must be configured locally in the DECT phone.
- **Number used for visibility checks:** Provides phone number or SIP user name used for standby OMM visibility checks.

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.

User service

- **Use SIP user name:** Specifies whether the XSI user name is taken from the user's SIP data. The generated format is <sip user name>@<sip registrar domain>. Possible values are **Global**, **On**, or **Off**.
- **Use SIP user authentication:** Specifies whether the XSI authentication name and password are taken from user's SIP data. The generated format is <sip authentication name>@<sip registrar domain>. Possible values are **Global**, **On**, or **Off**.
- **User name:** Specifies the user's user name for the XSI service (if **Use SIP user name** is set to **Off**). The user name is part of the access url path of a XSI request (e.g., /com.broadsoft.xsi-actions/v2.0/user/<service user name>/directories/Enterprise?firstName=A*).
- **Authentication name:** Specifies the name to authenticate the user for XSI services (if **Use SIP user authentication** is set to **Off**).
- **Password, Password confirmation:** Specifies the password to authenticate the user for XSI services.

Key lock

- **Active:** This enables the Key lock menu under System menu/Administration on the Mitel 600d DECT phone. To prevent change of the time by the user disable the feature here.
- **PIN, PIN confirmation:** The DECT phone default PIN is set to **0000**. It is the same default PIN as for the local DECT phone feature. Adjust a new PIN here if the user had forgotten its PIN.
- **Timer:** The phone is locked automatically after the selected time (in seconds). If the timer is set to **None**, the key lock is not automatically activated if the DECT phone is not used, and the long press of the # key does not activate the key lock with PIN.

5.7.2 IMPORTING DECT PHONE CONFIGURATION FILES

A set of DECT phones can also be configured in a semi-automatic manner by import of a configuration file.

- 1 On the **DECT Phones** page press the **Import** button.
The **DECT phone enrolment** page opens.
- 2 Select your configuration file and press the **Import** button. For information on the file layout, see section [12.2.1](#).
- 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.
- 4 Select the DECT phones you want to add to the OMM database by selecting the appropriate checkboxes, and click **Add**.

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

Failed records are marked with a red star.

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

5.7.3 SUBSCRIBING DECT PHONES

Preparation by OMM Web service

After adding a DECT phone configuration to the OMM, the DECT phone must be subscribed. The OMM must first be enabled to allow subscriptions from DECT phones. This is done by pressing the following buttons on the **DECT Phones** page.

- **Start** button under the “Subscription with configured IPEI” caption (see section 5.7.3.1). This button enables subscription for the next 24 hours.
- **Start** button and time interval parameter under the “Wildcard subscription” caption. This button enables 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 DECT phone (with IPEI) is set up in the database and no DECT phone is subscribed. After successful subscription of the first DECT phone the subscription will still be enabled for 24 hours. The time is further limited if the feature 'Restrict subscription duration' is active (see chapter [5.4.1.2 DECT settings](#)).

Subscription steps, done by DECT phone

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

On each DECT phone, 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 to subscribe to the system.

Please note: The PARK is displayed in the top-right corner of the **DECT Phones** page. Each SIP-DECT deployment has a unique PARK code.

If the administrator configured a global or device-specific DECT authentication code, the administrator/user must enter in the code before the DECT phone subscribes to the system.

For “wildcard subscription”, an additional ID may be configured (see sub section Wildcard Subscription).

5.7.3.1 Subscription with Configured IPEI

The DECT phone data to be assigned to the subscribing DECT phone are identified by the IPEI. The identity of a DECT phone (IPEI) is already known by the system before the DECT phone attempts to subscribe. Unknown DECT phones are not allowed to subscribe in this mode.

To enable subscriptions, click the **Start** button under the section **Subscription with configured IPEIs** caption on the **DECT Phones** page.

The OMM allows a subscription of configured but not subscribed DECT phones during the next 24 hours. The administrator must press the **Subscribe** button again to permit more DECT phones to subscribe to the SIP-DECT system.

Note: Older DECT phones may not offer the possibility to enter an access code (AC). You should always subscribe these DECT phones with configured IPEI to maintain security. The time is further limited if the feature 'Restrict subscription duration' is active (see chapter [5.4.1.2](#) DECT settings).

5.7.3.2 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 **DECT phones** 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 24 hours.

To achieve a selection of data during subscription (e.g. the user name being assigned to the DECT phone), 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 DECT phone.


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

Note: The time is further limited if the feature 'Restrict subscription duration' is active (see chapter [5.4.1.2](#) DECT settings).

Please note: The input of the additional ID is only possible with Mitel 142 and Mitel 600 DECT phones. The value is not supported on third party GAP phones. If GAP phones are going to subscribe wildcard, the first free DECT phone data record without any additional ID will be assigned.

5.7.4 DELETING DECT PHONES

To delete an existing DECT phone:

- 1 On the **DECT phone** page click on the  icon left beside the DECT phone entry.
The **Delete DECT phone?** dialog opens showing the current configuration of this DECT phone.
- 2 Press the **Delete** button.

5.7.5 SEARCHING THE DECT PHONE LIST

You can use the search function to search for a specific DECT phone in the DECT phone list. The search function allows you to find a DECT phone by a given number or IPEI.

- 1 On the **DECT phones** page click on the **Search** button.

The **Search DECT phone** dialog opens.

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

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

5.7.6 DISPLAYING USER AND DECT PHONE DATA

You can display a summary of user status and DECT phone configuration in a pop-up window on the **DECT Phone** page. Click the magnifying glass icon beside a DECT phone entry to view the **User/device status & configuration** window.

Note: A configuration and status summary for the DECT phone is also available on the DECT phone under the Administration menu. The presentation layout is similar to the OMM Web service window, but the DECT phone only displays its own data.

The following table describes the parameters in the **User/device status & configuration** window.

Parameter	Description
User status	
Registered	Current SIP user registration status Yes = registered No = not registered
Registrar server type	Current SIP registrar: Primary or backup SIP registrar (secondary or tertiary)
Registrar server	IP address of the SIP Registrar
Registrar port	Port number of the SIP Registrar
Calculated local port	SIP user's automatically determined client port
Silent charging	Current silent charging state Yes = in silent charging mode No = not in silent charging mode
CoA data loaded	COA data sent to DECT phone Yes = data has been sent No = no data sent
User configuration data	
User Id	Internal system identifier for the user
User rel. Type	Type of association between the user and DECT phone. Dynamic or fixed.
Name	User's name

Number	SIP user name or number
Description 1	Additional textual description for a user (e.g., department or function)
Description 2	Additional textual description for a user (e.g., department or function)
User lang.	Language setting on the DECT phone
SOS number	Emergency number to be dialed when the SOS key has been pressed
MD number	Emergency number to be dialed when a sensor alarm (Mitel 600 DECT phone) has been initiated
VM number	Voice mail number (dialed by a long press of '1' key on the Mitel 600 DECT phone)
SIP auth. user name	SIP authentication user name
SIP auth. password	SIP authentication password
Fixed local port	SIP user's configured fixed client port (used for SIP registration)
Login/Add ID	ID used for user identification during login procedure at the DECT phone OR ID used for wildcard subscription during DECT phone subscription procedure
PIN	PIN used for user identification during login procedure at the DECT phone "*****" = a PIN is set, empty = no PIN is set
External	User data provided by an external provisioning server (<user>.cfg) Yes = user data imported from a server No = user data only stored internally in the OMM DB
Permanent	Indicates whether the user is stored in all OMMs in a Multi-OMM Manager (MOM) managed system. Yes = user data is stored in all OMMs in the SIP-DECT system. No = user data only stored in the local OMM (i.e., where the device is currently registered).
VIP	To guarantee a minimum blackout for a very important person (e.g. emergency user) the SIP (re-)registration of such people can be prioritized. Yes = prioritized No = not prioritized
Visibility checks	The OMM standby feature uses an existing SIP account to check the availability of the registrar. Yes = this account is used No = this account is not used
Hot desking supported	Hot desking capability; only available for users with a dynamic association with a DECT phone. Yes = user is registered for hot desking on the call server. No = user is not registered for hot desking on the call server.
Auto logout on charging	A user can be logged out of the device automatically when the Mitel 600 DECT phone is placed in the charger cradle. Yes = automatic logout when put in charger No = no automatic logout
Authenticate logout	User log out requires authentication. Yes = user logout with authentication No = user logout without authentication
Sending messages	User's permissions to send text messages using the Mitel 600 DECT phone Yes = user is authorized to send text messages No = user is not authorized to send text messages

Sending vCards	User's permissions to send vCards using the Mitel 600 DECT phone Yes = user is authorized to send vCards No = user is not authorized to vCards
Receiving vCards	Indicates whether the user accepts received vCards Yes = incoming vCards are accepted No = incoming vCards are not accepted
Video stream perm.	User's permissions to access video using the Mitel 602 DECT phone Yes = user is authorized to access video No = user is not authorized to access video
Locate	User's permissions to locate other users using the Mitel 600 DECT phone Yes = user can locate other users No = user cannot locate other users
Tracking	Tracking forces the Mitel 600 DECT phone to indicate every change of the DECT base station even in idle state Yes = tracking is active No = tracking is inactive
DECT locatable	Permission to locate the user (i.e., through the SIP-DECT locating solution) Yes = locating the user is permitted No = not permitted
Keep personal dir.	The local directory of the Mitel 600 DECT phone is usually the user's personal directory and is cleared at logout. If deleting the directory content is not desirable, this option can be set Yes = local directory is not cleared No = local directory is cleared
Forward mode	Mode of Call diversion or Call forwarding (Off, Immediately, Busy, No answer, Busy & no answer)
Forward time	Time delay in seconds before the incoming call is redirected.
Forward dest.	Destination of the redirected call
Hold ring back time	Time in minutes after which the user wants to be reminded of the connection on hold 0 = Off, no reminder
Call waiting disabled	An incoming call is signaled in-band if the user is otherwise engaged (Call waiting). This feature can be disabled Yes = call waiting is disabled No = call waiting feature is active
Auto answer	Enables or disables auto-answer on incoming calls. If auto answer is enabled, the DECT phone plays a tone to alert the user before answering the call. If auto answer is disabled, the DECT phone treats the incoming call as a normal call.
Microphone mute	Enables or disables microphone muting when incoming calls are automatically answered.
Warning tone	Enables or disables a warning tone to play when the DECT phone receives an incoming call on an active line. A short ringtone is played if there are no active calls. If there is an active call in a "barge in" situation, the ringing will be in-band.
Allow barge in	Allows/disallows how the DECT phone handles incoming calls while the DECT phone is on an active call. When enabled an incoming call takes precedence over an active call, by placing the active call on hold and automatically answering the call. When disabled the DECT phone treats an incoming call like a normal call.
Monitoring mode	SIP-DECT supports a "User Monitoring" feature to check the availability of a user to

	<p>receive calls or messages. On = monitoring feature is active Off = monitoring feature is not activated</p>
Conference server type	<p>User-specific setting of the conference service to be used for three-way conferencing None = three-way conferencing is disabled Global = OMM system setting is used (default) Integrated = integrated conference server is used</p>
Conference server URI	URI for the external conference server
Use CoA profile	ID of the CoA (Central DECT phone configuration over air) profile
Use SIP user name	Uses SIP user name for XSI directory access
Use SIP user auth.	Uses SIP authentication credentials for XSI directory access
User service user name	User name for XSI service (if SIP credentials not used for XSI directory access)
User service auth name	Authentication name for XSI service (if SIP credentials not used for XSI directory access)
User service password	Password for XSI service (if SIP credentials not used for XSI directory access)
Device status	
IPEI	International Portable Equipment Identifier (globally unique identifier of the DECT phone)
HW type	Hardware type of 600 DECT phone or 142d otherwise "unknown"
SW version	Version of the software on the Mitel 600 DECT phone
Subscribed	<p>Subscription status of the DECT phone Yes = DECT phone is subscribed No = DECT phone is not subscribed</p>
Encryption	<p>DECT encryption status Yes = Encryption is enabled No = Encryption is disabled</p>
Capability "Messaging"	<p>Messaging capability of the DECT phone Yes = DECT phone supports messaging No = DECT phone does not support messaging</p>
Capability "Enh. Locating"	<p>Enhanced locating capability of the DECT phone Yes = DECT phone supports enhanced locating No = DECT phone does not support enhanced locating</p>
Capability "Video"	<p>Video capability of the DECT phone Yes = DECT phone supports video No = DECT phone does not support video</p>
Capability "CoA profile"	<p>CoA capability (Central DECT phone configuration over air) of the DECT phone Yes = DECT phone supports CoA No = DECT phone does not support CoA</p>
Device auto-created	<p>Auto-creation occurs when the DECT phone data set is automatically generated in the OMM's database at subscription time. No administrative task is required on the SIP-DECT system to subscribe a DECT phone in this auto-create mode. Yes = DECT phone has been subscribed in auto-create mode No = DECT phone has not been subscribed in auto-create mode</p>

Default CoA profile loaded	A default CoA profile (Central DECT phone configuration over air) can be sent to a 600 DECT phone Yes = a default profile was sent No = no default profile was sent
Device configuration data	
Device ID	Internal system identifier for the DECT phone

5.8 “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 base stations of the type RFP 42 WLAN and RFP 43 WLAN.

Note: You cannot activate the WLAN function for the OMM, even if the OMM base station is an RFP 42 WLAN.

For a detailed description on WLAN configuration, see the section [8.18](#).

5.8.1 “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. You can define more than one WLAN profile, to a maximum of 20 WLAN profiles. 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.

Note the different WLAN profile types:

RFP type	WLAN profile type
RFP 42 WLAN	RFP 42
RFP 43 WLAN	RFP 43
RFP 48 WLAN	RFP 48

- **HT40** (RFP 43/48 WLAN only): Very high throughout mode with 80 MHz bandwidth increases data rate up to 1300 MBit/s (3x3 MIMO).
- **HT80** (RFP 48 WLAN only): Includes the HT40/HT20 bandwidth setting. A channel with a bandwidth of 80 MHz occupies 4 WLAN channels with a bandwidth of 20 MHz.

The **WLAN profiles** menu allows configuration and administration of these WLAN profiles.

Status	WLAN Profiles					
System	<input type="button" value="New"/>					
Sites	Type RFP43: 1 WLAN profile					
Base Stations	Profile ID	SSID1	SSID2	SSID3	SSID4	WLAN Access Points
DECT Phones		1	TES3	-	-	2
WLAN	WLAN Profiles WLAN Clients System Features Licenses Info					

You can:

- create and change WLAN profiles (see section 5.8.1.1)
- delete WLAN profiles (see section 5.8.1.2)
- export WLAN profiles (see section 5.8.1.3)

The defined WLAN profiles are then assigned to one or more WLAN base stations (see section 5.8.2). 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 base station (see section 5.6.3).

5.8.1.1 Creating and Changing WLAN Profiles

You need at least one active WLAN profile in order to operate the WLAN function for an RFP 42/43/48 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 (**RFP 42**, **RFP 43** or **RFP 48**) 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.

- 4 Change the desired settings of the WLAN profile. You need at last 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 de-activates the WLAN function for base stations 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 base stations (see section 5.6.3). If you changed an existing WLAN profile, the settings are applied to the assigned base stations automatically.

The following parameters are available on the **New WLAN profile** page and 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 sections [8.18](#) and [8.12](#)).
- **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. This option is now unavailable for RFP 48.
- **Maximum rate** (list of rates in Mbps, 1..54, default: 54): This setting applies to RFP 42 WLAN only. 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 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 43/48 WLAN selection list: 802.11bg /802.11b only / 802.11g only / 802.11abg /802.11n, default: 802.11bg): On the **RFP 43/ RFP 48** profile you can choose additionally 802.11 modes 802.11abg, 802.11n and the mode 802.11ac is only available for RFP 48 WLAN.

Mode	802.11abg	802.11n/802.11ac
Open	yes	yes
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): This setting applies to RFP 42 WLAN only. Enables a WLAN procedure to enhance radio interference avoidance.

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 must 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 or 128 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.
 - (selection, WPA any / WPA v.1 / WPA v.2, default: WPA any): Select the **WPA Type** 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 enforces 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 must also specify the (see below). For details about the RADIUS authentication procedure, using the public keys, and importing certificates to the WLAN clients see the **Radius settings** 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.
- **MAC access filters** (on / off, default: off): This setting applies to RFP 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 (RFP 42 WLAN only), 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, 60..86400): 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)** configuration is used.

- **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:** (on / off, VLAN or DiffServ (RFP 42 WLAN only), default RFP 42 WLAN: off/VLAN, default RFP 43 WLAN: off): 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, including 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.

5.8.1.2 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 must select another WLAN profile for all assigned RFPs first (see section 5.6.3).
- 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.

5.8.1.3 Exporting WLAN Profiles

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

On Windows 7 you can use the “netsh wlan add profile filename=xxx” command 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).

5.8.2 “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.

5.9 “SYSTEM FEATURES” MENU

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

5.9.1 “DIGIT TREATMENT” MENU

A number manipulation is provided by the digit treatment feature for corporate directories that handles both incoming and outgoing calls.

Digit treatment for LDAP directories

A chosen number from an LDAP directory 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 characters are automatically removed from the LDAP directory entry: '%', space, '(' and ')'. The result of the conversion is sent to the DECT phone to be displayed e.g. in the directory entry details and entered in the redial list.

Note: A conversion performed for an LDAP directory 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 DECT phone to be displayed and entered in the call log¹.

Outgoing call

The dialed 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 en-bloc dialed numbers and to overlap sending as long as the SIP session has not been initiated.

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 DECT phone to be displayed or entered in the call log².

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

- creating and changing “Digit treatment” entries (see section 5.9.1.1)
- deleting “Digit treatment” entries(see section 5.9.1.2)

5.9.1.1 Creating and Changing “Digit treatment” Entries

1 To configure a new entry, click the **New** button on the **Digit treatment** page.

To change the configuration of an existing entry click on the  icon left beside the entry.

The **New digit treatment entry** or 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 a directory entry. The prefix to be substituted for calling party

¹ For Incoming Call/Calling Party Number: Depending on the capabilities of the DECT phone and the level of integration.

² For Outgoing Call/Called Number: If the user dials the number from the redial list again, the same procedure will be applied as for the initial dialing.

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 characters that replaces the external pattern for the directory entry / 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 only be dialed and transferred to a call log with a Mitel 600 DECT phone.

- 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 to directories only.
- 5 Directory:** This option can be used to specify the rule for incoming and/or outgoing calls. Activate this option if the rule applies to directories.
- 6 Sites:** Specifies the sites for which a rule is applied e.g. "1, 2" (see section 5.5). 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.

5.9.1.2 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.

5.9.2 "DIRECTORY" MENU


The **Directory** menu allows you to manage connections to one or more LDAP, XML or XMI servers to support central corporate directories. The OMM supports multiple LDAP, XML or XSI servers with specific parameter settings to support different types of directories (e.g. global corporate directory, group specific directory, personal directory). XML-based directory services can be implemented using the XML terminal interface.

If there is more than one directory server configured, all are displayed on the DECT phone interface when the user invokes the Central Directory function. 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 directory server entry. The OMM determines the display order of the directories in the DECT phone menu by the order specified by the administrator.

You can configure up to five external directories. If only one directory server is configured, the name configured in the OMM is ignored, and the directory is accessed directly when the user presses the System softkey on the DECT phone (>>>) or selects the **Central directory** option from the menu.

5.9.2.1 Creating and Changing Directory Entries

You can configure directory entries (or change existing entries) from the **Directory** page (or the **Directory (comp. mode)** page for older SIP-DECT systems) in the OMM web interface. Parameters that require configuration depend on the type of directory you are configuring.

To change the configuration of an existing entry click the **Edit** icon () beside the entry, and follow the steps described below to set parameter values.

You can change the order of the directory entries by selecting a directory entry in the list and clicking the up or down arrows in the right panel (under **Tasks**). Changing the order of directory entries in the list changes the order in which they appear on the DECT phone.

To create or edit a directory entry, do the following:


- 1 Select the **Directory** entry in the **System Features** menu (left pane).
- 2 Click **New** on the **Directory** page, or click the pencil icon beside an existing directory entry in the list. The **New directory entry** (or **Configure directory entry**) dialog opens.
- 3 Specify values for the directory server as described in the following table. Note that only certain parameters are required, depending on the directory server type.

Parameter	Description	LDAP	XML	XSI
Active	Enables or disables the directory entry on the DECT phone.	✓	✓	✓
Type	Interface type supported by the directory server. Possible values: <ul style="list-style-type: none"> • LDAP • XML • XSI Enterprise • XSI Enterprise common • XSI Group • XSI Group common • XSI Personal 	✓	✓	✓
Name	Name to be displayed for the directory (Latin-1 character set is supported).	✓	✓	✓
Search base	Location in the directory from which the search begins (e.g., "ou=people, o=my com"). The configuration is valid for all DECT phones that support the LDAP directory feature. To make search requests unique for different users, the search base configuration can include placeholders that are replaced by user-specific values when submitting the LDAP request to a server. The following placeholders are defined: <ul style="list-style-type: none"> • "<TEL>" (for the user's telephone number) • "<DESC1>" (for the user's "Description 1" attribute) • "<DESC2>" (for the user's "Description 2" attribute) • "SIPProxy" (for the current primary, secondary or tertiary SIP server address); supported for release 6.1 and later 	✓		
Search type	Attribute on which searches are performed (Surname or Given name).	✓		✓
Display type	Display mode for search results (Surname , First Name or Given name Surname).	✓		✓
Server search timeout	Interval (in seconds) during which the OMM waits for search results from the LDAP server (1 – 10 seconds).	✓		

Parameter	Description	LDAP	XML	XSI
Protocol	Transfer protocol used to communicate with the XML or XSI directory server (http or https).		✓	
Server port	Port for the LDAP directory server (default is 389). Note: SSL (default port 689) is not supported. Windows Active Directory Server uses port 3268.	✓		
Server	IP address or FQDN of the directory server.	✓	✓	✓
User name	Name of the account for directory server access, if required.	✓	✓	
Password	Password for directory server access, if required. Note: If no user/password is specified, an anonymous bind takes place. SIP-DECT supports LDAP simple bind.	✓	✓	
Path (and parameters)	URL (with parameters, if required) to the XML directory on the XML directory server.		✓	
Use common certificate configuration	Enables or disables use of the system's certificates (loaded for provisioning purposes) for HTTPS directory access		✓	✓

- 4 Click **OK** to save your changes.

5.9.2.2 Deleting Directory Entries

- 1 To delete an existing directory entry click on the  icon on the left of the entry on the **Directory** page.
The **Delete directory entry** dialog opens showing the current configuration of this entry.
- 2 Press the **Delete** button.

5.9.3 “DIRECTORY (COMP. MODE)” MENU

In SIP-DECT 6.2 and later, the underlying database model for directory support in SIP-DECT has changed. To support backwards compatibility, the **Directory (comp. mode)** page provides directory configuration and maintenance for existing SIP-DECT systems with LDAP or XML directory support.

To create or edit a directory entry using the old database model, do the following:

- 1 Select the **Directory (comp. mode)** entry in the **System Features** menu (left pane).
- 2 Click **New** on the **Directory (comp. mode)** page, or click the pencil icon beside an existing entry.
The **New directory entry** (or **Configure directory entry**) dialog opens.
- 3 In the **New directory entry** dialog (or the **Configure directory entry** dialog, for existing entries), specify values for the directory server as described in the following table. Note that only certain parameters are required, depending on the directory server type.

Parameter	Description	LDAP	XML
Active	Enables or disables the directory entry on the DECT phone.	✓	✓
Order	Specify where you want the directory entry to appear in the list.		
Type	Interface type supported by the directory server. Possible values: LDAP or XML.	✓	✓
Name	Name to be displayed for the directory (Latin-1 character set is supported).	✓	✓
Protocol	Transfer protocol used to communicate with the XML directory server (HTTP or HTTPS).		✓

Parameter	Description	LDAP	XML
Server name	IP address or FQDN of the directory server.	✓	✓
Server port	Port for the LDAP directory server (default is 389). Note: SSL (default port 689) is not supported. Windows Active Directory Server uses port 3268.	✓	
Search base	Location in the directory from which the search begins (e.g., "ou=people, o=my com"). The configuration is valid for all DECT phones that support the LDAP directory feature. To make search requests unique for different users, the search base configuration can include placeholders that are replaced by user-specific values when submitting the LDAP request to a server. The following placeholders are defined: <ul style="list-style-type: none"> • "<TEL>" (for the user's telephone number) • "<DESC1>" (for the user's "Description 1" attribute) • "<DESC2>" (for the user's "Description 2" attribute) • "SIPProxy" (for the current primary, secondary or tertiary SIP server address); supported for release 6.1 and later 	✓	
User name	Name of the account for directory server access, if required.	✓	✓
Password	Password for directory server access, if required. Note: If no user/password is specified, an anonymous bind takes place. SIP-DECT supports LDAP simple bind.	✓	✓
Search type	Attribute on which searches are performed (Surname or Given name).	✓	
Display type	Display mode for search results (Surname , First Name or Given name Surname).	✓	
Server search timeout	Interval (in seconds) during which the OMM waits for search results from the LDAP server (1 – 10 seconds).	✓	
Path (and parameters)	URL (with parameters, if required) to the XML directory on the XML directory server.		✓

4 Click **OK** to save your changes.

5.9.4 "FEATURE ACCESS CODES" MENU

Feature access codes (FAC) allow a DECT phone user to perform specific actions on the OMM from any subscribed DECT phone.

Status	Feature Access Codes	
System	<input type="button" value="OK"/> <input type="button" value="Cancel"/>	
Sites		
Base Stations		
DECT Phones	General settings	
WLAN	FAC number	*1
System Features	FAC action	
Digit Treatment	Activate subscription <input checked="" type="checkbox"/>	34567
Directory	Activate wildcard subscription <input checked="" type="checkbox"/>	34568
Directory (comp. mode)	Deactivate subscription <input checked="" type="checkbox"/>	9
Feature Access Codes	User login <input checked="" type="checkbox"/>	11
XML Applications	User logout <input checked="" type="checkbox"/>	12
Licenses	Set system credentials for provisioning <input type="checkbox"/>	
Info	Blind transfer <input type="checkbox"/>	

To configure the FAC feature, do the following:

- 1 **FAC number:** Enter a unique FAC number.
- 2 Activate the appropriate checkbox(es) to enable the corresponding FAC feature(s). For each enabled FAC feature enter an assigned access code.
 - **Activate subscription:** Activate subscription of the DECT phone.
 - **Activate wildcard subscription:** Activate subscription of the DECT phone (if no IPEI is configured).
 - **Deactivate subscription:** De-activate DECT phone subscription.
 - **User login:** Log the user into the DECT phone.
 - **User logout:** Log the user out of the DECT phone.
 - **Set system credentials for provisioning:** Allow a user to set system credentials via the Mitel 600 DECT phone.
 - **Blind transfer:** Initiate a blind transfer from the DECT phone. When a user dials the “Blind transfer” FAC en-bloc (in an active call state) followed by a target number, SIP-DECT initiates a blind transfer to the given target number.
- 3 Press the **OK** button.

Users can perform the relevant operations by dialing the “FAC number” followed by the “FAC access code” en-bloc from any subscribed DECT phone.

In the example above a subscribed user can activate the OMM DECT subscription by dialing “*134567” en-bloc.

Please note: Overlap sending is not supported for FAC. “FAC number” and “FAC action code” must be entered en-bloc.

FAC functions will be confirmed by an audible indication to the user (in-band tone signals).

5.9.5 "XML APPLICATIONS" MENU

The SIP-DECT XML terminal interface allows external applications to provide content for the user on the Mitel 600 DECT phone. To make the XML terminal interface applications available for the DECT phone user, you must configure the appropriate hooks in the **XML Applications** menu.

When the application hook is enabled in the OMM, Mitel 600 DECT phone users can program a softkey with the specific hook (or select the relevant menu option) to trigger the associated action. The side keys on the Mitel 600 DECT phones only display icons in idle state. In an active call state, only the two softkeys below the display indicate the active feature.

15 XML Applications			
Name	URL	Active	
Caller list	http://	X	
Redial list	http://	X	
Presence	http://	X	
Server menu	http://	X	
Action URI	http://	X	
Feature access codes	http://	X	
Call completion	http://	X	
Park call	http://	X	
Unpark call	http://	X	
Pickup	http://	X	
Take	http://	X	
Call forward	http://	X	
Call routing	http://	X	
Call protection	http://	X	
Voice box	http://	X	

The following table summarizes the predefined XML application hooks:

Hook	Description	DECT Phone menu
Caller list	<p>Hook to replace the local caller list.</p> <p>You can use this hook to enable the centralized call log feature (MX-ONE systems only).</p> <p>"Call log support provided on an external server":</p> <p>The call logs are located on an external XML server. Each call log action on the DECT phone is requested to the external XML server and the server answers this with XML responses. The content is displayed on the DECT phone for the user.</p> <p>The URL-path in the configuration differs from "<i>CSIntegration?object=history</i>" which is an indication for the OMM centralized call log feature.</p>	>>> > Info > Caller List
Redial list	<p>Hook to replace the local redial list.</p> <p>You can use this hook to enable the centralized call log feature (MX-ONE systems only).</p> <p>"OMM centralized Call log support provided by the OMM internally":</p> <p>The call logs are pushed from the PBX (e. g. Mitel MX-One) to the OMM through SIP and the OMM provides the call logs for all the DECT phones as an "XML server".</p> <p>The URL-path in the configuration be "<i>CSIntegration?object=history</i>" which is an indication for the OMM centralized call log feature.</p>	>>> > Info > Redial List

Hook	Description	DECT Phone menu
Presence	Hook to reach a presence application .	>>> > Presence
Server menu	Hook to reach a server menu. The OMM system menu is available as a menu entry in the local main menu of the DECT phone (>>> softkey). If no user is assigned to the DECT phone, the server menu is the only available XML application hook.	>>> > Info > Server
Action URI	URI to be called in case of user/device events. The URI is configured in the OMM via OMP. Content can be pushed towards the DECT phone via SIP notify.	n/a
Feature access codes	Hook to provide Feature Access Codes translation.	
Call completion	Hook to provide callback option when a user places an outgoing call and wants to request a callback before releasing the call.	>>> > Info > Callback
Park call	Hook to the Park Call service interface.	>>> > Call option > Park call
Unpark call	Hook to the Unpark Call service interface.	>>> > Unpark call
Pickup	Hook to the Pickup Call service interface.	>>> > Pickup
Take	Hook to Take Call service interface.	>>> > Take
Call forward	Hook to the Call Forward service interface.	>>> > Call forward
Call routing (Mitel 602 DECT phones only)	Hook to the Personal Call Routing service interface.	>>> > Call routing
Call protection (Mitel 602 DECT phones only)	Hook to the PBX call protection service interface.	>>> > Call protection
Voice box	Hook to Voice Mail service interface.	>>> > Info > Voice box

These hooks can be activated or deactivated but not deleted. You can create up to 10 additional hooks.

Note: The “Call forward” XML hook replaces the “Call forwarding / diversion” supplementary service. When activated, the “Call forwarding / diversion” supplementary service is automatically deactivated and all user-specific settings are removed.

5.9.5.1 Creating a New XML Hook

To create a new XML hook, do the following:

1 On the **XML Applications** page, click **New**.

The **New XML application** window opens.

2 Configure the following parameters for the XML hook:

- **Active:** Activates or deactivates the XML hook.
- **Name:** Name for the XML hook (not applicable for predefined XML hooks)
- **Protocol:** HTTP or HTTPS.
- **Server:** IP address or name of the server which provides the XML content.
- SIP-DECT 6.0 and later supports “SIPProxy” placeholders for XML Server application URLs in systems with SIP redundancy. Where applications are located on a SIP server, XML applications must be addressed using the current primary, secondary or tertiary SIP server address. In those cases, the “SIPProxy” placeholder can be used as server input.
- **User name:** Login user name if an authentication is required by the server.

- **Password, Password confirmation:** Password if authentication is required by the server.
- **Path (and parameter):** Path and query of the URI. For “Feature access codes translation”, the Path settings contains placeholders for the queried translation: {subsc} = Number, {ppn} = Device ID, {fac} = FAC.

3 Click **OK** to save your changes.

5.9.5.2 Modifying an XML Hook

To change the configuration of an existing XML hook, do the following:

- 1 On the **XML Applications** page, click on the **Edit** (pencil) icon beside the XML hook entry. The **Configure XML application** window opens.
- 2 Edit the XML application parameters (described above) as necessary. Note that you cannot change the name of a predefined XML hook.

Note: SIP-DECT 7.0 and later supports centralized call logs for systems using the MX-ONE call server. To enable this feature, you must enter “**CSIntegration?object=history**” as the value for the **Path** parameter. This applies to both the **Caller list** and **Redial list** predefined XML hooks.

3 Click **OK** to save your changes.

5.9.5.3 Deleting an XML Hook

You cannot delete any predefined XML hooks. You can only delete XML hooks that you have created.

To delete an XML hook, do the following:

- 1 On the **XML Applications** page, click on the **Delete** (garbage can) icon beside the XML hook entry. The **Delete XML application?** window opens.
- 2 Click **Delete** to confirm deletion of the XML hook.

5.10 “LICENSES” MENU

The **Licenses** page provides an overview on the currently used license. On this page you can also import an activation or license file:

- 1 Select the path and file name where the activation or license key is stored.
- 2 Click the **Import** button.

For a detailed description on the OMM licensing model, see section [3.3](#).

5.11 “INFO” MENU

The **Info** page displays the End User License Agreement (EULA).

With the first login to a new SIP-DECT software version, this page is displayed automatically and the user must accept the EULA by clicking the **Accept** button.

6 OM MANAGEMENT PORTAL (OMP)

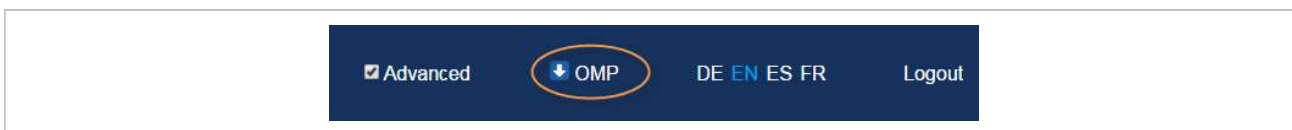
The OM Management Portal (OMP) is a Java tool used to manage the SIP-DECT solution. It can be used to view and configure OMM system data and has integrated monitoring and other maintenance features.

SIP-DECT supports Java web start to start the OMP. Java 1.7 is required to run OMP 5.0 or later. By default, the source for the OMP binary is a Mitel web server (RFP-OMM) or the OMP.jar from the RPM installation (PC-OMM).

You can also configure a different source (**System settings** -> **OMP web start** in the OMM Web service, or **System** -> **Advanced settings** -> **Additional services – OMP web start** in the OMP). The following configuration order is used:

- GUI-configured OMP web start URL in RFP-OMM installations
- Environment variable 'OM_WebStartUrl' (e.g. set by ipdect.cfg configuration file)
- Mitel web server (RFP-OMM) / from RPM installation (PC-OMM)

You can download the OMP jar file from the OMM Web service by clicking on the OMP link in the top bar:



Double-click on the downloaded file (OMP.jnlp) and click “Run” in the dialog window. The OM Management Portal starts and prompts for login credentials.

Please note: Configuration of a non-default source must not contain login credentials because this is not supported by the Java Web Start mechanism. The HTTP/FTP server must be configured accordingly.

This section lists all parameters which can be configured and viewed using OMP. All parameters which are also accessible by the OM Web service are described in the appropriate OM Web service section (section 5). New parameters which are only accessible via OMP are described in this section.

6.1 LOGIN

The OMM allows more than one user at a time to configure the system.

To log in to the system enter the following data:

- **IP address** of the OMM.
- **User name, Password:** Enter a user name and a password. Both strings are checked case sensitive.

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

The **System name** is set by the system administrator after first successful login to the OMM, see section 6.5.1.

The system name and the IP address of successful logins are stored in the local OMP preferences and can be reselected for further logins. Up to 10 different login datasets can be stored.


- On a Linux system, preferences are stored in the user's home directory “~/java/.userPrefs/...”.
- On a Windows system, preferences are stored in the registry node “HKEY_CURRENT_USER/Software/JavaSoft/Prefs/...”.

After login the OMP is set to the configuration mode page showing the system status page which contains health state information of the connected OMM (see section 6.4). If there is a version difference between the OMP and the OMM, this will also be indicated here. Details can be viewed in the **Help: About AXI** menu (see section 6.15).

6.2 LOGOUT

There is no automatic logout for the OMP. The user must log out manually.

To log out from the system:

- Click on the Close icon  in the upper right corner of the OMP window
- Select the **Exit** entry from the **General** drop-down menu.

Note: If the OMM link is broken, the OMP asks if you want to reconnect to the OMM. In that case, you must enter the login data again.




6.3 OMP MAIN WINDOW

The header of the OMP window shows the version of the connected OMM.

“OMP mode” toolbar buttons

The OMP provides different modes: **Configuration mode**, **Monitor mode** and **Planning mode**. Configuration mode allows changing of parameters. In monitor mode, parameters are only displayed, but are not changeable. Monitor mode provides additional features, e.g. system and RFP statistics and RFP synchronization monitoring. Planning mode enables the creation of graphics which can be used with the OM Locating application to visualize the placement of the RFPs (see also /27/).

To select the desired mode, press the appropriate button in the upper toolbar of the OMP window:

-  Configuration mode
-  Monitor mode
-  Planning mode

Main menus

The OMP provides two main menus which are available in all program situations:

- **General** menu, see section 6.14.
- **Help** menu, see section 6.15.


Navigation panel


Both configuration and monitor mode contain a navigation panel. This panel contains the mode-dependant menu.

Status bar

The status bar is located at the bottom of the main window. It shows the following items:


- Encryption state:


The  icon indicates that encryption is enabled.

The  icon indicates that encryption is disabled.

This setting can be configured in the **DECT** tab of the **System settings** menu (see also section 6.5.1).

- PARK,
- Subscription state: Clicking on one of the following icons enables / disables subscription.

The  icon indicates that subscription is enabled.

The  icon indicates that subscription is disabled.

Subscription can also be enabled / disabled in the **DECT phones** menu (see also section 6.7.8).

- Auto-create on subscription state: Clicking on one of the following icons enables / disables Auto-create on subscription.

The  icon indicates that Auto-create on subscription is enabled.

The  icon indicates that Auto-create on subscription is disabled.

This setting can also be configured in the **DECT** tab of the **System settings** menu (see also section 6.5.1).

- Connection status to the OMM:



If connected to the OMM, the IP address of the OMM is displayed.



OMP is disconnected from the OMM.

Info console

General OMP events are displayed the **Info console**.

6.4 “STATUS” MENU

The system status is displayed after startup of OMP. The **Status** panel provides information about the system health states, and contains the following tabs:

- Overview (see section 6.4.1)
- DECT base stations (see section 6.4.2)
- Users (see section 6.4.3)
- Devices (see section 6.4.4)

- Sites (see section 6.4.5)
- Conference (see section 6.4.6)
- Video devices (see section 6.4.7)

6.4.1 OVERVIEW

The “Overview” tab consists of a “System” panel providing general system health states information and a “Features” panel which shows health states of system features. Some of these features are optional; that means the relevant health state is only shown if the feature is activated in system.

System	Health Status	Features	Health Status
Uptime	3 Day(s) 01 h 56 min	OM Integrated Messaging & Alerting service	✓
Licenses	✓	Configuration over air	✓
Standby OMM (10.37.18.31)	✓	User data server	✓
Synchronization state	✓	SIP certificate server	✗
DECT base stations	✓		
SIP	✓		
DB import/export	✓		
Downloading new firmware to portable parts	✓		
Provisioning server	✓		
OMM configuration file processing	✓		

The “Overview” tab shows following system information:




- **System uptime:** Elapsed time since OMM start (in days, hours and minutes)
- **Licenses:** Licenses health state
- **Standby OMM:** Standby OMM IP address and health state of standby configuration (if no standby OMM is configured a grey cross is shown)
- **Synchronization state:** Synchronization health state
- **DECT base stations:** Base stations health state
- **SIP:** SIP health state
- **DB import/export:** DB import/export health state
- **Downloading new firmware to portable parts:** (Health) state of firmware download to DECT phones
- **Provisioning server:** Health state of provisioning server health state

- **OMM configuration file processing:** Health state of configuration file processing.

Depending on OMM system configuration, the “Features” tab consists of all or a subset of these health states:

- **OM Integrated Messaging & Alerting service:** Messaging and alerting feature health state (always active)
- **SIP certificate server:** SIP certificate server health state (always active)
- **Configuration over Air:** Central DECT phone configuration over air state (optional)
- **User data server:** User data server health state (optional)
- **User monitoring:** User monitoring health state (optional)
- **Video:** Video health state (optional)

Health states can have the following values:

-  – inactive or unknown
-  – error
-  – OK

6.4.1.1 OMM Standby Configuration

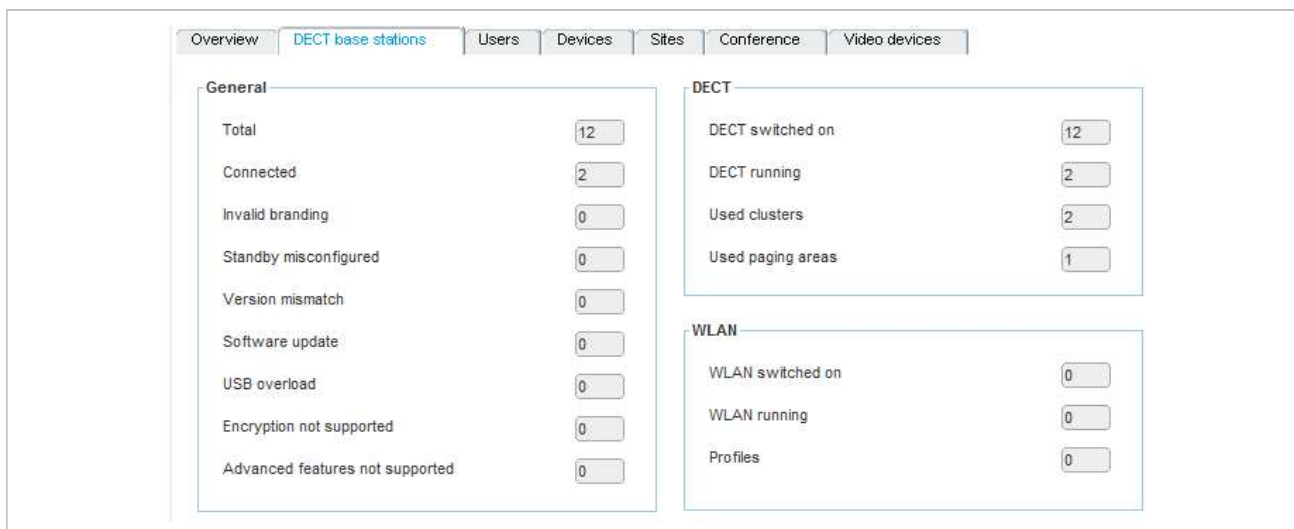
OMM standby configuration must be built of the same RFP generations. Valid configurations are:

- **RFP4G <- Standby -> RFP4G**
- **RFP3G <- Standby -> RFP3G**
- **Linux Server/OVA <- Standby -> Linux Server/OVA**

In previous releases, OMM standby configuration is not available for SIP-DECT with Cloud-ID, that is, in SDC mode.

6.4.2 DECT BASE STATIONS

The “DECT base stations” tab contains the following sections: “General”, “DECT” and “WLAN”.



The “General” panel provides counters related to RFP configuration and state:

- **Total:** Total number of RFPs configured

- **Connected:** Number of RFPs connected to OMM
- **Invalid branding:** Number of connected RFPs with invalid branding
- **Standby misconfigured:** Number of connected RFPs with wrong standby configuration
- **Version mismatch:** Number of connected RFPs running with wrong software version
- **Software update:** Number of connected RFPs requesting software update
- **USB overload:** Number of connected RFPs detecting overload at their USB port
- **Encryption not supported:** Number of connected RFPs not supporting encryption
- **Advanced features not supported:** Number of connected RFPs not supporting “Advanced features” which covers “Hi-Q audio technology”, “Terminal video”, “Enhanced DECT security” and “SRTP”.

The “DECT” panel provides counters related to RFPs DECT configuration and state:

- **DECT switched on:** Number of configured RFPs with DECT switched on
- **DECT running:** Number of connected RFPs with DECT running
- **Used cluster:** Number of configured clusters
- **Used paging areas:** Number of paging areas used by RFPs

The “WLAN” panel provides counters related to RFPs WLAN configuration and state:

- **WLAN switched on:** Number of configured RFPs with WLAN switched on
- **WLAN running:** Number of connected RFPs with WLAN running
- **Profiles:** Number of WLAN profiles used by RFPs

6.4.3 USERS

The “Users” tab provides information about DECT phone users.

Category	Item	Value
General	Total	84
	SIP registered	4
	Monitored active	0
	Monitored passive	0
	Sending messages permission	0
	DECT locatable	0
User monitoring states	Warning	0
	Unavailable	0
	Escalated	0
Number for visibility checks	Number/ SIP user name	25052

The “General” panel provides counters concerning DECT phones user configuration and states:

- **Total:** Total number of configured users
- **SIP registered:** Number of configured users registered at SIP server
- **Monitored active:** Number of configured users with active monitoring enabled
- **Monitored passive:** Number of configured users with passive monitoring enabled
- **Sending messages permission:** Number of configured users with message sending permission enabled
- **DECT locatable:** Number of configured users with DECT locatable enabled

The “User monitoring states” panel provides counters concerning DECT phone user monitoring state

- **Warning:** Number of monitored users in state ‘Warning’
- **Unavailable:** Number of monitored users in state ‘Unavailable’
- **Escalated:** Number of monitored users in state ‘Escalated’

The “Number for visibility checks” panel provides phone number or SIP user name used for standby OMM visibility checks.

6.4.4 DEVICES

The “Devices” tab provides information about DECT phones.

The screenshot shows the 'Devices' tab in the OMP interface. It features two main panels:

- General Panel:** Contains two counters: 'Total' with a value of 84 and 'Subscribed' with a value of 4.
- Downloading new firmware to portable parts Panel:** Shows the status of firmware downloads. The 'Status' is indicated by a green checkmark. The 'Loading firmware from' field contains the URL 'ftp://10.37.18.35/600.dnld'. The 'Firmware version' field contains '[600: 5.00.SP5.RC1] - [650,602: 6.0.RC8]'. Below these are several counters for different states: 'Known downloadable' (4), 'Already updated' (4), 'Waiting for download' (0), 'Currently downloading' (0), 'Barred' (0), 'Download error' (0), 'Unreachable' (0), and 'Detached' (0).

The “General” panel contains counters related to DECT phones:

- **Total:** Total number of configured DECT phones
- **Subscribed:** Number of configured DECT phones which are subscribed to OMM

The “Downloading new firmware to portable parts” panel provides information about state of DECT phone firmware download:

- **Status:** Status of firmware download
- **Loading firmware from:** URL of firmware download container
- **Firmware version:** Version info of firmware container
- **Known downloadable:** Number of DECT phones known as downloadable
- **Already updated:** Number of DECT phones already updated
- **Waiting for download:** Number of DECT phones waiting for download
- **Currently downloading:** Number of DECT phones currently downloading
- **Barred:** Number of downloadable DECT phones currently barred
- **Download error:** Number of downloadable DECT phones with download error
- **Unreachable:** Number of downloadable DECT phones currently unreachable
- **Detached:** Number downloadable DECT phones currently detached

6.4.5 SITES

The “Sites” tab provides counters concerning site configuration and state:

The screenshot shows the 'Sites' configuration tab with the following data:

Setting	Value
Total	2
Contains RFP(s)	2
Hi-Q audio technology	0
Enhanced DECT security	0
Secure real time transport protocol	2
Terminal video	0

- **Total:** Total number of configured sites
- **Contains RFPs:** Number of sites with dedicated RFPs
- **Hi-Q audio technology:** Number of sites with Hi-Q audio technology enabled
- **Enhanced DECT security:** Number of sites with “Enhanced DECT security” enabled
- **Secure real time transport protocol:** Number of sites with “Secure real time transport protocol” (SRTP) enabled
- **Terminal video:** Number of sites with terminal video enabled

6.4.6 CONFERENCE

The “**Conference**” tab provides conference channel information:

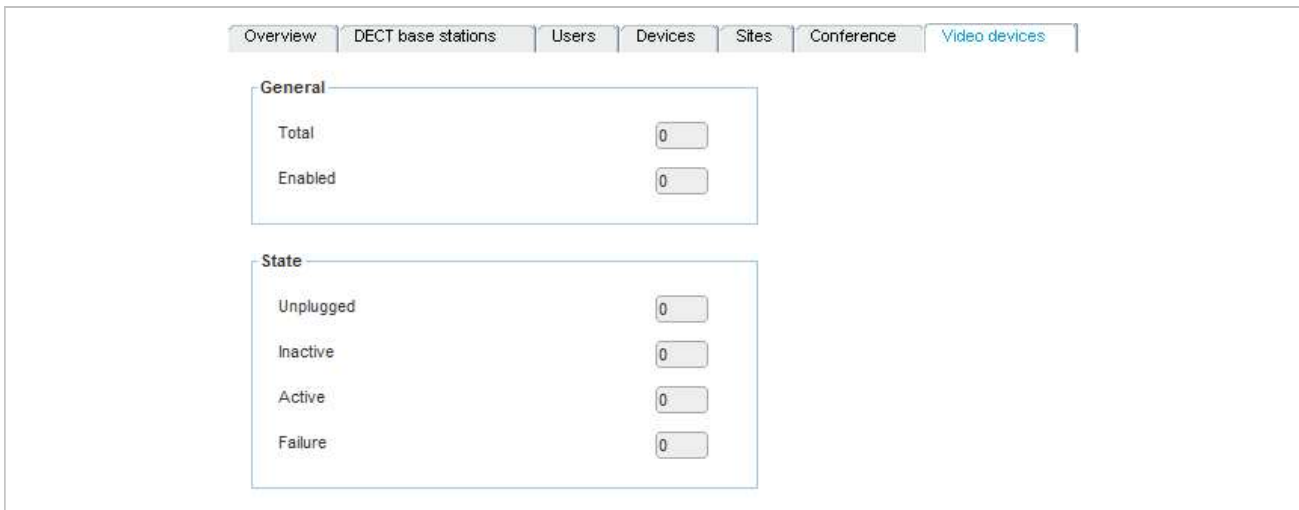
The screenshot shows the 'Conference' configuration tab with the following data:

Setting	Value
Total	6
Available	6

- **Total:** Total number of conference channels in system
- **Available:** Number of currently available conference channels

6.4.7 VIDEO DEVICES

The “**Video devices**” tab provides video device state information.



The “General” panel provides video device configuration related counters:

- **Total:** Total number of configured video devices
- **Checkpoint:** Number of video devices enabled

The “State” panel provides video device state related counters:

- **Unplugged:** Number of video devices in state unplugged
- **Inactive:** Number of video devices in state inactive
- **Active:** Number of video devices in state active
- **Failure:** Number of video devices in state failure

6.5 “SYSTEM” MENU

The **System** menu allows configuration and display of global OMM settings. The system settings are changeable in configuration mode. Change of some parameters can cause the OMM to be reset. In this case a new login is required.

The **System** menu provides the following entries:

Configuration mode	Monitor mode	See section
Basic settings	Basic settings	6.5.1
Advanced settings	Advanced settings	6.5.2
	Statistics	6.5.3
SIP	SIP	6.5.4
User administration	User administration	6.5.6
Data management	Data management	6.5.7

6.5.1 “BASIC SETTINGS” MENU

The **Basic settings** menu contains general settings for the OpenMobility Manager.

The screenshot shows the configuration interface for the SIP-DECT OM system. On the left is a navigation menu with categories like Status, System, SIP, Provisioning, etc. The main area is titled 'Configuration' and has four tabs: 'General', 'DECT', 'WLAN', and 'Software update URL'. The 'General' tab is selected and contains three sections: 'General' with fields for System name, Remote access (checkbox), Tone scheme (dropdown), and Time zone (dropdown); 'SysLog' with fields for Active (checkbox), IP address, and Port; and 'RFP software update' with fields for Mode (dropdown) and Time of day (time picker). At the bottom are four buttons: 'OK', 'Cancel', 'Update', and 'Restart'.

The Basic settings menu contains the following tabs:

- General (see section 6.5.1.1)
- DECT (see section 6.5.1.2)
- WLAN (see section 6.5.1.3)
- Software update URL (only on systems where the OMM is running on a DECT base station) (see section 6.5.1.4)

6.5.1.1 General settings

You can set the following parameters on the General tab of the “Basic Settings” menu.

General

- **System name:** Name of the SIP-DECT system.
- **Remote access:** Enables or disables SSH access to all RFPs in the DECT system. For more information on SSH access, see section [9.3.5](#).
- **Tone scheme:** Specifies the country in which the OMM resides, which enables country-specific tones (e.g., busy tone, dial tone, etc).
- **Time zone:** Specifies the time zone in which the OMM is operating.

Syslog

- **Active:** Enables propagation of syslog messages by the OMM and RFPs.
- **IP address:** Address of the host that collects the syslog messages.
- **Port:** Port of the host that collects the syslog messages.
- **Forward OMM Messages to syslog:** (Visible only on a PC-hosted OMM system) Enables/disables forwarding of syslog messages from the PC-hosted OMM.

RFP software update

- **Mode:** RFP update mode. Options are “One by one” (each RFP is updated separately) or “All at once” (all RFPs are updated in one operation).

- **Time-controlled:** Indicates whether the start of the RFP update is time-controlled.
- **Time of day:** Specifies the time for time-controlled RFP updates.

Note: Updates triggers can be controlled through update intervals (DHCP, config files) or manually triggered via the **Update** button.

The “General” tab contains two additional buttons (aside from default buttons):

- **Update:** Requests an immediate update of RFP software.
- **Restart:** Requests an OMM restart.

6.5.1.2 DECT settings

For a description of the parameters which can be set in the **DECT** tab, see the description of the **System settings** page of the OMM Web service (see section 5.4.1). The corresponding parameters are described in the **DECT settings** and **Downloading new firmware to portable parts** page sections, with the exceptions noted below.

The following settings are only available in the OMP.

- **Regulatory domain:** The OMP offers an additional regulatory domain selection (Radio 1910-1927MHz 250mW) for SIP-DECT operation in some South American countries. See section [2.12](#) for more information on this feature.
- **SARI:** Specify the Secondary Access Rights Identifier (SARI) for the Dual Homing feature. DECT phones subscribe to the SARI (instead of the PARK) to ensure that user data is synchronized across all OMMs in the system. See section [8.16](#) for more information on this feature. You can click the **Generate SARI** button to generate the SARI from the system PARK code.
- **Paging area size:** Select the number of paging areas for the SIP-DECT system. A paging area can consist of up to 256 RFPs (and the smallest group can consist of 16 RFPs). The configuration of the paging areas is done in the **Paging areas** menu of the OMP (see section 6.7.2).
- **Restricted subscription duration:** Restricts the time period throughout which a DECT phone can be subscribed to 2 minutes. Furthermore, the subscription mode will be disabled immediately after every successful subscription of a DECT phone.
- **Auto-create on subscription:** Activate this option if an unbound subscription of DECT phones should be allowed. See the *OM DECT Phone Sharing and Provisioning Guide* for more information.

6.5.1.3 WLAN settings

For a description of the parameters which can be set in the **WLAN** tab, see the description of the **System settings** page of the OMM Web service. The same parameters are described in the **WLAN settings** section (section 5.4.1.3).

6.5.1.4 Software Update URL settings

With SIP-DECT 6.0 or later, DECT base stations in small SIP-DECT systems (~10 RFPs) can obtain their software image from the RFP OMM, if they have no valid URL from which to load their software. If the OMM is running on a RFP, the RFP OMM delivers the software to the connected RFPs.

You configure the URL for the RFP software image (iprpf3G.dnld and iprpf4G.dnld) on this tab. This tab is only available when the OMM resides on an RFP.

For a description of the parameters that can be set in the **Software update URL** tab, see the description of the **System settings** page of the OMM Web service. The same parameters are described in the **Software update URL** (see section [5.4.1.12](#)).

6.5.2 “ADVANCED SETTINGS” MENU

The **Advanced settings** menu contains additional settings for the OpenMobility Manager.

The screenshot shows the 'Advanced settings' menu with the following configuration options:

Parameter	Value
Input format QoS parameter	ToS
QoS for voice packets	ToS: B8, DiffServ: 46
QoS for signalling packets	ToS: B8, DiffServ: 46
TTL (Time to live)	32
802.1p voice priority	6
802.1p signaling priority	6

The Advanced settings menu contains the following tabs:

- Net parameters (see section 6.5.2.1)
- DECT phones (see section 6.5.2.2)
- DECT phone firmware (see section 6.5.2.3)
- IMA (see section 6.5.2.4)
- Additional services (see section 6.5.2.5)
- User monitoring (see section 6.5.2.6)
- Special branding (see section 6.5.2.7)
- Core dump (see section 6.5.2.8)
- Remote system dump (see section 6.5.2.9)
- OMM certificate (see section 6.5.2.10)
- OMM certificate server (see section 6.5.2.11)
- SNMP (see section 6.5.2.12)
- Time zones (see section 6.5.2.13)
- Pre-Login banner (see section 6.5.2.14)

6.5.2.1 Net parameters

For a description of the parameters that can be set in the **Net parameters** tab, see the description of the **System settings** page of the OMM Web service. The same parameters are described in the **Net Parameters** section (section [5.4.1.15](#)).

- **Input format QoS parameter:** Format for quality of service parameter. Available options are ToS or DiffServ.
- **QoS for voice packets:** Specifies the value of the type of service (ToS) or DiffServ byte (depending on the QoS input format value) of the IP packet header for all packets that transport RTP voice streams.
- **QoS for signalling packets:** Specifies the value of the type of service (ToS) or DiffServ byte (depending on the QoS input format value) of the IP packet header for all packets related to VoIP signaling.
- **TTL (Time to live):** Specifies the maximum hop count for all IP packets.
- **802.1p voice priority:** Specifies the VLAN priority tag for RTP packets.
- **802.1p signaling priority:** Specifies the VLAN priority tag for VoIP signaling packets.

6.5.2.2 DECT Phones

The OMM can set certain start-up text settings on the DECT Phone over the air. For more information on this feature see section [2.13.5](#).

- **Dial editor supports digits only:** Enables a digits-only mode for the DECT phone dial editor. In this mode, the "*" has the meaning of a digit to be dialed, even if short-pressed. If the mode is not enabled, a short press of the "*" key changes the editor mode to alphanumeric.
- **Set startup window headline:** Enables display of the text string specified in the Startup window headline field.
- **Startup window headline:** Text headline to be displayed in the DECT phone window at startup. Default value is "my company".
- **Set startup window text:** Enables display of the text string specified in the Startup window text field.
- **Startup window text:** Text string to be displayed in the DECT phone window at start. Empty by default.
- **Truncate portable part user name:** Enables or disables truncating the name of the user registered to the DECT phone.

6.5.2.3 DECT phones firmware

The OMM can provide a DECT phone firmware update over the air. If the **Activate firmware update** checkbox is enabled, the “Download over Air” feature is activated. For more information on this feature, see section [8.22](#).

For a description of the parameters on the **DECT Phone firmware** tab, see section [5.4.1.8](#).

6.5.2.4 IMA

The Integrated Message and Alarm (IMA) configuration is stored in the OMM database. You can configure a specific URL for the OMM to retrieve the IMA configuration file (ima.cfg). The IMA configuration remains available even if the configured server becomes unavailable.

When you set a specific URL, the OMM uses that URL to load the IMA configuration file during startup. If no specific IMA configuration file source is configured, the provisioning server settings (ConfigURL) are used to retrieve the ‘ima.cfg’ file.

For a description of the parameters on the **IMA** tab, see the description of the **System settings** page of the OMM Web service. The same parameters are described in the **OM Integrated Messaging & Alerting service** section (section [5.4.1.10](#)).

6.5.2.5 Additional services

For a description of the parameters on the **Additional services** tab, see the description of the **System settings** page of the OMM Web service. The same parameters are described in the following sections:

- **Voice mail** (section [5.4.1.9](#))
- **OMP web start** (section [5.4.1.7](#))
- **Date and time** (for NTP servers, see section [5.4.1.16](#))

6.5.2.6 User monitoring

The **User monitoring** tab allows you to configure the system-wide parameters for the user monitoring feature.

- **Locating escalation:** If this option enabled, the alarm trigger “LOC-ERR-USERSTATE” will be generated by the OMM. Default setting is “off”.
- **Start-up delay:** The start-up delay defines the period of time the user monitoring start-up is delayed (between 2 and 15 minutes) after failover or system start-up.
- **Escalation delay:** The escalation delay defines the period of time the user monitoring will wait before the unavailable status is escalated.
- **Activity timeout 1:** The activity timeout 1 defines the maximum time (between 30 and 1440 minutes) between user activities in passive monitoring mode.
- **Activity timeout 2:** The activity timeout 2 defines the maximum time (between 5 and 60 minutes) between user activities in active monitoring mode.
- **Battery threshold:** The battery threshold defines the minimum battery load (between 0 and 100% in steps of 5%).

6.5.2.7 Special branding

With SIP-DECT 6.0 or later, you can integrate a customer-specific logo into the OMM Web service interface (displayed beside the Mitel logo in the top bar). The "Special Branding" tab allows you to specify the location of the branding image file (customer_image.png) on an external file server.

When you set a specific URL, the OMM uses that URL to load the image file during startup. If no specific customer logo file source is configured, the provisioning server settings (ConfigURL) are used to retrieve the image file.

The branding image is stored permanently in the OMM database. The file is deleted automatically when the branding image URL configuration is disabled. The picture should not be larger than 50 pixels high and 216 pixels wide.

By special request, you can use specific branding key to lock the OMM; the key must be branded to all DECT phones before they can be subscribed. See section [8.25](#) for more information on this feature.

PP Branding key

- **Active key:** Displays the current branding key associated with the DECT phones.
- **New key:** Specifies the new branding key generated through the `DECTSuiteBrandingInstallation.exe` utility.

Branding image URL

- **Active:** Enables the specific URL for downloading the customer_image.png file (as opposed to the ConfigURL, which points to an external file server for all configuration and resource files).
- **Protocol:** Specifies the protocol used to fetch the image file.
- **Port:** Specifies the port of the external file server.
- **Server:** Specifies the IP address or name of the external file server.
- **User name:** Specifies the user name to authenticate on the external file server.
- **Password:** Specifies the password to authenticate on the external file server.
- **Password confirmation:** Confirms the password to authenticate on the external file server.
- **Directory:** Specifies the location of the image file on the external file server.
- **Use common certificate configuration:** Enables the use of the same certificate validation settings for the image file URL as specified for the ConfigURL.

6.5.2.8 Core Dump

Fatal software problems may result in memory dumps, in core files. The IP RFP can transfer the core files to a remote fileserver. With SIP-DECT 6.0 or later, you can configure a specific URL to an external file server where core dump files should be transferred and stored. The Core dump URL is used by each RFP connected to the OMM.

Without a configured Core dump URL, whether and where core files are transferred is dependent on specific RFP settings. Without any special configuration, the files are transferred to the server that is used to retrieve the system software (i.e., the directory of the boot image).

For a description of the parameters on the **Core Dump** tab, refer to the description of the **System settings** page of the OMM Web service. The same parameters are described in the **Core dump URL** section (section [5.4.1.14](#)).

6.5.2.9 Remote system dump

A system dump is a file that holds information about the OpenMobility Manager and all connected RFPs. With the Remote System Dump feature, a system dump is transferred to a remote server. You can configure a specific destination, otherwise the system configuration URL is used.

The system dump is generated manually by pressing the dump button or automatically at the configured time. Please ensure that the used files server allows writing or creating system dumps.

For a description of the parameters on the **Remote system Dump** tab, refer to the description of the **System settings** page of the OMM Web service. The same parameters are described in the **System dump** section (section [5.4.1.13](#)).

6.5.2.10 OMM Certificate

You can overwrite the hard-coded OMM certificate by importing a local certificate chain and a private key file which may be password-protected. The OMM certificate will be used for incoming AXI and HTTPS connections to the OMM services. If the OMM can be reached from the internet by a domain and an appropriate CA certificate has been imported, no security warnings are displayed in web browsers that trust the CA root certificate.

For more information on this feature, see section [8.10](#).

Certificates/key

- **Private key:** Indicates whether the OMM has a private key file (read-only).
- **Local certificate chain:** Indicates the number of local certificate chains deployed on the OMM (read-only).
- **Delete certificates/key:** Allows you to delete any existing certificate or key files.

PEM file import

- **Import PEM file with:** Indicates the content type of the PEM file being imported. Available options are “Local certificate chain” or “Private key”.
- **File:** Specifies the location of the PEM file to be imported.
- **Import:** Triggers the import of the specified PEM file.

Private key password

- **Private key password:** Specifies the password to be used for the private key file if you want the file to be password-protected.
- **Password confirmation:** Confirms the password for the private key file.

6.5.2.11 OMM certificate server

OMM certificates can be updated automatically through configuration of a secure OMM certificate server URL.

- **Active:** Enables the feature.
- **Protocol:** Specifies the preferred protocol (FTP, TFTP, FTPS, HTTP, HTTPS, SFTP).
- **Server:** Specifies the name or IP address of the external file server.
- **Port:** Specifies the certificate server's port number
- **Use default port:** If selected, the default port associated with the selected protocol is used.
- **User name:** Specifies the user name to authenticate against the external file server.
- **Password:** Specifies the password to authenticate against the external file server.
- **Password confirmation:** Confirms the password to authenticate against the external file server.
- **Path without filename:** Specifies the path on the file server to the certificate files.
- **Use common certificate configuration:** Enables the use of the system-wide certificate validation settings, as configured under the **System -> Provisioning menu** (see section 6.5.5).
- **Local certificate file:** Specifies the name of the PEM file on the external server including the local certificate or a certificate chain.
- **Private key file:** Specifies the name of the PEM file on the external server including the local key.

6.5.2.12 SNMP

To manage a larger RFP network, an SNMP agent is provided for each RFP. The SNMP agent provides alarm information and allows an SNMP management system (such as "HP Open View") to manage this network. The SNMP sub menu of the OMP provides configuration of SNMP service settings.

For a description of the parameters on the **SNMP** tab, refer to the description of the **SNMP** menu of the OMM Web service (see section 5.4.6).

6.5.2.13 Time zones

The OMM provides all available time zones on the **Time zones** tab. They are set with their known daylight savings time rules adjusted to the Universal Coordinated Time (UTC) by default. The difference to the UTC time is shown in the **UTC difference** field.

In addition, you can configure a new (free) time zone.

The date and time are provided by the OMM to the Mitel 142d and Mitel 600 DECT phones if the DECT phone initiates a DECT location registration. The DECT phone initiates a DECT location registration when:

- subscribing to the OMM
- entering the network again after the DECT signal was lost

- at 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

You can change the time zone rules for up to five time zones. The changes are saved in the configuration file and are restored after each OpenMobility Manager startup.

General

- **Difference local standard time to UTC:** The difference (in minutes) between the local standard time and UTC time.
- **Daylight savings time:** Enables or disables application of Daylight Savings Time (DST) for the time zone. If disabled, the Standard time and Daylight savings time tabs are not accessible.
- **Difference daylight savings time to standard time:** The difference (in minutes) between Daylight Savings Time (DST) and Standard Time for the time zone.

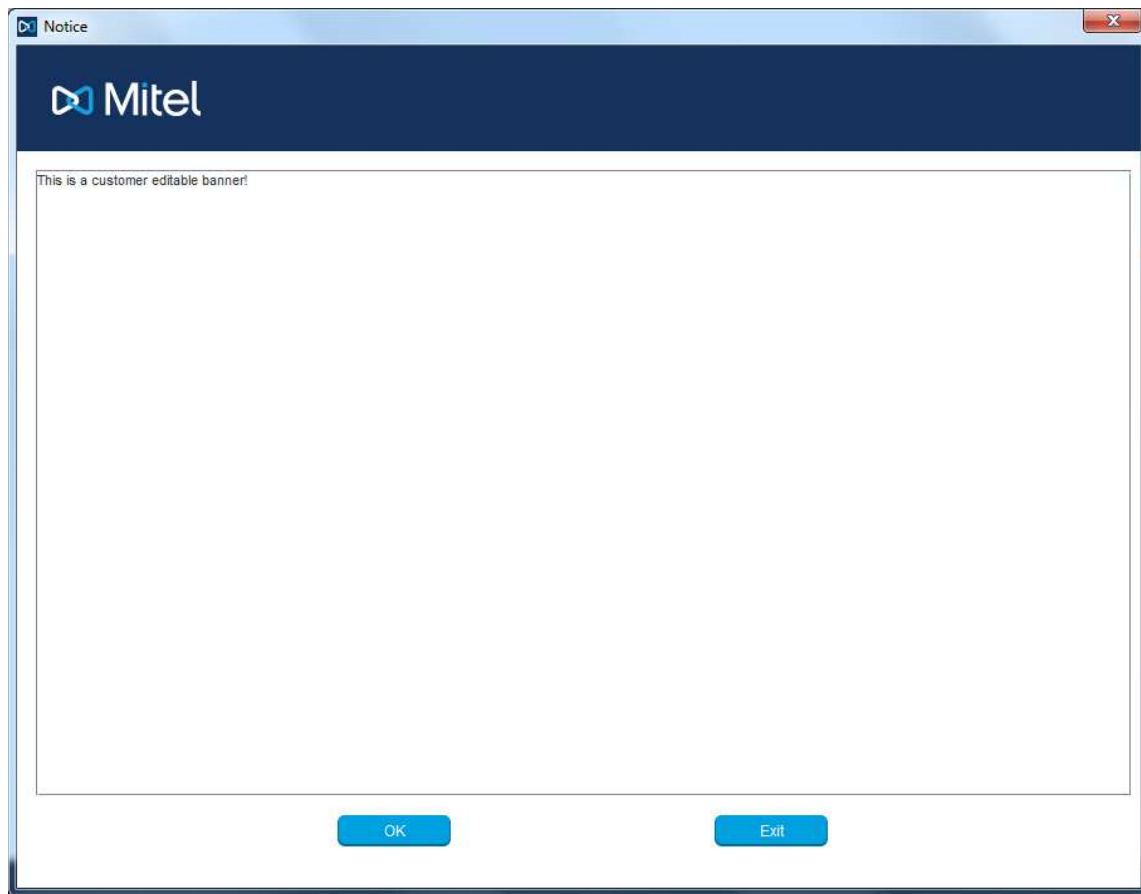
If the **Daylight savings time** parameter on the **General** tab is enabled, you can change the standard time and the daylight savings time (DST) of a time zone in the **Standard time** and **Daylight savings time** tabs. If the time zone has no DST, only the UTC difference can be configured. For the DST both points of time (begin of standard time and begin of daylight savings time) must be specified exactly. Therefore a certain day in the month or a certain week day in a month can be used.

The following commands are available to edit time zones:

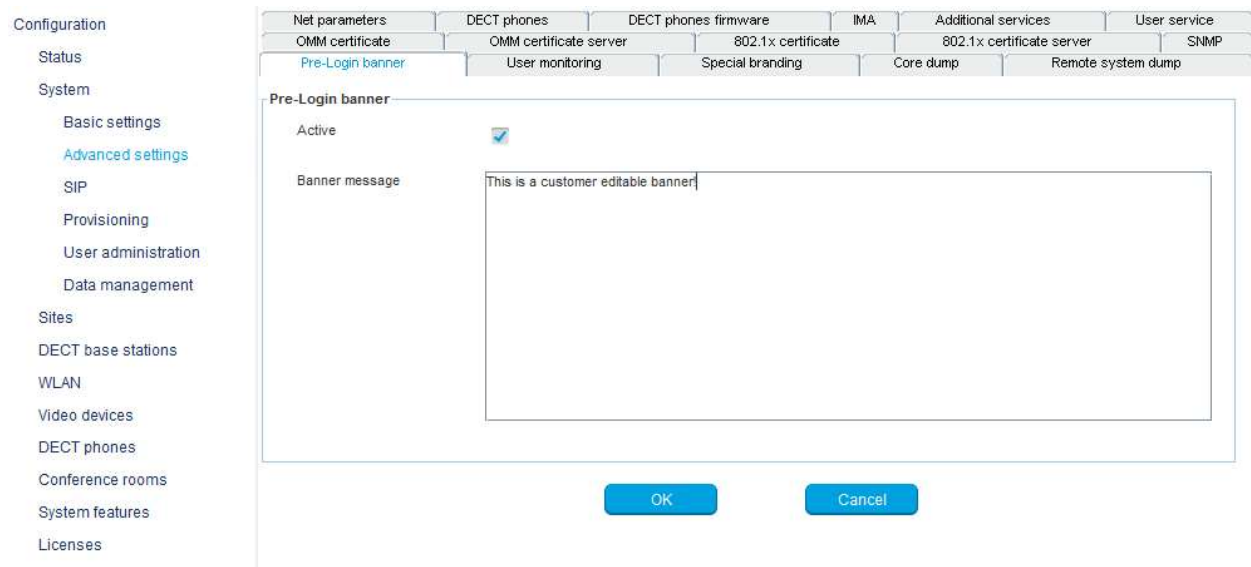
- **OK:** Confirm the changed time zone settings.
- **Cancel:** Cancels the operation and resets the changed time zone back to the default setting.
- **Default:** Resets all individual time zone settings to the default values and deletes the changed time zone rules in the configuration file.

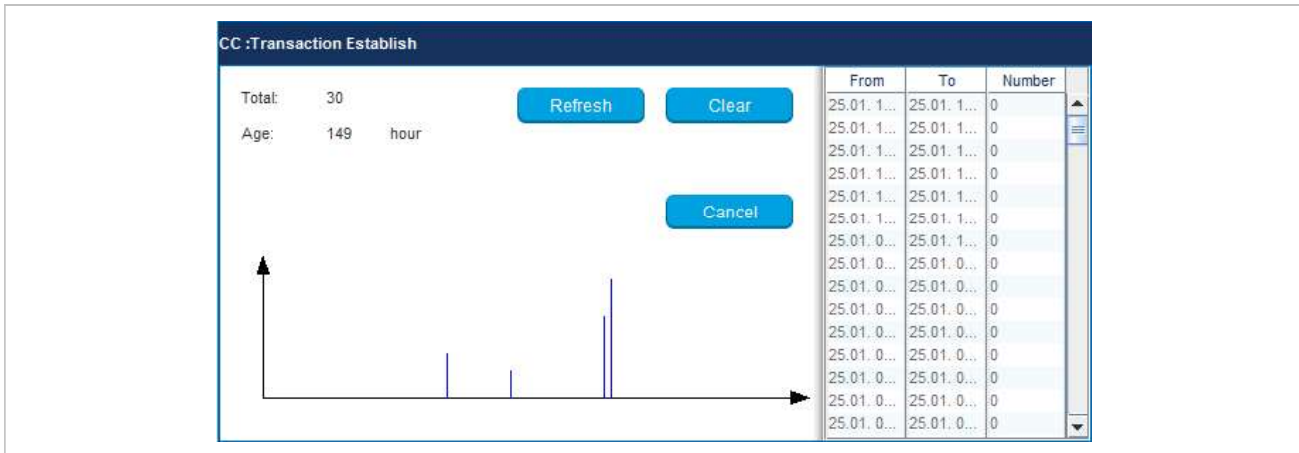
6.5.2.14 Pre-Login banner

There is an optional customer editable banner available, which allows to display security notes or similar on OMP and OMM's Web interface prior to login.



You can modify and activate the banner through OMP.





6.5.4 "SIP" MENU

The **SIP** menu contains global settings for SIP signaling and RTP voice streams.

The screenshot shows the "SIP" configuration menu. On the left is a navigation tree with categories like "Configuration", "Status", "System", "Provisioning", "User administration", "Data management", "Sites", "DECT base stations", "WLAN", "Video devices", "DECT phones", "Conference rooms", "System features", and "Licenses". The "SIP" menu item is selected. The main area shows the "SIP" configuration with several tabs: "Basic settings", "Advanced settings", "Registration traffic shaping", "Backup settings", "RTP settings", and "DTMF settings". The "Basic settings" tab is active, showing fields for "Proxy server" (10.103.35.11), "Proxy port" (5060), "Registrar server" (10.103.35.11), "Registrar port" (5060), "Registration period" (3600 sec), "Globally routable user agent URL" (checked), "Outbound proxy server", "Outbound proxy port" (5060), and "Transport protocol" (UDP). Below this is a "Local port range" section with fields for "PP user UDP/TCP" (5060), "Conference room UDP/TCP" (4060), "PP user TLS" (5061), and "Conference room TLS" (4061). "OK" and "Cancel" buttons are at the bottom.

The SIP menu contains the following tabs:

- Basic settings (see section 6.5.4.1)
- Advanced settings (see section 6.5.4.2)
- Registration traffic shaping (see section 6.5.4.3)
- Backup settings (see section 6.5.4.4)
- RTP settings (see section 6.5.4.5)
- DTMF settings (see section 6.5.4.6)
- Intercom Push-to-talk (see section 6.5.4.7)
- Supplementary services (see section 6.5.4.8)
- Conference (see section 6.5.4.9)

- Security (see section 6.5.4.10)
- Certificate server (see section 6.5.4.11)

6.5.4.1 Basic settings

For a description of the parameters on the **Basic settings** tab, see the description of the **System -> SIP** menu of the OMM Web service. The same parameters are described in the **Basic settings** section (section 5.4.3.1).

In addition, the following parameters (related to SIP multiport support) are available on the **Basic settings** tab:

Local port range

- **DECT phone user UDP/TCP**: The port range to be used for DECT users when UDP/TCP is used as the transport protocol. The default is 5060 – 5060.
- **DECT phone user TLS**: The port range to be used for DECT users when TLS is used as the transport protocol. The default is 5061 – 5061.
- **Conference room UDP/TCP**: The port range to be used for Conference Rooms when UDP/TCP is used as the transport protocol. The default is 4060 – 4060.
- **Conference room TLS**: The port range to be used for DECT users when TLS is used as the transport protocol. The default is 4061 – 4061.

Note: There are certain rules to note when configuring port ranges, see section [2.17](#) for more information.

6.5.4.2 Advanced settings

You can set several additional SIP parameters on the **Advanced settings** tab.

For a description of the parameters on the **Advanced settings** tab, refer to the description of the **System -> SIP** menu of the OMM Web service. The same parameters are described in the **Advanced settings** section (section 5.4.3.2).

In addition, the following parameters are available in the OMP only:

- **X-Aastra-Id info**: Enable or disable inclusion of the private X-Aastra-Id header in each SIP REGISTER message.
- **User agent info – compatibility mode**: If the **User agent info** option is enabled, the OMM sends information on his version inside the SIP User-Agent/Server headers; this parameter ensures backward compatibility with version information used in older SIP-DECT software releases.

6.5.4.3 Registration traffic shaping

Registration traffic shaping parameters allow you to limit the number of simultaneous SIP registrations at startup/fail over of the OMM. This feature is always activated because disabling it may overload the OMM or the call server.

For a description of the parameters on the **Registration traffic shaping** tab, see the description of the **System -> SIP** page of the OMM Web service. The same parameters are described in the **Registration traffic shaping** section (section 5.4.3.5).

6.5.4.4 Backup settings

To increase the operational availability of the system in critical environments like hospitals, the OMM offers a failover redundancy mechanism for the SIP server. In addition to the primary proxy, outbound proxy and registrar server, you can configure two additional levels of backup servers (secondary and tertiary servers).

The OMM failover behavior in detail depends on the backup server settings set here. A full description of the behavior and deployment hints can be found in section [8.20.3](#).

- **Secondary proxy server / port, Secondary registrar server / port, Secondary outbound server / port:** Enter the parameters for the secondary server in these fields.
- **Tertiary proxy server / port, Tertiary registrar server / port, Tertiary outbound server / port:** Enter the parameters for the tertiary server in these fields.

Note: Server addresses can be configured as IP addresses, names or a fully qualified domain names. It is possible to configure a mixture of IP addresses, names or fully qualified domain names for the different servers. If fully qualified domain names are configured and the respective port setting is configured to zero ("0"), DNS SRV queries will be performed to locate a list of servers in the domain (see 0).

- **Failover keep alive:** The keep-alive mechanism allows transferring all users registered on a failed server (failover) to secondary/tertiary servers as well as automatically switching back to primary servers. Otherwise, failover is executed only single users. Enable this option if you want to use this feature (default: off).
- **Failover keep alive time:** For each registration target, a user could be registered successful with, a keep alive procedure is started. Enter the time in this field after which a new keep-alive procedure must be started (1-60 minutes, default 10 min.).

For a detailed description of the keep-alive mechanism see section [8.20.4](#).

6.5.4.5 RTP settings

For a description of the parameters on the **RTP settings** tab, see the description of the **System -> SIP** page of the OMM Web service. The same parameters are described in the **RTP settings** section (section 5.4.3.3).

6.5.4.6 DTMF settings

For a description of the parameters on the **DTMF settings** tab, see the description of the **System -> SIP** page of the OMM Web service. The same parameters are described in the **DTMF settings** section (section 5.4.3.4).

6.5.4.7 Intercom Push-to-talk

You can set global auto-answer settings on the **Intercom Push-to-talk** tab. For more information on this feature, see section [2.31](#).

Incoming calls

- **Auto answer:** Enables or disables auto-answer on incoming calls.
- **Microphone mute:** Enables or disables microphone muting when incoming calls are automatically answered.
- **Warning tone:** Enables or disables warning tone on incoming call. A short ringtone is played if there are no active calls. If there is an active call in a “barge in” situation, the ringing will be in-band.
- **Allow barge in:** Allows/disallows “barge-in” on existing calls.

Outgoing calls

- **Initialization prefix for push-to-talk:** String to be entered when initiating an intercom call. An empty string indicates that the DECT phone cannot initiate an intercom call.

6.5.4.8 Supplementary services

For a description of the parameters on the **Supplementary services** tab, see the description of the **System -> SIP** page of the OMM Web service. The same parameters are described in the **Supplementary Services** section (section 5.4.3.6).

6.5.4.9 Conference

You can define the conference mode globally for all SIP-DECT users on the **Conference** tab. For more information on the Conferencing feature, see section [8.21](#).

- **Server type:** Specifies the operational mode for the conference server. Available options are:
 - **None:** Neither external nor internal conference server is used.
 - **Integrated:** The conference server integrated in the SIP-DECT system is used.
 - **External:** An external conference server (e.g., Broadsoft) is used.
 - **External – Blind Transfer:** An external conference server is used (e.g. MiVoice Business). The initiation of the conference is signaled as a blind transfer to the destination specified in the URL parameter.
- **URL:** Specifies the URL for the conference server.

6.5.4.10 Security

For a description of the parameters on the **Security** tab, see the description of the **System -> SIP** page of the OMM Web service. The same parameters are described in the **Security** section (section 5.4.3.8) and the **Manual Import** section (section 5.4.3.10).

6.5.4.11 Certificate server

For a description of the parameters on the **Certificate server** tab, see the description of the **System -> SIP** page of the OMM Web service. The same parameters are described in the **Certificate server** section (section 5.4.3.9).

6.5.5 "PROVISIONING" MENU

SIP-DECT supports provisioning through external configuration files. With SIP-DECT 6.0 or later, you can configure a URL for an external file server, from which all configuration files can be downloaded. The configured provisioning server URL is used for secure connections to the file server to retrieve configuration or firmware files.

The **Provisioning** menu contains settings related to the provisioning server.

The screenshot shows the Provisioning menu with the following settings:

- Configuration files URL:**
 - Active:
 - Protocol: HTTPS
 - Port:
 - Server:
 - Path: /pdect.cfg, /<MAC>.cfg, /<PARK>.cfg ...
- SSL settings:**
 - Validate certificates:
 - Validate expires:
 - Validate host name:
 - Allow unconfigured trusted certificates:
 - Import certificates with first connection:
 - SSL version: Auto
- Daily automatic reload of configuration and firmware files:**
 - Active:
 - Time of day: 00 : 00

The Provisioning menu contains the following tabs:

- Provisioning (see section 6.5.5.1)
- Provisioning certificate (see section 6.5.5.2)
- Certificate server (see section 6.5.5.3)
- System credentials (see section 6.5.5.4)

6.5.5.1 Provisioning

Configuration files URL

- **Active:** Enable the configuration file URL feature.
- **Protocol:** The protocol to be used to fetch the configuration files.
- **Port:** Provisioning server's port number.
- **Use default port:** If selected, the default port associated with the selected protocol is used.

- **Server:** IP address or name of the provisioning server.
- **Path:** Path to the configuration and resource files on the provisioning server.

SSL settings

- **Validate certificates:** Enables or disables certificate validation. If enabled, the server certificate is validated against trusted CA's (signed by a CA from the Mozilla CA certificate list) and the configured trusted certificates.
- **Validate expires:** Enables or disables the validation of certificate expiry. When this parameter is enabled, the client verifies whether or not a certificate has expired prior to accepting the certificate.
- **Validate host name:** Enables or disables the validation of hostnames on the OMM.
- **Allow unconfigured trusted certificates:** If enabled, this parameter disables any server certificate validation as long as no trusted certificate was imported into the OMM. AXI commands in a received configuration file may import such trusted certificates into the OMM.
- **Import certificates with first connection:** If enabled (in conjunction with the Allow unconfigured trusted certificates parameter), the trusted certificate will be imported from the cert chain delivered in the server response without any validation, as long as no trusted certificate was imported previously into the OMM.
- **SSL version:** The SSL protocol version to use for the configuration file server connection. Available options are: TLS1.0, TLS1.1, TLS1.2 or AUTO, where AUTO accepts all protocol versions.

Daily automatic reload of configuration and firmware files

- **Active:** Enables automatic reload of the configuration and resource files on a daily basis, at the specified time.
- **Time of day:** Time for scheduled reload of configuration and firmware files.

6.5.5.2 Provisioning certificates

Provisioning certificates are used for secure connections to configuration or firmware file servers that support mutual authentication.

A trusted certificate chain is used by the OMM to validate the server. This is required if the server has no certificate derived from a trusted CA root certificate, where the OMM uses the Mozilla CA Certificate List. If no server certificate is available, the validation against trusted and CA certificates can be disabled in the certificate validation options (only encrypted TLS connection).

The local certificate chain plus the private key are provided from the OMM to servers requesting mutual authentication. The private key file may be password protected.

6.5.5.3 Certificate server

The provisioning certificates can be updated automatically through configuration of a secure provisioning certificate server URL.

- **Active:** Enable automatic updating of certificates the feature.
- **Protocol:** Specifies the preferred protocol (FTP, TFTP, FTPS, HTTP, HTTPS, SFTP)
- **Server:** Specifies the name or IP address of the external file server.

- **Port:** Specifies the certificate server's port number
- **Use default port:** If selected, the default port associated with the selected protocol is used.
- **User name:** Specifies the user name to authenticate against the external file server.
- **Password:** Specifies the password to authenticate against the external file server.
- **Password confirmation:** Confirms the password to authenticate against the external file server.
- **Path without filename:** Specifies the path on the file server to the certificate files.
- **Use common certificate configuration:** Enables the use of the system-wide certificate validation settings, as configured on the **System -> Provisioning -> Provisioning certificates** page (see section 6.5.5.2)
- **Trusted certificate file:** Specifies the name of the PEM file on the specified server, including the trusted certificates.
- **Local certificate file:** Specifies the name of the PEM file on the external server including the local certificate or a certificate chain.
- **Private key file:** Specifies the name of the PEM file on the external server including the local key.

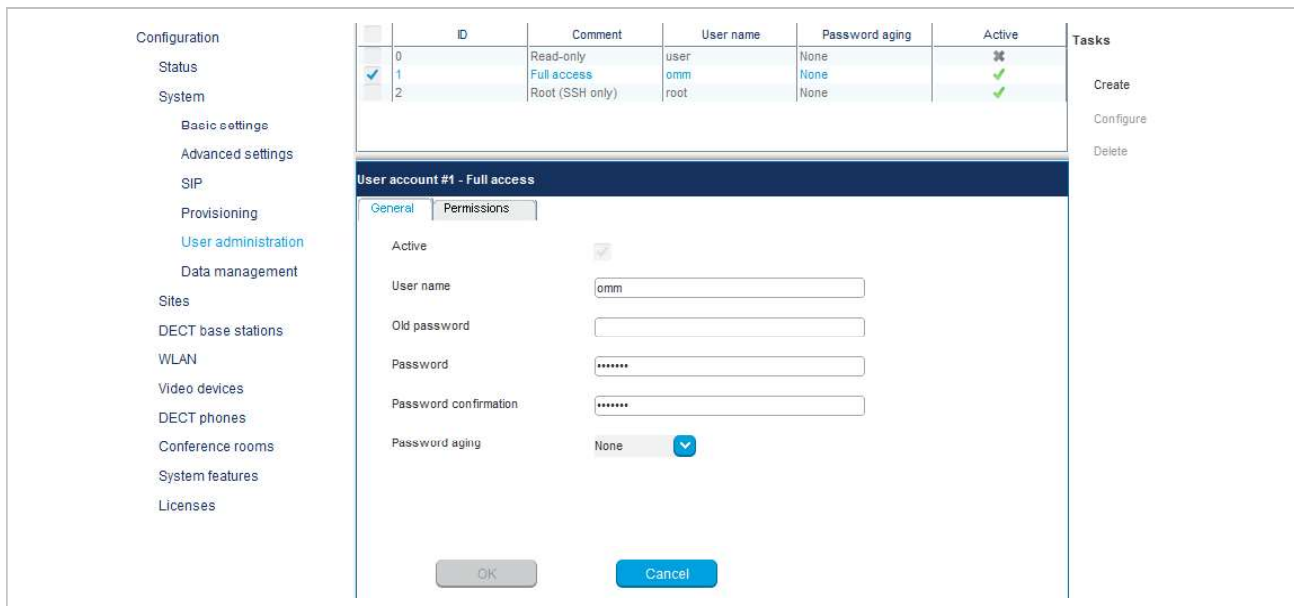
6.5.5.4 System credentials

System credentials are used to retrieve configuration and resource files from the configured provisioning server for protocols supporting authentication or servers requesting authentication. For HTTP/HTTPS, basic and digest authentication are supported.

- **User name:** Specifies the user name for authentication against the provisioning server.
- **Password:** Specifies the password for authentication against the provisioning server
- **Password confirmation:** Confirms the password for authentication against the provisioning server.

6.5.6 “USER ADMINISTRATION” MENU

In the **User administration** menu you configure the OMM user accounts.



The three user accounts “Full access”, “Read-only” and “Root (ssh only)” available via the **User administration** page of the OMM Web service can also be configured in the OMP. These three predefined user accounts cannot be removed or renamed. Only the “Read-only” account can be activated and deactivated. The permissions are fixed. This is consistent with the OMM WEB service. The meaning of the different account types is described in section [8.17.1](#). In addition, the OMP allows to create additional user accounts (login and password) and to assign specific permissions.

The tasks which can be performed are mode-dependant.

Configuration mode	Monitor mode	See section
Create: Create new user account		6.5.6.1
Configure: Configure selected user account in detail panel		6.5.6.2
	Show details: Shows selected user account in detail panel	6.5.6.3
Delete: Delete selected user account		6.5.6.4

6.5.6.1 Creating New User Accounts

It is possible to create additional user accounts (login and password) and to assign specific permissions. These accounts are mainly designed to have specific login data and permissions for applications which are using OM AXI to connect with the OMM.

Note: Individual user accounts cannot be used for a login to the OMM Web service nor SSH.

ID	Comment	User name	Password aging	Active
0	Read-only	user	None	<input checked="" type="checkbox"/>
1	Full access	omm	None	<input checked="" type="checkbox"/>
2	Root (SSH only)	root	None	<input checked="" type="checkbox"/>

New user account

General | Permissions

Active

User name

Old password

Password

Password confirmation

Password aging

OK Cancel

Adding individual user accounts is only possible in **Configuration Mode**. To add a user account, do the following:

- 1 In the **Tasks** bar click on the **Create** command.
The **New user account** panel opens. It provides various tabs where the account data must be entered.
- 2 Configure the user account, see parameter description below.
- 3 Press the **OK** button.

The following parameters can be set in the tabs of the **New user account** panel:

General

For a description of the parameters which can be set in the **General** tab, see the description of the **User administration** page of the OMM Web service (see section 6.5.6.).

Permissions

The permissions for an individual user account can be set independent from any license status even if some of the permissions can only be used with an appropriate license.

If an application connects with the OMM via OM AXI, then the permissions been sent from the OMM to the application is the result of the configured permissions for this account and the actual license status. For more information please see the OM Application XML Interface (OM AXI) specification /31/.

The permissions have the following meaning:

Permission	Description
Read	Read OMM data (OM AXI get requests)
Write	Set OMM data (OM AXI set requests)
Messaging info	Sent messages with priority "Info"
Messaging	Sent messages with priority "Low", "Normal" and "High"
Messaging emergency	Sent messages with priority "Emergency"
Messaging locating	Sent messages with priority "LocatingAlert"
Locating	Permission to query the position of DECT phones and to track DECT phone positions
Monitoring	Permission to monitor various technical aspects of the mobility system
Video	Permission for video streaming

6.5.6.2 Changing a User Account

Changing user accounts is only possible in **configuration mode**. To change the configuration of an existing user account, do the following:

- 1 Select the appropriate user account in the account table.
- 2 In the **Tasks** bar click on the **Configure** command.
- 3 Change the user account parameters (see parameter descriptions in section 6.5.6.1).
- 4 Press the **OK** button.

Please note: The predefined user accounts "Full access", "Read-only" and "Root (ssh only)" user accounts cannot be renamed. Also their permissions are fixed and cannot be changed.

6.5.6.3 Viewing User Account Details

You can view the configuration of a user account in **monitor mode**. Proceed as follows:

- 1 Select the appropriate user account in the table.
- 2 In the **Tasks** bar click on the **Show details** command.
The user account data is displayed in the user account detail panel.
- 3 To close the user account detail panel, click the **Cancel** button.

6.5.6.4 Deleting User Accounts

Deleting user accounts is only possible in **configuration mode**. To delete one or more existing user accounts proceed as follows:

- 1 Select the appropriate account(s) in the user account table by activating the corresponding checkbox(es).
- 2 In the **Tasks** bar click on the **Delete** command.
- 3 Confirm the displayed prompt with **OK**.

Please note: The predefined user accounts “Full access”, “Read-only” and “Root (ssh only)” user accounts cannot be removed.

6.5.7 “DATA MANAGEMENT” MENU

The **Data management** menu provides access to data related to import and export features.

The Data management contains the following tabs:

- **Auto DB export** (see section 6.5.7.1)
- **User data import** (see section 6.5.7.2)
- **DECT phones synchronization** (see section 6.5.7.3)
- **Manual DB import** (see section 6.5.7.4)
- **Manual DB export** (see section 6.5.7.5)
- **Maintenance** (see section 6.5.7.6)
- **IMA** (see section 6.5.7.7)

6.5.7.1 Automatic DB export

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

Please note: Synchronization with an NTP server is mandatory for an automatic database export. For NTP server configuration, see section [8.5.4](#) and section [5.4.1.16](#).

For a description of the parameters on the **Automatic DB export** tab, see the description of the **System** -> **Data management** page of the OMM Web service. The same parameters are described in the **Automatic Database Export** section (section 5.4.7.3).

6.5.7.2 User data import

The user data import feature allows the import of user data from an external provisioning server.

- **Configure specific source:** Enables the specific URL to an external file server for retrieving the user data file.
- **Protocol:** Specifies the preferred protocol.
- **Port:** Specifies the port on the server.
- **Server:** Specifies the IP address or the name of the server.
- **User name, Password, Password confirmation:** Specifies the credentials for the server.
- **Path:** Specifies the path to the file containing the user data.
- **Use common certificate configuration:** Enables the use of the system-wide certificate validation settings, as configured on the System -> Provisioning -> Certificates page (see section 5.4.2.8).

Please note: If no credentials are specified for secure protocols, the system credentials are automatically used (see section [5.4.2.2](#)). If the system credentials must not be used, the user name and password must be explicitly set here even for anonymous settings.

For further information on the user data import, see the *OM DECT Phone Sharing and Provisioning Guide*.

6.5.7.3 DECT phones synchronization

The user data synchronization feature ensures that all user and device database information is distributed to all OMM instances in the system. Each peripheral OMM must have a connection to the AXI interface of the central OMM (and the standby central OMM, if configured) to send and receive updated user data information. Specify the same user credentials used to access the central OMM via the OMP.

For more information on this feature, see section [8.16](#).

- **Activate synchronization:** Enable user data synchronization for the OMM.
- **OMM1:** Specifies the IP address of the central OMM.
- **OMM2:** Specifies the IP address of a second central OMM, in the case of a standby configuration.
- **User name:** Specifies the user name required to access the central OMM.
- **Password:** Specifies the password required to access the central OMM.
- **Password confirmation:** Confirms the password required to access the central OMM.

6.5.7.4 Manual DB import

The manual database import feature allows the import of an OMM database.

Please note: A manual import of a database results in a reset of the OMM.

For a description of the parameters on the **Manual DB import** tab, see the description of the **System -> Data management** page of the OMM Web service. The same parameters are described in the **Manual Database Import** section (section 5.4.7.1).

6.5.7.5 Manual DB export

The manual database export feature allows a manual database backup to an external server.

For a description of the parameters on the **Manual DB export** tab, see the description of the **System -> Data management** page of the OMM Web service. The same parameters are described in the **Manual Database Export** section (section 5.4.7.2).

6.5.7.6 Maintenance

In the **Maintenance** panel, you can perform a system dump, for example, for product support information purposes. A file “sysdump.txt” is created in the selected directory. Click the **Directory** button to select the directory, then click the **Download** button to start the system dump.

6.5.7.7 IMA

You can upload an IMA configuration file manually. To validate the existing configuration, the IMA configuration can be also downloaded. An uploaded IMA configuration may be overwritten if a server for the IMA configuration file is configured or if the ‘ima.cfg’ is available on the provisioning server. The IMA configuration can be deleted regardless of its source.

- **Config file import**

To upload an IMA configuration file, click the **File** button to browse to the file, then click **Import**.

- **Config file export**

To download the current IMA configuration file, click the **Directory** button to select the destination directory, then click **Export**.

- **Delete config file**

To delete the IMA configuration file, click **Delete**.

6.5.8 “EVENT LOG” MENU

The **Event Log** menu provides information about system events. The menu is only available in **Monitor Mode**.

	Severity	Subsystem	Count	Time	Event	Tasks
Monitoring	0	STB*	1	2015/01/19 15:56:50.0...	2 OMM(s) on comman...	
Status	2	AXI	1	2015/01/19 15:57:33.0...	[193] New secure co...	Show details
System	2	AXI	1	2015/01/19 15:57:33.1...	[193] Remote host clo...	
Basic settings	3	IPL	1	2015/01/21 21:00:50.2...	RFP(0000) reconnected	Clear all
Advanced settings	3	IPL	1	2015/01/21 21:00:53.6...	RFP(0001) reconnected	
Statistics	0	STB*	1	2015/01/21 21:00:56.5...	Activating former stan...	
SIP	0	CNF	1	2015/01/21 21:00:56.5...	SIP-DECT 6.0RC4 Buil...	
Provisioning	2	AXI	1	2015/01/21 21:00:56.9...	[194] New connection...	
User administration	2	AXI	1	2015/01/21 21:00:57.6...	[198] New connection...	
Data management	2	AXI	1	2015/01/21 21:00:57.7...	[199] New connection...	
Event log	3	STB	1	2015/01/21 21:00:58.2...	No Connection to stan...	
Sites	2	AXI	1	2015/01/21 21:01:01.9...	[201] New connection...	
DECT base stations	2	AXI	1	2015/01/21 21:01:16.6...	[202] New secure co...	
WLAN	2	IPL	1	2015/01/21 21:01:19.3...	2 of 12 RFPs connected	
Video devices	2	AXI	1	2015/01/21 21:01:20.7...	[204] New connection...	
DECT phones	3	STB	1	2015/01/21 21:01:22.4...	Broken Connection to ...	
Conference rooms	2	AXI	1	2015/01/21 21:29:05.4...	[203] New secure co...	
System features	3	DSIP	1	2015/01/21 21:36:26.7...	SIP registration to 10...	
Licenses	2	AXI	1	2015/01/21 22:28:44.8...	[203/omm] Remote ho...	
	2	AXI	1	2015/01/21 22:29:09.0...	[203] New secure co...	
	2	AXI	1	2015/01/21 22:29:09.6...	[203] Remote host clo...	
	2	AXI	1	2015/01/21 22:29:14.5...	[203] New secure co...	
	2	AXI	1	2015/01/21 22:34:26.0...	[203/omm] Remote ho...	
	2	AXI	1	2015/01/21 22:37:33.8...	[203] New secure co...	
	3	DSIP	2	2015/01/22 10:25:38.0...	SIP registration to 10...	
	3	AXI	1	2015/01/22 11:30:35.4...	[203] Disconnect clie...	
	2	AXI	1	2015/01/22 11:30:35.4...	[203/omm] Connection...	
	3	DSIP	1	2015/01/22 11:46:19.9...	SIP registration to 10...	
	2	AXI	1	2015/01/22 14:58:21.1...	[203] New secure co...	
	2	AXI	1	2015/01/22 15:19:26.9...	[202/omm] Remote ho...	
	2	AXI	1	2015/01/22 15:20:59.5...	[202] New secure co...	
	3	AXI	1	2015/01/22 17:38:20.4...	[203] Disconnect clie...	

6.5.8.1 Event log detail panel

Event log

General

Severity:

Subsystem:

Count:

Time:

Event:
[199] New connection from 10.37.18.32:58185

6.6 “SITES” MENU

DECT base stations can be grouped into different sites. The **Sites** menu allows configuration and display of configured sites. An empty system has one predefined site (ID: 1) named “default”. The system requires a minimum of one site.

ID	Name	Hi-Q audio	Enh. DECT sec...	SRTP	Terminal video	Number of RFPs
1	default	✘	✘	✔	✘	10
3	Real RFP	✘	✘	✔	✘	2

Site #3

General

Name:

Hi-Q audio technology:

Enhanced DECT security:

Terminal video:

SRTP: Preferred

Changing site parameters, may restart radio fixed parts in this site.

A site contains the following parameters:

- **ID:** 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.
- **Name:** The name of the site.
- **Hi-Q audio technology / Enhanced DECT security / Terminal video / SRTP:** These capabilities must be enabled or disabled specific for every site.
- In sites, which are configured to provide this functionality, exclusively 3rd and 4th generation RFPs are applicable.
- In sites without this capability, it is allowed to mix these new RFP types with 2nd generation RFPs.
- **Number of RFPs:** The number of RFPs which are assigned to this site.

You can perform the following tasks:

- **Create:** Create a new site in the General tab.
- **Configure:** Configure an existing site in the General tab.
- **Delete:** Delete selected sites (only sites without assigned RFPs can be deleted).
- **Show details** (only in **Monitor Mode**): Shows configuration of a selected site in the **General** tab.

6.7 “DECT BASE STATIONS” MENU

DECT base stations can be configured and viewed in the **DECT base stations** menu.

Configuration mode	Monitor mode	See section
Device list	Device list	6.7.1
Paging areas		6.7.2
Capturing		6.7.3
Enrolment		6.7.4
Export		6.7.5
	Sync view	6.7.6
	Statistics	6.7.7

6.7.1 “DEVICE LIST” MENU

The **Device list** panel displays all configured DECT base stations in a table. The device list is available in **Configuration Mode** and **Monitor Mode**.

Configuration	RFP ID	Name	MAC address	IP address	DECT cluster	Paging area	HW type	Conne...	Active	Tasks
Status	0x000	SVE RFP1	00:30:42:18:1D...	10.37.18.31	1	0	RFP 35	✓	✓	
	0x001	SVE RFP2	00:30:42:18:20...	10.37.18.32	1	0	RFP 35	✓	✓	Create
System	0x002	simu	01:02:03:04:05...	0.0.0.0	5	0	RFP 32	✗	✗	Configure
	0x003	simu	01:02:03:04:05...	0.0.0.0	5	0	RFP 32	✗	✗	
Sites	0x004	simu	01:02:03:04:05...	0.0.0.0	5	0	RFP 32	✗	✗	Delete
DECT base stations	0x005	simu	01:02:03:04:05...	0.0.0.0	5	0	RFP 32	✗	✗	
	0x006	simu	01:02:03:04:05...	0.0.0.0	5	0	RFP 32	✗	✗	Filter
Device list	0x007	simu	01:02:03:04:05...	0.0.0.0	5	0	RFP 32	✗	✗	
	0x008	simu	01:02:03:04:05...	0.0.0.0	5	0	RFP 32	✗	✗	Select columns
Paging areas	0x009	simu	01:02:03:04:05...	0.0.0.0	5	0	RFP 32	✗	✗	
Capturing	0x00A	simu	01:02:03:04:05...	0.0.0.0	5	0	RFP 32	✗	✗	
Enrolment	0x00B	simu	01:02:03:04:05...	0.0.0.0	5	0	RFP 32	✗	✗	
Export										

The **Active** column shows the following states:

- ✗ – DECT is not enabled and/or RFP not connected.
- ✗ – DECT is enabled and RFP connected, but DECT has not been activated yet.
- 🔍 – DECT is enabled and RFP is connected, but RFP is not synchronized and searches for other synchronized RFPs.
- ✓ – DECT is enabled and RFP is connected and synchronized.

Note: If the **Active** column is not displayed, you can activate it in the **Select columns** dialog, see section 6.7.1.7.

The tasks you can perform are mode-dependant.

Configuration mode	Monitor mode	See section
Create: Create new base station in detail panel		6.7.1.2
Configure: Configure selected base station in detail panel		6.7.1.3

Configuration mode	Monitor mode	See section
	Show details: Show selected base station in detail panel	6.7.1.4
Delete: Delete selected RFP		6.7.1.5
	Show sync. relations: Show synchronization relation for selected RFPs	6.7.1.6
Select columns: Select columns/parameters to be shown in RFP table	Select columns: Select columns/parameters to be shown in RFP table	6.7.1.7
Filter: Show only RFP datasets in table which contain a special search string	Filter: Show only RFP datasets in table which contain a special search string	6.7.1.8

6.7.1.1 DECT Base Station Detail Panel

The DECT base station detail panel is used for configuration/display of RFP settings and creation of new RFP datasets.

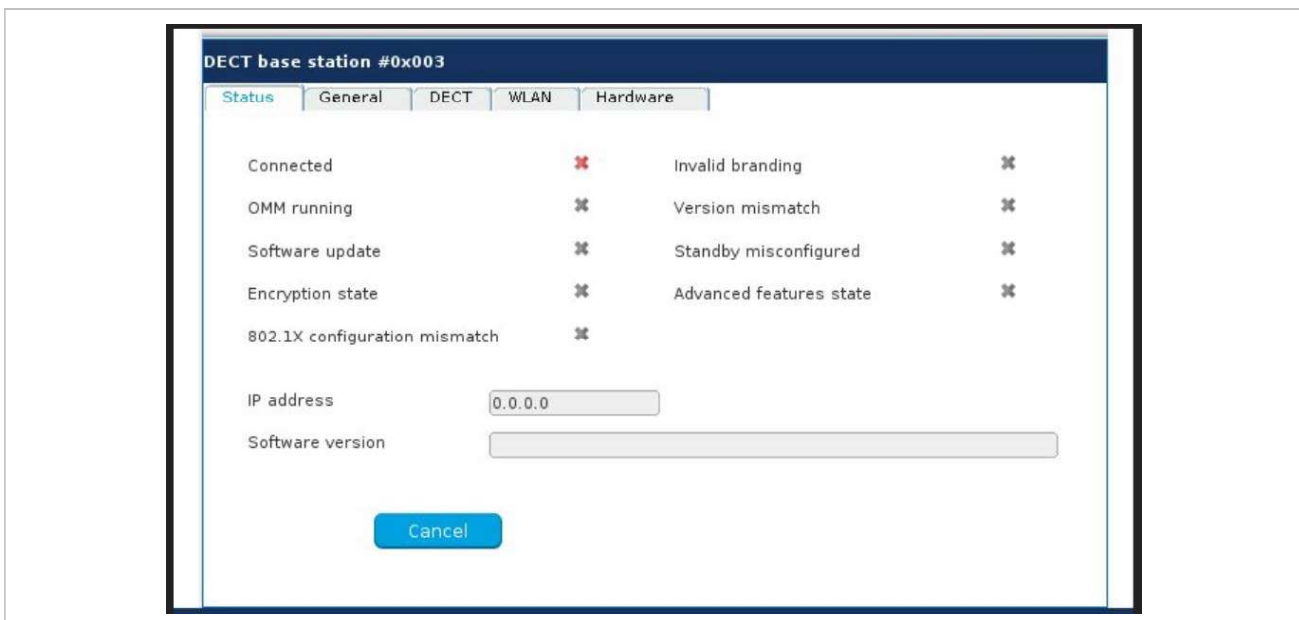
To call up the DECT base station detail panel, do one of the following:

- Choose one of the commands in the task bar on the right of the **DECT base stations** panel (**Create**, **Configure**, or **Show details**)
- Double-click on the appropriate RFP entry in the RFP table.

The DECT base station detail panel contains the following parameter groups sorted in different tabs.

“Status” tab

The Status tab is only available in **Monitor Mode**, and shows system status information for the selected DECT base station.



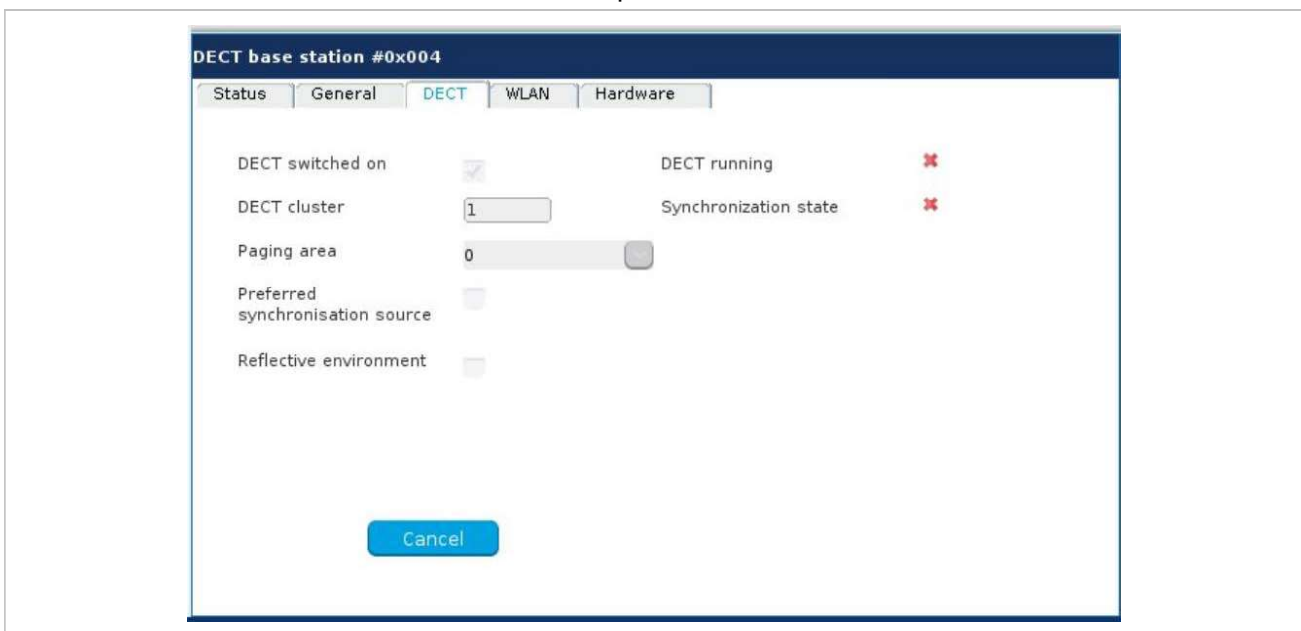
“General” tab

This tab contains the general DECT base station parameters.



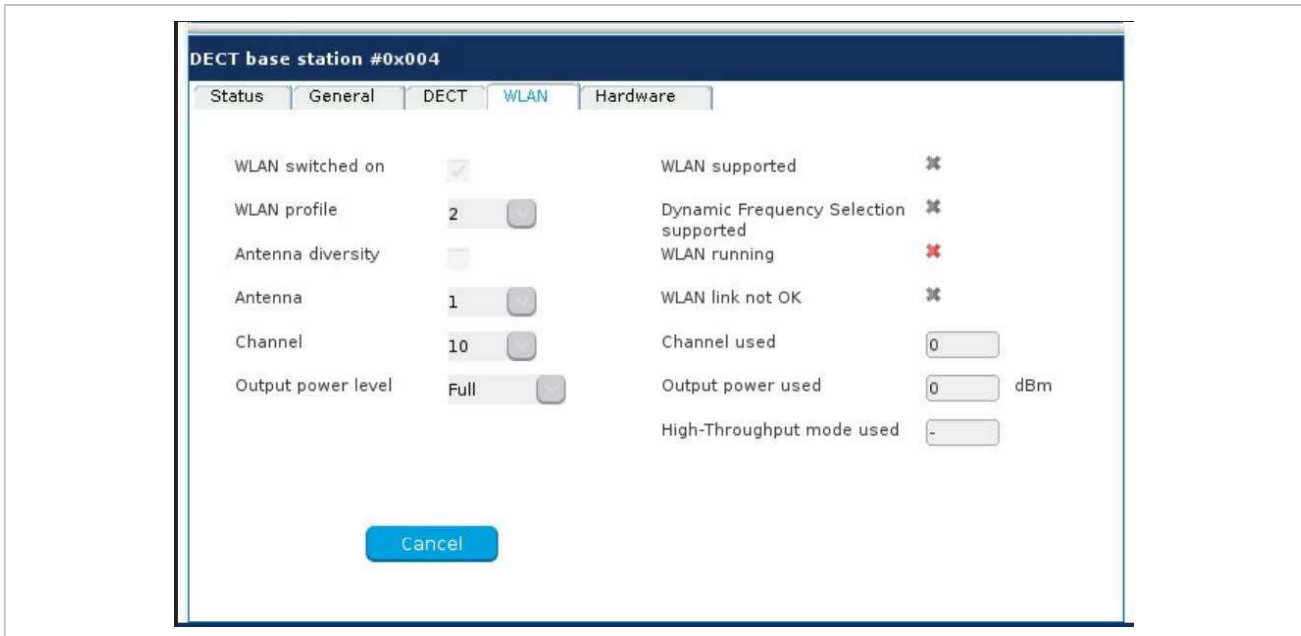
“DECT” tab

This tab contains the DECT base station's DECT parameters.



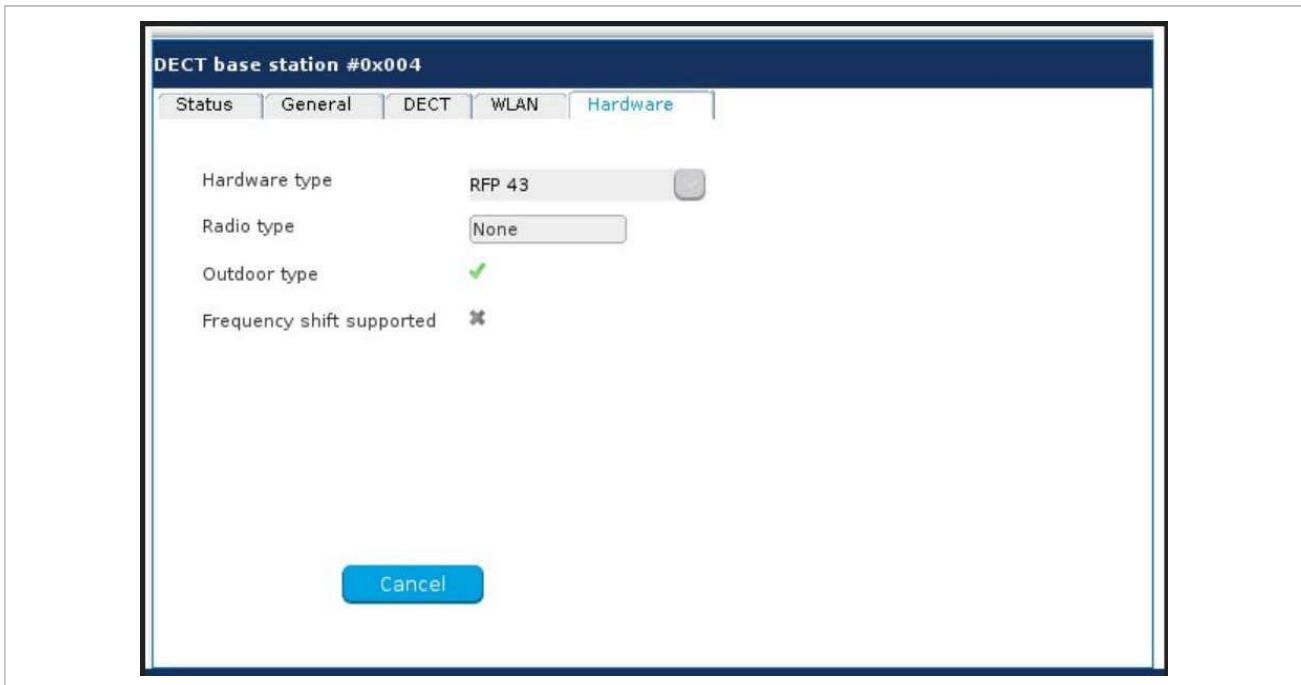
“WLAN” tab

This tab contains the DECT base station's WLAN parameters. Settings in the **WLAN** tab apply to RFP 42/43/48 WLAN base stations only.



“Hardware” tab

In **Monitor Mode**, this tab shows hardware information of the selected DECT base station.



In configuration mode, the DECT base station **Hardware type** can be set if it is connecting to the OMM for the first time. Once the correct hardware type is received from the DECT base station, you cannot change it.

6.7.1.2 Adding New DECT Base Stations

You must be in **Configuration Mode** to add a new DECT base station. To add a DECT base station to the list of known base stations, do the following:

- 1 Click **Create** under the Tasks lists on the right side of the **DECT base stations** window.

The **New radio fixed part** panel opens.

- 2 Configure the DECT base station (see parameter descriptions below).
- 3 Click **OK**.

The following parameters can be set in the tabs of the **New DECT base station** panel:

“General” tab

- **Name:** The name for the RFP.
- **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.
- **Site:** If several sites exist, select the site the RFP is assigned to.
- **Building, Floor, Room:** For easier localization of the RFP you can enter data in these fields.
- **Conference channels:** Activate this option to enable the RFP to provide channels for 3-way conferencing. This option is available for 3rd or 4th generation RFPs (see section [8.21.2](#)).

“DECT” tab

- **DECT switched on:** 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.
- **Paging area:** Enter the paging area, the RFP is assigned to.

Note: The **Paging area size** is set in the **DECT** tab of the **System settings** menu (see section 6.5.1). The assignment between RFPs and paging areas can be changed in the **Paging areas** menu (see section [6.7.2](#)).

- **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 see section [8.2](#).
- **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 DECT phone or RFP using multipath propagation. Calls may have permanent drop outs while moving and high error rates on the RFPs and DECT phones.

For such environment Mitel has developed the DECT XQ enhancement into base stations and the Mitel 600 DECT phones 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 32/34 respectively. RFP 42 WLAN, RFP 35/36/37 IP resp. RFP 43 WLAN or RFP 44/45/47 respectively. RFP 48 WLAN is reduced to 4 calls at the same time.

Please note: The RFPs and DECT phones 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” tab

Settings in the **WLAN** tab apply to RFPs of the type “RFP 42/43/48 WLAN”, “RFP 43 WLAN” and “RFP 48 WLAN” only. For details about WLAN configurations please see section [8.18](#).

Please note: WLAN properties can only be set if the correct hardware type is configured in the **Hardware** tab.

- **WLAN switched on:** The WLAN functionality for an RFP 42 WLAN, RFP 43 WLAN or RFP 48 WLAN can be switched on/off.
- For a description of the other parameters which can be set in the **WLAN** tab, see the description of the **DECT base stations** page of the OMM Web service (see section 5.6.3). The corresponding parameters can be found there in the **WLAN** settings section.

“Hardware” tab

WLAN properties can only be set if the correct hardware type is configured. This can be done manually before an RFP connects with the OMM and an automatic detection is possible (**Auto** setting).

6.7.1.3 Changing DECT base station configuration

Changing RFPs is only possible in **configuration mode**. To change the configuration of an existing RFP, do the following:

- 1 Select the appropriate RFP in the RFP table.
- 2 Click **Configure** under the Tasks lists on the right side of the **DECT base stations** window.
The DECT base station detail panel opens.
- 3 Change RFP parameters (see descriptions in section 6.7.1.2).
- 4 Click **OK**.

6.7.1.4 Viewing DECT base station Details

You can view the configuration of an RFP in **Monitor Mode**. Proceed as follows:

- 1 Select the appropriate RFP in the RFP table.
- 2 Click **Show details** under the Tasks lists on the right side of the **DECT base stations** window.
The DECT base station detail panel opens.
- 3 To close the RFP detail panel, click **Cancel**.

6.7.1.5 Deleting DECT base stations

You can only delete DECT base stations in **Configuration Mode**. To delete a DECT base station, do the following:

- 1 Select the DECT base station (s) in the table by selecting the corresponding checkbox(es).

- 2 Click **Delete** under the Tasks lists on the right side of the **DECT base stations** window.
The **Delete selected DECT base station(s)** dialog opens showing a confirmation prompt.
- 3 Click **OK** to confirm.

Please note: License DECT base stations cannot be deleted.

6.7.1.6 Showing Synchronization Relations

You can view the synchronization relations of a DECT base station in **Monitor Mode**. Do the following:

- 1 Select the appropriate RFPs in the RFP table. At least two RFPs must be selected to show their synchronization relations.
- 2 Click **Show sync. Relations** under the Tasks lists on the right side of the **DECT base stations** window.

The view switches to the **Sync view** menu . For further information see section 6.7.6.

6.7.1.7 Selecting Columns

You can customize the parameters shown in the DECT base station table:

- 1 Click **Select columns** under the Tasks lists on the right side of the **DECT base stations** window.
The **Select columns** dialog opens.
- 2 Select the columns that shall be shown by activating the appropriate checkboxes.
- 3 Click the **OK** button.

The DECT base station table is updated accordingly.

6.7.1.8 Filtering the DECT base station table

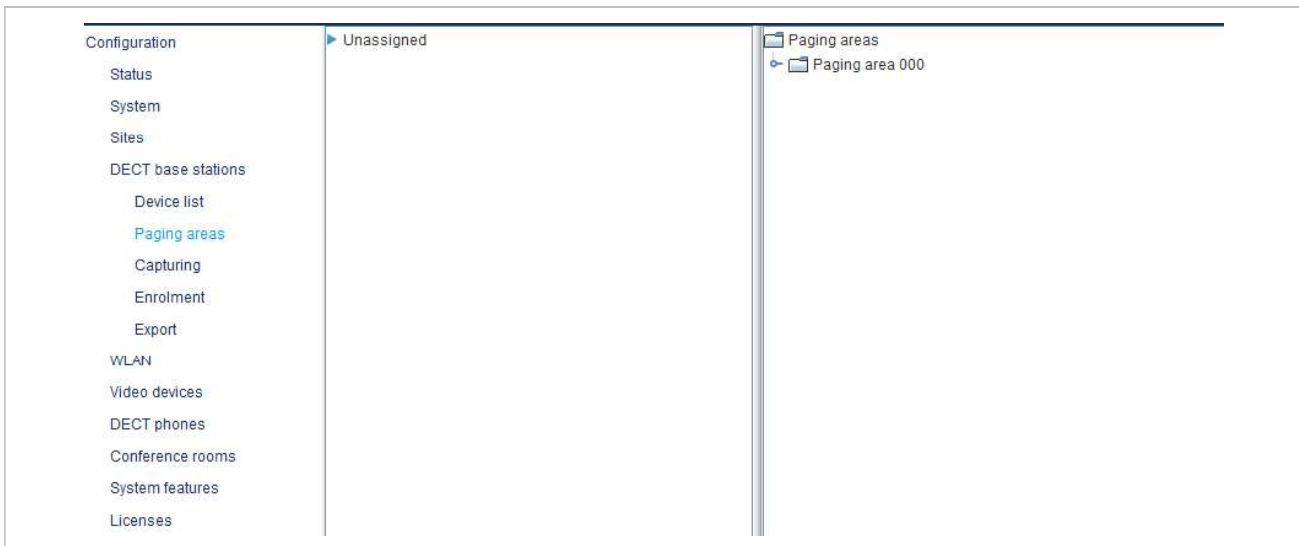
You can filter the list of DECT base station datasets shown in the table by using a filter.

- 1 Click **Filter** under the Tasks lists on the right side of the **DECT base stations** window.
The **Filter** dialog opens.
- 2 Enter the search string that serves as filter criterion. You can enter digits and characters. The search is case sensitive.
- 3 Click on the **Filter** button.
The **Filter** dialog is closed and the table is adjusted accordingly.
- 4 To reset the filter, click on the **Filter** command in the task bar on the right of the **DECT base stations** panel.
- 5 In the **Filter** dialog click on the **Reset** button.

6.7.2 “PAGING AREAS” MENU

The **Paging area** menu shows all configured RFPs in a tree structure consisting of two trees:

- The left **Unassigned RFPs** tree contains all RFPs without an assigned paging area.
- The right **Paging areas** tree shows all configured paging areas with RFPs assigned to these paging areas.



All DECT base stations are shown including their site and optional hierarchy (building, floor, and room) settings.

- DECT base stations can be moved by drag and drop from unassigned tree to paging area tree and vice versa, as well as between different paging areas inside the paging area tree.
- Only one DECT base station node can be moved at once.
- If a site or a hierarchy node is selected, all DECT base stations that are children of this node are moved.
- If a paging area is completely filled with DECT base stations, moving additional DECT base stations in that paging area is not permitted.
- If not all DECT base stations (selected by a site or hierarchy node) can be moved into a paging area, you are asked if you want to move as many DECT base stations as possible or if the operation should be cancelled.

Note: The **Paging area size** is set in the **DECT** tab of the **System settings** menu (see section 6.5.1).

6.7.3 “CAPTURING” MENU

OMP supports the capture of DECT base stations that try to connect to OMM. These DECT base stations are assigned to OMM by DHCP options or OMM Configurator settings. Capturing is only accessible in **Configuration Mode**.

Available tasks:

- **Capturing:** Start/stop capturing (active capturing is indicated with a green check mark)
- **Add all:** Add all captured DECT base stations to OMM
- **Add selected:** Add selected DECT base stations to OMM
- **Remove all:** Remove selected DECT base stations from list (without adding to OMM)

- **Remove selected:** Remove selected DECT base stations from list (without adding to OMM)
- **Select columns:** Select DECT base station capturing table columns to be shown

6.7.4 “ENROLMENT” MENU


The **Enrolment** menu allows import of DECT base station datasets using a configuration file. For information about required configuration file format, see section [12.3](#).

1 Click the **File** button.

A file system dialog opens in which you can select the configuration file. The configuration file must be encoded in UTF-8.

2 To check the results from reading the configuration file press the **Show log file** button. In case of file format errors these errors are listed here.

If reading of configuration file is successful, all DECT base station datasets read are shown in a newly created table. This table contains, apart from some DECT base station parameters, the **Status** column which shows the current import status for every DECT base station dataset:

 – Not enrolled yet

 – Enrolment failed

 – OK (Enrolment successful)

3 Start the import by selecting one of the following commands:

- **Add all:** Import all DECT base station datasets into the OMM.
- **Add selected:** Import selected DECT base station datasets to the OMM. For selection activate the corresponding checkboxes in the DECT base station table.
- **Remove all:** Remove all DECT base station datasets from table. The table will be hidden.
- **Remove selected:** Remove selected DECT base station datasets from table. If the table is empty after removing of datasets, the table will be hidden. For selection activate the corresponding checkboxes in the DECT base station table.
- **Show status:** Show import status of a selected DECT base station dataset. If enrolment failed for this DECT base station, a message describing the enrolment error is shown.
- **Select columns:** Select the columns that shall be shown in DECT base station table (see also 6.7.1.7).

6.7.5 “EXPORT” MENU

The **Export** menu allows export of all DECT base stations enrolled to the OMM to a “.csv” file. The generated file can be viewed with a standard spreadsheet application.

All enrolled DECT base stations are shown in a table.

Configuration	MAC address	Name	DECT cluster	Paging area	Site ID	HW type	Tasks
Status	<input checked="" type="checkbox"/> 00:30:42:18:1D:BD	SVE RFP1	1	0	3	RFP 35	Export all Export selected Select parameters Select columns
System	<input type="checkbox"/> 00:30:42:18:20:A2	SVE RFP2	1	0	3	RFP 35	
Sites	<input type="checkbox"/> 01:02:03:04:05:06	simu	5	0	1	RFP 32	
DECT base stations	<input type="checkbox"/> 01:02:03:04:05:07	simu	5	0	1	RFP 32	
Device list	<input type="checkbox"/> 01:02:03:04:05:08	simu	5	0	1	RFP 32	
Paging areas	<input type="checkbox"/> 01:02:03:04:05:09	simu	5	0	1	RFP 32	
Capturing	<input type="checkbox"/> 01:02:03:04:05:0A	simu	5	0	1	RFP 32	
Enrolment	<input type="checkbox"/> 01:02:03:04:05:0B	simu	5	0	1	RFP 32	
Export	<input type="checkbox"/> 01:02:03:04:05:0C	simu	5	0	1	RFP 32	
	<input type="checkbox"/> 01:02:03:04:05:0D	simu	5	0	1	RFP 32	
	<input type="checkbox"/> 01:02:03:04:05:0E	simu	5	0	1	RFP 32	
	<input type="checkbox"/> 01:02:03:04:05:0F	simu	5	0	1	RFP 32	

The following tasks can be performed:

- **Export all:** Export all DECT base station datasets.
- **Export selected:** Export selected DECT base station datasets.
- **Select parameters:** Select DECT base station parameters to be written to the .csv file (select all DECT base station parameters or a subset of these parameters).
- **Select columns:** Select the columns to be written to the .csv file.

When the export begins, a file system dialog opens where you can select the export file name. If all parameters are selected for export, the export file can be re-imported using the Enrolment function (see section 6.7.4). For information about DECT base station export file format, see **Appendix** (section 12.4).

6.7.6 “SYNC VIEW” MENU

The **Sync view** menu allows verification of the synchronization between DECT base stations in a graphical manner.

Note: For information on DECT base station synchronization, see section 8.2.

To open the task panel, click the arrow icon in the upper right corner of the **Sync view** panel.

The task panel is displayed on the right. The following tasks can be performed:

- **Show all RFPs:** If this checkbox is activated, all configured RFPs are shown in the sync panel; else only selected RFPs are shown.

- **RFP positioning:** If this checkbox is activated, RFP positions can be changed; else RFP positions are fixed.
- **Reset monitoring:** Reset all active sync view monitoring relations.
- **Image:** Select background image for sync panel.
- **Reset view:** Reset selected view (zero coordinates are reset to the left upper corner of the sync view panel).
- **Refresh RSSI:** Request new RSSI values from OMM for active sync relations.

Viewing sync relations

DECT base stations for which sync relations shall be shown, can be selected as follows:

- Select (more than one) DECT base station in device list table.

or

- Activate DECT base station mouse menu in sync view: Press the right mouse button while mouse cursor is on an DECT base station icon and select the **Activate Monitoring** command from the context menu.

The color of the DECT base station icon indicates synchronization state of that DECT base station:

- Grey: Inactive
- Red: Not synchronized
- Yellow: Searching
- Green: Synchronized

Sync relations between DECT base stations are represented by arrows.

Viewing RSSI values

The color of the arrows between DECT base stations is an indication of the RSSI value of the link:

- Red: RSSI < -90 dBm
- Orange: -90 dBm <= RSSI <= -70 dBm
- Green: RSSI > -70 dBm

If the mouse is moved over a DECT base station with monitoring activated, a tool tip with RSSI values is displayed.

You can use the **RSSI threshold** slider to limit the display of values in the tool tip.

6.7.7 “STATISTICS” MENU

The **DECT base stations** -> **Statistics** menu provides information about DECT base station statistics counters. It contains:

- an overview panel with all statistics counters (see section 6.7.7.1)
- multiple statistics group panels, where related statistics counter types are grouped together (see section 6.7.7.2).

The menu is only available in **Monitor Mode**.

6.7.7.1 DECT base station Statistics Overview

The DECT base station statistics overview page contains a list of DECT base stations by ID, and an overview of all DECT base station statistics counters.

	RFP ID	Element ID	Group	Counter	Value	Tasks
Monitoring	0x000	0	Voice channels	Only 2 voice channels fr...	0	
	0x001	1	Voice channels	Only 1 voice channels fr...	0	
Status	0x002	2	Voice channels	Voice channels busy	0	Refresh RFP
System	0x003	3	Voice channels	Voice channels busy an...	0	
	0x004	4	Air channels	Only 2-4 air channels free	0	Refresh all
Site	0x005	5	Air channels	Only 1 air channel free	0	Clear RFP
	0x006	6	Air channels	Air channels busy	0	
DECT base stations	0x007	7	Paging	Paging queue overflows	0	Clear all
Device list	0x008	8	Sync	Synchronisation losts	0	
Sync. view	0x009	9	Sync	Low relations	0	
Statistics	0x00A	10	Sync	OTset jumps	0	
	0x00B	11	RFP health	RFP resets	0	
Voice channels	12	RFP health	RFP connection timeouts	0		
Air channels	13	BMC: Connections	01 - 03	1368		
	14	BMC: Connections	04 - 06	0		
Paging	15	BMC: Connections	07 - 09	0		
	16	BMC: Connections	10 - 12	0		
Sync	17	BMC: DSP chan used	01 - 02	286		
RFP health	18	BMC: DSP chan used	03 - 04	3		
	19	BMC: DSP chan used	05 - 06	0		
BMC: Connections	20	BMC: DSP chan used	07 - 08	0		
	21	BMC: Miscellaneous	Lost connections	19		
BMC: DSP chan used	22	BMC: Miscellaneous	MAC reset	20		
	23	BMC: Miscellaneous	Reject dummy	0		
BMC: Miscellaneous	24	BMC: Miscellaneous	Ho timer > 150ms	244		
	25	BMC: Frame error rate	Bad frames	9427		
BMC: Frame error rate	26	BMC: Frame error rate	Good frames	625409		
	27	BMC: Frame error rate	Frame error rate in 1/1000	15		
Quality						
WLAN						
Video devices						

The following tasks can be performed:

- **Refresh RFP:** Request counter update by OMM for selected DECT base station statistics counters.
- **Refresh all:** Request counter update by OMM for all DECT base station statistics counters.
- **Clear RFP:** Clear all DECT base station statistics counters on selected DECT base station.
- **Clear all:** Clear all DECT base station statistics counters.

If a DECT base station is selected (left **RFP ID** table), the statistics counter table shows counter values for that DECT base station (right table). When a statistics counter entry is selected, a detail panel opens which shows more detailed information for that counter.

The detail panel shows values for total occurrence and occurrence in current and last week. You can clear the selected statistics counter on the selected DECT base station by pressing the **Clear** button.

6.7.7.2 DECT base station Statistics Group Panels

The DECT base station statistics group panels divide DECT base station statistics counters into logical groups. This allows display of all statistics counters of a special group of all DECT base stations in one table.

The group panels are listed under the **Statistics** menu entry in the left panel.

Note that with SIP-DECT 6.0 or later, the statistic data collected by the BMC part of each DECT base station device (in the DECT MAC layer) are now shown with the DECT base station statistic data collected by the OMM.

As an update between OMM and DECT base station usually occurs once every hour, it can take up to one hour for an event that increments a BMC statistic counter to appear in the OMP.

The following tasks can be performed:

- **Refresh RFP:** Request counter update by OMM for selected DECT base station.
- **Refresh all:** Request counter update by OMM for all counters.
- **Clear group RFP:** Clear counter group of selected DECT base stations.
- **Clear group:** Clear counter group of all DECT base stations.
- **Clear RFP:** Clear all counters of selected DECT base station.
- **Clear all:** Clear all counters of all DECT base stations.

6.7.8 “QUALITY” MENU

OMP provides a monitoring ability for critical IP network parameters. Administrators can check basic network quality information for all DECT base stations. This includes Voice quality (Jitter, Packet lost) and OMM to RFP link quality (Roundtrip delay).

The menu is only available in **Monitor Mode**.

6.7.8.1 IP

IP quality menu provides information about link quality between DECT base stations and OMM.

Monitoring	ID	Connecte...	Current R...	Max. RTT...	Count	< 25 msec	< 50 msec	< 150 msec	< 500 msec	>= 500 m...	Tasks
Status	0x000	354270	0.5	5.6	23617	23617	0	0	0	0	Select columns
System	0x001	354270	0.7	1.0	23617	23617	0	0	0	0	
Sites											
DECT base stations											
Device list											
Sync. view											
Statistics											
Quality											
IP											
Media stream											
Synchronization											

Displayed parameters:

- **ID:** Radio fixed part identifier
- **Connected time:** Time the RFP is connected to OMM (sec)
- **Current RTT:** Current roundtrip time between RFP and OMM (msec)
- **Max. RTT:** Maximal detected roundtrip time between RFP and OMM
- **Count:** Number of roundtrip time measures
- **< 25 msec:** Number of roundtrip time measures lower than 25 msec
- **< 50 msec:** Number of roundtrip time measures between 25 and 50 msec
- **< 150 msec:** Number of roundtrip time measures between 50 and 150 msec
- **< 500 msec:** Number of roundtrip time measures between 150 and 500 msec
- **>= 500 msec:** Number of roundtrip time measures 500 msec and more

Available tasks:

- **Select columns:** Columns to be shown in IP quality table

6.7.8.2 Media Stream

Media stream panel provides information about voice quality.

	ID	Connects	Duration [sec]	TX packets	RX packets	Lost packets	Max. jitter [msec]	Tasks
	0x000	24	124	10553	11893	3	1	
	0x001	7	36	2120	3409	0	0	Clear RFP
	0x002	0	0	0	0	0	0	
	0x003	0	0	0	0	0	0	Clear all
	0x004	0	0	0	0	0	0	
	0x005	0	0	0	0	0	0	Select columns
	0x006	0	0	0	0	0	0	
	0x007	0	0	0	0	0	0	
	0x008	0	0	0	0	0	0	
	0x009	0	0	0	0	0	0	
	0x00A	0	0	0	0	0	0	
	0x00B	0	0	0	0	0	0	

Displayed parameters:

- **ID:** Radio fixed part identifier
- **Connects**
- **Duration (sec)**
- **TX packets**
- **RX packets**
- **Lost packets**
- **Max. jitter(msec)**

Available tasks:

- **Clear RFP:** Clear values for selected RFPs
- **Clear all:** Clear values for all RFPs
- **Select columns:** Select media stream quality table columns to be shown

6.7.8.3 Synchronization

Synchronization panel allows checking the synchronization status of RFPs which allows identifying RFPs with bad synchronization coverage.

Synchronization monitoring can optionally be run in snapshot mode. If this mode is activated, data update must be triggered by a user otherwise data were updated automatically anytime if new values arrive from OMM.

	ID	DECT cluster	Sync. state	Strong relations	Low relations	Max. RSSI [dBm]	Min. RSSI [dBm]	Tasks
	0	1	✓	1	0	-43	-43	<input checked="" type="checkbox"/> Snapshot mode <input type="button" value="Update"/> <input type="button" value="Select columns"/>
	1	1	✓	1	0	-42	-42	

Available parameters:

- **ID:** Radio fixed part id
- **DECT cluster:** Cluster of the RFP
- **Sync state:** Synchronization state of the RFP
- **Strong relations**
- **Low relations**
- **Max. RSSI (dBm)**
- **Min. RSSI (dBm)**

Available tasks in media synchronization quality table:

- **Snapshot mode:** Enable snapshot mode (green check mark indicates snapshot mode is on)
- **Update:** Request data update in snapshot mode
- **Select columns:** Select synchronization quality table columns to be shown

6.8 “WLAN” MENU

OMP supports configuration of WLAN profiles and provides an overview of wireless clients currently connected.

6.8.1 PROFILES

OMM supports up to 20 WLAN profiles, which can be added, changed and deleted in OMP configuration mode. Configuration and state of any WLAN profile can be checked in monitoring mode.

6.8.1.1 WLAN Profiles - configuration mode

WLAN profile configuration menu provides an overview of all configured WLAN profiles.



The following tasks are available in this menu:

- **Create profile:** Create a new WLAN profile (available if the maximal number of 10 WLAN profiles is not yet reached)
- **Configure profile:** Reconfigure selected profile
- **Delete profile:** Deletes a selected profile (only available if selected profile is not in use by any Radio fixed part)
- **Delete all profiles:** Deletes all existing profiles (only available if none of these profiles is in use by any Radio fixed part)
- **Configure MAC filter:** Add, configure, delete MAC filter for selected profile
- **Select columns:** Select WLAN profile table columns to be shown

6.8.1.2 WLAN Profiles Monitoring Mode

WLAN profile monitoring menu shows all configured WLAN profiles.

The following tasks are available:

- **Show Profile:** Show details of selected WLAN profile
- **Show MAC filter:** Show configured MAC filter of selected WLAN profile
- **Select columns:** Select WLAN profile table columns to be shown

6.8.1.3 WLAN Profile Detail Panel

WLAN profile detail panel is used to create, reconfigure or show a profile. It consists of different tabs which are used for general settings of WLAN profile, SSID configuration and SSID security settings.

WLAN profile detail panel is opened if one of the following tasks is performed in WLAN profile menu:

- **Create profile** (configuration mode)
- **Configure profile** (configuration mode)
- **Show profile** (monitoring mode)

The “General” tab is always shown and configures/shows general settings of this profile like enabling of profile and profile type.

General SSID selection SSID 1 general SSID 1 security

Profile enabled Profile type RFP43

Avoid interferences 802.11 mode 802.11n

WME

Maximal bit rate Mbps

Beacon interval 100 msec

DTIM interval 5 Beacons

RTS threshold 2347 Bytes

Fragmentation threshold 2346 Bytes

OK Cancel

The "SSID selection" tab is used for enabling of SSIDs. At least "SSID 1" is always enabled. "SSID 2", "SSID 3" and "SSID 4" can be activated optional.

General SSID selection SSID 1 general SSID 1 security

	Configure	Name
SSID 1	<input checked="" type="checkbox"/>	<input type="text"/>
SSID 2	<input type="checkbox"/>	<input type="text"/>
SSID 3	<input type="checkbox"/>	<input type="text"/>
SSID 4	<input type="checkbox"/>	<input type="text"/>

OK Cancel

The "SSID x general" tab is shown for any activated SSID. Among other things, you can use it to select Security type.

General SSID selection SSID 1 general SSID 1 security

SSID enabled

VLAN tag

Security type Open

BSS isolation

Use MAC access filter

Hidden SSID mode

OK Cancel

A tab “SSID x security” is shown as well. It is accessible only for SSIDs with security type set to “WEP” or “WPA”. If security type stays at “Open” this tab is inactive. It allows setting of all necessary security parameters for this SSID.

The screenshot displays the 'WLAN profile #3' configuration interface, specifically the 'SSID 1 security' tab. The 'Security settings 'WPA':' section includes the following fields and options:

- WPA type:** WPA2 (selected)
- Distribution interval:** 600 sec
- Mode:** Pre shared key (selected)
- Pre shared key format:** Text (selected)
- Pre shared key:** PpNohquPO0GoSHGmfOyX
- Radius configuration:**
 - IP address:** [Empty text box]
 - Port:** [Empty text box]
 - Secret:** [Empty text box]

At the bottom of the configuration area, there is a blue 'Generate' button, and at the very bottom, there are 'OK' and 'Cancel' buttons.

6.8.1.4 MAC Access Filter Detail Panel

MAC access filter detail panel in configuration mode allows the adding, configuring and deleting of MAC access filters. File import and export of MAC access filters is supported as well.

Monitoring mode shows all configured MAC access filters only.

MAC access filter detail panel is opened if one of the following tasks is performed in WLAN profile menu:

- **Configure MAC filter** (configuration mode)
- **Show MAC filter** (monitoring mode)

The “General” tab in configuration mode shows all configured MAC access filter.

The following actions are available:

- **Create:** Create new MAC access filter
- **Configure:** Change name of selected MAC access filter
- **Delete:** Delete all selected MAC access filter

The “Import” tab (configuration mode only) provides import of a list of MAC access filter from file.

The “Export” tab (configuration mode only) provides export of all configured MAC access filters to file. If no MAC access filter is configured, this tab is inactive.





6.8.1.5 Clients

WLAN clients menu which is available in monitoring mode only, shows all currently connected wireless clients.

6.9 “VIDEO DEVICES” MENU

The **Video devices** panel lists all configured video devices. The device list is available in **Configuration Mode** as well as in **Monitor mode**.

New video device entries show up automatically after they are connected to and recognized by a DECT base station. The **Plugged** and **State** columns shows the following states:

-  / **unplugged** – Video device is not connected.
-  / **plugged** – Video device is connected.
-  / **started** – Video device is being watched in the OM Locating application.
-  / **stopped** – Video device is connected but disabled in the OMP.

The **Tag** column shows the USB ID of the connected video device. The **USB path** column shows the USB port number to be used, e.g. “1” is a video device connected directly to the RFP while “1.1” indicates an indirect connection using an USB hub.

The tasks which can be performed are mode-dependant.

Configuration mode	Monitor mode	See section
Configure: Configure selected video device in detail panel		6.9.1
	Show details: Show selected video device in detail panel	6.9.2
Delete: Delete selected disconnected video device		6.9.3
Filter: Show only video device entries in table which contains a special search string	Filter: Show only video device entries in table which contains a special search string	6.9.4

6.9.1 CHANGING VIDEO DEVICES

Changing video devices is only possible in **Configuration Mode**. To change the configuration of an existing video device, do the following:

- 1 Select the appropriate video device in the video devices table.
- 2 In the task bar on the right of the **Video devices** panel click on the **Configure** command.
The video device detail panel opens.
- 3 Change video device parameters, see description below.
- 4 Press the **OK** button.

Please note: You cannot change the configuration for a video device that is being watched in the OM Locating application (**State** column shows “active”). You must disable the video device first by deactivating the **Active** option.

The following parameters can be set in the **General** tab of the **Video devices** panel:

- **Active:** Disable this option to switch off the video device. This also switches off the status LED of the video device immediately (if applicable).
- **Name:** Enter a meaningful name for the video device.

- **Building, Floor, Room:** For easier localization of the video device you can enter data in these fields.
- **Resolution:** Select a resolution for the video device. Higher resolutions require more bandwidth when watching the video image in the OM Locating application. Note, that not all video devices support all available resolutions. Default: "VGA (640 x 480)".
- **Frame rate:** Select a frame rate (2-10 frames per second). Higher frame rates require more bandwidth when watching the video image in the OM Locating application.

6.9.2 VIEWING VIDEO DEVICE DETAILS

You can view the configuration of a video device in **monitor mode**. Proceed as follows:

- 1 Select the appropriate video device in the video devices table.
- 2 In the task bar on the right of the **Video devices** panel click on the **Show details** command.
The video device detail panel opens (see 0).
- 3 Click **Cancel** to close the video device detail panel.

6.9.3 DELETING VIDEO DEVICES

Deleting video devices is only possible in **Configuration Mode**. To delete one or more existing video devices proceed as follows:

- 1 Select the appropriate video device(s) in the video devices table by activating the corresponding checkbox(es). Note that you can only delete disconnected video devices.
- 2 In the task bar on the right of the **Video devices** panel click on the **Delete** command.
The **Delete selected video devices(s)** dialog opens showing a confirmation prompt.
- 3 Confirm the displayed prompt with **OK**.

6.9.4 FILTERING VIDEO DEVICE TABLE

You can filter the list of video device entries shown in the video devices table by using a filter.

- 1 In the task bar on the right of the **Video devices** panel click on the **Filter** command.
The **Filter** dialog opens.
- 2 Enter the search string that serves as filter criterion. You can enter digits and characters. The search is case sensitive.
- 3 Click on the **Filter** button.
The **Filter** dialog is closed and the video device table will be adapted accordingly.
- 4 To reset the filter, click on the **Filter** command in the task bar on the right of the **Video devices** panel.
- 5 In the **Filter** dialog click on the **Reset** button.

6.10 "DECT PHONES" MENU

DECT phone datasets can be configured and viewed in the **DECT phones** menu. The **DECT Phones** menu contains different submenus. Each submenu displays its own table of DECT phone datasets.

Configuration mode	Monitor mode	See section
Overview: Displays all user and device-related DECT phone data	Overview: Displays all user and device-related DECT phone data	6.10.1
Users: Displays all DECT phone user data		6.10.2
Devices: Displays all DECT phone device data	Devices: Displays all DECT phone device data	6.10.3
	User monitoring: Displays the status of all monitored users	8.29.7.3

6.10.1 "OVERVIEW" MENU

In the **Overview** panel, all user-related and device-related DECT phone data are listed in a table. The overview is available in **Configuration Mode** and **Monitor mode**.

Configuration	Device ID	IPEI	Name	Number/SIP user na...	User ID	User rel. type	Active	Tasks
Status	0x001	10345 0031639 *	x25052 612d	25052	0x001	Fixed	✓	<ul style="list-style-type: none"> Create Configure Delete Filter Subscription Wildcard subscription Select columns Change rel. type
	0x002	03586 0952116 0	x25053 622d	25053	0x002	Fixed	✓	
System	0x003	03586 0950946 7	x25054 622d	25054	0x003	Fixed	✓	
	0x004	03586 0952129 3	x42052 622d	42052	0x004	Fixed	✓	
Sites	0x05F	00100 0000000 3	simu pp 0	256001	0x04C	Fixed	✗	
DECT base stations	0x060	00100 0000001 4	simu pp 1	256002	0x04D	Fixed	✗	
	0x061	00100 0000002 5	simu pp 2	256003	0x04E	Fixed	✗	
WLAN	0x062	00100 0000003 6	simu pp 3	256004	0x04F	Fixed	✗	
	0x063	00100 0000004 7	simu pp 4	256005	0x050	Fixed	✗	
Video devices	0x064	00100 0000005 8	simu pp 5	256006	0x051	Fixed	✗	
DECT phones	0x065	00100 0000006 9	simu pp 6	256007	0x052	Fixed	✗	
	0x066	00100 0000007 *	simu pp 7	256008	0x053	Fixed	✗	
Overview	0x067	00100 0000008 0	simu pp 8	256009	0x054	Fixed	✗	
Users	0x068	00100 0000009 1	simu pp 9	256010	0x055	Fixed	✗	
	0x069	00100 0000010 3	simu pp 10	256011	0x056	Fixed	✗	
Devices	0x06A	00100 0000011 4	simu pp 11	256012	0x057	Fixed	✗	
	0x06B	00100 0000012 5	simu pp 12	256013	0x058	Fixed	✗	
Conference rooms	0x06C	00100 0000013 6	simu pp 13	256014	0x059	Fixed	✗	
	0x06D	00100 0000014 7	simu pp 14	256015	0x05A	Fixed	✗	
System features	0x06E	00100 0000015 8	simu pp 15	256016	0x05B	Fixed	✗	
	0x06F	00100 0000016 9	simu pp 16	256017	0x05C	Fixed	✗	
Licenses	0x070	00100 0000017 *	simu pp 17	256018	0x05D	Fixed	✗	
	0x071	00100 0000018 0	simu pp 18	256019	0x05E	Fixed	✗	
	0x072	00100 0000019 1	simu pp 19	256020	0x05F	Fixed	✗	
	0x073	00100 0000020 3	simu pp 20	256021	0x060	Fixed	✗	
	0x074	00100 0000021 4	simu pp 21	256022	0x061	Fixed	✗	
	0x075	00100 0000022 5	simu pp 22	256023	0x062	Fixed	✗	
	0x076	00100 0000023 6	simu pp 23	256024	0x063	Fixed	✗	
	0x077	00100 0000024 7	simu pp 24	256025	0x064	Fixed	✗	

In **Configuration Mode**, the **Overview** panel allows you to create **fixed** DECT phones (i.e., user and device are permanently associated).

The **Active** column shows the following states:

- ✗ - DECT phone is not subscribed to the system.
- ✓ - DECT phone is subscribed to the system.

Note: If the **Active** column is not displayed, you can activate it in the **Select columns** dialog, see section 6.10.9. To view the user-device-relation, ensure that the **User ID** and **Device ID** columns are also activated.

In monitor mode you can view the registration status of a DECT phone user by activating the **Registered**, **Registrar server type**, **Registrar server** and **Registrar port** columns. See section 6.10.9 for information on selecting columns and section [8.20.6](#) for information on the SIP registration status.

Monitoring	Device ID	IPEI	Subscri..	Number/SIP..	Last action	RFP ID	CC	MM	Info	Registe..	Tasks
Status	0x001	10345 003163...	✓	25052	25.01.21:42	0x000				✓	<ul style="list-style-type: none"> Show details Filter Log events Select columns
	0x002	03586 095211...	✓	25053	25.01.22:12	0x001				✓	
System	0x003	03586 095094...	✓	25054	25.01.20:42	0x001				✓	
	0x004	03586 095212...	✓	42052	25.01.22:25	0x000				✓	
Sites	0x05F	00100 000000...	✗	256001	-	-				✗	
DECT base stations	0x060	00100 000000...	✗	256002	-	-				✗	
	0x061	00100 000000...	✗	256003	-	-				✗	
WLAN	0x062	00100 000000...	✗	256004	-	-				✗	
	0x063	00100 000000...	✗	256005	-	-				✗	
Video devices	0x064	00100 000000...	✗	256006	-	-				✗	
DECT phones	0x065	00100 000000...	✗	256007	-	-				✗	
	0x066	00100 000000...	✗	256008	-	-				✗	
Overview	0x067	00100 000000...	✗	256009	-	-				✗	
Devices	0x068	00100 000000...	✗	256010	-	-				✗	
	0x069	00100 000001...	✗	256011	-	-				✗	
User monitoring	0x06A	00100 000001...	✗	256012	-	-				✗	
	0x06B	00100 000001...	✗	256013	-	-				✗	
Conference rooms	0x06C	00100 000001...	✗	256014	-	-				✗	
System features	0x06D	00100 000001...	✗	256015	-	-				✗	
	0x06E	00100 000001...	✗	256016	-	-				✗	
Licenses	0x06F	00100 000001...	✗	256017	-	-				✗	
	0x070	00100 000001...	✗	256018	-	-				✗	
	0x071	00100 000001...	✗	256019	-	-				✗	
	0x072	00100 000001...	✗	256020	-	-				✗	

The tasks you can perform are mode-dependant.

Configuration mode	Monitor mode	See section
Create: Create new fixed DECT phone dataset in detail panel		6.10.5
Configure: Configure selected DECT phone user and device dataset in detail panel		6.10.6
	Show details: Show selected DECT phone user and device dataset in detail panel	6.10.4
Delete: Delete selected DECT phone user and device dataset (in case of fixed relation) or delete DECT phone user and set device to unbound status (in case of dynamic relation)		6.10.8
Subscription: Start DECT phone subscription		6.10.7
Wildcard subscription: Start DECT phone wildcard subscription		6.10.7
Select columns: Select columns/parameters to be shown in DECT phone table	Select columns: Select columns/parameters to be shown in DECT phone table	6.10.9
Filter: Show only DECT phone datasets in table which contain a special search string	Filter: Show only DECT phone datasets in table which contain a special search string	6.10.10
Change rel. type: Change the DECT phone relation type		6.10.11
	Log events: Enable/disable DECT phone event log	6.10.11

6.10.2 “USERS” MENU

Configuration	User ID	Name	Number/SIP user n...	Login/Add ID	User rel. type	Rel. devic...	Active	External	Tasks
Status	0x001	x25052 612d	25052		Fixed	0x001	✓	✗	Create Configure Delete Filter Select columns
	0x002	x25053 622d	25053		Fixed	0x002	✓	✗	
System	0x003	x25054 622d	25054		Fixed	0x003	✓	✗	
	0x004	x42052 622d	42052		Fixed	0x004	✓	✗	
Sites	0x04C	simu pp 0	256001		Fixed	0x05F	✗	✗	
	0x04D	simu pp 1	256002		Fixed	0x060	✗	✗	
DECT base stations	0x04E	simu pp 2	256003		Fixed	0x061	✗	✗	
	0x04F	simu pp 3	256004		Fixed	0x062	✗	✗	
WLAN	0x050	simu pp 4	256005		Fixed	0x063	✗	✗	
	0x051	simu pp 5	256006		Fixed	0x064	✗	✗	
Video devices	0x052	simu pp 6	256007		Fixed	0x065	✗	✗	
	0x053	simu pp 7	256008		Fixed	0x066	✗	✗	
DECT phones	0x054	simu pp 8	256009		Fixed	0x067	✗	✗	
	0x055	simu pp 9	256010		Fixed	0x068	✗	✗	
Overview	0x056	simu pp 10	256011		Fixed	0x069	✗	✗	
	0x057	simu pp 11	256012		Fixed	0x06A	✗	✗	
Users	0x058	simu pp 12	256013		Fixed	0x06B	✗	✗	
	0x059	simu pp 13	256014		Fixed	0x06C	✗	✗	
Devices	0x05A	simu pp 14	256015		Fixed	0x06D	✗	✗	
	0x05B	simu pp 15	256016		Fixed	0x06E	✗	✗	
Conference rooms	0x05C	simu pp 16	256017		Fixed	0x06F	✗	✗	
	0x05D	simu pp 17	256018		Fixed	0x070	✗	✗	

In the **Users** panel, all DECT phone user data are listed in a table. The **Users** panel allows you to create (unbound) users (which should be able to login and logout at a device).

Note: Use the **Select columns** dialog (see section 6.10.9) to display the desired DECT phone user data.

The following tasks can be performed:

- **Create:** Create new unbound DECT Phone user dataset (see section 6.10.5).
- **Configure:** Configure selected DECT Phone user dataset (see section 6.10.6).
- **Delete:** Delete selected DECT Phone user dataset. Also delete device data in case of a fixed relation (see section 6.10.8).
- **Select columns:** Select parameter columns to be shown in table (see section 6.10.9).
- **Filter:** Filter DECT phone datasets shown in table for string set in filter mask (see section 6.10.10).
- **Change rel. type:** Change the DECT phone relation type (see section 6.10.11).

6.10.3 “DEVICES” MENU

In the **Devices** panel, all DECT phone device data are listed in a table. The **Device** panel allows you to configure the DECT part of a DECT phone device dataset.

Devices cannot be created separately. They are created automatically during subscription (unbound) or they are created fixed bound to a user when a user is created in the **Overview** submenu.

Configuration	Device ID	IPEI	DECT Auth. co...	Encryption	Device rel. type	Rel. user ID	Subscribed	Tasks
Status	0x001	10345 0031639 *		✓	Fixed	0x001	✓	<ul style="list-style-type: none"> Configure Delete Filter Subscription Wildcard subscription Select columns
	0x002	03586 0952116 0		✓	Fixed	0x002	✓	
System	0x003	03586 0950946 7	2222	✓	Fixed	0x003	✓	
	0x004	03586 0952129 3		✓	Fixed	0x004	✓	
Sites	0x05F	00100 0000000 3		✗	Fixed	0x04C	✗	
DECT base stations	0x060	00100 0000001 4		✗	Fixed	0x04D	✗	
	0x061	00100 0000002 5		✗	Fixed	0x04E	✗	
WLAN	0x062	00100 0000003 6		✗	Fixed	0x04F	✗	
	0x063	00100 0000004 7		✗	Fixed	0x050	✗	
Video devices	0x064	00100 0000005 8		✗	Fixed	0x051	✗	
DECT phones	0x065	00100 0000006 9		✗	Fixed	0x052	✗	
	0x066	00100 0000007 *		✗	Fixed	0x053	✗	
Overview	0x067	00100 0000008 0		✗	Fixed	0x054	✗	
Users	0x068	00100 0000009 1		✗	Fixed	0x055	✗	
	0x069	00100 0000010 3		✗	Fixed	0x056	✗	
Devices	0x06A	00100 0000011 4		✗	Fixed	0x057	✗	
	0x06B	00100 0000012 5		✗	Fixed	0x058	✗	
Conference rooms	0x06C	00100 0000013 6		✗	Fixed	0x059	✗	
	0x06D	00100 0000014 7		✗	Fixed	0x05A	✗	
System features	0x06E	00100 0000015 8		✗	Fixed	0x05B	✗	
Licenses	0x06F	00100 0000016 9		✗	Fixed	0x05C	✗	
	0x070	00100 0000017 *		✗	Fixed	0x05D	✗	
	0x071	00100 0000018 0		✗	Fixed	0x05E	✗	
	0x072	00100 0000019 1		✗	Fixed	0x05F	✗	
	0x073	00100 0000020 3		✗	Fixed	0x060	✗	

Note: Use the **Select columns** dialog (see section 6.10.9) to display the desired DECT phone device data.

The following tasks can be performed:

- **Configure:** Configure selected DECT phone device dataset (see section 6.10.6).
- **Delete:** Delete selected DECT phone device dataset (see section 6.10.8).
- **Subscription:** Start DECT phone subscription (see section 6.10.7).
- **Wildcard subscription:** Start DECT phone wildcard subscription (see section 6.10.7).
- **Select columns:** Select parameter columns to be shown in table (see section 6.10.9).
- **Filter:** Filter DECT phone datasets shown in table for string set in filter mask (see section 6.10.10).

6.10.4 DEVICE DETAIL PANEL

The **Device detail** panel is used for configuration/showing of device settings and creation of new DECT phone datasets.

To open the **Device detail** panel,

- choose one of the commands in the task bar on the right of the **DECT Phones** panel (**Configure**)

or

- double-click on the appropriate device entry in the device table

The **Device detail** panel contains the different parameter groups sorted in tabs. The tabs displayed depend on the current mode and the panel from which the DECT phone detail panel was invoked.

- **Overview** panel (configuration and monitor mode): The DECT phone detail panel contains all tabs listed below.

- **User panel** (configuration mode): The DECT phone detail panel contains all tabs but not DECT.
- **Device panel** (configuration mode): The DECT phone detail panel contains only DECT.

6.10.4.1 “General” tab

The General tab contains general settings for the DECT phone dataset.

- **Name:** The DECT phone user name (up to 20 characters).
- **Number:** The DECT phone telephone number, up to 31 characters (1234567890*#azAz+-_!\$%&/()=?\$&). Please be aware that only “*”, “#” and “0” to “9” can be dialed with a DECT phone.
- **Description 1** and **Description 2:** Free text comments with up to 16 characters each.
- **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).
- **PIN, PIN confirmation:** A user PIN to be entered during user login.

Note: The attempt to set the user PIN to an empty string sets the PIN to the default value “0000”.

6.10.4.2 “SIP” tab

The SIP contains the SIP authentication parameters for the DECT phone dataset.

- **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.
- **VIP:** Enable this option if the registration of this user should be prioritized (default off). VIP users will be registered first. For more information on prioritized registration, see section [8.20.5](#).
- **Used for visibility checks:** Enables the use of this user account to check the availability of the iPBX (e.g., in fail over situations). See section [8.20.7](#) for more information on this feature.
- **Fixed port:** Specifies the port used explicitly for SIP signaling. If set to 0, an automatically calculated port is used. The default is 0. See section [2.17](#) for more information on this feature.

6.10.4.3 “Incoming calls” tab

The Incoming calls tab allows you to set device-specific settings for auto-answering incoming calls. Default values for all parameters are inherited from global settings (see section 6.5.4.7).

- **Auto answer:** Enables or disables auto-answer on incoming calls.

- **Microphone mute:** Enables or disables microphone muting when incoming calls are automatically answered.
- **Warning tone:** Enables or disables warning tone on incoming call. A short ringtone is played if there are no active calls. If there is an active call in a “barge in” situation, the ringing will be in-band
- **Allow barge in:** Allows/disallows “barge-in” on existing calls.

6.10.4.4 “Conference” tab

The Conference tab contains parameters for three-way conferencing for the DECT phone dataset.

- **Server type:** Determines the conference service to be used for three-way conferencing. Possible values are:
 - **None:** Disables 3-way conferencing.
 - **Global:** The OMM system setting is used (default).
 - **Integrated:** The integrated conference server is used.
 - **External:** An external conference server is used.
 - **External – Blind Transfer:** An external conference server is used (e.g., MiVoice Business). The initiation of the conference is signaled as a blind transfer to the destination specified in the URL parameter.
- **URL:** Address of an external conference server (field only activated if the server type is “External”).

For more information see section [8.20.7](#).

6.10.4.5 “DECT” tab

The DECT tab contains parameters DECT configuration of the DECT phone dataset. When configuring a device (see 6.10.3), only the **DECT** tab is shown in the DECT phone detail panel.

- **IPEI:** This optional setting is the DECT phone IPEI number. On a Mitel DECT 142 / Mitel 142d DECT phone, the IPEI can be found via the following path of the device menu: **Main menu > Phone settings > System**. On a Mitel 600 DECT phone, the IPEI can be found in the **System** device menu. Consult the DECT phone’s user guide for further information.
- **DECT authentication code:** The DECT authentication code is used during initial DECT subscription as a security option and can be set here for each DECT phone device separately (DECT phone-specific DECT authentication code). If no DECT phone-specific DECT authentication code is set, the system-wide DECT authentication code is used.
- **Encryption:** If the encryption feature is enabled for the whole system (in the **System settings** menu, see section 6.5.1), you can de-activate the DECT encryption for this device.

Please note: The DECT phone device must support DECT encryption which is not a mandatory feature.

- **Subscribe to PARI only:** Ensures that the DECT phone subscribes to the PARK code (of a single OMM, within a Dual Homing installation) and not to the SARI. This option is only available for fixed user device pairs, and must be set before subscription takes place. For this reason, you should set the parameter immediately when creating the DECT phone device.
- **Delete subscription:** This option is only available when configuring an existing DECT phone. If this option is activated, the subscription data will be deleted which also requires a re-subscription of the DECT phone device.

6.10.4.6 “Messaging” tab

The Messaging tab contains parameters for the OM Integrated Messaging and Alerting service on the DECT phone dataset.

If a user is created independent of any specific configuration, the **Sending messages** and **Sending vCards** features are enabled by default.

- **Sending messages permission:** If this option is enabled, the DECT phone can send messages (if this function is supported by the device).
 - Note:** For further information see the document SIP-DECT OM Integrated Messaging & Alerting Application Installation, Administration & User Guide.
- **Sending vCards permission:** Allows the user to send personal directory entries as a vCard message from the DECT phone to other users (if this function is supported by the device).
- **Receiving vCards permission:** If this option is enabled, all received vCard messages are automatically processed and written into the personal directory of the DECT phone (if this function is supported by the device).

6.10.4.7 ”Locating” tab

The Locating tab contains parameters for configuring location parameters for the DECT phone.

- **Locating permission:** This option applies to Mitel 600 DECT phones only. If this option is enabled, the user is allowed to determine the location of other DECT phones. The main menu of the Mitel 600 DECT phones provides an extra **Locating** menu entry for this function.
- **Tracking:** If this option is enabled, the operator of the OM Locating application is able to use the constant tracking feature for the DECT phone. Note that this feature consumes more of the DECT phone’s battery power, because it activates a DECT base station update if the device roams and is not in communication. You also cannot enable this feature, if the **DECT locatable** option is disabled.
- **DECT locatable:** If this option is enabled, the DECT phone is locatable. Either with the OM Locating application or by querying it’s location from other DECT phones.

6.10.4.8 “Additional services” tab

The Additional services tab contains additional optional parameters for the DECT phone dataset.

- **SOS number:** User-specific SOS number that is dialed automatically if the SOS key on the DECT phone is pressed.

- **ManDown number:** User specific “Man down” number that is dialed automatically if a Man down event happens. This event is triggered by the sensor of a Mitel 600 DECT phone.

If no individual SOS or Man down number is configured for a DECT phone, the number of the appropriate alarm trigger will be used as calling number in case of a SOS or Man down event. Please see /31/ for details.

- **Voice mail number:** The number that will be automatically called as soon as a voice mail call is initiated on the Mitel 600 DECT phone. 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, section 6.5.1). If there is no voice mail number configured (neither the individual nor the system-wide) or another DECT phone type is used, then the voice mail number must be configured locally in the DECT phone.
- **Keep personal directory:** Activate this option, to keep the personal directory data in the DECT phone if the user logs out.
- **External:** A user data set can either be provisioned on an external user data server or locally in the OMM database. To provide an easy way to change the provisioning storage of user data sets, the user data sets can be moved from an external user data server into the local OMM database and vice versa.

Deactivate the **External** option if you want to move user data sets from an external user data server into the local OMM database.

External to internal transformation rules: To change a user data set from an external user data server to an internally provisioned one, the following conditions must be applied to the data set:

- external provisioned on an external user data server
- user data set device relation must not be “fixed”

Internal to external transformation rules: To change a user data set from local OMM database to an external user data server provisioned one the following conditions must be applied for the data set:

- external provisioned on an external server
- user data set device relation must not be “fixed”
- an external user data server must be available

- **Video stream permission:** Activate this option to allow video streaming on the Mitel 602 DECT phone. See section [8.28](#) for details on this feature.
- **Hot desking supported:** Enables or disables Hot desking functionality (for SIP-DECT systems using the MiVoice Business platform). Only available for users with a dynamic association with a DECT phone. When enabled, the user is registered as a Hot Desking user on the MiVoice Business call server. See section [2.14](#) for details on this feature.
- **Auto logout on charging:** Enables or disables automatic user log out on the DECT phone when the device is placed in the charger cradle. Only available for users with a dynamic association with a DECT phone. Note that the **Silent charging** option must be enabled on the DECT phone.
- **Authenticate logout:** Enables or disables whether it is necessary for the user to authenticate in case of logout.

6.10.4.9 “User monitoring” tab

The User monitoring tab contains parameters to configure the user-specific parameters for the User Monitoring feature. For a description of the parameters which can be set in the **User monitoring** tab, see the description in section [8.29.7.2](#).

6.10.4.10 “Configuration data” tab

The Configuration data tab allows you to assign a Configuration over Air (CoA) profile to a DECT phone user. See section [8.23](#) for more information on this feature.

- **Profile id:** Specifies the CoA configuration profile you want to assign to the DECT phone user.

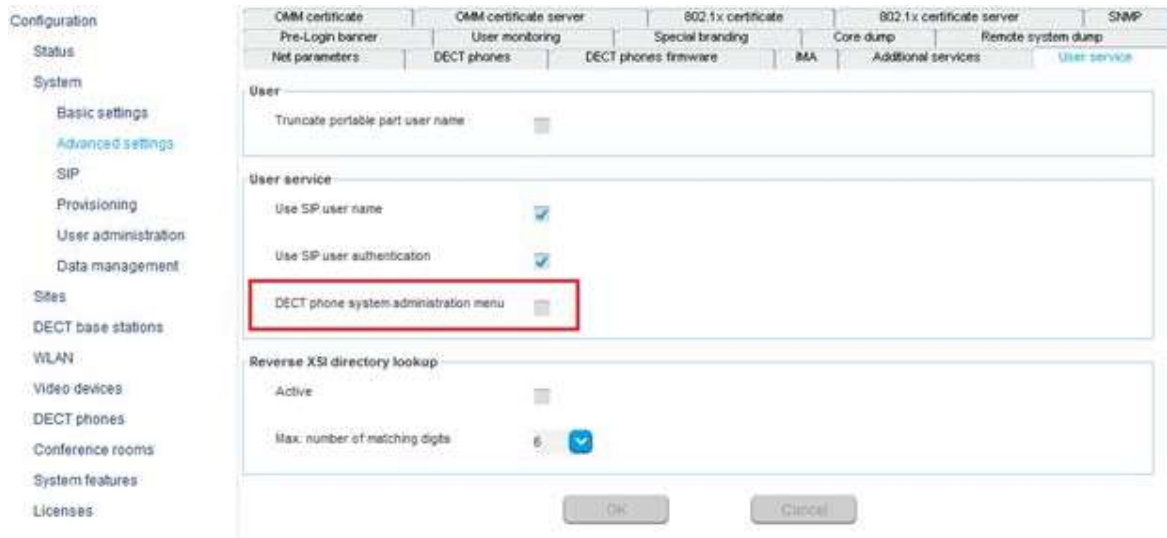
Note: When a COA profile is deleted, its profile ID assignment to DECT phone users remains. If a new CoA profile is created and acquires this profile ID (the IDs are assigned in sequential order), any DECT phone users with the old profile ID are automatically assigned to the new CoA profile.

If you do not want the DECT phone users to automatically inherit any new CoA profile that has the profile ID, you must remove the profile ID assignment manually.

6.10.4.11 “User service” tab

The User service tab allows you to specify parameters related to user authentication for XSI services.

- **Use SIP user name:** Specifies whether the XSI user name is taken from the user's SIP data. The generated format is <sip user name>@<sip registrar domain>. Possible values are **Global**, **On**, or **Off**.
- **Use SIP user authentication:** Specifies whether the XSI authentication name and password are taken from user's SIP data. The generated format is <sip authentication name>@<sip registrar domain>. Possible values are **Global**, **On**, or **Off**.
- **User name:** Specifies the user's user name for the XSI service (if **Use SIP user name** is set to Off). The username is part of the access url path of a XSI request (e.g., /com.broadsoft.xsi-actions/v2.0/user/<service user name>/directories/Enterprise?firstName=A*).
- **Authentication name:** Specifies the name to authenticate the user for XSI services (if **Use SIP user authentication** is set to Off).
- **Password:** Specifies the password to authenticate the user for XSI services.
- **Password confirmation:** confirms the password to authenticate the user for XSI services.



Please note: As of SIP-DECT 8.0, the access to the system configuration through the DECT phone UI is disabled by default to improve system security. The user can enable the menus through OMP.

6.10.4.12 “Key lock” tab

The Mitel 600d DECT phone family offers an optional PIN to protect the DECT Phone. For SIP-DECT 8.0 and the DECT phone SW 7.2, the key lock PIN is managed by the OMM to improve the shift worker support and the roaming between OMMs in a MOM setup.

The local DECT phone key lock PIN settings are suppressed if the DECT phone is subscribed with a SIP-DECT system.

The key lock with PIN can be managed through OMP, OMM configuration files and by the user through the DECT phone UI in System menu/ Administration/ Key lock.

Note that this is not possible for external users, that is, users who are provisioned through user.cfg file. If user data are provisioned through user.cfg files, then the provisioning platform is the data master and there is no option to update data towards the provisioning platform when changed in the SIP-DECT system. Therefore, data changes in the SIP-DECT system are prevented.

The following default values apply when creating a new user or when upgrading from the previous release 7.1-CK14 or older.

- **Active:** The feature is set active. This enables the Key lock menu under System menu/Administration on the Mitel 600d DECT phone. To prevent change of the time by the user disable the feature here.
- **Timer:** The timer is set to “None” (“Off” on the DECT phone). The key lock is not automatically activated if the DECT phone is not used, and the long press of the # key (#+) does not activate the key lock with PIN.

- **PIN and PIN confirmation:** The DECT phone default PIN is set to 0000. It is the same default PIN as for the local DECT phone feature. Adjust a new PIN here if the user had forgotten its PIN.

The screenshot shows the configuration interface for DECT phones. On the left is a navigation menu with options like Configuration, Status, System, Sites, DECT base stations, WLAN, Video devices, DECT phones, Overview, Users, Devices, Conference rooms, System features, and Licenses. The main area displays a table of users:

User ID	Name	Number/SIP user name	Login/Add ID	User rel. type
<input checked="" type="checkbox"/> 0x001	name 5001	5001	5001	Fixed
<input type="checkbox"/> 0x002	perm 5200	5200	5200	Fixed
<input type="checkbox"/> 0x003	my_5201	5201	5201	Fixed
<input type="checkbox"/> 0x004	crt omm 5203	5203	5203	Unbound
<input type="checkbox"/> 0x005	perm 5202	5202	5202	Fixed
<input type="checkbox"/> 0x006	set to perm 5204	5204	5204	Unbound

Below the table, the configuration for 'User #0x001' is shown. It includes tabs for General, SIP, Incoming calls, Conference, Messaging, Locating, Additional services, User monitoring, Configuration data, User service, and Key lock. The 'Key lock' tab is active, showing the following settings:

- Active:
- Time: None (dropdown menu)
- PIN: [masked with dots]
- PIN confirmation: [masked with dots]

Buttons for 'OK' and 'Cancel' are at the bottom.

From the user perspective, the DECT phone key lock with PIN is not active by default but can be activated through the DECT phone UI. For GDPR compliance activate the timer. The user may set his individual PIN.

If the active flag is not set, the whole feature is disabled, and the key lock DECT phone menu is removed from the DECT phone UI. The submenu “Enter new PIN” remains. This is necessary, because the PIN may be mandatory to open some DECT phone menus like “Security”, or others if configured by COA. The user shall have the opportunity to change the PIN by himself, even if key lock feature is disabled.

The DECT phone key lock PIN to protect the Mitel 600 DECT phone is reset to default “0000” on user logout to improve usability in shift worker scenarios. Additionally, user call filter and private caller lists are removed from the DECT phone.

The PIN for key lock is restored on user login to the DECT phone.

The Mitel 600 DECT Phone USB interface is locked automatically when the phone is locked with a PIN.

6.10.5 CREATING DECT PHONE DATASETS

Creating DECT phone datasets is only possible in Configuration Mode. You can create the fixed DECT phone dataset or only the DECT phone user data.

To create a DECT phone dataset, do the following:

- 1 Click **Create** under the Task list on the right-hand side of the **DECT Phones** window.

- In the **Overview** submenu you can create a fixed DECT phone dataset (with combined user and device data).
- In the **Users** submenu you can create an unbound user. This user can login and log out on any configured device.

The DECT phone detail panel opens and provides tabs where the DECT phone data must be entered.

- 2 Configure the DECT phone, see parameter description in section 6.10.4.
- 3 Press the **OK** button.

6.10.6 CONFIGURING DECT PHONE DATASETS

Configuring DECT phone datasets is only possible in Configuration Mode. To configure an existing DECT phone dataset proceed as follows:

- 1 Select a DECT Phone from the table, and click **Configure** under the Task list on the right-hand side of the **DECT Phones** window.
 - In the **Overview** submenu you can configure the whole DECT phone dataset (user and device data).
 - In the **Users** submenu you can configure the DECT phone user data.
 - In the **Device** submenu you can configure the DECT phone device data.

The DECT phone detail panel opens.

- 2 Change the DECT phone dataset as desired, see parameter description in section 6.10.4.
- 3 Press the **OK** button.

6.10.7 SUBSCRIBING DECT PHONE DATASETS

After adding a DECT phone dataset to the OMM, the DECT phone must be subscribed. The OMM must first be enabled to allow subscriptions from DECT phones. Subscribing DECT phone datasets is possible in the **Overview** panel and in the **Device** panel. To start subscription, press one of the following commands in the **DECT phones** menu:

- **Subscription:** Start DECT phone subscription with configured IPEI. For more information on this see section 5.7.3.1.
- **Wildcard subscription:** Start DECT phone wildcard subscription (without configured IPEI). In the **Wildcard subscription** dialog, which is now opened, enter the **Timeout** for this subscription method. Press the **Start** button. For more information on this see section 5.7.3.2.

6.10.8 DELETING DECT PHONE DATASETS

Deleting DECT phone datasets is only possible in **configuration mode**. You can delete the fixed DECT phone dataset (in case of fixed relation) or only the DECT phone user data resp. the DECT phone device data (in case of dynamic relation).

To delete one or more existing DECT phone datasets proceed as follows:

- 1 Select the appropriate DECT phone dataset(s) in the DECT phone table by activating the corresponding checkbox(es).
- 2 In the task bar on the right of the **DECT phones** panel click on the **Delete** command.

- In the **Overview** submenu the whole DECT phone dataset will be deleted.
- In the **Users** submenu only the DECT phone user data will be deleted.
- In the **Devices** submenu only the DECT phone device data will be deleted.

The **Delete [xxx]** dialog opens showing a confirmation prompt.

- 3 Confirm the displayed prompt with **OK**.

6.10.9 SELECTING COLUMNS

You can adapt the parameters shown in the DECT phone table to your needs:

- 1 Click **Select columns** under the Task list on the right-hand side of the **DECT Phones** window.
The **Select columns** dialog opens.
- 2 Select the columns that shall be shown by activating the appropriate checkboxes.
- 3 Click the **OK** button.
- 4 The DECT phone table will be adapted accordingly.

6.10.10 FILTERING DECT PHONE TABLE

You can filter the list of DECT phone datasets shown in the DECT phone table by using a filter.

- 1 Click **Filter** under the Task list on the right-hand side of the **DECT Phones** window.
The **Filter** dialog opens.
- 2 Enter the search string that serves as filter criterion. You can enter digits and characters. The search is case sensitive.
- 3 Click on the **Filter** button.
The **Filter** dialog is closed and the DECT phone table will be adapted accordingly.
- 4 To reset the filter, click on the **Filter** command in the task bar on the right of the **DECT phones** panel.
- 5 In the **Filter** dialog click on the **Reset** button.

6.10.11 CHANGING THE RELATION TYPE

You can change a user data-device relation data set from “fixed” to “dynamic” and vice versa. This means the login/logout feature can be enabled or disabled for a DECT phone. The user data device relation can only be changed by the admin user.

To change the relation type of a DECT phone:

- 1 Select the appropriate DECT phone dataset(s) in the DECT phone table by activating the corresponding checkbox(es).
- 2 Click **Change rel. type** under the Task list on the right-hand side of the **DECT Phones** window.

Rules to change the relation from “fixed” to “dynamic”

- The DECT phone must be subscribed.
- A user login/logout PIN is configured in the user data set.

- Depending on the DECT phone user login type (“LoginID”), in the **DECT** tab of the **System settings** menu, the **Login ID** option must be set in the **DECT phone user login type** field.

IMPORTANT : If there is no specific PIN configured then “0000” is automatically set.

Rules to change the relation from “dynamic” to “fixed”

- The user relation type must be “Dynamic” (not “Unbound”).
- The user data set is not retrieved from an external user data server / the user data set is provisioned locally in the OMM database.

6.10.12 ENABLING / DISABLING DECT PHONE EVENT LOG

You can store a DECT phone event log file in **Monitor Mode**. Do the following:

- 1 To enable/disable the DECT phone event log, click **Log events** under the Task list on the right-hand side of the **DECT Phones** window:

✓ - DECT phone event log is enabled.

✗ - DECT phone event log is disabled.

- 2 Repeat step 1 to disable/enable the DECT phone event log.

The DECT phone event log will be stored in a file called “pp_event.log“. This file can be found in the user’s home directory:

- On a Linux system it is located under ‘~/oamp’,
- On a windows system under ‘c:/Users/<user>/MyDocuments/.Oamp’.

6.10.13 USER MONITORING





User monitoring menu available in monitoring mode only a list of the DECT Phone users who are configured for user monitoring.

The following parameters are displayed for each DECT Phone user:

- User ID
- Name
- Number
- Related device ID
- Mode: User monitoring mode (active or passive)
- Combined User Status (CUS)
- Handset Assignment Status (HAS) (Dynamic User logged on)
- Handset Subscription Status (HSS) (DECT subscribed)
- Handset registration status (HRS) (DECT attached)
- Handset activity status (HCS) (Handset active within time period)
- SIP user registration status (SRS) (SIP user registered)
- Silent charging status (SCS) (Silent charging + Charger)
- Call diversion status (CDS) (immediate call diversion enabled)

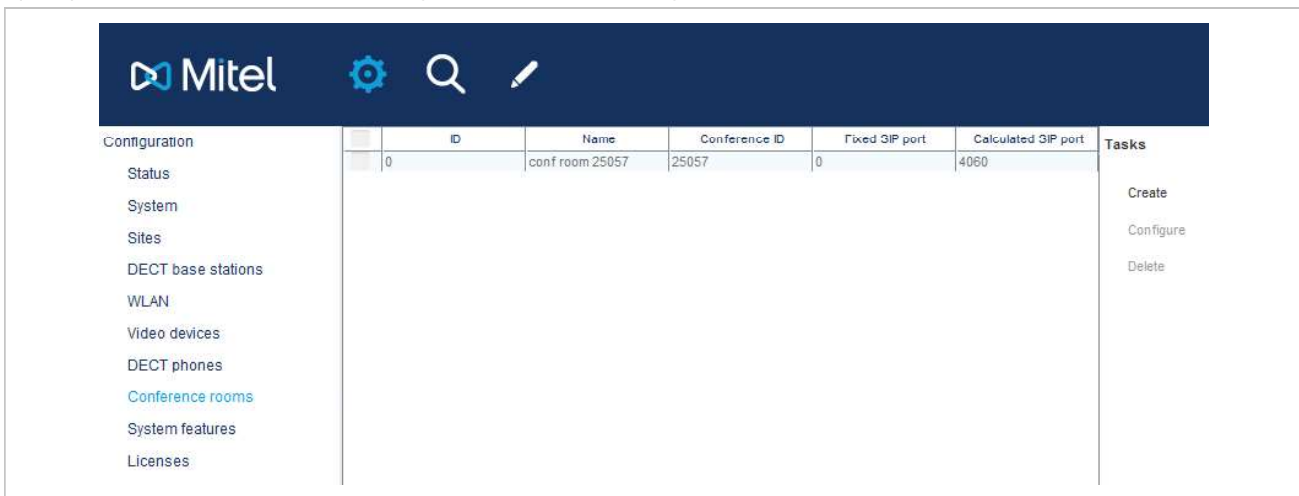
- Handset battery status (HBS) (Battery power above limit, warn only)
- Software status (SWS) (minimal required software version, warn only)

Monitoring parameter can have these values:

-  - Available
-  - Warning
-  - Unavailable
-  - Escalated

6.11 “CONFERENCE ROOMS” MENU

On this menu page you managed individual conference rooms for the Integrated Conference Server (ICS). For details on how to configure the conferencing feature, see section [8.21](#).



ID	Name	Conference ID	Fixed SIP port	Calculated SIP port	Tasks
0	conf room 25057	25057	0	4060	Create Configure Delete

The tasks which can be performed are mode-dependant.

Configuration mode	Monitor mode	See section
Create: Create conference room		6.11.1
Configure: Configure selected conference room		6.11.2
	Show details: Show details about a selected conference room	6.11.4
Delete: Delete selected conference room		6.11.3

6.11.1 CREATING CONFERENCE ROOMS

In **Configuration Mode** you can create new conference rooms. Conference rooms will be registered on the configured SIP registrar, thus you must enter the SIP account data to be used.

The screenshot shows a 'New conference room' dialog box with the following fields and controls:

- Name:** A text input field.
- Conference ID:** A text input field.
- User name:** A text input field.
- Password:** A password input field with masked characters (*****).
- Password confirmation:** A password input field with masked characters (*****).
- Fixed SIP port:** A numeric input field containing the value '0'.
- Calculated SIP port:** A disabled numeric input field.
- Buttons:** 'OK' (disabled) and 'Cancel' (active) buttons at the bottom.

- 1 Click **Create** in the **Tasks** menu of the **Conference rooms** page.
- 2 In the **General** tab, enter the conference room parameters.
 - **Name:** Enter the SIP display name for the SIP account to be used.
 - **Conference ID:** Enter the SIP user id.
 - **User name:** Enter the SIP authentication name.
 - **Password, Password confirmation:** Enter the password that is required by the SIP server.
 - **Fixed SIP port:** Enter the port used explicitly for SIP signaling. If set to 0, an automatically calculated port is used for this conference room. The default is 0. See section [2.17](#) for more information on this feature.
- 3 Click **OK**.

6.11.2 CONFIGURING CONFERENCE ROOMS

In **Configuration Mode** you can configure an existing conference room.

- 1 Select the appropriate conference room entry in the conference rooms table.
- 2 Click **Configure**.
The **General** tab is displayed showing the current conference room configuration.
- 3 Change the conference room parameters as required.
- 4 Click **OK**.

6.11.3 DELETING CONFERENCE ROOMS

In **Configuration Mode**, you can delete conference rooms.

- 1 Select one or more conference rooms entries in the conference rooms table.
- 2 Click **Delete**.
A confirmation dialog appears.
- 3 Click **OK** to confirm.

6.11.4 VIEWING CONFERENCE ROOM DETAILS

In **Monitor Mode**, you can view the details of a conference room.

- 1 Select the appropriate conference room entry in the conference room table.
- 2 Click **Show details**.
The **General** tab is displayed showing the conference room configuration.
- 3 Click **Cancel** to close the tab.

6.12 “ALARM TRIGGERS” MENU “SYSTEM FEATURES” MENU

The **System features** menu provides the following entries:

Configuration mode	Monitor mode	See section
General settings	General settings	6.12.1
Feature access codes	Feature access codes	6.12.2
Alarm triggers	Alarm triggers	6.12.3
Digit treatment	Digit treatment	6.12.4
Directory	Directory	6.12.5
XML applications	XML applications	6.12.8
CoA profiles	CoA profiles	6.12.9

6.12.1 “GENERAL SETTINGS” MENU

The **General settings** menu allows to configure/view the FAC number prefix used for feature access codes and alarm triggers.

- 1 **FAC number and prefix for alarm triggers:** Enter a unique FAC number.
- 2 Press the **OK** button.

6.12.2 “FEATURE ACCESS CODES” MENU

The **Feature access codes** menu is used to configure/view the feature access codes parameters.

The **FAC number** which introduces the feature access code (see also section 6.12.1) is displayed. For a description of the parameters which can be set in this menu see section 5.9.4.

6.12.3 “ALARM TRIGGERS” MENU

The **Alarm triggers** menu allows configuration and display of numerous alarm trigger datasets. There are two predefined alarm triggers (“SOS” and “MANDOWN”) which cannot be deleted.

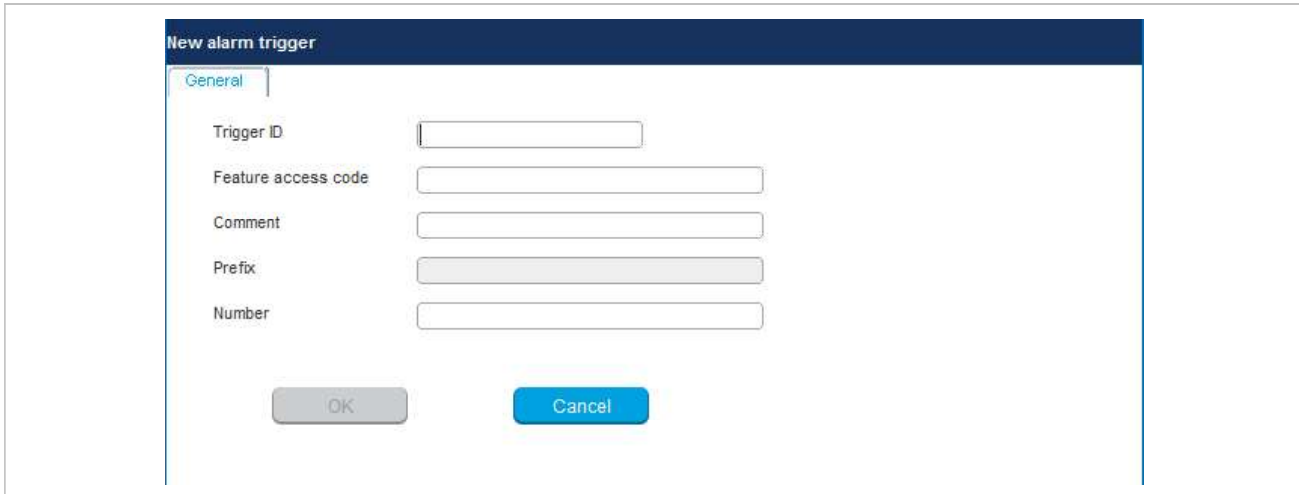
ID	Trigger ID	Feature access code	Comment	Number
0	SOS	SOS		
1	MANDOWN	MANDOWN		

The tasks which can be performed are mode-dependant.

Configuration mode	Monitor mode	See section
Create: Create alarm trigger		6.12.3.1
Configure: Configure a selected alarm trigger		6.12.3.2
	Show details: Show parameters of a selected alarm trigger	6.12.3.4
Delete: Delete selected alarm triggers		6.12.3.3

6.12.3.1 Creating “Alarm triggers”

In **Configuration Mode** you can create new alarm triggers.



- 1 Click **Create**. In the **General** tab enter the alarm trigger parameters.
- 2 **Trigger ID:** Enter the AlarmTrigger ID that the OMM sends to identify the alarm scenario and the source that triggers the alarm.
- 3 **Feature access code:** Enter the feature access code that the user dials to initiate the alarm.
- 4 **Comment:** Enter a comment for the new trigger.
- 5 **Prefix:** This field displays the **FAC number** which introduces the feature access code (see also section [6.12.1](#)).
- 6 **Number:** Enter the number to be called if the user triggers the alarm by dialing the feature access code. If no number is specified, the call is released.
- 7 Press the **OK** button.

6.12.3.2 Configuring “Alarm triggers”

In **Configuration Mode** you can configure an existing alarm trigger.

- 1 In the alarm trigger table click on the appropriate trigger entry.
- 2 Click **Configure**.
The **General** tab is displayed showing the current trigger configuration.
- 3 Change the trigger parameters.

4 Press the **OK** button.

6.12.3.3 Deleting “Alarm triggers”

In **Configuration mode** you can delete alarm triggers. The predefined alarm triggers ('SOS and 'Man down') cannot be deleted.

- 1 In the alarm trigger table click on one or more trigger entries.
- 2 Click **Delete**.
- 3 Confirm the displayed prompt with **OK**.

6.12.3.4 View “Alarm trigger” Details

In **Monitor Mode** you can view the details of an alarm trigger.

- 1 In the alarm trigger table click on the appropriate trigger entry.
- 2 Click **Show details**.
The **General** tab is displayed showing the trigger configuration.
- 3 Click **Cancel** to close the tab.

6.12.4 “DIGIT TREATMENT” MENU

The **Digit treatment** menu allows you to configure the number manipulation that is provided by the digit treatment feature for LDAP corporate directories.

ID	Type	Active	Name	Order
1	LDAP	✓	grmr	0
2	XML	✓	XML-Test	4
3	LDAP	✓	tres	1
4	LDAP	✓	nrtnrs	2
5	XSI Personal	✓	XSI personal	5

Directory entry #5

General | URL

Type: XSI Personal (dropdown menu open showing: LDAP, XML, XSI Enterprise, XSI Enterprise common, XSI Group, XSI Group common, XSI Personal)

Active:

Name:

Search base:

Search type: Surname (dropdown menu)

Display type: Surname, given name (dropdown menu)

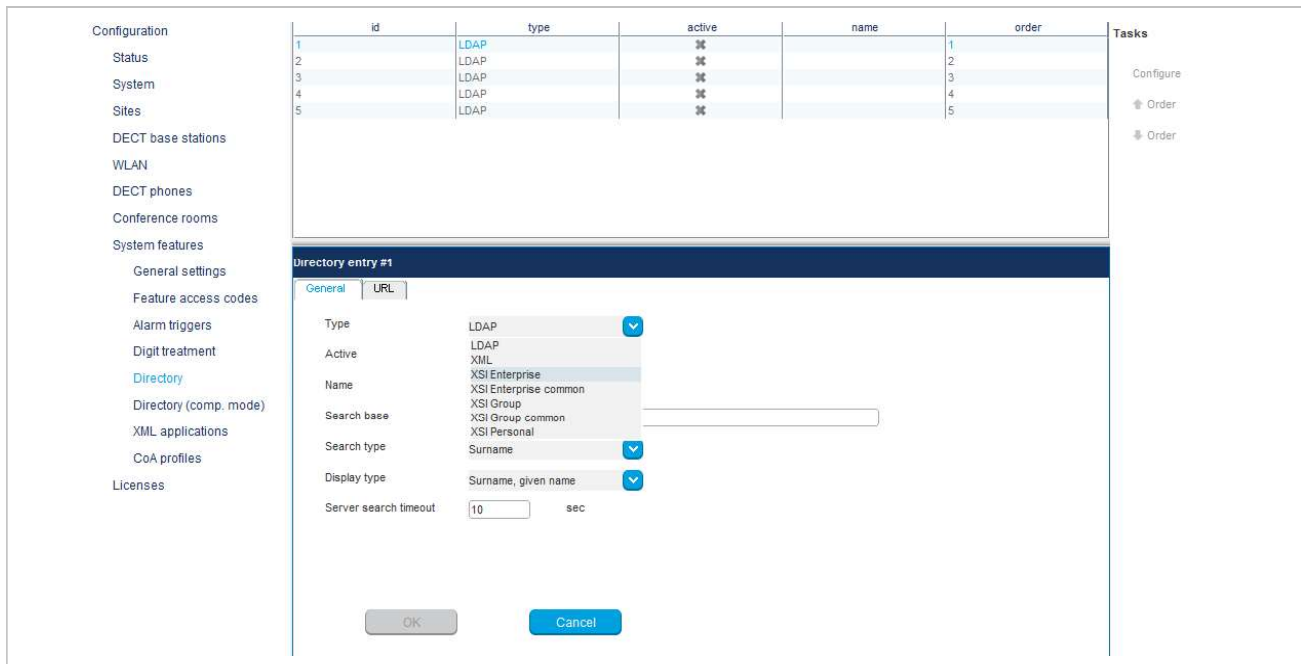
Server search timeout: 10 sec

OK | Cancel

For a description of tasks and parameters available in this menu, see section 5.9.1.

6.12.5 “DIRECTORY” MENU

The **Directory** menu allows configuration of LDAP, XML or XSI -based corporate directory services.



The tasks which can be performed are mode-dependant.

Configuration mode	Monitor mode	See section
Create: Create new directory entry in detail panel		6.12.5.1
Configure: Configure selected directory entry in detail panel		6.12.5.2
	Show details: Show selected directory entry in detail panel	6.12.5.3
Delete: Delete selected directory entry/entries		6.12.5.4

6.12.5.1 Creating New Directory Entries

Adding directory entries is only possible in **configuration mode**. You can configure up to five directory entries. To add a new entry, do the following:

- 1 In the **Tasks** panel, click **Create**.

The **New directory entry** panel opens and provides various tabs where the directory data must be entered.

- 2 Configure the directory entry (see parameter descriptions below).
- 3 Click **OK** to save your changes.

You can specify values for the following parameters in the **New directory entry** panel:

General tab

The following table describes the parameters on the General tab and to which directory type they apply.

Parameter	Description	LDAP	XML	XSI
Type	Interface type supported by the directory server. Possible values: <ul style="list-style-type: none"> • LDAP • XML • XSI Enterprise • XSI Enterprise common • XSI Group • XSI Group common • XSI Personal 	✓	✓	✓
Active	Enables or disables the directory entry on the DECT phone.	✓	✓	✓
Name	Name to be displayed for the directory (Latin-1 character set is supported). Note: If there is only one directory entry configured, this value is ignored when the user searches for a number in the telephone's central directory. SIP-DECT 6.0 and later supports the "SIPProxy" placeholder for a directory entry name, in place of the current primary, secondary or tertiary SIP server address.	✓	✓	✓
Search base	Location in the LDAP directory from which the search begins (e.g., "ou=people, o=my com"). The configuration is valid for all DECT phones that support the LDAP directory feature. To make search requests unique for different users, the search base configuration can include placeholders that are replaced by user-specific values when submitting the LDAP request to a server. The following placeholders are defined: <ul style="list-style-type: none"> • "<TEL>" (for the user's telephone number) • "<DESC1>" (for the user's "Description 1" attribute) • "<DESC2>" (for the user's "Description 2" attribute) • "SIPProxy" (for the current primary, secondary or tertiary SIP server address); supported for release 6.1 and later 	✓		
Search type	Attribute on which searches are performed (Surname or Given name).	✓		✓
Display type	Display mode for search results (Surname , First Name or Given name Surname).	✓		✓
Server search timeout	Interval (in seconds) during which the OMM waits for search results from the LDAP server (1 – 10 seconds).	✓		

URL tab

The following table describes the parameters on the URL tab and to which directory type they apply.

Parameter	Description	LDAP	XML	XSI
Protocol	Transfer protocol used to communicate with the XML or XSI directory server (http or https).		✓	✓
Port	Server port number. Specify a value, or enable the Use default port flag. For LDAP, the default is 389. SSL (default port 689) is not supported. Windows Active Directory Server uses port 3268.	✓	✓	✓

Parameter	Description	LDAP	XML	XSI
	For XML or XSI, the default is 80 for HTTP, and 443 for HTTPS.			
Server	IP address or FQDN of the directory server.	✓	✓	✓
User name	Name of the account for directory server access, if required.	✓	✓	
Password	Password for directory server access, if required. Confirm the password in the next field. Note: If no user/password is specified, an anonymous bind takes place. SIP-DECT supports LDAP simple bind.	✓	✓	
Path (and parameters)	URL (with parameters, if required) to the XML directory on the XML directory server.		✓	
Use common certificate configuration	Enables or disables use of the system's certificates (loaded for provisioning purposes) for HTTPS directory access.		✓	✓

6.12.5.2 Changing a Directory Entry

Changing directory entry is only possible in configuration mode. To change the configuration of an existing directory entry, do the following:

- 1 Select the appropriate directory entry in the table.
- 2 Click **Configure** in the **Tasks** panel.
- 3 Change the directory entry parameters as required (see parameter descriptions in section 6.12.5.1).
- 4 Click **OK**.

6.12.5.3 Viewing Directory Entry Details

You can view the configuration of a directory in **Monitor Mode**. Do the following:

- 1 Select the appropriate directory entry in the table.
- 2 In the **Tasks** bar click **Show details**.
The directory entry data is displayed in the detail panel.
- 3 Click **Cancel** to close the directory entry detail panel.

6.12.5.4 Deleting Directory Entries

Deleting directory entries is only possible in **Configuration Mode**. To delete one or more existing entries, do the following:

- 1 Select the appropriate entry/entries in the directory entry table by activating the corresponding checkbox(es).
- 2 In the **Tasks** pane, click **Delete**.
A confirmation dialog opens.
- 3 Click **OK** to confirm.

6.12.6 EASY MIGRATION FROM CORPORATE DIRECTORY (COMP. MODE) TO NEW CORPORATE DIRECTORY STRUCTURE

If there is a corporate directory (comp. mode) entry and a new corporate directory structure entry with identical settings, then the corporate directory (comp. mode) entry gets automatically removed.

Use case: Migration from old to new structure with provisioning files w/o manual configuration and to avoid double entries.

The following parameters is considered for comparison:

- **Directory type (LDAP, XML)**
- **Name**
- **Server**
- **Path**

6.12.7 “DIRECTORY (COMP. MODE)” MENU

With the introduction of XSI directory support in SIP-DECT 6.2, the underlying database model for directory support in SIP-DECT has changed. To support backwards compatibility, the Directory (comp) page provides directory configuration and maintenance for existing SIP-DECT systems with LDAP or XML directory support.

The **Directory (comp. mode)** menu allows configuration of LDAP or XML corporate directory services.

Order	Type	Active	Name	Server
2	LDAP	✖	LDAP-Comp	10.103.35.134
1	XML	✔	XML-comp	10.135.35.134

Directory entry

General | LDAP | XML application

Type: XML

Active:

Order: 1

Name: XML-comp

OK Cancel

6.12.7.1 Creating New Directory Entries

Adding directory entries is only possible in **configuration mode**. You can configure up to five directory entries. To add a new entry, do the following:

- 4 In the **Tasks** panel, click **Create**.

The **New directory entry** panel opens and provides various tabs where the directory data must be entered.

- 5 Configure the directory entry (see parameter descriptions below).

6 Click **OK** to save your changes.

You can specify values for the following parameters in the **New directory entry** panel:

General tab

The following table describes the parameters on the **General** tab.

Parameter	Description
Type	Interface type supported by the directory server. Possible values: LDAP or XML.
Active	Enables or disables the directory entry on the DECT phone.
Order	Specifies where you want the directory to appear in the list.
Name	Name to be displayed for the directory (Latin-1 character set is supported). Note: If there is only one directory entry configured, this value is ignored when the user searches for a number in the telephone's central directory. SIP-DECT 6.0 and later supports the "SIPProxy" placeholder for a directory entry name, in place of the current primary, secondary or tertiary SIP server address.

LDAP tab

The following table describes the parameters on the **LDAP** tab (only available when LDAP is selected as the directory type).

Parameter	Description
Search base	Location in the LDAP directory from which the search begins (e.g., "ou=people, o=my com"). The configuration is valid for all DECT phones that support the LDAP directory feature. To make search requests unique for different users, the search base configuration can include placeholders that are replaced by user-specific values when submitting the LDAP request to a server. The following placeholders are defined: <ul style="list-style-type: none"> "<TEL>" (for the user's telephone number) "<DESC1>" (for the user's "Description 1" attribute) "<DESC2>" (for the user's "Description 2" attribute) "SIPProxy" (for the current primary, secondary or tertiary SIP server address); supported for release 6.1 and later
Search type	Attribute on which searches are performed (Surname or Given name).
Display type	Display mode for search results (Surname, First Name or Given name Surname).
Server	IP address or FQDN of the directory server.
Port	Server port number. The default is 389. SSL (default port 689) is not supported. Windows Active Directory Server uses port 3268.
User name	Name of the account for directory server access, if required.
Password	Password for directory server access, if required. Confirm in the next field. Note: If no user/password is specified, an anonymous bind takes place. SIP-DECT supports LDAP simple bind.
Server search timeout	Interval (in seconds) during which the OMM waits for search results from the LDAP server (1 – 10 seconds).

XML application tab

The following table describes the parameters on the **XML application** tab (only available when XML is selected as the directory type).

Parameter	Description
Protocol	Transfer protocol used to communicate with the XML directory server (HTTP or HTTPS).
Port	Server port number. Default is 80 for HTTP, and 443 for HTTPS.
Server	IP address or FQDN of the directory server.
User name	Name of the account for directory server access, if required.
Password	Password for directory server access, if required. Confirm the password in the next field.
Path (and parameters)	URL (with parameters, if required) to the XML directory on the XML directory server.

6.12.7.2 Changing a Directory Entry

Changing directory entry is only possible in configuration mode. To change the configuration of an existing directory entry, do the following:

- 1 Select the appropriate directory entry in the table.
- 2 Click **Configure** in the **Tasks** panel.
- 3 Change the directory entry parameters as required (see parameter descriptions above).
- 4 Click **OK** to save your changes.

6.12.7.3 Viewing Directory Entry Details

You can view the configuration of a directory in **Monitor Mode**. Do the following:

- 1 Select the appropriate directory entry in the table.
- 2 In the **Tasks** bar click **Show details**.
The directory entry data is displayed in the detail panel.
- 3 Click **Cancel** to close the directory entry detail panel.

6.12.7.4 Deleting Directory Entries

Deleting directory entries is only possible in **Configuration Mode**. To delete one or more existing entries, do the following:

- 1 Select the appropriate entry/entries in the directory entry table by activating the corresponding checkbox(es).
- 2 In the **Tasks** bar click **Delete**.
A confirmation dialog opens.
- 3 Click **OK** to confirm.

6.12.8 “XML APPLICATIONS” MENU

The SIP-DECT XML terminal interface allows external applications to provide content for the user on the Mitel 600 DECT phone display. To make the XML terminal interface applications available to the DECT phone user, the relevant hooks must be configured in the **XML applications** menu.

There are 15 predefined hooks and 10 hooks which can be freely defined. For a full list of the predefined hooks and their descriptions, see section 5.9.5.

These hooks can be activated or deactivated but not deleted. Up to 10 additional hooks can be created dynamically.

Please note: “Caller list” and “Redial list” replace the local caller and redial lists of the Mitel 600 if activated. These XML hooks can also be used to enable the centralized call log feature (MX-ONE systems only). Additionally the list access must be set to “Automatic” or “PBX” on the DECT phone in the “Settings > List access” menu. If the list access is set to “Local”, the local list is used by the DECT phone.

Note: An XML directory entry is also read-only listed in the XML applications menu. For information on configuring XML directories please see section 6.12.5.1.

An activated hook becomes available on a DECT phone (including the corresponding menu entry) after the next DECT location registration of the DECT phone. This can be forced by switching the DECT phone off and on. The same applies if a hook is deactivated.

