

SIP-DECT OM System Manual

ADMINISTRATION GUIDE

Release 10.0



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 10.0 March 2025

®,™ Trademark of Mitel Networks Corporation
© Copyright 2025 Mitel Networks Corporation
All rights reserved

CONTENTS

1	Overview	12
1.1	The SIP-DECT Solution	12
1.2	About DECT Base Stations	13
1.2.1	DECT Base Station Families	13
1.2.2	OpenMobility Manager (OMM) Mode	16
1.3	About the OpenMobility Manager	17
1.3.1	OMM Tasks	17
1.3.2	SIP-DECT Special Features and Capabilities	18
1.3.3	OMM Capacities and Features	18
1.3.4	OMM Capacities and RFP Support	19
1.4	About DECT Phones	19
1.5	File naming conventions	20
1.6	Login and passwords	20
2	Enhanced Feature Overview	22
2.1	Application initiated SIP-DECT conference via messaging	22
2.2	Software Upload via OMM Web Interface on RFP4G	22
2.3	Dynamic XML application index	23
2.4	Restrict Access Attempts to the SIP-DECT OMM Web Administration Portal	24
2.5	Secure Remote Management for OMM and Event Manager on RFP4x through Mitel Administration Portal	24
2.6	732d and 742d Generate Distinct Sensor Alarm Types for Man Down, No Movement, and Escape	25
2.7	MDUG Prime DN on SIP DECT Idle Display	26
2.8	Support for Enable/disable 100rel tag in the SIP supported header via config parameter	28
2.9	Calls to/from SIP-DECT not possible or unencrypted	29
2.10	Signalling options for 'Hold' in Session Description Protocol (SDP) inactive / sendonly	30
2.11	Singular VOIP profile for each OS4K gateway	31
2.12	8 channel Hi-Q Audio with Mitel 700d DECT phones and 4th Generation RFPs	33
2.13	Enable/disable admin interfaces	34
2.14	BV32 Codec Support on Mitel 700d Handsets	36
2.15	Setting Security level via OMM Web service	36
2.16	Improvements of the time zone settings for SIP-DECT OVA deployments	37
2.17	ESXI time synchronization disabled for SIP-DECT OVA deployments	37
2.18	Migration from earlier releases	38
2.18.1	Conversion of provisioning related data	38
2.18.2	SW update	39
2.19	OMM Web Service	42
2.19.1	Provisioning & Software Update	43
2.19.2	Changes on the Status Web page	46
2.20	OMP	48
2.20.1	Provisioning & Software Update	48
2.20.2	Status DECT base station - Software Update	56
2.21	Keep DB from former release and support automatic fallback in upgrade/downgrade scenarios	57
2.22	SIP "TLS-Common-Name-Validation" flag renamed to "Validate host name"	58
2.23	SIP "TLS-Authentication" flag renamed to "Validate certificates"	60
2.24	Harmonization of the certificate validation & security handling settings	60
2.25	Validate host name and Validate expires only relevant if Validate certificates flag is set	60
2.26	URL parameter for various URLs "Use common certificate configuration" flag renamed to "Use provisioning security configuration"	60
2.27	OMP provisioning TLS/SSL settings renamed to "Security"	60
2.28	OMM Web Provisioning "Certificates" settings renamed to "Security"	61
2.29	OMM and MOM certificate update	62
2.30	RFP43 WLAN and RFP 48 WLAN affected by FragAttack vulnerability	62
2.31	Discontinue "SSL version" parameter in MOM	62
2.32	Emergency Location Identification Number (ELIN) support	62
2.33	Manual User Data Import AXI command discontinued	65
2.34	Update Trusted Cert Chain Store	66
2.35	Update to OpenLDAP 2.4.59	66

2.36	Update to AdoptOpenJDK 11.0.19	66
2.37	Enhancement to manual download	66
2.38	HTTP 302 status code supported by OMM provisioning	66
2.39	Restriction In Adding new directory entries in Directory	66
2.40	Enhancement to Default TTL value	66
2.41	Discontinue TFTP server list and preferred TFTP server	66
2.42	Discontinue non-encrypted XML API interfaces	67
2.43	Discontinued RFP35 USB Web Cam Video Support	67
2.44	mTLS support for provisioning	67
2.45	New OMM Web service and OMP section: "Support"	67
2.46	Support of Additional crypto suite	68
2.47	Enhancement to Base Station	68
2.48	Set Cloud-ID key Using OMM configuration files	68
2.49	Automatically truncate user names exceeding 20 characters	69
2.50	DNS SRV mode for SIP signaling	69
2.51	Supporting automatic fallback in upgrade/downgrade scenarios	70
2.52	Supporting Egyptian regulations	71
2.53	Enhancement to SDP signaling when holding a call	72
2.54	RFP43 and RFP48: 802.1x bind WPA supplicant to bridge interface	72
2.55	TLS cipher suites configuration	73
2.55.1	TLS Security Levels	73
2.55.2	Default settings	74
2.55.3	Customized cipher suites	75
2.55.4	Applying configuration changes	75
2.55.5	Retrieving factory defaults	76
2.55.6	Displaying supported cipher suites	76
2.56	Enhancement to TLS Support	77
2.57	Secure LDAP Support	78
2.58	New or changed Parameters	78
2.58.1	Provisioning parameters	78
2.58.2	RTP source port filter	87
2.58.3	SIP re-Register on TLS reconnects	88
2.59	User data import	89
2.59.1	User_common.cfg	89
2.59.2	<user>.cfg	89
2.59.3	Migration from previous releases:	90
2.60	Updating Software	90
2.60.1	Download and distribution of base station software	91
2.60.2	Activation of new base station software	91
2.60.3	Updating PC OMM	92
2.61	Enhancement to Provisioning	93
2.62	RFP Enrolment encryption with authentication key	97
2.62.1	RFP connection status in OMM: encryption activated	98
2.62.2	Re-enrolment function	98
2.62.3	Switch between software versions that support and do not support authentication keys	99
2.62.4	Authentication key mismatch scenarios	100
2.62.5	Support and maintenance	102
2.63	Distinctive ringtone	102
2.64	Software Update Dispersion	102
2.65	SIP-DECT XML terminal interface	103
2.65.1	Feature Access Codes Translation	103
2.65.2	Ring Tone Selection for (Alarm) Messages	104
2.65.3	DECT Phone Charger Events	104
2.65.4	RFP43 AND RFP48: 802.1X BIND WPA SUPPLICANT TO BRIDGE INTERFACE	106
2.66	Auto answer, intercom calls and audio settings	106
2.66.1	Intercom Calls	106
2.66.2	Auto answer audio settings	107
2.67	SIP enhancements	108
2.67.1	Globally Routable User-Agent URIs (GRUUs)	108
2.67.2	Session timer	108
2.67.3	SIP Contact matching	108

2.67.4	Configurable Call reject state codes	108
2.67.5	Call release timers	108
2.67.6	Incoming call timeout	108
2.67.7	Call reject on silent charging	108
2.67.8	route header	109
2.67.9	MWI SUBSCRIPTION period	109
2.68	System configuration tools	109
2.69	Integration into external management systems	110
2.70	Corporate directory integration	110
2.71	User monitoring	110
2.72	Extended messaging	111
2.73	Truncating SIP User Name in SIP URI	111
2.74	Call handling	111
2.74.1	Diversion indication	111
2.74.2	Call completed elsewhere	112
2.74.3	Semi-Attended Transfer	112
2.74.4	Third Line Handling for Mitel 142d and 600/700 DECT Phones	112
2.74.5	Call Transfer Enhancements for Mitel 142d DECT phones	113
2.75	Voice mail number	114
2.76	Alphanumeric dialing	114
2.77	UTF-8 encoding	114
2.78	SIP multiport	115
2.79	SIP over UDP/TCP/TLS	116
2.80	Conferencing	116
2.80.1	Conferencing audio notification	117
2.80.2	Centralized conferencing with MiVoice Business	117
2.80.3	N-WAY CONFERENCING	117
2.81	Hot Desking	118
2.82	DECT phone functionality	118
2.82.1	DECT Phone Download over Air	118
2.82.2	Central DECT Phone Configuration Over Air (CoA)	119
2.82.3	OMM DECT phone provisioning	120
2.82.4	Mitel 600/700 DECT Phone Dial Editor Mode	120
2.82.5	Mitel DECT Phone Customizable Boot Texts	120
2.82.6	OMM-Centralized call logs	120
2.82.7	User individual DECT Phone PIN Key Lock	121
2.83	Extended regulatory domain support	121
2.84	Simplified licensing	122
2.85	System redundancy	122
2.85.1	OMM standby	122
2.85.2	Backup SIP proxy/registrar	122
2.85.3	Configurable User Account for Standby Check	122
2.85.4	Multi-OMM Manager for OMM-centralized management	123
2.86	DECT base station Reset to Factory Settings	123
2.86.1	RFP4G reset to factory defaults	123
2.87	DECT base station synchronization	124
2.87.1	Clustering and paging areas	124
2.88	Wireless LAN (WLAN)	125
2.88.1	802.11i: WPA2-Enterprise Pre-Authentication for fast Roaming	125
2.88.2	Channel Configuration Feedback for HT40 and tx Power	125
2.88.3	Channel Configuration Feedback for HT80	125
2.89	VoIP encryption	126
2.90	Mixed DECT base station installations	126
2.91	DECT enhanced security	126
2.92	Wideband (Mitel Wideband Audio G.722 technology)	127
2.93	DECT XQ	127
2.94	PC-based OMM installation	128
3	Licensing	129
3.1	Licensing Model	129
3.1.1	System Licenses	129

3.1.2	About G.729 Channels	130
3.1.3	PARK Service	130
3.1.4	Upgrade License	131
3.1.5	Grace Period	131
3.1.6	License Violations and Restrictions	131
3.2	Uploading a License File	132
3.3	License Models	132
3.3.1	Small System (Unlicensed)	132
3.3.2	Medium or Large System	133
4	Getting Started.....	134
4.1	Base Station Startup Configuration	134
4.2	Configuring RFP by using the configuration button	134
4.2.1	Benefits	135
4.3	System Configuration	135
4.4	System Settings	135
4.5	Base Stations	136
4.6	SIP settings	136
4.7	DECT Phones	137
4.7.1	DECT Phone and SIP state verification	138
5	Local DECT Base Station Configuration (OM Configurator).....	140
5.1	Overview	140
5.2	Installation	141
5.3	Selecting the Network Interface	142
5.4	Adding DECT Base Stations for configuration	142
5.5	Scanning for DECT Base Stations	142
5.6	Adding DECT Base Stations manually	143
5.7	Loading DECT Base Station data from File	143
5.8	Editing DECT Base Station configuration data	143
5.8.1	Other parameter section	144
5.8.2	Copy and Paste	144
5.8.3	Configuration Parameters	145
5.9	Applying Configuration Changes	146
5.10	Factory Reset	146
5.11	Saving and Loading a DECT Base Station List	147
5.12	Removing DECT Base Station Entries	147
5.13	Compatibility with Older SIP-DECT Releases	147
6	OMM Web Service.....	148
6.1	Login	148
6.2	Logout	149
6.3	"Status" Menu	149
6.4	"System" Menu	150
6.4.1	"System Settings" Menu	150
6.4.2	"Provisioning & Software Update" Menu	154
6.4.3	"SIP" Menu	159
6.4.4	"User administration" Menu	169
6.4.5	"Time zones" Menu	170
6.4.6	"SNMP" Menu	172
6.4.7	"DB management" Menu	173
6.4.8	"Event log" Menu	175
6.5	"Sites" Menu	176
6.5.1	Creating a New Site	177
6.5.2	Editing a Site	177
6.5.3	Deleting a Site	178
6.6	"Base Stations" Menu	178
6.6.1	Base Station States	179
6.6.2	OMM / RFP Software Version Check	180
6.6.3	Creating and Changing Base Stations	180
6.6.4	Capturing DECT Base Stations	182

6.6.5	Deleting DECT Base Stations	182
6.6.6	Find my SIP-DECT Base Station	182
6.7	"SIP Users/Devices" menu	184
6.7.1	User-device relationship icons	184
6.7.2	Creating SIP Users/Devices	185
6.7.3	Editing SIP user/device settings	186
6.7.4	Importing SIP user or device Configuration Files	187
6.7.5	Searching the SIP user or device List	187
6.7.6	Deleting sip users/devices	188
6.7.7	Creating fixed or unbound linked users and devices	188
6.7.8	Modifying Fixed or unbound linked users and devices	189
6.7.9	Dect authentication code	189
6.7.10	Subscribing DECT Phones	190
6.7.11	Auto-create on subscription	191
6.7.12	Displaying User and DECT Phone Data	191
6.8	"WLAN" Menu	195
6.8.1	"WLAN profiles" Menu	195
6.8.2	"WLAN clients" Menu	201
6.9	"System features" Menu	201
6.9.1	"Digit treatment" Menu	201
6.9.2	"Directory" Menu	203
6.9.3	"Directory (comp. mode)" menu	204
6.9.4	"Feature Access Codes" Menu	206
6.9.5	"XML Applications" Menu	207
6.10	"Licenses" Menu	210
6.11	"Info" Menu	210
6.12	"Support" Menu	210
6.12.1	DECT phones firmware update	211
6.12.2	Syslog	212
6.12.3	System dump	212
6.12.4	Core Dump	212
7	OM Management Portal (OMP)	214
7.1	Overview	214
7.2	Installation	214
7.3	Login	214
7.4	Logout	215
7.5	OMP Main Window	215
7.6	"Status" Menu	216
7.6.1	Overview	217
7.6.2	DECT base stations	218
7.6.3	Users	219
7.6.4	Devices	220
7.6.5	Sites	221
7.6.6	Conference	222
7.6.7	Provisioning	222
7.6.8	Provisioning Health report	223
7.7	"System" Menu	223
7.7.1	"Basic settings" Menu	224
7.7.2	"Advanced settings" Menu	226
7.7.3	"Statistics" Menu (Monitoring Mode Only)	233
7.7.4	"SIP" Menu	234
7.7.5	"SIP Profiles" Menu	240
7.7.6	"Provisioning" Menu	241
7.7.7	"User administration" Menu	249
7.7.8	"Data management" Menu	252
7.7.9	"Event Log" Menu	254
7.8	"Sites" Menu	256
7.9	"DECT Base Stations" Menu	257
7.9.1	"Device list" Menu	257
7.9.2	"PAGING AREAS" MENU	265

7.9.3	"Capturing" Menu	266
7.9.4	"Enrolment" Menu	267
7.9.5	"Export" Menu	267
7.9.6	"Sync view" Menu	268
7.9.7	"Statistics" Menu	269
7.9.8	"Quality" Menu	270
7.10	"WLAN" Menu	273
7.10.1	Profiles	273
7.11	"DECT Phones" Menu	277
7.11.1	"Overview" Menu	277
7.11.2	"Users" Menu	280
7.11.3	"Devices" Menu	280
7.11.4	Device Detail Section	281
7.11.5	Creating DECT phone Datasets	288
7.11.6	Configuring DECT phone Datasets	289
7.11.7	Subscribing DECT phone Datasets	289
7.11.8	Deleting DECT phone Datasets	289
7.11.9	Selecting Columns	290
7.11.10	Filtering DECT phone Table	290
7.11.11	Changing the Relation Type	290
7.11.12	Enabling / Disabling DECT phone Event Log	291
7.11.13	User Monitoring	291
7.12	"Conference rooms" Menu	292
7.12.1	Creating Conference Rooms	292
7.12.2	Configuring Conference Rooms	293
7.12.3	Deleting Conference Rooms	293
7.12.4	Viewing Conference Room Details	294
7.13	"System features" Menu	294
7.13.1	"General settings" Menu	294
7.13.2	"Feature access codes" Menu	295
7.13.3	"Alarm triggers" Menu	296
7.13.4	"Digit treatment" Menu	298
7.13.5	"Directory" Menu	298
7.13.6	Easy migration from corporate Directory (comp. mode) to new corporate Directory structure	301
7.13.7	"Directory (comp. mode)" Menu	301
7.13.8	"XML applications" Menu	304
7.13.9	"CoA Profiles" Menu	307
7.14	"Licenses" Menu	308
7.15	"Support" menu	310
7.15.1	DECT phones firmware update	310
7.15.2	Syslog	311
7.15.3	SYSTEM DUMP	311
7.15.4	Remote system dump	311
7.15.5	Core Dump	311
7.16	"General" Menu	312
7.17	"Help" Menu	313
8	DECT Phone	315
8.1	Key lock with PIN	315
8.1.1	Maintain the PIN	315
8.1.2	Unlock a locked Mitel 600/700 DECT phone	315
8.1.3	Set up automatic key lock with PIN	316
9	Configuration and Administration	317
9.1	IP Signaling and Media Stream	317
9.2	DECT Base Station Synchronization	319
9.2.1	Initial Synchronization Procedure	320
9.2.2	Checking the Synchronization of a Network	321
9.3	DECT Base Station Channel Capacity	321
9.4	Network Infrastructure Prerequisites	322
9.5	SIP-DECT Startup	322

9.5.1	TFTP and DHCP Server Requirements	323
9.5.2	Booting Steps	323
9.5.3	Application Startup	323
9.5.4	RFP LEDs	327
9.6	SIP-DECT OMM setup using the configuration button	331
9.6.1	Find my SIP-DECT base station	333
9.6.2	Add RFPs to the installation	334
9.7	State Graph of the Start-up Phases	336
9.8	OMM Configuration and Resource Files	337
9.8.1	Configuration File URL	337
9.8.2	Specific Configuration URLs	339
9.8.3	ReLoad of Configuration and Resource files	340
9.8.4	AXI Commands in Configuration Files	340
9.8.5	User Configuration Files	343
9.8.6	Digest Authentication and Certificate Validation	344
9.8.7	DECT base station software Image from RFP OMM	345
9.8.8	Redirection and Configuration Service (RCS)	345
9.8.9	Customer Logo on OMM Web Service	346
9.9	DECT Base Station Configuration Files	346
9.9.2	Standard IP settings	347
9.9.3	Configuration file source	347
9.9.4	Parameter settings priority	348
9.9.5	Software update settings for 3 rd generation DECT base stations	348
9.9.6	SOFTWARE UPDATE SETTINGS FOR 4 th GENERATION DECT BASE STATIONS	348
9.9.7	Times when RFP configuration times are read	348
9.9.8	RFP configuration file update check	349
9.9.9	Handling of parameter changes	350
9.9.10	Configuration file syntax	350
9.10	Consolidated Certificate management	352
9.10.1	SIP over TLS certificates	352
9.10.2	OMM Certificate (Web service / AXI)	352
9.10.3	Provisioning certificates	353
9.10.4	Certificate validation	353
9.11	3 rd and 4 th Generation RFP Software Update	353
9.12	802.1Q Support	354
9.12.1	Boot Phase of IP RFPs (DHCP)	355
9.12.2	Boot Phase of IP RFPs (Local Configuration)	355
9.13	Installing OMM in Host Mode	355
9.13.1	System Requirements	356
9.13.2	Installing the OMM Software	356
9.13.3	Configuring the Start Parameters	357
9.13.4	Specific Commands – Troubleshooting	357
9.14	Updating the OMM	358
9.14.1	Updating a Single OMM Installation	358
9.14.2	Updating a Standby OMM Installation	359
9.15	OMM Standby	360
9.15.1	Configuring OMM Standby	361
9.15.2	Fail Over Situations	361
9.15.3	Failover Failure Situations	361
9.15.4	Specific standby situations	363
9.16	Managing Account Data for System Access	364
9.16.1	Account Types	364
9.16.2	Potential Pitfalls	365
9.17	WLAN Configuration	365
9.17.1	WLAN configuration steps (RFP 43 WLAN only)	365
9.17.2	WLAN configuration steps (RFP 48 WLAN)	366
9.17.3	Optimizing the WLAN	368
9.17.4	Securing the WLAN	370
9.18	SNMP Configuration	370
9.19	Backup SIP Proxy/Registrar	371
9.19.1	REGISTER Redirect	371

9.19.2	DNS SRV	371
9.19.3	Backup SIP Servers	373
9.19.4	Keep Alive Mechanism	375
9.19.5	Prioritized Registration	376
9.19.6	Monitoring the SIP Registration Status	376
9.19.7	Configurable User Account for Standby Check	376
9.19.8	OMM Standby Enhancement	376
9.20	Conferencing	377
9.20.1	Centralized Conferencing	378
9.20.2	Integrated Conference Server (ICS)	378
9.20.3	Configure conference rooms	381
9.20.4	Registration of conference rooms	383
9.21	Download Over Air	383
9.21.1	How “Download Over Air” Works	383
9.21.2	How to configure “Download Over Air”	384
9.22	Central DECT Phone Configuration Over Air (CoA)	386
9.22.1	Configuration files	386
9.22.2	Configuration file download to DECT phones	387
9.22.3	CoA Configuration using OMP	388
9.22.4	Configuration using usr_common.cfg/<user>/cfg Files	388
9.22.5	Variable lists	390
9.23	Call Deflection for incoming call in ringing state	394
9.24	Extended DECT Phone Interface	395
9.25	User Monitoring	396
9.25.1	Overview	396
9.25.2	Status Attributes and Validation Mechanisms	398
9.25.3	Escalation	401
9.25.4	Alarm Triggers	401
9.25.5	Licensing and System Capacities	401
9.25.6	Configuration	402
9.25.7	Start and Failover	403
9.25.8	Supported DECT phones	403
9.25.9	Restrictions	404
9.26	SRTP	405
9.27	SIP over TLS	405
9.27.2	Certificates	407
9.27.3	Private Key	408
9.27.4	TLS Transport Mode	408
9.27.5	Verification of Remote Certificates	408
9.27.6	Additional Security Considerations	409
9.28	DECT Enhanced Security	409
9.29	Migration of RFP SL35 IP from SIP-DECT Lite 3.1 to SIP-DECT 6.1	410
9.30	802.1x Certificate Based Authentication	410
9.30.1	802.1x Configuration	411
9.30.2	Prerequisites Referring to 802.1x Topology	412
9.30.3	802.1x Feature Description	412
9.31	802.1x Certificate Server Configuration	415
9.32	Initiate 802.1x by DHCP Options or OM_Configurator	416
9.32.1	DHCP Options	416
9.32.2	OM_Configurator	416
10	Maintenance.....	417
10.1	Site Survey Measurement Equipment	417
10.2	Checking the Mitel Handset Firmware Version	417
10.3	Diagnostic	417
10.3.1	Mitel DECT Phone Site Survey Mode	417
10.3.2	Mitel Handset Auto Call Test Mode	418
10.3.3	Mitel Handset Auto Answer Test Mode	418
10.3.4	Syslog	419
10.3.5	SSH user shell	420
10.3.6	Core File Capturing	425

11 Regulatory Compliance and Safety Information (4th Generation Dect Base Stations)	426
12 Safety Information (3rd Generation Dect Base Stations)	427
12.1 CE Marking	427
12.2 Communications Regulation Information	427
12.2.1 FCC Notices (U.S. Only)	427
12.3 Health and Safety	428
12.3.1 Exposure to Radio Frequency (RF) Signals:	428
12.3.2 Industry Canada (Canada only)	428
12.4 Informations réglementaires en matière de communications	428
12.4.1 Notes FCC (USA uniquement)	429
13 Appendix	430
13.1 Pre-Configuration File Rules	430
13.2 RFP Configuration File / Central (OMM Database)	431
13.2.2 RFP Configuration File / Local (OM Configurator)	434
13.3 RFP Export File Format	437
13.4 Protocols and Ports	439
13.5 Abbreviations	442
13.6 Definitions	443
13.7 References	445

1 OVERVIEW

This document describes the installation, configuration, administration, and maintenance of the SIP-DECT solution. Also, see the documents listed in the References section (section [13.9](#)) for additional details on different aspects of the SIP-DECT system.

For a list of abbreviations and definitions, see the appropriate sections in the Regulatory Compliance and Safety Information (4th Generation Dect Base Stations).

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)
- Open Mobility 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 (for example, 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 that are in a group of synchronized RFPs (called a cluster) and roaming between RFPs on remote sites.

Additional components include:

- An LDAP server to facilitate a central corporate directory
- A provisioning server to provide RFP configuration or user data files
- A data backup server to automatically backup an OMM database from the server
- SIP-DECT Event Manager or 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)

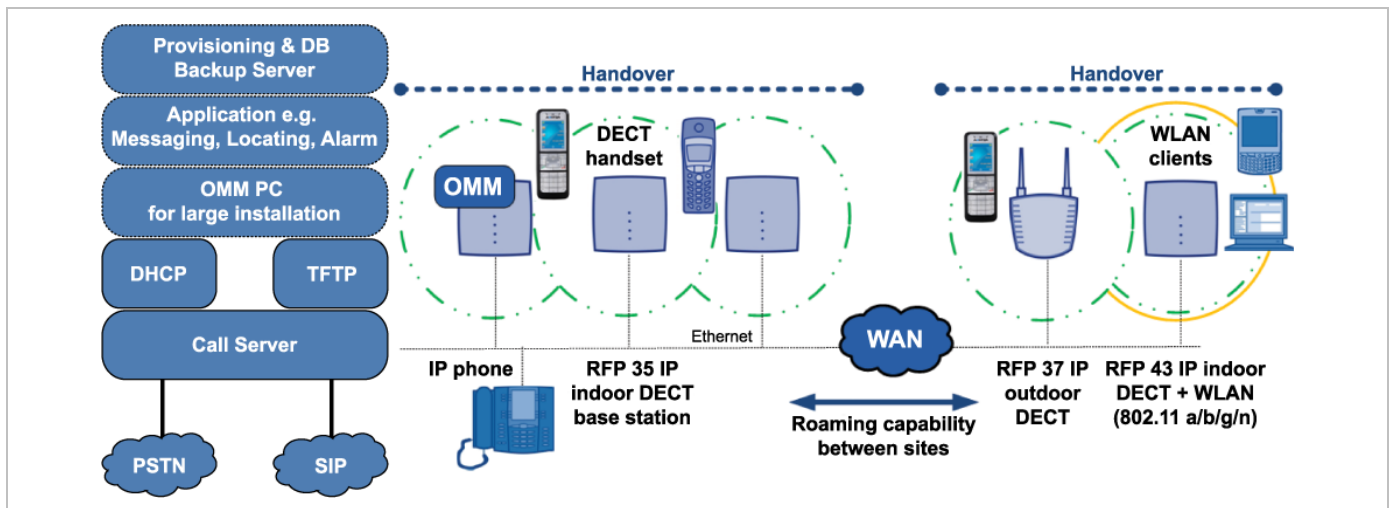


Figure 1 Architectural Overview of the SIP-DECT Infrastructure and Features

1.2 ABOUT DECT BASE STATIONS

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

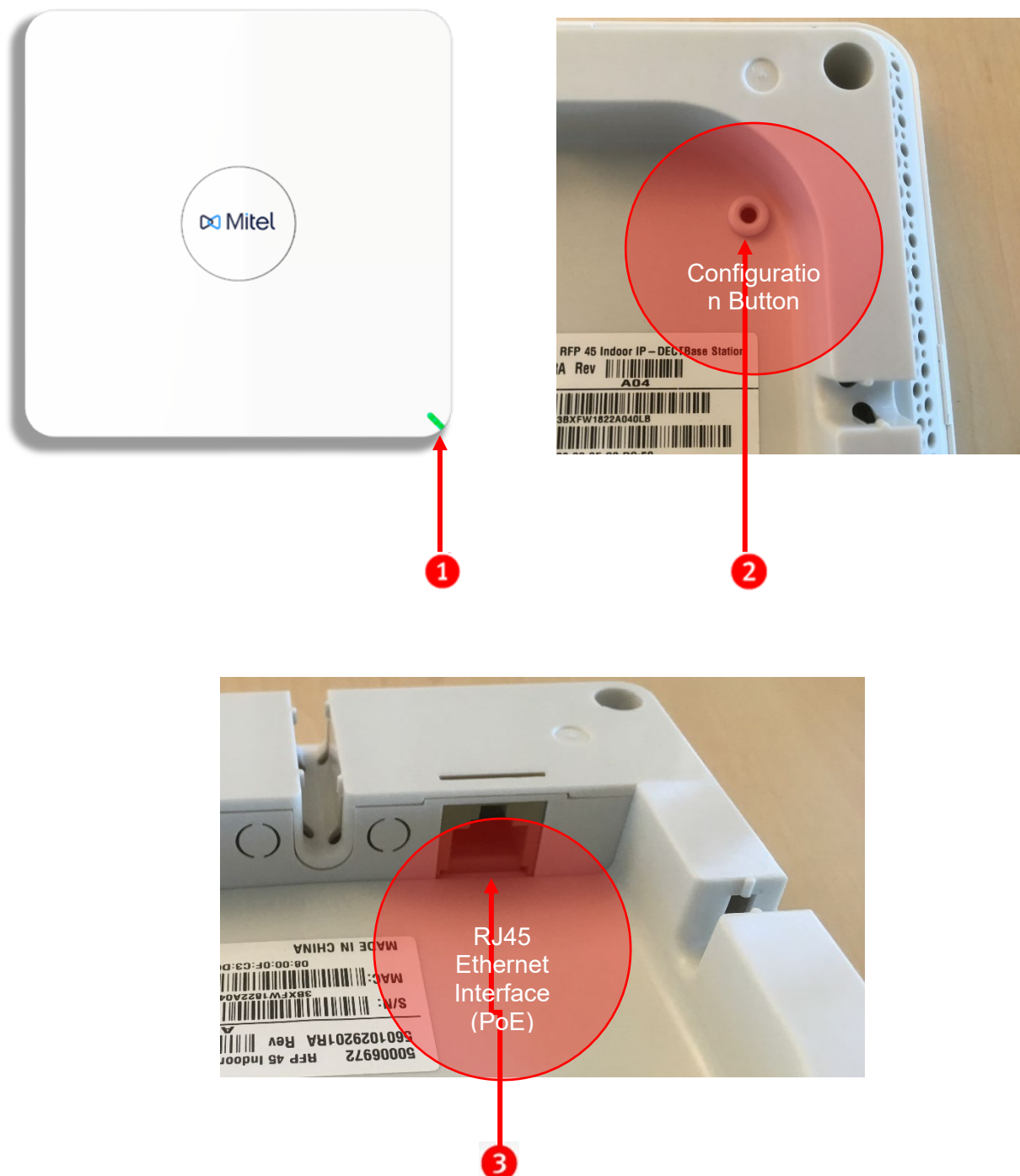
1.2.1 DECT BASE STATION FAMILIES

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.
Note: As of SIP-DECT 8.3SP5, SIP-DECT supports the RFP48 V2 WLAN. The RFP48 V2 WLAN will be the successor of the RFP48 WLAN and will provide the same functionality.

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, 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

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

The RF output of RFP 47 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 RFP 47 to the existing DECT antenna infrastructure.

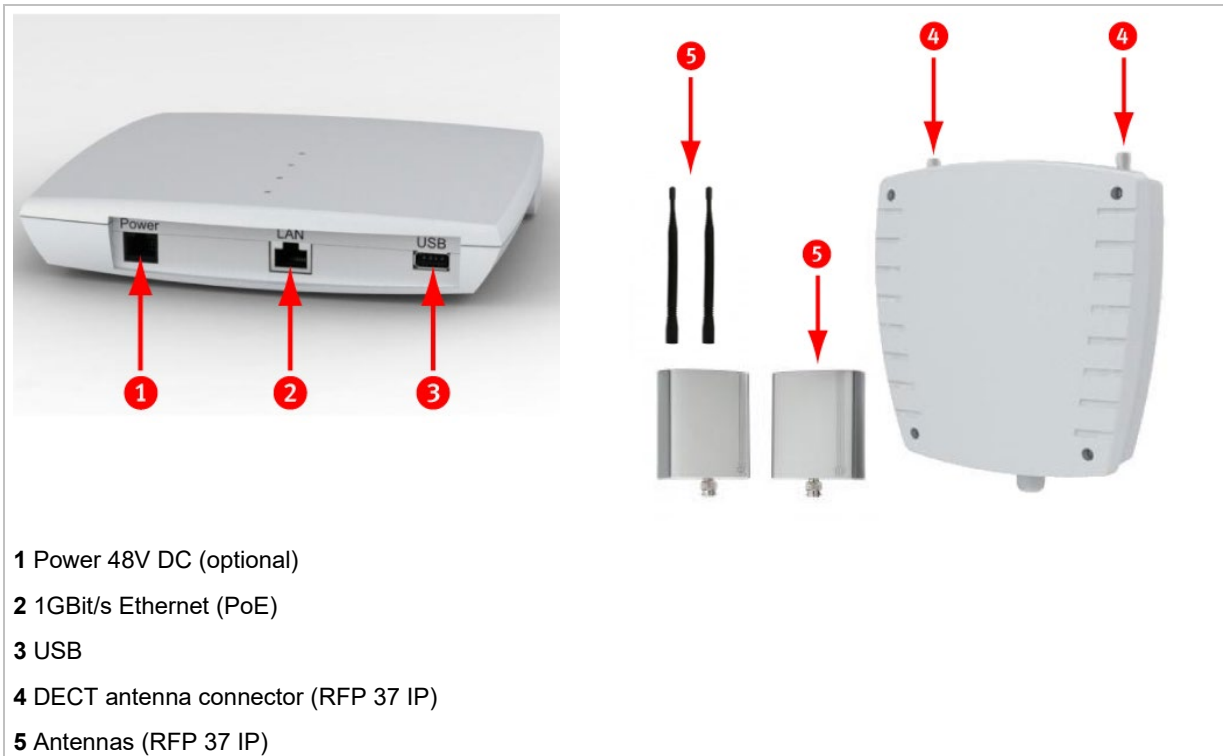
1.2.1.2 RFP 3G DECT Base Station Types

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.

The RFP3G supports the following features:

- 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
- 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

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 [9.5](#)) or by setting the data via the OM Configurator (see section [5](#)). 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.

Please 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 35/36/37/44/45/47 IP and RFP 43/48 WLAN or a dedicated Linux server.

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

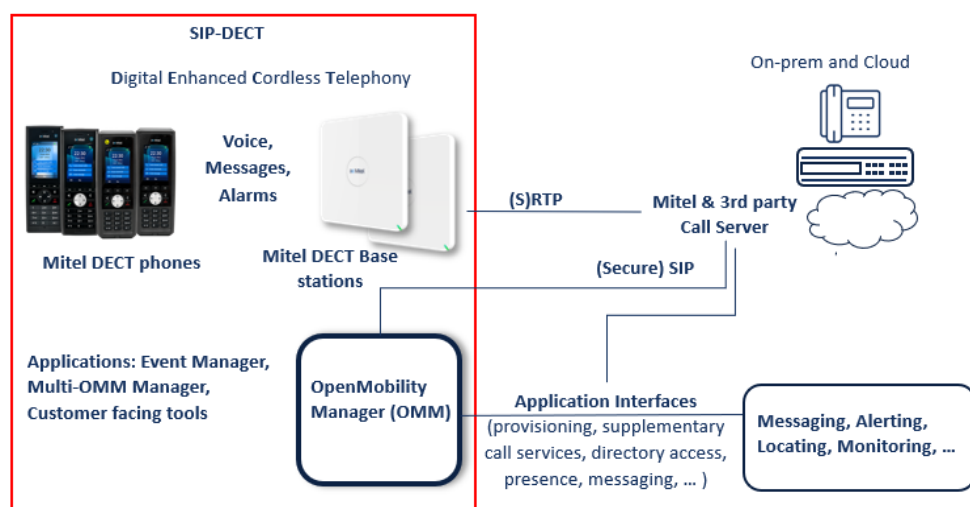
- If the OMM runs on a DECT base station, a 100 Mbit/s network link is required.
- If the OMM runs on a dedicated Linux server, a 1 GBit/s network link is required (see also section [9.13.1](#)).

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 [9.15](#).

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 Operation, Administration, Maintenance and Provisioning (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 600/700 DECT phone family is supported.



1.3.2 SIP-DECT SPECIAL FEATURES AND CAPABILITIES

Feature	GAP	142d	600	700
Large DECT Systems (XXL)	No connection handover beyond 256 RFPs	yes	yes	yes
Messaging & Alerting	no	no	yes	yes
Initiate Alarm Trigger	*, # feature access code procedure, no sensor alarm	*, # feature access code procedure, no sensor alarm	yes	yes
DECT XQ	no	no	yes	yes
UTF-8 and alphanumeric dialing support	no	no	yes	yes
SIP-DECT XML terminal API	no	no	yes	yes
Wideband Audio G.722	no	no	yes	no

1.3.3 OMM CAPACITIES AND FEATURES

The following table summarizes OMM capabilities:

Feature	Release 6.0 or later	
	RFP OMM	Linux server OMM
RFP 35/36/37/44/45/47 IP and RFP43/48 WLAN	256 ¹	4096 ¹
Handsets / users	512/1024 ³	10000
Message / Alarm receive	yes / yes ¹	yes / yes ¹
Message send	yes	yes

Feature	Release 6.0 or later	
	RFP OMM	Linux server OMM
Locating	yes ¹	yes ¹
DECT XQ	yes	yes
UTF-8 and alphanumeric dialing support	yes	yes
SIP-DECT XML terminal API	yes	yes
Wideband Audio G.722	yes ²	yes ²
8 Channel Hi-Q Audio	RFP 4G with 700d DECT phones only	

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. 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 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
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

- Mitel 700 DECT Phone series
 - Mitel 712 DECT Phone
 - Mitel 722 DECT Phone
 - Mitel 732 DECT Phone
 - Mitel 742 DECT Phone

Notes on the Mitel 600/700 DECT Phones

The Mitel 600/700 DECT phones support both the NA and EMEA regulatory requirements.

The latest Mitel 600/700 firmware release has the following characteristics:

- New user interface for example, 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 600/700 DECT phones)
- Additional subscription options
- Additional alarm melodies
- Profile indication in idle display

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

The Mitel 600/700 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 or higher	As of SIP-DECT 8.0 or higher
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	iprfp4G.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
SIP-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 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	"omm" / "omm"
Initial OMM configuration through Web or OMP standard full-access account login / password	"omm" / "omm" "omm" / "omm"	n/a
OMM access through Web or OMP (after initial OMM configuration)	Read-only or full-access accounts as configured	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
ssh (no previous connection with the OMM)	n/a	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

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 APPLICATION INITIATED SIP-DECT CONFERENCE VIA MESSAGING

Previously, local SIP DECT conferences could only be started manually through the DECT telephone user interface. Now, direct dial-in is available, enabling users to join conferences more conveniently. For example, the conference number can be sent in a text message as a callback number, allowing users to join the conference by simply pressing the green off-hook button.

If the conference room number @127.0.0.1 is used as the callback, the local conference room remains accessible even when the telephony platform does not support SIP-DECT conferencing. Additionally, internal conference calls can survive local disruptions. The system continues to support only 3-party conferences.

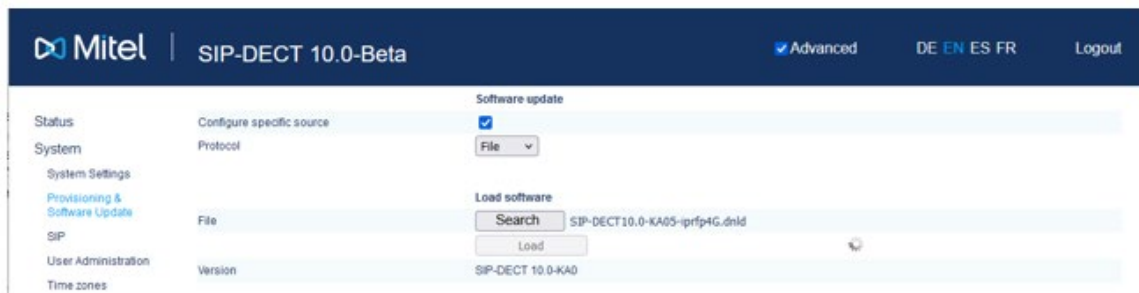
2.2 SOFTWARE UPLOAD VIA OMM WEB INTERFACE ON RFP4G

Starting with SIP-DECT 10.0, the RFP software can be loaded directly via the OMM Web service in the OMM RFP. As before, the software is automatically distributed to other RFPs during the update process, eliminating the need for a separate file server for manual updates.

However, this option is not available when the OMM is hosted on a Linux server. To enable this feature, set the software update protocol to "File" and confirm by clicking OK.

The screenshot shows the Mitel SIP-DECT 10.0 OMM Web Interface. In the top navigation bar, the 'Advanced' button is highlighted. The left sidebar shows the 'Provisioning & Software Update' menu item selected. The main content area displays the 'Software update' configuration page. A red box highlights the 'Software update' section, which includes a checked checkbox and a dropdown menu for the 'Protocol' field. The dropdown menu is open, showing options: File, FTP, TFTP, FTPS, HTTP, HTTPS, and SFTP. The 'Path' field is set to '/0/10.0-JL15'.

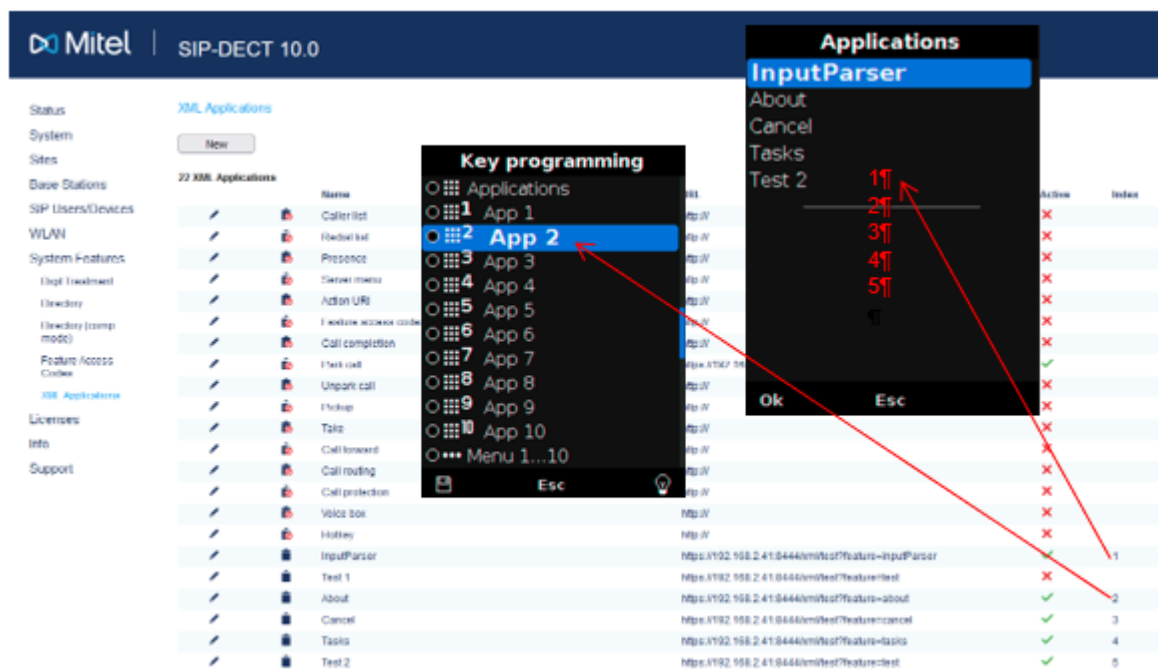
A file can then be selected from the file system and loaded into the OMM RFP via the browser. The file name is not predefined and may differ from iprfp4G.dnld.



Once the file is successfully loaded, the standard update process can be initiated, such as by clicking the update button. Additionally, other triggers, like a time-controlled update, will automatically start the update process if configured accordingly.

2.3 DYNAMIC XML APPLICATION INDEX

Starting with SIP-DECT 10.0, the "Index" column for dynamic XML applications shows the position of an entry in the application list on the DECT telephone and the corresponding reference for key programming. The index is for display purposes only and cannot be modified.



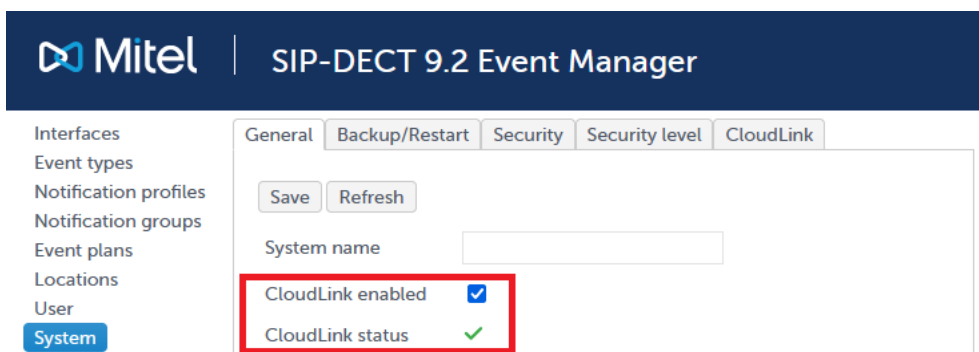
2.4 RESTRICT ACCESS ATTEMPTS TO THE SIP-DECT OMM WEB ADMINISTRATION PORTAL

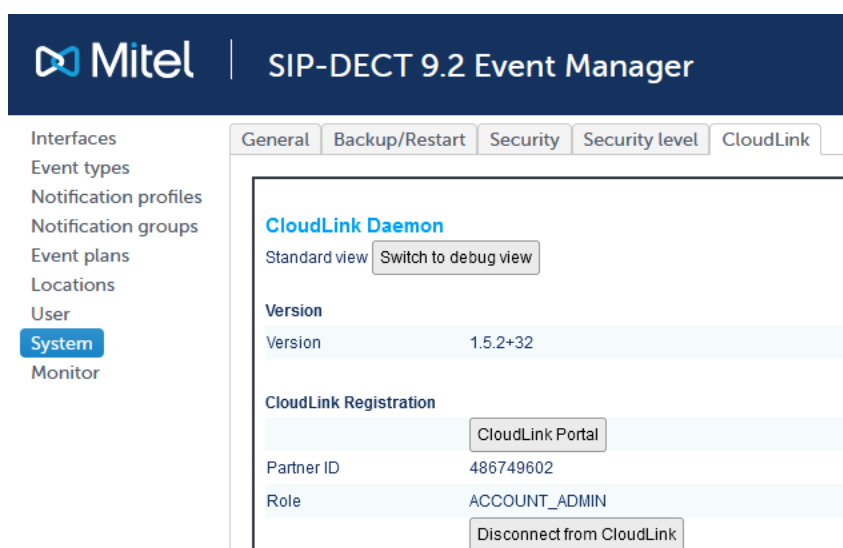
To enhance security, a new feature has been implemented for the SIP-DECT OMM web administration portal. If multiple failed login attempts occur, the OMM Web UI access page will be locked for an exponentially increasing period of time. The duration of the lockout increases with the number of failed attempts, as outlined in the table below.

No. of Failed Attempts	Lockout Time
1-5	N/A
6	1 minute
7	5 minutes
8	15 minutes
9-10	60 minutes / 1 hour
11+	12 hours

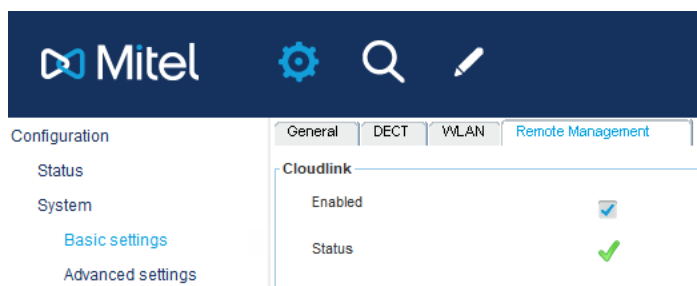
2.5 SECURE REMOTE MANAGEMENT FOR OMM AND EVENT MANAGER ON RFP4X THROUGH MITEL ADMINISTRATION PORTAL

Starting with SIP-DECT 9.2, the Mitel Administration portal is integrated into the 4th generation base stations (RFP44, RFP45, etc.). The OMM and Event Manager Web Services offer options to start the Mitel CloudLink Daemon service to access the Mitel Administration portal. This integration enables secure remote access to the OMM and Event Manager Web Services via the Mitel Administration portal.





The OMP does not integrate Mitel Administration portal but allows to enable the CloudLink Daemon service on the RFP.



Since the OMM and Event Manager, or the OMM in standby configuration, operate on different base stations, the CloudLink Daemon and the remote management service must be activated on each base station where the service is required.

To enable remote management functionality, follow these steps:

1. Set up your OMM or Event Manager as usual, ensuring you set an appropriate system name, as this will be your reference in the CloudLink portal.
2. Activate the CloudLink Daemon.
3. Connect the CloudLink Daemon to CloudLink.
4. Start the required tunnels.

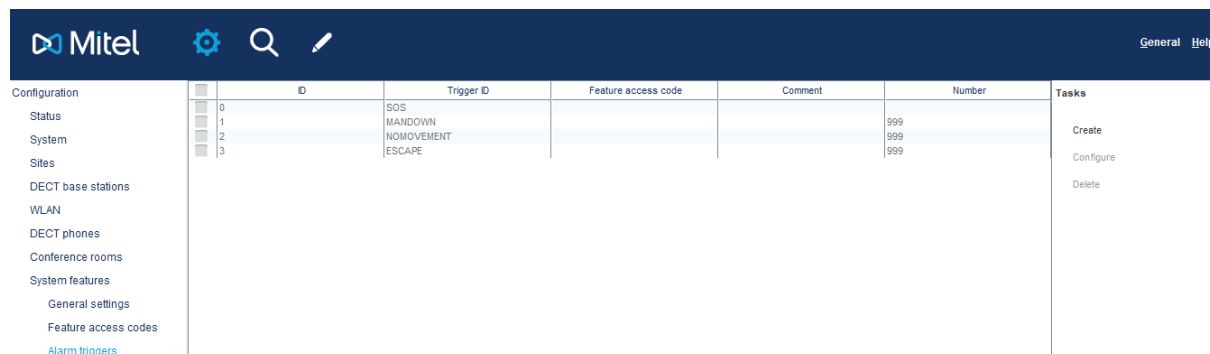
Before removing the OMM or Event Manager from an RFP, stop the tunnels and unlink the CloudLink Daemon from the Mitel Administration portal.

The CloudLink Daemon connects to *.mitel.io services via https (port 443).

2.6 732D AND 742D GENERATE DISTINCT SENSOR ALARM TYPES FOR MAN DOWN, NO MOVEMENT, AND ESCAPE

In earlier SIP-DECT versions, all sensor alarms were mapped to the MANDOWN alarm trigger. However, starting with SIP-DECT 9.2 and 700d SW 9.1.7.50, different alarm triggers are now generated for each type of sensor alarm. The new alarm

triggers "NOMOVEMENT" and "ESCAPE" are predefined, similar to the existing "SOS" and "MANDOWN" triggers and cannot be deleted. Apart from the comment field, no configurations can be made for these new alarm triggers. The telephone number to be called automatically is derived from the "MANDOWN" configuration. There are no changes for the Mitel DECT phone 632d models or for the 732d and 742d models with older software versions.



The screenshot shows the Mitel configuration interface. On the left is a navigation menu with options like Configuration, Status, System, Sites, DECT base stations, WLAN, DECT phones, Conference rooms, System features, General settings, Feature access codes, and Alarm triggers (highlighted). The main area displays a table of alarm triggers.

ID	Trigger ID	Feature access code	Comment	Number	Tasks
0	SOS				
1	MANDOWN			999	Create
2	NOMOVEMENT			999	Configure
3	ESCAPE			999	Delete

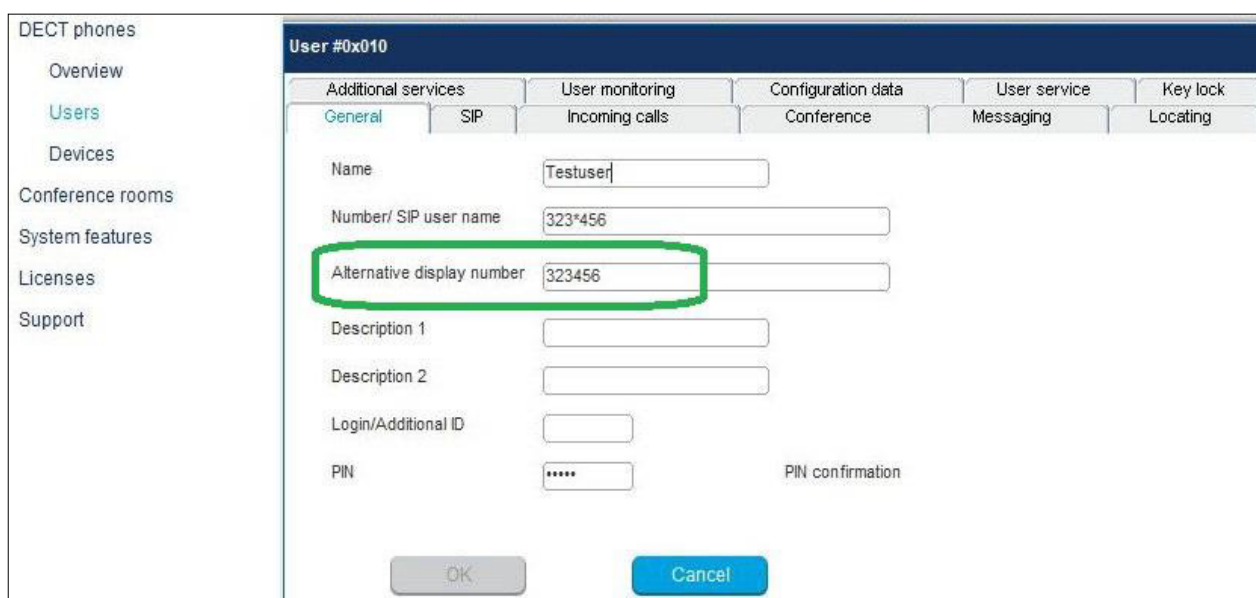
The additional alarm triggers are supported by the Event Manager as "Escape" and "No Movement" in the same way as "Man Down".

Note: This change affects all applications using the SIP-DECT AXI interface and supporting alarm triggers.

2.7 MDUG PRIME DN ON SIP DECT IDLE DISPLAY

Some call server assign a number to a user but define different individual numbers to the user's devices. To display the original user number at the device instead of the individual device number, set an alternative display number for the user.

Configuration in OMP



The screenshot shows the OMP configuration interface for User #0x010. The left sidebar lists various configuration categories, with 'Users' highlighted. The main panel shows the 'General' tab for the user. The 'Alternative display number' field is highlighted with a green box.

User #0x010					
Additional services	User monitoring	Configuration data	User service	Key lock	
General	SIP	Incoming calls	Conference	Messaging	Locating
Name	Testuser				
Number/ SIP user name	323*456				
Alternative display number	323456				
Description 1					
Description 2					
Login/Additional ID					
PIN	*****		PIN confirmation		
OK Cancel					

Configuration in OMM web service

Configure SIP User/Device

General settings

Display name	Testuser
Number/SIP user name	323*456
Alternative display number	323456
PIN	
User/Device relation	Unbound
IPEI	
DECT authentication code	

Configuration in MOM web service

Users / DECT phones						
+ Add new record Multi-Edit Multi-Delete More				Change view: Users		
User	SIP	Additional services	Incoming calls	Conference	Messaging	Locating
Number/SIP u...	User ID	Rel. device ID	Rel. type	Name	altern. Disp. Number	
☐ 27002	0x0036	0x0000	Unbound	nonPermUnbound		
☐ 323*456	0x003B	0x0000	Unbound	Testuser	323456	
☐ 4771	0x0001	0x0001	Fixed	4771		

Parameter / Parameter group	Alternative display number
Description	To display another user number than the regular number/SIP user name on the DECT device.
Format	String
Range	32 characters
Default value	Empty
Web	Configure SIP User/Device
OMP	DECT phones > Users > General
OMM configuration files	n.a.
DECT Phone	n.a.
User configuration files	n.a.
AXI command	<pre><SetPPUser seq="..."><user uid="..." altDisplayNum="1000" /></SetPPUser></pre> to set the number to be displayed to 1000.

Note: A display setting via XML notify has higher priority over an alternative display number configured via OMP or web service. An XML display notification once sets the user number, it can be configured via

OMP or web service, but the PP always shows the setting from the XML notification. The alternative display is only stored in config data.

2.8 SUPPORT FOR ENABLE/DISABLE 100REL TAG IN THE SIP SUPPORTED HEADER VIA CONFIG PARAMETER

Some PBX platforms or provider infrastructures don't support the SIP signaling feature "RFC3262: Reliability of Provisional Response in the Session Initiation Protocol (PRACK)". As of SIP-DECT 9.2, it is possible to suppress the signaling of support for this PRACK feature for outgoing calls.

Configuration in OMP

The screenshot shows the 'SIP' configuration page in the 'Advanced settings' tab. The 'General' section contains various SIP parameters. The 'Provisional response acknowledge' checkbox is checked and highlighted with a green box. Other visible settings include 'Remove route header', 'X-Aastra-Id info', 'DNS SRV failover following registration', 'Registration failed retry timer' (120 sec), 'Registration timeout retry timer' (180 sec), 'Determine remote party by' (P-Asserted-Identity), 'Call reject state code (user reject)' (486), 'Session timer' (240 sec), 'SIP contact matching' (URL), 'Explicit MWI subscription', 'Hold with SDP inactive', 'User agent info' (checked), 'User agent info - compatibility mode', 'Multiple 180 Ringing' (checked), 'Transaction timer' (4000 msec), 'Blacklist time out' (5 min), 'Dial terminator' (#), 'Call reject state code (device unreachable)' (486), 'Incoming call timeout' (240 sec), 'Explicit MWI subscription period' (600 sec), 'Semi-attended transfer' (Blind), and 'Refer-to with replaces'.

Parameter / Parameter group	Provisional response acknowledge
Description	To enable/disable the signaling (100rel in SIP supported header) of PRACK support for outgoing calls.
Format	Boolean
Range	1 or true: <i>PRACK support is signalled</i> 0 or false: <i>PRACK support is not signalled</i>
Default value	1 or true
Web	n.a.
OMP	System > SIP > Advanced settings
OMM configuration files	<SetAdvancedSIP prack="1" /> to enable PRACK support signalling.
DECT Phone	n.a.
User configuration files	n.a.

2.9 CALLS TO/FROM SIP-DECT NOT POSSIBLE OR UNENCRYPTED

The Mitel OpenScope platforms use a so called 2-m-line approach to signal the support of RTP and SRTP during a SIP call setup in the SDP negotiation.

As of SIP-DECT 9.2, SIP-DECT introduces the new SRTP mode “SRTP+RTP” which follows the 2-m-line approach and ensures compatibility with the OpenScope platforms.

Configuration in OMP

ID	Name	ELIN number	Wideband audio G.722	Enh. DECT security
1	default		✗	✓

Site #1

General

Name: default

Emergency location identification number:

Wideband audio G.722: ☐

Enhanced DECT security: ☒

SRTP: SRTP+RTP

Changing site parameters, may restart radio fixed parts in this site.

OK Cancel

Parameter / Parameter group	SRTP
Description	To configure the SRTP mode of a Site.
Format	Enumeration
Range	Only: Only SRTP calls will be accepted, all other will be rejected (the audiopart of the SDP contains RTP/SAVP). Preferred: All calls will be initiated as secured, but accepted if they are not secured (the audio part of the SDP contain RTP/AVP). Disabled: Only RTP calls will be initiated as not ciphered and incoming ciphering algorithm will be not accepted. All communications are established unencrypted. SrtpPlusRtp: All calls will be initiated as secured, but accepted if they are not secured (the audio part of the SDP contains 2 m-lines RTP/SAVP and RTP/AVP).
Default value	Disabled
Web	Avanced: Sites
OMP	Sites

OMM configuration files	<SetSite><site id="..." srtp="SrtpPlusRtp" /></SetSite>
DECT Phone	n.a
User configuration files	n.a.

2.10 SIGNALLING OPTIONS FOR 'HOLD' IN SESSION DESCRIPTION PROTOCOL (SDP) INACTIVE / SENDONLY

Classically, in SIP signaling, the hold of another subscriber is signaled by the SDP media attribute "sendonly" to put the remote subscriber into a state where he only receives audio. This leads to problems with some Mitel OpenScape platforms as they then expect the holding party to send audio and "music on hold" feature becomes not active.

As of SIP-DECT 9.2, the new configuration parameter "Hold with SDP inactive" allows to configure desired hold behavior.

Configuration in OMP

Parameter / Parameter group	Hold with SDP inactive
Description	To enable/disable hold with SDP inactive
Format	Boolean
Range	1 or true: <i>hold will be signalled with SDP inactive</i> 0 or false: <i>hold will be signalled with SDP sendonly</i>
Default value	0 or false
Web	n.a.

OMP	System > SIP > Advanced settings
OMM configuration files	<SetAdvancedSIP holdWithSdpInactive="1" /> to enable Hold with SDP inactive
DECT Phone	n.a
User configuration files	n.a.

2.11 SINGULAR VOIP PROFILE FOR EACH OS4K GATEWAY

The architecture of the Mitel OpenScape 4000 PBX platform (OS4K) provides up to 20 gateways via which the users are distributed. As of release 9.2, SIP-DECT supports this specific OS4K architecture by supporting up to 20 so-called "SIP profiles". The following data can be configured for each "SIP profile":

- Primary Proxy server
- Primary Registrar server
- Primary Outbound Proxy server
- Secondary Proxy server
- Secondary Registrar server
- Secondary Outbound Proxy server
- Tertiary Proxy server
- Tertiary Registrar server
- Tertiary Outbound Proxy server

Configuration in OMP (SIP profiles)

Configuration	ID	Pri proxy srv	Pri proxy port	Pri reg srv	Pri reg port	Pri outb proxy srv	Pri outb proxy port
Status	0	10.103.31.152	5060	10.103.31.152	5060		5060
	1	10.103.31.153	5060	10.103.31.153	5060		5060
System	2	127.0.0.1	5060	127.0.0.1	5060		5060
	3	127.0.0.1	5060	127.0.0.1	5060		5060
Basic settings	4	127.0.0.1	5060	127.0.0.1	5060		5060
Advanced settings	5	127.0.0.1	5060	127.0.0.1	5060		5060
SIP	6	127.0.0.1	5060	127.0.0.1	5060		5060
	7	127.0.0.1	5060	127.0.0.1	5060		5060
SIP profiles	8	127.0.0.1	5060	127.0.0.1	5060		5060
Provisioning	9	127.0.0.1	5060	127.0.0.1	5060		5060
	10	127.0.0.1	5060	127.0.0.1	5060		5060
User administration	11	127.0.0.1	5060	127.0.0.1	5060		5060
Data management	12	127.0.0.1	5060	127.0.0.1	5060		5060

SIP profile #0

General

	Primary	Secondary	Tertiary
Proxy server	10.103.31.152		
Proxy port	5060	5060	5060
Registrar server	10.103.31.152		
Registrar port	5060	5060	5060
Outbound proxy server			
Outbound proxy port	5060	5060	5060

OK

Cancel

By assigning a SIP-DECT user to such a "SIP profile", the users of a SIP-DECT system can be distributed to the different gateways of the OS4K. For this purpose, each "SIP profile" is assigned a

unique identifier (ID) from 0 to 19. In the respective user data record, the following can then be used for the profile assignment.

The profile with the ID 0 corresponds to the well-known general SIP proxy/registrar settings:

- OMP->System->SIP->Basic settings
- OMP->System->SIP->Backup settings

Configuration in OMP (user's profile assignment)

The screenshot shows the OMP configuration interface. On the left is a sidebar with a tree view containing: Configuration, Status, System, Sites, DECT base stations, WLAN, DECT phones, Overview, Users (highlighted), Devices, Conference rooms, System features, Licenses, and Support. The main area displays a table of users with columns: User ID, Name, Number/SIP user name, Description 2, SIP auth. user name, User rel. type, SIP profile ID, and Fixed SIP port. User #0x003 is selected. Below the table, the 'User #0x003' configuration page is shown with tabs for General, SIP, Incoming calls, Conference, Messaging, and Locating. The 'SIP' tab is active, showing fields for Authentication user name, Password, Password confirmation, VIP (checkbox), Used for visibility checks (checkbox), SIP profile ID (set to 1 and highlighted with a green box), Fixed port (0), and Calculated port (5060). At the bottom are OK and Cancel buttons.

User ID	Name	Number/SIP user name	Description 2	SIP auth. user name	User rel. type	SIP profile ID	Fixed SIP port
0x001	pp20001	20001			Dynamic	0	0
0x002	pp20002	20002			Dynamic	0	0
0x003	pp20021	20021			Dynamic	1	0
0x004	pp20022	20022			Unbound	1	0
0x005	pp20003	20003			Unbound	0	0
0x006	pp20020	20020			Dynamic	1	0

Parameter / Parameter group	PPUser – Profile ID
Description	To assign a user to SIP Profile
Format	Integer
Range	0..19
Default value	0
Web	n.a.
OMP	DECT phones -> Users
OMM configuration files	<SetPPUser> <user uid="..." sipProfileId="1" /> </SetPPUser>
DECT Phone	n.a
User configuration files	n.a.

Parameter / Parameter group	SIP Profile
Description	The proxy/registrar settings of a SIP profile.

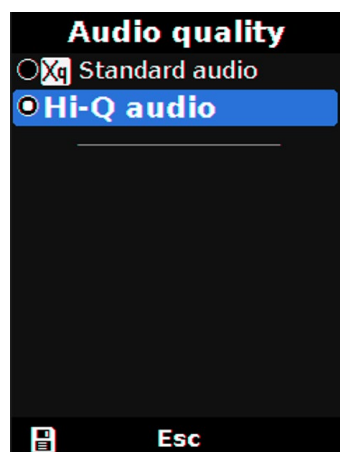
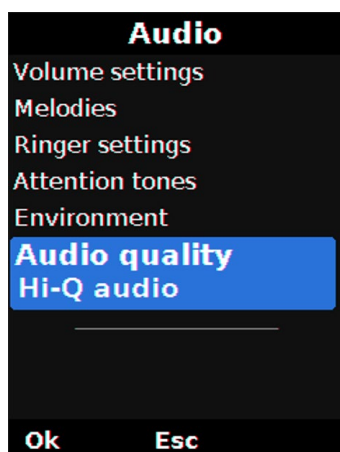
Format	Primary/Secondary/Tertiary: proxyServer: string proxyPort: integer regServer: string regPort: integer outboundProxyServer: string outboundProxyPort: integer
Range	n.a.
Default value	Primary: proxyServer: 127.0.0.1 proxyPort: 5060 or 5061 regServer: 127.0.0.1 regPort: 5060 or 5061
Web	n.a.
OMP	System -> SIP Profiles
OMM configuration files	<SetSIPProfile> <sipProfile id="..."> <Primary proxyServer="10.103.31.152" proxyPort="5060" regServer="10.103.31.152" regPort="5060" /> </sipProfile> </SetSIPProfile>
DECT Phone	n.a.
User configuration files	n.a.

Note: To make it easier to switch the "SIP Transport Protocol", all proxy/registrar port settings with a "5060" value are automatically changed to "5061" when switching from "unsecure" (UDP/TCP) to TLS. When switching from TLS to an unsecure (UDP/TCP) SIP transport, all proxy/registrar port settings with a "5061" value are automatically changed to "5060".

2.12 8 CHANNEL HI-Q AUDIO WITH MITEL 700D DECT PHONES AND 4TH GENERATION RFPs

As of SIP-DECT 9.1 the 700d DECT phone family together with the 4th generation RFPs support Hi-Q Audio to the maximum audio channel capacity of the RFPs i.e. 8 audio channels for all 4th generation RFPs except RFP44 which is in general limited to 4 voice channels. In previous versions, the number of voice connections was reduced to half when using Hi-Q Audio.

With the update to 9.1, Hi-Q audio is automatically activated (in the 700d DECT phone after update to the SW version provided with this SIP-DECT 9.1 SW package and in the system). The 700d audio quality menu allows to switch the audio modes.



However, the prerequisite is the exclusive use of 4th generation RFPs. In a mixed operation of 3rd and 4th generation RFPs, standard audio is used.

If an 3rd generation RFP (RFP35 etc.) is added to a site which operates in the Hi-Q audio mode for 700d DECT phones then the RFP does not become operational until a restart of the system. During restart the system then turns off the Hi-Q audio mode and the 3rd generation RFP is put into operation. In the opposite direction the system turns on the Hi-Q audio mode during restart after the 3rd generation has been removed from a site.

The Hi-Q audio does not support the special audio processing for reflective environments (Xq). If the Xq mode it is required to switch to the standard audio mode in the DECT phone settings.

Note: There is currently a restriction that disrupted voice connections occur when using Reflective environment in the RFP settings and Hi-Q Audio at the same time. Please deactivate the reflective environment setting or switch to standard voice in the DECT phone configuration.

[Configure base station](#)

[Re-enrolment](#)

ⓘ Please configure the WLAN regulatory domain on the system settings page.

ⓘ Please configure a WLAN profile of proper type.

General settings	
MAC address	08:00:0F:C3:DC:E5
Name	RFP
Site	1
Emergency Location Identification Number (ELIN)	

DECT settings	
☒ DECT Cluster	1
Preferred synchronization source	☐
Reflective environment	☒

WLAN settings	
☐ WLAN profile	0
802.11 channel	
Output power level	Full

OK
Cancel

2.13 ENABLE/DISABLE ADMIN INTERFACES

As of SIP-DECT 8.3SP3, it is possible to disable the admin interfaces OMM Web service and AXI (OMP) to increase security if they are not needed. This is available for SIP-DECT standard mode and for the SIP-DECT with CloudID mode.

Please be aware that AXI is used for various services not only with OMP.

Note: If the admin interfaces are disabled and OMM provisioning is not used or misconfigured, access to the OMM is completely blocked. In this state, the system is completely locked. Only for an OMM on a 4th generation RFP, the RFP configuration button can be used to re-enable the admin interfaces. Any other configuration will need to be set up from scratch.

The configuration is possible via OMP, OMM Web service and OMM configuration files.

The screenshot shows the Mitel OMM Web configuration interface. The top navigation bar includes the Mitel logo, a search icon, and a pencil icon. The 'General' tab is selected. The 'DECT' sub-tab is active. The 'System name' is set to '8.3SP3 TEF'. The 'Remote access' checkbox is checked. The 'AXI server access' and 'Web server access' checkboxes are highlighted with a red box. The 'Tone scheme' is set to 'DE' and the 'Time zone' is set to 'Central European (CET UTC+1 DST)'. The 'OK', 'Cancel', and 'Restart' buttons are visible at the bottom.

The interfaces configuration options are available in the OMM Web system settings section when the advanced view is active. In order to be able to access the individual settings, the interface area must first be expanded.

The screenshot shows the Mitel OMM Web configuration interface. The top navigation bar includes the Mitel logo, the text 'SIP-DECT 8.3', and the 'Advanced' checkbox, which is highlighted with a red box. The 'DE' language is selected. The 'System Settings' section is active. The 'System name' is set to '8.3SP3'. The 'Interfaces' section is expanded, showing 'Remote access', 'AXI server access', and 'Web server access' checkboxes, which are highlighted with a red box. The 'Tone scheme' is set to 'DE'. The 'OK', 'Cancel', and 'Restart' buttons are visible at the bottom.

Parameter / Group	OMM Web server access
Description	This parameter determines if the OMM Web access is accessible.
Format	Boolean
Range	1 or true – “ Access enabled ” 0 or false – “Access disabled”
Default value	1 or true
Web	Advanced: System/System Settings/Web server access
OMP/AXI	System/Basic settings/General/ Web server access
OMM configuration files	<SetWebServerAccess enable="1" />
User data import	n.a.
DECT Phone	n.a.

Parameter / Group	AXI server access
Description	This parameter determines if the AXI access is accessible (OMP, etc.)..
Format	Boolean
Range	1 or true – “ Access enabled ” 0 or false – “Access disabled”
Default value	1 or true
Web	Advanced: System/System Settings/Web server access
OMP/AXI	System/Basic settings/General/ Web server access
OMM configuration files	<SetAXIServerAccess enable="1" />
User data import	n.a.
DECT Phone	n.a.

When the OMM web service is disabled, it is immediately inaccessible.

When the AXI access is disabled via OMP, the current session is maintained until closed. Only new connections are no longer possible.



If the OMM is hosted on a 4th generation RFP e.g. RFP45 then the RFP configuration button can be used to re-enable the admin interfaces. To do so, press the RFP configuration button until the LED flashed Magenta (LED indication when pressing the RFP configuration button: flashing green -> flashing blue (1. Switch to SDC mode) -> flashing green -> flashing yellow (2. Make RFP a OMM RFP) -> flashing green -> **flashing magenta (3. Re-enable OMM Web service and AXI service (OMP))** -> flashing green -> flashing red (4. Reset to factory defaults)).

2.14 BV32 CODEC SUPPORT ON MITEL 700D HANDSETS

The Mitel 700d handsets are equipped with support for the BV32 codec, which provides efficient voice compression at a bitrate of 32 kbps, ensuring optimal performance in narrowband voice applications while maintaining excellent audio quality.

2.15 SETTING SECURITY LEVEL VIA OMM WEB SERVICE

As of SIP-DECT 8.3SP3, it is possible to set the security level via the OMM web service. In earlier 8.3 software versions this was only possible via OMP or OMM configuration files. This is available for SIP-DECT standard mode and for SIP-DECT with CloudID mode. The option is available in the system settings section when the advanced view is active.

2.16 IMPROVEMENTS OF THE TIME ZONE SETTINGS FOR SIP-DECT OVA DEPLOYMENTS

As of SIP-DECT 8.3SP2, the “message of the day” (MOD) and the OVA description includes hints how to configure the time zone of the virtual machine.

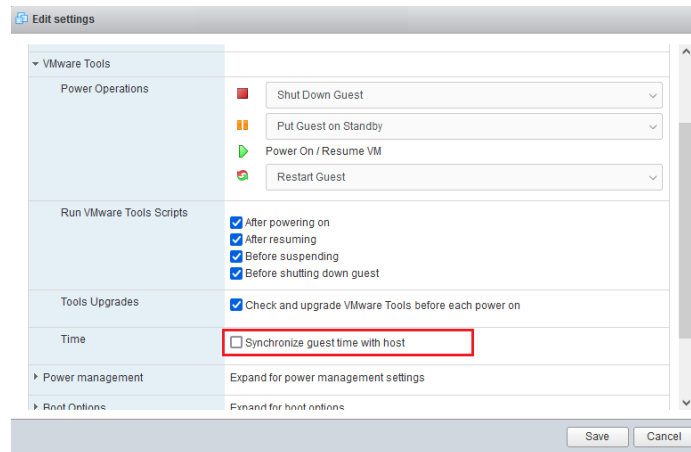
```
#####
Welcome to the SIP-DECT VM

usage:
- change keyboard: system-config-keyboard
- change password: passwd root
- configure network: nmtui
- to restart NIC: systemctl restart network
- not necessary when taking over a running
  SIP-DECT installation - but note the IP
  address of the interface to be used for
  SIP-DECT which is an optional user input
  for the ./setup skript.
- if OVA used outside of CET timezone
- check timezone: timedatectl
- find timezone: timedatectl list-timezones
- set timezone: timedatectl set-timezone "timezone"
- ./setup
  to install Mitel SIP-DECT OMM or MOM.
#####
[root@sip-dect ~]# _
```

In addition, the configured time zone of the source system is also taken over when a system is updated with via a new OVA deployment with a data takeover.

2.17 ESXI TIME SYNCHRONIZATION DISABLED FOR SIP-DECT OVA DEPLOYMENTS

As of SIP-DECT 8.3SP2, the VMware® ESXI host time synchronization of SIP-DECT OVA deployments is disabled to prevent conflicts with the running NTP client in the virtual machine.



2.18 MIGRATION FROM EARLIER RELEASES

2.18.1 CONVERSION OF PROVISIONING RELATED DATA

The provisioning URL and existing provisioning settings that have been set in earlier releases will continue to be used. New provisioning parameters are set to default values. Some existing data are automatically converted during the upgrade process.

The following table provides an overview of converted data.

#	Release 8.1 or earlier		Release 8.3 or later	
	Category	Parameter	Category	Parameter
1	Provisioning/Daily automatic reload of configuration and resource files	Active	Provisioning & Software Update/System update	Time-controlled
2		Autonomous SW update check by OMM	not applicable	
3		Time of day	Provisioning & Software Update/System update	Time of day
4		Maximum delay		Maximum delay (minutes)
5	System Settings/DECT base stations update	Mode		Mode
6		Trigger*		Time-controlled
7		Time*		Time of day
8		Maximum delay*		Maximum delay (minutes)

* DECT base stations update timer settings are converted only if there is no active Daily automatic reload of configuration and resource files.

Table: Data converted during upgrade to 8.3 or later

The DECT base station update configuration that was in the system settings section is no longer available. It is integrated into the provisioning settings. Only the time-controlled provisioning trigger remains.

2.18.2 SW UPDATE

The concepts for provisioning must be considered in all migration scenarios for SW updates. This includes for example: supported provisioning triggers, their configurations, SW download, and distribution, and activation. These are described in the preceding sections.

The following sections describe how to migrate the SW update from earlier releases to SIP-DECT Release 8.3 depending on the used configuration method.

2.18.2.1 DHCP next server & boot file name

8.1 or earlier base station configuration:	DHCP
SW update configuration:	next server & boot file name
Migration to:	Provisioning URL
Required action:	1. Set the provisioning URL 2. Copy iprpf3G.dnld/iprpf4G.dnld files to the location that the provisioning URL points to 3. Review and adjust provisioning trigger configuration
Comment:	If no provisioning URL is specified otherwise, then the DHCP next server and boot file name are used to create a provision URL. There is no action required if the default file names iprpf3G.dnld and iprpf4G.dnld are used and the default provisioning settings need not be changed.
Alternative:	SW update URL
Required action:	1. Set the SW update URL. 2. Copy iprpf3G.dnld/iprpf4G.dnld files to the location that the SW update URL points to. 3. Review and modify the provisioning trigger configuration.

2.18.2.2 OM Configurator TFTP server & file name

8.1 or earlier base station configuration:	OMM Configurator
SW update configuration:	TFTP server address & TFTP file name
Migration to:	Provisioning URL
Required action:	1. Set the provisioning URL. 2. Copy iprpf3G.dnld/iprpf4G.dnld files to the location that the provisioning URL points to. 3. Review and modify the provisioning trigger configuration.
Comment:	If no provisioning URL is specified otherwise, then the TFTP server address & TFTP file name are used to create a provision URL. Then there is no action required if the default file names iprpf3G.dnld and iprpf4G.dnld are used and the default provisioning settings need not be changed.
Alternative:	SW update URL

Required action:	1. Set the SW update URL. 2. Copy iprpf3G.dnld/iprpf4G.dnld files to the location that the SW update URL points to. 3. Review and modify the provisioning trigger configuration.

2.18.2.3 RFP configuration file SW update URL

8.1 or earlier base station configuration:	RFP configuration files
SW update configuration:	OM_SwImageUrl, OM_SwImageUrl3G, OM_SwImageUrl4G
Migration to:	Provisioning URL
Required action:	1. Set the provisioning URL. 2. Copy iprpf3G.dnld/iprpf4G.dnld files to the location that the provisioning URL points to. 3. Review and modify the provisioning trigger configuration.
Comment:	If no provisioning URL is specified otherwise, then the OM_SwImageUrl(3G,4G) are used to create a provision URL. Then there is no action required if the default file names iprpf3G.dnld and iprpf4G.dnld are used and the default provisioning settings need not be changed.
Alternative:	SW update URL
Required action:	1. Set the SW update URL. 2. Copy iprpf3G.dnld/iprpf4G.dnld files to the location that the SW update URL points to. 3. Review and modify the provisioning trigger configuration

2.18.2.4 DHCP or other basic configuration & OMM provisioning

8.1 or earlier base station configuration:	DHCP or OMC with or without RFP configuration files & OMM provisioning
SW update configuration:	DHCP or OMC with or without RFP configuration files
Migration to:	Provisioning URL
Required action:	1. Copy iprpf3G.dnld/iprpf4G.dnld files to the location that the provisioning URL points to. 2. Review and modify the provisioning trigger configuration.
Comment:	The provisioning URL and existing provisioning settings been set in previous release will continue to be used. New provisioning parameter are set to default.
Alternative:	SW update URL
Required action:	1. Set the SW update URL. 2. Copy iprpf3G.dnld/iprpf4G.dnld files to the location that the SW update URL points to.

	3. Review and modify the provisioning trigger configuration.

2.18.2.5 OMM provisioning

8.1 or earlier base station configuration:	OMM provisioning
SW update configuration:	Provisioning URL & additional provisioning settings
Migration to:	No change
Required action:	Review and modify the provisioning trigger configuration.
Comment:	The provisioning URL and existing provisioning settings been set in previous release will continue to be used. New provisioning parameter are set to default.
Alternative:	SW update URL
Required action:	1. Set the SW update URL. 2. Copy iprfp3G.dnld/iprfp4G.dnld files to the location that the SW update URL points to. 3. Review and modify the provisioning trigger configuration.

2.18.2.6 SW update URL

8.1 or earlier base station configuration:	SW update URL
SW update configuration:	SW update URL & additional provisioning settings
Migration to:	No change
Required action:	Review and modify the provisioning trigger configuration.
Comment:	The SW update URL and the provisioning settings set in the previous release will continue to be used. New provisioning parameter are set to default.
Alternative:	none
Required action:	n.a.

2.18.2.7 Multiple TFTP server

8.1 or earlier base station configuration:	DHCP or OMC with or without RFP configuration files
SW update configuration:	DHCP or OMC with or without RFP configuration files <u>with different server settings for various base stations to spread load</u>
Migration to:	Provisioning URL
Required action:	1. Copy iprfp3G.dnld/iprfp4G.dnld files to the location that the provisioning URL points to.

	2. Review and modify the provisioning trigger configuration.
Comment:	There is no need to maintain multiple servers to spread load because only the OMM base station downloads the SW, and only once. Other base stations do not reach out to file servers.
Alternative:	SW update URL
Required action:	1. Set the SW update URL. 2. Copy iprpf3G.dnld/iprpf4G.dnld files to the location that the SW update URL points to 3. Review and modify the provisioning trigger configuration

2.18.2.8 OMM configuration files and other configuration and resource files

In general, there are no changes from earlier releases with regard to the content and supported features. However, there are changes to AXI commands as described in the preceding section of the document; especially in the section "Conversion of provisioning related data"

The following table describes the replacements for commands supported in the earlier releases.

Previous AXI command	Example	Replaced by	Example
SetSystemProvUpdTrig	<pre><SetSystemProvUpdTrig enable="1" hour="2" minute="0" maxDelay="1439" autoSoftwareCheck="1" /></pre>	SetSystemUpdate	<pre><SetSystemUpdate timedUpdate="true" hour="2" minute="0" maxDelay="1439" swActTrigger="Automatic" swActAllAtOnce="true" /></pre>
SoftwareUpdate	<pre>< timedUpdate="true" allAtOnce="true" maxDelay="30" hour="1" minute="30" /></pre>		

2.18.2.9 RFP configuration files containing OMM configuration command

RFP configuration files are supported in Release 8.3 as with earlier releases.

2.19 OMM WEB SERVICE

To support SIP-DECT's reworked Provisioning & Software Update concept, parts of the OMM Web Service have been extended or otherwise adjusted to provide for a consistent and comprehensive configuration and status report interface. The overall look and feel of the OMM Web Service remains the same as in previous versions, with the addition of new configuration parameters and status information. Some existing sections have migrated or otherwise been rearranged, as they are now considered part of the Provisioning & Software Update concept. Obsolete and/or excess elements have been disabled or completely removed to avoid confusion and simplify the user experience.

All new and/or modified parameters described in the previous section are supported by the OMM Web Service. This enables the user to see the full extent of the current Provisioning & Software Update

configuration, adjust both general and trigger-specific parameters, as well as to enable or disable specific features such as automatic and time-based events at all times.

2.19.1 PROVISIONING & SOFTWARE UPDATE

The already existing Provisioning Web page has been renamed to Provisioning & Software Update to point out that SW update is now an integral part of provisioning. As the existing functionality has been enhanced, new parameters were added to this Web page. In addition, the pre-existing “Software update URL” section, formerly located on the System Settings page, has been moved to this page as well. The following table shows the settings available in the OMM Web provisioning & SW update view.

Provisioning & Software Update parameter	New in 8.3	Available in Web*	
		Basic view	Advanced view
Current Provisioning URL	-	Yes	Yes
System credentials	-	Yes	Yes
User name	-	Yes	Yes
Password	-	Yes	Yes
Password confirmation	-	Yes	Yes
Provisioning URL	-	-	Yes
Active	-	-	Yes
Protocol	-	-	Yes
Server	-	-	Yes
Port	-	-	Yes
Path	-	-	Yes
Software update URL ***	-	-	Yes
Configure specific source	-	-	Yes
Protocol	-	-	Yes
Server	-	-	Yes
Port	-	-	Yes
User name	-	-	Yes
Password	-	-	Yes
Password confirmation	-	-	Yes
Path	-	-	Yes
Use provisioning security configuration	-	-	Yes
System update	-	Yes	Yes
Order of download and application of files****	Yes	Yes	Yes
On OMM restart*****	Yes	Yes	Yes
Time-controlled	-	-	Yes

Provisioning & Software Update parameter	New in 8.3	Available in Web*	
		Basic view	Advanced view
Time of day	-	-	Yes
Maximum delay (minutes)	-	-	Yes
Calculated time of day	-	-	Yes
Start (or abort) system update manually Update Button / Abort Button	No/Yes	Yes, manual only	Yes
Trigger configuration per trigger: Manual trigger, RFP/OMM (re)start, SIP Notify, Scheduled update	Yes	Yes	Yes
Software update	Yes	Yes	Yes
RFP software	Yes	Yes	Yes
Configuration	Yes	Yes	Yes
OMM configuration	Yes	Yes	Yes
IMA configuration	Yes	Yes	Yes
Branding image	Yes	Yes	Yes
License**	Yes	Yes	Yes
User data	Yes	Yes	Yes
SIP certificates	Yes	Yes	Yes
Provisioning certificates	Yes	Yes	Yes
Web / AXI certificates	Yes	Yes	Yes
WPA supplicant certificates	Yes	Yes	Yes
Time to wait after error (seconds)	Yes	Yes	Yes
Random component (seconds)	Yes	Yes	Yes
Number of retries	Yes	Yes	Yes
Software activation	Yes	Yes	Yes
Trigger Automatic, Manual, Time-controlled	Yes	Yes	Yes
Time of day :	Yes	-	Yes
Calculated time of day --:--	Yes	-	Yes
Mode "on by one", "all at once"	-	Yes	Yes
One-by-one activation timeout	Yes	-	Yes
Time of day :	Yes	-	Yes
Calculated time of day --:--	Yes	-	Yes
Start new software activation manually Activate Button	Yes	Yes	Yes
Certificates	-	-	Yes

Provisioning & Software Update parameter	New in 8.3	Available in Web*	
		Basic view	Advanced view
Trusted certificate(s)	-		
Local certificate chain	-		
Private key	-		
Private key password	-		
Password confirmation	-		
Delete certificates/key	-		
SSL version	-		
Validate certificates	-		
Validate expires	-		
Validate host name	-		
Allow unconfigured trusted certificates	-		
Import certificates with first connection	-		
Manual import	-	-	Yes
Import PEM file with	-	-	Yes
Import PEM file	-	-	Yes
User data import	-	-	Yes
Configure specific source	-	-	Yes
Protocol	-	-	Yes
Server	-	-	Yes
Port	-	-	Yes
User name	-	-	Yes
Password	-	-	Yes
Password confirmation	-	-	Yes
Path	-	-	Yes
Use provisioning security configuration	-	-	Yes
OM Integrated Messaging & Alerting service	-	-	Yes
Configure specific source	-	-	Yes
Protocol	-	-	Yes
Server	-	-	Yes
Port	-	-	Yes
User name	-	-	Yes

Provisioning & Software Update parameter	New in 8.3	Available in Web*	
		Basic view	Advanced view
Password	-	-	Yes
Password confirmation	-	-	Yes
Path	-	-	Yes
Use provisioning security configuration	-	-	Yes

* SIP-DECT and SIP-DECT with Cloud-ID mode

** The application of a license file has only an effect in the standard SIP-DECT mode and not in SDC mode.

*** Moved from the system settings section to provisioning & SW update

**** This parameter is always set to "Configuration before SW" for the Linux server OMM and is read-only on the user interfaces.

***** This parameter is not relevant for the Linux server OMM and is not offered on the user interfaces.

2.19.2 CHANGES ON THE STATUS WEB PAGE

The already existing Status page has been extended with a **"Software update"** section, which contains information about the OMM/RFP software update process. This new section includes a global software update status, which is always displayed, followed by varying amounts of information depending on said global status.

The following section provide an overview of the new Status page content.

Note: The layout of the Status page is the same regardless of the selected view.

Global status

The first and most essential element, it indicates if a software update process is running at any given time and if so, which stage of the process the system is in.

There are only four possible global statuses, namely:

- **Idle:** No software update process is running at the time
- **In progress:** A software update process is running. Software is being downloaded, verified, and distributed from the OMM to all base stations in the system.
- **Awaiting activation:** A software update process is running. The software has been successfully downloaded, verified, and distributed to all base stations in the system. The OMM is waiting for a signal to initiate activation of the new software. This state can only be reached when software activation is configured not to occur automatically after download and distribution.
- **Activation in progress:** A software update process is running. The software is being activated on the base stations according to the current configuration.

Note: After successful activation of new software, the software update process is deemed finished and the global software update status goes back to idle.

New software version

A string that indicates the version of the software to be installed. It is only visible after successful verification of the software.

Software downloaded

A counter that indicates how many of the connected base stations have loaded the new software. It is only visible after successful verification of the software.

Software activated

A counter that indicates how many of the connected base stations have activated the new software. It is only visible after successful verification of the software.

The following figure presents a typical view of the Status page including the new “Software update” section.

Status	
General	
OpenMobility Manager	SIP-DECT 8.1
Uptime	4 Days, 16:19
Licenses	Built-in license for up to 5 DECT base stations
Standby OMM	 There is no OpenMobility Manager in standby mode configured!
OM Integrated Messaging & Alerting service	
Base Stations	
Total number	5
Connected	5 
DECT activated	5
DECT currently active	5 
DECT clusters	1
WLAN activated	0
Software update	
Global status	In progress
New software version	SIP-DECT 8.2
Software downloaded	3
Software activated	0
DECT Phones	
Users	15
Devices	10
Subscribed	10 
Subscription allowed	
Activate firmware update	
Loading firmware from	internal
Firmware version	[650,602: 7.3.2] - [602v2: 7.3.2]
Number of known downloadable DECT phones	1
Number of barred DECT phones	1

2.20 OMP

2.20.1 PROVISIONING & SOFTWARE UPDATE

The existing OMP Provisioning section has been renamed to Provisioning & Software Update to point out that SW update is now an integral part of provisioning. As the existing functionality has been enhanced, new parameters are added to this section. Some related configurations are moved from other parts of the OMP. Depending on the OMP mode – Configuration or Monitoring, it consists of these views:

- **General:** Configuration of Provisioning URL and TLS settings
- **System update:** Configuration of general provisioning and software activation parameters, as well as buttons to start and abort these processes manually
- **Current provisioning settings:** Shows 'Used Provisioning URL' and TLS settings (Monitor mode only)
- **Provisioning Certificates:** Loading of Provisioning certificates and Private Key
- **Provisioning certificate server:** Activation and configuration of a server URL for loading the Provisioning Certificates
- **System credentials:** Configuration of system credentials (Configuration mode only)
- **Event trigger:** Configuration of the Provisioning event trigger Manual, Reboot/Restart, SIP-Notify and Scheduled
- **User data import:** Activation and configuration of a specific User data server URL
- **Software update URL:** Activation and configuration of a specific DECT base station Software update URL
- **IMA:** Activation and configuration of a specific Integrated Messaging and Alarming server URL
- **Branding image URL:** Activation and configuration of a specific Branding image server URL
- **OMM certificate server:** Activation and configuration of a server URL for loading the OMM certificates
- **802.1x certificate server:** Activation and configuration of a server URL for loading the 802.1x WPA supplicant certificates
- **SIP certificate server:** Activation and configuration of a server URL for loading the SIP certificates

Most settings were already part of earlier SIP-DECT releases. Some are grouped into the Provisioning section for the first time. Sections **System update** and **Event trigger**, which are new to this release, will be described in detail.

OMP Provisioning Overview:

The screenshot displays the Mitel OMP Provisioning & Software Update configuration interface. The interface is divided into a sidebar on the left and a main configuration area on the right. The sidebar contains navigation links for Configuration, Status, System, Sites, and Licenses. The main area shows the 'Provisioning URL' and 'TLS settings' sections. The 'Provisioning URL' section includes fields for Active, Protocol (TFTP), Port, Server (10.103.35.14), and Path (/itkaule/prov_cnf). The 'TLS settings' section includes checkboxes for Validate certificates, Validate expires, and Validate host name, along with options for Allow unconfigured trusted certificates, Import certificates with first connection, and TLS version (Auto). The interface also features a 'General' tab and a 'System update' tab.

OMP Provisioning System update

This section provides access to Provisioning System update parameters and allows to start an update process manually, to abort an active update process and to manually start an activation process of new DECT base station software version. It is divided into three sections: **Update**, **Time-Controlled update**, and **Software activation**.

Update

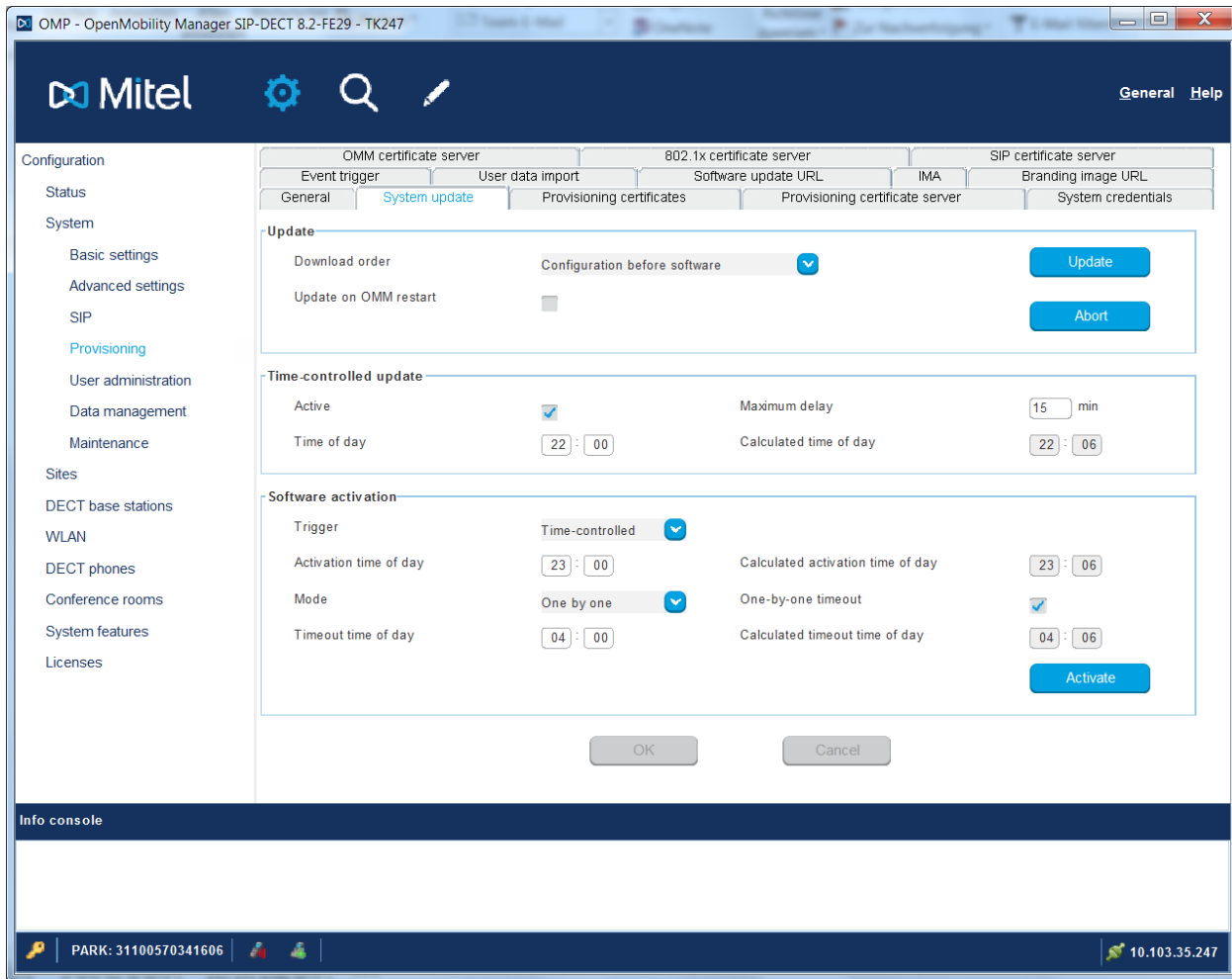
- **Download Order:** Select if configuration files are downloaded before the DECT base station software or vice versa. In the latter case, the DECT base stations are updated (and restarted) with the new software immediately after download.
- **Update on OMM restart:** If set, an OMM restart provokes a Reboot/Restart event trigger.
- **Button 'Update':** Provokes a Manual event trigger.
- **Button 'Abort':** Abort a currently active Provisioning event.

Time-controlled update

- **Active:** Activate the Provisioning event trigger Schedule
- **Time of day:** Set the time of day of the scheduling event.
- **Maximum delay:** A delay between 0 and the configured value (in minutes) is added to the time of day of the trigger, to allow a spreading of the schedule event for different SIP-DECT systems.
- **Calculated time of day:** Shows the concrete time of day of scheduled event.

Software activation

- **Trigger:** Set the DECT base station software activation method:
 - Time-controlled: Activation starts at a selected time of day
 - Automatic: Activation starts immediately after the download is finished
 - Manual: Activation is started by the user with the button 'Activate'
- **Activation time of day:** Time of day of software activation.
- **Calculated activation time of day:** Specific time of day of software activation (derived from Activation time of day and the delay calculated for the Update time of day in section 'Time-controlled update').
- **Mode:** Select if all DECT base stations are activated at once or one by one.
- **Timeout time of day:** If one by one is selected a timeout time can be configured. At that time, the one-by-one is cancelled, and all remaining DECT base stations are activated immediately.
- **Calculated timeout time of day:** Specific time of day of One by one timeout (derived from Timeout time of day and the delay calculated for the Update time of day in section 'Time-controlled update').
- **Button 'Activate':** Start the activation immediately.



OMP Provisioning Event trigger:

This section allows the configuration of the four different Provisioning trigger events:

- **Manual:** Triggered by button 'Update'
- **Reboot/restart:** Triggered by reboot of the DECT base station and optionally by an OMM restart.
- **SIP-Notify:** Triggered by receiving SIP-Notify events.
- **Scheduled:** Triggered if configured update time of day is approached.

The following settings can be configured for any single event trigger:

- **Software update:** Download the DECT base station software and activate it.
- **DECT base station software:** Select the mode of the software update:
 - **None:** Software is not downloaded. Do not select this, if Software update is activated.
 - **Optional:** Software download is optional. Unsuccessful downloading of the software does not cancel the currently running Provisioning process.
 - **Mandatory:** Software download is mandatory. If the software file cannot be downloaded by any reason, the currently running Provisioning process is cancelled.
- **Configuration:** Download configuration files from Provisioning server. The selection of files to be downloaded is configured by the following file selection. All files can be set to one of the following modes:
 - **None:** File shall not be downloaded
 - **Optional:** File download is optional, if it cannot be downloaded, the current Provisioning goes on

- **Mandatory:** File download is mandatory, if not downloadable, the current Provisioning process is stopped
- Following configuration files are supported:
 - OMM configuration
 - IMA configuration
 - Branding image
 - License
 - User data
 - SIP certificates
 - Provisioning certificates
 - OMM (WEB/AXI) certificates
 - 802.1x WPA supplicant certificates
- **Initial wait time after error:** Period of time to wait after a download trial failed (in sec.)
- **Random component:** A calculated time value between 0 and the selected random component (in sec.) is added to the Initial wait timer, to calculate the real wait time. For every retry the real wait time is doubled.
- **Number of retries:** Number retries in case of error for every single file to be downloaded.

Instead to configure any single event trigger individually, all can be set to the same values described above, by selecting the check box 'Select All'. By starting the OMP this check box is disabled, that means individually event trigger configuration is active. If the check box is (un)selected, all changes, which were not confirmed by button 'OK', are lost and the last stored configuration is active again.

Event trigger	Manual	Reboot/Start	SIP Notify	Scheduled	All
☐ Select 'All'					
Software update	☒	☐	☒	☒	☐
DECT base station software	M	M	M	M	M
Configuration	☒		☒	☒	☐
OMM configuration	O	O	O	O	O
IMA configuration	O	O	-	O	***
Branding image	O	-	-	O	***
License	O	-	-	O	***
User data	O	-	-	O	***
SIP certificates	O	-	-	O	***
Provisioning certificates	O	-	-	O	***
Web/AXI certificates	O	-	-	O	***
802.1x certificates	O	-	-	O	***
Initial wait time after error (sec)	10	10	10	10	10
Random component (sec)	10	10	10	10	10
Number of retries	3	3	1	3	***

The following table shows the settings available in the OMP provisioning & SW update section.

Provisioning & Software Update parameter	New in 8.3	Comment	Provisioning Configuration view Tab	Provisioning Monitor view Tab	Supported by OMM Web Service
Current Provisioning URL	-			Current Configuration file settings	Yes
System credentials	-		System credentials		Yes
User name	-				
Password	-				
Password confirmation	-				
Provisioning URL	-		General		Yes
Active	-				
Protocol	-				
Server	-				
Port	-				
Path	-				
Software update URL	-	Moved from system settings	Software update URL		Yes
Configure specific source	-				
Protocol	-				
Server	-				
Port	-				
User name	-				
Password	-				
Password confirmation	-				
Path	-				
Use provisioning security configuration	-				
System update	-		Update		Yes
Order of download and application of files*	Yes				
On OMM restart**	Yes				
Time-controlled	-				
Time of day	-				
Maximum delay (minutes)	-				

Provisioning & Software Update parameter	New in 8.3	Comment	Provisioning Configuration view Tab	Provisioning Monitor view Tab	Supported by OMM Web Service
Calculated time of day 00:00	-				
Start (or abort) system update manually Update Button / Abort Button	No/Yes				
Trigger configuration per trigger: Manual trigger, RFP/OMM (re)start, SIP Notify, Scheduled update	Yes		Event Trigger		Yes
Software update	Yes				Yes
RFP software	Yes				
Configuration	Yes				
OMM configuration	Yes				
IMA configuration	Yes				
Branding image	Yes				
License**	Yes				
User data	Yes				
SIP certificates	Yes				
Provisioning certificates	Yes				
Web / AXI certificates	Yes				
WPA supplicant certificates	Yes				
Time to wait after error (seconds)	Yes				
Random component (seconds)	Yes				
Number of retries	Yes				
Software activation	Yes		Update		Yes
Trigger Automatic, Manual, Time-controlled	Yes				
Time of day :	Yes				
Calculated time of day - :-	Yes				
Mode "on by one", "all at once"	-				

Provisioning & Software Update parameter	New in 8.3	Comment	Provisioning Configuration view Tab	Provisioning Monitor view Tab	Supported by OMM Web Service		
One-by-one activation timeout	Yes						
Time of day :	Yes						
Calculated time of day - :--	Yes						
Start new software activation manually Activate Button	Yes						
Provisioning Certificates	-		Provisioning Certificates	Yes			
Trusted certificate(s)	-						
Local certificate chain	-						
Private key	-						
Private key password	-						
Password confirmation	-						
Delete certificates/key	-						
TLS version	-		General				
Validate certificates	-						
Validate expires	-						
Validate host name	-						
Allow unconfigured trusted certificates	-						
Import certificates with first connection	-						
Manual import	-		Provisioning Certificates			Yes	
Import PEM file with	-						
Import PEM file	-						
Provisioning Certificate Server	-		Provisioning Certificate Server	No			
Active flag							
Protocol							
Server							
Port							
User name	-						
Password	-						
Password confirmation	-						

Provisioning & Software Update parameter	New in 8.3	Comment	Provisioning Configuration view Tab	Provisioning Monitor view Tab	Supported by OMM Web Service
Path without filename	-				
Use provisioning security configuration	-				
Trusted certificate file	-				
Local certificate chain file	-				
Private key file	-				
OM Integrated messaging and alerting service URL	-	Moved from System / Advanced settings / IMA	IMA / OM Integrated messaging and alerting service URL		Yes, under system settings
Configure specific source	-				
Protocol	-				
Server	-				
Port	-				
User name	-				
Password	-				
Password confirmation	-				
Path	-				
Use provisioning security configuration	-				
User data import	-	Moved from System/ Data Management/ User data import	User data import		Yes, SDC only
Configure specific source	-				
Protocol	-				
Server	-				
Port	-				
User name	-				
Password	-				
Password confirmation	-				
Path	-				
Use provisioning security configuration	-				
Branding image URL	-	Moved from System/ Advanced	Branding image URL		No
Configure specific source	-				

Provisioning & Software Update parameter	New in 8.3	Comment	Provisioning Configuration view Tab	Provisioning Monitor view Tab	Supported by OMM Web Service
Protocol	-	settings/ Special Branding			
Server	-				
Port	-				
User name	-				
Password	-				
Password confirmation	-				
Path	-				
Use provisioning security configuration	-				
OMM Certificate Server	-	Moved from System/ Advanced settings/ OMM Certificate Server	OMM Certificate Server		No
Active flag	-				
Protocol	-				
Server	-				
Port	-				
User name	-				
Password	-				
Password confirmation	-				
Path without filename	-				
Use provisioning security configuration	-				
Trusted certificate file	-				
Local certificate chain file	-				
Private key file	-				

* This parameter is always set to "Configuration before SW" for the Linux server OMM and is read-only on the user interfaces.

** This parameter is not relevant for the Linux server OMM and is not offered on the user interfaces.

2.20.2 STATUS DECT BASE STATION - SOFTWARE UPDATE

The Provisioning status page contains a new section 'Software update', which provides status information about the Update process:

- **Software downloaded:** Number of DECT base stations which have received a new software version.
- **Software activated:** Number of DECT base stations which have received and activated the new software.
- **Status:** Status of the Software update process (for further details see description in chapter 'Changes on the status Web page'):
 - Idle

- In progress
- Awaiting activation
- Activation in progress
- **New software version:** Name of the software which shall be provided in the system

The screenshot shows the Mitel Provisioning web interface. The top navigation bar includes the Mitel logo, a settings gear, a search icon, and a pencil icon. Below the navigation bar, there are tabs for Overview, DECT base stations, Users, Devices, Sites, Conference, Provisioning (selected), and Provisioning health report. On the left, a sidebar lists various configuration categories: Status, System, Sites, DECT base stations, WLAN, DECT phones, Conference rooms, System features, Licenses, and Support. The main content area is titled 'Update status' and contains two sections. The first section, 'Update status', has two dropdown menus: 'Software' (set to 'Idle') and 'Configuration' (set to 'Idle'). The second section, 'Software update', is highlighted with a red rectangular box and contains four fields: 'Software downloaded' (0), 'Software activated' (0), 'Status' (Idle), and 'New software version' (an empty text input field).

2.21 KEEP DB FROM FORMER RELEASE AND SUPPORT AUTOMATIC FALLBACK IN UPGRADE/DOWNGRADE SCENARIOS

Note: In principle the latest available software should be used because newer software provides new functions, bug fixes, fixes for security gaps etc. A downgrade to the previous software is an exception and should not occur. The only reason for a downgrade is a serious unexpected problem that makes it impossible to use the system after an upgrade.

SIP-DECT databases are not backwards compatible. When a system is upgraded, the database is automatically converted to the current data model. A downgrade requires the application of the DB backup that was generated before the upgrade.

Despite the various options to generate DB backups and to apply them there are scenarios which do not allow manual intervention e.g. in case of fallback to the previous SW for a bigger number of small installations. For small installations, automatic DB backup is often not enabled. In addition, the application of DB backups is time consuming if it is to be performed on many installations.

As of SIP-DECT 8.3, an automatic internal DB backup and fallback mechanism is supported. When a system is upgraded, the DB from the previous release remains in the file system of the OMM platform. This DB is automatically being used when downgrading to the previous SW. The mechanism is based on time stamps. Therefore, NTP is mandatory.

Only the DB file from the previous SW remains in the file system in addition to the DB file of the currently active SW.

The databases of SW builds in a major/minor release stream are compatible. Service packs and Hotfixes for a release does not contain incompatible DB changes.

If there is a downgrade to an older SW without a matching DB file in the file system, the system will start up with an empty database.

The following table provides an overview of various scenarios to illustrate the statements above.

Scenario	Active SW/ go from	passive SW/ previous	New SW/ go to	OMM DB files before update	OMM DB files after update (* = currently used)	Note
1	X.a < 8.3	-	8.3	X.a*	8.3*, X.a	X.a DB migrated to 8.3
2	8.3	X.a < 8.3	X.a < 8.3	8.3*, X.a	X.a*, 8.3	Fallback to X.a DB
3	X.a < 8.3	8.3	8.3	X.a*, 8.3	8.3*, X.a	X.a DB migrated to 8.3
4	8.3	X.a < 8.3	Y.b > 8.3	8.3*, X.a	Y.b*, 8.3	8.3 DB migrated to Y.b, X.a file removed
5	8.3	-	X.a < 8.3	8.3*	X.a*, 8.3	As there is no X.a DB to fallback to – X.a starts with empty DB
6	X.a < 8.3	-	Y.b	X.a*	Y.b*, X.a	X.a DB migrated to Y.b

It is still possible to manually apply DB's from later versions to older SW versions, but without guaranteed functionality and without a compatibility statement.

Selecting the 'Discard OMM DB' option during a restart of the OMM, does not only delete the DB of the currently running SIP-DECT SW version, but also the DB of the previously running SW version!

Note: One of the final steps before upgrading is to change the SW Update URL to point to the SW that the system is to be updated to. If this DB is restored during a later necessary downgrade, then the URL in the restored DB immediately points to the upgrade software again. To prevent another update, SW update in the reboot/restart, SIP Notify, and scheduled update trigger configuration is automatically disabled. If required, it needs to be enabled in a separate step later.

If no provisioning or software update URL is configured in the OMM, the trigger configuration is not automatically changed because the URL from which the software is to be retrieved is provided in another way, e.g. DHCP and these will be correct.

2.22 SIP “TLS-COMMON-NAME-VALIDATION” FLAG RENAMED TO “VALIDATE HOST NAME”

As of SIP-DECT 8.3SP1 the “TLS-Common-Name-Validation” flag in the SIP settings has been renamed to “Validate host name”. It corresponds to the “Validate host name” flag of the provisioning security settings.

Note on downgrade to a SW < 8.3: As explained above, the SW update in the reboot/restart, SIP Notify, and scheduled update trigger configuration is automatically disabled to prevent another update. This is not supported by SW older than 8.3SP1. If the provisioning or software update URL is used to configure the source of the new SW, other steps must be taken to prevent an immediate upgrade from being performed by the older SW.

Prevent access to the SW on the server

The SIP-DECT system will not update if the new SW cannot be accessed. There are various options to prevent the access e.g. block the IP traffic to the server e.g. pull the uplink, turn the server temporarily off, block the access by changing the access rights, remove the SW files, replace the SW files with the SW you want to run, etc.

Remove DB file from OMMs file system and apply DB backup afterwards

This requires that a DB backup file has been saved before changing the URL from which the new software is to be retrieved. To remove the DB files (omm_conf.txt for SW older than 8.3) from the RFP on which the OMM is running, log on to the RFP console via SSH. Please make sure that the SSH console is activated in the OMM configuration. After logging in successfully, change to the “root” user with the “su” command. Go to /var/opt/omm/ and remove the omm_conf.* Files. The same must be done on the standby OMM system.

```
rfp4g_C3DF0A login: omm
Password:
[root@rfp4g_C3DF0A]# Jun 23 14:28:06 su: + ttyMV0 omm:root
[root@rfp4g_C3DF0A]# cd /var/opt/omm/
[root@rfp4g_C3DF0A]# ll
 4 drwxr-xr-x    3 root root  4096 Jun 23 14:30 .
 4 drwxr-xr-x   15 root root  4096 Jun 22 16:13 ..
 4 -rw-r--r--    1 root root    7 May 31 06:42 RcsFile
 4 -rw-r--r--    1 root root    7 May 31 06:42 RcsParkFile
 4 -rw-----    1 root root   32 Jun 23 11:40 omm_access.log
 4 -rw-r--r--    1 root root    5 Jun 23 14:29 omm_conf.txt
 4 -rw-r--r--    1 root root    5 Jun 23 14:29 omm_conf.txt.backup
 4 -rw-----    1 root root   16 Jun 23 11:44 omm_conf_8.3SP1.md5
80 -rw-----    1 root root 78496 Jun 23 11:44 omm_conf_8.3SP1.txt
80 -rw-r--r--    1 root root 78496 Jun 23 11:44 omm_conf_8.3SP1.txt.backup
 4 drwxr-x---    2 root root  4096 Jun  3 16:15 spy
[root@rfp4g_C3DF0A]#
[root@rfp4g_C3DF0A]# rm omm_conf.*
[root@rfp4g_C3DF0A]# ll
 4 drwxr-xr-x    3 root root  4096 Jun 23 14:31 .
 4 drwxr-xr-x   15 root root  4096 Jun 22 16:13 ..
 4 -rw-r--r--    1 root root    7 May 31 06:42 RcsFile
 4 -rw-r--r--    1 root root    7 May 31 06:42 RcsParkFile
 4 -rw-----    1 root root   32 Jun 23 11:40 omm_access.log
 4 -rw-----    1 root root   16 Jun 23 11:44 omm_conf_8.3SP1.md5
80 -rw-----    1 root root 78496 Jun 23 11:44 omm_conf_8.3SP1.txt
80 -rw-r--r--    1 root root 78496 Jun 23 11:44 omm_conf_8.3SP1.txt.backup
 4 drwxr-x---    2 root root  4096 Jun  3 16:15 spy
[root@rfp4g_C3DF0A]#
```

After downgrade the system will start with an empty DB and the DB backup file must be applied.

Temporarily interrupting the IP connection to the software download server is probably the easiest way to prevent the immediate upgrade after the downgrade.

2.23 SIP “TLS-AUTHENTICATION” FLAG RENAMED TO “VALIDATE CERTIFICATES”

As of SIP-DECT 8.3SP1 the “TLS-Authentication” flag in the SIP settings has been renamed to “Validate certificates”. It corresponds to the “Validate certificates” flag of the provisioning security settings.

2.24 HARMONIZATION OF THE CERTIFICATE VALIDATION & SECURITY HANDLING SETTINGS

As of SIP-DECT 8.3SP1, various certificate validation and security handling settings has been harmonized between different SIP-DECT features.

2.25 VALIDATE HOST NAME AND VALIDATE EXPIRES ONLY RELEVANT IF VALIDATE CERTIFICATES FLAG IS SET

As of SIP-DECT 8.3SP1, the existing OMM provisioning settings “Validate host name” and “Validate expires” are only considered if “Validate certificates” is enabled. I.e. if certificates are not validated against trusted root certificates then the host name and validity dates are also not validated.

The handling is based on that of SIP and LDAPS.

2.26 URL PARAMETER FOR VARIOUS URLS “USE COMMON CERTIFICATE CONFIGURATION” FLAG RENAMED TO “USE PROVISIONING SECURITY CONFIGURATION”

As of SIP-DECT 8.3SP1 the flag ““Use common certificate configuration” of various URLs has been renamed to “Use provisioning security configuration”.

The screenshot shows a provisioning configuration form with the following fields and values:

- Configure specific source:** ☒
- Protocol:** HTTPS (dropdown menu)
- Server:** server (text input)
- Port:** (empty text input)
- User name:** (empty text input)
- Password:** (empty text input)
- Password confirmation:** (empty text input)
- Path:** path (text input)
- Use provisioning security configuration:** ☒ (This row is highlighted with a red border)

2.27 OMP PROVISIONING TLS/SSL SETTINGS RENAMED TO “SECURITY”

As of SIP-DECT 8.3SP1 the TLS/SSL setting section in the OMP provisioning general section has been renamed to “Security”.

SSL settings

Validate certificates	☒	Allow unconfigured trusted certificates	☐
Validate expires	☒	Import certificates with first connection	☐
Validate host name	☒	SSL version	Auto <input checked="" type="button" value="v"/>

SIP-DECT 8.1 OMP provisioning general section

Security

Validate certificates	☒	Allow unconfigured trusted certificates	☐
Validate expires	☒	Import certificates with first connection	☐
Validate host name	☒	TLS version	Auto <input checked="" type="button" value="v"/>
Security level	Global <input checked="" type="button" value="v"/>		

SIP-DECT 8.3 OMP provisioning general section

2.28 OMM WEB PROVISIONING “CERTIFICATES” SETTINGS RENAMED TO “SECURITY”

As of SIP-DECT 8.3SP1 the Certificate section on the OMM Web provisioning page has been renamed to “Security”.

The screenshot shows the Mitel OMM Web provisioning interface for SIP-DECT 8.1. The top navigation bar includes the Mitel logo, the device name 'SIP-DECT 8.1', and links for 'Advanced', language selection ('DE', 'EN', 'ES', 'FR'), and 'Logout'. A left sidebar lists navigation options: Status, System, System Settings, Provisioning (highlighted), SIP, User, and Administration. The main content area displays the 'Certificates' section, which is highlighted with a red rectangular box. This section contains fields for 'Trusted certificate(s)' (0), 'Local certificate chain' (0), 'Private key' (marked with a red 'X'), 'Private key password' (text input), 'Password confirmation' (text input), a 'Delete certificates/key' button, and 'SSL version' (set to 'Auto' with a dropdown arrow).

SIP-DECT 8.1 OMM Web provisioning settings

The screenshot shows the Mitel OMM Web provisioning interface for SIP-DECT 8.3. The top navigation bar is identical to the previous version, showing 'SIP-DECT 8.3' and the same utility links. The left sidebar is also identical. The main content area now displays the 'Security' section, which is highlighted with a red rectangular box. The layout and fields within this section are identical to the 'Certificates' section in the SIP-DECT 8.1 version, including 'Trusted certificate(s)' (0), 'Local certificate chain' (0), 'Private key' (marked with a red 'X'), password fields, a 'Delete' button, and 'TLS version' (set to 'Auto').

SIP-DECT 8.3 OMM Web provisioning settings

2.29 OMM AND MOM CERTIFICATE UPDATE

As of SIP-DECT 8.3SP1, the OMM and MOM default certificates are updated to extend the expire date from Sunday, October 27, 2024 to Monday, June 2, 2031.

2.30 RFP43 WLAN AND RFP 48 WLAN AFFECTED BY FRAGATTACK VULNERABILITY

The SIP-DECT base stations RFP 43 WLAN and RFP 48 WLAN are affected by low and medium severity FragAttack vulnerabilities. The following table provides an overview of which RFP is affected by which vulnerability, as of SIP-DECT 8.3SP1.

Vulnerabilities	CVSS 3.x Base Score		RFP43	RFP48
CVE-2020-24587 - Reassembling fragments encrypted under different keys	2.6	Low	No affected	Fixed
CVE-2020-24588 - Accepting non-SPP A-MSDU frames, which leads to payload being parsed as an L2 frame under an A-MSDU bit toggling attack	3.5	Low	Fixed	Affected
CVE-2020-26140 - Accepting plaintext data frames in protected networks	6.5	Medium	Fixed	Fixed
CVE-2020-26143 - Accepting fragmented plaintext frames in protected networks	6.5	Medium	Fixed	Fixed
CVE-2020-26146 - Reassembling encrypted fragments with non-consecutive packet numbers	5.3	Medium	Not affected	Affected
CVE-2020-26147 - Reassembling mixed encrypted/plaintext fragments	5.4	Medium	Fixed	Fixed

2.31 DISCONTINUE "SSL VERSION" PARAMETER IN MOM

As of SIP-DECT 8.3SP1, the "SSL version" setting in the OMMs certificate tab on the MOM Web service is discontinued. Instead of providing an option to select TLS 1.2, TLS 1.3 or "Auto", the mode "Auto" is set by the MOM in the OMM provisioning settings if the MOM is the source of provisioning data for the OMMs. "Auto" includes TLS 1.2 and TLS 1.3. If the default system security level and cipher suites are used then the OMM MOM connection is using TLS 1.3.

2.32 EMERGENCY LOCATION IDENTIFICATION NUMBER (ELIN) SUPPORT

As of SIP-DECT 8.3SP1, SIP-DECT supports providing an Emergency Location Identification Number (ELIN) in the SIP signaling of incoming and outgoing calls. This helps the call server (SIP proxy) to determine the correct public-safety answering point (PSAP) depending on where the call has made.

An ELIN can be set for:

- the system
- a site
- a specific base station

The more specific parameter value is used.

If the ELIN support is enabled the configured ELIN value is sent in the FROM header field of the SIP invite and the P-Asserted-Identity field of the 200 OK. The ELIN is a string of up to 31 characters. There is no specific limitation on character set. Characters are escaped in the SIP header if necessary.

Examples:

```
From: "Extension 5115" <sip:5115@example.com;elin=0123456789>;tag=f-5899462600ef0a1c
```

```
P-Asserted-Identity: <sip:5115@example.com;elin=0123456789>
```

The configuration can be done via the OMM web service or OMP. Only the general activation of this feature and the system-wide emergency location identification number can be set via the OMM configuration files.

Parameter / Group	System emergency location identification number enabled
Description	The parameter "enabled" of the system emergency location identification number configuration enables the sending of the configured ELIN in the SIP signaling.
Format	Boolean
Range	1 or true (enable) 0 or false (disable)
Default value	False
OMP	System/ Advanced settings / Emergency location / Emergency location identification number / Enabled
OMM Web	Advanced: System/ Advanced / Emergency location
MOM Web	n.a.
OMM configuration files	<SetELIN enable="1" />
DECT Phone	n.a.
User configuration files	n.a.

Parameter / Group	System emergency location identification number
Description	The system parameter "Emergency call identification number" provides the system-wide valid emergency call identification number. This value is used when there is no more specific ELIN set. The parameter can be used for small systems in which the same ELIN should be used for all base stations.
Format	String
Range	Up to 31 character
Default value	Empty
OMP	System/ Advanced settings / Emergency location / Emergency location identification number / Number
OMM Web	Advanced: System/ Advanced / Emergency location
MOM Web	n.a.
OMM configuration files	<SetELIN elinNumber="0123456" />
DECT Phone	n.a.
User configuration files	n.a.

Parameter / Group	Site emergency location identification number
Description	The site parameter "Emergency location identification number" provides the site-wide valid emergency location identification number. This value is used if there is no ELIN set for a specific base station. The parameter can be used for small sites in which the same ELIN should be used for all base stations.
Format	String
Range	Up to 31 characters
Default value	Empty
OMP	Sites/ Emergency location identification number
OMM Web	Sites/ Emergency location identification number
MOM Web	n.a.
OMM configuration files	n.a.
DECT Phone	n.a.
User configuration files	n.a.

Parameter / Group	Base station's emergency location identification number
Description	The base station parameter "Emergency location identification number" provides an emergency location identification number for a specific base station.
Format	String
Range	Up to 31 characters
Default value	Empty
OMP	DECT base stations/ Emergency location identification number
OMM Web	Base Stations/ Emergency location identification number
MOM Web	n.a.
OMM configuration files	n.a.
DECT Phone	n.a.
User configuration files	n.a.

If ELIN support is enabled and at least one RFP has no ELIN assigned, a warning is displayed on the status information page.

The screenshot shows the Mitel configuration interface. The top navigation bar includes the Mitel logo, a settings gear, a search icon, and a pencil icon. On the right, there are links for 'General' and 'Help'. Below the navigation bar, there are tabs for 'Overview', 'DECT base stations', 'Users', 'Devices', 'Sites', 'Conference', 'Provisioning', and 'Provisioning health report'. The 'Overview' tab is selected. On the left, there is a sidebar with a 'Configuration' section containing links for 'Status', 'System', 'Sites', 'DECT base stations', 'WLAN', 'DECT phones', 'Conference rooms', 'System features', 'Licenses', and 'Support'. The main content area is divided into two panels: 'System' and 'Features'. The 'System' panel shows various system status items with green checkmarks, indicating they are all enabled or successful. The 'Features' panel shows a list of features with status indicators: 'OM Integrated Messaging & Alerting service' (green checkmark), 'User data server' (green checkmark), 'MOM control' (red X), '802.1x state' (red X), 'OMM certificate server' (red X), 'Provisioning certificate server' (red X), '802.1x certificate server' (red X), and 'SIP certificate server' (green checkmark). At the bottom of the 'System' panel, there is a red-bordered box containing the text 'Emergency location configuration' with a yellow warning icon and a message: 'Emergency location identification number not provided for all DECT base stations!'.

2.33 MANUAL USER DATA IMPORT AXI COMMAND DISCONTINUED

The ManualUserDataImport request, response, and event set is removed from the AXI interface.

2.34 UPDATE TRUSTED CERT CHAIN STORE

SIP-DECT uses the Mozilla® trusted root certificate store. As of SIP-DECT 8.3SP1, the certificate data from Mozilla® as of Friday June 4th, 07:14:42 2021 GMT are used. Data are extracted from Mozilla's root certificates file (certdata.txt). This file can be found in the Mozilla® source tree:

<https://hg.mozilla.org/releases/mozilla-release/raw-file/default/security/nss/lib/ckfw/builtins/certdata.txt>

2.35 UPDATE TO OPENLDAP 2.4.59

As of SIP-DECT 8.3SP1, OpenLDAP has been updated to version 2.4.59.

2.36 UPDATE TO ADOPTOPENJDK 11.0.19

As of SIP-DECT 9.0, the AdoptOpenJDK runtime of the OMP and OMC has been updated to 11.0.19 for Linux and Win64.

2.37 ENHANCEMENT TO MANUAL DOWNLOAD

As of SIP-DECT 8.3, the OMM executes a file system flush for DB file before manual download to avoid gap between latest status und DB backup file.

2.38 HTTP 302 STATUS CODE SUPPORTED BY OMM PROVISIONING

An HTTP response with 302 status code that provide a URL in the header field Location forces the OMM to make a second, otherwise identical, request to the new URL. This does not affect the provisioning configuration itself. A new request will be sent to the configured URL again.

2.39 RESTRICTION IN ADDING NEW DIRECTORY ENTRIES IN DIRECTORY

Since SIP-DECT 6.2, a new directory configuration has been introduced which supports 3 types of directories: LDAP, XML and XSI (Enterprise, Group, Personal). Additionally, the configuration via provisioning (OMM configuration files) is supported for the new directory configuration.

To provide backwards compatibility, the old directory configuration "Directory (comp. mode))" for LDAP or XML directories is still supported.

As of 8.3, no new entries can be added to "Directory (Comp. Mode)" to encourage the use of the default directory configuration.

2.40 ENHANCEMENT TO DEFAULT TTL VALUE

As of 8.3, the default TTL value has been increased from 32 to 64.

2.41 DISCONTINUE TFTP SERVER LIST AND PREFERRED TFTP SERVER

As of SIP-DECT 8.3, the outdated TFTP server list and preferred TFTP server parameters have been removed from the base station SW and the OM Configurator Java tool.

2.42 DISCONTINUE NON-ENCRYPTED XML API INTERFACES

In previous SIP-DECT versions, the OMM/MOM has provided a non-encrypted application interface (TCP) for the AXI/MAXI protocol. These non-encrypted XML interfaces will now be discontinued.

Only in the OMM can the non-encrypted interface be explicitly switched on for test purposes via the following OMM command:

```
cnf sys uap on
```

Warning: Opening the unsecured AXI port induces security risks!
Enable the port only, if it is really required by your application and be aware of the security concerns!

An enabled interface can be disabled again with the OMM command:

```
cnf sys uap off
```

2.43 DISCONTINUED RFP35 USB WEB CAM VIDEO SUPPORT

As of SIP-DECT Release 8.3, the USB Web Cam support that was available with base station RFP35 family, is discontinued. The current base station generation (RFP45 family) does not support USB.

2.44 MTLS SUPPORT FOR PROVISIONING

As of SIP-DECT Release 8.3, mTLS is supported for HTTPS to download configuration files and SW files.

2.45 NEW OMM WEB SERVICE AND OMP SECTION: “SUPPORT”

As of SIP-DECT 8.3, the Support section summarizes existing SIP-DECT maintenance functions. These functions can be configured in one place and are clearly distinguished from other SIP-DECT features. The Maintenance section comprises:

- **DECT phone firmware update:** activation of the firmware update and configuration of an alternative update source
- **Syslog server:** activation and Syslog server address
- **System dump:** start of a manually local system dump onto the PC running the OMP
- **Remote System dump:** activation, time of day and destination of a system dump to a remote server
- **Core dump:** configuration of a specific server to which core dumps are sent.

2.46 SUPPORT OF ADDITIONAL CRYPTO SUITE

As of version 8.3, SIP-DECT additionally supports the crypto suite AES_CM_128_HMAC_SHA1_32 for the Secure Real-time Transport Protocol (SRTP).

When SRTP is enabled, AES_CM_128_HMAC_SHA1_32 is offered for every outgoing call as a second crypto suite in addition to the previous AES_CM_128_HMAC_SHA1_80. All incoming calls offering only the AES_CM_128_HMAC_SHA1_32 crypto suite will be accepted.

2.47 ENHANCEMENT TO BASE STATION

If the URL of the RFP configuration file is set, the RFP configuration file is mandatory for starting a base station. There are several situations when a base station tries to get the files for update. If files could not be loaded, even after retry attempts, the base station was taken out of service.

In order to be more robust in the event that infrastructure services are not available, a base station remains active as long as there is a connection to the OMM.

2.48 SET CLOUD-ID KEY USING OMM CONFIGURATION FILES

As of SIP-DECT Release 8.3, the Cloud-ID key can be set via OMM configuration files (for example, in ipdect.cfg).

If the Cloud-ID key is not set, the user agent header cannot include the Cloud-ID when requesting the OMM configuration files or other resource and configuration files. The MAC address of the OMM base station is used instead.

Following is an example of setting the Cloud-ID key via the OMM configuration file:

```
<SetCloudIDKey key="18TSK-TJE8V-74ZC6-XR67A-8CAAA" />
```

The Cloud-ID is communicated in the HTTP user agent header.


```
> Transmission Control Protocol, Src Port: 33550, Dst Port: 80, Seq: :
✓ Hypertext Transfer Protocol
  > GET /ipdetect.cfg HTTP/1.1\r\n
    Host: 192.168.1.107\r\n
    User-Agent: SIP-DECT 8.2-FF14 MAC:00-1F-10-2E-F0-AF\r\n
    Accept: */*\r\n
```

If the Cloud-ID is not set, then the OMM's base station MAC address is used.

```
> Transmission Control Protocol, Src Port: 33516, Dst Port: 80, Seq: :
✓ Hypertext Transfer Protocol
  > GET /ipdetect.cfg HTTP/1.1\r\n
    Host: 192.168.1.107\r\n
    User-Agent: SIP-DECT 8.2-FF14 MAC:08-00-0F-C3-DE-64\r\n
    Accept: */*\r\n
```

2.49 AUTOMATICALLY TRUNCATE USER NAMES EXCEEDING 20 CHARACTERS

If user data is set in OMM configuration files and the user name (display name) has more than 20 characters, then the configuration is rejected. Use the configuration parameter “Truncate portable part user name” to automatically truncate the display name.

Parameter	Truncate portable part user name
Description	Enables or disables automatic truncation of user's display name if it has more than 20 characters. “1” or “true”, to enable the truncating of the PP user name attribute to the maximum length, if a client sets or creates a longer name for the user.
Format	Boolean
Range	n.a.
Default value	False
OMP	System/ Advanced settings/ User service
Web	n.a.
OMM configuration files	<SetAdditionalSettings truncatePpUserName =“1” />
DECT Phone	n.a.
User configuration files	n.a.

2.50 DNS SRV MODE FOR SIP SIGNALING

SIP-DECT Release 8.3 introduces a new DNS SRV mode for SIP signaling.

This “DNS SRV failover following registration” mode supports Telefonica's special requirements for using DNS SRV for SIP.

The new configuration parameter “DNS SRV failover following registration” can be used to enable or disable this new mode.

When “DNS SRV failover following registration” is enabled, and the following conditions

- “proxy server”, and “registrar server” are configured identically
- “proxy server” or “registrar server” and “outbound proxy” are set to DNS SRV FQDN (port 0)

are true, the new mode is active.

In this case,

- the call traffic of a user follows the registration; this means when the user is registered on (outbound) server A, an outgoing call is directed to (outbound) server A.
- when a user is in a call active state, SIP-DECT does not try a fallback to another server but remains on the registered (outbound) server. After coming back into idle state, the normal DNS SRV behavior is applied.

Parameter	DNS SRV failover following registration
Description	Enables or disables the DNS SRV failover mode “following registration”.
Format	Boolean
Range	1 or true (enable) 0 or false (disable)
Default value	False
OMP	System/ SIP/ Advanced settings
Web	Advanced: System/ SIP/ Advanced
OMM configuration files	<SetAdvancedSIP dnsSrvFollowRegistration="1" />
DECT Phone	n.a.
User configuration files	n.a.

2.51 SUPPORTING AUTOMATIC FALLBACK IN UPGRADE/DOWNGRADE SCENARIOS

SIP-DECT databases are not backwards compatible. When a system is upgraded, the database is automatically converted to the current data model. A downgrade requires the application of the DB backup that was generated before the upgrade.

Despite the various options to generate DB backups and to apply them there are scenarios which do not allow manual intervention, for example, in case of fallback to the previous SW for a bigger number of small installations. For small installations, automatic DB backup is often not enabled. In addition, the application of DB backups is time consuming if it is to be performed on many installations.

As of SIP-DECT 8.3, an automatic internal DB backup and fallback mechanism is supported. When a system is upgraded, the DB from the previous release remains in the file system of the OMM platform. This DB is automatically been used when downgrading to the previous SW. The mechanism is based on time stamps. Therefore, NTP is mandatory.

Only the DB file from the previous SW remains in the file system in addition to the DB file of the currently active SW.

The databases of SW builds in a major/minor release stream are compatible. Service packs and Hotfixes for a release does not contain incompatible DB changes.

If there is a downgrade to an older SW without a matching DB file in the file system, the system will start up with an empty database.

The following table provides an overview of various scenarios to illustrate the statements above.

Scenario	Active SW/ go from	passive SW/ previous	New SW/ go to	OMM DB files before update	OMM DB files after update (* = currently used)	Note
1	X.a < 8.3	-	8.3	X.a*	8.3*, X.a	X.a DB migrated to 8.3
2	8.3	X.a < 8.3	X.a < 8.3	8.3*, X.a	X.a*, 8.3	Fallback to X.a DB
3	X.a < 8.3	8.3	8.3	X.a*, 8.3	8.3*, X.a	X.a DB migrated to 8.3
4	8.3	X.a < 8.3	Y.b > 8.3	8.3*, X.a	Y.b*, 8.3	8.3 DB migrated to Y.b, X.a file removed
5	8.3	-	X.a < 8.3	8.3*	X.a*, 8.3	As there is no X.a DB to fallback to – X.a starts with empty DB
6	X.a < 8.3	-	Y.b	X.a*	Y.b*, X.a	X.a DB migrated to Y.b

It is still possible to manually apply DB's from later versions to older SW versions, but without guaranteed functionality and without a compatibility statement.

2.52 SUPPORTING EGYPTIAN REGULATIONS

In order to comply with the Egyptian regulations, the DECT regulatory domain must be automatically and permanently set to “EMEA” and the WLAN regulatory domain must be automatically and permanently set to “EG” (Egypt). There must be no way to change it to anything else, intentionally, or accidentally.

This was ensured by Egypt-specific SIP-DECT-SW builds, which may not be used in other countries or regions.

As of 8.3, the standard SIP-DECT software supports the Egyptian regulations in order to avoid the need for specific software builds and to make every release, service pack or hotfix available in Egypt.

To achieve this, a country tag was introduced for base stations. Currently the only used country tag is “Egypt”.

Instead of delivering a base station with a specific SW to Egypt, only the country tag has to be programmed for the base station. The country code is reset proof.

If the OMM detects at least one base station with the country code in the installation, the OMM automatically and permanently switches to the required mode.

It is mandatory that existing installations were using the SIP-DECT SW build 8.1SP3-FK24_Egypt before updating to 8.3. The SIP-DECT SW build 8.1SP3-FK24_Egypt automatically programs the country tag into the base stations.

Note: Existing installations must use the SIP-DECT SW-Build 8.1SP3-FK24_Egypt before updating to 8.3. The SIP-DECT SW-Build 8.1SP3-FK24_Egypt programs the country tag automatically in the base stations.

2.53 ENHANCEMENT TO SDP SIGNALING WHEN HOLDING A CALL

In the previous SIP-DECT versions, the OMM used the nonspecific IP address 0.0.0.0 in SDP signaling to hold a call. This caused problems in individual specific environments

As of version 8.3, the OMM uses a valid media address when holding a call.

2.54 RFP43 AND RFP48: 802.1X BIND WPA SUPPLICANT TO BRIDGE INTERFACE

Since SIP-DECT 7.1, SIP-DECT supports the certificate-based 802.1x authentication for SIP-DECT base stations. The supplicant is usually linked to the base station's Ethernet interface. However, the combined DECT base station and WLAN access point devices RFP43 and RFP48 use a so-called bridge interface to connect the WLAN to the Ethernet interface.

In some scenarios the supplicant must be bound to the bridge interface and not to the Ethernet interface.

As of SIP-DECT 8.3, there is the system-wide option to connect the supplicant in all connected RFP43 and RFP48 with the bridge interface.

The configuration is available via OMP only.

The screenshot shows the Mitel OMM configuration interface. The left sidebar contains a navigation menu with options like Status, System, SIP, Provisioning, User administration, Data management, Sites, DECT base stations, WLAN, DECT phones, Conference rooms, System features, Licenses, and Support. The main content area is titled 'Configuration' and has tabs for Net parameters, DECT phones, DECT base stations, IMA, Additional services, User service, and Pre-Login banner. Under 'DECT base stations', there are sub-tabs for User monitoring, OMM certificate, 802.1x, and SNMP. The '802.1x' tab is active, showing sections for Certificates/key, PEM file import, Private key password, and General. The 'General' section has a 'Use bridge interface' checkbox, which is currently unchecked. At the bottom, there are 'OK', 'Cancel', and 'Start edit' buttons.

Parameter	802.1x use bridge interface
Description	The parameter determines whether the 802.1x supplicant is bound to the bridge interface of the RFP43 or RFP48.
Format	Boolean

Range	1 or true (enable) 0 or false (disable)
Default value	False
OMP	System/ Advanced settings/ 802.1x/ General
Web	n.a.
OMM configuration files	EventSupplicantCertificateCnf identity="LOCAL" bridgeInterface="true"/>
DECT Phone	n.a.
User configuration files	n.a.

2.55 TLS CIPHER SUITES CONFIGURATION

As of SIP-DECT Release 8.3, the usage of TLS in SIP-DECT has been enhanced to support the following:

- introduction of TLS security levels
- allow to customize the used TLS ciphers suites per security level
- use of intelligent default settings to increase security for new systems and maintain interoperability of legacy systems

2.55.1 TLS SECURITY LEVELS

A system-wide “TLS security level” configuration parameter is introduced for the OMM and MOM. This parameter allows to differentiate between the levels High, Medium and Legacy.

Parameter / Group	TLS security level
Description	The system wide TLS security level used for all TLS connections except 802.1x.
Format	Enumeration
Range	High, Medium, Legacy
Default value	High - when installing a new system Legacy - when upgrading a system with no security level
OMP	System/ Advanced settings/ Security
OMM Web	None
MOM Web	System settings/ Security
OMM configuration files	<SetSystemSecurity securityLevel="High" />
DECT Phone	n.a.
User configuration files	n.a.

This security level will be used for all TLS connections except 802.1x.

To maintain inter-operability with legacy server environments, a different "Security Level" can be configured for SIP and Provisioning. This prevents to use a system-wide low security level for compatibility reasons on specific interface.

Parameter / Group	SIP - TLS security level
Description	The TLS security level used for SIP. When set to Global the system-wide TLS security level will be used
Format	Enumeration
Range	Global, High, Medium, Legacy
Default value	Global
OMP	System/ SIP/ Security
OMM Web	None
MOM Web	n.a.
OMM configuration files	<SetSecureSIP securityLevel="Global" />
DECT Phone	n.a.
User configuration files	n.a.

Parameter / Group	Provisioning - TLS security level
Description	The TLS security level used for Provisioning. When set to Global the system-wide TLS security level will be used
Format	Enumeration
Range	Global, High, Medium, Legacy
Default value	Global
OMP	System/ Provisioning/ General
OMM Web	None
MOM Web	n.a.
OMM configuration files	<SetProvSecurity securityLevel="Global" />
DECT Phone	n.a.
User configuration files	n.a.

The system-wide default value "High" and the Provisioning/SIP specific default value "Global" ensure that the "High" level is used on all TLS interfaces when a new SIP-DECT system is installed.

2.55.2 DEFAULT SETTINGS

When updating a system without security level, the system-wide security level "Legacy" is used to ensure operability. While with a new SIP-DECT installation, the system-wide security level "High" is used to achieve the highest security.

Security level	Default cipher string (OpenSSL notation)
High	TLS_AES_256_GCM_SHA384:TLS_CHACHA20_POLY1305_SHA256:TLS_AES_128_GCM_SHA256:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-CHACHA20-POLY1305:ECDHE-RSA-CHACHA20-POLY1305:DHE-DSS-AES128-GCM-SHA256:DHE-RSA-AES128-GCM-SHA256:DHE-DSS-AES256-GCM-SHA384:DHE-RSA-AES256-GCM-SHA384
Medium	TLS_AES_256_GCM_SHA384:TLS_CHACHA20_POLY1305_SHA256:TLS_AES_128_GCM_SHA256:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-CHACHA20-POLY1305:ECDHE-RSA-CHACHA20-POLY1305:DHE-DSS-AES128-GCM-SHA256:DHE-RSA-AES128-GCM-SHA256:DHE-DSS-AES256-GCM-SHA384:DHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA256:ECDHE-ECDSA-AES256-SHA384:ECDHE-

	RSA-AES256-SHA384:AES128-GCM-SHA256:AES256-GCM-SHA384:AES128-SHA256:AES256-SHA256
Legacy	TLS_AES_256_GCM_SHA384:TLS_CHACHA20_POLY1305_SHA256:TLS_AES_128_GCM_SHA256:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-CHACHA20-POLY1305:ECDHE-RSA-CHACHA20-POLY1305:DHE-DSS-AES128-GCM-SHA256:DHE-RSA-AES128-GCM-SHA256:DHE-DSS-AES256-GCM-SHA384:DHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA256:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SHA384:AES128-GCM-SHA256:AES256-GCM-SHA384:AES128-SHA256:AES256-SHA256:ECDHE-ECDSA-AES128-SHA:ECDHE-RSA-AES128-SHA:ECDHE-ECDSA-AES256-SHA:ECDHE-RSA-AES256-SHA:AES128-SHA:AES256-SHA:DES-CBC3-SHA

Table 1: Default Cipher Strings per Security Level

2.55.3 CUSTOMIZED CIPHER SUITES

The cipher suites of each security level can be customized by specifying an own cipher string. Where each cipher string is a preferred ordered list of cipher names in OpenSSL notation separated by colons.

The cipher strings can be customized via MOM WebUI, OMP (SIP-DECT only) and OMM configuration files.

After modification of such cipher strings the defaults can be restored easily via a default button or selection field.

When the defaults are selected, the used default cipher string is displayed via MOM WebUI and OMP.

Parameter / Group	TLS cipher suites
Description	The TLS cipher suites for a specific security level.
Format	securityLevel: Enumeration (High, Medium, Legacy) useDefault: Boolean when "1" or "True", Mitel's recommended default ciphers will be used and cipherString has no meaning cipherString: String preferred ordered list of cipher names separated by colons for given level
Range	n.a.
Default value	useDefault: True cipherString: <i>see Table 1</i>
OMP	System/ Advanced settings/ Security
OMM Web	None
MOM Web	System settings/ Security
OMM configuration files	<SetCipherSuites securityLevel="High" useDefault="0" cipherString="ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-CHACHA20-POLY1305:ECDHE-RSA-CHACHA20-POLY1305" /> </SetCipherSuites>
DECT Phone	n.a.
User configuration files	n.a.

2.55.4 APPLYING CONFIGURATION CHANGES

Changes to the security level or an actively used cipher list affect the TLS interfaces at different times depending on the application.

While in general the new settings only take effect when a new TLS connection is established, the settings for the SIP interface take effect immediately. As with other configuration changes (e.g. certificates modifications), the SIP interface (OMM/ICS) closes all active TLS connections immediately and re-establish the connections using the new security settings. All users will be new registered at the PBX. This causes an outage of the call control.

On any change in the MOM Web service of the TLS Security Level or the Cipher Suite to the active Security Level in “System setting / Security” tab, the active OMM connections are not changed or interrupted, and the new setting is not applied automatically to not disturb any user or device synchronization or roaming. The security level is expected to have been set during the initial setup of the MOM, before the OMMs are added to the configuration, and not during normal system operation.

During normal operation, the new security setting will be applied to a OMM connection when a connection is re-established. The administrator can decide when a connection reset can be carried out and can manually disable and then enable the connection again for all connections one by one.

2.55.5 RETRIEVING FACTORY DEFAULTS

All changes to the TLS security settings also affect the SIP-DECT configuration interfaces OMM/MOM WebUI, AXI (OMP) and MAXI. In the worst case, this can lead to access becomes impossible if the configuration is incorrect. For example, the configuration tool OMP only supports a certain number of TLS cipher suites (see Table 3).

To be able to switch back the cipher suites settings to the factory defaults in the case of a misconfiguration, the following OMM console command is provided

```
cnf cs reset
```

The MOM offers the following MOM console command to switch back to the factory defaults:

```
mcnf cs reset
```

Warning: All changes to the "Cipher Suites" should only be made after considering all TLS services used including the SIP-DECT configuration interfaces. A previous backup of the configuration is strongly recommended.

Resetting the OMM “Cipher Suites” to factory settings can also be done via the admin menu of subscribed Mitel 600/700 handsets:

1. Long press the menu softkey to open the **System** menu.
2. Select **Administration**.
3. Select **Reset ciphers**.
4. Enter OMM login user name.
5. Enter OMM login password.
6. Click **OK** to confirm reset.

2.55.6 DISPLAYING SUPPORTED CIPHER SUITES

To ease the customization of ciphers for a security level, a list of all supported cipher suites can be retrieved via the MOM WebUI and OMP. The list includes the unique hex code of each cipher suite and the name in OpenSSL notation.

A new XML AXI Request **GetSupportedCiphers** and the associated response allows to retrieve the cipher list via OMP and other AXI clients.

2.56 ENHANCEMENT TO TLS SUPPORT

SIP-DECT supports OpenSSL 3.0.9. With this, SIP-DECT OMM and MOM supports the protocol version 1.3 on all interfaces using TLS, except 802.1x. Notably, the following new cipher suites are supported.

Hex Code	OpenSSL Cipher Suite Name [IANA name]	Security Level
0x13,0x02	TLS_AES_256_GCM_SHA384 [TLS_AES_256_GCM_SHA384]	High
0x13,0x03	TLS_CHACHA20_POLY1305_SHA256 [TLS_CHACHA20_POLY1305_SHA256]	High
0x13,0x01	TLS_AES_128_GCM_SHA256 [TLS_AES_128_GCM_SHA256]	High
0x13,0x05	TLS_AES_128_CCM_8_SHA256 [TLS_AES_128_CCM_8_SHA256]	High
0x13,0x04	TLS_AES_128_CCM_SHA256 [TLS_AES_128_CCM_SHA256]	High

In the OMM settings for loading configuration files from external servers (Provisioning) it is now possible to specify as TLS protocol version the value “TLS1.3”. Following the discontinuation of TLS 1.0/1.1 protocol the “Auto” mode will be redefined to allow automatic negotiation between TLS 1.2 and TLS 1.3.

Parameter / Group	Provisioning - TLS version
Description	The TLS protocol version to use for the configuration file server connection. “Auto” for automatic negotiation between TLS 1.2 – TLS 1.3.
Format	Enumeration
Range	TLS1.2, TLS1.3 , Auto
Default value	Auto
OMP	System/ Provisioning/ General
OMM Web	Advanced: System/ Provisioning & Software Update/ Certificates
MOM Web	n.a.
OMM configuration files	<pre><SetConfigURL> <url enable="1" protocol="HTTPS" host=www.provider.com path="directory" port="999" sslMethod="Auto" validateCerts="1" validateExpires="1" validateHostName="1" importCerts="0" allowNonConfTrustCerts="0" /> </SetConfigURL></pre>
DECT Phone	n.a.
User configuration files	n.a.

To maintain compatibility with legacy call servers, a “TLS version” parameter is added to the SIP settings.

Parameter / Group	SIP - TLS version
Description	The SSL protocol version to use for SIP. “Auto” for automatic negotiation between TLS 1.2 – TLS 1.3.
Format	Enumeration
Range	TLS1.2, TLS1.3 , Auto
Default value	Auto

OMP	System/ SIP/ Security
OMM Web	None
MOM Web	n.a.
OMM configuration files	<SetSecureSIP sslMethod="Auto" />
DECT Phone	n.a.
User configuration files	n.a.

2.57 SECURE LDAP SUPPORT

As of SIP-DECT 8.3, secure LDAP is supported. To enable secure LDAP the new parameter "LDAP security" can be set to "STARTTLS" or "LDAPS" under SYSTEM FEATURES > DIRECTORY MENU.

2.58 NEW OR CHANGED PARAMETERS

2.58.1 PROVISIONING PARAMETERS

2.58.1.1 Order of download and application of files

Parameter / Group	Order of download and application of files
Description	Parameter determines the download and application order of base station software and all other configuration and resource files. This parameter is always set to 1 (Configuration before software) for the Linux server OMM and is read-only on the user interfaces. The Linux server OMM will always run in the "Configuration before software" mode.
Format	Boolean
Range	1 or true (Configuration before software) 0 or false (Software before configuration)
Default value	0 or false
Web	Advanced: Provisioning & Software Update - Order of download and application of files
OMP/AXI	Provisioning / System Update / Update
OMM Configuration files	<SetSystemUpdate updateCfgFirst="1"/>
User data import	N/A
DECT Phone	N/A

2.58.1.2 System Update “On OMM restart”

Parameter / Group	On OMM restart
Description	The parameter determines whether the OMM restart also triggers the reboot/restart trigger and not only the base station reboot. This parameter is not relevant for the Linux server OMM and is not offered on the user interfaces. The restart trigger will always be executed in case of a Linux server OMM restart.
Format	Boolean
Range	1 or true – OMM restart triggers provisioning 0 or false
Default value	1 or true
Web	Advanced: Provisioning & Software Update - On OMM restart
OMP/AXI	Provisioning / System Update / Update
OMM Config. files	<code><SetSystemUpdate onRestart="1"/></code>
User data import	N/A
DECT Phone	N/A

2.58.1.3 Scheduled update

Parameter / Group	System update – scheduled time	
Description	Scheduled time trigger to initiate the provisioning process	
	Time-controlled	Enables/ disables time scheduled trigger
	Time of day	Hour and minutes of the day indicating when to start the provisioning process
	Maximum delay (minutes)	The maximum period for which the start of the provisioning process is randomly delayed
Format	Time-controlled	Boolean
	Time of day	Hour and minutes
	Maximum delay (minutes)	number
Range	Time-controlled	0 or false (off), 1 or true (on)
	Time of day	00:00 – 23:59
	Maximum delay (minutes)	0-1439
Default value	Time-controlled	0 or false (off)
	Time of day	00:00
	Maximum delay (minutes)	0
Web	Advanced: Provisioning & Software Update / System update	
OMP/AXI	Provisioning / System Update / Time-controlled update	
OMM Config. files	<pre><SetSystemUpdate timedUpdate="true" hour="1" minute="30" maxDelay="180" /></pre>	
User data import	N/A	
DECT Phone	N/A	

2.58.1.4 Trigger configuration

Parameter / Group	Trigger Configuration																																
Description	This parameter group decides what actions shall be executed when a specific trigger is received. The settings cannot be changed for an already received trigger. Additionally, the retry behavior is specified for a specific trigger event. <table> <tr> <td>triggerType</td><td>Defines the trigger to be configured</td></tr> <tr> <td>cfgUpdate</td><td>Defines if configuration files are to be processed</td></tr> <tr> <td>swUpdate</td><td>Defines if SW update is to be processed</td></tr> <tr> <td>errWaitTime</td><td>Start value for the retry timer in seconds</td></tr> <tr> <td>retryDelay</td><td>Max additional random value to be added to the retry timer</td></tr> <tr> <td>retryCount</td><td>Max. number of retries</td></tr> <tr> <td>rfpSW</td><td></td></tr> <tr> <td>ommCfg</td><td></td></tr> <tr> <td>imaCfg</td><td></td></tr> <tr> <td>branding</td><td></td></tr> <tr> <td>license</td><td></td></tr> <tr> <td>userCommonCfg</td><td>Defines if a file is mandatory, optional or shall not be downloaded</td></tr> <tr> <td>sipCerts</td><td></td></tr> <tr> <td>provCerts</td><td></td></tr> <tr> <td>webAxiCerts</td><td></td></tr> <tr> <td>wpaCerts</td><td></td></tr> </table>	triggerType	Defines the trigger to be configured	cfgUpdate	Defines if configuration files are to be processed	swUpdate	Defines if SW update is to be processed	errWaitTime	Start value for the retry timer in seconds	retryDelay	Max additional random value to be added to the retry timer	retryCount	Max. number of retries	rfpSW		ommCfg		imaCfg		branding		license		userCommonCfg	Defines if a file is mandatory, optional or shall not be downloaded	sipCerts		provCerts		webAxiCerts		wpaCerts	
triggerType	Defines the trigger to be configured																																
cfgUpdate	Defines if configuration files are to be processed																																
swUpdate	Defines if SW update is to be processed																																
errWaitTime	Start value for the retry timer in seconds																																
retryDelay	Max additional random value to be added to the retry timer																																
retryCount	Max. number of retries																																
rfpSW																																	
ommCfg																																	
imaCfg																																	
branding																																	
license																																	
userCommonCfg	Defines if a file is mandatory, optional or shall not be downloaded																																
sipCerts																																	
provCerts																																	
webAxiCerts																																	
wpaCerts																																	

Parameter / Group	Trigger Configuration	
Format	triggerType	Enumeration
	cfgUpdate	Boolean
	swUpdate	Boolean
	errWaitTime	Integer
	retryDelay	Integer
	retryCount	Integer
	rfpSW	
	ommCfg	
	imaCfg	
	branding	
	license	
	userCommonCfg	Enumeration
	sipCerts	
	provCerts	
	webAxiCerts	
	wpaCerts	
Range	triggerType	Restart, SipNotify, ScheduledUpdate, Manual
	cfgUpdate	1 or true; 0 or false
	swUpdate	1 or true; 0 or false
	errWaitTime	10, 30, 60, 120 and 180
	retryDelay	10, 20 and 30
	retryCount	1,2 or 3
	rfpSW	
	ommCfg	
	imaCfg	
	branding	
	license	
	userCommonCfg	None, Optional, Mandatory
	sipCerts	
	provCerts	
	webAxiCerts	
	wpaCerts	

Parameter / Group	Trigger Configuration	
Default value	triggerType	n/a
	cfgUpdate	true (Restart, ScheduledUpdate, SipNotify); false (Manual)
	swUpdate	true (Restart, ScheduledUpdate, Manual); false (SipNotify)
	errWaitTime	30
	retryDelay	10
	retryCount	1
	rfpSW	Optional (Restart, ScheduledUpdate, Manual); None (SipNotify)
	ommCfg	Optional (Restart, ScheduledUpdate, SipNotify); None (Manual)
	imaCfg	
	branding	
	license	
	userCommonCfg	
	sipCerts	None
	provCerts	
	webAxiCerts	
	wpaCerts	
Web	Provisioning & Software Update / Trigger	
OMP/AXI	Provisioning / Event Trigger	
OMM Config. files	<pre> <SetSystemUpdateTrigger triggerType="Restart" cfgUpdate="true" swUpdate="true" errWaitTime="10" retryDelay="10" retryCount="1" > <files rfpSW="Optional" ommCfg="Mandatory" imaCfg="Optional" branding="Optional" license="None" userCommonCfg="Optional" sipCerts="Optional" provCerts="Optional" webAxiCerts="Optional" wpaCerts="Optional" /> </SetSystemUpdateTrigger> </pre>	
User data import	N/A	

Parameter / Group	Trigger Configuration
DECT Phone	N/A

2.58.1.5 Software activation trigger

Parameter / Group	SW activation trigger
Description	This parameter defines how a new SW shall be activated: automatically after download, time-controlled at a specified point in time or manually. The value which is set when the trigger is received applies and cannot be changed for the trigger.
Format	Enumeration
Range	Automatic, Manual, TimeControlled
Default value	Automatic
Web	Provisioning & Software Update / SW activation
OMP/AXI	Provisioning / System Update / SW activation
OMM Configuration files	<code><SetSystemUpdate swActTrigger="Automatic"/></code>
User data import	N/A
DECT Phone	N/A

2.58.1.6 Software activation time-controlled

Parameter / Group	Software activation time-controlled	
Description	This parameter determines the scheduled time to initiate the software activation if activation trigger is set to "TimeControlled". If there is a random component for the time-controlled system update defined, then the same calculated random component is added to the time set. If the time is before the time-controlled update trigger, then it is applied 24 hours later. Time of day Hour and minutes in the day when to start the software activation	
Format	Time of day	Hour and minutes
Range	Time of day	00:00 – 23:59
Default value	Time of day	00:00
Web	Provisioning & Software Update / SW activation	
OMP/AXI	Provisioning / System Update / SW activation	
OMM Config. files	<pre><SetSystemUpdate swActTrigger="TimeControlled" swActHour="1" swActMinute="30" /></pre>	
User data import	N/A	
DECT Phone	N/A	

2.58.1.7 Software activation “Mode”

Parameter / Group	Software activation mode
Description	This parameter determines how a new SW is activate in the base stations; all base stations in one step (recommended) or one base station at a time and if the base station is in idle (no active call) and no active call in the system for OMM base station.
Format	Boolean
Range	1 or true – “All at once” 0 or false – “One by one”
Default value	1 or true
Web	Advanced: Provisioning & Software Update / Software activation / mode
OMP/AXI	Provisioning / System Update / Software activation
OMM Configuration files	<SetSystemUpdate swActAllAtOnce="1" />
User data import	N/A
DECT Phone	N/A

In SIP-DECT Release 8.1 and earlier, the default value for the update mode was “One by one”. Due to the new update

mechanisms the default is now “All at once”. “One by one” is recommended only for larger installations having a standby OMM and demanding a high availability. Without a standby OMM, the “One by one” mode does not provide a specific advantage except “one by one” checks for base station and system idle (no active calls).

2.58.1.8 One by One software activation time out

Parameter / Group	One-by-one software activation time out	
Description	This parameter determines the time by when the software activation should be completed and if not, then the activation shall be completed immediately in all-at-once mode without an idle check of the system or base station. If there is a random component defined for the time-controlled system update, then the same calculated random component is added to the time set. If the time out is before the activation time, then it applies 24 hours later. One-by-one activation timeout Enables or disables activation time out Time of day Hour and minutes of the day to start the software activation	
Format	One-by-one activation timeout	Boolean
	Time of day	Hour and minutes
Range	One-by-one activation timeout	0 or false (off), 1 or true (on)
	Time of day	00:00 – 23:59
Default value	One-by-one activation timeout	0 or false (off)
	Time of day	00:00
Web	Provisioning & Software Update / SW activation	
OMP/AXI	Provisioning / System Update / SW activation	
OMM Configuration files	<pre><SetSystemUpdate swActTimeout="false" swActTimeoutHour="0" swActTimeoutMinute="0" /></pre>	
User data import	N/A	
DECT Phone	N/A	

2.58.2 RTP SOURCE PORT FILTER

In special environments it can happen that the RTP media stream is not switched off although the opposite side has been taken on hold. In this case, audio interference may occur when another call is established, and two media streams are received from SIP-DECT from the same IP address.

As of version 8.3SP1, an RTP source port filter is now supported to avoid such audio interference.

Parameter	RTP source port filter
Description	The parameter determines whether RTP packets from unknown source ports are filtered out. If activated, SIP-DECT checks the source port in addition to the source IP address when receiving RTP packets.

	If one of the parameters does not match the signaled data, the packets are ignored.
Format	Boolean
Range	1 or true (enable) 0 or false (disable)
Default value	False
OMP	System/ SIP/ RTP settings
Web	Advanced: System/ SIP/ RTP settings
OMM configuration files	<SetRTP sourcePortFilter="1" />
DECT Phone	n.a.
User configuration files	n.a.

The screenshot shows the Mitel SIP settings interface. The 'RTP settings' tab is selected under 'Advanced settings'. The 'Source port filter' checkbox is checked and highlighted with a red rectangle. Other settings include RTP port base (16320), Preferred codec 1 (G.722), Preferred codec 2 (G.711-u-law), Preferred codec 3 (G.711-A-law), Preferred codec 4 (G.729-A), Preferred packet time (20 msec), Silence suppression, Receiver precedence on codec negotiation, Eliminate comfort noise packets, and Single codec reply in SDP.

2.58.3 SIP RE-REGISTER ON TLS RECONNECTS

On some PBX platforms it is necessary to renew the SIP registrations when a "persistent" TLS connection goes down and is re-established. As of version 8.3SP1, the new configuration parameter allows to enable re-registrations on reconnects.

Parameter	Re-register on reconnect
Description	This parameter determines whether the SIP registration will be refreshed when a persistent TLS connection is re-established after dropping. If activated, the SIP registration will be refreshed after re-connection.
Format	Boolean
Range	1 or true (enable) 0 or false (disable)

Default value	False
OMP	System/ SIP/ Security
Web	n.a.
OMM configuration files	<SetSecureSIP reRegisterOnReconnect="0"/>
DECT Phone	n.a.
User configuration files	n.a.

The screenshot shows the Mitel configuration interface. The 'Security' tab is selected, and the 'General' section is visible. The 'Re-register on reconnect' checkbox is checked and highlighted with a red box. Other settings include 'Persistent TLS keep alive timer active' (checked), 'Validate certificates' (unchecked), 'Send SIPs over TLS active' (checked), 'Security level' (Global), 'Private key password' (masked), and 'Password confirmation' (masked). The 'OK' and 'Cancel' buttons are at the bottom.

2.59 USER DATA IMPORT

The "User data import" function is a special provision function with deviating rules and mechanisms (for example, the point in time at which user.cfg files are requested depends on the user actions of the DECT telephone). However, the changes to the SIP-DECT provision feature described in this document also have a corresponding effect on the "User data import" function.

2.59.1 USER_COMMON.CFG

As of SIP-DECT 8.3, the general provision rules described in this document apply to the user_common.cfg file. The file is retrieved as configured.

M = Mandatory; **O** = Optional; files marked with "-" are not downloaded.

	Manual trigger	RFP / OMM (re)start	SIP Notify	Scheduled update
Configuration	☒	☒	☒	☒
User data	O	O	O	O

Therefore, the parameter UDS_CommonUpdateInterval, which defines the interval for re-importing the file user_common.cfg, is no longer supported.

As in previous releases, and unlike to other files, the OMM tries to get the user_common.cfg from the provisioning URL and, if configured, from the resource-specific URL. If the file exists in both sources, then the file from the specific URL is used.

A successful download and application of the user_common.cfg is not mandatory for a successful user login. If the user_common.cfg is not available at login then the available data are used.

2.59.2 <USER>.CFG

The user login is the initial trigger to download and apply a specific <user>.cfg file.

If a user has been created in the OMM by importing a <user>.cfg ,then the file is re-fetched by the OMM at the following occasions:

- RFP/OMM (re)start
- SIP-Notify event “check-sync” (instead of “prov-sync” and ”resync”)
- Scheduled update
- DECT phone menu “System menu”/”Administration”/”Sync user data”

A manual trigger does not force the re-fetching of <user>.cfg files.

The parameter UD_UpdateInterval is no longer supported. The interval to re import user data files is defined by the scheduled update configuration.

2.59.3 MIGRATION FROM PREVIOUS RELEASES:

If the OMM database contains user data that was created by the user data import or the specific user data import URL is active, the user data import is automatically set to optional for the following trigger:

- RFP/OMM (re)start
- SIP-Notify event “check-sync” (instead of “prov-sync” and ”resync”)

2.60 UPDATING SOFTWARE

The software update process for base stations has been extensively modified to achieve a widely manageable, predictable, and reliable software update behavior.

The update process of all base stations belonging to the same system is centrally managed by the OMM. Base stations no longer try to download and activate a new software by their own logic. There is only one exception: if a base station can establish a connection to OMM but communication fails (incompatible protocol version), then the base station downloads and activates a new software on its own.

The OMM standby/resiliency concept is supported. As an improvement, a second failover is no longer necessary during a software update in such an environment.

The update process consists of two separate steps managed by OMM with separate control mechanisms and configuration options:

1. Download of software and distribution to all the base stations of a system.
2. Activation of a new or different software for all base stations, either immediately after software distribution to all base stations or at a later time.

The OMM standby/resiliency concept is supported. As an improvement, a second failover is no longer necessary during a software update in such an environment.

The update process includes the update of OMM if it is running on a base station.

Note on systems operated by a 3rd generation base station (RFP35, RFP43) operating as OMM:

A 3rd generation base station cannot handle software container for 4th generation base stations (RFP44, RFP45, RFP47, RFP48). If the system operates at least one 4th generation base station, the OMM must be hosted by a 4th generation base station.

Software for 3rd generation base station is included in the software update container for 4th generation base station and will be extracted and distributed during the update process.

2.60.1 DOWNLOAD AND DISTRIBUTION OF BASE STATION SOFTWARE

A new base station software container file placed on an external server will be downloaded only once by the OMM base station or by a base station selected by OMM for PC OMM systems (Master base station). The server address/URL and the protocol to be used for download are configurable via service GUIs (Web service/OMP) or provisioning methods supported by OMM.

There is no need any more to configure a software update URL via DHCP, OM configurator or RFP configuration files. Although such configuration methods are still supported by SIP-DECT Release 8.3 for compatibility reasons, it is recommended to use the software update/provisioning configuration method in the service GUIs or provisioning itself for configuration.

If the OMM base station has a low bandwidth or high error rate on the network connection to the server hosting the software container file, then the maximum time after which the download is considered as failed has been extended to 4 hours.

After successful download of the file to the OMM/Master base station, the file is distributed to all base stations of the system by a transfer mechanism implemented in all base stations and controlled by OMM.

If a base station has received the new file other base stations will be requested by OMM to load the file from this base station taking the conditions listed below into account. This ensures a fast distribution of a new software in larger installations.

- A maximum of three parallel transfers to different base stations will be active at a time per base station acting as a server.
- Transfer of software file between base stations is limited to transfers between base stations belonging to same DECT cluster whenever possible. It is assumed that base stations belonging to same DECT cluster are belonging to same network region/segment allowing for high transfer speed.

There will be transfers of software file from OMM/Master base station to arbitrary base stations of each cluster in order to get the software file initial into each cluster.

Base stations configured as 'DECT inactive' won't follow the rule described above.

- In order not to overload local network during distribution of software a maximum of 21 transfers per DECT cluster at a time will be active.

On LAN with normal performance ($\geq 100\text{Mbit/s}$) transfer of the software container file between the OMM base station and another base station normally takes about 1 to 2 minutes for each base station.

Progress of distribution can be monitored on Web service or OMP. A transition to the activation phase is possible only if the software container file is distributed to all base stations that are connected to the OMM.

Note: A new firmware is only downloaded but not activated during this phase. No functionality of the current running software is affected by the download and distribution

2.60.2 ACTIVATION OF NEW BASE STATION SOFTWARE

Activation of a new software is also controlled by the OMM. Before Activation can begin, the download and distribution phase must be completed, and the new software to be activated must be ready to be started in all base stations connected to the OMM.

There are various options to start switchover to the new software:

- Manually
- Automatically immediately after the download and distribution phase has successfully ended
- Automatically at a configured time of day

There are two different activation modes that can be selected by configuration:

1. “All at Once”: All base station connected to the OMM and the base station hosting the OMM itself will be restarted with the new software at the same time. This way of restart is most predictable and quite fast but causes a short interruption in providing the DECT service to handsets. “All at Once” is the recommended method for activation in most cases and the new default preset with systems on which SIP-DECT 8.3 is installed.
For PC OMM systems follow the steps described in next section.

2. “One by One”: Only one DECT active base station per cluster gets restarted at a time. The system will provide DECT services via other base stations to the handsets during the time when the base station restarts. So possible impairment of DECT services depends on radio signal coverage on the systems location.

The next base station of a cluster will be scheduled for restart after a restarted base station has synchronized its air interface with the system again.

DECT inactive base stations and base stations that connected (or reconnected) to OMM due to any external reason will restart immediately if new firmware is present on these base stations.

A base station is only restarted if there is no active call on the base station (Idle check). In case there is no other base station without a call which could be restarted, an Idle check is done periodically on remaining base stations.

For systems running the OMM on a base station the OMM base station is restarted at the last and restart is done only if there is no active call in the system. For PC OMM systems the OMM has to be updated and restarted manually following the guidelines in next section.

If active calls prevent the restart for a configurable time the system is restarted in “All at Once” regardless of existing active calls.

If there is a Standby-OMM, the activation process includes a failover to the Standby-OMM when the active OMM restarts with new software. In case the Standby-OMM is running on a base station it will be restarted first during a “One by One” activation. In case of a failover during the restart phase, the already restarted Standby OMM will switchover all connected base stations of the system immediately to new software if not already done.

If the system is operated without a Standby OMM base station, a short service interruption during restart of OMM base station will occur with similar length than on “All at Once” activation. Therefore, it is strongly recommended to configure “All at Once” restart for such systems.

“One by One” activation is possible only if the version of the communication protocol between OMM and base stations is the same for current and new software. If the protocol version is different, then this will be detected by OMM and an “All at Once” restart will be executed automatically instead.

2.60.3 UPDATING PC OMM

Updating a PC OMM system is not as simple as updating a system controlled by a OMM base station. This is caused by the fact that OMM software running on PC has to be deployed in different way than software running on a base station.

As the software update of a PC OMM is a manual process the automatic and time controlled restart options for the base station update should normally not be used on PC OMM.

It is recommended to follow the steps below:

1. Upload base station software container iprfp3G.dnld, iprfp4G.dnld (depending on which type of base stations are installed) to file server configured in OMM as software update URL or provisioning URL.
2. Start software download/distribution by pressing button <Update> in OMM management GUI (Web service or OMP)
3. Wait until software distribution has finished (all base stations have received the new software)
4. If running with a standby OMM install and start new OMM software on standby OMM PC.

5. Activate new Software in all base stations by pressing button <Activate> in OMM management GUI (Web service or OMP).
6. Install and start new OMM software on PC running the currently active OMM.

The base stations will connect to the already updated standby OMM (or reconnect to the actual OMM if no standby OMM is running) and software update is finished.

Please note: Updating the PC OMM before a new software is distributed to all base stations and started should be avoided. Doing so in case the communication protocol version has changed between old and new software version will result in uncoordinated attempts to load the software by all base stations.

2.61 ENHANCEMENT TO PROVISIONING

As of SIP-DECT Release 8.3, the SIP-DECT provisioning feature, that is, the configuration and the SW update of SIP-DECT via configuration and resource files have been enhanced to support the following:

- a consistent, deterministic, predictable, and manageable behavior of resource download and application
- slow SW downloads to RFPs, for example, over low-bandwidth connections
- Update many base stations without the need for high capacity file servers

This has been achieved by the following means:

- only specific triggers initiate the provisioning
- configurable behavior for each trigger
- only OMM base station downloads files from the external server
- SW distribution only from OMM base station to other RFPs belonging to the installation
- activation of new SW managed by OMM

Please note: Because of the changes implemented, an OMM running on a 3rd generation base station such as RFP35 can manage only 3rd generation base stations. If a 4th generation base station such as RFP45 is being operated, then that base station must house the OMM.

2.61.1.1 Resource and configuration files supported by provisioning

The following table provides an overview of the supported files, dependencies on SIP-DECT mode, standard mode, and SIP-DECT with Cloud-ID mode, and the support for resource-specific URLs and the options for configuring them with regards to provisioning. Note that exceptions marked with an “N” – indicating “not supported”.

Resource Type	Files / file name	SIP-DECT mode		Fixed File Name	Supported URLs		Specific URL config		
		Std	SDC		Prov.	Res.-specific			
							Web	OMP*	OMM cnf. file

OMM config.	ipdect.cfg, <Cloud-ID>.cfg, <mac>.cfg	Y	Y	Y	Y	N	n.a.		
RFP Software	iprfp3G.dnld or iprfp4G.dnld	Y	Y	Y	Y	Y	Y	Y	Y
IMA config.	ima.cfg	Y	Y	Y	Y	Y	Y	Y	Y
Branding image	customer_image.png	Y	Y	Y	Y	Y	N	Y	Y
License**	license.xml	Y	N	Y	Y	N	n.a.		
User data	user_common.cfg, <user>.cfg	Y	Y	Y	Y	Y	Y	Y	Y
Certificates (Prov., Web/AXI, SIP, 802.1x)	local certificate, private key, trusted certificates	Y	Y	N	N	Y	N	Y	Y

* OMP is not supported in SIP-DECT with Cloud-ID mode.

** The application of a license file has only an effect in the standard SIP-DECT mode and not in SDC mode.

Resource and configuration files supported Provisioning URL in setups using DHCP

2.61.1.2 Supported provisioning triggers

To initiate the download and application procedure, four specific triggers are supported:

- Manual
- reboot/OMM restart
- time-controlled
- SIP notify

Additionally, a user login triggers the OMM to fetch the corresponding<user.cfg>.

OMM restart is a variant of the base station reboot trigger. These were already available in earlier releases. Other events no longer trigger an update procedure, to create a deterministic and predictable behavior. See the following table.

Trigger to initiate file updates	Supported by 8.1 or earlier	Supported by 8.3 or later
Manually via GUI (Web, OMP)	Yes	Yes*
Time-controlled (one point in the day)	Yes, for specific setups only	Yes*
SIP notify ("prov-sync" and "resync")	Yes, for specific setups only	Yes*
Base station reboot	Yes	Yes*
OMM application restart	Yes	Yes*
User login (<user>.cfg only)	Yes	Yes*

Trigger to initiate file updates	Supported by 8.1 or earlier	Supported by 8.3 or later
SIP notify ("check-sync", <user>.cfg only)	Yes	Yes
Configuration changes of related data (if they do not cause a restart)	Yes	No
DHCP renew	Yes, but could be disabled for specific setups	No
Base station loses connection to OMM (RFP requests SW from server)	Yes	No
Time controlled RFP configuration file reload	Yes	No
Various operation failure scenarios	Yes	No

* Configurable – As of SIP-DECT Release 8.3, there are several configurable parameters for each supported trigger.

Updated configuration will be used with the next trigger, for example, manually via the GUI.

User data import does not trigger any provisioning action outside of user data import.

As of SIP-DECT Release 8.3, the change of provisioning related configurations does not trigger the provisioning process in this release. However, it is required to support staging. Therefore, a change in the provisioning URL or SW update URL and related data such as login, password and so on during the update process re-triggers the provisioning update. A change of other specific source URL parameter does not re-trigger the download of the specific resource.

Following is the order of the events:

0. Initial trigger
1. Download all mandatory files successfully
2. Apply configuration files and if available, update to new SW*. The order can be configured.
3. If there is a change of URLs, and so on but no SW update*, then revert to 1 (process the same trigger but modified URLs).

* A SW update causes a reboot and therefore triggers provisioning (reboot trigger), that is, it can trigger an update of configuration files. This also applies to the scenario in which a new SW is required to apply a new configuration.

If relevant configuration changes do not occur in the context of an ongoing provisioning process, then these changes do not trigger any provisioning action.

Please note: The system detects that the current trigger initiates a provisioning staging (complete the current actions and re-trigger the process with changed provisioning / SW update URL) since a relevant parameter change occurs in context of the current provisioning step. The parameter change could also be caused by other reasons but result in the same behavior. However, this is not relevant for actual use cases, as there is no parallel trigger processing.

A staging process can only be initiated and further processed based on the trigger type (manually, reboot/restart, time-controlled, SIP notify), that is, the trigger that initiates the process will be automatically processed in the next step. As the staging process can be interrupted by SW update reboot or OMM restart, the reboot / OMM restart trigger is the only trigger that can be used for fail-safe automatic staging.

If a SW update is required in context of a provisioning staging, the SW will be automatically activated in all base stations in one step to complete this step as quickly as possible. Manual or time-controlled activation as well as the activation mode “one by one” is ignored.

2.61.1.3 Order of software and configuration files

For additional control over the staging process, there is the option to determine the order of download and application of SW versus configuration and other resource files. This allows updating to a new SW before a configuration is applied. The configured order applies to the provisioning process regardless of the initiating trigger.

Initially, the order is set to “SW before Configuration” to ensure that the SW updates to the required version in the first provisioning steps. This makes a provisioning staging fail-safe because the system remains at a specific stage until the SW is updated.

If “SW before Configuration” is set and a SW update is in progress, no further trigger is processed, that is, the configuration cannot be changed by provisioning means. Therefore “SW before Configuration” is not recommended for the standard operational mode. To execute the SW update as quickly as possible in the “SW before Configuration” mode, the SW will be automatically activated in all base stations in one step. Manual or time-controlled activation as well as the activation mode “one-by-one” is ignored.

The system switches automatically to “Configuration before SW” when a PARK is set (fetched from the server or via license file) or a Cloud-ID key is applied, because this indicated that the system is put in the operational mode. This avoids the need to explicitly change the mode from “SW before Configuration” to “Configuration before SW”.

The update process of all base stations belonging to the same system is centrally managed by the OMM. Base stations no longer try to download and activate a new software. There is only one exception: if a base station can establish a connection to OMM but communication fails (incompatible protocol version), then the base station downloads and activates a new software on its own.

The update process consists of two separate steps managed by OMM with separate control mechanisms and configuration options:

1. Download of software and distribution to all the base stations of a system.
2. Activation of a new or different software for all base stations, either immediately after software distribution to all base stations or at a later time.

The OMM standby/resiliency concept is supported. As an improvement, a second failover is no longer necessary during a software update in such an environment.

The update process includes the update of OMM if it is running on a base station.

Please note: A 3rd generation base station cannot handle software container for 4th generation base stations (RFP44, RFP45, RFP47, RFP48). If the system operates at least one 4th generation base station, the OMM must be hosted by a 4th generation base station. Software for 3rd generation base station is included in the software update container for 4th generation base station and will be extracted and distributed during the update process.

2.61.1.4 File download from external server

Only the OMM (OMM base station) downloads SW and configuration files from an external server to which the current provisioning URL or specific resource URLs refer to. The SW or the configuration files are downloaded and applied according to the setting “Order of SW and configuration files”. The configuration files are first downloaded and then applied according to the trigger configuration. The order of the file download and application corresponds to the order of configuration files displayed in the GUIs.

If a problem occurs, then download retries are handled according to the trigger configuration.

If a file download is finally unsuccessful, then the next attempt to download a resource is initiated with the next trigger.

Please note: If a server response indicates that the requested file does not exist, then there will be no download retry attempt to avoid unnecessary traffic. The file will be requested with the next provisioning cycle. This applies to configuration files only and not to SW.

If a server is not reachable within 30 seconds, then the connection attempt to that server is terminated.

2.61.1.5 Abort button

It is possible to manually cancel the provisioning processes with the Abort button that is available via OMM Web service and OMP. The abort stops all activities in progress and removes all queued triggers except the activation of SW and the application of configuration files.

The screenshot shows the 'Configuration' page with a sidebar on the left containing links like 'Status', 'System', 'Basic settings', 'Advanced settings', 'SIP', 'Provisioning', 'User administration', 'Data management', 'Maintenance', and 'Sites'. The main content area is titled 'System update' and contains several tabs: 'Branding image URL', 'System credentials', 'Event trigger', 'User data import', 'Software update URL', 'IMA', 'General', 'System update' (selected), 'Provisioning certificates', and 'Provisioning certificate server'. Under the 'System update' tab, there are two main sections. The first section, 'Update', has a dropdown menu for 'Download order' set to 'Configuration before software' and a checked checkbox for 'Update on OMM restart'. It includes an 'Update' button and an 'Abort' button (highlighted with a red rectangle). The second section, 'Time-controlled update', has a checked checkbox for 'Active', a 'Time of day' picker set to '00 : 00', and a 'Maximum delay' picker set to '0 min'. It also includes a 'Calculated time of day' picker set to '00 : 00'.

The Abort button is mainly used to cancel activities that were started manually but with incorrect parameters and should be restarted after the correction. The Abort process can take a considerable amount of time to process. Check the progress in the Status page.

2.62 RFP ENROLMENT ENCRYPTION WITH AUTHENTICATION KEY

During RFP enrolment, an RFP-specific random authentication key is exchanged between OMM and the RFP used for authentication and encryption.

The enrolment of RFPs comprises following steps:

- Add RFP to OMM database (create a DB entry for the RFP)
- Establish first connection between the RFP and OMM

It is a precondition that the enrolment of the RFP takes place in a safe environment. That is, the installer ensures that the exchange of the authentication key between the RFP and OMM during enrolment cannot be compromised: for example, no man-in-the-middle attack possible or no RFP tampering occurs.

Note: The key exchange is automatically executed when upgrading or updating to 8.1SP1.

To successfully enroll an RFP, the RFP must not have an authentication key from previous enrolments. An existing authentication key can be removed from an RFP by a reset to factory defaults. To remove an existing key for an RFP from the OMM, the RFP must be removed from the OMM DB.

If an RFP is removed from the OMM DB and then connected to the OMM, the authentication key is also automatically removed from the RFP. The RFP can be enrolled on this or another OMM without a reset to factory defaults.

2.62.1 RFP CONNECTION STATUS IN OMM: ENCRYPTION ACTIVATED

The administration interfaces of the OMM show the RFP connection status. The intermediate state between disconnected and successful connection (encrypted) is called “encryption activated” state. This intermediate state is indicated by a key icon  in the connection state column. This status is usually short-lived and therefore not easily noticeable. However, if there is an encryption issue, then the successful connection state, indicated by a green checkmark , cannot be reached and “encryption activated” state will last for approximately 20 seconds and switches to disconnected (Web: , OMP: ) periodically.

ID	Name	MAC address	IP address	HW type	RPN	Connected	Active
0000	OMM RFP	08:00:0F:C3:DF:0A	10.103.35.162	RFP 47	00		
0001	RFP 4x 2nd	08:00:0F:C3:DE:FD	10.103.35.123	RFP 47	01		–
0002	RFP32	00:30:42:12:33:16	10.103.35.239	RFP 32	02		
0003	RFP43 / 3X	00:30:42:17:8E:3E	10.103.35.172	RFP 43	03		

Encryption activated state displayed by Web UI

2.62.2 RE-ENROLMENT FUNCTION

The re-enrolment function can be used to address authentication key issues between OMM and RFP if the RFP was already enrolled in the OMM and encrypted communication was already in place before. Note that this function can help resolve only specific scenarios.

If re-enrolment is activated for an RFP, then the OMM sends an encrypted message (AES-256) to the RFP with the next connection attempt of the RFP. This message is validated by the RFP to ensure that the OMM is the sender (SHA-2, SHA256). The RFP can decrypt and validate the message only if the RFP has the same root credentials as the OMM (exchanged during earlier encrypted communication). The message provides a new authentication key to the RFP. The RFP uses the new authentication key for subsequent encryption of traffic.

See the following table for details about the re-enrolment function available through OMP and OMM Web UI.

Mitel  										General Help
Configuration	RFP ID	Name	MAC address	IP address	DECT cluster	HW type	Connection state	Active	Tasks	
Status	☐ 0x000	OMM RFP	08:00:0F:C3:DF:0A	10.103.35.162	1	RFP 47			Create Configure Delete Re-enrollment  Filter Select columns	
System	☒ 0x001	RFP 4x 2nd	08:00:0F:C3:DE:FD	10.103.35.123	1	RFP 47				
Sites	☐ 0x002	RFP32	00:30:42:12:33:16	10.103.35.239	1	RFP 32				
DECT base stations	☐ 0x003	RFP43 / 3X	00:30:42:17:8E:3E	10.103.35.172	1	RFP 43				

Re-enrolment via OMP

Configure base station

Re-enrolment

General settings

MAC address: 08:00:0F:C3:DE:FD

Name: RFP 4x 2nd

☐ **WLAN settings**

WLAN profile: 0

802.11 channel:

Output power level: Full

OK Cancel

Re-enrolment feature in the Configure Base Station dialog box of the Web user interface

To initiate the re-enrolment, select the RFP and press **Re-enrolment**. This action is ignored for successful connected RFPs.

2.62.3 SWITCH BETWEEN SOFTWARE VERSIONS THAT SUPPORT AND DO NOT SUPPORT AUTHENTICATION KEYS

Switching between software versions that support and do not support authentication keys causes a loss of keys in OMM. For all updates/upgrades to software with authentication key support, apply the OMM DB backup with the latest RFP authentication keys. RFPs cannot connect to the OMM if the RFPs have a key and the OMM does not, as shown in the following screen shot.

ID	Name	MAC address	IP address	HW type	RPN	Connected	Active
0000	OMM RFP	08:00:0F:C3:DF:0A	10.103.35.162	RFP 47	00	✓	✓
0001	RFP 4x 2nd	08:00:0F:C3:DE:FD	10.103.35.123	RFP 47	01	✗	–
0002	RFP32	00:30:42:12:33:16	10.103.35.239	RFP 32	02	✗	–
0003	RFP43 / 3X	00:30:42:17:8E:3E	10.103.35.172	RFP 43	03	✗	–

RFPs cannot connect because keys do not match

The event log messages provide further details of the connection failure.

Severity	Count	Time (UTC)	Event
3	1	2019/12/20 13:14:59.183	IPL : RFP(0001) disconnected, might have different encryption keys => try re-enrolment
3	1	2019/12/20 13:14:51.427	IPL : RFP(0003) reconnected
3	1	2019/12/20 13:14:49.402	IPL : RFP(0003) disconnected, might have different encryption keys => try re-enrolment
3	1	2019/12/20 13:14:40.437	IPL : RFP(0002) reconnected
3	1	2019/12/20 13:14:38.406	IPL : RFP(0002) disconnected, might have different encryption keys => try re-enrolment
3	1	2019/12/20 13:14:36.674	IPL : RFP(0001) reconnected
3	1	2019/12/20 13:14:34.662	IPL : RFP(0001) disconnected, might have different encryption keys => try re-enrolment
3	1	2019/12/20 13:14:26.895	IPL : RFP(0003) reconnected
3	1	2019/12/20 13:14:24.870	IPL : RFP(0003) disconnected, might have different encryption keys => try re-enrolment
3	1	2019/12/20 13:14:15.881	IPL : RFP(0002) reconnected

Event log messages if RFPs and OMM keys do not match

The problem is resolved on applying the correct OMM DB with the latest keys. Re-enrolment can be an alternative if the root credentials do not differ between RFPs and OMM.

	ID	Name	MAC address	IP address	HW type	RPN	Connected	Active
 	0000	OMM RFP	08:00:0F:C3:DF:0A	10.103.35.162	RFP 47	00	✓	✓
 	0001	RFP 4x 2nd	08:00:0F:C3:DE:FD	10.103.35.123	RFP 47	01	✓	✓
 	0002	RFP32	00:30:42:12:33:16	10.103.35.239	RFP 32	02	✓	✓
 	0003	RFP43 / 3X	00:30:42:17:8E:3E	10.103.35.172	RFP 43	03	✓	✓

RFPs are re-connected on applying an OMM DB with a matching key

2.62.4 AUTHENTICATION KEY MISMATCH SCENARIOS

There are various scenarios that can cause a key mismatch between RFP and OMM. In general, a mismatch is resolved after a factory reset of the RFP and deleting and re-creating the RFP in the OMM DB. This works for many scenarios and when the number of RFPs is small. In some scenarios, a mismatch occurs for many or all RFPs in one installation. To address such scenarios, a specific re-enrolment mechanism is available.

Note: The re-enrolment function will only work if root credentials match between OMM and RFP. It does not work, for example, if an RFP is moved to a different SIP-DECT installation, with different root credentials.

The following table lists various scenarios, how they can occur, and how they must be addressed.

Scenario	Causes (always based on a previous successful enrolment)	Comments	Default procedure	Alternative
OMM uses authentication key, but there is no in RFP	Factory reset of RFP	There can be no conflict for RFPs on which the OMM is running (both on the same device).	Delete and recreate RFP in OMM DB. (licensed RFPs cannot be deleted in OMM)	Delete authentication key in OMM using the OMM cnf console command "akd".
RFP uses an authentication key, but RFP is not enrolled in OMM	• SW down/upgrade (partially Loss OMM DB data); • Deletion and recreation of RFP in OMM DB (if RFP is not connected with OMM) • Applying a DB backup to OMM with outdated RFP data • OMM failover during key exchange • Discarding OM DB • RFP moved to another OMM/SIP-DECT installation	Keys are automatically removed from an RFP if the RFP is re-connected (encrypted connection in place) with an OMM after being deleted from the OMM. There can be no conflict for RFPs on which the OMM is running (both on the same device).	Factory reset all affected RFPs and re-enroll RFPs; if necessary, delete RFPs in OMM and re-enroll.	Re-enrolment function (if RFP was already connected with OMM and has the same root credentials -locally stored)
RFP and OMM are using different keys	Apply a DB backup to OMM with outdated RFP data*.		Factory reset of all affected RFPs, delete RFPs in OMM and enroll again.	Re-enrolment function (if RFP was already connected with OMM and has the same root credentials -locally stored)

***Example scenario:**

RFP OMM Standby configuration; OMM DB reset on OMM1; failover to OMM 2; automatic enrolment of RFP part of active OMM 2 (new authentication key); apply OMM DB backup; failover to OMM 1; mismatch of authentication keys in OMM 1 (old key) and RFP of OMM 2 (new key);

Solution: automatically corrected with the next failover to OMM 2 or use re-enrolment.

2.62.5 SUPPORT AND MAINTENANCE

To delete an authentication key in OMM, use the OMM cnf console command “akd”.

```
cnf rfp akd <dez RFP ID>
```

Note: An operational RFP goes out of operation if the authentication key is deleted from the OMM.

To trigger the re-enrolment, use the OMM cnf console command “ren”.

```
cnf rfp ren <dez RFP ID>
```

2.63 DISTINCTIVE RINGTONE

The OMM determines the call type in two ways based on either of the following:

- SIP header **Alert-Info** – The call type information in the Alert-Info is sent from the SIP proxy.
- Number of digits in the calling party’s number – The call type of the internal and external calls can be set by configuring the **Maximal digits of internal call number** parameter.

The call server string attached to the Alert-Info that is assigned to a particular call type in the OMP distinguishes the call type of a call as one of the following type:

- Internal
- External
- Emergency
- VIP
- Callback

The following table summarizes the call alert feature support for Mitel DECT phones and third-party GAP phones.

DECT phone Call types	Mitel 600/700	Mitel 142d	Mitel 56xx/DTxx	GAP
Internal	yes	yes	yes	yes
External	yes	yes	yes ¹	yes ¹
Call back	yes	yes	yes ¹	no
Emergency	yes	yes	no	no
VIP	yes	yes	no	no

- ¹ All call types other than internal will ring with the ringtone set for external calls; except for Emergency/SOS calls, which will ring with callback ringtone.

For details about setting a call server string to a call type and configure the length of the internal call phone number, see section 7.7.4.8.

2.64 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, ipdetect.cfg, <MAC>.cfg) happens.

2.65 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 for example, text messaging.

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

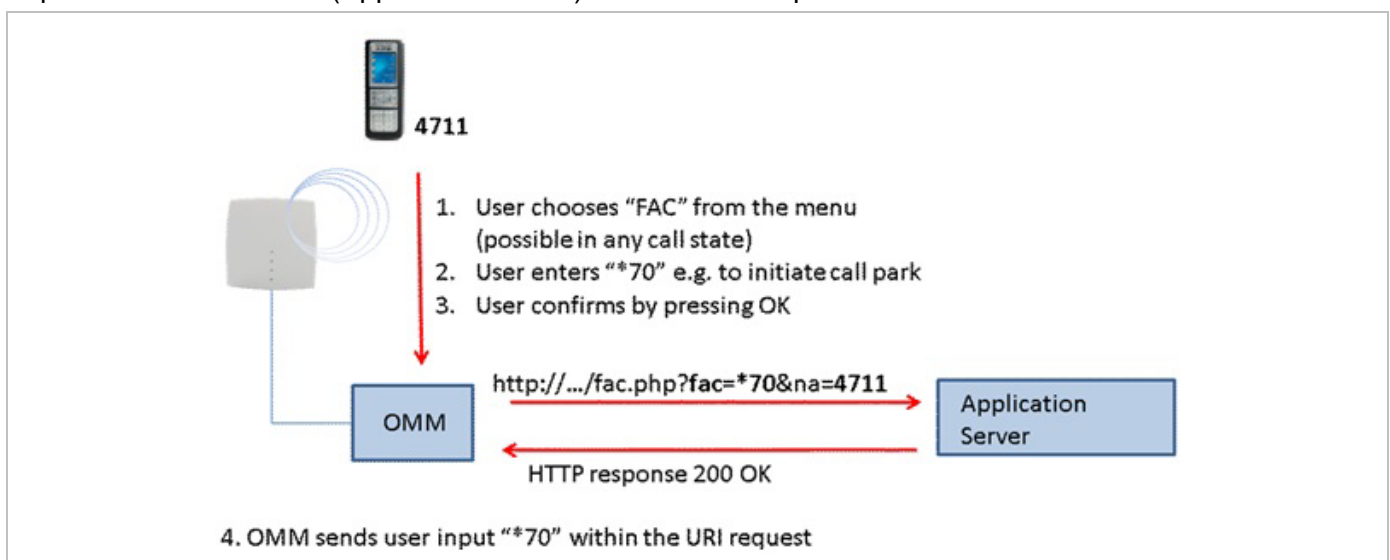
To call a certain URI, there are a number of hooks available for the Mitel 600/700 DECT phones which can be put on a programmable key or can be called from a menu. You can activate the predefined XML hooks via the OMM Web service (see section [6.9.5](#)) or the OMP (see section [7.13.8](#)).

You can also activate the XML hooks through the Configuration over Air (CoA) feature, see section [9.22](#) 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).

2.65.1 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 600/700 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 [7.13.8](#)).

2.65.2 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.

2.65.3 DECT PHONE CHARGER EVENTS

SIP-DECT supports DECT Phone charger events to be signaled via AXI and the XML Action URI application hook.

In the AXI EventPPState, the following two related state information is provided.

Parameter	Description
isUsbConnected	“1” or “true” if the DECT phone is connected to USB; else “0” or “false”.
isInCharger	“1” or “true” if the DECT phone is in charger; else “0” or “false”.

Examples of AXI Events	Description
<EventPPState ppn="1" ppnHex="0x1" isInCharger="0" isUsbConnected="0"/>	Not in charger; USB not connected
<EventPPState ppn="1" ppnHex="0x1" isInCharger="1" isUsbConnected="0"/>	In charger; USB not connected
<EventPPState ppn="1" ppnHex="0x1" isInCharger="0" isUsbConnected="1"/>	Not in charger; USB connected

Further information is provided in the SIP-DECT OM Application XML interface, which is available via MSA.

The XML Action URI provides the same status information if the following parameters are specified in the parameter set.

Parameter	Description
{usb_y}	USB connected
{usb_n}	USB disconnected
{chg_y}	DECT phone is in charger
{chg_n}	DECT phone is not in charger

Example:

path=sipDectTerm.xml?...&inCharger={chg_y}&notInCharger={chg_n}&usbconn={usb_y}&usbdiscn={usb_n}

For more information, see the SIP-DECT XML Terminal Interface for Mitel 600/700 DECT Phone Family.

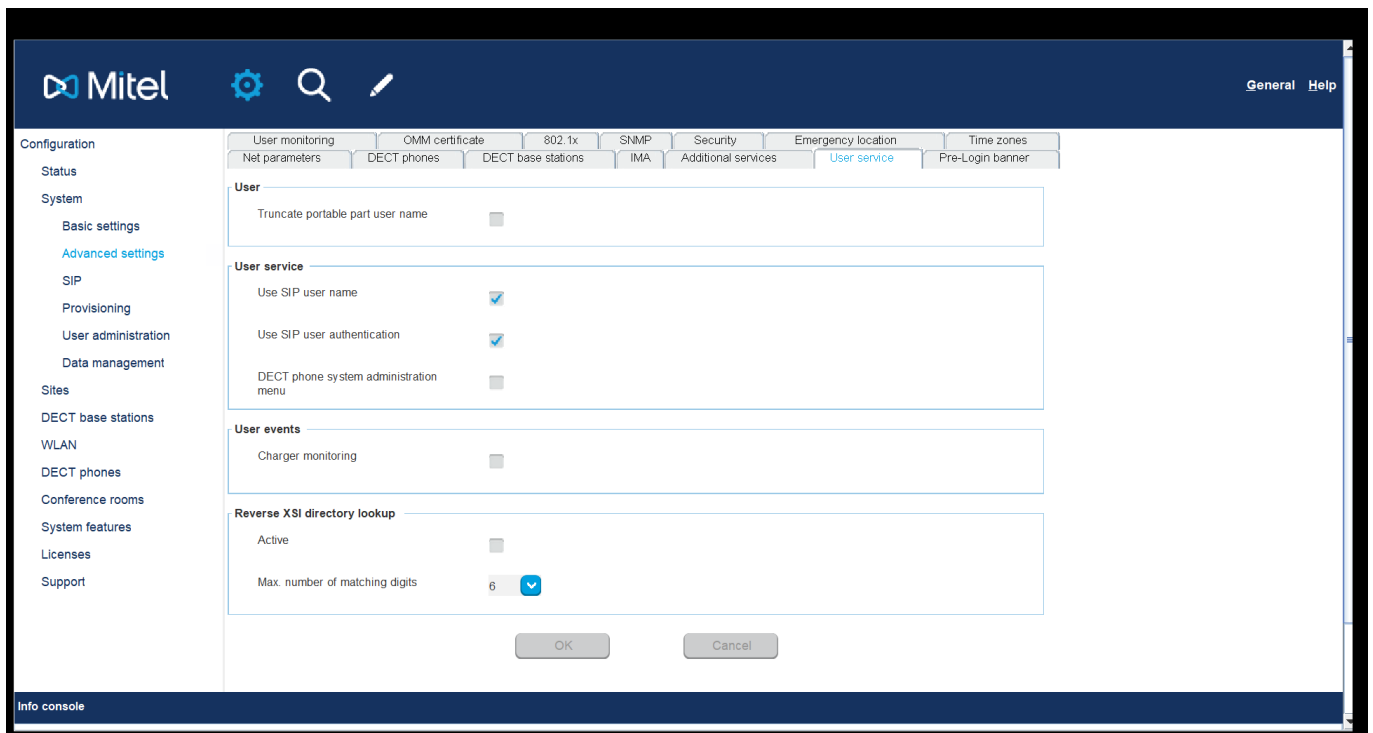
Note: If multiple state changes occur in a short period of time, then only the final state will be reported, and after approximately 10 seconds to avoid message bursts.

The charger event signaling can be activated via OMP. See section [7.7.2.6](#).

Use the following values to configure the **Charger monitoring** parameter in the configuration files.

Parameter / Parameter group	Charger monitoring
Description	Activates or deactivates sending a charger event via AXI or the XML Terminal Interface. To receive an event, a proper configuration of the XML action URI or an event subscription via AXI is also required.
Format	Boolean
Range	0, false; 1, true
Default value	0
Web	N/A
OMP	System > Advanced settings > User service > User events > Charger monitoring
OMM configuration files	<SetChargeStateMonitoring enable="1" />
DECT Phone	N/A
User configuration files	N/A

2.65.4 RFP43 AND RFP48: 802.1X BIND WPA SUPPLICANT TO BRIDGE INTERFACE



2.66 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.

2.66.1 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 600/700 DECT Phones, version 4.0 or higher.

2.66.1.1 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 (for example, 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.

2.66.1.2 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”

2.66.2 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.

2.66.2.1 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.

2.67 SIP ENHANCEMENTS

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

2.67.1 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**).

2.67.2 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**).

2.67.3 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**).

2.67.4 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**).

2.67.5 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**).

2.67.6 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**).

2.67.7 CALL REJECT ON SILENT CHARGING

If the following 2 conditions are fulfilled, all Mitel 600/700 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**.

2.67.8 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**).

2.67.9 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**).

2.68 SYSTEM CONFIGURATION TOOLS

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

- the Web-based OMM Web service (see section OMM Web Service)
- the Java-based OM Management Portal (see section OM Management Portal (OMP))

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

2.69 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 [9.18](#)).
- 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 [9.8](#).
- 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/.

2.70 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 600/700 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). Ensure 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 [7.13.5](#).

2.71 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. 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 AXI and OMP.

For a detailed description of the “User monitoring” feature, see section [9.25](#).

2.72 EXTENDED MESSAGING

You can set up an extended messaging and alarms system (for example, 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.

2.73 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 Called Identification” parameter in the OMP **System -> SIP -> Supplementary Services** menu.

2.74 CALL HANDLING

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

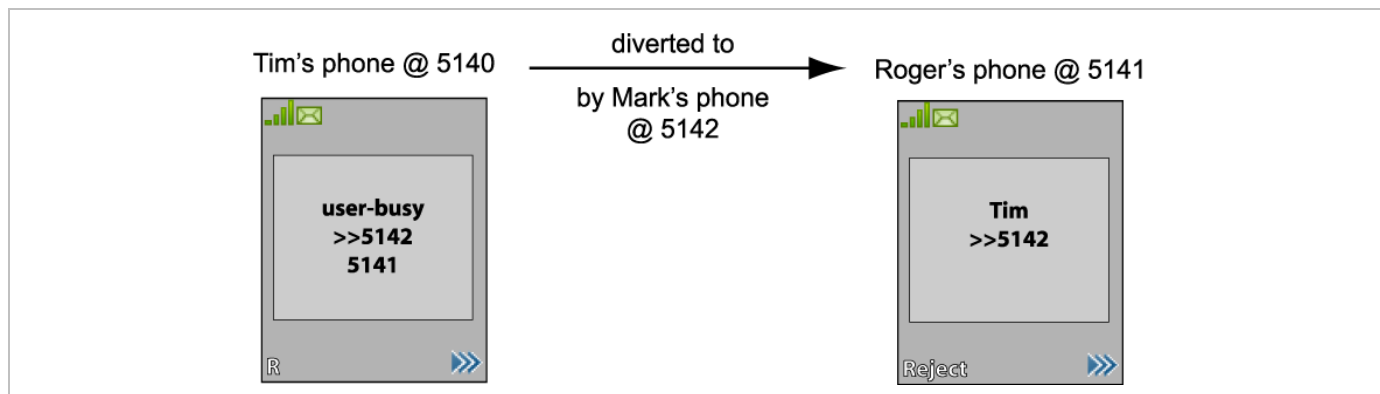
2.74.1 DIVERSION INDICATION

The OMM supports the displaying of diversion indications for Mitel 142d and Mitel 600/700 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 and Mitel 600/700 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).



2.74.2 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 600/700 and Mitel 142d phones.

2.74.3 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 [7.7.4.2](#)).

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.

2.74.4 THIRD LINE HANDLING FOR MITEL 142D AND 600/700 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 600/700 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 (for example, to open a further third line for an inquiry call in a brokering situation, where two lines are already involved).

2.74.5 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 600/700 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”

2.75 VOICE MAIL NUMBER

You can configure a system-wide voice mail number. This number is used by the Mitel 600/700 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" for example, "UD_VoiceMailNumber=222". For details, see the *SIP-DECT DECT Phone Sharing and Provisioning Guide*.

2.76 ALPHANUMERIC DIALING

SIP-DECT supports the dialing of alphanumeric characters. This allows a user to dial names (for example, "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.

2.77 UTF-8 ENCODING

The UTF-8 support allows the display of a wider range of language specific characters (for example, umlauts) and facilitates localization for different markets. The OMM and the Mitel 600/700 DECT phone family support UTF-8 for text messaging.

In addition, the OMM and the Mitel 600/700 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.

2.78 SIP MULTIPORT

Some call server platforms (for example, 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:

$$\text{UserPortCount} = \text{UserPortRangeStart} - \text{UserPortRangeEnd} + 1$$

$$\text{UserPort} = ((\text{UserID} - 1) \% \text{UserPortCount}) + \text{UserPortRangeStart}$$

$$\text{ConfRoomPortCount} = \text{ConfRoomPortRangeStart} - \text{ConfRoomPortRangeEnd} + 1$$

$$\text{ConfRoomPort} = (\text{ConfRoomID} \% \text{ConfRoomPortCount}) + \text{ConfRoomPortRangeStart}$$

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 [7.7.4.1](#)).

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 [13.6](#) 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 [10.3](#) 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.

Please note: Some server ports may have been changed in the SIP-DECT OMM configuration, e.g. the SIP port range. This requires additional firewall rules for changed ports in a Linux server OMM. If the Linux server OMM is updated via OVA and the system is taken over with the setup routine, the adapted firewall rules are not adopted. A manual transfer is also necessary if a new system is set up and a DB backup is imported. Sample: Port range for SIP UDP/TCP:

```
firewall-cmd --zone=public --add-port=17xxx-1xxxx/tcp --permanent
firewall-cmd --zone=public --add-port=17xxx-1xxxx/udp --permanent
firewall-cmd --reload
```

2.79 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.

2.80 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 (for example, Broadsoft or Sylantro 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 600/700 and Mitel 142d DECT phones.

For a detailed description of conferencing functionality, see section [9.20](#).

2.80.1 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.

2.80.2 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 600/700 DECT phone. You can configure the FAC via the OMM web service (see section [6.9.4](#)) or the OMP (see section [7.13.2](#)).

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 600/700 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 600/700 DECT phones.

2.80.3 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.

2.81 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.

2.82 DECT PHONE FUNCTIONALITY

2.82.1 DECT PHONE DOWNLOAD OVER AIR

The Mitel 600/700 series DECT Phones can download and upgrade their firmware via DECT over the air. The DECT base station software images (iprpf3G.dnld and iprpf4G.dnld) contains the Mitel 600/700 DECT phone software. The 3rd generation RFPs can house the SIP-DECT 8.0 OMM as in previous releases. The OMM supports the 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 DECT phone's firmware update).

The Mitel 600/700 DECT phone firmware packages are delivered in the "600.dnld/700.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 (iprpf3G.dnld and iprpf4G.dnld) without Mitel 600/700 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.

2.82.1.1 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.

The screenshot shows the Mitel SIP-DECT 8.3 configuration page. The left sidebar lists various configuration categories. The main content area is divided into sections: Status, System, System Settings, Provisioning & Software Update, SIP, User Administration, Time Zones, SNMP, DB Management, Event Log, Sites, Base Stations, SIP Users/Devices, WLAN, System Features, Licenses, and Info. The 'System' section is expanded, showing several configuration options. The 'Preserve user device relation at DB restore' checkbox is checked and highlighted with a red box. Other settings include DECT authentication code (35150), DECT phone user login type (Number), Auto-create on subscription (checked), Regulatory domain (None), Dynamic Frequency Selection (unchecked), QoS settings (ToS for voice packets: B8, ToS for signalling packets: B8, TTL: 32), DECT phone's firmware update (checked), and various fields for WLAN settings (Server, Port, User name, Password, Path) which are currently empty.

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.

2.82.2 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 (for example, nurses and doctors in hospital environments). See section [9.22](#) for more information on this feature.

2.82.2.1 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 [2.31](#)).

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 [9.22.5](#).

2.82.3 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.

2.82.4 MITEL 600/700 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.

2.82.5 MITEL DECT PHONE CUSTOMIZABLE BOOT TEXTS

By default, the text shown on the Mitel 600/700 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).

2.82.6 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 [6.9.5.2](#) (Modifying an XML Hook via the OMM web service) or section [7.13.8.2](#) (Modifying an XML Hook via the OMP).

2.82.7 USER INDIVIDUAL DECT PHONE PIN KEY LOCK

2.82.7.1 OMM Key Lock with PIN Management

The Mitel 600/700d DECT phone family offers 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 [7.11.4.12](#) “**Key lock**” tab.

2.82.7.2 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 [7.11.4.12](#) “**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* and *Mitel 700 DECT Phone User Guide*.

2.83 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 DECT settings 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.

2.84 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.

2.85 SYSTEM REDUNDANCY

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

2.85.1 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 OMM Standby).

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 Registration traffic shaping)

2.85.2 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 Backup SIP Servers).

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 Keep Alive Mechanism).

2.85.3 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 “SIP” tab).

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.

2.85.4 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*.

2.86 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 Factory Reset).

2.86.1 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.

2.87 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 DECT Base Station Synchronization).

2.87.1 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 “DECT settings” in Creating and Changing Base Stations or “DECT tab” in [section Adding New DECT Base Stations](#)).

Note: The 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).

A separate cluster number is also required for a remote site (for example, 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 Editing DECT Base Station configuration data).

2.88 WIRELESS LAN (WLAN)

If you have a number of WLAN DECT base stations (RFP 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 [6.8](#)).

2.88.1 802.11i: WPA2-ENTERPRISE PRE-AUTHENTICATION FOR FAST ROAMING

WLAN stations (for example, 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.

2.88.2 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.

2.88.3 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.

2.89 VOIP ENCRYPTION

To allow secured call connections over unsecured IP infrastructures (for example, 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 600/700 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 and DECT encryption together for a secure key exchange and a secure media transport.

2.90 MIXED DECT BASE STATION INSTALLATIONS

In sites (or whole systems) with Wideband Audio G.722 disabled, any combination of RFP 35/36/37 IP / RFP 43/48 WLAN is allowed.

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 [9.27](#).

2.91 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. 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 (for example, 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 (for example, 6x0d or 142d) or GAP phones still operate as normal, but do not support the new security mechanisms.

2.92 WIDEBAND (MITEL WIDEBAND AUDIO G.722 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 Wideband Audio G.722 terminal.

Each Wideband Audio G.722 connection uses twice the capacity on the DECT air interface, as compared to conventional narrowband. Therefore, four Wideband Audio G.722 connections can be established via one RFP, instead of eight narrowband calls.

Mitel Wideband Audio G.722 must be enabled or disabled per site (see section [6.5](#)). 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 Wideband Audio G.722 must be homogeneously available among synchronous RFPs.

As of SIP-DECT release 8.1, the Wideband Audio G.722 connections are supported for the Mitel 600/700 phones. For more details about the Wideband Audio option, see Audio Menu in the *Mitel 600/700 DECT Phone User Guide*.

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

2.93 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 600/700 DECT phone at the expense of DECT channel capacity (see [9.3](#)). Enable this feature for some or all of your DECT base stations (see section [6.4.1.2](#), "DECT settings" or section [7.7.1.2](#), "DECT tab").

DECT XQ audio cannot be combined with Wideband Audio G.722 within the same connection.

There are three operating modes related to audio quality available on the Mitel 650 DECT phone: standard audio, Wideband Audio G.722 and automatic.

- In Wideband Audio G.722 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.

2.94 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 [9.13](#)).

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*.

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

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.

Status

System

Sites

Base Stations

SIP Users/Devices

WLAN

System Features

Licenses

Info

Support

Licenses

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

OKCancel

License settings

Installation ID

271520138

License file import

Browse...

No file selected.

Import

General

License type

Built-in license for up to 5 DECT base stations

PARK

1F102F118A

(31100570430504)

System

Number of DECT base stations

5

Mitel SIP-DECT System License XXX

Messaging

Reception of text messages (Emergency, Locating alert) and enhanced messaging features

Mitel SIP-DECT Messaging & Alerting License Enterprise

Locating

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)

129

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

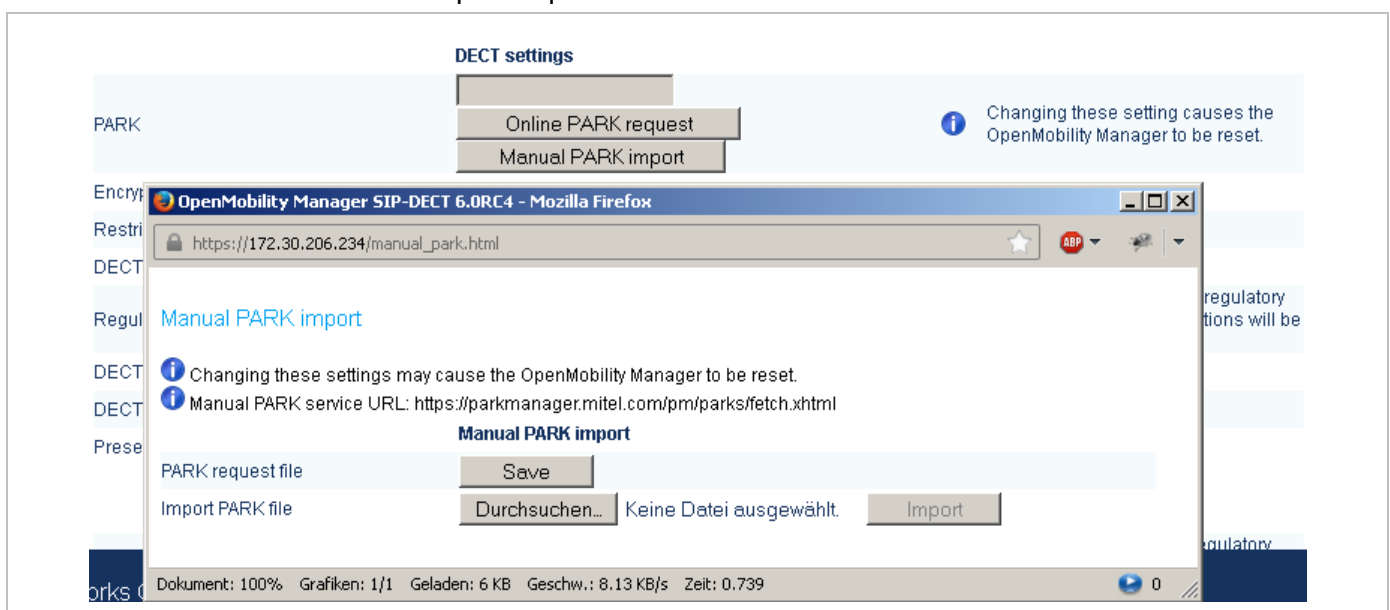
Note: With SIP-DECT Release 6.0 or later, there is no longer a demonstration mode for the OMM.

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/portal/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 [6.10](#)) or via the OMP (see section [7.14](#)).

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 shows the OMM web interface with the 'License file' tab selected. Under the 'Server' section, the 'General' sub-tab is active, displaying the 'Installation ID' as '270943175'. Below this are 'OK' and 'Cancel' buttons. The 'License file import' section features a 'File' button to select a license file, an 'Import' button, and a warning message: '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 [9.5.3.1](#)).

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 [9.8](#).
- 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**.

4.2 CONFIGURING RFP BY USING THE CONFIGURATION BUTTON

The configuration button of the RFP4G can be used to configure an RFP to start the OMM (that is, to become the OMM RFP). This allows SIP-DECT installation if there is a DHCP server in the network that does not support SIP-DECT-specific settings, such as the OMM IP address, and static local configuration using the OM Configurator or RFP configuration files are not suitable alternatives.



If the DHCP server does not support SIP DECT-specific DHCP options, the OMM's IP address is not predefined and set using the DHCP options, but is determined by the DHCP server. It is strongly recommended that the IP address must not change and be permanently assigned to the MAC address of

the RFP, which is supported by DHCP servers. Alternately, a long lease interval can be set to the OMM's IP address from changing frequently.

The RFPs in the network must automatically detect the OMM, because the OMM's IP address is not available to them as a configuration parameter (such as DHCP, RFP configuration files, or local static configuration). This OMM detection mechanism is based on broadcast traffic and is therefore limited to one broadcast domain, that is, the same network segment.

For more details about setting up an RFP4G using the configuration button, see [9.6](#).

4.2.1 BENEFITS

Configuring an RFP4G using the configuration button is beneficial for small and simple SIP DECT installation for the following reasons:

- RFPs can detect the OMM within a broadcast domain or network segment.
- RFPs can retrieve new software from the OMM RFP.
- The OMM RFP supports up to 5 simultaneous software downloads using TFTP.
- The OMM RFP distributes its own active software; that is, OMM RFP needs to update first before the software is available to additional RFPs.
- The stand-by OMM feature is not supported.

4.3 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).

4.4 SYSTEM SETTINGS

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

System name	SD 8.3
Remote access	☒
Tone scheme	DE
DECT settings	
PARK	1F102F118A (31100570430504)
DECT power limit 100mW	☐
Encryption	☒
Restrict subscription duration	☐
Authentication before ciphering	☐
DECT monitor	☐
Regulatory domain	EMEA
DECT authentication code	35150
DECT phone user login type	Number
Preserve user device relation at DB restore	☐
Auto-create on subscription	☒

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

Voice mail number	25711

Voice mail number: Your system voicemail number. A Mitel 600/700 phone will then offer the voice box in the Handset menu.

4.5 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

General settings	
MAC address	
Name	
Site	1
Emergency Location Identification Number (ELIN)	
☐ DECT settings	
DECT Cluster	1
Preferred synchronization source	☐
Reflective environment	☐
☐ WLAN settings	
WLAN profile	0
802.11 channel	
Output power level	Full

The base station configuration requires:

- base station MAC address
- Name for example, 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.

4.6 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

Basic settings	
Proxy server	10.103.35.71
Proxy port	5060
Registrar server	10.103.35.71
Registrar port	5060
Registration period	3600 sec
Globally Routable User-Agent URL	☒
Outbound proxy server	
Outbound proxy port	5060
Transport protocol	UDP
Local UDP/TCP port range	5060 - 5060
Local TLS port range	5061 - 5061

Advanced

RTP settings	
RTP port base	16320
Preferred codec 1	G.722
Preferred codec 2	G.711 u-law
Preferred codec 3	G.711 A-law
Preferred codec 4	G.729 A
Preferred packet time	20 msec
Silence suppression	☐
Receiver precedence on codec negotiation	☐
Eliminate comfort noise packets	☐
Single codec reply in SDP	☐

DTMF settings	
Out-of-band	☒
Method	RTP(RFC 2833)
Payload type	101

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

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

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

Please note: For MiCloud Flex deployments only, enter the FQDN of call server instead of the IP Address. For more information, see the MiCloud Flex Deployment Guide.

4.7 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 **SIP Users/Devices** menu (ensure the **Advanced** option in the top bar is enabled) and click **New**.

New DECT phone

General settings

Display name

Number/SIP user name

IPEI

DECT authentication code

Login/Additional ID

SOS number

ManDown number

Voice mail number

Number used for visibility checks

SIP authentication

Authentication user name

Password

Password confirmation

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 for example, 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 600/700 DECT phones, open the DECT phone **System > Subscriptions** menu. Select **New system** and enter the Authentication code provided in your System Settings (for example, 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.

4.7.1 DECT PHONE AND SIP STATE VERIFICATION

You can check the DECT phone state and SIP registration status from the **SIP Users/Devices** 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 name:	No

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

5 LOCAL DECT BASE STATION CONFIGURATION (OM CONFIGURATOR)

5.1 OVERVIEW

The OM Configurator (OMC) is a Java tool used to manage the SIP-DECT solution. A local (static) start up configuration can be stored permanently into RFP(s) using the OM Configurator on a PC in the local network.

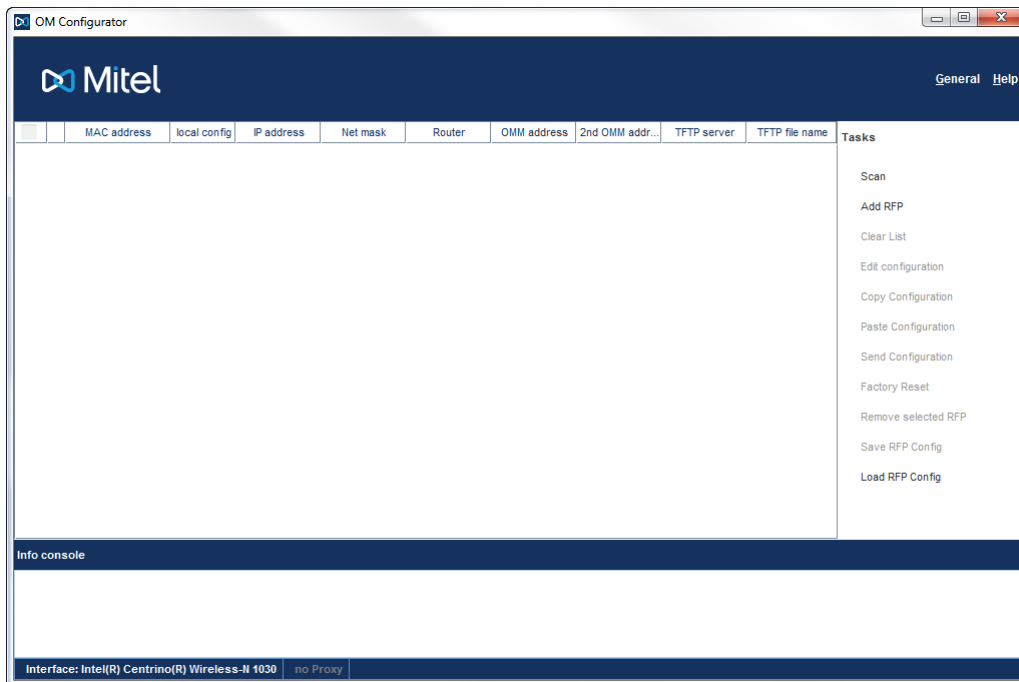
OMC offers the following communication options:

- Broadcast packets to the target MAC address and selected network interface.
For example, to reach RFPs in the local network / VLAN
- Unicast packets to a “proxy” RFP which forward the request as broadcast packet.
Each configured (running) RFP act as proxy RFP.
For example, PC is not located in the same IP subnet, as the RFPs to configure.

As an alternative to DHCP configuration, you can use the OM Configurator tool to statically configure the DECT base stations individually. RFP settings configured through the OM Configurator tool are saved permanently in the internal flash memory of the RFP. The OM Configurator version must match the installed SIP-DECT software version to be used for the local configuration of RFPs.

Please note: An initial configuration of the 3rd or 4th generation RFPs through the OM Configurator tool requires a login and password. The default login and password is “omm” and “omm”. If the RFP is configured by the OMM later on, the OMM also sets the configuration password. You must enter the OMM’s full access user and password in the OM Configurator tool then.

At start-up of the OM Configurator displays a table with configuration data for all RFPs. The task bar on the right side shows permitted actions. The Info console in the lower part of the window shows information and errors as they occur during OM Configurator operation



5.2 INSTALLATION

OMC is provided as an AdoptOpenJDK JAVA 11 application.

Notes:

- A locally installed Java Runtime Environment (JRE) is not required to run the application package. The JRE is now delivered as part of OMC application package.
- The OMC for Microsoft Windows installer includes the AdoptOpenJDK (OMP_Runtime_Image_Win.zip) runtime environment file for 64-bit Windows. 32-bit versions are not supported.

Perform the following steps to install OMC on a Windows environment or a Linux system:

- Windows:
 - Run the *OM_Configurator_Installer_SIP-DECT_8.1.exe* file and follow the on screen installation instructions.
After successful installation of the application, OMC is accessible from the **Start** menu in the folder path *Start Menu/Programs/Mitel/SIP-DECT 8.1* of the Windows system.
 - Alternatively, extract the files from *OMCFG_Runtime_Image_Win.zip* to access the application. After extracting the zip files, the application can be started by running the *omcfg.bat* file in *OMCFG_Runtime_Image_win\bin* folder.
- Linux:
 - Run the command `tar xfvz OMCFG_Runtime_Image_Linux.tar.gz` to extract the application.
 - Start OMCFG by running the script `ompcfg` in the extracted directory *OMCFG_Runtime_Image_Linux/bin*.

To uninstall the application, run the *Uninstall OM_Configurator* file in the folder path *Start Menu/Programs/Mitel/SIP-DECT 8.1* of the Windows system.

5.3 SELECTING THE NETWORK INTERFACE

You can select the network interface of the computer used by the OM Configurator via the **General -> Options** menu. The selected interface is shown on the status line of the program.

5.4 ADDING DECT BASE STATIONS FOR CONFIGURATION

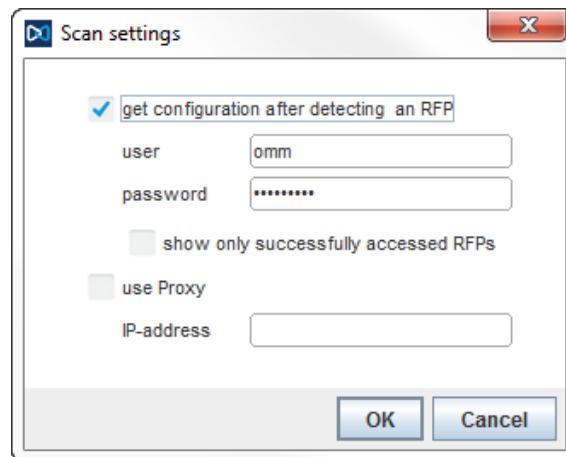
Before you can configure an RFP, you must add the RFP to the OM Configurator database. You can add an RFP record by:

- scanning for RFPs that are already attached to the network
- entering the MAC address of the RFP
- loading a configuration file that contains RFP MAC addresses and configuration parameters

Please note: Adding an RFP to the OM Configurator database does not modify the RFP configuration. Configuration data must be transmitted explicitly to the RFP(s) through the **Send Configuration** option.

5.5 SCANNING FOR DECT BASE STATIONS

The OM Configurator tool can scan for RFPs on the LAN segment.



- If **get configuration after detecting an RFP** is enabled, the OM Configurator attempts to fetch the local configuration settings from all RFPs that are detected during the scan. The program uses the **user/password** combination if an access without login data fails.
- If **show only successfully accessed RFPs** is enabled, the OM Configurator adds only RFPs that provide configuration information to its database, and displays those RFPs in the OM Configurator table.
- The **use Proxy** parameter allows access to RFPs that are located in network segments other than the segment that hosts the OM Configurator. The **IP-address** field must contain the address of a RFP located in the network segment to be scanned. This RFP works as proxy and must be up and running.

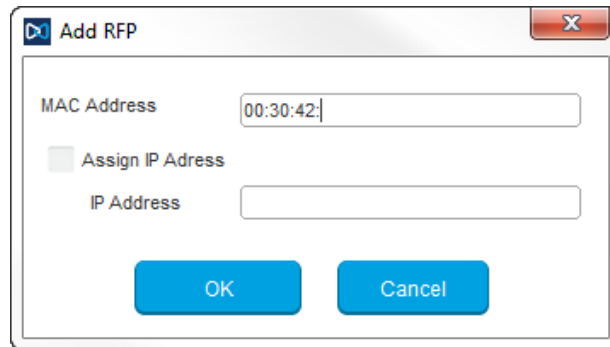
You initiate the scan process by clicking **OK** button. The OM Configurator adds the results to the table. In rare cases, it is possible that a RFP is expected to appear in the table after the scan operation but does not. If this occurs, repeat the scan operation.

5.6 ADDING DECT BASE STATIONS MANUALLY

You can add an RFP to the OMM Configurator database manually.

When you click the **Add RFP** option in the task bar, the OM Configurator displays the “Add RFP” dialog. You must specify the MAC address of the RFP in the **MAC Address** field.

Optionally, you can also specify an IP address. If an IP address is assigned, the OM Configurator automatically proposes an incremented IP address the next time the “Add RFP” function is invoked.



5.7 LOADING DECT BASE STATION DATA FROM FILE

You can import an RFP configuration file to the OM Configurator.

When you click on the **Load RFP Config** option, the OM Configurator opens a dialog window that prompts you to browse for the configuration file. All found valid RFP entries in the file are added to the OM Configurator database and displayed in the table.

5.8 EDITING DECT BASE STATION CONFIGURATION DATA

You can edit the configuration of a DECT base station stored in the OM Configurator database. When you double-click on a table row, the OM Configurator displays a Detail Data window below the table, with the “General” section activated. You can also access this window by selecting one or more entries in the table and clicking the **Edit configuration** option in the task bar.

You can change parameters for multiple RFPs by selecting more than one RFP in the table. Parameter settings that differ between the selected RFPs are shown as “****” and retain their values if you do not make any modifications.

You cannot change the IP address value when you select more than one RFP.

If more than one parameter value is allowed (for example, Router, DNS addresses), you must separate the values by a space.

If you click the **Reset Configuration** button, all configuration parameters are removed and local configuration in the OM Configurator is disabled. The **Send Configuration** option is also needed in this case in order to update the configuration of the RFP locally.

When you click the **OK** button, changed parameter values are committed to the database. The system performs validation checks for some parameter values. If this check fails, the system displays an error message in the Info console and the misconfigured parameter value is marked with a red frame (allowing you to correct the value). Modified RFP records are marked (▶) beside the corresponding table row.

If you press **Cancel** or select another RFP in the table, any changes are discarded.

When you press either **OK** or **Cancel**, the Detail Data section disappears and a number of task bar options (for example, **Send Configuration**) are re-enabled.

5.8.1 OTHER PARAMETER SECTION

You can set and edit less frequently used parameters on the **Other** section of the **Detail Data** window.

If the parameter you want to add or edit is listed in the table on the **Other** section, click on it to display the parameter name and value in the fields on the top-right side of the section. Click the **Change** button to commit the changed value.

If the parameter value field is empty, the parameter is cleared on the RFP when you click **Send Configuration**.

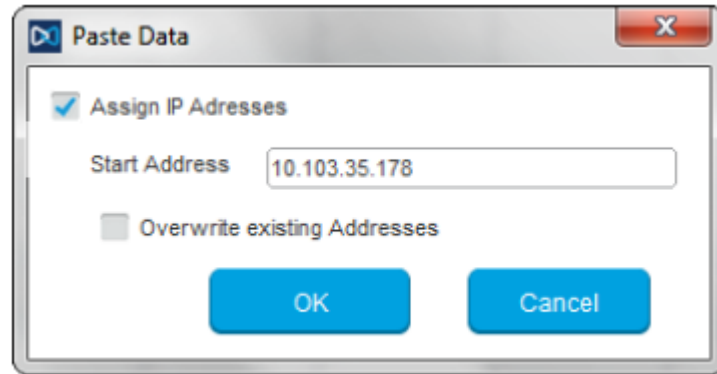
You can add a new parameter by selecting a parameter name from the drop-down list and clicking the **New** button.

5.8.2 COPY AND PASTE

You can assign parameter values from one RFP to one or more other RFPs.

To perform this operation, you must ensure that the **Detail Data** window is not active. If the **Detail Data** window is open, commit your changes or cancel to close the window.

Select an RFP in the table and click the **Copy Configuration** option in the task bar. Next, select one or more RFPs as destination RFP(s) and click the **Paste Configuration** option. The system displays the Paste Data dialog window.



If the **Assign IP Addresses** option is enabled, you must provide a valid IP address in the **Start Address** field. The system may display a suggested address, based on a previous paste or Add RFP operation. The IP address is incremented by one for each RFP.

If the **Overwrite existing addresses** parameter is not enabled, an IP address is only assigned if the IP address field of the target RFP is empty.

5.8.3 CONFIGURATION PARAMETERS

The following table lists the available configuration parameters for the DECT base station.

Parameter	Mandatory/Optional	Description
Use local config	Mandatory	Specifies whether the local configuration settings should be used at boot-up or not
IP Address	Mandatory	IP address of the DECT base station.
Net Mask	Mandatory	Subnet mask of the IP network
TFTP server address	Mandatory	IP address of the TFTP server (set to 0.0.0.0 if not used)
TFTP file name	Mandatory	The boot file to be read from the TFTP server
OMM address	Mandatory	IP address of the OpenMobility Manager
Router	Optional	IP address of the default gateway
DNS address	Optional	IP address of the DNS server
DNS domain	Optional	Domain name of the network
Broadcast address	Optional	Broadcast address for the network
2nd OMM address	Optional	IP address of the standby OMM
VLAN ID	Optional	VLAN identifier
Use VLAN and DHCP	Optional	Specifies whether only the local VLAN configuration settings should be used when booting or not
Syslog server address	Optional	Destination IP address for the syslog file
Syslog server port	Optional	Destination port address for the syslog file

RFP configuration file server	Optional	URL of a server with RFP configuration files (ipdect.cfg <MAC>.cfg) alternatively or in addition to OM Configurator settings. Syntax: {ftp https http https}://[user:password@]server/[directory/] or tftp://server/[directory/]

5.9 APPLYING CONFIGURATION CHANGES

To apply new or changed configuration to RFP devices, select one or more RFP entries from the table and click the **Send Configuration** option in the task bar.

Note: You must close the Detail Data window to apply configuration changes to an RFP. If the Detail Data window is open, the **Send Configuration** option is disabled.

The OM Configurator displays the **Protocol settings** dialog window.

The settings in the **Protocol settings** dialog are preset to the values used for the **Scan** operation or the last **Send Configuration** operation. If the values are correct, click **OK** to transfer the data to the RFP device.

Before sending the data, the system performs a check on mandatory parameters and the validity of some parameter values. If this check fails, an error is reported in the Info console.

The system displays a message in the Info console window indicating success or failure of the data transfer operation for each RFP.

If data is transferred successfully, the OM Configurator displays a checkmark beside the row for the corresponding RFP.

The OM Configurator attempts data transfer three times (two seconds apart) before reporting an error. Depending on the network environment and current RFP status, the data transfer may fail in rare cases. If a failure to transfer data occurs, click the **Send Configuration** option again to re-initialize the data transfer.

If the data transfer fails, the OM Configurator displays an "X" beside the row for the corresponding RFP.

5.10 FACTORY RESET

RFPs are protected against unauthorized configuration changes by user authentication (user and password), which are also used to configure the OMM via web service or OMP.

To reset a RFP's configuration, select the RFP entry in the table and click the **Factory Reset** option in the task bar. This option is only enabled when a single RFP entry is selected. The option is disabled if multiple RFPs are selected.

The system displays the **Factory reset settings** dialog window. Set the correct login data (user and password) and RFP proxy address (if required). The system auto-fills the fields with the values used for previous **Scan**, **Send Configuration** or **Factory Reset** operations.

If the specified login ("omm"/"omm") does not work and the login credentials of the last system the RFP was used with are unknown, you can reset the RFP to factory settings by sending a cookie string to the OpenMobility manufacturer support and entering the received reset key. The OM Configurator copies the cookie string to the clip board.

5.11 SAVING AND LOADING A DECT BASE STATION LIST

You can save the configuration of one or more RFPs to a RFP configuration file. Select the RFP entries in the table and click the **Save RFP Config** option in the task bar. (Note that if the **Detail Data** window is active, the **Save RFP Config** option is disabled.)

RFP configuration data is loaded from the file and added to the OM Configurator database via the **Load RFP config** option. You must initiate the **Send Configuration** operation after executing the **Load RFP config** operation for the configuration to take effect on the select RFPs.

Please note: The data sequence has been changed from previous releases of the SIP-DECT OM Configurator. Import of files based on the old data sequence format may result in import errors or the incorrect assignment of parameter values.

5.12 REMOVING DECT BASE STATION ENTRIES

You can remove all RFP data records from the OM Configurator different from the current SIP-DECT release database through the **Clear List** option in the OM Configurator task.

You can remove one or more RFP records from the OM Configurator database by selecting one or more entries in the table and clicking on the **Remove selected RFP** option.

Ensure that you do not remove data records before configuration is sent to the RFP device (via the **Send Configuration** operation). Changes made to RFP configuration data but not sent to RFP device are lost on the remove operation.

You can add RFP configuration data again through the operations described above.

5.13 COMPATIBILITY WITH OLDER SIP-DECT RELEASES

It is not recommended to use the OM Configurator for configuration different from the current SIP-DECT release for configuration of RFPs with software from an earlier SIP-DECT release.

Configured parameters of an RFP which are unknown to actual OM Configurator are shown in the “Other parameter” section with the name used at the protocol level. In most cases, this name will be different from the display name known from previous versions of OM Configurator.

You can edit or remove such parameters and new values will be transferred to the RFP when you execute the **Send configuration** operation.

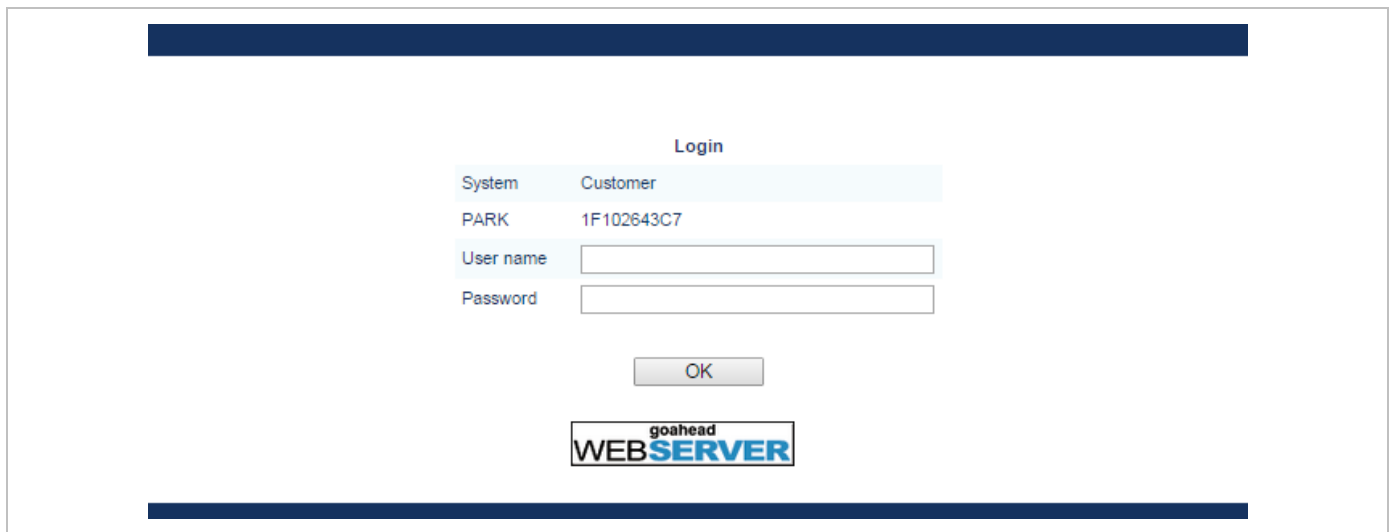
6 OMM WEB SERVICE

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.

6.1 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 [6.11](#)).

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 [9.16.1](#).

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.

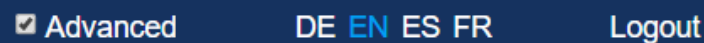
After login in, the following menus are available (with the **Advanced** option enabled in the top bar):

- **Status** menu: Displays the system status (see section [6.3](#)).
- **System** menu: Allows configuration of general SIP-DECT system parameters (see section [6.4](#)).
- **Sites** menu: Allows grouping of DECT base stations into different sites (see section [6.5](#)).
- **Base Stations** menu: Allows configuration and administration of the attached base stations (see section [6.6](#)).
- **SIP Users/Devices** menu: Allows administration of the DECT phones (see section [6.7](#)).
- **WLAN** menu: Allows configuration of WLAN parameters (see section [6.8](#)).

- **System Features** menu: Allows administration of system features like digit treatment and directory (see section [6.9](#)).
- **Licenses** menu: Allows administration of licenses (see section [6.10](#)).
- **Info** menu: Displays the End User License Agreement (EULA) (see section [6.11](#)).
- **Support menu**: Summarizes existing SIP-DECT maintenance functions (see section 6.12).

6.2 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.



Advanced DE EN ES FR Logout

6.3 “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.

In SIP-DECT 8.3, the Status page has been extended with a "**Software update**" section, which contains information about the OMM/RFP software update process:

- **Global Status:**
 - **Idle:** No software update process is running at the time
 - **In progress:** A software update process is running. Software is being downloaded, verified, and distributed from the OMM to all base stations in the system.
 - **Awaiting activation:** A software update process is running. The software has been successfully downloaded, verified, and distributed to all base stations in the system. The OMM is waiting for a signal to initiate activation of the new software. This state can only be reached when software activation is configured not to occur automatically after download and distribution.
- **New software version:** Indicates the version of the software to be installed. It is only visible after successful verification of the software.
- **Software downloaded:** Indicates how many of the connected base stations have loaded the new software. It is only visible after successful verification of the software.
- **Software activated:** Indicates how many of the connected base stations have activated the new software. It is only visible after successful verification of the software.

Status	Status	
System		
Sites	OpenMobility Manager	SIP-DECT 8.3SP1-GI15
Base Stations	Uptime	5 Days, 0:16
SIP Users/Devices	Licenses	Built-in license for up to 5 DECT base stations
WLAN	Standby OMM	There is no OpenMobility Manager in standby mode configured!
System Features	OM Integrated Messaging & Alerting service	✓
Licenses	Automatic database export	Successfully finished. 2022-01-26 10:38
Info	Provisioning	✓
Support		
		Base Stations
	Total number	2
	Connected	2
	DECT activated	2
	DECT currently active	2
	DECT clusters	1
	WLAN activated	0
		Software update
	Global status	Idle
		DECT Phones
	Users	2

6.4 “SYSTEM” MENU

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

6.4.1 “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 [6.4.1.15](#))
- update the OMM (see section [6.4.1.16](#))

Status
System
System Settings
Provisioning & Software Update
SIP
User Administration
Time zones
SNMP
DB Management
Event Log
Sites
Base Stations
SIP Users/Devices
WLAN
System Features
Licenses
Info
Support

OK Cancel

Restart

General settings

System nameSD 8.3

Interfacess

Tone schemeDE

DECT settings

PARK1F102F118A(31100570430504)

DECT power limit 100mW

Encryption

Restrict subscription duration

Authentication before ciphering

DECT monitor

Regulatory domainEMEA

DECT authentication code35150

DECT phone user login typeNumber

Preserve user device relation at DB restore

Auto-create on subscription

Emergency location

When changing the DECT regulatory domain all DECT base stations will be reset.

The following sections describe the parameters that can be set.

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

6.4.1.1 General settings

- **System Name:** Enter the system name.
- **Interfaces:** Used to enable or disable the admin interfaces OMM Web service and AXI (OMP) to increase security if they are not needed. Options available are:
 - **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 [10.3.5](#).
 - **AXI server access:** Enables/disables AXI server access.
 - **Web server access:** Enables/disables Web server access.
- **Tone scheme:** Select the country in which the OMM resides. This enables country specific tones (busy tone, dial tone, etc).

6.4.1.2 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 (for example, 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: Ensure that all deployed third party DECT phones support DECT encryption. If not, encryption can be disabled per DECT phone (see [7.11.4](#)).

- **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.
- **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.

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: **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.
- **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, 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.

- **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.

6.4.1.3 **Emergency location**

- **Enabled:** Enables Emergency location. This helps the call server (SIP proxy) to determine the correct public-safety answering point (PSAP) depending on where the call has made.
- **Emergency Location Identification Number (ELIN):** Enter the system-wide valid emergency call identification number. This value is used when there is no more specific ELIN set. The parameter can be used for small systems in which the same ELIN should be used for all base stations.

Note: Supported by 3rd and 4th generation RFPs where these features are enabled.

6.4.1.4 **Security**

- **Secutiy level:** Specifies the security level. Available options are High, Medium, Legacy.

6.4.1.5 WLAN settings

This setting applies to RFP 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 [6.8](#) and [9.17](#).

WARNING: 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.

- **Dynamic Frequency Selection (DFS):** DFS is a spectrum-sharing mechanism that allows wireless LANs (WLANs) to coexist with radar systems. Select the check box to allow SIP-DECT to automatically select a frequency that does not interfere with certain radar systems while operating in the 5 GHz band.

6.4.1.6 Voice mail

- **Voice mail number:** Specifies a system-wide voice mail number. This number is used by the Mitel 600/700 DECT phone family if the voice box is called.

6.4.1.7 QoS settings

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.

6.4.1.8 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 600/700 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 [6.4.5](#)).

- **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.

6.4.1.9 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.

6.4.1.10 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 [9.14](#).

6.4.2 "PROVISIONING & SOFTWARE UPDATE" 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/unsecure connections to the file server to retrieve configuration or firmware files. For more information on this feature, see section [9.8.1](#).

As of the SIP-DECT, 8.3 the **Provisioning** menu has been renamed to **Provisioning & Software Update**. The overall look and feel of the OMM Web Service remains the same as in previous versions, with the addition of new configuration parameters and status information. Some existing sections have migrated or otherwise been rearranged, as they are now considered part of the Provisioning & Software Update concept. Obsolete and/or excess elements have been disabled or completely removed to avoid confusion and simplify the user experience.

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

6.4.2.1 Current Provisioning URL

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

6.4.2.2 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.

6.4.2.3 Provisioning 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.

6.4.2.4 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 [9.9.3](#) 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 provisioning security configuration :** Enables the use of the system-wide certificate validation settings for this URL, as configured on the **System** -> **Provisioning & Software Update** -> **Certificates** page (see section [6.4.2.14](#)).

6.4.2.5 System update

- **Order of download and application of files:** Determines the download and application order of base station software and all other configuration and resource files. This parameter is always set to 1 (Configuration before software) for the Linux server OMM and is read-only on the user interfaces. The Linux server OMM will always run in the “ Configuration before software” mode.
- **On OMM restart:** Determines whether the OMM restart also triggers the reboot/restart trigger and not only the base station reboot. This parameter is not relevant for the Linux server OMM and is not offered on the user interfaces. The restart trigger will always be executed in case of a Linux server OMM restart.
- **Time-controlled:** Scheduled time trigger to initiate the provisioning process which enables/ disables time scheduled trigger
 - **Time of day:** Hour and minutes of the day indicating when to start the provisioning process
 - **Maximum delay (minutes):** The maximum period for which the start of the provisioning process is randomly delayed
- **Calculated time of day:** 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
- **Start (or abort) system update manually:** Select either **Update** or **Abort**.

6.4.2.6 Event Trigger

This section allows the configuration of the four different Provisioning trigger events:

- **Manual Trigger:** Triggered by button ‘Update’
- **RFP/OMM (re)start:** Triggered by reboot of the DECT base station and optionally by an OMM restart.

- **SIP Notify:** Triggered by receiving SIP-Notify events.
- **Scheduled update:** Triggered if configured update time of day is approached.

The following settings can be configured for any single event trigger:

- **Software update:** Download the DECT base station software and activate it.
- **RFP software:** Select the mode of the software update:
 - **None (marked with -):** Software is not downloaded. Do not select this, if Software update is activated.
 - **Optional:** Software download is optional. Unsuccessful downloading of the software does not cancel the currently running Provisioning process.
 - **Mandatory:** Software download is mandatory. If the software file cannot be downloaded by any reason, the currently running Provisioning process is cancelled.
- **Configuration:** Download configuration files from Provisioning server. The selection of files to be downloaded is configured by the following file selection. All files can be set to one of the following modes:
 - **None (marked with -):** File shall not be downloaded
 - **Optional:** File download is optional, if it cannot be downloaded, the current Provisioning goes on
 - **Mandatory:** File download is mandatory, if not downloadable, the current Provisioning process is stopped
- Following configuration files are supported:
 - OMM configuration
 - IMA configuration
 - Branding image
 - License
 - User data
 - SIP certificates
 - Provisioning certificates
 - WEB/AXI certificates
 - WPA supplicant certificates
- **Time to wait after error (seconds):** Period of time to wait after a download trial failed (in sec.)
- **Random component (seconds):** A calculated time value between 0 and the selected random component (in sec.) is added to the Initial wait timer, to calculate the real wait time. For every retry the real wait time is doubled.
- **Number of retries:** Number of retries in case of error for every single file to be downloaded.

6.4.2.7 Software activation

- **Trigger:** Set the DECT base station software activation method:
 - Time-controlled: Activation starts at a selected time of day
 - Automatic: Activation starts immediately after the download is finished
 - Manual: Activation is started by the user with the button 'Activate'
- **Time of day:** Time of day of software activation.
- **Calculated time of day:** Specific time of day of software activation (derived from Activation time of day and the delay calculated for the Update time of day in section 'Time-controlled update').
- **Mode:** Select if all DECT base stations are activated at once or one by one.
- **One-by-one activation timeout:** Enables or disables activation time out. Applicable only if one by one mode is selected. It determines the time by when the software activation should be completed and if not, then the activation shall be completed immediately in all-at-once mode without an idle check of the system or base station. If there is a random component defined for the time-controlled system update, then the same calculated random component is added to the time set. If the time out is before the activation time, then it applies 24 hours later.

- **Time of day:** If one by one mode is selected a timeout time can be configured. At that time, the one-by-one is cancelled and all remaining DECT base stations are activated immediately.
- **Calculated time of day:** Specific time of day of One by one timeout (derived from Timeout time of day and the delay calculated for the Update time of day in section 'Time-controlled update').
- **Button 'Activate':** Start the activation immediately.

6.4.2.8 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.

6.4.2.9 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 selected protocol. If the server does not respond to the selected protocol it will be treated as an error.
- **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 of all users.
- **Use provisioning security configuration:** Enables the use of the system-wide certificate validation settings, as configured on the **System -> Provisioning & Software Update -> Certificates** page (see section 7.7.5.2).

For further information on the user data import, see the *OM DECT Phone Sharing and Provisioning Guide*.

6.4.2.10 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.

- **Configure specific source:** 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:** Specifies the location and file name of the IMA configuration file on the external file server.
- **Use provisioning security configuration:** Enables the use of the system-wide certificate validation settings for this URL, as configured on the **System -> Provisioning -> Certificates** page (see section [6.4.2.14](#)).

6.4.2.11 Security

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.
- **TLS version:** The TLS protocol version to use for the configuration file server connection. Available options are: TLS1.2 TLS 1.3 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.

6.4.3 "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.

Status	SIP		
System	OK Cancel		
System Settings			
Provisioning & Software Update			
SIP			
User Administration			
Time zones			
SNMP			
DB Management			
Event Log			
Sites			
Base Stations			
SIP Users/Devices			
WLAN			
System Features			
Licenses			
Info			
Support			

Basic settings			
Proxy server	10.103.35.71		
Proxy port	5060		
Registrar server	10.103.35.71		
Registrar port	5060		
Registration period	3600		sec
Globally Routable User-Agent URL	☒		
Outbound proxy server			
Outbound proxy port	5060		
Transport protocol	UDP		
Local UDP/TCP port range	5060	-	5060
Local TLS port range	5061	-	5061

Advanced			
Explicit MWI subscription	☐		
Explicit MWI subscription period	86400		sec
User agent info	☒		
User agent info – compatibility mode	☐		
Dial terminator	#		
Registration failed retry timer	120		sec
Registration timeout retry timer	180		sec

6.4.3.1 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.

Please note: For MiCloud Flex deployments only, enter FQDN of the server instead of the IP Address. For more information, see the MiCloud Flex Deployment Guide.

- **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.

Please note: Some server ports may have been changed in the SIP-DECT OMM configuration, e.g. the SIP port range. This requires additional firewall rules for changed ports in a Linux server OMM. If the Linux server OMM is updated via OVA and the system is taken over with the setup routine, the adapted firewall rules are not adopted. A manual transfer is also necessary if a new system is set up and a DB backup is imported. Sample: Port range for SIP UDP/TCP:

```
firewall-cmd --zone=public --add-port=17xxx-1xxxx/tcp --permanent
firewall-cmd --zone=public --add-port=17xxx-1xxxx/udp --permanent
firewall-cmd --reload
```

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

6.4.3.2 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 600/700) 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 its 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 (that is, 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 (for example, SIP display name and user-id) will be displayed on Mitel 600/700 and Mitel 142d phones as new call target. In addition, the outgoing call log of the Mitel 600/700 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 header:** 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:
 - **URL** – 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 **URL**.

- **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”
- **Call reject state code(device unreachable):** Specifies the SIP state code sent as response when the incoming call is rejected because the DECT phone is unreachable (for example, the DECT phone is out of range or out of battery power). Valid values are “400” to “699”. The default is 486.
- **DNS SRV failover following registration:** Enables or disables the DNS SRV failover mode “following registration”. When “DNS SRV failover following registration” is enabled, and if the following conditions are true, the new mode is active:
 - “proxy server”, and “registrar server” are configured identically
 - “proxy server” or “registrar server” and “outbound proxy” are set to DNS SRV FQDN (port 0)

When the new mode is active:

- the call traffic of a user follows the registration; this means when the user is registered on (outbound) server A, an outgoing call is directed to (outbound) server A.
- when a user is in a call active state, SIP-DECT does not try a fallback to another server but remains on the registered (outbound) server. After coming back into idle state, the normal DNS SRV behavior is applied.

6.4.3.3 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 for example, 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 signalization) with a single codec in the SDP answer.
- **Source port filter:** Determines whether RTP packets from unknown source ports are filtered out. If activated, SIP-DECT checks the source port in addition to the source IP address when receiving RTP packets. If one of the parameters does not match the signaled data, the packets are ignored.

6.4.3.4 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/.

6.4.3.5 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.

6.4.3.6 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 “Location 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 sent 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 “Location 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 600/700):** Enables call transfer via the hook key on a Mitel 600/700 DECT phone (in addition to call transfer via menu).

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.

- **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.
- **Call reject on silent charging:** If the following 2 conditions are fulfilled, all Mitel 600/700 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.

6.4.3.7 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 [2.30](#).

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.

6.4.3.8 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”.
- **Validate certificates:** 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”.
- **Validate hostname:** 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 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.
- **Delete certificates/key:** Allows deletion of all certificates and the local key.

6.4.3.9 Certificate server

Set the parameters on the Certificate server section 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 servedr.
- **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 chain 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 provisioning security configuration:** Enables the use of the system-wide certificate validation settings, as configured on the **System -> Provisioning -> Certificates** page (see section [6.4.2.14](#)).

6.4.3.10 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.

6.4.4 “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 [9.16.1](#).

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	OK Cancel	
System Settings		
Provisioning & Software Update		
SIP		
User Administration		
Time zones		
SNMP		
DB Management		
Event Log		
Sites		
Base Stations		
SIP Users/Devices		
WLAN		
System Features		
Licenses		
Info		
Support		

	Local user account	
Account type	Full access ▾	
Active	☒	
User name	omm	
Old password	••••••	
Password		
Password confirmation		
Password aging	None ▾	

- **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 (for example, 'qwert')
- **Password aging:** A timeout for the password can be set. Select the duration, the password should be valid.

6.4.5 “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.

Status	Time zones			
System	Default			
System Settings	118 Time zones			
Provisioning & Software Update	Name	ID	UTC difference	DST
SIP	✎ Africa Central West	AFC	+1 h	✗
User	✎ Africa Central East	AFD	+2 h	✗
Administration	✎ Africa East	AFE	+3 h	✗
Time zones	✎ Afghanistan	AFG	+4.50 h	✗
SNMP	✎ Africa West	AFW	0 h	✗
DB Management	✎ Alaska	AK	-9 h	✓
Event Log	✎ Aleutian Islands	AKW	-10 h	✗
Sites	✎ Armenian Standard Time	ARM	+4 h	✓
Base Stations	✎ Asia UTC+4	AS4	+4 h	✗
SIP Users/Devices	✎ Asia UTC+5	AS5	+5 h	✗
WLAN	✎ Asia UTC+6	AS6	+6 h	✗
System Features	✎ Asia UTC+7	AS7	+7 h	✗
Licenses	✎ Asia UTC+8	AS8	+8 h	✗
Info	✎ Asia UTC+9	AS9	+9 h	✗
Support	✎ Atlantic	ATL	-4 h	✓
	✎ Australia East	AUE	+10 h	✓
	✎ Australia North	AUN	+9.50 h	✗
	✎ Australia East (No DST)	AUQ	+10 h	✗
	✎ Australia South	AUS	+9.50 h	✓

The date and time are provided by the OMM to the Mitel 142 and Mitel 600/700 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 [6.4.5.1](#))
- Resetting time zones (see section [6.4.5.2](#))

6.4.5.1 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.

6.4.5.2 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.

6.4.6 “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.

Status	SNMP	
System	OK Cancel	
System Settings		
Provisioning & Software Update		
SIP		
User Administration		
Time zones		
SNMP		
DB Management		
Event Log		
Sites		
Base Stations		
SIP Users/Devices		
WLAN		
System Features		
Licenses		
Info		
Support		

Read-only community	
System contact	
☐	
Trap community	
Trap host IP address	

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 [9.18](#).

6.4.7 “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.

Status	Database management	
System		
System Settings		
Provisioning & Software Update		
SIP		
User Administration		
DB Management		
Event Log		
Base Stations		
SIP Users/Devices		
WLAN		
Licenses		
Info		
	Manual import	
	Protocol	FILE ▾
	Server	
	Port	
	User name	
	Password	
	Password confirmation	
	File	Choose File No file chosen
	Use provisioning security configuration	☐
	Load	
	Manual export	
	Protocol	FILE ▾
	Server	
	Port	
	User name	
	Password	
	Password confirmation	
	File	220112_SD_8_3_1F102F118A_omm_conf.gz
	Use provisioning security configuration	☐
	Save	

The OMM database can be:

- manually imported from the Web browser’s file system or from an external server (see section [6.4.7.1](#)),
- manually exported to the Web browser’s file system or to an external server (see section [6.4.7.2](#)),
- automatically exported to an external server when configuration modifications are done (see section [6.4.7.3](#)).

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.

6.4.7.1 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 (for example, 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 provisioning security configuration: Enables the use of the system-wide certificate validation settings, as configured on the **Certificates** page (see section [6.4.2.14](#)).

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.

6.4.7.2 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 provisioning security configuration: Enables the use of the system-wide certificate validation settings, as configured on the **Certificates** page (see section [6.4.2.14](#)).

6 Press the **Save** button.

6.4.7.3 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 (for example, 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 [9.5.4](#) and section [9.6](#).

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 **Path:** Enter the path 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 provisioning security configuration:** Enables the use of the system-wide certificate validation settings, as configured **Certificates** page (see section [6.4.2.14](#)).
- 8 Press the **OK** button.

6.4.8 “EVENT LOG” MENU

The **Event log** page displays important event information on OMM system functions, for example, security aspects. A more detailed system log is available by configuring the **Syslog** function in the **Support** menu (see section [6.12.2](#)).

Status	Event Log			
System	Clear			
System Settings				
Provisioning & Software Update	Severity	Count	Time (UTC)	Event
SIP	2	1	2021/05/10 05:36:17.612	AXI : [202] New secure connection from 10.8.128.111:49854
User Administration	2	1	2021/05/06 17:00:14.401	AXI : [202] New secure connection from 10.8.128.111:61907
Time zones	2	1	2021/05/04 13:24:44.310	AXI : [202] New secure connection from 10.8.137.28:60128
SNMP	2	1	2021/04/30 07:11:40.334	AXI : [202] New secure connection from 10.8.128.57:54214
DB Management	2	1	2021/04/29 17:26:08.844	AXI : [202] New secure connection from 10.8.136.66:61290
Event Log	2	1	2021/04/23 06:05:48.786	AXI : [202] New secure connection from 10.8.130.42:63879
Sites	3	24	2021/04/22 11:19:10.452	DSIP: SIP registration to 10.103.35.71 failed - timed out
Base Stations	2	1	2021/04/22 07:15:27.521	AXI : [202] New secure connection from 10.8.138.249:63796
SIP Users/Devices	2	1	2021/04/21 16:49:13.901	AXI : [202] New secure connection from 10.8.130.188:49360
WLAN	2	1	2021/04/21 12:09:55.310	AXI : [202] New secure connection from 10.8.138.11:64200
System Features	7	1	2021/04/20 05:48:22.550	PROV: Finished provisioning service (trigger: Restart).
Licenses	7	1	2021/04/20 05:48:22.550	PROV: Software is up to date.
Info	7	1	2021/04/20 05:48:19.592	PROV: Software update started.
Support	7	1	2021/04/20 05:48:19.592	PROV: Starting provisioning service (trigger: Restart).
	7	1	2021/04/20 05:48:03.944	PROV: Provisioning service's start up phase finished.
	2	1	2021/04/20 05:46:25.407	IPL : 2 of 2 RFPs connected
	7	1	2021/04/20 05:46:04.896	CERT: All secure certificates and private key imported after stz
	7	1	2021/04/20 05:46:03.859	PROV: Provisioning is in start up phase. No action will be proci
	0	1	2021/04/20 05:46:01.828	CNF : SIP-DECT 8.3-GD18 (DIAG) private patch from jenkins 2

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

6.5 “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.
- **Wideband Audio G.722, 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.

Status	Sites					
System	New					
Sites	1 Site					
Base Stations	ID	Name	Wideband Audio G.722	SRTP	Enhanced DECT security	Base Stations
SIP Users/Devices	1	default	×	×	×	2
WLAN						
System Features						
Licenses						
Info						
Support						

You can perform the following tasks:

- create a new site (see section [6.5.1](#))
- edit a site (see section [6.5.2](#))
- delete a site (see section [6.5.3](#))

6.5.1 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.
- **Wideband Audio G.722:** Select the checkbox to enable wideband audio G.722
- **Enhanced DECT security:** Select the checkbox to enable enhanced DECT security.
- **SRTP:** These capabilities must be options that are enabled or disabled, preferred only, and SrtPPlusRtp. In sites, which are configured to provide this functionality, exclusively 3rd and 4th generation RFPs are applicable.
 - Only: Only SRTP calls will be accepted, all other will be rejected (the audiopart of the SDP contains RTP/SAVP).
 - Preferred: All calls will be initiated as secured, but accepted if they are not secured (the audio part of the SDP contain RTP/AVP).
 - Disabled: Only RTP calls will be initiated as not ciphered and incoming ciphering algorithm will be not accepted. All communications are established unencrypted.
 - SrtPPlusRtp: All calls will be initiated as secured, but accepted if they are not secured (the audio part of the SDP contains 2 m-lines RTP/SAVP and RTP/AVP).
- **Emergency Location Identification Number (ELIN):** Enter the system-wide valid emergency call identification number. This value is used when there is no more specific ELIN set. The parameter can be used for small systems in which the same ELIN should be used for all base stations.

Note: Supported by 3rd and 4th generation RFPs where these features are enabled.

3 Press the **OK** button to save your changes.

6.5.2 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.

6.5.3 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.

6.6 “BASE STATIONS” MENU

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

Status

System

Sites

Base Stations

DECT Cluster 1

SIP Users/Devices

WLAN

System Features

Licenses

Info

Support

Base Stations

Capturing unconfigured DECT base stations

Start

Capture allowed: ✗

Sorted by DECT clusters

2 Base Stations

DECT Cluster 1: 2 Base Stations

ID	Name	MAC address	IP address	HW type	Site	RPN	Reflective environment	Connected	Active
0000	OMM RFP 1	08:00:0F:C3:DE:FD	10.103.35.150	RFP 47	1	00	✗	✓	✓
0001	RFP 43	00:30:42:17:8E:3E	10.103.35.172	RFP 43	1	01	✗	✓	✓

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 [6.8](#)).
- **Sites:** The base stations are sorted by sites (see section [6.5](#)). 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 [6.6.3](#)).
- **MAC address:** Indicates the base station's MAC address (see section [6.6.3](#)).
- **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 [6.6.2](#)).
- **Site:** Indicates the site the base station is assigned to (see section [6.5](#)).
- **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 [6.6.3](#)).

- **Connected:** Indicates if the base station is connected to the OMM (see section [6.6.1](#)).
- **Active:** Indicates if the base station is active (see section [6.6.1](#)).

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

- Create and change base stations (see section [6.6.3](#)).
- Capture base stations (see section [6.6.4](#)).
- Delete base stations (see section [6.6.5](#)).
- Find my SIP-DECT base station (see section [6.6.6](#)).

6.6.1 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.

6.6.2 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.

6.6.3 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 [6.5](#)), select the site the RFP is assigned to.

- **Emergency Location Identification Number (ELIN):** Enter the system-wide valid emergency call identification number. This value is used when there is no more specific ELIN set. The parameter can be used for small systems in which the same ELIN should be used for all base stations.

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 [9.2](#).
- **Reflective environment:** Within areas containing lot of reflective surfaces (for example, 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 600/700 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.

With active DECT XQ , RFP 44 supports only 2 calls and other RFPs support 4 calls.

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 43 WLAN” and “RFP 48 WLAN” only. For details about WLAN configurations please see section [9.17](#).

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 [9.17.1](#).

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 [6.8.1](#)). 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.

- **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 1300 MBit/s (ac) 3x3 MIMO

6.6.4 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).

6.6.5 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](#).

6.6.6 FIND MY SIP-DECT BASE STATION

Perform the follownig steps to determine the IP address of the OMM using the *Find my SIP-DECT base station* java script 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.

1. Download the java script (FindMySIP-DECTbasestation.zip) from Mitel Software Download Center.
2. Extract the compressed folder.
3. Open the index.html file in the extracted folder.
The **Find my SIP-DECT base station** webpage opens from your local drive.
4. The search IP range is initialized automatically. You can adjust the IP address range if needed.


Find my SIP-DECT base station

My IP address

Base station's IP address range
 -

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.


Find my SIP-DECT base station

My IP address

Base station's IP address range
 -

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.

6.7 “SIP USERS/DEVICES” MENU

The **SIP Users/Devices** page provides an overview of all configured SIP users and devices sorted by their phone number. The complete list is split up into sub lists containing up to 100 entries each.

The **SIP Users/Devices** table provides the following information about a SIP user or device:

- **Display name:** Indicates the name of the user.
- **Number/SIP user name:** Indicates the internal call number of the user.
- **IPEI:** Indicates the IPEI of the related phone, if any.
- **Subscribed:** Indicates if the user phone is subscribed to the system.
- **Download:** This column is displayed only if the “Download over Air” feature is started successfully. It provides information about the download status of the DECT phone software (see section [9.21](#)).

The following tasks can be performed on the **SIP Users/Devices** page:

- Create; modify; and delete unbound, fixed, or dynamic linked users and devices.
- Show the current user-device relation type (unbound, fixed, or dynamic linked).
- Switch the user-device relation.

6.7.1 USER-DEVICE RELATIONSHIP ICONS

The following table describes the user-device relationship icons on the **SIP Users/Devices** page:

Icon	Description
	Fixed user-device relation
	Dynamic user-device relation
	Unbound user; no device relation; user is not bound to a device

	Unbound device; no user relation; device is not bound to a user

6.7.2 CREATING SIP USERS/DEVICES

Perform the following steps to create a new SIP user or device:

- 1 Click the **New** button beside **Create a new DECT Phone** on the **SIP Users/Devices** page. The **New SIP user** window opens.
- 2 Enter the values for the following fields in the **New SIP user** page.
- 3 Click the **OK** button.

The following parameters can be set in the **New SIP user** page:

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.
- **Alternative display number:** Certain call servers assign a single number to a user while assigning different individual numbers to the user's devices. To show the original user number on the device rather than the individual device number, use the **Alternative display number** parameter to configure an alternative display number for the user.
- **PIN:** The DECT phone default PIN is set to 0000. It is the same default PIN as for the local DECT phone feature.
- **User/Device relation:** Specifies the user-device relationship type as **Fixed** or **Unbound**.
- **IPEI:** This optional setting is the DECT phone IPEI number. On a Mitel DECT 142 / Mitel 142d DECT phone, the IPEI can be found along the following path of the DECT phone menu: **Main menu > Phone settings > System**. On a Mitel 600/700 DECT phone, the IPEI can be found in the **System** DECT phone menu. Consult the DECT phone user guide for more information.
- **DECT authentication code:** This parameter 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) and it is an optional parameter. 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 for data search within wildcard subscription (because the IPEI is not configured, which selects the data otherwise).
- **SOS number, ManDown number:** SOS and ManDown are calling numbers that are automatically called as soon as an SOS or ManDown event occurs. 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 when an SOS or a ManDown event occurs. See /31/ for details.

- **Voice mail number:** Specifies the number that will be automatically called as soon as a voice mail call is initiated on the Mitel 600/700 DECT phone. If no individual voice mail number is configured in this field, the system-wide voice mail number is used (see also the **System settings** menu, section [6.4.1.9](#)). If there is no voice mail number configured (neither individual nor the system-wide) or if 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 the 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 that will be used during SIP registration and authentication. If no name is specified, the number will be used by default.
- **Password, Password confirmation:** The password is used during SIP registration and authentication. Enter 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 an XSI request (for example, /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 the **System menu > Administration** on the Mitel 600/700 DECT phone. To prevent the user from setting the time, 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. Set a new PIN here if the user has 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.

6.7.3 EDITING SIP USER/DEVICE SETTINGS

Perform the following steps to edit an existing SIP user or device:

- 1 Click the  icon beside the SIP user or device you want to edit on the **SIP Users/Devices** table. The **Configure SIP User/Device** window opens.
- 2 Enter values in the fields on the **Configure SIP User/Device** page. For details about the fields, see [6.7.2](#) section.
- 3 Click the **OK** button.

6.7.4 IMPORTING SIP USER OR DEVICE CONFIGURATION FILES

A set of SIP users or devices can also be configured by importing a configuration file.

Note: Before making any change to a live system, click [here](#) to download and view the sample input file.

- 1 On the **SIP Users/Devices** page, press the **Import** button. The **Manual user data import** page opens.
 - 2 Click **Download sample input file** to download the Microsoft® Excel® file.
 - 3 Open the downloaded file and follow the instructions in the **Data line structure** tab and input the corresponding data in the **User-Data-SampleSheet** tab.
 - 4 Save the **User-Data-SampleSheet** as a csv file with semicolon separator. Before you save the file, ensure you change the **List separator** from comma to semicolon.
- Note: To locate the **List separator** field:
- On **Windows 10**: Click **Start**, start typing **Control Panel**, select it, navigate to **Region > Additional Settings... > List separator**.
 - On **Windows 8**: Click **Start** and navigate to **Control Panel > Regional and Language Options > Additional Settings... > List separator**.
 - On **Windows 7**: Click **Windows/Start** and navigate to **Control Panel > Region and Language > Formats tab > Additional Settings... > List separator**.
- 5 Click **Browse** and select the **User-Data-SampleSheet.csv** file.
 - 6 Click **Import** to import the **User-Data-SampleSheet.csv** file.
 - 7 The parsing protocol can be viewed by pressing the referring **Log file** button. All successfully imported data records are presented in a list.
 - 8 Select the SIP users or devices you want to add to the OMM database by selecting the corresponding check boxes, and click **Add**.

Notes:

- All successfully stored records are marked green in the **Added** column.
 - Failed records are marked with a red star.
- 9 To read error hints in the referring log file, press the **Log file** button. Error hints can also be read in a syslog trace.
 - 10 To remove imported data entries, select the entries by selecting the check boxes beside the entries and press **Delete**. The selected entries are removed.

6.7.5 SEARCHING THE SIP USER OR DEVICE LIST

You can use the search function to search for a specific SIP user or device in the **SIP Users/Devices** list.

Perform the following steps to search for SIP user or device by using the number or IPEI:

- 1 On the **SIP Users/Devices** page, click the **Search** button.

The **Search SIP Users/Device** window opens.

- Enter the SIP user or device number or IPEI. At least one parameter must be specified. The number or IPEI that you specify must exactly match with a SIP user number or device number, or IPEI. If both, number and IPEI are specified, then a SIP user or device must exist in the OMM's database whose number and IPEI both match exactly; otherwise the search fails.

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

6.7.6 DELETING SIP USERS/DEVICES

Perform the following steps to delete a SIP user or device:

- On the **SIP Users/Devices** page, click the  icon beside the SIP user or device entry.
The **Delete SIP user?** window opens showing the current configuration for the selected SIP user or device.

- Click the **Delete** button.

For fixed, dynamically linked and unbound, the user and device are deleted based on the user-device relationship as shown in the following table:

Icon	Relation	Result
	Fixed user-device relation	User and device are deleted.
	Dynamic user-device relation	User is deleted. The device becomes unbound.
	Unbound user, no device relation, user is not bound to a device.	User is deleted.
	Unbound device, no user relation, device is not bound to a user.	Device is deleted.

6.7.7 CREATING FIXED OR UNBOUND LINKED USERS AND DEVICES

Perform the following steps to create linked SIP users and devices:

- Click **New** on the **SIP Users/Devices** page.
The **New SIP user** window opens.

General settings

Display name

Number/SIP user name

PIN

User/Device relation 

IPEI

DECT authentication code

Login/Additional ID

SOS number

ManDown number

Voice mail number

Number used for visibility checks ☐

- From the **User/Device relation** drop-down list, select **Unbound** or **Fixed** to set the user-device relation.

For more details about other fields in the **New SIP Users** page, see [6.7.2](#).

Notes:

- If the relation set to **Unbound**, a new unbound user is created. The IPEI and DECT authentication code parameters are not configured as they are associated with device data. No device dataset is created.
 - If the relation set to **Fixed**, a fixed user-device pair is created. A device dataset is created and the IPEI and DECT authentication code are configured.
3. Click **OK** to create the user or device.

During normal subscription, an unbound device is automatically created if **Auto-Create on subscription** is enabled and a fixed user-device dataset does not exist with a matching IPEI.

6.7.8 MODIFYING FIXED OR UNBOUND LINKED USERS AND DEVICES

Perform the following steps to modify linked SIP users and devices:

1. Click the  icon beside the SIP user or device for which you want to modify the user-device relation on the **SIP Users/Devices** table.
The **Configure SIP User/Device** window opens.

Configure SIP User/Device

General settings	
Display name	Test 1000
Number/SIP user name	1000
PIN	••••••••••••••••
User/Device relation	Dynamic 
IPEI	Fixed 265 7
DECT authentication code	Dynamic
Login/Additional ID	

2. Select **Dynamic** or **Fixed** depending on the user-device relation from the **User/Device relation** drop-down list.
The relationship between fixed user-device relationship and dynamic user-device relation (not between fixed user-device relationship and unbound) and vice versa can be modified.
3. Click **OK** to save your changes.

Note: When changing from **Fixed** to **Dynamic**, the DECT phone must be subscribed because an unsubscribed dynamic DECT phone is not defined in SIP-DECT.

6.7.9 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.

6.7.10 SUBSCRIBING DECT PHONES

After adding a SIP user or device configuration to the OMM, the DECT phone must be subscribed. The OMM must first be enabled to allow subscriptions from DECT phones.

6.7.10.1 Subscription steps, done by OMM Web service

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 subscription, select **Subscription** from the **Subscription** drop-down list on the **SIP Users/Devices** page.

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

Notes:

- Older DECT phones may not offer the option of entering an Authentication 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 [6.4.1.2 DECT settings](#)).
- 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 [6.4.1.2 DECT settings](#)).

6.7.10.1.1 Subscription steps, done by DECT phone

After the DECT phone configuration is complete on the OMM and the OMM begins 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 code is displayed on the top of the **General** section of the **SIP Users/Devices** page.

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

For **wildcard subscription**, an additional ID may be configured (see [6.7.10.2](#)).

6.7.10.2 Wildcard Subscription

If the IPEI is not configured, administrative effort can be minimized by using subscription. But in view of the loss of the additional security provided by IPEI check, this kind of subscription is allowed only within a short default time interval of 2 minutes.

To enable subscription, select **Wildcard subscription** from the **Subscription** drop-down list on the **SIP Users/Devices** page.

The OMM will allow a wildcard subscription during the set time interval. In case of a timeout, the permission is lost. Only subscriptions with IPEI continue to be allowed for a fixed period of 24 hours.

To achieve a selection of data during subscription (that is, the user name being assigned to the DECT phone), the field **Additional ID** can be set for 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 by typing the R-key and then typing the additional ID.

Please Note:

- The time is further limited if the feature 'Restrict subscription duration' is active (see [6.4.1.2](#) DECT settings).
- The input of the additional ID is supported only on Mitel 142 and Mitel 600/700 DECT phones. The value is not supported on third-party GAP phones. If GAP phones will subscribe wildcards, the first free DECT phone data record without any additional ID will be assigned.

6.7.11 AUTO-CREATE ON SUBSCRIPTION

Activate this option if unbound subscription of a SIP user or device should be allowed.

Auto-create on subscription allows the automatic subscription of DECT phones, without any device administration. This subscription method creates an unbound device dataset. The device is mapped to a specific user dataset when the user logs in to the phone.

To activate this feature, you must enable the Auto-create on subscription option and also specify the subscription mode to be FAC, OMM Web service, or OMP. See the *OM DECT Phone Sharing and Provisioning Guide* for more information.

To enable the Auto-create on subscription option by using the OMM Web service, select the **Auto-create on subscription** check box on the **SIP Users/Devices** page.

6.7.12 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 **SIP Users/Devices** 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 displays only 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 (for example, department or function).
Description 2	Additional textual description for a user (for example, 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 600/700 DECT phone) has been initiated.
VM number	Voice mail number (dialed by a long press of '1' key on the Mitel 600/700 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 the login procedure at the DECT phone; or ID used for wildcard subscription during the 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 (that is, where the device is currently registered)
VIP	To guarantee a minimum blackout for very important persons (for example, emergency user) the SIP (re-)registration of such persons 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 having 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

Authenticate logout	User log out requires authentication. Yes = user logout with authentication No = user logout without authentication
Auto logout on charging	A user can be logged out of the device automatically when the Mitel 600/700 DECT phone is placed in the charger cradle. Yes = automatic logout when put in charger No = no automatic logout
Sending messages	User's permissions to send text messages using the Mitel 600/700 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 600/700 DECT phone. Yes = user is authorized to send vCards No = user is not authorized to send vCards
Receiving vCards	Indicates whether the user accepts received vCards. Yes = incoming vCards are accepted No = incoming vCards are not accepted
Tracking	Tracking forces the Mitel 600/700 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. Yes = locating the user is permitted No = not permitted
Keep personal dir.	The local directory of the Mitel 600/700 DECT phone is usually the user's personal directory and is cleared at logout. If deleting the directory content is not preferred, 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, or 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. If enabled, an incoming call takes precedence over an active call. The active call is placed on hold and the incoming call is automatically answered. When disabled, the DECT phone treats an incoming call as a normal call.
Monitoring mode	SIP-DECT supports a User Monitoring feature to check the availability of a user to receive calls or messages. On = monitoring feature is active Off = monitoring feature is not activated
Conference server type	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
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 are not used for XSI directory access).
User service auth. name	Authentication name for XSI service (if SIP credentials are not used for XSI directory access).
User service password	Password for XSI service (if SIP credentials not used for XSI directory access).
Key lock enabled	Key lock status of the DECT phone. Yes = Key lock is enabled No = Key lock is disabled
Key lock PIN	PIN to allow access to the Security menu and to lock the phone.
Key lock timeout	Automatic key lock timer (in seconds) selected for the DECT phone.
Device status	
IPEI	International Portable Equipment Identifier (globally unique identifier of the DECT phone).
HW type	Hardware type of 600/700 DECT phone or 142d; otherwise <i>unknown</i> .
SW version	Version of the software on the Mitel 600/700 DECT phone.
Subscribed	Subscription status of the DECT phone. Yes = DECT phone is subscribed No = DECT phone is not subscribed
Encryption	DECT encryption status. Yes = Encryption is enabled No = Encryption is disabled
Capability "Messaging"	Messaging capability of the DECT phone. Yes = DECT phone supports messaging No = DECT phone does not support messaging
Capability "Enh. Locating"	Enhanced locating capability of the DECT phone. Yes = DECT phone supports enhanced locating No = DECT phone does not support enhanced locating

Capability "CoA profile"	CoA capability (Central DECT phone configuration over air) of the DECT phone. Yes = DECT phone supports CoA No = DECT phone does not support CoA
Device auto-created	Auto-creation occurs when the DECT phone dataset is automatically generated in the OMM's database during subscription. No administrative task is required on the SIP-DECT system to subscribe a DECT phone in this mode. Yes = DECT phone has been subscribed in auto-create mode No = DECT phone has not been subscribed in auto-create mode
Default CoA profile loaded	A default CoA profile (Central DECT phone configuration over air) can be sent to a 600/700 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.

6.8 "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 43 WLAN.

Note: You cannot activate the WLAN function for the OMM.

For a detailed description on WLAN configuration, see the section [9.17](#).

6.8.1 "WLAN PROFILES" MENU

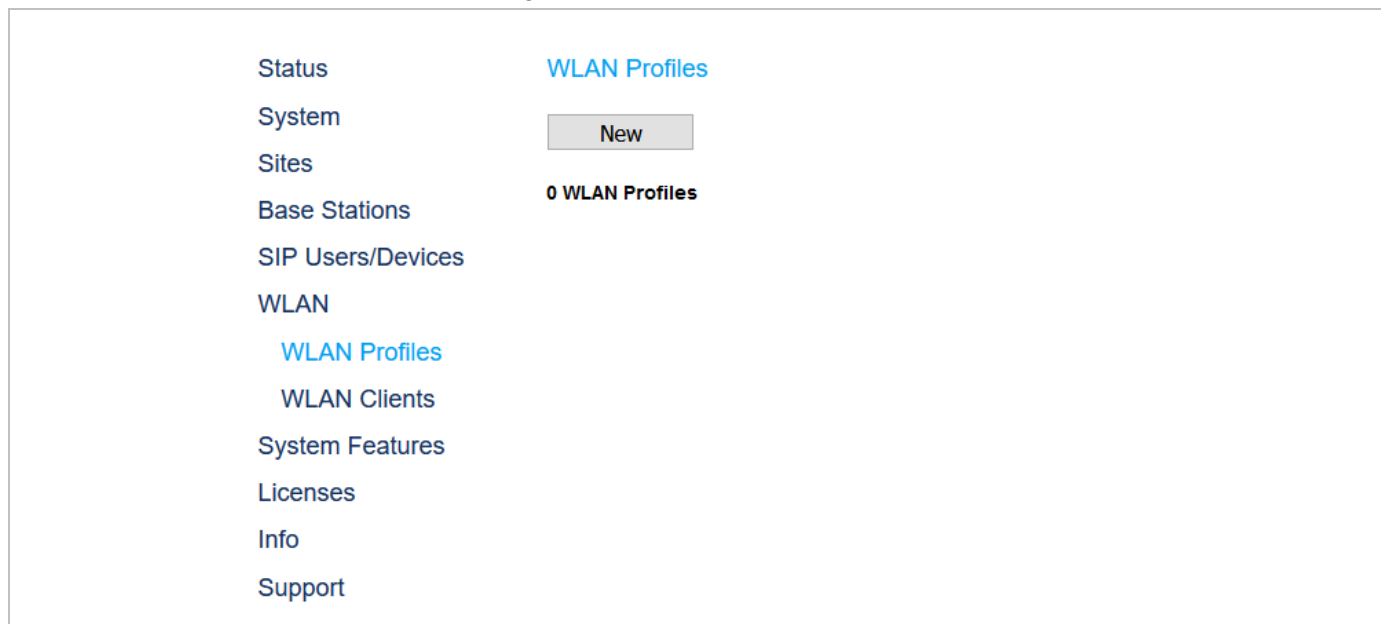
WLAN settings are grouped in WLAN profiles. You need at least one WLAN profile that can be assigned to one or more WLAN-RFPs. You can define more than one WLAN profile, to a maximum of 20 WLAN profiles. You can manage / change the desired WLAN settings for a group of WLAN-RFPs by changing their assigned 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 43 WLAN	RFP 43/48 (profile can be used for both RFP types max 802.11n possible)
RFP 48 WLAN	RFP 43/48 (profile can be used for both RFP types max 802.11n possible) RFP 48 (profile can be used for RFP 48 max 802.11ac possible)

- **HT40** (RFP 43/48 WLAN): In 802.11n HT40 combines two 20Mhz channel to reach higher bandwidth.
802.11n
RFP43 2 Antenna max 300 MBit/s
RFP48 3 antenna max 450 MBit/s
- **HT80** (RFP 48 WLAN): In 802.11ac combines up to 4 20Mhz channel to reach higher bandwidth (80Mhz). Increases data rate up to 1300 MBit/s (3x3 MIMO).

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



You can:

- create and change WLAN profiles (see section [6.8.1.1](#))
- delete WLAN profiles (see section [6.8.1.2](#))
- export WLAN profiles (see section [6.8.1.3](#))

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 [6.6.3](#)).

6.8.1.1 Creating and Changing WLAN Profiles

You need at least one active WLAN profile in order to operate the WLAN function for an RFP 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 43/48** or **RFP 48**) from the **WLAN profile type** selection list. Profile 43/48 can be used on both. Profile 48 is only supported by RFP 48.

- 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 [6.6.3](#)). 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 (for example, "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, for example, 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, for example, 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 [9.17](#) and [9.12](#)).
- **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 for example, that is critical for battery powered WLAN clients.
- **RTS threshold** (bytes, 0..4096, default: 2347): 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.

- **802.11 mode:** RFP 43/ RFP 48 selection list: 802.11bg /802.11b only / 802.11g only / 802.11abg /802.11n, default: 802.11bg. On the **RFP 48** profile you can choose additionally 802.11ac (only available for RFP 48)..

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

- **HT40** (RFP 43/48 WLAN): In 802.11n HT40 combines two 20Mhz channel to reach higher bandwidth.
802.11n
RFP43 2 Antenna max 300 MBit/s
RFP48 3 antenna max 450 MBit/s
- **HT80** (RFP 48 WLAN): In 802.11ac combines up to 4 20Mhz channel to reach higher bandwidth (80Mhz). Increases data rate up to 1300 MBit/s (3x3 MIMO)
- **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.

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, for example, 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: WPA2 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): You can limit WLAN access for WLAN clients with specified MAC addresses. Note, that without encryption this should not be used for security reasons. It is recommended to use Radius with user or certificate authentication. You can configure a list of MAC addresses that are allowed to connect via the MAC access filters tab on the WLAN profile page. The MAC filter list is limited to 512 entries per WLAN profile.
- **BSS isolation** (on / off, default: off): In a standard WLAN setup, each WLAN client can contact other WLAN clients. For special purposes (for example, “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, 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 WPA encryption is re-negotiated. This parameter can be set in the WPA mode of the web interface and the OM portal interface.

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, or 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, for example, 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.

6.8.1.2 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 [6.6.3](#)).
- 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.

6.8.1.3 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).

6.8.2 “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.

6.9 “SYSTEM FEATURES” MENU

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

6.9.1 “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 for example, 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.

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

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

The result of the conversion is not sent to the DECT phone to be displayed or entered in the call log ¹.

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

- creating and changing “Digit treatment” entries (see section [6.9.1.1](#))
- deleting “Digit treatment” entries (see section [6.9.1.2](#))

6.9.1.1 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 numbers has the same character set as the user telephone number (for example, :”+*~#;,-_!\$%&/()=?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 600/700 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 for example, “1, 2” (see section [6.5](#)). 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.

6.9.1.2 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.

¹ 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.

6.9.2 “DIRECTORY” MENU

The **Directory** menu allows you to manage connections to one or more LDAP, XML or XSI 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 (for example, 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.

6.9.2.1 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 section (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 On the **Directory** page, click the pencil icon beside an existing directory entry in the list.
The **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: • 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).	✓	✓	✓
LDAP Security	Enables secure LDAP . Possible values: • None	✓		

Parameter	Description	LDAP	XML	XSI
	- STARTTLS - LDAPS			
Search base	Location in the directory from which the search begins (for example, "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: "<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).	✓		
Protocol	Transfer protocol used to communicate with the XML or XSI directory server (http or https).		✓	
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 provisioning security 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.

6.9.2.2 Deleting Directory Entries

- 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.
- Press the **Delete** button.

6.9.3 "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 On the **Directory (comp. mode)** page, or click the pencil icon beside an existing entry.
The **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.

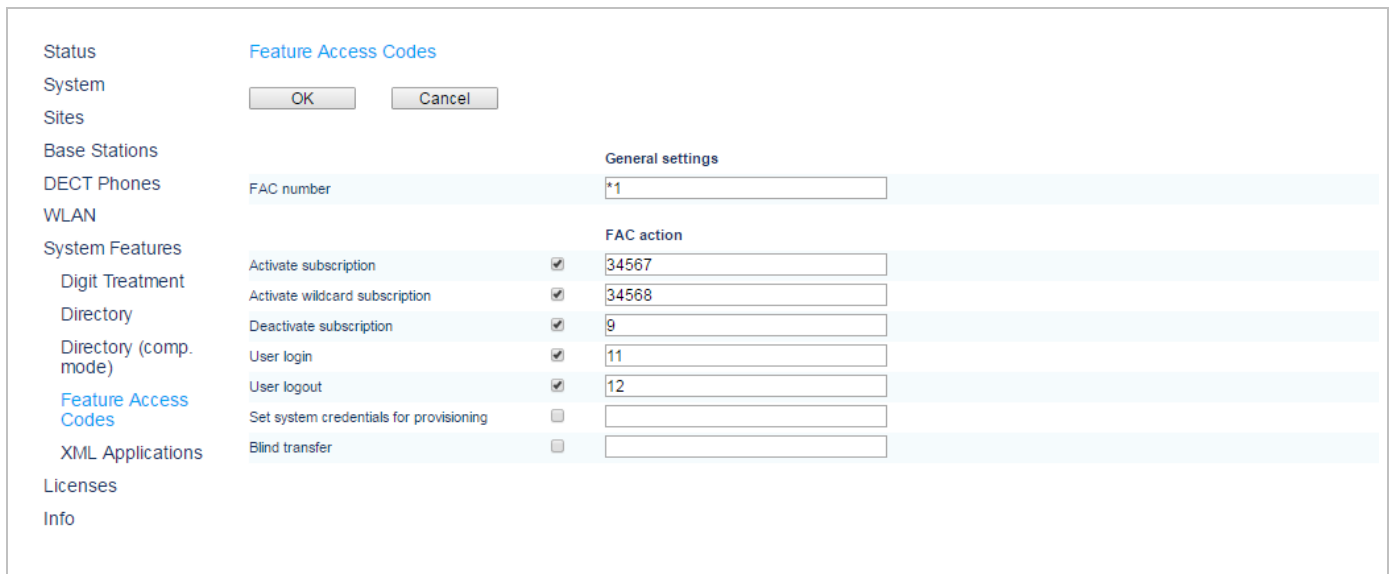
Parameter	Description	LDAP	XML
Active	Enables or disables the directory entry on the DECT phone.	✓	✓
Order	Specify where you want the directory entry to appear in the list.		
Type	Interface type supported by the directory server. Possible values: LDAP or XML.	✓	✓
LDAP Security	Enables secure LDAP . Possible values: • None • STARTTLS • LDAPS	✓	
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).		✓
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 (for example, "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: • "<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).	✓	

Parameter	Description	LDAP	XML
Path (and parameters)	URL (with parameters, if required) to the XML directory on the XML directory server.		✓

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

6.9.4 “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.



General settings		
FAC number		*1
FAC action		
Activate subscription	☒	34567
Activate wildcard subscription	☒	34568
Deactivate subscription	☒	9
User login	☒	11
User logout	☒	12
Set system credentials for provisioning	☐	
Blind transfer	☐	

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 600/700 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).

6.9.5 ”XML APPLICATIONS” MENU

The SIP-DECT XML terminal interface allows external applications to provide content for the user on the Mitel 600/700 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 600/700 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 600/700 DECT phones only display icons in idle state. In an active call state, only the two softkeys below the display indicate the active feature.

	ID	Name	Server	Active	Tasks
Configuration	0	Caller list		☑	
Status	1	Redial list		☑	
System	2	Presence		☑	Create
Sites	3	Server menu		☑	Configure/Show
DECT base stations	4	Action URI		☑	Delete
WLAN	5	Feature access codes		☑	
DECT phones	6	Call completion		☑	
Conference rooms	7	Park call		☑	
System features	8	Unpark call		☑	
General settings	9	Pickup		☑	
Feature access codes	10	Take		☑	
Alarm triggers	11	Call forward		☑	
Digit treatment	12	Call routing		☑	
Directory	13	Call protection		☑	
Directory (comp. mode)	14	Voice box		☑	
XML applications	15	Hotkey		☑	
CoA profiles					
Licenses					
Support					

The following table summarizes the predefined XML application hooks:

Hook	Description	DECT Phone menu
Caller list	Hook to replace the local caller list. You can use this hook to enable the centralized call log feature (MX-ONE systems only). "Call log support provided on an external server": 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	>>> > Info > Caller List

Hook	Description	DECT Phone menu
	the DECT phone for the user. The URL-path in the configuration differs from " <i>CSIntegration?object=history</i> " which is an indication for the OMM centralized call log feature.	
Redial list	Hook to replace the local redial list. You can use this hook to enable the centralized call log feature (MX-ONE systems only). "OMM centralized Call log support provided by the OMM internally": 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". The URL-path in the configuration be " <i>CSIntegration?object=history</i> " which is an indication for the OMM centralized call log feature.	>>> > Info > Redial List
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
Hotkey	Hook used by external application servers to provide additional functions for DECT telephone users via the SIP-DECT XML terminal interface. You can program this hook on a selected key of Mitel 602d DECT phone either manually or via CoA. The XML hook can be configured via OMP or OMM Web UI.	

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.

6.9.5.1 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.
 - **Port:** Specifies the port on 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.

6.9.5.2 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.

6.9.5.3 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.

6.10 “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](#).

The screenshot displays the 'Licenses' configuration page. On the left is a sidebar with navigation links: Status, System, Base Stations, SIP Users/Devices, WLAN, Licenses (highlighted), and Info. The main content area has a header 'Licenses' and a warning: 'Changing these settings may cause the OpenMobility Manager to be reset.' Below this are 'OK' and 'Cancel' buttons. The configuration is organized into sections: 'License settings' with fields for 'Installation ID' (271520138) and 'License file import' (Choose File, No file chosen, Import button); 'General' with 'License type' (Built-in license for up to 5 DECT base stations) and 'PARK' (1F102F118A, (31100570430504)); 'System' with 'Number of DECT base stations' (5, shown with a progress bar and 'Mitel SIP-DECT System License XXX'); 'Messaging' with 'Reception of text messages (Emergency, Locating alert) and enhanced messaging features' (marked with a red X and 'Mitel SIP-DECT Messaging & Alerting License Enterprise'); and 'Locating' with 'Number of users allowed to be located' (—, 'Mitel SIP-DECT Locating User License XXX') and 'OM Locating application' (marked with a red X, 'Mitel SIP-DECT Locating Server License').

6.11 “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.

6.12 “SUPPORT” MENU

Support section summarizes existing SIP-DECT maintenance functions. These functions can be configured in one place and are clearly distinguished from other SIP-DECT features. The Maintenance section comprises:

- **DECT phone firmware update:** activation of the firmware update and configuration of an alternative update source
- **Syslog server:** activation and Syslog server address
- **System dump:** start of a manually local system dump onto the PC running the OMP
- **Core dump:** configuration of a specific server to which core dumps are sent.

Status	Support	
System	OK Cancel	
Sites		
Base Stations		
SIP Users/Devices		
WLAN		
System Features		
Licenses		
Info		
Support		

	DECT phone's firmware update	
Activate firmware update	☒	
Configure specific source	☐	
Protocol	FTP ▾	
Server		
Port		
User name		
Password		
Password confirmation		
Path	/600.0	
Use common certificate configuration	☐	
	Syslog	
Active	☐	
IP address		
Port	514	Default
	System dump	
Trigger	☐	
Time	00 : 00	
Configure specific source	☐	Dump

6.12.1 DECT PHONES FIRMWARE UPDATE

With SIP-DECT 6.0 or later, the DECT base station software images (iprpf3G.dnld and iprpf4G.dnld) contains the Mitel 600/700 DECT phone software. For specific maintenance purposes only, you can configure a URL to use an alternative DECT phone software image. The Mitel 600/700 DECT phone firmware packages are delivered in the “600.dnld/700.dnld” file for the OMM running on a DECT base station.

- **Activate firmware update:** Enables or disables the “Download over Air” feature. The OMP provides a DECT phone firmware update over the air when this feature is activated. For more information on, see section [9.21](#).
- **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 provisioning security configuration:** Enables the use of the system-wide certificate validation settings for this URL, as configured on the **System -> Provisioning -> Provisioning certificates** page (see section [6.4.2.14](#)).

6.12.2 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.

6.12.3 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 provisioning security configuration:** Enables the use of the system-wide certificate validation settings for this URL, as configured on the **System -> Provisioning & Software Update -> Certificates** page (see section [6.4.2.14](#)).

6.12.4 CORE DUMP

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.
- **Path:** Specifies the location of the core files on the external file server.

7 OM MANAGEMENT PORTAL (OMP)

7.1 OVERVIEW

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

7.2 INSTALLATION

OMP is provided as an AdoptOpenJDK JAVA 11 application.

Notes:

- A locally installed Java Runtime Environment (JRE) is not required to run the application package. The JRE is now delivered as part of OMP application package.
- The OMP for Microsoft Windows installer includes the AdoptOpenJDK (OMP_Runtime_Image_Win.zip) runtime environment file for 64-bit Windows. 32-bit versions are not supported.

Perform the following steps to install OMP on a Windows environment or a Linux system:

- Windows:
 - Run the *OMP_Installer_SIP-DECT_8.3.exe* file and follow the on screen installation instructions.
After successful installation of the application, OMP is accessible from the Start menu in the folder path Start Menu/Programs/Mitel/SIP-DECT 8.3/OMP of the Windows system.
 - Alternatively, extract the files from *OMP_Runtime_Image_Win.zip* to access the application. After extracting the zip files, the application can be started by running the *omp.bat* file in *OMP_Runtime_Image_Win\bin* folder.
- Linux:
 - Run the command `tar xfvz OMP_Runtime_Image_Linux.tar.gz` to extract the application.
 - Start OMP by running the script `omp` in the extracted directory *OMP_Runtime_Image_Linux/bin*.

To uninstall the application, run the *Uninstall OMP* file in the folder path *Start Menu/Programs/Mitel/SIP-DECT 8.3*.

7.3 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 [6.4.1](#).

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 [7.6](#)). 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 [7.17](#)).

7.4 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.

7.5 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, for example, system and RFP statistics and RFP synchronization monitoring.

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

-  Configuration mode
-  Monitor mode

Main menus

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

- **General** menu, see section [7.15](#).
- **Help** menu, see section [7.17](#).

Navigation section

Both configuration and monitor mode contain a navigation section. This section contains the mode-dependent 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 **Basic 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 [7.7.2.2](#)).

- 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 **Basic settings** menu (see also section [7.7.1](#)).

- 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**.

7.6 “STATUS” MENU

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

- Overview (see section [7.6.1](#))
- DECT base stations (see section [7.6.2](#))
- Users (see section [7.6.3](#))
- Devices (see section [7.6.4](#))
- Sites (see section [7.6.5](#))
- Conference (see section [7.6.6](#))
- Provisioning (see section [7.6.7](#))
- Provisioning health report (see section [7.6.8](#))

7.6.1 OVERVIEW

The “Overview” tab consists of a “System” section providing general system health states information and a “Features” section 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 State	Health State	Feature	Health State
Uptime	0 Day(s) 00 h 00 min	OM Integrated Messaging & Alerting service	✓
Licenses	✓	User data server	✓
Standby OMM	✗	MOM control	✗
Synchronization state	✓	802.1x state	✗
DECT base stations	✓	OMM certificate server	✗
DB import/export	⚠	Provisioning certificate server	✗
Downloading new firmware to portable parts	⌚	802.1x certificate server	✗
Provisioning	⌚	SIP certificate server	✗
OMM configuration file processing	✓		
Emergency location configuration	✗		

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
- **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.
- **Emergency location configuration:** Specifies if ELIN support is enabled

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)
- **User data server:** User data server health state (optional)
- **MOM control:** Controlled by MOM and indicates the health state of MOM (optional)
- **802.1x control:** 802.1x loaded certificate health state (optional)
- **OMM certificate server:** OMM loaded and valid certificate health state (optional)
- **Provisioning certificate server:** Loaded and available provisioning configuration server certificate health state (optional)
- **802.1x certificate server:** 802.1x loaded and available server certificate health state (optional)
- **SIP certificate server:** SIP certificate server health state (always active)

Health states can have the following values:

-  – inactive or unknown
-  – error
-  – OK
-  – Warning
-  – Delay during startup phase

7.6.1.1 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.

7.6.2 DECT BASE STATIONS

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

Section	Item	Value
General	Total	2
	Connected	2
	Standby misconfigured	0
	Version mismatch	0
	802.1X configuration mismatch	0
DECT	DECT switched on	2
	DECT running	2
	Used clusters	1
	Used paging areas	1
WLAN	WLAN switched on	0
	WLAN running	0
	Profiles	0

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

- **Total:** Total number of RFPs configured
- **Connected:** Number of RFPs connected to OMM
- **Standby misconfigured:** Number of connected RFPs with wrong standby configuration
- **Version mismatch:** Number of connected RFPs running with wrong software version
- **802.1X Configuration mismatch:** Number of connected RFPs whose 802.1x configuration is not active or is different from OMM.

The “DECT” section 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” section 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

7.6.3 USERS

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

The screenshot displays the 'Users' configuration page. The sidebar on the left lists various configuration categories, with 'Users' being the active section. The main content area is divided into three sections:

- General:** Contains six counters with input fields:
 - Total: 2
 - SIP registered: 2
 - Monitored active: 0
 - Monitored passive: 0
 - Sending messages permission: 2
 - DECT locatable: 0
- User monitoring states:** Contains three counters with input fields:
 - Warning: 0
 - Unavailable: 0
 - Escalated: 0
- Number for visibility checks:** Contains a single input field for 'Number/ SIP user name' with the value 4368.

The “General” section 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

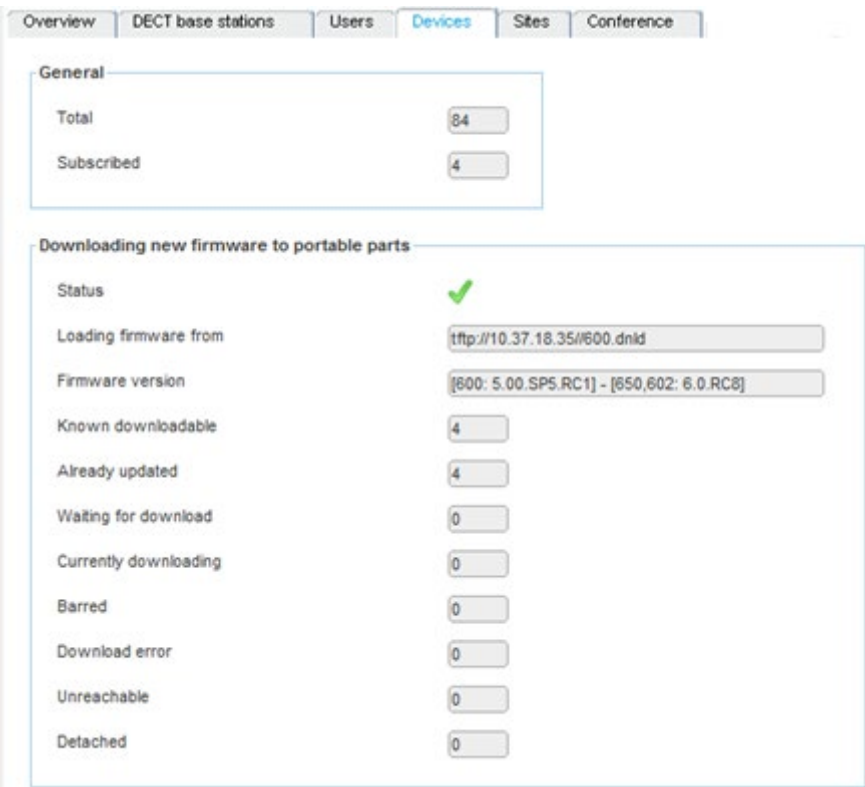
The “User monitoring states” section provides counters concerning DECT phone user monitoring state

- **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” section provides phone number or SIP user name used for standby OMM visibility checks.

7.6.4 DEVICES

The “**Devices**” tab provides information about DECT phones.



Overview DECT base stations Users **Devices** Sites Conference

General

Total 84

Subscribed 4

Downloading new firmware to portable parts

Status 

Loading firmware from

Firmware version

Known downloadable

Already updated

Waiting for download

Currently downloading

Barred

Download error

Unreachable

Detached

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

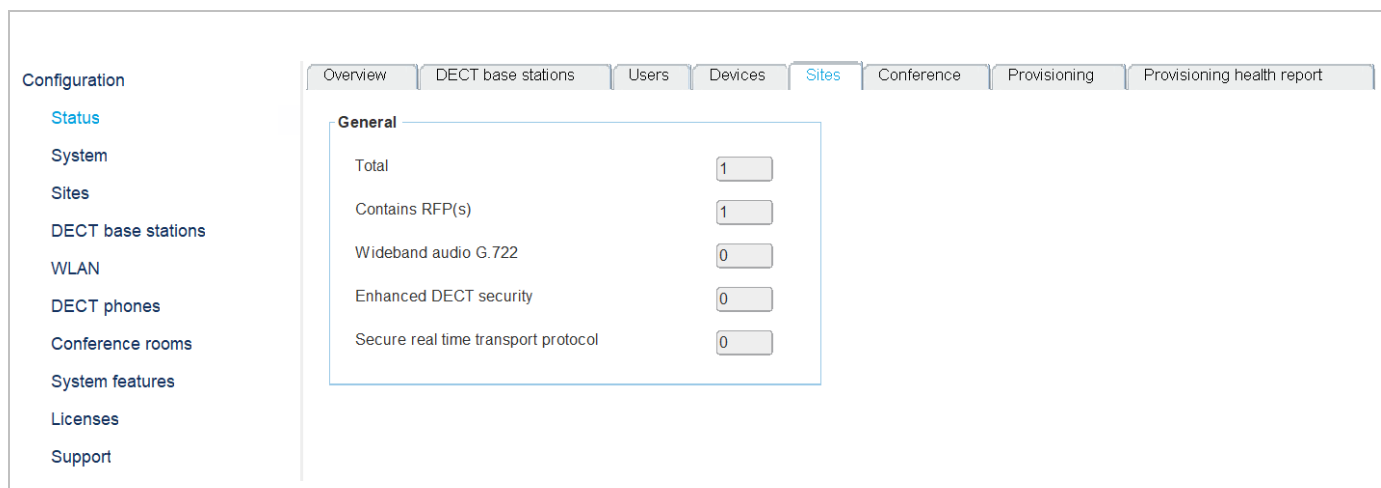
- **Total:** Total number of configured DECT phones
- **Subscribed:** Number of configured DECT phones which are subscribed to OMM

The “Downloading new firmware to portable parts” section 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

7.6.5 SITES

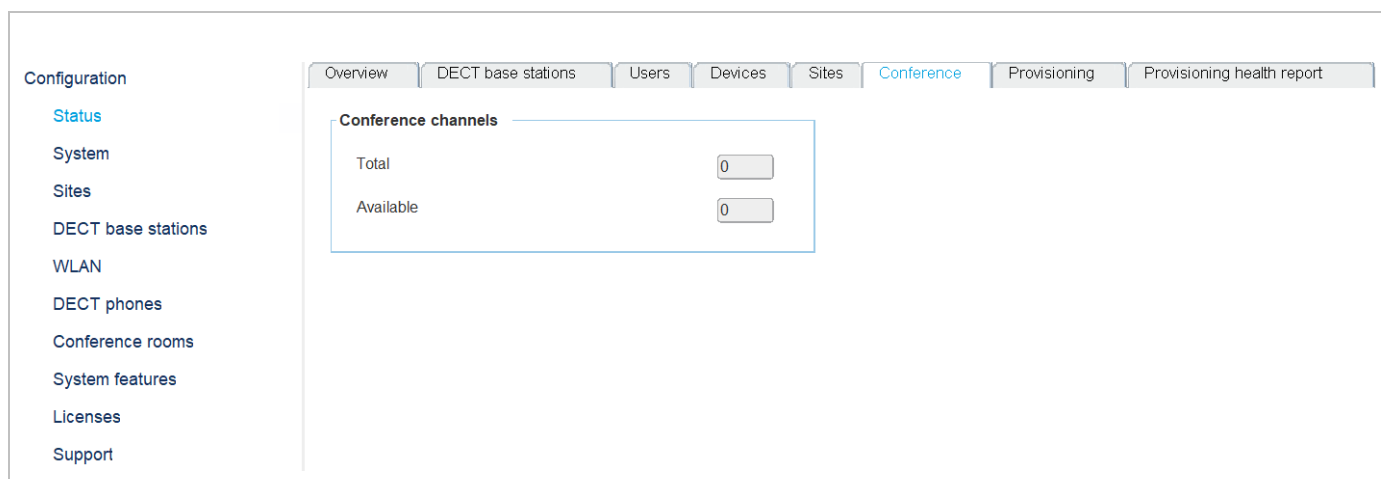
The “**Sites**” tab provides counters concerning site configuration and state:



- **Total:** Total number of configured sites
- **Contains RFPs:** Number of sites with dedicated RFPs
- **Wideband Audio G.722:** Number of sites with Wideband Audio G.722 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

7.6.6 CONFERENCE

The “**Conference**” tab provides conference channel information:



- **Total:** Total number of conference channels in system
- **Available:** Number of currently available conference channels

7.6.7 PROVISIONING

Provisioning status summary is displayed under **Configuration → Status → Provisioning** as shown in the the below figure.

Configuration

- Status
- System
- Sites
- DECT base stations
- WLAN
- DECT phones
- Conference rooms
- System features
- Licenses
- Support

Overview | DECT base stations | Users | Devices | Sites | Conference | **Provisioning** | Provisioning health report

Update status

Software: Idle

Configuration: Idle

Software update

Software downloaded: 0

Software activated: 0

Status: Idle

New software version:

7.6.8 PROVISIONING HEALTH REPORT

Provisioning health report is shown under **Configuration** → **Status** → **Provisioning health report** as shown in the below figure.

Configuration

- Status
- System
- Sites
- DECT base stations
- WLAN
- DECT phones
- Conference rooms
- System features
- Licenses
- Support

Overview | DECT base stations | Users | Devices | Sites | Conference | Provisioning | **Provisioning health report**

Health report

Timestamp: Tue Apr 20 05:48:19 2021
 Success: true
 Trigger: Restart
 Message: Provisioning successfully finished.
 File info:

7.7 “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	7.7.1
Advanced settings	Advanced settings	7.7.2

Statistics	Statistics	7.7.3
SIP	SIP	7.7.4
Provisioning	Provisioning	7.7.5
User administration	User administration	7.7.6
Data management	Data management	7.7.7

7.7.1 “BASIC SETTINGS” MENU

The **Basic settings** menu contains general settings for the OpenMobility Manager.

The screenshot displays the Mitel Basic Settings configuration window. The 'General' tab is selected, showing the following settings:

- System name:** SD 8.3
- Remote access:** ☒
- AXI server access:** ☒
- Web server access:** ☒
- Tone scheme:** DE
- Time zone:** Central European (CET UTC+1 DST)

Buttons at the bottom include OK, Cancel, and Restart.

The Basic settings menu contains the following tabs:

- **General** (see section [7.7.1.1](#))
- **DECT** (see section [7.7.1.2](#))
- **WLAN** (see section [7.7.1.3](#))

7.7.1.1 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 [10.3.5](#).
- **AXI server access:** Enables/disables AXI server access.
- **Web server access:** Enables/disables Web server access.
- **Tone scheme:** Specifies the country in which the OMM resides, which enables country-specific tones (for example, busy tone, dial tone, etc).
- **Time zone:** Specifies the time zone in which the OMM is operating.

The “General” tab contains one additional buttons (aside from default buttons):

- **Restart:** Requests an OMM restart.

7.7.1.2 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 [6.4.1](#)). 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.

- **PARK (Read-only):** 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.
- **SARI:** Specify the Secondary Access Rights Identifier (SARI) only when the OMM is connected to a MOM.
- **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.
- **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.
- **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 [1.1.1](#)).
- **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 (for example, 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.
Note: Ensure that all deployed third party DECT phones support DECT encryption. If not, encryption can be disabled per DECT phone (see [7.11.4](#)).
- **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.
- **Authenticate before Ciphering:** By default, SIP-DECT and DECT phones perform the DECT authentication procedure in a ciphered connection.
For compatibility reasons, it might be required to force the system to authenticate SIP-DECT and DECT phones before the connection is ciphered. To do this, enable the **Authenticate before Ciphering active** parameter.
By default, this parameter is disabled. You must enable this parameter only if there is an indication that enabling this parameter resolves the compatibility issues encountered in a specific SIP-DECT installation.
- **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.

- **Portable part user login type:** Specifies the system-wide variant for DECT phone login method.

DECT phones support the following types of login methods:

- Log in using the telephone number/SIP user name.
- Log in using the unique user login ID (Login ID).

Note: Changing this setting forces an automatic logout of all logged in DECT phones. If the OMM works within a system along with MOM, changing the setting logs out all OMMs of that 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.

7.7.1.3 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 [7.7.1.3](#)).

7.7.2 “ADVANCED SETTINGS” MENU

The **Advanced settings** menu contains additional settings for the OpenMobility Manager.

The screenshot shows the 'Advanced settings' menu. On the left is a sidebar with a navigation tree. The main area has a tabbed interface with the following tabs: User monitoring, OMM certificate, 802.1x, SNMP, Security, Emergency location, Time zones, Net parameters (selected), DECT phones, DECT base stations, IMA, Additional services, User service, and Pre-Login banner. The 'Net parameters' tab is active, showing settings for QoS and TTL. The settings are as follows:

Setting	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

At the bottom of the main area are 'OK' and 'Cancel' buttons.

The Advanced settings menu contains the following tabs:

- Net parameters (see section [7.7.2.1](#))
- DECT phones (see section [7.7.2.2](#))
- DECT base stations (see section [7.7.2.3](#))

- IMA (see section [7.7.2.4](#))
- Additional services (see section [7.7.2.5](#))
- User service (see section [7.7.2.6](#))
- Pre-Login banner (see section [7.7.2.7](#))
- User monitoring (see section [7.7.2.8](#))
- OMM certificate (see section [7.7.2.9](#))
- 802.1x certificate (see section [7.7.2.10](#))
- SNMP (see section [7.7.2.11](#))
- Security (see section [7.7.2.12](#))
- Time zones (see section [7.7.2.13](#))
- Emergency Location (see section [7.7.2.14](#))

7.7.2.1 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 [6.4.1.14](#)).

- **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.

7.7.2.2 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.

7.7.2.3 DECT base stations

The OMM can enable or disable the flashing of the LED on the device.

- **Disable LED:** Select the checkbox to disable flashing of the LED on the device.

7.7.2.4 IMA

The Integrated Message and Alerting (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 [6.4.1.9](#)).

7.7.2.5 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 [6.4.1.8](#))
- **NTP server settings:** You can specify the NTP servers (**NTP server 1**, **NTP server 2**, **NTP server 3**) used for time synchronization.

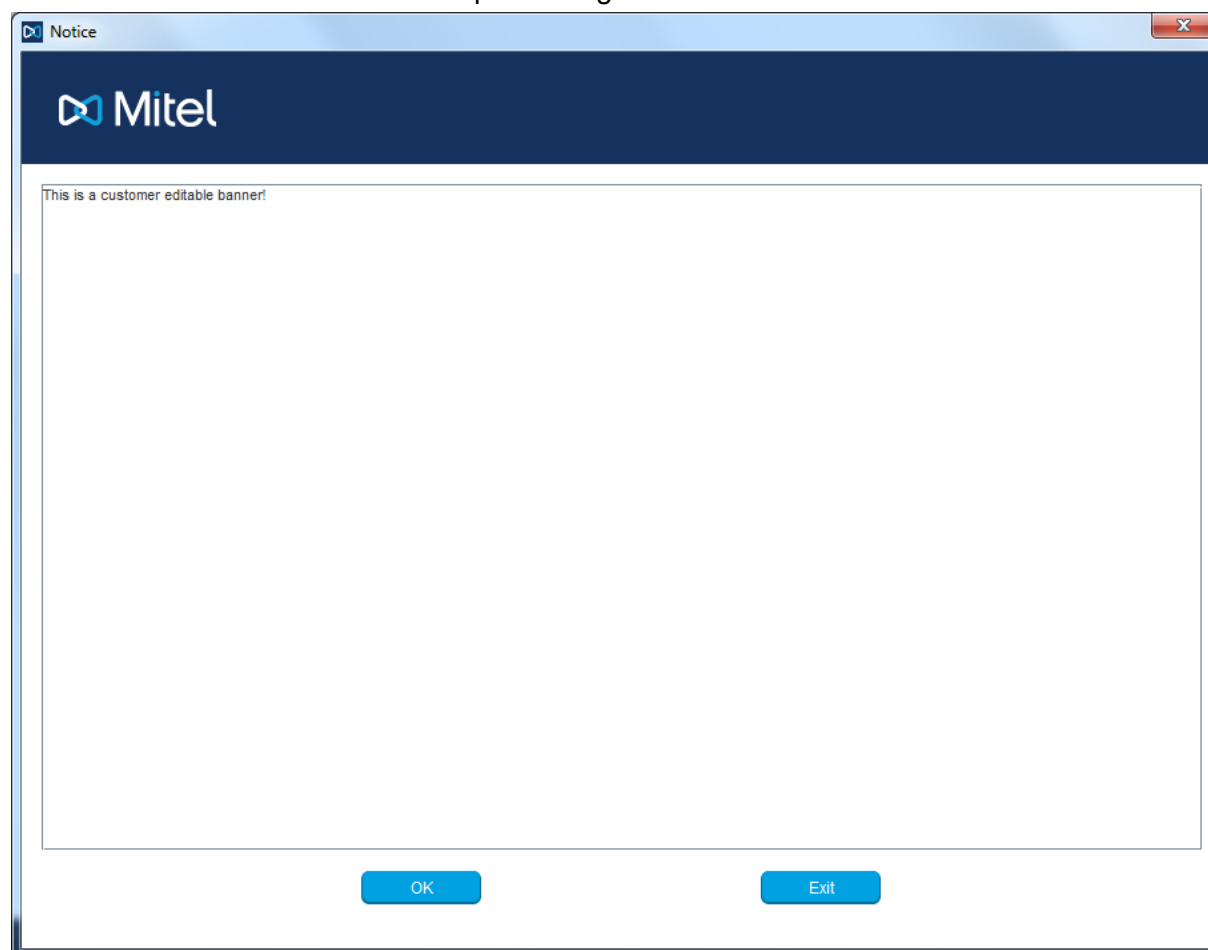
7.7.2.6 User service

- **Truncate portable part user name:** Enables or disables truncating the name of the user registered to the DECT phone.
- **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 **enabled** and **disabled**.
- **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 **enabled** and **disabled**.
- **DECT Phone System administration menu:** Specifies access to the system configuration using the DECT phone UI. By default, this parameter is disabled to improve the system security.
- **User events:** SIP-DECT supports charger events of the DECT phone to be signaled via AXI and XML Action URI application hook

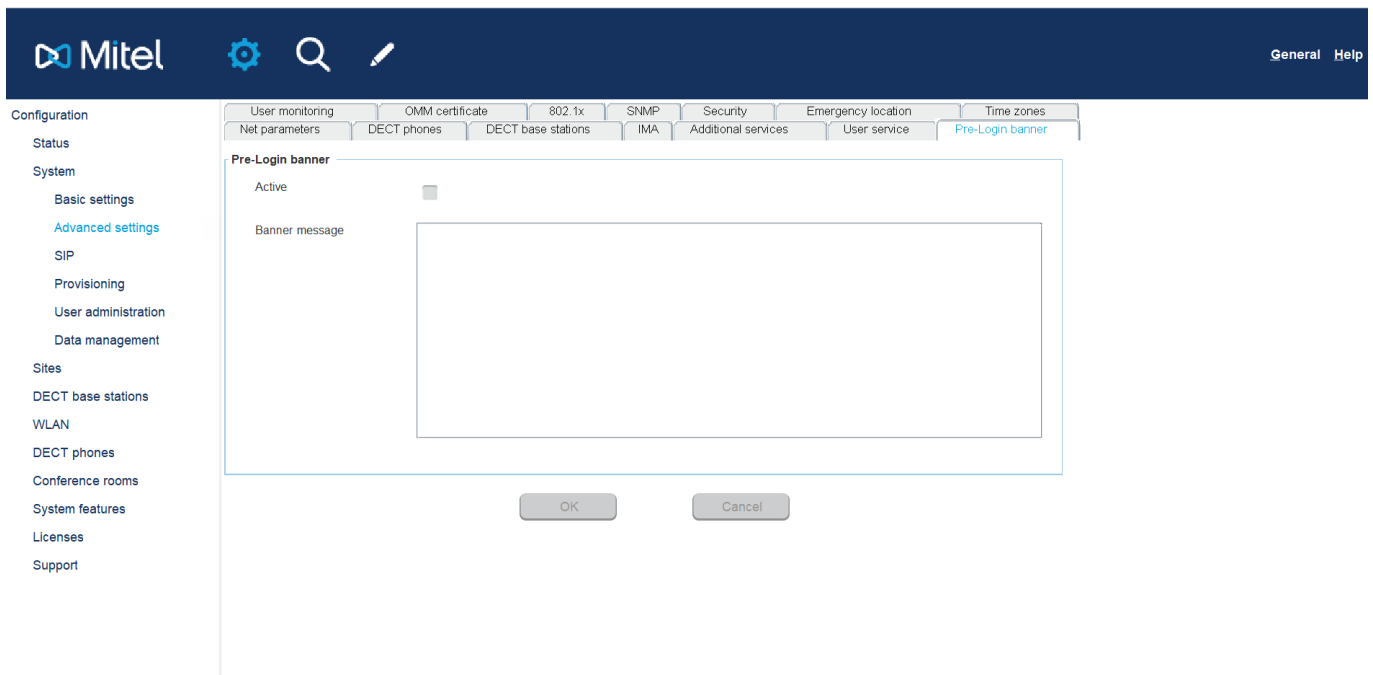
- **Charger monitoring:** Select the checkbox to activate sending a charger event via AXI or XML terminal IF.
- **Reverse XSI directory lookup:** SIP-DECT supports the XSI lookup for the caller number to display the caller's name if the name is not provided to an incoming call.
Note: If the reverse XSI directory lookup feature fails, the system picks up the caller's name from the SIP header fields that are selected from customer specific SIP DECT configuration.
 - **Active:** Select the check box to activate the **Reverse XSI directory lookup** feature.
- **Max. number of matching Digits:** Specifies the number of last digits used for a partly qualified search to avoid conflicts that occurs due to the difference in the representation of area codes or numbering plans.

7.7.2.7 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.



7.7.2.8 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”.
- **Startup delay:** The startup delay defines the period of time the user monitoring startup 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%).

7.7.2.9 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 [9.10](#).

IMPORTANT : If you upload a certificate chain, ensure the order is correct to prevent activation. The correct order is **ServerCert → Intermediate CA (interCA) → Root CA (RootCA)**..

WARNING: Uploaded certificates do not activate immediately. A restart of the OMM is required for the changes to take effect.

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.

7.7.2.10 802.1x certificate

You can import trusted certificates, a local certificate chain and a private key file for 802.1x certificate based authentication manually through OMP or OMM configuration files.

For more information, see 802.1x Feature Description.

- **Certificates/key:**
 - Shows the number of active 802.1x **Trusted certificates**, the number of 802.1x **Local certificate chains** and whether a 802.1x **Private key** is used. All can be deleted with the **Deletecertificates/key** button.
- **PEM file import /**
 - **Import PEM file with:** Specifies the type of file 802.1x (trusted certificate, local certificate, or private key) and the location of the file to be imported.
- **Private key password**
 - **Password:** Specifies the password for the 802.1x private key file.
- **General**
 - **Client identity:** 802.1x supplicant client identity.

- **Use bridge interface:** Determines whether the 802.1x supplicant is bound to the bridge interface of the RFP43 or RFP48.

7.7.2.11 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 OMM 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 [6.4.6](#)).

7.7.2.12 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 [6.4.3.8](#)) and the **Manual Import** section (section [6.4.3.10](#)).

7.7.2.13 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 600/700 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.

7.7.2.14 Emergency location

SIP-DECT supports providing an Emergency Location Identification Number (ELIN) in the SIP signaling of incoming and outgoing calls. This helps the call server (SIP proxy) to determine the correct public-safety answering point (PSAP) depending on where the call has made. The parameter “enabled” of the system emergency location identification number configuration enables the sending of the configured ELIN in the SIP signaling.

7.7.3 “STATISTICS” MENU (MONITORING MODE ONLY)

The **Statistics** page provides system statistics counters which can be used to check system behavior. The page is only available in **Monitor Mode**.

Monitoring	RFP ID	Element ID	Group	Counter	Value	Tasks
Status	0x000	0	Voice channels	Only 2 voice channels free	0	
System	0x001	1	Voice channels	Only 1 voice channels free	0	Refresh RFP
Sites		2	Voice channels	Voice channels busy	0	Refresh all
DECT base stations		3	Voice channels	Voice channels busy and call rejected	0	Clear RFP
Device list		4	Air channels	Only 2-4 air channels free	0	Clear all
Sync. view		5	Air channels	Only 1 air channel free	0	
Statistics		6	Air channels	Air channels busy	0	
Voice channels		7	Paging	Paging queue overflows	0	
Air channels		8	Sync	Synchronisation losts	0	
Paging		9	Sync	Low relations	0	
Sync		10	Sync	Offset jumps	24	
RFP health		11	RFP health	RFP resets	0	
BMC: Connections		12	RFP health	RFP connection timeouts	0	
BMC: DSP chan used		13	BMC: Connections	01 - 03	3797	
BMC: Miscellaneous		14	BMC: Connections	04 - 06	0	
BMC: Frame error rate		15	BMC: Connections	07 - 09	0	
Quality		16	BMC: Connections	10 - 12	0	
		17	BMC: DSP chan used	01 - 02	1452	
		18	BMC: DSP chan used	03 - 04	0	
		19	BMC: DSP chan used	05 - 06	0	
		20	BMC: DSP chan used	07 - 08	0	
		21	BMC: Miscellaneous	Lost connections	11	
		22	BMC: Miscellaneous	MAC reset	25	
		23	BMC: Miscellaneous	Reject dummy	0	
		24	BMC: Miscellaneous	Ho timer > 150ms	65535	
		25	BMC: Frame error rate	Bad frames	7399	
		26	BMC: Frame error rate	Good frames	1674607	
		27	BMC: Frame error rate	Frame error rate in 1/1000	4	

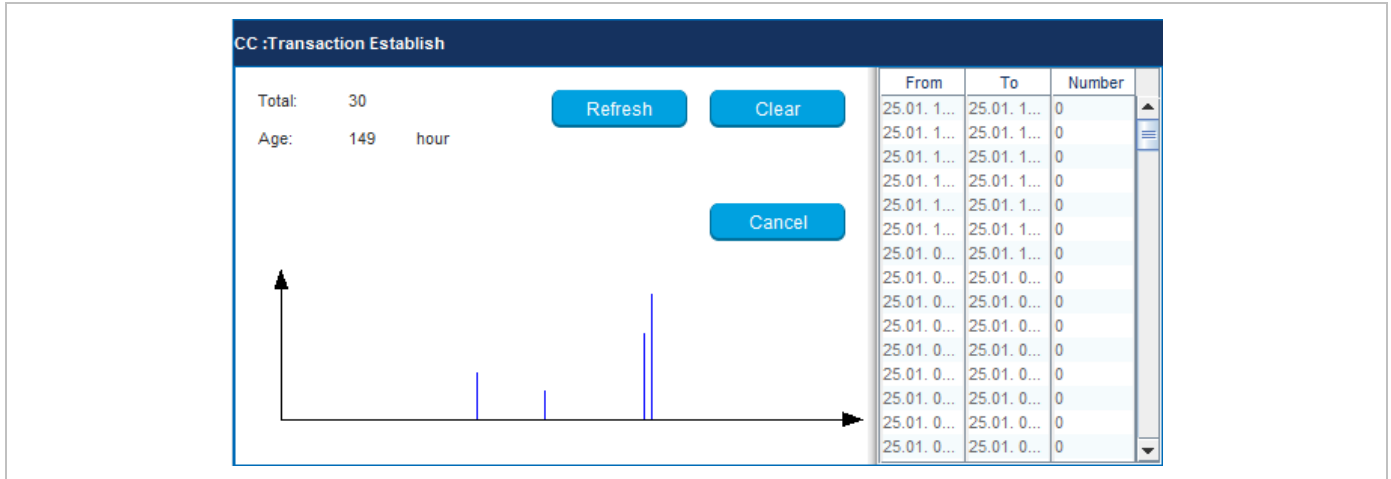
Statistic counters beginning with “+” are counters that are taken over by the standby OMM in case of a failover. All other counters are reset to default values in case of a failover. For more details about the standby feature, see section [9.15](#).

You can:

- **Refresh all:** request OMM update for all statistics counters.
- **Clear all:** reset all statistics counters in OMM.

If a statistics counter is selected in the table, it is shown in a detail section. This detail section provides all available information for this statistics counter. You can:

- update this single statistics counter by pressing the **Refresh** button, or
- reset this single statistics counter by pressing the **Clear** button.



7.7.4 “SIP” MENU

The **SIP** menu contains global settings for SIP signaling and RTP voice streams.

Configuration

Status

System

Basic settings

Advanced settings

SIP

Provisioning

User administration

Data management

Sites

DECT base stations

WLAN

DECT phones

Conference rooms

System features

Licenses

Support

DTMF settings

Intercom/Push-to-talk

Supplementary services

Conference

Security

Basic settings

Advanced settings

Registration traffic shaping

Backup settings

RTP settings

General

Proxy server

10.103.35.71

Proxy port

5060

Registrar server

10.103.35.71

Registrar port

5060

Registration period

3600

sec

Globally routable user agent URL

☒

Outbound proxy server

Outbound proxy port

5060

Transport protocol

UDP

Local port range

PP user UDP/TCP

5060

...

5060

Conference room UDP/TCP

4060

...

4060

PP user TLS

5061

...

5061

Conference room TLS

4061

...

4061

OK

Cancel

The SIP menu contains the following tabs:

- Basic settings (see section [7.7.4.1](#))
- Advanced settings (see section [7.7.4.2](#))
- Registration traffic shaping (see section [7.7.4.3](#))
- Backup settings (see section [7.7.4.4](#))

- RTP settings (see section [7.7.4.5](#))
- DTMF settings (see section [7.7.4.6](#))
- Intercom Push-to-talk (see section [7.7.4.7](#))
- Supplementary services (see section [7.7.4.8](#))
- Conference (see section [7.7.4.9](#))
- Security (see section [7.7.4.10](#))

7.7.4.1 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 [6.4.3.1](#)).

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.
- **PP 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.

Please note: Some server ports may have been changed in the SIP-DECT OMM configuration, e.g. the SIP port range. This requires additional firewall rules for changed ports in a Linux server OMM. If the Linux server OMM is updated via OVA and the system is taken over with the setup routine, the adapted firewall rules are not adopted. A manual transfer is also necessary if a new system is set up and a DB backup is imported. Sample: Port range for SIP UDP/TCP:

```
firewall-cmd --zone=public --add-port=17xxx-1xxxx/tcp --permanent
firewall-cmd --zone=public --add-port=17xxx-1xxxx/udp --permanent
firewall-cmd --reload
```

7.7.4.2 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 [6.4.3.2](#)).

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.
- **Provisional response acknowledge:** Enables or disables the signaling (100rel in SIP supported header) of PRACK support for outgoing calls.
- **Hold with SDP inactive:** In SIP signaling, when one subscriber places another on hold, the SDP media attribute "sendonly" is used to transition the remote subscriber into a mode where they solely receive audio. However, this method can pose challenges with specific Mitel OpenScape platforms, which anticipate the holding party to continue transmitting audio, thereby rendering the "music on hold" feature inactive. The "Hold with SDP inactive" parameter enables customization of hold behavior, offering a solution to the challenges faced with Mitel OpenScape platforms. Use this parameter to enable or disable this feature.

7.7.4.3 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 [6.4.3.5](#)).

7.7.4.4 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 [9.19.3](#).

- **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 [9.19.2](#)).

- **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.).
- **Auto switch back to primary server:** This parameter automatically switches back to the primary server in case of a SIP failover to a secondary or tertiary server. This parameter can be disabled if you want to control the switching back to the primary server mechanism through the IPBX platform using a 301/302 response (default value: on).

When the proxy server is set to 127.0.0.1, local calls can be performed without a SIP server. Local SIP redundancy is now supported for all transport protocols (UDP/TCP/TLS). In previous releases only UDP was supported for local SIP redundancy.

A SIP failover occurs in all cases when the response code is not:

- 486: Busy
- 487: Request Terminated
- 480: Temporary not available
- 484: Address incomplete
- Configured: Call reject state code (user reject)
- Configured: Call reject state code (device unreachable)

For all other error codes and timeout, a SIP failover takes place if the second SIP server is configured.

For a detailed description of the keep-alive mechanism see section [9.19.4](#).

Note: The SIP-DECT mechanism of polling the registration targets (Failover keep alive) is also disabled when "Auto switch back to primary" is disabled. Also, SIP Backup Server keep alive mechanism is not active when "Auto switch back to primary" is disabled.

7.7.4.5 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 [6.4.3.3](#)).

7.7.4.6 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 [6.4.3.4](#)).

7.7.4.7 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 [2.30](#).

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.

7.7.4.8 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 [6.4.3.6](#)).

Additionally, distinctive ring tones can be set for call types in the **Supplementary Services** tab of the OMP. These settings are not part of the **Supplementary Services** tab in the OMM web service. For more details about the **Distinctive ring tones for call types** feature, see section [2.33](#).

Configuration	Basic settings	Advanced settings	Registration traffic shaping	Backup settings	RTP settings																
Status	DTMF settings	Intercom/Push-to-talk	Supplementary services	Conference	Security																
System	Call behaviour <table> <tr> <td>Call transfer by hook (A142d)</td> <td>☐</td> <td>Call release timeout</td> <td>5 sec</td> </tr> <tr> <td>Call transfer by hook (6xxd)</td> <td>☒</td> <td>Hold call release timeout</td> <td>5 sec</td> </tr> <tr> <td>Ringback on hold</td> <td>☒</td> <td>Failed call release timeout</td> <td>5 sec</td> </tr> <tr> <td>Call reject on silent charging</td> <td>☐</td> <td></td> <td></td> </tr> </table>					Call transfer by hook (A142d)	☐	Call release timeout	5 sec	Call transfer by hook (6xxd)	☒	Hold call release timeout	5 sec	Ringback on hold	☒	Failed call release timeout	5 sec	Call reject on silent charging	☐		
Call transfer by hook (A142d)	☐	Call release timeout	5 sec																		
Call transfer by hook (6xxd)	☒	Hold call release timeout	5 sec																		
Ringback on hold	☒	Failed call release timeout	5 sec																		
Call reject on silent charging	☐																				
Basic settings	Miscellaneous <table> <tr> <td>Call forwarding / diversion</td> <td>☒</td> <td>Truncate Caller identification after “,”</td> <td>☐</td> </tr> <tr> <td>Local line handling</td> <td>☒</td> <td>SIP reRegister after 2 active OMM failover</td> <td>☐</td> </tr> <tr> <td>Maximal digits of internal call number</td> <td>0</td> <td></td> <td></td> </tr> </table>					Call forwarding / diversion	☒	Truncate Caller identification after “,”	☐	Local line handling	☒	SIP reRegister after 2 active OMM failover	☐	Maximal digits of internal call number	0						
Call forwarding / diversion	☒	Truncate Caller identification after “,”	☐																		
Local line handling	☒	SIP reRegister after 2 active OMM failover	☐																		
Maximal digits of internal call number	0																				
Advanced settings	Distinctive ring tone for call type <table> <tr> <td>Internal</td> <td> </td> <td>Emergency</td> <td> </td> </tr> <tr> <td>External</td> <td> </td> <td>VIP</td> <td> </td> </tr> <tr> <td>Callback</td> <td> </td> <td></td> <td></td> </tr> </table>					Internal		Emergency		External		VIP		Callback							
Internal		Emergency																			
External		VIP																			
Callback																					
SIP	OK Cancel																				
Provisioning																					
User administration																					
Data management																					
Sites																					
DECT base stations																					
WLAN																					
DECT phones																					
Conference rooms																					
System features																					
Licenses																					
Support																					

- **Maximal digits of internal call number:** Set the maximum number of digits for internal call phone numbers (all calls with more digits are signaled as external calls).
- **Distinctive ringing tone of call types:** Assign a ringing tone name to these call types:
 - Internal
 - External
 - Callback
 - Emergency

- VIP

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 [9.20](#).

- **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 (for example, Broadsoft) is used.
 - **External – Blind Transfer:** An external conference server is used (for example, 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.
- **Suppress audio on hold:** Improves the SIP-DECT interoperability with various call servers in addition to suppressing the hold tone when a user puts a conference on hold.

7.7.4.9 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 [6.4.3.8](#)) and the **Manual Import** section (section [6.4.3.10](#)).

7.7.5 "SIP PROFILES" MENU

Configuration

- Status
- System
 - Basic settings
 - Advanced settings
 - SIP
 - SIP profiles**
 - Provisioning
 - User administration
 - Data management
- Sites
- DECT base stations
- WLAN
- DECT phones
- Conference rooms
- System features
- Licenses
- Support

ID	Pri proxy srv	Pri proxy port	Pri reg srv	Pri reg port	Pri outb proxy srv	Pri outb proxy port
0	10.103.31.152	5060	10.103.31.152	5060		5060
1	10.103.31.153	5060	10.103.31.153	5060		5060
2	127.0.0.1	5060	127.0.0.1	5060		5060
3	127.0.0.1	5060	127.0.0.1	5060		5060
4	127.0.0.1	5060	127.0.0.1	5060		5060
5	127.0.0.1	5060	127.0.0.1	5060		5060
6	127.0.0.1	5060	127.0.0.1	5060		5060
7	127.0.0.1	5060	127.0.0.1	5060		5060
8	127.0.0.1	5060	127.0.0.1	5060		5060
9	127.0.0.1	5060	127.0.0.1	5060		5060
10	127.0.0.1	5060	127.0.0.1	5060		5060
11	127.0.0.1	5060	127.0.0.1	5060		5060
12	127.0.0.1	5060	127.0.0.1	5060		5060

SIP profile #0

General

	Primary	Secondary	Tertiary
Proxy server	10.103.31.152		
Proxy port	5060	5060	5060
Registrar server	10.103.31.152		
Registrar port	5060	5060	5060
Outbound proxy server			
Outbound proxy port	5060	5060	5060

OK Cancel

The Mitel OpenScape 4000 PBX platform (OS4K) architecture accommodates up to 20 gateways for user distribution. With the release of version 9.2, SIP-DECT supports this OS4K structure by enabling up to 20 "SIP profiles." Each "SIP profile" can be configured with the following data:

- Primary Proxy server
- Primary Registrar server
- Primary Outbound Proxy server
- Secondary Proxy server
- Secondary Registrar server
- Secondary Outbound Proxy server
- Tertiary Proxy server
- Tertiary Registrar server
- Tertiary Outbound Proxy server

By associating a SIP-DECT user with a specific "SIP profile," users within a SIP-DECT system can be distributed across the various gateways of the OS4K. Each "SIP profile" is designated a unique identifier (ID) ranging from 0 to 19. This ID is then utilized in the respective user data record for profile assignment. The profile with ID 0 corresponds to the familiar general SIP proxy/registrar settings found under:

- OMP->System->SIP->Basic settings
- OMP->System->SIP->Backup settings

7.7.6 "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/unsecure connections to the file server to retrieve configuration or firmware files.

The **Provisioning** menu contains settings related to the provisioning server.

Configuration

- Status
- System
 - Basic settings
 - Advanced settings
 - SIP
 - Provisioning**
 - User administration
 - Data management
- Sites
 - DECT base stations
 - WLAN
 - DECT phones
 - Conference rooms
 - System features
 - Licenses
 - Support

Provisioning URL

Active ☒ Changing one of the configuration file URL settings may cause logout of all users!

Protocol **TFTP**

Port Use default port ☒

Server

Path /ipdect.cfg, /<MAC>.cfg, /<PARK>.cfg ...

TLS settings

Validate certificates ☒ Allow unconfigured trusted certificates ☐

Validate expires ☒ Import certificates with first connection ☐

Validate host name ☒ TLS version **Auto**

Security level **Global**

OK Cancel

The Provisioning menu contains the following tabs:

- General (see section [7.7.5.1](#))
- System Update (see section [7.7.5.2](#))
- Provisioning certificate (see section [7.7.5.3](#))
- Provisioning Certificate server (see section [7.7.5.4](#))
- System credentials (see section [7.7.5.5](#))
- Event Trigger (see section [7.7.5.6](#))
- User Data Import (see section [7.7.5.7](#))
- Software Update URL (see section [7.7.5.8](#))
- IMA (see section [7.7.5.9](#))
- Branding Image URL (see section [7.7.5.10](#))
- OMM Certificate Server (see section [7.7.5.11](#))
- 802.1x Certificate Server (see section [7.7.5.12](#))
- SIP Certificate Server (see section [7.7.5.13](#))

7.7.6.1 General Provisioning

Provisioning 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.

Security

- **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.
- **TLS version:** The SSL protocol version to use for the configuration file server connection. Available options are: TLS1.2, TLS1.3 or AUTO, where AUTO accepts all protocol versions.
- **Time of day:** Time for scheduled reload of configuration and firmware files.
- **Maximum delay:** Specifies the maximum time (in minutes) and the OMM waits past the schedule time before starting the update process.
- **Autonomous SW update check by OMM:** Enable you 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.
- **Calculated time of day:** Specifies 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".

7.7.6.2 System Update

This section provides access to Provisioning System update parameters and allows to start an update process manually, to abort an active update process and to manually start an activation process of new DECT base station software version. It is divided into three sections: **Update**, **Time-Controlled update**, and **Software activation**.

Update

- **Download Order:** Select if configuration files are downloaded before the DECT base station software or vice versa. In the latter case, the DECT base stations are updated (and restarted) with the new software immediately after download. However, this setting is not fixed for PC OMM.
- **Update on OMM restart:** If set, an OMM restart provokes a Reboot/Restart event trigger.
- **Button 'Update':** Provokes a Manual event trigger.
- **Button 'Abort':** Abort a currently active Provisioning process.

Time-controlled update

- **Active:** Activate the Provisioning event trigger Schedule
- **Time of day:** Set the time of day of the scheduling event.
- **Maximum delay:** A delay between 0 and the configured value (in minutes) is added to the time of day of the trigger, to allow a spreading of the schedule event for different SIP-DECT systems.
- **Calculated time of day:** Shows the concrete time of day of scheduled event.

Software activation

- **Trigger:** Set the DECT base station software activation method:
 - Time-controlled: Activation starts at a selected time of day
 - Automatic: Activation starts immediately after the download is finished
 - Manual: Activation is started by the user with the button 'Activate'
- **Activation time of day:** Time of day of software activation.
- **One-by-one timeout:** Enables one-by-one timeout.
- **Calculated activation time of day:** Specific time of day of software activation (derived from Activation time of day and the delay calculated for the Update time of day in section 'Time-controlled update').
- **Mode:** Select if all DECT base stations are activated at once or one by one.
- **Timeout time of day:** If one by one is selected a timeout time can be configured. At that time, the one-by-one is cancelled and all remaining DECT base stations are activated immediately.
- **Calculated timeout time of day:** Specific time of day of One by one timeout (derived from Timeout time of day and the delay calculated for the Update time of day in section 'Time-controlled update').
- **Button 'Activate':** Start the activation immediately.
- **One-by-one timeout:**

7.7.6.3 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.

Certificates/key

- **Private key:** Indicates whether the OMM has a private key file (read-only).
- **Trusted certificates:** Indicates the number of active trusted certificates deployed on the OMM.

- **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.

7.7.6.4 Provisioning 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 provisioning security configuration:** Enables the use of the system-wide certificate validation settings, as configured on the **System -> Provisioning -> Provisioning certificates** page (see section [7.7.5.2](#))
- **Trusted certificate file:** Specifies the name of the PEM file on the specified server, including the trusted certificates.
- **Local certificate chain 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.

7.7.6.5 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.

7.7.6.6 Event Trigger

This section allows the configuration of the four different Provisioning trigger events:

- **Manual:** Triggered by button 'Update'
- **Reboot/restart:** Triggered by reboot of the DECT base station and optionally by an OMM restart.
- **SIP-Notify:** Triggered by receiving SIP-Notify events.
- **Scheduled:** Triggered if configured update time of day is approached.

The following settings can be configured for any single event trigger:

- **Software update:** Download the DECT base station software and activate it.
- **DECT base station software:** Select the mode of the software update:
 - **None (-):** Software is not downloaded. Do not select this, if Software update is activated.
 - **Optional (O):** Software download is optional. Unsuccessful downloading of the software does not cancel the currently running Provisioning process.
 - **Mandatory (M):** Software download is mandatory. If the software file cannot be downloaded by any reason, the currently running Provisioning process is cancelled.
- **Configuration:** Download configuration files from Provisioning server. The selection of files to be downloaded is configured by the following file selection. All files can be set to one of the following modes:
 - **None (-):** File shall not be downloaded
 - **Optional (O):** File download is optional, if it cannot be downloaded, the current Provisioning goes on
 - **Mandatory (M):** File download is mandatory, if not downloadable, the current Provisioning process is stopped
- Following configuration files are supported:
 - OMM configuration
 - IMA configuration
 - Branding image
 - License
 - User data
 - SIP certificates
 - Provisioning certificates
 - OMM (WEB/AXI) certificates
 - 802.1x WPA supplicant certificates
- **Initial wait time after error:** Period of time to wait after a download trial failed (in sec.)
- **Random component:** A calculated time value between 0 and the selected random component (in sec.) is added to the Initial wait timer, to calculate the real wait time. For every retry the real wait time is doubled.

- **Number of retries:** Number retries in case of error for every single file to be downloaded.

Instead to configure any single event trigger individually, all can be set to the same values described above, by selecting the check box 'Select All'. By starting the OMP this check box is disabled, that means individually event trigger configuration is active. If the check box is (un)selected, all changes, which were not confirmed by button 'OK', are lost and the last stored configuration is active again.

7.7.6.7 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 selected protocol. If the server does not respond to the selected protocol it will be treated as an error.
- **Default 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 of all users.
- **Use provisioning security configuration:** Enables the use of the system-wide certificate validation settings, as configured on the **Certificates page** (see section 7.7.5.2).

Please note: If no credentials are specified for secure protocols, the system credentials are automatically used (see section [7.7.5.5](#)). 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*.

7.7.6.8 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 [9.9.3](#) 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.
- **Default 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 provisioning security configuration:** Enables the use of the system-wide certificate validation settings for this URL, as configured on the **System -> Provisioning -> Certificates** page (see section [6.4.2.14](#)).

7.7.6.9 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 **Provisioning and Software update** page of the OMM Web service. The same parameters are described in the Provisioning & Software Update page of OMM Web Service.

7.7.6.10 Branding Image URL

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. If the branding image URL is disabled the image will be retrieved from the general config URL. Regardless of the used URL, if the image cannot be found at the server path the branding image will be deleted from data base. The picture should not be larger than 50 pixels high and 216 pixels wide.

- **Configure specific source:** 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.
- **Default 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 image file on the external file server.
- **Use provisioning security configuration:** Enables the use of the same certificate validation settings for the image file URL as specified for the ConfigURL.

7.7.6.11 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 provisioning security configuration:** Enables the use of the system-wide certificate validation settings, as configured under the System -> Provisioning menu (see section [7.7.5](#)).
- **Local certificate chain 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.

7.7.6.12 802.1 Certificate Server

Through configuration of a 802.1x certificate server URL, you can update the 802.1x certificate data automatically.

- **User name:** Specifies the user name for authentication against the certificate server.
- **Password:** Specifies the password for authentication against the certificate server.
- **Active:** Enables or disables the certificate server URL feature.
- **Protocol:** Specifies the protocol to be used to fetch the certificate files. One of FTP / FTPS / SFTP / HTTP / HTTPS / TFTP / None.
- **Default Port:** Specifies the certificate server's port number or use of the default port for the used protocol.
- **Server:** Specifies the IP address or name of the certificate server.

- **Path without the filename:** Specifies the path to the certificate files on the certificate server.
- **Use provisioning security configuration:** Enables the use of the system-wide certificate validation settings for this URL, as configured on the **System -> Provisioning -> Certificates** page (see section [6.4.2.14](#)).
- **Trusted certificates file:** Filename of the trusted certificates to read from the server.
- **Local certificate chain file:** Filename of the local certificates to read from the server.
- **Private key file:** Filename of the private key to read from the server.

7.7.6.13 SIP 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 provisioning security configuration:** Enables the use of the system-wide certificate validation settings, as configured under the System -> Provisioning menu (see section [7.7.5](#)).
- **Local certificate chain 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.

7.7.7 “USER ADMINISTRATION” MENU

In the **User administration** menu you configure the OMM user accounts.

ID	Comment	User name	Password aging	Active
0	Read-only	user	None	✖
1	Full access	omm	None	✔
2	Root (SSH only)	root	None	✔

New user account

General

Permissions

Active

☒

User name

Old password

Password

Password confirmation

Password aging

None ☐

OK

Cancel

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 [9.16.1](#). 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		7.7.6.1
Configure: Configure selected user account in detail section		7.7.6.1
	Show details: Shows selected user account in detail section	7.7.6.2
Delete: Delete selected user account		7.7.6.3

7.7.7.1 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.

Configuration	ID	Comment	User name	Password aging	Active	Tasks
Status	0	Read-only	user	None	✖	Create Configure Delete
System	1	Full access	omm	None	✔	
	2	Root (SSH only)	root	None	✔	

Configuration

Status

System

Basic settings

Advanced settings

SIP

Provisioning

User administration

Data management

Sites

DECT base stations

WLAN

DECT phones

Conference rooms

System features

Licenses

Support

New user account

General

Permissions

Active ☒

User name

Old password

Password

Password confirmation

Password aging None ☐

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** section 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** section:

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 6.4.4).

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 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

[7.7.5.1](#) 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 [7.7.5.1](#)).
- 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.

7.7.7.2 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 section.
- 3 To close the user account detail section, click the **Cancel** button.

7.7.7.3 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.

7.7.8 "DATA MANAGEMENT" MENU

The **Data management** menu provides access to data related to import and export features.

The screenshot shows the Mitel OM Management Portal (OMP) interface. The top navigation bar includes the Mitel logo, a settings gear icon, a search icon, and a pencil icon. On the right, there are links for 'General' and 'Help'. The left sidebar contains a 'Configuration' menu with various categories: Status, System, Basic settings, Advanced settings, SIP, Provisioning, User administration, Data management (highlighted), Sites, DECT base stations, WLAN, DECT phones, Conference rooms, System features, Licenses, and Support. The main content area is titled 'Auto DB export' and contains several configuration fields: 'Active' (checked), 'Protocol' (TFTP), 'Port' (empty), 'Use default port' (checked), 'Server' (10.103.35.14), 'User name' (empty), 'Password' (masked with asterisks), 'Password confirmation' (masked with asterisks), 'Path' (/lpuesche/8.2/), and 'Use provisioning security configuration' (unchecked). At the bottom of the form are 'OK' and 'Cancel' buttons. An 'Info console' bar is visible at the very bottom of the page.

The Data management contains the following tabs:

- **Auto DB export** (see section [7.7.7.1](#))
- **Manual DB import** (see section [7.7.7.2](#))
- **Manual DB export** (see section [7.7.7.3](#))
- **IMA** (see section [7.7.7.4](#))

7.7.8.1 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 [9.5.3](#) and section [6.4.1.16](#).

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 [6.4.7.3](#)).

Note: The **Use default port** parameter is available only for OMP.

7.7.8.2 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 [6.4.7.1](#)).

Note: The **Use default port** parameter is available only for OMP.

7.7.8.3 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 [6.4.7.2](#)).

Note: The **Use default port** parameter is available only for OMP.

7.7.8.4 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**.

7.7.9 “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 Bul...	
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	
DECT phones	2	AXI	1	2015/01/21 21:01:20.7...	[204] New connection...	
Conference rooms	3	STB	1	2015/01/21 21:01:22.4...	Broken Connection to ...	
System features	2	AXI	1	2015/01/21 21:29:05.4...	[203] New secure co...	
Licenses	3	DSIP	1	2015/01/21 21:36:26.7...	SIP registration to 10...	
	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 cle...	
	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 cle...	

7.7.9.1 Event log detail section

Event log

General

Severity

Subsystem

Count

Time

Event
[199] New connection from 10.37.18.32:58185

Cancel

7.8 “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.

The screenshot displays the Mitel SIP-DECT OM System Manual interface. The top navigation bar includes the Mitel logo, a settings gear icon, a search magnifying glass icon, and a pencil icon. The right side of the bar has 'General' and 'Help' links. A left sidebar lists configuration categories: Configuration, Status, System, Sites (highlighted), DECT base stations, WLAN, DECT phones, Conference rooms, System features, Licenses, and Support. The main content area shows a table of sites with columns: ID, Name, ELIN number, Wideband audio G.722, Enh. DECT security, SRTP, and Number of RFPs. The first row shows ID 1, Name 'default', and 2 RFPs. Below the table, the 'Site #1' configuration form is visible, with a 'General' tab selected. The form includes fields for Name (set to 'default'), Emergency location identification number, Wideband audio G.722 (checkbox), Enhanced DECT security (checkbox), and SRTP (set to 'Disabled' with a dropdown arrow). A blue information icon with text 'Changing site parameters, may restart radio fixed parts in this site.' is present. At the bottom are 'OK' and 'Cancel' buttons. The bottom status bar is labeled 'Info console'.

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.
- **Emergency Location Identification Number (ELIN):** Enter the system-wide valid emergency call identification number. This value is used when there is no more specific ELIN set. The parameter can be used for small systems in which the same ELIN should be used for all base stations.
- **Wideband Audio G.722:** Select the checkbox to enable wideband audio G.722
- **Enhanced DECT security:** Select the checkbox to enable enhanced DECT security.
- **SRTP:** These capabilities must be options that are enabled or disabled, preferred only, and SrtplusRtp. In sites, which are configured to provide this functionality, exclusively 3rd and 4th generation RFPs are applicable.
 - Only: Only SRTP calls will be accepted, all other will be rejected (the audiopart of the SDP contains RTP/SAVP).
 - Preferred: All calls will be initiated as secured, but accepted if they are not secured (the audio part of the SDP contain RTP/AVP).
 - Disabled: Only RTP calls will be initiated as not ciphered and incoming ciphering algorithm will be not accepted. All communications are established unencrypted.

- **SrtpPlusRtp:** All calls will be initiated as secured, but accepted if they are not secured (the audio part of the SDP contains 2 m-lines RTP/SAVP and RTP/AVP).
- **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).
- **Select Columns:** Select columns/parameters to be shown.
- **Show details** (only in **Monitor Mode**): Shows configuration of a selected site in the **General** tab.

7.9 “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	7.9.1
Paging areas		7.9.1
Capturing		7.9.2
Enrolment		7.9.3
Export		7.9.4
	Sync view	7.9.5
	Statistics	7.9.6
	Quality	7.9.7

7.9.1 “DEVICE LIST” MENU

The **Device list** section 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	ELIN number	IP address	DECT cluster	License RFP	Room	Connection state	Tasks
Status	0x000	OMM RFP 1	08:00:0F:C3:DE:FD		10.103.35.150	1	✖		✓	Create
System	0x001	RFP 43	00:30:42:17:8E:3E		10.103.35.172	1	✖		✓	Configure
Sites										Delete
DECT base stations										Re-enrollment
Device list										✖ Filter
Paging areas										Select columns
Capturing										
Enrolment										
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 [7.9.1.7](#).

The tasks you can perform are mode-dependant.

Configuration mode	Monitor mode	See section
Create: Create new base station in detail section		7.9.1.2
Configure: Configure selected base station in detail section		7.9.1.3
	Show details: Show selected base station in detail section	7.9.1.4
Delete: Delete selected RFP		7.9.1.5
Re-enrollment: Re-enroll the selected RFP		
	Show sync. relations: Show synchronization relation for selected RFPs	7.9.1.6
Select columns: Select columns/parameters to be shown in RFP table	Select columns: Select columns/parameters to be shown in RFP table	7.9.1.7
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	7.9.1.8

7.9.1.1 DECT Base Station Detail Section

The DECT base station detail section is used for configuration/display of RFP settings and creation of new RFP datasets.

To call up the DECT base station detail section, do one of the following:

- Choose one of the commands in the task bar on the right of the **DECT base stations** section (**Create**, **Configure**, or **Show details**)
- Double-click on the appropriate RFP entry in the RFP table.

The DECT base station detail section 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.

DECT base station #0x000

Status

General

DECT

WLAN

Hardware

Connection state	✓	Version mismatch	✖
OMM running	✓	Standby misconfigured	✖
Software update	✖	Advanced features state	✓
Encryption state	✓	802.1X configuration mismatch	✖
IP address	10.103.35.150		
Software version	SIP-DECT 8.3SP1-G15		

Cancel

“General” tab

This tab contains the general DECT base station parameters.

DECT base station #0x000

Status

General

DECT

WLAN

Hardware

Name	OMM RFP 1
MAC address	08:00:0F:C3:DE:FD
Emergency location identification number	
Site	default
Building	
Floor	
Room	
Conference channels	☐

Cancel

“DECT” tab

This tab contains the DECT base station's DECT parameters.

Note: The DECT running and Synchronization parameters are not available in the **Configuration Mode**.

DECT base station #0x000

Status

General

DECT

WLAN

Hardware

DECT switched on

☒

DECT running

DECT cluster

Synchronization state

Paging area

Preferred synchronisation source

☐

Reflective environment

☐

Cancel

“WLAN” tab

This tab contains the DECT base station's WLAN parameters. Settings in the **WLAN** tab apply to RFP 43/48 WLAN base stations only.

Monitor Mode

DECT base station #0x000

Status

General

DECT

WLAN

Hardware

WLAN switched on

☐

WLAN supported

WLAN profile

Dynamic Frequency Selection supported

Antenna diversity

☐

WLAN running

Antenna

WLAN link not OK

Channel

Channel used

Output power level

Output power used

dBm

High-Throughput mode used

Cancel

Configuration Mode

DECT base station #0x001

General DECT **WLAN** Hardware

WLAN switched on ☐

WLAN profile None

Antenna diversity ☐

Antenna 1

Channel 0

Output power level Full

 Please configure the WLAN regulatory domain on the system settings page.

“Hardware” tab

In **Monitor Mode**, this tab shows hardware information of the selected DECT base station.

DECT base station #0x000

Status General DECT WLAN **Hardware**

Hardware type RFP 47

Radio type ConfigurableTX

Outdoor type 

Frequency shift supported 

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.

DECT base station #0x001

General DECT WLAN Hardware

Hardware type RFP 43

OK Cancel

7.9.1.2 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** section 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** section:

“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.
- **Emergency location identification number:** Enter the system-wide valid emergency call identification number. This value is used when there is no more specific ELIN set. The parameter can be used for small systems in which the same ELIN should be used for all base stations.
- **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 [9.20.2](#)).

- **Emergency Location Identification Number (ELIN):** Enter the system-wide valid emergency call identification number. This value is used when there is no more specific ELIN set. The parameter can be used for small systems in which the same ELIN should be used for all base stations.

“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 [7.7](#)). The assignment between RFPs and paging areas can be changed in the **Paging areas** menu (see section [1.1.1](#)).

- **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 [9.2](#).
- **Reflective environment:** Within areas containing lot of reflective surfaces (for example, 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 600/700 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 35/36/37 IP, RFP 43 WLAN, RFP 44/45/47, or RFP 48 WLAN respectively supports 4 calls at the same time.

With active DECT XQ , RFP 44 supports only 2 calls and other RFPs support 4 calls.

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 43/48 WLAN”, “RFP 43 WLAN” and “RFP 48 WLAN” only. For details about WLAN configurations please see section [9.17](#).

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 43 WLAN or RFP 48 WLAN can be switched on/off.
- **WLAN profile:** Indicates the WLAN profile applied. This applies all settings made in the respective WLAN profile to the current RFP. For information on configuring WLAN profiles see section [9.17](#).
- **Antenna diversity:** Enables antenna diversity.
- **Antenna:** Indicates the antenna settings

- **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.

“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).

7.9.1.3 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 section opens.
- 3 Change RFP parameters (see descriptions in section [7.7.1.2](#)).
- 4 Click **OK**.

7.9.1.4 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 section opens.
- 3 To close the RFP detail section, click **Cancel**.

7.9.1.5 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.

7.9.1.6 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 [7.9.5](#).

7.9.1.7 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.

7.9.1.8 Filtering the DECT base station table

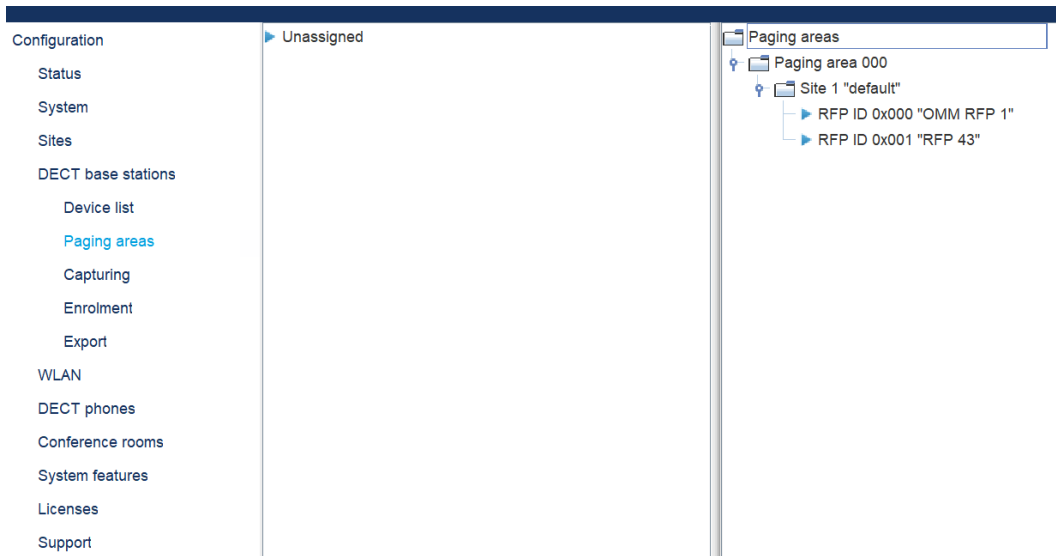
You can filter the list of DECT base station datasets shown in the table by using a filter.

- 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** section.
- 5 In the **Filter** dialog click on the **Reset** button.

“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 pagingarea.
- 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

7.9.3 “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

7.9.4 “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 [13.3](#).

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 [7.9.1.7](#)).

7.9.5 “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	☒	00:30:42:18:1D:BD	SVE RFP1	1	0	3	RFP 35	Export all
	☐	00:30:42:18:20:A2	SVE RFP2	1	0	3	RFP 35	
System	☐	01:02:03:04:05:06	simu	5	0	1	RFP 32	Export selected
	☐	01:02:03:04:05:07	simu	5	0	1	RFP 32	
Sites	☐	01:02:03:04:05:08	simu	5	0	1	RFP 32	Select parameters
	☐	01:02:03:04:05:09	simu	5	0	1	RFP 32	
DECT base stations	☐	01:02:03:04:05:0A	simu	5	0	1	RFP 32	Select columns
	☐	01:02:03:04:05:0B	simu	5	0	1	RFP 32	
Device list	☐	01:02:03:04:05:0C	simu	5	0	1	RFP 32	
Paging areas	☐	01:02:03:04:05:0D	simu	5	0	1	RFP 32	
Capturing	☐	01:02:03:04:05:0E	simu	5	0	1	RFP 32	
Enrolment	☐	01:02:03:04:05:0F	simu	5	0	1	RFP 32	
Export								

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 [7.9.3](#)). For information about DECT base station export file format, see **Appendix** (section [13.4](#)).

7.9.6 “SYNC VIEW” MENU

The **Sync view** menu allows verification of the synchronization between DECT base stations in a graphical manner.

Note: The Sync menu is available only in the **Monitoring Mode**.

Note: For information on DECT base station synchronization, see section [9.2](#).

To open the task section, click the arrow icon in the upper right corner of the **Sync view** section.

The task section 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 section; 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 section.
- **Reset view:** Reset selected view (zero coordinates are reset to the left upper corner of the sync view section).
- **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 <= -80 dBm
- Yellow: -80 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.

7.9.7 “STATISTICS” MENU

The **DECT base stations** -> **Statistics** menu provides information about DECT base station statistics counters. It contains:

- an overview section with all statistics counters (see section [7.9.6.1](#))
- multiple statistics group sections, where related statistics counter types are grouped together (see section [7.9.6.2](#)).

The menu is only available in **Monitor Mode**.

7.9.7.1 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.



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 section opens which shows more detailed information for that counter.

The detail section shows values for total occurrence and occurrence in current and last week.

7.9.7.2 DECT base station Statistics Group Sections

The DECT base station statistics group sections 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 sections are listed under the **Statistics** menu entry in the left section.

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:** Refresh all counters of selected DECT base station.
- **Refresh all:** Refresh all counters 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.

7.9.8 “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**.

7.9.8.1 RFP IP

IP quality menu provides information about link quality between DECT base stations and OMM.

Monitoring	☐	RFP ID	Connected tim...	Current RTT [...]	Max. RTT [msec]	Count	< 25 msec	< 50 msec	< 150 msec	< 500 msec	>= 500 msec	Tasks
Status	☐	0x000	454935	0.6	0.8	30328	30328	0	0	0	0	Select columns
System	☐	0x001	454935	0.7	1.0	30328	30328	0	0	0	0	
Sites												
DECT base stations												
Device list												
Sync. view												
Statistics												
Quality												
IP												
Media stream												
Synchronization												
WLAN												
DECT phones												
Conference rooms												
System features												
Licenses												
Support												

Displayed parameters:

- **RFP 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

7.9.8.2 Media Stream

Media stream section provides information about voice quality.

Monitoring		RFP ID	Connects	Duration [sec]	TX packets	RX packets	Lost packets	Max. jitter [msec]	Tasks
Status	☐	0x000	0	0	0	0	0	0	Clear RFP Clear all Select columns
System	☐	0x001	0	0	0	0	0	0	
Sites									
DECT base stations									
Device list									
Sync. view									
Statistics									
Quality									
IP									
Media stream									
Synchronization									
WLAN									
DECT phones									
Conference rooms									
System features									
Licenses									
Support									

Displayed parameters:

- **RFP 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

7.9.8.3 Synchronization

Synchronization section 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.

Monitoring	☐	RFP ID	DECT cluster	Sync. state	Strong relations	Low relations	Max. RSSI [dBm]	Min. RSSI [dBm]	Tasks
Status	☐	0x000	1	✓	0	1	-100	-	☒ Snapshot mode
System	☐	0x001	1	✓	1	0	-40	-40	Update
Sites									Select columns
DECT base stations									
Device list									
Sync. view									
Statistics									
Quality									
IP									
Media stream									
Synchronization									
WLAN									
DECT phones									
Conference rooms									
System features									
Licenses									
Support									

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

7.10 “WLAN” MENU

OMP supports configuration of WLAN profiles and provides an overview of wireless clients currently connected.

7.10.1 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.

7.10.1.1 WLAN Profiles - configuration mode

WLAN profile configuration menu provides an overview of all configured WLAN profiles.

Configuration	ID	Enabled	Profile type	Mode	SSID 1	DECT base stations	Tasks
Status							Create profile
System							Configure profile
Sites							Delete profile
DECT base stations							Delete all profiles
WLAN							Configure MAC filter
Profiles							Select columns
DECT phones							
Conference rooms							
System features							
Licenses							

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

7.10.1.2 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

7.10.1.3 WLAN Profile Detail Section

WLAN profile detail section 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 section 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.

New WLAN profile

General SSID selection SSID 1 general SSID 1 security

Profile enabled ☒ Profile type RFP43/48

Avoid interferences ☐ 802.11 mode 802.11n

HT40 mode ☐ WME ☒

HT80 mode ☐ 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.

New WLAN profile

General SSID selection SSID 1 general SSID 1 security

	Configure	Name
SSID 1	☒	
SSID 2	☐	
SSID 3	☐	
SSID 4	☐	

OK Cancel

The "SSID x general" tab is shown for any activated SSID. Among other things, you can use it to select Security type.

The screenshot shows the 'New WLAN profile' dialog box with the 'SSID 1 general' tab selected. The dialog has four tabs: 'General', 'SSID selection', 'SSID 1 general', and 'SSID 1 security'. The 'SSID 1 general' tab contains the following settings:

- SSID enabled: ☒
- VLAN tag: ☐ (with an empty text box next to it)
- Security type: Open (dropdown menu)
- BSS isolation: ☐
- Use MAC access filter: ☐
- Hidden SSID mode: ☐

At the bottom of the dialog are 'OK' and 'Cancel' buttons.

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 shows the 'WLAN profile #3' dialog box with the 'SSID 1 security' tab selected. The dialog has four tabs: 'General', 'SSID selection', 'SSID 1 general', and 'SSID 1 security'. The 'SSID 1 security' tab contains the following settings:

- Security settings 'WPA':
 - WPA type: WPA2 (dropdown menu)
 - Distribution interval: 600 sec
 - Mode: Pre shared key (dropdown menu)
 - Pre shared key format: Text (dropdown menu)
 - Pre shared key: PpNohquP00GoSHGmfOyX
 - Generate button
- Radius configuration:
 - IP address: (text box)
 - Port: (text box)
 - Secret: (text box)

At the bottom of the dialog are 'OK' and 'Cancel' buttons.

7.10.1.4 MAC Access Filter Detail Section

MAC access filter detail section 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 section 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.

7.10.1.5 Clients

WLAN clients menu which is available in monitoring mode only, shows all currently connected wireless clients.

7.11 “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	7.11.1
Users: Displays all DECT phone user data		7.11.2
Devices: Displays all DECT phone device data	Devices: Displays all DECT phone device data	7.11.3
	User monitoring: Displays the status of all monitored users	7.11.13

7.11.1 “OVERVIEW” MENU

In the **Overview** section, 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	✓	Create
		0x002	03586 0952116 0	x25053 622d	25053	0x002	Fixed	✓	Configure
System		0x003	03586 0950946 7	x25054 622d	25054	0x003	Fixed	✓	Delete
	✓	0x004	03586 0952129 3	x42052 622d	42052	0x004	Fixed	✓	✖ Filter
Sites		0x05F	00100 0000000 3	simu pp 0	256001	0x04C	Fixed	✖	✖ Subscription
DECT base stations		0x060	00100 0000001 4	simu pp 1	256002	0x04D	Fixed	✖	✖ Wildcard subscription
		0x061	00100 0000002 5	simu pp 2	256003	0x04E	Fixed	✖	Select columns
WLAN		0x062	00100 0000003 6	simu pp 3	256004	0x04F	Fixed	✖	Change rel. type
		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	✖	
Licenses		0x06F	00100 0000016 9	simu pp 16	256017	0x05C	Fixed	✖	
		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** section 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 [7.11.9](#).

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 7.11.9 for information on selecting columns and section [9.19.6](#) for information on the SIP registration status.

Monitoring	Device ID	IPEI	Subscri.	Number/SP..	Last action	RFP ID	CC	MM	Info	Registe..	Tasks
Status	0x001	10345 003163..	✓	25052	25.01. 21:42	0x000				✓	▲ Show details
	0x002	03586 095211..	✓	25053	25.01. 22:12	0x001				✓	⌘ Filter
System	0x003	03586 095094..	✓	25054	25.01. 20:42	0x001				✓	⌘ Log events
	0x004	03586 095212..	✓	42052	25.01. 22:25	0x000				✓	Select columns
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	-	-				✗	
DECT phones	0x064	00100 000000..	✗	256006	-	-				✗	
Overview	0x065	00100 000000..	✗	256007	-	-				✗	
Devices	0x066	00100 000000..	✗	256008	-	-				✗	
	0x067	00100 000000..	✗	256009	-	-				✗	
User monitoring	0x068	00100 000000..	✗	256010	-	-				✗	
	0x069	00100 000001..	✗	256011	-	-				✗	
Conference rooms	0x06A	00100 000001..	✗	256012	-	-				✗	
	0x06B	00100 000001..	✗	256013	-	-				✗	
System features	0x06C	00100 000001..	✗	256014	-	-				✗	
	0x06D	00100 000001..	✗	256015	-	-				✗	
Licenses	0x06E	00100 000001..	✗	256016	-	-				✗	
	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 section		7.11.5
Configure: Configure selected DECT phone user and device dataset in detail section		7.11.6
	Show details: Show selected DECT phone user and device dataset in detail section	7.11.4
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)		7.11.8
Subscription: Start DECT phone subscription		7.11.7
Wildcard subscription: Start DECT phone wildcard subscription		7.11.7
Select columns: Select columns/parameters to be shown in DECT phone table	Select columns: Select columns/parameters to be shown in DECT phone table	7.11.9
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	7.11.10
Change rel. type: Change the DECT phone relation type		7.11.11
	Log events: Enable/disable DECT phone event log	7.11.12

7.11.2 “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	✓	✕	
		0x002	x25053 622d	25053		Fixed	0x002	✓	✕	
System	✓	0x003	x25054 622d	25054		Fixed	0x003	✓	✕	Create
Sites		0x004	x42052 622d	42052		Fixed	0x004	✓	✕	Configure
DECT base stations		0x04C	simu pp 0	256001		Fixed	0x05F	✕	✕	Delete
WLAN		0x04D	simu pp 1	256002		Fixed	0x060	✕	✕	✕ Filter
Video devices		0x04E	simu pp 2	256003		Fixed	0x061	✕	✕	Select columns
DECT phones		0x04F	simu pp 3	256004		Fixed	0x062	✕	✕	
Overview		0x050	simu pp 4	256005		Fixed	0x063	✕	✕	
Users		0x051	simu pp 5	256006		Fixed	0x064	✕	✕	
Devices		0x052	simu pp 6	256007		Fixed	0x065	✕	✕	
Conference rooms		0x053	simu pp 7	256008		Fixed	0x066	✕	✕	
System features		0x054	simu pp 8	256009		Fixed	0x067	✕	✕	
Licenses		0x055	simu pp 9	256010		Fixed	0x068	✕	✕	
		0x056	simu pp 10	256011		Fixed	0x069	✕	✕	
		0x057	simu pp 11	256012		Fixed	0x06A	✕	✕	
		0x058	simu pp 12	256013		Fixed	0x06B	✕	✕	
		0x059	simu pp 13	256014		Fixed	0x06C	✕	✕	
		0x05A	simu pp 14	256015		Fixed	0x06D	✕	✕	
		0x05B	simu pp 15	256016		Fixed	0x06E	✕	✕	
		0x05C	simu pp 16	256017		Fixed	0x06F	✕	✕	
		0x05D	simu pp 17	256018		Fixed	0x070	✕	✕	

In the **Users** section, all DECT phone user data are listed in a table. The **Users** section 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 [7.11.9](#)) to display the desired DECT phone user data.

The following tasks can be performed:

- **Create:** Create new unbound DECT Phone user dataset (see section [7.11.5](#)).
- **Configure:** Configure selected DECT Phone user dataset (see section [7.11.6](#)).
- **Delete:** Delete selected DECT Phone user dataset. Also delete device data in case of a fixed relation (see section [7.11.8](#)).
- **Select columns:** Select parameter columns to be shown in table (see section [7.11.9](#)).
- **Filter:** Filter DECT phone datasets shown in table for string set in filter mask (see section [7.11.10](#)).
- **Change rel. type:** Change the DECT phone relation type (see section [7.11.11](#)).

7.11.3 “DEVICES” MENU

In the **Devices** section, all DECT phone device data are listed in a table. The **Device** section 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.

Mitel    								General
Configuration	Device ID	IPEI	DECT Auth. co...	Encryption	Device rel. type	Rel. user ID	Subscribed	Tasks
Status	0x001	10345 0031639 *		✓	Fixed	0x001	✓	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	✗	
	0x068	00100 0000009 1		✗	Fixed	0x055	✗	
Users	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 [7.11.9](#)) to display the desired DECT phone device data.

The following tasks can be performed:

- **Configure:** Configure selected DECT phone device dataset (see section [7.11.6](#)).
- **Delete:** Delete selected DECT phone device dataset (see section [7.11.8](#)).
- **Subscription:** Start DECT phone subscription (see section [7.11.7](#)).
- **Wildcard subscription:** Start DECT phone wildcard subscription (see section [7.11.7](#)).
- **Select columns:** Select parameter columns to be shown in table (see section [7.11.9](#)).
- **Filter:** Filter DECT phone datasets shown in table for string set in filter mask (see section [7.11.10](#)).

7.11.4 DEVICE DETAIL SECTION

The **Device detail** section is used for configuration/showing of device settings and creation of new DECT phone datasets.

To open the **Device detail** section,

- choose one of the commands in the task bar on the right of the **DECT Phones** section (**Configure**)

or

- double-click on the appropriate device entry in the device table

The **Device detail** section contains the different parameter groups sorted in tabs. The tabs displayed depend on the current mode and the section from which the DECT phone detail section was invoked.

- **Overview** section (configuration and monitor mode): The DECT phone detail section contains all tabs listed below.

- **User section** (configuration mode): The DECT phone detail section contains all tabs but not DECT.
- **Device section** (configuration mode): The DECT phone detail section contains only DECT.

7.11.4.1 “General” tab

The General tab contains general settings for the DECT phone dataset.

- **Name:** The DECT phone user name (up to 20 characters).
- **Number/SIP user name:** 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.
- **Alternative display number:** Certain call servers assign a single number to a user while assigning different individual numbers to the user's devices. To show the original user number on the device rather than the individual device number, use the **Alternative display number** parameter to configure an alternative display number for the user.
- **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”.

7.11.4.2 “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 [9.19.5](#).
- **Used for visibility checks:** Enables the use of this user account to check the availability of the iPBX (for example, in fail over situations). See section [9.19.7](#) for more information on this feature.
- **SIP Profile ID:** Specifies numerical value used to assign a user to a specific SIP Profile.
- **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.

- **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.

7.11.4.3 "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 [7.7.4.7](#)).

- **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.

7.11.4.4 "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 (for example, 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 [9.19.7](#).

7.11.4.5 "DECT" tab

The DECT tab contains parameters DECT configuration of the DECT phone dataset. When configuring a device (see [7.11.3](#)), only the **DECT** tab is shown in the DECT phone detail section.

- **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 600/700 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 [7.7.1](#)), 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) 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.

7.11.4.6 “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).

7.11.4.7 “Locating” tab

The Locating tab contains parameters for configuring location parameters for the DECT phone.

- **Tracking:** If this option is enabled, the operator of a 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.

7.11.4.8 “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 600/700 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 600/700 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
- **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.

- **Permanent:** Indicates that the user data set is deployed to all OMMs. This allows the user to roam between sites even if the connection between OMM and MOM is down.

The number of permanent users is limited to 512. Permanent users cannot be provisioned externally (that is, if the user type is set to **External**).

7.11.4.9 “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.

7.11.4.10 “Configuration data” tab

The Configuration data tab allows you to assign a Configuration over Air (CoA) profile to a DECT phone user. See section [9.22](#) 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.

7.11.4.11 “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 an XSI request (for example, /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.

Device #0x001 - User #0x001

General	SIP	Incoming calls	Conference	DECT	Messaging	Locating
Additional services	User monitoring	Configuration data	User service	Key lock		

Use SIP user name:

Use SIP user authentication:

User name:

Authentication name:

Password:

Password confirmation:

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.

7.11.4.12 “Key lock” tab

The Mitel 600/700 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 600/700 DECT phone. To prevent change of the time by the user disable the feature here.
- **Time:** The time 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.

	User ID	Name	Number/SIP user name	Login/Add ID	User rel. type
☒	0x001	name 5001	5001	5001	Fixed
☐	0x002	perm5200	5200	5200	Fixed
☐	0x003	my_5201	5201	5201	Fixed
☐	0x004	crt omm 5203	5203	5203	Unbound
☐	0x005	perm 5202	5202	5202	Fixed
☐	0x006	set to perm 5204	5204	5204	Unbound

User #0x001

General

SIP

Incoming calls

Conference

Messaging

Locating

Additional services

User monitoring

Configuration data

User service

Key lock

Active

☒

Time

None

▼

PIN

PIN confirmation

OK

Cancel

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 600/700 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 600/700 DECT Phone USB interface is locked automatically when the phone is locked with a PIN.

7.11.5 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 section opens and provides tabs where the DECT phone data must be entered.

- 2 Configure the DECT phone, see parameter description in section [7.11.4](#).
- 3 Press the **OK** button.

7.11.6 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 section opens.

- 2 Change the DECT phone dataset as desired, see parameter description in section [7.11.4](#).
- 3 Press the **OK** button.

7.11.7 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** section and in the **Device** section. 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 [6.7.10.1](#).
- **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 [6.7.10.2](#).

7.11.8 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** section 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**.

7.11.9 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.

7.11.10 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** section.
- 5 In the **Filter** dialog click on the **Reset** button.

7.11.11 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.

7.11.12 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'.

7.11.13 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

7.12 “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 [9.20](#).

Configuration	ID	Name	Conference ID	Fixed SIP port	Calculated SIP port	Tasks
- Status - System - Sites - DECT base stations - WLAN - DECT phones - Conference rooms - System features - Licenses - Support						- Create - Configure - Delete

The tasks which can be performed are mode-dependant.

Configuration mode	Monitor mode	See section
Configure: Configure selected conference room		7.12.2
	Show details: Show details about a selected conference room	7.12.3

7.12.1 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.

- 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**.

7.12.2 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**.

7.12.3 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.

7.12.4 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.

7.13 “SYSTEM FEATURES” MENU

The **System features** menu provides the following entries:

Configuration mode	Monitor mode	See section
General settings	General settings	7.13.1
Feature access codes	Feature access codes	7.13.2
Alarm triggers	Alarm triggers	7.13.3
Digit treatment	Digit treatment	7.13.4
Directory	Directory	7.13.5
Directory (comp.mode)	Directory (comp.mode)	7.13.7
XML applications	XML applications	7.13.8
CoA profiles	CoA profiles	7.13.9

7.13.1 “GENERAL SETTINGS” MENU

The **General settings** menu allows to configure/view the FAC number prefix used for feature access codes and alarm triggers.

Configuration

- Status
- System
- Sites
- DECT base stations
- WLAN
- DECT phones
- Conference rooms
- System features
 - General settings
 - Feature access codes
 - Alarm triggers
 - Digit treatment
 - Directory
 - Directory (comp. mode)
 - XML applications
 - CoA profiles

General

FAC number and prefix for alarm triggers

OK Cancel

- 1 **FAC number and prefix for alarm triggers:** Enter a unique FAC number.
- 2 Press the **OK** button.

7.13.2 “FEATURE ACCESS CODES” MENU

The **Feature access codes** menu is used to configure/view the feature access codes parameters.

Configuration

Status
System
Sites
DECT base stations
WLAN
DECT phones
Conference rooms
System features

General settings
Feature access codes
Alarm triggers
Digit treatment
Directory
Directory (comp. mode)
XML applications

Feature access codes

FAC number

Activate subscription
☐

Activate wildcard subscription
☐

Deactivate subscription
☐

User login
☐

User logout
☐

Set system credentials for provisioning
☐

Blind transfer
☐

OK
Cancel

The **FAC number** which introduces the feature access code (see also section [7.13.1](#)) is displayed. For a description of the parameters which can be set in this menu see section [6.9.4](#).

7.13.3 “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.

Configuration

Status
System
Sites
DECT base stations
WLAN
DECT phones
Conference rooms
System features

General settings
Feature access codes
Alarm triggers
Digit treatment
Directory
Directory (comp. mode)
XML applications
CoA profiles
Licenses

	ID	Trigger ID	Feature access code	Comment	Number	Tasks
☐	0	SOS	SOS			Create Configure Delete
☐	1	MANDOWN	MANDOWN			

New alarm trigger

General

Trigger ID

Feature access code

Comment

Prefix

Number

OK
Cancel

The tasks which can be performed are mode-dependant.

Configuration mode	Monitor mode	See section

Create: Create alarm trigger		7.13.3.1
Configure: Configure a selected alarm trigger		7.13.3.2
	Show details: Show parameters of a selected alarm trigger	7.13.3.3
Delete: Delete selected alarm triggers		7.13.3.4

7.13.3.1 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 [7.13.1](#)).
- 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.

7.13.3.2 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.

7.13.3.3 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**.

7.13.3.4 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.

7.13.4 “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.

Configuration	ID	External pattern	Internal pattern	Direction	Directory	Sites	Tasks
- Status - System - Sites - DECT base stations - WLAN - DECT phones - Conference rooms - System features - General settings - Feature access codes - Alarm triggers Digit treatment - Directory - Directory (comp. mode) - XML applications - CoA profiles - Licenses							- Create - Configure - Delete

New digit treatment entry

General

External pattern

Internal pattern

Direction

Apply to directory

Sites

OK

Cancel

Incoming and outgoing calls

▼

All

Select

For a description of tasks and parameters available in this menu, see section [6.9.1](#).

7.13.5 “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
Configure: Configure selected directory entry in detail section		7.13.5.2
	Show details: Show selected directory entry in detail section	7.13.5.3

7.13.5.1 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** section, click **Create**.

The **New directory entry** section 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** section:

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: • 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 (for example, "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: • "<TEL>" (for the user's telephone number) • "<DESC1>" (for the user's "Description 1" attribute) • "<DESC2>" (for the user's "Description 2" attribute)	ü		

Parameter	Description	LDAP	XML	XSI
	“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
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. 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 provisioning security configuration	Enables or disables use of the system's certificates (loaded for provisioning purposes) for HTTPS directory access.		✓	✓

7.13.5.2 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** section.
- 3 Change the directory entry parameters as required (see parameter descriptions in section [7.13.5.1](#)).
- 4 Click **OK**.

7.13.5.3 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 section.
- 3 Click **Cancel** to close the directory entry detail section.

7.13.6 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**

7.13.7 “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.

The screenshot displays the Mitel OMP Management Portal interface. The top navigation bar includes the Mitel logo, a settings gear icon, a search magnifying glass icon, and a pencil icon. On the right side of the top bar are links for 'General' and 'Help'. The left sidebar contains a 'Configuration' menu with various options: Status, System, Sites, DECT base stations, WLAN, DECT phones, Conference rooms, System features (with sub-items: General settings, Feature access codes, Alarm triggers, Digit treatment, Directory, **Directory (comp. mode)**, XML applications, CoA profiles), Licenses, and Support. The main content area shows a table with columns: Order, Type, Active, Name, and Server. The table is currently empty. To the right of the table, under the 'Tasks' header, are two buttons: 'Configure' and 'Delete'. At the bottom left of the interface is an 'Info console' section.

7.13.7.1 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:

- 1 In the **Tasks** section, click **Create**.

The **New directory entry** section 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** section:

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 (for example, "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: • "<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.

Parameter	Description
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.

7.13.7.2 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** section.
- 3 Change the directory entry parameters as required (see parameter descriptions above).
- 4 Click **OK** to save your changes.

7.13.7.3 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 section.
- 3 Click **Cancel** to close the directory entry detail section.

7.13.7.4 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.

7.13.8 “XML APPLICATIONS” MENU

The SIP-DECT XML terminal interface allows external applications to provide content for the user on the Mitel 600/700 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 [6.9.5](#).

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 600/700 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 [7.13.5.1](#).

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.



The tasks you can perform in the **XML applications** menu are mode-dependant.

Configuration mode	Monitor mode	See section
Create: Create new XML hooks		7.13.8.1
Configure: Configure selected XML hook in detail section		7.13.8.2
	Show details: Shows selected XML hook in detail section	7.13.8.3
Delete: Delete selected XML hook		7.13.8.4

7.13.8.1 Creating a New XML Hook

In addition to the 15 predefined XML hooks, you can create up to 10 additional XML hooks. You can only add XML hooks in **Configuration Mode**.

The screenshot shows a 'New XML application' dialog box with the following fields and options:

- Active:** A checkbox that is checked.
- Name:** A text input field.
- Protocol:** A dropdown menu currently set to 'HTTP'.
- Port:** A text input field.
- Use default port:** A checkbox that is checked.
- Server:** A text input field.
- User name:** A text input field.
- Password:** A text input field.
- Password confirmation:** A text input field.
- Path (and parameters):** A text input field.
- Buttons:** 'OK' and 'Cancel' buttons at the bottom.

To add an XML hook, do the following:

1 In the **Tasks** bar click on **Create**.

The **New XML application** section opens.

2 Specify values for the following XML hook parameters:

- **Active:** This setting activates or deactivates a configured XML application entry.
- **Name:** The predefined hooks have fixed predefined names. A name must be configured for the free defined hooks.
- **Port:** Specifies the certificate server's port number.
- **Use default port:** If selected, the default port associated with the selected protocol is used.
- **Protocol:** Select the protocol HTTP or HTTPS.
- **Server:** Enter the IP address or the name of the server which provides the XML content.

Note: SIP-DECT 6.0 and later supports "SIPProxy" placeholders for XML Server application URLs within SIP redundancy setups. In cases where applications are located on a SIP server, it is

necessary to address XML applications by using the current primary, secondary or tertiary SIP server address. In those cases, the "SIPProxy" placeholder can be used as server input.

- **User name:** Enter the login user name if an authentication is required by the server.
- **Password, Password confirmation:** Enter the password if the authentication is required by the server.
- **Path (and parameter):** Enter the 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.

7.13.8.2 Modifying an XML Hook

You can only modify XML hooks in **Configuration Mode**.

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

- 1 Select the appropriate XML hook in the table.
- 2 In the **Tasks** bar, click **Configure**.
- 3 Edit the XML application parameters (described above) as necessary. 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.

See the description comment in chapter 6.9.5.

4 Click **OK**.

7.13.8.3 Viewing XML Hook Details

You can view the configuration of an XML hook in **Monitor Mode**. Do the following:

- 1 Select the appropriate XML hook 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 section.
- 3 Click **Cancel** to close the XML hook detail section.

7.13.8.4 Deleting XML Hooks

You can only delete XML hooks in **Configuration Mode**. You cannot delete any predefined XML hooks.

To delete an XML hook, do the following:

- 1 Select the appropriate XML hook(s) in the table by activating the corresponding checkbox(es).
- 2 In the **Tasks** bar, click **Delete**.
A confirmation dialog opens.
- 3 Click **OK** to confirm.

7.13.9 “COA PROFILES” MENU

SIP-DECT 6.0 and later supports central configuration over the air (CoA) for Mitel 602 DECT phones. The CoA profiles page lists the available CoA profiles that can be downloaded to the DECT phones.

Note: The profiles generated by the user_common.cfg configuration file are also listed in this window. When managed with OMP, they can be overwritten when the user_common.cfg configuration file is reloaded. The maximum download size is 4kB.

You can import CoA profiles via the **CoA Profiles** menu. Once you have imported the profiles, you can assign them to specific DECT phone users.

The screenshot shows the OMP interface with the 'CoA profiles' menu item selected in the left sidebar. The main window displays a table with columns 'ID', 'Name', and 'Status'. Below the table, the 'New CoA profile' dialog box is open, showing the 'General' tab. The dialog has fields for 'Name', 'Default' (a checkbox), and 'ID' (a drop-down menu). An 'Import file' button is located below the 'ID' field. At the bottom of the dialog are 'OK' and 'Cancel' buttons. On the right side of the main window, under the 'Tasks' column, there are links for 'Create', 'Configure', and 'Delete'.

To create a new CoA profile:

- 1 Click **Create** under the Tasks list on the right-hand side of the **CoA profiles** window. The **New CoA profile** dialog opens.
- 2 Configure the settings for the CoA profile:
 - **Name:** Specify a name for the CoA profile
 - **Default:** Indicate whether this is the default CoA profile to be used
 - **ID:** Select an ID for the CoA profile from the drop-down menu.
- 3 Click **Import file** to select the CoA file to import.

The **CoA profiles** page displays the new CoA profile in the table.

7.14 “LICENSES” MENU

The **Licenses** page provides an overview of licenses currently in use. In **Configuration Mode**, you can also import a license file.

The license information is displayed in the following tabs:

- **Status:** Shows general license information.
- **License file:** Allows import of a license file.
- **System:** Shows system license status.
- **Messaging:** Shows Integrated Messaging and Alerting Service (IMA) license status.
- **Locating:** Shows Locating license status.

“Status” tab

The Status tab displays general information about the current system license.

“License file” tab

The License file tab allows you to import a license file (only possible in **Configuration Mode**).

- 1 Click the **File** button to select the path and file name where the license file is stored.
- 2 Click the **Import** button.

“System” tab

The “System” tab provides OM System license information. This includes supported software version and number of licensed DECT base stations (RFPs) compared to number of connected DECT base stations.

“Messaging” tab

The “Messaging” tab provides OM Messaging and Alerting license information.

“Locating” tab

The “Locating” tab provides Locating license information.

7.15 “SUPPORT” MENU

Support section summarizes existing SIP-DECT maintenance functions. These functions can be configured in one place and are clearly distinguished from other SIP-DECT features. The Maintenance section comprises:

- **DECT phone firmware update:** activation of the firmware update and configuration of an alternative update source
- **Syslog server:** activation and Syslog server address
- **System dump:** start of a manually local system dump onto the PC running the OMP
- **Remote System dump:** activation, time of day and destination of a system dump to a remote server
- **Core dump:** configuration of a specific server to which core dumps are sent.

7.15.1 DECT PHONES FIRMWARE UPDATE

With SIP-DECT 6.0 or later, the DECT base station software images (iprpf3G.dnld and iprpf4G.dnld) contains the Mitel 600/700 DECT phone software. For specific maintenance purposes only, you can configure a URL to use an alternative DECT phone software image. The Mitel 600/700 DECT phone firmware packages are delivered in the “600.dnld/700.dnld” file for the OMM running on a DECT base station.

- **Activate firmware update:** Enables or disables the “Download over Air” feature. The OMP provides a DECT phone firmware update over the air when this feature is activated. For more information on, see section [9.21](#).
- **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.
- **Default 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 provisioning security configuration:** Enables the use of the system-wide certificate validation settings for this URL, as configured on the **System -> Provisioning -> Provisioning certificates** page (see section [6.4.2.14](#)).

7.15.2 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.

7.15.3 SYSTEM DUMP

System Dump tab allows you to import a system file manually in local directory.

- 1 Click the **Directory** button to select the path where the system file needs to be stored.
- 2 Click the **Download** button.

7.15.4 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 fileserver allows writing or creating system dumps.

For a description of the parameters on the **Remote system Dump** tab, refer to the description of the **Support** page of the OMM Web service. The same parameters are described in the **System dump** section (section [6.12.3](#)).

7.15.5 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).

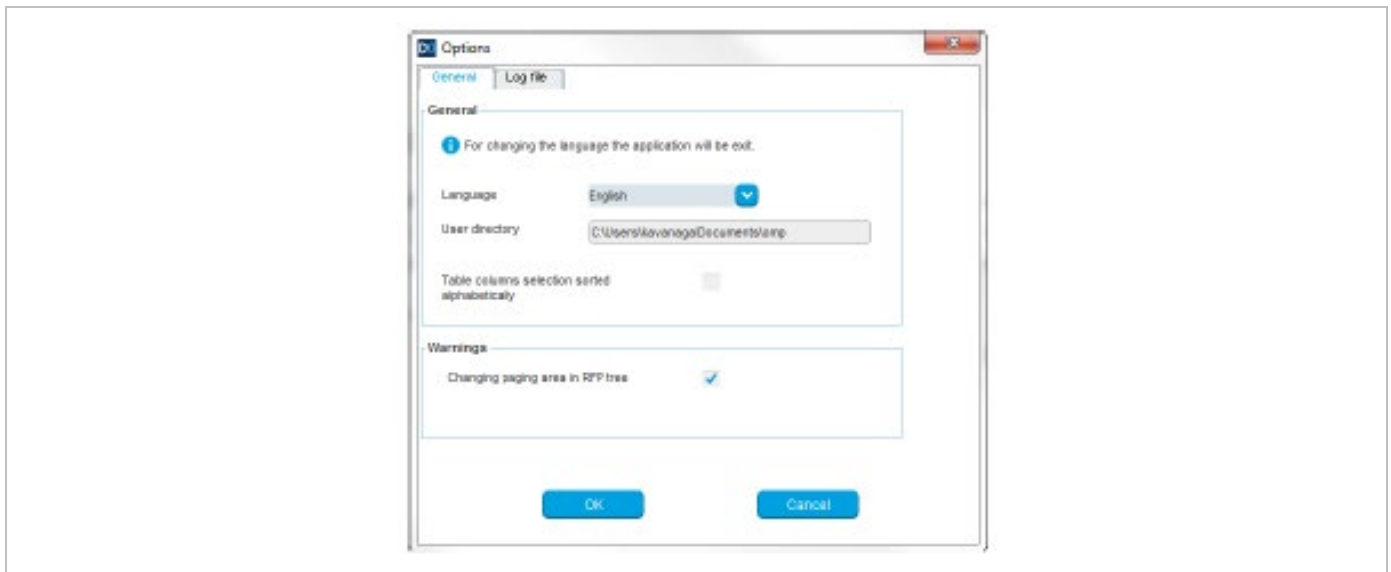
For a description of the parameters on the **Core Dump** tab, refer to the description of the **Support** page of the OMM Web service. The same parameters are described in the **Core dump URL** section (section 6.12.4).

7.16 “GENERAL” MENU

The **General** menu is available in all program situations. It contains following submenus:

- **Exit:** Selecting this menu entry opens the exit dialog to close the OMP.
- **Options:** Selecting this menu entry opens the **Options** dialog (see below).

“Options” - “General” tab



Language: You can select the OMP language. After changing the language, the OMP is automatically closed and must be started again.

The field **User directory** shows the path where the following files are saved if necessary:

- System dump file “sys_dump.txt”
- Expert console log file “spy.log” when the application terminates
- Exception log file “spy_trace_<date>_pxxx” in case of a Java exception, file name extension “xxx” ranges from 000 to 999

In the **Warnings** section you can activate/deactivate the display of warning messages in the OMP.

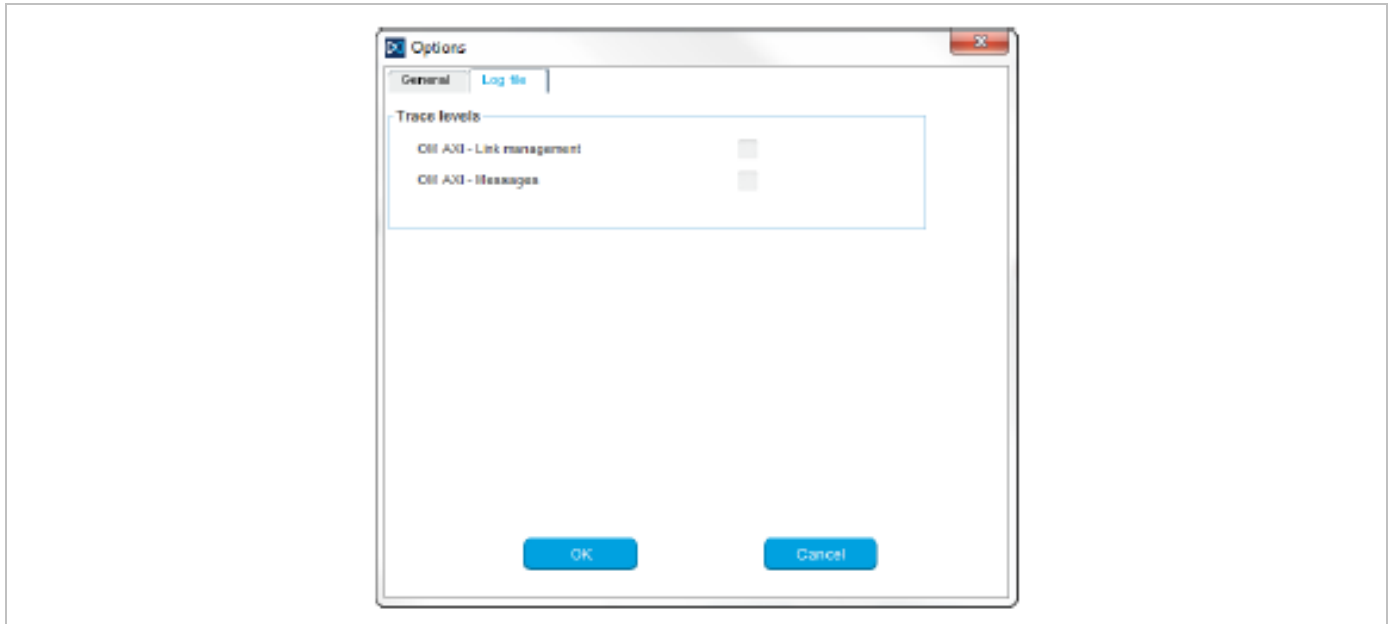
Notes on log files

The mechanism for creating the log files is the same as the PC OMM spy log mechanism, what means:

- The maximum size of the log file is 1 GB

- 1000 log files per day at maximum
- Only the 30 newest created log files are kept, older ones are removed automatically
- Log files older than 6 days are removed

“Options” - “Log file” tab

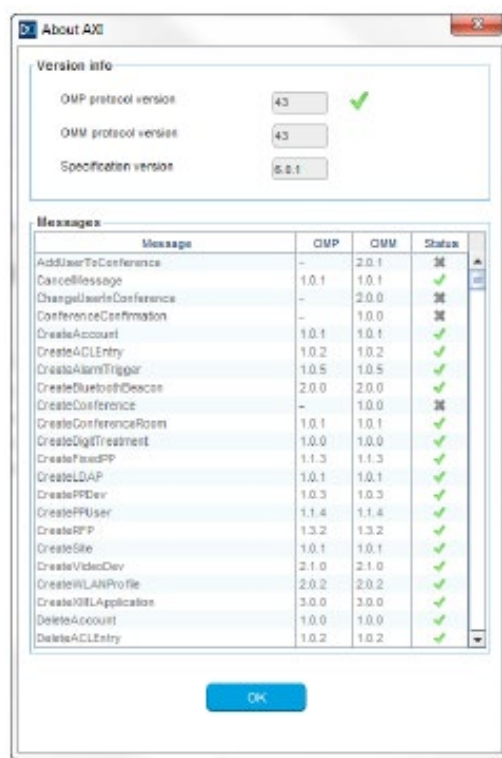


In the **Log file** tab you can enable several trace levels.

7.17 “HELP” MENU

The **Help** menu is available in all program situations. It contains following submenus:

- **Info:** Selecting this menu entry displays the End User License Agreement (EULA).
- **About AXI:** Selecting this menu entry displays the About AXI dialog. This dialog compares the protocol version numbers which are provided by the OMM with the protocol version numbers supported by the OMP. The warning icons ⚠ or ✖ show a version mismatch. A version number “-” means the protocol element is not used by OMP.



- **About OMP:** Selecting this menu entry displays the OMP version info and copyright.

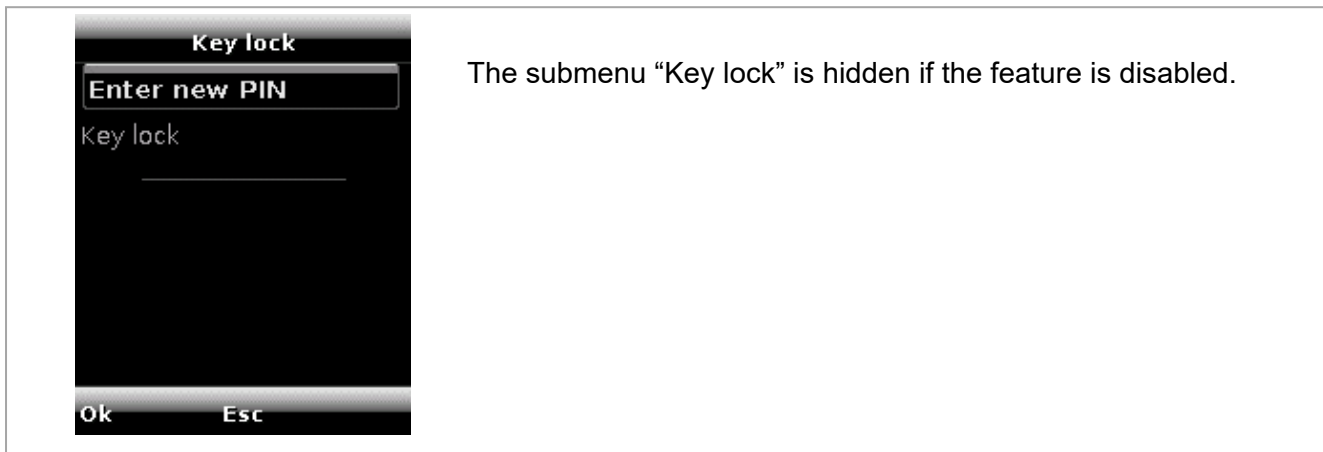
8 DECT PHONE

The DECT phone has a special system menu for administration of the DECT system.

8.1 KEY LOCK WITH PIN

8.1.1 MAINTAIN THE PIN

The PIN is used to allow access to the Security menu and to lock the phone. The user can adjust his PIN and the feature Key lock with PIN here: System menu/Administration.

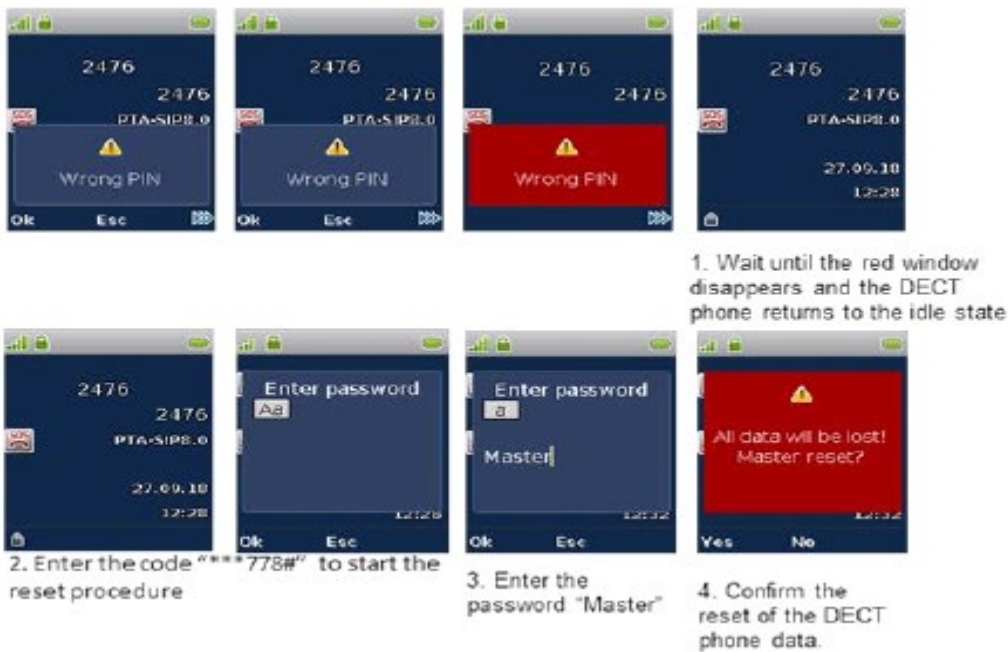


The update to SIP-DECT 7.1SP1 causes a reset of the DECT phone key lock PIN to default "0000".

8.1.2 UNLOCK A LOCKED MITEL 600/700 DECT PHONE

The DECT phone can be reset to factory defaults if the DECT phone is protected with a PIN, and no other option can be used to unlock the phone; for example, set the PIN through the OMM to a defined value.

If a wrong PIN are successively entered 3 times, then a reset procedure can be activated by entering the code "***778#".



The reset procedure requests the password "Master" to reset all data on the phone, which also removes the subscription and the PIN lock.

The DECT phone needs to be subscribed with a DECT system after the reset.

Note: Be aware that the **Master reset** deletes all data from the DECT phone.

8.1.3 SET UP AUTOMATIC KEY LOCK WITH PIN

The following pictures show an example how to turn off the DECT phone key lock with PIN through the Mitel 600/700 DECT Phone UI.

1. Select the lock key and enter the PIN to unlock the phone
2. Long press menu soft key to open the System menu
3. Select Administration
4. Select Key lock
5. Enter the new PIN and select OK
6. Change the key lock parameter (optional)
 - a. Time for the automatic key lock is set to 120 seconds
 - b. Off and various timer values are available
 - c. Choose the desired value, for example, Off and confirm with OK
7. Confirmation is displayed to show that the chosen values are stored.
8. Key lock with PIN is Turned Off.

The update to SIP-DECT 7.1SP1 causes a reset of the DECT phone key lock PIN to default "0000".

9 CONFIGURATION AND ADMINISTRATION

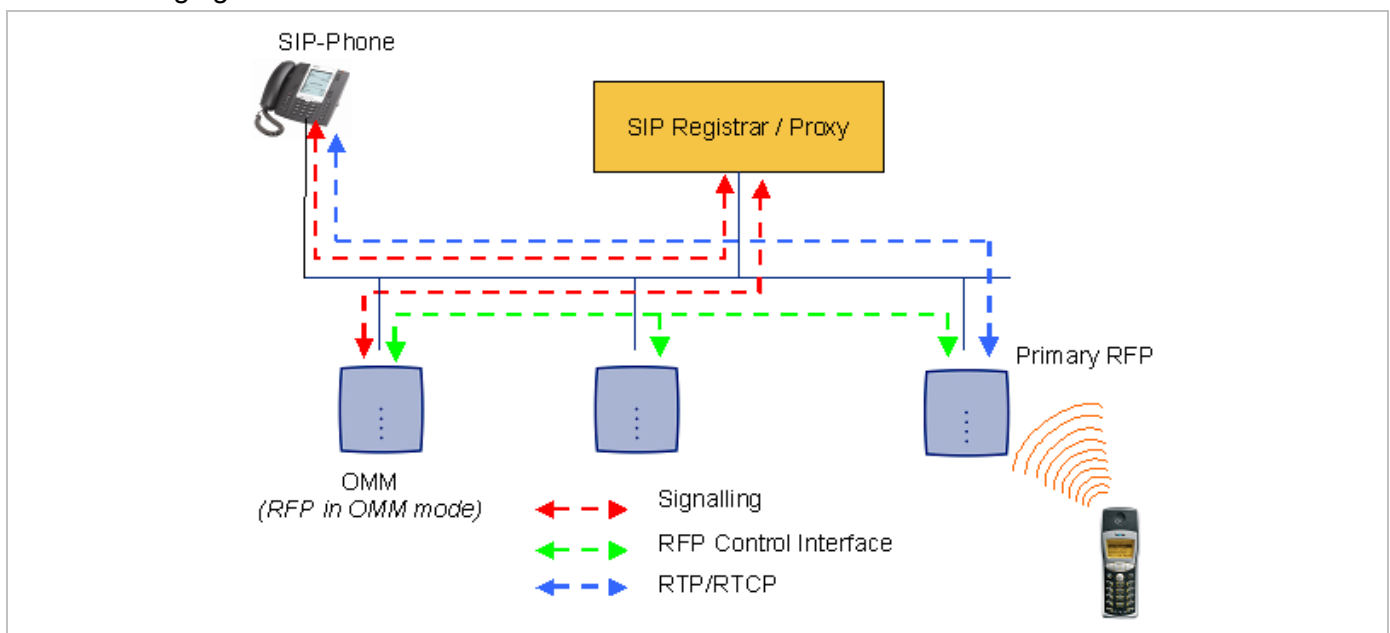
This section provides detailed information on various configuration and administration aspects of the SIP-DECT solution.

9.1 IP SIGNALING AND MEDIA STREAM

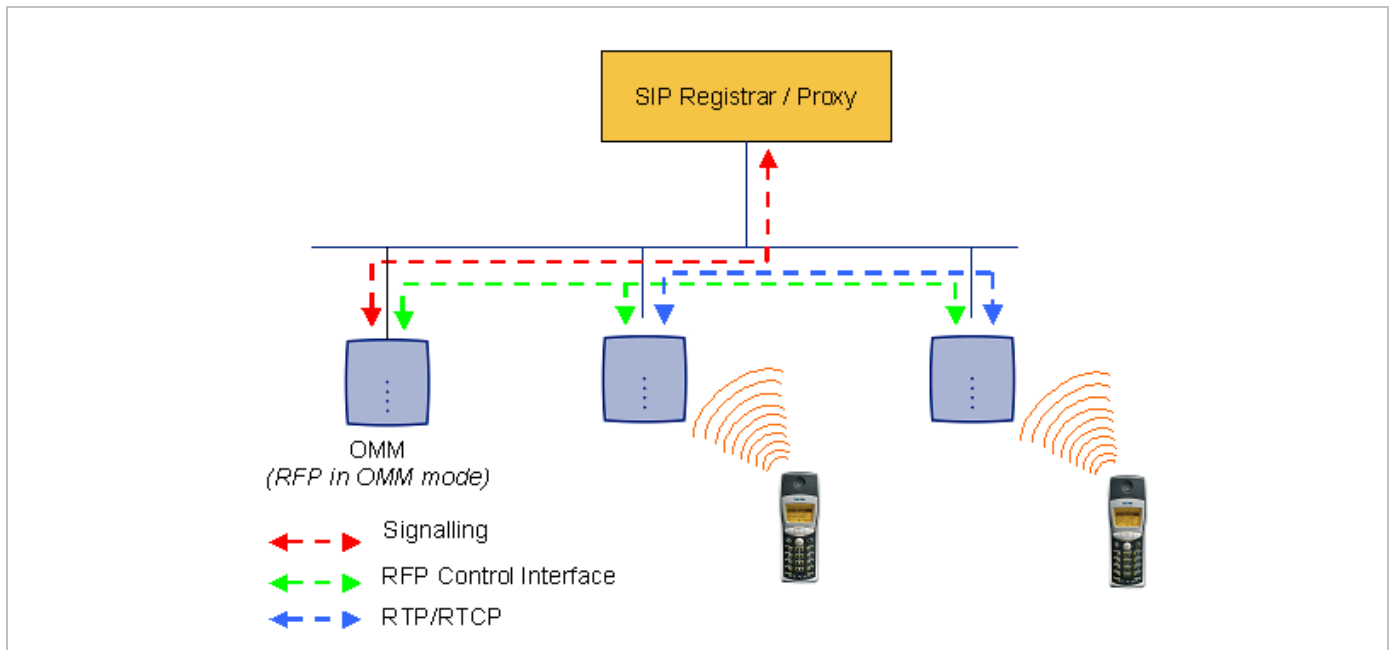
To establish a call between an IP Phone and a DECT phone (for example, Mitel 600/700), the following IP streams must be established:

- A signaling channel to and from the SIP phone.
- A signaling channel to and from the OMM.
- A control interface between the OMM and the RFP that has a connection to the DECT phone (known as the primary RFP).
- A Real Time Protocol (RTP) / Real Time Control Protocol (RTCP) connection between the SIP phone and the primary RFP.

The following figure illustrates this scenario.

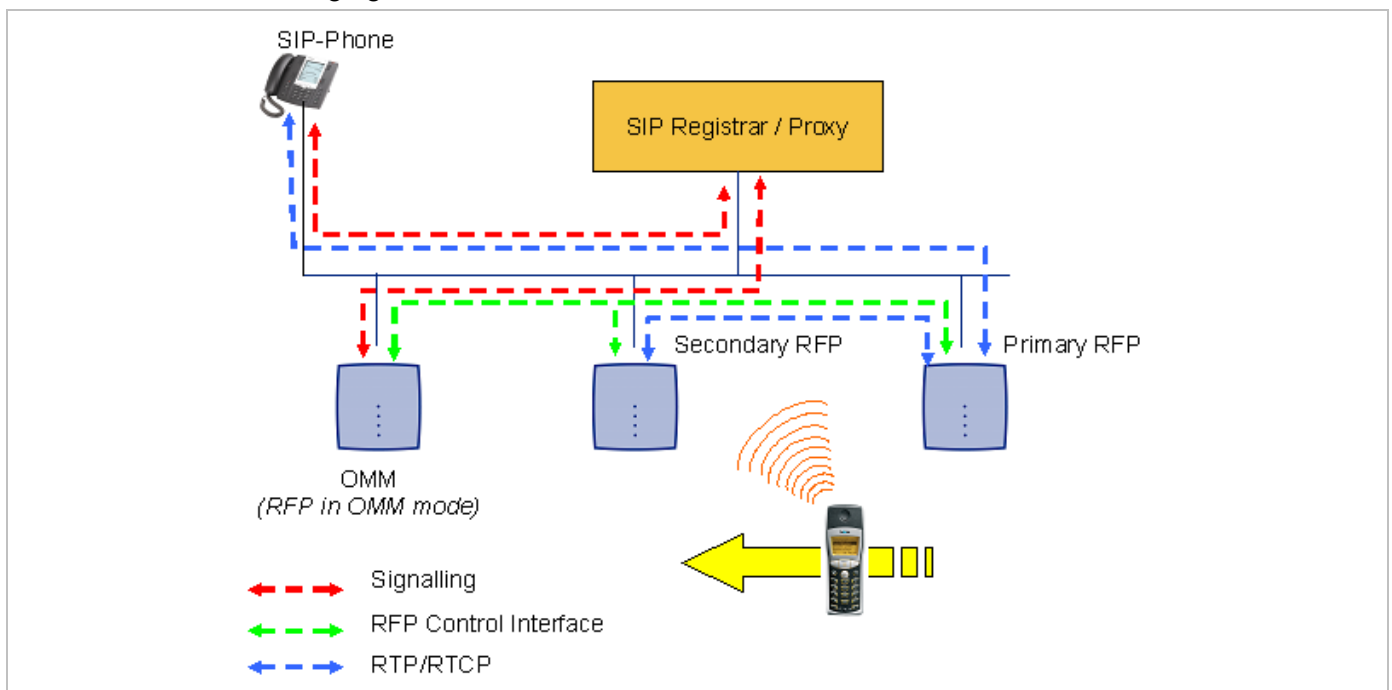


To establish a call between two DECT phones, the same IP streams must be established like in the scenario before, except the IP phone is not involved. The following figure illustrates this scenario.

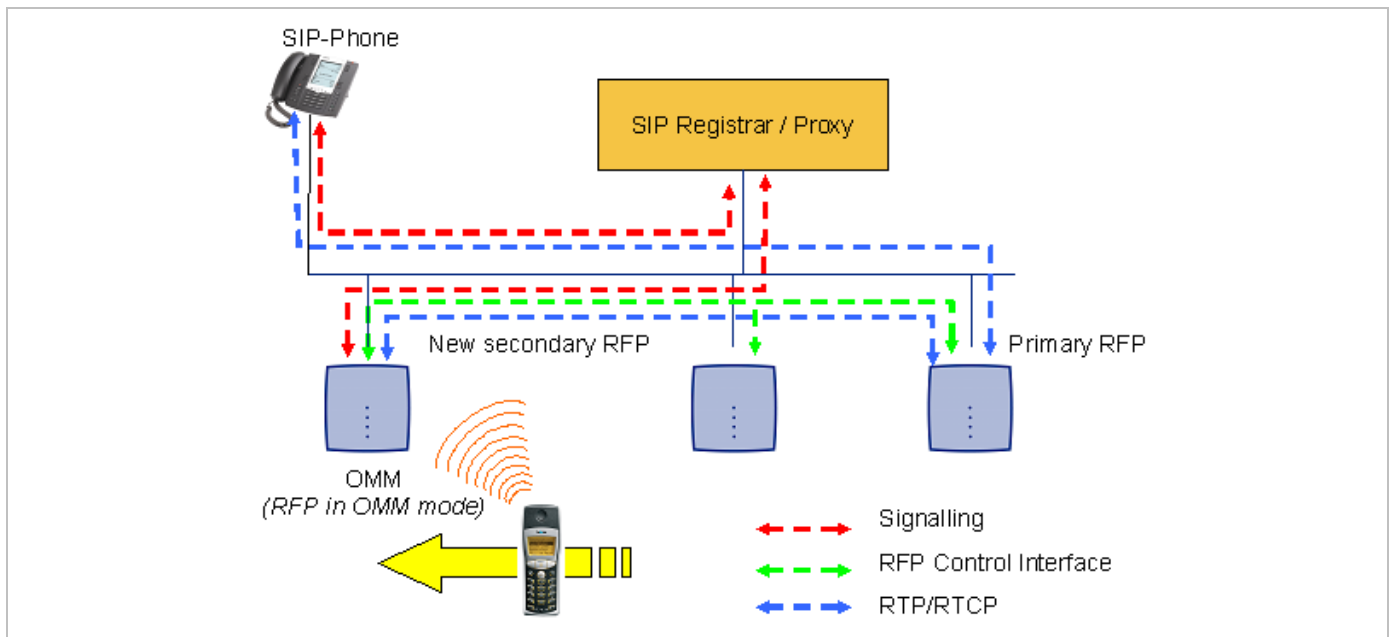


A call from one DECT phone to another that resides on the same RFP will loop back within the RFP if no media gateway is involved. So the call will not pass through to the Local Area Network (LAN). Although the voice packets will not impact LAN traffic, signal packets will.

If the DECT phone user is moving, the DECT phone detects that another RFP has a better signal strength and, therefore, it starts the handover process. The media stream from the IP phone cannot move to the secondary RFP, so the primary RFP uses the LAN to direct the voice to the secondary RFP, as shown in the following figure.



As the DECT phone user moves into the next RFP zone of coverage, the DECT phone detects that the RFP has a better signal strength. Again the media stream from the SIP phone cannot move to the secondary RFP, so the primary RFP uses the LAN to direct the voice to the new secondary RFP.

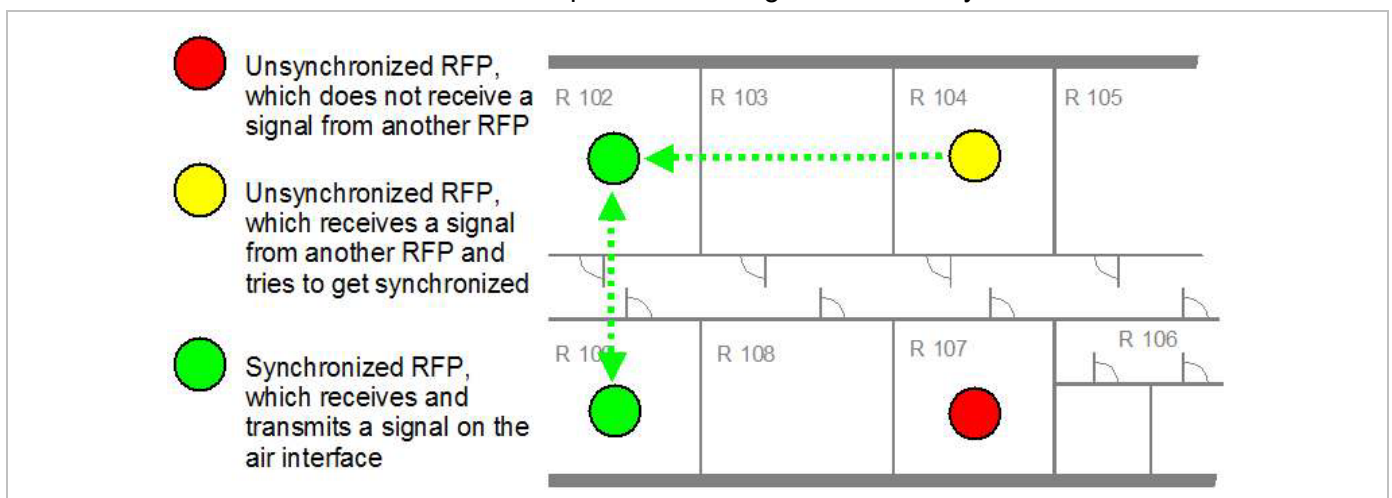


9.2 DECT BASE STATION SYNCHRONIZATION

To guarantee a seamless handover if a caller moves from one DECT base station zone of coverage to another DECT base station zone of coverage, an accurate synchronization of the DECT base stations is necessary.

The DECT base stations are synchronized over the air interface. The first DECT base station to complete startup transmits a signal on the air for the other DECT base stations to synchronize from. If a DECT base station gets in sync, it transmits a signal on the air and becomes the sync source for the next DECT base station. Only DECT base stations that can receive a synchronization signal become synchronized.

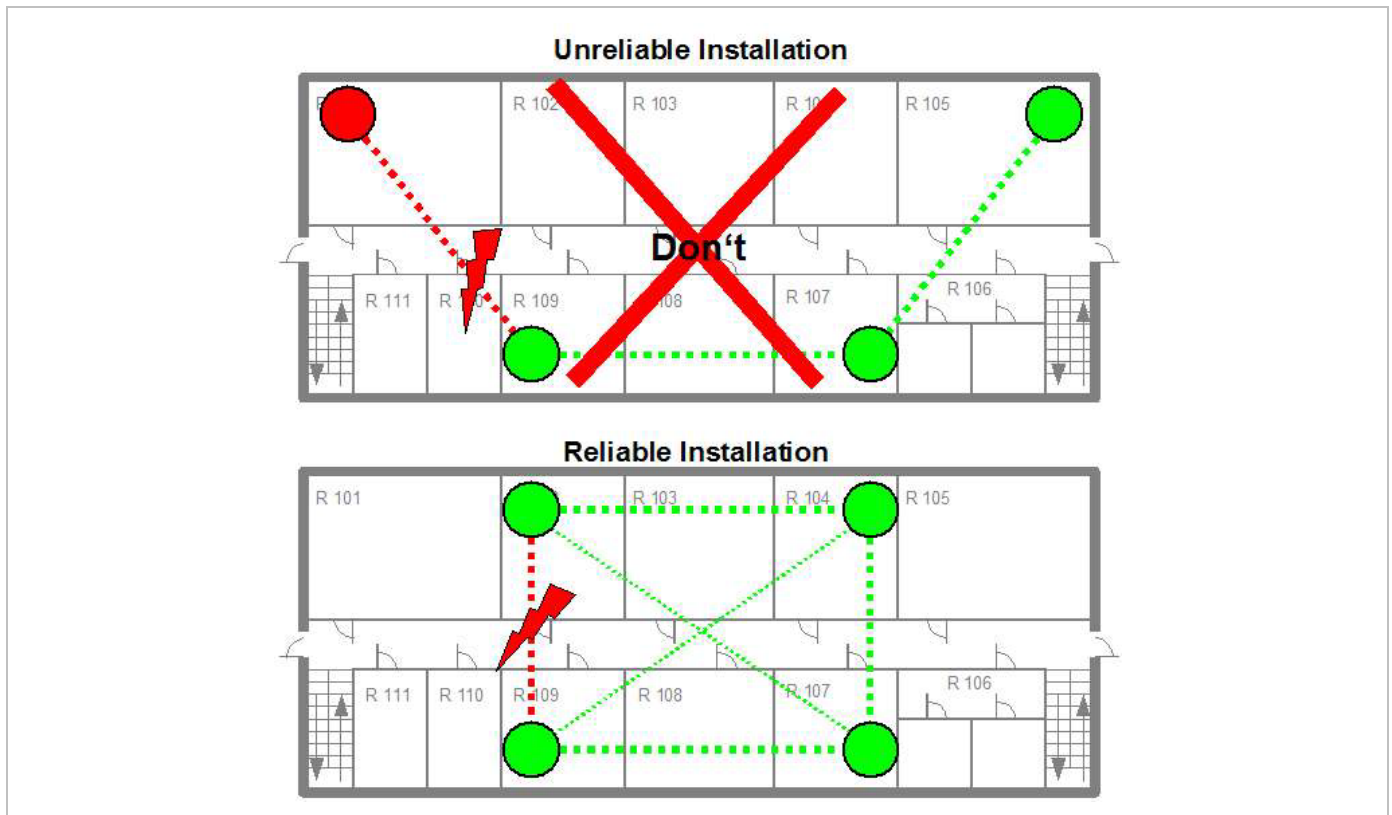
For the DECT base station to sync to another DECT base station, the signal strength cannot drop below -70 dBm. You must consider this requirement during the site survey.



As long as a DECT base station is not in sync, no calls can be established using this DECT base station.

If a DECT base station loses the synchronization, the DECT base station does not accept new calls ("busy bit"). There is a delay of maximum 3 minutes until the active calls on this DECT base station are finished. Then it tries to get synchronized again.

A SIP-DECT installation is more reliable if a DECT base station can receive the signal from more than only one DECT base station because the other signals are also used for synchronization.



The sync-over-air solution is very reliable because all existing redundant paths are used for synchronization. Thus, hardware tolerances have only very little influence. No DECT base station has a key position. Only unfavorable setups without redundant synchronization paths can cause problems. Sometimes DECT base stations do not need to be synchronized (for example, if they are in different buildings). These DECT base stations can be put into different clusters. DECT base stations in different clusters are not synchronized with each other. Different clusters start up at the same time independently.

9.2.1 INITIAL SYNCHRONIZATION PROCEDURE

To avoid synchronization problems and to speed up the synchronization on system startup, an initial synchronization procedure is used. For every cluster the following synchronization stages are defined.

- Synchronization stage 0
 - If at least one preferred DECT base station was configured, the synchronization process waits up to 30 seconds for an incoming startup message of such a preferred DECT base station. Receiving a message will finish stage 0 and the synchronization process jumps to stage 1.
 - If no message is received within 30 seconds, this stage will be terminated and the next stage begins.
 - If no preferred DECT base station was configured, this stage is ignored.
- Synchronization stage 1
 - If a preferred DECT base station was determined in stage 0, this one becomes the synchronization source for the subsequent DECT base stations. Otherwise

the first DECT base station that sends a startup message becomes the synchronization source for the subsequent DECT base stations.

- In this stage, only DECT base stations reporting an RSSI value better than -65 dBm are permitted to perform synchronization.
- If a DECT base station has completed its synchronization, this DECT base station will be also a synchronization source for other upcoming DECT base stations.
- The initial timeout for this stage is 30 seconds. Whenever a DECT base station has finished its synchronization in this stage a new stage timeout value is calculated.
- If no DECT base station comes up within the timeout time or if all the upcoming DECT base stations do not fit the RSSI threshold, this stage will be terminated and the next stage begins.
- Synchronization stage 2
 - The behavior of this stage is identical to stage 1, but an RSSI threshold value of -70 dBm is significant.
- Synchronization stage 3
 - The behavior of this stage is identical to stage 1, but an RSSI threshold value of -75 dBm is significant.
- Synchronization finished
 - No more RSSI threshold value is significant. All DECT base stations that failed the stage conditions above are now permitted to perform synchronization.

The last level “synchronization finished” will be achieved either all registered DECT base stations of this cluster are synchronized or the timer of stage 3 expires.

9.2.2 CHECKING THE SYNCHRONIZATION OF A NETWORK

For every cluster a periodically check of the synchronization of the network is done. If the network is split into at least two subnets, all the RFPs of the lesser subnet(s) will be resynchronized. While doing initial synchronization procedure this check is deactivated. You can check the DECT base station synchronization from the **Sync view** menu of the OM Management Portal (OMP), see section [7.9.5](#).

9.3 DECT BASE STATION CHANNEL CAPACITY

The DECT base station has 12 available time slots on air; eight can have associated DSP/media resources for media streams. All DECT time slots are used for control signaling, software download over air, messaging and bearer handover independent of associated DSP/media resources.

If all eight media stream channels are used, the DECT base station announces a “busy bit”. In that case, the DECT phones determine whether another DECT base station has an appropriate signal strength. If so, the DECT phone performs a handover to that DECT base station. Once the handover is complete, the DECT base station lowers its “busy bit”.

Whenever the busy state is announced a log entry is made to the system logs. If the announcement of busy raises in a specific area, an additional DECT base station should be installed to double the number of media streams available for calls.

Notes on Wideband Audio G.722 connections

Each Wideband Audio G.722 connection uses twice the capacity of conventional narrowband on the DECT air interface. Due to this fact, four Wideband Audio G.722 connections (instead of eight) can be established via one DECT base station except for RFP 44 (supports only 2 wideband calls).

It is not possible to have DECT XQ audio combined with Wideband Audio G.722 within the same connection.

9.4 NETWORK INFRASTRUCTURE PREREQUISITES

To establish and maintain an SIP-DECT installation, a network infrastructure is assumed, which comprises at least the following components:

- DECT base stations
- DECT phones
- IP PBX/media server (for example, Asterisk)

Depending on the operational modes the following services should be provided:

- DHCP
- SNTP
- DNS
- LDAP
- Syslog daemon
- File server for configuration files and software images: HTTP, HTTPS, FTP, FTPS, or TFTP

Notes on network infrastructure prerequisites

- In NA outdoor RFPs may only be installed with the antennas shipped with the units. No other antennas or cabling are permitted. In EMEA the outdoor RFPs are shipped without antennas and you may use the units with one of the optional antennas (separate order no.).
- A TFTP server is no longer required for boot of a 3rd or 4th generation RFPs.
- TFTP, FTP(S), HTTP(S), SFTP are supported for 3rd or 4th generation RFPs software update.

9.5 SIP-DECT STARTUP

This section contains detailed information on the startup (booting) process of the SIP-DECT solution.

The RFPs use the internal flash to start the boot image. A fileserver is only needed for software update over the network.

The essential network settings can be alternatively:

- Communicated by a DHCP server at startup time.
- Configured on the RFP with the OM Configurator tool (see section [9.5.4](#)). The settings made by the OM Configurator will be saved permanently in the internal flash memory of each OMM/RFP.

9.5.1 TFTP AND DHCP SERVER REQUIREMENTS

TFTP server requirements

The DECT base station can update the boot image file from a TFTP server. The RFC 1350 /1/ support is mandatory for the TFTP server.

Note: If many DECT base stations loading the boot image simultaneously, the network load could increase significant. To balance the network load or for backup reasons, it is possible to configure more than one TFTP server in a network.

DHCP server requirements

A DHCP server needs to support RFC 2131 /9/. The TFTP and DHCP server need not to reside on the same host.

9.5.2 BOOTING STEPS

Booting is performed in two steps:

- 1 Load the application image from internal flash.
- 2 Start the application.

9.5.3 APPLICATION STARTUP

After starting the application image, the RFP software checks the local network settings in its internal flash memory. If no settings are available or if they are disabled, the RFP software starts a DHCP client to determine the IP address of the OMM and other application startup settings.

The RFP software acquires the OMM IP address:

- within the local network settings if active
- through DHCP request
- DECT base station configuration file (see [5](#))
- With release 8.1, a 4th generation RFP can be switched to OMM mode by pressing the button of the RFP and executing a procedure.

If the IP address of the actual RFP device matches one of the acquired OMM IP addresses or if the IP address is configured as OMM RFP by pressing the button of the RFP and executing a procedure, the DECT base station software continues in OMM mode. Otherwise, the DECT base station runs as normal DECT base station without OMM mode.

9.5.3.1 DHCP Client

The DHCP client is capable of receiving broadcast and unicast DHCP replies. Therefore the flags field is 0x0000. The DHCP request contains the well-known magic cookie (0x63825363) and the end option (0xFF).

The DHCP client of the RFP family requests several parameters that are used to configure the RFP. The DHCP client vendor class identifier (option 60) is different for the different RFP generations as follows:

- The 3rd generation RFPs (RFP 35/36/37 IP / RFP 43 WLAN) use "OpenMobility3G".
- The 4th generation RFPs (RFP 44/45/47 IP / RFP 48 WLAN) use "OpenMobility4G".

Parameters

The following parameters are supported within this step:

Option / Field	Meaning	Mandatory	Type
yiaddr	IP address of the IP-RFP	yes	ip-address
siaddr	Parameter named "Boot Server Host Name" with value as the IP address of the TFTP server	no	ip-address
file	Parameter named "Bootfile Name" with value of the path (optional) and name of the application image. For example "iprfp3G.dnld" (3 rd generation RFPs) and "iprfp4G.dnld" (4 th generation RFPs).	no	string
option 1	Subnet mask	no	ip-address
option 3	Default Gateway	no	ip-address
option 6	Domain Name Server	no	ip-address
option 15	Domain Name	no	string
option 428	Broadcast Address	no	ip-address
option 43	Vendor-specific options (see table below)	yes	
option 66	Provisioning URL for the OMM (ConfigURL). URL of an external server that provides configuration files for the Base Station(s) hosting the OMM. Note: In SIP-DECT 2.1 - 6.1, this option was used for the RFP Config file server. If you want to specify a URL for the RFP Config file server, use option 233 instead.	no	string
option 132	VlanId	no	integer 16
option 224	Parameter named magic_string. Must be set to value "OpenMobility" or "OpenMobilitySIP-DECT". The client uses this option to select the server.	yes	string
option 226	Enabling 802.1X feature (set to 1).	no	integer 8
option 233	URL that specifies the protocol, server and path to access the DECT base station configuration files (see section 7.9). For SIP-DECT 6.1 or earlier, this option takes priority over option 66 when set.	no	string
option 234	Provisioning URL for the OMM (ConfigURL). URL of an external server that provides configuration files for the Base Station(s) hosting the OMM.	no	string

Option / Field	Meaning	Mandatory	Type
option 236	This mode value determines which instance (OMM, RFP) shall use the given Provisioning URL (Option 43-2, 66 or 234). Valid values are: 1. The RFP shall use the given Provisioning URL. 2. The OMM and RFP shall use the given Provisioning URL. Else: The OMM shall use the given Provisioning URL.	no	integer 8

Vendor specific options

The Vendor Specific Options consist of:

Vendor Specific Option	Meaning	Mandatory	Length
option 1 (SIP-DECT release 6.2 and later)	URL that specifies the protocol, server and path to access the DECT base station configuration files (see section 7.9).	no	string
option 2	Provisioning URL for the OMM (ConfigURL). URL of an external server that provides configuration files for the Base Station(s) hosting the OMM.	no	String
option 10	ommip1: Used to select the IP-RFP that hosts the Open Mobility Manager (OMM).	yes	4ip_address/ 4 byte
option 14	syslogip: IP address of a Syslog Daemon	no	ip_address/ 4 byte
option 15	syslogport: Port of a Syslog Daemon	no	integer 16
option 19	ommip2: Used to select a secondary IP-RFP that hosts the standby Open Mobility Manager (OMM). This option must be included if the OMM Standby feature is used (see section 7.14).	no	ip_address/ 4 byte
option 226	Enable 802.1x feature (set to 1).	no	integer 8

Note: Option 10 is not mandatory if the OMM functionality was selected by button

Example

An example of the minimal contents for the Option 43 parameter value would be:

0a 04 C0 A8 00 01 where “C0 A8 00 01” represents “192.168.0.1” for the OMM IP.

The option 43 contains a string of codes in hex the format is “option number” “length” “value” in this example

0a = option 10 (ommip1)

04 = following value is 4 blocks long

C0 A8 00 01 = 192.168.0.1

If there is more than one option, add the next option at the end of the previous one. Depending of the DHCP server you must end the option 43 with FF.

9.5.3.2 **Selecting the Right DHCP Server**

The DHCP client indicates its own IP address using option 50 to the DHCP server. The DHCP client will select the DHCP server that offers the currently used IP address. Additionally the mandatory options must be offered otherwise the DHCP offer is ignored by the DHCP client.

If no matching offer was received, the DHCP client resends the discover message 2 times with a timeout interval of 1 second. Then the DHCP client will wait for 1 minute before resending 3 requests again.

If no DHCP offer containing the mandatory options is received as answer to the first 3 discover messages, the RFP accepts any server offer even if the mandatory options are missing.

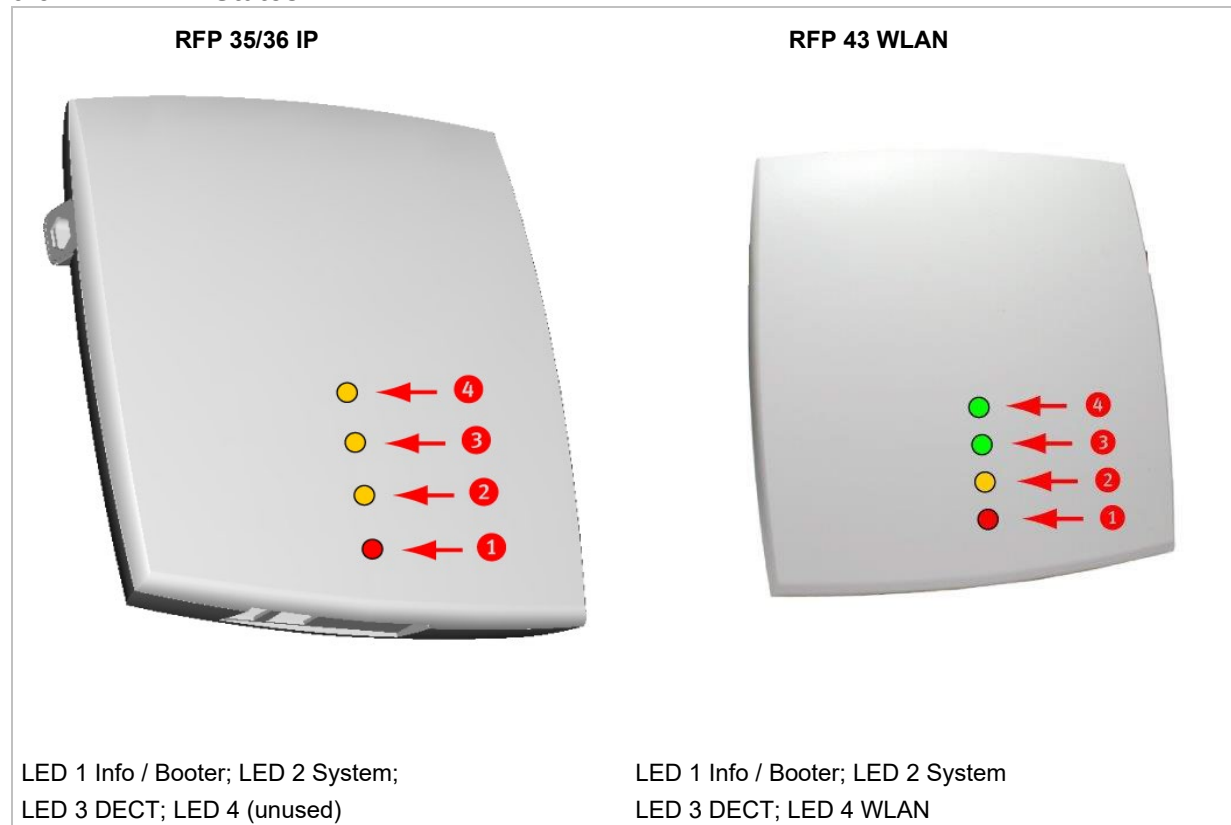
If the DHCP client cannot accept a DHCP offer within 20 minutes, the RFP is rebooted.

9.5.4 RFP LEDS

9.5.4.1 3rd Generation RFPs

- RFP 35 IP
- RFP 36 IP
- RFP 37 IP
- RFP 43 WLAN

9.5.4.1.1 LED States



9.5.4.1.2 Booter LED Status

RFP 35/36 IP, RFP 43 WLAN

The RFP 35/36 IP and RFP 43 WLAN booter uses LED1 for signaling its activity. After power up, the LED 1 (INFO) is red. The successful start of the boot image is signaled by the LED 1 turning orange.

9.5.4.1.3 Application LED Status

The following tables illustrate the different meaning of the LEDs while the application is starting or active.

RFP 35/36 IP, RFP 43 WLAN

	LED1 (INFO)		LED2 (OMM / SYSTEM)		LED3 (DECT)		LED4 (WLAN)		
Kernel	cont.								kernel boot phase (inflator, ...)
RFPM	1s	1s							DHCP phase
	1,85s	0,5s							DHCP failure (idle loop)
	0,5s	0,5s							obtaining external configuration
	0,85s	0,15s							external configuration failure
	cont.								Ready
	1,85s	0,15s							Up & running + RFP houses OMM
RFP general			1s	1s					OMM connect phase
			1,85s	0,15s					OMM connection failure (idle loop)
			cont.						Up & running (OMM connected)
			1,85s	0,15s					Up & running + OMM warning
			1,85s	0,15s					Up & running + OMM failure
RFP DECT					cont.				DECT not configured on this RFP
					1,85s	0,15s			DECT inactive (not synced yet)
					cont.				DECT 'on air'
					1,85s	0,15s			DECT + call active
					1,85s	0,15s			DECT + call active + busy bit
RFP WLAN							cont.		WLAN not configured on this RFP
							1,85s	0,15s	WLAN inactive yet
							cont.		WLAN 'on air'

	LED1 (INFO)		LED2 (OMM / SYSTEM)		LED3 (DECT)		LED4 (WLAN)		
							1,85s	0,15s	WLAN + assoc. clients
							cont.		WLAN failure (for example, 10 Mbit/s uplink)
Reboot request	cont.		cont.		cont.		cont.		RFP will reboot

9.5.4.2 4th Generation RFPs

- RFP 44
- RFP 45
- RFP 47 and RFP 47 DRC (Indoor and Outdoor Unit)
- RFP 48 WLAN

See the section [1.2.1.1](#) for more information.

9.5.4.2.1 LED States

The following tables show the LED status of an RFP according to the different states.

A red respectively orange colored field in the table means that the LED glows permanently in red or orange. A split field with for example, the specification 1s/1s means that the LED is flashing with a frequency of one second LED red on and one second LED off. Grey means that the LED is off.

The new RFP family is equipped with one colored LED, which shows the individual states of the 4th generation RFP.

LED color/rhythm		Description
continuous		Booter phase
continuous		Kernel boot phase
1s	1s	Configuration phase
1,9s	0,1s	DHCP failure (idle loop)
continuous		System up and Running (with or without OMM)
1s	1s	OMM connection phase
continuous		OMM connected
1s	1s	DECT inactive (not synced yet)
continuous		DECT "on air"
continuous		WLAN "on air"
1s	1s	DECT inactive (not synced yet) + WLAN "on air"
continuous		DECT + WLAN "on air"
0,1 sec	0,1 sec	Button pressed : 1 sec < t < 3 sec = no action
0,1 sec	0,1 sec	Button pressed : 3 sec < t < 7 sec = Activate Cloud-Id
0,1 sec	0,1 sec	Button pressed : 7 sec < t < 9 sec = no action
0,1 sec	0,1 sec	Button pressed : 9 sec < t < 13 sec = Activate OMM in SIP-DECT Standard Mode
0,1 sec	0,1 sec	Button pressed : 13 sec < t < 15 sec = no action
0,1 sec	0,1 sec	Button pressed : 15 sec < t < 19 sec = Re-enable OMM Web Service and AXI Service
0,1 sec	0,1 sec	Button pressed : 19 sec < t < 21 sec = no action
0,1 sec	0,1 sec	Button pressed : 21 sec < t < 25 sec = Factory Reset
0,1 sec	0,1 sec	Button pressed : 25 sec < t < oo sec = no action

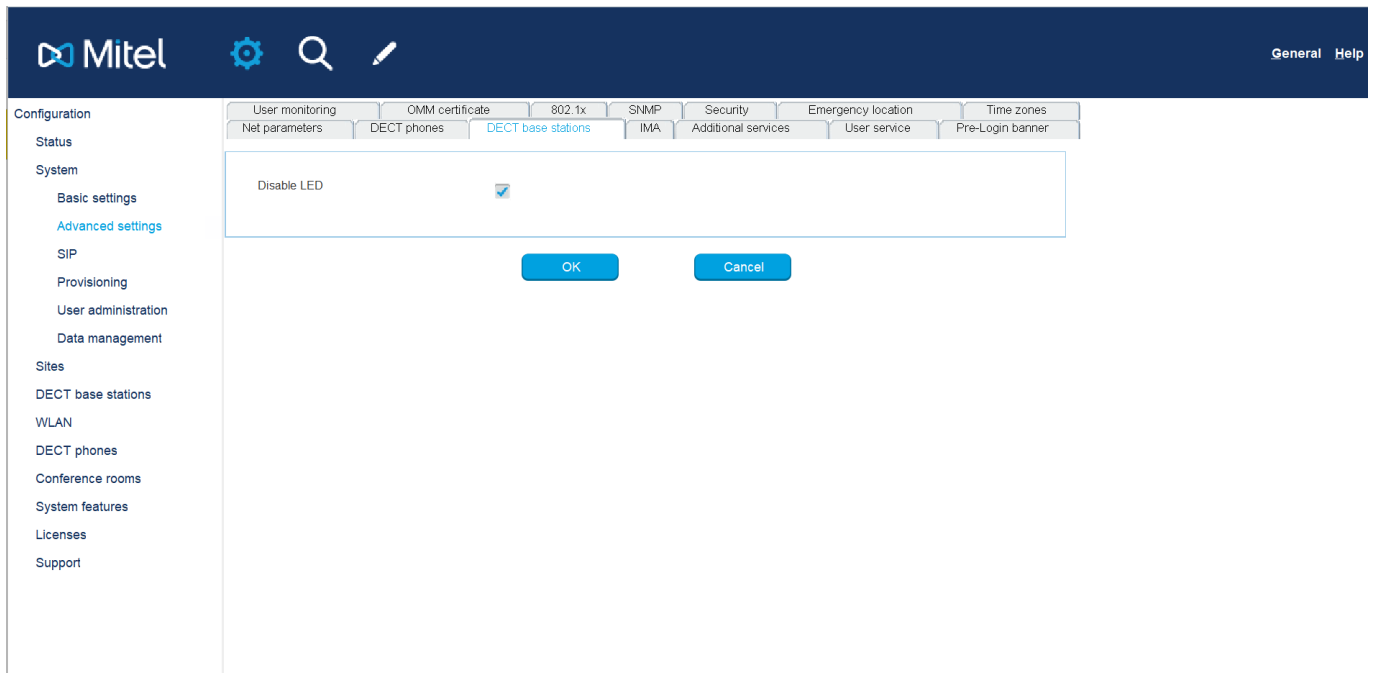
During the RFP4G startup, the LED flashing on the RFP4G indicates the active connection and the busy condition as follows:

- If at least one DECT connection is active, the LED flashes yellow every 2 seconds for 100 ms.
- If all DECT air resources are busy (no free resources), the LED flashes red every 2 seconds for 100 ms.

9.5.4.2.2 Turning Off the RFP 4G LED

To turn off the RFP 4G LED,

1. Go to the **DECT base stations** tab.
2. Select the **Advanced settings** option and select the **Disabled LED** check box to disable the LED for the active DECT and WLAN states.



9.6 SIP-DECT OMM SETUP USING THE CONFIGURATION BUTTON

Perform the following steps to set up a SIP-DECT OMM on an RFP4G using the configuration button:

1. Plug-in an Ethernet cable into the RFP and power it on (PoE is required).
2. Using a hex wrench, ballpoint pen, or a similar object, press the configuration button to make the RFP the OMM RFP. The LED starts flashing green to indicate that the button is pressed.



3. Release the button when the LED begins flashing yellow (which happens after the button is pressed for 10 to 15 seconds) to activate the OMM in standard SIP-DECT mode.



The RFP performs a reset to factory defaults and reboots. After the reboot, the OMM is started in the SIP-DECT standard mode.

Note: If the button is pressed for so long that the LED flashes green again, it means that the button press action has been canceled.

4. Assign an IP address for the RFP or OMM and connect to the OMM Web service after the OMM startup is complete, which is indicated by the LED changing from yellow to white.

Note: If the IP address assignment fails, use the java script *Find my SIP-DECT base station* to assign an IP address to the OMM. For more information, see [9.6.1](#).

5. Log in to the OMM Web service and configure the OMM. For details about configuring the OMM, see Base Station Startup Configuration.

The following table describes the RFP's configuration button functions and the corresponding LED indications.

LED Color/Rhythm		Description
0,1 sec	0,1 sec	Button pressed: 0 sec < t < 3 sec = no action
0,1 sec	0,1 sec	Button pressed: 3 sec < t < 8 sec = Activate the Cloud-ID mode
0,1 sec	0,1 sec	Button pressed: 8 sec < t < 10 sec = no action
0,1 sec	0,1 sec	

		Button pressed: 10 sec < t < 15 sec = Activate the OMM in SIP-DECT standard mode
0,1 sec	0,1 sec	Button pressed: 15 sec < t < 17 sec = no action
0,1 sec	0,1 sec	Button pressed: 17 sec < t < 22 sec = Reset to factory defaults
0,1 sec	0,1 sec	Button pressed: 22 sec < t < ∞ sec = no action

9.6.1 FIND MY SIP-DECT BASE STATION

Perform the follownig steps to determine the IP address of the OMM using the *Find my SIP-DECT base station* java script 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.

1. Download the java script (FindMySIP-DECTbasestation.zip) from Mitel Software Download Center.
2. Extract the compressed folder.
3. Open the index.html file in the extracted folder.
The **Find my SIP-DECT base station** webpage opens from your local drive.
4. The search IP range is initialized automatically. You can adjust the IP address range if needed.

File:///C:/Users//Documents/Find my SIP-DECT base station/Find my SIP-DECT base station.htm

Mitel | Find my SIP-DECT base station

My IP address 10 . 103 . 35 . 133

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

5. Click the search button and wait until the RFPs are searched.
The results get listed with the base station MAC address, IP address and optionally the RFP generation and configuration state.

6. Click the **Open** button beside the IP address of the RFP that is designated as OMM RFP. The configuration web GUI of the OMM running on the base station or the base station that is assigned as OMM opens.

7. Log in to the OMM web service.
The default login username and password is omm.

Note: A reset to factory defaults removes the configuration set using the RFP's configuration button. Execute a reset to factory defaults before the RFP is used with another OMM or another way of configuration can be used. For example, local static configuration using OM Configurator.

9.6.2 ADD RFPs TO THE INSTALLATION

The RFPs do not receive the IP address of the OMM as a configuration parameter, but they must automatically detect the OMM in the network.

The RFPs perform the following task to determine the IP address of the OMM:

- The RFPs send broadcast messages into the network to trigger the OMM to respond.
Note: As the broadcast messages are not routed, this mechanism is limited to the network segment the OMM is in.
- The OMM responds if the capturing of unconfigured DECT base stations is allowed.
- The RFPs are listed in the **Base Stations > Capturing unconfigured DECT Base Station** page of the OMM web service.
The 3rd generation RFPs are also supported.

Mitel | SIP-DECT 8.3 Advanced DE EN ES FR Logout

Status [Base Stations](#)

System New Sorted by Sites

Sites

[Base Stations](#) Capturing unconfigured DECT base stations Capture allowed: ✗

SIP Users/Devices Start

WLAN

System Features

Licenses

Info

Support

2 Base Stations

Site 1: 2 Base Stations

ID	Name	MAC address	IP address	HW type	Version	DECT Cluster	WLAN profile	Connected
0000	OMM RFP 1	08:00:0F:C3:DE:FD	10.103.35.150	RFP 47	SIP-DECT 8.3SP1-GI15	1	-	✓
0001	RFP 43	00:30:42:17:8E:3E	10.103.35.172	RFP 43	SIP-DECT 8.3SP1-GI15	1	-	✓

- Wait until the new RFPs appears in the unconfigured base station list.
The search can extend more than a minute depending on timing and status of RFP and OMM.
- Click the  icon to edit the RFP configuration (such as, activate DECT, set a proper name and so on) and add the RFP to the database.
The RFP then appears in the list of configured RFPs.

New base station

General settings

MAC address

Name

Site

☒ **DECT settings**

DECT Cluster

Preferred synchronization source ☐

Reflective environment ☐

☐ **WLAN settings**

WLAN profile

802.11 channel

Output power level

OK Cancel

- After the RFP is added to the OMM's configuration, the RFP can fetch a software update from the OMM RFP.

Mitel | SIP-DECT 8.3 Advanced DE EN ES FR Logout

Status [Base Stations](#)

System New Sorted by DECT clusters

Sites

[Base Stations](#) Capturing unconfigured DECT base stations Capture allowed: ✗

DECT Cluster 1 Start

SIP Users/Devices

WLAN

System Features

Licenses

Info

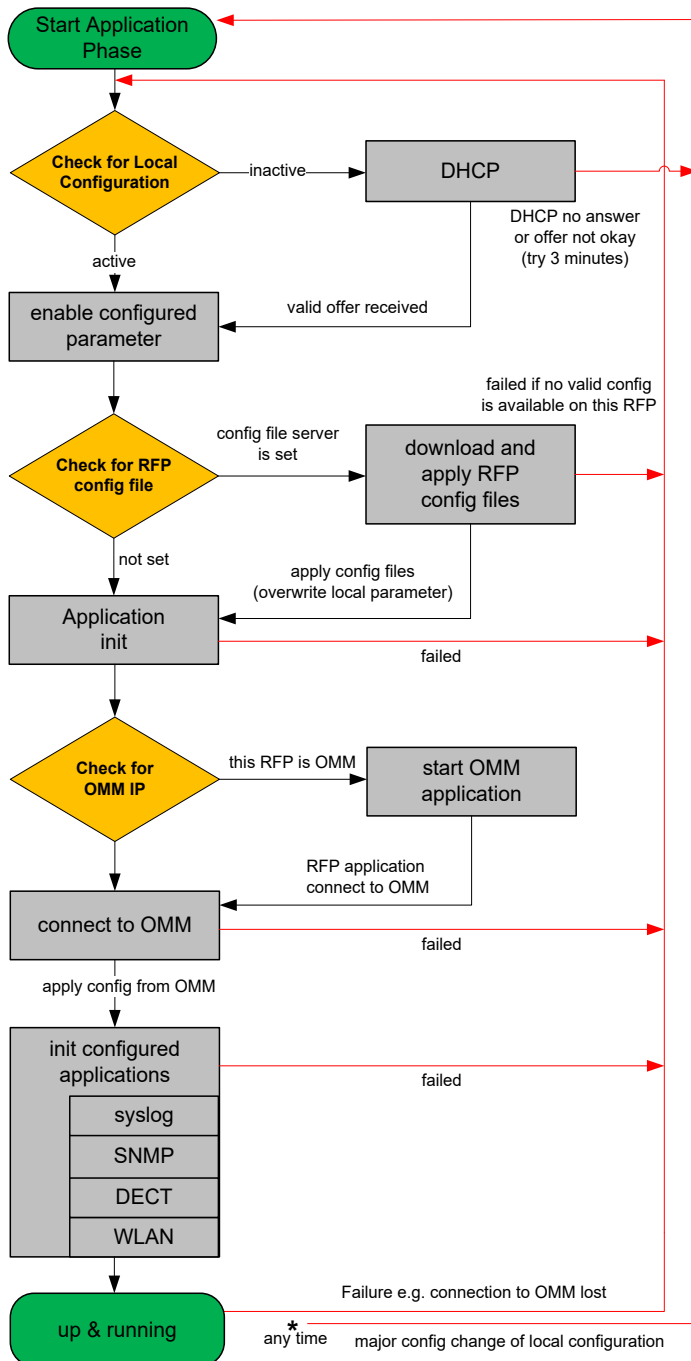
2 Base Stations

DECT Cluster 1: 2 Base Stations

ID	Name	MAC address	IP address	HW type	Site	RPN	Reflective environment	Connected	Active
0000	OMM RFP 1	08:00:0F:C3:DE:FD	10.103.35.150	RFP 47	1	00	✗	✓	✓
0001	RFP 43	00:30:42:17:8E:3E	10.103.35.172	RFP 43	1	01	✗	✓	✓

9.7 STATE GRAPH OF THE START-UP PHASES

The 3rd and 4th generation RFPs use a similar start-up sequence, but they start with the application phase (see below).



9.8 OMM CONFIGURATION AND RESOURCE FILES

The OMM supports certain configuration files containing commands in AXI style, to support auto-configuration of small and simple installations in provider environments. It is assumed that the configuration files are automatically generated in a standardized way, to prevent configuration failures. The following list summarizes all of the configuration and resource files related to the provisioning of a SIP-DECT system:

- ipdetect.cfg / <MAC>.cfg / <PARK>.cfg

These files contain configuration parameters and are used to configure the OMM automatically. There is one common file “ipdetect.cfg” for all RFPs and one file “<MAC>.cfg” for every single IP-RFP. The RFP specific <MAC>.cfg is requested if indicated in the common “ipdetect.cfg” file. It is possible that all RFPs request “ipdetect.cfg” and only selected RFPs request the <MAC>.cfg (for specific configuration on some RFPs).

- usr_common.cfg / <user>.cfg

These files are related to the “External User Data Provisioning” feature, whereby <user> refers to <Number/SIP user name> or <LoginID>.

<user>.cfg can also refer to user.cfg, a common file name for all users. This concept allows a provisioning server to provide user-specific settings on demand using one file name based on the specific user credentials.

- ima.cfg

This file includes the configuration for Integrated Messaging & Alerting Application, and can be loaded permanently.

- iprpf3G.dnld

This file includes the software image for RFP 35/36/37 IP / RFP 43 WLAN. This file also includes the software images for the Mitel 600/700 DECT phone family. RFPs can load their software image directly from the RFP OMM.

- iprpf4G.dnld

This file includes the software image for RFP 44/45 IP and RFP 48 WLAN. This file also includes the software images for the Mitel 600/700 DECT phone family. RFPs can load their software image directly from the RFP OMM.

- license.xml

This file includes the license for a specific SIP-DECT system.

- customer_image.png

This resource file can include a customer logo displayed to display on the OMM Web service.

With SIP-DECT 6.0 or later, all of these files can be loaded from the same external file server, if configured (see the below **CONFIGURATION FILE URL** section).

9.8.1 CONFIGURATION FILE URL

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 configuration file server URL (ConfigURL) can be configured in the OMM (**System -> Provisioning -> General Tab Provisioning URL Section/Section**), via DHCP or the Redirection and Configuration Service (RCS).

Note: If the external file server requires credentials for authentication, the credentials must be configured using the DECT phone or the Web service.

The following files are automatically requested if a provisioning server is set:

- Configuration files supporting startup parameters and OM AXI code for the OMM configuration
 - ipdect.cfg
 - <mac>.cfg (note that if a standby OMM is set, two MACs are present)
 - <PARK>.cfg (PARK in MAC address format: for example, 001F11234001)
 - User configuration files (for user login on DECT phone)
 - user_common.cfg
 - <user.cfg>
 - user.cfg
- Integrated Messaging and Alerting Service (IMA) (for alarm scenarios, email accounts, RSS feeds) - ima.cfg
- OMM license file - license.xml
- Logo for OM Web-Portal (Branding) - customer_image.png

You can also configure individual URLs for most configuration files. If present, the individual URL is used for the configured feature.

At startup, the OMM tries to retrieve the configuration file URL (ConfigURL) from the following sources, in the order listed. The OMM uses the first URL it finds to load the configuration and resource files.

The URL can be set through the following methods (in order of priority):

- 1 OMM database (for example, **System > Provisioning > General Tab Provisioning URL Section/section** in either OMM Web service or OMP)
- 2 DHCP option 66 (SIP-DECT 6.2 or higher)
- 3 DHCP vendor specific option 43 – sub-option 2
- 4 DHCP option 234
- 5 Redirection and Configuration Service (RCS) – on initial setup only

Once a URL is set, it is stored in the OMM database. The URL can be overwritten at a later time for example, during provisioning after authentication.

Note: The ConfigURL only applies to the RFP OMM, which must be running SIP-DECT 6.0 or higher. Other DECT base stations only apply the ipdect.cfg and <mac>.cfg files without OM AXI.

9.8.1.1 Syntax

The ConfigURL has the following syntax:

<protocol>://<user>:<password>@<server>/<path>?<parameter>&<parameter>

- Supported protocols: ftp,ftps,tftp,sftp,http,https
- Credentials should be secured by transport protocol or digest authentication.

The ConfigURL supports additional parameters to modify the certificate validation behavior for the configuration file server:

- **cm:** <https client method > - TLS1.2 or AUTO (AUTO= all)
- **vc:** <validate certificates> - valid settings are: 0 or 1
The OMM includes a list of trusted CA's (Mozilla CA certificate list)
- **ve:** <validate expires> - validation of certificate expiry: 0 or 1
- **vh:** <validate hostname> - validation of hostnames: 0 or 1
- **uc:** allow un-configured trusted certificates> - allow untrusted certs: 0 or 1
If set to 1, validation is disabled as long as no trusted certificate was imported.
- **ic:** <import certificate> - import server certificate as trusted: 0 or 1
If ic=1 + uc=1, the trusted certificate will be imported without any validation, as long as no trusted certificate was imported previously.

You can view and change the ConfigURL via the OMM Web service (see section [6.4.2](#)) or the OMP (see section [7.7.5](#)).

9.8.2 SPECIFIC CONFIGURATION URLS

In addition to the common ConfigURL, you can configure specific URLs for individual configuration and resource files in the OMM database. As soon as a specific URL is set, the OMM uses that URL to load the appropriate configuration/resource file during startup.

Note that the user_common.cfg file is loaded from the ConfigURL and the specific URL when both URLs are set.

Configuration / Resource File	Location of Specific URL	
	OMM Web Service	OMP
user_common.cfg / <user>.cfg	N/A	System > Data management > User data import See section 7.7.6.7
ima.cfg	System > System settings > OM Integrated Messaging & Alerting service See section 6.4.1.9 .	System > Advanced settings > IMA See section 7.7.2.4 .
iprfp3G.dnld	System > Provisioning and Software Update > Software update URL section/section See section 6.4.1.11 .	System > Provisioning > Software Update URL See section 7.7.6.8
lprfp4G.dnld	System > Provisioning and Software Update > Software update URL section/section See section 6.4.1.11 .	System > Provisioning > Software Update URL See section 7.7.6.8 .
600.dnld 700.dnld	Support > DECT phone's firmware update See section 6.4.1.7 .	Support > DECT phone's firmware update See section 7.15.1
customer_image.png	N/A	System > Provisioning > Branding Image URL See section 7.7.6.10
iprfp2G.tftp		

9.8.3 RELOAD OF CONFIGURATION AND RESOURCE FILES

The OMM automatically tries to load all configuration and resource files (ipdect.cfg, <MAC>.cfg, PARK.cfg, ima.cfg, user_common.cfg, update check for iprpf3G.dnld and iprpf4G.dnld, and so on) from the retrieved ConfigURL or specific URL (if present in the OMM database) at startup.

Note: The <user>.cfg and user.cfg files are only loaded on demand. They are not loaded automatically.

In addition, the OMM supports several mechanisms for updating the configuration by triggering a reload of the configuration and resource files:

- DHCP lease time

If the OMM is running on a RFP and DHCP is used, all configuration and resource files are reloaded when half of the DHCP lease time has elapsed.

- Daily automatic reload of configuration and firmware files

You can enable this option and specify a specific time of day to reload configuration files via the OMM Web service or the OMP (System -> Provisioning -> Daily automatic reload of configuration and firmware files).

- Manual reload via **Update** button

You can trigger a manual reload of all configuration and resource files by clicking the **Update** button in the OMM Web service (**System -> Provisioning and software update -> System update section/section**) or OMP (**System -> Provisioning -> System Update**).

- 600/700 DECT phone **Administration** menu
 - When a user with a 600/700 DECT Phone selects the **Sync system data** option in the **Administration** menu, the OMM reloads all configuration and resource files.
 - When a user with a 600/700 DECT Phone selects the **Sync user data** option in the **Administration** menu, the OMM reloads the <user>.cfg file for that user.
- SIP Notify message
 - When the OMM receives a SIP Notify message with the “**check-sync**” event for a user, the OMM reloads the configuration file <user>.cfg for that user.
 - When the OMM receives a SIP Notify message with the “**prov-sync**” or “**resync**” event for any user, the OMM reloads all configuration and resource files. The SIP Notify with “prov-sync” or “resync” can be also addressed to the OMM (without the user portion in the request URI).

9.8.4 AXI COMMANDS IN CONFIGURATION FILES

With SIP-DECT 6.0 or later, the OMM supports configuration files containing commands in AXI style, for OMM configuration.

The OMM attempts to load the following files from the Configuration File URL, and processes them in this order:

- 1 ipdect.cfg
- 2 <MAC>.cfg (RFP OMM only)

3 <PARK>.cfg (PARK in MAC address format: for example, PARK: 1F11234001; MAC address format 001F11234001)

Note that the actual file name of the <MAC>.cfg depends on MAC address of the RFP where the OMM is running.

The active OMM and the standby OMM request different files, even if they belong to one system. To ensure that both OMMs can retrieve the same file independent of which one is active, each OMM requests the <PARK>.cfg. The PARK identifies a SIP-DECT system in a unique way.

None of the files are mandatory and they can be empty. The AXI commands can be all in one file or split up as needed.

Example configuration file

The following example shows how to include AXI commands in a configuration file.

```
### SIP-DECT OMM Config example - pls. be aware that some commands cannot be applied to
SIP-DECT with Cloud-ID for example, request PARK from server, set regulatory domain etc.
and some commands depend on the actual use case/setup

### Confirm EULA
<SetEULAConfirm confirm="1" />

### Set full access account
<SetAccount plainText="1" > <account id="1" password="Sip!12" active="1" aging="none" />
</SetAccount>

### Set root account
<SetAccount plainText="1" > <account id="2" password="Sip!12" active="1" aging="none" />
</SetAccount>

### Set system name
<SetSystemName name="6.1 NB" />

### Tone scheme
<SetSysToneScheme toneScheme="DE" />

### Enable SSH ###
<SetRemoteAccess enable="1" />

### Request a valid PARK from a Server ####
<PARKFromServer />

### Set DECT Regulatory Domain ###
<SetDECTRegDomain regDomain="EMEA" />

### Set WLAN Domain/contry ###
<SetWLANRegDomain regDomain="DE" />

### Enable Auto-create on subscription ####
<SetDevAutoCreate enable="1" />

### Set DECT AC ####
<SetDECTAuthCode ac="35239" />

### Set specific user data URL ####
<SetUserDataServer plainText="1" useCommonFileNameOnServer="1" ><url enable="1"
protocol="HTTPS" host="www.domain.de" path="/lpueschel/test/" username="lpueschel"
password="lpueschel" validateCerts="0" /></SetUserDataServer>

### Set SIP Proxy and Registrar ###
<SetBasicSIP transportProt="UDP" proxyServer="172.30.206.9" proxyPort="5060"
regServer="172.30.206.9" regPort="5060" regPeriod="3600" />
```

```

### use addId="" for Login at DECT DECT phone ###
<SetDECT phoneLoginVariant login="ID" />
#### Set Portrange 17000 - 32767 ####
<SetPortRangeSIP ><userUdpTcp startPort="17000" endPort="17511" /><userTls
startPort="18000" endPort="18511" /></SetPortRangeSIP>
#### Set SOS/ManDown emergency number ####
<SetAlarmTrigger><trigger id="0" triggerId="SOS" fac="SOS" comment="" num="110"
/></SetAlarmTrigger>
<SetAlarmTrigger><trigger id="1" triggerId="MANDOWN" fac="MANDOWN" comment="" num="112"
/></SetAlarmTrigger>
### Set common voice mail number ###
<SetSysVoiceboxNum voiceboxNum="6333" />

```

WARNING: Configuration files must be automatically generated in a standardized way to avoid configuration failures. Configuration failures could cause a SIP-DECT system outage.

Note that this configuration file approach has limitations. For example:

- Insufficient for managing data objects that are dynamically created and addressed by an index (for example, RFPs)
- No administrator feedback for commands that cannot be processed (for example, unknown commands, invalid parameter, conflicts which other configuration settings)

9.8.4.1 User Data in Configuration Files

Configuration files are generally insufficient for managing data objects that are dynamically created and addressed by an index. Therefore, it is necessary to configure user data also. This allows providers to manage the user data (to a limited extent) without using the <user>.cfg files.

The <user>.cfg concept supports the complete range of user-related SIP-DECT functions, including a user-specific DECT phone configuration. The user data in configuration files as described here supports only a limited set of parameters.

To allow user data in configuration files, the following rules must be applied:

- 1 Initialize all possible data sets with default values Number/SIP user name is automatically set to uid<X> (e.g., uid1):

```

<CreatePPUser plainText=1 replaceData=1><user uid="1" name="" num="" addId=""
sipAuthId="" sipPw="" pin="" fixedSipPort="0" /> </CreatePPUser>
...
<CreatePPUser plainText=1 replaceData=1><user uid="512" name="" num="" addId=""
sipAuthId="" sipPw="" pin="" fixedSipPort="0" /> </CreatePPUser>

```

- 2 To “add” a user, set appropriate data:

```

<CreatePPUser plainText=1 replaceData=1><user uid="1" name="Account004 Mitel"
num="040226332195" addId="195" sipAuthId="040226332195" sipPw="broadnet.01" pin="195"
fixedSipPort="0" /> </CreatePPUser>

```

- 3 To “remove” a user, set to default data:

```

<CreatePPUser plainText=1 replaceData=1><user uid="1" name="" num="" addId=""
sipAuthId="" sipPw="" pin="" fixedSipPort="0" /></CreatePPUser>

```

This supports the use of templates such as the following:

```
<CreatePPUser plainText=1 replaceData=1><user uid="1" name="%BWNAME-1%" num="%BWLINEPORT-1%" addId="%BWEXTENSION-1%" sipAuthId="%BWAUTHUSER-1%" sipPw="%BWAUTHPASSWORD-1%" pin="%BWEXTENSION-1%" fixedSipPort="0" /></CreatePPUser>
```

9.8.5 USER CONFIGURATION FILES

The user configuration files (user_common.cfg and <user>.cfg) enable the “External User Data Provisioning” feature, which allows customers to import user data from a provisioning server. See the *SIP-DECT OM DECT Handset Sharing & Provisioning Installation & Administration User Guide* for a full description of that feature.

In addition <user>.cfg can also refer to user.cfg, a common file name for all users.

SIP-DECT 6.0 introduced the *UDS_CommonUserFileName* configuration attribute. When enabled, the OMM tries to fetch the same user.cfg file from the provisioning server for each user executing the login procedure, such that the login credentials of each user are used to access the provisioning server. This means that the provisioning server executes user authentication and provides a user-specific user.cfg when the user is authorized.

The *UDS_CommonUserFileName* attribute is enabled/disabled via the user_common.cfg file.

Please note: The common user file name feature is only applicable in combination with the file transfer protocols FTP, FTPS, HTTP, HTTPS or SFTP, which may require user/password credentials. Changing this attribute might cause login/logout problems for the users, because of changed authentication. It is up to the administrator to force user logouts (delete users) optionally. In any case, the administrator must publish new authentication data to users for their logins and logouts. This value is stored in the OMM database. So, the setting is stored over system restart and has no default value when not explicitly set in the user_common.cfg file.

Note that the *OM_UniqueId=NUMBER/UID* variable in the user_common.cfg file is no longer supported.

The following table summarizes the combinations of provisioning server access and type of user validation supported:

Provisioning Server access	Requested files	User validation	Supported DECT phones
- User data import URL - User data import credentials - No certificate validation	<number SIP user name>.cfg <loginID>.cfg	OMM authenticates user against PIN from .cfg files	- GAP - Mitel 142d - Mitel 600/700

- User data import URL - User data import credentials - System Provisioning Certificate validation	<number SIP user name>.cfg <loginID>.cfg	OMM authenticates user against PIN from .cfg files	- GAP - Mitel 142d - Mitel 600/700
- System Provisioning URL - System Provisioning credentials - System Provisioning Certificate validation	<number SIP user name>.cfg <loginID>.cfg	OMM authenticates user against PIN from .cfg files	- GAP - Mitel 142d - Mitel 600/700
- User data import URL - User credentials (UDS_CommonUserFile=NAME=YES) - No certificate validation	user.cfg	Provisioning server authenticates user at file request with user credentials	Mitel 600/700
- User data import URL - User credentials (UDS_CommonUserFile=NAME=YES) - System Provisioning Certificate validation	user.cfg	Provisioning server authenticates user at file request with user credentials	Mitel 600/700
- System provisioning URL - User credentials (UDS_CommonUserFile=NAME=YES) - System Provisioning Certificate validation	user.cfg	Provisioning server authenticates user at file request with user credentials	Mitel 600/700

9.8.6 DIGEST AUTHENTICATION AND CERTIFICATE VALIDATION

The OMM supports system credentials for provisioning to retrieve configuration and resource files from a server that requires user/password authentication.

System credentials are used to retrieve files from the external provisioning server defined by the configuration file URL, for protocols supporting authentication or servers requesting authentication. For HTTP/HTTPS, basic and digest authentication are supported.

You can set the system credentials via:

- OMM Web service **System -> Provisioning -> System credentials** page (see section [6.4.2.7](#))
- OMP **System -> Provisioning -> System credentials** tab (see section [7.7.5.5](#))

- Mitel 600/700 DECT phone user interface (through Feature Access Code or the Administration menu)

System credentials are also inherited if sources other than the configuration file URL are configured for specific configuration or resource files, without credentials. The system credentials are used only if requested by the file server.

9.8.6.1 System credentials via Mitel 600/700 DECT Phone user interface

A Mitel 600/700 DECT phone user can set, change or delete system credentials from the Mitel 600/700 DECT phone via:

- a configured feature access code (FAC)
- the **Administration** menu on the user interface

Note: The user must log in to OMM before being allowed to change valid credentials. If credentials are not set or are invalid (indicated by a health state), the OMM login is omitted.

Setting the credentials via feature access codes requires configuration of a FAC number through the **System Features -> Feature Access Codes** menu of the OMM web service (see section [6.9.4](#)) or the OMP (see section [7.13.2](#)).

When the user dials the configured feature access code, the user can select between the “Create/Change” and “Delete” options. The Administration menu additionally offers a health indication (ok or not ok). Depending on the health state, the user may be forced to login to the OMM first.

9.8.7 DECT BASE STATION SOFTWARE IMAGE FROM RFP OMM

To simplify the upgrade process for existing SIP-DECT installations in provider environments, SIP-DECT 6.0 and later provides support for a feature that allows RFPs to load their software image directly from the connected OMM.

If the RFP has no valid URL from which to load the software, they attempt to load the software from the connected OMM. If the OMM is running on a RFP, the RFP OMM delivers the software to the connected RFPs.

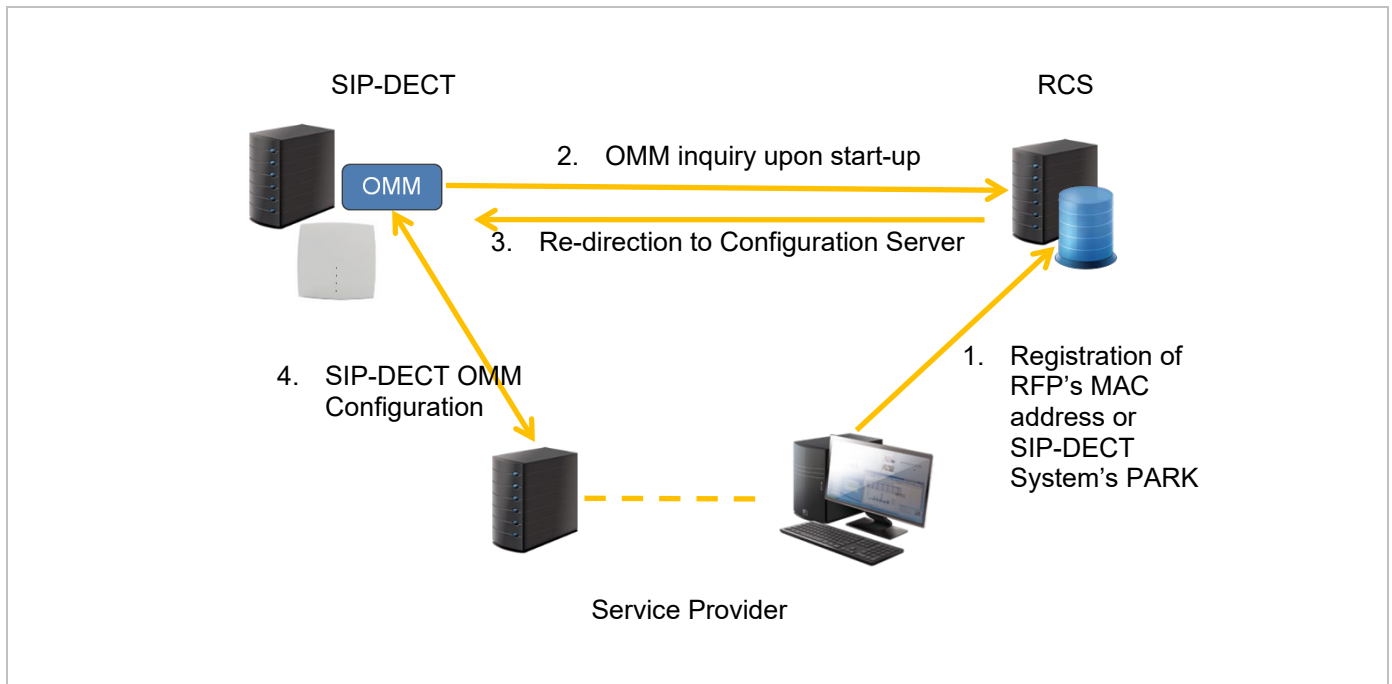
A new software image for the RFP OMM can be provided as a iprpf3G.dnld/iprpf4G.dnld file on an external file server. The software update URL can be configured via the OMM Web service (see section [6.4.1.11](#)) or OMP (see section [1.1.1.1](#)).

In SIP-DECT 8.0, OMM RFP4G provides SW images for RFP3G and RFP4G base stations. Because, the RFP3G is not able to hold the RFP4G SW image, an OMM RFP3G cannot provide the iprpf4G.dnld to an RFP4G.

9.8.8 REDIRECTION AND CONFIGURATION SERVICE (RCS)

The Redirection and Configuration Service (RCS) simplifies SIP DECT installation and management. When the MAC address or the PARK of a SIP-DECT OMM is entered in the RCS server, a SIP-DECT OMM is routed to its assigned server for configuration upon initial start-up.

If the OMM does not find a ConfigURL during initial setup, the OMM contacts the RCS to request a ConfigURL, using its RFP MAC address. If the RFP MAC Address is configured in the RCS, the RCS provides a ConfigURL that points to an external provisioning server. The OMM attempts to load all configuration and resource files from the ConfigURL received from RCS.



Note: The SIP-DECT OMM only uses the ConfigURL from RCS. Other information provided from RCS is not supported.

The OMM requests information from RCS only if no information has been retrieved from RCS prior to the request. The response is stored permanently in the OMM. To force a new RCS request, the OMM must be reset to default settings, through the **Discard OMM DB and configuration files** or **Reset OMM RFP(s) to factory defaults** on restart (see section [6.4.1.16](#)).

9.8.9 CUSTOMER LOGO ON OMM WEB SERVICE

SIP-DECT 6.0 and later supports the integration of a customer-specific logo on the OMM Web service interface. If a `customer_image.png` file is available on an external file server, customers can integrate their own logo into the OMM. This logo is displayed beside the Mitel logo on the top bar.

This image can be imported by:

- Configuration of a branding image URL to a file server using OMP (see section [7.7.2.8](#))
- Automatic search for a file named 'customer_image.png' on the provisioning server

The branding image is stored permanently in the OMM database, ensuring that the image is available even if a configured file server or provisioning server is not reachable. The file is deleted automatically from the server on a "file not found" response or by disabling the branding image URL configuration.

The picture should not be larger than 50 pixels high and 216 pixels wide.

9.9 DECT BASE STATION CONFIGURATION FILES

9.9.1.1 Third Generation DECT base Stations Configuration Files

IP-RFPs support two DECT base stations configuration files (downloaded from a server) to get configuration settings. There is one common file "ipdect.cfg" for all DECT base stations and one file specific file "<MAC>.cfg" for every IP-RFP. The DECT base station requests the "ipdect.cfg" file if a URL is provided. The RFP specific <MAC>.cfg is requested if this is indicated in the common "ipdect.cfg" file.

It is possible that all RFPs request “ipdetect.cfg” and only selected RFPs request the <MAC>.cfg to obtain a specific configuration on some RFPs.

9.9.1.2 Fourth Generation DECT Base Stations Configuration Files

The 4G RFP supports configuration files known as RFP or base station configurations files. Such files can contain the URL for the RFP SW update.

As of SIP-DECT 8.0, the new parameter OM_SwImageUrl4G is introduced to configure the SW update URL for 4G RFPs.

The SW update URL for 3G RFPs can be configured with the existing parameter OM_SwImageUrl or the new parameter OM_SwImageUrl3G. For example:

- # path to the software image
- OM_SwImageUrl=ftp://login:password@server/iprfp3G.dnld
- OM_SwImageUrl3G= ftp://login:password@server/iprfp3G.dnld
- OM_SwImageUrl4G= ftp://login:password@server/iprfp4G.dnld.

9.9.2 STANDARD IP SETTINGS

Standard IP settings (which are necessary for access to the RFP configuration files) are configured via DHCP (see section [9.5](#)) or OM Configurator (see section [9.8](#)). These are:

- IP address
- Net mask
- Gateway (i.e. router)
- Boot file name
- TFTP server
- Public option 224: “OpenMobility” or “OpenMobilitySIP-DECT” (to identify the relevant DHCP offer)
- Domain Name Server (optional)
- Domain Name (optional)
- URL to the RFP configuration files

All other parameters can be set by using an RFP configuration file even if standard DHCP options or OM Configurator parameters exist.

9.9.3 CONFIGURATION FILE SOURCE

A TFTP / FTP(S) / HTTP(S) URL specifies the protocol, server and path to access the RFP configuration files. The URL can include account data if appropriate.

Syntax:

```
{ftp|ftps|http|https}://[user:password@]server/[directory/]
```

or

```
tftp://server/[directory/]
```

The URL configuration is provided via DHCP option code 233 (prio1), or the OM Configurator.

- “ipdect.cfg” is mandatory if an URL is provided by DHCP or local static configuration via the OM Configurator.
- “<MAC>.cfg” is mandatory if it is indicated in the “ipdect.cfg” that a “<MAC>.cfg” exists for the DECT base station. (There is a key word to indicate that a “<MAC>.cfg” exists for every DECT base station.)

Mandatory means that if a file cannot be loaded, the DECT base station does not start. This is relevant for the following scenarios:

- RFP boot / startup (after power on, software update, etc)
- A change of the URL

9.9.4 PARAMETER SETTINGS PRIORITY

Some parameters can be set via DHCP / OM Configurator or by using the files “ipdect.cfg” or “<MAC>.cfg”. If a parameter is provided through more than one of the possible ways, the last setting has priority. There is the following order:

- DHCP / OM Configurator
- ipdect.cfg
- <MAC>.cfg

It is also possible to remove settings.

9.9.5 SOFTWARE UPDATE SETTINGS FOR 3RD GENERATION DECT BASE STATIONS

A configuration parameter specifies the location of the software that will be installed into the flash of an RFP 35/36/37 IP / RFP 43 WLAN and activated by the OpenMobility Manager.

`OM_SwImageUrl=ftp://172.30.207.21/openmobility/iprfp3G.dnld`

TFTP, FTP(S), HTTP(S) are supported for an RFP 35/36/37 IP / RFP 43 WLAN software update.

9.9.6 SOFTWARE UPDATE SETTINGS FOR 4TH GENERATION DECT BASE STATIONS

A configuration parameter specifies the location of the software that gets installed into the flash of an RFP 44/45/47 IP / RFP 48 WLAN and activated by the OpenMobility Manager.

`OM_SwImageUrl=ftp://172.30.207.21/openmobility/iprfp4G.dnld`

TFTP, FTP(S), HTTP(S) are supported for an RFP 44/45/47 IP / RFP 48 WLAN software update.

9.9.7 TIMES WHEN RFP CONFIGURATION TIMES ARE READ

The configuration files are read by the RFP application for example, during startup as shown in the following figure.

Configuration files are read by the RFP application at the following times:

9.9.8 RFP CONFIGURATION FILE UPDATE CHECK

RFP configuration file update check has the following characteristics:

If the configuration file(s) cannot be retrieved ...

- The RFP continues operation with the last successfully retrieved configuration file(s).
- The RFP will try to retrieve the configuration files again, starting with an interval of one minute and doubling this interval with each retry, not exceeding the update check interval (either default or configured).
- If the RFP is using DHCP, a renewal of the lease is scheduled so that possible changes in DHCP configuration will be detected.
- Failure to retrieve the configuration files is reported via Syslog.

9.9.9 HANDLING OF PARAMETER CHANGES

A change of a parameter (DHCP / OM Configurator, RFP configuration files) does not necessarily mean a change to the RFP's configuration because the parameter could be covered up or previously set using an alternative way.

Example 1:

IP address of a Syslog Daemon has been changed in "ipdetect.cfg" but is covered up by "<MAC>.cfg" in which this parameter has not been changed.

Example 2:

A parameter is new in "<MAC>.cfg" but has been set previously in "ipdetect.cfg" with the same parameter value.

Only if a parameter change causes a change in RFP configuration (as a sum of for example, DHCP / OM Configurator, "ipdetect.cfg" and "<MAC>.cfg" files) will the RFP perform a configuration update procedure.

Depending on the changed parameter, an RFP configuration update is done:

- On the fly without any service interruption for example, IP address of a Syslog Daemon has been changed.
- With an application restart for example, OMM IP address has been changed.

9.9.10 CONFIGURATION FILE SYNTAX

```
#####
# sample configuration file for the OpenMobility system
# retrieved via the net using file transfer protocols
# like tftp, ftp, http, https, ftps
#
#####
# comments start with the hash sign: "#"
#
#####
# BOOL variables support the following values
# YES Y 1 TRUE (case does not matter)
# NO N 0 FALSE (case does not matter)
# other values are interpreted as false
#
```

```
#####
# personal configuration files
#
# personal configuration files have the following name
# <OWN-MAC>.cfg, where <OWN-MAC>.cfg is of the form
# for example, 003042ABCDEF.cfg

# all RFPs will also load the <OWN-MAC>.cfg file
OM_PersonalConfigAll=1 # BOOL

# DO load the individual file for the RFP with mac 003042FFF0D0
# no matter what OM_PersonalConfigAll says
OM_PersonalConfig_003042FFF0D0=y

# DO NOT load the individual file for the RFP with mac 003042ABCDEF
# no matter what OM_PersonalConfigAll says
OM_PersonalConfig_003042ABCDEF=n # BOOL

# time interval for checking the remote cfg files in seconds
# minimum value is 300 (5 minutes)
# maximum value is 604800 (7 days)
OM_ConfigCheckInterval=500

#####
# OpenMobility system
#
# the OpenMobilityManager ip addresses
OM_ManagerIpAddress1=172.30.205.17
OM_ManagerIpAddress2=172.30.205.18

# path to the software image
OM_SwImageUrl=ftp://172.30.207.21/openmobility/sw/iprfp3G.dnld

#####
# SYSLOG
#
OM_SyslogIpAddress=172.30.207.20
OM_SyslogPort=10115

#####
# transfer core files to the following directory
#
OM_CoreFileSrvUrl=ftp://10.103.35.20/corefiles
```

9.10 CONSOLIDATED CERTIFICATE MANAGEMENT

SIP-DECT has various secured interfaces to support secure connections for file imports from local servers or provisioning servers. By default, the OMM Web server uses the hardcoded self-signed OMM certificate as local certificate for encrypted AXI connections, for provisioning (mutual authentication), and for SIP-over-TLS connections.

Certificate and authentication validation settings for these secure connections can be inherited from the configuration file URL (see section [9.8.1](#)).

9.10.1 SIP OVER TLS CERTIFICATES

SIP over TLS certificates are used for secure SIP connections. The hard coded self-signed OMM certificate is used by default, however you can import trusted certificates, a local certificate chain and a private key file (optionally password-protected) via:

- OMP (**System -> SIP -> Security** tab)
- OMM Web service (**System -> SIP -> Security**)
- A certificate server (usually running on a Mitel call server)

9.10.2 OMM CERTIFICATE (WEB SERVICE / AXI)

By default, the OMM Web server uses a hardcoded self-signed certificate for encrypted AXI connections. However, since self-signed certificates can trigger security warnings in browsers, it is recommended to replace them with a trusted certificate from an official Certificate Authority (CA).

You can overwrite the default OMM certificate by **importing a certificate chain and private key** (optionally password-protected) via the OMP (**System -> Advanced settings -> OMM Certificate** tab). You can also configure an OMM certificate server (**System -> Provisioning -> OMM Certificate Server**) to enable provisioning of OMM certificate files.

IMPORTANT : If you upload a certificate chain, ensure the order is correct to prevent activation. The correct order is ServerCert → Intermediate CA (interCA) → Root CA (RootCA)..

WARNING: Uploaded certificates do not activate immediately. A restart of the OMM is required for the changes to take effect.

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 trusting the CA root certificate.

9.10.3 PROVISIONING CERTIFICATES

Provisioning certificates are used for secure connections to configuration or firmware file servers with support for mutual authentication (i.e., for FTP, FTPS, and HTTPs protocols).

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. If no server certificate is available, you can disable the validation against trusted and CA certificates.

By default, the hard-coded self-signed OMM certificate is used for mutual authentication. You can overwrite the hard coded OMM certificate by importing trusted certificates, a local certificate chain and a private key file (optionally password-protected) via:

- OMM Web service System -> Provisioning -> Certificates page (see section [6.4.2.14](#))
- OMP System -> Provisioning -> Provisioning Certificates tab (see section [7.7.5.2](#))
- A provisioning certificate server through OMP System -> Provisioning -> Certificates server tab (see section [7.7.5.4](#))

The OMM provides the local certificate chain and the private key to servers requesting mutual authentication. The private key file may be password protected.

The system credentials can be inherited if specific sources for configuration and resource files are configured, where the 'Use provisioning security configuration' option is enabled.

9.10.4 CERTIFICATE VALIDATION

If the HTTPS or FTPS protocol is used to retrieve files from the configured provisioning server, the OMM validates the server certificates according to the certificate validation settings.

You can configure the certificate validation settings via OMP (**System -> Provisioning -> Provisioning – SSL settings**) or the OMM Web service (**System -> Provisioning -> Certificates**). Certificate validation settings can also be part of the ConfigURL provided by the RCS or via DHCP.

If you want to use the same validation settings for a specific URL (i.e., other than the configuration file URL), enable the "Use provisioning security configuration" parameter when configuring the URL (unless the "Import certificates with first connection" parameter is enabled).

9.11 3RD AND 4TH GENERATION RFP SOFTWARE UPDATE

The DECT base station checks several locations for a software update. If found, the software is copied to the flash memory, leaving the current software intact. After successful installation, the OMM is notified about the new software. Activation of the software is then managed by the active OMM. DECT base stations that do not have a connection to the OMM activate and start the software immediately.

Locations for software updates:

- Attached USB mass storage device with a software image iprpf3G.dnld in its root directory (Only 3rd generation RFPs). The USB mass storage device must be formatted using the vfat32 file system.
- If ipdetect.cfg supplies the OM_SwImageUrl variable, the URI is used to get the boot image. See section [9.9](#).
- TFTP server, path and file configured using the OM Configurator or via DHCP.

- OMM (SIP-DECT 6.0 or later): If the RFP has no valid URL from which to load the software, they attempt to load the software from the connected OMM. If the OMM is running on a DECT base station, the RFP OMM delivers the software to the connected base stations. See section [9.8.7](#) for more information.

9.12 802.1Q SUPPORT

The IP RFPs support VLANs according to IEEE 802.1Q. VLAN can be administered

- on a per port basis of the LAN switch assuming that the IP RFPs are connected to a single port of a switched Ethernet environment, or
- by assigning a VLAN ID to the IP RFP matching the VLAN they should operate in.

VLAN tagging has only to be set to IP RFPs' in the last case. The whole section refers to that case. With this, also 802.1p priority within Ethernet frames is enabled.

The scope of the following description is restricted to VLAN tagging and obtaining the VLAN ID. Quality of Service mechanisms like 802.1p priority and DiffServ are not described in this section.

VLAN implementation notes referring to IP RFPs:

- IP RFPs are not able to support VLAN ID 0 as described later in this section. Any other valid VLAN ID can be configured.
- If a VLAN ID is configured, all traffic from an IP RFP will be tagged with this VLAN ID.
- The VLAN ID configured for an IP RFP is also used for the OMM running on this IP RFP.
- Once a VLAN ID is set to the IP RFP, incoming frames are only accepted if they are tagged as well. Therefore the switch port must be configured as a tagged trunk for this VLAN.
- The VLAN configurations can be done using DHCP or the interface for the local static configuration, the OM Configurator.
- The use of VLAN does influence the boot up process of the IP RFP because the VLAN configuration takes place during the boot up phase.
- The default setting is not to tag the traffic. 802.1Q tagging is enabled if the VLAN ID is set. If no VLAN ID is set 802.1Q is disabled.

VLAN ID 0

VLAN ID 0 means that the IP RFP's traffic belongs to the port/native VLAN. The Ethernet switch port to which the IP RFP is connected must be configured to accept 802.1Q tagging for this to work and the switch must interpret VLAN ID 0 as the port/native VLAN ID per the IEEE 802.1Q standard.

The packets from the IP RFP are tagged with VLAN ID 0 and the packets sent to the IP RFP are tagged with the port/native VLAN ID. This scenario does not work, because the IP RFP supports only one VLAN ID in both directions. That means the VLAN ID in the receive direction must be the same as the send direction.

9.12.1 BOOT PHASE OF IP RFPs (DHCP)

Because the IP RFP does not know about VLAN at the beginning of the start up, two DHCP scopes are required. This applies regardless of the Ethernet switch being used. The following scenario with arbitrary VLAN IDs details the steps an IP RFP would go through in a typical dual-VLAN implementation.

Step A. DHCP scope within the native VLAN:

- 1 IP RFP boots up and obtains an address on the native VLAN.
- 2 The data VLAN DHCP option 132 directs the IP RFP to go to voice VLAN.

Step B. DHCP scope within the voice VLAN:

- 1 IP RFP releases the data VLAN address and obtains an address on the voice VLAN and all other parameters.

The voice VLAN does not have the DHCP option 132, because an IP RFP already on the voice VLAN does not need to be directed to go there.

- 2 IP RFP is operational on the voice VLAN.

If a reboot or power cycle occurs, the IP RFP returns to step A.

If an IP RFP cannot obtain an address on the voice VLAN, due to network or DHCP problems then the IP RFP falls back automatically to untagged frames (native VLAN).

To avoid the DHCP scope within the native VLAN the VLAN ID to be used can be set permanently via OMC without losing the ability to provide other parameter via DHCP, see section [9.7](#).

9.12.2 BOOT PHASE OF IP RFPs (LOCAL CONFIGURATION)

The PC running the OM Configurator must be a member of the native VLAN for the first configuration, later on within the voice VLAN set.

If a wrong or unknown VLAN ID is set, you can overwrite or read the configuration using no VLAN tag on the switch port in the first six seconds after the RFP is connected to a power supply / PoE. After six seconds the RFP applies the local configuration and starts using the parameters.

9.13 INSTALLING OMM IN HOST MODE

In this case, the OMM software must be installed on a PC running Red Hat Enterprise Linux 7 or CentOS 7. The network parameters with which the OMM works in this mode depend on this PC's network configuration.

Once started, OMM works permanently on the PC. In case of fatal error or PC restart, OMM will restart automatically.

Please note: Check that the versions of the OMM and RFP software on your SIP-DECT installation are the same.

9.13.1 SYSTEM REQUIREMENTS

The OMM application is a 32-bit/x86 application that can be installed on a 32-bit or 64-bit (recommended) operating system. The PC-based OMM requires the following configuration:

- Red Hat Enterprise Linux 7 or CentOS 7 operating system
- Server hardware minimum:
 - Processor : Dual Core Intel® Xeon® 3065, 2.33GHz, 4MB cache
 - Bus 1333 MHz
 - Memory : 4GB DDR2 SDRAM 667 MHz
 - Hard disk: 80 GB SATA 7200 rpm
 - 1 GBit/s Ethernet interface

9.13.2 INSTALLING THE OMM SOFTWARE

The OMM software for the Linux Redhat server is provided as a self-extracting executable file (for example, SIP-DECT_6.1.bin). This binary file contains two Red Hat packages:

- SIP-DECT-OMM-<SIP-DECT-version>.i586.rpm
OpenMobility Manager software.
- SIP-DECT-HANDSET-<DECT phone-version>.i586.rpm
Software for Mitel 600/700 DECT phones

The Mitel 600/700 DECT phone software can be updated via the Air interface, see section [9.21](#). A separate software package can also be provided for specific updates of the DECT phone software.

IMPORTANT : Log in as “root” to install and/or update OMM. If you do not login as root to open the OMM console, the path to ommconsole is not set. You must enter the whole path “/usr/sbin/ommconsole” to start the OMM console.

Command syntax

For extraction and automatic standard installation

sh SIP-DECT_<version>.bin

For extraction and automatic standard installation

sh SIP-DECT_<version>.bin -f

For extraction of RFP packages only

sh SIP-DECT_<version>.bin -x

RPM packages can also be installed manually.

For a first OMM type installation

rpm -i SIP-DECT-OMM-<version>.i586.rpm

For an OMM software update (see section [7.14](#))

rpm -U SIP-DECT-OMM-<version>.i586.rpm

For Mitel 600/700 DECT phone software installation

rpm -i SIP-DECT-HANDSET-<version>.i586.rpm

To delete a software release

**rpm -e SIP-DECT-HANDSET and
rpm -e SIP-DECT-OMM**

To check an installed release

rpm -qi SIP-DECT-OMM

or

rpm -qi SIP-DECT- HANDSET

After the installation phase, start OMM by running the command

“/etc/init.d/sip-dect-omm start”

9.13.3 CONFIGURING THE START PARAMETERS

The basic data for initializing OMM is stored in the file “/etc/sysconfig/SIP-DECT”. It can be edited to modify the OMM interface.

```
#####
# OMM configuration file
#####
# if you use a different interface for omm activate/correct parameter below
#OMM_IF="eth0"
#
OMM_CONFIG_FILE=/opt/SIP-DECT/tmp/omm_conf.txt
#
#if you use OMM resiliency for OMM activate parameter below with OMMs IP addresses
#OMM_RESILIENCY="192.168.0.1:192.168.0.2"
#
# Automatic OMM database import:
# TFTP / FTP / HTTP(S) URL specifies the import server and file
```

Parameters	Description
OMM_IF	Interface for communicating with the RFPs (by default: eth0)
OMM_CONFIG_FILE	File that contains the OMM configuration (by default: /opt/SIP-DECT/tmp/omm_conf.txt)
OMM_RESILIENCY	In case of OMM redundancy, enter the two IP addresses of the OMMs. See also section 7.14 .

9.13.4 SPECIFIC COMMANDS – TROUBLESHOOTING

The OMM software is installed but does not work automatically when the PC starts. The command below stops or starts OMM manually (User root):

`/etc/init.d/sip-dect [start|stop|restart].`

The command line interface for OMM is accessible via telnet on port 8107.

Malfunction

To check whether OMM is working, see the list of procedures for the “SIP-DECT” process. If OMM does not start, delete the lock file “/var/lock/subsys/SIP-DECT”.

To delete the OMM configuration remove the OMM configuration file “/opt/SIP-DECT/tmp/omm_conf.txt” (by default).

9.14 UPDATING THE OMM

The procedures for updating an existing DECT installation with new software depend on

- whether a single OMM or standby OMM installation is used
- whether the OMM is running on an RFP or PC

The OMM “standby” feature is described in section [9.15](#).

The update mechanism allows an update of the RFPs with minimum impact to DECT services, especially for installations with a standby OMM.

All RFPs check the availability of a new boot image file automatically when:

- the DHCP lease is refreshed,
- the RFP lost the connection to the OMM,
- one of the service applications running on the RFP must be restarted, and
- an RFP configuration file update check is done (see section [9.9.8](#)).

Please note: Make sure that all configured software sources point to the same software version, so that the OMM and all RFPs are running the same software version.

Please note: RFPs without a configured software image URL (via DHCP, OMC or ipdetect.cfg/<mac>.cfg) retrieve their software directly from the OMM. In this case, the RFP activates the software immediately. This feature is only available with 3G RFPs.

As soon as an RFP detects a new boot image file on the TFTP server (or the software download server using FTPS or HTTPS), it notifies the OMM. The OMM keeps track when it is safe to restart an RFP in order to leave the DECT service synchronized.

RFPs scheduled for restart are marked with a yellow sign within the Web service (see section [6.6.1](#)) or in a separate column within the OM Management Portal (OMP), see section [7.9.1.1](#).

Please note: Only software upgrades from the preceding two releases are tested for upgrade to the current release. Additional steps may be required to upgrade systems with software that is three or more releases behind the current release.

9.14.1 UPDATING A SINGLE OMM INSTALLATION

In the case of a single OMM installation, a DECT network outage during the update procedure is unavoidable.

Please note: Updating a single OMM installation results in a DECT network outage during the update procedure.

For the update, replace the boot image file on the TFTP server(s) with the new one.

OMM in RFP mode

If the OMM is running on an RFP, force the update of this RFP by pressing the **Update** button on the **Provisioning & Software Update** web page (see section [6.4.1.17](#)). The RFP checks the boot image file on the TFTP server and reboots if a new one is found.

OMM in host mode (on Linux server)

If the OMM is running on a dedicated Linux server, install the new software as described in section [9.13.2](#) on the PC with the command “**SIP-DECT_<version>.bin**”. This stops the running OMM automatically and installs the new software. After the installation phase, restart the OMM by executing the command “**/etc/init.d/sip-dect-omm start**”.

As soon as the RFPs lose the connection to the OMM (because of the update), the RFPs detect that a new image file is on the TFTP server and reboot with the new image file.

9.14.2 UPDATING A STANDBY OMM INSTALLATION

Please note: Updating a standby OMM installation causes a switch over between both OMMs. All active calls will be dropped.

For the update replace the boot image file on the TFTP server(s) with the new one.

OMM in RFP mode

Force the update by pressing the **Update** button on the **Provisioning & Software Update** web page (see section [6.4.1.17](#)). The OMM-RFP checks the boot image file on the TFTP server and initiates an update procedure, if a new image file has been found.

The automated update procedure performs the following steps:

- 1 Reboot the RFP residing the standby OMM.
- 2 Reboot the RFP residing the active OMM which causes a failover to the standby OMM.
- 3 Reboot all other RFPs that are able to find the new boot image file one by one. This is managed by the new active OMM.

This procedure reduces the downtime of the SIP-DECT system to a minimum due to the optimized failover.

Please note: Please be aware that a minimum downtime of the system can only be reached if the system was in a stable working state when initiating the update and the IP infrastructure guarantees a fast update of the OMM RFPs (for example, no 64kbit/s line to download the SW into the RFP).

OMM in host mode (on Linux server)

For an update with a minimum impact to the DECT service do the following:

- 1 Replace the boot image file on the TFTP server(s).
- 2 Manually update the standby OMM.
 - a) Stop the OMM service.

- b) Install the new software.
 - c) Start the OMM service.
 - d) Wait at least 30 seconds before you go on with updating the active OMM.
- 3** Manually update the active OMM.
- a) Stop the OMM service.
 - b) Install the new software.
 - c) Wait at least 30 seconds.
 - d) Start the OMM service.

Please note: A one-by-one update of RFPs is not possible if the signaling interface between the OMM and the RFP has been changed. Please see the release notes delivered with the software.

To enforce an update of the whole DECT system at once, deactivate / update both OMMs simultaneously. The RFPs will lose the connection to both OMMs and will automatically restart with the new boot image file.

9.15 OMM STANDBY

To perform OMM standby, two OpenMobility Managers must be provided in an OMM network. One operates as the active OMM, and the other operates as the standby OMM.

In the event that the RFP designated as the OMM fails, the other RFP, designated as the secondary OMM automatically assumes the role of the OpenMobility Manager.

How OMM Standby works

During system start-up, each RFP retrieves either one (if no standby OMM is configured) or two (if OMM Standby is configured) OMM IP addresses and both try to connect to each other. The active OMM serves all connections from RFPs or DECT phones.

During normal operations, both the active and the standby OMM are in contact and monitor each other's operational state. They continually exchange their current standby states and the standby OMM receives a copy of any configuration changes on the active OMM. As long as both OMMs are in contact, their databases are synchronized automatically.

If the primary OMM fails, the OMM responsibilities are taken over by the standby OMM to maintain operation. A "No Standby" warning is displayed on the OMM web interface, indicating that there are no longer two functioning OMMs in the network or cluster. Configuration changes are made unsafely in this situation.

If the active OMM fails, the inactive OMM recognizes this and begins to act as the active OMM, and starts the web service.

If the connection between the two OMMs fails, the network or cluster essentially breaks into two operational parts. The standby OMM becomes the active OMM. At this point, the two OMMs cannot detect one another and, therefore, cannot synchronize. When the connection between the two OMMs is re-established, the synchronization of the OMMs forces one OMM to become the standby OMM again. Once the recently failed OMM returns to service and becomes the inactive OMM, it does not resume the role of active OMM.

9.15.1 CONFIGURING OMM STANDBY

Each RFP of the DECT system must be configured with two OMM IP addresses. Both OMM addresses can be either configured via DHCP (see section [9.5.1](#)) or with the OM Configurator (see section [9.8](#)).

9.15.2 FAIL OVER SITUATIONS

Fail over occurs when:

- an OMM error occurs on the active OMM.
- the RFP acting as the active OMM is shut down or rebooted at the SSH console.
- the OMM is rebooted in the web browser menu.
- the active OMM is unreachable.

The standby OMM becomes the active OMM when:

- the configured SIP Proxy/Registrar is reachable.
- the other OMM has a larger IP Address while no OMM is active and both OMMs are in contact with each other (normally at system startup).

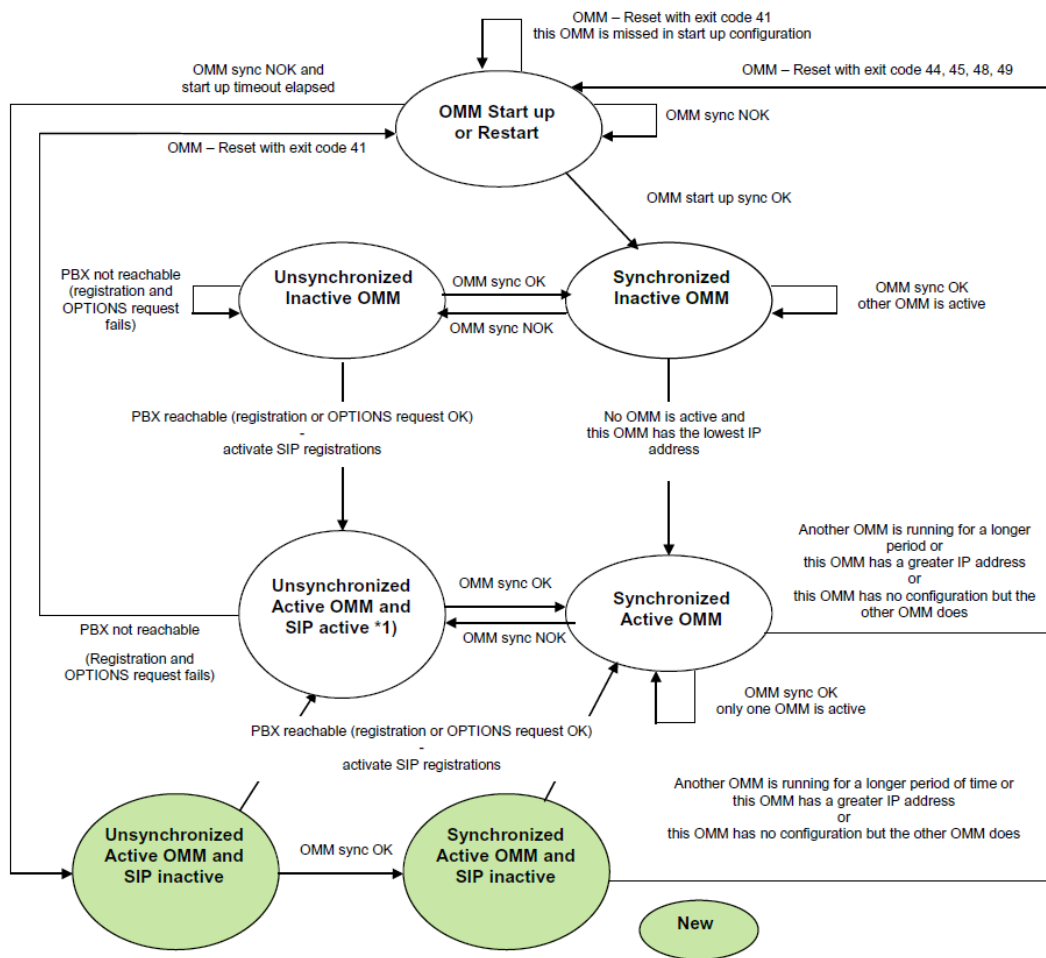
When the OMMs get in contact again:

- both OMMs check which one ran for a longer period. That one will become the active OMM. The other one falls back to the standby one.

9.15.3 FAILOVER FAILURE SITUATIONS

Failover failure occurs when the connection between OMMs fails and the configured SIP Proxy/Registrar is unreachable. In this case the active OMM waits until the SIP Proxy/Registrar is reachable.

The following state diagram shows the OMM Standby states:



“OMM sync OK”: OMMs are synchronized and are able to exchange their operational states

“OMM sync NOK”: OMMs are not synchronized and are not able to exchange their operational states

*1) In this state the DECT air interface might not be in a definite state as both OMMs are active but cannot connect with each other! This is caused by IP network failures and cannot be handled by the SIP-DECT system in a proper automatic way. In such a scenario it is not predetermined which RFP connects with which of the 2 OMMs. The DECT network can split-up into two unsynchronized DECT sub-networks. This can cause voice quality and handover problems.

With these states (“... SIP inactive”) the OMM standby mechanism takes care in the start up phase that all SIP users does not become active if the PBX is not reachable. This avoids a possible double SIP registration when the PBX and the other OMM is reachable again before both OMMs negotiate which OMM becomes the active one.

The double SIP registrations might cause a user not to be reachable when his latest SIP registration came from that OMM that was negotiated to be the inactive one and the SIP registrar cannot handle two or more simultaneous registrations (non-forking proxy).

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

To prevent such problems a mechanism is implemented to detect situations with two active OMMs. If such a situation is detected the remaining active OMM SIP re-registers all users to the PBX if the OMM **SIP reRegister after 2 active OMM failover** parameter is set (see section [6.4.3.5](#)).

9.15.4 SPECIFIC STANDBY SITUATIONS

Some aspects must be described in case of OMM state changes when they are unsynchronized.

9.15.4.1 How a standby OMM becomes active

In an unsynchronized OMM state, the standby OMM must decide whether to become active or not.

The OMM tries to contact the configured SIP proxy and registrar. If a specific user account has not been designated to use for visibility checks (see section [9.19.7](#)), the OMM starts a SIP registration for the DECT phone with the lowest phone number and sends an OPTIONS request to the configured proxy. If there is an answer the SIP proxy/registrar is considered reachable and the OMM becomes active.

9.15.4.2 When OMMs are not synchronized

In an unsynchronized OMM Standby state, the connection between the OMMs is broken. In case of a network problem, both OMMs might be in this state. During this time an inconsistent OpenMobility system is operational with some constraints.

The OMM Web service issues a warning with the message “No Standby” for both OMMs and it is possible that configuration changes made are not saved.

When both OMMs are in contact again, the longer running OMM becomes the active OMM and overwrites the database file in the standby OMM. Configuration changes made in this OMM instance are lost.

9.15.4.3 Two DECT air interfaces

When both OMMs are in an unsynchronized and active state, they are fully operational. DECT base stations that lose their connection to the OMM because of a network outage might connect to the other OMM. Two DECT air interfaces are present and work in parallel.

Note: Since both air interfaces use the same PARK, it is impossible to determine on which OMM a location registration succeeds.

For DECT phones different situations are possible:

- They do not notice this situation:
 - active calls stay established, depending on network conditions;
 - DECT phones can make and receive new calls, depending on an available PBX connection;
 - DECT phones can do handover to RFPs connected to the same OMM;
 - DECT phones can call DECT phones that are registered to the other OMM
- They lose their RFP base station and perform a new location registration:
 - active calls are broken;
 - DECT phones can make and receive new calls, depending on an available PBX connection;

- DECT phones can do handover to RFPs connected to the same OMM;
 - DECT phones can call DECT phones that are registered to the other OMM;
- They lose their RFP base station and search the DECT network without finding another one:
 - active calls are broken;
 - DECT phones stay in searching for network until an air interface is available again.

Note: Handover between DECT phones located to RFPs that are controlled by different OMMs is not possible.

When the OMMs are in contact again, the inconsistencies are resolved.

9.16 MANAGING ACCOUNT DATA FOR SYSTEM ACCESS

Each RFP provides different independent access types:

- The OMM Web service/HTTPS interface (see section [6](#));
- The OMP (see section [7](#));

The OMM Web service and the OMP are mainly used for configuration and administration.

- The OM Configurator (see section [9.8](#));

The OM Configurator is mainly used for static local configuration of an RFP.

- The SSH user shell (see section [10.3.5](#)).

The SSH user shell is mainly used from experts for diagnosis.

Each of these access types uses the same account data.

The account data can be altered at the **System -> User Administration** page of the OMM Web.

The OMM delivers all the necessary account data to all connected RFPs. The RFPs save the account data inside their permanent memory. This has some implications:

- An RFP out of the box uses the default account data as long as this RFP is not connected to the OMM.
- An RFP which was connected for at least one time with the OMM uses the account data from the OMM.
- When the account data are changed on the OMM, any not connected RFPs will continue to use the older passwords.

9.16.1 ACCOUNT TYPES

There are three different account types:

- **Full access:** This access type is the “normal” access for the configuration. Using this access it is allowed to configure the OMM and each RFP. On the SSH interface of an RFP this access type allows login for debug information e. g. “pinging” another RFP to check visibility.

The factory setting for this account is

Name: 'omm'

Password: 'omm'

Active: 'n/a'

- **Read-only access:** As the name suggests this access type is not allowed to configure any item of the OMM installation. This access type can only be used on the OM Web service. The account can be deactivated.

The factory setting for this account is

Name: 'user'

Password: 'user'

Active: 'yes'

- **Root (SSH only) access:** This access type is only applicable on the SSH interface of an RFP. Its purpose is to get detailed information e. g. parameters from the kernel. The access using this account type is not reachable from other hosts hence a login using the full access type is necessary.

The factory setting for this account is

Name: 'root'

Password: '22222'

Active: 'n/a'

Please note: It is highly recommended not to use the “Root (SSH only) access” account type. It is meant for technical support only.

9.16.2 POTENTIAL PITFALLS

When an RFP is configured via the OM Configurator and is taken out of an installation, the RFP may become unusable:

- When this RFP comes up, it finds a valid configuration in its permanent memory. It will hence skip DHCP for booting.
- But when this configuration is not valid anymore (for example, the TFTP server has a new IP address meanwhile), the RFP isn't able to complete the boot and is hence not able to connect to the OMM.
- The RFP will not get newer passwords from the OMM.

It is therefore recommended to switch off the OM Configurator before taking an RFP out of an installation. But nevertheless the OM Configurator allows to reset the permanent memory of an RFP (the Mitel support must be connected).

9.17 WLAN CONFIGURATION

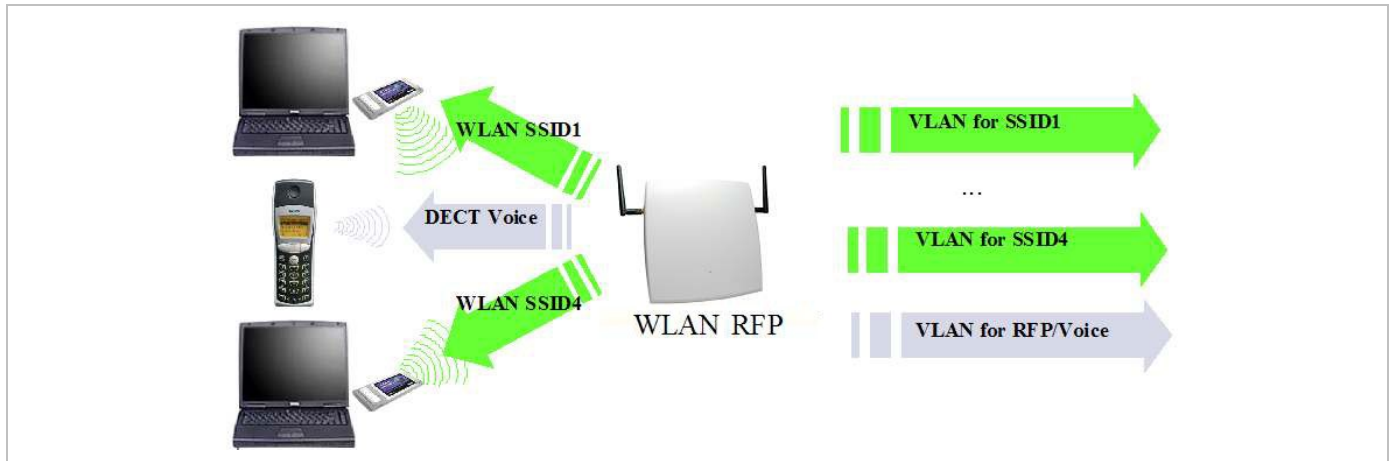
9.17.1 WLAN CONFIGURATION STEPS (RFP 43 WLAN ONLY)

The correct configuration of an RFP with a WLAN interface requires the correct configuration of the DECT part. The second step is to specify the **Regulatory domain** of the WLAN network at the **System settings** page of the OMM web service (see section [6.4.1.3](#)).

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

Select one of the two-letter country codes. 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.

The third step is to specify the WLAN parameters in a profile (see section [6.8.1](#)). The WLAN profile determines the name (SSID) of the WLAN network and other parameters. The encryption and authentication procedures are especially important and must be planned carefully beforehand.



The access point can be assigned to a VLAN that conforms to 802.1q. All the data that is received from and that is to be forwarded to the WLAN clients is then carried by the configured VLAN. All other data, such as VoIP packets, configuration data or authentication data (Radius), is given the VLAN tag configured for the RFP. The switch port of the network component to which the access point is connected must be configured as a trunk port.

Note: The RFP 43/48 WLAN must be connected at least via a 100BaseT Ethernet link in order to activate the RFP's WLAN function.

As a forth step, you must assign a WLAN profile to a configured RFP. This can be done on the **DECT base stations** page of the OMM web service or on the OMP **DECT base stations** -> **Device list** page. Note that specific radio settings for the RFP, such the channel-, 802.11abgn mode-, or antenna settings, are also done in this step.

9.17.2 WLAN CONFIGURATION STEPS (RFP 48 WLAN)

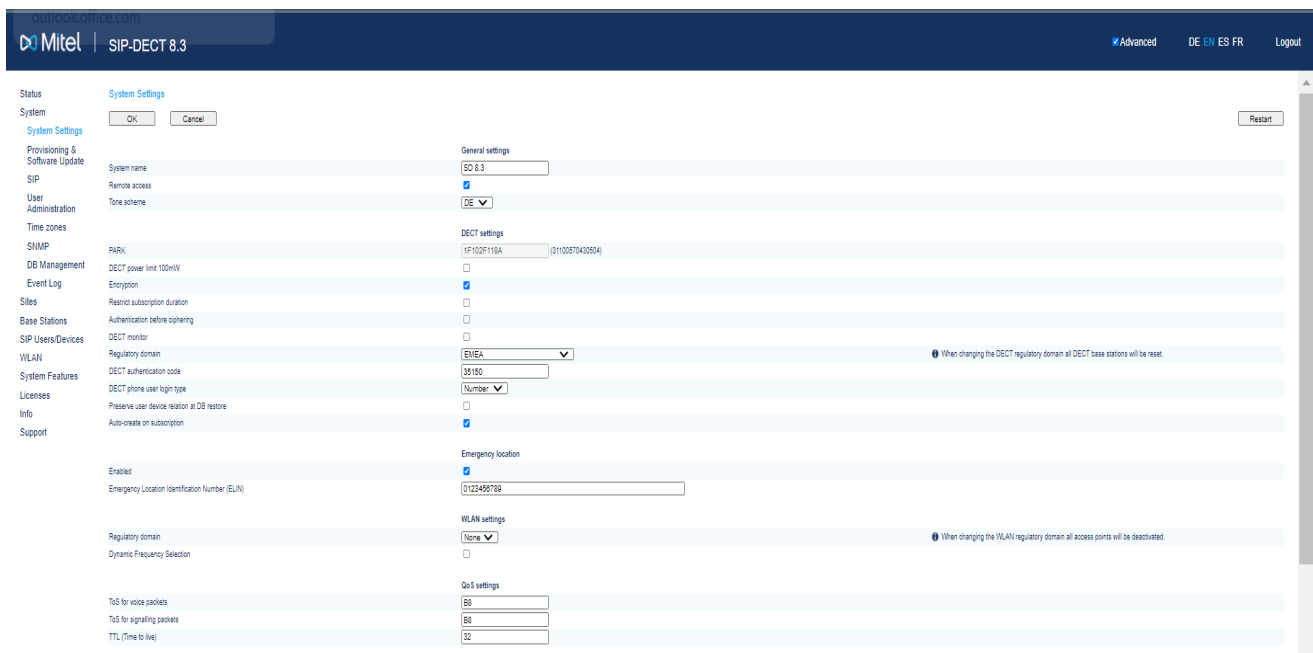
9.17.2.1 Support of 802.11ac WLAN

802.11ac is backward compatible with 802.11a and 'n'. Like the RFP 43, the RFP 48 can only work in one WLAN spectrum at the same time (2.4 GHz or 5 GHz). Within the 2.4 GHz spectrum, the WLAN module supports the 802.11b/g/n modes in the same way as the RFP 43. The third antenna of the RFP 48 increases the data throughput in n mode from 300Mbit/s to 450 Mbps.

In ac mode, HT80 channel bandwidth and 256-QAM modulation increase the data throughput up to 1300 Mbps.

To enable the DFS channels,

- Go to **System>System Settings** (Advanced).
- Select the **Dynamic Frequency Selection** (DFS)



System Settings

General settings

System name:

Remote access: ☒

Tone scheme:

DECT settings

PARC:

DECT power limit 100mW: ☐

Encryption: ☒

Restricted subscription duration: ☐

Authentication before ephering: ☐

DECT monitor: ☐

Regulatory domain:

DECT authentication code:

DECT phone user login type:

Preserve user device relation at DB restore: ☐

Auto-create on subscription: ☒

Emergency location

Enabled: ☒

Emergency Location Identification Number (ELIN):

Regulatory domain:

WLAN settings

Dynamic Frequency Selection: ☐

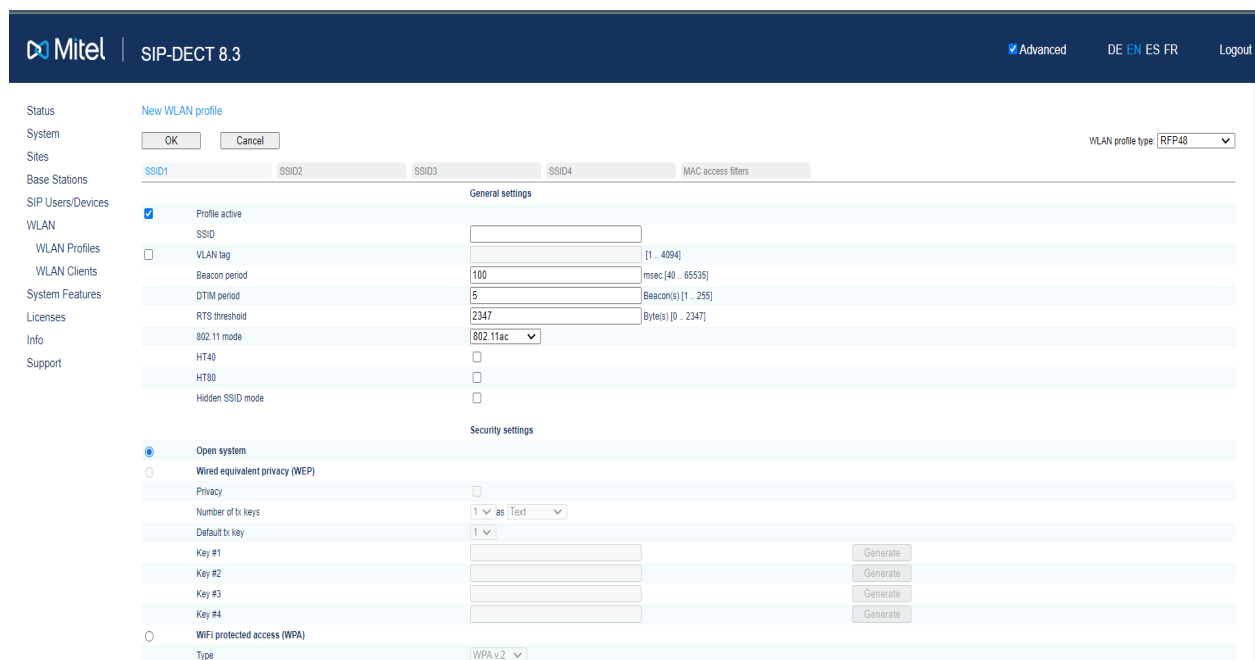
QoS settings

ToS for voice packets:

ToS for signaling packets:

TTL (Time to live):

- to enable the ac mode and HT80: WLAN\WLAN Profiles (new/edit).



New WLAN profile

WLAN profile type:

General settings

Profile active: ☒

SSID:

VLAN tag: [1..4094]

Beacon period: msec [40..65535]

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

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

802.11 mode:

HT40: ☐

HT80: ☐

Hidden SSID mode: ☐

Security settings

Open system: ☒

Wired equivalent privacy (WEP): ☐

Privacy: ☐

Number of tx keys: as

Default tx key:

Key #1:

Key #2:

Key #3:

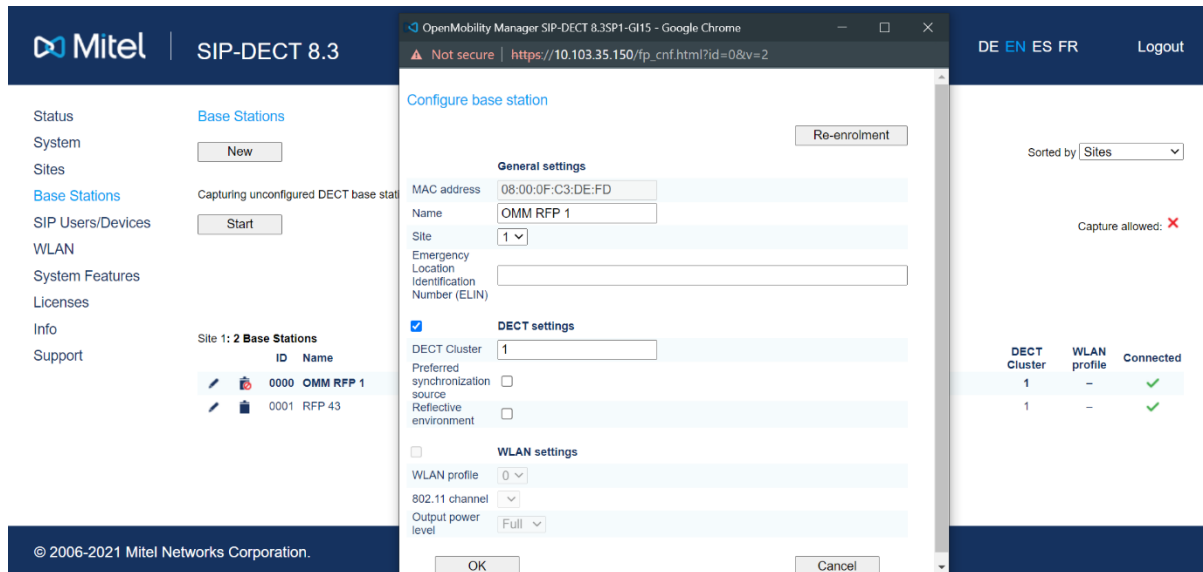
Key #4:

WiFi protected access (WPA): ☐

Type:

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.

- to activate WLAN and to set the WLAN profile / channel / power level for a base station (edit):



The selected WLAN channels have a default bandwidth of 20 MHz. If the WLAN profile options like HT80/ HT40 MHz is activated, the necessary center channel is automatically selected in the corresponding areas during the configuration itself.

In the 2.4 GHz band, a channel with 40 MHz bandwidth is only established if no other 20 MHz channel is disturbed. Otherwise, a fallback to 20 MHz bandwidth is made.

WLAN is a shared media. Depending on the application, it is useful to have 4 RFPs with a bandwidth of 20 MHz (for canteen room) or to have one RFP with a bandwidth with 80 MHz (for large conference room).

9.17.3 OPTIMIZING THE WLAN

Beacon Interval

Transmitting beacons requires transmission channel capacity. A shorted beacon interval increases the WLAN network's ability to detect signals, thus improving its availability. At the same time, it increases the network's ability to adjust the mutually negotiated signal strength. A longer beacon interval saves WLAN air time and also reduces the power consumption of mobile WLAN clients.

RTS Threshold

If the network throughput is low or if many retransmissions occur, the RTS/CTS handshake can be activated by reducing the RTS threshold value below 1500 byte. This can improve throughput, especially in environments where reflection and attenuation cause problems for HF.

Fragmentation Threshold

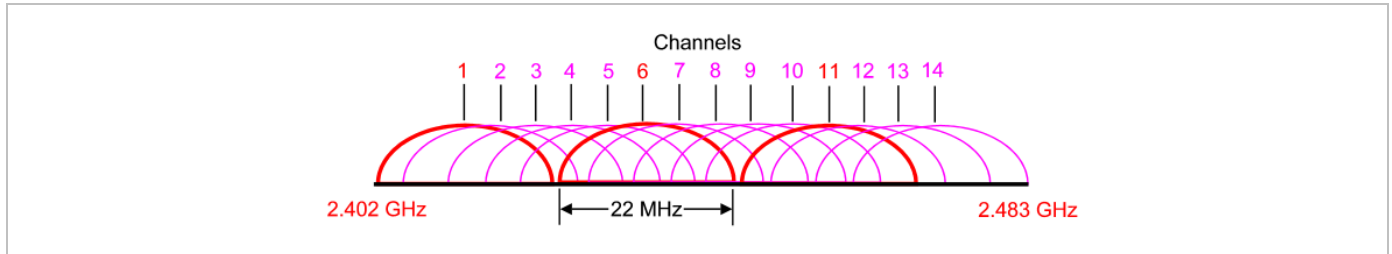
In environments where there is lot of interference and poor radio quality, reducing the fragment size below 1500 bytes can improve the effective throughput. However, transmitted data frames must be fragmented, which means a higher load on the RFP's processor. This option is not configurable with RFP 48 WLAN.

DTIM Period

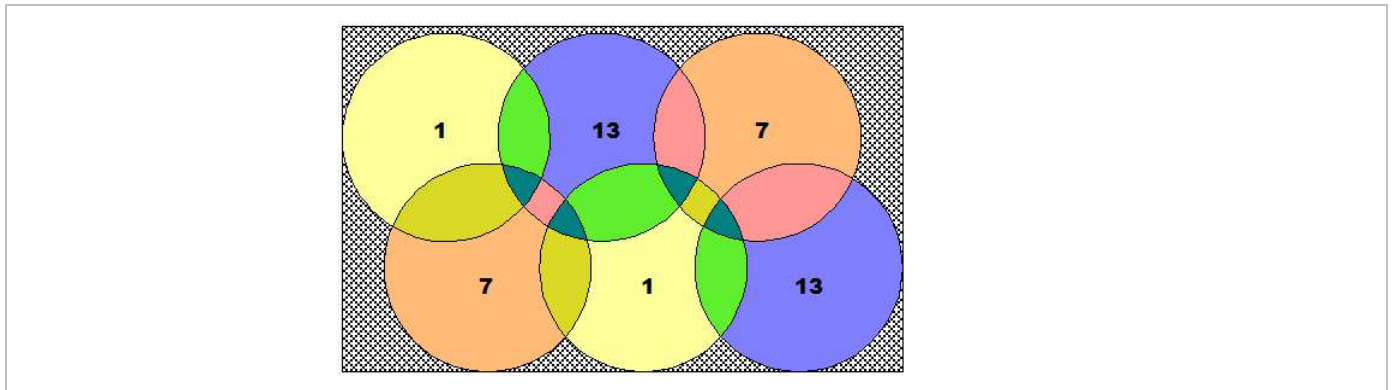
The DTIM period specifies the interval between transmissions of the broadcast and multicast packets. All WLAN clients must be active during this interval. Increasing the DTIM period lowers the client's power consumption slightly. Not all programs can manage the increase in response times, however.

Channel Allocation

Every WLAN RFP must be configured to a channel. You should ensure that the channel settings do not overlap. WLAN RFPs within range of each other should be configured at least five channels apart. When the radio field is planned, the WLAN RFPs of foreign WLANs that may be operating in the vicinity must be taken into account.



When planning the radio coverage for a two-dimensional area, please bear in mind that the distance between any two base stations operating on the same frequency must be at least twice their range. The range can be adjusted by lowering the output power level.



802.11i: WPA2-Enterprise Pre-Authentication for fast Roaming

WLAN stations (for example, 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.

Channel Configuration Feedback for HT40 and Transmit 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 will fall back to HT20.

The effective channel configuration and the transmit power are reported to the OpenMobility Manager.

Users can inspect these parameters using the WEB interface and the OMP and may change the channel to a frequency without overlapping APs.

Support of 802.11ac-WLAN for RFP 48 WLAN

The RFP 48 WLAN is a new WLAN module, which supports the WLAN ac mode wave 1. Within the 5 GHz spectrum, the ac mode is 2.5x faster as the 'n' mode of WLAN. The RFP 48 is 4x faster with comparison to the RFP 43 having two antennas. This is achieved by more efficient coding (256-QAM)

with more bandwidth (HT80) per channel and one more antenna (3x3 MIMO compared to the RFP 43: 2x2 MIMO).

For more information about data rates, see: <http://mcsindex.com/>

9.17.4 SECURING THE WLAN

In order to ensure that communication in the WLAN network is secure, several measures must be taken. Firstly, data packets transmitted via the openly visible radio interface must be encrypted, and secondly, all WLAN components that provide services must authenticate themselves.

There are different encryption methods available that you configure within the WLAN profile (see section [6.8.1](#)). However, only the recent WiFi protected access (WPA) encryption offers sufficient security against possible intruders. You should not use the (older) WEP encryption for your company LAN.

Especially with larger WLAN installations, the single shared secret offered by WPA-personal may not be sufficient for your security requirements, because any person that connects to the WLAN needs to know the same shared secret. For this reason, you should also setup RADIUS authentication that is supported by all RFP 42 WLAN, RFP 43 WLAN and RFP 48 WLAN devices.

A Radius Server (Remote Authentication Dial In User Service) handles 802.1x Authentication, thus authorizing different WLAN clients with an individual username / password combination to log in. We recommend a Radius Server with EAP-TLS (for example, FreeRadius or MS Windows 2003 IAS Server) and a Certificate Authority (CA).

The RADIUS authentication takes place between the RADIUS server and the RADIUS client, with the WLAN RFP to pass-through this communication. You should refer to the documentation that comes with your RADIUS product for details on how to setup, maintain and operate the RADIUS system.

The WLAN module of RFP 48 supports Dynamic Frequency Selection (DFS) and Transmit Power Control (TPC). These features are required for the radar detection (flight and weather) and are necessary to use the WLAN channels 52 – 140 in Europe and USA. If radar pattern detected, the RFP 48 changes its WLAN channel by itself to another channel without radar for half an hour. The 5GHz high band with its channels 149 – 165 is supported too.

9.18 SNMP CONFIGURATION

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. The SNMP agents can be configured in the **SNMP** menu of the OM Web service (see section [6.4.6](#)).

All SNMP agents are configured by the OMM. Additional parameters that are valid for the individual RFP (for example, “sysLocation” and “sysName”) are generated. The “sysLocation” parameter corresponds to the location configured via the OMM web interface. The “sysName” parameter is generated using the MAC address and the RFP device type (for example, RFP 43 WLAN). The RFP uptime can be requested by reading the “sysUpTime” parameter. This value indicates how long the RFP application software is running. It does not indicate the uptime of the operating system which does not correspond to the operational RFP state.

The SNMP agent responds to SNMPv1-read and SNMPv2c-read requests for the standard MIB-II objects. The Management Information Base (MIB-II) contains 11 object groups. The agent receives both SNMPv1 and SNMPv2c traps. It sends a “coldStart” trap when it first starts up. It also sends an enterprise-specific trap “nsNotifyShutdown” when it stops. When the SNMP agent receives an SNMP request using an unknown community name, it sends an “authenticationFailure” trap. The SNMP agent also generates an enterprise-specific trap “nsNotifyRestart” (rather than the standard “coldStart” or “warmStart” traps) after being reconfigured.

9.19 BACKUP SIP PROXY/REGISTRAR

This section provides an overview about the supported redundancy concepts with SIP-DECT to realize a high availability solution together with IPBX redundancy mechanism.

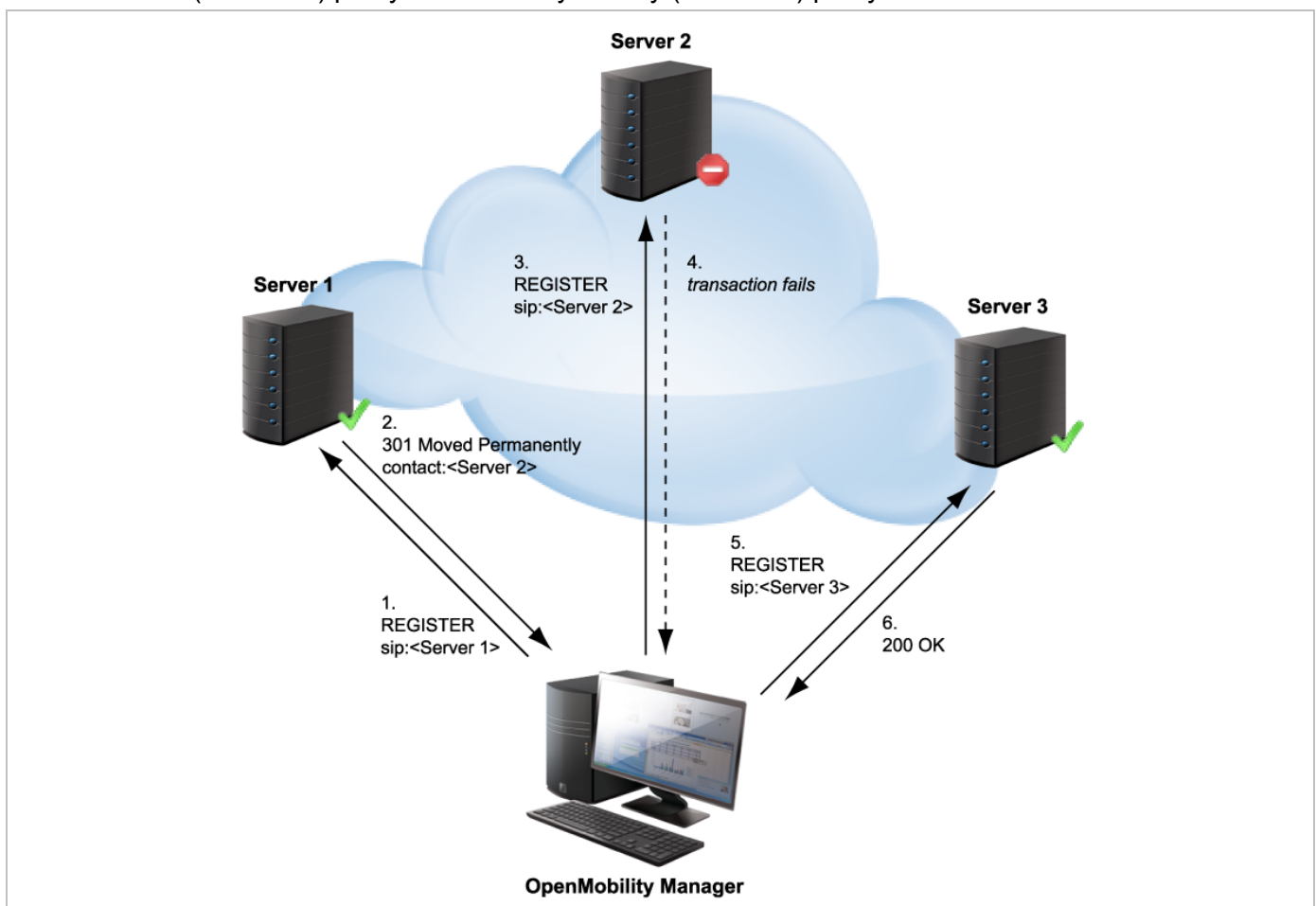
The focus of this section is IPBX redundancy. For information regarding OMM redundancy, see section [9.15](#).

9.19.1 REGISTER REDIRECT

To allow IPBX systems to spread the registration and call traffic over different servers the OMM supports 301 (Moved Permanently) or 302 (Moved Temporarily) responses for registrations.

When a 301 or 302 response is received, the OMM follows the redirect and registers the concerning user to the given address. If more than one contact address are given in the 301/302 response, the OMM tries to contact the registrars successively until the registration succeeds.

If the redirected register succeeds and if the configured proxy and registrar are identical, all subsequent INVITE requests are sent to the redirected server. In the other case all subsequent INVITE requests will be sent to the (outbound) proxy or secondary/tertiary (outbound) proxy.



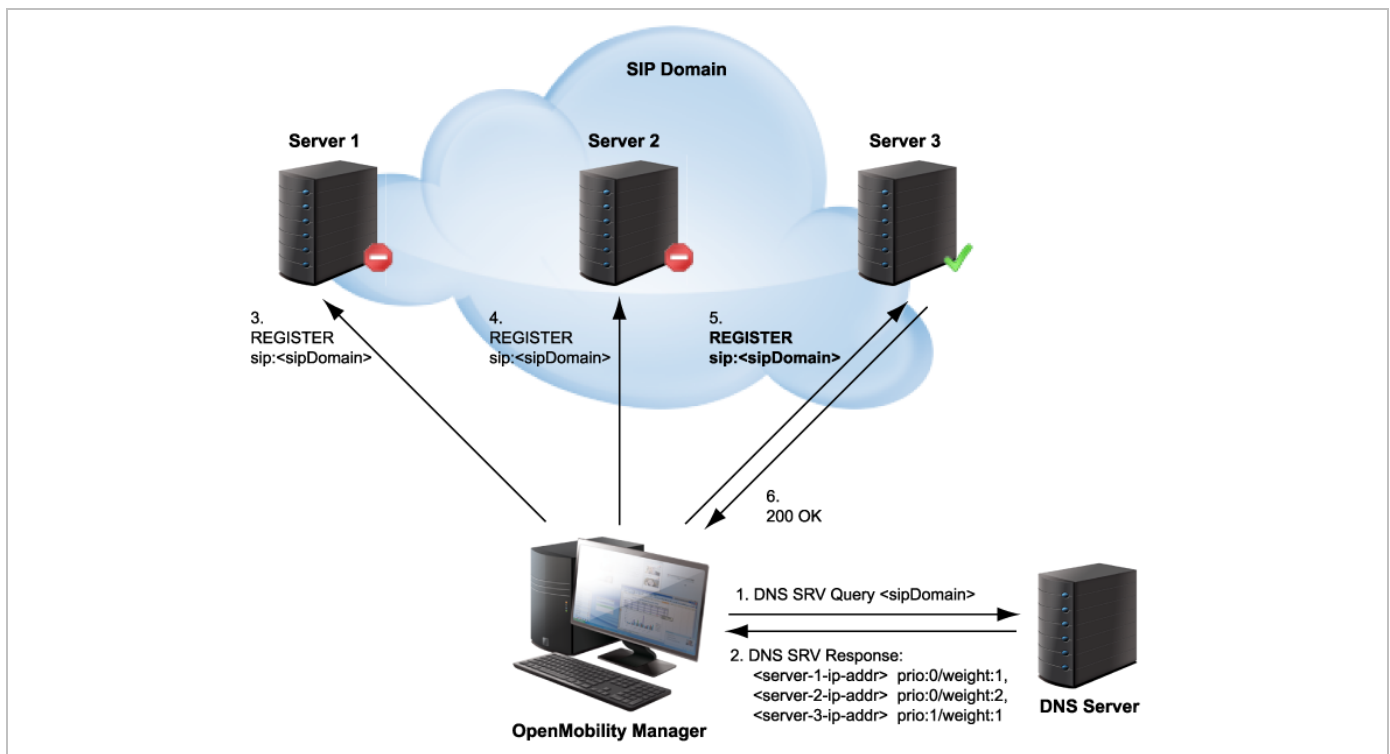
9.19.2 DNS SRV

If a full qualified domain name is configured as proxy, outbound proxy or registrar server and the respective port setting is set to zero ("0"), the OMM performs a DNS SRV query before an appropriate SIP transaction is started. Herewith the OMM locates a list of servers responsible for the given SIP

domain. With this configuration, the default port ("5060") is used for every server address acquired with this mechanism.

The DNS SRV results are sorted by priority and weight in ascending order by the OMM. As soon as the DNS SRV query succeeds, the OMM starts the appropriate SIP transaction by sending the request to the server with the uppermost priority and weight of the DNS SRV result.

If there is no answer from the first SIP server in a configurable time frame ("Transaction Timer" parameter), or a 5xx response is received, it will be assumed as unreachable and the OMM tries to contact the next server of the DNS SRV result. Therefore the request will be send to the second server of the DNS SRV query result. If there is also no answer in the given time frame or a 5xx response is received from the second server, the request will be send to the third server and so on. When there is an answer other than 5xx from one of the contacted servers, this server will be used for this transaction.



To prevent situations where the OMM tries to contact with each new transaction servers which are unreachable (out of service), the OMM offers a blacklist feature. If there is no answer from a SIP server, this specific server can be put into a blacklist and will not be contacted anymore for a configurable time of "Blacklist time out" minutes by all adjacent SIP transactions.

In differentiation to the concepts described in the following sections note that independent of which SIP server is used, all requests send by the OMM carry the same sender Address-of-Record (AOR)¹. This means that the sender URI consisting of user-ID and domain is not changed during a failover to another server.

¹ RFC 3261: An address-of-record (AOR) is a SIP or SIPS URI that points to a domain with a location service that can map the URI to another URI where the user might be available. Typically, the location service is populated through registrations. An AOR is frequently thought of as the "public address" of the user.

9.19.2.1 IP address retention during DNS server failure

To increase the SIP resiliency when a DNS server fails or becomes unreachable, the SIP-DECT solution retains the resolved IP addresses for a SIP call traffic even after the configured TTL value is crossed.

If the DNS server fails, the following event log is generated and the SIP signaling continues to use the previously determined IP address until the DNS server becomes reachable again.

DSIP: resolving of mysipproxy.mitel.com failed

The expired IP addresses matching the configured SIP (Outbound) Proxy/Registrar settings (FQDN) are stored until any of the following occurs:

- OMM restart,
- SIP (Outbound) Proxy/Registrar reconfiguration, or
- DNS server becomes reachable again.

All other expired entries will be discarded when they are not used within 4 hours.

9.19.3 BACKUP SIP SERVERS

The SIP-DECT solution allows configuration of two additional levels of backup servers, in addition to the primary proxy, outbound proxy and registrar server. These two additional levels of backup servers are referred to as secondary and tertiary servers in the following sections.

SIP backup servers can be configured in the **System -> SIP** menu of the OM Management Portal (OMP), see also section [7.7.4](#).

You can configure IP addresses, names or full qualified domain names as server addresses. It is also possible to configure a mixture of IP addresses, names or full 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 are performed to locate a list of servers in the domain. It is assumed that all server addresses are specified by name or IP address. With fully qualified domain names, the behavior described in section [9.19.2](#) is performed in addition to contact the SIP servers in the given domain.

This redundancy mechanism is based on a failover concept where the OMM first tries to contact the primary server. If the primary server fails, the OMM tries to contact the secondary server and if the secondary server fails also, the OMM tries to contact the tertiary server.

The OMM failover behavior in detail depends on the backup server settings.

9.19.3.1 No Secondary/Tertiary Proxy, Outbound Proxy and Registrar Configured

In this case no failover to a secondary/tertiary (outbound) proxy / registrar is possible.

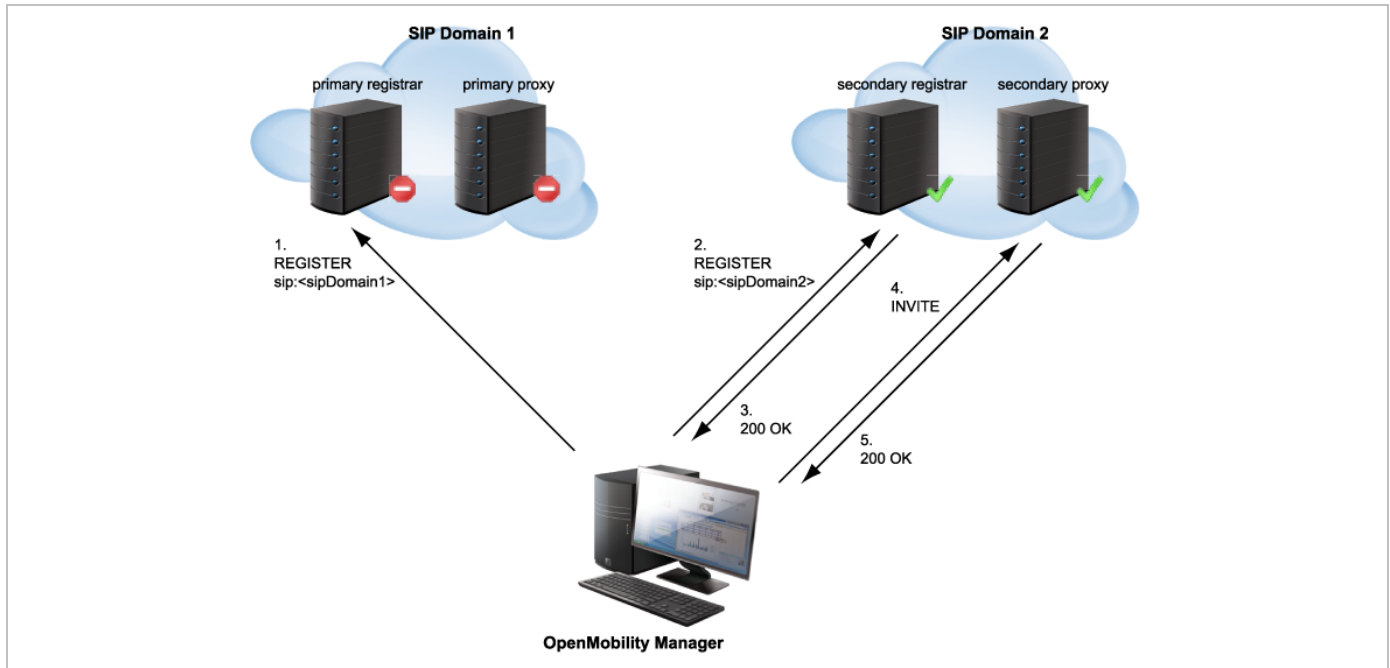
9.19.3.2 Secondary/Tertiary Proxy and Registrar Configured

All REGISTER and re-REGISTER requests attempt to use the primary registrar first.

If the primary registrar fails (for example, no answer in "transaction timer" time frame), the user is tried to register with the secondary/tertiary registrar using as AOR the secondary/tertiary proxy address.

When the registration with the secondary/tertiary registrar succeeds:

- the MWI subscription is moved to the secondary/tertiary proxy,
- all subsequent INVITE requests attempt to use the secondary/tertiary proxy,
- the registration of all other users currently registered with the failed server will be automatically refreshed if the “Failover keep alive” setting is enabled (see page 237). For this purpose, the re-register requests will be queued and proceed according to the settings for “Registration traffic shaping” (see section [6.4.3.5](#)).



If a user was registered successfully with the secondary/tertiary registrar and can be registered again with the primary registrar for example, during a re-registration:

- the MWI subscription is moved back to the primary (outbound) proxy,
- all subsequent INVITE requests attempt to use the primary (outbound) proxy again,
- the registration of all other users currently registered with the secondary/tertiary registrar will be automatically refreshed.

As long as no successful registration exists, all INVITE requests attempt to use the primary (outbound) proxy as first.

If the INVITE request to the primary proxy fails, the INVITE request attempts to use the secondary/tertiary proxy. If an INVITE request fails (no answer in “transaction timer” time frame) send to a proxy identical with own registrar, the registration will be refreshed.

9.19.3.3 Secondary/Tertiary Proxy, Registrar and Outbound Proxy Configured

In this case, the OMM behavior is as described in section [9.19.3.2](#) but all requests for the secondary/tertiary proxy/registrar are sent through the outbound proxy.

9.19.3.4 Secondary/Tertiary Proxy Configured Only

All REGISTER, INVITE and SUBSCRIBE requests attempt to use the primary proxy or registrar first.

If an INVITE/SUBSCRIBE request fails, the INVITE/SUBSCRIBE request attempts to use the secondary/tertiary proxy.

9.19.3.5 Secondary/Tertiary Outbound Proxy Configured Only

The OMM behavior is as described in section [9.19.3.2](#), but:

- all requests for the secondary/tertiary proxy/registrar are sent through the outbound proxy;
- if the registration with the primary registrar fails, the registration is re-tried using the primary proxy address as AOR sent through the outbound proxy.

9.19.3.6 Secondary/Tertiary Registrar Configured Only

All REGISTER, INVITE and SUBSCRIBE requests attempt to use the primary proxy or registrar first.

If a REGISTER request fails, the request attempts to use the secondary/tertiary registrar.

9.19.4 KEEP ALIVE MECHANISM

A keep-alive mechanism implemented in the OMM allows the automatic failover to secondary/tertiary servers or automatic coming back to primary servers. The keep-alive mechanism is based on the registration process and utilizes the special behavior that all REGISTER and re-REGISTER requests are sent to the primary registrar first.

The following configuration parameters are introduced: **Failover keep alive** and **Failover keep alive time**. These parameters are set in the OM Management Portal (OMP) on the **Backup settings** tab of the **System: SIP** menu (see page 237).

For each registration target, a user could be registered successfully with, a keep alive procedure is started. For this purpose the first user registered successfully on a registration target will be selected to re-register all "Failover keep alive time" before the registration period expires.

If the re-registration of this selected user detects that the current primary server fails, the registration of all users registered on the same server will be refreshed automatically. For this purpose the re-register requests are queued and proceed according to the registration traffic settings (see section [6.4.3.5](#) for OMM Web or section [7.7.4.3](#) for OMP).

If the re-registration of a selected user detects that the primary server is available again, the registration of all users registered on a secondary/tertiary registrar will be refreshed.

When the proxy server is set to 127.0.0.1, local calls can be performed without a SIP server. Local SIP redundancy is now supported for all transport protocols (UDP/TCP/TLS). In previous releases only UDP was supported for local SIP redundancy.

A SIP failover occurs in all cases when the response code is not:

- 486: Busy
- 487: Request Terminated
- 480: Temporary not available
- 484: Address incomplete
- Configured: Call reject state code (user reject)
- Configured: Call reject state code (device unreachable)

Note: The SIP-DECT mechanism of polling the registration targets (Failover keep alive) is also disabled when "Auto switch back to primary" is disabled. Also, SIP Backup Server keep alive mechanism is not active when "Auto switch back to primary" is disabled.

9.19.5 PRIORITIZED REGISTRATION

Depending on the settings for “Registration traffic shaping”, the registration of a high number of users could need minutes. In effect single users could not be reachable for minutes during startup.

To guarantee a minimum blackout for very important people (for example, emergency user) the registration of such people can be prioritized. Therefore a special user attribute VIP (very important person) is introduced. The corresponding option is set in the **SIP** tab of the DECT phone **Detail** Section (see [7.11.4](#)).

9.19.6 MONITORING THE SIP REGISTRATION STATUS

The SIP registration status of a DECT phone user can be monitored by using the OpenMobility Management Portal (OMP). In OMP monitor mode you can view on which registrar a specific DECT phone user is registered and whether the server is a primary, secondary or tertiary server. To monitor the SIP registration status proceed as follows:

- 1 Launch the OMP (see section [7.1](#)) and navigate to the **DECT Phones -> Overview** menu.
- 2 Switch to **Monitor Mode**.
- 3 Activate the **Registered**, **Registrar server type**, **Registrar server** and **Registrar port** columns (see section [7.11.9](#)).

9.19.7 CONFIGURABLE USER ACCOUNT FOR STANDBY CHECK

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

Therefore, 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 older 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 on the **SIP** tab when creating or editing a DECT phone.

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

9.19.8 OMM STANDBY ENHANCEMENT

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

To prevent such problems a mechanism is realized 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 via the OMP **SIP->Supplementary Services** tab (see section [7.7.4.8](#)).

The screenshot displays the Mitel OMP configuration interface. The top navigation bar includes the Mitel logo and icons for settings, search, and edit. The sidebar on the left lists various configuration categories: Configuration, Status, System, Basic settings, Advanced settings, SIP, Provisioning, User administration, Data management, Sites, DECT base stations, WLAN, DECT phones, Conference rooms, System features, Licenses, and Support. The main content area is titled 'Supplementary services' and is divided into three sections:

- Call behaviour:**
 - Call transfer by hook (A142d): ☐
 - Call transfer by hook (6xxd): ☒
 - Ringback on hold: ☒
 - Call reject on silent charging: ☐
 - Call release timeout: 5 sec
 - Hold call release timeout: 5 sec
 - Failed call release timeout: 5 sec
- Miscellaneous:**
 - Call forwarding / diversion: ☒
 - Local line handling: ☒
 - Maximal digits of internal call number: 0
 - Truncate Caller identification after ",": ☐
 - SIP reRegister after 2 active OMM failover: ☐
- Distinctive ring tone for call type:**
 - Internal:
 - External:
 - Callback:
 - Emergency:
 - VIP:

At the bottom of the configuration area are 'OK' and 'Cancel' buttons.

9.20 CONFERENCING

Depending on the type of conference server used, SIP-DECT offers the following operational modes:

- **None:** Neither external nor internal conference server is used.
- **Integrated:** The conference server integrated in SIP-DECT is used.
- **External:** An external conference server is used, for example, Broadsoft or Sylantro. 407-oamp-sys-sip-conference.tif
- **External – Blind Transfer:** A MiVoice Business conference server is used, whose proprietary SIP signaling requires that the initiation of the conference be signaled to the destination (as specified in the URL parameter) as a blind transfer.

The conference mode can be configured globally for all SIP-DECT users on the OMP **System -> SIP -> Conference** tab (see section [7.7.4.9](#)). Alternatively, the conference mode for individual users can be configured on the OMP **DECT Phones -> Overview -> Conference** tab (see section [7.11.4.4](#)). When the **Global** setting is selected for a user, the global system conference mode will be used for this user.

The default for the global system conference mode is **None**. For the user-specific mode, the default is **Global**.

The global and/or user specific conference mode can also be configured via OMM configuration files or the OMM application XML interface (AXI).

9.20.1 CENTRALIZED CONFERENCING

To enable SIP centralized conferencing on DECT phones select **External** as **Server type** for all users on the OMP's **System** -> **SIP** page or for specific users on the OMP's **DECT Phones** -> **Users** page. If there is specified a proxy / registrar server, then to reach the conference media server via the proxy server, set the **URL** field to one of the following prefixes:

- **Conf** (Sylantro server)
- **Conference** (Broadsoft server)

Examples

To set the **URI** field to "conf" or "Conference", specify "conf@<proxy-server-address>:<proxy-port>" or "Conference@<proxy-server-address>:<proxy-port>".

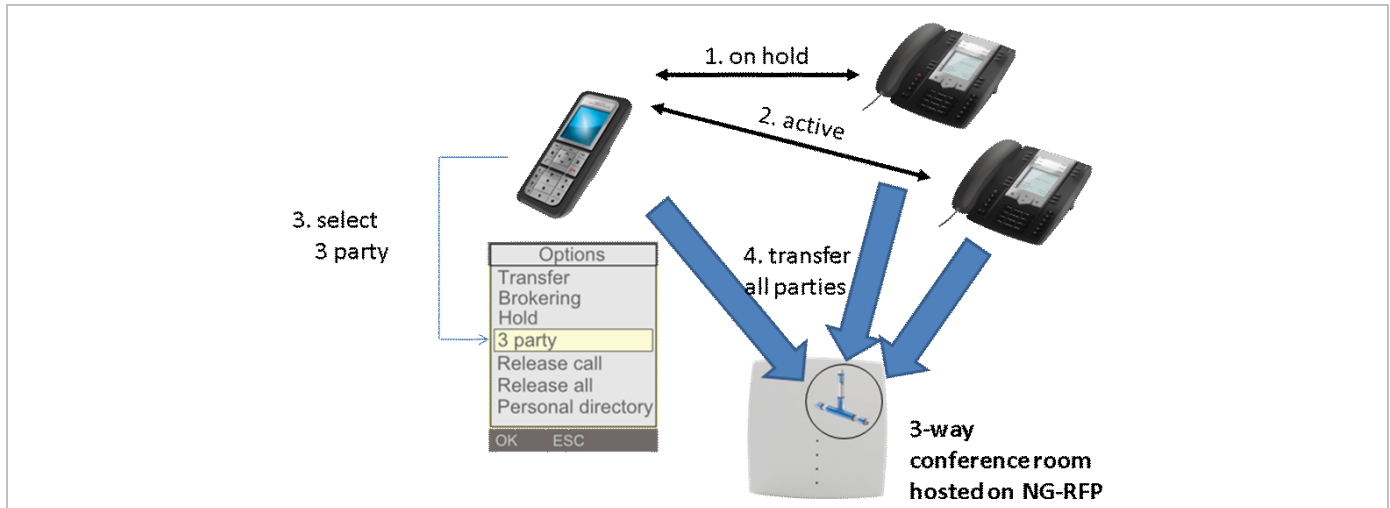
To reach the conference media server using a different address/port then that is specified by the proxy, set the **URI** field to "conf@<media-server-address>:<media-port>"

9.20.2 INTEGRATED CONFERENCE SERVER (ICS)

The conference server integrated in SIP-DECT is based on the SIP standard RFC 4579 and allows SIP-DECT users the ad-hoc initiation of 3-way conferences.

If this feature is enabled, it allows SIP-DECT users having an active call and holding another call to select **3 party** in the **Options** menu of a Mitel 600/700 DECT phone to initiate an ad-hoc 3-way conference. If a 3-way conference is initiated, the conference initiator and both connected parties are transferred to the next free conference room hosted on one of the RFP 35 / 36 / 37 / 43 devices.

ICS provides the full range of voice codecs (G722, G711 μ -law, G711 a-law and G729) and supports trans-coding for all parties in a three-way conference session.



Enabling the SIP-DECT integrated 3-way conferencing requires the following configuration steps:

- Enable internal conference mode
- Select RFP devices for conferencing
- Configure conference rooms

9.20.2.1 Enable internal conference mode

To enable SIP-DECT internal 3-way conferencing for DECT phones select **Integrated** as the **Server type** setting for all users on the OMP's **System-> SIP** page or for specific users on the OMP's **DECT Phones -> Users** page.

9.20.2.2 Disable the hold tone for a conference

To disable the hold tone provided by a call server for conferences, select the **Suppress audio on hold** check box on the OMP's **System -> SIP -> Conference -> Internal conference** page.

The **Suppress audio on hold** option improves the SIP-DECT interoperability with various call servers in addition to suppressing the hold tone when a user puts a conference on hold.

Basic settings	Advanced settings	Registration traffic shaping	Backup settings	RTP settings
DTMF settings	Intercom/Push-to-talk	Supplementary services	Conference	Security

Conference server

Server type: None
URL:

Internal conference

Suppress audio on hold: ☒

9.20.2.3 Select RFP devices for conferencing

Select some of the RFP devices from your SIP-DECT infrastructure to provide conferences. For this enable the **Conference channels** flag for each selected RFP on the OMP's **DECT base stations** -> **Devices** -> **General** tab.

Please note: Only RFP 35 / 36 / 37 / 43 / 44 / 45 / 48 devices support 3-way conferences.

DECT base station #0x000

General | DECT | WLAN | Hardware

Name:
MAC address:
Emergency location identification number:
Site: default
Building:
Floor:
Room:
Conference channels: ☐

OK Cancel

Depending on the DECT and G.729 configuration, an RFP device enabled for conferencing provides between 3 and 24 conference channels. To compute one 3-way conference 3 conference channels are necessary.

In particular, the G.729 codec, with its high consumption of computing time, reduces the number of available conference channels according to the following table.

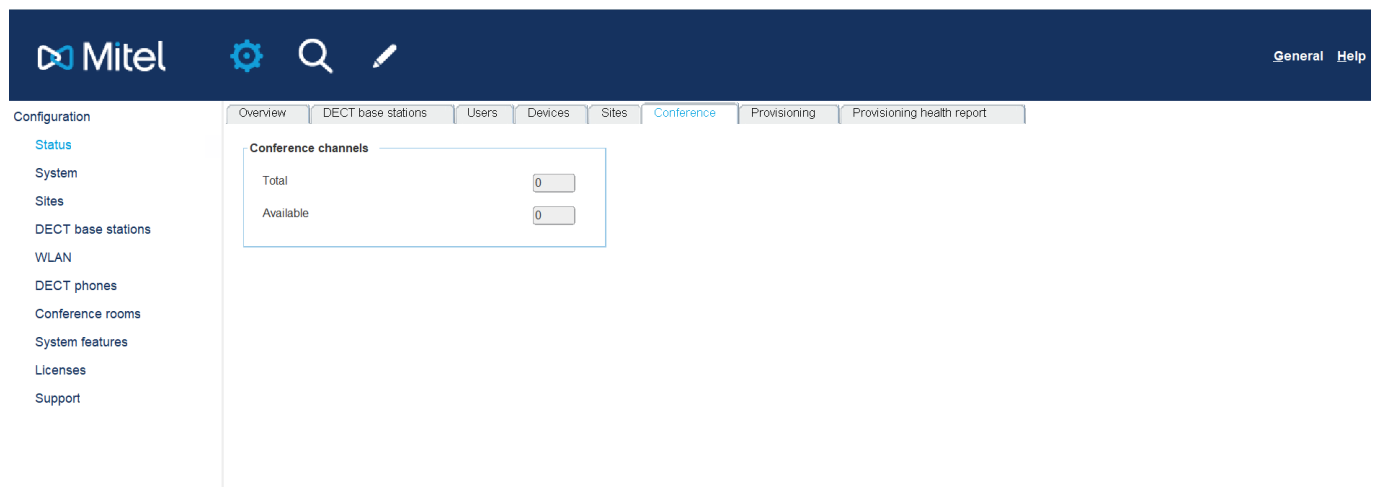
DECT enabled	Conferencing enabled	G.729 enabled	Conference channels	DECT voice channels
Yes	No	Yes/No	0	8

DECT enabled	Conferencing enabled	G.729 enabled	Conference channels	DECT voice channels
Yes	Yes	No	15	8
Yes	Yes	Yes	3	5
No	Yes	No	24	0
No	Yes	Yes	9	0

Please note: Activating the **Conference channels** option on an RFP with enabled DECT and in a system with enabled G.729 reduces the available DECT channels on that RFP from 8 to 5.

If the G.729 codec is not necessary on your iPBX platform, disable the G.729 codecs on the OMP's the **System: SIP** page / **RTP settings** tab to obtain the maximum number of conference channels.

The total number of conference channels in the SIP-DECT system is presented the OMP's **Status -> Conference** tab. The **Total** parameter provides the total number of conference channels in the system and the **Available** parameter provides the current number of available conference channels.



9.20.3 CONFIGURE CONFERENCE ROOMS

When a three-way conference is initiated by a SIP-DECT user, the initiator and the connected parties will be transferred to the next free conference room using SIP signalling. These conference rooms must be configured on the OMP's **Conference rooms** page with their SIP user id and SIP password (see section [7.12](#)).

Configure as many conference rooms as necessary and as conference channels are available (3 channels per conference).

These conference rooms will be SIP registered on the configured SIP registrar and must be reachable via the configured SIP proxy for SIP signalling.

The following parameters can be configured for each conference room

- **Name:** SIP display name
- **Conference ID:** SIP user id
- **User Name:** SIP authentication name
- **Password:** SIP password
- **Fixed SIP port:** Port used explicitly for SIP signaling. If set to 0 (default), an automatically calculated port is used for this conference room. See section [2.17](#) for more information.
- **Calculated SIP port:** Auto-calculated port used for SIP signaling (read-only). Only used if no value is specified for **Fixed SIP port**.

All configured conference rooms will be registered on the registrar / iPBX configured in OMM. If the **X-Aastra-Id Info** option is enabled on the OMP's **System: SIP -> Advanced settings** tab, a private X-Aastra-Id header is sent out which identifies that these are conference rooms.

The screenshot displays the 'Advanced settings' tab for a conference room configuration. The 'General' section contains various parameters for SIP signaling and registration, including timers, retry attempts, and contact matching. The 'Semi-attended transfer' section shows options for transfer mode and replacing. The interface includes 'OK' and 'Cancel' buttons at the bottom.

The X-Aastra-Id header has the following format for all conference rooms:

```
X-Aastra-Id: type="29" model="01" version="1.0.0"
```

The header's attributes have the following properties:

type

- the type parameter contains the phone type
- the value for all SIP-DECT conference rooms is "29"
- type = DQUOTE (1*2HEXDIG) DQUOTE

model

- it's the model of the terminal
- the value for all SIP-DECT conference rooms is "01"
- model = DQUOTE (1*2HEXDIG) DQUOTE

version

- the version is intended for later releases
- the value for all SIP-DECT conference rooms is “1.0.0”
- version = DQUOTE (1*16token) DQUOTE

9.20.4 REGISTRATION OF CONFERENCE ROOMS

In SIP-DECT Release 8.0 and earlier releases, SIP-DECT conference room users does not reboot for an indefinite interval of time after any process such as a restart, reset, or update of a call manager that requires a reboot of the call manager and registration of SIP-DECT users. This is because, after the reboot, the call manager sends a SIP Notify event to the OMM to prompt the registration of SIP-DECT users, and the registration process initiated by this event does not apply to SIP-DECT conference room users.

In SIP DECT Release 8.0 SP1, SIP registration through the XML terminal interface API is supported, which enables the registration of SIP-DECT conference room users. An internal registration is triggered for SIP-DECT conference room users by the SIP Notify event `aastra-xml` and body `Command:SipRegister` after a call manger reboot. This enables the call manager to initiate the registration of SIP-DECT conference room users after any process that involves a reboot; for example, after a restart of the call manager.

Note: The XML terminal interface API is supported only to register the SIP users of the conference rooms.

9.21 DOWNLOAD OVER AIR

The “Download Over Air” feature allows updating the DECT phone firmware without any user interaction or interruption of the telephony services over the existing DECT air interface. This feature is currently available for the Mitel 600/700 DECT Phones.

With SIP-DECT 6.0 and later, the SIP-DECT RFP software images (`iprfp3G.dnld` or `iprfp4G.dnld`) contains the Mitel 600 DECT phone software. If the RFP houses the OMM, the OMM uses this software to update the DECT phones. The RFP OMM no longer automatically attempts to load a DECT phone software image from a RFP 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 [6.4.1.7](#)). The Mitel 600/700 DECT phone firmware packages are delivered in the “600.dnld/700dnld” file for the OMM running on an RFP.

9.21.1 HOW “DOWNLOAD OVER AIR” WORKS

If the “Download over Air” feature is activated (see section [6.4.1.7](#)), the OMM acts as a download server that provides the firmware for downloads.

The DECT phone sends its firmware version within the DECT attachment procedure. If the firmware version does not match the version provided by the OMM, the DECT phone will be queued into the update-queue. Later on the queued DECT phones will be paged to establish a download connection. After the connection is established, the OMM sends its actual DECT phone firmware version and the DECT phone will request a DECT phone description file. After receiving the DECT phone description file, the DECT phone decides which files are missing or must be updated. If files are missing or must be updated the DECT phone initiates the download procedure.

The OMM takes care of the following download scenarios automatically:

- If a DECT phone becomes unreachable for example, when the DECT phone is switched off, the OMM will update the DECT phone when the DECT phone becomes available again.
- The OMM will take care of the software download while the user is moving between base stations (roaming) and location areas.
- The OMM has the capability of resuming a download from the point where it was last interrupted (for example, the user leaves the coverage area during download or the DECT phone runs out of battery power).
- The OMM updates new DECT phones subscribed to the system.
- While the DECT phone is barred (for example, low battery or “Download over Air” is disabled at the local menu), the download will be postponed.

The download happens without any user intervention. During the download, the telephony services, the roaming- and handover procedures are still available. The download stops automatically when e. g. the DECT phone leaves the coverage area or the RFP gets busy. The download resumes automatically when the stop cause is solved.

The Mitel 600/700 DECT phones have two partitions in the internal flash memory to hold 2 different software versions. During the download the new firmware is written to one partition and the DECT phone is running from the other partition.

After the download is successfully completed, the new firmware will be activated when the DECT phone is in the idle state.

The download of a single DECT phone with a firmware of 1 MB takes approximately 90 minutes. The number of DECT phones which can be downloaded depends on the available system resources.

The number of simultaneous downloads is limited per OMM (RFP: 30, PC: unlimited) and per RFP (6, decreased with each call).

The “Download over Air” service is delayed after a system startup for a while to allow the whole DECT system to become active. This may last several minutes.

9.21.2 HOW TO CONFIGURE “DOWNLOAD OVER AIR”

This section describes configuration of the “Download Over Air” feature via the OM Web service. The feature can also be configured using the OM Management Portal (OMP).

The “Download over Air” feature can be activated or deactivated on the **Support** web page (see section [6.4.1.7](#)).

In the OMP, you can enable the “Download over Air” feature in the **Support -> DECT phone’s firmware update** tab.

If the “Download over Air feature” is activated, the status of the **Activate firmware update** parameter is shown as enabled, service together with some statistics is displayed in the **DECT phones** section of the **Status** web page.

DECT Phones	
Users	2
Devices	2
Subscribed	2
Subscription allowed	✗
Activate firmware update	✓
Loading firmware from	internal
Firmware version	[650,602: 7.3.3] - [602v2: 7.4.5]

The DECT phone firmware container for DECT phone firmware update over the air includes packages for the Mitel 600/700 DECT phones. The available versions are also displayed on the **Status** web page.

Please note: The “Loading firmware from” on the OpenMobility Manager **Status** web page is only updated on restart of the OpenMobility Manager. Changing the location while the OpenMobility Manager is running has no effect.

The individual download status of each DECT phone is shown on the **SIP Users/Devices** web page.

SIP Users/Devices

OK Cancel

General

Base Stations: PARK 1F102F118A (31100570430504)

DECT authentication code: 35150

Subscription

Auto-create on subscription: ☒ Auto-create on subscription: ✓

Subscription: Off Subscription allowed: ✗

Wildcard subscription: 2 min

SIP User/Device

Create a new SIP User/Device: New

Import: Import

Search: Search

1 - 2 SIP Users/Devices

Display name	Number/SIP user name	IPEI	Subscribed	Download
Peter	4368	11041 0239039 9	✓	-
Georg	4369	12519 0000034 7	✓	-

The details in the **Download** column have the following meaning:

Icon	Meaning
-	Impossible to download the firmware to that DECT phone (for example, not a Mitel 600/700 DECT phone)
	The DECT phone is paged to establish a download connection. In case of a successful connection establishment the DECT phone calculates the number of bytes to download. This may take several seconds.
xx kbytes left	The download is ongoing and xx kbytes are left.
✓	The firmware of this DECT phone is up to date.
	The DECT phone is queued in the update-queue for updating (pending).
	Warning The download is barred because of one of the following reasons: – The DECT phone is busy (temporary status). – The battery power is lower than 50% and the DECT phone is not connected to the docking station or the USB interface. – This is not the master download system. A DECT phone can be enrolled on several OpenMobility systems. The first system to which the DECT phone will be enrolled is the “master system”. The DECT phone downloads only from the “master system”. A different “master system” can be chosen inside the local menu of the DECT phone. – The download is disabled in the local menu of the DECT phone. The specific reason is shown as a tooltip.

Icon	Meaning
	Error The download failed because of one of the following reasons: – checksum error, – file system error, – error while writing firmware to flash, – version mismatch, – error while expanding firmware container. The specific reason is shown as a tooltip.
	Info The download is not possible because: – the DECT phone is not reachable – the DECT phone is detached The specific reason is shown as a tooltip.

In the OMP, the “Download over Air” service status is displayed in the **Status** menu (see section [7.6](#)).

9.22 CENTRAL DECT PHONE CONFIGURATION OVER AIR (COA)

Centralized DECT phone configuration over the air is supported for Mitel 602 DECT phones. Configurable parameters include:

- settings (loudness, contrast, etc)
- menu items (switch on or off, enable password protection)
- key assignments (including an override of manual key programming)
- variable lists

DECT phone configuration over air (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 DECT phone profiles make it easy to adapt to different usage scenarios for heterogeneous user groups (for example, nurses and doctors in hospital environments).

IMPORTANT : This feature requires 6.00 DECT phone software or later.

IMPORTANT : Centralized DECT phone configuration over the air is only available on the Download over Air (DoA) master system.

9.22.1 CONFIGURATION FILES

You can use three kinds of configuration files:

- Default DECT phone configuration profile

Default configuration file used for all suitable DECT phones. The configuration is loaded into the DECT phone when subscription is complete, even if a user has not logged in to the device.

- DECT phone configuration profiles

User-focused DECT phone configuration file used for a group of users. The configuration is loaded into the DECT phone when a user belonging to this group logs in to the device.

- DECT phone user individual configuration settings

Individual DECT phone configuration settings used for a single user. The configuration is loaded into the DECT phone when the user logs in to the device.

The system consolidates the DECT phone settings before loading the configuration settings for a logged-in user into the DECT phone. Settings from DECT phone profiles overwrite default configuration settings, and individual user configuration settings overwrite DECT phone profiles and default configuration settings. For a complete list of supported settings, see section [13.5](#).

Configuration can be completed by using OMP (file import and download configuration settings) and user configuration files (user_common.cfg and <user.cfg files), wherein a list of user friendly settings can be used for the DECT phone configuration.

Please note: Deleting or overwriting configuration files on a DECT phone does not restore configuration to default or previous settings. Configuration elements that are not part of the new downloaded configuration file persist. To restore all settings, the administrator must initiate a power off/on at the DECT phone or use a default configuration file that contains all relevant settings.

To avoid interfering with the telephony or message service (especially with respect to alarm messages within the SIP-DECT system), only one configuration data download to the DECT phone is performed at a time. Therefore, changing the default profile settings or other profile settings may take some time in a large system, until all the related DECT phones are updated.

9.22.2 CONFIGURATION FILE DOWNLOAD TO DECT PHONES

Profiles are downloaded to the DECT phone via the messaging mechanism, in conjunction with the internal message type “CONF_OVER_AIR”. This occurs in parallel with general message transfer to the DECT phone, and the lowest priority is used to ensure that the download does not interfere with the delivery of urgent messages. The message mechanism is also used to confirm a successful profile download, through AXI events.

Profile downloads to DECT phones are limited system-wide to a maximum of one download at a time to ensure no interference with OMM system operation. You can view the download on the OMM console (console command `hcm`). The download state is also part of the system dump.

9.22.2.1 Download Triggers

The OMM maintains a profile download list for all DECT phones that have configuration data to be set. These DECT phones are stored with the checksum of configuration data to be set. A DECT phone is included in this list when:

- the OMM system starts up and the associated DECT phone has configuration data to be set
- the associated DECT phone’s configuration data changes (this is communicated via AXI), such as:

- change in the default configuration profile
- change in the configuration profile for the user of the associated DECT phone
- change in the individual user configuration profile for the user using the associated DECT phone
- change in the configuration profile assigned to the user using the associated DECT phone

Profile downloads to the DECT phones (as maintained in the profile download list) are scheduled at regular intervals. A new download to DECT phones in the profile download list is scheduled when:

- a configuration change occurs on the DECT phone (via AXI notification)
- a location registration is received, and the checksum of the configuration data stored in the profile download list is different from the checksum sent in the location registration
- a download to a DECT phone completes

9.22.3 COA CONFIGURATION USING OMP

OMP configuration of DECT phones is restricted. You can do the following through OMP:

- List the current user and device state via the **DECT Phones -> Overview** menu and **DECT Phones -> Devices -> Configuration data** tab (in Monitoring mode)
- Import the default profile and one to 20 individual profiles via the **System features -> COA profiles** menu (see section [7.13.9](#))
- Assign one of 20 profiles to an internal user via the **DECT Phones -> Users -> Configuration data** tab (see section [7.11.4.10](#))

The syntax of the profiles that can be imported by the OMP is the same as that specified for the user_common.cfg and <user>.cfg files.

Please note: CoA configuration via OMM Web service is not supported. You can only list the current user and DECT phone state in the “User and DECT phone configuration and status data summary”.

9.22.4 CONFIGURATION USING USR_COMMON.CFG/<USER>/CFG FILES

The user_common.cfg and <user>.cfg configuration files are used for DECT phone configuration. The following configuration attributes in the user_common.cfg file control central DECT phone configuration:

- Default profile settings

```
OM_Profile.0.Default.<key>=<values>
...
OM_Profile.0.Default.<key>=<values>
```

Where “Default” is the reserved name for the default profile, and <key> is one of the configuration settings with its <values> to be set.

Example:

```
OM_Profile.0.Default.UD_DisLang="en"
OM_Profile.0.Default.UD_DisFont="large"
```



```
OM_Profile.0.Default.UD_DispColor="black"
```

- one of up to 20 profile settings

```
OM_Profile.<no>.<name>.<key>=<values>
```

```
...
```

```
OM_Profile.<no>.<name>.<key>=<values>
```

Where <no> is the number of the profile, <name> is the name of the profile to be configured, and <key> is one of the configuration settings with its <values> to be set.

Example:

```
OM_Profile.5.Doctor.UD_Displang="en"
OM_Profile.5. Doctor.UD_DispFont="large"
OM_Profile.5. Doctor .UD_DispColor="black"
```

Please note: To assign a profile to a user, you can use the UD_PpProfileId= <profileNo> setting in <user>.cfg files. When <profileNo> is 0, no profile or (depending on configuration) the default profile is used. The default profile is defined in user_common.cfg.

Please note: A complete removal of a profile from user_common.cfg does not remove the profile in the OMM database. It must be explicitly deleted in the OMM database.

For individual user DECT phone configuration settings, the following configuration attributes are available in the <user>.cfg file:

- User configuration settings

```
<key>=<values>
```

```
...
```

```
<key>=<values>
```

Where <key> is one of the configuration settings with its <values> to be set.

Example:

```
UD_Displang="en"
UD_DispFont="large"
UD_DispColor="black"
```

9.22.4.1 CoA Example

```
UD_ConfigurationName = "omm-test"
UD_Displang="en"
UD_DispFont="small"
UD_DispColor="black"
UD_RingerMelodyIntern="ringing_1"
UD_RingerMelodyExtern="ringing_2"
UD_RingerVolumeIntern="increasing"
UD_RingerVolumeExtern="increasing"
```

Configuration file is named "omm-test"
 Language is set to English
 Display font is set to small
 Display color scheme is set to black
 Internal call melody is set to melody "ringing_1"
 Internal call melody is set to melody "ringing_2"
 Internal call ringer volume is set to increasing
 External call ringer volume is set to increasing

See *SIP-DECT CoA Programming Reference Manual* for a full list of supported CoA configuration parameters.

9.22.5 VARIABLE LISTS

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.

A list item consists of an index identifier (1..15) and either a number (to be dialed) or a function/feature that is supported by the DECT phone. Other attributes are optional. If there is a FunctionID, the entry does not have a sub key line in the variable list. If there is a number and a FunctionID the DECT phone executes the associated action (if available); otherwise, the DECT phone dials the number.

Item Attribute	Type	Description	Example
Index	Decimal number	Index of list item (1..15)	7
Number	quoted UTF8-string	Number to dial	"\x2312*777*" (use \x23 for # in configuration file)
Name	quoted UTF8-string	Text displayed for item	"My Voice Box"
FunctionID	Function-ID-string	Function or feature to execute	pbx_directory
ShortName/Icon	quoted UTF8-string	Short name and/or icon displayed	"\xEE808B VB"
Handsfree	Boolean ("1" or 0)	Dial in hands-free mode	1
VisibleSpecifier	4 digit string of "0" or "1"	Item visible in idle, dial, alerting and active state	1000

With Mitel DECT Phone Firmware 7.3.2, CoA profile supports 5 variable lists, each with up to 15 entries. The maximum file size for a CoA file is 4000 bytes. 5 times 15 entries already exceed the maximum size.

Example:

```
UD_ConfigurationName=VLIST TEST

UD_KeyAssignmentIdleMaster = long.d1 vlst1
...
UD_KeyAssignmentIdleMaster = long.d5 vlst5

UD_VListName = 1 "VL1" #Titel
UD_VListShortName = 1 "VL1" #Softkey
UD_VListSubItems = 1 0

...

UD_VListName = 5 "VL5" #Titel
UD_VListShortName = 5 "VL5" #Softkey
UD_VListSubItems = 5 0

UD_VListEntry = 1 1 "<inf=VL1 E_1><r=2000>" "VL1 E_1" "" "" ""
...

UD_VListEntry = 5 15 "<inf=VL5 E_15><r=2000>" "VL5 E_15" "" "" ""
```

Use the `UD_VListEntry` configuration command to configure an item for one of the lists. The first value specifies the index (1 -5) of the list, followed by the attributes listed above.

The values-attribute pairs must be separated by a space and their position in the configuration command are fixed. Unused attributes must be indicated by empty strings if they are followed by non-empty attributes. Unused attributes (empty strings) can be omitted at the end of the configuration command.

A variable list can hold a name and/or short name (used to represent it in another list or near a programmed soft key or side key). The 'short name' attribute also allows you to specify an icon. A third attribute, 'sub item', determines whether or not subitems (sub key lines) of a list are displayed. By default, the subitem (sub key line) is only displayed if the item is selected.

List Attribute	Type	Description	Example
Name	quoted UTF8-string	Text displayed for list	"My Own Menu"
ShortName/Icon	quoted UTF8-string	Short name and/or icon displayed	"\xEE808B M1"
SubItems	Boolean (0 or 1)	Show sub-key line of selected item	1

Examples:

```
#PBX Menu using COA variable list
```

```
UD_ConfigurationName=PBX Menu
```

```
#Key assignment (function: vlst1, vlst2)
```

```
UD_KeyAssignmentIdle=esc vlst1
```

```
#Menu Design
```

```
UD_VListName = 1 "Call services" #Titel
```

```
UD_VListShortName = 1 "More" #Softkey
```

```
UD_VListSubItems = 1 0 #Display Details per Item
```

```
### PLACEHOLDERS to add into Number field:
```

```
#<no> will be replaced with a number from handset editor for example, "*12*<no>#"
```

```
#<dial> will be replaced with a number from handset editor or directory, caller-list...
```

```
#<t=...> following dial-digits will be delayed for ... ms for example, <t=3000ms>
```

```
#<inf=...> set info-box with ... string for (3000ms) continue dialing after info box for example,
```

```
#<inf=Please wait>
```

```
#<r=...> call will be released after ... ms for example, <r=10000>
```

```
#<close> will close this Menu.
```

```
### Entry: UD_VListEntry = List Index "Number" "Name" FunctionID "ShortName" Handsfree  
# Visible
```

#ITEM	TYPE	DESCRIPTION
#List	decimal number	item belong to variable list (1..2)
#Index	decimal number	index of list item (1..10)
#Number	quoted UTF8-string	number to dial "*1234" (use \x23 for #)
#Name	quoted UTF8-string	displayed text of item "My Voice Box"

```

#FunctionID      function-ID-string      function/feature to execute for example,
pbx_directory
#                (if available, preference over number)
#ShortName       quoted UTF8-string      displayed short name and/or icon
#Handsfree       Boolean (0 or 1)         dial in hands-free-mode
#Visible         4-digit-string of 0 or 1 item visible in idle-, dial-, alerting- and
#                active-state for example,1000
#notice: to skip a parameter in the row use "" (even if the type is unquoted)

```

```

### idle menu functions

```

```

#Call Forward      **8 (predial) + number
#Call Forward Cancel ##8 (dial)
#Do Not Disturb    *5 (dial)
#Do Not Dist. Cancel #5 (dial)
#Call Pickup       *6 (dial)
#Call Park Retrieve *8# (predial) + number
#Direct/Group Page *37 (predial) + number
#Loudspeaker Page  **9 (dial)

```

```

UD_VListEntry = 1 1 ""*8<dial>\x23<inf=Call FWD enabled><r=2000>" "Call Forward" "" "" ""
UD_VListEntry = 1 2 "\x23\x238<inf=CallFWD off><r=1000><close>" "Call Forward Cancel" ""
"" ""
UD_VListEntry = 1 3 ""*5<inf=DND enabled><r=1000><close>" "Do Not Disturb" "" ""
UD_VListEntry = 1 4 "\x235<inf=DND off><r=1000><close>" "Do Not Dist. Cancel" "" ""
UD_VListEntry = 1 5 ""*6<close>" "Call Pickup" "" "" ""
UD_VListEntry = 1 6 ""*8\x23<dial>" "Call Park Retrieve" "" "" ""
UD_VListEntry = 1 7 ""*37<dial>" "Direct/Group Page" "" "" ""
UD_VListEntry = 1 8 ""*9<close>" "Loudspeaker Page" "" "" ""

```

9.22.5.1 Icon coding

The following table lists the UTF8-codes for Mitel 602 DECT phone icons.

ICON	UTF8-Code	Description
	\xEE8083	Arrow Up
	\xEE8084	Arrow Down
	\xEE8085	Arrow Left
	\xEE8086	Arrow Right
	\xEE8088	Fox Key
	\xEE80B0	Locked
	\xEE80BC	Search
	\xEE80BE	Info

ICON	UTF8-Code	Description
	\xEE81A5	Attention
	\xEE80BA	Tip
	\xEE808A	Telbook Private number
	\xEE808B	Telbook Mobile number
	\xEE808C	Telbook Business number
	\xEE818C	VIP number
	\xEE808D	Telbook Fax number
	\xEE808E	Telbook Email address
	\xEE808F	Telbook Name
	\xEE809B	Hook off / Predial
	\xEE809C	Hook on / Release
	\xEE81B0	Register recall
	\xEE8092	DTMF
	\xEE8182	3-party
	\xEE80A0	List Incoming call list
	\xEE80A1	List Outgoing call list
	\xEE8196	List Private directory /
	\xEE8199	List Central directory
	\xEE818C	List VIP
	\xEE8181	List Filter / Call Filtered
	\xEE80A1	Call outgoing
	\xEE8099	Call Waiting
	\xEE80A7	Call Rejected
	\xEE81AD	Call SOS
	\xEE809D	Call Headset autoanswer
	\xEE8098	Call Loudspeaker autoanswer
	\xEE809B	Call Hook autoanswer
	\xEE80B8	Call deflected
	\xEE80A3	Call missed
	\xEE80A4	Call answered
	\xEE8195	Call on Voicebox
	\xEE81AE	Call VIP
	\xEE81B1	Pickup

ICON	UTF8-Code	Description
	\xEE81B2	Pickup select
	\xEE8296	Call Park
	\xEE80BF	Call protection
	\xEE8298	Call routing
	\xEE8292	Callback

9.23 CALL DEFLECTION FOR INCOMING CALL IN RINGING STATE

In this, an incoming call can be deflected to another extension. In ringing state, “Deflect call” is offered in the option menu.

This option allows to enter the target extension to which the call gets deflected. The target can also be chosen from one of the directories or call logs.



The DECT phone returns to the idle state after confirming the target extension. Depending on the actual call log management of the call server platform, the deflected call is shown as an answered or missed call.

9.23.1.1 Number string coding

Note that the number specified in the list item may include one or more placeholders, so that, for example, the user can enter a number before the number is dialed. The placeholder keywords are specified in angle brackets ("< >").

If the dialed number includes angle brackets, you must use "<< >>".

Number Placeholder	Description
<no>	If the number strings consists of <no>, it is replaced with a number from the DECT phone editor
<dial>	If the number string consists of <dial> it is replaced with a number from the DECT phone editor or directory, caller-list. For example, "**12*<no>#" -> ok <edit-number> send cc-info"*12*"<edit-number>"# (numbers may include letters like abcd... if the system supports alpha dialing)

Number Placeholder	Description
<close>	All parents (e.g a list from which this item is started) are closed
<t=...>	Following dial-digits are delayed for ... ms for example, <t=3000ms>
<inf=...>	Set info-box with ... string for (3000ms) continue dialing after info box (for example, <inf=Please wait>)
<r=...>	Call is released after ... ms for example, <r=10000>

9.24 EXTENDED DECT PHONE INTERFACE

The Mitel 600/700 DECT phones include an **Administration** menu that offers administrative functions to the user such as login, logout, and configuration and status summary display. The menu is available as an option under the **System menu** which can be accessed via the main menu of the DECT phone, or directly by a long press of the right soft key.

The following table summarizes the options under the **Administration** menu. The menus allow basic OMM configuration and require a login (the same account and password as used for administrative access via OMP or Web service).

	Menu option	Description	OMM login
1.	Login	User can log in to the DECT phone (free DECT phone only)	
2.	Logout	User can log out of the DECT phone (free DECT phone only)	
3.	PP state	Display user/device configuration and status data summary (see section 6.7 for details)	
4.	Sync user data	Refresh SIP registration and synchronize user data, if they are stored externally	
5.	Sync system data	Reload configuration and resource files	Yes
6.	System credentials	Set authentication for provisioning servers (see section 9.8.6.1)	Conditional
7.	Status	Display basic OMM network settings (for example, DHCP, IP addresses)	
8.	System	Set basic OMM system data	Yes
9.	SIP users/devices	Perform basic configuration of users and DECT phones	Yes
10.	Version	Display current OMM software version	

The options available depend on the DECT phone state and the OMM platform (i.e., RFP OMM or Linux Server). The following table summarizes the options under the **Administration** menu according to device state and OMM platform.

	Menu option	Fixed device	Logged out	Logged in	RFP OMM	Linux Server OMM
1.	Login		√		√	√

2.	Logout			√	√	√
3.	PP state	√		√	√	√
4.	Sync user data	√		√	√	√
5.	Sync system data	√	√	√	√	√
6.	System credentials	√	√	√	√	√
7.	Status	√	√	√	√	
8.	System	√	√	√	√	√
9.	SIP users/devices	√	√	√	√	√
10.	Version	√	√	√	√	√

The following table summarizes the submenus available according to the OMM platform.

	Submenu	SIP-DECT	RFP OMM	Linux Server OMM
1.	System name	√	√	√
2.	Date and Time	√	√	
3.	SIP	√	√	√
4.	User administration	√	√	√
5.	Restart	√	√	√

9.25 USER MONITORING

To check the availability of a user in terms of the possibility to receive calls or messages, the OMM monitors the status of the user's DECT device.

9.25.1 OVERVIEW

With the "user monitoring" feature the following fixed set of status information is monitored:

Is a DECT phone assigned to the user?	Handset assignment status (HAS)
Is the DECT phone subscribed to the DECT system?	Handset subscription status (HSS)
Is the DECT phone currently registered /signed in?	Handset registration status (HRS)
Are there DECT phone activities within a specific timeframe?	Handset activity status (HCS)
Is the user registered at the SIP registrar?	SIP user registration status (SRS)

Is the DECT phone not in silent charging mode (silent charging option active and in the charger cradle)? Silent charging status (SCS)

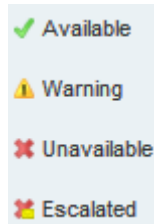
Is the feature “immediate call diversion” inactive? Call diversion status (CDS)

Is the battery charge higher than the configured threshold? Handset battery state (HBS)

Does the DECT phone have the minimum required software version? Software Status (SWS)

If all questions can be answered with “Yes” then the user status is set to “Available”. This set of status information is monitored if user monitoring is enabled for a user.

The status of all monitored users is displayed in the **DECT Phones -> User monitoring** menu (see also section [9.25.7.3](#)). The status information can have one of the following values:



The sum of all specific states is presented by the “Combined User Status”.

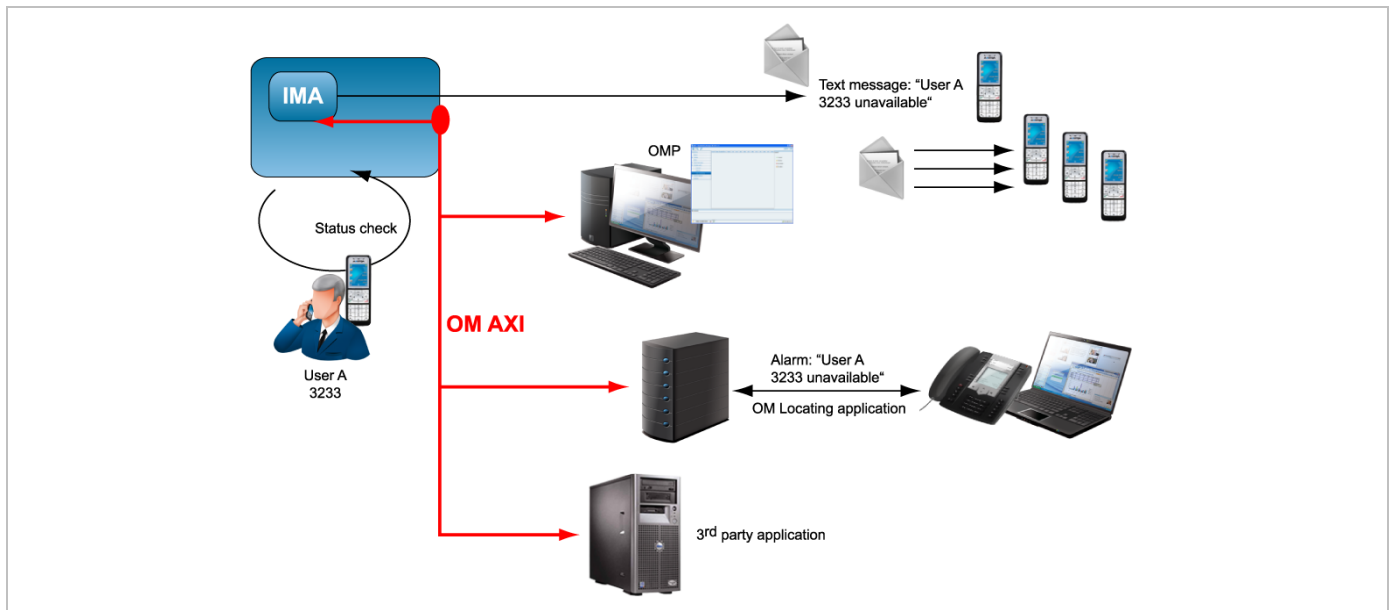
User ID	Name	Number	Rel. dev.	Mode	CUS	HAS	HSS	HRS	HCS	SRS	SCS	CDS	HBS	BTS	SWS
0x03D	Georg Wolf	2358	0x056	Passive	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓

If one of the states is set to unavailable, the resulting Combined User Status is set to unavailable as well.

0x00E	Lutz Püschel	2476	0x0E0	Passive	✗	✗						✓			

Because of dependencies between the states, some states cannot be determined if a higher level state is not fulfilled. For example, if the user has no DECT phone assigned, the DECT phone registration status cannot be determined. If a status cannot be determined, the status value is set to “Unknown” (empty in OMP).

The status information is available via OM AXI and OMP.



IMPORTANT : To address customer specific requirements, external applications (for example, 3rd party software) can provide an adapted functionality of the user monitoring or even more just by using OM AXI. This can be completed by the use of the XML terminal interface.

In addition to the standard request, response and notification messages, the OMM generates alarm triggers if a user becomes unavailable. If a user becomes available again, the OMM informs about this status change by sending an additional alarm trigger.

9.25.2 STATUS ATTRIBUTES AND VALIDATION MECHANISMS

The combined user status (CUS) is the sum of the specific status information.

The CUS is calculated based on the following rules:

- Specific states which are set to "Unknown" are ignored.
- CUS is set to "Available" if none of the specific states is set to "Warning", "Unavailable" or "Escalated".
- CUS is set to "Warning" if at least one of the specific states is set to "Warning" and none of the other states is set to "Unavailable" or "Escalated".
- CUS is set to "Unavailable" if at least one of the specific states is set to "Unavailable" and none of the other states is set to "Escalated".
- CUS is set to "Escalated" if at least one of the specific states is set to "Escalated".

The status "Unavailable" is changed to "Escalated" after the escalation timeout has elapsed and an alarm trigger has been generated.

9.25.2.1 Handset Assignment Status (HAS)

A DECT phone must be assigned to the user otherwise the status is "Unavailable".

Fixed user device relation

A DECT phone can be assigned permanently to a user (fixed user device relation). Then the status is always “available”.

Dynamic user device relation

A DECT phone can be dynamically assigned to a user (dynamic user device relation) and login and logout on a DECT phone is used.

If the user is logged out (unbound), the status is “Unavailable”. If the user is logged in (dynamic), the status is “available”. Login and logout also change the SIP registration.

Precondition: The user must exist in the OMM database.

9.25.2.2 Handset Subscription Status (HSS)

The DECT phone must be subscribed otherwise the status is “Unavailable”.

Precondition: A DECT phone must be assigned to the user.

9.25.2.3 Handset Registration Status (HRS)

The DECT phone must be attached / signed in (successful location registration) otherwise the status is “Unavailable”

The DECT phone may sent a detach message if it is switched off.

Precondition: A DECT phone must be assigned to the user (fixed, logged in) and the DECT phone is subscribed.

9.25.2.4 Handset Activity Status (HCS)

A communication over the air must occur regularly otherwise the status is “Unavailable”.

Passive monitoring

With every activity between DECT phone and the DECT system (for example, call setup) the activity information will be updated (last activity, current activity status). This indicates when the DECT phone was the last time able to communicate with the DECT system i.e. within the area of coverage, sufficient battery level, etc. There must be an activity within the timeframe defined by the Activity timeout 1 (min. 30 minutes, max. 1440 minutes).

Any activity between the DECT phone and the systems sets the status to “available”.

Active monitoring

Each DECT phone, that shall be monitored actively, will refresh its registration automatically within the “Activity timeout 2” (min. 5 minutes, max. 60 minutes). Each activity sets the status to “available”.

Active and passive monitoring

If the DECT phone was not active for the period of time defined by the activity timeout, the OMM automatically initiates an activity between the DECT phone and the DECT system to check the DECT connectivity. If this fails, the OMM sets the status to “Unavailable” but tries to connect to the DECT phone two times more within the next 2 minutes.

The OMM then continues to check the DECT connectivity base on the configured time frame. If the status is already “Unavailable”, the OMM does not verify the status by two additional tests within 2 minutes. If a check was successful, the status is set to “available”.

If a DECT phone could not be reached (for example, during call setup or messaging delivery), the OMM tries to connect to the DECT phone two times more within the next 2 minutes before the status is set to “Unavailable”.

Precondition: A DECT phone must be assigned to the user (fixed, logged in). The DECT phone is subscribed and attached (at least once).

9.25.2.5 SIP User Registration Status (SRS)

The user must be successfully registered at the configured SIP registrar otherwise the status is “Unavailable”.

A SIP registration is initiated automatically by the OMM during start-up if the user’s DECT phone was attached to the DECT system before restart/failover.

The SIP registration will not initiated automatically by the OMM during start-up if

- the user has no assigned DECT phone (fixed user device relation, login),
- the DECT phone is not subscribed or
- the DECT phone was detached (for example, switched off) before restart/failover.

A user will be deregistered if

- the DECT phone subscription is deleted/terminated,
- the user logs off from a DECT phone or
- the DECT phone is detached (for example, switch off).

Precondition: A DECT phone must be assigned to the user (fixed, logged in). The DECT phone is subscribed and attached (at least once).

9.25.2.6 Silent Charging Status (SCS)

If silent charging is enabled and the DECT phone is put into the charger, the DECT phone is in silent charging mode and does not indicate incoming calls with an audible signal. The DECT phone must not be in silent charging mode otherwise the status is “Unavailable”.

Precondition: A DECT phone must be assigned to the user (fixed, logged in). The DECT phone is subscribed and attached/signed in to the DECT system.

9.25.2.7 Call Diversion Status (CDS)

The user has no immediate call diversion (unconditional call forwarding) configured otherwise the status is “Unavailable”.

If the user has configured a call diversion for “No answer” / “Busy no answer” with a forward time ‘0’, this will be handled by user monitoring like unconditional call forwarding.

Precondition: The user must exist in the OMM database. The SIP supplementary service “Call forwarding / Diversion” is enabled in the OMM (see [6.4.3.5](#) and [7.7.4.7](#)).

9.25.2.8 Handset Battery Status (HBS)

The battery level of the DECT phone must be greater than the configured threshold value; otherwise the status is set to “Warning”.

Precondition: A DECT phone must be assigned to the user (fixed, logged in). The DECT phone is subscribed and attached. Delivery of battery level is supported.¹

9.25.2.9 Software Status (SWS)

The DECT phone software must provide the minimum of required features which could be controlled by the current OMM version. Therefore the appropriate minimum DECT phone software version is hard coded in the OMM and validated by user monitoring. The status will be set to “Warning” if the DECT phone software version is less than the hard coded value of the OMM.

Delivery of the software version is supported only by Mitel 600/700 devices.

Precondition: A DECT phone must be assigned to the user (fixed, logged in). The DECT phone is subscribed and attached.²

9.25.3 ESCALATION

If the OMM detects the unavailability of a user (marked as “unavailable”), this will be escalated only once by submitting a warning alarm trigger via OM AXI.

If the OMM detects finally the unavailability of a user (marked as “unavailable/escalated”), this will be escalated only once by submitting an alarm trigger via OM AXI.

The user must become available again before the unavailability of a user will be escalated the next time.

9.25.4 ALARM TRIGGERS

- The “UMON-WARNING-USERSTATE” alarm trigger is used to escalate the detection of the unavailability.
- The alarm triggers “UMON-ERROR-USERSTATE” and “LOC-ERROR-USERSTATE” are used to escalate the final detection of the unavailability.
- The “UMON-OK-USERSTATE” alarm trigger is sent by the OMM if a user becomes available again.

These are static, predefined alarm triggers like “SOS” and “MANDOWN” which do not have a telephone number to call.

The alarm triggers “UMON-WARN-USERSTATE”, “UMON-ERR-USERSTATE” and “LOCERR-USERSTATE” provide information about the cause why the user became unavailable (one or more of status attribute IDs: HAS, HSS, HRS, HCS, SRS, SCS, CDS, ...).

9.25.5 LICENSING AND SYSTEM CAPACITIES

The “User monitoring” feature does not require a specific license.

The number of monitored users is limited, as follows:

¹ The Mitel 600/700 DECT phone family provides battery status information if the DECT phones are updated to the current software version.

² The Mitel 600/700 DECT phone family provides software version information if the DECT phones are updated to the current software version.

RFP OMM

- Passive monitored users: 30
- Active monitored users: 20

PC OMM

- Passive monitored users: 300
- Active monitored users: 200

An OMM system health state will be set if the number of monitored users exceeds the system capabilities. In this case also an associated health state alarm trigger will be generated.

9.25.6 CONFIGURATION

User monitoring can be administered via the OMP.

9.25.6.1 “Settings -> Advance Settings -> User Monitoring” Menu

The following parameters can be configured on system level.

- **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%).

9.25.6.2 “DECT Phones” Menu

The following parameter can be configured on user level.

Monitoring mode: The user monitoring mode can be set to **Off**, **Passive** or **Active**. **Off** disables user monitoring. **Passive** and **Active** enable user monitoring and control the mode of the DECT phone activity status supervision. Default setting is **Off**.

If user monitoring is activated, the **VIP** option in the **DECT Phones -> Users -> SIP** tab for the user will be set automatically (see [7.11.4.3](#)). The **VIP** option will not be reset if the user monitoring mode is set to “Off”.

9.25.6.3 “DECT Phones -> User monitoring” Menu

The status of all monitored users is presented by the OMM in the **DECT Phones -> User monitoring** menu.

9.25.6.4 User Configuration Files

The parameter “UD_UserMonitoring” controls the monitoring for a user. The parameter can be set to “Off”, “Passive”, or “Active”.

9.25.6.5 OM IMA Application

If messages shall be sent out by the OM IMA application, the administrator must configure appropriate alarm scenarios for the alarm triggers in the OM IMA configuration file:

- UMON-OK-USERSTATE
- UMON-WARN-USERSTATE
- UMON-ERR-USERSTATE

9.25.7 START AND FAILOVER

The availability status is set to “Unknown” at start-up.

The monitoring feature does not escalate any user status during start-up until a configurable delay of min. 2 minutes and max. 15 minutes has elapsed.

The start-up delay should be adjusted according to the system start-up. The system start-up depends on the actual physical configuration, infrastructure components and parameter settings.

The statistic counter “Sync RFP start-up time” and “Sync Cluster start-up time” help to find an appropriate value for the start-up delay.

As soon as the start-up delay has elapsed, the status attributes are checked and the availability status will be determined. If the result is “Unavailable”, the status will be escalated.

The SIP registration process runs independently from the user monitoring start-up and infrastructure start-up. Monitored users as well as other users, who have the VIP flag set, are registered first.

9.25.8 SUPPORTED DECT PHONES

The Mitel 600/700 DECT phone family is fully supported.¹

The following states are managed independent of the DECT phone type:

- Handset assignment status (HAS)
- Handset subscription status (HSS)
- Handset registration status (HRS)
- Handset activity status (HCS)7F7F2

¹ The DECT phones must be equipped with the software version that corresponds to the SIP-DECT release. Otherwise, functionality may be limited.

² GAP devices do not support the active monitoring.

- SIP user registration status (SRS)
- Call diversion status (CDS)

Notes on Mitel 142d

The Mitel 142d DECT phones are supported by SIP-DECT and have an enhanced feature set compared to GAP DECT phones. For Mitel 142d the availability status is always set to “Warning” because of the limited feature set.

User ID	Name	Number	Rel. devi...	Mode	CUS	HAS	HSS	HRS	HCS	SRS	SCS	CDS	HBS	BTS	SWS
0x001	142d	3000	0x001	Active	⚠	✓	✓	✓	✓	✓		✓			⚠

The following states are not supported:

- Handset battery state (HBS)
always set to “Unknown”
- Software Status (SWS)
always set to “Warning” to indicate the limited feature set
- Silent charging state (SCS)
always “Unknown”

If the DECT phone is put into silent charging mode then it sends a “Detach”, like it is switched off.

Comments on GAP DECT phones

GAP DECT phones are supported by SIP-DECT with a basic feature set. The availability status is always set to “Warning” because of the limited feature set.

User ID	Name	Number	Rel. devi...	Mode	CUS	HAS	HSS	HRS	HCS	SRS	SCS	CDS	HBS	BTS	SWS
0x001	GAP	3000	0x001	Passive	⚠	✓	✓	✓	✓	✓		✓			⚠

The following states are not supported:

- Handset battery state (HBS)
always “Unknown”
- Software Status (SWS)
always set to “Warning” to indicate the limited feature set
- Silent charging state (SCS)
always “Unknown”

GAP DECT phones do not support the active monitoring (Handset activity status /HCS). In general, there is no guarantee for the correct interworking of the 3rd party DECT phone with SIP-DECT.

9.25.9 RESTRICTIONS

The described mechanisms check the status information in the OMM. Therefore the solution has certain limitations.

The OMM determines the availability of the DECT device which does not necessarily represents the availability of the user.

- It is not possible to determine whether a user actually carries his device with or not.
- The check of the availability does not include the infrastructure to which the OMM is connected (for example, call manager, etc.). A user appears as available even if the call manager fails.

- Feature (especially call diversion) when managed by the call server can undermine the monitoring.
- If a user is removed from the OMM, the monitoring stops without escalation. It cannot be checked if the user belongs to an alarm scenario configured in the alarm server or any other application scenario.

9.26 SRTP

Together with the new 3rd or 4th generation RFPs, SIP-DECT supports SRTP to encrypt the RTP voice streams and SDES for the SRTP key exchange.

There are three options for SRTP:

- **SRTP only:** Only SRTP calls will be accepted, all other will be rejected (the audio part of the SDP contains RTP/SAVP).
- **SRTP preferred:** All calls will be initiated as secured, but accepted if they are not secured (the audio part of the SDP contain RTP/AVP).
- **SRTP disabled:** Only RTP calls will be initiated as not ciphered and incoming ciphering algorithm will be not accepted. All communications are established unencrypted.

SIP-DECT provides the cipher suite AES_CM_128_HMAC_SHA1_32 and AES_CM_128_HMAC_SHA1_80.

SRTP calls from DECT phones with DECT handover require that the SRTP functionality must be homogenously available on all effected RFPs. Whereby, SRTP can only be activated on sites with only 3rd or 4th generation RFPs included.

IMPORTANT : A handover of an SRTP call to a site with disabled SRTP will drop the call.

IMPORTANT : SDES specifies as key exchange method the negotiation over SDP included in the SIP signaling. Therefore, we recommend to use TLS to encrypt the key exchange.

IMPORTANT : Please enable “SRTP = only” mode exclusively when all communication can be established with SRTP. Depending on the call server some features or gateways may not offer SRTP.

9.27 SIP OVER TLS

The transport protocol modes “TLS” or “Persistent TLS” enable a private and authenticated signaling, including safe key exchange for SRTP encryption.

The transport protocol and all further security settings can be set via the OMP **System -> SIP-> Security** tab and the OMM **System -> SIP-> Certificate Server** tab.

The following parameters can be set:

9.27.1.1 General

- **Transport protocol:** The protocol used by the OMM to send/receive SIP signaling. Default is “UDP”.
- **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, in seconds, between keep-alive messages sent out by the OMM. 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”.
- **Validate Certificates:** 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”.
- **Validate hostname:** 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.

9.27.1.2 PEM file import

- Allows the manual import of Trusted, Local Certificates and a Private Key in PEM file format.

The following parameters can only be read and should ease the handling of certificates:

- **Trusted Certificates:** The number of imported trusted certificates.
- **Local Certificate chain:** The number of imported certificates in the local certificate chain.
- **Private Key:** Is a private key imported or not.

9.27.1.3 Certificate server

Optionally is also an automatic import of Trusted, Local Certificates and a Private Key files from an external server possible. This can be configured on the “Certificate Server” tab.

The following parameters allow an automatic import:

- **Active:** Enable or disable the automatic import.
- **Protocol:** Selects the preferred protocol (FTP, TFTP, FTPS, HTTP, HTTPS, SFTP)
- **Server:** IP address or name of the server
- **User Name / Password / Password confirmation:** The server account data if necessary.
- **Path:** The path on the server to certificate files.
- **Trusted certificate file:** The name of the PEM file on the given server including the trusted certificates.
- **Local certificate file:** The name of the PEM file on the given server including the local certificate or a certificate chain.
- **Private key file:** The name of the PEM file on the given server including the local key.

9.27.2 CERTIFICATES

The use of “TLS” or “Persistent TLS” requires the import of certificates to become operational.

Item	When Needed	Setting
Trusted Certificates	For TLS and Persistent TLS	A PEM file with a list of all (self-signed) CA certificates needed to verify remote certificates. May also contain trusted intermediate certificates instead of or in addition to self-signed certificates In many cases there is only one certificate in this list: The self-signed certificate which is used by the SIP proxy and registrar or which was used to sign that certificate.
Local Certificate	For TLS: Always	A PEM file with the OMM's certificate chain
Private Key	For Persistent TLS: Only if the server verifies the client certificate	A PEM file with the OMM's private key

All certificates and keys must be provided as X.509 certificates in PEM file format. They must use the RSA algorithm for their keys and signatures and MD5 or SHA-1 for their hashes.

Although PEM files usually contain a textual description of the certificate, only the Base64-encoded portions between

```
-----BEGIN CERTIFICATE-----
```

and

```
-----END CERTIFICATE-----
```

are actually evaluated. However, the files can be uploaded to the OMM with their full content.

There are two sets of certificates which can be set up in the OMM, which are described in the following sections.

Trusted Certificates

The trusted certificates are used to verify the signatures of certificates sent by remote hosts. The corresponding PEM file may contain multiple certificates. Their order is not relevant. Certificates are searched in the trust store according their subject name, the key identifier (if present), and the serial number as taken from the certificate to be verified.

Local Certificates

The local certificate or local certificate chain is sent to remote hosts for authentication.

In corresponding PEM files the host certificate must be in the first position, followed by intermediate certificates if applicable. The last certificate is the self-signed root-certificate of the CA. The root certificate may be omitted from the list, as the remote host must possess it anyway to verify the validity. This means that if there are no intermediate certificates, this file may contain only one single certificate.

9.27.3 PRIVATE KEY

The Private Key is also contained in a PEM file. The *Local Certificate* must match to the *Private Key*. Although PEM files may contain a textual description of the key, only the Base64-encoded portions between

```
-----BEGIN RSA PRIVATE KEY-----
```

and

```
-----END RSA PRIVATE KEY-----
```

is actually evaluated. However, the file can be uploaded to the OMM with its full content.

9.27.4 TLS TRANSPORT MODE

The OMM distinguishes the both TLS transport modes **TLS** and **Persistent TLS**.

When the OMM is configured to use **TLS** (Transport protocol: TLS), TLS connections to remote peers, for example, SIP proxies and registrars, are connected as needed. For TLS connections initiated by the OMM, it is a TLS client. If a remote peer sets up a TLS connection, the OMM is the TLS server. Connections are closed when they have not been in use for a certain time. The terms *server* and *client* refer to TLS connections below, not to SIP transactions.

The OMM always verifies the server certificate when it sets up an outgoing connection and it verifies the client certificate on incoming connections. Therefore following configuration parameters must be set for this mode: *Trusted Certificates*, *Local Certificate* and *Private Key*.

When the OMM is configured to use **persistent TLS** (Transport protocol: Persistent TLS), it sets up TLS connections to SIP Servers and keeps them connected. When a connection is closed for whatever reason, the OMM tries to re-establish it immediately. It does not accept incoming connections from remote ends. Thus the OMM is always TLS client when Persistent TLS is in use.

The advantage of Persistent TLS is a faster call setup time and lower processing power needed on both sides.

The OMM always verifies the server certificate, therefore following configuration parameters must be set for this mode: *Trusted Certificates*

If the server verifies the client certificate, additionally *Local Certificate* and *Private Key* must be set.

9.27.5 VERIFICATION OF REMOTE CERTIFICATES

When "TLS authentication" is "ON", a remote certificate is verified by the OMM as follows:

The signature of the certificate is checked with the public key of the signing certificate. The certificate chain is checked until a *Trusted Certificate* is found. If self-signed certificate is found which is not trusted, the verification fails.

The current time must be in the validity period of the certificate. For this mechanism a correct system time must be provided (for example, NTP).

If one or more of these checks fail, the TLS connection will be closed.

Please note: All certificates are only valid for a limited time given by the issuer. As soon as the validity is expired no further communication is possible. The certificates must be replaced before to prevent a breakdown of call services.

When “TLS authentication” is “OFF”, the OMM verifies the remote certificates and logs any failure but the established TLS connection will not be closed in case of verification failures.

IMPORTANT : To prevent man-in-the-middle attacks we recommend not to disable the “TLS authentication” in unsecure environments. We recommend setting “TLS authentication” and “TLS common name validation” to “ON” in any unsecure environments for the best security.

9.27.6 ADDITIONAL SECURITY CONSIDERATIONS

For highest security requirements there are additional considerations to be taken into account when enrolling an OpenMobility system.

To prevent manipulations during the initial upload of certificates and keys to the OMM completely, this should be done in a small private network without a physical connection to an insecure network.

IMPORTANT : To prevent manipulation of certificates and keys in unsecure environments we recommend not to use the automatic import of certificates and keys. Especially the unsecure protocols TFTP, FTP and HTTP must be avoided. It is also recommended to protect the selected protocol with a login to prevent unauthorized access to the private key file.

Furthermore, it is important that the root and administrator passwords of the OpenMobility system are safe, because with these passwords an attacker could change the configuration to manipulate the system in various ways.

Although all keys and certificates in the database are encrypted, an automated database backup or download could be a security leak if the network, transport protocol or servers used are not protected against manipulations.

9.28 DECT ENHANCED SECURITY

Security aspects in the DECT standard have been improved after concerns were raised in the market in recent years. Therefore various enhancements have been introduced.

The usage of many security features, which were already available in the DECT standard (respectively GAP) from the beginning, was left optional for the devices. Almost each of these functionalities 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 procedure brings additional guarantee on security and is an integral part of the SIP-DECT solution. The feature set can be enabled or disabled per site. This distinction is necessary due to the fact, that enhanced security is available with RFPs 35/36/37/43/44/45/48 only.

From release 5.0 on, when DECT enhanced security is enabled, every connection will be encrypted, not only voice calls, but also such as service calls (for example, 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 together with Mitel 602 DECT phones. Older terminals (for example, 6x0d or 142d) or GAP phones will still operate as ever, but not provide the new security mechanisms.

9.29 MIGRATION OF RFP SL35 IP FROM SIP-DECT LITE 3.1 TO SIP-DECT 6.1

The SIP-DECT Lite solution realized a single-cell DECT network that offered only limited radio coverage and was operated with one RFP SL35 IP. The SIP-DECT Lite solution was part of the SIP-DECT product family that offered larger radio coverage by realizing multi-cell DECT networks with up to 256 RFPs.

You can integrate the RFP SL35 IP to a multi-cell SIP-DECT network. The migration from SIP-DECT Lite to the current release of the standard SIP-DECT system is supported. During the migration the SIP-DECT Lite software is replaced by the standard SIP-DECT software on the RFP SL35 IP and a reset to the factory setting is performed. All configuration data are removed from the base station.

The following migration process must be performed.

Precondition: Unique UNLOCK.xml file is available for the specific RFP SL35 IP.

- 1 Remove the USB flash memory from the RFP SL35 IP and plug it into your computer.
- 2 Copy the unlock.xml file onto the USB flash memory.
- 3 Copy the standard SIP-DECT SW (iprfp3G.dnld) onto the USB flash memory of the RFP.
- 4 Check if the following files are on the USB flash memory (no other files should be on the USB flash memory except SIP-DECT™ Lite DB backup field “omm_conf.txt” which is not relevant).
 - a. PARK.xml
 - b. UNLOCK.xml
 - c. iprfp3G.dnld
- 5 Remove the USB flash memory from your computer and plug into the RFP SL35 IP.
- 6 The migration process starts automatically after plugging the USB flash memory into the RFP.
- 7 Wait for the RFP reboot and start-up. Do not interrupt the electric power during this process.
- 8 The SW update for RFPs in standard SIP-DECT installations are provided by other means than to copy the SW on the USB flash memory. Therefore the iprfp3G.dnld must be removed from the USB flash memory.

Make sure that the PARK.xml and UNLOCK.xml remain on the USB flash memory.
- 9 Also after the migration, make sure that the USB flash memory is always plugged in the RFP.
- 10 Now, the RFP SL35 IP has the standard SIP-DECT SW and the UNLOCK.xml file and can be operated in standard SIP-DECT installations. Please follow the standard procedures to setup a SIP-DECT installation.

9.30 802.1X CERTIFICATE BASED AUTHENTICATION

You can assign a group certificate to all RFPs of a SIP-DECT installation for certificate based authentication to open the switch ports the RFPs are connected to.

The screenshot shows the Mitel configuration interface. The top navigation bar includes the Mitel logo, a settings icon, a search icon, and a pencil icon. The right side of the bar has links for 'General' and 'Help'. The left sidebar lists various configuration categories: Configuration, Status, System (with sub-items like Basic settings, Advanced settings, SIP, Provisioning, User administration, Data management), Sites, DECT base stations, WLAN, DECT phones, Conference rooms, System features, Licenses, and Support. The main content area is titled '802.1X' and contains several sections: 'Certificates/key' with 'Trusted certificate(s)' and 'Local certificate chain' both set to '0', and a 'Private key' field with a delete icon; 'PEM file import' with a radio button for 'Trusted certificate' and a file upload area; 'Private key password' with 'Password' and 'Password confirmation' fields; and 'General' with 'Client identity' and 'Use bridge interface' fields. At the bottom are 'OK', 'Cancel', and 'Start edit' buttons.

9.30.1 802.1X CONFIGURATION

You can import trusted certificates, a local certificate chain and a private key file for 802.1x certificate based authentication manually through OMP or OMM configuration files.

9.30.1.1 Configure and store 802.1x certificate settings

- 802.1x certificate data are optional parameters. 802.1x certificate based authentication works only if valid certificate data is configured and the feature is set to enabled.
- 802.1x certificate data is stored centrally in OMM database and can be set by OMP, through an OMM provisioning file or from a certificate server.
- The centrally stored 802.1x certificate data remains valid until it is changed or removed by one of the configuration sources.
- The stored 802.1x certificate data is used after a reset/reboot/power cycle even if the provisioning server is not reachable.
- RFPs receive the encrypted 802.1x certificate data from OMM via a HTTP file request, for example, after reboot or after notification of new certificate data from the OMM. Only RFPs can decrypt and use the certificate data.
- The 802.1x certificate data will be stored locally on RFPs.

9.30.1.2 Configure and store 802.1x certificate server settings

- 802.1x certificate server settings are optional parameters. If configured, the OMM uses the configured file server to load/update the 802.1x certificate data (group certificate, private key, Trusted (CA) certificate(s))
- 802.1x certificate server settings are stored centrally in OMM database and can be set by OMP or via an OMM provisioning file.

9.30.1.3 Discard OMM DB or RFP factory reset, which are offered as restart options

- The 802.1x certificate data and the 802.1x certificate server settings on the (RFP-) OMM are lost.
- The 802.1x certificate data and the 802.1x certificate server settings have to be configured again; otherwise, the RFPs receive empty 802.1x certificate data on the next 802.1x update.
- To delete 802.1x certificate data from a RFP, the data can be deleted on the OMM (applies to connected RFPs), or a factory reset of an RFP can be initiated (OM-Configurator or through an prepared USB stick).

9.30.2 PREREQUISITES REFERRING TO 802.1X TOPOLOGY

802.1x group certificate based authentication runs in networks, which fulfill needs of a proper running 802.1x administration:

- Radius server
- Switch port configuration
- Closed mode (initial 802.1x configuration in safe environment) or low-impact mode (DHCP, DNS, NTP, TFTP, HTTP (for the transfer of the 802.1x configuration to the RFPs)) enabled. HTTP traffic between the OMM and RFPs in different VLAN (guest VLAN for unauthorized clients) needs to be routed by a layer 3 switch or router so authorized RFPs can receive their 802.1x configuration or guest VLAN (DHCP, DNS, NTP, TFTP - HTTPS to OMM needs to be routed). Traffic between different VLANs (including the native VLAN) is routed by a layer 3 switch or router. Even a proper routing between native VLAN and SDC VLAN is mandatory or guest VLAN (DHCP, DNS, NTP, TFTP - HTTPS to OMM needs to be routed)
- Full access to productive network after successful 802.1x authentication

9.30.3 802.1X FEATURE DESCRIPTION

- All RFPs of an installation needs to get updated to a firmware which supports 802.1x (either in a secure environment or on a switch port in low-impact mode or in a guest VLAN where access to DHCP and TFTP is possible).
- Initial 802.1x certificate request from OMM needs to be enabled on the RFP through local configuration (OM-Configurator parameter independent from local configuration flag) or a DHCP option (option 43 suboption + unused DHCP option) to prevent impact on existing installations. If 802.1x certificates are already loaded to an RFP, updates are requested independent from this local or DHCP configuration.
- OMM supports the configuration of 802.1x group certificate data or alternatively the configuration of a certificate server for automatic update of the certificates from a file server.
- For the group certificate, a unique 802.1x identity for all RFPs is supported.
- To enable 802.1x on RFP each of them is initialized by DHCP option or OM_Configurator. Otherwise the feature is inactive for a RFP (see [9.32](#)).

- RFPs request RSA encrypted 802.1x certificate data through HTTP from the active OMM (either in a secure environment or on a switch port in low-impact mode or in a guest VLAN where access to DHCP and to the OMM via HTTP is possible).
- Certificate data is requested/updated, for example on RFP startup or after a certificate update has been triggered by the OMM.
- In addition to the certificate data, a RFP receives and applies the admin and root login credentials (user name and password hash). Thereby access to the RFP root file system is no longer possible with the default password of previously unconfigured RFPs.
- The certificate data is stored reset proof in the RFPs.
- If an 802.1x certificate data file was received from the OMM, RFP admin and root login credentials cannot be changed through the IPL protocol between OMM and RFP (for example, by connecting to a different OMM system > factory reset required).
- You can delete 802.1x certificate data from the OMM. Afterwards, the data is deleted from connected RFPs.
- New edit mode in OMP for 802.1x certificate settings to prevent inconsistent configuration (changed settings will not be used before leaving the edit mode).
- New DECT base station attribute 802.1x configuration mismatch for the device list in OMP monitoring mode.
- New health states for 802.1x are supported. A warning message appears while the 802.1x edit mode is active and shows mismatch errors if certificates cannot be updated from the 802.1x certificate server or if not all RFPs have the correct certificate checksum (certificate mismatch).

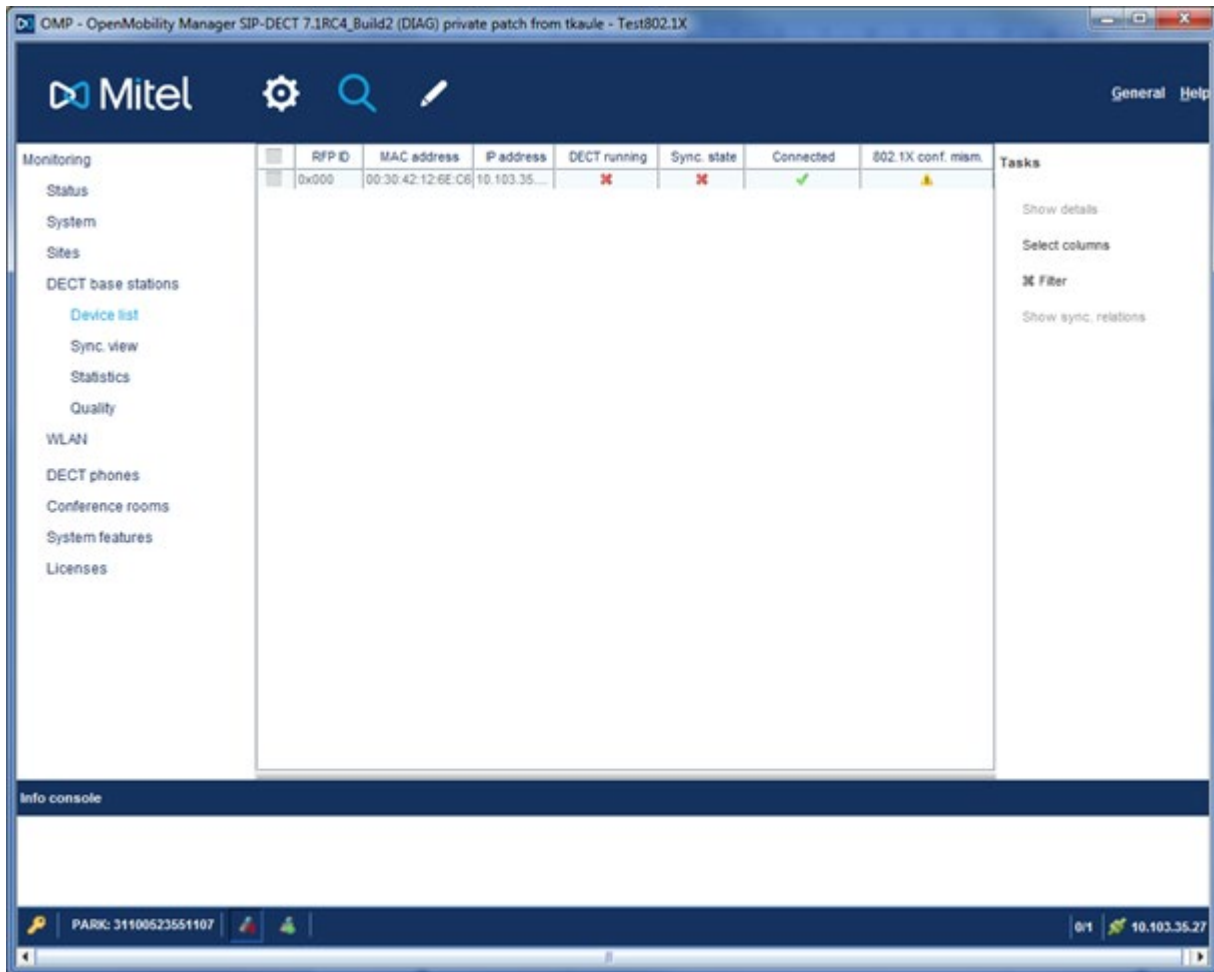
The screenshot displays the Mitel OMM web interface. The top navigation bar includes the Mitel logo, a settings icon, a search icon, and a 'General Help' link. Below the navigation bar, there are tabs for 'Overview', 'DECT base stations', 'Users', 'Devices', 'Sites', 'Conference', 'Provisioning', and 'Provisioning health report'. The 'Overview' tab is selected, showing a 'System' section with various status indicators and a 'Features' section with a list of services and their health status.

System	Status
Uptime	108 Day(s) 00 h 29 min
Licenses	✓
Standby OMM	✗
Synchronization state	✓
DECT base stations	✓
DB import/export	✓
Downloading new firmware to portable parts	✓
Provisioning	✓
OMM configuration file processing	✓
Emergency location configuration	✓

Features	Status
OM Integrated Messaging & Alerting service	✓
User data server	✓
MOM control	✗
802.1x state	✗
OMM certificate server	✗
Provisioning certificate server	✗
802.1x certificate server	✗
SIP certificate server	✗

New health state for 802.1x

802.1x configuration mismatch in DECT base stations device list (OMP monitoring mode).



You can import trusted certificates, a local certificate chain and a private key file for 802.1x certificate based authentication manually through OMP or OMM configuration files.

- **Certificates/key:** Shows the number of active 802.1x trusted certificates, the number of 802.1x local certificate chains and whether a 802.1x private key is used. All can be deleted with the Deletecertificates/key button.
- **PEM file import / Import PEM file with:** Specifies the type of file 802.1x (trusted certificate, local certificate, or private key) and the location of the file to be imported.
- **General/Client identity:** 802.1x supplicant client identity.
- **Private key password/ Password:** Specifies the password for the 802.1x private key file.

9.31 802.1X CERTIFICATE SERVER CONFIGURATION

Through configuration of a 802.1x certificate server URL, you can update the 802.1x certificate data automatically.

The screenshot shows the Mitel OMP - OpenMobility Manager SIP-DECT 8.1-EF23 - Connect web interface. The left sidebar contains a navigation menu with categories like Configuration, Status, System, Sites, DECT base stations, WLAN, DECT phones, Conference rooms, System features, and Licenses. The main content area displays the '802.1x certificate server' configuration page. At the top, there are tabs for various settings: User service, Pre-Login banner, User monitoring, Special branding, Core dump, Remote system dump, Net parameters, DECT phones, DECT phones firmware, DECT base stations, IMA, and Additional services. The '802.1x certificate server' tab is selected. The configuration form includes fields for:

- Active:** A checkbox to enable or disable the feature.
- Protocol:** A dropdown menu currently set to 'HTTPS'.
- Server:** A text input field for the server IP or name.
- Port:** A text input field with a 'Use default port' checkbox checked.
- User name:** A text input field for authentication.
- Password:** A masked text input field.
- Password confirmation:** A masked text input field for re-entering the password.
- Path without file name:** A text input field for the certificate path.
- Use common certificate configuration:** A checkbox.
- Trusted certificates file:** A text input field.
- Local certificate chain file:** A text input field.
- Private key file:** A text input field.

 At the bottom of the form are 'OK' and 'Cancel' buttons. The bottom of the interface shows an 'Info console' bar.

Configuration of the 802.1x certificate server using OMP.

- **User name:** Specifies the user name for authentication against the certificate server.
- **Password:** Specifies the password for authentication against the certificate server.
- **Active:** Enables or disables the certificate server URL feature.
- **Protocol:** Specifies the protocol to be used to fetch the certificate files. One of FTP / HTTPS / SFTP / HTTP / HTTPS / TFTP / None.
- **Port:** Specifies the certificate server's port number or use of the default port for the used protocol.
- **Server:** Specifies the IP address or name of the certificate server.
- **Path without the filename:** Specifies the path to the certificate files on the certificate server.
- **Use Provisioning security configuration:** Enables the use of the system-wide certificate validation settings for this URL, as configured on the **System -> Provisioning and Software Update -> Security** page (see section [6.4.2.14](#)).

- **Trusted certificates file:** Filename of the trusted certificates to read from the server.
- **Local certificate chain file:** Filename of the local certificates to read from the server.
- **Private key file:** Filename of the private key to read from the server.

9.32 INITIATE 802.1X BY DHCP OPTIONS OR OM_CONFIGURATOR

Before 802.1x starts the feature, it has to be initialized by DHCP or by the OM_Configurator tool.

9.32.1 DHCP OPTIONS

There are two ways, either DHCP option 226 or the vendor specific option 43 (code 226) can be used.

DHCP option 226	set this option to 1	the option is optional

Vendor specific option 43	set code 226 to 1	code 226 is optional

9.32.2 OM_CONFIGURATOR

Select the parameter *Activate 802.1x* and set it to true. If `.CSV` config files are used, set the common value `use_802_1x=1`.

10 MAINTENANCE

10.1 SITE SURVEY MEASUREMENT EQUIPMENT

If a SIP-DECT installation must be planned, a sufficient distribution of DECT base stations that meets the requirements for reliable synchronization and connectivity to the DECT phones is necessary. The site survey kit may help you. It comprises:

- One measuring RFP with its own power supply.
- A tripod and a battery for the RFP.
- Two reference DECT phones with chargers.
- Battery chargers.
- Optional a measuring DECT phone which can monitor other makers DECT radio sources.

10.2 CHECKING THE MITEL HANDSET FIRMWARE VERSION

You can display the version information of a Mitel 600/700 or Mitel 142d DECT phone with a few keystrokes. Check the firmware version to determine whether an update is required to overcome any user issues.

- 1 Press the **Menu** soft key.
- 2 Select **System** (only to highlight).
- 3 Press **OK**.
- 4 Select **Version Info**.
- 5 Press **OK**.

The display shows the software and the hardware version of the Mitel DECT phone.

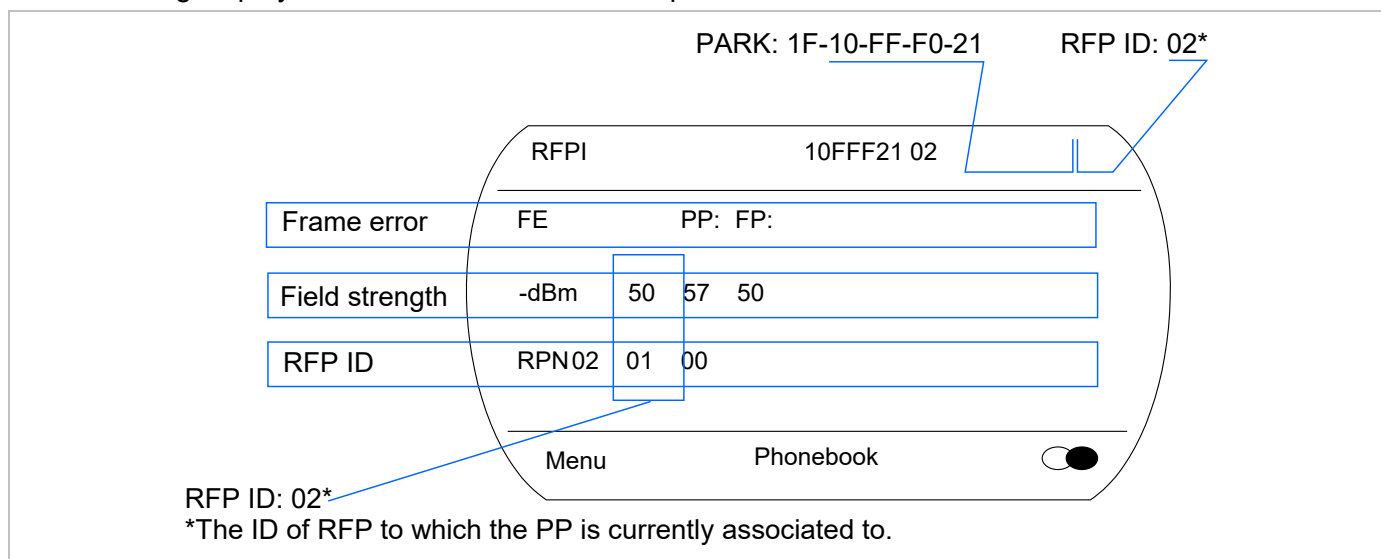
10.3 DIAGNOSTIC

10.3.1 MITEL DECT PHONE SITE SURVEY MODE

You can switch a Mitel 600/700 or Mitel 142d DECT phones into “site survey mode” with a few keystrokes. In this mode the phone will display the RFPs and the actual field strength of the receiving signal in dBm.

- 1 Press the **Menu** soft key.
- 2 Enter the following key sequence “***76#” (Mitel 600/700) or “R***76#” (Mitel 142d).
- 3 Select Site Survey.
- 4 Press OK.
- 5 To leave the site survey mode, switch the phone off and on again.

The following display is shown on the Mitel DECT phone:



In this example the DECT phone is currently connected to the RFP with the number 02. The RFPs 01 and 00 are also visible. The number “10FFF21 02” on the upper right side refers to the PARK (Example 1F-10-F2-21) of the SIP-DECT system and to the RFP to which the phone is currently connected to.

10.3.2 MITEL HANDSET AUTO CALL TEST MODE

You can switch a Mitel 600/700 or Mitel 142d DECT phones into “auto call test mode” with a few keystrokes. In this mode the phone will call a specified number cyclically. You can use this feature to generate traffic for test purposes. This mode is also active if the phone is on the charger.

- 1 Press the **Menu** soft key.
- 2 Enter the following key sequence “***76#” (Mitel 600/700) or “R***76#” (Mitel 142d).
- 3 Select Auto Call Test.
- 4 Press OK.
- 5 Enter the phone number to call.
- 6 Press OK.
- 7 Enter a number of seconds between two calls.
- 8 Press OK.
- 9 Enter a number of seconds a call shall be active.
- 10 Press OK. The test will be started automatically.
- 11 To stop the test, switch the phone off and on again.

10.3.3 MITEL HANDSET AUTO ANSWER TEST MODE

You can switch a Mitel 600/700 or Mitel 142d DECT phone into “auto answer test mode” with a few keystrokes. In this mode, the phone answers incoming calls automatically. You can use this feature

together with phones in the “auto call test mode” (see the above section [10.3.2](#)) for test purposes. This mode is also active if the phone is on the charger.

- 1 Press the **Menu** soft key.
- 2 Enter the following key sequence “***76#” (Mitel 600/700) or “R***76#” (Mitel 142d).
- 3 Select Auto Answer.
- 4 Press OK.
- 5 Enter a number of seconds the phone shall ring before it will answer the call.
- 6 Press OK.
- 7 Enter a number of seconds a call shall be active.
- 8 Press OK. The test will be started automatically.
- 9 To stop the test, switch the phone off and on again.

10.3.4 SYSLOG

The OpenMobility Manager and the RFPs are capable of propagating Syslog messages conforming to RFC 3164 (see /13/). This feature together with the IP address of a host collecting these messages can be configured.

Syslog must be enabled by:

- DHCP using the suboption 14 and 15 of vendor option 43.
- Setting the syslog daemon server and port via the web interface.

To set up the syslog via DHCP or the OM Configurator has the advantage that syslogs are available in earlier states of the RFP startup.

Date	Time	Priority	Hostname	Message
11-16-2006	18:18:56	User.Warning	172.30.206.122	OMM: 0000029970 *** IPL: RFP 00:30:42:0C:BE:AF not configured
11-16-2006	18:18:56	User.Warning	172.30.206.122	OMM: 0000029955 *** IPL: RFP 00:30:42:0C:BE:B2 not configured
11-16-2006	18:18:56	User.Warning	172.30.206.122	OMM: 0000029955 *** IPL: RFP 00:30:42:0C:BE:A2 not configured
11-16-2006	18:18:49	Daemon.Info	172.30.206.41	/opt/ntp.ntpd[411]: peer 131.188.3.220 now valid
11-16-2006	18:18:44	User.Warning	172.30.206.122	OMM: 0000017265 *** CNF: license state changed to ACTIVE LICENSE
11-16-2006	18:18:44	Syslog.Info	172.30.206.121	syslogd: received HUP signal
11-16-2006	18:18:44	User.Warning	172.30.206.122	OMM: 0000017255 *** CNF: license state changed to HURT LICENSE
11-16-2006	18:18:44	User.Notice	172.30.206.122	OMM: 0000017240 ** KI: RFP(01): Connection Established
11-16-2006	18:18:44	User.Emerg	172.30.206.121	RFP: 0000015775 ***** MAIN: UP & RUNNING (0.1.0)
11-16-2006	18:18:44	Syslog.Info	172.30.206.120	syslogd: received HUP signal
11-16-2006	18:18:44	User.Emerg	172.30.206.120	RFP: 0000015765 ***** MAIN: UP & RUNNING (0.1.0)
11-16-2006	18:18:44	User.Notice	172.30.206.122	OMM: 0000017225 ** KI: RFP(00): Connection Established
11-16-2006	18:18:43	User.Emerg	172.30.206.121	RFP: 0000015300 ***** BMC: HW capabilities info: 0x000001DC
11-16-2006	18:18:43	User.Emerg	172.30.206.120	RFP: 0000015300 ***** BMC: HW capabilities info: 0x000001DC
11-16-2006	18:18:40	Syslog.Info	172.30.206.122	syslogd: received HUP signal
11-16-2006	18:18:40	User.Emerg	172.30.206.122	RFP: 0000015950 ***** MAIN: UP & RUNNING (0.1.0)
11-16-2006	18:18:40	User.Notice	172.30.206.122	OMM: 0000013625 ** KI: RFP(02): Connection Established
11-16-2006	18:18:40	User.Emerg	172.30.206.122	RFP: 0000015490 ***** BMC: HW capabilities info: 0x000001DC
11-16-2006	18:18:28	User.Emerg	172.30.206.121	RFP: 0000000020 ***** MAIN: starting application
11-16-2006	18:18:28	User.Emerg	172.30.206.120	RFP: 0000000020 ***** MAIN: starting application
11-16-2006	18:18:28	User.Emerg	172.30.206.121	syslog: 0000000000 ***** ALL: hw_rftype = HW_RFP32
11-16-2006	18:18:28	User.Emerg	172.30.206.120	syslog: 0000000000 ***** ALL: hw_rftype = HW_RFP32
11-16-2006	18:18:27	User.Emerg	172.30.206.122	OMM: 0000000130 ***** WEBS: webs: Listening for HTTP requests at address

The level of syslog messages in the default state allows the user to have control over the general system state and major failures.

10.3.5 SSH USER SHELL

Each RFP offers a lot of commands within the SSH shell. Most of them are useful for diagnostics and may help experts to resolve failures.

Note: Some commands can harm the system operation.

The SSH access of an RFP is open if

- the RFP is connected to an OMM and the “Remote Access” is switched on or
- the RFP is not connected to an OMM.

To activate the SSH access of an RFP that has a connection to an OMM, enable the **Remote access** checkbox on the OMM **System settings** web page (see section [6.4.1.1](#)). In the OMP, the SSH access is activated/deactivated in the **General** tab of the **System -> Basic settings** menu (see section [7.7.1](#)).

10.3.5.1 Login

To log into the SSH user shell:

- 1 Open an SSH session to the IP DECT base station with the “Full access” user name.
- 2 Enter the password for the “Full access” account (see also [9.16.1](#)).

The output should look like:

```
Welcome to IP RFP OpenMobility SIP Only Version 2.1.x

last reset cause: hardware reset (Power-on reset)

omm@172.30.206.94's password:
omm@172.30.206.94 >
```

10.3.5.2 SSH Connection to RFP

Run the following command to establish ssh connections to other RFPs:

```
dropbearmulti ssh omm@<IP address of other RFP>
```

10.3.5.3 Command Overview

Type `help` to get a command overview:

Command	Description
exit,quit,bye	Leave session
ommconsole	OMM console
ip_rfpconsole	RFP console
rfpm_console	RFP manager console
wlan_console	WLAN console
ics_console	ICS console
ldb	View / set local configuration (OmConfigurator)
setconsole	Duplicate messages to console
noconsole	Do not duplicate messages to console
dmesg	Messages from last boot
logread	Last messages
su	Switch to user root
ping	Well known ping
traceroute	Well known traceroute
free	Well known free
ps	Well known ps
top	Well known top
ifconfig	Well known ifconfig
uptime	Well known uptime
reboot	Well known reboot
date	Well known date (time in UTC)

10.3.5.4 OMM Console On Linux Server

You can call the OMM console on the Linux server which runs the OMM using the “ommconsole” command. Log on as root as it is necessary to install and/or update OMM.

IMPORTANT : If you not login as root to open the OMM console then the path to ommconsole is not set and you must enter the whole path “/usr/sbin/ommconsole” to start the OMM console.

10.3.5.5 RFP Console Commands

If you type `ip_rfpconsole` you are able to use the following commands on each RFP:

Command	Description
?	Displays Command Help Table
bt	Bluetooth commands
confmix	Displays status of conference mixer

Command	Description
help	Displays Command Help Table
logger	Send a string to the syslog daemon
deftrc	Resets all trace settings to default
runtime	Reports the process runtime
mem	Show memory and heap
exit	Leave this console
heap	Shows heap buffer statistics
heapcheck	Verifies the guard space of all via dross allocated buffer. Heap functions are locked during check
heapdetails	Print detailed heap usage
jpeg	Jpeg helper commands
lu10	Lu10 SDU <-> PDU converter
mclose	Close a media channel
mconf	Configure IP settings for a media channel
media	Display state of media channels
mopen	Open a media channel
mroute	Display media routes
mstart	Start a media channel
mstop	Stop a media channel
mswo	Codec switch over for an active call
mtime	Display media time statistics
mutex	Lists all created MXP mutexes
omms	Shows connection status to OMM(s)
otpdbCheck	Check all OTP pages for valid elements
queues	Lists all created MXP queues
reset	Resets the IPRFP application
resume	Resume bmc activity
sem	Lists all created MXP semaphores
signals	Print signal dwell time in queues
spy	Set/display spy levels: [<key #> <level #>]
suspend	Suspend bmc activity
tasks	Lists all running MXP tasks
tickres	Print tick resolution
timer	Print running timer

Please note: The “spy” command enables you to increase the level of syslog messages. This should be only used by instructions of the support organization because it can harm the system operation.

10.3.5.6 OMM Console Commands

If you have opened the session on the OMM RFP and you type “ommconsole”, you are able to use the following OpenMobility Manager (OMM) related commands:

Command	Description
?	Displays Command Help Table
adb	Automatic DB export and import (ADB) console
axi	AXI commands
axic	Task console for AXI command processing of provisioning files
cert	Certificate import console
cmi	CMI commands
cnf	Show configuration parameters
cron	Display pending cron jobs
help	Displays Command Help Table
logger	Send a string to the syslog daemon
deftrc	Resets all trace settings to default
dlc	DECT Data Link Control
dm	Download Over Air Manager
dsip	DSIP commands
epr	External provisioning task (EPR) console and dynamic users console
runtime	Report the process runtime
mem	Show memory and heap
exit	Leave this console
gmi	DECTnet2 Inter Working Unit
hcm	Handset configuration management task (HCM) console
heartbeat	Configure heartbeat mechanism for IP-RFPs
ima	IMA commands
inspect	Display information of a user
ipc	Display socket communication
ipl	Display connected RFPs
iplfilter	Configure which RFPs spy messages are generated for
lic	LIC commands
loc	Info about locating extension

Command	Description
mon	Toggle monitor functionality
msm	Display states within MediaStreamManagement
msmtrc	Display / modify list of traced DECT phoneNs
mutex	List all created MXP mutexes
nwk	DECT network layer
prov	Prov-related commands
queues	List all created MXP queues
rcmd	Remote command on RFPs shell
rfp	Radio Fixed Part Control
rfpd	Radio Fixed Part Debug
rfps	Radio Fixed Part Statistic
rping	Request one or more RFPs to ping a host
rspy	Remote configure spy levels on IP-RFPs
rsx	Toggle RSX debug port on RFPs
rtt	Set event flag for high RTT values / clear values
sem	List all created MXP semaphores
spy	Set/display spy levels: [<key #> <level #>]
standby	Displays redundant OMMs
stat	Statistic
sync	Commands for RFP synchronization
sysdump	Initiate system dump
tasks	List all running MXP tasks
tickres	Print tick resolution
trc	Back trace task
tzone	Time zone commands
uds	UDS commands
umo	UMO commands
upd	Display update status of RFPs
update	Force all connected RFPs to search for new software
uptime	Display OpenMobility Manager uptime
ver	Version information
wlan	Display states within Wireless LAN Management
xml	XML browser task (XML) console
xsc	XSC commands

Please note: The “spy” command enables you to increase the level of syslog messages especially for subsystems of the OMM. This should be only used by instructions of the support organization because it can harm the system operation.

10.3.6 CORE FILE CAPTURING

Fatal software problems may result in memory dumps, so called core files. These core files are helpful in analyzing the problem that caused the abnormal termination of the program. The IP RFP is capable of transferring the core files to a remote fileserver. Without any special configuration the files are transferred to the TFTP server that is used to get the system software. The path used is the directory of the boot image. These two configuration items are retrieved from DHCP or via local configuration using the OM Configurator.

You can configure the URL to a writable directory via the OMM (see section [6.4.1.14](#)) or through the “OM_CoreFileSrvUrl” variable in the ipdetect.cfg configuration files.

Please note: The server must allow writing new files (not typically enabled by default).

11 REGULATORY COMPLIANCE AND SAFETY INFORMATION (4TH GENERATION DECT BASE STATIONS)

For regulatory and basic installation guidelines necessary for the proper and safe functioning of this equipment, refer to the Safety Instructions (document part number **5701204601RA**) packaged with the system and posted on the eDocs web site (<http://edocs.mitel.com/>).

Read and follow all information contained in the Safety Instructions document before attempting to install or use Mitel products. Only trained, qualified service personnel shall install or maintain Mitel products.

12 SAFETY INFORMATION (3RD GENERATION DECT BASE STATIONS)

12.1 CE MARKING

This certifies the conformity of the product placed on the market prior to June 13th 2017 with the regulations which apply in accordance with the RTTE Directive 1999/5/EC.

For a copy of the original signed declaration (in full conformance with EN45014), contact the Regulatory Approvals Manager at Mitel Networks Ltd., Castlegate Business Park, Portskewett, Monmouthshire, NP26 5Yr, United Kingdom, or visit <http://www.mitel.com/regulatory-declarations>.

On or after June 13th 2017 hereby, Mitel Networks declares that the product is in compliance with Directive 2014/53/EU. The full text of the EU declaration of conformity is available at the following internet address: <http://www.mitel.com/regulatory-declarations>.

12.2 COMMUNICATIONS REGULATION INFORMATION

The regulation information in this section applies to the following supported DECT base stations:

- RFP 35 IP
- RFP 36 IP
- RFP 37 DRC

12.2.1 FCC NOTICES (U.S. ONLY)

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Modifications not expressly approved by this company could void the user's authority to operate the equipment.

NOTE: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

12.3 HEALTH AND SAFETY

12.3.1 EXPOSURE TO RADIO FREQUENCY (RF) SIGNALS:

The wireless phone is a radio transmitter and receiver. It is designed and manufactured not to exceed the emission limits for exposure to radio frequency (RF) energy set by the Federal Communications Commission (FCC) of the U.S. Government. These limits are part of comprehensive guidelines and establish permitted levels of RF energy for the general population. The guidelines are based on the safety standards previously set by both U.S. and international standards bodies. These standards include a substantial safety margin designed to assure the safety of all persons, regardless of age and health.

This device and its antenna must not be co-located or operating in conjunction with any other antenna or transmitter.

The radiating element of the RFP should be installed during operating at a separation distance greater than 20 cm between user and device. The device complies with the requirements for routine evaluation limits.

12.3.2 INDUSTRY CANADA (CANADA ONLY)

Operation of this device is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.

Privacy of communications may not be ensured when using this telephone.

Exposure to Radio Frequency (RF) Signals:

The wireless phone is a radio transmitter and receiver. It is designed and manufactured not to exceed the emission limit for exposure to radio frequency (RF) energy set by the Ministry of Health (Canada), Safety Code 6. These limits are part of comprehensive guidelines and established permitted levels of RF energy for the general population. These guidelines are based on the safety standards previously set by international standard bodies. These standards include a substantial safety margin designed to assure the safety of all persons, regardless of age and health.

This device and its antenna must not be co-located or operating in conjunction with any other antenna or transmitter.

The radiating element of the RFP should be installed during operating at a separation distance greater than 20 cm between user and device. This device complies with the requirements for routine evaluation limits.

12.4 INFORMATIONS RÉGLEMENTAIRES EN MATIÈRE DE COMMUNICATIONS

Les informations dans cette section concerne les suivantes stations radio :

- RFP 35 IP
- RFP 36 IP
- RFP 37 DRC

12.4.1 NOTES FCC (USA UNIQUEMENT)

Cet appareil est conforme à la partie 15 des règles FCC. Son exploitation est soumise aux deux conditions suivantes: (1) Cet appareil ne doit causer aucune interférence dommageable et (2) cet appareil doit tolérer toute interférence reçue à l'inclusion des interférences susceptibles de causer une opération non désirée. Les modifications non expressément agréées par cette entreprise pourraient rendre caduque l'habilitation de l'utilisateur à exploiter cet équipement.

NOTA: Cet équipement a été testé et jugé conforme aux limitations pour un appareil numérique de classe B en vertu de la partie 15 des règles FCC. Ces limitations ont été conçues pour garantir une protection raisonnable contre les interférences dommageables dans les installations résidentielles. Cet équipement génère, utilise et peut rayonner des ondes radio et peut causer des interférences dommageables dans les communications par radio s'il n'est pas installé et utilisé conformément aux instructions. Cependant, l'absence d'interférences dans une installation particulière n'est pas garantie. Si cet équipement perturbe de façon importante la réception de la radio ou de la télévision (interférences qui peuvent être déterminées en arrêtant et en remettant l'appareil en marche), l'utilisateur est invité à tenter de corriger les interférences en prenant une ou plusieurs des mesures suivantes:

- Réorienter ou déplacer l'antenne de réception.
- Éloigner l'équipement du récepteur.
- Raccorder l'équipement à une prise d'un circuit différent de celui auquel est raccordé le récepteur.
- Consulter le revendeur ou un technicien radio/TV.

13 APPENDIX

This Appendix contains additional information and examples for configuring your SIP-DECT system.

13.1 PRE-CONFIGURATION FILE RULES

The following file format description can be used to administrate the RFP and DECT phone configuration with external applications, for example, an external configuration management tool or a PBX communications system.

The framework of the text file follows strictly defined rules. The main framework is divided in two parts:

- 1 An **instruction section** is used to drive a generic data creation for those fields not filled within data sequence section.
- 2 A data sequence section defines data record fields. Each of them is explicitly set.

Layout rules in detail are:

- Comments start with “#”.
- Each record is terminated by the regular expressions “\r” or “\n”.
- Instruction settings are made like: <tag> = <value>.
- Data sequence sections start with the key word “data_sequence”. This key word is **mandatory** for file processing to proceed. All instructions must be written before this row.
- Data sequence record fields are separated by colon “;”. Colons have also to be set for empty fields if at least one follows which is not empty. Otherwise a position mismatch of fields will occur.
- If fields have several values assigned (that may be true for a few local RFP configuration fields like “ntp_address”), they must be separated by comma “,”.

Notes:

- Because data sequence fields are separated by a colon, the content of that section can be generated by a *.csv export of Excel Sheet and copied into the configuration file.
- Instructions are only processed on those fields that are left empty within the data sequence section.

13.2 RFP CONFIGURATION FILE / CENTRAL (OMM DATABASE)

You can import of DECT base station configurations using files via the OMP.

13.2.1.1 Supported Instructions

All instructions are taken as a common value and are applied to all records in the data sequence section of that file if the corresponding field is empty.

Instruction	Explanation
active	Activation of DECT: {'0' or 'false' = inactive, '1' or 'true' = active }
cluster	Cluster, the RFP is referred to - RFP-OMM: {1..256}, PC-OMM: {1..4096}
paging_area	Paging area, the RFP is referred to: {'unassigned', '0'..'127'} Ignored by WEB import and always set to '0' (Paging area 0)
sync_source	Synchronization source: {'0' or 'false' = inactive, '1' or 'true' = active }
refl_env	Reflective environment: {'0' or 'false' = no, '1' or 'true' = yes }
site	Site Id: {1..250}
wlan_profile	Reference key to an existing WLAN profile
wlan_antenna	Antenna settings: {0=diversity, 1, 2}
wlan_channel_bg	WLAN channel: {0..14 (size depends on regulatory domain) }
wlan_power	WLAN power: {6, 12, 25, 50,100 (in percent)}
wlan_act	Activation of WLAN: {'0' or 'false' = inactive, '1' or 'true' = active }

13.2.1.2 Data Section Fields

The data section contains the following field order:

- 1 MAC address
- 2 Name
- 3 DECT activated
- 4 DECT cluster
- 5 Paging area (always set to "0", PA0)
- 6 Preferred sync.
- 7 Reflective env.
- 8 Site ID (if left empty then set to the lowest Site ID)
- 9 Building (ignored by Web import and always set to "")
- 10 Floor (ignored by Web import and always set to "")
- 11 Room (ignored by Web import and always set to "")
- 12 WLAN profile
- 13 WLAN antenna
- 14 WLAN channel
- 15 WLAN power
- 16 WLAN activated

13.2.1.3 Example

The following figure shows the results of a DECT base station enrolment operation via the OMP **DECT base stations -> Enrolment** page.

Select RFP enrolment import file

File

/home/calange/Desktop/file.txt

Show log file

	MAC address	Name	DECT cluster	Paging area	Site ID	HW type	Status	
☐	00:30:42:0D:97:1A	R451P31a03054	1	0	1	Auto	✖	
☐	00:30:42:0D:95:D8	R439 SWT 31A-0-3-1-2	1	0	1	Auto	✖	
☐	00:30:42:0C:8D:78	R440 P31a-03-07-4	1	0	3	Auto	✖	
☐	00:30:42:0D:95:CE	Patchschrank Kueche	1	0	3	Auto	✖	
☐	00:30:42:0D:95:CC	R414 OpenMob lab	2	0	3	Auto	✖	
☐	00:30:42:0D:95:CA	R414 OpenMob lab	2	0	3	Auto	✖	
☐	00:30:42:0C:8D:DD	R403 System test lab	2	0	3	Auto	✖	
☐	00:30:42:0D:95:D8	R451 P31a-4-2-15-8	1	0	1	Auto	✖	
☐	00:30:42:0D:95:D9	R439 P31a-4-2-12-13	1	0	3	Auto	✖	
☐	00:30:42:0D:95:D6	R447 P31a-4-2-13-18	1	0	3	Auto	✖	
☐	00:30:42:0D:95:E7	R447 P31a-4-2-14-13	1	0	1	Auto	✖	
☐	00:30:42:0D:22:5A	R433 P31a-4-2-11-10	1	0	3	Auto	✖	
☐	00:30:42:0C:8D:68	R433 P31a-4-2-11-13	1	0	1	Auto	✖	
☐	00:30:42:08:92:FC	R443 Test board	1	0	1	Auto	✖	
☐	00:30:42:FF:F0:D0	plexiglas	1	0	1	Auto	✖	
☐	00:30:42:0D:27:7D	R434 P31M-0-1-5-19	1	0	3	Auto	✖	
☐	00:30:42:0A:C9:62	R439 Decke re.	1	0	1	Auto	✖	
☐	00:30:42:0D:E3:F6	R436 Wand oben In	1	0	1	Auto	✖	
☐	00:30:42:08:31:5F	R434 Decke In. Tür	1	0	1	Auto	✖	
☐	00:30:42:08:31:64	R440 Decke re Fnstr	1	0	1	Auto	✖	

Add all
 Add selected
 Remove all
 Remove selected
 Show status
 Select columns

RFP configuration file/central:

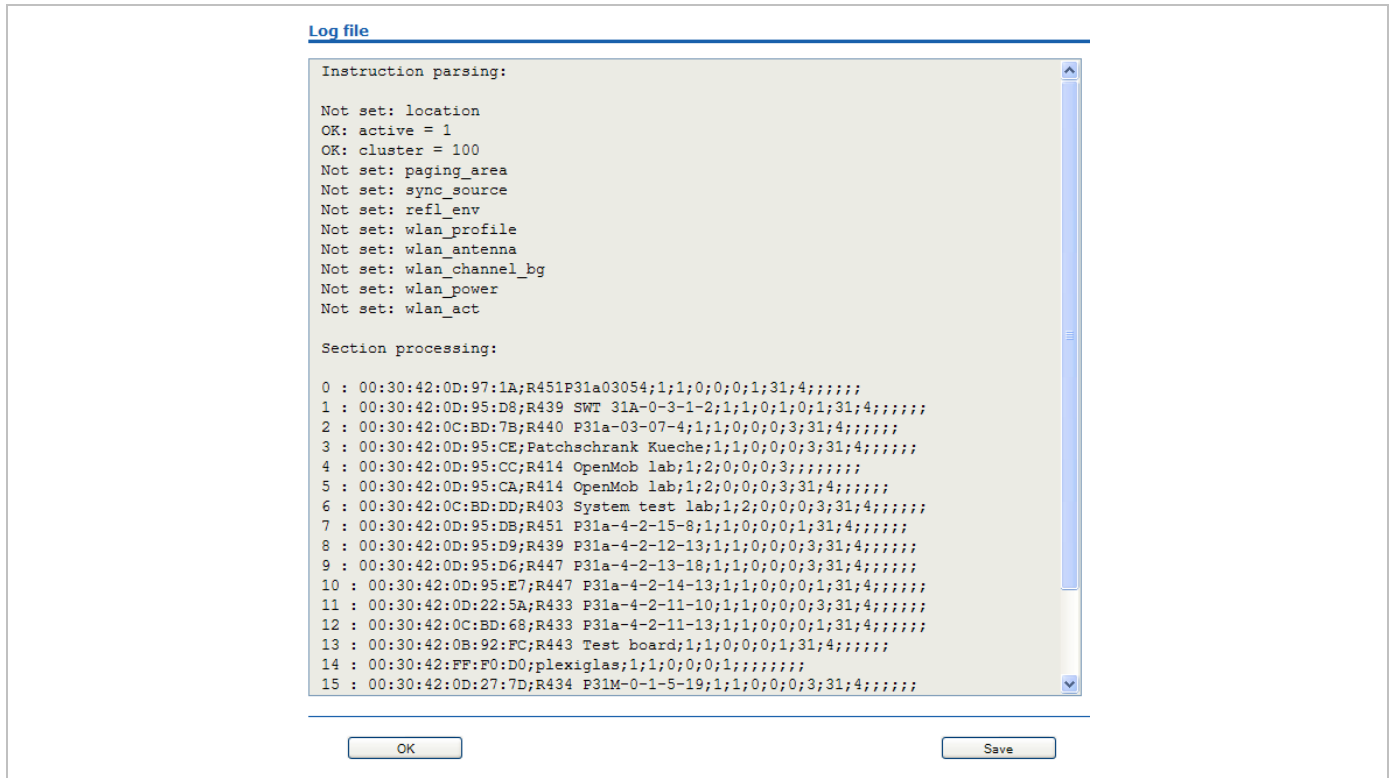
```
#####
# instruction section:
#####
#active
#
#           Activation of DECT:
#
#           {'0' or 'false '= inactive, '1' or 'true' = active}
#cluster
#
#           Cluster, the RFP is referred to:
#
#           {1..256} (RFP OMM) or {1..4096} (PC OMM)
#paging_area
#
#           Ignored by Web import and always set to "0" (PA0)
#
#           Paging area, the RFP is referred to: {'unassigned', '0'..'127'}
#sync_source
#
#           Synchronisation source:
#
#           '0' or 'false '= inactive, '1' or 'true' = active}
#refl_env
#
#           Reflective environment:
#
#           '0' or 'false '= no, '1' or 'true' = yes}
#site
#
#           Site Id: {1..250}
#wlan_profile
#
#           Reference key to an existing WLAN profile
#wlan_antenna
#
#           Antenna settings: {0=diversity, 1, 2}
#wlan_channel_bg
```

```
#           WLAN channel: {0..14 (size depends on regulatory domain) }
#wlan_power
#           WLAN power = { 6, 12, 25, 50,100 (in percent)}
#wlan_act
#           Activation of WLAN:
#           '0' or 'false '= inactive, '1' or 'true' = active}
#Note: Web import allows only "0" or "1" for Boolean
#####

active=1
cluster=100
refl_evc=1
site=1

#####
data_sequence
#####
#MAC address;Name;DECT activated;DECT cluster;Paging area;Preferred sync.;
#Reflective env.;Site ID;Building;Floor;Room;WLAN profile;WLAN antenna;
#WLAN channel;WLAN power;WLAN activated
00:30:42:0D:97:1A;R451P31a03054;1;1;0;0;0;1;31;4;;;
00:30:42:0D:95:D8;R439 SWT 31A-0-3-1-2;1;1;0;1;0;1;31;4;;;
00:30:42:0C:BD:7B;R440 P31a-03-07-4;1;1;0;0;0;3;31;4
00:30:42:0D:95:CE;Patcheschrank Kueche;1;1;0;0;0;3;31;4
00:30:42:0D:95:CC;R414 OpenMob lab;1;2;0;0;0;3;;
00:30:42:0D:95:CA;R414 OpenMob lab;1;2;0;0;0;3;31;4
00:30:42:0C:BD:DD;R403 System test lab;1;2;0;0;0;3;31;4
00:30:42:0D:95:DB;R451 P31a-4-2-15-8;1;1;0;0;0;1;31;4
00:30:42:0D:95:D9;R439 P31a-4-2-12-13;1;1;0;0;0;3;31;4
00:30:42:0D:95:D6;R447 P31a-4-2-13-18;1;1;0;0;0;3;31;4
00:30:42:0D:95:E7;R447 P31a-4-2-14-13;1;1;0;0;0;1;31;4
00:30:42:0D:22:5A;R433 P31a-4-2-11-10;1;1;0;0;0;3;31;4
00:30:42:0C:BD:68;R433 P31a-4-2-11-13;1;1;0;0;0;1;31;4
00:30:42:0B:92:FC;R443 Test board;1;1;0;0;0;1;31;4
00:30:42:FF:F0:D0;plexiglas;1;1;0;0;0;1;;
00:30:42:0D:27:7D;R434 P31M-0-1-5-19;1;1;0;0;0;3;31;4
00:30:42:0A:C9:62;R439 Decke re.;1;1;0;0;0;1;;
00:30:42:0D:E3:F6;R436 Wand oben ln;1;1;0;0;0;1;;
00:30:42:08:31:5F;R434 Decke ln. Tür;1;1;0;0;0;1
00:30:42:08:31:64;R440 Decke re Fnstr;1;1;0;0;0;1
```

Parse log about import / instruction processing



13.2.2 RFP CONFIGURATION FILE / LOCAL (OM CONFIGURATOR)

13.2.2.1 Supported Instructions

All instructions are taken as a common value and are applied to all records in the data sequence section of that file if the corresponding field is empty.

Instruction	Explanation
active	Local configuration active: {0=inactive(use DHCP instead), 1=active}
net_mask	Net mask
tftp_server	IP address of TFTP server
tftp_file	Path and name of boot file
omm_1	OMM IP address
omm_2	IP address of backup OMM
gateway	Default gateway
dns_server	Up to two DNS server IP addresses
dns_domain	local DNS domain
syslog_addr	IP address of syslog daemon
syslog_port	Listen port of syslog daemon
use_vlan	VLAN is enabled
broadcast_addr	local broadcast address
vlan_id	VLAN Id

Instruction	Explanation
config_file_server	configuration server

13.2.2.2 Data Section Fields

The data section contains the following field order:

- 1 MAC address of RFP
- 2 Local configuration active flag
- 3 IP address of RFP
- 4 Net mask
- 5 TFTP server
- 6 TFTP_FILE
- 7 OMM IP address
- 8 IP address of backup OMM
- 9 Default gateway
- 10 DNS server
- 11 DNS domain
- 12 Syslog daemon IP address
- 13 Syslog listen port
- 14 Use VLAN
- 15 Broadcast address
- 16 VLAN Id
- 17 Configuration file server

13.2.2.3 Example

RFP configuration file/local (OM Configurator):

```
# -----#
# instruction section #
# -----#

active      = 1
net_mask    = 255.255.0.0
tftp_server= 172.30.200.92
tftp_file   = iprfp2G.tftp
omm_1       = 172.30.111.188
omm_2       = 172.30.11.181
gateway     = 172.30.0.2
dns_server  = 172.30.0.4,172.30.0.21
dns_domain  = aastra.de
syslog_addr = 172.30.200.92
use_vlan    = 1
broadcast_addr = 172.30.255.255
```

```
vlan_id = 4
config_file_server = https://server/configfiles/

# -----#
# data sequence #
# -----#
# 1. MAC_ADDR          ! no instruction supported !
# 2. ACTIVE_FLAG
# 3. RFPADDR          ! no instruction supported !
# 4. NET_MASK
# 5. TFTP_SERVER
# 6. TFTP_FILE
# 7. OMM1
# 8. OMM2
# 9. GATEWAY
#10. DNS_SERVER
#11. DNS_DOMAIN
#12. SYSLOG_ADDR
#13. SYSLOG_PORT
#14. USE_VLAN
#15. BROADCAST_ADDR
#16. VLAN_ID
#17. CONFIG_FILE_SERVER

data_sequence
00-30-42-01-01-01;;172.30.111.1
00-30-42-02-02-02;;172.30.111.2
```

Parse log for import / instruction processing

```
ok: active = 1
ok: net_mask = 255.255.0.0
ok: tftp_server = 172.30.200.92
ok: tftp_file = iprfp2G.tftp
ok: omm_1 = 172.30.111.188
ok: omm_2 = 172.30.11.181
ok: gateway = 172.30.0.2
ok: dns_server = 172.30.0.4,172.30.0.21
ok: dns_domain = mitel.com
ok: syslog_addr = 172.30.200.92
not set: syslog_port
ok: use_vlan = 1
ok: broadcast_addr = 172.30.255.255
ok: vlan_id = 4
```



```
ok: config_file_server = https://server/configfiles/
```

```
:parsing ok:
```

```
processing of section: data_sequence
```

```
[...]
```

```
create data:
```

```
[...]
```

```
RFP configuration:
```

```
[...]
```

13.3 RFP EXPORT FILE FORMAT

General

RFP export files are created by OMM Management Portal in 'csv'-file format which can be easily viewed by a spreadsheet application. Export file contains all or a part of the following parameters:

- MAC address
- Location name
- DECT active
- Cluster
- Paging area
- Synchronization source
- Reflective environment
- Site
- Building
- Floor
- Room
- WLAN profile reference
- WLAN antenna
- WLAN Channel_bg
- WLAN power
- WLAN active

Example

Following example RFP export file contains all exportable RFP parameters and is re-importable by OMM Management Portal.

```
#####  
# RFP data export file: '/home/user/example.csv'
```

```
# Date: 24.09.10   Time: 15:58:19
#####
#
# Exported parameters:
#
# MAC address
# Name
# DECT activated
# DECT cluster
# Paging area
# Preferred sync.
# Reflective env.
# Site ID
# Building
# Floor
# Room
# WLAN profile
# WLAN antenna
# WLAN channel
# WLAN power
# WLAN activated
#
#####
```

```
MAC address;Name;DECT activated;DECT cluster;Paging area;Preferred sync.;Reflective
env.;Site ID;Building;Floor;Room;WLAN profile;WLAN antenna;WLAN channel;WLAN power;WLAN
activated
```

```
data_sequence
```

```
00:30:42:0E:71:41;License RFP 1;
true;1;0;false;true;1;B1;F1;R1;1;0;;100;false
```

```
00:30:42:0E:26:F1;License RFP 2;
true;1;0;false;false;1;B1;F2;R1;1;0;;100;false
```

```
00:30:42:0E:75:59;License RFP 3;
true;1;0;true;false;1;B1;F2;R2;1;0;;100;false
```

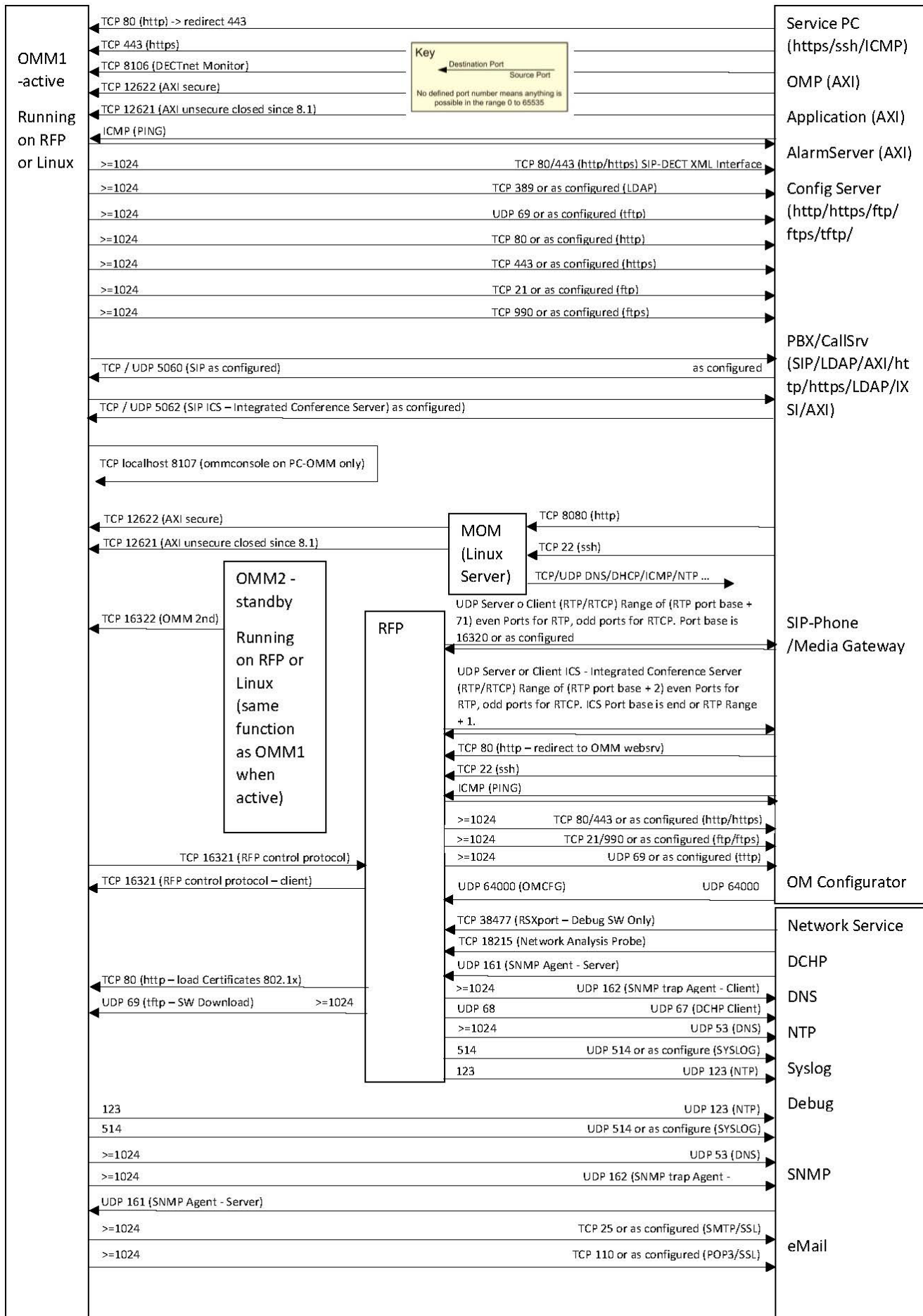
13.4 PROTOCOLS AND PORTS

Protocol		OpenMobility Manager	
		Server port	Client port
HTTPS server	tcp server	443 or as configured	any
HTTP server (redirect to https)	tcp server	80 or as configured	any
HTTP/HTTPS client for the SIP-DECT XML terminal interface	tcp	80/443	> 1024
RFP control protocol	tcp server	16321	any
OMM Standby	tcp server	16322	any
OM AXI	tcp server	12622	any
DECTnet monitor	tcp server	8106	any
LDAP	tcp client	389 or as configured	>=1024 (see note)
TFTP client	udp	69 / given by server	>=1024 (see note)
HTTP client	tcp	80 or as configured	>=1024 (see note)
HTTPS client	tcp	443 or as configured	>=1024 (see note)
explicit FTPS client	tcp	21 or as configured	>=1024 (see note)
implicit FTPS client	tcp	990 or as configured	>=1024 (see note)
OM AXI server TCP	tcp server	12621 Note: This port is: - Available only when switching on (cnf sys uap on) - Dedicated only for test purpose and it is not recommended to use this port.	Any
OM AXI server TLS	tcp server	12622	Any
SIP	udp	5060	as configured
Integrated Conference Server (ICS)	udp	5062	as configured
Telnet (OMM console, Linux server based OMM only)	tcp server	localhost 8107	localhost any

Note: Unbound ports start at port 1024.

Protocol		IP-RFP	
		Server port	Client port
HTTP/HTTPS client for the SIP-DECT XML terminal interface	tcp	80/443	> 1024
RFP control protocol	tcp client	16321	>=1024 (see note)

Protocol		IP-RFP	
		Server port	Client port
HTTP server (redirect to OMM web server (http))	tcp server	80 or as configured	Any
SSH server	tcp server	22	Any
DHCP client	udp	67	68
TFTP client	udp	69 / given by server	>=1024 (see note)
OMCFG server	udp	64000	64000
NTP client	udp	123	123
Syslog client	udp	514 or as configured	514
DNS client	udp	53	>=1024 (see note)
SNMP agent (server)	udp	161	Any
SNMP trap agent (client)	udp	>=1024 (see note)	162
RSXport (debug only)	tcp server	38477	Any
RTP/RTCP (server)	udp	Range of [RTP port base + 71] even ports for RTP, odd ports for RTCP. Port base is 16320 or as configured.	Any
RTP/RTCP (client)	udp	any	Range of [RTP port base + 71] even ports for RTP, odd ports for RTCP. Port base is 16320 or as configured.
Integrated Conference Server (ICS) RTP/RTCP (server)		Range of [ICS RTP port base + 2 * no. conf. channels] even ports for RTP, odd ports for RTCP. ICS Port base is end of RTP range plus 1.	Any
Integrated Conference Server (ICS) RTP/RTCP (client)		any	Range of [ICS RTP port base + 2 * no. conf. channels] even ports for RTP, odd ports for RTCP. ICS Port base is end of RTP range plus 1.
Network Analysis Probe	tcp server	18215	Any



13.5 ABBREVIATIONS

AC	Authentication Code
ADPCM	Adaptive Differential Pulse Code Modulation
COA	Configuration Over Air
DECT	Digital Enhanced Cordless Telecommunication
DHCP	Dynamic Host Configuration Protocol
DSP	Digital Signal Processor
FCC	Federal Communications Commission
GAP	Generic Access Profile
IMA	Integrated Messaging and Alerting Service
IPBX	IP PBX, a telephony system using IP / VoIP
IPEI	International Portable Equipment Identity
OM	OpenMobility
OM AXI	OM Application XML Interface
OMC	OM Configurator
OMM	OpenMobility Manager
OMP	OM Management Portal
PARK	Portable Access Rights Key
PBX	Private Branch Exchange, a customer premises telephony system
PP	Portable Part (DECT phone or device)
RCS	Redirection and Configuration Service
RFP	Radio Fixed Part (DECT base station)
RTCP	Real Time Control Protocol
RTP	Real Time Protocol
TFTP	Trivial File Transfer Protocol

13.6 DEFINITIONS

Asterisk	Asterisk is a complete Open Source PBX in software. It runs on Linux, BSD and MacOSX and provides many features. Asterisk supports voice over IP in many protocols, and can interoperate with almost all standards-based telephony equipment.
Base station	Please see: RFP or Radio Fixed Part
DECT	Digital Enhanced Cordless Telecommunication The standard (ETS 300 175) essentially specifies the air interface, known as the radio interface. Voice and data can both be transmitted via this interface. Its technical key characteristics for Europe are: Frequency range: Approx. 1880 – 1900 MHz (approximately 20 MHz bandwidth) 10 carrier frequencies (1728 kHz spacing) with 12 time slots each Doubling the number of time slots (to 24) using the TDMA process Net data rate per channel of 32 kbps (for voice transmission using ADPCM) Voice coding using the ADPCM method Its technical key characteristics for North American are: Frequency range: Approx. 1920 – 1930 MHz (approximately 10 MHz bandwidth) 5 carrier frequencies (1728 kHz spacing) with 12 time slots each) Doubling the number of time slots (to 24) using the TDMA process Net data rate per channel of 32 kbps (for voice transmission using ADPCM) Voice coding using the ADPCM method
GAP	Generic Access Profile The GAP standard (ETS 300 444) is based on the same technology as DECT, but is limited to the most important basic features. This standard was created in order to allow telephones of different vendors to be used on any type of DECT system. It thus represents the smallest common denominator of all manufacturer-specific variants of the DECT standard. An important limitation in the GAP standard is that external handover is not possible. For this reason connection handover is used, which is supported by GAP terminals. The operation of GAP-capable telephones is comparable to that of analogue terminals. For example, features can be called up via '*' and '#' procedures.
Handover	A handover is similar to roaming, but occurs during an ongoing call. A handover normally takes place "in the background", without disrupting the call (seamless handover).
IPEI	International Portable Equipment Identify 13-digit identification code for DECT phones Example: 00019 0592015 3 (the final digit is the checksum). The code is represented in decimal form. This code is globally unique.

PARK	Portable Access Rights Key Access code for the Portable Part. This code determines whether a DECT phone can access a particular DECT system. Used for unique selection of a dedicated the system from a DECT phone at enrolment/subscription time. Provided via the PARK online service and unique to each SIP-DECT deployment.
Radio Fixed Part (RFP)	An RFP provides a DECT radio cell and terminates the radio link from the portable DECT device. One or more RFPs build the area of radio coverage.
Roaming	While in motion, the DECT phone performs ongoing measurements to determine which RFP is best received. The one that can be best received is defined as the active RFP. To prevent the DECT phone from rapidly switching back and forth between two RFPs that have similar signal strength, certain threshold values are in effect.

13.7 REFERENCES

- /1/ RFC 1350, The TFTP Protocol, Revision 2, July 1992
- /2/ RFC 2090, TFTP Multicast Option, February 1997
- /3/ RFC 2347, TFTP Option Extension, May 1998
- /4/ RFC 2348, TFTP Block size Option, May 1998
- /5/ RFC 2349, TFTP Timeout Interval and Transfer Size Options, May 1998
- /6/ RFC 2236, Internet Group Management Protocol, Version 2, November 1997
- /7/ RFC 1889, RTP: A Transport Protocol for Real-Time Applications, January 1996
- /8/ RFC 2030, Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI, October 1996
- /9/ RFC 2131, Dynamic Host Configuration Protocol, March 1997
- /10/ RFC 2327, SDP: Session Description Protocol, April 1998
- /11/ RFC 2474, Definition of the Differentiated Service Field (DS Field) in the IPv4 and IPv6 Headers, December 1998
- /12/ RFC 2617, HTTP Authentication: Basic and Digest Access Authentication, June 1999
- /13/ RFC 3164, The BSD Sys Log Protocol, August 2001
- /14/ RFC 2833, RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals, May 2000
- /15/ RFC 3261, Session Initiation Protocol (SIP), June 2002
- /16/ RFC 3264, An Offer/Answer Model with Session Description Protocol (SDP), June 2002
- /17/ RFC 3326, The Reason Header Field for SIP, December 2002
- /18/ RFC 3420, Internet Media Type message/sipfrag, November 2002
- /19/ RFC 3515, The Session Initiation Protocol (SIP) Refer method, April 2003
- /20/ RFC 3665, The Session Initiation Protocol (SIP) Basic Call Flow Examples, December 2003
- /21/ RFC 3842, A Message Summary and Message Waiting Indication Event Package for the Session Initiation Protocol (SIP), August 2004
- /22/ RFC 3891, The Session Initiation Protocol (SIP) "Replaces" Header, September 2004
- /23/ RFC 3892, The Session Initiation Protocol (SIP) Referred-By Mechanism, September 2004
- /24/ RFC 4566, SDP: Session Description Protocol
- /25/ RFC 5806, Diversion Indication in SIP, March 2010
- /26/ Compendium "OpenMobility SIP-DECT 4.0 Solution; Installation & Administration"
- /27/ SIP-DECT; OM Integrated Messaging & Alerting Application; Installation, Administration & User Guide
- /28/ SIP-DECT; OM Handset Sharing & Provisioning; User Guide
- /29/ SIP-DECT; OM User Monitoring; User Guide
- /30/ SIP-DECT; Mitel 600 ; Messaging & Alerting Applications; User Guide
- /31/ Mitel 600 series SIP-DECT User's Guide
- /32/ aad-0384 SIP_DECT OM Application XML Interface
- /33/ RFC 2782, A DNS RR for specifying the location of services (DNS SRV)
- /34/ RFC 3262, Reliability of Provisional Responses in the Session Initiation Protocol (SIP)
- /35/ RFC 3311, The Session Initiation Protocol (SIP) UPDATE Method
- /36/ req-0175 SIP-DECT XML Terminal Interface for Mitel 600/700 DECT Phone Family
- /37/ RFC 4579, Session Initiation Protocol (SIP) Call Control - Conferencing for User Agents

- /38/ RFC 5589, Session Initiation Protocol (SIP) Call Control – Transfer
- /39/ RFC 2459, Internet X.509 Public Key Infrastructure certificate
- /40/ RFC 3711, The Secure Real-Time Transport Protocol (SRTP)
- /41/ RFC 4346, The Transport Layer Security (TLS) Protocol Version 1.1
- /42/ RFC 4568, Session Description Protocol (SDP); Security Description for Media Streams
- /43/ RFC 5246, The Transport Layer Security (TLS) Protocol Version 1.2
- /44/ RFC 5630, The Use of the SIPS URI Scheme in the Session Initiation Protocol (SIP)
- /45/ SIP-DECT_LinuxServerInstallation
- /46/ SIP-DECT; Mitel 700 ; Messaging & Alerting Applications; User Guide
- /47/ Mitel 700 series SIP-DECT User's Guide
- /48/ Mitel SIP-DECT CoA Programming Reference Manual

