SIP-DECT OM System Manual

NOTICE

The information contained in this document is believed to be accurate in all respects but is not warranted by Mitel Networks™ Corporation (MITEL®). 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.

CONTENTS

1 OVERVIEW

This document describes the installation / configuration, administration, and maintenance of the SIP-DECT solutions. Please also see the documents listed in the References section (section 10.8) for additional details on different aspects of the SIP-DECT system.

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

1.1 THE SIP-DECT SOLUTION

The SIP-DECT solution includes the following main components:

- SIP-DECT base stations that are distributed over an IP network and offer DECT, WLAN, and IP interfaces

- DECT phones (portable DECT devices)

- OpenMobility Manager (OMM): Management and signaling software for the SIP-DECT solution, which runs on one of the DECT base stations or on a dedicated Linux server (for large installations). In addition, a standby OMM can be configured to ensure OMM function in case of failure or loss of network connection.

- A SIP Call Manager/IP PBX/Media Server platform (e.g. Asterisk)

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

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

Additional components include:

- LDAP server to facilitate a central corporate directory

- Provisioning server to provide RFP configuration or user data files

- Data backup server to automatically backup an OMM database from the server

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

- 3rd party messaging or alarm server to integrate the SIP-DECT text messaging into a unified messaging or alarm environment

- Computer for administration and maintenance tools: Web browser, OM Management Portal (OMP), DECT Monitor

---
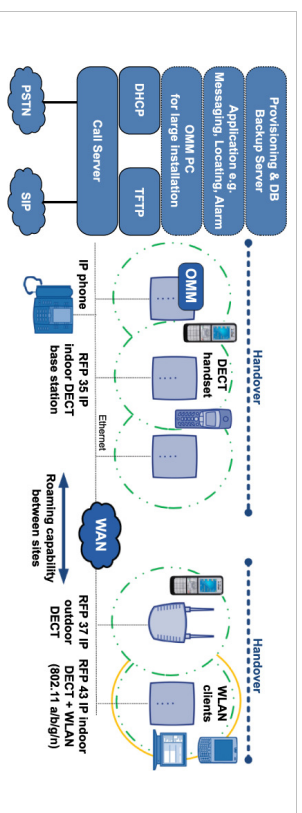
1.2 ABOUT DECT BASE STATIONS

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

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

1.2.1 DECT BASE STATION FAMILIES

1.2.1.1 RFP 4G DECT Base Station family

- 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 connectors for external directional antennas

- RFP 47 DRC (Outdoor Unit)
  RFP 47 preinstalled with directional antennas and 3m cable in an outdoor enclosure

- RFP 48
  DECT RFP with 8 narrow band voice channels + WLAN Access Point as indoor model with internal antennas for DECT and WLAN

The hardware of all the RFPs complies with the different regulatory domains. There are no specific hardware variants required to use specific frequency bands and field strengths. Transmit Power, frequency band and carrier frequencies are controlled by software.
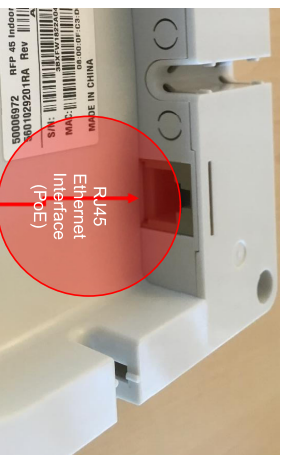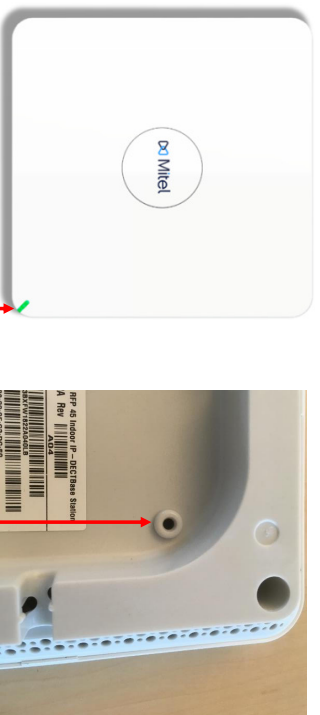
1 RFP 44/45/47/48 (1 LED)

2 Configuration Button

3 100Mbit/s Ethernet Interface, PoE (RFP 44, 45, 47) and 1Gbit/s Ethernet Interface, PoE (RFP 48)

Other differences compared to the previous 3rd RFP family (RFP 35, 36, 37 IP and RFP 42/43 WLAN):

- 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 interfaces

- 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 RFP generation, except a SW update through USB is not possible; because, the RFP 4G does not come with a USB interface.

1.2.1.1 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 3.32 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.
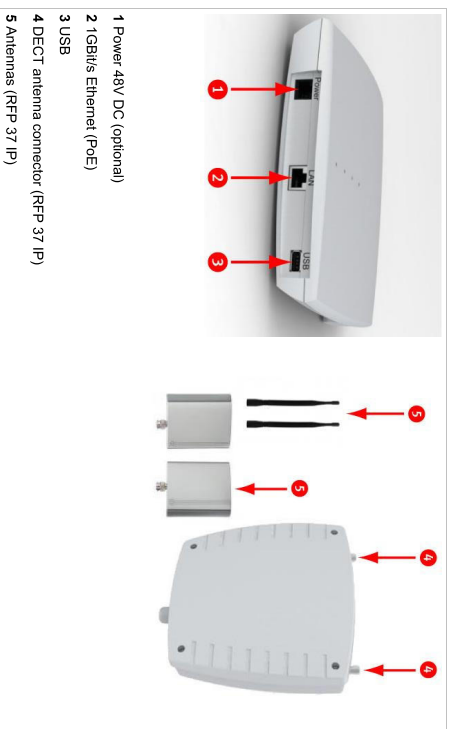
1 Power 48V DC (optional)
2 1GBit/s Ethernet (PoE)
3 USB
4 DECT antenna connector (RFP 37 IP)
5 Antennas (RFP 37 IP)

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

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

- Boots from internal flash memory instead of net-boot (SIP-DECT software is already on board)

- Software update via TFTP, FTP(S), HTTP(S), SFTP supported

- Supports 1GBit/s Ethernet

- Supports CAT-iq 1.0 level high definition voice for the Mitel 650 DECT phone

- Hardware can support Secure SIP and SRTP (with SIP-DECT 5.0 or later)

- Uses an external 48V DC Power Supply (if no PoE available) which meets the latest environmental requirements (RFP 37: PoE only)

- RFP 43 WLAN supports the 802.11a/b/g/n standards

- Any 3G RFP can host the OMM

- Indoor RFPs have a USB 2.0 interface to connect external hardware for future applications (e.g., video camera)

1.2.1.2 Older RFP Types

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

- RFP 32 IP
- DECT RFP as indoor model
- RFP 34 IP
- DECT RFP as outdoor model
- RFP 42 WLAN
- DECT RFP + WLAN Access Point as indoor model

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

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

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

RFP 32 IP / RFP 32 NA
RFP 34 IP / RFP 34 NA

RFP 42 WLAN

1 Power jack (120 V/230 V AC adapter)
2 Ethernet jack; Power supply in line with Power over Ethernet standard IEEE 802.3af

As of SIP-DECT 6.0, there is no distinction between RFP soft brands (i.e., L-RFPs and non-L-RFPs). With SIP-DECT 5.0 and older releases, the "L" variants have built-in licenses. See section 3.32 (Licensing) for more information.

Note: The software package for previous RFPs has a tftp extension e.g. "iprfp2G.tftp. With SIP-DECT 3.0 or higher, you need a 3G RFP to run the Open Mobility Manager.

1.2.1.3 Older RFP Types

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

- RFP 32 IP
  DECT RFP as indoor model
- RFP 34 IP
  DECT RFP as outdoor model
- RFP 42 WLAN
  DECT RFP + WLAN Access Point as indoor model

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

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

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

RFP 32 IP / RFP 32 NA
RFP 34 IP / RFP 34 NA

RFP 42 WLAN

1 Power jack (120 V/230 V AC adapter)
2 Ethernet jack: Power supply in line with Power over Ethernet standard IEEE 802.3af

As of SIP-DECT 6.0, there is no distinction between RFP soft brands (i.e., L-RFPs and non-L-RFPs). With SIP-DECT 5.0 and older releases, the "L" variants have built-in licenses. See section 3.32 (Licensing) for more information.

> **Note:** The software package for previous RFPs has a tftp extension e.g. "prfp2G.tftp. With SIP-DECT 3.0 or higher, you need a 3G RFP to run the Open Mobility Manager.

1.2.2 OPENMOBILITY MANAGER (OMM) MODE

If the OMM is not running on a dedicated Linux server, one RFP within a SIP-DECT installation must be declared to operate as the OpenMobility Manager (OMM). The RFP acting as the OMM may also act as a regular RFP if it is part of a DECT cluster.

In OMM mode, an RFP functions as a regular RFP. Additionally, it is responsible for SIP signaling between the SIP-DECT system and the IP PBX/SIP server. Further on, it takes over the management part of the SIP-DECT solution. You designate an RFP as the OMM by assigning an IP address to the RFP within the DHCP scope (see section 7.5) or by setting the data via the OM Configurator (see section 7.7). After an RFP is designated as the OMM, it starts the extra services on board (for example, the web service that supports the management interface). All RFPs download the same firmware (for their RFP type), but only one RFP (or two, in standby implementations) activates the OMM services.

> **Note:** It is possible to deactivate the DECT part of an RFP. If the DECT interface is deactivated, all resources (CPU and memory) are available for the OMM. This might be necessary, for example, in configurations where a mix of OpenMobility Manager, G.729/Conferencing and WLAN is provided by the same RFP.

1.3 ABOUT THE OPENMOBILITY MANAGER

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

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

- If the OMM runs on a DECT base station, a 100 Mbit/s network link is required.
- If the OMM runs on a dedicated Linux server, a 1 GBit/s network link is required (see also section 7.13.1).

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 7.15.

1.3.1 OMM TASKS

The OMM performs the following tasks:

- Signaling gateway (SIP <-> DECT)
- Media stream management
- Managing sync-over-air functions between RFPs
- Provides a Web service for system configuration
- Provides additional services such as
  – LDAP based central corporate directory
  – OM Application XML Interface (OM AXI) for OAM&P, messaging, alerting service and locating

– Integrated Messaging and Alerting Service (OM IMA)
– Data backup and provisioning services
– SIP-DECT XML terminal interface. This interface adapts the "XML API for SIP Phones" to SIP-DECT phones. The Mitel 600 DECT phone family is supported.
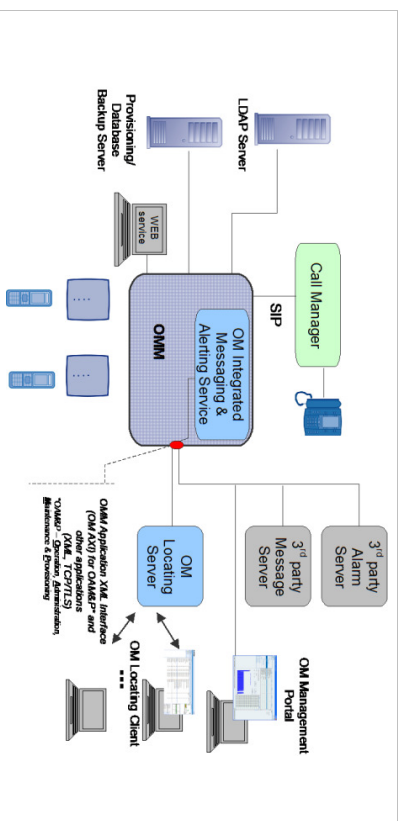
Additional information on the following functionality is available in separate documents.

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

1.3.2 SIP-DECT SPECIAL FEATURES AND CAPABILITIES

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

Diagram labels: LDAP Server; Provisioning/Database Backup Server; WEB service; Call Manager; SIP; OMM; OM Integrated Messaging & Alerting Service; 3rd party Alarm Server; 3rd party Message Server; OM Locating Server; OM Management Portal; OM Locating Client; OMM Application XML Interface (OM AXI) for OAM&P and other applications (XML, TCP/TLS) "OMM" Location, Administration, Maintenance & Provisioning.

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

1.3.3 OMM CAPACITIES AND FEATURES

The following table summarizes OMM capabilities:

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

[1] The feature requires a license.
[2] The feature is available with the RFP 35/36/37 IP and RFP 43 WLAN and the Mitel 650 DECT phone (or other CAT-iq-capable devices). The feature is enabled per site and requires that the RFPs are configured in the same site and cluster.
[3] Release 8.0 or later: If RFP 4G runs as OMM, 1024 users/handsets are supported.

1.3.4 OMM CAPACITIES AND RFP SUPPORT

The following table summarizes OMM and RFP Support capabilities:

Feature	As of SIP-DECT 6.0		As of SIP-DECT 8.0	
	RFP OMM	Linux server OMM	RFP OMM	Linux server OMM
RFP 32/34 IP and RFP 42 WLAN	256	2048	256	4096

Feature	As of SIP-DECT 6.0		As of SIP-DECT 8.0	
	RFP OMM	**Linux server OMM**	**RFP OMM**	**Linux server OMM**
RFP 35/36/37 IP and RFP 43 WLAN	256	2048	256	4096
RFP 44/45/47 IP and RFP 48	Not applicable	Not applicable	256	4096
DECT phones / users	512	4500	1024 (RFP 4G OMM) 512 (RFP 3G OMM)	10000

1.4 ABOUT DECT PHONES

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

Mitel provides the following DECT phones:

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

Notes on the Mitel 600 DECT Phones

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

The latest Mitel 600 firmware release has the following characteristics:

- New user interface e.g. new dial editor with alphanumerical and always en-bloc dialing
- Support of UTF-8 in over the air signaling with the OMM
- Digit and alphanumeric dialing
- Support of SIP-DECT XML terminal interface
- Support of microSD card to save subscription data and the most important local device data (not supported by Mitel 600 DECT phones)
- Additional subscription options
- Additional alarm melodies
- Profile indication in idle display

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

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

The Mitel 600 DECT phone also supports DECT enhanced security.

1.5 FILE NAMING CONVENTIONS

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

Software package	**As of SIP-DECT 7.1**	**As of SIP-DECT 8.0**
Software image for RFP 32/34 IP / RFP 42 WLAN	omm_ffsip.tftp	iprfp2G.tftp
Software image for RFP 35/36/37 IP / RFP 43 WLAN	iprfp3G.dnld	iprfp3G.dnld
Software image for RFP 44/45/47 IP / RFP 48	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
DECT phone software rpm	SIP-DECT-HANDSET-<version>.i686.rpm	SIP-DECT-HANDSET-<version>.i686.rpm
SIP-DECT OMM/MOM OVA	SIP-DECT-<version>.ova	SIP-DECT-<version>.ova

1.6 LOGIN AND PASSWORDS

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

Interface/Tool	**SIP-DECT OMM SDC OMM**	**RFP 32/34 IP / RFP 42 WLAN**	**RFP 35/36/37 IP / RFP 43 WLAN RFP 44/45/47 IP / RFP 48**
Initial configuration through OM Configurator login / password (no previous connection with the OMM)	n/a	No login required	"omm" / "omm"
OMM access through Web or OMP (after initial OMM configuration)	Read-only or full-access accounts as configured	n/a	n/a
Configuration through OM Configurator after connection with OMM login / password (system-wide set by OMM)	n/a	OMM standard full-access account login / password	OMM standard full-access account login / password
Initial OMM configuration through Web or OMP standard full-access account login / password	"omm" / "omm" "omm" / "omm"	n/a	n/a
ssh (no previous connection with the OMM)	n/a	User shell: "omm" / "omm" Root shell: "root" / "22222"	User shell: "omm" / "omm" Root shell: "root" / "22222"
ssh	n/a	User shell:	User shell:

Interface/Tool	SIP-DECT OMM SDC OMM	RFP 32/34 IP / RFP 42 WLAN	RFP 35/36/37 IP / RFP 43 WLAN RFP 44/45/47 IP / RFP 48
(with previous connection with the OMM) (system-wide set by OMM)		OMM standard full-access account login / password Root shell: as configured	OMM standard full-access account login / password Root shell: as configured

2 ENHANCED FEATURE OVERVIEW

A SIP-DECT system can scale from a small system of five or less DECT base stations to a larger SIP-DECT system that may include hundreds of DECT base stations. Some of the more advanced features target larger DECT systems. You may browse the following list of features in order to get an overview and to decide if it's relevant for your requirements. You find in-depth explanations in the referenced sections.

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

2.1 PC-BASED OMM INSTALLATION

A very large number of DECT base stations or a large number of DECT phones may exceed the storage capacity or processing power of the embedded DECT base station. For this reason, it is also possible to operate the OMM on a standard PC under the Linux operating system (see section 7.12).

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

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

2.2 DECT XQ

The DECT radio communication generally suffers from attenuation and radio wave reflection. In particular, if a building's walls and ceilings contain a higher portion of metal-based material or if larger metal surfaces are present, the DECT XQ improves the radio communication between a DECT base station and a Mitel 600 DECT phone at the expense of DECT channel capacity (see 7.3). Enable this feature for some or all of your DECT base stations (see section 5.6.3, "DECT settings" or section 6.7.1.2, "DECT tab").

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

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

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

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

- In automatic mode, the connection establishment depends on whether the current base provides DECT XQ or not. If DECT XQ is available, a narrowband connection will be established. Otherwise a wideband connection will be established.

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

In conjunction with the RFP 35/36/37 IP and RFP 43 WLAN, the Mitel 650 DECT phone can act as a Mitel Hi-Q audio terminal. This feature is realized using wideband speech according to CAT-iq.

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

Mitel Hi-Q audio technology must be enabled or disabled per site (see section 5.5). This functionality must be homogeneously available among synchronous RFPs (members of the same cluster). Each site with enabled Hi-Q audio must exclusively contain new RFP 35/36/37 IP or RFP 43 WLAN.

Typically one site is identical with one cluster, i.e. all RFPs belonging to a specific site belong to a specific cluster. However a site can have more than one cluster. The OMM allows configuration of a cluster that contains multiple sites. Such configuration could annul the rule that Hi-Q audio must be homogeneously available among synchronous RFPs.

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

2.4 DECT ENHANCED SECURITY

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

Furthermore, some new features have been added to GAP:

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

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

The feature set can be enabled or disabled per site, because enhanced security is available with RFPs 35/36/37/43. Roaming between sites where enhanced security is enabled and disabled respectively should be avoided.

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

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

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

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

2.5 VOIP ENCRYPTION

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

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

- Authentication
- Integrity
- Confidentiality
- Privacy

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

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

2.6 MIXED DECT BASE STATION INSTALLATIONS

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

For a detailed description see section 7.30.

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.

2.7 WIRELESS LAN (WLAN)

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

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

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

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

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

2.7.2 CHANNEL CONFIGURATION FEEDBACK FOR HT40 AND TX POWER

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

2.8 DECT BASE STATION SYNCHRONIZATION

To ensure a seamless communication experience, the SIP-DECT system switches an ongoing DECT phone call from one DECT base station to another if the radio communication quality drops below a certain threshold. The seamless handover is possible only if the participating DECT base stations are synchronized. DECT base station synchronization is performed via radio communication between DECT base stations, which in turn requires a decent radio coverage planning (see section 7.2).

2.8.1 CLUSTERING AND PAGING AREAS

Your SIP-DECT system may include different locations, where the distances between the locations prevent the RFPs from performing the over-the-air synchronization. In this case, you must split your network into clusters (or "synchronization domains"). You assign DECT base stations to cluster numbers for this purpose (see section 5.6.3 "DECT settings" or section 6.7.1.2, "DECT tab"). Note that overlap between different clusters on one campus or site must be avoided.

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

A separate cluster number is also required for a remote site (e.g., for a single DECT base station servicing an office abroad). Also, if the VPN network connection to the isolated site's DECT base station cannot transport DHCP, you may use static IP address configuration for the single DECT base station (see section 7.6).

2.9 DECT BASE STATION RESET TO FACTORY SETTINGS

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

You can also reset the base station to default settings using the OM Configurator or the OMM Web service (see section 7.7.8).

2.10 SYSTEM REDUNDANCY

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

2.10.1 OMM STANDBY

The OMM is the central management entity in a SIP-DECT system and therefore constitutes a single point of failure. It is possible to automatically transfer the OMM function to a second DECT base station in case of failure or loss of network connection (see section 7.15).

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

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

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

2.10.2 BACKUP SIP PROXY/REGISTRAR

To increase the operational availability of the system in critical environments like hospitals, the OMM offers a new failover mechanism for the SIP server. Therefore, in addition to the primary proxy, outbound proxy and registrar server, it is possible to configure two additional levels of backup servers named "secondary" and "tertiary" servers (see section 7.20.3).

In addition, a keep-alive mechanism implemented in the OMM allows the automatic failover to secondary/tertiary servers or automatic coming back to primary servers (see section 7.20.4).

2.10.3 CONFIGURABLE USER ACCOUNT FOR STANDBY CHECK

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

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

With previous SIP-DECT releases, the OMM used the user account with the lowest phone number for the check procedure. To select a specific user account for this purpose, enable the "Used for visibility checks" flag in the user settings (see section 6.10.4).

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

2.10.4 USER DATA SYNCHRONIZATION (MIVOICE 5000 DUAL HOMING SUPPORT)

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

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

For more information on this feature, see section 7.16.

2.10.5 MULTI-OMM MANAGER FOR OMM-CENTRALIZED MANAGEMENT

With SIP-DECT 7.0 and later, SIP-DECT supports centralized OMM provisioning and user/device data 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. Instead of deploying one OMM with DECT base stations installed at different sites, or deploying DECT base stations and a dedicated OMM at each site, you can create a multi-site SIP-DECT system with local survivability and centralized management capabilities. You deploy OMMs and DECT base stations as a standalone system at each site, but manage the entire SIP-DECT system through the MOM interface.

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

2.11 SIMPLIFIED LICENSING

With SIP-DECT 6.0 or later, the licensing model is simplified. The system no longer distinguishes between different DECT base station "soft-brands", and some licenses are deprecated. See section 3.32 for more information.

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

2.12 EXTENDED REGULATORY DOMAIN SUPPORT

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

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

A new regulatory domain, 1910-1927MHz, 250mW, has been added for South America. You can configure this regulatory domain via the OMP (**System** -> **Basic settings** -> **DECT** tab); see section 6.5.1.2 for configuration details.

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

2.13 DECT PHONE FUNCTIONALITY

2.13.1 DECT PHONE DOWNLOAD OVER AIR

The Mitel 600 series DECT Phones can download and upgrade their firmware via DECT over the air.

As of SIP-DECT 6.0, the DECT base station software image (iprfp3G.dnld) contains the Mitel 600 DECT phone software. If the DECT base station houses the OMM, the OMM uses this software to update the DECT phones. The DECT base station OMM no longer automatically attempts to load a DECT phone software image from a DECT base station software URL when provided via DHCP or local configuration.

For specific maintenance purposes only, SIP-DECT allows configuration of a URL via the OMM Web service or OMP to use an alternative DECT phone software image (see section 5.4.1.6). The Mitel 600 DECT phone firmware packages are delivered in the "600.dnld" file for the OMM running on a DECT base station.

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

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

> **Please note:** An DECT base station upgrade from SIP-DECT 3.0 to 6.0 or later is not supported due to the extended DECT base station software image. The 3.0 software does not accept the extended software image.
>
> For large installations using a Linux Server OMM, the DECT base station software image (iprfp3G.dnld) without Mitel 600 DECT phone software can be used. This software image supports a direct RFP upgrade from SIP-DECT 3.0 to 6.1.

2.13.2 CENTRAL DECT PHONE CONFIGURATION OVER AIR (COA)

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

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

Configuration of all DECT phones with a predefined default profile is also supported. Up to 20 possible DECT phone profiles make it easy to adapt to different usage scenarios for heterogeneous user groups (e.g., nurses and doctors in hospital environments). See section 7.23 for more information on this feature.

2.13.2.1 CoA enhancements

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

New configuration commands allow you to overwrite local key programming on the Mitel 602 DECT phones. SIP-DECT 6.1 also supports configuration of the new XML application hooks introduced for the XML terminal interface via CoA (see section 3.32).

In addition, the Mitel 602 DECT phone 6.1 firmware introduces variable lists. A variable list includes a number of items, each of which corresponds to an action to be performed on the DECT phone. For more information, see section 7.23.5.

2.13.3 OMM DECT PHONE PROVISIONING

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

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

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

2.13.4 MITEL 600 DECT PHONE DIAL EDITOR MODE

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

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

2.13.5 MITEL 602 DECT PHONE CUSTOMIZABLE BOOT TEXTS

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

2.13.6 OMM-CENTRALIZED CALL LOGS

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

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

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

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

For information on how to enable OMM-centralized call logs, see section 5.9.5.2 (modifying an XML hook via the OMM web service) or section 6.12.7.2 (modifying an XML hook via the OMP).

2.14 HOT DESKING

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

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

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

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

2.15 CONFERENCING

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

The centralized conferencing feature is based on RFC 4579 and supports the use of external third party conference servers (e.g. Broadsoft or 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 and Mitel 142d DECT phones.

For a detailed description of conferencing functionality, see section 7.21.

2.15.1 CONFERENCING AUDIO NOTIFICATION

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

2.15.2 CENTRALIZED CONFERENCING WITH MIVOICE BUSINESS

SIP-DECT 6.1 introduces support for centralized conferences hosted by the MiVoice Business platform.

The SIP signaling implemented by the MiVoice Business platform require that the SIP-DECT implementation initiate a conference via blind transfer. The conference mode (External – blind transfer) can be configured globally for all SIP-DECT users (via the OMP **System -> SIP -> Conference** tab) or configured individually for SIP-DECT users (via the OMP **DECT Phones -> Users -> Conference** tab).

SIP-DECT 6.1 also introduces a new Feature Access Code. The new "Blind transfer" Feature Access Code allows a user to initiate a SIP blind transfer from the Mitel 600 DECT phone. You can configure the FAC via the OMM web service (see section 5.9.4) or the OMP (see section 6.12.2).

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

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

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

2.15.3 N-WAY CONFERENCING

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

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

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

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

2.16 SIP OVER UDP/TCP/TLS

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

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

2.17 SIP MULTIPORT

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

The port range is set per protocol (i.e., UDP/TCP and TLS), and must not overlap with other ports in use. The following parameters can be configured or read per user (see section 6.10.4) and conference room:

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

The calculation is based on the following rules:

UserPortCount = UserPortRangeStart - UserPortRangeEnd + 1
UserPort = ((UserID – 1) % UserPortCount) + UserPortRangeStart

ConfRoomPortCount = ConfRoomPortRangeStart - ConfRoomPortRangeEnd + 1
ConfRoomPort = (ConfRoomID % ConfRoomPortCount) + 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 6.5.4.1).

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

Configuration Rules for Port Ranges

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

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

2.18 UTF-8 ENCODING

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

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

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

For third-party GAP DECT phones, Mitel DECT 142 / Mitel 142d or Mitel 600 with older firmware releases, the UTF-8 character set is not supported. If possible, the OMM maps UTF-8 character to LATIN-1.

> **Please note:** The available set of characters is defined by the DECT phone. Please see /31/. User configuration files must be encoded in UTF-8.

2.19 ALPHANUMERIC DIALING

SIP-DECT supports the dialing of alphanumeric characters. This allows a user to dial names (e.g. "Heinrich Mueller") as well as digits.
If SIP URI dialing such as "name@domain" is used, you must use an (outbound) proxy that supports the interpretation of SIP user names, including domain names.

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

2.20 VOICE MAIL NUMBER

You can configure a system-wide voice mail number. This number is used by the Mitel 600 DECT phone family if a voice box call is initiated. The system-wide voice mail number can be overruled by a user-specific voice mail number. If there is no voice mail number configured or another type of DECT phone is used, the voice mail number must be configured locally on the DECT phone.

> **Please note:** The voice mail number is supported by the external user data configuration files. The parameter UD_VoiceMailNumber can be set in the user_common.cfg and/or "user.cfg" or "LoginID.cfg" e.g. "UD_VoiceMailNumber=222". For details, see the SIP-DECT DECT Phone Sharing and Provisioning Guide.

2.21 CALL HANDLING

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

2.21.1 DIVERSION INDICATION

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

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

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

Tim's phone @ 5140 — diverted to by Mark's phone @ 5142 ➤ Roger's phone @ 5141

user-busy
>>5142
5141

Tim
>>5142
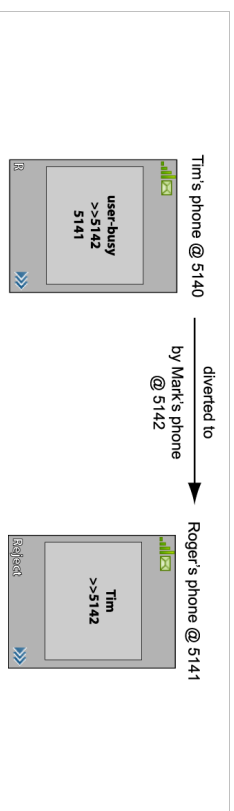
2.21.2 CALL COMPLETED ELSEWHERE

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

2.21.3 SEMI-ATTENDED TRANSFER

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

The supported modes are:

Semi-attended transfer mode	Refer-to with replaces	Behavior

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

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

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

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

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

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

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

• R-Key will accept the incoming call. All supplementary services will involve that incoming call directly or indirectly.

• Selecting "Transfer" or "Brokering" offers the possibility to keep the waiting call and continue supplementary services with the former line only. The waiting call is not involved but can be accepted later.

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

2.21.5 CALL TRANSFER ENHANCEMENTS FOR MITEL 142D DECT PHONES

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

• Press I-Key within a basic call
• Select "Transfer"

• Select editor or phonebooks
• Edit or select destination and press "OK"

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

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

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

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

You can still initiate a transfer via the menu.

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

• Press I-Key within an inquiry call or brokering state
• Select "Release"

2.22 TRUNCATING SIP USER NAME IN SIP URI

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

Example: If the DECT phone receives

Contact: "Dominique B." sip:5405;opensSipsTestproxy@testlab.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 "opensSipsTestproxy" will be removed.

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

2.23 OM LOCATING APPLICATION

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

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

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

Images showing the floor plan of the buildings belonging to the OM system can be imported into the OMP. In a next step the RFPs of the SIP-DECT system can be placed on these images with drag and

drop. Finally for each of the RFPs, the graphic map images will be generated in the format and size as required by the OM Locating application.

The process and the OMP functionality for this feature are described in detail in section 7.23.

2.24 EXTENDED MESSAGING

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

2.25 VIDEO SUPPORT

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

2.25.1 USB VIDEO DEVICES

You can configure and use USB video devices that are fully supported by the UVC video class device driver. The USB video device is connected to the USB port of a SIP-DECT RFP 35. In conjunction with the "Surveillance" feature of the OM Locating application, the USB video devices generate snapshot images and video streams.
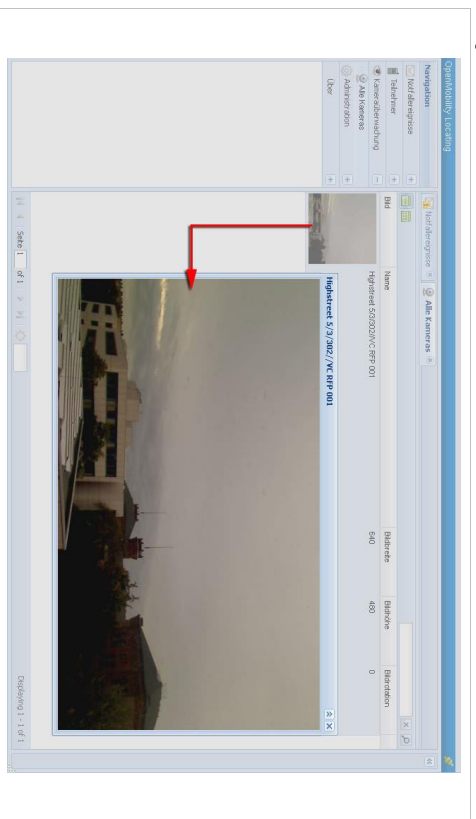
For a detailed description see section 7.27.

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

2.25.2 TERMINAL VIDEO

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

Video Streaming is only available when the DECT phone is connected to a RFP 35/36/37/43 and the permission is set for the site and the DECT phone.

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

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

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

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

- Enable all sites that have the technical capability (only RFP 35/36/37/43) via OMP for terminal video.
- Enable the additional service "Video stream permission" via OMP (**DECT Phones -> Users**) for those users who are allowed to use this feature.

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

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

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

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

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

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

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

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

2.26 USER MONITORING

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

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

User status information is available via OM AXI and OMP.

For a detailed description of the "User monitoring" feature see section 7.29.

2.27 CORPORATE DIRECTORY INTEGRATION

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

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

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

For configuration information see section 6.12.5.

2.28 INTEGRATION INTO EXTERNAL MANAGEMENT SYSTEMS

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

• Each DECT base station may run an SNMP agent that can be queried by SNMP management software (see 7.19).

• To further integrate into external configuration management systems, the DECT system's configuration is available my means of ASCII-based configuration files. You can configure automatic import of configuration files from an external server. For more information, see section 7.8.

• The OM AXI software application interface can also be used for integration into external systems. Refer to the OM Application XML Interface (OM AXI) specification, see /31/.

2.29 SYSTEM CONFIGURATION TOOLS

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

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

Both applications support the essential configuration and administration settings required for smaller SIP-DECT systems. However, for larger SIP-DECT systems using enhanced features, some settings are only available in the OMP application.

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

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

2.30 SIP ENHANCEMENTS

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

2.30.1 GLOBALLY ROUTABLE USER-AGENT URIS (GRUUS)

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

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

2.30.2 SESSION TIMER

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

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

2.30.3 SIP CONTACT MATCHING

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

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

2.30.4 CONFIGURABLE CALL REJECT STATE CODES

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

2.30.5 CALL RELEASE TIMERS

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

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

2.30.6 INCOMING CALL TIMEOUT

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

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

2.30.7 CALL REJECT ON SILENT CHARGING

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

* If the flag "Call reject on silent charging" is set.

* If the phones are in charging mode and "silent charging" is activated in the phone.

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

2.30.8 ROUTE HEADER

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

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

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

2.30.9 MWI SUBSCRIPTION PERIOD

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

2.31 AUTO ANSWER, INTERCOM CALLS AND AUDIO SETTINGS

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

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

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

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

2.31.1 INTERCOM CALLS

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

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

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

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

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

2.31.1.1 Barge-in of incoming intercom call

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

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

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

2.31.1.2 Outgoing intercom calls

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

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

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

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

2.31.2 AUTO ANSWER AUDIO SETTINGS

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

Incoming call settings:

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

Outgoing call setting:

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

2.31.2.1 User-specific incoming call setting

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

2.32 SIP-DECT XML TERMINAL INTERFACE

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

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

To call a certain URI, there are a number of hooks available for the Mitel 600 DECT phones which can be put on a programmable key or can be called from a menu. You can activate the predefined XML hooks via the OMM Web service (see section 5.9.5) or the OMP (see section 6.12.7).

You can also activate the XML hooks through the Configuration over Air (CoA) feature; see section 7.23 for more information.

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

2.32.1 FEATURE ACCESS CODES TRANSLATION

Many PBXs allow the control of PBX supplementary services by dialing specific numbers called feature access codes (FAC). SIP-DECT supports the "Feature Access Codes Translation" XML application to avoid conflicts between SIP-DECT feature access codes or digit treatment rules and PBX feature access codes. If "Feature Access Codes Translation" is activated, SIP-DECT users can chose "FAC" menu on the Mitel 600 or Mitel 142d DECT phones in any call state and enter the feature code en-bloc. The input is sent to the PBX (Application server) within a URI request.
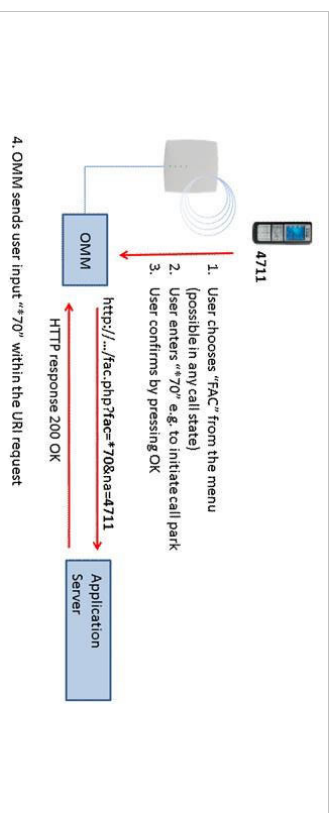
This feature can be configured using OMP on the **XML applications** page (see section 6.12.7).

2.32.2 RING TONE SELECTION FOR (ALARM) MESSAGES

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

In previous SIP-DECT releases, the "melody" field offered ten tones, selected by an identifier. In the current release, the "explicitToneSelection" field allows the user to select a tone, which does not have to

belong to the set of "melody" tones, by the name string. If both are set, the explicit ToneSelection value takes precedence.

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

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

2.33 SOFTWARE UPDATE DISPERSION

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

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

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

3 LICENSING

3.1 LICENSING MODEL

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

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

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

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

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

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.

Status	**License settings**		
System	Installation ID	272643175	
Base Stations	License file import	Choose File No file chosen	Import
DECT Phones			
WLAN	**General**		
Licenses	Status	✓ Standard license	
Info	License type	Standard license	
	Grace period	720:00	
	PARK	1F1024507	
	MAC address 1	00:30:42:18:1D:BD	(31102450?348)
	MAC address 2	--	
	MAC address 3	--	
	System		
	Number of DECT base stations	256	Mitel SIP-DECT System License XXX
	License key	U5TJKJ-T4SBD-VM5FGR-2E343-3SDDM	
	Messaging		
	Receiving text messages (Emergency, Locating alert) and enhanced messaging features	✓	Mitel SIP-DECT Messaging & Alerting License Enterprise
	License key	TNC5K-DX1D-T4UJM-MEFNG-MDM83	
	Locating		
	Number of users allowed to be located	10000	Mitel SIP-DECT Locating User License XXX
	OM Locating application	✓	Mitel SIP-DECT Locating Server License
	License key	P2MVK-HTPK-RHG5R-CMCL6-UJU37B	

Small systems – 1 ... 5 DECT base stations

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

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

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

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

Large systems – up to 4,096 DECT base stations

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

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

3.1.2 ABOUT G.729 CHANNELS

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

3.1.3 PARK SERVICE

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

DECT settings

PARK
Online PARK request
Manual PARK import

Changing these setting causes the OpenMobility Manager to be reset.

OpenMobility Manager SIP-DECT 6.0RC4 – Mozilla Firefox

Encry...
Restri... https://172.30.206.234/manual_park.html
DECT...
Regul...

Manual PARK import
DECT... Changing these settings may cause the OpenMobility Manager to be reset.
DECT... Manual PARK service URL: https://iparkmanager.mitel.com/pm/parks/fetch.xhtml
Prese...

Manual PARK import

PARK request file — Save
Import PARK file — Durchsuchen... Keine Datei ausgewählt — Import

orks (...

Dokument: 100% Grafiken: 1/1 Geladen: 6 KB Geschw.: 8.13 KB/s Zeit: 0.739

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://iparkmanager.mitel.com/pm/parks/fetch.xhtml) and upload it to the PARK server from a computer that is connected to the Internet. You can then import the file into the OMM.

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

3.1.4 UPGRADE LICENSE

With SIP-DECT Release 6.0 or later, you do not require a license to upgrade to a newer release. Older systems with an OM Activation License for L-RFPs (3...20 RFP-L) require a license upgrade, which is available from the License server at no cost. Note that you must already have three MAC addresses registered on the license server for the license upgrade.

3.1.5 GRACE PERIOD

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

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

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

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

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

3.1.6 LICENSE VIOLATIONS AND RESTRICTIONS

A license can be violated in three ways:

- The number of configured items exceeds the number of licensed items. In this case the associated feature is restricted:

  - the audio stream of calls is dropped after 30 seconds when the number of connected DECT base stations exceeds the licensed number

  - the messaging application limits the type of messages to "info", "low", "normal" and "high"

  - the locating feature is stopped

- For SIP-DECT 5.0 (or older) systems, the software version in the license file does not match the software version running on the OMM.

- The OMM has no connection to at least two of the validation DECT base stations and the grace period has expired.

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

3.2 UPLOADING A LICENSE FILE

A license file must be generated on the Mitel license server. The license confirmation provided when you order your system contains detailed information on how to generate the license file. The file can be uploaded into the OMM either via Web service (see section 5.10) or via the OMP (see section 6.12.7).

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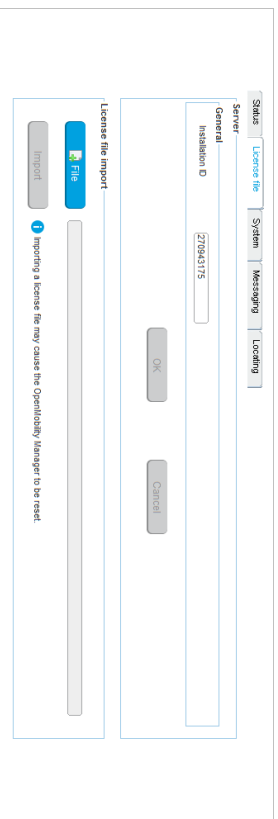
The SIP-DECT license file format prepares the system for receiving licenses from Mitel PBXs or to act as a license key server for other Mitel products in future releases.

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 4.1.5.

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 7.5.4.1).

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

1 Connect the DECT base station(s) to your LAN and power up the units.
2 Open the OM Configurator and select your network interface via the **General -> Options** menu.
3 Click **Scan** to find the base stations connected to your LAN (enter user name and password: "omm" / "omm" for initial configuration until start-up)
4 Select a base station entry and double-click for configuration.
5 Enter the configuration parameters for the base station. For configuration details, see section 7.7.
6 Click **OK** when you have entered configuration parameters.
7 Click **Send Configuration** to apply the configuration to the DECT base station.
8 To configure the next unit, select another base station entry from the table, set the appropriate parameters (and confirm with **OK**), and click **Send Configuration.**

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

4.2 SYSTEM CONFIGURATION

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

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

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

53

4.3 SYSTEM SETTINGS

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

General settings

System name	Customer
Remote access	☑
Tone scheme	US ▼

System name: Customer Name
Remote access: Allow SSH access
Tone Scheme: Scheme to simulate call control tones (country-dependent).

DECT settings

PARK	1F1026A3C7
DECT power limit 100mW	☐
Encryption	☐
Restrict subscription duration	☐
DECT monitor	☐
Regulatory domain	US (FCC/IC) ▼
DECT authentication code	2222
DECT phone user login type	Number ▼
Preserve user device relation at DB restore	☐

PARK: The system needs a PARK code to operate. Use the Online PARK service to obtain a PARK code (see section 4.1.3) (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 phone will then offer the voice box in the Handset menu.

54

4.4 BASE STATIONS

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

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

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

New base station

ⓘ Please configure a WLAN profile of proper type.

General settings	
MAC address	
Name	
Site	1 ▼

DECT settings	
DECT Cluster	1
Preferred synchronization source	
Reflective environment	☐

WLAN settings	
WLAN profile	1 ▼
802.11 channel	▼
Output power level	Full ▼

OK   Cancel

The base station configuration requires:

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

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

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

4.5 SIP SETTINGS

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

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

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

SIP

Basic settings	
Proxy server	10.37.44.99
Proxy port	5060
Registrar server	10.37.44.99
Registrar port	5060
Registration period	300 sec
Globally Routable User-Agent URL	☑
Outbound proxy server	5060
Outbound proxy port	5060
Transport protocol	UDP ▼
Local UDP/TCP port range	5060
Local TLS port range	5061 ,

RTP settings	
RTP port base	16320
Preferred codec 1	G.711 u-law ▼
Preferred codec 2	G.711 A-law ▼
Preferred codec 3	G.729 A ▼
Preferred codec 4	G.722 ▼
Preferred packet time	10 ▼ msec
Silence suppression	☐
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

OK   Cancel

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.

4.6 DECT PHONES

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

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

New DECT phone

General settings

Display name	
Number/SIP user name	
IPEI	
DECT authentication code	2222
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 e.g. terminal phone number

IPEI: Handset hardware identifier (optional)

DECT authentication code: Code for Handset subscription. If this field is left empty, the system-wide DECT authentication code is used (see section 2.3).

Authentication user name: SIP user name

Password: SIP Extension password

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

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

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

4.6.1 DECT PHONE AND SIP STATE VERIFICATION

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

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

User/device status & configuration

User status:

Registered:	Yes
Registrar server type:	Primary
Registrar server:	10.37.44.99
Registrar port:	5060
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:	25053
Description 2:	
User lang.:	English
SOS number:	
MD number:	
VM number:	
SIP auth. user name:	25053
SIP auth. password:	********
Fixed local port:	
Login/Add ID:	
PIN:	********
External:	No
VIP:	Yes
Visibility checks:	No
Sending messages:	No
Sending vCards:	No
Receiving vCards:	No
Video stream perm.:	No

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

5 OMM WEB SERVICE

The OMM acts as an HTTP/HTTPS server. The HTTP server binds to port 80 and HTTPS binds to port 443 by default. A HTTP request on port 80 will be redirected to HTTPS on port 443.

5.1 LOGIN

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

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

With the first login to a new SIP-DECT software version, the user must accept the End User License Agreement (EULA) (see section 5.11).

If the default built-in user account is active, the administrator must change the default account data (passwords) of the "Full access" and "root" account. The meaning of the different account types is described in section 7.17.1.

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

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

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

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

5.2 LOGOUT

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

5.3 "STATUS" MENU

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

General	
OpenMobility Manager	SIP-DECT 8.0RC4 Build 2
Uptime	20:32
Licenses	✓
Grace period	720:00
Standby OMM	✓
IP address	10.37.18.31
Number used for visibility checks	20552
OM Integrated Messaging & Alerting service	✓

Base Stations	
Total number	12
Connected	2
DECT activated	12
DECT currently active	2
DECT clusters	2
WLAN activated	0

| DECT Phones	
Total number	84
Subscribed	4
Subscription allowed	✗
Activate firmware update	✓
Loading firmware from	http://10.37.18.35/800.dnld
Firmware version	[800: 5.00.SP5.RC01] [650: 5.00.SP5.RC01] [650_002: 6.0.RC8]
Number of known downloadable DECT phones	4

5.4 "SYSTEM" MENU

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

5.4.1 "SYSTEM SETTINGS" MENU

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

- configure global settings (see the following sub-sections)
- restart the OMM (see section 5.4.1.15)
- update the OMM (see section 5.4.1.16)
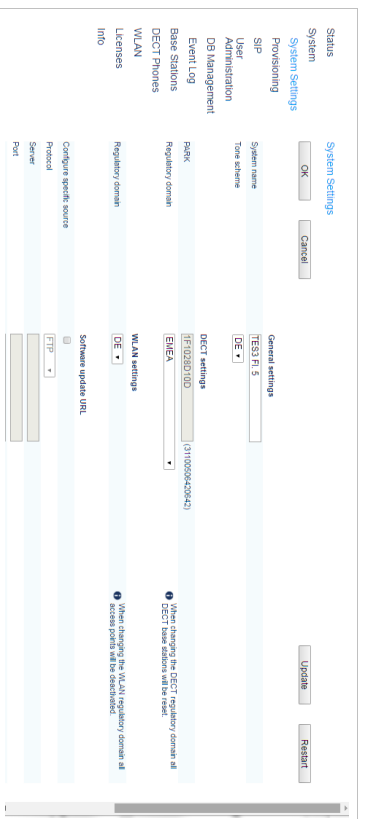
The following sections describe the parameters that can be set.

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

5.4.1.1 General settings

The following information describes the parameters that can be set.

- **System Name**: Enter the system name.
- **Remote Access**: Switches on/off the SSH access to all DECT base stations of the DECT system. For more information on the SSH access see section 8.3.5.
- **Tone scheme**: Select the country in which the OMM resides. This enables country specific tones (busy tone, dial tone, etc).

5.4.1.2 DECT settings

- **PARK**: This setting depends on the licensing mode. Small systems: Enter the PARK code obtained from the PARK service (see section 4.1.3). License file: Shows the PARK included in the license file.

- **DECT power limit 100mW**: Limits the DECT base station transmit power to 100mW, independent of the selected regulatory domain. Enable for SIP-DECT installations that are mobile (e.g., on cruise liners that travel between countries). See section 3.11 for more information on this feature.

- **Encryption**: Activate this option if you want to enable DECT encryption for the whole system.

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

- **Restrict subscription duration**: Activate this option if you want to restrict the duration for DECT phone subscriptions to 2 minutes after subscription activation. This option is not useful in case that you want to subscribe more than one DECT phone at a time or together with auto-create on subscription. It should be activated exclusively in case that there is a special need.

- **DECT monitor**: For monitoring the DECT system behavior of the OpenMobility Manager, the separate DECT monitor application exists. This tool needs an access to the OpenMobility Manager which is disabled by default and can be enabled here. Because of security, the DECT monitor flag is not stored permanently in the internal flash memory of the OMM/DECT base station. After a reset, the DECT monitor flag is ever disabled.

- **Regulatory domain**: Specifies where the IP DECT is used. Supported regulatory domains are:
  – EMEA
  – US (FCC/IC)
  – Brazil
  – Taiwan

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

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

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

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

- **DECT authentication code**: The authentication code is used during initial DECT phone subscription as a security option. A code entered here provides a system-wide DECT authentication code for each DECT phone subscription. Alternatively, a DECT phone-specific authentication code can be set (see section 5.7.1).

- **DECT phone user login type**: Specifies the system-wide variant for DECT phone login method. Two kinds of login types are supported: the user can either be determined by the telephone number (**Number**) or by the unique user login ID (**Login ID**). Both elements are part of each user data set.

  Note: Changing this setting forces an automatic logout of all logged in DECT phones.
  In case, the OMM works within a system along with MOM or UDS, this will happen in all OMMs of this system.

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

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

5.4.1.3 WLAN settings

This setting applies to RFP 42 WLAN and RFP 43 WLAN base stations.

- **Regulatory domain**: Select the regulatory domain of the WLAN network. This setting depends on the country and is prescribed by the laws of that country. Only the setting prescribed for that country must be used. For more information on the WLAN settings see the sections 5.8 and 7.18.

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

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

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

5.4.1.4 DECT base stations update

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

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

- **Time**: Time for time controlled updates

5.4.1.5 Maximum delay

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

5.4.1.6 Calculated time of delay

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

5.4.1.7 OMP web start

- **Configure specific source**: Enables the specific URL to an external file server for retrieving the OMP jar file.

- **Protocol**: Specifies the protocol used to retrieve the OMP file.

- **Server**: Specifies the IP address or name of the external file server.

- **Port**: Specifies the port of the external file server.

- **Path**: Specifies the location of the OMP jar file on the external file server.

5.4.1.8 DECT phone's firmware update

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

- **Activate firmware update**: Enables or disables the "Download over Air" feature. The OMM provides a DECT phone firmware update over the air when this feature is activated. For more information on, see section 7.22.

- **Configure specific source**: Enables the specific URL to an external file server for retrieving the DECT phone firmware file.

- **Protocol**: Specifies the protocol used to retrieve the firmware file from the external server.

- **Server**: Specifies the IP address or name of the external file server.

- **Port**: Specifies the port of the external file server.

- **User name**: Specifies the user name to authenticate on the external file server.

- **Password**: Specifies the password to authenticate on the external file server.

- **Password confirmation**: Confirms the password to authenticate on the external file server.

- **Path**: Specifies the location of the firmware file on the external file server.

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

5.4.1.9 Voice mail

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

5.4.1.10   OM Integrated Messaging & Alerting service

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

- **Internal message routing (phone <> phone):** Enables or disables internal messaging between DECT phones.

- **Configure specific destination:** Enables the specific URL to an external file server for retrieving the IMA configuration file.

- **Protocol:** Specifies the protocol used to retrieve the IMA configuration file from the external server.

- **Server:** Specifies the IP address or name of the external file server.

- **Port:** Specifies the port of the external file server.

- **User name:** Specifies the user name to authenticate on the external file server.

- **Password:** Specifies the password to authenticate on the external file server.

- **Password confirmation:** Confirms the password to authenticate on the external file server.

- **Path & filename:** Specifies the location and file name of the IMA configuration file on the external file server.

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

5.4.1.11   Syslog

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

- **Active:** Enables or disables collection of syslog messages.

- **IP address:** Address of the host that should collect the syslog messages.

- **Port:** Port of the host that should collect the syslog messages.

- **Forward OMM Messages to syslog:** (Visible only on a PC-hosted OMM system) Enables/disables forwarding of syslog messages from the PC-hosted OMM.