SIP-DECT with Cloud-ID System Manual

ADMINISTRATION GUIDE

RELEASE 8.0

NOTICE

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

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

TRADEMARKS

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

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

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

SIP-DECT with Cloud-ID System Manual
Administration Guide
Release 8.0 - October 2018

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

CONTENTS

1 About this Document 7

2 SIP-DECT with Cloud-ID Solution 8

2.1 System components 8

3 Notes on Safety 10

3.1 Installation 10
3.2 Connection to the mains power supply 10
3.3 AC adapter 11
3.4 Cable 11
3.5 Usage 11

4 Getting Started 12

4.1 Installation Site 12
4.2 Initial Setup 13
4.2.1 Operational mode of additional RFPs 23
4.2.2 Migration from RFP3G SIP-DECT with Cloud-ID 7.1 23
4.2.3 Operate the former RFP3G OMM RFP in RFP-Only Mode 26
4.2.4 Operate RFP4G and RFP3G in one SDC installation 27

5 Network Configuration 28

5.1 Configuration via DHCP 28
5.2 Static network configuration 28
5.2.1 DECT Phone User Interface (UI) 30
5.2.2 Web User Interface 31
5.2.3 Intergrated DHCP Server 31
5.2.4 VLAN CONFIGURATION 32

6 Provisioning 35

6.1 SIP-DECT provisioning overview 35
6.2 Configuration file URL 36
6.3 System credentials 37
6.4 Configuration file URL 38
6.5 Daily automatic reload of configuration and firmware files 40
6.6 Certificates 42
6.7 Manual import of certficates 45
6.8 Secure Provisioning Certificate Server URL 45
6.9 Secure OMM Certificate Server URL 50

7 SIP Features 54

7.1 Basic SIP settings 54
7.1.1 Configuration of SIP settings via the Web UI 55
7.1.2 Configuration of the SIP proxy and registrar via the Phone UI 55
7.2 Advanced SIP settings 60
7.3 Real-time Transport Protocol (RTP) Settings 68
7.4 DTMF Settings 71
7.5 SIP telephony Issues 73
7.5.1 DECT phone, SIP user and expected available lines 73
7.5.2 SIP User "not registered" 74
7.5.3 Diversion indication 74
7.5.4 Call completed elsewhere 75
7.5.5 Call reject on silent charging 75

8 Mitel 600 DECT Phone Menu 76

8.1 "System" Submenu 76
8.2 "SIP Users/Devices" Submenu 77
8.3 Supported Languages 77

9 Status 78

10 System Settings 79

10.1 General 79
10.2 DECT Settings 80
10.3 WLAN 83
10.4 QoS Settings 83
10.5 Voice mail 84
10.6 OM Integrated Messaging & Alerting service 84
10.7 Syslog 88
10.8 Software update URL 88
10.9 System dump 89
10.10 Core dump URL 90
10.11 Date and time 91

11 Advanced SIP Operational Features 92

11.1 DNS SRV 92
11.2 Backup SIP Proxy/Registar 93
11.3 Backup Keep Alive 98
11.4 Register Redirect 99
11.5 SRTP 100
11.6 SIP over TLS 101
11.6.1 Certificates 103
11.6.2 Private Key 104
11.6.3 TLS Transport Mode 104
11.6.4 Verification of Remote Certificates 104
11.6.5 Additional Security Considerations 105
11.6.6 Manual import of SIP certificates 105
11.6.7 Automatic import of SIP certificates 106
11.7 Registration Traffic Shaping 111
11.8 Conferencing 112
11.9 Supplementary Services 114
11.10 Auto Answer, Intercom Calls and Audio Settings 117
11.10.1 Intercom Calls 117
11.10.2 Auto Answer Audio Settings 118
11.11 X-Aastra-Id 120

12 User Administration 122

13 Time Zones 126

13.1 Time Zones Configuration 126
13.2 Resetting Time Zones 128

14 SNMP 129

15 Database Management 131

15.1 Manual Database Import 132
15.2 Manual Database Export 132
15.3 User data import 133

16 Event Log 135

17 Base Stations 136

17.1 Installation of additional Base Stations 136
17.2 Register New Base Stations 137
17.2.1 OMM Discovery 137
17.2.2 Manual Registration 138
17.3 Web Service Base Stations Menu 140
17.3.1 Base Station States 140

18 SIP Users/Devices 142

18.1 Users 142
18.1.1 User Configuration Files 142

18.1.2 User Configuration 143
18.2 Devices 160
18.2.1 Create / Delete devices 160
18.2.2 Subscribe devices 160
18.2.3 Unsubscribe Devices 162
18.3 User Login / Logout 163
18.3.1 Login procedure 163
18.3.2 Logout procedure 164
18.4 Wireless LAN (WLAN) 165
18.4.1 802.11i: WPA2-Enterprise Pre-Authentication for fast Roaming 165
18.4.2 Creating and Changing WLAN Profiles 166
18.4.3 WLAN configuration steps (RFP 48 WLAN) 166
18.5 WLAN Regulatory Domain 168
18.6 WLAN Profiles 169
18.6.1 General settings 169
18.6.2 Security settings 170
18.6.3 Key settings 171
18.6.4 Radius settings 171
18.6.5 QoS settings 172
18.6.6 Additional SSID 172
18.6.7 MAC access filters 172
18.7 Base Stations 172
18.8 WLAN Clients 173

19 Digit Treatment 174

19.1 Creating and Changing “Digit treatment” Entries 175
19.2 Deleting “Digit treatment” Entries 175

20 Directory 176

20.1 Creating and Changing Directory Entries 176
20.2 Deleting Directory Entries 180

21 Feature Access Codes 181

22 XML Applications 185

22.1 Built-in XML Applications 185
22.1.1 Feature Access Code Translation 186
22.1.2 Built-in XML Applications Configuration 186
22.2 Additional XML Applications 193
22.3 Integration of Corporate Directories 194
22.4 Support “SIPProxy” Placeholder in XML Hooks 194
22.5 XML Terminal Interface Extensions 195
22.5.1 CTI Call Answer 195
22.5.2 Auto Answer, Intercom Calls and Audio Settings 195

23 Central DECT Phone Configuration Over Air (CoA) 196

23.1 Download of Configuration Files to DECT Phones 197
23.2 Variable lists 197
23.2.1 Icon coding 200
23.2.2 Number string coding 201
23.3 Default CoA Profile Configuration 202
23.4 CoA Profile Configuration 203
23.5 User-Specific CoA Configuration 204
23.6 States of CoA Configuration Settings 204
23.7 COA Configuration Parameters 206
23.7.1 Configuration of Variable Lists 206
23.7.2 Extended COA Examples 207
23.7.3 Example 1 207
23.7.4 Example 2 208
23.7.5 Example 3 211
23.7.6 Example 4 211
23.7.7 Example 5 213

23.7.8 Supported COA Parameters 214

24 Consolidated Certificate Management 243

24.1 SIP over TLS certificates 243
24.2 OMM Certificate (Web service) 243
24.3 Provisioning certificates 243
24.4 Certificate validation 243

25 Regulatory Compliance and Safety Information 245

25.1 MITEL RFP44/45/47/48 245
25.2 Communications Regulation Information for RFP 35, RFP 36 and RFP 37 245
25.2.1 FCC Notices (U.S. Only) 245
25.2.2 Industry Canada (Canada only) 246
25.3 Supporting Documentation 246
25.4 Declaration of Conformity 246

26 Appendix 247

26.1 Abbreviations 247
26.2 Definitions 248
26.3 References 249
26.4 Protocols and Ports 251
26.5 Radio Coverage Area 253
26.5.1 Radio Propagation Conditions 253
26.5.2 Disclaimer 255

1 ABOUT THIS DOCUMENT

This document describes the installation / configuration, administration, and maintenance of the SIP-DECT with Cloud-ID solution. Please also see the documents listed in the References section (section 27.3) for additional details on different aspects of the SIP-DECT system.

2 SIP-DECT WITH CLOUD-ID SOLUTION

The SIP-DECT with Cloud-ID (SDC) solution is a variation of the full SIP-DECT solution, designed for small and medium-sized service provider environments (5 to 10 DECT base stations). This limits the need for site survey and for changes to the configuration of the IP network.

The SDC solution provides the proven SIP-DECT network with a focus on simplified provisioning and reduced complexity. With centralized auto-provisioning from the cloud, installation and set-up is fast and easy, with minimum effort required at the customer site.

The SDC solution features the following:

- Standard DHCP client to obtain basic network parameters
- Simplified administration (on the DECT phone interface and via the Web Portal)
- Base station auto-discovery that allows other DECT base stations in the same LAN to discover the OMM automatically, to be combined into one DECT multi cell network
- Integrated Messaging and Alerting (IMA) service

The SDC solution supports the standard SIP-DECT feature set, but does not support additional licensed services (e.g., enhanced Messaging, Locating), or redundant (standby) OMM systems. In addition, there is no support for external applications over the OM AXI interface (e.g., OMP, Alarm Server).

2.1 SYSTEM COMPONENTS

The SIP-DECT with Cloud-ID solution includes the following main components:

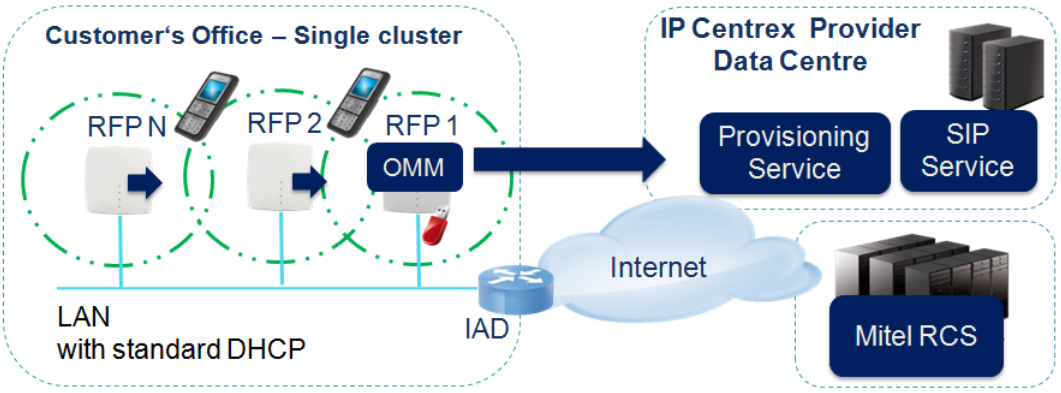
- SIP-DECT base stations (also known as Radio Fixed Parts, or RFPs) that are distributed over an IP network and offer DECT and IP interfaces (currently supported DECT base stations: RFP44/45/47/48 as OMM and RFP; RFP35/36/37/43 as RFP only).
- DECT phones (portable DECT devices); currently supported devices include Mitel 602 DECT phone family.
- OpenMobility Manager (OMM): Management and signaling software for the SIP-DECT solution, which runs on the DECT base station assigned to be the OMM thorugh the RFP Configuration button.
- A SIP Call Manager (for example, Asterisk).

The SIP Call Manager, OMM and the DECT base stations communicate through the IP infrastructure. The DECT base stations and 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 DECT base stations.

Additional components include:

- LDAP server to facilitate a central corporate directory
- Provisioning server to provide OMM configuration and resource files
- Data backup server to backup or restore an OMM database from the server
- Computer for administration and maintenance tools: Web browser

The following figure shows the main components of the SIP-DECT with Cloud-ID solution.



OMM = OpenMobility Manager
RFP = DECT base station
RCS = Redirection and Configuration Service
IAD = Internet Access Device e.g. NAT Router
= Cloud-ID USB flash drive for OMM

3 NOTES ON SAFETY

Please note: See the notes on Safety for the DECT base stations provied with the ”Regulatory Compliance and Safety Information”.

Please note: Also, see the notes on safety for the DECT phones provided in the “Mitel 600 Series DECT Phone User Guide”. This user guide is available for download on the Mitel website.

3.1 INSTALLATION

The RFP44/45/48 and RFP35/43 base station may only be installed inside buildings and should be operated when mounted on a wall.

Do not install the base station during a thunderstorm. Do not connect and disconnect lines during a thunderstorm.

CAUTION!	Static charges can damage the base stations electronic components. Please make sure that you discharge yourself and your tools before and during any installation work on the base station.	

3.2 CONNECTION TO THE MAINS POWER SUPPLY

The base station may only be plugged into mains power sockets that have a protective earth conductor. It is not necessary to provide any additional earthing for the base station.

Recommendation: Connect the base station to a separate power circuit so that short circuits occurring in other devices do not put the base station out of operation. The mains power connection must be installed by a licenced electrician to avoid danger to people or materials!

DANGER!	Hazardous voltages inside the device! The RFP35/RFP43 base stations may not be opened as this may lead to exposure to hazardous voltage! The RFP36/RFP37 base stations should not be attached to a Power over Ethernet switch while opened for installation purposes.

The base station does not have its own power supply switch. To disconnect the base station from the mains power supply, pull the plug out of the power socket or disconnect the Ethernet cable in case of PoE supply.

3.3 AC ADAPTER

The base station supports PoE (Power over Ethernet), Class 3, if provided. For RFP35/RFP43 alternatively you can use the provided AC adapter.

Use only the AC adapter provided to connect an RFP35/RFP43 to the mains power supply. Other AC adapters may cause malfunctions or electric shock and damage the base station.

CAUTION!	Never start or operate the RFP35/RFP43 if the AC adapter is damaged. Serious danger to life from electric shock may result.

3.4 CABLE

Ensure that all cables are laid in such a way that nobody can walk on or trip over them.

Use a shielded Ethernet cable (STP cable, Shielded Twisted Pair cable) to connect the base station to a local network (LAN, Local Area Network).

3.5 USAGE

Make sure no fluids get into a base station: Electric shock or short circuit may result.

Repairs to the base station and all its accessories must be carried out by accredited specialists. Inappropriate repairs may damage the base station and will render any warranty claims invalid.

Keep the base station and its accessories and packaging out of reach of children!

4 GETTING STARTED

4.1 INSTALLATION SITE

The SIP-DECT with Cloud-ID base station is a device that enables the operation of DECT phones and WLAN clients (depending on the base station type). The base station must establish and maintain a digital radio connection to all DECT Phones and WLAN clients. To find a suitable installation site, you should consider the following:

- **Environment**: The base station RFP 44/45/48 (RFP35/RFP43) operates in standard indoor conditions. This means that you should not expose the device to heat, coldness, or moisture that exceeds the conditions specified (refer to the appropriate datasheets). Also remember the notes on safety stated in chapter 3.
  For environmental conditions for the RFP4x IP66 rated external housing and outdoor RFP36/RFP37 base stations (usable as extension base stations only) refer to the appropriate datasheets.
- **Connectivity**: The base station must be connected to the network by means of a wired Ethernet connection. Also, you must provide a power supply by PoE (Power over Ethernet).
- **Radio Coverage**: Due to the coverage / supply range of radio waves, you should select the installation site carefully:
  - Place the base station at the center of the area which shall be covered by the system.
  - An ideal location for installing the base station is a height of between 6.6 ft and 8.2 ft (2 m and 2.50 m) for room heights between 8.2 ft and 9.8 ft (2.50 m and 3 m). For higher rooms, the ideal installation height increases accordingly while maintaining a minimum ceiling distance of 1.6 ft (0.50 m). An installation height of less than 4.9 ft (1.50 m) is not recommended. Installation inside a dropped ceiling, cabinets or other enclosed furnishings is not recommended as this considerably impairs the radio range.
  - Do not mount the base station directly on metal surfaces. If possible keep a distance of at least 1 ft (30 cm) distance from metal constructions (e.g. steel beams, metal walls, metal coated glass etc.)
  - Do not mount the base station close to electric power distribution systems.
  - Do not mount the base station close to other radio emitting devices (WLAN, other DECT base stations). Keep a distance of at least 1.6 ft (50 cm) vertical and 6.5 ft (2m) horizontal distance)

See section 27.5 for more detailed information about the influence of the environment to radio wave propagation.

The RFP35/RFP43 base station is mounted on the wall with two screws. Please use the drilling template included with the base station.

4.2 INITIAL SETUP

The following sequence describes the steps required to prepare the base station and DECT phone for receiving/making phone calls. The following steps assume there is a DHCP server running in the LAN (usually provided by the internet access router).

The 4th generation RFPs are not equipped with an USB interface. Therefore, SIP-DECT 8.0 does not support the Cloud-ID stick anymore and a 4th generation HW is required, to run the OMM in the SDC mode.

1 Unpack the Mitel RFP kit.

2 Remove the back cover of RFP carefully.

3 Insert the Ethernet cable into the port.

4 Press the RFP button located at the center.

5 The LED turns to Red indicating that power is On and booting phase is started.

6 After few seconds, the LED turns to Yellow at the startup phase.

7 When the LED turns to Magenta, it indicates that the system is UP and running.

8 Press the Configuration button to appoint RFP to the OMM RFP and switch to SDC mode (SIP-DECT with Cloud-ID mode). The LED starts flashing green indicating that the button is pressed.

9 Keep the button pressed until it starts flashing blue (approximately 5 seconds).

10 Release the button while the LED is flashing blue to switch to SDC mode.

The RFP performs a reset to factory defaults and reboots. After reboot, the OMM is started and the SDC mode is set.

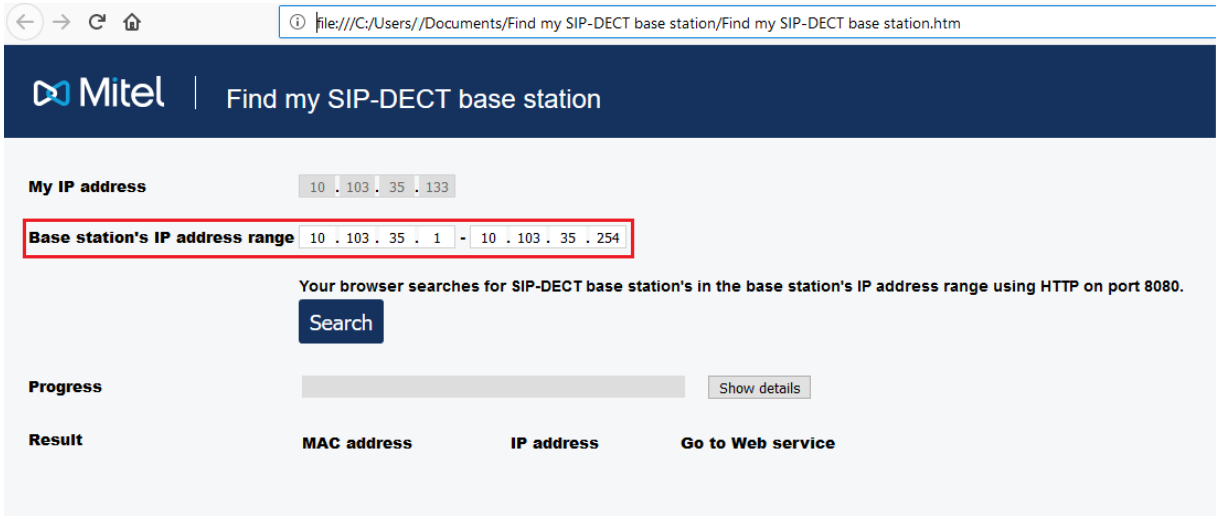
Note: If the button is pressed until it is flashing green again, then the button has no effect.

11 Determine the RFP's/OMM's IP address and connect to the OMM's Web service after the startup phase (LED: yellow).

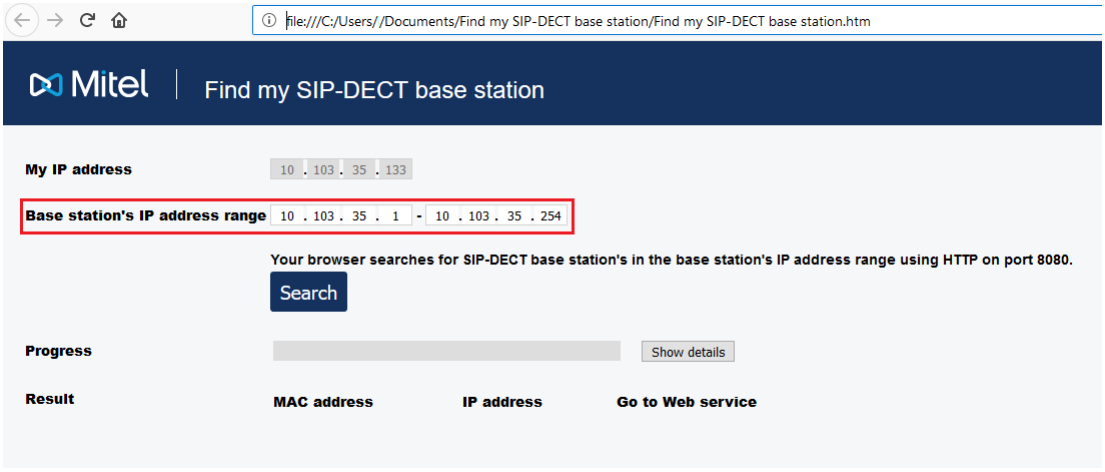
Note: If the IP address cannot be determined, then the java script "Find my SIP-DECT base station" can be used.

The java script of "Find my SIP-DECT base station" is executed in a Web browser from a local drive. Download and extract the FindMySIP-DECTbasestation.zip and open the index.html.

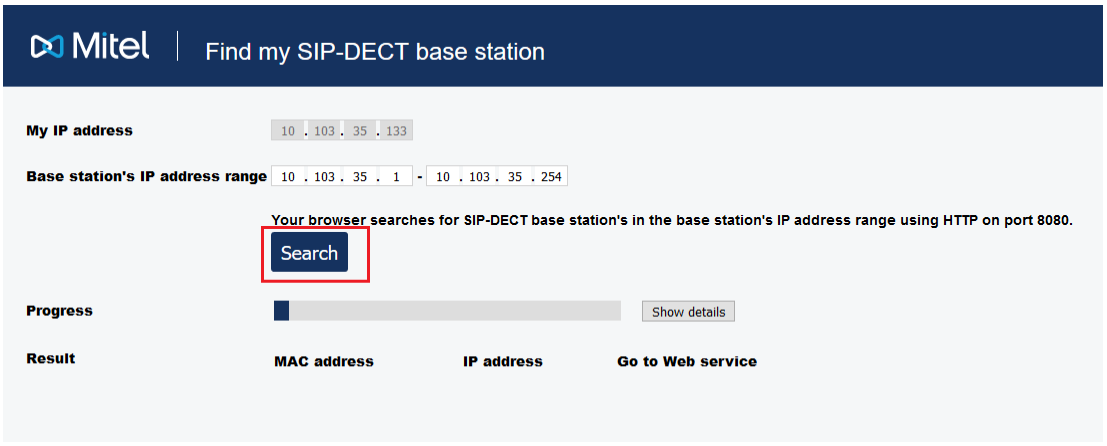
12 Open "Find my SIP-DECT base station" in your Web browser from the URL or from the extracted zip archive.



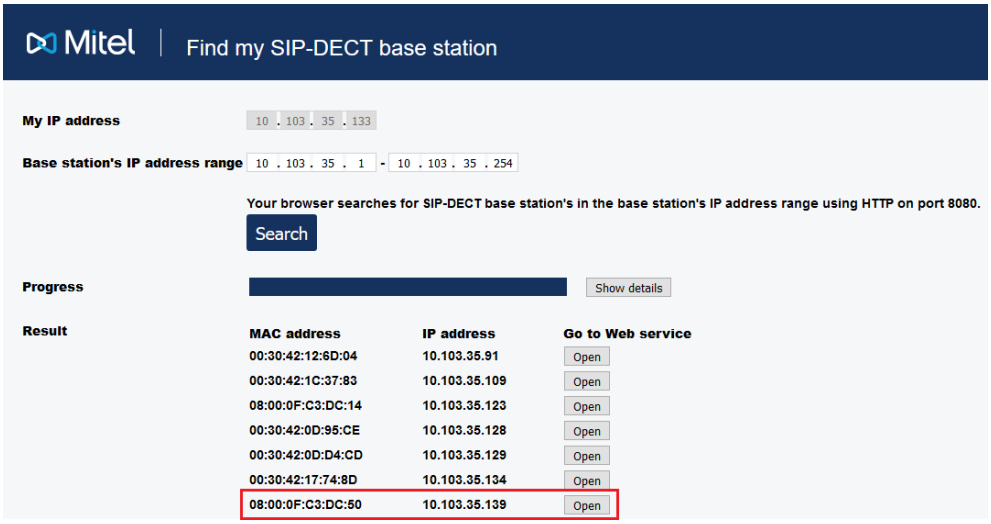
i) Check and adjust the **Base srations' IP address range** if necessary.



ii) Click the **Search** button and wait for results.



iii) Select the RFP's **MAC address** and click **Open** button to connect to the OMM's Web service.

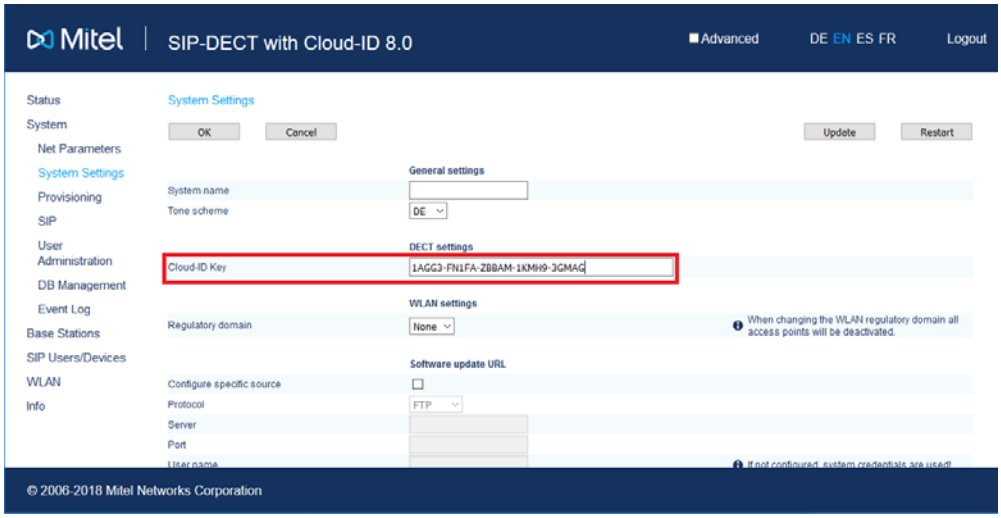


13 Login at the OMM's Web service.

14 Use the default login and password and bookmark link to the OMM's Web service.

15 Click **Accept** button to confirm EULA.

16 Enter the **Cloud-ID key** to set Cloud-ID, PARK and **Regulatory domain**.

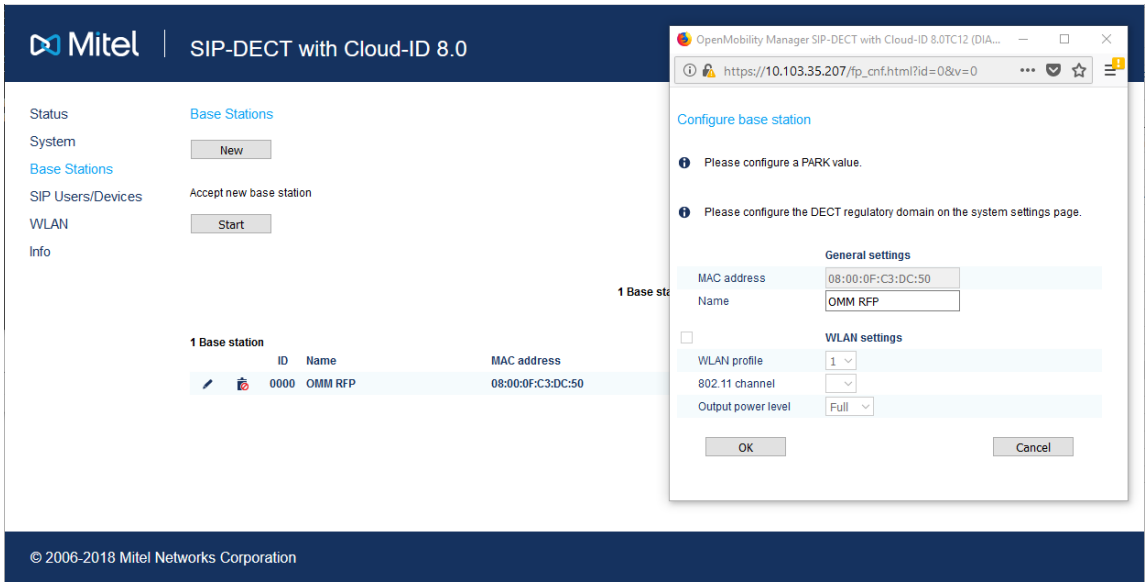


17 The RFP automatically restarts after applying a valid Cloud-ID Key.

18 After restart, the PARK is display at the Web server and the DECT air interface is active. The active DECT interface is indicated by a green LED.

Note: The RFP and OMM have the same operational status as the previous RFP generation after the USB stick is plugged, which causes a SW update to the SDC SW that appoints the RFP to be the OMM RFP and the Cloud-ID and applies the PARK and regulatory domain from the Cloud-ID.xml file.

Also, note that the following notices regarding PARK and DECT regulatory domain is displayed as long as no Cloud-ID key is applied.



19 Assemble and switch on a new Mitel 600 DECT Phone.

For detailed instructions on this topic, please refer to the “Mitel 600 Series DECT Phone; User Guide”/31/. Briefly, proceed in the following order:

- **Unpack the DECT phone**: Unpack the DECT phone from its packaging. The box contains a DECT phone, a battery, a DECT phone charger cradle, a plug-in power supply, and a number of interchangeable AC clips for different countries.
- **Connect the power supply**: Select the AC clip that matches your mains wall sockets. Insert the AC clip into the DECT phone’s plug-in power supply. Make sure the AC clip is firmly inserted and locked. Insert the low voltage connector of the plug-in power supply into the socket of the DECT phone charger cradle. Connect the plug-in power supply to a mains power socket.
- **Insert the battery**: Open the DECT phone’s rear battery compartment. Insert the battery. Close the DECT phone’s rear battery compartment.
- **Charge the DECT phone**: Place the DECT phone into the charger cradle.
- The DECT phone’s signalling LED lights red after some seconds, indicating that the battery is charging. A full charging cycle takes up to 2.5 hours. The DECT phone’s signalling LED lights green to indicate a fully charged battery.

20 Subscribe the DECT Phone using the system authentication code (e.g., 22222) within 60 minutes after power up of the base station.

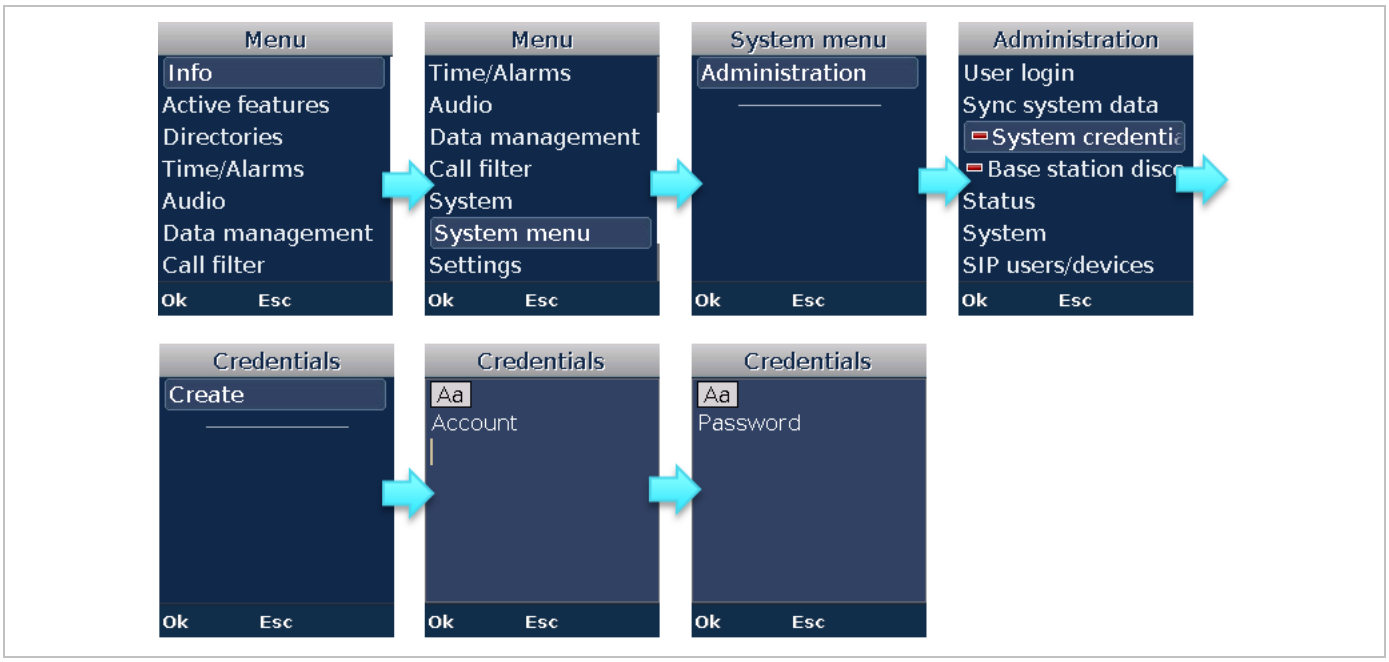
21 The following workflow is based on a scenario where provisioning is used. If the provisioning server requires system credentials, you must enter them to authenticate the SIP-DECT with Cloud-ID (SDC) system at the provider services.

22 To provide the SIP-DECT provisioning system credentials, you can use one of the following:

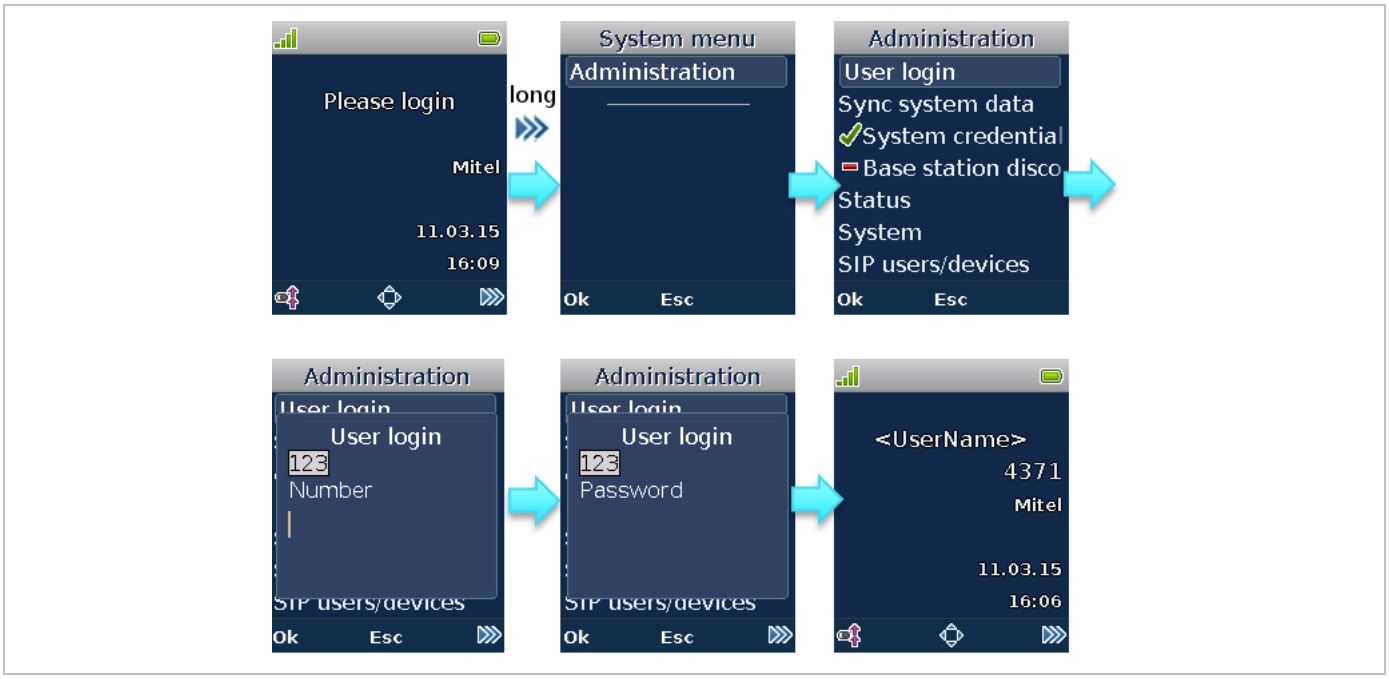
- The WEB service System/Provisioning page (see the following figure).

- The DECT phone as follows:

  Press the menu softkey and follow the sequence shown in the following figure. If you press and hold the menu softkey, the **System** menu opens immediately.



23 Perform a user login at the DECT phone to authenticate the user with the provider services. Open the **System menu** (press and hold the menu softkey) and select **Administration** -> **User login**:



The user can now make and receive calls. In addition, the following steps can be performed on the customer side:

- Subscribe DECT phones and perform user logins to authenticate the user with the provider services.
- Connect more DECT base stations to the LAN segment to extend the DECT coverage as described in chapter 17.1.

4.2.1 OPERATIONAL MODE OF ADDITIONAL RFPS

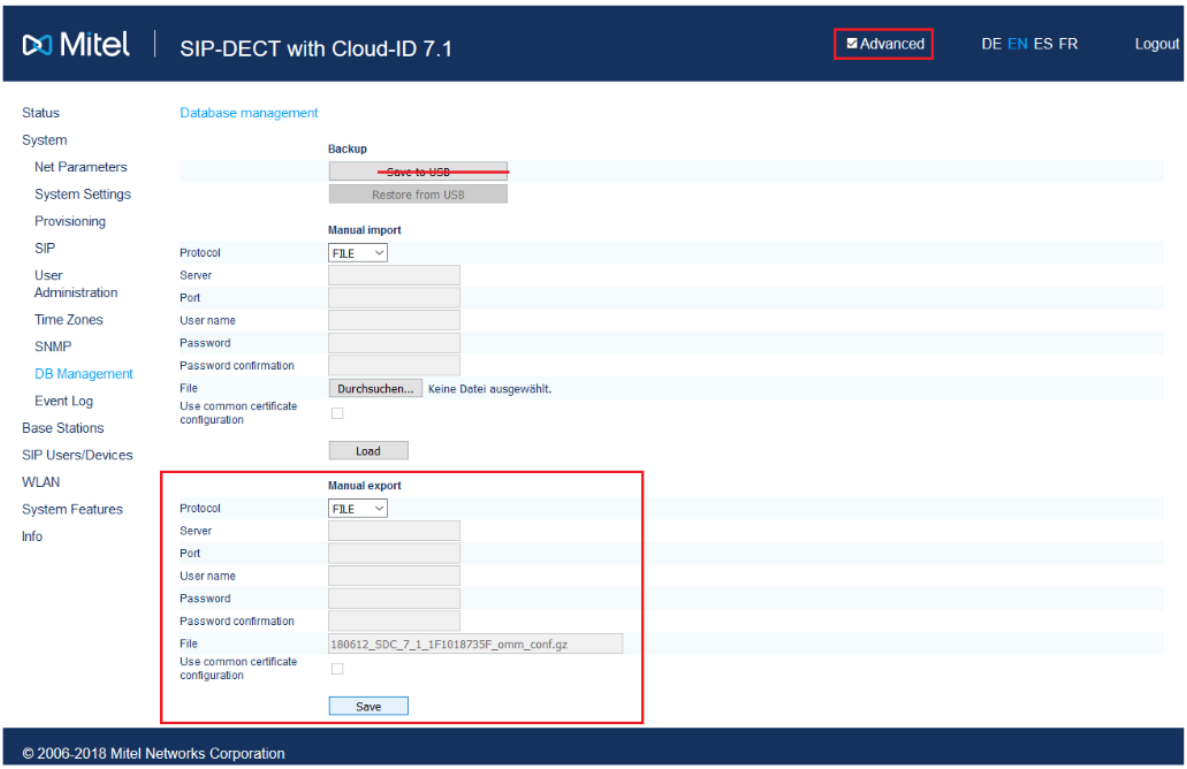
The operational mode “SIP-DECT” or “SDC” of additional RFPs within an installation is managed by the OMM.

If the mode is unknown and if there is no OMM to connect to, then the RFP can be reset to factory defaults through the Configuration button.

4.2.2 MIGRATION FROM RFP3G SIP-DECT WITH CLOUD-ID 7.1

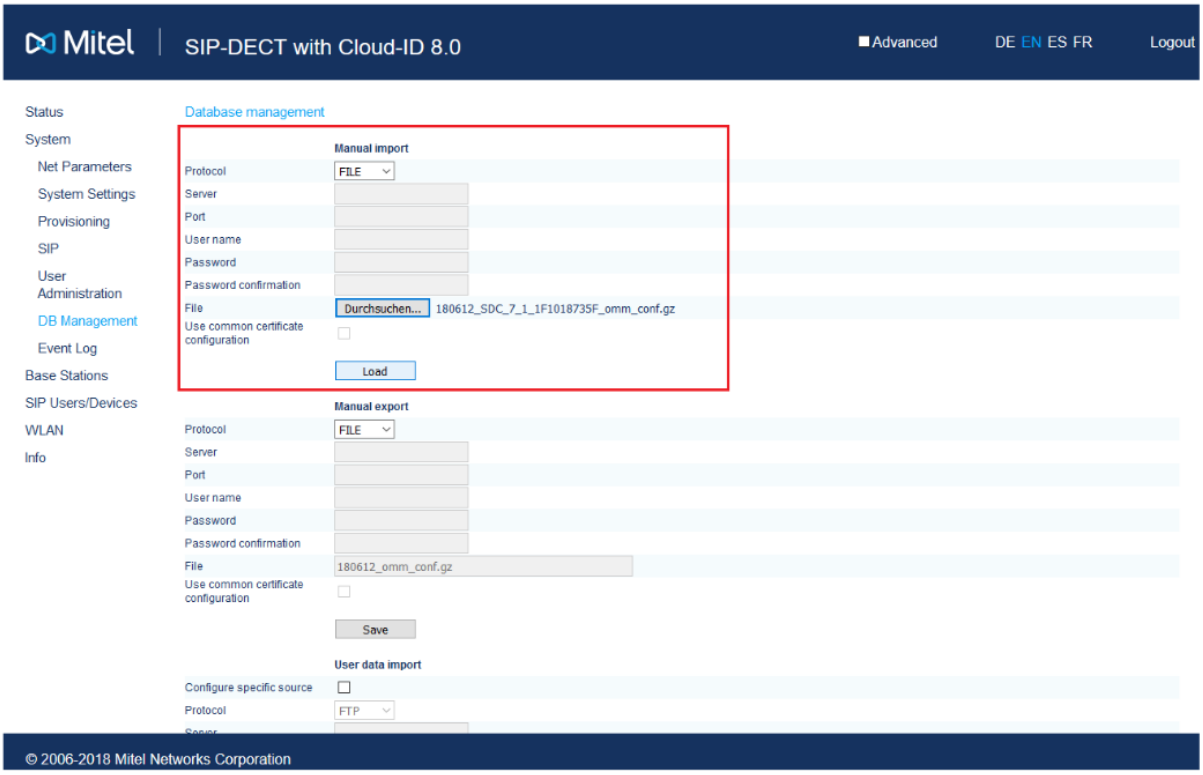
This section describes the migration from RFP3G SIP-DECT with Cloud-ID 7.1 to RFP4G SIP-DECT with Cloud-ID 8.0. No Cloud-ID key is required to migrate from a RFP3G SIP-DECT with Cloud-ID system to RFP4G SIP-DECT with Cloud-ID as the relevant data Cloud-ID, PARK and DECT regulatory domain are stored in the OMM database.

4.2.2.1 Creating OMM DB backup from RFP3G SIP-DECT with Cloud-ID 7.1



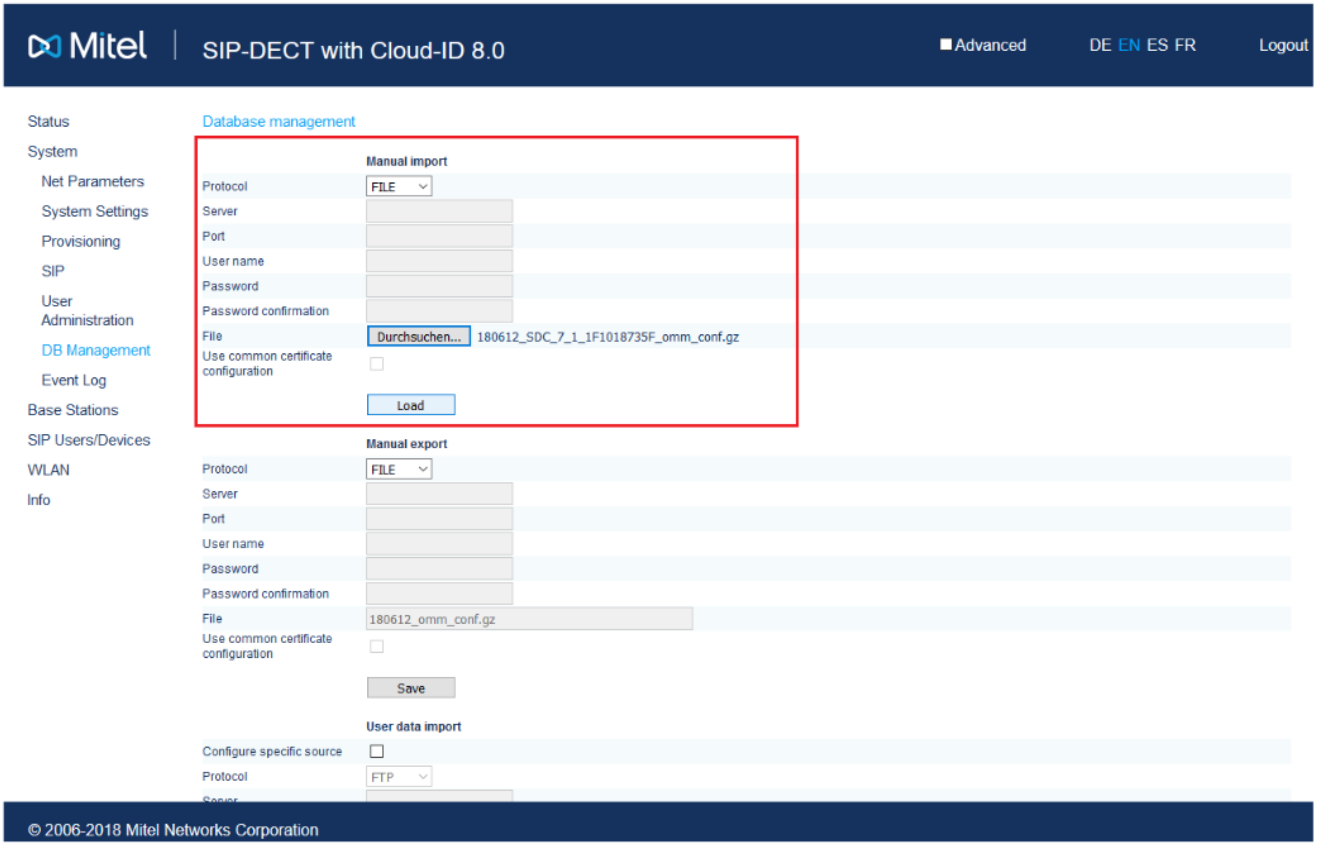
1. Use the Manual Export option to save the RFP3G SIP-DECT with Cloud-ID 7.1 data backup on your PC.
2. Save to USB” cannot be used as the RFP4G cannot restore the backup from USB.

4.2.2.2 Initiating of RFP4G as a SIP-DECT with Cloud-ID OMM



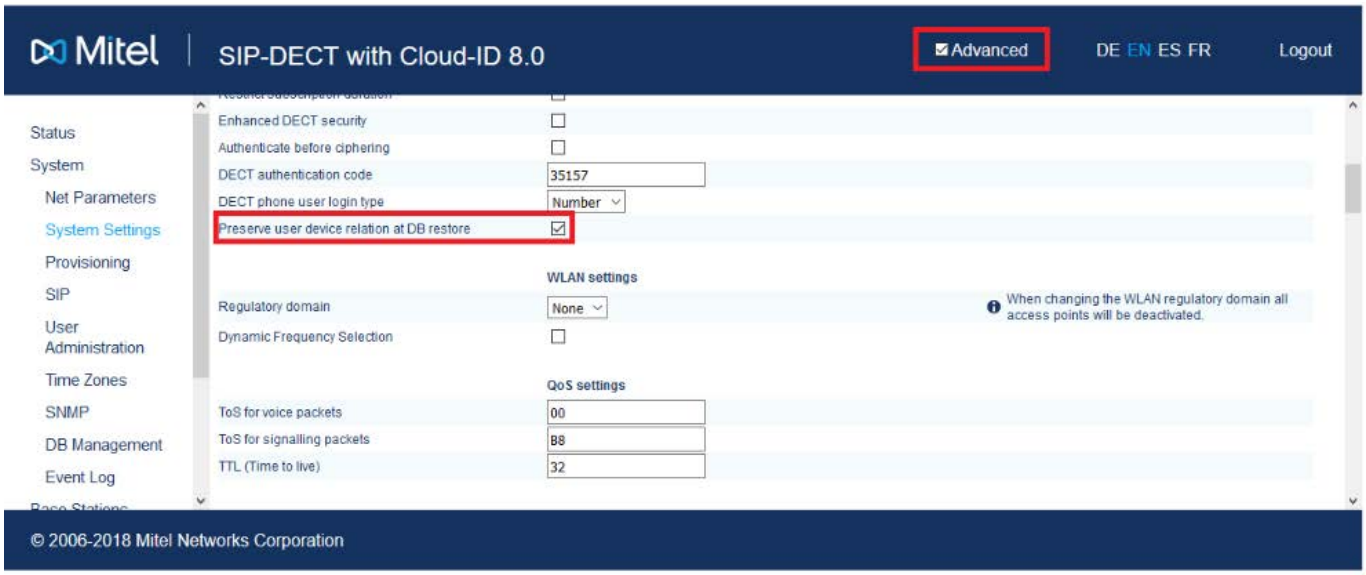
See the section 4.2 “Initial Setup” to execute all steps as described including to confirm the EULA. Stop the process before “Enter Cloud-ID key to set Cloud-ID, PARK and regulatory domain”.

4.2.2.3 Applying the OMM DB backup from RFP3G SIP-DECT with Cloud-ID 7.1 to the RFP4G SDC OMM



Note: Activate the option **Preserve user device relation at DB restore** in the new OMM. The new OMM restores the relation between the user and the DECT phone during DB import. If this option is not set, then all dynamic users get logged out from their DECT phones when importing the OMM DB into the new OMM.

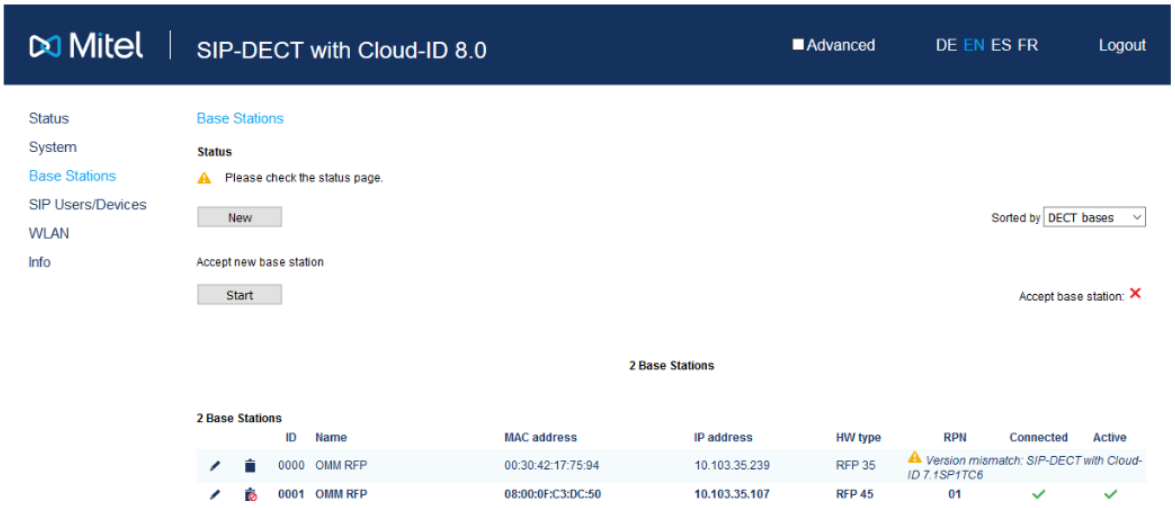
Keep the SIP-DECT with Cloud-ID 7.1 OMM out of operation, as it is not possible for two SDC systems with the same identification at the same time.



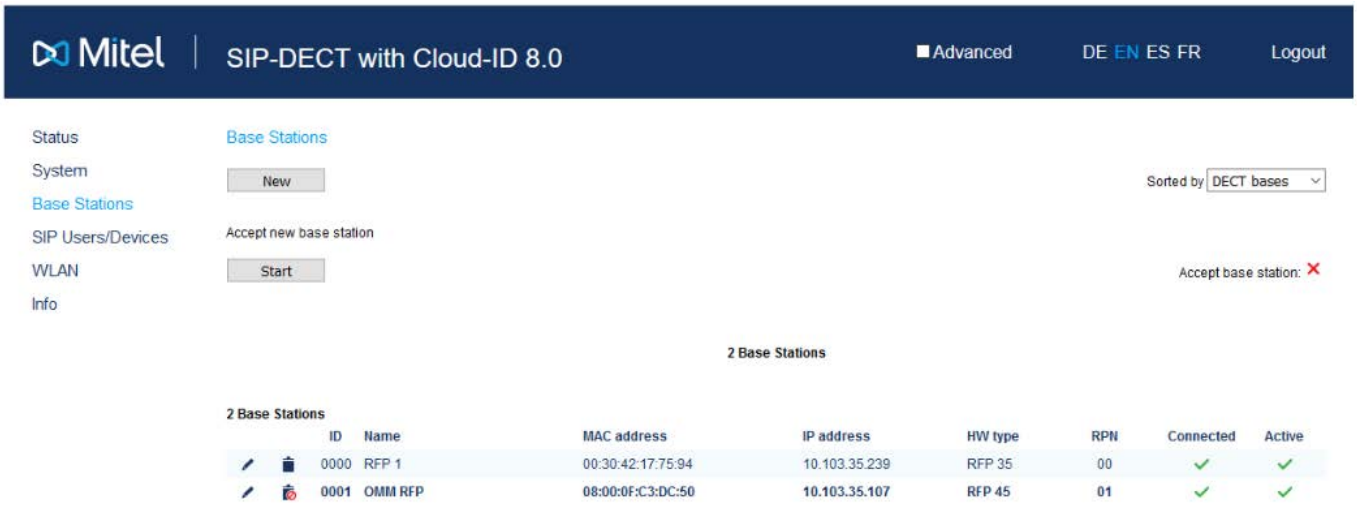
4.2.3 OPERATE THE FORMER RFP3G OMM RFP IN RFP-ONLY MODE

The RFP3G, which were housing the SIP-DECT with Cloud-ID 7.1 OMM, can be operated in an RFP-only mode with the new RFP4G SDC OMM. This requires resetting the RFP3G to factory defaults, so that the RFP does not house its own OMM anymore. After reset, the RFP can be operated as any other RFP with the RFP4G SDC OMM.

The RFP automatically finds the new OMM, performs a SW update to SIP-DECT 8.0 and is put into operation.



Before the SW update, the OMM reports a SW version mismatch.

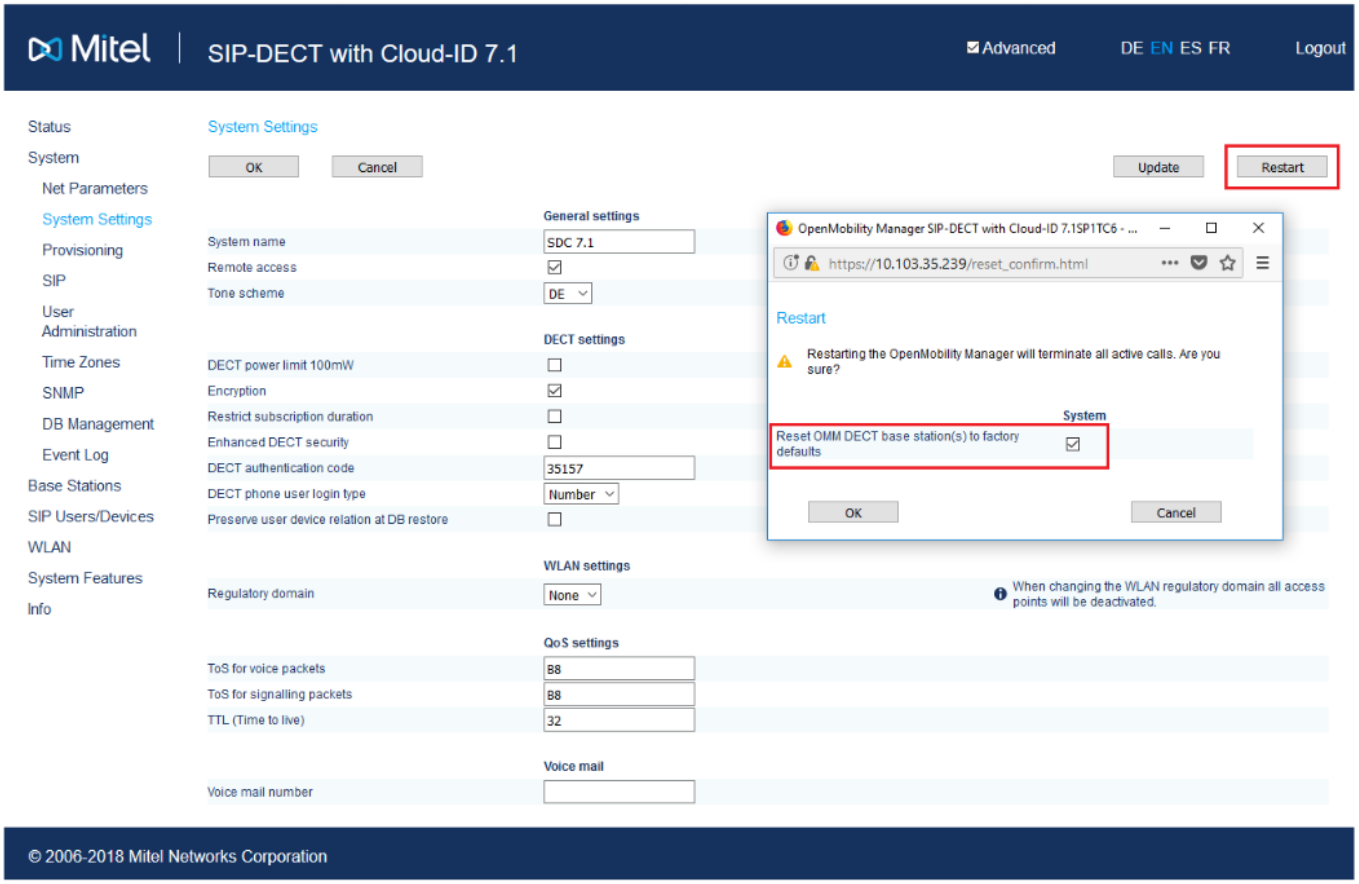


After the automatic SW update, the SW version mismatch disappears, and the RFP is automatically put into operation. The name of the previous OMM RFP can be changed to avoid confusion.

There are two options available to reset the RFP3G to factory defaults:

1. Reset to factory defaults via the OMM's Web service.
2. Reset using the USB stick.

4.2.3.1 Reset to factory defaults through the OMM's Web service



Execute the reset to factory defaults via the Web service of the SIP-DECT with Cloud-ID 7.1 OMM.

Ensure that you have removed the USB Cloud-ID stick from the RFP right after the reset is initiated to avoid that the RFP reads again the information from the stick during startup.

4.2.3.2 Reset using the USB stick

Create a file "factoryReset" on the USB Cloud-ID stick. This file must not have a file extension. Plug the stick in the RFP which houses the SIP-DECT with Cloud-ID 7.1 OMM. Remove the USB stick right when the RFP restarts to avoid that the RFP reads again the information from the stick during startup.

4.2.4 OPERATE RFP4G AND RFP3G IN ONE SDC INSTALLATION

As of SIP-DECT 8.0, the OMM in the SDC mode can only be operated on a 4th generation RFP (RFP4G). 3rd generation RFPs (for example, RFP 35), and 2nd generation RFPs (for example, RFP 32) can not be used as OMM, just RFP-only mode is possible.

As in previous releases, the OMM RFP provides SW updates to the other RFPs of the installation. SW updates are supported for both RFP generations, RFP4G and RF3G. This is possible since the RFP4G SW image (iprfp4G.dnld) includes the RFP3G SW image.

5 NETWORK CONFIGURATION

The network configuration of the SIP-DECT with Cloud-ID DECT base station is usually done via DHCP. Therefore, a standard DHCP server is required in the network where the base station is attached.

Additional base stations in the system are always configured using DHCP. Static network configuration of these base stations is not possible. If there is no DHCP server in the network, the internal DHCP server of the OMM can be configured so that additional base stations obtain their network configuration via DHCP.

The OMM internal DHCP server provides IP address to SIP-DECT base stations only.

5.1 CONFIGURATION VIA DHCP

Without a static network configuration, the base station starts a DHCP client and accepts the standard DHCP offer from a server using the following parameters:

- IP address
- Netmask
- Gateway
- DNS server
- DNS domain

The base station signals a successful network configuration via a green LED1. The SIP-DECT with Cloud-ID base station interrupts the continous green with a short orange flash, signaling that the base station is hosting the OpenMobility Manager.

You can verify the network configuration of the SIP-DECT with Cloud-ID base station from the DECT phone interface.

1. Press and hold the the **softkey in idle mode to open the System menu (or press the** softkey and select **System menu**).
2. Use the down navigation key to select the **Administration** menu.
3. Use the down navigation key to select the **Status** menu.
   The network configuration in effect is displayed.

5.2 STATIC NETWORK CONFIGURATION

A static network configuration is possible for the OMM. The static network configuration can be done only after the initial setup using DHCP. The Web interface or the DECT phone interface can be used.

Parameter / Parameter group	**Local network configuration**
Description	Activate or deactivate the Local network configuration. If disabled, DHCP (default) is performed.
Format	boolean
Range	“on” or “off”
Default value	“off”
Web	System / Net Parameters

OMM Configuration files	n.a.
DECT Phone	System menu / Administation / System / Net parameters / Static config
User configuration files	n.a.

Parameter / Parameter group	**IP address**
Description	The IP address of the SIP-DECT with Cloud-ID RFP
Format	IP address
Range	valid IP address
Default value	n.a.
Web	System / Net Parameters
OMM Configuration files	n.a.
DECT Phone	System menu / Administation / System / Net parameters / Static config.
User configuration files	n.a.

Parameter / Parameter group	**Net mask**
Description	The netmask of the SIP-DECT with Cloud-ID RFP
Format	IP netmask
Range	valid IP netmask
Default value	n.a.
Web	System / Net Parameters
OMM Configuration files	n.a.
DECT Phone	System menu / Administation / System / Net parameters / Static config.
User configuration files	n.a.

Parameter / Parameter group	**Gateway**
Description	The IP address of the default router or gateway to use
Format	IP address
Range	valid IP address directly reachable using the IP address/netmask
Default value	n.a.
Web	System / Net Parameters
OMM Configuration files	n.a.
DECT Phone	System menu / Administation / System / Net parameters / Static config.
User configuration files	n.a.

Parameter / Parameter group	**DNS server**
Description	The IP address of the DNS server to use
Format	IP address

Range	valid IP address
Default value	n.a.
Web	System / Net Parameters
OMM Configuration files	n.a.
DECT Phone	System menu / Administation / System / Net parameters / Static config.
User configuration files	n.a.

Parameter / Parameter group	**DNS search domain**
Description	The IP address of the gateway to use
Format	string
Range	Space separated list domain
Default value	n.a.
Web	System / Net Parameters (Advanced mode)
OMM Configuration files	n.a.
DECT Phone	n.a.
User configuration files	n.a.

5.2.1 DECT PHONE USER INTERFACE (UI)

1. Press **longer** when idle or press **briefly** when idle. Select **System menu**.
2. Use the down navigation key to select the **Administration** menu.
3. Use the down navigation key to select the **System** menu.
4. Login with the Full access User name and Password (see section 12 “User Administration” for information on default login credentials).
5. Use the down navigation key to select the **Net parameters** menu.
6. Use the down navigation key to select the **Static config.** menu.
7. Enter values for the following parameters:
   - IP address
   - Net mask
   - Gateway
   - DNS0
   - DNS1
   - DNS2

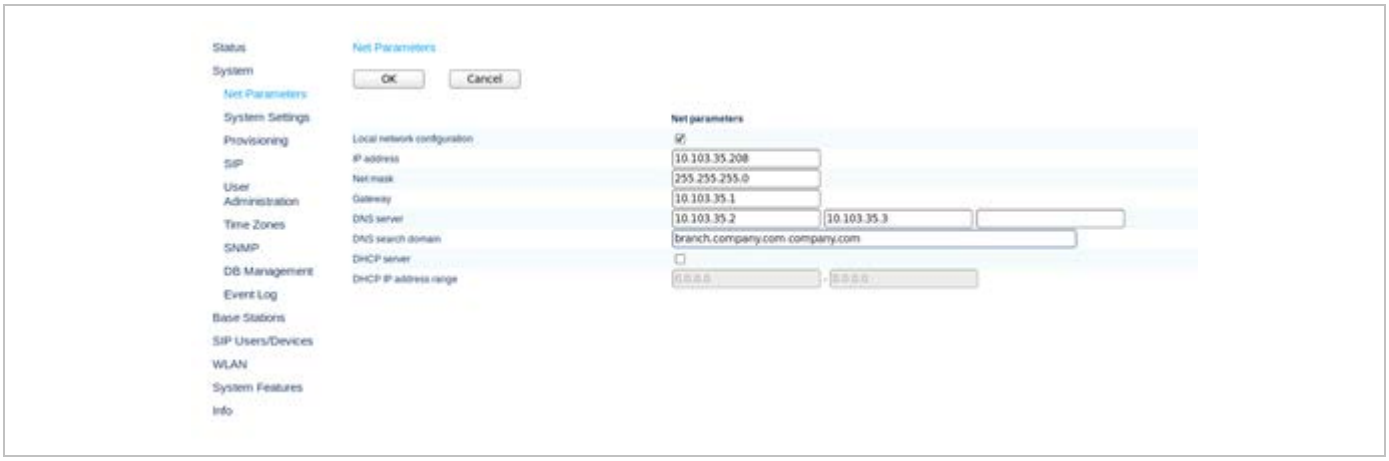
Changes to network parameters trigger a restart of the OpenMobility Manager and therefore result in a loss of DECT phone connection.

5.2.2 WEB USER INTERFACE

Systems with IP connectivity support reconfiguration using the Web service. When you login with the **Full access** account, you can configure the system network parameters (see section 12 “User Administration” for information on default login credentials).

1 Navigate to the **System > Net Parameters** menu in the left panel of the window, and activate the **Advanced** checkbox in the top bar.

2 Configure the network parameters and click **OK** to confirm your changes.

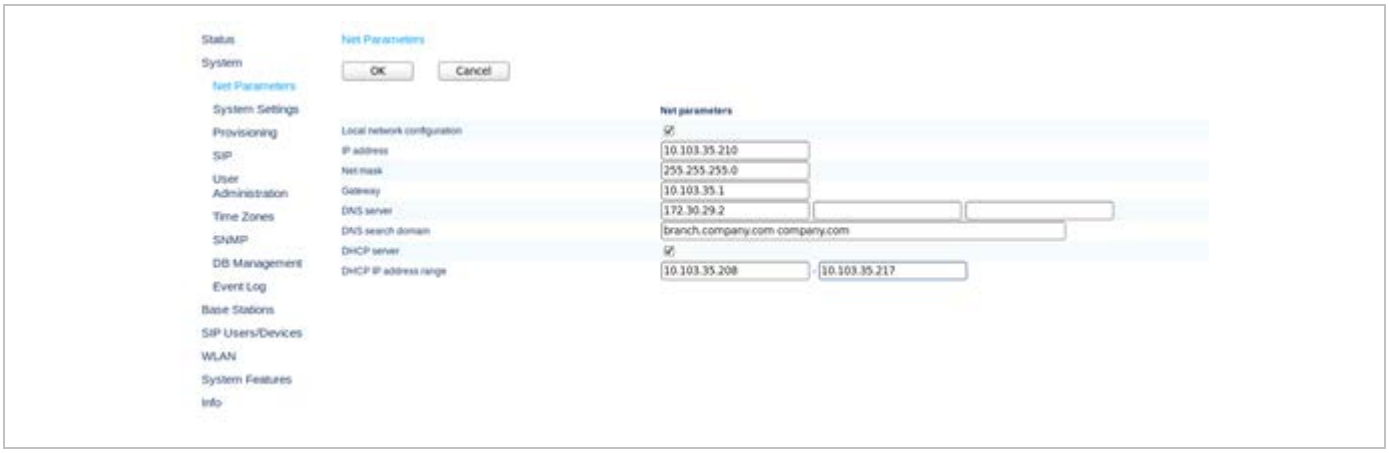


Changes to network parameters trigger a restart of the OpenMobility Manager and therefore result in a loss of the browser connection.

5.2.3 INTERGRATED DHCP SERVER

The internal DHCP server of the SIP-DECT with Cloud-ID base station can only be activated when the local network configuration for this base station is active. The SIP-DECT with Cloud-ID OMM can provide a DHCP Server for additional DECT base stations if no DHCP Server is available in the local network.

The start and end IP address of the **DHCP IP address range** must be in the same network used for the **Local network configuration**. The configured IP address of the base station may be within the configured range, it is excluded from the offered IP addresses. (If the network offers DHCP, this step is not necessary).



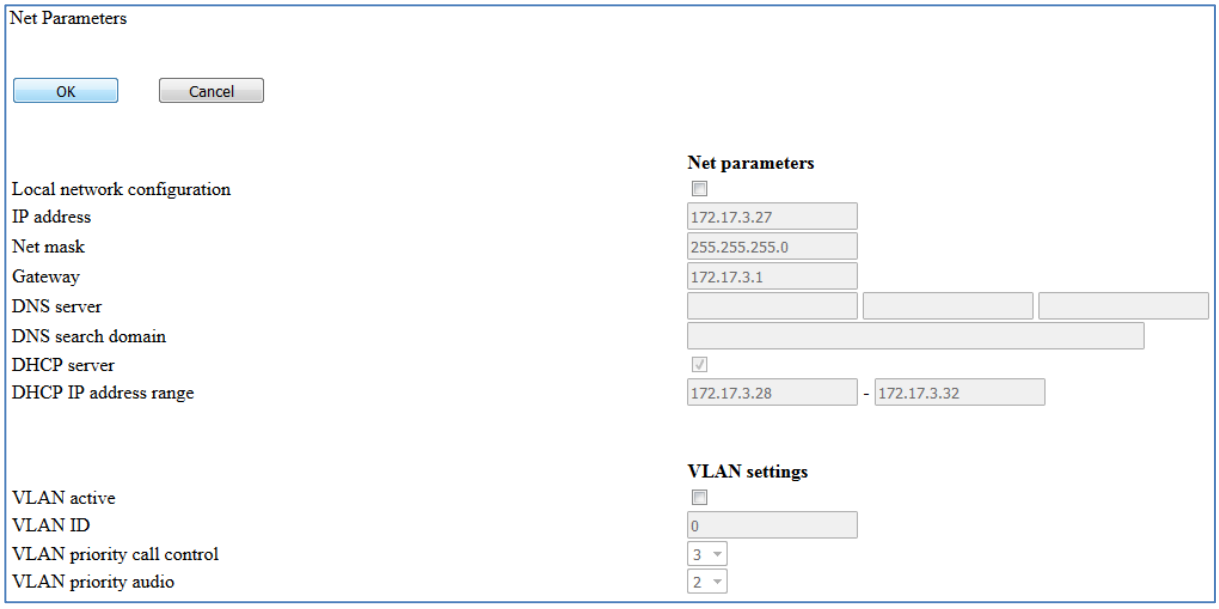
Please note: The DHCP server offers network configuration for DECT base stations only. The base stations must be known to the system, either through manual configuration or the Accept new base station feature. The IP address range may not be greater than the maximum number of base stations allowed in the system.

Parameter / Parameter group	**DHCP server**
Description	Start DHCP server
Format	boolean
Range	“off” / “on”
Default value	off
Web	Advanced: System > Net Parameters
OMM Configuration files	n.a.
DECT Phone	n.a.
User configuration files	n.a.

Parameter / Parameter group	**DHCP IP address range**
Description	Configure the IP address range served by the DHCP server
Format	IP address
Range	The range configured must correspond to the **Local network configuration**
Default value	n.a
Web	Advanced: System > Net Parameters
OMM Configuration files	n.a.
DECT Phone	n.a.
User configuration files	n.a.

5.2.4 VLAN CONFIGURATION

The following parameters can be configured independent from the “Local network configuration” setting.



Parameter / Parameter group	**VLAN active**
Description	When activated the configured VLAN-ID is used for the SIP-DECT system.
Format	Boolean
Range	n.a.
Default value	False
Web	Advanced: System > Net Parameters > VLAN settings > VLAN active
OMAP (*SD only*)	n.a.
OMM configuration files	<SetRFPM vlanTag="0" /> // no VLAN usage, disable VLAN <SetRFPM vlanTag="4" /> // VLAN usage, enable VLAN wth, for example ID 4
DECT Phone	System menu > Administration > System > Net parameters > VLAN active
User configuration files	n.a.

Parameter / Parameter group	**VLAN-ID**
Description	VLAN-ID for the SIP-DECT system (no impact on current behavior for WLAN with SSID <-> VLAN configuration).
Format	Integer
Range	1 – 4094 for valid VLAN-IDs 0 is only used in OMM configuration files to disable VLAN
Default value	n.a.
Web	Advanced: System > Net Parameters > VLAN settings > VLAN-ID
OMAP (*SD only*)	n.a.
OMM configuration files	<SetRFPM vlanTag="0" /> // no VLAN usage, disable VLAN <SetRFPM vlanTag="3" /> // VLAN usage, enable VLAN wth, for example ID 3
DECT Phone	System menu > Administration > System > Net parameters > VLAN-ID
User configuration files	n.a.

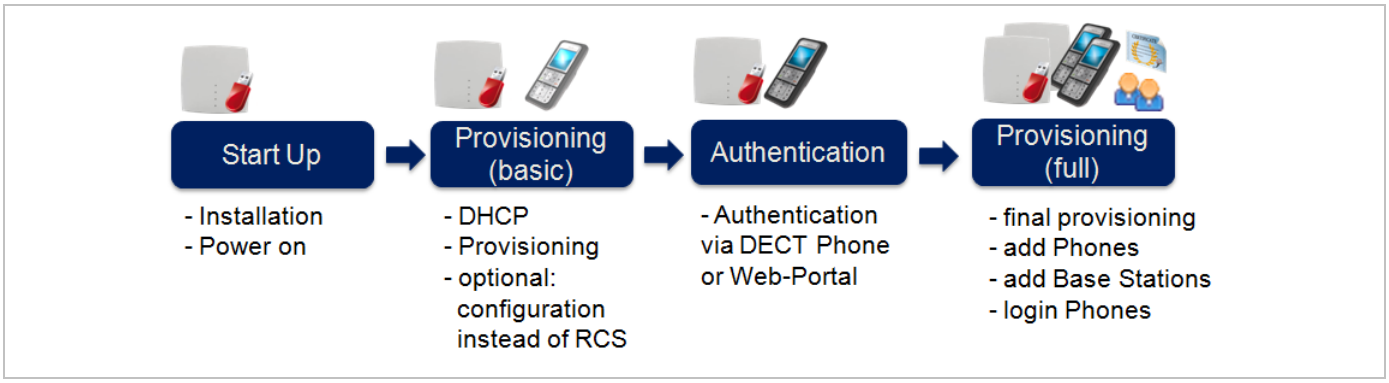
Parameter / Parameter group	**VLAN priority call control**
Description	Specifies the VLAN priority tag for VoIP signaling packets as in SD
Format	Integer
Range	0 – 7
Default value	0
Web	Advanced: System > Net Parameters > VLAN settings > VLAN priority call control
OMAP (*SD only*)	n.a.
OMM configuration files	<SetNetParams><net voiceEthPrio="5” **sigEthPrio="4**"/> </SetNetParams>
DECT Phone	n.a.
User configuration files	n.a.

Parameter / Parameter group	**VLAN priority audio**
Description	Specifies the VLAN priority tag for RTP packets as in SD
Format	Integer
Range	0 – 7
Default value	0
Web	Advanced: System > Net Parameters > VLAN settings > VLAN priority call audio
OMAP (*SD only*)	n.a.
OMM configuration files	<SetNetParams><net **voiceEthPrio="5**” **sigEthPrio="4**"/> </SetNetParams>
DECT Phone	n.a.
User configuration files	n.a.

6 PROVISIONING

6.1 SIP-DECT PROVISIONING OVERVIEW

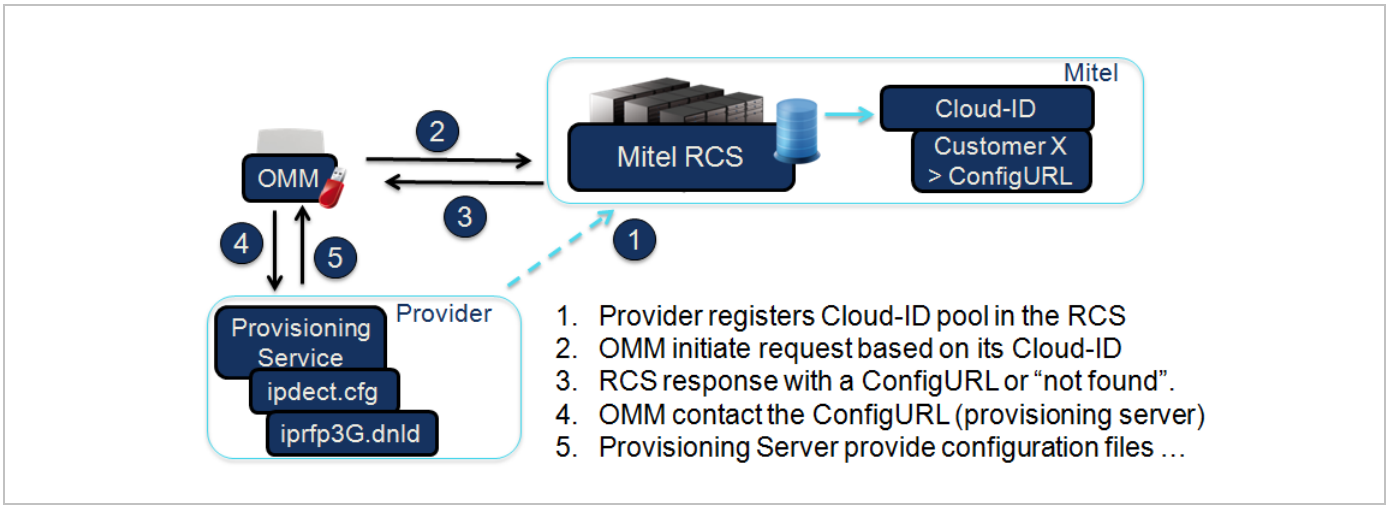
The following figure shows the main steps to set up and provision the SIP-DECT with Cloud ID system:



Once the OMM is up, configuration can be performed manually, or by fetching files from the provisioning server.

If a configuration file server (ConfigURL) is configured, the OMM automatically requests configuration files from that server and checks for software updates. If the configuration server requires authentication with credentials, those credentials must be configured using the DECT phone or the Web service.

If no ConfigURL is provided during the initial setup, the OMM contacts the Mitel Redirection and Configuration Service (RCS). If the Cloud-ID is configured in RCS, a ConfigURL that points to a provisioning system is provided.



The OMM (re)loads all external configuration files on startup and when explicitly triggered.

The following triggers force a reload of configuration and resource files:

- DHCP renew - If the OMM is using DHCP, after half of the lease time.
- Daily Time trigger - A time can be set in the OMM provisioning settings.
- Mitel 600 DECT phone **Administration** menu - “Sync user data” (this user) or “Sync system data”
- **Update** button in the OMM system settings
- SIP Notify with Event “resync” or “prov-sync”

The OMM checks for software updates with every reload of configuration files. If no specific software download URL is provided to the DECT base stations, they check for software updates from the OMM.

> **Please note:** The SIP Notify ”check-sync” also exists but only forces the reload the user configuration files.

6.2 CONFIGURATION FILE URL

SIP-DECT supports provisioning through external configuration files. As of SIP-DECT 6.0, you can configure a URL for an external file server, from which all configuration files can be downloaded. The configuration file server URL (ConfigURL) can be configured in the OMM Web service, via DHCP or the Redirection and Configuration Service (RCS).

The following files are automatically requested if a ConfigURL is set:

- Configuration files supporting startup parameters and OM AXI code for the OMM configuration
  - ipdect.cfg
  - <mac>.cfg
  - <PARK>.cfg (PARK in MAC address format: e.g. 001F11234001, and matches the Cloud-ID)
- User configuration files (for user login on DECT phone)
  - user_common.cfg
  - <user>.cfg (only loaded on demand; not loaded automatically)
  - user.cfg (only loaded on demand; not loaded automatically)
- Integrated Messaging and Alerting Service (IMA) alarm scenarios
  - ima.cfg
- Logo for OM Web-Portal (Branding)
  - customer_image.png

You can also configure individual URLs for most configuration files. If present, the individual URL is used for the configured feature.

At startup, the OMM tries to retrieve the configuration file URL (ConfigURL) from the following sources, in the order listed. The OMM uses the first URL it finds to load the configuration and resource files.

The URL can be set through the following methods (in order of priority):

1. OMM database (**System** > **Provisioning** > **Configuration file URL** in the OMM Web service)
2. DHCP vendor specific option 43 – sub-option 2
3. DHCP option 234
4. DHCP option 66 (SIP-DECT 6.2 or later)
5. Redirection and Configuration Service (RCS) – a request to the RCS is required on initial setup only. The RCS answer is stored in flash and is reused after reboot. Only the RCS request itself is limited to the initial setup.

Once a URL is set, it is stored in the OMM database. The URL can be overwritten at a later time (e.g., during provisioning after authentication).

Please note: The ConfigURL only applies to the DECT base station hosting the OMM, which must be running SIP-DECT 6.0 with Cloud-ID or higher.

Syntax

The ConfigURL has the following syntax:

```
<protocol>://<user>:<password>@<server>/<path>?<parameter>&<parameter>
```

- Supported protocols: ftp,ftps,tftp,sftp,http,https
- Credentials should be secured by transport protocol or digest authentication.

The ConfigURL supports additional parameters to modify the certificate validation behavior for the configuration file server:

- **cm:** <https client method > - TLS1.0, TLS1.1, TLS1.2 or AUTO (AUTO= all)
- **vc:** <validate certificates> - valid settings are: 0 or 1
  The OMM includes a list of trusted CA's:
  - Mozilla CA certificate list
  - SubjectCN: Symantec Class 3 Secure Server CA - G4
  - SubjectCN: Mitel Networks Root CA/emailAddress=Lee_Dilkie@Mitel.com
- **ve:** <validate expires> - validation of certificate expiry: 0 or 1
- **vh:** <validate hostname> - validation of hostnames: 0 or 1
- **uc:** allow un-configured trusted certificates> - allow untrusted certs: 0 or 1
  If set to 1, validation is disables as long as no trusted certificate was imported.
- **ic:** <import certificate> - import server certificate as trusted: 0 or 1
  If ic=1 + uc=1, the trusted certificate will be imported without any validation, as long as no trusted certificate was imported previously.

You can view and change the ConfigURL via the OMM Web service, through the parameter:

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

6.3 SYSTEM CREDENTIALS

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

Parameter / Parameter group	**User name**
Description	Specifies the user name for authentication against the provisioning server.
Format	String
Range	n.a.
Default value	Empty
Web	System > Provisioning > System credentials
OMM Configuration files	<SetSystemCredentials **username="admin"** password="secret" plainText="1"/>

DECT Phone	System menu > Administration > System credentials > Change | Change > Account
User configuration files	n.a.

Parameter / Parameter group	**Password (Password confirmation)**
Description	Specifies (and confirms) the password for authentication against the provisioning server
Format	String
Range	n.a.
Default value	Empty
Web	System > Provisioning > System credentials
OMM Configuration files	<SetSystemCredentials username="admin" **password="secret" plainText="1"**/>
DECT Phone	System menu > Administration > System credentials > Change | Change > Account > Password
User configuration files	n.a.

6.4 CONFIGURATION FILE URL

Parameter / Parameter group	**Active**
Description	Enables or disables the configuration file URL feature.
Format	Boolean
Range	n.a.
Default value	False
Web	Advanced: System > Provisioning > Configuration file URL
OMM Configuration files	<SetConfigURL> <url **enable="1"** protocol="HTTP" host="10.103.30.40" path="prov" port="911" /> </SetConfigURL>
DECT Phone	n.a.
User configuration files	n.a.

Parameter / Parameter group	**Protocol**
Description	Specifies the protocol to be used to fetch the configuration files.
Format	Enumerated (FTP / FTPS / SFTP / HTTP / HTTPS / TFTP / None)
Range	n.a.
Default value	HTTPS
Web	Advanced: System > Provisioning > Configuration file URL
OMM Configuration files	<SetConfigURL> <url enable="1" **protocol="HTTP"** host="10.103.30.40" path="prov"

	port="911" /> </SetConfigURL>
DECT Phone	n.a.
User configuration files	n.a.
Parameter / Parameter group	**Port**
Description	Specifies the provisioning server's port number.
Format	Integer
Range	1-65535 ; 0=default port of protocol
Default value	0
Web	Advanced: System > Provisioning > Configuration file URL
OMM Configuration files	<SetConfigURL> <url enable="1" protocol="HTTP" host="10.103.30.40" path="prov" **port="911"** /> </SetConfigURL>
DECT Phone	n.a.
User configuration files	n.a.

Parameter / Parameter group	**Server**
Description	Specifies the IP address or name of the provisioning server.
Format	String
Range	n.a.
Default value	Empty
Web	Advanced: System > Provisioning > Configuration file URL
OMM Configuration files	<SetConfigURL> <url enable="1" protocol="HTTP" **host="10.103.30.40"** path="prov" port="911" /> </SetConfigURL>
DECT Phone	n.a.
User configuration files	n.a.

Parameter / Parameter group	**Path**
Description	Specifies the path to the configuration and resource files on the provisioning server.
Format	String
Range	n.a.
Default value	Empty
Web	Advanced: System > Provisioning > Configuration file URL
OMM Configuration files	<SetConfigURL> <url enable="1" protocol="HTTP" host="10.103.30.40" **path="prov"** port="911" /> </SetConfigURL>
DECT Phone	n.a.

User configuration files	n.a.

6.5 DAILY AUTOMATIC RELOAD OF CONFIGURATION AND FIRMWARE FILES

Parameter / Parameter group	**Active**
Description	Enables automatic reload of the configuration and resource files on a daily basis, at the specified time.
Format	Boolean
Range	n.a.
Default value	False
Web	Advanced: System > Provisioning > Daily automatic reload of configuration and firmware files
OMM Configuration files	<SetSystemProvUpdTrig **enable="1"** hour="1" minute="10" />
DECT Phone	n.a.
User configuration files	n.a.

Parameter / Parameter group	**Time of day**
Description	Time for scheduled reload of configuration and firmware files (24h time format).
Format	Integer
Range	n.a.
Default value	0
Web	Advanced: System > Provisioning > Daily automatic reload of configuration and firmware files
OMM Configuration files	<SetSystemProvUpdTrig enable="1" **hour="1" minute="10"** />
DECT Phone	n.a.
User configuration files	n.a.

Parameter	**Maximum delay**
Description	This parameter specifies maximum time (in minutes), and the OMM waits past the schedule time before starting starting the reload of configuration and firmware files. The Maximum Delay has only an effect when "*Daily automatic reload of configuration and firmware files*" is activated.
Format	Integer
Range	0 – 1439
Default value	0
Web	Advanced: **System**>**Provisioning**> **Daily automatic reload of configuration and firmware files**
OMM configuration files	<SetSystemProvUpdTrig

	enable=”1” hour=”0” minute=”0” **maxDelay**=”0” />
DECT Phone	n.a.
User configuration files	n.a.

Parameter	**Calculated Time of Day (read-only)**
Description	The calculated time for scheduled reload of configuration and firmware files (24h time format). This parameter is read-only and is calculated by the OMM based on given “Time of Day” and “Maximum Delay”.
Format	Integer
Range	n.a.
Default value	0
Web	Advanced: **System**>**Provisioning**> **Daily automatic reload of configuration and firmware files**
OMM configuration files	n.a.
DECT Phone	n.a.
User configuration files	n.a.

Parameter	**Auto Software Check**
Description	When activated the RFP-OMMs (active, standby) check autonomous for a new software, whenever a RFP re-configuration (DHCP renew, OM Configurator, ipdect.cfg, <MAC>.cfg) happens.
Format	Boolean
Range	n.a.
Default value	True
Web	Advanced: **System**>**Provisioning**>**Daily automatic reload of configuration and firmware files**
OMM configuration files	<SetSystemProvUpdTrig enable=”1” hour=”0” minute=”0” maxDelay=”0” **autoSoftwareCheck**=”1” />
DECT Phone	n.a.
User configuration files	n.a.

6.6 CERTIFICATES

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

- **Trusted certificate(s)**: Read-only; specifies the number of trusted certificates deployed on the OMM.
- **Local certificate chain**: Read-only; specifies the number of local certificate chains deployed on the OMM.
- **Private key**: Read-only; specifies whether a private key file is deployed on the OMM.

Parameter / Parameter group	**Private key password (Password confirmation)**
Description	Specifies (and confirms) a password for the private key file.
Format	String
Range	n.a.
Default value	Empty
Web	System > Provisioning > Certificates
OMM Configuration files	<SetConfigURL plainText="1"> <url privateKeyPassword="secret" /> </SetConfigURL>
DECT Phone	n.a.
User configuration files	n.a.

Parameter / Parameter group	**Delete certificates/key**
Description	Allows the user to delete existing certificates and private key files from the OMM.
Format	Button
Range	n.a.
Default value	n.a.
Web	System > Provisioning > Certificates
OMM Configuration files	<SetConfigURL> <url> <trustedCertificates /> <localCertificates /> <privateKeys /> </url> </SetConfigURL>
DECT Phone	n.a.
User configuration files	n.a.

Parameter / Parameter group	**SSL version**
Description	The SSL protocol version to use for the configuration file server connection. AUTO accepts all supported protocol versions.
Format	Enumerated (TLS1.0 / TLS1.1 / TLS1.2 / Auto)

Range	n.a.
Default value	Auto
Web	System > Provisioning > Certificates
OMM Configuration files	<SetConfigURL> <url enable="1" protocol="HTTPS" host="www.provider.com" path="directory" port="999" **sslMethod="Auto"** validateCerts="1" validateExpires="1" validateHostName="1" importCerts="0" allowNonConfTrustCerts="0" /> </SetConfigURL>
DECT Phone	n.a.
User configuration files	n.a.

Parameter / Parameter group	**Validate certificates**
Description	Enables or disables certificate validation. If enabled, the server certificate is validated against trusted CA's (signed by a CA from the Mozilla CA certificate list) and the configured trusted certificates.
Format	Boolean
Range	n.a.
Default value	True
Web	System > Provisioning > Certificates
OMM Configuration files	<SetConfigURL> <url enable="1" protocol="HTTPS" host="www.provider.com" path="directory" port="999" sslMethod="Auto" **validateCerts="1"** validateExpires="1" validateHostName="1" importCerts="0" allowNonConfTrustCerts="0" /> </SetConfigURL>
DECT Phone	n.a.
User configuration files	n.a.

Parameter / Parameter group	**Validate expires**
Description	Enables or disables the validation of certificate expiry. When enabled, the client verifies whether a certificate has expired before accepting the certificate.
Format	Boolean
Range	n.a.
Default value	True
Web	System > Provisioning > Certificates
OMM Configuration files	<SetConfigURL> <url enable="1" protocol="HTTPS" host="www.provider.com" path="directory" port="999" sslMethod="Auto" validateCerts="1" **validateExpires="1"** validateHostName="1" importCerts="0" allowNonConfTrustCerts="0" /> </SetConfigURL>
DECT Phone	n.a.
User configuration files	n.a.

Parameter / Parameter group	**Validate host name**
Description	Enables or disables the validation of hostnames on the OMM.
Format	Boolean
Range	n.a.
Default value	True
Web	System > Provisioning > Certificates
OMM Configuration files	<SetConfigURL> <url enable="1" protocol=" HTTPS" host="www.provider.com" path="directory" port="999" sslMethod="Auto" validateCerts="1" validateExpires="1" **validateHostName="1"** importCerts="0" allowNonConfTrustCerts="0" /> </SetConfigURL>
DECT Phone	n.a.
User configuration files	n.a.

Parameter / Parameter group	**Allow unconfigured trusted certificates**
Description	If enabled, this parameter disables any server certificate validation as long as no trusted certificate was imported into the OMM. AXI commands in a received configuration file may import such trusted certificates into the OMM.
Format	Boolean
Range	n.a.
Default value	False
Web	System > Provisioning > Certificates
OMM Configuration files	<SetConfigURL> <url enable="1" protocol=" HTTPS" host="www.provider.com" path="directory" port="999" sslMethod="Auto" validateCerts="1" validateExpires="1" validateHostName="1" importCerts="0" **allowNonConfTrustCerts="0"** /> </SetConfigURL>
DECT Phone	n.a.
User configuration files	n.a.

Parameter / Parameter group	**Import certificates with first connection**
Description	If enabled (in conjunction with the Allow unconfigured trusted certificates parameter), the trusted certificate will be imported from the cert chain delivered in the server response without any validation, as long as no trusted certificate was imported previously into the OMM.
Format	Boolean
Range	n.a.
Default value	False
Web	System > Provisioning > Certificates

OMM Configuration files	<SetConfigURL> <url enable="1" protocol=" HTTPS" host="www.provider.com" path="directory" port="999" sslMethod="Auto" validateCerts="1" validateExpires="1" validateHostName="1" **importCerts="0"** allowNonConfTrustCerts="0" /> </SetConfigURL>
DECT Phone	n.a.
User configuration files	n.a.

6.7 MANUAL IMPORT OF CERTFICATES

You can import trusted certificates, a local certificate chain and a private key file for manual provisioning.

Parameter / Parameter group	**Import PEM file with / Import PEM file**
Description	Specifies the type of file (trusted certificate, local certificate, or private key) and the location of the file to be imported.
Format	String
Range	n.a.
Default value	Empty
Web	System > Provisioning > Certificates
OMM Configuration files	<SetConfigURL> <url> <localCertificates> <certificate key="-----BEGIN CERTIFICATE----- MIIEATCCAumg ... -----END CERTIFICATE-----" /> </localCertificates> <privateKeys> <certificate key="-----BEGIN RSA PRIVATE KEY-----MIIEpQIBAAKC ... -----END RSA PRIVATE KEY-----" /> </privateKeys> <trustedCertificates> <certificate key="-----BEGIN CERTIFICATE----- MIIEFTCCAv2g ... -----END CERTIFICATE-----" /> </trustedCertificates> </url> </SetConfigURL>
DECT Phone	n.a.
User configuration files	n.a.

6.8 SECURE PROVISIONING CERTIFICATE SERVER URL

The provisiong certificates can be updated automatically when a secure provisioning certificate server URL is configured.

Parameter / Parameter group	**User name**
Description	Specifies the user name for authentication against the certificate server.
Format	String
Range	n.a.

Default value	Empty
Web	n.a.
OMM Configuration files	<SetSecurePROVCertificateServerImport plainText="1" trustedCertificates="trusted.pem" localCertificates="local.pem" privateKeys="private.pem"> <url enable="1" protocol="HTTPS" host="10.103.30.40" path="directory" **username="admin"** password="secret" port="999" useCommonCerts="1" /> </SetSecurePROVCertificateServerImport>
DECT Phone	System menu > Administration > System credentials > Change | Change > Account
User configuration files	n.a.

Parameter / Parameter group	**Password**
Description	Specifies the password for authentication against the certificate server
Format	String
Range	n.a.
Default value	Empty
Web	n.a.
OMM Configuration files	<SetSecurePROVCertificateServerImport plainText="1" trustedCertificates="trusted.pem" localCertificates="local.pem" privateKeys="private.pem"> <url enable="1" protocol="HTTPS" host="10.103.30.40" path="directory" username="admin" **password="secret"** port="999" useCommonCerts="1" /> </SetSecurePROVCertificateServerImport>
DECT Phone	System menu > Administration > System credentials > Change | Change > Account > Password
User configuration files	n.a.

Parameter / Parameter group	**Active**
Description	Enables or disables the certificate server URL feature.
Format	Boolean
Range	n.a.
Default value	False
Web	n.a.
OMM Configuration files	<SetSecurePROVCertificateServerImport plainText="1" trustedCertificates="trusted.pem" localCertificates="local.pem" privateKeys="private.pem"> <url **enable="1"** protocol="HTTPS" host="10.103.30.40" path="directory" username="admin" password="secret" port="999" useCommonCerts="1" /> </SetSecurePROVCertificateServerImport>
DECT Phone	n.a.
User configuration files	n.a.

Parameter / Parameter group	**Protocol**
Description	Specifies the protocol to be used to fetch the certificate files.
Format	Enumerated (FTP / FTPS / SFTP / HTTP / HTTPS / TFTP / None)
Range	n.a.
Default value	HTTPS
Web	n.a.
OMM Configuration files	<SetSecurePROVCertificateServerImport plainText="1" trustedCertificates="trusted.pem" localCertificates="local.pem" privateKeys="private.pem"> <url enable="1" **protocol="HTTPS"** host="10.103.30.40" path="directory" username="admin" password="secret" port="999" useCommonCerts="1" /> </SetSecurePROVCertificateServerImport>
DECT Phone	n.a.
User configuration files	n.a.

Parameter / Parameter group	**Port**
Description	Specifies the certificate server's port number.
Format	Integer
Range	1-65535 ; 0=default port of protocol
Default value	0
Web	n.a.
OMM Configuration files	<SetSecurePROVCertificateServerImport plainText="1" trustedCertificates="trusted.pem" localCertificates="local.pem" privateKeys="private.pem"> <url enable="1" protocol="HTTPS" host="10.103.30.40" path="directory" username="admin" password="secret" **port="999"** useCommonCerts="1" /> </SetSecurePROVCertificateServerImport>
DECT Phone	n.a.
User configuration files	n.a.

Parameter / Parameter group	**Server**
Description	Specifies the IP address or name of the certificate server.
Format	String
Range	n.a.
Default value	Empty
Web	n.a.
OMM Configuration files	<SetSecurePROVCertificateServerImport plainText="1" trustedCertificates="trusted.pem" localCertificates="local.pem" privateKeys="private.pem"> <url enable="1" protocol="HTTPS" **host="10.103.30.40"** path="directory" username="admin" password="secret" port="999"

	useCommonCerts="1" /> </SetSecurePROVCertificateServerImport>
DECT Phone	n.a.
User configuration files	n.a.

Parameter / Parameter group	**Path**
Description	Specifies the path to the certificate files on the certificate server.
Format	String
Range	n.a.
Default value	Empty
Web	n.a.
OMM Configuration files	<SetSecurePROVCertificateServerImport plainText="1" trustedCertificates="trusted.pem" localCertificates="local.pem" privateKeys="private.pem"> <url enable="1" protocol="HTTPS" host="10.103.30.40" **path="directory"** username="admin" password="secret" port="999" useCommonCerts="1" /> </SetSecurePROVCertificateServerImport>
DECT Phone	n.a.
User configuration files	n.a.

Parameter / Parameter group	**trustedCertificates**
Description	Filename of the trusted certificates to read from the server.
Format	String
Range	n.a.
Default value	Empty
Web	n.a.
OMM Configuration files	<SetSecurePROVCertificateServerImport plainText="1" **trustedCertificates="trusted.pem"** localCertificates="local.pem" privateKeys="private.pem"> <url enable="1" protocol="HTTPS" host="10.103.30.40" path="directory" username="admin" password="secret" port="999" useCommonCerts="1" /> </SetSecurePROVCertificateServerImport>
DECT Phone	n.a.
User configuration files	n.a.

Parameter / Parameter group	**localCertificates**
Description	Filename of the local certificates to read from the server.
Format	String
Range	n.a.
Default value	Empty

Web	n.a.
OMM Configuration files	<SetSecurePROVCertificateServerImport plainText="1" trustedCertificates="trusted.pem" **localCertificates="local.pem"** privateKeys="private.pem"> <url enable="1" protocol="HTTPS" host="10.103.30.40" path="directory" username="admin" password="secret" port="999" useCommonCerts="1" /> </SetSecurePROVCertificateServerImport>
DECT Phone	n.a.
User configuration files	n.a.

Parameter / Parameter group	**PrivateKeys**
Description	Filename of the private key to read from the server.
Format	String
Range	n.a.
Default value	Empty
Web	n.a.
OMM Configuration files	<SetSecurePROVCertificateServerImport plainText="1" trustedCertificates="trusted.pem" localCertificates="local.pem" **privateKeys="private.pem"**> <url enable="1" protocol="HTTPS" host="10.103.30.40" path="directory" username="admin" password="secret" port="999" useCommonCerts="1" /> </SetSecurePROVCertificateServerImport>
DECT Phone	n.a.
User configuration files	n.a.
User configuration files	n.a.

Parameter / Parameter group	**Use common certificate configuration**
Description	Enables the use of the system-wide certificate validation settings for this URL, as configured on the **System** > **Provisioning** > **Certificates** page.
Format	Boolean
Range	n.a.
Default value	False
Web	n.a.
OMM Configuration files	<SetSecurePROVCertificateServerImport plainText="1" trustedCertificates="trusted.pem" localCertificates="local.pem" privateKeys="private.pem"> <url enable="1" protocol="HTTPS" host="10.103.30.40" path="directory" username="admin" password="secret" port="999" **useCommonCerts="1"** /> </SetSecurePROVCertificateServerImport>
DECT Phone	n.a.
User configuration files	n.a.

6.9 SECURE OMM CERTIFICATE SERVER URL

OMM certificates can be updated automatically through configuration of a secure OMM certificate server URL.

Parameter / Parameter group	**User name**
Description	Specifies the user name for authentication against the certificate server.
Format	String
Range	n.a.
Default value	Empty
Web	n.a.
OMM Configuration files	<SetSecureOMMCertificateServerImport plainText="1" localCertificates="local.pem" privateKeys="private.pem"> <url enable="1" protocol="HTTPS" host="10.103.30.40" path="directory" **username="admin"** password="secret" port="999" useCommonCerts="1" /> </SetSecureOMMCertificateServerImport>
DECT Phone	System menu > Administration > System credentials > Change | Change > Account
User configuration files	n.a.

Parameter / Parameter group	**Password**
Description	Specifies the password for authentication against the certificate server
Format	String
Range	n.a.
Default value	Empty
Web	n.a.
OMM Configuration files	<SetSecureOMMCertificateServerImport plainText="1" localCertificates="local.pem" privateKeys="private.pem"> <url enable="1" protocol="HTTPS" host="10.103.30.40" path="directory" username="admin" **password="secret"** port="999" useCommonCerts="1" /> </SetSecureOMMCertificateServerImport>
DECT Phone	System menu > Administration > System credentials > Change | Change > Account > Password
User configuration files	n.a.

Parameter / Parameter group	**Active**
Description	Enables or disables the certificate server URL feature.
Format	Boolean
Range	n.a.
Default value	False
Web	n.a.
OMM Configuration files	<SetSecureOMMCertificateServerImport plainText="1" localCertificates="local.pem" privateKeys="private.pem">

	<url **enable="1"** protocol="HTTPS" host="10.103.30.40" path="directory" username="admin" password="secret" port="999" useCommonCerts="1" /> </SetSecureOMMCertificateServerImport>
DECT Phone	n.a.
User configuration files	n.a.

Parameter / Parameter group	**Protocol**
Description	Specifies the protocol to be used to fetch the certificate files.
Format	Enumerated (FTP / FTPS / SFTP / HTTP / HTTPS / TFTP / None)
Range	n.a.
Default value	HTTPS
Web	n.a.
OMM Configuration files	<SetSecureOMMCertificateServerImport plainText=”1” localCertificates="local.pem" privateKeys="private.pem"> <url enable="1" **protocol="HTTPS"** host="10.103.30.40" path="directory" username="admin" password="secret" port="999" useCommonCerts="1" /> </SetSecureOMMCertificateServerImport>
DECT Phone	n.a.
User configuration files	n.a.

Parameter / Parameter group	**Port**
Description	Specifies the certificate server’s port number.
Format	Integer
Range	1-65535 ; 0=default port of protocol
Default value	0
Web	n.a.
OMM Configuration files	<SetSecureOMMCertificateServerImport plainText="1" localCertificates="local.pem" privateKeys="private.pem"> <url enable="1" protocol="HTTPS" host="10.103.30.40" path="directory" username="admin" password="secret" **port="999"** useCommonCerts="1" /> </SetSecureOMMCertificateServerImport>
DECT Phone	n.a.
User configuration files	n.a.

Parameter / Parameter group	**Server**
Description	Specifies the IP address or name of the certificate server.
Format	String
Range	n.a.
Default value	Empty

Web	n.a.
OMM Configuration files	<SetSecureOMMCertificateServerImport plainText="1" localCertificates="local.pem" privateKeys="private.pem"> <url enable="1" protocol="HTTPS" **host="10.103.30.40"** path="directory" username="admin" password="secret" port="999" useCommonCerts="1" /> </SetSecureOMMCertificateServerImport>
DECT Phone	n.a.
User configuration files	n.a.

Parameter / Parameter group	**Path**
Description	Specifies the path to the certificate files on the certificate server.
Format	String
Range	n.a.
Default value	Empty
Web	n.a.
OMM Configuration files	<SetSecureOMMCertificateServerImport plainText="1" localCertificates="local.pem" privateKeys="private.pem"> <url enable="1" protocol="HTTPS" host="10.103.30.40" **path="directory"** username="admin" password="secret" port="999" useCommonCerts="1" /> </SetSecureOMMCertificateServerImport>
DECT Phone	n.a.
User configuration files	n.a.

Parameter / Parameter group	**localCertificates**
Description	Filename of the local certificates to read from the server.
Format	String
Range	n.a.
Default value	Empty
Web	n.a.
OMM Configuration files	<SetSecureOMMCertificateServerImport plainText="1" **localCertificates="local.pem"** privateKeys="private.pem"> <url enable="1" protocol="HTTPS" host="10.103.30.40" path="directory" username="admin" password="secret" port="999" useCommonCerts="1" /> </SetSecureOMMCertificateServerImport>
DECT Phone	n.a.
User configuration files	n.a.

Parameter / Parameter group	**PrivateKeys**
Description	Filename of the private key to read from the server.
Format	String
Range	n.a.
Default value	Empty
Web	n.a.
OMM Configuration files	<SetSecureOMMCertificateServerImport plainText="1" localCertificates="local.pem" **privateKeys="private.pem"**> <url enable="1" protocol="HTTPS" host="10.103.30.40" path="directory" username="admin" password="secret" port="999" useCommonCerts="1" /> </SetSecureOMMCertificateServerImport>
DECT Phone	n.a.
User configuration files	n.a.
User configuration files	n.a.

Parameter / Parameter group	**Use common certificate configuration**
Description	Enables the use of the system-wide certificate validation settings for this URL, as configured on the **System** > **Provisioning** > **Certificates** page.
Format	Boolean
Range	n.a.
Default value	False
Web	n.a.
OMM Configuration files	<SetSecureOMMCertificateServerImport plainText="1" localCertificates="local.pem" privateKeys="private.pem"> <url enable="1" protocol="HTTPS" host="10.103.30.40" path="directory" username="admin" password="secret" port="999" **useCommonCerts="1"** /> </SetSecureOMMCertificateServerImport>
DECT Phone	n.a.
User configuration files	n.a.

7 SIP FEATURES

7.1 BASIC SIP SETTINGS

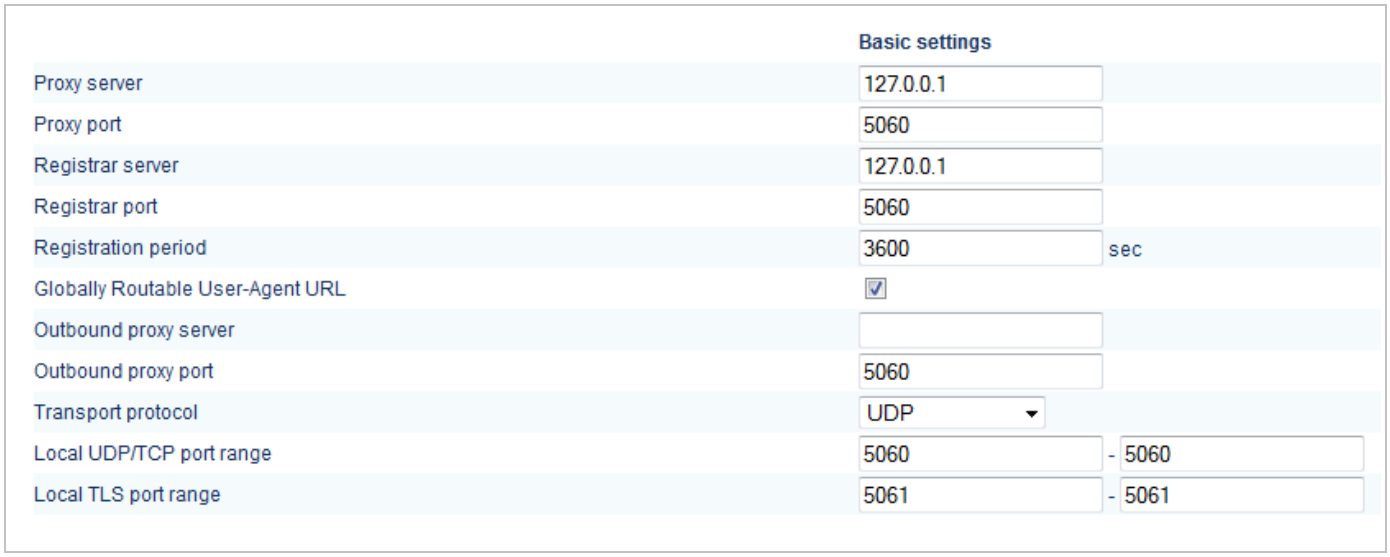
The SIP-DECT system requires some basic SIP settings to register DECT users on a SIP Call Manager and to allow SIP-based call features.

- **Proxy server**: IP address or name of the SIP proxy server. A SIP proxy is a server that initiates and forwards requests generated by the OMM to the targeted user. If a host name and domain are used for the proxy server parameter, ensure that a DNS server and a domain are specified for your SIP-DECT system via DHCP.
- **Proxy port**: SIP proxy server's port number. Default is "5060". To enable DNS SRV support for proxy lookups, use a value of "0" for the proxy port. If TLS is used, the value must be changed to "5061".
- **Registrar server**: IP address or name of the SIP registrar. Enables the DECT users to be registered with a registrar. If a host name and domain are used for the proxy server parameter, ensure that a DNS server and a domain are specified for your SIP-DECT system via DHCP.
- **Registrar port**: SIP registrar's port number. Default is "5060". To enable DNS SRV support for registrar lookups, use a value of "0" for the registrar port. In case that TLS is used, the value must be changed to "5061".
- **Registration period**: The requested registration period, in seconds, from the registrar.
- **Globally Routable User-Agent URL**: Enables support for Globally Routable User-Agent URIs (GRUUs). GRUUs provide a way for anyone on the Internet to route a call to a specific instance of a SIP User-Agent.
- **Outbound proxy server**: Address of the outbound proxy server. This setting is optional. All SIP messages originating from the OMM are sent to this server. For example, if you have a Session Border Controller in your network, then you would set its address here.
- **Outbound proxy port**: The port on the proxy server to which the OMM sends all SIP messages. Default is "5060". If TLS is used, the value must be changed to "5061".
- **Transport protocol**: The protocol used by the OMM to send/receive SIP signaling. Default is "UDP". 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 and TCP**: All outgoing connections are always set up via TCP, but incoming SIP messages are also accepted when being 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 Call Manager permanently open.
- **Local UDP/TCP port range**: The port range to be used for DECT users when UDP/TCP is used as the transport protocol. The default is 5060 – 5060.
- **Local TLS port range**: The port range to be used for DECT users when TLS is used as the transport protocol. The default is 5061 – 5061.

You configure and modify the basic SIP settings parameters and associated values using the configuration files or the Mitel Web UI. You can also configure some (though not all) basic SIP settings using the DECT phone UI; please refer to the following sections.

7.1.1 CONFIGURATION OF SIP SETTINGS VIA THE WEB UI

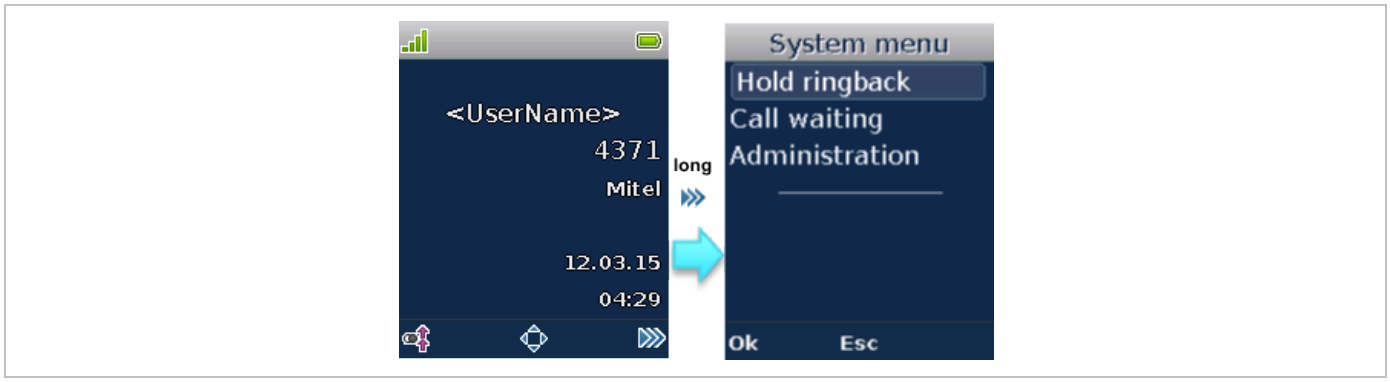
1 Navigate to the **System** -> **SIP** menu.



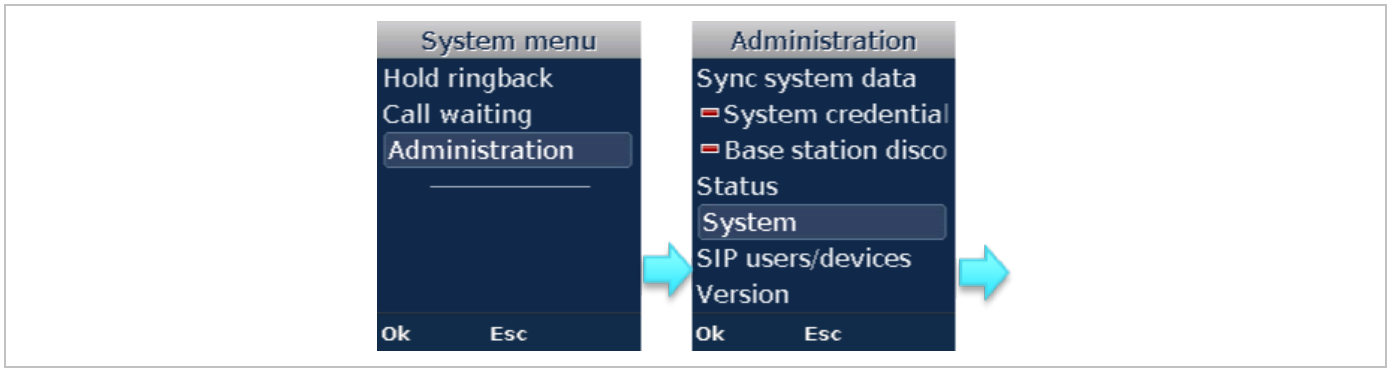
2 Enter the settings of your SIP Call Server platform or the settings received from your SIP provider.

7.1.2 CONFIGURATION OF THE SIP PROXY AND REGISTRAR VIA THE PHONE UI

1 Open the System menu by pressing and holding the menu softkey ( ):



2 Select **Administration**, then select **System**:



3 When prompted, enter the the credentials of your SIP-DECT system to log in (default is Omm/Omm) and select **SIP**:

4 Enter the proxy server, proxy port, registar server and registrar port:

Parameter / Parameter group	**Proxy server**
Description	The IP address of the SIP proxy server to which the OMM sends all SIP requests.
Format	IP address or fully qualified host name
Range	n.a.
Default value	127.0.0.1
Web	System > SIP > Basic settings
OMM Configuration files	<SetBasicSIP transportProt="UDP" proxyServer="127.0.0.1" proxyPort="5060" regServer="127.0.0.1" regPort="5060" regPeriod="3600" />
DECT Phone	System menu > Administation > System > SIP
User configuration files	n.a.

Parameter / Parameter group	**Proxy port**
Description	SIP proxy server's port number. To enable DNS SRV support for proxy lookups, use a value of "0" for the proxy port. In case that TLS is used, the value shall be changed to "5061".
Format	Integer
Range	0, 1024-65535
Default value	5060
Web	System > SIP > Basic settings

OMM Configuration files	<SetBasicSIP transportProt="UDP" proxyServer="127.0.0.1" proxyPort="5060" regServer="127.0.0.1" regPort="5060" regPeriod="3600" />
DECT Phone	System menu > Administation > System > SIP
User configuration files	n.a.

Parameter / Parameter group	**Registrar server**
Description	IP address or name of the SIP registrar the OMM uses to register DECT users.
Format	IP address or fully qualified host name
Range	n.a.
Default value	127.0.0.1
Web	System > SIP > Basic settings
OMM Configuration files	<SetBasicSIP transportProt="UDP" proxyServer="127.0.0.1" proxyPort="5060" regServer="127.0.0.1" regPort="5060" regPeriod="3600" />
DECT Phone	System menu > Administation > System > SIP
User configuration files	n.a.

Parameter / Parameter group	**Registrar port**
Description	SIP registrar's port number. To enable DNS SRV support for registrar lookups, use a value of "0" for the registrar port. In case that TLS is used, the value shall be changed to "5061".
Format	Integer
Range	0, 1024-65535
Default value	5060
Web	System > SIP > Basic settings
OMM Configuration files	<SetBasicSIP transportProt="UDP" proxyServer="127.0.0.1" proxyPort="5060" regServer="127.0.0.1" regPort="5060" regPeriod="3600" />
DECT Phone	System menu > Administation > System > SIP
User configuration files	n.a.

Parameter / Parameter group	**Registration period**
Description	The requested registration period, in seconds, from the registrar.
Format	Integer
Range	60- 2147483647
Default value	3600
Web	System > SIP > Basic settings
OMM Configuration files	<SetBasicSIP transportProt="UDP" proxyServer="127.0.0.1" proxyPort="5060" regServer="127.0.0.1" regPort="5060" regPeriod="3600" />
DECT Phone	n.a.
User configuration files	n.a.

Parameter / Parameter group	**Globally Routable User-Agent URL**
Description	Enables or disables GRUU support according to RFC 5627. When enabled, SIP-DECT generates a unique “sip.instance” identifier for each DECT user.
Format	Boolean
Range	n.a.
Default value	1 (*True*)
Web	System > SIP > Basic settings
OMM Configuration files	<SetBasicSIP transportProt="UDP" gruu="true" />
DECT Phone	n.a.
User configuration files	n.a.

Parameter / Parameter group	**Transport protocol**
Description	The protocol that the IP phone uses to send out SIP messages.
Format	Enumeration
Range	UDP, TCP, UDPandTCP, TCP, TLS, PersistentTLS
Default value	UDP
Web	System > SIP > Basic settings
OMM Configuration files	<SetBasicSIP transportProt="UDP" proxyServer="127.0.0.1" proxyPort="5060" regServer="127.0.0.1" regPort="5060" regPeriod="3600" />
DECT Phone	System menu > Administation > System > SIP
User configuration files	n.a.

Parameter / Parameter group	**Outbound proxy server**
Description	Address of the outbound proxy server.
Format	IP address or fully qualified host name.
Range	n.a.
Default value	
Web	System > SIP > Basic settings
OMM Configuration files	<SetBasicSIP transportProt="UDP" outboundProxyServer="192.186.10.100" outboundProxyPort="5060" />
DECT Phone	n.a.
User configuration files	n.a.

Parameter / Parameter group	**Outbound proxy port**
Description	SIP outbound proxy's port number. To enable DNS SRV support for outbound proxy lookups, use a value of "0" for the registrar port. If TLS is used, the value is changed to "5061".
Format	Integer
Range	0, 1024-65535
Default value	5060
Web	System > SIP > Basic settings
OMM Configuration files	<SetBasicSIP transportProt="UDP" outboundProxyServer="192.186.10.100" outboundProxyPort="5060" />
DECT Phone	n.a.
User configuration files	n.a.

Parameter / Parameter group	**Local UDP/TCP port range**
Description	The local port range to be used for DECT users for UDP/TCP transport.
Format	Integer
Range	5060, 17000-32767 (range may not exceed 512 ports, one port per user)
Default value	5060 – 5060
Web	System > SIP > Basic settings
OMM Configuration files	<SetPortRangeSIP> <userUdpTcp startPort="5060" endPort ="5060"> <userTls startPort="5061" endPort ="5061"> </SetPortRangeSIP>
DECT Phone	n.a.
User configuration files	n.a.

Parameter / Parameter group	**Local TLS port range**
Description	The local port range to be used for DECT users in case of TLS transport.
Format	Integer
Range	5060, 17000-32767 (range may not exceed 512 ports, one port per user)
Default value	5061 – 5061
Web	System > SIP > Basic settings
OMM Configuration files	<SetPortRangeSIP> <userUdpTcp startPort="5060" endPort ="5060" /> <userTls startPort="5061" endPort ="5061" /> </SetPortRangeSIP>
DECT Phone	n.a.
User configuration files	n.a.

7.2 ADVANCED SIP SETTINGS

SIP-DECT offers a variety of advanced settings to adapt the SIP behavior to your specific SIP Call Manager platform.

- **Explicit MWI subscription**: Some SIP Call Managers (such as the Asterisk) support Message Waiting Indication (MWI) based on RFC 3842. A MWI icon is displayed on a DECT phone (Mitel 600) if the user has received a voice message on his voice box which is supported by the SIP Call Manager. If *Explicit MWI subscription* is enabled, the OMM sends an explicit MWI subscription message for each DECT phone to the Proxy or Outbound Proxy Server.
- **Explicit MWI subscription period**: The requested duration in seconds, before the MWI subscription times out. SIP-DECT re-subscribes to MWI before the subscription period ends.
- **User agent info**: If this option is enabled, the OMM sends information on his version inside the SIP headers *User-Agent/Server*.
- **Dial terminator**: The dial terminator is configurable (up to 2 characters; “0” – “9”, “*”, “#” or empty). The default dial terminator is “#”. A dial terminator is necessary if digit treatment is applied on outgoing calls and overlapped sending is used. Note that Mitel 600 DECT phones typically use en-bloc sending.
- **Registration failed retry timer**: Specifies the time, in seconds, that the OMM waits between registration attempts when the registration is rejected by the registrar.
- **Registration timeout retry timer**: Specifies the time that the OMM waits between registration attempts when the registration times out.
- **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. This parameter allows configuration of an interval, in seconds, between re-INVITE requests sent from the OMM to keep a SIP session alive.
- **Transaction timer**: The time period in milliseconds that the OMM allows a call server (proxy/registrar) to respond to SIP messages that it sends. If the OMM does not receive a response in the time period specified for this parameter, the OMM assumes the message as timed out. When DNS SRV is used and there is no answer in time, the call server is recorded in the blacklist. For more information on DNS SRV, see section 11.1.
- **Blacklist timeout**: The time period, in minutes, that an unreachable call server stays in the blacklist. For more information on DNS SRV and the blacklist, see section 11.1.
- **Incoming call timeout**: The time, in seconds, that the OMM waits for a user to accept an incoming call before rejecting the call automatically.
- **Determine remote party by**: You can select the SIP header from which the remote party information (user id and display name) should be determined. If P-Asserted-Identity (default value) is selected but no such header is received, a fallback to the mandatory From / To header will be done. This feature can be configured by choosing one of the two values.
- **Note:** When SIP-DECT receives a SIP header P-Asserted-Identity in ringing state during an outgoing call, the included identity information (e.g. SIP display name and user-id) is displayed on Mitel 600 phones as new call target. In addition, the outgoing call log of the Mitel 600 phones is updated with the new given identity.
- **Multiple 180 Ringing**: If this feature is deactivated, the OMM sends out only one “180 Ringing“ response for an incoming call if PRACK is not supported. If this feature is activated, the OMM retransmits the 180 Ringing response multiple times for an incoming call if PRACK is not supported. This ensures that the calling side receives a 180 Ringing response in case of packet loss on the network.

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

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

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

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

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

- **SIP contact matching**: 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. Available options are:
- *URI* – match user username, domain name, phone IP and port and transport
- *IP only* – match the IP address of the phone only
- *Username only* – match the username only
- *IP and user name* – match the IP address of the phone and the username
- **Call reject state code (user reject)**: Specifies the SIP state code sent as response when the user rejects an incoming call by pressing the “Reject” option.
- **Call reject state code (device unreachable)**: Specifies the SIP state code sent as response when the incoming call is rejected because the DECT phone is unreachable (e.g., the DECT phone is out of range or out of battery power).

You configure and modify the advanced SIP settings parameters and associated values using the configuration files or the Mitel Web UI.

Configuration via the Web UI:

1. Click on the **System** -> **SIP** menu item.
2. Make sure the **Advanced** checkbox in the top bar is enabled.
3. Modify the settings in the *Advanced* section to adapt the OMM behavior to your SIP Call Manager.

Parameter / Parameter group	**Explicit MWI subscription**
Description	If *Explicit MWI subscription* is enabled, the OMM sends explicit for each DECT phone an MWI subscription message to the Proxy or Outbound Proxy Server.
Format	Boolean
Range	n.a.
Default value	0 (False)
Web	Advanced: System > SIP > Advanced
OMM Configuration files	<SetAdvancedSIP mwiSubscription="0" />
DECT Phone	n.a.
User configuration files	n.a.

Parameter / Parameter group	**User agent info**
Description	If this option is enabled, the OMM sends information on his version inside the *User-Agent/Server* SIP header.
Format	Boolean
Range	n.a.
Default value	1 (True)
Web	Advanced: System > SIP > Advanced
OMM Configuration files	<SetAdvancedSIP userAgentInfo="1" />
DECT Phone	n.a.
User configuration files	n.a.

Parameter / Parameter group	**Dial terminator**
Description	The dial terminator is configurable (up to 2 characters; “0” – “9”, “*”, “#” or empty). A dial terminator is necessary if digit treatment is applied on outgoing calls and overlapped sending is used.
Format	Up to 2 characters
Range	0–9, *, #
Default value	#
Web	Advanced: System > SIP > Advanced
OMM Configuration files	<SetAdvancedSIP dialTerminator="#" />
DECT Phone	n.a.
User configuration files	n.a.

Parameter / Parameter group	**Registration failed retry timer**
Description	Specifies the time, in seconds, that the OMM waits between registration attempts when the registration is rejected by the registrar.
Format	Integer
Range	120-86400 sec.
Default value	120 sec.
Web	Advanced: System > SIP > Advanced
OMM Configuration files	<SetAdvancedSIP regFailedRetryTimer="120" />
DECT Phone	n.a.
User configuration files	n.a.

Parameter / Parameter group	**Registration timeout retry timer**
Description	Specifies the time that the OMM waits between registration attempts when the registration times out.
Format	Integer
Range	120-86400 sec.
Default value	180 sec.
Web	Advanced: System > SIP > Advanced
OMM Configuration files	<SetAdvancedSIP regTimeoutRetryTimer="180" />
DECT Phone	n.a.
User configuration files	n.a.

Parameter / Parameter group	**Session timer**
Description	The interval, in seconds, between re-INVITE requests sent from the OMM to keep a SIP session alive. The minimum session timer is 90 seconds and the maximum is 86400 seconds. The default is 0 (i.e., feature is disabled).
Format	Integer
Range	0, 90-86400 sec.
Default value	0 (disabled)
Web	Advanced: System > SIP > Advanced
OMM Configuration files	<SetAdvancedSIP sessionTimer="0" />
DECT Phone	n.a.
User configuration files	n.a.

Parameter / Parameter group	**Transaction timer**
Description	The time period in milliseconds that the OMM allows a call server (proxy/registrar) to respond to SIP messages that it sends. If the OMM does not receive a response in the time period designated for this parameter, the OMM assumes the message as timed out.
Format	Integer
Range	4000-64000 msec.
Default value	4000 msec.
Web	Advanced: System > SIP > Advanced
OMM Configuration files	<SetAdvancedSIP transactionTimer="4000" />
DECT Phone	n.a.
User configuration files	n.a.

Parameter / Parameter group	**Blacklist timeout**
Description	The time period, in minutes, that an unreachable call server stays in the blacklist. For more information on DNS SRV and the blacklist, see section 11.1.
Format	Integer
Range	0-1440
Default value	5 min.
Web	Advanced: System > SIP > Advanced
OMM Configuration files	<SetAdvancedSIP blacklistTimeout="5" />
DECT Phone	n.a.
User configuration files	n.a.

Parameter / Parameter group	**Incoming call timeout**
Description	The time, in seconds, that the OMM waits for a user to accept an incoming call before rejecting the call automatically.
Format	Integer
Range	30-300 sec.
Default value	180 sec.
Web	Advanced: System > SIP > Advanced
OMM Configuration files	<SetAdvancedSIP incomingCallTimeout="180" />
DECT Phone	n.a.
User configuration files	n.a.

Parameter / Parameter group	**Determine remote party by**
Description	The SIP header from which the remote party information (user id and display name) should be determined.
Format	Enumeration
Range	*P-Asserted-Identity* – determine remote party by P-Asserted-Identity header *From/To* – determine remote party by From/To header
Default value	P-Asserted-Identity
Web	Advanced: System > SIP > Advanced
OMM Configuration files	<SetAdvancedSIP callerDetermination="P-Assert-Identity" />
DECT Phone	n.a.
User configuration files	n.a.

Parameter / Parameter group	**Multiple 180 Ringing**
Description	If this feature is deactivated, the OMM sends out only one 180 Ringing response for an incoming call if PRACK is not supported. If this feature is activated, the OMM retransmits the 180 Ringing response multiple times for an incoming call if PRACK is not supported.
Format	Boolean
Range	n.a.
Default value	1 (True)
Web	Advanced: System > SIP > Advanced
OMM Configuration files	<SetAdvancedSIP multipleRing="1" />
DECT Phone	n.a.
User configuration files	n.a.

Parameter / Parameter group	**Semi-attended transfer mode**
Description	Specifies the semi-attended transfer mode to be used.
Format	Enumeration
Range	Blind – the semi-attended transfer is handled as blind transfer Attended – the semi-attended transfer is handled as an attended transfer
Default value	Blind
Web	Advanced: System > SIP > Advanced
OMM Configuration files	<SetAdvancedSIP semiAttendedTransferMode="Blind" />
DECT Phone	n.a.
User configuration files	n.a.

Parameter / Parameter group	**Refer-to with replaces**
Description	When *Semi-attended transfer mode* is *Blind* this paremeter specifies wether a REFER request with *Replaces* header is used or not.
Format	Boolean
Range	n.a.
Default value	0 (False)
Web	Advanced: System > SIP > Advanced
OMM Configuration files	<SetAdvancedSIP referToWithReplaces="0" />
DECT Phone	n.a.
User configuration files	n.a.

Parameter / Parameter group	**SIP Contact matching**
Description	Specifies the method used by the OMM to match the Contact header in a SIP response to a REGISTER request.
Format	Enumeration
Range	*Uri* - match user username, domain name, phone IP and port and transport *IpOnly* - match the IP address of the phone only *IpAndUsername* - match the IP address of the phone and the username *UsernameOnly* - match the username only
Default value	Uri
Web	Advanced: System > SIP > Advanced
OMM Configuration files	<SetAdvancedSIP contactMatching="Uri" />
DECT Phone	n.a.
User configuration files	n.a.

Parameter / Parameter group	**Call reject state code (user reject)**
Description	Specifies the SIP state code sent as response when the user rejects an incoming call by pressing the “Reject” option.
Format	Integer
Range	400-699
Default value	486
Web	Advanced: System > SIP > Advanced
OMM Configuration files	<SetAdvancedSIP callRejectStateCodeUsr="486" />
DECT Phone	n.a.
User configuration files	n.a.

Parameter / Parameter group	**Call reject state code (device unreachable)**
Description	Specifies the SIP state code sent as response when the incoming call is rejected because the DECT phone is unreachable (e.g., the DECT phone is out of range or out of battery power).
Format	Integer
Range	400-699
Default value	486
Web	Advanced: System > SIP > Advanced
OMM Configuration files	<SetAdvancedSIP callRejectStateCodeDev="486" />
DECT Phone	n.a.
User configuration files	n.a.

Parameter	**Remove route**
Description	Enables or disables the addition of the Route header in a SIP packet. Enable this parameter for outbound proxies that do not support Route headers. **Note**: When enabled, this breaks all support for SIP routing. So, if some other devices in the network attempts to add itself to the route, it fails.
Format	Boolean
Range	n.a.
Default value	False
Web	Advanced: System > SIP > Advanced
OAMP	System > SIP > Advanced Settings > General
OMM Configuration files	<SetAdvancedSIP removeRoute=”0” />
DECT Phone	n.a.
User configuration files	n.a.

Parameter	**Explicit MWI subscription period**
Description	The requested duration in seconds, before the MWI subscription times out. SIP-DECT re-subscribes to MWI before the subscription period ends.
Format	Integer
Range	60 – 2147483647
Default value	86400
Web	Advanced: System > SIP > Advanced
OAMP	System > SIP > Advanced Settings > General
OMM Configuration files	<SetAdvancedSIP mwiSubscriptionPeriod=”86400” />
DECT Phone	n.a.
User configuration files	n.a.

7.3 REAL-TIME TRANSPORT PROTOCOL (RTP) SETTINGS

Real-time Transport Protocol (RTP) is used as the bearer path for voice packets sent over the IP network. Information in the RTP header tells the receiver how to reconstruct the data and describes how the bit streams are packetized (i.e. which codec is in use). Session Initiation Protocol (SIP) uses RTP for the media stream, with User Datagram Protocol (UDP) as the transport layer encapsulation protocol.

You can set the following parameters for RTP:

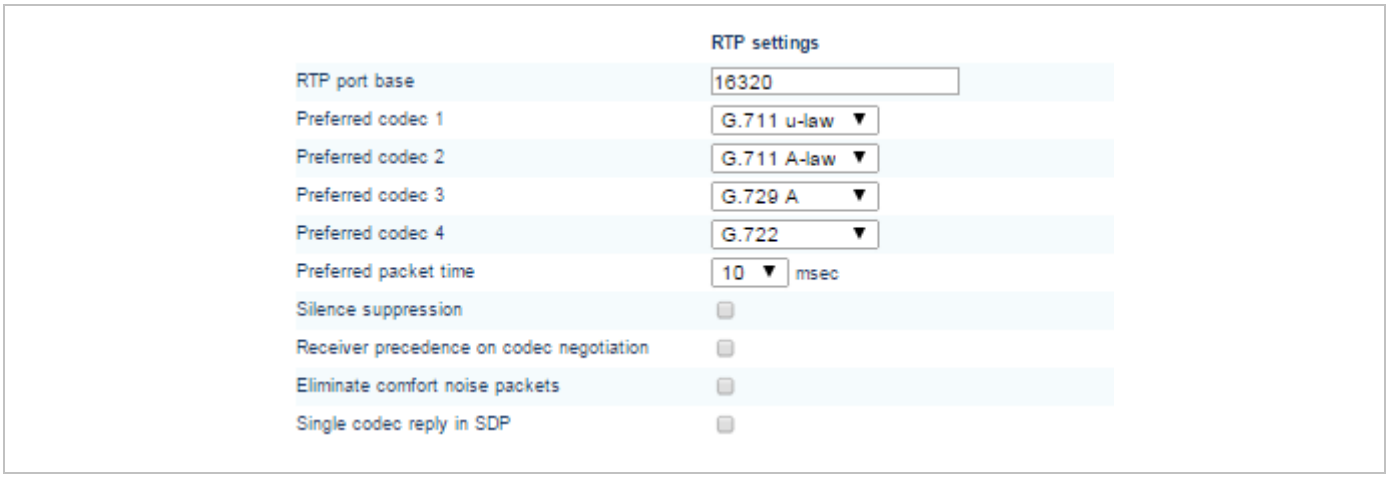
- **RTP port base**: Each base station needs a continuous port area of 68 UDP ports for RTP voice streaming. The RTP port base is the start port number of that area.
- **Preferred codec 1 – 4**: Specifies a customized codec preference list that allows you to use the preferred codecs. *Codec 1* has the highest and *Codec 4* the lowest priority.
- **Preferred paket time**: Determines the length of voice samples collected before sending out a new RTP packet. A small setting improves voice quality at the expense of data transmission overhead.
- **Silence suppression**: Enables automatic silence detection in the RTP voice data stream to optimize the data transfer volume.
- **Receiver precedence on CODEC negotiation**: Specifies the precedence procedure for SDP offers on incoming calls
- ON (option is enabled): The CODEC selection for incoming SDP offers is based on the preference order list. The first entry in the OMM preferred codec list matching an entry in the incoming SDP offer will be selected.
- OFF (option is disabled): The CODEC selection is based on the preference order list of incoming SDP offer. The first entry in the incoming order list matching an entry of OMM preferred codec list will be selected. This is the default and is as recommended in RFC 3264.
- **Eleminate comfort noise packets**: If this feature is activated, comfort noise packets are removed from the RTP media stream, which causes gaps in the sequence numbers. This can be used if comfort noise packets (e.g. in G.711 media streams) disturb voice calls in certain installations.
- **Single code reply in SDP**: If this feature is activated, the OMM answers SDP offers (included in the SIP signalization) with a single codec in the SDP answer.

You configure and modify the RTP settings parameters and associated values using the configuration files or the Mitel Web UI.

Configuration via the Web UI

1 Click on the **System** -> **SIP** menu item. Make sure the **Advanced** checkbox in the top bar is enabled.

2 Modify the settings in the *RTP settings* section to adapt the OMM behavior to your SIP Call Manager.



Parameter / Parameter group	**RTP port base**
Description	Starting port number of the continuous port area of 68 UDP ports required by every DECT base station for RTP voice streaming.
Format	Integer
Range	
Default value	16320
Web	Advanced: System > SIP > RTP settings
OMM Configuration files	<SetRTP portBase="16320" />
DECT Phone	n.a.
User configuration files	n.a.

Parameter / Parameter group	**Preferred Codec 1-4**
Description	Specifies a customized codec preference list that allows you to use preferred codecs. Codec 1 has the highest and Codec 4 the lowest priority.
Format	Enumeration
Range	G.711-u-law G.711-A-law G.729 A G.722 none
Default value	n.a.
Web	Advanced: System > SIP > RTP settings
OMM Configuration files	<SetRTP> <codec type="G.722" /> <codec type="G.711-u-law" /> <codec type="G.711-A-law" />

	<codec type="G.729-A" /> </SetRTP>
DECT Phone	n.a.
User configuration files	n.a.

Parameter / Parameter group	**Preferred packet time**
Description	Determines the length of voice samples collected before sending out a new RTP packet. A small setting improves voice quality at the expense of data transmission overhead.
Format	Enumeration
Range	10 20 30
Default value	20 msec.
Web	Advanced: System > SIP > RTP settings
OMM Configuration files	<SetRTP packetTime="20" />
DECT Phone	n.a.
User configuration files	n.a.

Parameter / Parameter group	**Silence Suppression**
Description	Enables automatic silence detection in the RTP voice data stream to optimize the data transfer volume.
Format	Boolean
Range	n.a.
Default value	0 (False)
Web	Advanced: System > SIP > RTP settings
OMM Configuration files	<SetRTP silenceSupp="0" />
DECT Phone	n.a.
User configuration files	n.a.

Parameter / Parameter group	**Receiver precedence on CODEC negotiation**
Description	Specifies the precedence procedure for SDP offers on incoming calls ON (option is enabled): The CODEC selection for incoming SDP offers based on the own preference order list. The first entry in the OMM preferred codec list matching an entry in the incoming SDP offer will be selected. OFF (option is disabled): The CODEC selection based on the preference order list of incoming SDP offer. The first entry in the incoming order list matching an entry of OMM preferred codec list will be selected. This is the default and is as recommended in RFC 3264.
Format	Boolean
Range	n.a.

Default value	0 (False)
Web	Advanced: System > SIP > RTP settings
OMM Configuration files	<SetRTP receiverPrecedence="0" />
DECT Phone	n.a.
User configuration files	n.a.

Parameter / Parameter group	**Eleminate comfort noise packets**
Description	When activated, comfort noise packets are removed from the RTP media stream, which causes gaps in the sequence numbers. Used if comfort noise packets (e.g. G.711 media streams) disturb voice calls in certain installations.
Format	Boolean
Range	n.a.
Default value	0 (False)
Web	Advanced: System > SIP > RTP settings
OMM Configuration files	<SetRTP comfortNoisePktElim="0" />
DECT Phone	n.a.
User configuration files	n.a.

Parameter / Parameter group	**Single codec reply in SDP**
Description	If this feature is activated, the OMM answers SDP offers (included in the SIP signalization) with a single codec in the SDP answer.
Format	Boolean
Range	n.a.
Default value	0 (False)
Web	Advanced: System > SIP > RTP settings
OMM Configuration files	<SetRTP singleCodecReplyInSDP="0" />
DECT Phone	n.a.
User configuration files	n.a.

7.4 DTMF SETTINGS

SIP-DECT supports the following modes for Dual-Tone Multifrequency (DTMF) digits:

- Out-of-band as referenced in RFC 2833 / RFC 4733
- In-band
- SIP Info

You can set the following parameters for DTMF:

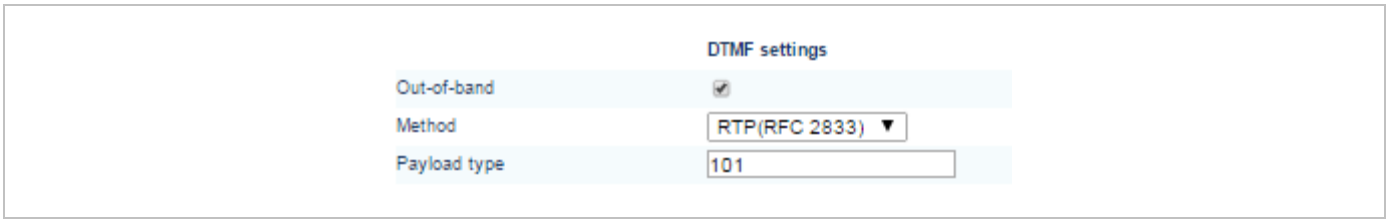
- **Out-of-band**: Used to configure whether DTMF Out-of-band is preferred or not.
- **Method**: The OMM supports the following DTMF Out-of-band methods:
- RTP (RFC 2833 / RFC 4733)
  Transmits DTMF as RTP events according to RFC 2833 after the payload type negotiation via SIP/SDP. If the payload type is not negotiated, “in band” will be used automatically.
- INFO
  Transmits DTMF tones as telephone events (application/dtmf-relay). This setting should be used if RFC 2833 is not supported.
- BOTH
  DTMF telephones events are sent according to RFC 2833 and as well as SIP INFO method.
  Note: It is possible that the other party recognizes events twice.
- **Payload type**: If the Out-of-band option is enabled, this setting specifies the payload type which is used for sending DTMF events based on section 3.1, reference RFC 2833.

You configure and modify the DTMF settings parameters and associated values using the configuration files or the Mitel Web service.

Configuration via the Web service

1 Click on the **System** -> **SIP** menu item. Make sure the **Advanced** checkbox in the top bar is enabled

2 Modify the settings in the *DTMF settings* section to adapt the OMM behavior to your SIP Call Manager.



Parameter / Parameter group	**Out-of-band**
Description	Used to configure whether DTMF Out-of-band is preferred or not.
Format	Boolean
Range	n.a.
Default value	1 (True)
Web	Advanced: System > SIP > DTMF settings
OMM Configuration files	<SetDTMF outOfBand="1" method="RFC2833" payloadType="101" />
DECT Phone	n.a.
User configuration files	n.a.

Parameter / Parameter group	**Method**
Description	Specifies the method for sending out DTMF events when Out-of-band is enabled.
Format	Enumeration
Range	RFC2833 - Transmits DTMF as RTP events according to RFC 2833 after the payload type negotiation via SIP/SDP. If the payload type is not negotiated, “in band” will be used automatically. INFO - The SIP INFO method is used to transmit DTMF tones as telephone events (application/dtmf-relay). This setting should be used if RFC 2833 is not supported. Both - DTMF telephones events are send according to RFC 2833 and as well as SIP INFO method. Note: Possibly, the other party recognizes events twice.
Default value	RFC2833
Web	Advanced: System > SIP > DTMF settings
OMM Configuration files	<SetDTMF outOfBand="1" method="RFC2833" payloadType="101" />
DECT Phone	n.a.
User configuration files	n.a.

Parameter / Parameter group	**Payload type**
Description	If the Out-of-band option is enabled, this setting specifies the payload type which is used for sending DTMF events based on section 3.1, RFC 2833.
Format	Integer
Range	96-127
Default value	101
Web	Advanced: System > SIP > DTMF settings
OMM Configuration files	<SetDTMF outOfBand="1" method="RFC2833" payloadType="101" />
DECT Phone	n.a.
User configuration files	n.a.

7.5 SIP TELEPHONY ISSUES

Information about making calls and maintaining supplementary services is specified in “Mitel 600 Series DECT Phone; User Guide” /31/. This chapter focuses on preconditions, exceptions or specific behavior that is dependent on settings in the SIP Call Manager with which the OMM is integrated.

7.5.1 DECT PHONE, SIP USER AND EXPECTED AVAILABLE LINES

- When users are”logged in”, each DECT phone is associated with exactly one SIP user, to be registered at the SIP registrar.
- In default operational mode, where multiple lines are treated locally by the OMM, up to three lines can be terminated in a call to maintain supplementary features.

- Additionally, a **SOS or MANDOWN** alarm call may occupy **up to two more lines** for a moment until formerly active lines are completely released.

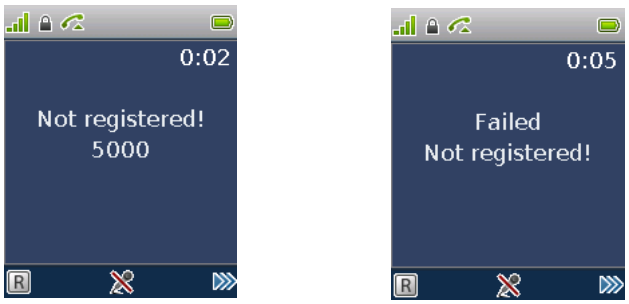
> **Please note:** A user typically has one active line and a second line for other features (e.g., call waiting, call hold, etc). However, if the OMM runs in ”local line handling” mode, the SIP Call Manager must guarantee support of up to 5 lines per SIP user, for all supplementary features and alarm calls (SOS, ManDown) to run properly in situations where the user’s two lines are in use.

7.5.1.1 Local line handling is switched off

In this mode, a SIP Call Manager maintains all supplementary features. There will be exactly one line established between OMM and the SIP Call Manager. R-Key (hook-flash) is signalled as DTMF in this case.

7.5.2 SIP USER “NOT REGISTERED”

SIP users may not have a valid SIP registration to a registrar (e.g., registration has failed or a time limit has been exceeded due to a temporarily unreachable server). The OMM does not prevent SIP users from making or accepting calls in such a situation, but the system displays a ”Not registered!” message in an additional info line on the DECT Phone call display.



> **Please note:** There is one exception: if the SIP registrar or proxy are set to local loop (127.0.0.1) and there is no backup server configured, the ”Not registered” message is not displayed.

7.5.3 DIVERSION INDICATION

The OMM supports the display of diversion indications for 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.

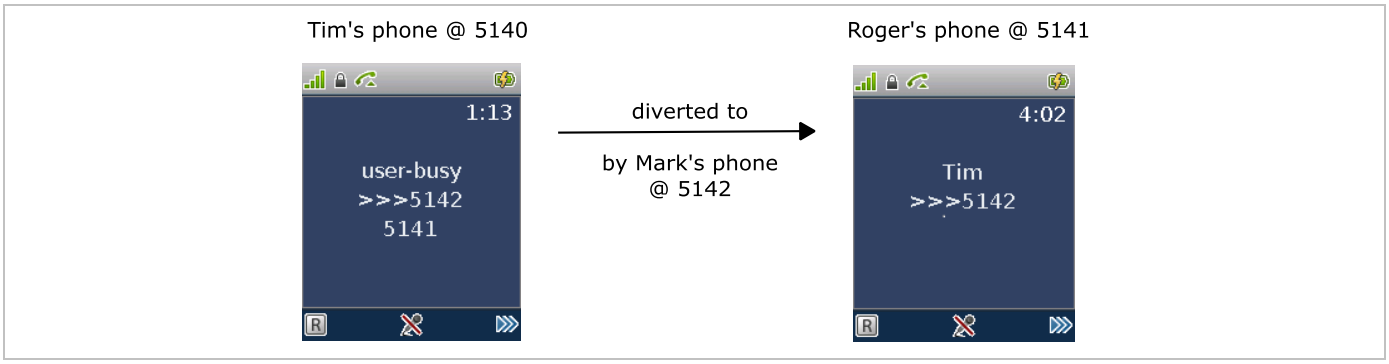
When an outgoing call from a Mitel 600 phone is being diverted to another destination (i.e., via call forward), the phone displays the Caller ID (phone number and/or caller name) of the new destination and the reason for the call diversion (if delivered from IPBX). Similarly, at the new destination, 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 for the incoming call (Tim) and the original called destination (5142).



7.5.4 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 phones.

7.5.5 CALL REJECT ON SILENT CHARGING

If 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.

Parameter	**Call Reject on Silent Charging**
Description	If the flag "Call reject on silent charging" is set, all Mitel 600 DECT phones reject incoming calls if the phones are in charging mode and "silent charging" is activated in the phone.
Format	Bool
Range	True, False
Default Value	False
Web	Advanced: System->SIP->Supplementary services
OMP (SD only)	System->SIP->Supplementary services
OMM Configuration Files	<SetSuplServ callRejectOnSilentCharging="1" />
DECT Phone	n.a.
User Configuration Files	n.a.

8 MITEL 600 DECT PHONE MENU

The **Administration** menu on Mitel 600 DECT phones offers administrative functions to the user such as login, logout, and display configuration and status summary. It also allows basic OMM configuration, which requires a login.

The menu is available as an option under the **System menu**:

1. Press and hold the menu softkey when idle (or press the menu softkey briefly and select **System menu**).
2. Use the down navigation key to select the **Administration** menu.

The following list summarizes the options under the **Administration** menu. If a login is required, use the same account and password as used for administrative access through the Web service.

- **Login**: User can login to that free device.
- **Logout**: User can logout from that device.
- **Key lock**: User can set/change its PIN and is able to set the time that takes to lock the phone automatically.
- **Phone state**: Display of user/device configuration and status data summary. This menu is only applicable if the user is logged in.
- **Sync user data**: Refresh SIP registration and sync user data, if they are stored externally. This menu is only applicable if the user is logged in.
- **Sync system data**: Reload all configuration and resource files (requires **OMM login**).
- **System credentials**: Authentication for service provider servers (requires **OMM login**, if valid credentials are set).
- **Base station discovery**: Accept new base station (requires **OMM login**).
- **Status**: Show basic OMM network settings (DHCP, IP addresses etc).
- **System**: Set basic system data of the OMM (requires **OMM login**).
- **Sip users/devices**: Basic configuration of users and devices (requires **OMM login**).
- **Version**: Show current software version of the OMM.

8.1 “SYSTEM” SUBMENU

The following list summarizes the submenus:

- **System name**: User can configure the system name.
- **Net parameter**: User can configure basic network settings.
  - Enable DHCP
  - Static IP configuration
- **Date and time**:
  - Set NTP servers
  - Set time zone
- **SIP**: Configuration of SIP proxy and Registrar
- **User administration**: Configuration of OMM user
- **Restart**: Restart the OMM
- **Factory reset**: Reset the OMM to factory defaults (Caution! The DECT phones lose subscription)

8.2 “SIP USERS/DEVICES” SUBMENU

The following list summarizes the submenus:

- **Subscription allowed**: Enable/disable DECT subscription of phones.
- **New SIP user**: Ctreate a new SIP user with some mandatory basic settings
- **Users**: List all configures users
- **Devices**: List all DECT phones.

8.3 SUPPORTED LANGUAGES

The same languages are supported on the DECT phone user interface as on the Web service:

- English
- German
- French
- Spanish

The DECT phones support additional languages, but the administration interfaces are displayed in English.

9 STATUS

The Status page (in the Web UI) provides information about the SIP-DECT with Cloud-ID system status. In case of system errors, system warning messages are also displayed on this page.

10 SYSTEM SETTINGS

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
- Update the OMM

The following sections describe the parameters that can be set.

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

10.1 GENERAL

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

Parameter / Parameter group	**System name**
Description	Name of this OpenMobility system.
Format	String
Range	10
Default value	n.a.
Web	System > System settings > General
OMM Configuration files	<SetSystemName name="our system" />
DECT Phone	n.a.
User configuration files	n.a.

Parameter / Parameter group	**Remote access**
Description	Switches on/off the SSH access to all RFPs of the DECT system .
Format	Boolean
Range	n.a.
Default value	False
Web	Advanced: System > System settings > General
OMM Configuration files	<SetRemoteAccess enable="1" />
DECT Phone	n.a.
User configuration files	n.a.
Parameter / Parameter group	**Tone scheme**
Description	Select country specific tones.

Format	Enumerated			
Range	AU	Australian tone scheme	HU	Hungarian tone scheme
	AT	Austrian tone scheme	IT	Italian tone scheme
	BE	Belgian tone scheme	LT	Lithuanian tone scheme
	BY	Belorussian tone scheme	LV	Latvian tone scheme
	BR	Brazilian tone scheme	NL	Dutch tone scheme
	CH	Swiss tone scheme	NO	Norwegian tone scheme
	CZ	Czech tone scheme	PL	Polish tone scheme
	DK	Danish tone scheme	RU	Russian tone scheme
	ES	Spanish tone scheme	SK	Slovakian tone scheme
	EE	Estonian tone scheme	SE	Swedish tone scheme
	FI	Finnish tone scheme	TW	Taiwanese tone scheme
	FR	French tone scheme	UA	Ukrainian tone scheme
	GB,UK	British tone scheme	US	American tone scheme
	DE	German tone scheme		
Default value	“DE”			
Web	System > System settings > General			
OMM Configuration files	<SetSysToneSchemeResp toneScheme="DE" />			
DECT Phone	n.a.			
User configuration files	n.a.			

10.2 DECT SETTINGS

- **DECT power limit 100mW**: Activate this option if you want to limit 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).
- **Encryption**: Activate this option if you want to enable DECT encryption on voice calls for the whole system (recommended). Encryption is enabled by default.
- **Restricted 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 if you want to subscribe more than one DECT phone at a time or together with auto-create on subscription. It should be activated only if there is a special need.
- **Enhanced DECT security:** If DECT enhanced security is enabled, every connection will be encrypted, not only voice calls, but also calls such as service calls (e.g. list access) or messaging. Additionally, the cipher key used for encryption during an ongoing call is changed every 60 seconds. 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 supported with Mitel 600 DECT phones. These mechanisms became mandatory together with CAT-iq.
- **DECT authentication code**: The authentication code is used during initial DECT phone subscription as a security option. A code entered here provides a system-wide DECT authentication code for each DECT phone subscription.
- **DECT phone user login type**: Specifies the system-wide variant for DECT phone login method. Two kinds of login types are supported: The user can either be determined by the telephone number (**Number**) or by the unique user login ID (**Login ID**). Both elements are part of each user data set.

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

- **Preserve user device relation at DB restore:** Enables the preservation of the user – DECT phone association with an OMM database restore.

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

Parameter / Parameter group	**DECT power limit 100mW**
Description	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).
Format	Boolean
Range	n.a.
Default value	False
Web	Advanced: System > System settings > DECT settings
OMM Configuration files	<SetDECTPowerLimit enable="0" />
DECT Phone	n.a.
User configuration files	n.a.

Parameter / Parameter group	**Encryption**
Description	Activates DECT encryption on voice calls
Format	Boolean
Range	n.a.
Default value	True
Web	Advanced: System > System settings > DECT settings
OMM Configuration files	<SetDECTEncryption enable="1" />
DECT Phone	n.a.
User configuration files	n.a.

Parameter / Parameter group	**Restrict subscription duration**
Description	Restricts the duration for DECT phone subscriptions to 2 minutes after subscription activation.
Format	Boolean
Range	n.a.
Default value	False
Web	Advanced: System > System settings > DECT settings
OMM Configuration files	<SetRestrictedSubscriptionDuration restrictedSubscrDur="0" />
DECT Phone	n.a.
User configuration files	n.a.

Parameter / Parameter group	**Enhanced DECT security**
Description	Activates enhanced DECT security.
Format	Boolean
Range	n.a.
Default value	False
Web	Advanced: System > System settings > DECT settings
OMM Configuration files	<SetSite seq ="1"> <site id="1" dectSecurity="0" /> </SetSite>
DECT Phone	n.a.
User configuration files	n.a.

Parameter / Parameter group	**DECT authentication code**
Description	Authentication code used during initial DECT phone subscription as a security option .
Format	Digits
Range	Up to 8 digits
Default value	22222
Web	Advanced: System > System settings > DECT settings
OMM Configuration files	<SetDECTAuthCode ac="4711" />
DECT Phone	n.a.
User configuration files	n.a.

Parameter / Parameter group	**DECT phone user login type**
Description	Specifies the system-wide variant for DECT phone login method .
Format	Enumeration
Range	“ID”, “NUMBER”
Default value	“NUMBER”
Web	Advanced: System > System settings > DECT settings
OMM Configuration files	<SetPPLoginVariant login="NUMBER" />
DECT Phone	n.a.
User configuration files	n.a.

Parameter / Parameter group	**Preserve user device relation at DB restore**
Description	Enables the preservation of the user – DECT phone association with an OMM database restore.
Format	Boolean
Range	n.a.

Default value	False
Web	Advanced: System > System settings > DECT settings
OMM Configuration files	<SetPreserveUserDeviceRelation enable="0" />
DECT Phone	n.a.
User configuration files	n.a.

10.3 WLAN

This setting applies to DECT base stations of the type RFP 48 WLAN.

In the **Regulatory domain** field, 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.

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

Parameter / Parameter group	**Regulatory domain**
Description	Specifies the regulatory domain of the WLAN network .
Format	Enumerated
Range	Possible values are a 2-character string as country code for the regulatory domain. Valid strings are defind in ISO-3166-1.
Default value	“None”
Web	Advanced: System > System settings > WLAN
OMM Configuration files	<SetWLANRegDomain regDomain="DE" />
DECT Phone	n.a.
User configuration files	n.a.

10.4 QOS SETTINGS

- **QoS for voice packets**: Specifies the value of the type of service (ToS) of the IP packet header for all packets that transport RTP voice streams. Default: 0xB8.
- **QoS for signalling packets**: Specifies the value of the type of service (ToS of the IP packet header for all packets related to VoIP signaling. Default: 0xB8.
- **TTL (Time to live)**: Specifies the maximum hop count for all IP packets. Default: 32

10.5 VOICE MAIL

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

Parameter / Parameter group	**Voice mail number**
Description	System-wide voice mail number .
Format	String
Range	n.a.
Default value	n.a,
Web	Advanced: System > System settings > Voice mail
OMM Configuration files	<SetSysVoiceboxNum voiceboxNum="5555" />
DECT Phone	n.a.
User configuration files	UD_VoiceMailNumber=22222

10.6 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. The configuration of this service can be provided by configuration files loaded a configured URL. Please see /27/ SIP-DECT; OM Integrated Messaging & Alerting Application; Installation, Administration & User Guide.

Parameter / Parameter group	**Internal message routing (phone <> phone)**
Description	Enables or disables internal messaging between DECT phones.
Format	Boolean
Range	n.a.
Default value	True
Web	Advanced: System > System Settings > OM Integrated Messaging & Alerting service
OMM Configuration files	<SetIMA **enable="1"** plainText="1"> <url enable="1" protocol="FTPS" host="10.103.30.40" path="prov/ima.cfg" username="admin" password="secret" port="911" useCommonCerts="1" /> </SetIMA>
DECT Phone	n.a.
User configuration files	n.a.

Parameter / Parameter group	**Configure specific destination**
Description	Enables the specific URL to an external file server for retrieving the IMA configuration file.
Format	Boolean
Range	n.a.
Default value	False
Web	Advanced: System > System Settings > OM Integrated Messaging & Alerting service
OMM Configuration files	<SetIMA enable="1" plainText="1"> <url **enable="1"** protocol="FTPS" host="10.103.30.40" path="prov/ima.cfg" username="admin" password="secret" port="911" useCommonCerts="1" /> </SetIMA>
DECT Phone	n.a.
User configuration files	n.a.

Parameter / Parameter group	**Protocol**
Description	The protocol used to retrieve the IMA configuration file from the external server.
Format	Enumerated (FTP / FTPS / SFTP / HTTP / HTTPS / TFTP / None)
Range	n.a.
Default value	FTP
Web	Advanced: System > System Settings > OM Integrated Messaging & Alerting service
OMM Configuration files	<SetIMA enable="1" plainText="1" > <url enable="1" **protocol="FTPS"** host="10.103.30.40" path="prov/ima.cfg" username="admin" password="secret" port="911" useCommonCerts="1" /> </SetIMA>
DECT Phone	n.a.
User configuration files	n.a.

Parameter / Parameter group	**Port**
Description	Port of the external file server.
Format	Integer
Range	1-65535 ; 0=default port of protocol
Default value	0
Web	Advanced: System > System Settings > OM Integrated Messaging & Alerting service
OMM Configuration files	<SetIMA enable="1" plainText="1" > <url enable="1" protocol="FTPS" host="10.103.30.40" path="prov/ima.cfg" username="admin" password="secret" **port="911"** useCommonCerts="1" /> </SetIMA>

DECT Phone	n.a.
User configuration files	n.a.

Parameter / Parameter group	**Server**
Description	The IP address or name of the external file server.
Format	String
Range	n.a.
Default value	Empty
Web	Advanced: System > System Settings > OM Integrated Messaging & Alerting service
OMM Configuration files	<SetIMA enable="1" plainText="1" > <url enable="1" protocol="FTPS" **host="10.103.30.40"** path="prov/ima.cfg" username="admin" password="secret" port="911" useCommonCerts="1" /> </SetIMA>
DECT Phone	n.a.
User configuration files	n.a.

Parameter / Parameter group	**User name**
Description	The user name to authenticate on the external file server.
Format	String
Range	n.a.
Default value	Empty
Web	Advanced: System > System Settings > OM Integrated Messaging & Alerting service
OMM Configuration files	<SetIMA enable="1" plainText="1" > <url enable="1" protocol="FTPS" host="10.103.30.40" path="prov/ima.cfg" **username="admin"** password="secret" port="911" useCommonCerts="1" /> </SetIMA>
DECT Phone	n.a.
User configuration files	n.a.

Parameter / Parameter group	**Password (Password confirmation)**
Description	The password to authenticate on the external file server.
Format	String
Range	n.a.
Default value	Empty
Web	Advanced: System > System Settings > OM Integrated Messaging & Alerting service
OMM Configuration files	<SetIMA enable="1" plainText="1" > <url enable="1" protocol="FTPS" host="10.103.30.40" path="prov/ima.cfg"

	username="admin" **password="secret"** port="911" useCommonCerts="1" /> </SetIMA>
DECT Phone	n.a.
User configuration files	n.a.

Parameter / Parameter group	**Path & filename**
Description	The location and file name of the IMA configuration file on the external file server.
Format	String
Range	n.a.
Default value	Empty
Web	Advanced: System > System Settings > OM Integrated Messaging & Alerting service
OMM Configuration files	<SetIMA **enable="1"** plainText="1" > <url enable="1" protocol="FTPS" host="10.103.30.40" **path="prov/ima.cfg"** username="admin" password="secret" port="911" useCommonCerts="1" /> </SetIMA>
DECT Phone	n.a.
User configuration files	n.a.

Parameter / Parameter group	**Use common certificate configuration**
Description	Enables the use of the system-wide certificate validation settings for this URL, as configured on the **System** / **Provisioning** / **Certificates** page.
Format	Boolean
Range	n.a.
Default value	False
Web	Advanced: System > System Settings > OM Integrated Messaging & Alerting service
OMM Configuration files	<SetIMA enable="1" plainText="1" > <url enable="1" protocol="FTPS" host="10.103.30.40" path="prov/ima.cfg" username="admin" password="secret" port="911" **useCommonCerts="1"** /> </SetIMA>
DECT Phone	n.a.
User configuration files	n.a.

10.7 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.

Parameter / Parameter group	**Syslog**
Description	Propagation of syslog messages.
Format	IP address and port
Range	n.a.
Default value	Not activated
Web	Advanced: System > System settings > Syslog
OMM Configuration files	<SetSyslogServer enable="1" ipAddr="10.103.111.111" port="514" />
DECT Phone	n.a.
User configuration files	n.a.

10.8 SOFTWARE UPDATE URL

The new software image for the OMM can be provided as an iprfp3G.dnld file on an external file server. You configure the URL for the software image as described in this section.

- **Configure specific source**: Enables the specific URL for downloading the iprfp3G.dnld file (as opposed to the ConfigURL, which points to an external file server for all configuration and resource files).
- **Protocol**: Specifies the protocol used to fetch the software image file.
- **Port**: Specifies the port of the external file server.
- **Server**: Specifies the IP address or name of the external file server.
- **User name**: Specifies the user name to authenticate on the external file server.
- **Password**: Specifies the password to authenticate on the external file server.
- **Password confirmation**: Confirms the password to authenticate on the external file server.
- **Path**: Specifies the location of the software image file on the external file server.
- **Use common certificate configuration**: Enables the use of the system-wide certificate validation settings for this URL, as configured on the **System** -> **Provisioning** -> **Certificates** page.

Parameter / Parameter group	**Software update URL**
Description	Specifies the URL where the OMM looks for the software image iprfp3G.dnld.
Format	String
Range	n.a.
Default value	Empty
Web	Advanced: System > System settings > Software update URL

OMM Configuration files	<SetSoftwareImageURL plainText="1"> <url enable="1" protocol="HTTP" host="10.103.35.14" path="/jenkins/Oberbrandmeister/omm_scsip/rfp43" password="topsecret" port="0" useCommonCerts="0" /> </SetSoftwareImageURL>
DECT Phone	n.a.
User configuration files	n.a.

10.9 SYSTEM DUMP

To obtain information for product support or for other maintenance purposes, a system dump can be initiated immediately or at periodic intervals. The system dump comprises the event log, status counter, state of tasks, mutexes/semaphores, actual configuration data und the last syslog-/spy- logs.

You can initiate system dumps as described below.

- **Trigger:** Enable automatic system dump in a 24h time interval. Default “off”
- **Time[hour:minute]:** Set time of automatic system dump. Default “00:00”
- **DUMP:** Start dump immediately
- **Configure specific source**: Enables a specific URL for downloading system dump. Default is “off”, the system dump is stored on the provisioning server then.
- **Protocol**: Specifies the protocol used.
- **Port**: Specifies the port of the external file server.
- **Server**: Specifies the IP address or name of the external file server.
- **User name**: Specifies the user name to authenticate on the external file server.
- **Password**: Specifies the password to authenticate on the external file server.
- **Password confirmation**: Confirms the password to authenticate on the external file server.
- **Path**: Specifies the location 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.

Parameter / Parameter group	**System dump / Trigger time**
Description	Specifies the time at which the OMM generates a system dump.
Format	String
Range	n.a.
Default value	Enable=”0” hour=”0” minute=”0”
Web	Advanced: System > System settings > System dump > Trigger
OMM Configuration files	<SetRemoteSystemDump **enable="1" hour="3" minute="0"** plainText="1"> <url enable="1" protocol="TFTP" host="ber-rd5014" path="" password="topsecret" port="0" useCommonCerts="0" /> </SetRemoteSystemDump>
DECT Phone	n.a.
User configuration files	n.a.

Parameter / Parameter group	**System dump / Specific URL**
Description	Specifies the URL where the OMM writes the generated system dump.
Format	String
Range	n.a.
Default value	Empty
Web	Advanced: System > System settings > System dump > Configure specific source
OMM Configuration files	<SetRemoteSystemDump enable="1" hour="3" minute="0" plainText="1"> **<url enable="1" protocol="FTP" host="ber-rd5014" path="/path/where/to/write/the/dump" password="topsecret" port="0" useCommonCerts="0" />** </SetRemoteSystemDump>
DECT Phone	System / Date and time
User configuration files	n.a.

10.10 CORE DUMP URL

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

Without any special configuration, the files are transferred to the server that is used to retrieve the system software (i.e., the directory of the boot image).

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

Parameter / Parameter group	**Core dump URL**
Description	Specifies the URL where the OMM writes a generated core dump.
Format	String
Range	n.a.
Default value	Empty
Web	Advanced: System / System settings / Core dump URL
OMM Configuration files	<SetCoreDumpURL plainText="1" protocol="FTP" host="ber-rd5014" path="/pub/core port="0" /> </SetCoreDumpURL>
DECT Phone	n.a.
User configuration files	n.a.

10.11 DATE AND TIME

If SNTP is configured, the date and time of the configured time zone can be synchronized with the Mitel 600 DECT phones. The date and time are provided by the OMM to the DECT phones if they initiate a DECT location registration. The rules for a time zone can be configured in the **Time zones** menu.

- **NTP server**: The NTP servers used for time synchronization.
- **Time zone**: Specifies the time zone in which the OMM is operating.

Parameter / Parameter group	**Date and time**
Description	Specifies up to 3 NTP servers and the timzone.
Format	String
Range	n.a.
Default value	1.mitel.pool.ntp.org 2.mitel.pool.ntp.org 3.mitel.pool.ntp.org
Web	System / System settings / Date and time
OMM Configuration files	<SetNTPServer ntpServerName1="1.mitel.pool.ntp.org" ntpServerName2="2.mitel.pool.ntp.org" ntpServerName3="3.mitel.pool.ntp.org" />
DECT Phone	n.a.
User configuration files	n.a.

For information on time zone configuration see section 13.

11 ADVANCED SIP OPERATIONAL FEATURES

11.1 DNS SRV

If a fully qualified domain name is configured (port=0) as proxy, outbound proxy or registrar server, the OMM performs a DNS SRV query before an appropriate SIP transaction is started, to obtain a list of servers responsible for the given SIP domain.

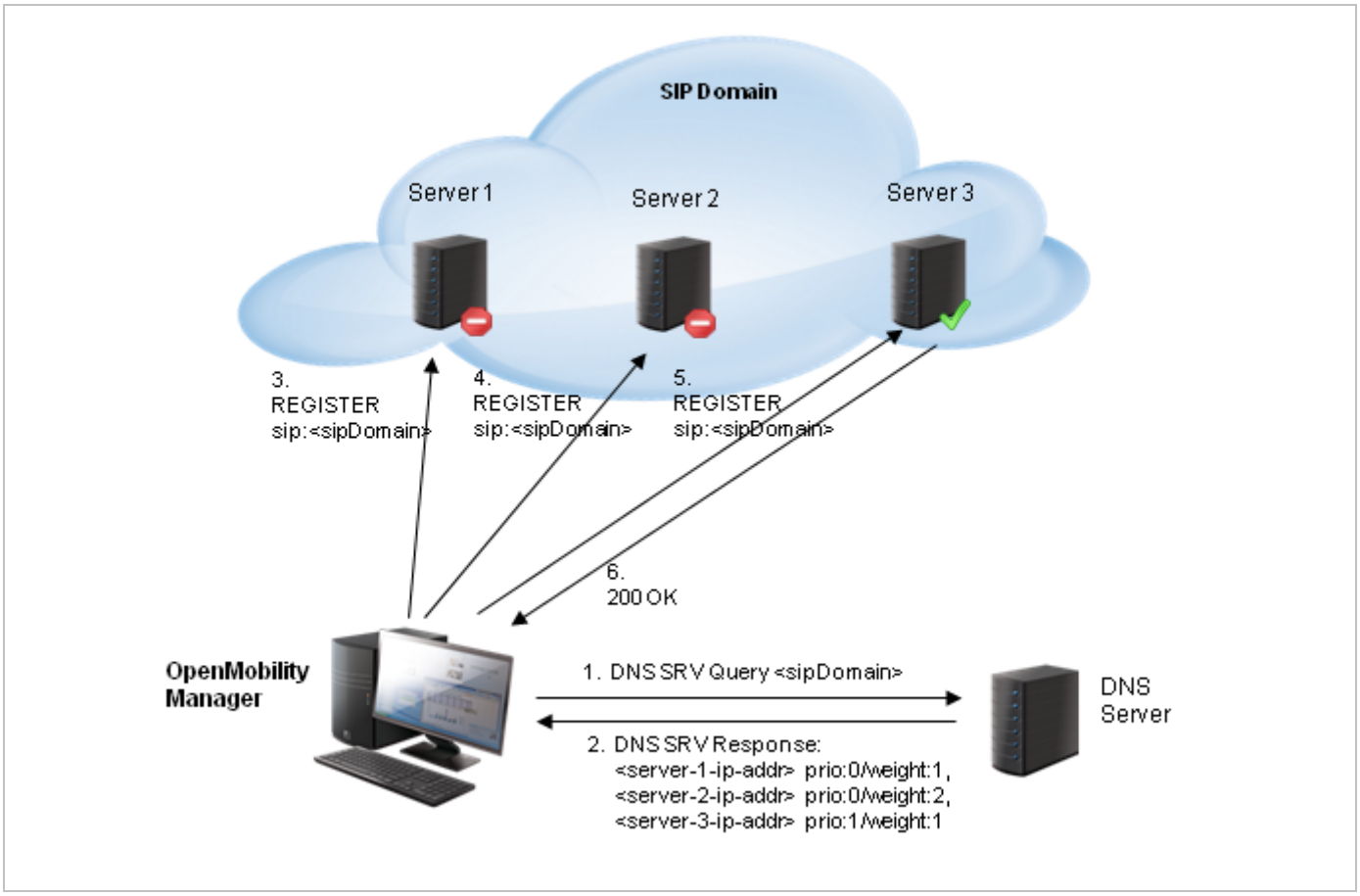
The DNS SRV results are sorted by priority and weight in ascending order by the OMM.

As soon as the DNS SRV query succeeds, the OMM starts the appropriate SIP transaction by sending the request to the server with the uppermost priority and weight of the DNS SRV result.

If there is no answer from the first SIP Call Manager within a configurable time frame (“Transaction Timer” parameter) or a 5xx response is received, it is assumed to be unavailable. The OMM tries to contact the next server in the list (that is, the second server in the DNS SRV query results).

If there is no answer in the given time frame or a 5xx response is received from the second server, the request will be sent to the third server in the list, and so on.

When there is an answer other than 5xx from one of the contacted servers, that server will be used for the SIP transaction.



To prevent situations where the OMM tries to contact servers that are unreachable (out of service) with each new transaction, the OMM offers a blacklist feature. If there is no answer from a SIP Call Manager, this specific server can be put on a blacklist and is not contacted anymore for a configurable time (“Blacklist time out”) for all subsequent SIP transactions.

In differentiation to the concepts described in the following sections, please note that regardless of which SIP Call Manager is used, all requests sent by the OMM carry the same sender Address-of-Record[1] (AOR). This means that the sender URI consisting of user-ID and domain is not changed during a failover to another server.

11.2 BACKUP SIP PROXY/REGISTAR

The OMM supports a backup SIP proxy and backup SIP registrar feature.

In addition to the primary proxy, the outbound proxy and registrar server allow the OMM to configure two additional levels of backup servers. These two additional levels of backup servers are referred to as the secondary and tertiary servers in the following sections.

Server addresses can be configured as IP addresses, names, or fully qualified domain names (port=0). It is possible to configure a mixture of IP addresses, names or fully qualified domain names for the different servers.

If fully qualified domain names are configured (port=0), the OMM uses DNS SRV queries to locate a list of servers in the domain. For simplicity in the following descriptions, it is assumed that all server addresses are given by name or IP address. Where fully qualified domain names are used, the behavior described in section 11.1 applies to contact the SIP Call Manager in the given domain.

This redundancy mechanism is based on a failover concept where the OMM tries to contact the primary server first. If the primary server fails, the OMM tries to contact the secondary server, and if the secondary server fails also, the OMM tries to contact the tertiary server.

The OMM failover behavior in detail depends on the backup server settings. The following table identifies configuration scenarios, and the method by which this specific feature works in each scenario.

IF	THEN
No secondary/tertiary proxy, outbound proxy or registrar configured	No failover to a secondary/tertiary (outbound) proxy / registrar is possible.
Secondary/Tertiary proxy and registrar are configured	All REGISTER and re-REGISTER requests attempt to use the primary registrar first. If the primary registrar fails (no answer in "transaction timer" time frame), the OMM tries to register the user with the secondary/tertiary registrar using AOR as the secondary/tertiary proxy address. When the registration with the secondary/tertiary registrar succeeds: • the MWI subscription is moved to the secondary/tertiary proxy • the OMM attempts to use the secondary/tertiary proxy for all subsequent INVITE requests

[1] RFC 3261: An address-of-record (AOR) is a SIP or SIPS URI that points to a domain with a location service that can map the URI to another URI where the user might be available. Typically, the location service is populated through registrations. An AOR is frequently thought of as the "public address" of the user.

	• the registration of all other users currently registered with the failed server will be automatically refreshed. Re-register requests will be queued and proceed according the settings for "register traffic shaping". If a user was registered successfully with the secondary/tertiary registrar and can be registered again with the primary registrar (e.g. during a re-registration): • the MWI subscription is moved back to the primary (outbound) proxy • the OMM attempts to use the primary (outbound) proxy again for all subsequent INVITE requests • the registration of all other users currently registered with secondary/tertiary registrar will be automatically refreshed As long as no successful registration exist, the OMM attempts to use the primary (outbound) proxy first for all INVITE requests. If the INVITE request to the primary proxy fails, the OMM attempts to use the secondary/tertiary proxy for the INVITE request. If an INVITE request sent to a proxy identical with own registrar fails (no answer in "transaction timer" time frame), the registration will be refreshed.
Secondary/Tertiary proxy, registrar and outbound proxy configured	Same behavior as above (Secondary/Tertiary proxy and registrar configured) but all requests for the secondary/tertiary proxy/registrar are sent through the outbound proxy.
Ony Secondary/Tertiary proxy configured	The OMM attempts to use the primary proxy or registrar first for all REGISTER, INVITE and SUBSCRIBE requests. If an INVITE/SUBSCRIBE request fails, the OMM attempts to use the secondary/tertiary proxy for the INVITE/SUBSCRIBE request.
Only Secondary/Tertiary outbound proxy configured	The OMM behavior is as described above in line “Secondary/Tertiary proxy and registrar configured”, but: • all requests for the secondary/tertiary proxy/registrar are sent through the outbound proxy • if the registration to the primary registrar fails, the registration is re-tried using the AOR as primary proxy address and is sent through the outbound proxy
Only Secondary/Tertiary registrar configured	The OMM attempts to use the primary proxy or registrar first for all REGISTER, INVITE and SUBSCRIBE requests. If a REGISTER request fails, the OMM attempts to use the secondary/tertiary registrar for the request.

Parameter / Parameter group	**Secondary proxy server**
Description	The IP address or name of the secondary SIP proxy server. If a host name and domain are used for the proxy server parameter, ensure that a DNS server and a domain are specified e.g. via DHCP.
Format	IP address or fully qualified host name
Range	n.a.

Default value	
Web	n.a.
OMM configuration files	<SetBackupSIP secondaryProxyServer="127.0.0.1" secondaryProxyPort="5060" />
DECT Phone	n.a.
User configuration files	n.a.

Parameter / Parameter group	**Secondary proxy port**
Description	Secondary SIP proxy server's port number. To enable DNS SRV support for proxy lookups, use a value of "0" for the proxy port. In case that TLS is used, the value shall be changed to "5061".
Format	Integer
Range	0, 1024-65535
Default value	5060
Web	n.a.
OMM configuration files	<SetBackupSIP secondaryProxyServer="127.0.0.1" secondaryProxyPort="5060" />
DECT Phone	n.a.
User configuration files	n.a.

Parameter / Parameter group	**Secondary registrar server**
Description	The IP address or name of the secondary SIP registrar. If a host name and domain are used for the registrar server parameter, ensure that a DNS server and a domain are specified e.g. via DHCP.
Format	IP address or fully qualified host name
Range	n.a.
Default value	
Web	n.a.
OMM configuration files	<SetBackupSIP secondaryRegServer="192.168.1.10" secondaryRegPort="5060" />
DECT Phone	n.a.
User configuration files	n.a.

Parameter / Parameter group	**Secondary registrar port**
Description	Secondary SIP registrar's port number. To enable DNS SRV support for registrar lookups, use a value of "0" for the registrar port. In case that TLS is used, the value shall be changed to "5061".
Format	Integer
Range	0, 1024-65535
Default value	5060

Web	n.a.
OMM configuration files	<SetBackupSIP secondaryRegServer="192.168.1.10" secondaryRegPort="5060" />
DECT Phone	n.a.
User configuration files	n.a.

Parameter / Parameter group	**Secondary outbound proxy server**
Description	This is the address or name of the secondary outbound proxy server.
Format	IP address or fully qualified host name.
Range	n.a.
Default value	
Web	n.a.
OMM configuration files	<SetBackupSIP secondaryOutboundProxyServer="192.168.1.20" secondaryOutboundProxyPort="5060" />
DECT Phone	n.a.
User configuration files	n.a.

Parameter / Parameter group	**Secondary outbound proxy port**
Description	Secondary SIP outbound proxy's port number. To enable DNS SRV support for outbound proxy lookups, use a value of "0" for the registrar port. In case that TLS is used, the value shall be changed to "5061".
Format	Integer
Range	0, 1024-65535
Default value	5060
Web	n.a.
OMM configuration files	<SetBackupSIP secondaryOutboundProxyServer="192.168.1.20" secondaryOutboundProxyPort="5060" />
DECT Phone	n.a.
User configuration files	n.a.

Parameter / Parameter group	**Tertiary proxy server**
Description	The IP address or name of the tertiary SIP proxy server. If a host name and domain are used for the proxy server parameter, ensure that a DNS server and a domain are specified (e.g. via DHCP).
Format	IP address or fully qualified host name
Range	n.a.
Default value	
Web	n.a.
OMM configuration files	<SetBackupSIP tertiaryProxyServer="127.0.0.1" tertiaryProxyPort="5060" />

DECT Phone	n.a.
User configuration files	n.a.

Parameter / Parameter group	**Tertiary proxy port**
Description	Tertiary SIP proxy server's port number. To enable DNS SRV support for proxy lookups, use a value of "0" for the proxy port. If TLS is used, the value shall be changed to "5061".
Format	Integer
Range	0, 1024-65535
Default value	5060
Web	n.a.
OMM configuration files	<SetBackupSIP tertiaryProxyServer="127.0.0.1" tertiaryProxyPort="5060" />
DECT Phone	n.a.
User configuration files	n.a.

Parameter / Parameter group	**Tertiary registrar server**
Description	The IP address or name of the tertiary SIP registrar. If a host name and domain are used for the registrar server parameter, ensure that a DNS server and a domain are specified (e.g. via DHCP).
Format	IP address or fully qualified host name
Range	n.a.
Default value	
Web	n.a.
OMM configuration files	<SetBackupSIP tertiaryRegServer="192.168.1.10" tertiaryRegPort="5060" />
DECT Phone	n.a.
User configuration files	n.a.

Parameter / Parameter group	**Tertiary registrar port**
Description	Tertiary SIP registrar's port number. To enable DNS SRV support for registrar lookups, use a value of "0" for the registrar port. If TLS is used, the value shall be changed to "5061".
Format	Integer
Range	0, 1024-65535
Default value	5060
Web	n.a.
OMM configuration files	<SetBackupSIP tertiaryRegServer="192.168.1.10" tertiaryRegPort="5060" />
DECT Phone	n.a.
User configuration files	n.a.

Parameter / Parameter group	**Tertiary outbound proxy server**
Description	The address or name of the tertiary outbound proxy server.
Format	IP address or fully qualified host name.
Range	n.a.
Default value	
Web	n.a.
OMM configuration files	<SetBackupSIP tertiaryOutboundProxyServer="192.168.1.20" tertiaryOutboundProxyPort="5060" />
DECT Phone	n.a.
User configuration files	n.a.

Parameter / Parameter group	**Tertiary outbound proxy port**
Description	Tertiary SIP outbound proxy's port number. To enable DNS SRV support for outbound proxy lookups, use a value of "0" for the registrar port. If TLS is used, the value shall be changed to "5061".
Format	Integer
Range	0, 1024-65535
Default value	5060
Web	n.a.
OMM configuration files	<SetBackupSIP tertiaryOutboundProxyServer="192.168.1.20" tertiaryOutboundProxyPort="5060" />
DECT Phone	n.a.
User configuration files	n.a.

11.3 BACKUP KEEP ALIVE

A keep alive mechanism implemented in the OMM allows the automatic failover to secondary/tertiary servers or automatic return to primary servers.

The keep alive mechanism is based on the registration process and utilizes the special behavior that all REGISTER and re-REGISTER requests are sent to the primary registrar first.

The following configuration parameters are introduced:

- Failover keep alive: on/off
- Failover keep alive time: 5-60 minutes

For each registration target (SIP Call Manager) that a user can successfully register with, a keep alive process is started. For this purpose, the first user registered successfully on the registration target is selected to re-register at regular intervals to ensure that the target is still accessible. Each re-registration is performed before the registration period, adjusted by "Failover keep alive time", has expired.

If the re-registration of this selected user detects that the current primary server fails, the registration of all users registered on the same server will be refreshed automatically. The re-register requests will be queued and proceed according to the settings for "register traffic shaping".

If the re-registration of a selected user detects that the primary server is available again, the registration of all users registered on a secondary/tertiary registrar will be refreshed.

Parameter / Parameter group	**Failover keep alive**
Description	Enables / Disables the keep alive mechanism. Setting this parameter to 1 starts the keep alive mechanism for each registration target.
Format	Boolean
Range	n.a.
Default value	0
Web	n.a.
OMM configuration files	<SetBackupSIP failoverActive="0" failoverTime="10" />
DECT Phone	n.a.
User configuration files	n.a.

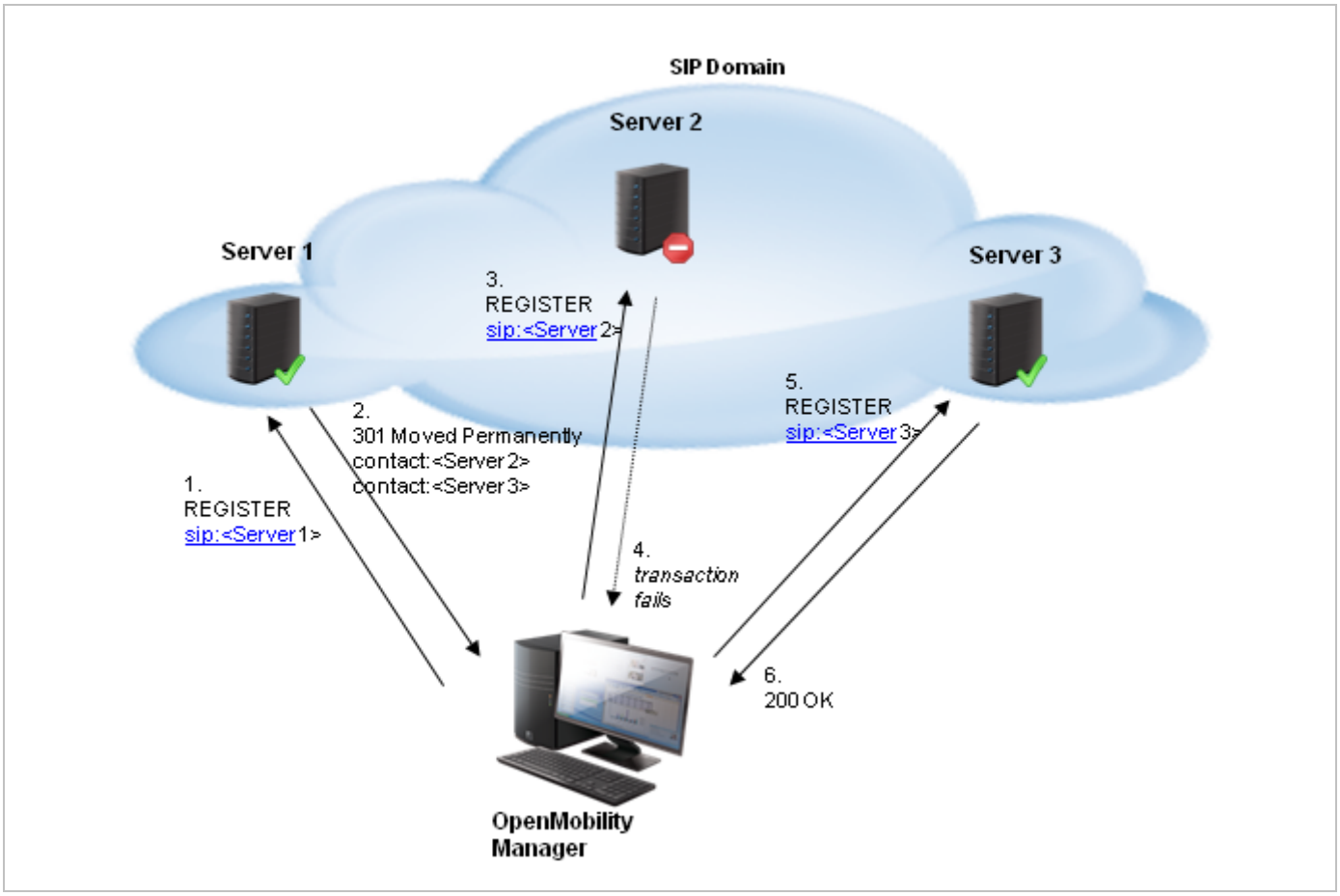
Parameter / Parameter group	**Failover keep alive time**
Description	The time, in minutes, the OMM sends out a re-REGISTER to a registration target before the registration period expires.
Format	Integer
Range	5-60 min.
Default value	10 min.
Web	n.a.
OMM configuration files	<SetBackupSIP failoverActive="0" failoverTime="10" />
DECT Phone	n.a.
User configuration files	n.a.

11.4 REGISTER REDIRECT

The OMM supports a load sharing feature based on 301 (Moved Permanently) or 302 (Moved Temporarily) responses for registrations.

When a 301 or 302 response is received, the OMM follows the redirect and registers the user concerned at the given address. If more than one contact address are given in the 301/302 response, the OMM tries to contact the registrars successively until the registration succeeds.

If the redirected register succeeds and if the configured proxy and registrar are identical, all subsequent INVITE requests are sent to the redirected server. In the other case, all subsequent INVITE requests will be sent to the (outbound) proxy or secondary/tertiary (outbound) proxy.



11.5 SRTP

SIP-DECT with Cloud-ID supports SRTP to encrypt the RTP voice streams and SDES for the SRTP key exchange.

There are three options for SRTP:

- **SRTP only**: Only SRTP calls will be accepted, all others will be rejected (the audio part of the SDP contains RTP/SAVP)
- **SRTP preferred**: All calls will be initiated as secured, but accepted if they are not secured (the audio part of the SDP contain RTP/AVP)
- **SRTP disabled**: Only RTP calls will be initiated as not ciphered and an incoming ciphering algorithm will be not accepted. All established communications are unencrypted.

SIP-DECT with Cloud-ID provides the cipher suite AES_CM_128_HMAC_SHA1_80.

Please note: SDES specifies the negotiation over SDP included in the SIP signaling as the key exchange method. Therefore, we recommend using TLS to encrypt the key exchange.

Please note: Enable “SRTP = only” mode exclusively when all communication can be established with SRTP. Depending on the call server, some features or gateways may not offer SRTP.

You configure and modify the SRTP mode using the configuration files or the OMM Web UI.

Parameter / Parameter group	**SRTP**
Description	Set the SRTP mode used by the OMM to encrypt the RTP voice streams.
Format	Enumeration
Range	**Disabled** - all communications established are unencrypted **Preferred** - all calls will be initiated as secured, but accepted if they are not secured **Only** - only SRTP calls will be accepted, all others will be rejected
Default value	Disabled
Web	System > SIP > Security
OMM configuration files	<SetSite> <site id="1" srtp="Disabled" /> </SetSite>
DECT Phone	n.a.
User configuration files	n.a.

11.6 SIP OVER TLS

The supported SIP transport protocol modes “TLS” or “Persistent TLS” enable private and authenticated signaling, including safe key exchange for SRTP encryption.

The following parameters can be set via Mitel Web UI or configuration files, and allow you to modify OMM behavior:

Parameter / Parameter group	**Persistent TLS keep alive timer active**
Description	When enabled and “Persistent TLS” is selected as transport protocol, the OMM sends keep-alive messages periodically to keep the TLS connection open.
Format	Boolean
Range	n.a.
Default value	1 (True)
Web	System > SIP > Security
OMM configuration files	<SetSecureSIP keepAliveTimeoutEnable="1" timeout="30" />
DECT Phone	n.a.
User configuration files	n.a.
Parameter / Parameter group	**Persistent TLS keep alive timer timeout**
Description	Specifies the time, in seconds, between keep-alive messages from the OMM.
Format	Integer
Range	10-3600 sec.
Default value	30 sec.
Web	System > SIP > Security

OMM configuration files	<SetSecureSIP keepAliveTimeoutEnable="1" timeout="30" />
DECT Phone	n.a.
User configuration files	n.a.

Parameter / Parameter group	**Send SIPS over TLS active**
Description	When enabled and “TLS” or “Persistent TLS” is selected as transport protocol, the OMM uses SIPS URIs in the SIP signaling.
Format	Boolean
Range	n.a.
Default value	1 (True)
Web	System > SIP > Security
OMM configuration files	<SetSecureSIP sendSipsOverTLS="1" />
DECT Phone	n.a.
User configuration files	n.a.

Parameter / Parameter group	**TLS authentication**
Description	When enabled and “TLS” or “Persistent TLS” is selected as transport protocol, the OMM validates the authenticity of the remote peer via exchanged certificates and the configured “Trusted certificates”.
Format	Boolean
Range	n.a.
Default value	1 (True)
Web	System > SIP > Security
OMM configuration files	<SetSecureSIP authenticationTLS="1" />
DECT Phone	n.a.
User configuration files	n.a.

Parameter / Parameter group	**TLS common name validation**
Description	When enabled and “TLS authentication” is selected the OMM validates the “Alternative Name” and “Common Name” of the remote peer certificate against the configured proxy, registrar and outbound proxy settings. If there is no match, an established TLS connection will be closed immediately.
Format	Boolean
Range	n.a.
Default value	0 (False)
Web	System > SIP > Security
OMM configuration files	<SetSecureSIP commonNameValidationTLS="0" />
DECT Phone	n.a.

User configuration files	n.a.

11.6.1 CERTIFICATES

The use of “TLS” or “Persistent TLS” requires the import of certificates to become operational.

Item	When Needed	Setting
Trusted Certificates	For TLS and Persistent TLS	A PEM file with a list of all (self-signed) CA certificates is required to verify remote certificates. May also contain trusted intermediate certificates instead of, or in addition to, self-signed certificates In many cases there is only one certificate in this list: The self-signed certificate which is used by the SIP proxy and registrar or which was used to sign that certificate.
Local Certificate	For TLS: Always	A PEM file with the OMM’s certificate chain
Private Key	For Persistent TLS: Only if the server verifies the client certificate	A PEM file with the OMM’s private key

All certificates and keys must be provided as X.509 certificates in PEM file format. They must use the RSA algorithm for their keys and signatures and MD5 or SHA-1 for their hashes.

Although PEM files usually contain a textual description of the certificate, only the Base64-encoded portions between

-----BEGIN CERTIFICATE-----

and

-----END CERTIFICATE-----

are actually evaluated. However, the files can be uploaded to the OMM with their full content.

There are two sets of certificates which can be set up in the OMM, which are described in the following sections.

11.6.1.1 Trusted Certificates

The trusted certificates are used to verify the signatures of certificates sent by remote hosts. The corresponding PEM file may contain multiple certificates. Their order is not relevant. Certificates are searched in the trust store according to their subject name, the key identifier (if present), and the serial number as taken from the certificate to be verified.

11.6.1.2 Local Certificates

The local certificate or local certificate chain is sent to remote hosts for authentication.

In corresponding PEM files, the host certificate must be in the first position, followed by intermediate certificates if applicable. The last certificate is the self-signed root-certificate of the CA. The root certificate may be omitted from the list, as the remote host must possess it anyway to confirm validity. This means that if there are no intermediate certificates, this file may contain only one single certificate.

11.6.2 PRIVATE KEY

The Private Key is also contained in a PEM file. The *Local Certificate* must match to the *Private Key*.

Although PEM files may contain a textual description of the key, only the Base64-encoded portions between
`-----BEGIN RSA PRIVATE KEY-----`

and

`-----END RSA PRIVATE KEY-----`

is actually evaluated. However, the file can be uploaded to the OMM with its full content.

11.6.3 TLS TRANSPORT MODE

The OMM distinguishes both TLS transport modes, **TLS** and **Persistent TLS**.

When the OMM is configured to use **TLS** (Transport protocol: TLS), TLS connections to remote peers, (e.g. SIP proxies and registrars) are established as needed. For TLS connections initiated by the OMM, it is a TLS client. If a remote peer sets up a TLS connection, the OMM is the TLS server. Connections are closed when they have not been in use for a certain time. The terms server and client refer to TLS connections below, not to SIP transactions.

The OMM always verifies the server certificate when it sets up an outgoing connection and verifies the client certificate on incoming connections. Therefore, the following configuration parameters must be set for this mode: *Trusted Certificates*, *Local Certificate* and *Private Key*.

When the OMM is configured to use **persistent TLS** (Transport protocol: Persistent TLS), it sets up TLS connections to SIP Call Managers and keeps them connected. When a connection is closed for any reason, the OMM tries to re-establish it immediately. It does not accept incoming connections from remote ends. Thus the OMM is always TLS client when Persistent TLS is in use.

The advantage of Persistent TLS is a faster call setup time and lower processing power required on both sides.

The OMM always verifies the server certificate, therefore following configuration parameters must be set for this mode: *Trusted Certificates*.

If the server verifies the client certificate, additionally the *Local Certificate* and *Private Key* parameters must be set.

11.6.4 VERIFICATION OF REMOTE CERTIFICATES

When “TLS authentication” is “ON”, a remote certificate is verified by the OMM as follows:

The signature of the certificate is checked with the public key of the signing certificate. The certificate chain is checked until a *Trusted Certificate* is found. The OMM validates against trusted CA’s (signed by a CA from the Mozilla CA certificate list) and the configured trusted certificates.

If a self-signed certificate is found which is not trusted, the verification fails.

The current time must be in the validity period of the certificate. For this mechanism a correct system time must be provided (e.g. NTP).

If one or more of these checks fail, the TLS connection will be closed.

Please note: All certificates are only valid for a limited time given by the issuer. As soon as the validity period expires, no further communication is possible. The certificates must be replaced prior to expiry, to prevent an interruption in call services.

When “TLS authentication” is “OFF”, the OMM verifies the remote certificates and logs any failure. However, the established TLS connection will not be closed in the case of verification failures.

IMPORTANT : To prevent man-in-the-middle attacks, we recommend that you do not disable the “TLS authentication” in unsecure environments. We recommend setting “TLS authentication” and “TLS common name validation” to “ON” in any unsecure environments for the best security.

11.6.5 ADDITIONAL SECURITY CONSIDERATIONS

For highest security requirements, there are additional considerations to be taken into account when enrolling a SIP-DECT with Cloud-ID system.

To prevent manipulation during the initial upload of certificates and keys to the OMM, installation of certificates should be done in a small private network without a physical connection to an insecure network.

IMPORTANT : To prevent manipulation of certificates and keys in unsecure environments, we recommend not to use the automatic import of certificates and keys. In particular, the unsecure protocols TFTP, FTP and HTTP must be avoided. It is also recommended to protect the selected protocol with a login to prevent unauthorized access to the private key file.

Furthermore, it is important that the root and administrator passwords of the OpenMobility system be safe, because with these passwords an attacker could change the configuration to manipulate the system in various ways.

Although all keys and certificates in the database are encrypted, an automated database backup or download could be a security leak if the network, transport protocol or servers used are not protected against manipulation.

11.6.6 MANUAL IMPORT OF SIP CERTIFICATES

You can import trusted certificates, a local certificate chain and a private key file for SIP manually via Web or OMM Configuration files.

Parameter / Parameter group	**Import PEM file with / Import PEM file**
Description	Specifies the type of file (trusted certificate, local certificate, or private key) and the location of the file to be imported.
Format	String
Range	n.a.
Default value	Empty
Web	System / SIP / Manual Import
OMM Configuration files	<SetSecureSIPCertificate plainText="1"> <trustedCertificates> <certificate key="-----BEGIN CERTIFICATE-----...-----END CERTIFICATE-----"/>

	<certificate key="-----BEGIN CERTIFICATE-----...-----END CERTIFICATE-----"/> </trustedCerificates> <localCertificates> <certificate key="-----BEGIN CERTIFICATE-----...-----END CERTIFICATE-----"/> </localCertificates> <privateKeys> <certificate key="-----BEGIN CERTIFICATE-----...-----END CERTIFICATE-----"/> </privateKeys> <privateKeyPassword="myPrivateKeyPassword"> </SetSecureSIPCertificate>
DECT Phone	n.a.
User configuration files	n.a.

11.6.7 AUTOMATIC IMPORT OF SIP CERTIFICATES

Optionally, there is also an automatic import of Trusted, Local Certificates and a Private Key files from an external server possible. The follwing parameters allow an automatic import:

Parameter / Parameter group	**Active**
Description	Enable or disable the automatic import.
Format	Boolean
Range	n.a.
Default value	0 (False)
Web	System / SIP / Certificate Server
OMM configuration files	<SetSecureSIPCertificateServerImport plainText="1" trustedCertificates="trust.pem" localCertificates="local.pem" privateKeys="private.pem" > <url enable="1" protocol="HTTPS" host="10.103.35.99" path="" username="" password="mypassword" port="0" useCommonerts="0" /> </SetSecureSIPCertificateServerImport>
DECT Phone	n.a.
User configuration files	n.a.

Parameter / Parameter group	**Protocol**
Description	Selects the preferred protocol

Format	Enumeration (FTP, TFTP, FTPS, HTTP, HTTPS, SFTP)
Range	n.a.
Default value	HTTPS
Web	System / SIP / Certificate Server
OMM configuration files	<SetSecureSIPCertificateServerImport plainText="1" trustedCertificates="trust.pem" localCertificates="local.pem" privateKeys="private.pem" > <url enable="1" protocol="HTTPS" host="10.103.35.99" path="" username="" password="mypassword" port="0" useCommonerts="0" /> </SetSecureSIPCertificateServerImport>
DECT Phone	n.a.
User configuration files	n.a.

Parameter / Parameter group	**Server**
Description	IP address or name of the server
Format	String
Range	n.a.
Default value	
Web	System / SIP / Certificate Server
OMM configuration files	<SetSecureSIPCertificateServerImport plainText="1" trustedCertificates="trust.pem" localCertificates="local.pem" privateKeys="private.pem" > <url enable="1" protocol="HTTPS" host="10.103.35.99" path="" username="" password="mypassword" port="0" useCommonerts="0" /> </SetSecureSIPCertificateServerImport>
DECT Phone	n.a.
User configuration files	n.a.

Parameter / Parameter group	**Port**
Description	Specifies the server’s port number.
Format	Integer
Range	1-65535; 0 = default port of protocol

Default value	0
Web	System / SIP / Certificate Server
OMM configuration files	<SetSecureSIPCertificateServerImport plainText="1" trustedCertificates="trust.pem" localCertificates="local.pem" privateKeys="private.pem" > <url enable="1" protocol="HTTPS" host="10.103.35.99" path="" username="" password="mypassword" port="0" useCommonerts="0" /> </SetSecureSIPCertificateServerImport>
DECT Phone	n.a.
User configuration files	n.a.

Parameter / Parameter group	**User name**
Description	The user name of the server account data if necessary.
Format	String
Range	n.a.
Default value	
Web	System / SIP / Certificate Server
OMM configuration files	<SetSecureSIPCertificateServerImport plainText="1" trustedCertificates="trust.pem" localCertificates="local.pem" privateKeys="private.pem" > <url enable="1" protocol="HTTPS" host="10.103.35.99" path="" username="" password="mypassword" port="0" useCommonerts="0" /> </SetSecureSIPCertificateServerImport>
DECT Phone	n.a.
User configuration files	n.a.

Parameter / Parameter group	**Password**
Description	The password of the server account data if necessary.
Format	String
Range	n.a.
Default value	
Web	System / SIP / Certificate Server

OMM configuration files	<SetSecureSIPCertificateServerImport plainText="1" trustedCertificates="trust.pem" localCertificates="local.pem" privateKeys="private.pem" > <url enable="1" protocol="HTTPS" host="10.103.35.99" path="" username="" password="mypassword" port="0" useCommonerts="0" /> </SetSecureSIPCertificateServerImport>
DECT Phone	n.a.
User configuration files	n.a.

Parameter / Parameter group	**Path**
Description	The path on the server to certificates files
Format	String
Range	n.a.
Default value	
Web	System / SIP / Certificate Server
OMM configuration files	<SetSecureSIPCertificateServerImport plainText="1" trustedCertificates="trust.pem" localCertificates="local.pem" privateKeys="private.pem" > <url enable="1" protocol="HTTPS" host="10.103.35.99" path="" username="" password="mypassword" port="0" useCommonerts="0" /> </SetSecureSIPCertificateServerImport>
DECT Phone	n.a.
User configuration files	n.a.

Parameter / Parameter group	**Use common certificate configuration**
Description	Enables the use of the system-wide certificate validation settings for this URL, as configured on the **System** / **Provisioning** / **Certificates** page.
Format	Boolean
Range	n.a.
Default value	0 (False)
Web	System / SIP / Certificate Server
OMM configuration files	<SetSecureSIPCertificateServerImport plainText="1" trustedCertificates="trust.pem" localCertificates="local.pem" privateKeys="private.pem" > <url enable="1" protocol="HTTPS" host="10.103.35.99" path="" username="" password="mypassword" port="0" useCommonerts="0" /> </SetSecureSIPCertificateServerImport>

DECT Phone	n.a.
User configuration files	n.a.

Parameter / Parameter group	**Trusted certificates file**
Description	The name of the PEM file on the given server including the trusted certificates
Format	String
Range	n.a.
Default value	
Web	System / SIP / Certificate Server
OMM configuration files	<SetSecureSIPCertificateServerImport plainText="1" trustedCertificates="trust.pem" localCertificates="local.pem" privateKeys="private.pem" > <url enable="1" protocol="HTTPS" host="10.103.35.99" path="" username="" password="mypassword" port="0" useCommonerts="0" /> </SetSecureSIPCertificateServerImport>
DECT Phone	n.a.
User configuration files	n.a.

Parameter / Parameter group	**Local certificate chain file**
Description	The name of the PEM file on the given server including the local certificate or a certificate chain
Format	Boolean
Range	n.a.
Default value	
Web	System / SIP / Certificate Server
OMM configuration files	<SetSecureSIPCertificateServerImport plainText="1" trustedCertificates="trust.pem" localCertificates="local.pem" privateKeys="private.pem" > <url enable="1" protocol="HTTPS" host="10.103.35.99" path="" username="" password="mypassword" port="0" useCommonerts="0" /> </SetSecureSIPCertificateServerImport>
DECT Phone	n.a.
User configuration files	n.a.

Parameter / Parameter group	**Private key file**
Description	The name of the PEM file on the given server including the local key

Format	String
Range	n.a.
Default value	
Web	System / SIP / Certificate Server
OMM configuration files	<SetSecureSIPCertificateServerImport plainText="1" trustedCertificates="trust.pem" localCertificates="local.pem" privateKeys="private.pem" > <url enable="1" protocol="HTTPS" host="10.103.35.99" path="" username="" password="mypassword" port="0" useCommonerts="0" /> </SetSecureSIPCertificateServerImport>
DECT Phone	n.a.
User configuration files	n.a.

11.7 REGISTRATION TRAFFIC SHAPING

The SIP-DECT with Cloud-ID system supports a feature called “Registration traffic shaping” that spreads the registration renewals of all DECT users to prevent bottlenecks in large systems. This feature is enabled by default.

Some providers use a keep-alive functionality based on SIP registration renewals for remote endpoints (IP-Centrex solution) that are behind a NAT. This feature from an SBC keeps the pinhole open and communication between the remote endpoint and the SBC is given. The “Registration traffic shaping” feature is not compatible with this NAT feature.

The two configuration parameters “Spread registration renewals” and “Renewal timer” allow you to disable the distribution mechanism and to configure a registration renewal timer, making the OMM compatible with that specific NAT feature.

Parameter / Parameter group	**Spread registration renewal**
Description	If set to ON, the OMM automatically spreads the registration renewals of all phones between the half-way mark of the registration period and 30 seconds prior to the expiration. This prevents large batches of registration renewals.
Format	Boolean
Range	n.a.
Default value	1 (ON)
Web	System > SIP > Registration traffic shaping
OMM configuration files	<SetRegistrationTrafficShaping spreadRegRenew="1" renewalTimer="15" />
DECT Phone	n.a.
User configuration files	n.a.

Parameter / Parameter group	**Renewal timer**

Description	If “Spread registration renewals” is set to OFF, the “Renewal timer” is the value, in seconds, prior to expiration, that the OMM renews registrations. The phone will automatically send registration renewals half-way through the registration period, unless half-way is more than the threshold value. For example, if the threshold value is set to 60 seconds and if the registration period is 600 seconds, the renewal REGISTER message will be sent 60 seconds prior to the expiration, as half-way (600/2) > 60. If the registration period is 100 seconds, then the renewal would be sent at the half-way point, as (100/2) < 60.
Format	Integer
Range	0-2147483647
Default value	15
Web	System > SIP > Registration traffic shaping
OMM configuration files	<SetRegistrationTrafficShaping spreadRegRenew="1" renewalTimer="15" />
DECT Phone	n.a.
User configuration files	n.a.

11.8 CONFERENCING

To improve integration with different SIP Call Managers, SIP-DECT includes support for centralized three/n-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.

The centralized 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

Conferences can be initiated from the Mitel 600 phones.

SIP-DECT with Cloud-ID 6.1 supports centralized conferences hosted by the MiVoice Business platform.

The SIP signaling implemented by MiVoice Business and MiVoice Office platforms require that the SIP-DECT implementation initiate a conference via blind transfer.

The use of some centralized call features (e.g. Park) on the MiVoice Business platform requires a SIP blind transfer in call active state. To enforce the integration with the MiVoice Business the OMM offer the initiation of such transfer by a Feature Access Code. The new “Blind transfer” Feature Access Code that 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 or the OMP.

You can define the conference mode globally for all SIP-DECT users on the **Conference** tab.

- **Server type**: Specifies the operational mode for the conference server. Available options are:
  - **None**: Neither external nor internal conference server is used.
  - **External**: An external conference server (e.g., Broadsoft) is used.

- **External – Blind Transfer**: An external conference server is used (e.g., MiVoice Business). The initiation of the conference is signaled as a blind transfer to the destination specified in the URL parameter.

- **URL**: Specifies the URL for the conference server.

Parameter / Parameter group	**Set and enable conference server**
Description	Set the centralized three/n-way conferencing feature, based on RFC 4579.
Format	conferenceServerType: Enumeration conferenceServerURI: URL
Range	conferenceServerType: “External", “External – Blind Transfer”, “None” conferenceServerURI: 380 characters. **Note**: The options “External – Blind Transfer”, “None” do not apply to n-way conference.
Default value	n.a.
Web	Advanced: System > SIP > Conference
OMM Configuration files	<SetConferenceServerSIP conferenceServerType="External" conferenceServerURI="de.mycom.conference.at.all.de" />
DECT Phone	n.a.
User configuration files	n.a.

Parameter / Parameter group	**Delete and disable conference server**
Description	Delete the centralized three/n-way conferencing feature, based on RFC 4579.
Format	conferenceServerType: enumeration conferenceServerURI: URL
Range	conferenceServerType: “External", “External – Blind Transfer”, “None” conferenceServerURI: 380 characters. **Note**: The options “External – Blind Transfer”, “None” do not apply to n-way conference.
Default value	n.a.
Web	Advanced: System > SIP > Conference
OMM Configuration files	<SetConferenceServerSIP conferenceServerType="None" conferenceServerURI="" />
DECT Phone	n.a.
User configuration files	n.a.

11.9 SUPPLEMENTARY SERVICES

The SIP supplementary services affect parameters that have direct impact on DECT Phone call processing behavior.

- **Call forwarding / Diversion**: The DECT phone user can (de)activate call forwarding/diversion in the OMM via the DECT phone menu. In some installations, the call forwarding/diversion feature in the SIP Call Manager conflicts with the OMM-based call forwarding/diversion. In this case, the OMM-based call forwarding/diversion can be deactivated so that the menu on the DECT phone is removed. This setting becomes active on DECT phones with the next DECT “Locating Registration” process (can be forced by switching the DECT phone off and on again). Call forwarding that is already activated is ignored if the call forwarding feature is deactivated.
- **Local line handling**: In some installations the implemented multiple line support in the IPBX system is in conflict with the OMM-based multiple line support. Thus, the OMM-based multiple line support can be deactivated. Note that the OMM-based multiple line support is active by default.

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

  - Only one line is handled for each user (except for an SOS call [1])
  - If a user presses the “R” key or hook-off key in a call active state, a DTMF event is sent to the IPBX via SIP INFO including signal 16 (hook-flash). All Hook-flash events are sent in every case via SIP INFO, independent of the configured or negotiated DTMF method during call setup. All other key events are sent via the configured or negotiated DTMF method.
  - The OMM-based call features “Call waiting”, “Call Transfer”, “Brokering” and “Hold” are no longer supported.
  - This setting becomes active on DECT phones with the next DECT “Locating Registration” process (can be forced by switching the DECT phone off and on again).
- **Automatic ringback on hold call:** Enables or disables a ringback on the loudspeaker if the B party of the active line releases the call. The ringing begins after the call release timeout interval (see description below).
- **Call transfer by hook (on Mitel 600)**: Enables call transfer via the hook key on a Mitel 600 DECT phone (in addition to call transfer via menu).
- **Truncate Caller Indication after ‘;’**: If the user name info in SIP to-/from-/contact headers or p-asserted-identity is extended by a suffix, which is separated by a semicolon, this suffix is truncated before the username is shown in call displays or DECT phone internal call logs.
- **Call release timeout**: Specifies the time, in seconds, after which an active line is released if the DECT phone user has not gone on-hook after the B party on an active call releases the call.
- **Hold call release timeout**: Specifies the time, in seconds, after which the active line is released if the DECT phone user has not switched to a held line (when the B party on a held call releases the call).
- **Failed call release timeout**: Specifies the time, in seconds, after which an active line is released if the called party is busy, or the call is rejected for any reason.

Parameter / Parameter group	**Call Forwarding / Diversion**
Description	The OMM-based call forwarding/diversion can be deactivated to disable the menu on the DECT phone.
Format	Boolean

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

Range	n.a.
Default value	true
Web	Advanced: System > SIP > Supplementary services
OMM Configuration files	<SetSuplServ callForwDiv="true" />
DECT Phone	n.a.
User configuration files	n.a.

Parameter / Parameter group	**Local line handling**
Description	If the implemented multiple line support in the IPBX system is in conflict with the OMM-based multiple line support, the OMM-based multiple line support can be deactivated.
Format	Boolean
Range	n.a.
Default value	true
Web	Advanced: System > SIP > Supplementary services
OMM Configuration files	<SetSuplServ locLineHndlg="true" />
DECT Phone	n.a.
User configuration files	n.a.

Parameter / Parameter group	**Automatic ringback on hold**
Description	Enables or disables a ringback on the loudspeaker if the B party of the active line releases the call.
Format	Boolean
Range	n.a.
Default value	true
Web	Advanced: System > SIP > Supplementary services
OMM Configuration files	<SetSuplServ ringingOnHold="true" />
DECT Phone	n.a.
User configuration files	n.a.

Parameter / Parameter group	**Call transfer by hook on**
Description	Enables call transfer via the hook key on a Mitel 600 DECT phone (in addition to call transfer via menu).
Format	bool
Range	n.a.
Default value	true
Web	Advanced: System > SIP > Supplementary services

OMM Configuration files	<SetSuplServ transferByHook6xxd="true" />
DECT Phone	n.a.
User configuration files	n.a.

Parameter / Parameter group	**Truncate Caller Indication after ';'**
Description	If the user name info in SIP to-/from-/contact headers or p-asserted-identity is extended by a suffix, which is separated by a semicolon, this suffix is truncated.
Format	bool
Range	n.a.
Default value	false
Web	Advanced: System > SIP > Supplementary services
OMM Configuration files	<SetSuplServ uriSeparator ="false" />
DECT Phone	n.a.
User configuration files	n.a.

Parameter / Parameter group	**Call release timeout**
Description	Specifies the time, in seconds, after which an active line is released if the DECT phone user has not gone on-hook after the B party on an active call releases the call.
Format	integer
Range	0..10
Default value	5
Web	Advanced: System > SIP > Supplementary services
OMM Configuration files	<SetSuplServ releaseInfoTimerActiveCall ="5" />
DECT Phone	n.a.
User configuration files	n.a.

Parameter / Parameter group	**Hold call release timeout**
Description	Specifies the time, in seconds, after which the active line is released if the DECT phone user has not switched to a held line (when the B party on a held call releases the call).
Format	integer
Range	0..10
Default value	5
Web	Advanced: System > SIP > Supplementary services
OMM Configuration files	<SetSuplServ releaseInfoTimerHoldCall="5" />

DECT Phone	n.a.
User configuration files	n.a.

Parameter / Parameter group	**Failed call release timeout**
Description	Specifies the time, in seconds, after which an active line is released if the called party is busy, or the call is rejected for any reason.
Format	integer
Range	0..10
Default value	5
Web	Advanced: System > SIP > Supplementary services
OMM Configuration files	<SetSuplServ releaseInfoTimerFailedCall="5" />
DECT Phone	n.a.
User configuration files	n.a.

11.10 AUTO ANSWER, INTERCOM CALLS AND AUDIO SETTINGS

Certain call features (e.g., “Auto callback”, initiated by a text message or “directDial” URI in XML notifications) 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.

The SIP-DECT solution 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

The SIP-DECT solution 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.

11.10.1 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, firmware version 4.0 or higher.

11.10.1.1 Barge-in of Incoming Intercom Calls

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

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

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

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

11.10.1.2 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”

11.10.2 AUTO ANSWER AUDIO SETTINGS

You can configure global auto-answer settings through the OMM Web service. 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.

11.10.2.1 Configuration

You can set global auto-answer settings on the **Intercom Push-to-talk** tab.

Incoming calls

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

Outgoing calls

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

Parameter / Parameter group	**Auto answer**
Description	Enables or disables auto-answer on incoming calls
Format	bool
Range	n.a.
Default value	true
Web	Advanced: System > SIP > Intercom/Push to talk
OMM Configuration files	< SetIntercomCallHandlingSIP autoAnswer="true" />
DECT Phone	n.a.
User configuration files	n.a.

Parameter / Parameter group	**Microphone mute**
Description	Enables or disables microphone muting when incoming calls are automatically answered.
Format	bool
Range	n.a.
Default value	true
Web	Advanced: System > SIP > Intercom/Push to talk
OMM Configuration files	< SetIntercomCallHandlingSIP microphoneMute="true" />
DECT Phone	n.a.
User configuration files	n.a.

Parameter / Parameter group	**Warning tone**
Description	Enables or disables warning tone on incoming call. A short ringtone is played if there are no active calls. If there is an active call in a “barge in” situation, the ringing will be in-band
Format	bool
Range	n.a.
Default value	true
Web	Advanced: System > SIP > Intercom/Push to talk

OMM Configuration files	< SetIntercomCallHandlingSIP warningTone="true" />
DECT Phone	n.a.
User configuration files	n.a.

Parameter / Parameter group	**Allow barge in**
Description	Allows/disallows “barge-in” on existing calls
Format	bool
Range	n.a.
Default value	true
Web	Advanced: System > SIP > Intercom/Push to talk
OMM Configuration files	< SetIntercomCallHandlingSIP allowBargeIn="true" />
DECT Phone	n.a.
User configuration files	n.a.

Parameter / Parameter group	**Initialisation prefix for push-to-talk**
Description	String to be entered by a DECT phone user when initiating an intercom call (which automatically triggers the destination to talk).
Format	string
Range	n.a.
Default value	String is empty, which means the feature is disabled
Web	Advanced: System > SIP > Intercom/Push to talk
OMM Configuration files	<SetIntercomCallHandlingSIP pushToTalkPrefix="" />
DECT Phone	n.a.
User configuration files	n.a.

11.11 X-AASTRA-ID

Some Mitel iPBXs need information about the type, model, version and IPEI of subscribed DECT terminals to manage them appropriately. This can be determined during the SIP registration with the SIP header X-Aastra-Id. For terminal type identification purposes, the private X-Aastra-Id header can be sent out with each SIP REGISTER message when this feature is activated.

Parameter / Parameter group	**X-Aastra-ID info**
Description	Enables or disables sending out the private X-Aastra-Id header during SIP registrations.
Format	Boolean
Range	n.a.

Default value	0 (OFF)
Web	n.a.
OMM Configuration files	<SetAdvancedSIP xAastraId="0" />
DECT Phone	n.a.
User configuration files	n.a.

12 USER ADMINISTRATION

The OMM provides three different user account types to manage the SIP-DECT with Cloud-ID solution. These user accounts are preset on delivery. They can be changed in the **User administration** menu of the OMM web service or on the DECT phone via the **System menu** > **Administration** > **System** > **User administration** menu entry.

Full access:

This access type is the “normal” access for configuration. An account with full access allows you to configure the OMM and each DECT base station. On the SSH interface of a base station, this access type allows login for debug information (e.g. “pinging” another RFP to check visibility).

Factory settings for this account are:
Name: 'Omm'
Password: 'Omm'
Active: 'n/a'

After initial installation or after resetting the OMM to factory settings, the OMM web service is accessible via the default Full access user account with the name and password noted above.

Read only:

As the name suggests, this access type does not permit configuration of any part of the OMM installation. This access type can only be used on the OMM Web service. The account can be optionally enabled.

Factory settings for this account are:
Name: 'user'
Password: 'user'
Active: 'no’

Root (SSH only):

This access type is only applicable on the SSH interface of a DECT base station. This access type can be used to obtain detailed information (e.g., parameters from the kernel). The access using this account type is not reachable from other hosts, hence a login using the full access type is necessary.

The factory setting for this account is
Name: 'root'
Password: '22222'
Active: 'n/a'

Note that access to the root user level by ssh is only possible after a Full access user login.

> **Please note:** It is highly recommended not to use the “Root (SSH only) access” account type. It is meant for technical support only.

You configure the user accounts to manage the SIP-DECT with Cloud-ID system on the OMM **User administration** page. The following parameters can be configured:

- **Account type:** Select the account type you wish to change.

- **Active:** Applies to the Read-only account. Using this account, a user cannot configure any part of the SIP-DECT with Cloud-ID system. The account can be deactivated.
- **User name:** If desired, enter a new user name.
- **Password, Password confirmation:** Enter the appropriate data in these fields.
- **Password aging:** A timeout for the password can be set. Select the duration for which the password should be valid.

Parameter / Parameter group	**AccountType**
Description	Contains all parameters required for changing a user account.
Format	n.a.
Range	n.a.
Default value	n.a.
Web	System > User Administration
OMM Configuration files	<SetAccount plainText="1"> <account id="0" username="ro" password="topSecret" active="1" aging="none"> <permission>AllCnfRead</permission> </account> </SetAccount>
DECT Phone	System menu > Administration > System > User administration
User configuration files	n.a.

Parameter / Parameter group	**AccountType / id**
Description	Select user account to be changed.
Format	Integer
Range	0 .. Read only 1 .. Full access 2 .. Root (SSH only)
Default value	n.a.
Web	System > User Administration > Account type
OMM Configuration files	<SetAccount plainText="1"> <account id="0" username="ro" password="topSecret" active="1" aging="none"> <permission>AllCnfRead</permission> </account> </SetAccount>
DECT Phone	System menu > Administration > System > User administration > <USER>
User configuration files	n.a.

Parameter / Parameter group	**AccountType / username**
Description	Select new user name.

Format	String
Range	0..32 characters
Default value	n.a.
Web	System > User Administration > User name
OMM Configuration files	<SetAccount plainText="1"> <account id="0" **username="ro**" password="topSecret" active="1" aging="none"> <permission>AllCnfRead</permission> </account> </SetAccount>
DECT Phone	System menu > Administration > System > User administration > <USER> > User name
User configuration files	n.a.

Parameter / Parameter group	**AccountType / password**
Description	Select new password.
Format	String
Range	0..32 characters
Default value	n.a.
Web	System > User Administration > Password
OMM Configuration files	<SetAccount plainText="1"> <account id="0" username="ro" **password="topSecret"** active="1" aging="none"> <permission>AllCnfRead</permission> </account> </SetAccount>
DECT Phone	System menu > Administration > System > User administration > <USER> > Password
User configuration files	n.a.

Parameter / Parameter group	**AccountType / active**
Description	Enable/disable account (Applicable for ‘Read only’ account only).
Format	Integer
Range	0..deactivate 1.. activate
Default value	n.a.
Web	System > User Administration > Active
OMM Configuration files	<SetAccount plainText="1"> <account id="0" username="ro" password="topSecret" **active="1"** aging="none"> <permission>AllCnfRead</permission>

	</account> </SetAccount>
DECT Phone	n.a.
User configuration files	n.a.

Parameter / Parameter group	**AccountType / aging**
Description	Select password aging.
Format	String
Range	none time3Month time6Month
Default value	none
Web	System > User Administration > Password aging
OMM Configuration files	<SetAccount plainText="1"> <account id="0" username="ro" password="topSecret" active="1" **aging="none"**> <permission>AllCnfRead</permission> </account> </SetAccount>
DECT Phone	n.a.
User configuration files	n.a.

13 TIME ZONES

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

The OMM provides all available **Time zones**. They are set with their known Daylight Savings Time rules adjusted to the Universal Coordinated Time (UTC) per default. The difference to the UTC time is shown at the WEB service in the **UTC difference** column. If there is a configured Daylight Savings Time rule (**DST** column), this is also marked for each time zone.

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

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

The following actions can be performed for the **Time zones**:

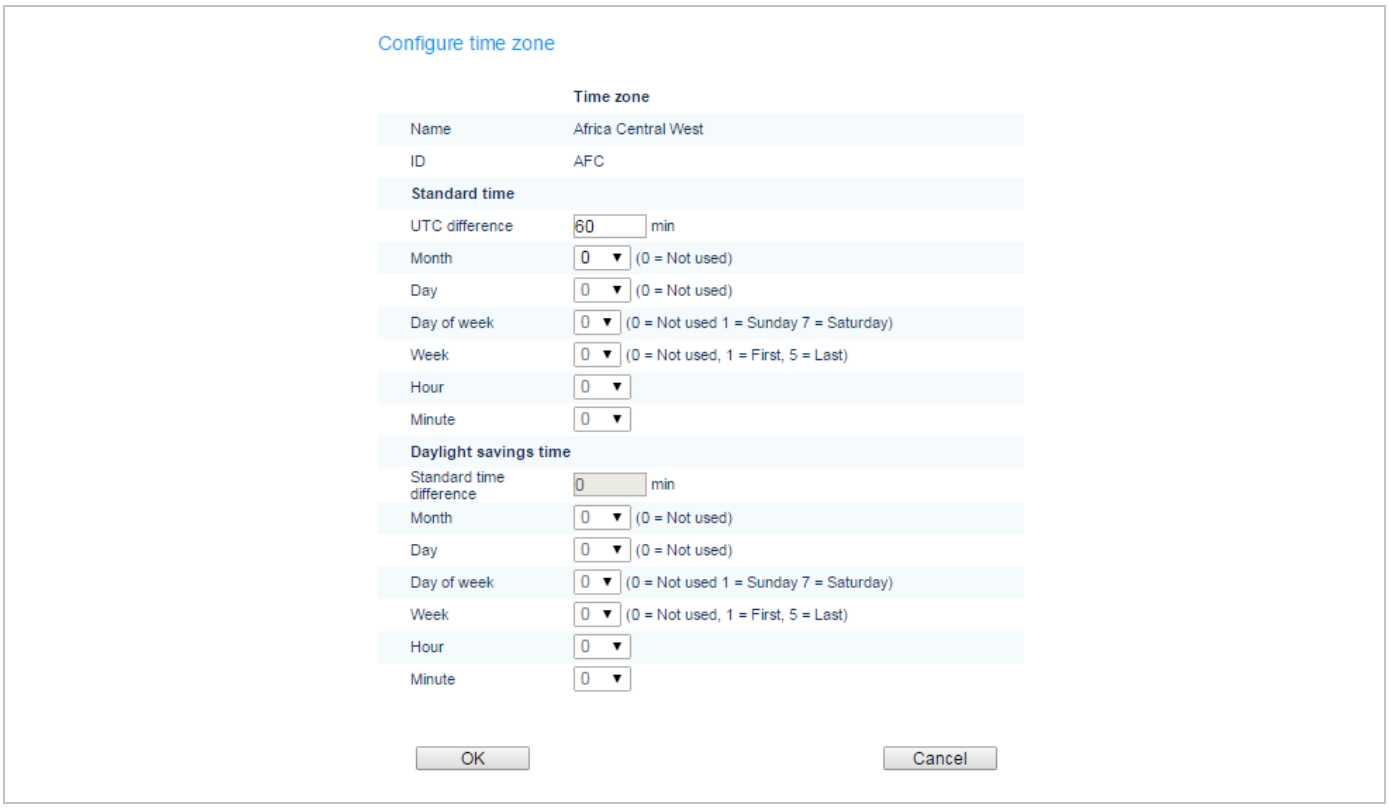
- changing the time zones
- resetting time zones

13.1 TIME ZONES CONFIGURATION

You can change the time zone rules for a maximum of five time zones. Changed rules are marked with a bold time zone name in the table in the Web service. Changes are saved in the configuration file and are restored after each OpenMobility Manager startup.

3 To change time zone settings in the Web service, click on the icon beside the time zone entry.
The **Configure time zone** dialog opens.

4 You can change the standard time and the Daylight Savings Time (DST) of a time zone. If the time zone has no DST, only the UTC difference can be configured. For the DST, both points of time (start of Standard Time and start of Daylight Savings Time) must be specified exactly. Therefore a certain day in the month or a certain week day in a month can be used. See the following screenshot as an example:



Please note: The “One free time zone” item at the end of the list is available for setting up a non-covered time zone or for test purposes to edit.

Parameter / Parameter group	**Time zone standard time (all OMM known time zones)**
Description	Each OMM time zone standard is setup per default and can be configured individually by setting the standard time.
Format	n.a.
Range	n.a.
Default value	n.a.
Web	Advanced: System > Time Zones > > <standard time values (see below)> UTC difference - in minutes Month - month the DST ends, 0 when DST is not used Day - day the DST ends, 0 when DST is not used Day of week - day of week the DST ends, 0 when DST is not used Week - week the DST ends, 0 when DST is not used Hour - hour the DST ends, 0 when DST is not used Minute - minute the DST ends, 0 when DST is not used
OMM configuration files	n.a.
DECT Phone	n.a.

User configuration files	n.a.

Parameter / Parameter group	**Time zone DST time (all OMM known time zones)**
Description	Each OMM time zone Daylight Saving Time (DST) is setup per default and can be configured individually by setting the Daylight Saving Time.
Format	n.a.
Range	n.a.
Default value	n.a.
Web	Advanced: System > Time Zones > > <DST values (see below)> Standard time difference - in minutes Month - month the DST starts, 0 when DST is not used Day - day the DST starts, 0 when DST is not used Day of week - day of week the DST starts, 0 when DST is not used Week - week the DST starts, 0 when DST is not used Hour - hour the DST starts, 0 when DST is not used Minute - minute the DST starts, 0 when DST is not used
OMM configuration files	n.a.
DECT Phone	n.a.
User configuration files	n.a.

13.2 RESETTING TIME ZONES

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

Parameter / Parameter group	**Time zone reset (all OMM known time zones)**
Description	Resets all time zones back to OMM defaults.
Format	n.a.
Range	n.a.
Default value	n.a.
Web	Advanced: System > Time Zones > Default
OMM configuration files	n.a.
DECT Phone	n.a.
User configuration files	n.a.

14 SNMP

Each DECT base station implements an SNMP agent with read-only functionality. Networks with SNMP manager can monitor basic network statistics and operating system information.

All SNMP agents are configured by the OMM. Additional parameters that are valid for the individual base station (e.g. “sysLocation” and “sysName”) are generated. The “sysLocation” parameter corresponds to the configured location. The “sysName” parameter is generated using the MAC address and the base station device type (e.g. RFP 43 WLAN). The DECT base station is available in the “sysUpTime” parameter. This value indicates how long the base station application has been connected to the OpenMobilityManager.

The SNMP agent responds to SNMPv1-read and SNMPv2c-read requests for the standard MIB-II objects. The Management Information Base (MIB-II) contains eleven object groups. If configured, the agent sends SNMPv1 and SNMPv2c traps. It sends a “coldStart” trap when it first starts up. It also sends an enterprise-specific trap “nsNotifyShutdown” when it stops. When the SNMP agent receives an SNMP request using an unknown community name, it sends an “authenticationFailure” trap. The SNMP agent also generates an enterprise-specific trap “nsNotifyRestart” (rather than the standard “coldStart” or “warmStart” traps) after being reconfigured.

Parameter / Parameter group	**readCommunity**
Description	The readCommunity is a string sent by the SNMP management system when querying devices. The query is answered by the SNMP agent only if the SNMP community string matches.
Format	String
Range	20 characters
Default value	n.a.
Web	Advanced: System > SNMP
OMM configuration files	<SetSNMP readCommunity="readOnly" contact="admin@company.com" enableTraps="1" trapCommunity="trap" trapHostAddr="10.103.35.100" />
DECT Phone	n.a.
User configuration files	n.a.

Parameter / Parameter group	**contact**
Description	A descriptive text that is typically displayed in the SNMP management software.
Format	String
Range	40 characters
Default value	n.a.
Web	Advanced: System > SNMP
OMM configuration files	<SetSNMP readCommunity="readOnly" contact="admin@company.com" enableTraps="1" trapCommunity="trap" trapHostAddr="10.103.35.100" />
DECT Phone	n.a.
User configuration files	n.a.

Parameter / Parameter group	**enableTraps**
Description	If enabled, traps are sent by the SNMP agent.
Format	boolean
Range	“0” or “1”
Default value	“0”
Web	Advanced: System > SNMP
OMM configuration files	<SetSNMP readCommunity="readOnly" contact="admin@company.com" enableTraps="1" trapCommunity="trap" trapHostAddr="10.103.35.100" />
DECT Phone	n.a.
User configuration files	n.a.

Parameter / Parameter group	**trapCommunity**
Description	Community name for traps sent to the SNMP manager.
Format	string
Range	20 characters
Default value	n.a.
Web	Advanced: System > SNMP
OMM configuration files	<SetSNMP readCommunity="readOnly" contact="admin@company.com" enableTraps="1" trapCommunity="trap" trapHostAddr="10.103.35.100" />
DECT Phone	n.a.
User configuration files	n.a.

Parameter / Parameter group	**trapHostAddr**
Description	Community name for traps send to the SNMP manager.
Format	string
Range	IP address
Default value	n.a.
Web	Advanced: System > SNMP
OMM configuration files	<SetSNMP readCommunity="readOnly" contact="admin@company.com" enableTraps="1" trapCommunity="trap" trapHostAddr="10.103.35.100" />
DECT Phone	n.a.
User configuration files	n.a.

15 DATABASE MANAGEMENT

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

The OMM database can be saved to an external server. If the OMM DECT base station experiences a failure, the databse can be restored on another base station.

In addition, you can configure whether the user-device associations are preserved (or not) when the database is restored. A backup can be initiated from the OMM Web service.

The OMM database can be:

- manually imported from the Web browser's file system or from an external server (see section 15.1)
- manually exported to the Web browser's file system or to an external server (see section 15.2)

> **Please note:** The OMM database is saved in a compressed file in a proprietary format. Any modification of this file outside the OMM is not allowed and the database cannot be re-imported.

Additionally this section also contains the configuration of the external user data provisioning / external user data server.

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

15.1 MANUAL DATABASE IMPORT

Before the OMM accepts the database from the specified source, a validation check is performed to verify that the database is valid. For errors during the database import, please refer to the **Status** page on the WEB service (see section 9).

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

Parameter / Parameter group	**Manual database import**
Description	Specifies the source of the OMM database configuration files for manual import. The following parameters are relevant: - Protocol: kind of protocol - Server: server address when a protocol to a server is used - Port: optional server port - User name: optional for used accounts on the server - Password: optional for used accounts on the server - Path: path location on the server - Use common certificate configuration: enables/disables the config URL certificate usage when a protocol to a server is used
Format	n.a.
Range	Protocol: TFTP | FTP | FTPS | HTTP | HTTPS | SFTP | FILE (local file system) Server: n.a. / mandatory when a protocol to a server is used Port: n.a. / optional User name: n.a. / optional Password: n.a. / optional Path: n.a. / optional Use common certificate configuration: n.a. / optional
Default value	None
Web	Advanced: System > DB Management > Manual import : <parameter>
OMM configuration files	n.a.
DECT Phone	n.a.
User configuration files	n.a.

15.2 MANUAL DATABASE EXPORT

For errors during the database export, refer to the **Status** page on the WEB service (see section 9).

Parameter / Parameter group	**Manual database export**
Description	Specifies the destination of the OMM database configuration for export. The following parameters are relevant: Protocol: kind of protocol Server: server address when a protocol from a server is used

	Port: optional server port User name: optional for used accounts on the server Password: optional for used accounts on the server Path: path location on the server Use common certificate configuration: enables/disables the config URL certificate usage when a protocol from a server is used
Format	n.a.
Range	Protocol: TFTP | FTP | FTPS | HTTP | HTTPS | SFTP | FILE (local file system) Server: n.a. / mandatory when a protocol from a server is used Port: n.a. / optional User name: n.a. / optional Password: n.a. / optional Path: n.a. / optional Use common certificate configuration: n.a. / optional
Default value	None
Web	Advanced: System > DB Management > Manual export : <parameter>
OMM configuration files	n.a.
DECT Phone	n.a.
User configuration files	n.a.

15.3 USER DATA IMPORT

The user data import feature allows the import of user data from an external provisioning server.

For further information on the user data import, refer to the “OpenMobility Provisioning” User Guide for details see /28/.

Parameter / Parameter group	**User data import**
Description	Specifies the server source where the user configuration files can be obtained and whether this source/feature shall be used. The following parameters are relevant (Web service names / XML names in OMM configuration files): • Configure specific source / enable: enables/disables the feature usage • Protocol / protocol: kind of protocol Server / server: server address • Port / port: server port • User name / user: optional for used accounts on the server • Password / password: optional for used accounts on the server • Path / path: path location on the server • Use common certificate configuration/ useCommonCerts: enables/disables the config URL certificate usage **Note**: If no credentials are specified for secure protocols, the system credentials are automatically used (see section 6.3). If the system credentials must not be used, the user name and password must be explicitly set here even for anonymous settings.

Format	n.a.
Range	• Configure specific source: n.a. • Protocol: TFTP | FTP | FTPS | HTTP | HTTPS | SFTP • Server: n.a. / mandatory when feature activated • Port: n.a. / optional • User name: n.a. / optional • Password: n.a. / optional • Path: n.a. / optional • Use common certificate configuration: n.a. / optional
Default value	None
Web	Advanced: System> DB Management > User data server : <parameter>
OMM configuration files	**Activate feature**: <SetUserDataServer> <url enable="1" protocol="TFTP" host="10.103.35.14" path="/userConfigFiles/" /> </SetUserDataServer> or <SetUserDataServer plainText="1" > <url enable="1" protocol="HTTPS" host="10.103.35.14" port="8443" path="/userConfigFiles/" user="User" password="Password" useCommonCerts="1" /> </SetUserDataServer> **Note**: These are examples, certain server conditions have to be adapted. **Deactivate feature**: <SetUserDataServer><url enable="0" /></SetUserDataServer>
DECT Phone	n.a.
User configuration files	n.a.

16 EVENT LOG

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

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

17 BASE STATIONS

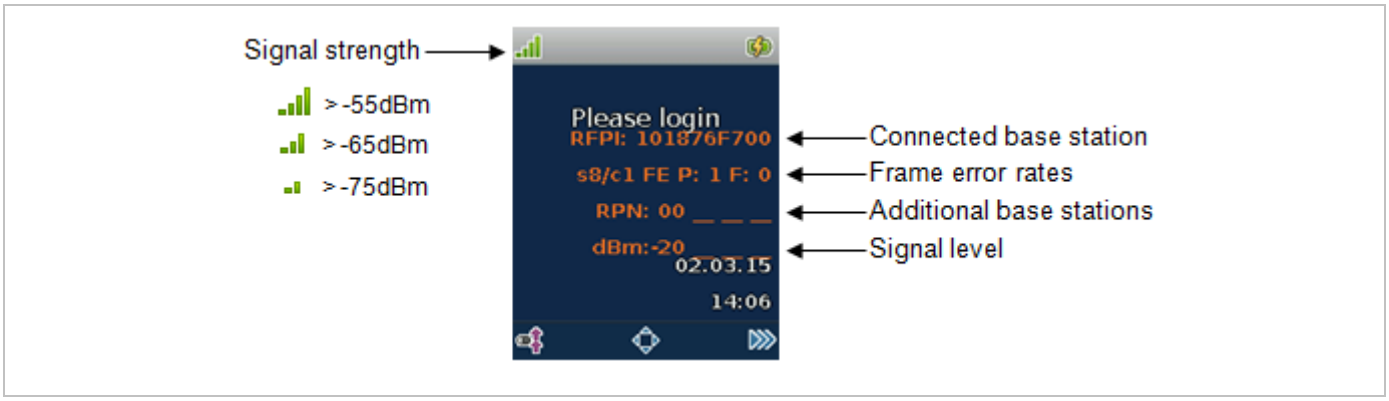
To extend the coverage area of the DECT system, you can install up to 10 DECT base stations to build a multi-cellular DECT network controlled by the OMM. The base stations must be connected to the same network subnet.

DECT phones are reachable in the entire network and can perform seamless handovers as the user moves through the network. This requires an overlapping area between base stations (requires an overlap of -60 to -65 dBm).

Base stations with visibility to each other can synchronize over the air to build one cluster. Handover is only possible within a cluster and requires base station-to-base station visibility of -70 dBm. Note that SIP-DECT with Cloud-ID only supports one DECT cluster, so all connected DECT base stations must be in sync.

To determine the correct base station position, you can use the DECT phone to measure the base station signal levels with the built-in site survey mode. (Menu > * 2 #).

The Mitel 600 DECT Phone site survey mode displays the following:



17.1 INSTALLATION OF ADDITIONAL BASE STATIONS

The voice quality of the system depends on the distance beween DECT Phone and base station and the environment of the base station. The range around a base station which allows calls with good voice quality is called the coverage area of a base station.

The radio coverage range of a base station depends on several factors:

- transmission power of the base station and DECT Phone, which is different depending on the regulatory domain the system is used in
- structure and material of the building the system is installed in. In particular, the following materials cause a significant reduction of coverage range: reinforced concrete, metal plated walls, metal coated glass, metal installations and machines.

For a rough first estimation of radio coverage area, the following guidelines can be used:

- inside a building without walls and no reflecting environment: 20..30m
- inside a building with light weight construction walls without metallic shielding: 10..20m
- inside a building with reinforced conrete walls: 5..15m

See chapter 27.5 for more details about radio wave propagation.

The coverage area of the system can be increased by installing additional base stations.

You can determine the position for an additional base station using the following procedure:

1. Establish a call via the installed and running system with a DECT Phone.
2. Walk (with the DECT Phone) in direction of the area which shall be covered by the system and monitor the voice quality of the DECT Phone.
3. If the voice quality of the call deteriorates (massive clicks, dropouts and/or noise artefacts), an additional base station should be mounted close to this position.

Since the coverage area of the new base station will overlap with the coverage area of the already installed base station(s), it should be possible to choose the next possible place a short distance away from the point estimated by the procedure described above. Verify that the base station is synchronized with its neighbours by checking the **Base stations** page in the Web service (see section 17.3 for more information).

Beside the coverage area aspects, the considerations described in chapter 4.1 must also be taken into account when installing additional base stations.

17.2 REGISTER NEW BASE STATIONS

A new base station must be registered with the OMM.

The registration can be set up in a automatic manner (OMM discovery) or by manual input of the base station's MAC address through the Web service.

> **Please note:** For OMM discovery, the new base stations must be running SIP-DECT software 6.0SP2 or higher.

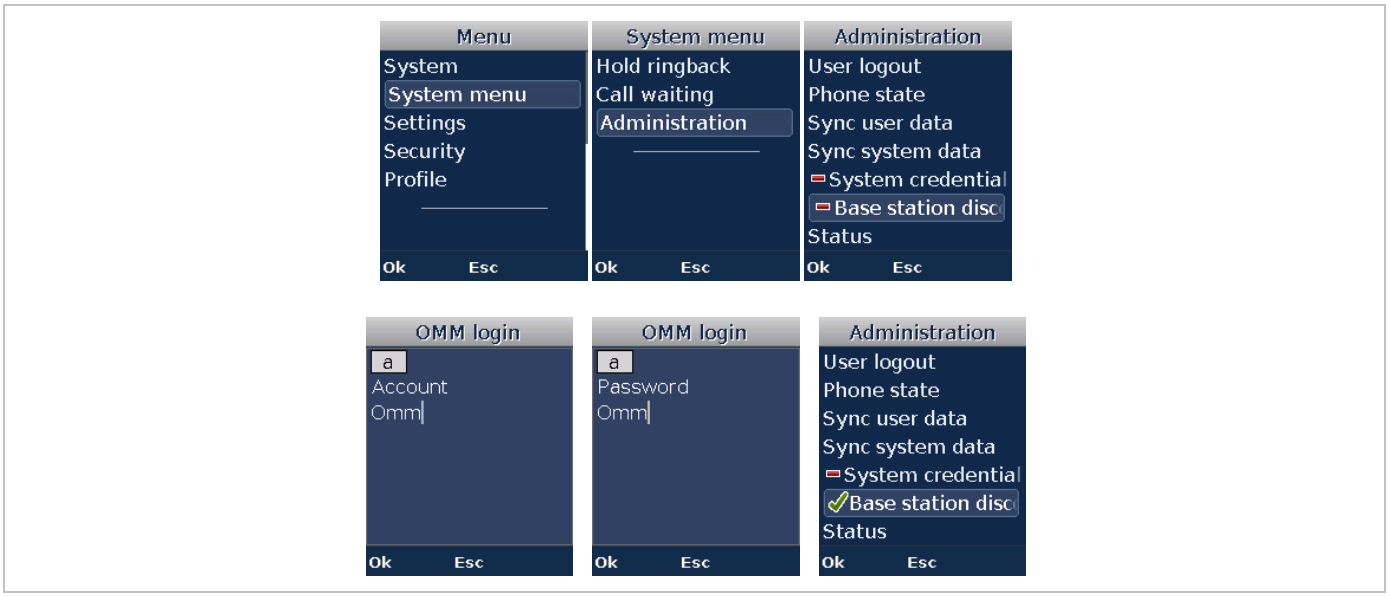
17.2.1 OMM DISCOVERY

With the OMM-discovery function, a new installed base station is able to find and register itself automatically with the OMM.

After successful registration of a base station. the OMM discovery protocol will be deactivated and must be activated again for every additional base station. There are two ways to start the OMM-discovery protocol: through the DECT phone or the Web service.

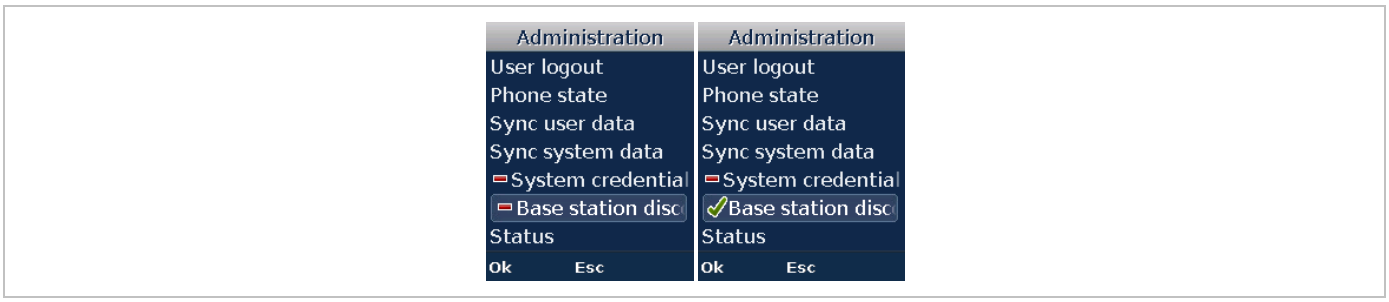
17.2.1.1 Activation using the DECT Phone

1. Position the new base station and connect it to the network.
2. Activate the base station discovery protocol as follows:



3 Wait until the first 3 LEDs on the base station are green (this may take up to 1 minute). The discovery function stops after successful registration.

4 Press the <Ok> button twice to reactivate base station discovery.



5 Repeat step 4 for every additional base station.

17.2.1.2 Activation using the Web service

1 Position the new base station and connect it to the network.

2 Activate the base station discovery protocol by pressing the **Start** button at the “Accept new base station” entry on the **Base Stations** Web service page. The new installed base station will find the OMM automatically.

3 Wait until the base station is listed in the Web service (this may take up to 1 minute). The discovery function stops after successful registration.

4 Repeat these steps for every further base station.

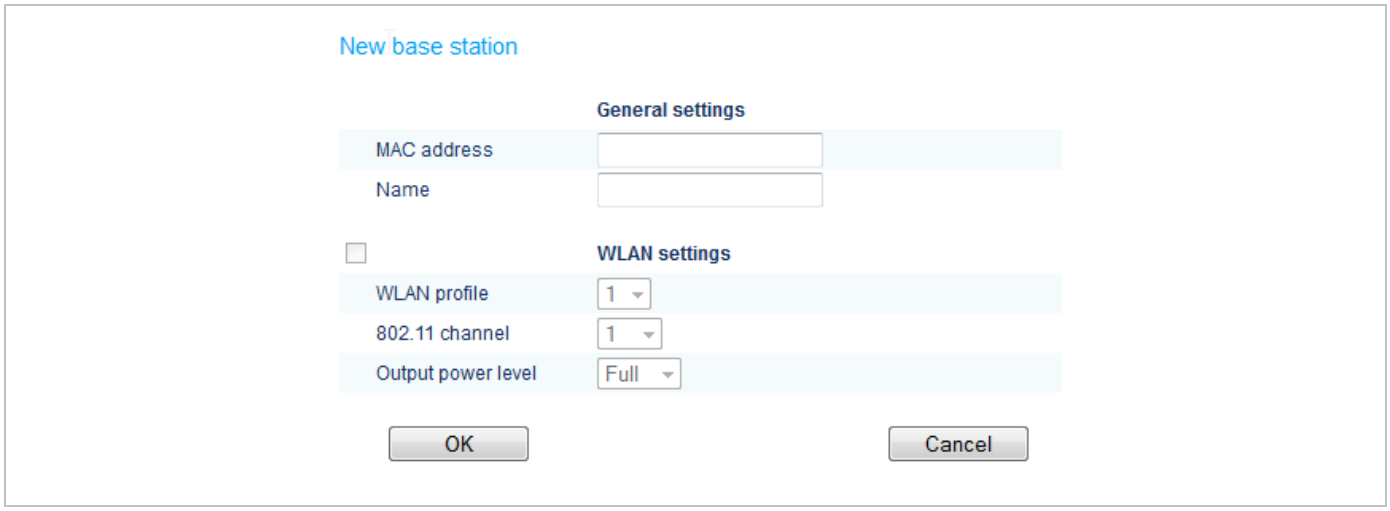
17.2.2 MANUAL REGISTRATION

17.2.2.1 Register a new base station using the Web service

A new base station can registered by setting the base station MAC address and name in the Web service.

1 Navigate to the **Base Stations** page (see section 17.3).

2 Enter the MAC Address and a name for the base station and click **OK**.



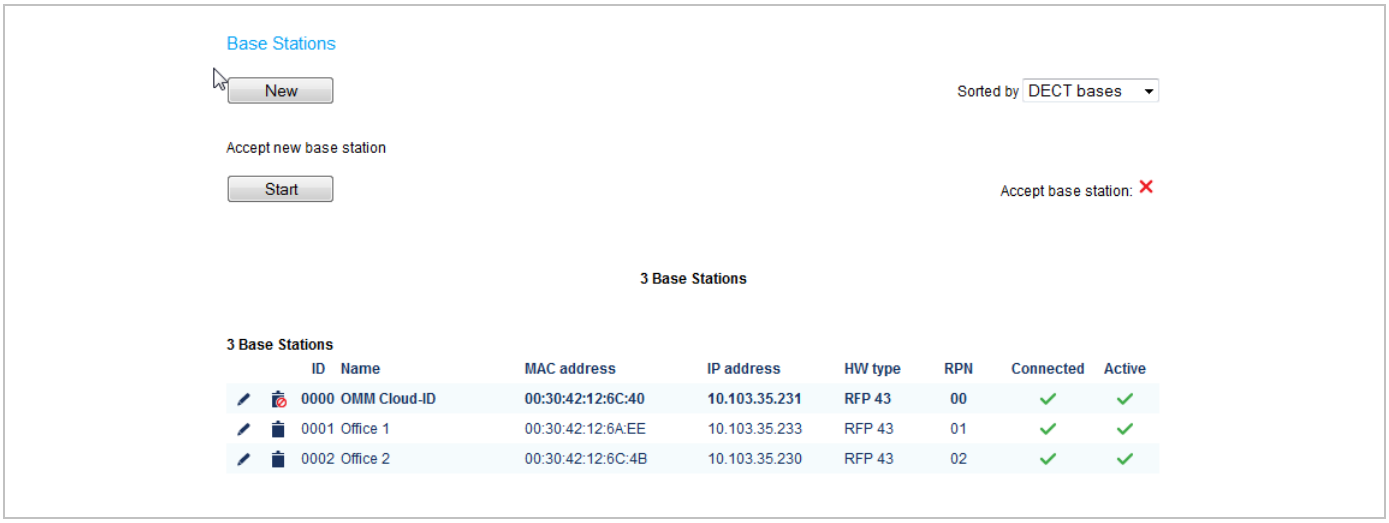
3 Repeat step 2 for every new base station.

4 Position all base stations and connect them to the network.

5 Wait until all base stations are listed in the Web service.

Parameter / Parameter group	**Register new base station**
Description	Register a new base station with the OMM.
Format	n.a.
Range	n.a.
Default value	n.a.
Web	Base Stations -> New MAC Address - Ethernet address of the base station Name - Name or location of the base station
OMM Configuration files	n.a.
DECT Phone	n.a.
User configuration files	n.a.

17.3 WEB SERVICE BASE STATIONS MENU



- **New**: Register a new base station with the OMM.
- **Activate new base station:** Start/Stop the OMM discovery protocol.

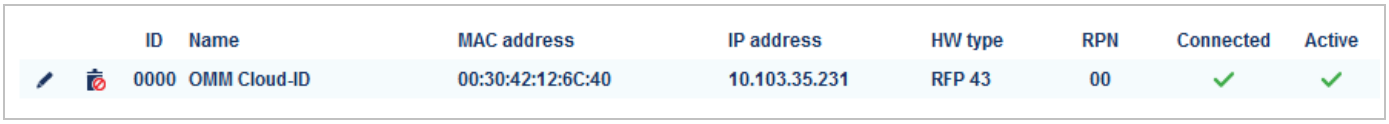
The table provides information on all configured base stations and their status in several columns:

- **ID**: An internal number that is used to manage the base station.
- **Name**: The name assigned to the base station.
- **MAC address**: MAC address of the base station.
- **IP address**: Current IP address of the base station. The IP address may change over time by using dynamic IP assignment on the DHCP server.
- **HW type**: Hardware type of the base station, submitted by the base station when it connects to the OMM. If an error message is indicated in this column, there is a mismatch between the base station and the OMM software version
- **RPN**: The Radio Fixed Part Number that is currently used by the base station.
- **Connected**: Indicates if the base station is connected to the OMM.
- **Active**: Indicates if the base station is active

17.3.1 BASE STATION STATES

For each base station, the state of the DECT subsystem is displayed. These states are:

Synchronous



The base station is up and running. The base station recognizes and is recognized by other base stations through its air interface, and delivers a synchronous clock signal to the DECT phones.

Asynchronous

ID	Name	MAC address	IP address	HW type	RPN	Connected	Active
0000	OMM Cloud-ID	00:30:42:12:6C:40	10.103.35.231	RFP 43	00	✓	✗

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

Searching

ID	Name	MAC address	IP address	HW type	RPN	Connected	Active
0000	OMM Cloud-ID	00:30:42:12:6C:40	10.103.35.231	RFP 43	00	✓	🔍

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

Not connected

ID	Name	MAC address	IP address	HW type	RPN	Connected	Active
0000	OMM Cloud-ID	00:30:42:12:6C:40	–	RFP 43	00	✗	–

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

18 SIP USERS/DEVICES

18.1 USERS

After a DECT phone is subscribed to the SIP-DECT with Cloud-Id system, a user is requested to login at the DECT phone. The user must be created in the system and on the SIP call server for a successful login, and prior to being able to set up and receive calls at the DECT phone.

User configuration in the the SIP-DECT with Cloud-Id system can be accomplished through configuration files on a provisioning server, user configuration files located on a user data server, or through the OMM web service.

18.1.1 USER CONFIGURATION FILES

The user configuration files (user_common.cfg and <user>.cfg) enable the “External User Data Provisioning” feature, which allows customers to import user data from a provisioning server. See the OM DECT Phone Sharing & Provisioning User Guide /28/ for a full description of this feature.

In addition, <user>.cfg can also refer to user.cfg, a common file name for all users depending on the **Use Common Filename On Server** (*UDS_CommonUserFileName)* configuration attribute. When enabled, the OMM tries to fetch the same user.cfg file from the provisioning server for each user executing the login procedure, such that the login credentials of each user are used to access the provisioning server. This means that the provisioning server executes user authentication and provides a user-specific user.cfg when the user is authorized.

In this mode, the user authentication is performed on the server providing the user configuration (not on the OMM). It is recommended that you use Digest authentication on the server to secure the user login credentials.

The **User Commn Configuration File Update Interval** and **Common Filename On Server** attributes are set via the *user_common.cfg* file.

> **Please note:** The common user file name feature is only applicable in combination with the file transfer protocols FTP, FTPS, HTTP, HTTPS or SFTP, which may require user/password credentials. Changing this attribute might cause login/logout problems for the users, because of changed authentication. It is up to the administrator to trigger user forced logouts (delete users). The administrator must provide new authentication data to users for their logins and logouts. This value is stored in the OMM database. So, the setting is stored over system restart and has no default value when not explicitly set in the user_common.cfg file.

The following table summarizes the combinations of provisioning server access and type of user validation supported (for Mitel 600 DECT phones):

Provisioning Server access	Requested files	User validation
User data import URL User data import credentials No certificate validation	<number | SIP user name>.cfg <loginID>.cfg	OMM authenticates user against PIN from .cfg files
User data import URL User data import credentials System Provisioning Certificate validation	<number | SIP user name>.cfg <loginID>.cfg	OMM authenticates user against PIN from .cfg files

System Provisioning URL System Provisioning credentials System Provisioning Certificate validation	<number | SIP user name>.cfg <loginID>.cfg	OMM authenticates user against PIN from .cfg files
User data import URL User credentials (UDS_CommonUserFIleName=YES) No certificate validation	user.cfg	Provisioning server authenticates user at file request with user credentials
User data import URL User credentials (UDS_CommonUserFIleName=YES) System Provisioning Certificate validation	user.cfg	Provisioning server authenticates user at file request with user credentials
System provisioning URL User credentials (UDS_CommonUserFIleName=YES) System Provisioning Certificate validation	user.cfg	Provisioning server authenticates user at file request with user credentials

18.1.2 USER CONFIGURATION

[1] Footnote for OMM configuration files below:
With user configuration files for user administration, it is necessary to use unique user identifiers (*uid*'s). New users in the SIP-DECT system must be created with AXI requests (*CreatePPUser*) and changes to existing users must be made through AXI requests (*SetPPUser*). This cannot be handled by the provisioning server. Therefore, the *CreatePPUser* AXI request can also handle change requests by using a unique user identifier for each user. This is identified with the element *replaceData="1"* in each request. When sending encrypted data (e. g. passwords), the elements can optionally be sent decrypted by using the *plainText="1"* element.

Please note: Two user provisioning concepts are supported: user configuration files and user configuration via AXI (in the ipdect.cfg file). Combining these concepts in user provisioning is not recommended.

Parameter / Parameter group	**Number or SIP user name**
Description	Indicates the users SIP call number or SIP user name used at the DECT phone.
Format	String
Range	32 characters
Default value	n.a.

Web	Basic: SIP User/Devices > New User > Number/SIP user name or SIP User/Devices > > Number/SIP user name
OMM configuration files[1]	<CreatePPUser plainText="1" replaceData="1"> <user uid="3" num="5002" /> </CreatePPUser>
DECT Phone	Administration > SipUsers/devices > New SIP user > Number
User configuration files	UD_Number=5002 When the *DECT phone user login type* is set to *number*, this value is ignored because the user enters the number during login and the number represents the user filename *5002.cfg* at the server (see section 9 for more information).

Parameter / Parameter group	**Display name**
Description	Indicates the user's name displayed on the DECT phone.
Format	String
Range	20 characters
Default value	n.a.
Web	Basic: SIP User/Devices > New User > Display name or SIP User/Devices > > Display name
OMM Configuration files[1]	<CreatePPUser plainText="1" replaceData="1"> <user uid="3" name="User-1" /> </CreatePPUser>
DECT Phone	Administration > SipUsers/devices > New SIP user > Display name
User configuration files	UD_Name=User-1

Parameter / Parameter group	**PIN**
Description	PIN used for user authentication during login procedure on the DECT phone.
Format	String
Range	8 Characters
Default value	n.a.
Web	Basic: SIP User/Devices > New User > PIN or SIP User/Devices > > PIN
OMM Configuration files[1]	<CreatePPUser plainText="1" replaceData="1"> <user uid="3" pin="5002" /> </CreatePPUser>
DECT Phone	Administration > SipUsers/devices > New SIP user > PIN
User configuration files	UD_Pin=5002

Parameter / Parameter group	**Login identification**
Description	ID used for user authentication during login procedure on the DECT phone.
Format	Integer

Range	32 numbers
Default value	n.a.
Web	Basic: SIP User/Devices > New User > Login ID or SIP User/Devices > > Login ID
OMM Configuration files[1]	<CreatePPUser plainText="1" replaceData="1"> <user uid="3" addId="3" /> </CreatePPUser>
DECT Phone	n.a.
User configuration files	n. a. When the *DECT phone user login type* is set to *Login ID*, this value is ignored because the user enters the login ID during login and the input represents the user filename *3.cfg* at the server (see section 9 for more information on this setting).

Parameter / Parameter group	**SOS number or SOS SIP name**
Description	Emergency number to be dialed when the SOS key is pressed.
Format	String
Range	32 characters
Default value	n.a.
Web	Basic: SIP User/Devices > New User > SOS number or SIP User/Devices > > SOS number
OMM Configuration files[1]	<CreatePPUser plainText="1" replaceData="1"> <user uid="3" sosNum="0815" /> </CreatePPUser>
DECT Phone	n.a.
User configuration files	UD_SosNum=0815

Parameter / Parameter group	**Man down number or Man down SIP name**
Description	Emergency number to be dialed when a sensor alarm (Mitel 600 DECT phone) has been initiated.
Format	String
Range	32 characters
Default value	n.a.
Web	Basic: SIP User/Devices > New User > ManDown number or SIP User/Devices > > ManDown number
OMM Configuration files[1]	<CreatePPUser plainText="1" replaceData="1"> <user uid="3" manDownNum="0816" /> </CreatePPUser>
DECT Phone	n.a.
User configuration files	UD_ManDownNumber=0816

Parameter / Parameter group	**Voice mail number or voice mail SIP name**
Description	Voice mail number (dialed by a long press of '1' key on the Mitel 600 DECT phone).
Format	String
Range	32 characters
Default value	n.a.
Web	Basic: SIP User/Devices > New User > SOS number or SIP User/Devices > > SOS number
OMM Configuration files[1]	<CreatePPUser plainText="1" replaceData="1"> <user uid="3" voiceboxNum="5002" /> </CreatePPUser>
DECT Phone	n.a.
User configuration files	UD_VoiceMailNumber=5002

Parameter / Parameter group	**Hot desking supported**
Description	Enables or disables the user's capability for Hot Desking. This parameter is only avaialbe for users with a dynamic association to a DECT phone (i.e., not fixed). When enabled, the user is registered as a Hot Desking user on the call server. Only supported for SIP-DECT systems using the MiVoice Business platform.
Format	Boolean
Range	True, false
Default value	False
Web	Basic: SIP User/Devices > New User > Hot desking supported or SIP User/Devices > > Hot desking supported
OMM Configuration files[1]	<CreatePPUser plainText="1" replaceData="1"> <user uid="3" num="5002" relType="Unbound" hotDeskingSupport="1" /> </CreatePPUser>
DECT Phone	n.a.
User configuration files	UD_HotDesking=true

Parameter / Parameter group	**Auto logout on charging**
Description	Enables or disables an automatic user logout when the DECT phone is placed in the charger cardle (and "Silent charging" is enabled on the phone). This parameter is only available for users with a dynamic association to a DECT phone (i.e., not fixed).
Format	Boolean
Range	True, false
Default value	False
Web	Basic: SIP User/Devices > New User > Auto logout on charging or SIP User/Devices > > Auto logout on charging

OMM Configuration files[1]	<CreatePPUser plainText="1" replaceData="1"> <user uid="3" num="5002" relType="Unbound" hotDeskingSupport="1" autoLogoutOnCharge="1" /> </CreatePPUser>
DECT Phone	n.a.
User configuration files	UD_AutoLogoutOnCharge=true

Parameter / Parameter group	**Authenticate logout**
Description	This parameter is only dedicated for login/logout users with a dynamic relation to a DECT phone. When enabled the user is able to logged out only when the PIN based authentication succeed.
Format	Boolean
Range	n.a.
Default value	True
Web	Basic: SIP User/Devices
OMM Configuration files	<CreatePPUser plainText="1" replaceData="1"> <user uid="3" num="5002" relType="Unbound" hotDeskingSupport="1" authenticateLogout="1" /> </CreatePPUser>
DECT Phone	n.a.
User configuration files	UD_AuthenticateLogout=true

Parameter / Parameter group	**SIP authentication user name**
Description	User name when the SIP Call Manager requires user authentication for SIP registration.
Format	String
Range	63 characters
Default value	n.a.
Web	Basic: SIP User/Devices > New User > Authentication user name or SIP User/Devices > > Authentication user name
OMM Configuration files[1]	<CreatePPUser plainText="1" replaceData="1"> <user uid="3" sipAuthId="SIPAccount" /> </CreatePPUser>
DECT Phone	Administration > SipUsers/devices > New SIP user > SIP user name
User configuration files	UD_SipAccount=SIPAccount

Parameter / Parameter group	**SIP authentication password**
Description	Password when the SIP Call Manager requires user authentication for SIP registration.
Format	String

Range	32 characters
Default value	n.a.
Web	Basic: SIP User/Devices > New User > Password, Password confirmation or SIP User/Devices > > Password, Password confirmation
OMM Configuration files[1]	<CreatePPUser plainText="1" replaceData="1"> <user uid="3" sipPw="SIPPw" /> </CreatePPUser>
DECT Phone	Administration > SipUsers/devices > New SIP user > SIP password
User configuration files	UD_SipPassword=SIPPw

Parameter / Parameter group	**Use SIP user name**
Description	Indicates whether the XSI service user name is taken from the user's SIP data (for XSI directory support). The generated format is <sip user name>@<sip registrar domain>. If set to “Global”, the setting applies to all users in the SIP-DECT system.
Format	Enumeration
Range	Global, On, Off
Default value	Global
Web	Basic: SIP User/Devices > New User > Use SIP user name or SIP User/Devices > > Use SIP user name
OMM Configuration files[1]	<SetPPUser plainText="1" replaceData="1"> <user uid="4711" useSIPUserName="Global" /> </SetPPUser>
DECT Phone	n.a.
User configuration files	UD_UseSIPUserName=Global

Parameter / Parameter group	**Use SIP user authentication**
Description	Indicates whether the XSI service authentication name and password are taken from the user’s SIP data (for XSI directory support). The generated format of the XSI authentication name is <sip authentication name>@<sip registrar domain>. If set to “Global”, the setting applies to all users in the SIP-DECT system.
Format	Enumeration
Range	Global, On, Off
Default value	Global
Web	Basic: SIP User/Devices > New User > Use SIP user authentication or SIP User/Devices > > Use SIP user authentication
OMM Configuration files[1]	<SetPPUser plainText="1" replaceData="1"> <user uid="4711" useSIPUserAuthentication="Global" /> </SetPPUser>
DECT Phone	n.a.

User configuration files	UD_UseSIPUserAuth=Global

Parameter / Parameter group	**Service user name**
Description	The name used for all supported XSI services for the user (if not using SIP credentials).
Format	string
Range	64 characters
Default value	n.a.
Web	Basic: SIP User/Devices > New User > User name SIP User/Devices > > User name
OMM Configuration files[1]	<SetPPUser plainText="1" replaceData="1"> <user uid="4711" serviceUserName="username" /> </SetPPUser>
DECT Phone	n.a.
User configuration files	UD_ServiceUserName=username

Parameter / Parameter group	**Service authentication name**
Description	The authentication name used for all supported XSI services for the user (if not using SIP credentials).
Format	string
Range	64 characters
Default value	n.a.
Web	Basic: SIP User/Devices > New User > Authentication name SIP User/Devices > > Authentication name
OMM Configuration files[1]	<SetPPUser plainText="1" replaceData="1"> <user uid="4711" serviceAuthName="authname" /> </SetPPUser>
DECT Phone	n.a.
User configuration files	UD_ServiceAuthName=username

Parameter / Parameter group	**Service password**
Description	The password used for all supported XSI services for the user.
Format	string
Range	32 characters
Default value	n.a.
Web	Basic: SIP User/Devices > New User > Password, Password confirmation or SIP User/Devices > > Password, Password confirmation

OMM Configuration files[1]	<SetPPUser plainText="1" replaceData="1"> <user uid="4711" serviceAuthPassword="authpassword" /> </SetPPUser>
DECT Phone	n.a.
User configuration files	UD_ServiceAuthPasswd=password

Parameter / Parameter group	**Fixed local SIP port**
Description	SIP user's configured fixed client port (used for SIP registration)
Format	Integer
Range	n.a.
Default value	n.a.
Web	Current state can only be listed: Basic: SIP User/Devices >
OMM Configuration files[1]	<CreatePPUser plainText="1" replaceData="1"> <user uid="3" fixedSipPort="4711" /> </CreatePPUser>
DECT Phone	n.a.
User configuration files	UD_FixedSIPPort=4711

Parameter / Parameter group	**Description 1**
Description	Additional text (part 1) description for a user (e.g., department or function).
Format	String
Range	16 characters
Default value	n.a.
Web	Current state can only be listed: Basic: SIP User/Devices >
OMM Configuration files[1]	<CreatePPUser plainText="1" replaceData="1"> <user uid="3" hierarchy1="Department" /> </CreatePPUser>
DECT Phone	n.a.
User configuration files	UD_HierarchyName1=Department

Parameter / Parameter group	**Description 2**
Description	Additional text (part 2) description for a user (e.g., department or function).
Format	String
Range	16 characters
Default value	n.a.
Web	Current state can only be listed:

	Basic: SIP User/Devices >
OMM Configuration files[1]	<CreatePPUser plainText="1" replaceData="1"> <user uid="3" hierarchy2="Room-44" /> </CreatePPUser>
DECT Phone	n.a.
User configuration files	UD_HierarchyName2=Room-44

Parameter / Parameter group	**External User**
Description	User data provided by an external provisioning server (<user>.cfg). True/1/Yes = user data imported from a server False/0/No = user data only stored internally in the OMM database
Format	Boolean
Range	n.a.
Default value	n.a.
Web	Current state can only be listed: Basic: SIP User/Devices >
OMM configuration files[1]	n.a.
DECT Phone	n.a.
User configuration files	n.a.

Parameter / Parameter group	**Send message permission**
Description	User's permissions to send text messages using the Mitel 600 DECT phone. True/1/Yes = user is authorized to send text messages False/0/No = user is not authorized to send text messages
Format	Boolean
Range	n.a.
Default value	True
Web	Current state can only be listed: Basic: SIP User/Devices >
OMM configuration files[1]	<CreatePPUser plainText="1" replaceData="1"> <user uid="3" msgRight="1" /> </CreatePPUser>
DECT Phone	Current state can only be listed: Basic: SIP User/Devices >
User configuration files	UD_AllowMsgSend=True

Parameter / Parameter group	**Send vCard permission**
Description	User's permissions to send visiting/business cards using the Mitel 600 DECT phone.

	True/1/Yes = user is authorized to send vCards False/0/No = user is not authorized to vCards
Format	Boolean
Range	n.a.
Default value	True
Web	Current state can only be listed: Basic: SIP User/Devices >
OMM configuration files[1]	<CreatePPUser plainText="1" replaceData="1"> <user uid="3" sendVcardRight="1" /> </CreatePPUser>
DECT Phone	n.a.
User configuration files	UD_AllowVcardSend=True

Parameter / Parameter group	**Receive vCard permission**
Description	Indicates whether the user accepts received vCards. True/1/Yes = incoming vCards are accepted False/0/No = incoming vCards are not accepted
Format	Boolean
Range	n.a.
Default value	n.a.
Web	Current state can only be listed: Basic: SIP User/Devices >
OMM configuration files[1]	<CreatePPUser plainText="1" replaceData="1"> <user uid="3" recvVcardRight="1" /> </CreatePPUser>
DECT Phone	n.a.
User configuration files	UD_AllowVcardRecv=True

Parameter / Parameter group	**User specific conference server type**
Description	User-specific setting of the conference service to be used for three/n-way conferencing. None = three-way conferencing is disabled Global = OMM system setting is used (default) Integrated = integrated conference server is used
Format	String
Range	n. a.
Default value	None / Off
Web	Current state can only be listed: Basic: SIP User/Devices >

OMM configuration files[1]	<CreatePPUser plainText="1" replaceData="1"> <user uid="3 conferenceServerType="Global" | "External" | "None" /> </CreatePPUser>
DECT Phone	n. a.
User configuration files	UD_ConferenceServerType=Off/Global/External/Integrated

Parameter / Parameter group	**User specific conference URI**
Description	URI for the external conference server
Format	String
Range	n. a.
Default value	n. a.
Web	Current state can only be listed: Basic: SIP User/Devices >
OMM configuration files[1]	<CreatePPUser plainText="1" replaceData="1"> <user uid="3" conferenceServerURI="conference.provider.com" /> </CreatePPUser>
DECT Phone	n. a.
User configuration files	UD_ConferenceServerURI=conference.provider.com

Parameter / Parameter group	**CoA profile identification**
Description	ID of the CoA (Central DECT phone configuration Over Air) profile to use. If the value of ID is 0, no data are to be loaded for this user. **Note:** When a COA profile is deleted, its profile ID assignment to DECT phone users remains. If a new CoA profile is created and acquires this profile ID (the IDs are assigned in sequential order), any DECT phone users with the old profile ID are automatically assigned to the new CoA profile.
Format	Integer
Range	0 .. 20
Default value	0
Web	Current state can only be listed: Basic: SIP User/Devices >
OMM configuration files[1]	<CreatePPUser plainText="1" replaceData="1"> <user uid="3" ppProfileId="11" /> </CreatePPUser>
DECT Phone	n.a.
User configuration files	UD_PpProfileId=11

Parameter / Parameter group	**CoA configuration data**

Description	Configuration data to be downloaded to the DECT phone for this user. Maximum size is 4 kByte.
Format	String
Range	n.a.
Default value	n.a.
Web	n.a.
OMM configuration files[1]	n.a.
DECT Phone	n.a.

User configuration files	List of CoA configuration data to be set (see section **Error! Reference source not found.** for available settings), e. g.:
	# display-settings
	UD_DispLanguage=en
	UD_DispFont=large
	UD_DispColor=black
	# ringer-settings
	UD_RingerVolumeIntern=level-1

Parameter / Parameter group	**Auto answer**
Description	Auto-answer setting for incoming calls. One of “On”, “Off” or “Global”. For more information, see also incoming call settings for SIP.
Format	String
Range	On | Off | Global
Default value	Off
Web	Current state can only be listed: Basic: SIP User/Devices >
OMM configuration files[1]	<CreatePPUser plainText="1" replaceData="1"> <user uid="3" autoAnswer=“Global”/> </CreatePPUser>
DECT Phone	n.a.
User configuration files	UD_AutoAnswer=Global

Parameter / Parameter group	**Microphone mute**
Description	Microphone mute setting for incoming calls. One of “On”, “Off” or “Global”. For more information, see also incoming call settings for SIP.
Format	String
Range	On | Off | Global
Default value	Off
Web	Current state can only be listed: Basic: SIP User/Devices >

OMM configuration files[1]	<CreatePPUser plainText="1" replaceData="1"> <user uid="3" microphoneMute="Off"/> </CreatePPUser>
DECT Phone	n.a.
User configuration files	UD_MicrophoneMute=Off

Parameter / Parameter group	**Warning tone**
Description	Warning tone setting for incoming calls. One of “On”, “Off” or “Global”. For more information, see also incoming call settings for SIP.
Format	String
Range	On | Off | Global
Default value	Off
Web	Current state can only be listed: Basic: SIP User/Devices >
OMM configuration files[1]	<CreatePPUser plainText="1" replaceData="1"> <user uid="3" warningTone="On"/> </CreatePPUser>
DECT Phone	n.a.
User configuration files	UD_WarningTone= On

Parameter / Parameter group	**Allow barge in**
Description	Allow barge in setting for incoming calls. One of “On”, “Off” or “Global”. For more information, see also incoming call settings for SIP.
Web	Current state can only be listed: Basic: SIP User/Devices >
OMM configuration files[1]	<CreatePPUser plainText="1" replaceData="1"> <user uid="3" allowBargeIn="On" | "Off" | "Global"/> </CreatePPUser>
DECT Phone	n.a.
User configuration files	UD_AllowBargeIn= On | Off | Global

Parameter / Parameter group	**User Configuration File Update Interval**
Description	Interval, in hours, to re-import the *<user>.cfg* configuration file from the user data or provisioning server.
Format	n.a.
Range	n.a.
Default value	24 / hours, when not set in the user_common.cfg and not set in <user>.cfg file
Web	n.a.
OMM configuration files[1]	n.a.
DECT Phone	n.a.

User configuration files	UD_UpdateInterval=2 Can be set in *user_common.cfg* and /or *<user>.cfg* configuration file. When set in both files, the user file setting takes precedence.

Parameter / Parameter group	**Call waiting disable**
Description	An incoming call is signaled in-band if the user is otherwise engaged (Call waiting). This feature can be disabled. True/1/Yes = call waiting is disabled False/0/No = call waiting feature is active
Format	n.a.
Range	n.a.
Default value	n.a.
Web	Current state can only be listed: Basic: SIP User/Devices >
OMM configuration files[1]	n.a.
DECT Phone	Soft key or directly available by a long press of the soft key > Call waiting > Off | On
User configuration files	n.a.

Parameter / Parameter group	**Forward mode**
Description	Mode of Call diversion or Call forwarding (Off, Immediately, Busy, No answer, Busy & no answer).
Format	n.a.
Range	n.a.
Default value	n.a.
Web	Current state can only be listed: Basic: SIP User/Devices >
OMM configuration files[1]	n.a.
DECT Phone	Menu key > Call diversion > Off | Immediately | Busy | No answer | Busy no answer
User configuration files	n.a.

Parameter / Parameter group	**Forward time**
Description	Time delay, in seconds, before the incoming call is redirected.
Format	n.a.
Range	n.a.
Default value	n.a.
Web	Current state can only be listed:

	Basic: SIP User/Devices >
OMM configuration files[1]	n.a.
DECT Phone	Menu key > x [sec]
User configuration files	n.a.

Parameter / Parameter group	**Forward destination**
Description	Destination of the redirected call.
Format	n.a.
Range	n.a.
Default value	n.a.
Web	Current state can only be listed: Basic: SIP User/Devices >
OMM configuration files[1]	n.a.
DECT Phone	Menu key > No ()
User configuration files	n.a.

Parameter / Parameter group	**Hold ring back time**
Description	Time, in minutes, after which the user wants to be reminded of the connection on hold. 0 = Off, no reminder
Format	n.a.
Range	n.a.
Default value	n.a.
Web	Current state can only be listed: Basic: SIP User/Devices >
OMM configuration files[1]	n.a.
DECT Phone	Soft key or directly available by a long press of the soft key > Hold ringback > x [min]
User configuration files	n.a.

Parameter / Parameter group	**Key lock: Active**
Description	Enable key lock management: Set "1" or "true", if the key lock management of the DECT phone user shall be enabled. The user can activate the automatic key lock, if the key LockTime is unequal to 0. The manual key lock ( ) is activated then too. Set "0" or "false", if the key lock management of the DECT phone user is disabled. Any key lock is disabled on the users DECT phone. Default value is "true".

Format	Bool
Range	True/False
Default value	True
Web	Advanced: Dect Phones
OMP/AXI	DECT Phones -> Users -> Key lock

OMM Configuration files	AXI commands:
	`<SetPPUser> <user uid="8" keyLockEnable="1"/> </SetPPUser>`
	`# keyLockEnable="1","true" # keylock management enabled`
	`# keyLockEnable="0","false"# keylock management disabled`
	<user>.cfg files:
	`UD_KeyLockEnable=1`

DECT Phone	n.a.

Parameter / Parameter group	**Key lock: Time**
Description	Set key lock time: If **keyLockEnable** is “true”, the key lock can be activated by setting the key lock time for the DECT phone user. The valid activation values are 10, 20, 30, 60, 90 or 120 seconds. The deactivation value is 0. Default setting is 0 seconds.
Format	Enumerated
Range	0 (None, Off), 10, 20, 30, 60, 90 or 120 seconds.
Default value	0 (None, Off).
Web	Advanced: Dect Phones
OMP/AXI	DECT Phones -> Users -> Key lock

OMM Configuration files	AXI commands:
	`<SetPPUser> <user uid="8" keyLockTime="60"/> </SetPPUser>`
	`# keyLockTime={"0","10","20","30","60","90","120"}`
	<user>.cfg files:
	`UD_KeyLockTime=60`

DECT Phone	Only applicable if “key lock active=true”: (long pressed “>>>” key) -> Administration->Key lock->Key lock.

Parameter / Parameter group	**Key lock: PIN**
Description	Set key lock PIN: Key-Lock-PIN number to unlock the DECT phone. This is encrypted with the public key. Default value is “0000”.
Format	Exactly 4 digits.
Range	Exactly 4 digits.

Default value	“0000”.
Web	Advanced: Dect Phones
OMP/AXI	DECT Phones -> Users -> Key lock

OMM Configuration files	AXI commands:
	`<SetPPUser plainText="1">`
	`<user uid="8" keyLockPin="4711" />`
	`</SetPPUser >`
	`# Please note: the tag plainText="1" is mandatory for PIN`
	`# settings by AXI configuration files`
	<user>.cfg files:
	`UD_KeyLockPin=4711`

DECT Phone	(long pressed “>>>” key) -> Administration->Key lock->Enter new PIN.

18.2 DEVICES

18.2.1 CREATE / DELETE DEVICES

18.2.1.1 Creating a device

DECT phone devices are subscribed automatically, if being subscribed for the first time.

18.2.1.2 Deleting a device

Devices can be deleted:

- through the OMM Web service
- through the DECT phone **Administration** menu
- indirectly by the DECT phone itself, if the subscription is deleted

Parameter / Parameter group	**Delete device**
Description	Delete a DECT phone device
Format	n.a.
Range	n.a.
Default value	n.a.
Web	Basic: SIP User/Devices > <selected device> >
OMM configuration files[1]	n.a.
DECT Phone	Administration > SipUsers/devices > Devices > <selected device> > Delete
User configuration files	n.a.

Please note: If the device is associated with a SIP user who is logged in, the user is not deleted. The user remains, but the relationship is eliminated.

18.2.2 SUBSCRIBE DEVICES

18.2.2.1 Enable / Disable subscription permission

For DECT phone subscription, the base station must be switched to a special operation mode. The subscription mode is active for 60 minutes after powering on the base station and for 24 hours after the subscription mode has been explicitly activated.

Administrators can disable subscription manually to prevent unauthorized subscriptions.

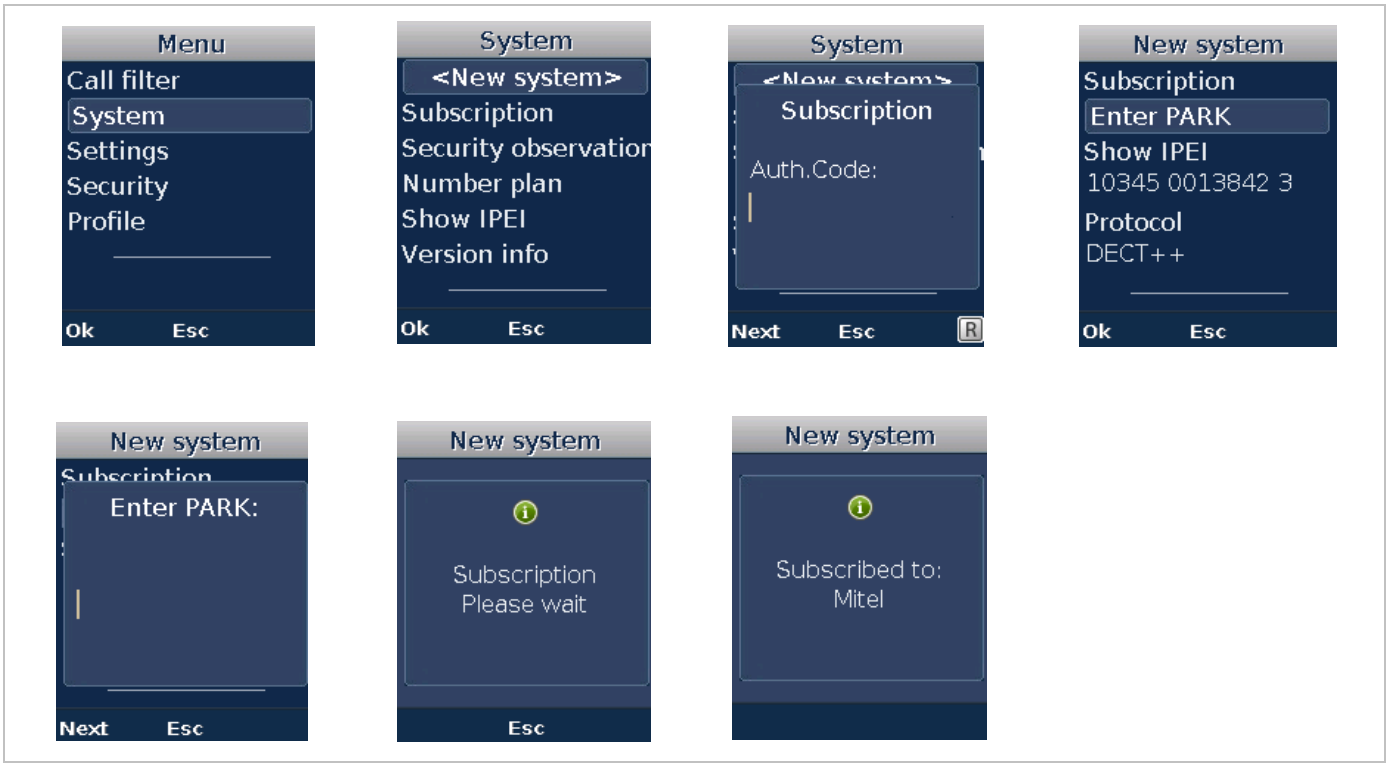
Parameter / Parameter group	**Enable subscription permission**
Description	Enables the general permission to subscribe DECT phones
Format	Boolean

Range	n.a.
Default value	n.a.
Web	Basic: SIP User/Devices > Subscription allowed
OMM configuration files[1]	<SetDECTSubscriptionMode mode="Configured" />
DECT Phone	Administration > SipUsers/devices > Subscription allowed
User configuration files	n.a.

Parameter / Parameter group	**Disable subscription permission**
Description	Disables the general permission to subscribe DECT phones
Format	Boolean
Range	n.a.
Default value	n.a.
Web	Basic: SIP User/Devices > Subscription allowed
OMM configuration files[1]	<SetDECTSubscriptionMode mode="Off" />
DECT Phone	Administration > SipUsers/devices > Subscription allowed
User configuration files	n.a.

18.2.2.2 Subscribe DECT phone devices

1. On the DECT phone, briefly press the menu softkey (») to open the system menu. Navigate to the **System** > **New system** and click **Ok** to confirm.
2. Enter the authentication code in the **Auth. Code** field when prompted (for factory default configuration, enter “22222”).
3. Confirm with **Ok**.
4. An **Info** box is displayed with the message **Subscription - Please wait**. The subscription should finish shortly after this with a success message. You can abort the subscription at any time by pressing the **Esc** softkey.



Please note: As an optional step, you can enter the PARK code of the DECT system to ensure that the DECT phone subscribes to the correct DECT system. The PARK is a globally unique decimal number that you find on the Status page of the OMM web service. After entering the Auth. Code, select the Enter PARK menu entry before proceeding with the subscription (note that you must enter the PARK value in decimal format, not hex format).

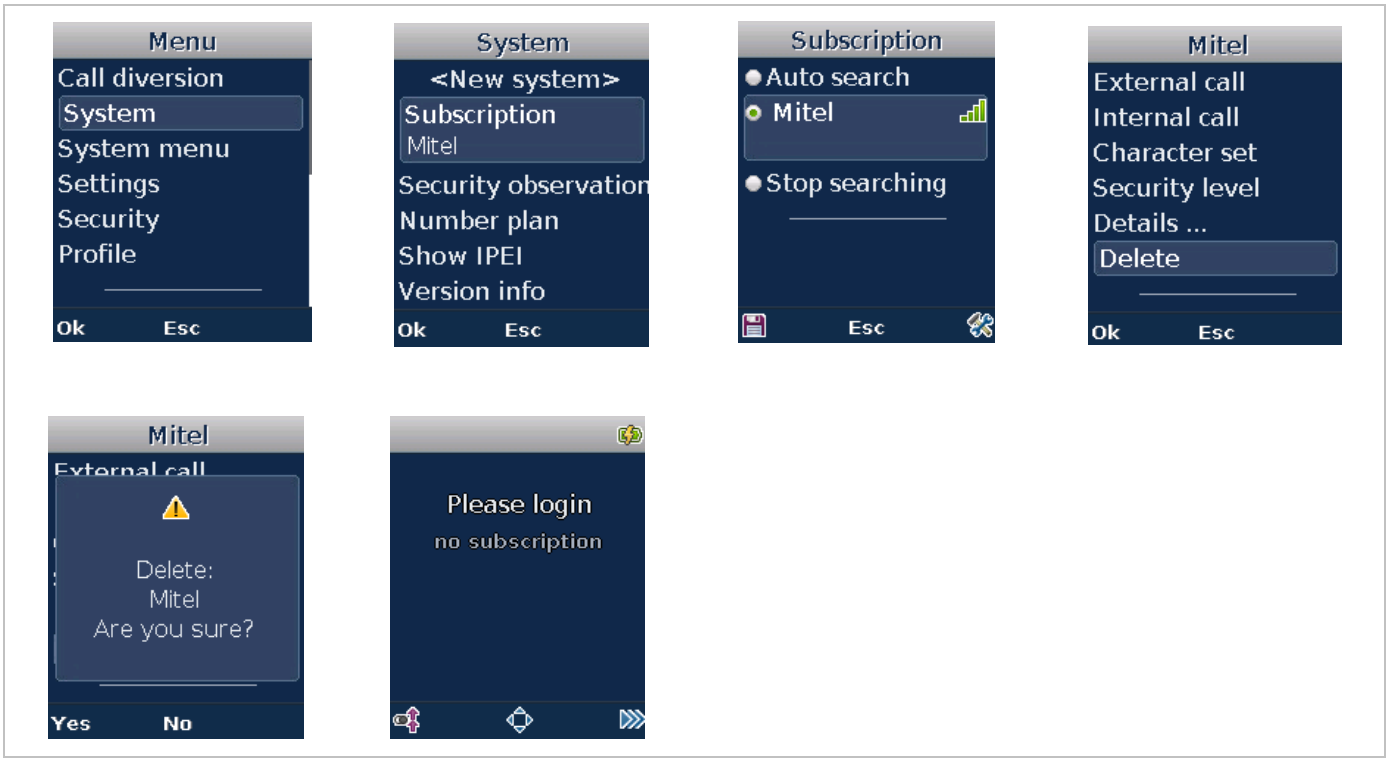
Security does not rely on subscription alone. You cannot perform any critical functions without logging in – either with a SIP user account / PIN combination for telephony or by entering the user name / password combination that is valid for the OMM web service for changing the system configuration.

Please note: Software downloads and Configuration over Air are only provided from the first DECT system subscribed to. You can configure the "Master download system" from the DECT phone user interface (using the menu * 6 # option).

18.2.3 UNSUBSCRIBE DEVICES

You can unsubscribe a device. When you unsubscribe a device, the device is deleted.

1. On the DECT phone, briefly press the softkey to bring up the system **Menu**. Navigate to the **System** > **Subscription** menu entry. Confirm with **Ok**.
2. Select the system for which you want to delete the subscription and press the Settings ( ) softkey.
3. Select **Delete** and press **Ok**.
4. When prompted to confirm, confirm with **Ok**. If you want to cancel the operation, press **Esc**.



18.3 USER LOGIN / LOGOUT

To make calls, a SIP user must be logged in to a DECT phone device. SIP users are allowed to use other devices, but only one device at a time.

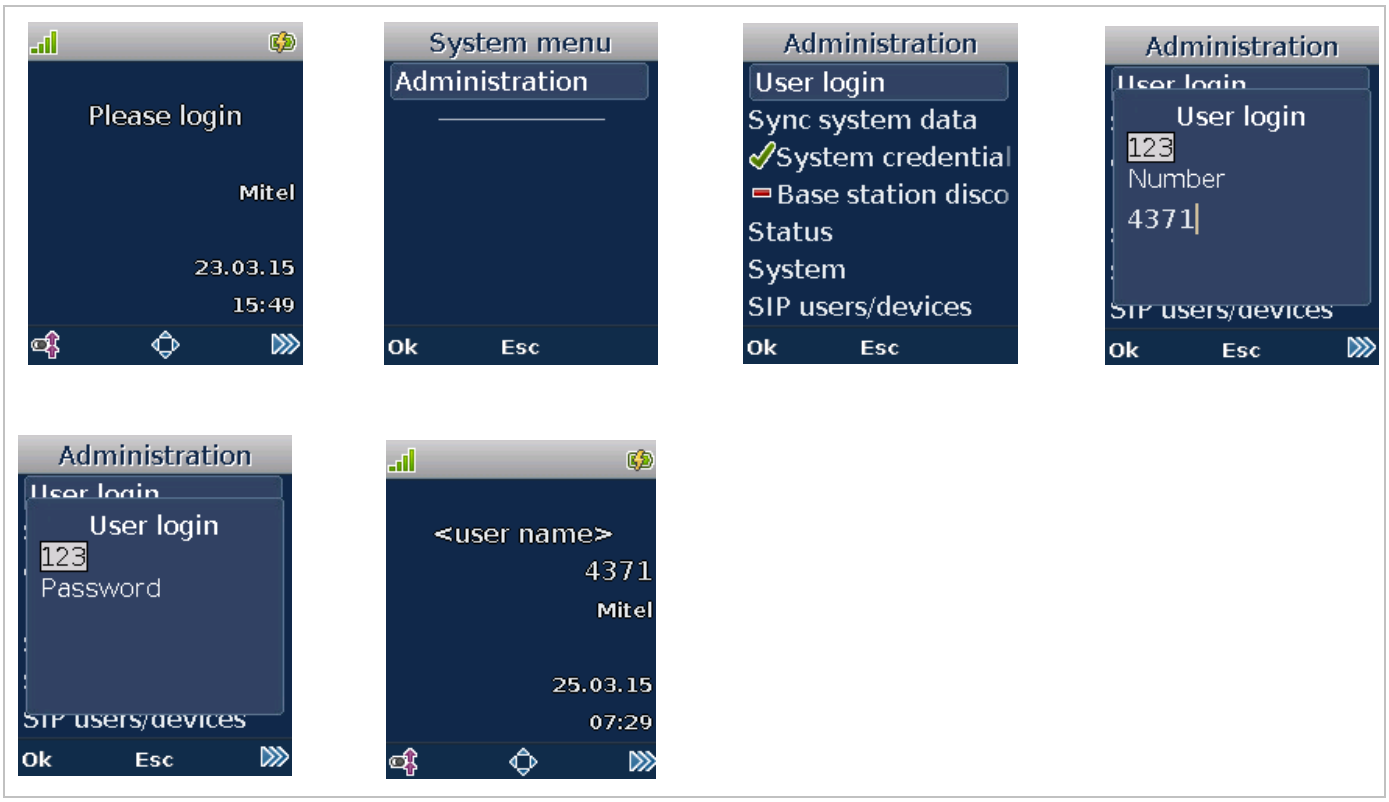
> **Please note:** It is not possible to login with the same SIP user account on different DECT phones concurrently. If the login sequence for a SIP user account is performed on another DECT phone, that user is logged out automatically from the the DECT phone that he was previously logged into.

18.3.1 LOGIN PROCEDURE

Users must execute a login sequence to use any telephony services with the DECT phone. The user must dial the phone number / user ID and PIN code of a SIP user account.

1. Press and hold the softkey » to bring up the **System menu**. The **Administration** menu entry is displayed. Confirm with **Ok**.
2. Select the **User login** menu entry and confirm with **Ok**. An input field is displayed, prompting you to enter a **Number** or a **User ID**.
3. Enter the phone number / user ID of the SIP user account and confirm with **Ok**. An input field is displayed, prompting you to enter a **PIN**.
4. Enter the PIN code that is configured for the SIP user account. Confirm with **Ok**.

> **IMPORTANT : If there is no specific PIN configured then “0000” is automatically set.**

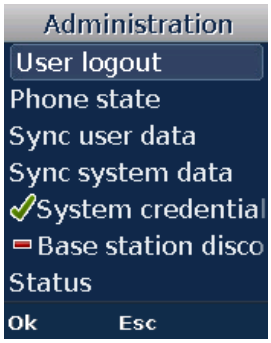


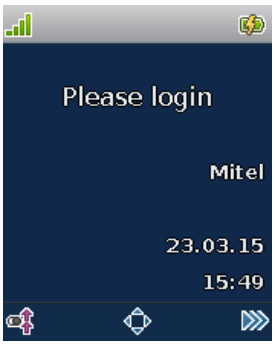
The DECT phone's standard screen displays the user's name as well as the phone number that is configured with the SIP user account. The DECT phone is ready to be used for telephony functions.

18.3.2 LOGOUT PROCEDURE

If the DECT phone is logged in, it is possible to log out via the the **System menu** >**Administration** > **User logout** menu entry.

1. Press and hold the softkey to bring up the **System menu**.
2. Navigate to the **Administration** menu entry and confirm with **Ok**.
3. Select the **User logout** menu entry and confirm with **Ok**.
   An input field is displayed, prompting you to enter a **PIN**.
4. Enter the PIN code that is configured for the currently used SIP user account. Confirm with **Ok**.





18.4 WIRELESS LAN (WLAN)

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

The RFP48 WLAN adds 802.11a/b/g/n access point functionality in addition to DECT functionality.

All RFP48 WLAN base stations are managed by the OpenMobility Manger.

The following steps must be completed manually to enable WLAN functionality:

- Configure WLAN regulatory domain
- Configure at least one profile specifying SSID, 802.11 mode and security configuration
- Assign a profile to a base station and select the channel number and channel bandwidth

18.4.1 802.11I: 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.

18.4.2 CREATING AND CHANGING WLAN PROFILES

You need at least one active WLAN profile in order to operate the WLAN function for an RFP 42/43/48 WLAN device.

1. Navigate to the **WLAN profiles** page. This page shows the number of existing WLAN profiles and a list of available WLAN profiles.
2. If you create a new WLAN profile, configure the RFP type first to get the correct input fields. Select the appropriate profile (**RFP 42, RFP 43** or **RFP 48**) from the **WLAN profile type** selection list.
3. To add a new WLAN profile, press the **New** button. To change an existing WLAN profile, click on the icon available on the left of the WLAN profile entry.

   The **New WLAN profile** page resp. the **WLAN profile [Number]** page shows the WLAN profile configuration.
4. Change the desired settings of the WLAN profile. You need at last to define the ESSID setting. The different settings are explained in detail in the sections below.
5. Activate the **Profile active** setting; otherwise the WLAN profile is inactive which de-activates the WLAN function for base stations that are assigned to this WLAN profile.
6. Press the **OK** button to apply the settings. If you created a new WLAN profile, you can proceed by assigning the WLAN profile to the desired base stations (see section 5.6.3). If you changed an existing WLAN profile, the settings are applied to the assigned base stations automatically.

1. **802.11 mode** (RFP 42 WLAN selection list: Mixed / 802.11b only / 802.11g only, default: Mixed): Both the older and long-ranged B-Mode and the newer and faster G-Mode are typically supported by WLAN clients. You can change this setting to prevent problems with very old WLAN clients.
   (RFP 43/48 WLAN selection list: 802.11bg /802.11b only / 802.11g only / 802.11abg /802.11n, default: 802.11bg): On the **RFP 43/ RFP 48** profile you can choose additionally 802.11 modes 802.11abg, 802.11n and the mode 802.11ac is only available for RFP 48 WLAN.
2. Select the desired mode in 802.11 mode. Available modes are 802.11n, 802.11abg, 802.11ag, 802.11b only and 802.11g only.

18.4.3 WLAN CONFIGURATION STEPS (RFP 48 WLAN)

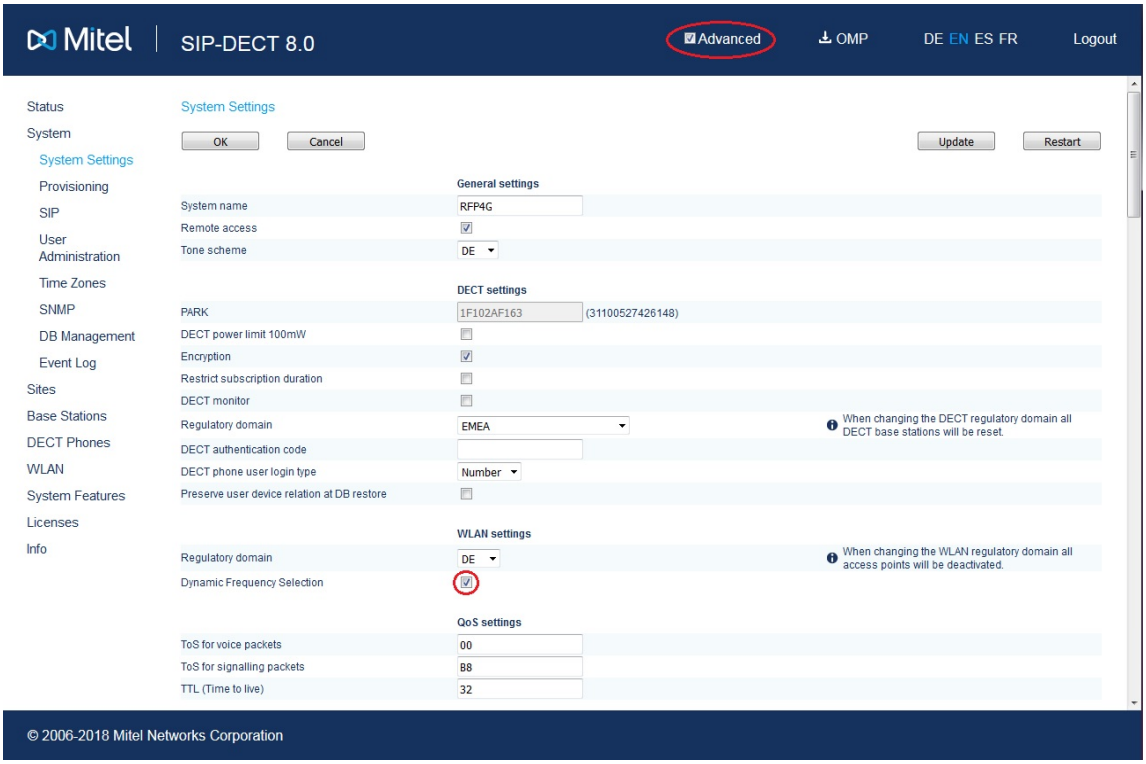
Support of 802.11ac WLAN

802.11ac is backward compatible with 802.11a and ‘n’. Like the RFP 43, the RFP 48 can only work in one WLAN spectrum at the same time (2.4 GHz or 5 GHz). Within the 2.4 GHz spectrum, the WLAN module supports the 802.11b/g/n modes in the same way as the RFP 43. The third antenna of the RFP 48 increases the data throughput in n mode from 300Mbit/s to 450 Mbps.

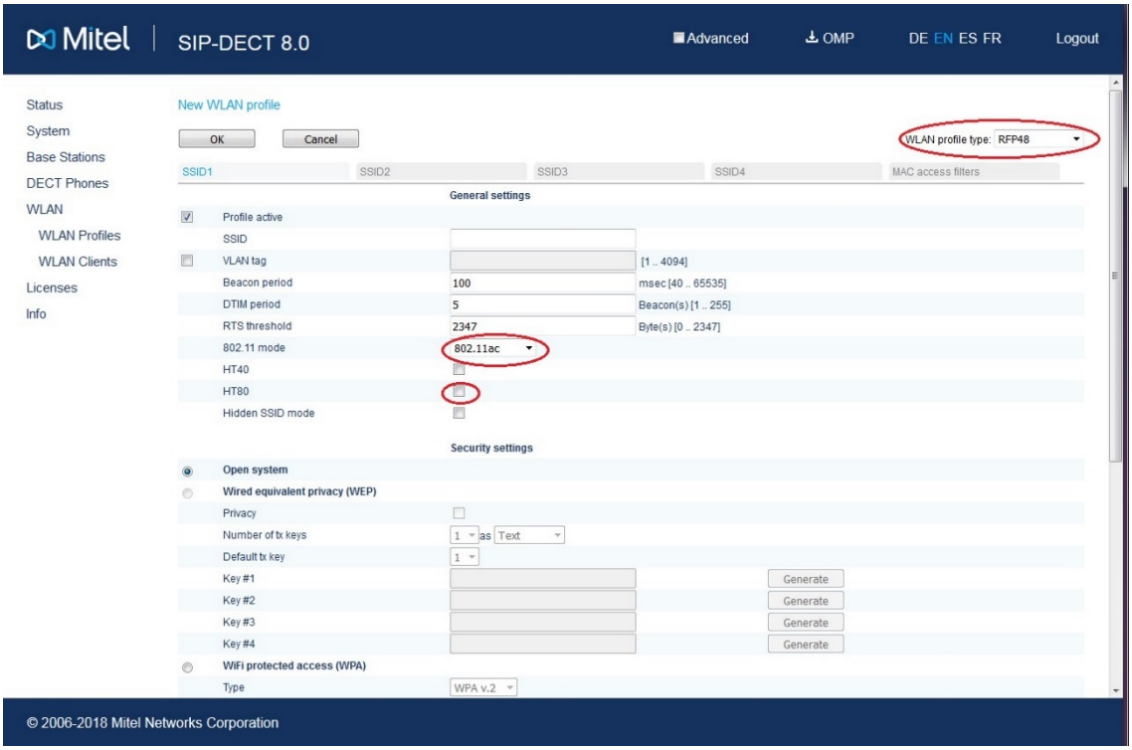
In ac mode, HT80 channel bandwidth and 256-QAM modulation increase the data throughout up to 1300 Mbps.

To enable the DFS channels,

- Go to **System>System Settings** (Advanced).
- Select the **Dynamic Frequency Selection** (DFS)

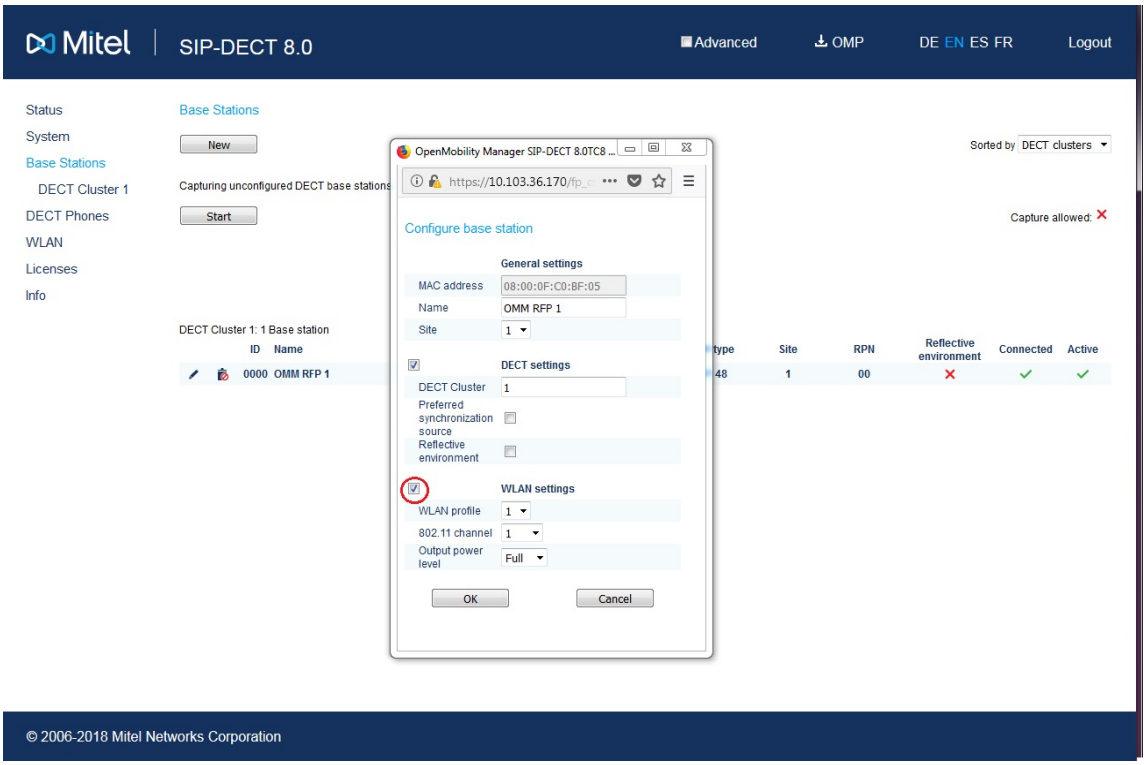


- to enable the ac mode and HT80: WLAN\WLAN Profiles (new/edit).



HT80 includes the HT40/HT20 bandwidth setting. A channel with a bandwidth of 80 MHz occupies 4 WLAN channels with a bandwidth of 20 MHz.

- to activate WLAN and to set the WLAN profile / channel / power level for a base station (edit):



The selected WLAN channels have a default bandwidth of 20 MHz. If the WLAN profile options like HT80/ HT40 MHz is activated, the necessary center channel is automatically selected in the corresponding areas during the configuration itself.

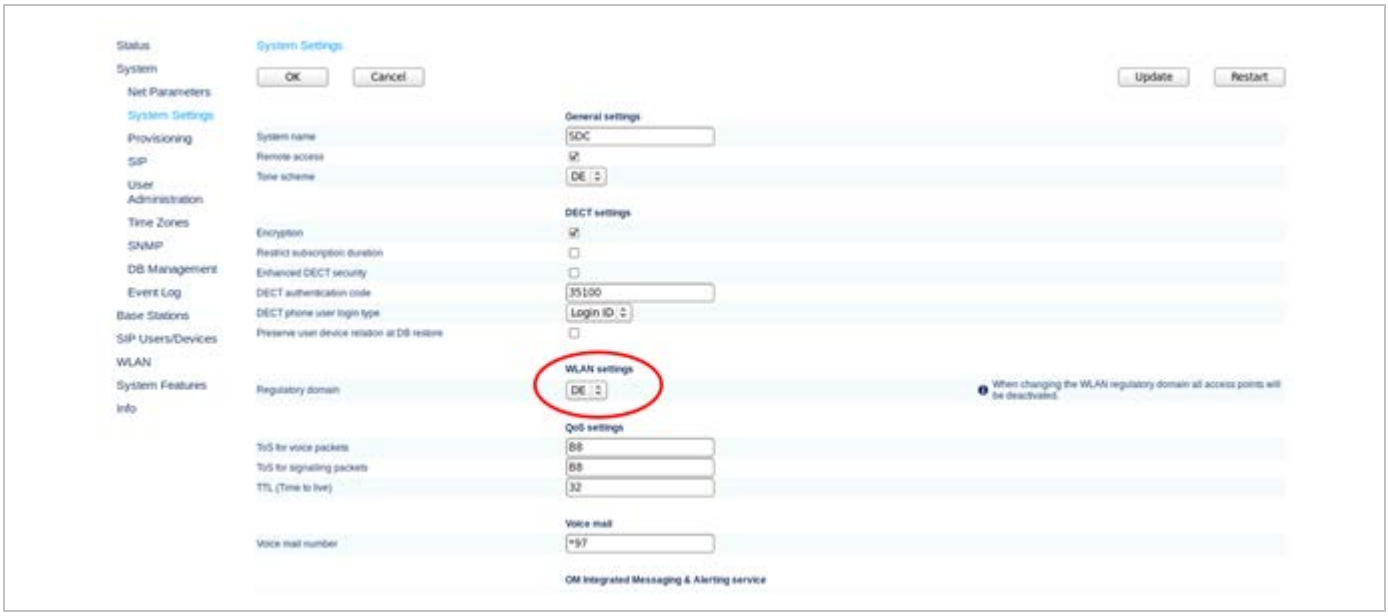
In the 2.4 GHz band, a channel with 40 MHz bandwidth is only established if no other 20 MHz channel is disturbed. Otherwise, a fallback to 20 MHz bandwidth is made.

WLAN is a shared media. Depending on the application, it is useful to have 4 RFPs with a bandwidth of 20 MHz (for canteen room) or to have one RFP with a bandwidth with 80 MHz (for video conference room).

18.5 WLAN REGULATORY DOMAIN

The value specified in the **Regulatory domain** field specifies 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.

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



18.6 WLAN PROFILES

You need at least one active WLAN profile to operate the WLAN function on an RFP 43 WLAN base station. Up to 20 WLAN profiles are supported.

WLAN profile configuration is only available through the OMP.

1. Navigate to the **WLAN** / **WLAN Profiles** page. This page shows the number of existing WLAN profiles and a list of available WLAN profiles.
2. To add a new WLAN profile, press the **New** button. To change an existing WLAN profile, click on the icon to the left of the WLAN profile entry.
3. The **New WLAN profile** page or the **WLAN profile** [Number] page shows the profile configuration.
4. Change the desired settings of the WLAN profile. You need to define at least one SSID. The different settings are explained in detail in the sections below.
5. Activate the **Profile active** setting; otherwise the WLAN profile is inactive, which de-activates the WLAN function for base stations that are assigned to this WLAN profile.
6. Press the **OK** button to apply the settings. If you created a new WLAN profile, you can proceed by assigning the WLAN profile to the desired base stations (see section 7.6.3). If you changed an existing WLAN profile, the settings are applied to the assigned base stations automatically.

18.6.1 GENERAL SETTINGS

- **Profile active**: Activate this checkbox to activate the profile. This in turn activates the WLAN function for all base stations that are assigned to the WLAN profile.

- **SSID**: Enter a descriptive character string to identify the WLAN network (e.g. “OurCompany”). The base station broadcasts the Service Set Identifier (SSID) within “WLAN beacons” at regularl intervals. The SSID identifies the WLAN network and is visible to all WLAN clients. This is typically used with a scan function (e.g. from a WLAN client trying to establish a connection). The SSID should not exceed 32 characters and it is advisable not to use unusual characters that may trigger WLAN client software bugs.
- **VLAN tag** (number, 1..4094, default: off): You can separate VoIP and client data traffic (transferred via WLAN) by using different virtual LANs (e.g. to prevent bulk data transfers to interfere with VoIP). To use a separate VLAN for client data traffic, activate the check box and enter the desired VLAN number (see sections 9.17 and 9.12).
- **Beacon period** (1024µsec, 40..65535, default: 100): Determines the WLAN beacon interval. A higher value can save some WLAN airtime that can be used for data transfers.
- **DTIM period** (number, 1..255, default: 5): Determines the number of beacons between DTIM messages. These messages manage the WLAN wakeup/sleep function (critical for battery powered WLAN clients).
- **RTS threshold** (bytes, 0..4096, default: 2346): If a WLAN packet exceeds this threshold, it will be transferred with RTS/CTS handshake. This may improve transfer reliability if several WLANs share the same channel. The default of 2346 byte switches off this function because the IP-MTU is typically only 1500 bytes.
- **Fragmentation threshold** (bytes, 256..2346, default: 2346): If a WLAN packet exceeds this threshold, it will be transferred in chunks. This may improve transfer reliability for a weak connection. The default of 2346 bytes switches off this function because the IP-MTU is typically only 1500 byte.
- **802.11 mode**: Select the desired mode. Available modes are 802.11n, 802.11abg, 802.11ag, 802.11b only and 802.11g only.
- **Hidden SSID mode**: Check this box if you do not want the SSID to be broadcasted in beacon frames.

18.6.2 SECURITY SETTINGS

You configure the following security parameters in the this section:

- **Open system**: Enable this option to disable authentication and encryption (“Hotel mode”). Note that all data is transferred un-encrypted in this mode, which can be easily eavesdropped with any WLAN equipment.
- **Wired Equivalent Privacy (WEP)**: Enable this option to use the WEP encryption mode. This mode may be useful (e.g., if your WLAN supports older WLAN clients that do not implement the recommended WPA encryption).
  - **Privacy** (on / off, default: off): De-activate this setting to use no authentication (“Open System”) with standard WEP encryption. Activate this setting to use an additional shared key authentication between the base station and the WLAN client.
    - **Number of tx keys** (number, 1..4, default: 1): The WEP encryption can use a single shared key or multiple shared keys (“key rotation”). Select the number of shared keys, select how to enter a shared key (by default as **Text** or as **Hex value**), and select the **Cipher length** (see **Key settings** below).
    - **Default tx key** (number, 1..4, default: 1): If more than one shared keys is used, you can select the default shared key. You must configure the same default key on the WLAN client.
    - **Key #1 – Key #4**: Enter one or more shared key. The **Cipher length** setting (see **Key settings** below) determines the length of the required input. If you select to enter as **Text** (see above), input a password with 5, 13, or 29 characters that matches a 64 or 128 bit cipher. If you select to enter as **Hex value**, you can input a hexadecimal number with 10, 26,

or 58 characters (0-9, a-f). Press the **Generate** button to generate a random shared key that matches the current settings.

Please note: When using 802.11n, WEP is not supported. It is recommended that you always use the most secure encryption (e.g., WPA2).

- **WiFi protected access (WPA)**: Enable this option to use the recommended WPA encryption mode.
  - **Type** (selection, WPA any / WPA v.1 / WPA v.2, default: WPA v.2): Select the WPA version required for WLAN clients. The **WPA any** setting allows WPA v.1 and WPA v.2 to be used concurrently. The **WPA v.1** setting enforces the use of the older RC4-based encryption. The **WPA v.2** setting enforces the use of the stronger AES encryption. You can also change the distribution interval (see **Key settings** below).
  - **802.1x (Radius)**: Select this option if your WLAN should use a RADIUS server for WLAN client authentication ("Enterprise WPA" with different username/password combinations per client). You must also specify the **Radius settings** (see below). For details about the RADIUS authentication procedure, using the public keys, and importing certificates to the WLAN clients refer to the documentation of your RADIUS server product.
  - **Pre-shared key**: Select this option to use a single shared key for all WLAN clients (**Value** setting below). A WLAN client user needs to enter the shared key in order to connect.
  - **Value**: You can enter a shared key as **Text**. Use a longer text sequence with alphanumeric characters and special characters to enhance the shared key strength. A text shared key is case sensitive. Alternatively, the shared key can be entered as **Hex value** (hexadecimal number, 0-9, a-f). Press the **Generate** button to generate a random shared key that matches the current settings.
- **MAC access filter**: Activate the MAC access filter.
- **BSS isolation**: Checking this prevents bridging traffic between stations associated to the same WLAN AccessPoint.

18.6.3 KEY SETTINGS

- **Cipher length** (selection, 64 Bits / 128 Bits, default: 64 Bits): Determines the key length used for the WEP encryption. Larger bit sequences provide better security but may be unsupported by legacy WLAN clients.
- **Distribution interval** (seconds, 1..86400, default: 600): Determines how often the WPA encryption is re-negotiated.

18.6.4 RADIUS SETTINGS

The parameters in this section can only be configured if the **802.1x (Radius)** configuration is used.

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

18.6.5 QOS SETTINGS

- **WME**: (on / off): You can enable the Wireless Multimedia Extensions to prioritize WLAN traffic. The WLAN traffic priority is determined by **VLAN** number or by examining the **DiffServ** data field of IP packets. WME is mandatory for 802.11n and therefore auomatically enabled.

18.6.6 ADDITIONAL SSID

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

1. Switch to the appropriate **SSID** tab (e.g. SSID2). Activate the **Active** check box to enable the additional virtual WLAN. The tab provides separate configuration items for the selected SSID.
2. Enter at least a new **SSID**. Also enter a currently unused **VLAN tag** number.
3. You can specify different authentication/encryption settings for each SSID section. For example, you can use **WPA / Pre-shared key** with different passwords.

18.6.7 MAC ACCESS FILTERS

MAC access filters are used to allow access from listed WLAN stations only.

You can import a prepared list of MAC addresses (*.txt. file, one line per MAC address, a Name may be added on the same line separated by ;). Use the **Browse** button to select the file from the file system. Afterwards press the **Import** button.

To configure single MAC addresses, use the **New** button in the **General settings** section. Enter the address in the following **New MAC access filter** dialog.

To delete a single MAC address, click on the icon left behind the address entry. Use the **Delete all** button to delete the entire list.

Using the **Save** button you can export the MAC address filter list.

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

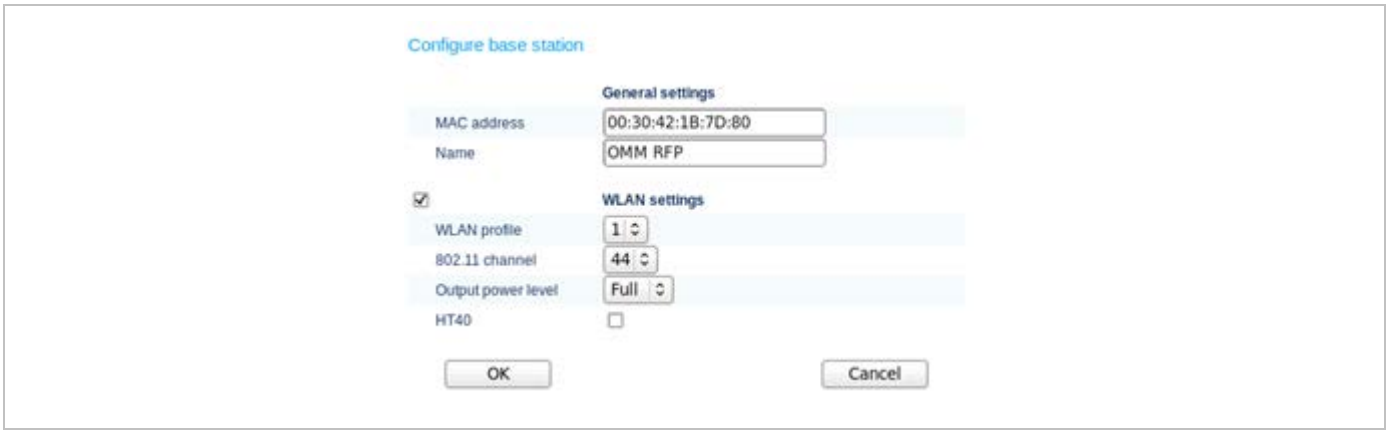
The usage of the MAC access filter is controlled by the checkbox in the SSID configuration tab.

18.7 BASE STATIONS

The **Base Stations** menu lists the known base stations, either sorted by the **DECT bases** or by **WLAN profiles**. The **Sorted by WLAN Profiles** lists all Base Stations by their associated WLAN profile, showing the selected channel and the transmission power.

Assigning WLAN Profile and configuring Channel and transmit power

After select and click on the icon a configuration window opens. Parameters like **Name**, **WLAN profile**, **802.11 channel**, **Output power level** and the **HT40** option may be configured.



Please note: Some options and parameters may not be available due to regulatory restrictions or because of configuration done in the WLAN profile.

18.8 WLAN CLIENTS

Associated WLAN stations are listed in the **WLAN Clients** menu.

19 DIGIT TREATMENT

Digit treatment can be configured to modify outgoing or incoming numbers, as well as numbers returned in LDAP and XSI directory queries (corporate directories).

Digit treatment for corporate directories

The system checks a number chosen from an LDAP or XSI directory entry against the external prefix pattern and if a pattern matches, it is replaced by the configured internal prefix pattern. Only the best matching rule is applied.

Before a rule is applied, the following characters are automatically removed from the directory entry: '%', space, '(' and ')'. The result is sent to the DECT phone for display (e.g., in the directory entry details and entered in the redial list).

> **Please note:** Digit treatment applies to "number" anmd "mobile" numbers in an XSI directory entry, but not to extensions or "emailAddress" fields.
>
> **Please note:** A conversion performed for an LDAP directory entry can be reversed if the rule is also activated for an outgoing call.

Incoming call

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

The result of the conversion is sent to the DECT phone to be displayed and entered in the call log.[1]

Outgoing call

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

> **Please note:** To support digit treatment and overlap sending, a dial terminator must be configured.

The result of the conversion is not sent to the DECT phone to be displayed or entered in the call log.[2]

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

- creating and changing "Digit treatment" entries
- deleting "Digit treatment" entries

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

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

19.1 CREATING AND CHANGING “DIGIT TREATMENT” ENTRIES

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

2 **External pattern**: Enter an external prefix pattern with up to 32 characters that matches an incoming call number or a number received via a directory entry. The prefix to be substituted for calling party numbers has the same character set as the user telephone number (e.g., :”+*~#,;.-_!$%&/()=?09aAzZ”).

3 **Internal pattern**: Enter an internal prefix pattern with up to 32 characters that replaces the external pattern for the directory entry / incoming calls or vice versa for outgoing calls. An internal prefix pattern can be composed of characters “*”, ”#” and “0” – “9”.

> **Please note:** The plus character (“+”) can only be dialed and transferred to a call log with a Mitel 600 DECT phone.

4 **Direction**: Select one of the following options:

- “Incoming calls”: Rule applies on incoming calls.
- “Outgoing calls”: Rule applies on outgoing calls.
- “Incoming and outgoing calls”: Rule applies on incoming and outgoing calls.
- “Apply on directory only”: Rule applies to directories only.

5 **Directory**: This option can be used to specify the rule for incoming and/or outgoing calls. Activate this option if the rule applies to directories.

6 Press the **OK** button.

Parameter / Parameter group	**Digit treatment**
Description	A number manipulation is provided by the digit treatment feature for corporate directories but also to handle both incoming and outgoing calls.
Web	Advanced: System Features > Digit treatment
OMM Configuration files	n.a.
DECT Phone	n.a.
User configuration files	n.a.

19.2 DELETING “DIGIT TREATMENT” ENTRIES

To delete an existing entry:

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

2 Press the **Delete** button.

20 DIRECTORY

The **Directory** menu allows you to manage connections to one or more LDAP, XML, or XSI servers to support central corporate directories.

The OMM supports multiple LDAP, XML or XSI servers with specific parameter settings to support different types of directories (e.g., global corporate directory, group specific directory, personal directory). XML-based directory services can be implemented using the XML terminal interface.

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

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

The Personal directory on the Mitel 600 DECT phone can hold up to 200 entries (stored on the phone or the microSD card). The directory is auto-filled and stores names and numbers from the caller list.

> **Please note:** With the introduction of XSI directory support in SIP-DECT 6.2, the underlying database model for directory support in SIP-DECT has changed. To support backwards compatibility, the **Directory (comp. mode)** page provides directory configuration and maintenance for existing SIP-DECT systems with LDAP or XML directories.

20.1 CREATING AND CHANGING DIRECTORY ENTRIES

You can configure directory entries (or change existing entries) from the **Directory** page (or the **Directory (comp. mode)** page for older SIP-DECT systems) in the OMM web interface.

To change the configuration of an existing entry click on the pencil icon beside the entry, and follow the steps described below to set parameter values.

To create a new directory entry, do the following:

1. Select the **Directory** entry in the **System Features** menu (left pane).
2. Click **New** on the **Directory** page.
3. On the **New directory entry** page, specify values for the directory server, as described in the following table. Note that only certain parameters are required, depending on the directory server type.

Parameter	Description	LDAP	XML	XSI
Active	Enables or disables the directory entry on the DECT phone.	✓	✓	✓
Type	Interface supported by the directory server. Possible values: • LDAP • XML • XSI/enterprise • XSI/enterprise common • XSI/group • XSI/group common • XSI/personal	✓	✓	✓
Name	Name to be displayed for the directory (Latin-1 character set is supported).	✓	✓	✓
Search base	Location in the directory from which the search begins (e.g., ”ou=people, o=my com”). The configuration is valid for all DECT phones that support the LDAP directory feature. To make search requests unique for different users, the search base configuration can include placeholders that are replaced by user-specific values when submitting the LDAP request to a server. The following placeholders are defined: • “<TEL>” (for the user’s telephone number) • “<DESC1>” (for the user’s “Description 1” attribute) • “<DESC2>” (for the user’s “Description 2” attribute) • “SIPProxy” (for the current primary, secondary or tertiary SIP server address); supported for release 6.1 and later	✓		
Search type	Attribute on which searches are performed (**Surname** or **Given name**).	✓		✓
Display type	Display mode for search results (**Surname, First Name** or **Given name Surname**).	✓		✓
Server search timeout	Interval (in seconds) during which the OMM waits for search results from the LDAP server (1 – 10 seconds).	✓		
Protocol	Transfer protocol used to communicate with the directory server (**http** or **https**).		✓	✓
Server port	Port on the directory server. LDAP: default is 389. SSL (default port 689) is not supported. Windows Active Directory Server uses port 3268. XML or XSI: Default is 80 (for http) or 443 (for https).	✓	✓	✓
Server name	IP address or FQDN of the directory server.	✓	✓	✓

Parameter	Description	LDAP	XML	XSI
User name	Name of the account for directory server access, if required.	✓	✓	
Password	Password for directory server access, if required. **Note**: If no user/password is specified, an anonymous bind takes place. SIP-DECT supports LDAP simple bind.	✓	✓	
Path (and parameters)	URL (with parameters, if required) to the XML directory on the directory server.		✓	
Use common certificate configuration	Enables or disables use of the system's certificates (loaded for provisioning purposes) for HTTPS directory access		✓	✓

4 Click **OK** to create the directory entry.

Please note: To change the order of the directory entries, click the up or down arrow in the Order column to move the entry up or down in the list. Changing the order of directory entries in the list changes the order in which they appear on the DECT phone.

You can also configure directory entries using the AXI commands in the OMM configuration files. The following example shows the commands and attributes used to create an XSI Enterprise directory entry:

```
<SetCorporateDirectory plainText="1">
<directory id="3" active="1" type="XSIenterprise"
  name="XSI enterprise"
  searchType="SN"
  displayType="SN, GN">
<url
  protocol="HTTPS"
  host="xsi.customer.net"
  useCommonCerts="1" />
</directory>
</SetCorporateDirectory>
```

If you want to specify a specific place for the directory entry in the list, you can use the following command:

```
<SetCorporateDirectoryOrder >
<directory order="1" id="3" />
<directory order="2" id="4" />
<directory order="3" id="1" />
<directory order="4" id="2" />
<directory order="5" id="5" />
</SetCorporateDirectoryPrder>
```

For more information on configuration via OMM AXI commands, see the *SIP-DECT OM Application XML Interface Reference Guide*.

To create a new directory entry or change an existing entry using the old database model, do the following:

1 Select the **Directory (comp. Mode)** entry in the **System Features** menu (left pane).
2 Click **New** on the **Directory (comp. Mode)** page.
3 On the **New directory entry** page, specify values for the directory server, as described in the following table. Note that only certain parameters are required, depending on the directory server type.

Parameter	Description	LDAP	XML
Active	Enables or disables the directory entry on the DECT phone.	✓	✓
Order	Specify where you want the directory entry to appear in the list.	✓	✓
Type	Interface supported by the directory server. Possible values: LDAP or XML.	✓	✓
Name	Name to be displayed for the directory (Latin-1 character set is supported).	✓	✓
Protocol	Transfer protocol used to communicate with the directory server (**HTTP** or **HTTPS**).		✓
Server name	IP address or FQDN of the directory server.	✓	✓
Server port	Port on the directory server. LDAP: Default is 389. SSL (default port 689) is not supported. Windows Active Directory Server uses port 3268. XML: Default is 80 (for http) or 443 (for https).	✓	✓
Search base	Location in the directory from which the search begins (e.g., ”ou=people, o=my com”). The configuration is valid for all DECT phones that support the LDAP directory feature. To make search requests unique for different users, the search base configuration can include placeholders that are replaced by user-specific values when submitting the LDAP request to a server. The following placeholders are defined: • “<TEL>” (for the user’s telephone number) • “<DESC1>” (for the user’s “Description 1” attribute) • “<DESC2>” (for the user’s “Description 2” attribute) • “SIPProxy” (for the current primary, secondary or tertiary SIP server address); supported for release 6.1 and later	✓	
User name	Name of the account for directory server access, if required.	✓	✓
Password	Password for directory server access, if required. **Note**: If no user/password is specified, an anonymous bind takes place. SIP-DECT supports LDAP simple bind.	✓	✓
Search type	Attribute on which searches are performed (**Surname** or **Given name**).	✓	

Parameter	Description	LDAP	XML
Display type	Display mode for search results (**Surname, First Name** or **Given name Surname**).	✓	
Server search timeout	Interval (in seconds) during which the OMM waits for search results from the LDAP server (1 – 10 seconds).	✓	
Path (and parameters)	URL (with parameters, if required) to the XML directory on the directory server.		✓

4 Click **OK** to create the directory entry.

> **Please note:** To change the order of the directory entries, you can click the up or down arrow in the Order column to move the entry up or down in the list. Changing the order of directory entries in the list changes the order in which they appear on the DECT phone.

20.2 DELETING DIRECTORY ENTRIES

1 To delete an existing directory entry, click on the icon beside the entry on the **Directory** or **Directory (comp. mode)** page.

The **Delete directory entry** dialog opens showing the current configuration of this entry.

2 Press the **Delete** button.

21 FEATURE ACCESS CODES

There are two kinds of feature access codes (FACs) supported

- **XML application “Feature Access Codes”** (see section 23.1.1): This FAC is directed to send codes to a XML server. The functionality depends on providers rules.
- **OMM-specific “Feature Access Codes”:** These FACs drive OMM features. The configuration and some notes on the corresponding features are described in this chapter.

> **Please note:** Adminstrators should be aware that any configured feature access codes inherit potential conflicts with dialing plans of the whole telephony environment.

To configure a specific FAC feature, do the following (on the **Feature Access Codes** page):

1 **FAC number**: Enter a unique FAC number (Default = *##). This number is a mandatory prefix for each specific FAC. This prefix is the indication for the OMM to treat the dialed digits as a FAC.

2 Check the appropriate checkbox(es) to enable the corresponding FAC feature(s) you want to activate. For each enabled FAC feature, enter an assigned access code.

Afterwards the appropriate action can be performed by dialing the FAC number, followed by the FAC access code en-bloc from any subscribed DECT phone.

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

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

The following FAC options are available:

- **Activate subscription**: Allow DECT phone subscription.
- **Deactivate subscription**: Disable subscription permission.
- **User Login**: Login a user.
- **User logout**: Logout the user.
- **Set system credentials for provisioning:** The user can set system credentials via the Mitel 600 DECT phone using the FAC code.
- **Blind transfer:** Initiate a blind transfer from the DECT phone (for conferencing with MiVoice Business conference server). When a DECT phone user dials the ”Blind transfer” FAC en-bloc (in an active call state) followed by a target number, SIP-DECT initiates a blind transer to the specified target number.

Configuration details

Parameter / Parameter group	**FAC number**
Description	Mandatory prefix of each specific FAC. This prefix is the indication for the OMM to treat the dialed digits as a feature access code.
Format	String
Range	62 characters
Default value	*##
Web	Advanced: System features > Feature access code
OMM Configuration files	<SetFACPrefix prefix="*##" />

DECT Phone	n.a.
User configuration files	n.a.

Parameter / Parameter group	**Activate subscription**
Description	Allow DECT phone subscription
Format	String
Range	62 characters
Default value	Not enabled and string is empty
Web	Advanced: System features / Feature access code
OMM Configuration files	<SetFAC> <fac feature="ActivateSubscription" enable="1" fac="1" /> </SetFAC>
DECT Phone	n.a.
User configuration files	n.a.

Parameter / Parameter group	**Deactivate subscription**
Description	Disable subscription permission
Format	String
Range	62 characters
Default value	Not enabled and string is empty
Web	Advanced: System features > Feature access code
OMM Configuration files	<SetFAC> <fac feature="DeactivateSubscription" enable="1" fac="2" /> </SetFAC>
DECT Phone	n.a.
User configuration files	n.a.

Parameter / Parameter group	**User login**
Description	Login a user
Format	String
Range	62 characters
Default value	Not enabled and string is empty
Web	Advanced: System features > Feature access code
OMM Configuration files	<SetFAC> <fac feature="UserLogin" enable="1" fac="3" /> </SetFAC>
DECT Phone	n.a.
User configuration files	n.a.

Parameter / Parameter group	**User logout**
Description	Logout the user
Format	String
Range	62 characters
Default value	Not enabled and string is empty
Web	Advanced: System features > Feature access code
OMM Configuration files	<SetFAC> <fac feature="UserLogout" enable="1" fac="4" /> </SetFAC>
DECT Phone	n.a.
User configuration files	n.a.

Parameter / Parameter group	**Set system credentials for provisioning**
Description	The user can set system credentials via the Mitel 600 DECT phone using the FAC code.
Format	String
Range	62 characters
Default value	Not enabled and string is empty
Web	Advanced: System features > Feature access code
OMM Configuration files	<SetFAC> <fac feature="SystemCredentialPasswd" enable="1" fac="5" /> </SetFAC>
DECT Phone	n.a.
User configuration files	n.a.

Parameter / Parameter group	**Blind transfer**
Description	Initiate a blind transfer from the DECT phone (for conferencing with MiVoice Business conference server). When a user dials the ”Blind transfer” FAC en-bloc (in an active call state) followed by a target number, SIP-DECT initiates a blind transer to the specified target number.
Format	String
Range	62 characters
Default value	Not enabled and string is empty
Web	Advanced: System features > Feature access code
OMM Configuration files	<SetFAC> <fac feature="BlindTransfer" enable="1" fac="6" /> </SetFAC>
DECT Phone	n.a.

User configuration files	n.a.

22 XML APPLICATIONS

The SIP-DECT XML terminal interface allows external applications to provide content to 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).

Please note: SIP-DECT releases apply behavior to XML objects as defined in SIP-DECT XML terminal interface specifications /46/ and /36/.
Partners can access the interface specification /36/ by registering for the A2P2 program.

22.1 BUILT-IN XML APPLICATIONS

The SIP-DECT XML terminal interface allows external applications to provide content to the user on the Mitel 600 DECT phone display, and much more. To make the XML terminal interface applications available to the DECT phone user, you must configure the appropriate hooks.
The following built-in applications can be used:

Hook	Description	Programmable Key	Menu entry
Caller list	Hook to replace the local caller list	yes	yes
Redial list	Hook to replace the local redial list	yes	yes
Presence	Hook to reach a presence application	yes	yes
Server Menu	Hook to reach a server menu	yes	yes [1]
Action URI	URI to be called in case of user/DECT phone events	no [2]	no [2]
Feature access codes	Hook to provide “Feature Access Codes Translation”	yes	yes
Call Completion	Hook to provide callback option when user places outgoing call and wants to request a callback before hanging up	yes	yes
Park call	Hook to the Park Call service interface.	yes	yes
Unpark call	Hook to the Unpark Call service interface.	yes	yes
Pickup	Hook to the Pickup Call service interface.	yes	yes
Take	Hook to the Take Call service interface.	yes	yes
Call forward	Hook to the Call Forward service interface.	yes	yes
Call routing	Hook to the Personal Call Routing service interface (Mitel 602 DECT phones only).	yes	yes
Call protection	Hook to the PBX Call Protection service interface (Mitel 602 DECT phones only).	yes	yes
Voice box	Hook to Voice Mail service interface.	yes	yes

[1] The server menu is integrated in the OMM system menu. The OMM system menu is available as a menu entry in the local main menu of the DECT phone (soft key ») or directly available by a long press of the » soft key. If no user is assigned to the DECT phone, the server menu is the only available XML application hook.

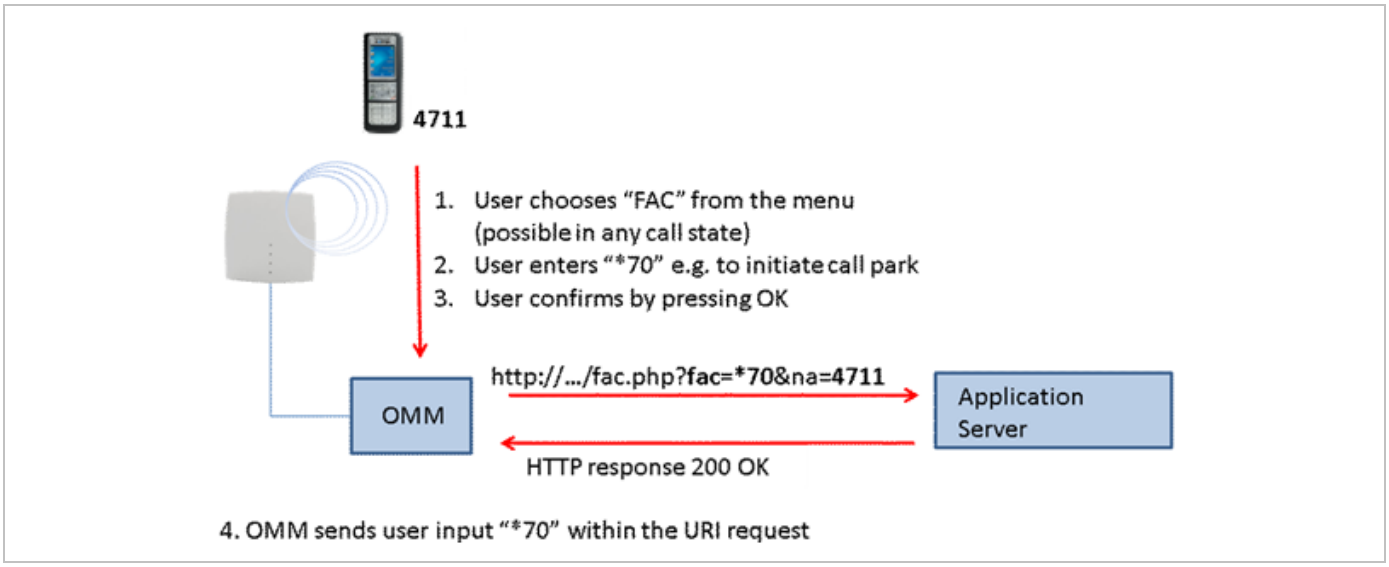
[2] The URI to be called is configured via OMM configuration files or WEB service. Content can be pushed towards the DECT phone via SIP notify. For more information please see /36/.

22.1.1 FEATURE ACCESS CODE TRANSLATION

Many PBXs allow the control of PBX supplementary services by dialing specific numbers (Feature Access Codes (FAC)).

SIP-DECT supports the “Feature Access Codes Translation” XML application to avoid any conflict with SIP-DECT feature access codes or digit treatment rules with PBX feature access codes.

- If “Feature Access Codes Translation” is activated, SIP-DECT users can choose the “FAC” menu on the Mitel 600 DECT phone in any call state and enter the feature code en-bloc. The input is sent to the PBX (Application server) within a URI request.



22.1.1.1 Call Completion

This feature assumes the presence of an application server, which maintains callback or call completion. In interaction with such a server, the caller can ask for a callback before he gives up calling. If the service is activated, the DECT phone offers the menu option “callback” whenever the active call is an outgoing one. This menu is also offered if a SIP BYE notification is received and the “Failed call release timeout” value is greater than zero.

Please note: IMPORTANT: If call completion is pressed, the call line is not released automatically by the OMM. It is the responsibility of the customer’s XML service and call server to maintain that situation.

22.1.2 BUILT-IN XML APPLICATIONS CONFIGURATION

Parameter / Parameter group	**DECT phone caller list**
Description	Hook to replace the local caller list (displayed via the “Info > Caller List” DECT phone menu entry) and use a call server-provided list instead. To use this hook, the user must be logged in.
Format	n.a.
Range	n.a.

Default value	Disabled
Web	Advanced: System Features > XML Applications > Caller List
OMM configuration files	<SetXMLApplication > <xmlAppl enable="1" id="0" name="callerList" type="BuiltIn" > <url protocol="HTTP" host="10.103.35.22" path="callerList?key=20&na={number}" /> </xmlAppl> </ SetXMLApplication > Note: This is an example; certain server conditions must be adapted.
DECT Phone	n.a.
User configuration files	n.a.

Parameter / Parameter group	**DECT phone redial list**
Description	Hook to replace the local redial list (displayed via the “Info > Redial List” DECT phone menu entry) and use a call server-provided list instead. To use this hook, the user must be logged in.
Format	n.a.
Range	n.a.
Default value	Disabled
Web	Advanced: System Features > XML Applications > Redial List
OMM configuration files	<SetXMLApplication plainText="1"> <xmlAppl enable="1" id="1" name="redialList" type="BuiltIn" > <url protocol="HTTPS" host="10.103.35.22" username="testUser" password="TestPassword" path="redialList?key=18&na={number}" /> </xmlAppl> </ SetXMLApplication > Note: This is an example; certain server conditions must be adapted. Also “plainText” attribute must be left when an encrypted password is used.
DECT Phone	n.a.
User configuration files	n.a.

Parameter / Parameter group	**DECT phone presence**
Description	Hook to reach a presence application (displayed as additional “Presence” DECT phone menu entry). To use this hook, the user must be logged in.
Format	n.a.
Range	n.a.
Default value	Disabled
Web	Advanced: System Features > XML Applications > Presence
OMM configuration files	<SetXMLApplication > <xmlAppl enable="1" id="2" name="userPresence" type="BuiltIn" > <url protocol="HTTP" host="10.103.35.22"

	path="presence?na={number}" /> </xmlAppl> </ SetXMLApplication > Note: This is an example, certain server conditions has to be adapted.
DECT Phone	n.a.
User configuration files	n.a.

Parameter / Parameter group	**DECT phone server menu**
Description	Hook to reach a server menu (displayed as an additional “System > Server” DECT phone menu entry). The server menu is integrated in the OMM system menu. The OMM system menu is available as a menu entry in the local main menu of the DECT phone (soft key or directly available by a long press of the soft key). If no user is assigned to the DECT phone, the server menu is the only available XML application hook.
Format	n.a.
Range	n.a.
Default value	Disabled
Web	Advanced: System Features / XML Applications / Server menu
OMM configuration files	<SetXMLApplication > <xmlAppl enable="1" id="3" name="systemApplMenu" type="BuiltIn" > <url protocol="HTTP" host="10.103.35.22" path="serverMenu?na={number}" /> </xmlAppl> </ SetXMLApplication > Note: This is an example; certain server conditions has to be adapted.
DECT Phone	n.a.
User configuration files	n.a.

Parameter / Parameter group	**DECT phone event actions**
Description	URI to be called in case of user/device events at the DECT phone. Depending on these events, a server can take action (e.g., to push content towards the DECT phone via SIP NOTIFY).
Format	n.a.
Range	n.a.
Default value	Disabled
Web	Advanced: System Features / XML Applications / Action URI
OMM configuration files	<SetXMLApplication > <xmlAppl enable="1" id="4" name="eventActions” type="BuiltIn" > <url protocol="HTTP" host="10.103.35.22" path="eventAction?na={subsc}&ppn={ppn}&dis={dis}&reg={rege}" />

	</xmlAppl> </ SetXMLApplication > Note: This is an example; certain server conditions must be adapted.
DECT Phone	n.a.
User configuration files	n.a.

Parameter / Parameter group	**DECT phone “Feature Access Codes Translation”**
Description	Hook to provide “Feature Access Codes Translation”. To use this hook, the user must be logged in.
Format	n.a.
Range	n.a.
Default value	Disabled
Web	Advanced: System Features / XML Applications / Feature access codes
OMM configuration files	<SetXMLApplication > <xmlAppl enable="1" id="5" name="featureAccessCodes" type="BuiltIn" > <url protocol="HTTP" host="10.103.35.22" path="serviceCodes?na={number}" /> </xmlAppl> </ SetXMLApplication > Note: This is an example; certain server conditions must be adapted.
DECT Phone	n.a.
User configuration files	n.a.

Parameter / Parameter group	**DECT phone call completion**
Description	Hook to provide a “callback” option in the DECT phone menu when a user places an outgoing call and wants to request a callback before releasing the call. To use this hook, the user must be logged in.
Format	n.a.
Range	n.a.
Default value	Disabled
Web	Advanced: System Features / XML Applications / Call completion
OMM configuration files	<SetXMLApplication > <xmlAppl enable="1" id="6" name="callCompletion" type="BuiltIn" > <url protocol="HTTP" host="10.103.35.22" path="callCompletion?na={number}" /> </xmlAppl> </ SetXMLApplication > Note: Example only.
DECT Phone	n.a.
User configuration files	n.a.

Parameter / Parameter group	**DECT phone park call**
Description	Hook to provide a “park call” option in the DECT phone menu when a user wants to place an active call on hold so that the call can be picked up from another DECT phone. To use this hook, the user must be logged in.
Format	n.a.
Range	n.a.
Default value	Disabled
Web	Advanced: System Features / XML Applications / Park call
OMM configuration files	<SetXMLApplication > <xmlAppl enable="1" id="7" name="parkCall" type="BuiltIn" > <url protocol="HTTP" host="10.103.35.22" path="parkCall?na={number}" /> </xmlAppl> </ SetXMLApplication > Note: Example only.
DECT Phone	n.a.
User configuration files	n.a.

Parameter / Parameter group	**DECT phone unpark call**
Description	Hook to provide an “unpark call” option in the DECT phone menu when a user wants to retrieve a call that has been parked. To use this hook, the user must be logged in.
Format	n.a.
Range	n.a.
Default value	Disabled
Web	Advanced: System Features / XML Applications / Unpark call
OMM configuration files	<SetXMLApplication > <xmlAppl enable="1" id="8" name="unparkCall" type="BuiltIn" > <url protocol="HTTP" host="10.103.35.22" path="unparkCall?na={number}" /> </xmlAppl> </ SetXMLApplication > Note: Example only.
DECT Phone	n.a.
User configuration files	n.a.

Parameter / Parameter group	**DECT phone pickup call**
Description	Hook to provide a “pickup” option in the DECT phone menu when a user wants to answer a call that has come in on a directory number other than their own. To use this hook, the user must be logged in.
Format	n.a.
Range	n.a.

Default value	Disabled
Web	Advanced: System Features / XML Applications / Pickup
OMM configuration files	<SetXMLApplication > <xmlAppl enable="1" id="9" name="pickup" type="BuiltIn" > <url protocol="HTTP" host="10.103.35.22" path="pickup?na={number}" /> </xmlAppl> </ SetXMLApplication > Note: Example only.
DECT Phone	n.a.
User configuration files	n.a.

Parameter / Parameter group	**DECT phone take call**
Description	Hook to provide a “take” option in the DECT phone menu when a user wants to take over or continue an active call from another device without interruption (e.g., user has an active call on a desk phone and wants to continue the call on a DECT phone). To use this hook, the user must be logged in.
Format	n.a.
Range	n.a.
Default value	Disabled
Web	Advanced: System Features / XML Applications / Take
OMM configuration files	<SetXMLApplication > <xmlAppl enable="1" id="10" name="take" type="BuiltIn" > <url protocol="HTTP" host="10.103.35.22" path="take?na={number}" /> </xmlAppl> </ SetXMLApplication > Note: Example only.
DECT Phone	n.a.
User configuration files	n.a.

Parameter / Parameter group	**DECT phone call forward**
Description	Hook to provide a “call forward” option in the DECT phone menu when a user wants to forward a call to another number. To use this hook, the user must be logged in.
Format	n.a.
Range	n.a.
Default value	Disabled
Web	Advanced: System Features / XML Applications / Call forward
OMM configuration files	<SetXMLApplication > <xmlAppl enable="1" id="11" name="callForward" type="BuiltIn" > <url protocol="HTTP" host="10.103.35.22" path="callForward?na={number}" />

	</xmlAppl> </ SetXMLApplication > Note: Example only.
DECT Phone	n.a.
User configuration files	n.a.

Parameter / Parameter group	**DECT phone call routing**
Description	Hook to provide a “call routing” option in the DECT phone menu when a user wants to route incoming calls to one or more pre-programmed destinations. To use this hook, the user must be logged in. This option is only avaialbe for Mitel 602 DECT phones.
Format	n.a.
Range	n.a.
Default value	Disabled
Web	Advanced: System Features / XML Applications / Call routing
OMM configuration files	<SetXMLApplication > <xmlAppl enable="1" id="12" name="callRouting" type="BuiltIn" > <url protocol="HTTP" host="10.103.35.22" path="callRouting?na={number}" /> </xmlAppl> </ SetXMLApplication > Note: Example only.
DECT Phone	n.a.
User configuration files	n.a.

Parameter / Parameter group	**DECT phone call protection**
Description	Hook to provide a “call protection” option in the DECT phone menu when a user wants to secure calls between DECT phones. To use this hook, the user must be logged in. This option is only avaialbe for Mitel 602 DECT phones.
Format	n.a.
Range	n.a.
Default value	Disabled
Web	Advanced: System Features / XML Applications / Call protection
OMM configuration files	<SetXMLApplication > <xmlAppl enable="1" id="13" name="callProtection" type="BuiltIn" > <url protocol="HTTP" host="10.103.35.22" path="callProtection?na={number}" /> </xmlAppl> </ SetXMLApplication > Note: Example only.
DECT Phone	n.a.

User configuration files	n.a.

Parameter / Parameter group	**DECT phone voice box**
Description	Hook to allow the user to dial the voice mail system. To use this hook, the user must be logged in.
Format	n.a.
Range	n.a.
Default value	Disabled
Web	Advanced: System Features / XML Applications / Voice box
OMM configuration files	<SetXMLApplication > <xmlAppl enable="1" id="14" name="voiceBox" type="BuiltIn" > <url protocol="HTTP" host="10.103.35.22" path="voiceBox?na={number}" /> </xmlAppl> </ SetXMLApplication > Note: Example only.
DECT Phone	n.a.
User configuration files	n.a.

All hooks can be activated or deactivated, but not deleted.

Please note: “Caller list” and “Redial list” replace the local caller and redial lists of the Mitel 600 if activated. Additionally, the list access must be set to “Automatic” or “PBX” on the DECT phone in the “Settings > List access” menu. If the list access is set to “Local”, the DECT phone uses the local list.

An activated hook becomes available on a DECT phone (including the corresponding menu entry) after the next DECT location registration of the DECT phone. This can be forced by switching the DECT phone off and on. The same applies for deactivating a hook.

22.2 ADDITIONAL XML APPLICATIONS

In addition to the built-in XML applications, SIP-DECT supports the creation of additional XML applications to provide content to the user on the Mitel 600 DECT phone display. To make the XML terminal interface applications available to the DECT phone user, the appropriate hooks must be configured in the OMM. Up to 10 additional hooks can be created dynamically.

Additional XML Applications Configuration

Parameter / Parameter group	**DECT phone additional XML applications 1 ... 10**
Description	Application hooks 1-10 to provide to the DECT phone for end users (accessed via “ » > Applications” DECT phone menu entry). All available XML applications are listed by name dynamically. To use these hooks, the user must be logged in.

Format	n.a.
Range	n.a.
Default value	Disabled
Web	Advanced: System Features > XML Applications > XML-1 … XML-10
OMM configuration files	n.a.
DECT Phone	n.a.
User configuration files	n.a.

22.3 INTEGRATION OF CORPORATE DIRECTORIES

The SIP-DECT solution supports integration of LDAP, XML, and XSI-based corporate directory services. This feature works in conjunction with additional XML applications. Each XML-based directory reduces the additional XML applications and vice versa. Therefore, XML-based directories are listed in the **XML Applications** page on the OMM web service, while they are configured in the “System Features / Directory / “type XML” web service section. Please refer to corporate directories (section 21) for more information.

22.4 SUPPORT “SIPPROXY” PLACEHOLDER IN XML HOOKS

In addition to the built-in XML applications, SIP-DECT allows the use of additional XML applications to provide content to the user on the Mitel 600 DECT phone display. To make the XML terminal interface applications available to the DECT phone user, the appropriate hooks must be configured in the OMM. Up to 10 additional hooks can be created dynamically.

“SIPProxy” Placeholder in XML Hooks Configuration

Parameter / Parameter group	**“SIPProxy” placeholder in XML applications for “Server”**
Description	In cases where XML applications are located on a SIP Call Manager, it is necessary to address XML applications by using the current primary, secondary or tertiary SIP Call Manager address. In those cases, the “SIPProxy” placeholder can be used as server input.
Format	n.a.
Range	n.a.
Default value	n.a.
Web	Advanced: System Features > XML Applications > all applications > Server
OMM configuration files	<SetXMLApplication > <xmlAppl enable="1" id="0" name="callerList" type="BuiltIn" > <url protocol="HTTP" host="SIPProxy" path="callerList?key=20&na={number}" /> </xmlAppl> </ SetXMLApplication > Note: This is an example, certain server conditions has to be adapted.
DECT Phone	n.a.

User configuration files	n.a.

22.5 XML TERMINAL INTERFACE EXTENSIONS

SIP-DECT supports certain extensions for the XML terminal interface. These include specific actions on existing XML sessions, as well as the processing of an XML action response (HTTP 200 OK with content).

The following SIP-DECT XML terminal interface extensions are available:

- New element "*allowDestroyAndReplaceSession*" in XML objects.
  This element is used to handle sessions on a DECT phone. If this element is present, an existing session is cleared before the new object is pushed to the DECT phone. This is used in a SIP NOTIFY or in an HTTP response (e.g., as an answer to an XML DECT phone FAC Notification), which is normally empty, to push the object content to the DECT phone, independent of the current DECT phone state.
- New XML-Execute URI keys "*Key:Headset*", "*Key:OnHook*" and "*Key:OffHook*"
  Used for call control, to accept an incoming call or end an existing call at the DECT phone.
- New XML-Execute URI keys "*Command:SipRegister*"
  Used to force a new registration of a SIP device/DECT phone.
- A SIP registration for a specific user can be triggered from an external application (e.g., from a call server) by sending a PhoneExecute with *URI="Command:SipRegister"* in the SIP Notify message.

The features work without any configuration. They are fully controlled by an external XML-application or call server.

22.5.1 CTI CALL ANSWER

Using the XML Terminal Interface, a CTI application can force the answering of a call from a remote desktop instead of pressing the hook key on the DECT phone. Speech path is automatically established. (For technical details see "req-0715: SIP-DECT® XML Terminal Interface /36/)

22.5.2 AUTO ANSWER, INTERCOM CALLS AND AUDIO SETTINGS

Some call features that fall under the category of "auto call" are:

- "Auto callback", initiated by a text message
- "directDial" URI in XML notifications

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

SIP-DECT allows control of some of the 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

In addition, SIP-DECT supports intercom calls. This means that the originating B party can force the called party's phone to establish the speech path immediately. Audio settings (mute, etc.) follow the permitted options.

23 CENTRAL DECT PHONE CONFIGURATION OVER AIR (COA)

Centralized DECT phone configuration over the air is supported for Mitel 612, 622, 632 and 650 DECT phones. Configurable parameters include:

- settings (loudness, contrast, etc)
- menu items (switch on or off, enable password protection)
- key assignments (including an override of manual key programming)

DECT phone configuration over air (CoA) is useful for deployment of special configuration to a single DECT phone or a large number of DECT phones. No local access to the DECT phone is required.

DECT phone CoA is implemented by providing additional configuration information to the well-known configuration files. 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 available. 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).

IMPORTANT : Centralized DECT phone Configuration over Air (CoA) requires 6.00 DECT phone software or later, and is only available on the Download over Air (DoA) master system.

You can configure three kinds of configuration files:

- Default DECT phone configuration profile
  Default configuration file used for all suitable DECT phones. The configuration is loaded into the DECT phone when subscription is complete, even if a user has not logged in to the device.
- DECT phone configuration profiles
  User-focused DECT phone configuration file used for a group of users. The configuration is loaded into the DECT phone when a user belonging to this group logs in to the device.
- DECT phone user individual configuration settings
  Individual DECT phone configuration settings used for a single user. The configuration is loaded into the DECT phone when the user logs in to the device.

The system consolidates the DECT phone settings before loading the configuration settings for a logged-in user into the DECT phone. Settings from DECT phone profiles overwrite default configuration settings, and individual user configuration settings overwrite DECT phone profiles and default configuration settings.

Configuration can be completed via user configuration files (user_common.cfg and <user.cfg> files), wherein a list of user-friendly settings can be used for the DECT phone configuration.

Please note: Deleting or overwriting configurations files on a DECT phone does not restore configuration to default or previous settings. Configuration elements that are not part of the new downloaded configuration file persist. To restore all settings, the administrator must initiate a power off/on at the DECT phone or use a default configuration file that contains all relevant settings.

To avoid interfering with the telephony or message service (especially with respect to alarm messages within the SIP-DECT system), only one configuration data download to the DECT phone is performed at a time. Therefore,

changing the default profile settings or other profile settings may take some time in a large system, until all the related DECT phones are updated.

23.1 DOWNLOAD OF CONFIGURATION FILES TO DECT PHONES

Profiles are downloaded to the DECT phone via the messaging mechanism, in conjunction with the internal message type “CONF_OVER_AIR”. This occurs in parallel with general message transfer to the DECT phone, and the lowest priority is used to ensure that the download does not interfere with the delivery of urgent messages. The message mechanism is also used to confirm a successful profile download, through AXI events.

Profile downloads to DECT phones are limited system-wide to a maximum of one download at a time to ensure no interference with OMM system operation. You can view the download on the OMM console (console command hcm).The download state is also part of the system dump.

Download Triggers

The OMM maintains a profile download list for all DECT phones that have configuration data to be set. These DECT phones are stored with the checksum of configuration data to be set. A DECT phone is included in this list when:

- the OMM system starts up and the associated DECT phone has configuration data to be set
- the associated DECT phone’s configuration data changes (this is communicated via AXI), such as:
  - change in the default configuration profile
  - change in the configuration profile for the user of the associated DECT phone
  - change in the individual user configuration profile for the user using the associated DECT phone
  - change in the configuration profile assigned to the user using the associated DECT phone

Profile downloads to the DECT phones (as maintained in the profile download list) are scheduled at regular intervals. A new download to DECT phones in the profile download list is scheduled when:

- a configuration change occurs on the DECT phone (via AXI notification)
- a location registration is received, and the checksum of the configuration data stored in the profile download list is different from the checksum sent in the location registration
- a download to a DECT phone completes

23.2 VARIABLE LISTS

The Mitel 602 DECT phone 6.1 firmware introduces variable lists. A variable list includes a number of items, each of which corresponds to an action to be performed on the DECT phone.

A list item consists of an index identifier (1..10) and either a number (to be dialed) or a function/feature that is supported by the DECT phone. Other attributes are optional. If there is a FunctionID, the entry does not have a sub key line in the variable list. If there is a number and a FunctionID, the DECT phone executes the associated action (if available); otherwise, the DECT phone dials the number.

Item Attribute	Type	Description	Example
Index	Decimal number	Index of list item (1..10)	7

Number	quoted UTF8-string	Number to dial	“\x2312*777*” (use \x23 for # in configuration file)
Name	quoted UTF8-string	Text displayed for item	“My Voice Box”
FunctionID	Function-ID-string	Function or feature to execute	pbx_directory
ShortName/Icon	quoted UTF8-string	Short name and/or icon displayed	“\xEE808B VB”
Handsfree	Boolean (“” or 1)	Dial in hands-free mode	1
VisibleSpecifier	4 digit string of “0” or “1”	Item visible in idle, dial, alerting and active state	1000

The CoA profile supports two variable lists for each DECT phone. Each list can contain up to 10 items.

Use the `UD_VListEntry` configuration command to configure an item for one of the lists. The first value specifies the index (1 or 2) of the list, followed by the attributes listed above.

The values-attribute pairs must be separated by a space and their position in the configuration command are fixed. Unused attributes must be indicated by empty strings if they are followed by non-empty attributes. Unused attributes (empty strings) can be omitted at the end of the configuration command.

A variable list can hold a name and/or short name (used to represent it in another list or near a programmed soft key or side key). The ‘short name’ attribute also allows you to specify an icon. A third attribute, ‘sub item’, determines whether or not subitems (sub key lines) of a list are displayed. By default, the subitem (sub key line) is only displayed if the item is selected.

List Attribute	Type	Description	Example
Name	quoted UTF8-string	Text displayed for list	“My Own Menu”
ShortName/Icon	quoted UTF8-string	Short name and/or icon displayed	“\xEE808B M1”
SubItems	Boolean (0 or 1)	Show sub-key line of selected item	1

Examples:

```
#PBX Menu using COA variable list
UD_ConfigurationName=PBX Menu

#Key assignment (function: vlst1 and vlst2)
UD_KeyAssignmentIdle=esc vlst1

#Menu Design
UD_VListName = 1 "Call services" #Titel
UD_VListShortName = 1 "More" #Softkey
UD_VListSubItems = 1 0 #Display Details per Item

### PLACEHOLDERs to add into Number field:
#<no>  will be replaced with a number from handset editor e.g. "*12*<no>#"
#<dial> will be replaced with a number from handset editor or directory, caller-list...
```

```
#<t=…> following dial-digits will be delayed for ... ms e.g. <t=3000ms>

#<inf=...> set info-box with ... string for (3000ms) continue dialing after info box e.g.
#<inf=Please wait>

#<r=...> call will be released after ... ms e.g. <r=10000>

#<close> will close this Menu.


### Entry: UD_VListEntry = List Index "Number" "Name" FunctionID "ShortName" Handsfree
# Visible

#ITEM           TYPE                       DESCRIPTION

#List           decimal number             item belong to variable list (1..2)

#Index          decimal number             index of list item (1..10)

#Number         quoted UTF8-string         number to dial "*1234" (use \x23 for #)

#Name           quoted UTF8-string         displayed text of item "My Voice Box"

#FunctionID     function-ID-string         function/feature to execute e.g. pbx_directory
#                                          (if available, preference over number)

#ShortName      quoted UTF8-string         displayed short name and/or icon

#Handsfree      Boolean (0 or 1)           dial in hands-free-mode

#Visible        4-digit-string of 0 or 1   item visible in idle-, dial-, alerting- and
#                                          active-state e.g.1000

#notice: to skip a parameter in the row use "" (even if the type is unquoted)


### idle menu functions

#Call Forward           **8 (predial) + number

#Call Forward Cancel    ##8 (dial)

#Do Not Disturb         *5  (dial)

#Do Not Dist. Cancel    #5  (dial)

#Call Pickup            *6  (dial)

#Call Park Retrieve     *8# (predial) + number

#Direct/Group Page      *37 (predial) + number

#Loudspeaker Page       **9 (dial)


UD_VListEntry = 1 1 "**8<dial>\x23<inf=Call FWD enabled><r=2000>" "Call Forward" "" "" ""

UD_VListEntry = 1 2 "\x23\x238<inf=CallFWD off><r=1000><close>" "Call Forward Cancel" ""
"" "" ""

UD_VListEntry = 1 3 "*5<inf=DND enabled><r=1000><close>" "Do Not Disturb" "" ""

UD_VListEntry = 1 4 "\x235<inf=DND off><r=1000><close>" "Do Not Dist. Cancel" "" ""

UD_VListEntry = 1 5 "*6<close>" "Call Pickup" "" "" ""

UD_VListEntry = 1 6 "*8\x23<dial>" "Call Park Retrieve" "" "" ""

UD_VListEntry = 1 7 "*37<dial>" "Direct/Group Page" "" "" ""

UD_VListEntry = 1 8 "**9<close>" "Loudspeaker Page" "" "" ""
```

23.2.1 ICON CODING

The following table lists the UTF8-codes for Mitel 602 DECT phone icons.

ICON	UTF8-Code	Description
	\xEE8083	Arrow Up
	\xEE8084	Arrow Down
	\xEE8085	Arrow Left
	\xEE8086	Arrow Right
	\xEE8088	Fox Key
	\xEE80B0	Locked
	\xEE80BC	Search
	\xEE80BE	Info
	\xEE81A5	Attention
	\xEE80BA	Tip
	\xEE808A	Telbook Private number
	\xEE808B	Telbook Mobile number
	\xEE808C	Telbook Business number
	\xEE818C	VIP number
	\xEE808D	Telbook Fax number
	\xEE808E	Telbook Email address
	\xEE808F	Telbook Name
	\xEE809B	Hook off / Predial
	\xEE809C	Hook on / Release
	\xEE81B0	Register recall
	\xEE8092	DTMF
	\xEE8182	3-party
	\xEE80A0	List Incoming call list
	\xEE80A1	List Outgoing call list
	\xEE8196	List Private directory /
	\xEE8199	List Central directory
	\xEE818C	List VIP

ICON	UTF8-Code	Description
	\xEE8181	List Filter / Call Filtered
	\xEE80A1	Call outgoing
	\xEE8099	Call Waiting
	\xEE80A7	Call Rejected
	\xEE81AD	Call SOS
	\xEE809D	Call Headset autoanswer
	\xEE8098	Call Loudspeaker autoanswer
	\xEE809B	Call Hook autoanswer
	\xEE80B8	Call deflected
	\xEE80A3	Call missed
	\xEE80A4	Call answered
	\xEE8195	Call on Voicebox
	\xEE81AE	Call VIP
	\xEE81B1	Pickup
	\xEE81B2	Pickup select
	\xEE8296	Call Park
	\xEE80BF	Call protection
	\xEE8298	Call routing
	\xEE8292	Callback

23.2.2 NUMBER STRING CODING

Note that the number specified in the list item may include one or more placeholders, so that, for example, the user can enter a number before the number is dialed. The placeholder keywords are specified in angle brackets ("< >"). If the dialed number includes angle brackets, you must use “<< >>”.

Number Placeholder	Description
<no>	If the number strings consists of <no>, it is replaced with a number from the DECT phone editor
<dial>	If the number string consists of <dial> it is replaced with a number from the DECT phone editor or directory, caller-list. For example, "*12*<no>#" -> ok <edit-number> send cc-info"*12*"<edit-number>"# (numbers may include letters like abcd... if the system supports alpha dialing)
<close>	All parents (e.g a list from witch this item is started) are closed
<t=…>	Following dial-digits are delayed for ... ms e.g. <t=3000ms>

Number Placeholder	Description
<inf=...>	Set info-box with ... string for (3000ms) continue dialing after info box (e.g. <inf=Please wait>)
<r=...>	Call is released after ... ms e.g. <r=10000>

23.3 DEFAULT COA PROFILE CONFIGURATION

Parameter / Parameter group	**Default Coa profile**
Description	The default CoA profile contains settings that are used for all subscribed DECT phones, even when no user is logged in. When a user is logged in, the default profile settings are merged with settings that the user is configured with (see profile settings for a user or user specific CoA settings).
Format	n.a.
Range	n.a.
Default value	n.a.
Web	n.a.
OMM configuration files	n.a.
DECT Phone	n.a.
User configuration files	Supported in the *user_common.cfg* configuration file: OM_Profile.0.Default.<key>=<values> … OM_Profile.0.Default.<key>=<values> Where “Default” is the reserved name for the default profile, and <key> is one of the configuration settings with its <values> to be set (see section 24.6 for available settings). Example: OM_Profile.0.Default.UD_DispLang="en" OM_Profile.0.Default.UD_DispFont="normal" OM_Profile.0.Default.UD_DispColor="black"

Parameter / Parameter group	**Default CoA profile delete**
Description	Deletion of the default profile.
Format	n.a.
Range	n.a.
Default value	n.a.
Web	n.a.
OMM configuration files	n.a.

DECT Phone	n.a.
User configuration files	Supported in the *user_common.cfg* configuration file: OM_Profile.0.Delete=yes

Please note: A complete removal of the default profile from user_common.cfg does not remove the profile in the OMM database. It must be explicitly deleted in the OMM database.
Note further that the settings in the DECT phone might stay set until the next master reset at the DECT phone is done or each setting has been overwritten by other related settings.

23.4 COA PROFILE CONFIGURATION

Parameter / Parameter group	**CoA profile 1 … 20**
Description	Up to 20 CoA profiles can be configured for groups of users. The user must be logged in to receive the profile settings assinged to the user. The settings are merged with default profile settings if set. Default profile settings have lower priority (see also default profile settings or user-specific CoA settings). **Note:** When a COA profile is deleted, its profile ID assignment to DECT phone users remains. If a new CoA profile is created and acquires this profile ID (the IDs are assigned in sequential order), any DECT phone users with the old profile ID are automatically assigned to the new CoA profile.
Format	n.a.
Range	n.a.
Default value	n.a.
Web	n.a.
OMM configuration files	n.a.
DECT Phone	n.a.
User configuration files	Supported in the *user_common.cfg* configuration file: OM_Profile.<no>.<name.<key>=<values> … OM_Profile.<no>.<name>.<key>=<values> Where <no> is the number of the profile, <name> is the name for the numbered profile (must be identical for all settings of the numbered profile), and <key> is one of the configuration settings with its <values> to be set (see section 24.6 for available settings). Example: OM_Profile.5.Doctor.UD_DispLang="en" OM_Profile.5. Doctor.UD_DispFont="large" OM_Profile.5. Doctor .UD_DispColor="black" OM_Profile.6.Nurse.UD_DispLang="en" OM_Profile.6.Nurse.UD_DispFont="normal" OM_Profile.6.Nurse.UD_DispColor="business"

Parameter / Parameter group	**Coa profile 1 … 20 delete**
Description	Deletion of a profile.
Format	n.a.
Range	n.a.
Default value	n.a.
Web	n.a.
OMM configuration files	n.a.
DECT Phone	n.a.
User configuration files	Supported in the *user_common.cfg* configuration file: OM_Profile.<no>.Delete=yes Where <no> is the number of the profile to be deleted.

Please note: A complete removal of the numbered profile from user_common.cfg does not remove the profile in the OMM database. It must be explicitly deleted in the OMM database.
Note further that the settings in the DECT phone might stay set until the next master reset of the DECT phone or each setting has been overwritten by other related settings.

23.5 USER-SPECIFIC COA CONFIGURATION

See section 18.1.2 for user-specific CoA configurations and information on assigning a profile to users.

23.6 STATES OF COA CONFIGURATION SETTINGS

The configuration state of CoA settings are listed in the WEB service.

Parameter / Parameter group	**DECT phone CoA capability**
Description	CoA capability state of the DECT phone.
Format	n.a.
Range	n.a.
Default value	n.a.
Web	Basic: SIP User/Devices > 🔍 > Capability ”CoA profile” Yes = DECT phone supports CoA No = DECT phone does not support CoA
OMM configuration files	n.a.
DECT Phone	n.a.
User configuration files	n.a.

Parameter / Parameter group	**Default CoA data loaded**
Description	State of the default CoA profile to be sent to the DECT phone
Format	n.a.
Range	n.a.
Default value	n.a.
Web	Basic: SIP User/Devices > 🔍 > Default CoA profile loaded Yes = a default profile was sent No = no default profile was sent
OMM configuration files	n.a.
DECT Phone	n.a.
User configuration files	n.a.

Parameter / Parameter group	**CoA data loaded**
Description	State of the user COA data sent to the DECT phone.
Format	n.a.
Range	n.a.
Default value	n.a.
Web	Basic: SIP User/Devices > 🔍 > CoA data loaded Yes = data has been sent No = no data sent
OMM configuration files	n.a.
DECT Phone	n.a.
User configuration files	n.a.

Parameter / Parameter group	**CoA profile usage**
Description	States the CoA profile ID to be loaded for the user.
Format	n.a.
Range	n.a.
Default value	n.a.
Web	Basic: SIP User/Devices > 🔍 > Use CoA profile ID of the CoA profile to be loaded for the user.
OMM configuration files	n.a.
DECT Phone	n.a.
User configuration files	n.a.

23.7 COA CONFIGURATION PARAMETERS

In addition to the information provided in this section above, the following sections provide examples of CoA configuration files, and an overview of all supported parameters.

23.7.1 CONFIGURATION OF VARIABLE LISTS

A *variable list* includes a number of *list items*, each of which can be executed in the usual way by selecting it. A list item consists of an item index (1..10) and either a number (to be dialed) or a function/feature that is supported by the handset. Other attributes of a list item are optional.

Item-Attribute	***Type***	***Description***	***Example***
Index	decimal number	index of list item (1..10)	7
Number	quoted UTF8-string	'number' to dial	"#12#777#"
Name	quoted UTF8-string	displayed text of item	"My Voice Box"
FunctionID	function-ID-string	function/feature to execute	pbx_directory
ShortName/Icon	quoted UTF8-string	displayed short name and/or icon	"\xEE808B VB"
Handsfree	Boolean (0 or 1)	dial in hands-free-mode	1
VisibleSpecifier	4-digit-string of '0' or '1'	item visible in idle-, dial-, alerting- and active-state	1000

There are 2 variable lists available, and each can hold up to 10 list items.

To configure an item for one of the lists the command key ***UD_VListEntry*** is used. The first value specifies the index (1 or 2) of the considered list, followed by the above mentioned attributes in the given order.

Always remember that the different values/attributes must be separated by whitespace and their positions in the configuration command are fixed. Unused attributes must be indicated by empty strings if they are followed by nonempty attributes, unused attributes (empty strings) can be omitted at the end of the configuration command.

Examples:

```
UD_VListEntry = 1 1  "#12#777#"      "My Voice Box"  ""   "VB"           1
UD_VListEntry = 1 2  "043116967777"  "Alice"
UD_VListEntry = 1 3  "043116968888"  "Bob\'s Phone"  ""   "BP \xEE808B"
UD_VListEntry = 2 1  ""              "App 5"         f_5  "A5"           ""  1000
```

Additionally a variable list can hold a name and/or short name used for representing it in another list or near a programmed soft key or side key. Again, the 'short name' attribute allows specifying an icon as well. A third attribute, 'sub item', determines whether or not a selected list item is to be displayed with sub item (sub key line).

List-Attribute	*Type*	*Description*	*Example*
Name	quoted UTF8-string	displayed text of list	“My Own Menu”
ShortName/Icon	quoted UTF8-string	displayed short name and/or icon	“\xEE808B M1”
SubItems	Boolean (0 or 1)	show sub key line of selected item	1

Again, the corresponding configuration commands take the list index (1 or 2) as first value.

Examples:

```
UD_VListName      = 1 "My Own Menu"
UD_VListShortName = 1 "\xEE808B M1"
UD_VListSubItems  = 1 1
```

23.7.2 EXTENDED COA EXAMPLES

23.7.3 EXAMPLE 1

```
UD_ConfigurationName="Umlaute (UTF-8): äöüÄÖÜß, Escape-Sequenzen: ' \" \\ \r \n \t \f,
andere UTF-8-Zeichen: µ ® €"


# display-settings
UD_DispLang=en
UD_DispFont=large
UD_DispColor=black

# ringer-settings
UD_RingerVolumeIntern=level_1
UD_RingerVolumeExtern=level_2
UD_RingerMelodyIntern=classical_1
UD_RingerMelodyExtern=pippi_longstocking

# ausblenden/sperren von features
UD_FunctionMenuHide=active_features true
UD_FunctionMenuHide=prog_x true
UD_FunctionUserProtected=system_x true

# programmieren von tasten (idle-zustand)
UD_KeyAssignmentIdle=side1 voice_box
UD_KeyAssignmentIdle=ok MenuInfNew
UD_KeyAssignmentIdle=long.esc inf
UD_KeyAssignmentIdle=esc pbx_directory
UD_KeyAssignmentIdle=long.esc directories
```

23.7.4 EXAMPLE 2

```
UD_ConfigurationName = "omm-test"   # dies definiert den namen des coa-files (versys)

### message options
UD_MessageMelodyNormal = basic_1
UD_MessageMelodyUrgent = basic_2
UD_MessageMelodyAlarm = basic_3

UD_MessageVolumeNormal = level_1
UD_MessageVolumeUrgent = level_2
UD_MessageVolumeAlarm = level_3

UD_MessageOverwrite = true

### ringer melody options
UD_RingerMelodyIntern = butterfly
UD_RingerMelodyExtern = barock
UD_RingerMelodyUnknown = ballade
UD_RingerMelodyCallback = fancy
UD_RingerMelodyRecall = comelody
UD_RingerMelodyVip = easy_groove
UD_RingerMelodySpecial = happy_fair
UD_RingerMelodyAlarm = kitafun
UD_RingerMelodyAppointment = latin_dance

### ringer volume options
UD_RingerVolumeIntern = off
UD_RingerVolumeExtern = increasing
UD_RingerVolumeUnknown = level_1
UD_RingerVolumeCallback = level_2
UD_RingerVolumeRecall = level_3
UD_RingerVolumeVip = level_4
UD_RingerVolumeSpecial = level_5
UD_RingerVolumeAlarm = level_6
UD_RingerVolumeAppointment = level_7

### ringer settings
UD_RingMode = repeat
UD_RingBuzz = true
UD_RingVibra = true
UD_RingHeadset = false
```

```
### attention tones
UD_ToneKey = inactive active
UD_ToneCnf = active
UD_ToneMnend = active no_speaker
UD_ToneAccu = active vibra
UD_ToneRange = inactive active no_speaker vibra
UD_ToneOutrange = inactive

### audio
UD_AudioNoisedetect = true
UD_AudioLoudenv = false
UD_AudioSpkCharger = handsfree

### Systems/Subscription/<System X>
UD_DialCharset = ABC_123
UD_DialCodeImax = 3
UD_DialCodeSys = "6"

### display
UD_DispLang=en
UD_DispFont=large
UD_DispColor=black

### illumination
UD_LightDim = 2h
UD_LightDisp = 2m
UD_LightKey = 45s
UD_LightKeyoptIncom = true
UD_LightKeyoptAlarm = false
UD_LightKeyoptCharge = false
UD_LightCharge = 60s
UD_LightCall = 30s
UD_LightMsgMsg = 10s
UD_LightMsgInf = 20s
UD_LightMsgJob = 30s
UD_LightMsgSos = 60s

### led indications
UD_LedAlive = true
UD_LedIncom = true
UD_LedRange = false
```

```
UD_LedCharge = true
UD_LedInfo = false
UD_LedSpk = true
UD_LedAutoans = false
UD_LedAppoint = false
UD_LedAlarm = false

### list access
UD_ListmodeRedial = pbx
UD_ListmodeCaller = pbx
UD_ListmodeFilter = block_list

### device options
UD_ModeSilentcharge = true
UD_ModeChargeranswr = false
UD_ModeAutoanswr = true
UD_ModeAutoquickhook = false
UD_ModeKey = oem

### phone lock
UD_LockKeyAuto = true
UD_LockKeyTime = 30s
UD_LockKeyPin = true
UD_LockPin = "1234"
UD_LockAdmin = "4711"

### SOS call
UD_SosNum = "4711"
UD_SosMelody = weekend
UD_SosVolume = increasing
UD_SosHandsfree = true

### alarm sensor
UD_SosMdNumber = "0815"
UD_SosMdAutoanswr = true
UD_SosMdModePre = false
UD_SosMdModeDown = true
UD_SosMdModeNomove = true
UD_SosMdModeEsc = false
UD_SosMdModeRep = false
UD_SosMdSenseAngle = flat
UD_SosMdSenseMove = high
```

```
UD_SosMdSenseEsc = medium
UD_SosMdNomoDown = conversation system_menu local_menu
UD_SosMdNomoNomove = conversation
UD_SosMdNomoEsc = idle conversation system_menu local_menu
UD_SosMdDelayDown = 20s
UD_SosMdDelayNomove = 30s
UD_SosMdDelayEsc = 45s
UD_SosMdTimePre = 30s
UD_SosMdTimeRep = 60s
UD_SosMdTone = true
UD_SosMdVibra = false

### function/feature access
UD_FunctionMenuHide=active_features true
UD_FunctionMenuHide=prog_x TRUE
UD_FunctionLocked=time_x true
UD_FunctionUserProtected=system_x true
UD_FunctionUserProtected=dir_x true
UD_FunctionAdminProtected=system_x true
UD_FunctionGrayed=system_x true

### assignment of keys
UD_KeyAssignmentIdle=side1 caller
UD_KeyAssignmentIdle=ok MenuInfNew
UD_KeyAssignmentIdle=long.ok inf
UD_KeyAssignmentIdle=esc pbx_directory
UD_KeyAssignmentIdle=long.esc directories

UD_KeyAssignmentActive=esc nop
```

23.7.5 EXAMPLE 3

```
UD_ConfigurationName = "omm-test"   # dies definiert den namen des coa-files (versys)

### function/feature access
UD_FunctionMenuHide = scheme true
UD_FunctionLocked = scheme true
UD_FunctionGrayed = scheme true
UD_FunctionUserProtected = scheme true
UD_FunctionAdminProtected = scheme true
```

23.7.6 EXAMPLE 4

```
#UD_ConfigurationName = "omm-test"   # dies definiert den namen des coa-files (versys)
```

```
### assignment of keys
#UD_KeyAssignmentIdle=side1 sos_loc
#UD_KeyAssignmentIdle=side2 shock
#UD_KeyAssignmentIdle=side3 sensor_menu

#UD_KeyAssignmentIdleMaster=side1 sos_loc
#UD_KeyAssignmentIdleMaster=side2 shock
#UD_KeyAssignmentIdleMaster=side3 sensor_menu

UD_KeyAssignmentIdle=down gappp_directory

UD_ConfigurationName=  jwede-1
UD_DispFont=           normal
UD_DispColor=          black

UD_KeyAssignmentIdle=side1 vlst1
UD_KeyAssignmentActive=side1 vlst2

UD_VListEntry = 1 1 "*8010" "Unpark 10" "" "" ""
UD_VListEntry = 1 2 "80*11" "Unpark 11" "" "" ""

UD_VListName = 1 "Unpark call"
UD_VListShortName = 1 "\xEE8296"
UD_VListSubItems = 1 0

UD_VListEntry = 2 1 "#58110" "Park 10" "" "" ""
UD_VListEntry = 2 2 "58#111" "Park 11" "" "" ""

UD_VListName = 2 "Park call"
UD_VListShortName = 2 "\xEE8296"
UD_VListSubItems = 2 0

### var-lists
#UD_VListName      = 1 "Extra-Menü 1"
#UD_VListName      = 2 "Extra-Menü 2"
#UD_VListShortName = 2 \xEE808B
#UD_VListSubItems  = 2 1

### var-list entries
# parameters:  list  item   number-to-dial          name          fkt
shortname/icon    handsfree    visible(idle,dial,alert,active)
```

```
#              1..2  1..10  quoted-string          quoted-string  string   quoted-string
0..1         4-digit-string-of(0,1)
#UD_VListEntry= 1     9      "*7*<no>#"             "Kröger's"     f_1      "«nam»
\xEE808B"
#UD_VListEntry= 2     2      "043116962222<ln=4>"   "xx\\yy"       f_5      "nam2"
""           1000
#UD_VListEntry= 1     3      "043116967777<<>"      "xx\"yy"       inf
"\238\128\139"
#UD_VListEntry= 1     7      "043116960000"         "xx\'yy"       ""       "$ €
\xEE808B"


## max=20 30
## mul=11 3
## substr = 1001 1 1
## xxx = bbb


# in strings: so soll es sein:
#  cfg       ->  lua
# "xx\\yy"   -> 'xx\\yy'
# "xx\'yy"   -> 'xx\'yy'  (auch: "xx'yy" -> 'xx\'yy')
# "xx\"yy"   -> 'xx"yy'
# "xx\ryy"   -> 'xx\ryy'
# "xx\nyy"   -> 'xx\nyy'
# "xx\tyy"   -> 'xx\tyy'
# "xx\fyy"   -> 'xx\fyy'
# "xx\234yy" -> 'xx\234yy'


# icons:
# "xx\x01yy" -> 'xxyy'
#   :
# "xx\x1fyy" -> 'xxyy'
# "xx\xee808byy" -> 'xx□yy'
```

23.7.7 EXAMPLE 5

```
#UD_ConfigurationName = "omm-test"   # dies definiert den namen des coa-files (versys)


### assignment of keys
UD_KeyAssignmentIdle=side1 sos_loc
UD_KeyAssignmentIdle=side2 shock
UD_KeyAssignmentIdle=side3 sensor_menu

UD_KeyAssignmentIdleMaster=side1 sos_loc
UD_KeyAssignmentIdleMaster=side2 shock
UD_KeyAssignmentIdleMaster=side3 sensor_menu
```

```
UD_KeyAssignmentActiveSos=red nop
UD_KeyAssignmentActiveSos=d0 dial_0
UD_KeyAssignmentActiveSos=d1 dial_1
UD_KeyAssignmentActiveSos=d2 dial_2
UD_KeyAssignmentActiveSos=d3 dial_3
UD_KeyAssignmentActiveSos=d4 dial_4
UD_KeyAssignmentActiveSos=d5 dial_5
UD_KeyAssignmentActiveSos=d6 dial_6
UD_KeyAssignmentActiveSos=d7 dial_7
UD_KeyAssignmentActiveSos=d8 dial_8
UD_KeyAssignmentActiveSos=d9 dial_9
UD_KeyAssignmentActiveSos=star dial_star
UD_KeyAssignmentActiveSos=hash dial_hash

UD_KeyAssignmentActiveSosMaster=red nop
```

23.7.8 SUPPORTED COA PARAMETERS

The following keys and values are supported in the CoA configuration files.

```
     used in configuration commands: <key> = <value> [ <value> ]
// KEY_xxx   key
// VAL_xxx   value

   "UD_ConfigurationName"   // <string>

// message melody options
   "UD_MessageMelodyNormal"     // VAL_MELODY_xxx
   "UD_MessageMelodyUrgent"     // VAL_MELODY_xxx
   "UD_MessageMelodyAlarm"      // VAL_MELODY_xxx

// message volume options
   "UD_MessageVolumeNormal"     // VAL_VOLUME_xxx
   "UD_MessageVolumeUrgent"     // VAL_VOLUME_xxx
   "UD_MessageVolumeAlarm"      // VAL_VOLUME_xxx

// message overwrite
   "UD_MessageOverwrite"        // true/false

// ringer melody options
   "UD_RingerMelodyIntern"      // VAL_MELODY_xxx
   "UD_RingerMelodyExtern"      // VAL_MELODY_xxx
```

```
    "UD_RingerMelodyUnknown"     // VAL_MELODY_xxx
    "UD_RingerMelodyCallback"    // VAL_MELODY_xxx
    "UD_RingerMelodyRecall"      // VAL_MELODY_xxx
    "UD_RingerMelodyVip"         // VAL_MELODY_xxx
    "UD_RingerMelodySpecial"     // VAL_MELODY_xxx
    "UD_RingerMelodyAlarm"       // VAL_MELODY_xxx
    "UD_RingerMelodyAppointment" // VAL_MELODY_xxx

// ringer volume options
    "UD_RingerVolumeIntern"      // VAL_VOLUME_xxx
    "UD_RingerVolumeExtern"      // VAL_VOLUME_xxx
    "UD_RingerVolumeUnknown"     // VAL_VOLUME_xxx
    "UD_RingerVolumeCallback"    // VAL_VOLUME_xxx
    "UD_RingerVolumeRecall"      // VAL_VOLUME_xxx
    "UD_RingerVolumeVip"         // VAL_VOLUME_xxx
    "UD_RingerVolumeSpecial"     // VAL_VOLUME_xxx
    "UD_RingerVolumeAlarm"       // VAL_VOLUME_xxx
    "UD_RingerVolumeAppointment" // VAL_VOLUME_xxx

// melodies
    "weekend"            // Weekend
    "butterfly"          // Butterfly
    "barock"             // Barock
    "ballade"            // Ballade
    "fancy"              // Fancy
    "comelody"           // Comelody
    "easy_groove"        // Easy groove
    "happy_fair"         // Happy fair
    "kitafun"            // Kitafun
    "latin_dance"        // Latin dance
    "little_asia"        // Little asia
    "mango_selassi"      // Mango selassi
    "parka"              // Parka
    "remember"           // Remember
    "rocky_lane"         // Rocky lane
    "ringing_1"          // Ringing 1
    "ringing_2"          // Ringing 2
    "ringing_3"          // Ringing 3
    "ringing_4"          // Ringing 4
    "ringing_5"          // Ringing 5
    "ringing_6"          // Ringing 6
    "ringing_7"          // Ringing 7
```

```
"ring_vintage"       // Ring vintage
"vibes"              // Vibes
"attack"             // Attack
"doorbell"           // Doorbell
"boogie"             // Boogie
"polka"              // Polka
"classical_1"        // Classical 1
"classical_2"        // Classical 2
"classical_3"        // Classical 3
"classical_4"        // Classical 4
"alla_turca"         // Alla turca
"entertainer"        // Entertainer
"jollygood"          // Jollygood
"in_the_saints"      // In the saints
"drunken_sailor"     // Drunken sailor
"mary_had"           // Mary had
"shell_be_walking"   // Shell be walking
"pippi_longstocking" // Pippi longstocking
"policehorn"         // Policehorn
"synthesizer"        // Synthesizer
"after_work"         // After work
"beep"               // Beep
"basic_1"            // Basic 1
"basic_2"            // Basic 2
"basic_3"            // Basic 3
"basic_4"            // Basic 4
"basic_5"            // Basic 5
"basic_6"            // Basic 6
"basic_7"            // Basic 7
"basic_8"            // Basic 8
"alarm_1"            // Alarm 1
"alarm_2"            // Alarm 2
"alarm_3"            // Alarm 3
"alarm_4"            // Alarm 4
"alarm_5"            // Alarm 5
"alarm_6"            // Alarm 6
"alarm_7"            // Alarm 7
"6700_one"           // 6700 One
"6700_two"           // 6700 Two
"6700_three"         // 6700 Three
"6700_four"          // 6700 Four
"6700_five"          // 6700 Five
```

```
   "1_attention_tone"   // 1 Attention tone
   "2_attention_tones"  // 2 Attention tones
   "3_attention_tones"  // 3 Attention tones
   "4_attention_tones"  // 4 Attention tones
   "5_attention_tones"  // 5 Attention tones
   "6_attention_tones"  // 6 Attention tones
   "7_attention_tones"  // 7 Attention tones
   "8_attention_tones"  // 8 Attention tones
   "9_attention_tones"  // 9 Attention tones
   "10_attention_tones" // 10 Attention tones

// volumes
   "off"                // off
   "increasing"         // increasing
   "level_1"            // Level-1
   "level_2"            // Level-2
   "level_3"            // Level-3
   "level_4"            // Level-4
   "level_5"            // Level-5
   "level_6"            // Level-6
   "level_7"            // Level-7

// ringer settings
   "UD_RingMode"    // VAL_RING_MODE_xxx
   "UD_RingBuzz"    // true/false
   "UD_RingVibra"   // true/false
   "UD_RingHeadset" // true/false

   "repeat"             // repeat
   "once"               // once

// attention tones
   "UD_ToneKey"      // VAL_TONE_xxx (up to 3 values)
   "UD_ToneCnf"      // VAL_TONE_xxx (up to 3 values)
   "UD_ToneMnend"    // VAL_TONE_xxx (up to 3 values)
   "UD_ToneAccu"     // VAL_TONE_xxx (up to 3 values)
   "UD_ToneRange"    // VAL_TONE_xxx (up to 3 values)
   "UD_ToneOutrange" // VAL_TONE_xxx (up to 3 values)

   "inactive"           // inactive
   "active"             // active
   "no_speaker"         // without Loudspeaker
```

```
      "vibra"              // Vibration

   // audio
      "UD_AudioNoisedetect" // true/false
      "UD_AudioLoudenv"     // true/false
      "UD_AudioSpkCharger"  // VAL_AUDIO_SPK_CHARGER_xxx

      "release"            // Release
      "handsfree"          // Handsfree

   // Systems/Subscription/<System X>
      "UD_DialCharset"    // VAL_DIAL_ABC_xxx
      "UD_DialCodeImax"   // VAL_DIAL_CODE_IMAX_xxx
      "UD_DialCodeSys"    // <digit-string>

      "123_"               // 123...
      "ABC_123"            // ABC...123
      "123_ABC_äöü"        // 123...ABC...äöü
      "ABC_äöü_123"        // ABC...äöü...123
      "123_ABC"            // 123...ABC

      "automatic"          // automatic
      "1"                  // 1
      "2"                  // 2
      "3"                  // 3
      "4"                  // 4
      "5"                  // 5
      "6"                  // 6
      "7"                  // 7
      "8"                  // 8

   // display
      "UD_DispLang"   // VAL_DISP_LANG_xxx
      "UD_DispFont"   // VAL_DISP_FONT_xxx
      "UD_DispColor"  // VAL_DISP_COLOR_xxx

      "default"            // default
      "de"                 // D - Deutsch
      "en"                 // GB - English
      "fr"                 // FR - Français
      "es"                 // ES - Español
      "it"                 // I - Italiano
```

```
    "nl"                // NL - Nederlands
    "sv"                // S - Svenska
    "da"                // DK - Dansk
    "pt"                // P - Português
    "no"                // N - Norsk
    "cs"                // Cz - Cesky
    "sk"                // SK - Sloven\u010dina - Slovensky
    "fi"                // Su - Suomi
    "hu"                // H - Magyar - Hungarian
    "ru"                // RU - \u0420\u0443\u0441\u0441\u043a\u0438\u0439 - Russian
    "tr"                // TURK - Türkçe
    "pl"                // PL - Polski
    "et"                // EST - Esti

    "small"             // Small
    "normal"            // Normal
    "large"             // Large

    "gray"              // Gray
    "black"             // Black
    "business"          // Business
    "future"            // Future
    "plain"             // Plain
    "sweet"             // Sweet

// illumination
    "UD_LightDim"           // VAL_LIGHT_DIM_xxx
    "UD_LightDisp"          // VAL_LIGHT_DISP_xxx
    "UD_LightKey"           // VAL_LIGHT_KEY_xxx
    "UD_LightKeyoptIncom"   // true/false
    "UD_LightKeyoptAlarm"   // true/false
    "UD_LightKeyoptCharge"  // true/false
    "UD_LightCharge"        // VAL_LIGHT_CHARGE_xxx
    "UD_LightCall"          // VAL_LIGHT_CALL_xxx
    "UD_LightMsgMsg"        // VAL_LIGHT_MSG_MSG_xxx
    "UD_LightMsgInf"        // VAL_LIGHT_MSG_INF_xxx
    "UD_LightMsgJob"        // VAL_LIGHT_MSG_JOB_xxx
    "UD_LightMsgSos"        // VAL_LIGHT_MSG_SOS_xxx

    "off"               // off
    "1m"                // 1 min
    "10m"               // 10 min
```

```
"1h"                // 60 min
"2h"                // 120 min
"4h"                // 240 min
"10h"               // 600 min
"on"                // on

"10s"               // 10 sec
"20s"               // 20 sec
"30s"               // 30 sec
"45s"               // 45 sec
"60s"               // 60 sec
"2m"                // 120 sec
"4m"                // 240 sec

"off"               // off
"1s"                // 1 sec
"3s"                // 3 sec
"5s"                // 5 sec
"10s"               // 10 sec
"20s"               // 20 sec
"30s"               // 30 sec
"45s"               // 45 sec
"60s"               // 60 sec
"2m"                // 120 sec
"4m"                // 240 sec

"off"               // off
"1s"                // 1 sec
"3s"                // 3 sec
"5s"                // 5 sec
"10s"               // 10 sec
"20s"               // 20 sec
"30s"               // 30 sec
"45s"               // 45 sec
"60s"               // 60 sec
"2m"                // 120 sec
"4m"                // 240 sec

"off"               // off
"1s"                // 1 sec
"3s"                // 3 sec
"5s"                // 5 sec
```

```
"10s"               // 10 sec
"20s"               // 20 sec
"30s"               // 30 sec
"45s"               // 45 sec
"60s"               // 60 sec
"2m"                // 120 sec
"3m"                // 180 sec
"4m"                // 240 sec
"on"                // on

"nochange"          // No change
"dimmed"            // Light dimmed
"5s"                // 5 sec
"10s"               // 10 sec
"20s"               // 20 sec
"30s"               // 30 sec
"45s"               // 45 sec
"60s"               // 60 sec
"2m"                // 120 sec
"4m"                // 240 sec

"nochange"          // No change
"dimmed"            // Light dimmed
"5s"                // 5 sec
"10s"               // 10 sec
"20s"               // 20 sec
"30s"               // 30 sec
"45s"               // 45 sec
"60s"               // 60 sec
"2m"                // 120 sec
"4m"                // 240 sec

"nochange"          // No change
"dimmed"            // Light dimmed
"5s"                // 5 sec
"10s"               // 10 sec
"20s"               // 20 sec
"30s"               // 30 sec
"45s"               // 45 sec
"60s"               // 60 sec
"2m"                // 120 sec
"4m"                // 240 sec
```

```
   "dimmed"             // Light dimmed
   "30s"                // 30 sec
   "60s"                // 60 sec
   "2m"                 // 120 sec
   "3m"                 // 180 sec
   "4m"                 // 240 sec
   "5m"                 // 300 sec

// led indications
   "UD_LedAlive"           // true/false
   "UD_LedIncom"           // true/false
   "UD_LedRange"           // true/false
   "UD_LedCharge"          // true/false
   "UD_LedInfo"            // true/false
   "UD_LedSpk"             // true/false
   "UD_LedAppoint"         // true/false
   "UD_LedAlarm"           // true/false

// list access
   "UD_ListmodeRedial"   // VAL_LISTMODE_REDIAL_xxx
   "UD_ListmodeCaller"   // VAL_LISTMODE_CALLER_xxx
   "UD_ListmodeFilter"   // VAL_LISTMODE_FILTER_xxx

   "local"              // local
   "automatic"          // automatic
   "pbx"                // PBX

   "local"              // local
   "automatic"          // automatic
   "pbx"                // PBX

   "accept_list"        // Accept list
   "block_list"         // Block list
   "filter_off"         // Filter off

// device options
   "UD_ModeSilentcharge"   // true/false
   "UD_ModeChargeranswr"   // true/false
   "UD_ModeAutoanswr"      // true/false
   "UD_ModeAutoquickhook"  // true/false
   "UD_ModeKey"            // VAL_MODE_KEY_xxx
```

```
   "emo"               // Esc  >>>  Ok
   "oem"               // Ok  Esc  >>>
   "eom"               // Esc  Ok  >>>
   "meo"               // >>>  Esc  Ok
   "EMO"               // Esc  Menu Ok
   "OEM"               // Ok  Esc Menu
   "EOM"               // Esc  Ok Menu
   "MEO"               // Menu Esc  Ok

// phone lock
   "UD_LockKeyAuto"        // true/false
   "UD_LockKeyTime"        // VAL_LOCK_KEY_T_xxx
   "UD_LockKeyPin"         // true/false
   "UD_LockPin"            // <digit-string>
   "UD_LockAdmin"          // <digit-string>

   "5s"                // 5 sec
   "10s"               // 10 sec
   "20s"               // 20 sec
   "30s"               // 30 sec
   "40s"               // 40 sec
   "50s"               // 50 sec
   "60s"               // 60 sec
   "90s"               // 90 sec
   "120s"              // 120 sec

// SOS call
   "UD_SosNum"          // <digit-string>
   "UD_SosMelody"       // VAL_MELODY_xxx
   "UD_SosVolume"       // VAL_VOLUME_xxx
   "UD_SosHandsfree"    // true/false

// alarm sensor
   "UD_SosMdNumber"       // <digit-string>
   "UD_SosMdAutoanswr"    // true/false
   "UD_SosMdModePre"      // true/false
   "UD_SosMdModeDown"     // true/false
   "UD_SosMdModeNomove"   // true/false
   "UD_SosMdModeEsc"      // true/false
   "UD_SosMdModeRep"      // true/false
   "UD_SosMdSenseAngle"   // VAL_SOSMD_SENSE_ANGLE_xxx
```

```
"UD_SosMdSenseMove"    // VAL_SOSMD_SENSE_MOVE_xxx
"UD_SosMdSenseEsc"     // VAL_SOSMD_SENSE_ESC_xxx
"UD_SosMdNomoDown"     // VAL_SOSMD_NOMO_xxx (up to 4 values)
"UD_SosMdNomoNomove"   // VAL_SOSMD_NOMO_xxx (up to 4 values)
"UD_SosMdNomoEsc"      // VAL_SOSMD_NOMO_xxx (up to 4 values)
"UD_SosMdDelayDown"    // VAL_SOSMD_DELAY_DOWN_xxx
"UD_SosMdDelayNomove"  // VAL_SOSMD_DELAY_NOMOVE_xxx
"UD_SosMdDelayEsc"     // VAL_SOSMD_DELAY_ESC_xxx
"UD_SosMdTimePre"      // VAL_SOSMD_T_PRE_xxx
"UD_SosMdTimeRep"      // VAL_SOSMD_T_REP_xxx
"UD_SosMdTone"         // true/false
"UD_SosMdVibra"        // true/false

"steep"              // Steep
"medium"             // Medium
"flat"               // Flat

"low"                // Low
"medium"             // Medium
"high"               // High

"low"                // Low
"medium"             // Medium
"high"               // High

"idle"               // in idle
"conversation"       // during conversation
"local_menu"         // in local menu
"system_menu"        // in system menu

"1s"                 // 1 sec
"2s"                 // 2 sec
"5s"                 // 5 sec
"10s"                // 10 sec
"20s"                // 20 sec
"30s"                // 30 sec
"45s"                // 45 sec
"60s"                // 60 sec
"75s"                // 75 sec

"10s"                // 10 sec
"20s"                // 20 sec
```

```
   "30s"                // 30 sec
   "45s"                // 45 sec
   "60s"                // 60 sec
   "75s"                // 75 sec

   "1s"                 // 1 sec
   "2s"                 // 2 sec
   "5s"                 // 5 sec
   "10s"                // 10 sec
   "20s"                // 20 sec
   "30s"                // 30 sec
   "45s"                // 45 sec
   "60s"                // 60 sec
   "75s"                // 75 sec

   "10s"                // 10 sec
   "20s"                // 20 sec
   "30s"                // 30 sec
   "45s"                // 45 sec
   "60s"                // 60 sec
   "75s"                // 75 sec

   "5s"                 // 5 sec
   "10s"                // 10 sec
   "20s"                // 20 sec
   "30s"                // 30 sec
   "45s"                // 45 sec
   "60s"                // 60 sec
   "75s"                // 75 sec
   "120s"               // 120 sec
   "240s"               // 240 sec

// function/feature access
   "UD_FunctionMenuHide"       // VAL_FUNCTION_xxx and true/false
   "UD_FunctionLocked"         // VAL_FUNCTION_xxx and true/false
   "UD_FunctionGrayed"         // VAL_FUNCTION_xxx and true/false
   "UD_FunctionUserProtected"  // VAL_FUNCTION_xxx and true/false
   "UD_FunctionAdminProtected" // VAL_FUNCTION_xxx and true/false

// functions/features available on device
   "pbx_unpark"         // <<< Unpark call(*)
   "pbx_park"           // <<< Pickup/Park(*)
```

```
"gappp_pickup"       // <<< Pickup call(*)
"pbx_take"           // <<< Take call(*)
"gappp_call_forward" // <<< Call diversion(*)
"pbx_call_routing"   // <<< Call routing(*)
"gappp_pickup_select" // Pickup select
"gappp_announcement" // Announcement
"gappp_intercom"     // Intercom
"gappp_vip_call"     // VIP call
"inf"                // >>> Info (menu item only)
"caller"             // Caller list
"redial"             // Redial list
"box_x"              // >>> Voice box
"box_set_x"          // Voice box settings
"voice_box_menu"     // Settings/Voice mail(*)
"active_features"    // >>> Active features
"msg_x"              // >>> Text message / Jobs / Mails(*)
"omm_def_msg"        // Pre-defined messages
"msg_opt_x"          // Message options
"mel_msg_x"          // Melodies
"mel_msg"            // Normal message
"mel_msgurg"         // Urgent message
"mel_msgsos"         // Alarm  message
"vol_msg_x"          // Volume
"vol_msg"            // Normal message
"vol_msgurg"         // Urgent message
"vol_msgsos"         // Alarm  message
"msg_pop"            // Popup
"msg_ovwr"           // Overwrite
"msg_del"            // Delete/Delete all
"directory_x"        // >>> Directories
"vip"                // VIP list
"vip_x"              // Edit/Add VIP list entry
"dir_x"              // Personal directory
"book_x"             // Edit/Add personal directory entry
"quick_x"            // Quick call
"add_to"             // Add to...(VIP/Filter/Personal/Central directory)
"pbx_directory"      // Central directory(*)
"time_x"             // >>> Time functions
"alarm_x"            // Alarm clock 1...3
"appointment_x"      // Appointment 1...3
"tea_timer"          // Timer
"audio_x"            // >>> Audio
```

```
"volume_menu"        // Volume settings
"tone_menu"          // Attention tones
"tone_key"           // Key click
"tone_cnf"           // Confirm tones
"tone_end"           // End of menu
"tone_bat"           // Battery warning
"tone_charger"       // Charger beep
"tone_cov"           // Coverage warning
"tone_range"         // Out of range
"tone_wait"          // Call waiting
"tone_sensor"        // Pre alarm (63x only)
"load_environment"   // Loud environment
"audio_hd"           // Audio quality (only 650)
"ring_x"             // >>> Ringing
"ring_mel_x"         // Ringer melodies
"mel_int"            // Internal call
"mel_ext"            // External call
"mel_unk"            // Unknown number
"mel_nym"            // Anonymous
"mel_ccbs"           // Callback
"mel_recall"         // Recall
"mel_vip"            // VIP call
"mel_special"        // Special call
"mel_sos"            // Emergency call
"mel_alarm"          // Alarm
"mel_app"            // Appointment
"ring_volume"        // Ringer volume
"vol_int"            // Internal call
"vol_ext"            // External call
"vol_unk"            // Unknown number
"vol_nym"            // Anonymous
"vol_ccbs"           // Callback
"vol_recall"         // Recall
"vol_vip"            // VIP call
"vol_special"        // Special call
"vol_sos"            // Emergency call
"vol_alarm"          // Alarm
"vol_app"            // Appointment
"ring_type_x"        // Ringer type
"play_once"          // Play melody once on/off
"silent_charging"    // Silent charging
"noise_detection"    // Noise detection on/off
```

```
"ring_device_x"      // Ringer device
"ring_off"           // Ringer/Buzzer on/off
"ring_hs"            // Corded headset-ring on/off
"ring_vibra"         // Vibrator-ring on/off
"datamanagment"      // >>> Data management / SD Card
"filter_xx"          // >>> Call filter
"filter_x"           // Edit call filter
"system_x"           // >>> System/Subscription
"start_enrol"        // <New system>
"subs_auto"          // Auto search
"subs_sel"           // Select subscription
"subs_stop"          // Stop searching
"subs_opt"           // >Edit subscription
"no_plan"            // Number plan
"ehs_x"              // >>> Enhanced security
"bt_x"               // >>> Bluetooth (only 62x/63x/65x)
"bt_edit_x"          // >Edit Bluetooth
"set_xx"             // >>> User settings
"prog_x"             // Key programming
"disp_x"             // Display settings
"language"           // Language
"font"               // Font settings
"color"              // Color schemes
"scheme"             // Menu structure
"pic_x"              // Idle picture
"illu_x"             // Illumination/Light
"disp_dim"           // Display dimming
"disp_light"         // Display
"disp_key"           // Keyboard
"disp_charger"       // Charger
"disp_call"          // Conversation
"disp_inf"           // Info message
"disp_msg"           // Text message
"disp_job1"          // Job
"disp_sos"           // SOS alarm
"disp_led"           // LED indications
"led_alife"          // Life indication
"led_incom"          // Incoming call
"led_range"          // Out of range
"led_charge"         // Charge indication
"led_inf"            // Infos
"led_spk"            // Handsfree
```

```
"led_app"           // Appointment
"led_alarm"         // Alarm
"list_settings"     // List access
"device_opt"        // Device options
"security_x"        // >>> Security
"lock_x"            // >>> Lock
"keylock"           // Key lock
"pinlock"           // Phone lock
"change_pin"        // Change PIN
"sos_x"             // >>> SOS call
"tms_x"             // >>> Alarm sensor (63x only)
"set_pre_alarm"     // Pre alarm
"set_mandown"       // Mandown
"set_no_move"       // No movement alarm
"set_shock"         // Shock alarm
"set_rep_alarm"     // Repeate alarm
"tms_opt_x"         // >Sensor options
"rst_x"             // >>> Reset to default
"off_menu"          // >>> Off menu
"off"               // Power off
"menu"              // Menu
"ring_toggle"       // Ringer/Buzzer on/off
"profile_x"         // >>> Profiles
"prof_no"           // <No profile>
"prof_norm"         // Normal
"prof_hs"           // Headset
"prof_meet"         // Meeting
"prof_loud"         // Loud
"prof_my"           // <Profile 05>
"prof_ed_x"         // Edit profiles
"prof_ed_norm"      // Edit Normal
"prof_ed_hs"        // Edit Headset
"prof_ed_meet"      // Edit Meeting
"prof_ed_loud"      // Edit Loud
"usb_mode"          // USB mode
"doa_master"        // DOA master
"f_x"               // <<< XML Applications / Functions 01..10(*)
"pbx_fkeys"         // <<< List of applications / functions(*)
"f_1"               // App/F01(*)
"f_2"               // App/F02(*)
"f_3"               // App/F03(*)
"f_4"               // App/F04(*)
```

```
    "f_5"               // App/F05(*)
    "f_6"               // App/F06(*)
    "f_7"               // App/F07(*)
    "f_8"               // App/F08(*)
    "f_9"               // App/F09(*)
    "f_10"              // App/F10(*)
    "vlstx"             // Variable lists
    "vlst1"             // Variable list 1
    "vlst1_1"           // List 1 item 1
    "vlst1_2"           // List 1 item 2
    "vlst1_3"           // List 1 item 3
    "vlst1_4"           // List 1 item 4
    "vlst1_5"           // List 1 item 5
    "vlst1_6"           // List 1 item 6
    "vlst1_7"           // List 1 item 7
    "vlst1_8"           // List 1 item 8
    "vlst1_9"           // List 1 item 9
    "vlst1_10"          // List 1 item 10
    "vlst2"             // Variable list 2
    "vlst2_1"           // List 2 item 1
    "vlst2_2"           // List 2 item 2
    "vlst2_3"           // List 2 item 3
    "vlst2_4"           // List 2 item 4
    "vlst2_5"           // List 2 item 5
    "vlst2_6"           // List 2 item 6
    "vlst2_7"           // List 2 item 7
    "vlst2_8"           // List 2 item 8
    "vlst2_9"           // List 2 item 9
    "vlst2_10"          // List 2 item 10
    "menu_x"            // All menus
    "opt"               // All dial/call options

// assignment of keys
    "UD_KeyAssignmentIdle"          // VAL_KEY_xxx and VAL_FKT_IDLE_xxx
    "UD_KeyAssignmentDial"          // VAL_KEY_xxx and VAL_FKT_DIAL_xxx
    "UD_KeyAssignmentAlert"         // VAL_KEY_xxx and VAL_FKT_ALERT_xxx
    "UD_KeyAssignmentActive"        // VAL_KEY_xxx and VAL_FKT_ACTIVE_xxx
    "UD_KeyAssignmentActiveSos"     // VAL_KEY_xxx and VAL_FKT_ACTIVE_SOS_xxx

    "UD_KeyAssignmentIdleMaster"    // VAL_KEY_xxx and VAL_FKT_IDLE_xxx
    "UD_KeyAssignmentDialMaster"    // VAL_KEY_xxx and VAL_FKT_DIAL_xxx
    "UD_KeyAssignmentAlertMaster"   // VAL_KEY_xxx and VAL_FKT_ALERT_xxx
```

```
    "UD_KeyAssignmentActiveMaster"    // VAL_KEY_xxx and VAL_FKT_ACTIVE_xxx
    "UD_KeyAssignmentActiveSosMaster" // VAL_KEY_xxx and VAL_FKT_ACTIVE_SOS_xxx

// keys available on device
    "sos"                // SOS-key (sos)
    "side1"              // Side key up (side1)
    "side2"              // Side key middle (side2)
    "side3"              // Side key down (side3)
    "vip"                // Hotkey (vip)
    "ok"                 // Softkey left (ok)
    "esc"                // Softkey middle (esc)
    "opt"                // Softkey right (opt)
    "left"               // Navi. left (left)
    "right"              // Navi. right (right)
    "up"                 // Navi. up (up)
    "down"               // Navi. down (down)
    "green"              // Hook off (green)
    "red"                // Hook on (red)
    "long.sos"           // SOS-key long (long.sos)
    "long.side1"         // Side key up long (long.side1)
    "long.side2"         // Side key middle long (long.side2)
    "long.side3"         // Side key down long (long.side3)
    "long.vip"           // Hotkey long (long.vip)
    "long.ok"            // Softkey left long (long.ok)
    "long.esc"           // Softkey middle long (long.esc)
    "long.opt"           // Softkey right long (long.opt)
    "long.left"          // Navi. left long (long.left)
    "long.right"         // Navi. right long (long.right)
    "long.green"         // Hook off long (long.green)
    "long.red"           // Hook on long (long.red)
    "long.d0"            // Key 0 long (long.d0)
    "long.d1"            // Key 1 long (long.d1)
    "long.d2"            // Key 2 long (long.d2)
    "long.d3"            // Key 3 long (long.d3)
    "long.d4"            // Key 4 long (long.d4)
    "long.d5"            // Key 5 long (long.d5)
    "long.d6"            // Key 6 long (long.d6)
    "long.d7"            // Key 7 long (long.d7)
    "long.d8"            // Key 8 long (long.d8)
    "long.d9"            // Key 9 long (long.d9)
    "long.star"          // Star key long (long.star)
    "long.hash"          // Hash key long (long.hash)
```

```
   "d0"                // Key 0 (d0)
   "d1"                // Key 1 (d1)
   "d2"                // Key 2 (d2)
   "d3"                // Key 3 (d3)
   "d4"                // Key 4 (d4)
   "d5"                // Key 5 (d5)
   "d6"                // Key 6 (d6)
   "d7"                // Key 7 (d7)
   "d8"                // Key 8 (d8)
   "d9"                // Key 9 (d9)
   "star"              // Star key (star)
   "hash"              // Hash key (hash)
   "del"               // C-key (del)
   "spk"               // Handsfree (spk)
   "long.del"          // C-key long (long.del)
   "long.spk"          // Handsfree long (long.spk)

// functions available in IDLE state
   "nop"                 // <no function>
   "prog"                // <key programming>
   "menu"                // >>>Menu
   "dyn_pbx_option"      // >>>System options / main menu
   "pbx_server_menu"     // >>>Server menu
   "alarm_time"          // Time/Alarms
   "alarm"               //     Alarm clock
   "appointment"         //     Appointment
   "tea_timer"           //     Timer
   "directories"         // Directories (Personal/Central/VIP-list)
   "get_name"            //     Get name from personal directory
   "book"                //     Personal directory
   "gappp_directory"     //     Central directory (obsolete)
   "pbx_directory"       //     Central directory(*)
   "vip"                 //     VIP list
   "quick0"              // Quick call list
   "sos_menu"            // SOS call: with confirmation
   "sos"                 // SOS call
   "sos_loc"             // Localisation alarm
   "shock"               // Shock detection
   "alarm_call"          // Alarm call
   "sensor_menu"         // Alarm sensor
   "navi"                // Navigation key
   "inf"                 // (i) Info menu
```

```
"MenuInfNew"           // (i) New infos
"voice_box"            //     Voice box
"caller"               //     Caller list
"redial"               //     Redial list
"omm_jobs"             //     Job list
"BestMsg"              //     Text messages
"omm_inbox"            //     Inbox/Text messages
"omm_outbox"           //     Outbox/Text messages
"omm_def_msg"          //     Pre-defined messages
"txt_send"             //     Send new text message
"active_features"      // Active Handset features
"feature_access_code"  // Feature access codes(*)
"pbx_unpark"           // Unpark call(*)
"gappp_pickup"         // Pickup call(*)
"pbx_take"             // Take call(*)
"locating_editor"      // Locating(*)
"pbx_presence"         // Presence(*)
"pbx_dnd"              // Call protection(*)
"gappp_call_forward"   // Call diversion(*)
"pbx_call_routing"     // Call routing(*)
"profile"              // Profile
"datamanagment"        // Data managment
"keylock"              // Key lock
"pinlock"              // Pin/Phone lock
"light_toggle"         // Light on/off
"bt"                   // Bluetooth settings
"bt_state"             // BT status (on/off)
"ring_off"             // Ringer on/off
"vol_ok"               // Volume settings
"audio_hd"             // HiQ audio on/off
"off"                  // Power off
"predial"              // Please dial editor
"version"              // Version info
"filter_menu"          // Call filter
"filter_state"         //    Call filter state
"pbx_fkeys"            // XML Applications
"f_1"                  //     App 1
"f_2"                  //     App 2
"f_3"                  //     App 3
"f_4"                  //     App 4
"f_5"                  //     App 5
"f_6"                  //     App 6
```

```
    "f_7"                 //     App 7
    "f_8"                 //     App 8
    "f_9"                 //     App 9
    "f_10"                //     App 10
    "vlstx"               // Variable lists
    "vlst1"               //   Variable list 1
    "vlst1_1"             //     List 1 item 1
    "vlst1_2"             //     List 1 item 2
    "vlst1_3"             //     List 1 item 3
    "vlst1_4"             //     List 1 item 4
    "vlst1_5"             //     List 1 item 5
    "vlst1_6"             //     List 1 item 6
    "vlst1_7"             //     List 1 item 7
    "vlst1_8"             //     List 1 item 8
    "vlst1_9"             //     List 1 item 9
    "vlst1_10"            //     List 1 item 10
    "vlst2"               //   Variable list 2
    "vlst2_1"             //     List 2 item 1
    "vlst2_2"             //     List 2 item 2
    "vlst2_3"             //     List 2 item 3
    "vlst2_4"             //     List 2 item 4
    "vlst2_5"             //     List 2 item 5
    "vlst2_6"             //     List 2 item 6
    "vlst2_7"             //     List 2 item 7
    "vlst2_8"             //     List 2 item 8
    "vlst2_9"             //     List 2 item 9
    "vlst2_10"            //     List 2 item 10

// functions available in DIAL state
    "nop"                 // <no function>
    "sk_dyn1"             // <dynamic soft-key>
    "caller"              // Caller list
    "redial"              // Redial list
    "get_name"            // Get name from personal directory
    "book_req"            // Personal directory
    "gappp_directory"     //     Central directory (obsolete)
    "pbx_directory"       // Central directory(*)
    "vip"                 //     VIP list
    "add_to"              //     Add to... (VIP-, Filter-list, Personal directory)
    "gappp_pickup_select" // Pickup select
    "gappp_vip_call"      // VIP call
    "gappp_announcement"  // Announcement
```

```
    "gappp_intercom"       // Intercom
    "vlstx"                // Variable lists
    "vlst1"                //   Variable list 1
    "vlst1_1"              //     List 1 item 1
    "vlst1_2"              //     List 1 item 2
    "vlst1_3"              //     List 1 item 3
    "vlst1_4"              //     List 1 item 4
    "vlst1_5"              //     List 1 item 5
    "vlst1_6"              //     List 1 item 6
    "vlst1_7"              //     List 1 item 7
    "vlst1_8"              //     List 1 item 8
    "vlst1_9"              //     List 1 item 9
    "vlst1_10"             //     List 1 item 10
    "vlst2"                //   Variable list 2
    "vlst2_1"              //     List 2 item 1
    "vlst2_2"              //     List 2 item 2
    "vlst2_3"              //     List 2 item 3
    "vlst2_4"              //     List 2 item 4
    "vlst2_5"              //     List 2 item 5
    "vlst2_6"              //     List 2 item 6
    "vlst2_7"              //     List 2 item 7
    "vlst2_8"              //     List 2 item 8
    "vlst2_9"              //     List 2 item 9
    "vlst2_10"             //     List 2 item 10

// functions available in ALERTING state
    "nop"                  // <no function>
    "sk_dyn1"              // <dynamic soft-key>
    "opt"                  // >>>Call options
    "acc"                  // Accept call / Hook off
    "rej"                  // Reject call / Hook on
    "ring_off"             // Ringing off
    "add_to"               // Add to... (VIP-, Filter-list, Personal directory)
    "opt_ccbs"             // Callback CCBS
    "opt_ccnr"             // Callback CCNR
    "opt_mcid"             // Intercept MCID
    "opt_pickup"           // Pickup call
    "opt_pickup_select"    // Pickup select
    "opt_park"             // Park call/Unpark call
    "opt_take"             // Take call
    "vlstx"                // Variable lists
    "vlst1"                //   Variable list 1
```

```
    "vlst1_1"              //     List 1 item 1
    "vlst1_2"              //     List 1 item 2
    "vlst1_3"              //     List 1 item 3
    "vlst1_4"              //     List 1 item 4
    "vlst1_5"              //     List 1 item 5
    "vlst1_6"              //     List 1 item 6
    "vlst1_7"              //     List 1 item 7
    "vlst1_8"              //     List 1 item 8
    "vlst1_9"              //     List 1 item 9
    "vlst1_10"             //     List 1 item 10
    "vlst2"                //   Variable list 2
    "vlst2_1"              //     List 2 item 1
    "vlst2_2"              //     List 2 item 2
    "vlst2_3"              //     List 2 item 3
    "vlst2_4"              //     List 2 item 4
    "vlst2_5"              //     List 2 item 5
    "vlst2_6"              //     List 2 item 6
    "vlst2_7"              //     List 2 item 7
    "vlst2_8"              //     List 2 item 8
    "vlst2_9"              //     List 2 item 9
    "vlst2_10"             //     List 2 item 10

// functions available in ACTIVE state
    "nop"                  // <no function>
    "sk_dyn1"              // <dynamic soft-key>
    "opt"                  // >>>Call options
    "pbx_server_menu"      // >>>Server menu(*)
    "feature_access_code"  // >>>Feature access codes(*)
    "dial_r"               // (R) Register recall
    "opt_ect"              // Transfer call
    "opt_brokering"        // Brokering
    "opt_hold"             // Hold call
    "opt_3pty"             // Conference start/stopp
    "opt_park"             // Park call/Unpark call
    "rel"                  // Release call / Hook on
    "add_to"               // Add to... (VIP-, Filter-list, Personal directory)
    "book"                 // Personal directory
    "gappp_directory"      //     Central directory (obsolete)
    "pbx_directory"        // Central directory(*)
    "vip"                  // VIP list
    "quick0"               // Quick call list
    "filter"               // Call filter list
```

```
    "caller"               // Caller list
    "redial"               // Redial list
    "txt_send"             // Send new text message
    "vol_ok"               // Volume settings
    "vol_up"               // Volume +
    "vol_down"             // Volume -
    "mute"                 // Microphone on/off
    "audio_hd"             // HiQ audio on/off
    "bt_toggle"            // Transfer BT <-> Handset
    "opt_ccbs"             // Callback CCBS
    "opt_ccnr"             // Callback CCNR
    "opt_mcid"             // Intercept MCID
    "opt_pickup"           // Pickup
    "opt_pickup_select"    // Pickup select
    "opt_take"             // Take call
    "vlstx"                // Variable lists
    "vlst1"                //   Variable list 1
    "vlst1_1"              //     List 1 item 1
    "vlst1_2"              //     List 1 item 2
    "vlst1_3"              //     List 1 item 3
    "vlst1_4"              //     List 1 item 4
    "vlst1_5"              //     List 1 item 5
    "vlst1_6"              //     List 1 item 6
    "vlst1_7"              //     List 1 item 7
    "vlst1_8"              //     List 1 item 8
    "vlst1_9"              //     List 1 item 9
    "vlst1_10"             //     List 1 item 10
    "vlst2"                //   Variable list 2
    "vlst2_1"              //     List 2 item 1
    "vlst2_2"              //     List 2 item 2
    "vlst2_3"              //     List 2 item 3
    "vlst2_4"              //     List 2 item 4
    "vlst2_5"              //     List 2 item 5
    "vlst2_6"              //     List 2 item 6
    "vlst2_7"              //     List 2 item 7
    "vlst2_8"              //     List 2 item 8
    "vlst2_9"              //     List 2 item 9
    "vlst2_10"             //     List 2 item 10

// functions available in ACTIVE_SOS state
    "nop"                  // <no function>
    "sk_dyn1"              // <dynamic soft-key>
```

```
"opt"                  // >>>Call options
"pbx_server_menu"      // >>>Server menu(*)
"feature_access_code"  // >>>Feature access codes(*)
"dial_r"               // (R) Register recall
"opt_ect"              // Transfer call
"opt_brokering"        // Brokering
"opt_hold"             // Hold call
"opt_3pty"             // Conference start/stopp
"opt_park"             // Park call/Unpark call
"rel"                  // Release call / Hook on
"add_to"               // Add to... (VIP-, Filter-list, Personal directory)
"book"                 // Personal directory
"gappp_directory"      //     Central directory (obsolete)
"pbx_directory"        // Central directory(*)
"vip"                  // VIP list
"quick0"               // Quick call list
"filter"               // Call filter list
"caller"               // Caller list
"redial"               // Redial list
"txt_send"             // Send new text message
"vol_ok"               // Volume settings
"vol_up"               // Volume +
"vol_down"             // Volume -
"mute"                 // Microphone on/off
"audio_hd"             // HiQ audio on/off
"bt_toggle"            // Transfer BT <-> Handset
"opt_ccbs"             // Callback CCBS
"opt_ccnr"             // Callback CCNR
"opt_mcid"             // Intercept MCID
"opt_pickup"           // Pickup
"opt_pickup_select"    // Pickup select
"opt_take"             // Take call
"predial_hook_dyn"     // Dial editor
"dial_0"               //     Dial 0
"dial_1"               //     Dial 1
"dial_2"               //     Dial 2
"dial_3"               //     Dial 3
"dial_4"               //     Dial 4
"dial_5"               //     Dial 5
"dial_6"               //     Dial 6
"dial_7"               //     Dial 7
"dial_8"               //     Dial 8
```

```
        "dial_9"              //     Dial 9
        "dial_star"           //     Dial *
        "dial_hash"           //     Dial #
        "dial_dtmf"           //     Dial DTMF
        "vlstx"               // Variable lists
        "vlst1"               //   Variable list 1
        "vlst1_1"             //     List 1 item 1
        "vlst1_2"             //     List 1 item 2
        "vlst1_3"             //     List 1 item 3
        "vlst1_4"             //     List 1 item 4
        "vlst1_5"             //     List 1 item 5
        "vlst1_6"             //     List 1 item 6
        "vlst1_7"             //     List 1 item 7
        "vlst1_8"             //     List 1 item 8
        "vlst1_9"             //     List 1 item 9
        "vlst1_10"            //     List 1 item 10
        "vlst2"               //   Variable list 2
        "vlst2_1"             //     List 2 item 1
        "vlst2_2"             //     List 2 item 2
        "vlst2_3"             //     List 2 item 3
        "vlst2_4"             //     List 2 item 4
        "vlst2_5"             //     List 2 item 5
        "vlst2_6"             //     List 2 item 6
        "vlst2_7"             //     List 2 item 7
        "vlst2_8"             //     List 2 item 8
        "vlst2_9"             //     List 2 item 9
        "vlst2_10"            //     List 2 item 10

        "UD_VListName"      // <list-index 1..2> <utf8-string>
        "UD_VListShortName" // <list-index 1..2> <utf8-string>
        "UD_VListSubItems"  // <list-index 1..2> <boolean>

// list-index    item-index    number-to-dial  longname       function-id
shortname/icon   handsfree        visible(idle,dial,alert,active
// 1..2          1..10         VAL_FKT_VLIST_xxx                  true/false/1/0
        "UD_VListEntry"     // <string>      <string>      <utf8-string>   <utf8-string>
     <string>           <utf8-string>    <boolean>        <4-digit-string-of(0,1)>
```

```
// functions available in VLIST
   "x"                    // Dummy-Function-ID
   "vlst1"                //     Variable list 1
   "vlst2"                //     Variable list 2
   "menu"                 // Menu
   "active_features"      // Active Handset features
   "alarm"                // Alarm clock
   "appointment"          // Appointment
   "tea_timer"            // Timer
   "show_time_date"       // Date/Time
   "bt"                   // Bluetooth settings
   "bt_state"             // BT status (on/off)
   "datamanagment"        // Data managment
   "keylock"              // Key lock
   "pinlock"              // Pin/Phone lock
   "profile"              // Profile
   "predial"              // Please dial editor
   "off"                  // Power off
   "off_menu"             // Off menu
   "ring_off"             // Ringer on/off
   "audio_hd"             // HiQ audio on/off
   "vol_ok"               // Volume settings
   "light_toggle"         // Light on/off
   "version"              // Version info
   "navi"                 // Navigation key
   "inf"                  // (i) Info menu
   "MenuInfNew"           // (i) New infos
   "voice_box"            //     Voice box
   "caller"               //     Caller list
   "redial"               //     Redial list
   "pbx_email"            //     Email list
   "pbx_fax"              //     Fax list
   "omm_jobs"             //     Job list
   "BestMsg"              //     Text messages
   "omm_inbox"            //     Inbox/Text messages
   "omm_outbox"           //     Outbox/Text messages
   "omm_def_msg"          //     Pre-defined messages
   "txt_send"             //     Send new text message
   "gappp_cost"           //     Cost infos
   "pbx_feature"          //     Active PBX features
   "filter_menu"          // Call filter
   "filter_state"         //     Call filter state
   "filter_list"          //     Call filter list
```

```
"directories"          // Directories (Personal/Central/VIP-list)
"get_name"             //     Get name from personal directory
"book"                 //     Personal directory
"gappp_intern"         //     Internal directory
"pbx_directory"        //     Central directory
"vip"                  //     VIP list
"feature_access_code"  //     Feature access codes
"pbx_reception"        //     Hotel reception
"quick0"               //     Quick call list
"sos_menu"             // SOS call: with confirmation
"sos"                  // SOS call
"sos_loc"              // Localisation alarm
"shock"                // Shock detection
"alarm_call"           // Alarm call
"sensor_menu"          // Alarm sensor
"dyn_pbx_option"       // System options / Main menu
"pbx_server_menu"      // Server menu
"pbx_options"          // System Options
"gappp_call_forward"   // Call diversion
"pbx_call_routing"     // Call routing
"pbx_dnd"              // Call protection
"pbx_presence"         // Presence
"locating_editor"      // Locating
"pbx_take"             // Take call
"pbx_unpark"           // Unpark call
"pbx_park"             // Park/Pickup
"gappp_pickup"         // Pickup call
"pbx_fkeys"            // XML Applications
"f_1"                  //     App 1
"f_2"                  //     App 2
"f_3"                  //     App 3
"f_4"                  //     App 4
"f_5"                  //     App 5
"f_6"                  //     App 6
"f_7"                  //     App 7
"f_8"                  //     App 8
"f_9"                  //     App 9
"f_10"                 //     App 10
"gappp_door"           // Door opener
"gappp_door1"          //     Door 1
"gappp_door2"          //     Door 2
"gappp_pickup_select"  // Pickup select
"gappp_announcement"   // Announcement
"gappp_intercom"       // Intercom
```

```
"gappp_vip_call"       // VIP call
"suppress_no"          // Suppress no on/off
"sel_line"             // Select line
"line_1"               //     L1
"line_2"               //     L2
"line_3"               //     L3
"line_4"               //     L4
"line_5"               //     L5
"line_6"               //     L6
"line_7"               //     L7
"line_8"               //     L8
"line_9"               //     L9
"line_10"              //     L10
"sk_dyn1"              // <dynamic soft-key>
"opt"                  // Call options
"add_to"               // Add to... (VIP-, Filter-list, Personal directory)
"filter"               // Call filter list
"opt_called_lines"     // Called lines
"dial_r"               // (R) Register recall
"opt_ect"              // Transfer call
"opt_deflect"          // Deflect call
"opt_ccbs"             // Callback CCBS
"opt_ccnr"             // Callback CCNR
"opt_mcid"             // Intercept MCID
"opt_receive"          // Receive call
"opt_reject"           // Reject call
"opt_int"              // DECT intern
"opt_brokering"        // Brokering
"opt_hold"             // Hold call
"opt_3pty"             // Conference start/stopp
"opt_record"           // Recording start/stopp
"opt_retrieve"         // Retrieve call in hold
"opt_privious"         // Previous call
"opt_release"          // Release call
"rel"                  // Release call / Hook on
"pbx_park"             // Park call/Unpark call
"opt_booking_no"       // Booking no
"vol_up"               // Volume +
"vol_down"             // Volume -
"mute"                 // Microphone on/off
"bt_toggle"            // Transfer BT <-> Handset
```

24 CONSOLIDATED CERTIFICATE MANAGEMENT

SIP-DECT with Cloud-ID has various secured interfaces to support secure connections for file imports from local servers or provisioning servers. By default, the OMM Web server uses the hard coded self-signed OMM certificate as local certificate for provisioning (mutual authentication) and for SIP-over-TLS connections.

Certificate and authentication validation settings for these secure connections can be inherited from the configuration file URL (see section 6.1).

24.1 SIP OVER TLS CERTIFICATES

SIP over TLS certificates are used for secure SIP connections. The hard coded self-signed OMM certificate is used by default, however you can import trusted certificates, a local certificate chain and a private key file (optionally password-protected) via:

- OMM Web service (**System** -> **SIP** -> **Security**); see section 11.6.6
- a certificate server (usually running on a Mitel call server); see section 11.6.7

24.2 OMM CERTIFICATE (WEB SERVICE)

The OMM Web server uses the hard coded self-signed OMM certificate by default.

A provider can configure a certificate server to update the hard coded OMM certificate with a local certificate chain and a private key file (optionally password-protected) via provisioning files (see section 6.9).

The OMM certificate will be used for HTTPS connections to the OMM web service. If the OMM can be reached from the internet by a domain and an appropriate CA certificate has been imported, no security warnings are displayed in web browsers trusting the CA root certificate.

24.3 PROVISIONING CERTIFICATES

Provisioning certificates are used for secure connections to configuration or firmware file servers with support for mutual authentication (i.e. for FTPS and HTTPs protocols).

The OMM uses a trusted certificate chain to validate the server. This is required if the server has no certificate derived from a trusted CA root certificate, where the OMM uses the Mozilla CA Certificate List. If no server certificate is available, you can disable the validation against trusted and CA certificates.

By default, the hard-coded self-signed OMM certificate is used for mutual authentication. You can overwrite the hard coded OMM certificate by importing trusted certificates, a local certificate chain and a private key file (optionally password-protected) via:

- OMM Web service **System** -> **Provisioning** -> **Certificates** page (see section 6.6)
- A certificate server configured by the provider (see section 6.8)

The OMM provides the local certificate chain and the private key to servers that request mutual authentication.

The system credentials can be inherited if specific sources for configuration and resource files are configured, where the ‘Use common certificate configuration’ option is enabled.

24.4 CERTIFICATE VALIDATION

If the HTTPS or FTPS protocol is used to retrieve files from the configured provisioning server, the OMM validates the server certificates according to the certificate validation settings.

You can configure the certificate validation settings via the OMM Web service (**System** -> **Provisioning** -> **Certificates**). Certificate validation settings can also be part of the ConfigURL provided by the RCS or via DHCP.

If you want to use the same validation settings for a specific URL (i.e., other than the configuration file URL), enable the “Use common certificate configuration” parameter when configuring the URL (unless the “Import certificates with first connection” parameter is enabled).

25 REGULATORY COMPLIANCE AND SAFETY INFORMATION

25.1 MITEL RFP44/45/47/48

For basic installation guidelines necessary for the proper and safe functioning of this equipment, refer to the Safety Instructions (document part number 5701204601RA) packaged with the system and posted on the eDocs web site (http://edocs.mitel.com/).

Read and folow all information contained in the Safety Instructions document before attempting to install or use Mitel products. Only trained, qualified service personnel shall install or maintain Mitel products.

For regulatory information for U.S., Canada, and Europe, refer to the Regulatory Notices section in the Safety Instructions (document part number 5701204601RA) packaged with the system and posted on the eDocs web site (http://edocs.mitel.com/).

25.2 COMMUNICATIONS REGULATION INFORMATION FOR RFP 35, RFP 36 AND RFP 37

25.2.1 FCC NOTICES (U.S. ONLY)

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Modifications not expressly approved by this company could void the user's authority to operate the equipment.

NOTE: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Exposure to Radio Frequency (RF) Signals:

The wireless phone is a radio transmitter and receiver. It is designed and manufactured not to exceed the emission limits for exposure to radio frequency (RF) energy set by the Federal Communications Commission (FCC) of the U.S. Government. These limits are part of comprehensive guidelines and establish permitted levels of RF energy for the general population. The guidelines are based on the safety standards previously set by both U.S. and international standards bodies. These standards include a substantial safety margin designed to assure the safety of all persons, regardless of age and health.

This device and its antenna must not be co-located or operating in conjunction with any other antenna or transmitter.

The radiating element of the RFP should be installed during operating at a separation distance greater than 20 cm between user and device. The device complies with the requirements for routine evaluation limits.

25.2.2 INDUSTRY CANADA (CANADA ONLY)

Operation of this device is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.

Privacy of communications may not be ensured when using this telephone.

Exposure to Radio Frequency (RF) Signals:

The wireless phone is a radio transmitter and receiver. It is designed and manufactured not to exceed the emission limit for exposure to radio frequency (RF) energy set by the Ministry of Health (Canada), Safety Code 6. These limits are part of comprehensive guidelines and established permitted levels of RF energy for the general population. These guidelines are based on the safety standards previously set by international standard bodies. These standards include a substantial safety margin designed to assure the safety of all persons, regardless of age and health.

This device and its antenna must not be co-located or operating in conjunction with any other antenna or transmitter.

The radiating element of the RFP should be installed during operating at a separation distance greater than 20 cm between user and device. This device complies with the requirements for routine evaluation limits.

25.3 SUPPORTING DOCUMENTATION

For information on how to install and configure your Mitel RFP Base station and to access system-specific documentation, do the following:

1. Log in to Mitel Connect.
2. In left-hand menu, click **Mitel OnLine**.
3. Click Product Documentation under the Technical Support section

Select **SIP-DECT** under the **Phones** drop-down menu.

25.4 DECLARATION OF CONFORMITY

We, Mitel Networks Corporation, declare that the RFP 45, RFP 47, RFP 47 DRC and RFP 48 meet the essential requirements of Directives 2014/53/EC (RED) and 2011/65/EU (RoHS). A copy of this declaration may be found at the following internet address:

https://www.mitel.com/legal/regulatory-declarations

Any unauthorized modification of the product voids this declaration. For a copy of the original signed Declaration Of Conformity please contact Mitel at the following address:

Mitel Deutschland GmbH
Zeughofstrasse 1
10997 Berlin
Germany

26 APPENDIX

26.1 ABBREVIATIONS

AC	Authentication Code
CoA	Central DECT Phone Configuration Over Air
DECT	Digital Enhanced Cordless Telecommunication
DHCP	Dynamic Host Configuration Protocol
FCC	Federal Communications Commission
GAP	Generic Access Profile
OM IMA	Integrated Messaging and Alerting Service
IPEI	International Portable Equipment Identity
HTTP	Hyper Text Transfer Protocol
IPBX	IP PBX, a telephony system using IP / VoIP
OM	OpenMobility
OM AXI	OM Application XML Interface
OMC	OM Configurator
OML	OM Locating
OMM	OpenMobility Manager
PARK	Portable Access Rights Key
PBX	Private Branch Exchange, a customer premises telephony system
SNMP	Simple Network Management Protocol
TFTP	Trivial File Transfer Protocol
RFP	DECT Radio Fixed Part (DECT base station)
RTCP	Real Time Control Protocol
RTP	Real Time Protocol

26.2 DEFINITIONS

Asterisk	A complete Open Source PBX in software. It runs on Linux, BSD and MacOSX and provides many features. Asterisk supports voice over IP in many protocols, and can interoperate with almost all standards-based telephony equipment.
Base station	Please see: RFP or Radio Fixed Part
DECT	**D**igital **E**nhanced **C**ordless **T**elecommunication The standard (ETS 300 175) specifies the air interface, known as the radio interface. Voice and data can both be transmitted via this interface. Key technical characteristics for Europe: • frequency range: approx. 1880 – 1900 MHz (approximately 20 MHz bandwidth) • carrier frequencies (1728 kHz spacing) with 12 time slots each • double the number of time slots (to 24) using the TDMA process • net data rate per channel of 32 kbps (for voice transmission using ADPCM) • voice coding using the ADPCM method Key technical characteristics for North America: • frequency range: approx. 1920 – 1930 MHz (approximately 10 MHz bandwidth) • 5 carrier frequencies (1728 kHz spacing) with 12 time slots each) • doube the number of time slots (to 24) using the TDMA process • net data rate per channel of 32 kbps (for voice transmission using ADPCM) • voice coding using the ADPCM method
GAP	**G**eneric **A**ccess **P**rofile The GAP standard (ETS 300 444) is based on the same technology as DECT, but is limited to the most important basic features. This standard was created to allow telephones from different vendors to be used on any type of DECT system. It represents the smallest common denominator of all manufacturer-specific variants of the DECT standard. An important limitation in the GAP standard is that external handover is not supported. For this reason, connection handover is used, which is supported by GAP terminals. The operation of GAP-capable telephones is comparable to that of analogue terminals. For example, features can be called up via '*' and '#' procedures.
Handover	A handover is similar to roaming, but occurs during an ongoing call. A handover normally takes place seamlessly in the background, without disrupting the call.
IPEI	**I**nternational **P**ortable **E**quipment **I**dentity 13-digit identification code for DECT phones Example: 00019 0592015 3 (the final digit is the checksum). The code is represented in decimal form and is globally unique.
PARK	**P**ortable **A**ccess **R**ights **K**ey Access code that determines whether a DECT phone can access a particular DECT system. Used for unique selection of a dedicated system at subscription time. Provided via the PARK online service and unique to each SIP-DECT deployment.
Radio Fixed Part (RFP)	An RFP (or base station) provides a DECT radio cell and terminates the radio link from the portable DECT device. One or more RFPs build the area of radio coverage.
Roaming	While in motion, the DECT phone performs ongoing measurements to determine which RFP is best received. The one that can be best received is defined as the active RFP. To prevent the DECT phone from rapidly switching back and forth between two RFPs that have similar signal strength, certain threshold values are in effect.

26.3 REFERENCES

/1/ RFC 1350, The TFTP Protocol, Revision 2, July 1992

/2/ RFC 2090, TFTP Multicast Option, February 1997

/3/ RFC 2347, TFTP Option Extension, May 1998

/4/ RFC 2348, TFTP Block size Option, May 1998

/5/ RFC 2349, TFTP Timeout Interval and Transfer Size Options, May 1998

/6/ RFC 2236, Internet Group Management Protocol, Version 2, November 1997

/7/ RFC 1889, RTP: A Transport Protocol for Real-Time Applications, January 1996

/8/ RFC 2030, Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI, October 1996

/9/ RFC 2131, Dynamic Host Configuration Protocol, March 1997

/10/ RFC 2327, SDP: Session Description Protocol, April 1998

/11/ RFC 2474, Definition of the Differentiated Service Field (DS Field) in the IPv4 and IPv6 Headers, December 1998

/12/ RFC 2617, HTTP Authentication: Basic and Digest Access Authentication, June 1999

/13/ RFC 3164, The BSD Sys Log Protocol, August 2001

/14/ RFC 2833, RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals, May 2000

/15/ RFC 3261, Session Initiation Protocol (SIP), June 2002

/16/ RFC 3264, An Offer/Answer Model with Session Description Protocol (SDP), June 2002

/17/ RFC 3326, The Reason Header Field for SIP, December 2002

/18/ RFC 3420, Internet Media Type message/sipfrag, November 2002

/19/ RFC 3515, The Session Initiation Protocol (SIP) Refer method, April 2003

/20/ RFC 3665, The Session Initiation Protocol (SIP) Basic Call Flow Examples, December 2003

/21/ RFC 3842, A Message Summary and Message Waiting Indication Event Package for the Session Initiation Protocol (SIP), August 2004

/22/ RFC 3891, The Session Initiation Protocol (SIP) “Replaces” Header, September 2004

/23/ RFC 3892, The Session Initiation Protocol (SIP) Referred-By Mechanism, September 2004

/24/ RFC 4566, SDP: Session Description Protocol

/25/ RFC 5806, Diversion Indication in SIP, March 2010

/26/ SIP-DECT; OM Locating Application; Installation, Administration & User Guide

/27/ SIP-DECT; OM Integrated Messaging & Alerting Application; Installation, Administration & User Guide

/28/ SIP-DECT; OM DECT Phone Sharing & Provisioning; User Guide

/29/ SIP-DECT; OM User Monitoring; User Guide

/30/ SIP-DECT; Mitel 600 Messaging & Alerting Applications; User Guide

/31/ SIP-DECT; Mitel 600 Series DECT Phone; User Guide

/32/ aad-0384 OM Application XML Interface specification (OM AXI)

/33/ RFC 2782, A DNS RR for specifying the location of services (DNS SRV)

/34/ RFC 3262, Reliability of Provisional Responses in the Session Initiation Protocol (SIP)

/35/ RFC 3311, The Session Initiation Protocol (SIP) UPDATE Method

/36/ SIP-DECT XML terminal interface specification (req-0785 version 6.0)

/37/ RFC 4579, Session Initiation Protocol (SIP) Call Control - Conferencing for User Agents

/38/ RFC 5589, Session Initiation Protocol (SIP) Call Control – Transfer

/39/ RFC 2246, The TLS Protocol Version 1.0
/40/ RFC 2459, Internet X.509 Public Key Infrastructure certificate
/41/ RFC 3711, The Secure Real-Time Transport Protocol (SRTP)
/42/ RFC 4346, The Transport Layer Security (TLS) Protocol Version 1.1
/43/ RFC 4568, Session Description Protocol (SDP); Security Description for Media Streams
/44/ RFC 5246, The Transport Layer Security (TLS) Protocol Version 1.2
/45/ RFC 5630, The Use of the SIPS URI Scheme in the Session Initiation Protocol (SIP)
/46/ Development Guide XML API for Aastra SIP Phones (PA-001008-05-00)
/47/ Redirection and Configuration Service (RCS) USER GUIDE (41-001302-01 REV01)

26.4 PROTOCOLS AND PORTS

Protocol		OpenMobility Manager	
		Server port	Client port
HTTPS server	tcp server	443 or as configured	any
HTTP server (redirect to https)	tcp server	80 or as configured	any
HTTP/HTTPS client for the SIP-DECT XML terminal interface	tcp	80/443	> 1024
RFP control protocol	tcp server	16321	any
LDAP	tcp client	389 or as configured	>=1024 (see note)
TFTP client	udp	69 / given by server	>=1024 (see note)
HTTP client	tcp	80 or as configured	>=1024 (see note)
HTTPS client	tcp	443 or as configured	>=1024 (see note)
explicit FTPS client	tcp	21 or as configured	>=1024 (see note)
implicit FTPS client	tcp	990 or as configured	>=1024 (see note)
SIP	udp	5060	as configured
Telnet (OMM console, Linux x86 server based OMM only)	tcp server	localhost 8107	localhost any

Unbound ports start at port 1024.

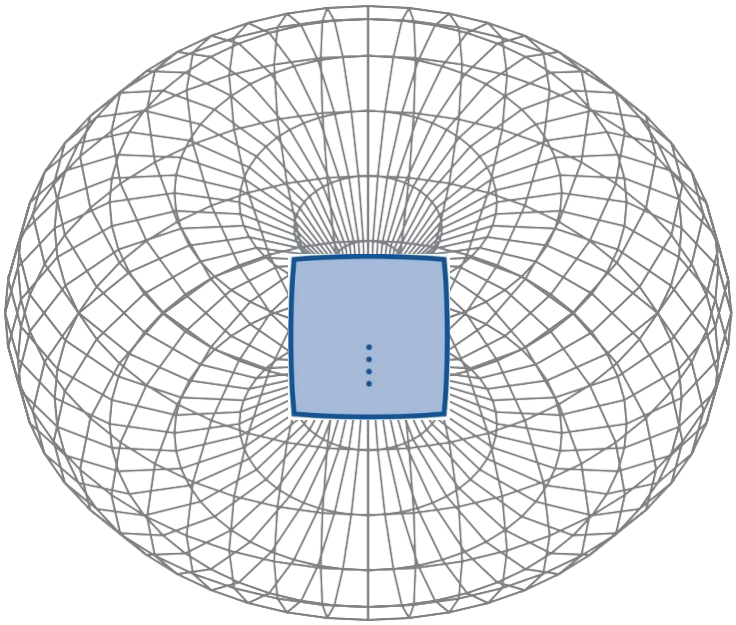
Protocol		IP-RFP	
		Server port	Client port
HTTP/HTTPS client for the SIP-DECT XML terminal interface	tcp	80/443	> 1024
RFP control protocol	tcp client	16321	>=1024 (see note)
HTTP server (redirect to OMM web server (http))	tcp server	80 or as configured	Any
SSH server	tcp server	22	Any
DHCP client	udp	67	68
TFTP client	udp	69 / given by server	>=1024 (see note)
OMCFG server	udp	64000	64000
ODIP (OMM discovery)	udp	64002	Any
NTP client	udp	123	123
Syslog client	udp	514 or as configured	514
DNS client	udp	53	>=1024 (see note)
SNMP agent (server)	udp	161	Any
SNMP trap agent (client)	udp	>=1024 (see note)	162
RSXport (debug only)	tcp server	38477	Any
RTP/RTCP (server)	udp	Range of [RTP port base + 71] even ports for RTP, odd ports for RTCP. Port base is 16320 or as configured.	Any
RTP/RTCP (client)	udp	any	Range of [RTP port base + 71] even ports for RTP, odd ports for RTCP. Port base is 16320 or as configured.
Integrated Conference Server (ICS) RTP/RTCP (server)		Range of [ICS RTP port base + 2 * no. conf. channels] even ports for RTP, odd ports for RTCP. ICS Port base is end of RTP range plus 1.	Any
Integrated Conference Server (ICS) RTP/RTCP (client)		any	Range of [ICS RTP port base + 2 * no. conf. channels] even ports for RTP, odd ports for RTCP. ICS Port base is end of RTP range plus 1.

Unbound ports start at port 1024.

26.5 RADIO COVERAGE AREA

The supply range of a DECT system can vary greatly from a geographical point of view. The DECT base station transmits and receives the radio signal through two integrated antennas inside the housing. The radio characteristic of internal antennas is doughnut (or torus) shaped under ideal conditions.

This does not take into account the topology / environment that further attenuates the signal's propagation. The radio characteristic within the area to be covered is influenced by the objects and materials typically located in buildings. The doughnut-shaped radio characteristic is therefore deformed accordingly.



26.5.1 RADIO PROPAGATION CONDITIONS

The typical radio range of a single DECT base station depends on the regulatory domain (due to regulatory transmit power limits) as well as on the environment:

- US: Outdoor range is up to 590 ft, while indoor range is up to 80 ft.
- EU: Outdoor range is up to 300 m, while indoor range is up to 30 m.

An ideal location for installing the base station is a height of between 6.6 ft and 8.2 ft (2 m and 2.50 m) for room heights between 8.2 ft and 9.8 ft (2.50 m and 3 m). For rooms with higher ceilings, the ideal installation height increases accordingly while maintaining a minimum ceiling distance of 1.6 ft (0.50 m). An installation height of less than 4.9 ft (1.50 m) is not recommended. Installation inside a dropped ceiling, cabinets or other enclosed furnishings is not recommended as this considerably impairs the radio range.

In radio technology there are many interference factors that affect mainly the range and quality of the transmission. In principle, you need to differentiate between two types of interference factors:

- Interference by obstacles that attenuate and/or reflect radio propagation, causing dead spots
- Interference due to other radio signals (e.g. other non-synchronous DECT systems) which lead to transmission errors.

The receive power of DECT signals can fluctuate a great deal locally, within only a few centimetres. This means that signal interference can be reduced or eliminated simply by altering the position of the base station.

Obstacles may include:

- Moving metal objects such as lifts, cranes, carriages, escalators, blinds, especially ones that are actuated automatically (the influence of such obstacles varies and is therefore difficult to assess).

- Metal-panelled rooms and large metal-clad objects such as air conditioners, com- puter rooms, metallized glassed areas (mirrored), fire protection walls, storage tank installations, refrigerating units, boilers, pipes.
- Building structures and installations such as steel-reinforced concrete ceilings and walls, stairways, long corridors, rising mains, cable ducts.
- Room furnishings such as metal shelves, file cabinets.

The following table shows range losses (in percent compared to ideal conditions):

Building materials	Range loss
Glass, timber, untreated	approx. 10 %
Timber, treated	approx. 25 %
Plasterboard	approx. 27 - 41 %
Brick wall, 3.94 to 4.72 in (10 to 12 cm)	approx. 44 %
Brick wall, 9.45 in (24 cm)	approx. 60 %
Aerated concrete wall	approx. 78 %
Armoured glass partition	approx. 84 %
Steel-reinforced concrete ceiling	approx. 75 - 87 %
Metal-coated glass	approx. 100 %

26.5.2 DISCLAIMER

Mitel will not accept liability for any damages and/or long distance charges, which result from unauthorized and/or unlawful use. While every effort has been made to ensure accuracy, Mitel will not be liable for technical or editorial errors or omissions contained within this documentation. The information contained in this documentation is subject to change without notice.

Mitel.com

© Copyright 2018, Mitel Networks Corporation. All Rights Reserved. The Mitel word and logo are trademarks of Mitel Networks Corporation. Any reference to third party trademarks are for reference only and Mitel makes no representation of ownership of these marks.