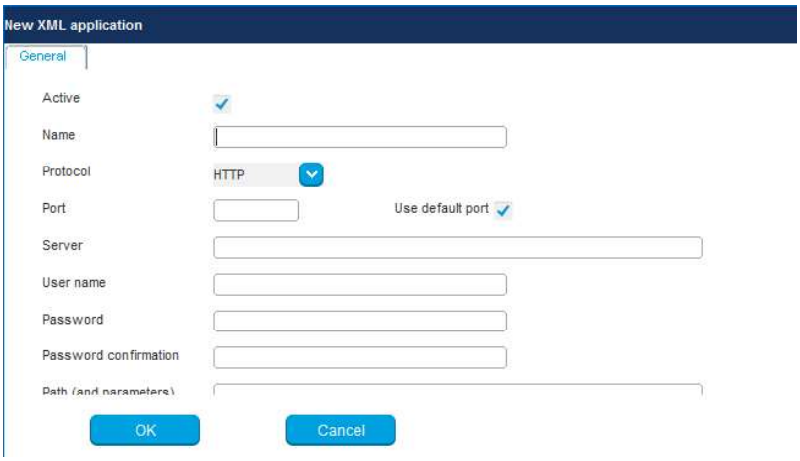
The tasks you can perform in the **XML applications** menu are mode-dependant.

Configuration mode	Monitor mode	See section
Create: Create new XML hooks		6.12.8.1
Configure: Configure selected XML hook in detail panel		6.12.8.2
	Show details: Shows selected XML hook in detail panel	6.12.8.3
Delete: Delete selected XML hook		6.12.8.4

6.12.8.1 Creating a New XML Hook

In addition to the 15 predefined XML hooks, you can create up to 10 additional XML hooks. You can only add XML hooks in **Configuration Mode**.



To add an XML hook, do the following:

1 In the **Tasks** bar click on **Create**.

The **New XML application** panel opens.

2 Specify values for the following XML hook parameters:

- **Active**: This setting activates or deactivates a configured XML application entry.
- **Name**: The predefined hooks have fixed predefined names. A name must be configured for the free defined hooks.
- **Protocol**: Select the protocol HTTP or HTTPS.
- **Server**: Enter the IP address or the name of the server which provides the XML content.

Note: SIP-DECT 6.0 and later supports “SIPProxy” placeholders for XML Server application URLs within SIP redundancy setups. In cases where applications are located on a SIP server, it is necessary to address XML applications by using the current primary, secondary or tertiary SIP server address. In those cases, the “SIPProxy” placeholder can be used as server input.

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

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

6.12.8.2 Modifying an XML Hook

You can only modify XML hooks in **Configuration Mode**.

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

1 Select the appropriate XML hook in the table.

2 In the **Tasks** bar, click **Configure**.

3 Edit the XML application parameters (described above) as necessary. You cannot change the name of a predefined XML hook.

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

See the description comment in chapter 5.9.5.

4 Click **OK**.

6.12.8.3 Viewing XML Hook Details

You can view the configuration of an XML hook in **Monitor Mode**. Do the following:

1 Select the appropriate XML hook in the table.

2 In the **Tasks** bar click on the **Show details** command.

The user account data is displayed in the user account detail panel.

3 Click **Cancel** to close the XML hook detail panel.

6.12.8.4 Deleting XML Hooks

You can only delete XML hooks in **Configuration Mode**. You cannot delete any predefined XML hooks.

To delete an XML hook, do the following:

1 Select the appropriate XML hook(s) in the table by activating the corresponding checkbox(es).

2 In the **Tasks** bar, click **Delete**.

A confirmation dialog opens.

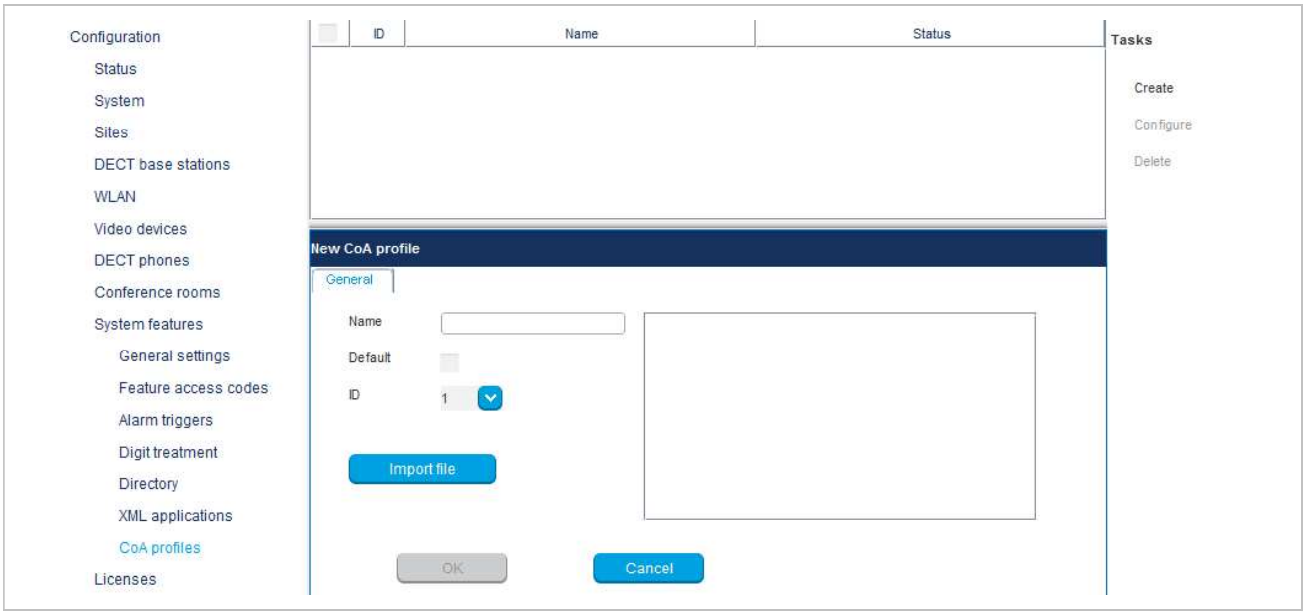
3 Click **OK** to confirm.

6.12.9 “COA PROFILES” MENU

SIP-DECT 6.0 and later supports central configuration over the air (CoA) for Mitel 602 DECT phones. The CoA profiles page lists the available CoA profiles that can be downloaded to the DECT phones.

Note: The profiles generated by the user_common.cfg configuration file are also listed in this window. When managed with OMP, they can be overwritten when the user_common.cfg configuration file is reloaded. The maximum download size is 4kB.

You can import CoA profiles via the **CoA Profiles** menu. Once you have imported the profiles, you can assign them to specific DECT phone users.



To create a new CoA profile:

1 Click **Create** under the Tasks list on the right-hand side of the **CoA profiles** window.
The **New CoA profile** dialog opens.

2 Configure the settings for the CoA profile:

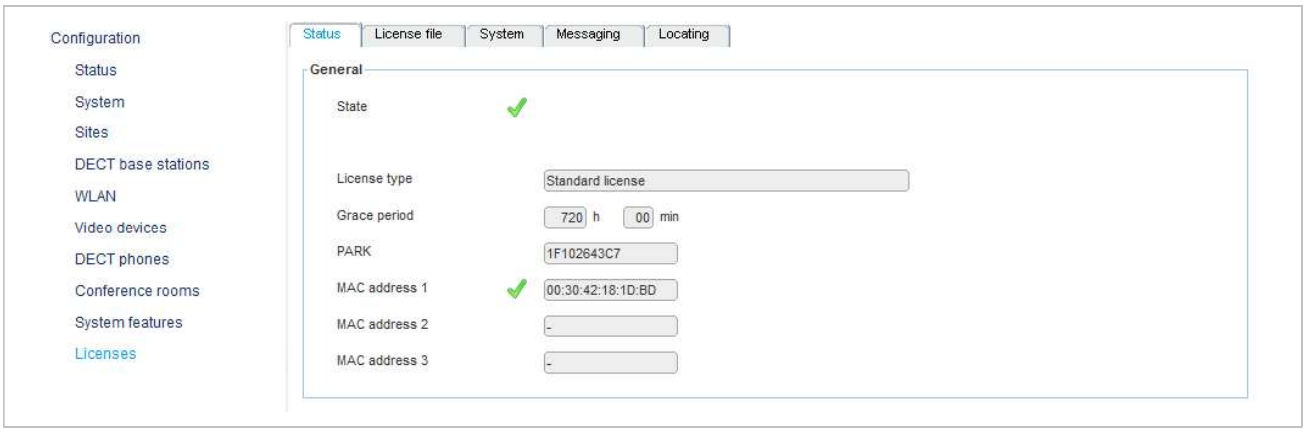
- **Name**: Specify a name for the CoA profile
- **Default**: Indicate whether this is the default CoA profile to be used
- **ID**: Select an ID for the CoA profile from the drop-down menu.

3 Click **Import file** to select the CoA file to import.

The **CoA profiles** page displays the new CoA profile in the table.

6.13 “LICENSES” MENU

The **Licenses** pageprovides an overview of licenses currently in use. In **Configuration Mode**, you can also import a license file.



The license information is displayed in the following tabs:

- **Status**: Shows general license information.
- **License file**: Allows import of a license file.
- **System**: Shows system license status.
- **Messaging**: Shows Integrated Messaging and Alerting Service (IMA) license status.
- **Locating**: Shows Locating license status.

“General” tab

The General tab displays general information about the current system license.

“License file” tab

The License file tab allows you to import a license file (only possible in **Configuration Mode**).

1 Click the **File** button to select the path and file name where the license file is stored.
2 Click the **Import** button.

“System” tab

The “System” tab provides OM System license information. This includes supported software version and number of licensed DECT base stations (RFPs) compared to number of connected DECT base stations.

“Messaging” tab

The “Messaging” tab provides OM Messaging and Alerting license information.

“Locating” tab

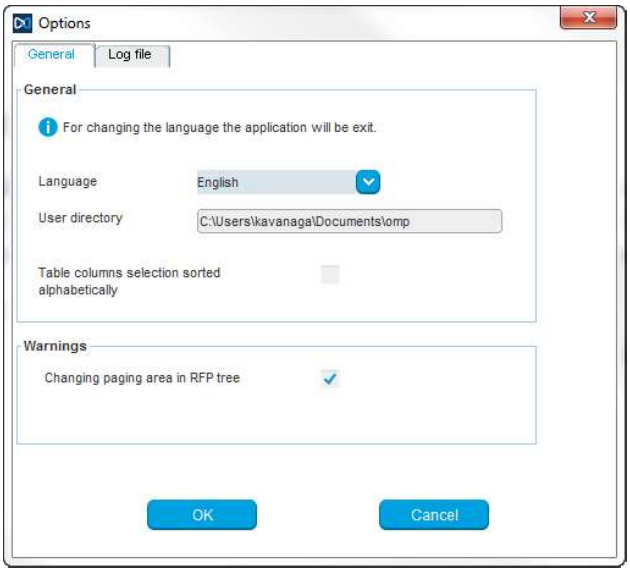
The “Locating” tab provides OM Locating license information.

6.14 “GENERAL” MENU

The **General** menu is available in all program situations. It contains following submenus:

- **Exit**: Selecting this menu entry opens the exit dialog to close the OMP.
- **Options**: Selecting this menu entry opens the **Options** dialog (see below).

“Options” - “General” tab



Language: You can select the OMP language. After changing the language, the OMP is automatically closed and must be started again.

The field **User directory** shows the path where the following files are saved if necessary:

- System dump file “sys_dump.txt”
- Expert console log file “spy.log” when the application terminates
- Exception log file “spy_trace_<date>_pxxx” in case of a Java exception, file name extension “xxx” ranges from 000 to 999

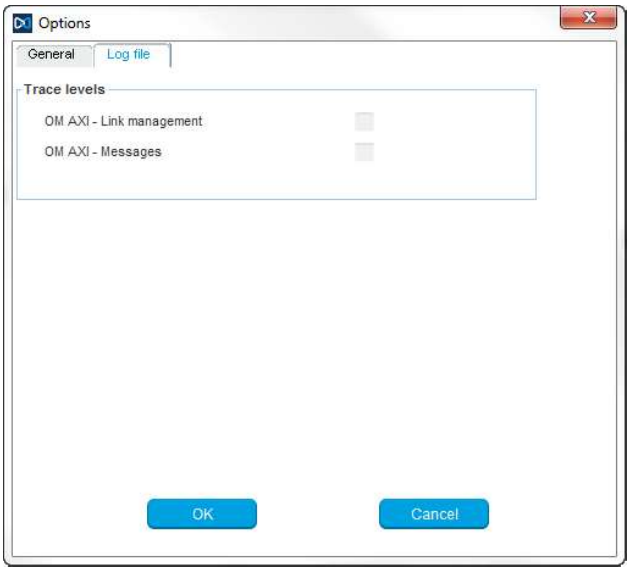
In the **Warnings** section you can activate/deactivate the display of warning messages in the OMP.

Notes on log files

The mechanism for creating the log files is the same as the PC OMM spy log mechanism, what means:

- The maximum size of the log file is 1 GB
- 1000 log files per day at maximum
- Only the 30 newest created log files are kept, older ones are removed automatically
- Log files older than 6 days are removed

“Options” - “Log file” tab

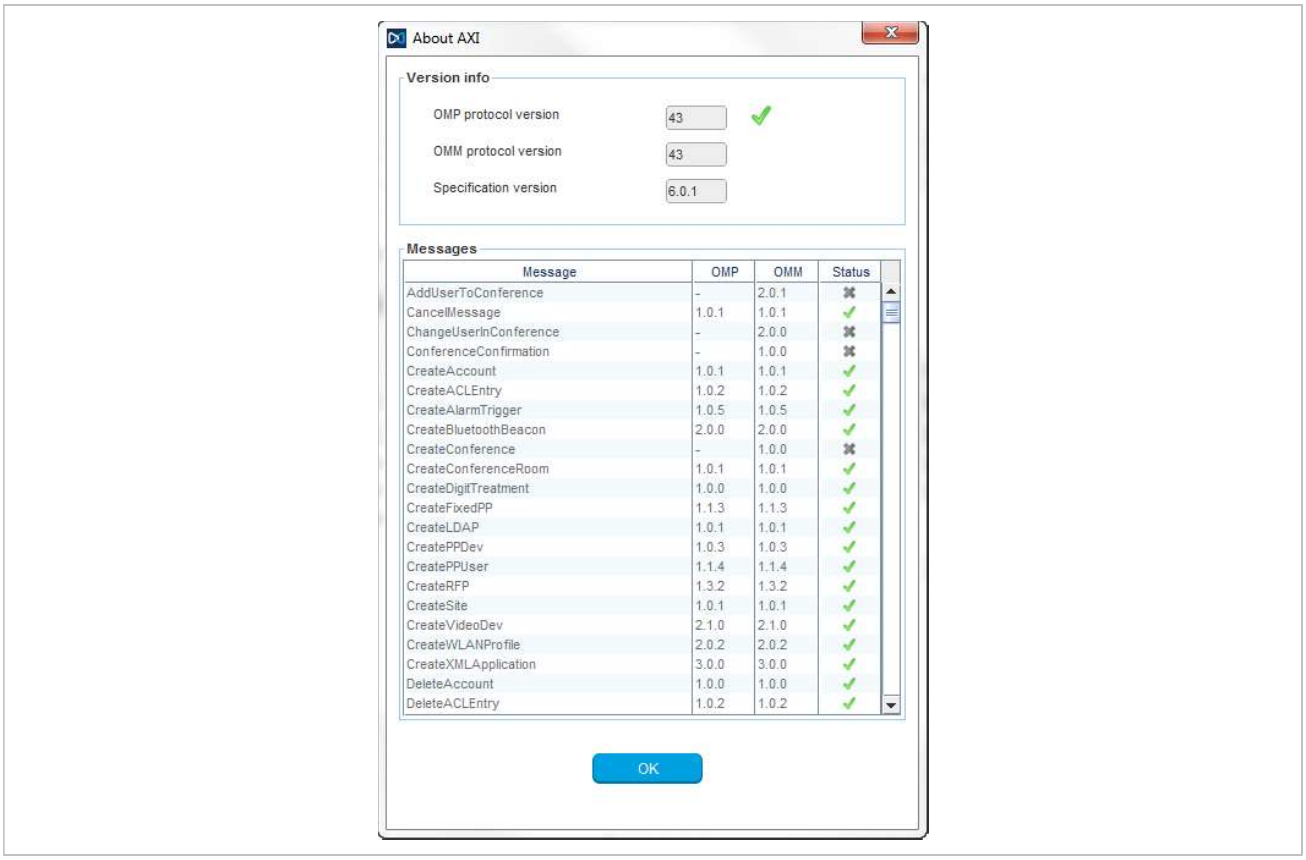


In the **Log file** tab you can enable several trace levels.

6.15 “HELP” MENU

The **Help** menu is available in all program situations. It contains following submenus:

- **Info**: Selecting this menu entry displays the End User License Agreement (EULA).
- **About AXI**: Selecting this menu entry displays the About AXI dialog. This dialog compares the protocol version numbers which are provided by the OMM with the protocol version numbers supported by the OMP. The warning icons ⚠ or ✖ show a version mismatch. A version number “-” means the protocol element is not used by OMP.



- **About OMP**: Selecting this menu entry displays the OMP version info and copyright.

7 DECT PHONE

The DECT phone has a special system menu for administration of the DECT system.

7.1 KEY LOCK WITH PIN

7.1.1 MAINTAIN THE PIN

The PIN is used to allow access to the Security menu and to lock the phone. The user can adjust his PIN and the feature Key lock with PIN here: System menu/Administration.

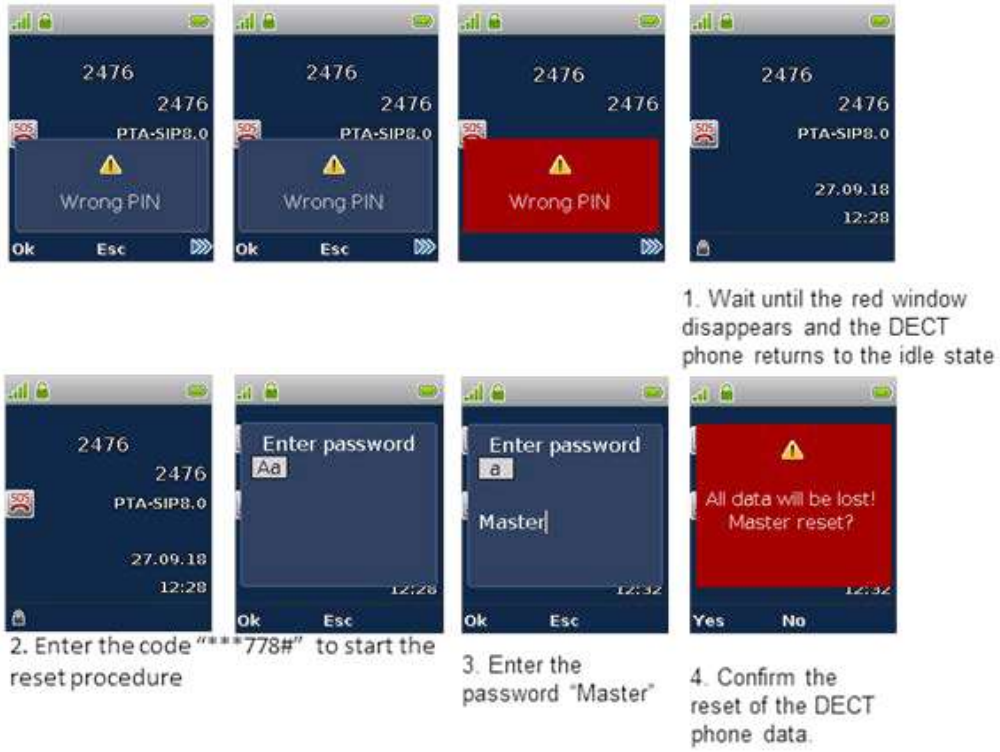
The submenu “Key lock” is hidden if the feature is disabled.

The update to SIP-DECT 7.1SP1 causes a reset of the DECT phone key lock PIN to default “0000”.

7.1.2 UNLOCK A LOCKED MITEL 600 DECT PHONE

As of SIP-DECT 8.0 and DECT phone SW 7.2, the DECT phone can be reset to factory defaults if the DECT phone is protected with a PIN, and no other option can be used to unlock the phone; for example, set the PIN through the OMM to a defined value.

If a wrong PIN are successively entered 3 times, then a reset procedure can be activated by entering the code “***778#”.



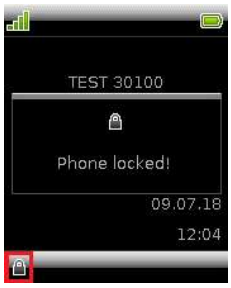
The reset procedure requests the password “Master” to reset all data on the phone, which also removes the subscription and the PIN lock.

The DECT phone needs to be subscribed with a DECT system after the reset.

Note: Be aware that the **Master reset** deletes all data from the DECT phone.

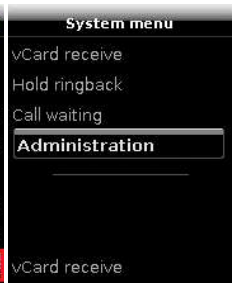
7.1.3 SETUP AUTOMATIC KEY LOCK WITH PIN

The following pictures show an example how to turn off the DECT phone key lock with PIN through the Mitel 600d DECT Phone UI.



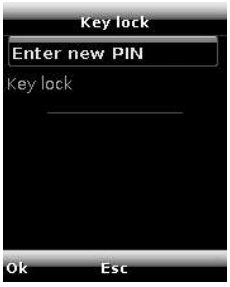
Select the lock key and enter the PIN to unlock the phone

Long press of the option soft key opens the system menu

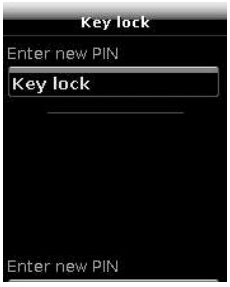


Select Administration

Select Key lock

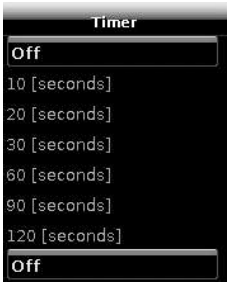


Option to change the PIN



Option to change the key lock parameter

Time for the automatic key lock is set to 120 seconds



Off and various timer values are available

Choose the desired value, for example, Off and confirm with OK

Confirmation that the chosen values is stored

Key lock with PIN is Turned Off

The update to SIP-DECT 7.1SP1 causes a reset of the DECT phone key lock PIN to default “0000”.

8 CONFIGURATION AND ADMINISTRATION

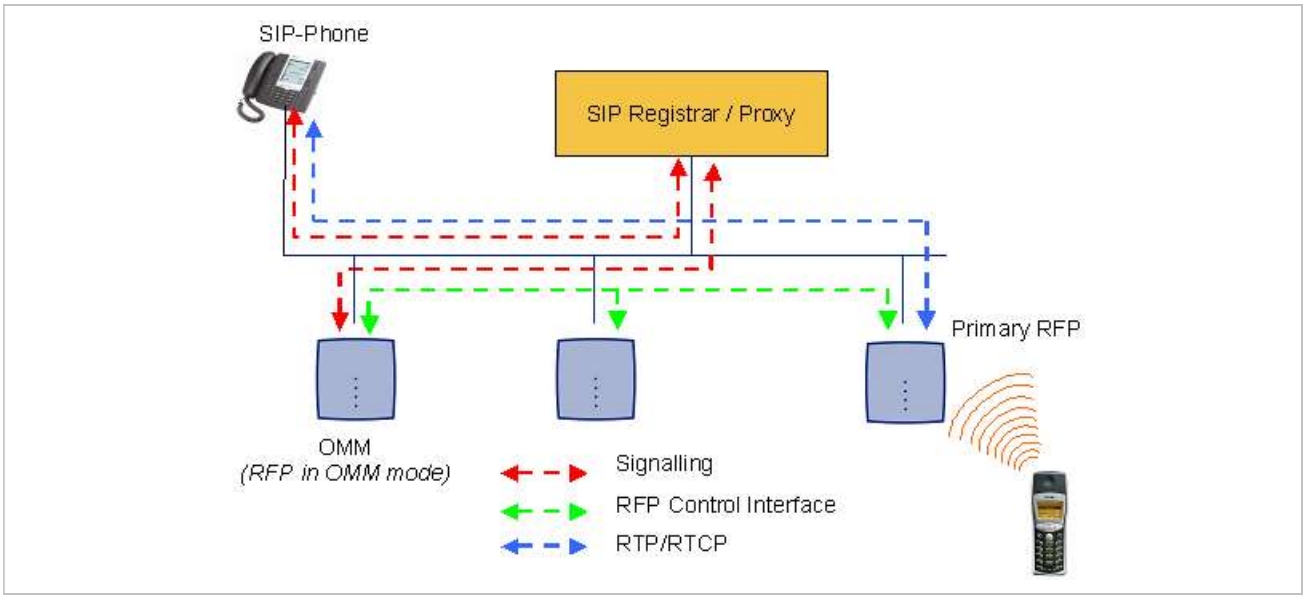
This section provides detailed information on various configuration and administration aspects of the SIP-DECT solution.

8.1 IP SIGNALING AND MEDIA STREAM

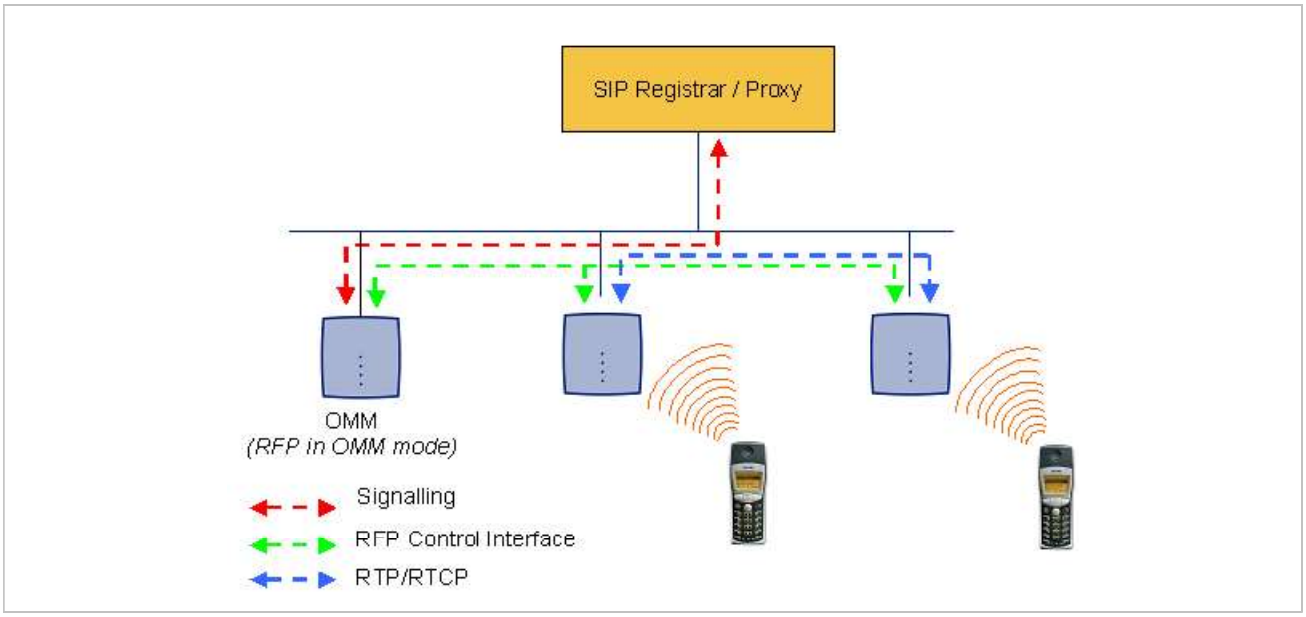
To establish a call between an IP Phone and a DECT phone (for example, Mitel 600), the following IP streams must be established:

- A signaling channel to and from the SIP phone.
- A signaling channel to and from the OMM.
- A control interface between the OMM and the RFP that has a connection to the DECT phone (known as the primary RFP).
- A Real Time Protocol (RTP) / Real Time Control Protocol (RTCP) connection between the SIP phone and the primary RFP.

The following figure illustrates this scenario.

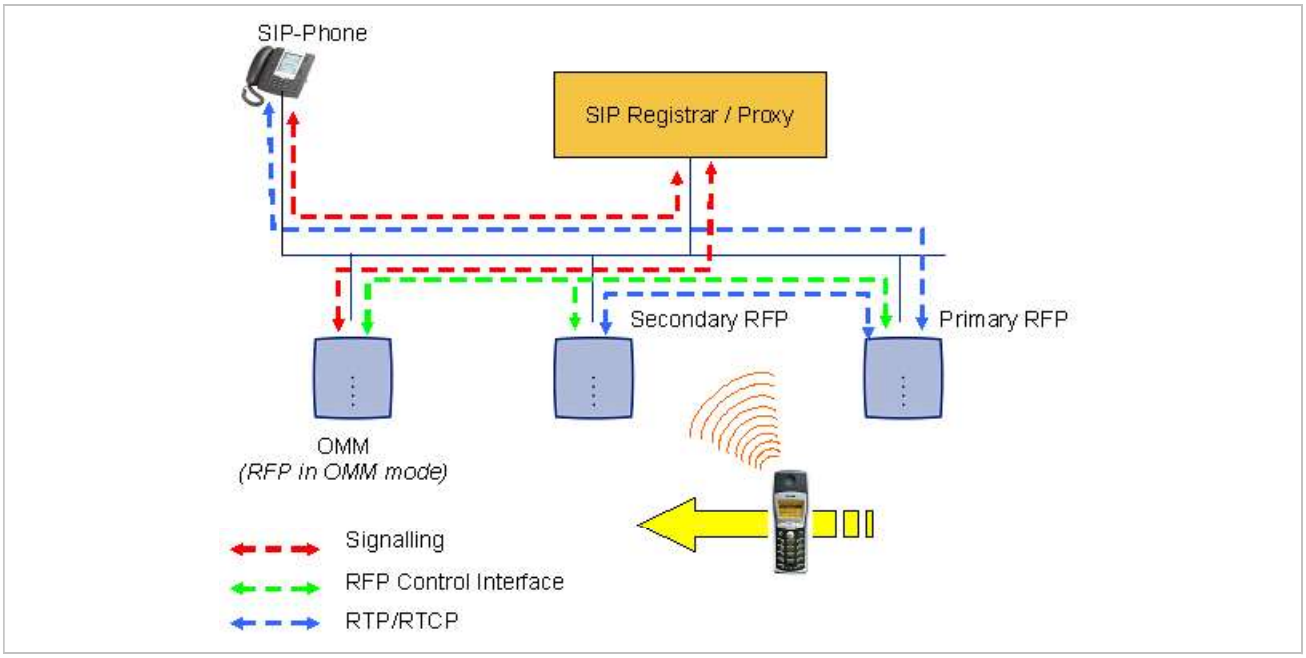


To establish a call between two DECT phones, the same IP streams must be established like in the scenario before, except the IP phone is not involved. The following figure illustrates this scenario.

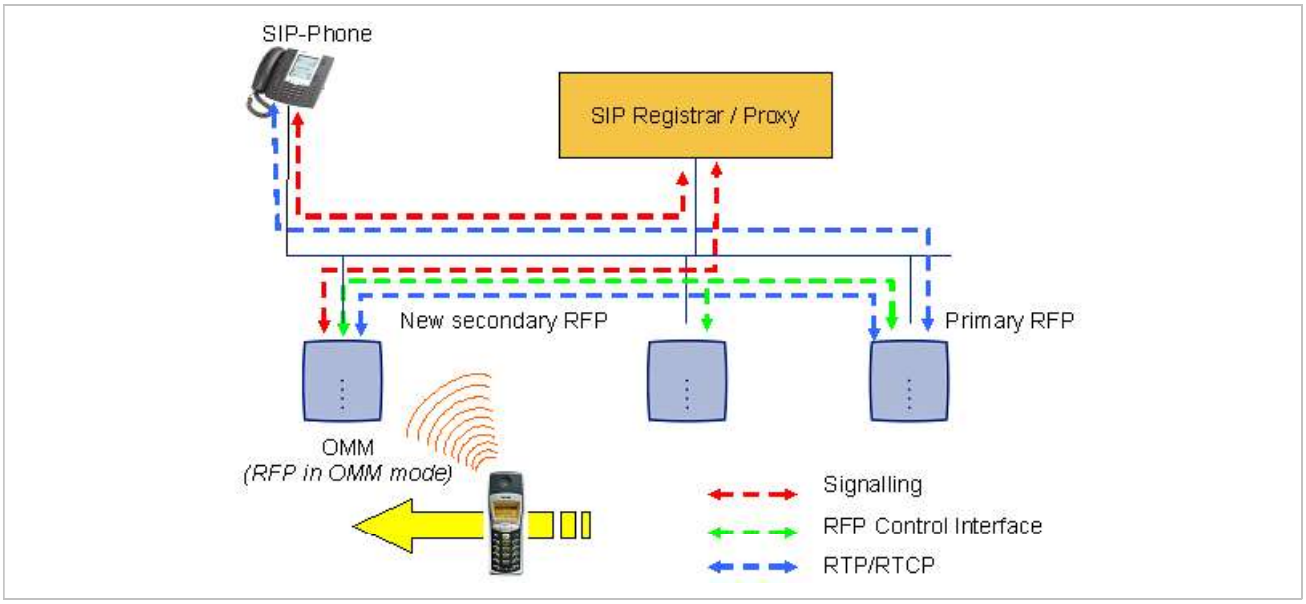


A call from one DECT phone to another that resides on the same RFP will loop back within the RFP if no media gateway is involved. So the call will not pass through to the Local Area Network (LAN). Although the voice packets will not impact LAN traffic, signal packets will.

If the DECT phone user is moving, the DECT phone detects that another RFP has a better signal strength and, therefore, it starts the handover process. The media stream from the IP phone cannot move to the secondary RFP, so the primary RFP uses the LAN to direct the voice to the secondary RFP, as shown in the following figure.



As the DECT phone user moves into the next RFP zone of coverage, the DECT phone detects that the RFP has a better signal strength. Again the media stream from the SIP phone cannot move to the secondary RFP, so the primary RFP uses the LAN to direct the voice to the new secondary RFP.

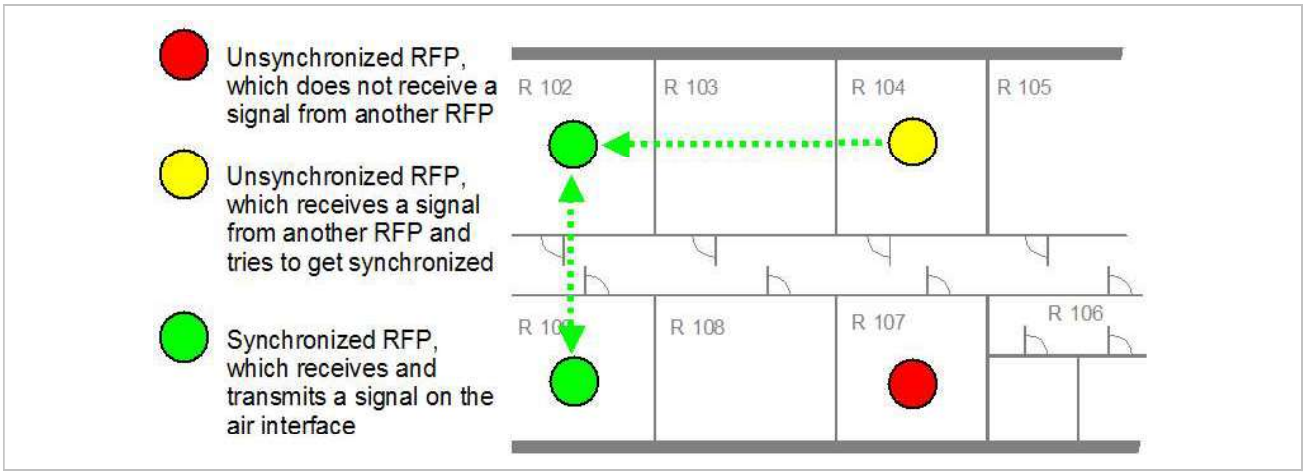


8.2 DECT BASE STATION SYNCHRONIZATION

To guarantee a seamless handover if a caller moves from one DECT base station zone of coverage to another DECT base station zone of coverage, an accurate synchronization of the DECT base stations is necessary.

The DECT base stations are synchronized over the air interface. The first DECT base station to complete startup transmits a signal on the air for the other DECT base stations to synchronize from. If a DECT base station gets in sync, it transmits a signal on the air and becomes the sync source for the next DECT base station. Only DECT base stations that can receive a synchronization signal become synchronized.

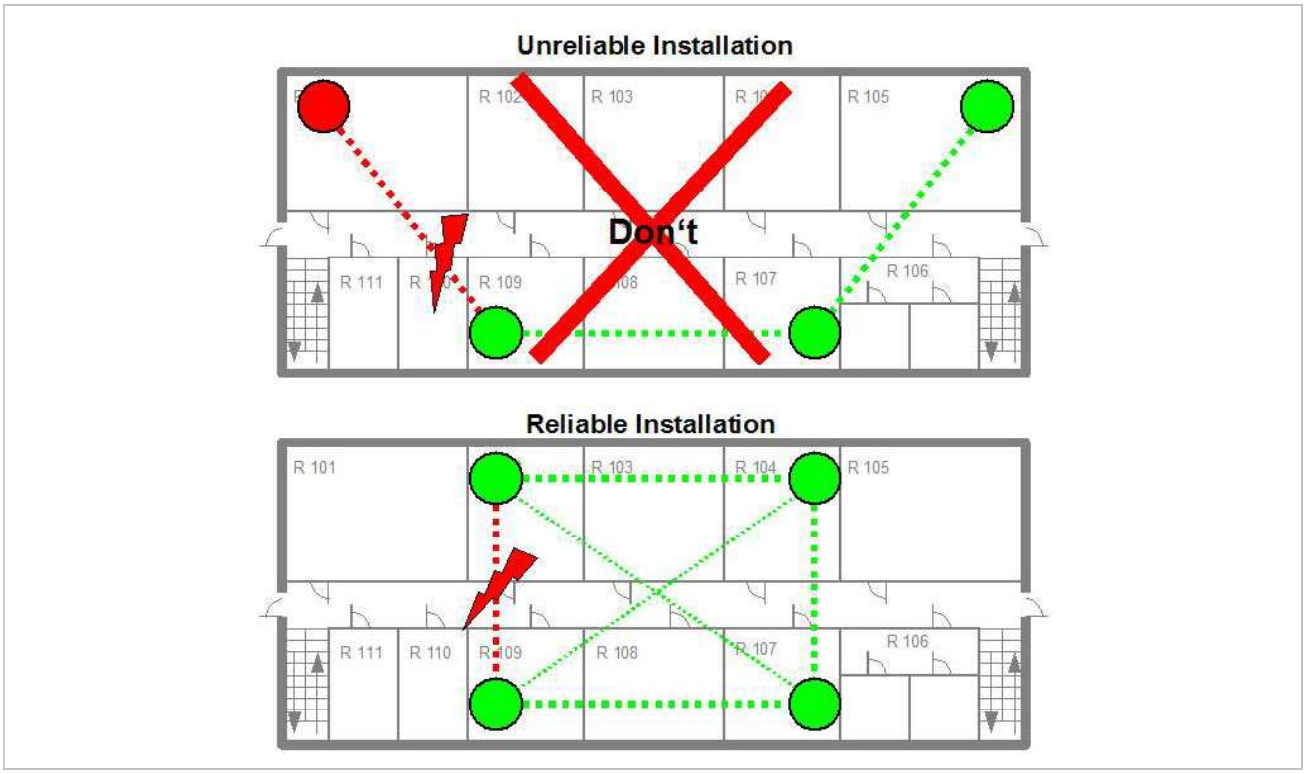
For the DECT base station to sync to another DECT base station, the signal strength cannot drop below -70 dBm. You must consider this requirement during the site survey.



As long as a DECT base station is not in sync, no calls can be established using this DECT base station.

If a DECT base station loses the synchronization, the DECT base station does not accept new calls (“busy bit”). There is a delay of maximum 3 minutes until the active calls on this DECT base station are finished. Then it tries to get synchronized again.

A SIP-DECT installation is more reliable if a DECT base station can receive the signal from more than only one DECT base station because the other signals are also used for synchronization.



The sync-over-air solution is very reliable because all existing redundant paths are used for synchronization. Thus, hardware tolerances have only very little influence. No DECT base station has a key position. Only unfavorable setups without redundant synchronization paths can cause problems.

Sometimes DECT base stations do not need to be synchronized (e.g. if they are in different buildings). These DECT base stations can be put into different clusters. DECT base stations in different clusters are not synchronized with each other. Different clusters start up at the same time independently.

8.2.1 INITIAL SYNCHRONIZATION PROCEDURE

To avoid synchronization problems and to speed up the synchronization on system startup, an initial synchronization procedure is used. For every cluster the following synchronization stages are defined.

- Synchronization stage 0
  - If at least one preferred DECT base station was configured, the synchronization process waits up to 30 seconds for an incoming startup message of such a preferred DECT base station. Receiving a message will finishing stage 0 and the synchronization process jumps to stage 1.
  - If no message is received within 30 seconds, this stage will be terminated and the next stage begins.
  - If no preferred DECT base station was configured, this stage is ignored.
- Synchronization stage 1
  - If a preferred DECT base station was determined in stage 0, this one becomes the synchronization source for the subsequent DECT base stations. Otherwise

the first DECT base station that sends a startup message becomes the synchronization source for the subsequent DECT base stations.

  - In this stage, only DECT base stations reporting an RSSI value better than -65 dBm are permitted to perform synchronization.
  - If a DECT base station has completede its synchronization, this DECT base station will be also a synchronization source for other upcoming DECT base stations.
  - The initial timeout for this stage is 30 seconds. Whenever a DECT base station has finished its synchronization in this stage a new stage timeout value is calculated.
  - If no DECT base station comes up within the timeout time or if all the upcoming DECT base stations do not fit the RSSI threshold, this stage will be terminated and the next stage begins.
- Synchronization stage 2
  - The behavior of this stage is identical to stage 1, but an RSSI threshold value of -70 dBm is significant.
- Synchronization stage 3
  - The behavior of this stage is identical to stage 1, but an RSSI threshold value of -75 dBm is significant.
- Synchronization finished
  - No more RSSI threshold value is significant. All DECT base stations that failed the stage conditions above are now permitted to perform synchronization.

The last level “synchronization finished” will be achieved either all registered DECT base stations of this cluster are synchronized or the timer of stage 3 expires.

8.2.2 CHECKING THE SYNCHRONIZATION OF A NETWORK

For every cluster a periodically check of the synchronization of the network is done. If the network is split into at least two subnets, all the RFPs of the lesser subnet(s) will be resynchronized. While doing initial synchronization procedure this check is deactivated. You can check the DECT base station synchronization from the **Sync view** menu of the OM Management Portal (OMP), see section 6.7.6.

8.3 DECT BASE STATION CHANNEL CAPACITY

The DECT base station has 12 available time slots on air; eight can have associated DSP/media resources for media streams. All DECT time slots are used for control signaling, software download over air, messaging and bearer handover independent of associated DSP/media resources.

If all eight media stream channels are used, the DECT base station announces a “busy bit”. In that case, the DECT phones determine whether another DECT base station has an appropriate signal strength. If so, the DECT phone performs a handover to that DECT base station. Once the handover is complete, the DECT base station lowers its “busy bit”.

Whenever the busy state is announced a log entry is made to the system logs. If the announcement of busy raises in a specific area, an additional DECT base station should be installed to double the number of media streams available for calls.

Notes on Hi-Q connections

Each Hi-Q connection uses twice the capacity of conventional narrowband on the DECT air interface. Due to this fact, four Hi-Q connections (instead of eight) can be established via one DECT base station.

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

8.4 NETWORK INFRASTRUCTURE PREREQUISITES

To establish and maintain an SIP-DECT installation, a network infrastructure is assumed, which comprises at least the following components:

- DECT base stations
- DECT phones
- IP PBX/media server (for example, Asterisk)
- TFTP server

Depending on the operational modes the following services should be provided:

- DHCP
- TFTP
- SNTP
- DNS
- LDAP
- Syslog daemon

Notes on network infrastructure prerequisites

- In NA outdoor RFPs may only be installed with the antennas shipped with the units. No other antennas or cabling are permitted. In EMEA the outdoor RFPs are shipped without antennas and you may use the units with one of the optional antennas (separate order no.).
- A TFTP server is no longer required for boot of a 3rd or 4th generation RFPs.
- TFTP, FTP(S), HTTP(S), SFTP are supported for 3rd or 4th generation RFPs software update.

8.5 SIP-DECT STARTUP

This section contains detailed information on the startup (booting) process of the SIP-DECT solution.

For booting 2nd generation RFPs, there must be at least one TFTP server on the attached network to load the OMM/RFP application software.

3rd or 4th generation RFPs uses the internal flash to start the boot image. A fileserver is only needed for software update over the network.

The essential network settings can be alternatively:

- Communicated by a DHCP server at startup time.
- Configured on the RFP with the OM Configurator tool (see section 7.6). The settings made by the OM Configurator will be saved permanently in the internal flash memory of each OMM/RFP.

8.5.1 TFTP AND DHCP SERVER REQUIREMENTS

TFTP server requirements

The DECT base station obtains the boot image file from a TFTP server. The requirement list for the used TFTP server is defined as follows:

- The support of RFC 1350 /1/ is mandatory.
- To accelerate the download of a boot image file for older 2nd generation DECT base stations, it is possible to increase the packet size of the transmitted TFTP packets from 512 bytes per packet to 1468 bytes per packet. To use this optional feature, the TFTP server must support RFC 2347 /3/ and RFC 2348 /4/.
- To reduce the overall download time of the older 2nd generation DECT base stations in a system, it is possible to use TFTP multicast download. To use this optional feature, the TFTP server must support RFC 2090 /2/ and RFC 2349 /5/.

To use the TFTP multicast option, the attached network must support multicast too. Furthermore a support of IGMP, RFC 2236 /6/ is required.

Note: If many DECT base stations loading the boot image simultaneously, the network load could increase significant. To balance the network load or for backup reasons, it is possible to configure more than one TFTP server in a network.

DHCP server requirements

A DHCP server needs to support RFC 2131 /9/. The TFTP and DHCP server need not to reside on the same host.

8.5.2 BOOTING STEPS

Booting is performed in two steps:

1 Starting the boot process.

2 Starting the application.

Booter startup

On startup each DECT base station tries to determine its own IP address and other settings of the IP interface from the configuration settings in the internal flash memory. If no settings are available or these settings are disabled, the DECT base station tries to determine these settings via DHCP. Depending on the DECT base station type, the DECT base station software is to be loaded:

- A 3rd generation DECT base station gets the application image from internal flash memory.

- An older 2nd generation DECT base station only has a small standalone application built into the flash. This software realizes the so-called net boot process. The RFP gets the application image file from the TFTP server.

Application startup

After starting the application image, the RFP software checks the local network settings in its internal flash memory. If no settings are available or if they are disabled, the RFP software starts a DHCP client to determine the IP address of the OMM and other application startup settings.

The RFP software acquires the OMM IP address:

- within the local network settings if active
- through DHCP request
- DECT base station configuration file (see 8.7.7)

If the IP address of the actual RFP device matches one of the acquired OMM IP addresses, the DECT base station software continues in OMM mode. Otherwise, the DECT base station runs as normal DECT base station without OMM mode.

Note: Only 3rd generation DECT base stations are able to run in OMM mode while older 2nd generation DECT base stations cannot function as OMM.

8.5.3 BOOTER STARTUP

The SIP-DECT DECT base station software includes a booter with the following features:

- VLAN can be configured via the OM Configurator without a static IP configuration. This means that the first DHCP request will be done by using VLAN.
- To balance the network load with older 2nd generation RFP devices, up to three TFTP servers can be configured. This can be done using the OM Configurator (local setting) or using the DHCP option 150. Before starting the download, the TFTP server will be selected randomly by the booter. But, if the option “Preferred TFTP server” was set by the OM Configurator, the option “TFTP server address” will specify the TFTP server to use. No randomly selection will be done in this case.
- Older 2nd generation RFPs only: to reduce the number of TFTP packets sent by the TFTP server, the packet size can be increased. This will be done by using a TFTP option (see 8.5.1 “TFTP server requirements”).
- Older 2nd generation RFPs only: Multicast TFTP download is possible if the TFTP server and the connected network support this.
- To indicate the actual state of the booter, the LEDs of the RFP will be used (see 8.5.5).

8.5.3.1 DHCP Client

Within the initial boot process the DHCP client supports the following parameters:

- IP address mandatory
- Net mask mandatory
- Gateway mandatory

- Boot file name mandatory for older RFPs
- TFTP server mandatory for older RFPs
- Public option 224: “OpenMobility” / “OpenMobilitySIP-DECT” mandatory
- VLAN-ID optional
- TFTP server list optional

8.5.3.1.1 DHCP Request

The DHCP client sends the vendor class identifier (code 60) “OpenMobility3G” (3rd generation RFPs) or “OpenMobility” (older 2nd generation RFPs) and requests the following options in the parameter request list (code 55):

- Subnet mask option (code 1)
- Router option (code 3)
- VLAN ID option (code 132)
- TFTP server list (code 150)
- Public option 224 (code 224) *(string “OpenMobility” or “OpenMobilitySIP-DECT”)*
- Public option 225 (code 225) *(*VLAN ID, not relevant for SIP-DECT)
- Public option 226 (code 226) *(not relevant* for SIP-DECT)

8.5.3.1.2 DHCP Offer

The DHCP client selects the DHCP server according to the following rules:

- The **public option 224** (**code 224**) has a value equal to the string “OpenMobility”,

or

- The **public option 224** (**code 224**) has a value equal to the string “OpenMobilitySIP-DECT”.

If none of the two rules above match, the DHCP offer is ignored.

Information retrieved from the DHCP offer:

- The IP address to use is taken from the **yiaddr** field in the DHCP message.
- The IP net mask is taken from the **subnet mask option (code 1)**.
- The default gateway is taken from the **router option (code 3)**.
- The TFTP server IP address is taken from the **siaddr** field in the DHCP message and additionally DHCP option 150, if available.
- The boot image filename is taken from the **file** field in the DHCP message, if this field is empty, the default filename is used.

8.5.3.1.3 Retries

If the DHCP client does not get an appropriate DHCP offer, a new DHCP request is send after 1 second. After 3 DHCP requests are sent the DHCP client will sleep for 60 seconds. During this time the booter accepts a local configuration with the OM Configurator.

This cycle repeats every 3 minutes until either **all** the required DHCP options are provided or the system is manually configured using the OM Configurator tool.

8.5.3.2 TFTP Client

The TFTP client will download the application image from the TFTP server. Both TFTP server and the name of the application image are supplied via the DHCP client. The application image is checksum protected.

Downloading the application image via TFTP is mandatory for older 2nd generation RFPs only. 3rd generation RFPs will load the application image from the internal flash, and (if configured) also download the application image via TFTP for update.

8.5.3.3 Booter Update

With older second generation RFPs, each application software image comes with the latest released booter software. The application software will update the booter automatically. With third generation RFPs, the booter will only be updated if you update the software.

If you downgrade the RFP's application software image to an older release, the booter does not downgrade automatically. In addition, if you want to use the OM Configurator tool (see 8.7), the OM Configurator version must match the booter software version.

8.5.4 APPLICATION STARTUP

After successfully starting the application software, the DECT base station checks the local network settings in its internal flash. If no settings are available or if they are disabled, it starts a DHCP client to determine the IP address of the OMM and other application startup settings.

8.5.4.1 DHCP Client

The DHCP client is capable of receiving broadcast and unicast DHCP replies. Therefore the flags field is `0x0000`. The DHCP request contains the well-known magic cookie `(0x63825363)` and the end option `(0xFF)`.

Parameters

The following parameters are supported within this step:

Option / Field	Meaning	Mandatory
yiaddr	IP address of the IP-RFP	yes
siaddr	Parameter named "Boot Server Host Name" with value as the IP address of the TFTP server	no (3G/4G RFPs) yes (older 2G RFPs)
file	Parameter named "Bootfile Name" with value of the path (optional) and name of the application image. For example "iprfp3G.dnld" (3rd generation RFPs) and "iprfp4G.dnld" (4th generation RFPs), or "iprfp2G.tftp" (older 2nd generation RFPs).	no (3G/4G RFPs) yes (older 2G RFPs)
option 1	Subnet mask	no
option 3	Default Gateway	no
option 6	Domain Name Server	no

Option / Field	Meaning	Mandatory
option 15	Domain Name	no
option 42	IP address of a NTP server	no
option 43	Vendor-specific options (see table below)	yes
option 66	Provisioning URL for the OMM (ConfigURL). URL of an external server that provides configuration files for the Base Station(s) hosting the OMM. **Note**: In SIP-DECT 2.1 - 6.1, this option was used for the RFP Config file server. If you want to specify a URL for the RFP Config file server, use option 233 instead.	no
option 132	VlanId	no
option 150	TftpServerIpList	no
option 224	Parameter named magic_str must be set to value "OpenMobility" or "OpenMobilitySIP-DECT".	yes
option 226	Enabling 802.1X feature (set to 1).	no
option 233	URL that specifies the protocol, server and path to access the DECT base station configuration files (see section 7.9). For SIP-DECT 6.1 or earlier, this option takes priority over option 66 when set.	no
option 234	Provisioning URL for the OMM (ConfigURL). URL of an external server that provides configuration files for the Base Station(s) hosting the OMM.	no
option 236	This mode value determines which instance (OMM, RFP) shall use the given Provisioning URL (Option 43-2, 66 or 234). Valid values are: 1. The RFP shall use the given Provisioning URL. 2. The OMM and RFP shall use the given Provisioning URL. Else: The OMM shall use the given Provisioning URL.	no

Vendor specific options

The Vendor Specific Options consist of:

Vendor Specific Option	Meaning	Length	Mandatory
option 10	ommip1: Used to select the IP-RFP that hosts the Open Mobility Manager (OMM).	4	yes
option 14	syslogip: IP address of a Syslog Daemon	4	no
option 15	syslogport: Port of a Syslog Daemon	2	no
option 17 (SIP-DECT 5.0 and older)	Country: Used to select the country in which the OMM resides. This enables country specific tones (busy tone, dial tone, …).	2	no

option 18 (SIP-DECT 5.0 and older)	ntpservname: Name of a NTP Server	x	no
option 19	ommip2: Used to select a secondary IP-RFP that hosts the standby Open Mobility Manager (OMM). This option must be included if the OMM Standby feature is used (see section 7.15).	4	no
option 43 sub-option 1 (SIP-DECT 6.2 and later)	URL that specifies the protocol, server and path to access the DECT base station configuration files (see section 7.9).		no
option 43 sub-option 2	Provisioning URL for the OMM (ConfigURL). URL of an external server that provides configuration files for the Base Station(s) hosting the OMM.		no
option 43 sub-option 226	Enable 802.1x feature (set to 1).	1	no

Example

An example of the minimal contents for the Option 43 parameter value would be:

0a 04 C0 A8 00 01 where “C0 A8 00 01” represents “192.168.0.1” for the OMM IP.

The option 43 contains a string of codes in hex the format is “option number” “length” “value” in this example
0a = option 10 (ommip1)
04 = following value is 4 blocks long
C0 A8 00 01 = 192.168.0.1

If there is more than one option, add the next option at the end of the previous one. Depending of the DHCP server you must end the option 43 with FF.

Country specific tones (SIP-DECT 5.0 and older ONLY)

Tones for the following countries are supported:

Country code	Country		Country code	Country
1	Germany		15	Hungary
2	Great Britain		16	Poland
3	Switzerland		17	Belarus
4	Spain		18	Estonia
6	Italy		19	Latvia
7	Russia		20	Lithuania
8	Belgium		21	Ukraine
9	Netherlands		22	Norway
10	Czechoslovakia		24	Sweden
11	Austria		25	Taiwan
12	Denmark		100	North America
13	Slovakia		101	France

14	Finland		102	Australia

8.5.4.2 Configuration using DHCP

The DHCP client of the RFP family requests several parameters that are used to configure the RFP. The DHCP client vendor class identifier (option 60) is different for the different RFP generations:

- 3rd generation RFPs (RFP 35/36/37 IP / RFP 43 WLAN) use “OpenMobility3G”.
- 4th generation RFPs (RFP 44/45/47 IP / RFP 48 WLAN) use “OpenMobility4G”.
- Older 2nd generation RFPs (RFP 32/34 / RFP 42 WLAN use) “OpenMobility”.

BOOTP/DHCP Option	Meaning	Type	Remarks
siaddr	IP address of the TFTP server	4 octets	Optional for 3G/4G RFPs for SW update; Mandatory for older 2G RFPs because of the NETBOOT process;
File	Path to the boot image server by the TFTP server	N octets	Optional for 3G and 4G RFPs for SW update; Mandatory for older 2G RFPs because of the NETBOOT process
150	TFTP server list	N * 4 octets	Only used by the NETBOOT process of older 2G RFPs
224	Magic String	“OpenMobility” or “OpenMobilitySIP-DECT”	The client uses this option to select the server, mandatory

* The magic string “OpenMobilitySIP-DECT” instead of “OpenMobility” (as defined in SIP-DECT 2.x) makes sure that a SIP-DECT software is loaded into 3rd or 4th generation RFPs eventhough a different, non-SIP-DECT SW is previously installed and running.

8.5.4.3 Selecting the Right DHCP Server

The DHCP client requests its own IP address using code 50. The DHCP client will select the DHCP server that offers the currently used IP address. Additionally the mandatory options must be offered otherwise the DHCP offer is ignored by the DHCP client.

If no matching reply was received, the DHCP client resends the request 2 times after 1 second. Then the DHCP client will wait for 1 minute before resending 3 requests again.

If the DHCP client cannot accept a DHCP offer within 30 minutes, the RFP is rebooted.

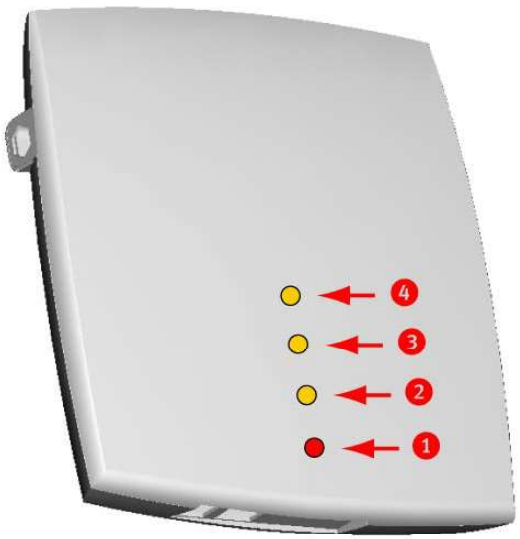
8.5.5 RFP LEDS

8.5.5.1 3rd Generation RFPs

- RFP 35 IP
- RFP 36 IP
- RFP 37 IP
- RFP 43 WLAN

8.5.5.1.1 LED States

RFP 32/34 IP
RFP 32/34 NA
RFP 35/36 IP



LED 1 Info / Booter; LED 2 System;
LED 3 DECT; LED 4 (unused)

RFP 42 WLAN
RFP 43 WLAN

LED 1 Info / Booter; LED 2 System
LED 3 DECT; LED 4 WLAN

8.5.5.1.2 Booter LED Status

RFP 35/36 IP, RFP 43 WLAN

The RFP 35/36 IP and RFP 43 WLAN booter uses LED1 for signaling its activity. After power up, the LED 1 (INFO) is red. The successful start of the boot image is signaled by the LED 1 turning orange.

RFP 32/34 IP, RFP 32/34 NA, RFP 42 WLAN

The following table illustrates the different meaning of the LEDs while the booter is active.

	LED1 (INFO)		LED2 (OMM / SYSTEM)		LED3 (DECT)		LED4 (WLAN)		
Booter	cont.								Power connected
	cont.		cont.		cont.		cont.		Wait for OMM Configurator Input
	1s	1s							DHCP
	1,9s	0,1s	cont.		cont.		cont.		DHCP failed, wait for OMM Configurator Input
	0,25s	0,25s							TFTP download after DHCP
	0,25s	0,25s	cont.						TFTP download after local configuration
	0,25s	0,25s			cont.				TFTP download after DHCP Multicast
	0,25s	0,25s	cont.		cont.				TFTP download after local configuration and multicast
	3,9s	0,1s	cont.		cont.		cont.		TFTP failed, wait for OMM Configurator Input
Now, the kernel / application is running: LED1 will never be RED									

8.5.5.1.3 Application LED Status

The following tables illustrate the different meaning of the LEDs while the application is starting or active.

RFP 35/36 IP, RFP 43 WLAN

	LED1 (INFO)		LED2 (OMM / SYSTEM)		LED3 (DECT)		LED4 (WLAN)		
Kernel	cont.								kernel boot phase (inflator, …)
RFPM	1s	1s							DHCP phase
	1,85s	0,5s							DHCP failure (idle loop)
	0,5s	0,5s							obtaining external configuration
	0,85s	0,15s							external configuration failure
	cont.								Ready

	LED1 (INFO)		LED2 (OMM / SYSTEM)		LED3 (DECT)		LED4 (WLAN)		
	1,85s	0,15s							Up & running + RFP houses OMM
RFP general			1s	1s					OMM connect phase
			1,85s	0,15s					OMM connection failure (idle loop)
			cont.						Up & running (OMM connected)
			1,85s	0,15s					Up & running + OMM warning
			1,85s	0,15s					Up & running + OMM failure
RFP DECT					cont.				DECT not configured on this RFP
					1,85s	0,15s			DECT inactive (not synced yet)
					cont				DECT 'on air'
					1,85s	0,15s			DECT + call active
					1,85s	0,15s			DECT + call active +busy bit
RFP WLAN							cont.		WLAN not configured on this RFP
							1,85s	0,15s	WLAN inactive yet
							cont.		WLAN 'on air'
							1,85s	0,15s	WLAN + assoc. clients
							cont.		WLAN failure (e.g. 10 Mbit/s uplink)
Reboot request	cont.		cont.		cont.		cont.		RFP will reboot

8.5.5.2 4th Generation RFPs

- RFP 44
- RFP 45
- RFP 47 and RFP 47 DRC (Indoor and Outdoor Unit)
- RFP 48 WLAN

See the section 1.2.1.1 RFP 4G DECT Base Station family for more information.

8.5.5.2.1 LED States

The following tables show the LED status of an RFP according to the different states.

A red respectively orange colored field in the table means that the LED glows permanently in red or orange. A split field with e.g. the specification 1s/1s means that the LED is flashing with a frequency of one second LED red on and one second LED off. Grey means that the LED is off.

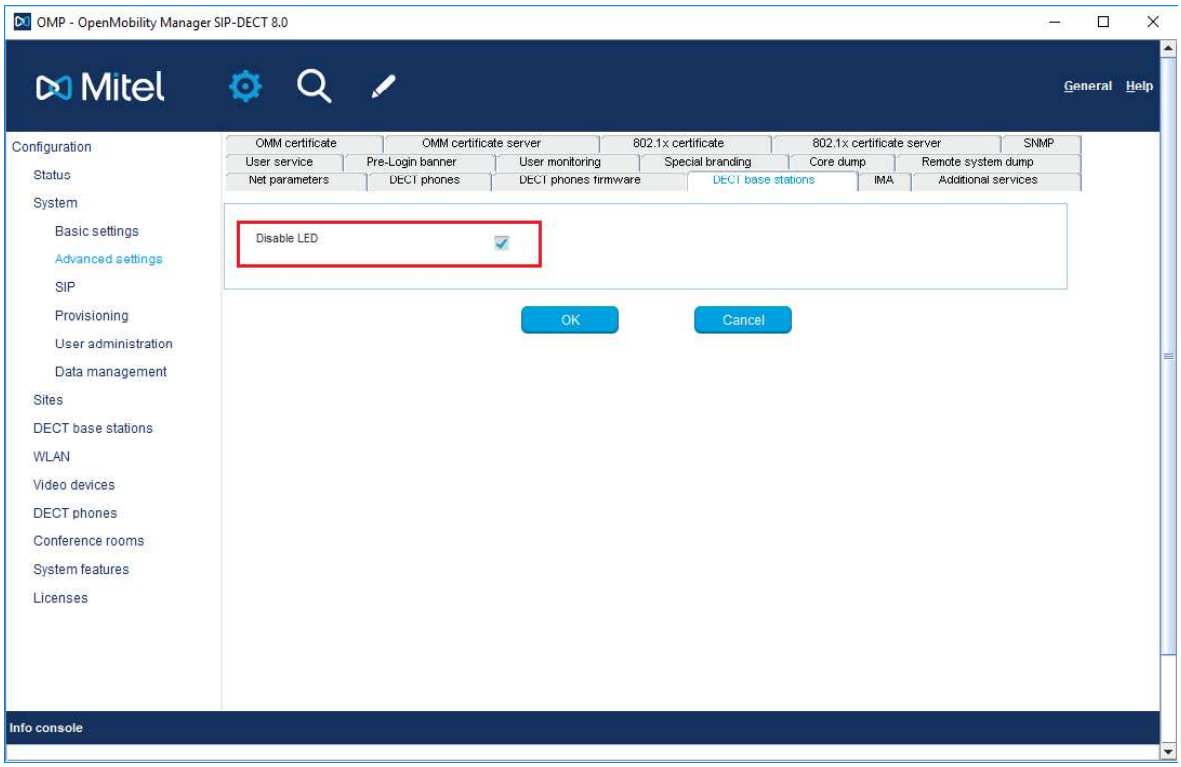
The new RFP family is equipped with one colored LED, which shows the individual states of the 4th generation RFP.

LED color/rhythm		Description
continuous		Booter phase
continuous		Kernel boot phase
1s	1s	Configuration phase
1,9s	0,1s	DHCP failure (idle loop)
continuous		System up and Running (with or without OMM)
1s	1s	OMM connection phase
continuous		OMM connected
1s	1s	DECT inactive (not synced yet)
continuous		DECT “on air”
continuous		WLAN “on air”
1s	1s	DECT inactive (not synced yet) + WLAN “on air”
continuous		DECT + WLAN “on air”
0,1 sec	0,1 sec	Button pressed: 0 sec < t < 3 sec = no action
0,1 sec	0,1 sec	Button pressed: 3 sec < t < 8 sec = Activate Cloud-Id
0,1 sec	0,1 sec	Button pressed: 8 sec < t < 10 sec = no action
0,1 sec	0,1 sec	Button pressed: 10 sec < t < 15 sec = Factory Reset
0,1 sec	0,1 sec	Button pressed: 15 sec < t < oo = no action

8.5.5.2.2 Turning Off the RFP 4G LED

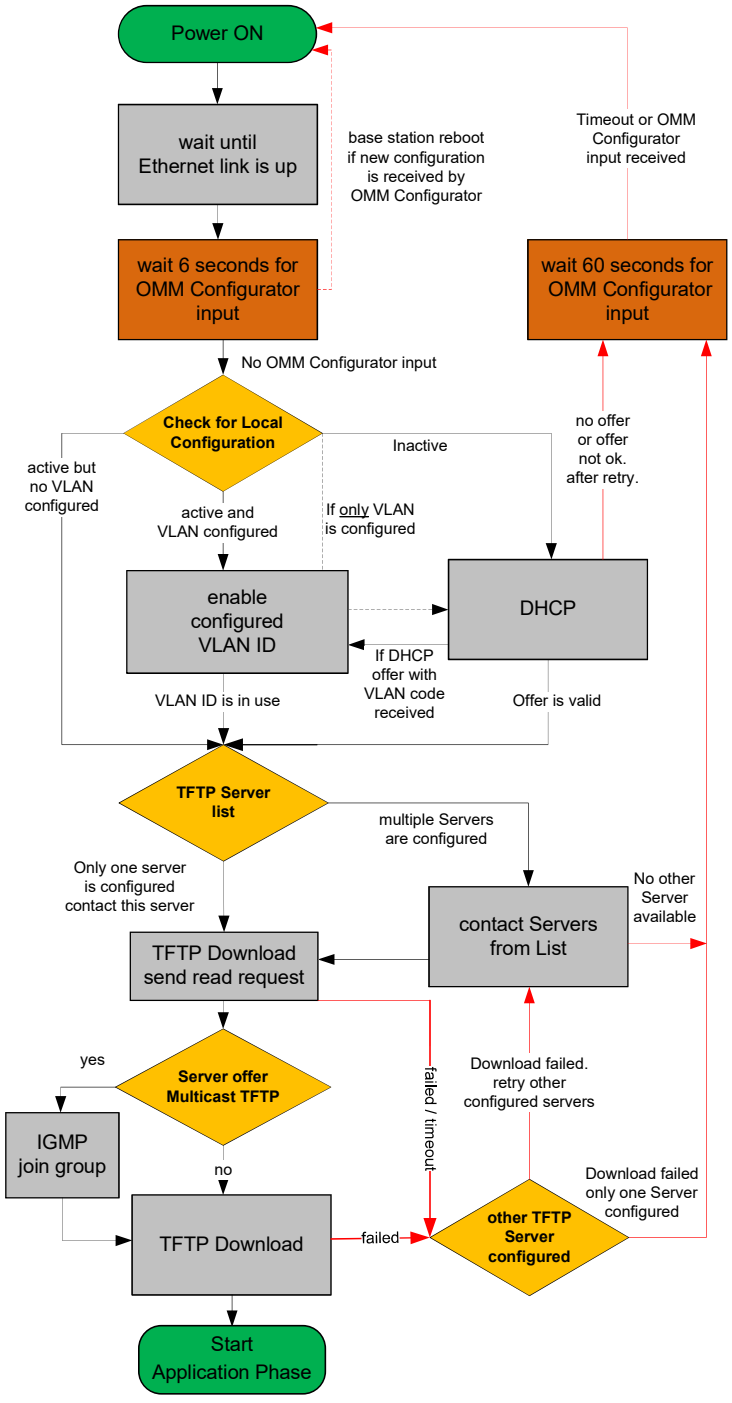
To turn off the RFP 4G LED,

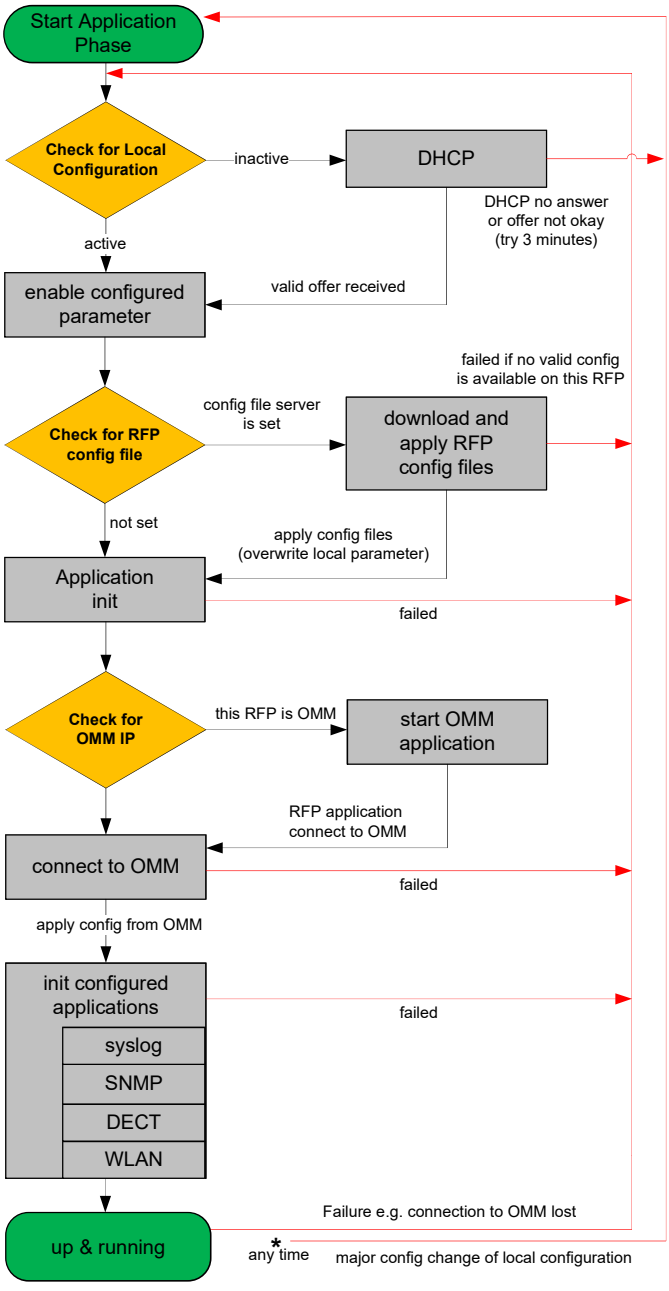
1. Go to the **DECT base stations** tab.
2. Select the **Advanced settings** option and select the **Disabled LED** check box to disable the LED for the active DECT and WLAN states.



8.6 STATE GRAPH OF THE START-UP PHASES

The following figure illustrates the start-up phase for older 2nd generation RFPs. 3rd and 4th generation RFPs use a similar start-up sequence, but they start with the application phase (see below).


Power ON
wait until Ethernet link is up
base station reboot if new configuration is received by OMM Configurator
Timeout or OMM Configurator input received
wait 6 seconds for OMM Configurator input
wait 60 seconds for OMM Configurator input
No OMM Configurator input
Check for Local Configuration
active but no VLAN configured
active and VLAN configured
Inactive
If only VLAN is configured
no offer or offer not ok. after retry.
enable configured VLAN ID
DHCP
If DHCP offer with VLAN code received
VLAN ID is in use
Offer is valid
TFTP Server list
multiple Servers are configured
Only one server is configured contact this server
No other Server available
contact Servers from List
TFTP Download send read request
yes
Server offer Multicast TFTP
failed / timeout
Download failed. retry other configured servers
IGMP join group
no
Download failed only one Server configured
TFTP Download
failed
other TFTP Server configured
Start Application Phase


Start Application Phase
Check for Local Configuration
inactive
DHCP
DHCP no answer or offer not okay (try 3 minutes)
active
enable configured parameter
valid offer received
failed if no valid config is available on this RFP
Check for RFP config file
config file server is set
download and apply RFP config files
not set
apply config files (overwrite local parameter)
Application init
failed
Check for OMM IP
this RFP is OMM
start OMM application
RFP application connect to OMM
connect to OMM
failed
apply config from OMM
init configured applications
failed
syslog
SNMP
DECT
WLAN
Failure e.g. connection to OMM lost
up & running
* any time
major config change of local configuration

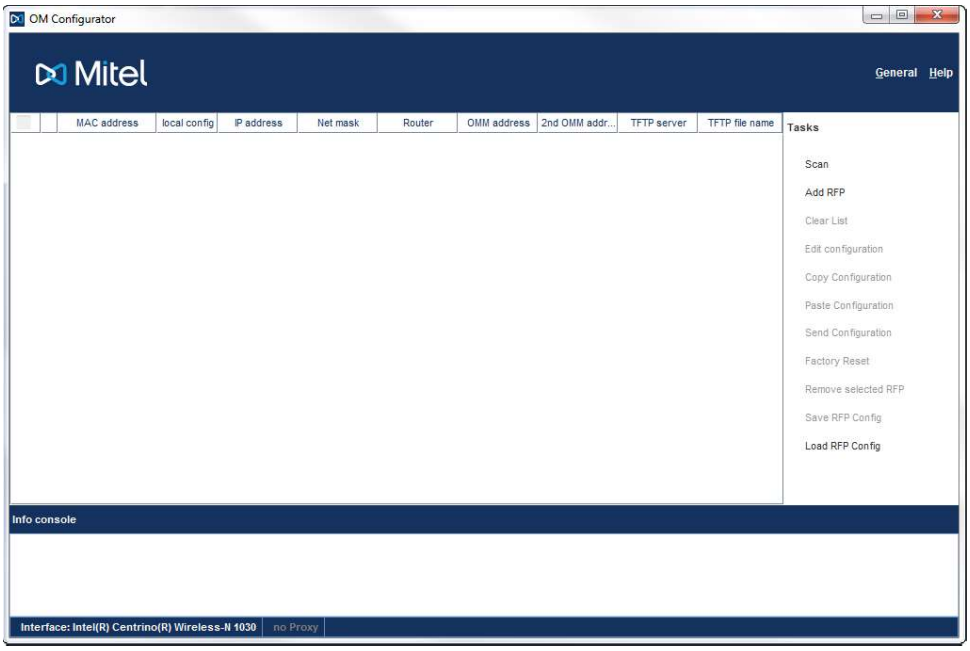
8.7 LOCAL DECT BASE STATION CONFIGURATION (OM CONFIGURATOR)

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

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

Please note: An initial configuration of the 3rd or 4th generation RFPs through the OM Configurator tool requires a login and password. The default login and password is “omm” and “omm”. No login is required for the initial configuration of the previous RFP family (2nd generation). If the RFP is configured by the OMM later on, the OMM also sets the configuration password. You must enter the OMM’s full access user and password in the OM Configurator tool then.

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



8.7.1 SELECTING THE NETWORK INTERFACE

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

8.7.2 ADDING DECT BASE STATIONS FOR CONFIGURATION

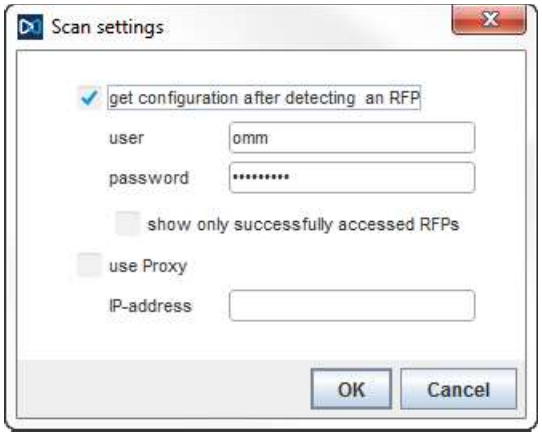
Before you can configure an RFP, you must add the RFP to the OM Configurator database. You can add an RFP record by:

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

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

8.7.3 SCANNING FOR DECT BASE STATIONS

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



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

You initiate the scan process by clicking **OK** button. The OM Configurator adds the results to the table.

In rare cases, it is possible that a RFP is expected to appear in the table after the scan operation but does not. If this occurs, repeat the scan operation.

8.7.4 ADDING DECT BASE STATIONS MANUALLY

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

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

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

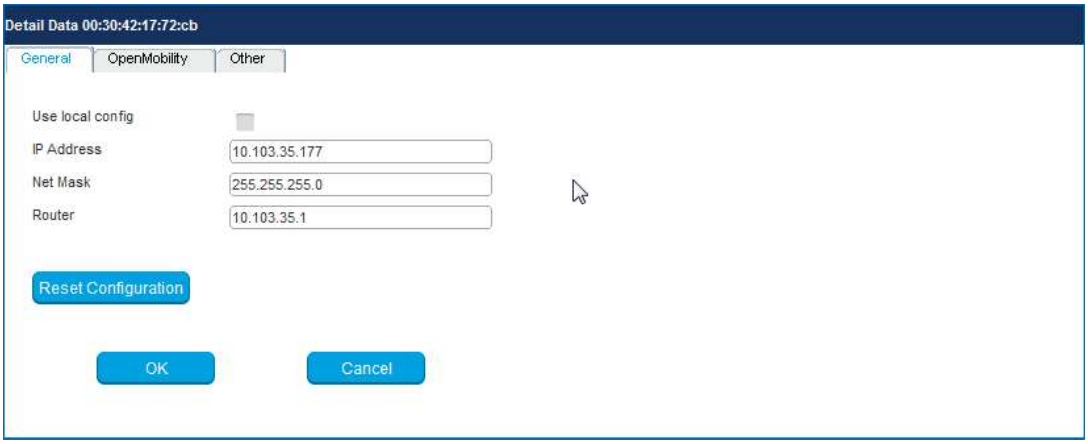
8.7.5 LOADING DECT BASE STATION DATA FROM FILE

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

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

8.7.6 EDITING DECT BASE STATION CONFIGURATION DATA

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



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

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

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

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

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

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

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

8.7.6.1 Other parameter panel

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

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

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

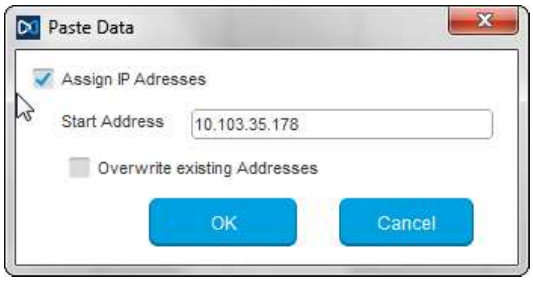
You can add a new parameter by selecting a parameter name from the drop-down list and clicking the **New** button.

8.7.6.2 Copy and Paste

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

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

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



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

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

8.7.6.3 Configuration Parameters

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

Parameter	Mandatory/Optional	Description
Use local config	Mandatory	Specifies whether the local configuration settings should be used at boot-up or not
IP Address	Mandatory	IP address of the DECT base station.
Net Mask	Mandatory	Subnet mask of the IP network
TFTP server address	Mandatory	IP address of the TFTP server (set to 0.0.0.0 if not used)
TFTP file name	Mandatory	The boot file to be read from the TFTP server
TFTP server list	Used only by: RFP 32/34 RFP 42 WLAN Optional	List of additional TFTP servers to load the boot file
Preferred TFTP server	Used only by: RFP 32/34 RFP 42 WLAN Optional	TFTP server from which to load the boot file first
OMM address	Mandatory	IP address of the OpenMobility Manager
Router	Optional	IP address of the default gateway
DNS address	Optional	IP address of the DNS server
DNS domain	Optional	Domain name of the network
Broadcast address	Optional	Broadcast address for the network
2nd OMM address	Optional	IP address of the standby OMM
VLAN ID	Optional	VLAN identifier
Use VLAN and DHCP	Optional	Specifies whether only the local VLAN configuration settings should be used when booting or not
Syslog server address	Optional	Destination IP address for the syslog file
Syslog server port	Optional	Destination port address for the syslog file
RFP configuration file server	Optional	URL of a server with RFP configuration files (ipdect.cfg|<MAC>.cfg) alternatively or in addition to OM Configurator settings. Syntax: {ftp|ftps|http|https}://[user:password@]server/[directory/] or tftp://server/[directory/]

8.7.7 APPLYING CONFIGURATION CHANGES

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

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

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

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

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

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

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

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

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

8.7.8 FACTORY RESET

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

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

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

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

8.7.9 SAVING AND LOADING A DECT BASE STATION LIST

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

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

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

8.7.10 REMOVING DECT BASE STATION ENTRIES

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

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

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

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

8.7.11 COMPATIBILITY WITH OLDER SIP-DECT RELEASES

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

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

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

8.8 OMM CONFIGURATION AND RESOURCE FILES

The OMM supports certain configuration files containing commands in AXI style, to support auto-configuration of small and simple installations in provider environments. It is assumed that the configuration files are automatically generated in a standardized way, to prevent configuration failures.

The following list summarizes all of the configuration and resource files related to the provisioning of a SIP-DECT system:

- ipdect.cfg / <MAC>.cfg / <PARK>.cfg

These files contain configuration parameters and are used to configure the OMM automatically. There is one common file “ipdect.cfg” for all RFPs and one file “<MAC>.cfg” for every single IP-RFP. The RFP specific <MAC>.cfg is requested if indicated in the common “ipdect.cfg” file. It is possible that all RFPs request “ipdect.cfg” and only selected RFPs request the <MAC>.cfg (for specific configuration on some RFPs).

- usr_common.cfg / <user>.cfg

These files are related to the “External User Data Provisioning” feature, whereby <user> refers to <Number/SIP user name> or <LoginID>.

<user>.cfg can also refer to user.cfg, a common file name for all users. This concept allows a provisioning server to provide user-specific settings on demand using one file name based on the specific user credentials.

- ima.cfg

This file includes the configuration for Integrated Messaging & Alerting Application, and can be loaded permanently.

- iprfp3G.dnld

This file includes the software image for RFP 35/36/37 IP / RFP 43 WLAN. This file also includes the software images for the Mitel 600 DECT phone family. RFPs can load their software image directly from the RFP OMM.

- iprfp4G.dnld

This file includes the software image for RFP 44/45 IP and RFP 48 WLAN. This file also includes the software images for the Mitel 600 DECT phone family. RFPs can load their software image directly from the RFP OMM.

- license.xml

This file includes the license for a specific SIP-DECT system.

- customer_image.png

This resource file can include a customer logo displayed to display on the OMM Web service.

With SIP-DECT 6.0 or later, all of these files can be loaded from the same external file server, if configured (see the below **CONFIGURATION FILE URL** section).

8.8.1 CONFIGURATION FILE URL

SIP-DECT supports provisioning through external configuration files. With SIP-DECT 6.0 or later, you can configure a URL for an external file server, from which all configuration files can be downloaded.

The configuration file server URL (ConfigURL) can be configured in the OMM (**System** -> **Provisioning** -> **Configuration file URL**), via DHCP or the Redirection and Configuration Service (RCS).

Note: If the external file server requires credentials for authentication, the credentials must be configured using the DECT phone or the Web service.

The following files are automatically requested if a provisioning server is set:

- Configuration files supporting startup parameters and OM AXI code for the OMM configuration
  - ipdect.cfg
  - <mac>.cfg (note that if a standby OMM is set, two MACs are present)
  - <PARK>.cfg (PARK in MAC address format: e.g. 001F11234001)
  - User configuration files (for user login on DECT phone)
  - user_common.cfg
  - <user.cfg>
  - user.cfg

- Integrated Messaging and Alerting Service (IMA) (for alarm scenarios, email accounts, RSS feeds) - ima.cfg
- OMM license file - license.xml
- Logo for OM Web-Portal (Branding) - customer_image.png

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

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

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

1 OMM database (e.g. **System** > **Provisioning** > **Configuration file URL** in either OMM Web service or OMP)
2 DHCP option 66 (SIP-DECT 6.2 or higher)
3 DHCP vendor specific option 43 – sub-option 2
4 DHCP option 234
5 Redirection and Configuration Service (RCS) – on initial setup only

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

Note: The ConfigURL only applies to the RFP OMM, which must be running SIP-DECT 6.0 or higher.

Other DECT base stations only apply the ipdect.cfg and <mac>.cfg files without OM AXI.

8.8.1.1 Syntax

The ConfigURL has the following syntax:

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

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

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

- **cm**: <https client method > - TLS1.0, 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)
- **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 (see section 5.4.2) or the OMP (see section 6.5.5.1).

8.8.2 SPECIFIC CONFIGURATION URLS

In addition to the common ConfigURL, you can configure specific URLs for individual configuration and resource files in the OMM database. As soon as a specific URL is set, the OMM uses that URL to load the appropriate configuration/resource file during startup.

Note that the user_common.cfg file is loaded from the ConfigURL and the specific URL when both URLs are set.

Configuration / Resource File	Location of Specific URL	
	OMM Web Service	**OMP**
user_common.cfg / <user>.cfg	N/A	**System** > **Data management** > **User data import** See section 6.5.7.2.
ima.cfg	**System** > **System settings** > **OM Integrated Messaging & Alerting service** See section 5.4.1.	**System** > **Advanced settings** > **IMA** See section 6.5.2.4.
iprfp3G.dnld	**System** > **System settings** > **Software update URL** See section 5.4.1.10.	**System** > **Basic settings** > **Software Update URL** See section 6.5.1.4.
Iprfp4G.dnld	**System** > **System settings** > **Software update URL** See section 5.4.1.10.	**System** > **Basic settings** > **Software Update URL** See section 6.5.1.4.
600.dnld	**System** > **System settings** > **DECT phone's firmware update** See section 5.4.1.6.	**System** > **Advanced settings** > **PP firmware** See section 6.5.2.3.
customer_image.png	N/A	**System** > **Advanced settings** > **Special Branding** See section 6.5.2.7
iprfp2G.tftp		

8.8.3 RELOAD OF CONFIGURATION AND RESOURCE FILES

The OMM automatically tries to load all configuration and resource files (ipdect.cfg, <MAC>.cfg, PARK.cfg, ima.cfg, user_common.cfg, update check for iprfp3G.dnld and iprfp4G.dnld, and so on) from the retrieved ConfigURL or specific URL (if present in the OMM database) at startup.

Note: The <user>.cfg and user.cfg files are only loaded on demand. They are not loaded automatically.

In addition, the OMM supports several mechanisms for updating the configuration by triggering a reload of the configuration and resource files:

- DHCP lease time

If the OMM is running on a RFP and DHCP is used, all configuration and resource files are reloaded when half of the DHCP lease time has elapsed.

- Daily automatic reload of configuration and firmware files

You can enable this option and specify a specific time of day to reload configuration files via the OMM Web service or the OMP (System -> Provisioning -> Daily automatic reload of configuration and firmware files).

- Manual reload via **Update** button

You can trigger a manual reload of all configuration and resource files by clicking the **Update** button in the OMM Web service (**System** ->**System settings** page) or OMP (**System** -> **System settings** -> **General** tab).

- 600 DECT phone **Administration** menu
  - When a user with a 600 DECT Phone selects the **Sync system data** option in the **Administration** menu, the OMM reloads all configuration and resource files.
  - When a user with a 600 DECT Phone selects the **Sync user data** option in the **Administration** menu, the OMM reloads the <user>.cfg file for that user.
- SIP Notify message
  - When the OMM receives a SIP Notify message with the “**check-sync**” event for a user, the OMM reloads the configuration file <user>.cfg for that user.
  - When the OMM receives a SIP Notify message with the “**prov-sync**” or ”**resync**” event for any user, the OMM reloads all configuration and resource files. The SIP Notify with ”prov-sync” or ”resync” can be also addressed to the OMM (without the user portion in the request URI).

8.8.4 AXI COMMANDS IN CONFIGURATION FILES

With SIP-DECT 6.0 or later, the OMM supports configuration files containing commands in AXI style, for OMM configuration.

The OMM attempts to load the following files from the Configuration File URL, and processes them in this order:

1. ipdect.cfg
2. <MAC>.cfg (RFP OMM only)
3. <PARK>.cfg (PARK in MAC address format: e.g. PARK: 1F11234001; MAC address format 001F11234001)

Note that the actual file name of the <MAC>.cfg depends on MAC address of the RFP where the OMM is running.

The active OMM and the standby OMM request different files, even if they belong to one system. To ensure that both OMMs can retrieve the same file independent of which one is active, each OMM requests the <PARK>.cfg. The PARK identifies a SIP-DECT system in a unique way.

None of the files are mandatory and they can be empty. The AXI commands can be all in one file or split up as needed.

Example configuration file

The following example shows how to include AXI commands in a configuration file.

```
### SIP-DECT OMM Config example – pls. be aware that some commands cannot be applied to
SIP-DECT with Cloud-ID e.g. request PARK from server, set regulatory domain etc. and some
commands depend on the actual use case/setup

### Confirm EULA

<SetEULAConfirm confirm="1" />

### Set full access account
```

```
<SetAccount plainText="1" > <account id="1" password="Sip!12" active="1" aging="none" />
</SetAccount>

### Set root account

<SetAccount plainText="1" > <account id="2" password="Sip!12" active="1" aging="none" />
</SetAccount>

### Set system name

<SetSystemName name="6.1 NB" />

### Tone scheme

<SetSysToneScheme toneScheme="DE" />

### OMP web start #####

<SetOMPURL> <url enable="1" protocol="FTP" host="ber-rd5014" path="/pub/SIP-DECT/Linux"
/></SetOMPURL>

### Enable SSH ###

<SetRemoteAccess enable="1" />

### Request a valid PARK from a Server ####

<PARKFromServer />

### Set DECT Regulatory Domain ###

<SetDECTRegDomain regDomain="EMEA" />

### Set WLAN Domain/contry ###

<SetWLANRegDomain regDomain="DE" />

### Enable Auto-create on subscription ####

<SetDevAutoCreate enable="1" />

### Set DECT AC ####

<SetDECTAuthCode ac="35239" />

### Set specific user data URL ####

<SetUserDataServer plainText="1" useCommonFileNameOnServer="1" ><url enable="1"
protocol="HTTPS" host="wwww.domain.de" path="/lpueschel/test/" username="lpueschel"
password="lpueschel" validateCerts="0" /></SetUserDataServer>

### Set SIP Proxy and Registrar ###

<SetBasicSIP transportProt="UDP" proxyServer="172.30.206.9" proxyPort="5060"
regServer="172.30.206.9" regPort="5060" regPeriod="3600" />

### use addId="" for Login at DECT DECT phone ####

<SetDECT phoneLoginVariant login="ID" />

#### Set Portrange 17000 - 32767 ####

<SetPortRangeSIP ><userUdpTcp startPort="17000" endPort="17511" /><userTls
startPort="18000" endPort="18511" /></SetPortRangeSIP>

#### Set SOS/ManDown emergency number ####

<SetAlarmTrigger><trigger id="0" triggerId="SOS" fac="SOS" comment="" num="110"
/></SetAlarmTrigger>

<SetAlarmTrigger><trigger id="1" triggerId="MANDOWN" fac="MANDOWN" comment="" num="112"
/></SetAlarmTrigger>

### Set common voice mail number ###

<SetSysVoiceboxNum voiceboxNum="6333" />
```

WARNING: **Configuration files must be automatically generated in a standardized way to avoid configuration failures. Configuration failures could cause a SIP-DECT system outage.**

Note that this configuration file approach has limitations. For example:

- Insufficient for managing data objects that are dynamically created and addressed by an index (e.g. RFPs)
- No administrator feedback for commands that cannot be processed (e.g., unknown commands, invalid parameter, conflicts which other configuration settings)

8.8.4.1 User Data in Configuration Files

Configuration files are generally insufficient for managing data objects that are dynamically created and addressed by an index. Therefore, it is necessary to configure user data also. This allows providers to manage the user data (to a limited extent) without using the <user>.cfg files.

The <user>.cfg concept supports the complete range of user-related SIP-DECT functions, including a user-specific DECT phone configuration. The user data in configuration files as described here supports only a limited set of parameters.

To allow user data in configuration files, the following rules must be applied:

1 Initialize all possible data sets with default values Number/SIP user name is automatically set to uid<X> (e.g,. uid1):

```
<CreatePPUser plainText=1 replaceData=1><user uid="1" name="" num="" addId=""
sipAuthId="" sipPw="" pin="" fixedSipPort="0" /> </CreatePPUser>

…

<CreatePPUser plainText=1 replaceData=1><user uid="512" name="" num="" addId=""
sipAuthId="" sipPw="" pin="" fixedSipPort="0" /> </CreatePPUser>
```

2 To “add” a user, set appropriate data:

```
<CreatePPUser plainText=1 replaceData=1><user uid="1" name="Account004 Mitel"
num="040226332195" addId="195" sipAuthId="040226332195" sipPw="broadnet.01" pin="195"
fixedSipPort="0" /> </CreatePPUser>
```

3 To “remove” a user, set to default data:

```
<CreatePPUser plainText=1 replaceData=1><user uid="1" name="" num="" addId=""
sipAuthId="" sipPw="" pin="" fixedSipPort="0" /></CreatePPUser>
```

This supports the use of templates such as the following:

```
<CreatePPUser plainText=1 replaceData=1><user uid="1" name="%BWNAME-1%" num="%BWLINEPORT-
1%" addId="%BWEXTENSION-1%" sipAuthId="%BWAUTHUSER-1%" sipPw="%BWAUTHPASSWORD-1%"
pin="%BWEXTENSION-1%" fixedSipPort="0" /></CreatePPUser>
```

8.8.5 USER CONFIGURATION FILES

The user configuration files (user_common.cfg and <user>.cfg) enable the “External User Data Provisioning” feature, which allows customers to import user data from a provisioning server. See the *SIP-DECT OM DECT Handset Sharing & Provisioning Installation & Administration User Guide* for a full description of that feature.

In addition <user>.cfg can also refer to user.cfg, a common file name for all users.

SIP-DECT 6.0 introduced the *UDS_CommonUserFileName* configuration attribute. When enabled, the OMM tries to fetch the same user.cfg file from the provisioning server for each user executing the login procedure, such that the login credentials of each user are used to access the provisioning server. This

means that the provisioning server executes user authentication and provides a user-specific user.cfg when the user is authorized.

The *UDS_CommonUserFileName* attribute is enabled/disabled via the user_common.cfg file.

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

Note that the *OM_UniqueId=NUMBER/UID* variable in the user_common.cfg file is no longer supported.

The following table summarizes the combinations of provisioning server access and type of user validation supported:

Provisioning Server access	Requested files	User validation	Supported DECT phones
• User data import URL • User data import credentials • No certificate validation	• <number | SIP user name>.cfg • <loginID>.cfg	OMM authenticates user against PIN from .cfg files	• GAP • Mitel 142d • Mitel 600
• User data import URL • User data import credentials • System Provisioning Certificate validation	• <number | SIP user name>.cfg • <loginID>.cfg	OMM authenticates user against PIN from .cfg files	• GAP • Mitel 142d • Mitel 600

• System Provisioning URL • System Provisioning credentials • System Provisioning Certificate validation	• <number | SIP user name>.cfg • <loginID>.cfg	OMM authenticates user against PIN from .cfg files	• GAP • Mitel 142d • Mitel 600
• User data import URL • User credentials (UDS_CommonUserFIleName=YES) • No certificate validation	• user.cfg	Provisioning server authenticates user at file request with user credentials	• Mitel 600
• 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	• Mitel 600
• System provisioning URL • User credentials • (UDS_CommonUserFIleName=YES) • System Provisioning Certificate validation	• user.cfg	Provisioning server authenticates user at file request with user credentials	• Mitel 600

8.8.6 DIGEST AUTHENTICATION AND CERTIFICATE VALIDATION

The OMM supports system credentials for provisioning to retrieve configuration and resource files from a server that requires user/password authentication.

System credentials are used to retrieve files from the external provisioning server defined by the configuration file URL, for protocols supporting authentication or servers requesting authentication. For HTTP/HTTPS, basic and digest authentication are supported.

You can set the system credentials via:

- OMM Web service **System** -> **Provisioning** -> **System credentials** page (see section 5.4.2.2)
- OMP **System** -> **Provisioning** -> **System credentials** tab (see section 6.5.5.4)
- Mitel 600 DECT phone user interface (through Feature Access Code or the Administration menu)

System credentials are also inherited if sources other than the configuration file URL are configured for specific configuration or resource files, without credentials. The system credentials are used only if requested by the file server.

8.8.6.1 System credentials via Mitel 600 DECT Phone user interface

A Mitel 600 DECT phone user can set, change or delete system credentials from the Mitel 600 DECT phone via:

- a configured feature access code (FAC)
- the A**dministration** menu on the user interface

Note: The user must log in to OMM before being allowed to change valid credentials. If credentials are not set or are invalid (indicated by a health state), the OMM login is omitted.

Setting the credentials via feature access codes requires configuration of a FAC number through the **System Features** -> **Feature Access Codes** menu of the OMM web service (see section 5.9.4) or the OMP (see section 6.12.2).

When the user dials the configured feature access code, the user can select between the “Create/Change” and “Delete” options. The Administration menu additionally offers a health indication (ok or not ok). Depending on the health state, the user may be forced to login to the OMM first.

8.8.7 DECT BASE STATION SOFTWARE IMAGE FROM RFP OMM

To simplify the upgrade process for existing SIP-DECT installations in provider environments, SIP-DECT 6.0 and later provides support for a feature that allows RFPs to load their software image directly from the connected OMM.

If the RFP has no valid URL from which to load the software, they attempt to load the software from the connected OMM. If the OMM is running on a RFP, the RFP OMM delivers the software to the connected RFPs.

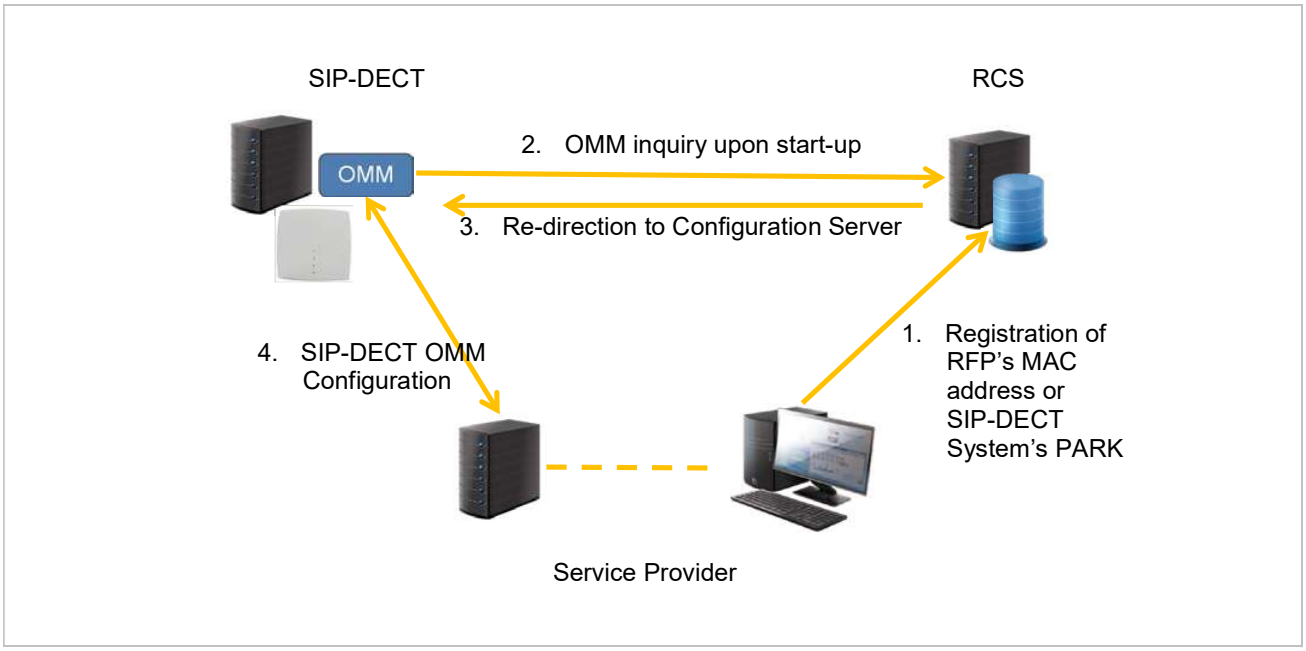
A new software image for the RFP OMM can be provided as a iprfp3G.dnld/iprfp4G.dnld file on an external file server. The software update URL can be configured via the OMM Web service (see section 5.4.1.12) or OMP (see section 6.5.1.4).

In SIP-DECT 8.0, OMM RFP4G provides SW images for RFP3G and RFP4G base stations. Because, the RFP3G is not able to hold the RFP4G SW image, an OMM RFP3G cannot provide the iprfp4G.dnld to an RFP4G.

8.8.8 REDIRECTION AND CONFIGURATION SERVICE (RCS)

The Redirection and Configuration Service (RCS) simplifies SIP DECT installation and management. When the MAC address or the PARK of a SIP-DECT OMM is entered in the RCS server, a SIP-DECT OMM is routed to its assigned server for configuration upon initial start-up.

If the OMM does not find a ConfigURL during initial setup, the OMM contacts the RCS to request a ConfigURL, using its RFP MAC address. If the RFP MAC Address is configured in the RCS, the RCS provides a ConfigURL that points to an external provisioning server. The OMM attempts to load all configuration and resource files from the ConfigURL received from RCS.



Note: The SIP-DECT OMM only uses the ConfigURL from RCS. Other information provided from RCS is not supported.

The OMM requests information from RCS only if no information has been retrieved from RCS prior to the request. The response is stored permanently in the OMM. To force a new RCS request, the OMM must be reset to default settings, through the **Discard OMM DB and configuration files** or **Reset OMM RFP(s) to factory defaults** on restart (see section 5.4.1.17).

8.8.9 CUSTOMER LOGO ON OMM WEB SERVICE

SIP-DECT 6.0 and later supports the integration of a customer-specific logo on the OMM Web service interface. If a customer_image.png file is available on an external file server, customers can integrate their own logo into the OMM. This logo is displayed beside the Mitel logo on the top bar.

This image can be imported by:

- Configuration of a branding image URL to a file server using OMP (see section 6.5.2.7)
- Automatic search for a file named 'customer_image.png' on the provisioning server

The branding image is stored permanently in the OMM database, ensuring that the image is available even if a configured file server or provisioning server is not reachable. The file is deleted automatically from the server on a "file not found" response or by disabling the branding image URL configuration.

The picture should not be larger than 50 pixels high and 216 pixels wide.

8.9 DECT BASE STATION CONFIGURATION FILES

8.9.1.1 Third Generation DECT base Stations Configuration Files

IP-RFPs support two DECT base stations configuration files (downloaded from a server) to get configuration settings. There is one common file "ipdect.cfg" for all DECT base stations and one file specific file "<MAC>.cfg" for every IP-RFP. The DECT base station requests the "ipdect.cfg" file if a URL is provided. The RFP specific <MAC>.cfg is requested if this is indicated in the common "ipdect.cfg" file.

It is possible that all RFPs request “ipdect.cfg” and only selected RFPs request the <MAC>.cfg to obtain a specific configuration on some RFPs.

8.9.1.2 Fourth Generation DECT Base Stations Configuration Files

The 4G RFP supports configuration files known as RFP or base station configurations files. Such files can contain the URL for the RFP SW update.

As of SIP-DECT 8.0, the new parameter OM_SwImageUrl4G is introduced to configure the SW update URL for 4G RFPs.

The SW update URL for 3G RFPs can be configured with the existing parameter OM_SwImageUrl or the new parameter OM_SwImageUrl3G. For example:

- # path to the software image
- OM_SwImageUrl=ftp://login:password@server/iprfp3G.dnld
- OM_SwImageUrl3G= ftp://login:password@server/iprfp3G.dnld
- OM_SwImageUrl4G= ftp://login:password@server/iprfp4G.dnld.

8.9.2 STANDARD IP SETTINGS

Standard IP settings (which are necessary for access to the RFP configuration files) are configured via DHCP (see section 8.5) or OM Configurator (see section 8.7). These are:

- IP address
- Net mask
- Gateway (i.e. router)
- Boot file name
- TFTP server
- Public option 224: “OpenMobility” or “OpenMobilitySIP-DECT” (to identify the relevant DHCP offer)
- Domain Name Server (optional)
- Domain Name (optional)
- URL to the RFP configuration files

All other parameters can be set by using an RFP configuration file even if standard DHCP options or OM Configurator parameters exist.

8.9.3 CONFIGURATION FILE SOURCE

A TFTP / FTP(S) / HTTP(S) URL specifies the protocol, server and path to access the RFP configuration files. The URL can include account data if appropriate.

Syntax:

{ftp|ftps|http|https}://[user:password@]server/[directory/]

or

tftp://server/[directory/]

The URL configuration is provided via DHCP option code 233 (prio1), or the OM Configurator.

- “ipdect.cfg” is mandatory if an URL is provided by DHCP or local static configuration via the OM Configurator.
- “<MAC>.cfg” is mandatory if it is indicated in the “ipdect.cfg” that a “<MAC>.cfg” exists for the DECT base station. (There is a key word to indicate that a “<MAC>.cfg” exists for every DECT base station.)

Mandatory means that if a file cannot be loaded, the DECT base station does not start. This is relevant for the following scenarios:

- RFP boot / startup (after power on, software update, etc)
- A change of the URL

8.9.4 PARAMETER SETTINGS PRIORITY

Some parameters can be set via DHCP / OM Configurator or by using the files “ipdect.cfg” or “<MAC>.cfg”. If a parameter is provided through more than one of the possible ways, the last setting has priority. There is the following order:

- DHCP / OM Configurator
- ipdect.cfg
- <MAC>.cfg

It is also possible to remove settings.

8.9.5 SOFTWARE UPDATE SETTINGS FOR 3RD GENERATION DECT BASE STATIONS

A configuration parameter specifies the location of the software that will be installed into the flash of an RFP 35/36/37 IP / RFP 43 WLAN and activated by the OpenMobility Manager.

OM_SwImageUrl=ftp://172.30.207.21/openmobility/iprfp3G.dnld

TFTP, FTP(S), HTTP(S) are supported for an RFP 35/36/37 IP / RFP 43 WLAN software update.

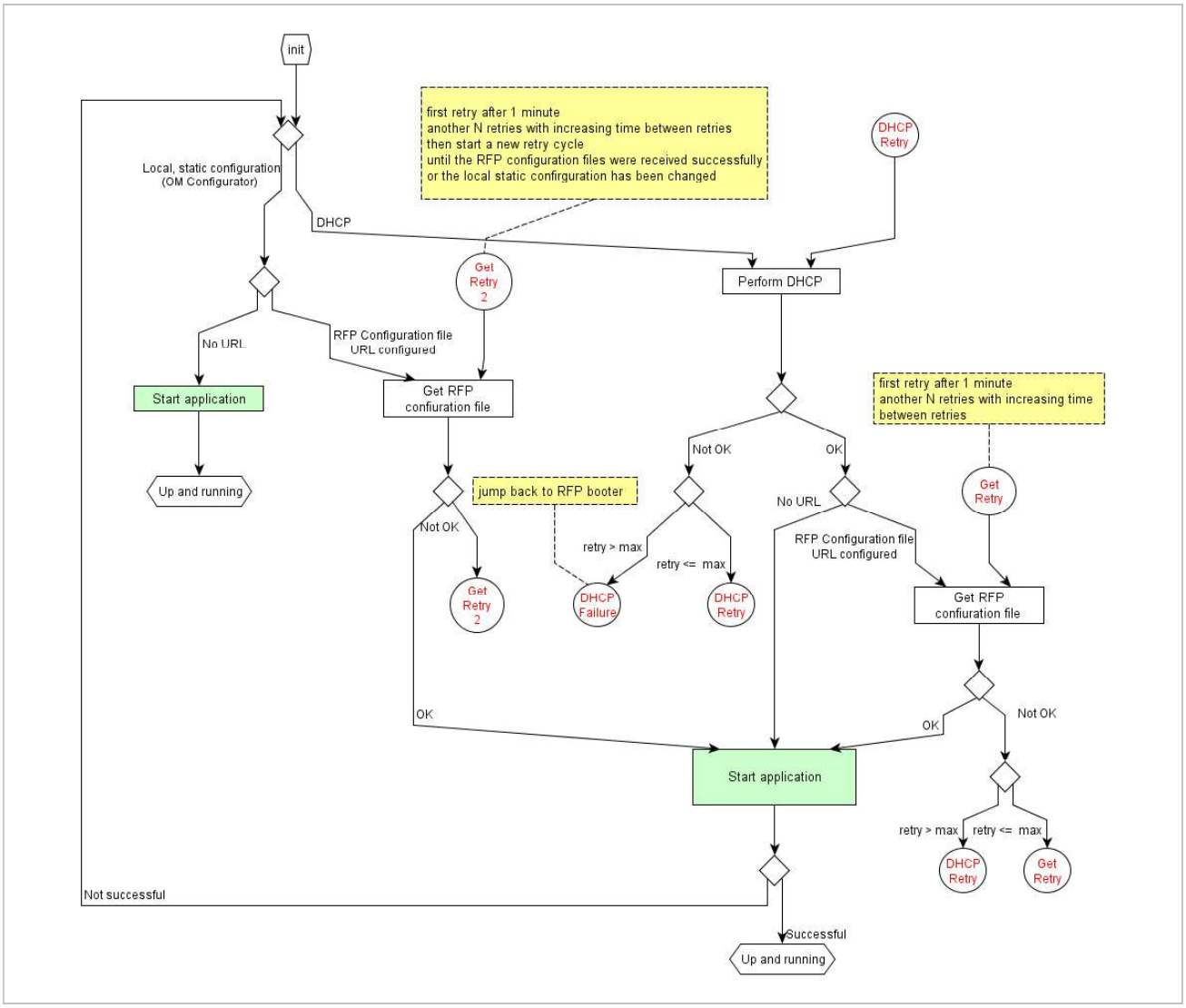
8.9.6 SOFTWARE UPDATE SETTINGS FOR 4TH GENERATION DECT BASE STATIONS

A configuration parameter specifies the location of the software that gets installed into the flash of an RFP 44/45/47 IP / RFP 48 WLAN and activated by the OpenMobility Manager.
OM_SwImageUrl=ftp://172.30.207.21/openmobility/iprfp4G.dnld

TFTP, FTP(S), HTTP(S) are supported for an RFP 44/45/47 IP / RFP 48 WLAN software update.

8.9.7 TIMES WHEN RFP CONFIGURATION TIMES ARE READ

The configuration files are read by the RFP application e.g. during startup as shown in the following figure.



Configuration files are read by the RFP application at the following times:

- RFP reboot
- Restart of an application e.g. OMM
- DHCP renew and DHCP bound
- Configuration changes via OM Configurator
- RFP configuration file update check

8.9.8 RFP CONFIGURATION FILE UPDATE CHECK

RFP configuration file update check has the following characteristics:

- The interval is configurable in the RFP configuration files (minimum interval: 5 minutes; maximum interval: 7 days).
- Default interval: 24 hours.
- Both RFP configuration files are checked if relevant.

If the configuration file(s) cannot be retrieved …

- The RFP continues operation with the last successfully retrieved configuration file(s).
- The RFP will try to retrieve the configuration files again, starting with an interval of one minute and doubling this interval with each retry, not exceeding the update check interval (either default or configured).
- If the RFP is using DHCP, a renewal of the lease is scheduled so that possible changes in DHCP configuration will be detected.
- Failure to retrieve the configuration files is reported via Syslog.

8.9.9 HANDLING OF PARAMETER CHANGES

A change of a parameter (DHCP / OM Configurator, RFP configuration files) does not necessarily mean a change to the RFP's configuration because the parameter could be covered up or previously set using an alternative way.

Example 1:
IP address of a Syslog Daemon has been changed in "ipdect.cfg" but is covered up by "<MAC>.cfg" in which this parameter has not been changed.

Example 2:
A parameter is new in "<MAC>.cfg" but has been set previously in "ipdect.cfg" with the same parameter value.

Only if a parameter change causes a change in RFP configuration (as a sum of e.g. DHCP / OM Configurator, "ipdect.cfg" and "<MAC>.cfg" files) will the RFP perform a configuration update procedure.

Depending on the changed parameter, an RFP configuration update is done:

- On the fly without any service interruption e.g. IP address of a Syslog Daemon has been changed.
- With an application restart e.g. OMM IP address has been changed.

8.9.10 CONFIGURATION FILE SYNTAX

```
##############################################################################
# sample configuration file for the OpenMobility system
# retrieved via the net using file transfer protocols
# like tftp, ftp, http, https, ftps
#
##############################################################################
# comments start with the hash sign: "#"
#
##############################################################################
# BOOL variables support the following values
# YES Y 1 TRUE (case does not matter)
# NO  N 0 FALSE (case does not matter)
# other values are interpreted as false
```

```
#
################################################################################
# personal configuration files
#
# personal configuration files have the following name
# <OWN-MAC>.cfg, where <OWN-MAC>.cfg is of the form
# e.g. 003042ABCDEF.cfg

# all RFPs will also load the <OWN-MAC>.cfg file
OM_PersonalConfigAll=1 # BOOL

# DO load the individual file for the RFP with mac 003042FFF0D0
#   no matter what OM_PersonalConfigAll says
OM_PersonalConfig_003042FFF0D0=y

# DO NOT load the individual file for the RFP with mac 003042ABCDEF
#   no matter what OM_PersonalConfigAll says
OM_PersonalConfig_003042ABCDEF=n # BOOL

# time interval for checking the remote cfg files in seconds
# minimum value is 300   (5 minutes)
# maximum value is 604800 (7 days)
OM_ConfigCheckInterval=500

################################################################################
# OpenMobility system
#
# the OpenMobilityManager ip addresses
OM_ManagerIpAddress1=172.30.205.17
OM_ManagerIpAddress2=172.30.205.18

# path to the software image
OM_SwImageUrl=ftp://172.30.207.21/openmobility/sw/iprfp3G.dnld

################################################################################
# SYSLOG
#
OM_SyslogIpAddress=172.30.207.20
OM_SyslogPort=10115

################################################################################
# transfer core files to the following directory
#
```

```
OM_CoreFileSrvUrl=ftp://10.103.35.20/corefiles
```

8.10 CONSOLIDATED CERTIFICATE MANAGEMENT

SIP-DECT has various secured interfaces to support secure connections for file imports from local servers or provisioning servers. By default, the OMM Web server uses the hardcoded self-signed OMM certificate as local certificate for encrypted AXI connections, for provisioning (mutual authentication), and for SIP-over-TLS connections.

Certificate and authentication validation settings for these secure connections can be inherited from the configuration file URL (see section 8.8.1).

8.10.1 SIP OVER TLS CERTIFICATES

SIP over TLS certificates are used for secure SIP connections. The hard coded self-signed OMM certificate is used by default, however you can import trusted certificates, a local certificate chain and a private key file (optionally password-protected) via:

- OMP (**System -> SIP -> Security** tab)
- OMM Web service (**System -> SIP -> Security**)
- A certificate server (usually running on a Mitel call server)

8.10.2 OMM CERTIFICATE (WEB SERVICE / AXI)

The OMM Web server uses the hard coded self-signed OMM certificate by default as the local certificate for encrypted AXI connections.

You can overwrite the hard coded OMM certificate by importing a local certificate chain and a private key file (optionally password-protected) via the OMP (**System** -> **Advanced settings** -> **OMM Certificate** tab). You can also configure an OMM certificate server (**System** -> **Advanced settings** -> **OMM Certificate server** tab) to enable provisioning of OMM certificate files.

The OMM certificate will be used for incoming AXI and HTTPS connections to the OMM services. If the OMM can be reached from the internet by a domain and an appropriate CA certificate has been imported, no security warnings are displayed in web browsers trusting the CA root certificate.

8.10.3 PROVISIONING CERTIFICATES

Provisioning certificates are used for secure connections to configuration or firmware file servers with support for mutual authentication (i.e., for FTP, FTPS, and HTTPs protocols).

The OMM uses a trusted certificate chain to validate the server. This is required if the server has no certificate derived from a trusted CA root certificate, where the OMM uses the Mozilla CA Certificate List. If no server certificate is available, you can disable the validation against trusted and CA certificates.

By default, the hard-coded self-signed OMM certificate is used for mutual authentication. You can overwrite the hard coded OMM certificate by importing trusted certificates, a local certificate chain and a private key file (optionally password-protected) via:

- OMM Web service System -> Provisioning -> Certificates page (see section 5.4.2.8)

- OMP System -> Provisioning -> Provisioning Certificates tab (see section 6.5.5.2)
- A provisioning certificate server through OMP System -> Provisioning -> Certificates server tab (see section 6.5.5.3)

The OMM provides the local certificate chain and the private key to servers requesting mutual authentication. The private key file may be password protected.

The system credentials can be inherited if specific sources for configuration and resource files are configured, where the 'Use common certificate configuration' option is enabled.

8.10.4 CERTIFICATE VALIDATION

If the HTTPS or FTPS protocol is used to retrieve files from the configured provisioning server, the OMM validates the server certificates according to the certificate validation settings.

You can configure the certificate validation settings via OMP (**System** -> **Provisioning** -> **Provisioning – SSL settings**) or the OMM Web service (**System** -> **Provisioning** -> **Certificates**). Certificate validation settings can also be part of the ConfigURL provided by the RCS or via DHCP.

If you want to use the same validation settings for a specific URL (i.e., other than the configuration file URL), enable the "Use common certificate configuration" parameter when configuring the URL (unless the "Import certificates with first connection" parameter is enabled).

8.11 3RD AND 4TH GENERATION RFP SOFTWARE UPDATE

The DECT base station checks several locations for a software update. If found, the software is copied to the flash memory, leaving the current software intact. After successful installation, the OMM is notified about the new software. Activation of the software is then managed by the active OMM. DECT base stations that do not have a connection to the OMM activate and start the software immediately.

Locations for software updates:

- Attached USB mass storage device with a software image iprfp3G.dnld in its root directory (Only 3rd generation RFPs). The USB mass storage device must be formatted using the vfat32 file system.
- If ipdect.cfg supplies the OM_SwImageUrl variable, the URI is used to get the boot image. See section 8.9.
- TFTP server, path and file configured using the OM Configurator or via DHCP.
- OMM (SIP-DECT 6.0 or later): If the RFP has no valid URL from which to load the software, they attempt to load the software from the connected OMM. If the OMM is running on a DECT base station, the RFP OMM delivers the software to the connected base stations. See section 8.8.7 for more information.

8.12 802.1Q SUPPORT

The IP RFPs support VLANs according to IEEE 802.1Q. VLAN can be administered

- on a per port basis of the LAN switch assuming that the IP RFPs are connected to a single port of a switched Ethernet environment, or
- by assigning a VLAN ID to the IP RFP matching the VLAN they should operate in.

VLAN tagging has only to be set to IP RFPs' in the last case. The whole section refers to that case. With this, also 802.1p priority within Ethernet frames is enabled.

The scope of the following description is restricted to VLAN tagging and obtaining the VLAN ID. Quality of Service mechanisms like 802.1p priority and DiffServ are not described in this section.

VLAN implementation notes referring to IP RFPs:

- IP RFPs are not able to support VLAN ID 0 as described later in this section. Any other valid VLAN ID can be configured.
- If a VLAN ID is configured, all traffic from an IP RFP will be tagged with this VLAN ID.
- The VLAN ID configured for an IP RFP is also used for the OMM running on this IP RFP.
- Once a VLAN ID is set to the IP RFP, incoming frames are only accepted if they are tagged as well. Therefore the switch port must be configured as a tagged trunk for this VLAN.
- The VLAN configurations can be done using DHCP or the interface for the local static configuration, the OM Configurator.
- The use of VLAN does influence the boot up process of the IP RFP because the VLAN configuration takes place during the boot up phase.
- The default setting is not to tag the traffic. 802.1Q tagging is enabled if the VLAN ID is set. If no VLAN ID is set 802.1Q is disabled.

VLAN ID 0

VLAN ID 0 means that the IP RFP's traffic belongs to the port/native VLAN. The Ethernet switch port to which the IP RFP is connected must be configured to accept 802.1Q tagging for this to work and the switch must interpret VLAN ID 0 as the port/native VLAN ID per the IEEE 802.1Q standard.

The packets from the IP RFP are tagged with VLAN ID 0 and the packets sent to the IP RFP are tagged with the port/native VLAN ID. This scenario does not work, because the IP RFP supports only one VLAN ID in both directions. That means the VLAN ID in the receive direction must be the same as the send direction.

8.12.1 BOOT PHASE OF IP RFPS (DHCP)

Because the IP RFP does not know about VLAN at the beginning of the start up, two DHCP scopes are required. This applies regardless of the Ethernet switch being used. The following scenario with arbitrary VLAN Ids' details the steps an IP RFP would go through in a typical dual-VLAN implementation.

Step A. DHCP scope within the native VLAN:

1. IP RFP boots up and obtains an address on the native VLAN.
2. The data VLAN DHCP option 132 directs the IP RFP to go to voice VLAN.

Step B. DHCP scope within the voice VLAN:

1. IP RFP releases the data VLAN address and obtains an address on the voice VLAN and all other parameters.

   The voice VLAN does not have the DHCP option 132, because an IP RFP already on the voice VLAN does not need to be directed to go there.

2 IP RFP is operational on the voice VLAN.

If a reboot or power cycle occurs, the IP RFP returns to step A.

If an IP RFP cannot obtain an address on the voice VLAN, due to network or DHCP problems then the IP RFP falls back automatically to untagged frames (native VLAN).

To avoid the DHCP scope within the native VLAN the VLAN ID to be used can be set permanently via OMC without losing the ability to provide other parameter via DHCP, see section 8.7.

8.12.2 BOOT PHASE OF IP RFPS (LOCAL CONFIGURATION)

The PC running the OM Configurator must be a member of the native VLAN for the first configuration, later on within the voice VLAN set.

If a wrong or unknown VLAN ID is set, you can overwrite or read the configuration using no VLAN tag on the switch port in the first six seconds after the RFP is connected to a power supply / PoE. After six seconds the RFP applies the local configuration and starts using the parameters.

8.13 INSTALLING OMM IN HOST MODE

In this case, the OMM software must be installed on a PC running Red Hat Enterprise Linux 7 or CentOS 7. The network parameters with which the OMM works in this mode depend on this PC's network configuration.

Once started, OMM works permanently on the PC. In case of fatal error or PC restart, OMM will restart automatically.

> **Please note:** Check that the versions of the OMM and RFP software on your SIP-DECT installation are the same.

8.13.1 SYSTEM REQUIREMENTS

The OMM application is a 32-bit/x86 application that can be installed on a 32-bit or 64-bit (recommended) operating system. The PC-based OMM requires the following configuration:

- Red Hat Enterprise Linux 7 or CentOS 7 operating system
- Server hardware minimum:
  - Processor : Dual Core Intel® Xeon® 3065, 2.33GHz, 4MB cache
  - Bus 1333 MHz
  - Memory : 4GB DDR2 SDRAM 667 MHz
  - Hard disk: 80 GB SATA 7200 rpm
  - 1 GBit/s Ethernet interface

8.13.2 INSTALLING THE OMM SOFTWARE

The OMM software for the Linux Redhat server is provided as a self-extracting executable file (e.g., SIP-DECT_6.1.bin). This binary file contains two Red Hat packages:

- SIP-DECT-OMM-<SIP-DECT-version>.i586.rpm
  OpenMobility Manager software.
- SIP-DECT-HANDSET-<DECT phone-version>.i586.rpm
  Software for Mitel 600 DECT phones

The Mitel 600 DECT phone software can be updated via the Air interface, see section 8.22. A separate software package can also be provided for specific updates of the DECT phone software.

IMPORTANT : Log in as "root" to install and/or update OMM. If you do not login as root to open the OMM console, the path to ommconsole is not set. You must enter the whole path "/usr/sbin/ommconsole" to start the OMM console.

Command syntax

For extraction and automatic standard installation
sh **SIP-DECT_<version>.bin**

For extraction and automatic standard installation
sh **SIP-DECT_<version>.bin -f**

For extraction of RFP packages only
sh **SIP-DECT_<version>.bin –x**

RPM packages can also be installed manually.

For a first OMM type installation
rpm –i SIP-DECT-OMM-<version>.i586.rpm

For an OMM software update (see section 7.14)
rpm –U SIP-DECT-OMM-<version>.i586.rpm

For Mitel 600 DECT phone software installation
rpm –i SIP-DECT-HANDSET-<version>.i586.rpm

To delete a software release
rpm –e SIP-DECT-HANDSET and
rpm –e SIP-DECT-OMM

To check an installed release
rpm –qi SIP-DECT-OMM
or
rpm –qi SIP-DECT- HANDSET

After the installation phase, start OMM by running the command
"/etc/init.d/sip-dect-omm start"

8.13.3 CONFIGURING THE START PARAMETERS

The basic data for initializing OMM is stored in the file "/etc/sysconfig/SIP-DECT". It can be edited to modify the OMM interface.

```
##############################################
# OMM configuration file
##############################################
# if you use a different interface for omm  activate/correct parameter below
#OMM_IF="eth0"
```

```
#
OMM_CONFIG_FILE=/opt/SIP-DECT/tmp/omm_conf.txt
#
#if you use OMM resiliency for OMM activate parameter below with OMMs IP adresses
#OMM_RESILIENCY="192.168.0.1:192.168.0.2"
#
# Automatic OMM database import:
# TFTP / FTP  / HTTP(S) URL specifies the import server and file
```

Parameters	Description
OMM_IF	Interface for communicating with the RFPs (by default: eth0)
OMM_CONFIG_FILE	File that contains the OMM configuration (by default: /opt/SIP-DECT/tmp/omm_conf.txt)
OMM_RESILIENCY	In case of OMM redundancy, enter the two IP addresses of the OMMs. See also section 7.15.

8.13.4 SPECIFIC COMMANDS – TROUBLESHOOTING

The OMM software is installed but does not work automatically when the PC starts. The command below stops or starts OMM manually (User root):

/etc/init.d/sip-dect [start|stop|restart].

The command line interface for OMM is accessible via telnet on port 8107.

Malfunction

To check whether OMM is working, see the list of procedures for the “SIP-DECT” process. If OMM does not start, delete the lock file “/var/lock/subsys/SIP-DECT”.

To delete the OMM configuration remove the OMM configuration file “/opt/SIP-DECT/tmp/omm_conf.txt” (by default).

8.14 UPDATING THE OMM

The procedures for updating an existing DECT installation with new software depend on

- whether a single OMM or standby OMM installation is used
- whether the OMM is running on an RFP or PC

The OMM “standby” feature is described in section 8.15.

The update mechanism allows an update of the RFPs with minimum impact to DECT services, especially for installations with a standby OMM.

All RFPs check the availability of a new boot image file automatically when:

- the DHCP lease is refreshed,
- the RFP lost the connection to the OMM,
- one of the service applications running on the RFP must be restarted, and
- an RFP configuration file update check is done (see section 8.7.7).

Please note: Make sure that all configured software sources point to the same software version, so that the OMM and all RFPs are running the same software version.

Please note: RFPs without a configured software image URL (via DHCP, OMC or ipdect.cfg/<mac>.cfg) retrieve their software directly from the OMM. In this case, the RFP activates the software immediately. This feature is only available with 3G RFPs.

As soon as an RFP detects a new boot image file on the TFTP server (or the software download server using FTPS or HTTPS), it notifies the OMM. The OMM keeps track when it is safe to restart an RFP in order to leave the DECT service synchronized.

RFPs scheduled for restart are marked with a yellow sign within the Web service (see section 5.6.1) or in a separate column within the OM Management Portal (OMP), see section 6.7.1.1.

Please note: Only software upgrades from the preceding two releases are tested for upgrade to the current release. Additional steps may be required to upgrade systems with software that is three or more releases behind the current release.

8.14.1 UPDATING A SINGLE OMM INSTALLATION

In the case of a single OMM installation, a DECT network outage during the update procedure is unavoidable.

Please note: Updating a single OMM installation results in a DECT network outage during the update procedure.

For the update, replace the boot image file on the TFTP server(s) with the new one.

OMM in RFP mode

If the OMM is running on an RFP, force the update of this RFP by pressing the **Update** button on the **System settings** web page (see section 5.4.1.18). The RFP checks the boot image file on the TFTP server and reboots if a new one is found.

OMM in host mode (on Linux server)

If the OMM is running on a dedicated Linux server, install the new software as described in section 8.13.2 on the PC with the command "**SIP-DECT_<version>.bin**". This stops the running OMM automatically and installs the new software. After the installation phase, restart the OMM by executing the command "**/etc/init.d/sip-dect-omm start**".

As soon as the RFPs lose the connection to the OMM (because of the update), the RFPs detects that a new image file is on the TFTP server and reboot with the new image file.

8.14.2 UPDATING A STANDBY OMM INSTALLATION

Please note: Updating a standby OMM installation causes a switch over between both OMMs. All active calls will be dropped.

For the update replace the boot image file on the TFTP server(s) with the new one.

OMM in RFP mode

Force the update by pressing the **Update** button on the **System settings** web page (see section 5.4.1.18). The OMM-RFP checks the boot image file on the TFTP server and initiates an update procedure, if a new image file has been found.

The automated update procedure performs the following steps:

1. Reboot the RFP residing the standby OMM.
2. Reboot the RFP residing the active OMM which causes a failover to the standby OMM.
3. Reboot all other RFPs that are able to find the new boot image file one by one. This is managed by the new active OMM.

This procedure reduces the downtime of the SIP-DECT system to a minimum due to the optimized failover.

> **Please note:** Please be aware that a minimum downtime of the system can only be reached if the system was in a stable working state when initiating the update and the IP infrastructure guarantees a fast update of the OMM RFPs (e.g., no 64kbit/s line to download the SW into the RFP).

OMM in host mode (on Linux server)

For an update with a minimum impact to the DECT service do the following:

1. Replace the boot image file on the TFTP server(s).
2. Manually update the standby OMM.
   a) Stop the OMM service.
   b) Install the new software.
   c) Start the OMM service.
   d) Wait at least 30 seconds before you go on with updating the active OMM.
3. Manually update the active OMM.
   a) Stop the OMM service.
   b) Install the new software.
   c) Wait at least 30 seconds.
   d) Start the OMM service.

> **Please note:** A one-by-one update of RFPs is not possible if the signaling interface between the OMM and the RFP has been changed. Please see the release notes delivered with the software.

To enforce an update of the whole DECT system at once, deactivate / update both OMMs simultaneously. The RFPs will lost the connection to both OMMs and will automatically restart with the new boot image file.

8.15 OMM STANDBY

To perform OMM standby, two OpenMobility Managers must be provided in an OMM network. One operates as the active OMM, and the other operates as the standby OMM.

In the event that the RFP designated as the OMM fails, the other RFP, designated as the secondary OMM automatically assumes the role of the OpenMobility Manager.

How OMM Standby works

During system start-up, each RFP retrieves either one (if no standby OMM is configured) or two (if OMM Standby is configured) OMM IP addresses and both try to connect to each other. The active OMM serves all connections from RFPs or DECT phones.

During normal operations, both the active and the standby OMM are in contact and monitor each other's operational state. They continually exchange their current standby states and the standby OMM receives a copy of any configuration changes on the active OMM. As long as both OMMs are in contact, their databases are synchronized automatically.

If the primary OMM fails, the OMM responsibilities are taken over by the standby OMM to maintain operation. A "No Standby" warning is displayed on the OMM web interface, indicating that there are no longer two functioning OMMs in the network or cluster. Configuration changes are made unsafely in this situation.

If the active OMM fails, the inactive OMM recognizes this and begins to act as the active OMM, and starts the web service.

If the connection between the two OMMs fails, the network or cluster essentially breaks into two operational parts. The standby OMM becomes the active OMM. At this point, the two OMMs cannot detect one another and, therefore, cannot synchronize. When the connection between the two OMMs is re-established, the synchronization of the OMMs forces one OMM to become the standby OMM again. Once the recently failed OMM returns to service and becomes the inactive OMM, it does not resume the role of active OMM.

8.15.1 CONFIGURING OMM STANDBY

Each RFP of the DECT system must be configured with two OMM IP addresses. Both OMM addresses can be either configured via DHCP (see section 8.5.1) or with the OM Configurator (see section 8.7).

8.15.2 FAIL OVER SITUATIONS

Fail over occurs when:

- an OMM error occurs on the active OMM.
- the RFP acting as the active OMM is shut down or rebooted at the SSH console.
- the OMM is rebooted in the web browser menu.
- the active OMM is unreachable.

The standby OMM becomes the active OMM when:

- the configured SIP Proxy/Registrar is reachable.
- the other OMM has a larger IP Address while no OMM is active and both OMMs are in contact with each other (normally at system startup).

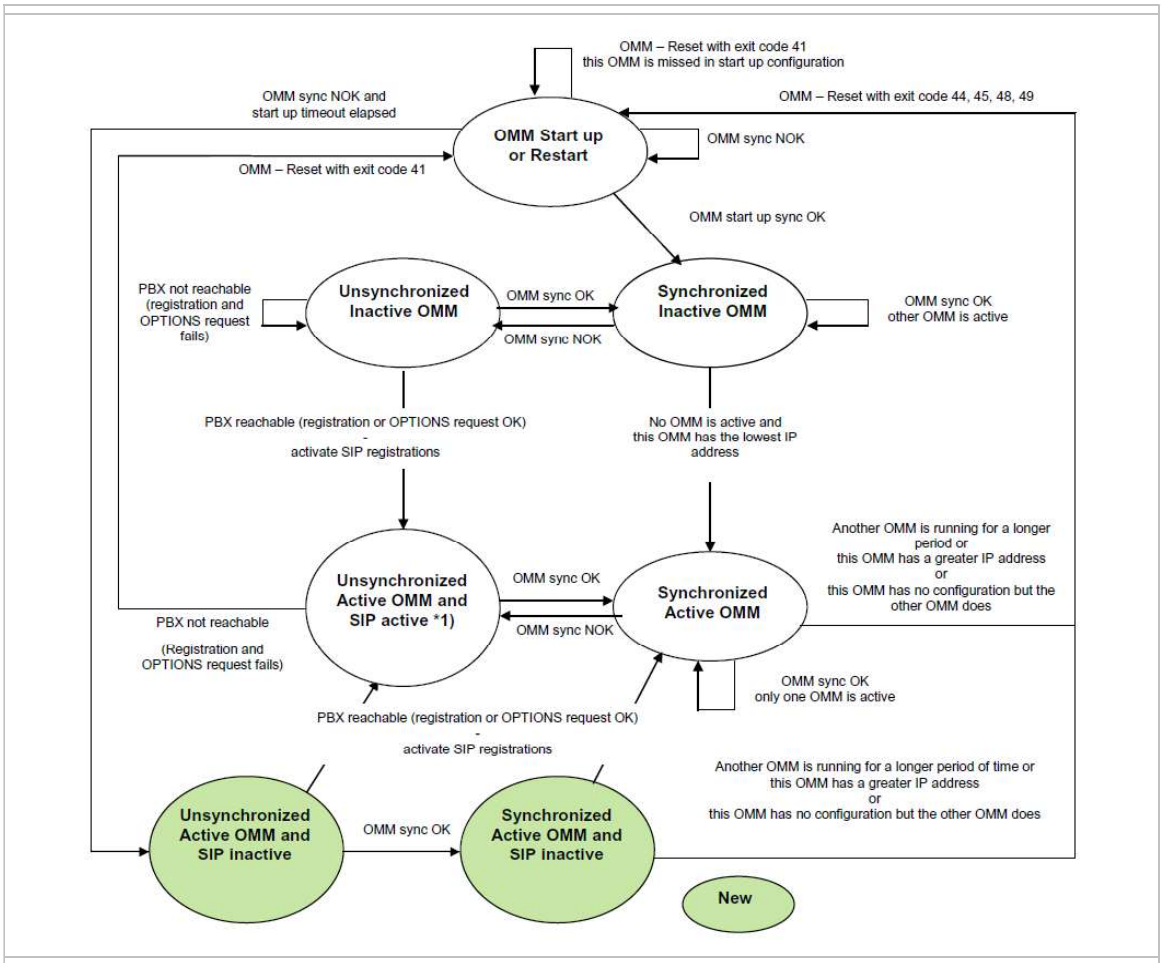
When the OMMs get in contact again:

- both OMMs check which one ran for a longer period. That one will become the active OMM. The other one falls back to the standby one.

8.15.3 FAILOVER FAILURE SITUATIONS

Failover failure occurs when the connection between OMMs fails and the configured SIP Proxy/Registrar is unreachable. In this case the active OMM waits until the SIP Proxy/Registrar is reachable.

The following state diagram shows the OMM Standby states:



"**OMM sync OK**": OMMs are synchronized and are able to exchange their operational states

"**OMM sync NOK**": OMMs are not synchronized and are not able to exchange their operational states

*1) In this state the DECT air interface might not be in a definite state as both OMMs are active but cannot connect with each other! This is caused by IP network failures and cannot be handled by the SIP-DECT system in a proper automatic way. In such a scenario it is not predetermined which RFP connects with which of the 2 OMMs. The DECT network can split-up into two unsynchronized DECT sub-networks. This can cause voice quality and handover problems.

With these states ("… SIP inactive") the OMM standby mechanism takes care in the start up phase that all SIP users does not become active if the PBX is not reachable. This avoids a possible double SIP

registration when the PBX and the other OMM is reachable again before both OMMs negotiate which OMM becomes the active one.

The double SIP registrations might cause a user not to be reachable when his latest SIP registration came from that OMM that was negotiated to be the inactive one and the SIP registrar cannot handle two or more simultaneous registrations (non-forking proxy).

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

To prevent such problems a mechanism is implemented to detect situations with two active OMMs. If such a situation is detected the remaining active OMM SIP re-registers all users to the PBX if the OMM **SIP reRegister after 2 active OMM failover** parameter is set (see section 5.4.3.6).

8.15.4 SPECIFIC STANDBY SITUATIONS

Some aspects must be described in case of OMM state changes when they are unsynchronized.

8.15.4.1 How a standby OMM becomes active

In an unsynchronized OMM state, the standby OMM must decide whether to become active or not.

The OMM tries to contact the configured SIP proxy and registrar. If a specific user account has not been designated to use for visibility checks (see section 8.20.7), the OMM starts a SIP registration for the DECT phone with the lowest phone number and sends an OPTIONS request to the configured proxy. If there is an answer the SIP proxy/registrar is considered reachable and the OMM becomes active.

8.15.4.2 When OMMs are not synchronized

In an unsynchronized OMM Standby state, the connection between the OMMs is broken. In case of a network problem, both OMMs might be in this state. During this time an inconsistent OpenMobility system is operational with some constraints.

The OMM Web service issues a warning with the message “No Standby” for both OMMs and it is possible that configuration changes made are not saved.

When both OMMs are in contact again, the longer running OMM becomes the active OMM and overwrites the database file in the standby OMM. Configuration changes made in this OMM instance are lost.

8.15.4.3 Two DECT air interfaces

When both OMMs are in an unsynchronized and active state, they are fully operational. DECT base stations that lose their connection to the OMM because of a network outage might connect to the other OMM. Two DECT air interfaces are present and work in parallel.

Note: Since both air interfaces use the same PARK, it is impossible to determine on which OMM a location registration succeeds.

For DECT phones different situations are possible:

- They do not notice this situation:
  - active calls stay established, depending on network conditions;

  - DECT phones can make and receive new calls, depending on an available PBX connection;
  - DECT phones can do handover to RFPs connected to the same OMM;
  - DECT phones can call DECT phones that are registered to the other OMM
- They lose their RFP base station and perform a new location registration:
  - active calls are broken;
  - DECT phones can make and receive new calls, depending on an available PBX connection;
  - DECT phones can do handover to RFPs connected to the same OMM;
  - DECT phones can call DECT phones that are registered to the other OMM;
- They lose their RFP base station and search the DECT network without finding another one:
  - active calls are broken;
  - DECT phones stay in searching for network until an air interface is available again.

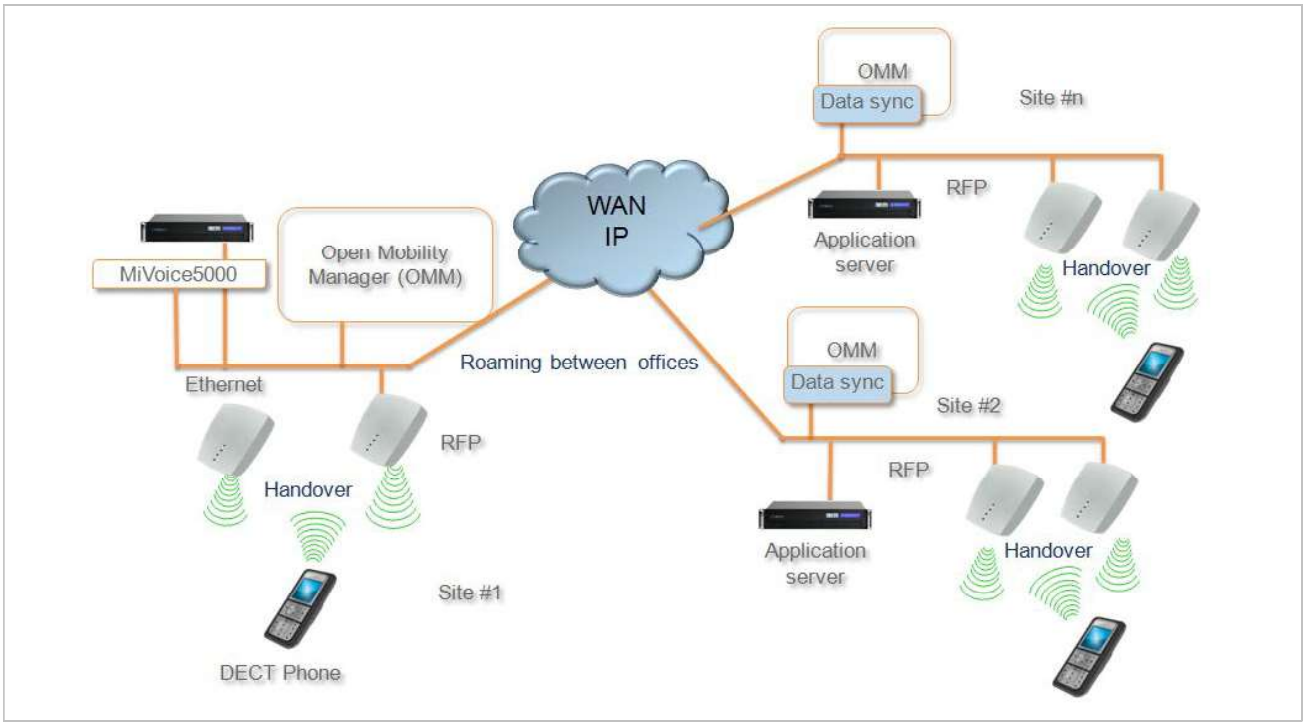
Note: Handover between DECT phones located to RFPs that are controlled by different OMMs is not possible.

When the OMMs are in contact again, the inconsistencies are resolved.

8.16 USER DATA SYNCHRONIZATION (MIVOICE 5000 DUAL HOMING SUPPORT)

SIP-DECT 6.1 introduces support for user data synchronization to ensure that SIP-DECT telephony services survive if the network connection to the OMM goes down. The feature ensures user and device database redundancy among all OMM instances in the system.

When user data synchronization is enabled on an OMM instance, the OMM propagates changes in user, device, Configuration over Air (CoA) profiles or SARI configuration to a central OMM. AXI is used to distribute configuration changes between the central and peripheral OMMs.



Instead of subscribing to the standard Primary Access Rights Key (PARK) of a single OMM when registering with the system, the DECT phones subscribe using the Secondary Access Rights Identifier (SARI) that applies to multiple OMMs in the system. All DECT phones that are subscribed to the system using the SARI can roam between sites (and OMMs). The PARK of the central OMM is defined to be the SARI.

Please note: Subscription to the SARI and successful roaming is only supported for Mitel 600 DECT phones. Behavior of third party GAP phones is not guaranteed. It is recommended that you add 3rd party GAP phones as fixed devices and configure them to subscribe to the “PARI only”. See section 6.10.4.5 for more information.

All DECT phone users are registered to a central SIP proxy, used by all OMM sites (as long as the network environment is stable). OMM sites may implement local secondary SIP proxies, where local DECT phones register in case of a failed network connection.

8.16.1 ROAMING

The following sections describe the roaming concepts supported with the user data synchronization feature.

8.16.1.1 Device roaming

All DECT phones that subscribe successfully to the system SARI can roam between sites. Subscription to the system SARI is enabled by default when a DECT phone is created. SIP registration is renewed automatically with the OMM at the new site so that users can make and receive calls from all sites.

Unbound devices can also roam, but they are not SIP registered.

8.16.1.2 User roaming

Users with existing DECT phones can go to another site and log into an unbound DECT phone. The login to the old DECT phone is removed, and when the SIP registration is renewed, the DECT phone is registered with the OMM at the new site, so that the user can make and receive calls from there.

8.16.1.3 Move of SIP registration

The SIP registration follows the user's location, according to the following rules:

- When the change in site location is detected, the new OMM initiates a SIP registration.
- All other OMM sites are notified of the change, such that the OMM for the previous site does not renew the DECT phone SIP registration and broadcasts the change to all other OMMs.
- When the new OMM receives the update from the previous OMM, the SIP registration is repeated.

If there is any interruption in the user data synchronization, other OMMs are not notified of the change. In this case, the OMM at the new site initiates a SIP registration a soon as the change in site is detected. If the OMM does not receive an update within 30 seconds, the new OMM renews the SIP registration anyway.

When user data synchronization is restored, the appropriate notifications resume:

- The previous OMM does not renew SIP registration for the DECT phone and broadcasts the information to all other OMMs.
- The OMM at the new site repeats the SIP registration when the update is received.

Please note: If the OMM hosting an active Mitel DECT phone does not receive an updated location registration for the device for more than two hours, the OMM does not renew the SIP registration until the location registration is refreshed.

8.16.2 SETTING UP USER DATA SYNCHRONIZATION

Data synchronization is only implemented for user, DECT phone, and Configuration over Air (CoA) data. The SARI is copied from the central OMM to the peripheral OMMs. All other data must be configured on each OMM individually. If there are any configuration conflicts due to network connection failure, the user and device changes (that have the same key id) with the most recent time stamp are used.

To set up user data synchronization for your SIP-DECT system, you must:

- define the central OMM and generate a SARI for all OMMs to use when registering to the system
- configure links to the central OMM from every peripheral OMM in the system
- create a dedicated user account to verify standby OMM availability

8.16.2.1 Defining the central OMM

You must select an OMM to act as the central OMM for user data synchronization. When you have selected the OMM, generate the SARI from the OMM's PARK value (via the OMP **System** -> **Basic settings** -> **DECT** tab). See section 6.5.1.2 for configuration details.

All Mitel 600 DECT phones registered with the OMM can then roam to all other OMM sites (which may be added later).

8.16.2.2 Configuring links to the the central OMM

Each peripheral OMM in the system must connect to the AXI interface of the central OMM for user data synchronization. If a standby configuration is used for the central system, both OMMs must be configured in the peripheral OMMs. You configure the connection to the central OMM via the OMP **System** -> **Data management** -> **DECT phones synchronization** tab (see section 6.5.7.3 for configuration details).

Before you link a peripheral OMM to the central OMM, you must delete all user and device data, and CoA profiles from the local OMM. After the connection is established, verify that the user and device data from the central OMM have been received, then reconfigure the deleted users and devices.

> **Please note:** Concurrent configuration of user and device data may cause conficts. This can happen if one or more OMMs are not visible due to network issues. If conflicts are detect for user or devices with the same key Id, those with the most recent timestamp are kept.

SIP-DECT provisioning mechanisms ensure that there are no conflicts with user data synchronization. However, the system cannot regulate operations such as "auto-create on subscription". Under rare circumstances, conflicts can arise with the result that a user action may be ignored. Repeat the action to ensure it is registered by the system.

You must also ensure that the calling party numbers do not conflict with any conference room, FAC prefix or alarm trigger number across all OMMs in the system.

> **Please note:** The user data synchronisation mechanism does not validate conference room, FAC prefix or alarm trigger numbers. If such numbers conflict with a user's calling number, synchronisation terminates immediately.

8.16.2.3 Creating a user account for standby visibility checks

If the active or standby OMM loses connectivity, each OMM checks connectivity to the SIP proxy. By default, a real SIP user account is used to check the availability of the OMM (via a SIP registration to the SIP proxy). In a dual homing environment, this may impact the user's telephony services due to the data synchronization.

To avoid this issue, you must create a virtual SIP user to be used exclusively for checking OMM availability (one account for the entire system). See 8.20.7 for more information on this feature.

8.16.3 USER DATA SYNCHRONIZATION MODES

The user/device synchronization runs on every peripheral OMM with a configured link to the central OMM. The synchronization function requires an internal AXI connection and an external AXI connection to the central OMM.

There are two synchronization modes: System startup or reconnection to resolve conflicts and copy new or changed datasets, and dynamic synchronization mode.

8.16.3.1 Start-up / reconnection mode

In start-up/reconnection mode, the user data synchronization service reconciles the data in the peripheral OMMs and central OMM. The steps in the user data synchronization mechanism are:

1 Read user/device data and profiles from internal AXI.

2 Read SARI from external AXI.

3 Set SARI on internal AXI.

4 Read user/device data and profiles from external AXI.

5 Resolve conflicts.

- **Inconsistent associations** (one device bound to two different users): Association is deleted on the system with the older user/device timestamps. An unbound user remains.
- **Inconsistent number** (two different user datasets using the same number): The user with the older timestamp is deleted (including any existing device associations)
- **Inconsistent additional ID** (two different user datasets with the same additional ID): The user with the older timestamp is deleted (including any existing device associations)
- **Inconsistent association** (one user bound to two different devices): Association is deleted on the system with older user/device timestamps. An unbound device may remain if an IPEI was configured, otherwise the device is deleted.
- **Inconsistent IPEI** (two different device datasets with the same IPEI): The device with the older timestamp is deleted (including any existing user associations)

6 Copy data.

Data with the most recent timestamp is copied to either the peripheral OMM (if data in the central OMM is more recent) or the central OMM (if data in the peripheral OMM is more recent), including:

- profile datasets with newer timestamps
- changed users with newer timestamps (with the device dataset, if bound)
- new users (with the device dataset, if bound)
- changed unbound devices with newer timestamps
- new unbound devices

8.16.3.2 Dynamic mode

In dynamic synchronization mode, events related to new, changed, or deleted users/devices received from one OMM are applied on the other OMM.

In rare cases, when configuration changes are made on multiple OMMs simultaneously (e.g. by configuration via OMP/Web, login/logout on devices, auto-create on subscription, etc), thereby creating new conflicts, the user data synchronization service closes the AXI connections and restarts after a minute to initiate a new synchronization.

8.17 MANAGING ACCOUNT DATA FOR SYSTEM ACCESS

Each RFP provides different independent access types:

- The OMM Web service/HTTPS interface (see section 5);
- The OMP (see section 6);

The OMM Web service and the OMP are mainly used for configuration and administration.

- The OM Configurator (see section 8.7);

The OM Configurator is mainly used for static local configuration of an RFP.

- The SSH user shell (see section 9.3.5).

The SSH user shell is mainly used from experts for diagnosis.

Each of this these access types uses the same account data.

The account data can be altered at the **User account** page of the OMM Web.

The OMM delivers all the necessary account data to all connected RFPs. The RFPs save the account data inside their permanent memory. This has some implications:

- An RFP out of the box uses the default account data as long as this RFP is not connected to the OMM.
- An RFP which was connected for at least one time with the OMM uses the account data from the OMM.
- When the account data are changed on the OMM, any not connected RFPs will continue to use the older passwords.

8.17.1 ACCOUNT TYPES

There are three different account types:

- **Full access**: This access type is the “normal” access for the configuration. Using this access it is allowed to configure the OMM and each RFP. On the SSH interface of an RFP this access type allows login for debug information e. g. “pinging” another RFP to check visibility.

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

- **Read-only access**: As the name suggests this access type is not allowed to configure any item of the OMM installation. This access type can only be used on the OM Web service. The account can be deactivated.

The factory setting for this account is
Name: 'user'
Password: 'user'
Active: 'yes

- **Root (SSH only) access**: This access type is only applicable on the SSH interface of an RFP. Its purpose is to get detailed information e. g. parameters from the kernel. The access using this account type is not reachable from other hosts hence a login using the full access type is necessary.

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

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

8.17.2 POTENTIAL PITFALLS

When an RFP is configured via the OM Configurator and is taken out of an installation, the RFP may become unusable:

- When this RFP comes up, it finds a valid configuration in its permanent memory. It will hence skip DHCP for booting.
- But when this configuration is not valid anymore (e.g. the TFTP server has a new IP address meanwhile), the RFP isn't able to complete the boot and is hence not able to connect to the OMM.
- The RFP will not get newer passwords from the OMM.

It is therefore recommended to switch of the OM Configurator before taking an RFP out of an installation. But nevertheless the OM Configurator allows to reset the permanent memory of an RFP (the Mitel support must be connected).

8.18 WLAN CONFIGURATION

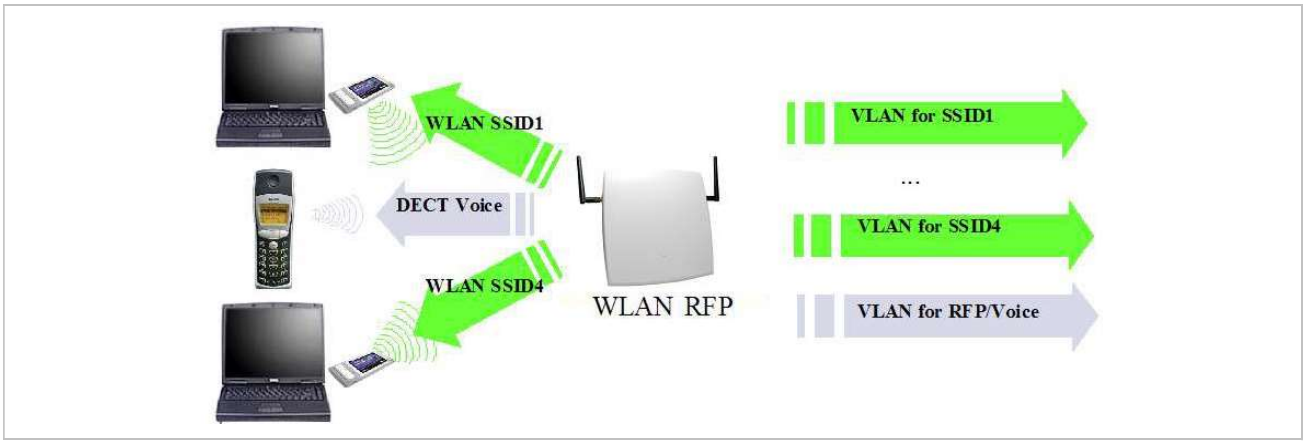
8.18.1 WLAN CONFIGURATION STEPS (RFP 42 WLAN / RFP 43 WLAN ONLY)

The correct configuration of an RFP with a WLAN interface requires the correct configuration of the DECT part. The second step is to specify the **Regulatory domain** of the WLAN network at the **System settings** page of the OMM web service (see section 5.4.1.3).

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

Select one of the two-letter country codes. This setting depends on the country and is prescribed by the laws of that country. Only the setting prescribed for that country must be used.

The third step is to specify the WLAN parameters in a profile (see section 5.8.1). The WLAN profile determines the name (SSID) of the WLAN network and other parameters. The encryption and authentication procedures are especially important and must be planned carefully beforehand.



The access point can be assigned to a VLAN that conforms to 802.1q. All the data that is received from and that is to be forwarded to the WLAN clients is then carried by the configured VLAN. All other data, such as VoIP packets, configuration data or authentication data (Radius), is given the VLAN tag configured for the RFP. The switch port of the network component to which the access point is connected must be configured as a trunk port.

Note: The RFP 42/43/48 WLAN must be connected at least via a 100BaseT Ethernet link in order to activate the RFP's WLAN function.

As a forth step, you must assign a WLAN profile to a configured RFP. This can be done on the **DECT base stations** page of the OMM web service or on the OMP **DECT base stations** -> **Device list** page. Note that specific radio settings for the RFP, such the channel-, 802.11abgn mode-, or antenna settings, are also done in this step.

8.18.2 WLAN CONFIGURATION STEPS (RFP 48 WLAN)

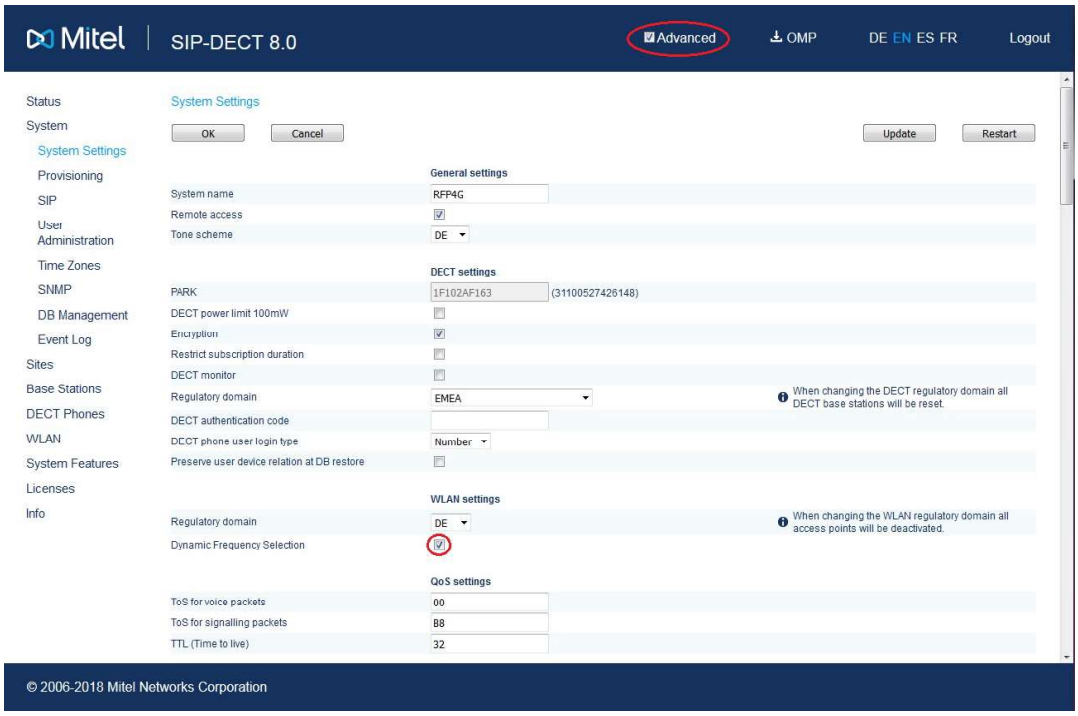
8.18.2.1 Support of 802.11ac WLAN

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

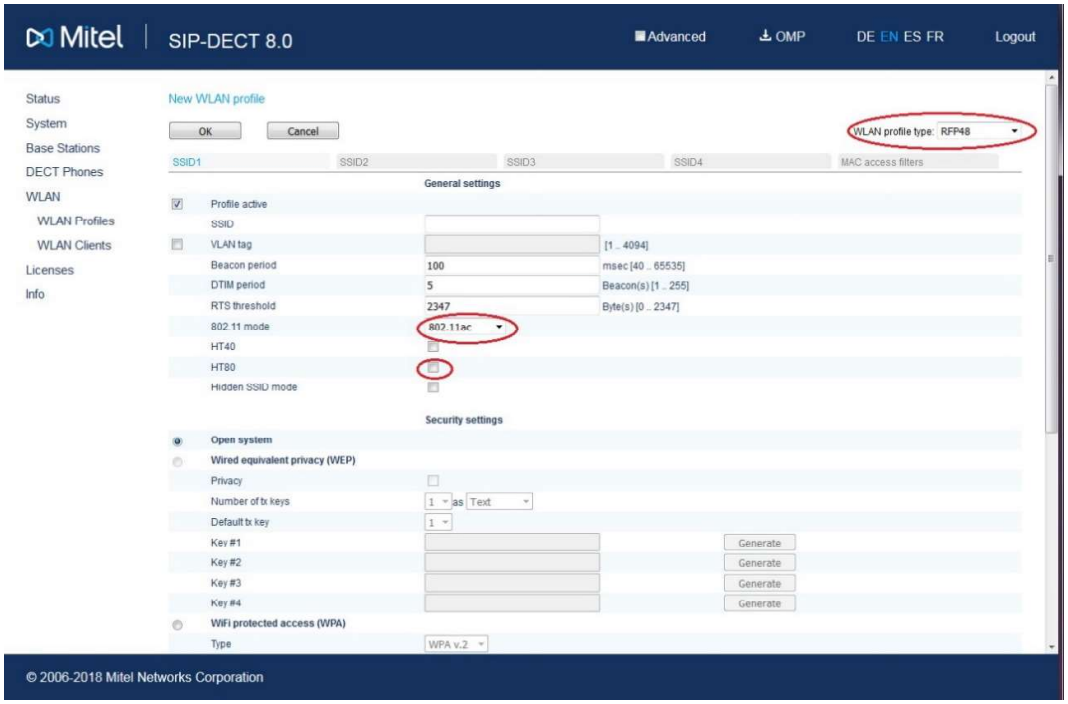
In ac mode, HT80 channel bandwidth and 256-QAM modulation increase the data throughout up to 1300 Mbps.

To enable the DFS channels,

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

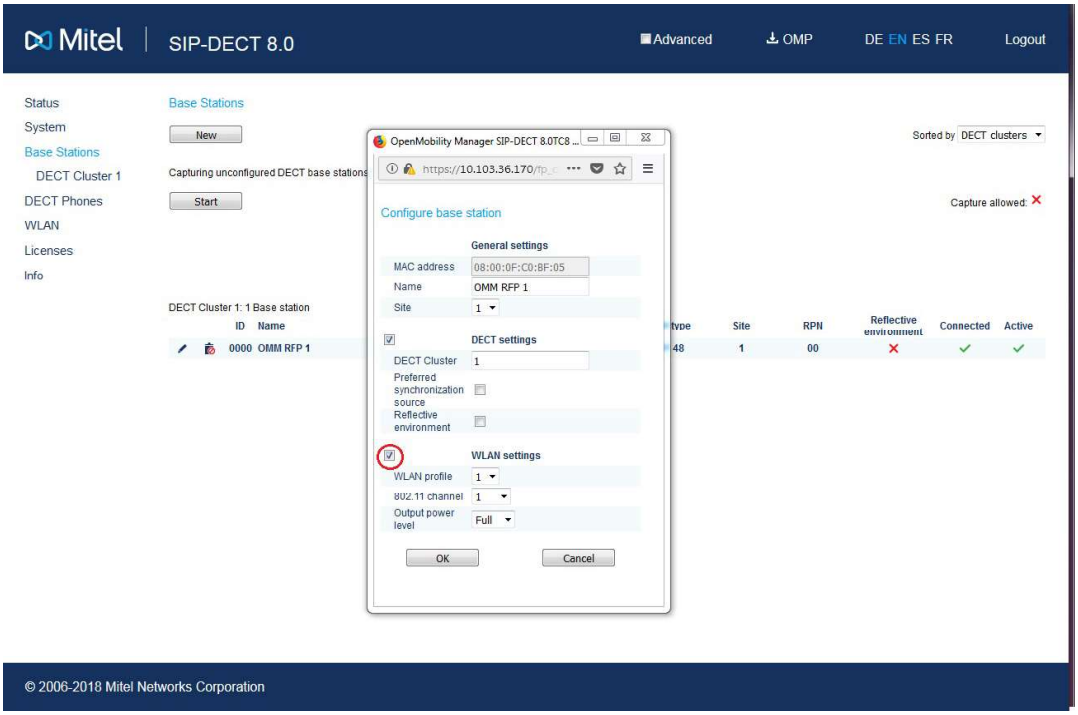


- to enable the ac mode and HT80: WLAN\WLAN Profiles (new/edit).



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).

8.18.3 OPTIMIZING THE WLAN

Beacon Interval

Transmitting beacons requires transmission channel capacity. A shorted beacon interval increases the WLAN network's ability to detect signals, thus improving its availability. At the same time, it increases the network's ability to adjust the mutually negotiated signal strength. A longer beacon interval saves WLAN air time and also reduces the power consumption of mobile WLAN clients.

RTS Threshold

If the network throughput is low or if many retransmissions occur, the RTS/CTS handshake can be activated by reducing the RTS threshold value below 1500 byte. This can improve throughput, especially in environments where reflection and attenuation cause problems for HF.

Fragmentation Threshold

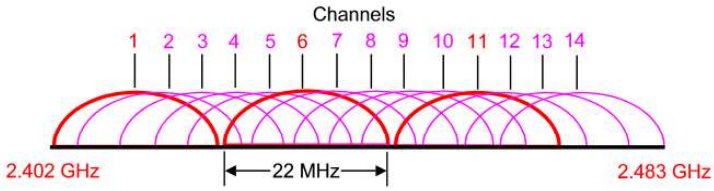
In environments where there is lot of interference and poor radio quality, reducing the fragment size below 1500 bytes can improve the effective throughput. However, transmitted data frames must be fragmented, which means a higher load on the RFP’s processor. This option is not configurable with RFP 48 WLAN.

DTIM Period

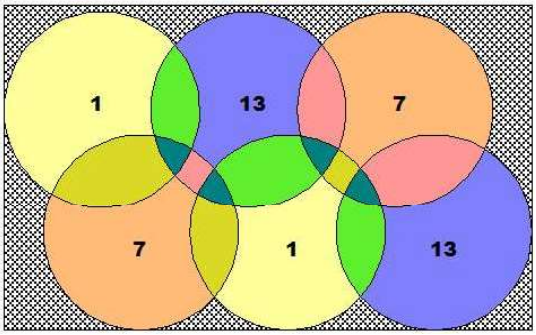
The DTIM period specifies the interval between transmissions of the broadcast and multicast packets. All WLAN clients must be active during this interval. Increasing the DTIM period lowers the client's power consumption slightly. Not all programs can manage the increase in response times, however.

Channel Allocation

Every WLAN RFP must be configured to a channel. You should ensure that the channel settings do not overlap. WLAN RFPs within range of each other should be configured at least five channels apart. When the radio field is planned, the WLAN RFPs of foreign WLANs that may be operating in the vicinity must be taken into account.



When planning the radio coverage for a two-dimensional area, please bear in mind that the distance between any two base stations operating on the same frequency must be at least twice their range. The range can be adjusted by lowering the output power level.



802.11i: WPA2-Enterprise Pre-Authentication for fast Roaming

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

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

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

Channel Configuration Feedback for HT40 and Transmit Power

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

The effective channel configuration and the transmit power are reported to the OpenMobility Manager.

Users can inspect these parameters using the WEB interface and the OMP and may change the channel to a frequency without overlapping APs.

Support of 802.11ac-WLAN for RFP 48 WLAN

The RFP 48 WLAN is a new WLAN module, which supports the WLAN ac mode wave 1. Within the 5 GHz spectrum, the ac mode is 2,5x faster as the ‘n’ mode of WLAN. The RFP 48 is 4x faster with comparison to the RFP 43 having two antennas. This is achieved by more efficient coding (256-QAM) with more bandwidth (HT80) per channel and one more antenna (3x3 MIMO compared to the RFP 43: 2x2 MIMO).

For more information about data rates, see: *http://mcsindex.com/*

8.18.4 SECURING THE WLAN

In order to ensure that communication in the WLAN network is secure, several measures must be taken. Firstly, data packets transmitted via the openly visible radio interface must be encrypted, and secondly, all WLAN components that provide services must authenticate themselves.

There are different encryption methods available that you configure within the WLAN profile (see section 5.8.1). However, only the recent WiFi protected access (WPA) encryption offers sufficient security against possible intruders. You should not use the (older) WEP encryption for your company LAN.

Especially with larger WLAN installations, the single shared secret offered by WPA-personal may not be sufficient for your security requirements, because any person that connects to the WLAN needs to know the same shared secret. For this reason, you should also setup RADIUS authentication that is supported by all RFP 42 WLAN, RFP 43 WLAN and RFP 48 WLAN devices.

A Radius Server (Remote Authentication Dial In User Service) handles 802.1x Authentication, thus authorizing different WLAN clients with an individual username / password combination to log in. We recommend a Radius Server with EAP-TLS (e.g. FreeRadius or MS Windows 2003 IAS Server) and a Certificate Authority (CA).

The RADIUS authentication takes place between the RADIUS server and the RADIUS client, with the WLAN RFP to pass-through this communication. You should refer to the documentation that comes with your RADIUS product for details on how to setup, maintain and operate the RADIUS system.

The WLAN module of RFP 48 supports Dynamic Frequency Selection (DFS) and Transmit Power Control (TPC). These features are required for the radar detection (flight and weather) and are necessary to use the WLAN channels 52 – 140 in Europe and USA. If radar pattern detected, the RFP 48 changes its WLAN channel by itself to another channel without radar for half an hour. The 5GHz high band with its channels 149 – 165 is supported too.

8.19 SNMP CONFIGURATION

To manage a larger RFP network, an SNMP agent is provided for each RFP. This will give alarm information and allow an SNMP management system (such as “HP Open View”) to manage this network. The SNMP agents can be configured in the **SNMP** menu of the OM Web service (see section 5.4.6).

All SNMP agents are configured by the OMM. Additional parameters that are valid for the individual RFP (e.g. “sysLocation” and “sysName”) are generated. The “sysLocation” parameter corresponds to the location configured via the OMM web interface. The “sysName” parameter is generated using the MAC address and the RFP device type (e.g. RFP 43 WLAN). The RFP uptime can be requested by reading the “sysUpTime” parameter. This value indicates how long the RFP application software is running. It does not indicate the uptime of the operating system which does not correspond to the operational RFP state.

The SNMP agent responds to SNMPv1-read and SNMPv2c-read requests for the standard MIB-II objects. The Management Information Base (MIB-II) contains 11 object groups. The agent receives both SNMPv1 and SNMPv2c traps. It sends a “coldStart” trap when it first starts up. It also sends an

enterprise-specific trap “nsNotifyShutdown” when it stops. When the SNMP agent receives an SNMP request using an unknown community name, it sends an “authenticationFailure” trap. The SNMP agent also generates an enterprise-specific trap “nsNotifyRestart” (rather than the standard “coldStart” or “warmStart” traps) after being reconfigured.

8.20 BACKUP SIP PROXY/REGISTRAR

This section provides an overview about the supported redundancy concepts with SIP-DECT to realize a high availability solution together with IPBX redundancy mechanism.

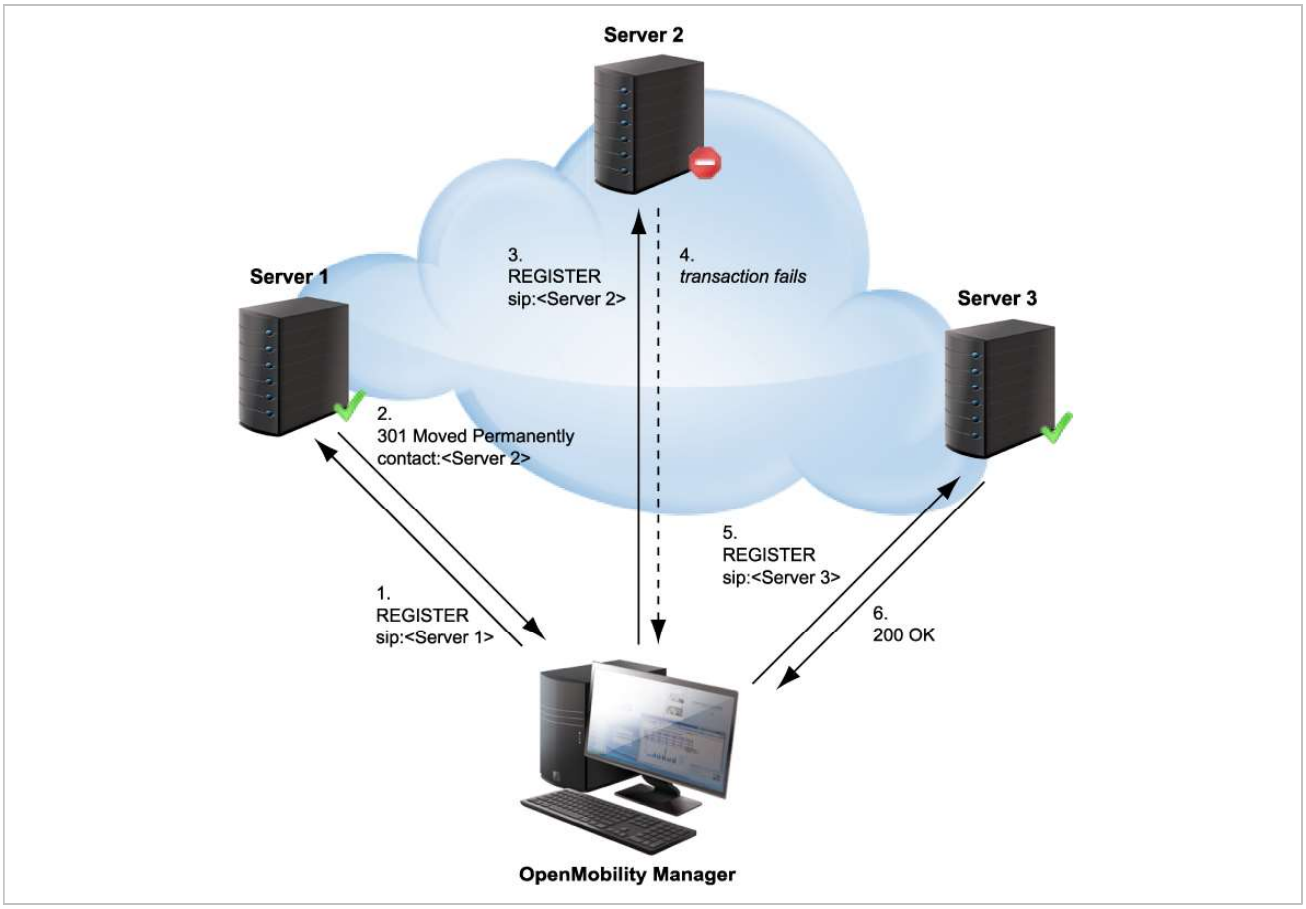
The focus of this section is IPBX redundancy. For information regarding OMM redundancy, see section 8.15.

8.20.1 REGISTER REDIRECT

To allow IPBX systems to spread the registration and call traffic over different servers the OMM supports 301 (Moved Permanently) or 302 (Moved Temporarily) responses for registrations.

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

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

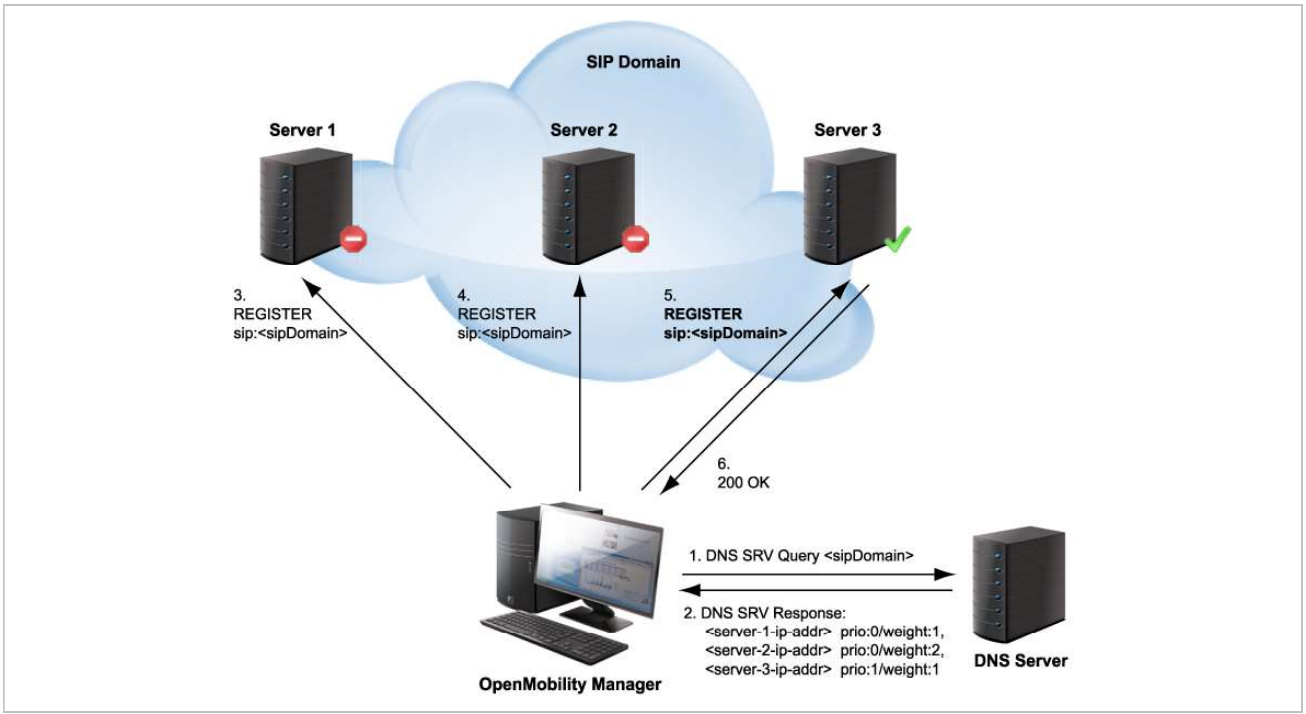


8.20.2 DNS SRV

If a full qualified domain name is configured as proxy, outbound proxy or registrar server and the respective port setting is set to zero (“0”), the OMM performs a DNS SRV query before an appropriate SIP transaction is started. Herewith the OMM locates a list of servers responsible for the given SIP domain. With this configuration, the default port (“5060”) is used for every server address acquired with this mechanism.

The DNS SRV results are sorted by priority and weight in ascending order by the OMM. As soon as the DNS SRV query succeeds, the OMM starts the appropriate SIP transaction by sending the request to the server with the uppermost priority and weight of the DNS SRV result.

If there is no answer from the first SIP server in a configurable time frame (“Transaction Timer” parameter), or a 5xx response is received, it will be assumed as unreachable and the OMM tries to contact the next server of the DNS SRV result. Therefore the request will be send to the second server of the DNS SRV query result. If there is also no answer in the given time frame or a 5xx response is received from the second server, the request will be send to the third server and so on. When there is an answer other than 5xx from one of the contacted servers, this server will be used for this transaction.



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

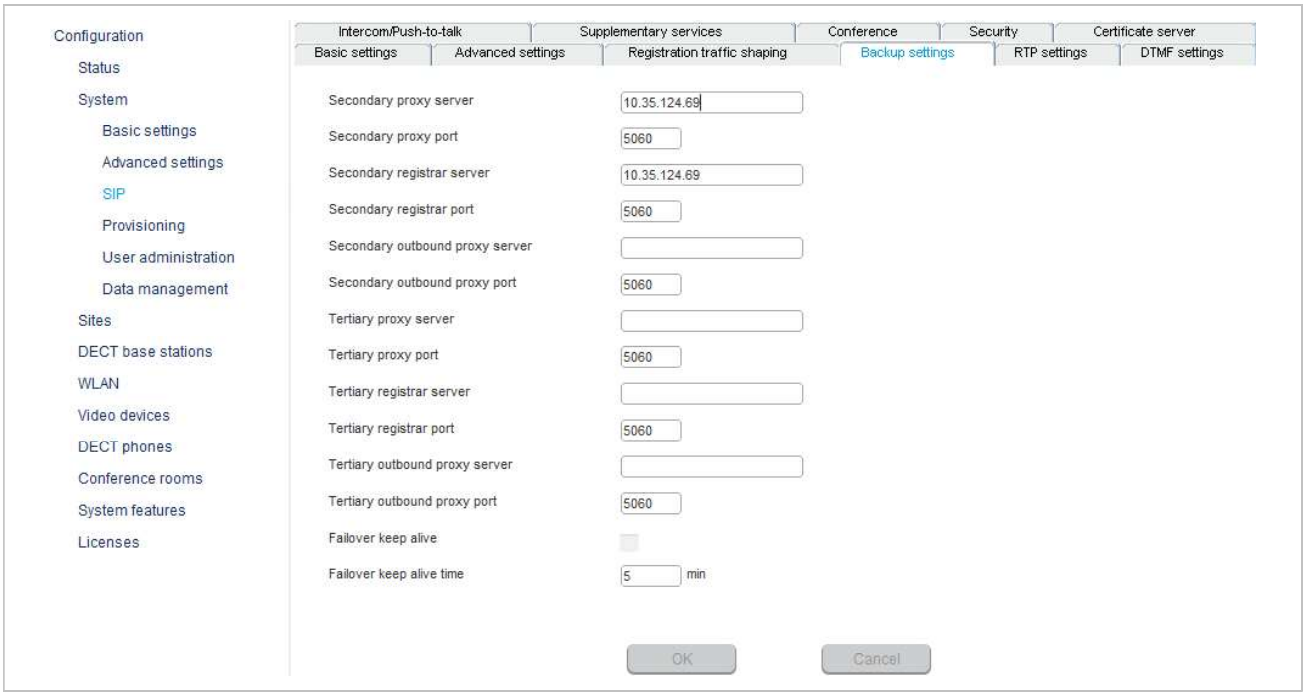
In differentiation to the concepts described in the following sections note that independent of which SIP server is used, all requests send by the OMM carry the same sender Address-of-Record (AOR)[1]. This

[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.

means that the sender URI consisting of user-ID and domain is not changed during a failover to another server.

8.20.3 BACKUP SIP SERVERS

The SIP-DECT solution allows configuration of two additional levels of backup servers, in addition to the primary proxy, outbound proxy and registrar server. These two additional levels of backup servers are referred to as secondary and tertiary servers in the following sections.



SIP backup servers can be configured in the **System** -> **SIP** menu of the OM Management Portal (OMP), see also section 6.5.4.

You can configure IP addresses, names or full qualified domain names as server addresses. It is also possible to configure a mixture of IP addresses, names or full qualified domain names for the different servers.

If fully qualified domain names are configured and the respective port setting is configured to zero (“0”), DNS SRV queries are performed to locate a list of servers in the domain. It is assumed that all server addresses are specified by name or IP address. With fully qualified domain names, the behavior described in section 8.20.2 is performed in addition to contact the SIP servers in the given domain.

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

The OMM failover behavior in detail depends on the backup server settings.

8.20.3.1 No Secondary/Tertiary Proxy, Outbound Proxy and Registrar Configured

In this case is no failover to a secondary/tertiary (outbound) proxy / registrar is possible.

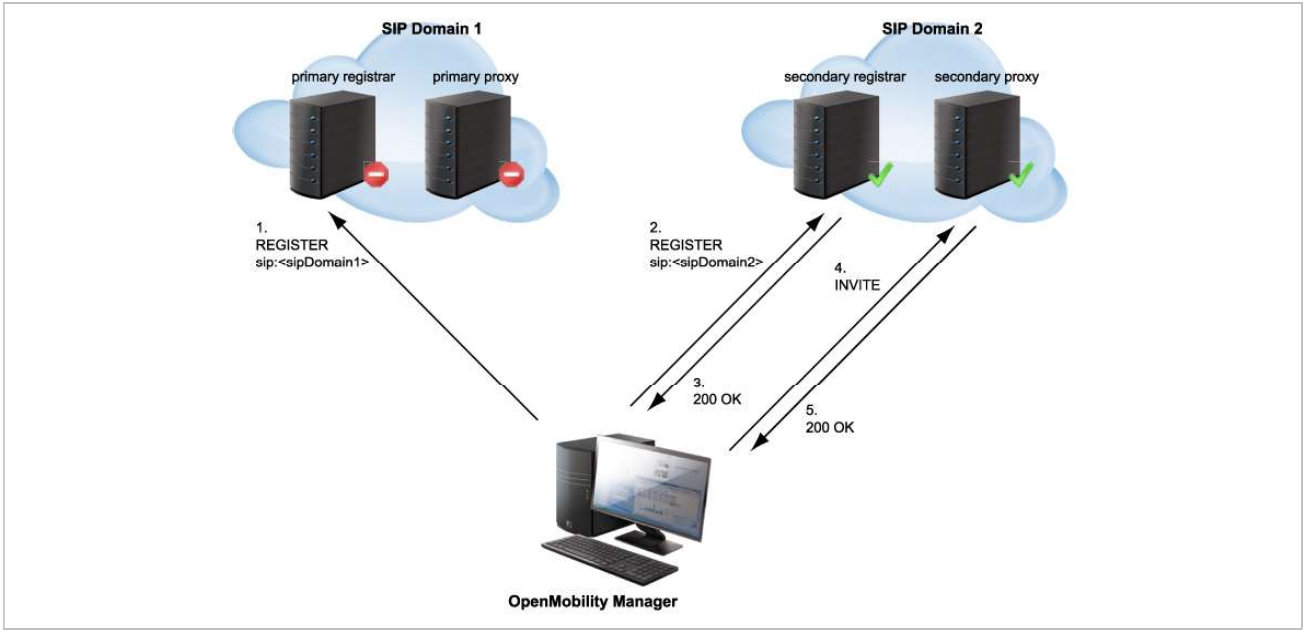
8.20.3.2 Secondary/Tertiary Proxy and Registrar Configured

All REGISTER and re-REGISTER requests attempt to use the primary registrar first.

If the primary registrar fails (e.g. no answer in “transaction timer” time frame), the user is tried to register with the secondary/tertiary registrar using as AOR the secondary/tertiary proxy address.

When the registration with the secondary/tertiary registrar succeeds:

- the MWI subscription is moved to the secondary/tertiary proxy,
- all subsequent INVITE requests attempt to use the secondary/tertiary proxy,
- the registration of all other users currently registered with the failed server will be automatically refreshed if the “Failover keep alive” setting is enabled (see page 141). For this purpose, the re-register requests will be queued and proceed according to the settings for “Registration traffic shaping” (see section 5.4.3.5).



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,
- all subsequent INVITE requests attempt to use the primary (outbound) proxy again,
- the registration of all other users currently registered with the secondary/tertiary registrar will be automatically refreshed.

As long as no successful registration exists, all INVITE requests attempt to use the primary (outbound) proxy as first.

If the INVITE request to the primary proxy fails, the INVITE request attempts to use the secondary/tertiary proxy. If an INVITE request fails (no answer in “transaction timer” time frame) send to a proxy identical with own registrar, the registration will be refreshed.

8.20.3.3 Secondary/Tertiary Proxy, Registrar and Outbound Proxy Configured

In this case, the OMM behavior is as described in section 8.20.3.2 but all requests for the secondary/tertiary proxy/registrar are sent through the outbound proxy.

8.20.3.4 Secondary/Tertiary Proxy Configured Only

All REGISTER, INVITE and SUBSCRIBE requests attempt to use the primary proxy or registrar first.

If an INVITE/SUBSCRIBE request fails, the INVITE/SUBSCRIBE request attempts to use the secondary/tertiary proxy.

8.20.3.5 Secondary/Tertiary Outbound Proxy Configured Only

The OMM behavior is as described in section 8.20.3.2, but:

- all requests for the secondary/tertiary proxy/registrar are send through the outbound proxy;
- if the registration with the primary registrar fails, the registration is re-tried using the primary proxy address as AOR sent through the outbound proxy.

8.20.3.6 Secondary/Tertiary Registrar Configured Only

All REGISTER, INVITE and SUBSCRIBE requests attempt to use the primary proxy or registrar first.

If a REGISTER request fails, the request attempts to use the secondary/tertiary registrar.

8.20.4 KEEP ALIVE MECHANISM

A keep-alive mechanism implemented in the OMM allows the automatic failover to secondary/tertiary servers or automatic coming back to primary servers. The keep-alive mechanism is based on the registration process and utilizes the special behavior that all REGISTER and re-REGISTER requests are sent to the primary registrar first.

The following configuration parameters are introduced: **Failover keep alive** and **Failover keep alive time**. These parameters are set in the OM Management Portal (OMP) on the **Backup settings** tab of the **System**: **SIP** menu (see page 141).

For each registration target, a user could be registered successful with, a keep alive procedure is started. For this purpose the first user registered successful on a registration target will be selected to re-register all “Failover keep alive time” before the registration period expires.

If the re-registration of this selected user detects that the current primary server fails, the registration of all users registered on the same server will be refreshed automatically. For this purpose the re-register requests are queued and proceed according to the registration traffic settings (see section 5.4.3.5 for OMM Web or section 6.5.4.3 for OMP).

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

8.20.5 PRIORITIZED REGISTRATION

Depending on the settings for “Registration traffic shaping”, the registration of a high number of users could need minutes. In effect single users could not be reachable for minutes during startup.

To guarantee a minimum blackout for very important people (e.g. emergency user) the registration of such people can be prioritized. Therefore a special user attribute VIP (very important person) is introduced. The corresponding option is set in the **SIP** tab of the DECT phone **Detail** Panel (see page 178).

8.20.6 MONITORING THE SIP REGISTRATION STATUS

The SIP registration status of a DECT phone user can be monitored by using the OpenMobility Management Portal (OMP). In OMP monitor mode you can view on which registrar a specific DECT phone user is registered and whether the server is a primary, secondary or tertiary server. To monitor the SIP registration status proceed as follows:

1 Launch the OMP (see section 6.1) and navigate to the **DECT Phones** -> **Overview** menu.

2 Switch to **Monitor Mode**.

3 Activate the **Registered**, **Registrar server type**, **Registrar server** and **Registrar port** columns (see section 6.10.9).

8.20.7 CONFIGURABLE USER ACCOUNT FOR STANDBY CHECK

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

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

With older SIP-DECT releases, the OMM used the user account with the lowest phone number for the check procedure.

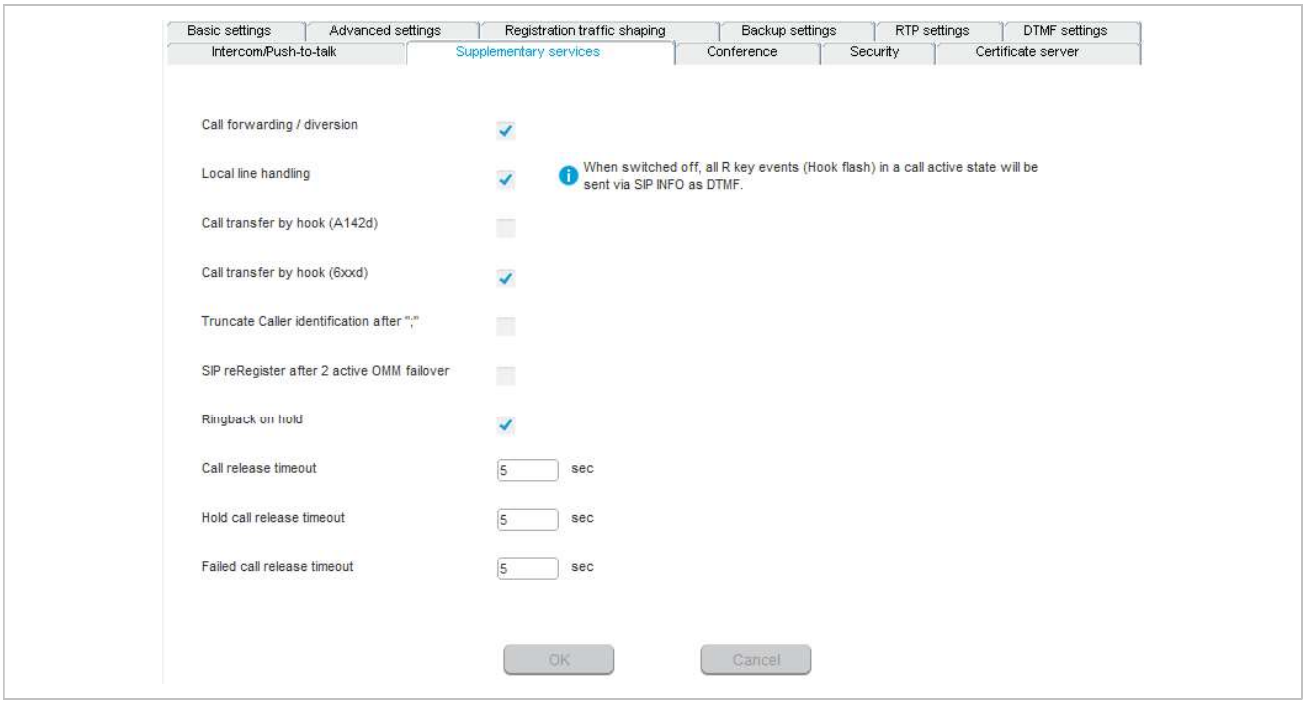
To select a specific user account for this purpose, enable the **Used for visibility checks** flag on the **SIP** tab when creating or editing a DECT phone.

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

8.20.8 OMM STANDBY ENHANCEMENT

With SIP-DECT systems using the OMM standby feature it could happen in rare cases that both OMMs become temporarily active. In such a situation all SIP-DECT users were SIP registered from both OMMs to the configured PBX. This can cause problems, when the PBX accepts only one registration per user (non-forking proxy).
To prevent such problems a mechanism is realized to detect situations with two active OMMs. When such a situation is detected the remaining active OMM will SIP re-register all users to the PBX.

This mechanism can be enabled/disabled via the OMP **SIP->Supplementary Services** tab (see section 6.5.4.8).

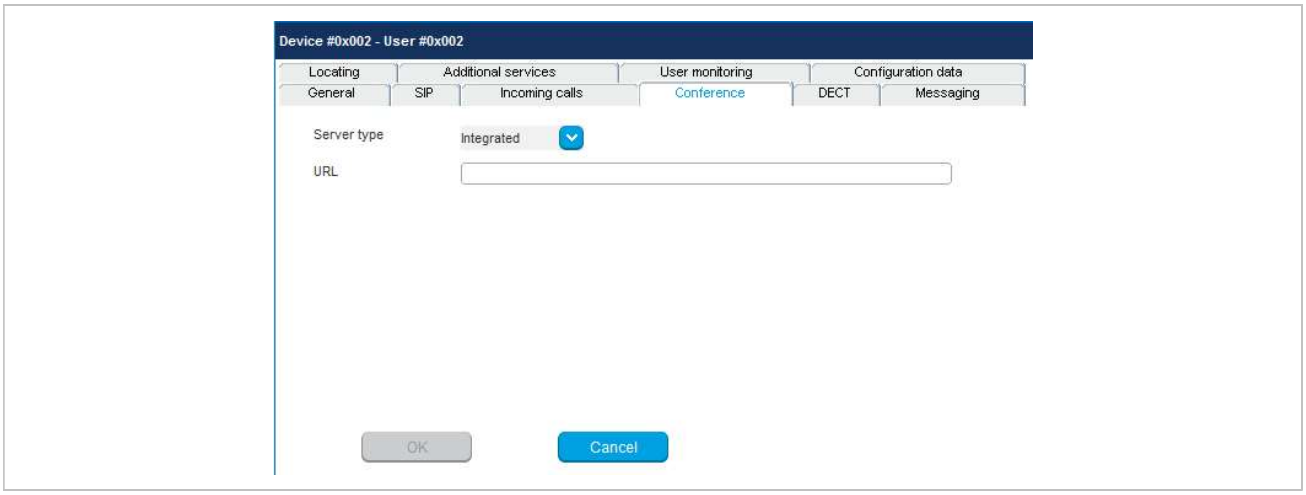


8.21 CONFERENCING

Depending on the type of conference server used, SIP-DECT offers the following operational modes:

- **None**: Neither external nor internal conference server is used.
- **Integrated**: The conference server integrated in SIP-DECT is used.
- **External**: An external conference server is used, e.g. Broadsoft or Sylantro. 407-oamp-sys-sip-conference.tif
- **External** – Blind Transfer: A MiVoice Business conference server is used, whose proprietary SIP signaling requires that the initiation of the conference be signaled to the destination (as specified in the URL parameter) as a blind transfer.

The conference mode can be configured globally for all SIP-DECT users on the OMP **System** -> **SIP** -> **Conference** tab (see section 6.5.4.9). Alternatively, the conference mode for individual users can be configured on the OMP **DECT Phones** -> **Users** -> **Conference** tab (see section 6.10.4.4). When the **Global** setting is selected for a user, the global system conference mode will be used for this user.



The default for the global system conference mode is **None**. For the user-specific mode, the default is **Global**.

The global and/or user specific conference mode can also be configured via OMM configuration files or the OMM application XML interface (AXI).

8.21.1 CENTRALIZED CONFERENCING

To enable SIP centralized conferencing on DECT phones select **External** as **Server type** for all users on the OMP's **System** -> **SIP** page or for specific users on the OMP's **DECT Phones** -> **Users** page.

If there is specified a proxy / registrar server, then to reach the conference media server via the proxy server, set the **URI** field to one of the following prefixes:

- **Conf** (Sylantro server)
- **Conference** (Broadsoft server)

Examples

To set the **URI** field to "conf" or "Conference", specify "conf@<proxy-server-address>:<proxy-port>" or "Conference@<proxy-server-address>:<proxy-port>".

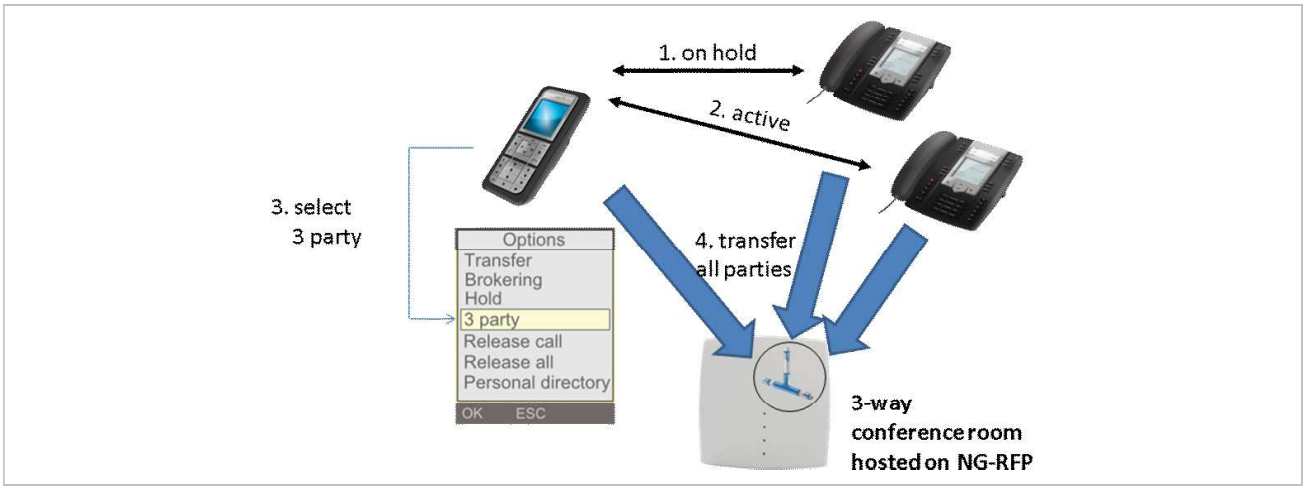
To reach the conference media server using a different address/port then that is specified by the proxy, set the **URI** field to "conf@<media-server-address>:<media-port>"

8.21.2 INTEGRATED CONFERENCE SERVER (ICS)

The conference server integrated in SIP-DECT is based on the SIP standard RFC 4579 and allows SIP-DECT users the ad-hoc initiation of 3-way conferences.

If this feature is enabled, it allows SIP-DECT users having an active call and holding another call to select **3 party** in the **Options** menu of a Mitel 600 DECT phone to initiate an ad-hoc 3-way conference. If a 3-way conference is initiated, the conference initiator and both connected parties are transferred to the next free conference room hosted on one of the RFP 35 / 36 / 37 / 43 devices.

ICS provides the full range of voice codecs (G722, G711 µ-law, G711 a-law and G729) and supports trans-coding for all parties in a three-way conference session.



Enabling the SIP-DECT integrated 3-way conferencing requires the following configuration steps:

- Enable internal conference mode
- Select RFP devices for conferencing
- Configure conference rooms

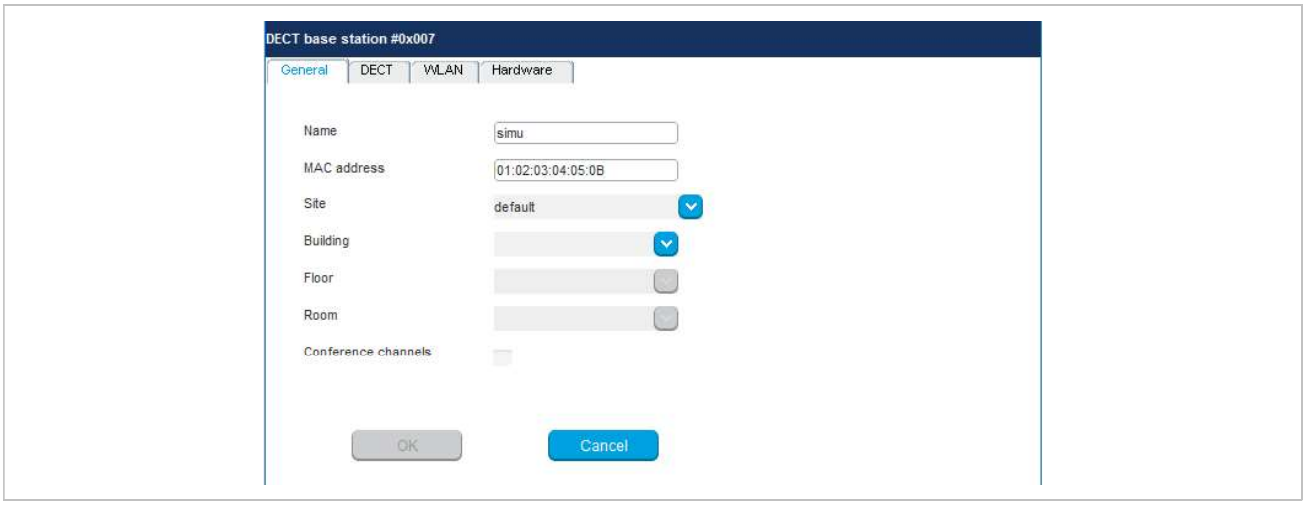
8.21.2.1 Enable internal conference mode

To enable SIP-DECT internal 3-way conferencing for DECT phones select **Integrated** as the **Server type** setting for all users on the OMP's **System**-> **SIP** page or for specific users on the OMP's **DECT Phones** -> **Users** page.

8.21.2.2 Select RFP devices for conferencing

Select some of the RFP devices from your SIP-DECT infrastructure to provide conferences. For this enable the **Conference cannels** flag for each selected RFP on the OMP's **DECT base stations** -> **Devices** -> **General** tab.

Please note: Only RFP 35 / 36 / 37 / 43 / 44 / 45 / 48 devices support 3-way conferences.



Depending on the DECT and G.729 configuration, an RFP device enabled for conferencing provides between 3 and 24 conference channels. To compute one 3-way conference 3 conference channels are necessary.

In particular, the G.729 codec, with its high consumption of computing time, reduces the number of available conference channels according to the following table.

DECT enabled	Conferencing enabled	G.729 enabled	Conference channels	DECT voice channels
Yes	No	Yes/No	0	8
Yes	Yes	No	15	8
Yes	Yes	Yes	3	5
No	Yes	No	24	0
No	Yes	Yes	9	0

Please note: Activating the **Conference channels** option on an RFP with enabled DECT and in a system with enabled G.729 reduces the available DECT channels on that RFP from 8 to 5.

If the G.729 codec is not necessary on your iPBX platform, disable the G.729 codecs on the OMP's the **System**: **SIP** page / **RTP settings** tab to obtain the maximum number of conference channels.

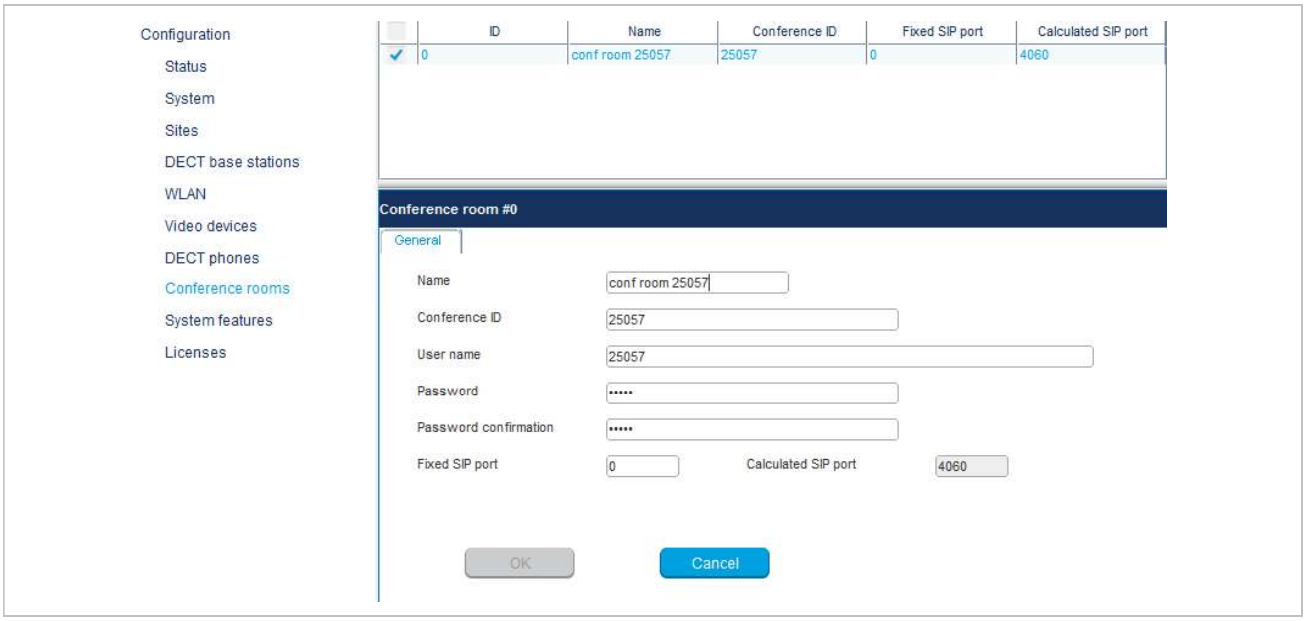
The total number of conference channels in the SIP-DECT system is presented the OMP's **Status** -> **Conference** tab. The **Total** parameter provides the total number of conference channels in the system and the **Available** parameter provides the current number of available conference channels.

8.21.3 CONFIGURE CONFERENCE ROOMS

When a three-way conference is initiated by a SIP-DECT user, the initiator and the connected parties will be transferred to the next free conference room using SIP signalling. These conference rooms must be configured on the OMP's **Conference rooms** page with their SIP user id and SIP password (see section 6.11).

Configure as many conference rooms as necessary and as conference channels are available (3 channels per conference).

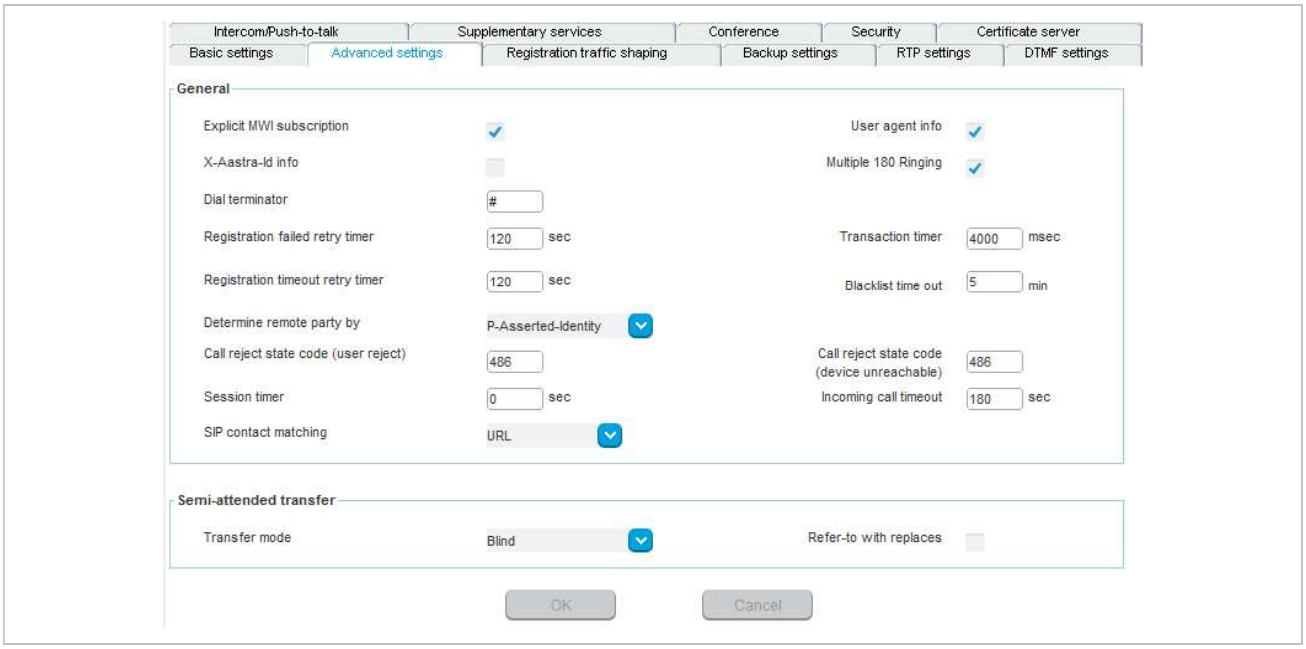
These conference rooms will be SIP registered on the configured SIP registrar and must be reachable via the configured SIP proxy for SIP signalling.



The following parameters can be configured for each conference room

- **Name**: SIP display name
- **Conference ID**: SIP user id
- **User Name**: SIP authentication name
- **Password**: SIP password
- **Fixed SIP port**: Port used explicitly for SIP signaling. If set to 0 (default), an automatically calculated port is used for this conference room. See section 2.17 for more information.
- **Calculated port**: Auto-calculated port used for SIP signaling (read-only). Only used if no value is specified for **Fixed SIP port**.

All configured conference rooms will be registered on the registrar / iPBX configured in OMM. If the **X-Aastra-Id Info** option is enabled on the OMP's **System**: **SIP** -> **Advanced settings** tab, a private X-Aastra-Id header is sent out which identifies that these are conference rooms.



The X-Aastra-Id header has the following format for all conference rooms:

```
X-Aastra-Id: type="29" model="01" version="1.0.0"
```

The header's attributes have the following properties:

type

- the type parameter contains the phone type
- the value for all SIP-DECT conference rooms is "29"
- type = DQUOTE (1*2HEXDIG) DQUOTE

model

- it's the model of the terminal
- the value for all SIP-DECT conference rooms is "01"
- model = DQUOTE (1*2HEXDIG) DQUOTE

version

- the version is intended for later releases
- the value for all SIP-DECT conference rooms is "1.0.0"
- version = DQUOTE (1*16token) DQUOTE

8.22 DOWNLOAD OVER AIR

The “Download Over Air” feature allows updating the DECT phone firmware without any user interaction or interruption of the telephony services over the existing DECT air interface. This feature is currently available for the Mitel 600 DECT Phones.

With SIP-DECT 6.0 and later, the SIP-DECT RFP software images (iprfp3G.dnld or iprfp4G.dnld) contains the Mitel 600 DECT phone software. If the RFP houses the OMM, the OMM uses this software to update the DECT phones. The RFP OMM no longer automatically attempts to load a DECT phone software image from a RFP software URL when provided via DHCP or local configuration.

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

8.22.1 HOW “DOWNLOAD OVER AIR” WORKS

If the “Download over Air” feature is activated (see section 5.4.1.8), the OMM acts as a download server that provides the firmware for downloads.

The DECT phone sends its firmware version within the DECT attachment procedure. If the firmware version does not match the version provided by the OMM, the DECT phone will be queued into the update-queue. Later on the queued DECT phones will be paged to establish a download connection. After the connection is established, the OMM sends its actual DECT phone firmware version and the DECT phone will request a DECT phone description file. After receiving the DECT phone description file, the DECT phone decides which files are missing or must be updated. If files are missing or must be updated the DECT phone initiates the download procedure.

The OMM takes care of the following download scenarios automatically:

- If a DECT phones becomes unreachable e.g. when the DECT phone is switched off, the OMM will update the DECT phone when the DECT phone becomes available again.
- The OMM will take care of the software download while the user is moving between base stations (roaming) and location areas.
- The OMM has the capability of resuming a download from the point where it was last interrupted (e.g., the user leaves the coverage area during download or the DECT phone runs out of battery power).
- The OMM updates new DECT phones subscribed to the system.
- While the DECT phone is barred (e.g. low battery or “Download over Air“ is disabled at the local menu), the download will be postponed.

The download happens without any user intervention. During the download, the telephony services, the roaming- and handover procedures are still available. The download stops automatically when e. g. the DECT phone leaves the coverage area or the RFP gets busy. The download resumes automatically when the stop cause is solved.

The Mitel 600 DECT phones have two partitions in the internal flash memory to hold 2 different software versions. During the download the new firmware is written to one partition and the DECT phone is running from the other partition.

After the download is successfully completed, the new firmware will be activated when the DECT phone is in the idle state.

The download of a single DECT phone with a firmware of 1 MB takes approximately 90 minutes. The number of DECT phones which can be downloaded depends on the available system resources.

The number of simultaneous downloads is limited per OMM (RFP: 30, PC: unlimited) and per RFP (6, decreased with each call).

The “Download over Air” service is delayed after a system startup for a while to allow the whole DECT system to become active. This may last several minutes.

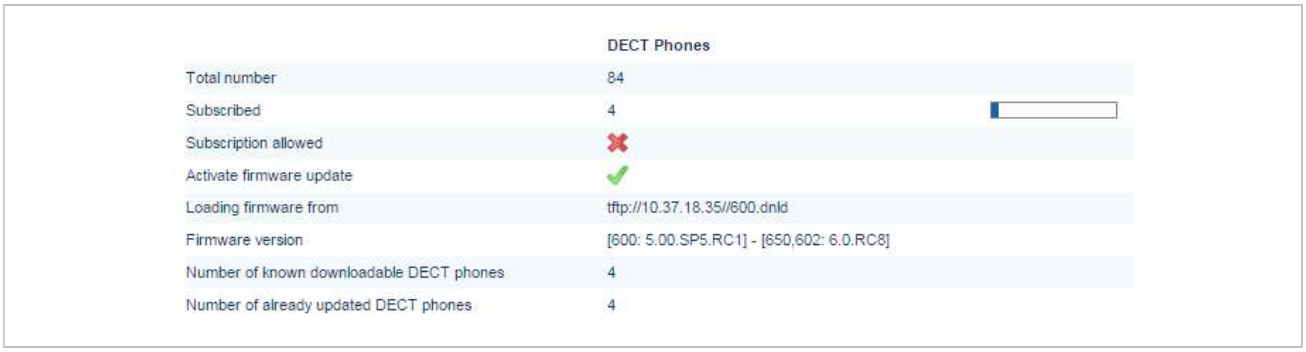
8.22.2 HOW TO CONFIGURE “DOWNLOAD OVER AIR”

This section describes configuration of the “Download Over Air” feature via the OM Web service. The feature can also be configured using the OM Management Portal (OMP).

The “Download over Air” feature can be activated or deactivated on the **System Settings** web page (see section 5.4.1.8).

In the OMP, you can enable the “Download over Air” feature in the **System** -> **Advanced settings** -> **PP firmware** tab (see section 6.5.2.3).

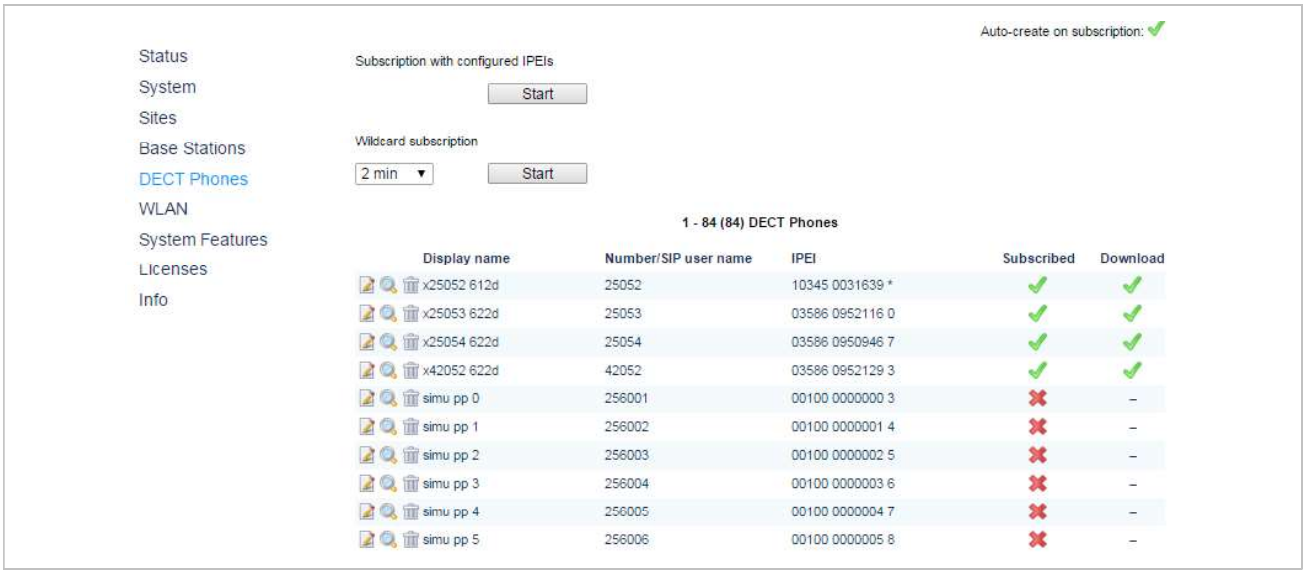
If the “Download over Air feature” is activated, the status of the **Activate firmware update** parameter is shown as enabled, service together with some statistics is displayed in the **DECT phones** section of the **Status** web page.



The DECT phone firmware container for DECT phone firmware update over the air includes packages for the Mitel 600 DECT phones. The available versions are also displayed on the **Status** web page.

Please note: The “Loading firmware from” on the OpenMobility Manager **Status** web page is only updated on restart of the OpenMobility Manager. Changing the location while the OpenMobility Manager is running has no effect.

The individual download status of each DECT phone is shown on the **DECT Phones** web page.



The details in the **Download** column have the following meaning:

Icon	Meaning
-	Impossible to download the firmware to that DECT phone (e.g. not a Mitel 600 DECT phone)
	The DECT phone is paged to establish a download connection. In case of a successful connection establishment the DECT phone calculates the number of bytes to download. This may take several seconds.
xx kbytes left	The download is ongoing and xx kbytes are left.
	The firmware of this DECT phone is up to date.
	The DECT phone is queued in the update-queue for updating (pending).
	Warning The download is barred because of one of the following reasons: – The DECT phone is busy (temporary status). – The battery power is lower than 50% and the DECT phone is not connected to the docking station or the USB interface. – This is not the master download system. A DECT phone can be enrolled on several OpenMobility systems. The first system to which the DECT phone will be enrolled is the “master system”. The DECT phone downloads only from the “master system”. A different “master system” can be chosen inside the local menu of the DECT phone. – The download is disabled in the local menu of the DECT phone. The specific reason is shown as a tooltip.
	Error The download failed because of one of the following reasons: – checksum error, – file system error, – error while writing firmware to flash, – version mismatch, – error while expanding firmware container. The specific reason is shown as a tooltip.

Icon	Meaning
	Info The download is not possible because: – the DECT phone is not reachable – the DECT phone is detached The specific reason is shown as a tooltip.

In the OMP, the “Download over Air” service status is displayed in the **Status** menu (see section 6.4).

8.23 CENTRAL DECT PHONE CONFIGURATION OVER AIR (COA)

Centralized DECT phone configuration over the air is supported for Mitel 602 DECT phones. Configurable parameters include:

- settings (loudness, contrast, etc)
- menu items (switch on or off, enable password protection)
- key assignments (including an override of manual key programming)
- variable lists

DECT phone configuration over air (CoA) is useful for deployment of special configuration to a single DECT phone or a large number of DECT phones. No local access to the DECT phone is required.

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

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

IMPORTANT : This feature requires 6.00 DECT phone software or later.

IMPORTANT : Centralized DECT phone configuration over the air is only available on the Download over Air (DoA) master system.

8.23.1 CONFIGURATION FILES

You can use three kinds of configuration files:

- Default DECT phone configuration profile

Default configuration file used for all suitable DECT phones. The configuration is loaded into the DECT phone when subscription is complete, even if a user has not logged in to the device.

- DECT phone configuration profiles

User-focused DECT phone configuration file used for a group of users. The configuration is loaded into the DECT phone when a user belonging to this group logs in to the device.

- DECT phone user individual configuration settings

Individual DECT phone configuration settings used for a single user. The configuration is loaded into the DECT phone when the user logs in to the device.

The system consolidates the DECT phone settings before loading the configuration settings for a logged-in user into the DECT phone. Settings from DECT phone profiles overwrite default configuration settings, and individual user configuration settings overwrite DECT phone profiles and default configuration settings. For a complete list of supported settings, see section 12.5.

Configuration can be completed by using OMP (file import and download configuration settings) and user configuration files (user_common.cfg and <user.cfg files), wherein a list of user friendly settings can be used for the DECT phone configuration.

> **Please note:** Deleting or overwriting configuration files on a DECT phone does not restore configuration to default or previous settings. Configuration elements that are not part of the new downloaded configuration file persist. To restore all settings, the administrator must initiate a power off/on at the DECT phone or use a default configuration file that contains all relevant settings.

To avoid interfering with the telephony or message service (especially with respect to alarm messages within the SIP-DECT system), only one configuration data download to the DECT phone is performed at a time. Therefore, changing the default profile settings or other profile settings may take some time in a large system, until all the related DECT phones are updated.

8.23.2 CONFIGURATION FILE DOWNLOAD TO DECT PHONES

Profiles are downloaded to the DECT phone via the messaging mechanism, in conjunction with the internal message type “CONF_OVER_AIR”. This occurs in parallel with general message transfer to the DECT phone, and the lowest priority is used to ensure that the download does not interfere with the delivery of urgent messages. The message mechanism is also used to confirm a successful profile download, through AXI events.

Profile downloads to DECT phones are limited system-wide to a maximum of one download at a time to ensure no interference with OMM system operation. You can view the download on the OMM console (console command `hcm`).The download state is also part of the system dump.

8.23.2.1 Download Triggers

The OMM maintains a profile download list for all DECT phones that have configuration data to be set. These DECT phones are stored with the checksum of configuration data to be set. A DECT phone is included in this list when:

- the OMM system starts up and the associated DECT phone has configuration data to be set
- the associated DECT phone’s configuration data changes (this is communicated via AXI), such as:
  - change in the default configuration profile
  - change in the configuration profile for the user of the associated DECT phone
  - change in the individual user configuration profile for the user using the associated DECT phone
  - change in the configuration profile assigned to the user using the associated DECT phone

Profile downloads to the DECT phones (as maintained in the profile download list) are scheduled at regular intervals. A new download to DECT phones in the profile download list is scheduled when:

- a configuration change occurs on the DECT phone (via AXI notification)

- a location registration is received, and the checksum of the configuration data stored in the profile download list is different from the checksum sent in the location registration
- a download to a DECT phone completes

8.23.3 COA CONFIGURATION USING OMP

OMP configuration of DECT phones is restricted. You can do the following through OMP:

- List the current user and device state via the **DECT Phones** -> **Overview** menu and **DECT Phones** -> **Devices** -> **Configuration data** tab (in Monitoring mode)
- Import the default profile and one to 20 individual profiles via the **System features** -> **COA profiles** menu (see section 6.12.9)
- Assign one of 20 profiles to an internal user via the **DECT Phones** -> **Users** -> **Configuration data** tab (see section 6.10.4.10)

The syntax of the profiles that can be imported by the OMP is the same as that specified for the user_common.cfg and <user>.cfg files.

Please note: CoA configuration via OMM Web service is not supported. You can only list the current user and DECT phone state in the “User and DECT phone configuration and status data summary”.

8.23.4 CONFIGURATION USING USR_COMMON.CFG/<USER>/CFG FILES

The user_common.cfg and <user>.cfg configuration files are used for DECT phone configuration. The following configuration attributes in the user_common.cfg file control central DECT phone configuration:

- Default profile settings

```
OM_Profile.0.Default.<key>=<values>
 …
OM_Profile.0.Default.<key>=<values>
```

Where “Default” is the reserved name for the default profile, and <key> is one of the configuration settings with its <values> to be set.

Example:

```
OM_Profile.0.Default.UD_DispLang="en"
OM_Profile.0.Default.UD_DispFont="large"
OM_Profile.0.Default.UD_DispColor="black"
```

- one of up to 20 profile settings

```
OM_Profile.<no>.<name.<key>=<values>
…
OM_Profile.<no>.<name>.<key>=<values>
```

Where <no> is the number of the profile, <name> is the name of the profile to be configured, and <key> is one of the configuration settings with its <values> to be set.

Example:

```
OM_Profile.5.Doctor.UD_DispLang="en"
OM_Profile.5. Doctor.UD_DispFont="large"
OM_Profile.5. Doctor .UD_DispColor="black"
```

Please note: To assign a profile to a user, you can use the UD_PpProfileId= <profileNo> setting in <user>.cfg files. When <profileNo> is 0, no profile or (depending on configuration) the default profile is used. The default profile is defined in user_common.cfg.

Please note: A complete removal of a profile from user_common.cfg does not remove the profile in the OMM database. It must be explicitly deleted in the OMM database.

For individual user DECT phone configuration settings, the following configuration attributes are available in the <user>.cfg file:

- User configuration settings

```
<key>=<values>
…
<key>=<values>
```

Where <key> is one of the configuration settings with its <values> to be set.

Example:

```
UD_DispLang=”en”
UD_DispFont=”large”
UD_DispColor=”black”
```

8.23.4.1 CoA Example

`UD_ConfigurationName = "omm-test"`	Configuration file is named “omm-test”
`UD_DispLang="en"`	Language is set to English
`UD_DispFont="small"`	Display font is set to small
`UD_DispColor="black"`	Display color scheme is set to black
`UD_RingerMelodyIntern="ringing_1"`	Internal call melody is set to melody “ringing_1”
`UD_RingerMelodyExtern="ringing_2"`	Internal call melody is set to melody “ringing_2”
`UD_RingerVolumeIntern="increasing"`	Internal call ringer volume is set to increasing
`UD_RingerVolumeExtern="increasing"`	External call ringer volume is set to increasing

See section 10.4 for a full list of supported CoA configuration parameters.

8.23.5 VARIABLE LISTS

The Mitel 602 DECT phone 6.1 firmware introduces variable lists. A variable list includes a number of items, each of which corresponds to an action to be performed on the DECT phone.

A list item consists of an index identifier (1..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" "" "" ""
```

8.23.5.1 Icon coding

The following table lists the UTF8-codes for Mitel 602 DECT phone icons.

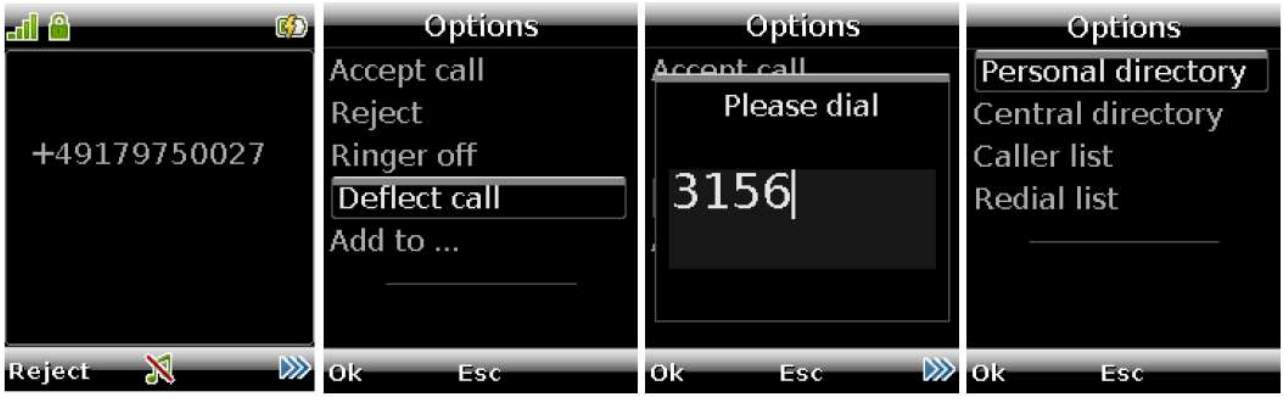
ICON	UTF8-Code	Description
	\xEE8083	Arrow Up
	\xEE8084	Arrow Down
	\xEE8085	Arrow Left
	\xEE8086	Arrow Right
	\xEE8088	Fox Key
	\xEE80B0	Locked
	\xEE80BC	Search
	\xEE80BE	Info
	\xEE81A5	Attention
	\xEE80BA	Tip
	\xEE808A	Telbook Private number
	\xEE808B	Telbook Mobile number
	\xEE808C	Telbook Business number
	\xEE818C	VIP number
	\xEE808D	Telbook Fax number
	\xEE808E	Telbook Email address
	\xEE808F	Telbook Name
	\xEE809B	Hook off / Predial
	\xEE809C	Hook on / Release
	\xEE81B0	Register recall
	\xEE8092	DTMF
	\xEE8182	3-party
	\xEE80A0	List Incoming call list
	\xEE80A1	List Outgoing call list
	\xEE8196	List Private directory /
	\xEE8199	List Central directory
	\xEE818C	List VIP
	\xEE8181	List Filter / Call Filtered
	\xEE80A1	Call outgoing
	\xEE8099	Call Waiting
	\xEE80A7	Call Rejected
	\xEE81AD	Call SOS

ICON	UTF8-Code	Description
	\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

8.23.5.2 Call Deflection for incoming call in ringing state

In this, an incoming call can be deflected to another extension. In ringing state, “Deflect call” is offered in the option menu.

This option allows to enter the target extension to which the call gets deflected. The target can also be chosen from one of the directories or call logs.



The DECT phone returns to the idle state after confirming the target extension. Depending on the actual call log management of the call server platform, the deflected call is shown as an answered or missed call.

8.23.5.3 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>
<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>

8.24 EXTENDED DECT PHONE INTERFACE

With SIP-DECT 6.0 and later, the Mitel 600 DECT phones include an **Administration** menu that offers administrative functions to the user such as login, logout, and configuration and status summary display. The menu is available as an option under the **System menu** which can be accessed via the main menu of the DECT phone, or directly by a long press of the right soft key “**>>>**”.

> **Please note:** The **Administration** menu is only available on Mitel 600 DECT phones, version 4.0 or higher.

The following table summarizes the options under the **Administration** menu. The menus allow basic OMM configuration and require a login (the same account and password as used for administrative access via OMP or Web service).

	Menu option	Description	OMM login
1.	**Login**	User can log in to the DECT phone (free DECT phone only)	
2.	**Logout**	User can log out of the DECT phone (free DECT phone only)	
3.	**PP state**	Display user/device configuratoin and status data summary (see section 5.7.6 for details)	
4.	**Sync user data**	Refresh SIP registration and synchronize user data, if they are stored externally	
5.	**Sync system data**	Reload configuration and resource files	Yes

6.	**System credentials**	Set authentication for provisioning servers (see section 8.8.6.1)	Conditional
7.	**Status**	Display basic OMM network settings (e.g., DHCP, IP addresses)	
8.	**System**	Set basic OMM system data	Yes
9.	**SIP users/devices**	Perform basic configuration of users and DECT phones	Yes
10.	**Version**	Display current OMM software version	

The options available depend on the DECT phone state and the OMM platform (i.e., RFP OMM or Linux Server). The following table summarizes the options under the **Administration** menu according to device state and OMM platform.

	Menu option	Fixed device	Logged out	Logged in	RFP OMM	Linux Server OMM
1.	**Login**		√		√	√
2.	**Logout**			√	√	√
3.	**PP state**	√		√	√	√
4.	**Sync user data**	√		√	√	√
5.	**Sync system data**	√	√	√	√	√
6.	**System credentials**	√	√	√	√	√
7.	**Status**	√	√	√	√	
8.	**System**	√	√	√	√	√
9.	**SIP users/devices**	√	√	√	√	√
10.	**Version**	√	√	√	√	√

The following table summarizes the submenus available according to the OMM platform.

	Submenu	SIP-DECT	RFP OMM	Linux Server OMM
1.	**System name**	√	√	√
2.	**Date and Time**	√	√	
3.	**SIP**	√	√	√
4.	**User administration**	√	√	√
5.	**Restart**	√	√	√

8.25 OMM/DECT PHONE LOCK WITH BRANDING ID

With SIP-DECT 6.0 and later, customers can use a specific branding key to lock the OMM. The key must be branded to all DECT phones before they can be subscribed.

Note: This feature is only available by special request. Please contact your Mitel representative for more information.

You generate the branding key using the `DECTSuiteBrandingInstallation.exe` tool (provided by Mitel on special request). When you have the generated keys, you set the branding key in the OMP, via the **System** -> **Advanced Settings** -> **Special branding** tab (see section 6.5.2.7).

The branding key can be only removed from the OMM system by using a special key, also generated with the DECT-Suite PC Tool and entered in the OMP Special branding tab. You must remove the branding key before changing to a different brand.

8.25.1 SUBSCRIBING THE DECT PHONE

The user who subscribes the DECT phone must explicitly invoke the transfer of the branding key (done in the AC-Editor).

Add “R*” (or “R<additional_id>” in one case) as a suffix to the typed AC code (or just R*, if there is no AC code).

- Type R* for normal subscription for fixed devices.
- Type R* for auto-create by subscription.
- Type R* for wildcard subscription without DECT phone data record selection.
- Type R<additional_id> for wildcard subscription with record selection by the additional id.

8.26 DEVICE PLACEMENT

The OM Locating application uses small graphic maps for visualization of DECT base station placement. From SIP-DECT release 3.1 on, these graphics can be created with the OMP in **Planning Mode**.

8.26.1 “PLACEMENT” VIEW

By using the mouse with drag and drop, you can move RFP icons to their correct mounting position on the loaded background image. Note that you must provide background images first (see also /27/).

A DECT base station is drawn as green circle with its ID number inside.

Background images can be loaded into the application on the **Image Management** panel (see section 8.26.3).

The assignment of devices to the currently active image must be done on the **DECT base stations** page.

8.26.1.1 Functionality of the “Placement” View

- Left mouse click selects/deselects the DECT base station the mouse is pointing to. A selected device is shown with thicker border.
- Drag and drop functionality: a device can be moved while the left mouse button is pressed and hold.

- If left mouse button is hold and no device is selected, the complete view content gets moved.
- By turning the mouse wheel the view gets scaled up or down depending from the direction of turning.
- By pressing the right mouse button a pop-up menu is displayed:
  000-oamp-planning-mode-context-menu.tif
  - **Move selected RFPs**: All selected devices (drawn with a thick border) will be moved to the current position of the mouse pointer. Distances between the devices are not changed as long as all devices can be drawn inside the background image. Moving devices to the area outside the upper or left border of the image is not possible.
  - **Reset selection**: The selection is canceled for all currently selected devices.
  - **Remove selected device(s)**: Selected devices are removed from the current image after confirmation in a dialog box. Those devices can be assigned to an image again via the **DECT base stations** menu (see also section 8.26.2).
    If no devices are selected but the mouse is pointing to a device, that device is removed from the image without further inquiry.
  - **Reset view**: The view is redrawn in its original appearance. Any translation and scaling applied to the view is cancelled.

8.26.1.2 Activation of the “Placement View”

The **Placement view** can be activated by:

- Selecting the **Placement view** menu entry. The currently loaded image with its assigned devices is displayed. If no image is currently loaded, the view is empty.
- Double-clicking on a table row in the **DECT base stations** view. This activates the placement view with the image the clicked device is assigned to.
- Selecting the **Assign to active image** task in the **DECT base stations** view. The selected devices are assigned from the table to the current image.
  If a selected device was already assigned to another image, the assignment is changed upon confirmation in a dialog window.
- Selecting an entry in the **Image management** view (double-click or click on **Show image** task).

8.26.2 “DECT BASE STATIONS” VIEW

The view shows a table based list of RFP.

When you select table rows and click **Assign to active image**, the selected devices are assigned to the currently active image. Devices already assigned are tagged with a green sign in the table column **Positioned**.

If a selected device was already assigned to another image, the assignment will be changed when confirmed through a confirmation dialog.

8.26.3 “IMAGE MANAGEMENT” VIEW

With the **Image management** view all background images assigned to the SIP-DECT system can be managed. Also, the generation of the graphic maps used by the OM Locating application can be started by this view.

If the user activates this view and a background image was loaded, the OMP automatically creates a project file the current SIP-DECT system on the PC. This file contains references to the background image files and the device assignment and placement coordinates. It automatically gets reloaded to the application if the OMP user enters the **Device Placement** menu again during a connection to the same SIP-DECT system.

The images and placement coordinates are stored only on the local PC and not together with the SIP-DECT system configuration (due to storage size limitations). Therefore it is recommended to export the project and save the project data at a secure place after finishing the placement of devices for a SIP-DECT system.

8.26.3.1 “Show image” Task

After selecting an image entry from the table with a left mouse click and then selecting the **Show image** task, the image will be displayed with its assigned devices in the **Placement view**.

A left mouse double click on a table entry also opens the **Placement view**.

8.26.3.2 “Add image” Task

With the **Add image** task, the user calls up a File Open dialog which allows the addition of one or more background images stored on the PC to the system.

The OMP supports *.jpg and *.png image files. A maximum of 800 images can be managed by the OMP.

The maximum size per image is limited to 3000 pixel in both height and width.

8.26.3.3 “Remove image” Task

The selected image table entries will be removed from the current project after an inquiry dialog. All devices which were already assigned to one of the removed images will be reset to unassigned state.

8.26.3.4 “Generate” Task

By choosing this task the user can start the generation of the graphics data needed by the OM Locating application. The OMP will only create graphics data for selected image table.

In a file save dialog the user can select a storage directory for the generated graphics data. A progress dialog informs about the actual status of the generation process. If the process is canceled by the user, the OMP will finish generation of graphics data for the actual background image before stopping the process.

8.26.3.5 “Import project” Task

With the **Import project** task the user can load a previously exported project. Images and device placements done before importing a project will be substituted by the data contained in the project.

The system name and the PARK are not checked during this operation. It is possible to import a project created for another system or after the system name or PARK was changed.

Devices are managed by their IDs. If a device ID from imported data cannot be matched with a device ID from the system the OMP is currently connected to, the placement data for such a device will not be imported.

The image files will not be copied. The actual project will save references to the storage place of the images.

8.26.3.6 “Export project” Task

With the **Export project** task, the user opens a File Save dialog where the user can select a directory for the exported data, or create a new one.

The OMP exports the project file and copies all background image files to the chosen destination.

A project exported with this task can be imported again via the **Import project** task.

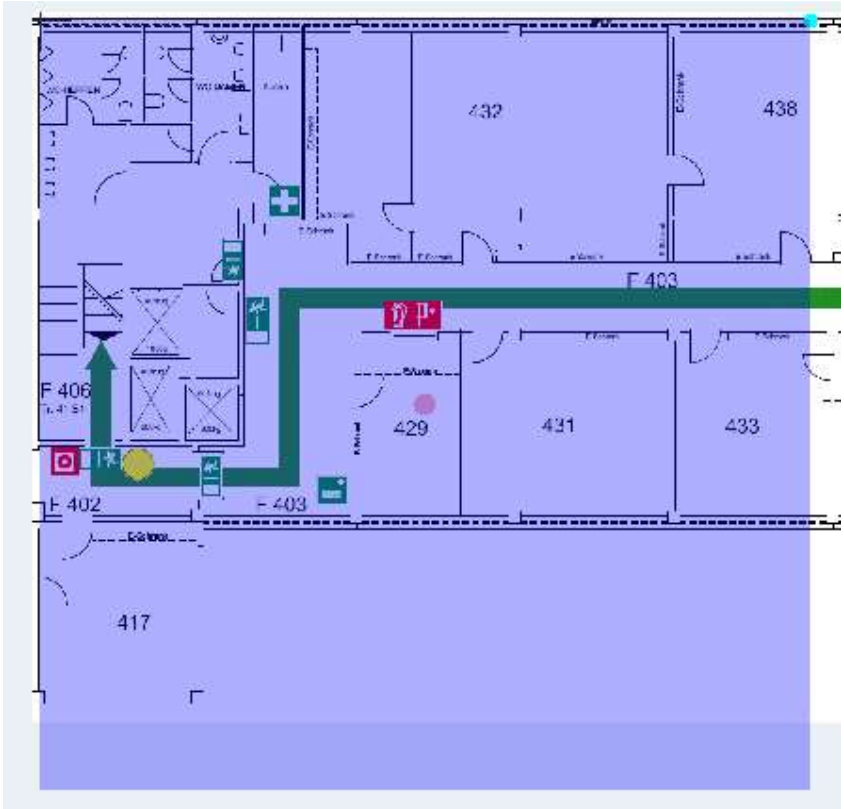
8.26.3.7 “Adjust overview size” Task

The OM Locating application needs two graphic maps for each device:

- One detail map image showing the position of an RFP in same scale as the background image on which the device was placed.
- An overview map showing a bigger area of the background image down scaled and the position of the RFP.

There is no special requirement to the scale of the used background images. The selection of the overview scale may differ depending from building or area proportions.

With the **Adjust overview zoom** task the user can adjust the down scale zoom factor for the overview map images (2) individually for the currently selected background image.



The content of an area generated as overview map is shown by the transparent overlay square. Changing the size of this area can be done by grabbing the light blue point at the right upper edge and moving the edge to (or away from) the center of the area.

By grabbing the red point in the middle of the overlay square it is possible to move the overlay square around.

For generation of the overview map images the position of overlay square does not matter. Only the size is important to calculate the scale ratio for down scaling.

8.26.3.8 "Set overview size" Task

Instead of adjusting the scale factor for down scaling on generation of overview maps with the method described in section 8.26.3.7 it is possible to set a scale factor for the selected images.

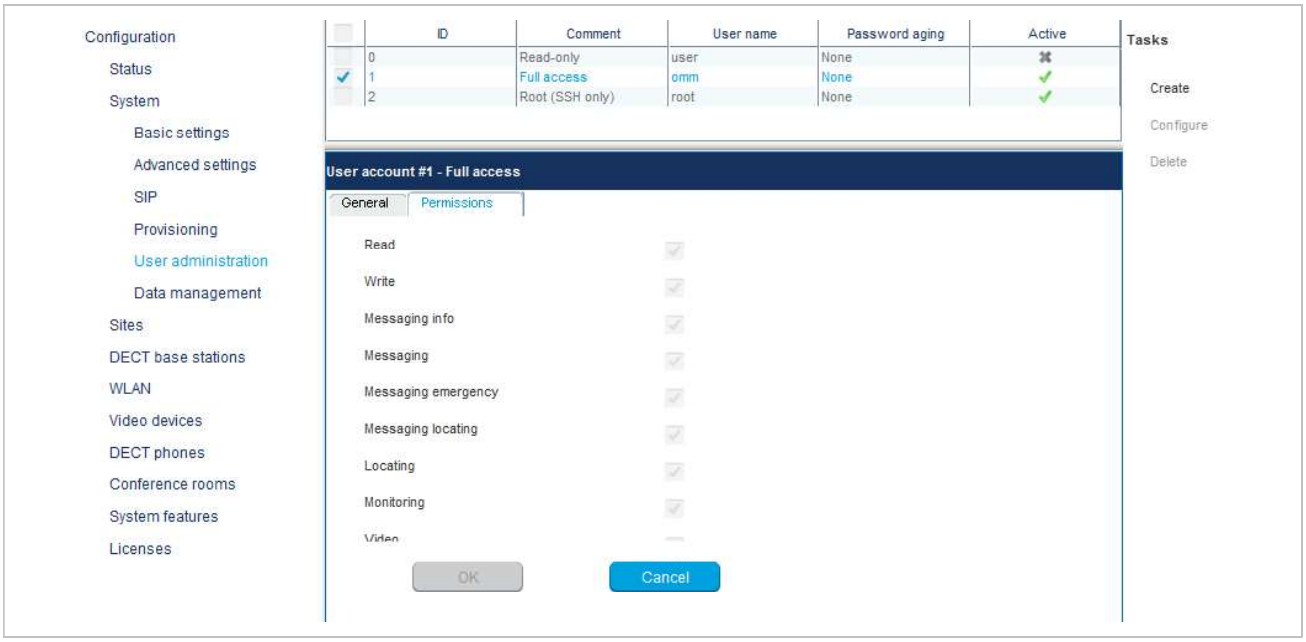
The value of the scale factor must be chosen with the slider **Overview size** in the task panel prior to assign it to one, several or all images with the **Set overview size** task.

8.27 MONITORING WITH USB VIDEO DEVICES

To use an USB video device in interaction with the OM Locating application, a video user account must to be configured. In addition the configuration and activation of a video device ("USB Web Cam") itself is needed.

8.27.1 CONFIGURATION OF A VIDEO USER ACCOUNT

An active user account with at least read and video permissions must to be configured, to use it inside the OM Locating application.



Please note: If you have already configured the OMM's "Full access" account within the OM Locating application to access OMM service, you must change this account to the video-enabled account created in this step.

8.27.2 CONFIGURATION OF USB VIDEO DEVICES

You configure video devices on the OMP's **Video devices** page (see section 6.9). The **Video devices** page contains a list of known video devices and you can access the configuration window for the video devices by double-clicking on an entry. Use the left side of the panel to enter a description of the camera and its position. On the right side of the window, you can set the parameters for **Resolution** and **Frame rate**.

The selected values for resolution and frame rate must fit the parameter specifications of the camera device. Changes to these settings are not possible on cameras in a "started" state (i.e., viewed in the OM Location application).

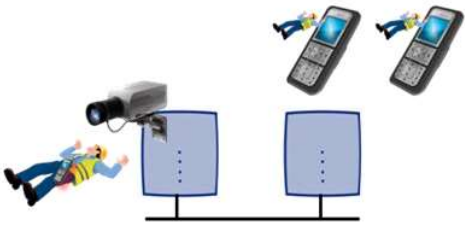
By setting the **Active** option, the video device is permitted to send images.

8.27.3 MONITORING WITH USB VIDEO DEVICES

Using the OMP monitoring mode for a video device opens a window with two tabs, the **General** tab and the **Status** tab. On the **General** tab the actual configuration of the video device will be shown. On the **Status** tab the actual status of the camera device will be shown. The tag is an internal identifier of a video device, the **RFP ID** is the identifier of the RFP the video device is plugged in, **USB path** is an identification of the plug-in position and **State** is the actual state of the video device.

8.28 TERMINAL VIDEO

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



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

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

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

8.28.1 TECHNICAL DETAILS

Terminal video resolution and framerate are independent from the configured camera resolution and framerate.

The resolution of the terminal video stream is automatically downscaled to 176 * 144 pixels (QCIF) with a frame rate of approximately 2 frames per second.

The resulting overall delay is below 2 seconds.

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

8.28.2 OMP CONFIGURATION STEPS

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

- Enable all sites, which have the technical capability (only 3rd or 4th generation RFPs are referred to it), via OMP for terminal video.
- Enable via OMP (**DECT Phones** -> **Users** -> **Additional services**) by setting the "Video stream permission" for those users who are allowed to use this feature.

Please note: It is strongly recommended that you set the DECT base station attributes "building", "floor" and "room", if you configure a large system with a large number of cameras. This makes selection of cameras on the DECT phone menu easier.

8.28.3 CAMERA SELECTION VIA DECT PHONE MENU

The **Cameras** menu is available in the Mitel 602 DECT phone **System menu**, if

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

The user navigates within the camera menu using the **OK** (and **ESC**) keys. When the desired camera is selected in the list, the user can press the "hook off" button to establish a video stream.

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

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

Please note: During an established video link, audio calls or any system service activities are not possible.

Any kind of auto callback (initiated by a message by a message or pushed by xml notification to direct dial) is not supported.

8.29 USER MONITORING

To check the availability of a user in terms of the possibility to receive calls or messages, the OMM monitors the status of the user's DECT device.

8.29.1 OVERVIEW

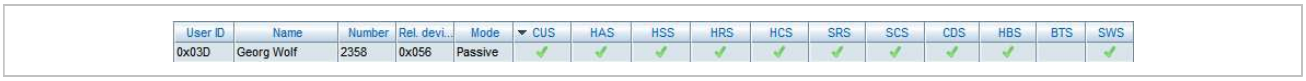
With the “user monitoring” feature the following fixed set of status information is monitored:

Is a DECT phone assigned to the user?	Handset assignment status (HAS)
Is the DECT phone subscribed to the DECT system?	Handset subscription status (HSS)
Is the DECT phone currently registered /signed in?	Handset registration status (HRS)
Are there DECT phone activities within a specific timeframe?	Handset activity status (HCS)
Is the user registered at the SIP registrar?	SIP user registration status (SRS)
Is the DECT phone not in silent charging mode (silent charging option active and in the charger cradle)?	Silent charging status (SCS)
Is the feature “immediate call diversion” inactive?	Call diversion status (CDS)
Is the battery charge higher than the configured threshold?	Handset battery state (HBS)
Does the DECT phone have the minimum required software version?	Software Status (SWS)

If all questions can be answered with “Yes” then the user status is set to “Available”. This set of status information is monitored if user monitoring is enabled for a user.

The status of all monitored users is displayed in the **DECT Phones** -> **User monitoring** menu (see also section 8.29.7.3). The status information can have one of the following values:

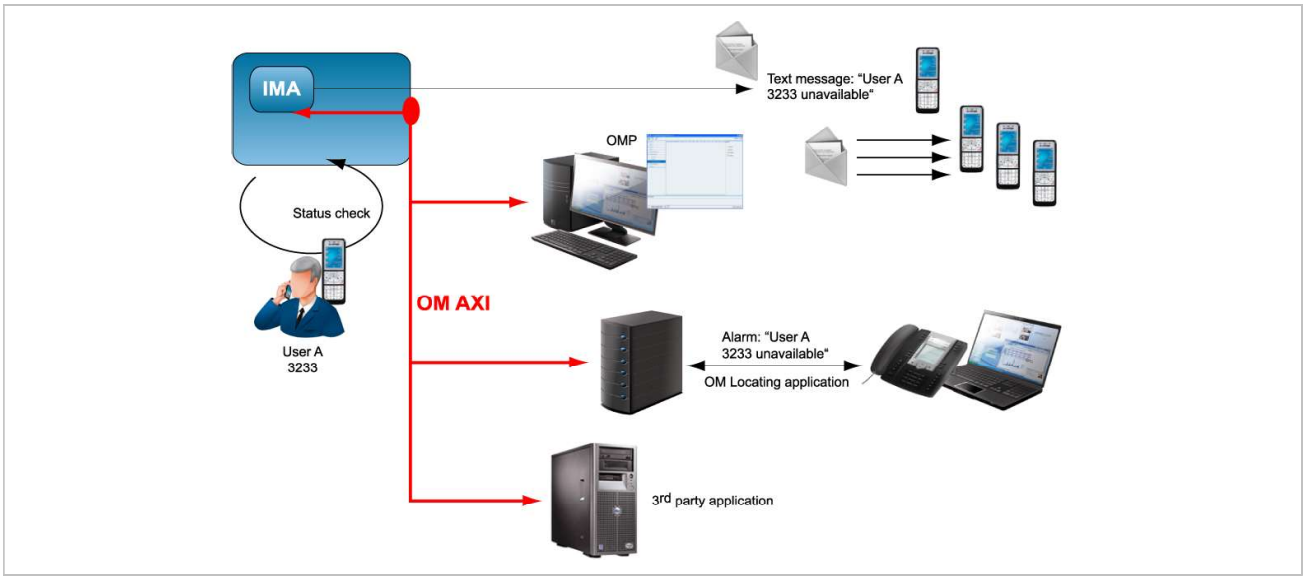
The sum of all specific states is presented by the “Combined User Status”.



If one of the states is set to unavailable, the resulting Combined User Status is set to unavailable as well.

Because of dependencies between the states, some states cannot be determined if a higher level state is not fulfilled. For example, if the user has no DECT phone assigned, the DECT phone registration status cannot be determined. If a status cannot be determined, the status value is set to “Unknown” (empty in OMP).

The status information is available via OM AXI and OMP.



IMPORTANT : To address customer specific requirements, external applications (e.g. 3rd party software) can provide an addapted functionality of the user monitoring or even more just by using OM AXI. This can be completed by the use of the XML terminal interface.

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

The specific alarm trigger "LOC-ERR-USERSTATE" is defined for locating. This alarm trigger is displayed in the OM Locating application with the icon.

IMPORTANT : The OM Locating application does not list users who are not locatable, e.g. locating not enabled for the users or because they have no DECT phone assigned. Therefore, the OM Locating application can not handle the LOC-ERR-USERSTATE with the escalation of the DECT phones assignment state (HAS).

8.29.2 STATUS ATTRIBUTES AND VALIDATION MECHANISMS

The combined user status (CUS) is the sum of the specific status information.

The CUS is calculated based on the flowing rules:

- Specific states which are set to "Unknown" are ignored.

- CUS is set to “Available” if none of the specific states is set to “Warning”, “Unavailable” or “Escalated”.
- CUS is set to “Warning” if at least one of the specific states is set to “Warning” and none of the other states is set to “Unavailable” or “Escalated”.
- CUS is set to “Unavailable” if at least one of the specific states is set to “Unavailable” and none of the other states is set to “Escalated”.
- CUS is set to “Escalated” if at least one of the specific states is set to “Escalated”.

The status “Unavailable” is changed to “Escalated” after the escalation timeout has elapsed and an alarm trigger has been generated.

8.29.2.1 Handset Assignment Status (HAS)

A DECT phone must be assigned to the user otherwise the status is “Unavailable”.

Fixed user device relation

A DECT phone can be assigned permanently to a user (fixed user device relation). Then the status is always “available”.

Dynamic user device relation

A DECT phone can be dynamically assigned to a user (dynamic user device relation) and login and logout on a DECT phone is used.

If the user is logged out (unbound), the status is “Unavailable”. If the user is logged in (dynamic), the status is “available”. Login and logout also change the SIP registration.

Precondition: The user must exist in the OMM database.

8.29.2.2 Handset Subscription Status (HSS)

The DECT phone must be subscribed otherwise the status is “Unavailable”.

Precondition: A DECT phone must be assigned to the user.

8.29.2.3 Handset Registration Status (HRS)

The DECT phone must be attached / signed in (successful location registration) otherwise the status is “Unavailable”

The DECT phone may sent a detach message if it is switched off.

Precondition: A DECT phone must be assigned to the user (fixed, logged in) and the DECT phone is subscribed.

8.29.2.4 Handset Activity Status (HCS)

A communication over the air must occur regularly otherwise the status is “Unavailable”.

Passive monitoring

With every activity between DECT phone and the DECT system (e.g. call setup) the activity information will be updated (last activity, current activity status). This indicates when the DECT phone was the last time able to communicate with the DECT system i.e. within the area of coverage, sufficient battery level,

etc. There must be an activity within the timeframe defined by the Activity timeout 1 (min. 30 minutes, max. 1440 minutes).

Any activity between the DECT phone and the systems sets the status to “available”.

Active monitoring

Each DECT phone, that shall be monitored actively, will refresh its registration automatically within the “Activity timeout 2” (min. 5 minutes, max. 60 minutes). Each activity sets the status to “available”.

Active and passive monitoring

If the DECT phone was not active for the period of time defined by the activity timeout, the OMM automatically initiates an activity between the DECT phone and the DECT system to check the DECT connectivity. If this fails, the OMM sets the status to “Unavailable” but tries to connect to the DECT phone two times more within the next 2 minutes.

The OMM then continues to check the DECT connectivity base on the configured time frame. If the status is already “Unavailable”, the OMM does not verify the status by two additional tests within 2 minutes. If a check was successful, the status is set to “available”.

If a DECT phone could not be reached (e.g. during call setup or messaging delivery), the OMM tries to connect to the DECT phone two times more within the next 2 minutes before the status is set to “Unavailable”.

Precondition: A DECT phone must be assigned to the user (fixed, logged in). The DECT phone is subscribed and attached (at least once).

8.29.2.5 SIP User Registration Status (SRS)

The user must be successfully registered at the configured SIP registrar otherwise the status is “Unavailable”.

A SIP registration is initiated automatically by the OMM during start-up if the user’s DECT phone was attached to the DECT system before restart/failover.

The SIP registration will not initiated automatically by the OMM during start-up if

- the user has no assigned DECT phone (fixed user device relation, login),
- the DECT phone is not subscribed or
- the DECT phone was detached (e.g. switched off) before restart/failover.

A user will be deregistered if

- the DECT phone subscription is deleted/terminated,
- the user logs off from a DECT phone or
- the DECT phone is detached (e.g. switch off).

Precondition: A DECT phone must be assigned to the user (fixed, logged in). The DECT phone is subscribed and attached (at least once).

8.29.2.6 Silent Charging Status (SCS)

If silent charging is enabled and the DECT phone is put into the charger, the DECT phone is in silent charging mode and does not indicate incoming calls with an audible signal. The DECT phone must not be in silent charging mode otherwise the status is “Unavailable”.

Precondition: A DECT phone must be assigned to the user (fixed, logged in). The DECT phone is subscribed and attached/signed in to the DECT system.

8.29.2.7 Call Diversion Status (CDS)

The user has no immediate call diversion (unconditional call forwarding) configured otherwise the status is “Unavailable”.

If the user has configured a call diversion for “No answer” / “Busy no answer” with a forward time ‘0’, this will be handled by user monitoring like unconditional call forwarding.

Precondition: The user must exist in the OMM database. The SIP supplementary service “Call forwarding / Diversion” is enabled in the OMM (see pages 76 and 142).

8.29.2.8 Handset Battery Status (HBS)

The battery level of the DECT phone must be greater than the configured threshold value; otherwise the status is set to “Warning”.

Precondition: A DECT phone must be assigned to the user (fixed, logged in). The DECT phone is subscribed and attached. Delivery of battery level is supported. [1]

8.29.2.9 Software Status (SWS)

The DECT phone software must provide the minimum of required features which could be controlled by the current OMM version. Therefore the appropriate minimum DECT phone software version is hard coded in the OMM and validated by user monitoring. The status will be set to “Warning” if the DECT phone software version is less than the hard coded value of the OMM.

Delivery of the software version is supported only by Mitel 600 devices.

Precondition: A DECT phone must be assigned to the user (fixed, logged in). The DECT phone is subscribed and attached. [2]

8.29.3 ESCALATION

If the OMM detects the unavailability of a user (marked as “unavailable”), this will be escalated only once by submitting a warning alarm trigger via OM AXI.

If the OMM detects finally the unavailability of a user (marked as “unavailable/escalated”), this will be escalated only once by submitting an alarm trigger via OM AXI.

The user must become available again before the unavailability of a user will be escalated the next time.

8.29.4 ALARM TRIGGERS

- The “UMON-WARNING-USERSTATE” alarm trigger is used to escalate the detection of the unavailability.
- The alarm triggers “UMON-ERROR-USERSTATE” and “LOC-ERROR-USERSTATE” are used to escalate the final detection of the unavailability.

[1] The Mitel 600 DECT phone family provides battery status information if the DECT phones are updated to the current software version.

[2] The Mitel 600 DECT phone family provides software version information if the DECT phones are updated to the current software version.

- The “UMON-OK-USERSTATE” alarm trigger is sent by the OMM if a user becomes available again.

These are static, predefined alarm triggers like “SOS” and “MANDOWN” which do not have a telephone number to call.

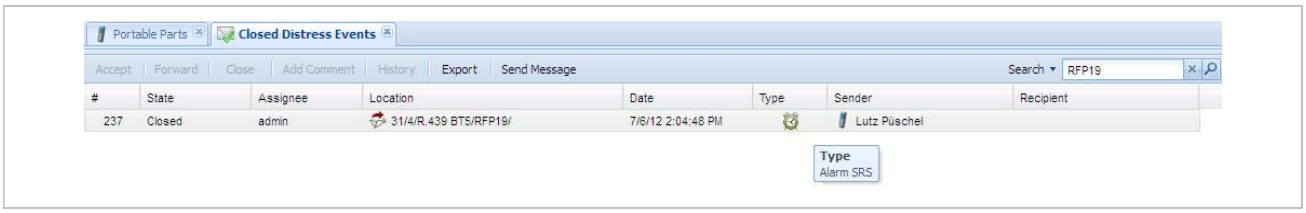
The alarm triggers “UMON-WARN-USERSTATE”, “UMON-ERR-USERSTATE” and “LOCERR-USERSTATE” provide information about the cause why the user became unavailable (one or more of status attribute IDs: HAS, HSS, HRS, HCS, SRS, SCS, CDS, …).

8.29.5 OM LOCATING APPLICATION

To be visible in the OM Locating application, the monitored user must be locatable. Tracking can be enabled.

The alarm trigger “LOC-ERR-USERSTATE” is handled like SOS (), ManDown () but no voice call will be established.

The alarm trigger “LOC-ERR-USERSTATE” will be displayed as a Customer specific event ().



8.29.6 LICENSING AND SYSTEM CAPACITIES

The “User monitoring” feature does not require a specific license.

The number of monitored users is limited, as follows:

RFP OMM

- Passive monitored users: 30
- Active monitored users: 20

PC OMM

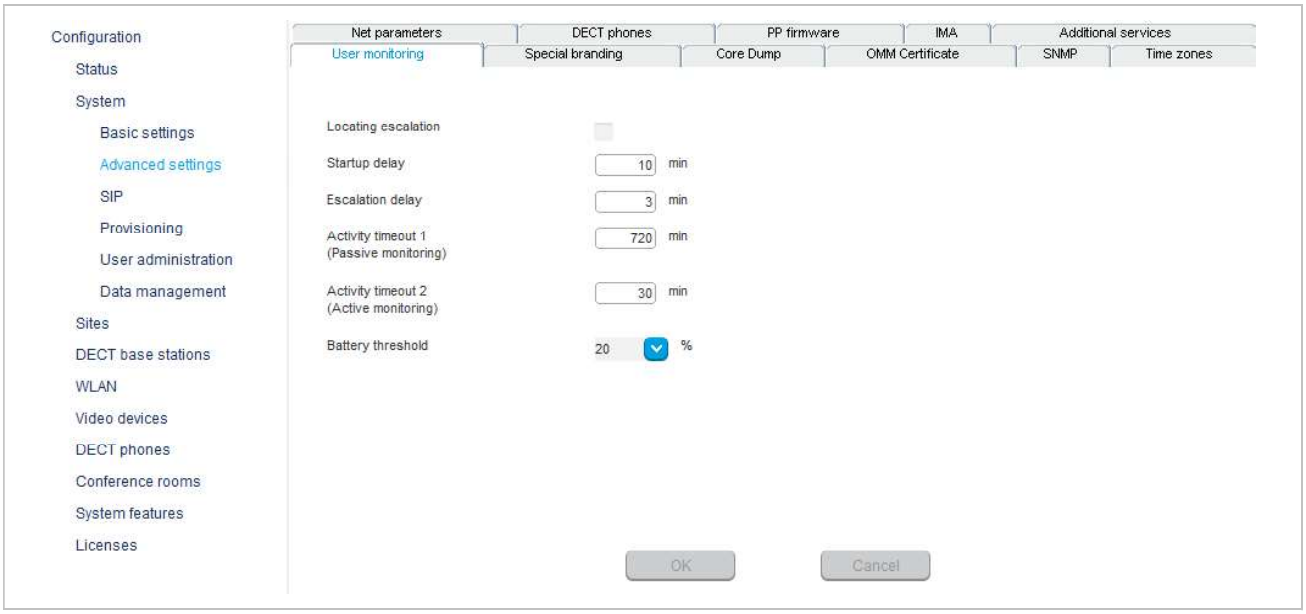
- Passive monitored users: 300
- Active monitored users: 200

An OMM system health state will be set if the number of monitored users exceeds the system capabilities. In this case also an associated health state alarm trigger will be generated.

8.29.7 CONFIGURATION

User monitoring can be administered via the OMP.

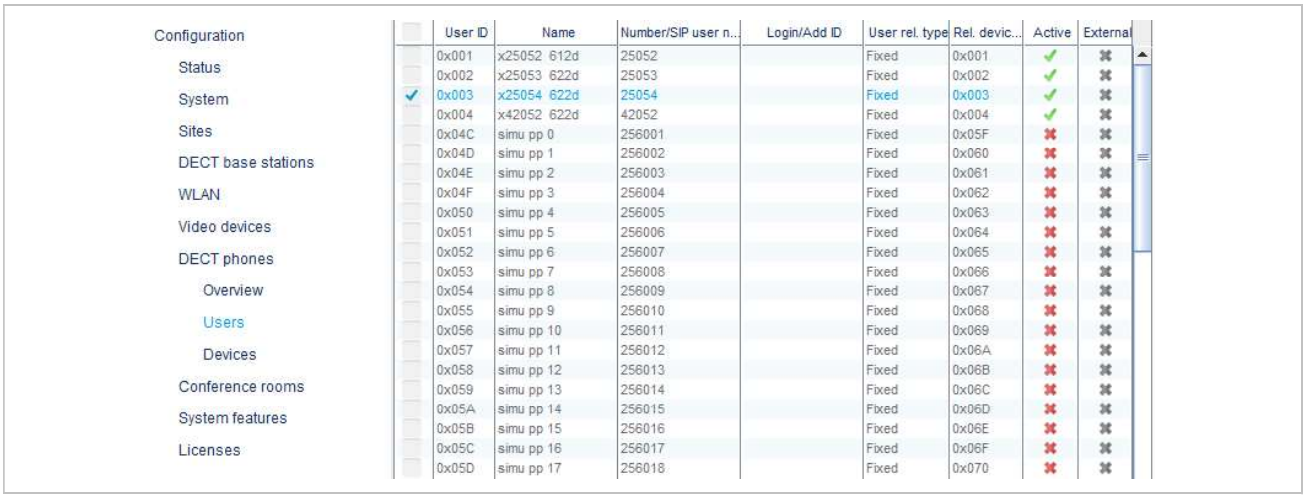
8.29.7.1 “System settings: User monitoring” Menu



The following parameters can be configured on system level.

- **Locating escalation**: If this option enabled, the alarm trigger “LOC-ERR-USERSTATE” will be generated by the OMM. Default setting is “off”.
- **Start-up delay**: The start-up delay defines the period of time the user monitoring start-up is delayed (between 2 and 15 minutes) after failover or system start-up.
- **Escalation delay**: The escalation delay defines the period of time the user monitoring will wait before the unavailable status is escalated.
- **Activity timeout 1**: The activity timeout 1 defines the maximum time (between 30 and 1440 minutes) between user activities in passive monitoring mode.
- **Activity timeout 2**: The activity timeout 2 defines the maximum time (between 5 and 60 minutes) between user activities in active monitoring mode.
- **Battery threshold**: The battery threshold defines the minimum battery load (between 0 and 100% in steps of 5%).

8.29.7.2 “DECT Phones” Menu



The following parameter can be configured on user level.

Monitoring mode: The user monitoring mode can be set to **Off**, **Passive** or **Active**. **Off** disables user monitoring. **Passive** and **Active** enable user monitoring and control the mode of the DECT phone activity status supervision. Default setting is **Off**.

If user monitoring is activated, the **VIP** option in the **DECT Phones** -> **Users** -> **SIP** tab for the user will be set automatically (see page 178). The **VIP** option will not be reset if the user monitoring mode is set to “Off”.

8.29.7.3 “DECT Phones -> User monitoring” Menu

The status of all monitored users is presented by the OMM in the **DECT Phones** -> **User monitoring** menu.

8.29.7.4 User Configuration Files

The parameter “UD_UserMonitoring” controls the monitoring for a user. The parameter can be set to “Off”, “Passive”, or “Active”.

8.29.7.5 OM IMA Application

If messages shall be sent out by the OM IMA application, the administrator must configure appropriate alarm scenarios for the alarm triggers in the OM IMA configuration file:

- UMON-OK-USERSTATE
- UMON-WARN-USERSTATE
- UMON-ERR-USERSTATE

8.29.8 START AND FAILOVER

The availability status is set to “Unknown” at start-up.

The monitoring feature does not escalate any user status during start-up until a configurable delay of min. 2 minutes and max. 15 minutes has elapsed.

The start-up delay should be adjusted according to the system start-up. The system start-up depends on the actual physical configuration, infrastructure components and parameter settings.

The statistic counter “Sync RFP start-up time” and “Sync Cluster start-up time” help to find an appropriate value for the start-up delay.

As soon as the start-up delay has elapsed, the status attributes are checked and the availability status will be determined. If the result is “Unavailable”, the status will be escalated.

The SIP registration process runs independently from the user monitoring start-up and infrastructure start-up. Monitored users as well as other users, who have the VIP flag set, are registered first.

8.29.9 SUPPORTED DECT PHONES

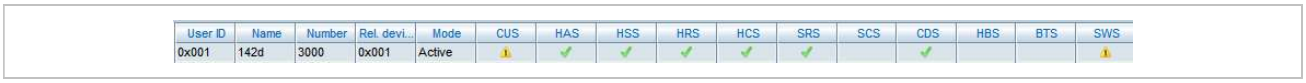
The Mitel 600 DECT phone family is fully supported. [1]

The following states are managed independent of the DECT phone type:

- Handset assignment status (HAS)
- Handset subscription status (HSS)
- Handset registration status (HRS)
- Handset activity status (HCS)7F7F2
- SIP user registration status (SRS)
- Call diversion status (CDS)

Notes on Mitel 142d

The Mitel 142d DECT phones are supported by SIP-DECT and have an enhanced feature set compared to GAP DECT phones. For Mitel 142d the availability status is always set to “Warning” because of the limited feature set.



User ID	Name	Number	Rel. devi...	Mode	CUS	HAS	HSS	HRS	HCS	SRS	SCS	CDS	HBS	BTS	SWS
0x001	142d	3000	0x001	Active	⚠	✓	✓	✓	✓	✓		✓			⚠

The following states are not supported:

- Handset battery state (HBS)
  always set to “Unknown”
- Software Status (SWS)
  always set to “Warning” to indicate the limited feature set
- Silent charging state (SCS)
  always “Unknown”

If the DECT phone is put into silent charging mode then it sends a “Detach”, like it is switched off.

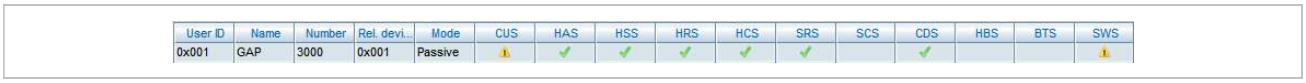
Comments on GAP DECT phones

GAP DECT phones are supported by SIP-DECT with a basic feature set. The availability status is always set to “Warning” because of the limited feature set.

---

[1] The DECT phones must be equipped with the software version that corresponds to the SIP–DECT® release. Otherwise, functionality may be limited.

[2] GAP devices do not support the active monitoring.



User ID	Name	Number	Rel. devi...	Mode	CUS	HAS	HSS	HRS	HCS	SRS	SCS	CDS	HBS	BTS	SWS
0x001	GAP	3000	0x001	Passive	⚠	✓	✓	✓	✓	✓		✓			⚠

The following states are not supported:

- Handset battery state (HBS)
  always “Unknown”
- Software Status (SWS)
  always set to “Warning” to indicate the limited feature set
- Silent charging state (SCS)
  always “Unknown”

GAP DECT phones do not support the active monitoring (Handset activity status /HCS). In general, there is no guarantee for the correct interworking of the 3rd party DECT phone with SIP-DECT.

8.29.10 RESTRICTIONS

The described mechanisms check the status information in the OMM. Therefore the solution has certain limitations.

The OMM determines the availability of the DECT device which does not necessarily represents the availability of the user.

- It is not possible to determine whether a user actually carries his device with or not.
- The check of the availability does not include the infrastructure to which the OMM is connected (e.g. call manager, etc.). A user appears as available even if the call manager fails.
- Feature (especially call diversion) when managed by the call server can undermine the monitoring.
- If a user is removed from the OMM, the monitoring stops without escalation. It cannot be checked if the user belongs to an alarm scenario configured in the alarm server or any other application scenario.

8.30 SRTP

Together with the new 3rd or 4th generation RFPs, SIP-DECT supports SRTP to encrypt the RTP voice streams and SDES for the SRTP key exchange.

There are three options for SRTP:

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

SIP-DECT provides the cipher suite AES_CM_128_HMAC_SHA1_80.

SRTP calls from DECT phones with DECT handover require that the SRTP functionality must be homogenously available on all effected RFPs. To allow mixed installations with the older RFP types 32/34 and 42 WLAN, the SRTP feature can be enabled or disabled per site. Whereby, SRTP can only be activated on sites with only 3rd or 4th generation RFPs included.

IMPORTANT : A handover of an SRTP call to a site with disabled SRTP will drop the call.

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

IMPORTANT : Please enable "SRTP = only" mode exclusively when all communication can be established with SRTP. Depending on the call server some features or gateways may not offer SRTP.

8.31 SIP OVER TLS

The transport protocol modes "TLS" or "Persistent TLS" enable a private and authenticated signaling, including safe key exchange for SRTP encryption.

The transport protocol and all further security settings can be set via the OMP **System** -> **SIP**-> **Security** tab and the OMP **System** -> **SIP**-> **Certificate Server** tab.

The following parameters can be set:

8.31.1.1 General

- **Transport protocol**: The protocol used by the OMM to send/receive SIP signaling. Default is "UDP".
- **Persistent TLS Keep alive timer active**: When enabled and "Persistent TLS" is selected as transport protocol, the OMM sends out keep alive messages periodically to keep the TLS connection open.
- **Persistent TLS Keep alive timer timeout**: Specifies the time, in seconds, between keep-alive messages sent out by the OMM. Valid values are "10" to "3600". Default is "30" seconds.
- **Send SIPS over TLS active**: When enabled and "TLS" or "Persistent TLS" is selected as transport protocol, the OMM uses SIPS URIs in the SIP signaling. Default is "ON".
- **TLS authentication**: When enabled and "TLS" or "Persistent TLS" is selected as transport protocol, the OMM validates the authenticity of the remote peer via exchanged certificates and the configured "Trusted certificates". Default is "ON".
- **TLS common name validation**: When enabled and "TLS authentication" is selected the OMM validates the "Alternative Name" and "Common Name" of the remote peer certificate against the configured proxy, registrar and outbound proxy settings. If there is no match an established TLS connection will be closed immediately.

8.31.1.2 PEM file import

- Allows the manual import of Trusted, Local Certificates and a Private Key in PEM file format.

The following parameters can only be read and should ease the handling of certificates:

- **Trusted Certificates**: The number of imported trusted certificates.
- **Local Certificate chain**: The number of imported certificates in the local certificate chain.
- **Private Key**: Is a private key imported or not.

8.31.1.3 Certificate server

Optionally is also an automatic import of Trusted, Local Certificates and a Private Key files from an external server possible. This can be configured on the “Certificate Server” tab.

The following parameters allow an automatic import:

- **Active**: Enable or disable the automatic import.
- **Protocol**: Selects the preferred protocol (FTP, TFTP, FTPS, HTTP, HTTPS, SFTP)
- **Server**: IP address or name of the server
- **User Name / Password / Password confirmation**: The server account data if necessary.
- **Path**: The path on the server to certificate files.
- **Trusted certificate file**: The name of the PEM file on the given server including the trusted certificates.
- **Local certificate file**: The name of the PEM file on the given server including the local certificate or a certificate chain.
- **Private key file**: The name of the PEM file on the given server including the local key.

8.31.2 CERTIFICATES

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

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

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

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

```
-----BEGIN CERTIFICATE-----
```

and

```
-----END CERTIFICATE-----
```

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

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

Trusted Certificates

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

Local Certificates

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

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

8.31.3 PRIVATE KEY

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

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

```
-----BEGIN RSA PRIVATE KEY-----
```

and

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

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

8.31.4 TLS TRANSPORT MODE

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

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

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

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

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

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

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

8.31.5 VERIFICATION OF REMOTE CERTIFICATES

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

The signature of the certificate is checked with the public key of the signing certificate. The certificate chain is checked until a *Trusted Certificate* is found. If self-signed certificate is found which is not trusted, the verification fails.

The current time must be in the validity period of the certificate. For this mechanism a correct system time must be provided (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 is expired no further communication is possible. The certificates must be replaced before to prevent a breakdown of call services.

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

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

8.31.6 ADDITIONAL SECURITY CONSIDERATIONS

For highest security requirements there are additional considerations to be taken into account when enrolling an OpenMobility system.

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

> **IMPORTANT : To prevent manipulation of certificates and keys in unsecure environments we recommend not to use the automatic import of certificates and keys. Especially the unsecure protocols TFTP, FTP and HTTP must be avoided. It is**

also recommended to protect the selected protocol with a login to prevent unauthorized access to the private key file.

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

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

8.32 DECT ENHANCED SECURITY

Security aspects in the DECT standard have been improved after concerns were raised in the market in recent years. Therefore various enhancements have been introduced.

The usage of many security features, which were already available in the DECT standard (respectively GAP) from the beginning, was left optional for the devices. These mechanisms became mandatory together with CAT-iq. Almost each of these functionalities was present and used within SIP-DECT right from the start.

Furthermore, some new features have been added to GAP:

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

Each procedure brings additional guarantee on security and is an integral part of the SIP-DECT solution.

The feature set can be enabled or disabled per site. This distinction is necessary due to the fact, that enhanced security is available with RFPs 35/36/37/43/44/45/48 only.

From release 5.0 on, when DECT enhanced security is enabled, every connection will be encrypted, not only voice calls, but also such as service calls (e.g. list access) or messaging.

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

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

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

8.33 MIGRATION OF RFP SL35 IP FROM SIP-DECT LITE 3.1 TO SIP-DECT 6.1

The SIP-DECT Lite solution realized a single-cell DECT network that offered only limited radio coverage and was operated with one RFP SL35 IP. The SIP-DECT Lite solution was part of the SIP-DECT product family that offered larger radio coverage by realizing multi-cell DECT networks with up to 256 RFPs.

You can integrate the RFP SL35 IP to a multi-cell SIP-DECT network. The migration from SIP-DECT Lite to the current release of the standard SIP-DECT system is supported. During the migration the SIP-DECT Lite software is replaced by the standard SIP-DECT software on the RFP SL35 IP and a reset to the factory setting is performed. All configuration data are removed from the base station.

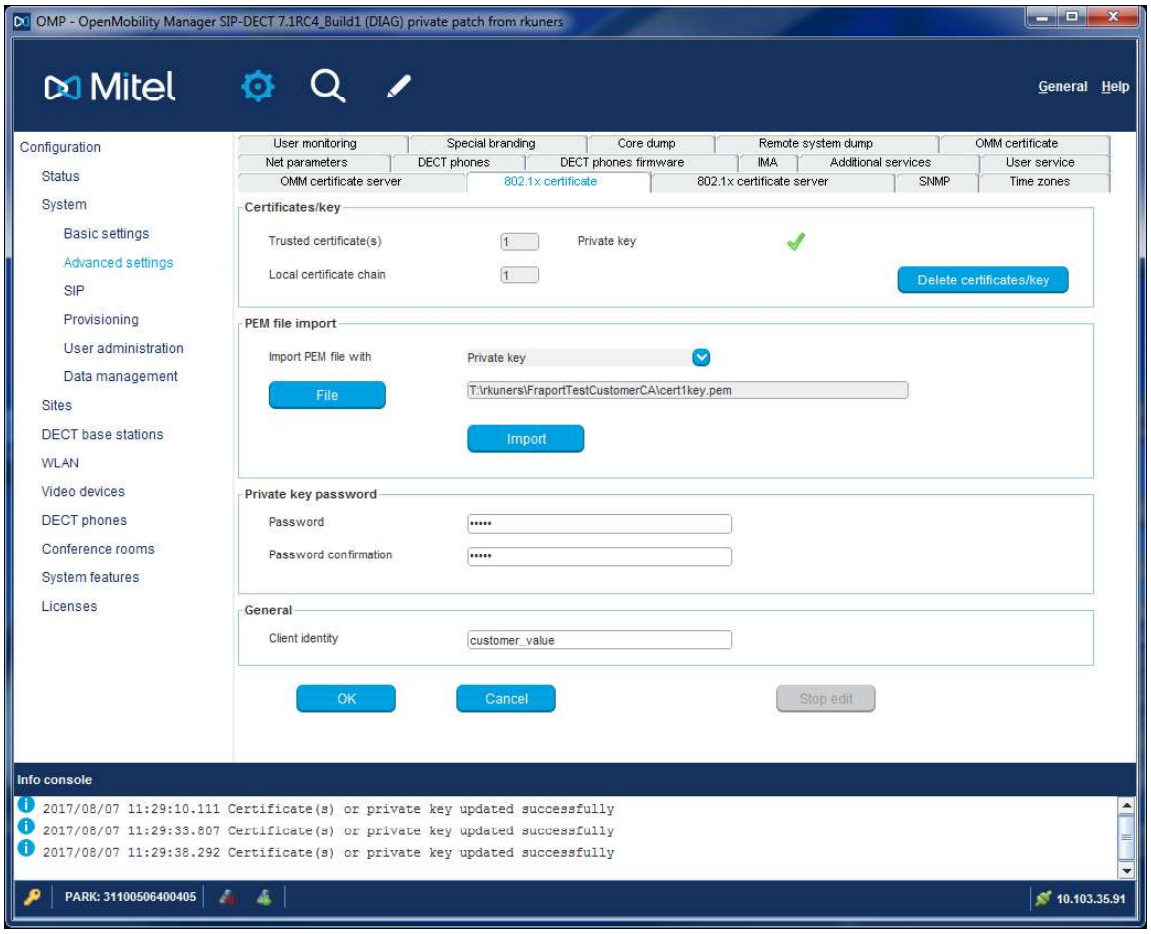
The following migration process must be performed.

Precondition: Unique UNLOCK.xml file is available for the specific RFP SL35 IP.

1. Remove the USB flash memory from the RFP SL35 IP and plug it into your computer.
2. Copy the unlock.xml file onto the USB flash memory.
3. Copy the standard SIP-DECT SW (iprfp3G.dnld) onto the USB flash memory of the RFP.
4. Check if the following files are on the USB flash memory (no other files should be on the USB flash memory except SIP-DECT™ Lite DB backup field “omm_conf.txt” which is not relevant).
   a. PARK.xml
   b. UNLOCK.xml
   c. iprfp3G.dnld
5. Remove the USB flash memory from your computer and plug into the RFP SL35 IP.
6. The migration process starts automatically after plugging the USB flash memory into the RFP.
7. Wait for the RFP reboot and start-up. Do not interrupt the electric power during this process.
8. The SW update for RFPs in standard SIP-DECT installations are provided by other means than to copy the SW on the USB flash memory. Therefore the iprfp3G.dnld must be removed from the USB flash memory.
   Make sure that the PARK.xml and UNLOCK.xml remain on the USB flash memory.
9. Also after the migration, make sure that the USB flash memory is always plugged in the RFP.
10. Now, the RFP SL35 IP has the standard SIP-DECT SW and the UNLOCK.xml file and can be operated in standard SIP-DECT installations. Please follow the standard procedures to setup a SIP-DECT installation.

8.34 802.1X CERTIFICATE BASED AUTHENTICATION

You can assign a group certificate to all RFPs of a SIP-DECT installation for certificate based authentification to open the switch ports the RFPs are connected to.



8.34.1 802.1X CONFIGURATION

You can import trusted certificates, a local certificate chain and a private key file for 802.1x certificate based authentication manually through OMP or OMM configuration files.

8.34.1.1 Configure and store 802.1x certificate settings

- 802.1x certificate data are optional parameters. 802.1x certificate based authentication works only if valid certificate data is configured and the feature is set to enabled.
- 802.1x certificate data is stored centrally in OMM database and can be set by OMP, through an OMM provisioning file or from a certificate server.
- The centrally stored 802.1x certificate data remains valid until it is changed or removed by one of the configuration sources.
- The stored 802.1x certificate data is used after a reset/reboot/power cycle even if the provisioning server is not reachable.
- RFPs receive the encrypted 802.1x certificate data from OMM via a HTTP file request, for example, after reboot or after notification of new certificate data from the OMM. Only RFPs can decrypt and use the certificate data.
- The 802.1x certificate data will be stored locally on RFPs.

8.34.1.2 Configure and store 802.1x certificate server settings

- 802.1x certificate server settings are optional parameters. If configured, the OMM uses the configured file server to load/update the 802.1x certificate data (group certificate, private key, Trusted (CA) certificate(s))
- 802.1x certificate server settings are stored centrally in OMM database and can be set by OMP or via an OMM provisioning file.

8.34.1.3 Discard OMM DB or RFP factory reset, which are offered as restart options

- The 802.1x certificate data and the 802.1x certificate server settings on the (RFP-) OMM are lost.
- The 802.1x certificate data and the 802.1x certificate server settings have to be configured again; otherwise, the RFPs receive empty 802.1x certificate data on the next 802.1x update.
- To delete 802.1x certificate data from a RFP, the data can be deleted on the OMM (applies to connected RFPs), or a factory reset of an RFP can be initiated (OM-Configurator or through an prepared USB stick).

8.34.2 PREREQUISITES REFERRING TO 802.1X TOPOLOGY

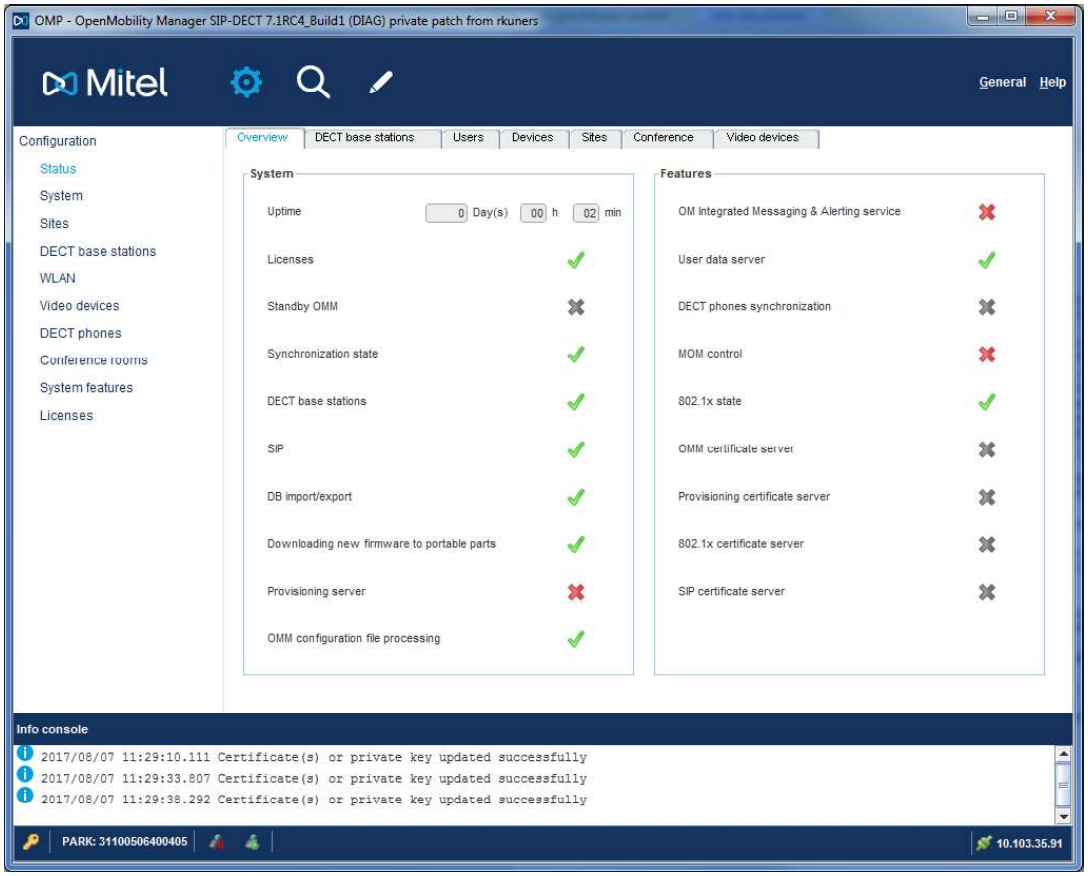
802.1x group certificate based authentication runs in networks, which fulfill needs of a proper running 802.1x administration:

- Radius server
- Switch port configuration
- Closed mode (initial 802.1x configuration in safe environment) or low-impact mode (DHCP, DNS, NTP, TFTP, HTTP (for the transfer of the 802.1x configuration to the RFPs)) enabled. HTTP traffic between the OMM and RFPs in different VLAN (guest VLAN for unauthorized clients) needs to be routed by a layer 3 switch or router so authorized RFPs can receive their 802.1x configuration or guest VLAN (DHCP, DNS, NTP, TFTP - HTTPS to OMM needs to be routed). Traffic between different VLANs (including the native VLAN) is routed by a layer 3 switch or router. Even a proper routing between native VLAN and SDC VLAN is mandatory or guest VLAN (DHCP, DNS, NTP, TFTP - HTTPS to OMM needs to be routed)
- Full access to productive network after successfull 802.1x authentication

8.34.3 802.1X FEATURE DESCRIPTION

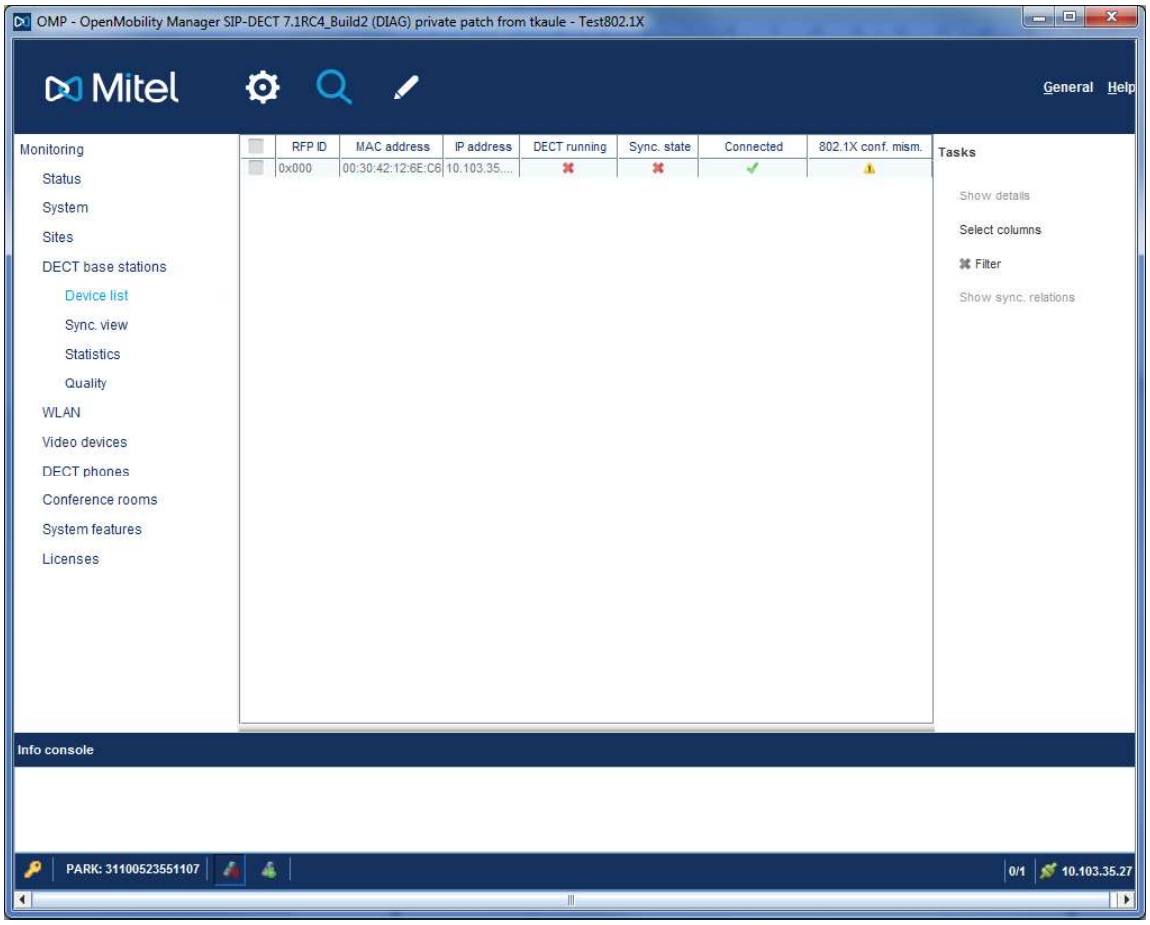
- All RFPs of an installation needs to get updated to a firmware which supports 802.1x (either in a secure environment or on a switch port in low-impact mode or in a guest VLAN were access to DHCP and TFTP is possible).

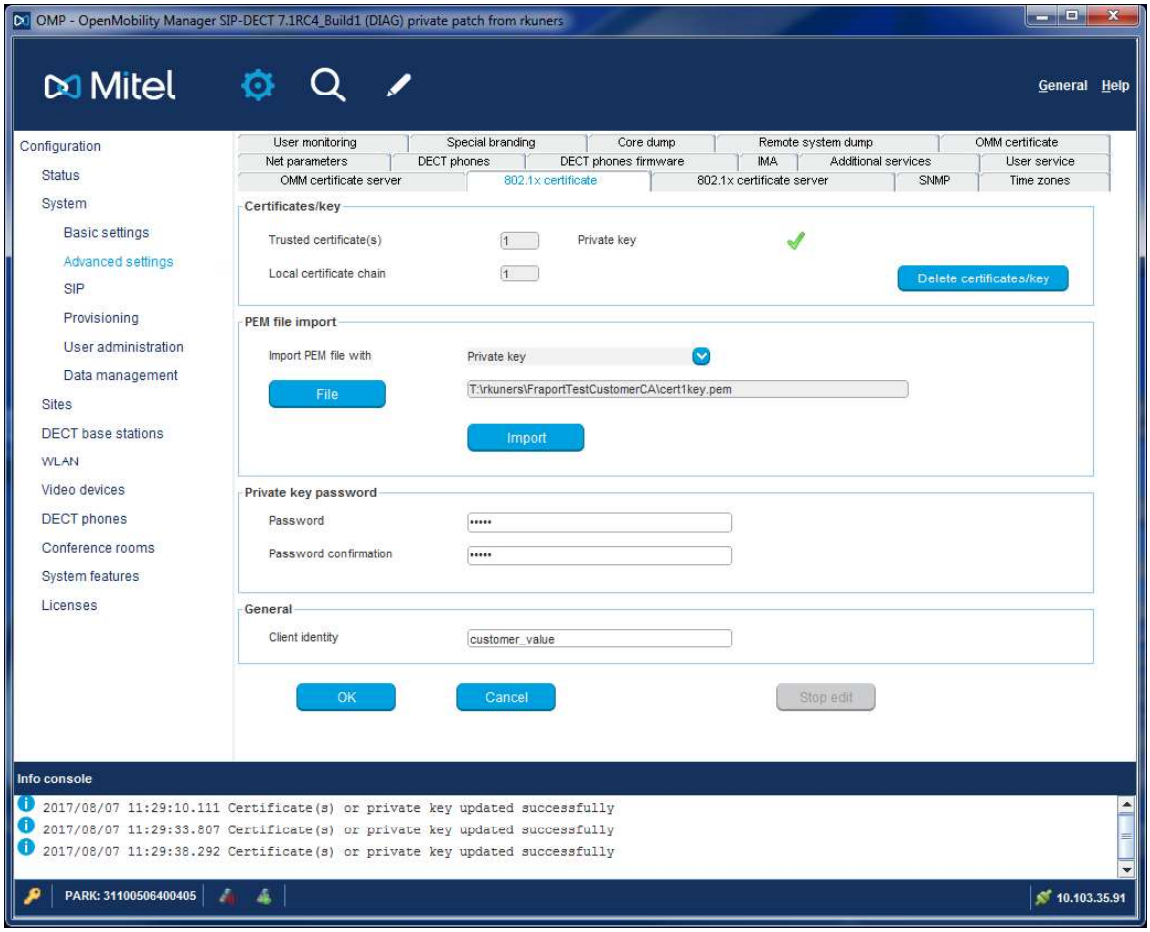
- Initial 802.1x certificate request from OMM needs to be enabled on the RFP through local configuration (OM-Configurator parameter independent from local configuration flag) or a DHCP option (option 43 suboption + unused DHCP option) to prevent impact on existing installations. If 802.1x certificates are already loaded to an RFP, updates are requested independent from this local or DHCP configuration.
- OMP supports the configuration of 802.1x group certificate data or alternatively the configuration of a certificate server for automatic update of the certificates from a file server.
- For the group certificate, a unique 802.1x identity for all RFPs is supported.
- To enable 802.1x on RFP each of them is initialized by DHCP option or OM_Configurator. Otherwise the feature is inactive for a RFP (see 7.36).
- RFPs request RSA encrypted 802.1x certificate data through HTTP from the active OMM (either in a secure environment or on a switch port in low-impact mode or in a guest VLAN were access to DHCP and to the OMM via HTTP is possible).
- Certificate data is requested/updated, for example on RFP startup or after a certificate update has been triggered by the OMM.
- In addition to the certificate data, a RFP receives and applies the admin and root login credentials (user name and password hash). Thereby access to the RFP root file system is no longer possible with the default password of previously unconfigured RFPs.
- The certificate data is stored reset proof in the RFPs.
- If an 802.1x certificate data file was received from the OMM, RFP admin and root login credentials cannot be changed through the IPL protocol between OMM and RFP (for example, by connecting to a different OMM system > factory reset required).
- You can delete 802.1x certificate data from the OMM. Afterwards, the data is deleted from connected RFPs.
- New edit mode in OMP for 802.1x certificate settings to prevent inconsistent configuration (changed settings will not be used before leaving the edit mode).
- New DECT base station attribute 802.1x configuration mismatch for the device list in OMP monitoring mode.
- New health states for 802.1x are supported. A warning message appears while the 802.1x edit mode is active and shows mismatch errors if certificates cannot be updated from the 802.1x certificate server or if not all RFPs have the correct certificate checksum (certificate mismatch).



New health state for 802.1x

802.1x configuration mismatch in DECT base stations device list (OMP monitoring mode).


OMP - OpenMobility Manager SIP-DECT 7.1RC4_Build2 (DIAG) private patch from tkaule - Test802.1X
Mitel
General
Help
Monitoring
Status
System
Sites
DECT base stations
Device list
Sync. view
Statistics
Quality
WLAN
Video devices
DECT phones
Conference rooms
System features
Licenses
RFP ID
MAC address
IP address
DECT running
Sync. state
Connected
802.1X conf. mism.
0x000
00:30:42:12:6E:C6
10.103.35....
Tasks
Show details
Select columns
Filter
Show sync. relations
Info console
PARK: 31100523551107
0/1
10.103.35.27

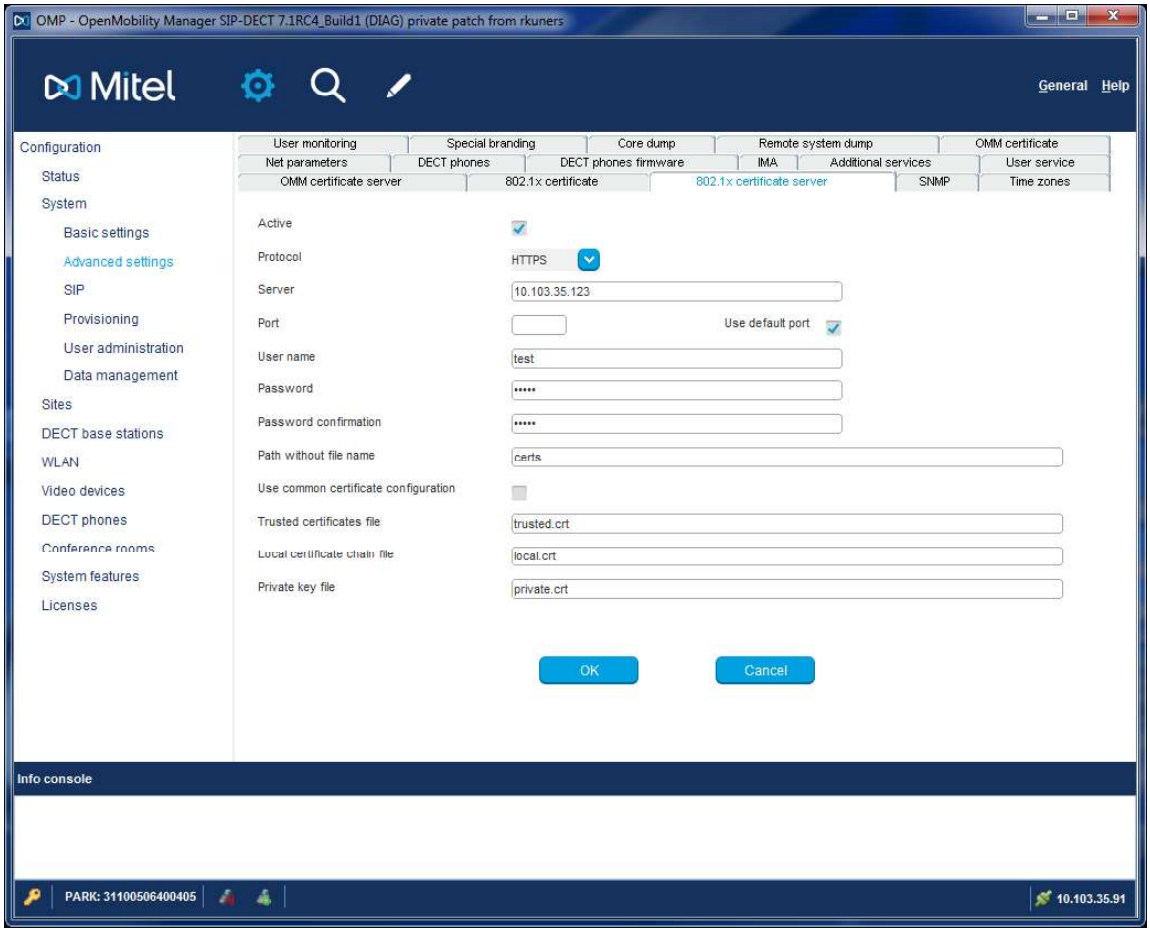


You can import trusted certificates, a local certificate chain and a private key file for 802.1x certificate based authentication manually through OMP or OMM configuration files.

- **Certificates/key**: Shows the number of active 802.1x trusted certificates, the number of 802.1x local certificate chains and whether a 802.1x private key is used. All can be deleted with the Deletecertificates/key button.
- **PEM file import / Import PEM file with**: Specifies the type of file 802.1x (trusted certificate, local certificate, or private key) and the location of the file to be imported.
- **General/Client identity**: 802.1x supplicant client identity.
- **Private key password/ Password**: Specifies the password for the 802.1x private key file.

8.35 802.1X CERTIFICATE SERVER CONFIGURATION

Through configuration of a 802.1x certificate server URL, you can update the 802.1x certificate data automatically.



Configuration of the 802.1x certificate server using OMP.

- **User name**: Specifies the user name for authentication against the certificate server.
- **Password**: Specifies the password for authentication against the certificate server.
- **Active**: Enables or disables the certificate server URL feature.
- **Protocol**: Specifies the protocol to be used to fetch the certificate files. One of FTP / FTPS / SFTP / HTTP / HTTPS / TFTP / None.
- **Port**: Specifies the certificate server's port number or use of the default port for the used protocol.
- **Server**: Specifies the IP address or name of the certificate server.
- **Path without the filename**: Specifies the path to the certificate files on the certificate server.
- **Trusted certificates file**: Filename of the trusted certificates to read from the server.

- **Local certificate chain file**: Filename of the local certificates to read from the server.
- **Private key file**: Filename of the private key to read from the server.

8.36 INITIATE 802.1X BY DHCP OPTIONS OR OM_CONFIGURATOR

Before 802.1x starts the feature, it has to be initialized by DHCP or by the OM_Configurator tool.

8.36.1 DHCP OPTIONS

There are two ways, either DHCP option 226 or the vendor specific option 43 (code 226) can be used.

DHCP option 226	set this option to 1	the option is optional
Vendor specific option 43	set code 226 to 1	code 226 is optional

8.36.2 OM_CONFIGURATOR

Select the parameter *Activate 802.1x* and set it to true. If `.csv` config files are used, set the common value *use_802_1x=1*.

9 MAINTENANCE

9.1 SITE SURVEY MEASUREMENT EQUIPMENT

If a SIP-DECT installation must be planned, a sufficient distribution of DECT base stations that meets the requirements for reliable synchronization and connectivity to the DECT phones is necessary. The site survey kit may help you. It comprises:

- One measuring RFP with its own power supply.
- A tripod and a battery for the RFP.
- Two reference DECT phones with chargers.
- Battery chargers.
- Optional a measuring DECT phone which can monitor other makers DECT radio sources.

9.2 CHECKING THE MITEL HANDSET FIRMWARE VERSION

You can display the version information of a Mitel 600 or Mitel 142d DECT phone with a few keystrokes. Check the firmware version to determine whether an update is required to overcome any user issues.

11 Press the **Menu** soft key.

12 Select **System** (only to highlight).

13 Press **OK**.

14 Select **Version Number**.

15 Press **OK**.

The display shows the software and the hardware version of the Mitel DECT phone.

9.3 DIAGNOSTIC

9.3.1 MITEL DECT PHONE SITE SURVEY MODE

You can switch a Mitel 600 or Mitel 142d DECT phones into “site survey mode” with a few keystrokes. In this mode the phone will display the RFPs and the actual field strength of the receiving signal in dBm.

1 Press the **Menu** soft key.

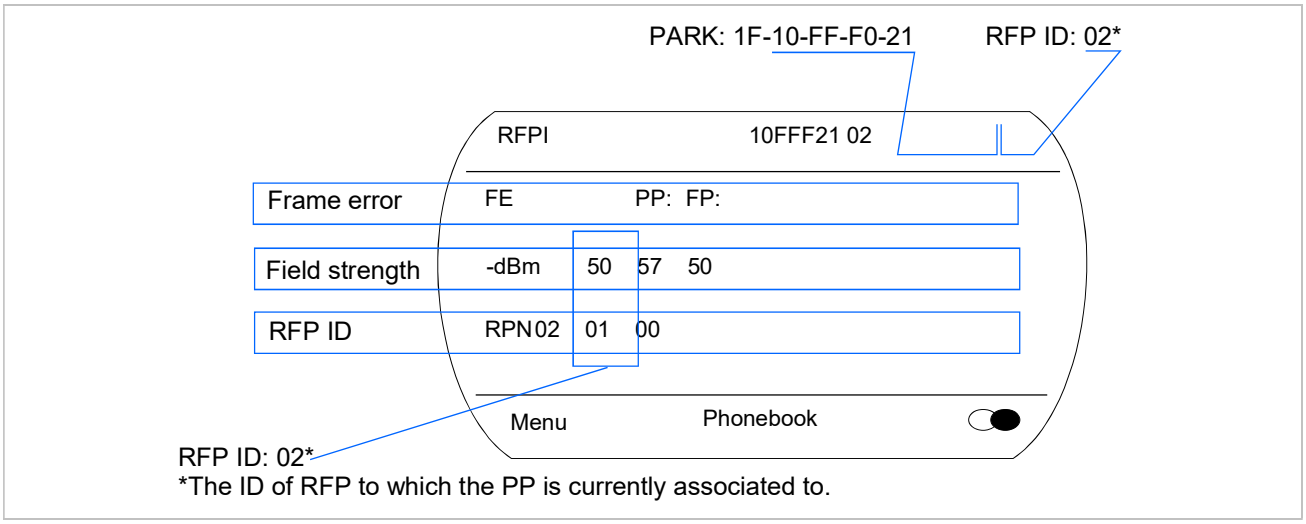
2 Enter the following key sequence “***76#” (Mitel 600) or “R***76#” (Mitel 142d).

3 Select Site Survey.

4 Press OK.

5 To leave the site survey mode, switch the phone off and on again.

The following display is shown on the Mitel DECT phone:



In this example the DECT phone is currently connected to the RFP with the number 02. The RFPs 01 and 00 are also visible. The number “10FFF221 02” on the upper right side refers to the PARK (Example 1F-10-F2-21) of the SIP-DECT system and to the RFP to which the phone is currently connected to.

9.3.2 MITEL HANDSET AUTO CALL TEST MODE

You can switch a Mitel 600 or Mitel 142d DECT phones into “auto call test mode” with a few keystrokes. In this mode the phone will call a specified number cyclically. You can use this feature to generate traffic for test purposes. This mode is also active if the phone is on the charger.

1 Press the **Menu** soft key.

2 Enter the following key sequence “***76#” (Mitel 600) or “R***76#” (Mitel 142d).

3 Select Auto Call Test.

4 Press OK.

5 Enter the phone number to call.

6 Press OK.

7 Enter a number of seconds between two calls.

8 Press OK.

9 Enter a number of seconds a call shall be active.

10 Press OK. The test will be started automatically.

11 To stop the test, switch the phone off and on again.

9.3.3 MITEL HANDSET AUTO ANSWER TEST MODE

You can switch a Mitel 600 or Mitel 142d DECT phone into “auto answer test mode” with a few keystrokes. In this mode, the phone answers incoming calls automatically. You can use this feature together with phones in the “auto call test mode” (see the above section 9.3.2) for test purposes. This mode is also active if the phone is on the charger.

1 Press the **Menu** soft key.
2 Enter the following key sequence “***76#” (Mitel 600) or “R***76#” (Mitel 142d).
3 Select Auto Answer.
4 Press OK.
5 Enter a number of seconds the phone shall ring before it will answer the call.
6 Press OK.
7 Enter a number of seconds a call shall be active.
8 Press OK. The test will be started automatically.
9 To stop the test, switch the phone off and on again.

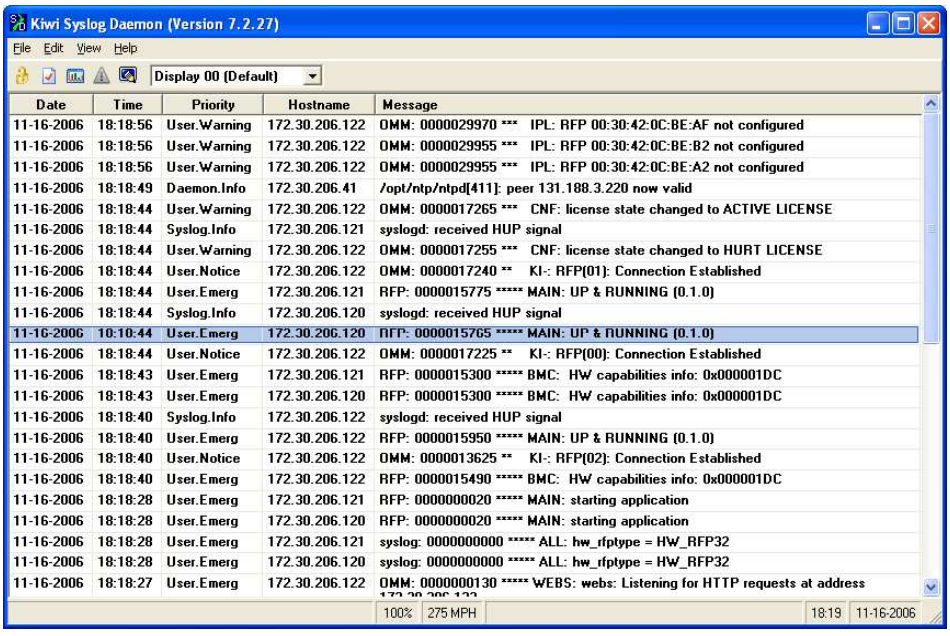
9.3.4 SYSLOG

The OpenMobility Manager and the RFPs are capable of propagating Syslog messages conforming to RFC 3164 (see /13/). This feature together with the IP address of a host collecting these messages can be configured.

Syslog must be enabled by:

- DHCP using the suboption 14 and 15 of vendor option 43.
- Setting the syslog daemon server and port via the web interface.

To set up the syslog via DHCP or the OM Configurator has the advantage that syslogs are available in earlier states of the RFP startup.



The level of syslog messages in the default state allows the user to have control over the general system state and major failures.

9.3.5 SSH USER SHELL

Each RFP offers a lot of commands within the SSH shell. Most of them are useful for diagnostics and may help experts to resolve failures.

Note: Some commands can harm the system operation.

The SSH access of an RFP is open if

- the RFP is connected to an OMM and the “Remote Access” is switched on or
- the RFP is not connected to an OMM.

To activate the SSH access of an RFP that has a connection to an OMM, enable the **Remote access** checkbox on the OMM **System settings** web page (see section 5.4.1.1). In the OMP, the SSH access is activated/deactivated in the **General** tab of the **System** -> **Basic settings** menu (see section 6.5.1).

9.3.5.1 Login

To log into the SSH user shell:

1 Open an SSH session to the IP DECT base station with the “Full access” user name.

2 Enter the password for the “Full access” account (see also 8.17.1).

The output should look like:

```
Welcome to IP RFP OpenMobility SIP Only Version 2.1.x

last reset cause: hardware reset (Power-on reset)

omm@172.30.206.94's password:
omm@172.30.206.94 >
```

9.3.5.2 Command Overview

Type `help` to get a command overview:

Command	Description
exit,quit,bye	Leave session
ommconsole	OMM console
ip_rfpconsole	RFP console
rfpm_console	RFP manager console
wlan_console	WLAN console
ics_console	ICS console
ldb	View / set local configuration (OmConfigurator)
setconsole	Duplicate messages to console
noconsole	Do not duplicate messages to console
dmesg	Messages from last boot
logread	Last messages
su	Switch to user root

ping	Well known ping
traceroute	Well known traceroute
free	Well known free
ps	Well known ps
top	Well known top
ifconfig	Well known ifconfig
uptime	Well known uptime
reboot	Well known reboot
date	Well known date (time in UTC)

9.3.5.3 OMM Console On Linux Server

You can call the OMM console on the Linux server which runs the OMM using the “ommconsole” command. Log on as root as it is necessary to install and/or update OMM.

> **IMPORTANT : If you not login as root to open the OMM console then the path to ommconsole is not set and you must enter the whole path “/usr/sbin/ommconsole” to start the OMM console.**

9.3.5.4 RFP Console Commands

If you type `ip_rfpconsole` you are able to use the following commands on each RFP:

Command	Description
?	Displays Command Help Table
bt	Bluetooth commands
confmix	Displays status of conference mixer
help	Displays Command Help Table
logger	Send a string to the syslog daemon
deftrc	Resets all trace settings to default
runtime	Reports the process runtime
mem	Show memory and heap
exit	Leave this console
heap	Shows heap buffer statistics
heapcheck	Verifies the guard space of all via doss allocated buffer. Heap functions are locked during check
heapdetails	Print detailed heap usage
jpeg	Jpeg helper commands
lu10	Lu10 SDU <-> PDU converter
mclose	Close a media channel

Command	Description
mconf	Configure IP settings for a media channel
media	Display state of media channels
mopen	Open a media channel
mroute	Display media routes
mstart	Start a media channel
mstop	Stop a media channel
mswo	Codec switch over for an active call
mtime	Display media time statistics
mutex	Lists all created MXP mutexes
omms	Shows connection status to OMM(s)
otpdbCheck	Check all OTP pages for valid elements
queues	Lists all created MXP queues
reset	Resets the IPRFP application
resume	Resume bmc activity
sem	Lists all created MXP semaphores
signals	Print signal dwell time in queues
spy	Set/display spy levels: [<key #> <level #>]
suspend	Suspend bmc activity
tasks	Lists all running MXP tasks
tickres	Print tick resolution
timer	Print running timer
video	Video commands

Please note: The “spy” command enables you to increase the level of syslog messages. This should be only used by instructions of the support organization because it can harm the system operation.

9.3.5.5 OMM Console Commands

If you have opened the session on the OMM RFP and you type “ommconsole”, you are able to use the following OpenMobility Manager (OMM) related commands:

Command	Description
?	Displays Command Help Table
adb	Automatic DB export and import (ADB) console
axi	AXI commands
axic	Task console for AXI command processing of provisioning files

Command	Description
cert	Certificate import console
cmi	CMI commands
cnf	Show configuration parameters
cron	Display pending cron jobs
help	Displays Command Help Table
logger	Send a string to the syslog daemon
deftrc	Resets all trace settings to default
dlc	DECT Data Link Control
dm	Download Over Air Manager
dsip	DSIP commands
epr	External provisioning task (EPR) console and dynamic users console
runtime	Report the process runtime
mem	Show memory and heap
exit	Leave this console
gmi	DECTnet2 Inter Working Unit
hcm	Handset configuration management task (HCM) console
heartbeat	Configure heartbeat mechanism for IP-RFPs
ima	IMA commands
inspect	Display information of a user
ipc	Display socket communication
ipl	Display connected RFPs
iplfilter	Configure which RFPs spy messages are generated for
lic	LIC commands
loc	Info about locating extension
mon	Toggle monitor functionality
msm	Display states within MediaStreamManagement
msmtrc	Display / modify list of traced DECT phoneNs
mutex	List all created MXP mutexes
nwk	DECT network layer
prov	Prov-related commands
queues	List all created MXP queues
rcmd	Remote command on RFPs shell
rfp	Radio Fixed Part Control
rfpd	Radio Fixed Part Debug
rfps	Radio Fixed Part Statistic

Command	Description
rping	Request one or more RFPs to ping a host
rspy	Remote configure spy levels on IP-RFPs
rsx	Toggle RSX debug port on RFPs
rtt	Set event flag for high RTT values / clear values
sem	List all created MXP semaphores
spy	Set/display spy levels: [<key #> <level #>]
standby	Displays redundant OMMs
stat	Statistic
sync	Commands for RFP synchronization
sysdump	Initiate system dump
tasks	List all running MXP tasks
tickres	Print tick resolution
trc	Back trace task
tzone	Time zone commands
uds	UDS commands
umo	UMO commands
upd	Display update status of RFPs
update	Force all connected RFPs to search for new software
uptime	Display OpenMobility Manager uptime
ver	Version information
video	Command for video devices
wlan	Display states within Wireless LAN Management
xml	XML browser task (XML) console
xsc	XSC commands

Please note: The “spy” command enables you to increase the level of syslog messages especially for subsystems of the OMM. This should be only used by instructions of the support organization because it can harm the system operation.

9.3.6 CORE FILE CAPTURING

Fatal software problems may result in memory dumps, so called core files. These core files are helpful in analyzing the problem that caused the abnormal termination of the program. The IP RFP is capable of transferring the core files to a remote fileserver. Without any special configuration the files are transferred to the TFTP server that is used to get the system software. The path used is the directory of

the boot image. These two configuration items are retrieved from DHCP or via local configuration using the OM Configurator.

You can configure the URL to a writable directory via the OMM (see section 5.4.1.14) or through the “OM_CoreFileSrvUrl” variable in the ipdect.cfg configuration files.

> **Please note:** The server must allow writing new files (not typically enabled by default).

9.3.7 DECT MONITOR

> **Please note:** The DECT Monitor has been replaced by OMP but the DECT Monitor can still be used without warranty for SIP-DECT installations with a standard PARK and up to 256 RFPs all within paging area 0.

For better error detection in the SIP-DECT system the DECT Monitor can be used. The DECT Monitor is an MS Windows based stand-alone program. It provides the possibility to give a real-time overview of the current IP DECT base station and telephone states in the SIP-DECT system.

The following features are provided by the DECT Monitor:

- Reading out of the DECT configuration of an SIP-DECT system.
- Configuration can be stored in an ASCII file.
- Display of DECT transactions IP DECT base station <–> telephone in clear tabular form with highlighting of handover situations. Real-time display.
- Display of further events concerning the status or actions of IP DECT base stations and telephones of the SIP-DECT system.
- All events can also be recorded in a log file.
- Display of the synchronization relations between the RFPs.
- Monitoring of systems with up to 256 IP DECT base stations and 512 DECT phones.
- Reading out and display of IP DECT RFP statistics data, either for a single IP DECT RFP or for all IP DECT RFPs.
- Display of DECT central data of the SIP-DECT system.

The DECT Monitor program can only be used when the **DECT monitor** checkbox is activated on the flag in the OMM **System settings** web page.

> **Please note:** Because of security, the DECT monitor flag is not stored permanently in the internal flash memory of the OMM/RFP. After a reset the DECT monitor flag is disabled.

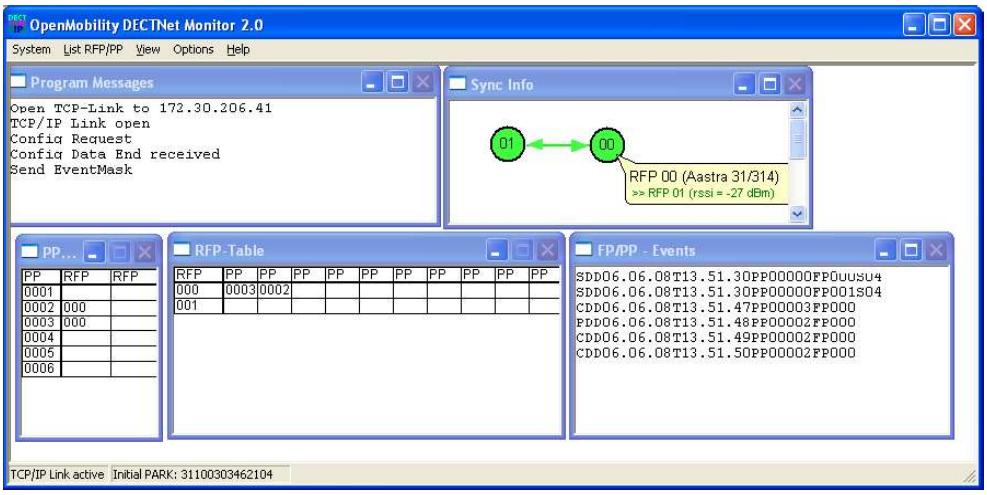
The DECT monitor program is used together with the SIP-DECT system. When the program is started, the user is requested to enter the IP address of the IP DECT RFP or the server running the OpenMobility Manager (OMM) software.

There can be several reasons for an unsuccessful link establishment:

- Operation of DECT monitor is not enabled inside the OMM. Use the OMM web service to enable DECT monitor operation.
- IP address is not correct. It must be the address of the RFP the OMM is running on.

- A link routed to the RFP is not supported.

The program displays the IP address which was used last time. When the program is started, a link to the OMM is automatically established and the program window shows all user configured child windows and tables. When all links have been established, the DECT data of the system are automatically read out and entered in the tables “RFP-Table” and “DECT phone-Table”. This procedure is called “Config Request”.



Next, the defined trace options (Event Mask) are sent to the OMM. The options which are sent to the OMM are always those which were active the last time the program was exited.

If the trace option “Transaction establish/release” is activated, the OMM will deliver all existing transactions.

Following this, the OMM system delivers the desired trace data. The user can either communicate with the program interactively (see below) or he can simply activate a log file in which to record the data.

Following this initialization, the user can carry out the following modifications:

- The trace settings can be modified using the menu item **Options-Event Mask**. Transmission to the OMM takes place after confirmation of the settings with **OK**.
- A Config Request can be sent again to the OMM.
- A log file can be activated.
- By means of various dialogs, the configuration data of the telephones, RFPs and control modules can be displayed and stored in ASCII files.

The following information is displayed dynamically in the tables:

- Transactions between telephone and DECT system. These are displayed in both tables. Simple transactions are displayed in black on a white background; during handover, both transactions involved are displayed in white on a red background.
- The Location Registration and Detach events are displayed in the tables for approx. 1-2s after their occurrence (light green background), if possible. There is no display in the FP table if there is no column free for display. If the event has already been displayed, it can be overwritten at any time. The events are not displayed if they occur during an on-going transaction. Irrelevant of whether the events are displayed in the tables, they are always entered in the **FP/DECT phone-Events** window and in the log file (provided that this is open).

The following color scheme is used for display of the RFPs in the RFP table:

- RFP gray-blue: IP DECT base station is not active (not connected or disturbance).
- RFP black: IP DECT base station is active.

The data of an RFP are displayed in a dialogue box after clicking on the respective RFP field in the RFP table. The statistics data of the RFP can be called up from this dialogue box.

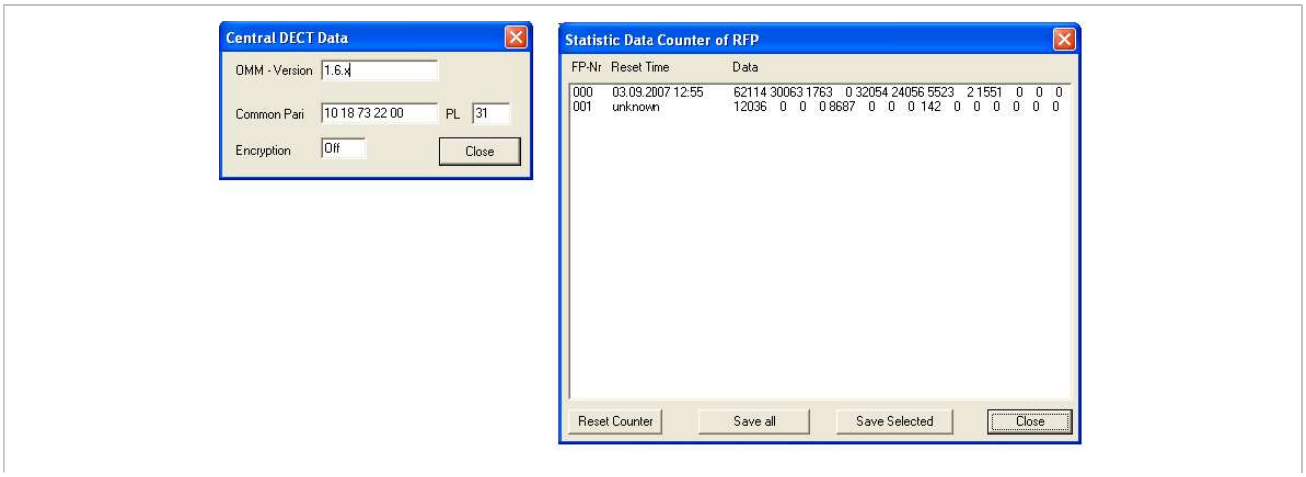
The following color scheme is used for display of the telephone in the DECT phone table:

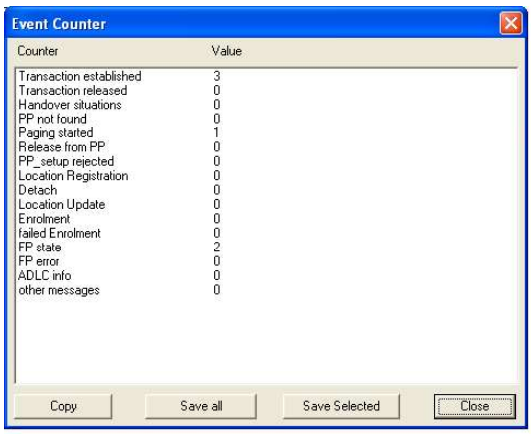
- DECT phone black: Handset is enrolled. It is assumed that the telephone can be reached.
- DECT phone blue: Handset can presumably not be reached. Detach was received, or when an attempt was made to reach a telephone, the DECT phone did not answer.
- DECT phone gray blue: Handset not enrolled.

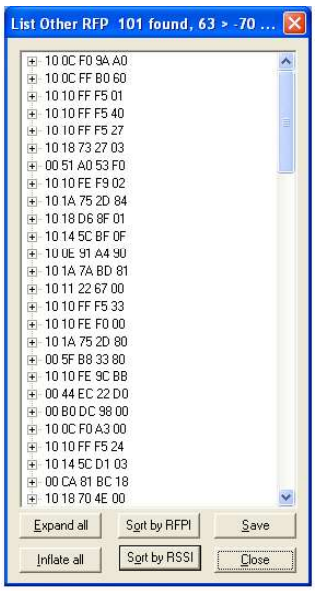
The data of a telephone are displayed in a dialog box after clicking on the respective telephone field in the FP table.

The **Sync Info** child window contains all IP DECT base stations and shows their synchronization and relation states to each other. Selecting the IP DECT base stations with the right mouse button, the user can change visibility views and can even force a resynchronization of an IP DECT base station.

There are several optional child windows selectable. They are all listed below and give some more information about the SIP-DECT systems. Mostly they are statistics and for internal use only.




Event Counter
Counter
Value
Transaction established 3
Transaction released 0
Handover situations 0
PP not found 0
Paging started 1
Release from PP 0
PP_setup rejected 0
Location Registration 0
Detach 0
Location Update 0
Enrolment 0
failed Enrolment 0
FP state 2
FP error 0
ADLC info 0
other messages 0
Copy
Save all
Save Selected
Close


List Other RFP 101 found, 63 > -70 ...
10 0C F0 9A A0
10 0C FF B0 60
10 10 FF F5 01
10 10 FF F5 40
10 10 FF F5 27
10 18 73 27 03
00 51 A0 53 F0
10 10 FE F9 02
10 1A 75 2D 84
10 18 D6 8F 01
10 14 5C BF 0F
10 0E 91 A4 90
10 1A 7A BD 81
10 11 22 67 00
10 10 FF F5 33
10 10 FE F0 00
10 1A 75 2D 80
00 5F B8 33 80
10 10 FE 9C BB
00 44 EC 22 D0
00 B0 DC 98 00
10 0C F0 A3 00
10 10 FF F5 24
10 14 5C D1 03
00 CA 81 BC 18
10 18 70 4E 00
Expand all
Sort by RFPI
Save
Inflate all
Sort by RSSI
Close

10 REGULATORY COMPLIANCE AND SAFETY INFORMATION (4TH GENERATION DECT BASE STATIONS)

For regulatory and basic installation guidelines necessary for the proper and safe functioning of this equipment, refer to the Safety Instructions (document part number **5701204601RA**) packaged with the system and posted on the eDocs web site (http://edocs.mitel.com/).

Read and follow all information contained in the Safety Instructions document before attempting to install or use Mitel products. Only trained, qualified service personnel shall install or maintain Mitel products.

11 SAFETY INFORMATION (3RD GENERATION DECT BASE STATIONS)

11.1 CE MARKING

This certifies the conformity of the product placed on the market prior to June 13th 2017 with the regulations which apply in accordance with the RTTE Directive 1999/5/EC.

For a copy of the original signed declaration (in full conformance with EN45014), contact the Regulatory Approvals Manager at Mitel Networks Ltd., Castlegate Business Park, Portskewett, Monmouthshire, NP26 5Yr, United Kingdom, or visit http://www.mitel.com/regulatory-declarations.

On or after June 13th 2017 hereby, Mitel Networks declares that the product is in compliance with Directive 2014/53/EU. The full text of the EU declaration of conformity is available at the following internet address: http://www.mitel.com/regulatory-declarations.

11.2 COMMUNICATIONS REGULATION INFORMATION

The regulation information in this section applies to the following supported DECT base stations:

- RFP 32 IP
- RFP 34 IP
- RFP 35 IP
- RFP 36 IP
- RFP 37 DRC

11.2.1 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.

11.3 HEALTH AND SAFETY

11.3.1 EXPOSURE TO RADIO FREQUENCY (RF) SIGNALS:

The wireless phone is a radio transmitter and receiver. It is designed and manufactured not to exceed the emission limits for exposure to radio frequency (RF) energy set by the Federal Communications Commission (FCC) of the U.S. Government. These limits are part of comprehensive guidelines and establish permitted levels of RF energy for the general population. The guidelines are based on the safety standards previously set by both U.S. and international standards bodies. These standards include a substantial safety margin designed to assure the safety of all persons, regardless of age and health.

This device and its antenna must not be co-located or operating in conjunction with any other antenna or transmitter.

The radiating element of the RFP should be installed during operating at a separation distance greater than 20 cm between user and device. The device complies with the requirements for routine evaluation limits.

11.3.2 INDUSTRY CANADA (CANADA ONLY)

Operation of this device is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.

Privacy of communications may not be ensured when using this telephone.

Exposure to Radio Frequency (RF) Signals:

The wireless phone is a radio transmitter and receiver. It is designed and manufactured not to exceed the emission limit for exposure to radio frequency (RF) energy set by the Ministry of Health (Canada), Safety Code 6. These limits are part of comprehensive guidelines and established permitted levels of RF energy for the general population. These guidelines are based on the safety standards previously set by international standard bodies. These standards include a substantial safety margin designed to assure the safety of all persons, regardless of age and health.

This device and its antenna must not be co-located or operating in conjunction with any other antenna or transmitter.

The radiating element of the RFP should be installed during operating at a separation distance greater than 20 cm between user and device. This device complies with the requirements for routine evaluation limits.

11.4 INFORMATIONS RÉGLEMENTAIRES EN MATIÈRE DE COMMUNICATIONS

Les informations dans cette section concerne les suivantes stations radio :

- RFP 32 IP
- RFP 34 IP
- RFP 35 IP
- RFP 36 IP
- RFP 37 DRC

11.4.1 NOTES FCC (USA UNIQUEMENT)

Cet appareil est conforme à la partie 15 des règles FCC. Son exploitation est soumise aux deux conditions suivantes: (1) Cet appareil ne doit causer aucune interférence dommageable et (2) cet appareil doit tolérer toute interférence reçue à l'inclusion des interférences susceptibles de causer une opération non désirée. Les modifications non expressément agrées par cette entreprise pourraient rendre caduque l'habilitation de l'utilisateur à exploiter cet équipement.

NOTA: Cet équipement a été testé et jugé conforme aux limitations pour un appareil numérique de classe B en vertu de la partie 15 des règles FCC. Ces limitations ont été conçues pour garantir une protection raisonnable contre les interférences dommageables dans les installations résidentielles. Cet équipement génère, utilise et peut rayonner des ondes radio et peut causer des interférences dommageables dans les communications par radio s'il n'est pas installé et utilisé conformément aux instructions. Cependant, l'absence d'interférences dans une installation particulière n'est pas garantie. Si cet équipement perturbe de façon importante la réception de la radio ou de la télévision (interférences qui peuvent être déterminées en arrêtant et en remettrant l'appareil en marche), l'utilisateur est invité à tenter de corriger les interférences en prenant une ou plusieurs des mesures suivantes:

- Réorienter ou déplacer l'antenne de réception.
- Éloigner l'équipement du récepteur.
- Raccorder l'équipement à une prise d'un circuit différent de celui auquel est raccordé le récepteur.
- Consulter le revendeur ou un technicien radio/TV.

12 APPENDIX

This Appendix contains additional information and examples for configuring your SIP-DECT system.

12.1 PRE-CONFIGURATION FILE RULES

The following file format description can be used to administrate the RFP and DECT phone configuration with external applications, e.g. an external configuration management tool or a PBX communications system.

The framework of the text file follows strictly defined rules. The main framework is divided in two parts:

1 An **instruction section** is used to drive a generic data creation for those fields not filled within data sequence section.

2 A data sequence section defines data record fields. Each of them is explicitly set.

Layout rules in detail are:

- Comments start with “#”.
- Each record is terminated by the regular expressions “\r” or “\n”.
- Instruction settings are made like: <tag> = <value>.
- Data sequence sections start with the key word “data_sequence”. This key word is **mandatory** for file processing to proceed. All instructions must be written before this row.
- Data sequence record fields are separated by colon “;”. Colons have also to be set for empty fields if at least one follows which is not empty. Otherwise a position mismatch of fields will occur.
- If fields have several values assigned (that may be true for a few local RFP configuration fields like “ntp_address”), they must be separated by comma “,”.

Notes:

- Because data sequence fields are separated by a colon, the content of that section can be generated by a *.csv export of Excel Sheet and copied into the configuration file.
- Instructions are only processed on those fields that are left empty within the data sequence section.

12.2 DECT PHONE CONFIGURATION FILE (OMM DATABASE)

12.2.1 SUPPORTED INSTRUCTIONS

Instruction	Explanation
start_number	Numbers can be generated automatically. This instruction defines the start value.
no_of_number	If “start_number” is given, this instruction defines the maximum of numbers which are generated.
ac (authentication code)	If set to “number”, “ac” will be equal to number.

additional_pin	If a value is advised, it will be taken as a start number which will be increased for each new record.
sip_user	
sip_pw	
sos_number	If these instructions are set, the value will be taken as default value for the empty corresponding field within the data sequence section records. SOS/Mandown denote the user specific numbers. The Locatable, Localization, and Tracking flags are ignored by Web import.
mandown_number	
locatable	
localization	
tracking	

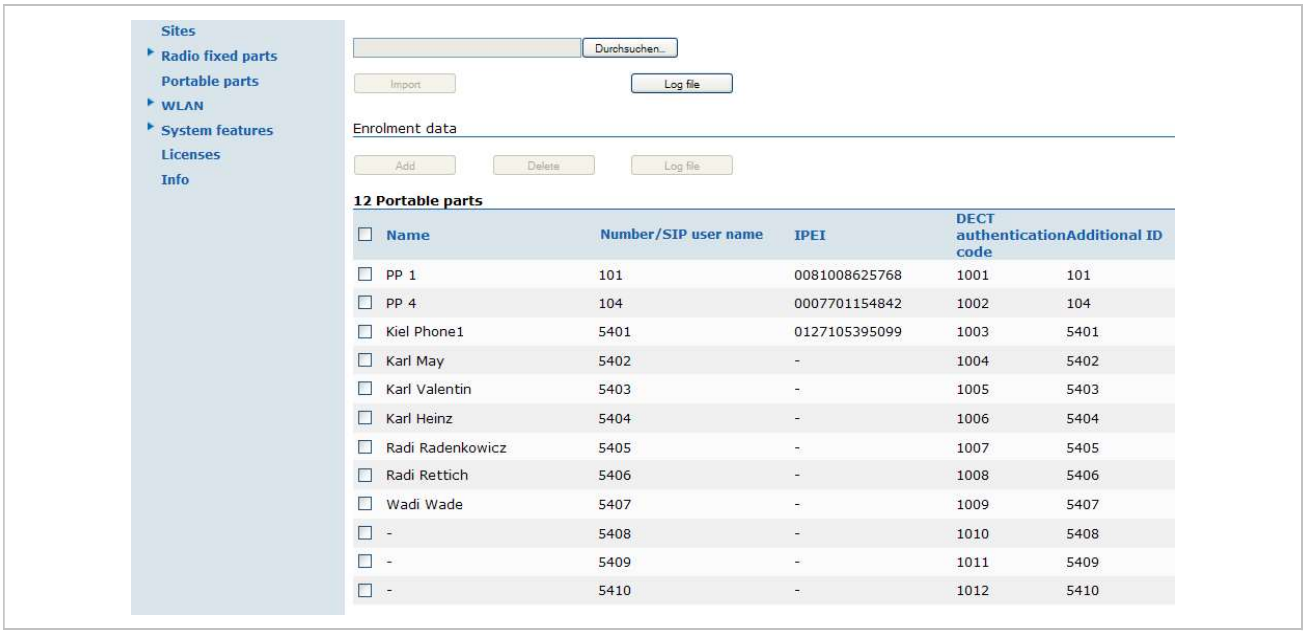
12.2.2 DATA SECTION FIELDS

The data section contains the following field order:

1 Number
2 Name
3 AC
4 IPEI
5 Additional ID
6 Sip user name
7 Sip password
8 SOS number
9 Mandown number
10 Locatable (ignored by Web import and always set to “inactive”)
11 Localization (ignored by Web import and always set to “inactive”)
12 Tracking (ignored by Web import and always set to “inactive”)
13 Description1 (ignored by Web import and always set to “”)
14 Description2 (ignored by Web import and always set to “”)

12.2.3 EXAMPLE

The following screen shot shows a DECT phone configuration. This corresponds to the given configuration file.



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

DECT phone configuration file:

```
# ------------------------#
# instruction section:
# ------------------------#
# -- start_number    = {<start value for numbers to be generated>}
# -- no_of_number    = {<maximum of generated numbers>}
# -- ac   = {<""number"">, <start value for ac's to be generated>}
# -- additional_pin = {<""number"">, <start value for id's >}
# -- sip_user       = {<""number"">, <start value for id's >}
# -- SIP password    = {<""number"">, <start value for id's >}
# -- SOS number      = {<common default>)
# -- Mandown number
# -- Locatable (ignored by Web import and always set to inactive)
# -- Localization (ignored by Web import and always set to inactive)
# -- Tracking (ignored by Web import and always set to inactive)

start_number = 5401
no_of_number = 10
ac  = 1001
additional_pin = number
sip_user = number
sip_pw = number
```

```
sos_number=5002
mandown_number=5002

# ---------------------#
# data sequence:
# ---------------------#
# 1. number
# 2. name
# 3. AC
# 4. IPEI
# 5. additionalId
# 6. SIP user
# 7. SIP password
# 8. sos no
# 9. mandown no
# 10. locatable (ignored by Web import and always set to inactive)
# 11. localization (ignored by Web import and always set to inactive)
# 12. tracking (ignored by Web import and always set to inactive)
# 13. descr1 (ignored by Web import and always set to "")
# 14. descr2 (ignored by Web import and always set to "")
data_sequence;;;;;;;;;;;;
# 1. number;2. name;3. AC;4. IPEI ;5. additionalId;6. SIP user;7. SIP password;8. sos
no;9. mandown no;10. locatable;11. localization;12. tracking;13. descr1;14. descr2
101;DECT phone 1;;0081008625768;;;;;;;;;
104;DECT phone 4;;0007701154842;;;;;;;;;
;Kiel Phone1;;0127105395099;5401;5401;5401;30;30;;;;;
;Karl May;;;;;;;;;;;;
;Karl Valentin;;;;;;;;;;;;
;Karl Heinz;;;;;;;;;;;;
;Radi Radenkowicz;;;;;;;;;;;;
;Radi Rettich;;;;;;;;;;;;
;Wadi Wade;;;;;;;;;;;;
```

Parse log about import / instruction processing

```
OK: start_number = 5401
OK: ac = 1001
OK: additional_pin = number
OK: sip_user = number
OK: sip_pw = number
OK: sos_number = 5002
OK: mandown_number = 5002
```

```
OK: no_of_number = 10

Section processing:
```

[…]

12.3 RFP CONFIGURATION FILE / CENTRAL (OMM DATABASE)

You can import of DECT base station configurations using files via the OMP.

12.3.1.1 Supported Instructions

All instructions are taken as a common value and are applied to all records in the data sequence section of that file if the corresponding field is empty.

Instruction	Explanation
active	Activation of DECT: {‘0’ or ‘false ’= inactive, ‘1’ or ‘true’ = active }
cluster	Cluster, the RFP is referred to - RFP-OMM: {1..256}, PC-OMM: {1..4096}
paging_area	Paging area, the RFP is referred to: {‘unassigned, ’0’..’127’} Ignored by WEB import and always set to ‘0’ (Paging area 0)
sync_source	Synchronization source: {‘0’ or ‘false ’= inactive, ‘1’ or ‘true’ = active }
refl_env	Reflective environment: {‘0’ or ‘false ’= no, ‘1’ or ‘true’ = yes }
site	Site Id: {1..250}
wlan_profile	Reference key to an existing WLAN profile
wlan_antenna	Antenna settings: {0=diversity, 1, 2}
wlan_channel_bg	WLAN channel: {0..14 (size depends on regulatory domain) }
wlan_power	WLAN power: {6, 12, 25, 50,100 (in percent)}
wlan_act	Activation of WLAN: {‘0’ or ‘false ’= inactive, ‘1’ or ‘true’ = active }

12.3.1.2 Data Section Fields

The data section contains the following field order:

1 MAC address
2 Name
3 DECT activated
4 DECT cluster
5 Paging area (always set to “0”, PA0)
6 Preferred sync.
7 Reflective env.
8 Site ID (if left empty then set to the lowest Site ID)
9 Building (ignored by Web import and always set to “”)
10 Floor (ignored by Web import and always set to “”)
11 Room (ignored by Web import and always set to “”)
12 WLAN profile
13 WLAN antenna
14 WLAN channel
15 WLAN power
16 WLAN activated

12.3.1.3 Example

The following figure shows the results of a DECT base station enrolment operation via the OMP **DECT base stations** -> **Enrolment** page.

RFP configuration file/central:

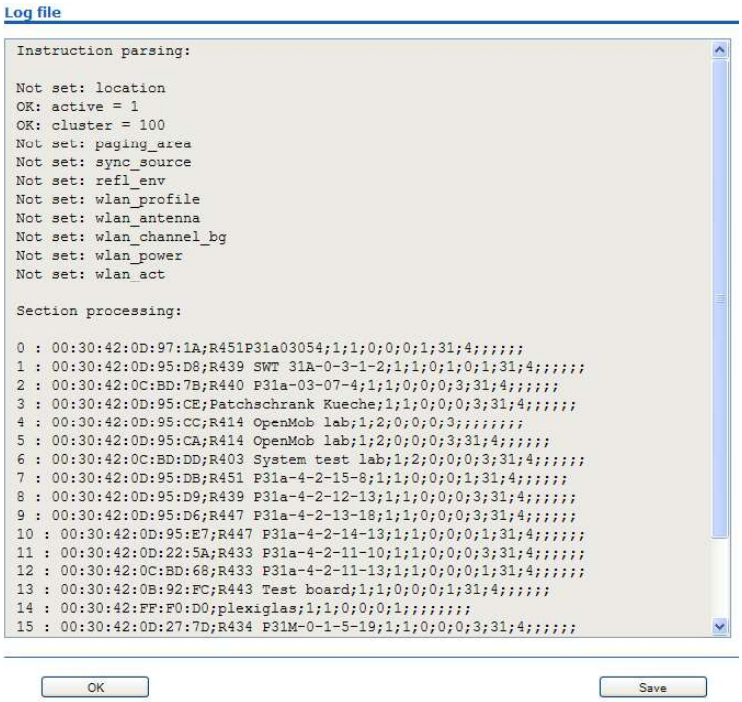
```
###############################################################################
# instruction section:
###############################################################################
#active
#               Activation of DECT:
#               {'0' or 'false '= inactive, '1' or 'true' = active}
#cluster
#               Cluster, the RFP is referred to:
#               {1..256} (RFP OMM) or {1..4096} (PC OMM)
#paging_area
#               Ignored by Web import and always set to "0" (PA0)
#               Paging area, the RFP is referred to: {'unassigned, '0'..'127'}
#sync_source
#               Synchronisation source:
#               '0' or 'false '= inactive, '1' or 'true' = active}
#refl_env
#               Reflective environment:
#               '0' or 'false '= no, '1' or 'true' = yes}
#site
#               Site Id: {1..250}
#wlan_profile
#               Reference key to an existing WLAN profile
#wlan_antenna
#               Antenna settings: {0=diversity, 1, 2}
```

```
#wlan_channel_bg
#               WLAN channel: {0..14 (size depends on regulatory domain) }
#wlan_power
#               WLAN power = { 6, 12, 25, 50,100 (in percent)}
#wlan_act
#               Activation of  WLAN:
#               '0' or 'false '= inactive, '1' or 'true' = active}
#Note: Web import allows only "0" or "1" for Boolean
################################################################################

active=1
cluster=100
refl_evc=1
site=1

################################################################################
data_sequence
################################################################################
#MAC address;Name;DECT activated;DECT cluster;Paging area;Preferred sync.;
#Reflective env.;Site ID;Building;Floor;Room;WLAN profile;WLAN antenna;
#WLAN channel;WLAN power;WLAN activated
00:30:42:0D:97:1A;R451P31a03054;1;1;0;0;0;1;31;4;;;;;;
00:30:42:0D:95:D8;R439 SWT 31A-0-3-1-2;1;1;0;1;0;1;31;4;;;;;;
00:30:42:0C:BD:7B;R440 P31a-03-07-4;1;1;0;0;0;3;31;4
00:30:42:0D:95:CE;Patchschrank Kueche;1;1;0;0;0;3;31;4
00:30:42:0D:95:CC;R414 OpenMob lab;1;2;0;0;0;3;;
00:30:42:0D:95:CA;R414 OpenMob lab;1;2;0;0;0;3;31;4
00:30:42:0C:BD:DD;R403 System test lab;1;2;0;0;0;3;31;4
00:30:42:0D:95:DB;R451 P31a-4-2-15-8;1;1;0;0;0;1;31;4
00:30:42:0D:95:D9;R439 P31a-4-2-12-13;1;1;0;0;0;3;31;4
00:30:42:0D:95:D6;R447 P31a-4-2-13-18;1;1;0;0;0;3;31;4
00:30:42:0D:95:E7;R447 P31a-4-2-14-13;1;1;0;0;0;1;31;4
00:30:42:0D:22:5A;R433 P31a-4-2-11-10;1;1;0;0;0;3;31;4
00:30:42:0C:BD:68;R433 P31a-4-2-11-13;1;1;0;0;0;1;31;4
00:30:42:0B:92:FC;R443 Test board;1;1;0;0;0;1;31;4
00:30:42:FF:F0:D0;plexiglas;1;1;0;0;0;1;;
00:30:42:0D:27:7D;R434 P31M-0-1-5-19;1;1;0;0;0;3;31;4
00:30:42:0A:C9:62;R439 Decke re.;1;1;0;0;0;1;;
00:30:42:0D:E3:F6;R436 Wand oben ln;1;1;0;0;0;1;;
00:30:42:08:31:5F;R434 Decke ln. Tür;1;1;0;0;0;1
00:30:42:08:31:64;R440  Decke re Fnstr;1;1;0;0;0;1
```

Parse log about import / instruction processing



12.3.2 RFP CONFIGURATION FILE / LOCAL (OM CONFIGURATOR)

12.3.2.1 Supported Instructions

All instructions are taken as a common value and are applied to all records in the data sequence section of that file if the corresponding field is empty.

Instruction	Explanation
active	Local configuration active: {0=inactive(use DHCP instead), 1=active}
net_mask	Net mask
tftp_server	IP address of TFTP server
tftp_file	Path and name of boot file
omm_1	OMM IP address
omm_2	IP address of backup OMM
gateway	Default gateway
dns_server	Up to two DNS server IP addresses
dns_domain	local DNS domain
syslog_addr	IP address of syslog daemon
syslog_port	Listen port of syslog daemon
use_vlan	VLAN is enabled

Instruction	Explanation
srvlst	List of further tftp server
broadcast_addr	local broadcast address
vlan_id	VLAN Id
preferred_tftp	tftp_server is preferred
config_file_server	configuration server

12.3.2.2 Data Section Fields

The data section contains the following field order:

1. MAC address of RFP
2. Local configuration active flag
3. IP address of RFP
4. Net mask
5. TFTP server
6. TFTP_FILE
7. OMM IP address
8. IP address of backup OMM
9. Default gateway
10. DNS server
11. DNS domain
12. Syslog daemon IP address
13. Syslog listen port
14. Use VLAN
15. Server list
16. Broadcast address
17. VLAN Id
18. Preferred TFTP server
19. Configuration file server

12.3.2.3 Example

RFP configuration file/local (OM Configurator):

```
# --------------------#
# instruction section #
# --------------------#

active     = 1
net_mask   = 255.255.0.0
tftp_server= 172.30.200.92
tftp_file  = iprfp2G.tftp
```

```
omm_1      = 172.30.111.188
omm_2      = 172.30.11.181
gateway    = 172.30.0.2
dns_server = 172.30.0.4,172.30.0.21
dns_domain = aastra.de
syslog_addr= 172.30.200.92
use_vlan = 1
srvlist = 172.30.0.4,172.30.0.21
broadcast_addr = 172.30.255.255
vlan_id = 4
preferred_tftp = 1
config_file_server = https://server/configfiles/

# --------------#
# data sequence #
# --------------#
# 1. MAC_ADDR           ! no instruction supported !
# 2. ACTIVE_FLAG
# 3. RFPADDR            ! no instruction supported !
# 4. NET_MASK
# 5. TFTP_SERVER
# 6. TFTP_FILE
# 7. OMM1
# 8. OMM2
# 9. GATEWAY
#10. DNS_SERVER
#11. DNS_DOMAIN
#12. SYSLOG_ADDR
#13. SYSLOG_PORT
#14. USE_VLAN
#15. SRVLIST
#16. BROADCAST_ADDR
#17. VLAN_ID
#18. PREFERRED_TFTP
#19. CONFIG_FILE_SERVER

data_sequence
00-30-42-01-01-01;;172.30.111.1
00-30-42-02-02-02;;172.30.111.2
```

Parse log for import / instruction processing

```
ok: active = 1
ok: net_mask = 255.255.0.0
ok: tftp_server = 172.30.200.92
ok: tftp_file = iprfp2G.tftp
ok: omm_1 = 172.30.111.188
ok: omm_2 = 172.30.11.181
ok: gateway = 172.30.0.2
ok: dns_server = 172.30.0.4,172.30.0.21
ok: dns_domain = mitel.com
ok: syslog_addr = 172.30.200.92
not set: syslog_port
ok: use_vlan = 1
ok: srvlist = 172.30.0.4,172.30.0.21
ok: broadcast_addr = 172.30.255.255
ok: vlan_id = 4
ok: preferred_tftp = 1
ok: config_file_server = https://server/configfiles/

:parsing ok:

processing of section: data_sequence

[…]

create data:

[…]

RFP configuration:

[…]
```

12.4 RFP EXPORT FILE FORMAT

General

RFP export files are created by OMM Management Portal in ‘csv’-file format which can be easily viewed by a spreadsheet application. Export file contains all or a part of the following parameters:

- MAC address
- Location name
- DECT active
- Cluster
- Paging area
- Synchronization source
- Reflective environment
- Site
- Building
- Floor
- Room
- WLAN profile reference
- WLAN antenna
- WLAN Channel_bg
- WLAN power
- WLAN active

Example

Following example RFP export file contains all exportable RFP parameters and is re-importable by OMM Management Portal.

```
################################################
# RFP data export file: '/home/user/example.csv'
# Date: 24.09.10  Time: 15:58:19
################################################
#
# Exported parameters:
#
# MAC address
# Name
# DECT activated
# DECT cluster
# Paging area
# Preferred sync.
# Reflective env.
# Site ID
# Building
# Floor
```

```
# Room
# WLAN profile
# WLAN antenna
# WLAN channel
# WLAN power
# WLAN activated
#
################################################


MAC address;Name;DECT activated;DECT cluster;Paging area;Preferred sync.;Reflective
env.;Site ID;Building;Floor;Room;WLAN profile;WLAN antenna;WLAN channel;WLAN power;WLAN
activated


data_sequence


00:30:42:0E:71:41;License RFP 1;
true;1;0;false;true;1;B1;F1;R1;1;0;;100;false


00:30:42:0E:26:F1;License RFP 2;
true;1;0;false;false;1;B1;F2;R1;1;0;;100;false


00:30:42:0E:75:59;License RFP 3;
true;1;0;true;false;1;B1;F2;R2;1;0;;100;false
```

12.5 COA CONFIGURATION PARAMETERS

In addition to the information provided in section 8.23, the following sections provide examples of a CoA configuration files, and an overview of all supported parameters.

12.5.1 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
```

12.5.2 EXTENDED COA EXAMPLES

12.5.3 EXAMPLE 1

```
UD_ConfigurationName="Umlaute (UTF-8): äöüÄÖÜß, Escape-Sequenzen: ' \" \\ \r \n \t \f,
andere UTF-8-Zeichen: µ ® €"

# display-einstellungen
UD_DispLang=en
UD_DispFont=large
UD_DispColor=black

# ringer-einstellungen
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
```

12.5.4 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
```

12.5.5 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
```

12.5.6 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'
```

12.5.7 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
```

12.5.8 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
```

12.6 PROTOCOLS AND PORTS

Protocol		OpenMobility Manager	
		Server port	Client port
HTTPS server	tcp server	443 or as configured	any
HTTP server (redirect to https)	tcp server	80 or as configured	any
HTTP/HTTPS client for the SIP-DECT XML terminal interface	tcp	80/443	> 1024
RFP control protocol	tcp server	16321	any
OMM Standby	tcp server	16322	any
OM AXI	tcp server	12622	any
DECTnet monitor	tcp server	8106	any
LDAP	tcp client	389 or as configured	>=1024 (see note)
TFTP client	udp	69 / given by server	>=1024 (see note)
HTTP client	tcp	80 or as configured	>=1024 (see note)
HTTPS client	tcp	443 or as configured	>=1024 (see note)
explicit FTPS client	tcp	21 or as configured	>=1024 (see note)
implicit FTPS client	tcp	990 or as configured	>=1024 (see note)
OM AXI server TCP	tcp server	12621	Any
OM AXI server TLS	tcp server	12622	Any
SIP	udp	5060	as configured
Integrated Conference Server (ICS)	udp	5062	as configured
Telnet (OMM console, Linux server based OMM only)	tcp server	localhost 8107	localhost any

Note: Unbound ports start at port 1024.

Protocol		IP-RFP	
		Server port	Client port
HTTP/HTTPS client for the SIP-DECT XML terminal interface	tcp	80/443	> 1024
RFP control protocol	tcp client	16321	>=1024 (see note)
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)

Protocol		IP-RFP	
		Server port	**Client port**
OMCFG server	udp	64000	64000
NTP client	udp	123	123
Syslog client	udp	514 or as configured	514
DNS client	udp	53	>=1024 (see note)
SNMP agent (server)	udp	161	Any
SNMP trap agent (client)	udp	>=1024 (see note)	162
RSXport (debug only)	tcp server	38477	Any
RTP/RTCP (server)	udp	Range of [RTP port base + 71] even ports for RTP, odd ports for RTCP. Port base is 16320 or as configured.	Any
RTP/RTCP (client)	udp	any	Range of [RTP port base + 71] even ports for RTP, odd ports for RTCP. Port base is 16320 or as configured.
Integrated Conference Server (ICS) RTP/RTCP (server)		Range of [ICS RTP port base + 2 * no. conf. channels] even ports for RTP, odd ports for RTCP. ICS Port base is end of RTP range plus 1.	Any
Integrated Conference Server (ICS) RTP/RTCP (client)		any	Range of [ICS RTP port base + 2 * no. conf. channels] even ports for RTP, odd ports for RTCP. ICS Port base is end of RTP range plus 1.
Network Analysis Probe	tcp server	18215	Any

Note: Unbound ports start at port 1024.

12.7 ABBREVIATIONS

AC	Authentication Code
ADPCM	Adaptive Differential Pulse Code Modulation
COA	Configuration Over Air
DECT	Digital Enhanced Cordless Telecommunication
DHCP	Dynamic Host Configuration Protocol
DSP	Digital Signal Processor
FCC	Federal Communications Commission
GAP	Generic Access Profile
IMA	Integrated Messaging and Alerting Service
IPBX	IP PBX, a telephony system using IP / VoIP
IPEI	International Portable Equipment Identity
OM	OpenMobility
OM AXI	OM Application XML Interface
OMC	OM Configurator
OML	OM Locating
OMM	OpenMobility Manager
OMP	OM Management Portal
PARK	Portable Access Rights Key
PBX	Private Branch Exchange, a customer premises telephony system
PP	Portable Part (DECT phone or device)
RCS	Redirection and Configuration Service
RFP	Radio Fixed Part (DECT base station)
RTCP	Real Time Control Protocol
RTP	Real Time Protocol
TFTP	Trivial File Transfer Protocol

12.8 DEFINITIONS

Asterisk	Asterisk is a complete Open Source PBX in software. It runs on Linux, BSD and MacOSX and provides many features. Asterisk supports voice over IP in many protocols, and can interoperate with almost all standards-based telephony equipment.
Base station	Please see: RFP or Radio Fixed Part
DECT	**D**igital **E**nhanced **C**ordless **T**elecommunication The standard (ETS 300 175) essentially specifies the air interface, known as the radio interface. Voice and data can both be transmitted via this interface. Its technical key characteristics for Europe are: Frequency range: Approx. 1880 – 1900 MHz (approximately 20 MHz bandwidth) 10 carrier frequencies (1728 kHz spacing) with 12 time slots each Doubling the number of time slots (to 24) using the TDMA process Net data rate per channel of 32 kbps (for voice transmission using ADPCM) Voice coding using the ADPCM method Its technical key characteristics for North American are: Frequency range: Approx. 1920 – 1930 MHz (approximately 10 MHz bandwidth) 5 carrier frequencies (1728 kHz spacing) with 12 time slots each) Doubling the number of time slots (to 24) using the TDMA process Net data rate per channel of 32 kbps (for voice transmission using ADPCM) Voice coding using the ADPCM method
GAP	**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 in order to allow telephones of different vendors to be used on any type of DECT system. It thus represents the smallest common denominator of all manufacturer-specific variants of the DECT standard. An important limitation in the GAP standard is that external handover is not possible. For this reason connection handover is used, which is supported by GAP terminals. The operation of GAP-capable telephones is comparable to that of analogue terminals. For example, features can be called up via '*' and '#' procedures.
Handover	A handover is similar to roaming, but occurs during an ongoing call. A handover normally takes place "in the background", without disrupting the call (seamless handover).
IPEI	**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. This code is globally unique.

PARK	**P**ortable **A**ccess **R**ights **K**ey Access code for the Portable Part. This code determines whether a DECT phone can access a particular DECT system. Used for unique selection of a dedicated the system from a DECT phone at enrolment/subscription time. Provided via the PARK online service and unique to each SIP-DECT deployment.
Radio Fixed Part (RFP)	An RFP provides a DECT radio cell and terminates the radio link from the portable DECT device. One or more RFPs build the area of radio coverage.
Roaming	While in motion, the DECT phone performs ongoing measurements to determine which RFP is best received. The one that can be best received is defined as the active RFP. To prevent the DECT phone from rapidly switching back and forth between two RFPs that have similar signal strength, certain threshold values are in effect.

12.9 REFERENCES

/1/ RFC 1350, The TFTP Protocol, Revision 2, July 1992

/2/ RFC 2090, TFTP Multicast Option, February 1997

/3/ RFC 2347, TFTP Option Extension, May 1998

/4/ RFC 2348, TFTP Block size Option, May 1998

/5/ RFC 2349, TFTP Timeout Interval and Transfer Size Options, May 1998

/6/ RFC 2236, Internet Group Management Protocol, Version 2, November 1997

/7/ RFC 1889, RTP: A Transport Protocol for Real-Time Applications, January 1996

/8/ RFC 2030, Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI, October 1996

/9/ RFC 2131, Dynamic Host Configuration Protocol, March 1997

/10/ RFC 2327, SDP: Session Description Protocol, April 1998

/11/ RFC 2474, Definition of the Differentiated Service Field (DS Field) in the IPv4 and IPv6 Headers, December 1998

/12/ RFC 2617, HTTP Authentication: Basic and Digest Access Authentication, June 1999

/13/ RFC 3164, The BSD Sys Log Protocol, August 2001

/14/ RFC 2833, RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals, May 2000

/15/ RFC 3261, Session Initiation Protocol (SIP), June 2002

/16/ RFC 3264, An Offer/Answer Model with Session Description Protocol (SDP), June 2002

/17/ RFC 3326, The Reason Header Field for SIP, December 2002

/18/ RFC 3420, Internet Media Type message/sipfrag, November 2002

/19/ RFC 3515, The Session Initiation Protocol (SIP) Refer method, April 2003

/20/ RFC 3665, The Session Initiation Protocol (SIP) Basic Call Flow Examples, December 2003

/21/ RFC 3842, A Message Summary and Message Waiting Indication Event Package for the Session Initiation Protocol (SIP), August 2004

/22/ RFC 3891, The Session Initiation Protocol (SIP) “Replaces” Header, September 2004

/23/ RFC 3892, The Session Initiation Protocol (SIP) Referred-By Mechanism, September 2004

/24/ RFC 4566, SDP: Session Description Protocol

/25/ RFC 5806, Diversion Indication in SIP, March 2010

/26/ Compendium “OpenMobility SIP-DECT 4.0 Solution; Installation & Administration”

/27/ SIP-DECT; OM Locating Application; Installation, Administration & User Guide

/28/ SIP-DECT; OM Integrated Messaging & Alerting Application; Installation, Administration & User Guide

/29/ SIP-DECT; OM Handset Sharing & Provisioning; User Guide

/30/ SIP-DECT; OM User Monitoring; User Guide

/31/ SIP-DECT; Mitel 600 ; Messaging & Alerting Applications; User Guide

/32/ Mitel 600 series SIP-DECT User’s Guide

/33/ aad-0384 SIP_DECT OM Application XML Interface

/34/ RFC 2782, A DNS RR for specifying the location of services (DNS SRV)

/35/ RFC 3262, Reliability of Provisional Responses in the Session Initiation Protocol (SIP)

/36/ RFC 3311, The Session Initiation Protocol (SIP) UPDATE Method

/37/ req-0175 SIP-DECT XMLTerminal Interface for Mitel 600 DECT Phone Family
/38/ RFC 4579, Session Initiation Protocol (SIP) Call Control - Conferencing for User Agents
/39/ RFC 5589, Session Initiation Protocol (SIP) Call Control – Transfer
/40/ RFC 2246, The TLS Protocol Version 1.0
/41/ RFC 2459, Internet X.509 Public Key Infrastructure certificate
/42/ RFC 3711, The Secure Real-Time Transport Protocol (SRTP)
/43/ RFC 4346, The Transport Layer Security (TLS) Protocol Version 1.1
/44/ RFC 4568, Session Description Protocol (SDP); Security Description for Media Streams
/45/ RFC 5246, The Transport Layer Security (TLS) Protocol Version 1.2
/46/ RFC 5630, The Use of the SIPS URI Scheme in the Session Initiation Protocol (SIP)
/47/ SIP-DECT_LinuxServerInstallation