

- **USB overload:** Number of connected RFPs detecting overload at their USB port
- **Encryption not supported:** Number of connected RFPs not supporting encryption
- **Advanced features not supported:** Number of connected RFPs not supporting "Advanced features" which covers "Hi-Q audio technology", "Terminal video", "Enhanced DECT security" and "SRTP".

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

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

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

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

6.4.3 USERS

The "Users" tab provides information about DECT phone users.

Overview

DECT base stations

Users

Devices

Sites

Conference

Video devices

General

Total

SIP registered

4

Monitored active

0

Monitored passive

0

Sending messages permission

0

DECT locatable

0

User monitoring states

Warning

0

Unavailable

0

Escalated

0

Number for visibility checks

Number/SIP user name

25052

- The "General" panel provides counters concerning DECT phones user configuration and states:
- **Total:** Total number of configured users
 - **SIP registered:** Number of configured users registered at SIP server
 - **Monitored active:** Number of configured users with active monitoring enabled

- **Monitored passive:** Number of configured users with passive monitoring enabled
 - **Sending messages permission:** Number of configured users with message sending permission enabled
 - **DECT locatable:** Number of configured users with DECT locatable enabled
- The "User monitoring states" panel provides counters concerning DECT phone user monitoring state

- **Warning:** Number of monitored users in state 'Warning'
 - **Unavailable:** Number of monitored users in state 'Unavailable'
 - **Escalated:** Number of monitored users in state 'Escalated'
- The "Number for visibility checks" panel provides phone number or SIP user name used for standby OMM visibility checks.

6.4.4 DEVICES

The "Devices" tab provides information about DECT phones.

Overview

DECT base stations

Users

Devices

Sites

Conference

Video devices

General

Total

4

Subscribed

4

Downloading new firmware to portable parts

Status

⬆

Downloading firmware from

http://10.37.18.50/60_ahd

Firmware version

[R00 5.00 SP5 RC1] - [R50.002; 6.0 RC8]

Known downloadable

4

Already updated

4

Waiting for download

0

Currently downloading

0

Barred

0

Download error

0

Unreachable

0

Detached

0

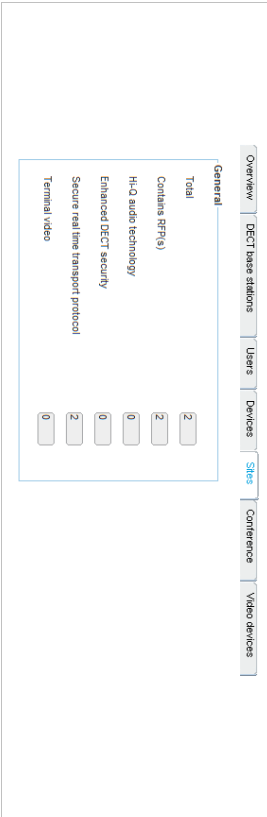
- The "General" panel contains counters related to DECT phones:
- **Total:** Total number of configured DECT phones
 - **Subscribed:** Number of configured DECT phones which are subscribed to OMM
- The "Downloading new firmware to portable parts" panel provides information about state of DECT phone firmware download:

- **Status:** Status of firmware download
- **Loading firmware from:** URL of firmware download container
- **Firmware version:** Version info of firmware container

- **Known downloadable:** Number of DECT phones known as downloadable
- **Already updated:** Number of DECT phones already updated
- **Waiting for download:** Number of DECT phones waiting for download
- **Currently downloading:** Number of DECT phones currently downloading
- **Barred:** Number of downloadable DECT phones currently barred
- **Download error:** Number of downloadable DECT phones with download error
- **Unreachable:** Number of downloadable DECT phones currently unreachable
- **Detached:** Number downloadable DECT phones currently detached

6.4.5 SITES

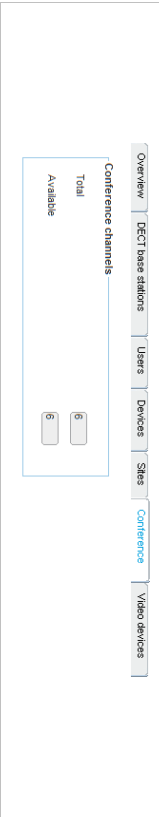
The "Sites" tab provides counters concerning site configuration and state:



- **Total:** Total number of configured sites
- **Contains RFPs:** Number of sites with dedicated RFPs
- **Hi-Q audio technology:** Number of sites with Hi-Q audio technology enabled
- **Enhanced DECT security:** Number of sites with "Enhanced DECT security" enabled
- **Secure real time transport protocol:** Number of sites with "Secure real time transport protocol" (SRTP) enabled
- **Terminal video:** Number of sites with terminal video enabled

6.4.6 CONFERENCE

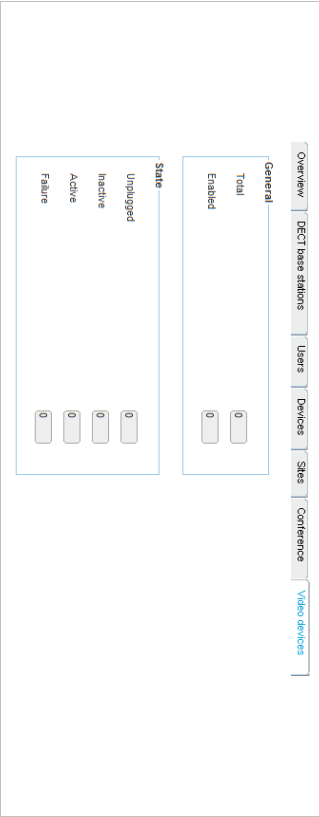
The "Conference" tab provides conference channel information:



- **Total:** Total number of conference channels in system
- **Available:** Number of currently available conference channels

6.4.7 VIDEO DEVICES

The "Video devices" tab provides video device state information.



The "General" panel provides video device configuration related counters:

- **Total:** Total number of configured video devices
- **Checkpoint:** Number of video devices enabled

The "State" panel provides video device state related counters:

- **Unplugged:** Number of video devices in state unplugged
- **Inactive:** Number of video devices in state inactive
- **Active:** Number of video devices in state active
- **Failure:** Number of video devices in state failure

6.5 "SYSTEM" MENU

The **System** menu allows configuration and display of global OMM settings. The system settings are changeable in configuration mode. Change of some parameters can cause the OMM to be reset. In this case a new login is required.

The **System** menu provides the following entries:

Configuration mode	Monitor mode	See section
Basic settings	Basic settings	6.5.1
Advanced settings	Advanced settings	6.5.2
	Statistics	6.5.3
SIP	SIP	6.5.4
User administration	User administration	6.5.6

Data management	Data management	6.5.7
-----------------	-----------------	-------

6.5.1 “BASIC SETTINGS” MENU

The **Basic settings** menu contains general settings for the OpenMobility Manager.

The Basic settings menu contains the following tabs:

- **General** (see section 6.5.1.1)
- **DECT** (see section 6.5.1.2)
- **WLAN** (see section 6.5.1.3)
- **Software update URL** (only on systems where the OMM is running on a DECT base station) (see section 6.5.1.4)

6.5.1.1 General settings

You can set the following parameters on the General tab of the “Basic Settings” menu.

General

- **System name:** Name of the SIP-DECT system.
- **Remote access:** Enables or disables SSH access to all RFPs in the DECT system. For more information on SSH access, see section 8.3.5.
- **Tone scheme:** Specifies the country in which the OMM resides, which enables country-specific tones (e.g., busy tone, dial tone, etc).
- **Time zone:** Specifies the time zone in which the OMM is operating.

Syslog

- **Active:** Enables propagation of syslog messages by the OMM and RFPs.
- **IP address:** Address of the host that collects the syslog messages.
- **Port:** Port of the host that collects the syslog messages.

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

RFP software update

- **Mode:** RFP update mode. Options are “One by one” (each RFP is updated separately) or “All at once” (all RFPs are updated in one operation).
- **Time-controlled:** Indicates whether the start of the RFP update is time-controlled.
- **Time of day:** Specifies the time for time-controlled RFP updates.

Note: Updates triggers can be controlled through update intervals (DHCP, config files) or manually triggered via the **Update** button.

The “General” tab contains two additional buttons (aside from default buttons):

- **Update:** Requests an immediate update of RFP software.
- **Restart:** Requests an OMM restart.

6.5.1.2 DECT settings

For a description of the parameters which can be set in the **DECT** tab, see the description of the **System settings** page of the OMM Web service (see section 5.4.1). The corresponding parameters are described in the **DECT settings** and **Downloading new firmware to portable parts** page sections, with the exceptions noted below.

The following settings are only available in the OMP.

- **Regulatory domain:** The OMP offers an additional regulatory domain selection (Radio 1910-1927MHz 250mW) for SIP-DECT operation in some South American countries. See section 3.11 for more information on this feature.
- **SARI:** Specify the Secondary Access Rights Identifier (SARI) for the Dual Homing feature. DECT phones subscribe to the SARI (instead of the PARK) to ensure that user data is synchronized across all OMMs in the system. See section 7.16 for more information on this feature. You can click the **Generate SARI** button to generate the SARI from the system PARK code.
- **Paging area size:** Select the number of paging areas for the SIP-DECT system. A paging area can consist of up to 256 RFPs (and the smallest group can consist of 16 RFPs). The configuration of the paging areas is done in the **Paging areas** menu of the OMP (see section 6.7.2).
- **Restricted subscription duration:** Restricts the time period throughout which a DECT phone can be subscribed to 2 minutes. Furthermore, the subscription mode will be disabled immediately after every successful subscription of a DECT phone.
- **Auto-create on subscription:** Activate this option if an unbound subscription of DECT phones should be allowed. See the *OM DECT Phone Sharing and Provisioning Guide* for more information.

6.5.1.3 WLAN settings

For a description of the parameters which can be set in the **WLAN** tab, see the description of the **System settings** page of the OMM Web service. The same parameters are described in the **WLAN settings** section (section 5.4.1.3).

6.5.1.4 Software Update URL settings

With SIP-DECT 6.0 or later, DECT base stations in small SIP-DECT systems (~10 RFPs) can obtain their software image from the RFP OMM, if they have no valid URL from which to load their software. If the OMM is running on a RFP, the RFP OMM delivers the software to the connected RFPs. You configure the URL for the RFP software image (iprfp3G.dnld and **iprfp4G.dnld**) on this tab. This tab is only available when the OMM resides on an RFP.

For a description of the parameters that can be set in the **Software update URL** tab, see the description of the **System settings** page of the OMM Web service. The same parameters are described in the **Software update URL** section (section 5.4.1.10).

6.5.2 “ADVANCED SETTINGS” MENU

The **Advanced settings** menu contains additional settings for the OpenMobility Manager.

The **Advanced settings** menu contains the following tabs:

- **Net parameters** (see section 6.5.2.1)
- **DECT phones** (see section 6.5.2.2)
- **DECT phone firmware** (see section 6.5.2.3)
- **OMA** (see section 6.5.2.4)
- **Additional services** (see section 6.5.2.5)
- **User monitoring** (see section 6.5.2.6)
- **Special branding** (see section 6.5.2.7)
- **Core dump** (see section 6.5.2.8)
- **Remote system dump** (see section 6.5.2.9)
- **OMM certificate** (see section 6.5.2.10)
- **OMM certificate server** (see section 6.5.2.11)

6.5.2.1 Net parameters

For a description of the parameters that can be set in the **Net parameters** tab, see the description of the **System settings** page of the OMM Web service. The same parameters are described in the **Net Parameters** section (section 5.4.1.13).

- **SNMP** (see section 6.5.2.12)
- **Time zones** (see section 6.5.2.13)
- **Input format QoS parameter**: Format for quality of service parameter. Available options are ToS or DiffServ.
- **QoS for voice packets**: Specifies the value of the type of service (ToS) or DiffServ byte (depending on the QoS input format value) of the IP packet header for all packets that transport RTP voice streams.
- **QoS for signaling packets**: Specifies the value of the type of service (ToS) or DiffServ byte (depending on the QoS input format value) of the IP packet header for all packets related to VoIP signaling.
- **TTL (Time to live)**: Specifies the maximum hop count for all IP packets.
- **802.1p voice priority**: Specifies the VLAN priority tag for RTP packets.
- **802.1p signaling priority**: Specifies the VLAN priority tag for VoIP signaling packets.

6.5.2.2 DECT Phones

The OMM can set certain start-up text settings on the DECT Phone over the air. For more information on this feature see section 3.13.5.

- **Dial editor supports digits only**: Enables a digits-only mode for the DECT phone dial editor. In this mode, the “*” has the meaning of a digit to be dialed, even if short-pressed. If the mode is not enabled, a short press of the “*” key changes the editor mode to alphanumeric.
- **Set startup window headline**: Enables display of the text string specified in the **Startup window headline** field.
- **Startup window headline**: Text headline to be displayed in the DECT phone window at startup. Default value is “my company”.
- **Set startup window text**: Enables display of the text string specified in the **Startup window text** field.
- **Startup window text**: Text string to be displayed in the DECT phone window at start. Empty by default.
- **Truncate portable part user name**: Enables or disables truncating the name of the user registered to the DECT phone.

6.5.2.3 DECT phones firmware

The OMM can provide a DECT phone firmware update over the air. If the **Activate firmware update** checkbox is enabled, the "Download over Air" feature is activated. For more information on this feature see section 7.22.

For a description of the parameters on the **DECT Phone firmware** tab, see section 5.4.1.6.

6.5.2.4 IMA

The Integrated Message and Alarm (IMA) configuration is stored in the OMM database. You can configure a specific URL for the OMM to retrieve the IMA configuration file (ima.cfg). The IMA configuration remains available even if the configured server becomes unavailable.

When you set a specific URL, the OMM uses that URL to load the IMA configuration file during startup. If no specific IMA configuration file source is configured, the provisioning server settings (ConfigURL) are used to retrieve the ima.cfg file.

For a description of the parameters on the **IMA** tab, see the description of the **System settings** page of the OMM Web service. The same parameters are described in the **OM Integrated Messaging & Alerting service** section (section 5.4.1.8).

6.5.2.5 Additional services

For a description of the parameters on the **Additional services** tab, see the description of the **System settings** page of the OMM Web service. The same parameters are described in the following sections:

- **Voice mail** (section 5.4.1.7)
- **OMP web start** (section 5.4.1.5)
- **Date and time** (for NTP servers) (section 5.4.1.14)

6.5.2.6 User monitoring

The **User monitoring** tab allows you to configure the system-wide parameters for the user monitoring feature.

- **Locating escalation:** If this option enabled, the alarm trigger "LOC-ERR-USERSTATE" will be generated by the OMM. Default setting is "off".
- **Start-up delay:** The start-up delay defines the period of time the user monitoring start-up is delayed (between 2 and 15 minutes) after failover or system start-up.
- **Escalation delay:** The escalation delay defines the period of time the user monitoring will wait before the unavailable status is escalated.
- **Activity timeout 1:** The activity timeout 1 defines the maximum time (between 30 and 1440 minutes) between user activities in passive monitoring mode.
- **Activity timeout 2:** The activity timeout 2 defines the maximum time (between 5 and 60 minutes) between user activities in active monitoring mode.

- **Battery threshold:** The battery threshold defines the minimum battery load (between 0 and 100% in steps of 5%).

6.5.2.7 Special branding

With SIP-DECT 6.0 or later, you can integrate a customer-specific logo into the OMM Web service interface (displayed beside the Mitel logo in the top bar). The "Special Branding" tab allows you to specify the location of the branding image file (customer_image.png) on an external file server.

When you set a specific URL, the OMM uses that URL to load the image file during startup. If no specific customer logo file source is configured, the provisioning server settings (ConfigURL) are used to retrieve the image file.

The branding image is stored permanently in the OMM database. The file is deleted automatically when the branding image URL configuration is disabled. The picture should not be larger than 50 pixels high and 216 pixels wide.

By special request, you can use specific branding key to lock the OMM; the key must be branded to all DECT phones before they can be subscribed. See section 7.25 for more information on this feature.

PP Branding key

- **Active key:** Displays the current branding key associated with the DECT phones.
- **New key:** Specifies the new branding key generated through the `DECTSuiteBrandingInstallation.exe` utility.

Branding image URL

- **Active:** Enables the specific URL for downloading the customer_image.png file (as opposed to the ConfigURL, which points to an external file server for all configuration and resource files).
- **Protocol:** Specifies the protocol used to fetch the image file.
- **Port:** Specifies the port of the external file server.
- **Server:** Specifies the IP address or name of the external file server.
- **User name:** Specifies the user name to authenticate on the external file server.
- **Password:** Specifies the password to authenticate on the external file server.
- **Password confirmation:** Confirms the password to authenticate on the external file server.
- **Directory:** Specifies the location of the image file on the external file server.
- **Use common certificate configuration:** Enables the use of the same certificate validation settings for the image file URL as specified for the ConfigURL.

6.5.2.8 Core Dump

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

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

For a description of the parameters on the **Core Dump** tab, refer to the description of the **System settings** page of the OMM Web service. The same parameters are described in the **Core dump URL** section (section 5.4.1.12).

6.5.2.9 Remote system dump

A system dump is a file that holds information about the OpenMobility Manager and all connected RFPs. With the Remote System Dump feature, a system dump is transferred to a remote server. You can configure a specific destination, otherwise the system configuration URL is used.

The system dump is generated manually by pressing the dump button or automatically at the configured time. Please ensure that the used fileserver allows writing or creating system dumps.

For a description of the parameters on the **Remote system Dump** tab, refer to the description of the **System settings** page of the OMM Web service. The same parameters are described in the **System dump** section (section 5.4.1.11).

6.5.2.10 OMM Certificate

You can overwrite the hard-coded OMM certificate by importing a local certificate chain and a private key file which may be password-protected. The OMM certificate will be used for incoming AXI and HTTPS connections to the OMM services. If the OMM can be reached from the internet by a domain and an appropriate CA certificate has been imported, no security warnings are displayed in web browsers that trust the CA root certificate.

For more information on this feature, see section 7.10.

Certificates/key

- **Private key:** Indicates whether the OMM has a private key file (read-only).
- **Local certificate chain:** Indicates the number of local certificate chains deployed on the OMM (read-only).
- **Delete certificates/key:** Allows you to delete any existing certificate or key files.

PEM file import

- **Import PEM file with:** Indicates the content type of the PEM file being imported. Available options are "Local certificate chain" or "Private key".
- **File:** Specifies the location of the PEM file to be imported.
- **Import:** Triggers the import of the specified PEM file.

Private key password

- **Private key password:** Specifies the password to be used for the private key file, if you want the file to be password-protected.
- **Password confirmation:** Confirms the password for the private key file.

6.5.2.11 OMM certificate server

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

- **Active:** Enables the feature.
- **Protocol:** Specifies the preferred protocol (FTP, TFTP, FTPS, HTTP, HTTPS, SFTP).
- **Server:** Specifies the name or IP address of the external file server.
- **Port:** Specifies the certificate server's port number
- **Use default port:** If selected, the default port associated with the selected protocol is used.
- **User name:** Specifies the user name to authenticate against the external file server.
- **Password:** Specifies the password to authenticate against the external file server.
- **Password confirmation:** Confirms the password to authenticate against the external file server.
- **Path without filename:** Specifies the path on the file server to the certificate files.
- **Use common certificate configuration:** Enables the use of the system-wide certificate validation settings, as configured under the **System** -> **Provisioning** menu (see section 6.5.5).
- **Local certificate file:** Specifies the name of the PEM file on the external server including the local certificate or a certificate chain.
- **Private key file:** Specifies the name of the PEM file on the external server including the local key.

6.5.2.12 SNMP

To manage a larger RFP network, an SNMP agent is provided for each RFP. The SNMP agent provides alarm information and allows an SNMP management system (such as "HP Open View") to manage this network. The SNMP sub menu of the OMP provides configuration of SNMP service settings.

For a description of the parameters on the **SNMP** tab, refer to the description of the **SNMP** menu of the OMM Web service (see section 5.4.6).

6.5.2.13 Time zones

The OMM provides all available time zones on the **Time zones** tab. They are set with their known daylight savings time rules adjusted to the Universal Coordinated Time (UTC) by default. The difference to the UTC time is shown in the **UTC difference** field.

In addition, you can configure a new (free) time zone.

The date and time are provided by the OMM to the Mitel 142d and Mitel 600 DECT phones if the DECT phone initiates a DECT location registration. The DECT phone initiates a DECT location registration when:

- subscribing to the OMM
- entering the network again after the DECT signal was lost

- at power on
 - silent charging feature is active at the phone and the phone is taken out of the charger
 - after a specific time to update date and time
- You can change the time zone rules for up to five time zones. The changes are saved in the configuration file and are restored after each OpenMobility Manager startup.

General

- **Difference local standard time to UTC:** The difference (in minutes) between the local standard time and UTC time.
- **Daylight savings time:** Enables or disables application of Daylight Savings Time (DST) for the time zone. If disabled, the Standard time and Daylight savings time tabs are not accessible.
- **Difference daylight savings time to standard time:** The difference (in minutes) between Daylight Savings Time (DST) and Standard Time for the time zone.

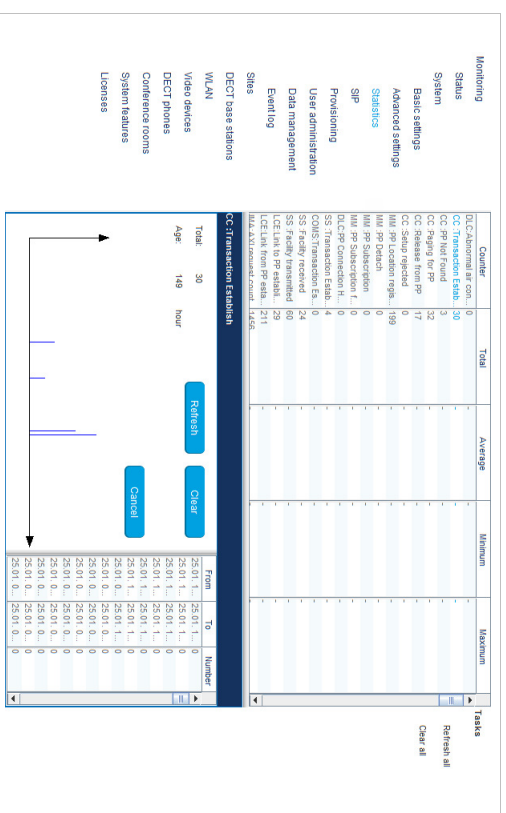
If the **Daylight savings time** parameter on the **General** tab is enabled, you can change the standard time and the daylight savings time (DST) of a time zone in the **Standard time** and **Daylight savings time** tabs. If the time zone has no DST, only the UTC difference can be configured. For the DST both points of time (begin of standard time and begin of daylight savings time) must be specified exactly. Therefore a certain day in the month or a certain week day in a month can be used.

The following commands are available to edit time zones:

- **OK:** Confirm the changed time zone settings.
- **Cancel:** Cancels the operation and resets the changed time zone back to the default setting.
- **Default:** Resets **all** individual time zone settings to the default values and deletes the changed time zone rules in the configuration file.

6.5.3 "STATISTICS" MENU (MONITORING MODE ONLY)

The **Statistics** page provides system statistics counters which can be used to check system behavior. The page is only available in **Monitor Mode**.

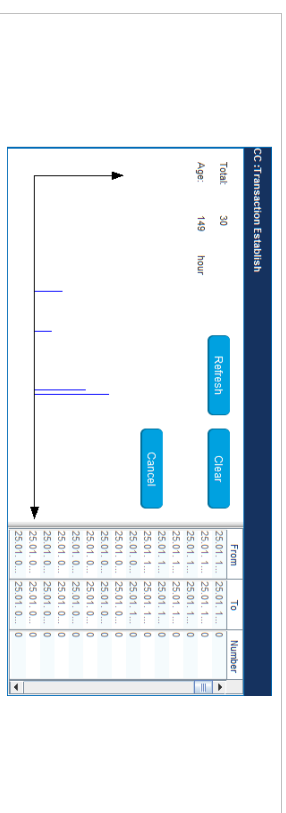


Statistic counters beginning with "+" are counters that are taken over by the standby OMM in case of a failover. All other counters are reset to default values in case of a failover. For more details about the standby feature, see section 7.15.

You can:

- **Refresh all:** request OMM update for all statistics counters.
- **Clear all:** reset all statistics counters in OMM.
- update this single statistics counter by pressing the **Refresh** button, or
- reset this single statistics counter by pressing the **Clear** button.

If a statistics counter is selected in the table, it is shown in a detail panel. This detail panel provides all available information for this statistics counter. You can:



6.5.4 “SIP” MENU

The SIP menu contains global settings for SIP signaling and RTP voice streams.

The SIP menu contains the following tabs:

- Basic settings (see section 6.5.4.1)
- Advanced settings (see section 6.5.4.2)
- Registration traffic shaping (see section 6.5.4.3)
- Backup settings (see section 6.5.4.4)
- RTP settings (see section 6.5.4.5)
- DTMF settings (see section 6.5.4.6)
- Intercom Push-to-talk (see section 6.5.4.7)
- Supplementary services (see section 6.5.4.8)
- Conference (see section 6.5.4.9)
- Security (see section 6.5.4.10)
- Certificate server (see section 6.5.4.11)

6.5.4.1 Basic settings

For a description of the parameters on the **Basic settings** tab, see the description of the **System** -> **SIP** menu of the OMM Web service. The same parameters are described in the **Basic settings** section (section 5.4.3.1).

In addition, the following parameters (related to SIP multipoint support) are available on the **Basic settings** tab:

Local port range

- **DECT phone user UDP/TCP**: The port range to be used for DECT users when UDP/TCP is used as the transport protocol. The default is 5060 – 5060.
- **DECT phone user TLS**: The port range to be used for DECT users when TLS is used as the transport protocol. The default is 5061 – 5061.
- **Conference room UDP/TCP**: The port range to be used for Conference Rooms when UDP/TCP is used as the transport protocol. The default is 4060 – 4060.
- **Conference room TLS**: The port range to be used for DECT users when TLS is used as the transport protocol. The default is 4061 – 4061.

Note: There are certain rules to note when configuring port ranges; see section 3.17 for more information.

6.5.4.2 Advanced settings

You can set several additional SIP parameters on the **Advanced settings** tab.

For a description of the parameters on the **Advanced settings** tab, refer to the description of the **System** -> **SIP** menu of the OMM Web service. The same parameters are described in the **Advanced settings** section (section 5.4.3.2).

In addition, the following parameters are available in the OMP only:

- **X-Aastra-id info**: Enable or disable inclusion of the private X-Aastra-id header in each SIP REGISTER message.
- **User agent info – compatibility mode**: If the **User agent info** option is enabled, the OMM sends information on this version inside the SIP User-Agent/Server headers; this parameter ensures backward compatibility with version information used in older SIP-DECT software releases.

6.5.4.3 Registration traffic shaping

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

For a description of the parameters on the **Registration traffic shaping** tab, see the description of the **System** -> **SIP** page of the OMM Web service. The same parameters are described in the **Registration traffic shaping** section (section 5.4.3.5).

6.5.4.4 Backup settings

To increase the operational availability of the system in critical environments like hospitals, the OMM offers a failover redundancy mechanism for the SIP server. In addition to the primary proxy, outbound proxy and registrar server, you can configure two additional levels of backup servers (secondary and tertiary servers).

The OMM failover behavior in detail depends on the backup server settings set here. A full description of the behavior and deployment hints can be found in section 7.20.3.

- **Secondary proxy server / port, Secondary registrar server / port, Secondary outbound server / port:** Enter the parameters for the secondary server in these fields.
- **Tertiary proxy server / port, Tertiary registrar server / port, Tertiary outbound server / port:** Enter the parameters for the tertiary server in these fields.

Note: Server addresses can be configured as IP addresses, names or a fully qualified domain names. It is possible to configure a mixture of IP addresses, names or fully qualified domain names for the different servers. If fully qualified domain names are configured and the respective port setting is configured to zero ("0"), DNS SRV queries will be performed to locate a list of servers in the domain (see 0).

- **Failover keep alive:** The keep-alive mechanism allows transferring all users registered on a failed server (failover) to secondary/tertiary servers as well as automatically switching back to primary servers. Otherwise, failover is executed only single users. Enable this option if you want to use this feature (default: off).
 - **Failover keep alive time:** For each registration target, a user could be registered successful with, a keep alive procedure is started. Enter the time in this field after which a new keep-alive procedure must be started (1-60 minutes, default: 10 min.).
- For a detailed description of the keep-alive mechanism see section 7.20.4.

6.5.4.5 RTP settings

For a description of the parameters on the **RTP settings** tab, see the description of the **System** -> **SIP** page of the OMM Web service. The same parameters are described in the **RTP settings** section (section 5.4.3.3).

6.5.4.6 DTMF settings

For a description of the parameters on the **DTMF settings** tab, see the description of the **System** -> **SIP** page of the OMM Web service. The same parameters are described in the **DTMF settings** section (section 5.4.3.4).

6.5.4.7 Intercom Push-to-talk

You can set global auto-answer settings on the **Intercom Push-to-talk** tab. For more information on this feature, see section 3.31.

Incoming calls

- **Auto answer:** Enables or disables auto-answer on incoming calls.
- **Microphone mute:** Enables or disables microphone muting when incoming calls are automatically answered.

- **Warning tone:** Enables or disables warning tone on incoming call. A short ringtone is played if there are no active calls. If there is an active call in a "barge in" situation, the ringing will be in-band
- **Allow barge in:** Allows/disallows "barge-in" on existing calls.

Outgoing calls

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

6.5.4.8 Supplementary services

For a description of the parameters on the **Supplementary services** tab, see the description of the **System** -> **SIP** page of the OMM Web service. The same parameters are described in the **Supplementary Services** section (section 5.4.3.6).

6.5.4.9 Conference

You can define the conference mode globally for all SIP-DECT users on the **Conference** tab. For more information on the Conferencing feature, see section 7.21.

- **Server type:** Specifies the operational mode for the conference server. Available options are:
 - **None:** Neither external nor internal conference server is used.
 - **Integrated:** The conference server integrated in the SIP-DECT system is used.
 - **External:** An external conference server (e.g., Broadsoft) is used.
 - **External – Blind Transfer:** An external conference server is used (e.g., MVoice Business). The initiation of the conference is signaled as a blind transfer to the destination specified in the URL parameter.
- **URL:** Specifies the URL for the conference server.

6.5.4.10 Security

For a description of the parameters on the **Security** tab, see the description of the **System** -> **SIP** page of the OMM Web service. The same parameters are described in the **Security** section (section 5.4.3.8) and the **Manual Import** section (section 5.4.3.10).

6.5.4.11 Certificate server

For a description of the parameters on the **Certificate server** tab, see the description of the **System** -> **SIP** page of the OMM Web service. The same parameters are described in the **Certificate server** section (section 5.4.3.9).

6.5.5 "PROVISIONING" MENU

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

configured provisioning server URL is used for secure connections to the file server to retrieve configuration or firmware files.
The **Provisioning** menu contains settings related to the provisioning server.

The Provisioning menu contains the following tabs:

- **Provisioning** (see section 6.5.5.1)
- **Provisioning certificate** (see section 6.5.5.2)
- **Certificate server** (see section 6.5.5.3)
- **System credentials** (see section 6.5.5.4)

6.5.5.1 Provisioning

Configuration files URL

- **Active:** Enable the configuration file URL feature.
- **Protocol:** The protocol to be used to fetch the configuration files.
- **Port:** Provisioning server's port number.
- **Use default port:** If selected, the default port associated with the selected protocol is used.
- **Server:** IP address or name of the provisioning server.
- **Path:** Path to the configuration and resource files on the provisioning server.

SSL settings

- **Validate certificates:** Enables or disables certificate validation. If enabled, the server certificate is validated against trusted CAs (signed by a CA from the Mozilla CA certificate list) and the configured trusted certificates.

139

- **Validate expires:** Enables or disables the validation of certificate expiry. When this parameter is enabled, the client verifies whether or not a certificate has expired prior to accepting the certificate.
- **Validate host name:** Enables or disables the validation of hostnames on the OMM.
- **Allow unconfigured trusted certificates:** If enabled, this parameter disables any server certificate validation as long as no trusted certificate was imported into the OMM. AXI commands in a received configuration file may import such trusted certificates into the OMM.
- **Import certificates with first connection:** If enabled (in conjunction with the **Allow unconfigured trusted certificates** parameter), the trusted certificate will be imported from the cert chain delivered in the server response without any validation, as long as no trusted certificate was imported previously into the OMM.
- **SSL version:** The SSL protocol version to use for the configuration file server connection. Available options are: TLS1.0, TLS1.1, TLS1.2 or AUTO, where AUTO accepts all protocol versions.

Daily automatic reload of configuration and firmware files

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

6.5.5.2 Provisioning certificates

Provisioning certificates are used for secure connections to configuration or firmware file servers that support mutual authentication.

A trusted certificate chain is used by the OMM to validate the server. This is required if the server has no certificate derived from a trusted CA root certificate, where the OMM uses the Mozilla CA Certificate List. If no server certificate is available, the validation against trusted and CA certificates can be disabled in the certificate validation options (only encrypted TLS connection).

The local certificate chain plus the private key are provided from the OMM to servers requesting mutual authentication. The private key file may be password protected.

6.5.5.3 Certificate server

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

- **Active:** Enable automatic updating of certificates the feature.
- **Protocol:** Specifies the preferred protocol (FTP, TFTP, FTPS, HTTP, HTTPS, SFTP)
- **Server:** Specifies the name or IP address of the external file server.
- **Port:** Specifies the certificate server's port number
- **Use default port:** If selected, the default port associated with the selected protocol is used.
- **User name:** Specifies the user name to authenticate against the external file server.

140

- **Password:** Specifies the password to authenticate against the external file server.
- **Password confirmation:** Confirms the password to authenticate against the external file server.
- **Path without filename:** Specifies the path on the file server to the certificate files.
- **Use common certificate configuration:** Enables the use of the system-wide certificate validation settings, as configured on the **System** -> **Provisioning** -> **Provisioning certificates** page (see section 6.5.5.2)
- **Trusted certificate file:** Specifies the name of the PEM file on the specified server, including the trusted certificates.
- **Local certificate file:** Specifies the name of the PEM file on the external server including the local certificate or a certificate chain.
- **Private key file:** Specifies the name of the PEM file on the external server including the local key.

6.5.5.4 System credentials

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

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

6.5.6 "USER ADMINISTRATION" MENU

In the **User administration** menu you configure the OMM user accounts.

Configuration

Status

System

Basic settings

Advanced settings

SIP

Provisioning

User administration

Data management

Stats

DECT base stations

WLAN

Video devices

DECT phones

Conference rooms

System features

Licenses

ID	Comment	User name	Password aging	Active	Tasks
1	Full access	admin	None	✓	Create
2	Read-only (ssh only)	read	None	✓	Configure

User account - Full access

CreatePermissions

Active

User name

Old password

Password

Password confirmation

Password aging

None

OK

Cancel

The three user accounts "Full access", "Read-only" and "Root (ssh only)" available via the **User administration** page of the OMM Web service can also be configured in the OMP. These three predefined user accounts cannot be removed or renamed. Only the "Read-only" account can be activated and deactivated. The permissions are fixed. This is consistent with the OMM WEB service. The meaning of the different account types is described in section 7.17.1. In addition, the OMP allows to create additional user accounts (login and password) and to assign specific permissions. The tasks which can be performed are mode-dependant.

Configuration mode	Monitor mode	See section
Create: Create new user account		6.5.6.1
Configure: Configure selected user account in detail panel		6.5.6.2
	Show details: Shows selected user account in detail panel	6.5.6.3
Delete: Delete selected user account		6.5.6.4

6.5.6.1 Creating New User Accounts

It is possible to create additional user accounts (login and password) and to assign specific permissions. These accounts are mainly designed to have specific login data and permissions for applications which are using OM AXI to connect with the OMM.

Note: Individual user accounts cannot be used for a login to the OMM Web service nor SSH.

The screenshot shows the 'new user account' form. The 'General' tab is selected. It contains a table with columns: ID, Username, Password, User name, Password aging, and Active. Below the table are input fields for 'Active' (checkbox), 'User name', 'Password', and 'Password confirmation'. There are 'OK' and 'Cancel' buttons at the bottom. The 'Tasks' tab is also visible, showing a table with columns: Task, Create, and Configure.

Adding individual user accounts is only possible in **Configuration Mode**. To add a user account, do the following:

- 1 In the **Tasks** bar click on the **Create** command.
The **New user account** panel opens. It provides various tabs where the account data must be entered.
- 2 Configure the user account, see parameter description below.
- 3 Press the **OK** button.

The following parameters can be set in the tabs of the **New user account** panel:

General

For a description of the parameters which can be set in the **General** tab, see the description of the **User administration** page of the OMM Web service (see section 6.5.6.).

Permissions

The permissions for an individual user account can be set independent from any license status even if some of the permissions can only been used with an appropriate license.

If an application connects with the OMM via OM AXI, then the permissions been sent from the OMM to the application is the result of the configured permissions for this account and the actual license status. For more information please see the OM Application XML Interface (OM AXI) specification /31/.

The permissions have the following meaning:

Permission	Description
Read	Read OMM data (OM AXI get requests)
Write	Set OMM data (OM AXI set requests)
Messaging info	Sent messages with priority "Info"
Messaging	Sent messages with priority "Low", "Normal" and "High"
Messaging emergency	Sent messages with priority "Emergency"
Messaging locating	Sent messages with priority "LocatingAlert"
Locating	Permission to query the position of DECT phones and to track DECT phone positions
Monitoring	Permission to monitor various technical aspects of the mobility system
Video	Permission for video streaming

6.5.6.2 Changing a User Account

Changing user accounts is only possible in **configuration mode**. To change the configuration of an existing user account, do the following:

- 1 Select the appropriate user account in the account table.
- 2 In the **Tasks** bar click on the **Configure** command.
- 3 Change the user account parameters (see parameter descriptions in section 6.5.6.1).
- 4 Press the **OK** button.

Please note: The predefined user accounts "Full access", "Read-only" and "Root (ssh only)" user accounts cannot be renamed. Also their permissions are fixed and cannot be changed.

6.5.6.3 Viewing User Account Details

You can view the configuration of a user account in **monitor mode**. Proceed as follows:

- 1 Select the appropriate user account in the table.

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

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

- 3 To close the user account detail panel, click the **Cancel** button.

6.5.6.4 Deleting User Accounts

Deleting user accounts is only possible in **configuration mode**. To delete one or more existing user accounts proceed as follows:

- 1 Select the appropriate account(s) in the user account table by activating the corresponding checkbox(es).
- 2 In the **Tasks** bar click on the **Delete** command.
- 3 Confirm the displayed prompt with **OK**.

Please note: The predefined user accounts "Full access", "Read-only" and "Root (ssh only)" user accounts cannot be removed.

6.5.7 "DATA MANAGEMENT" MENU

The **Data management** menu provides access to data related to import and export features.

The Data management contains the following tabs:

- **Auto DB export** (see section 6.5.7.1)
- **User data import** (see section 6.5.7.2)
- **DECT phones synchronization** (see section 6.5.7.3)
- **Manual DB import** (see section 6.5.7.4)
- **Manual DB export** (see section 6.5.7.5)
- **Maintenance** (see section 6.5.7.6)
- **IMA** (see section 6.5.7.7)

6.5.7.1 Automatic DB export

The automatic database export feature allows an automatic database backup to an external server for each configuration modification.

Please note: Synchronization with an NTP server is mandatory for an automatic database export. For NTP server configuration, see section 7.5.4 and section 7.6.

For a description of the parameters on the **Automatic DB export** tab, see the description of the **System** -> **Data management** page of the OMM Web service. The same parameters are described in the **Automatic Database Export** section (section 5.4.7.3).

6.5.7.2 User data import

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

- **Configure specific source:** Enables the specific URL to an external file server for retrieving the user data file.
- **Protocol:** Specifies the preferred protocol.
- **Port:** Specifies the port on the server.
- **Server:** Specifies the IP address or the name of the server.
- **User name, Password, Password confirmation:** Specifies the credentials for the server.
- **Path:** Specifies the path to the file containing the user data.
- **Use common certificate configuration:** Enables the use of the system-wide certificate validation settings, as configured on the **System** -> **Provisioning** -> **Certificates** page (see section 5.4.2.8).

Please note: If no credentials are specified for secure protocols, the system credentials are automatically used (see section 5.4.2.2). If the system credentials must not be used, the user name and password must be explicitly set here even for anonymous settings.

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

6.5.7.3 DECT phones synchronization

The user data synchronization feature ensures that all user and device database information is distributed to all OMM instances in the system. Each peripheral OMM must have a connection to the AXI interface of the central OMM (and the standby central OMM, if configured) to send and receive updated user data information. Specify the same user credentials used to access the central OMM via the OMP. For more information on this feature, see section 7.16.

- **Activate synchronization:** Enable user data synchronization for the OMM.
- **OMM1:** Specifies the IP address of the central OMM.
- **OMM2:** Specifies the IP address of a second central OMM, in the case of a standby configuration.
- **User name:** Specifies the user name required to access the central OMM.
- **Password:** Specifies the password required to access the central OMM.
- **Password confirmation:** Confirms the password required to access the central OMM.

6.5.7.4 Manual DB import

The manual database import feature allows the import of an OMM database.

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

For a description of the parameters on the **Manual DB import** tab, see the description of the **System** -> **Data management** page of the OMM Web service. The same parameters are described in the **Manual Database Import** section (section 5.4.7.1).

6.5.7.5 Manual DB export

The manual database export feature allows a manual database backup to an external server.

For a description of the parameters on the **Manual DB export** tab, see the description of the **System** -> **Data management** page of the OMM Web service. The same parameters are described in the **Manual Database Export** section (section 5.4.7.2).

6.5.7.6 Maintenance

In the **Maintenance** panel, you can perform a system dump, for example, for product support information purposes. A file "sysdump.txt" is created in the selected directory. Click the **Directory** button to select the directory, then click the **Download** button to start the system dump.

6.5.7.7 IMA

You can upload an IMA configuration file manually. To validate the existing configuration, the IMA configuration can be also downloaded. An uploaded IMA configuration may be overwritten if a server for the IMA configuration file is configured or if the 'ima.cfg' is available on the provisioning server. The IMA configuration can be deleted regardless of its source.

- **Config file import**
To upload an IMA configuration file, click the **File** button to browse to the file, then click **Import**.
- **Config file export**
To download the current IMA configuration file, click the **Directory** button to select the destination directory, then click **Export**.
- **Delete config file**
To delete the IMA configuration file, click **Delete**.

6.5.8 "EVENT LOG" MENU

The **Event Log** menu provides information about system events. The menu is only available in **Monitor Mode**.

Monitoring					Tasks				
Status	Severity	Subsystem	Count	Time	Event	Show details			
System	AVO	STB	1	2015/01/19 16:06:00	[199] New connection from 10.37.18.32 to 50.85	Cancel all			
	AVO	AVO	1	2015/01/19 16:07:30.1	[193] Remote host co...				
	AVO	AVO	1	2015/01/21 21:06:59.2	[197/1000] Remote host co...				
Basic settings	AVO	STB	1	2015/01/21 21:06:59.5	[197/1000] Remote host co...				
	AVO	STB	1	2015/01/21 21:06:59.5	[194] SIP-DECT 6.0RC4 fail...				
	AVO	AVO	1	2015/01/21 21:05:59.9	[194] New connection...				
Statistics	AVO	AVO	1	2015/01/21 21:06:59.6	[198] New connection...				
	AVO	STB	1	2015/01/21 21:06:59.2	[197/1000] Remote host co...				
	AVO	STB	1	2015/01/21 21:06:59.2	[194] SIP-DECT 6.0RC4 fail...				
SIP	AVO	AVO	1	2015/01/21 21:07:01.9	[191] New connection...				
	AVO	AVO	1	2015/01/21 21:07:01.9	[191] New connection...				
	AVO	AVO	1	2015/01/21 21:07:01.9	[191] New connection...				
User administration	AVO	AVO	1	2015/01/21 21:07:01.9	[191] New connection...				
	AVO	AVO	1	2015/01/21 21:07:01.9	[191] New connection...				
	AVO	AVO	1	2015/01/21 21:07:01.9	[191] New connection...				
Data management	AVO	STB	1	2015/01/21 21:07:01.9	[191] New connection...				
	AVO	STB	1	2015/01/21 21:07:01.9	[191] New connection...				
	AVO	STB	1	2015/01/21 21:07:01.9	[191] New connection...				
Event log	AVO	AVO	1	2015/01/21 21:07:01.9	[191] New connection...				
	AVO	AVO	1	2015/01/21 21:07:01.9	[191] New connection...				
	AVO	AVO	1	2015/01/21 21:07:01.9	[191] New connection...				
SIPs	AVO	AVO	1	2015/01/21 21:07:01.9	[191] New connection...				
	AVO	AVO	1	2015/01/21 21:07:01.9	[191] New connection...				
	AVO	AVO	1	2015/01/21 21:07:01.9	[191] New connection...				
DECT base stations	AVO	AVO	1	2015/01/21 21:07:01.9	[191] New connection...				
	AVO	AVO	1	2015/01/21 21:07:01.9	[191] New connection...				
	AVO	AVO	1	2015/01/21 21:07:01.9	[191] New connection...				
WLAN	AVO	AVO	1	2015/01/21 21:07:01.9	[191] New connection...				
	AVO	AVO	1	2015/01/21 21:07:01.9	[191] New connection...				
	AVO	AVO	1	2015/01/21 21:07:01.9	[191] New connection...				
Video services	AVO	AVO	1	2015/01/21 21:07:01.9	[191] New connection...				
	AVO	AVO	1	2015/01/21 21:07:01.9	[191] New connection...				
	AVO	AVO	1	2015/01/21 21:07:01.9	[191] New connection...				
DECT phones	AVO	AVO	1	2015/01/21 21:07:01.9	[191] New connection...				
	AVO	AVO	1	2015/01/21 21:07:01.9	[191] New connection...				
	AVO	AVO	1	2015/01/21 21:07:01.9	[191] New connection...				
Conference rooms	AVO	AVO	1	2015/01/21 21:07:01.9	[191] New connection...				
	AVO	AVO	1	2015/01/21 21:07:01.9	[191] New connection...				
	AVO	AVO	1	2015/01/21 21:07:01.9	[191] New connection...				
System features	AVO	AVO	1	2015/01/21 21:07:01.9	[191] New connection...				
	AVO	AVO	1	2015/01/21 21:07:01.9	[191] New connection...				
	AVO	AVO	1	2015/01/21 21:07:01.9	[191] New connection...				
Licenses	AVO	AVO	1	2015/01/21 21:07:01.9	[191] New connection...				
	AVO	AVO	1	2015/01/21 21:07:01.9	[191] New connection...				
	AVO	AVO	1	2015/01/21 21:07:01.9	[191] New connection...				

6.5.8.1 Event log detail panel

Event log

Cancel

Severity

2

Subsystem

AVO

Count

1

Time

2015/01/21 21:06:57:729 UTC

Event

[199] New connection from 10.37.18.32 to 50.85

Cancel

6.6 “SITES” MENU

DECT base stations can be grouped into different sites. The **Sites** menu allows configuration and display of configured sites. An empty system has one predefined site (ID: 1) named “default”. The system requires a minimum of one site.

A site contains the following parameters:

- **ID:** Identification number of the site. A value between 1 and 250 is possible. If no value is given, the OMM selects the next free ID.
- **Name:** The name of the site.
- **Hi-Q audio technology / Enhanced DECT security / Terminal video /**
 - **SRTP:** These capabilities must be enabled or disabled specific for every site.
 - In sites, which are configured to provide this functionality, exclusively RFP 35/36/37 IP and RFP 43 WLAN are applicable.
 - In sites without this capability, it is allowed to mix these new RFP types with RFP 32/34 IP and RFP 42 WLAN.
- **Number of RFPs:** The number of RFPs which are assigned to this site.

You can perform the following tasks:

- **Create:** Create a new site in the **General** tab.
- **Configure:** Configure an existing site in the **General** tab.
- **Delete:** Delete selected sites (only sites without assigned RFPs can be deleted).
- **Show details (only in Monitor Mode):** Shows configuration of a selected site in the **General** tab.

6.7 “DECT BASE STATIONS” MENU

DECT base stations can be configured and viewed in the **DECT base stations** menu.

Configuration mode		Monitor mode	See section
Device list		Device list	6.7.1
Paging areas			6.7.2
Capturing			6.7.3
Enrolment			6.7.4
Export			6.7.5
		Sync view	6.7.6
		Statistics	6.7.7

6.7.1 “DEVICE LIST” MENU

The **Device list** panel displays all configured DECT base stations in a table. The device list is available in **Configuration Mode** and **Monitor Mode**.

Configuration											
	RFP ID	Name	MAC address	IP address	DECT cluster	Paging area	Hi-Q type	Connect.	Active	Tasks	
Status	0x001	SVC RFP1	00:20:42:18:1D:	10.37.18.31	1		RFP 35		✓	✓	Create
	0x002	SVC RFP2	00:20:42:18:20:	10.37.18.32	1		RFP 35		✓	✓	Create
	0x003	System	01:02:23:54:05:	0.0.0.0	5	0	RFP 32	✗	✗	✗	Configure
	0x004	System	01:02:23:54:05:	0.0.0.0	5	0	RFP 32	✗	✗	✗	Configure
Sites	0x005	System	01:02:23:54:05:	0.0.0.0	5	0	RFP 32	✗	✗	✗	Delete
	0x006	System	01:02:23:54:05:	0.0.0.0	5	0	RFP 32	✗	✗	✗	Delete
	0x007	System	01:02:23:54:05:	0.0.0.0	5	0	RFP 32	✗	✗	✗	Delete
	0x008	System	01:02:23:54:05:	0.0.0.0	5	0	RFP 32	✗	✗	✗	Delete
DECT base stations	0x009	System	01:02:23:54:05:	0.0.0.0	5	0	RFP 32	✗	✗	✗	Delete
	0x00A	System	01:02:23:54:05:	0.0.0.0	5	0	RFP 32	✗	✗	✗	Delete
	0x00B	System	01:02:23:54:05:	0.0.0.0	5	0	RFP 32	✗	✗	✗	Delete
	0x00C	System	01:02:23:54:05:	0.0.0.0	5	0	RFP 32	✗	✗	✗	Delete
Paging areas	0x00D	System	01:02:23:54:05:	0.0.0.0	5	0	RFP 32	✗	✗	✗	Delete
	0x00E	System	01:02:23:54:05:	0.0.0.0	5	0	RFP 32	✗	✗	✗	Delete
	0x00F	System	01:02:23:54:05:	0.0.0.0	5	0	RFP 32	✗	✗	✗	Delete
	0x010	System	01:02:23:54:05:	0.0.0.0	5	0	RFP 32	✗	✗	✗	Delete
Capturing	0x011	System	01:02:23:54:05:	0.0.0.0	5	0	RFP 32	✗	✗	✗	Delete
	0x012	System	01:02:23:54:05:	0.0.0.0	5	0	RFP 32	✗	✗	✗	Delete
	0x013	System	01:02:23:54:05:	0.0.0.0	5	0	RFP 32	✗	✗	✗	Delete
	0x014	System	01:02:23:54:05:	0.0.0.0	5	0	RFP 32	✗	✗	✗	Delete
Enrolment	0x015	System	01:02:23:54:05:	0.0.0.0	5	0	RFP 32	✗	✗	✗	Delete
	0x016	System	01:02:23:54:05:	0.0.0.0	5	0	RFP 32	✗	✗	✗	Delete
	0x017	System	01:02:23:54:05:	0.0.0.0	5	0	RFP 32	✗	✗	✗	Delete
	0x018	System	01:02:23:54:05:	0.0.0.0	5	0	RFP 32	✗	✗	✗	Delete
Export											

The **Active** column shows the following states:

- ✗ – DECT is not enabled and/or RFP not connected.
 - ✗ – DECT is enabled and RFP connected, but DECT has not been activated yet.
 - 🔍 – DECT is enabled and RFP is connected, but RFP is not synchronized and searches for other synchronized RFPs.
 - ✓ – DECT is enabled and RFP is connected and synchronized.
- Note:** If the **Active** column is not displayed, you can activate it in the **Select columns** dialog, see section 6.7.1.7.

The tasks you can perform are mode-dependent.

Configuration mode	Monitor mode	See section
Create: Create new base station in detail panel		6.7.1.2
Configure: Configure selected base station in detail panel		6.7.1.3

Configuration mode	Monitor mode	See section
	Show details: Show selected base station in detail panel	6.7.1.4
Delete: Delete selected RFP		6.7.1.5
	Show sync. relations: Show synchronization relation for selected RFPs	6.7.1.6
Select columns: Select columns/parameters to be shown in RFP table	Select columns: Select columns/parameters to be shown in RFP table	6.7.1.7
Filter: Show only RFP datasets in table which contain a special search string	Filter: Show only RFP datasets in table which contain a special search string	6.7.1.8

6.7.1.1 DECT Base Station Detail Panel

The DECT base station detail panel is used for configuration/display of RFP settings and creation of new RFP datasets.

To call up the DECT base station detail panel, do one of the following:

- Choose one of the commands in the task bar on the right of the **DECT base stations** panel (**Create**, **Configure**, or **Show details**)
- Double-click on the appropriate RFP entry in the RFP table.

The DECT base station detail panel contains the following parameter groups sorted in different tabs.

“Status” tab

The Status tab is only available in **Monitor Mode**, and shows system status information for the selected DECT base station.

DECT base station #0007

Status

General

DECT

WLAN

Hardware

Connected

❌

Invalid branding

❌

OMM routing

❌

Version mismatch

❌

Software update

❌

Standby misconfigured

❌

Encryption state

❌

Advanced features state

❌

P address

0.0.0.0

Software version

Cancel

“General” tab

This tab contains the general DECT base station parameters.

DECT base station #0007

General

DECT

WLAN

Hardware

Name

gsm

MAC address

01:02:03:04:05:06

Site

default

Building

Floor

Room

Conference channels

OK

Cancel

“DECT” tab

This tab contains the DECT base station's DECT parameters.

DECT base station #0007

General

DECT

WLAN

Hardware

DECT switched on

5

✓

DECT cluster

0

▼

Paging area

Preferred synchronisation source

Reflective environment

☐

OK

Cancel

"WLAN" tab

This tab contains the DECT base station's WLAN parameters. Settings in the **WLAN** tab apply to RFP 42 WLAN and RFP 43 WLAN base stations only.

"Hardware" tab

In **Monitor Mode**, this tab shows hardware information of the selected DECT base station.

In configuration mode, the DECT base station **Hardware type** can be set, if it is connecting to the OMM for the first time. Once the correct hardware type is received from the DECT base station, you cannot change it.

6.7.1.2 Adding New DECT Base Stations

You must be in **Configuration Mode** to add a new DECT base station. To add a DECT base station to the list of known base stations, do the following:

- 1 Click **Create** under the Tasks lists on the right side of the **DECT base stations** window.
- 2 The **New radio fixed part** panel opens.
- 3 Configure the DECT base station (see parameter descriptions below).
- 3 Click **OK**.

The following parameters can be set in the tabs of the **New DECT base station** panel:

"General" tab

- **Name:** The name for the RFP.
- **MAC address:** Each RFP is identified by its unique MAC address (6 bytes hex format, colon separated). Enter the MAC address, it can be found on the back of the chassis.
- **Site:** If several sites exist, select the site the RFP is assigned to.
- **Building, Floor, Room:** For easier localization of the RFP you can enter data in these fields.
- **Conference channels:** Activate this option to enable the RFP to provide channels for 3-way conferencing. This option is available for RFP 35 / 36 / 37 / 43 (see section 7.20.7).

"DECT" tab

- **DECT switched on:** The DECT functionality for each RFP can be switched on/off.
- **DECT cluster:** If DECT is active the RFP can be assigned to a cluster.
- **Paging area:** Enter the paging area, the RFP is assigned to.

Note: The **Paging area size** is set in the **DECT** tab of the **System settings** menu (see section 6.5.1). The assignment between RFPs and paging areas can be changed in the **Paging areas** menu (see section 6.7.1.8).

- **Preferred synchronization source:** Activate this checkbox if the RFP should be used as synchronization source for the other RFPs in the cluster. For background information on RFP synchronization see section 7.2.
- **Reflective environment:** Within areas containing lot of reflective surfaces (e.g. metal or metal coated glass) in an open space environment the voice quality of a DECT call can be disturbed because of signal reflections which arrive on the DECT phone or RFP using multipath propagation. Calls may have permanent drop outs while moving and high error rates on the RFPs and DECT phones.

For such environment Mitel has developed the DECT XQ enhancement into base stations (RFP 32/34, RFP 42 WLAN and RFP 35/36/37 IP, RFP 43 WLAN) and the Mitel 600 DECT phones family. Using this enhancement by switching the **Reflective environment** flag on might reduce drop outs and cracking noise.

As soon as **Reflective environment** is switched on, the number of calls on an RFP 32/34 resp. RFP 42 WLAN or RFP 35/36/37 IP resp. RFP 43 WLAN is reduced to 4 calls at the same time.

Please note: The RFPs and DECT phones use more bandwidth on the Air Interfaces if the "Reflective environment" is switched on. Therefore this shall only be used when problems sourced by metal reflections are detected.

"WLAN" tab

Settings in the **WLAN** tab apply to RFPs of the type "RFP 42 WLAN" and "RFP 43 WLAN" only. For details about WLAN configurations please see section 7.18.

Please note: WLAN properties can only be set if the correct hardware type is configured in the **Hardware** tab.

- **WLAN switched on:** The WLAN functionality for an RFP 42 WLAN or an RFP 43 WLAN can be switched on/off.
 - For a description of the other parameters which can be set in the **WLAN** tab, see the description of the **DECT base stations** page of the OMM Web service (see section 5.6.3). The corresponding parameters can be found there in the **WLAN settings** section.
- Note:** Configuration of WLAN profiles is only possible with the OM Web service, see section 5.8.1.

"Hardware" tab

WLAN properties can only be set if the correct hardware type is configured. This can be done manually before an RFP connects with the OMM and an automatic detection is possible (**Auto** setting).

6.7.1.3 Changing DECT base station configuration

Changing RFPs is only possible in **configuration mode**. To change the configuration of an existing RFP, do the following:

- 1 Select the appropriate RFP in the RFP table.
- 2 Click **Configure** under the Tasks lists on the right side of the **DECT base stations** window. The DECT base station detail panel opens.
- 3 Change RFP parameters (see descriptions in section 6.7.1.2).
- 4 Click **OK**.

6.7.1.4 Viewing DECT base station Details

You can view the configuration of an RFP in **Monitor Mode**. Proceed as follows:

- 1 Select the appropriate RFP in the RFP table.
- 2 Click **Show details** under the Tasks lists on the right side of the **DECT base stations** window. The DECT base station detail panel opens.
- 3 To close the RFP detail panel, click **Cancel**.

6.7.1.5 Deleting DECT base stations

You can only delete DECT base stations in **Configuration Mode**. To delete a DECT base station, do the following:

- 1 Select the DECT base station (s) in the table by selecting the corresponding checkbox(es).
- 2 Click **Delete** under the Tasks lists on the right side of the **DECT base stations** window. The **Delete selected DECT base station(s)** dialog opens showing a confirmation prompt.
- 3 Click **OK** to confirm.

Please note: License DECT base stations cannot be deleted.

6.7.1.6 Showing Synchronization Relations

You can view the synchronization relations of a DECT base station in **Monitor Mode**. Do the following:

- 1 Select the appropriate RFPs in the RFP table. At least two RFPs must be selected to show their synchronization relations.
 - 2 Click **Show sync. Relations** under the Tasks lists on the right side of the **DECT base stations** window.
- The view switches to the **Sync view** menu. For further information see section 6.7.6.

6.7.1.7 Selecting Columns

You can customize the parameters shown in the DECT base station table:

- 1 Click **Select columns** under the Tasks lists on the right side of the **DECT base stations** window. The **Select columns** dialog opens.
 - 2 Select the columns that shall be shown by activating the appropriate checkboxes.
 - 3 Click the **OK** button.
- The DECT base station table is updated accordingly.

6.7.1.8 Filtering the DECT base station table

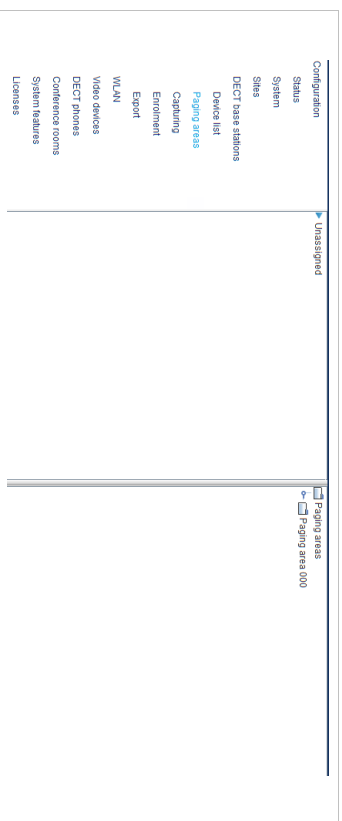
You can filter the list of DECT base station datasets shown in the table by using a filter.

- 1 Click **Filter** under the Tasks lists on the right side of the **DECT base stations** window. The **Filter** dialog opens.
- 2 Enter the search string that serves as filter criterion. You can enter digits and characters. The search is case sensitive.
- 3 Click on the **Filter** button. The **Filter** dialog is closed and the table is adjusted accordingly.
- 4 To reset the filter, click on the **Filter** command in the task bar on the right of the **DECT base stations** panel.
- 5 In the **Filter** dialog click on the **Reset** button.

6.7.2 "PAGING AREAS" MENU

The **Paging area** menu shows all configured RFPs in a tree structure consisting of two trees:

- The left **Unassigned RFPs** tree contains all RFPs without an assigned paging area.
- The right **Paging areas** tree shows all configured paging areas with RFPs assigned to these paging areas.



All DECT base stations are shown including their site and optional hierarchy (building, floor, and room) settings.

- DECT base stations can be moved by drag and drop from unassigned tree to paging area tree and vice versa, as well as between different paging areas inside the paging area tree.
- Only one DECT base station node can be moved at once.
- If a site or a hierarchy node is selected, all DECT base stations that are children of this node are moved.
- If a paging area is completely filled with DECT base stations, moving additional DECT base stations in that paging area is not permitted.
- If not all DECT base stations (selected by a site or hierarchy node) can be moved into a paging area, you are asked if you want to move as many DECT base stations as possible or if the operation should be cancelled.

Note: The **Paging area size** is set in the **DECT** tab of the **System settings** menu (see section 6.5.1).

6.7.3 "CAPTURING" MENU

OMP supports the capture of DECT base stations that try to connect to OMM. These DECT base stations are assigned to OMM by DHCP options or OMM Configurator settings. Capturing is only accessible in **Configuration Mode**.

Available tasks:

- **Capturing:** Start/stop capturing (active capturing is indicated with a green check mark)
- **Add all:** Add all captured DECT base stations to OMM
- **Add selected:** Add selected DECT base stations to OMM

- **Remove all:** Remove selected DECT base stations from list (without adding to OMM)
- **Remove selected:** Remove selected DECT base stations from list (without adding to OMM)
- **Select columns:** Select DECT base station capturing table columns to be shown

6.7.4 "ENROLMENT" MENU

The **Enrolment** menu allows import of DECT base station datasets using a configuration file. For information about required configuration file format see section 10.2.

- 1 Click the **File** button.
A file system dialog opens in which you can select the configuration file. The configuration file must be encoded in UTF-8.
- 2 To check the results from reading the configuration file press the **Show log file** button. In case of file format errors these errors are listed here.

If reading of configuration file is successful, all DECT base station datasets read are shown in a newly created table. This table contains, apart from some DECT base station parameters, the **Status** column which shows the current import status for every DECT base station dataset:

- ✗ – Not enrolled yet
- ✗ – Enrolment failed
- ✓ – OK (Enrolment successful)

- 3 Start the import by selecting one of the following commands:

Add all: Import all DECT base station datasets into the OMM.

Add selected: Import selected DECT base station datasets to the OMM. For selection activate the corresponding checkboxes in the DECT base station table.

Remove all: Remove all DECT base station datasets from table. The table will be hidden.

Remove selected: Remove selected DECT base station datasets from table. If the table is empty after removing of datasets, the table will be hidden. For selection activate the corresponding checkboxes in the DECT base station table.

Show status: Show import status of a selected DECT base station dataset. If enrolment failed for this DECT base station, a message describing the enrolment error is shown.

Select columns: Select the columns that shall be shown in DECT base station table (see also 6.7.1.7).

6.7.5 "EXPORT" MENU

The **Export** menu allows export of all DECT base stations enrolled to the OMM to a ".csv" file. The generated file can be viewed with a standard spreadsheet application.

All enrolled DECT base stations are shown in a table.

Configuration	MAC address	Name	DECT cluster	Paging area	Site ID	RFP type	Tasks
Status	00:30:42:18:20:A2	SVT RFP2	1	0	3	RFP 35	Export all
System	01:02:03:04:05:06	latnu	0	0	0	RFP 32	Export selected
Sites	01:02:03:04:05:08	latnu	0	0	0	RFP 32	Select parameters
DECT base stations	01:02:03:04:05:09	latnu	0	0	0	RFP 32	Select columns
Device list	01:02:03:04:05:0A	latnu	0	0	0	RFP 32	
Paging areas	01:02:03:04:05:0C	latnu	0	0	0	RFP 32	
Capturing	01:02:03:04:05:0D	latnu	0	0	0	RFP 32	
Enrolment	01:02:03:04:05:0E	latnu	0	0	0	RFP 32	
Export	01:02:03:04:05:0F	latnu	0	0	0	RFP 32	

The following tasks can be performed:

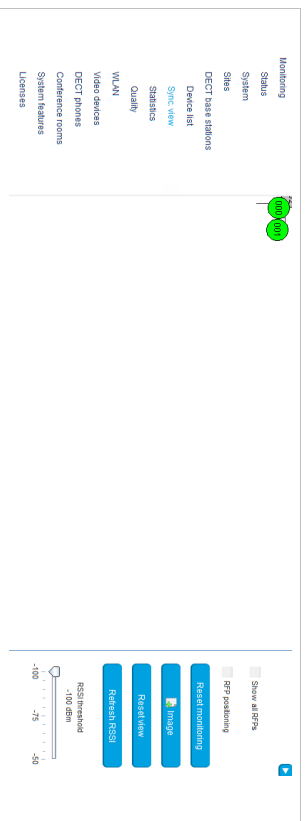
- **Export all:** Export all DECT base station datasets.
- **Export selected:** Export selected DECT base station datasets.
- **Select parameters:** Select DECT base station parameters to be written to the .csv file (select all DECT base station parameters or a subset of these parameters).
- **Select columns:** Select the columns to be written to the .csv file.

When the export begins, a file system dialog opens where you can select the export file name. If all parameters are selected for export, the export file can be re-imported using the Enrolment function (see section 6.7.3). For information about DECT base station export file format see Appendix, section 10.3).

6.7.6 “SYNC VIEW” MENU

The **Sync view** menu allows verification of the synchronization between DECT base stations in a graphical manner.

Note: For information on DECT base station synchronization, see section 7.2.



To open the task panel, click the arrow icon in the upper right corner of the **Sync view** panel. The task panel is displayed on the right. The following tasks can be performed:

- **Show all RFPs:** If this checkbox is activated, all configured RFPs are shown in the sync panel; else only selected RFPs are shown.

- **RFP positioning:** If this checkbox is activated, RFP positions can be changed; else RFP positions are fixed.
- **Reset monitoring:** Reset all active sync view monitoring relations.
- **Image:** Select background image for sync panel.
- **Reset view:** Reset selected view (zero coordinates are reset to the left upper corner of the sync view panel).
- **Refresh RSSI:** Request new RSSI values from OMM for active sync relations.

Viewing sync relations

DECT base stations for which sync relations shall be shown, can be selected as follows:

- Select (more than one) DECT base station in device list table

or

- Activate DECT base station mouse menu in sync view: Press the right mouse button while mouse cursor is on an DECT base station icon and select the **Activate Monitoring** command from the context menu.

The color of the DECT base station icon indicates synchronization state of that DECT base station:

- Grey: Inactive
- Red: Not synchronized
- Yellow: Searching
- Green: Synchronized

Sync relations between DECT base stations are represented by arrows.

Viewing RSSI values

The color of the arrows between DECT base stations is an indication of the RSSI value of the link:

- Red: RSSI < -90 dBm
- Orange: -90 dBm <= RSSI <= -70 dBm
- Green: RSSI > -70 dBm

If the mouse is moved over a DECT base station with monitoring activated, a tool tip with RSSI values is displayed.

You can use the **RSSI threshold** slider to limit the display of values in the tool tip.

6.7.7 “STATISTICS” MENU

The **DECT base stations** -> **Statistics** menu provides information about DECT base station statistics counters. It contains:

- an overview panel with all statistics counters (see section 6.7.7.1)
- multiple statistics group panels, where related statistics counter types are grouped together (see section 6.7.7.2).

The menu is only available in **Monitor Mode**.

6.7.7.1 DECT base station Statistics Overview

The DECT base station statistics overview page contains a list of DECT base stations by ID, and an overview of all DECT base station statistics counters.

Monitoring	Testset	Value	Channel	Group	Expected D	RPD D	RPD E
Shells	Refset: RP	0	Only 3 voice channels R	Voice channels	0	0/000	0/000
System	Refset: al	0	Only 1 voice channels R	Voice channels	0	0/001	0/001
Site	Clear: RP	0	Voice channels busy	Voice channels	2	0/002	0/002
		0	Voice channels busy	Voice channels	1	0/003	0/003
		0	Only 1 air channel free	Air channels	5	0/004	0/004
		0	Air channels busy	Air channels	6	0/005	0/005
		0	Paging queue overflows	Paging	7	0/006	0/006
DECT base stations	Clear: RP	0	Paging queue overflows	Paging	7	0/007	0/007
0		Uplink channel busy	Uplink channels	8	0/008	0/008	
0		Uplink channel busy	Uplink channels	9	0/009	0/009	
0		Other signals	Synch	10	0/010	0/010	
0		RPD results	RPD results	11	0/011	0/011	
Dynamic	Clear: al	0	RPD results	RPD results	12	0/012	0/012
		0	RPD results	RPD results	13	0/013	0/013
		0	RPD results	RPD results	14	0/014	0/014
		0	RPD results	RPD results	15	0/015	0/015
		0	RPD results	RPD results	16	0/016	0/016
Voice channels	Clear: RP	0	RPD results	RPD results	17	0/017	0/017
		0	RPD results	RPD results	18	0/018	0/018
		0	RPD results	RPD results	19	0/019	0/019
		0	RPD results	RPD results	20	0/020	0/020
		0	RPD results	RPD results	21	0/021	0/021
Air channels	Clear: RP	0	RPD results	RPD results	22	0/022	0/022
		0	RPD results	RPD results	23	0/023	0/023
		0	RPD results	RPD results	24	0/024	0/024
		0	RPD results	RPD results	25	0/025	0/025
		0	RPD results	RPD results	26	0/026	0/026
Paging	Clear: RP	0	RPD results	RPD results	27	0/027	0/027
		0	RPD results	RPD results	28	0/028	0/028
		0	RPD results	RPD results	29	0/029	0/029
		0	RPD results	RPD results	30	0/030	0/030
		0	RPD results	RPD results	31	0/031	0/031
Synch	Clear: RP	0	RPD results	RPD results	32	0/032	0/032
		0	RPD results	RPD results	33	0/033	0/033
		0	RPD results	RPD results	34	0/034	0/034
		0	RPD results	RPD results	35	0/035	0/035
		0	RPD results	RPD results	36	0/036	0/036
RPD health	Clear: RP	0	RPD results	RPD results	37	0/037	0/037
		0	RPD results	RPD results	38	0/038	0/038
		0	RPD results	RPD results	39	0/039	0/039
		0	RPD results	RPD results	40	0/040	0/040
		0	RPD results	RPD results	41	0/041	0/041
BMC Connections	Clear: RP	0	RPD results	RPD results	42	0/042	0/042
		0	RPD results	RPD results	43	0/043	0/043
		0	RPD results	RPD results	44	0/044	0/044
		0	RPD results	RPD results	45	0/045	0/045
		0	RPD results	RPD results	46	0/046	0/046
BMC Connections	Clear: RP	0	RPD results	RPD results	47	0/047	0/047
		0	RPD results	RPD results	48	0/048	0/048
		0	RPD results	RPD results	49	0/049	0/049
		0	RPD results	RPD results	50	0/050	0/050
		0	RPD results	RPD results	51	0/051	0/051
BMC DSP data used	Clear: RP	0	RPD results	RPD results	52	0/052	0/052
		0	RPD results	RPD results	53	0/053	0/053
		0	RPD results	RPD results	54	0/054	0/054
		0	RPD results	RPD results	55	0/055	0/055
		0	RPD results	RPD results	56	0/056	0/056
BMC DSP data used	Clear: RP	0	RPD results	RPD results	57	0/057	0/057
		0	RPD results	RPD results	58	0/058	0/058
		0	RPD results	RPD results	59	0/059	0/059
		0	RPD results	RPD results	60	0/060	0/060
		0	RPD results	RPD results	61	0/061	0/061
BMC Miscellaneous	Clear: RP	0	RPD results	RPD results	62	0/062	0/062
		0	RPD results	RPD results	63	0/063	0/063
		0	RPD results	RPD results	64	0/064	0/064
		0	RPD results	RPD results	65	0/065	0/065
		0	RPD results	RPD results	66	0/066	0/066
BMC Miscellaneous	Clear: RP	0	RPD results	RPD results	67	0/067	0/067
		0	RPD results	RPD results	68	0/068	0/068
		0	RPD results	RPD results	69	0/069	0/069
		0	RPD results	RPD results	70	0/070	0/070
		0	RPD results	RPD results	71	0/071	0/071
BMC Frame error rate	Clear: RP	0	RPD results	RPD results	72	0/072	0/072
		0	RPD results	RPD results	73	0/073	0/073
		0	RPD results	RPD results	74	0/074	0/074
		0	RPD results	RPD results	75	0/075	0/075
		0	RPD results	RPD results	76	0/076	0/076
BMC Frame error rate	Clear: RP	0	RPD results	RPD results	77	0/077	0/077
		0	RPD results	RPD results	78	0/078	0/078
		0	RPD results	RPD results	79	0/079	0/079
		0	RPD results	RPD results	80	0/080	0/080
		0	RPD results	RPD results	81	0/081	0/081
BMC Frame error rate	Clear: RP	0	RPD results	RPD results	82	0/082	0/082
		0	RPD results	RPD results	83	0/083	0/083
		0	RPD results	RPD results	84	0/084	0/084
		0	RPD results	RPD results	85	0/085	0/085
		0	RPD results	RPD results	86	0/086	0/086
BMC Frame error rate	Clear: RP	0	RPD results	RPD results	87	0/087	0/087
		0	RPD results	RPD results	88	0/088	0/088
		0	RPD results	RPD results	89	0/089	0/089
		0	RPD results	RPD results	90	0/090	0/090
		0	RPD results	RPD results	91	0/091	0/091
BMC Frame error rate	Clear: RP	0	RPD results	RPD results	92	0/092	0/092
		0	RPD results	RPD results	93	0/093	0/093
		0	RPD results	RPD results	94	0/094	0/094
		0	RPD results	RPD results	95	0/095	0/095
		0	RPD results	RPD results	96	0/096	0/096
BMC Frame error rate	Clear: RP	0	RPD results	RPD results	97	0/097	0/097
		0	RPD results	RPD results	98	0/098	0/098
		0	RPD results	RPD results	99	0/099	0/099
		0	RPD results	RPD results	100	0/100	0/100
		0	RPD results	RPD results	101	0/101	0/101
BMC Frame error rate	Clear: RP	0	RPD results	RPD results	102	0/102	0/102
		0	RPD results	RPD results	103	0/103	0/103
		0	RPD results	RPD results	104	0/104	0/104
		0	RPD results	RPD results	105	0/105	0/105
		0	RPD results	RPD results	106	0/106	0/106
BMC Frame error rate	Clear: RP	0	RPD results	RPD results	107	0/107	0/107
		0	RPD results	RPD results	108	0/108	0/108
		0	RPD results	RPD results	109	0/109	0/109
		0	RPD results	RPD results	110	0/110	0/110
		0	RPD results	RPD results	111	0/111	0/111
BMC Frame error rate	Clear: RP	0	RPD results	RPD results	112	0/112	0/112
		0	RPD results	RPD results	113	0/113	0/113
		0	RPD results	RPD results	114	0/114	0/114
		0	RPD results	RPD results	115	0/115	0/115
		0	RPD results	RPD results	116	0/116	0/116
BMC Frame error rate	Clear: RP	0	RPD results	RPD results	117	0/117	0/117
		0	RPD results	RPD results	118	0/118	0/118
		0	RPD results	RPD results	119	0/119	0/119
		0	RPD results	RPD results	120	0/120	0/120
		0	RPD results	RPD results	121	0/121	0/121
BMC Frame error rate	Clear: RP	0	RPD results	RPD results	122	0/122	0/122
		0	RPD results	RPD results	123	0/123	0/123
		0	RPD results	RPD results	124	0/124	0/124
		0	RPD results	RPD results	125	0/125	0/125
		0	RPD results	RPD results	126	0/126	0/126
BMC Frame error rate	Clear: RP	0	RPD results	RPD results	127	0/127	0/127
		0	RPD results	RPD results	128	0/128	0/128
		0	RPD results	RPD results	129	0/129	0/129
		0	RPD results	RPD results	130	0/130	0/130
		0	RPD results	RPD results	131	0/131	0/131
BMC Frame error rate	Clear: RP	0	RPD results	RPD results	132	0/132	0/132
		0	RPD results	RPD results	133	0/133	0/133
		0	RPD results	RPD results	134	0/134	0/134
		0	RPD results	RPD results	135	0/135	0/135
		0	RPD results	RPD results	136	0/136	0/136
BMC Frame error rate	Clear: RP	0	RPD results	RPD results	137	0/137	0/137
		0	RPD results	RPD results	138	0/138	0/138
		0	RPD results	RPD results	139	0/139	0/139
		0	RPD results	RPD results	140	0/140	0/140
		0	RPD results	RPD results	141	0/141	0/141
BMC Frame error rate	Clear: RP	0	RPD results	RPD results	142	0/142	0/142
		0	RPD results	RPD results	143	0/143	0/143
		0	RPD results	RPD results	144	0/144	0/144
		0	RPD results	RPD results	145	0/145	0/145
		0	RPD results	RPD results	146	0/146	0/146
BMC Frame error rate	Clear: RP	0	RPD results	RPD results	147	0/147	0/147
		0	RPD results	RPD results	148	0/148	0/148
		0	RPD results	RPD results	149	0/149	0/149
		0	RPD results	RPD results	150	0/150	0/150
		0	RPD results	RPD results	151	0/151	0/151
BMC Frame error rate	Clear: RP	0	RPD results	RPD results	152	0/152	0/152
		0	RPD results	RPD results	153	0/153	0/153
		0	RPD results	RPD results	154	0/154	0/154
		0	RPD results	RPD results	155	0/155	0/155
		0	RPD results	RPD results	156	0/156	0/156
BMC Frame error rate	Clear: RP	0	RPD results	RPD results	157	0/157	0/157
		0	RPD results	RPD results	158	0/158	0/158
		0	RPD results	RPD results	159	0/159	0/159
		0	RPD results	RPD results	160	0/160	0/160
		0	RPD results	RPD results	161	0/161	0/161
BMC Frame error rate	Clear: RP	0	RPD results	RPD results	162	0/162	0/162
		0	RPD results	RPD results	163	0/163	0/163
		0	RPD results	RPD results	164	0/164	0/164
		0	RPD results	RPD results	165	0/165	0/165
		0	RPD results	RPD results	166	0/166	0/166
BMC Frame error rate	Clear: RP	0	RPD results	RPD results	167	0/167	0/167
		0	RPD results	RPD results	168	0/168	0/168
		0	RPD results	RPD results	169	0/169	0/169
		0	RPD results	RPD results	170	0/170	0/170
		0	RPD results	RPD results	171	0/171	0/171
BMC Frame error rate	Clear: RP	0	RPD results	RPD results	172	0/172	0/172
		0	RPD results	RPD results	173	0/173	0/173
		0	RPD results	RPD results	174	0/174	0/174
		0	RPD results	RPD results	175	0/175	0/175
		0	RPD results	RPD results	176	0/176	0/176
BMC Frame error rate	Clear: RP	0	RPD results	RPD results	177	0/177	0/177
		0	RPD results	RPD results	178	0/178	0/178
		0	RPD results	RPD results	179	0/179	0/179
		0	RPD results	RPD results	180	0/180	0/180
		0	RPD results	RPD results	181	0/181	0/181
BMC Frame error rate	Clear: RP	0	RPD results	RPD results	182	0/182	0/182
		0	RPD results	RPD results	183	0/183	0/183
		0	RPD results	RPD results	184	0/184	0/184
		0	RPD results	RPD results	185	0/185	0/185
		0	RPD results	RPD results	186	0/186	0/186
BMC Frame error rate	Clear: RP	0	RPD results	RPD results	187	0/187	0/187
		0	RPD results	RPD results	188	0/188	0/188
		0	RPD results	RPD results	189	0/189	0/189
		0	RPD results	RPD results	190	0/190	0/190
		0	RPD results	RPD results	191	0/191	0/191
BMC Frame error rate	Clear: RP	0	RPD results	RPD results	192	0/192	0/192
		0	RPD results	RPD results	193	0/193	0/193
		0	RPD results	RPD results	194	0/194	0/194
		0	RPD results	RPD results	195	0/195	0/195
		0	RPD results	RPD results	196	0/196	0/196
BMC Frame error rate	Clear: RP	0	RPD results	RPD results	197	0/197	0/197
		0	RPD results	RPD results	198	0/198	0/198
		0	RPD results	RPD results	199	0/199	0/199
		0	RPD results	RPD results	200	0/200	0/200
		0	RPD results	RPD results	201	0/201	0/201
BMC Frame error rate	Clear: RP	0	RPD results	RPD results	202	0/202	0/202
		0	RPD results	RPD results	203	0/203	0/203
		0	RPD results	RPD results	204	0/204	0/204
		0	RPD results	RPD results	205	0/205	0/205
		0	RPD results	RPD results	206	0/206	0/206
BMC Frame error rate	Clear: RP	0	RPD results	RPD results	207	0/207	0/207
		0	RPD results	RPD results	208	0/208	0/208
		0	RPD results	RPD results	209	0/209	0/209
		0	RPD results	RPD results	210	0/210	0/210
		0	RPD results	RPD results	211		

The following tasks can be performed:

- **Refresh RFP:** Request counter update by OMM for selected DECT base station statistics counters.
- **Refresh all:** Request counter update by OMM for all DECT base station statistics counters.
- **Clear RFP:** Clear all DECT base station statistics counters on selected DECT base station.
- **Clear all:** Clear all DECT base station statistics counters.

If a DECT base station is selected (left **RFP ID** table), the statistics counter table shows counter values for that DECT base station (right table). When a statistics counter entry is selected, a detail panel opens which shows more detailed information for that counter.

The detail panel shows values for total occurrence and occurrence in current and last week. You can clear the selected statistics counter on the selected DECT base station by pressing the **Clear** button.

6.7.7.2 DECT base station Statistics Group Panels

The DECT base station statistics group panels divide DECT base station statistics counters into logical groups. This allows display of all statistics counters of a special group of all DECT base stations in one table.

The group panels are listed under the **Statistics** menu entry in the left panel.

Note that with SIP-DECT 6.0 or later, the statistic data collected by the BMC part of each DECT base station device (in the DECT MAC layer) are now shown with the DECT base station statistic data collected by the OMM.

As an update between OMM and DECT base station usually occurs once every hour, it can take up to one hour for an event that increments a BMC statistic counter to appear in the OMP.

The following tasks can be performed:

- **Refresh RFP:** Request counter update by OMM for selected DECT base station.
- **Refresh all:** Request counter update by OMM for all counters.
- **Clear group RFP:** Clear counter group of selected DECT base stations.
- **Clear group:** Clear counter group of all DECT base stations.
- **Clear RFP:** Clear all counters of selected DECT base station.
- **Clear all:** Clear all counters of all DECT base stations.

6.7.8 “QUALITY” MENU

OMP provides a monitoring ability for critical IP network parameters. Administrators can check basic network quality information for all DECT base stations. This includes Voice quality (Jitter, Packet lost) and OMM to RFP link quality (Roundtrip delay).

The menu is only available in **Monitor Mode**.

6.7.8.1 IP

IP quality menu provides information about link quality between DECT base stations and OMM.

[illegible]

Displayed parameters:

- **ID:** Radio fixed part identifier
- **Connected time:** Time the RFP is connected to OMM (sec)
- **Current RTT:** Current roundtrip time between RFP and OMM (msec)
- **Max. RTT:** Maximal detected roundtrip time between RFP and OMM
- **Count:** Number of roundtrip time measures
 - **< 25 msec:** Number of roundtrip time measures lower than 25 msec
 - **< 50 msec:** Number of roundtrip time measures between 25 and 50 msec
 - **< 150 msec:** Number of roundtrip time measures between 50 and 150 msec
 - **< 500 msec:** Number of roundtrip time measures between 150 and 500 msec
 - **>= 500 msec:** Number of roundtrip time measures 500 msec and more

Available tasks:

- **Select columns:** Columns to be shown in IP quality table

6.7.8.2 Media Stream

Media stream panel provides information about voice quality.

Monitoring

- Status
- System
- Sites
- DECT base stations
- Device list
- Sync view
- Statistics
- Quality
- IP
- Media stream
- Synchronization

	ID	Connects	Duration (sec)	TX packets	RX packets	Lost packets	Max. jitter (msec)
boot0	24	36	124	1053	1183	3	0
boot1	7	1	0	0	0	0	0
boot2	0	0	0	0	0	0	0
boot3	0	0	0	0	0	0	0
boot4	0	0	0	0	0	0	0
boot5	0	0	0	0	0	0	0
boot6	0	0	0	0	0	0	0
boot7	0	0	0	0	0	0	0
boot8	0	0	0	0	0	0	0
boot9	0	0	0	0	0	0	0
bootA	0	0	0	0	0	0	0
bootB	0	0	0	0	0	0	0

Tasks

- Clear RFP
- Clear all
- Select columns

Displayed parameters:

- **ID:** Radio fixed part identifier
- **Connects**
- **Duration (sec)**
- **TX packets**
- **RX packets**
- **Lost packets**
- **Max. jitter(msec)**

Available tasks:

- **Clear RFP:** Clear values for selected RFPs
- **Clear all:** Clear values for all RFPs
- **Select columns:** Select media stream quality table columns to be shown

6.7.8.3 Synchronization

Synchronization panel allows checking the synchronization status of RFPs which allows identifying RFPs with bad synchronization coverage.

Synchronization monitoring can optionally be run in snapshot mode. If this mode is activated, data update must be triggered by a user otherwise data were updated automatically anytime if new values arrive from OMM.

Monitoring

- Status
- System
- Sites
- DECT base stations
- Device list
- Sync view
- Statistics
- Quality
- IP
- Media stream
- Synchronization

	ID	DECT cluster	Sync state	Strong relations	Low relations	Max. RSSI (dBm)	Min. RSSI (dBm)
0	1	1	✓	1	0	-43	-42

Tasks

- 2K Snapshot mode
- Snapshot
- Select columns

Available parameters:

- **ID:** Radio fixed part id
- **DECT cluster:** Cluster of the RFP
- **Sync state:** Synchronization state of the RFP
- **Strong relations**
- **Low relations**
- **Max. RSSI (dBm)**
- **Min. RSSI (dBm)**

Available tasks in media synchronization quality table:

- **Snapshot mode:** Enable snapshot mode (green check mark indicates snapshot mode is on)
- **Update:** Request data update in snapshot mode
- **Select columns:** Select synchronization quality table columns to be shown

6.8 “WLAN” MENU

OMP supports configuration of WLAN profiles and provides an overview of wireless clients currently connected.

6.8.1 PROFILES

OMM supports up to 20 WLAN profiles, which can be added, changed and deleted in OMP configuration mode. Configuration and state of any WLAN profile can be checked in monitoring mode.

6.8.1.1 WLAN Profiles - configuration mode

WLAN profile configuration menu provides an overview of all configured WLAN profiles.

Configuration

Status

System

Sites

DECT base stations

WLAN

Profiles

Video devices

DECT phones

Conference rooms

System features

Licenses

ID	Enabled	Profile type	Mode	SSID 1	DECT base station
----	---------	--------------	------	--------	-------------------

Tasks

Create profile

Configure profile

Delete profile

Delete all profiles

Configure MAC filter

Select columns

The following tasks are available in this menu:

- **Create profile:** Create a new WLAN profile (available if the maximal number of 10 WLAN profiles is not yet reached)
- **Configure profile:** Reconfigure selected profile
- **Delete profile:** Deletes a selected profile (only available if selected profile is not in use by any Radio fixed part)
- **Delete all profiles:** Deletes all existing profiles (only available if none of these profiles is in use by any Radio fixed part)
- **Configure MAC filter:** Add, configure, delete MAC filter for selected profile
- **Select columns:** Select WLAN profile table columns to be shown

6.8.1.2 WLAN Profiles Monitoring Mode

WLAN profile monitoring menu shows all configured WLAN profiles.

The following tasks are available:

- **Show Profile:** Show details of selected WLAN profile
- **Show MAC filter:** Show configured MAC filter of selected WLAN profile
- **Select columns:** Select WLAN profile table columns to be shown

6.8.1.3 WLAN Profile Detail Panel

WLAN profile detail panel is used to create, reconfigure or show a profile. It consists of different tabs which are used for general settings of WLAN profile, SSID configuration and SSID security settings.

WLAN profile detail panel is opened if one of the following tasks is performed in WLAN profile menu:

- **Create profile** (configuration mode)
- **Configure profile** (configuration mode)
- **Show profile** (monitoring mode)

The "General" tab is always shown and configures/shows general settings of this profile like enabling of profile and profile type.

General | SSID selection | SSID 1 general | SSID 1 security

Profile enabled

Avoid interferences

Profile type

802.11 mode

WLAN

Internal bit rate

Beacon interval

DTIM interval

RTS threshold

Fragmentation threshold

802.11n

802.11n

100 Mbps

100 mac

5 Beacons

2347 Bytes

2346 Bytes

OK

Cancel

The "SSID selection" tab is used for enabling of SSIDs. At least "SSID 1" is always enabled. "SSID 2", "SSID 3" and "SSID 4" can be activated optional.

General | SSID selection | SSID 1 general | SSID 1 security

Configure

SSID 1

SSID 2

SSID 3

SSID 4

Name

OK

Cancel

The "SSID x general" tab is shown for any activated SSID. Among other things, you can use it to select Security type.

General | SSID selection | SSID 1 general | SSID 1 security

SSID enabled

VLAN tag

Security type

BSS isolation

Use MAC access filter

Hidden SSID mode

Open

Open

OK

Cancel

A tab "SSID x security" is shown as well. It is accessible only for SSIDs with security type set to "WEP" or "WPA". If security type stays at "Open" this tab is inactive. It allows setting of all necessary security parameters for this SSID.

6.8.1.4 MAC Access Filter Detail Panel

MAC access filter detail panel in configuration mode allows the adding, configuring and deleting of MAC access filters. File import and export of MAC access filters is supported as well.

Monitoring mode shows all configured MAC access filters only.

MAC access filter detail panel is opened if one of the following tasks is performed in WLAN profile menu:

- **Configure MAC filter** (configuration mode)
- **Show MAC filter** (monitoring mode)

The "General" tab in configuration mode shows all configured MAC access filter.

The following actions are available:

- **Create:** Create new MAC access filter
- **Configure:** Change name of selected MAC access filter
- **Delete:** Delete all selected MAC access filter

The "Import" tab (configuration mode only) provides import of a list of MAC access filter from file.

The "Export" tab (configuration mode only) provides export of all configured MAC access filters to file. If no MAC access filter is configured, this tab is inactive.

6.8.1.5 Clients

WLAN clients menu which is available in monitoring mode only, shows all currently connected wireless clients.

6.9 "VIDEO DEVICES" MENU

The **Video devices** panel lists all configured video devices. The device list is available in **Configuration Mode** as well as in **Monitor mode**.

New video device entries show up automatically after they are connected to and recognized by a DECT base station. The **Plugged** and **State** columns shows the following states:

-  / **unplugged** – Video device is not connected.
-  / **plugged** – Video device is connected.
-  / **started** – Video device is being watched in the OM Locating application.
-  / **stopped** – Video device is connected but disabled in the OMP.

The **Tag** column shows the USB ID of the connected video device. The **USB path** column shows the USB port number to be used, e.g. "1" is a video device connected directly to the RFP while "1.1" indicates an indirect connection using an USB hub.

The tasks which can be performed are mode-dependant.

Configuration mode	Monitor mode	See section
Configure: Configure selected video device in detail panel		6.9.1
	Show details: Show selected video device in detail panel	6.9.2
Delete: Delete selected disconnected video device		6.9.3
Filter: Show only video device entries in table which contains a special search string	Filter: Show only video device entries in table which contains a special search string	6.9.4

6.9.1 CHANGING VIDEO DEVICES

Changing video devices is only possible in **Configuration Mode**. To change the configuration of an existing video device, do the following:

- 1 Select the appropriate video device in the video devices table.
- 2 In the task bar on the right of the **Video devices** panel click on the **Configure** command. The video device detail panel opens.
- 3 Change video device parameters, see description below.
- 4 Press the **OK** button.

Please note: You cannot change the configuration for a video device that is being watched in the OM Locating application (**State** column shows "active"). You must disable the video device first by deactivating the **Active** option.

The following parameters can be set in the **General** tab of the **Video devices** panel:

- **Active:** Disable this option to switch off the video device. This also switches off the status LED of the video device immediately (if applicable).
- **Name:** Enter a meaningful name for the video device.
- **Building, Floor, Room:** For easier localization of the video device you can enter data in these fields.
- **Resolution:** Select a resolution for the video device. Higher resolutions require more bandwidth when watching the video image in the OM Locating application. Note, that not all video devices support all available resolutions. Default: "VGA (640 x 480)".
- **Frame rate:** Select a frame rate (2-10 frames per second). Higher frame rates require more bandwidth when watching the video image in the OM Locating application.

6.9.2 VIEWING VIDEO DEVICE DETAILS

You can view the configuration of a video device in **monitor mode**. Proceed as follows:

- 1 Select the appropriate video device in the video devices table.
- 2 In the task bar on the right of the **Video devices** panel click on the **Show details** command.

The video device detail panel opens (see 0).

3 Click **Cancel** to close the video device detail panel.

6.9.3 DELETING VIDEO DEVICES

Deleting video devices is only possible in **Configuration Mode**. To delete one or more existing video devices proceed as follows:

- 1 Select the appropriate video device(s) in the video devices table by activating the corresponding checkbox(es). Note that you can only delete disconnected video devices.
- 2 In the task bar on the right of the **Video devices** panel click on the **Delete** command.
- 3 The **Delete selected video devices(s)** dialog opens showing a confirmation prompt.

6.9.4 FILTERING VIDEO DEVICE TABLE

You can filter the list of video device entries shown in the video devices table by using a filter.

- 1 In the task bar on the right of the **Video devices** panel click on the **Filter** command.
- The **Filter** dialog opens.
- 2 Enter the search string that serves as filter criterion. You can enter digits and characters. The search is case sensitive.
- 3 Click on the **Filter** button.
- The **Filter** dialog is closed and the video device table will be adapted accordingly.
- 4 To reset the filter, click on the **Filter** command in the task bar on the right of the **Video devices** panel.
- 5 In the **Filter** dialog click on the **Reset** button.

6.10 “DECT PHONES” MENU

DECT phone datasets can be configured and viewed in the **DECT phones** menu. The **DECT Phones** menu contains different submenus. Each submenu displays its own table of DECT phone datasets.

Configuration mode	Monitor mode	See section
Overview: Displays all user and device-related DECT phone data	Overview: Displays all user and device-related DECT phone data	6.10.1
Users: Displays all DECT phone user data		6.10.2
Devices: Displays all DECT phone device data	Devices: Displays all DECT phone device data	6.10.3
	User monitoring: Displays the status of all monitored users	7.29.7.3

6.10.1 “OVERVIEW” MENU

In the **Overview** panel, all user-related and device-related DECT phone data are listed in a table. The overview is available in **Configuration Mode** and **Monitor mode**.

Configuration						
System	Shells	Sites	DECT base stations	VLANs	Video devices	DECT phones
Overview						
Users	Devices	Conference rooms	System features	Licenses		
Device ID	PEI	Number/SIP user no.	User ID	User rel. type	Active	Tasks
0x001	01545 0031639	250552	0x001	Fixed	✓	Create
0x002	03586 0823116 0	250553	0x002	Fixed	✓	Configure
0x003	03586 0825646 7	250554	0x003	Fixed	✓	Delete
0x004	00100 000000 3	250001	0x004	Fixed	✗	
0x005	00100 000000 3	250002	0x005	Fixed	✗	
0x006	00100 000000 1 4	250003	0x006	Fixed	✗	
0x007	00100 000002 5	250004	0x007	Fixed	✗	
0x008	00100 000002 5	250005	0x008	Fixed	✗	
0x009	00100 000002 5	250006	0x009	Fixed	✗	
0x010	00100 000005 8	250007	0x010	Fixed	✗	
0x011	00100 000005 8	250008	0x011	Fixed	✗	
0x012	00100 000005 8	250009	0x012	Fixed	✗	
0x013	00100 000006 9	250010	0x013	Fixed	✗	
0x014	00100 000006 9	250011	0x014	Fixed	✗	
0x015	00100 000006 9	250012	0x015	Fixed	✗	
0x016	00100 000007 7	250013	0x016	Fixed	✗	
0x017	00100 000007 7	250014	0x017	Fixed	✗	
0x018	00100 000007 7	250015	0x018	Fixed	✗	
0x019	00100 000008 3	250016	0x019	Fixed	✗	
0x020	00100 000008 3	250017	0x020	Fixed	✗	
0x021	00100 000008 3	250018	0x021	Fixed	✗	
0x022	00100 000009 1	250019	0x022	Fixed	✗	
0x023	00100 000009 1	250020	0x023	Fixed	✗	
0x024	00100 000009 1	250021	0x024	Fixed	✗	
0x025	00100 000010 4	250022	0x025	Fixed	✗	
0x026	00100 000010 4	250023	0x026	Fixed	✗	
0x027	00100 000010 4	250024	0x027	Fixed	✗	
0x028	00100 000011 5	250025	0x028	Fixed	✗	
0x029	00100 000011 5	250026	0x029	Fixed	✗	
0x030	00100 000011 5	250027	0x030	Fixed	✗	
0x031	00100 000012 6	250028	0x031	Fixed	✗	
0x032	00100 000012 6	250029	0x032	Fixed	✗	
0x033	00100 000012 6	250030	0x033	Fixed	✗	
0x034	00100 000013 7	250031	0x034	Fixed	✗	
0x035	00100 000013 7	250032	0x035	Fixed	✗	
0x036	00100 000013 7	250033	0x036	Fixed	✗	
0x037	00100 000014 8	250034	0x037	Fixed	✗	
0x038	00100 000014 8	250035	0x038	Fixed	✗	
0x039	00100 000014 8	250036	0x039	Fixed	✗	
0x040	00100 000015 9	250037	0x040	Fixed	✗	
0x041	00100 000015 9	250038	0x041	Fixed	✗	
0x042	00100 000015 9	250039	0x042	Fixed	✗	
0x043	00100 000016 0	250040	0x043	Fixed	✗	
0x044	00100 000016 0	250041	0x044	Fixed	✗	
0x045	00100 000016 0	250042	0x045	Fixed	✗	
0x046	00100 000017 1	250043	0x046	Fixed	✗	
0x047	00100 000017 1	250044	0x047	Fixed	✗	
0x048	00100 000017 1	250045	0x048	Fixed	✗	
0x049	00100 000018 2	250046	0x049	Fixed	✗	
0x050	00100 000018 2	250047	0x050	Fixed	✗	
0x051	00100 000018 2	250048	0x051	Fixed	✗	
0x052	00100 000019 3	250049	0x052	Fixed	✗	
0x053	00100 000019 3	250050	0x053	Fixed	✗	
0x054	00100 000019 3	250051	0x054	Fixed	✗	
0x055	00100 000020 4	250052	0x055	Fixed	✗	
0x056	00100 000020 4	250053	0x056	Fixed	✗	
0x057	00100 000020 4	250054	0x057	Fixed	✗	
0x058	00100 000021 5	250055	0x058	Fixed	✗	
0x059	00100 000021 5	250056	0x059	Fixed	✗	
0x060	00100 000021 5	250057	0x060	Fixed	✗	
0x061	00100 000022 6	250058	0x061	Fixed	✗	
0x062	00100 000022 6	250059	0x062	Fixed	✗	
0x063	00100 000022 6	250060	0x063	Fixed	✗	
0x064	00100 000023 7	250061	0x064	Fixed	✗	
0x065	00100 000023 7	250062	0x065	Fixed	✗	
0x066	00100 000023 7	250063	0x066	Fixed	✗	
0x067	00100 000024 8	250064	0x067	Fixed	✗	
0x068	00100 000024 8	250065	0x068	Fixed	✗	
0x069	00100 000024 8	250066	0x069	Fixed	✗	
0x070	00100 000025 9	250067	0x070	Fixed	✗	
0x071	00100 000025 9	250068	0x071	Fixed	✗	
0x072	00100 000025 9	250069	0x072	Fixed	✗	
0x073	00100 000026 0	250070	0x073	Fixed	✗	
0x074	00100 000026 0	250071	0x074	Fixed	✗	
0x075	00100 000026 0	250072	0x075	Fixed	✗	
0x076	00100 000027 1	250073	0x076	Fixed	✗	
0x077	00100 000027 1	250074	0x077	Fixed	✗	
0x078	00100 000027 1	250075	0x078	Fixed	✗	
0x079	00100 000028 2	250076	0x079	Fixed	✗	
0x080	00100 000028 2	250077	0x080	Fixed	✗	
0x081	00100 000028 2	250078	0x081	Fixed	✗	
0x082	00100 000029 3	250079	0x082	Fixed	✗	
0x083	00100 000029 3	250080	0x083	Fixed	✗	
0x084	00100 000029 3	250081	0x084	Fixed	✗	
0x085	00100 000030 4	250082	0x085	Fixed	✗	
0x086	00100 000030 4	250083	0x086	Fixed	✗	
0x087	00100 000030 4	250084	0x087	Fixed	✗	
0x088	00100 000031 5	250085	0x088	Fixed	✗	
0x089	00100 000031 5	250086	0x089	Fixed	✗	
0x090	00100 000031 5	250087	0x090	Fixed	✗	
0x091	00100 000032 6	250088	0x091	Fixed	✗	
0x092	00100 000032 6	250089	0x092	Fixed	✗	
0x093	00100 000032 6	250090	0x093	Fixed	✗	
0x094	00100 000033 7	250091	0x094	Fixed	✗	
0x095	00100 000033 7	250092	0x095	Fixed	✗	
0x096	00100 000033 7	250093	0x096	Fixed	✗	
0x097	00100 000034 8	250094	0x097	Fixed	✗	
0x098	00100 000034 8	250095	0x098	Fixed	✗	
0x099	00100 000034 8	250096	0x099	Fixed	✗	
0x000	00100 000000 0	250000	0x000	Fixed	✗	

Monitoring										Tasks												
Status	System	Sites	DECT base stations	WLAN	Video devices	DECT phones	Devices	User monitoring	Conference rooms	System features	Licenses	Device ID	PEI	Subscription	Number of users	Last action	RFP ID	CC	MM	h/s	Repeat	
00001	00000	00000	00000	00000	00000	00000	00000	00000	00000	00000	00000	00001	00000	00000	25000	25.01.21.42	00000					✓
00002	00000	00000	00000	00000	00000	00000	00000	00000	00000	00000	00000	00002	00000	00000	25000	25.01.22.12	00001					✓
00003	00000	00000	00000	00000	00000	00000	00000	00000	00000	00000	00000	00003	00000	00000	25000	25.01.22.25	00000					✓
00004	00000	00000	00000	00000	00000	00000	00000	00000	00000	00000	00000	00004	00000	00000	25000	25.01.22.25	00000					✓
00005	00000	00000	00000	00000	00000	00000	00000	00000	00000	00000	00000	00005	00000	00000	25000	25.01.22.25	00000					✓
00006	00000	00000	00000	00000	00000	00000	00000	00000	00000	00000	00000	00006	00000	00000	25000	25.01.22.25	00000					✓
00007	00000	00000	00000	00000	00000	00000	00000	00000	00000	00000	00000	00007	00000	00000	25000	25.01.22.25	00000					✓
00008	00000	00000	00000	00000	00000	00000	00000	00000	00000	00000	00000	00008	00000	00000	25000	25.01.22.25	00000					✓
00009	00000	00000	00000	00000	00000	00000	00000	00000	00000	00000	00000	00009	00000	00000	25000	25.01.22.25	00000					✓
00010	00000	00000	00000	00000	00000	00000	00000	00000	00000	00000	00000	00010	00000	00000	25000	25.01.22.25	00000					✓
00011	00000	00000	00000	00000	00000	00000	00000	00000	00000	00000	00000	00011	00000	00000	25000	25.01.22.25	00000					✓
00012	00000	00000	00000	00000	00000	00000	00000	00000	00000	00000	00000	00012	00000	00000	25000	25.01.22.25	00000					✓
00013	00000	00000	00000	00000	00000	00000	00000	00000	00000	00000	00000	00013	00000	00000	25000	25.01.22.25	00000					✓
00014	00000	00000	00000	00000	00000	00000	00000	00000	00000	00000	00000	00014	00000	00000	25000	25.01.22.25	00000					✓
00015	00000	00000	00000	00000	00000	00000	00000	00000	00000	00000	00000	00015	00000	00000	25000	25.01.22.25	00000					✓
00016	00000	00000	00000	00000	00000	00000	00000	00000	00000	00000	00000	00016	00000	00000	25000	25.01.22.25	00000					✓
00017	00000	00000	00000	00000	00000	00000	00000	00000	00000	00000	00000	00017	00000	00000	25000	25.01.22.25	00000					✓
00018	00000	00000	00000	00000	00000	00000	00000	00000	00000	00000	00000	00018	00000	00000	25000	25.01.22.25	00000					✓
00019	00000	00000	00000	00000	00000	00000	00000	00000	00000	00000	00000	00019	00000	00000	25000	25.01.22.25	00000					✓
00020	00000	00000	00000	00000	00000	00000	00000	00000	00000	00000	00000	00020	00000	00000	25000	25.01.22.25	00000					✓
00021	00000	00000	00000	00000	00000	00000	00000	00000	00000	00000	00000	00021	00000	00000	25000	25.01.22.25	00000					✓
00022	00000	00000	00000	00000	00000	00000	00000	00000	00000	00000	00000	00022	00000	00000	25000	25.01.22.25	00000					✓
00023	00000	00000	00000	00000	00000	00000	00000	00000	00000	00000	00000	00023	00000	00000	25000	25.01.22.25	00000					✓
00024	00000	00000	00000	00000	00000	00000	00000	00000	00000	00000	00000	00024	00000	00000	25000	25.01.22.25	00000					✓
00025	00000	00000	00000	00000	00000	00000	00000	00000	00000	00000	00000	00025	00000	00000	25000	25.01.22.25	00000					✓
00026	00000	00000	00000	00000	00000	00000	00000	00000	00000	00000	00000	00026	00000	00000	25000	25.01.22.25	00000					✓
00027	00000	00000	00000	00000	00000	00000	00000	00000	00000	00000	00000	00027	00000	00000	25000	25.01.22.25	00000					✓
00028	00000	00000	00000	00000	00000	00000	00000	00000	00000	00000	00000	00028	00000	00000	25000	25.01.22.25	00000					✓
00029	00000	00000	00000	00000	00000	00000	00000	00000	00000	00000	00000	00029	00000	00000	25000	25.01.22.25	00000					✓
00030	00000	00000	00000	00000	00000	00000	00000	00000	00000	00000	00000	00030	00000	00000	25000	25.01.22.25	00000					✓
00031	00000	00000	00000	00000	00000	00000	00000	00000	00000	00000	00000	00031	00000	00000	25000	25.01.22.25	00000					✓
00032	00000	00000	00000	00000	00000	00000	00000	00000	00000	00000	00000	00032	00000	00000	25000	25.01.22.25	00000					✓
00033	00000	00000	00000	00000	00000	00000	00000	00000	00000	00000	00000	00033	00000	00000	25000	25.01.22.25	00000					✓
00034	00000	00000	00000	00000	00000	00000	00000	00000	00000	00000	00000	00034	00000	00000	25000	25.01.22.25	00000					✓
00035	00000	00000	00000	00000	00000	00000	00000	00000	00000	00000	00000	00035	00000	00000	25000	25.01.22.25	00000					✓
00036	00000	00000	00000	00000	00000	00000	00000	00000	00000	00000	00000	00036	00000	00000	25000	25.01.22.25	00000					✓
00037	00000	00000	00000	00000	00000	00000	00000	00000	00000	00000	00000	00037	00000	00000	25000	25.01.22.25	00000					✓
00038	00000	00000	00000	00000	00000	00000	00000	00000	00000	00000	00000	00038	00000	00000	25000	25.01.22.25	00000					✓
00039	00000	00000	00000	00000	00000	00000	00000	00000	00000	00000	00000	00039	00000	00000	25000	25.01.22.25	00000					✓
00040	00000	00000	00000	00000	00000	00000	00000	00000	00000	00000	00000	00040	00000	00000	25000	25.01.22.25	00000					✓
00041	00000	00000	00000	00000	00000	00000	00000	00000	00000	00000	00000	00041	00000	00000	25000	25.01.22.25	00000					✓
00042	00000	00000	00000	00000	00000	00000	00000	00000	00000	00000	00000	00042	00000	00000	25000	25.01.22.25	00000					✓
00043	00000	00000	00000	00000	00000	00000	00000	00000	00000	00000	00000	00043	00000	00000	25000	25.01.22.25	00000					✓
00044	00000	00000	00000	00000	00000	00000	00000	00000	00000	00000	00000	00044	00000	00000	25000	25.01.22.25	00000					✓
00045	00000	00000	00000	00000	00000	00000	00000	00000	00000	00000	00000	00045	00000	00000	25000	25.01.22.25	00000					✓
00046	00000	00000	00000	00000	00000	00000	00000	00000	00000	00000	00000	00046	00000	00000	25000	25.01.22.25	00000					✓
00047	00000	00000	00000	00000	00000	00000	00000	00000	00000	00000	00000	00047	00000	00000	25000	25.01.22.25	00000					✓
00048	00000	00000	00000	00000	00000	00000	00000	00000	00000	00000	00000	00048	00000	00000	25000	25.01.22.25	00000					✓
00049	00000	00000	00000	00000	00000	00000	00000	00000	00000	00000	00000	00049	00000	00000	25000	25.01.22.25	00000					✓
00050	00000	00000	00000	00000	00000	00000	00000	00000	00000	00000	00000	00050	00000	00000	25000	25.01.22.25	00000					✓

Configuration

⚙️

🔍

✓

General

	Device ID	PEI	DECT Auth. co.	European	Device no.	Device type	Reg. user ID	Subscribed	Tasks
SIPMS	D0001	10345 0031039 *		✓	Fixed	D0001		✓	Tasks Configure ✓ Delete ✗ Filter ✗ Subscription ✗ Wildcard subscription ✗ Select columns ✗

	D0003	10345 0031039 *		✓	Fixed	D0003		✓	
	D0004	03286 DECT129 3		✓	Fixed	D0004		✓	
SIPMS	D0007	00100 0000000 2		✓	Fixed	D0004		✓	
	D0008	00100 0000000 2		✓	Fixed	D0004		✓	
	D0009	00100 0000000 2		✓	Fixed	D0004		✓	
DECT base stations WLAN	D0001	00100 0000002 5		✗	Fixed	D0001		✗	
	D0002	00100 0000003 8		✗	Fixed	D0002		✗	
	D0004	00100 0000005 6		✗	Fixed	D0001		✗	
Video devices	D0005	00100 0000006 8		✗	Fixed	D0002		✗	
	D0006	00100 0000007 7		✗	Fixed	D0003		✗	
	D0008	00100 0000009 1		✗	Fixed	D0005		✗	
DECT phones	D0009	00100 0000010 3		✗	Fixed	D0006		✗	
	D0009	00100 0000011 5		✗	Fixed	D0006		✗	
	D0009	00100 0000012 5		✗	Fixed	D0006		✗	
Users	D0002	00100 0000013 5		✗	Fixed	D0009		✗	
	D0002	00100 0000014 5		✗	Fixed	D0009		✗	
	D0002	00100 0000015 5		✗	Fixed	D0009		✗	
Conference rooms	D0007	00100 0000016 5		✗	Fixed	D0003		✗	
	D0007	00100 0000017 *		✗	Fixed	D0003		✗	
	D0007	00100 0000018 5		✗	Fixed	D0003		✗	
System features	D0007	00100 0000019 1		✗	Fixed	D0007		✗	
	D0007	00100 0000019 1		✗	Fixed	D0007		✗	
	D0022	100100 0000019 1		✗	Fixed	D0007		✗	
Licenses	D0022	100100 0000019 1		✗	Fixed	D0007		✗	

Note: Use the **Select columns** dialog (see section 6.10.9) to display the desired DECT phone device data.

The following tasks can be performed:

- **Configure:** Configure selected DECT phone device dataset (see section 6.10.6).
- **Delete:** Delete selected DECT phone device dataset (see section 6.10.8).
- **Subscription:** Start DECT phone subscription (see section 6.10.7).
- **Wildcard subscription:** Start DECT phone wildcard subscription (see section 6.10.7).
- **Select columns:** Select parameter columns to be shown in table (see section 6.10.9).
- **Filter:** Filter DECT phone datasets shown in table for string set in filter mask (see section 6.10.10).

6.10.4 DEVICE DETAIL PANEL

The **Device detail** panel is used for configuration/showing of device settings and creation of new DECT phone datasets.

To open the **Device detail** panel,

- choose one of the commands in the task bar on the right of the **DECT Phones** panel (**Configure**)

or

- double-click on the appropriate device entry in the device table

The **Device detail** panel contains the different parameter groups sorted in tabs. The tabs displayed depend on the current mode and the panel from which the DECT phone detail panel was invoked.

- **Overview** panel (configuration and monitor mode): The DECT phone detail panel contains all tabs listed below.

- **User** panel (configuration mode): The DECT phone detail panel contains all tabs but not **DECT**.
- **Device** panel (configuration mode): The DECT phone detail panel contains only **DECT**.

6.10.4.1 "General" tab

The **General** tab contains general settings for the DECT phone dataset.

- **Name:** The DECT phone user name (up to 20 characters).
- **Number:** The DECT phone telephone number, up to 31 characters (1234567890#azAz+~!\$%&/'=?*&). Please be aware that only ~!\$%&/'=?*& and "0" to "9" can be dialed with a DECT phone.
- **Description 1** and **Description 2:** Free text comments with up to 16 characters each.
- **Login/Additional ID:** The additional ID can be used as a mean for data search within wildcard subscription (because of the IPEI is not configured which selects the data otherwise).
- **PIN, PIN confirmation:** A user PIN to be entered during user login.
Note: The attempt to set the user PIN to an empty string sets the PIN to the default value "0000".

6.10.4.2 "SIP" tab

The **SIP** contains the SIP authentication parameters for the DECT phone dataset.

- **Authentication user name:** The SIP Authentication user name is optional but recommended. It represents the name which will be used during SIP registration and authentication. If no name is given the number will be used by default.
- **Password, Password confirmation:** The password will be used during SIP registration and authentication. Enter the appropriate data in these fields.
- **VIP:** Enable this option if the registration of this user should be prioritized (default off). VIP users will be registered first. For more information on prioritized registration see section 7.20.5.
- **Used for visibility checks:** Enables the use of this user account to check the availability of the IPBX (e.g., in fail over situations). See section 7.20.7 for more information on this feature.
- **Fixed port:** Specifies the port used explicitly for SIP signaling. If set to 0, an automatically calculated port is used. The default is 0. See section 3.17 for more information on this feature.

6.10.4.3 "Incoming calls" tab

The **Incoming calls** tab allows you to set device-specific settings for auto-answering incoming calls. Default values for all parameters are inherited from global settings (see section 6.5.4.7).

6.10.4.4 "Conference" tab

The Conference tab contains parameters for three-way conferencing for the DECT phone dataset.

- **Auto answer:** Enables or disables auto-answer on incoming calls.
 - **Microphone mute:** Enables or disables microphone muting when incoming calls are automatically answered.
 - **Warning tone:** Enables or disables warning tone on incoming call. A short ringtone is played if there are no active calls. If there is an active call in a "barge in" situation, the ringing will be in-band
 - **Allow barge in:** Allows/disallows "barge-in" on existing calls.
- **Server type:** Determines the conference service to be used for three-way conferencing. Possible values are:
- **None:** Disables 3-way conferencing.
 - **Global:** The OMM system setting is used (default).
 - **Integrated:** The integrated conference server is used.
 - **External:** An external conference server is used.
 - **External – Blind Transfer:** An external conference server is used (e.g., MIVoice Business). The initiation of the conference is signaled as a blind transfer to the destination specified in the URL parameter.
 - **URL:** Address of an external conference server (field only activated if the server type is "External").
- For more information see section 7.20.7.

6.10.4.5 "DECT" tab

The DECT tab contains parameters DECT configuration of the DECT phone dataset. When configuring a device (see 6.10.3), only the **DECT** tab is shown in the DECT phone detail panel:

- **IPEI:** This optional setting is the DECT phone IPEI number. On a Mitel 142 / Mitel 142d DECT phone, the IPEI can be found via the following path of the device menu: **Main menu > Phone settings > System**. On a Mitel 600 DECT phone, the IPEI can be found in the **System** device menu. Consult the DECT phone's user guide for further information.
- **DECT authentication code:** The DECT authentication code is used during initial DECT subscription as a security option and can be set here for each DECT phone device separately (DECT phone-specific DECT authentication code). If no DECT phone-specific DECT authentication code is set, the system-wide DECT authentication code is used.
- **Encryption:** If the encryption feature is enabled for the whole system (in the **System settings** menu, see section 6.5.1), you can de-activate the DECT encryption for this device.

Please note: The DECT phone device must support DECT encryption which is not a mandatory feature.

175

6.10.4.6 "Messaging" tab

The Messaging tab contains parameters for the OM Integrated Messaging and Alerting service on the DECT phone dataset.

If a user is created independent of any specific configuration, the **Sending messages** and **Sending vCards** features are enabled by default.

- **Subscribe to PARI only:** Ensures that the DECT phone subscribes to the PARI code (of a single OMM, within a Dual Homing installation) and not to the SARL. This option is only available for fixed user device pairs, and must be set before subscription takes place. For this reason, you should set the parameter immediately when creating the DECT phone device.
- **Delete subscription:** This option is only available when configuring an existing DECT phone. If this option is activated, the subscription data will be deleted which also requires a re-subscription of the DECT phone device.
- **Sending messages permission:** If this option is enabled, the DECT phone can send messages (if this function is supported by the device).
Note: For further information see the document SIP-DECT OM Integrated Messaging & Alerting Application Installation, Administration & User Guide.
- **Sending vCards permission:** Allows the user to send personal directory entries as a vCard message from the DECT phone to other users (if this function is supported by the device).
- **Receiving vCards permission:** If this option is enabled, all received vCard messages are automatically processed and written into the personal directory of the DECT phone (if this function is supported by the device).
- **Locating permission:** This option applies to Mitel 600 DECT phones only. If this option is enabled, the user is allowed to determine the location of other DECT phones. The main menu of the Mitel 600 DECT phones provides an extra **Locating** menu entry for this function.
- **Tracking:** If this option is enabled, the operator of the OM Locating application is able to use the constant tracking feature for the DECT phone. Note that this feature consumes more of the DECT phone's battery power, because it activates a DECT base station update if the device roams and is not in communication. You also cannot enable this feature, if the **DECT locatable** option is disabled
- **DECT locatable:** If this option is enabled, the DECT phone is locatable. Either with the OM Locating application or by querying it's location from other DECT phones.

6.10.4.7 "Locating" tab

The Locating tab contains parameters for configuring location parameters for the DECT phone.

6.10.4.8 "Additional services" tab

The Additional services tab contains additional optional parameters for the DECT phone dataset.

176

- **SOS number:** User-specific SOS number that is dialed automatically if the SOS key on the DECT phone is pressed.
 - **ManDown number:** User specific "Man down" number that is dialed automatically if a Man down event happens. This event is triggered by the sensor of a Mitel 600 DECT phone.
 - If no individual SOS or Man down number is configured for a DECT phone, the number of the appropriate alarm trigger will be used as calling number in case of a SOS or Man down event. Please see /31/ for details.
 - **Voice mail number:** The number that will be automatically called as soon as a voice mail call is initiated on the Mitel 600 DECT phone. If there is no individual voice mail number configured in this field, then the system-wide voice mail number is used (see also the **System setting** menu, section 6.5.1). If there is no voice mail number configured (neither the individual nor the system-wide) or another DECT phone type is used, then the voice mail number must be configured locally in the DECT phone.
 - **Keep personal directory:** Activate this option, to keep the personal directory data in the DECT phone if the user logs out.
 - **External:** A user data set can either be provisioned on an external user data server or locally in the OMM database. To provide an easy way to change the provisioning storage of user data sets, the user data sets can be moved from an external user data server into the local OMM database and vice versa.
- Deactivate the **External** option if you want to move user data sets from an external user data server into the local OMM database.
- External to internal transformation rules:** To change a user data set from an external user data server to an internally provisioned one, the following conditions must be applied to the data set:
- external provisioned on an external user data server
 - user data set device relation must not be "fixed"
 - external provisioned on an external server
 - user data set device relation must not be "fixed"
 - an external user data server must be available
- Internal to external transformation rules:** To change a user data set from local OMM database to an external user data server provisioned one the following conditions must be applied for the data set:
- **Video stream permission:** Activate this option to allow video streaming on the Mitel 602 DECT phone. See section 7.28 for details on this feature.
 - **Hot desking supported:** Enables or disables Hot desking functionality (for SIP-DECT systems using the MiVoice Business platform). Only available for users with a dynamic association with a DECT phone. When enabled, the user is registered as a Hot Desking user on the MiVoice Business call server. See section 3.14 for details on this feature.
 - **Auto logout on charging:** Enables or disables automatic user log out on the DECT phone when the device is placed in the charger cradle. Only available for users with a dynamic association with a DECT phone. Note that the **Silent charging** option must be enabled on the DECT phone.

- **Authenticate logout:** Enables or disables whether it is necessary for the user to authenticate in case of logout.

6.10.4.9 "User monitoring" tab

The User monitoring tab contains parameters to configure the user-specific parameters for the User Monitoring feature. For a description of the parameters which can be set in the **User monitoring** tab, see the description in section 7.29.7.2.

6.10.4.10 "Configuration data" tab

The Configuration data tab allows you to assign a Configuration over Air (CoA) profile to a DECT phone user. See section 7.23 for more information on this feature.

- **Profile id:** Specifies the CoA configuration profile you want to assign to the DECT phone user.

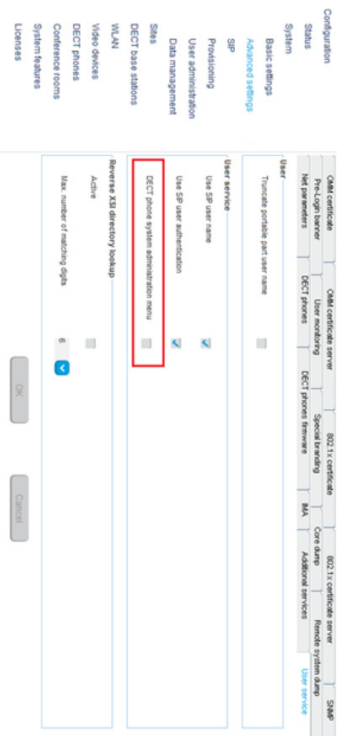
Note: When a CoA profile is deleted, its profile ID assignment to DECT phone users remains. If a new CoA profile is created and acquires this profile ID (the IDs are assigned in sequential order), any DECT phone users with the old profile ID are automatically assigned to the new CoA profile.

If you do not want the DECT phone users to automatically inherit any new CoA profile that has the profile ID, you must remove the profile ID assignment manually.

6.10.4.11 "User service" tab

The User service tab allows you to specify parameters related to user authentication for XSI services.

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



Please note: As of SIP-DECT 8.0, the access to the system configuration through the DECT phone UI is disabled by default to improve system security. The user can enable the menus through OMP.

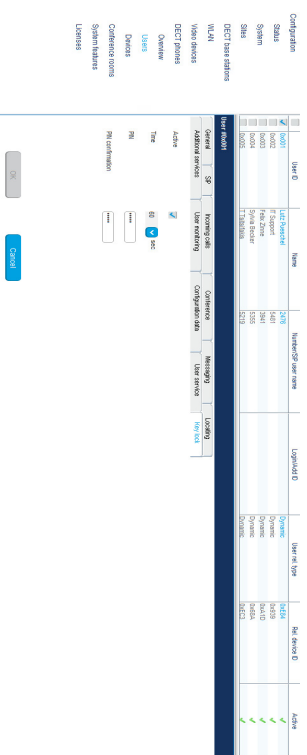
6.10.4.12 "Key lock" tab

The Mitel 600d DECT phone family offers an optional PIN to protect the DECT Phone. For SIP-DECT 8.0 and the DECT phone SW 7.2, the key lock PIN is managed by the OMM to improve the shift worker support and the roaming between OMMs in a MOM setup.

The local DECT phone key lock PIN settings are suppressed if the DECT phone is subscribed with a SIP-DECT system.

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

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



The update to SIP-DECT 8.0 causes a reset of the DECT phone key lock PIN to default "0000".

6.10.5 CREATING DECT PHONE DATASETS

Creating DECT phone datasets is only possible in Configuration Mode. You can create the fixed DECT phone dataset or only the DECT phone user data.

To create a DECT phone dataset, do the following:

- 1 Click **Create** under the Task list on the right-hand side of the **DECT Phones** window.
 - In the **Overview** submenu you can create a fixed DECT phone dataset (with combined user and device data).
 - In the **Users** submenu you can create an unbound user. This user can login and log out on any configured device.

The DECT phone detail panel opens and provides tabs where the DECT phone data must be entered.

- 2 Configure the DECT phone, see parameter description in section 6.10.4.
- 3 Press the **OK** button.

6.10.6 CONFIGURING DECT PHONE DATASETS

Configuring DECT phone datasets is only possible in Configuration Mode. To configure an existing DECT phone dataset proceed as follows:

- 1 Select a DECT Phone from the table, and click **Configure** under the Task list on the right-hand side of the **DECT Phones** window.
 - In the **Overview** submenu you can configure the whole DECT phone dataset (user and device data).
 - In the **Users** submenu you can configure the DECT phone user data.
 - In the **Device** submenu you can configure the DECT phone device data.
- 2 The DECT phone detail panel opens.
- 2 Change the DECT phone dataset as desired, see parameter description in section 6.10.4.
- 3 Press the **OK** button.