

5.4.1.12 Software update URL

With SIP-DECT 6.0 or later, DECT base stations in small SIP-DECT systems (~10 RFPs) can obtain their software image from the DECT base station hosting the OMM, if they have no valid URL from which to load their software (see section 7.9.2 for information on URL syntax). If the OMM is running on a DECT base station, the OMM DECT base station delivers the software to the connected DECT base stations.

The new software image for the OMM DECT base station can be provided as an `iprf3G.dnd` file on an external file server. You configure the URL for the software image in this section.

- **Configure specific source:** Enables the specific URL for downloading the `iprf3G.dnd` file (as opposed to the ConfigURL, which points to an external file server for all configuration and resource files).
- **Protocol:** Specifies the protocol used to fetch the software image file.
- **Port:** Specifies the port of the external file server.
- **Server:** Specifies the IP address or name of the external file server.
- **User name:** Specifies the user name to authenticate on the external file server.
- **Password:** Specifies the password to authenticate on the external file server.
- **Password confirmation:** Confirms the password to authenticate on the external file server.
- **Path:** Specifies the location of the software image file on the external file server.
- **Use common certificate configuration:** Enables the use of the system-wide certificate validation settings for this URL, as configured on the **System** -> **Provisioning** -> **Certificates** page (see section 5.4.2).

5.4.1.13 System dump

A system dump is a file that holds information about the OpenMobility Manager and all connected DECT base stations. With the Remote System Dump feature, a system dump is transferred to a remote server. You can configure a specific destination, otherwise the system ConfigURL is used. The system dump is generated manually by pressing the **Dump** button or automatically at the specified time.

Please ensure that the files server used allows writing or creation of system dumps.

- **Trigger:** Enables the automatic generation of a system dump time every day at the time specified in the **Time** field.
- **Time:** The time of day the system automatically generates a system dump file (only activated if the **Trigger** checkbox is enabled).
- **Dump:** Immediately triggers the generation of a system dump file.
- **Configure specific source:** Enables the specific URL for transferring the system dump file (as opposed to the ConfigURL, which points to an external file server for all configuration and resource files).
- **Protocol:** Specifies the protocol used to transfer the system dump file.
- **Port:** Specifies the port of the external file server.
- **Server:** Specifies the IP address or name of the external file server.
- **User name:** Specifies the user name to authenticate on the external file server.

- **Password:** Specifies the password to authenticate on the external file server.
- **Password confirmation:** Confirms the password to authenticate on the external file server.
- **Path:** Specifies where the system dump file is stored on the external file server.
- **Use common certificate configuration:** Enables the use of the system-wide certificate validation settings for this URL, as configured on the **System** -> **Provisioning** -> **Certificates** page (see section 5.4.2).

5.4.1.14 Core dump URL

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

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

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

5.4.1.15 Net parameters

To allow the prioritization of Voice Packets and/or Signaling Packets (SIP) inside the used network, the IP parameter **ToS** (Type of Service) should be configured.

- **ToS for voice packets:** Determines the type of service (ToS resp. DiffServ) byte of the IP packet header for all packets that transport RTP voice streams.
- **ToS for signalling packets:** Determines the type of service (ToS resp. DiffServ) byte of the IP packet header for all packets related to VoIP signaling.
- **TTL (Time to live):** Determines the maximum hop count for all IP packets.

5.4.1.16 Date and time

If OMM DECT base stations start an SNTP client, the date and time of the configured time zone is synchronized with the Mitel DECT 142 / Mitel 142d and Mitel 600 DECT phones. The date and time will be provided by the OMM to these DECT phones if they initiate a DECT location registration. The rules for a time zone can be configured in the **Time zones** menu (see section 5.4.5).

- **NTP server:** The NTP servers used for time synchronization.

- **Time zone:** Specifies the time zone in which the OMM is operating. This feature is exclusively available on the OMM DECT base station. On PC-OMM configurations, the PC time and time zone is used.

5.4.1.17 Restarting the OMM

You can restart the OMM by clicking on the **Restart** button in the top right corner of the **System Settings** page.

1 Click on the **Restart** button.

The **Restart** dialog window opens.

2 In the **Restart** dialog window, set the following options:

- **Discard OMM DB and configuration files:** Specifies whether OMM database and configuration data is removed from the DECT base station, including the data retrieved from RCS. Local IP configuration remains unaffected. This parameter is only available on an OMM DECT base station.
- **Reset OMM RFP(s) to factory defaults:** Specifies whether all data is removed from the DECT BASE STATION including the OMM database, configuration files and local IP configuration.

Note: Both options also affect the standby OMM.

3 Click **OK**.

A Restart web page opens and displays a progress bar. The login page is loaded automatically if the OMM is reachable again.

5.4.1.18 Updating the OMM

An **Update** button is available on the **System settings** web page. Pressing the **Update** button forces the DECT base stations to check for new software and initiates the software update. For more details about updating the OMM see the section 7.14.

5.4.2 "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. For more information on this feature, see section 7.8.1.

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

5.4.2.1 Current configuration file URL

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

5.4.2.2 System credentials

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

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

5.4.2.3 Configuration file URL

- **Active:** Enables or disables the configuration file URL feature.
- **Protocol:** Specifies the protocol to be used to fetch the configuration files.
- **Server:** Specifies the IP address or name of the provisioning server.
- **Port:** Specifies the provisioning server's port number.
- **Path:** Specifies the path to the configuration and resource files on the provisioning server.

5.4.2.4 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.

5.4.4.2.5 Autonomous SW update check by OMM

When this is activated, the RFP-OMMs (active, standby) checks autonomously for a new software, whenever a RFP re-configuration (DHCP renew, OM Configurator, ipdetect.cfg, <MAC>.cfg) happens.

5.4.2.6 Maximum delay

This parameter specifies the maximum time (in minutes) and the OMM waits past the scheduled time before starting the reload of configuration and firmware files. The Maximum Delay has only an effect, when "Daily automatic reload of configuration and firmware files" is activated.

5.4.4.2.7 Calculated time of delay

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

5.4.2.8 Certificates

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

- **Trusted certificate(s):** Read-only; specifies the number of trusted certificates deployed on the OMM.
- **Local certificate chain:** Read-only; specifies the number of local certificate chains deployed on the OMM.
- **Private key:** Read-only; specifies whether a private key file is deployed on the OMM.
- **Private key password:** Specifies a password for the private key file.
- **Password confirmation:** Confirms the password for the private key file.
- **Delete certificates/key:** Allows the user to delete existing certificates and private key files from the OMM.
- **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.
- **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.

5.4.4.2.9 Manual import

You can overwrite the hard coded OMM certificate by importing trusted certificates, a local certificate chain and a private key file.

- **Import PEM file with:** Specifies the type of file to be imported (trusted certificate, local certificate, or private key).
- **Import PEM file:** Specifies the location of the file to be imported.

5.4.4.3 "SIP" MENU

The SIP settings cover all global settings matching the SIP signaling and the RTP voice streams. Parameters are grouped under the tabs described below.

Status
System settings
Provisioning
SIP
OK Cancel
Base settings
Proxy server 10.103.25.11
Registrar port 5060
Registrar server 10.103.25.11
Registrar port 5060
SNMP 3000
Registration period sec
Optional Invitable User-Agent URL
Outbound proxy server
Outbound proxy port
T transport protocol UDP
Local UDP/TCP port range - 5060
Local TLS port range - 5061
Advanced
Explicit AVDP subscription
User agent ratio
User agent ratio - compatible mode

5.4.4.3.1 Basic settings

You can set basic SIP settings for the system on the Basic settings menu.

- **Proxy server:** IP address or name of the SIP proxy server. If a host name and domain are used for the proxy server parameter, ensure that a DNS server and a domain are specified for your SIP-DECT system via DHCP or the OM Configurator tool.
- **Proxy port:** SIP proxy server's port number. Default is "5060". To enable DNS SRV support for proxy lookups, use a value of "0" for the proxy port. In case that TLS is used, the value shall be changed to "5061".
- **Registrar server:** IP address or name of the SIP registrar. Enables the DECT phones to be registered with a registrar. If a host name and domain are used for the proxy server parameter, ensure that a DNS server and a domain are specified for your SIP-DECT system via DHCP or the OM Configurator tool.
- **Registrar port:** SIP registrar's port number. Default is "5060". To enable DNS SRV support for registrar lookups, use a value of "0" for the registrar port. In case that TLS is used, the value shall be changed to "5061".
- **Registration period:** The requested registration period. In seconds, from the registrar. Default is "3600".
- **Globally Routable User Agent (URL):** Enables support for Globally Routable User-Agent URIs (GRUUs). GRUUs provide a way for anyone on the Internet to route a call to a specific instance of a SIP User-Agent.
- **Outbound proxy server:** This setting is optional. You can enter the address of the outbound proxy server in this field. All SIP messages originating from the OMM are sent to this server. For example, if you have a Session Border Controller in your network, then you would normally set its address here.
- **Outbound proxy port:** The proxy port on the proxy server to which the OMM sends all SIP messages. Default is "5060". In case that TLS is used, the value shall be changed to "5061".
- **Transport protocol:** The protocol used by the OMM to send/receive SIP signaling. Default is "UDP".
- **Local UDP/TCP port range:** The port range to be used for DECT users when UDP/TCP is used as the transport protocol. The default is 5060 – 5060.
- **Local TLS port range:** The port range to be used for DECT users when TLS is used as the transport protocol. The default is 5061 – 5061.

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

5.4.3.2 Advanced settings

You can set more advanced SIP settings for the system on the Advanced settings menu.

- **Explicit MMI subscription:** Some SIP Call Managers such as the Asterisk support Message Waiting Indication (MWI) based on /21/. An MMI icon is displayed on a DECT phone (Mitel DECT 142 / Mitel 142d, Mitel 600) if the user has received a voice message on his voice box which is supported by the SIP Call Manager. If **Explicit MMI subscription** is enabled, the OMM sends explicit for each DECT phone an MMI subscription message to the Proxy or Outbound Proxy Server.
- **Explicit MMI subscription period:** The requested duration in seconds, before the MMI subscription times out. SIP-DECT re-subscribes to MMI before the subscription period ends.

- **User agent info:** If this option is enabled, the OMM sends information on his version inside the SIP headers *User-Agent/Server*.
- **Dial terminator:** The dial terminator is configurable (up to 2 characters; "0" – "9", "*", "#", or empty). The default dial terminator is "#". A dial terminator is necessary if digit treatment shall be applied on outgoing calls and overlapped sending is used.
- **Registration failed retry timer:** Specifies the time, in seconds, that the OMM waits between registration attempts when the registration is rejected by the registrar. Default is "1200" seconds.
- **Registration timeout retry timer:** Specifies the time that the OMM waits between registration attempts when the registration timed out. Default is "180" seconds.
- **Session timer:** The interval, in seconds, between re-INVITE requests sent from the OMM to keep a SIP session alive. The minimum session timer is 90 seconds and the maximum is 86400 seconds. The default is 0 (i.e., feature is disabled).
- **Transaction timer:** The time period in milliseconds that the OMM allows a call server (proxy/registrar) to respond to SIP messages that it sends. If the OMM does not receive a response in the time period designated for this parameter, the OMM assumes the message as timed out. In this case the call server is recorded to the blacklist. Valid values are "4000" to "64000". Default is "4000" milliseconds.
- **Blacklist time out:** The time period in minutes an unreachable call server stays in the blacklist. Valid values are "0" to "1440". Default is "5" minutes.
- **Incoming call timeout:** The time, in seconds, that the OMM waits for a user to accept an incoming call before rejecting the call automatically. The minimum time is 30 seconds and the maximum is 300 seconds. The default is 180 seconds.
- **Determine remote party by:** You can select the SIP header from which the remote party information (user id and display name) should be determined. If **P-Asserted-Identity** (default value) is selected but no such header is received, a fallback to the mandatory **From / To** header will be done. This feature can be configured by choosing one of the two values.

Note: When SIP-DECT receives a SIP header **P-Asserted-Identity** in ringing state during an outgoing call, the included identity information (e.g. SIP display name and user-id) will be displayed on Mitel 600 and Mitel 142d phones as new call target. In addition, the outgoing call log of the Mitel 600 and Mitel 142d phones will be updated with the new given identity.

- **Multiple 180 Ringing:** If this feature is deactivated, the OMM sends out only one 180 Ringing response for an incoming call if PRACK is not supported. If this feature is activated, the OMM retransmits multiple times the 180 Ringing response for an incoming call if PRACK is not supported. This ensures that the calling side receives a 180 Ringing response in case of packet losses on the network. By default this feature is active.
- **Semi-attended transfer mode and Refer-to with replaces:**

Semi-attended transfer mode	Refer-to with replaces	Behavior
Blind	No	The semi-attended transfer is handled as a blind transfer. The phone sends CANCEL before REFER for semi-attended transfer.

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

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

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

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

- **SIP contact matching:** Specifies the method used by the OMM to match the Contact header in a SIP response to a REGISTER request. Available options are:
 - **URI** – Match user username, domain name, phone IP and port and transport
 - **IP only** – Match the IP address of the phone only
 - **Username only** – Match the username only
 - **IP and user name** – Match the IP address of the phone and the username

The default is URI.

- **Call reject state code (user reject):** Specifies the SIP state code sent as response when the user rejects an incoming call by pressing the "Reject" option. Valid values are "400" to "699". The default is "486"
- **Out of range state code (device unreachable):** Specifies the SIP state code sent as response when the incoming call is rejected because the DECT phone is unreachable (e.g., the DECT phone is out of range or out of battery power). Valid values are "400" to "699". The default is 486.

5.4.3.3 RTP settings

You can set RTP parameters in the RTP settings section.

- **RTP port base:** Each RFP needs a continuous port area of 68 UDP ports for RTP voice streaming. The RTP port base is the start port number of that area. Default is "16320".

- **Preferred codec 1 – 4:** Specifies a customized codec preference list which allows you to use the preferred codecs. The Codec 1 has the highest and Codec 4 the lowest priority.

Note: With SIP-DECT Release 3.0 or higher the voice codecs G.722 (wideband), G.711 u-law, G.711 A-law and G.729 A are supported. The previously supported codec G.723 is no longer available.

5.4.3.4 DTMF settings

You can set DTMF parameters in the DTMF section.

- **Preferred packet time** (10, 20 or 30 msec): Determines the length of voice samples collected before sending out a new RTP packet. A small setting improves voice quality at the expense of data transmission overhead. Default is "20" milliseconds.
 - **Silence suppression:** Enables automatic silence detection in the RTP voice data stream to optimize the data transfer volume.
 - **Receiver precedence on CODEC negotiation:**
 - The ON (option is enabled) setting means: The CODEC selection for incoming SDP offers based on the own preference order list. The first entry in the OMM preferred codec list matching an entry in the incoming SDP offer will be selected.
 - The OFF (option is disabled) setting means: The CODEC selection based on the preference order list of incoming SDP offer. The first entry in the incoming order list matching an entry of OMM preferred codec list will be selected. This is the default and is as recommended in RFC 3264.
 - **Eliminate comfort noise packets:** If this feature is activated, then comfort noise packets are removed from the RTP media stream which causes gaps in the sequence numbers. This can be used if comfort noise packets e.g. in G.711 media streams disturb voice calls in certain installations.
 - **Single codec reply in SDP:** If this feature is activated, the OMM answers to SDP offers (included in the SIP signalization) with a single codec in the SDP answer.
- 5.4.3.4 DTMF settings**
- You can set DTMF parameters in the DTMF section.
- **Out-of-band:** Used to configure whether DTMF Out-of-band is preferred or not.
 - **Method:** The OMM supports the following DTMF Out-of-band methods:
 - **RTP** (RFC 2833)
 - Transmits DTMF as RTP events according to RFC 2833 (/14/) after the payload type negotiation via SIP/SDP. If the payload type is not negotiated, "in band" will be used automatically.
 - **INFO**
 - The SIP INFO method is used to transmit DTMF tones as telephone events (application/dtmf-relay). This setting should be used if RFC 2833 is not supported.
 - **BOTH**
 - **DTMF telephones events** are send according to RFC 2833 and as well as SIP INFO method. **Note:** Possibly, the other party recognizes events twice.
 - **Payload type:** If the **Out-of-band** option is enabled, this setting specifies the payload type which is used for sending DTMF events based on section 3.1, reference /14/.

5.4.3.5 Registration traffic shaping

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

Some providers use a keep-alive mechanism based on SIP registration renewals for remote endpoints that are behind a Network Address Translator (NAT), as in an IP-Centrex solution. The keep-alive mechanism keeps the pinhole open and ensures communication between the remote endpoint and the Session Border Controller (SBC).

The OMM feature that spreads the registration renewals to prevent bottlenecks in large systems is not compatible with the keep-alive mechanism. With SIP-DECT 6.0 or later, you can disable the spread mechanism and configure a registration renewal timer to allow support for the NAT feature.

- **Simultaneous registrations:** The maximum number of simultaneously started registrations.
- **Waiting time:** The waiting time between a registration finish and starting the next registration in ms (0-1000ms).
- **Spread registration renewals:** If set to ON, the OMM distributes all DECT phone registration renewals automatically, between half-way through the registration period and 30 seconds before expiry. This prevents registration renewal bottlenecks. Default is ON.
- **Renewal timer:** The time, in seconds, during which the OMM renews DECT phone registrations before expiry (if "Spread registration renewals" is set OFF). The DECT phone automatically sends registration renewals half-way through the registration period, unless the half-way point is greater than the threshold value. For example, if the threshold value is set to 60 seconds and the registration period is 600 seconds, the phone sends the renewal REGISTER message 60 seconds prior to the expiration of the registration period. If the registration period is 100 seconds, the renewal is sent at the half-way point as $(100/2) < 60$. Valid values are 0 to 2147483647. Default is 15.

5.4.3.6 Supplementary Services

The Supplementary Services section contains various parameters related to call control.

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

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

- Only one line is handled for each user (except for an SOS call 0F0F1)
- If a user presses the "R" key or hook-off key in a call active state, a DTMF event is sent to the IPBX via SIP INFO including signal 16 (hook-flash). All Hook-flash events are sent in every case via SIP INFO, independent of the configured or negotiated DTMF method during call setup. All other key events are sent via the configured or negotiated DTMF method.
- The OMM-based call features "Call waiting", "Call Transfer", "Brokerling" and "Hold" are no longer supported.
- This setting becomes active on DECT phones with the next DECT "Locating Registration" process (can be forced by switching the DECT phone off and on again).
- **Automatic ringback on hold call:** Enables or disables a ringback on the loudspeaker if the B party of the active line releases the call. The ringing begins after the call release timeout interval (see description below).
- **Call transfer by hook on (Mitel 600):** Enables call transfer via the hook key on a Mitel 600 DECT phone (in addition to call transfer via menu).
- **Call transfer by hook on (Mitel 142):** Enables call transfer via the hook key on a Mitel 142 DECT phone (in addition to call transfer via menu).
- **Truncate Caller Indication after *:** If the user name info in SIP to-/from/contact headers or p-asserted-identity is extended by a suffix, which is separated by a semicolon, this suffix is truncated before the username is printed to call displays or DECT phone internal call logs.
- **SIP reRegister after 2 active OMM failover:** Enables SIP re-registration of all users from the active OMM when the system detects two active OMMs (in a failover scenario).
- **Call release timeout:** Specifies the time, in seconds, after which an active line is released if the DECT phone user has not gone on-hook after the B party on an active call releases the call.
- **Hold call release timeout:** Specifies the time, in seconds, after which the active line is released if the DECT phone user has not switched to a held line (when the B party on a held call releases the call).
- **Failed call release timeout:** Specifies the time, in seconds, after which an active line is released if the called party is busy, or the call is rejected for any reason.

5.4.3.7 Intercom Push-to-talk-Outgoing calls/Incoming calls

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

Outgoing calls

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

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

Incoming calls

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

5.4.3.8 Security

You can set security-specific settings in the Security section.

- **Persistent TLS keep alive timer active:** When enabled and "Persistent TLS" is selected as transport protocol, the OMM sends out keep alive messages periodically to keep the TLS connection open.
- **Persistent TLS keep alive timer timeout:** Specifies the time pattern, in seconds, in which the OMM sends out keep-alive messages. Valid values are "10" to "3600". Default is "30" seconds.
- **Send SIPs over TLS active:** When enabled, and "TLS" or "Persistent TLS" is selected as transport protocol, the OMM uses SIPs URIs in the SIP signaling. Default is "ON".
- **TLS-Authentication:** When enabled and "TLS" or "Persistent TLS" is selected as transport protocol, the OMM validates the authenticity of the remote peer via exchanged certificates and the configured "Trusted certificates". Default is "ON".
- **TLS-Common-Name-Validation:** When enabled and "TLS authentication" is selected, the OMM validates the "Alternative Name" and "Common Name" of the remote peer certificate against the configured proxy, registrar and outbound proxy settings. If there is no match, an established TLS connection will be closed immediately.
- **Trusted certificate(s):** The number of imported trusted certificates (read-only).
- **Local certification chain:** Indicates the number of imported certificates in the local certificate chain (read-only).
- **Private key:** Indicates whether the OMM has a private key file (read-only).
- **Delete certificates/key:** Allows deletion of all certificates and the local key.

5.4.3.9 Certificate server

Set the parameters on the Certificate server tab to automatically import Trusted, Local Certificates and a Private Key files from an external server for SIP signaling.

- **Active:** Enables the feature.
- **Protocol:** Specifies the preferred protocol (FTP, TFTP, FTPS, HTTP, HTTPS, SFTP)
- **Server:** Specifies the name or IP address of the external file served.
- **User name:** Specifies the user name to authenticate against the external file server.
- **Password:** Specifies the password to authenticate against the external file server.
- **Password confirmation:** Confirms the password to authenticate against the external file server.
- **Path:** Specifies the path on the file server to the certificate files.
- **Trusted certificate file:** Specifies the name of the PEM file on the specified server, including the trusted certificates.
- **Local certificate file:** Specifies the name of the PEM file on the external server including the local certificate or a certificate chain.
- **Private key file:** Specifies the name of the PEM file on the external server including the local key.
- **Port:** Specifies the certificate server's port number.
- **Use default port:** If selected, the default port associated with the selected protocol is used.
- **Use common certificate configuration:** Enables the use of the system-wide certificate validation settings, as configured on the **System** -> **Provisioning** -> **Certificates** page (see section 5.4.2.5).

5.4.3.10 Manual import

Set the parameters for manual import of certificate keys.

- **Import PEM file with:** Allows selection of the kind of certificate/key to be imported.
- **Import PEM file:** Specifies the file to be imported.
- **Import:** Triggers an import of the file

5.4.4 "USER ADMINISTRATION" MENU

After initial installation or after removing the configuration file, the OMM Web service is accessible via a built-in user account with user "omm" and password "omm".

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

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

These settings are case sensitive and can be changed on the **User administration** web page.

Status

System

System Settings

Provisioning

SIP

User Administration

Time Zones

SNMP

DB Management

Event Log

Sites

Base Stations

DECT Phones

WLAN

System Features

Licenses

Info

User Administration

OK

Cancel

Account type

Local user account

Full access

Active

User name

admin

Old password

Password

Password confirmation

Password aging

None

- **Account type:** Select the account type you wish to change.
 - **Active:** This setting applies to the **Read-only access** account. Using this account, a user is not allowed to configure any item of the OMM installation. The account can be deactivated.
 - **User name:** If desired, enter a new user name.
 - **Old password:** Related to the "Full Access Account", to change the password the old password must be typed in again.
 - **Password, Password confirmation:** Enter the appropriate data in these fields.
- The OMM has several rules to check the complexity of the new password. A new password will not be accepted if:

- the new password is not five or more characters long
- the new password does not contain characters from at least three of the following groups: lower case, upper case, digits or other characters
- the new password has 50% or more of the same character ('World1111' or 'W101r11d1')
- the new password contains one of the following items (either upper or lower case as well as forward or backward):
 - account name
 - host name (IP address)
 - old password
 - some adjoining keystrokes (e.g. 'qwert')
- **Password aging:** A timeout for the password can be set. Select the duration, the password should be valid.

5.4.5 "TIME ZONES" MENU

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

Status	Time Zones
System	Default
System Settings	119 Time Zones
Provisioning	
SIP	
User Administration	
Time Zones	
SNMP	
DB Management	
Event Log	
Sites	
Base Stations	
DECT Phones	
WLAN	
System Features	
Licenses	
Info	

Name	ID	UTC difference	DST
Asia Central West	APC	+1 h	✗
Asia Central East	APD	+2 h	✗
Asia East	APF	+3 h	✗
Asia East	APG	+4:30 h	✗
Asia West	APV	0 h	✗
Asia	AK	-8 h	✓
Arctic Islands	AKV	-10 h	✓
Armenian Standard Time	APU	+4 h	✗
Asia UTC-4	AS4	+4 h	✗
Asia UTC-5	AS5	+5 h	✗
Asia UTC-6	AS6	+6 h	✗
Asia UTC-7	AS7	+7 h	✗
Asia UTC-8	AS8	+8 h	✗
Asia UTC-9	AS9	+9 h	✗
Adonis	ATL	+4 h	✓
Adonis East	ATL	+10 h	✓

The date and time are provided by the OMM to the Mitel 142 and Mitel 600 DECT phones if the DECT phone initiates a DECT location registration. This will be done in the following cases:

- Subscribing to the OMM
- Entering the network again after the DECT signal was lost
- Power on
- Silent charging feature is active at the phone and the phone is taken out of the charger
- After a specific time to update date and time

The following tasks can be performed on the **Time zones** page:

- Changing the time zones (see section 5.4.5.1)
- Resetting time zones (see section 5.4.5.2)

5.4.5.1 Changing Time Zones

It is possible to change the time zone rules for maximal five time zones. Changed rules are marked with a bold time zone name in the table. The changes are saved in the configuration file and are restored after each OpenMobility Manager startup.

- 1 To change the settings of a time zone, click on the  icon left behind the time zone entry. The **Configure time zone** dialog opens.

- 2 You can change the standard time and the daylight savings time (DST) of a time zone.

If the time zone has no DST, only the UTC difference can be configured.

For the DST both points of time (begin of standard time and begin of daylight savings time) must be specified exactly. Therefore a certain day in the month or a certain week day in a month can be used.

5.4.5.2 Resetting Time Zones

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

5.4.6 “SNMP” MENU

To manage a larger RFP network, an SNMP agent is provided for each RFP. This will give alarm information and allow an SNMP management system (such as “HP Open View”) to manage this network. On the **SNMP** page of the OMM Web service you configure the SNMP service settings.

You can configure the following SNMP parameters using the OMM web service:

General settings

- **Read-only community:** The SNMP community string forms a password that is sent by the SNMP management system when querying devices. The query is answered only if the SNMP community string matches. You may use “public” as a default keyword for read-only access.
- **System contact:** Enter a descriptive text that typically is displayed in the SNMP management software.

Trap handling

Activate the checkbox behind the **Trap handling** section to enable this feature.

- **Trap community:** This community string is used if the SNMP agent informs the SNMP management system about events (traps).
- **Trap host IP address:** Enter the IP Address that the SNMP agent uses to send traps.

Further notes

- The RFP needs an initial (one-time) OMM connection to receive its SNMP configuration. In case of a reset, this configuration does not change. Changing the SNMP configuration on the OMM forces all agents to be reconfigured.
- The agent does not support MIB-II write access, SNMPv2-MIB read/write access, NET-SNMP-MIB read/write access, NET-SNMP-AGENT-MIB read/write access and SNMPv3.
- For background information on using SNMP with the SIP-DECT system see section 7.19.

5.4.7 “DB MANAGEMENT” MENU

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

The OMM database can be

- manually imported from the Web browser's file system or from an external server (see section 5.4.7.1),
- manually exported to the Web browser's file system or to an external server (see section 5.4.7.2),
- automatically exported to an external server when configuration modifications are done (see section 5.4.7.3).

Note: The OMM database is saved in a compressed file in a proprietary format. Any modification of this file outside the OMM is not allowed.

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

5.4.7.1 Manual Database Import

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

In the **Manual import** section of the **Database management** page enter the following:

- 1 **Protocol:**
 - To import a database from the Web browser's file system the protocol **FILE** must be selected.
 - To import a database from an external server select the preferred protocol (e.g. HTTP).
 - 2 **Server:** IP address or the name of the external server.
 - 3 **User name, Password** (in case of import from an external server): If necessary, enter the account data of the server.
 - 4 **File:** Path and file name which include the OMM database. If you have selected the **FILE** protocol, the **Browse** button is displayed and you can to select the file from the file system.
 - 5 **Use common certificate configuration:** Enables the use of the system-wide certificate validation settings, as configured on the **System** -> **Provisioning** -> **Certificates** page (see section 5.4.2.5).
 - 6 Press the **Load** button.
- Before the OMM accepts the database, a validation check is performed. If the database is verified as valid, the OMM will be reset to activate the new database.

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

5.4.7.2 Manual Database Export

In the **Manual export** section of the **Database management** page enter the following:

- 1 **Protocol:** Select the preferred protocol. If you want to export the database to the Web browser's file system, select the **FILE** setting.

- 2 **Server:** Enter the IP address or the name of the server.
- 3 **User name, Password:** If necessary, enter the account data of the server.
- 4 **File:** Enter the path and filename where the database is to be saved.
- 5 **Use common certificate configuration:** Enables the use of the system-wide certificate validation settings, as configured on the **System** -> **Provisioning** -> **Certificates** page (see section 5.4.2.5).
- 6 Press the **Save** button.

5.4.7.3 Automatic Database Export

The automatic database export feature allows an automatic database backup to an external server for each configuration modification. If this feature is activated, the OMM transfers a backup file to a configured external server any time configuration changes occur (e.g. DECT phone subscription). The backup file overwrites any existing backup files.

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

In the **Automatic export** section of the **Database management** page enter the following:

- 1 **Active:** Activate this option to enable the automatic export feature.
- 2 **Protocol:** Select the preferred protocol.
- 3 **Server:** Enter the IP address or the name of the server.
- 4 **Port:** Enter the port of the server.
- 5 **User name, Password:** If necessary, enter the account data of the server.
- 6 **File:** Enter the path and filename where the database is to be saved.
The OMM writes the database into a file on the external server with following name convention:
<yyymmdd>_<system_name>_<PARK>_<omn_conf.gz
If the system name contains non-standard ASCII character then these character are replaced by "_".
- 7 **Use common certificate configuration:** Enables the use of the system-wide certificate validation settings, as configured on the **System** -> **Provisioning** -> **Certificates** page (see section 5.4.2.5).
- 8 Press the **OK** button.

5.4.8 "EVENT LOG" MENU

The **Event log** page displays important event information on OMM system functions, e.g. security aspects. A more detailed system log is available by configuring the **Syslog** function in the **System settings** menu (see section 5.4.1.9).

Status	Event Log			Event
System	Clear			
System Settings				
Provisioning	Severity	Count	Time (UTC)	
SIP	3	1	20160625 18:31:57:379	AOI: [2110nm] Alert Information: Security SUBSCRIPTION in OMM with MCM is connected and does not handle reduction on two unwanted results
User Administration	3	1	20160625 18:31:57:377	AOI: [2110nm] Alert Information: MCM request sent: DECTSubscriberInfo -> OFF
Time Zones	3	1	20160625 18:31:54:367	AOI: [2110nm] Alert Information: MCM request sent: MLCARD (broadcast) (multiple)
SNMP	3	1	20160625 07:04:11:513	AOI: [2110nm] Disconnected alert (10, 10, 31, 100) because of dropped alert timeout timer
DB Management	2	1	20160623 06:55:04:715	AOI: [2130nm] Permission: Warning: disabled: No License
Event Log	2	1	20160623 06:55:04:715	AOI: [2130nm] Permission: Warning: disabled: No License
	2	1	20160623 06:55:04:716	AOI: [2130nm] Permission: Warning: disabled: No License
Sites	2	1	20160623 06:55:04:405	AOI: [2130nm] Permission: Warning: disabled: No License
DECT Phones	2	1	20160623 01:17:25:442	AOI: [2130nm] Alert Information: MCM moved to MCM: device not located in the OMM
WLAN	2	1	20160622 22:02:20:627	Pg. 3 of 3 RFPs connected
	2	1	20160622 22:02:19:246	AOI: [2110nm] Alert Information: MCM moved to MCM: device not located in the OMM
System Features	3	1	20160622 22:02:16:526	AOI: [2110nm] Alert Information: MCM request sent: DECTSubscriberInfo -> OFF
Licenses	3	1	20160622 22:02:16:557	AOI: [2110nm] Permission: Warning: disabled: No License
Info	2	1	20160622 22:02:16:557	AOI: [2110nm] Permission: Warning: alert: disabled: No License
	2	1	20160622 22:02:16:557	AOI: [2110nm] Permission: Warning: alert: disabled: No License

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

5.5 “SITES” MENU

DECT base stations can be grouped into different sites. A site consists of the following parameters:

- **ID**: Identification number of the site.
- **Name**: The name of the site.
- **Hi-Q Audio Technology, SRTP, Enhanced DECT Security**: Indicates whether (one of) these features are enabled for the site.
- **Base stations**: The number of base stations assigned to the site.

Sites				
New				
2 Sites				
ID	Name	Hi-Q audio technology	SRTP	Enhanced DECT security
1	default	✗	✓	✗
3	Real RFP	✗	✓	✗
				Base Stations 10

You can perform the following tasks:

- create a new site (see section 5.5.1)
- edit a site (see section 5.5.2)
- delete a site (see section 5.5.3)

5.5.1 CREATING A NEW SITE

- 1 On the **Sites** page press the **New** button.
The **Configure site** dialog opens.

- 2 In the **Configure site** window, specify values for the following parameters:

- **ID**: Enter the identification number of the site. A value between 1 and 250 is possible. If no value is given, the OMM selects the next free ID.
- **Name**: Enter the name of the site.
- **Hi-Q audio technology, SRTP, Enhanced DECT security**: Enable or disable these capabilities.
 - Only RFP 35/36/37 IP and RFP 43 WLAN are supported where these features are enabled.
 - You can mix new RFP types with older RFP 32/34 and RFP 42 WLAN base stations where these features are disabled.

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

5.5.2 EDITING A SITE

You can change the name of an existing site:

- 1 On the **Sites** page click on the  icon left behind the site entry.
The **Configure site** dialog opens.
- 2 Change the site name.
- 3 Press the **OK** button.

5.5.3 DELETING A SITE

Note:

Only sites without assigned base stations can be deleted. At least one site must remain, so the last site cannot be deleted.

To delete an existing site:

- 1 On the **Sites** web page click on the  icon left behind the site entry.
The **Delete site** dialog opens.
- 2 Press the **Delete** button.

5.6 “BASE STATIONS” MENU

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

Base Stations

New

Capturing unconfigured DECT base stations

Send by DECT clusters

Capture allowed

Save

DECT Cluster 1: 2 Base Stations

ID	Name	MAC address	IP address	HW type	Site	RPN	Reflective environment	Connected	Active
0000	SITE RFP1	00:30:42:10:10:80	10.37.78.31	RFP 35	3	00	✓	✓	✓
0001	SITE RFP2	00:30:42:10:20:A2	10.37.78.32	RFP 35	3	01	✓	✓	✓

12 Base Stations

DECT Cluster 5: 10 Base Stations

ID	Name	MAC address	IP address	HW type	Site	RPN	Reflective environment	Connected	Active
0002	airpu	01:02:03:04:05:06	-	RFP 32	1	02	✗	✗	-
0003	airpu	01:02:03:04:05:07	-	RFP 32	1	03	✗	✗	-
0004	airpu	01:02:03:04:05:08	-	RFP 32	1	04	✗	✗	-
0005	airpu	01:02:03:04:05:09	-	RFP 32	1	05	✗	✗	-

10 Base Stations

You can select a sorting criterion for the RFP table. In the **Sorted by** field, select the criterion:

- DECT clusters:** The base stations are sorted by clusters. All used clusters are displayed in the navigation bar on the left side. The OMM base station is marked with a bold font.
- WLAN profiles:** The base stations are sorted by WLAN profile (see section 5.8).
- Sites:** The base stations are sorted by sites (see section 5.5). All used sites are displayed in the navigation bar on the left side. The OMM base station is marked with a bold font.

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

- ID:** An internal number that is used to manage the base station.
- Name:** Indicates the base station's name (see section 5.6.3).
- MAC address:** Indicates the base station's MAC address (see section 5.6.3).
- IP address:** Shows the current IP address of the RFP. The IP address may change over time by using dynamic IP assignment on the DHCP server.
- HW type:** When the base stations connect to the OMM, they submit their hardware type. The hardware type is displayed in this column. If an error message is indicated in this column, there is a mismatch between the base station and the OMM software version (see section 5.6.2).
- Site:** Indicates the site the base station is assigned to (see section 5.5).
- RPN:** Shows the Radio Fixed Part Number that is currently used by the RFP.
- Reflective environment:** Indicates if the base station is operated in a reflective environment (see section 5.6.3).
- Connected:** Indicates if the base station is connected to the OMM (see section 5.6.1).
- Active:** Indicates if the base station is active (see section 5.6.1).

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

- Create and change base stations (see section 5.6.3).

- Capture base stations (see section 5.6.4).
- Delete base stations (see section 5.6.5).

5.6.1 BASE STATION STATES

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

Synchronous

ID	Name	MAC address	IP address	HW type	Site	RPN	Reflective environment	Connected	Active
0000	License RFP 3	00:30:42:00:0F:33	192.168.112.33	RFP L32	1	01	✗	✓	✓

The RFP is up and running. The RFP recognizes and is recognized by other RFPs in its cluster through its air interface and delivers a synchronous clock signal to the DECT phones.

Asynchronous

ID	Name	MAC address	IP address	HW type	Site	RPN	Reflective environment	Connected	Active
0000	License RFP 3	00:30:42:00:0F:33	192.168.112.33	RFP L32	1	01	✗	✓	✗

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

Searching

ID	Name	MAC address	IP address	HW type	Site	RPN	Reflective environment	Connected	Active
0000	License RFP 3	00:30:42:00:0F:33	192.168.112.33	RFP L32	1	01	✗	✗	✗

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

Inactive

ID	Name	MAC address	IP address	HW type	Site	RPN	Reflective environment	Connected	Active
0000	License RFP 3	00:30:42:00:0F:33	192.168.112.33	RFP L32	1	-	-	✓	-

The RFP has connected to the OMM but the air interface has not been switched on yet. For any RFP with activated DECT functionality this phase should last only for a few seconds after starting up the RFP. If this state lasts longer this may indicate a hardware failure.

Not connected

ID	Name	MAC address	IP address	HW type	Site	RPN	Reflective environment	Connected	Active
0000	License RFP 3	00:30:42:00:0F:33	-	RFP L32	1	-	-	✗	-

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

Software Update available

ID	Name	MAC address	IP address	HW type	Site	RFP environment	Reflective	Connected	Active
1	0000 License RFP 3	00:30:42:00:0F:33	192.168.1.12.3	RFP 1.2.2	1	01			

The RFP is connected to the OMM. The OMM has found new software on the TFTP server. The RFP is waiting for the OMM to initiate a reboot. In the meantime is the RFP fully operational.

5.6.2 OMM / RFP SOFTWARE VERSION CHECK

When the DECT base stations connect to the OMM, they submit their software version. If this version differs from the OMM software version and the versions are incompatible, the RFP connection attempt is rejected. This could happen when using several TFTP servers with different OpenMobility software versions. In this case, the RFP is marked with an error message. Moreover a global error message is displayed on the RFP list web page if at least one version mismatch has been found.

5.6.3 CREATING AND CHANGING BASE STATIONS

- 1 To configure a new RFP, click the **New** button on the **Base Stations** page.
To change the configuration of an existing RFP click on the icon left beside the base station entry.
The **New base station** (or the **Configure base station**) dialog opens.
- 2 Configure the base station (see parameter descriptions below).
- 3 Click **OK**.

Please note: DECT regulatory domain, WLAN regulatory domain and WLAN profile must be configured first. Otherwise DECT and/or WLAN cannot be enabled.

The following parameters can be set in the **New base station** and the **Configure base station** dialogs:

General settings

- **MAC address:** Each RFP is identified by its unique MAC address (6 bytes hex format, colon separated). Enter the MAC address (as it appears on the back of the base station chassis).
- **Name:** For easier administration each RFP can be associated with a location string. The location string can hold up to 20 characters.
- **Site:** If several sites exist (see section 5.5), select the site the RFP is assigned to.

DECT settings

The DECT functionality for each RFP can be switched on/off.

- **DECT cluster:** If DECT is active the RFP can be assigned to a cluster.
- **Preferred synchronization source:** Activate this checkbox if the RFP should be used as synchronization source for the other RFPs in the cluster. For background information on RFP synchronization see section 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 the RFP base stations 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 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" attribute is switched on. Therefore this is used when problems caused by metal reflections are detected.

WLAN settings

The WLAN section applies to RFPs of the type "RFP 42 WLAN" and "RFP 43 WLAN" only. For details about WLAN configurations please see section 7.18.

RFP 42 WLAN and RFP 43 WLAN have different WLAN parameters, which are configurable in the RFP configuration dialog.

- Activation check box: Enables or disables the WLAN function for this RFP.
- **WLAN profile:** Select the desired profile from the list. This applies all settings made in the respective WLAN profile to the current RFP. For information on configuring WLAN profiles see section 5.8.1.

Please note: WLAN settings are only configurable if the RFP has been connected at least once to detect the hardware type and a proper WLAN profile is configured (see also section 5.8.1). WLAN cannot be enabled in the **New DECT base station** dialog if the hardware type is unknown.

The following settings are not applied by the WLAN profile. Configure these settings for each DECT base station individually.

- **Antenna diversity** (RFP 42 WLAN only): This option should generally be activated so that the AP (Access Point) can automatically select the antenna with the best transmission and reception characteristics.
- **Antenna** (RFP 42 WLAN only): If **Antenna diversity** is switched off, this setting determines the antenna that is used for transmitting or receiving WLAN data.
- **802.11 channel:** Determines the WLAN channel used by the current RFP. The channel numbers available are determined by the WLAN **Regulatory domain** setting on the **System settings** page.
- **Output power level** (default: "Full"): Determines the signal power level used by the RFP to send WLAN data. You may limit the power level to minimize interferences with other WLAN devices. The actual power level is also capped by the WLAN **Regulatory domain** setting on the **System settings** page.
- **HT40** (RFP 43 WLAN only): High throughput mode with 40 MHz bandwidth increases data rate up to 300 MBit/s.

5.6.6.4 CAPTURING DECT BASE STATIONS

Base stations that are assigned to the OMM by DHCP options or OM Configurator settings may connect to the system.

- 1** On the **Base Stations** page, press the **Start** button below the "Capturing unconfigured DECT base stations" caption.

The page is updated with the MAC addresses of those base stations that attempted to register with the OMM (unregistered RFPs).

Note: These entries are not actually stored, and are lost after an OMM reset.

- 2** By clicking on the edit icon  of the appropriate base station, you can add further data and store the base station (see section 5.6.3).

5.6.6.5 DELETING DECT BASE STATIONS

To delete an existing DECT base station:

- 1 On the **Base Stations** page, click on the  icon left beside the RFP entry. The **Delete base station?** dialog opens showing the current configuration of this RFP.
- 2 Click the **Delete** button.

Please note: The RFPs bound to a license (License RFPs) cannot be deleted. The License RFPs are displayed in the list with a license icon  instead of the trash icon. For further information on licenses see section 3.32).

5.7 “DECT PHONES” MENU

The **DECT Phones** page provides an overview of all configured DECT phones sorted by their number. To keep the list concise, the complete list is split up into sub lists containing up to 100 DECT phones. You can move back and forth in increments of 100 DECT phones.

Status

System

Sites

Base Stations

DECT Phones

WLAN

System Features

Licenses

Info

DECT Phones

New

Import

Search

Subscription with configured PEs

Shift

Wireless subscription

2 min

Shift

Display name

Number/SP user name

PGI

Subscribed

Download

🔍 🔍 🔍 Adipen Widenmyer Adipen Widenmyer Adipen Widenmyer	2075	0268 0677032-4	✓	-
	6241	0268 0677066 -		

Peak: 1110059420842

Subscription allowed: ✗

Auto-raise on subscription: ✗

The table provides information on the DECT phones and their status in several columns:

- **Display name:** Indicates the DECT phone name.
- **Number/SIP user name:** Indicates the internal call number of the DECT phone.
- **IPEI:** Indicates the DECT phone IPEI.
- **Subscribed:** Indicates if the DECT phone is subscribed to the system.
- **Download:** This column is only displayed if the "Download over Air" feature is started successfully and provides information about the download status of the DECT phone software (see section 7.20).

DECT phone software (see section 7.20).

Note: All DECT phone data that are configured as unbound (split into DECT phone and user data) are also listed at the OM Web service when a user is logged in at the DECT phone, but they cannot be deleted or changed. This is indicated by the  and  icons. Unbound DECT phones where no user is logged in are not displayed on the **DECT phones** page.

The following tasks can be performed on the **DECT Phones** page:

- create and change DECT phones (see section 5.7.1)
- import DECT phone configuration files (see section 5.7.2).
- subscribe DECT phones (see section 5.7.3)
- delete DECT phones (see section 5.7.4)
- search within the DECT phone list (see section 5.7.5)

5.7.1 CREATING AND CHANGING DECT PHONES

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

- 2 Configure the DECT phone (see parameter descriptions below).
- 3 Press the **OK** button.

The following parameters can be set in the **New DECT phone** and the **Configure DECT phone** dialog:

General settings

- **Display name:** The name parameter represents the SIP Display Name field. This parameter is optional but recommended.
- **Number/SIP user name:** The number is the SIP account number or extension for the DECT phone.
- **IPEI:** This optional setting is the DECT phone IPEI number. On a Mitel DECT 142 / Mitel 142d DECT phone, the IPEI can be found via the following path of the DECT phone menu: **Main menu > Phone settings > System**. On a Mitel 600 DECT phone, the IPEI can be found in the **System** DECT phone 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 separately (DECT phone-specific DECT authentication code). This parameter is optional. If no DECT phone-specific DECT authentication code is set, the system-wide DECT authentication code is used.
- **Login/additional ID:** The additional ID can be used as a mean for data search within wildcard subscription (because of the IPEI is not configured which selects the data otherwise).
- **Delete subscription:** This option is only available when configuring an existing DECT phone (in the **Configure DECT phone** dialog). If this option is selected, the DECT phone will be unsubscribed.
- **SOS number, ManDown number:** SOS and ManDown are calling numbers which will be automatically called as soon as an SOS or ManDown event happens. If no individual SOS or ManDown number is configured for a DECT phone, the number of the appropriate alarm trigger will be used as a system-wide calling number in case of a SOS or ManDown event. Please see 3/1/ for details.
- **Voice mail number:** The voice mail number is the number which 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 5.4.1.). 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.
- **Number used for visibility checks:** Provides phone number or SIP user name used for standby OMM visibility checks.

SIP authentication

- **User name:** The SIP Authentication user name is optional but recommended. It represents the name 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.

5.7.2. IMPORTING DECT PHONE CONFIGURATION FILES

A set of DECT phones can also be configured in a semi-automatic manner by import of a configuration file.

- 1 On the **DECT Phones** page press the **Import** button.
The **DECT phone enrolment** page opens.
- 2 Select your configuration file and press the **Import** button. For information on the file layout see section 10.1.1.
- 3 A parsing protocol can be read, if you press the referring **Log file** button. All successfully imported data records are presented in a list.
- 4 Select the DECT phones you want to add to the OMM database by selecting the appropriate checkboxes, and click **Add**.
All successfully stored records are marked green in the **Added** column.
- 5 Failed records are marked with a red star.
- 5 To read error hints in the referring log file, press the **Log file** button. Error hints can also be read in a syslog trace.
- 6 To remove imported data entries, activate the check box next to the desired entries. Press **Delete** to remove the selected entries.

5.7.3. SUBSCRIBING DECT PHONES

Preparation by OMM Web service

After adding a DECT phone configuration to the OMM, the DECT phone must be subscribed. The OMM must first be enabled to allow subscriptions from DECT phones. This is done by pressing the following buttons on the **DECT Phones** page.

- **Start** button under the "Subscription with configured IPEI" caption (see section 5.7.3.1). This button enables subscription for the next 24 hours.
- **Start** button and time interval parameter under the "Wildcard subscription" caption. This button enables wildcard subscription for the selected time. After expiry the "subscription with configured IPEIs" is still enabled for 24 hours.

Note: To ease the first installation of a DECT system, the subscription is enabled permanently while at least one DECT phone (with IPEI) is set up in the database and no DECT phone is subscribed. After successful subscription of the first DECT phone the subscription will still be enabled for 24 hours.

Subscription steps, done by DECT phone

After the DECT phone configuration is complete on the OMM and the OMM is allowing new subscriptions, each DECT phone must subscribe to the system.

On each DECT phone, the administrator or user must subscribe to the SIP-DECT system through the **System** -> **Subscriptions** menu. The specific PARK code for the SIP-DECT system should be entered to subscribe to the system.

Please note: The PARK is displayed in the top-right corner of the **DECT Phones** page. Each SIP-DECT deployment has a unique PARK code.

If the administrator configured a global or device-specific DECT authentication code, the administrator/user must enter in the code before the DECT phone subscribes to the system.

For "wildcard subscription", an additional ID may be configured (see sub section Wildcard Subscription).

5.7.3.1 Subscription with Configured IPEI

The DECT phone data to be assigned to the subscribing DECT phone are identified by the IPEI. The identity of a DECT phone (IPEI) is already known by the system before the DECT phone attempts to subscribe. Unknown DECT phones are not allowed to subscribe in this mode.

To enable subscriptions, click the **Start** button under the section **Subscription with configured IPEIs** caption on the **DECT Phones** page.

The OMM allows a subscription of configured but not subscribed DECT phones during the next 24 hours. The administrator must press the Subscribe button again to permit more DECT phones to subscribe to the SIP-DECT system.

Note: Older DECT phones may not offer the possibility to enter an access code (AC). You should always subscribe these DECT phones with configured IPEI to maintain security.

5.7.3.2 Wildcard Subscription

To minimize administration effort, subscription is also possible, if the IPEI is not configured. But because of the loss of further security by IPEI check, this kind of subscription is only allowed within a short default time interval of 2 minutes.

To enable subscriptions, press the **Start** button of the section **Wildcard subscription** on the **DECT phones** page. If necessary, increase the time interval (or refresh subscription permission in time).

The OMM will allow a wildcard subscription during the set time interval. In case of timeout the permission is lost. Only subscription with IPEI remains allowed within the fixed limit of 24 hours.

To achieve a selection of data during subscription (e.g. the user name being assigned to the DECT phone), the field "additional ID" can be set in OMM data. If the OMM receives a valid "additional ID" during subscription, the referring data are assigned to the DECT phone.

If the additional ID is requested for a data record, the DECT phone user must type it. "Additional ID" can be set within the authentication code menu. Please type the R-Key and type the additional ID.

Please note: The input of the additional ID is only possible with Mitel 142 and Mitel 600 DECT phones. The value is not supported on third party GAP phones. If GAP phones are going to subscribe wildcard, the first free DECT phone data record without any additional ID will be assigned.

5.7.4 DELETING DECT PHONES

To delete an existing DECT phone:

- 1 On the **DECT phone** page click on the  icon left beside the DECT phone entry.
The **Delete DECT phone?** dialog opens showing the current configuration of this DECT phone.
- 2 Press the **Delete** button.

5.7.5 SEARCHING THE DECT PHONE LIST

You can use the search function to search for a specific DECT phone in the DECT phone list. The search function allows you to find a DECT phone by a given number or IPEI.

- 1 On the **DECT phones** page click on the **Search** button.
The **Search DECT phone** dialog opens.
- 2 Enter the DECT phone's number or IPEI. At least one parameter must be set. The entered number or IPEI must match exactly with a DECT phone's number or IPEI. If number **and** IPEI are given then a DECT phone must exist in the OMM's database whose number and IPEI match both otherwise the search fails.

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

5.7.6 DISPLAYING USER AND DECT PHONE DATA

You can display a summary of user status and DECT phone configuration in a pop-up window on the **DECT Phone** page. Click the magnifying glass icon beside a DECT phone entry to view the **User/device status & configuration** window.

Note: A configuration and status summary for the DECT phone is also available on the DECT phone under the Administration menu.
The presentation layout is similar to the OMM Web service window, but the DECT phone only displays its own data.

The following table describes the parameters in the **User/device status & configuration** window.

Parameter	Description
User status	
Registered	Current SIP user registration status Yes = registered No = not registered
Registrar server type	Current SIP registrar: Primary or backup SIP registrar (secondary or tertiary)
Registrar server	IP address of the SIP Registrar
Calculated local port	Port number of the SIP Registrar
Silent charging	SIP user's automatically determined client port Current silent charging state Yes = in silent charging mode No = not in silent charging mode
COA data loaded	COA data sent to DECT phone Yes = data has been sent No = no data sent

User configuration data

User Id	Internal system identifier for the user
User real Type	Type of association between the user and DECT phone. Dynamic or fixed.
Name	User's name

Number	SIP user name or number
Description 1	Additional textual description for a user (e.g., department or function)
Description 2	Additional textual description for a user (e.g., department or function)
User lang.	Language setting on the DECT phone
SOS number	Emergency number to be dialed when the SOS key has been pressed
MD number	Emergency number to be dialed when a sensor alarm (Mitel 600 DECT phone) has been initiated
VM number	Voice mail number (dialed by a long press of '1' key on the Mitel 600 DECT phone)
SIP auth. user name	SIP authentication user name
SIP auth. password	SIP authentication password
Fixed local port	SIP user's configured fixed client port (used for SIP registration)
Login/Add ID	ID used for user identification during login procedure at the DECT phone OR ID used for wildcard subscription during DECT phone subscription procedure
PIN	PIN used for user identification during login procedure at the DECT phone ***** = a PIN is set, empty = no PIN is set
External	User data provided by an external provisioning server (<user> cfg) Yes = user data imported from a server No = user data only stored internally in the OMM DB
Permanent	Indicates whether the user is stored in all OMMs in a Multi-OMM Manager (MOM) managed system. Yes = user data is stored in all OMMs in the SIP-DECT system. No = user data only stored in the local OMM (i.e., where the device is currently registered).
VIP	To guarantee a minimum blackout for a very important person (e.g. emergency user) the SIP (re-)registration of such people can be prioritized. Yes = prioritized No = not prioritized
Visibility checks	The OMM standby feature uses an existing SIP account to check the availability of the registrar. Yes = this account is used No = this account is not used
Hot desking supported	Hot desking capability, only available for users with a dynamic association with a DECT phone. Yes = user is registered for hot desking on the call server. No = user is not registered for hot desking on the call server.
Auto logout on charging	A user can be logged out of the device automatically when the Mitel 600 DECT phone is placed in the charger cradle. Yes = automatic logout when put in charger No = no automatic logout
Authenticate logout	User log out requires authentication. Yes = user logout with authentication No = user logout without authentication
Sending messages	User's permissions to send text messages using the Mitel 600 DECT phone Yes = user is authorized to send text messages No = user is not authorized to send text messages

Sending vCards	User's permissions to send vCards using the Mitel 600 DECT phone Yes = user is authorized to send vCards No = user is not authorized to vCards
Receiving vCards	Indicates whether the user accepts received vCards Yes = incoming vCards are accepted No = incoming vCards are not accepted
Video stream perm.	User's permissions to access video using the Mitel 602 DECT phone Yes = user is authorized to access video No = user is not authorized to access video
Locate	User's permissions to locate other users using the Mitel 600 DECT phone Yes = user can locate other users No = user cannot locate other users
Tracking	Tracking forces the Mitel 600 DECT phone to indicate every change of the DECT base station even in idle state Yes = tracking is active No = tracking is inactive
DECT locatable	Permission to locate the user (i.e., through the SIP-DECT locating solution) Yes = locating the user is permitted No = not permitted
Keep personal dir.	The local directory of the Mitel 600 DECT phone is usually the user's personal directory and is cleared at logout. If deleting the directory content is not desirable, this option can be set Yes = local directory is not cleared No = local directory is cleared
Forward mode	Mode of Call diversion or Call forwarding (Off, Immediately, Busy, No answer, Busy & no answer)
Forward time	Time delay in seconds before the incoming call is redirected.
Forward dest.	Destination of the redirected call
Hold ring back time	Time in minutes after which the user wants to be reminded of the connection on hold 0 = Off, no reminder
Call waiting disabled	An incoming call is signaled in-band if the user is otherwise engaged (Call waiting). This feature can be disabled Yes = call waiting is disabled No = call waiting feature is active
Auto answer	Enables or disables auto-answer on incoming calls. If auto answer is enabled, the DECT phone plays a tone to alert the user before answering the call. If auto answer is disabled, the DECT phone treats the incoming call as a normal call.
Microphone mute	Enables or disables microphone muting when incoming calls are automatically answered.
Warning tone	Enables or disables a warning tone to play when the DECT phone receives an incoming call on an active line. A short ringtone is played if there are no active calls. If there is an active call in a "barge in" situation, the ringing will be in-band.
Allow barge in	Allows/disallows how the DECT phone handles incoming calls while the DECT phone is on an active call. When enabled an incoming call takes precedence over an active call, by placing the active call on hold and automatically answering the call. When disabled the DECT phone treats an incoming call like a normal call.
Monitoring mode	SIP-DECT supports a "User Monitoring" feature to check the availability of a user to

	receive calls or messages. On = monitoring feature is active Off = monitoring feature is not activated
Conference server type	User-specific setting of the conference service to be used for three-way conferencing None = three-way conferencing is disabled Global = OMM system setting is used (default) Integrated = integrated conference server is used
Conference server URI	URI for the external conference server
Use CoA profile	ID of the CoA (Central DECT phone configuration over air) profile
Use SIP user name	Uses SIP user name for XSI directory access
Use SIP user auth.	Uses SIP authentication credentials for XSI directory access
User service user name	User name for XSI service (if SIP credentials not used for XSI directory access)
User service auth name	Authentication name for XSI service (if SIP credentials not used for XSI directory access)
User service password	Password for XSI service (if SIP credentials not used for XSI directory access)
Device status	
IPEI	International Portable Equipment Identifier (globally unique identifier of the DECT phone)
HW type	Hardware type of 600 DECT phone or 142d otherwise "unknown"
SW version	Version of the software on the Mitel 600 DECT phone
Subscribed	Subscription status of the DECT phone Yes = DECT phone is subscribed No = DECT phone is not subscribed
Encryption	DECT encryption status Yes = Encryption is enabled No = Encryption is disabled
Capability "Messaging"	Messaging capability of the DECT phone Yes = DECT phone supports messaging No = DECT phone does not support messaging
Capability "Enh. Locating"	Enhanced locating capability of the DECT phone Yes = DECT phone supports enhanced locating No = DECT phone does not support enhanced locating
Capability "Video"	Video capability of the DECT phone Yes = DECT phone supports video No = DECT phone does not support video
Capability "CoA profile"	CoA capability (Central DECT phone configuration over air) of the DECT phone Yes = DECT phone supports CoA No = DECT phone does not support CoA
Device auto-created	Auto-creation occurs when the DECT phone data set is automatically generated in the OMM's database at subscription time. No administrative task is required on the SIP-DECT system to subscribe a DECT phone in this auto-create mode. Yes = DECT phone has been subscribed in auto-create mode No = DECT phone has not been subscribed in auto-create mode

Default CoA profile loaded	A default CoA profile (Central DECT phone configuration over air) can be sent to a 600 DECT phone Yes = a default profile was sent No = no default profile was sent
Device configuration data	
Device ID	Internal system identifier for the DECT phone

5.8 "WLAN" MENU

The **WLAN** menu allows you to manage the wireless LAN function of all WLAN capable RFPs that are connected to the OMM. You can view and change wireless parameters and security settings to adapt the WLAN configuration to suit your needs. You can also check how many and which wireless clients are currently connected. Nevertheless, the WLAN function is only available for base stations of the type RFP 42 WLAN and RFP 43 WLAN.

Note: You cannot activate the WLAN function for the OMM, even if the OMM base station is an RFP 42 WLAN.

For a detailed description on WLAN configuration see the section 7.18.

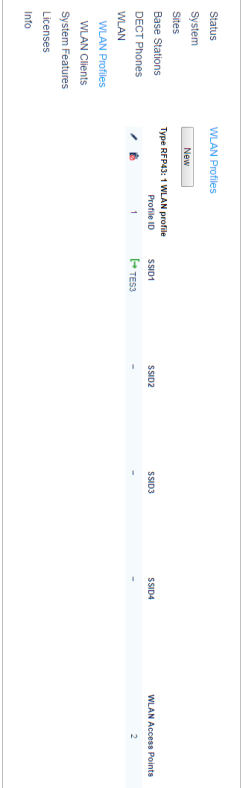
5.8.1 "WLAN PROFILES" MENU

WLAN settings are grouped in WLAN profiles. You need at least one WLAN profile that can be assigned to one or more WLAN-RFPs. You can define more than one WLAN profile, to a maximum of 20 WLAN profiles. You can manage / change the desired WLAN settings for a group of WLAN-RFPs by changing their assigned WLAN profiles. Moreover, you can manage different settings, for example separate WLAN profiles for different buildings, a special WLAN profile for temporary use, or WLAN profile for RFPs only useable by guests.

Note the different WLAN profile types:

RFP type	WLAN profile type
RFP 42 WLAN	RFP 42
RFP 43 WLAN	RFP 43

The **WLAN profiles** menu allows configuration and administration of these WLAN profiles.



You can:

- create and change WLAN profiles (see section 5.8.1.1)
- delete WLAN profiles (see section 5.8.1.2)
- export WLAN profiles (see section 5.8.1.3)

The defined WLAN profiles are then assigned to one or more WLAN base stations (see section 5.8.2). Note, that some device-specific WLAN settings are not part of a WLAN profile, such as the channel and the antenna configuration. These settings are defined separately for each base station (see section 5.6.3).

5.8.1.1 Creating and Changing WLAN Profiles

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

- 1 Navigate to the **WLAN profiles** page. This page shows the number of existing WLAN profiles and a list of available WLAN profiles.
- 2 If you create a new WLAN profile, configure the RFP type first to get the correct input fields. Select the appropriate profile (**RFP 42** or **RFP 43**) from the **WLAN profile type** selection list.
- 3 To add a new WLAN profile, press the **New** button. To change an existing WLAN profile, click on the  icon available on the left of the WLAN profile entry.
The **New WLAN profile** page resp. the **WLAN profile [Number]** page shows the WLAN profile configuration.
- 4 Change the desired settings of the WLAN profile. You need at last to define the ESSID setting. The different settings are explained in detail in the sections below.
- 5 Activate the **Profile active** setting; otherwise the WLAN profile is inactive which de-activates the WLAN function for base stations that are assigned to this WLAN profile.
- 6 Press the **OK** button to apply the settings. If you created a new WLAN profile, you can proceed by assigning the WLAN profile to the desired base stations (see section 5.6.3). If you changed an existing WLAN profile, the settings are applied to the assigned base stations automatically.

The following parameters are available on the **New WLAN profile** page and on the **WLAN profile [Number]** page:

General settings

- **Profile active:** Activate this checkbox to activate the profile. This in turn activates the WLAN function for all RFPs that are assigned to the WLAN profile.
- **SSID:** Enter a descriptive character string to identify the WLAN network (e.g. "OurCompany"). The service set identifier is broadcasted by the RFP within "WLAN beacons" in a regularly interval. The SSID identifies the WLAN network and is visible by all WLAN clients. This is typically used with a scan function, e.g. from a WLAN client that tries to establish a connection. The SSID should not exceed 32 characters and it is advisable not to use unusual characters that may trigger WLAN client software bugs.
- **WLAN tag** (number, 1..4094, default: off): You can separate VoIP and client data traffic (transferred via WLAN) by using different virtual LANs, e.g. to prevent bulk data transfers to interfere with VoIP. To use a separate VLAN for the client data traffic, activate the check box and enter the desired VLAN number (see sections 7.18 and 7.12).

- **Beacon period** (milliseconds, 50..65535, default: 100 ms): Determines the WLAN beacon interval. A higher value can save some WLAN airtime that can be used for data transfers.
- **DTIM period** (number, 1..255, default: 5): Determines the number of beacons between DTIM messages. These messages manage the WLAN wakeup/sleep function e.g. that is critical for battery powered WLAN clients.
- **RTS threshold** (bytes, 0..4096, default: 2346): If a WLAN packet exceeds this threshold, it will be transferred with RTS/CTS handshake. This may improve transfer reliability if several WLANs share the same channel. The default of 2346 byte switches off this function because the IP-MTU is typically only 1500 byte.

- **Fragmentation threshold** (bytes, 0..4096, default: 2346): If a WLAN packet exceeds this threshold, it will be transferred in chunks. This may improve transfer reliability for a weak connection. The default of 2346 bytes switches off this function because the IP-MTU is typically only 1500 byte.
- **Maximum rate** (list of rates in Mbps, 1..54, default: 54): This setting applies to RFP 42 WLAN only. Determines the maximum transfer rate used by the RFP. You can limit the rate to increase the WLAN range, e.g. to prevent WLAN clients in the vicinity of the RFP to disturb distant WLAN clients.
- **802.11 mode** (RFP 42 WLAN selection list: Mixed / 802.11b only / 802.11g only, default: Mixed): Both the older and long-ranged B-Mode and the newer and faster G-Mode are typically supported by WLAN clients. You can change this setting to prevent problems with very old WLAN clients.
(RFP 43 WLAN selection list: 802.11bg / 802.11b only / 802.11g only / 802.11n, default: 802.11bg): On the **RFP 43** profile you can choose additionally 802.11 modes 802.11abg and 802.11n.

Mode	802.11abg	802.11n
Open	yes	yes
WEP	yes	no
WPA v.1 (802.1x + PSK)	yes	no
WPA v.2 (802.1x + PSK)	yes	yes

- **Hidden SSID mode** (on / off, default: off): If switched on, the transmission of the SSID within beacons is suppressed. This in turn requires a more elaborate and manual connection procedure for WLAN clients.
- **Interference avoidance** (on / off, default: off): This setting applies to RFP 42 WLAN only. Enables a WLAN procedure to enhance radio interference avoidance.

Security settings

These settings determine the encryption used for the WLAN connection. Select one of the four modes (Open, WEP, WPA, or Radius). This will activate / gray-out the necessary additional input fields that specify further security settings on the **WLAN profile** page.

- **Open system:** Enable this option to deactivate authentication and encryption ("Hotel mode"). Note, that all data is transferred un-encrypted in this mode, which can be easily eavesdropped with any WLAN equipment.
- **Wired equivalent privacy (WEP):** Enable this option to use the older WEP encryption mode. This mode may be useful, e.g. if your WLAN should support older WLAN clients that do not implement the recommended WPA encryption.
 - **Privacy** (on / off, default: off): De-activate this setting to use no authentication ("Open System") with standard WEP encryption. Activate this setting to use an additional shared key authentication between the RFP and the WLAN client.
 - **Number of tx keys** (number, 1..4, default: 1): The WEP encryption can use a single shared key or multiple shared keys ("key rotation"). Select the number of shared keys, select how to enter a shared key (by default as **Text** or as **Hex value**), and select the **Cipher length** (see **Key settings** below).
 - **Default tx key** (number, 1..4, default: 1): If more than one shared keys is used, you can select the default shared key. You must configure the same default key on the WLAN client.
 - **Key #1 – Key #4:** Enter one or more shared key. The **Cipher length** setting (see **Key settings** below) determines the length of the required input. If you selected to enter as **Text** (see above), input a password with 5, 13, or 29 characters that matches a 64 or 128 bit cipher. If you selected to enter as **Hex value**, you can input a hexadecimal number with 10, 26, or 58 characters (0-9, a-f). Press the **Generate** button to generate a random shared key that matches the current settings.
- **WIFI protected access (WPA):** Enable this option to use the recommended WPA encryption mode.
 - (selection, WPA any / WPA v.1 / WPA v.2, default: WPA any): Select the **WPA Type** version required for WLAN clients. The **WPA any** setting allows WPA v.1 and WPA v.2 to be used concurrently. The **WPA v.1** setting enforces the use of the older RC4-based encryption. The **WPA v.2** setting enforces the use of the stronger AES encryption. You can also change the distribution interval (see **Key settings** below).
 - **802.1x (Radius):** Select this option if your WLAN should use a RADIUS server for WLAN client authentication ("Enterprise WPA" with different username/password combinations per client). You must also specify the (see below). For details about the RADIUS authentication procedure, using the public keys, and importing certificates to the WLAN clients refer to the **Radius settings** documentation of your RADIUS server product.
 - **Pre-shared key:** Select this option to use a single shared key for all WLAN clients (Value setting below). A WLAN client user needs to enter the shared key in order to connect.
 - **Value:** You can enter a shared key as **Text**. Use a longer text sequence with alphanumeric characters and special characters to enhance the shared key strength. A text shared key is case sensitive. Alternatively, the shared key can be entered as **Hex value** (hexadecimal number, 0-9, a-f). Press the **Generate** button to generate a random shared key that matches the current settings.
- **MAC access filters** (on / off, default: off): This setting applies to RFP 43 WLAN only. You can limit WLAN access for WLAN clients with specified MAC addresses. Note, that without encryption this should not be used for security reasons. You can configure a list of MAC addresses that are allowed to connect via the **MAC access filters** tab on the WLAN profile page.

Key settings

- **BSS isolation** (on / off, default: off): In a standard WLAN setup, each WLAN client can contact other WLAN clients. For special purposes (e.g. "Internet café setup"), you may switch on this options to protect WLAN clients from eavesdropping on other WLAN clients.
- **Cipher length** (selection, 64 Bits / 128 Bits / 256 Bits (RFP 42 WLAN only), default: 64 Bits): Determines the key length used for the WEP encryption. Larger bit sequences provide better security but may be unsupported by very old WLAN clients.
- **Distribution interval** (seconds, 1..65535, default: 20): Determines how often the WEP encryption is re-negotiated.

Radius settings

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

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

QoS settings

- **WME** (on / off, WLAN or DiffServ (RFP 42 WLAN only), default RFP 42 WLAN: off/WLAN: default RFP 43 WLAN: off): You can enable the Wireless Media Extensions to prioritize WLAN traffic. The WLAN traffic priority is determined by **WLAN** number or by examining the **DiffServ** data field of IP packets.

SSID – SSID4 Tabs

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

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

Note that some configuration combinations are incompatible with multiple SSIDs. For example, the wireless hardware only manages a single WEP encryption key. Also, some features apply to all defined SSIDs, including the **MAC access filters** list.

You can edit the **MAC access filters** list via the **MAC access filters** tab on the WLAN profile page.

- You can import a prepared list of MAC addresses (*.txt, file, one line per MAC address). Use the **Browse** button to select the file from the file system. Afterwards press the **Import** button.
- To configure single MAC addresses, use the **New** button in the **General settings** section. Enter the address in the following **New MAC access filter** dialog.
- To delete a single MAC address, click on the  icon left behind the address entry. Use the **Delete all** button to delete the entire list.

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

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

5.8.1.2 Deleting WLAN Profiles

To delete an existing WLAN profile:

- 1 You cannot remove WLAN profile that is in use. To remove a currently used WLAN profile, you must select another WLAN profile for all assigned RFPs first (see section 5.6.3).
- 2 On the **WLAN profiles** page click on the  icon next to the profile entry.
- 3 The **Delete WLAN profile?** dialog opens showing a summary of the WLAN profile's configuration. Press the **Delete** button.

5.8.1.3 Exporting WLAN Profiles

To simplify the configuration of wireless devices, you can export SSID configuration to a XML WLAN profile file. To export the configuration, click on the  icon.

On Windows 7 you can use the "netsh wlan add profile filename=xxx" command to import a WLAN configuration. Many other tools to import WLAN configuration files are available for Windows Vista / Windows XP systems (for example wlan.exe from Microsoft).

5.8.2 "WLAN CLIENTS" MENU

The **WLAN clients** page shows the status of all WLAN clients currently connected to the WLAN. This can be used for example for troubleshooting purposes. The display shows the total number of connected WLAN clients and a list of RFPs that are part of the WLAN. For each RFP, the WLAN client connected to the RFP are listed. You can view the **MAC address** and the current **Status** of each WLAN client.

5.9 "SYSTEM FEATURES" MENU

The **System features** menu allows administration of system features concerning call number handling and directory access.

5.9.1 "DIGIT TREATMENT" MENU

A number manipulation is provided by the digit treatment feature for corporate directories that handles both incoming and outgoing calls.

Digit treatment for LDAP directories

A chosen number from an LDAP directory entry is checked against the external prefix pattern and if a pattern matches, it is replaced by the configured internal prefix pattern. Only the best matching rule will be applied.

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

Note: A conversion performed for an LDAP directory entry can be reversed if the rule is also activated for an outgoing call.

Incoming call

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

The result of the conversion is sent to the DECT phone to be displayed and entered in the call log¹.

Outgoing call

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

Note: To support digit treatment and overlap sending, it is necessary to have a dial terminator configured.

The result of the conversion is not sent to the DECT phone to be displayed or entered in the call log².

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

- creating and changing "Digit treatment" entries (see section 5.9.1.1)
- deleting "Digit treatment" entries(see section 5.9.1.2)

5.9.1.1 Creating and Changing "Digit treatment" Entries

- 1 To configure a new entry, click the **New** button on the **Digit treatment** page.

To change the configuration of an existing entry click on the  icon left beside the entry.

The **New digit treatment entry** or the **Configure digit treatment entry** dialog opens.

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

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

Please note: The plus character ("+") can only be dialed and transferred to a call log with a Mitel 6000 DECT phone.

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

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

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

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

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

- 6 Sites:** Specifies the sites for which a rule is applied e.g. "1, 2" (see section 5.5). If set to "0", the rule applies to all sites i.e. the rule will be applied to all calls or corporate directory requests.
- 7** Press the **OK** button.

5.9.1.2 Deleting "Digit treatment" Entries

To delete an existing entry:

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

5.9.2 "DIRECTORY" MENU

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

If there is more than one directory server configured, all are displayed on the DECT phone interface when the user invokes the Central Directory function. The user can choose one of the entries in the list. The name of an entry shown in the list is configured in the OMM when creating the directory server entry. The OMM determines the display order of the directories in the DECT phone menu by the order specified by the administrator.

You can configure up to five external directories. If only one directory server is configured, the name configured in the OMM is ignored, and the directory is accessed directly when the user presses the System softkey on the DECT phone (<=>) or selects the **Central directory** option from the menu.

5.9.2.1 Creating and Changing Directory Entries

You can configure directory entries (or change existing entries) from the **Directory** page (or the **Directory (comp. model)** page for older SIP-DECT systems) in the OMM web interface. Parameters that require configuration depend on the type of directory you are configuring.

To change the configuration of an existing entry click the **Edit icon** () beside the entry, and follow the steps described below to set parameter values.

You can change the order of the directory entries by selecting a directory entry in the list and clicking the up or down arrows in the right panel (under **Tasks**). Changing the order of directory entries in the list changes the order in which they appear on the DECT phone.

To create or edit a directory entry, do the following:

- 1 Select the **Directory** entry in the **System Features** menu (left pane).
- 2 Click **New** on the **Directory** page, or click the pencil icon beside an existing directory entry in the list.
The **New directory entry (or Configure directory entry)** dialog opens.
- 3 Specify values for the directory server as described in the following table. Note that only certain parameters are required, depending on the directory server type.

Parameter	Description	LDAP	XML	XSI
-----------	-------------	------	-----	-----

Parameter	Description	LDAP	XML	XSI
Active	Enables or disables the directory entry on the DECT phone.	✓	✓	✓
Type	Interface type supported by the directory server. Possible values: • LDAP • XML • XSI Enterprise • XSI Enterprise common • XSI Group • XSI Group common • XSI Personal	✓	✓	✓
Name	Name to be displayed for the directory (Latin-1 character set is supported).	✓	✓	✓
Search base	Location in the directory from which the search begins (e.g., "ou=people, o=my.com"). The configuration is valid for all DECT phones that support the LDAP directory feature. To make search requests unique for different users, the search base configuration can include placeholders that are replaced by user-specific values when submitting the LDAP request to a server. The following placeholders are defined: • "<TEL>" (for the user's telephone number) • "<DESC1>" (for the user's "Description 1" attribute) • "<DESC2>" (for the user's "Description 2" attribute) • "SIPProxy" (for the current primary, secondary or tertiary SIP server address); supported for release 6.1 and later	✓		
Search type	Attribute on which searches are performed (Surname or Given name).	✓		✓
Display type	Display mode for search results (Surname , First Name or Given name Surname).	✓		✓
Server search timeout	Interval (in seconds) during which the OMM waits for search results from the LDAP server (1 – 10 seconds).	✓		
Protocol	Transfer protocol used to communicate with the XML or XSI directory server (http or https).		✓	
Server port	Port for the LDAP directory server (default is 389). Note: SSL (default port 689) is not supported. Windows Active Directory Server uses port 3268.	✓		
Server	IP address or FQDN of the directory server.	✓	✓	✓
User name	Name of the account for directory server access, if required.	✓	✓	
Password	Password for directory server access, if required. Note: If no user/password is specified, an anonymous bind takes place. SIP-DECT supports LDAP simple bind.	✓	✓	
Path (and parameters)	URL (with parameters, if required) to the XML directory on the XML directory server.		✓	
Use common certificate configuration	Enables or disables use of the system's certificates (loaded for provisioning purposes) for HTTPS directory access		✓	✓

- 4 Click **OK** to save your changes.

5.9.2.2 Deleting Directory Entries

- 1 To delete an existing directory entry click on the  icon on the left of the entry on the **Directory** page. The **Delete directory entry** dialog opens showing the current configuration of this entry.
- 2 Press the **Delete** button.

5.9.3 “DIRECTORY (COMP. MODE)” MENU

In SIP-DECT 6.2 and later, the underlying database model for directory support in SIP-DECT has changed. To support backwards compatibility, the **Directory (comp. mode)** page provides directory configuration and maintenance for existing SIP-DECT systems with LDAP or XML directory support.

To create or edit a directory entry using the old database model, do the following:

- 1 Select the **Directory (comp. mode)** entry in the **System Features** menu (left pane).
- 2 Click **New** on the **Directory (comp. mode)** page, or click the pencil icon beside an existing entry. The **New directory entry** (or **Configure directory entry**) dialog opens.
- 3 In the **New directory entry** dialog (or the **Configure directory entry** dialog, for existing entries), specify values for the directory server as described in the following table. Note that only certain parameters are required, depending on the directory server type.

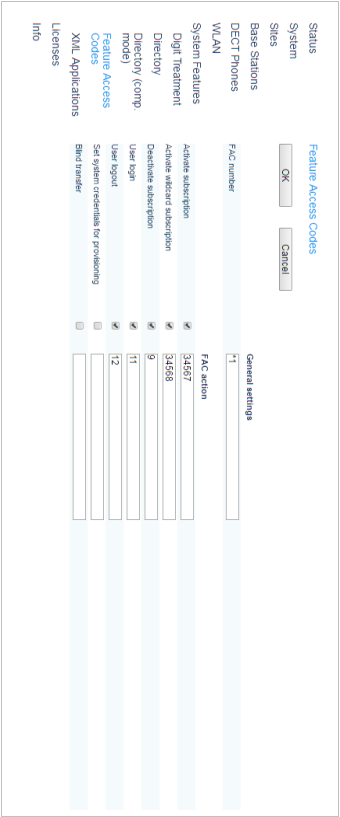
Parameter	Description	LDAP	XML
Active	Enables or disables the directory entry on the DECT phone.	✓	✓
Order	Specify where you want the directory entry to appear in the list.		
Type	Interface type supported by the directory server. Possible values: LDAP or XML.	✓	✓
Name	Name to be displayed for the directory (Latin-1 character set is supported).	✓	✓
Protocol	Transfer protocol used to communicate with the XML directory server (HTTP or HTTPS).		✓
Server name	IP address or FQDN of the directory server.	✓	✓
Server port	Port for the LDAP directory server (default is 389). Note: SSL (default port 689) is not supported. Windows Active Directory Server uses port 3268.	✓	
Search base	Location in the directory from which the search begins (e.g., “ou=people, o=my.com”). The configuration is valid for all DECT phones that support the LDAP directory feature. To make search requests unique for different users, the search base configuration can include placeholders that are replaced by user-specific values when submitting the LDAP request to a server. The following placeholders are defined: • “<TEL>” (for the user’s telephone number) • “<DESC1>” (for the user’s “Description 1” attribute) • “<DESC2>” (for the user’s “Description 2” attribute) • “SIPProxy” (for the current primary, secondary or tertiary SIP server address), supported for release 6.1 and later	✓	
User name	Name of the account for directory server access, if required.	✓	✓
Password	Password for directory server access, if required. Note: If no user/password is specified, an anonymous bind takes place. SIP-DECT supports LDAP simple bind.	✓	✓

Parameter	Description	LDAP	XML
Search type	Attribute on which searches are performed (Surname or Given name).	✓	
Display type	Display mode for search results (Surname, First Name or Given name Surname).	✓	
Server search timeout	Interval (in seconds) during which the OMM waits for search results from the LDAP server (1 – 10 seconds).	✓	
Path (and parameters)	URL (with parameters, if required) to the XML directory on the XML directory server.		✓

- 4 Click **OK** to save your changes.

5.9.4 “FEATURE ACCESS CODES” MENU

Feature access codes (FAC) allow a DECT phone user to perform specific actions on the OMM from any subscribed DECT phone.



To configure the FAC feature, do the following:

- 1 **FAC number:** Enter a unique FAC number.
- 2 Activate the appropriate checkbox(es) to enable the corresponding FAC feature(s). For each enabled FAC feature enter an assigned access code.
 - **Activate subscription:** Activate subscription of the DECT phone.
 - **Activate wildcard subscription:** Activate subscription of the DECT phone (if no IP/EI is configured).
 - **Deactivate subscription:** De-activate DECT phone subscription.
 - **User login:** Log the user into the DECT phone.
 - **User logout:** Log the user out of the DECT phone.
 - **Set system credentials for provisioning:** Allow a user to set system credentials via the Mitel 600 DECT phone.

- **Blind transfer** Initiate a blind transfer from the DECT phone. When a user dials the "Blind transfer" FAC en-bloc (in an active call state) followed by a target number, SIP-DECT initiates a blind transfer to the given target number.

Users can perform the relevant operations by dialing the "FAC number" followed by the "FAC access code" en-bloc from any subscribed DECT phone.

In the example above a subscribed user can activate the OMM DECT subscription by dialing ^{**}134567^{**} en-bloc.

Please note: Overlap sending is not supported for FAC. "FAC number" and "FAC action code" must be entered en-bloc.

FAC functions will be confirmed by an audible indication to the user (in-band tone signals).

5.9.5 "XML APPLICATIONS" MENU

The SIP-DECT XML terminal interface allows external applications to provide content for the user on the Mitel 600 DECT phone. To make the XML terminal interface applications available for the DECT phone user, you must configure the appropriate hooks in the **XML Applications** menu.

When the application hook is enabled in the OMM, Miel 600 DECT phone users can program a softkey with the specific hook (or select the relevant menu option) to trigger the associated action. The side keys on the Miel 600 DECT phones only display icons in idle state. In an active call state, only the two softkeys below the display indicate the active feature.

Status	
System	
Sites	
Blue Stations	
DECT Phones	
WLAN	
System Features	
Digital Treatment	
Directory	
Feature Access Codes	
XML Applications	
Licenses	
Info	

XML Applications

New

15 XML Applications

Name	URL	Action
Call list	http://	
Recall list	http://	
Presence	http://	
Server status	http://	
Action URI	http://	
Failure access codes	http://	
Code completion	http://	
Push call	http://	
Urgent call	http://	
Paging	http://	
Tune	http://	
Call forward	http://	
Call routing	http://	
Call protection	http://	
Voice box	http://	

The following table summarizes the predefined XML application hooks:

Hook	Description	DECT Phone menu
Caller list	Hook to replace the local caller list. You can use this hook to enable the centralized call log feature (MX-ONE systems only).	>>> > Info > Caller List
	"Call log support provided on an external server".	

Hook	Description	DECT Phone menu
	The call logs are located on an external XML server. Each call log action on the DECT phone is requested to the external XML server and the server answers this with XML responses. The content is displayed on the DECT phone for the user. The URL-path in the configuration differs from "CSIntegration/Subject=history" which is an indication for the OMM centralized call log feature.	
Redial list	Hook to replace the local redial list. You can use this hook to enable the centralized call log feature (MX-ONE systems only). OMM centralized call log support provided by the OMM internally: The call logs are pushed from the PBX (e. g. Mitel MX-One) to the OMM through SIP and the OMM provides the call logs for all the DECT phones as an "XML server". The URL-path in the configuration be "CSIntegration/Subject=history" which is an indication for the OMM centralized call log feature.	>>> > Info > Redial List
Presence	Hook to reach a presence application .	>>> > Presence
Server menu	Hook to reach a server menu. The OMM system menu is available as a menu entry in the local main menu of the DECT phone (>>> softkey). If no user is assigned to the DECT phone, the server menu is the only available XML application hook.	>>> > Info > Server
Action URI	URI to be called in case of user/feature events. The URI is configured in the OMM via OMP. Content can be pushed towards the DECT phone via SIP notify.	n/a
Feature access codes	Hook to provide Feature Access Codes translation.	>>> > Info > Callback
Call completion	Hook to provide callback option when a user places an outgoing call and wants to request a callback before releasing the call.	
Park call	Hook to the Park Call service interface.	>>> > Call option > Park call
Unpark call	Hook to the Unpark Call service interface.	>>> > Unpark call
Pickup	Hook to the Pickup Call service interface.	>>> > Pickup
Take	Hook to Take call service interface.	>>> > Take
Call forward	Hook to the Call Forward service interface.	>>> > Call forward
Call routing (Mitel 602 DECT phones only)	Hook to the Personal Call Routing service interface.	>>> > Call routing
Call protection (Mitel 602 DECT phones only)	Hook to the PBX call protection service interface.	>>> > Call protection
Voice box	Hook to Voice Mail service interface.	>>> > Info > Voice box

These hooks can be activated or deactivated but not deleted. You can create up to 10 additional hooks.

Note: The "Call forward" XML hook replaces the "Call forwarding / diversion" supplementary service. When activated, the "Call forwarding / diversion" supplementary service is automatically deactivated and all user-specific settings are removed.

5.9.5.1 Creating a New XML Hook

To create a new XML hook, do the following:

- 1 On the **XML Applications** page, click **New**. The **New XML application** window opens.
- 2 Configure the following parameters for the XML hook:

- **Active:** Activates or deactivates the XML hook.
- **Name:** Name for the XML hook (not applicable for predefined XML hooks)
- **Protocol:** HTTP or HTTPS.
- **Server:** IP address or name of the server which provides the XML content.
- SIP-DECT 6.0 and later supports "SIPProxy" placeholders for XML Server application URLs in systems with SIP redundancy. Where applications are located on a SIP server, XML applications must be addressed using the current primary, secondary or tertiary SIP server address. In those cases, the "SIPProxy" placeholder can be used as server input.
- **User name:** Login user name if an authentication is required by the server.
- Password, Password confirmation: Password if authentication is required by the server.
- **Path (and parameter):** Path and query of the URL. For "Feature access codes translation", the Path settings contains placeholders for the queried translation: {subsc} = Number, {ppn} = Device ID, {fac} = FAC

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

5.9.5.2 Modifying an XML Hook

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

- 1 On the **XML Applications** page, click on the **Edit** (pencil) icon beside the XML hook entry. The **Configure XML application** window opens.
- 2 Edit the XML application parameters (described above) as necessary. Note that you cannot change the name of a predefined XML hook.

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

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

5.9.5.3 Deleting an XML Hook

You cannot delete any predefined XML hooks. You can only delete XML hooks that you have created. To delete an XML hook, do the following:

- 1 On the **XML Applications** page, click on the **Delete** (garbage can) icon beside the XML hook entry. The **Delete XML application?** window opens.
- 2 Click **Delete** to confirm deletion of the XML hook.

5.10 "LICENSES" MENU

The **Licenses** page provides an overview on the currently used license. On this page you can also import an activation or license file:

- 1 Select the path and file name where the activation or license key is stored.
 - 2 Click the **Import** button.
- For a detailed description on the OMM licensing model see section 3.32.

5.11 "INFO" MENU

The **Info** page displays the End User License Agreement (EULA).

With the first login to a new SIP-DECT software version, this page is displayed automatically and the user must accept the EULA by clicking the **Accept** button.

6 OM MANAGEMENT PORTAL (OMP)

The OM Management Portal (OMP) is a Java tool used to manage the SIP-DECT solution. It can be used to view and configure OMM system data and has integrated monitoring and other maintenance features.

SIP-DECT supports Java web start to start the OMP. Java 1.7 is required to run OMP 5.0 or later. By default, the source for the OMP binary is a Mitiel web server (RFP-OMM) or the OMP.jar from the RPM installation (PC-OMM).

You can also configure a different source (**System settings** -> **OMP web start** in the OMM Web service, or **System** -> **Advanced settings** -> **Additional services** – **OMP web start** in the OMP). The following configuration order is used:

- GUI-configured OMP web start URL in RFP-OMM installations
- Environment variable 'OM_WebStartUrl' (e.g. set by ipded.cfg configuration file)
- Mitiel web server (RFP-OMM) / from RPM installation (PC-OMM)

You can download the OMP.jar file from the OMM Web service by clicking on the OMP link in the top bar:



Double-click on the downloaded file (OMP.jar) and click "Run" in the dialog window. The OM Management Portal starts and prompts for login credentials.

Please note: Configuration of a non-default source must not contain login credentials because this is not supported by the Java Web Start mechanism. The HTTP/FTP server must be configured accordingly.

This section lists all parameters which can be configured and viewed using OMP. All parameters which are also accessible by the OM Web service are described in the appropriate OM Web service section (section 5). New parameters which are only accessible via OMP are described in this section.

6.1 LOGIN

The OMM allows more than one user at a time to configure the system.

To log in to the system enter the following data:

- **IP address** of the OMM.
- **User name, Password:** Enter a user name and a password. Both strings are checked case sensitive.

With initial installation or after removing the configuration file, the OMM Web service is accessible via a default built-in user account with user "omni" and password "omni".

The **System name** is set by the system administrator after first successful login to the OMM, see section 6.5.1.

The system name and the IP address of successful logins are stored in the local OMP preferences and can be reselected for further logins. Up to 10 different login datasets can be stored.

- On a Linux system, preferences are stored in the user's home directory
"~/java/userPrefs/...."
- On a Windows system, preferences are stored in the registry node
"HKEY_CURRENT_USER/Software/JavaSoft/Prefs/...."

After login the OMP is set to the configuration mode page showing the system status page which contains health state information of the connected OMM (see section 6.4). If there is a version difference between the OMP and the OMM, this will also be indicated here. Details can be viewed in the **Help**. **About AXI** menu (see section 6.15).

6.2 LOGOUT

There is no automatic logout for the OMP. The user must log out manually.

To log out from the system:

- Click on the Close icon  in the upper right corner of the OMP window
- Select the **Exit** entry from the **General** drop-down menu.

Note: If the OMM link is broken, the OMP asks if you want to reconnect to the OMM. In that case, you must enter the login data again.

6.3 OMP MAIN WINDOW

The header of the OMP window shows the version of the connected OMM.

"OMP mode" toolbar buttons

The OMP provides different modes: **Configuration mode**, **Monitor mode** and **Planning mode**.

Configuration mode allows changing of parameters. In monitor mode, parameters are only displayed, but are not changeable. Monitor mode provides additional features, e.g. system and RFP statistics and RFP synchronization monitoring. Planning mode enables the creation of graphics which can be used with the OM Locating application to visualize the placement of the RFPs (see also 12/7).

To select the desired mode, press the appropriate button in the upper toolbar of the OMP window:

-  Configuration mode
-  Monitor mode
-  Planning mode

Main menus

The OMP provides two main menus which are available in all program situations:

- **General** menu, see section 6.14.
- **Help** menu, see section 6.15.

Navigation panel

Both configuration and monitor mode contain a navigation panel. This panel contains the mode-dependant menu.

Status bar

The status bar is located at the bottom of the main window. It shows the following items:

- Encryption state:

The  icon indicates that encryption is enabled.

The  icon indicates that encryption is disabled.

This setting can be configured in the **DECT** tab of the **System settings** menu (see also section 6.5.1).

- PARK.
- Subscription state: Clicking on one of the following icons enables / disables subscription.

The  icon indicates that subscription is enabled.

The  icon indicates that subscription is disabled.

Subscription can also be enabled / disabled in the **DECT phones** menu (see also section 6.7.8).

- Auto-create on subscription state: Clicking on one of the following icons enables / disables Auto-create on subscription.

The  icon indicates that Auto-create on subscription is enabled.

The  icon indicates that Auto-create on subscription is disabled.

This setting can also be configured in the **DECT** tab of the **System settings** menu (see also section 6.5.1).

- Connection status to the OMM:

If connected to the OMM, the IP address of the OMM is displayed.

 OMM is disconnected from the OMM.

Info console

General OMM events are displayed the **Info console**.

6.4 “STATUS” MENU

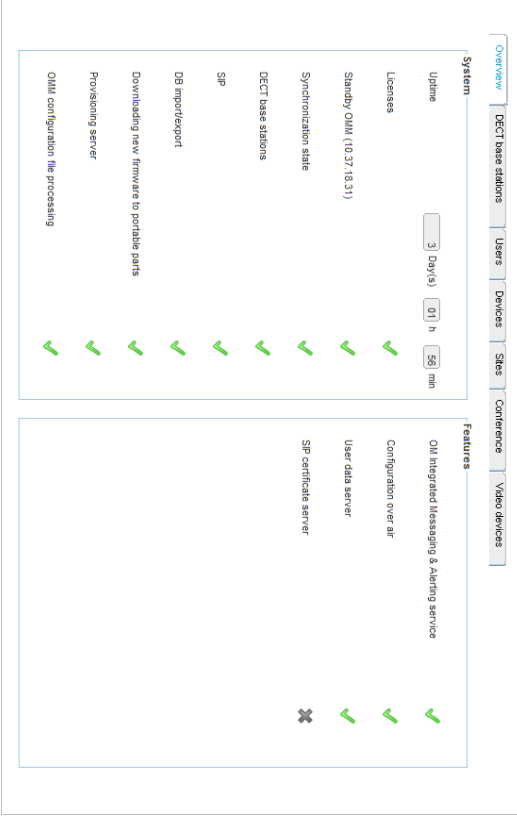
The system status is displayed after startup of OMM. The **Status** panel provides information about the system health states, and contains the following tabs:

- Overview (see section 6.4.1)
- DECT base stations (see section 6.4.2)
- Users (see section 6.4.3)
- Devices (see section 6.4.4)

- Sites (see section 6.4.5)
- Conference (see section 6.4.6)
- Video devices (see section 6.4.7)

6.4.1 OVERVIEW

The “Overview” tab consists of a “System” panel providing general system health states information and a “Features” panel which shows health states of system features. Some of these features are optional; that means the relevant health state is only shown if the feature is activated in system.



The “Overview” tab shows following system information:

- **System uptime:** Elapsed time since OMM start (in days, hours and minutes)
- **Licenses:** Licenses health state
- **Standby OMM:** Standby OMM IP address and health state of standby configuration (if no standby OMM is configured a grey cross is shown)
- **Synchronization state:** Synchronization health state
- **DECT base stations:** Base stations health state
- **SIP:** SIP health state
- **DB import/export:** DB import/export health state
- **Downloading new firmware to portable parts:** (Health) state of firmware download to DECT phones
- **Provisioning server:** Health state of provisioning server health state

- **OMM configuration file processing:** Health state of configuration file processing. Depending on OMM system configuration, the "Features" tab consists of all or a subset of these health states:
 - **OM Integrated Messaging & Alerting service:** Messaging and alerting feature health state (always active)
 - **SIP certificate server:** SIP certificate server health state (always active)
 - **Configuration over Air:** Central DECT phone configuration over air state (optional)
 - **User data server:** User data server health state (optional)
 - **User monitoring:** User monitoring health state (optional)
 - **Video:** Video health state (optional)

Health states can have the following values:

- — inactive or unknown
- — error
- — OK

6.4.2 DECT BASE STATIONS

The "DECT base stations" tab contains the following sections: "General", "DECT" and "WLAN".

Overview

DECT base stations

Users

Devices

Sites

Conference

Video services

General

Total

12

Connected

2

Invalid branding

0

Standby misconfigured

0

Version mismatch

0

Software update

0

USB overheat

0

Encryption not supported

0

Advanced features not supported

0

DECT

DECT switched on

12

DECT running

2

Used childrens

2

Used paging areas

1

WLAN

WLAN switched on

0

WLAN running

0

Profiles

0

The "General" panel provides counters related to RFP configuration and state:

- **Total:** Total number of RFPs configured
- **Connected:** Number of RFPs connected to OMM
- **Invalid branding:** Number of connected RFPs with invalid branding
- **Standby misconfigured:** Number of connected RFPs with wrong standby configuration
- **Version mismatch:** Number of connected RFPs running with wrong software version
- **Software update:** Number of connected RFPs requesting software update