Please note: It is strongly recommended that you set the DECT base station attributes "building", "floor" and "room", if you configure a large system with a large number of cameras. This makes selection of cameras on the DECT phone menu easier.

7.28.3 CAMERA SELECTION VIA DECT PHONE MENU

The **Cameras** menu is available in the Mitel 602 DECT phone **System menu**, if

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

The user navigates within the camera menu using the **OK** (and **ESC**) keys. When the desired camera is selected in the list, the user can press the "hook off" button to establish a video stream.

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

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

Please note: During an established video link, audio calls or any system service activities are not possible.

Any kind of auto callback (initiated by a message by a message or pushed by xml notification to direct dial) is not supported.

7.29 USER MONITORING

To check the availability of a user in terms of the possibility to receive calls or messages, the OMM monitors the status of the user's DECT device.

7.29.1 OVERVIEW

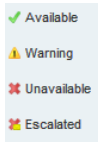
With the "user monitoring" feature the following fixed set of status information is monitored:

Is a DECT phone assigned to the user?	Handset assignment status (HAS)
Is the DECT phone subscribed to the DECT system?	Handset subscription status (HSS)
Is the DECT phone currently registered /signed in?	Handset registration status (HRS)
Are there DECT phone activities within a specific timeframe?	Handset activity status (HCS)
Is the user registered at the SIP registrar?	SIP user registration status (SRS)
Is the DECT phone not in silent charging mode (silent charging option active and in the charger cradle)?	Silent charging status (SCS)
Is the feature "immediate call diversion" inactive?	Call diversion status (CDS)
Is the battery charge higher than the configured threshold?	Handset battery state (HBS)

Does the DECT phone have the minimum required software version?	Software Status (SWS)

If all questions can be answered with "Yes" then the user status is set to "Available". This set of status information is monitored if user monitoring is enabled for a user.

The status of all monitored users is displayed in the **DECT Phones** -> **User monitoring** menu (see also section 7.29.7.3). The status information can have one of the following values:



The sum of all specific states is presented by the "Combined User Status".

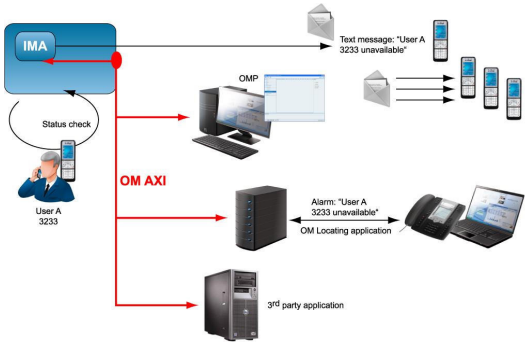
User ID	Name	Number	Rel. devi...	Mode	CUS	HAS	HSS	HRS	HCS	SRS	SCS	CDS	HBS	BTS	SWS
0x03D	Georg Wolf	2358	0x056	Passive	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓

If one of the states is set to unavailable, the resulting Combined User Status is set to unavailable as well.

0x00E	Lutz Püschel	2476	0x0E0	Passive	✗	✗						✓			

Because of dependencies between the states, some states cannot be determined if a higher level state is not fulfilled. For example, if the user has no DECT phone assigned, the DECT phone registration status cannot be determined. If a status cannot be determined, the status value is set to "Unknown" (empty in OMP).

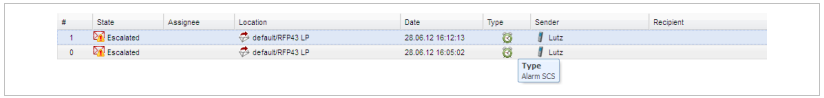
The status information is available via OM AXI and OMP.



IMPORTANT : To address customer specific requirements, external applications (e.g. 3rd party software) can provide an addapted functionality of the user monitoring or even more just by using OM AXI. This can be completed by the use of the XML terminal interface.

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

The specific alarm trigger “LOC-ERR-USERSTATE” is defined for locating. This alarm trigger is displayed in the OM Locating application with the icon.



#	State	Assignee	Location	Date	Type	Sender	Recipient
1	Escalated		default/RFP43 LP	28.06.12 16:12:13		Lutz	
0	Escalated		default/RFP43 LP	28.06.12 16:05:02		Lutz	

Type
Alarm SCS

IMPORTANT : The OM Locating application does not list users who are not locatable, e.g. locating not enabled for the users or because they have no DECT phone assigned. Therefore, the OM Locating application can not handle the LOC-ERR-USERSTATE with the escalation of the DECT phones assignment state (HAS).

7.29.2 STATUS ATTRIBUTES AND VALIDATION MECHANISMS

The combined user status (CUS) is the sum of the specific status information.

The CUS is calculated based on the flowing rules:

- Specific states which are set to “Unknown” are ignored.
- CUS is set to “Available” if none of the specific states is set to “Warning”, “Unavailable” or “Escalated”.
- CUS is set to “Warning” if at least one of the specific states is set to “Warning” and none of the other states is set to “Unavailable” or “Escalated”.
- CUS is set to “Unavailable” if at least one of the specific states is set to “Unavailable” and none of the other states is set to “Escalated”.
- CUS is set to “Escalated” if at least one of the specific states is set to “Escalated”.

The status “Unavailable” is changed to “Escalated” after the escalation timeout has elapsed and an alarm trigger has been generated.

7.29.2.1 Handset Assignment Status (HAS)

A DECT phone must be assigned to the user otherwise the status is “Unavailable”.

Fixed user device relation

A DECT phone can be assigned permanently to a user (fixed user device relation). Then the status is always “available”.

Dynamic user device relation

A DECT phone can be dynamically assigned to a user (dynamic user device relation) and login and logout on a DECT phone is used.

If the user is logged out (unbound), the status is “Unavailable”. If the user is logged in (dynamic), the status is “available”. Login and logout also change the SIP registration.

Precondition: The user must exist in the OMM database.

7.29.2.2 Handset Subscription Status (HSS)

The DECT phone must be subscribed otherwise the status is “Unavailable”.

Precondition: A DECT phone must be assigned to the user.

7.29.2.3 Handset Registration Status (HRS)

The DECT phone must be attached / signed in (successful location registration) otherwise the status is “Unavailable”

The DECT phone may sent a detach message if it is switched off.

Precondition: A DECT phone must be assigned to the user (fixed, logged in) and the DECT phone is subscribed.

7.29.2.4 Handset Activity Status (HCS)

A communication over the air must occur regularly otherwise the status is “Unavailable”.

Passive monitoring

With every activity between DECT phone and the DECT system (e.g. call setup) the activity information will be updated (last activity, current activity status). This indicates when the DECT phone was the last time able to communicate with the DECT system i.e. within the area of coverage, sufficient battery level, etc. There must be an activity within the timeframe defined by the Activity timeout 1 (min. 30 minutes, max. 1440 minutes).

Any activity between the DECT phone and the systems sets the status to “available”.

Active monitoring

Each DECT phone, that shall be monitored actively, will refresh its registration automatically within the “Activity timeout 2” (min. 5 minutes, max. 60 minutes). Each activity sets the status to “available”.

Active and passive monitoring

If the DECT phone was not active for the period of time defined by the activity timeout, the OMM automatically initiates an activity between the DECT phone and the DECT system to check the DECT connectivity. If this fails, the OMM sets the status to “Unavailable” but tries to connect to the DECT phone two times more within the next 2 minutes.

The OMM then continues to check the DECT connectivity base on the configured time frame. If the status is already “Unavailable”, the OMM does not verify the status by two additional tests within 2 minutes. If a check was successful, the status is set to “available”.

If a DECT phone could not be reached (e.g. during call setup or messaging delivery), the OMM tries to connect to the DECT phone two times more within the next 2 minutes before the status is set to “Unavailable”.

Precondition: A DECT phone must be assigned to the user (fixed, logged in). The DECT phone is subscribed and attached (at least once).

7.29.2.5 SIP User Registration Status (SRS)

The user must be successfully registered at the configured SIP registrar otherwise the status is “Unavailable”.

A SIP registration is initiated automatically by the OMM during start-up if the user’s DECT phone was attached to the DECT system before restart/failover.

The SIP registration will not initiated automatically by the OMM during start-up if

- the user has no assigned DECT phone (fixed user device relation, login),
- the DECT phone is not subscribed or
- the DECT phone was detached (e.g. switched off) before restart/failover.

A user will be deregistered if

- the DECT phone subscription is deleted/terminated,
- the user logs off from a DECT phone or
- the DECT phone is detached (e.g. switch off).

Precondition: A DECT phone must be assigned to the user (fixed, logged in). The DECT phone is subscribed and attached (at least once).

7.29.2.6 Silent Charging Status (SCS)

If silent charging is enabled and the DECT phone is put into the charger, the DECT phone is in silent charging mode and does not indicate incoming calls with an audible signal. The DECT phone must not be in silent charging mode otherwise the status is “Unavailable”.

Precondition: A DECT phone must be assigned to the user (fixed, logged in). The DECT phone is subscribed and attached/signed in to the DECT system.

7.29.2.7 Call Diversion Status (CDS)

The user has no immediate call diversion (unconditional call forwarding) configured otherwise the status is “Unavailable”.

If the user has configured a call diversion for “No answer” / “Busy no answer” with a forward time ‘0’, this will be handled by user monitoring like unconditional call forwarding.

Precondition: The user must exist in the OMM database. The SIP supplementary service “Call forwarding / Diversion” is enabled in the OMM (see pages 76 and 137).

7.29.2.8 Handset Battery Status (HBS)

The battery level of the DECT phone must be greater than the configured threshold value; otherwise the status is set to “Warning”.

Precondition: A DECT phone must be assigned to the user (fixed, logged in). The DECT phone is subscribed and attached. Delivery of battery level is supported. [1]

[1] The Mitel 600 DECT phone family provides battery status information if the DECT phones are updated to the current software version.

7.29.2.9 Software Status (SWS)

The DECT phone software must provide the minimum of required features which could be controlled by the current OMM version. Therefore the appropriate minimum DECT phone software version is hard coded in the OMM and validated by user monitoring. The status will be set to “Warning” if the DECT phone software version is less than the hard coded value of the OMM.

Delivery of the software version is supported only by Mitel 600 devices.

Precondition: A DECT phone must be assigned to the user (fixed, logged in). The DECT phone is subscribed and attached. [1]

7.29.3 ESCALATION

If the OMM detects the unavailability of a user (marked as “unavailable”), this will be escalated only once by submitting a warning alarm trigger via OM AXI.

If the OMM detects finally the unavailability of a user (marked as “unavailable/escalated”), this will be escalated only once by submitting an alarm trigger via OM AXI.

The user must become available again before the unavailability of a user will be escalated the next time.

7.29.4 ALARM TRIGGERS

- The “UMON-WARNING-USERSTATE” alarm trigger is used to escalate the detection of the unavailability.
- The alarm triggers “UMON-ERROR-USERSTATE” and “LOC-ERROR-USERSTATE” are used to escalate the final detection of the unavailability.
- The “UMON-OK-USERSTATE” alarm trigger is sent by the OMM if a user becomes available again.

These are static, predefined alarm triggers like “SOS” and “MANDOWN” which do not have a telephone number to call.

The alarm triggers “UMON-WARN-USERSTATE”, “UMON-ERR-USERSTATE” and “LOCERR-USERSTATE” provide information about the cause why the user became unavailable (one or more of status attribute IDs: HAS, HSS, HRS, HCS, SRS, SCS, CDS, …).

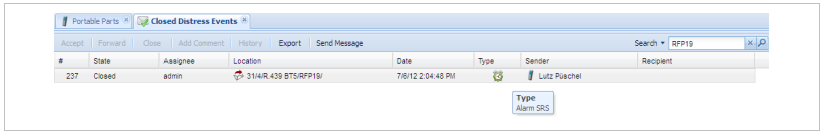
7.29.5 OM LOCATING APPLICATION

To be visible in the OM Locating application, the monitored user must be locatable. Tracking can be enabled.

The alarm trigger “LOC-ERR-USERSTATE” is handled like SOS ( ), ManDown ( ) but no voice call will be established.

The alarm trigger “LOC-ERR-USERSTATE” will be displayed as a Customer specific event ( ).

[1] The Mitel 600 DECT phone family provides software version information if the DECT phones are updated to the current software version.



7.29.6 LICENSING AND SYSTEM CAPACITIES

The “User monitoring” feature does not require a specific license.

The number of monitored users is limited, as follows:

RFP OMM

- Passive monitored users: 30
- Active monitored users: 20

PC OMM

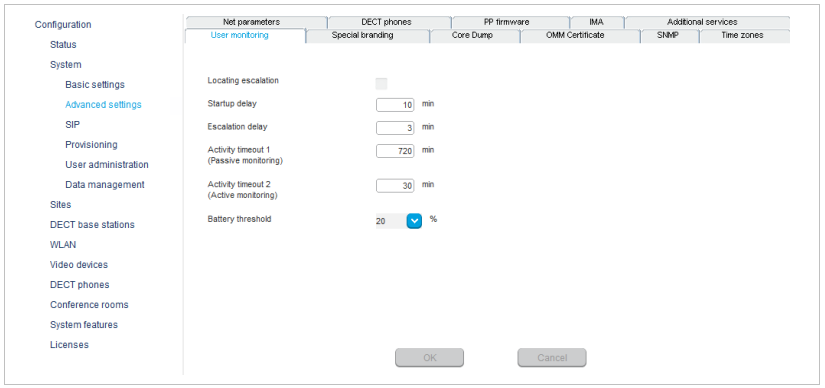
- Passive monitored users: 300
- Active monitored users: 200

An OMM system health state will be set if the number of monitored users exceeds the system capabilities. In this case also an associated health state alarm trigger will be generated.

7.29.7 CONFIGURATION

User monitoring can be administered via the OMP.

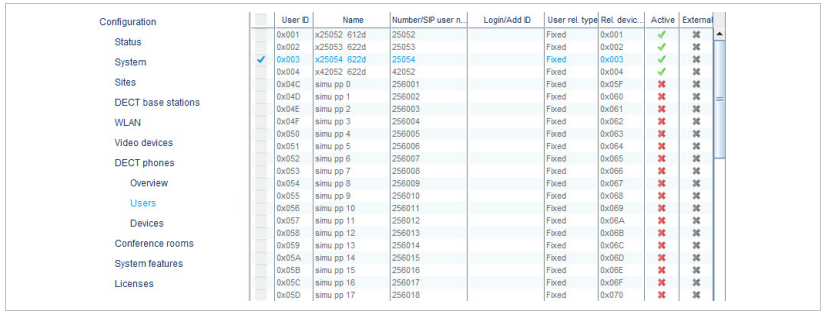
7.29.7.1 “System settings: User monitoring” Menu



The following parameters can be configured on system level.

- **Locating escalation**: If this option enabled, the alarm trigger “LOC-ERR-USERSTATE” will be generated by the OMM. Default setting is “off”.
- **Start-up delay**: The start-up delay defines the period of time the user monitoring start-up is delayed (between 2 and 15 minutes) after failover or system start-up.
- **Escalation delay**: The escalation delay defines the period of time the user monitoring will wait before the unavailable status is escalated.
- **Activity timeout 1**: The activity timeout 1 defines the maximum time (between 30 and 1440 minutes) between user activities in passive monitoring mode.
- **Activity timeout 2**: The activity timeout 2 defines the maximum time (between 5 and 60 minutes) between user activities in active monitoring mode.
- **Battery threshold**: The battery threshold defines the minimum battery load (between 0 and 100% in steps of 5%).

7.29.7.2 “DECT Phones” Menu



The following parameter can be configured on user level.

Monitoring mode: The user monitoring mode can be set to **Off**, **Passive** or **Active**. **Off** disables user monitoring. **Passive** and **Active** enable user monitoring and control the mode of the DECT phone activity status supervision. Default setting is **Off**.

If user monitoring is activated, the **VIP** option in the **DECT Phones** -> **Users** -> **SIP** tab for the user will be set automatically (see page 174). The **VIP** option will not be reset if the user monitoring mode is set to “Off”.

7.29.7.3 “DECT Phones -> User monitoring” Menu

The status of all monitored users is presented by the OMM in the **DECT Phones** -> **User monitoring** menu.

7.29.7.4 User Configuration Files

The parameter “UD_UserMonitoring” controls the monitoring for a user. The parameter can be set to “Off”, “Passive”, or “Active”.

7.29.7.5 OM IMA Application

If messages shall be sent out by the OM IMA application, the administrator must configure appropriate alarm scenarios for the alarm triggers in the OM IMA configuration file:

- UMON-OK-USERSTATE
- UMON-WARN-USERSTATE
- UMON-ERR-USERSTATE

7.29.8 START AND FAILOVER

The availability status is set to “Unknown” at start-up.

The monitoring feature does not escalate any user status during start-up until a configurable delay of min. 2 minutes and max. 15 minutes has elapsed.

The start-up delay should be adjusted according to the system start-up. The system start-up depends on the actual physical configuration, infrastructure components and parameter settings.

The statistic counter “Sync RFP start-up time” and “Sync Cluster start-up time” help to find an appropriate value for the start-up delay.

As soon as the start-up delay has elapsed, the status attributes are checked and the availability status will be determined. If the result is “Unavailable”, the status will be escalated.

The SIP registration process runs independently from the user monitoring start-up and infrastructure start-up. Monitored users as well as other users, who have the VIP flag set, are registered first.

7.29.9 SUPPORTED DECT PHONES

The Mitel 600 DECT phone family is fully supported.[1]

The following states are managed independent of the DECT phone type:

- Handset assignment status (HAS)
- Handset subscription status (HSS)
- Handset registration status (HRS)
- Handset activity status (HCS)[2]
- SIP user registration status (SRS)
- Call diversion status (CDS)

Notes on Mitel 142d

The Mitel 142d DECT phones are supported by SIP-DECT and have an enhanced feature set compared to GAP DECT phones. For Mitel 142d the availability status is always set to “Warning” because of the limited feature set.

User ID	Name	Number	Rel. devi...	Mode	CUS	HAS	HSS	HRS	HCS	SRS	SCS	CDS	HBS	BTS	SWS
0x001	142d	3000	0x001	Active	⚠	✓	✓	✓	✓	✓		✓			⚠

[1] The DECT phones must be equipped with the software version that corresponds to the SIP–DECT® release. Otherwise, functionality may be limited.

[2] GAP devices do not support the active monitoring.

The following states are not supported:

- Handset battery state (HBS)
  always set to “Unknown”
- Software Status (SWS)
  always set to “Warning” to indicate the limited feature set
- Silent charging state (SCS)
  always “Unknown”

If the DECT phone is put into silent charging mode then it sends a “Detach”, like it is switched off.

Comments on GAP DECT phones

GAP DECT phones are supported by SIP-DECT with a basic feature set. The availability status is always set to “Warning” because of the limited feature set.

User ID	Name	Number	Rel. devi...	Mode	CUS	HAS	HSS	HRS	HCS	SRS	SCS	CDS	HBS	BTS	SWS
0x001	GAP	3000	0x001	Passive	⚠	✓	✓	✓	✓	✓		✓			⚠

The following states are not supported:

- Handset battery state (HBS)
  always “Unknown”
- Software Status (SWS)
  always set to “Warning” to indicate the limited feature set
- Silent charging state (SCS)
  always “Unknown”

GAP DECT phones do not support the active monitoring (Handset activity status /HCS). In general, there is no guarantee for the correct interworking of the 3rd party DECT phone with SIP-DECT.

7.29.10 RESTRICTIONS

The described mechanisms check the status information in the OMM. Therefore the solution has certain limitations.

The OMM determines the availability of the DECT device which does not necessarily represents the availability of the user.

- It is not possible to determine whether a user actually carries his device with or not.
- The check of the availability does not include the infrastructure to which the OMM is connected (e.g. call manager, etc.). A user appears as available even if the call manager fails.
- Feature (especially call diversion) when managed by the call server can undermine the monitoring.
- If a user is removed from the OMM, the monitoring stops without escalation. It cannot be checked if the user belongs to an alarm scenario configured in the alarm server or any other application scenario.

7.30 SRTP

Together with the new RFP 35/36/37 IP and 43 WLAN, SIP-DECT supports SRTP to encrypt the RTP voice streams and SDES for the SRTP key exchange.

There are three options for SRTP:

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

SIP-DECT provides the cipher suite AES_CM_128_HMAC_SHA1_80.

SRTP calls from DECT phones with DECT handover require that the SRTP functionality must be homogenously available on all effected RFPs. To allow mixed installations with the older RFP types 32/34 and 42 WLAN, the SRTP feature can be enabled or disabled per site. Whereby, SRTP can only be activated on sites with only RFPs 35/36/37/43 included.

IMPORTANT : **A handover of an SRTP call to a site with disabled SRTP will drop the call.**

IMPORTANT : **SDES specifies as key exchange method the negotiation over SDP included in the SIP signaling. Therefore, we recommend to use TLS to encrypt the key exchange.**

IMPORTANT : **Please enable "SRTP = only" mode exclusively when all communication can be established with SRTP. Depending on the call server some features or gateways may not offer SRTP.**

7.31 SIP OVER TLS

The transport protocol modes "TLS" or "Persistent TLS" enable a private and authenticated signaling, including safe key exchange for SRTP encryption.

The transport protocol and all further security settings can be set via the OMP **System** -> **SIP**-> **Security** tab and the OMP **System** -> **SIP**-> **Certificate Server** tab.

The following parameters can be set:

7.31.1.1 General

- **Transport protocol**: The protocol used by the OMM to send/receive SIP signaling. Default is "UDP".
- **Persistent TLS Keep alive timer active**: When enabled and "Persistent TLS" is selected as transport protocol, the OMM sends out keep alive messages periodically to keep the TLS connection open.

- **Persistent TLS Keep alive timer timeout**: Specifies the time, in seconds, between keep-alive messages sent out by the OMM. Valid values are "10" to "3600". Default is "30" seconds.
- **Send SIPS over TLS active**: When enabled and "TLS" or "Persistent TLS" is selected as transport protocol, the OMM uses SIPS URIs in the SIP signaling. Default is "ON".
- **TLS authentication**: When enabled and "TLS" or "Persistent TLS" is selected as transport protocol, the OMM validates the authenticity of the remote peer via exchanged certificates and the configured "Trusted certificates". Default is "ON".
- **TLS common name validation**: When enabled and "TLS authentication" is selected the OMM validates the "Alternative Name" and "Common Name" of the remote peer certificate against the configured proxy, registrar and outbound proxy settings. If there is no match an established TLS connection will be closed immediately.

7.31.1.2 PEM file import

- Allows the manual import of Trusted, Local Certificates and a Private Key in PEM file format.

The following parameters can only be read and should ease the handling of certificates:

- **Trusted Certificates**: The number of imported trusted certificates.
- **Local Certificate chain**: The number of imported certificates in the local certificate chain.
- **Private Key**: Is a private key imported or not.

7.31.1.3 Certificate server

Optionally is also an automatic import of Trusted, Local Certificates and a Private Key files from an external server possible. This can be configured on the "Certificate Server" tab.

The following parameters allow an automatic import:

- **Active**: Enable or disable the automatic import.
- **Protocol**: Selects the preferred protocol (FTP, TFTP, FTPS, HTTP, HTTPS, SFTP)
- **Server**: IP address or name of the server
- **User Name** / **Password** / **Password confirmation**: The server account data if necessary.
- **Path:** The path on the server to certificate files.
- **Trusted certificate file:** The name of the PEM file on the given server including the trusted certificates.
- **Local certificate file:** The name of the PEM file on the given server including the local certificate or a certificate chain.
- **Private key file:** The name of the PEM file on the given server including the local key.

7.31.2 CERTIFICATES

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

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

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

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

```
-----BEGIN CERTIFICATE-----
```

and

```
-----END CERTIFICATE-----
```

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

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

Trusted Certificates

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

Local Certificates

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

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

7.31.3 PRIVATE KEY

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

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

```
-----BEGIN RSA PRIVATE KEY-----
```

and

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

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

7.31.4 TLS TRANSPORT MODE

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

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

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

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

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

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

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

7.31.5 VERIFICATION OF REMOTE CERTIFICATES

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

The signature of the certificate is checked with the public key of the signing certificate. The certificate chain is checked until a *Trusted Certificate* is found. If self-signed certificate is found which is not trusted, the verification fails.

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

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

> **Please note:** All certificates are only valid for a limited time given by the issuer. As soon as the validity is expired no further communication is possible. The certificates must be replaced before to prevent a breakdown of call services.

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

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

7.31.6 ADDITIONAL SECURITY CONSIDERATIONS

For highest security requirements there are additional considerations to be taken into account when enrolling an OpenMobility system.

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

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

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

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

7.32 DECT ENHANCED SECURITY

Security aspects in the DECT standard have been improved after concerns were raised in the market in recent years. Therefore various enhancements have been introduced.

The usage of many security features, which were already available in the DECT standard (respectively GAP) from the beginning, was left optional for the devices. These mechanisms became mandatory together with CAT-iq. Almost each of these functionalities was present and used within SIP-DECT right from the start.

Furthermore, some new features have been added to GAP:

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

Each procedure brings additional guarantee on security and is an integral part of the SIP-DECT solution.

The feature set can be enabled or disabled per site. This distinction is necessary due to the fact, that enhanced security is available with RFPs 35/36/37/43 only.

From release 5.0 on, when DECT enhanced security is enabled, every connection will be encrypted, not only voice calls, but also such as service calls (e.g. list access) or messaging.

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

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

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

7.33 MIGRATION OF RFP SL35 IP FROM SIP-DECT LITE 3.1 TO SIP-DECT 6.1

The SIP-DECT Lite solution realized a single-cell DECT network that offered only limited radio coverage and was operated with one RFP SL35 IP. The SIP-DECT Lite solution was part of the SIP-DECT product family that offered larger radio coverage by realizing multi-cell DECT networks with up to 2.56 RFPs.

You can integrate the RFP SL35 IP to a multi-cell SIP-DECT network. The migration from SIP-DECT Lite to the current release of the standard SIP-DECT system is supported. During the migration the SIP-DECT Lite software is replaced by the standard SIP-DECT software on the RFP SL35 IP and a reset to the factory setting is performed. All configuration data are removed from the base station.

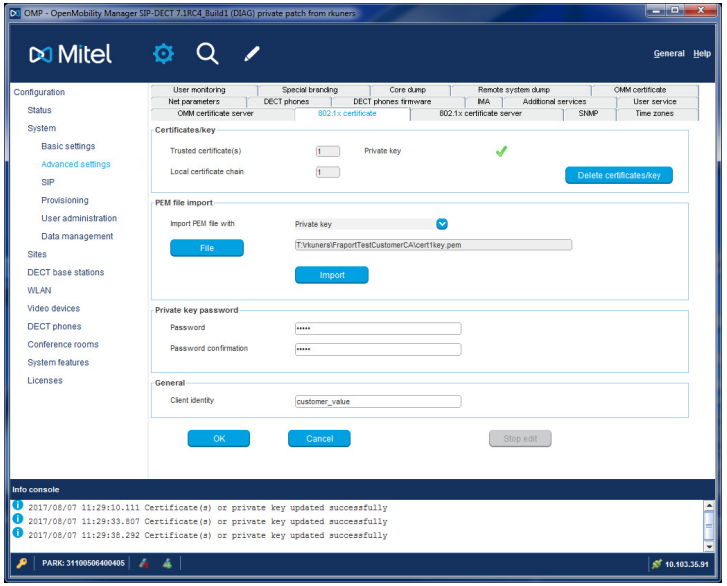
The following migration process must be performed.

Precondition: Unique UNLOCK.xml file is available for the specific RFP SL35 IP.

1. Remove the USB flash memory from the RFP SL35 IP and plug it into your computer.
2. Copy the unlock.xml file onto the USB flash memory.
3. Copy the standard SIP-DECT SW (iprfp3G.dnld) onto the USB flash memory of the RFP.
4. Check if the following files are on the USB flash memory (no other files should be on the USB flash memory except SIP-DECT™ Lite DB backup field "omm_conf.txt" which is not relevant).
   a. PARK.xml
   b. UNLOCK.xml
   c. iprfp3G.dnld
5. Remove the USB flash memory from your computer and plug into the RFP SL35 IP.
6. The migration process starts automatically after plugging the USB flash memory into the RFP.
7. Wait for the RFP reboot and start-up. Do not interrupt the electric power during this process.
8. The SW update for RFPs in standard SIP-DECT installations are provided by other means than to copy the SW on the USB flash memory. Therefore the iprfp3G.dnld must be removed from the USB flash memory.
   Make sure that the PARK.xml and UNLOCK.xml remain on the USB flash memory.
9. Also after the migration, make sure that the USB flash memory is always plugged in the RFP.
10. Now, the RFP SL35 IP has the standard SIP-DECT SW and the UNLOCK.xml file and can be operated in standard SIP-DECT installations. Please follow the standard procedures to setup a SIP-DECT installation.

7.34 802.1X CERTIFICATE BASED AUTHENTICATION

You can assign a group certificate to all RFPs of a SIP-DECT installation for certificate based authentification to open the switch ports the RFPs are connected to.



7.34.1 802.1X CONFIGURATION

You can import trusted certificates, a local certificate chain and a private key file for 802.1x certificate based authentication manually through OMP or OMM configuration files.

7.34.1.1 Configure and store 802.1x certificate settings

- 802.1x certificate data are optional parameters. 802.1x certificate based authentication works only if valid certificate data is configured and the feature is set to enabled.
- 802.1x certificate data is stored centrally in OMM database and can be set by OMP, through an OMM provisioning file or from a certificate server.
- The centrally stored 802.1x certificate data remains valid until it is changed or removed by one of the configuration sources.
- The stored 802.1x certificate data is used after a reset/reboot/power cycle even if the provisioning server is not reachable.
- RFPs receive the encrypted 802.1x certificate data from OMM via a HTTP file request, for example, after reboot or after notification of new certificate data from the OMM. Only RFPs can decrypt and use the certificate data.
- The 802.1x certificate data will be stored locally on RFPs.

7.34.1.2 Configure and store 802.1x certificate server settings

- 802.1x certificate server settings are optional parameters. If configured, the OMM uses the configured file server to load/update the 802.1x certificate data (group certificate, private key, Trusted (CA) certificate(s))
- 802.1x certificate server settings are stored centrally in OMM database and can be set by OMP or via an OMM provisioning file.

7.34.1.3 Discard OMM DB or RFP factory reset, which are offered as restart options

- The 802.1x certificate data and the 802.1x certificate server settings on the (RFP-) OMM are lost.
- The 802.1x certificate data and the 802.1x certificate server settings have to be configured again; otherwise, the RFPs receive empty 802.1x certificate data on the next 802.1x update.
- To delete 802.1x certificate data from a RFP, the data can be deleted on the OMM (applies to connected RFPs), or a factory reset of an RFP can be initiated (OM-Configurator or through an prepared USB stick).

7.34.2 PREREQUISITES REFERRING TO 802.1X TOPOLOGY

802.1x group certificate based authentication runs in networks, which fulfill needs of a proper running 802.1x administration:

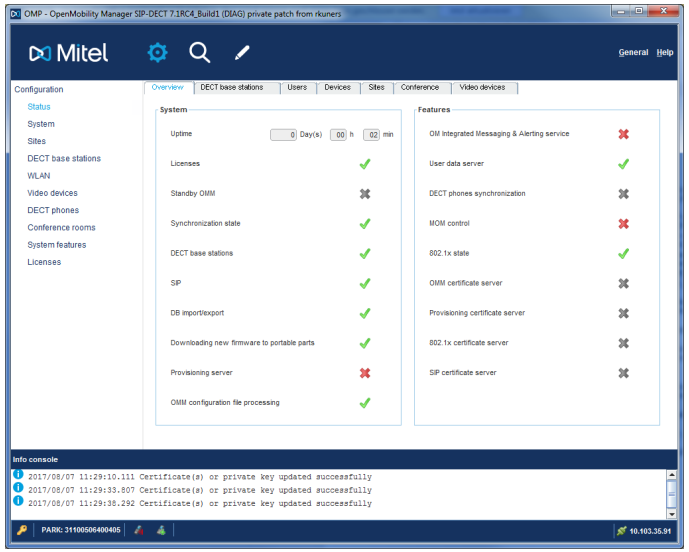
- Radius server
- Switch port configuration
- Closed mode (initial 802.1x configuration in safe environment) or low-impact mode (DHCP, DNS, NTP, TFTP, HTTP (for the transfer of the 802.1x configuration to the RFPs)) enabled. HTTP traffic between the OMM and RFPs in different VLAN (guest VLAN for unauthorized clients) needs to be routed by a layer 3 switch or router so authorized RFPs can receive their 802.1x configuration or guest VLAN (DHCP, DNS, NTP, TFTP - HTTPS to OMM needs to be routed). Traffic between different VLANs (including the native VLAN) is routed by a layer 3 switch or router. Even a proper routing between native VLAN and SDC VLAN is mandatory or guest VLAN (DHCP, DNS, NTP, TFTP - HTTPS to OMM needs to be routed)
- Full access to productive network after successfull 802.1x authentication

7.34.3 802.1X FEATURE DESCRIPTION

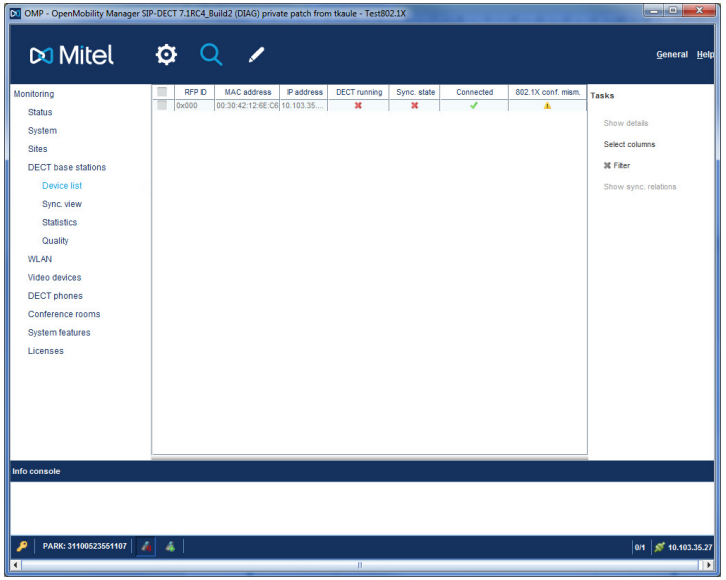
- All RFPs of an installation needs to get updated to a firmware which supports 802.1x (either in a secure environment or on a switch port in low-impact mode or in a guest VLAN were access to DHCP and TFTP is possible).
- Initial 802.1x certificate request from OMM needs to be enabled on the RFP through local configuration (OM-Configurator parameter independent from local configuration flag) or a DHCP option (option 43 suboption + unused DHCP option) to prevent impact on existing installations. If 802.1x certificates are already loaded to an RFP, updates are requested independent from this local or DHCP configuration.
- OMP supports the configuration of 802.1x group certificate data or alternatively the configuration of a certificate server for automatic update of the certificates from a file server.
- For the group certificate, a unique 802.1x identity for all RFPs is supported.

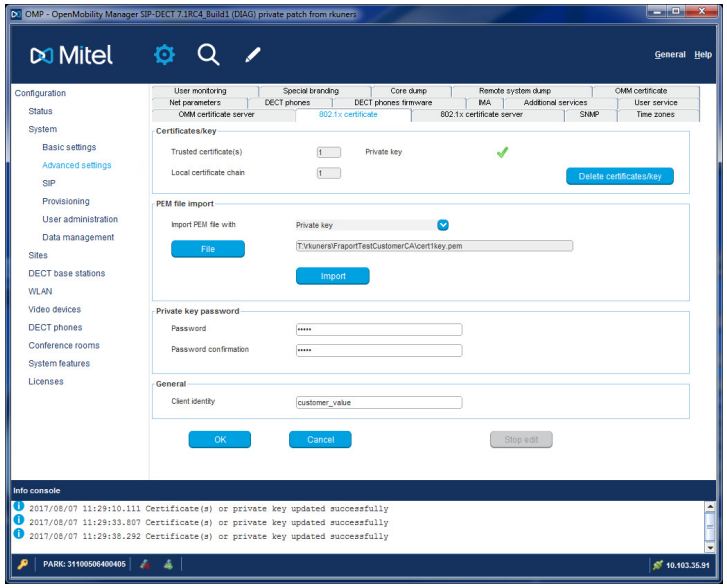
- To enable 802.1x on RFP each of them is initialized by DHCP option or OM_Configurator. Otherwise the feature is inactive for a RFP (see 7.36).
- RFPs request RSA encrypted 802.1x certificate data through HTTP from the active OMM (either in a secure environment or on a switch port in low-impact mode or in a guest VLAN were access to DHCP and to the OMM via HTTP is possible).
- Certificate data is requested/updated, for example on RFP startup or after a certificate update has been triggered by the OMM.
- In addition to the certificate data, a RFP receives and applies the admin and root login credentials (user name and password hash). Thereby access to the RFP root file system is no longer possible with the default password of previously unconfigured RFPs.
- The certificate data is stored reset proof in the RFPs.
- If an 802.1x certificate data file was received from the OMM, RFP admin and root login credentials cannot be changed through the IPL protocol between OMM and RFP (for example, by connecting to a different OMM system > factory reset required).
- You can delete 802.1x certificate data from the OMM. Afterwards, the data is deleted from connected RFPs.
- New edit mode in OMP for 802.1x certificate settings to prevent inconsistent configuration (changed settings will not be used before leaving the edit mode).
- New DECT base station attribute 802.1x configuration mismatch for the device list in OMP monitoring mode.
- New health states for 802.1x are supported. A warning message appears while the 802.1x edit mode is active and shows mismatch errors if certificates cannot be updated from the 802.1x certificate server or if not all RFPs have the correct certificate checksum (certificate mismatch).

New health state for 802.1x



802.1x configuration mismatch in DECT base stations device list (OMP monitoring mode).





You can import trusted certificates, a local certificate chain and a private key file for 802.1x certificate based authentication manually through OMP or OMM configuration files.

- Certificates/key: Shows the number of active 802.1x trusted certificates, the number of 802.1x local certificate chains and whether a 802.1x private key is used. All can be deleted with the Deletecertificates/key button.

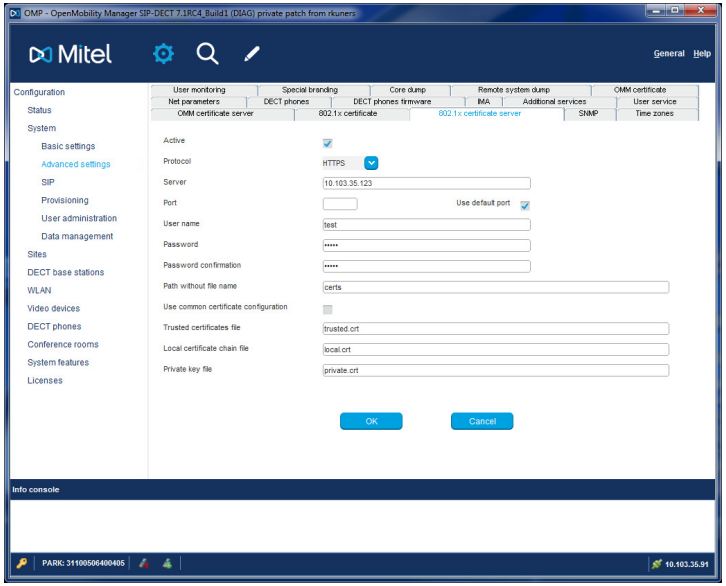
- **PEM file import / Import PEM file with**: Specifies the type of file 802.1x (trusted certificate, local certificate, or private key) and the location of the file to be imported.

- **General/Client identity**: 802.1x supplicant client identity.

- **Private key password/ Password**: Specifies the password for the 802.1x private key file.

7.35 802.1X CERTIFICATE SERVER CONFIGURATION

Through configuration of a 802.1x certificate server URL, you can update the 802.1x certificate data automatically.



Configuration of the 802.1x certificate server using OMP.

- **User name**: Specifies the user name for authentication against the certificate server.
- **Password**: Specifies the password for authentication against the certificate server.
- **Active**: Enables or disables the certificate server URL feature.
- **Protocol**: Specifies the protocol to be used to fetch the certificate files. One of FTP / FTPS / SFTP / HTTP / HTTPS / TFTP / None.
- **Port**: Specifies the certificate server's port number or use of the default port for the used protocol.

- **Server**: Specifies the IP address or name of the certificate server.
- **Path without the filename**: Specifies the path to the certificate files on the certificate server.
- **Trusted certificates file**: Filename of the trusted certificates to read from the server.
- **Local certificate chain file**: Filename of the local certificates to read from the server.
- **Private key file**: Filename of the private key to read from the server.

7.36 INITIATE 802.1X BY DHCP OPTIONS OR OM_CONFIGURATOR

Before 802.1x starts the feature, it has to be initialized by DHCP or by the OM_Configurator tool.

7.36.1 DHCP OPTIONS

There are two ways, either DHCP option 226 or the vendor specific option 43 (code 226) can be used.

DHCP option 226	set this option to 1	the option is optional
Vendor specific option 43	set code 226 to 1	code 226 is optional

7.36.2 OM_CONFIGURATOR

Select the parameter *Activate 802.1x* and set it to true. If `.csv` config files are used, set the common value *use_802_1x=1*.

8 MAINTENANCE

8.1 SITE SURVEY MEASUREMENT EQUIPMENT

If a SIP-DECT installation must be planned, a sufficient distribution of DECT base stations that meets the requirements for reliable synchronization and connectivity to the DECT phones is necessary. The site survey kit may help you. It comprises:

- One measuring RFP with its own power supply.
- A tripod and a battery for the RFP.
- Two reference DECT phones with chargers.
- Battery chargers.
- Optional a measuring DECT phone which can monitor other makers DECT radio sources.

8.2 CHECKING THE MITEL HANDSET FIRMWARE VERSION

You can display the version information of a Mitel 600 or Mitel 142d DECT phone with a few keystrokes. Check the firmware version to determine whether an update is required to overcome any user issues.

11 Press the **Menu** soft key.

12 Select **System** (only to highlight).

13 Press **OK**.

14 Select **Version Number**.

15 Press **OK**.

The display shows the software and the hardware version of the Mitel DECT phone.

8.3 DIAGNOSTIC

8.3.1 MITEL DECT PHONE SITE SURVEY MODE

You can switch a Mitel 600 or Mitel 142d DECT phones into “site survey mode” with a few keystrokes. In this mode the phone will display the RFPs and the actual field strength of the receiving signal in dBm.

1 Press the **Menu** soft key.

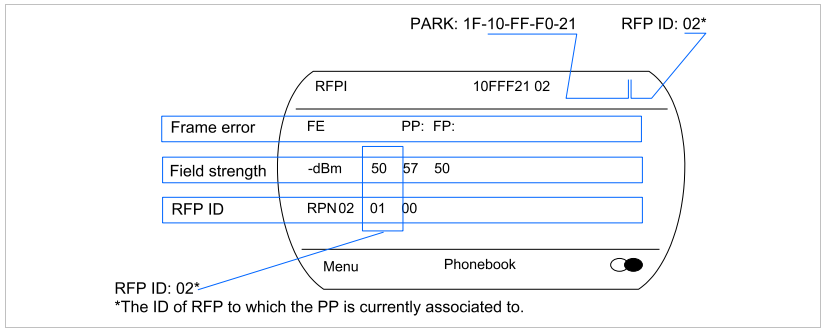
2 Enter the following key sequence “***76#” (Mitel 600) or “R***76#” (Mitel 142d).

3 Select Site Survey.

4 Press OK.

5 To leave the site survey mode, switch the phone off and on again.

The following display is shown on the Mitel DECT phone:



In this example the DECT phone is currently connected to the RFP with the number 02. The RFPs 01 and 00 are also visible. The number “10FFF221 02” on the upper right side refers to the PARK (Example 1F-10-F2-21) of the SIP-DECT system and to the RFP to which the phone is currently connected to.

8.3.2 MITEL HANDSET AUTO CALL TEST MODE

You can switch a Mitel 600 or Mitel 142d DECT phones into “auto call test mode” with a few keystrokes. In this mode the phone will call a specified number cyclically. You can use this feature to generate traffic for test purposes. This mode is also active if the phone is on the charger.

1 Press the **Menu** soft key.

2 Enter the following key sequence “***76#” (Mitel 600) or “R***76#” (Mitel 142d).

3 Select Auto Call Test.

4 Press OK.

5 Enter the phone number to call.

6 Press OK.

7 Enter a number of seconds between two calls.

8 Press OK.

9 Enter a number of seconds a call shall be active.

10 Press OK. The test will be started automatically.

11 To stop the test, switch the phone off and on again.

8.3.3 MITEL HANDSET AUTO ANSWER TEST MODE

You can switch a Mitel 600 or Mitel 142d DECT phone into “auto answer test mode” with a few keystrokes. In this mode, the phone answers incoming calls automatically. You can use this feature together with phones in the “auto call test mode” (see section 8.3.2) for test purposes. This mode is also active if the phone is on the charger.

1 Press the **Menu** soft key.
2 Enter the following key sequence “***76#” (Mitel 600) or “R***76#” (Mitel 142d).
3 Select Auto Answer.
4 Press OK.
5 Enter a number of seconds the phone shall ring before it will answer the call.
6 Press OK.
7 Enter a number of seconds a call shall be active.
8 Press OK. The test will be started automatically.
9 To stop the test, switch the phone off and on again.

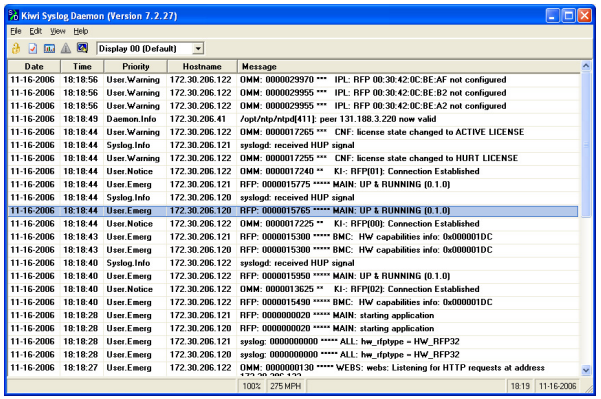
8.3.4 SYSLOG

The OpenMobility Manager and the RFPs are capable of propagating Syslog messages conforming to RFC 3164 (see /13/). This feature together with the IP address of a host collecting these messages can be configured.

Syslog must be enabled by:

- DHCP using the public options 227 and 228.
- Setting the syslog daemon server and port via the web interface.

To set up the syslog via DHCP or the OM Configurator has the advantage that syslogs are available in earlier states of the RFP startup.



The level of syslog messages in the default state allows the user to have control over the general system state and major failures.

8.3.5 SSH USER SHELL

Each RFP offers a lot of commands within the SSH shell. Most of them are useful for diagnostics and may help experts to resolve failures.

Note: Some commands can harm the system operation.

The SSH access of an RFP is open if

- the RFP is connected to an OMM and the “Remote Access” is switched on or
- the RFP is not connected to an OMM.

To activate the SSH access of an RFP that has a connection to an OMM, enable the **Remote access** checkbox on the OMM **System settings** web page (see section 5.4.1.1). In the OMP, the SSH access is activated/deactivated in the **General** tab of the **System** -> **Basic settings** menu (see section 6.5.1).

8.3.5.1 Login

To log into the SSH user shell:

1 Open an SSH session to the IP DECT base station with the “Full access” user name.
2 Enter the password for the “Full access” account (see also 7.17.1).

The output should look like:

```
Welcome to IP RFP OpenMobility SIP Only Version 2.1.x

last reset cause: hardware reset (Power-on reset)

omm@172.30.206.94's password:
omm@172.30.206.94 >
```

8.3.5.2 Command Overview

Type `help` to get a command overview:

Command	Description
exit,quit,bye	Leave session
ommconsole	OMM console
ip_rfpconsole	RFP console
rfpm_console	RFP manager console
wlan_console	WLAN console
ics_console	ICS console
ldb	View / set local configuration (OmConfigurator)
setconsole	Duplicate messages to console
noconsole	Do not duplicate messages to console
dmesg	Messages from last boot
logread	Last messages
su	Switch to user root

ping	Well known ping
traceroute	Well known traceroute
free	Well known free
ps	Well known ps
top	Well known top
ifconfig	Well known ifconfig
uptime	Well known uptime
reboot	Well known reboot
date	Well known date (time in UTC)

8.3.5.3 OMM Console On Linux Server

You can call the OMM console on the Linux server which runs the OMM using the “ommconsole” command. Log on as root as it is necessary to install and/or update OMM.

IMPORTANT : If you not login as root to open the OMM console then the path to ommconsole is not set and you must enter the whole path “/usr/sbin/ommconsole” to start the OMM console.

8.3.5.4 RFP Console Commands

If you type `ip_rfpconsole` you are able to use the following commands on each RFP:

Command	Description
?	Displays Command Help Table
bt	Bluetooth commands
confmix	Displays status of conference mixer
help	Displays Command Help Table
logger	Send a string to the syslog daemon
deftrc	Resets all trace settings to default
runtime	Reports the process runtime
mem	Show memory and heap
exit	Leave this console
heap	Shows heap buffer statistics
heapcheck	Verifies the guard space of all via doss allocated buffer. Heap functions are locked during check
heapdetails	Print detailed heap usage
jpeg	Jpeg helper commands
lu10	Lu10 SDU <-> PDU converter
mclose	Close a media channel

Command	Description
mconf	Configure IP settings for a media channel
media	Display state of media channels
mopen	Open a media channel
mroute	Display media routes
mstart	Start a media channel
mstop	Stop a media channel
mswo	Codec switch over for an active call
mtime	Display media time statistics
mutex	Lists all created MXP mutexes
omms	Shows connection status to OMM(s)
otpdbCheck	Check all OTP pages for valid elements
queues	Lists all created MXP queues
reset	Resets the IPRFP application
resume	Resume bmc activity
sem	Lists all created MXP semaphores
signals	Print signal dwell time in queues
spy	Set/display spy levels: [<key #> <level #>]
suspend	Suspend bmc activity
tasks	Lists all running MXP tasks
tickres	Print tick resolution
timer	Print running timer
video	Video commands

Please note: The “spy” command enables you to increase the level of syslog messages. This should be only used by instructions of the support organization because it can harm the system operation.

8.3.5.5 OMM Console Commands

If you have opened the session on the OMM RFP and you type “ommconsole”, you are able to use the following OpenMobility Manager (OMM) related commands:

Command	Description
?	Displays Command Help Table
adb	Automatic DB export and import (ADB) console
axi	AXI commands
axic	Task console for AXI command processing of provisioning files

Command	Description
cert	Certificate import console
cmi	CMI commands
cnf	Show configuration parameters
cron	Display pending cron jobs
help	Displays Command Help Table
logger	Send a string to the syslog daemon
deftrc	Resets all trace settings to default
dlc	DECT Data Link Control
dm	Download Over Air Manager
dsip	DSIP commands
epr	External provisioning task (EPR) console and dynamic users console
runtime	Report the process runtime
mem	Show memory and heap
exit	Leave this console
gmi	DECTnet2 Inter Working Unit
hcm	Handset configuration management task (HCM) console
heartbeat	Configure heartbeat mechanism for IP-RFPs
ima	IMA commands
inspect	Display information of a user
ipc	Display socket communication
ipl	Display connected RFPs
iplfilter	Configure which RFPs spy messages are generated for
lic	LIC commands
loc	Info about locating extension
mon	Toggle monitor functionality
msm	Display states within MediaStreamManagement
msmtrc	Display / modify list of traced DECT phoneNs
mutex	List all created MXP mutexes
nwk	DECT network layer
prov	Prov-related commands
queues	List all created MXP queues
rcmd	Remote command on RFPs shell
rfp	Radio Fixed Part Control
rfpd	Radio Fixed Part Debug
rfps	Radio Fixed Part Statistic

Command	Description
rping	Request one or more RFPs to ping a host
rspy	Remote configure spy levels on IP-RFPs
rsx	Toggle RSX debug port on RFPs
rtt	Set event flag for high RTT values / clear values
sem	List all created MXP semaphores
spy	Set/display spy levels: [<key #> <level #>]
standby	Displays redundant OMMs
stat	Statistic
sync	Commands for RFP synchronization
sysdump	Initiate system dump
tasks	List all running MXP tasks
tickres	Print tick resolution
trc	Back trace task
tzone	Time zone commands
uds	UDS commands
umo	UMO commands
upd	Display update status of RFPs
update	Force all connected RFPs to search for new software
uptime	Display OpenMobility Manager uptime
ver	Version information
video	Command for video devices
wlan	Display states within Wireless LAN Management
xml	XML browser task (XML) console
xsc	XSC commands

Please note: The “spy” command enables you to increase the level of syslog messages especially for subsystems of the OMM. This should be only used by instructions of the support organization because it can harm the system operation.

8.3.6 CORE FILE CAPTURING

Fatal software problems may result in memory dumps, so called core files. These core files are helpful in analyzing the problem that caused the abnormal termination of the program. The IP RFP is capable of transferring the core files to a remote fileserver. Without any special configuration the files are transferred to the TFTP server that is used to get the system software. The path used is the directory of

the boot image. These two configuration items are retrieved from DHCP or via local configuration using the OM Configurator.

You can configure the URL to a writable directory via the OMM (see section 5.4.1.12) or through the “OM_CoreFileSrvUrl” variable in the ipdect.cfg configuration files.

> **Please note:** The server must allow writing new files (not typically enabled by default).

8.3.7 DECT MONITOR

> **Please note:** The DECT Monitor has been replaced by OMP but the DECT Monitor can still be used without warranty for SIP-DECT installations with a standard PARK and up to 256 RFPs all within paging area 0.

For better error detection in the SIP-DECT system the DECT Monitor can be used. The DECT Monitor is an MS Windows based stand-alone program. It provides the possibility to give a real-time overview of the current IP DECT base station and telephone states in the SIP-DECT system.

The following features are provided by the DECT Monitor:

- Reading out of the DECT configuration of an SIP-DECT system.
- Configuration can be stored in an ASCII file.
- Display of DECT transactions IP DECT base station <–> telephone in clear tabular form with highlighting of handover situations. Real-time display.
- Display of further events concerning the status or actions of IP DECT base stations and telephones of the SIP-DECT system.
- All events can also be recorded in a log file.
- Display of the synchronization relations between the RFPs.
- Monitoring of systems with up to 256 IP DECT base stations and 512 DECT phones.
- Reading out and display of IP DECT RFP statistics data, either for a single IP DECT RFP or for all IP DECT RFPs.
- Display of DECT central data of the SIP-DECT system.

The DECT Monitor program can only be used when the **DECT monitor** checkbox is activated on the flag in the OMM **System settings** web page.

> **Please note:** Because of security, the DECT monitor flag is not stored permanently in the internal flash memory of the OMM/RFP. After a reset the DECT monitor flag is disabled.

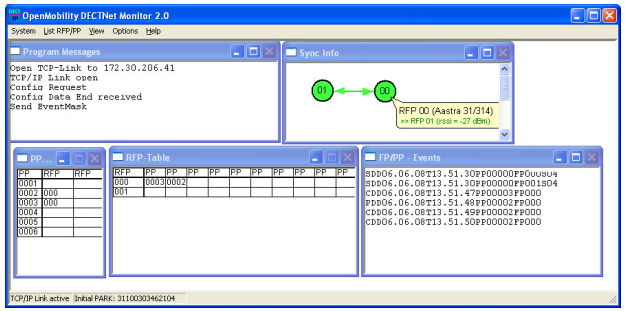
The DECT monitor program is used together with the SIP-DECT system. When the program is started, the user is requested to enter the IP address of the IP DECT RFP or the server running the OpenMobility Manager (OMM) software.

There can be several reasons for an unsuccessful link establishment:

- Operation of DECT monitor is not enabled inside the OMM. Use the OMM web service to enable DECT monitor operation.

- IP address is not correct. It must be the address of the RFP the OMM is running on.
- A link routed to the RFP is not supported.

The program displays the IP address which was used last time. When the program is started, a link to the OMM is automatically established and the program window shows all user configured child windows and tables. When all links have been established, the DECT data of the system are automatically read out and entered in the tables “RFP-Table” and “DECT phone-Table”. This procedure is called “Config Request”.



Next, the defined trace options (Event Mask) are sent to the OMM. The options which are sent to the OMM are always those which were active the last time the program was exited.

If the trace option “Transaction establish/release” is activated, the OMM will deliver all existing transactions.

Following this, the OMM system delivers the desired trace data. The user can either communicate with the program interactively (see below) or he can simply activate a log file in which to record the data.

Following this initialization, the user can carry out the following modifications:

- The trace settings can be modified using the menu item **Options-Event Mask**. Transmission to the OMM takes place after confirmation of the settings with **OK**.
- A Config Request can be sent again to the OMM.
- A log file can be activated.
- By means of various dialogs, the configuration data of the telephones, RFPs and control modules can be displayed and stored in ASCII files.

The following information is displayed dynamically in the tables:

- Transactions between telephone and DECT system. These are displayed in both tables. Simple transactions are displayed in black on a white background; during handover, both transactions involved are displayed in white on a red background.
- The Location Registration and Detach events are displayed in the tables for approx. 1-2s after their occurrence (light green background), if possible. There is no display in the FP table if there is no column free for display. If the event has already been displayed, it can be overwritten at any time. The events are not displayed if they occur during an on-going transaction. Irrelevant of whether the events are displayed in the tables, they are always entered in the **FP/DECT phone-Events** window and in the log file (provided that this is open).

The following color scheme is used for display of the RFPs in the RFP table:

- RFP gray-blue: IP DECT base station is not active (not connected or disturbance).
- RFP black: IP DECT base station is active.

The data of an RFP are displayed in a dialogue box after clicking on the respective RFP field in the RFP table. The statistics data of the RFP can be called up from this dialogue box.

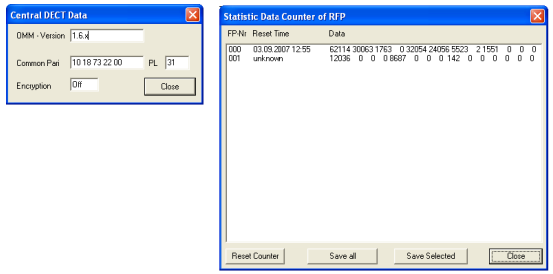
The following color scheme is used for display of the telephone in the DECT phone table:

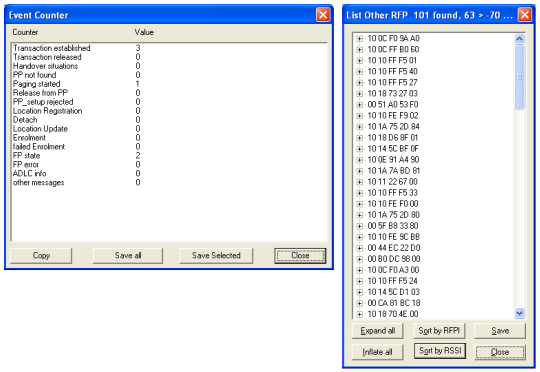
- DECT phone black: Handset is enrolled. It is assumed that the telephone can be reached.
- DECT phone blue: Handset can presumably not be reached. Detach was received, or when an attempt was made to reach a telephone, the DECT phone did not answer.
- DECT phone gray blue: Handset not enrolled.

The data of a telephone are displayed in a dialog box after clicking on the respective telephone field in the FP table.

The **Sync Info** child window contains all IP DECT base stations and shows their synchronization and relation states to each other. Selecting the IP DECT base stations with the right mouse button, the user can change visibility views and can even force a resynchronization of an IP DECT base station.

There are several optional child windows selectable. They are all listed below and give some more information about the SIP-DECT systems. Mostly they are statistics and for internal use only.





9 REGULATORY COMPLIANCE AND SAFETY INFORMATION

9.1 MITEL RFP44/45/47/48

9.1.1 SUPPORTING DOCUMENTATION

For information on how to install and configure your Mitel RFP Base station and to access system-specific documentation, do the following:

1 Log in to **Mitel Connect**.
2 In left-hand menu, click **Mitel OnLine**.
3 Click **Product Documentation** under the **Technical Support** section
4 Select **SIP-DECT** under the **Phones** drop-down menu.

9.1.2 IMPORTANT SAFETY INSTRUCTIONS AND PRECAUTIONS

These notices may appear on the product or in the technical documentation:

DANGER	Danger indicates an imminently hazardous situation which, if not avoided, will result in death or serious injury.
WARNING	Warning indicates a potentially hazardous situation which, if not avoided, could result in death or serious injury.
CAUTION	Caution indicates a potentially hazardous situation which, if not avoided, may result in minor or moderate injury and/or damage to the equipment or property.

This symbol may appear on the product:

⚠	The exclamation point within an equilateral triangle indicates that important operatingandmaintenance(servicing)instructionsareincludedintheliterature accompanying the product.

To ensure safe and proper use, please read the following information carefully before using this product. The safety instructions include important information on safe handling of the product and on general safety issues. Cautions regarding the device connected to this product are also included.

WARNING: KEEP THE CORD AND CABLES AWAY FROM CHILDREN.

WARNING: IF THE DEVICE HAS A GROUND WIRE, IT MUST BE USED TO PREVENT ELECTROCUTION OR POWER SURGES.

WARNING: THIS PRODUCT MUST BE INSTALLED IN A LIGHTNING PROTECTED ENVIRONMENT.

CAUTION: VERIFY ALL CABLES ARE PROPERLY AND SAFELY CONNECTED BEFORE USING THIS PRODUCT.

CAUTION: DO NOT USE OR STORE THIS PRODUCT UNDER THE FOLLOWING CONDITIONS TO AVOID POTENTIAL DAMAGE TO THIS PRODUCT:

- Hard vibrations
- Tilted or unstable places
- Humid or dusty places
- Strong electromagnetic field (near magnets, radio or wireless device)

Maintenance and Repair: There are no user serviceable parts inside this device. For repairs, return the device to an authorized Mitel dealer.

9.1.3 SAFETY INSTRUCTIONS REGARDING RADIO WAVES

Note the following instructions:

- Do not use this product near medical devices such as a heart pacemaker. The radio wave generated by this product may interfere with the operation of these devices and may threaten one's life.
- Do not use this product near microwave ovens. The radio wave used by microwave ovens may cause interference to this product.
- The antennas must be installed at least 20 cm from all personnel.

Notes on Wireless Devices Using 2.4GHz Band

This product uses a 2.4GHz band. This band of equipment is used by a microwave, industry, science, medical equipment and licensed in room or low power (non-licensed) radio stations.

1 Before you use this equipment, verify that it will not interfere with other broadcasting.
2 If interference happens, stop using the equipment or change the band. Contact Mitel to discuss ways of avoiding interference (for example, create a wall).

Notes on Wireless Devices Using 5GHz Band

This product uses a 5GHz band. Note that this product cannot be used in Ad hoc mode when it is running in 5GHz band. Use Infrastructure mode when running in 5GHz band. Maximum radio frequency power is 100mW.

9.1.4 NOTES ON SECURITY

Because a WLAN uses electromagnetic signals instead of a network cable to establish communication with network devices, it has the advantage of allowing devices to connect to the network easily. However, a disadvantage of this is that within a certain range, the electromagnetic signals can pass through barriers such as walls, and if security countermeasures are not implemented in some way, problems such as the following may occur:

- Communication is intercepted by a third party
- Unauthorized access to the network
- Leakage of personal information (ID and card information)

- Spoofing and the falsification of intercepted data
- System crashes and data corruption

Nowadays, WLAN cards or access points are equipped with security measures that address such security problems, so that you can enable security-related settings for WLAN products in order to reduce the likelihood of problems occurring.

It is recommend that you make yourself fully acquainted with the possible implications of what might happen if you use a wireless product without enabling security features, and that you configure security-related settings and use wireless products at your own responsibility.

9.1.5 NOTICE TO CANADIAN CUSTOMERS

This Class B digital apparatus complies with Canadian ICES-003.

CAN ICES-3 (B)/NMB-3(B)

IC: 1884E-68645001

9.1.6 NOTICE TO U.S. CUSTOMERS

FCC ID: **UOU**68645001

NOTE: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

NOTE: Changes or modifications not expressly approved by Mitel Networks Corporation may void the user's right to operate the equipment.

Refer all servicing to a Mitel authorized repair facility. If you require a Mitel return authorization number, or information on obtaining service or repairs, please contact Mitel at the following telephone number: 1-800-722-1301.

A Mitel return authorization number must be obtained before sending equipment to the Mitel repair facility.

Repair facility:

Mitel Networks

2160 West Broadway, Suite #103

Mesa, AZ

U.S.A 85202

Email: us_repair@mitel.com

9.1.7 NOTICE TO EUROPEAN CUSTOMERS

CE

English

We, Mitel Networks Corporation, declare that the RFP models 44, 45, 47 and 48 meet the essential requirements of Directives 2014/53/EC (RED) and 2011/65/EU (RoHS). A copy of this declaration may be found at the following internet address:

https://www.mitel.com/legal/regulatory-declarations

Any unauthorized modification of the product voids this declaration. For a copy of the original signed Declaration Of Conformity please contact Mitel at the following address:

Mitel Deutschland GmbH

Zeughofstrasse 1

10997 Berlin

Germany

9.1.8 NOTICE TO CUSTOMERS IN AUSTRALIA

- Do not use in areas where there are explosive hazards.
- Manufacturer: Mitel Networks Corporation 350 Legget Drive, Kanata, Ontario, Canada.
- Importer: Mitel Networks Corporation 350 Legget Drive, Kanata, Ontario, Canada.

9.1.9 NOTICE TO U.S. CUSTOMERS

FCC ID: **UOU**68645001

NOTE: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.

- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

NOTE: Changes or modifications not expressly approved by Mitel Networks Corporation may void the user's right to operate the equipment.

Refer all servicing to a Mitel authorized repair facility. If you require a Mitel return authorization number, or information on obtaining service or repairs, please contact Mitel at the following telephone number: 1-800-722-1301.

A Mitel return authorization number must be obtained before sending equipment to the Mitel repair facility.

Repair facility:

Mitel Networks

2160 West Broadway, Suite #103

Mesa, AZ

U.S.A 85202

Email: us_repair@mitel.com

10 SAFETY INFORMATION (3RD GENERATION DECT BASE STATIONS)

10.1 CE MARKING

This certifies the conformity of the product placed on the market prior to June 13th 2017 with the regulations which apply in accordance with the RTTE Directive 1999/5/EC.

For a copy of the original signed declaration (in full conformance with EN45014), contact the Regulatory Approvals Manager at Mitel Networks Ltd., Castlegate Business Park, Portskewett, Monmouthshire, NP26 5Yr, United Kingdom, or visit http://www.mitel.com/regulatory-declarations.

On or after June 13th 2017 hereby, Mitel Networks declares that the product is in compliance with Directive 2014/53/EU. The full text of the EU declaration of conformity is available at the following internet address: http://www.mitel.com/regulatory-declarations.

10.2 COMMUNICATIONS REGULATION INFORMATION

The regulation information in this section applies to the following supported DECT base stations:

- RFP 32 IP
- RFP 34 IP
- RFP 35 IP
- RFP 36 IP
- RFP 37 DRC

10.2.1 FCC NOTICES (U.S. ONLY)

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Modifications not expressly approved by this company could void the user's authority to operate the equipment.

NOTE: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

- Consult the dealer or an experienced radio/TV technician for help.

10.3 HEALTH AND SAFETY

10.3.1 EXPOSURE TO RADIO FREQUENCY (RF) SIGNALS:

The wireless phone is a radio transmitter and receiver. It is designed and manufactured not to exceed the emission limits for exposure to radio frequency (RF) energy set by the Federal Communications Commission (FCC) of the U.S. Government. These limits are part of comprehensive guidelines and establish permitted levels of RF energy for the general population. The guidelines are based on the safety standards previously set by both U.S. and international standards bodies. These standards include a substantial safety margin designed to assure the safety of all persons, regardless of age and health.

This device and its antenna must not be co-located or operating in conjunction with any other antenna or transmitter.

The radiating element of the RFP should be installed during operating at a separation distance greater than 20 cm between user and device. The device complies with the requirements for routine evaluation limits.

10.3.2 INDUSTRY CANADA (CANADA ONLY)

Operation of this device is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.

Privacy of communications may not be ensured when using this telephone.

Exposure to Radio Frequency (RF) Signals:

The wireless phone is a radio transmitter and receiver. It is designed and manufactured not to exceed the emission limit for exposure to radio frequency (RF) energy set by the Ministry of Health (Canada), Safety Code 6. These limits are part of comprehensive guidelines and established permitted levels of RF energy for the general population. These guidelines are based on the safety standards previously set by international standard bodies. These standards include a substantial safety margin designed to assure the safety of all persons, regardless of age and health.

This device and its antenna must not be co-located or operating in conjunction with any other antenna or transmitter.

The radiating element of the RFP should be installed during operating at a separation distance greater than 20 cm between user and device. This device complies with the requirements for routine evaluation limits.

10.4 INFORMATIONS RÉGLEMENTAIRES EN MATIÈRE DE COMMUNICATIONS

Les informations dans cette section concerne les suivantes stations radio :

- RFP 32 IP

- RFP 34 IP
- RFP 35 IP
- RFP 36 IP
- RFP 37 DRC

10.4.1 NOTES FCC (USA UNIQUEMENT)

Cet appareil est conforme à la partie 15 des règles FCC. Son exploitation est soumise aux deux conditions suivantes: (1) Cet appareil ne doit causer aucune interférence dommageable et (2) cet appareil doit tolérer toute interférence reçue à l'inclusion des interférences susceptibles de causer une opération non désirée. Les modifications non expressément agrées par cette entreprise pourraient rendre caduque l'habilitation de l'utilisateur à exploiter cet équipement.

NOTA: Cet équipement a été testé et jugé conforme aux limitations pour un appareil numérique de classe B en vertu de la partie 15 des règles FCC. Ces limitations ont été conçues pour garantir une protection raisonnable contre les interférences dommageables dans les installations résidentielles. Cet équipement génère, utilise et peut rayonner des ondes radio et peut causer des interférences dommageables dans les communications par radio s'il n'est pas installé et utilisé conformément aux instructions. Cependant, l'absence d'interférences dans une installation particulière n'est pas garantie. Si cet équipement perturbe de façon importante la réception de la radio ou de la télévision (interférences qui peuvent être déterminées en arrêtant et en remettrant l'appareil en marche), l'utilisateur est invité à tenter de corriger les interférences en prenant une ou plusieurs des mesures suivantes:

- Réorienter ou déplacer l'antenne de réception.
- Éloigner l'équipement du récepteur.
- Raccorder l'équipement à une prise d'un circuit différent de celui auquel est raccordé le récepteur.
- Consulter le revendeur ou un technicien radio/TV.

11 SAFETY INFORMATION (4TH GENERATION DECT BASE STATIONS)

11.1 CE MARKING

We, Mitel Networks Corporation, declare that the RFP 45, RFP 47, RFP 47 DRC and RFP 48 meet the essential requirements of Directives 2014/53/EC (RED) and 2011/65/EU (RoHS). A copy of this declaration may be found at the following internet address:

https://www.mitel.com/legal/regulatory-declarations

Any unauthorized modification of the product voids this declaration. For a copy of the original signed Declaration Of Conformity please contact Mitel at the following address:

Mitel Deutschland GmbH
Zeughofstrasse 1
10997 Berlin
Germany

11.2 COMMUNICATIONS REGULATION INFORMATION

The regulation information in this section applies to the following supported DECT base stations:

- RFP 45
- RFP 47
- RFP 47 DRC
- RFP 48

11.2.1 FCC NOTICES (U.S. ONLY)

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Refer all servicing to a Mitel authorized repair facility. If you require a Mitel return authorization number, or information on obtaining service or repairs, please contact Mitel at the following telephone number: 1-800-722-1301.

A Mitel return authorization number must be obtained before sending equipment to the Mitel repair facility.

Repair facility:
Mitel Networks
2160 West Broadway, Suite #103
Mesa, AZ
U.S.A 85202
Email: us_repair@mitel.com

11.3 HEALTH AND SAFETY

11.3.1 EXPOSURE TO RADIO FREQUENCY (RF) SIGNALS:

The wireless phone is a radio transmitter and receiver. It is designed and manufactured not to exceed the emission limits for exposure to radio frequency (RF) energy set by the Federal Communications Commission (FCC) of the U.S. Government. These limits are part of comprehensive guidelines and establish permitted levels of RF energy for the general population. The guidelines are based on the safety standards previously set by both U.S. and international standards bodies. These standards include a substantial safety margin designed to assure the safety of all persons, regardless of age and health.

This device and its antenna must not be co-located or operating in conjunction with any other antenna or transmitter.

The radiating element of the RFP should be installed during operating at a separation distance greater than 20 cm between user and device. The device complies with the requirements for routine evaluation limits.

11.3.2 INNOVATION, SCIENCE AND ECONOMIC DEVELOPMENT (ISED) CANADA

This device contains licence-exempt transmitter(s)/receiver(s) that comply with Innovation, Science and Economic Development Canada’s licence-exempt RSS(s).

Operation is subject to the following 2 conditions:

1. This device may not cause interference.
2. This device must accept any interference, including interference that may cause undesired operation of the device.

Exposure to Radio Frequency (RF) Signals:

The wireless phone is a radio transmitter and receiver. It is designed and manufactured not to exceed the emission limit for exposure to radio frequency (RF) energy set by the Ministry of Health (Canada), Safety Code 6. These limits are part of comprehensive guidelines and established permitted levels of RF energy for the general population. These guidelines are based on the safety standards previously set by international standard bodies. These standards include a substantial safety margin designed to assure the safety of all persons, regardless of age and health.

This device and its antenna must not be co-located or operating in conjunction with any other antenna or transmitter.

The radiating element of the RFP should be installed during operating at a separation distance greater than 20 cm between user and device. This device complies with the requirements for routine evaluation limits.

11.4 INFORMATIONS RÉGLEMENTAIRES EN MATIÈRE DE COMMUNICATIONS

Les informations dans cette section concerne les suivantes stations radio :

- RFP 32 IP
- RFP 34 IP
- RFP 35 IP
- RFP 36 IP
- RFP 37 DRC

11.4.1 NOTES FCC (USA UNIQUEMENT)

Cet appareil est conforme à la partie 15 des règles FCC. Son exploitation est soumise aux deux conditions suivantes: (1) Cet appareil ne doit causer aucune interférence dommageable et (2) cet appareil doit tolérer toute interférence reçue à l'inclusion des interférences susceptibles de causer une opération non désirée. Les modifications non expressément agrées par cette entreprise pourraient rendre caduque l'habilitation de l'utilisateur à exploiter cet équipement.

NOTA: Cet équipement a été testé et jugé conforme aux limitations pour un appareil numérique de classe B en vertu de la partie 15 des règles FCC. Ces limitations ont été conçues pour garantir une protection raisonnable contre les interférences dommageables dans les installations résidentielles. Cet équipement génère, utilise et peut rayonner des ondes radio et peut causer des interférences dommageables dans les communications par radio s'il n'est pas installé et utilisé conformément aux instructions. Cependant, l'absence d'interférences dans une installation particulière n'est pas garantie. Si cet équipement perturbe de façon importante la réception de la radio ou de la télévision (interférences qui peuvent être déterminées en arrêtant et en remettrant l'appareil en marche), l'utilisateur est invité à tenter de corriger les interférences en prenant une ou plusieurs des mesures suivantes:

- Réorienter ou déplacer l'antenne de réception.
- Éloigner l'équipement du récepteur.
- Raccorder l'équipement à une prise d'un circuit différent de celui auquel est raccordé le récepteur.
- Consulter le revendeur ou un technicien radio/TV.

11.5 SANTÉ ET SÉCURITÉ

11.5.1 EXPOSITION AUX SIGNAUX RADIO (RF)

Votre téléphone sans fil est un émetteur-récepteur radio. Il a été conçu pour ne pas dépasser les limitations en matière d'exposition aux ondes radio établies par la Federal Communications Commission

(FCC) du gouvernement des États-Unis. Ces limitations font partie de directives complètes et établissent des niveaux admissibles d'énergie RF pour l'ensemble de la population. Ces directives sont basées sur des normes de sécurité établies par des organes de normalisation américains et internationaux. Ces normes intègrent une importante marge de sécurité censée garantir la sécurité de toute personne, quels que soient son âge et son état de santé.

Cet appareil et son antenne ne doivent pas être installés ou exploités conjointement avec d'autres antennes ou émetteurs.

L'élément rayonnant de la station radio doit être installé à une distance de 20 cm ou plus entre l'utilisateur et l'appareil. Cet appareil est conforme aux exigences relatives aux limites d'évaluation de routine .

11.5.2 INDUSTRIE CANADA (CANADA UNIQUEMENT)

L'exploitation de cet appareil est soumise aux deux conditions suivantes: (1) Cet appareil ne doit causer aucune interférence et (2) cet appareil doit tolérer toute interférence reçue à l'inclusion des interférences susceptibles de causer une opération non désirée.

La confidentialité des communications risque de ne pas être garantie lorsque vous utilisez ce téléphone.

Exposition aux ondes radio (RF):

Votre téléphone sans fil est un émetteur-récepteur radio. Il a été conçu pour ne pas dépasser les limitations en matière d'exposition aux ondes radio émises par le Ministère de la Santé (Canada,) Code de sécurité 6. Ces limitations font partie de directives complètes et établissent des niveaux admissibles d'énergie RF pour l'ensemble de la population. Ces directives sont basées sur des normes de sécurité établies par des organes de normalisation internationaux.

Ces normes intègrent une importante marge de sécurité censée garantir la sécurité de toute personne, quels que soient son âge et son état de santé.

Cet appareil et son antenne ne doivent pas être installés ou exploités conjointement avec d'autres antennes ou émetteurs.

L'élément rayonnant de la station radio doit être installé à une distance de 20 cm ou plus entre l'utilisateur et l'appareil. Cet appareil est conforme aux exigences relatives aux limites d'évaluation de routine .

12 SAFETY INFORMATION (3RD GENERATION DECT BASE STATIONS)

12.1 CE MARKING

This certifies the conformity of the product placed on the market prior to June 13th 2017 with the regulations which apply in accordance with the RTTE Directive 1999/5/EC.

For a copy of the original signed declaration (in full conformance with EN45014), contact the Regulatory Approvals Manager at Mitel Networks Ltd., Castlegate Business Park, Portskewett, Monmouthshire, NP26 5Yr, United Kingdom, or visit http://www.mitel.com/regulatory-declarations.

On or after June 13th 2017 hereby, Mitel Networks declares that the product is in compliance with Directive 2014/53/EU. The full text of the EU declaration of conformity is available at the following internet address: http://www.mitel.com/regulatory-declarations.

12.2 COMMUNICATIONS REGULATION INFORMATION

The regulation information in this section applies to the following supported DECT base stations:

- RFP 32 IP
- RFP 34 IP
- RFP 35 IP
- RFP 36 IP
- RFP 37 DRC

12.2.1 FCC NOTICES (U.S. ONLY)

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Modifications not expressly approved by this company could void the user's authority to operate the equipment.

NOTE: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

- Consult the dealer or an experienced radio/TV technician for help.

12.3 HEALTH AND SAFETY

12.3.1 EXPOSURE TO RADIO FREQUENCY (RF) SIGNALS:

The wireless phone is a radio transmitter and receiver. It is designed and manufactured not to exceed the emission limits for exposure to radio frequency (RF) energy set by the Federal Communications Commission (FCC) of the U.S. Government. These limits are part of comprehensive guidelines and establish permitted levels of RF energy for the general population. The guidelines are based on the safety standards previously set by both U.S. and international standards bodies. These standards include a substantial safety margin designed to assure the safety of all persons, regardless of age and health.

This device and its antenna must not be co-located or operating in conjunction with any other antenna or transmitter.

The radiating element of the RFP should be installed during operating at a separation distance greater than 20 cm between user and device. The device complies with the requirements for routine evaluation limits.

12.3.2 INDUSTRY CANADA (CANADA ONLY)

Operation of this device is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.

Privacy of communications may not be ensured when using this telephone.

Exposure to Radio Frequency (RF) Signals:

The wireless phone is a radio transmitter and receiver. It is designed and manufactured not to exceed the emission limit for exposure to radio frequency (RF) energy set by the Ministry of Health (Canada), Safety Code 6. These limits are part of comprehensive guidelines and established permitted levels of RF energy for the general population. These guidelines are based on the safety standards previously set by international standard bodies. These standards include a substantial safety margin designed to assure the safety of all persons, regardless of age and health.

This device and its antenna must not be co-located or operating in conjunction with any other antenna or transmitter.

The radiating element of the RFP should be installed during operating at a separation distance greater than 20 cm between user and device. This device complies with the requirements for routine evaluation limits.

12.4 INFORMATIONS RÉGLEMENTAIRES EN MATIÈRE DE COMMUNICATIONS

Les informations dans cette section concerne les suivantes stations radio :

- RFP 32 IP
- RFP 34 IP

- RFP 35 IP
- RFP 36 IP
- RFP 37 DRC

12.4.1 NOTES FCC (USA UNIQUEMENT)

Cet appareil est conforme à la partie 15 des règles FCC. Son exploitation est soumise aux deux conditions suivantes: (1) Cet appareil ne doit causer aucune interférence dommageable et (2) cet appareil doit tolérer toute interférence reçue à l'inclusion des interférences susceptibles de causer une opération non désirée. Les modifications non expressément agrées par cette entreprise pourraient rendre caduque l'habilitation de l'utilisateur à exploiter cet équipement.

NOTA: Cet équipement a été testé et jugé conforme aux limitations pour un appareil numérique de classe B en vertu de la partie 15 des règles FCC. Ces limitations ont été conçues pour garantir une protection raisonnable contre les interférences dommageables dans les installations résidentielles. Cet équipement génère, utilise et peut rayonner des ondes radio et peut causer des interférences dommageables dans les communications par radio s'il n'est pas installé et utilisé conformément aux instructions. Cependant, l'absence d'interférences dans une installation particulière n'est pas garantie. Si cet équipement perturbe de façon importante la réception de la radio ou de la télévision (interférences qui peuvent être déterminées en arrêtant et en remettrant l'appareil en marche), l'utilisateur est invité à tenter de corriger les interférences en prenant une ou plusieurs des mesures suivantes:

- Réorienter ou déplacer l'antenne de réception.
- Éloigner l'équipement du récepteur.
- Raccorder l'équipement à une prise d'un circuit différent de celui auquel est raccordé le récepteur.
- Consulter le revendeur ou un technicien radio/TV.

12.5 SANTÉ ET SÉCURITÉ

12.5.1 EXPOSITION AUX SIGNAUX RADIO (RF)

Votre téléphone sans fil est un émetteur-récepteur radio. Il a été conçu pour ne pas dépasser les limitations en matière d'exposition aux ondes radio établies par la Federal Communications Commission (FCC) du gouvernement des États-Unis. Ces limitations font partie de directives complètes et établissent des niveaux admissibles d'énergie RF pour l'ensemble de la population. Ces directives sont basées sur des normes de sécurité établies par des organes de normalisation américains et internationaux. Ces normes intègrent une importante marge de sécurité censée garantir la sécurité de toute personne, quels que soient son âge et son état de santé.

Cet appareil et son antenne ne doivent pas être installés ou exploités conjointement avec d'autres antennes ou émetteurs.

L'élément rayonnant de la station radio doit être installé à une distance de 20 cm ou plus entre l'utilisateur et l'appareil. Cet appareil est conforme aux exigences relatives aux limites d'évaluation de routine .

12.5.2 INDUSTRIE CANADA (CANADA UNIQUEMENT)

L'exploitation de cet appareil est soumise aux deux conditions suivantes: (1) Cet appareil ne doit causer aucune interférence et (2) cet appareil doit tolérer toute interférence reçue à l'inclusion des interférences susceptibles de causer une opération non désirée.

La confidentialité des communications risque de ne pas être garantie lorsque vous utilisez ce téléphone.

Exposition aux ondes radio (RF):

Votre téléphone sans fil est un émetteur-récepteur radio. Il a été conçu pour ne pas dépasser les limitations en matière d'exposition aux ondes radio émises par le Ministère de la Santé (Canada,) Code de sécurité 6. Ces limitations font partie de directives complètes et établissent des niveaux admissibles d'énergie RF pour l'ensemble de la population. Ces directives sont basées sur des normes de sécurité établies par des organes de normalisation internationaux.

Ces normes intègrent une importante marge de sécurité censée garantir la sécurité de toute personne, quels que soient son âge et son état de santé.

Cet appareil et son antenne ne doivent pas être installés ou exploités conjointement avec d'autres antennes ou émetteurs.

L'élément rayonnant de la station radio doit être installé à une distance de 20 cm ou plus entre l'utilisateur et l'appareil. Cet appareil est conforme aux exigences relatives aux limites d'évaluation de routine .

13 APPENDIX

This Appendix contains additional information and examples for configuring your SIP-DECT system.

13.1 PRE-CONFIGURATION FILE RULES

The following file format description can be used to administrate the RFP and DECT phone configuration with external applications, e.g. an external configuration management tool or a PBX communications system.

The framework of the text file follows strictly defined rules. The main framework is divided in two parts:

3 An **instruction section** is used to drive a generic data creation for those fields not filled within data sequence section.

4 A data sequence section defines data record fields. Each of them is explicitly set.

Layout rules in detail are:

- Comments start with “#”.
- Each record is terminated by the regular expressions “\r” or “\n”.
- Instruction settings are made like: <tag> = <value>.
- Data sequence sections start with the key word “data_sequence”. This key word is **mandatory** for file processing to proceed. All instructions must be written before this row.
- Data sequence record fields are separated by colon “;”. Colons have also to be set for empty fields if at least one follows which is not empty. Otherwise a position mismatch of fields will occur.
- If fields have several values assigned (that may be true for a few local RFP configuration fields like “ntp_address”), they must be separated by comma “,”.

Notes:

- Because data sequence fields are separated by a colon, the content of that section can be generated by a *.csv export of Excel Sheet and copied into the configuration file.
- Instructions are only processed on those fields that are left empty within the data sequence section.

13.2 DECT PHONE CONFIGURATION FILE (OMM DATABASE)

13.2.1 SUPPORTED INSTRUCTIONS

Instruction	Explanation
start_number	Numbers can be generated automatically. This instruction defines the start value.
no_of_number	If “start_number” is given, this instruction defines the maximum of numbers which are generated.
ac (authentication code)	If set to “number”, “ac” will be equal to number.

additional_pin	If a value is advised, it will be taken as a start number which will be increased for each new record.
sip_user	
sip_pw	
sos_number	If these instructions are set, the value will be taken as default value for the empty corresponding field within the data sequence section records. SOS/Mandown denote the user specific numbers. The Locatable, Localization, and Tracking flags are ignored by Web import.
mandown_number	
locatable	
localization	
tracking	

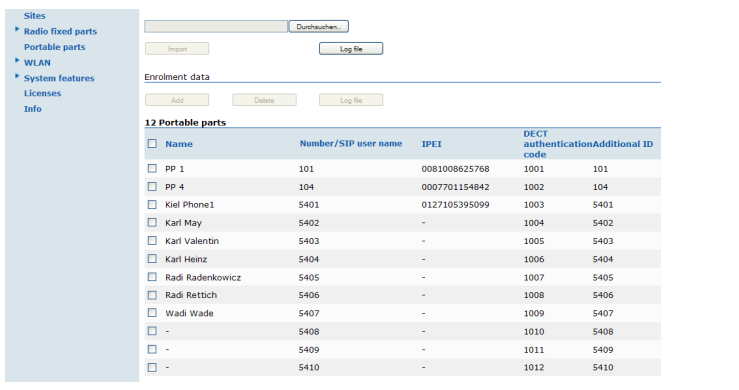
13.2.2 DATA SECTION FIELDS

The data section contains the following field order:

1 Number
2 Name
3 AC
4 IPEI
5 Additional ID
6 Sip user name
7 Sip password
8 SOS number
9 Mandown number
10 Locatable (ignored by Web import and always set to “inactive”)
11 Localization (ignored by Web import and always set to “inactive”)
12 Tracking (ignored by Web import and always set to “inactive”)
13 Description1 (ignored by Web import and always set to “”)
14 Description2 (ignored by Web import and always set to “”)

13.2.3 EXAMPLE

The following screen shot shows a DECT phone configuration. This corresponds to the given configuration file.



Name	Number/SIP user name	IPEI	DECT authentication code	Additional ID
PP 1	101	0081008625768	1001	101
PP 4	104	0007701154842	1002	104
Kiel Phone1	5401	0127105395099	1003	5401
Karl May	5402	-	1004	5402
Karl Valentin	5403	-	1005	5403
Karl Heinz	5404	-	1006	5404
Radi Radenkowicz	5405	-	1007	5405
Radi Rettich	5406	-	1008	5406
Wadi Wade	5407	-	1009	5407
-	5408	-	1010	5408
-	5409	-	1011	5409
-	5410	-	1012	5410

DECT phone configuration file:

```
# ----------------------#
# instruction section:
# ----------------------#
# -- start_number    = {<start value for numbers to be generated>}
# -- no_of_number    = {<maximum of generated numbers>}
# -- ac   = {<""number""">, <start value for ac's to be generated>}
# -- additional_pin = {<""number""">, <start value for id's >}
# -- sip_user       = {<""number""">, <start value for id's >}
# -- SIP password    = {<""number""">, <start value for id's >}
# -- SOS number      = {<common default>)
# -- Mandown number
# -- Locatable (ignored by Web import and always set to inactive)
# -- Localization (ignored by Web import and always set to inactive)
# -- Tracking (ignored by Web import and always set to inactive)

start_number = 5401
no_of_number = 10
ac  = 1001
additional_pin = number
sip_user = number
sip_pw = number
```



```
sos_number=5002
mandown_number=5002

# ---------------------#
# data sequence:
# ---------------------#
# 1. number
# 2. name
# 3. AC
# 4. IPEI
# 5. additionalId
# 6. SIP user
# 7. SIP password
# 8. sos no
# 9. mandown no
# 10. locatable (ignored by Web import and always set to inactive)
# 11. localization (ignored by Web import and always set to inactive)
# 12. tracking (ignored by Web import and always set to inactive)
# 13. descr1 (ignored by Web import and always set to "")
# 14. descr2 (ignored by Web import and always set to "")
data_sequence;;;;;;;;;;;;
# 1. number;2. name;3. AC;4. IPEI ;5. additionalId;6. SIP user;7. SIP password;8. sos
no;9. mandown no;10. locatable;11. localization;12. tracking;13. descr1;14. descr2
101;DECT phone 1;;0081008625768;;;;;;;;;
104;DECT phone 4;;0007701154842;;;;;;;;;
;Kiel Phone1;;0127105395099;5401;5401;5401;30;30;;;;;
;Karl May;;;;;;;;;;;
;Karl Valentin;;;;;;;;;;;
;Karl Heinz;;;;;;;;;;;
;Radi Radenkowicz;;;;;;;;;;;;
;Radi Rettich;;;;;;;;;;;
;Wadi Wade;;;;;;;;;;;
```

Parse log about import / instruction processing

```
OK: start_number = 5401
OK: ac = 1001
OK: additional_pin = number
OK: sip_user = number
OK: sip_pw = number
OK: sos_number = 5002
OK: mandown_number = 5002

OK: no_of_number = 10
```

```
Section processing:

[...]
```


13.3 RFP CONFIGURATION FILE / CENTRAL (OMM DATABASE)

You can import of DECT base station configurations using files via the OMP.

13.3.1.1 Supported Instructions

All instructions are taken as a common value and are applied to all records in the data sequence section of that file if the corresponding field is empty.

Instruction	Explanation
active	Activation of DECT: {‘0’ or ‘false ’= inactive, ‘1’ or ‘true’ = active }
cluster	Cluster, the RFP is referred to - RFP-OMM: {1..256}, PC-OMM: {1..4096}
paging_area	Paging area, the RFP is referred to: {‘unassigned, ’0’..’127’} Ignored by WEB import and always set to ‘0’ (Paging area 0)
sync_source	Synchronization source: {‘0’ or ‘false ’= inactive, ‘1’ or ‘true’ = active }
refl_env	Reflective environment: {‘0’ or ‘false ’= no, ‘1’ or ‘true’ = yes }
site	Site Id: {1..250}
wlan_profile	Reference key to an existing WLAN profile
wlan_antenna	Antenna settings: {0=diversity, 1, 2}
wlan_channel_bg	WLAN channel: {0..14 (size depends on regulatory domain) }
wlan_power	WLAN power: {6, 12, 25, 50,100 (in percent)}
wlan_act	Activation of WLAN: {‘0’ or ‘false ’= inactive, ‘1’ or ‘true’ = active }

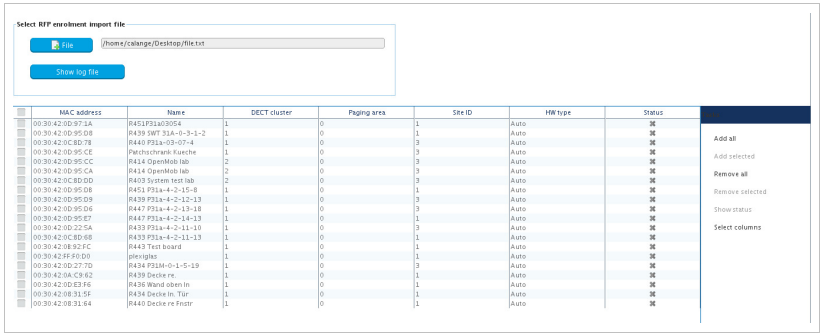
13.3.1.2 Data Section Fields

The data section contains the following field order:

1 MAC address
2 Name
3 DECT activated
4 DECT cluster
5 Paging area (always set to “0”, PA0)
6 Preferred sync.
7 Reflective env.
8 Site ID (if left empty then set to the lowest Site ID)
9 Building (ignored by Web import and always set to “”)
10 Floor (ignored by Web import and always set to “”)
11 Room (ignored by Web import and always set to “”)
12 WLAN profile
13 WLAN antenna
14 WLAN channel
15 WLAN power
16 WLAN activated

13.3.1.3 Example

The following figure shows the results of a DECT base station enrolment operation via the OMP **DECT base stations** -> **Enrolment** page.



RFP configuration file/central:

```
##############################################################################
# instruction section:
##############################################################################
#active
#               Activation of DECT:
#               {'0' or 'false '= inactive, '1' or 'true' = active}
#cluster
#               Cluster, the RFP is referred to:
#               {1..256} (RFP OMM) or {1..4096} (PC OMM)
#paging_area
#               Ignored by Web import and always set to "0" (PA0)
#               Paging area, the RFP is referred to: {'unassigned, '0'..'127'}
#sync_source
#               Synchronisation source:
#               '0' or 'false '= inactive, '1' or 'true' = active}
#refl_env
#               Reflective environment:
#               '0' or 'false '= no, '1' or 'true' = yes}
#site
#               Site Id: {1..250}
#wlan_profile
#               Reference key to an existing WLAN profile
#wlan_antenna
```



```
#               Antenna settings: {0=diversity, 1, 2}
#wlan_channel_bg
#               WLAN channel: {0..14 (size depends on regulatory domain) }
#wlan_power
#               WLAN power = { 6, 12, 25, 50,100 (in percent)}
#wlan_act
#               Activation of  WLAN:
#               '0' or 'false '= inactive, '1' or 'true' = active}
#Note: Web import allows only "0" or "1" for Boolean
##############################################################################

active=1
cluster=100
refl_evc=1
site=1

##############################################################################
data_sequence
##############################################################################
#MAC address;Name;DECT activated;DECT cluster;Paging area;Preferred sync.;
#Reflective env.;Site ID;Building;Floor;Room;WLAN profile;WLAN antenna;
#WLAN channel;WLAN power;WLAN activated
00:30:42:0D:97:1A;R451P31a03054;1;1;0;0;0;1;31;4;;;;;;
00:30:42:0D:95:D8;R439 SWT 31A-0-3-1-2;1;1;0;1;0;1;31;4;;;;;;
00:30:42:0C:BD:7B;R440 P31a-03-07-4;1;1;0;0;0;3;31;4
00:30:42:0D:95:CE;Patchschrank Kueche;1;1;0;0;0;3;31;4
00:30:42:0D:95:CC;R414 OpenMob lab;1;2;0;0;0;3;;
00:30:42:0D:95:CA;R414 OpenMob lab;1;2;0;0;0;3;31;4
00:30:42:0C:BD:DD;R403 System test lab;1;2;0;0;0;3;31;4
00:30:42:0D:95:DB;R451 P31a-4-2-15-8;1;1;0;0;0;1;31;4
00:30:42:0D:95:D9;R439 P31a-4-2-12-13;1;1;0;0;0;3;31;4
00:30:42:0D:95:D6;R447 P31a-4-2-13-18;1;1;0;0;0;3;31;4
00:30:42:0D:95:E7;R447 P31a-4-2-14-13;1;1;0;0;0;1;31;4
00:30:42:0D:22:5A;R433 P31a-4-2-11-10;1;1;0;0;0;3;31;4
00:30:42:0C:BD:68;R433 P31a-4-2-11-13;1;1;0;0;0;1;31;4
00:30:42:0B:92:FC;R443 Test board;1;1;0;0;0;1;31;4
00:30:42:FF:F0:D0;plexiglas;1;1;0;0;0;1;;
00:30:42:0D:27:7D;R434 P31M-0-1-5-19;1;1;0;0;0;3;31;4
00:30:42:0A:C9:62;R439 Decke re.;1;1;0;0;0;1;;
00:30:42:0D:E3:F6;R436 Wand oben ln;1;1;0;0;0;1;;
00:30:42:08:31:5F;R434 Decke ln. Tür;1;1;0;0;0;1
00:30:42:08:31:64;R440  Decke re Fnstr;1;1;0;0;0;1
```