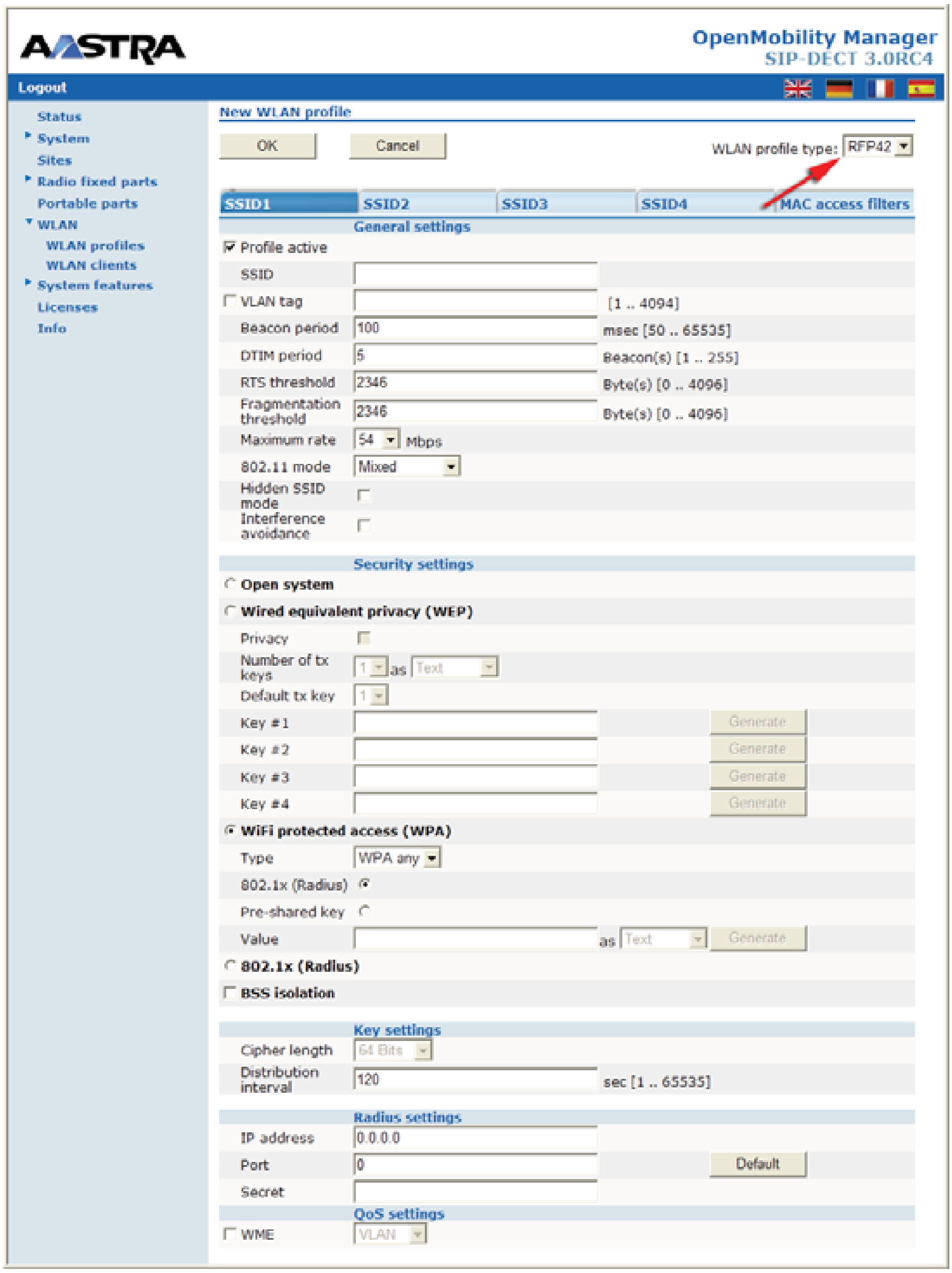


New WLAN profile

WLAN profile type: RFP42

General settings

☑ Profile active		
SSID		
□ VLAN tag		[1 .. 4094]
Beacon period	100	msec [50 .. 65535]
DTIM period	5	Beacon(s) [1 .. 255]
RTS threshold	2346	Byte(s) [0 .. 4096]
Fragmentation threshold	2346	Byte(s) [0 .. 4096]
Maximum rate	54	Mbps
802.11 mode	Mixed	
Hidden SSID mode	□	
Interference avoidance	□	

Security settings

○ Open system		
○ Wired equivalent privacy (WEP)		
Privacy	□	
Number of tx keys	1 as Text	
Default tx key	1	
Key #1		Generate
Key #2		Generate
Key #3		Generate
Key #4		Generate
● WiFi protected access (WPA)		
Type	WPA any	
802.1x (Radius)	●	
Pre-shared key	○	
Value	as Text	Generate
○ 802.1x (Radius)		
□ BSS isolation		

Key settings

Cipher length	64 Bits	
Distribution interval	120	sec [1 .. 65535]

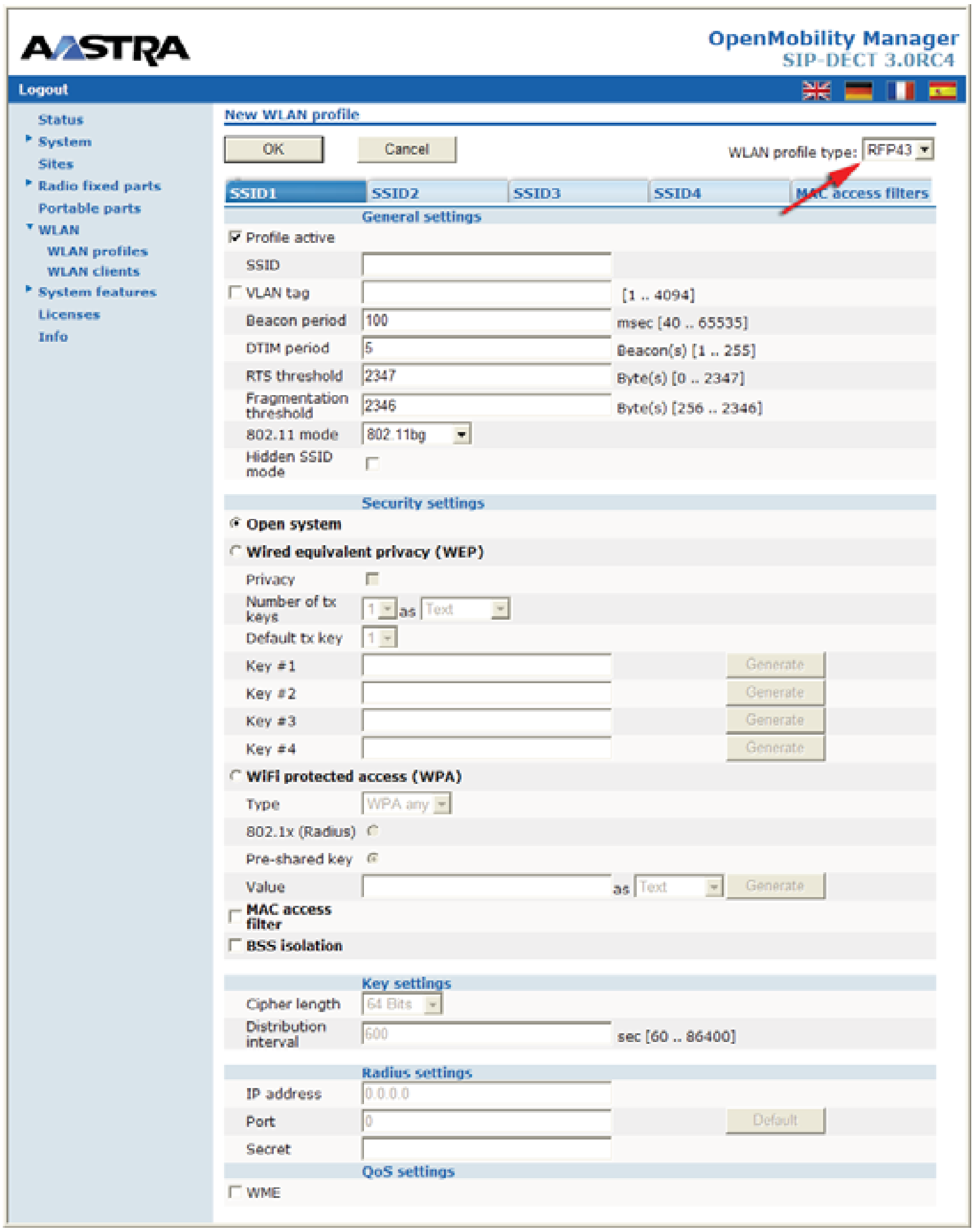
Radius settings

IP address	0.0.0.0	
Port	0	Default
Secret		

QoS settings

□ WME	VLAN

RFP 42 WLAN profile configuration



New WLAN profile

WLAN profile type: RFP43

General settings

☑ Profile active

SSID

☐ VLAN tag [1 .. 4094]

Beacon period 100 msec [40 .. 65535]

DTIM period 5 Beacon(s) [1 .. 255]

RTS threshold 2347 Byte(s) [0 .. 2347]

Fragmentation threshold 2346 Byte(s) [256 .. 2346]

802.11 mode 802.11bg

Hidden SSID mode ☐

Security settings

● Open system

○ Wired equivalent privacy (WEP)

Privacy ☐

Number of tx keys 1 as Text

Default tx key 1

Key #1 Generate

Key #2 Generate

Key #3 Generate

Key #4 Generate

○ WiFi protected access (WPA)

Type WPA any

802.1x (Radius) ○

Pre-shared key ●

Value as Text Generate

☐ MAC access filter

☐ BSS isolation

Key settings

Cipher length 64 Bits

Distribution interval 600 sec [60 .. 86400]

Radius settings

IP address 0.0.0.0

Port 0 Default

Secret

QoS settings

☐ WME

RFP 43 WLAN profile configuration

4 Change the desired settings of the WLAN profile. You need at last to define the ESSID setting. The different settings are explained in detail in the sections below.

5 Activate the **Profile active** setting, otherwise the WLAN profile is inactive which de-activates the WLAN function for RFPs that are assigned to this WLAN profile.

6 Press the **OK** button to apply the settings. If you created a new WLAN profile, you can proceed by assigning the WLAN profile to the desired RFPs (see chapter 7.6.3). If you changed an existing WLAN profile, the settings are applied to the assigned RFPs automatically.

The following description details the different parameters that are available on the **New WLAN profile** page resp. on the **WLAN profile [Number]** page.

General settings

- **Profile active**: Activate this checkbox to activate the profile. This in turn activates the WLAN function for all RFPs that are assigned to the WLAN profile.
- **SSID**: Enter a descriptive character string to identify the WLAN network (e.g. "OurCompany").The service set identifier is broadcasted by the RFP within "WLAN beacons" in a regularly interval. The SSID identifies the WLAN network and is visible by all WLAN clients. This is typically used with a scan function, e.g. from a WLAN client that tries to establish a connection. The SSID should not exceed 32 characters and it is advisable not to use unusual characters that may trigger WLAN client software bugs.
- **VLAN tag** (number, 1..4094, default: off): You can separate VoIP and client data traffic (transferred via WLAN) by using different virtual LANs, e.g. to prevent bulk data transfers to interfere with VoIP. To use a separate VLAN for the client data traffic, activate the check box and enter the desired VLAN number (see chapters 9.15 and 9.10).
- **Beacon period** (milliseconds, 50..65535, default: 100 ms): Determines the WLAN beacon interval. A higher value can save some WLAN airtime that can be used for data transfers.
- **DTIM period** (number, 1..255, default: 5): Determines the number of beacons between DTIM messages. These messages manage the WLAN wakeup/sleep function e.g. that is critical for battery powered WLAN clients.
- **RTS threshold** (bytes, 0..4096, default: 2346): If a WLAN packet exceeds this threshold, it will be transferred with RTS/CTS handshake. This may improve transfer reliability if several WLANs share the same channel. The default of 2346 byte switches off this function because the IP-MTU is typically only 1500 byte.
- **Fragmentation threshold** (bytes, 0..4096, default: 2346): If a WLAN packet exceeds this threshold, it will be transferred in chunks. This may improve transfer reliability for a weak connection. The default of 2346 bytes switches off this function because the IP-MTU is typically only 1500 byte.
- **Maximum rate** (list of rates in Mbps, 1..54, default: 54): Determines the maximum transfer rate used by the RFP. You can limit the rate to increase the WLAN range, e.g. to prevent WLAN clients in the vicinity of the RFP to disturb distant WLAN clients.
- **802.11 mode** (RFP 42 (L) WLAN selection list: Mixed / 802.11b-only / 802.11g-only, default: Mixed): Both the older and long-ranged B-Mode and the newer and faster G-Mode are typically supported by WLAN clients. You can change this setting to prevent problems with very old WLAN clients.
(RFP 43 (L) WLAN selection list: 802.11bg /802.11b-only / 802.11g-only / 802.11abg /802.11n, default: 802.11bg): On the new RFP43 profiles you can choose additional 802.11 modes 802.11abg and 802.11n.

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

- **Hidden SSID mode** (on / off, default: off): If switched on, the transmission of the SSID within beacons is suppressed. This in turn requires a more elaborate and manual connection procedure for WLAN clients.

- **Interference avoidance** (on / off, default: off): Enables a WLAN procedure to enhance radio interference avoidance. This setting applies to RFP (L)42 WLAN only.

Security settings

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

- **Open system**: Enable this option to deactivate authentication and encryption ("Hotel mode"). Note, that all data is transferred un-encrypted in this mode, which can be easily eavesdropped with any WLAN equipment.
- **Wired equivalent privacy (WEP)**: Enable this option to use the older WEP encryption mode. This mode may be useful, e.g. if your WLAN should support older WLAN clients that do not implement the recommended WPA encryption.
  - **Privacy** (on / off, default: off): De-activate this setting to use no authentication ("Open System") with standard WEP encryption. Activate this setting to use an additional shared key authentication between the RFP and the WLAN client.
  - **Number of tx keys** (number, 1..4, default: 1): The WEP encryption can use a single shared key or multiple shared keys ("key rotation"). Select the number of shared keys, select how to enter a shared key (by default as **Text** or as **Hex value**), and select the **Cipher length** (see **Key settings** below).
  - **Default tx key** (number, 1..4, default: 1): If more than one shared keys is used, you can select the default shared key. You need to configure the same default key on the WLAN client.
  - **Key #1** – **Key #4**: Enter one or more shared key. The **Cipher length** setting (see **Key settings** below) determines the length of the required input. If you selected to enter as **Text** (see above), input a password with 5, 13, or 29 characters that matches a 64, 128, or 256 bit cipher. If you selected to enter as **Hex value**, you can input a hexadecimal number with 10, 26, or 58 characters (0-9, a-f). Press the **Generate** button to generate a random shared key that matches the current settings.
- **WiFi protected access (WPA)**: Enable this option to use the recommended WPA encryption mode.
  - **Type** (selection, WPA any / WPA v.1 / WPA v.2, default: WPA any): Select the WPA version required for WLAN clients. The **WPA any** setting allows WPA v.1 and WPA v.2 to be used concurrently. The **WPA v.1** setting enforces the use of the older RC4-based encryption. The **WPA v.2** setting enforce the use of the stronger AES encryption. You can also change the distribution interval (see **Key settings** below).
  - **802.1x (Radius)**: Select this option if your WLAN should use a RADIUS server for WLAN client authentication ("Enterprise WPA" with different username/password combinations per client). You also need to specify the **Radius settings** (see below). For details about the RADIUS authentication procedure, using the public keys, and importing certificates to the WLAN clients refer to the documentation of your RADIUS server product.
  - **Pre-shared key**: Select this option to use a single shared key for all WLAN clients (**Value** setting below). A WLAN client user needs to enter the shared key in order to connect.

  - **Value**: You can enter a shared key as **Text**. Use a longer text sequence with alphanumeric characters and special characters to enhance the shared key strength. A text shared key is case sensitive. Alternatively, the shared key can be entered as **Hex value** (hexadecimal number, 0-9, a-f). Press the **Generate** button to generate a random shared key that matches the current settings.

- **802.1x (Radius)**: This setting applies to RFP (L)42 WLAN only. Enable this option to use the RADIUS authentication without the stronger WPA encryption. You also need to specify the **Radius settings** and you may adapt the **Key settings** (see below).
- **MAC access filters** (on / off, default: off): This setting applies to RFP (L)43 WLAN only. You can limit WLAN access for WLAN clients with specified MAC addresses. Note, that without encryption this should not be used for security reasons. You can configure a list of MAC addresses that are allowed to connect via the **MAC access filters** tab on the WLAN profile page.
- **BSS isolation** (on / off, default: off): In a standard WLAN setup, each WLAN client can contact other WLAN clients. For special purposes (e.g. “Internet café setup”), you may switch on this options to protect WLAN clients from eavesdropping on other WLAN clients.

Key settings

- **Cipher length** (selection, 64 Bits / 128 Bits / 256 Bits, default: 64 Bits): Determines the key length used for the WEP encryption. Larger bit sequences provide better security but may be unsupported by very old WLAN clients.
- **Distribution interval** (seconds, 1..65535, default: 20): Determines how often the WEP encryption is re-negotiated.

Radius settings

The parameters in this section can only be configured if the **802.1x (Radius)** option has been selected.

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

QoS settings

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

SSID2 – SSID4 Tabs

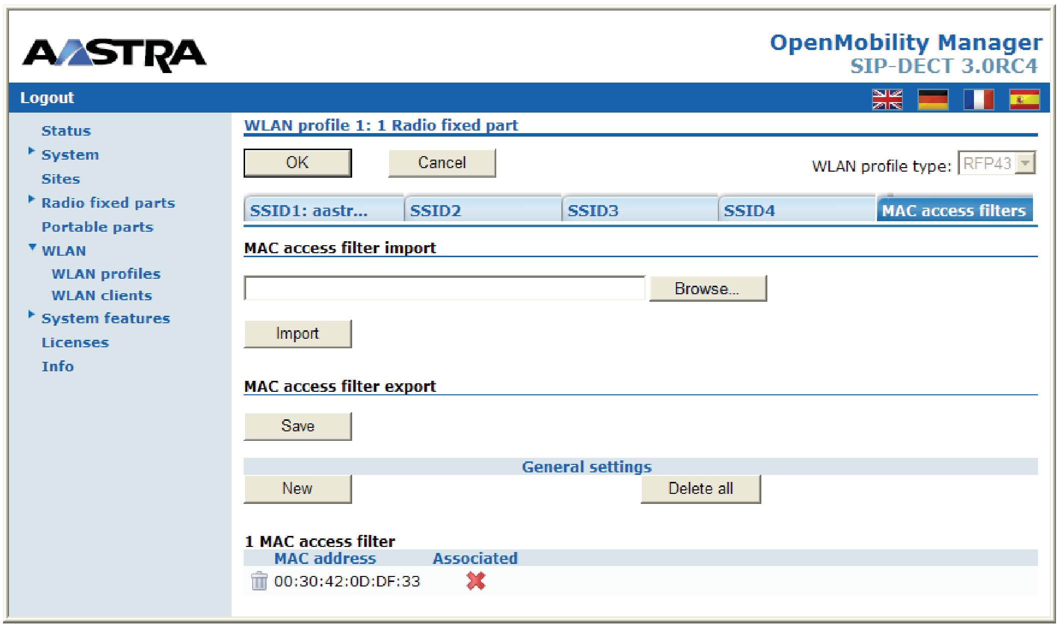
You can enable up to three additional virtual WLAN networks that are managed by their SSID. This can be used for example to provide WLAN access for guests that is separated from the company WLAN by means of VLAN tags and encryption settings. To activate this feature proceed as follows:

1. Switch to the appropriate **SSID** tab, e.g. SSID2. Activate the **Active** check box to enable the additional virtual WLAN. The tab provides separate configuration items for the selected SSID.
2. Enter at least a new **SSID**. Also enter a currently unused **VLAN tag** number.

3 You can specify different authentication/encryption settings for each SSID section. For example, you can use **WPA** / **Pre-shared key** with different passwords.

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

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



WLAN profile 1: 1 Radio fixed part

WLAN profile type: RFP43

MAC access filter import

MAC access filter export

General settings

1 MAC access filter

MAC address	Associated
🗑 00:30:42:0D:DF:33	✖

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

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

7.8.1.2 Deleting WLAN Profiles

To delete an existing WLAN profile:

1 You cannot remove WLAN profile that is in use. To remove a currently used WLAN profile, you need to select another WLAN profile for all assigned RFPs first (see chapter 7.6.3.

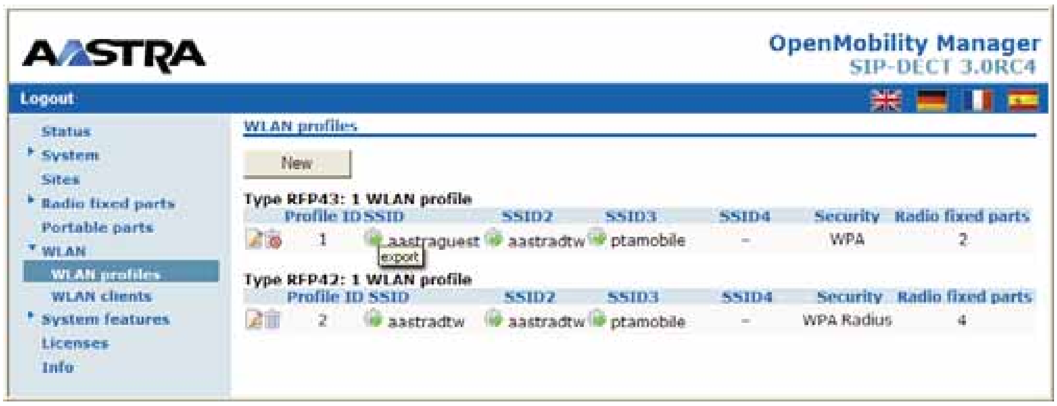
2 On the **WLAN profiles** page click on the 🗑 icon next to the profile entry.

The **Delete WLAN profile?** dialog opens showing a summary of the WLAN profile’s configuration.

3 Press the **Delete** button.

7.8.1.3 Exporting WLAN Profiles

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



Type RFP43: 1 WLAN profile

	Profile ID	SSID	SSID2	SSID3	SSID4	Security	Radio fixed parts
	1	aastraguest	aastradtw	ptamobile	-	WPA	2

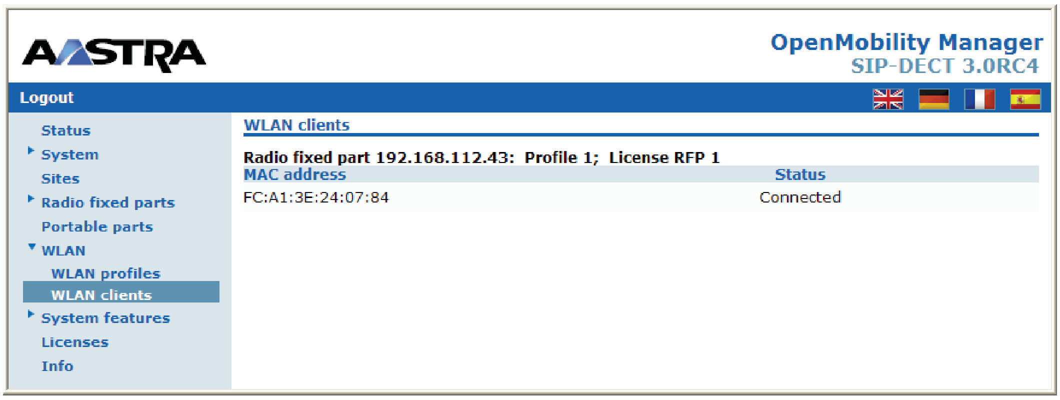
Type RFP42: 1 WLAN profile

	Profile ID	SSID	SSID2	SSID3	SSID4	Security	Radio fixed parts
	2	aastradtw	aastradtw	ptamobile	-	WPA Radius	4

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

7.8.2 “WLAN clients” Menu

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



Radio fixed part 192.168.112.43: Profile 1; License RFP 1

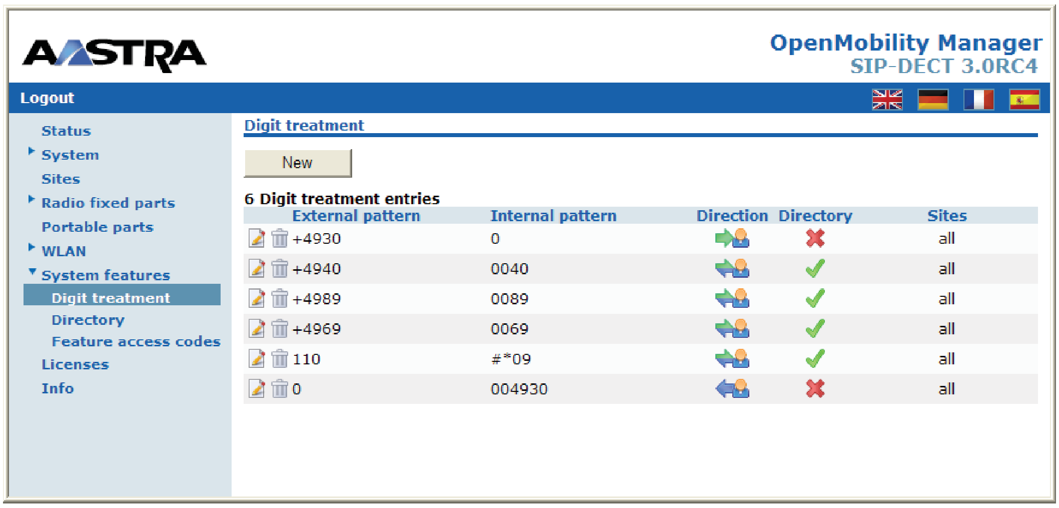
MAC address	Status
FC:A1:3E:24:07:84	Connected

7.9 “System features” Menu

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

7.9.1 “Digit treatment” Menu

A number manipulation is provided by the digit treatment feature for LDAP corporate directories, that handles both incoming and outgoing calls (see chapter 7.9.2).



6 Digit treatment entries

External pattern	Internal pattern	Direction	Directory	Sites
+4930	0	→	✗	all
+4940	0040	⇄	✓	all
+4989	0089	⇄	✓	all
+4969	0069	⇄	✓	all
110	#*09	⇄	✓	all
0	004930	←	✗	all

LDAP

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

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

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

Incoming Call

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

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

Outgoing Call

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

[1] For Incoming Call/Calling Party Number; Depending on the capabilities of the handset and the level of integration.

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

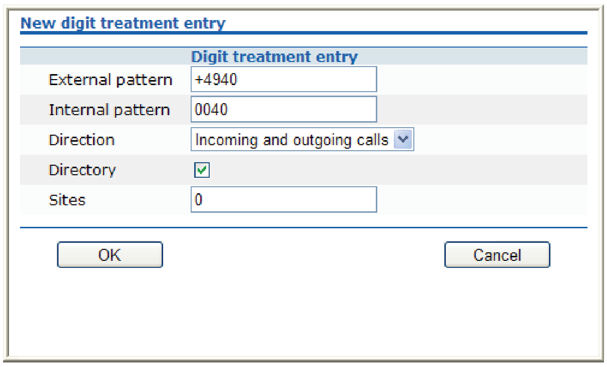
The result of the conversion is not sent to the handset to be displayed or entered in the call log[1].

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

- creating and changing “Digit treatment” entries (see chapter 7.9.1.1),
- deleting “Digit treatment” entries(see chapter 7.9.1.2).

7.9.1.1 Creating and Changing “Digit treatment” Entries

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



New digit treatment entry

Digit treatment entry

External pattern	+4940
Internal pattern	0040
Direction	Incoming and outgoing calls
Directory	☑
Sites	0

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

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

Please note: The plus character (“+”) can not be dialled from a handset and can not be transferred to a call log.

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

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

5 **Directory**: Activate this option if the rule applies to LDAP directories (see chapter 7.9.2).

[1] For Outgoing Call/Called Number; If the user would dial the number from the redial list again the same procedure will be applied as for the initial dialling.

6 **Sites**: Specifies the sites for which a rule shall be applied e.g. “1,2” (see chapter 7.5). If set to “0” the rule applies to all sites i.e. the rule will be applied to all calls or corporate directory requests.

7 Press the **OK** button.

7.9.1.2 Deleting “Digit treatment” Entries

To delete an existing entry:

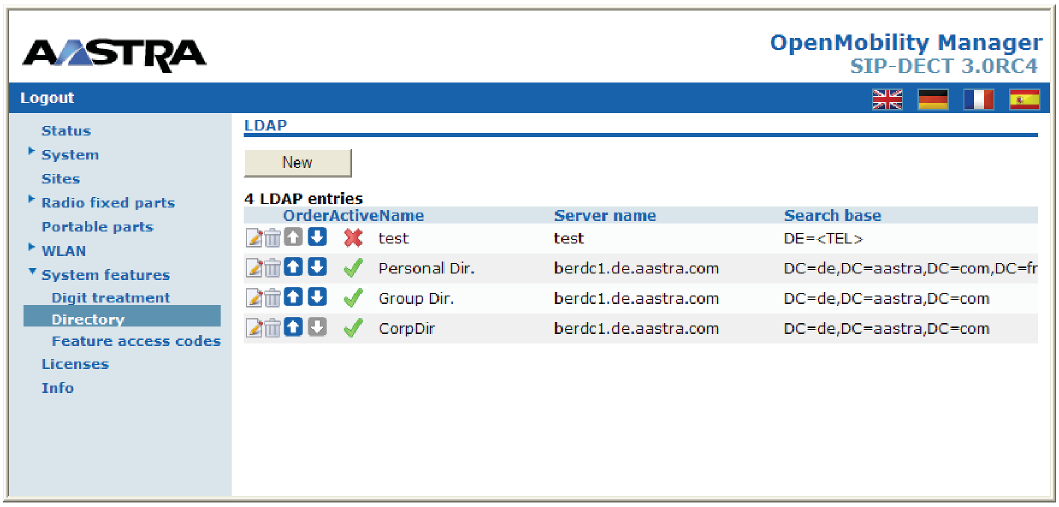
1 On the **Digit treatment** page click on the 🗑 icon left behind the entry.

The **Delete digit treatment entry?** dialog opens showing the current configuration of this entry.

2 Press the **Delete** button.

7.9.2 “Directory” Menu

The **System features** menu allows you to manage connections to one or more LDAP servers that in turn facilitate central corporate directories. The OMM supports multiple LDAP servers with specific parameter settings to support different types of directories e.g. global corporate directory, group specific directory, personal directory.



4 LDAP entries

Order	Active	Name	Server name	Search base
	✗	test	test	DE=<TEL>
	✓	Personal Dir.	berdc1.de.aastra.com	DC=de,DC=aastra,DC=com,DC=fr
	✓	Group Dir.	berdc1.de.aastra.com	DC=de,DC=aastra,DC=com
	✓	CorpDir	berdc1.de.aastra.com	DC=de,DC=aastra,DC=com

If there is more than one LDAP server configured then the multiple options are offered to the user as a list. The list is presented to the user if the central directory is called e.g. via soft key or selecting central directory from the menu. The user can choose one of the entries in the list. The name of an entry shown in the list is configured in the OMM when creating the LDAP server entry. (Latin-1 character set is supported).

- If there is only one LDAP server configured then the directory function is directly started when pressing the soft key or selecting central directory from the menu.
- The name configured in the OMM is not relevant and ignored if there is only one LDAP server configured.
- There are up to 5 LDAP directories configurable.

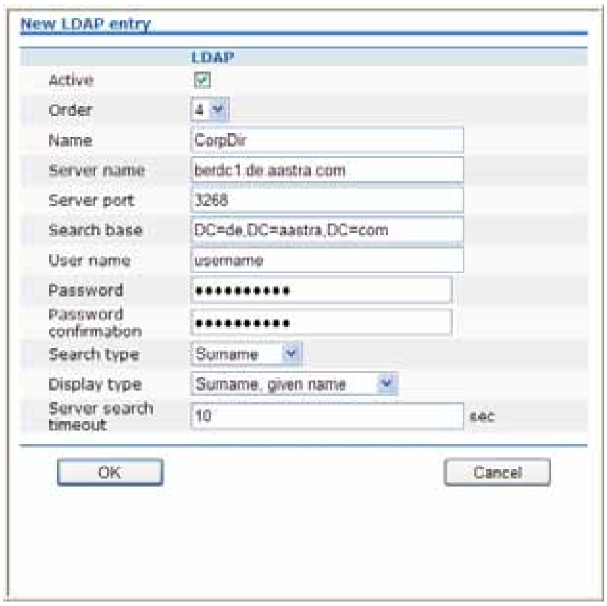
The OMM determines the display order of the directories in the handset menu by the order specified by the administrator.

The following tasks can be performed on the **Directory** page:

- creating and changing LDAP entries (see chapter 7.9.1.1),
- deleting LDAP entries(see chapter 7.9.2.2).

7.9.2.1 Creating and Changing LDAP Servers

1 To configure a new LDAP entry press the **New** button on the **Directory** page.
To change the configuration of an existing entry click on the ✎ icon left behind the entry.
The **New LDAP entry** resp. the **Configure LDAP entry** dialog opens.



New LDAP entry

	LDAP	
Active	☑	
Order	4	
Name	CorpDir	
Server name	berdc1.de.aastra.com	
Server port	3268	
Search base	DC=de,DC=aastra,DC=com	
User name	username	
Password	••••••••••	
Password confirmation	••••••••••	
Search type	Surname	
Display type	Surname, given name	
Server search timeout	10	sec

1 On the **LDAP entry** page enter the parameters for the LDAP access, see parameter description below.

2 Press the **OK** button to create or change an LDAP directory entry.

The following parameters can be set per LDAP directory entry:

- **Active flag**: allows to enable/disable a specific entry.
- **Order**: determines the position in the handset menu (1 – top; 5 – bottom).
- **Server name** (mandatory): Enter the name or IP address of the LDAP server.
- **Server port** (mandatory): Enter the server port number (default: 389)

Note: SSL (default port 689) is not supported.
Windows® Active Directory Server uses port 3268.

- **Search base**: The search base has to be edited (e.g. “ou=people,o=my com”).
- **User name**, **Password**: User name (a distinguished name) and password may be filled, if requested by the LDAP Server. Otherwise an anonymous bind takes place.

Note: The DECT IP OMM supports LDAP simple bind.

- **Search type**: Searches will be done for one of the following attributes:
  – Name (sn) // Surname (default)
  – First name (Given name)

- **Display type**: Selection between the following two alternatives is possible:
  – Surname (sn), first name (given name) (default)
  – first name (Given name) and Surname (sn)
- **Server search timeout**: The search results will be accepted within the entered search time (value range: 1 - 99 sec).

The configuration is valid for all PP handsets which support the LDAP directory feature. To make search requests unique for different users the search base configuration can include space holders which are replaced by user specific values when submitting the LDAP request to a server.

The following placeholders are defined:

- "<TEL>" which is replaced by the specific telephone number of the user,
- "<DESC1>" which is replaced by the "Description 1" attribute value of the user
- "<DESC2>" which is replaced by the "Description 2" attribute value of the user

Note: The telephone number in SIP–DECT is not limited to numeric character.

7.9.2.2 Deleting LDAP Entries

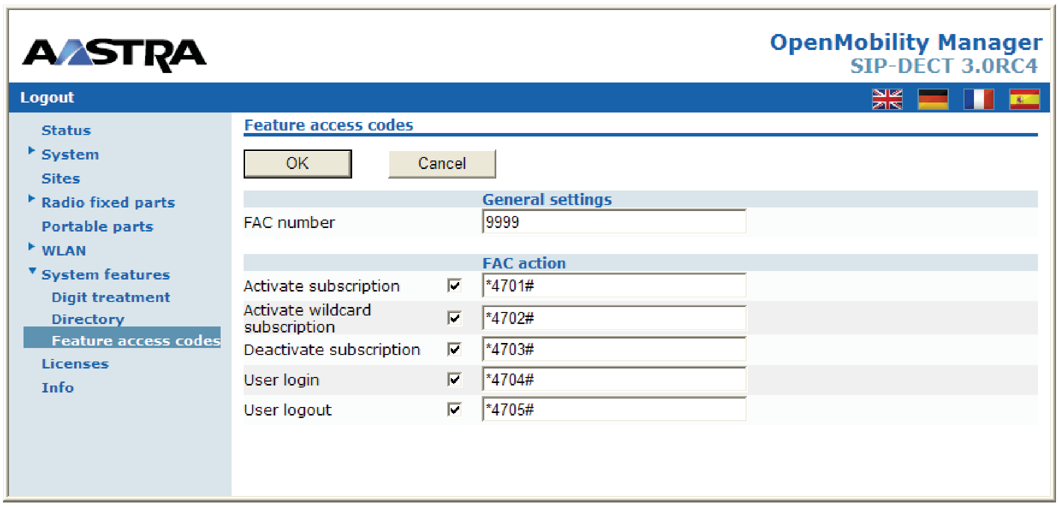
To delete an existing LDAP directory entry:

1 On the **Directory** page click on the 🗑 icon left behind the entry.
The **Delete LDAP entry** dialog opens showing the current configuration of this entry.

2 Press the **Delete** button.

7.9.3 "Feature access codes" Menu

Features access codes (FAC) allow to perform specific actions on the OMM from any subscribed DECT handset.



Feature access codes

General settings

FAC number		9999

FAC action

Activate subscription	☑	*4701#
Activate wildcard subscription	☑	*4702#
Deactivate subscription	☑	*4703#
User login	☑	*4704#
User logout	☑	*4705#

To configure the FAC feature:

1 **FAC number**: Enter a unique FAC number.

2 Activate the appropriate checkbox(es) to enable the corresponding FAC feature(s). For each enabled FAC feature enter an assigned access code.

3 Press the **OK** button.

Afterwards the appropriate action can be performed by dialing the “FAC number” followed by the “FAC access code” en bloc from any subscribed DECT handset.

In the example above a subscribed user can activate the OMM DECT subscription by dialing “9999*4701#” en bloc.

> **Please note:** Overlap sending is not supported for FAC. “FAC number” and “FAC action code” must be entered en bloc.

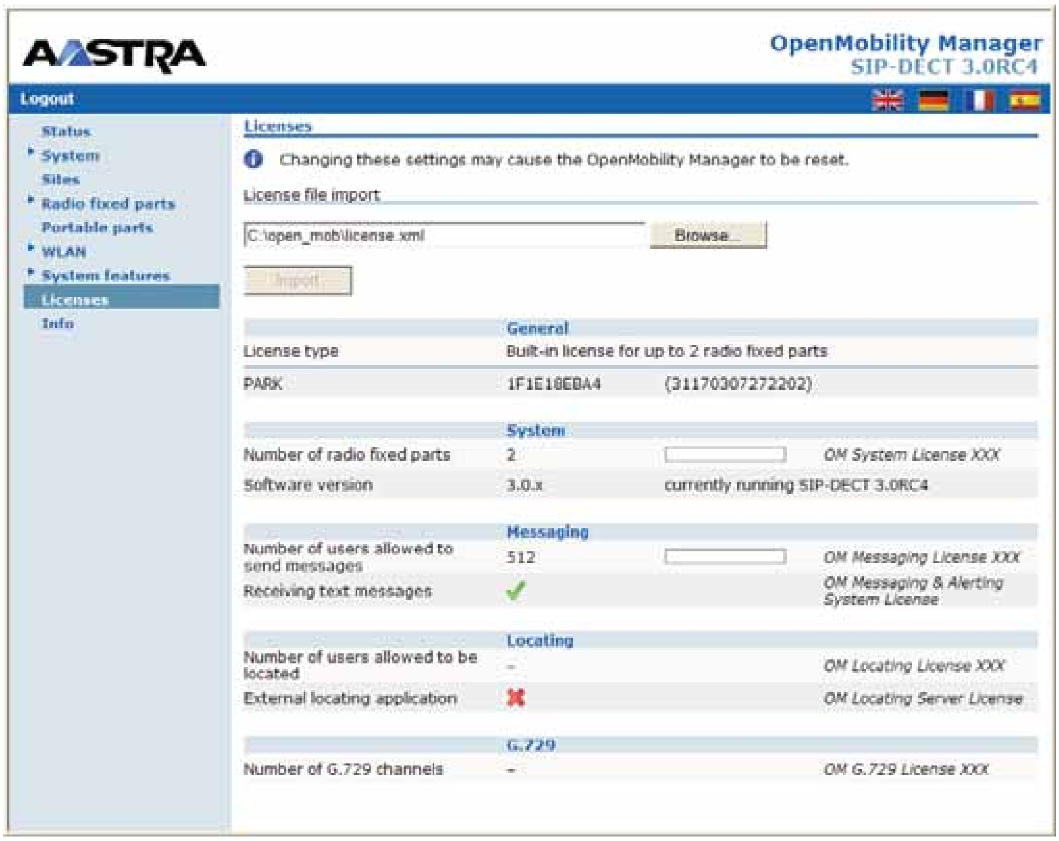
FAC functions will be confirmed by an audible indication to the user (in-band tone signals).

7.10 “Licenses” Menu

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

1 Select the path and file name where the activation or license key is stored.

2 Afterwards press the Import button.



Licenses

Changing these settings may cause the OpenMobility Manager to be reset.

License file import

C:\open_mob\license.xml

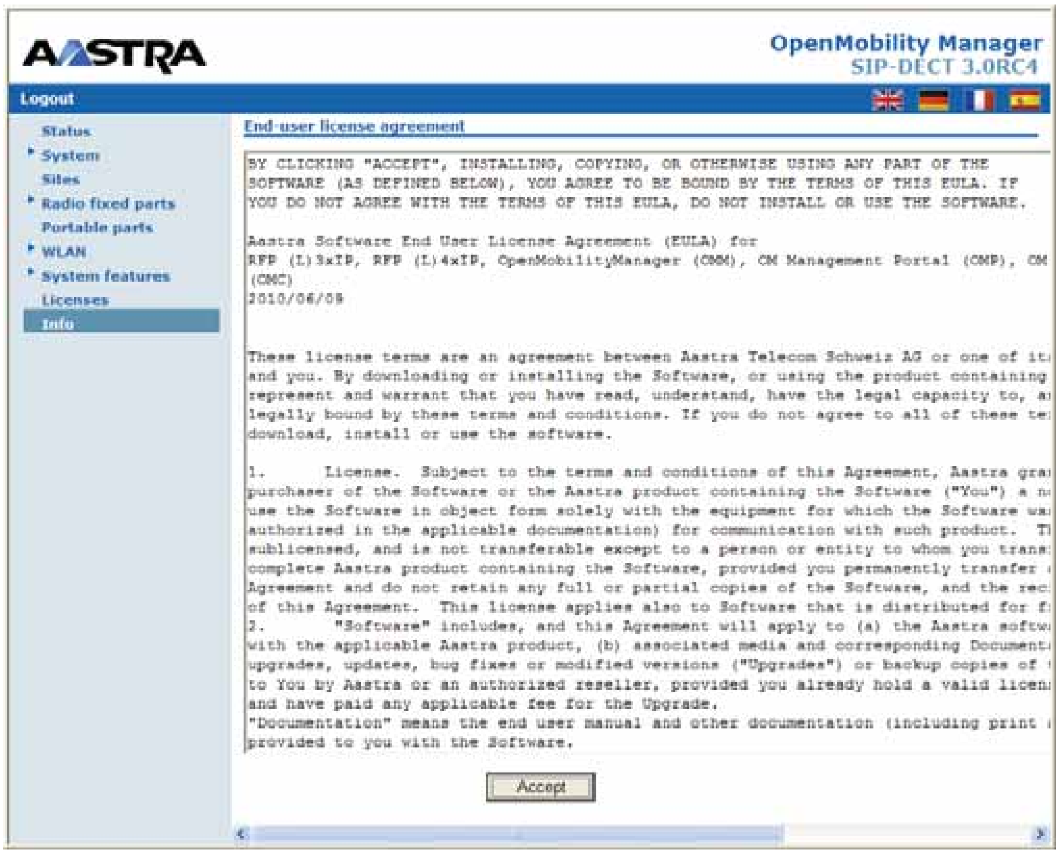
	General		
License type	Built-in license for up to 2 radio fixed parts		
PARK	1F1E18EBA4	(31170307272202)	
	System		
Number of radio fixed parts	2		OM System License XXX
Software version	3.0.x	currently running SIP-DECT 3.0RC4	
	Messaging		
Number of users allowed to send messages	512		OM Messaging License XXX
Receiving text messages	✓		OM Messaging & Alerting System License
	Locating		
Number of users allowed to be located	-		OM Locating License XXX
External locating application	✗		OM Locating Server License
	G.729		
Number of G.729 channels	-		OM G.729 License XXX

For a detailed description on the OMM licensing model see chapter 4.

7.11 “Info” Menu

On the **Info** page, the End User License Agreement (EULA) is displayed.

With the first login into a new SIP–DECT SW version, this page is displayed automatically and the user has to accept the EULA by pressing the **Accept** button.



BY CLICKING "ACCEPT", INSTALLING, COPYING, OR OTHERWISE USING ANY PART OF THE
SOFTWARE (AS DEFINED BELOW), YOU AGREE TO BE BOUND BY THE TERMS OF THIS EULA. IF
YOU DO NOT AGREE WITH THE TERMS OF THIS EULA, DO NOT INSTALL OR USE THE SOFTWARE.

Aastra Software End User License Agreement (EULA) for
RFP (L)3xIP, RFP (L)4xIP, OpenMobilityManager (OMM), OM Management Portal (OMP), OM
(OMC)
2010/06/08

These license terms are an agreement between Aastra Telecom Schweiz AG or one of it
and you. By downloading or installing the Software, or using the product containing
represent and warrant that you have read, understand, have the legal capacity to, a
legally bound by these terms and conditions. If you do not agree to all of these te
download, install or use the software.

1. License. Subject to the terms and conditions of this Agreement, Aastra gra
purchaser of the Software or the Aastra product containing the Software ("You") a n
use the Software in object form solely with the equipment for which the Software wa
authorized in the applicable documentation) for communication with such product. T
sublicensed, and is not transferable except to a person or entity to whom you trans
complete Aastra product containing the Software, provided you permanently transfer
Agreement and do not retain any full or partial copies of the Software, and the rec
of this Agreement. This license applies also to Software that is distributed for f
2. "Software" includes, and this Agreement will apply to (a) the Aastra softw
with the applicable Aastra product, (b) associated media and corresponding Document
upgrades, updates, bug fixes or modified versions ("Upgrades") or backup copies of
to You by Aastra or an authorized reseller, provided you already hold a valid licen
and have paid any applicable fee for the Upgrade.
"Documentation" means the end user manual and other documentation (including print
provided to you with the Software.

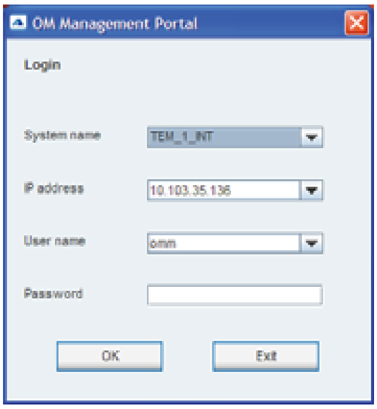
8 OM Management Portal (OMP)

The OM Management Portal (OMP) is a Java tool to manage the SIP–DECT solution. It can be used to view and configure OMM system data in the same way as the OM Web service.

This section lists all parameters which can be configured and viewed using OMP. All parameters which are also accessible by the OM Web service are described in the appropriate OM Web service section (section 7). New parameters which are only accessible via OMP are described in this section.

8.1 Login

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



OM Management Portal

Login

System name: TEM_1_INT

IP address: 10.103.35.136

User name: omm

Password:

To log in to the system enter the following data:

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

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

The **System name** is set by the system administrator after first successful login to the OMM, see chapter 8.5.1.

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

- On a Linux system, preferences are stored in the users home directory “~/.java/.userPrefs/…”.
- On a windows system in the registry node “HKEY_CURRENT_USER/Software/JavaSoft/Prefs/…”.

Note:	The OMM password can not be changed using OMP, please use the OM Web service instead (see chapter 7.4.3).

After login the OMP is set to the configuration mode page showing the system status page which contains health state information of the connected OMM (see chapter 8.4).

8.2 Logout

There is no automatically logout for the OMP. The user has to log out manually.

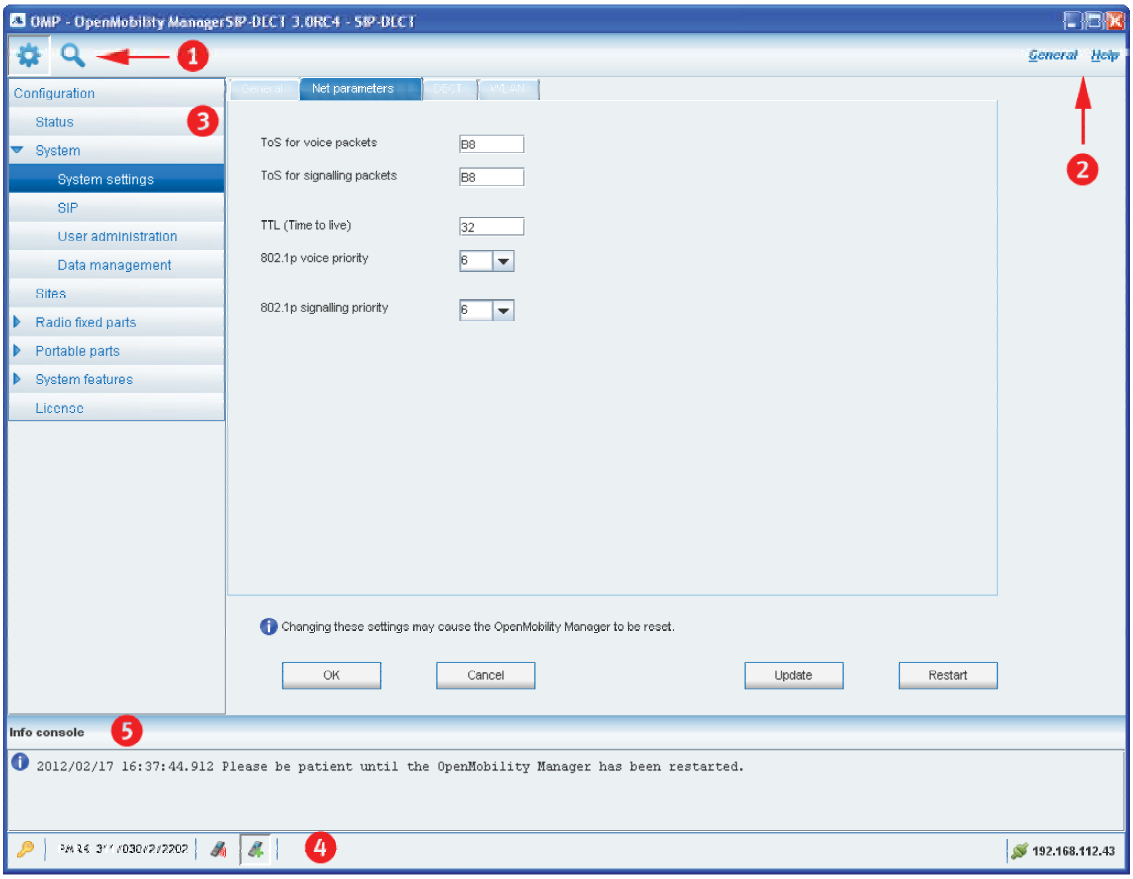
To log out from the system:

- click on the closing icon ☒ on the upper left in the upper right corner of the OMP window
- or select the **Exit** entry from the **General** menu.

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

8.3 OMP Main Window

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



ToS for voice packets: B8

ToS for signalling packets: B8

TTL (Time to live): 32

802.1p voice priority: 6

802.1p signalling priority: 6

Changing these settings may cause the OpenMobility Manager to be reset.

```
2012/02/17 16:37:44.912 Please be patient until the OpenMobility Manager has been restarted.
```

1 – "OMP mode" toolbar buttons

The OMP provides two different modes: the **configuration mode** and the **monitor mode**. The configuration mode allows changing of parameters. In monitor mode parameters are only displayed, they are not changeable. The monitor mode provides additional features, e.g. system and RFP statistics and RFP synchronization monitoring.

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

- ⚙ configuration mode,
- 🔍 monitor mode.

2 – Main menus

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

- **General** menu, see chapter 8.11.
- **Help** menu, see chapter 8.12.

3 – Navigation panel

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

4 – Status bar

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

- Encryption state:

  The 🔑 icon indicates that encryption is enabled.

  The 🔑 icon indicates that encryption is disabled.

  This setting can be configured in the **DECT** tab of the **System settings** menu (see also chapter 8.5.1).
- PARK,
- Subscription state: Clicking on one of the following icons enables / disables subscription.

  The 📱 icon indicates that subscription is enabled.

  The 📱 icon indicates that subscription is disabled.

  Subscription can also be enabled / disabled in the **Portable parts** menu (see also chapter 8.8).
- Auto-create on subscription state: Clicking on one of the following icons enables / disables Auto-create on subscription.

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

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

  This setting can also be configured in the **DECT** tab of the **System settings** menu (see also chapter 8.5.1).
- Connection status to the OMM:

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

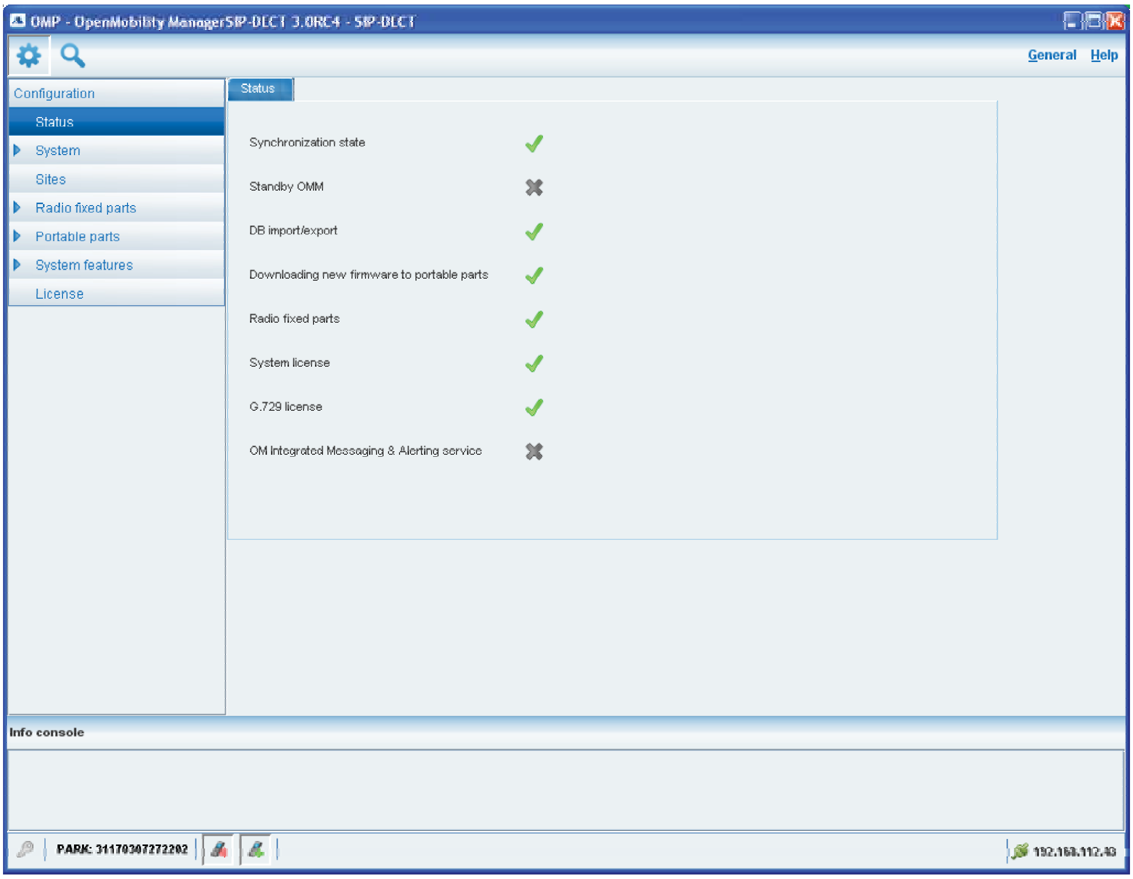
  🔌 OMP is disconnected from the OMM.

5 – Info console

Since SIP–DECT release 3.0, general OMP events are displayed the **Info console**.

8.4 “Status” Menu

The system status is displayed after startup of OMP. The **Status** panel provides information about the system health state.



Synchronization state	✓
Standby OMM	✖
DB import/export	✓
Downloading new firmware to portable parts	✓
Radio fixed parts	✓
System license	✓
G.729 license	✓
OM Integrated Messaging & Alerting service	✖

The following health state items are displayed:

- **Synchronization state**: indicates the current synchronization state for **all** RFPs (see chapter 8.7.5).
- **Standby OMM**: indicates if the status of the standby OMM (see chapter 9.13).
- **DB import/export**: indicates the status of a current database import/export (see chapter 8.5.4).
- **Downloading new firmware to portable parts**: indicates the status of the “Download over Air” service (see chapter 9.17).
- **Radio fixed parts**: indicates the status of **all** RFPs. The status of an individual RFP can be viewed in the RFP detail panel (see chapter 8.7.1.1).
- **System license**: indicates the status of the current system license (see chapter 4).
- **G.729 license**: indicates the status of the G.729 codec license (see chapter 4).
- **OM Integrated Messaging and Alerting service**: indicates the status of the integrated message and alarm server (see chapter 8.5.1).

Health states can be set to these values:

- ✖ – inactive or unknown; no G.729 channels are licensed
- ❌ – error
- ⚠ – warning; all G.729 channels are consumed

- ✓ – OK; G.729 licenses are available

8.5 “System” Menu

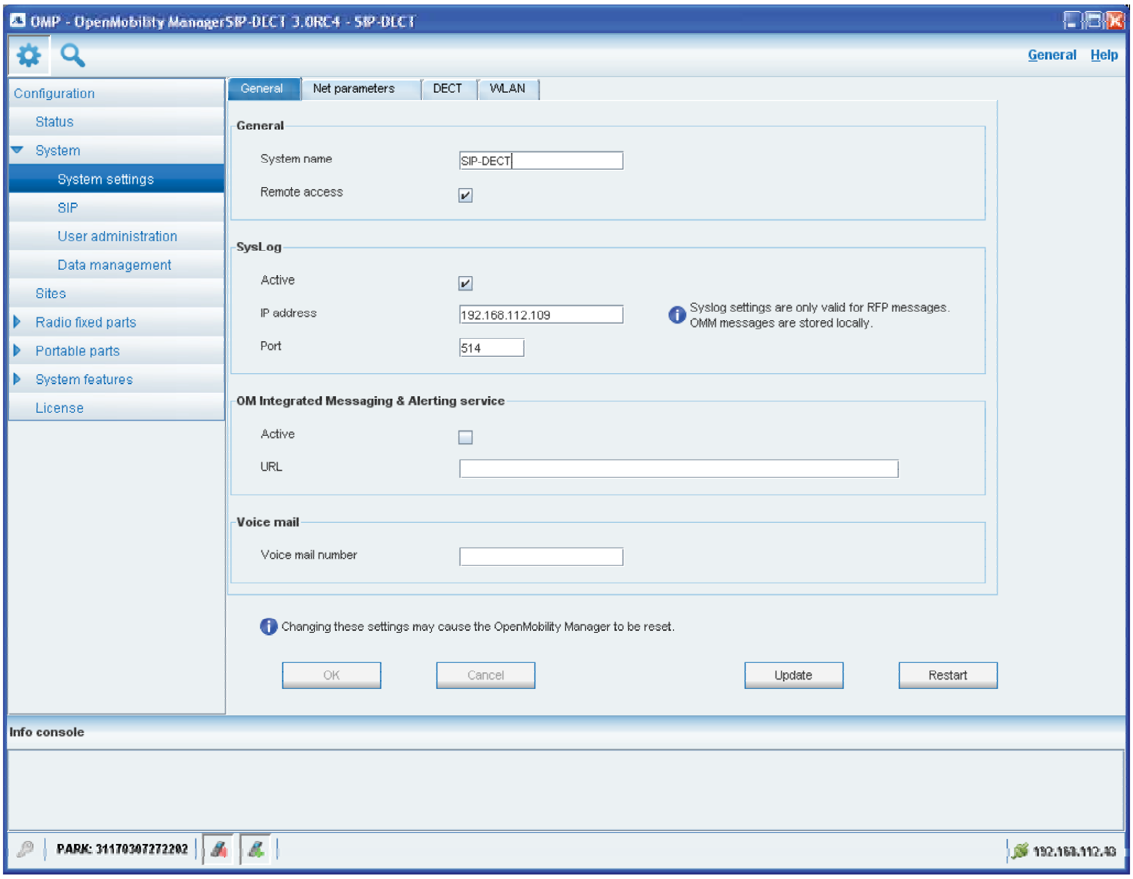
The **System** menu allows to configure/view the global settings of the OMM. The systems settings are changeable in configuration mode. Change of some parameters can cause the OMM to be reset. In this case a new login is required.

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

Configuration mode	Monitor mode	See chapter
System settings	System settings	8.5.1
	Statistics	8.5.2
SIP	SIP	8.5.3
Data management	Data management	8.5.4

8.5.1 “System settings” Menu

The **System settings** menu contains general settings of the OpenMobility Manager.



General

System name: SIP-DECT

Remote access ☑

SysLog

Active ☑

IP address: 192.168.112.109

Port: 514

Syslog settings are only valid for RFP messages. OMM messages are stored locally.

OM Integrated Messaging & Alerting service

Active ☐

URL:

Voice mail

Voice mail number:

Changing these settings may cause the OpenMobility Manager to be reset.

PARK: 31170307272202

192.168.112.43

The menu provides the settings in several tabs:

General

For a description of the parameters which can be set in the **General** tab, please refer to the description of the **System settings** page of the OMM Web service (see chapter 7.4.1). The corresponding parameters can be found there in the **General settings**, **Syslog**, **OM Integrated Messaging and Alerting service** and **Voice mail** page sections.

Net parameters

For a description of the parameters which can be set in the **Net parameters** tab, please refer to the description of the **System settings** page of the OMM Web service (see chapter 7.4.1). The corresponding parameters can be found there in the **IP parameters** page section.

Notes:

- The **802.1p signalling priority** parameter (OMP) corresponds to the **VLAN priority Call control** parameter (OMM Web service).
- The **802.1p voice priority** parameter (OMP) corresponds to the **VLAN priority Audio** parameter (OMM Web service).

DECT

For a description of the parameters which can be set in the **DECT** tab, please refer to the description of the **System settings** page of the OMM Web service (see chapter 7.4.1). The corresponding parameters can be found there in the **DECT settings** and **Downloading new firmware to portable parts** page sections.

The following settings are only available in the OMP.

- **Paging area size**: Select the number of paging areas for the SIP–DECT system. A paging area can consist of up to 16 RFPs. The configuration of the paging areas is done in the **Paging areas** menu of the OMP (see chapter 8.7.2).
- **Auto-create on subscription**: Activate this option if an unbound subscription of portable parts should be allowed. Please see the SIP–DECT; OM Handset Sharing & Provisioning; User Guide /27/ for details.

WLAN

For a description of the parameters which can be set in the **WLAN** tab, please refer to the description of the **System settings** page of the OMM Web service (see chapter 7.4.1). The corresponding parameters can be found there in the **WLAN settings** page section.

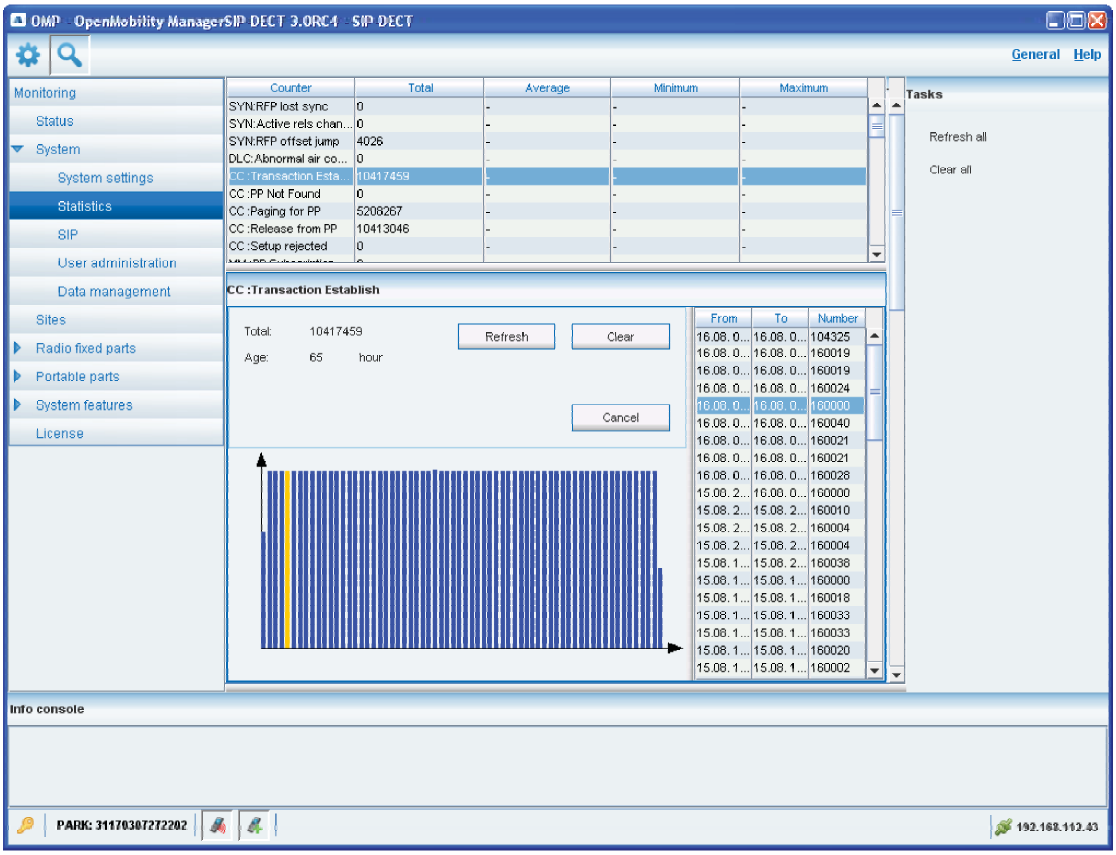
Restarting or Updating the OMM

For a restart of the OMM, press the **Restart** button in the **System settings** menu. For more information see chapter 7.4.1.1.

To update the OMM software, press the **Update** button in the **System settings** menu. For more information see the chapters 7.4.1.2 and chapter 9.12.

8.5.2 “Statistics” Menu

The **Statistics** menu provides system statistics information. It contains a table with numerous system statistics counters which can be used to check the system behavior. The menu is only available in **monitor mode**.



Counter	Total	Average	Minimum	Maximum
SYN:RFP lost sync	0	-	-	-
SYN:Active rels chan...	0	-	-	-
SYN:RFP offset jump	4026	-	-	-
DLC:Abnormal air co...	0	-	-	-
CC :Transaction Esta...	10417459	-	-	-
CC :PP Not Found	0	-	-	-
CC :Paging for PP	5208267	-	-	-
CC :Release from PP	10413046	-	-	-
CC :Setup rejected	0	-	-	-

CC :Transaction Establish

Total: 10417459

Age: 65 hour

From	To	Number
16.08. 0...	16.08. 0...	104325
16.08. 0...	16.08. 0...	160019
16.08. 0...	16.08. 0...	160019
16.08. 0...	16.08. 0...	160024
16.08. 0...	16.08. 0...	160000
16.08. 0...	16.08. 0...	160040
16.08. 0...	16.08. 0...	160021
16.08. 0...	16.08. 0...	160021
16.08. 0...	16.08. 0...	160028
15.08. 2...	16.08. 0...	160000
15.08. 2...	15.08. 2...	160010
15.08. 2...	15.08. 2...	160004
15.08. 2...	15.08. 2...	160004
15.08. 1...	15.08. 2...	160038
15.08. 1...	15.08. 1...	160000
15.08. 1...	15.08. 1...	160018
15.08. 1...	15.08. 1...	160033
15.08. 1...	15.08. 1...	160033
15.08. 1...	15.08. 1...	160020
15.08. 1...	15.08. 1...	160002

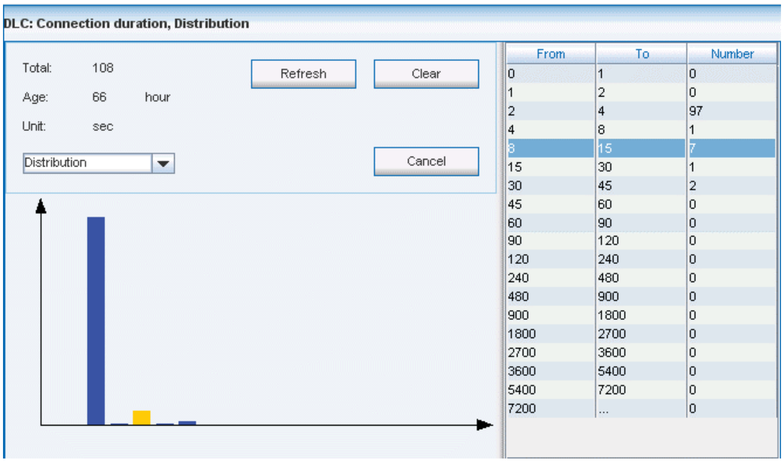
Statistic counters beginning with "+" are counters which are taken over by standby OMM in case of a failover. All other counters will be reset to the defaults in case of a failover. For more details about the standby feature, see section 9.13.

The following tasks can be performed:

- **Refresh all**: request OMM update for all statistics counters.
- **Clear all**: reset all statistics counters in OMM.

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

- update this single statistics counter by pressing the **Refresh** button or
- reset this single statistics counter by pressing the **Clear** button.



DLC: Connection duration, Distribution

Total: 108

Age: 66 hour

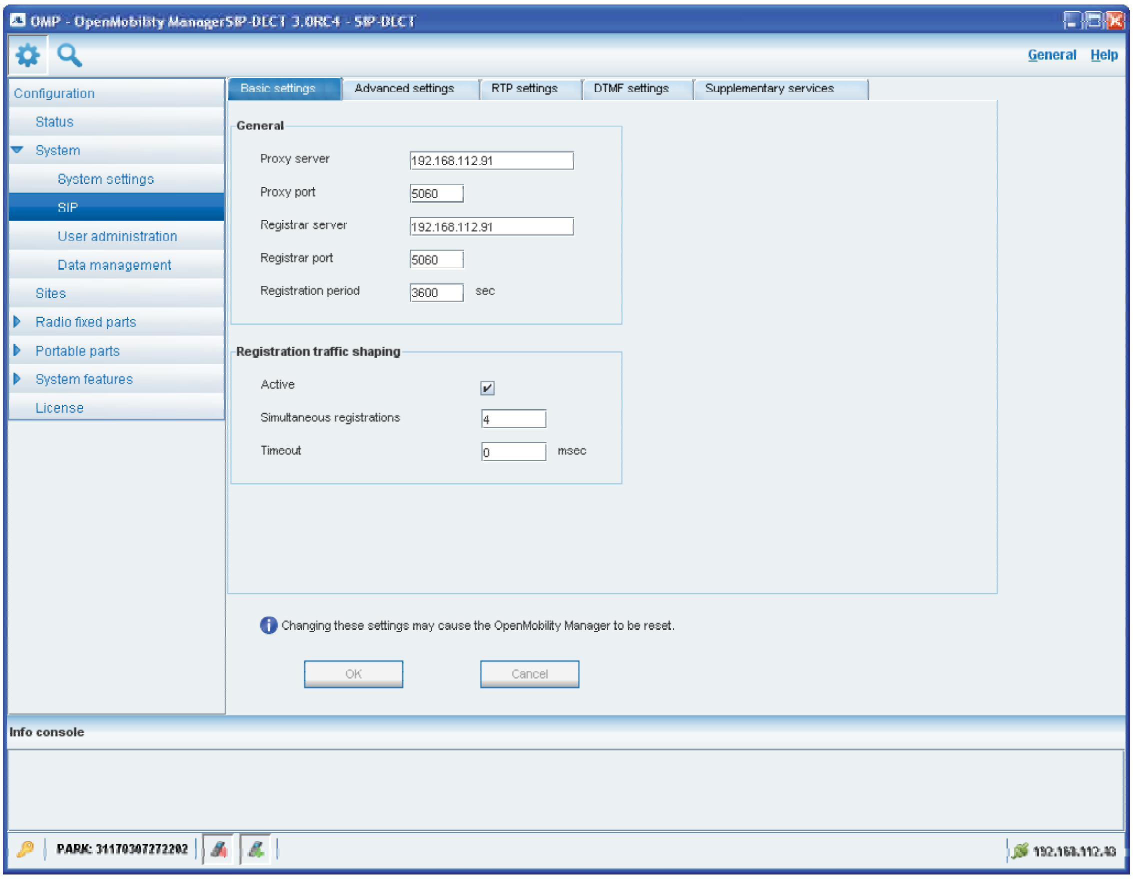
Unit: sec

Distribution

From	To	Number
0	1	0
1	2	0
2	4	97
4	8	1
8	15	7
15	30	1
30	45	2
45	60	0
60	90	0
90	120	0
120	240	0
240	480	0
480	900	0
900	1800	0
1800	2700	0
2700	3600	0
3600	5400	0
5400	7200	0
7200	...	0

8.5.3 “SIP” Menu

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



General

Proxy server 192.168.112.91

Proxy port 5060

Registrar server 192.168.112.91

Registrar port 5060

Registration period 3600 sec

Registration traffic shaping

Active ☑

Simultaneous registrations 4

Timeout 0 msec

Changing these settings may cause the OpenMobility Manager to be reset.

PARK: 31170307272202

192.168.112.43

The menu provides the settings in several tabs:

Basic settings

For a description of the parameters which can be set in the **Basic settings** tab, please refer to the description of the **SIP** page of the OMM Web service (see chapter 7.4.2). The corresponding parameters can be found there in the **Basic settings** and **Registration traffic shaping** page sections.

Note that the **Registration traffic Shaping – Timeout** parameter (OMP) corresponds to the **Waiting time** parameter (OMM Web service).

Advanced settings

For a description of the parameters which can be set in the **Advanced settings** tab, please refer to the description of the **SIP** page of the OMM Web service (see chapter 7.4.2). The corresponding parameters can be found there in the **Advanced settings** page section.

RTP settings

For a description of the parameters which can be set in the **RTP settings** tab, please refer to the description of the **SIP** page of the OMM Web service (see chapter 7.4.2). The corresponding parameters can be found there in the **RTP settings** page section.

DTMF settings

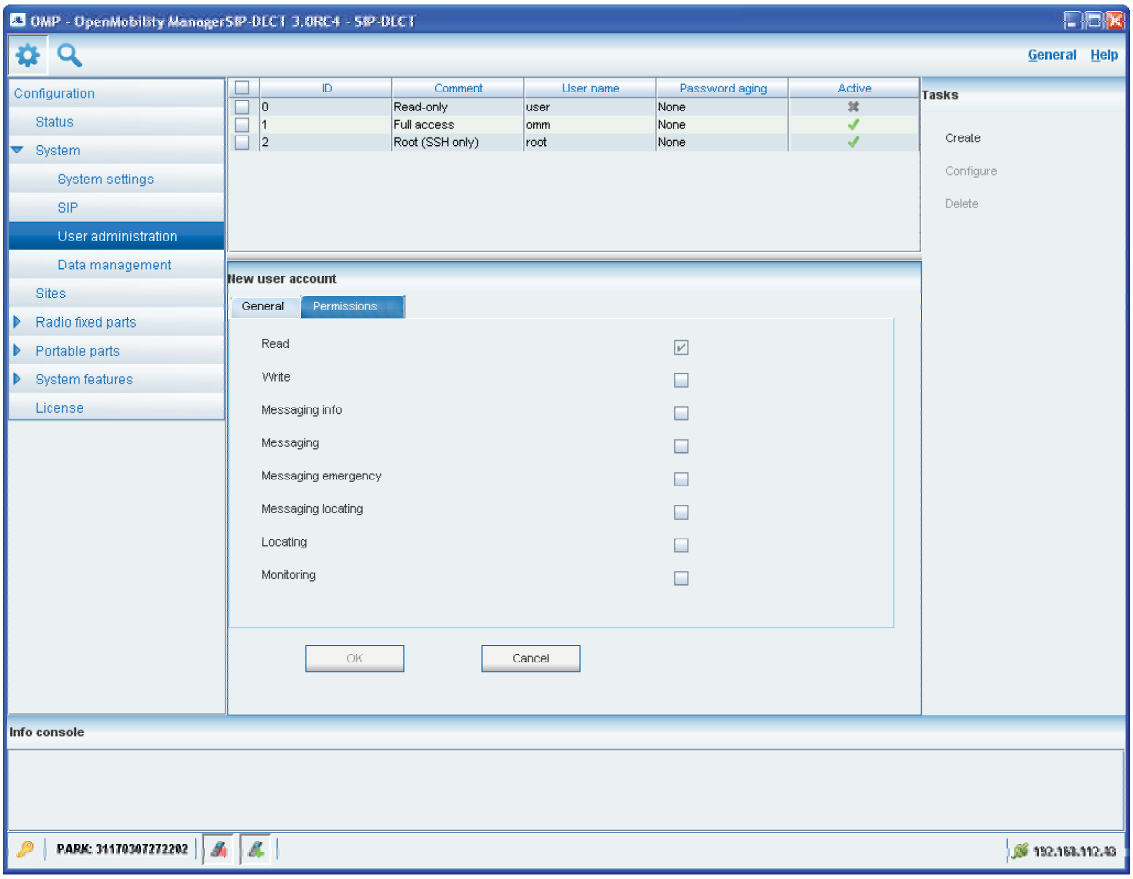
For a description of the parameters which can be set in the **DTMF settings** tab, please refer to the description of the **SIP** page of the OMM Web service (see chapter 7.4.2). The corresponding parameters can be found there in the **DTMF settings** page section.

Supplementary services

For a description of the parameters which can be set in the **Supplementary services** tab, please refer to the description of the **SIP** page of the OMM Web service (see chapter 7.4.2). The corresponding parameters can be found there in the **Supplementary Services** page section.

8.5.4 “User administration” Menu

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



□	ID	Comment	User name	Password aging	Active
□	0	Read-only	user	None	✗
□	1	Full access	omm	None	✓
□	2	Root (SSH only)	root	None	✓

New user account

General | Permissions

- Read ☑
- Write □
- Messaging info □
- Messaging □
- Messaging emergency □
- Messaging locating □
- Locating □
- Monitoring □

OK | Cancel

User administration menu in configuration mode

The 3 user accounts “Full access”, “Read-only” and “Root (ssh only)” available via the **User administration** page of the OMM Web service (see chapter 7.4.3) can also be configured in the OMP. These are 3 predefined user accounts, which cannot be removed or renamed. Only the “Root (ssh only)” account can be deactivated. The permissions are fixed. This is consistent with the OMM WEB service. The meaning of the different account types is described in section 9.14.1. In addition, the OMP allows to create additional user accounts (login and password) and to assign specific permissions.

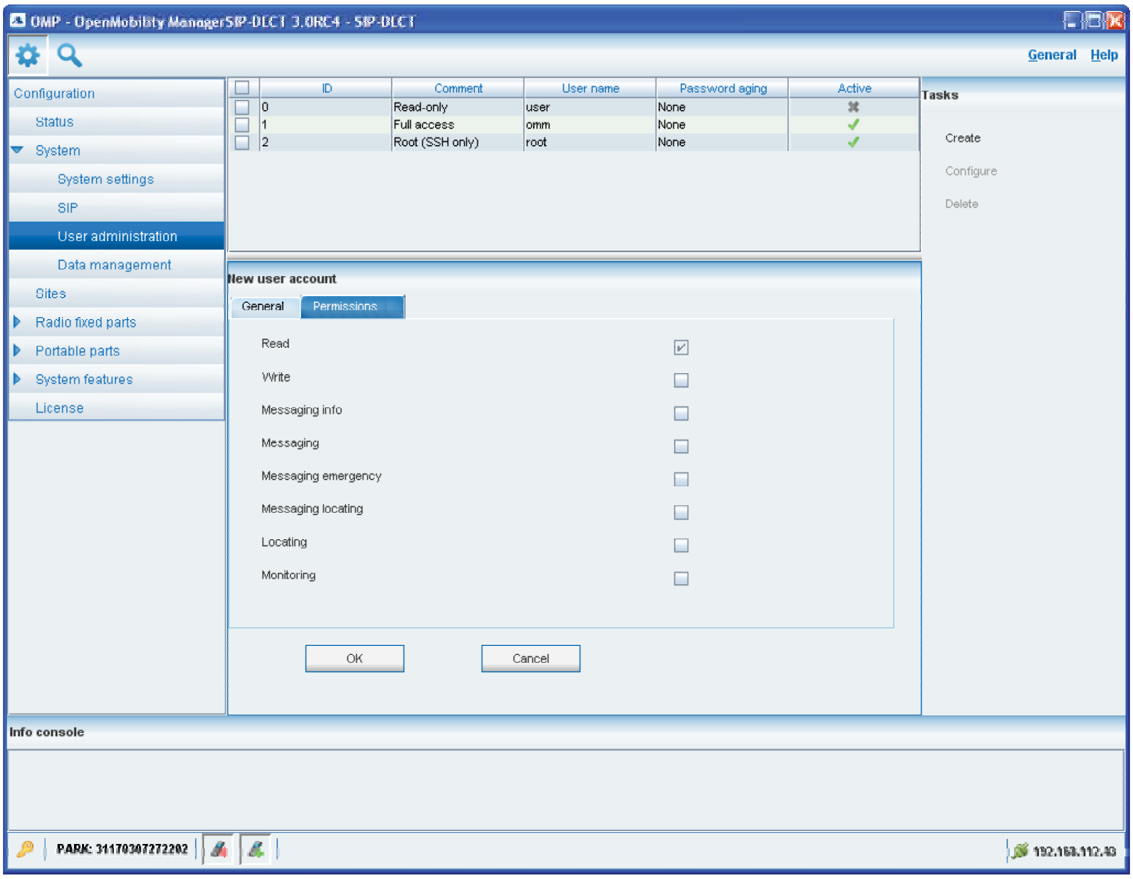
The tasks which can be performed are mode-dependant.

Configuration mode	Monitor mode	See chapter
Create: create new user account		8.5.4.1
Configure: configure selected user account in detail panel		8.5.4.2
	Show details: shows selected user account in detail panel	8.5.4.3
Delete: delete selected user account		8.5.4.4

8.5.4.1 Creating New User Accounts

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

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



□	ID	Comment	User name	Password aging	Active
□	0	Read-only	user	None	✗
□	1	Full access	omm	None	✓
□	2	Root (SSH only)	root	None	✓

Read	☑
Write	□
Messaging info	□
Messaging	□
Messaging emergency	□
Messaging locating	□
Locating	□
Monitoring	□

Adding individual user accounts is only possible in **configuration mode**. To add a user account proceed as follows:

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

   The **New user account** panel opens. It provides various tabs where the account data has to be entered.

2. Configure the user account, see parameter description below.

3. Press the **OK** button.

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

General

For a description of the parameters which can be set in the **General** tab, please refer to the description of the **User administration** page of the OMM Web service (see chapter 7.4.3).

Permissions

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

If an application connects with the OMM via OM AXI, then the permissions been sent from the OMM to the application is the result of the configured permissions for this account and the actual license status. For more information please see the OM Application XML Interface (OM AXI) specification /28/.

The permissions have the following meaning:

Permission	Description
Read	Read OMM data (OM AXI get requests)
Write	Read OMM data (OM AXI set requests)
Messaging info	Sent messages with prio “Info”
Messaging	Sent messages with prio “Low”, “Normal” and “High”
Messaging emergency	Sent messages with prio “Emergency”
Messaging locating	Sent messages with prio “LocatingAlert”
Locating	Permission to query the position of PPs and to track PP positions
Monitoring	Permission to monitor various technical aspects of the mobility system

8.5.4.2 Changing a User Account

Changing user accounts is only possible in **configuration mode**. To change the configuration of an existing user account proceed as follows:

1 Select the appropriate user account in the account table.

2 In the **Tasks** bar click on the **Configure** command.

3 Change the user account parameters, see parameter description in chapter 8.5.4.1.

4 Press the **OK** button.

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

8.5.4.3 Viewing User Account Details

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

1 Select the appropriate user account in the table.

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

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

3 To close the user account detail panel press the **Cancel** button.

8.5.4.4 Deleting User Accounts

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

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

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

8.5.5 "Data management" Menu

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

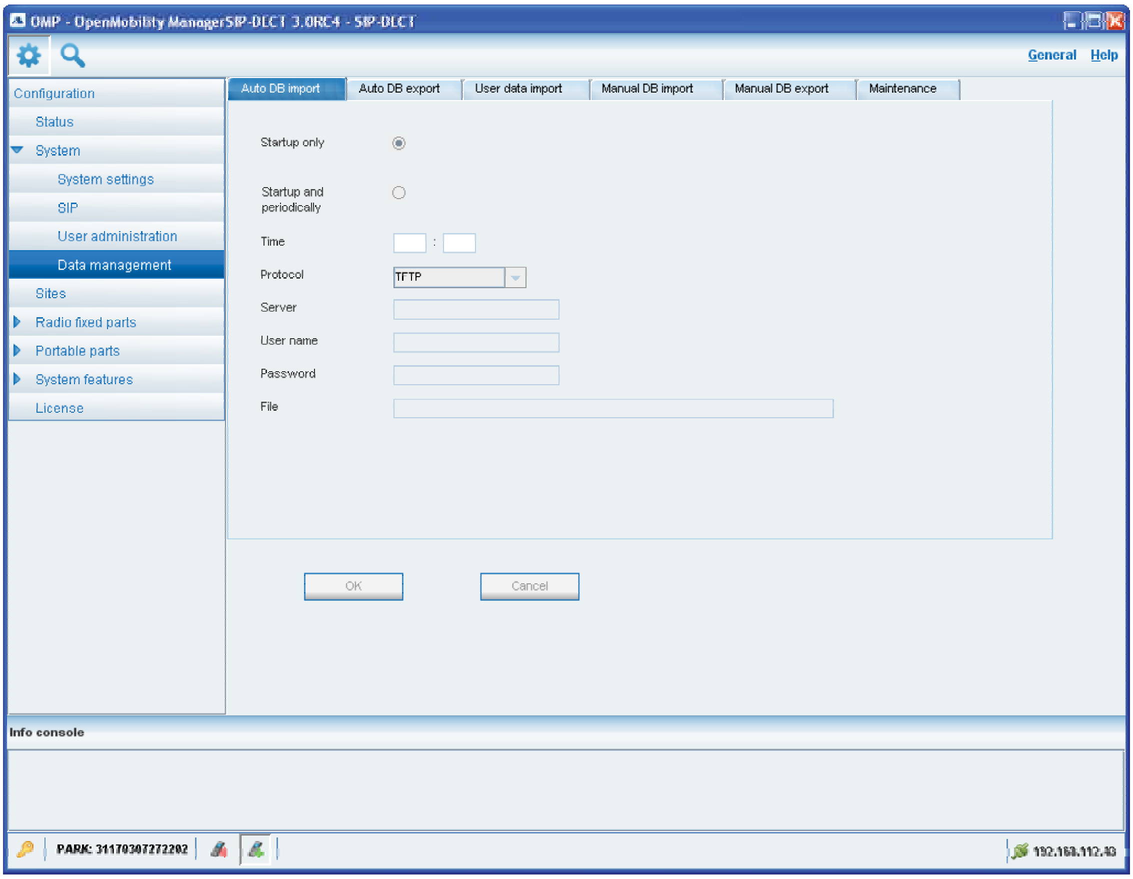
The menu provides the settings in several tabs:

- **Automatic DB import** (see chapter 8.5.5.1),
- **Automatic DB export** (see chapter 8.5.5.2),
- **User data import** (see chapter 8.5.5.3),
- **Manual DB import** (see chapter 8.5.5.4),
- **Manual DB export** (see chapter 8.5.5.5),
- **Maintenance** (see chapter 8.5.5.6).

8.5.5.1 "Automatic DB import" Tab

The automatic database (DB) import feature makes it easier to restore a prepared OMM database into an OMM for an initial configuration or for update reasons.

> **Please note:** An automatic import of a database leads to a reset of the OMM to take effect.



Startup only ●

Startup and periodically ○

Time :

Protocol TFTP

Server

User name

Password

File

In the **Automatic DB import** panel enter the following:

1 **Startup only**: Activate this option if the import should be started for an initial configuration.

2 **Startup and periodically**: If this option is activated, the OMM tries to import the configured database file during startup and at the configured time of day.

3 **Time**: Enter the time, the import should be started.

Please note: An automatic database import at a configured time recommends the time synchronization with an NTP server. For NTP server configuration see chapter 9.5.4 and chapter 9.6.

4 **Protocol**: To import a database from an external server select the preferred protocol. The following protocols are supported: FTP, FTPS, HTTP, HTTPS, TFTP.

5 **Server**: Enter the IP address or the name of the external server.

6 **User name**, **Password**: If necessary, enter the account data of the server.

7 **File**: Enter the path and file name which include the OMM database.

The database file for an automatic import has to be configured in an URL format like

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

or

tftp://[server]/[directory/]file.To be available at OMM startup time and to allow an initial configuration via automatic import, this URL has to be specified via DHCP (option 24, see chapter 9.5.4) or the OM Configurator (see chapter 9.6). If such a URL is given by DHCP or the OM Configurator, the OMM tries to import a configured database file automatically during the OMM startup.

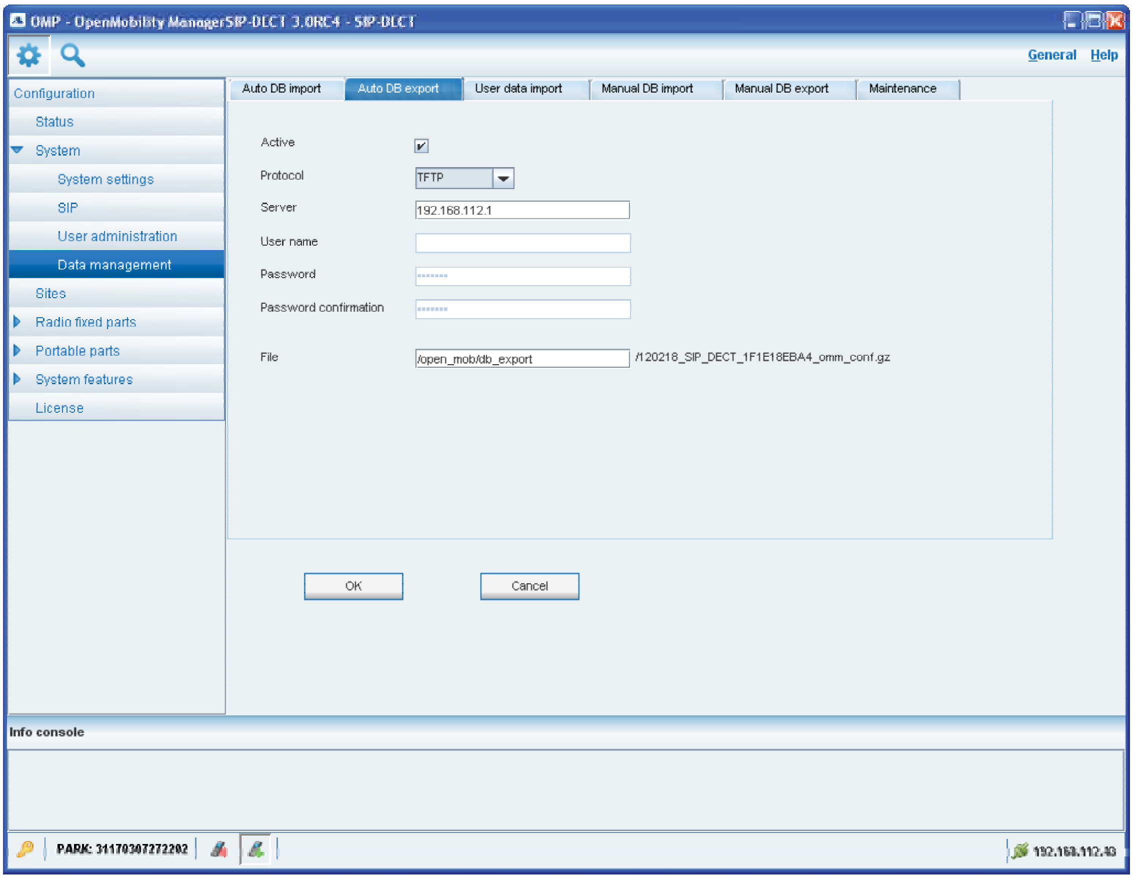
8 Click **OK** to confirm the settings for the automatic import.

For further information on the automatic database import process please refer to the chapter 7.4.6.2.

8.5.5.2 “Automatic DB export” Tab

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

Please note: For an automatic database export a time synchronization with an NTP server is mandatory. For NTP server configuration see chapter 9.5.4 and chapter 9.6.



Active ☑

Protocol TFTP

Server 192.168.112.1

User name

Password ••••••••

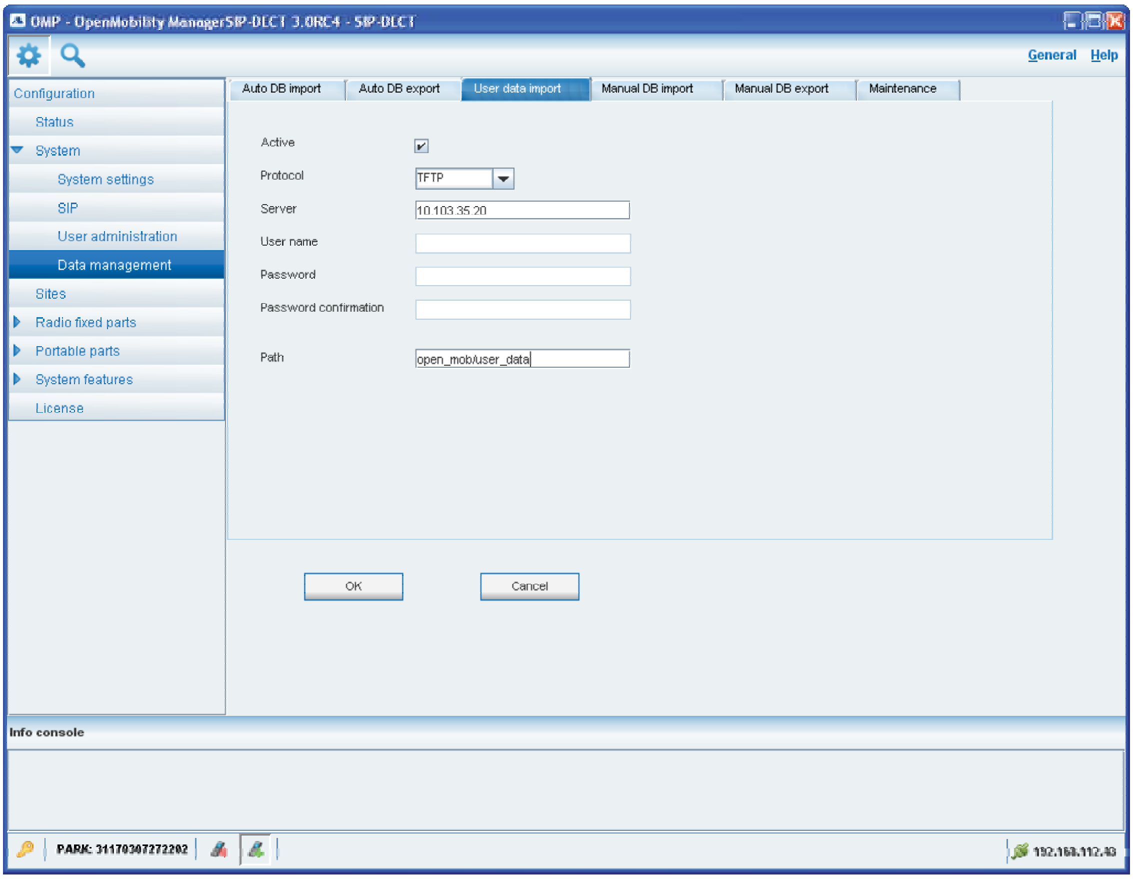
Password confirmation ••••••••

File /open_mob/db_export /120218_SIP_DECT_1F1E18EBA4_omm_conf.gz

For a description of the parameters which can be set in the **Automatic DB export** tab, please refer to the corresponding description in the chapter 7.4.6.4.

8.5.5.3 “User data import” Tab

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



Active ☑

Protocol TFTP

Server 10.103.35.20

User name

Password

Password confirmation

Path open_mob/user_data

1 **Active**: Activate this option to enable the user data import feature.

2 **Protocol**: Select the preferred protocol.

3 **Server**: Enter the IP address or the name of the server.

4 **User name**, **Password**: If necessary, enter the account data of the server.

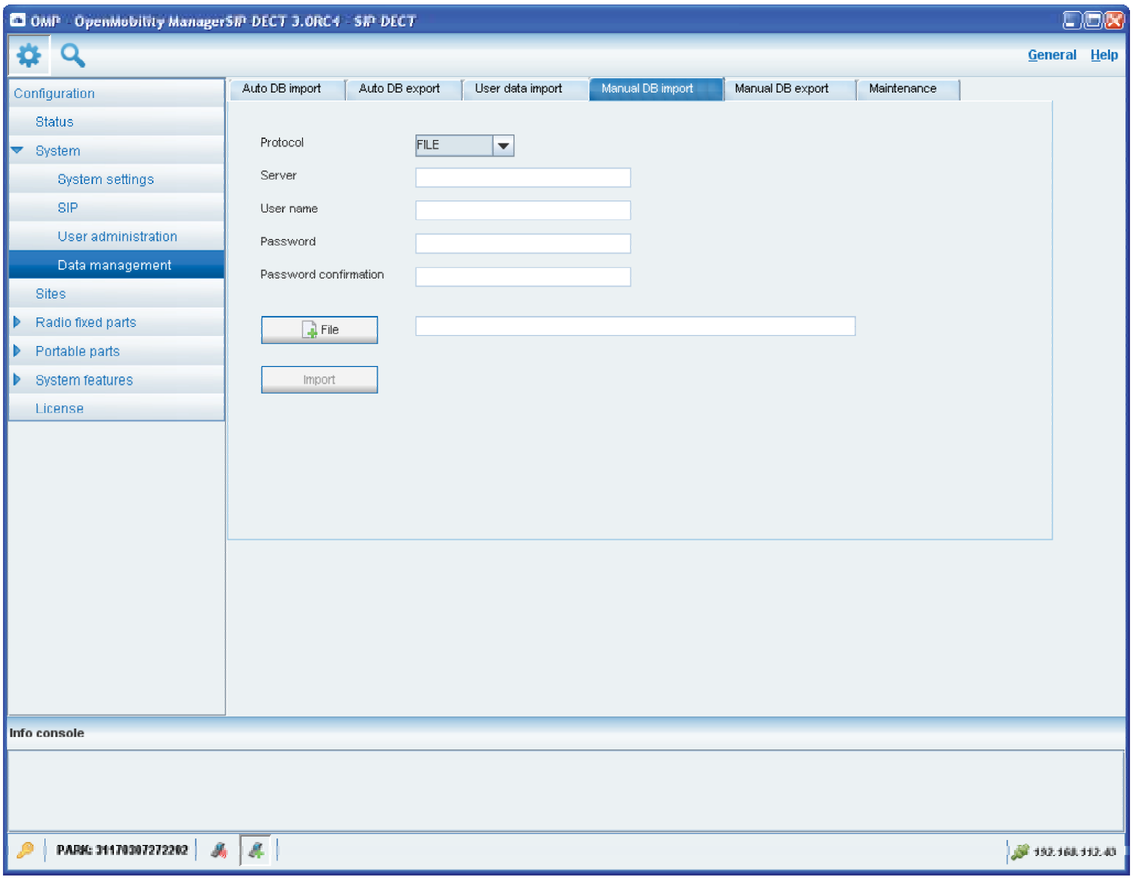
5 **Path**: Enter the path which includes the user data.

6 Click **OK** to confirm the settings for the user data import.

For further information on the user data import please refer to the “OpenMobility Provisioning” user guide for details see /27/.

8.5.5.4 “Manual DB import” Tab

Please note: A manual import of a database leads to a reset of the OMM to take effect.



Protocol FILE

1 **Protocol**:

– To import a database from the file system the protocol **FILE** has to be selected.

– To import a database from an external server select the preferred protocol (e.g. HTTP).

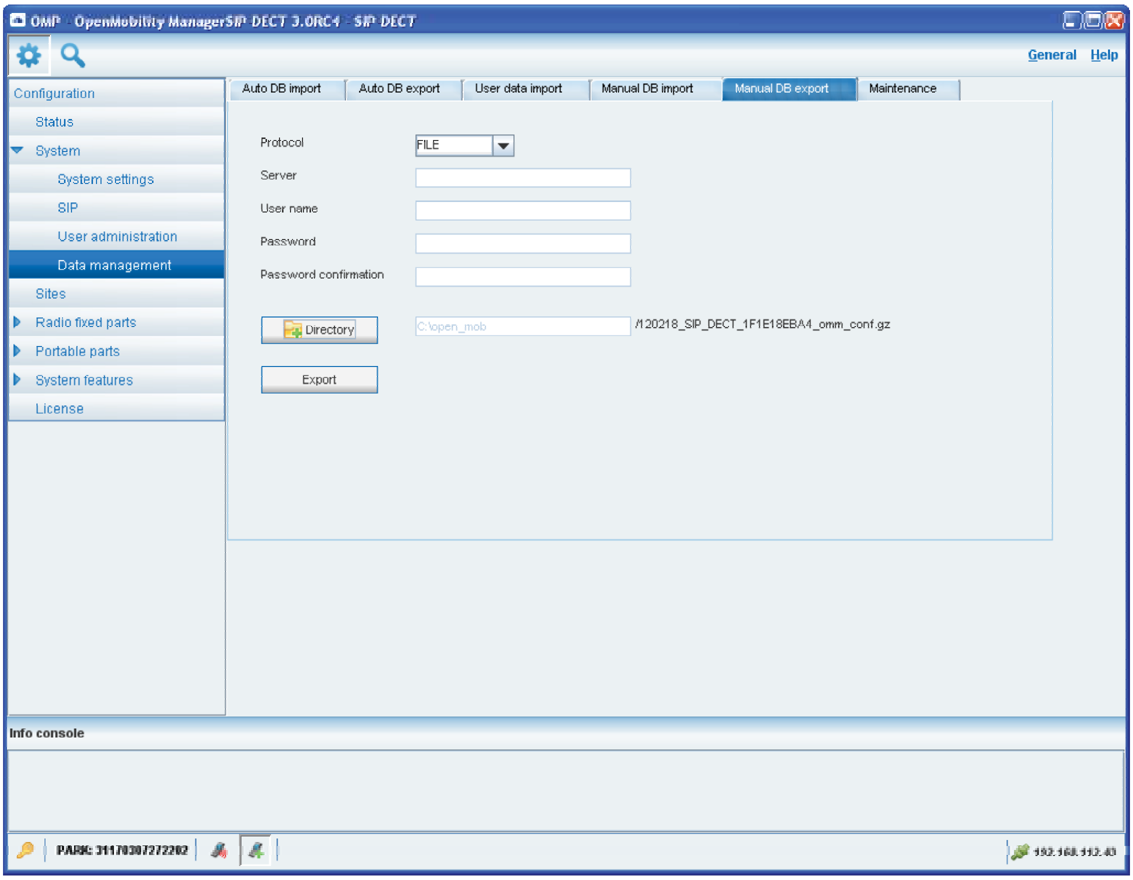
2 **Server**: Enter the IP address or the name of the external server.

3 **User name**, **Password**, **Password confirmation** (in case of import from an external server): If necessary, enter the account data of the server.

4 **File** (only if you have selected the **FILE** protocol): Enter the path and file name which include the OMM database or select a file by pressing the **File** button.

5 Press the **Import** button.

8.5.5.5 “Manual DB export” Tab



Protocol FILE

Server

User name

Password

Password confirmation

C:\open_mob /120218_SIP_DECT_1F1E18EBA4_omm_conf.gz

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

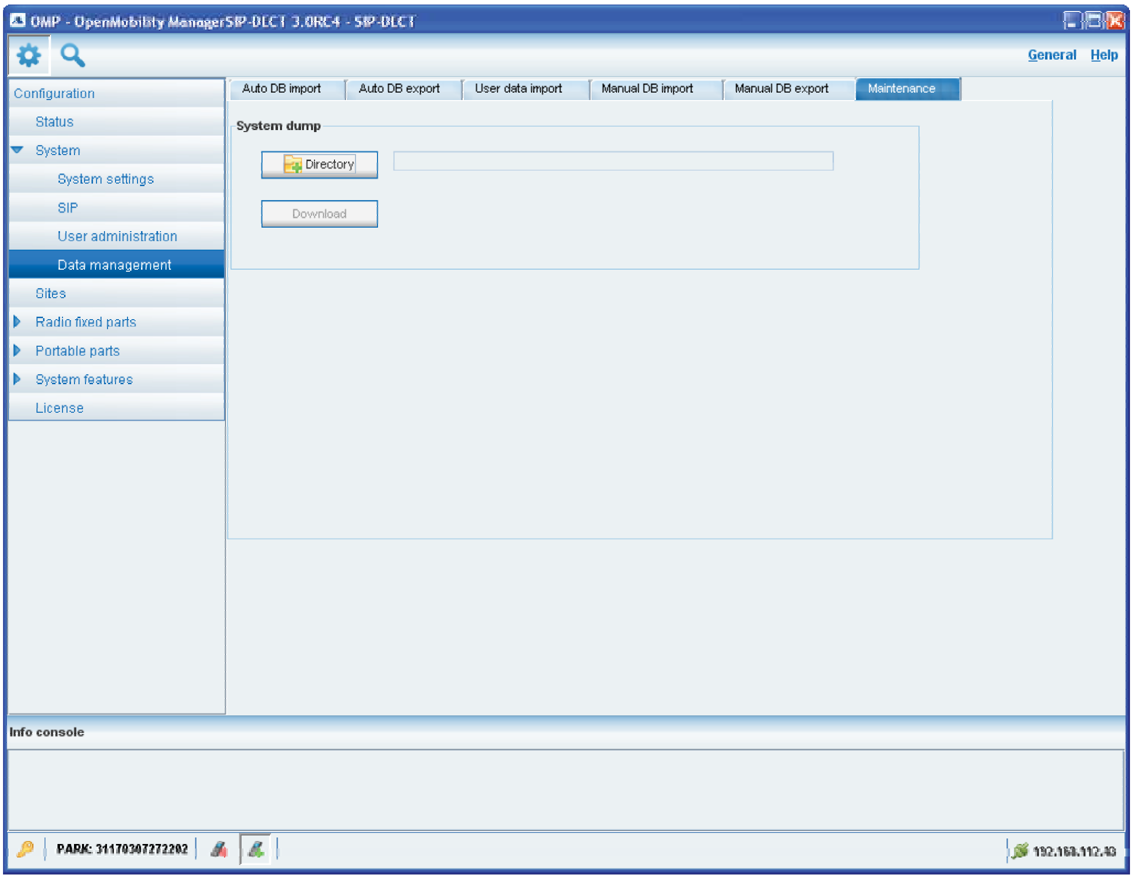
2 **Server**: Enter the IP address or the name of the server.

3 **User name**, **Password**, **Password confirmation**: If necessary, enter the account data of the server.

4 **Directory** (only if you have selected the **FILE** protocol): Select a directory by pressing the **Directory** button.

5 Press the **Export** button.

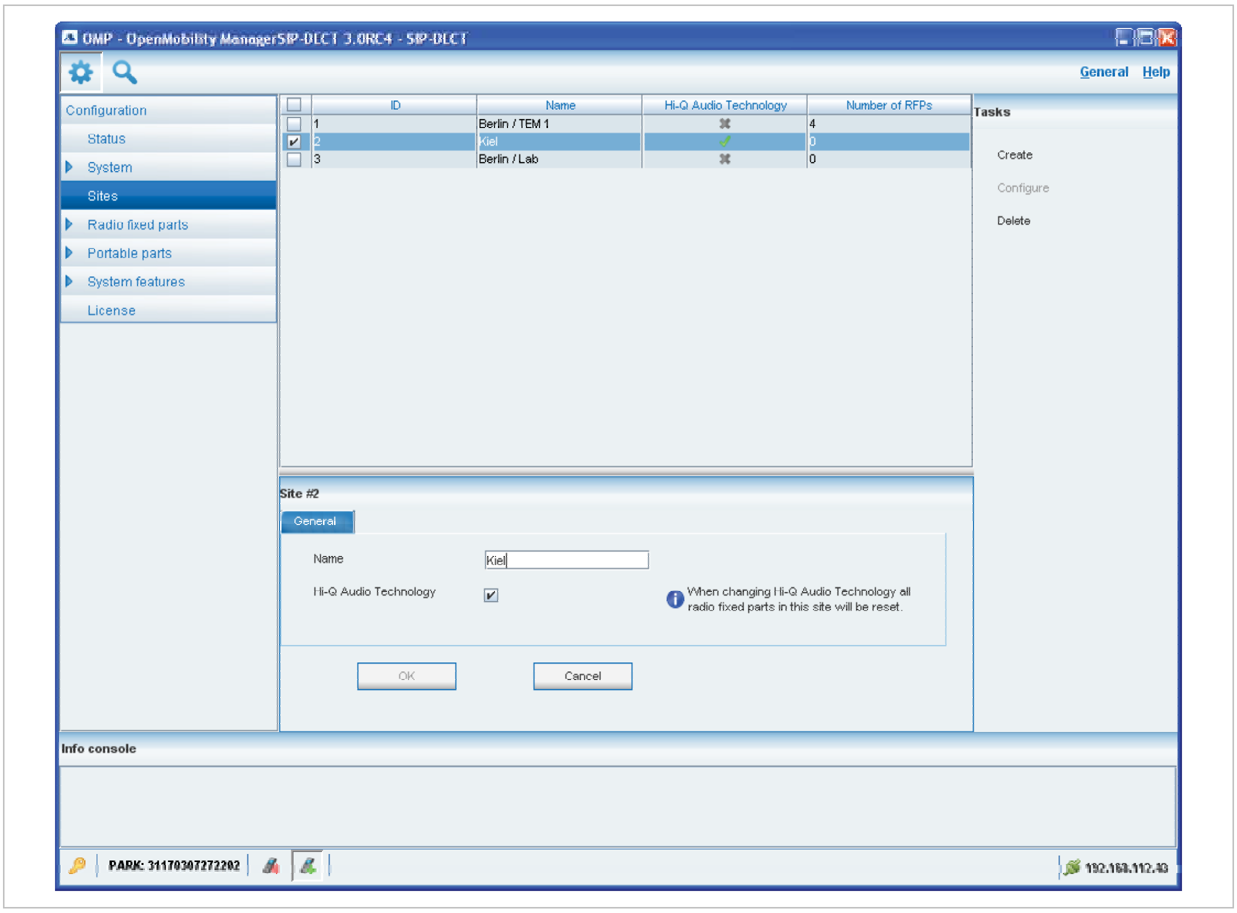
8.5.5.6 “Maintenance” Tab



In the **Maintenance** panel you can configure and start a system dump. A file “sysdump.txt” is created in the selected directory. Press the **Directory** button to select the directory. Then press the **Download** button to start the system dump.

8.6 “Sites” Menu

RFPs can be grouped into different sites. The **Sites** menu allows to configure/view the configured sites. An empty system has one predefined site (ID: 1) named “default”. Minimum one site is required by the system.



□	ID	Name	Hi-Q Audio Technology	Number of RFPs
□	1	Berlin / TEM 1	✖	4
☑	2	Kiel	✓	0
□	3	Berlin / Lab	✖	0

Site #2

General

Name: Kiel

Hi-Q Audio Technology ☑

When changing Hi-Q Audio Technology all radio fixed parts in this site will be reset.

PARK: 31170307272202

192.168.112.43

A site consists of the following parameters:

- **ID**: Identification number of the site. A value between 1 and 250 is possible. If no value is given, the OMM selects the next free ID.
- **Name**: The name of the site.
- **Hi-Q Audio Technology**: The capability Hi-Q TM audio technology must be enabled or disabled specific for every site.

  – In sites, which are configured to provide this functionality, exclusively RFP 35 / 36 / 37 and RFP 43 WLAN are applicable.

  – In sites without this capability, it is allowed to mix these new RFP-types with RFP 32 / 34 and RFP 42 WLAN.
- **Number of RFPs**: The number of RFPs which are assigned to this site.

The following tasks can be performed:

- **Create**: create a new site in the **General** tab.
- **Configure**: configure an existing site in the **General** tab.
- **Delete**: delete selected sites.
- **Show details** (only in **monitor mode**): shows configuration of a selected site in the **General** tab.

Note: Only sites without assigned RFPs can be deleted.

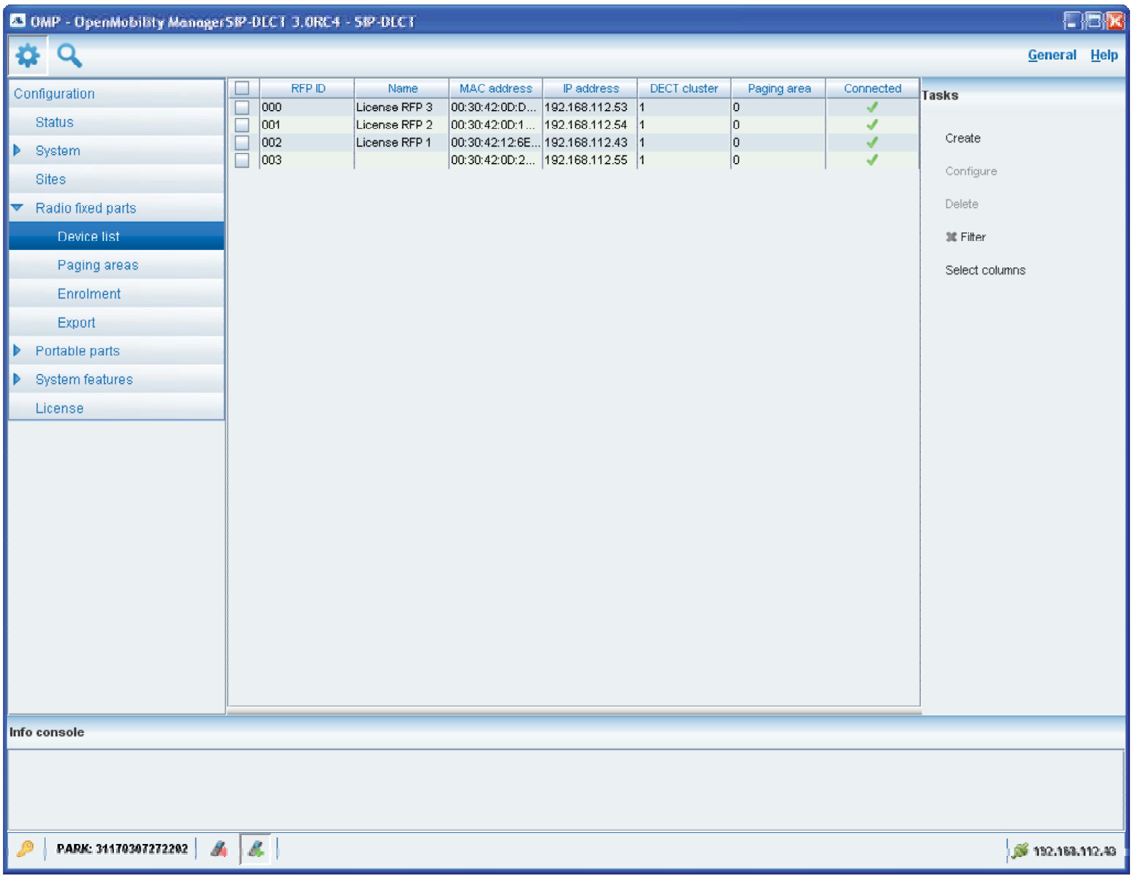
8.7 “Radio fixed parts” Menu

RFPs can be configured and viewed in the **Radio fixed parts** menu. The **Radio fixed parts** menu provides the following entries:

Configuration mode	Monitor mode	See chapter
Device list	Device list	8.7.1
Paging areas		8.7.2
Enrolment		8.7.3
Export		8.7.4
	Sync view	8.7.5
	Statistics	8.7.6

8.7.1 “Device list” Menu

In the **Device list** panel, all configured RFPs are listed in a table. The device list is available in **configuration mode** as well as in **monitor mode**.



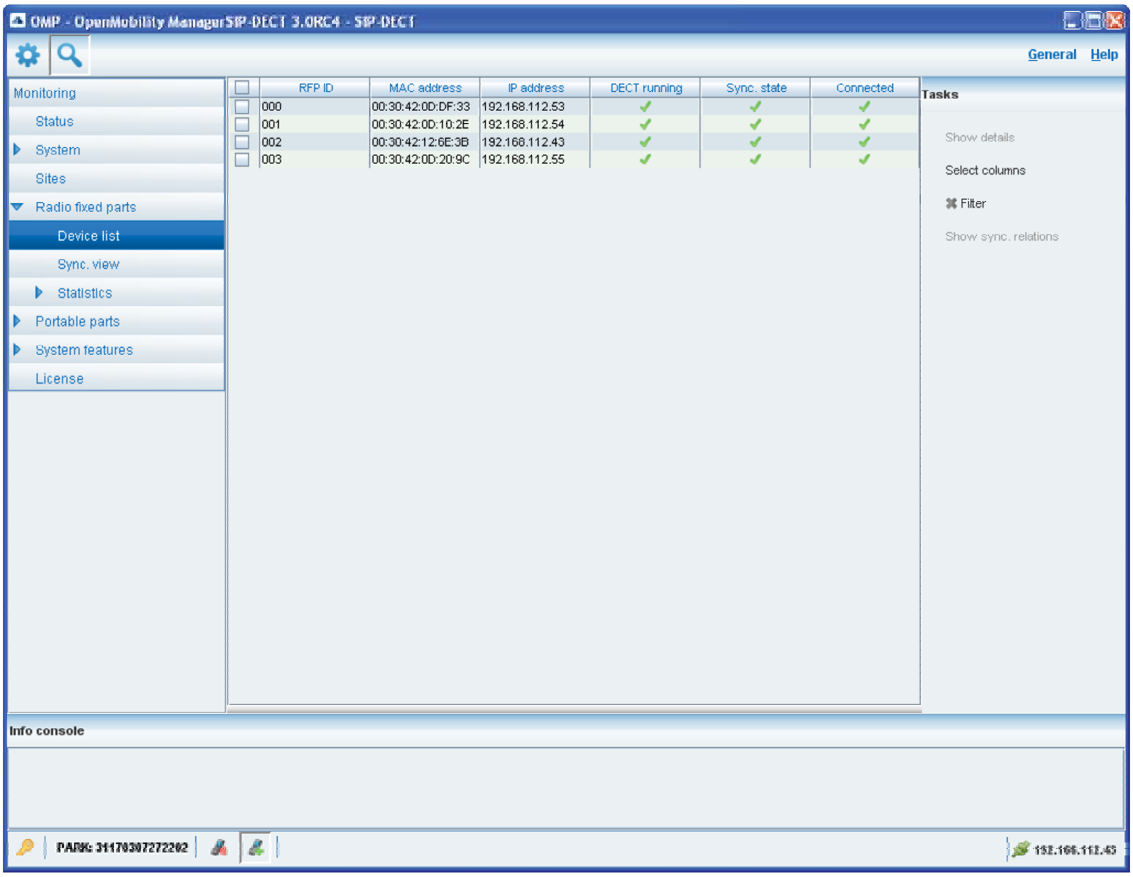
□	RFP ID	Name	MAC address	IP address	DECT cluster	Paging area	Connected
□	000	License RFP 3	00:30:42:0D:D...	192.168.112.53	1	0	✓
□	001	License RFP 2	00:30:42:0D:1...	192.168.112.54	1	0	✓
□	002	License RFP 1	00:30:42:12:6E...	192.168.112.43	1	0	✓
□	003		00:30:42:0D:2...	192.168.112.55	1	0	✓

Device list in configuration mode

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

- ✖ – DECT is not enabled and/or RFP not connected.
- ✖ – DECT is enabled and RFP connected, but DECT has not been activated yet.
- 🔍 – DECT is enabled and RFP is connected, but RFP is not synchronized and searches for other synchronized RFPs.
- ✓ – DECT is enabled and RFP is connected and synchronized.

Note:	If the **Active** column is not displayed, you can activate it in the **Select columns** dialog, see chapter 8.7.1.7.



□	RFP ID	MAC address	IP address	DECT running	Sync. state	Connected
□	000	00:30:42:0D:DF:33	192.168.112.53	✓	✓	✓
□	001	00:30:42:0D:10:2E	192.168.112.54	✓	✓	✓
□	002	00:30:42:12:6E:3B	192.168.112.43	✓	✓	✓
□	003	00:30:42:0D:20:9C	192.168.112.55	✓	✓	✓

Device list in monitor mode

The tasks which can be performed are mode-dependant.

Configuration mode	Monitor mode	See chapter
Create: create new RFP in detail panel		8.7.1.2
Configure: configure selected RFP in detail panel		0
	Show details: show selected RFP in detail panel	8.7.1.4
Delete: delete selected RFP		8.7.1.5
	Show sync. relations: show synchronization relation for selected RFPs	8.7.1.6

Select columns: select columns/parameters to be shown in RFP table	**Select columns**: select columns/parameters to be shown in RFP table	8.7.1.7
Filter: show only RFP datasets in table which contain a special search string	**Filter**: show only RFP datasets in table which contain a special search string	8.7.1.8

8.7.1.1 RFP Detail Panel

The RFP detail panel is used for configuration/showing of RFP settings and creation of new RFP datasets.

To call up the RFP detail panel

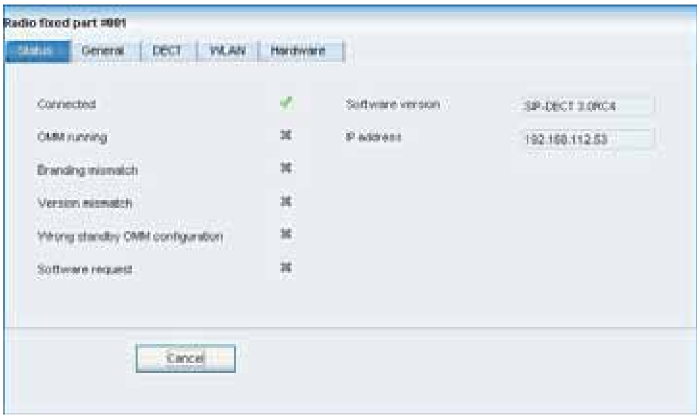
- choose one of the commands in the task bar on the right of the **Radio fixed parts** panel (**Create**, **Configure**, or **Show details**)

  or
- select the appropriate RFP in the RFP table and double-click the entry.

The RFP detail panel contains the following parameter groups sorted in different tabs.

“Status” tab

This tab is only available in **monitor mode**. It shows system status information relating to the selected RFP.



Radio fixed part #001

Connected ✓

OMM running ✗

Branding mismatch ✗

Version mismatch ✗

Wrong standby OMM configuration ✗

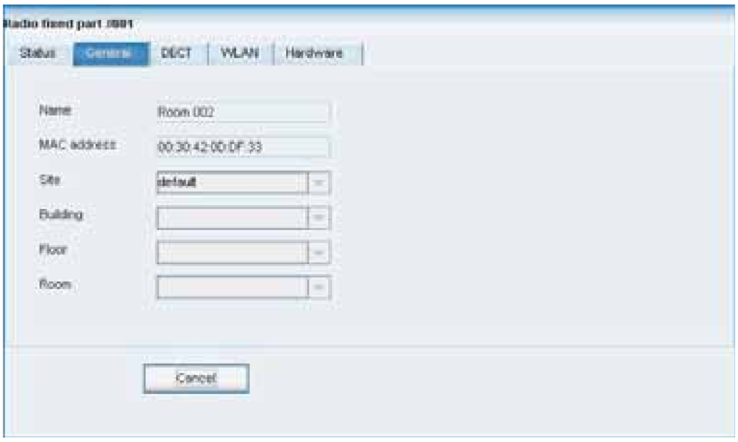
Software request ✗

Software version: SIP-DECT 3.0RC4

IP address: 192.168.112.53

“General” tab

This tab contains the general RFP parameters.



Name: Room 002

MAC address: 00:30:42:0D:DF:33

Site: default

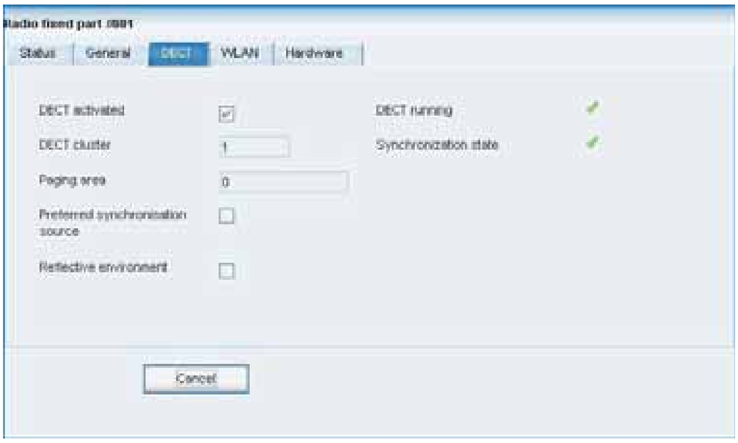
Building:

Floor:

Room:

“DECT” tab

This tab contains the RFP's DECT parameters.



DECT activated ☑

DECT cluster: 1

Paging area: 0

Preferred synchronization source □

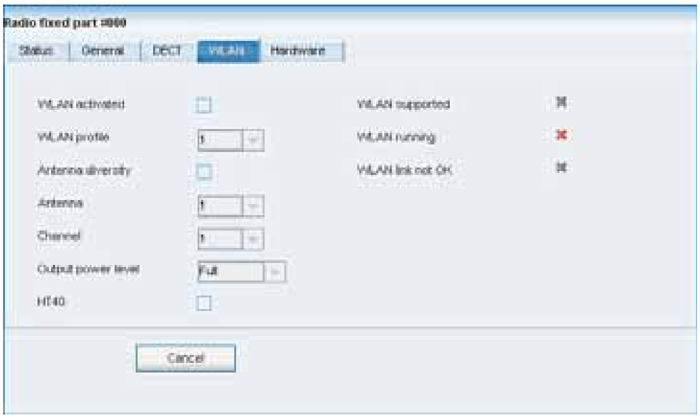
Reflective environment □

DECT running ✓

Synchronization state ✓

“WLAN” tab

This tab contains the RFP WLAN parameters. Settings in the **WLAN** tab apply to RFPs of the type “RFP (L) 42 WLAN” and “RFP (L) 43 WLAN” only.



WLAN activated □

WLAN profile: 1

Antenna diversity □

Antenna: 1

Channel: 1

Output power level: Full

HT40 □

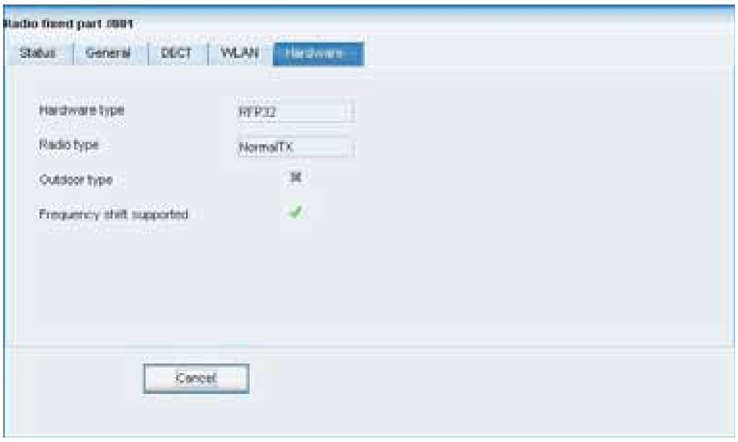
WLAN supported ✗

WLAN running ✗

WLAN link not OK ✗

“Hardware” tab

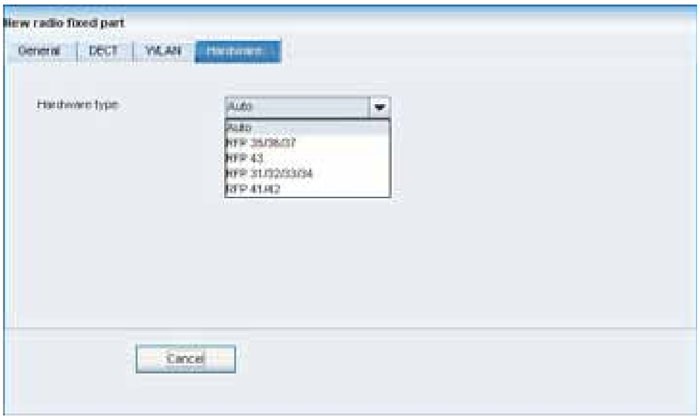
In **monitor mode** this tab shows hardware information of the selected RFP.



Hardware type: RFP32
Radio type: NormalTX
Outdoor type: ✗
Frequency shift supported: ✓

RFP Hardware tab in monitor mode

In configuration mode, the RFP hardware type can be set.



Hardware type: Auto

- Auto
- RFP 35/36/37
- RFP 43
- RFP 31/32/33/34
- RFP 41/42

8.7.1.2 Adding New RFPs

Adding new RFPs is only possible in **configuration mode**. To add an RFP to the list of known RFP proceed as follows:

1. In the task bar on the right of the **Radio fixed parts** panel click on the **Create** command.
   The **New radio fixed part** panel opens. It provides various tabs where the RFP data has to be entered, see chapter 8.7.1.1.
2. Configure the RFP, see parameter description below.
3. Press the **OK** button.

The following parameters can be set in the tabs of the **New radio fixed part** panel:

"General" tab

- **Name**: The a name for the RFP.
- **MAC address**: Each RFP is identified by its unique MAC address (6 bytes hex format, colon separated). Enter the MAC address, it can be found on the back of the chassis.
- **Site**: If several sites exist (see chapter 0), select the site the RFP is assigned to.
- **Building**, **Floor**, **Room**: For easier localization of the RFP you can enter data in these fields.

“DECT” tab

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

Note: The **Paging area size** is set in the **DECT** tab of the **System settings** menu (see chapter 8.5.1). The assignment between RFPs and paging areas can be changed in the **Paging areas** menu (see chapter 8.7.1.8).

- **Preferred synchronization source**: Activate this checkbox if the RFP should be used as synchronization source for the other RFPs in the cluster. For background information on RFP synchronization please refer to chapter 9.2.
- **Reflective environment**: Within areas containing lot of reflective surfaces (e.g. metal or metal coated glass) in an open space environment the voice quality of a DECT call can be disturbed because of signal reflections which arrive on the handset or RFP using multipath propagation. Calls may have permanent drop outs while moving and high error rates on the RFPs and handsets.

  For such environment Aastra has developed the DECT XQ enhancement into base stations (RFP 32 / 34 / 42 WLAN and RFP 35 / 36 / 37 / 43 WLAN) and the Aastra 600d / Aastra 650c handsets family. Using this enhancement by switching the **Reflective environment** flag on might reduce drop outs and cracking noise.

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

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

“WLAN” tab

Settings in the **WLAN** tab apply to RFPs of the type “RFP (L) 42 WLAN” and “RFP (L) 43 WLAN” only. For details about WLAN configurations please see chapter 9.15.

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

For a description of the parameters which can be set in the **WLAN** tab, please refer to the description of the **Radio fixed parts** page of the OMM Web service (see chapter 7.6.3). The corresponding parameters can be found there in the **WLAN settings** section.

Note: Configuration of WLAN profiles is only possible with the OM Web service, see chapter 7.8.1.

“Hardware” tab

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

8.7.1.3 Changing RFPs

Changing RFPs is only possible in **configuration mode**. To change the configuration of an existing RFP proceed as follows:

1. Select the appropriate RFP in the RFP table.
2. In the task bar on the right of the **Radio fixed parts** panel click on the **Configure** command.

   The RFP detail panel opens, see chapter 8.7.1.1.
3. Change RFP parameters, see parameter description in chapter 8.7.1.2.
4. Press the **OK** button.

8.7.1.4 Viewing RFP Details

You can view the configuration of an RFP in **monitor mode**. Proceed as follows:

1. Select the appropriate RFP in the RFP table.
2. In the task bar on the right of the **Radio fixed parts** panel click on the **Show details** command.

   The RFP detail panel opens, see chapter 8.7.1.1.
3. To close the RFP detail panel press the **Cancel** button.

8.7.1.5 Deleting RFPs

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

1. Select the appropriate RFP(s) in the RFP table by activating the corresponding checkbox(es).
2. In the task bar on the right of the **Radio fixed parts** panel click on the **Delete** command.

   The **Delete selected radio fixed part(s)** dialog opens showing a confirmation prompt.
3. Confirm the displayed prompt with **OK**.

Please note: License RFPs cannot be deleted.

8.7.1.6 Showing Synchronization Relations

You can view the synchronization relations of an RFP in **monitor mode**. Proceed as follows:

1. Select the appropriate RFP in the RFP table.
2. In the task bar on the right of the **Radio fixed parts** panel click on the **Show sync. relations** command.

   The view switches to the **Sync view** menu . For further information see chapter 8.7.5.

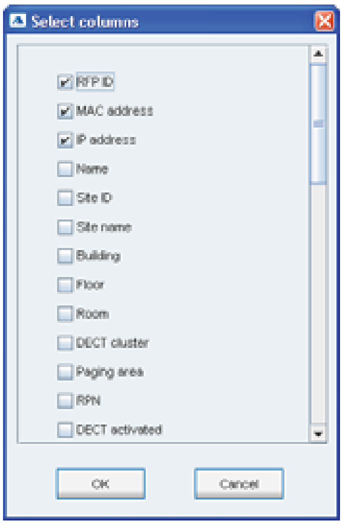
Note: At least two RFPs must be selected for showing their synchronization relations.

8.7.1.7 Selecting Columns

You can adapt the parameters shown in the RFP table to your needs:

1 In the task bar on the right of the **Radio fixed parts** panel click on the **Select columns** command.

The **Select columns** dialog opens.



☑ RFP ID
☑ MAC address
☑ IP address
☐ Name
☐ Site ID
☐ Site name
☐ Building
☐ Floor
☐ Room
☐ DECT cluster
☐ Paging area
☐ RPN
☐ DECT activated

2 Select the columns that shall be shown by activating the appropriate checkboxes.

3 Click the **OK** button.

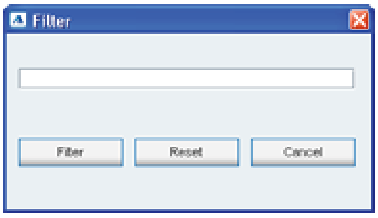
The RFP table will be adapted accordingly.

8.7.1.8 Filtering RFP Table

You can filter the list of RFP datasets shown in the RFP table by using a filter.

1 In the task bar on the right of the **Radio fixed parts** panel click on the **Filter** command.

The **Filter** dialog opens.



2 Enter the search string that serves as filter criterion. You can enter digits and characters. The search is case sensitive.

3 Click on the **Filter** button.

The **Filter** dialog is closed and the RFP table will be adapted accordingly.

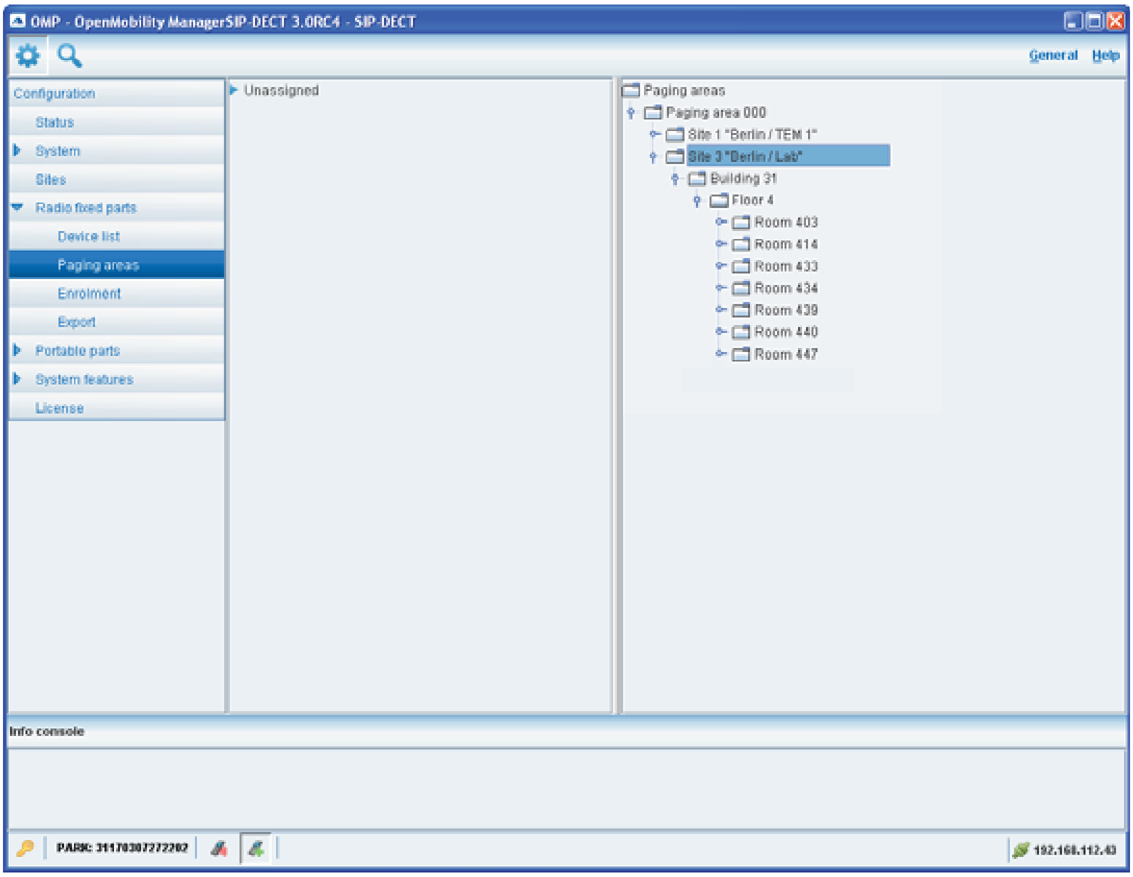
4 To reset the filter, click on the **Filter** command in the task bar on the right of the **Radio fixed parts** panel.

5 In the **Filter** dialog click on the **Reset** button.

8.7.2 “Paging areas” Menu

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

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



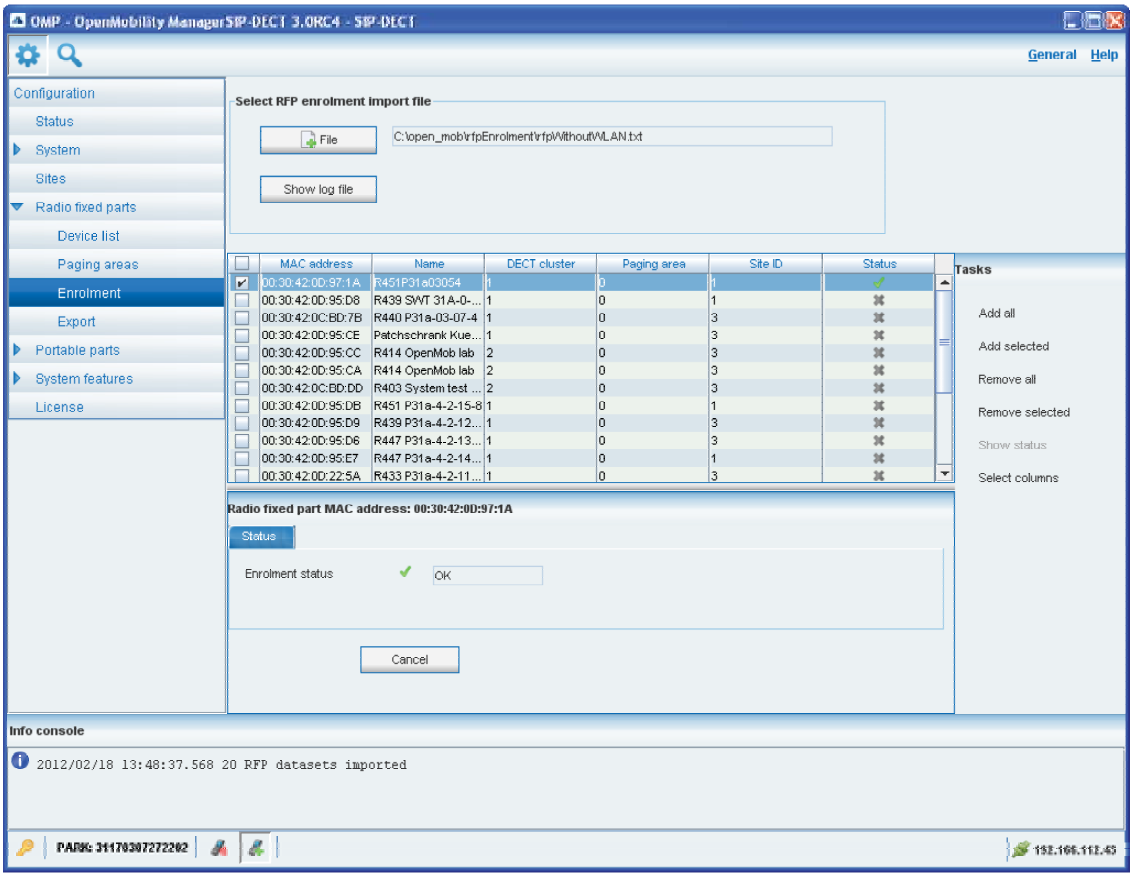
All RFPs are shown including their site and optional hierarchy (building, floor, and room) settings.

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

Note: The **Paging area size** is set in the **DECT** tab of the **System settings** menu (see chapter 8.5.1).

8.7.3 “Enrolment” Menu

The **Enrolment** menu allows import of RFP datasets using a configuration file. For information about required configuration file format see chapter 11.7.2.



Select RFP enrolment import file

C:\open_mob\rfpEnrolment\rfpWithoutWLAN.txt

☐	MAC address	Name	DECT cluster	Paging area	Site ID	Status
☑	00:30:42:0D:97:1A	R451P31a03054	1	0	1	✓
☐	00:30:42:0D:95:D8	R439 SWT 31A-0-...	1	0	1	✖
☐	00:30:42:0C:BD:7B	R440 P31a-03-07-4	1	0	3	✖
☐	00:30:42:0D:95:CE	Patchschrank Kue...	1	0	3	✖
☐	00:30:42:0D:95:CC	R414 OpenMob lab	2	0	3	✖
☐	00:30:42:0D:95:CA	R414 OpenMob lab	2	0	3	✖
☐	00:30:42:0C:BD:DD	R403 System test ...	2	0	3	✖
☐	00:30:42:0D:95:DB	R451 P31a-4-2-15-8	1	0	1	✖
☐	00:30:42:0D:95:D9	R439 P31a-4-2-12...	1	0	3	✖
☐	00:30:42:0D:95:D6	R447 P31a-4-2-13...	1	0	3	✖
☐	00:30:42:0D:95:E7	R447 P31a-4-2-14...	1	0	1	✖
☐	00:30:42:0D:22:5A	R433 P31a-4-2-11...	1	0	3	✖

Radio fixed part MAC address: 00:30:42:0D:97:1A

Enrolment status ✓ OK

Info console

```
2012/02/18 13:48:37.568 20 RFP datasets imported
```

1 Press the **File** button.

A file system dialog opens in which you can select the configuration file.

2 To check the results from reading the configuration file press the **Show log file** button. In case of file format errors these errors are listed here.

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

✖ – Not enrolled yet

❌ – Enrolment failed

✓ – OK (Enrolment successful)

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

Add all: import all RFP datasets into the OMM.

Add selected: import selected RFP datasets to the OMM. For selection activate the corresponding checkboxes in the RFP table.

Remove all: remove all RFP datasets from table. The table will be hidden.

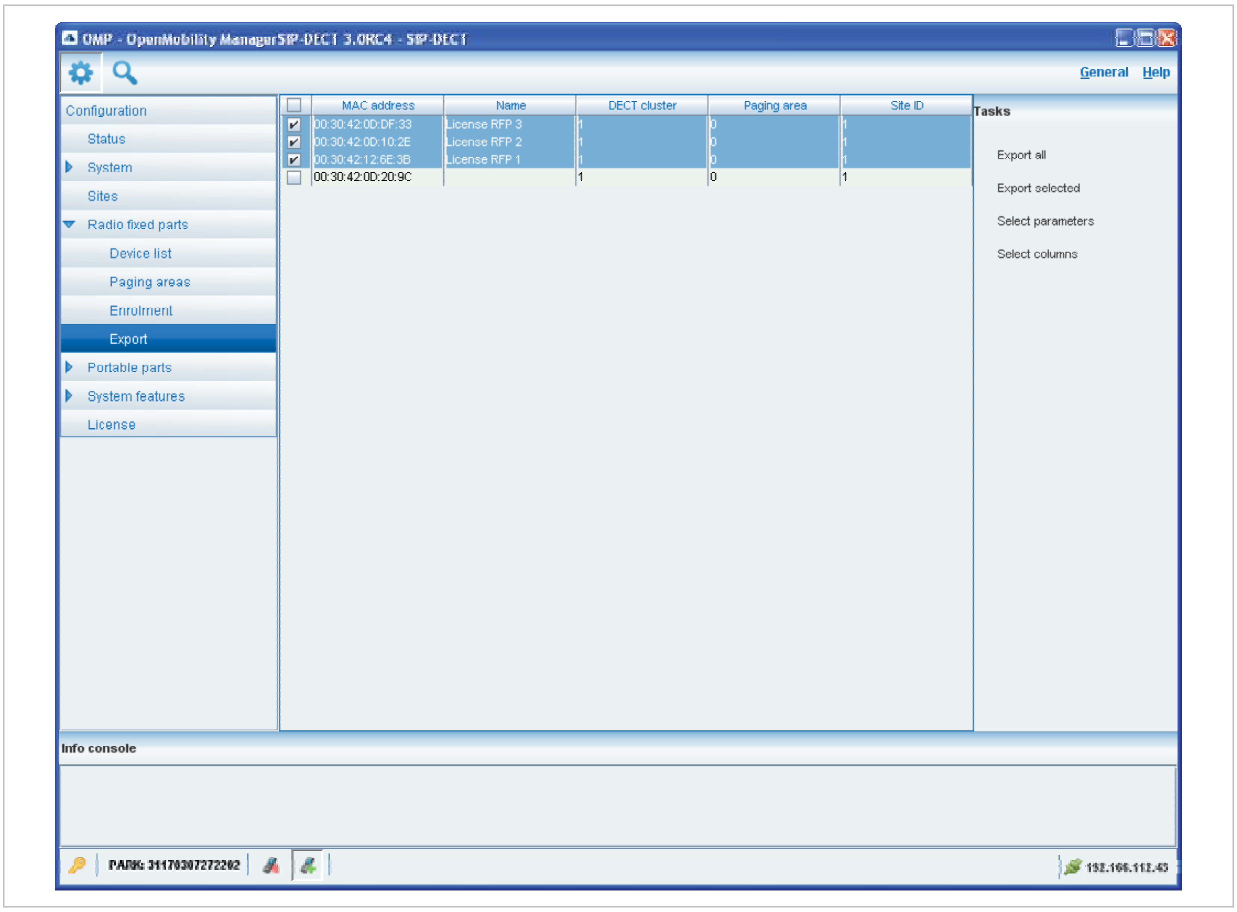
Remove selected: remove selected RFP datasets from table. If the table is empty after removing of datasets, the table will be hidden. For selection activate the corresponding checkboxes in the RFP table.

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

8.7.4 “Export” Menu

The **Export** menu allows export of all RFPs enrolled to the OMM into an file using “*.csv” file format. The created file can be viewed externally with a standard spreadsheet application.

All enrolled RFPs are shown in a table.



□	MAC address	Name	DECT cluster	Paging area	Site ID
☑	00:30:42:0D:DF:33	License RFP 3	1	0	1
☑	00:30:42:0D:10:2E	License RFP 2	1	0	1
☑	00:30:42:12:6E:3B	License RFP 1	1	0	1
□	00:30:42:0D:20:9C		1	0	1

The following tasks can be performed:

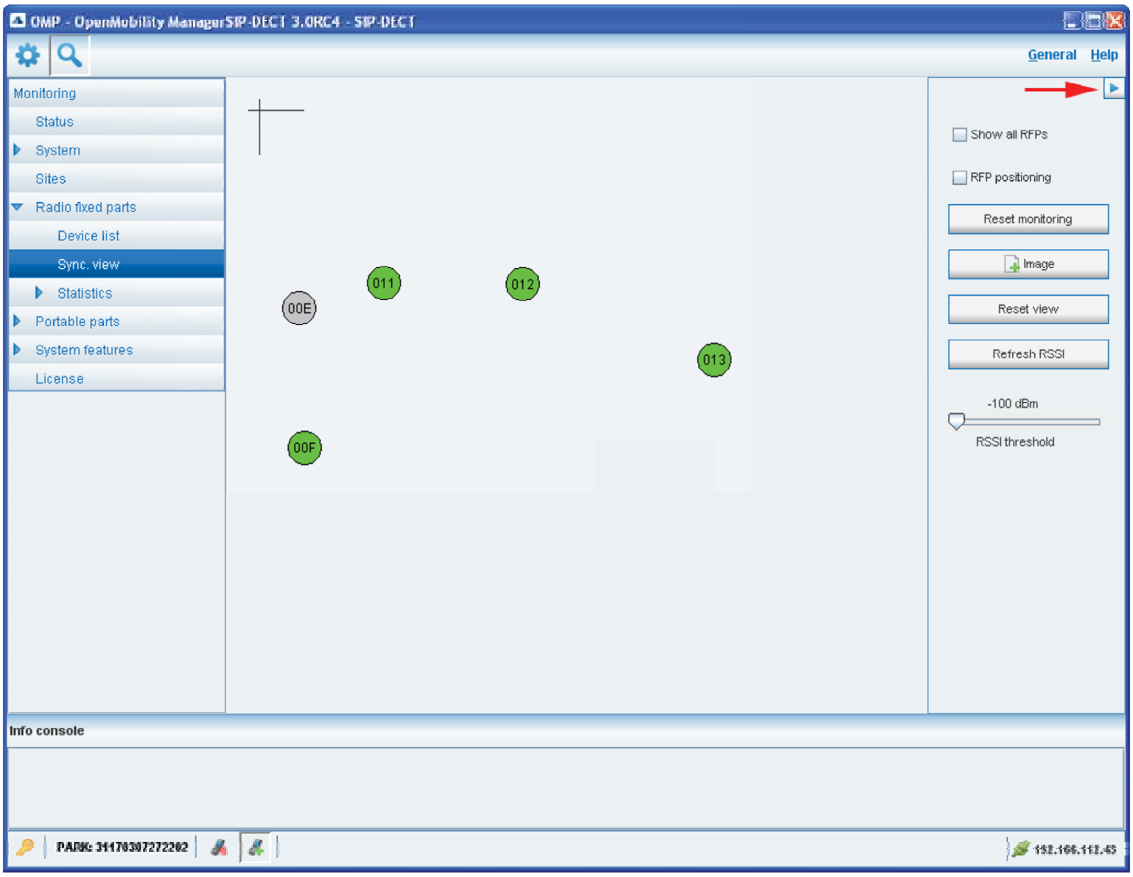
- **Export all**: export all RFP datasets.
- **Export selected**: export selected RFP datasets.
- **Select parameters**: select RFP parameters which shall be written to csv file (select all RFP parameters or a subset of these parameters).
- **Select columns**: select the columns thst shall be written to the csv file.

When the export is started, a file system dialog will be opened and the export file name can be selected. If all parameters are selected for export, the export file can be re-imported using Enrolment (see chapter 8.7.3). For information about RFP export file format see Appendix, chapter 11.8).

8.7.5 "Sync view" Menu

The Sync view menu allows to check the synchronization relations between RFPs in a graphical manner.

Note: For background information on RFP synchronization please refer to chapter 9.2.



To open the task panel for sync view press the arrow icon in the upper right corner of the sync view panel.

The task panel is displayed on the right. The following tasks can be performed:

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

Viewing sync relations

RFPs for which sync relations shall be shown, can be selected as follows:

- Select (more than one) RFP in device list table (see chapter 8.7.1)

  or

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

The color of the RFP icon indicates synchronization state of that RFP:

- Grey: inactive
- Red: not synchronized
- Yellow: searching
- Green: synchronized

Sync relations between RFPs are represented by arrows.

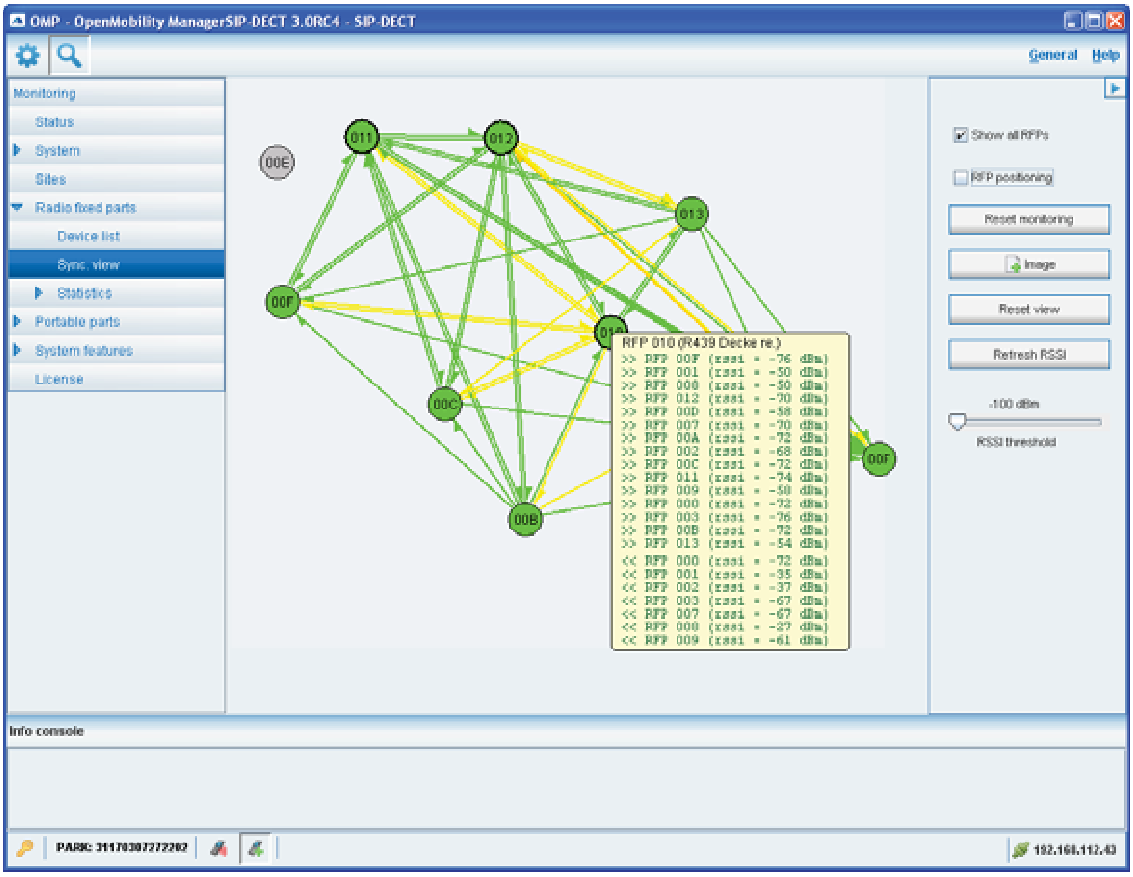
Viewing RSSI values

The color of the arrows between RFPs is an indication of the RSSI value of the link:

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

If the mouse is moved over an RFP with monitoring activated, a tool tip with RSSI values will be opened.

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



☑ Show all RFPs

☐ RFP positioning

-100 dBm

```
RFP 010 (R439 Decke re.)
>> RFP 00F (rssi = -76 dBm)
>> RFP 001 (rssi = -50 dBm)
>> RFP 000 (rssi = -50 dBm)
>> RFP 012 (rssi = -70 dBm)
>> RFP 00D (rssi = -58 dBm)
>> RFP 007 (rssi = -70 dBm)
>> RFP 00A (rssi = -72 dBm)
>> RFP 002 (rssi = -68 dBm)
>> RFP 00C (rssi = -72 dBm)
>> RFP 011 (rssi = -74 dBm)
>> RFP 009 (rssi = -50 dBm)
>> RFP 000 (rssi = -72 dBm)
>> RFP 003 (rssi = -76 dBm)
>> RFP 00B (rssi = -72 dBm)
>> RFP 013 (rssi = -54 dBm)
<< RFP 000 (rssi = -72 dBm)
<< RFP 001 (rssi = -35 dBm)
<< RFP 002 (rssi = -37 dBm)
<< RFP 003 (rssi = -67 dBm)
<< RFP 007 (rssi = -67 dBm)
<< RFP 000 (rssi = -27 dBm)
<< RFP 009 (rssi = -61 dBm)
```

8.7.6 “Statistics” Menu

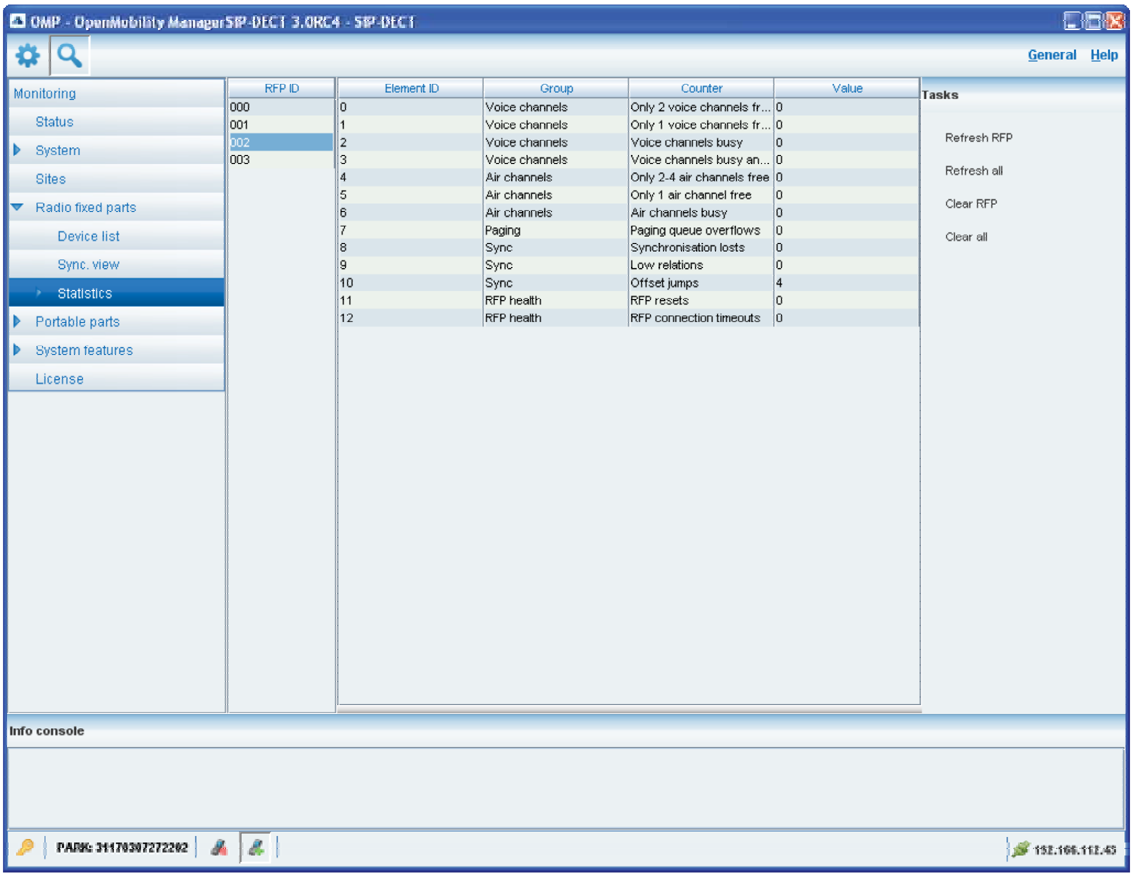
The **Radio fixed parts** > **Statistics** menu provides information about RFP statistics counters. It contains:

- an overview panel with all statistics counters (see chapter 8.7.6.1) and
- several statistics group panels. In these groups statistics counter types which are related are pooled together (see chapter 8.7.6.2).

The menu is only available in **monitor mode**.

8.7.6.1 RFP Statistics Overview

The RFP statistics overview consists of two tables, left RFP ID table and right an overview of all RFP statistics counters.



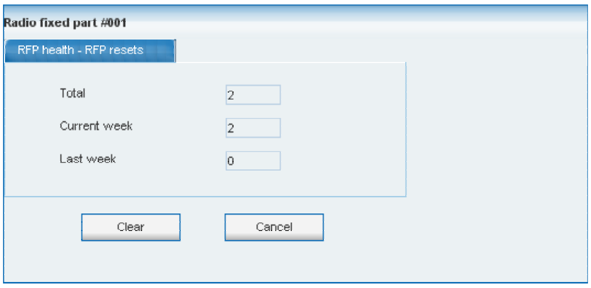
RFP ID
000
001
002
003

Element ID	Group	Counter	Value
0	Voice channels	Only 2 voice channels fr...	0
1	Voice channels	Only 1 voice channels fr...	0
2	Voice channels	Voice channels busy	0
3	Voice channels	Voice channels busy an...	0
4	Air channels	Only 2-4 air channels free	0
5	Air channels	Only 1 air channel free	0
6	Air channels	Air channels busy	0
7	Paging	Paging queue overflows	0
8	Sync	Synchronisation losts	0
9	Sync	Low relations	0
10	Sync	Offset jumps	4
11	RFP health	RFP resets	0
12	RFP health	RFP connection timeouts	0

The following tasks can be performed:

- **Refresh RFP**: request counter update by OMM for selected RFPs statistics counters.
- **Refresh all**: request counter update by OMM for all RFP statistics counters.
- **Clear RFP**: clear all RFP statistics counters on selected RFP.
- **Clear all**: clear all RFP statistics counters.

If an RFP is selected (left **RFP ID** table), the statistics counter table shows counter values of that RFP (right table). By selecting a statistics counter entry, a detail panel is opened which shows more detailed information of that counter.



Radio fixed part #001

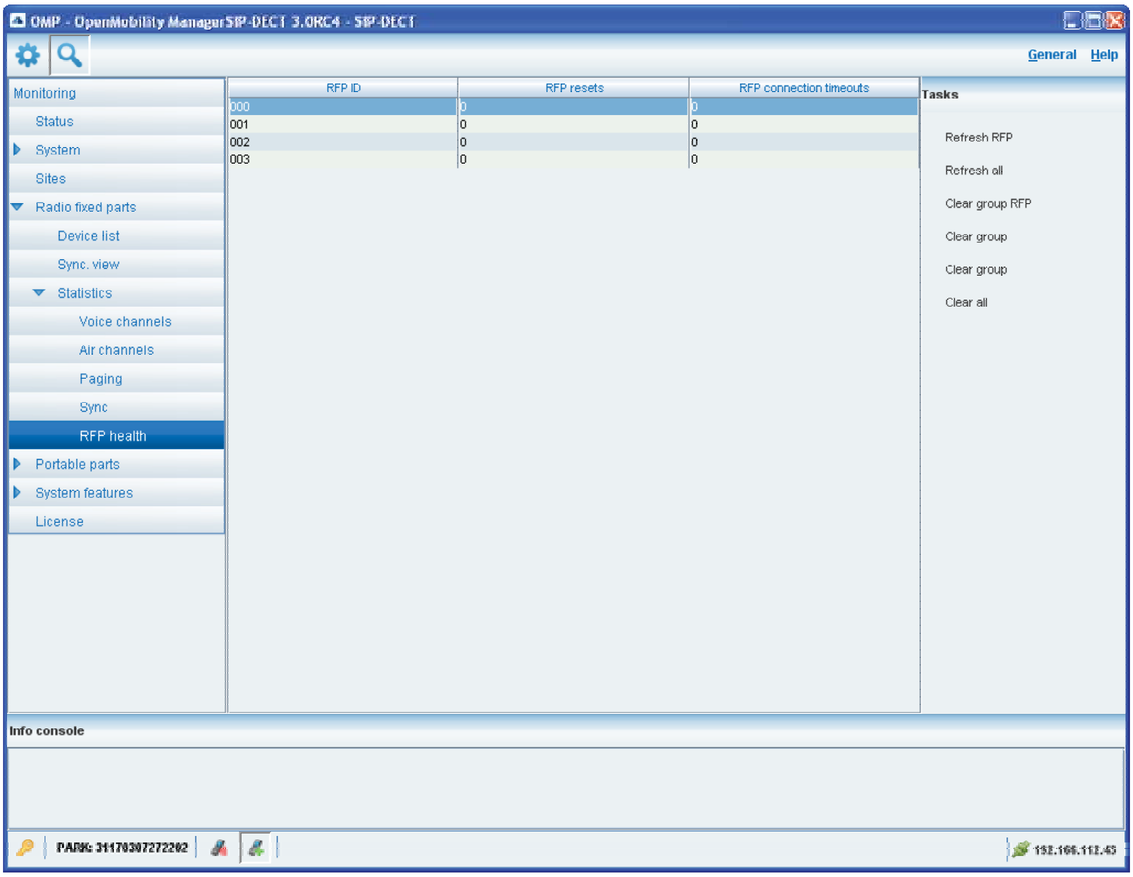
RFP health - RFP resets

Total	2
Current week	2
Last week	0

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

8.7.6.2 RFP Statistics Group Panels

The RFP statistics group panels divide RFP statistics counters into logical groups. This allows to view all statistics counters of a special group of all RFPs in one table.



OMP - OpenMobility ManagerSIP-DECT 3.0RC4 - SIP-DECT

RFP ID	RFP resets	RFP connection timeouts
000	0	0
001	0	0
002	0	0
003	0	0

The following tasks can be performed:

- **Refresh RFP**: request counter update by OMM for selected RFP.
- **Refresh all**: request counter update by OMM for all counters.
- **Clear group RFP**: clear counter group of selected RFP.
- **Clear group**: clear counter group of all RFPs.

- **Clear RFP**: clear all counters of selected RFP.<Anmerkung von Commando an Aastra: In der SW-Version 3.0RC4 ist dieser String offenbar fälschlich (?) geändert worden zu **Clear group**, String wäre dann doppelt, siehe Screenshot → Bug?
- **Clear all**: clear all counters of all RFPs.

8.8 “Portable parts” Menu

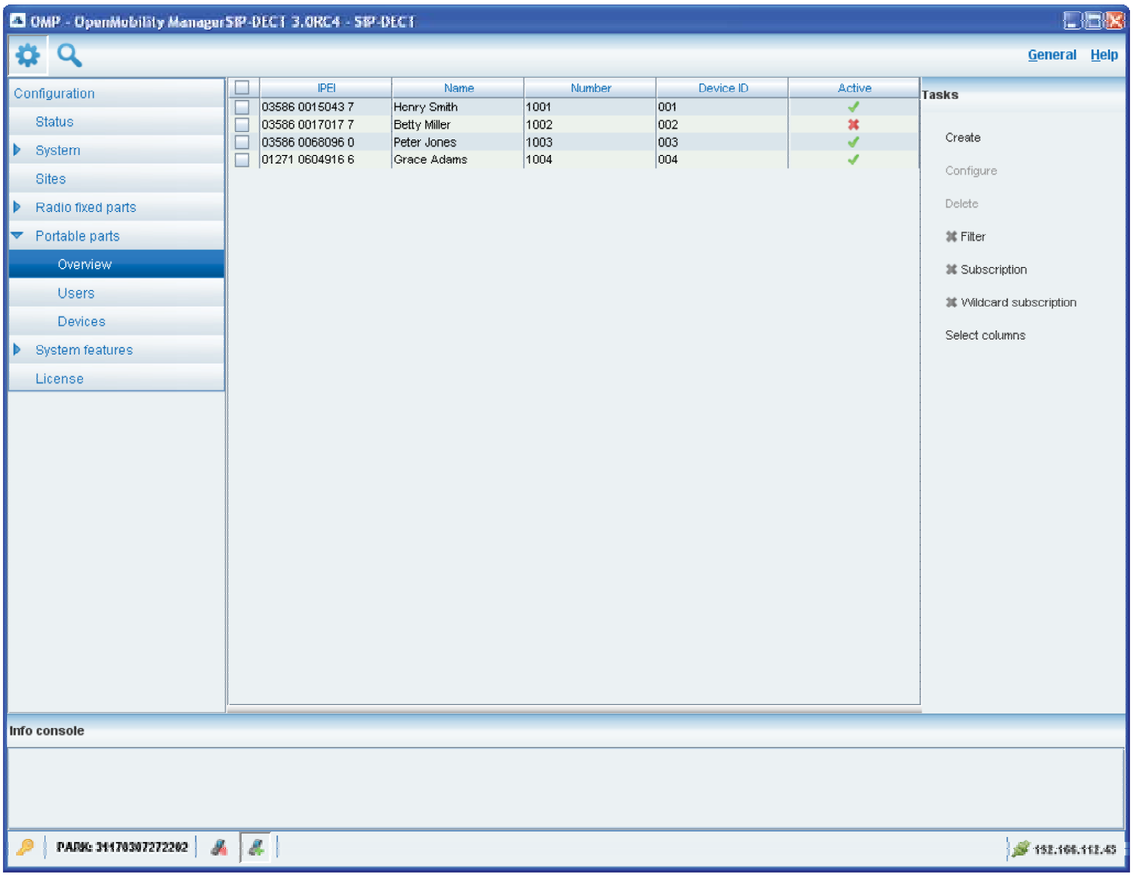
Portable parts datasets can be configured and viewed in the **Portable parts** menu. The **Portable parts** menu provides the different submenus. Each submenu displays an own table of PP datasets.

Configuration mode	Monitor mode	See chapter
Overview: displays the table of all PP data, user and device related	Overview: displays the table of all PP data, user and device related	8.8.1
Users: displays the table of all PP user data		8.8.2
Devices: displays the table of all PP device data		8.8.3

8.8.1 Overview” Menu

In the **Overview** panel, all PPs data are listed in a table, user related as well as device related. The overview is available in **configuration mode** as well as in **monitor mode**.

In **configuration mode**, the **Overview** panel allows to create **fixed** PPs (user and device are permanently associated).



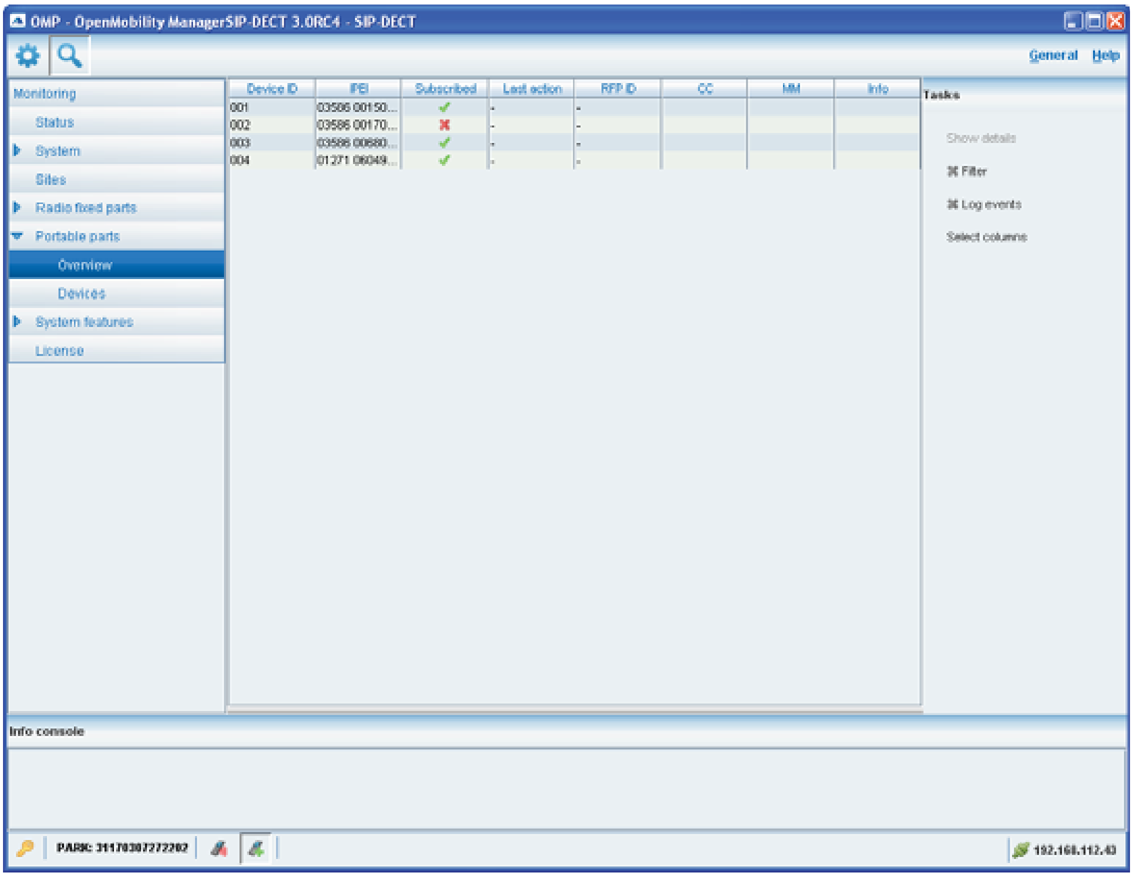
□	IPEI	Name	Number	Device ID	Active
□	03586 0015043 7	Henry Smith	1001	001	✓
□	03586 0017017 7	Betty Miller	1002	002	✗
□	03586 0068096 0	Peter Jones	1003	003	✓
□	01271 0604916 6	Grace Adams	1004	004	✓

PP overview in configuration mode

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

- ✗ - PP is not subscribed to the system.
- ✓ - PP is subscribed to the system.

Note: If the **Active** column is not displayed, you can activate it in the **Select columns** dialog, see chapter 8.8.9.
To view the user-device-relation, ensure that the **User ID** and **Device ID** columns are also activated.



Device ID	IPEI	Subscribed	Last action	RFP ID	CC	MM	Info
001	03586 00150...	✓	-	-			
002	03586 00170...	✗	-	-			
003	03586 00680...	✓	-	-			
004	01271 06049...	✓	-	-			

PP overview in monitor mode

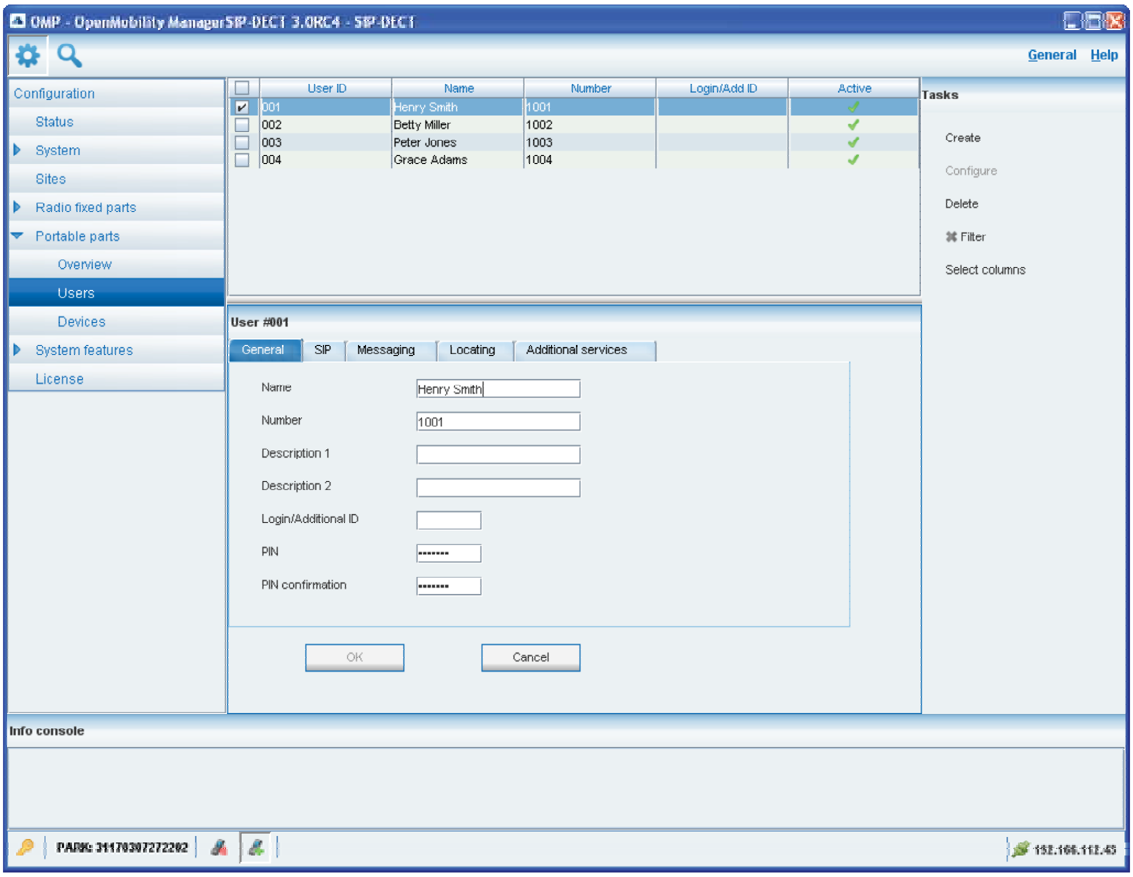
The tasks which can be performed are mode-dependant.

Configuration mode	Monitor mode	See chapter
Create: create new fixed PP dataset in detail panel		8.8.5
Configure: configure selected PP user and device dataset in detail panel		8.8.6
	Show details: show selected PP user and device dataset in detail panel	8.8.4
Delete: delete selected PP user and device dataset (in case of fixed relation) or delete PP user and set device to unbound status (in case of dynamic relation)		8.8.8
Subscription: start PP subscription		8.8.7
Wildcard subscription: start PP wildcard subscription		8.8.7
Select columns: select columns/parameters to be shown in PP table	**Select columns**: select columns/parameters to be shown in PP table	8.8.9
Filter: show only PP datasets in	**Filter**: show only PP datasets in	8.8.10

table which contain a special search string	table which contain a special search string	
	Log events: enable/disable PP event log	8.8.11

8.8.2 "Users" Menu

In the **Users** panel, all PP user data are listed in a table. The **Users** panel allows to create (unbound) users (which should be able to login and logout at a device).



☐	User ID	Name	Number	Login/Add ID	Active
☑	001	Henry Smith	1001		✓
☐	002	Betty Miller	1002		✓
☐	003	Peter Jones	1003		✓
☐	004	Grace Adams	1004		✓

User #001

Name	Henry Smith
Number	1001
Description 1	
Description 2	
Login/Additional ID	
PIN	•••••••
PIN confirmation	•••••••

Note: Use the **Select columns** dialog (see chapter 8.8.9) to display the desired PP user data.

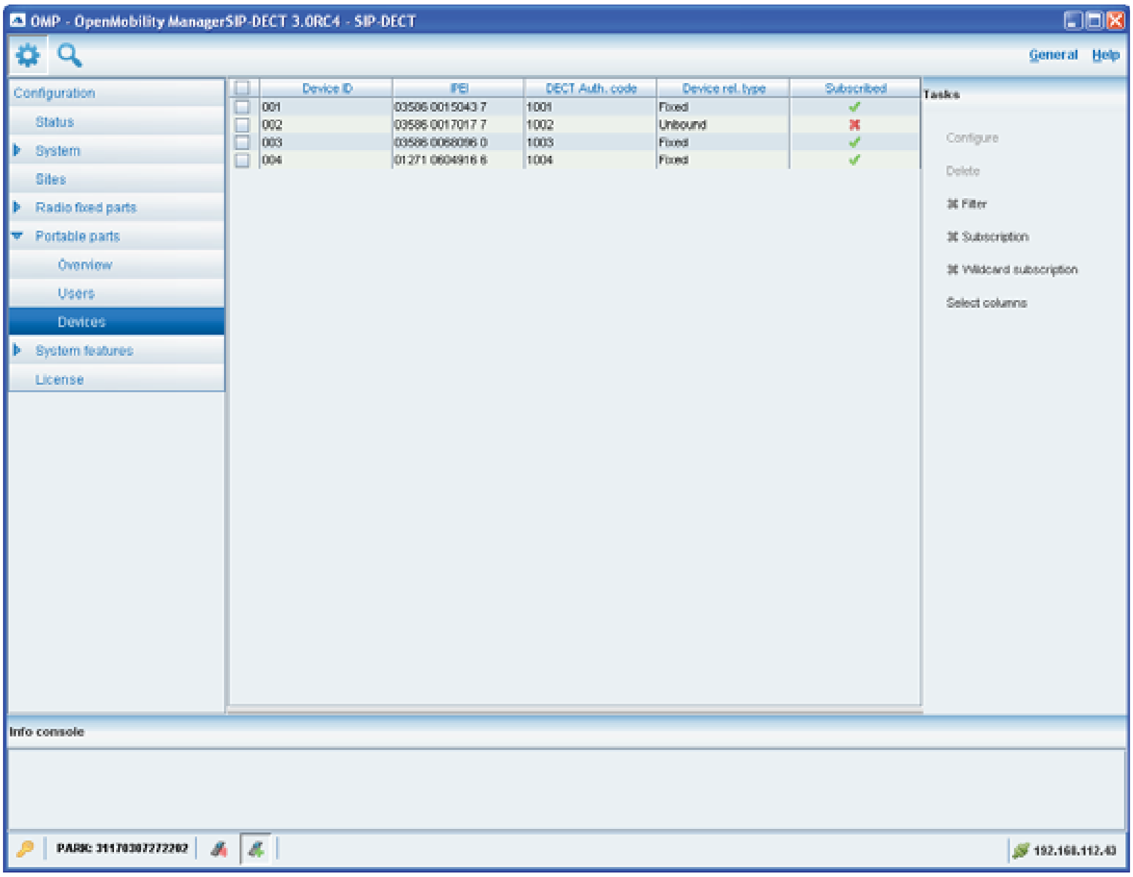
The following tasks can be performed:

- **Create**: create new unbound PP user dataset (see chapter 8.8.5).
- **Configure**: configure selected PP user dataset (see chapter 8.8.6).
- **Delete**: delete selected PP user dataset and user data in case of fixed relation (see chapter 8.8.8).
- **Select columns**: select parameter columns to be shown in table (see chapter 8.8.9).
- **Filter**: filter PP datasets shown in table for string set in filter mask (see chapter 8.8.10).

8.8.3 “Devices” Menu

In the **Devices** panel, all PP device data are listed in a table. The **Device** panel allows to configure the DECT part of a PP device dataset.

Devices can not be created separately. They will be automatically created during subscription (unbound) or they will be created fixed bound to a user when a user is created in the **Overview** submenu (see chapter 8.8.1).



□	Device ID	IPEI	DECT Auth. code	Device rel. type	Subscribed
□	001	03586 0015043 7	1001	Fixed	✓
□	002	03586 0017017 7	1002	Unbound	✗
□	003	03586 0068096 0	1003	Fixed	✓
□	004	01271 0604916 6	1004	Fixed	✓

Note: Use the **Select columns** dialog (see chapter 8.8.9) to display the desired PP device data.

The following tasks can be performed:

- **Configure**: configure selected PP device dataset (see chapter 8.8.6).
- **Delete**: delete selected PP device dataset (see chapter 8.8.8).
- **Subscription**: start PP subscription (see chapter 8.8.7).
- **Wildcard subscription**: start PP wildcard subscription (see chapter 8.8.7).
- **Select columns**: select parameter columns to be shown in table (see chapter 8.8.9).
- **Filter**: filter PP datasets shown in table for string set in filter mask (see chapter 8.8.10).

8.8.4 PP Detail Panel

The PP detail panel is used for configuration/showing of PP settings and creation of new PP datasets.

To call up the PP detail panel

- choose one of the commands in the task bar on the right of the **Portable parts** panel (**Create**, **Configure**, or **Show details**)

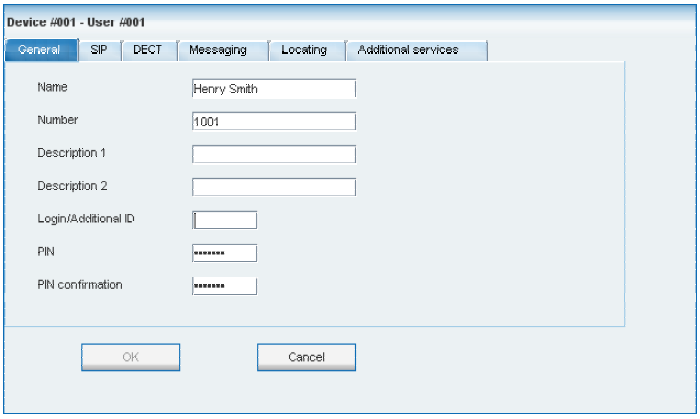
  or
- select the appropriate PP in the PP table and double-click the entry.

The PP detail panel contains the different parameter groups sorted in tabs. Which tabs are displayed depends on the current mode and from which panel the PP detail panel was called up:

- **Overview** panel (configuration and monitor mode): The PP detail panel contains all tabs listed below.
- **User** panel (configuration mode): The PP detail panel contains all tabs but not **DECT**.
- **Device** panel (configuration mode): The PP detail panel contains only **DECT**.

"General" tab

This tab enables to configure the general settings for the PP dataset.



Name: Henry Smith
Number: 1001
Description 1:
Description 2:
Login/Additional ID:
PIN: •••••••
PIN confirmation: •••••••

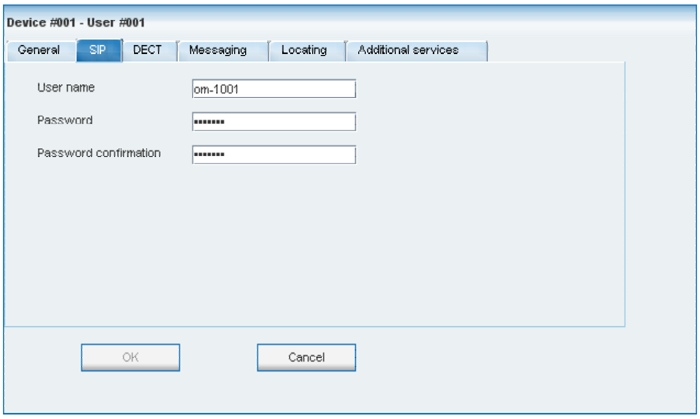
- **Name**: represents the handset user name with up to 20 characters
- **Number**: the handset telephone number with up to 31 characters (1234567890*#azAz+-_.!$%&/()=?$&). Please be aware that only "*","#" and "0" to "9" can be dialled with a handset.
- **Description 1** and **Description 2**: free text comments with up to16 characters each.
- **Login/Additional ID**: The additional ID can be used as a mean for data search within wildcard subscription (because of the IPEI is not configured which selects the data otherwise).

Note: The authentication code and additional ID can only be changed if the PP is not subscribed.

- **PIN**, **PIN confirmation**: a user PIN to be entered during user login.

"SIP" tab

This tab enables to configure the SIP authentication for the PP dataset.



Device #001 - User #001

User name: om-1001

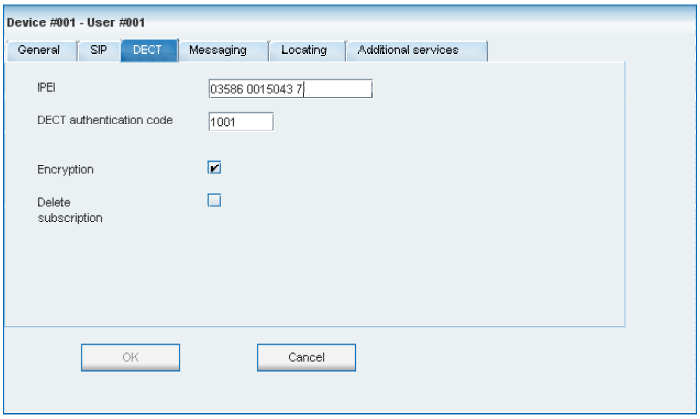
Password: •••••••

Password confirmation: •••••••

- **User name**: The SIP Authentication user name is optional but recommended. It represents the name which will be used during SIP registration and authentication. If no name is given the number will be used by default.
- **Password**, **Password confirmation**: The password will be used during SIP registration and authentication. Enter the appropriate data in these fields.

“DECT” tab

This tab enables to configure the DECT part for the PP dataset. When configuring a device (see 8.8.3), only the **DECT** tab is shown in the PP detail panel.



Device #001 - User #001

IPEI: 03586 0015043 7

DECT authentication code: 1001

Encryption ☑

Delete subscription □

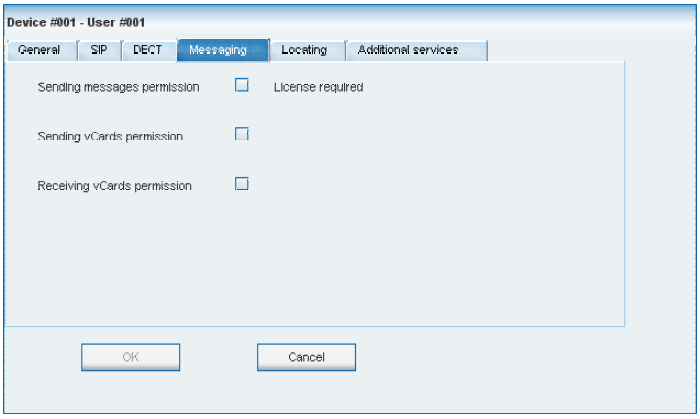
- **IPEI**: The IPEI is the DECT 142 / 600d / 650c handset IPEI number which can be found in the **System Options** menu of the DECT 142 / 600d / 650c handset.
- **DECT authentication code**: The DECT authentication code is used during initial DECT subscription as an security option and can be set here for each PP device separately. If a global DECT authentication code is given on the **System settings** page (see chapter 8.5.1), this value is filled in here as default. This parameter is optional.
- **Encryption**: If the encryption feature is enabled for the whole system (in the **System settings** menu, see chapter 8.5.1), you can de-activate the DECT encryption for this device.

Please note: The PP device has to support DECT encryption which is not a mandatory feature.

- **Delete subscription**: This option is only available when configuring an existing PP. If this option is activated, the subscription data will be deleted which also requires a re-subscription of the handset device.

“Messaging” tab

This tab enables to configure the OM Integrated Messaging and Alerting service for the PP dataset.



Device #001 - User #001

Sending messages permission □ License required

Sending vCards permission □

Receiving vCards permission □

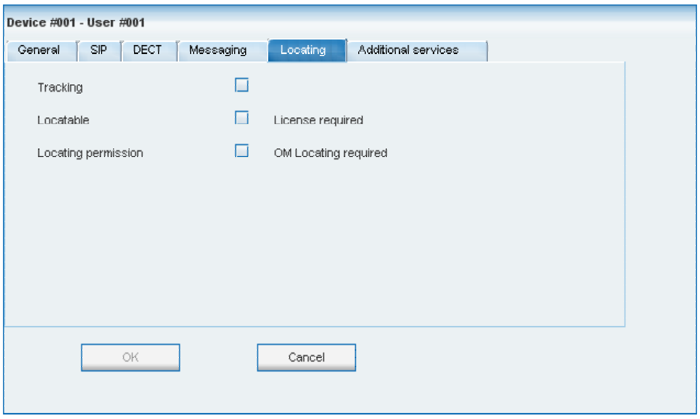
- **Sending messages permission**: If this option is enabled, the PP can send messages (if this function is supported by the device).

Note: For further information please refer to the separate document SIP–DECT; OM Integrated Messaging & Alerting Application; Installation, Administration & User Guide.

- **Sending vCards permission**: Allows the user to send personal directory entries as a vCard message from the handset to other users (if this function is supported by the device).
- **Receiving vCards permission**: If this option is enabled, all received vCard messages are automatically processed and written into the personal directory of the handset (if this function is supported by the device).

“Locating” tab

This tab enables to configure the OM Locating Application for the PP dataset.



Device #001 - User #001

Tracking □

Locatable □ License required

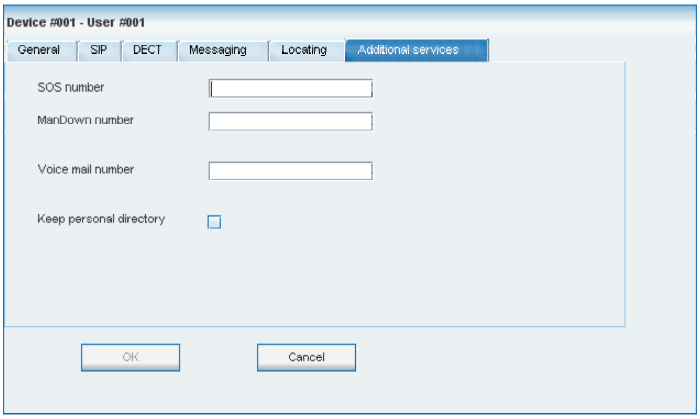
Locating permission □ OM Locating required

- **Tracking**: If this option is enabled, the operator of the OM Locating application is able to use the constant tracking feature for the portable part. Note, that this feature consumes more of the portable part's battery power, because it activates an RFP update information if the device roams and is not in communication. You also cannot enable this feature, if the **Locatable** option is disabled.
- **Locatable**: If this option is enabled, the portable part is locatable. Either with the OM Locating application or by querying it's location from other portable parts.
- **Locating permission**: This option applies to Aastra 610d/620d/630d/650c handsets only. If this option is enabled, the portable part is able to determine the location of other portable parts. The main menu of the Aastra 610d/620d/630d/650c phones provides an extra menu entry **Locating** for this.

Note: For further information please refer to the separate document SIP–DECT; OM Locating Application; Installation, Administration & User Guide.

"Additional services" tab

This tab enables to configure extra configuration items for the PP dataset.



- **SOS number**: User specific SOS number that is dialled automatically if the SOS key on the handset is pressed.
- **ManDown number**: User specific "Man down" number that is dialed automatically if a Man down event happens. This event is triggered by the sensor of an Aastra630d handset.

  If no individual SOS or Man down number is configured for a handset, the number of the appropriate alarm trigger will be used as calling number in case of a SOS or Man down event. Please see chapter 8.9.3 and /28/ for details.
- **Voice mail number**: The voice mail number is the number which will be automatically called as soon as a voice mail call is initiated on the Aastra 600d / Aastra 650c handset. If there is no individual voice mail number configured in this field, then the system wide voice mail number is used (see also the **System setting** menu, chapter 8.5.1). If there is no voice mail number configured (neither the individual nor the system wide) or another handset type is used, then the voice mail number must be configured locally in the handset.
- **Keep personal directory**: Activate this option, to keep the personal directory data in the handset if the user logs out.

8.8.5 Creating PP Datasets

Creating PP datasets is only possible in **configuration mode**. You can create the fixed PP dataset or only the PP user data.

To create a PP dataset proceed as follows:

1. In the task bar on the right of the **Portable parts** panel click on the **Create** command.

   – In the **Overview** submenu you can now create a fixed PP dataset (with combined user and device data).

   – In the **Users** submenu you can create an unbound user. This user can login and logout at any prepared device.

   The PP detail panel opens. It provides various tabs where the PP data has to be entered.

2. Configure the PP, see parameter description in chapter 8.8.4.

3. Press the **OK** button.

8.8.6 Configuring PP Datasets

Configuring PP datasets is only possible in **configuration mode**. To configure an existing PP dataset proceed as follows:

1. In the task bar on the right of the **Portable parts** panel click on the **Configure** command.

   – In the **Overview** submenu you can configure the whole PP dataset (user and device data).

   – In the **Users** submenu you can configure the PP user data.

   – In the **Device** submenu you can configure the PP device data.

   The PP detail panel opens.

2. Change the PP dataset as desired, see parameter description in chapter 8.8.4.

3. Press the **OK** button.

8.8.7 Subscribing PP Datasets

After adding a PP dataset to the OMM, the PP must be subscribed. The OMM must first be enabled to allow subscriptions to be take place from PP handsets. Subscribing PP datasets is possible in the **Overview** panel and in the **Device** panel. To start subscription, press one of the following commands in the **Portable parts** menu:

- **Subscription**: start PP subscription with configured IPEI. For more information on this see chapter 7.7.3.1.
- **Wildcard subscription**: start PP wildcard subscription (without configured IPEI). In the **Wildcard subscription** dialog, which is now opened, enter the **Timeout** for this subscription method. Press the **Start** button. For more information on this see chapter 7.7.3.2.

8.8.8 Deleting PP Datasets

Deleting PP datasets is only possible in **configuration mode**. You can delete the fixed PP dataset (in case of fixed relation) or only the PP user data resp. the PP device data (in case of dynamic relation).

To delete one or more existing PP datasets proceed as follows:

1 Select the appropriate PP dataset(s) in the PP table by activating the corresponding checkbox(es).

2 In the task bar on the right of the **Portable parts** panel click on the **Delete** command.

– In the **Overview** submenu the whole PP dataset will be deleted.

– In the **Users** submenu only the PP user data will be deleted.

– In the **Devices** submenu only the PP device data will be deleted.

The **Delete [xxx]** dialog opens showing a confirmation prompt.

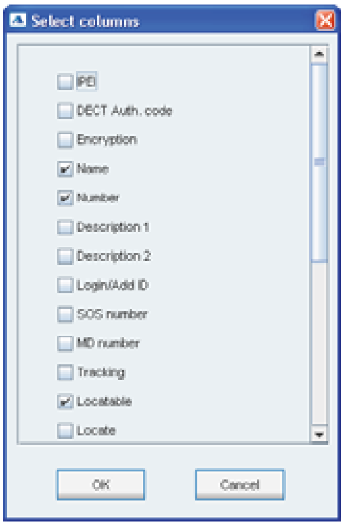
3 Confirm the displayed prompt with **OK**.

8.8.9 Selecting Columns

You can adapt the parameters shown in the PP table to your needs:

1 In the task bar on the right of the **Portable parts** panel click on the **Select columns** command.

The **Select columns** dialog opens.



☐ IPEI
☐ DECT Auth. code
☐ Encryption
☑ Name
☑ Number
☐ Description 1
☐ Description 2
☐ Login/Add ID
☐ SOS number
☐ MD number
☐ Tracking
☑ Locatable
☐ Locate

2 Select the columns that shall be shown by activating the appropriate checkboxes.

3 Click the **OK** button.

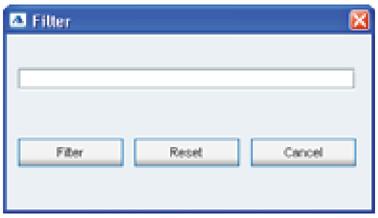
The PP table will be adapted accordingly.

8.8.10 Filtering PP Table

You can filter the list of PP datasets shown in the PP table by using a filter.

1 In the task bar on the right of the **Portable parts** panel click on the **Filter** command.

The **Filter** dialog opens.



2 Enter the search string that serves as filter criterion. You can enter digits and characters. The search is case sensitive.

3 Click on the **Filter** button.

The **Filter** dialog is closed and the PP table will be adapted accordingly.

4 To reset the filter, click on the **Filter** command in the task bar on the right of the **Portable parts** panel.

5 In the **Filter** dialog click on the **Reset** button.

8.8.11 Enabling / Disabling PP Event Log

You can store an PP event log file in **monitor mode**. Proceed as follows:

1 To enable/disable the PP event log, click on the **Log events** command in the task bar on the right of the **Portable parts** panel:

✓ - PP event log is enabled.

✗ - PP event log is disabled.

2 Repeat step 1 to disable/enable the PP event log.

The PP event log will be stored in a file called “pp_event.log“. This file can be found in the users home directory:

- on a Linux it is located under ‘~/.oamp’,
- on a windows system under ‘c:/Users/<user>/MyDocuments/.Oamp’.

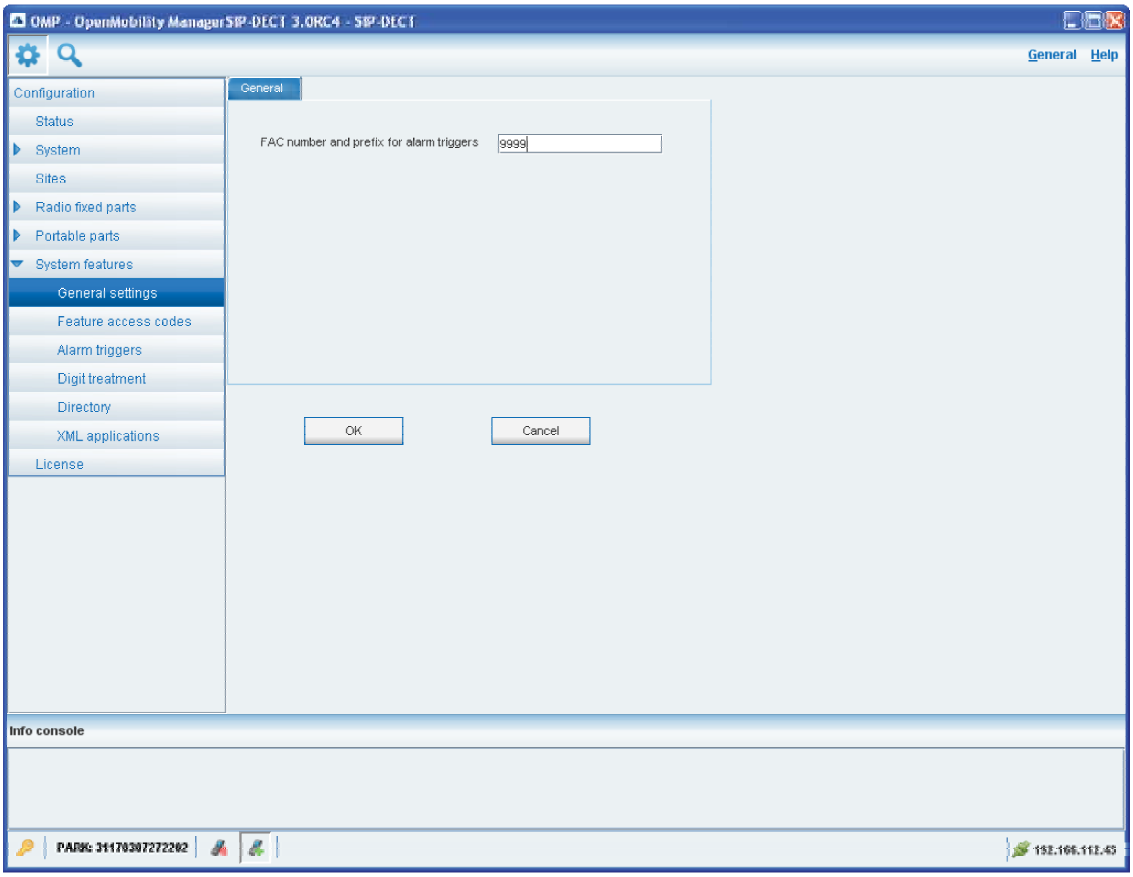
8.9 “System features” Menu

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

Configuration mode	Monitor mode	See chapter
General settings	General settings	8.9.1
Feature access codes (FAC)	Feature access codes (FAC)	8.9.2
Alarm triggers	Alarm triggers	8.9.3
Digit treatment	Digit treatment	8.9.4
Directory	Directory	8.9.5
XML applications	XML applications	8.9.6

8.9.1 “General settings” Menu

The **General settings** menu allows to configure/view the FAC number prefix used for feature access codes and alarm triggers.



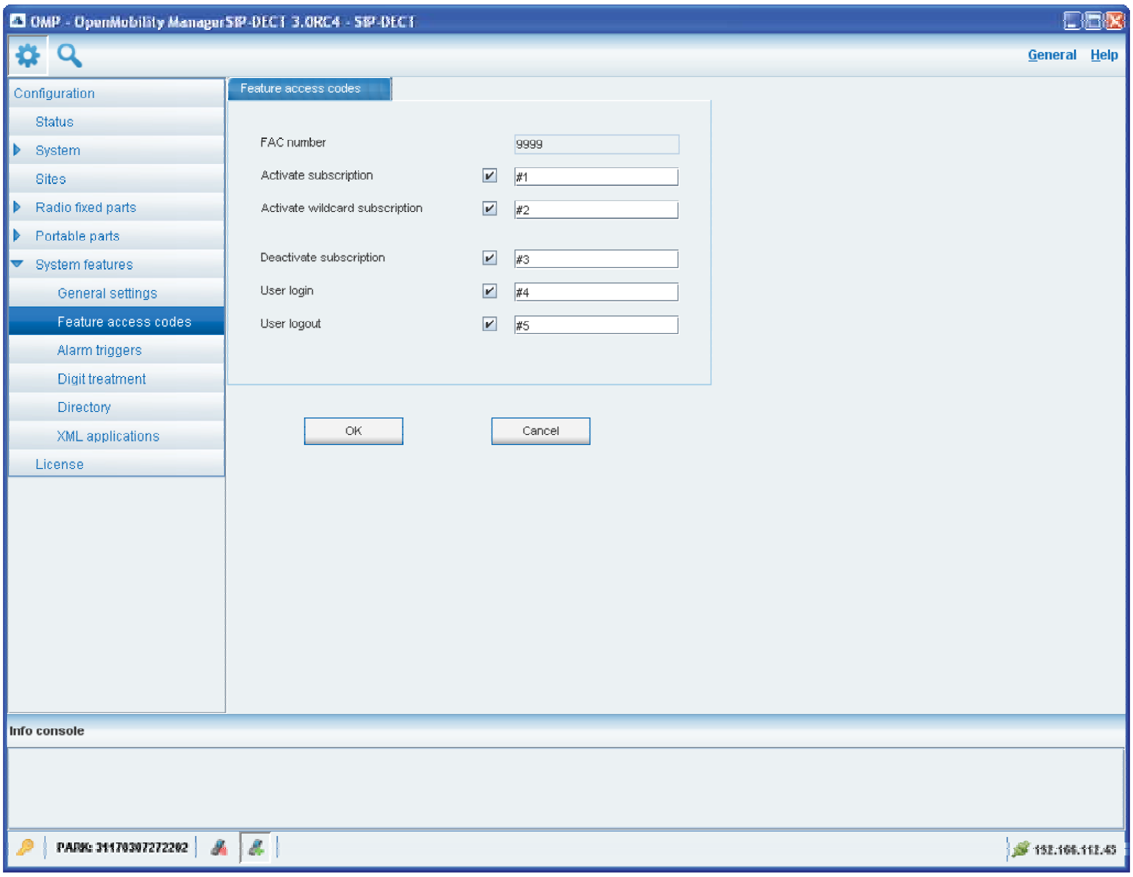
FAC number and prefix for alarm triggers: 9999

1 **FAC number and prefix for alarm triggers**: Enter a unique FAC number.

2 Press the **OK** button.

8.9.2 “Feature access codes” Menu

The **Feature access codes** menu is used to configure/view the feature access codes parameters.



FAC number: 9999

Activate subscription ☑ #1

Activate wildcard subscription ☑ #2

Deactivate subscription ☑ #3

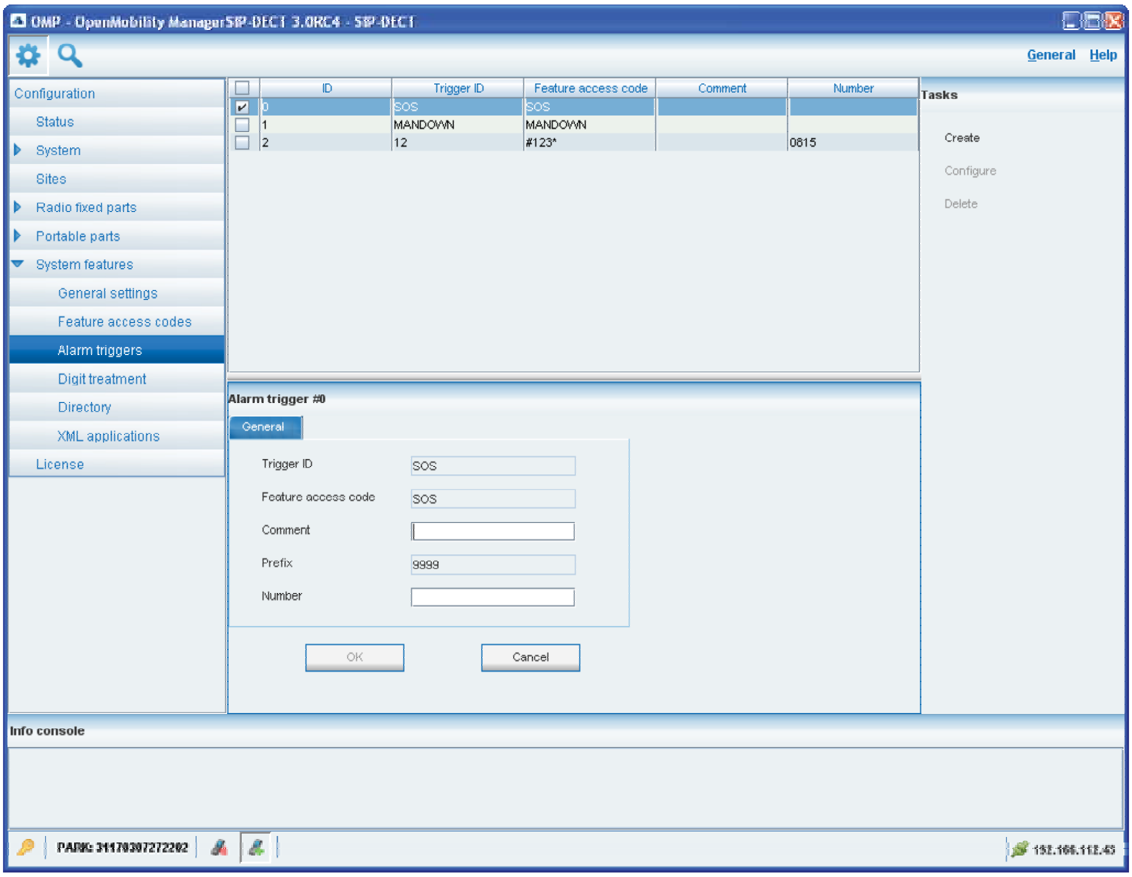
User login ☑ #4

User logout ☑ #5

The **FAC number** which introduces the feature access code (see also chapter 8.9.1) is displayed. For a description of the parameters which can be set in this menu see chapter 7.9.3.

8.9.3 “Alarm triggers” Menu

The **Alarm triggers** menu allows to configure/view numerous alarm trigger datasets. There are two predefined alarm triggers (‘SOS and ’Man down‘) which can not be deleted.



OMP - OpenMobility ManagerSIP-DECT 3.0RC4 - SIP-DECT

	ID	Trigger ID	Feature access code	Comment	Number
☑	0	SOS	SOS		
□	1	MANDOWN	MANDOWN		
□	2	12	#123*		0815

Alarm trigger #0

General

Trigger ID	SOS
Feature access code	SOS
Comment	
Prefix	9999
Number	

PARK: 31170307272202

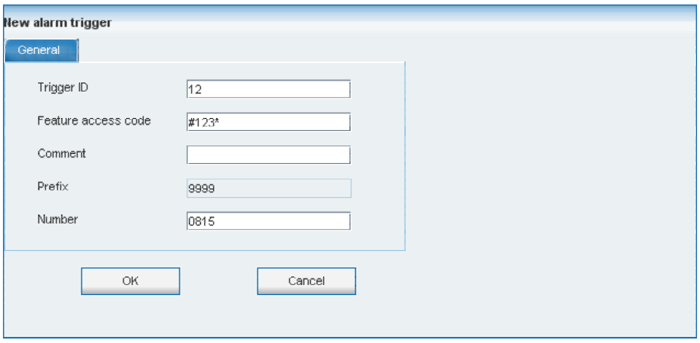
192.168.112.45

The following tasks can be performed:

- **Create**: create alarm trigger (see chapter 8.9.3.1).
- **Configure**: configure a selected alarm trigger (see chapter 8.9.3.2).
- **Delete**: delete selected alarm triggers (see chapter 8.9.3.3).
- **Show details**: shows parameters of a selected alarm trigger (see chapter 8.9.3.4).

8.9.3.1 Creating “Alarm triggers”

In **configuration mode** you can create new alarm triggers.



New alarm trigger

General

Trigger ID	12
Feature access code	#123*
Comment	
Prefix	9999
Number	0815

1 Click **Create**. In the **General** tab enter the alarm trigger parameters.

2 **Trigger ID**: Enter the Trigger ID. The Trigger ID identifies the alarm scenario and also selects the source which triggers the alarm.

3 **Feature access code**: Enter the access code which should be assigned to the alarm trigger.

4 **Comment**: Enter a comment for the new trigger.

5 **Prefix**: This field displays the **FAC number** which introduces the feature access code (see also chapter 8.9.1).

6 **Number**: Enter the number to be called in case of this alarm trigger.

7 Press the **OK** button.

8.9.3.2 Configuring “Alarm triggers”

In **configuration mode** you can configure an existing alarm trigger.

1 In the alarm trigger table click on the appropriate trigger entry.

2 Click **Configure**.
The **General** tab is displayed showing the current trigger configuration.

3 Change the trigger parameters, see chapter 8.9.3.1.

4 Press the **OK** button.

8.9.3.3 Deleting “Alarm triggers”

In **configuration mode** you can delete alarm triggers. The predefined alarm triggers (‘SOS and ’Man down‘) can not be deleted.

1 In the alarm trigger table click on one or more trigger entries.

2 Click **Delete**.

3 Confirm the displayed prompt with **OK**.

8.9.3.4 View “Alarm trigger” Details

In **monitor mode** you can view the details of an alarm trigger.

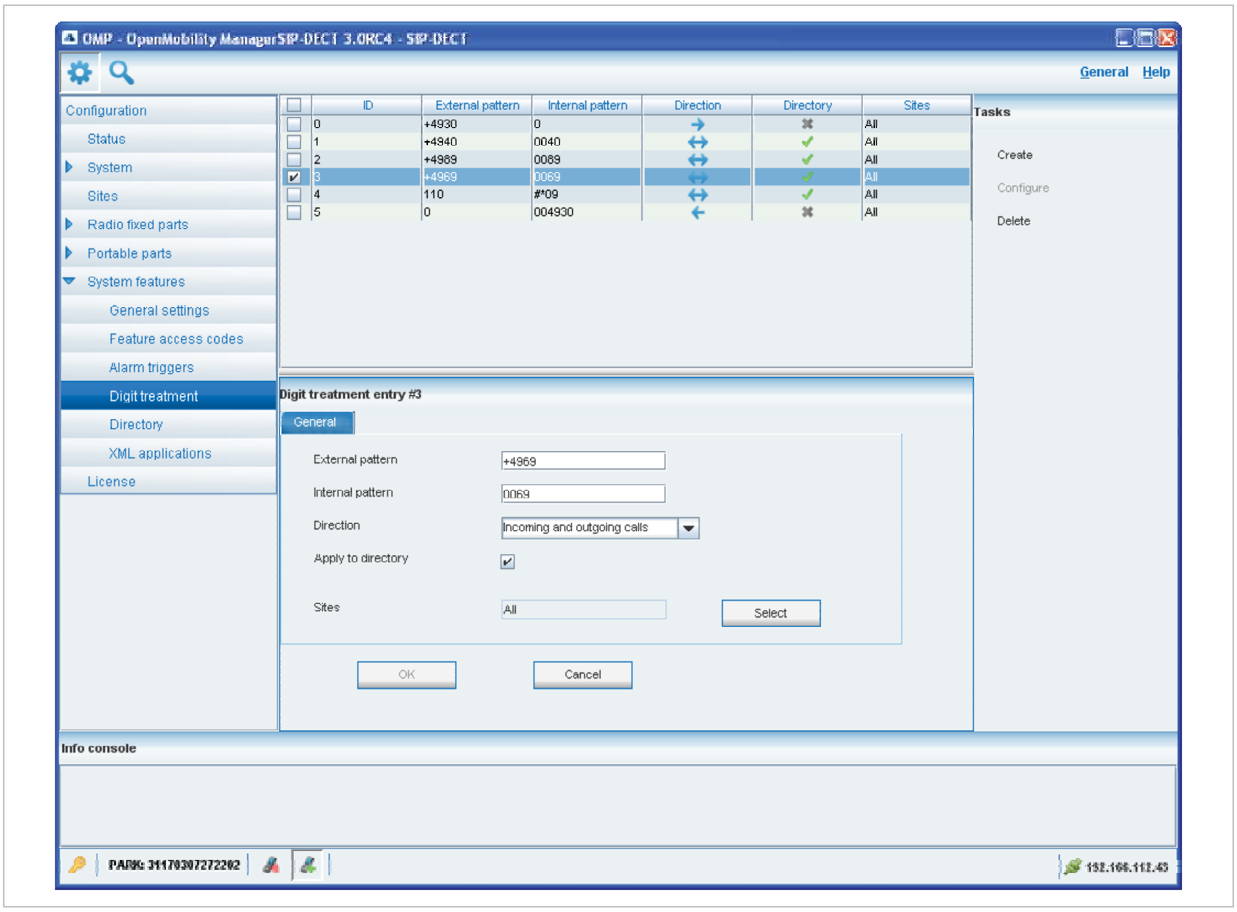
1 In the alarm trigger table click on the appropriate trigger entry.

2 Click **Show details**.
The **General** tab is displayed showing the trigger configuration.

3 Click **Cancel** to close the tab.

8.9.4 “Digit treatment” Menu

The **Digit treatment** menu allows to configure the number manipulation that is provided by the digit treatment feature for LDAP corporate directories.



□	ID	External pattern	Internal pattern	Direction	Directory	Sites
□	0	+4930	0	→	✖	All
□	1	+4940	0040	↔	✓	All
□	2	+4989	0089	↔	✓	All
☑	3	+4969	0069	↔	✓	All
□	4	110	#*09	↔	✓	All
□	5	0	004930	←	✖	All

Digit treatment entry #3

General

External pattern	+4969
Internal pattern	0069
Direction	Incoming and outgoing calls
Apply to directory	☑
Sites	All

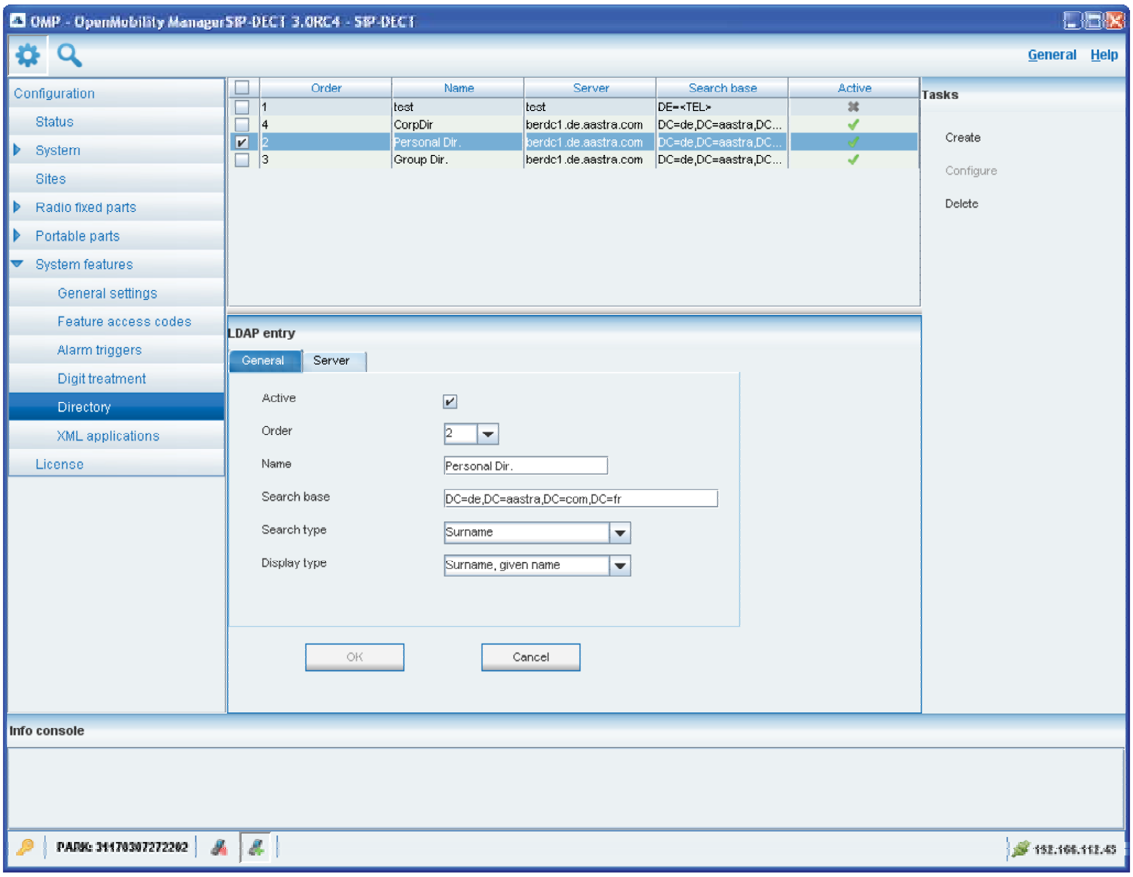
Select

OK Cancel

For a description of tasks and parameters available in this menu, refer to chapter 7.9.1.

8.9.5 “Directory” Menu

The **Directory** menu allows to configure the LDAP corporate directory services.



□	Order	Name	Server	Search base	Active
□	1	test	test	DE=<TEL>	✖
□	4	CorpDir	berdc1.de.aastra.com	DC=de,DC=aastra,DC...	✓
☑	2	Personal Dir.	berdc1.de.aastra.com	DC=de,DC=aastra,DC...	✓
□	3	Group Dir.	berdc1.de.aastra.com	DC=de,DC=aastra,DC...	✓

LDAP entry

General | Server

Active ☑

Order 2

Name Personal Dir.

Search base DC=de,DC=aastra,DC=com,DC=fr

Search type Surname

Display type Surname, given name

OK Cancel

For a description of tasks and parameters available in this menu, refer to chapter 7.9.2.

8.9.6 “XML applications” Menu

The SIP–DECT XML terminal interface allows external applications to provide content for the user on the DECT handsets Aastra 600d / Aastra 650c display and much more. To make the XML terminal interface applications available for the handset user, the relevant hooks must be configured in the **XML applications** menu.

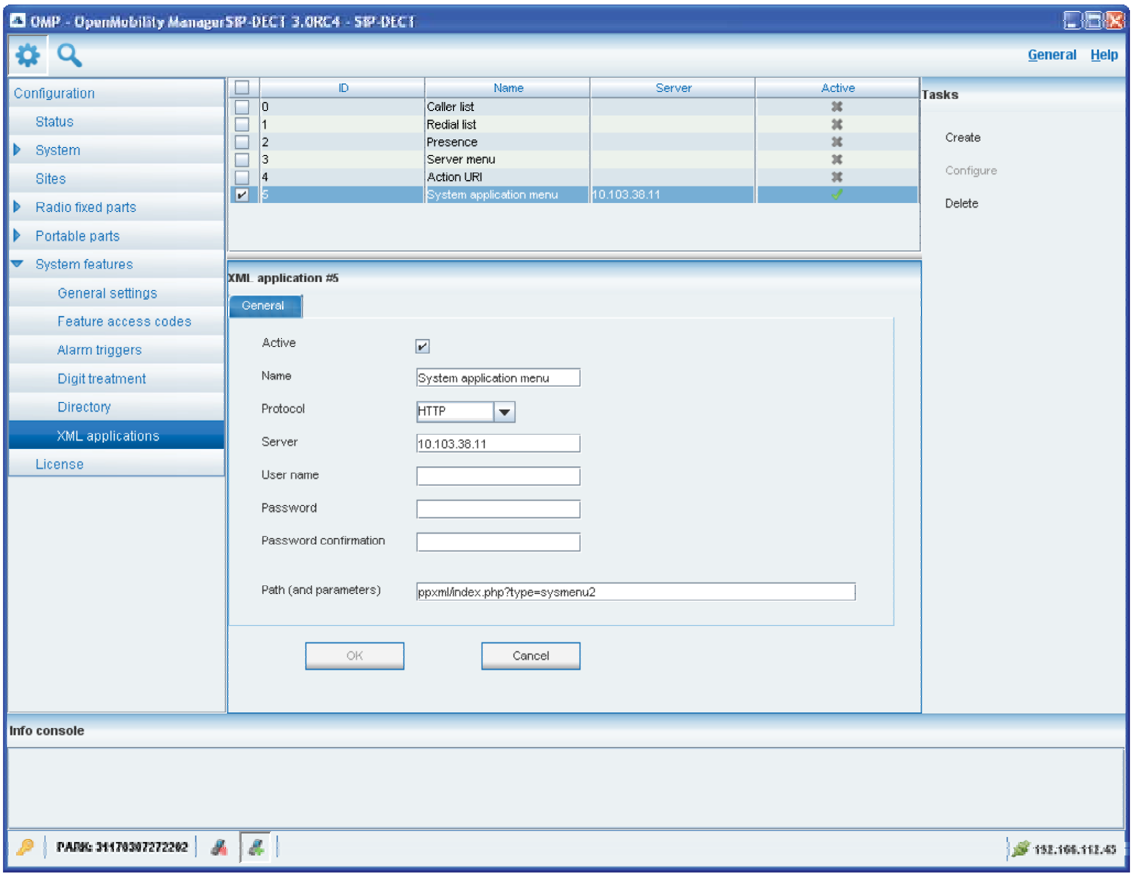
There are 5 predefined hooks and 10 hooks which can be freely defined. The 5 predefined hooks are:

- Call log: to replace the local call log
- Redial list: to replace the local redial list
- Presence: hook to reach a presence application
- Server Menu: hook to reach a server menu
- Action URIs: URI to be called in case of user/device events

These hooks can be activated or deactivated but not deleted. Up to 10 additional hooks can be created dynamically.

Please note: “Call log” and “Redial list” are replacing the local call log and redial list of the Aastra 600d / Aastra 650c if activated. Additionally the list access must be set to “automatic” or “PBX” on the handset in the settings / list access menu. If the list access is is set to “local”, the local list are used by the handset.

An activated hook becomes available on a handset (incl. the cooresponding menu entry) after the next DECT location registration of the handset. This can be foreced by switching the handset off and on. The same applies if a hook shall be deactivated.



□	ID	Name	Server	Active
□	0	Caller list		✗
□	1	Redial list		✗
□	2	Presence		✗
□	3	Server menu		✗
□	4	Action URI		✗
☑	5	System application menu	10.103.38.11	✓

XML application #5

General

Active ☑

Name: System application menu

Protocol: HTTP

Server: 10.103.38.11

User name:

Password:

Password confirmation:

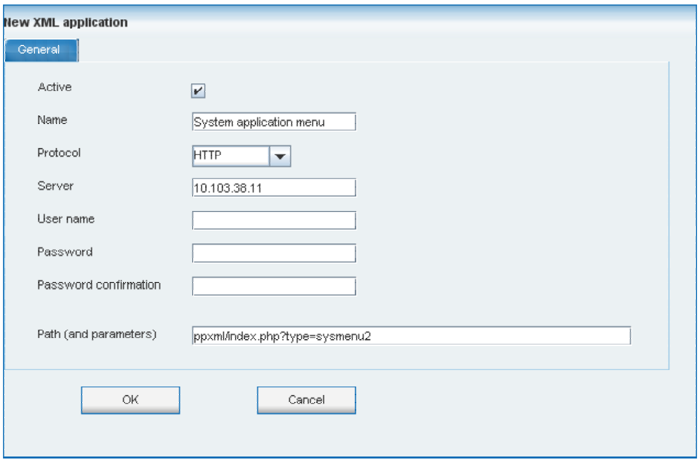
Path (and parameters): ppxml/index.php?type=sysmenu2

The tasks which can be performed in the **XML applications** menu are mode-dependant.

Configuration mode	Monitor mode	See chapter
Create: create new XML hooks		8.9.6.1
Configure: configure selected XML hook in detail panel		8.9.6.2
	Show details: shows selected XML hook in detail panel	8.9.6.3
Delete: delete selected XML hook		8.9.6.4

8.9.6.1 Creating a New XML Hook

Besides the 5 predefined XML hooks you can create up to 10 additional XML hooks.



New XML application

General

Active ☑

Name: System application menu

Protocol: HTTP

Server: 10.103.38.11

User name:

Password:

Password confirmation:

Path (and parameters): ppxml/index.php?type=sysmenu2

Adding individual XML hooks is only possible in **configuration mode**. To add an XML hook proceed as follows:

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

The **New XML application** panel opens.

2 Configure the XML hook, see parameter description below.

3 Press the **OK** button.

The following parameters can be set in the tabs of the **New XML application** panel:

- **Active**: This setting activates or deactivated a configured XML application entry.
- **Name**: The predefined hooks have fixed predefined names. A name has to be configured for the free defined hooks.

  The following parameters specify the URI:
- **Protocol**: Select the protocol HTTP or HTTPS.
- **Server**: Enter the IP address or the name of the server which provides the XML content.
- **User name**: Enter the login user name if an authentication is required by the server.
- **Password**, **Password confirmation**: Enter the password if the authentication is required by the server.
- **Path** (and parameter): Enter the path and query of the URI.

8.9.6.2 Changing an XML Hook

Changing XML hooks is only possible in **configuration mode**. To change the configuration of an existing XML hook proceed as follows:

1 Select the appropriate XML hook in the account table.

2 In the **Tasks** bar click on the **Configure** command.

3 Change the XML hook parameters, see parameter description in chapter 8.9.6.1.

4 Press the **OK** button.

Please note: The 5 predefined XML hooks cannot be renamed.

8.9.6.3 Viewing XML Hook Details

You can view the configuration of an XML hook in **monitor mode**. Proceed as follows:

1 Select the appropriate XML hook in the table.

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

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

3 To close the XML hook detail panel press the **Cancel** button.

8.9.6.4 Deleting XML Hooks

Deleting XML hooks is only possible in **configuration mode**. To delete one or more existing XML hook proceed as follows:

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

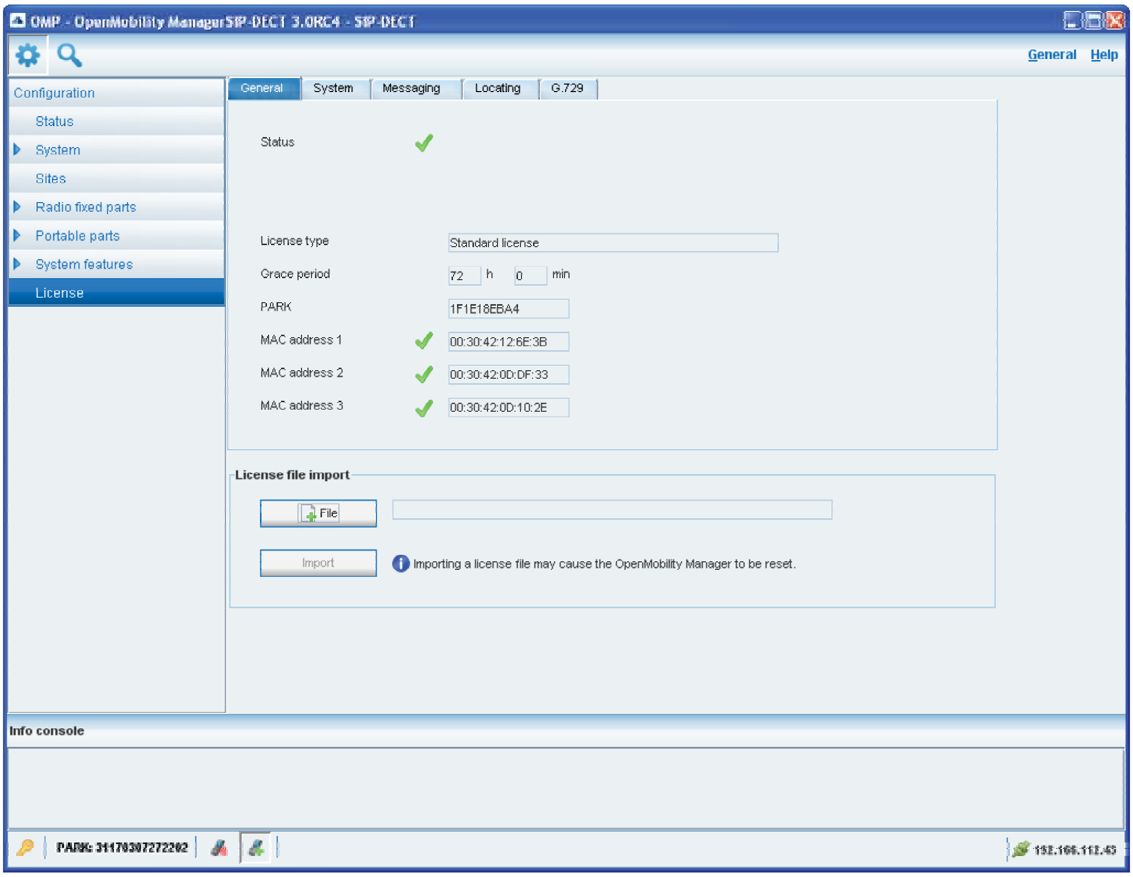
2 In the **Tasks** bar click on the **Delete** command.

3 Confirm the displayed prompt with **OK**.

Please note: The 5 predefined XML hooks cannot be removed.

8.10 “License” Menu

The **License** panel provides an overview on the currently used licenses. In **configurator mode** you can also import an activation or a license file:



Status ✓

License type: Standard license

Grace period: 72 h 0 min

PARK: 1F1E18EBA4

MAC address 1 ✓ 00:30:42:12:6E:3B

MAC address 2 ✓ 00:30:42:0D:DF:33

MAC address 3 ✓ 00:30:42:0D:10:2E

License file import

Importing a license file may cause the OpenMobility Manager to be reset.

PARK: 31170307272202

192.168.112.43

The license information is displayed in the following tabs:

- **General**: shows general license status.
- **System**: shows system license status.
- **Messaging**: shows Integrated Messaging and Alerting Service (IMA) license status.
- **Locating**: shows Locating license status.
- **G.729**: provides information about how many G.729 channels are licensed and how many licenses are temporarily in use.

To import an activation or a license file (only possible in **configuration mode**):

1. Press the **File** button to select the path and file name where the activation or license key is stored.
2. Afterwards press the **Import** button.

For a detailed description on the OMM licensing model see chapter 4.

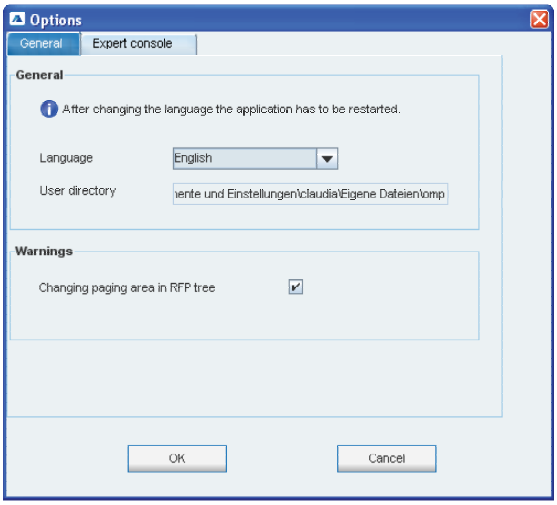
8.11 “General” Menu

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

- **Exit**: Selecting this menu entry opens the exit dialog to close the OMP.

- **Options**: Selecting this menu entry opens the **Options** dialog (see below).

“Options” dialog, “General” tab



General

After changing the language the application has to be restarted.

Language: English

User directory: ıente und Einstellungen\claudia\Eigene Dateien\omp

Warnings

Changing paging area in RFP tree ☑

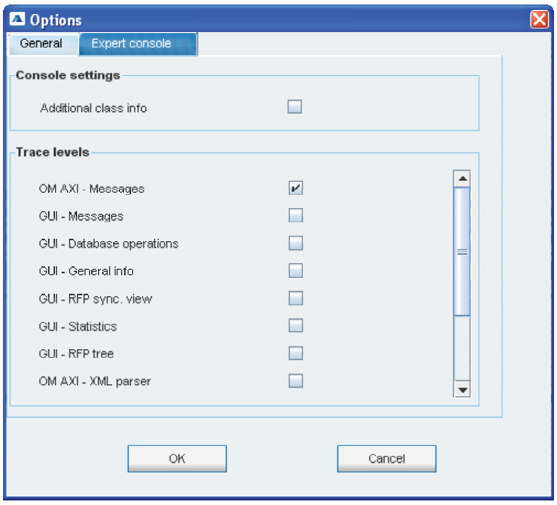
Language: You can select the OMP language. After changing the language, the OMP is automatically closed and has to be started again.

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

- System dump file “sys_dump.txt”
- Expert console log file “spy.log” when the application terminates
- Exception log file “exception.log” in case of a Java exception

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

“Options” dialog, “Expert console” tab



Console settings

Additional class info □

Trace levels

OM AXI - Messages ☑
GUI - Messages □
GUI - Database operations □
GUI - General info □
GUI - RFP sync. view □
GUI - Statistics □
GUI - RFP tree □
OM AXI - XML parser □

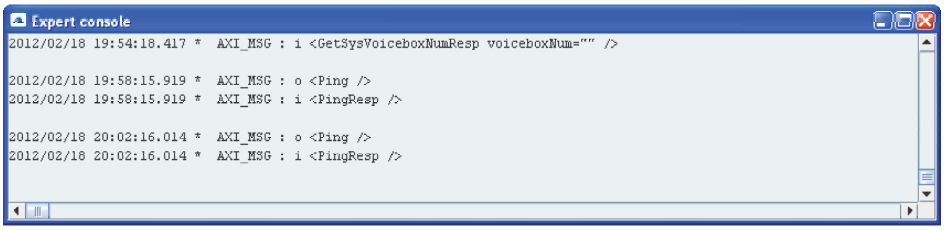
In the **Expert console** tab you can enable several trace levels. The trace messages will be shown in the expert console which can be called up via the **Help** menu (see chapter 8.12).

Moreover **Additional class info** can be enabled to show in which Java class the message has been generated.

8.12 “Help” Menu

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

- **Expert console**: Selecting this menu entry enable/disables the expert console. The expert console allows to trace OMP messages and to check the messages sent and received from the OMM. The expert console will be opened in a secondary window.

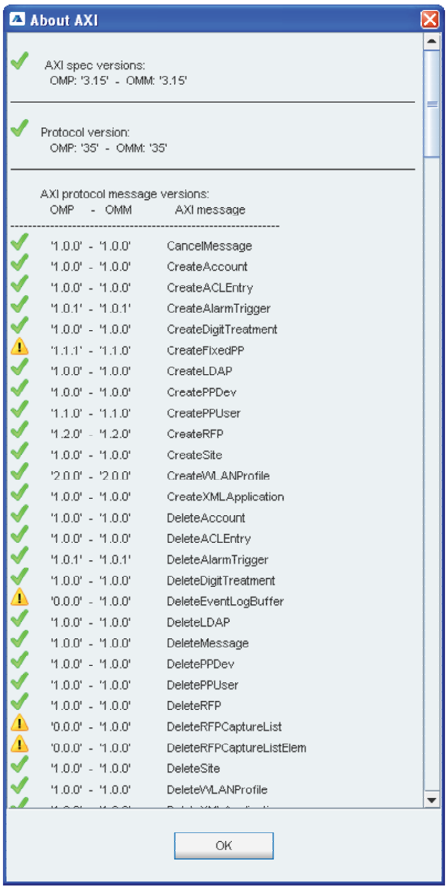


```
2012/02/18 19:54:18.417 *  AXI_MSG : i <GetSysVoiceboxNumResp voiceboxNum="" />

2012/02/18 19:58:15.919 *  AXI_MSG : o <Ping />
2012/02/18 19:58:15.919 *  AXI_MSG : i <PingResp />

2012/02/18 20:02:16.014 *  AXI_MSG : o <Ping />
2012/02/18 20:02:16.014 *  AXI_MSG : i <PingResp />
```

- **Info**: Selecting this menu entry displays the End User License Agreement (EULA).
- **About AXI**: Selecting this menu entry displays the About AXI dialog. This dialog compares the protocol version numbers which are provided by the OMM with the protocol version numbers supported by OMP. The warning icon ⚠ shows a version mismatch. A version number “0.0.0” means the protocol element is not used by OMP.



```
✓  AXI spec versions:
     OMP: '3.15'  -  OMM: '3.15'

✓  Protocol version:
     OMP: '35'  -  OMM: '35'

   AXI protocol message versions:
     OMP   -  OMM        AXI message
---------------------------------------------------
✓    '1.0.0' - '1.0.0'     CancelMessage
✓    '1.0.0' - '1.0.0'     CreateAccount
✓    '1.0.0' - '1.0.0'     CreateACLEntry
✓    '1.0.1' - '1.0.1'     CreateAlarmTrigger
✓    '1.0.0' - '1.0.0'     CreateDigitTreatment
⚠    '1.1.1' - '1.1.0'     CreateFixedPP
✓    '1.0.0' - '1.0.0'     CreateLDAP
✓    '1.0.0' - '1.0.0'     CreatePPDev
✓    '1.1.0' - '1.1.0'     CreatePPUser
✓    '1.2.0' - '1.2.0'     CreateRFP
✓    '1.0.0' - '1.0.0'     CreateSite
✓    '2.0.0' - '2.0.0'     CreateWLANProfile
✓    '1.0.0' - '1.0.0'     CreateXMLApplication
✓    '1.0.0' - '1.0.0'     DeleteAccount
✓    '1.0.0' - '1.0.0'     DeleteACLEntry
✓    '1.0.1' - '1.0.1'     DeleteAlarmTrigger
✓    '1.0.0' - '1.0.0'     DeleteDigitTreatment
⚠    '0.0.0' - '1.0.0'     DeleteEventLogBuffer
✓    '1.0.0' - '1.0.0'     DeleteLDAP
✓    '1.0.0' - '1.0.0'     DeleteMessage
✓    '1.0.0' - '1.0.0'     DeletePPDev
✓    '1.0.0' - '1.0.0'     DeletePPUser
✓    '1.0.0' - '1.0.0'     DeleteRFP
⚠    '0.0.0' - '1.0.0'     DeleteRFPCaptureList
⚠    '0.0.0' - '1.0.0'     DeleteRFPCaptureListElem
✓    '1.0.0' - '1.0.0'     DeleteSite
✓    '1.0.0' - '1.0.0'     DeleteWLANProfile
```

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

9 Configuration und Administration Aspects

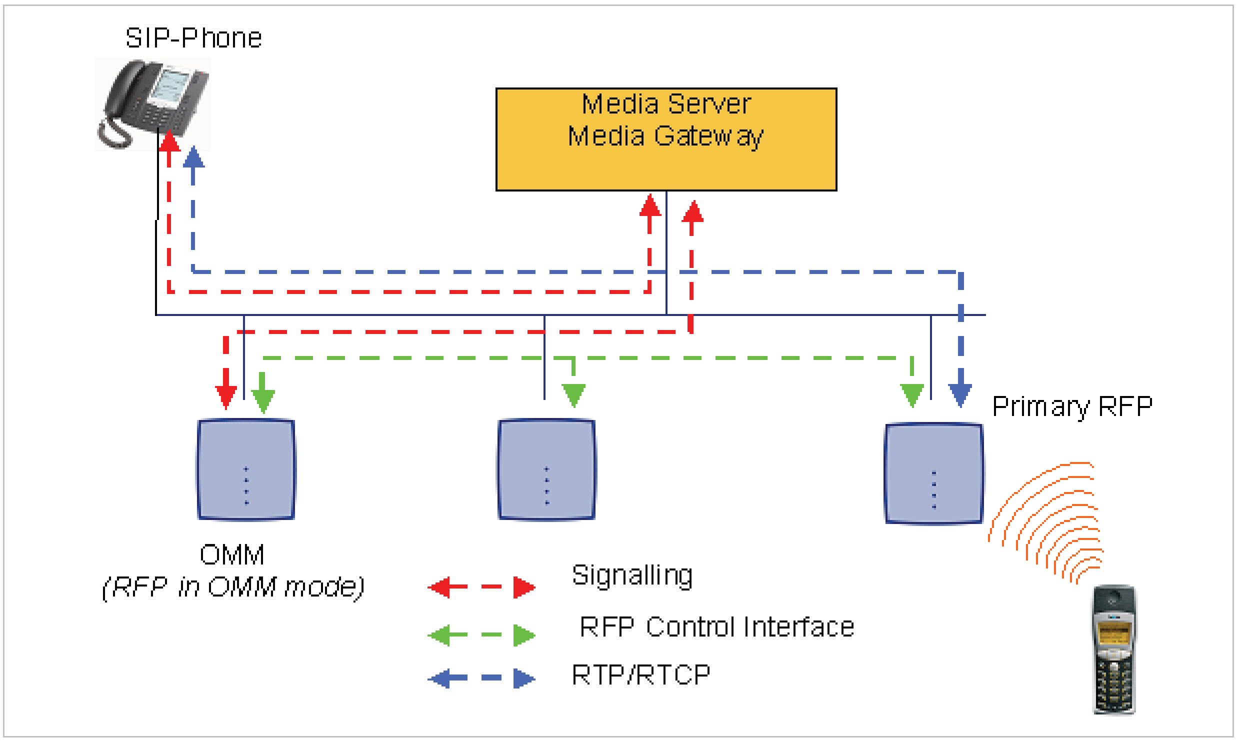
This chapter provides detailed information on various configuration and administration aspects regarding the SIP–DECT solution.

9.1 IP Signaling and Media Stream

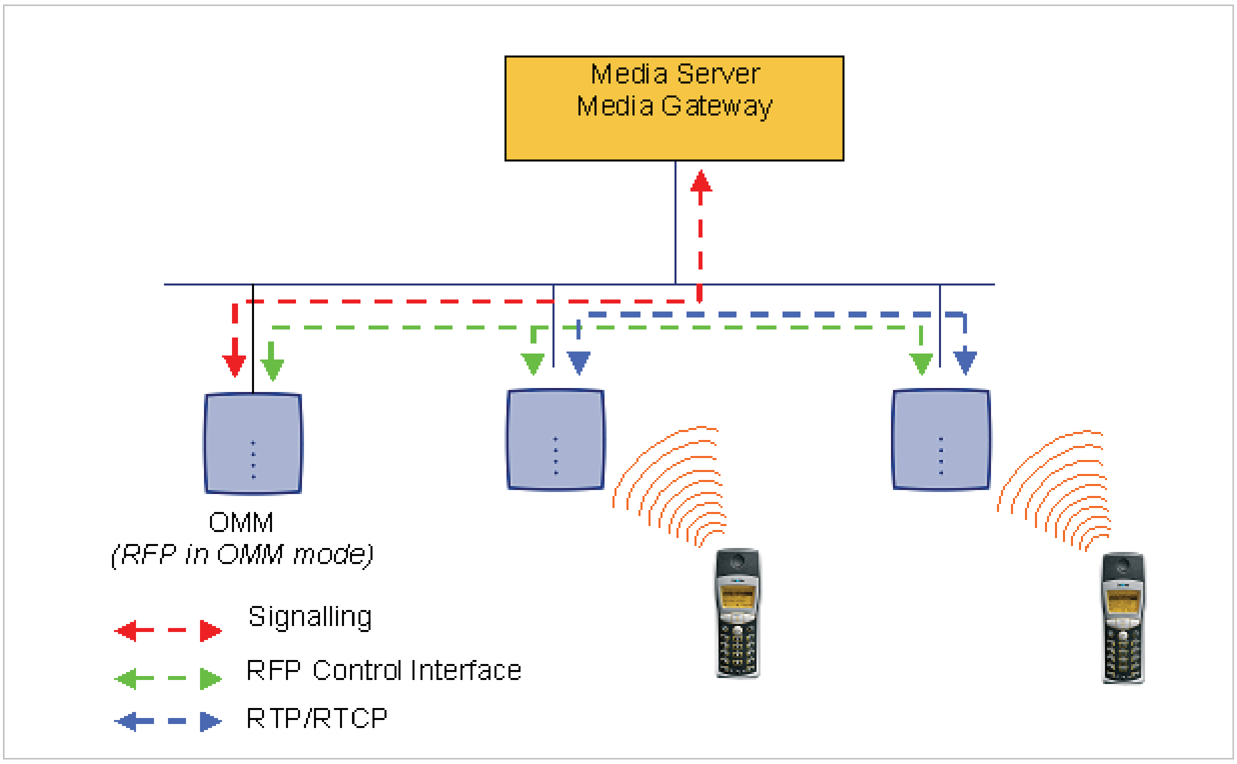
To establish a call between an IP Phone and a PP (e.g. Aastra 620d), the following IP streams must be established:

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

The following figure illustrates this scenario.

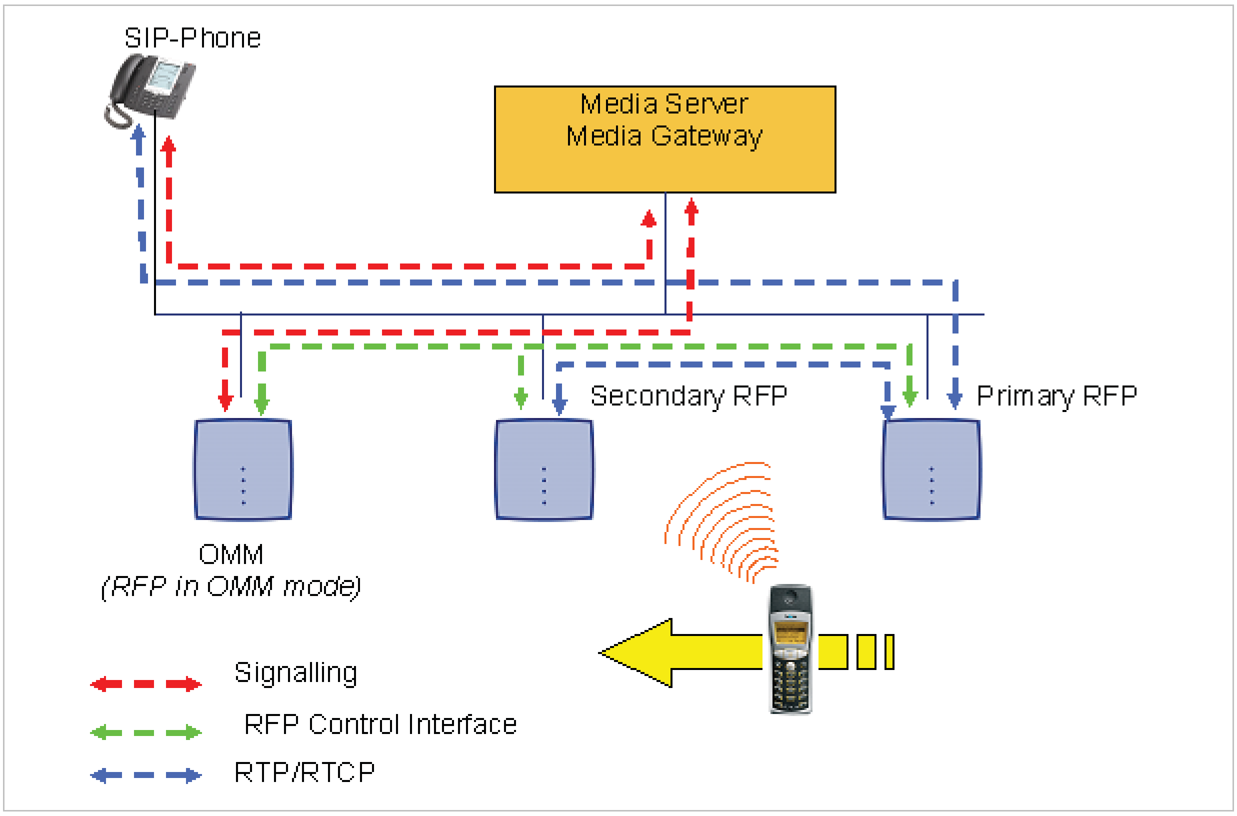


To establish a call between two PPs, the same IP streams must be established like in the scenario before, except the IP phone is not involved. The following figure illustrates this scenario.

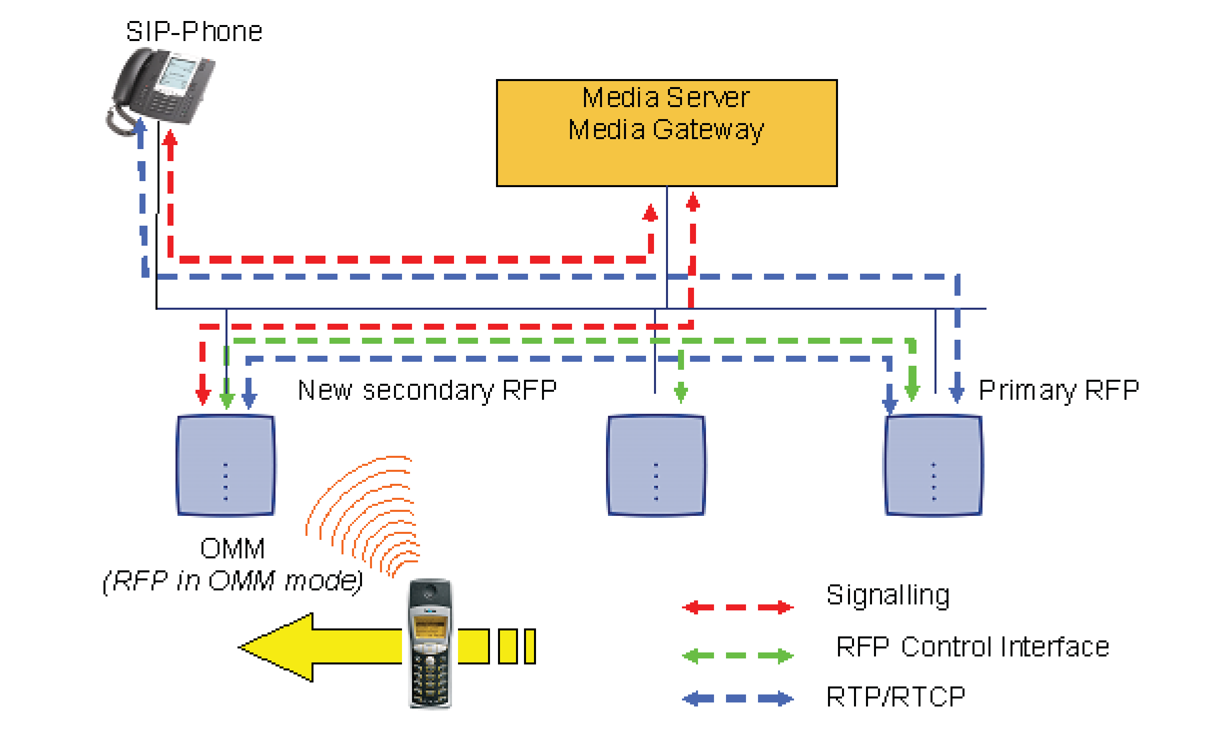


A call from one PP to another that resides on the same RFP will loop back within the RFP if no media gateway is involved. So the call will not pass through to the Local Area Network (LAN). Although the voice packets will not impact LAN traffic, signal packets will.

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



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

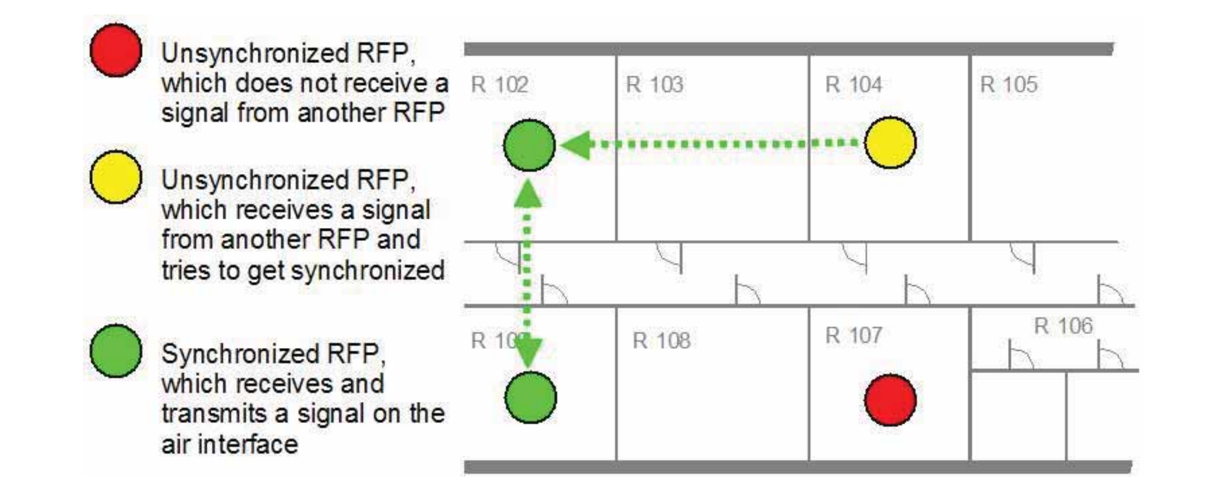


9.2 RFP Synchronization

To guarantee a seamless handover if a caller moves from one RFP zone of coverage to another RFP zone of coverage, an accurate synchronization of the RFPs is necessary.

The RFPs are synchronized over the air interface. The first RFP to complete startup will transmit a signal on the air for the other RFPs to synchronize from. If an RFP gets in sync, then it will transmit a signal on the air and will be the sync source for the next RFP. Only RFPs which can receive a synchronization signal will become synchronized.

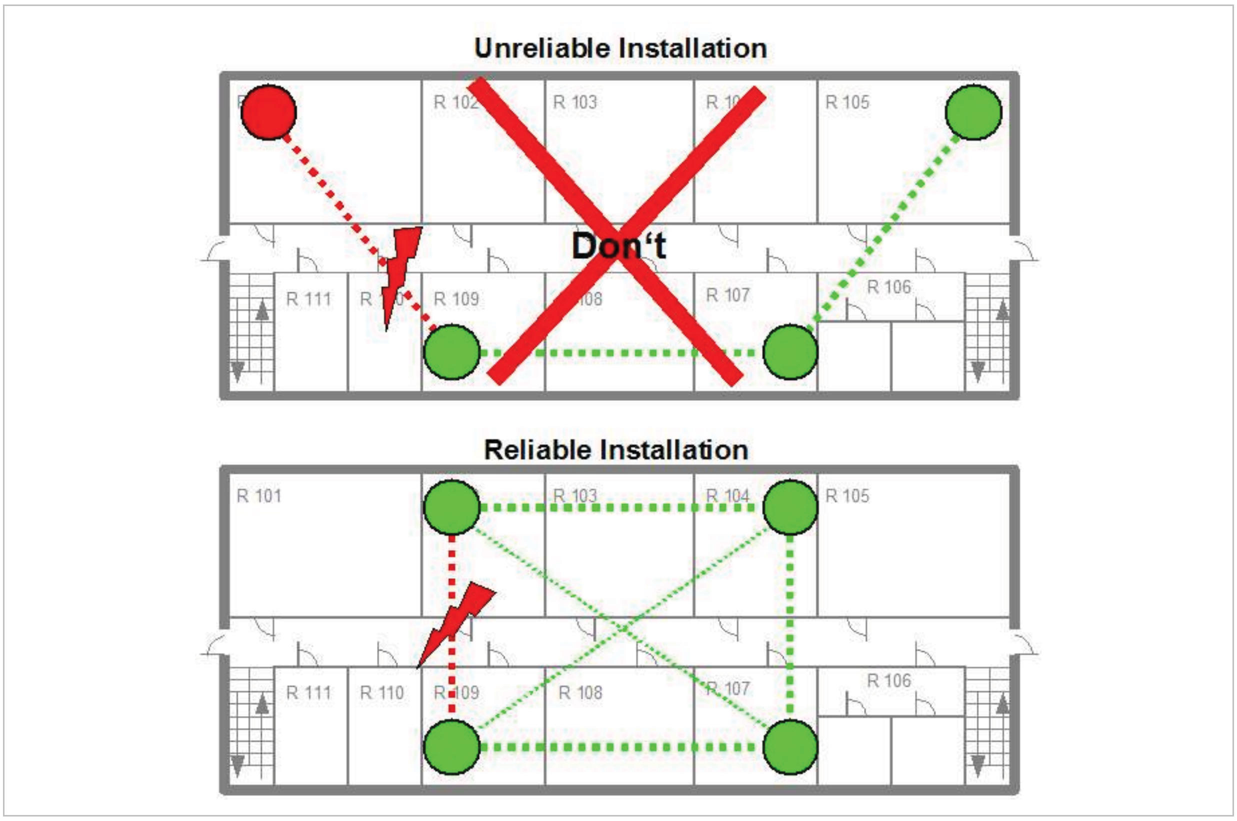
For the RFP to sync to another RFP the signal strength cannot drop below -70 dBm. You must consider this requirement during the site survey.


Unsynchronized RFP, which does not receive a signal from another RFP
Unsynchronized RFP, which receives a signal from another RFP and tries to get synchronized
Synchronized RFP, which receives and transmits a signal on the air interface
R 102
R 103
R 104
R 105
R 109
R 108
R 107
R 106

As long as an RFP is not in sync, no calls can be established using this RFP.

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

A SIP–DECT installation is more reliable if an RFP can receive the signal from more than only one RFP because the other signals are also used for synchronization.



The sync-over-air solution is very reliable because all existing redundant paths are used for synchronization. Thus, hardware tolerances have only very little influence. No RFP has a key position.

Only unfavorable setups without redundant synchronization paths can cause problems.

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

9.2.1 Initial Synchronization Procedure

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

- Synchronization stage 0
  - If at least one preferred RFP was configured, the synchronization process will wait up to 30 seconds for an incoming startup message of such a preferred RFP. Receiving a message will finishing stage 0 and the synchronization process jumps to stage 1.

  - If no message was received within the 30 seconds this stage will be terminated and the next stage will be started.
  - If no preferred RFP was configured, this stage will be ignored.
- Synchronization stage 1
  - If a preferred RFP was determined in stage 0, this one will be the synchronization source for the next upcoming RFPs. Otherwise the first RFP which sends a startup message will be the synchronization source for the next upcoming RFPs.
  - In this stage only RFPs reporting an RSSI value better than -65 dBm will be permitted to do a synchronization.
  - If an RFP has done its synchronization, this RFP will be also a synchronization source for other upcoming RFPs.
  - The initial timeout for this stage is 30 seconds. Whenever an RFP has finished its synchronization in this stage a new stage timeout value will be calculated.
  - If no RFP comes up within the timeout time or if all the upcoming RFPs do not fit the RSSI threshold, this stage will be terminated and the next stage will be started.
- Synchronization stage 2
  - The behavior of this stage is identical to stage 1, but an RSSI threshold value of -70 dBm is significant.
- Synchronization stage 3
  - The behavior of this stage is identical to stage 1, but an RSSI threshold value of -75 dBm is significant.
- Synchronization finished
  - No more RSSI threshold value is significant. All the RFPs which failed the stage conditions above, are now permitted to do a synchronization.

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

9.2.2 Checking the Synchronization of a Network

For every cluster a periodically check of the synchronization of the network is done. If the network is split into at least two subnets, all the RFPs of the lesser subnet(s) will be resynchronized. While doing initial synchronization procedure this check is deactivated. You can check the RFP synchronization using the Sync view menu of the OM Management Portal (OMP), see chapter 8.7.5.

9.3 RFP Channel Capacity

On air the RFP has 12 available time slots, 8 can have associated DSP resources for media streams. All DECT time slots are used for control signaling, SW download over air, messaging and bearer handover independent of associated DSP resources.

If all 8 media stream channels are used the RFP announces a “busy bit”. In that case the PPs determine whether another RFP has an appropriate signal strength. If so, the PP will handover to that RFP. Once the handover has been completed, the RFP will then lower its “busy bit”.

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

Notes on Hi-Q connections

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

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

9.4 Network Infrastructure Prerequisites

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

- RFPs
- PPs
- IP PBX/media server (e.g. Asterisk)
- TFTP server

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

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

Notes on network infrastructure prerequisites

- In NA outdoor RFPs may only be installed with the antennas shipped with the units. No other antennas or cabling are permitted. In EMEA the outdoor RFPs are shipped without antennas and you may use the units with one of the optional antennas (separate order no.).
- A TFTP server is no longer required for boot of an RFP (L) 35/36/37 IP or RFP (L) 43WLAN.
- TFTP, FTP(S), HTTP(S) are supported for RFP (L) 35/36/37 IP or RFP (L) 43WLAN software update.

9.5 SIP–DECT Startup

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

For booting an RFP (L) 32/34 IP or RFP (L) 42 WLAN, there must be at least one TFTP server on the attached network to load the OMM/RFP application software.

RFP (L) 35/36/37 IP or RFP (L) 43 WLAN uses the internal flash to start the boot image. A fileserver is only needed for software update over the network, please see chapter 9.11.5.

The essential network settings can be alternatively:

- Communicated by a DHCP server at startup time.
- Configured on the RFP with the OM Configurator tool (see chapter 9.6). The settings made by the OM Configurator will be saved permanently in the internal flash memory of each OMM/RFP.

9.5.1 TFTP and DHCP Server Requirements

TFTP server requirements

The RFP gets the boot image file from a TFTP server. The requirement list for the used TFTP server is defined as follows:

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

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

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

DHCP server requirements

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

9.5.2 Booting Steps

Booting is performed in two steps:

1 Starting the boot process.

6 Starting the application.

Booter startup

The RFP has only a little standalone application built into the flash. This software realizes the so called net boot process. On startup each RFP tries to determine its own IP address and other settings of the IP interface from the configuration settings in the internal flash memory. If no settings are available or these settings are disabled, the RFP tries to determine these settings via DHCP. The RFP gets the application image file from the TFTP server.

Application startup

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

Depending on the given settings the following service applications will be started in these phase: OMM (OpenMobility Manager), SNTP, SNMP.

There is no difference in booting that RFP which is chosen to be running in OMM mode from those which are in the RFP only mode. The decision is driven by the OMM IP address, which is read

- within the local network settings, if active;
- via DHCP request;
- RFP configuration file (see 9.8).

The RFP which has the same IP address as the dedicated OMM IP address will be the RFP which the OMM application runs on.

9.5.3 Booter Startup

The SIP–DECT Release 2.0 (and higher) includes a booter version 3.4 with the following new features:

- VLAN can be configured via the OM Configurator without a static IP configuration. This means that the first DHCP request will be done by using VLAN.
- To balance the network load, up to three TFTP servers can be configured. This can be done using the OM Configurator (local setting) or using the DHCP option 150. Before starting the download, the TFTP server will be selected randomly by the booter. **But**, if the option “Preferred TFTP server” was set by the OM Configurator, the option “TFTP server address” will specify the TFTP server to use. No randomly selection will be done in this case.
- To reduce the number of TFTP packets sent by the TFTP server, the packet size can be increased. This will be done by using a TFTP option (see 9.5.1 “TFTP server requirements”).
- Multicast TFTP download is possible if the TFTP server and the connected network support this.
- To indicate the actual state of the booter, the four LEDs of the RFP will be used (see 9.5.5).

9.5.3.1 DHCP Client

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

• IP address	mandatory
• Net mask	mandatory
• Gateway	mandatory
• Boot file name	mandatory
• TFTP server	mandatory
• Public option 224: “OpenMobility”	mandatory

• VLAN-ID	optional
• TFTP server list	optional

9.5.3.1.1 DHCP Request

The DHCP client sends the vendor class identifier (code 60) “OpenMobility” and requests the following options in the parameter request list (code 55):

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

9.5.3.1.2 DHCP Offer

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

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

  or
- the **file** field in the DHCP message has a sub string equal to “ip_rfp.cnt”.

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

Information retrieved from the DHCP offer:

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

9.5.3.1.3 Retries

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

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

9.5.3.2 TFTP Client

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

9.5.3.3 Booter Update

Each application SW comes with the latest released booter SW. The application SW will update the booter automatically.

Please note: After an upgrade from an older OpenMobility Release (< 2.0) to an OpenMobility Release 2.x the booter of the RFPs will be updated to Version 3.4.x. The OpenMobility Configurator 2.x is required to configure RFPs with this new booter version. If you downgrade the RFP to an older release, the booter will not downgrade automatically.

9.5.4 Application Startup

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

9.5.4.1 DHCP Client

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

Parameters

The following parameters will be supported within this step:

Option / Field	Meaning	Mandatory
yiaddr	IP address of the IP-RFP	yes
siaddr	Parameter named “Boot Server Host Name” with value as the IP address of the TFTP server	yes
File	Parameter named “Bootfile Name” with value of the path (optional) and name of the application image. For exampleiprfp2g.tftp.	yes
code 1	Subnet mask	yes
code 3	Default Gateway	yes
code 6	Domain Name Server	no
code 15	Domain Name	no
code 42	IP address of a NTP server	no
code 43	Vendor Specific Options	yes
code 66	URL specifies the protocol, server and path to access the RFP configuration files (see 9.8).	no
public option 224	Parameter named magic_str must be set to value "OpenMobility".	yes

Vendor specific options

The Vendor Specific Options consist of:

Vendor Specific Option	Meaning	Length	Mandatory
option 10	ommip1: Used to select the IP-RFP who should reside the Open Mobility Manager (OMM).	4	yes
option 14	syslogip: IP address of a Syslog Daemon	4	no
option 15	syslogport: Port of a Syslog Daemon	2	no
option 17	Country: Used to select the country in which the OMM resides. This enables country specific tones (busy tone, dial tone, …).	2	no
option 18	ntpservname: Name of a NTP Server	x	no
option 19	ommip2: Used to select a secondary IP-RFP who should reside the standby Open Mobility Manager (OMM). This option must be given if the OMM Standby feature should be used (see chapter 9.13).	4	no
option 24	rsturl: Restore URL URL for an automatic OMM Database import (see chapter 7.4.6.2 and chapter 8.5.5.1)	x	no

Example

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

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

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

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

Country specific tones

Tones for the following countries are supported:

Country code	Country
1	Germany
2	Great Britain
3	Switzerland
4	Spain
6	Italy
7	Russia
8	Belgium

9	Netherlands
10	Czechoslovakia
11	Austria
12	Denmark
13	Slovakia
14	Finland
15	Hungary
16	Poland
17	Belarus
18	Estonia
19	Latvia
20	Lithuania
21	Ukraine
22	Norway
24	Sweden
25	Taiwan
100	North America
101	France
102	Australia

9.5.4.2 Configuration using DHCP

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

- The second generation Hardware RFP (L) 32/34 IP / RFP (L) 42 WLAN use “OpenMobility”.
- The third generation RFP (L) 35/36/37 IP / RFP (L) 43 WLAN use “OpenMobility3G”.

> **Please note:** The first lot of RFP (L) 35/36/37 IP / RFP (L) 43 WLAN comes with a prefieldtrial software on board which uses “OpenMobility” as DHCP client vendor class identifier. After update to SIP-DECT 3.0RC3 or later the DHCP client vendor class identifier is “OpenMobility3G”.

BOOTP/DHCP Option	Meaning	Type	Remarks
siaddr	IP address of the TFTP server	4 octets	Only mandatory for RFP (L) 32/34 IP / RFP (L) 42 WLAN because of the NETBOOT process; optional for RFP (L) 35/36/37 IP/

			RFP (L) 43 WLAN SW update
File	Path to the boot image server by the TFTP server	N octets	Only mandatory for RFP (L) 32/34 IP / RFP (L) 42 WLAN because of the NETBOOT process; optional for RFP (L) 35/36/37 IP/ RFP (L) 43 WLAN SW update
150	TFTP server list	N * 4 octets	Only used by the NETBOOT process of the RFP (L) 32/34 IP / RFP (L) 42 WLAN, optional
224	Magic String	“OpenMobilitySIP-DECT” *	The client uses this option to select the server, mandatory

* The magic string “OpenMobilitySIP-DECT” instead of “OpenMobility” (as defined in SIPDECT 2.x) makes sure that a SIP-DECT software is loaded into the RFP (L) 35/36/37 IP/ RFP (L) 43 WLAN even an different, non-SIP-DECT SW is previously installed and running.

9.5.4.3 Selecting the Right DHCP Server

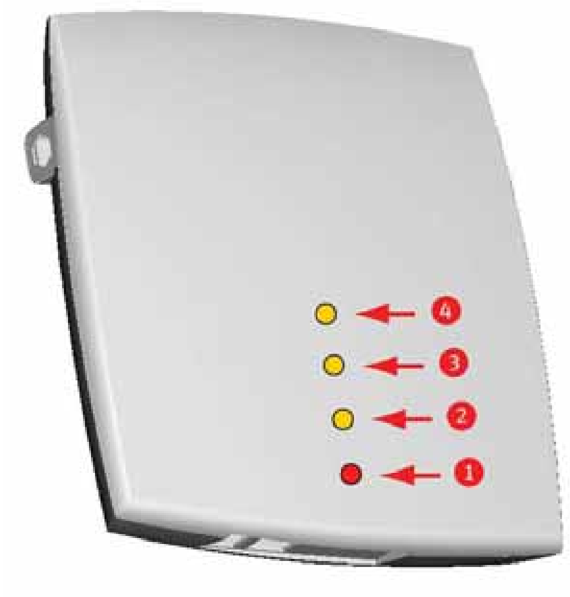
The DHCP client requests its own IP address using code 50. The DHCP client will select the DHCP server that offers the currently used IP address. Additionally the mandatory options must be offered otherwise the DHCP offer is ignored by the DHCP client.

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

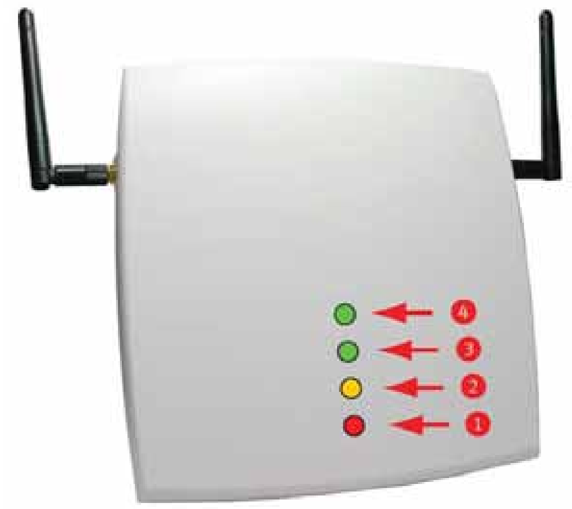
If the DHCP client cannot accept an DHCP offer within 3 minutes the RFP is rebooted.

9.5.5 RFP LED Status

RFP (L) 32/34 IP RFP 32/34 NA RFP (L) 35/36 IP	RFP (L) 42 WLAN RFP (L) 43 WLAN



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



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

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

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

9.5.5.1 Booter LED Status

RFP (L) 35/36/37 IP, RFP (L) 43 WLAN

The RFP (L) 35/36/37 IP and RFP (L) 43 WLAN booter uses LED1 for signaling its activity. After power up the LED 1 (INFO) is turned on red continuously. The successful start of the boot image is signaled by turning on LED 1 orange.

Frage von Commando an Aastra: Wo sind die LED am Outdoor RFP 37 IP? Auf den bisher uns bekannten Fotos sind keine LED zu sehen…

RFP (L) 32/34 IP, RFP 32/34 NA, RFP (L) 42 WLAN

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

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

9.5.5.2 Application LED Status

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

RFP (L) 35/36/37 IP, RFP (L) 43 WLAN

	LED1 (INFO)		LED2 (OMM / SYSTEM)		LED3 (DECT)		LED4 (WLAN)		
Kernel	🟧 cont.		⬛	⬛	⬛	⬛	⬛	⬛	kernel boot phase (inflator, …)
RFPM	🟧 1s	⬛ 1s							DHCP phase
	🟧 1,85s	⬛ 0,1s							DHCP failure (idle loop)
	🟧 0,5s	⬛ 0,5s							obtaining external configuration
	🟧 0,85s	⬛ 0,1s							external configuration failure
	🟩 cont.								Ready
	🟩 1,85s	🟧 0,15s							Up&Running + RFP houses OMM
RFP general			🟧 1s	⬛ 1s					OMM connect phase

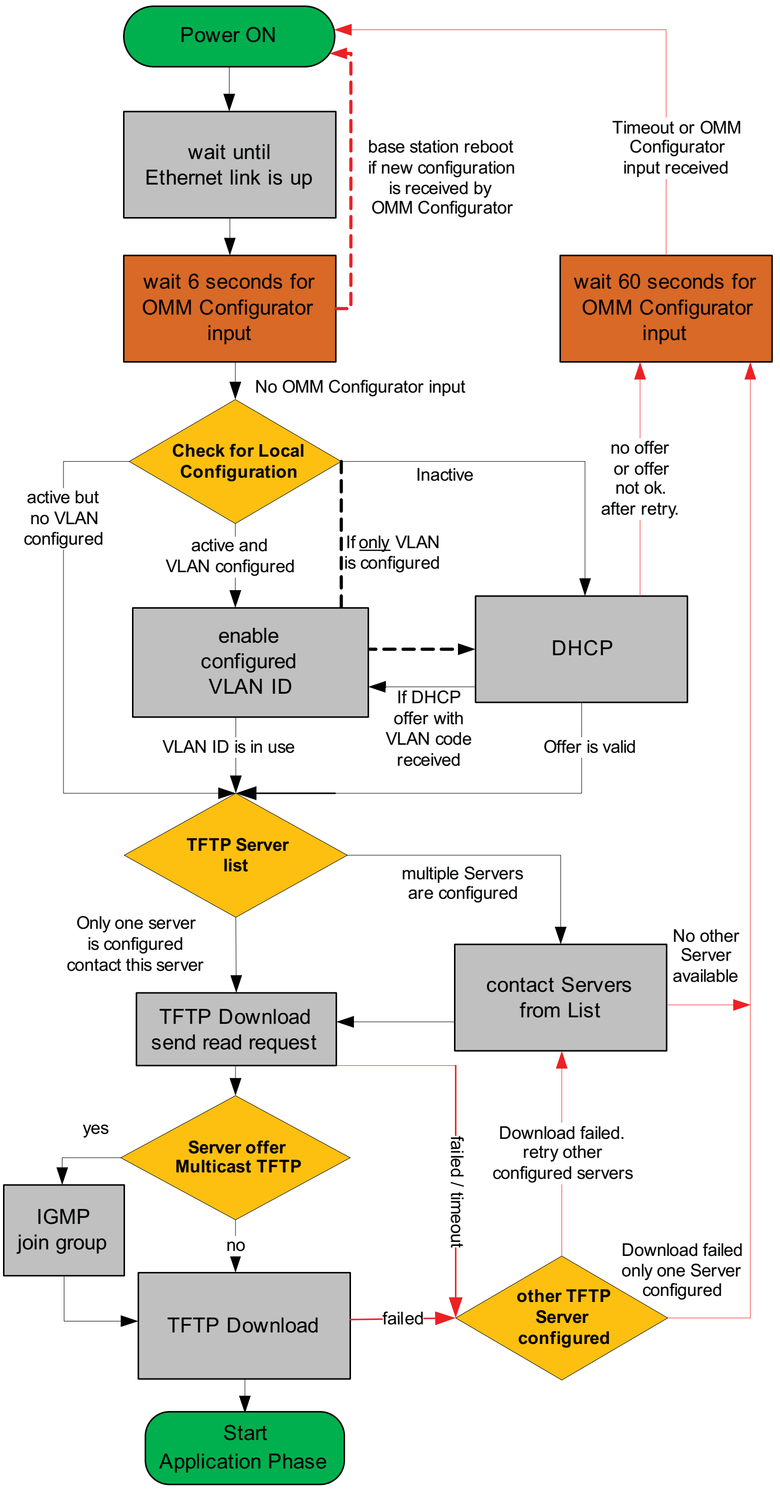
	LED1 (INFO)		LED2 (OMM / SYSTEM)		LED3 (DECT)		LED4 (WLAN)		
			1,85s	0,15s					OMM connection failure (idle loop)
			cont.						Up&Running (OMM connected)
			1,85s	0,15s					Up&Running + OMM warning
			1,85s	0,15s					Up&Running + OMM failure
RFP DECT					cont.				DECT not configured on this RFP
		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

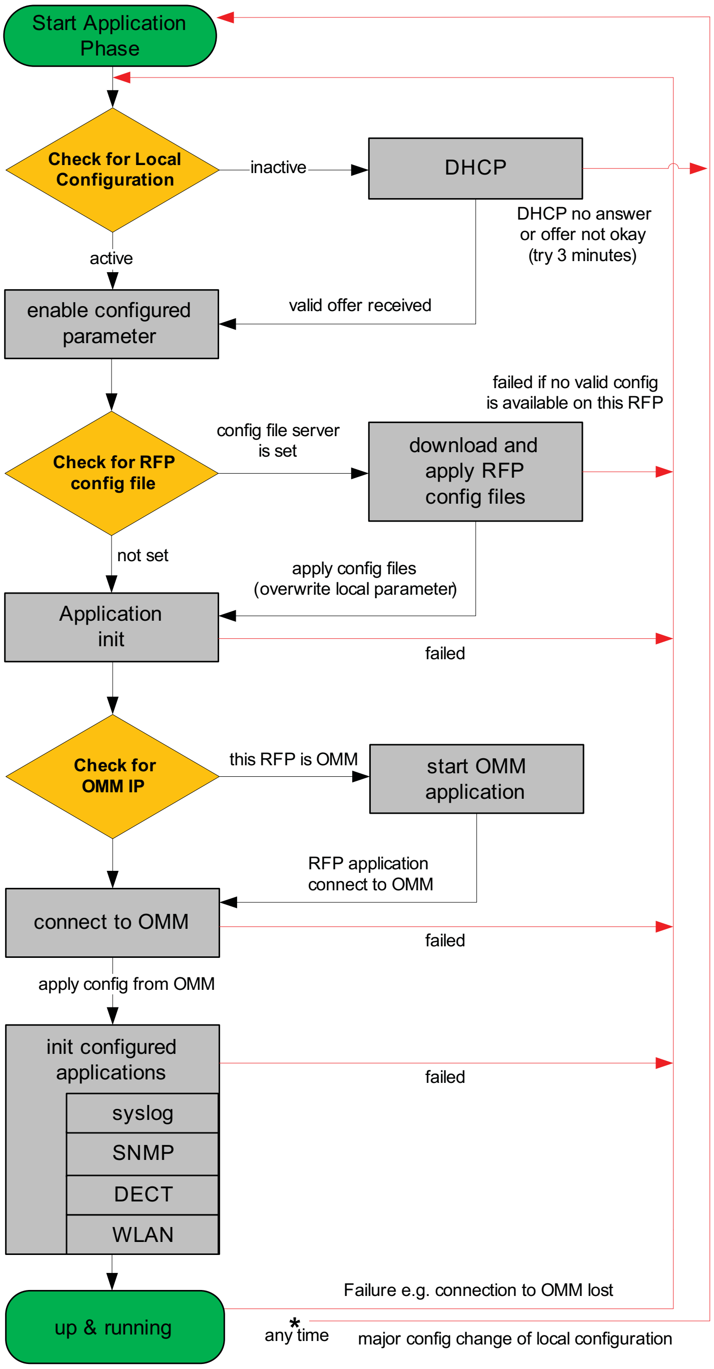
RFP (L) 32/34 IP, RFP 32/34 NA, RFP (L) 42 WLAN

	LED1 (INFO)		LED2 (OMM / SYSTEM)		LED3 (DECT)		LED4 (WLAN)		
Now, the kernel / application is running: LED1 will never be RED									
Kernel	cont.		⬛	⬛	⬛	⬛	⬛	⬛	kernel boot phase (inflator, …)
RFPM	1s	1s							DHCP phase
	1,9s	0,1s							DHCP failure (idle loop)
	0,5s	0,5s							obtaining external configuration

	LED1 (INFO)		LED2 (OMM / SYSTEM)		LED3 (DECT)		LED4 (WLAN)		
	0,9s	0,1s							external configuration failure
	cont.								Ready
	1,9s	0,1s							Ready + OMM reside on this RFP
RFP general			1s	1s					OMM connect phase
			1,9s	0,1s					OMM connection failure (idle loop)
			cont.						Ready (OMM connected)
			1,9s	0,1s					Ready + OMM has a warning
			1,9s	0,1s					Ready + OMM has an error
RFP DECT					cont.				DECT not configured on this RFP
					1,9s	0,1s			DECT inactive (not synced yet)
					cont				DECT 'on air'
					1,9s	0,1s			DECT + call active
					1,9s	0,1s			DECT + call active +busy bit
RFP WLAN							cont.		WLAN not configured on this RFP
							1,9s	0,1s	WLAN inactive yet
							cont.		WLAN 'on air'
							1,9s	0,1s	WLAN + assoc. clients
							cont.		WLAN failure (e.g. 10 Mbit uplink)
License			cont.		cont.		cont.		Branding mismatch (RFP not functional)

9.6 State Graph of the Start-up Phases


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


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

9.7 Static Local Configuration of an RFP (OM Configurator)

As an alternative to DHCP configuration, the RFPs/OMM may be individually statically configured using the OM Configurator tool.

Note: The OM Configurator requires the Java Runtime Environment version 1.6 or higher.

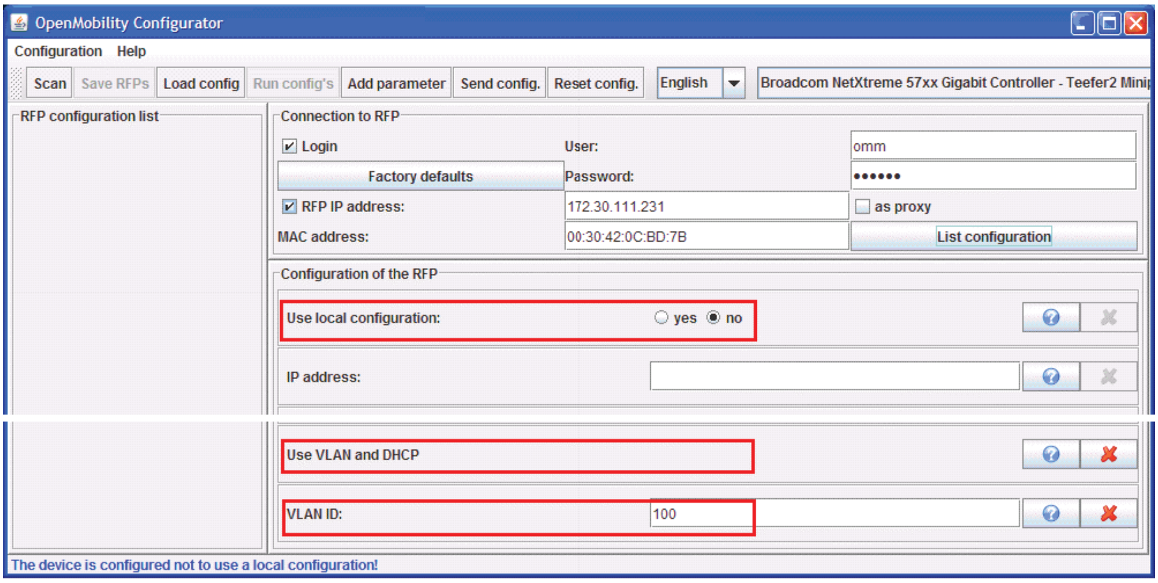
The settings, which are configured on the RFP with the tool OM Configurator, will be saved permanently in the internal flash memory of the RFP.

Note: An initial configuration of the RFPs (L) 35/36/37 IP / RFP (L) 43 WLAN via the OM Configurator tool requires a login and password. The default login and password is “omm” and “omm”. No login is required for the initial configuration of the previous RFP family (RFPs (L) 32/34 IP / RFP (L) 42 WLAN.

With the launch of SIP–DECT 3.0 the appropriate OM Configurator especially for the stream ‘SIP-DECT’ must be used for the local configuration of RFPs.

There are two modes of operation.

- The OM Configurator is used to set a VLAN ID but other parameters are still requested via DHCP.



☑ Login User: omm

Password: ••••••

☑ RFP IP address: 172.30.111.231 ☐ as proxy

MAC address: 00:30:42:0C:BD:7B

Use local configuration: ○ yes ● no

IP address:

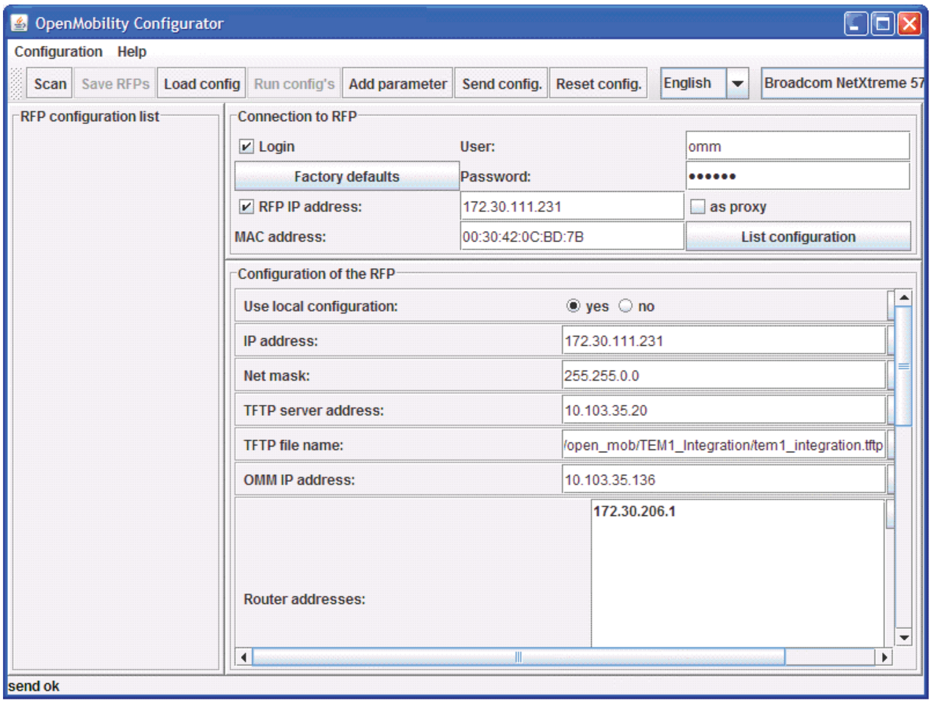
Use VLAN and DHCP

VLAN ID: 100

The device is configured not to use a local configuration!

OR

- All parameters are set via the OM Configurator and DHCP is not used anymore. The parameters configurable via the OM Configurator comply with the DHCP option, please see chapter 9.5.4 for details.



English

Broadcom NetXtreme 57

RFP configuration list

Connection to RFP

☑ Login User: omm

Password: ••••••

☑ RFP IP address: 172.30.111.231 □ as proxy

MAC address: 00:30:42:0C:BD:7B

Configuration of the RFP

Use local configuration: ● yes ○ no

IP address: 172.30.111.231

Net mask: 255.255.0.0

TFTP server address: 10.103.35.20

TFTP file name: /open_mob/TEM1_Integration/tem1_integration.tftp

OMM IP address: 10.103.35.136

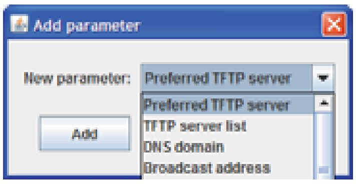
Router addresses: 172.30.206.1

send ok

On systems with multiple Ethernet adapters select the interface to use for the configuration of the RFPs. To configure an RFP, at least the MAC address and all mandatory options (see table below) have to be set. The MAC address must be entered in a format such as xx-xx-xx-xx-xx-xx.

If the RFP has already an IP address, enter this address in the IP address field. In this case you can reach the RFP from outside the local LAN segment. This setting is optional.

To set additional parameters, press the **Add parameter** button and choose the desired parameter.



New parameter: Preferred TFTP server

Please note: Select the **yes** checkbox for the RFP to **Use local configuration** otherwise DHCP will be used.

Press the **Send configuration** button to transmit the parameters to an RFP.

Boot parameters (comply with DCHP options)

Parameter	Type	Meaning
Use local configuration	mandatory	The parameter defines whether the local configuration settings should be used when booting or not.
IP Address	mandatory	IP address of the RFP
Net mask	mandatory	Subnet mask of the IP network

TFTP Server Address	Only mandatory for RFP (L) 32/34 IP / RFP (L) 42 WLAN because of the NETBOOT process; Optional for RFP (L) 35/36/37 IP / RFP (L) 42 WLAN SW update	IP address of the TFTP server, set to 0.0.0.0 is not used
TFTP File Name	Only mandatory for RFP (L) 32/34 IP / RFP (L) 42 WLAN because of the NETBOOT process; Optional for RFP (L) 35/36/37 IP / RFP (L) 42 WLAN SW update	The boot file be read from the TFTP server.
TFTP server list	Only used by the RFP (L) 32/34 IP / RFP (L) 42 WLAN, optional	List of additional TFTP servers to load the boot file
Preferred TFTP server	Only used by the RFP (L) 32/34 IP / RFP (L) 42 WLAN, optional	Try to load the boot file from 'TFTP Server Address' as first.
OMM IP Address	mandatory	IP address of the OpenMobility Manager
Router addresses	optional	IP address of Default gateway
DNS Addresses	optional	IP address of DNS server
DNS Domain	optional	Domain name of the network
Broadcast Address	optional	The broadcast address for that network
2nd OMM IP Address	optional	IP address of the standby OMM
Country	optional	Defines the country in which the OMM resides to handle country specific call progress tones.
NTP Server Address	optional	IP address of an NTP Server
NTP Server Name	optional	Name of an NTP Server
VLAN ID	optional	VLAN identifier
Use VLAN and DHCP	optional	The parameter defines whether only the local VLAN configuration settings should be used when booting or not.
Syslog IP Address	optional	Destination IP address for the syslog
Syslog Port	optional	Destination port for the syslog
Restore URL	optional	URL for an automatic OMM Database import (see chapter 7.4.6.2 and

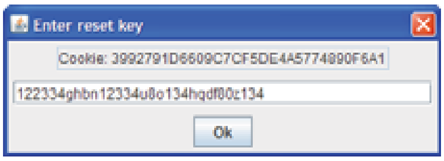
		chapter 8.5.5.1)
Configuration file server	optional	URL of a server with configuration files (ipdect.cfg|<mac>.cfg) alternatively/in addition to OM Configurator settings. Syntax: {ftp|ftps|http|https}://[user:password@] server/[directory/] or tftp://server/[directory/]
Core dump* * can not be set via DHCP	optional	In case of an system error the RFP creates core dump files and transfers them using TFTP to the folder configured in the TFTP file name.

The configuration can only be set after powering up or at the retry phase (LED flashing 0.25 Hz) or in kernel mode, please see chapter 9.5 for details. The OM Configurator tool waits 2 seconds and retries transmitting the data 3 times.

If you want to read the configuration parameters from an RFP, set the MAC address and the IP address additionally and press the **List configuration** button. All parameters will be listed in the OM Configurator tool.

Press the **Reset configuration** button to clean all input fields and additional parameters.

Since the OpenMobility version 1.5, login data can be used to prevent against unauthorized configuration changes. If authorization is used, mark the **Login** checkbox and enter the user name and the password into the fields **User** and **Password**. This OM Configurator is backward compatible to previous OpenMobility versions without login support.



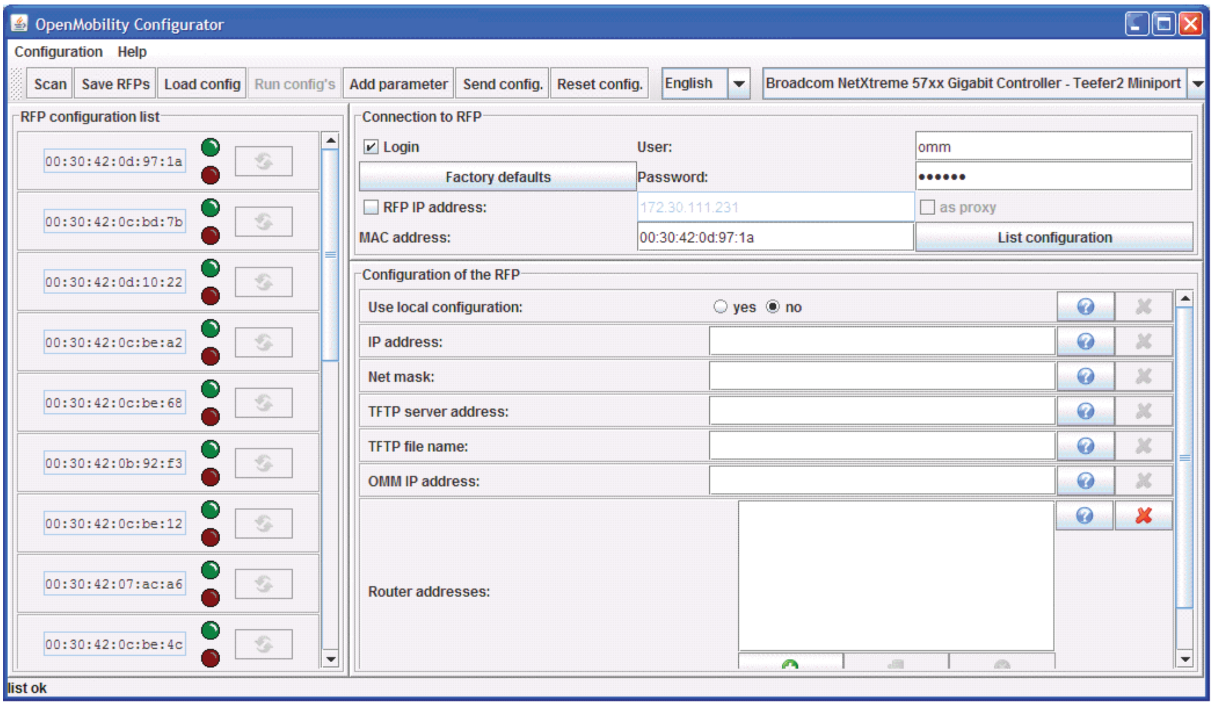
Cookie: 3992791D6609C7CF5DE4A5774890F6A1

122334ghbn12334u8o134hqdf80z134

A forgotten password could not be recovered but deleted using the **Factory defaults** button. Send the displayed cookie to the OpenMobility manufacturer support. After receiving the password reset key from the support, enter it into the **Enter reset key** dialog. This will delete the complete local configurations from the internal flash memory of the RFP, too!

Please note: With the password reset all local configurations inclusively possible existing OpenMobility configurations will be deleted.

An RFP outside the local LAN segment could also work as proxy. Mark the **as proxy** checkbox to enable this functionality. Then the MAC address will be used to address an RFP in the LAN segment of the proxy RFP. Scanning for available RFPs and configuration of multiple RFPs via a configuration file could be used also with the proxy mechanism.



English
Broadcom NetXtreme 57xx Gigabit Controller - Teefer2 Miniport

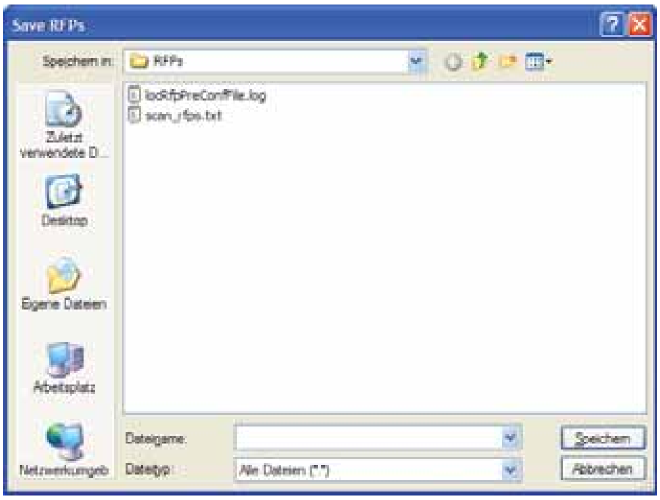
00:30:42:0d:97:1a
00:30:42:0c:bd:7b
00:30:42:0d:10:22
00:30:42:0c:be:a2
00:30:42:0c:be:68
00:30:42:0b:92:f3
00:30:42:0c:be:12
00:30:42:07:ac:a6
00:30:42:0c:be:4c

☑ Login
User: omm
Password: ••••••
□ RFP IP address: 172.30.111.231 □ as proxy
MAC address: 00:30:42:0d:97:1a

Use local configuration: ○ yes ● no
IP address:
Net mask:
TFTP server address:
TFTP file name:
OMM IP address:
Router addresses:

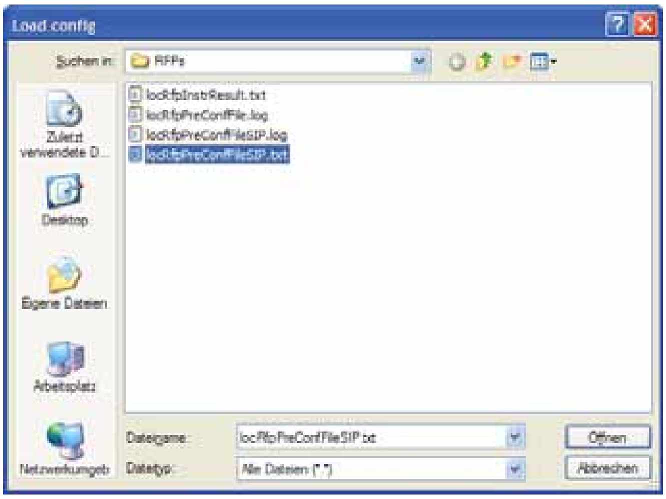
list ok

Use the **Scan** button to search for available RFPs in the local LAN segment or via the proxy mechanism in outside LAN segments. All MAC addresses of the found RFPs will be displayed in the left RFP list. The status LEDs and the update button are disabled after scanning for RFPs.



Speichern in: RFPs
lockRfpPreConfFile.log
scan_rfps.txt
Dateiname:
Dateityp: Alle Dateien (*.*)

The list of RFPs could be saved by using the **Save RFPs** button. This enables an administrator to edit the configuration data of multiple RFPs via a text editor or a spread sheet application like described in section 11.7.3.

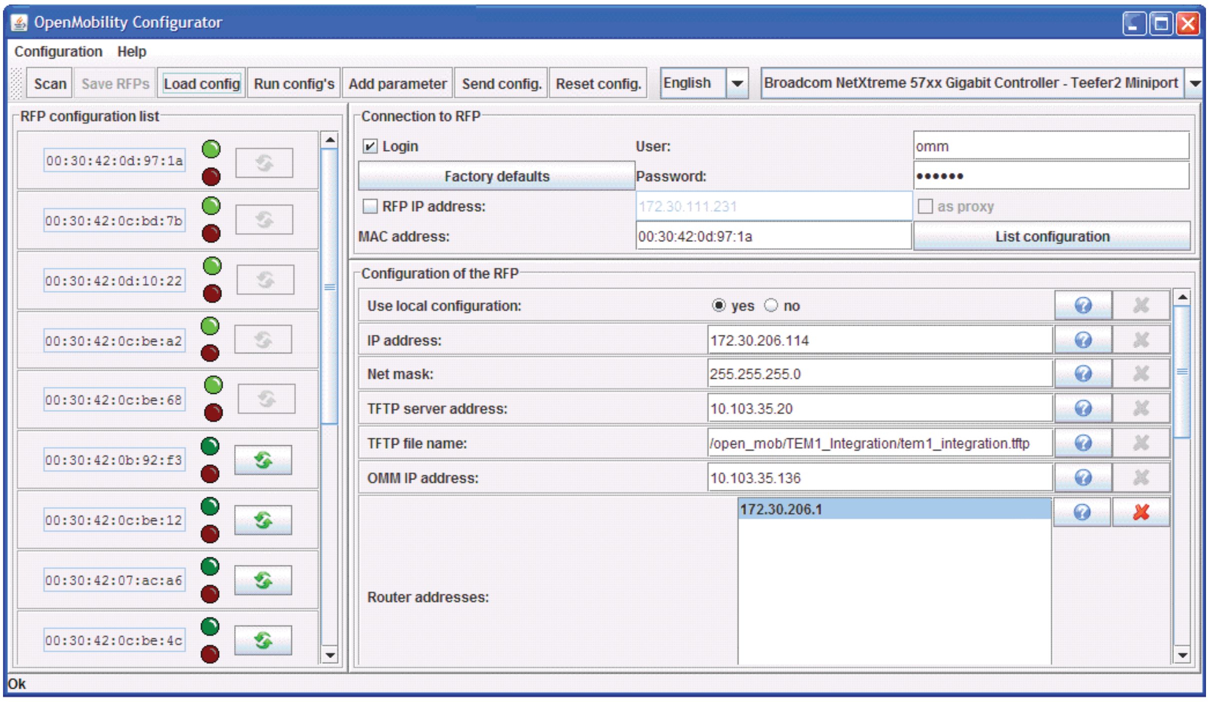


Suchen in: RFPs

locRfpInstResult.txt
locRfpPreConfFile.log
locRfpPreConfFileSIP.log
locRfpPreConfFileSIP.txt

Dateiname: locRfpPreConfFileSIP.txt
Dateityp: Alle Dateien (*.*)

The prepared configuration file can be loaded using the **Load config.** button. Log files with status information about parsing and executing the configuration file and data are stored into the same directory.



English

Broadcom NetXtreme 57xx Gigabit Controller - Teefer2 Miniport

RFP configuration list:

- 00:30:42:0d:97:1a
- 00:30:42:0c:bd:7b
- 00:30:42:0d:10:22
- 00:30:42:0c:be:a2
- 00:30:42:0c:be:68
- 00:30:42:0b:92:f3
- 00:30:42:0c:be:12
- 00:30:42:07:ac:a6
- 00:30:42:0c:be:4c

☑ Login User: omm
Password: ••••••
☐ RFP IP address: 172.30.111.231 ☐ as proxy
MAC address: 00:30:42:0d:97:1a

Use local configuration:	● yes ○ no
IP address:	172.30.206.114
Net mask:	255.255.255.0
TFTP server address:	10.103.35.20
TFTP file name:	/open_mob/TEM1_Integration/tem1_integration.tftp
OMM IP address:	10.103.35.136
Router addresses:	172.30.206.1

Ok

Use the **Run configs** button to start the iterative configuration of multiple RFPs using the prepared and loaded configuration file. The LEDs will display whether the configuration has succeeded or failed. See the log file content for further information. If the configuration has failed for an RFP, the configuration could be repeated using the update button beside the LEDs.

Note:	Note that the login and proxy data will be used for the whole configuration file!

9.8 RFP Configuration Files

RFP (L) 35/36/37 IP / RFP (L) 43 WLAN configuration files

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

```
OM_SwImageUrl=ftp://172.30.207.21/openmobility/SIP-DECT_3.0.dnld
```

TFTP, FTP(S), HTTP(S) are supported for an RFP (L) 35/36/37 IP / RFP (L) 43 WLAN software update, please see section 9.11.5.

RFP (L) 32/34 IP / RFP (L) 42 WLAN configuration files

IP-RFPs support two RFP configuration files which are downloaded from a server to get configuration settings. There is one common file “ipdect.cfg” for all RFPs and there is one file specific file “<MAC>.cfg” for every single IP-RFP. The RFP requests the “ipdect.cfg” file if an URL is given. The RFP specific <MAC>.cfg is requested if this is indicated in the common “ipdect.cfg” file. It is possible that all RFPs request “ipdect.cfg” and only selected RFPs request the <MAC>.cfg to have a specific configuration on some RFPs.

Standard IP settings

Standard IP settings which are necessary to have access to the RFP configuration files are configured via DHCP (see chapter 9.5) or OM Configurator (see chapter 9.6). These are:

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

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

Configuration file source

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

Syntax:

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

The URL configuration is done via DHCP option code 66 or the OM Configurator.

- “ipdect.cfg” is mandatory if an URL is given by DHCP option code 66 or local static configuration via the OM Configurator.

- “<MAC>.cfg” is mandatory if it is indicated in the “ipdect.cfg” that a “<MAC>.cfg” exists for the RFP. (There is a key word to indicated that a “<MAC>.cfg” exists for every RFP.)

Mandatory means: if a file can not be loaded then the RFP will not start. This is relevant for the following scenarios:

- RFP boot / startup (after power on, SW update, …),
- a change of the URL.

Parameter settings priority

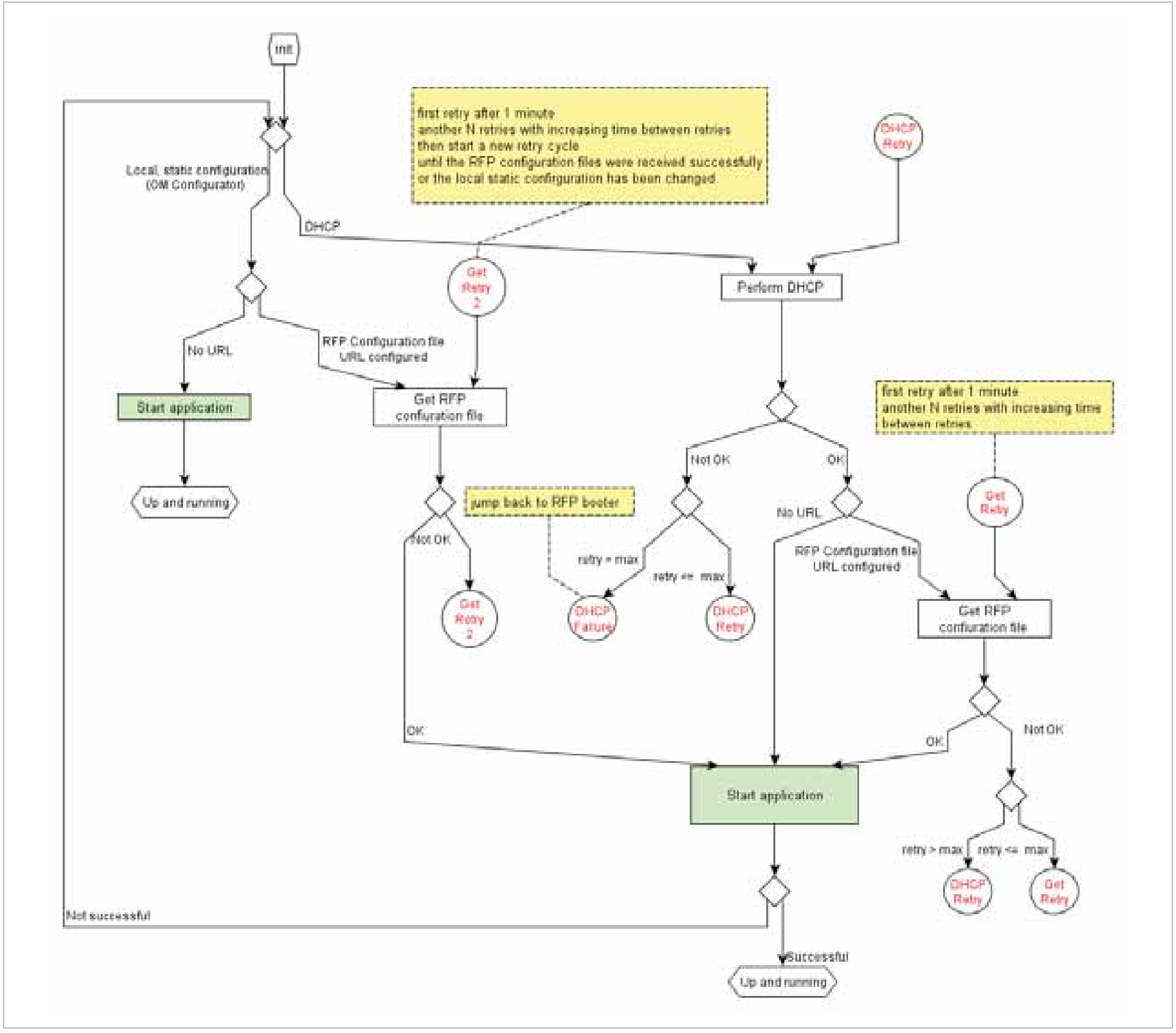
Some parameters can be set via DHCP / OM Configurator or by using the files “ipdect.cfg” or “<MAC>.cfg”. If a parameter is provided by more than one of the possible ways, the last setting has priority. There is the following order:

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

It is also possible to remove settings.

Times when RFP configuration times are read

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


init
Local, static configuration
(OM Configurator)
DHCP
first retry after 1 minute
another N retries with increasing time between retries
then start a new retry cycle
until the RFP configuration files were received successfully
or the local static configuration has been changed
DHCP Retry
Get Retry 2
Perform DHCP
No URL
RFP Configuration file URL configured
Start application
Get RFP confiuration file
Up and running
first retry after 1 minute
another N retries with increasing time between retries
Not OK
OK
jump back to RFP booter
Not OK
retry = max
retry <= max
No URL
RFP Configuration file URL configured
Get Retry
Get Retry 2
DHCP Failure
DHCP Retry
Get RFP confiuration file
OK
OK
Not OK
Start application
retry > max
retry <= max
DHCP Retry
Get Retry
Not successful
Successful
Up and running

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

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

RFP configuration file update check

RFP configuration file update check has the following characteristics:

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

What if the configuration file(s) cannot be retrieved

- The RFP continues operation with the last successfully retrieved configuration file(s).
- The RFP will retry to get the configuration files, starting with an interval of 1 minute and doubling this interval with each retry, not exceeding the update check interval (either default or configured).
- If the RFP is using DHCP, a renew of the lease is scheduled so that possible changes in DHCP configuration will be detected.
- Failures in getting the configuration files is reported via Syslog.

Handling of parameter changes

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

> **Example 1:**
> IP address of a Syslog Daemon has been changed in “ipdect.cfg” but is covered up by “<MAC>.cfg” in which this parameter has not been changed.
>
> **Example 2:**
> A parameter is new in “<MAC>.cfg” but has been set previously in “ipdect.cfg” with the same parameter value.

Only if a parameter change causes a change of RFP configuration as a sum of e.g. DHCP / OM Configurator, “ipdect.cfg” and “<MAC>.cfg” then the RFP will perform an configuration update procedure.

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

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

Configuration file syntax

```
##############################################################################
# sample configuration file for the OpenMobility system
# retrieved via the net using file transfer protocols
# like tftp, ftp or http
#
##############################################################################
# comments are starting with the hash sign: "#"
#
##############################################################################
##
# BOOL variables support the following values
# YES Y 1 TRUE (case does not matter)
# NO  N 0 FALSE (case does not matter)
# other values are interpreted as false
#
##############################################################################
# configuration files check interval
# time interval for checking the remote cfg files in seconds
# minimum value is 300   (5 minutes)
# maximum value is 604800 (7 days)
OM_ConfigCheckInterval=500
##############################################################################
# personal configuration files
# personal configuration files have the following name
# <OWN-MAC>.cfg, where <OWN-MAC>.cfg is of the form
# e.g. 003042ABCDEF.cfg

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

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

# DO NOT load the individual file for the RFP with mac 003042ABCDEF
# no matter what OM_PersonalConfigAll says
OM_PersonalConfig_003042ABCDEF=n # BOOL
##############################################################################
# OpenMobility system
# the OpenMobilityManager IP addresses
OM_ManagerIpAddress1=172.30.205.17
OM_ManagerIpAddress2=172.30.205.18

OM_ManagerRestoreDbUrl=ftp://172.30.207.21/pub/backup.txt
OM_ManagerCountry=2
##############################################################################
# SYSLOG
OM_SyslogIpAddress=172.30.207.20
OM_SyslogPort=10115
##############################################################################
# NTP
OM_NtpServerName=de.pool.ntp.org
OM_NtpServerIPAddress=131.188.3.220 130.149.17.21
##############################################################################
# MISC
# transfer core files to the following url location
OM_CoreFileTransfer=ftp://172.30.206.21/pub          # currently not
implemented
##############################################################################
```

9.9 RFP (L) 35/36/37 IP / RFP (L) 43 WLAN Software Update

The software checks several locations for a software update (software different from the currently active software). If found then the software is copied to the flash leaving the running software intact. After successful installation the OMM is informed about the different software. Activation of the software is then managed by the active OMM. RFPs that do not have a connection to the OMM activate and start the software immediately.

Locations for SW update are:

- Attached USB mass storage device with a software image **iprfp3g.dnld** in its root. The USB mass storage device must be formatted using the vfat32 file system.
- If ipdect.cfg supplies the **OM_SwImageUrl** variable then the URI is used to get the boot image. Please see chapter 9.8.
- TFTP server, path and file configured using the OM Configurator or via DHCP.

9.10 802.1Q Support

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

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

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

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

VLAN implementation notes referring to IP RFPs:

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

Why not VLAN ID 0 ?

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

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

9.10.1 Boot Phase of IP RFPs (DHCP)

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

Step A. DHCP scope within the native VLAN:

1 IP RFP boots up and obtains an address on the native VLAN.

2 The data VLAN DHCP option 132 directs the IP RFP to go to voice VLAN.

Step B. DHCP scope within the voice VLAN:

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

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

2 IP RFP is operational on the voice VLAN.

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

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

To avoid the DHCP scope within the native VLAN the VLAN ID to be used can be set permanently via OMC without losing the ability to provide other parameter via DHCP, please see section 0 Static Local Configuration Of An RFP.

9.10.2 Boot Phase of IP RFPs (Local Configuration)

The PC running the OM Configurator has to be a member of the native VLAN for the 1st configuration, later on within the voice VLAN set.

If a wrong or unknown VLAN ID is set, you can overwrite or read the configuration using no VLAN tag on the switch port in the first 6 seconds after the RFP is connected to a power supply / PoE. After 6 seconds the RFP apply the local configurations and start using the parameters.

9.11 Installing OMM in Host Mode

In this case the OMM software has to be installed on a PC running with Red Hat Linux. The network parameters with which the OMM works in this mode depend on this PC's network configuration.

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

Please note: Check that the versions of the OMM and RFP software on your SIP–DECT installation are the same. Note that the OMM in host mode is not supported on virtual machines.

9.11.1 System Requirements

The Linux PC OMM requires the following configuration:

- Red Hat© Enterprise Linux 6 for x86 server
- Server HW minimum:
  - Processor : Dual Core Intel® Xeon® 3065, 2.33GHz, 4MB cache
  - Bus 1333 MHz
  - Memory : 2GB DDR2 SDRAM 667 MHz
  - Hard disk: 80 GB SATA 7200 rpm
  - 1 Gbit/s Ethernet interface

9.11.2 Installing the OMM Software

The OMM software for Linux Redhat x86 server is provided in form of a self-extracting executable file e.g. “SIP-DECT_3.0.bin”. This binary file comprises two Red Hat© packages:

- SIP-DECT-OMM-<*SIP-DECT-version*>.i586.rpm
  OpenMobility Manager software.
- SIP-DECT -HANDSET-<handset-version>.i586.rpm
  Software for Aastra 610d/620d/630d and Aastra 650c handsets

The Aastra 610d/620d/630d and Aastra 650c handset software can be updated via the Air interface, see chapter 9.17. A separate software package can also be provided for specific updates of the handset software.

IMPORTANT : Log on as user root to install and/or update OMM. If you do not login as root to open the OMM console, the path to ommconsole is not set and you have to enter the whole path “/usr/sbin/ommconsole” to start the OMM console.

Command syntax

For extraction and automatic standard installation
SIP-DECT_3.0.bin

For extraction and automatic standard installation
SIP-DECT_3.0.bin -f

For extraction of RFP packages only
SIP-DECT_3.0.bin –x

RPM packages can also be installed manually.

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

For an OMM software update (see chapter 9.12)
rpm –U SIP-DECT-OMM-<version>.i586.rpm

For Aastra 610d/620d/630d and Aastra 650c handset software installation
rpm –i SIP-DECT-HANDSET-<version>.i586.rpm

To delete a software release

rpm –e SIP-DECT-HANDSET and
rpm –e SIP-DECT-OMM

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

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

9.11.3 Configuring the Start Parameters

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

```
##############################################
# OMM configuration file
##############################################
# if you use a different interface for omm  activate/correct parameter below
#OMM_IF="eth0"
#
OMM_CONFIG_FILE=/opt/SIP-DECT/tmp/omm_conf.txt
#
#if you use OMM resiliency for OMM activate parameter below with OMMs IP
adresses
#OMM_RESILIENCY="192.168.0.1:192.168.0.2"
#
# Automatic OMM database import:
# TFTP / FTP  / HTTP(S) URL specifies the import server and file
#RST_URL=ftp://download-url.com/directory/file.dat
# country tones:
#  VS_COUNTRY_DEU = 1,  VS_COUNTRY_GBR = 2,  VS_COUNTRY_CHE = 3,
VS_COUNTRY_ESP = 4, VS_COUNTRY_FRA = 5, VS_COUNTRY_ITA = 6,
#  VS_COUNTRY_RUS = 7,  VS_COUNTRY_BEL = 8,  VS_COUNTRY_NLD = 9,
VS_COUNTRY_CZE = 10, VS_COUNTRY_AUT = 11, VS_COUNTRY_DNK = 12,
#  VS_COUNTRY_SVK = 13, VS_COUNTRY_FIN = 14, VS_COUNTRY_HUN = 15,
VS_COUNTRY_POL = 16, VS_COUNTRY_BLR = 17, VS_COUNTRY_EST = 18,
#  VS_COUNTRY_LVA = 19, VS_COUNTRY_LTU = 20, VS_COUNTRY_UKR = 21,
VS_COUNTRY_NOR = 22,  VS_COUNTRY_EUN = 23, VS_COUNTRY_SWE = 24,
#  VS_COUNTRY_TWN = 25
COUNTRY="2"
```

Parameters	Description
OMM_IF	Interface for communicating with the RFPs (by default: eth0)
OMM_CONFIG_FILE	Directory containing the OMM configuration file (by default: /etc/omm_conf.txt)
OMM_RESILIENCY	In case of OMM redundancy, enter the two IP addresses of the OMMs. See also section 9.13.
Restore URL	Restore URL for an automatic OMM database import (see chapter 7.4.6.2)
COUNTRY	Country tone schema

9.11.4 Specific Commands – Troubleshooting

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

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

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

Malfunction

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

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

9.11.5 Upgrade from OMM Version 2.x to 3.x in Host Mode

To update a OMM system from version 2.x to 3.x, you must delete the old OMM software package **rpm –e omm_ffsip-OMM omm_ffsip-HANDSET** and install the **SIP-DECT_3.0.bin** software.

In this case the installation routine copies automaticly the OMM database.
If there are changes in start parameters you can copy the old saved config file from /etc/sysconfig/omm_ffsip.rpmsave to /etc/sysconfig/SIP-DECT.

9.12 Updating the OMM

To prevent a full breakdown of the DECT network for large systems during an update, a new mechanism has been introduced.

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

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

The OMM “standby” feature is described in section 9.13.

Especially for installations using a standby OMM this new update mechanism allows an update of the RFPs with a minimum impact to the DECT services.

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

- the DHCP lease is refreshed,
- the RFP lost the connection to the OMM,
- one of the service applications running on the RFP must be restarted, and
- an RFP configuration file update check is done (see chapter 9.8).

As soon as an RFP detects a new boot image file on the TFTP server it notifies this to the OMM. The OMM keeps track when it is save to restart an RFP in order to leave the DECT service synchronal.

RFPs scheduled for restart are marked with a yellow sign within the Web service (see chapter 7.6.1) or in a separate column within the OM Management Portal (OMP), see chapter 8.7.1.1.

9.12.1 Updating a Single OMM Installation

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

Please note: Updating a single OMM installation will cause a breakdown of the DECT network during the update procedure.

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

OMM in RFP mode

If the OMM is running on an RFP force the update of this RFP by pressing the **Update** button on the **System settings** web page (see chapter 7.4.1.2). The RFP checks the boot image file on the TFTP server and reboots if a new one is found.

OMM in host mode (on Linux PC)

If the OMM is running on a dedicated Linux PC, install the new software as described in section 9.11.2 on that PC with the command "**SIP-DECT_3.0.bin**". This stops automatically the running OMM and installs the new software. After the installation phase, restart the OMM by running the command "**/etc/init.d/sip-dect-omm start**".

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

9.12.2 Updating a Standby OMM Installation

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

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

OMM in RFP mode

Force the update by pressing the **Update** button on the **System settings** web page (see chapter 7.4.1.2). The OMM-RFP checks the boot image file on the TFTP server and initiates an update procedure, if a new image file has been found. The automated update procedure performs the following steps:

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

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

Please note: Please be aware that a minimum downtime of the system can only be reached if the system was in a stable working state when initiating the update and the IP infrastruckture guarantees a fast update of the OMM RFPs e.g. no 64kbit/s line to donload the SW into the RFP. A RFP typically laods the SW from a server within 12 seconds in a LAN environment.

OMM in host mode (on Linux PC)

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

1. Replace the boot image file on the TFTP server(s).
2. Manually update the standby OMM.
   a) Stop the OMM service.
   b) Install the new SW.

c) Start the OMM service.

d) Wait at least 30 seconds before you go on with updating the active OMM.

3 Manually update the active OMM.

a) Stop the OMM service.

b) Install the new SW.

c) Wait at least 30 seconds.

d) Start the OMM service.

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

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

9.13 OMM Standby

To perform OMM standby, two OpenMobility Managers have to be provided in an OMM network. One is working as the active OMM, and the other one is working as the standby OMM.

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

How OMM Standby Works

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

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

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

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

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

9.13.1 Configuring OMM Standby

Each RFP of the DECT system have to be configured with two OMM IP addresses. This both OMM addresses can be either configured via DHCP (see chapter 9.5.1) or with the OM Configurator (see chapter 9.6).

9.13.2 Fail Over Situations

Fail over occurs under following circumstances:

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

The standby OMM becomes the active OMM under following circumstances:

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

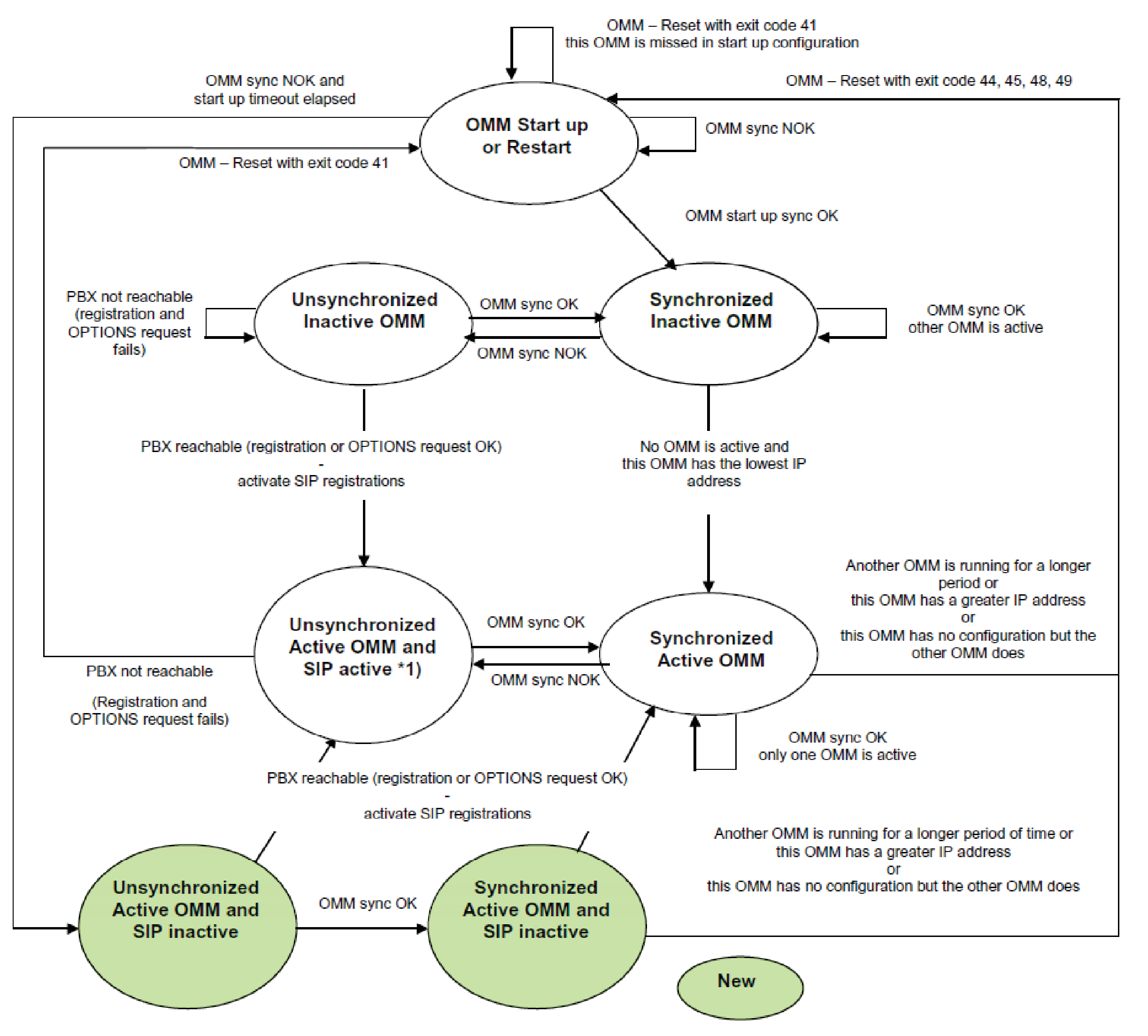
When the OMMs get in contact again:

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

9.13.3 Fail Over Failure Situations

Fail over failure occurs under following circumstances: The IP connection between OMMs fails and the configured SIP Proxy/Registrar is unreachable. In this case the active OMM shall wait until the SIP Proxy/Registrar is reachable.

The following state diagram shows the OMM Standby states:



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

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

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

With these new states ("… SIP inactive") the OMM standby mechanism takes care in the start up phase that all SIP users does not become active if the PBX is not reachable. This avoids a possible double SIP registration when the PBX and the other OMM is reachable again before both OMMs negotiate with each other which OMM becomes the active one.

The double SIP registrations might cause a user not to be reachable when his latest SIP registration came from that OMM that was negotiated to be the inactive one and the SIP registrar cannot handle 2 or more simultaneous registrations (non-forking proxy).

9.13.4 Specific Standby Situations

Some aspects have to looked at in case of OMM state changes when they are unsynchronized.

9.13.4.1 How A Standby OMM Becomes Active

As the above figure shows in case of an unsynchronized OMM state the standby OMM has to decide whether to become active or not.

For this purpose the OMM tries to contact the configured SIP proxy and registrar. The OMM starts a SIP registration for the handset with the lowest phone number and sends an OPTIONS request to the configured proxy. If there is an answer the SIP proxy/registrar will be considered as reachable and the OMM becomes active.

9.13.4.2 Handling When Both OMMs Are Not Synchronized

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

The Web service will warn with the warning “No Standby” for both OMMs in this situation and possible made configuration changes are not save.

In any case, when both OMMs get in contact again with each other, the longer running one becomes the active one and that will overwrite the database file in the standby OMM. Configurations made in this becoming standby OMM would be lost!

9.13.4.3 Two DECT Air Interfaces

In case of both OMMs are in an unsynchronized and active state they are fully working. RFPs which lose connection to the OMM because of the network break down might connect to the other OMM. Two DECT air interfaces will be present but are working parallel.

Note: Both air interfaces are using the same PARK. So it can not determined to which OMM a location registration succeeds.

For PPs different situations are possible:

- They do not notice this situation:
  - active calls stay established, depending on network conditions;
  - PPs can make and receive new calls, depending on an available PBX connection;
  - PPs can do handover to RFPs connected to the same OMM;
  - PPs can call PPs that are registered to the other OMM
- They lose their RFP base station and perform a new location registration:
  - active calls are broken;
  - PPs can make and receive new calls, depending on an available PBX connection;
  - PPs can do handover to RFPs connected to the same OMM;
  - PPs can call PPs that are registered to the other OMM;

- They lose their RFP base station and search the DECT network without finding another one:
  - active calls are broken;
  - PPs stay in searching for network until an air interface is available again.

Note: Handover between PPs located to RFPs which are controlled by different OMMs is not possible.

When the OMMs get in contact again with each other this inconsistent OpenMobility system situation will end.

9.14 Managing Account Data for System Access

Each RFP provides different independent access types:

- the OMM Web service/HTTPS interface (see chapter 7);
- the OMP (see chapter 8);

  The OMM Web service and the OMP are mainly used for configuration and administration.
- the OM Configurator (see chapter 9.6);

  The OM Configurator is mainly used for static local configuration of an RFP.
- the SSH user shell (see chapter 10.3.5).

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

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

The account data can be altered at the **User account** page of the OMM Web service (see chapter 7.4.3).

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

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

9.14.1 Account Types

There are three different account types:

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

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

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

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

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

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

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

9.14.2 Potential Pitfalls

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

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

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

9.15 WLAN Configuration (RFP (L) 42 WLAN / RFP (L) 43 WLAN only)

9.15.1 WLAN configuration steps

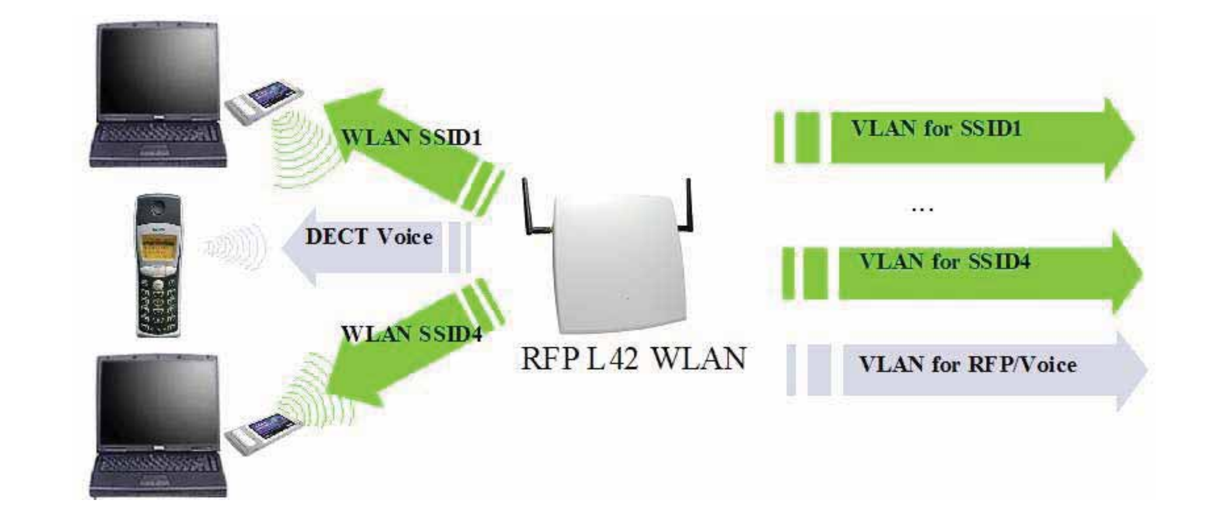
The correct configuration of an RFP with a WLAN interface requires the correct configuration of the DECT part. The second step is to specify the regulatory domain of the WLAN network at the **System settings** page of the OMM web service (see chapter 7.4.1).

Regulatory Domain	Country
0x10: FCC	USA, Australia
0x20: IC	Canada
0x30: ETSI	Europe (excluding Spain, France)

0x31: SPAIN	Spain
0x32: FRANCE	France
0x40: MKK	Japan
0x41: MKK1	Japan (MKK1)

This setting depends on the country and is prescribed by the laws of that country. Only the setting prescribed for that country must be used.

The third step is to specify the WLAN parameters in a profile (see chapter 7.8.1). The WLAN profile determines the name (SSID) of the WLAN network and other parameters. The encryption and authentication procedures are especially important and must be planned carefully beforehand.



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

Note: The RFP (L) 42 WLAN and RFP (L) 43 WLAN must be connected at least via a 100BaseT Ethernet link in order to activate the RFP’s WLAN function.

9.15.2 Optimizing the WLAN

Beacon Interval

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

RTS Threshold

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

Fragmentation Threshold

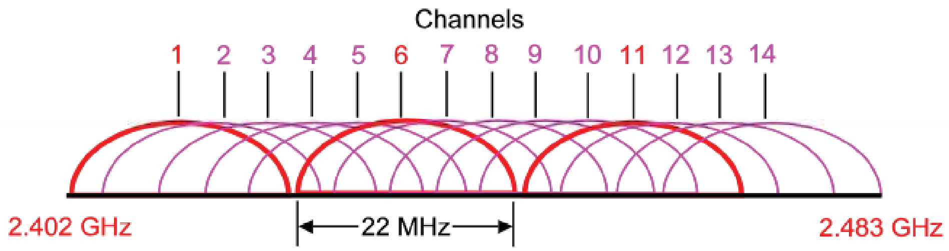
In environments where there is lot of interference and poor radio quality, reducing the fragment size below 1500 bytes can improve the effective throughput. However, transmitted data frames have to be fragmented, which means a higher load on the RFP's processor.

DTIM Period

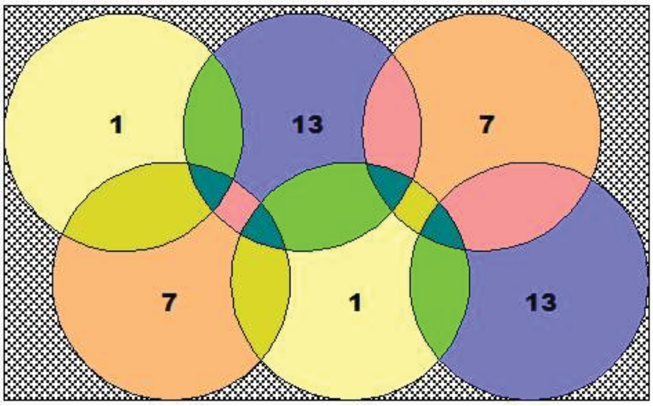
The DTIM period specifies the interval between transmissions of the broadcast and multicast packets. All WLAN clients must be active during this interval. Increasing the DTIM period lowers the clients power consumption slightly. Not all programs can manage the increase in response times, however.

Channel Allocation

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



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



9.15.3 Securing the WLAN

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

There are different encryption methods available which you configure within the WLAN profile (see chapter 7.8.1). However, only the recent WiFi protected access (WPA) encryption offers sufficient security against possible intruders. You should not use the (older) WEP encryption for your company LAN.

Especially with larger WLAN installations, the single shared secret offered by WPA-personal may not be sufficient for your security requirements, because any person that connects to the WLAN needs to know the same shared secret. For this reason, you should also setup RADIUS authentication that is supported by all RFP 42/L42 devices.

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

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

9.16 SNMP Configuration

To manage a larger RFP network, an SNMP agent is provided for each RFP. This will give alarm information and allow an SNMP management system (such as HP Open View) to manage this network. The SNMP agents can be configured in the SNMP menu of the OM Web service, see chapter 7.4.5.

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

The SNMP agent responds to SNMPv1-read and SNMPv2c-reads requests for the standard MIB-II objects. The Management Information Base (MIB-II) contains 11 object groups. The agent receives both SNMPv1 and SNMPv2c traps. It sends a “coldStart” trap when it first starts up. It also sends an enterprise-specific trap “nsNotifyShutdown” when it stops. When the SNMP agent receives an SNMP request using an unknown community name, it sends an “authenticationFailure” trap. The SNMP agent also generates an enterprise-specific trap “nsNotifyRestart” (rather than the standard “coldStart” or “warmStart” traps) after being re-configured.

9.17 Download Over Air

The “Download Over Air” feature allows updating the handset firmware without any user interaction or interruption of the telephony services over the existing DECT air interface. This features is currently available for the handset types Aastra 600d and Aastra 650c.

The PP firmware is part of each OpenMobility software package which is delivered by Aastra. The PP firmware is delivered in the package file “aafon6xxd.dnld”. This package file must be put on the same tftp server and path where the OMM-RFP gets his boot image file (e.g. iprfp3g.dnld).

9.17.1 How “Download Over Air” Works

If the “Download over Air” feature is activated, the OMM acts as a download server which provides the firmware for downloads.

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

The OMM takes care of the following download scenarios automatically:

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

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

The Aastra 610d/620d/630d/650c handsets have two partitions in the internal flash memory to hold 2 different software versions. During the download the new firmware is written to one partition and the PP is running from the other partition.

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

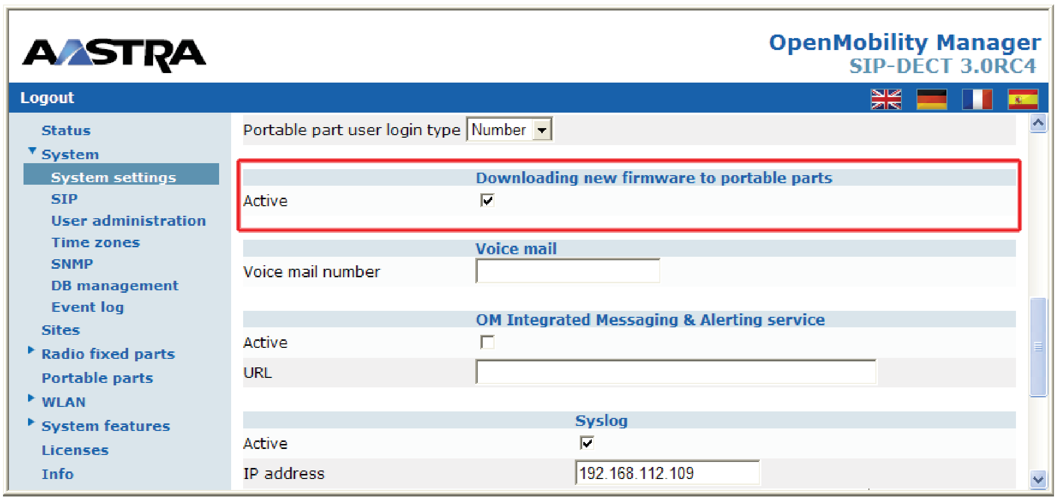
The download of a single PP with a firmware of 1 MB lasts approximately 90 minutes. The number of PPs which can be downloaded depends on the available system resources.

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

9.17.2 How to configure “Download Over Air”

In the following, the configuration of the “Download Over Air” feature is described by using the OM Web service. The feature can also be configured using the OM Management Portal (OMP). Therefore, links to the corresponding OMP settings are also given, but without screenshots.

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



Portable part user login type: Number

Downloading new firmware to portable parts
Active ☑

Voice mail
Voice mail number

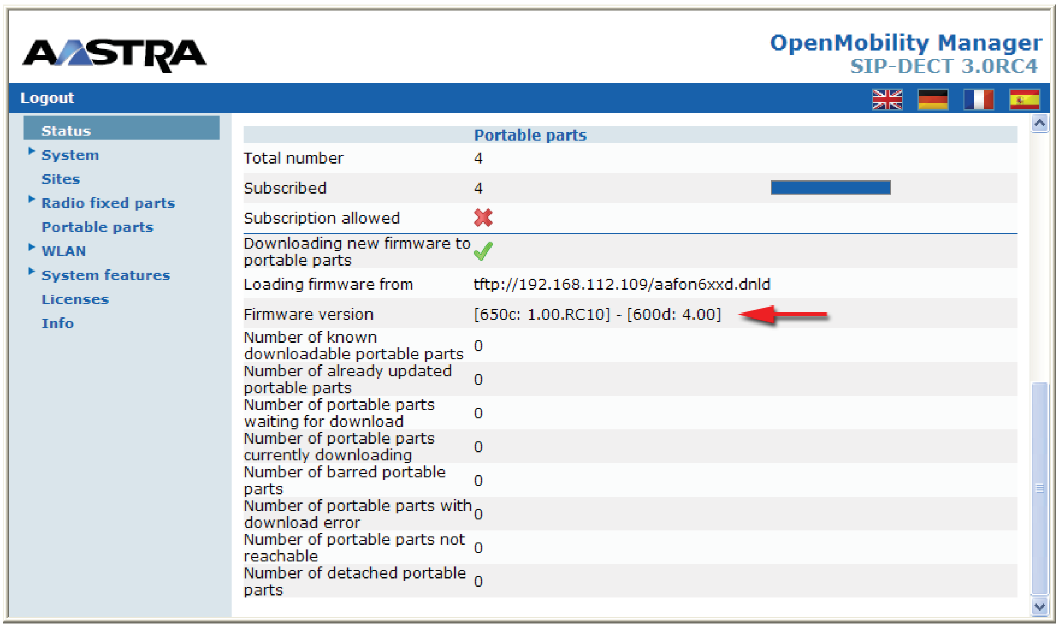
OM Integrated Messaging & Alerting service
Active □
URL

Syslog
Active ☑
IP address 192.168.112.109

In the OMP, the “Download over Air” feature is activated/deactivated in the **Miscellaneous** tab of the **Data management** menu (see chapter 8.5.5.6).

Please note: Before a new handset firmware package is put on a tftp server, the “Download over Air” feature must be deactivated. After the copy or installation the “Download over Air” feature can be activated again.

If the “Download over Air feature” is activated, the status of the “Download over Air” service together with some statistics is presented in the **Portable parts** section on the **Status** web page.

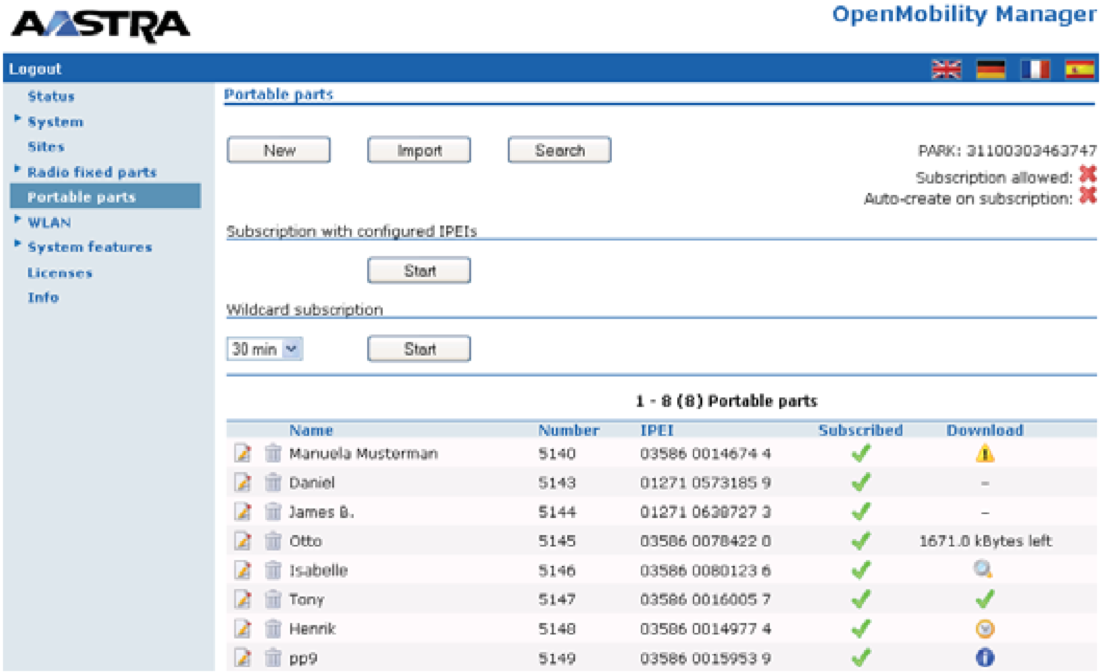


Portable parts	
Total number	4
Subscribed	4
Subscription allowed	✗
Downloading new firmware to portable parts	✓
Loading firmware from	tftp://192.168.112.109/aafon6xxd.dnld
Firmware version	[650c: 1.00.RC10] - [600d: 4.00]
Number of known downloadable portable parts	0
Number of already updated portable parts	0
Number of portable parts waiting for download	0
Number of portable parts currently downloading	0
Number of barred portable parts	0
Number of portable parts with download error	0
Number of portable parts not reachable	0
Number of detached portable parts	0

The handset firmware container for handset firmware update over the air includes packages for the Aastra 600d and Aastra 650c handsets. The available versions are also displayed on the **Status** web page.

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

The individual download status of each PP is presented on the **Portable part** web page.



PARK: 31100303463747
Subscription allowed: ✗
Auto-create on subscription: ✗

Subscription with configured IPEIs

Wildcard subscription

30 min

1 - 8 (8) Portable parts

Name	Number	IPEI	Subscribed	Download
Manuela Musterman	5140	03586 0014674 4	✓	⚠
Daniel	5143	01271 0573185 9	✓	-
James B.	5144	01271 0638727 3	✓	–
Otto	5145	03586 0078422 0	✓	1671.0 kBytes left
Isabelle	5146	03586 0080123 6	✓	🔍
Tony	5147	03586 0016005 7	✓	✓
Henrik	5148	03586 0014977 4	✓	◷
pp9	5149	03586 0015953 9	✓	ℹ

The different icons and texts of the **Download** column have the following meaning:

Icon	Meaning

-	Impossible to download the firmware to that handset (e.g. noAastra 610d/620d/630d/650c)
🔍	The PP is paged to establish a download connection. In case of a successful connection establishment the PP calculates the number of bytes to download. This may last several seconds.
xx kbytes left	The download is ongoing and xx kbytes are left.
✓	The firmware of this PP is up to date.
🕓	The PP is queued in the update-queue for updating (pending).
⚠	Warning. The download is barred because of one of the following reasons: – The PP is busy (temporary status). – The battery power is lower than 50% and the PP is not connected to the docking station or the USB-Interface. – This is not the master download system. A PP can be enrolled on several OpenMobility systems. The first system to which the handset will be enrolled is the “master system”. The PP downloads only from the “master system”. A different “master system” can be chosen inside the local menu of the handset. – The download is disabled in the local menu of the handset. The specific reason is shown as a tooltip.
⛔	Error The download failed because of one of the following reasons: – checksum error, – file system error, – error while writing firmware to flash, – version mismatch, – error while expanding firmware container. The specific reason is shown as a tooltip.
ℹ	Info The download is not possible because of: – the handset is not reachable, – the handset is detached. The specific reason is shown as a tooltip.

In the OMP, the “Download over Air” service status is displayed in the **Status** menu (see chapter 8.4).

10 Maintenance

10.1 Site Survey Measurement Equipment

If a SIP–DECT installation has to be planned, a sufficient distribution of the RFPs is necessary which fulfills the requirements for reliable synchronization and connectivity to the Portable Parts. 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 PPs with chargers.
- Battery chargers.
- Optional a measuring handset which can monitor other makers DECT radio sources.

10.2 Checking the Aastra DECT 142 / Aastra 142d Handset Firmware Version

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

1 Press the **Menu** soft key.

7 Select System (only to highlight).

8 Press OK.

9 Select Version Number.

10 Press OK.

The display will show the software and the hardware version of the Aastra DECT 142 / Aastra 142d handset.

10.3 Diagnostic

10.3.1 Aastra DECT 142 / Aastra 142d Site Survey Mode

You can set the Aastra DECT 142 / Aastra 142d handset in “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.

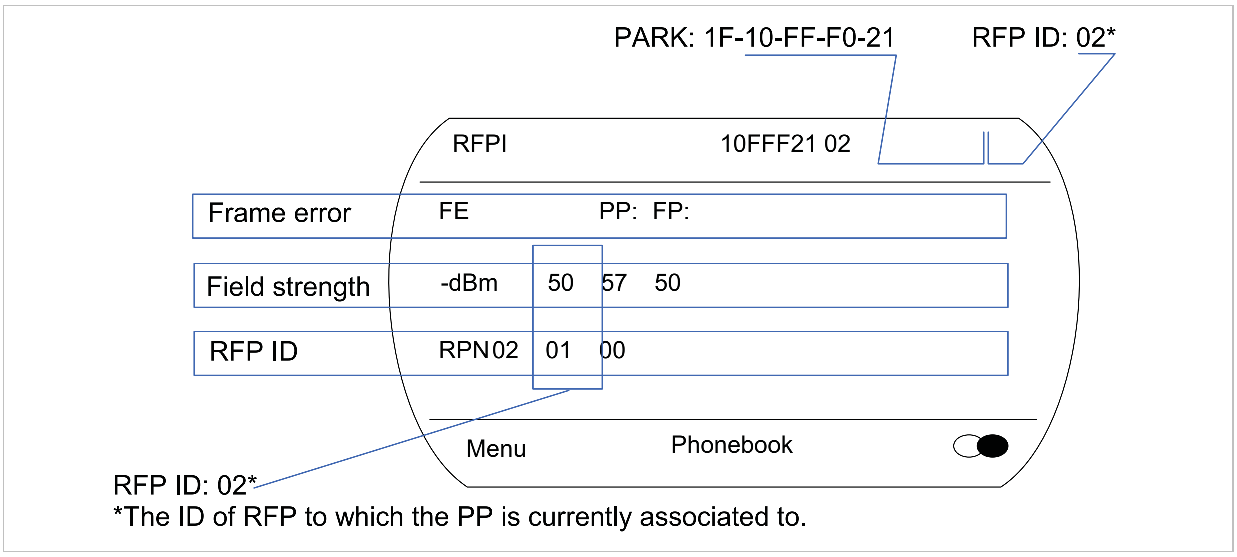
11 Enter the following key sequence “R***76#”.

12 Select Site Survey.

13 Press OK.

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

The following display is shown on the Aastra DECT 142 / Aastra 142d handset:



*The ID of RFP to which the PP is currently associated to.

In this example the PP 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.

10.3.2 Aastra DECT 142 / Aastra 142d Auto Call Test Mode

You can set the Aastra DECT 142 / Aastra 142d handset to “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.

15 Enter the following key sequence “R***76#”.

16 Select Auto Call Test.

17 Press OK.

18 Enter the phone number to call.

19 Press OK.

20 Enter a number of seconds between two calls.

21 Press OK.

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

23 Press OK. The test will be started automatically.

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

10.3.3 Aastra DECT 142 / Aastra 142d Auto Answer Test Mode

You can set the Aastra DECT 142 / Aastra 142d handset to “auto answer test mode” with a few keystrokes. In this mode the phone will answer incoming calls automatically. You can use this feature together with phones in the “auto call test mode” (see chapter 10.3.2) for test purposes. This mode is also active if the phone is on the charger.

1 Press the **Menu** soft key.

25 Enter the following key sequence “R***76#”.

26 Select Auto Answer.

27 Press OK.

28 Enter a number of seconds the phone shall ring before it will answer the call.

29 Press OK.

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

31 Press OK. The test will be started automatically.

32 To stop the test switch the phone off and on again.

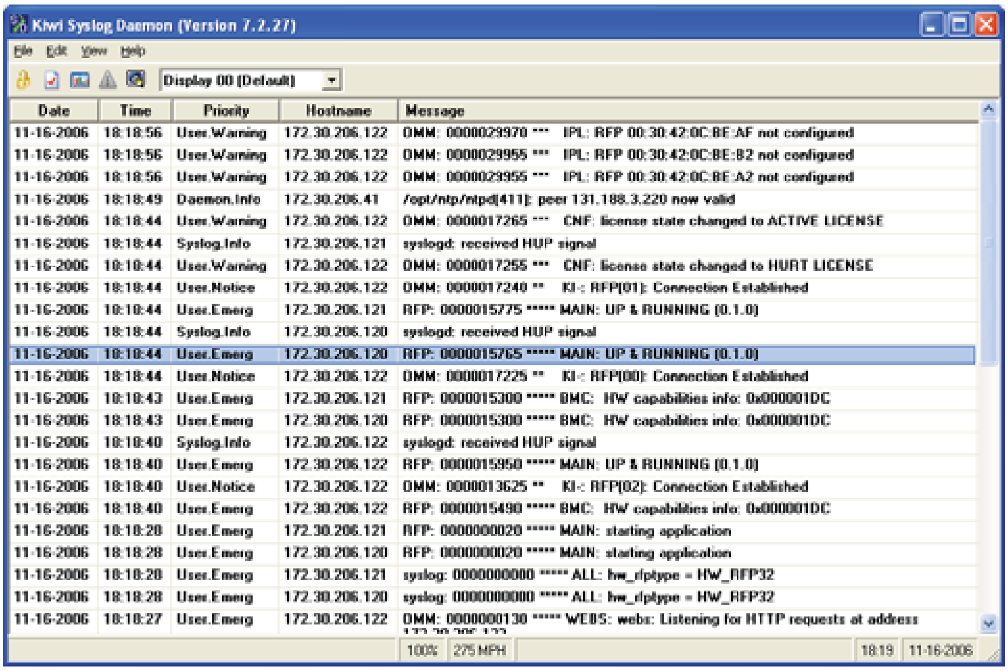
10.3.4 Syslog

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 has to 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.



Date	Time	Priority	Hostname	Message
11-16-2006	18:18:56	User.Warning	172.30.206.122	OMM: 0000029970 *** IPL: RFP 00:30:42:0C:BE:AF not configured
11-16-2006	18:18:56	User.Warning	172.30.206.122	OMM: 0000029955 *** IPL: RFP 00:30:42:0C:BE:B2 not configured
11-16-2006	18:18:56	User.Warning	172.30.206.122	OMM: 0000029955 *** IPL: RFP 00:30:42:0C:BE:A2 not configured
11-16-2006	18:18:49	Daemon.Info	172.30.206.41	/opt/ntp/ntpd[411]: peer 131.188.3.220 now valid
11-16-2006	18:18:44	User.Warning	172.30.206.122	OMM: 0000017265 *** CNF: license state changed to ACTIVE LICENSE
11-16-2006	18:18:44	Syslog.Info	172.30.206.121	syslogd: received HUP signal
11-16-2006	18:18:44	User.Warning	172.30.206.122	OMM: 0000017255 *** CNF: license state changed to HURT LICENSE
11-16-2006	18:18:44	User.Notice	172.30.206.122	OMM: 0000017240 ** KI-: RFP[01]: Connection Established
11-16-2006	18:18:44	User.Emerg	172.30.206.121	RFP: 0000015775 ***** MAIN: UP & RUNNING (0.1.0)
11-16-2006	18:18:44	Syslog.Info	172.30.206.120	syslogd: received HUP signal
11-16-2006	18:18:44	User.Emerg	172.30.206.120	RFP: 0000015765 ***** MAIN: UP & RUNNING (0.1.0)
11-16-2006	18:18:44	User.Notice	172.30.206.122	OMM: 0000017225 ** KI-: RFP[00]: Connection Established
11-16-2006	18:18:43	User.Emerg	172.30.206.121	RFP: 0000015300 ***** BMC: HW capabilities info: 0x000001DC
11-16-2006	18:18:43	User.Emerg	172.30.206.120	RFP: 0000015300 ***** BMC: HW capabilities info: 0x000001DC
11-16-2006	18:18:40	Syslog.Info	172.30.206.122	syslogd: received HUP signal
11-16-2006	18:18:40	User.Emerg	172.30.206.122	RFP: 0000015950 ***** MAIN: UP & RUNNING (0.1.0)
11-16-2006	18:18:40	User.Notice	172.30.206.122	OMM: 0000013625 ** KI-: RFP[02]: Connection Established
11-16-2006	18:18:40	User.Emerg	172.30.206.122	RFP: 0000015490 ***** BMC: HW capabilities info: 0x000001DC
11-16-2006	18:18:28	User.Emerg	172.30.206.121	RFP: 0000000020 ***** MAIN: starting application
11-16-2006	18:18:28	User.Emerg	172.30.206.120	RFP: 0000000020 ***** MAIN: starting application
11-16-2006	18:18:28	User.Emerg	172.30.206.121	syslog: 0000000000 ***** ALL: hw_rfptype = HW_RFP32
11-16-2006	18:18:28	User.Emerg	172.30.206.120	syslog: 0000000000 ***** ALL: hw_rfptype = HW_RFP32
11-16-2006	18:18:27	User.Emerg	172.30.206.122	OMM: 0000000130 ***** WEBS: webs: Listening for HTTP requests at address 172.30.206.122

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

10.3.5 SSH user shell

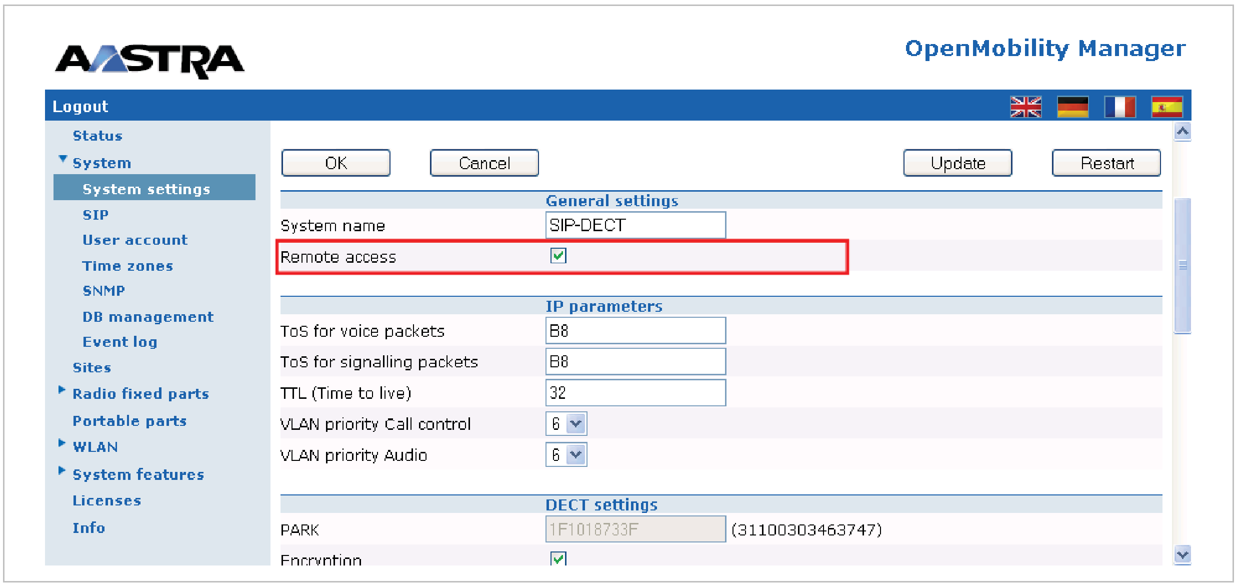
Each RFP offers a lot of commands within the SSH shell. Most of them are useful for diagnostic and may help experts to resolve failures.

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 which has a connection to an OMM, activate the **Remote access** checkbox on the OMM **System settings** web page (see also chapter 7.4.1).



General settings

System name: SIP-DECT

Remote access: ☑

IP parameters

ToS for voice packets: B8

ToS for signalling packets: B8

TTL (Time to live): 32

VLAN priority Call control: 6

VLAN priority Audio: 6

DECT settings

PARK: 1F1018733F (31100303463747)

Encryption: ☑

→ In the OMP, the SSH access is activated/deactivated in the **General** tab of the **System settings** menu (see chapter 8.5.1).

10.3.5.1 Login

To log in to the SSH user shell:

1 Open SSH session to the IP DECT base station with the “Full access” user name.

33 Enter the password for the “Full access” account (see also 9.14.1).

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 >
```

10.3.5.2 Command Overview

Type `help` to get a command overview:

Command	Description
exit,quit,bye	Leave session
ommconsole	OMM console
ip_rfpconsole	RFP console
rfpmconsole	RFP manager console
wlanconsole	WLAN console
wpaconsole	WPA console
flash	Shows information from flash
link	Shows status of ethernet interface
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)
rfpm_console	RFP manager console
wlan_console	WLAN console

10.3.5.3 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 user 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 have to enter the whole path “/usr/sbin/ommconsole” to start the OMM console.

10.3.5.4 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
help	Displays Command Help Table
logger	Send a string to the syslog daemon
deftrc	Resets all trace settings to default
dsp	Shows channel config
dump	Creates system state dump file /tmp/sys_dump.txt.gz
mem	Show memory and heap
exit	Leave this console
heap	Shows heap buffer statistics
lec	Adjust linear echo canceler parameters
media	Display state of media channels
mutex	Lists all created MXP mutexes
omms	Shows connection status to OMM(s)
queues	Lists all created MXP queues
reset	Resets the IPRFP application
resume	Resume bmc activity
rsx	Allows RSX connection to BMC via TCP
sem	Lists all created MXP semaphores
spy	Set/display spy levels: [<key #> <level #>]
suspend	Suspend bmc activity
tasks	Lists all running MXP tasks
voice	Displays the state of voice handling
wlan	Configure wlan card on cmdline
runtime	Report the process runtime
lu10	Lu10 SDU <-> PDU converter (RFP (L) 35/36/37 IP and RFP (L) 43 WLAN only)
mroute	Display media routes

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.

10.3.5.5 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
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
mem	Show memory and heap
exit	Leave this console
fts	Requesting FTS to download file
gmi	DECTnet2 Inter Working Unit
heartbeat	Configure heartbeat mechanism for IP-RFPs
ima	IMA commands
ipc	Displays socket communication
ipl	Displays connected RFPs
iplfilter	Configures for which RFPs spy messages shall be generated
mon	Toggle monitor functionality
msm	Display states within MediaStreamManagement
mutex	Lists all created MXP mutexes
nwk	DECT network layer
omi	OMI commands
queues	Lists all created MXP queues
rfp	Radio Fixed Part Control
rfpd	Radio Fixed Part Debug
rfps	Radio Fixed Part Statistic
rping	Requests one or more RFPs to ping a host
rspy	Remote configure spy levels on IP-RFPs
rsx	Toggles RSX debug port on RFPs

rtt	Set event flag for high RTT values / clears values
sem	Lists all created MXP semaphores
spy	Set/display spy levels: [<key #> <level #>]
standby	Displays redundant OMMs
stat	Statistic
sync	Commands for RFP synchronisation
tasks	Lists all running MXP tasks
tzone	Time zone commands
uptime	Displays system uptime
ver	Version information
wlan	Display states within Wireless LAN Management
axi	AXI commands
runtime	Report the process runtime
upd	Displays update status of RFPs
xml	XML browser task (XML) console

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.

10.3.6 Core File Capturing

If there some fatal error on the OMM and the software is breaking down, the OMM is able to generate memory dump. If you send these generated core files to the support, you help them to resolve this failures. The OMM is able to store these core files on a TFTP server in your local network.

To enabling core file creation write on the OMM command line:

`ldb core=yes`
`ldb core_srv=server-ip` – TFTP server IP address
`ldb core_path=path` – file path on TFTP server (must be writeable)

If no `ldb_core_srv` and `ldb_core_path` is given, the OMM tries to write the core files to the TFTP server and path where the OMM/RFP application was downloaded.

After restarting the OMM, the core files are automatically transferred to the TFTP server.

Please note: The TFTP server must allow writing new files, this is usually not standard.

To disable core file capturing writer on command line: `ldb core=`.

10.3.7 DECT Monitor

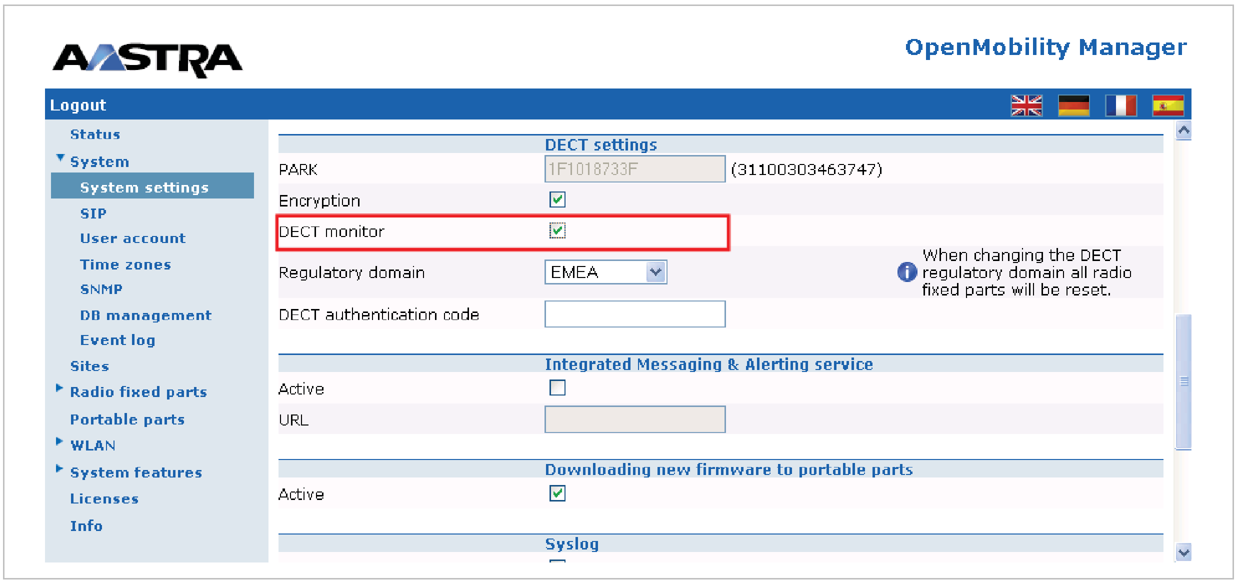
Please note: The DECT Monitor has been replaced by OMP but the DECT Monitor can still be used without warrenty for SIP–DECT installations with a standard PARK and up to 256 RFPs' all within paging area 0.

For a 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 PPs.
- 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 (see also chapter 7.4.1).



DECT settings

PARK	1F1018733F (31100303463747)	
Encryption	☑	
DECT monitor	☑	
Regulatory domain	EMEA	When changing the DECT regulatory domain all radio fixed parts will be reset.
DECT authentication code		

Integrated Messaging & Alerting service

Active	□
URL	

Downloading new firmware to portable parts

Active	☑

Syslog

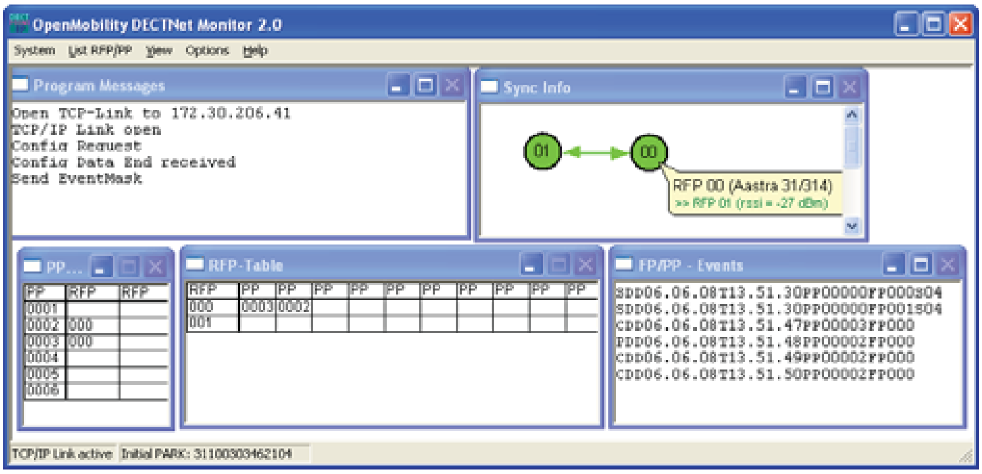
Please note: Because of security, the DECT monitor flag is not stored permanently in the internal flash memory of the OMM/RFP. After a reset the DECT monitor flag is disabled.

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 has to 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 “PP-Table”. This procedure is called “Config Request”.



```
Open TCP-Link to 172.30.206.41
TCP/IP Link open
Config Request
Config Data End received
Send EventMask
```

PP	RFP	RFP
0001		
0002	000	
0003	000	
0004		
0005		
0006		

RFP	PP	PP	PP	PP	PP	PP	PP	PP	PP	PP
000	0003	0002								
001										

```
SDD06.06.08T13.51.30PP00000FP000S04
SDD06.06.08T13.51.30PP00000FP001S04
CDD06.06.08T13.51.47PP00003FP000
PDD06.06.08T13.51.48PP00002FP000
CDD06.06.08T13.51.49PP00002FP000
CDD06.06.08T13.51.50PP00002FP000
```

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/PP-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.

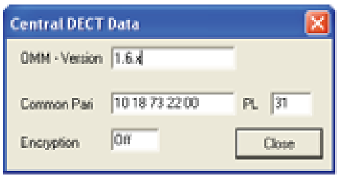
The following color scheme is used for display of the telephone in the PP table:

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

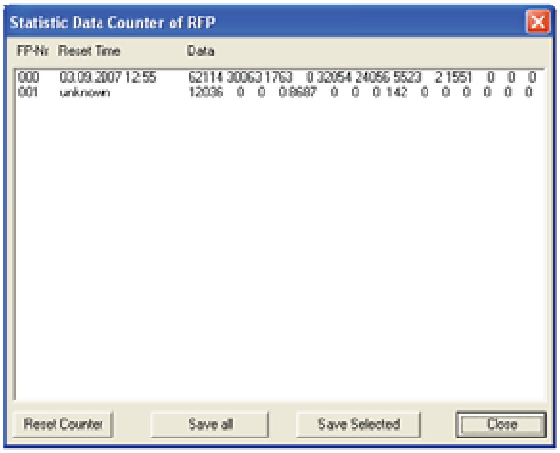


Central DECT Data

OMM - Version: 1.6.x

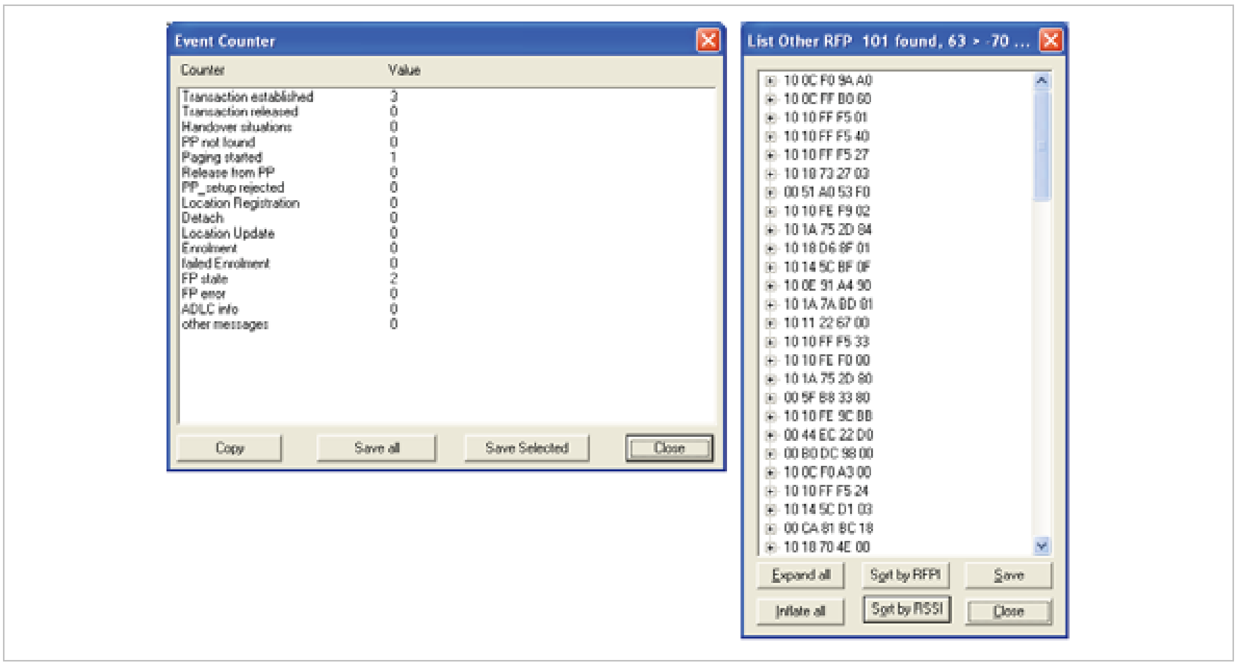
Common Pari: 10 18 73 22 00   PL: 31

Encryption: Off



Statistic Data Counter of RFP

FP-Nr	Reset Time	Data
000	03.09.2007 12:55	62114 30063 1763 0 32054 24056 5523 2 1551 0 0 0
001	unknown	12036 0 0 0 8687 0 0 0 142 0 0 0 0 0 0



Counter	Value
Transaction established	3
Transaction released	0
Handover situations	0
PP not found	0
Paging started	1
Release from PP	0
PP_setup rejected	0
Location Registration	0
Detach	0
Location Update	0
Enrolment	0
failed Enrolment	0
FP state	2
FP error	0
ADLC info	0
other messages	0

```
10 0C F0 9A A0
10 0C FF B0 60
10 10 FF F5 01
10 10 FF F5 40
10 10 FF F5 27
10 18 73 27 03
00 51 A0 53 F0
10 10 FE F9 02
10 1A 75 2D 84
10 18 D6 8F 01
10 14 5C BF 0F
10 0E 91 A4 90
10 1A 7A BD 01
10 11 22 67 00
10 10 FF F5 33
10 10 FE F0 00
10 1A 75 2D 80
00 5F B8 33 80
10 10 FE 9C B0
00 44 EC 22 D0
00 B0 DC 98 00
10 0C F0 A3 00
10 10 FF F5 24
10 14 5C D1 03
00 CA 81 BC 18
10 18 70 4E 00
```

11 Appendix

11.1 Declaration of Conformity

The CE mark on the product certifies its conformity with the technical guidelines for user safety and electromagnetic compatibility, valid from the date of issue of the relevant Declaration of Conformity pursuant to European Directive 99/5/EC.

The Declaration of Conformity can be viewed on the Aastra homepage.

11.2 Communications Regulation Information for Aastra 142d, Aastra 600d

11.2.1 FCC Notices (U.S. Only)

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

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

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

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

Health and Safety Information

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.

This EUT has been shown to be capable of compliance for localized specific absorption rate (SAR) for uncontrolled environment/general population exposure limits specified in ANSI/IEEE Std. C95.1-1992 and had been tested in accordance with the measurement procedures specified in FCC/OET Bulletin 65 Supplement C (2001) and IEEE 1528-2003.

11.2.2 Industry Canada (Canada only, not for Aastra 600d)

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.

This device has been shown to be capable of compliance for localized specific absorption rate (SAR) for uncontrolled environment / general public exposure limits specific in ANSI/IEEE C95.1-1992 and had been tested in accordance with the measurement procedures specified in IEEE 1528-2003.

11.3 Communications Regulation Information for RFP 32, RFP 34 and RFP 35

11.3.1 FCC Notices (U.S. Only)

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

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

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

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

Exposure to Radio Frequency (RF) Signals:

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

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

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

11.3.2 Industry Canada (Canada only)

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

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

Exposure to Radio Frequency (RF) Signals:

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

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

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

11.4 Abbreviations

AC	Authentication Code
ADPCM	Adaptive Differential Pulse Code Modulation
DECT	Digital Enhanced Cordless Telecommunication
DHCP	Dynamic Host Configuration Protocol
DSP	Digital Signal Processor
FCC	Federal Communications Commission
GAP	Generic Access Profile
OM IMA	Integrated Messaging and Alerting Service
IPEI	International Portable Equipment Identity
HTTP	Hyper Text Transfer Protocol
OAM&P	Operation, Administration, Maintenance & Provisioning
OM	OpenMobility
OM AXI	OM Application XML Interface
OMC	OM Configurator
OML	OM Locating
OMM	OpenMobility Manager
OMP	OM Management Portal
PARK	Portable Access Rights Key
PP	Portable Part (DECT handset or device)
SNMP	Simple Network Management Protocol
TFTP	Trivial File Transfer Protocol
RFP	DECT Radio Fixed Part (DECT base station)
RTCP	Real Time Control Protocol
RTP	Real Time Protocol

11.5 Definitions

Aastra DECT 142 / Aastra 142d Handset	In the context of the SIP–DECT solution, an Aastra DECT 142 Handset, Aastra 142d and Portable Part (PP) are interchangeable. In consideration of differences in regulatory requirements between North America and all other areas of the world exist two different PP variants which use specific frequency bands and field strengths: - Aastra DECT 142: For use in North America and Canada only. - Aastra 142d: For global use.

Asterisk	Asterisk is a complete Open Source PBX in software. It runs on Linux, BSD and MacOSX and provides many features. Asterisk supports voice over IP in many protocols, and can interoperate with almost all standards-based telephony equipment.
Base station	Please see: RFP or Radio Fixed Part
DECT	**D**igital **E**nhanced **C**ordless **T**elecommunication The standard (ETS 300 175) essentially specifies the air interface, known as the radio interface. Voice and data can both be transmitted via this interface. Its technical key characteristics for Europe are: - Frequency range: approx. 1880 – 1900 MHz (approximately 20 MHz bandwidth) - carrier frequencies (1728 kHz spacing) with 12 time slots each - Doubling the number of time slots (to 24) using the TDMA process - Net data rate per channel of 32 kbps (for voice transmission using ADPCM) - Voice coding using the ADPCM method Its technical key characteristics for North American are: - Frequency range: approx. 1920 – 1930 MHz (approximately 10 MHz bandwidth) - 5 carrier frequencies (1728 kHz spacing) with 12 time slots each) - Doubling the number of time slots (to 24) using the TDMA process - Net data rate per channel of 32 kbps (for voice transmission using ADPCM) - Voice coding using the ADPCM method
GAP	**G**eneric **A**ccess **P**rofile - The GAP standard (ETS 300 444) is based on the same technology as DECT, but is limited to the most important basic features. This standard was created in order to allow telephones of different vendors to be used on any type of DECT system. It thus represents the smallest common denominator of all manufacturer-specific variants of the DECT standard. - An important limitation in the GAP standard is that external handover is not possible. For this reason connection handover is used, which is supported by GAP terminals. - The operation of GAP-capable telephones is comparable to that of analogue terminals. For example, features can be called up via ‘*’ and ‘#’ procedures.
Handover	A handover is similar to roaming, but occurs during an ongoing call. A handover normally takes place “in the background”, without disrupting the call (seamless handover).

IPEI	**I**nternational **P**ortable **E**quipment **I**dentity - 13-digit identification code for PPs - Example: 00019 0592015 3 (the final digit is the checksum). - The code is represented in decimal form. - This code is globally unique.
PARK	**P**ortable **A**ccess **R**ights **K**ey Access code for the Portable Part. This code determines whether a PP can access a particular DECT system. Used for unique selection of a dedicated the system from a handset at enrolment/subscription time. Labeled on the OpenMobility CD and unique to each SIP–DECT deployment.
Radio Fixed Part (RFP)	An RFP provides a DECT radio cell and terminates the radio link from the portable DECT device. One or more RFPs build the area of radio coverage.
Roaming	While in motion, the PP performs ongoing measurements to determine which RFP is best received. The one that can be best received is defined as the active RFP. To prevent the PP from rapidly switching back and forth between two RFPs that have similar signal strength, certain threshold values are in effect.

11.6 References

/1/ RFC 1350, The TFTP Protocol, Revision 2, July 1992

/2/ RFC 2090, TFTP Multicast Option, February 1997

/3/ RFC 2347, TFTP Option Extension, May 1998

/4/ RFC 2348, TFTP Block size Option, May 1998

/5/ RFC 2349, TFTP Timeout Interval and Transfer Size Options, May 1998

/6/ RFC 2236, Internet Group Management Protocol, Version 2, November 1997

/7/ RFC 1889, RTP: A Transport Protocol for Real-Time Applications, January 1996

/8/ RFC 2030, Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI, October 1996

/9/ RFC 2131, Dynamic Host Configuration Protocol, March 1997

/10/ RFC 2327, SDP: Session Description Protocol, April 1998

/11/ RFC 2474, Definition of the Differentiated Service Field (DS Field) in the IPv4 and IPv6 Headers, December 1998

/12/ RFC 2617, HTTP Authentication: Basic and Digest Access Authentication, June 1999

/13/ RFC 3164, The BSD Sys Log Protocol, August 2001

/14/ RFC 2833, RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals, May 2000

/15/ RFC 3261, Session Initiation Protocol (SIP), June 2002

/16/ RFC 3264, An Offer/Answer Model with Session Description Protocol (SDP), June 2002

/17/ RFC 3420, Internet Media Type message/sipfrag, November 2002

/18/ RFC 3515, The Session Initiation Protocol (SIP) Refer method, April 2003

/19/ RFC 3665, The Session Initiation Protocol (SIP) Basic Call Flow Examples, December 2003

/20/ RFC 3842, A Message Summary and Message Waiting Indication Event Package for the Session Initiation Protocol (SIP), August 2004

/21/ RFC 3891, The Session Initiation Protocol (SIP) “Replaces” Header, September 2004

/22/ RFC 3892, The Session Initiation Protocol (SIP) Referred-By Mechanism, September 2004

/23/ RFC 4566, SDP: Session Description Protocol

/24/ Compendium “OpenMobility SIP–DECT 3.0 Solution; Installation & Administration”

/25/ SIP–DECT; OM Locating Application; Installation, Administration & User Guide

/26/ SIP–DECT; OM Integrated Messaging & Alerting Application; Installation, Administration & User Guide

/27/ SIP–DECT; OM Handset Sharing & Provisioning; User Guide

/28/ SIP–DECT; Aastra 610d, 620d, 630d; Messaging & Alerting Applications; User Guide Issue 4

/29/ Aastra 610d, 620d, 630d SIP–DECT User’s Guide Issue 4

/30/ aad-0384 OM Application XML Interface specification (OM AXI)

/31/ RFC 2782, A DNS RR for specifying the location of services (DNS SRV)

/32/ RFC 3262, Reliability of Provisional Responses in the Session Initiation Protocol (SIP)

/33/ RFC 3311, The Session Initiation Protocol (SIP) UPDATE Method

/34/ SIP–DECT XML terminal interface specification

11.7 Pre-Configuration File Rules

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

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

1. An **instruction section** is used to drive a generic data creation for those fields not filled within data sequence section.
2. A data sequence section defines data record fields. Each of them are 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 starts with the key word “data_sequence”. This key word is always **mandatory to proceed the file**. All instructions have to 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 of data sequence fields are separated by colon the content of that section can possibly be generated by a *.csv export of Excel Sheet and copied into the configuration file.
- Instructions are only proceeded on those fields which are left empty within the data sequence section.

11.7.1 PP Configuration File (OMM Database)

11.7.1.1 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. If a value is advised, it will be taken as a start number which will be increased for each new record.
additional_pin	
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	

11.7.1.2 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”)

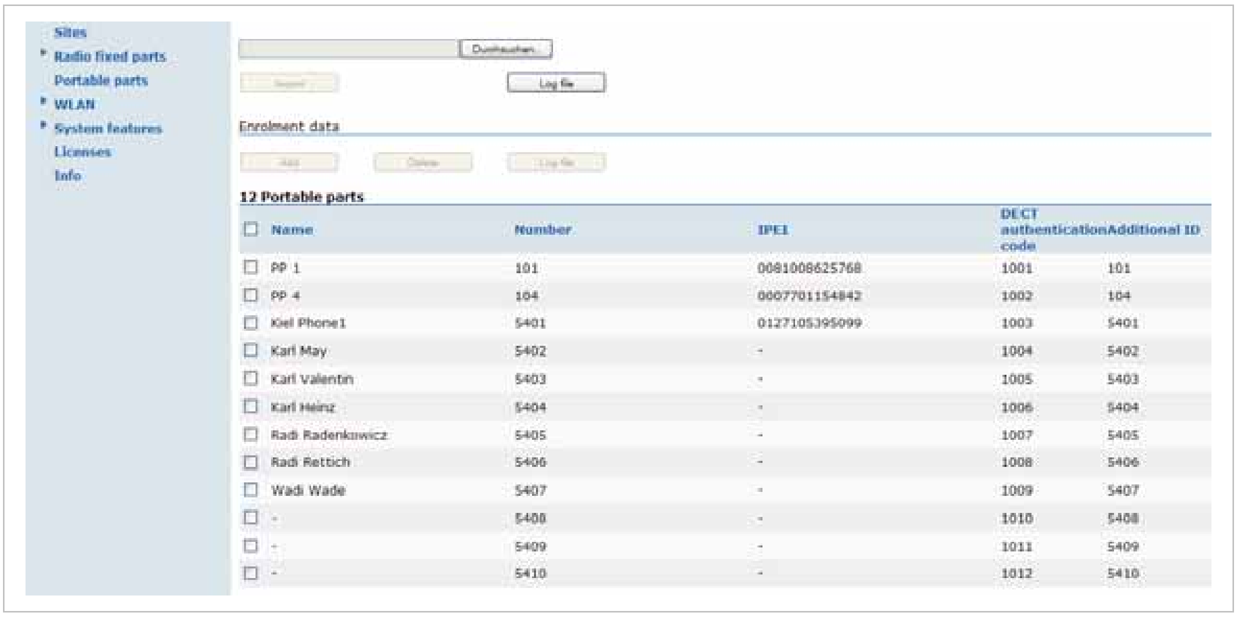
12 Tracking (ignored by Web import and always set to “inactive”)

13 Description1 (ignored by Web import and always set to “”)

14 Description2 (ignored by Web import and always set to “”)

11.7.1.3 Example

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



Enrolment data

12 Portable parts

□	Name	Number	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

PP 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;PP 1;;0081008625768;;;;;;;;;;
104;PP 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:

[…]
```

11.7.2 RFP Configuration File / Central (OMM Database)

Import of RFP configurations using files is possible with Web Service or OMM Management portal.

11.7.2.1 Supported Instructions

All instructions are taken as common value which are set to all records of 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..2048}
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 }

Note: Web import allows currently only ‘0’ or ‘1’ for Boolean parameters.

11.7.2.2 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 (ignored by Web import and 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

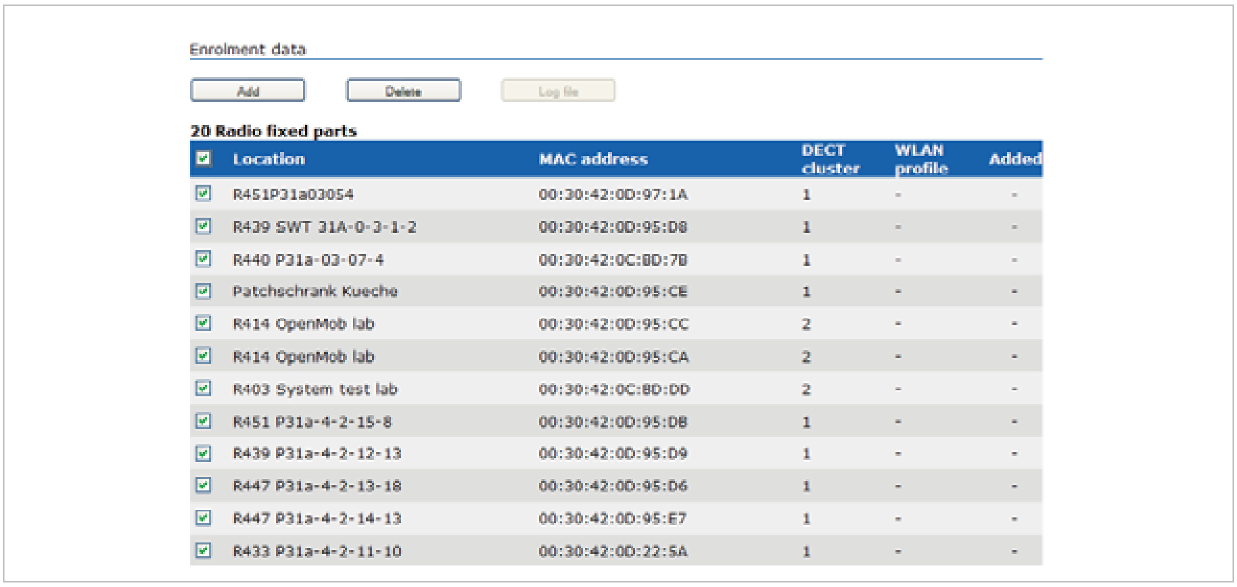
14 WLAN channel

15 WLAN power

16 WLAN activated

11.7.2.3 Example

The following screenshot shows an RFP enrolment data import dialog that is shown if the corresponding configuration file is imported.



Enrolment data

20 Radio fixed parts

☑	Location	MAC address	DECT cluster	WLAN profile	Added
☑	R451P31a03054	00:30:42:0D:97:1A	1	-	-
☑	R439 SWT 31A-0-3-1-2	00:30:42:0D:95:D8	1	-	-
☑	R440 P31a-03-07-4	00:30:42:0C:8D:7B	1	-	-
☑	Patchschrank Kueche	00:30:42:0D:95:CE	1	-	-
☑	R414 OpenMob lab	00:30:42:0D:95:CC	2	-	-
☑	R414 OpenMob lab	00:30:42:0D:95:CA	2	-	-
☑	R403 System test lab	00:30:42:0C:8D:DD	2	-	-
☑	R451 P31a-4-2-15-8	00:30:42:0D:95:D8	1	-	-
☑	R439 P31a-4-2-12-13	00:30:42:0D:95:D9	1	-	-
☑	R447 P31a-4-2-13-18	00:30:42:0D:95:D6	1	-	-
☑	R447 P31a-4-2-14-13	00:30:42:0D:95:E7	1	-	-
☑	R433 P31a-4-2-11-10	00:30:42:0D:22:5A	1	-	-

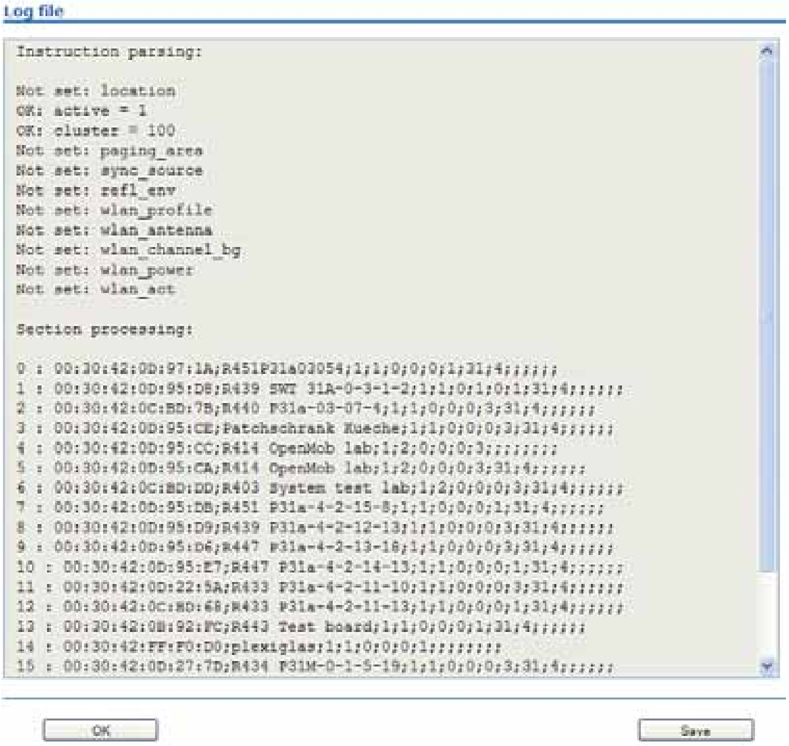
RFP configuration file/central:

```
##############################################################################
# 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..2048} (PC OMM)
#paging_area
#               Ignored by Web import and always set to "0" (PA0)
#               Paging area, the RFP is referred to: {'unassigned, '0'..'127'}
#sync_source
#               Synchronisation source:
#               '0' or 'false '= inactive, '1' or 'true' = active}
#refl_env
#               Reflective environment:
#               '0' or 'false '= no, '1' or 'true' = yes}
#site
#               Site Id: {1..250}
#wlan_profile
#               Reference key to an existing WLAN profile
#wlan_antenna
#               Antenna settings: {0=diversity, 1, 2}
#wlan_channel_bg
#               WLAN channel: {0..14 (size depends on regulatory domain) }
#wlan_power
#               WLAN power = { 6, 12, 25, 50,100 (in percent)}
#wlan_act
#               Activation of  WLAN:
#               '0' or 'false '= inactive, '1' or 'true' = active}
#Note: Web import allows only "0" or "1" for Boolean
##############################################################################


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

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

Parse log about import / instruction processing



```
Instruction parsing:

Not set: location
OK: active = 1
OK: cluster = 100
Not set: paging_area
Not set: sync_source
Not set: refl_env
Not set: wlan_profile
Not set: wlan_antenna
Not set: wlan_channel_bg
Not set: wlan_power
Not set: wlan_act

Section processing:

0 : 00:30:42:0D:97:1A;R451P31a03054;1;1;0;0;0;1;31;4;;;;;;
1 : 00:30:42:0D:95:D8;R439 SWT 31A-0-3-1-2;1;1;0;1;0;1;31;4;;;;;;
2 : 00:30:42:0C:BD:7B;R440 P31a-03-07-4;1;1;0;0;0;3;31;4;;;;;;
3 : 00:30:42:0D:95:CE;Patchschrank Kueche;1;1;0;0;0;3;31;4;;;;;;
4 : 00:30:42:0D:95:CC;R414 OpenMob lab;1;2;0;0;0;3;;;;;;;;
5 : 00:30:42:0D:95:CA;R414 OpenMob lab;1;2;0;0;0;3;31;4;;;;;;
6 : 00:30:42:0C:BD:DD;R403 System test lab;1;2;0;0;0;3;31;4;;;;;;
7 : 00:30:42:0D:95:DB;R451 P31a-4-2-15-8;1;1;0;0;0;1;31;4;;;;;;
8 : 00:30:42:0D:95:D9;R439 P31a-4-2-12-13;1;1;0;0;0;3;31;4;;;;;;
9 : 00:30:42:0D:95:D6;R447 P31a-4-2-13-18;1;1;0;0;0;3;31;4;;;;;;
10 : 00:30:42:0D:95:E7;R447 P31a-4-2-14-13;1;1;0;0;0;1;31;4;;;;;;
11 : 00:30:42:0D:22:5A;R433 P31a-4-2-11-10;1;1;0;0;0;3;31;4;;;;;;
12 : 00:30:42:0C:BD:68;R433 P31a-4-2-11-13;1;1;0;0;0;1;31;4;;;;;;
13 : 00:30:42:0B:92:FC;R443 Test board;1;1;0;0;0;1;31;4;;;;;;
14 : 00:30:42:FF:F0:D0;plexiglas;1;1;0;0;0;1;;;;;;;;
15 : 00:30:42:0D:27:7D;R434 P31M-0-1-5-19;1;1;0;0;0;3;31;4;;;;;;
```

11.7.3 RFP Configuration File / Local (OM Configurator)

11.7.3.1 Supported Instructions

All instructions are taken as common value which are set to all records of data sequence section of that file if the corresponding field is empty.

Instruction	Explanation
active	Local configuration active: {0=inactive(use DHCP instead), 1=active}
net_mask	Net mask
tftp_server	IP address of TFTP server
tftp_file	Path and name of boot file
omm_1	OMM IP address
omm_2	IP address of backup OMM
gateway	Default gateway
dns_server	Up to two DNS server IP addresses
dns_domain	local DNS domain
ntp_address	Up to two NTP server IP addresses
ntp_name	Up to two NTP server names
syslog_addr	IP address of syslog daemon
syslog_port	Listen port of syslog daemon
core	Flag to enable core dumps
use_vlan	VLAN is enabled
srvlst	List of further tftp server
broadcast_addr	local broadcast address
vlan_id	VLAN Id
country	Country code
preferred_tftp	tftp_server is preferred
import_url	URL
config_file_server	configuration server

11.7.3.2 Data Section Fields

The data section contains the following field order:

1 MAC address of RFP

34 Local configuration active flag

35 IP address of RFP

36 Net mask

37 TFTP server

38 TFTP_FILE

39 OMM IP address

40 IP address of backup OMM

41 Default gateway

42 DNS server

43 DNS domain

44 NTP server IP address

45 NTP server name

46 Syslog daemon IP address

47 Syslog listen port

48 Core

49 Use VLAN

50 Server list

51 Broadcast address

52 VLAN Id

53 Country code

54 Preferred TFTP server

55 Import URL

56 Configuration file server

11.7.3.3 Example

RFP configuration file/local (OM Configurator):

```
# --------------------#
# instruction section #
# --------------------#

active     = 1
net_mask   = 255.255.0.0
tftp_server= 172.30.200.92
tftp_file  = iprfp2g.tftp
omm_1      = 172.30.111.188
omm_2      = 172.30.11.181
gateway    = 172.30.0.2
dns_server = 172.30.0.4,172.30.0.21
dns_domain = aastra.de
ntp_addr   = 192.53.103.108,192.53.103.104
ntp_name   = ptbtime1.ptb.de,ptbtime2.ptb.de
syslog_addr= 172.30.200.92
core = 0
use_vlan = 1
srvlist = 172.30.0.4,172.30.0.21
broadcast_addr = 172.30.255.255
vlan_id = 4
country = 1
preferred_tftp = 1
```

```
import_url = https://server/importfiles/ommxy_conf.gz

config_file_server = https://server/configfiles/

# ---------------#
# data sequence #
# ---------------#
# 1. MAC_ADDR           ! no instruction supported !
# 2. ACTIVE_FLAG
# 3. RFPADDR            ! no instruction supported !
# 4. NET_MASK
# 5. TFTP_SERVER
# 6. TFTP_FILE
# 7. OMM1
# 8. OMM2
# 9. GATEWAY
#10. DNS_SERVER
#11. DNS_DOMAIN
#12. NTP_ADDR
#13. NTP_NAME
#14. SYSLOG_ADDR
#15. SYSLOG_PORT
#16. CORE
#17. USE_VLAN
#18. SRVLIST
#19. BROADCAST_ADDR
#20. VLAN_ID
#21. COUNTRY
#22. PREFERRED_TFTP
#23. IMPORT_URL
#24. CONFIG_FILE_SERVER

data_sequence
00-30-42-01-01-01;;172.30.111.1
00-30-42-02-02-02;;172.30.111.2
```

Parse log about import / instruction processing

```
 ok: active = 1
 ok: net_mask = 255.255.0.0
 ok: tftp_server = 172.30.200.92
 ok: tftp_file = iprfp2g.tftp
 ok: omm_1 = 172.30.111.188
 ok: omm_2 = 172.30.11.181
 ok: gateway = 172.30.0.2
 ok: dns_server = 172.30.0.4,172.30.0.21
 ok: dns_domain = Aastra.com
 ok: ntp_addr = 192.53.103.108,192.53.103.104
 ok: ntp_name = ptbtime1.ptb.de,ptbtime2.ptb.de
 ok: syslog_addr = 172.30.200.92
 not set: syslog_port
 ok: core = 0
 ok: use_vlan = 1
 ok: srvlist = 172.30.0.4,172.30.0.21
 ok: broadcast_addr = 172.30.255.255
 ok: vlan_id = 4
 ok: country = 1
 ok: preferred_tftp = 1
 ok: import_url = https://server/importfiles/ommxyz_conf.gz
 ok: config_file_server = https://server/configfiles/

 :parsing ok:

 processing of section: data_sequence

[…]

create data:
```

```
[…]

RFP configuration:

[…]
```

11.8 RFP Export File Format

General

RFP export files are created by OMM Management Portal in ‘csv’-file format which can be easily viewed by a spreadsheet application. Export file contains all or a part of the following parameters:

- MAC address
- Location name
- DECT active
- Cluster
- Paging area
- Synchronisation source
- Reflective environment
- Site
- Building
- Floor
- Room
- WLAN profile reference
- WLAN antenna
- WLAN Channel_bg
- WLAN power
- WLAN active

Example

Following example RFP export file contains all exportable RFP parameters and is re-importable by OMM Management Portal.

```
##################################################
# RFP data export file: '/home/user/example.csv'
# Date: 24.09.10  Time: 15:58:19
##################################################
#
# Exported parameters:
#
# MAC address
# Name
# DECT activated
# DECT cluster
# Paging area
# Preferred sync.
# Reflective env.
# Site ID
# Building
# Floor
# Room
# WLAN profile
# WLAN antenna
# WLAN channel
# WLAN power
# WLAN activated
#
##################################################

MAC address;Name;DECT activated;DECT cluster;Paging area;Preferred
sync.;Reflective env.;Site ID;Building;Floor;Room;WLAN profile;WLAN
antenna;WLAN channel;WLAN power;WLAN activated

data_sequence

00:30:42:0E:71:41;License RFP 1;
true;1;0;false;true;1;B1;F1;R1;1;0;;100;false

00:30:42:0E:26:F1;License RFP 2;
true;1;0;false;false;1;B1;F2;R1;1;0;;100;false

00:30:42:0E:75:59;License RFP 3;
true;1;0;true;false;1;B1;F2;R2;1;0;;100;false
```

11.9 Protocols and Ports

Protocol		OpenMobility Manager	
		Server port	Client port
HTTPS server	tcp server	443 or as configured	any
HTTP server (redirect to https)	tcp server	80 or as configured	any
HTTP/HTTPS client for the SIP–DECT XML terminal interface	tcp	80/443	> 1024
RFP control protocol	tcp server	16321	any
OMM Standby	tcp server	16322	any
OM AXI	tcp server	12622	any
DECTnet monitor	tcp server	8106	any
LDAP	tcp client	389 or as configured	>=1024 (see note)
TFTP client	udp	69 / given by server	>=1024 (see note)
HTTP client	tcp	80 or as configured	>=1024 (see note)
HTTPS client	tcp	443 or as configured	>=1024 (see note)
explicit FTPS client	tcp	21 or as configured	>=1024 (see note)
implicit FTPS client	tcp	990 or as configured	>=1024 (see note)
OM AXI server TCP	tcp server	12621	any
OM AXI server TLS	tcp server	12622	any
SIP	udp	5060	as configured
Telnet (OMM console, Linux PC based OMM only)	tcp server	localhost 8107	localhost any

Note: Unbound ports start at port 1024.

Protocol		IP-RFP	
		Server port	Client port
HTTP/HTTPS client for the SIP–DECT XML terminal interface	tcp	80/443	> 1024
RFP control protocol	tcp client	16321	>=1024 (see note)
HTTP server (redirect to OMM web server (http))	tcp server	80 or as configured	any
SSH server	tcp server	22	any
DHCP client	udp	67	68
TFTP client	udp	69 / given by server	>=1024 (see note)
OMCFG server	udp	64000	64000
NTP client	udp	123	123
Syslog client	udp	514 or as configured	514
DNS client	udp	53	>=1024 (see note)
SNMP agent (server)	udp	161	any
SNMP trap agent (client)	udp	>=1024 (see note)	162
RSXport (debug only)	tcp server	38477	any
RTP/RTCP (server)	udp	Range of [RTP port base + 71] even ports for RTP, odd ports for RTCP. Port base is 16320 or as configured.	any
RTP/RTCP (client)	udp	any	Range of [RTP port base + 71] even ports for RTP, odd ports for RTCP. Port base is 16320 or as configured.

Note: Unbound ports start at port 1024.

12 Index