



**OpenMobility
SIP-DECT™ Lite**

ASTRA

**Installation &
Administration**
System Manual

Welcome to Aastra

Thank you for choosing this Aastra product. Our product meets the strictest requirements with regard to quality and design.

The following compendium will assist you in installing and configuring your SIP-DECT™ Lite solution and provide answers to your most important questions.

If you should require further technical support or information about other Aastra products, please contact the person responsible for your system or get in touch with your local dealer.

You can also find information about this device and other products on our website at **<http://www.aastrausa.com>**.

Contents

SIP-DECT™ Lite Solution	5
Scope of Delivery	6
Notes on Safety	7
Installation Site	9
Radio Coverage Area	9
Radio Propagation Conditions	10
Wall Mounting	12
Getting Started	13
LAN Prerequisites	14
Unpacking the DECT Handset	15
Unpacking the RFP SL35 IP	16
Checking IP Configuration	18
Configuring a Static IP	19
Configuring SIP-DECT™ Lite	20
Configuration via the DECT Handset	21
Configuration via the OMM Web Service	22
User Login / Logout on the Handset	24
Subscribing DECT Handsets	26
Activating the Subscription Mode on the Handset	26
Activating the Subscription Mode in the OMM Web Service	27
Subscription Procedure on the Handset	27
Advanced Configuration	29
Updating the Software	30
Manual Update	30
Background Update	30
Restoring Factory Defaults	31

Backing up and Restoring the SIP-DECT™ Lite Configuration	33
Download Over Air	34
OMM User Account Types	37
SSH User Shell	38
Using Directories	39
SNMP Configuration	41
Configuring VLAN	42

Menu Tree on the Handset	43
“User login” / “User logout” Menu Entries	44
“Status” Menu Entry	44
“System” Menu Entry	44
“SIP users / devices” Menu Entry	46
“Versions” Menu Entry	47
“Factory reset” Menu Entry	48

OMM Web Service Reference	49
General Usage	49
“Status” Menu	49
“System” Menu	50
“System settings” Menu	50
“SIP” Menu	53
“User administration” Menu	57
“Time zones” Menu	57
Changing Time Zones	58
Resetting Time Zones	58
“SNMP” Menu	58
“DB management” Menu	59
“Event log” Menu	60
“SIP users / devices” Menu	61
Creating and Changing SIP User Accounts	62
Deleting SIP User Accounts	63

“System features” Menu	63
“Digit treatment” Menu	63
Creating and Changing “Digit treatment” Entries	63
Deleting “Digit treatment” Entries	64
“Directory” Menu	64
Creating and Changing Directory Entries	64
Deleting Directory Entries	66
“Feature access codes” Menu	66
“XML applications” Menu	67
Creating and Changing “XML application” Hooks	68
Deleting “XML application” Hooks	69
“Info” Menu	69

Configuration Files..... 70

Hosting Configuration Files 70

System Configuration 72

Activating System Configuration Files 72

Example System Configuration Files..... 74

Processing System Configuration Files 78

XML Statement Reference 79

 Basic Configuration 80

 System: System settings..... 80

 System: SIP 83

 System: User administration 87

 System: Time zones 88

 System: SNMP 90

 System: DB management..... 90

 SIP users / devices..... 92

 System features: digit treatment..... 93

 System features: Directory..... 94

 System features: Feature access codes 96

 System features: XML applications..... 98

User Data..... 100

Activating User Data Configuration 101

Example: Common Configuration..... 101

Example: User Data Configuration 102

Messaging	102
Activating Messaging Configuration File	103
Example Messaging Configuration File	103
XML Application	104
Activating an XML Application	104
Example XML Application	105
Appendix	106
Declaration of Conformity	106
Communications Regulation Information	106
Warranty Repair Services	108
After Warranty Service	108
Technical Data	109
RFP SL35 IP	109
Aastra 610d, 620d, 630d	109
Abbreviations	111
Definitions	112
Trademarks	113
References	113
Other Valid Documentation	113
RFC Reference	114
Index	116

SIP-DECT™ Lite Solution

SIP-DECT® adds the comfort of mobility to VoIP networks, based on two technologies:

- Voice over IP (VoIP) – Voice is conveyed via an IP data network to an IP radio fixed part.
- DECT (Digital Enhanced Cordless Telecommunications) – Tried and tested technology for conveying voice securely via the air from the IP radio fixed part to the handset.

The SIP-DECT™ Lite solution provides a professional DECT system, thus operating DECT handsets as SIP clients. The SIP-DECT™ Lite solution includes one DECT base station “RFP SL35 IP” (RFP, “Radio Fixed Part”) and supports up to 512 users and devices.

The SIP-DECT™ Lite solution may also extend an existing SIP communications system (PBX). For this purpose, the RFP SL35 IP can be interconnected with the PBX via an Ethernet/IP network that is used to transport the SIP/VoIP data streams as well as management data.

The SIP-DECT™ Lite solution can be configured via the DECT handsets as well as with a web-based configuration software – the OMM web service. Furthermore, experts can configure the SIP-DECT™ Lite solution via configuration files.

About this manual

This manual describes the installation, configuration, administration, and maintenance of the SIP-DECT™ Lite solution.

Other valid documentation

Please observe also the information to other parts of your SIP-DECT™ Lite solution given in the documents listed in the section entitled References starting on page 113.

Reference

For a list of abbreviations and definitions valid for this manual please refer to the appropriate chapters in the Appendix starting on page 106.

Scope of Delivery

The SIP-DECT™ Lite product delivery varies with your purchase. You typically receive the following components:

- Radio Fixed Part device RFP SL35 IP
- AC adapter for powering the RFP SL35 IP (if PoE (Power over Ethernet) is not available)
- DECT handset Aastra 610d or Aastra 620d (pre-subscribed)
- Battery, charger cradle, AC adapter for the DECT handset
- USB flash drive with software and PARK.xml file containing the unique system identification.
- Paper manual entitled "OpenMobility, SIP-DECT™ Lite, Getting Started, Quick User Guide" (short version of the PDF manual entitled "OpenMobility, SIP-DECT™ Lite, Installation & Administration System Manual" which is available online)

Notes on Safety

Please note: Also observe the notes on safety for the DECT handsets given in the “Aastra 610d, 620d, 630d; SIP-DECT User’s Guide; Handset Release \geq 4.0”. This user guide is available for download on the Aastra website.

Installation

The RFP SL35 IP may only be installed inside buildings and should be operated when mounted on a wall.

Do not install the RFP SL35 IP during a thunderstorm. Do not connect and disconnect lines during a thunderstorm.

CAUTION!

Static charges can damage the RFP SL35 IP’s electronic components. Please make sure that you discharge yourself and your tools before and during any installation work on the RFP SL35 IP.



Connection to the mains power supply

The RFP SL35 IP may only be plugged into mains power sockets which have a protective earth conductor. It is not necessary to provide any additional earthing for the RFP SL35 IP.

Recommendation: Connect the RFP SL35 IP to a separate power circuit so that short circuits occurring in other devices do not put the RFP SL35 IP out of operation. The mains power connection must be installed by a licenced electrician to avoid danger to people or materials!

DANGER!

Hazardous voltages inside the device! The RFP SL35 IP may not be opened as this may lead to exposure to hazardous voltage!

The RFP SL35 IP does not have its own power supply switch. To disconnect the RFP SL35 IP from the mains power supply, pull the plug out of the power socket.

Install the RFP SL35 IP near an easily-accessible mains power socket so that the plug can be quickly pulled out of the power socket in a hazardous situation.

AC adapter

The RFP SL35 IP supports PoE (Power over Ethernet), Class 3, if provided. Alternatively you can use the provided AC adapter.

Use only the AC adapter provided to connect the RFP SL35 IP to the mains power supply. Other AC adapters may cause malfunctions or electric shock and damage the RFP SL35 IP.

CAUTION!

Never start or operate the RFP SL35 IP if the AC adapter is damaged. Serious danger to life from electric shock may result.

Cables

Ensure that all cables are laid in such a way that nobody can walk on or trip over them.

Use a shielded Ethernet cable (STP cable, Shielded Twisted Pair cable) to connect RFP SL35 IP to a local network (LAN, Local Area Network).

Usage

Make sure no fluids get into the RFP SL35 IP: electric shock or short circuit may result.

Repairs to the RFP SL35 IP and all its accessories must be carried out by accredited specialists. Inappropriate repairs may damage the RFP SL35 IP and will render any warranty claims invalid.

Keep the RFP SL35 IP and its accessories and packaging out of reach of children!

Installation Site

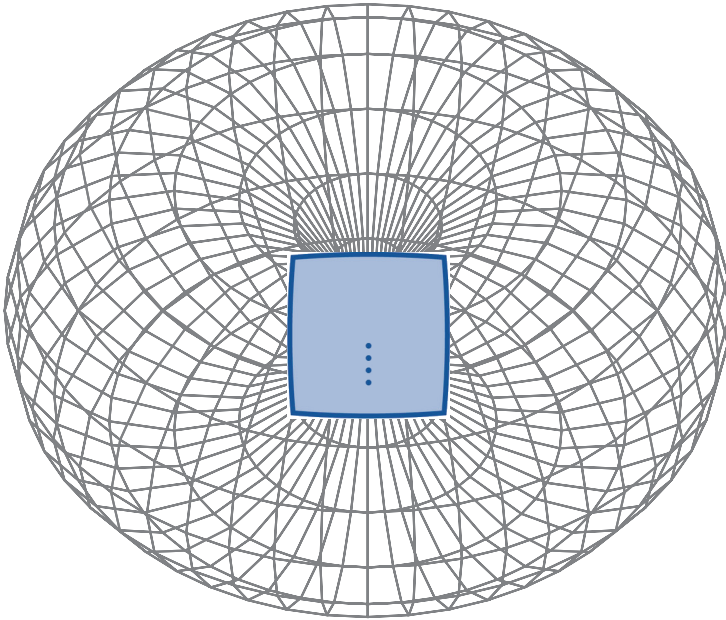
The RFP SL35 IP (Radio Fixed Part, RFP) is a device that allows to operate DECT handsets (Portable Parts, PP). For this, the RFP needs to establish and maintain a digital radio connection to all DECT handsets. To find a suitable installation site, you should consider the following facts:

- **Environment:** the RFP SL35 IP device operates in standard indoor conditions. This means that you should not expose the device to heat, coldness, or moisture that exceeds the conditions specified (see Technical Data starting on page 109). Also mind the Notes on Safety starting on page 7.
- **Connectivity:** the RFP SL35 IP device needs to be connected to the Internet by means of a wired Ethernet connection. Also, you need to provide a power supply either by connecting the AC adapter that in turn requires a near-by wall socket or by PoE (Power over Ethernet).
- **Radio Coverage:** due to the limited coverage / supply range of radio waves you should select the installation site carefully. The following explanations emphasize on this topic.

Radio Coverage Area

The supply range of a DECT system can vary greatly from a geographical point of view. The RFP transmits and receives the radio signal through two integrated antennas inside the housing. The radio characteristic of internal antennas is doughnut (or torus) shaped under ideal conditions.

This does not take into account the topology / environment that further attenuates the signal's propagation. The radio characteristic within the area to be covered is influenced by the objects and materials typically located in buildings. The doughnut-shaped radio characteristic is therefore deformed accordingly.



Doughnut-shaped radio characteristic of a DECT base station

Radio Propagation Conditions

The typical radio range of a single RFP depends on the regulatory domain (due to regulatory transmit power limits) as well as on the environment:

- US: outdoor range is up to 590 ft, while indoor range is up to 80 ft.
- EU: outdoor range is up to 300 m, while indoor range is up to 30 m.

An ideal location for installing the RFP is a height of between 6.6 ft and 8.2 ft (2 m and 2.50 m) for room heights between 8.2 ft and 9.8 ft (2.50 m and 3 m). For higher rooms, the ideal installation height increases accordingly while maintaining a minimum ceiling distance of 1.6 ft (0.50 m). An installation height of less than 4.9 ft (1.50 m) is not recommended. Installation inside a dropped ceiling, cabinets or other enclosed furnishings is not recommended as this considerably impairs the radio range.

In radio technology there are many interference factors that affect mainly the range and quality of the transmission. In principle you need to differentiate between two types of interference factors:

- Interference by obstacles that attenuate and/or reflect radio propagation, causing dead spots
- Interference due to other radio signals (e.g. other non-synchronous DECT systems) which lead to transmission errors.

The receive power of DECT signals can fluctuate a great deal locally, within only a few centimetres. This means that signal interference can be reduced or eliminated simply by altering the position of the base station.

Obstacles may include:

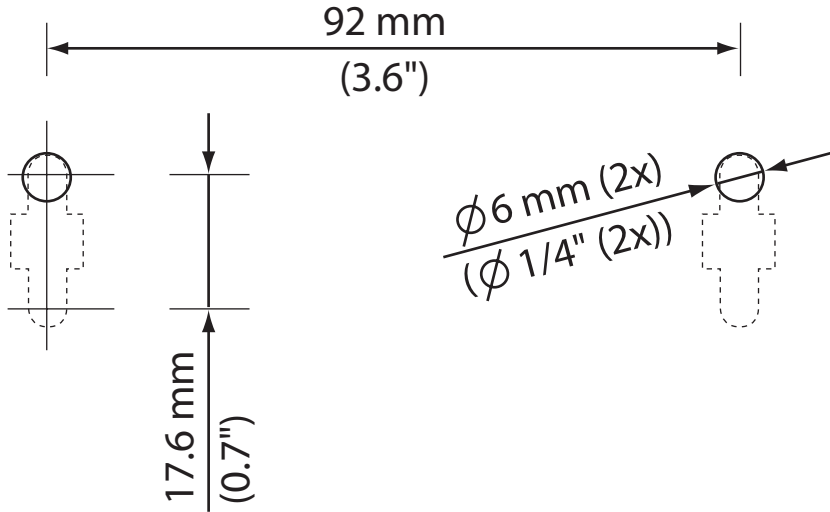
- Moving metal objects such as lifts, cranes, carriages, escalators, blinds, especially ones that are actuated automatically (the influence of such obstacles varies and is therefore difficult to assess).
- Metal-panelled rooms and large metal-clad objects such as air conditioners, computer rooms, metallized glassed areas (mirrored), fire protection walls, storage tank installations, refrigerating units, boilers, pipes.
- Building structures and installations such as steel-reinforced concrete ceilings and walls, stairways, long corridors, rising mains, cable ducts.
- Room furnishings such as metal shelves, file cabinets.

The following tables shows range losses (in percent compared to ideal conditions)

Building materials	Range loss
Glass, timber, untreated	approx. 10 %
Timber, treated	approx. 25 %
Plasterboard	approx. 27 % – 41 %
Brick wall, 3.94 to 4.72 in (10 to 12 cm)	approx. 44 %
Brick wall, 9.45 in (24 cm)	approx. 60 %
Aerated concrete wall	approx. 78 %
Armoured glass partition	approx. 84 %
Steel-reinforced concrete ceiling	approx. 75 % – 87 %
Metal-coated glass	approx. 100 %

Wall Mounting

The RFP SL35 IP is mounted on the wall with two screws as shown in this figure:



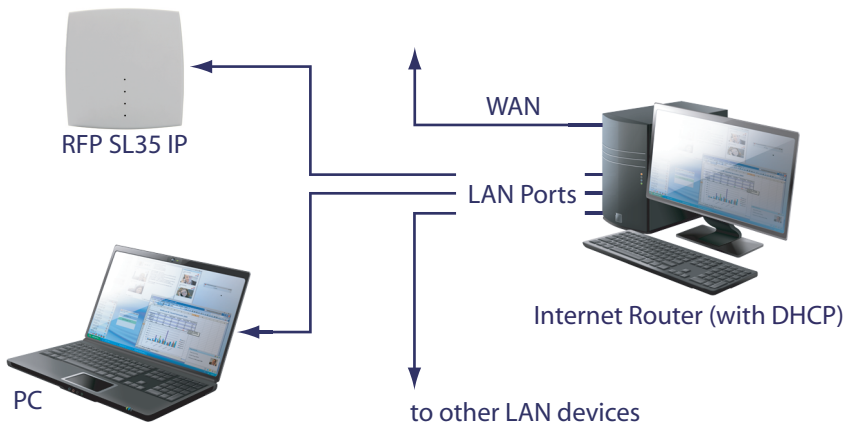
Mounting plan (not to scale, please use drilling template included with the RFP)

Getting Started

This chapter describes how to integrate the SIP-DECT™ Lite solution into an existing local area network (LAN) and operate one or more DECT handsets. There are two possible scenarios described that are depicted below.

Provider-operated SIP server

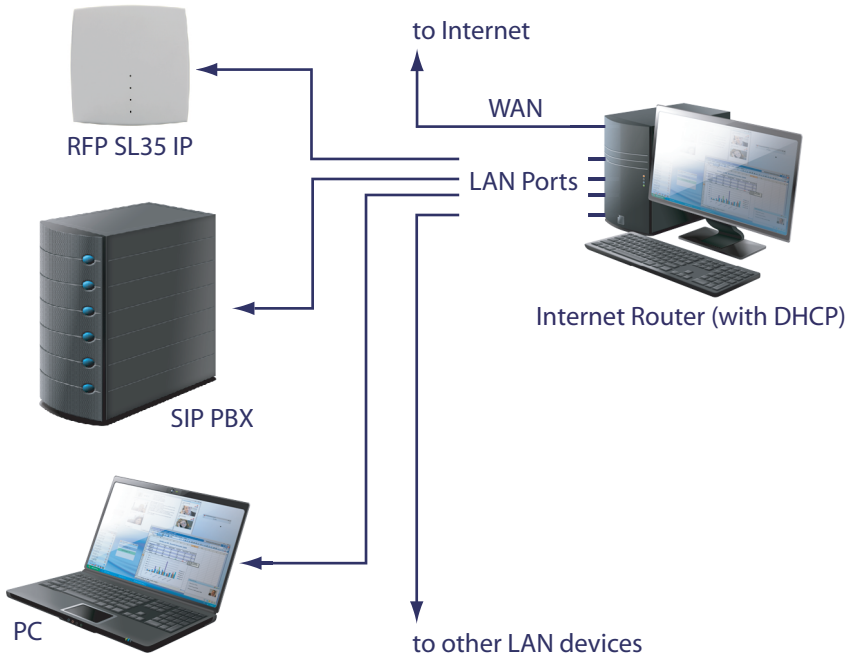
You received the SIP-DECT™ Lite solution as part of a provider package. In this scenario, the provider operates the SIP server. The SIP server offers one or more SIP accounts where you can log in and use telephony services. Such a delivery package may e.g. include a list of SIP phone numbers and PIN codes.



Provider-operated SIP Server

User-operated SIP PBX

You operate your own SIP PBX. In this scenario you can use the SIP-DECT™ Lite solution to use DECT handsets. You need to create SIP user accounts that match existing SIP accounts on the SIP PBX.



User-operated SIP PBX

LAN Prerequisites

The description emphasizes on a LAN setup that should match most smaller LANs as depicted above. In this LAN setup, the Internet router provides the IP configuration via DHCP. The RFP SL35 IP and a number of workstation PCs are connected by means of a switch device that is normally integrated with the Internet router (LAN ports).

The Internet router also provides access to the Internet (WAN port). Depending on the Internet connection technique, the WAN connection may be different (e.g. include a splitter device for DSL). Refer to the Internet router's documentation for details.

This depicted LAN setup should match most LAN environments, but your specific LAN setup may be different, especially if you operate a larger company LAN. Contact your LAN administrator to plan and coordinate the necessary LAN setup.

The RFP SL35 IP should be connected by means of a wired LAN connection that offers at least 100 Mbit/s.

Provider-operated SIP server

During start-up, the RFP contacts a configuration service via the Internet connection (“Aastra Redirection and Configuration Service”, RCS) that in turn redirects to your providers services. With this, the RFP queries the configuration necessary to be operated automatically.

User-operated SIP PBX

Basic configuration is possible via the DECT handset that is included in the delivery package. However, for extended configuration settings, you also need a workstation PC in order to connect to the OMM web service of the RFP SL35 IP.

Unpacking the DECT Handset

Start by unpacking and charging the DECT handset that is part of the delivery. For detailed instructions on this topic, please refer to the “Aastra 610d, 620d, 630d; SIP-DECT User’s Guide; Handset Release \geq 4.0”. Briefly, proceed in the following order:

- 1.** Unpack the DECT handset’s delivery box. The box contains a DECT handset, a battery, a DECT handset charger cradle, a plug-in power supply, and a number of interchangeable AC clips for different countries.
- 2.** Select the AC clip that matches your mains wall sockets. Insert the AC clip into the DECT handset’s plug-in power supply. Make sure the AC clip is firmly inserted and locked. Insert the low voltage connector of the plug-in power supply into the socket of the DECT handset charger cradle. Connect the plug-in power supply to a mains power socket.
- 3.** Open the DECT handset’s rear battery compartment. Insert the battery. Close the DECT handset’s rear battery compartment. Place the DECT handset into the charger cradle.

The DECT handset’s signalling LED lights up in red after some seconds, indicating that it charges the battery. A full charging cycle requires up to 2.5 hours. The handset’s signalling LED lights up in green to indicate a fully charged battery.

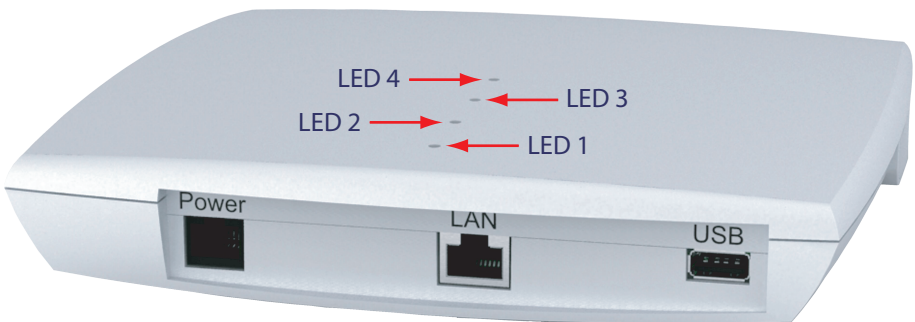
Note

You can wait until the DECT handset is fully charged. Alternatively, operate the DECT handset while it is placed in the charger cradle or wait at least 15 minutes until the battery has reached a decent charging status.

Unpacking the RFP SL35 IP

Continue by unpacking and connecting the RFP SL35 IP that is part of the delivery. Proceed in the following order:

1. Unpack the RFP SL35 IP delivery box. The box contains the RFP and a plugged in standard USB flash drive. As an option, a plug-in power supply and a number of interchangeable AC clips for different countries are included.
2. You can wall-mount the RFP later on, but for getting started it is sufficient to place the RFP on a table. The rear panel of the RFP provides 3 sockets that are labelled "Power", "LAN" and "USB". The USB flash drive may contain a software update that is activated automatically if the RFP is powered on. Also, the RFP writes a backup of the current PARK to the USB flash drive during power-on.



RFP SL35 IP: LEDs and sockets

Meaning of the LEDs:

LED 1: Info / Booter status LED,

LED 2: System status LED,

LED 3: DECT status LED,

LED 4: unused

3. Connect the RFP to your LAN. For this, insert one end of a LAN connection cable in the LAN socket. Insert the other end of the LAN connection cable in a free port of your LAN switch / Internet router. If the switch device supports PoE (Power over Ethernet), the RFP is powered on now.

The SIP-DECT™ Lite package includes an external power supply to be used if you cannot operate the RFP via PoE. Select the AC clip that matches your mains wall sockets. Insert the AC clip into the RFP's plug-in power supply. Make sure the AC clip is firmly inserted and locked. Insert the low voltage connector of the plug-in power supply into the "Power" socket of the RFP. Connect the plug-in power supply to a mains power socket. The RFP is powered on now.

4. During start-up, the RFP signals its status with 3 LEDs. The first LED for example lights up in red shortly after power-on. After some seconds, the first LED changes to orange during software start-up / IP address configuration, then it changes to green to indicate an operational RFP. Wait until the operational status is reached.

Note

If the RFP cannot acquire an IP configuration via DHCP during start-up, the first LED indicates this status by staying orange while LED 2 and LED 3 are lighted up in green. Check your DHCP server / Internet router's DHCP configuration. You may also continue by configuring a static IP address with the next steps.






Tip: If you power down the RFP later on (e.g. to mount the RFP to its final wall mounted position), you can plug out the USB flash drive. You should make a backup of the USB drive. Insert the USB flash drive in a free USB socket on your PC and copy the contents to a safe location. Especially the "PARK.xml" file is required later on if you need to perform the factory reset procedure.

Fast Forward

If you received the SIP-DECT™ Lite solution as part of a provider package, you may optionally read and perform the steps in the following sections ([Checking IP Configuration](#), [Configuring a Static IP](#), and [Configuring SIP-DECT™ Lite](#)). However, in a typical scenario you simply perform the login procedure on the DECT handset using a phone number and a PIN code from the list that you have received (see User Login / Logout on the Handset starting on page 24). After this, you are able to use telephony services offered by your provider.

Checking IP Configuration

The RFP SL35 IP and the DECT handset of a delivery package are pre-subscribed during product packing. For this reason, it is possible to query the RFP status and IP configuration from the DECT handset's system menu (see also Menu Tree on the Handset on page 43).



1. Press and hold the red end key  for one second to power on the DECT handset. Wait until the DECT handset is started up and displays the standard screen.
2. Press and hold the softkey  to bring up the **System menu**. Repeatedly press the down navigation key  to highlight the **Administration** entry. Press the  softkey to activate the menu entry.
3. The **Admin Menu** contains different menu entries. Highlight the **Status** menu entry and confirm with . The following IP address configuration items are displayed:

Configuration via: With a typical LAN setup (see User-operated SIP PBX on page 14), this item should display "DHCP".

IP address: This item shows the IP address that is aquired via DHCP. You can start a web browser and type in the numbers displayed under **IP address** in the browser's address input field in order to bring up the OMM web service of the RFP SL35 IP. Some browsers require the "https://" prefix, i.e. you need to enter "https://192.168.1.1/".

Netmask: This item determines the IP address range that is valid in the LAN. Devices with an IP address in this range can be contacted directly whithout forwarding data packets via a gateway / router device.

Gateway: If the RFP SL35 IP needs to contact an IP address that is outside the IP address range of the LAN, the data packets are forwarded to this IP address. With a typical LAN setup, this configuration item shows the IP address of the Internet router.

4. Close the display with the  softkey. You may also return to the standard screen by briefly pressing the end key .

Note

If the RFP cannot determine an IP address configuration via DHCP during start-up, the displayed configuration items are empty. You may change the configuration of your Internet router / DHCP server and restart the RFP. Otherwise you may continue with a static IP address configuration as it is described in the next section.

Configuring a Static IP

In a typical LAN setup, the automatic IP address configuration via DHCP should work for you and you can skip to Configuring SIP-DECT™ Lite starting on page 20. If the automatic IP address configuration does not match your requirements or if there is no working DHCP server in your LAN, you may change to a static IP address configuration.

1. On the DECT handset, press and hold the softkey **»»»** to bring up the **System menu**. Navigate to the **Administration** menu entry and confirm with **Ok**.
2. Navigate to the **System** menu entry and confirm with **Ok**.
3. The **System** menu entry requires an administrator login. Enter the **User name** that is configured for the "Full access" user account of the SIP-DECT™ Lite solution. With the factory default configuration, enter "Omm".

To do so, press the **6** key three times to enter the uppercase letter "O". Wait a second, then press the **6** key to enter the letter "m". Again wait a second, then press the **6** key to enter a second "m". Press the **C** key to delete mistyped characters. Confirm with **Ok**.

4. Enter the **Password**. In factory default configuration, the password is "Omm" which requires the same input sequence as described in the previous step. If necessary, press the star key ***** to change the input mode (first uppercase -> uppercase -> lowercase). Press and hold keys for one second to enter a digit. Confirm the password with **Ok**.
5. Navigate to the **Net parameters** menu entry. Highlight the **Static config** menu entry and confirm with **Ok**.

A sequence of input fields is displayed, prompting you the configuration data. You can abort at any time by pressing the **Esc** softkey.

6. Enter the **IP address**, **Netmask**, and **Gateway IP** addresses. You need to enter valid IP addresses in this step.

The mode for each input starts with the digits mode. Press the **0** to **9** keys to enter the first digits of the IP address. Press the star key ***** to change the input mode to letters. Press the **0** key to enter a dot. Wait a second, then press the star key ***** to change back to digit mode, then enter the next digits of the IP address.

Confirm each input with **Ok**.

7. An **Info** box is displayed, stating **Settings saved**. Confirm with **Ok**.

The **Net parameters** menu now indicates a static IP address configuration by displaying a green check mark besides the **Static config** entry.

Configuring SIP-DECT™ Lite

In order to operate the RFP SL35 IP, the SIP server / SIP PBX IP address as well as a number of SIP user accounts need to be configured.

Note

It is possible to do basic configuration using the DECT handset (see Configuration via the DECT Handset starting on page 21). However, it is much more convenient to use the OMM web service of the RFP SL35 IP for this task (see Configuration via the OMM Web Service starting on page 22).

Provider-operated SIP server

You may check the configuration that was acquired automatically, e.g. compare the SIP user accounts to the list of phone numbers that you received. Typically, you should not change the settings on the **System: SIP** page of the OMM web service. Also, you should not alter the SIP authentication of the SIP user accounts listed on the **SIP users / devices** page of the OMM web service.

User-operated SIP PBX

If you operate your own SIP PBX, you are required to set up the SIP PBX IP address as well as a number of SIP user accounts that matches already existing accounts on your SIP PBX.

Configuration via the DECT Handset

1. On the DECT handset, press and hold the softkey **»»** to bring up the **System menu**. Navigate to the **Administration** menu entry and confirm with **Ok**.
2. Navigate to the **System** menu entry and confirm with **Ok**.
3. Enter the **User name** and the **Password** that are configured for the "Full access" user account of the SIP-DECT™ Lite solution (see description on page 19).
4. Navigate to the **SIP** menu entry and confirm with **Ok**.

A sequence of input fields is displayed, prompting you to enter the configuration data. You can abort at any time by pressing the **Esc** softkey.

5. Enter the IP address of your SIP PBX in the **Proxy server** and **Registrar server** input fields. Typically, you should leave the default port number (5060) in the **Proxy port** and **Registrar port** input fields unchanged. Confirm each input with **Ok**.
6. An **Info** box is displayed, stating **Settings saved**. Confirm with **Ok**.
7. Press the **Esc** softkey to return to the **Admin Menu**.
8. Navigate to the **SIP users / devices** menu entry and confirm with **Ok**.
9. Navigate to the **New SIP user** menu entry and confirm with **Ok**.

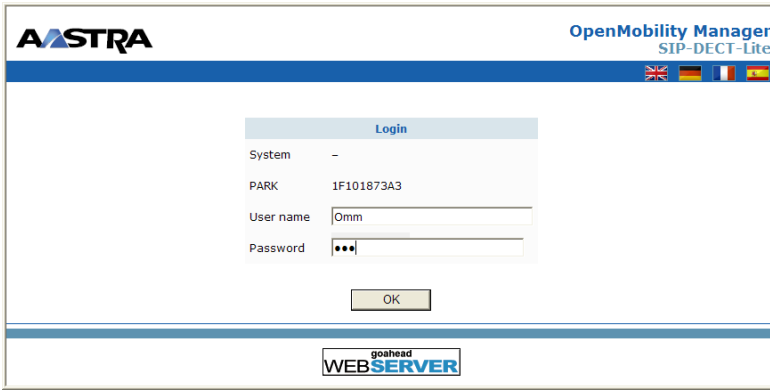
A sequence of input fields is displayed, prompting you to enter the configuration data. You can abort at any time by pressing the **Esc** softkey.

10. You need to configure SIP user account data that matches accounts on your SIP PBX. Enter the **Display name** ("display name"), **Number** ("sip id"), and **PIN** to be used on the DECT handset for login in. Enter the **SIP user name** ("SIP authentication user name"), **SIP password** that are required to authenticate on the SIP PBX. Confirm with **OK**.
11. An **Info** box is displayed, stating **Settings saved**. Confirm with **Ok**.

You can create multiple SIP user accounts that can be used with a DECT handset by logging in and out. If you subscribe more DECT handsets later on, you can login to an arbitrary SIP user account from any DECT handset. Make sure to configure secure and different PIN codes for each SIP user account (other than 0000 and 1234).

Configuration via the OMM Web Service

1. Start a web browser on a PC connected to your LAN. Enter the IP address of the RFP SL35 IP in the address input of the browser (see Checking IP Configuration on page 18 on how to query the IP address). Some browsers require the “https://” prefix, i.e. you need to enter “https://192.168.1.1/” instead.

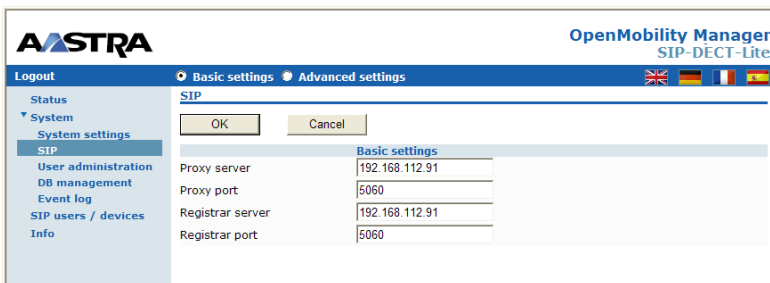


2. Enter the default **User name** (“Omm”) and **Password** (“Omm”). Confirm with **OK**.

On initial login, the end user license agreement is displayed. Read the license text and confirm with **Accept**.

Optionally you may change the default passwords for the “Full Access” and “Root (SSH only)” user accounts. Navigate to the **System: User administration** page. Type in a secure password in the **Password** and **Password confirmation** input fields. Proceed with **OK**.

3. Use the menu available on the left to navigate to the **System: SIP** page.



Enter the IP address of your SIP PBX in the **Proxy server** and **Registrar server** input fields. Typically, you should leave the default port number (5060) in the **Proxy port** and **Registrar port** input fields unchanged. Confirm with **OK**.

4. Navigate to the **SIP users / devices** page. Click on **New** to create a new SIP user account.

The screenshot shows the Aastra Manager DECT-Lite interface. The main window is titled "New SIP user" and contains two sections: "General settings" and "SIP authentication".

General settings:



- Display name: John Miller
- Number: 3001
- PIN: 874421
- Login/Additional ID: [empty]
- SOS number: [empty]
- ManDown number: [empty]
- Voice mail number: [empty]

SIP authentication:

- User name: sds-3001
- Password: [masked with dots]
- Password confirmation: [masked with dots]

At the bottom of the form are "OK" and "Cancel" buttons. The background shows the Aastra Manager interface with a sidebar menu and a "New" button highlighted with a red arrow.

You need to configure SIP user account data that matches accounts on your SIP PBX. Enter the **Display name** ("display name"), **Number** ("sip id"), and **PIN** to be used on the DECT handset for login in. Enter the **User name** ("SIP authentication user name"), **Password**, and **Password confirmation** that are required to authenticate on the SIP PBX. Confirm with **OK**.

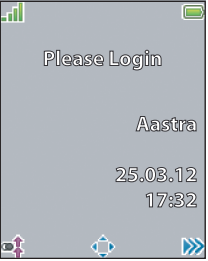
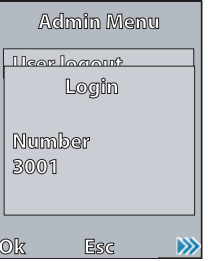

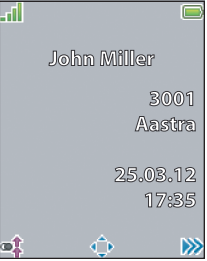
On delivery a device entry is preconfigured. This is indicated by the  icon on the **SIP users / devices** page. After you have configured the first SIP user account, a second (SIP user account) entry is displayed (indicated by the  icon).

You can create multiple SIP user accounts that can be used with a DECT handset by logging in and out. If you subscribe more DECT handsets later on, you can login to an arbitrary SIP user account from any DECT handset. Make sure to configure secure and different PIN codes for each SIP user account (other than 0000 and 1234).

User Login / Logout on the Handset

You need to execute a login sequence to use any telephony services with the DECT handset. For this, you dial the phone number / user ID and pin code of the SIP user account that you want to occupy.

Login Procedure

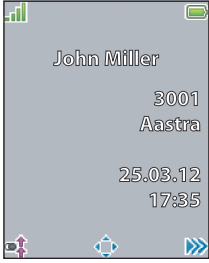
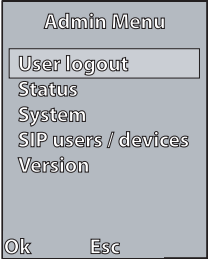

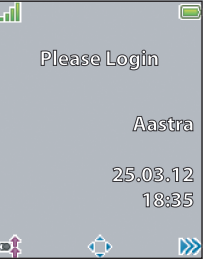
			
Display of an unused phone.	Enter phone number or user ID.	Enter the PIN to gain access.	You are logged in right now.

1. Press and hold the softkey **»»»** to bring up the **System menu**. The **Administration** menu entry is displayed. Confirm with **Ok**.
2. Select the **User login** menu entry and confirm with **Ok**. An input field is displayed, prompting you to enter a **Number** or a **User ID**.
3. Enter the phone number / user ID of the SIP user account and confirm with **Ok**.
4. An input field is displayed, prompting you to enter a **PIN**. Enter the pin code that is configured for the SIP user account. Confirm with **Ok**.

The DECT handset's standard screen now displays the user's name as well as the phone number that is configured with the SIP user account. The DECT handset is ready to be used for telephony functions now.

If the DECT handset is logged in, it is possible to log out via the the **System menu** > **Administration** > **User logout** menu entry.

Logout Procedure

			
Display of a used phone.	Select the user logout menu entry.	Enter PIN to proceed.	Display of an unused phone.

1. Press and hold the softkey **»»»** to bring up the **System menu**.
2. Navigate to the **Administration** menu entry and confirm with **Ok**. Then select the **User logout** menu entry and confirm with **Ok**.
An input field is displayed, prompting you to enter a **PIN**.
3. Enter the pin code that is configured for the currently used SIP user account. Confirm with **Ok**.

Note

It is not possible to login to the same SIP user account on different handsets concurrently. If the login sequence for a SIP user account is performed on another DECT handset, the DECT handset that was previously logged in to the SIP user account will be logged out automatically.







Subscribing DECT Handsets


The SIP-DECT™ Lite solution is delivered with one pre-subscribed DECT handset. Additionally, further DECT handsets can be subscribed to the system. The subscription procedure announces the DECT handset to the RFP SL35 IP and also configures the encryption used on the air interface. After performing the subscription procedure, the DECT handset is able to log in, thus enabling telephony functions.

For subscribing DECT handsets, the RFP needs to be switched to a special operation mode. The subscription mode is active for five minutes after powering on the RFP and also after the subscription mode has been activated.

Activating the Subscription Mode on the Handset

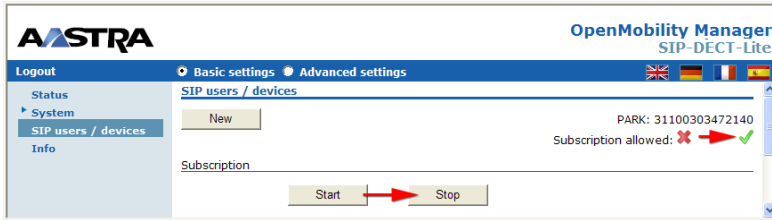
Use the following procedure to activate the subscription mode on the handset.

1. On the DECT handset, press and hold the softkey  to bring up the **System menu**. Navigate to the **Administration** menu entry and confirm with .
2. Navigate to the **SIP users / devices** menu entry and confirm with .
3. Enter the **User name** and the **Password** that are configured for the “Full access” user account of the SIP-DECT™ Lite solution (see description on page 19).
4. Navigate to the **Subscription allowed** menu entry. The  icon indicates that the subscription mode is disabled.
5. Press the  softkey. The subscription mode is enabled (indicated by the  icon).

After activating the subscription mode, you can subscribe new DECT handsets to the system. The subscription mode is deactivated automatically after five minutes. Alternatively, press the  softkey.

Activating the Subscription Mode in the OMM Web Service

Alternatively, you can activate the subscription mode using the OMM web service.


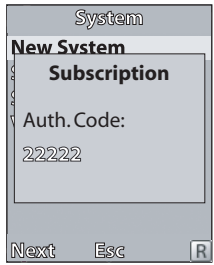




1. Log in to the OMM web service. Navigate to the **SIP users / devices** page.
2. Under the **Subscription** heading, click the **Start** button.

After activating the subscription mode, you can subscribe new DECT handsets to the system. The subscription mode is deactivated automatically after five minutes. Alternatively, click the **Stop** button on the **SIP users / devices** page.

Subscription Procedure on the Handset

Handset display while performing the subscription procedure

			
Display of unsubscribed phone.	Enter authentication code.	Start the subscription.	Subscription executes.

To subscribe Aastra 610d / 620d / 630d DECT handsets, proceed as follows:

1. On the DECT handset, briefly press the softkey **»»»** to bring up the **Menu**. Navigate to the **System > New system** menu entry. Confirm with **Ok**.

An input field is displayed, prompting you to enter an **Auth Code**.

2. Enter the authentication code. With the factory default configuration, enter "22222". Confirm with **Ok**.

You may view and change the **DECT authentication code** setting on the **System: System settings** page of the OMM web service (**Advanced settings** mode only).

3. Highlight the **Subscription** menu entry. Confirm with **Ok**.

An **Info** box is displayed, stating **Subscription - Please wait**. The subscription should finish shortly after this with a success message. You can abort the subscription at any time using the **Esc** softkey.

Tip: As an optional step, you can enter the PARK code of the SIP-DECT™ Lite to ensure that the DECT handset subscribes to the correct DECT system. The PARK is a globally unique decimal number that you may view on the **Status** page of the OMM web service. After entering the **Auth Code** select the **Enter PARK** menu entry before proceeding with the subscription.

You can subscribe a larger number of DECT handsets (up to 512), but you should be aware that only 8 concurrent channels are available for DECT telephony with a single RFP SL35 IP.

Furthermore, the SIP-DECT™ Lite security concept does not rely on subscription alone. You cannot perform any critical function without logging in – either with a SIP user account / PIN combination for telephony or by entering the user name / password combination that is valid for the OMM web service for changing the system configuration (see Configuring a Static IP starting on page 19).

Advanced Configuration

Besides setting up basic telephony services which is described under Getting Started starting on page 13, the SIP-DECT™ Lite solution supports additional features and settings that are e.g. available on the OMM web service.

The following sections emphasizes on advanced topics. However, you should be aware that the SIP-DECT™ Lite solution provides a single-cell DECT network that offers only limited radio coverage. The SIP-DECT™ Lite solution is part of the SIP-DECT® product family that offers larger radio coverage by supporting multi-cell DECT networks with up to 2.048 RFPs. The different entities that form those large networks are also available with the SIP-DECT™ Lite solution:

- DECT handsets (PP, portable parts): mobile telephones that communicate via DECT radio. Communication includes voice data as well as management data (e.g. the phone directory is transferred via radio).
- RFP (Radio Fixed Part): a hardware device that runs the SIP-DECT™ Lite software. The SIP-DECT™ Lite RFP has a DECT radio that is used to communicate with DECT handsets. Also, the RFP communicates via Ethernet / IP with a SIP PBX / SIP server.
- OMM (OpenMobility Manager): The OMM is the software running on the RFP SL35 IP. It allows to manage configuration, telephony and messaging. The OMM is presented as a web-based configurator – the OMM web service.

Note

You cannot integrate the RFP SL35 IP to a multi-cell SIP-DECT® network. While the hardware is fully compatible, only the SIP-DECT™ Lite software is accepted. Contact an Aastra sales representative for upgrading conditions.

Basic Settings and Advanced Settings

Features that are relevant for most users of the SIP-DECT™ Lite solution are available with the OMM web service's default **Basic settings** mode. You can view additional settings if you switch to **Advanced settings** mode at any time.



Updating the Software

The RFP has an internal flash memory that stores the SIP-DECT™ Lite software. This software is loaded and started if you power on the RFP. The software consists of the following components:

- Boot loader, operating system, and OMM software
- Firmware for Aastra 610d / 620d / 630d DECT handsets

Manual Update

You can download the SIP-DECT™ Lite software package from the Aastra web pages on demand. To update the software stored on the RFP, proceed as follows:

1. Insert the USB flash drive in a free USB port on your PC.
2. Unpack the SIP-DECT™ Lite software package to the toplevel directory of the USB flash drive. Do **not** unpack the software package to any subdirectory.
3. Transfer the USB flash drive to the RFP. Unplug the RFP's power supply.
4. Insert the USB flash drive into the backside port that is labelled "USB".
5. Restore power to start the update procedure.

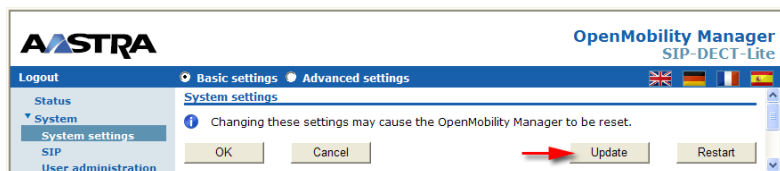
During power-on, the RFP detects the newer software on the USB flash drive and updates the internal flash memory from these files.

Note

All settings are preserved when updating to newer software versions.

Background Update

It is also possible to update the SIP-DECT™ Lite software in the background. This procedure only updates the internal flash. The newer software version is activated if the system is restarted later on.



1. Log in to the OMM web service. Navigate to the **System: System settings** page.
2. Click on the **Update** button to start the background update procedure.

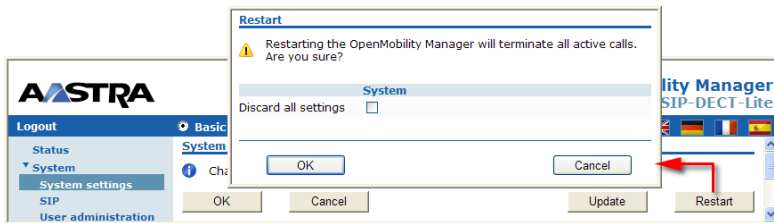
Note

Switch to **Advanced settings** mode to view the **URI for SW update** setting on the **System settings** page. The software download URL may be changed via configuration files that are acquired during provisioning (see LAN Prerequisites starting on page 14 under the *Provider-operated SIP server* heading).

Restoring Factory Defaults

To restore the factory default settings, you will need the USB flash drive that is part of the delivery. Proceed as follows:

1. Insert the USB flash drive in a free USB port on your PC. Verify that the necessary "PARK.xml" file is present in the toplevel directory of the USB flash drive.
2. Insert the USB flash drive into the backside port that is labelled "USB".
3. Log in to the OMM web service. Navigate to the **System: System settings** page.



4. Click the **Restart** button to open the restart options window. Activate the **Discard all settings** option. Note that this option is automatically disabled if the "PARK.xml" file is missing on the USB flash drive. Confirm with **OK**.

The RFP restarts with the factory default configuration of the SIP-DECT™ Lite solution. This also includes removing all DECT handset subscriptions. In order to view the current IP configuration, you may want to subscribe at least one DECT handset Aastra 600d (see also the chapter entitled Subscription Procedure on the Handset starting on page 27). You may also restore a previous configuration (see also the chapter entitled Backing up and Restoring the SIP-DECT™ Lite Configuration starting on page 33).

Note

The "PARK.xml" file contains the globally unique PARK code and the regulatory domain. If you discard the configuration, the RFP needs to read this file from the USB flash drive during startup. You can backup this file from the internal flash of the RFP to an empty USB flash drive before you discard the configuration. For this, insert the empty USB flash drive into the RFP. Power off the RFP and then power it on again.

After powering on the RFP again you can also perform a factory reset within a few minutes by one of the following procedures:

- On the DECT handset press and hold the softkey **»»»** to bring up the **System menu**. Repeatedly press the down navigation key **▼** to highlight the **Factory reset** menu entry. Press the **OK** softkey. An enquiry is displayed. Confirm the enquiry by pressing the **OK** softkey again.
- On the **Login** page of the OMM web service press the **Restart** button. The restart options window opens. Activate the **Discard all settings** option. Note that this option is automatically disabled if the "PARK.xml" file is missing on the USB flash drive. Confirm with **OK**.

The screenshot displays the login interface for the OpenMobility Manager SIP-DECT-Lite system. At the top left is the Astra logo, and at the top right is the text 'OpenMobility Manager SIP-DECT-Lite' with flags for UK, Germany, France, and Spain. The main section is titled 'Login' and contains the following fields and buttons:

Login	
System	-
PARK	1F101873A3
User name	<input type="text"/>
Password	<input type="password"/>
<input type="button" value="OK"/> <input type="button" value="Restart"/>	

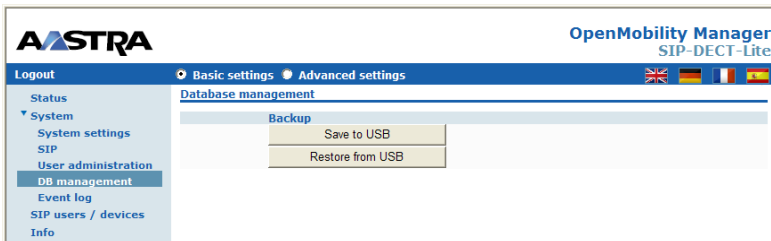
At the bottom of the page, there is a logo for 'goahead WEB SERVER'.

Backing up and Restoring the SIP-DECT™ Lite Configuration

The OMM database contains all configuration settings which are configurable via the OMM web service interface. This includes the OMM configuration, the DECT handset subscriptions, and the SIP user accounts. You should make backups of the OMM database on a regular basis.

Backup / restore configuration via the OMM web service

1. Make sure the USB flash drive is inserted to the backside port of the RFP that is labelled "USB".
2. Log in to the OMM web service. Navigate to the **System: DB management** page.



3. Click on the **Save to USB** button to start the backup procedure. The OMM configuration is saved to the "omm_conf.txt" file in the toplevel directory of the USB flash drive.
4. Click on the **Restore from USB** button to restore a previously created backup.

After restoring a backup, you should navigate to the **System: System settings** page. Click the **Restart** button to activate the restored configuration.

Restoring a backup does not overwrite the currently valid passwords with those from the backup. This ensures that you can still log in to the OMM web service with a known password.

Tip: You should transfer the USB flash drive to your PC and copy the flash drives contents to a secure storage location.

Other backup options exist, if you switch to the **Advanced settings** mode of the OMM web service. Refer to page 59 for details.

Backup / restore configuration via the DECT handset

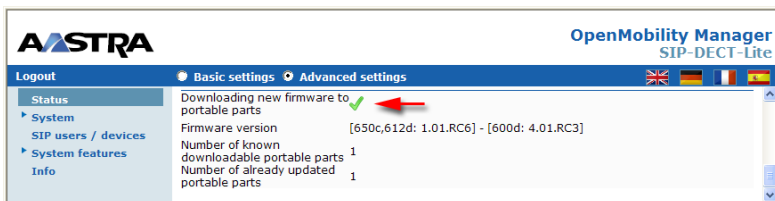
1. Make sure the USB flash drive is inserted to the backside port of the RFP that is labelled "USB".
2. On the DECT handset, press and hold the softkey **»»»** to bring up the **System menu**. Navigate to the **Administration** menu entry and confirm with **Ok**.
3. Navigate to the **System** menu entry and confirm with **Ok**.
4. Enter the **User name** and the **Password** that are configured for the "Full access" user account of the SIP-DECT™ Lite solution (see description on page 19).
5. Navigate to the **DB management** menu entry and confirm with **Ok**.
6. Select the **Save to USB** menu entry to save the current OMM configuration on the USB flash drive. Select the **Restore from USB** menu entry to restore a previously created backup from the USB flash drive.

Download Over Air

The "Download over Air" feature allows to update the handset firmware without any user interaction over the existing DECT air interface. This feature is available for Aastra 600d handsets. "Download over Air" is a background process, i.e. it is executed without any interruption of the telephony services.

The handset firmware is part of the SIP-DECT™ Lite software package. On delivery this software package is included on the USB flash drive.

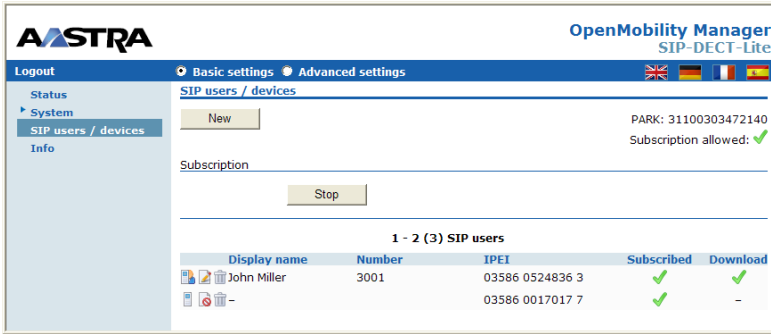
The status of the "Download over Air" service together with some statistics is presented in the **SIP users / devices** section on the **Status** web page.







The screenshot shows the OpenMobility Manager SIP-DECT-Lite web interface. The top navigation bar includes "Logout", "Basic settings", and "Advanced settings". The left sidebar shows a menu with "Status", "System", "SIP users / devices", "System features", and "Info". The main content area displays the status of the download over air service, which is "Downloading new firmware to portable parts" with a green checkmark and a red arrow pointing to it. Below this, the firmware version is listed as "[650c,612d: 1.01.RC6] - [600d: 4.01.RC3]". Statistics show "Number of known downloadable portable parts" as 1 and "Number of already updated portable parts" as 1.



Logout	Basic settings	Advanced settings
Status	Downloading new firmware to portable parts	[650c,612d: 1.01.RC6] - [600d: 4.01.RC3]
System	Firmware version	
SIP users / devices	Number of known downloadable portable parts	1
System features	Number of already updated portable parts	1
Info		

The individual download status of each PP is presented on the **SIP users / devices** web page.



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. it is not an Astra 600d)
	The handset is paged to establish a download connection. In case of a successful connection establishment the handsets calculates the number of bytes to download. This may take several seconds.
xx kbytes left	The download is ongoing and xx kbytes are left.
	The firmware of this handset is up to date.
	The handset is queued in the update-queue for updating (pending).
	<p>Warning</p> <p>The download is barred because of one of the following reasons:</p> <ul style="list-style-type: none"> • The handset is busy (temporary status). • The battery power is lower than 50 % and the handset is not connected to the docking station or the USB interface. • This is not the master download system. A handset can be subscribed on several OpenMobility systems. The first system to which the handset will be subscribed is the “master system”. The handset downloads only from the “master system”. A different “master system” can be chosen inside the local menu of the handset (System > Subscription menu).

Icon	Meaning
	<ul style="list-style-type: none">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: <ul style="list-style-type: none">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.
	Info The download is not possible because of: <ul style="list-style-type: none">the handset is not reachable,the handset is detached. The specific reason is shown as a tooltip.

Background information: 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 Aastra 600d handset sends its actual firmware version within the DECT attachment procedure. If the firmware version does not match the version provided by the OMM, the handset will be queued into the update-queue. Later on the queued handsets will be paged to establish a download connection. After the connection is established, the OMM sends its actual handset firmware version and the handset will request a handset description file. After receiving the handset description file, the handset decides which files are missing or need to be updated. If files are missing or need to be updated the handset initiates the download procedure.

The OMM takes care of the following download scenarios automatically:

- If a handset becomes unreachable e.g. when the handset is switched off, the OMM will update the handset when the PP becomes available again.

- The OMM has the capability of resuming a download from the point where it was last interrupted. e.g. the user leaves the coverage area during download or the 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 resumes automatically when the stop cause is solved.

The Aastra 600d 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 handset 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 handset with a firmware of 1 MB takes approximately 90 minutes.

The “Download over Air” service is delayed after a system startup for one minute to allow the whole DECT system to become active.

OMM User Account Types

The OMM provides three different user account types to manage the SIP-DECT™ Lite solution. These user accounts are preset on delivery. They can be changed in the **User administration** menu of the OMM web service (see page 57) or on the handset via the **System menu > Administration > System > User administration** menu entry (see page 46).

“Full access” account

This account is the “normal” access for the configuration of the SIP-DECT™ Lite solution. You can also use this account to log into the SSH interface of the OMM (see page 38) for debug information. Factory settings are:

- User name: “Omm”
- Password: “Omm”

After initial installation or after resetting the OMM to the factory settings (see page 31), the OMM web service is accessible via the default **Full access** user account with user “Omm” and password “Omm”.

“Read-only” account

Using this account a user is not allowed to configure any item of the SIP-DECT™ Lite solution. This account can only be used on the OMM web service. The account is activated by default and can be deactivated. Factory settings are:

- User name: “user”
- Password: “user”

“Root (SSH only)” account

This account is only applicable on the SSH interface of the OMM (see also page 38). Its purpose is to get detailed information e.g. parameters from the kernel. Factory settings are:

- User name: “root”
- Password: “22222”

Please note: It is highly recommended not to use the **Root (SSH only)** account. It is intended for use by the Aastra technical support only!

SSH User Shell

This SSH user shell addresses administrators with expert experience and the Aastra technical support. Within the SSH user shell the OMM offers a lot of commands. Most of them are useful for diagnostics and may help experts to resolve failures.

To activate the SSH access enable the **Remote access** option on the **System settings** page in the OMM web service (see page 50).

Please note: Some commands can harm the system operation. For this reason you should not activate the **Remote access** option for normal operation.

To log into the SSH user shell:

1. Open an SSH session to the OMM with the “Full access” user name (see also OMM User Account Types starting on page 37).

Example: “ssh Omm@192.168.112.17”

2. Enter the password for the “Full access” account.
3. Type “help” to get a command overview.

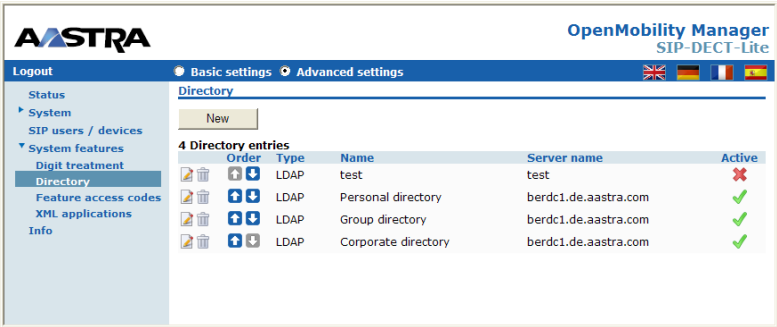
Tip: Microsoft Windows users may use the free SSH client “PuTTY” to get access to the SSH user shell.

Using Directories

Configuration of directories

The SIP-DECT™ Lite system supports connections to one or more LDAP or XML servers that in turn facilitate central corporate directories. These server connections can be configured in the **Directory** menu of the OMM web service (see “Directory” Menu starting on page 64).

You can configure up to 5 directory entries to access multiple servers with specific parameter settings to support different types of directories e.g. global corporate directory, group specific directory, personal directory.





The screenshot shows the OMM web service interface for SIP-DECT-Lite. The left sidebar contains navigation options like Status, System, SIP users / devices, Digit treatment, Directory (selected), Feature access codes, XML applications, and Info. The main content area is titled 'Directory' and shows a 'New' button and a table of 4 Directory entries.

Order	Type	Name	Server name	Active
1	LDAP	test	test	✗
2	LDAP	Personal directory	berdc1.de.aastra.com	✓
3	LDAP	Group directory	berdc1.de.aastra.com	✓
4	LDAP	Corporate directory	berdc1.de.aastra.com	✓

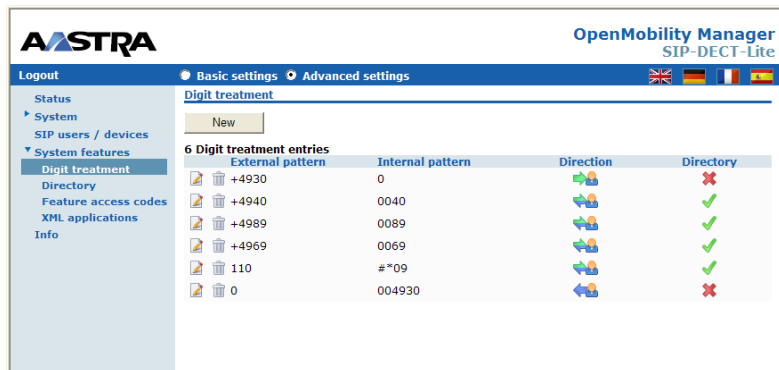
Presentation of directories on the handset

The configured directories are presented to the handset user if he called up the telephone’s central directory (via softkey or via the handset menu). The handset user can choose one of the entries in the list. The name of a directory shown in the list is configured in the OMM when creating the server entry. If only one directory is configured, the telephone’s central directory is displayed immediately when pressing the softkey or selecting central directory from the menu. For information on using the Aastra 600d handsets please refer to the handsets’ user guides (see also Other Valid Documentation starting on page 113).

You can specify the order of the directories in the handset menu on the **Directory** web page of the OMM web service. Use the   icons to define the desired directory order.

Digit treatment for directories

The SIP-DECT™ Lite system supports a number manipulation by the digit treatment feature for corporate directories that handles both incoming and outgoing calls. The rules for digit treatment can be configured in the **Digit treatment** menu of the OMM web service, see “Digit treatment” Menu starting on page 63.



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

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

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

- Incoming call: The calling party number of an incoming call is checked against the configured external prefix pattern. 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 caller list.
- Outgoing call: A dialled number of an outgoing call is checked against the configured internal prefix pattern. If a pattern matches, it will be replaced by the external prefix pattern. This applies to en-bloc dialled numbers and to overlap sending as long as the SIP session has not been initiated. The result of the conversion is not sent to the handset to be displayed or entered in the caller list. If the

user dials the number from the redial list again, the same procedure will be applied as for the initial dialling.

Note: To support digit treatment, it is necessary to have a dial terminator configured. The dial terminator can be configured in the SIP menu of the OMM web service, see “SIP” Menu starting on page 53.

SNMP Configuration

The SIP-DECT™ Lite system is provided with an SNMP agent. This will give alarm information and allow an SNMP management system (such as “HP Open View”) to manage the network.

The SNMP agent can be configured in the **SNMP** menu of the OMM web service, see “SNMP” Menu starting on page 58.

SNMP	
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	
General settings	
Read-only community	public
System contact	Charles Brown
Trap handling	
<input checked="" type="checkbox"/>	
Trap community	trap-secret
Trap host IP address	192.168.112.51

SNMP agent features

- Parameters that are valid for the SIP-DECT™ Lite system (e.g. “sysName”) are generated.
- The RFP uptime can be requested by reading the “sysUpTime” parameter. This value indicates how long the RFP application software (OMM) is running.
- The SNMP agent responds to SNMPv1-read and SNMPv2c-read requests for the standard MIB-II objects. The Management Information Base (MIB-II) contains 11 object groups.
- The SNMP agent receives both SNMPv1 and SNMPv2c traps. It sends a “coldStart” trap when it first starts up. It also sends an enterprise-specific trap “nsNotify-Shutdown” when it stops. When the SNMP agent receives an SNMP request using

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

- The SNMP agent does not support MIB-II write access, SNMPv2-MIB read/write access, NET-SNMP-MIB read/write access, NET-SNMP-AGENT-MIB read/write access and SNMPv3.
- In case of an RFP reset, the SNMP agent configuration does not change. Changing the SNMP configuration on the OMM web service forces the SNMP agent to be reconfigured.

Configuring VLAN

You can operate the SIP-DECT™ Lite RFP in a VLAN, for example to separate the VoIP network traffic from other LAN applications. Two different configuration options exist to support VLANs:

Static VLAN configuration

Activate the **VLAN active** option available on the **System settings** menu page in **Advanced settings** mode (see Net parameters starting on page 51). Also enter the desired **VLAN ID** and restart the RFP. All subsequent data traffic including DHCP queries will be sent and received using the statically configured VLAN ID. Also, to operate the OMM web service with this configuration, your workstation PC needs to be operated in the same VLAN.

Tip: If you cannot reach the Web UI because of a static VLAN setting, you can change the VLAN configuration using the DECT handset's system menu (see [Configuring a Static IP](#) starting on page 19 and [“System” Menu Entry](#) starting on page 44).

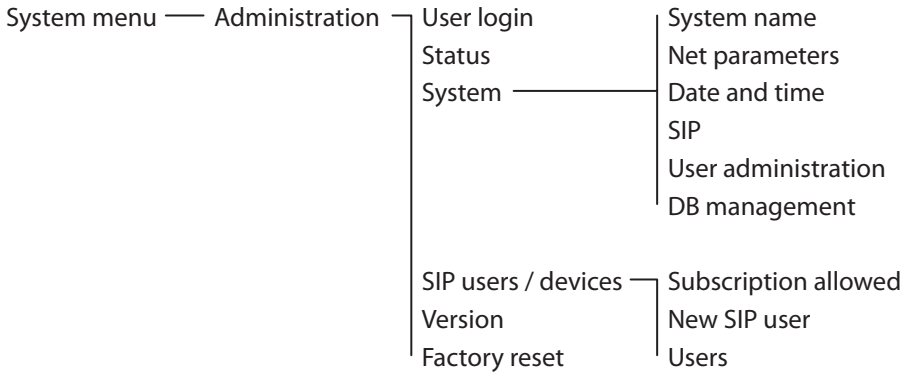
Dynamic VLAN configuration

It is also possible to assign the VLAN ID with DHCP. For this, change your DHCP server configuration for sending the desired VLAN ID via option 132. This will change the start-up sequence of the RFP:

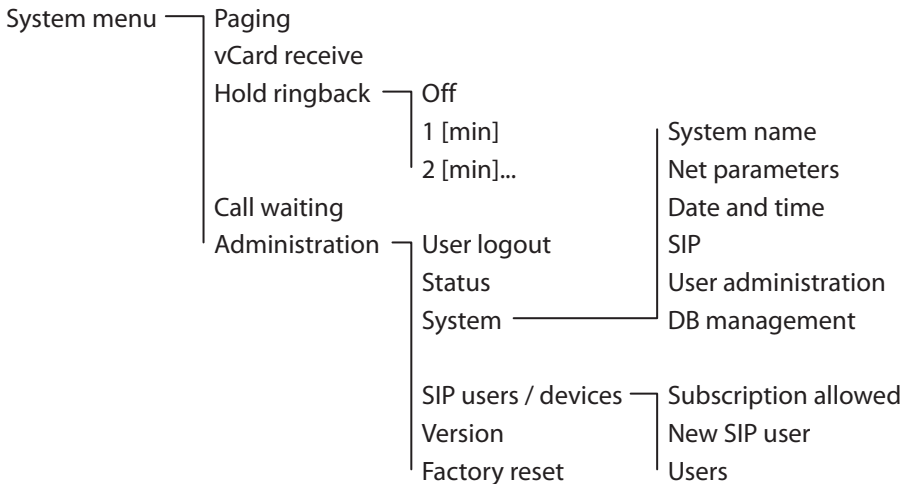
1. During start-up, the RFP sends a DHCP request without any VLAN tagging. The acquired DHCP answer includes option 132 to set the VLAN ID.
2. The RFP switches to the configured VLAN. A second DHCP request is sent with the configured VLAN tag to fetch the IP configuration and other DHCP options.

Menu Tree on the Handset

The menu structure of the DECT handsets is described in-depth in the “Aastra 610d, 620d, 630d; SIP-DECT User’s Guide; Handset Release ≥ 4.0”. However, when using the DECT handsets with the SIP-DECT™ Lite solution, the additional **Administration** menu appears in the **System menu** of the DECT handset:



System menu (DECT handset not logged in)



System menu (DECT handset logged in)

The **System menu > Administration** menu allows to perform basic administration tasks, for example to set a static IP address configuration or to add new SIP user accounts during commissioning (see Configuring a Static IP starting on page 19).

Access the “System menu > Administration” menu


To call up the **System menu > Administration** menu, do the following:

1. Press **»» longer** when idle or
press **»» briefly** when idle. Select **System menu**.
2. Use the down navigation key **▼** to select the **Administration** menu.

Administrator login / logout on the handset

The **System** and **SIP users / devices** menu entries require an administrator login. The login data are the same as for the **Full access** account on the OMM web service (see also the chapter entitled OMM User Account Types starting on page 37). Factory settings are:

- User name: “Omm”
- Password: “Omm”

To logout press the red end key .

“User login” / “User logout” Menu Entries

Use this menu entries to login the handset to the OMM or logout it (see also User Login / Logout on the Handset starting on page 24).

“Status” Menu Entry

Use this menu entry to check the current OMM IP configuration (see also Checking IP Configuration starting on page 18).

“System” Menu Entry

In this menu you configure basic settings of the SIP-DECT™ Lite system. To open the menu enter the **User name** and the **Password** in the **Admin login** mask (see also Administrator login / logout on the handset on page 44).

System name: Enter the system name. The system name is displayed on the OMM login web page and on the subscribed portable parts.

Net parameters: The OMM can be configured via DHCP or via a static IP address configuration. The configuration type is displayed by a symbol:

✓ configuration is enabled

— configuration is disabled

DHCP: Enable this option if the OMM is operated as DHCP client and gets the IP configuration from a DHCP server in your network (DHCP configuration).

Static config.: Alternatively, you can configure a static IP address configuration via the following menu entries:

IP address: Enter the IP address of the OMM. This entry is mandatory.

Netmask: Enter the netmask that the OMM is informed of. This entry is mandatory




Gateway: Enter the IP address of the gateway (i.e router) allocated to the OMM. This entry is mandatory.

DNS server 1 ... DNS server 3: Enter up to three DNS server IP addresses that the OMM is informed of. This entry is optional.

VLAN: You can also operate the RFP in a statically configured VLAN. Change the VLAN configuration with the following menu entries:

Active: Activate this option to use a statically configured VLAN ID.

VLAN ID: Enter the desired ID tag for the statically configured VLAN.

Date and time: The OMM provides a list of pre-configured time zones. Press the  softkey. Select the **Time zone** menu entry to open the list of configured time zones. Select the desired time zone with the down navigation key . The selected time zone is marked with the  symbol.

SIP: The SIP settings cover all global settings matching the SIP signalling and the RTP voice streams. Enter the SIP settings via the following menu entries:


Proxy server: Enter the IP address or the name of the SIP proxy server. If a host name and domain are used for the proxy server parameter, ensure that a DNS server and a domain are specified for your SIP-DECT™ Lite system.

You can configure a DNS server and a DNS domain in the OMM web service (**Net parameters** section on the **System settings** web page).

Proxy port: Enter the SIP proxy server's port number. Default is "5060". To enable DNS SRV support for proxy lookups, use a value of "0" for the proxy port.

Registrar server: Enter the IP address or name of the SIP registrar. This enables the portable parts to be registered with a registrar. If a host name and domain are used for the proxy server parameter, ensure that a DNS server and a domain are specified for your SIP-DECT™ Lite system. You can configure a DNS server and a DNS domain in the OMM web service (**Net parameters** section on the **System settings** web page).

Registrar port: Enter the SIP registrar's port number. Default is "5060". To enable DNS SRV support for registrar lookups, use a value of "0" for the registrar port.

User administration: The OMM provides three different user account types to manage the SIP-DECT™ Lite solution. These user accounts are preset on delivery and can be changed here. The user account types are listed by their current user name. Select the desired account type and press the  softkey.

For information on the different user account types please refer to the chapter entitled OMM User Account Types starting on page 37.

User name: If desired, enter a new user name.

Password: If desired, enter a password.

DB management: The database management (DB management) allows a flexible backup and restore management of the OMM database (see also Backing up and Restoring the SIP-DECT™ Lite Configuration starting on page 33).

Save to USB: You save the current OMM configuration on the USB flash drive.


Restore from USB: You restore a previously created backup from the USB flash drive.

"SIP users / devices" Menu Entry

In this menu you can create new SIP user accounts and edit or delete existing ones. To open the menu enter the **User name** and the **Password** in the **Admin login** mask (see also Administrator login / logout on the handset on page 44).

Subscription allowed: Enable this option to allow further DECT handsets to subscribe to the system.

- ✓ subscription mode is enabled
- subscription mode is disabled

New SIP user: You create a new SIP user account. Press the  softkey and configure the account data with the following menu entries:


Display name: The name parameter represents the SIP Display Name field. This parameter is optional but recommended.

Number: Enter the SIP account number or extension for the SIP user.


PIN: Enter the PIN that has to be entered to log in the DECT handset to the SIP-DECT™ Lite system (see User Login / Logout on the Handset starting on page 24).

SIP 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.

SIP password: The password will be used during SIP registration and authentication.

Users: Press the  softkey to open the list of configured SIP user accounts. The login state of each SIP user account is displayed by a symbol:

- ✓ logged in
- logged out

Select a list entry and press the  softkey.

Edit: You can edit the current data of the selected SIP user account.

Delete: The SIP user account is deleted after an enquiry.

“Versions” Menu Entry

This menu entry displays information on the OpenMobility Manager software version.

“Factory reset” Menu Entry

This menu entry is only displayed after the RFP SL35 IP has been powered on. You can reset the SIP-DECT™ Lite solution to the factory default configuration (see also the chapter entitled Restoring Factory Defaults starting on page 31). Press the **OK** softkey. An enquiry is displayed. Confirm the enquiry by pressing the **OK** softkey again.

OMM Web Service Reference

This chapter describes all features and functions of the OMM web service.

General Usage

The browser used for the OMM web service access has to be at least Microsoft Internet Explorer 6.0 or Mozilla Firefox 1.5 and must have frame support, JavaScript and cookies enabled.

Login / logout

A user must authenticate with a user name and a password. Both strings are checked case sensitive.

After initial installation or after discarding all settings, the OMM web service is accessible via a default built-in user account with user "Omm" and password "Omm" (see also OMM User Account Types starting on page 37).

To logout click on the **Logout** command in the upper toolbar of the OMM web service.

Selecting the administration mode

The OMM web service provides two different administration modes:

- Use the **Basic settings** mode to configure the basic features and function of your SIP-DECT™ Lite system. Most of these basic settings can also be configured via the Aastra 600d handsets.
- In the **Advanced settings** mode an expert users is able to configure advanced network and SIP settings, e.g. to adopt the SIP-DECT™ Lite to the existing LAN.

Switching the language

The OMM web service provides multiple languages. To switch the language, click on the appropriate flag symbol in the upper toolbar.

"Status" Menu

The **Status** web page provides information on the SIP-DECT™ Lite system status. In case of system errors, system warning messages are also displayed on this page.

- The **General** section displays information on the OpenMobility Manager: software version, uptime duration, PARK (Portable Access Rights Key) and the preset regulatory domain for operation of the SIP-DECT™ Lite system. Also the activation status of the **OM Integrated Messaging & Alerting service** is displayed (see also “System settings” Menu starting on page 50).
- The **Radio fixed part** section displays the RFP activation state.
- The **SIP users / devices** section displays information on the number of configured SIP user accounts and devices. The **Subscription allowed** field indicates if currently further portable parts can be subscribed (see also “SIP users / devices” Menu starting on page 61). Additionally, status information on the “Download over Air” feature is displayed (see also Download Over Air starting on page 34).

“System” Menu

The **System** menu comprises general parameters to configure and administrate the system parameters of the SIP-DECT™ Lite system.

“System settings” Menu

The system settings cover global settings for the OpenMobility Manager. The following tasks can be performed:

- configuring the global settings (see the following description),
- updating the OMM (see Updating the Software starting on page 30),
- restarting the OMM (see Using Directories starting on page 39).

General settings

- **System name:** Enter the system name. The system name is displayed on the OMM login web page and on the subscribed portable parts.

The following **General settings** fields are only displayed in **Advanced settings** mode.

- **Remote access:** Switches on/off the SSH access to the OMM. For more information on the SSH access (see also SSH User Shell starting on page 38).
- **URI for configuration files:** The OMM can be configured via a configuration file. Enter the URI from which the OMM can load this file. For more information on con-

figuration files please refer to the chapter entitled Configuration Files starting on page 70.

- **URI for SW update:** If you want to load an OMM software update not via USB flash drive but from a file system, enter the URI where the file is located here (see also Updating the Software starting on page 30).

Net parameters

- **DHCP:** Enable this option if the OMM is operated as DHCP client and gets the IP configuration from a DHCP server in your network (DHCP configuration). If this option is disabled, you can configure a static IP address configuration in the following fields.
- **IP address:** Enter the IP address of the OMM. This entry is mandatory.
- **Netmask:** Enter the netmask that the OMM is informed of. This entry is mandatory.
- **Gateway:** Enter the IP address of the gateway (i.e router) allocated to the OMM. This entry is mandatory.
- **DNS server:** Enter up to three DNS server IP addresses that the OMM is informed of. This entry is optional.
- **DNS search domain:** Enter the domain name of the network where the OMM is operated in order to use DNS name shortcuts. This entry is optional.

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

- **ToS for voice packets:** Determines the type of service byte of the IP packet header for all packets that transport RTP voice streams.
- **ToS for signalling packets:** Determines the type of service byte of the IP packet header for all packets related to VoIP signaling.
- **TTL (Time to live):** Determines the maximum hop count for all IP packets.
- **VLAN active:** Activate this option, to operate the RFP in a statically configured VLAN. With this, subsequent DHCP requests will also be sent using the configured VLAN ID (see Configuring VLAN starting on page 42).
- **VLAN ID:** Determines the ID tag to be used in a statically configured VLAN.
- **VLAN priority call control:** Determines the VLAN priority tag for VoIP signaling packets.
- **VLAN priority audio:** Determines the VLAN priority tag for RTP packets.

DECT settings

The **DECT settings** section is only displayed in **Advanced settings** mode.

- **Tone scheme:** Select the country in which the OMM resides. This enables country specific tones on the operated handsets (busy tone, dial tone, ...).
- **Encryption:** Activate this option if you want to enable DECT encryption for the SIP-DECT™ Lite system.

Please note: If you enable encryption, make sure that all deployed 3rd party handsets support DECT encryption.

- **DECT authentication code:** The authentication code is used during initial PP subscription as a security option. A code entered here provides a system-wide DECT authentication code for each PP subscription.
- **Portable part user login type:** One handset can be shared by different users at different points in time ("free seating"). Two kinds of user login types are supported. During the login the handset user can either be determined by the telephone number (**Number**) or by the unique user login ID (**Login ID**). Both elements are part of each user data set. The **Portable part user login type** setting specifies the system-wide login variant.

Note

Changing this setting forces an automatic logout of all logged in DECT handsets.

Voice mail

This setting is only displayed in **Advanced settings** mode. **Voice mail number:** You can configure a system-wide voice mail number. This number is used by the Aastra 600d handsets if the voice box is called. For information on calling the voice box please refer to the "Aastra 610d, 620d, 630d; SIP-DECT User's Guide; Handset Release ≥ 4.0".

OM Integrated Messaging & Alerting service

This setting is only displayed in **Advanced settings** mode. The OMM provides a integrated message and alarm service, which could be activated/deactivated and configured here. For a detailed description please refer to the user guide entitled "SIP-DECT; OM Integrated Messaging & Alerting Application" (see also page 113).

Syslog

This setting is only displayed in **Advanced settings** mode. The OMM is capable of propagating syslog messages. Enable the **Active** checkbox if you want to use this feature. Enter the **IP address** and the **Port** of the host which should collect these messages. Click the **Default** button to set a default value for the host port.

For a quick overview on system messages you can also use the **Event log** menu of the OMM web service to gain information (see page 60).

Date and time

If an SNTP is configured, the date and time of the configured time zone can be synchronized with the Aastra 600d handsets. The date and time will be provided by the OMM to these handsets if they initiate a DECT location registration.

- **NTP server:** This setting belongs to the static IP address configuration of the OMM. Enter up to three NTP server IP addresses or NTP server names that the OMM is informed of. This entry is optional.
- Select the desired zone in the **Time Zone** field. The rules for the displayed time zones can be configured on the **Time zones** web page (see page 57).

“SIP” Menu

The SIP settings cover all global settings matching the SIP signalling and the RTP voice streams.

Basic settings

- **Proxy server:** Enter the IP address or the name of the SIP proxy server. If a host name and domain are used for the proxy server parameter, ensure that a DNS server and a domain are specified for your SIP-DECT™ Lite system (see page 51, **Net parameters** section on the **System settings** web page).
- **Proxy port:** Enter the SIP proxy server's port number. Default is “5060”. To enable DNS SRV support for proxy lookups, use a value of “0” for the proxy port.
- **Registrar server:** Enter the IP address or name of the SIP registrar. This enables the portable parts to be registered with a registrar. If a host name and domain are used for the proxy server parameter, ensure that a DNS server and a domain are specified for your your SIP-DECT™ Lite system (see page 51, **Net parameters** section on the **System settings** web page).
- **Registrar port:** Enter the SIP registrar's port number. Default is “5060”. To enable DNS SRV support for registrar lookups, use a value of “0” for the registrar port.

- **Registration period:** This setting is only displayed in **Advanced settings** mode. Enter the requested registration period from the registrar. Default is “3600” seconds.

Advanced settings

The **Advanced settings** section is only displayed in **Advanced settings** mode.

- **Outbound proxy server:** This setting is optional. You can enter the address of the outbound proxy server in this field. All SIP messages originating from the OMM are sent to this server. For example, if you have a Session Border Controller in your network, then you would normally set its address here.
- **Outbound proxy port:** The proxy port on the proxy server to which the OMM sends all SIP messages. Default is “5060”.
- **Explicit MWI subscription:** Some Media Servers such as the Asterisk support Message Waiting Indication (MWI) based on RFC 3842 (see also page 114). An MWI icon will be presented on an Aastra 600d handset if the user has received a voice message on his voice box which is supported by the Media Server. If **Explicit MWI subscription** is enabled, the OMM sends explicit for each portable part an MWI subscription message to the Proxy or Outbound Proxy Server.
- **User agent info:** If this option is enabled, the OMM sends information on his version inside the SIP headers “User-Agent/Server”.
- **Dial terminator:** A dial terminator is necessary if digit treatment shall be applied on outgoing calls. The dial terminator is configurable (up to 2 characters; “0” - “9”, “*”, “#” or empty). The default dial terminator is “#”.
- **Registration failed retry timer:** Specifies the time that the OMM waits between registration attempts when the registration is rejected by the registrar. Default is “1200” seconds.
- **Registration timeout retry timer:** Specifies the time that the OMM waits between registration attempts when the registration timed out. Default is “180” seconds.
- **Transaction timer:** The time period that the OMM allows a call server (proxy/registrar) to respond to SIP messages that it sends. If the OMM does not receive a response in the time period designated for this parameter, the OMM assumes the message as timed out. In this case the call server is recorded to the blacklist. Valid values are “4000” to “64000” milliseconds. Default is “4000” milliseconds.
- **Blacklist time out:** Specified the time period that an unreachable call server stays in the blacklist. Valid values are “0” to “1440” minutes. Default is “5” minutes.

- **Determine remote party by ... header:** You can select the SIP header from which the remote party information (user id and display name) should be determined. If **P-Asserted-Identity** (default value) is selected but no such header is received, a fallback to the mandatory **From / To** header will be done. You can configure this feature by choosing one of the two values.
- **Multiple 180 Ringing:** If this feature is deactivated, the OMM sends out only one 180 Ringing response for an incoming call if PRACK is not supported. If this feature is activated, the OMM retransmits multiple times the 180 Ringing response for an incoming call if PRACK is not supported. This ensures that the calling side receives a 180 Ringing response in case of packet losses on the network. By default this feature is active.

RTP settings

The **RTP settings** section is only displayed in **Advanced settings** mode.

- **RTP port base:** Each RFP needs a continuous port area of 68 UDP ports for RTP voice streaming. The RTP port base is the start port number of that area. Default is "16320".
- **Preferred codec 1 – 4:** Specifies a customized codec preference list which allows you to use the preferred codecs. The Codec 1 has the highest and Codec 4 the lowest priority.
- **Preferred packet time:** This setting determines the length of voice samples collected before sending out a new RTP packet. A small setting improves voice quality at the expense of data transmission overhead. Valid values are "10", "20" or "30" milliseconds. Default is "20" milliseconds.
- **Silence suppression:** This option enables automatic silence detection in the RTP voice data stream to optimize the data transfer volume.
- **Receiver precedence on CODEC negotiation:** If this option is enabled, it means: The CODEC selection for incoming SDP offers based on the own preference order list. The first entry in the OMM preferred codec list matching an entry in the incoming SDP offer will be selected. If this option is disabled (default setting), it means: The CODEC selection based on the preference order list of incoming SDP offer. The first entry in the incoming order list matching an entry of OMM preferred codec list will be selected. This is the default and is as recommended in RFC 3264.
- **Eliminate comfort noise packets:** If this feature is activated, then comfort noise packets are removed from the RTP media stream which causes gaps in the sequence numbers. This can be used if comfort noise packets e.g. in G.711 media streams disturb voice calls in certain installations.

DTMF settings

The **DTMF settings** section is only displayed in **Advanced settings** mode.

- **Out-of-band:** With this option you configure whether DTMF Out-of-band is preferred or not.
- **Method:** The OMM supports the following DTMF Out-of-band methods:
 - **RTP (RFC 2833):** Transmits DTMF as RTP events according to RFC 2833 after the payload type negotiation via SIP/SDP. If the payload type is not negotiated, “in band” will be used automatically.
 - **Info:** The SIP INFO method is used to transmit DTMF tones as telephone events (application/DTMF-relay). This setting should be used if RFC 2833 is not supported.
 - **Both:** DTMF telephones events are send according to RFC 2833 and as well as SIP INFO method. **Note:** Possibly, the other party recognizes events twice.
- **Payload type:** If the **Out-of-band** option is enabled, this setting specifies the payload type which is used for sending DTMF events according to RFC 2833.

Supplementary Services

The **Supplementary Services** section is only displayed in **Advanced settings** mode.

- **Call forwarding / Diversion:** The handset user can (de)activate call forwarding/diversion in the OMM via menu. In some installations the implemented call forwarding/diversion feature in the PBX system is in conflict with the OMM based call forwarding/diversion. Thus, the OMM based call forwarding/diversion can be deactivated to let the menu on the handset disappear. This setting becomes active on handsets with the next DECT “Locating Registration” process (can be forced by switching the handset off and on again). An already activated call forwarding is ignored if the call forwarding feature is deactivated.
- **Local line handling:** A deactivation of the “Local line handling” flag results in the following implications:
 - Only one line is handled for each handset user, except for an “SOS call”. The initiation of a SOS call in call active state results in the creation of a new line which handles the SOS call.
 - If a handset user presses the “R” key or hook-off key in a call active state, a DTMF event is send to the PBX via SIP INFO including signal 16 (hook-flash). All Hook-flash events are send in every case via SIP INFO independently from the configured or negotiated DTMF method during call setup. All other key events are send via configured or negotiated DTMF method.

– This setting becomes active on handsets with the next DECT “Locating Registration” process (can be forced by switching the handset off and on again).

“User administration” Menu

In the **User administration** menu you configure the user accounts which allow to manage the SIP-DECT™ Lite system. For information on the different user account types please refer to the chapter entitled OMM User Account Types starting on page 37.

- **Account type:** Select the account type you wish to change.
- **Active:** This setting applies to the **Read-only** account. Using this account, a user is not allowed to configure any item of the SIP-DECT™ Lite system. The account can be deactivated.
- **User name:** If desired, enter a new user name.
- **Password, Password confirmation:** Enter the appropriate data in these fields.
- **Password aging:** A timeout for the password can be set. Select the duration, the password should be valid.

“Time zones” Menu

The **Time zones** menu is only displayed in **Advanced settings** mode.


The **Time zones** web page provides all available time zones. They are set with their known daylight savings time rules adjusted to the Universal Coordinated Time (UTC) per default. The difference to the UTC time is shown in the **UTC difference** column. In case of a configured daylight savings time rule (**DST** column) this is also marked for each time zone.

The date and time will be provided by the OMM to the Aastra 600d handsets if the handset initiates a DECT location registration. This will be done in the following cases:

- subscribing to the OMM,
- entering the network again after the DECT signal was lost,
- power on,
- silent charging feature is active at the phone and the phone is taken out of the charger,
- after a specific time to update date and time.

Changing Time Zones

You can change the time zone rules for up to five time zones. Changed rules are marked with a bold time zone name in the table. The changes are saved in the OMM configuration file and are restored after each OMM startup.

1. To change the settings of a time zone, click on the  icon on the left of the time zone entry.

The **Configure time zone** dialog opens.

2. You can change the standard time and the daylight savings time (DST) of a time zone. If the time zone has no DST, only the UTC difference can be configured. For the DST both points of time (begin of standard time and begin of daylight savings time) have to be specified exactly. Therefore a certain day in the month or a certain week day in a month can be used.

Resetting Time Zones

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

“SNMP” Menu

The **SNMP** menu is only displayed in **Advanced settings** mode.

The SIP-DECT™ Lite system is provided with an SNMP agent. This will give alarm information and allow an SNMP management system (such as “HP Open View”) to manage the network. On the **SNMP** web page you configure the SNMP service settings.

General settings

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

Trap handling

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

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

For further information on using SNMP with the SIP-DECT™ Lite system please refer to the chapter entitled SNMP Configuration starting on page 41.

“DB management” Menu

The database management (DB management) allows a flexible backup and restore management of the OMM database (see also Backing up and Restoring the SIP-DECT™ Lite Configuration starting on page 33).

Note

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

Backup

Using the **Save to USB** and **Restore from USB** buttons you can backup and restore the OMM database from the delivered USB flash drive. The buttons are disabled when no USB flash drive is plugged in.

Please note: Restoring a database from the USB flash drive leads to a reset of the OMM to take effect.

Manual import

The **Manual import** section is only displayed in **Advanced settings** mode.

- **Protocol:** To import a database from the web browser’s file system select the **FILE** protocol and press the **Browse** button behind the **File** field to select the file from the file system. To import a database from an external server select the preferred protocol (e.g. HTTP) and specify the entries in the following fields.
- **Server:** Enter the IP address or the name of the external server.
- **User name, Password:** If necessary, enter the account data of the server.
- **File:** Enter the path and file name which include the OMM database.

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

Manual export

The **Manual export** section is only displayed in **Advanced settings** mode.

- **Protocol:** Select the preferred protocol. If you want to export the database to the web browser's file system, select the **FILE** setting.
- **Server:** Enter the IP address or the name of the server.
- **User name, Password:** If necessary, enter the account data of the server.
- **File:** Enter the path and filename where the database is to be saved and press the **Save** button.

User data import

The **User data import** section is only displayed in **Advanced settings** mode. With this feature you can import the data of one or multiple SIP users from an external server instead of creating them via the **SIP users / devices** menu (see page 61) or via the handsets (see page 43).

- **Active:** Activate this checkbox to enable the **User data import** feature.
- **Protocol:** Select the preferred protocol.
- **Server:** Enter the IP address or the name of the server.
- **User name, Password:** If necessary, enter the account data of the server.
- **Path:** Enter the path where the user data files are stored and press the **OK** button.

“Event log” Menu

The **Event log** page displays important event information on OMM system functions, e.g. security aspects. A more detailed system log can be obtained by configuring the **Syslog** function in the **System settings** menu, see page 53.






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

“SIP users / devices” Menu

The **SIP users / devices** web page provides an overview of all configured SIP user accounts and devices (handsets) sorted by their number. The table provides configuration and status information in several columns:

- **Display name:** Indicates the SIP Display name.
- **Number:** Indicates the internal call number of the handset.
- **IPEI:** Indicates the handset IPEI.
- **Subscribed:** Indicates if the handset is subscribed to the system.
- **Download:** This column is only presented if the “Download over Air” feature is started successfully and gives information about the download status of the handset software (see Download Over Air starting on page 34).

The configuration and status information are also indicated by the following icons:

Icon	Meaning
	Indicates a SIP user account with the “logged out” status.
	Indicates a SIP user account with the “logged in” status.
	Indicates a subscribed handset which is currently not used, i.e. no SIP user is logged in on that device.
	Indicates an entry which has been created by user data import or an entry of a handset which is currently not used. Such entries can not be edited in the OMM web service.
	Indicates that the entry can be edited.


Subscription

In the **Subscription** section of the **SIP users / devices** web page you can activate / deactivate the subscription mode:

- Press the **Start** button to activate the subscription mode.
- Press the **Stop** button to deactivate it.

For more information on subscribing handset please refer to the chapter entitled Subscribing DECT Handsets starting on page 26.

Creating and Changing SIP User Accounts

1. To configure a new SIP user account press the **New** button on the **SIP users / devices** web page. To change the configuration of an existing SIP user account click on the  icon on the left of the entry.

The **New SIP user** resp. the **Configure SIP user** dialog opens.

2. Configure the SIP user account parameters (see parameter description below) and press the **OK** button.

The following parameters can be set per SIP user account:


General settings

- **Display name:** The name parameter represents the SIP Display Name field. This parameter is optional but recommended.
- **Number:** Enter the SIP account number or extension for the SIP user.
- **PIN:** Enter the PIN that has to be entered to log in the DECT handset to the SIP-DECT™ Lite system (see User Login / Logout on the Handset starting on page 24).
- **Login/Additional ID:** If you have configured the **Portable part user login type** setting to **Login ID** (see page 52), you need to provide the LoginID for the SIP user account.
- **SOS number, ManDown number:** SOS and ManDown are calling numbers which will be automatically called as soon as an SOS or ManDown event happens.
- **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 handset. If there is no individual voice mail number configured in this field, then the system-wide voice mail number is used (see also page 52). 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.

SIP authentication

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

Deleting SIP User Accounts

1. To delete an existing SIP user account click on the  icon on the left of the entry on the **SIP users / devices** web page.

The **Delete SIP user** dialog opens showing the current configuration of this SIP user account.

2. Press the **Delete** button.

“System features” Menu


The **System features** menu is only displayed in **Advanced settings** mode. This menu allows administration of system features concerning call number handling, directory access, and the configuration of XML applications.

“Digit treatment” Menu

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

For overview information on using “digit treatment” with the SIP-DECT™ Lite system please refer to the chapter entitled Using Directories starting on page 39.

Creating and Changing “Digit treatment” Entries

1. To configure a new “digit treatment” entry press the **New** button on the **Digit treatment** web page. To change the configuration of an existing entry click on the  icon on the left of the entry.

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


2. Enter the entry parameters (see parameter description below) and press the **OK** button.

The following parameters can be set per “digit treatment” entry:

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

- **Internal pattern:** Enter an internal prefix pattern with up to 32 characters that replaces the external pattern for the directory entry / incoming calls or vice versa for outgoing calls. An internal prefix pattern can be composed of: characters “*, # and 0 - 9”.
- **Direction:** Select the rule which should be applied to this entry:
 - **Incoming calls:** The rule applies on incoming calls.
 - **Outgoing calls:** The rule applies on outgoing calls.
 - **Incoming and outgoing calls:** The rule applies on incoming and outgoing calls.
 - **Apply on directory only:** The rule applies to directories only (see also “Directory” Menu starting on page 64).
- **Directory:** This option can be used to specify the rule for incoming and/or outgoing calls. Activate this option if the rule applies to directories.

Deleting “Digit treatment” Entries

1. To delete an existing “digit treatment” entry click on the  icon on the left of the entry on the **Digit treatment** web page.

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


2. Press the **Delete** button.

“Directory” Menu

The **Directory** menu allows you to manage connections to up to 5 LDAP or XML servers (directory entries) that in turn facilitate central corporate directories.

For overview information on using directory servers with the SIP-DECT™ Lite system please refer to the chapter entitled Using Directories starting on page 39.

Creating and Changing Directory Entries

1. To configure a new directory entry press the **New** button on the **Directory** web page. To change the configuration of an existing entry click on the  icon on the left of the entry.

The **New directory entry** resp. the **Configure directory entry** dialog opens.

2. Enter the parameters for the server access (see parameter description below) and press the **OK** button.

The following parameters can be set per directory entry:

- **Active:** With this option you enable / disable the entry.
- **Order:** This setting determines the position in the handset menu (1 - top; 5 - bottom).
- **Type:** Select the protocol that is supported by the directory server (**LDAP** or **XML**).
- **Name:** Enter a name for the directory entry. Latin-1 character set is supported.

Note: The name configured here is not relevant and ignored when the handset user searches for a call number in the telephone's central directory if there is only one directory entry configured.

- **Protocol:** This setting applies only to XML directory entries. Select the preferred transfer protocol.
- **Server name** (mandatory): Enter the name or IP address of the directory server.
- **Server port** (mandatory): Enter the server port number. Default is "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, Password confirmation:** User name (a distinguished name) and password may be filled if requested by the directory server. Otherwise an anonymous bind takes place.

Note: The SIP-DECT™ Lite system 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), given name (default)
- Given name and surname (sn)

- **Server search timeout:** The search results will be accepted within the entered search time (value range: 1 - 99 seconds).

- **Path and parameters:** This setting applies only to XML directory entries. Enter the URL (if required with parameters) where the XML directory is located on the directory server.


The configuration is valid for all handsets which support the LDAP or XML directory feature. To make search requests unique for different users the search base configuration can include place holders which are replaced by user specific values when submitting the request to a server. The following place holders 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 the SIP-DECT™ Lite system is not limited to numeric characters.

Deleting Directory Entries

1. To delete an existing directory entry click on the  icon on the left of the entry on the **Directory** web page.

The **Delete directory entry** dialog opens showing the current configuration of this entry.

2. Press the **Delete** button.

“Feature access codes” Menu

Feature access codes (FAC) allow to perform specific actions, e.g. user login or user logout to the SIP-DECT™ Lite system, from any subscribed DECT handset.

To configure the FAC feature:

1. **FAC number:** Enter a unique FAC number in the **General settings** section.
2. In the **FAC action** section activate the appropriate checkbox(es) to enable the corresponding FAC feature(s). For each enabled FAC feature enter an assigned access code and press the **OK** button.

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

Example: If you adopt the preset **FAC number** = “*##” and **User login** FAC = “1”, the user can log in to the SIP-DECT™ Lite system by dialling “*##1[phone number / user ID]” en-bloc instead of navigating through the handset’s **Administration** menu (see also the chapter entitled User Login / Logout on the Handset starting on page 24).

“XML applications” Menu

The SIP-DECT™ Lite XML terminal interface allows external applications to provide content for the user on the DECT handsets Aastra 600d 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 6 predefined hooks and 10 hooks which can be freely defined. The predefined hooks can be edited (with exception of the “admin” hook) but not deleted. The following XML application hooks for DECT handsets are predefined:

XML hook	Description
callerList	Displayed with Info: Caller List menu entry
redialList	Displayed with Info: Redial List menu entry
userPresence	Displayed as additional Presence menu entry
systemAppMenu	Displayed as additional System: Server menu entry
eventActions	XML application triggered by SIP Notify events
admin	Displayed with System menu menu entry (no customization)


Please note: “callerList” and “redialList” replace the local caller and redial lists of the Aastra 600d 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 set to **Local**, the local lists are used by the handset.

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

Note

For information on configuring XML applications via configuration files please refer to the chapter entitled XML Application starting on page 104.

Creating and Changing “XML application” Hooks

1. To configure a new “XML application” hook press the **New** button on the **XML application** web page. To change the configuration of an existing entry click on the  icon on the left of the entry.

The **New XML application** resp. the **Configure XML application** dialog opens.

2. Enter the entry parameters (see parameter description below) and press the **OK** button.

The following parameters can be set per XML application hook:

- **Name:** Enter a name for the XML application hook.


The following parameters specify the XML application URI:

- **Protocol:** Select the preferred transfer protocol.
- **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.
- **File:** Enter the path and query of the URI.

Note

The predefined “admin” hook can not be edited. It represents the **System menu > Administration** menu entry on the handset.

Deleting “XML application” Hooks

1. To delete an existing “XML application” hook click on the  icon on the left of the entry on the **XML application** web page.
The **Delete XML application entry?** dialog opens showing the current configuration of this entry.
2. Press the **Delete** button.

Note

The predefined hooks can not be deleted.

“Info” Menu

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

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

Configuration Files

As mentioned in other parts of this document, the SIP-DECT™ Lite solution configuration can be changed with configuration files. Configuration files are basically text files that contain configuration items on a line-by-line basis. By using configuration files, the following is possible:

- The SIP-DECT™ Lite configuration can be automated. For example by generating configuration files based on user data stored in an external provisioning system.
- Some SIP-DECT™ Lite features cannot be configured using a static user interface (OMM web service or DECT handset menu item). For example, you can define an alarm scenario for messaging or an interactive XML application for DECT handsets.

Using configuration files primarily targets SIP providers that want to deploy the auto configured SIP-DECT™ Lite solution to their customers. Also, if you have advanced configuration requirements, using configuration files offers the necessary flexibility, e.g. to integrate SIP-DECT™ Lite into the information technology already running on site.

This chapter provides a summarized overview on how to implement configuration files. However, you should keep in mind that SIP-DECT™ Lite is a single-cell solution that is part of the SIP-DECT® product family that offers larger radio coverage by supporting multi-cell DECT networks with up to 2.048 RFPs. For this reason, only the applicable sub-set of configuration items can be applied to SIP-DECT™ Lite.

Hosting Configuration Files

Operating with configuration files basically includes the following steps:

1. You create a new static configuration file using a text editor. You store the configuration file on a server for downloading. Alternatively, you set up a server-side program that dynamically generates the configuration file.
2. You activate the SIP-DECT™ Lite configuration file feature. For this, you need to configure a URI for downloading the configuration file. Supported download protocols include HTTP(S), FTP(S), SFTP and TFTP.
3. During startup or (periodically) during runtime, the OMM downloads the configuration file. The contents of the configuration file is interpreted which in turn triggers configuration changes or functions.

As a prerequisite, you need to operate the server for downloading or generating configuration files, either within your company LAN or on the Internet. This server is not included with the SIP-DECT™ Lite solution.

The following table gives an overview of configuration file features and their respective URI configuration settings.

Feature	Configuration (OMM web service and alternatives)
<i>System Configuration</i>	System: System setting: URI for configuration files, DHCP options, or Astra Redirection and Configuration Service
<i>User Data</i>	System: DB management: User data import or <code><SetUserDataServer /></code> in <i>System Configuration</i>
<i>Messaging</i>	System: System setting: OM Integrated Messaging... or <code><SetIMA /></code> in <i>System Configuration</i>
<i>XML Application</i>	System features: XML applications or <code><SetXMLApplication /></code> in <i>System Configuration</i> (not a configuration file, but described here due to similarities)

Notes

A configuration file is interpreted line-by-line. You can include comments that are ignored after a hash character. Empty lines or lines starting with a hash sign are ignored. The file should be encoded as UTF-8. Both Windows and Unix line end encodings are accepted.

A server for dynamically generating configuration files is most likely a web server. You implement programs or scripts that run in the context of the web server in order to generate configuration files. Most web server products offer a Common Gateway Interface (CGI) for this. Refer to your web server documentation for details.

When transferring configuration files via Internet, you should use a secured protocol such as HTTPS. It is also possible to add a username / password combination to HTTP and FTP download URLs for additional security.

System Configuration

The system configuration file changes the configuration of the SIP-DECT™ Lite system. If activated, the RFP SL35 IP downloads a file named “ipdect.cfg” from the download server. The system configuration file contains various system settings written in an assignment notation. Example: `OM_SwImageUrl=ftp://server/iprfp3G.dnld`

For SIP-DECT™ Lite, it is also possible to add XML statements to the system configuration file. By adding XML statements, you can change the configuration of the SIP-DECT™ Lite solution. Example: `<SetEULAConfirm confirm="1"/>`

Note

If the “ipdect.cfg” file sets a parameter `OM_PersonalConfigAll=1`, an additional RFP specific configuration file will be read in. The file name of this configuration file is determined by the MAC address of the RFP, for example: “0030420A1B2C.cfg”. Basically both configuration files support the same configuration options. If you manage multiple SIP-DECT™ Lite RFPs on a central site, you may want to split the delivered configuration options as needed.

Activating System Configuration Files

You can activate the SIP-DECT™ Lite system configuration file download with one of the following mechanisms. Note that the mechanism with the highest priority is listed first.

Manual configuration

You can manually configure a URI for downloading the system configuration file. Log in to the OMM web service. Enable the **Advanced settings** option. Navigate to the **System: System settings** page. Enter the desired URI in the **URI for configuration files** input field.

Alternatively, you can change the configuration download URI on the DECT handset. Navigate to the **System menu > Administration > System** page. Enter the user name and password for the full access user account. Select the respective configuration option. Enter the desired URI.

The URI needs to follow a specific syntax to specify protocol and options.

Example URI	Description
ftp://192.168.1.1/	Addresses a local FTP server (root directory).
ftps://domain.com/sip-dect/	Addresses a subdirectory of an FTPS server located on the Internet.
http://user:pass@192.168.1.1/	For FTP(S) and HTTP(S) it is possible to specify login credentials prepending the “at” character. Separate user and password with a colon.
https://domain.com/sub/dir/	For Internet downloads, FTPS or HTTPS are recommended.
tftp://192.168.1.1/tftpboot/	TFTP is also supported (recommended for LAN downloads only).

DHCP options

It is possible to trigger the configuration file mechanism by providing options in the DHCP answer of your DHCP server. For this mechanism, you need a DHCP server in your LAN that allows to specify advanced DHCP options. Typically, you configure a DHCP entry that is bound the MAC address of the SIP-DECT™ Lite RFP for this.

You can trigger the configuration file download with the following DHCP options.

DHCP Option	Description	Prio
Option 43 Suboption 2 “OM_ConfigUrl”	The DHCP option 43 “Vendor Specific Information” may include several suboption fields. Format: 1 byte sub-option, 1 byte length, [length] bytes data	1
Option 233 “OM_ConfigUrl”	This site specific DHCP option with code 233 can also be used to configure a download URI.	2
Option 66 “TFTP Server”	This DHCP option can be used if you provide configuration files in the root directory of a TFTP server.	3

Note

The DHCP triggered configuration file mechanism does not work if a static IP address configuration is active.

“Aastra Redirection and Configuration Service (RCS)”

Upon startup and if no download URI is configured, the OMM queries the Aastra Redirection and Configuration Service (RCS). This service is located on the Aastra’s global RCS server. If the OMM successfully contacts the RCS server, the download URI will be stored in the configuration. Thus, the acquired download URI is will be used until the factory default settings are applied.

The Aastra Redirection and Configuration Service can be used to trigger downloading configuration files that you can provide on your own servers via Internet. Please contact Aastra sales for details.

Note

The RCS mechanism can be disabled locally with a specific option in the DHCP answer, specifically the boolean sub-option 3 (“ContactRCS”) encapsulated with DHCP option 43 (“Vendor Specific Information”).

Example System Configuration Files

The following example depicts the possible contents of system configuration files (“ipdect.cfg” and <MAC>.cfg). The example contains XML statements to configure SIP settings, SIP user accounts, messaging, and XML applications as well.

ipdect.cfg

```
#####
# sample configuration file (ipdect.cfg, <MAC>.cfg) for the SIP-DECT Lite system
# retrieved via the net using file transfer protocols like tftp,ftp, http,
# ftps or https
# Insert the URL to the folder containing this file into DHCP option 66
# (TFTP Server) or use the URI for configuration files in the Web Service
#
# Insert a URL e.g. ftp://server/path/ (http, https, tftp, ftp, ftps)
#####
# comments are starting with the hash sign: "#"
#
#####
# 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=300
#####
# 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
# If this parameter is set to yes(y,1) there have to be a valid mac.cfg!
# until the MAC is excluded with OM_PersonalConfig_<MAC>=n
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

#####
#
# RFP (L) 35,36,37,43 software update URL (http, https, tftp, ftp, ftps)
#
#OM_SwImageUrl=ftp://server/iprpf3G_Addons.dnld
#####
# SYSLOG
#
OM_SyslogIpAddress=10.103.35.20
OM_SyslogPort=10104

#####
# NTP
#
OM_NtpServerName=de.pool.ntp.org
OM_NtpServerIpAddress=131.188.3.220 130.149.17.21

##### OMM Data Configuration section #####
##### Basic Configuration #####
### Confirm EULA
<SetEULAConfirm confirm="1" />

### Set full access account
<SetAccount plainText="1" > <account id="1" password="Sip!12" active="1" aging="none" /> </
SetAccount>

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

### Set system name
<SetSystemName name="SIP-DECT L" />

### Set basic SIP Settings proxy and registrat IP address and port
<SetBasicSIP proxyServer="172.30.206.9" proxyPort="5060" regServer="172.30.206.9" regPort="5060" />

##### Create User
<CreatePPUser plainText="1" replaceData="1"><user relType="Unbound" name="Lutz" num="4366"
sipAuthId="4366" sipPw="4366" pin="4366" /></CreatePPUser>
<CreatePPUser plainText="1" replaceData="1"><user relType="Unbound" name="Peter" num="4361"
sipAuthId="4361" sipPw="4361" pin="4361" /></CreatePPUser>
<CreatePPUser plainText="1" replaceData="1"><user relType="Unbound" name="Jens" num="4362"
sipAuthId="4362" sipPw="4362" pin="4362" /></CreatePPUser>

##### Advanced Configuration #####
# General settings

### Set read only account
<SetAccount plainText="1" > <account id="0" username="user" password="Sip!12" active="1"
aging="none" /> </SetAccount>

```

Configuration Files

```
### Active Remote Access
<SetRemoteAccess enable="1" />

### URI for configuration files - Not applicable as this is the configuration file
### URI for SW update - Please use OM_SwImageUrl in the section above

## Net parameters

### ToS for voice packets, ToS for signalling packets, TTL (Time to live, VLAN priority call control, VLAN priority audio
<SetNetParams ><net voiceToS="184" sigToS="184" ttl="32" voiceEthPrio="6" sigEthPrio="6" /></SetNetParams>

## DECT settings

### Tone scheme
<SetSysToneScheme toneScheme="US" />

### Encryption
<SetDECTEncryption enable="1" />

### DECT authentication code
<SetDECTAuthCode ac="12345678" />

### Portable part user login type
<SetPPLoginVariant login="NUMBER" />

## Downloading new firmware to portable parts
### Active
<SetPPFirmwareUpdate enable="1" />

## Voice mail
### Voice mail number
<SetSysVoiceboxNum voiceboxNum="6333" />

## OM Integrated Messaging & Alerting service
### Active, URL
<SetIMA enable="1" url="tftp://10.103.35.20/open_mob/lp_int/ima.cfg" />

## Syslog
### Active, IP address, Port - please use OM_SyslogIpAddress in the section above
<SetSyslogServer enable="1" ipAddr="10.103.35.20" port="10104" />

## Date and time
### NTP server - please use OM_NtpServerName or OM_NtpServerIpAddress in the section above
### Time zone
<SetTimeZone id="EIS" />

# SIP
## Basic settings Registration period
<SetBasicSIP regPeriod="3600" />

## Advanced settings

### Outbound proxy server, Outbound proxy port, Explicit MWI subscription,
### User agent info, Dial terminator,Registration failed retry timer ,
### Registration timeout retry timer, Transaction timer, Blacklist time out
### Determine remote party by header, Multiple 180 Ringing
<SetAdvancedSIP mwiSubscription="0" userAgentInfo="0" dialTerminator="#"
regTimeoutRetryTimer="180" regFailedRetryTimer="180" transactionTimer="4000" blacklistTimeout="5"
callerDetermination="P-Assert-Identity" multipleRing="1" />

#<SetAdvancedSIP outboundProxyServer="172.30.206.9" outboundProxyPort="5060"
mwiSubscription="0" userAgentInfo="0" dialTerminator="#" regTimeoutRetryTimer="180"
regFailedRetryTimer="180" transactionTimer="4000" blacklistTimeout="5" callerDetermination="From/To"
multipleRing="1" />

## RTP settings
### RTP port base,Preferred codec 1, Preferred codec 2, Preferred codec 3,
```

```

### Preferred codec 4, Preferred packet time, Silence suppression, Receiver
### precedence on CODEC negotiation, Eliminate comfort noise packets
<SetRTP portBase="16320" packetTime="30" silenceSupp="0" receiverPrecedence="0"
comfortNoisePktElim="0" ><codec type="G.722" /><codec type="G.711-A-law" /><codec type="G.711-u-
law" /><codec type="None" /></SetRTP>

## DTMF settings
### Out-of-band, Method, Payload type
<SetDTMF outOfBand="1" payloadType="101" method="RFC2833" />

## Supplementary Services
### Call forwarding / Diversion
### Local line handling
<SetSuplServ callForwDiv="1" locLineHndlg="1" />

#Time zones
<SetTimeZoneDetails ><zone id="EIS" name="Easter Island (EIS UTC-6 DST)" stdOffset="-360"
stdMonth="3" stdDay="0" stdDoW="7" stdWoM="2" stdHour="23" stdMin="0" dstOffset="-60"
dstMonth="10" dstDay="0" dstDoW="7" dstWoM="2" dstHour="0" dstMin="0" /></SetTimeZoneDetails>

#SNMP
## General settings
### Read-only community
### System contact
## Trap handling
### Trap community
### Trap host IP address
<SetSNMP readCommunity="Aastra" contact="Aastra" enableTraps="1" trapCommunity="Aastra"
trapHostAddr="172.17.5.20" />

# User data import
### Active, Protocol, Server, User name, Password,Path
<SetUserDataServer enable="1"><url protocol="TFTP" host="10.103.35.20" path="/open_mob/lp_int" /></
SetUserDataServer>

# Create User
### Display name,Number, PIN, Login/Additional ID, SOS number,
### ManDown number, Voice mail number, User name, Password
<CreatePPUser plainText="1" replaceData="1"><user relType="Unbound" name="Michael" num="4364"
pin="4364" addId="4364" sosNum="112" manDownNum="115" voiceboxNum="2222" sipAuthId="4364"
sipPw="4364" /></CreatePPUser>
<CreatePPUser plainText="1" replaceData="1"><user relType="Unbound" name="Andy" num="4365"
pin="4365" addId="4365" sosNum="112" manDownNum="115" voiceboxNum="2222" sipAuthId="4365"
sipPw="4365" /></CreatePPUser>

#System features
##Digit treatment
<CreateDigitTreatment replaceData="1"><rule externalPattern="+4930" internalPattern="0" directory="1"
direction="Outgoing" /></CreateDigitTreatment>

##Directory
<CreateLDAP plainText="1" replaceData="1"><ldap name="Aastra" active="1" order="1"
server="berdc1.de.aastra.com" port="389" searchBase="DC=de,DC=aastra,DC=com"
username="ocphone@de" password="Qrb254Lma" searchType="SN" displayType="SN,GN" timeout="10" /
></CreateLDAP>

<CreateXMLApplication plainText="1" replaceData="1"><xmlAppl enable="1" name="XML Dir"
type="CorpDir" corpDirOrder="2" ><url protocol="HTTP" host="10.103.38.11" path="ppxml/
index.php?type=directory2&search=menu" username="" password="" /></xmlAppl></
CreateXMLApplication>

##Feature access codes
<SetFACPrefix prefix="*###" />

```

```
<SetFAC seq="0" ><fac feature="DeactivateSubscription" enable="1" fac="4" /></SetFAC>
<SetFAC seq="0" ><fac feature="UserLogin" enable="1" fac="1" /></SetFAC>
<SetFAC seq="0" ><fac feature="ActivateSubscription" enable="1" fac="3" /></SetFAC>
<SetFAC seq="0" ><fac feature="DeactivateSubscription" enable="1" fac="4" /></SetFAC>

##XML applications
### Built-in
### id="0" name="callerList"
### id="1" name="redialList"
### id="3" name="systemApplMenu"
### id="2" name="userPresence"
### id="4" name="eventActions"
<SetXMLApplication plainText="1" replaceData="1"><xmlAppl enable="1" id="2" name="userPresence"
type="BuiltIn" ><url protocol="HTTP" host="10.103.38.11" path="ppxml/
index.php?type=directory2&sub=set" username="" password="" /></xmlAppl></
SetXMLApplication>
<SetXMLApplication plainText="1" replaceData="1"><xmlAppl enable="1" id="3"
name="systemApplMenu" type="BuiltIn" ><url protocol="HTTP" host="10.103.38.11" path="ppxml/
index.php?type=servermenu" username="" password="" /></xmlAppl></SetXMLApplication>

### up to 10 dynamic applications
<CreateXMLApplication plainText="1" replaceData="1"><xmlAppl enable="1" name="Demo Apps"
type="Dynamic" ><url protocol="HTTP" host="10.103.38.11" path="ppxml/appl_demo.php" username=""
password="" /></xmlAppl></CreateXMLApplication>
```

<MAC>.cfg

```
<CreatePPUser plainText="1" replaceData="1"><user relType="Unbound" name="James" num="4367"
pin="4367" addId="4367" sosNum="112" manDownNum="115" voiceboxNum="2222" sipAuthId="4367"
sipPw="4367" /></CreatePPUser>
<CreatePPUser plainText="1" replaceData="1"><user relType="Unbound" name="Tom" num="4368"
pin="4368" addId="4368" sosNum="112" manDownNum="115" voiceboxNum="2222" sipAuthId="4368"
sipPw="4368" /></CreatePPUser>

### up to 10 dynamic applications
<CreateXMLApplication plainText="1" replaceData="1"><xmlAppl enable="1" name="Demo Apps2"
type="Dynamic" ><url protocol="HTTP" host="10.103.38.11" path="ppxml/appl_demo.php" username=""
password="" /></xmlAppl></CreateXMLApplication>
```

Processing System Configuration Files

It is possible to view messages emitted by the OMM while processing the system configuration files for debugging purposes. For this, you need to log in to the SSH console of the SIP-DECT™ Lite RFP:

1. Activate the **System: System settings: Remote access** option.
2. Log in with SSH. Either enter “ssh Omm@rfp” on a Unix command line or you may use the PuTTY SSH program for this purpose. Enter the password (default: “Omm”).
3. Enter “su root” to switch to the root user account. Enter the password (default: “2222”).
4. Enter “cat /tmp/OMM_Config.log” or “cat /tmp/OMM_Config.log.backup” to view log messages written during system configuration file processing.

If both system configuration files are used, the “OMM_Config.log” file contains the logging for “<MAC>.cfg”, while “OMM_Config.log.backup” contains the logging for “ipdetect.cfg”. You can view XML statements that are sent to the OMM as well as OMM responses. For example:

```
## SKIP ## OMM CFG: OM_NtpServerName=de.pool.ntp.org
## SKIP ## OMM CFG: OM_NtpServerIPAddress=131.188.3.220 130.149.17.21
## SEND ## AXI REQ: <GetVersions />
## DONE ## AXI RSP: <GetVersionsResp ...
## SEND ## AXI REQ: <CreateXMLApplication replaceData="1"> <xmlAppl type="CorpDir" ...
## FAIL ## AXI RSP: <CreateXMLApplicationResp seq="28" errCode="ENoMem" bad="id" />
```

XML Statement Reference

This XML statement reference lists all XML statements that are valid in a system configuration file. The reference follows the structure of the user interface presented by the OMM Web service.

Each XML statement represents a configuration request sent from the system configuration file to the OMM during start-up. Each XML statement - even if composed from multiple XML tags - should be written to a single line of the configuration file.

XML statements generally are case sensitive, i.e. you should maintain the upper and lower case notation of the XML tags and field / attribute names. Conforming to XML standards, you can write a single XML tag with embedded slash (e.g. “<XML/>”) or as separated opening / closing tags (e.g. “<XML></XML>”).

Note

Some XML statements are valid as a single XML tag, while others are only valid with a complete set of one or more required sub-tags. For example, <SetXMLApplication> always require at least one enclosed <xmlAppl/> sub-tag. The complete XML statements in this case: <SetXMLApplication><xmlAppl/></SetXMLApplication>.

Basic Configuration

<SetEULAConfirm>

With this request the client can confirm the EULA. The following fields are defined:

Name	Type	Mandatory	Description
confirm	boolean	yes	"1" or "true", to confirm the EULA

<GetVersions>, <Limits>

These requests can be used for debugging purposes. Request answers can be viewed with the OMM's processing log files (see Processing System Configuration Files starting on page 78).

System: System settings

<SetSystemName>

With this request the client can set the system name. The following fields are defined:

Name	Type	Mandatory	Description
name	string	yes	system name

<SetRemoteAccess>

With this request the client can set the configuration of the remote access (i.e. SSH access). The following fields are defined:

Name	Type	Mandatory	Description
enable	boolean	yes	"1" or "true", to enable the remote access

<SetNetParams>

With this request the client can set some properties of the network interface. The following fields are defined:

Name	Type	Mandatory	Description
<net/>	element	no	Network parameters, see <i>NetParamType</i> below

NetParamType: this type contains all data fields of the network parameters. It is used in different requests and responses defined in this chapter. Not all fields are used in all OMM versions and in all Request and Response types.

Name	Type	Mandatory	Description
voiceToS	integer	yes	ToS for voice packets, 0...255
sigToS	integer	yes	ToS for signalling packets, 0...255
ttl	integer	yes	Time To Life
voiceEthPrio	integer	no	802.1p priority for voice packets, 0...7
sigEthPrio	integer	no	802.1p priority for signalling packets, 0...7

The attributes *voiceEthPrio* and *sigEthPrio* are mandatory on OMM versions which support this feature.

<SetSysToneScheme>

With this request the client can set the current tone scheme (dial tone, busy tone, ...). The following fields are defined:

Name	Type	Mandatory	Description
toneScheme	string	yes	Tone scheme country (e.g. "US")

<SetDECTEncryption>

With this request the client can enable or disable DECT encryption. The following fields are defined:

Name	Type	Mandatory	Description
enable	boolean	yes	"1" or "true", to enable encryption

<SetDECTAuthCode>

With this request the client can set the global DECT authentication code. The following fields are defined:

Name	Type	Mandatory	Description
ac	string	yes	DECT authentication code

<SetPPLoginVariant>

With this request the client can set the PP login variant. The following fields are defined:

Name	Type	Mandatory	Description
login	enum	yes	One of "NUMBER" or "ID"

<SetPPFirmwareUpdate>

With this request the client can enable or disable PP firmware updates (also known as "download over air"). The following fields are defined:

Name	Type	Mandatory	Description
enable	boolean	yes	"1" or "true", to enable PP firmware updates

<SetSysVoiceboxNum>

This request is sent from the Client to the OMM. With this request the client can set the system voice box number configuration. The following fields are defined:

Name	Type	Mandatory	Description
voiceboxNum	string	yes	System wide voice box number

<SetIMA>

With this request the client can set the configuration of IMA. The following fields are defined:

Name	Type	Mandatory	Description
enable	boolean	no	"1" or "true", to enable IMA
url	string	no	URL of IMA configuration file

<SetSyslogServer>

This request is sent from the Client to the OMM. With this request the client can set the syslog server configuration. The following fields are defined:

Name	Type	Mandatory	Description
enable	boolean	yes	"1" or "true", syslog server is enabled
ipAddr	string	yes	IP address of syslog server
port	integer	yes	Port number of syslog server

<SetTimeZone>

With this request the client can set the active time zone. The following fields are defined:

Name	Type	Mandatory	Description
id	string	yes	Time zone ID, format like "CET"

System: SIP**<SetBasicSIP>**

With this request the client can set the basic SIP settings. The following fields are defined:

Name	Type	Mandatory	Description
proxyServer	string	no	Proxy Server name or IP address
proxyPort	integer	no	Proxy Server port
regServer	string	no	Registrar Server name or IP address
regPort	integer	no	Registrar Server port
regPeriod	integer	no	Registration period in seconds

All attributes which have to be changed must be filled in by the client.

<SetAdvancedSIP>

With this request the client can set the basic SIP settings. The following fields are defined:

Name	Type	Mandatory	Description
outboundProxyServer	string	no	Proxy Server name or IP address
outboundProxyPort	integer	no	Proxy Server port
mwiSubscription	boolean	no	"1" or "true", for explicit MWI subscription
userAgentInfo	boolean	no	"1" or "true", for sending the <i>UserAgent</i> header field
dialTerminator	string	no	Two character dial string, that separates a dialled number to dialling information and digit treatment processing.
regTimeoutRetryTimer	integer	no	Time to retry registrations in seconds
regFailedRetryTimer	integer	no	Time to retry failed registrations in seconds
transactionTimer	integer	no	Transaction timer in milliseconds
blacklistTimeout	integer	no	Blacklist time out in seconds
callerDetermination	enum	no	One of "P-Assert-Identity" (default) or "From/To"
multipleRing	boolean	no	"1" or "true", for multiple 180 ringing support

All attributes which have to be changed must be filled in by the client.

<SetRTP>

With this request the client can set the basic SIP settings. The following fields are defined:

Name	Type	Mandatory	Description
portBase	integer	no	RTP port base
packetTime	integer	no	RTP packet size in milliseconds
silenceSupp	boolean	no	"1" or "true", for silence suppression
receiverPrecedence	boolean	no	"1" or "true", for receiver precedence on CODEC negotiation
comfortNoisePktElim	boolean	no	"1" or "true", for eliminate comfort noise packets in media streams
<codec/>	element	no	One or more codecs to be used, see below

All attributes which have to be changed must be filled in by the client.

Additionally, this request contains a sequence of elements called <codec>. This is the list of preferred codecs. Each of these elements has following attribute:

Name	Type	Mandatory	Description
type	enum	yes	Type of codec, see <i>CodecType</i> below

If the sequence of codecs is empty, the codec list is not changed. It is only replaced by a new list if the sequence contains at least one entry. The list may have up to 5 entries, spare entries are ignored. The list may also contain entries with value None. These entries can be used as a place holder.

CodecType is an enumeration value defined as follows:

Value	Description
None	No codec
G.711-u-law	G.711 μ -law
G.711-A-law	G.711 A-law
G.729-A	G.729 A
G.722	G.722 Wideband

<SetDTMF>

With this request the client can set the DTMF settings. The following fields are defined:

Name	Type	Mandatory	Description
outOfBand	boolean	no	"1" or "true", for out-of-band DTMF
payloadType	integer	no	DTMF payload type
method	enum	no	DTMF out-of-band method, see <i>DTMFMethodType</i> below

All attributes which have to be changed must be filled in by the client.

DTMFMethodType is an enumeration with one of these values:

Value	Description
RFC2833	DTMF according to RFC 2833
INFO	DTMF in SIP INFO
Both	RFC 2833 and SIP INFO

<SetSuplServ>

With this request the client can set the SIP supplementary service (SuplServ) settings. The following fields are defined:

Name	Type	Mandatory	Description
callForwDiv	boolean	no	"1" or "true", for call forwarding/diversion active
locLineHndlg	boolean	no	"1" or "true", for local line handling active
method	enum	no	Kind of DTMF method for 'R' key events. One of "INFO" (default) or "DTMF"

All attributes which have to be changed must be filled in by the client.

System: User administration

<SetAccount>

The client can send this request to change an account data set. The id has to be filled in by the client to identify the record to be changed. Additionally the attributes which have to be changed must be filled in by the client. The following fields are defined:

Name	Type	Mandatory	Description
plainText	boolean	no	"1" or "true", to use plain text passwords
<account/>	element	yes	Data of account to change, see <i>AccountType</i> below

AccountType: this type contains all data fields of an account. The following fields are defined:

Name	Type	Description
id	integer	Account ID, numbering starts at 0, -1 is invalid
username	string	User name
password	string	Password; if <i>plainText=1</i> attribute in <code><SetAccount></code> not given: encrypted with public key
active	boolean	If true account this is active. Optional set/create parameter. Default value=false.
aging	enum	Selected type of password aging (time out or number of logins). One of "none", "time3Months", "time6Months", "count50Logins", "count100Logins". Optional set/create parameter. Default value=none.

System: Time zones

<SetTimeZoneDetails>

With this request the client can modify the details of a time zone. The following fields are defined:

Name	Type	Mandatory	Description
<code><zone/></code>	element	yes	Modified time zone, see <i>TimeZoneType</i> below

TimeZoneType: this type contains all data of a time zone, including DST (daylight saving time). The following fields are defined:

Name	Type	Description
id	string	Time zone ID, format like "CET"
name	string	Human readable zone name, in English
stdOffset	integer	Offset of standard time to UTC in minutes
stdMonth	integer	Start month of standard time, 0...12, 0 means not used
stdDay	integer	Start day of standard time, 0...31, 0 means not used
stdDoW	integer	Start day of week of standard time, 0...7, 0 means not used
stdWoM	integer	Start week of month of standard time, 0...5, 0 means not used, 1 means first week, 5 means last week
stdHour	integer	Start hour of standard time, 0...23
stdMin	integer	Start minute of standard time, 0...59
dstOffset	integer	Offset of DST to UTC in minutes
dstMonth	integer	Start month of DST, 0...12, 0 means not used
dstDay	integer	Start day of DST, 0...31, 0 means not used
dstDoW	integer	Start day of week of DST, 0...7, 0 means not used
dstWoM	integer	Start week of month of DST, 0...5, 0 means not used, 1 means first week, 5 means last week
dstHour	integer	Start hour of DST, 0...23
dstMin	integer	Start minute of DST, 0...59

System: SNMP

<SetSNMP>

With this request the client can configure the SNMP settings. Only attributes which have to be changed need to be specified. The following fields are defined:

Name	Type	Mandatory	Description
readCommunity	string	no	Read-only community
contact	string	no	System contact
enableTraps	boolean	no	"1" or "true", if trap handling is enabled
trapCommunity	string	no	Trap community
trapHostAddr	string	no	IP address of trap host

System: DB management

<SetUserDataServer>

This request is sent from the Client to the OMM. With this request the client can set the configuration of the User Data Server. The following fields are defined:

Name	Type	Mandatory	Description
enable	boolean	no	"1" or "true", external user data set shall be retrieved from the server
<url/>	element	no	User data configuration settings, see <i>URLType</i> below

UrlType: this type contains all fields of an URL. The following fields are defined:

Name	Type	Mandatory	Description
protocol	enum	yes	Type of the used protocol to the server, see <i>ProtType</i> below
host	string	yes	Server name or address
path	string	yes	Server directory and/or file name
username	string	no	Optional user name for server access
password	string	no	Optional password for server access, if <i>plainText=1</i> attribute in parent element not given: encrypted with public key

ProtType: this type contains types of transfer protocols. These are possible values:

Value	Description
FTP	FTP protocol
FTPS	FTPS protocol
HTTP	HTTP protocol
HTTPS	HTTPS protocol
TFTP	TFTP protocol

SIP users / devices

<CreatePPUser>

The client can send this request to create a new PP User data set. The following fields are defined:

Name	Type	Mandatory	Description
plainText	boolean	no	"1" or "true", to use plain text passwords
replaceData	boolean	no	"1" or "true", to replace existing entries
<user/>	element	yes	Data of PP User to create, see <i>PPUserType</i> below

Depending from the OMM type it may be allowed to create a PP User without any pre-defined attribute. In this case the client may send an empty CreatePPUser request. If no pin is given or if it is empty, it is set to "0000" automatically. The relation type will be set to "Unbound" automatically.

PPUserType: this type contains all data fields of a PP User. It is used in different requests and responses defined in this document. Not all fields are used in all OMM versions and in all requests. The following fields are defined:

Name	Type	Description
relType	enum	Type or state of a relationship to a PP Device, see <i>PPRelTypeType</i> below
name	string	User name
num	string	Phone number or SIP user ID
addId	string	Additional ID/User Login Id, either "AdditionalId"/user pin for the subscription process or "User Login Id" for the PP login process with unbound devices.
pin	string	PIN number, for the PP login process with unbound devices, if <i>plainText=1</i> attribute in <CreatePPUser> not given: encrypted with public key

Name	Type	Description
sipAuthId	string	SIP authentication user
sipPw	string	SIP authentication password, if <i>plainText=1</i> attribute in <CreatePPUser> not given: encrypted with public key
sosNum	string	SOS number
voiceboxNum	string	Voice box number
manDownNum	string	MANDOWN number

PPRelTypeType is an enumeration value which describes the type of a relation between a PP Device and a PP User. It is defined as follows:

Value	Description
Unbound	This PP Device or PP User can be bound dynamically, currently it is unbound
Dynamic	This PP Device or PP User can be bound dynamically, currently it is bound
Fixed	This PP Device or PP User has a fixed relation

System features: digit treatment

<CreateDigitTreatment>

The client can send this request to create a new digit treatment rule. The following fields are defined:

Name	Type	Mandatory	Description
replaceData	boolean	no	"1" or "true", to replace existing entries
<rule/>	element	yes	Data of digit treatment rule to create, see <i>DigitTreatmentType</i> below

DigitTreatmentType: This type contains all data fields of a digit treatment rule. It is used in different requests and responses defined in this document. The following fields are defined:

Name	Type	Description
externalPattern	string	External numbers to be replaced or scanned
internalPattern	string	Internal numbers to be replaced or scanned
directory	boolean	If true, rules applies to corporate directory entries; default false
direction	enum	One of "Incoming", "Outgoing", "Both" "Incoming": Rule applies to the calling party number of an incoming call "Outgoing": Rule applies to the dialled number of an outgoing call "Both": Rule applies to the calling party number of an incoming call and the reverse rule to the dialled number of an outgoing call "Directory": Rule applies to corporate directory (LDAP) entries

System features: Directory

<CreateLDAP>

With this request the client can create a corporate directory data set. The OMM supports a limited number of LDAP data sets. The following fields are defined:

Name	Type	Mandatory	Description
plainText	boolean	no	"1" or "true", to use plain text passwords
replaceData	boolean	no	"1" or "true", to replace existing entries
<ldap/>	element	yes	LDAP configuration, see <i>LDAPType</i> below

LDAPType: this type contains all attributes needed to configure an LDAP server. The following fields are defined:

Name	Type	Mandatory	Description
name	string	yes	LDAP data set name description
active	boolean	yes	"1" or "true", if this data set is active
order	integer	no	Order number to prioritize this LDAP data set. This setting might effect the order number in other LDAP data-sets. A reordering of all LDAP data sets will be performed. If empty, the LDAP data set is queued as last entry.
server	string	yes	LDAP server name or IP address
port	integer	yes	LDAP server port
username	string	yes	User name for server access
password	string	yes	Password for server access, if <i>plainText=1</i> attribute in <CreateLDAP> not given: encrypted with public key
displayType	enum	yes	One of "CN", "SN, GN"
timeout	integer	yes	Search timeout in seconds
searchType	enum	yes	One of "GN" (given name), "SN" (surname), "CN" (common/complete name). Note: Up to now CN is not supported

Name	Type	Mandatory	Description
searchBase	string	yes	<p>Search base: to make search requests unique for different users the search base configuration can include place holders which are replaced by user specific values when submitting the LDAP request to a server.</p> <p>The following place holders are defined: "<TEL>" which is replaced by the specific telephone number of the user, "<DESC1>" which is replaced by the "hierarchy1" attribute value of the user "<DESC2>" which is replaced by the "hierarchy2" attribute value of the user.</p> <p>Note: The telephone number in SIP - DECT is not limited to numeric character.</p>

The search type "Name" means search for surname, "Full" means search for given name. The display type "Name" means display Surname, given name, "Full" means given name and surname.

System features: Feature access codes

<SetFACPrefix>

A client can change the global FAC prefix using this request. The following fields are defined:

Name	Type	Mandatory	Description
prefix	string	yes	New FAC prefix

<SetFAC>

A client can change a FAC using this request. The following fields are defined:

Name	Type	Mandatory	Description
seq	boolean	yes	Should be "0"
<fac/>	element	yes	FAC to be changed, see <i>FAC-Type</i> below

Only one FAC can be changed at once.

FeatureType: This type contains all attributes of a FAC. The following fields are defined:

Name	Type	Description
feature	enum	The feature invoked by this FAC, see <i>Feature-Type</i> below
enable	boolean	"1" or "true", if this FAC is enabled
fac	string	The code, a dialable number

FeatureType is an enumeration value defined as follows:

Value	Description
ActivateSubscription	Activate the subscription mode
ActivateWildcard	Activate wild card subscription mode
DeactivateSubscription	Deactivate subscription mode
UserLogin	User Login
UserLogout	User Logout
PINChange	Change the PIN

UserLogin, *UserLogout*, *PINChange* are not available on all OMM versions.

System features: XML applications

<SetXMLApplication>

The client can send this request to change an XML application setting. The following fields are defined:

Name	Type	Mandatory	Description
plainText	boolean	no	"1" or "true", to use plain text passwords
replaceData	boolean	no	"1" or "true", to replace existing entries
<xmlAppl/>	element	yes	Data of record to be changed, see <i>XMLApplicationType</i> below

XMLApplicationType: this type contains all data fields of an XML application setting. The following fields are defined:

Name	Type	Description
name	string	Name of the XML application. For built-in XML applications predefined names have to be used. The following built-in names for XML applications are available: <i>callerList</i> : External PBX caller list support. The local PP caller list is disabled when set. <i>redialList</i> : External PBX redial list support The local PP redial list is disabled when set. <i>userPresence</i> : XML user presence application support by an external server. <i>systemAppMenu</i> : XML system application menu support by an external server. <i>eventActions</i> : Call event action URI support to an external XML server.
enable	boolean	"1" or "true", the XML application shall be activated

Name	Type	Description
id	integer	ID of the XML application. This value can not be used by the client in <CreateXMLApplication>.
type	enum	Specifies the application type as "BuiltIn" or "Dynamic"
<url/>	element	User data server configuration settings, see <i>URLType</i> on page 91

The path of the *URLType* includes the path, query and fragment of the URI, e.g. "omm.callLists?key=17&cnt={count}&na={number}" As shown the *URLType* path contains predefined replacements. The following predefined replacements are known by the OMM:

Value	Description
{count}	Number of items to be requested from the XML server
{subsc} or {number}	Identification of the XML client e. g. its subscriber number
{sicha}	Silent charging indication
{boot}	End of boot sequence indication
{reg}	Successful registration indication
{onho}	On-hook indication
{offho}	Off-hook indication
{in}	Incoming call indication
{out}	Outgoing call indication
{poll}	Time based indication
{sip}	SIP Notify indication
{con}	Connect indication
{dis}	Disconnect indication
{rege}	Registration event indication

<CreateXMLApplication>

The client can send this request to create a new XML application setting. Built-in application settings can not be created. The following fields are defined:

Name	Type	Mandatory	Description
plainText	boolean	no	"1" or "true", to use plain text passwords
replaceData	boolean	no	"1" or "true", to replace existing entries
<xmlAppl/>	element	yes	Data of XML application to create (see <i>XMLApplication-Type</i> on page 98)

User Data

With external user data configuration files, you can manage / import SIP user accounts without adding them manually on the OMM web service. The mechanism basically works with the following steps.

1. The OMM loads an additional configuration file ("user_common.cfg") that defines various default settings.
2. On the DECT handset, a user starts the login procedure by entering a phone number (for example "4360") and a PIN.
3. The OMM imports an additional user configuration file ("4360.cfg"). This configuration file provides the SIP user account to be used.

Note

With SIP-DECT™ Lite, you can also add SIP user accounts by adding <CreatePPUser/> XML statements to the system configuration file (see Example System Configuration Files starting on page 74).

Activating User Data Configuration

You can manually configure a URI for downloading the provisioning configuration files. Log in to the OMM web service. Enable the **Advanced settings** option. Navigate to the **System: DB management** page. In the **User data import** section, activate the **Active** option. Also select the desired Protocol, enter the **Server** address and set the subdirectory **Path**. Optional provide **User name** and **Password**.

Alternatively, add a <SetUserDataServer/> XML statement to the system configuration file (see Example System Configuration Files starting on page 74).

Example: Common Configuration

The following example depicts the possible contents of a common configuration file ("user_common.cfg") to be used for external user data provisioning.

```
# user_common.cfg sample configuration file for Automatic User Import
# retrieved via the net using file transfer protocols like tftp, ftp(s) or http(s)
# comments are starting with the hash sign: "#"
# BOOL variables support YES Y 1 TRUE or NO N 0 FALSE (case does not matter),
# other values are interpreted as false

# Common User data configuration possibilities:
# OM_<variable> # Identifier for an OMM variable setting
# UDS_<variable> #Identifier for a user data server variable setting
# UD_<variable> # Identifier for a user data variable setting

OM_Uniqueid=NUMBER
# What will be the unique user identification in the system, e. g. NUMBER or UID (login
# user id) / default=NUMBER "<user>.cfg" <--> "<NUMBER>.cfg" or "<UID>.cfg"
# if UID is used, it must be for sure, that all login user ids are different from all OMM
# internal user ids! The login user id will be stored in the 'login/additional id' data
# element of the user data set within the OMM data base.

UDS_CommonUpdateInterval=6
# Interval to re import this file in hours / default=24 hours if not set

UDS_UseExternalUsers=YES
# Enables / disables user data import - if disabled all users are deleted in the OMM
# (incl. private data) and gets unlinked from the handset / default=yes

UD_SosNumber=112
# Common SOS number

UD_ManDownNumber=112
# Common ManDown number

UD_VoiceMailNumber=22222
# Common VoiceMail

UD_Pin=1234
# User PIN, all user data sets will be set to this value initially when
# not set in the # "<user>.cfg" file / default=0000

UD_UpdateInterval=4
# Interval to re import user data files in hours / default=24 hours when not set
```

Example: User Data Configuration

The following example depicts the possible contents of a provisioning user configuration file (“[number].cfg”) to be used for external user data provisioning.

```
# 4360.cfg sample user configuration file
# Possible user data configuration settings:
UD_PinDel=FALSE
# BOOL, if TRUE the user PIN will be deleted in OMM private data to default "0000",
UD_Pin=4360
# User PIN to login and logout
UD_UpdateInterval=1
# Interval to re import user data files in hours / default=24 hours if not set
UD_Number=4360
# Subscriber number, ignored when NUMBER is unique (OM_Uniquelid=NUMBER)
UD_Name=Julian
# Displayed name
UD_SosNumber=112
# User SOS number
UD_ManDownNumber=112
# User ManDown number
UD_SipAccount=4360
# SIP account
UD_SipPassword=4360
# SIP password
UD_VoiceMailNumber=22222
# User VoiceMail
```

Messaging

The SIP-DECT™ Lite solution supports messaging that can be used for example to send text messages between DECT handsets. If enabled, sending and receiving messages and local phone book entries (“vcards”) on DECT handsets is possible without an extra configuration file. To use additional messaging features, you need to provide a configuration file.

With SIP-DECT™ Lite, the messaging service is limited to message priorities “Info”, “Low”, “Normal” and “High”. Messages with priority “Emergency” and “Locating Alert” as well as paging functions are not supported. This means that you cannot use the locating service and extended alarm scenarios that are available with multi-cell SIP-DECT® with SIP-DECT™ Lite.

Tip: Developing a messaging application is described in depth in a manual valid for the multi-cell SIP-DECT® product (see References on page 113). You can use this manual, but restrictions as mentioned above will apply.

Activating Messaging Configuration File

You can manually configure a URL for downloading the messaging configuration file. Log in to the OMM web service. Enable the **Advanced settings** option. Navigate to the **System: System settings** page. In the **OM Integrated Messaging & Alerting service** section, activate the **Active** option. Also enter the **URL** to download the configuration file. The **URL** typically addresses a single configuration file named "img.cfg".

Alternatively, add a <SetIMA/> XML statement to the system configuration file (see Example System Configuration Files starting on page 74).

Note

Basic messaging is activated by default without the support of a configuration file.

Example Messaging Configuration File

The following example depicts the possible contents of a message configuration file ("img.cfg"). The example queries a popular RSS feed and displays arriving news on some DECT handsets. The example also displays e-mail that is sent to a "dect@sip-dect.com" e-mail account on arbitrary DECT handsets. You need to send an e-mail with a specific subject line to this account, for example "tel:3001 You got mail!".

```
<MailBoxAccount
  mailBox="EmailPOP3"
  trySslFirst="false"
  pollTime="10"
  mbServer="192.168.112.1"
  mbUser="dect"
  mbPassword="s3creTs"
/>
<SendmailAccount
  auth="AuthNone"
  trySslFirst="false"
  smtpServer="192.168.112.1"
  senderAddress="dect@sip-dect.com"
/>
<RSS>
<feed refresh="40" trigger="RSSslashdot"
  url="http://rss.slashdot.org/Slashdot/slashdotatom"
/>
</RSS>
```

```
<AlarmScenario>  
  <as alarmMsg="/.news:%c" alarmTriggerId="RSSslashdot" autoDelete="true"  
    confirmTimeout="0" level="1" popUp="false" priority="PriInfo"  
    recipients="tel:3001;tel:3002"  
    requiredPosConfirmCount="0" />  
</AlarmScenario>
```

Tip: For developing a messaging application, you can use the RFP's SSH console for debugging. Activate the **System: System settings: Remote access** option. Log in with SSH ("ssh Omm@rpf"). Enter "setconsole" to view debug messages. Enter "ommconsole" and "ima" to view available commands.

XML Application

The SIP-DECT™ Lite solution supports customized XML applications for Aastra 600d DECT handsets. With this, powerful applications can be created that extend the feature set of the SIP-DECT™ Lite solution. As an example, the **System menu** available on the DECT handsets for managing SIP-DECT™ Lite features is realized using this technique.

Note

Creating an interactive XML application typically requires a server that executes scripts or programs. Also, you will need to read the XML terminal interface specification (see References on page 113) for developing a new XML application.

Activating an XML Application

You can manually configure a URL for different application hooks on the DECT handsets. Log in to the OMM web service. Enable the **Advanced settings** option. Navigate to the **System features: XML applications** page. Click on the edit icon of the desired XML application. Select the desired Protocol (HTTP or HTTPS). Enter the **Server** address and set the **File** to the server side program name. Optional provide **User name** and **Password**.

Alternatively, add a <SetXMLApplication/> XML statement to the system configuration file (see Example System Configuration Files starting on page 74).

Example XML Application

The following example requires an Apache web server that executes scripts in the PHP programming language.

```
<?php
# sample info dialog for OMM Handset XML interface
### output($xml)
# prepare XML output by remove and convert strings
# echo output($xml,"UTF-8");
function output($xml,$encode)
{
    if ($encode == "UTF-8")
    {
        header("Content-Type: text/xml; charset=UTF-8");
        $xml = '<?xml version="1.0" encoding="UTF-8"?>\n'.$xml;
    }
    $xml = str_replace("\r\n", "\n", $xml); #replace CRLF
    $xml = str_replace("\n", "\n", $xml); #replace "\n"
    $xml = str_replace("\r", "\r", $xml); #replace "\r"
    $xml = str_replace("\t", "", $xml); #replace tab
    $xml = str_replace("&", "&amp;", $xml); #replace &
    return $xml;
}
$user_agent=$_SERVER["HTTP_USER_AGENT"];
if(stristr($user_agent,'Aastra'))
{
    $value=preg_split('/ MAC:/', $user_agent);
    $fin=preg_split('/ /', $value[1]);
    $value[1]=preg_replace('/\./', $fin[0]);
    $value[2]=preg_replace('/\./', $fin[1]);
    $userinfo['IP']=$_SERVER['REMOTE_ADDR']; # OMM IP-Address
    $userinfo['LANG']=$_SERVER['HTTP_ACCEPT_LANGUAGE']; # Handset Language
    $userinfo['AGENT']=$_SERVER['HTTP_USER_AGENT']; # User Agent
    $userinfo['NUMBER']=$value[1]; # Extension Number
    $userinfo['FIRMWARE']=$value[2]; # OMM Firmware
}
# Info
$xml = '<AstralPPhoneTextScreen destroyOnExit="yes">\n';
$xml .= '<Title wrap="no">System Info</Title>\n';
$xml .= '<Text>SW: '.$userinfo['FIRMWARE'].'
IP: '.$userinfo['IP'].'
LANG: '.$userinfo['LANG'].'
AGENT: '.$userinfo['AGENT'].'
NUMBER: '.$userinfo['NUMBER'].'</Text>\n';
$xml .= '</AstralPPhoneTextScreen>';
echo output($xml,"UTF-8");
?>
```

The PHP script typically generates the following XML answer.

```
<?xml version="1.0" encoding="UTF-8"?>
<AstralPPhoneTextScreen destroyOnExit="yes">
<Title wrap="no">System Info</Title>
<Text>SW: 3.1RC1
IP: 192.168.112.17
LANG: en
AGENT: Aastra SIP-DECT
NUMBER: 3001</Text>
</AstralPPhoneTextScreen>
```

Appendix

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 on the Internet.

Communications Regulation Information

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.

Any changes or modifications not expressly approved by Aastra could void the user's authority to operate this equipment.

This device complies with part 15 of the FCC Rules and with RSS-210 of Industry Canada. 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.

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes :

- (1) l'appareil ne doit pas produire de brouillage, et
- (2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

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

Exposure to radio frequency (RF) signals

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

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

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

The mobile device 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 has been tested in accordance with the measurement procedures specified in FCC/OET Bulletin 65 Supplement C (2001) and IEEE 1528-2003.

Warranty Repair Services

Should the product fail during the Warranty Period, please call 1-800-574-1611 for further information.

You will be responsible for shipping charges, if any. When you return this product for warranty service, you must present proof of purchase.

After Warranty Service

Aastra offers ongoing repair and support for this product. This service provides repair or replacement of your Aastra product, at Aastra's option, for a fixed charge. You are responsible for all shipping charges. For further information and shipping instructions, contact our service information number: 1-800-574-1611.

Note

Repairs to this product may be made only by the manufacturer and its authorized agents, or by others who are legally authorized. This restriction applies during and after the Warranty Period. Unauthorized repair will void the warranty.

Technical Data

RFP SL35 IP

Power supply:	Power over Ethernet IEEE 802.3af, class 3 or AC adapter (110 – 240 V / 50/60 Hz)
Ambient temperature:	23 °F to 113 °F
Relative humidity:	5 to 95 % (non-condensing)
Storage temperature:	-40 °F to 158 °F
Current consumption:	120 mA
Type of ingress protection:	IP 20
Flame resistance:	UL94 V0-5VB
Colour:	ice grey
Weight:	14.71 oz (without AC adapter)
Dimensions (Width x Height x Depth):	7.68 x 7.87 x 1.18 in; wall-mountable

Aastra 610d, 620d, 630d

Standard:	DECT / GAP
No. of channels:	60 duplex channels
Frequencies:	1920 MHz to 1930 MHz (UPCS)
Duplex method:	Time-division multiplex, 10 ms frame length
Channel subdivision:	1728 kHz
Bitrate:	1152 kbps
Modulation:	GFSK
Voice coding:	32 kpbs
Output:	5 mW (average output per active channel)

Appendix

Range:	up to 980 ft outdoors, 160 ft indoors
Bluetooth QD ID Aastra 620d, 630d:	B014700
Power supply charger cradle:	AC 110 – 240 V / 50/60 Hz
Handset operating time (standard battery):	Stand-by time: up to 95 hours Talk time: up to 15 hours
Handset operating time (power battery):	Stand-by time: up to 190 hours Talk time: up to 30 hours
Standard rechargeable battery:	Li-Ion battery, 3.7 V / 850 (880) mAh / 3.15 (3.3) Wh
Power battery (Aastra 620d / 630d):	Li-Ion battery, 3.7 V / 1800 (2030) mAh / 6.66 (7.6) Wh
Time to charge completely discharged standard batteries:	2.5 hours
Permissible ambient temperatures for operating the handset:	41 °F to 104 °F
Permissible storage temperature:	23 °F to 113 °F
Charger cradle dimensions (Length x Width x Height):	2.99 x 2.95 x 0.94 in
Handset dimensions (Length x Width x Height):	Aastra 610d / 620d: 5.31 x 1.93 x 0.89 in Aastra 630d: 5.31 x 2.08 x 0.89 in
Charger cradle weight:	1.41 oz
Handset weight:	Aastra 610d / 620d (with battery): 4.23 oz Aastra 630d (with battery): 4.41 oz
Length of power supply cable:	5 ft

Abbreviations

API	Application Programming Interface
DECT	Digital Enhanced Cordless Telecommunication
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Server
GAP	Generic Access Profile
LDAP	Lightweight Directory Access Protocol
NTP	Network Time Protocol
OM AXI	OM Application XML Interface
OM IMA	OM Integrated Messaging & Alerting service
OML	OM Locating application
OMM	OpenMobility Manager
PARK	Portable Access Rights Key
PBX	Private Branch Exchange (i. e. communications system)
PP	Portable Part, handset
RFP	Radio Fixed Part, base station
SIP	Session Initiation Protocol
SNTP	Simple Network Time Protocol
ToS	Type of Service
URI	Uniform Resource Identifier
VoIP	Voice over IP

Definitions

Asterisk Asterisk is a complete Open Source PBX in software. It runs on Linux, BSD and MacOSX and provides many features. Asterisk supports voice over IP in many protocols, and can interoperate with almost all standards-based telephony equipment.

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 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.

The operation of GAP-capable telephones is comparable to that of analogue terminals. For example, features can be called up via “*” and “#” procedures.

IPEI	International Portable Equipment Identity 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	Portable Access Rights Key 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.
Radio Fixed Part (RFP)	An RFP provides a DECT radio cell and terminates the radio link from the portable DECT device.

Trademarks

SIP-DECT® and SIP-DECT™ Lite are registered trademarks of Aastra.

Windows® is a registered trademark of Microsoft Corporation.

All other product and brand names are trademarks, registered trademarks, or service marks of their respective holders.

References

Other Valid Documentation

This user guide describes installation, administration and usage of the SIP-DECT™ Lite system. Please observe also the information given in the documentation listed below. These documents describe the larger feature set of the multi-cell SIP-DECT®, but apply also to the feature set of SIP-DECT™ Lite.

- Aastra 610d, 620d, 630d; SIP-DECT User's Guide; Handset Release ≥ 4.0
- SIP-DECT; OM Integrated Messaging & Alerting Application; Installation, Administration & User Guide
- SIP-DECT XML terminal interface specification
- Aastra Redirection and Configuration Service (RCS); User Guide

Note

The latest update of the documentation is available for downloading at <http://www.aastrausa.com>.

RFC Reference

The SIP-DECT™ Lite system complies to the following RFCs:

- RFC 1350, The TFTP Protocol, Revision 2, July 1992
- RFC 2090, TFTP Multicast Option, February 1997
- RFC 2347, TFTP Option Extension, May 1998
- RFC 2348, TFTP Block size Option, May 1998
- RFC 2349, TFTP Timeout Interval and Transfer Size Options, May 1998
- RFC 2236, Internet Group Management Protocol, Version 2, November 1997
- RFC 1889, RTP: A Transport Protocol for Real-Time Applications, January 1996
- RFC 2030, Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI, October 1996
- RFC 2131, Dynamic Host Configuration Protocol, March 1997
- RFC 2327, SDP: Session Description Protocol, April 1998
- RFC 2474, Definition of the Differentiated Service Field (DS Field) in the IPv4 and IPv6 Headers, December 1998
- RFC 2617, HTTP Authentication: Basic and Digest Access Authentication, June 1999
- RFC 3164, The BSD Sys Log Protocol, August 2001
- RFC 2833, RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals, May 2000
- RFC 3261, Session Initiation Protocol (SIP), June 2002
- RFC 3264, An Offer/Answer Model with Session Description Protocol (SDP), June 2002
- RFC 3420, Internet Media Type message/sipfrag, November 2002
- RFC 3515, The Session Initiation Protocol (SIP) Refer method, April 2003

- RFC 3665, The Session Initiation Protocol (SIP) Basic Call Flow Examples, December 2003
- RFC 3842, A Message Summary and Message Waiting Indication Event Package for the Session Initiation Protocol (SIP), August 2004
- RFC 3891, The Session Initiation Protocol (SIP) "Replaces" Header, September 2004
- RFC 3892, The Session Initiation Protocol (SIP) Referred-By Mechanism, September 2004
- RFC 4566, SDP: Session Description Protocol
- RFC 2782, A DNS RR for specifying the location of services (DNS SRV)
- RFC 3262, Reliability of Provisional Responses in the Session Initiation Protocol (SIP)
- RFC 3311, The Session Initiation Protocol (SIP) UPDATE Method

Index

A

- Astra Redirection and Configuration Service 15
- AC clips 15
- Advanced settings (OMM web service) 29
- Authentication code (factory default) 28

B

- Backup 17, 33
- Basic settings (OMM web service) 29
- Battery 15

C

- Charger cradle 15

D

- DECT handsets (subscribe) 26
- DHCP configuration 14, 17, 18, 45, 51
- DSL 14
- Dynamic VLAN configuration 42

F

- Factory defaults 31
- Feature access codes (FAC) 66

G

- Gateway 18

I

- Input mode (static IP address configuration) 20
- IP address (via DHCP) 18
- IP configuration 14, 18

L

- LAN 13
 - socket 16
- LAN connection 17
- LED (handset) 15
- LED (RFP) 17
- License agreement 22
- Login
 - administrator login on the handset 44
 - OMM web service 49
 - user login on the handset 24
- Logout
 - administrator logout on the handset 44
 - OMM web service 49
 - user logout on the handset 25

N

- Netmask 18
- Number (phone) 21, 23

O

- OMM (OpenMobility Manager) 29
- OMM Web service (Web configurator) 20
- OMM web service (web configurator) 18

P

- PARK 28, 32
- Password
 - default 19, 22
 - SIP 21, 23

Phone number 24
PIN 21, 23
PoE 17
Power (socket) 16
Provider-operated SIP server 13
Proxy server 21, 23

R

RCS 15
Registrar server 21, 23
Restore 33

S

Security 28
SIP PBX 13, 20
SIP user accounts 20
SNMP
 configuration 58
 overview 41
Static IP address configuration 19, 45,
 51, 53
Static VLAN configuration 42
Subscribe (DECT handsets) 26
Subscription mode 26, 27, 47

U

Updating (software) 30
USB
 flash drive 16
 socket 16
User ID 24
User-operated SIP PBX 13

V

VLAN 42, 45, 51

W

WAN port 14



Copyright 2012 www.aastrausa.com
All rights reserved
As of 22.06.2012
Subject to changes

CE

AASTRA