SIP - DECT
OM Integrated Messaging & Alerting Application

Installation, Administration & User Guide

AASTRA

Welcome to Aastra

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

The following user guide will assist you in using your
SIP - DECT OM Integrated Messaging & Alerting Application
and provide answers to all 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.aastra.de** or **http://www.aastra.com**.

We hope you enjoy using your SIP - DECT OM Integrated Messaging & Alerting Application.

Contents

OM Integrated Messaging & Alerting 1

Supported Message Format 2
OM IMA Service Features 2
Other Valid Documentation 3
Notes on Licences 4

Installation 5

Activating the OM IMA Service 5
Enabling Messaging for DECT Handsets 7
Configuring the OM IMA Service 8

Configuration 10

Basic Messaging Concepts 10
Message Matrix 11
URI Syntax 13
vCard Support 13
Configuration File Syntax 15
Configuration File Reference 16
MailBoxAccount 16
SendmailAccount 18
RSS / feed 19
AlarmScenario / as 20

Debugging the OM IMA Setup 27

OMM Console Login 27
Using the OMM Console 30
OMM Console Reference 31

Appendix 32

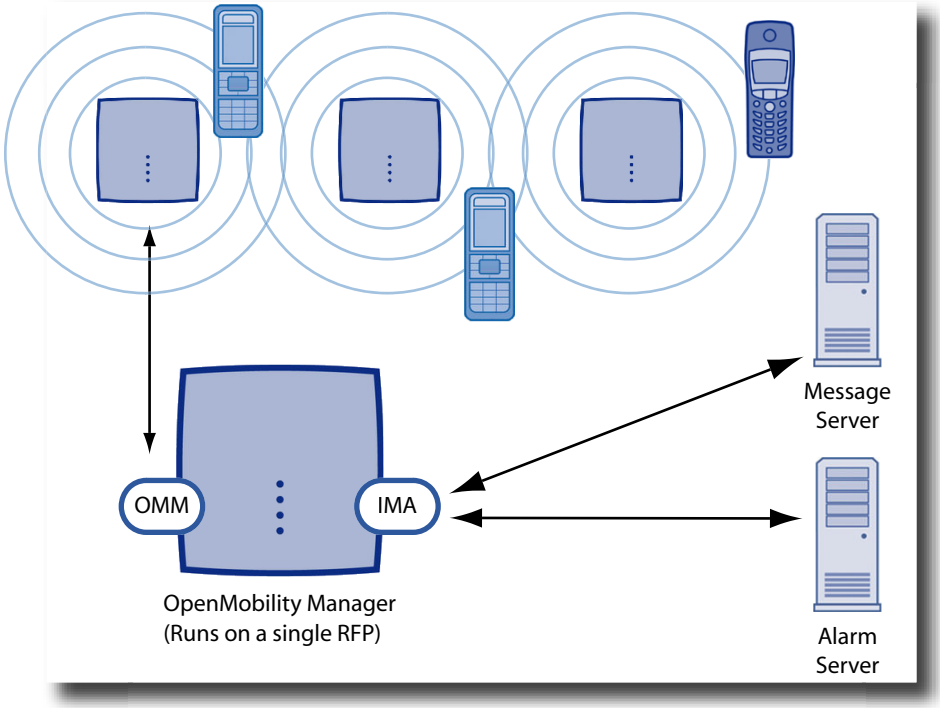
Abbreviations 32
Trademarks 32

Index 33

OM Integrated Messaging & Alerting

The **OpenMobility Integrated Messaging & Alerting** service (in the following "OM Integrated Messaging & Alerting service" or "OM IMA") is a messaging and alarm service for the OMM-SIP / SIP – DECT solution. The OM Integrated Messaging & Alerting service supports the delivery of messages to or from DECT portable parts.

The OMM-SIP / SIP – DECT solution generally targets larger DECT networks. A complete system comprises as many as 4500 DECT handsets communicating in a DECT network with up to 2048 RFPs. The following figure depicts the overall architecture of the complete messaging solution.



Architecture of the OpenMobility Messaging & Alerting service

The OpenMobility Manager (OMM) and the OM Integrated Messaging & Alerting service (OM IMA) both run on a single Radio Fixed Part (RFP) or on a dedicated Linux server system. External messaging solutions, such as a message server or an alarm server, communicate by means of a networked and encrypted XML interface with the OM IMA service.

Supported Message Format

The main purpose of the OM IMA service is to deliver text messages, track alarms and control the necessary signalling to the RFPs available in the DECT network. All delivered text messages support the following characteristics:

- messages contain up to 1000 characters;
- messages have a priority such as bulk, normal, or high;
- messages can be received in the background or in the foreground (pop-up);
- messages may trigger a read confirmation which is sent to the originator;
- messages may require a manual confirmation from the receiver;
- messages may transport a vCard that is automatically stored in the recipients phone book which may also configure a short dialling entry;
- paging messages include a call back number that is dialled immediately if the receiver presses the off hook key while the message is displayed.

OM IMA Service Features

The OM IMA service runs directly on the same RFP or server that also runs the OMM. Therefore, no additional hardware is required for the following set of features:

- sending and receiving text messages between DECT portable parts which includes normal messages, alarm messages or messages queuing up in a job list;
- sending messages from a messaging server such as the OpenMobility Locating application to the DECT portable parts;
- sending of alarm messages from a DECT portable part (triggered by pressing a predefined SOS key or by the ManDown function).

With additional configuration, the following features are possible:

- management of confirmations and applying escalation rules for alarm messages;
- querying arrived mail from an E-Mail server, triggering alarm messages by E-Mails, or sending E-Mail via a messages gateway (requires additional configuration);
- subscribe to RSS feeds and either receive news as text message or trigger an alarm message based on RSS feed contents (requires additional configuration);

- sending entries stored in the personal telephone book of a DECT handsets as vCard to another DECT handset;
- sending vCards from a messaging server, e.g. to configure a short dialling entry for a feature access code (FAC) that triggers a function such as a door opener;
- sending a paging message from a DECT handset that requests the sender to immediately dial a call back number that is part of the paging message.

Note, that the limited storage capacity of the RFP does not allow to store the message contents. However, it is possible to extend the OM IMA service with a separate messaging application, which runs for example on a PC server system.

Other Valid Documentation

This user guide describes installation, administration and usage of the OM Integrated Messaging & Alerting service. Please observe also the information given in the documentation to other parts of your OMM SIP - DECT installation:

- SIP - DECT; OM System Manual
  Describes the installation, administration, and maintenance of the SIP - DECT system.
- SIP - DECT; OM Locating Application
  If you have also purchased the “OpenMobility Locating” application, please refer to this user guide which describes the installation, administration, and usage of the OM Locating application.
- SIP - DECT; OM Handset Sharing & Provisioning
  This user guide describes the enhanced user and handset management features and the OM provisioning concept.
- SIP - DECT; Aastra 610d, 620d, 630d Messaging & Alerting Applications
  This user guide describes the special messaging features of the Aastra 6x0d DECT terminal series and how to use them.

Notes on Licences

Application licence
In order to use the OM IMA service, you need the appropriate licences to configure and use the application. Upload the received licence file either in the "OM Management Portal" (Java tool) or via the OMM Web service. To operate the OM IMA service, the following licences are required:

- OM System Licence [Number]: Enables telephony for a number of RFPs
- OM Messaging & Alerting System Licence and
  OM Messaging Licence [Number]: Enables messaging for a number of handsets

The licence confirmation you received contains detailed information on activating the service. Note, that you can also start with the automatically applied demo license, which is valid for 72 hours.

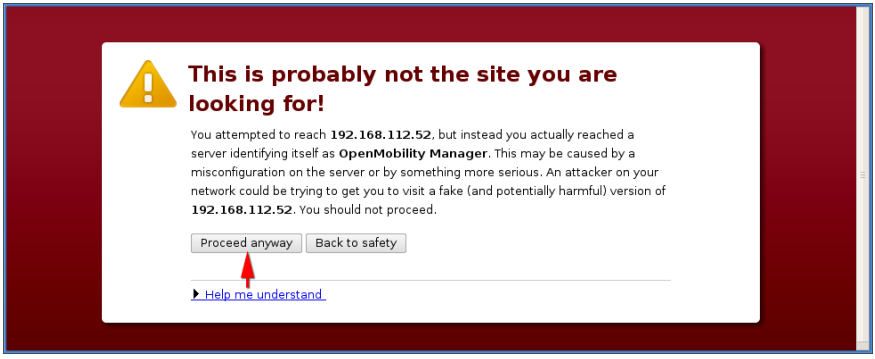
Installation

The **OM Integrated Messaging & Alerting** service does not require any installation, because the necessary software is already present in the software container of the OMM. However, you need to activate the OM IMA service to be started.

Activating the OM IMA Service

You can activate the OM IMA service on the OMM.

1. Start a web browser. Enter the DNS name or IP address of the OMM in the browser's address input. The OMM's web server switches to the secured HTTPS protocol and you will typically see a browser display like the following one.



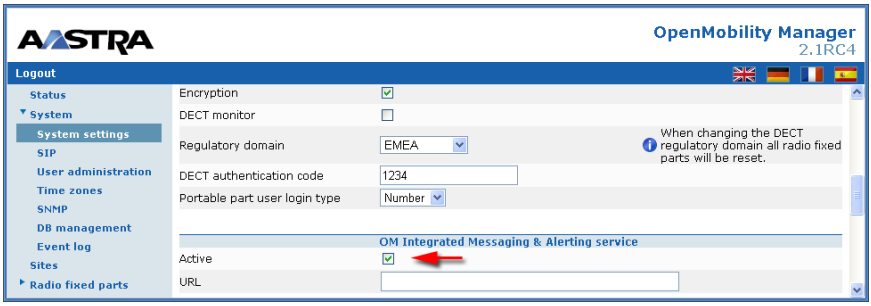
Certificate warning

To overcome the browser warning automatically, a regularly re-paid validation certificate for the OMM's network address needs to be issued by a third party. For connecting to the web user interface of the OMM in your LAN you can safely ignore this message and store a permanent exception in your browser.

After accepting the certificate warning, the browser displays the OMM's login page.

2. Enter the **User name** that is configured at the OMM for the "Full access" account type. This is "omm" by default, but you may have changed this setting at the OMM. Enter the **Password** for the OMM. Confirm with **OK**.

3. The OMM's web service main page is displayed. In the menu tree to the left, navigate to the **System**: **System settings** page. Scroll down to the **OM Integrated Messaging & Alerting service** section.



Activating the OM IMA service

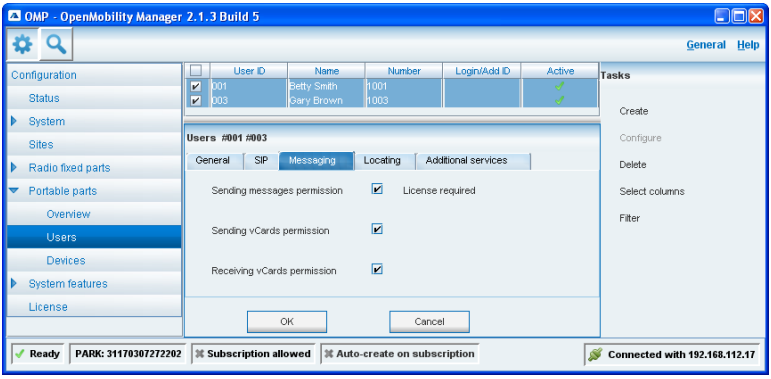
Activate the **Active** check box. Leave the **URL** input field blank for the basic OM IMA service. Confirm with the **OK** button available at the top of the page.

Switching on the **Active** check box starts the OM IMA service on the OMM. If the OM IMA service is running, you can for example send messages from one DECT portable part to another. To stop the OM IMA service, repeat the above procedure and de-activate the **Active** check box.

Enabling Messaging for DECT Handsets

There are several options that you can enable or disable for a DECT handsets. However, you cannot view or change these options in the OMM's web service. Start the OM Management Portal ("OMP") for this task:

1. Double click the "OMP.jar" file that is available on the OMM SIP 2.1 installation medium. Note, that you need the Sun/Oracle Java runtime environment installed on your PC in order to run the OMP.
2. Enter the **IP address**, **User name**, and **Password** for accessing the OMM.
3. Navigate to the **Portable parts**: **Users page**. Activate the check box for one or more of the displayed user entries. In the **Tasks** pane, click the **Configure** link to view the user entry details. Switch to the **Messaging** tab.



OM Management Portal ("OMP") - Messaging options for users

4. Activate or de-activate the desired options:

   Sending messages permission: Enable this option to allow DECT handset users to send messages.

   Sending vCards permission: Enable this option to allow DECT handset users to send private phone book entries as vCard messages.

   Receiving vCards permission: Enable this option if received vCard messages should be stored in the private phone book of the respective DECT handset users automatically. If this option is disabled, the DECT handset user needs to manually enable receiving vCards. The manually enabled vCard receiving mode ends automatically after 10 minutes.

5. Confirm your settings with **OK**.

Configuring the OM IMA Service

To configure and use additional functions with the OM IMA service, you need to provide a configuration file. Here is a first example of the configuration file, which will send a message if the SOS button is pressed on a DECT portable part:

```
<AlarmScenario>
<as alarmTriggerId="SOS" level="1" recipients="tel:1001"
priority="PrioHigh" alarmMsg="SOS from %n (%R)">
</AlarmScenario>
```

To activate this configuration, proceed as follows:

1. Copy the above example to the clipboard. Start an ASCII editor such as the Windows “Notepad” application. Paste the example into the ASCII editor and save to a new file. Change the phone number in the “recipients” attribute to match a currently subscribed DECT portable part.

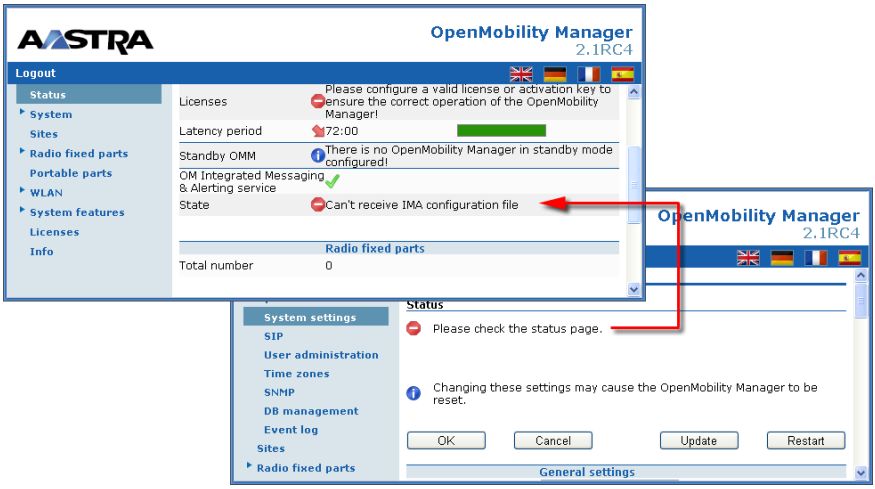
2. Place the configuration file on a server located in your LAN and configure the download **URL** on the OMM’s **System**: **System settings** page accordingly (see also Activating the OM IMA Service starting on page 5). Here are some examples for this setting:

   tftp://192.168.1.1/IMA.cfg: If you use the automatic DHCP configuration for the OMM, you already have an active TFTP server. Place the configuration file in it’s TFTP upload directory next to the OMM firmware file (“omm_ffsip.tftp”).

   http://omm/subdir/ima.cfg: You can also provide the configuration file on any web server in your LAN. If you develop an sophisticated IMA application, it is handy to start a web server on your PC to provide frequently changed configuration files during development and testing.

   ftp://omm.company.lan/subdir/IMA-CONFIG.XML: you can also provide the configuration file on any FTP server in your LAN.

   Note, that on most operating systems the directory and file names of the URL are case sensitive. If you confirm the changed **URL** setting, the OM IMA service is restarted. It will download the configuration file which in turn changes the OM IMA service configuration. If the OM IMA service cannot load the configuration file, you will see a small red warning sign on the OMM’s **System**: **System settings** page.



OM IMA Service: cannot download configuration file

Examine the detailed status message on the OMM's **Status** page. Correct the settings or change the TFTP, HTTP, or FTP server's configuration until no further errors are indicated.

3. Press the configured SOS softkey on a second DECT portable part. This should place the SOS call and concurrently sends a text message to the number you entered in the configuration file.

Configuration

The **OM Integrated Messaging & Alerting** service is configured by writing down the desired configuration in a configuration file. The configuration file is then downloaded by the OM IMA service on startup. Before we dive into the configuration file details, you need some basic information about the message structure and some basic concepts.

Basic Messaging Concepts

While the **OM Integrated Messaging & Alerting** service allows messaging service for all types of DECT portable parts, only the Aastra 610d/620d/630d DECT handsets offer the full feature set. This includes support for the following message types:

- Idle Box: a system pop-up message without confirmation nor tone;
- Info Message / Confirmation: a system pop-up message announced by a tone;
- Normal Message: a standard message from another user without confirmation; pop-up display only if that is configured on the receiving DECT handset;
- Urgent Message: a message from a user, with pop-up display and confirmation;
- Alarm Message: a system message (from alarm application only);
- Normal Job: a message automatically added to the job list;
- Urgent Job: a job message with completion confirmation;
- Alarm Job: a system urgent job message (from alarm application only);
- Localization Alert: a special system message which triggers an audible tone typically used to locate a person in danger (e.g. after Man-Down or SOS).

Each message consists of the following components:

OMM Message Structure

Component	Format / Purpose
Date/Time, ID	Time stamp when message was sent, and a unique ID
Sender	Identifies originator, URI (e.g. tel:1001 or maito:a@b)
Sender's Name	For displaying purposes only
Recipient	Identifies addressee, URI (e.g. tel:2002)

OMM Message Structure

Component	Format / Purpose
Recipient's Name	For displaying purposes only
Priority	Info, low, normal, high, alarm, locating alert
Flags	Message or job, auto delete flag
Encoding	Content encoding (typically UTF-8)
Confirmations required	Msg received, msg read, accept task, complete task
Content Type	Typically "plain text", others reserved for future ext.
Content	If content type is "plain text": up to 1000 characters

While different message types can be identified by specific display icons, the specific message handling will support the message purpose. For example, a **Pop-up** message is displayed in a window overlaying the current display. If the DECT handset user closes the window temporarily, the message is re-displayed (**Re-Popup**) after some activity e.g. after the user completed a phone call. Also, each message carries a flag (**Auto Delete Option**) which deletes the message automatically after the final confirmation.

Message Matrix

The following table show how specific message types are handled on the Aastra 6x0d DECT handsets.

Messaging Matrix: Message Handling

Message Type	Priority	Stored in Folder	Auto Delete Opt.	Pop-up	Re-Popup
Idle Box	-	-	Yes	No	No
Info / Confirmation	Low	-	Yes	Yes	No
Normal Message	Normal	Inbox	Yes	As configured	After Call (if popup)
Urgent Message	High	Inbox	Yes	Yes	Yes
Alarm Message	Alarm	Inbox	Yes	Yes	Yes
Normal Job	Normal	Jobs	Yes	Yes	Yes

Messaging Matrix: Message Handling

Message Type	Priority	Stored in Folder	Auto Delete Opt.	Pop-up	Re-Popup
Urgent Job	High	Jobs	Yes	Yes	Yes
Alarm Job	Alarm	Jobs	Yes	Yes	Yes
Localization Alert	Loc-Alert	-	Yes	Yes	Yes

Messaging Matrix: Message Confirmation and Signal

Message Type	Confirmation			Audible Signal
	Read	Accepted	Completed	
Idle Box	None			-
Info / Confirmation	None			Confirmation tone
Normal Message	None			Handset config: normal msg. tone
Urgent Message	Yes	-	-	Handset config: urgent msg. tone
Alarm Message	Yes	-	-	Handset config: alarm msg. tone
Normal Job	Yes	Yes	-	Handset config: normal msg. tone
Urgent Job	Yes	Yes	Yes	Handset config: urgent msg. tone
Alarm Job	Yes	Yes	Yes	Handset config: alarm msg. tone
Localization Alert	Yes	-	-	Defined by admin.

URI Syntax

For some configuration items, you need to specify recipient or destination attributes. These are encoded with a specific syntax, denoted as URI.

URI Types

URI	Description
tel:	Addresses a DECT handset by phone number
ppn:	Addresses a DECT handset by portable part number
cb:	Call back number (for callBackNumber parameter only)
mailto:	Addresses an e-mail recipient
alarm:	Triggers an alarm
omm:	URI for trigger by OMM (internal only)
loc:	URI for trigger by locating server (internal only)
emailsubject:	Configures alarm trigger that is matched by e-mail subject

Some URIs also support an asterisk wildcard:

- The “tel:*” URI addresses all DECT handsets that are able to use messaging. Note, that messages sent to this URI cannot enforce confirmations, thus also no confirmation timeout and no alarm scenario escalation is supported.
- The “emailsubject:Example*” URI matches all subjects starting with “Example”.

vCard Support

The Aastra 6x0d DECT handsets support receiving vCards that are automatically pushed to the personal directory of the DECT handset. The vCard syntax (RFC 2426) defines different keys that needs to be translated to the directory entry keys of the DECT handsets:

vCard Keys

Directory Key	vCard Keys	Content
Name	Primary: “FN:” Secondary: “N:”	[String] (UTF-8 or Latin-1)

vCard Keys

Directory Key	vCard Keys	Content
Private number	Primary: “TEL;HOME” Secondary: “…;HOME;VOICE” Tertiary: “TEL;ISDN”	[Number]
Business number	Primary: “TEL;WORK” Secondary: “…;WORK;VOICE” Tertiary: “TEL;VOICE” Quaternary: “TEL;PREF”	[Number]
Mobile number	Primary: “TEL;CELL” Secondary: “…;CELL;VOICE”	[Number]
Fax number	Primary: “TEL;FAX” Secondary: “…;FAX”	[Number]
E-Mail	Primary: “EMAIL” Secondary: “EMAIL;PREF;INTERNET”	[E-mail Address]
Quick-dial	“X-QC”	“2” - “9”
Melody name	“X-MEL”	[String]
VIP-number	“X-VIP”	[Number]
Character set	Primary: “VERSION” Secondary: “CHARSET”	[Mapping ID]
Framing	...of vCard: “BEGIN:VCARD” and “END:VCARD”	

During translation, the DECT handset evaluates the primary key first. If this is not found, the subsequent keys alternatives are evaluated. The following example shows an alarm scenario with vcard:

```
<AlarmScenario>
  <as alarmTriggerId="VCARD" level="1"
    recipients="tel:*" priority="PrioNormal"
    alarmMsg="BEGIN:VCARD&#x0D;&#x0A;VERSION:3.0&#x0D;&#x0A;
      FN:Miller&#x0D;&#x0A;TEL;HOME;VOICE:1234&#x0D;&#x0A;
      END:VCARD" vCard="true" />
</AlarmScenario>
```

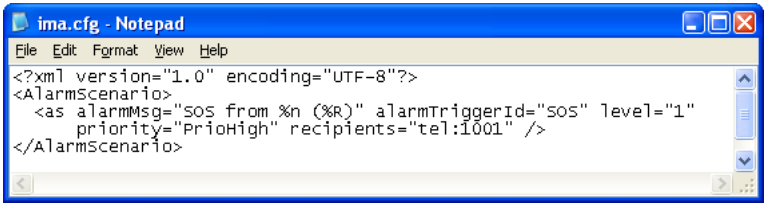
Please note: Remove the line breaks in the “alarmMsg” attribute.

Configuration File Syntax

The **OM Integrated Messaging & Alerting** service configuration file has an XML syntax which can be edited by using a plain text editor such as the Windows "Notepad" application. If you are already familiar with the XML syntax requirements, you may skip to Configuration File Reference starting on page 16.

The XML configuration file is always encoded in UTF-8. If you need to enter characters not available in the standard ASCII 32-127 character set, make sure to save the file as UTF-8. For example, in the Windows "Notepad" application, select the "UTF-8" entry from the **Encoding** selection of the **File**: **Save As** dialogue.

In the first line of the configuration file, the optional XML declaration may be used. All subsequent lines should follow a well formed XML syntax. The following basic example illustrates the syntax. This example will send a high priority message to the 1001 phone number if someone presses the SOS button on the DECT handset:



Basic OM IMA configuration file, displayed in Windows Notepad

Each configuration file consists of a series of XML tags. Each XML tag can be written as single tag (e.g. <as />) or as start-end tag combination which may nest other tags (e.g. <AlarmScenario><as /><AlarmScenario>). If you write down start-end tags, the tags needs to be balanced. For example, the following nesting is invalid: <AlarmScenario><as></AlarmScenario></as>.

Between two tags, you can insert any number of white space characters (that is: the space character, the tab character, or a line end character). This helps you to make up a user friendly and readable display. You can also include XML comments between tags (e.g. <!-- this is a comment -->) to improve readability.

An XML tag may have one or more attributes (e.g. "level="1""). An attribute needs to be separated from predecessing characters by a white space. The attribute value needs to be enclosed in single or double quotation marks.

The XML tag names and the attribute names are case sensitive. For example <A> and <a> are handled as different tags. The OMM service only accepts known XML tags and attributes. Moreover, the XML tags needs to follow a prescribed sequence and nesting and only pre-defined attributes are allowed for specific tags.

Configuration File Reference

In the **OM Integrated Messaging & Alerting** service configuration file, you will configure e-mail accounts, RSS feeds as well as alarm scenarios. You can write down the desired configuration statements in any sequence, provided that you keep the necessary XML syntax.

The following tables determine required attributes as “Mandatory” in the **Default** column. This column will otherwise show the default setting applied if the attribute is omitted. A minus character denotes an empty default string.

MailBoxAccount

This configuration file item is used to configure an e-mail account for polling available messages. The OM IMA service will poll this account and forward the acquired E-mails as text messages to different DECT handsets.

<MailBoxAccount />

Attribute	Type/Values	Default	Description
mailbox	EmailNone, EmailPOP3, NONE	Mandatory	Determines the mailbox account type; Use “NONE” to stop polling the account
mbServer	[IP or DNS]	Mandatory	Determines the maibox server; Either IP address or DNS name
trySslFirst	true, false	false	If set to “true” the OM IMA service tries to use SSL for encryption; If that fails, the standard port is tried (optional encryption with StartTLS)
pollTime	[Number]	30	Poll interval (minimum time in seconds, 10-3600s are allowed)
sinceTimestamp	[Number]	0	Used to ignore older mails stored in the mailbox; Use “0” to poll all mails, otherwise use value in seconds after 01-01-1970

<MailBoxAccount />

Attribute	Type/Values	Default	Description
mbPort	[Number]	0	The port number for POP3; Use “0” for standard port
mbSslPort	[Number]	0	The port number for SSL encrypted POP3; Use “0” for standard port
mbUser	[String]	-	user name for the POP3 mailbox account
mbPassword	[String]	-	password for the POP3 mailbox account

The E-mail account will be polled by the OM IMA service on a regularly basis. If a new E-mail comes in, the E-mail will be fetched and removed from the E-mail server. The OM IMA service then forwards the E-mail to the recipient mentioned in the subject of the E-mail. For example, to send to a particular DECT handset, send an E-mail with the following subject:

tel:1001 Hello, you just got mail!

If the E-mail cannot be delivered, the OM IMA service will reply with an error mail provided that the SendmailAccount is configured. For example:

IMA [noreply:ima]: Error: Transmission attempt repeatedly failed

Otherwise, the E-mail is send as normal text message to the addressed DECT handset. The DECT handset user may response to this text message, which in turn the text message is forwarded to the original E-mail sender.

Notes

- You can define only one <MailBoxAccount />configuration. If the configuration file contains more than one configuration entries, only the last configuration entry is used.
- Incoming E-mail is converted to the UTF-8 character set if applicable.
- If an incoming E-mail cannot be delivered e.g. because the DECT handset cannot be reached, the original sender will get an error E-mail after a certain time.

SendmailAccount

This configuration file item is used to configure an e-mail account for sending messages. The OM IMA service will forward text messages received from DECT handsets to this E-mail account.

<SendmailAccount />

Attribute	Type/Values	Default	Description
auth	AuthNone, AuthPOP3, AuthSMTP	Mandatory	The mail is always sent with SMTP; Some SMTP servers require authentication with user name and password (“AuthSMTP” setting); Some SMTP servers require to be polled first (send-after-poll: “AuthPOP3” setting)
smtpServer	[IP or DNS]	Mandatory	Determines the SMTP server; Either IP address or DNS name
senderAddress	[String]	-	The E-mail address used as the sender for all outgoing E-mails
trySslFirst	true, false	false	If set to “true” the OM IMA service tries to use SSL for encryption; If that fails, the standard port is tried (optional encryption with StartTLS)
smtpPort	[Number]	0	The port number for SMTP; Use “0” for standard port
smtpSslPort	[Number]	0	The port number for SSL encrypted SMTP; Use “0” for standard port
smtpUser	[String]	-	“AuthSMTP” only: User name for SMTP
smtpPassword	[String]	-	“AuthSMTP” only: Password for SMTP

<SendmailAccount />

Attribute	Type/Values	Default	Description
mbPort	[Number]	0	“AuthPOP3” only: The port number for POP3; Use “0” for standard port
mbSslPort	[Number]	0	“AuthPOP3” only: The port number for SSL encrypted POP3; Use “0” for standard port
mbUser	[String]	-	“AuthPOP3” only: User name for the POP3 mailbox account
mbPassword	[String]	-	“AuthPOP3” only: Password for the POP3 mailbox account

RSS / feed

These configuration file items are used to configure one or more news sources which are then typically polled to deliver text messages to DECT handsets. You configure an RSS feed which is usually offered by a web site that publishes frequently updated content. The RSS feed is then polled on a regularly basis. If a new RSS entry appears, a message is sent to the DECT handsets which are attached to the service. The necessary configuration is splitted in two parts:

1. You define the RSS feed to poll. For example:

```
<RSS>
   <feed url="http://rss.cnn.com/rss/cnn_tech.rss" trigger="CNNtech"/>
</RSS>
```

2. You define a corresponding alarm scenario (see AlarmScenario / as starting on page 20) which is used to send a text message when a new RSS entry is detected. For example:

```
<AlarmScenario>
   <as alarmTriggerId="CNNtech" level="1"
      recipients="tel:1001;tel:1002" alarmMsg="CNN: %c"
      priority="PrioInfo" autoDelete="true" popUp="false" />
</AlarmScenario>
```

Only the <feed /> tag carries attributes that configure the RSS feed properties. Each single <feed /> tag needs to be enclosed by <RSS></RSS> tags.

<feed />

Attribute	Type/Values	Default	Description
url	[String]	Mandatory	The URL of the RSS feed; Typically http protocol and *.xml or *.rss file type
trigger	[String]	Mandatory	An ID string which identifies the alarm scenario used to send out received news; You need an <as /> tag with a matching alarmTriggerId attribute
refresh	[Number]	3600	Poll interval for the RSS feed

To prevent the RSS feed source from overloading the OM IMA service, only one new RSS entry is considered when the RSS feed is polled. During a poll operation, the ID and content of the newest RSS entry is compared against the values stored during the previous poll operation for this. If, for example, the RSS feed delivers a bulk update which marks several RSS entries as new, the next poll operation will only forward the newest entry as text message.

Tip: If you expect the RSS feed to update frequently, you should consider using a shorter **refresh** setting.

AlarmScenario / as

These configuration file items are used to configure one or more alarm scenarios. Each alarm scenario is triggered by a pre-defined signal. You can establish a tiered escalation system with up to three escalation levels. This can be used to trigger subsequent alarms if the original alarm is not confirmed by it's recipients as in the following example:

```
<AlarmScenario>
  <as alarmTriggerId="MANDOWN" level="1"
    recipients="tel:1001;tel:1002;tel:1003"
    requiredPosConfirmCount="1" confirmTimeout="30"
    priority="PrioAlarm" alarmMsg="%n (%R) MAN Down!">
      <alarmConfirm>ConfRead</alarmConfirm>
  </as>
</AlarmScenario>
```

```
<AlarmScenario>
  <as alarmTriggerId="MANDOWN" level="2"
    recipients="tel:*;mailto:manager@company.com"
    priority="PrioAlarm" alarmMsg="Unhandled: %n (%R) MAN Down!"/>
</AlarmScenario>
```

Only the <as /> tag carries attributes that configure the alarm scenario. Each single <as /> tag needs to be enclosed by <AlarmScenario></AlarmScenario> tags.

<as />

Attribute	Type/Values	Default	Description
alarmTriggerId	[String]	Mandatory	An ID value or a string with keywords that trigger the alarm; See section below: Details on alarmTriggerId Attribute
level	[Number]	Mandatory	The escalation level for the alarm scenario; Use “1” for the first level alarm scenario. Add alarm scenarios with higher escalation levels but an identical “alarmTriggerId” setting
recipients	[String]	Mandatory	A semicolon separated list of URIs that should receive the alarm message; Up to 10 recipients can be addressed; See section below: Details on recipients Attribute
alarmMsg	[String]	Mandatory	Text message template to be send to the recipients; See section below: Details on alarmMsg Attribute
<alarmConfirm>	XML tags	None	Expected recipient confirmation; See section below: Details on <alarmConfirm> tag sequence

<as />

Attribute	Type/Values	Default	Description
requiredPosConfirmCount	[Number]	0	Number of expected confirmations; Use “0” to disable alarm scenario escalation; Use “1” or above to escalate to the next alarm scenario level if less than defined confirmations are detected
confirmTimeout	[Number]	0	Time to wait until the alarm scenario escalates; Use “0” to disable alarm scenario escalation
priority	PrioInfo, PrioLow, PrioNormal, PrioHigh, PrioAlarm	PrioHigh	Priority setting for the text messages to be sent; For details, refer to Message Matrix starting on page 11
popUp	true, false	true	Set to “true” to display text message as pop-up; Set to “false” otherwise
autoDelete	true, false	false	Set to “true” to auto-delete the message from the DECT handset when it reaches the final state; Set to “false” otherwise
vCard	true, false	false	If set to “true”, the alarm message contains a vCard
postDialSeperator	[String] (arbitrary combination of “#” and “*”)	-	Treats post-dialled digits that are dialled after the configured alarm trigger FAC (Feature Access Code). The separator characters splits the post-dialled digits into calling party numbers

<as />

Attribute	Type/Values	Default	Description
callbackNumber	cb:[String] or tel:[String]	-	Callback number that is sent within the alarm message to the recipient; Enables the recipient to dial this number with the off-hook key; cb:[Number]: call back to this number, e.g. “cb:1234”; cb:#%1R: call back to first number extracted from post-dialled digits (“#%1R” - “#%9R”); cb:%R: call back to originator of alarm message if applicable (i.e. the originator has a phone number). Note: the “tel:” URI type is equivalent to “cb:”. Other URI types are not allowed.

The most versatile feature of an alarm scenario is the ability to escalate to the next alarm level if an alarm is not sufficiently confirmed by the alarm recipients. If you configure such a multi-level alarm scenario, you should bear in mind how a typical escalation scenario takes place:

1. The alarm is triggered, e.g. by a DECT handset user pressing the SOS button or similar. The OM IMA service sends a text message to the recipients as configured.
2. The OM IMA service now waits for confirmations from the alarm recipients.

Note

Alarm scenario messages of the previous alarm level or messages that received the required confirmations are deleted automatically.

Details on alarmTriggerId Attribute
The “alarmTriggerId” identifies the alarm scenario and also selects the source which triggers the alarm. The following alarm triggers are supported:

Alarm Trigger	Description
emailsubject:text	Matches a specific subject received via the OMM’s e-mail account (see MailBoxAccount starting on page 16). Note that the URI text may be terminated by an asterisk character to ignore trailing subject text. Thus, the “emailsubject:*” URI matches all e-mails.
SOS	SOS call from a DECT handset detected
MANDOWN	Man-down alarm from a DECT handset detected
DISTRESS_OPERATOR_TIMEOUT	No operator reaction on alarm condition detected by the locating server.
PAGEBYMENU	Paging with optional call back triggered by DECT handset menu command detected
CALLBACK	Callback by a DECT handset triggered by paging message detected
VCARD	Special VCARD alarm trigger (see vCard Support starting on page 13)
OMM-	OMM health state trigger: These start with “OMM-”, followed by “OK-”, “WARNING-”, or “ERROR-” and “SYNC”, “STANDBY”, “AUTODB”, “DOWNLOAD”, “PROTOCOL”, “BRANDING”, “ENCRYPTION”, or “LICENSE”. Example: “OMM-WARNING-SYNC”. This trigger supports a wildcard, e.g. “OMM-WARNING-*” matches all warnings. Also, a reason suffix is supported e.g. “-License hurt” makes up “OMM-WARNING-LICENSE-License hurt”.
[RSS-Trigger]	Trigger defined by trigger attribute of an RSS feed (see RSS / feed starting on page 19).

Details on recipients Attribute
The mandatory “recipients” attribute defines a semicolon separated list of URIs (see URI Syntax starting on page 13). You can mix different URI types, e.g. “mailto:admin@domain.com;tel:1001” is valid. In the “recipients” context, handling of post-dialled digits is supported also. For example, “tel:#%1R” sends the alarm

message to the first number extracted from the post-dialled digits (valid from #%1 to #%9).

Details on alarmMsg Attribute
The mandatory “alarmMsg” attribute defines a template for the text message. The template includes place holders which are replaced before the message is sent to all recipients. The following place holders are supported:

Place holder	Replacement by
%s	Sender (URI), e.g. “tel:1001” if SOS button pressed on this phone
%r	Receiver (URI), e.g. “tel:30” if SOS button called this number
%t	Sending time (24 hour format, HH:MM:SS)
%T	Sending time (12 hour format, HH:MM:SS am/pm)
%d	Sending date (EU format, DD.MM.YYYY)
%D	Sending date (US format, YY-MM-DD)
%p	DECT portable part number (ppn), e.g. “1” for first entry in list
%n	DECT portable part user name
%R	DECT portable part calling party number (CPN)
%#1n	Name of the number extracted from post dialled-digits (#1 - #9)
%#1R	Number extracted from post-dialled digits (#1 - #9)
%c	Message content - from source that triggered the alarm
%i	Alarm trigger ID, e.g. “sos”
%l	Previous alarm escalation level
%u	Confirmations received (from previous escalation level)
%x	Rejects received (from previous escalation level)
%e	Confirmations expected (of previous escalation level)
%o	Escalation time-out (of previous escalation level)

Details on <alarmConfirm> tag sequence
It is possible to attach one or more alarm confirmations to the alarm scenario. These can be added to an <as> tag as enclosed tag sequence as shown in the following example:

```
<AlarmScenario>
   <as alarmTriggerId="SOS" level="1" recipients="tel:1001">
      <alarmConfirm>ConfRead</alarmConfirm>
      </as>
</AlarmScenario>
```

You can add the following alarm confirmations:

- <alarmConfirm>ConfRead</alarmConfirm>
- <alarmConfirm>ConfOrder</alarmConfirm>
- <alarmConfirm>ConfCompletion</alarmConfirm>

Note, that the alarm confirmations are ignored, if you broadcast all DECT handsets by adding the “tel:*” URI to the “recipients” attribute.

Debugging the OM IMA Setup

If you develop a complex OM IMA configuration, you will need to create the configuration in several iterative steps. For example, you start with a simple configuration and add new features step by step. During this iterative development process, you need to repeatedly restart the OM IMA service, watch the configuration file parsing and verify the message processing triggered by the configuration.

To support the OM IMA configuration development, the RFP and the OMM running on the RFP offer a debugging console which can be used during the OM IMA configuration development cycle. For example, you can start and stop the OM IMA service, re-load the configuration file, and watch the debugging console output.

CAUTION! Only use the console commands described here! Other available commands may destroy you configuration leaving you with an unusable OMM-SIP system!

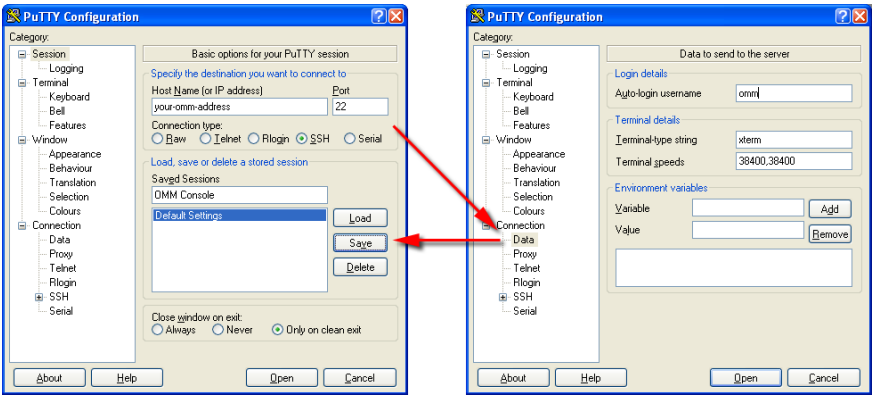
OMM Console Login

The following description applies, if you run the OMM on an RFP.

Please note: For a PC-based OMM, log in to the Linux GUI and open a terminal window. Enter the “su” command to elevate to administrative rights. Start the OMM console with the “/usr/sbin/ommconsole” command.

For using the RFP/OMM console, you need a secure shell (SSH) program such as the OpenSSH client (Linux) or the PuTTY SSH client (Open Source, Windows). Install the SSH client software on your PC and start an SSH session as described for Windows/PuTTY in the following steps. Under Linux, start a terminal program and execute the “ssh omm@your-omm-address” command.

1. Start the “PuTTY” SSH client program. The **PuTTY Configuration** dialogue opens. In the **Host Name** input field, enter the IP address or DNS-Name of the RFP running the OMM. Do not change the default **Port** (22) and **Connection type** (SSH) settings.

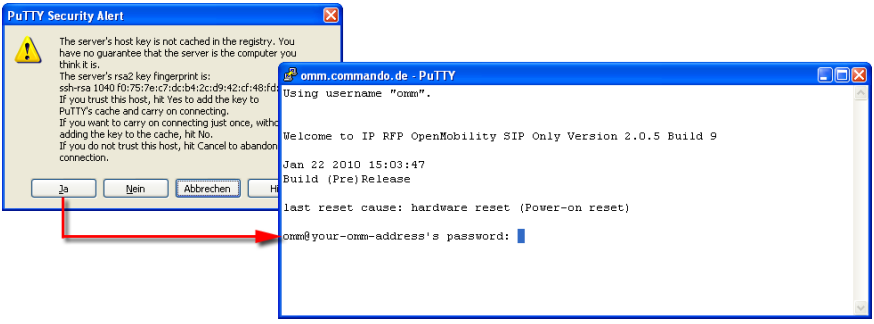


Creating an SSH session (Windows, PuTTY)

Switch to the **Connection/Data** category available in the navigation tree on the left side of the **PuTTY Configuration** dialogue. In the **Auto-login username** input field, enter the user name that is configured at the OMM's web console for the "Full access" account type. This is "omm" by default.

Switch back to the **Session** category of the **PuTTY Configuration** dialog. Enter a descriptive name in the **Saved Sessions** input field. Click the **Save** button.

2. To open a saved session, select the desired entry in the **Saved Sessions** list of the **PuTTY Configuration** dialog. Click the **Open** button to start the session. For any initial SSH session, an alert dialog informs you about the SSH server's key fingerprint. Proceed by clicking the **Yes** button.



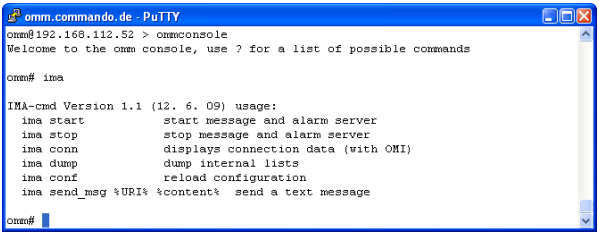
Opening an SSH session (Windows, PuTTY)

At the password prompt, enter the OMM's the password for the "Full access" account. Press the [Enter] key to proceed.

The RFP's console prompt is displayed, offering several commands ready to be executed. For example, you can type in the "help" command and confirm with the [Enter] key. This will display a list of available commands.

3. Enter the "setconsole" command. This will redirect the OMM's syslog messages to the current SSH session. For example, you will see a syslog message if you log in to the Web console of the OMM concurrently. Note, that the syslog message redirection is automatically cancelled if you close the SSH session.

4. Enter the "ommconsole" command. This will call up the separate command line of the currently running OMM service program. The command prompt changes to "omm" and a different set of commands is available.



Displaying the OMM console (help output of IMA command)

5. Enter the "ima" command to display a list of available options. Refer to the OMM Console: IMA Command Reference table below.

6. To end the OMM console, enter the "exit" command. To end the RFP console and close the SSH session enter a second "exit" command. Alternatively, close the PuTTY terminal window.

Using the OMM Console

The OMM console accepts only a single internal telnet connection. Therefore, you cannot open another SSH session to display a second OMM console. If you do not enter a command while the OMM console is opened, the internal telnet session is closed after some time. This will end the OMM console automatically and in turn the RFP's console prompt is displayed. For this reason, you may need to re-enter the "ommconsole" command after a pause.

During a typical development cycle you proceed as follows:

1. Change the configuration file located on your (FTP/HTTP/TFTP) server.
2. Start the SSH session towards the RFP. Enter the "setconsole" command.
3. Enter the "ommconsole" and "ima load" commands. If no error message is displayed, the configuration file has no syntax errors and is accepted.
4. Test the desired message/alarm functions. Recycle with Step 1 as needed.
5. When finished, enter the "exit" command twice or close the SSH session.

Tip: In PuTTY, you can switch to a more readable black-on-white display. In the **PuTTY Configuration** dialog, load the desired session configuration. Navigate to the **Window/Colours** category. Activate the **Use system colours** switch. Save the session configuration.

OMM Console Reference

The following table gives a brief description of the IMA commands available in the OMM console.

OMM Console: IMA Command Reference

Command	Purpose
ima start	Starts the OM IMA service program this is currently not running. The OM IMA configuration file is loaded and all configured messaging functions are started.
ima stop	Ends the running OM IMA service program, thereby stopping all messaging functions. The internal network connection between the OM IMA service program and the OMM is closed also.
ima conn	Displays the network connection status of the OM IMA service program. Display the next prompt line by pressing the [Return] key.
ima dump	Displays the status of messages and alarms currently in the sending queue. Optionally, the registered backtrace subscriptions are displayed also. You can use this command to check for and view undelivered messages. Display the next prompt line by pressing the [Return] key.
ima conf	Reloads the OM IMA configuration from the server address which you configured in the OMM's web console. Note, an unchanged OM IMA configuration file is ignored, this only a changed OM IMA configuration file triggers the reconfiguration of the OM IMA service program.
ima send_msg	Sends a text message directly to the addressed device. You need to add the receivers address (URI) and the message content. Example: ima send_msg tel:1001 this-is-a-message The command accepts any valid URI and a single word without spaces as message content. The message word is converted from ISO-8859-1 (Windows ANSI), so if your SSH client uses for example UTF-8 all characters expect ASCII-32 to ASCII-127 will show up as double characters on the receiving DECT portable part.

Appendix

Abbreviations

OM	OpenMobility
OM AXI	OM Application XML Interface
OMC	OM Configurator
OM IMA	OM Integrated Messaging & Alerting service
OML	OM Locating
OMM	OpenMobility Manager
OMP	OM Management Portal
PP	Portable Part
RFP	Radio Fixed Part
SIP	Session Initiation Protocol
URL	Uniform Resource Locator

Trademarks

Microsoft®, Windows®, Windows XP®, Windows Vista®, and Windows 7® are registered trademark of Microsoft Corporation.

Linux® is a registered trademark of Linus Torvalds.

Firefox®, Mozilla® are registered trademark of the Mozilla Foundation.

Oracle™ and Java™ are a registered trademarks of Oracle Corporation.

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

Index

A
Alarm Trigger 24
AlarmScenario / as 20
Architecture 1

B
Basic Concepts 10

C
Certificate 5
Confirmation 2, 10
Console 27

D
Debugging 27
DECT network 1
Development cycle 30

E
E-Mail 2
Example (first) 8

F
ftp 8

H
http 8
HTTPS 5

I
Idle Box 10
IMA 1
IMA commands 31
Info Message 10

M
MailBoxAccount 16
ManDown 2
Messaging solution 1

O
OMM 1
ommconsole (command) 29

P
Password 5
Place holder 25
Pop-up 2
Priority 2

R
Reference 16
RFP 1
RSS / feed 19
RSS feed 2

S
SendmailAccount 18
setconsole (command) 29
Size of messages 2
SOS 2
SSH 27
Syntax 15

T
tftp 8
TriggerId 24

U
URI 13
URL 6, 8
User name 5
UTF-8 15

V
vCard 13

W
Warning sign (red) 8
Web service 5

X

XML interface 1
XML syntax 15

Copyright 2011 www.aastra.com
All rights reserved
As of 09.03.2011 • Subject to changes