



Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Aastra SIP-DECT with Avaya Aura® Communication Manager R6.3 and Avaya Aura® Session Manager R6.3 – Issue 1.0

Abstract

These Application Notes describe the configuration steps for provisioning Aastra SIP-DECT to interoperate with Avaya Aura® Communication Manager and Avaya Aura® Session Manager.

Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

1. Introduction

These Application Notes describe the configuration steps for provisioning Aastra SIP-DECT to interoperate with Avaya Aura® Communication Manager R6.3 and Avaya Aura® Session Manager R6.3. The Aastra SIP-DECT solution provides a DECT system that extends an existing SIP communications system (PABX), thus operating DECT handsets as SIP clients. The SIP-DECT solution includes up to 4,096 DECT base stations (RFP, “Radio Fixed Parts”) that form a DECT radio system. The RFPs and the SIP communications system are interconnected via an Ethernet/IP network that is used to transport the SIP/VoIP data streams as well as management data.

Within the DECT radio system, a single entity exists that controls all RFPs and manages communication streams, the Open Mobility Manager (OMM). For smaller DECT systems (1 – 256 RFPs), the OMM can be hosted on an RFP. A larger DECT system (256 – 4,096 RFPs) requires hosting the OMM on a Linux PC server system.

2. General Test Approach and Test Results

Each Aastra Open Mobility Manager (OMM) must be configured as a SIP Entity in Session Manager and the Aastra SIP-DECT handsets are configured as SIP users on Communication Manager as Avaya 9620 SIP endpoints. The SIP-DECT handsets are configured to register with Session Manager using SIP and are also subscribed to the RFP using DECT. The SIP-DECT handsets then behave as third-party sip extensions on Communication Manager, they are able to make/receive internal calls and have voicemail and other telephony facilities available on Communication Manager.

The interoperability compliance testing evaluates the ability of Aastra SIP-DECT handsets to make and receive calls to and from Avaya H.323 and SIP deskphones. Avaya Aura® Messaging (messaging) was used to allow users leave voicemail messages and to demonstrate Message Waiting Indication was working on the Aastra SIP-DECT handsets.

DevConnect Compliance Testing is conducted jointly by Avaya and DevConnect members. The jointly-defined test plan focuses on exercising APIs and/or standards-based interfaces pertinent to the interoperability of the tested products and their functionalities. DevConnect Compliance Testing is not intended to substitute full product performance or feature testing performed by DevConnect members, nor is it to be construed as an endorsement by Avaya of the suitability or completeness of a DevConnect member’s solution.

2.1. Interoperability Compliance Testing

The compliance testing included the test scenarios shown below. Note that when applicable, all tests were performed with Avaya SIP deskphones, Avaya H.323 deskphones, Aastra SIP-DECT handsets and PSTN endpoints.

- Registration
- Protocol Access
- Basic Calls
- Hold and Retrieve
- Attended and Blind Transfer
- Call Forwarding Unconditional, No Reply and Busy
- Call Waiting
- Call Park/Pickup
- EC500
- Do Not Disturb
- Calling Line Name/Identification
- Codec Support
- DTMF Support
- Message Waiting Indication

2.2. Test Results

The following observations were noted during testing.

1. TLS negotiation between the Aastra SIP-DECT handsets and Session Manager was not tested; all compliance testing was carried out using TCP and/or UDP as the transport protocol.
2. A SIP Entity and a SIP Entity Link must be added for each Aastra Open Mobility Manager (OMM) as per **Section 6.4**.

2.3. Support

Support from Avaya is available by visiting the website <http://support.avaya.com> and a list of product documentation can be found in **Section 11** of these Application Notes. Technical support for the Aastra SIP-DECT can be obtained as follows.

- Web: www.aastra.com (please refer to the local country web sites which offer a support section)

3. Reference Configuration

Figure 1 shows the network topology during compliance testing. The Aastra SIP-DECT OMM is placed on the LAN. The DECT handsets register with Session Manager in order to be able to make/receive calls to and from the Avaya H.323 and SIP deskphones on Communication Manager.

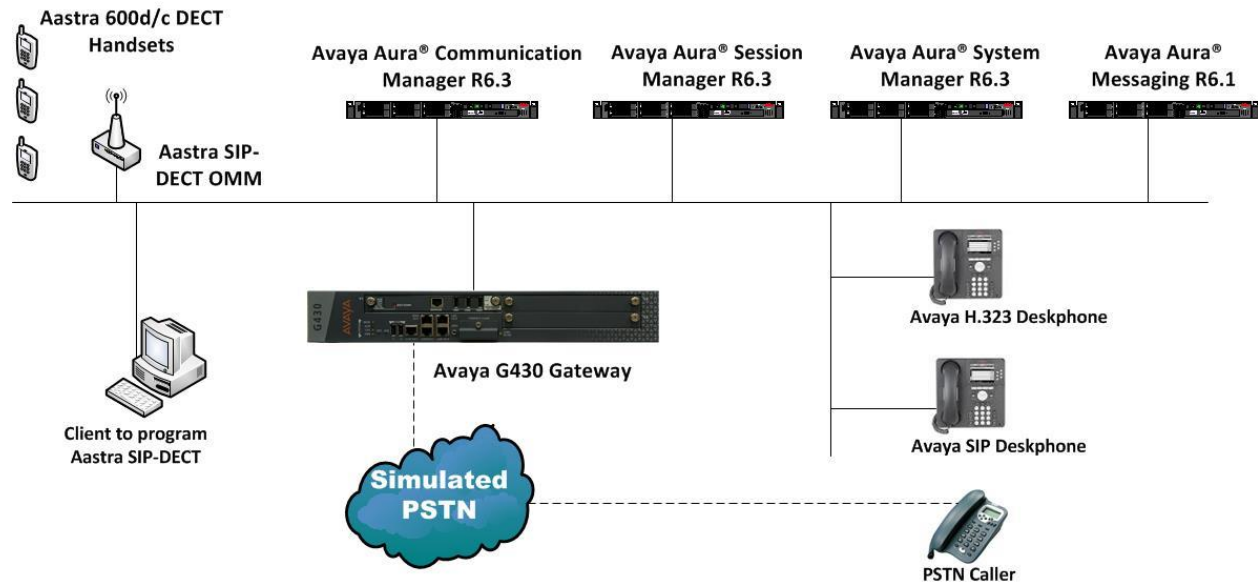


Figure 1: Network Solution of Aastra SIP-DECT Handsets with Avaya Aura® Communication Manager R6.3 and Avaya Aura® Session Manager R6.3

4. Equipment and Software Validated

The following equipment and software was used for the compliance test.

Equipment/Software	Version/Release
Avaya Aura® System Manager running on an Avaya virtual platform	R6.3 SP3 Build 6.3.0.8.5682-6.3.8.1814 Software Update Revision 6.3.3.5.1719
Avaya Aura® Communication Manager running on an Avaya virtual platform	R6.3 SP1 R016x.03.0.124.0
Avaya Aura® Session Manager running on an Avaya virtual platform	R6.3 SP3 6.3.3.0.633004
Avaya Aura® Messaging running on S8800 Server	R6.1
Avaya 96xx Series Deskphone	96xx H.323 Release 3.1 SP2 96xx SIP Release 2.6 SP3
Aastra SIP-DECT OMM	5.0RC9
Aastra 600d/c DECT Handsets	5.5RC13
Aastra RFP 35/36/37/43	5.0RC9

5. Configure Avaya Aura® Communication Manager

It is assumed that a fully functioning Communication Manager is in place with the necessary licensing with a SIP Trunk in place to Session Manager. For further information on the configuration of Communication Manager please see **Section 11** of these Application Notes. The following sections go through the following.

- Dial Plan Analysis
- Feature Access Codes
- IP Interfaces
- Network Region
- IP Codec
- Coverage Path and Hunt Group for voicemail

5.1. Configure Dial Plan Analysis

Use the **change dialplan analysis** command to configure the dial plan using the parameters shown below. Extension numbers (**ext**) are those beginning with **2, 3, 4** and **5**. Feature Access Codes (**fac**) use digits **8** and **9** or **#**.

change dialplan analysis			DIAL PLAN ANALYSIS TABLE						Page 1 of 12	
			Location: all			Percent Full: 1				
Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type		
2	4	ext								
3	4	ext								
4	4	ext								
5	4	ext								
8	1	fac								
9	1	fac								
*	3	dac								
#	3	fac								

5.2. Configure Feature Access Codes

Use the **change feature-access-codes** command to configure access codes which can be entered from Aastra handsets to initiate Communication Manager call features. These access codes must be compatible with the dial plan described in **Section 5.1**. The following access codes need to be setup.

- **Answer Back Access Code** : **#22**
- **Auto Alternate Routing (AAR) Access Code** : **8**
- **Auto Route Selection (ARS) - Access Code 1** : **9**
- **Call Park Access Code** : **#11**

change feature-access-codes		Page 1 of 10
FEATURE ACCESS CODE (FAC)		
Abbreviated Dialing List1 Access Code:		
Abbreviated Dialing List2 Access Code:		
Abbreviated Dialing List3 Access Code:		
Abbreviated Dial - Prgm Group List Access Code:		
Announcement Access Code:		
Answer Back Access Code:	#22	
Attendant Access Code:		
Auto Alternate Routing (AAR) Access Code:	8	
Auto Route Selection (ARS) - Access Code 1:	9	Access Code 2:
Automatic Callback Activation:		Deactivation:
Call Forwarding Activation Busy/DA:	All:	Deactivation:
Call Forwarding Enhanced Status:	Act:	Deactivation:
Call Park Access Code:	#11	
Call Pickup Access Code:		
CAS Remote Hold/Answer Hold-Unhold Access Code:		
CDR Account Code Access Code:		
Change COR Access Code:		
Change Coverage Access Code:		
Conditional Call Extend Activation:		Deactivation:
Contact Closure Open Code:		Close Code:
CDR Account Code Access Code:		
Change COR Access Code:		
Change Coverage Access Code:		
Conditional Call Extend Activation:		Deactivation:
Contact Closure Open Code:		Close Code:

5.3. Configure IP Interfaces

Shown below is an example of the nodes names used in the compliance testing. Use the **change node-names ip** command to configure the IP address of Session Manager. **SM100** is the **Name** used for Session Manager and **10.10.40.34** is the **IP Address**.

change node-names ip		Page 1 of 2
IP NODE NAMES		
Name	IP Address	
SM100	10.10.40.34	
default	0.0.0.0	
g430	10.10.40.15	
procr	10.10.40.13	
procr6	::	

5.4. Configure Network Region

Use the **change ip-network-region x** (where x is the network region to be configured) command to assign an appropriate domain name to be used by Communication Manager, in the example below **devconnect.local** is used. Note this domain is also configured in **Section 6.2** of these Application Notes.

```
change ip-network-region 1                                     Page 1 of 20
                                                                IP NETWORK REGION
    Region: 1
    Location: 1          Authoritative Domain: devconnect.local
    Name: default NR
MEDIA PARAMETERS                                           Intra-region IP-IP Direct Audio: yes
    Codec Set: 1                                           Inter-region IP-IP Direct Audio: yes
    UDP Port Min: 2048                                     IP Audio Hairpinning? y
    UDP Port Max: 3329
DIFFSERV/TOS PARAMETERS
    Call Control PHB Value: 46
    Audio PHB Value: 46
    Video PHB Value: 26
802.1P/Q PARAMETERS
    Call Control 802.1p Priority: 6
    Audio 802.1p Priority: 6
    Video 802.1p Priority: 5      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                         RSVP Enabled? n
    H.323 Link Bounce Recovery? y
    Idle Traffic Interval (sec): 20
    Keep-Alive Interval (sec): 5
    Keep-Alive Count: 5
```

5.5. Configure IP-Codec

Use the **change ip-codec-set x** (where x is the ip-codec set used) command to designate a codec set compatible with the Aastra SIP-DECT handsets, which support both **G.711A** and **G.729A**.

```
change change ip-codec-set 1                                   Page 1 of 2
                                                                IP Codec Set

    Codec Set: 1

    Audio      Silence      Frames      Packet
    Codec      Suppression   Per Pkt    Size(ms)
1: G.711A      n            2          20
2: G.729A      n            2          20
```


5.6. Configuration of Coverage Path and Hunt Group for voicemail

The coverage path setup used for compliance testing is illustrated below. Note the following:

Don't Answer is set to **y** The coverage path will be used in the event the phone set is not answered.

Number of Rings is set to **4** The coverage path will be used after 4 rings.

Point 1: is set to **h59** Hunt Group 59 is utilised by this coverage path.

```
display coverage path 1

                                COVERAGE PATH

                                Coverage Path Number: 1
                                Cvg Enabled for VDN Route-To Party? n      Hunt after Coverage? n
                                Next Path Number:                        Linkage

COVERAGE CRITERIA
  Station/Group Status      Inside Call      Outside Call
    Active?                  n                n
    Busy?                    y                y
    Don't Answer?            y                y      Number of Rings: 4
    All?                     n                n
  DND/SAC/Goto Cover?       y                y
  Holiday Coverage?         n                n

COVERAGE POINTS
  Terminate to Coverage Pts. with Bridged Appearances? n
  Point1: h59               Rng:      Point2:
  Point3:                   Point4:
  Point5:                   Point6:
```

The hunt group used for compliance testing is shown below. Note on **Page 1** the **Group Extension** is **5999** which is the voicemail number for Messaging and on **Page 2 Message Center** is set to **sip-adjunct**.

```
display hunt-group 59                                     Page 1 of 60

                                HUNT GROUP

                                Group Number: 59                      ACD? n
                                Group Name: Voicemail                   Queue? n
                                Group Extension: 5999                  Vector? n
                                Group Type: ucd-mia                    Coverage Path:
                                TN: 1                                  Night Service Destination:
                                COR: 1                                MM Early Answer? n
                                Security Code:                        Local Agent Preference? n
                                ISDN/SIP Caller Display: mbr-name
```

```
display hunt-group 59                                     Page 2 of 60

                                HUNT GROUP

                                Message Center: sip-adjunct

Voice Mail Number      Voice Mail Handle      Routing Digits
(e.g., AAR/ARS Access Code)
5999                    5999                    8
```

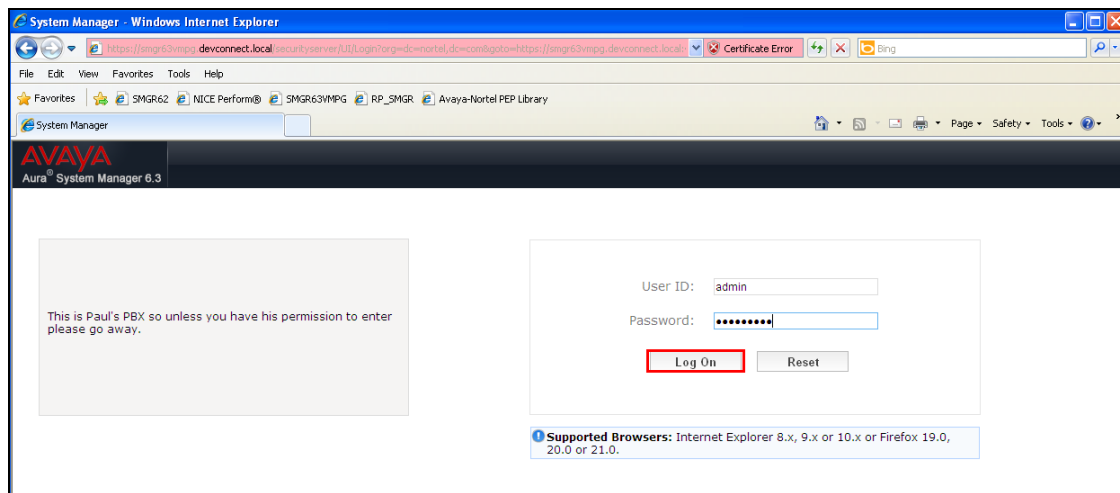
6. Configure Avaya Aura® Session Manager

This section provides the procedures for configuring Session Manager. Session Manager is configured via System Manager. The procedures include the following areas:

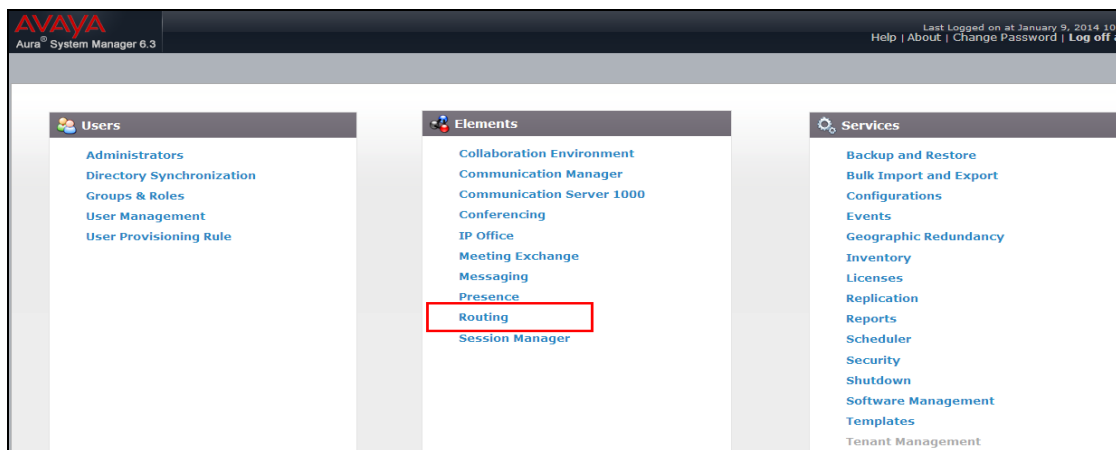
- Log in to Avaya Aura® Session Manager
- Administer SIP Domain
- Administer Location
- Administer SIP Entities
- Administer Entity Link
- Adding Aastra SIP Users

6.1. Log in to Avaya Aura® System Manager

Access the System Manager using a Web Browser by entering **http://<FQDN>/SMGR**, where **<FQDN>** is the fully qualified domain name of System Manager or **http://<IP Address>/SMGR**. Log in using appropriate credentials.

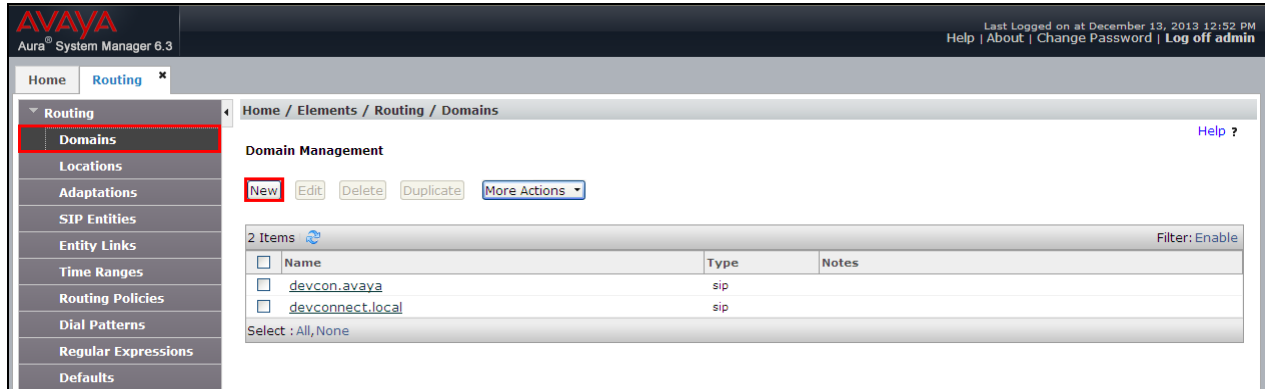


Once logged in click on **Routing** as highlighted.

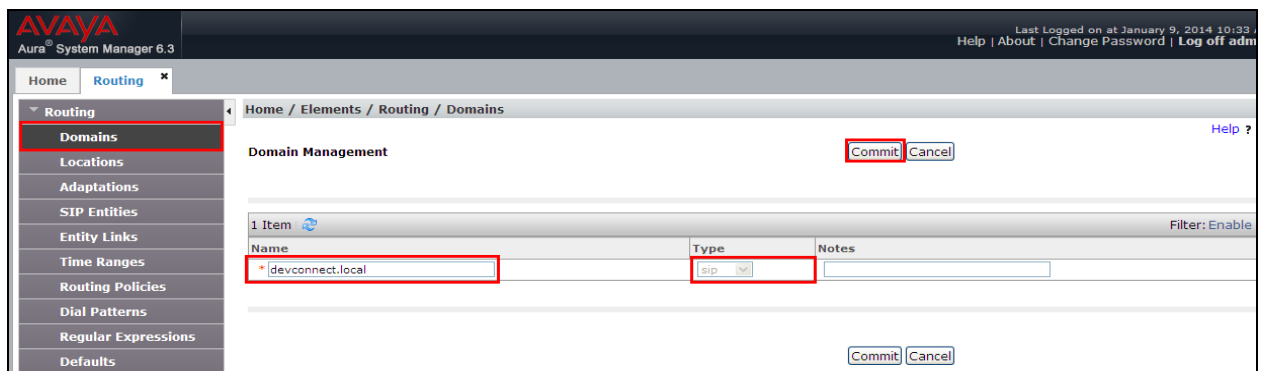


6.2. Administer SIP Domain

Click on **Domains** in the left window. If there is not a domain already configured click on **New** highlighted below.

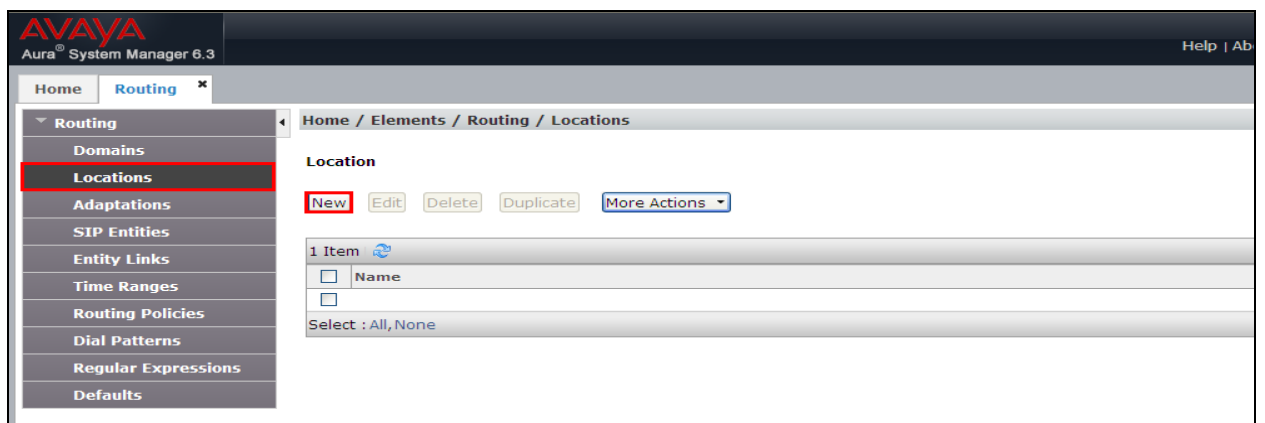


Enter the name of the domain note this was referenced in **Section 5.4**. The **Type** should be **sip**. Click on **Commit** once done.



6.3. Configure Location

Select **Locations** from the left window and select **New** from the main window.



Enter a suitable name for the location and scroll down to the bottom of the page and enter the IP addresses associated with the location, in this case there are two ranges **10.10.40.x** and **192.168.50.x**, then click on **Add**. Once completed, click on **Commit** to continue.

AVAYA
Aura® System Manager 6.3

Home / Elements / Routing / Locations

Location Details Commit Cancel

General

* Name: DevConnectPG63

Notes:

Dial Plan Transparency in Survivable Mode

Enabled: ☐

Listed Directory Number:

Associated CM SIP Entity:

* Minimum Multimedia Bandwidth: 64 Kbit/Sec

* Default Audio Bandwidth: 80 Kbit/sec

Alarm Threshold

Overall Alarm Threshold: 80 %

Multimedia Alarm Threshold: 80 %

* Latency before Overall Alarm Trigger: 5 Minutes

* Latency before Multimedia Alarm Trigger: 5 Minutes

Location Pattern

Add Remove

2 Items

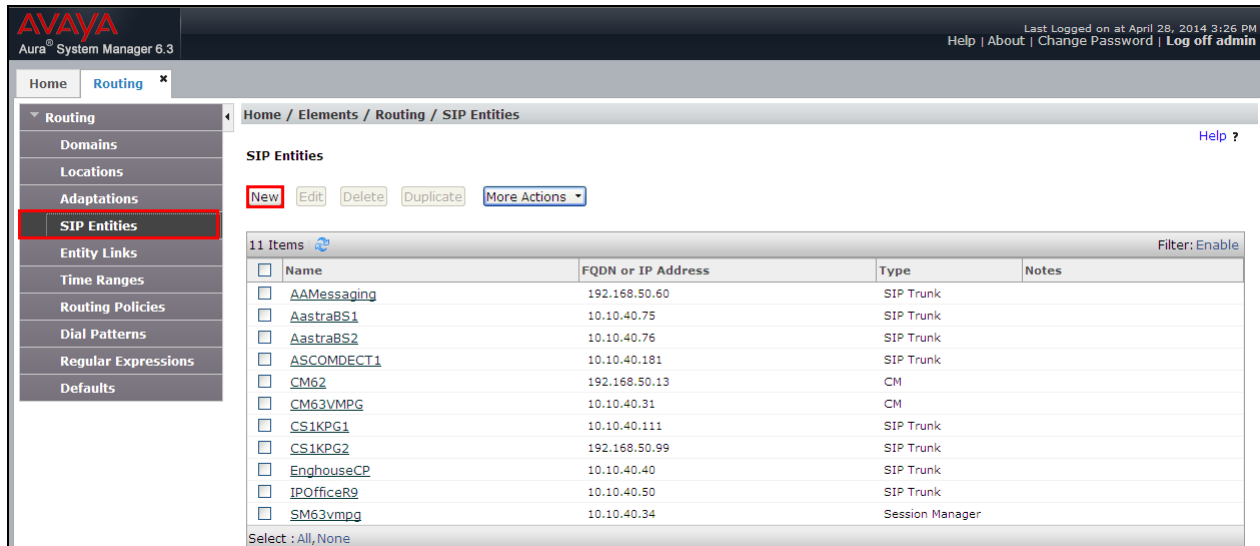
<input type="checkbox"/>	IP Address Pattern	Notes
<input checked="" type="checkbox"/>	* 10.10.40.*	
<input checked="" type="checkbox"/>	* 192.168.50.*	

Select : All, None

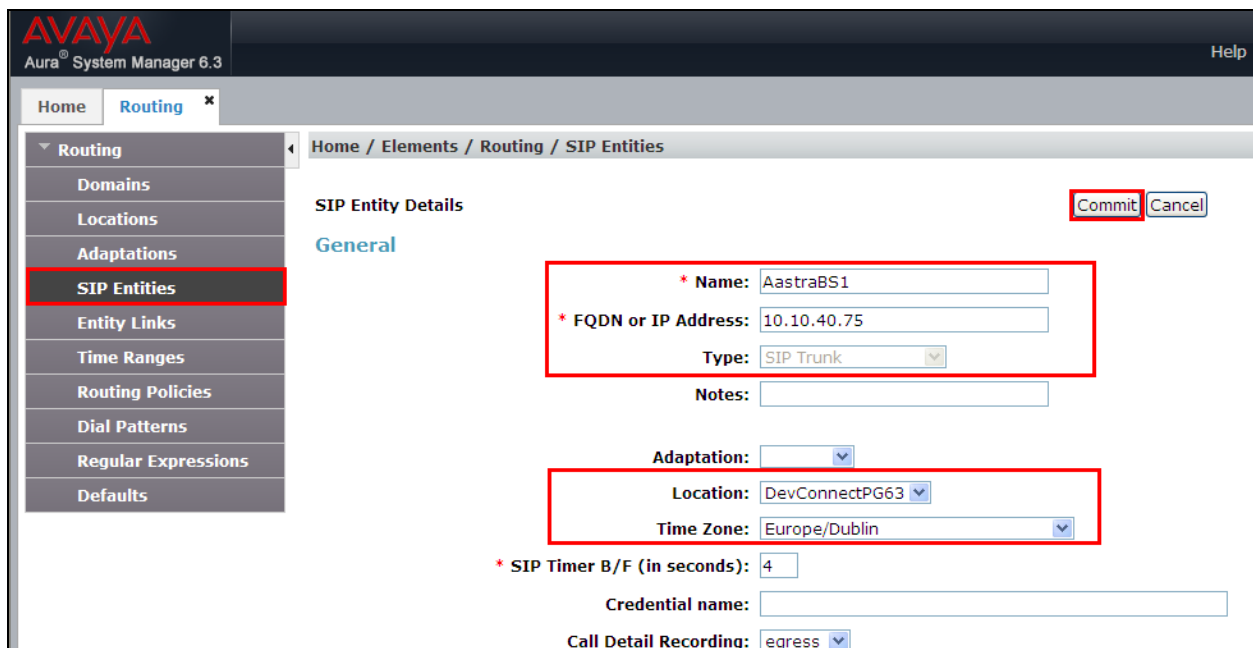
Commit Cancel

6.4. Configure SIP Entities for Aastra Open Mobility Manager

To create a new SIP Entity, select **SIP Entities** in the left window and click on **New** in the main window.



Enter a suitable **Name** and the **IP Address** of the Aastra Open Mobility Manager (OMM). A SIP Entity must be created for each Aastra OMM present.



6.5. Administer Entity Link

Select **Entity Links** from the left window and select **New** from the right window in order to add the new Aastra Entity Link.

Note: A SIP Entity and Entity link are required for all Aastra OMM's.

The screenshot shows the Avaya Aura System Manager 6.3 interface. The left sidebar has a menu with 'Entity Links' highlighted. The main area displays the 'Entity Links' page with a 'New' button and a table of existing links. The table has 10 items and the following columns: Name, SIP Entity 1, Protocol, Port, SIP Entity 2, DNS Override, Port, Connection Policy, Deny New Service, and Notes.

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	DNS Override	Port	Connection Policy	Deny New Service	Notes
<input type="checkbox"/> AAMessaging	SM63vmppg	TCP	5060	AAMessaging	<input type="checkbox"/>	5060	trusted	<input type="checkbox"/>	
<input type="checkbox"/> Aastra1_UDP	SM63vmppg	UDP	5060	AastraBS1	<input type="checkbox"/>	5060	trusted	<input type="checkbox"/>	
<input type="checkbox"/> Aastra2_UDP	SM63vmppg	UDP	5060	AastraBS2	<input type="checkbox"/>	5060	trusted	<input type="checkbox"/>	
<input type="checkbox"/> ASCOMDECT1	SM63vmppg	TCP	5060	ASCOMDECT1	<input type="checkbox"/>	5060	trusted	<input type="checkbox"/>	

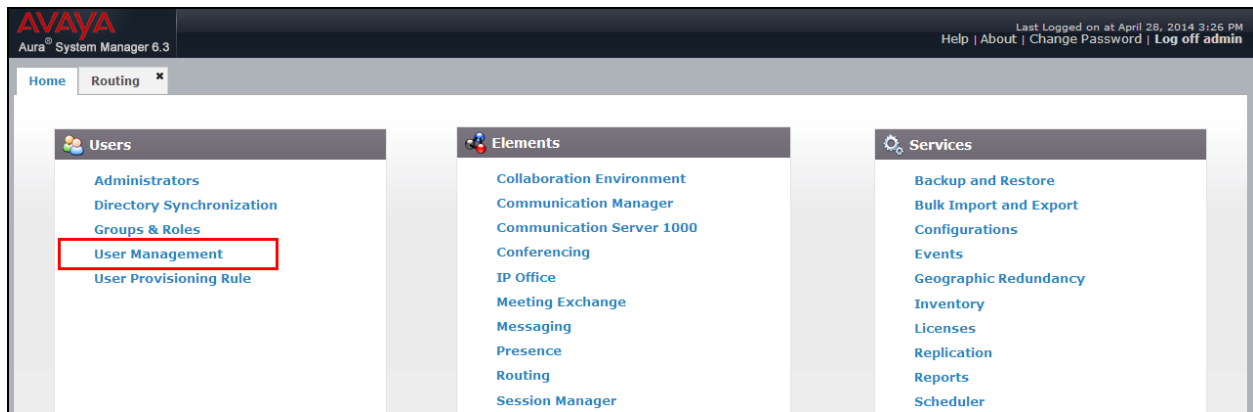
Note that Aastra supports both **UDP** and **TCP** as the transport protocol so ensure that whichever is chosen the same is done in **Section 8.2**. **5060** is entered for the **Port**. Click on **Commit** once completed.

The screenshot shows the 'Entity Links' page in the Avaya Aura System Manager 6.3 interface. The 'New' button from the previous screenshot is now a form. The form has a 'Commit' button and a 'Cancel' button. The table below the form shows the details of the new entity link being created. The table has 1 item and the following columns: Name, SIP Entity 1, Protocol, Port, SIP Entity 2, DNS Override, Port, Connection Policy, Deny New Service, and Notes.

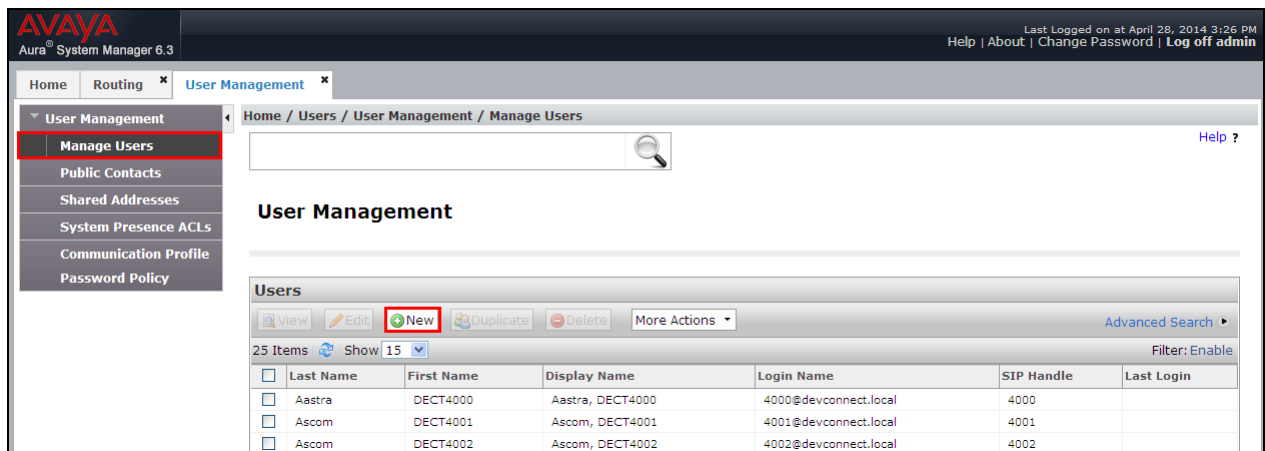
Name	SIP Entity 1	Protocol	Port	SIP Entity 2	DNS Override	Port	Connection Policy	Deny New Service	Notes
<input type="checkbox"/> *Aastra1_UDP	*SM63vmppg	UDP	*5060	*AastraBS1	<input type="checkbox"/>	*5060	trusted	<input type="checkbox"/>	

6.6. Adding Aastra SIP Users

From the home page click on **User Management** highlighted below.



Click on **New**, highlighted below to add a new SIP user.



Under the **Identity** tab fill in the user's **Last Name** and **First Name** as shown below. Enter the **Login Name** and ensure **Authentication Type** is set to **Basic** and enter a suitable **Password**.

The screenshot shows the 'User Profile Edit' page for user '4000@devconnect.local'. The left sidebar has 'Manage Users' selected. The main content area has tabs for 'Identity', 'Communication Profile', 'Membership', and 'Contacts'. The 'Identity' tab is active and contains the following fields:

- User Provisioning Rule:** A dropdown menu.
- Identity:**
 - Last Name:** Aastra
 - Last Name (Latin Translation):** Aastra
 - First Name:** DECT4000
 - First Name (Latin Translation):** DECT4000
 - Middle Name:** (empty)
 - Description:** (empty)
 - Update Time:** September 10, 2013 10:00
 - Login Name:** 4000@devconnect.local
 - Authentication Type:** Basic

Buttons at the bottom include 'Change Password' and 'New Password'.

Under the **Communication Profile** tab enter a suitable **Communication Profile Password** and click on **Done** when added, note that this password is required when configuring the Aastra handset in **Section 8.3**. Click on **New** to add a new **Communication Address**.

The screenshot shows the 'User Profile Edit' page for user '4000@devconnect.local'. The left sidebar has 'Manage Users' selected. The main content area has tabs for 'Identity', 'Communication Profile', 'Membership', and 'Contacts'. The 'Communication Profile' tab is active and contains the following fields:

- Communication Profile:**
 - Communication Profile Password:** (empty)
 - Confirm Password:** (empty)

Buttons at the bottom include 'New', 'Delete', 'Done', and 'Cancel'. Below these buttons is a table for 'Communication Address' with columns for 'Type', 'Handle', and 'Domain'.

Enter the extension number and the domain for the **Fully Qualified Address** and click on **Add** once finished.

Communication Address ▼

New Edit Delete

Type	Handle	Domain
Avaya SIP	4000	devconnect.local

Select : All, None

Type: Avaya SIP ▼

* Fully Qualified Address: 4000 @ devconnect.local ▼

Add Cancel

Ensure **Session Manager Profile** is checked and enter the **Primary Session Manager** details, enter the **Origination Application Sequence** and the **Termination Application Sequence** and the **Home Location** as highlighted below.

☒ **Session Manager Profile** ▼

SIP Registration

* Primary Session Manager SM63vmpg ▼

Primary	Secondary	Maximum
24	0	24

Secondary Session Manager (None) ▼

Survivability Server (None) ▼

Max. Simultaneous Devices 1 ▼

Block New Registration When Maximum Registrations Active? ☐

Application Sequences

Origination Sequence CM63AppSEQ ▼

Termination Sequence CM63AppSEQ ▼

Call Routing Settings

* Home Location DevConnectPG63 ▼

Conference Factory Set (None) ▼

Ensure that **CM Endpoint Profile** is selected and choose the **9620SIP_DEFAULT_CM_6_3** as the **Template** and ensure **Port** is set to **IP**. Click **Endpoint Editor** to configure the buttons and features for that handset on Communication Manager.

☒ **CM Endpoint Profile**

* **System** CM63VMPG

* **Profile Type** Endpoint

Use Existing Endpoints ☐

* **Extension** 4000 **Endpoint Editor**

Template 9620SIP_DEFAULT_CM_6_3

Set Type 9620SIP

Security Code

Port IP

Voice Mail Number

Preferred Handle (None)

Enhanced Callr-Info display for 1-line phones ☐

Delete Endpoint on Unassign of Endpoint from User or on Delete User ☒

Override Endpoint Name ☒

Under the **General Options** tab ensure that **Coverage Path 1** is set to that configured in **Section 5.6**. Also ensure that **Message Lamp Ext.** is showing the correct extension number.

General Options (G) * Feature Options (F) Site Data (S) Abbreviated Call Dialing (A) Enhanced Call Fwd (E)

Button Assignment (B) Group Membership (M)

* **Class of Restriction (COR)** 1

* **Emergency Location Ext** 4000

* **Tenant Number** 1

* **SIP Trunk** 1

Coverage Path 1 1

Lock Message ☐

Multibyte Language Not Applicable

* **Class Of Service (COS)** 1

* **Message Lamp Ext.** 4000

Type of 3PCC Enabled None

Coverage Path 2

Localized Display Name Ascom, DECT4000

Under the tab **Feature Options** ensure that **MWI Served User Type** is set to **sip-adjunct**. Ensure the **Voice Mail Number** is set to that configured in **Section 5.6**.

General Options (G) *		Feature Options (F)		Site Data (S)		Abbreviated Call Dialing (A)		Enhanced Call Fwd (E)	
Button Assignment (B)		Group Membership (M)							
Active Station Ringing		single		Auto Answer		none			
MWI Served User Type		sip-adjunct		Coverage After Forwarding		system			
Per Station CPN - Send Calling Number		None		Display Language		english			
AUDIX Name		None		Hunt-to Station					
Remote Soft Phone Emergency Calls		as-on-local		Loss Group		19			
LWC Reception		spe		Survivable COR		internal			
IP Phone Group ID				Time of Day Lock Table		None			
Speakerphone				Voice Mail Number		5999			
Short/Prefixed Registration Allowed		default							
EC500 State		enabled							

There must be 3 call appearances setup for the DECT sets for Call Waiting to work. However the number of call appearances must be changed from 3 to 2 in order to allow the call forward when busy to work properly. Once the **Button Assignment** is completed click on **Done** to finish.

General Options (G) *		Feature Options (F)		Site Data (S)		Abbreviated Call Dialing (A)		Enhanced Call Fwd (E)	
Button Assignment (B)		Group Membership (M)							
Main Buttons		Feature Buttons							
1	call-appr								
2	call-appr								
3	call-appr								
4	None								
5	None								
6	None								

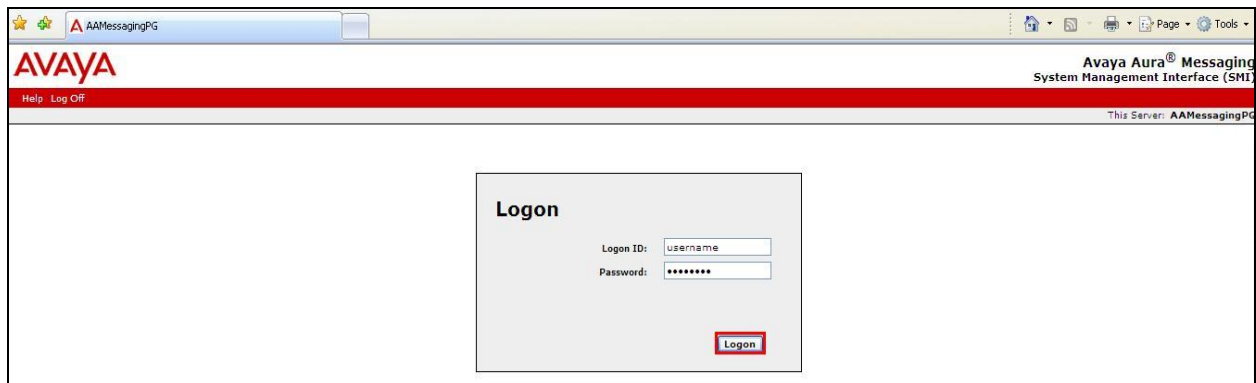
*Required

Done Cancel

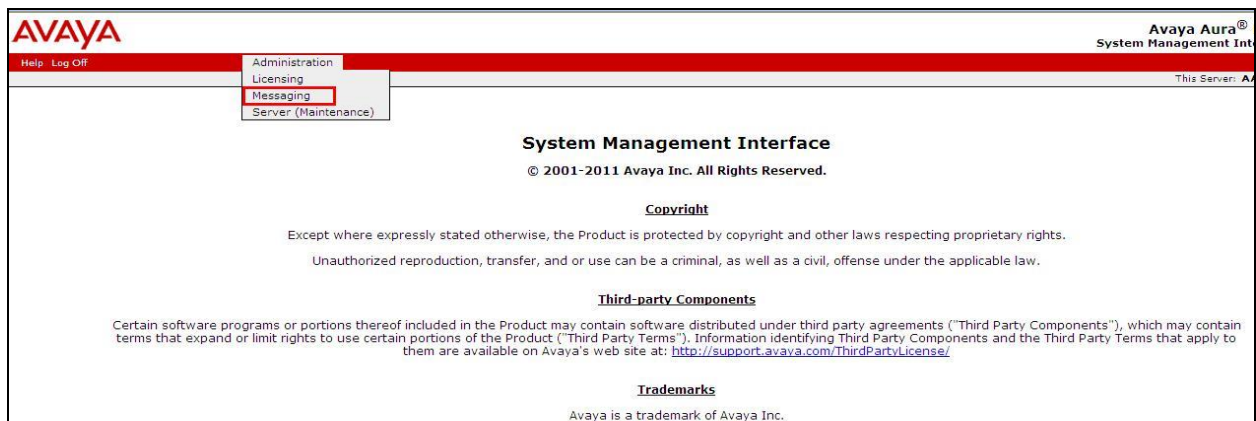
7. Configure Avaya Aura® Messaging

It is assumed that a fully working messaging system is in place and the necessary configuration for Communication Manager and Session Manager has already been done. For further information on the installation and configuration of Messaging please refer to **Section 11** of these Application Notes.

Navigate to <http://<Messaging IP Address>>. Enter the appropriate credentials and click on **Logon** highlighted below.



Once logged on select **Messaging** under **Administration** as shown below.



Click on **User Management** in the left hand column and click on **Add** under **Add User/Info Mailbox** as highlighted below.

AVAYA

Help Log Off Administration

Administration / Messaging

Messaging System (Storage)

User Management

Class of Service

Sites

Topology

Storage Destinations

System Policies

Enhanced List Management

System Mailboxes

System Ports and Access

User Activity Log Configuration

Reports (Storage)

Users

Info Mailboxes

Remote Users

Uninitialized Mailboxes

Login Failures

Locked Out Users

Server Information

System Status (Storage)

System Status (Application)

Alarm Summary

Voice Channels (Application)

Cache Statistics (Application)

Server Settings (Storage)

External Hosts

User Management

License Status

License mode: Normal

Edit User/Info Mailbox

Edit a user's properties. Possible identifiers are: mailbox number.

Identifier:

Edit

Add User/Info Mailbox

Add a new user:

Add

Add a new Info Mailbox:

Enter a suitable **First Name** and **Last Name**. Select the appropriate **Site** from the drop down box. Enter the correct **Mailbox number** and **Extension**. Select the appropriate **Class of Service**.

AVAYA

Help Log Off Administration

Administration / Messaging

Messaging System (Storage)

User Management

Class of Service

Sites

Topology

Storage Destinations

System Policies

Enhanced List Management

System Mailboxes

System Ports and Access

User Activity Log Configuration

Reports (Storage)

Users

Info Mailboxes

Remote Users

Uninitialized Mailboxes

Login Failures

Locked Out Users

Server Information

System Status (Storage)

System Status (Application)

Alarm Summary

Voice Channels (Application)

Cache Statistics (Application)

Server Settings (Storage)

External Hosts

Trusted Servers

Networked Servers

Request Remote Update

MAP/SMTP Settings (Storage)

General Options

Mail Options

IMAP/SMTP Status

User Management > Properties for New User

User Properties

First name:

Last name:

Display name:

ASCII name:

Site:

Mailbox number:

Extension:

☐ Include in Auto Attendant directory

Additional extensions:

Class of Service:

Ensure that **MWI Enabled** is set to **Yes**. Enter a suitable **password** and click on **Save** once finished.

The screenshot shows the Avaya Administration web interface. The left sidebar contains a navigation tree with categories like 'Messaging System (Storage)', 'Reports (Storage)', 'Server Information', and 'Server Settings (Storage)'. The main content area is titled 'Administration' and shows configuration options for a messaging system. The 'MWI enabled' dropdown is set to 'Yes' and is highlighted with a red box. Below it, the 'New password' and 'Confirm password' fields are also highlighted with a red box. At the bottom, the 'Save' button is highlighted with a red box. Other visible options include 'Class of Service' (Standard), 'Pronounceable name', 'Miscellaneous 1' and '2' text boxes, and three checkboxes for password and login settings.

AVAYA

Help Log Off Administration

Administration / Messaging

Messaging System (Storage)

- User Management
- Class of Service
- Sites
- Topology
- Storage Destinations
- System Policies
- Enhanced List Management
- System Mailboxes
- System Ports and Access
- User Activity Log Configuration

Reports (Storage)

- Users
- Info Mailboxes
- Remote Users
- Uninitialized Mailboxes
- Login Failures
- Locked Out Users

Server Information

- System Status (Storage)
- System Status (Application)
- Alarm Summary
- Voice Channels (Application)
- Cache Statistics (Application)

Server Settings (Storage)

- External Hosts
- Trusted Servers
- Networked Servers
- Request Remote Update

Class of Service: Standard

Pronounceable name:

MWI enabled: Yes

Miscellaneous 1:

Miscellaneous 2:

New password:

Confirm password:

☐ User must change voice messaging password at next login

☐ Voice messaging password expired

☐ Locked out from voice messaging

Save Delete

8. Configure Aastra SIP-DECT Base Station and Handsets

In the following example the mandatory steps for a minimal SIP-DECT configuration are covered. Please refer to **Section 11** of these Application Notes for the Aastra SIP-DECT documentation, e.g. System Manual, for more details. The configuration of the Aastra SIP-DECT Base Station and Handsets are both achieved through the web interface of the Aastra SIP-DECT base station. Open a web session to the IP address of the DECT base station, enter the appropriate credentials and click on **OK** as shown below.

The screenshot shows a web browser window with the address bar displaying `https://10.10.40.76/index.html`. The page title is "OpenMobility Manager SIP-DECT 5.0RC9". The main content area features the Aastra logo on the left and the text "OpenMobility Manager SIP-DECT 5.0RC9" on the right. Below the logo is a blue bar with the text "OM Management Portal" and flags for the UK, Germany, France, and Spain. The central part of the page contains a login form with the following fields:

Login	
System	Devconnect
PARK	1F1018725E
User name	omm
Password	••••••••

Below the login form is an "OK" button. The "User name" and "Password" fields, along with the "OK" button, are highlighted with a red border.


8.1. Aastra SIP-DECT System Settings

The OMM system settings provide the fundamental settings to operate the SIP-DECT system. Enter the following details.



- **System Name:** Customer Name
- **Remote access:** Allow SSH access
- **Tone scheme:** Set to the correct country to simulate call control tones
- Insert the **PARK** code from the system CD or license file
- Set the **DECT Regulatory domain**
- Define a **DECT authentication code** for the subscription of new handsets

General settings	
System name	Devconnect
Remote access	<input checked="" type="checkbox"/>
Tone scheme	GB ▼
Net parameters	
ToS for voice packets	B8
ToS for signalling packets	B8
TTL (Time to live)	32
VLAN priority call control	6 ▼
VLAN priority audio	6 ▼
DECT settings	
PARK	1F1018725E (31100303445701)
Encryption	<input checked="" type="checkbox"/>
Restrict subscription duration	<input type="checkbox"/>
DECT monitor	<input type="checkbox"/>
Regulatory domain	EMEA ▼
DECT authentication code	2222

Set the **Voice mail number**.

Radio fixed parts update	
Mode	One by one ▾
Trigger	<input type="checkbox"/>
Time	00 : 00
OMP web start	
Codebase	<input type="text"/>
Downloading new firmware to portable parts	
Active	<input checked="" type="checkbox"/>
Voice mail	
Voice mail number	5999
OM Integrated Messaging & Alerting service	
Internal message routing (PP <> PP)	<input type="checkbox"/>
URL	<input type="text"/> <input type="button" value="Update"/>
Syslog	
Active	<input checked="" type="checkbox"/>
IP address	10.10.16.182
Port	514 <input type="button" value="Default"/>
WLAN settings	
Regulatory domain	DE ▾
 When changing the WLAN regulatory domain all access points will be deactivated.	
Date and time	
Time zone	Western European (WET DST) ▾

Once everything is properly set, scroll to the top of the page and click on **OK**.


System settings	
Status	
 Please check the status page.	
 Changing these settings may cause the OpenMobility Manager to be reset.	
<input checked="" type="button" value="OK"/>	<input type="button" value="Cancel"/>
<input type="button" value="Update"/>	<input type="button" value="Restart"/>

Configure all base stations as Radio fixed Part (RFP) to be operational. Click on New or edit already captured RFPs to start with the configuration (not shown). Fill in the following information correctly.

- **RFP MAC address**
- **Name**
- **Site**

Ensure that **DECT settings** is ticked and enter the **DECT cluster**, (default is **1**). Click on **OK** once this is done.

Configure radio fixed part

 Please configure a WLAN profile of proper type.

General settings

MAC address

00:30:42:12:6D:D1

Name

OMM RFP

Site

1 ▾

☒ **DECT settings**

DECT cluster

1

Preferred synchronization source

☐

Reflective environment

☐

☐ **WLAN settings**

WLAN profile

1 ▾

802.11 channel

▾

Output power level

Full ▾

HT40

☐

OK

8.2. Aastra SIP-DECT SIP Settings

To configure the SIP connection to Session Manager, the OMM requires the SIP user account information as outlined in **Section 6.6**. To connect SIP-DECT with Session Manager, the SIP Domain Name must match to the configured Proxy server and Registrar in SIP-DECT. If the SIP domain cannot be resolved via DNS, configure the Session Manager as an outbound proxy server (+Port) in SIP-DECT. The default SIP signalling port for SIP-Terminals is 5060. The SIP-DECT OMM(s) IP-Address must be configured as that of the SIP Entity created in **Section 6.4**. Please fill in the following details, all others can be left as default.

- **Proxy server** SIP domain configured in **Section 6.2**
- **Proxy port** **5060**
- **Registrar server** SIP domain configured in **Section 6.2**
- **Registrar port** **5060**
- **Registration period** **360**
- **Outbound proxy server** Session Manager IP
- **Outbound proxy port** **5060**
- **Explicit MWI subscription** enabled

Basic settings		
Proxy server	<input type="text" value="devconnect.local"/>	
Proxy port	<input type="text" value="5060"/>	
Registrar server	<input type="text" value="devconnect.local"/>	
Registrar port	<input type="text" value="5060"/>	
Registration period	<input type="text" value="360"/>	sec
Advanced settings		
Outbound proxy server	<input type="text" value="10.10.40.34"/>	
Outbound proxy port	<input type="text" value="5060"/>	
Explicit MWI subscription	<input checked="" type="checkbox"/>	
User agent info	<input checked="" type="checkbox"/>	
Dial terminator	<input type="text" value="#"/>	
Registration failed retry timer	<input type="text" value="120"/>	sec
Registration timeout retry timer	<input type="text" value="180"/>	sec
Transaction timer	<input type="text" value="4000"/>	msec
Blacklist time out	<input type="text" value="5"/>	min
Determine remote party by	<input type="text" value="P-Asserted-Identity"/>	header
Multiple 180 Ringing	<input checked="" type="checkbox"/>	
Semi-attended transfer mode	<input type="text" value="Blind"/>	
Refer-to with replaces	<input type="checkbox"/>	


The default **RTP settings**, **DTMF settings** and **Registration traffic shaping** are known to work. These settings were used during configuration testing. Change the configuration only if specifically required.

RTP settings	
RTP port base	16320
Preferred codec 1	G.722 ▾
Preferred codec 2	G.711 u-law ▾
Preferred codec 3	G.711 A-law ▾
Preferred codec 4	G.729 A ▾
Preferred packet time	20 ▾ msec
Silence suppression	<input type="checkbox"/>
Receiver precedence on codec negotiation	<input type="checkbox"/>
Eliminate comfort noise packets	<input type="checkbox"/>
Single codec reply in SDP	<input type="checkbox"/>

DTMF settings	
Out-of-band	<input checked="" type="checkbox"/>
Method	RTP(RFC 2833) ▾
Payload type	101

Registration traffic shaping	
Active	<input checked="" type="checkbox"/>
Simultaneous registrations	4
Waiting time	0 msec

To avoid invalid Caller Identifications (e.g.; phone-context) on the handset, enable **Truncate Caller identification after “;”** other **Supplementary Services** can be left as default and the **Transport protocol** can be set to either **UDP** or **TCP** as both are supported. Not that this setting will need to match that of the Entity Link setting in **Section 6.5**.

Supplementary Services	
Call forwarding / Diversion	<input checked="" type="checkbox"/>
Local line handling	<input checked="" type="checkbox"/>
Call transfer by hook (A142d)	<input type="checkbox"/>
Truncate Caller Indication after ';'	<input checked="" type="checkbox"/>
SIP reRegister after 2 active OMM failover	<input type="checkbox"/>
Security	
Transport protocol	UDP <input type="button" value="v"/>
Persistent TLS keep alive timer active	<input type="checkbox"/>
Persistent TLS keep alive timer timeout	30 <input type="text"/> sec
Send SIPs over TLS active	<input type="checkbox"/>
TLS-Authentication	<input type="checkbox"/>
TLS-Common-Name-Validation	<input type="checkbox"/>
Trusted certificate(s)	0
Local certificate chain	0
Private key	
Delete certificates/key	<input type="button" value="Delete"/>


8.3. Configure Aastra SIP-DECT Handsets

SIP-DECT allows multiple configuration and provisioning methods for handsets or Portable Parts. In this example fixed Portable Parts were used, for further methods please refer to the manuals outlined in **Section 11** of these Application Notes.

For each Handset (user) in SIP-DECT, a SIP-Extension on Communication Manager (as outlined in **Section 6.6**) must be configured. To create new portable parts go to Portable Parts and click on **New**.

Portable parts

Status


 Please check the status page.


New

Import

Search

PARK: 31100303445701

Subscription allowed: 

Auto-create on subscription: 

Subscription with configured IPEIs










Start

Wildcard subscription

2 min ▾

Start

1 - 3 (3) Portable parts

Display name	Number/SIP user name	IPEI	Subscribed
  DECT 1	4000	03586 0677849 3	
  DECT 2	4001	03586 0677940 4	
  DECT 3	4002	03586 0732594 8	

Enter the following information.

- **Display Name** Contact information of the handset
- **Number/SIP User name** This is the extension number configured in **Section 6.6**
- **IPEI** Handset hardware identifier (optional)
- **DECT authentication code** This is the same as that configured in **Section 8.1**
- **Authentication user name** This is the extension number configured in **Section 6.6**
- **Password** This is the password configured in **Section 6.6**

Configure portable part	
General settings	
Display name	DECT 1
Number/SIP user name	4000
IPEI	03586 0677849 3
DECT authentication code	2222
Login/Additional ID	
Delete subscription	<input type="checkbox"/>
SOS number	
ManDown number	
Voice mail number	
Number used for visibility checks	<input type="checkbox"/>
SIP authentication	
Authentication user name	4000
Password	••••••••••••••••
Password confirmation	••••••••••••••••

To subscribe new handsets, subscriptions need to be permitted by the OMM. Use Wildcard subscription if no IPEI is set.

Wildcard subscription	
10 min ▾	Start

8.4. Subscribe Aastra SIP-DECT Handsets

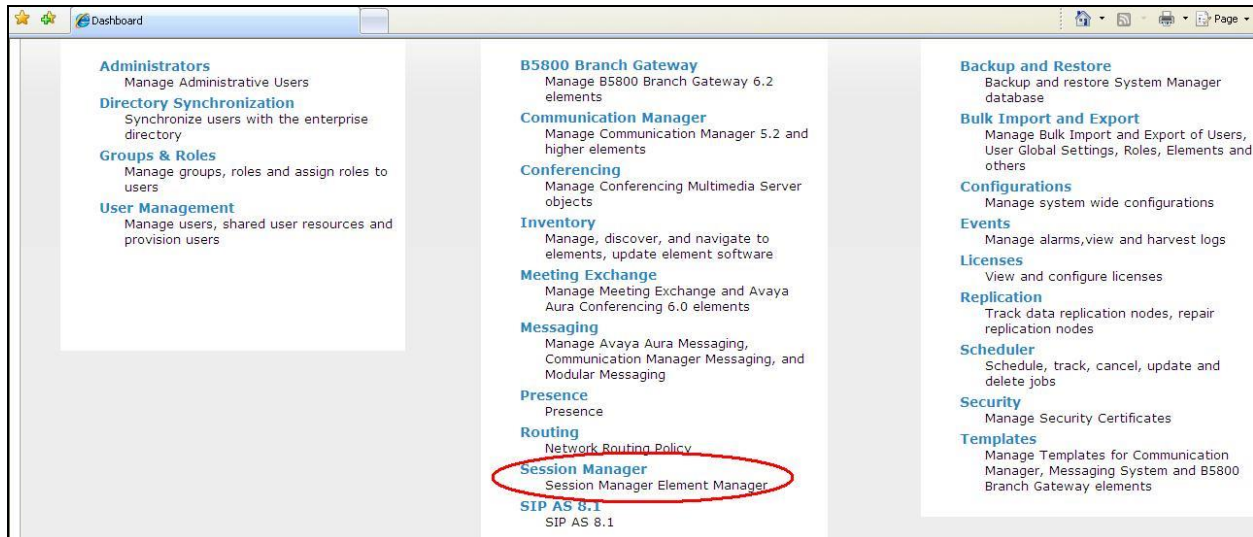
To subscribe new Aastra 600c/d handsets, open the handset Menu and navigate to **Menu → System → Subscriptions**. Select **New system** and enter the Authentication code provided in the System Settings in **Section 8.1** (2222). The handset allows to enter a PARK or to proceed without a PARK. Set the PARK if several DECT systems are around otherwise the handset try to subscribe to the first available DECT system.

9. Verification Steps

The following steps can be taken to ensure that connections between Aastra SIP-DECT handsets and Session Manager and Communication Manager are up.

9.1. Avaya Aura® Session Manager Registration

Log into System Manager as done previously in **Section 6.1**, select **Session Manager** as highlighted below.



Select **System Status** and **User Registrations** in the left column. This displays the users that are currently registered with Session Manager. The DECT users should show as being registered as they are below for extensions **4001** and **4003** highlighted.

Avaya Aura® System Manager 6.3

Last Logged on at October 4, 2013 1:08 PM
Help | About | Change Password | Log off admin

Session Manager * Home

Home / Elements / Session Manager / System Status / User Registrations

User Registrations

Select rows to send notifications to devices. Click on Details column for complete registration status.

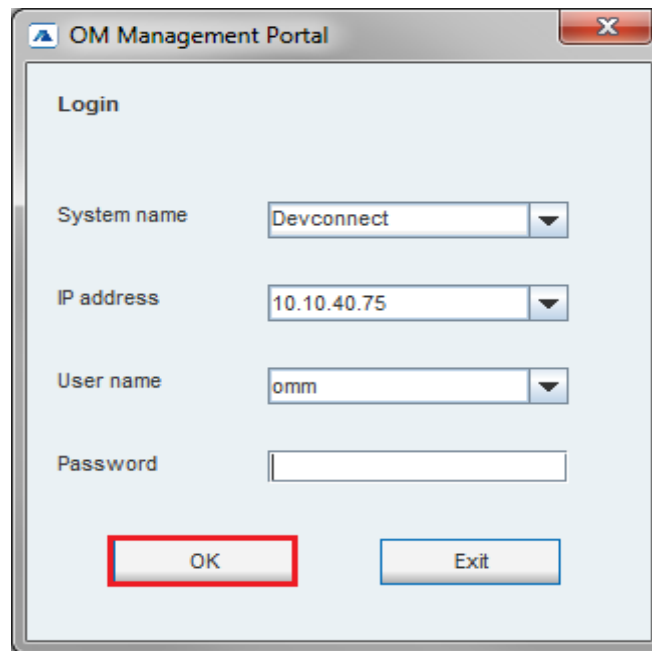
View: Default Force Unregister AST Device Notifications: Reboot Reload Failback As of 1:15 PM Advanced Search

22 Items Refresh Show 15 Filter: Enable

	Details	Address	First Name	Last Name	Actual Location	IP Address	Remote Office	Shared Control	Simult. Devices	AST Device	Registration
<input type="checkbox"/>	Show	4108@devconnect.local	WLESS4108	Ascom	DevConnectPG63	10.10.40.248:5060	<input type="checkbox"/>	<input type="checkbox"/>	1/1	<input type="checkbox"/>	<input checked="" type="checkbox"/> (AC)
<input type="checkbox"/>	Show	4003@devconnect.local	DECT4003	Ascom	DevConnectPG63	10.10.40.181:2055	<input type="checkbox"/>	<input type="checkbox"/>	1/1	<input type="checkbox"/>	<input checked="" type="checkbox"/> (AC)
<input type="checkbox"/>	Show	4001@devconnect.local	DECT4001	Ascom	DevConnectPG63	10.10.40.181:2056	<input type="checkbox"/>	<input type="checkbox"/>	1/1	<input type="checkbox"/>	<input checked="" type="checkbox"/> (AC)
<input type="checkbox"/>	Show	1001@devconnect.local	EXT1001	SIP	DevConnectPG63	10.10.40.155:5061	<input type="checkbox"/>	<input type="checkbox"/>	1/1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> (AC)
<input type="checkbox"/>	Show	1000@devconnect.local	EXT1000	SIP	DevConnectPG63	10.10.40.153:5061	<input type="checkbox"/>	<input type="checkbox"/>	1/1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> (AC)
<input type="checkbox"/>	Show	---	WLESS4106	Ascom	---	---	<input type="checkbox"/>	<input type="checkbox"/>	0/1	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	Show	---	DECT4009	Ascom	---	---	<input type="checkbox"/>	<input type="checkbox"/>	0/1	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	Show	---	DECT4005	Ascom	---	---	<input type="checkbox"/>	<input type="checkbox"/>	0/1	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	Show	---	DECT4007	Ascom	---	---	<input type="checkbox"/>	<input type="checkbox"/>	0/1	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	Show	---	DECT4006	Ascom	---	---	<input type="checkbox"/>	<input type="checkbox"/>	0/1	<input type="checkbox"/>	<input type="checkbox"/>

9.2. Verify Aastra SIP-DECT Handset Registration

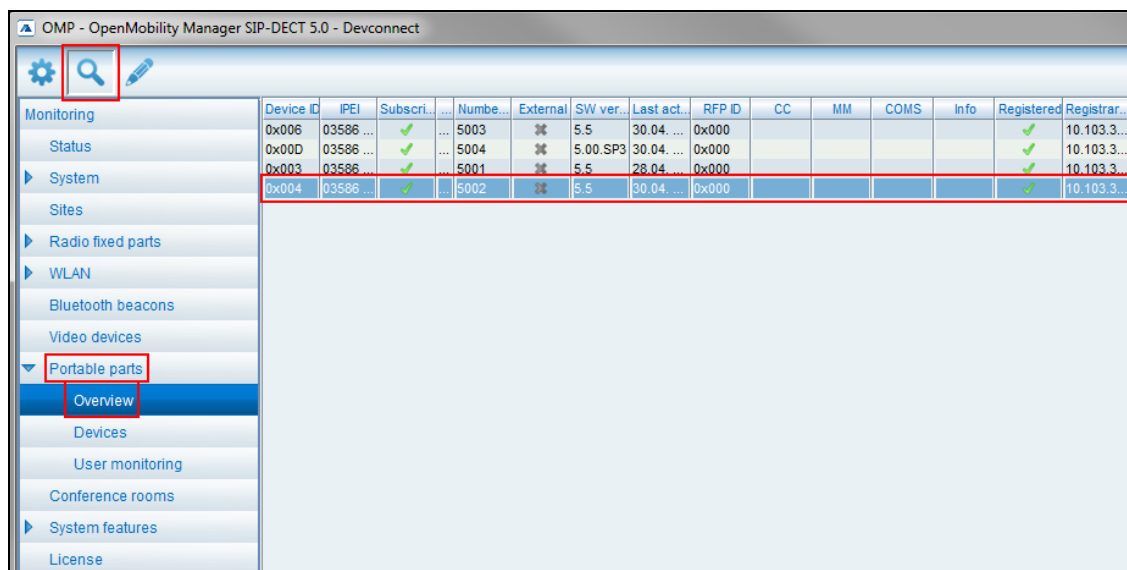
To check the handset state and SIP registration status, OMP (OpenMobility Management Portal) offer a monitoring mode. Select the correct **System name** and **IP address** and enter the appropriate credentials and click on **OK**.



The screenshot shows the 'OM Management Portal' login window. It contains the following fields:

- System name:** A dropdown menu with 'Devconnect' selected.
- IP address:** A dropdown menu with '10.10.40.75' selected.
- User name:** A dropdown menu with 'omm' selected.
- Password:** An empty text input field.
- Buttons:** 'OK' and 'Exit' buttons at the bottom. The 'OK' button is highlighted with a red rectangle.

Open OMP and go to **Monitoring** → **Portable Parts** → **Overview**. The following details should be displayed with a green tick under **Registered** showing the device is registered correctly.



The screenshot shows the OMP interface with the 'Portable parts' section expanded and 'Overview' selected. The table below displays the registration status of several devices. The 'Registered' column shows green checkmarks for all listed devices.

Device ID	IPEI	Subscri...	Numbe...	External	SW ver...	Last act...	RFP ID	CC	MM	COMS	Info	Registered	Registrar...
0x006	03586 ...	✓	5003	⌘	5.5	30.04. ...	0x000					✓	10.103.3...
0x00D	03586 ...	✓	5004	⌘	5.00.SP3	30.04. ...	0x000					✓	10.103.3...
0x003	03586 ...	✓	5001	⌘	5.5	28.04. ...	0x000					✓	10.103.3...
0x004	03586 ...	✓	5002	⌘	5.5	30.04. ...	0x000					✓	10.103.3...

Switch off / on the DECT handset to force SIP user registrations.

10. Conclusion

These Application Notes describe the configuration steps required for Aastra SIP-DECT to successfully interoperate with Avaya Aura® Communication Manager R6.3 and Avaya Aura® Session Manager R6.3 by registering the Aastra SIP-DECT handsets with Avaya Aura® Session Manager as third-party SIP phones. Please refer to **Section 2.2** for test results and observations.

11. Additional References

This section references documentation relevant to these Application Notes. The Avaya product documentation is available at <http://support.avaya.com> where the following documents can be obtained.

- [1] *Administering Avaya Aura® Communication Manager*, Document ID 03-300509
- [2] *Avaya Aura® Communication Manager Feature Description and Implementation*, Document ID 555-245-205
- [3] *Implementing Avaya Aura® Session Manager* Document ID 03-603473
- [4] *Administering Avaya Aura® Session Manager*, Doc ID 03-603324

Aastra's technical documentation is available at www.aastra.com. Please see a list of the documentation used for these Application Notes.

- [6] *SIP-DECT® OM System Manual: Installation, Administration, and Maintenance Release 5.0*
- [7] *SIP-DECT® Knowledge Base: Avaya Aura® Communication Manager*

©2014 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya DevConnect Program at devconnect@avaya.com.