



Avaya Solution & Interoperability Test Lab

**Application Notes for Configuring Ascom DECT Handsets
and Ascom IPBS Access Point with Avaya Aura®
Communication Manager R6.2 and Avaya Aura® Session
Manager R6.2 – Issue 1.2**

Abstract

These Application Notes describe the configuration steps for provisioning Ascom's IP DECT Base Station and Handsets 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 Ascom's IP DECT Base Station and DECT Handsets to interoperate with Avaya Aura® Communication Manager R6.2 and Avaya Aura® Session Manager R6.2. Ascom's DECT handsets are configured to register with Session Manager and are also configured on Avaya Aura® Communication Manager as Avaya 9600 SIP endpoints. The Ascom DECT handsets then behave as third-party sip extensions on Communication Manager able to make/receive internal calls and have full voicemail and other telephony facilities available on Communication Manager.

2. General Test Approach and Test Results

The interoperability compliance testing evaluates the ability of Ascom DECT sets 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 Ascom 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, Ascom DECT endpoints and PSTN endpoints.

- Basic Calls
- Hold and Retrieve
- Attended and Blind Transfer
- Call Forwarding Unconditional, No Reply and Busy (Controlled on PBX)
- Call Waiting
- Call Park/Pickup
- EC500
- Conference
- 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 Ascom Dect IP Base Station and Session Manager is not supported. All compliance testing was carried out using TCP and/or UDP as the transport protocol.
2. Although the Ascom handsets are added as SIP users when using TCP as the transport protocol a SIP Entity and a SIP Entity Link must be added as per **Section 6.2**. Note this is not required when using UDP.
3. When the Ascom handset transfers “blind” to the Avaya deskphones there is no ringback heard from the Ascom handset.
4. Handsets d41 and d62 do not update with the A-Party number on transfer.
5. Cannot hear incoming DTMF tones on the Ascom DECT handsets from PSTN caller.
6. If there are active calls present on the SIP trunk between the Communication Manager and the Session Manager when a standby base station takes over from the master base station these trunks remain busy due to Communication Managers ‘Connection Preservation’ timer which is hardcoded, they will clear after 2 hours. This may result in a “Service” message from Communication Manager stating “no signaling available”. Please note this may only occur if there are insufficient trunks available for further calls to be made.
7. When there is a Message Waiting Indicator on an Ascom handset when registered to the master base station and a failover to the secondary base station is done the Message Waiting indicator fails to get removed when the voicemail is emptied. This can also be cleared by turning the handset off and on again.

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 Ascom IP DECT product can be obtained through a local Ascom supplier. Ascom global technical support:

- Email: support@ascom.se
- Help desk: +46 31 559450

3. Reference Configuration

Figure 1 shows the network topology during compliance testing. The Ascom DECT Handsets connect to the Ascom DECT Base Station which 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.

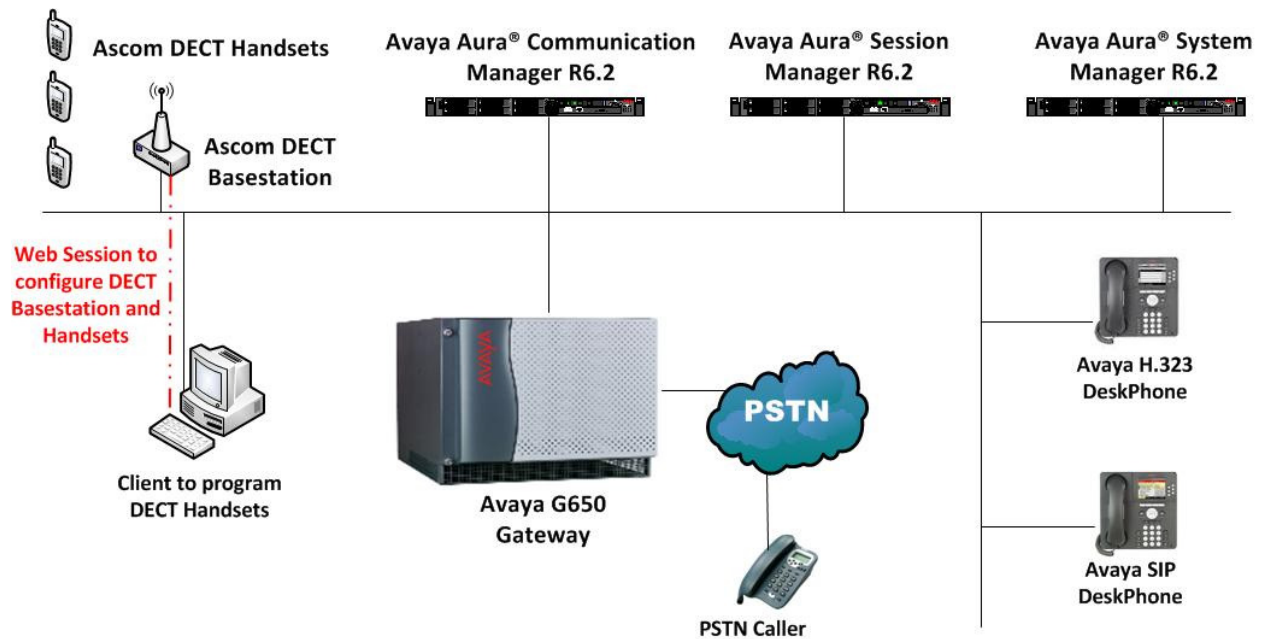


Figure 1: Network Solution of Ascom DECT Handsets with Avaya Aura® Communication Manager R6.2 and Avaya Aura® Session Manager R6.2

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 S8800 Server	R6.2 SP4 Build 6.2.0.0.15669-6.2.12.408
Avaya Aura® Communication Manager running on an Avaya S8800 Server	R6.2 SP4 R016x.02.0.823.0
Avaya Aura® Session Manager running on an Avaya S8800 Server	R6.2 SP3 6.2.3.0.623006
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
Ascom DECT Base Station	IPBS V5.1.2
Ascom DECT Handsets	Mixture of 9 D41, D62, D81 handsets D62-Talker 3.0.9 D62-Protector 3.5.11 D41-Basic 3.0.6 D41-Advanced 3.5.11 D81-Messenger 3.4.11 D81-Messenger 2.0.17

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

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                                     Page 1 of 12
                                                           DIAL PLAN ANALYSIS TABLE
                                                           Location: all                                     Percent Full: 1
Dialed Total Call      Dialed Total Call      Dialed Total Call
String Length Type     String Length Type     String Length 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 Ascom 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. Note that Ascom does not feature in this setup only the name and IP address of Session Manager is added. Use the **change node-names ip** command to configure the IP address of Session Manager. **SM100** is the **Name** used for Session Manager and **192.168.50.16** is the **IP Address**.

```

change node-names ip                                         Page 1 of 2
                                IP NODE NAMES
Name      IP Address
SM100     192.168.50.16
default   0.0.0.0
g250-dcp  192.168.50.18
procr     192.168.50.13
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 **devcon.avaya** is used. Note this domain is also configured in **Section 6.1** of these Application Notes.

```
change ip-network-region 1                                     Page 1 of 20
                                                           IP NETWORK REGION
  Region: 1
  Location: 1          Authoritative Domain: devcon.avaya
    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
  H.323 IP ENDPOINTS                                       AUDIO RESOURCE RESERVATION PARAMETERS
    H.323 Link Bounce Recovery? y                          RSVP Enabled? n
    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 Ascom 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 59
                                COVERAGE PATH

                                Coverage Path Number: 59
                                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
                                HUNT GROUP
                                Page 1 of 60

                                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
                                HUNT GROUP
                                Page 2 of 60

                                Message Center: sip-adjunct

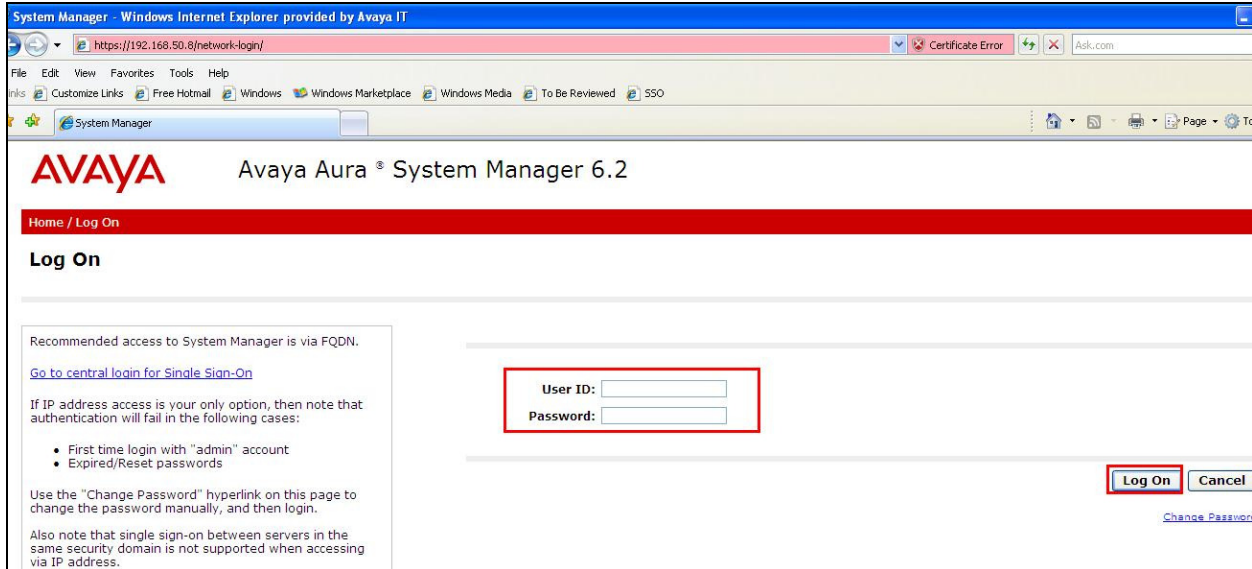
                                Voice Mail Number   Voice Mail Handle   Routing Digits
                                (e.g., AAR/ARS Access Code)
                                59000                59000              *99
```

6. Configure Avaya Aura® Session Manager

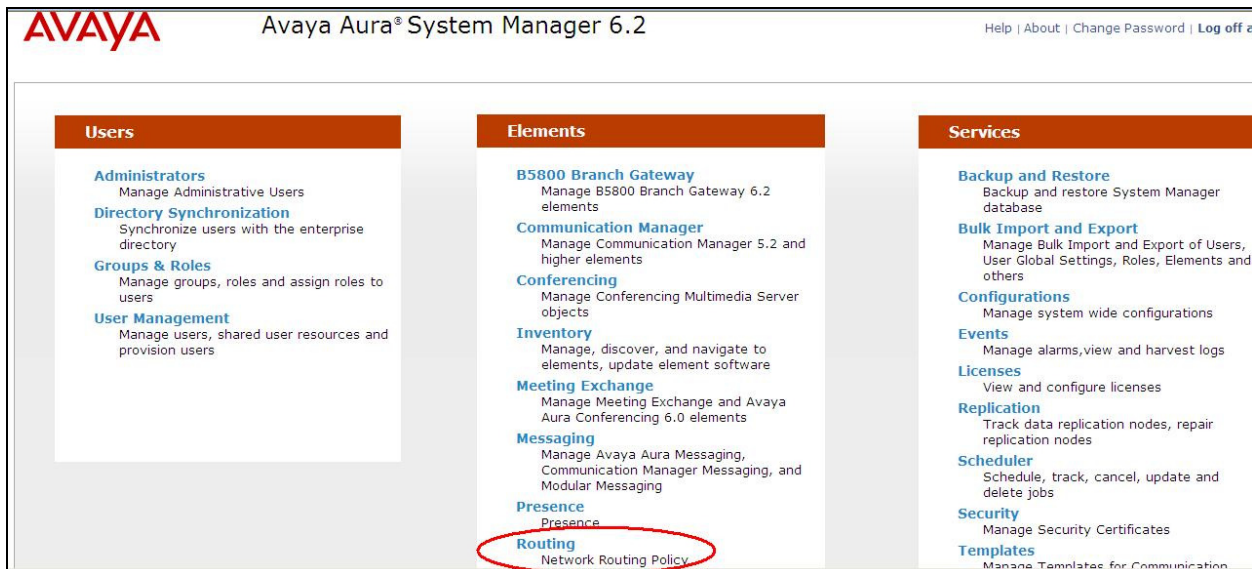
The Ascom DECT Handsets are added to Session Manager as SIP Users. In order make changes in Session Manager a web session to System Manager is opened.

6.1. Configuration of a Domain

Navigate to <http://<System Manager IP Address>/SMGR>, enter the appropriate credentials and click on **Log On** as shown below.



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



Click on **Domains** in the left window. If there is not a domain already configured click on **New** highlighted below and enter a suitable domain name. Note the domain **Name** used in the compliance testing was **devcon.avaya**. Note this domain is also referenced in **Section 5.4** of these Application Notes.

AVAYA Avaya Aura® System Manager 6.2 Help | About

Home / Elements / Routing / Domains

Domain Management

1 Item Refresh

<input type="checkbox"/>	Name	Type	Default	Notes
<input type="checkbox"/>	devcon.avaya	sip	<input type="checkbox"/>	

Select : All, None

6.2. Configuration of SIP Entities

Navigate to <http://<System Manager IP Address>/SMGR>, enter the appropriate credentials and click on **Log On** as shown in **Section 6.1**. Once logged in click on **Routing** highlighted below.

The screenshot shows the Avaya Aura System Manager 6.2 interface. The top navigation bar includes the Avaya logo, the product name, and links for Help, About, Change Password, and Log off. The main content area is divided into three columns: Users, Elements, and Services. Under the Elements column, the 'Routing' option is circled in red, with the sub-option 'Network Routing Policy' visible below it.

Click on **SIP Entities** highlighted below.

The screenshot shows the 'Routing' configuration page in Avaya Aura System Manager 6.2. The left-hand navigation menu is expanded to show 'Routing' options, with 'SIP Entities' circled in red. The main content area displays the 'Introduction to Network Routing Policy' page, which includes a list of steps for configuring the routing workflow.

Introduction to Network Routing Policy

Network Routing Policy consists of several routing applications like "Domains", "Locations", "SIP Entities", etc. The recommended order to use the routing applications (that means the overall routing workflow) to configure

- Step 1: Create "Domains" of type SIP (other routing applications are referring domains of type SIP).
- Step 2: Create "Locations"
- Step 3: Create "Adaptations"
- Step 4: Create "SIP Entities"

- SIP Entities that are used as "Outbound Proxies" e.g. a certain "Gateway" or "SIP Trunk"
- Create all "other SIP Entities" (Session Manager, CM, SIP/PSTN Gateways, SIP Trunks)

Clicking on **SIP Entities** shows what SIP Entities have been added to the system and allows the addition of any new SIP Entity that may be required. Please note the SIP Entities already present for the Compliance Testing of Ascom DECT Handsets.

- Communication Manager SIP Entity
- Session Manager SIP Entity
- Messaging SIP Entity

Note: There is no SIP Entity required if UDP is chosen for the transport protocol in **Section 8.3**, where TSIP is chosen for TCP protocol and SIP for UDP protocol.

If TCP is chosen as the transport protocol for the Ascom DECT then a SIP Entity and an Entity Link are required for the Ascom IPBS. Select **SIP Entities** in the left window and click on **New** in the main window.

Note: A SIP Entity and Entity link are required for both the Master and Standby Base Stations.

The screenshot shows the Avaya Aura System Manager 6.2 interface. The left navigation pane has 'SIP Entities' highlighted. The main content area shows a list of 3 SIP Entities:

Name	FQDN or IP Address	Type
AMessaging	192.168.50.60	Modular Messaging
CommunicationManager	192.168.50.13	CM
SessionManager	192.168.50.16	Session Manager

Enter a suitable **Name** and enter the **IP Address** of the DECT Base Station. Select the correct **Location** and **Time Zone**. Click on **Commit** once completed.

The screenshot shows the 'SIP Entity Details' form in Avaya Aura System Manager 6.2. The 'General' tab is active. The form fields are as follows:

- Name:** AscomDECT
- FQDN or IP Address:** 192.168.50.100
- Type:** SIP Trunk
- Notes:** (empty)
- Adaptation:** (dropdown menu)
- Location:** DevconLAB
- Time Zone:** Europe/Dublin
- Override Port & Transport with DNS SRV:** (checkbox, unchecked)
- SIP Timer B/F (in seconds):** 4
- Credential name:** (empty)

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

Avaya Aura® System Manager 6.2

Home / Elements / Routing / Entity Links

Entity Links

Buttons: Edit, **New**, Duplicate, Delete, More Actions

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy
AAessaging	SessionManager	TCP	5060	AAessaging	5060	Trusted
DS3000	SessionManager	UDP	5060	DS3000	5060	Trusted
IPOffice	SessionManager	TCP	5060	IPOfficePG	5060	Trusted
RPMessaging	SessionManager	TCP	5060	RichardAuraMessaging	5060	Trusted
SessionManager_CommunicationManager_5061_TLS	SessionManager	TLS	5061	CommunicationManager	5061	Trusted
ToCS1KPG2	SessionManager	TCP	5060	CS1KPG2	5060	Trusted
ToSBC	SessionManager	TCP	5060	SIPERASBC	5060	Trusted

Ensure that **TCP** is selected for the **Protocol** and **5060** for the **Port**. Click on **Commit** once completed.

Avaya Aura® System Manager 6.2

Home / Elements / Routing / Entity Links

Entity Links

Buttons: Commit

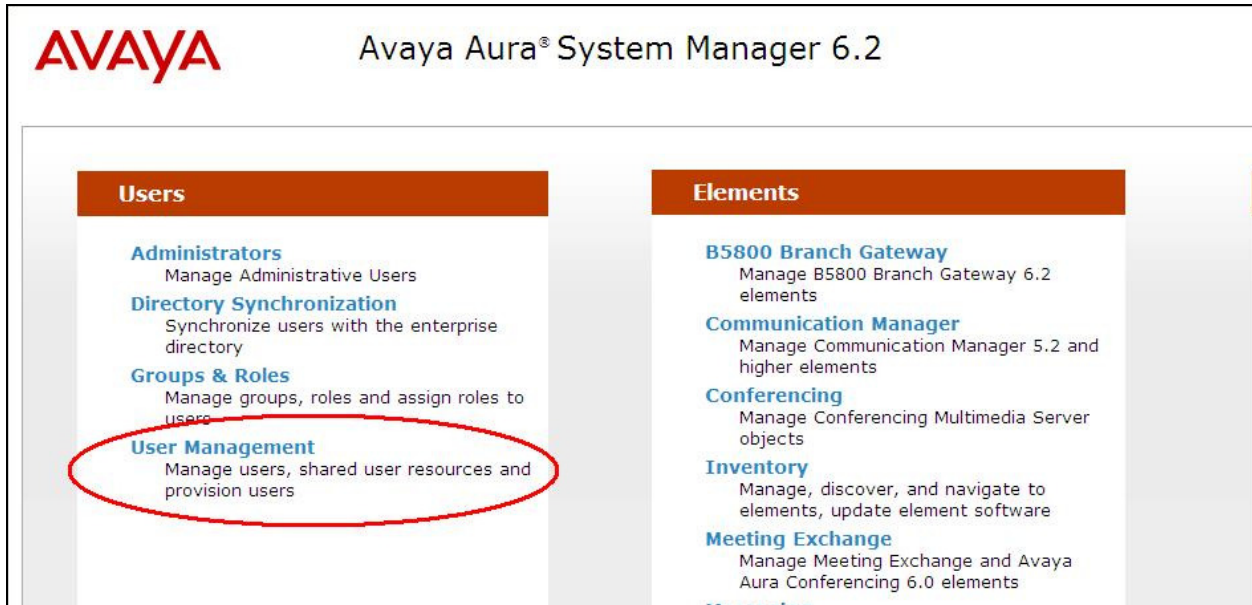
Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Notes
* Ascom	* SessionManager	TCP	* 5060	* AscomDECT	* 5060	Trusted	

* Input Required

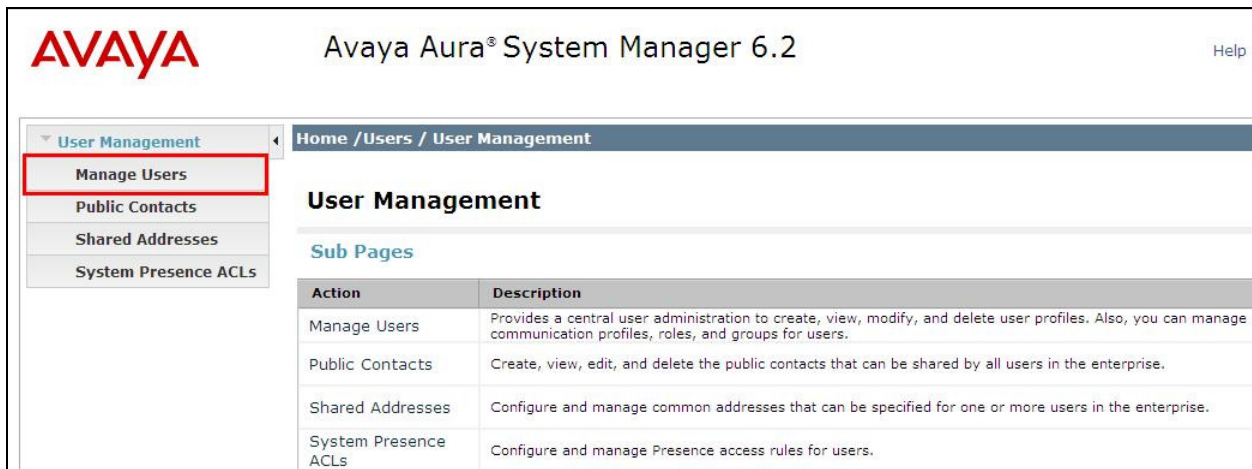
Buttons: Commit

6.3. Adding Ascom SIP Users

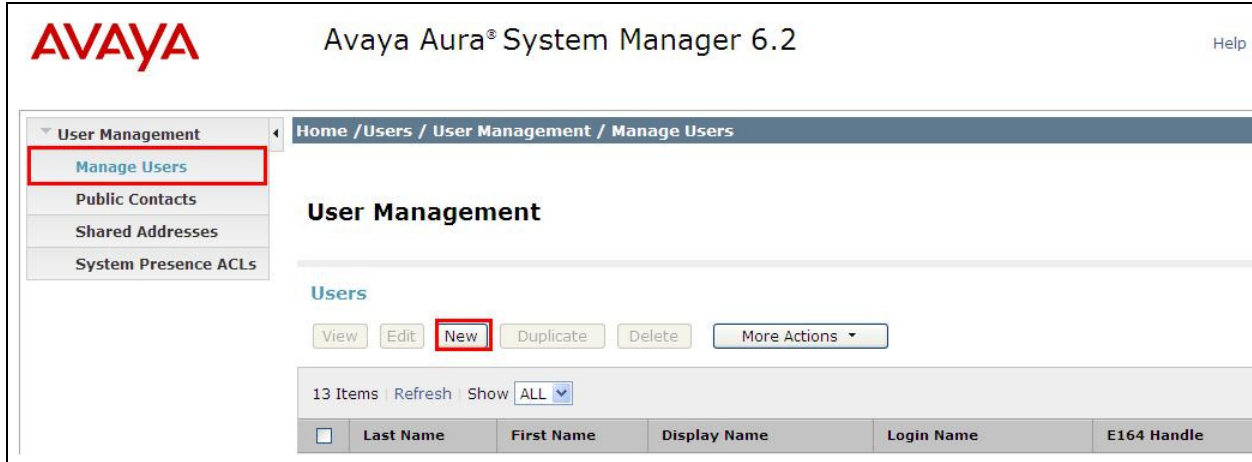
From the home page click on **User Management** highlighted below.



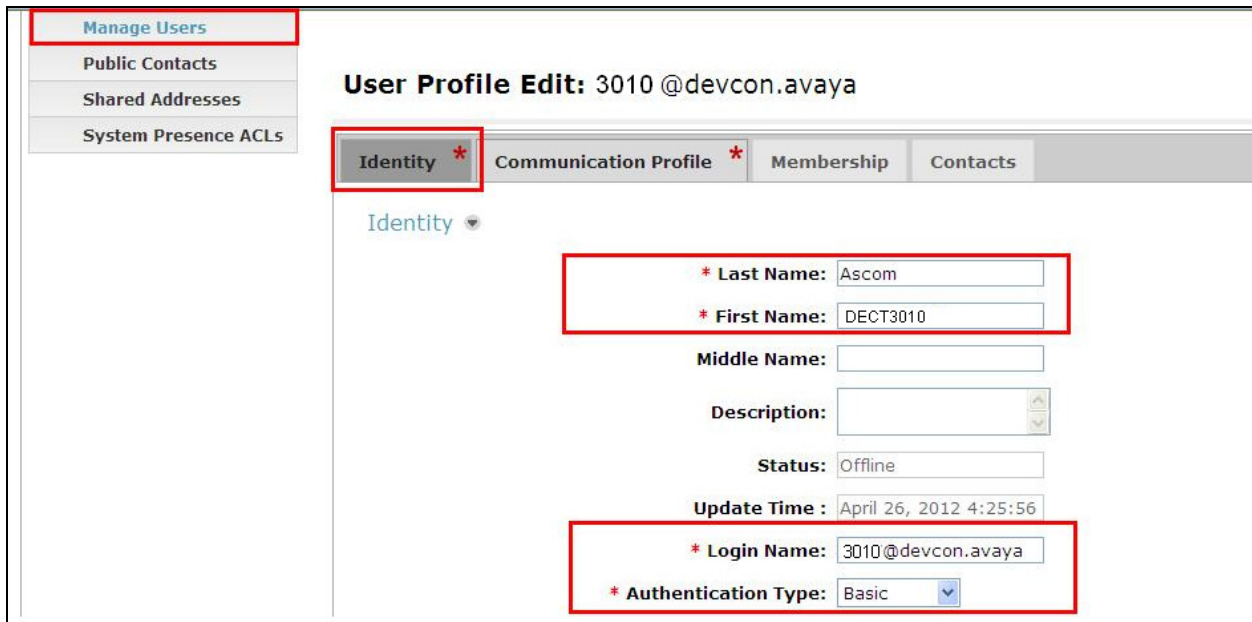
Click on **Manage Users**.



Click on **New** highlighted 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**.



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 Ascom handset in **Section 8.2**. Click on **New** to add a new **Communication Address**.

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

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.

Primary	Secondary	Maximum
12	0	12

Primary	Secondary	Maximum

Ensure that **CM Endpoint Profile** is selected and choose the **DEFAULT_9620SIP_CM_6_2** 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.

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.

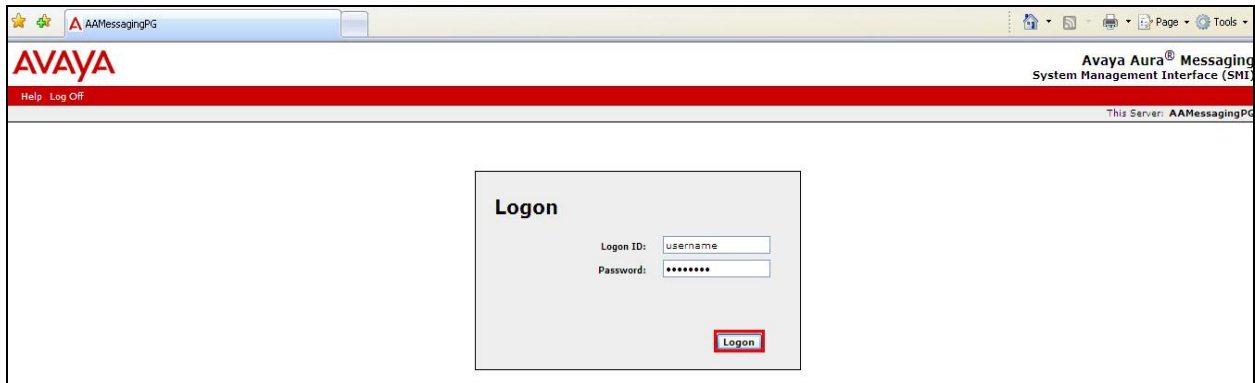
Under the tab **Feature Options** ensure that **EC500 State** is **enabled**.

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	Select	Coverage After Forwarding	system	Per Station CPN - Send Calling Number	Select	Display Language	english	Hunt-to Station	
AUDIX Name	Select	Loss Group	19	Remote Soft Phone Emergency Calls	as-on-local	Survivable COR	internal	LWC Reception	spe	Time of Day Lock Table	Select	Voice Mail Number	
IP Phone Group ID		EC500 State	enabled	Speakerphone	2-way								
Short/Prefixed Registration Allowed	Select												

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.

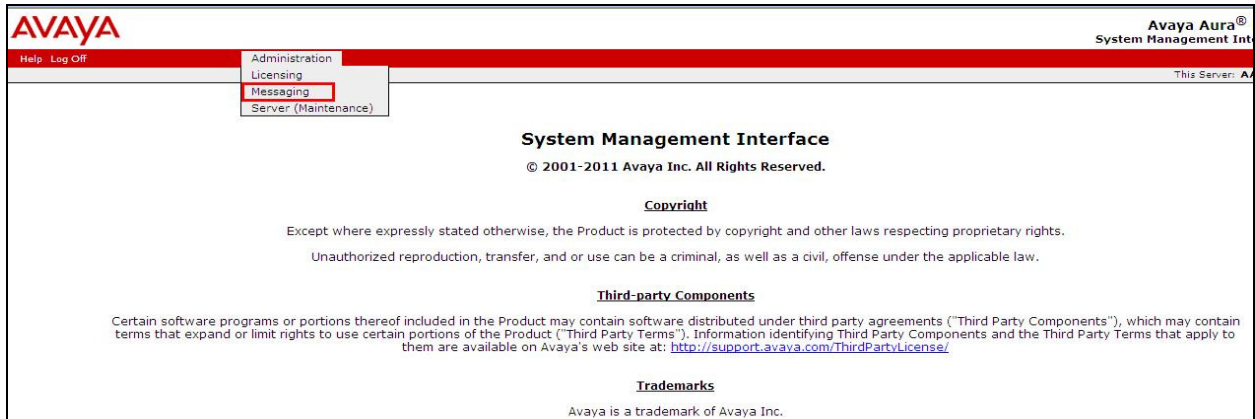
Navigate to <http://<Messaging IP Address>>. Enter the appropriate credentials and click on **Logon** highlighted below.



The screenshot shows a web browser window with the address bar displaying 'AAMessagingPG'. The page header includes the Avaya logo and 'Avaya Aura® Messaging System Management Interface (SMI)'. Below the header, there is a 'Logon' form with the following fields and elements:

- Logon ID:
- Password:
- Logon button (highlighted in red)

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



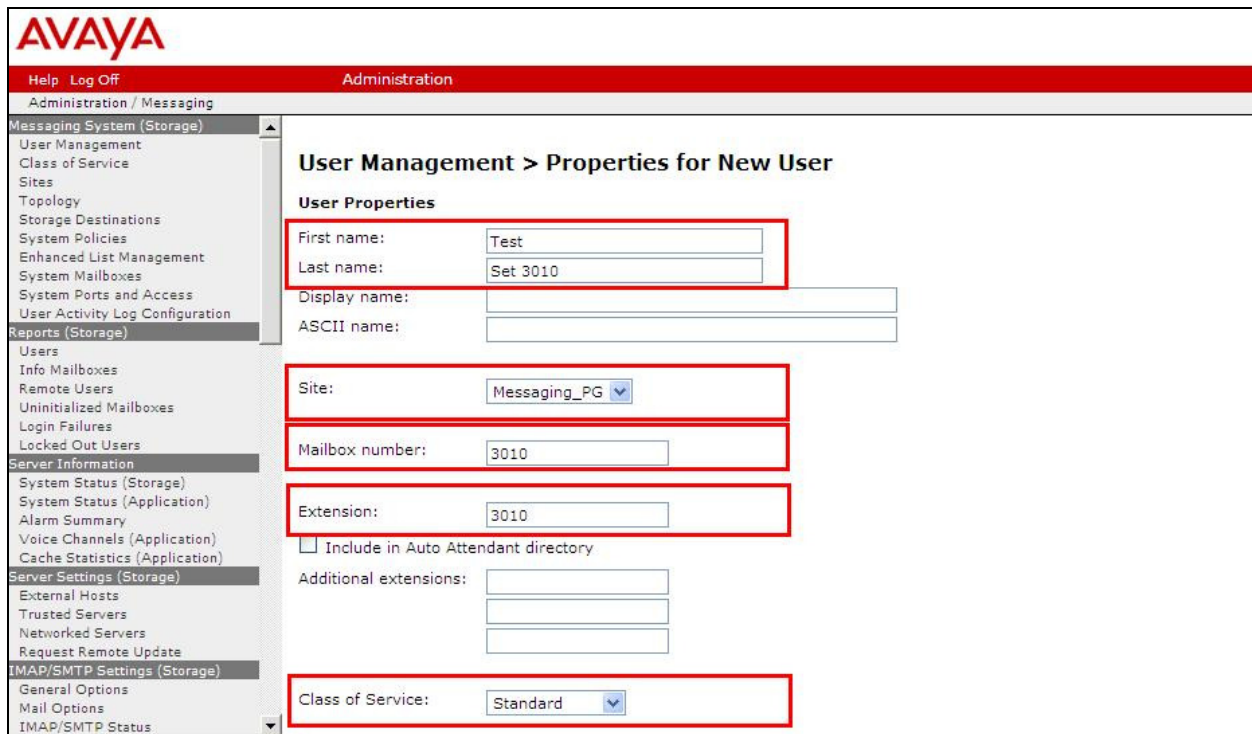
The screenshot shows the main page of the Avaya Aura® Messaging System Management Interface (SMI). The 'Administration' menu is open, and 'Messaging' is highlighted with a red box. The main content area displays the following information:

- System Management Interface**
- © 2001-2011 Avaya Inc. All Rights Reserved.
- Copyright**
- Except where expressly stated otherwise, the Product is protected by copyright and other laws respecting proprietary rights. Unauthorized reproduction, transfer, and or use can be a criminal, as well as a civil, offense under the applicable law.
- Third-party Components**
- Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements ("Third Party Components"), which may contain terms that expand or limit rights to use certain portions of the Product ("Third Party Terms"). Information identifying Third Party Components and the Third Party Terms that apply to them are available on Avaya's web site at: <http://support.avaya.com/ThirdPartyLicense/>
- Trademarks**
- Avaya is a trademark of Avaya Inc.

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



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**.



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

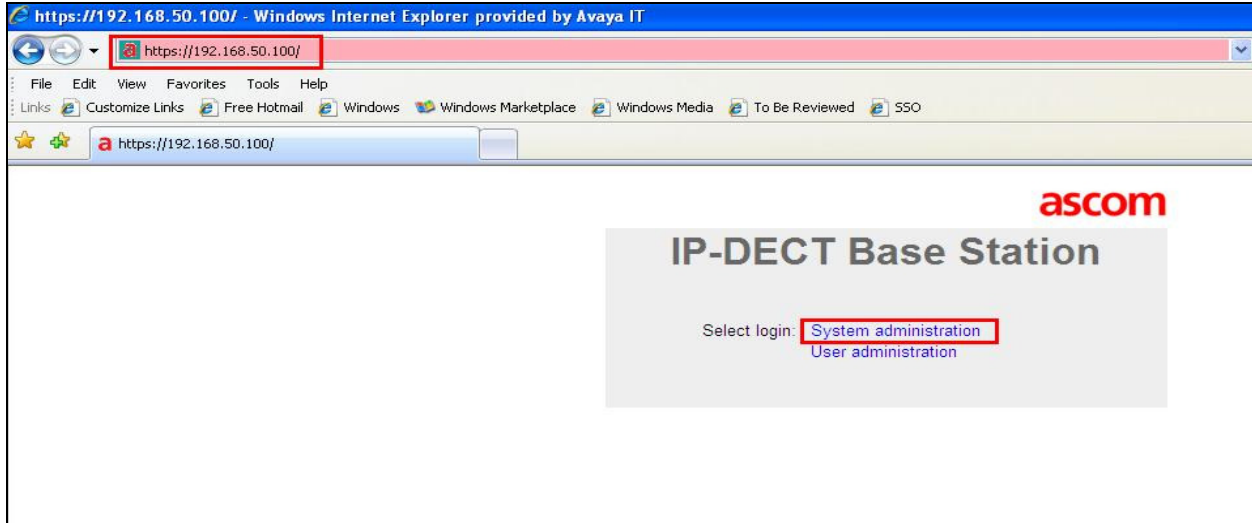
The screenshot shows the Avaya Administration web interface. The top navigation bar includes 'Help' and 'Log Off'. The main header is 'Administration'. The left sidebar contains a tree view of administrative categories: 'Administration / Messaging', 'Messaging System (Storage)', 'Reports (Storage)', 'Server Information', and 'Server Settings (Storage)'. The main content area is titled 'Administration / Messaging' and contains the following fields and options:

- Class of Service: Standard (dropdown)
- Pronounceable name: (text input)
- MWI enabled: Yes (dropdown, highlighted with a red box)
- Miscellaneous 1: (text input)
- Miscellaneous 2: (text input)
- New password: (password input, highlighted with a red box)
- Confirm password: (password input, highlighted with a red box)
- User must change voice messaging password at next login
- Voice messaging password expired
- Locked out from voice messaging

At the bottom of the form, there are two buttons: 'Save' (highlighted with a red box) and 'Delete'.

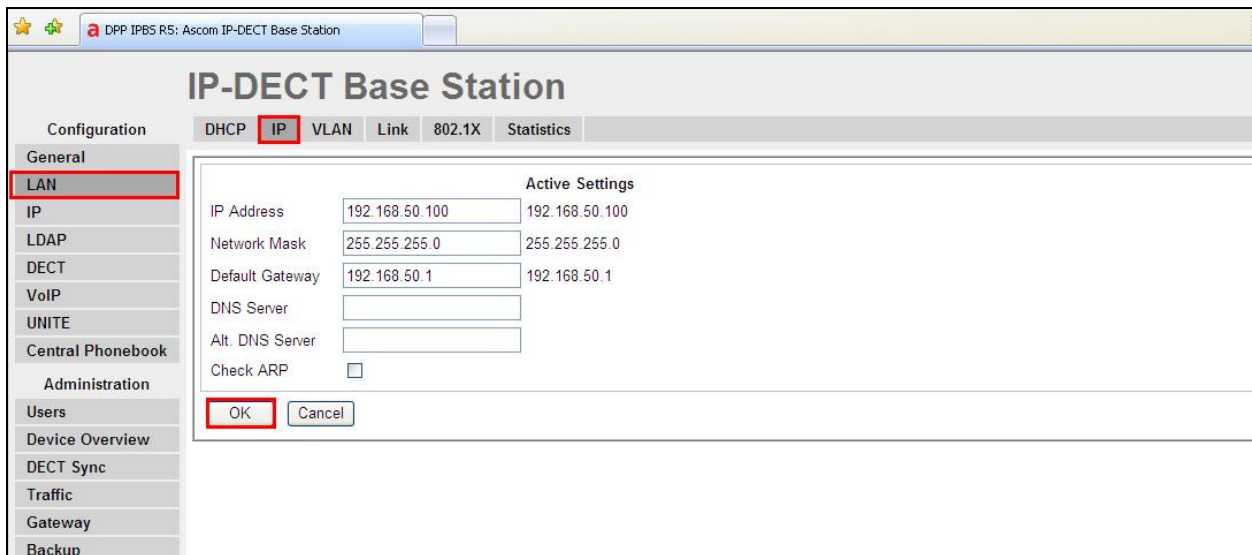
8. Configure Ascom DECT Base Station and Handsets

The configuration of the DECT Base Station and the DECT handsets are both achieved through a http session to the web interface of the DECT base station. Open a web session to the IP address of the DECT base station as and click on **System administration** as shown below.



8.1. Configure DECT Base Station IP address

In order to change the IP Address of the DECT Base Station in order to connect to the local LAN select **LAN** in the left column and click on the **IP** tab. Enter the **IP Address** information of the DECT Base Station and click on **OK**. Ensure also that DHCP mode is set to disabled under the **DHCP** tab.



Please refer to Ascom's documentation listed in **Section 11** of these Application Notes for further information about DECT configuration. The following sections cover specific settings concerning SIP and the connection to Session Manager.

8.2. Configure IP-DECT Base Station System Information

Select **DECT** in the left column and click on the **System** tab in the main window. Ensure that **Subscriptions** is set to **With System AC** and enter an appropriate **Authentication Code**, note this will be used again in subscribing the DECT handsets in **Section 6.3**. Select the appropriate country for **Tones**, note for these compliance tests **IRELAND** was selected. Select **Europe** for the **Frequency** and ensure that **Local R-Key Handling** is ticked. For **Coder** select **G711A** from the drop-down box note that this will be the same codec used in **Section 5.5**.

The screenshot displays the 'IP-DECT Base Station' configuration window. The 'System' tab is selected and highlighted with a red box. The left-hand navigation menu also has 'DECT' highlighted with a red box. The configuration fields are as follows:

Field	Value
System Name	DECT
Password	••••••••
Confirm Password	••••••••
Subscriptions	With System AC
Authentication Code	9999
Tones	IRELAND
Default Language	English
Frequency	Europe
Enabled Carriers (0-9)	All checked
Local R-Key Handling	Checked
No Transfer on Hangup	Unchecked
No On-Hold Display	Unchecked
Coder	G711A
Frame (ms)	20
Secure RTP	Exclusive
SC	Unchecked

Buttons for 'OK' and 'Cancel' are located at the bottom of the configuration area.

8.3. Configure Session Manager Information

Select **DECT** in the left column and select the **Master** tab. Ensure the **Protocol** is set to **TSIP** if TCP is the chosen transport protocol and **SIP** if UDP is the chosen transport protocol and enter the Session Manager IP address for **Proxy**. Enter the **Domain** that was configured in **Section 6.1** and enter the length of digits used for internal numbers. All other values can be accepted as default.

Note: If TSIP is selected below a SIP Entity must be added for the Ascom IP Base Station as per **Section 6.2**.

The screenshot shows the 'IP-DECT Base Station' configuration interface. The 'Master' tab is selected. The 'DECT' option is highlighted in the left-hand navigation menu. The 'IP-PBX' section is highlighted with a red box and contains the following settings:

- Mode: Active
- Multi-Master: Master ID: 0, Enable PARI Function:
- IP-PBX: Protocol: TSIP, Proxy: 192.168.50.16, Alt. Proxy: (empty), Domain: devcon.avaya, Max. Internal Number Length: 4 (used to decide internal/external ring signal)
- International CPN Prefix: (empty)
- Enbloc Dialing:
- Enable Enbloc Send-Key:
- Send Inband DTMF:
- Allow DTMF Through RTP:
- Short Disconnect Tone:
- Configured With Local GK:

Scroll down and click on **OK** as highlighted below to save the new configuration.

The screenshot shows the 'IP-DECT Base Station' configuration interface, scrolled down to the 'Registration' and 'Mobility Master' sections. The 'Master' tab is selected. The 'DECT' option is highlighted in the left-hand navigation menu. The 'OK' button is highlighted with a red box.

Registration settings:

- Registration Time-To-Live: 120 [sec]
- Hold Signalling: inactive
- Hold Before Transfer:
- Accept Inbound Calls Not Routed Via Home Proxy:
- Register With Number:
- KPML support:

Registration For Anonymous Devices:

- Registration Name / Number: (empty) / (empty)
- Deactivate Master If No Connection:

Mobility Master settings:

- Name: (empty)
- Password: (empty)
- IP Address: (empty)
- Alt. IP Address: (empty)
- Status: (empty)

Click on the **Suppl. Serv.** tab and ensure that **Enable Supplementary Services** is checked. Take note of the activation and deactivation codes for services such as **Call Forwarding**, **Call Waiting** and **Do Not Disturb**. Click on **OK** when finished.

The screenshot shows the 'IP-DECT Base Station' configuration window. The 'Suppl. Serv.' tab is selected, and the 'Enable Supplementary Services' checkbox is checked. The 'DECT' category is highlighted in the left sidebar. The main area contains a table of services with their respective activation and deactivation codes, and a 'Disable' checkbox for each.

Service	Activate	Deactivate	Disable
Call Forwarding Unconditional	*21*\$#	#21#	<input type="checkbox"/>
Call Forwarding Busy	*67*\$#	#67#	<input type="checkbox"/>
Call Forwarding No Reply	*61*\$#	#61#	<input type="checkbox"/>
Do Not Disturb	*42#	#42#	<input type="checkbox"/>
Call Waiting	*43#	#43#	<input type="checkbox"/>
Call Completion Busy Subscriber	-	-	<input checked="" type="checkbox"/>
Logout User	#11*\$#		<input type="checkbox"/>
Clear Local Setting	*00#		<input type="checkbox"/>
MWI Mode	User dependent interrogate number		
MWI Notify Number	5999		
Local Clear of MWI	-		
External Idle Display			<input type="checkbox"/>

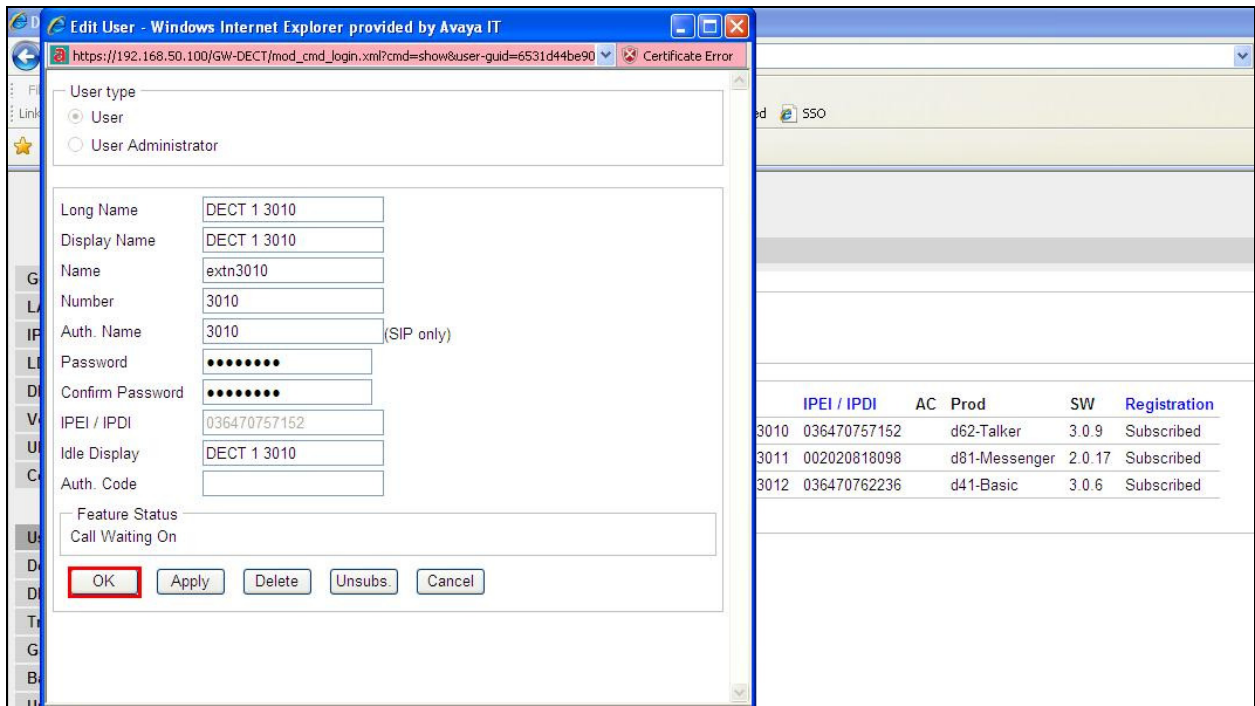
At the bottom of the window, there are 'OK' and 'Cancel' buttons.

8.4. Adding DECT Users

Click on **Users** in the left column and click **new** to add a new DECT user.



Enter the appropriate information for the new DECT user and once all the information has been correctly filled in click on **OK** as highlighted. The Handset is registered with the DECT system, according to Ascom's documentation.



To change features such as **Call Waiting** or **Do not Disturb** click on the **+** icon under **Fty** as highlighted below. This opens a new window where these services can be selected or deselected. Click on **OK** once the appropriate services are selected.

The screenshot shows a web browser window with a URL of `https://192.168.50.100/GW-DECT/mo...`. A modal dialog box is open, allowing selection of features. The dialog has the following options:

- CFU:
- CFB:
- CFNR:
- Do not Disturb Int.:
- Do not Disturb Ext.:
- Call Waiting:

Buttons: **OK** (highlighted with a red box), **Cancel**.

The background page shows a table of users with the following columns: Long Name, Name, No, Fty, Display, IPEI / IPDI, AC, Prod, SW, Registration. The 'Fty' column is highlighted with a red box.

Long Name	Name	No	Fty	Display	IPEI / IPDI	AC	Prod	SW	Registration
DECT 1 3010	extn3010	3010	+	DECT 1 3010	036470757152		d62-Talker	3.0.9	Subscribed
DECT 2 3011	extn3011	3011	+	DECT 2 3011	002020818098		d81-Messenger	2.0.17	Subscribed
DECT 3 3012	extn3012	3012	+	DECT 3 3012	036470762236		d41-Basic	3.0.6	Subscribed

Users: 3, Registrations: 0

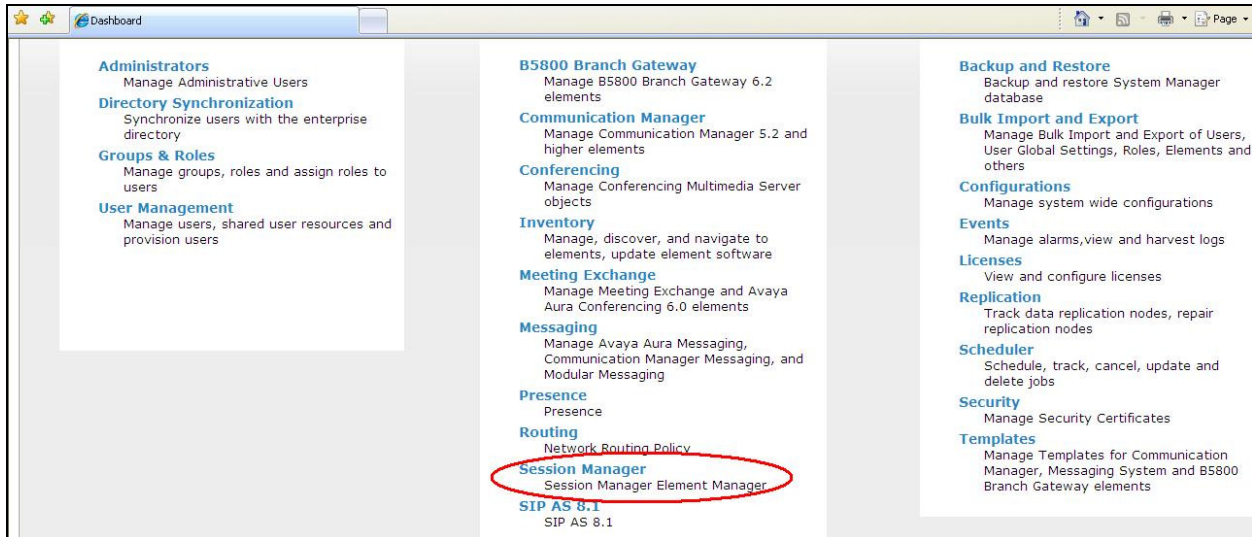
Telephony features, such as Call Waiting and Call Forwarding, can be programmed by entering feature codes on the handset. Please refer to the **Suppl. Serv.** tab in **Section 8.3** above.

9. Verification Steps

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

9.1. 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 **3010**, **3011** and **3012** highlighted.

Application Configuration	Details	Address	Login Name	First Name	Last Name	Location	IP Address	AST Device	Registered		
									Prim	Sec	S
System Status	Show	2000@devcon.avaya	2000@devcon.avaya	EXT2000	SIP	DevconLAB	192.168.50.170:5060	<input checked="" type="checkbox"/>	(AC)	<input type="checkbox"/>	<input type="checkbox"/>
	Show	3010@devcon.avaya	3010@devcon.avaya	DECT3010	Ascom	DevconLAB	192.168.50.100:2057	<input checked="" type="checkbox"/>	(AC)	<input type="checkbox"/>	<input type="checkbox"/>
	Show	3011@devcon.avaya	3011@devcon.avaya	DECT3011	Ascom	DevconLAB	192.168.50.100:2058	<input checked="" type="checkbox"/>	(AC)	<input type="checkbox"/>	<input type="checkbox"/>
	Show	---	3001@devcon.avaya	DECT3001	Ascom	DevconLAB	---	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>
	Show	---	3003@devcon.avaya	DECT3003	Ascom	DevconLAB	---	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>
	Show	---	3000@devcon.avaya	DECT3000	Ascom	DevconLAB	---	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>
	Show	---	3008@devcon.avaya	WLESS3008	Ascom	DevconLAB	---	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>
	Show	---	3006@devcon.avaya	WLESS3006	Ascom	DevconLAB	---	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>
	Show	---	3005@devcon.avaya	WLESS3005	Ascom	DevconLAB	---	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>
	Show	---	3007@devcon.avaya	WLESS3007	Ascom	DevconLAB	---	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>
	Show	3012@devcon.avaya	3012@devcon.avaya	DECT3012	Ascom	DevconLAB	192.168.50.100:2059	<input checked="" type="checkbox"/>	(AC)	<input type="checkbox"/>	<input type="checkbox"/>
	Show	---	3002@devcon.avaya	DECT3002	Ascom	DevconLAB	---	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>

9.2. Ascom DECT Registration

To verify that Ascom DECT Handsets are registered to the Ascom Base Station correctly click on **Users** in the left column and select the **Users** tab in the displayed window. Select **show** highlighted below, this displays the DECT handsets that are registered in the example below extensions **3010** and **3012** are registered correctly.



IP-DECT Base Station

Configuration: **Users** | Anonymous

General

LAN: PARK 31100363521040

IP: PARK 3rd pty 2110025026

LDAP: Master Id 0

DECT: **show**

VoIP: new

UNITE: import

Central Phonebook: export

Administration

Users

Device Overview

DECT Sync

Traffic

Gateway

User Administrators

Long Name Name

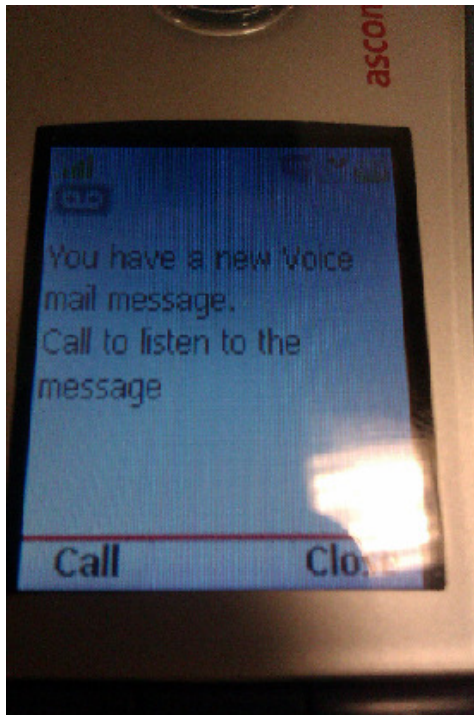
User Administrators: 0

Users

Long Name	Name	No	Fty	Display	IPEI / IPDI	AC	Prod	SW	Registration
DECT 1 3010	extn3010	3010	+	DECT 1 3010	036470757152		d62-Talker	3.0.9	192.168.50.16
DECT 2 3011	extn3011	3011	+	DECT 2 3011	002020818098				Subscribed
DECT 3 3012	extn3012	3012	+	DECT 3 3012	036470762236		d41-Basic	3.0.6	192.168.50.16

Users: 3, Registrations: 2

Check that MWI is working by leaving a voicemail for the DECT user. Once a voicemail message has been left the following message should appear on the DECT handset.



10. Conclusion

These Application Notes describe the configuration steps required for Ascom's DECT IP Base Station and DECT Handsets to successfully interoperate with Avaya Aura® Communication Manager and Avaya Aura® Session Manager by registering the Ascom Handsets with 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

Ascom's technical documentation is available through a local supplier. Please see a list of the documentation used for these Application Notes.

- [6] *Installation and Operation Manual IP-DECT Base Station and IP-DECT Gateway (software version 5.1.x) (TD 92579EN)*
- [7] *System Description Ascom IP-DECT System (TD 92375EN)*
- [8] *System Planning Ascom IP-DECT System (TD 92422EN)*

©2013 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.