Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Ascom i62 Wireless Handsets 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 Ascom's i62 Wireless 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 i62 Wireless handsets to interoperate with Avaya Aura® Communication Manager R6.3 and Avaya Aura® Session Manager R6.3. Ascom's i62 handsets are configured to register with Avaya Aura® Session Manager and are also configured on Avaya Aura® Communication Manager as 9620 SIP endpoints. The Ascom i62 handsets then behave as third-party SIP extensions on Avaya Aura® Communication Manager able to make/receive internal and PSTN/external calls and have full voicemail and other telephony facilities available on Avaya Aura® Communication Manager.

2. General Test Approach and Test Results

The interoperability compliance testing evaluates the ability of Ascom i62 Wireless sets to make and receive calls to and from Avaya H.323, SIP deskphones, and PSTN endpoints. Avaya Aura® Messaging was used to allow users leave voicemail messages and to demonstrate Message Waiting Indication and DTMF 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 i62 endpoints and PSTN endpoints.

- Basic Calls
- Hold and Retrieve
- Attended and Blind Transfer
- Call Forwarding Unconditional, No Reply and Busy
- 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 i62 handsets and Session Manager fails. All compliance testing was done using UDP and TCP as the transport protocol.

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 i62 wireless handsets 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 i62 Wireless Handsets connect to the Wireless router which is placed on the LAN. The i62 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.

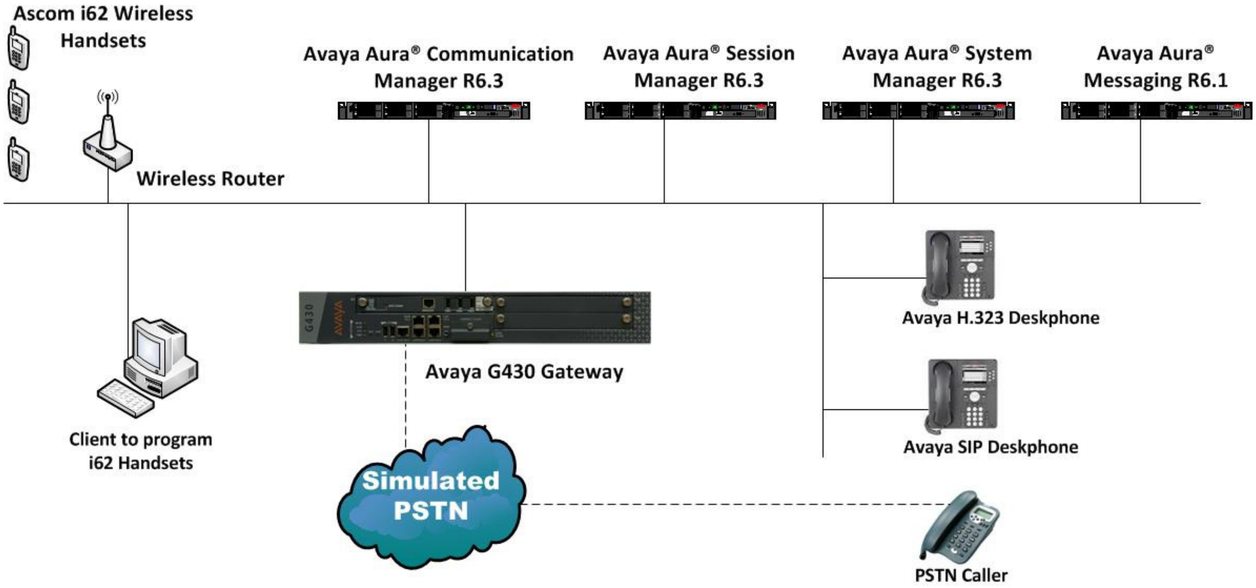

Ascom i62 Wireless Handsets
Avaya Aura® Communication Manager R6.3
Avaya Aura® Session Manager R6.3
Avaya Aura® System Manager R6.3
Avaya Aura® Messaging R6.1
Wireless Router
Avaya G430 Gateway
Avaya H.323 Deskphone
Avaya SIP Deskphone
Client to program i62 Handsets
Simulated PSTN
PSTN Caller

Figure 1: Network Solution of Ascom i62 Wireless 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 S8800 Server	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 S8800 Server	R6.3 SP1 R016x.03.0.124.0
Avaya Aura® Session Manager running on an Avaya S8800 Server	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
Ascom Device Manager Platform	MS XP Professional SP3
Ascom Device Manager	3.8.1
Ascom i62 Telephone	v. 4.3.16

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

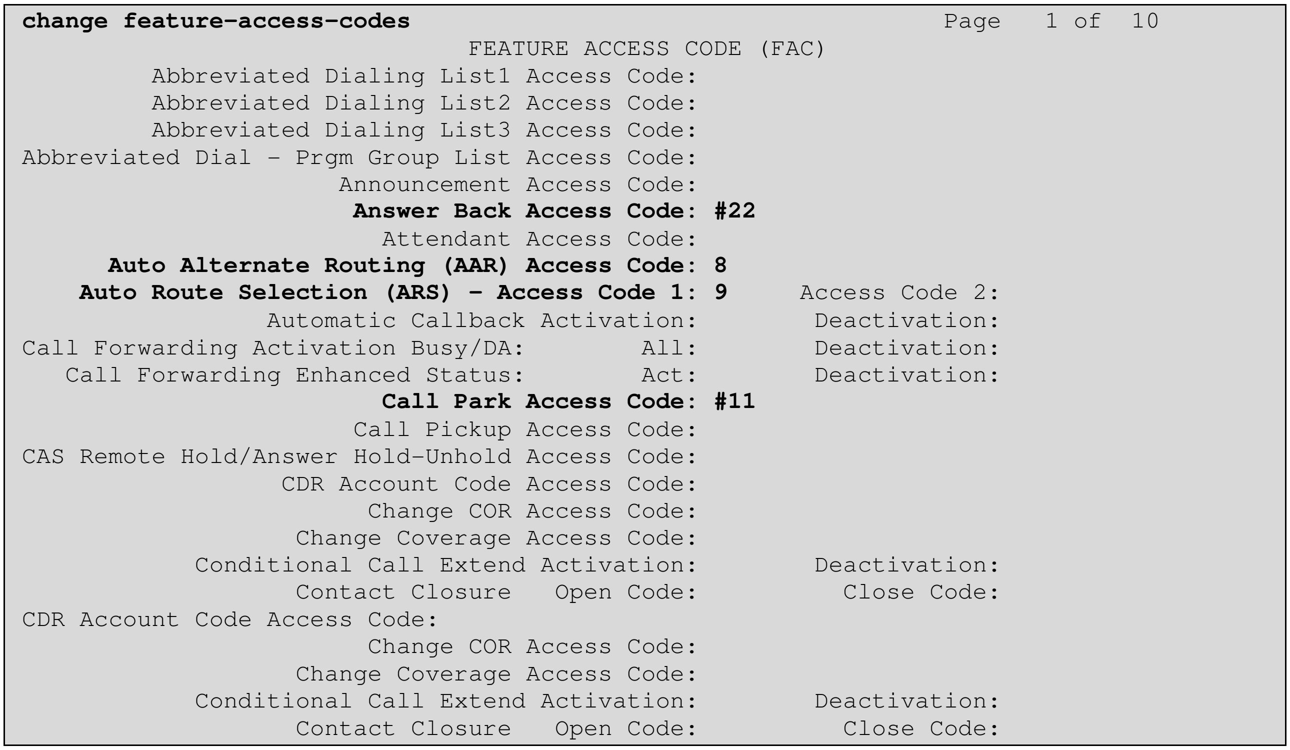
Use the **change dialplan analysis** command to configure the dial plan using the parameters shown below. Extension numbers (**ext**) are those beginning with **2**, **3**, **4** and **5**. Feature Access Codes (**fac**) use digits **8** and **9** or **#**.

```
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 feature 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.

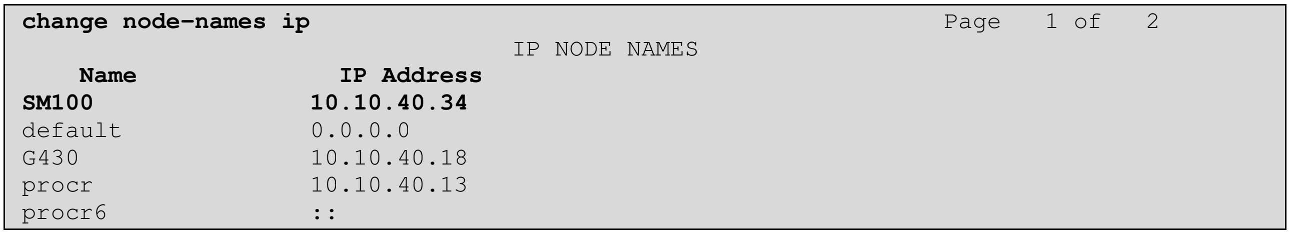
Answer Back Access Code	**:**	**#22**
Auto Alternate Routing (AAR) Access Code	**:**	**8**
Auto Route Selection (ARS) - Access Code 1	**:**	**9**
Call Park Access Code	**:**	**#11**



```
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 and 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 **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                10.10.40.18
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 6.1** 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-Set

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 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 pilot number for Messaging and on **Page 2 Message Center** is set to **sip-adjunct,** and both **Voice Mail Number** and **Voice Mail Handle** were set to **5999**.

```
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
```

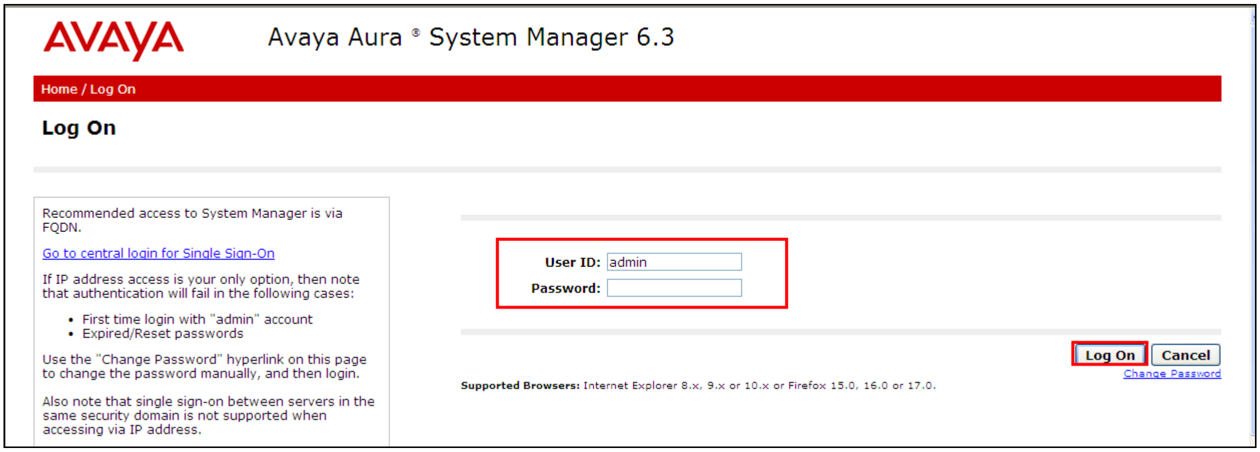
```
display hunt-group 59                                              Page   2 of  60
                                  HUNT GROUP

                      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

The Ascom i62 Wireless Handsets are added to Session Manager as SIP Users. In order to 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.



AVAYA Avaya Aura ® System Manager 6.3

Home / Log On

Log On

Recommended access to System Manager is via FQDN.

Go to central login for Single Sign-On

If IP address access is your only option, then note that authentication will fail in the following cases:

- First time login with "admin" account
- Expired/Reset passwords

Use the "Change Password" hyperlink on this page to change the password manually, and then login.

Also note that single sign-on between servers in the same security domain is not supported when accessing via IP address.

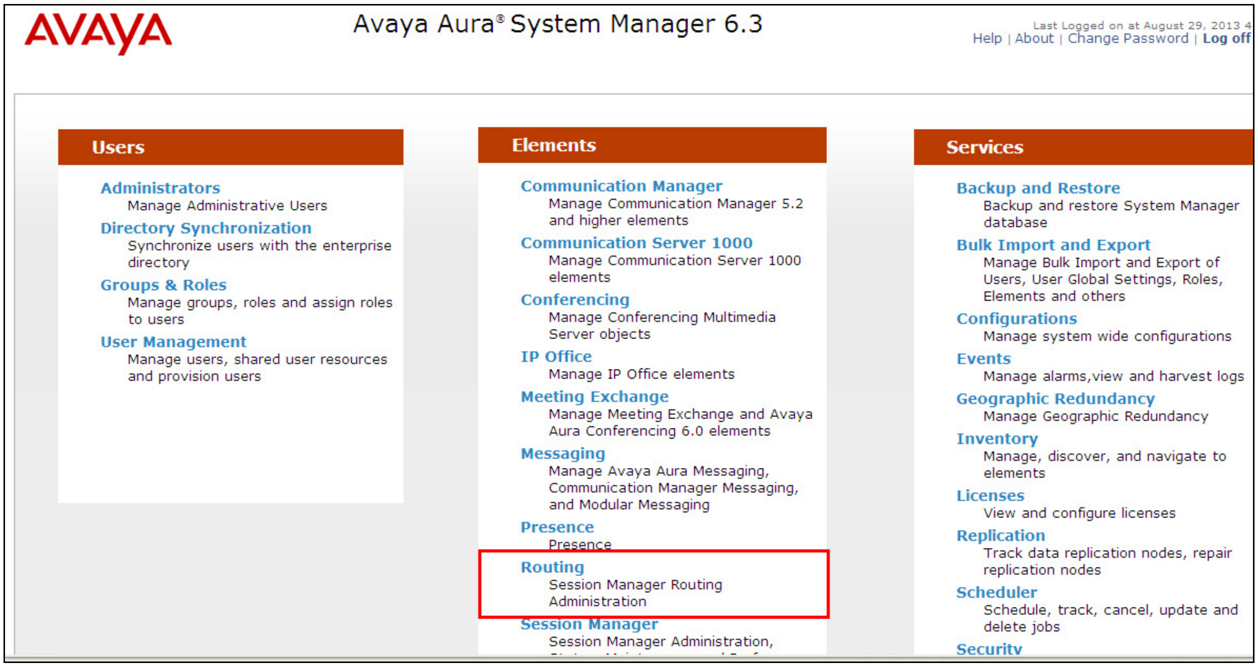
User ID: admin
Password:

Log On | Cancel

Change Password

Supported Browsers: Internet Explorer 8.x, 9.x or 10.x or Firefox 15.0, 16.0 or 17.0.

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



AVAYA Avaya Aura® System Manager 6.3

Last Logged on at August 29, 2013 4
Help | About | Change Password | Log off

Users

Administrators
Manage Administrative Users

Directory Synchronization
Synchronize users with the enterprise directory

Groups & Roles
Manage groups, roles and assign roles to users

User Management
Manage users, shared user resources and provision users

Elements

Communication Manager
Manage Communication Manager 5.2 and higher elements

Communication Server 1000
Manage Communication Server 1000 elements

Conferencing
Manage Conferencing Multimedia Server objects

IP Office
Manage IP Office elements

Meeting Exchange
Manage Meeting Exchange and Avaya Aura Conferencing 6.0 elements

Messaging
Manage Avaya Aura Messaging, Communication Manager Messaging, and Modular Messaging

Presence
Presence

Routing
Session Manager Routing Administration

Session Manager
Session Manager Administration,

Services

Backup and Restore
Backup and restore System Manager database

Bulk Import and Export
Manage Bulk Import and Export of Users, User Global Settings, Roles, Elements and others

Configurations
Manage system wide configurations

Events
Manage alarms,view and harvest logs

Geographic Redundancy
Manage Geographic Redundancy

Inventory
Manage, discover, and navigate to elements

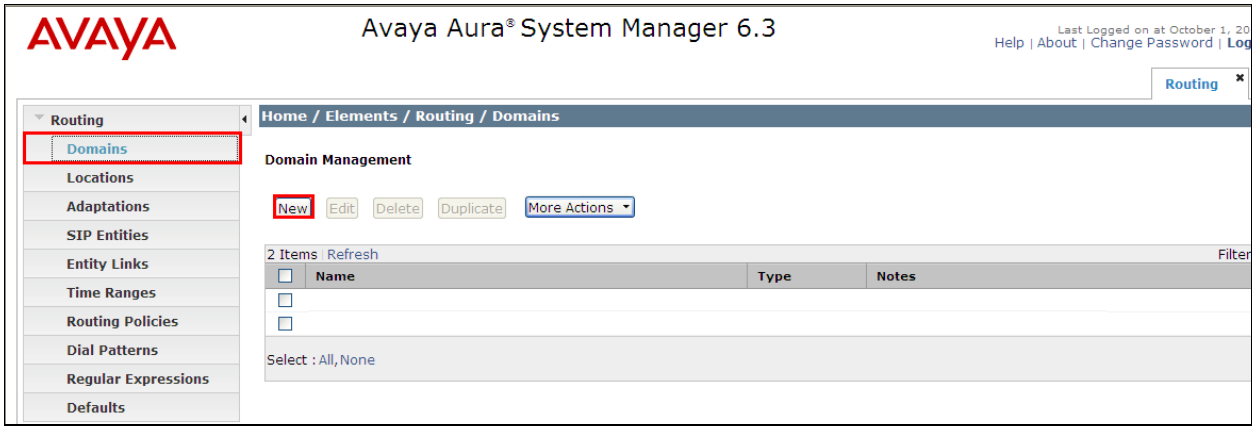
Licenses
View and configure licenses

Replication
Track data replication nodes, repair replication nodes

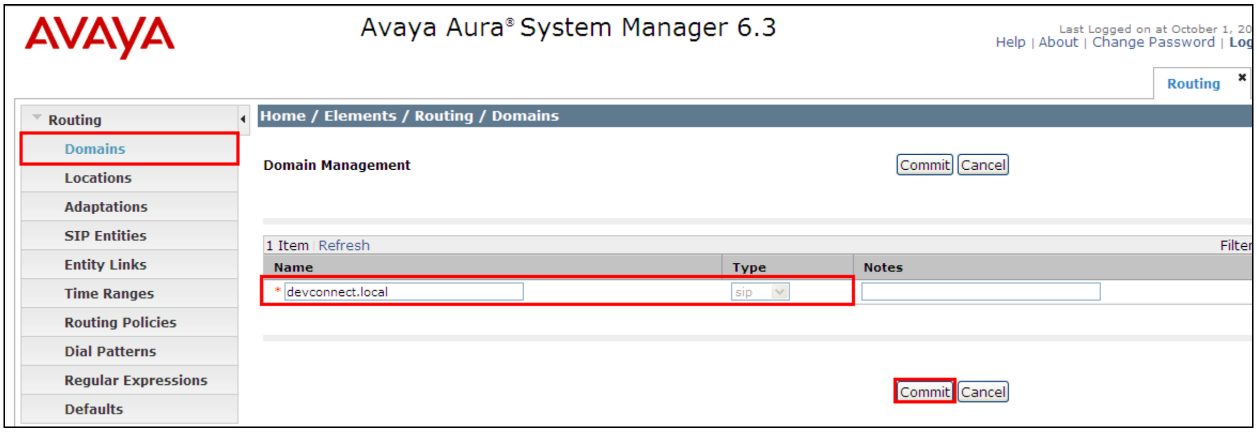
Scheduler
Schedule, track, cancel, update and delete jobs

Security

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



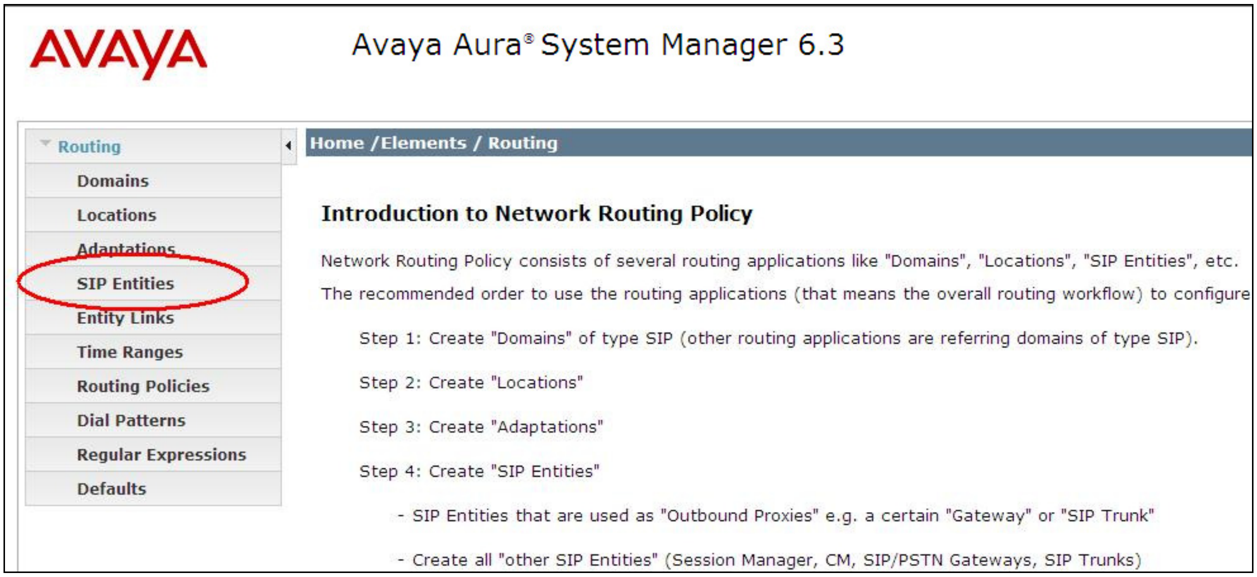
Note the domain **Name** used in the compliance testing was **devconnect.local**. Note this domain is also referenced in **Section 5.4**. Once the domain name is entered click on **Commit** to save this.



Name	Type	Notes
* devconnect.local	sip	

6.2. Configuration of SIP Entities

Log into System Manager as described in **Section 6.1** above, click on **SIP Entities** highlighted below.



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"

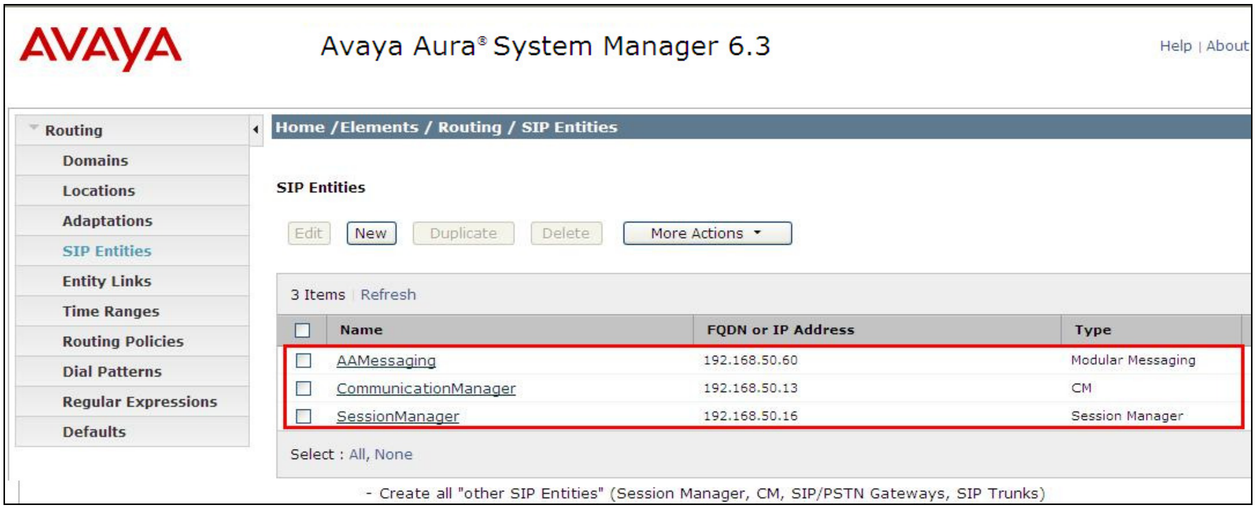
Step 4: Create "SIP Entities"

- 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 present for the Compliance Testing of Ascom i62 Wireless Handsets.

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

Note: There is no SIP Entity present or required for Ascom.



SIP Entities

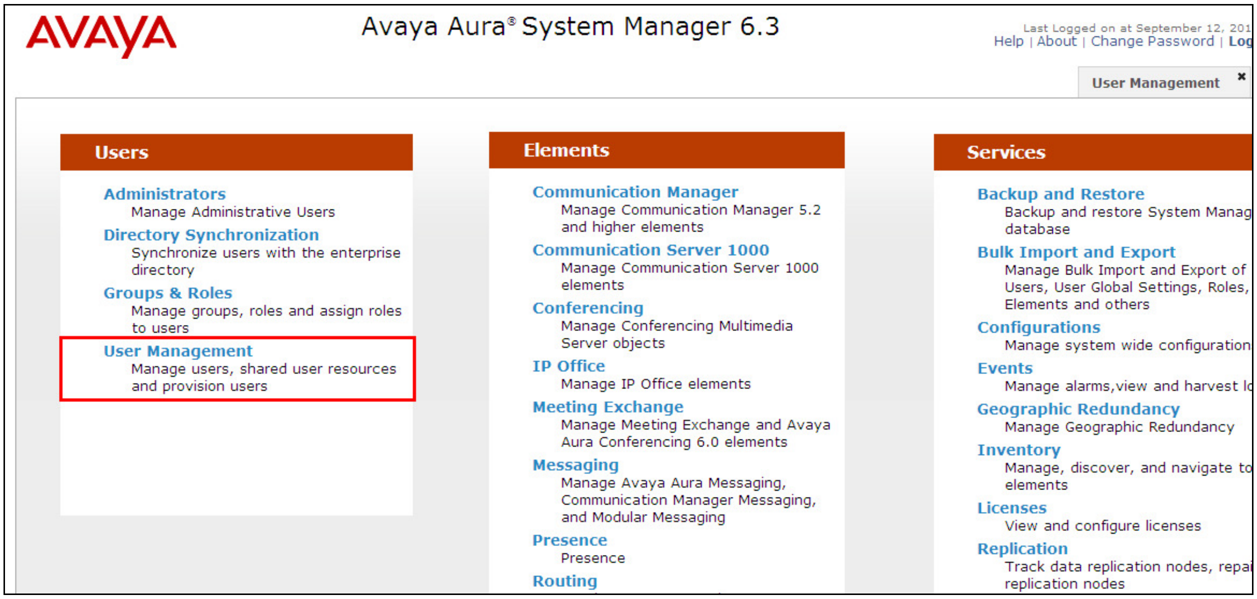
3 Items

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

- Create all "other SIP Entities" (Session Manager, CM, SIP/PSTN Gateways, SIP Trunks)

6.3. Adding Ascom SIP Users

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



AVAYA Avaya Aura® System Manager 6.3

Last Logged on at September 12, 201
Help | About | Change Password | Log

User Management ✖

Users

Administrators
Manage Administrative Users

Directory Synchronization
Synchronize users with the enterprise directory

Groups & Roles
Manage groups, roles and assign roles to users

User Management
Manage users, shared user resources and provision users

Elements

Communication Manager
Manage Communication Manager 5.2 and higher elements

Communication Server 1000
Manage Communication Server 1000 elements

Conferencing
Manage Conferencing Multimedia Server objects

IP Office
Manage IP Office elements

Meeting Exchange
Manage Meeting Exchange and Avaya Aura Conferencing 6.0 elements

Messaging
Manage Avaya Aura Messaging, Communication Manager Messaging, and Modular Messaging

Presence
Presence

Routing

Services

Backup and Restore
Backup and restore System Manag database

Bulk Import and Export
Manage Bulk Import and Export of Users, User Global Settings, Roles, Elements and others

Configurations
Manage system wide configuration

Events
Manage alarms,view and harvest l

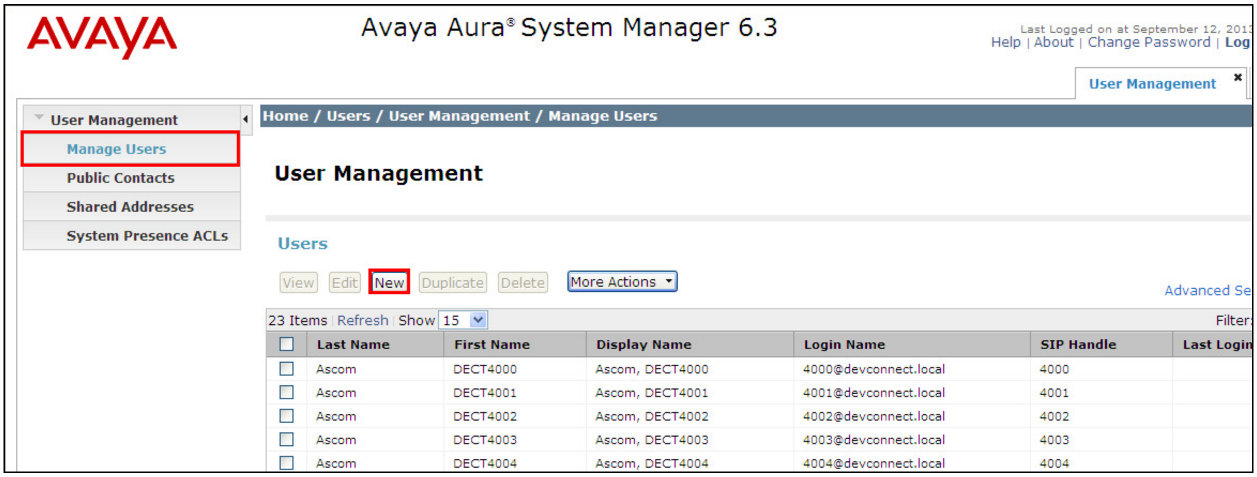
Geographic Redundancy
Manage Geographic Redundancy

Inventory
Manage, discover, and navigate to elements

Licenses
View and configure licenses

Replication
Track data replication nodes, repai replication nodes

Click on **Manage Users**. Click on **New** highlighted to add a new SIP user.



AVAYA Avaya Aura® System Manager 6.3

Last Logged on at September 12, 201
Help | About | Change Password | Log

User Management ✖

User Management
- Manage Users
- Public Contacts
- Shared Addresses
- System Presence ACLs

Home / Users / User Management / Manage Users

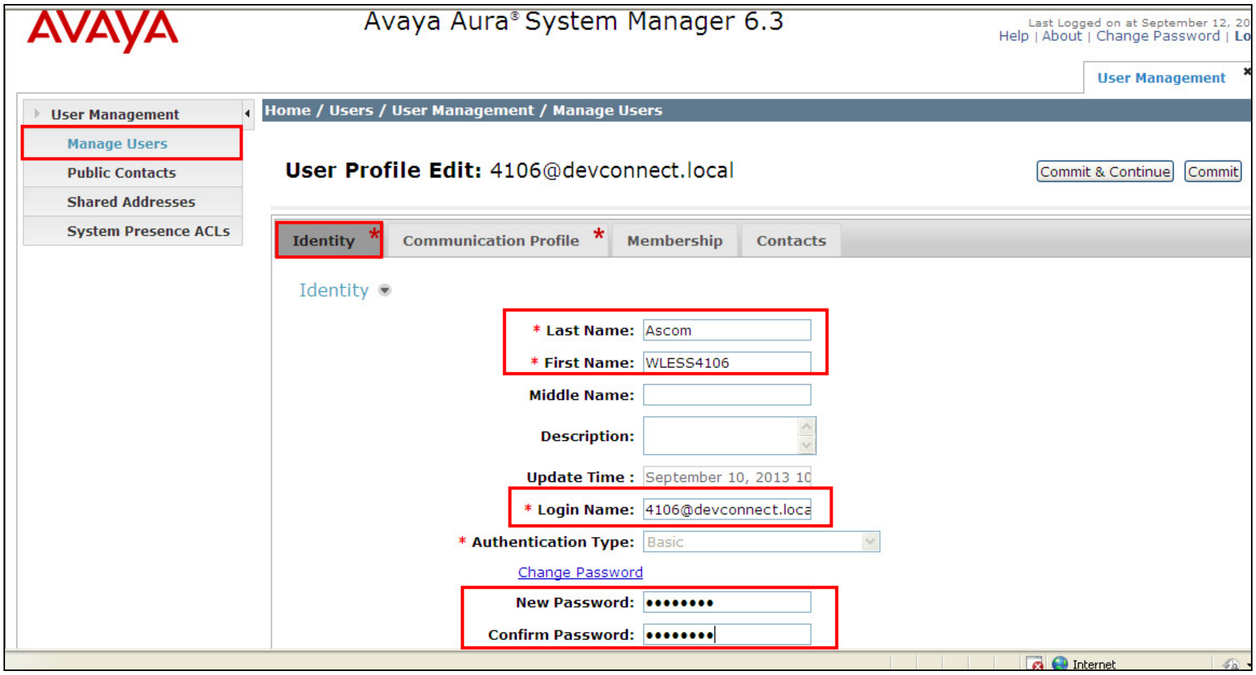
User Management

Users

23 Items | Refresh | Show 15 Filter:

□	Last Name	First Name	Display Name	Login Name	SIP Handle	Last Login
□	Ascom	DECT4000	Ascom, DECT4000	4000@devconnect.local	4000	
□	Ascom	DECT4001	Ascom, DECT4001	4001@devconnect.local	4001	
□	Ascom	DECT4002	Ascom, DECT4002	4002@devconnect.local	4002	
□	Ascom	DECT4003	Ascom, DECT4003	4003@devconnect.local	4003	
□	Ascom	DECT4004	Ascom, DECT4004	4004@devconnect.local	4004	

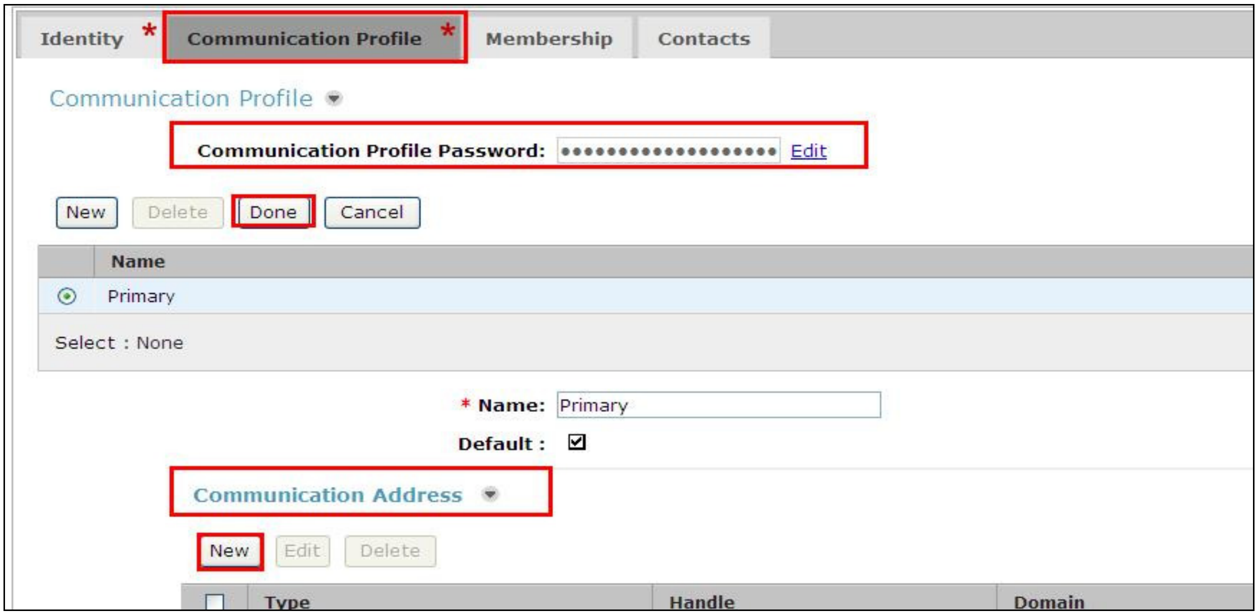
Under the **Identity** tab fill in the user's **Last Name** and **First Name** as shown below. Enter the **Login Name** and ensure **Authentication Type** is set to **Basic**. Enter a suitable **Password**.



User Profile Edit: 4106@devconnect.local

* Last Name: Ascom
* First Name: WLESS4106
Middle Name:
Description:
Update Time : September 10, 2013 10
* Login Name: 4106@devconnect.loca
* Authentication Type: Basic
New Password: ••••••••
Confirm 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 Ascom handset in **Section 8**. Click on **New** to add a new **Communication Address**.



Communication Profile Password: •••••••••••••••••••

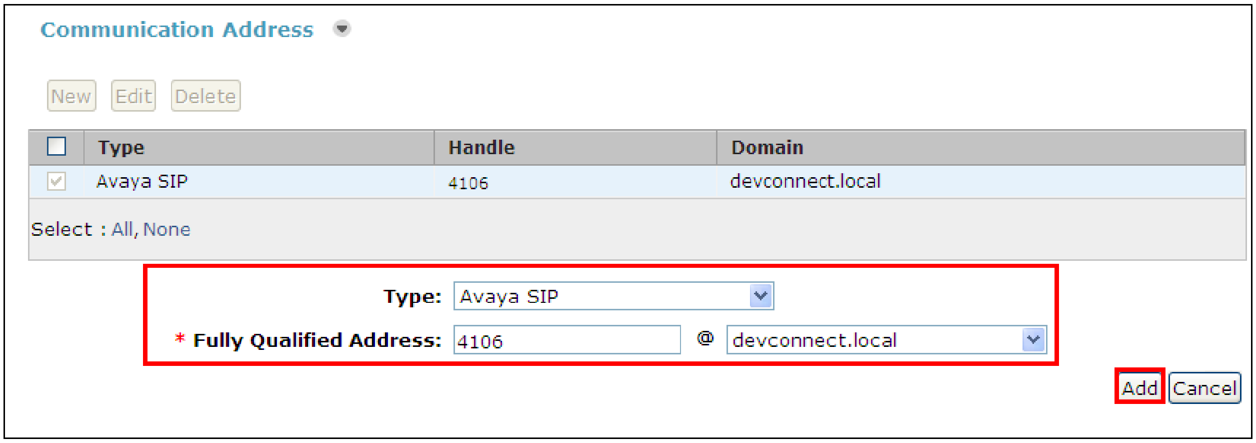
	Name
●	Primary

Select : None

* Name: Primary
Default : ☑

□	Type	Handle	Domain

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



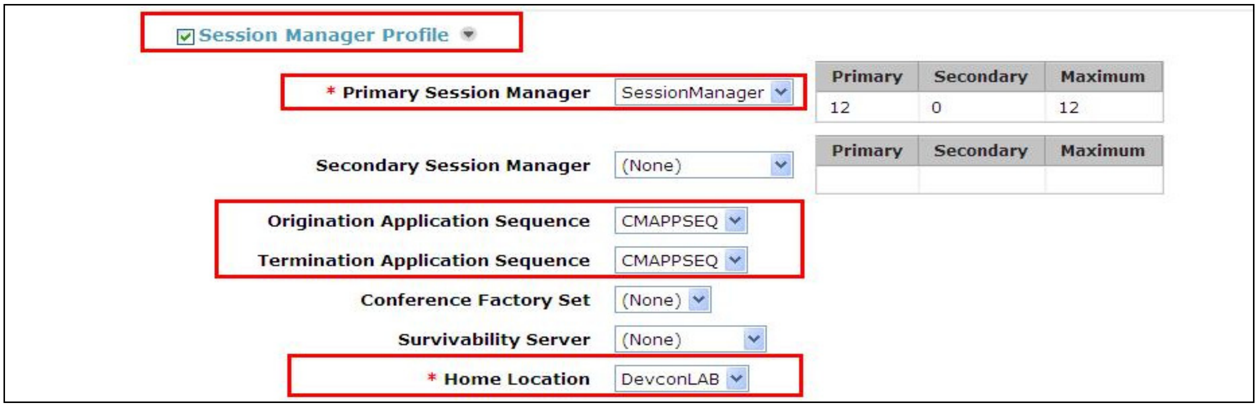
☐	Type	Handle	Domain
☑	Avaya SIP	4106	devconnect.local

Select : All, None

Type: Avaya SIP

* Fully Qualified Address: 4106 @ devconnect.local

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. Note that **CMAPPSEQ** is an application sequence that corresponds to the Communication Manager in the test configuration and has been configured in the system previously.



* Primary Session Manager: SessionManager

Primary	Secondary	Maximum
12	0	12

Secondary Session Manager: (None)

Primary	Secondary	Maximum

Origination Application Sequence: CMAPPSEQ

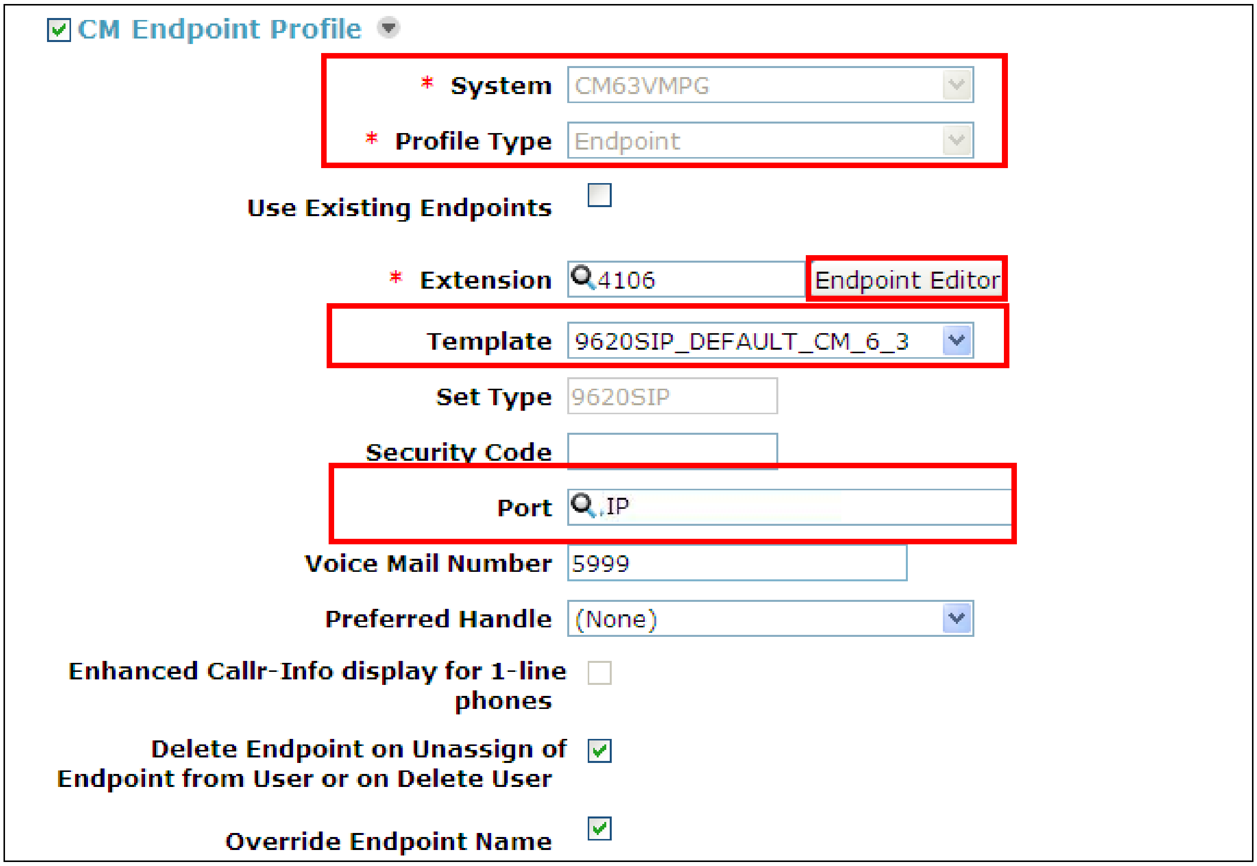
Termination Application Sequence: CMAPPSEQ

Conference Factory Set: (None)

Survivability Server: (None)

* Home Location: DevconLAB

Ensure that **CM Endpoint Profile** is selected and choose the **DEFAULT_9620SIP_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: 4106

Template: 9620SIP_DEFAULT_CM_6_3

Set Type: 9620SIP

Security Code:

Port: IP

Voice Mail Number: 5999

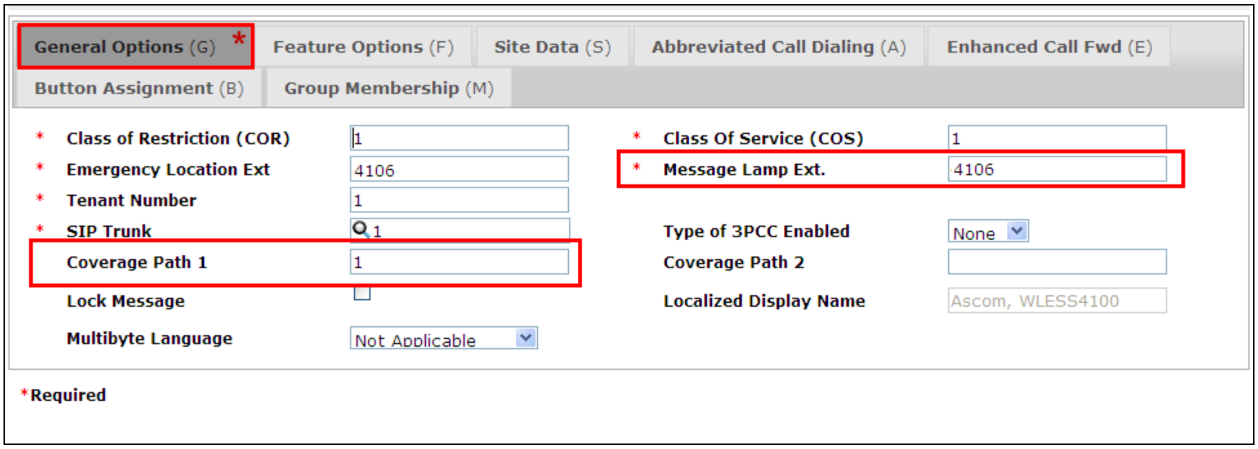
Preferred Handle: (None)

Enhanced Callr-Info display for 1-line phones: □

Delete Endpoint on Unassign of Endpoint from User or on Delete User: ☑

Override Endpoint Name: ☑

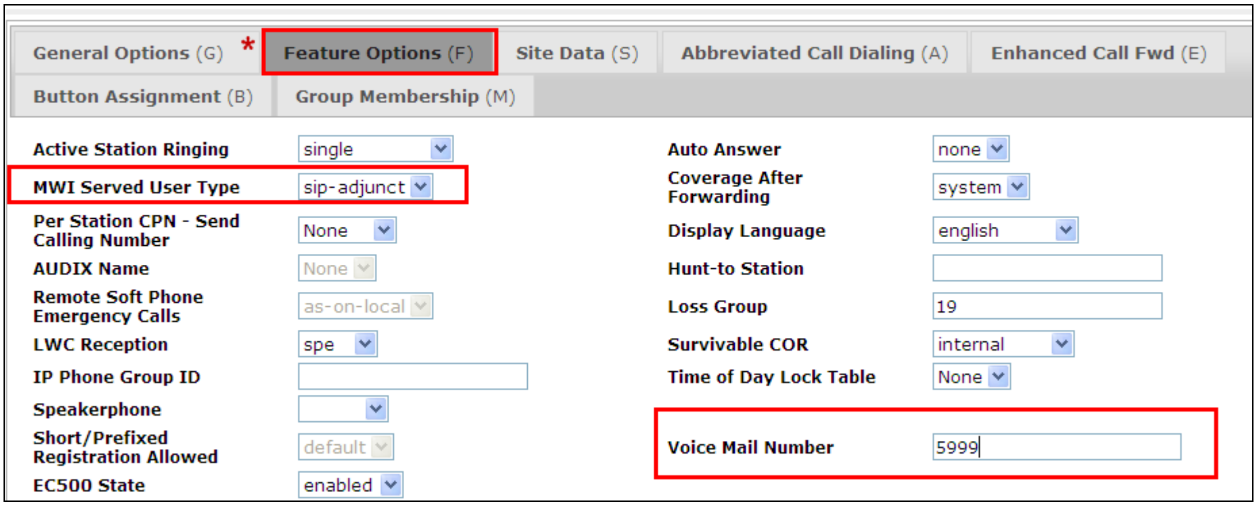
Under the **General Options** tab ensure that **Coverage Path 1** is set to that configured in **Section 5.6**. Also ensure that **Message Lamp Ext.** is showing the correct extension number.



* Class of Restriction (COR)	1	* Class Of Service (COS)	1
* Emergency Location Ext	4106	* Message Lamp Ext.	4106
* Tenant Number	1		
* SIP Trunk	1	Type of 3PCC Enabled	None
Coverage Path 1	1	Coverage Path 2	
Lock Message	□	Localized Display Name	Ascom, WLESS4100
Multibyte Language	Not Applicable		

*Required

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**.

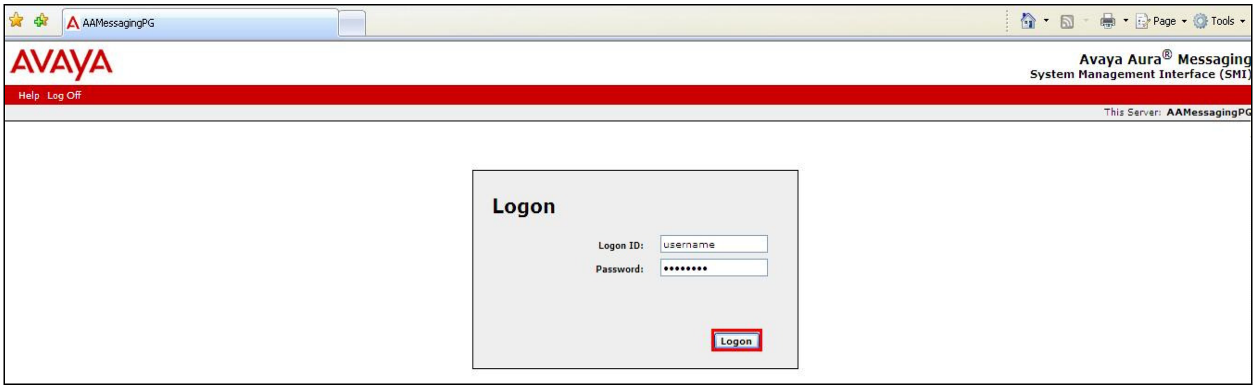


Active Station Ringing	single	Auto Answer	none
MWI Served User Type	sip-adjunct	Coverage After Forwarding	system
Per Station CPN - Send Calling Number	None	Display Language	english
AUDIX Name	None	Hunt-to Station	
Remote Soft Phone Emergency Calls	as-on-local	Loss Group	19
LWC Reception	spe	Survivable COR	internal
IP Phone Group ID		Time of Day Lock Table	None
Speakerphone			
Short/Prefixed Registration Allowed	default	Voice Mail Number	5999
EC500 State	enabled		

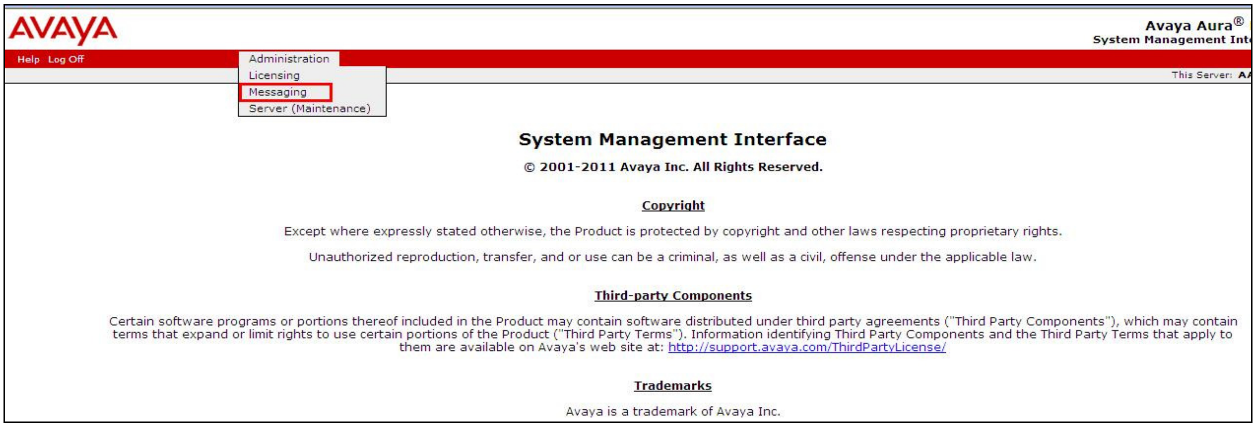
7. Configure Avaya Aura® Messaging

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.



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.

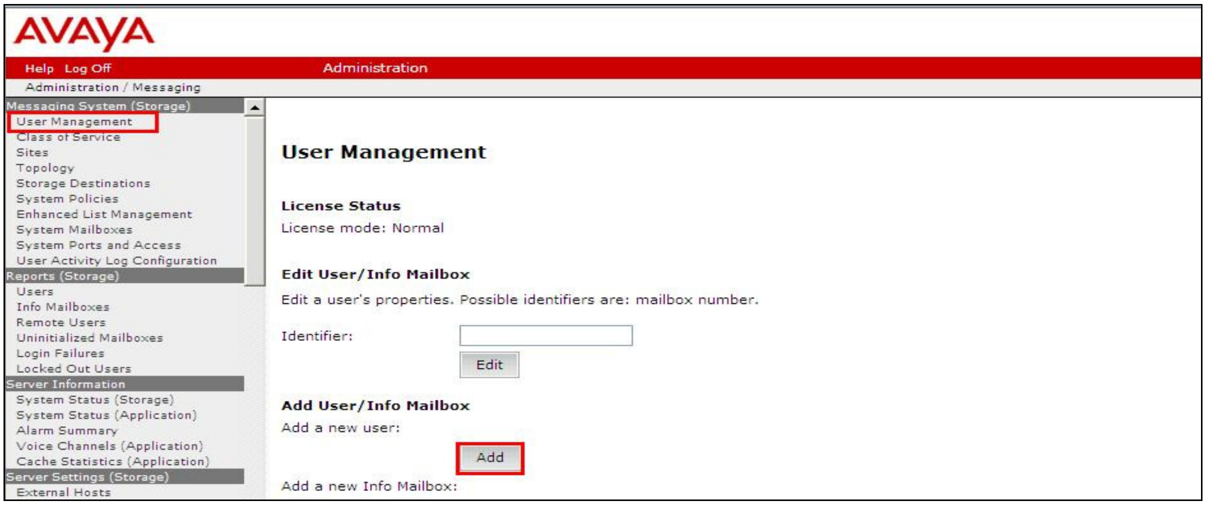
Third-party Components

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.



User Management

License Status

License mode: Normal

Edit User/Info Mailbox

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

Identifier:

Edit

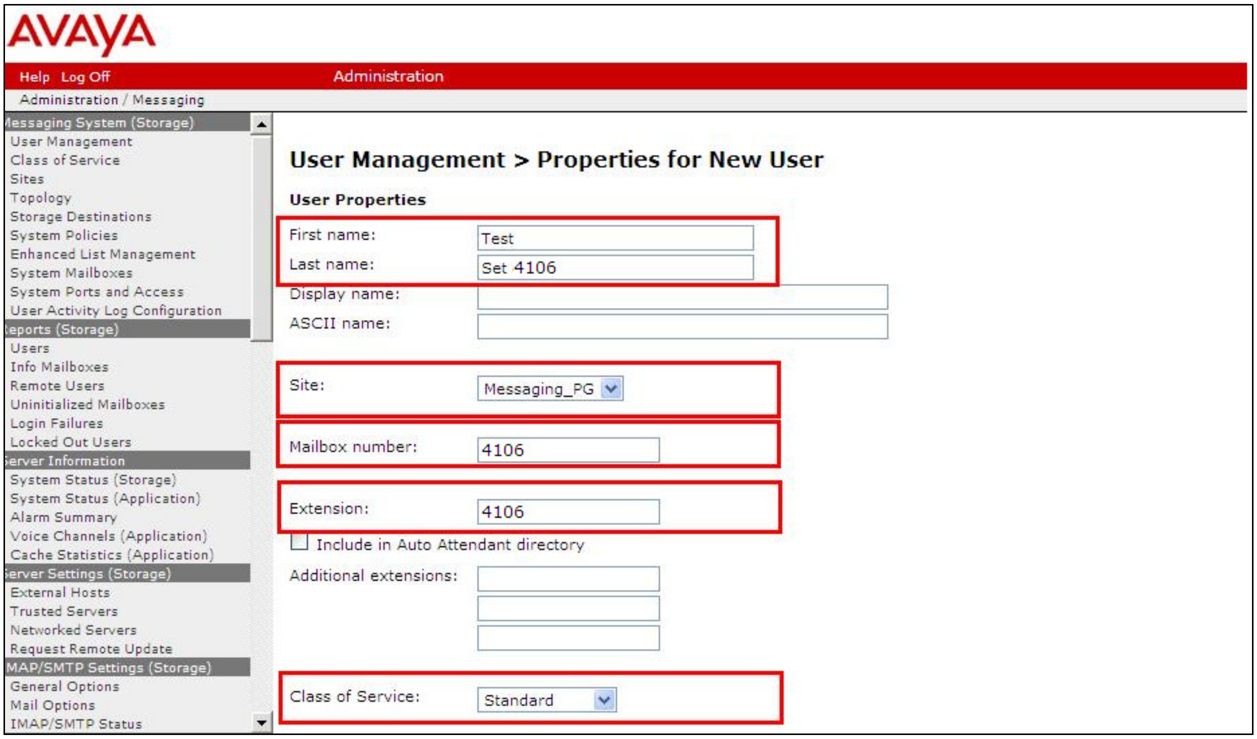
Add User/Info Mailbox

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**.



User Management > Properties for New User

User Properties

First name: Test

Last name: Set 4106

Display name:

ASCII name:

Site: Messaging_PG

Mailbox number: 4106

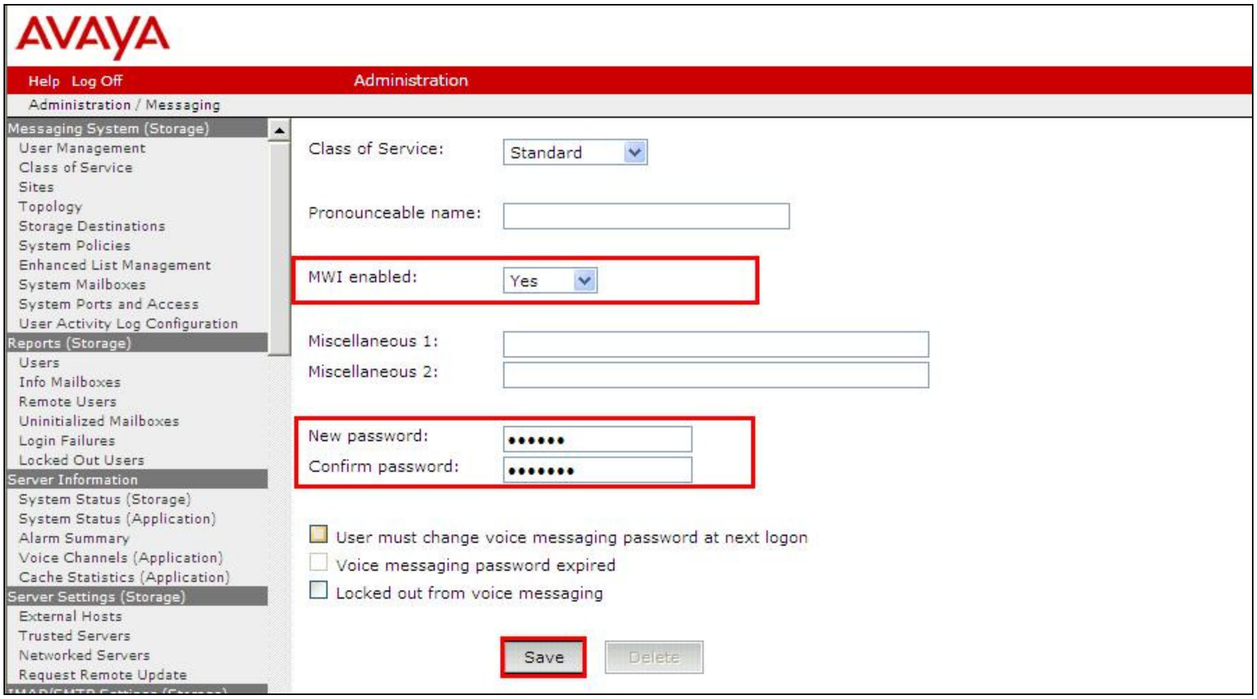
Extension: 4106

□ Include in Auto Attendant directory

Additional extensions:

Class of Service: Standard

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



Class of Service: Standard

Pronounceable name:

MWI enabled: Yes

Miscellaneous 1:

Miscellaneous 2:

New password: ••••••

Confirm password: •••••••

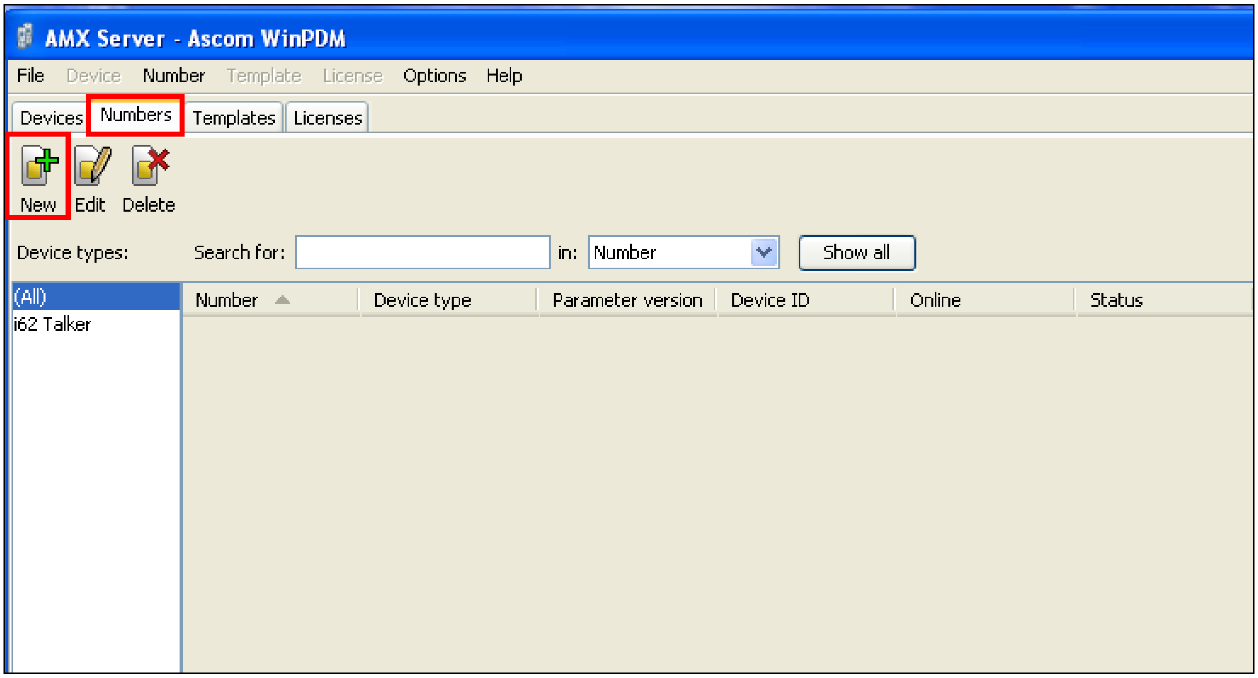
□ User must change voice messaging password at next logon

□ Voice messaging password expired

□ Locked out from voice messaging

8. Configure Ascom i62 Wireless Handsets

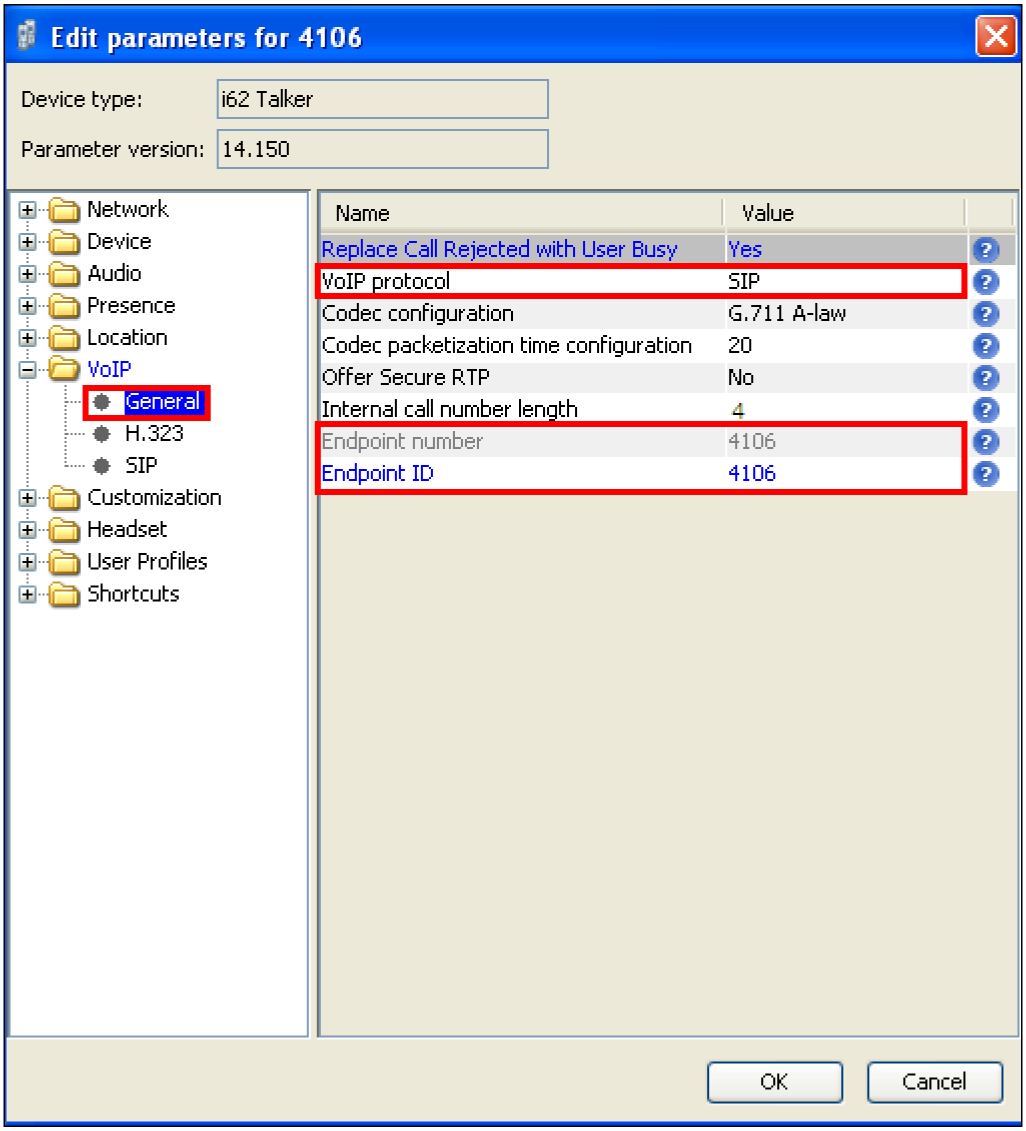
The configuration of the i62 Wireless handsets is done using Ascom's WinPDM software installed on a PC. Attach the Ascom DP1 USB Cradle to a PC on which the Ascom Device Manager (WinPDM) has been installed. Insert the handset to be configured in the DP1 USB Cradle, start the Ascom Device Manager, select the **Numbers** tab and click **New** icon highlighted below.



8.1. Configure SIP settings

Select **VoIP → General** from the left window. In the main window ensure the following are set.

Replace Call Rejected with User Busy	**Yes**
VoIP Protocol	**SIP**
Codec configuration	**G.711A-law** (as set in **Section 5.5**)
Codec packetization time	**20**
Internal call number length	**4**
Endpoint number	Ext number of set as set in **Section 6.3**
Endpoint ID	Ext number of set as set in **Section 6.3**



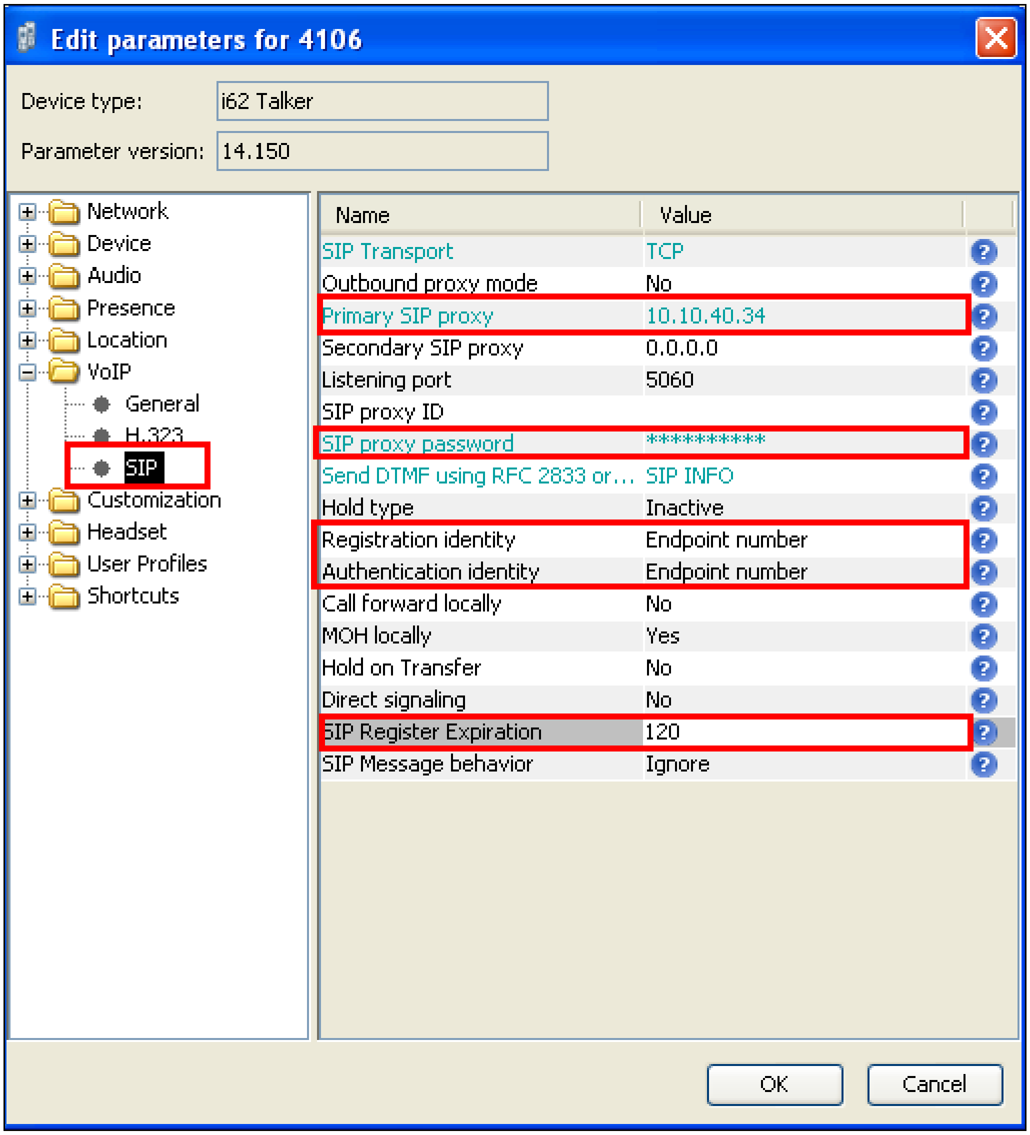
Device type: i62 Talker

Parameter version: 14.150

Name	Value
Replace Call Rejected with User Busy	Yes
VoIP protocol	SIP
Codec configuration	G.711 A-law
Codec packetization time configuration	20
Offer Secure RTP	No
Internal call number length	4
Endpoint number	4106
Endpoint ID	4106

Select the **VoIP→SIP** menu point, and enter the values shown below.

SIP proxy IP address	IP address of Session Manager
SIP proxy password	Password assigned to the endpoint in **Section 6.3**
Registration identity	Enter **Endpoint ID**
Authentication identity	Enter **Endpoint ID**
SIP Register Expiration	**120 (recommended** value)



Edit parameters for 4106

Device type: i62 Talker

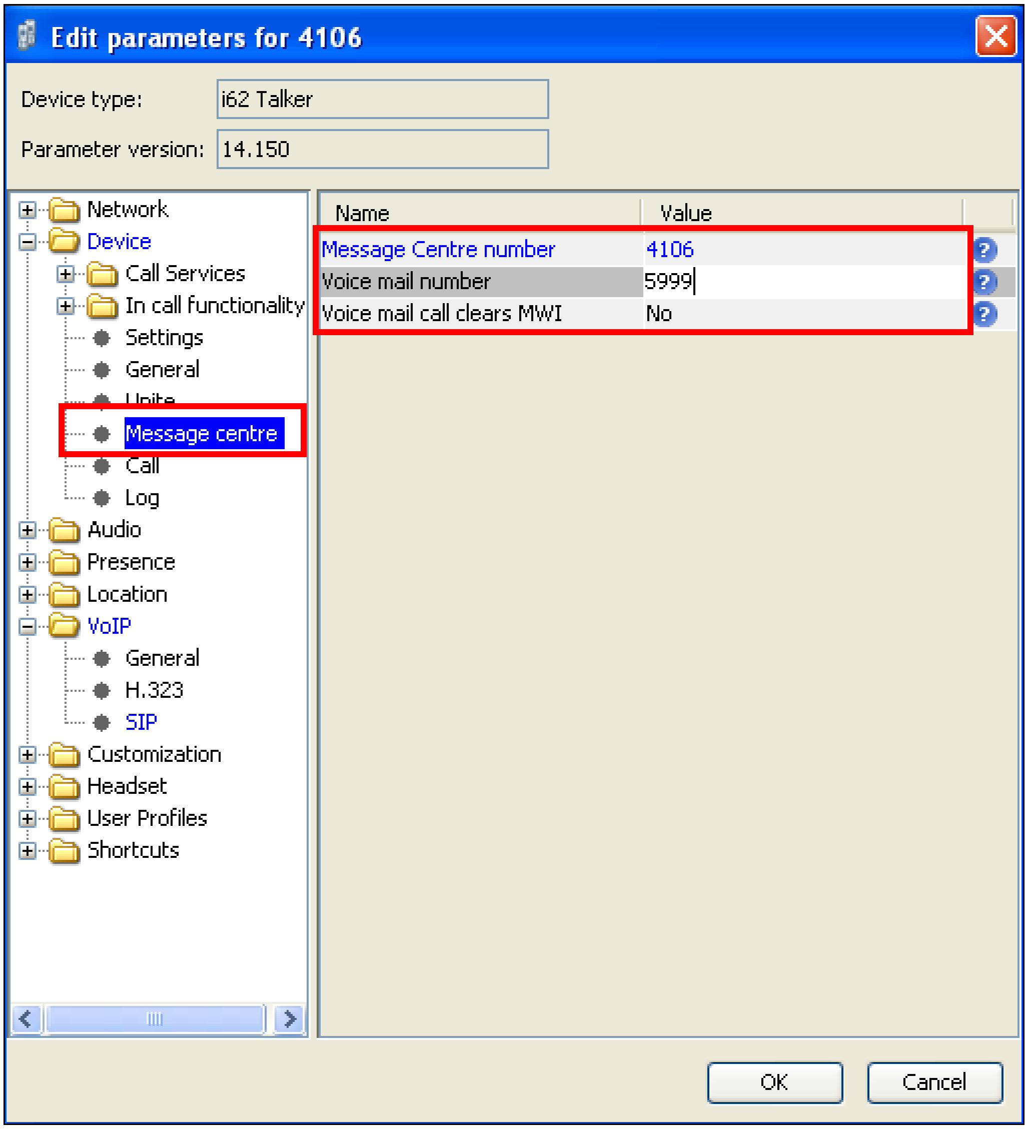
Parameter version: 14.150

Name	Value
SIP Transport	TCP
Outbound proxy mode	No
Primary SIP proxy	10.10.40.34
Secondary SIP proxy	0.0.0.0
Listening port	5060
SIP proxy ID	
SIP proxy password	***********
Send DTMF using RFC 2833 or…	SIP INFO
Hold type	Inactive
Registration identity	Endpoint number
Authentication identity	Endpoint number
Call forward locally	No
MOH locally	Yes
Hold on Transfer	No
Direct signaling	No
SIP Register Expiration	120
SIP Message behavior	Ignore

For further information about the Ascom i62 WiFi configurations please refer to Ascom's documentation in **Section 11** of these Application Notes. This section covers specific settings concerning SIP.

8.2. Configure Message Centre

Click on **Device → Message centre** in the left window. In the right window enter the **Voice mail number** as configured in **Section 5.6** and the **Message Centre number** which is the extension number of the handset.



Device type: i62 Talker

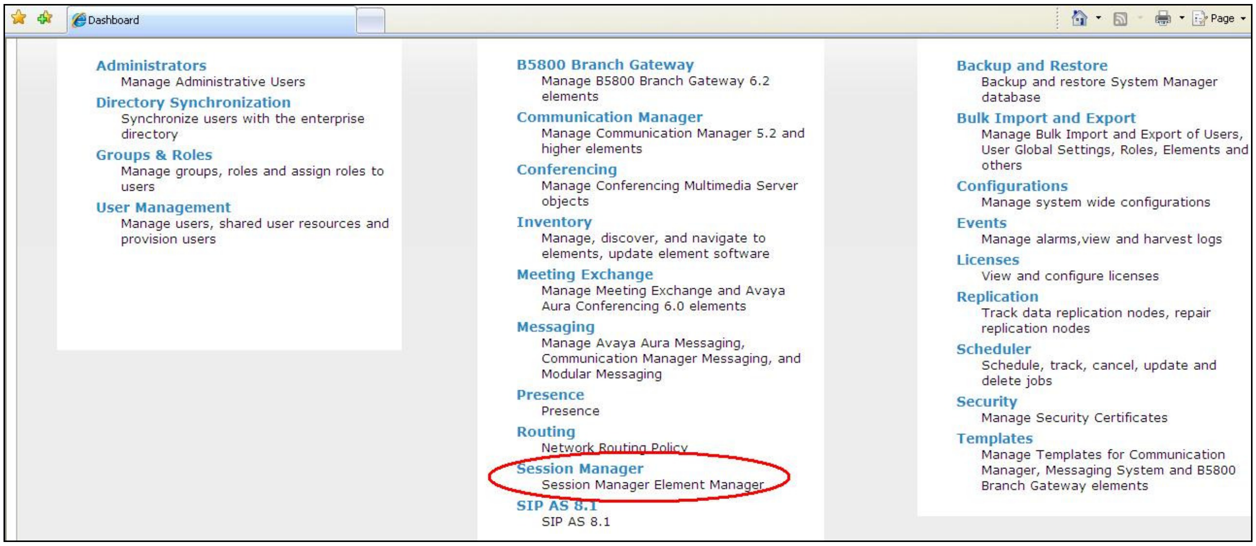
Parameter version: 14.150

Name	Value
Message Centre number	4106
Voice mail number	5999
Voice mail call clears MWI	No

9. Verification Steps

The following steps can be taken to ensure that connections between Ascom i62 handsets and Session Manager and Communication Manager are up.

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



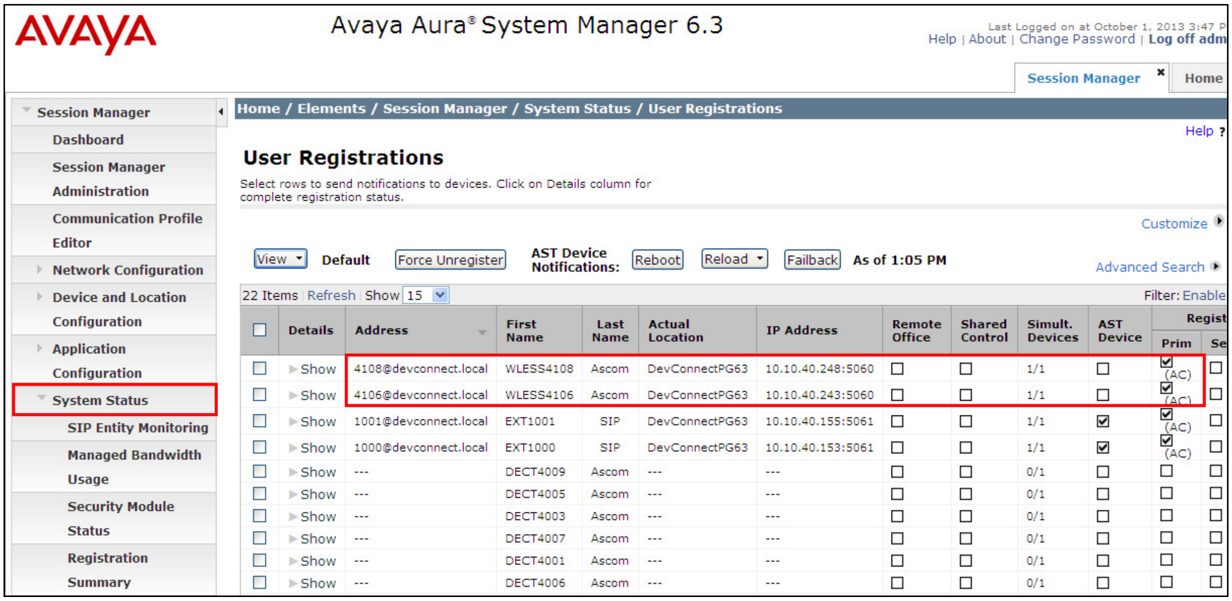
Dashboard

Administrators
Manage Administrative Users
Directory Synchronization
Synchronize users with the enterprise directory
Groups & Roles
Manage groups, roles and assign roles to users
User Management
Manage users, shared user resources and provision users

B5800 Branch Gateway
Manage B5800 Branch Gateway 6.2 elements
Communication Manager
Manage Communication Manager 5.2 and higher elements
Conferencing
Manage Conferencing Multimedia Server objects
Inventory
Manage, discover, and navigate to elements, update element software
Meeting Exchange
Manage Meeting Exchange and Avaya Aura Conferencing 6.0 elements
Messaging
Manage Avaya Aura Messaging, Communication Manager Messaging, and Modular Messaging
Presence
Presence
Routing
Network Routing Policy
Session Manager
Session Manager Element Manager
SIP AS 8.1
SIP AS 8.1

Backup and Restore
Backup and restore System Manager database
Bulk Import and Export
Manage Bulk Import and Export of Users, User Global Settings, Roles, Elements and others
Configurations
Manage system wide configurations
Events
Manage alarms,view and harvest logs
Licenses
View and configure licenses
Replication
Track data replication nodes, repair replication nodes
Scheduler
Schedule, track, cancel, update and delete jobs
Security
Manage Security Certificates
Templates
Manage Templates for Communication Manager, Messaging System and B5800 Branch Gateway elements

Select **System Status** and **User Registrations** in the left column. This displays the users that are currently registered with Session Manager. The i62 users should show as being registered as they are below for extensions **4106**and **4108** highlighted.



AVAYA Avaya Aura® System Manager 6.3

Last Logged on at October 1, 2013 3:47 P
Help | About | Change Password | Log off adm

Session Manager × Home

- Session Manager
  - Dashboard
  - Session Manager Administration
  - Communication Profile Editor
  - Network Configuration
  - Device and Location Configuration
  - Application Configuration
  - System Status
    - SIP Entity Monitoring
    - Managed Bandwidth Usage
    - Security Module Status
    - Registration Summary

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

Help ?

User Registrations

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

Customize

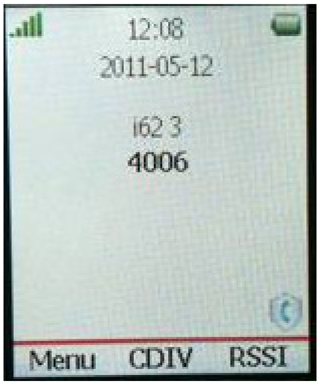
View ▾ Default Force Unregister AST Device Notifications: Reboot Reload ▾ Failback As of 1:05 PM

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	Regist	
											Prim	Se
□	▶ Show	4108@devconnect.local	WLESS4108	Ascom	DevConnectPG63	10.10.40.248:5060	□	□	1/1	□	☑ (AC)	□
□	▶ Show	4106@devconnect.local	WLESS4106	Ascom	DevConnectPG63	10.10.40.243:5060	□	□	1/1	□	☑ (AC)	□
□	▶ Show	1001@devconnect.local	EXT1001	SIP	DevConnectPG63	10.10.40.155:5061	□	□	1/1	☑	☑ (AC)	□
□	▶ Show	1000@devconnect.local	EXT1000	SIP	DevConnectPG63	10.10.40.153:5061	□	□	1/1	☑	☑ (AC)	□
□	▶ Show	---	DECT4009	Ascom	---	---	□	□	0/1	□	□	□
□	▶ Show	---	DECT4005	Ascom	---	---	□	□	0/1	□	□	□
□	▶ Show	---	DECT4003	Ascom	---	---	□	□	0/1	□	□	□
□	▶ Show	---	DECT4007	Ascom	---	---	□	□	0/1	□	□	□
□	▶ Show	---	DECT4001	Ascom	---	---	□	□	0/1	□	□	□
□	▶ Show	---	DECT4006	Ascom	---	---	□	□	0/1	□	□	□

The Ascom i62 handset connection to Session Manager can be verified by an absence of an error message on the handset display just above the red line at the bottom of the display, as shown in the following illustration, (note this is an example from a previous testing).



10. Conclusion

These Application Notes describe the configuration steps required for Ascom's i62 Wireless Handsets to successfully interoperate with Avaya Aura® Communication Manager R6.3 and Avaya Aura® Session Manager R6.3 by registering the Ascom 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

Please see below for a list of documentation used during the compliance testing information on Ascom i62 Wireless Handsets. A full list of Ascom's technical documentation is available through a local supplier. Please refer to **Section 2.3** of these Application Notes for information on Ascom support.

[5] *User Manual Ascom i62 VoWiFi Handset* (TD 92599EN)

[6] *Configuration Manual Ascom i62 VoWiFi Handset* (TD 92675EN)

[7] *System Description Ascom VoWiFi System* (TD 92313EN)

[8] *System Planning Ascom VoWiFi System* (TD 92408EN)

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.