Application Notes for configuring Ascom DECT Handsets and Ascom IPBS Access Point with Avaya Aura® Communication Manager R7.0 and Avaya Aura® Session Manager R7.0 – Issue 1.0

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.

Readers should pay particular attention to the scope of testing as outlined in Section 2.1, as well as observations noted in Section 2.2 to ensure that their own use cases are adequately covered by this scope and results.

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 R7.0 and Avaya Aura® Session Manager R7.0. Ascom's DECT handsets are configured to register with Session Manager via SIP and are also subscribed to the base station via DECT. Each handset is configured as a SIP user on Avaya Aura® Communication Manager as Avaya 9620 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 to leave voicemail messages and to demonstrate Message Waiting Indication was working on the Ascom handsets.

Ascom can use both UDP and TCP as the SIP transport protocol; however, 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 DECT master and standby base stations. The setup of a SIP Entity must use the "Endpoint Concentrator Connection Policy".

Starting with Session Manager Release 6.3.9, an "Endpoint Concentrator" can be selected as a SIP Entity type. This Endpoint Concentrator type, allows up to 1000 connections from a single IP address. The single IP address can be shared by multiple Windows instances running on a Virtualized server or multiple DECT handsets sharing the same base station IP address.

A new connection policy, Endpoint Concentrator, can be assigned to a SIP entity link. The Session Manager (ASSET) allows up to 1000 connections on that SIP entity link. The Endpoint Concentrator policy is an untrusted policy based on the current Default (endpoint) policy. That is, the requests arriving over the SIP entity link with the connection policy Endpoint Concentrator are challenged as for any other endpoint. To identify and administer the SIP entities hosting multiple endpoints, this release introduces a new entity type, Endpoint Concentrator.

Note: SIP Link Monitoring is not available for SIP entities of type Endpoint Concentrator.

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. A SIP Entity with “Endpoint Concentrator” assigned was setup for both the Master and Standby Base Stations, the corresponding TCP entity links need to be of type “untrusted”.

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.

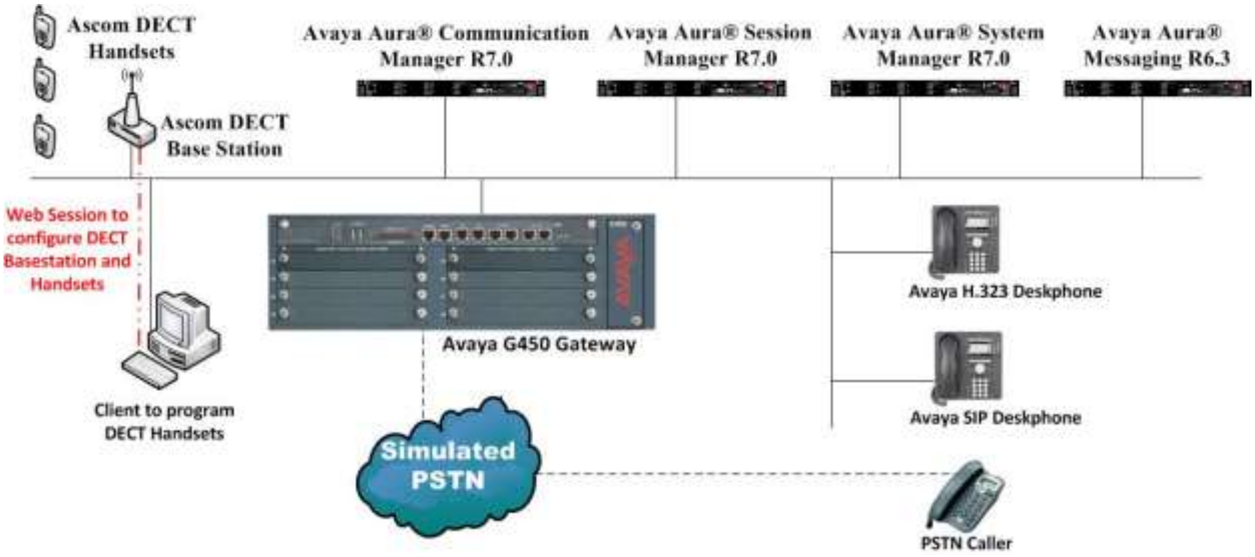

Ascom DECT Handsets
Ascom DECT Base Station
Avaya Aura® Communication Manager R7.0
Avaya Aura® Session Manager R7.0
Avaya Aura® System Manager R7.0
Avaya Aura® Messaging R6.3
Web Session to configure DECT Basestation and Handsets
Avaya G450 Gateway
Avaya H.323 Deskphone
Avaya SIP Deskphone
Client to program DECT Handsets
Simulated PSTN
PSTN Caller

Figure 1: Network Solution of Ascom DECT Handsets with Avaya Aura® Communication Manager R7.0 and Avaya Aura® Session Manager R7.0

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya Aura® System Manager running on Virtual Server	R7.0.0.0.0 Build 7.0.0.0.16266-7.0.9.9.902 SW Update Revision No. 7.0.0.0.3873
Avaya Aura® Session Manager running on Virtual Server	R7.0.0.0.700007
Avaya Aura® Communication Manager running on Virtual Server	R7.0 Build 017x.00.0.441.0
Avaya Aura® Messaging running on Virtual Server	R6.3 Build No – 6.3.3
Avaya G450 Gateway	37.19.0 /1
Avaya 96xxH323 Deskphone	96xx H.323 Release 3.1 SP2
Avaya 9641 SIP Deskphone Avaya 9608 SIP Deskphone	96x1-IPT-SIP-R6_4_1-081114
Ascom DECT Master Base Station Ascom DECT Standby Base Station	IPBS2 V8.0.8
Ascom DECT Handsets	Mixture of 4 D41, D62, D81 handsets D62-Talker 4.3.17 D41-Advanced 4.3.17 D81-Messenger 4.3.17

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.
- Network Region.
- IP Codec.
- Coverage Path/Hunt Group.

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 **6** and **7**. 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   udp
   3           4   udp
   4           4   udp
   5           4   udp
   5999        4   ext
   6           4   ext
   7           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 : #21**
- **Auto Alternate Routing (AAR) Access Code : 8**
- **Auto Route Selection (ARS) - Access Code 1 : 9**
- **Call Park Access Code : #20**

```
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: #21
                         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:#31     All:#30     Deactivation:#32
   Call Forwarding Enhanced Status:        Act:        Deactivation:
                         Call Park Access Code: #20
                       Call Pickup Access Code: #22
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 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
```

5.4. 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
```

5.5. 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:
```

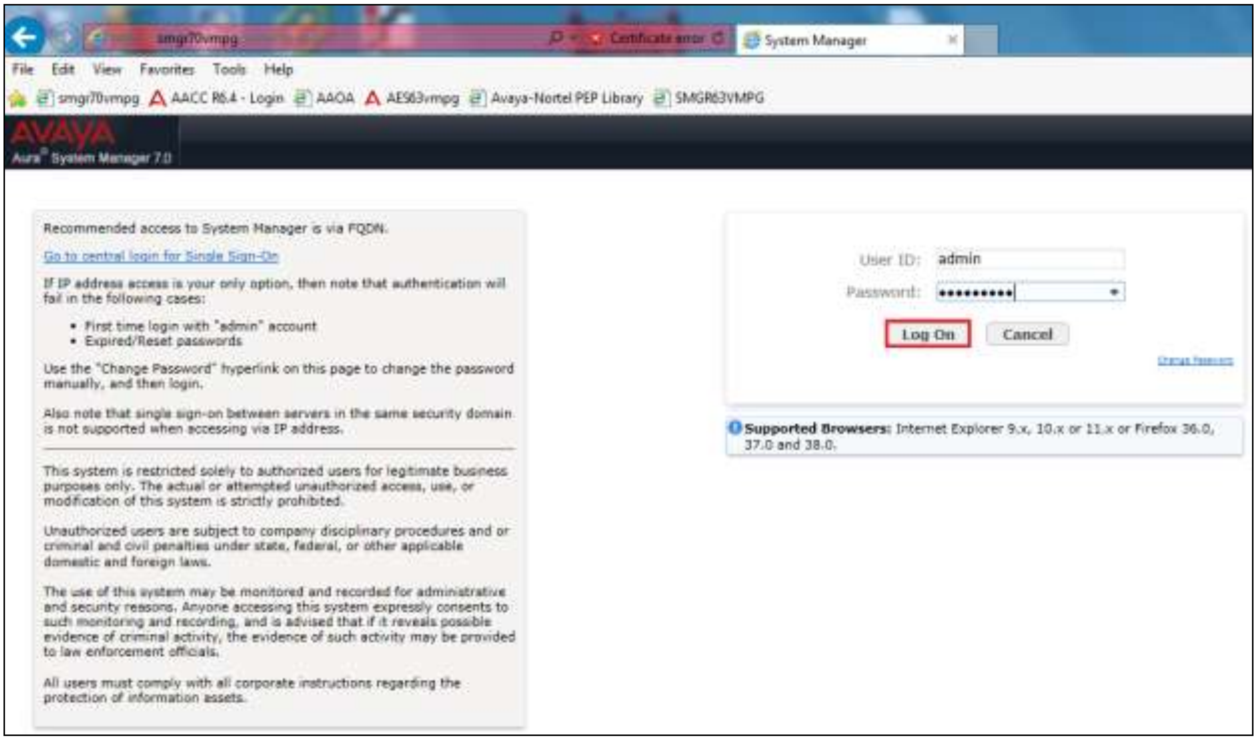
The hunt group used for compliance testing is shown below. Note on **Page 1** the **Group Extension** is **5999** which is the voicemail number for Messaging and on **Page 2 Message Center** is set to **sip-adjunct**.

```
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

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



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.

This system is restricted solely to authorized users for legitimate business purposes only. The actual or attempted unauthorized access, use, or modification of this system is strictly prohibited.

Unauthorized users are subject to company disciplinary procedures and or criminal and civil penalties under state, federal, or other applicable domestic and foreign laws.

The use of this system may be monitored and recorded for administrative and security reasons. Anyone accessing this system expressly consents to such monitoring and recording, and is advised that if it reveals possible evidence of criminal activity, the evidence of such activity may be provided to law enforcement officials.

All users must comply with all corporate instructions regarding the protection of information assets.

User ID: admin

Password: ••••••••••

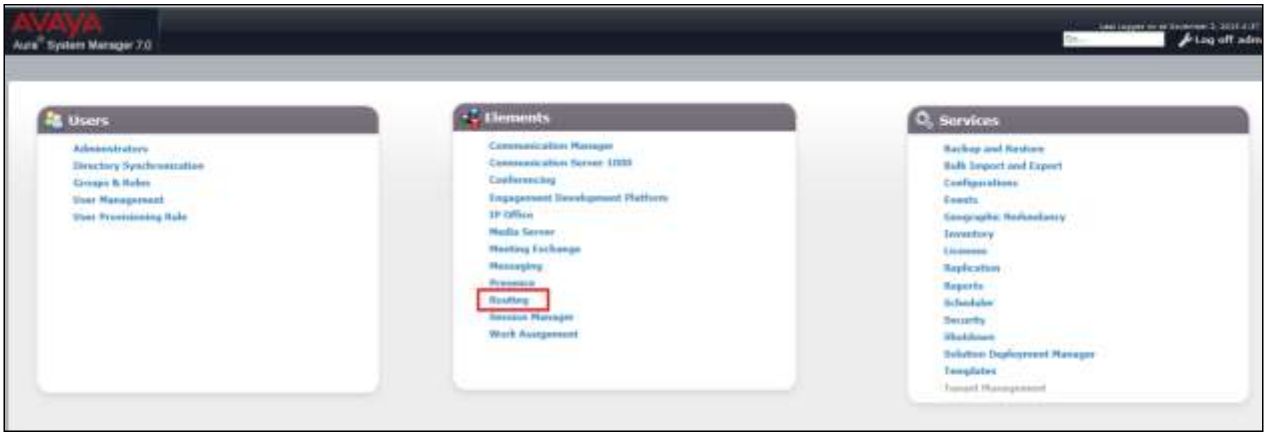
Log On Cancel

Change Password

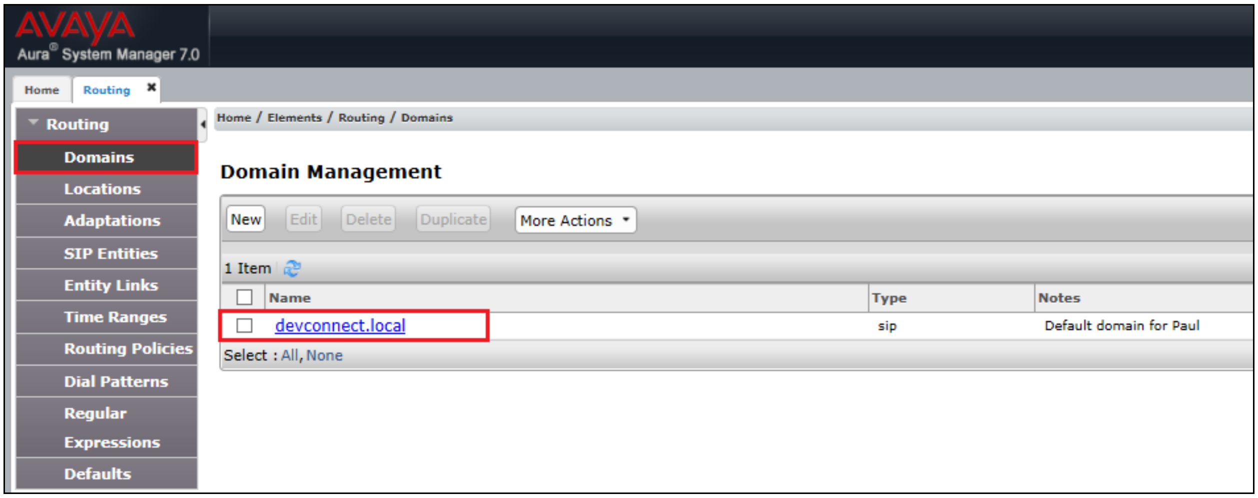
Supported Browsers: Internet Explorer 9.x, 10.x or 11.x or Firefox 36.0, 37.0 and 38.0.

6.1. Configuration of a Domain

Click on **Routing** highlighted below.

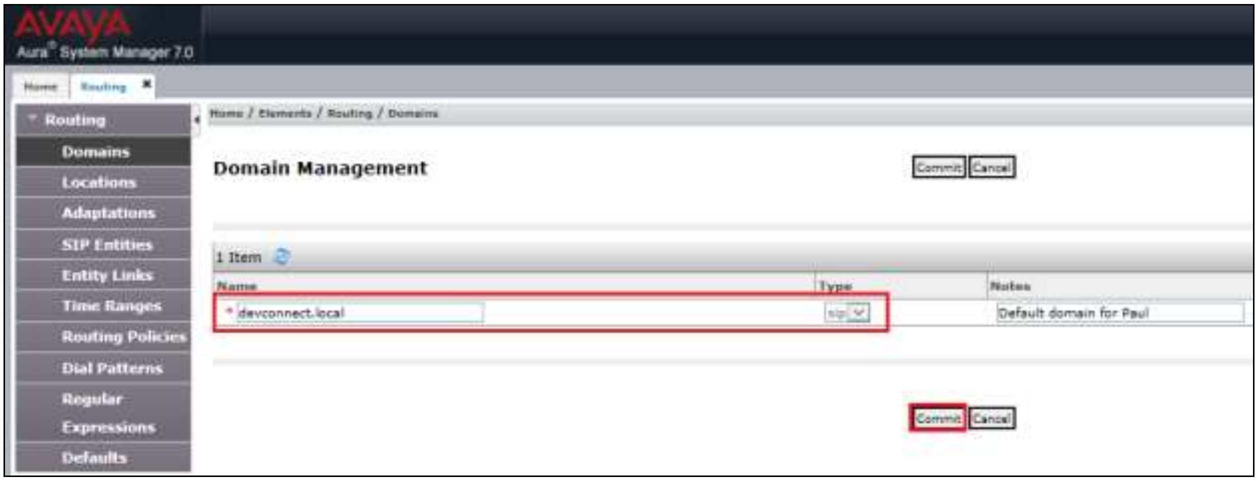


Click on **Domains** in the left window. If there is not a domain already configured click on **New**. In the example below there exists a domain called devconnect.local which has been already configured.



	Name	Type	Notes
□	devconnect.local	sip	Default domain for Paul

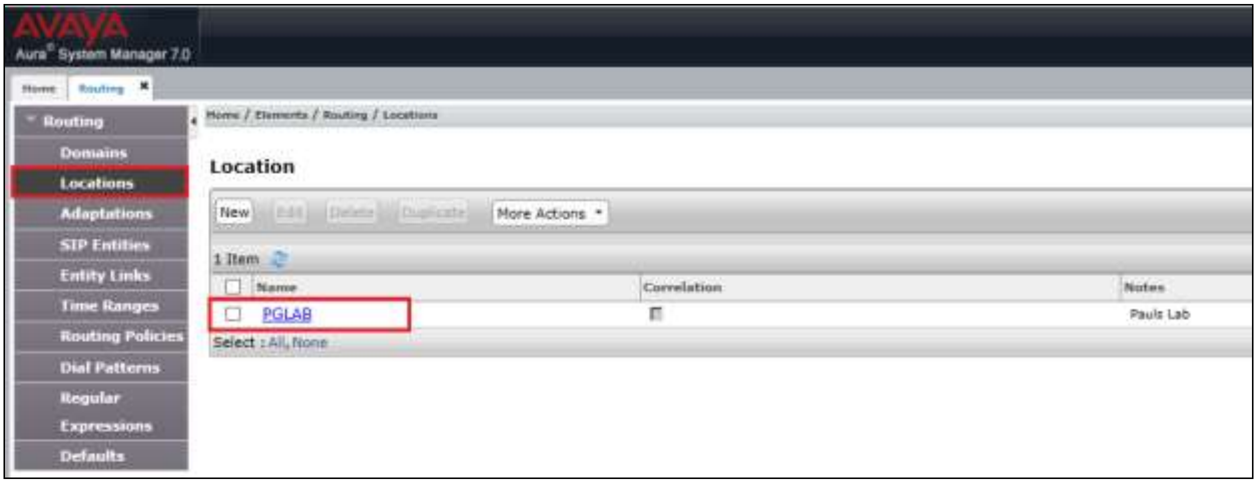
Clicking on the domain name above will open the following window; this is simply to show an example of such a domain. When entering a new domain the following should be entered, once the domain name is entered click on **Commit** to save this.



Name	Type	Notes
* devconnect.local	sip	Default domain for Paul

6.2. Configuration of a Location

Click on **Locations** in the left window and if there is no Location already configured then click on **New**, however in the screen below a location called **PGLAB** is already setup and configured and clicking into this will show its contents.

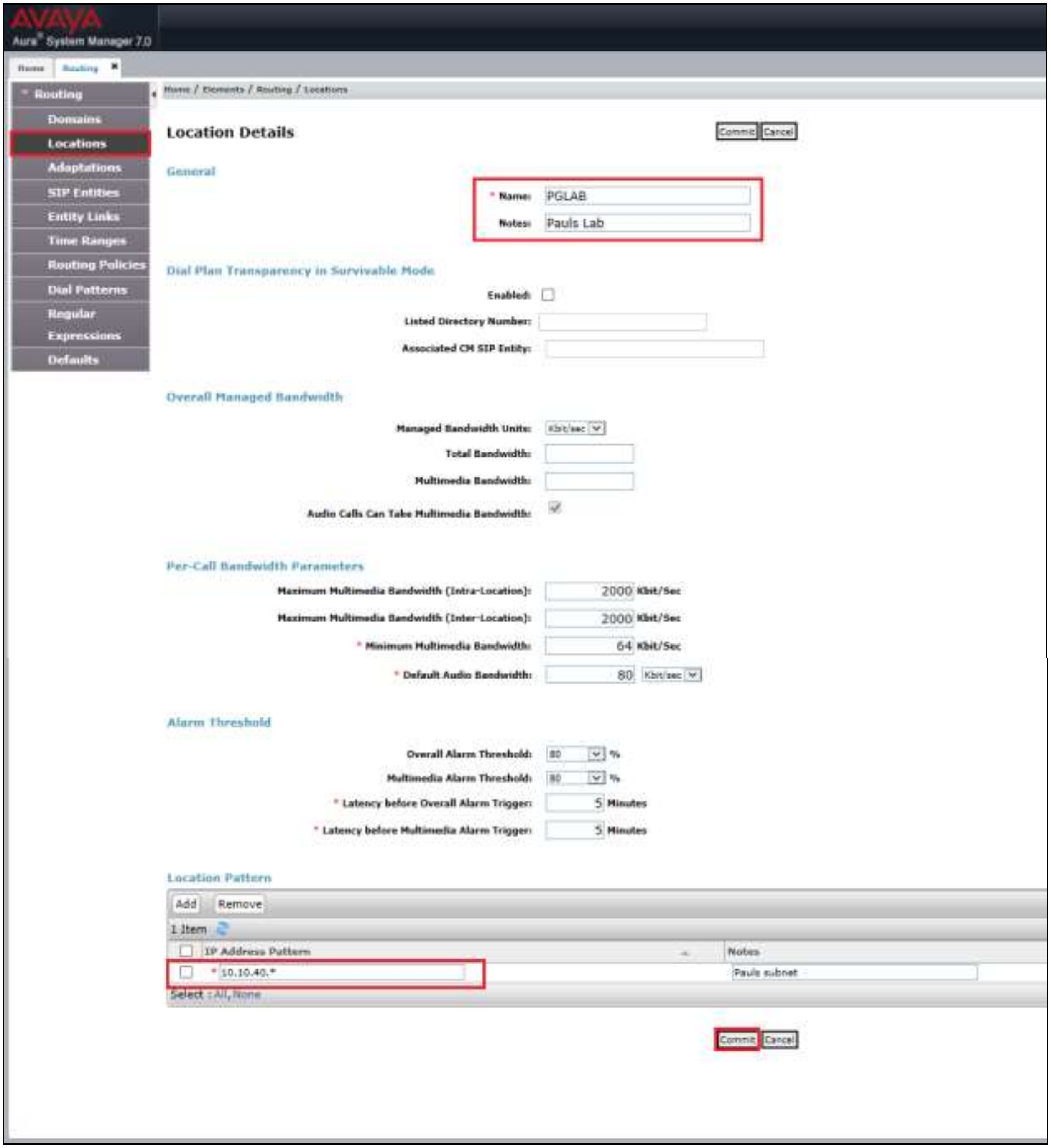


Location

1 Item

	Name	Correlation	Notes
□	PGLAB	□	Pauls Lab

The Location below shows a suitable **Name** with a **Location Pattern** of **10.10.40.***. Once this is configured, click on **Commit**.



Location Details

General

* Name: PGLAB

Notes: Pauls Lab

Dial Plan Transparency in Survivable Mode

Enabled: □

Listed Directory Number:

Associated CM SIP Entity:

Overall Managed Bandwidth

Managed Bandwidth Units: Kbit/sec

Total Bandwidth:

Multimedia Bandwidth:

Audio Calls Can Take Multimedia Bandwidth: ☑

Per-Call Bandwidth Parameters

Maximum Multimedia Bandwidth (Intra-Location): 2000 Kbit/Sec

Maximum Multimedia Bandwidth (Inter-Location): 2000 Kbit/Sec

* 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

1 Item

□	IP Address Pattern	Notes
□	* 10.10.40.*	Pauls subnet

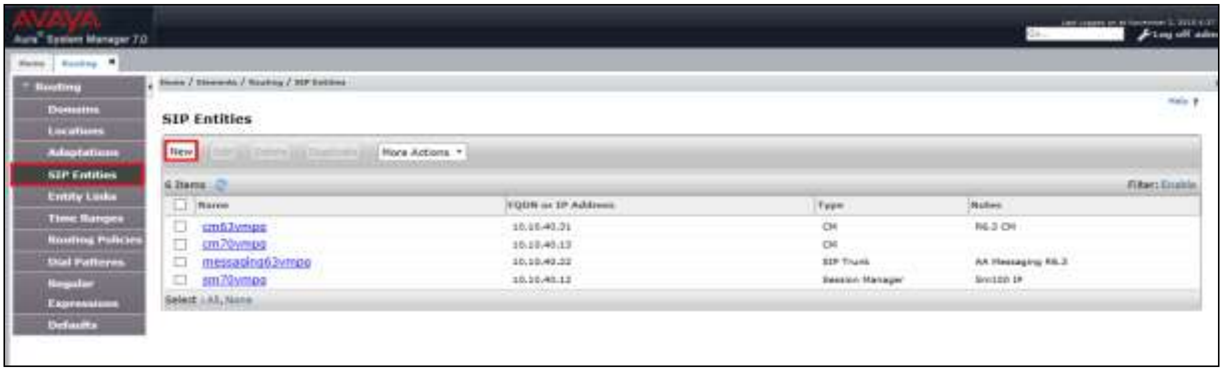
6.3. Configuration of SIP Entities

Clicking on **SIP Entities** in the left window 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.

There is no SIP Entity required if UDP is chosen for the transport protocol in **Section 8.3**, however 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.

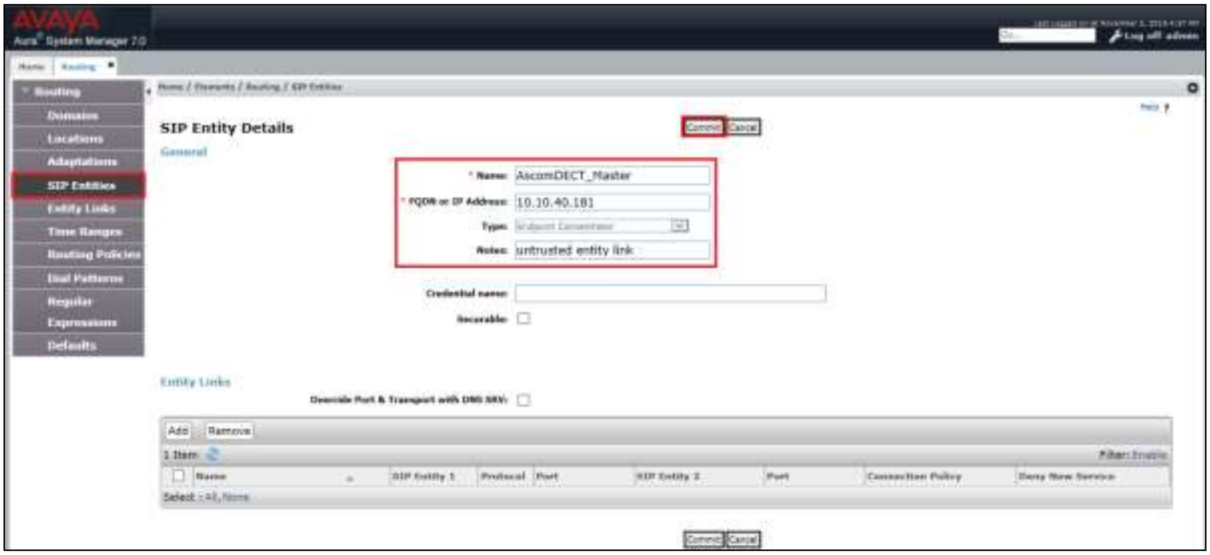
Note: A SIP Entity and Entity link are required for both the Master and Standby base stations.



SIP Entities

Name	FQDN or IP Address	Type	Notes
cm63vmpg	10.10.40.31	CM	R6.3 CM
cm70vmpg	10.10.40.13	CM	
messaging63vmpg	10.10.40.32	SIP Trunk	AA Messaging R6.3
sm70vmpg	10.10.40.12	Session Manager	SM100 IP

Enter a suitable **Name** and enter the **IP Address** of the DECT Base Station. Select **Endpoint Concentrator** as the **Type**. Click on **Commit** once completed.



SIP Entity Details

General

* Name: AscomDECT_Master

* FQDN or IP Address: 10.10.40.181

Type: Endpoint Concentrator

Notes: untrusted entity link

Credential name:

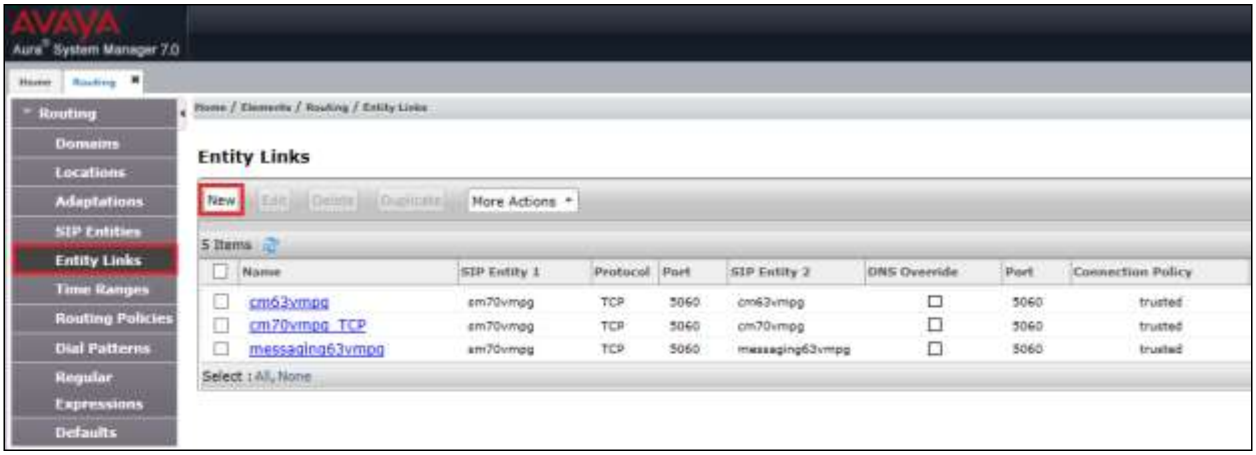
Securable: □

Entity Links

Override Port & Transport with DNS SRV: □

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Deny New Service

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



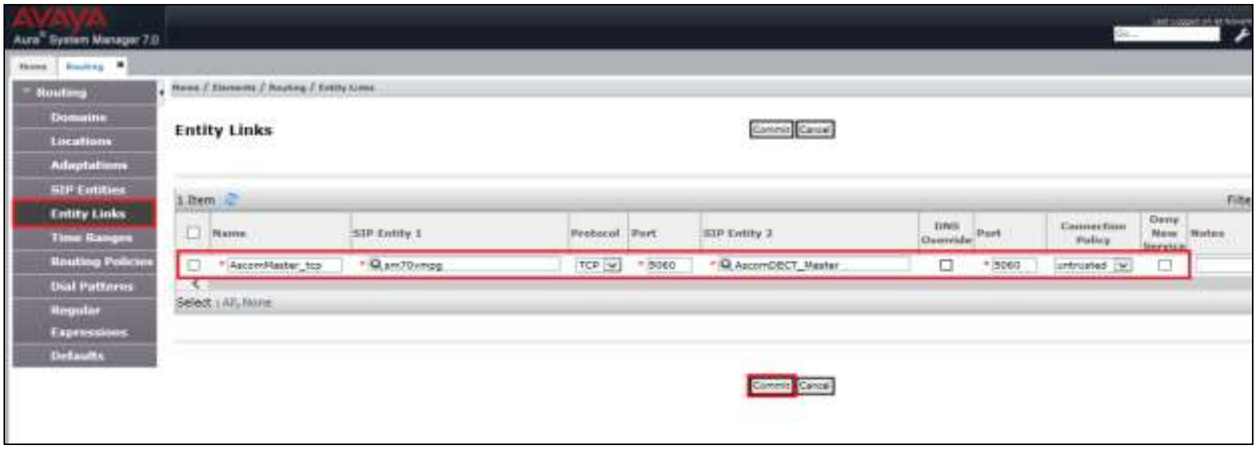
Entity Links

5 Items

☐	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	DNS Override	Port	Connection Policy
☐	cm63vmpg	sm70vmpg	TCP	5060	cm63vmpg	☐	5060	trusted
☐	cm70vmpg_TCP	sm70vmpg	TCP	5060	cm70vmpg	☐	5060	trusted
☐	messaging63vmpg	sm70vmpg	TCP	5060	messaging63vmpg	☐	5060	trusted

Select : All, None

Ensure that **TCP** is selected for the **Protocol** and **5060** for the **Port**. The **Connection Policy** must be set to **untrusted**. Click on **Commit** once completed.



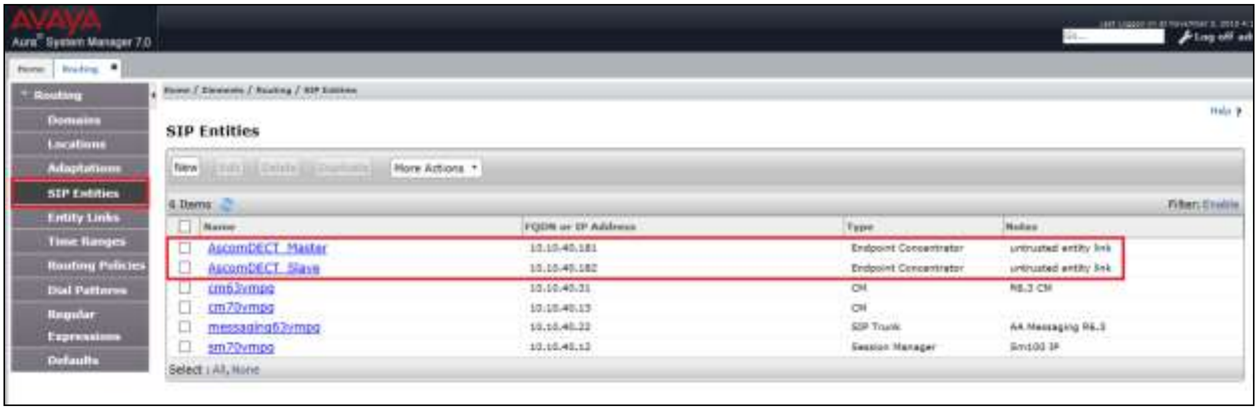
Entity Links

1 Item

☐	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	DNS Override	Port	Connection Policy	Deny New Service	Notes
☐	* AscomMaster_tcp	* sm70vmpg	TCP	* 5060	* AscomDECT_Master	☐	* 5060	untrusted	☐	

Select : All, None

A SIP Entity and Entity link must be added for both the Ascom Master base station and the Ascom Slave base station.



SIP Entities

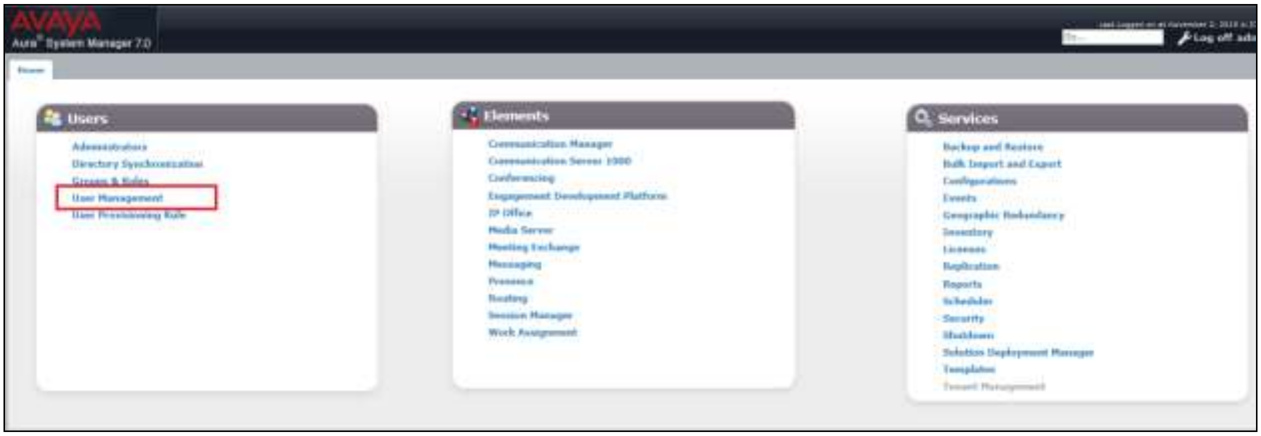
6 Items

☐	Name	FQDN or IP Address	Type	Notes
☐	AscomDECT_Master	10.10.40.181	Endpoint Concentrator	untrusted entity link
☐	AscomDECT_Slave	10.10.40.182	Endpoint Concentrator	untrusted entity link
☐	cm63vmpg	10.10.40.31	CM	R6.3 CM
☐	cm70vmpg	10.10.40.13	CM	
☐	messaging63vmpg	10.10.40.22	SIP Trunk	AA Messaging R6.3
☐	sm70vmpg	10.10.40.12	Session Manager	Sm100 IP

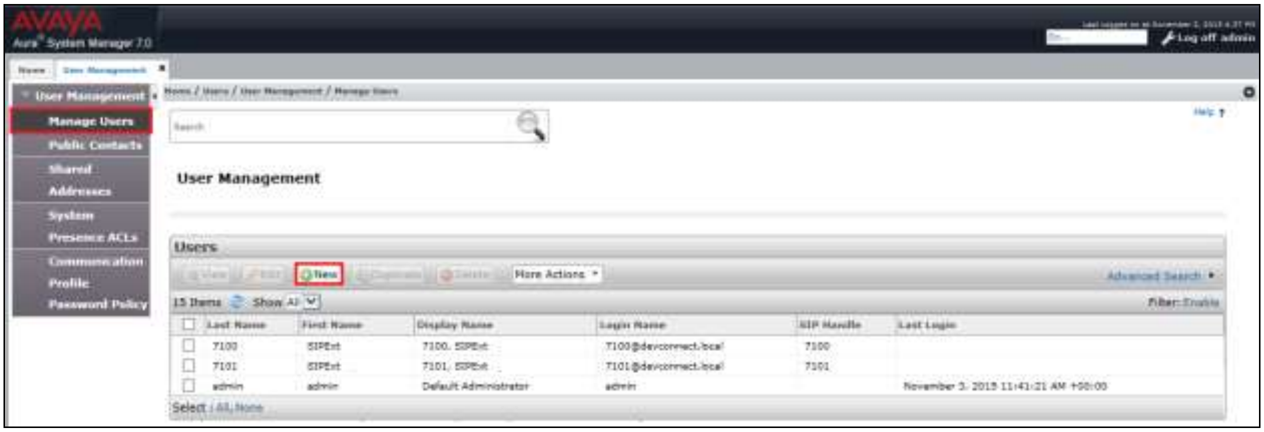
Select : All, None

6.4. Adding Ascom SIP Users

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

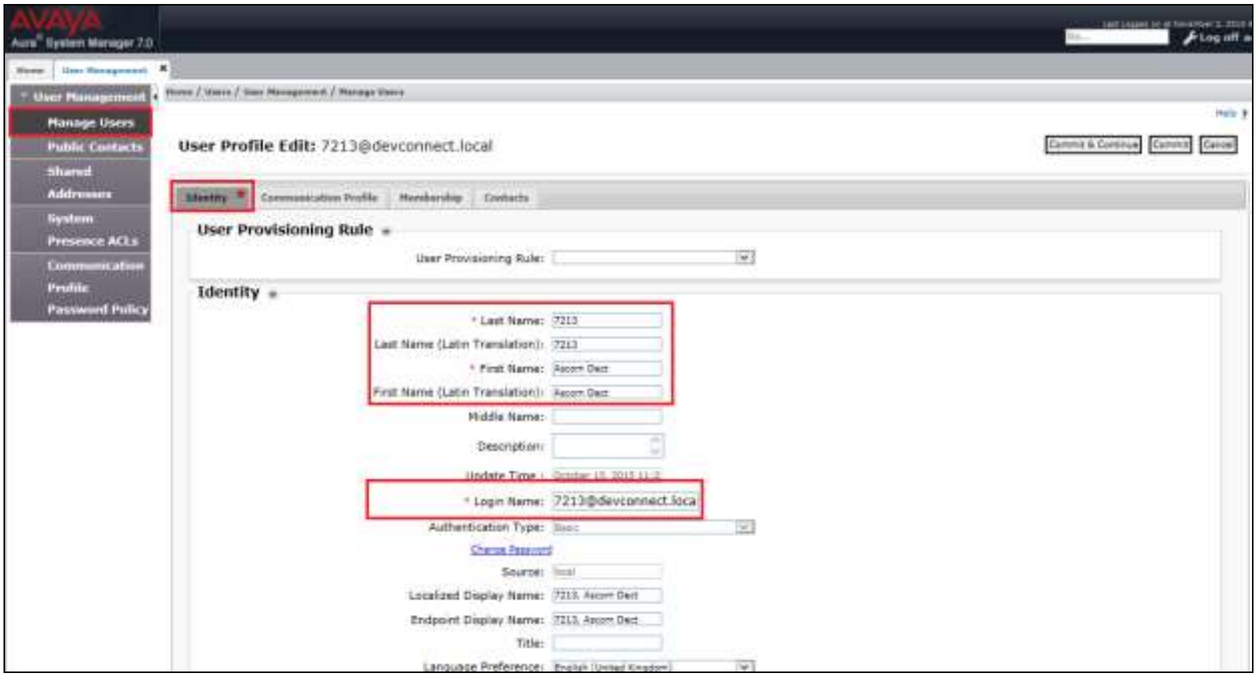


Click on **New** highlighted to add a new SIP user.



□	Last Name	First Name	Display Name	Login Name	SIP Handle	Last Login
□	7100	SIPExt	7100, SIPExt	7100@devconnect.local	7100	
□	7101	SIPExt	7101, SIPExt	7101@devconnect.local	7101	
□	admin	admin	Default Administrator	admin		November 3, 2015 11:41:21 AM +00:00

Under the **Identity** tab fill in the user's **Last Name** and **First Name** as shown below. Enter the **Login Name**. The remaining fields can be left as default.



User Profile Edit: 7213@devconnect.local

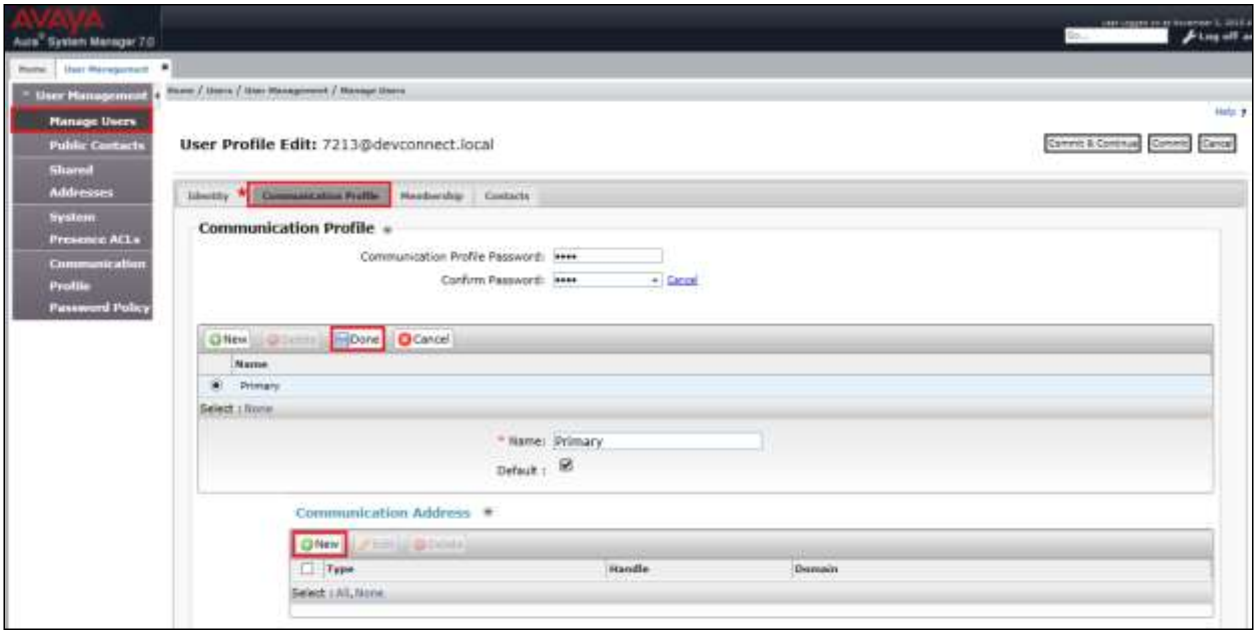
User Provisioning Rule

User Provisioning Rule:

Identity

* Last Name: 7213
Last Name (Latin Translation): 7213
* First Name: Ascom Dect
First Name (Latin Translation): Ascom Dect
Middle Name:
Description:
Update Time : October 15, 2015 11:2
* Login Name: 7213@devconnect.loca
Authentication Type: Basic
Change Password
Source: local
Localized Display Name: 7213, Ascom Dect
Endpoint Display Name: 7213, Ascom Dect
Title:
Language Preference: English (United Kingdom)

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 8.4**. Click on **New** to add a new **Communication Address**.



User Profile Edit: 7213@devconnect.local

Communication Profile

Communication Profile Password: ••••
Confirm Password: •••• Cancel

	Name
●	Primary

Select : None

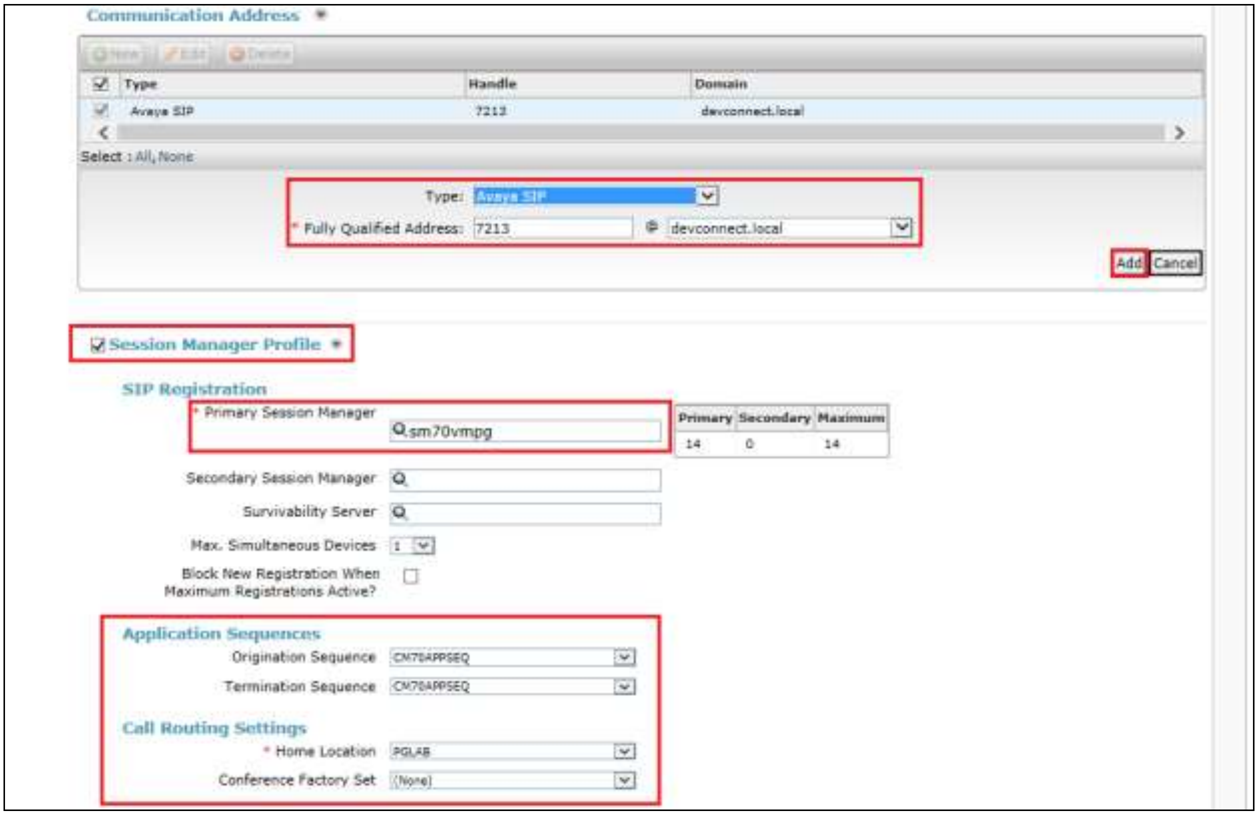
* Name: Primary
Default : ☑

Communication Address

□	Type	Handle	Domain

Select : All, None

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.



Communication Address

☑	Type	Handle	Domain
☑	Avaya SIP	7213	devconnect.local

Select : All, None

Type: Avaya SIP

* Fully Qualified Address: 7213 @ devconnect.local

☑ Session Manager Profile

SIP Registration

* Primary Session Manager: sm70vmpg

Primary	Secondary	Maximum
14	0	14

Secondary Session Manager:

Survivability Server:

Max. Simultaneous Devices: 1

Block New Registration When Maximum Registrations Active? □

Application Sequences

Origination Sequence: CM70APPSEQ

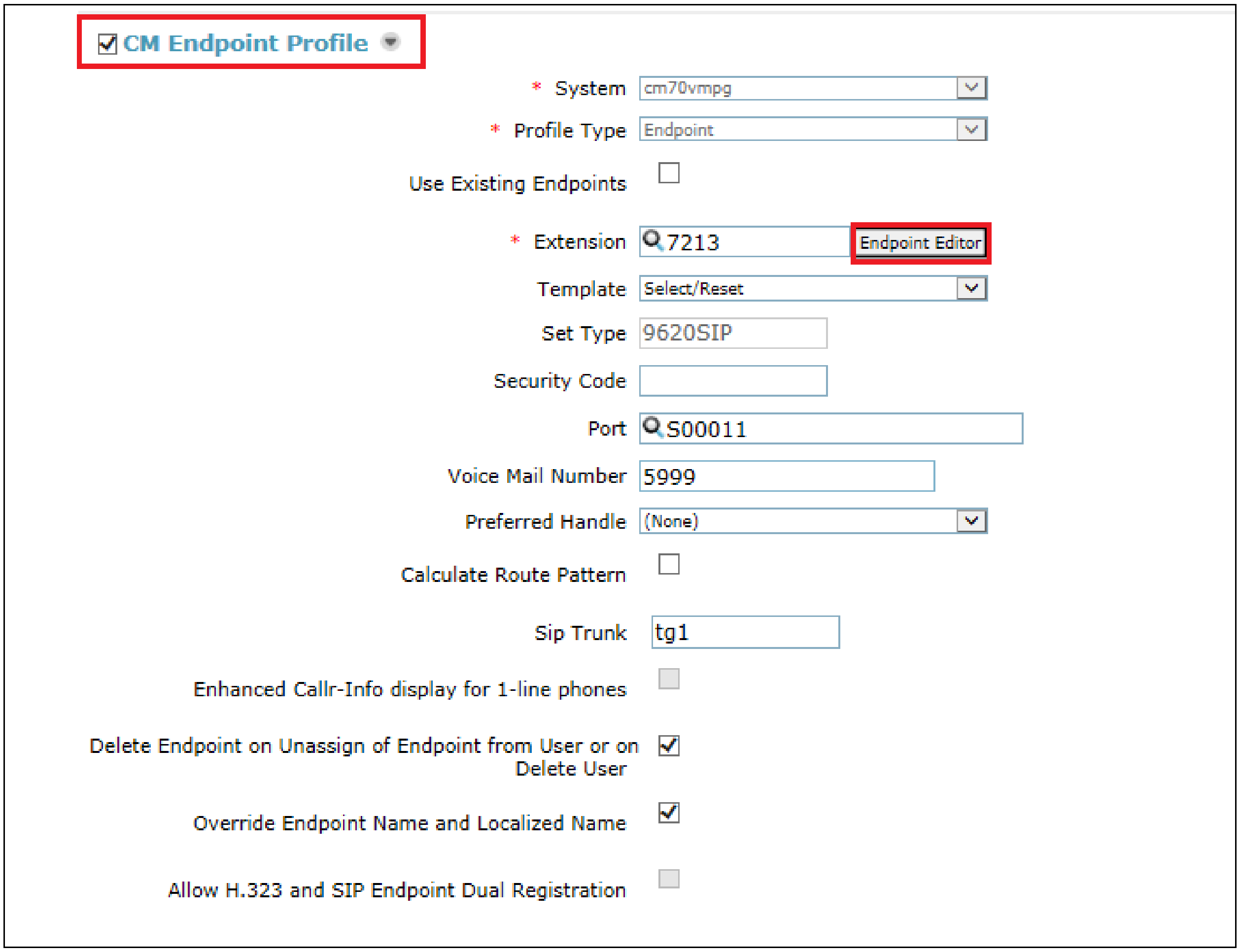
Termination Sequence: CM70APPSEQ

Call Routing Settings

* Home Location: PGLAB

Conference Factory Set: (None)

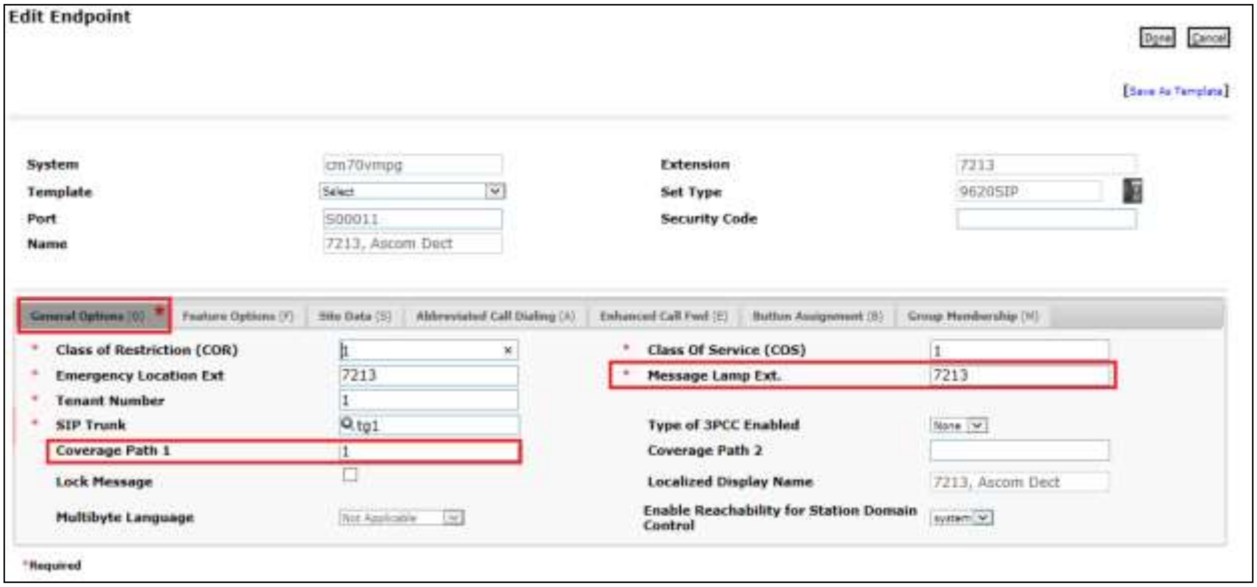
Ensure that **CM Endpoint Profile** is selected and choose the **9620SIP** as the **Template**. Click on **Endpoint Editor** to configure the buttons and features for that handset on Communication Manager.



☑ CM Endpoint Profile

* System	cm70vmpg
* Profile Type	Endpoint
Use Existing Endpoints	☐
* Extension	7213 [Endpoint Editor]
Template	Select/Reset
Set Type	9620SIP
Security Code	
Port	S00011
Voice Mail Number	5999
Preferred Handle	(None)
Calculate Route Pattern	☐
Sip Trunk	tg1
Enhanced Callr-Info display for 1-line phones	☐
Delete Endpoint on Unassign of Endpoint from User or on Delete User	☑
Override Endpoint Name and Localized Name	☑
Allow H.323 and SIP Endpoint Dual Registration	☐

Under the **General Options** tab ensure that **Coverage Path 1** is set to that configured in **Section 5.5**. Also ensure that **Message Lamp Ext.** is showing the correct extension number.

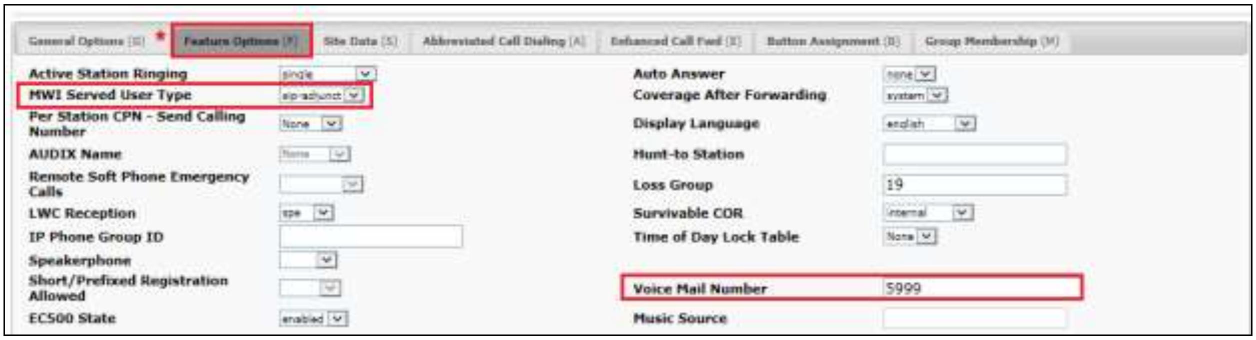


System	cm70vmpg	Extension	7213
Template	Select	Set Type	9620SIP
Port	S00011	Security Code	
Name	7213, Ascom Dect		

* Class of Restriction (COR)	1	* Class Of Service (COS)	1
* Emergency Location Ext	7213	* Message Lamp Ext.	7213
* Tenant Number	1		
* SIP Trunk	tg1	Type of 3PCC Enabled	None
Coverage Path 1	1	Coverage Path 2	
Lock Message	□	Localized Display Name	7213, Ascom Dect
Multibyte Language	Not Applicable	Enable Reachability for Station Domain Control	system

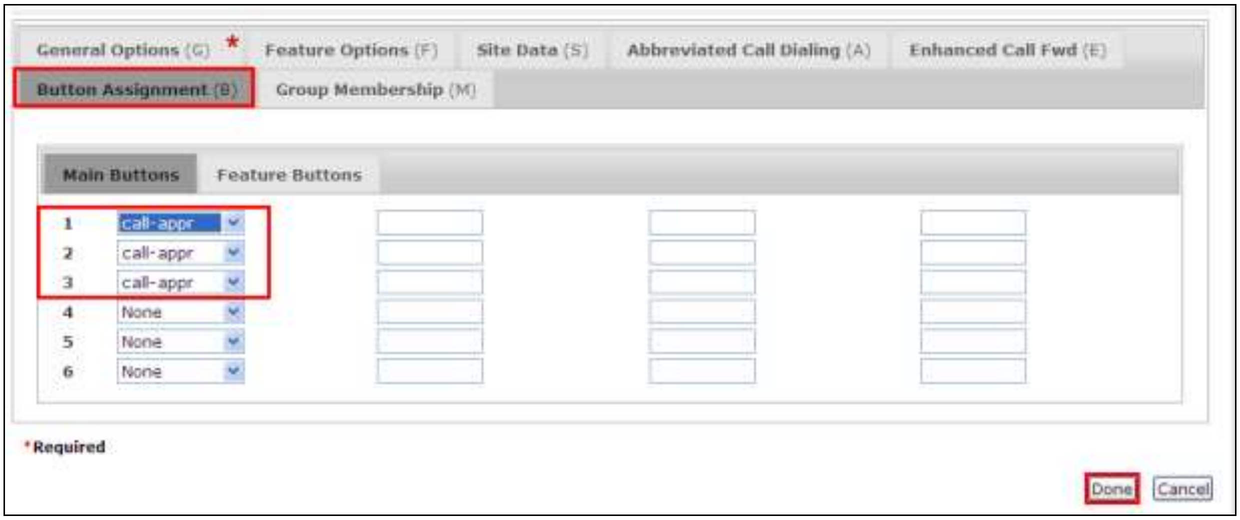
*Required

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 5.5**.



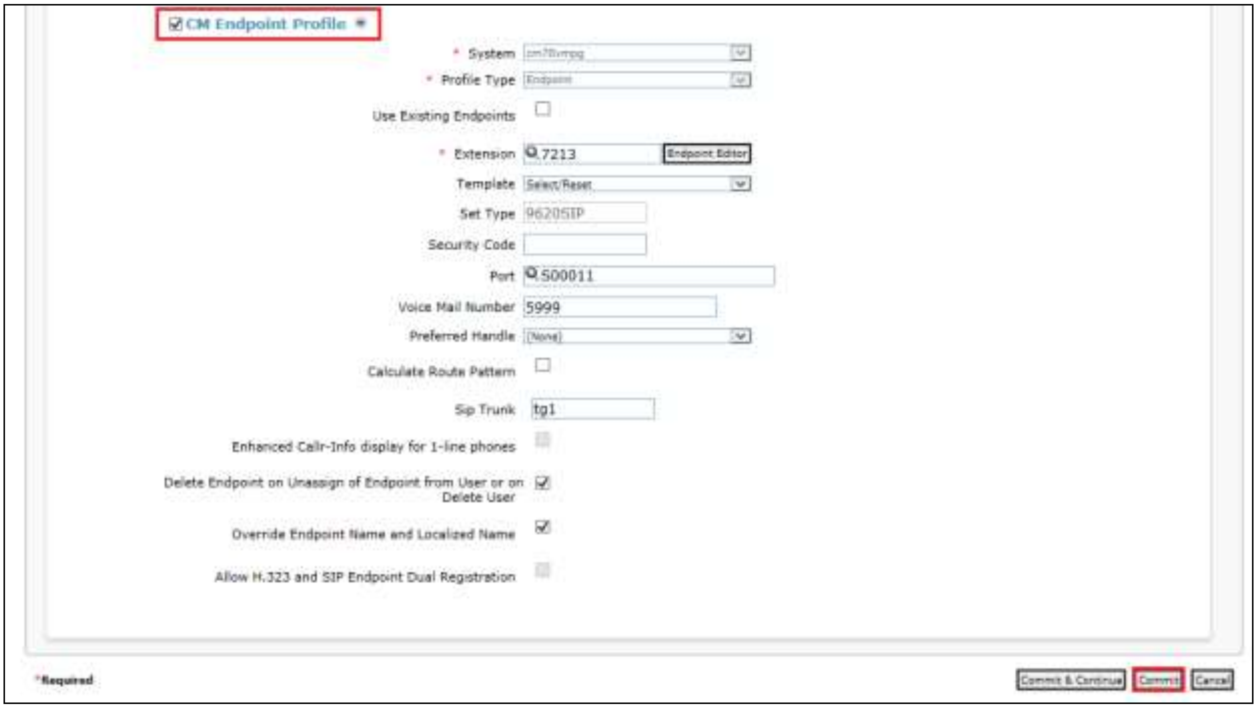
Active Station Ringing	single	Auto Answer	none
MWI Served User Type	sip-adjunct	Coverage After Forwarding	system
Per Station CPN - Send Calling Number	None	Display Language	english
AUDIX Name	None	Hunt-to Station	
Remote Soft Phone Emergency Calls		Loss Group	19
LWC Reception	spe	Survivable COR	internal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

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.



1	call-appr			
2	call-appr			
3	call-appr			
4	None			
5	None			
6	None			

Once the **CM Endpoint Profile** is completed correctly, click on **Commit** to save the new user.



* System: cm70vmpg

* Profile Type: Endpoint

Use Existing Endpoints: □

* Extension: 7213

Template: Select/Reset

Set Type: 9620SIP

Security Code:

Port: 500011

Voice Mail Number: 5999

Preferred Handle: (None)

Calculate Route Pattern: □

Sip Trunk: tg1

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

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

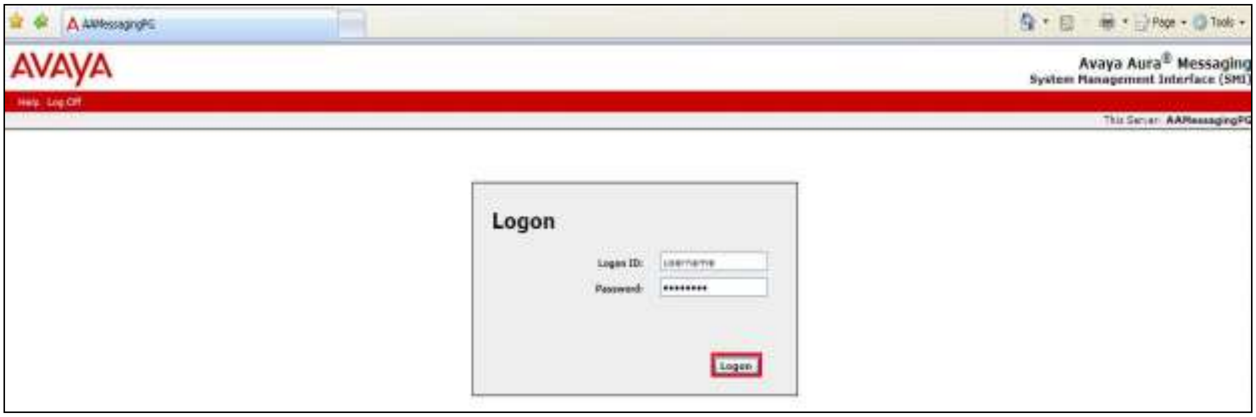
Override Endpoint Name and Localized Name: ☑

Allow H.323 and SIP Endpoint Dual Registration: □

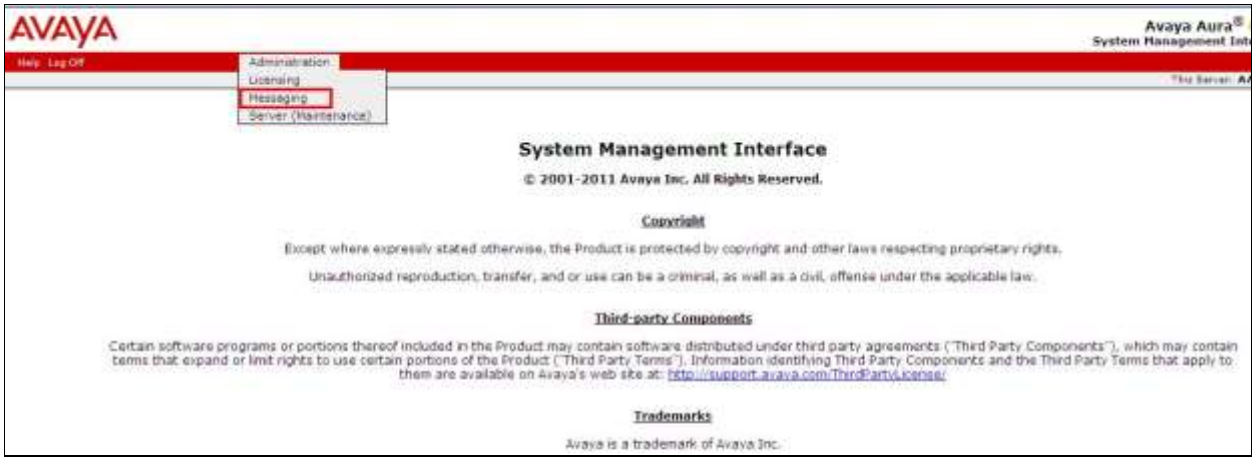
7. Configure Avaya Aura® Messaging

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.

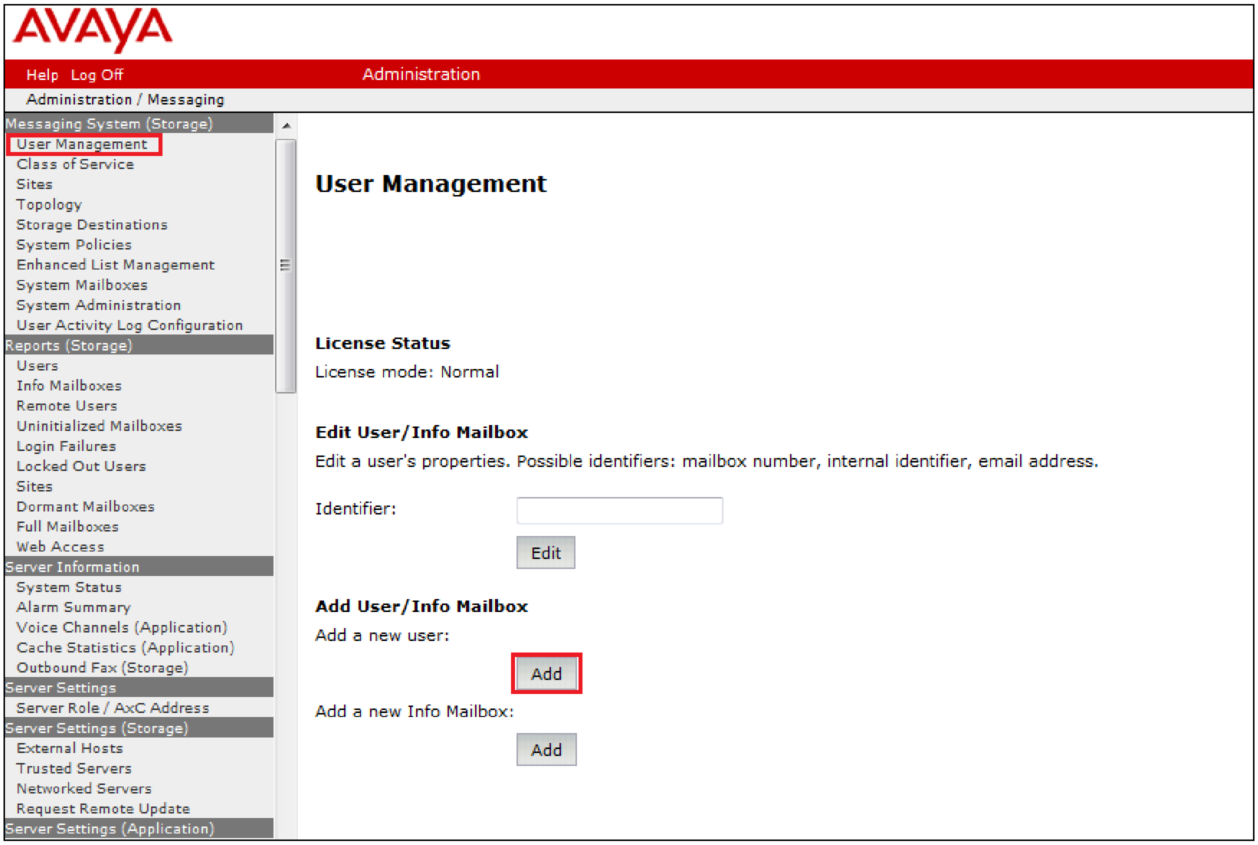
Third-party Components

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: mailbox number, internal identifier, email address.

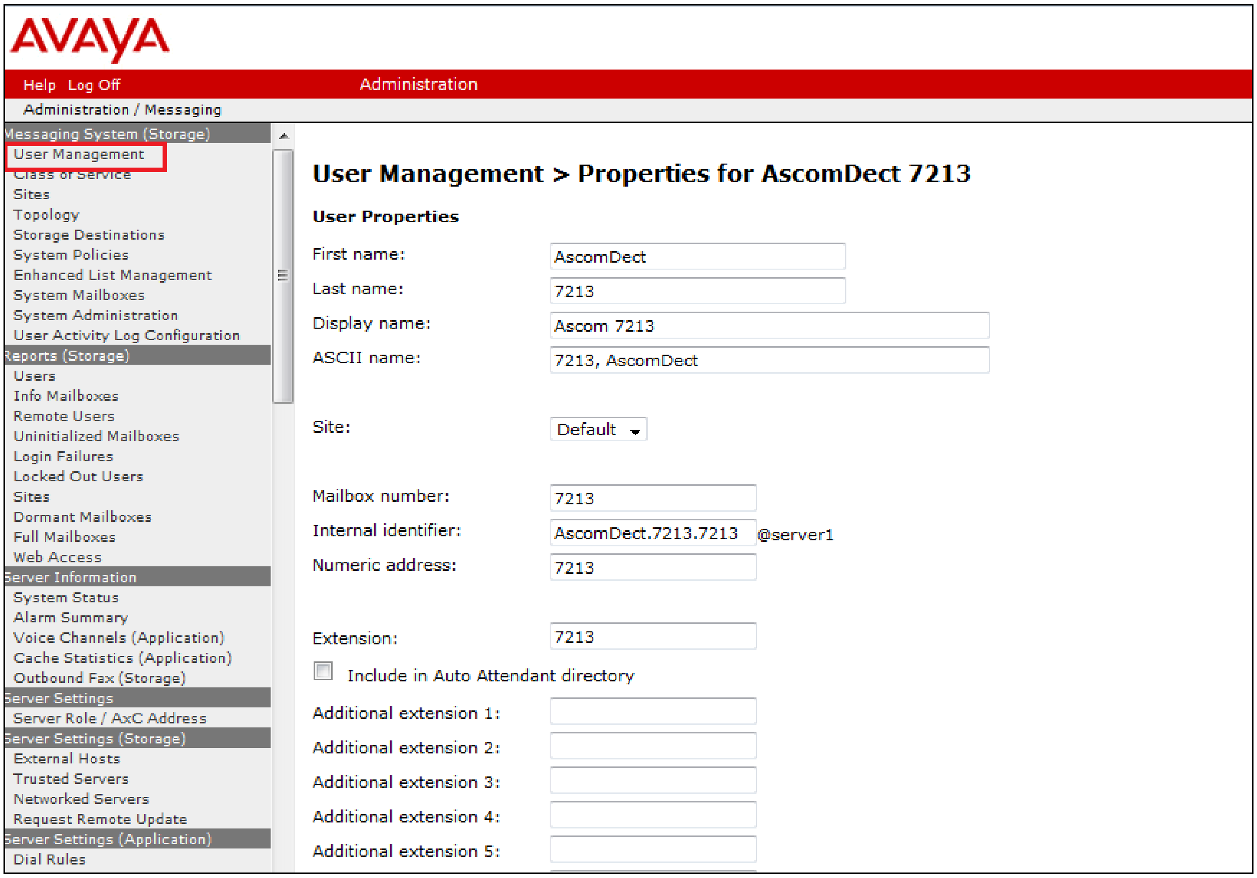
Identifier:

Add User/Info Mailbox

Add a new user:

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**.



User Management > Properties for AscomDect 7213

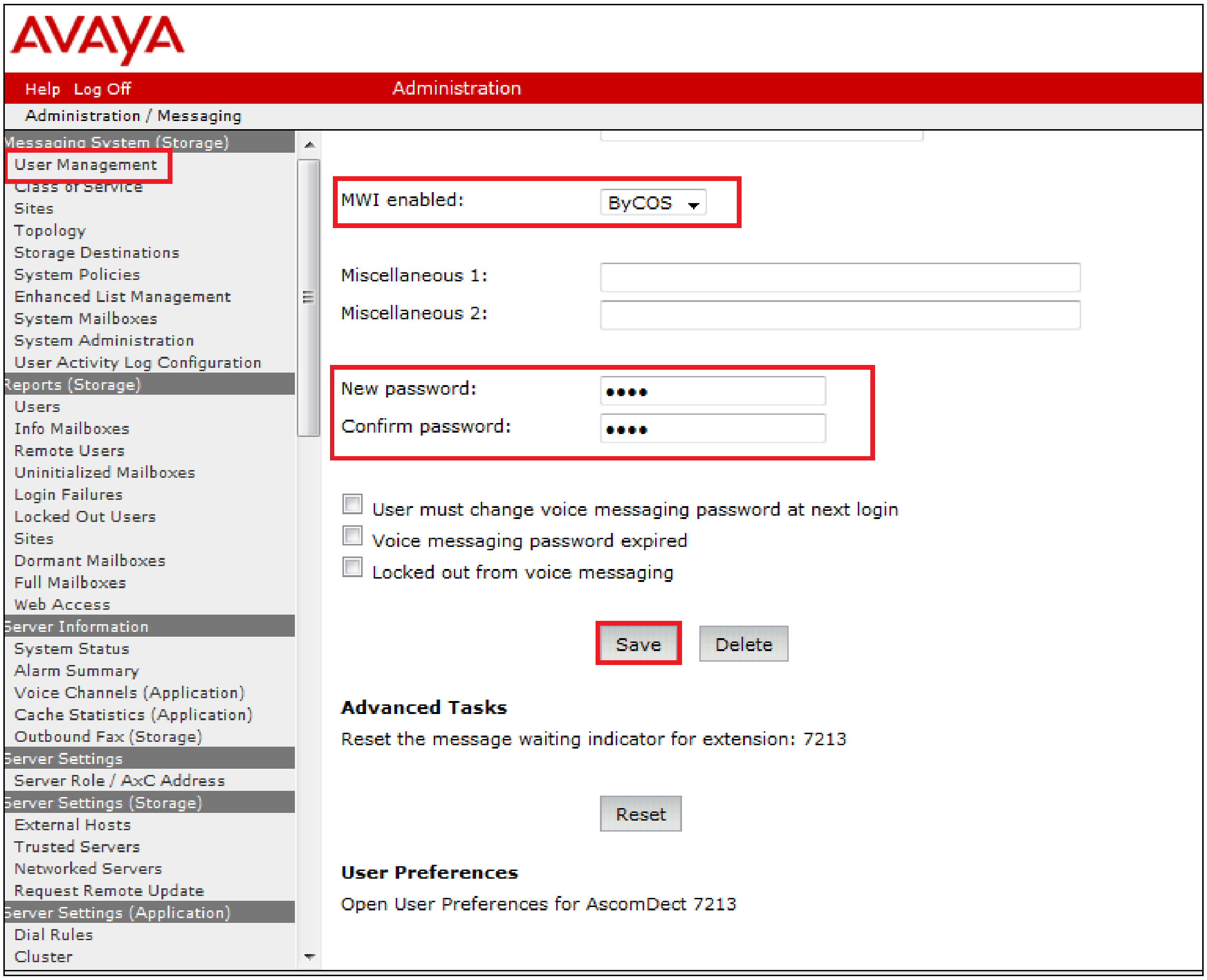
User Properties

First name:	AscomDect
Last name:	7213
Display name:	Ascom 7213
ASCII name:	7213, AscomDect
Site:	Default
Mailbox number:	7213
Internal identifier:	AscomDect.7213.7213 @server1
Numeric address:	7213
Extension:	7213

□ Include in Auto Attendant directory

Additional extension 1:	
Additional extension 2:	
Additional extension 3:	
Additional extension 4:	
Additional extension 5:	

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



MWI enabled: ByCOS

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

Advanced Tasks

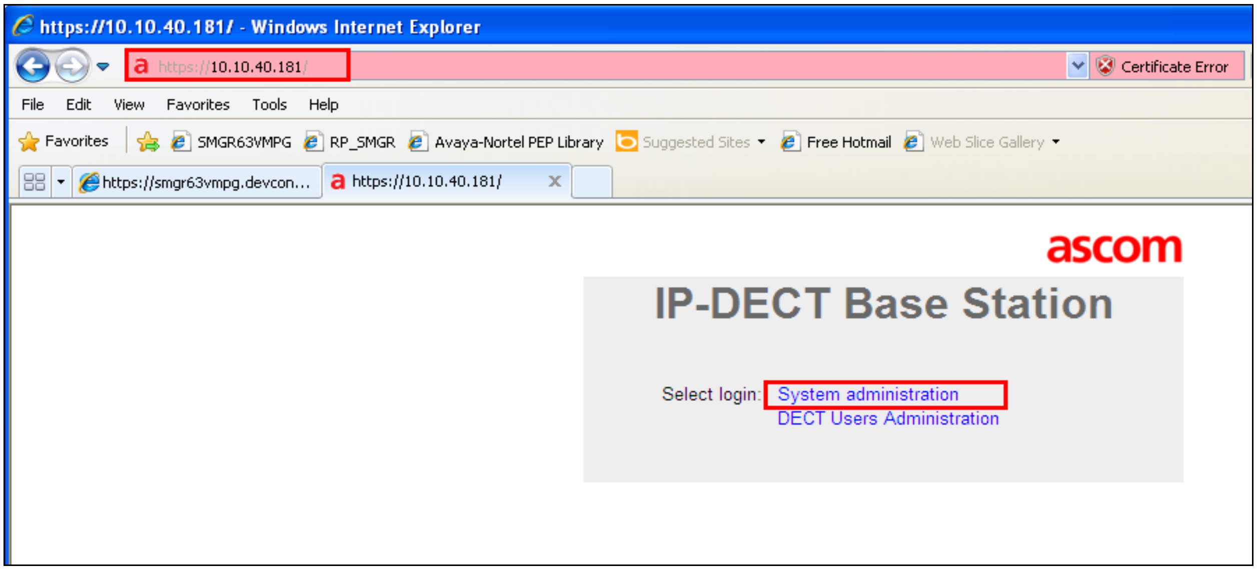
Reset the message waiting indicator for extension: 7213

User Preferences

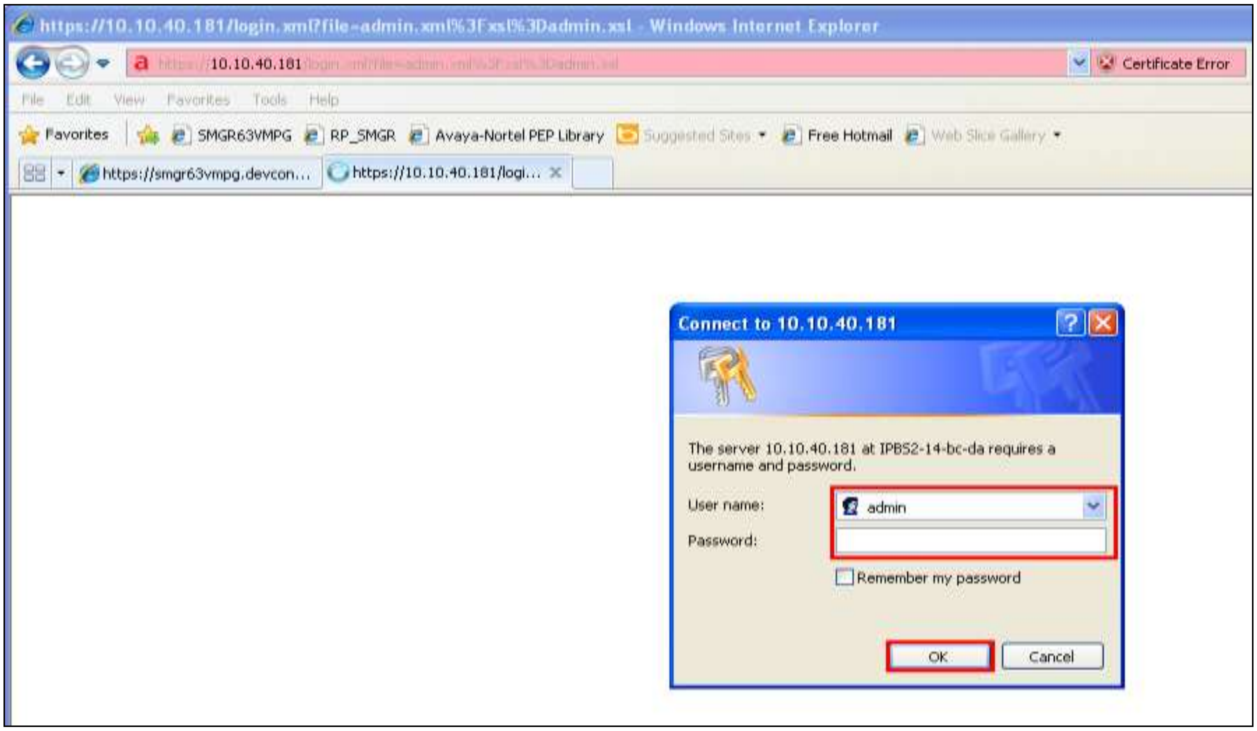
Open User Preferences for AscomDect 7213

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 and click on **System administration** as shown below.


https://10.10.40.181/ - Windows Internet Explorer
https://10.10.40.181/
Certificate Error
File Edit View Favorites Tools Help
Favorites SMGR63VMPG RP_SMGR Avaya-Nortel PEP Library Suggested Sites Free Hotmail Web Slice Gallery
https://smgr63vmpg.devcon... https://10.10.40.181/
ascom
IP-DECT Base Station
Select login: System administration
DECT Users Administration

Enter the proper credentials and click on **OK** to log in.


https://10.10.40.181/login.xml?file=admin.xml%3Fxsl%3Dadmin.xsl - Windows Internet Explorer
Certificate Error
File Edit View Favorites Tools Help
Favorites SMGR63VMPG RP_SMGR Avaya-Nortel PEP Library Suggested Sites Free Hotmail Web Slice Gallery
https://smgr63vmpg.devcon... https://10.10.40.181/logi...
Connect to 10.10.40.181

The server 10.10.40.181 at IPBS2-14-bc-da requires a username and password.

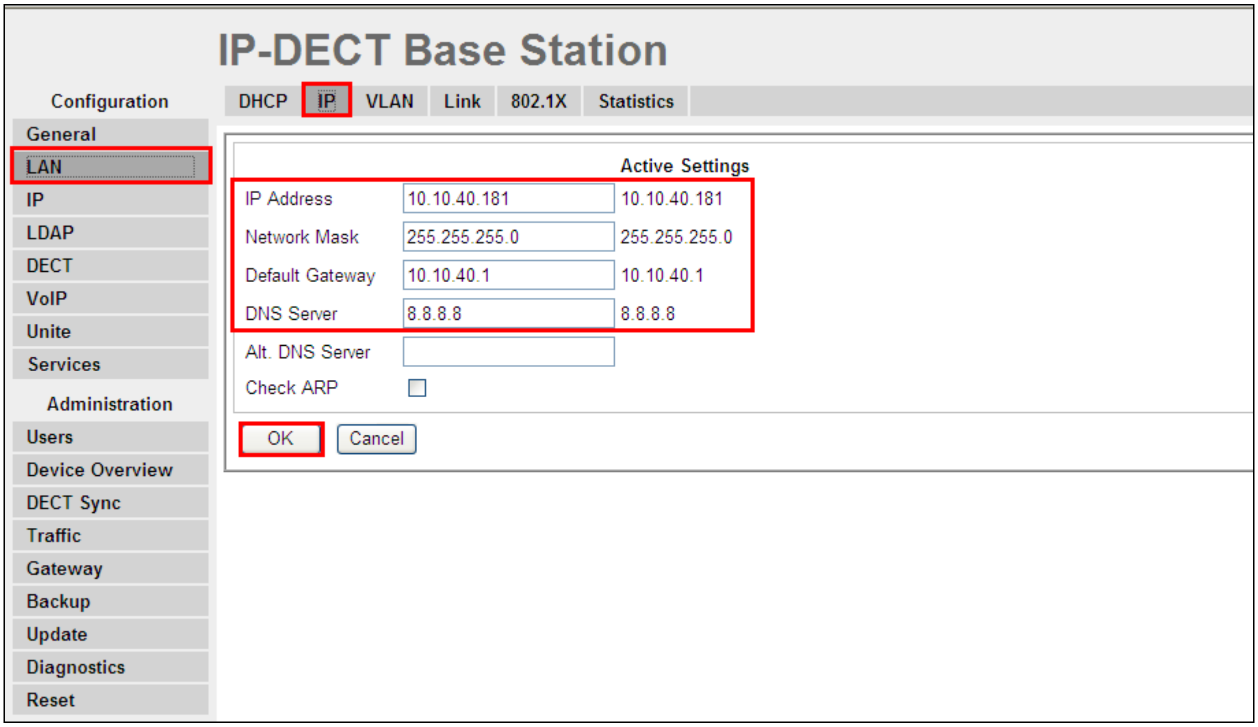
User name: admin

Password:

□ Remember my password

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 DCHP mode is set to disabled under the **DHCP** tab (not shown).

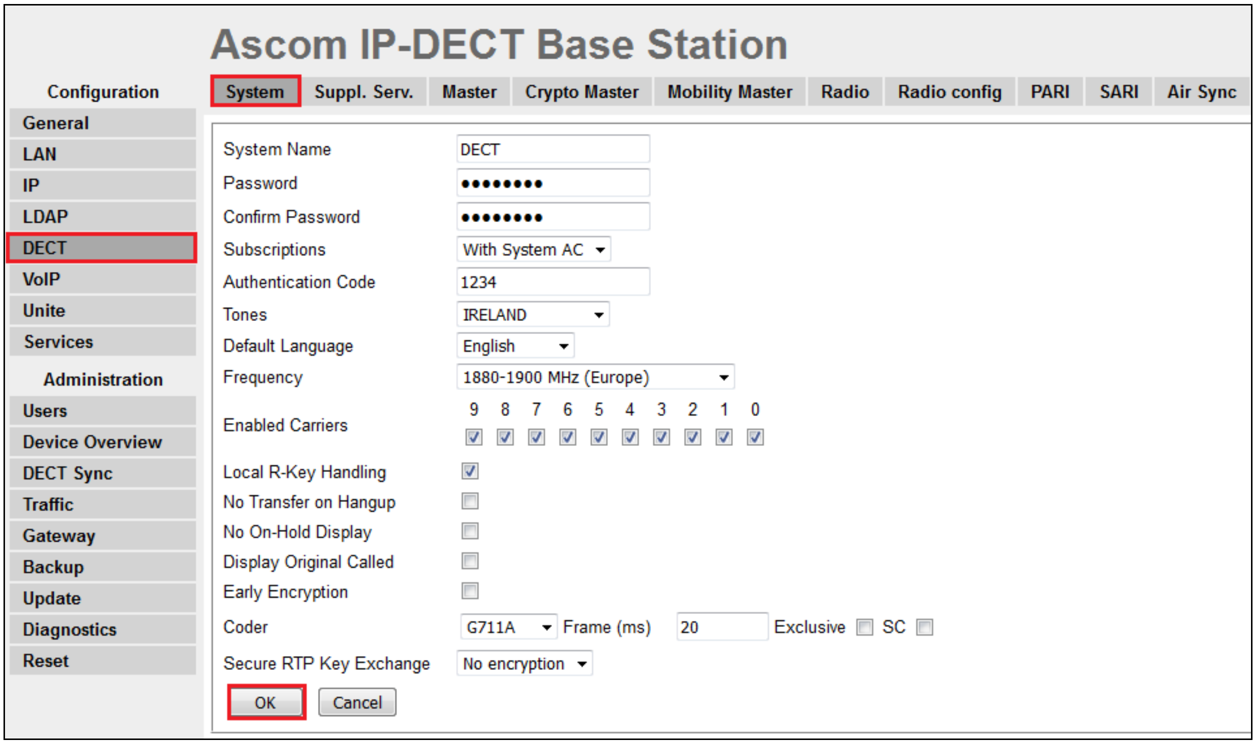


		Active Settings
IP Address	10.10.40.181	10.10.40.181
Network Mask	255.255.255.0	255.255.255.0
Default Gateway	10.10.40.1	10.10.40.1
DNS Server	8.8.8.8	8.8.8.8
Alt. DNS Server		
Check ARP	□	

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 is not the password for the SIP users on Session Manager; this is a password used to subscribe to the DECT system itself. 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**. Click on **OK** to save the changes.

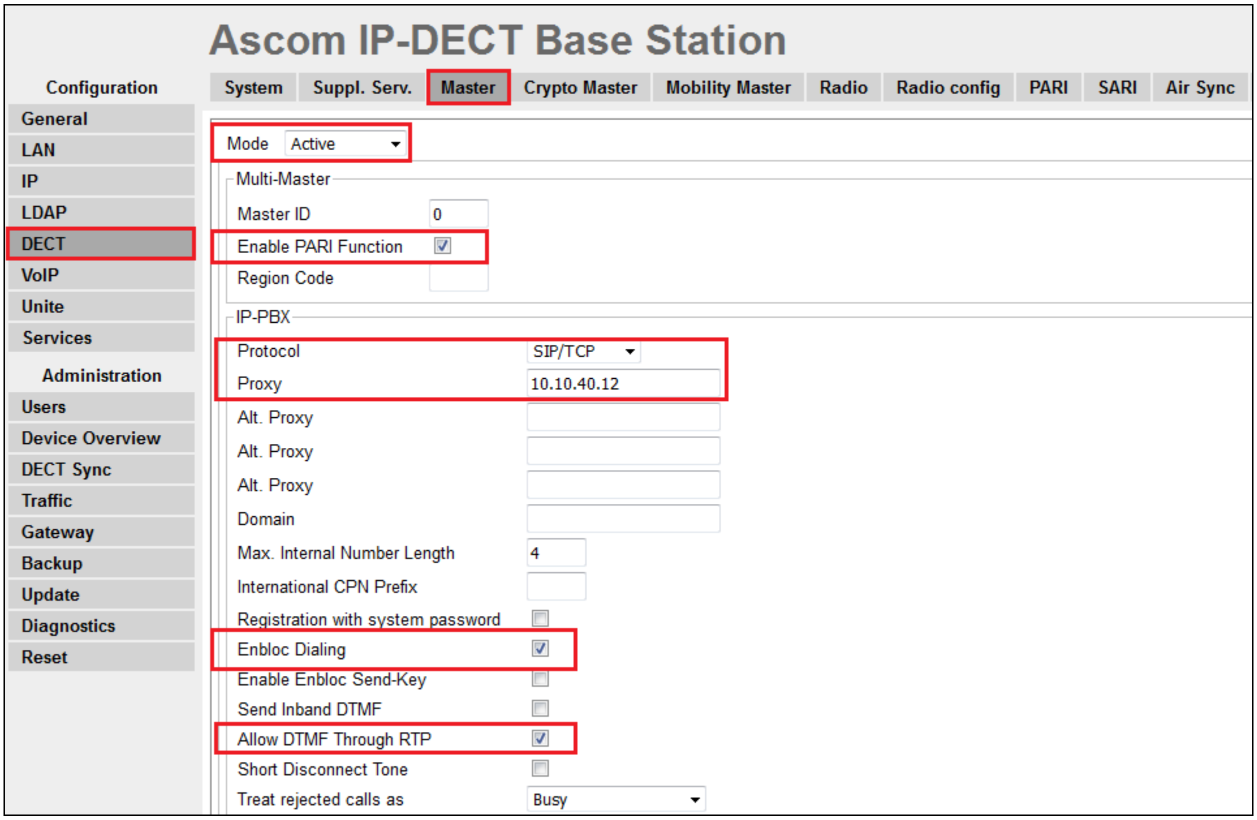


System Name	DECT
Password	••••••••
Confirm Password	••••••••
Subscriptions	With System AC
Authentication Code	1234
Tones	IRELAND
Default Language	English
Frequency	1880-1900 MHz (Europe)
Enabled Carriers	9 ☑ 8 ☑ 7 ☑ 6 ☑ 5 ☑ 4 ☑ 3 ☑ 2 ☑ 1 ☑ 0 ☑
Local R-Key Handling	☑
No Transfer on Hangup	□
No On-Hold Display	□
Display Original Called	□
Early Encryption	□
Coder	G711A Frame (ms) 20 Exclusive □ SC □
Secure RTP Key Exchange	No encryption

8.3. Configure Session Manager Information

Select **DECT** in the left column and select the **Master** tab. Ensure the **Protocol** is set to **SIP/TCP** if TCP is the chosen transport protocol and **SIP/UDP** if UDP is the chosen transport protocol and enter the Session Manager IP address for **Proxy**. Enter the length of digits used for internal numbers. Note, for compliance testing **Enbloc Dialing** and **Allow DTMF through RTP** were ticked but these settings will depend on the customer site and how the Communication Manger is configured. All other values can be accepted as default.

Note: If SIP/TCP is selected below a SIP Entity must be added for the Ascom IP Base Station as per **Section 6.3**.

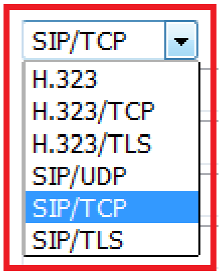


Mode: Active

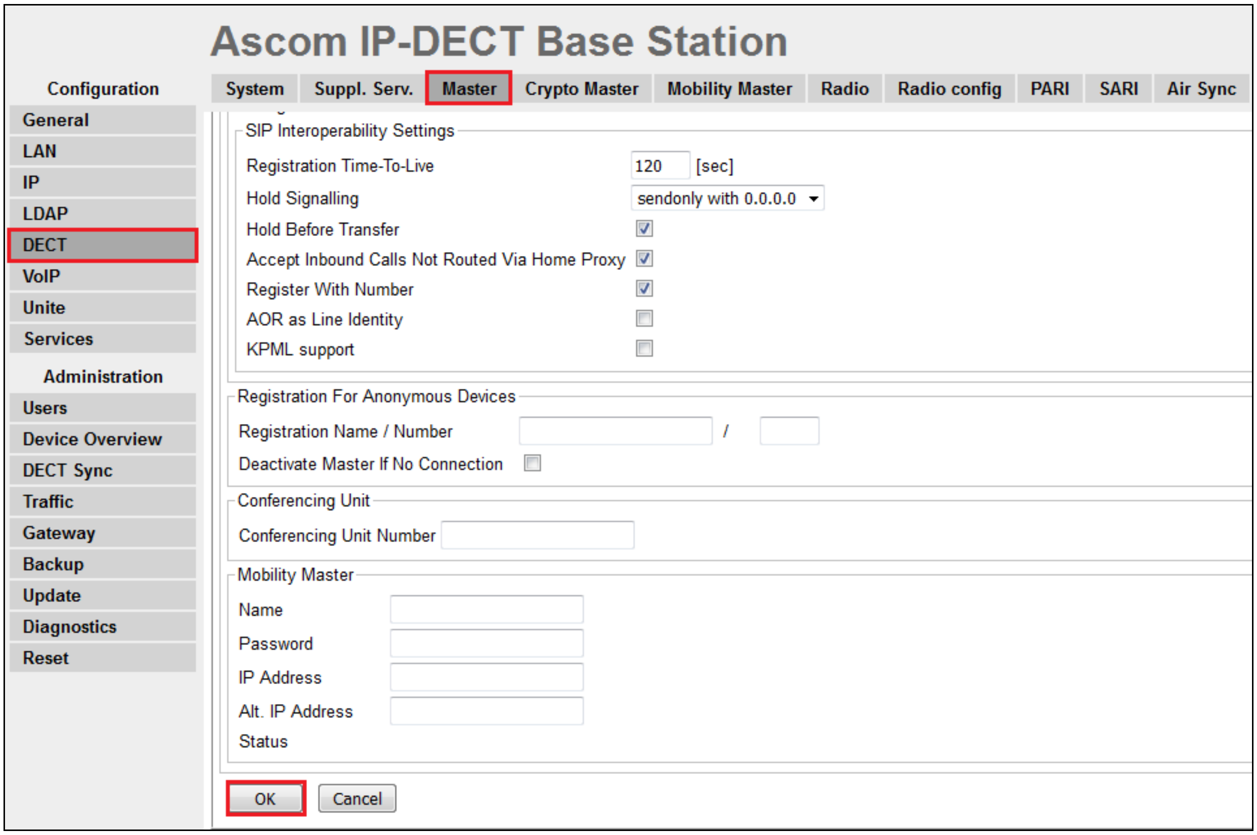
Multi-Master
Master ID: 0
Enable PARI Function ☑
Region Code

IP-PBX
Protocol: SIP/TCP
Proxy: 10.10.40.12
Alt. Proxy
Alt. Proxy
Alt. Proxy
Domain
Max. Internal Number Length: 4
International CPN Prefix
Registration with system password ☐
Enbloc Dialing ☑
Enable Enbloc Send-Key ☐
Send Inband DTMF ☐
Allow DTMF Through RTP ☑
Short Disconnect Tone ☐
Treat rejected calls as: Busy

Note that these are the choices available to set for **Protocol** above.



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



SIP Interoperability Settings

Registration Time-To-Live	120 [sec]
Hold Signalling	sendonly with 0.0.0.0
Hold Before Transfer	☑
Accept Inbound Calls Not Routed Via Home Proxy	☑
Register With Number	☑
AOR as Line Identity	□
KPML support	□

Registration For Anonymous Devices

Registration Name / Number	/
Deactivate Master If No Connection	□

Conferencing Unit

Conferencing Unit Number

Mobility Master

Name

Password

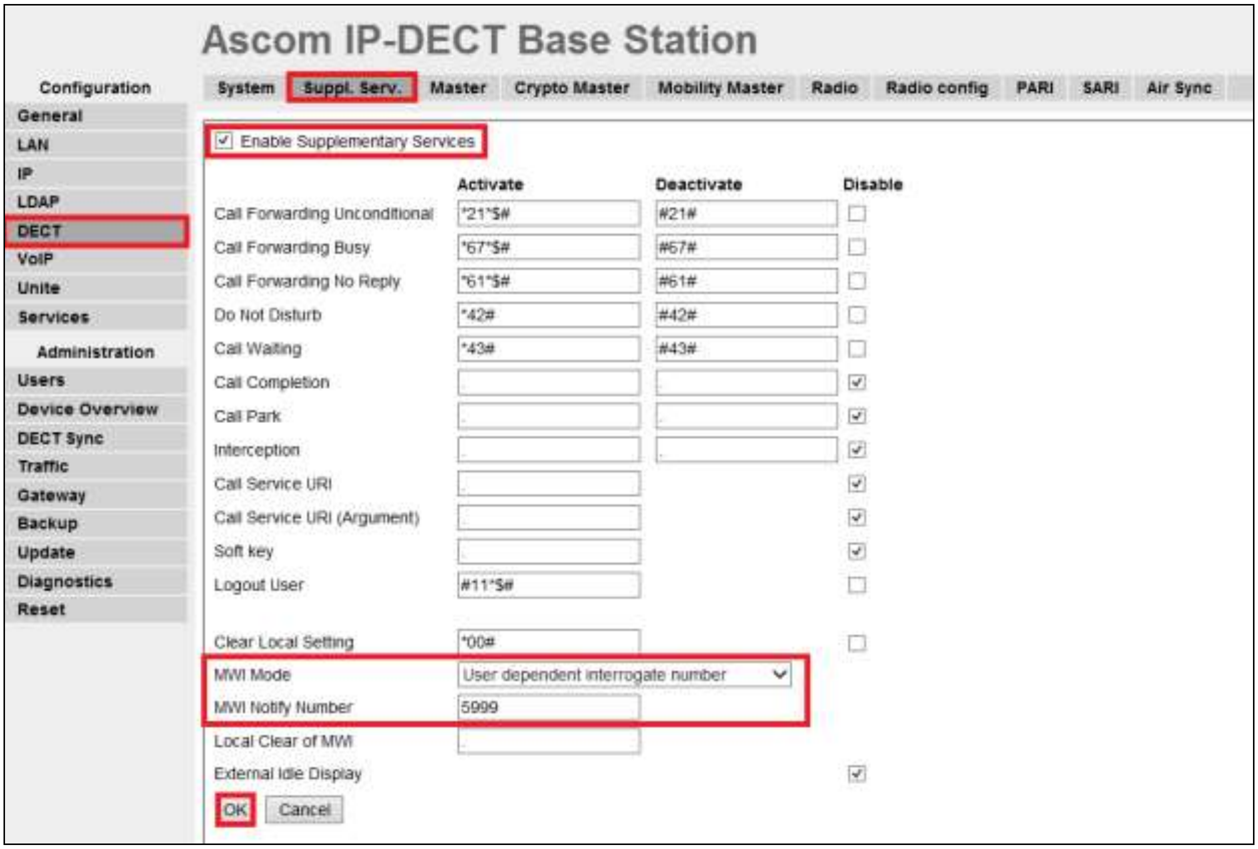
IP Address

Alt. IP Address

Status

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. These codes are unique to the Ascom DECT system.

Note that **MWI Mode** is set to **User dependent interrogate number** and the **MWI Notify Number** is set to the messaging voicemail number for the solution which is **5999**.

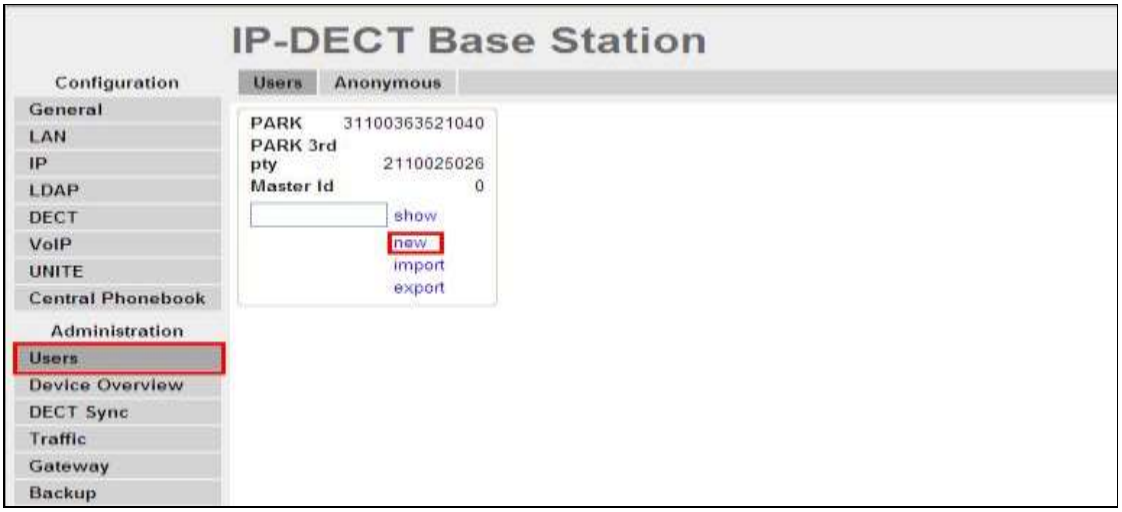


☑ Enable Supplementary Services

	Activate	Deactivate	Disable
Call Forwarding Unconditional	*21*$#	#21#	☐
Call Forwarding Busy	*67*$#	#67#	☐
Call Forwarding No Reply	*61*$#	#61#	☐
Do Not Disturb	*42#	#42#	☐
Call Waiting	*43#	#43#	☐
Call Completion			☑
Call Park			☑
Interception			☑
Call Service URI			☑
Call Service URI (Argument)			☑
Soft key			☑
Logout User	#11*$#		☐
Clear Local Setting	*00#		☐
MWI Mode	User dependent interrogate number		
MWI Notify Number	5999		
Local Clear of MWI			
External Idle Display			☑

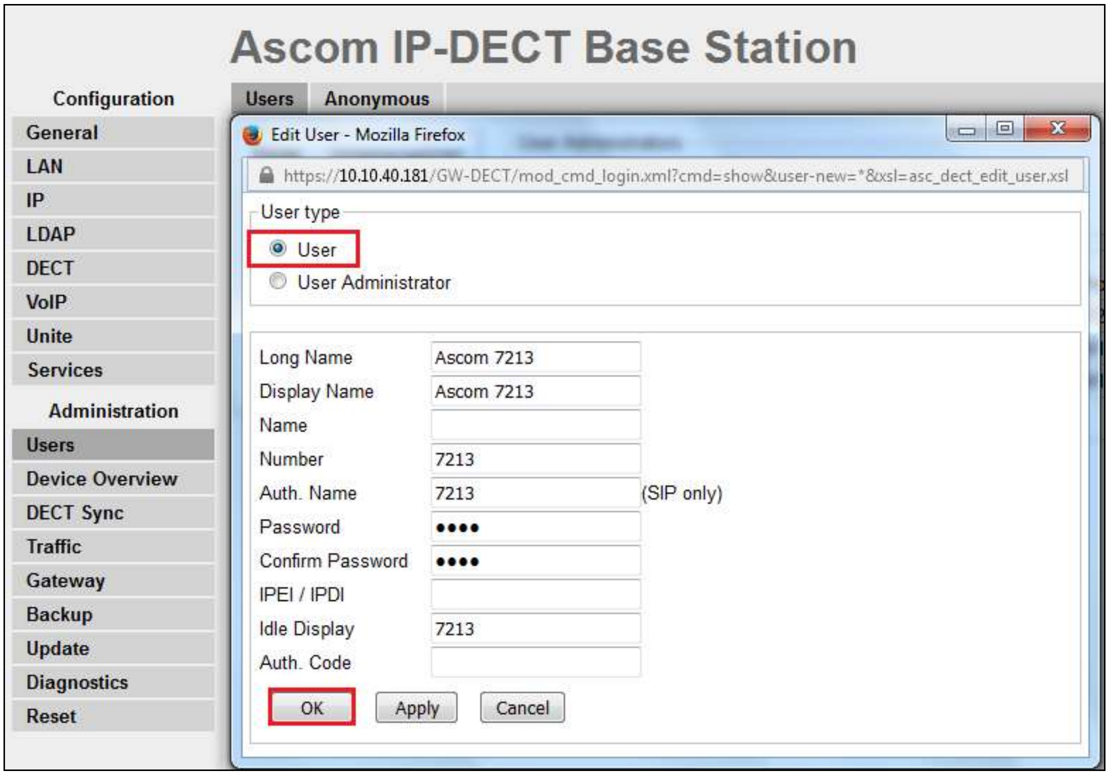
8.4. Adding DECT Users

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



PARK 31100363521040
PARK 3rd pty 2110025026
Master Id 0

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. The Password entered should be the same as that configured in **Section 6.4**.

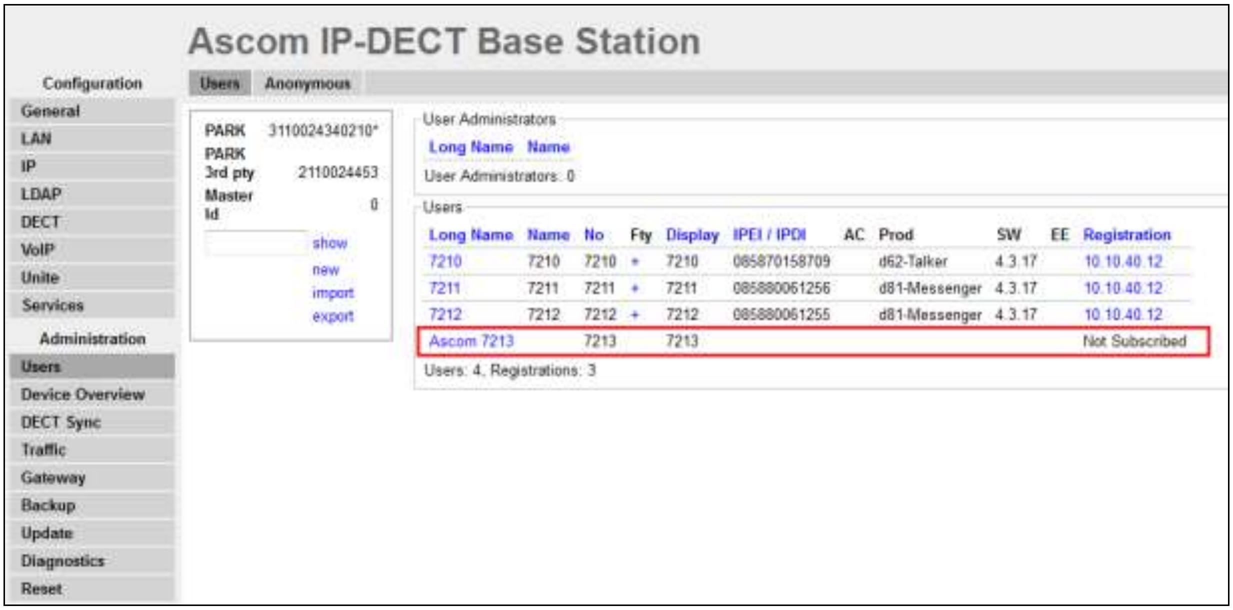


https://10.10.40.181/GW-DECT/mod_cmd_login.xml?cmd=show&user-new=*&xsl=asc_dect_edit_user.xsl

User type
● User
○ User Administrator

Long Name	Ascom 7213
Display Name	Ascom 7213
Name	
Number	7213
Auth. Name	7213 (SIP only)
Password	••••
Confirm Password	••••
IPEI / IPDI	
Idle Display	7213
Auth. Code	

At this point the handset is **Not Subscribed** to the DECT base station; please refer to the DECT Handset user guide (see **Section 11**) in order to correctly subscribe to the base station. Note that every handset may be slightly different to setup but typically navigate to Menu → Settings → System → Subscribe. The park number must be entered correctly, note that the password configured in **Section 8.2** is required here.



Ascom IP-DECT Base Station

PARK	3110024340210*
PARK 3rd pty	2110024453
Master Id	0

User Administrators

Long Name	Name

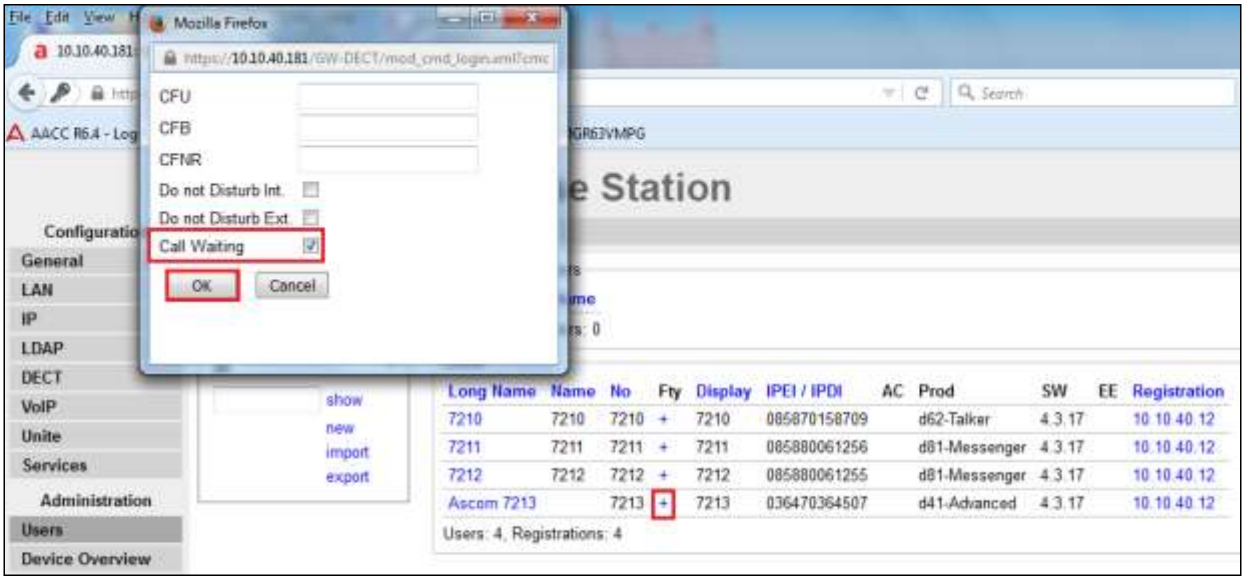
User Administrators: 0

Users

Long Name	Name	No	Fty	Display	IPEI / IPDI	AC	Prod	SW	EE	Registration
7210	7210	7210	+	7210	085870158709		d62-Talker	4.3.17		10.10.40.12
7211	7211	7211	+	7211	085880061256		d81-Messenger	4.3.17		10.10.40.12
7212	7212	7212	+	7212	085880061255		d81-Messenger	4.3.17		10.10.40.12
Ascom 7213		7213		7213						Not Subscribed

Users: 4, Registrations: 3

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.



CFU

CFB

CFNR

Do not Disturb Int. ☐

Do not Disturb Ext. ☐

Call Waiting ☑

Long Name	Name	No	Fty	Display	IPEI / IPDI	AC	Prod	SW	EE	Registration
7210	7210	7210	+	7210	085870158709		d62-Talker	4.3.17		10.10.40.12
7211	7211	7211	+	7211	085880061256		d81-Messenger	4.3.17		10.10.40.12
7212	7212	7212	+	7212	085880061255		d81-Messenger	4.3.17		10.10.40.12
Ascom 7213		7213	+	7213	036470364507		d41-Advanced	4.3.17		10.10.40.12

Users: 4, Registrations: 4

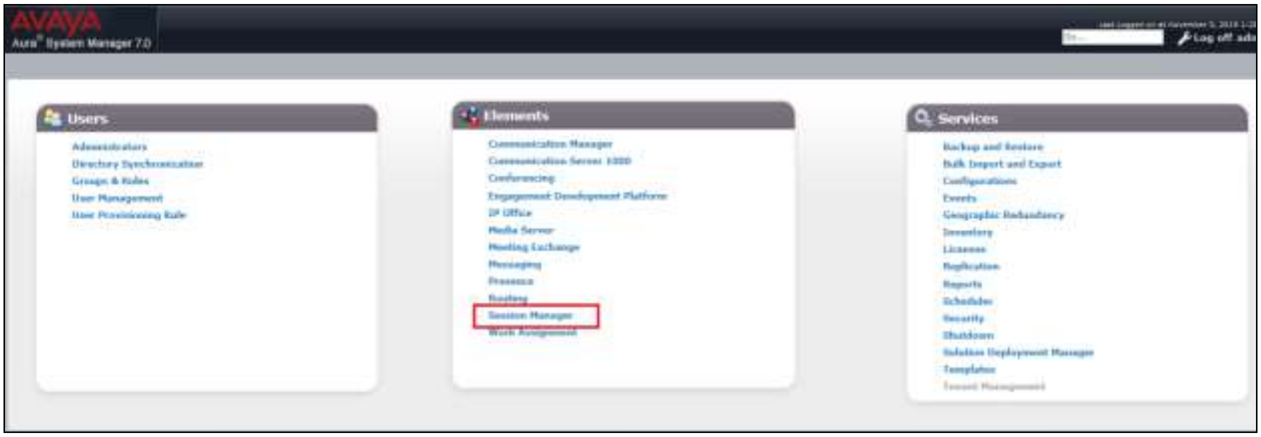
Telephony features, such as Call Waiting and Call Forwarding, can be programmed by entering feature codes on the handset. Please refer to the **Suppl. Serv**. tab in **Section 8.3**.

9. Verification Steps

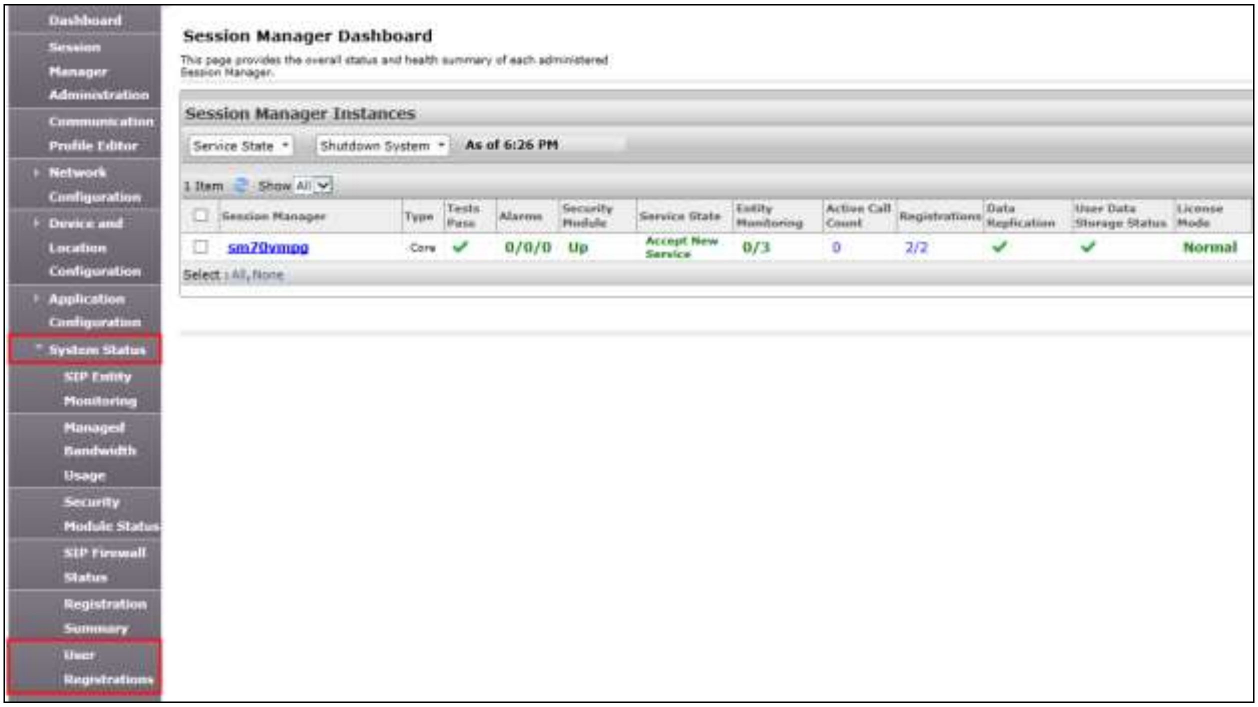
The following steps can be taken to ensure that connections between Ascom DECT handsets and Session Manager and Communication Manager are up.

9.1. Session Manager Registration

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



Under **System Status** in the left window, select **User Registrations** to display all the SIP users that are currently registered with Session Manager.



Session Manager Dashboard

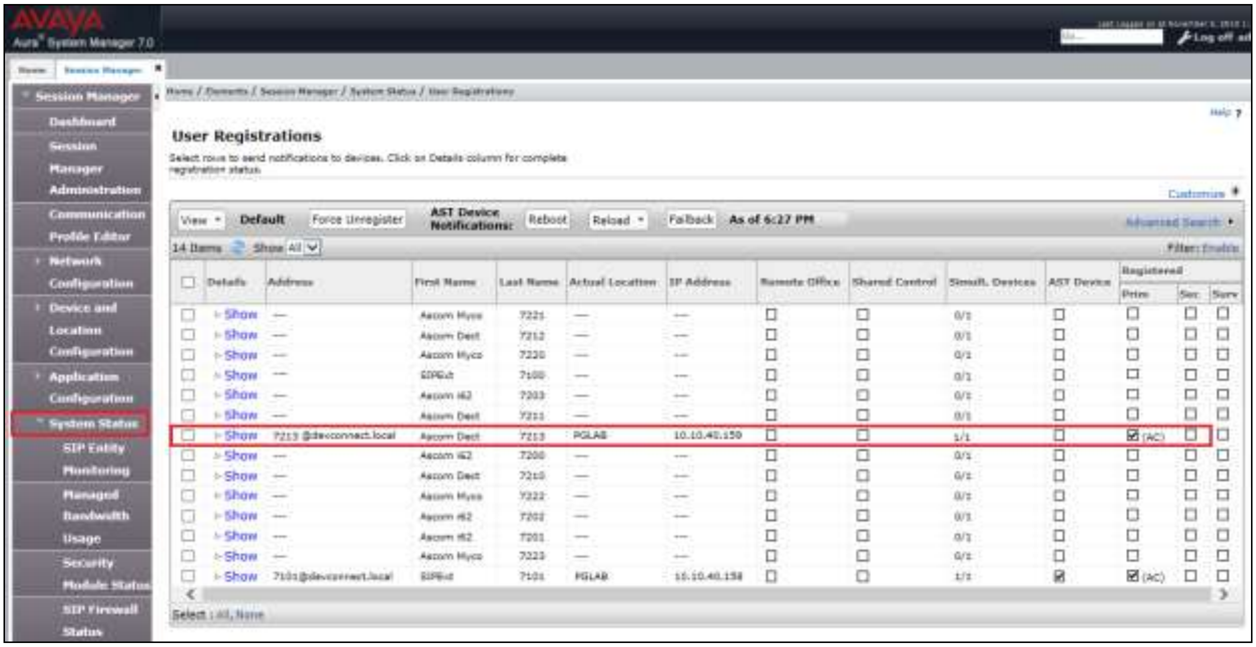
This page provides the overall status and health summary of each administered Session Manager.

Session Manager Instances

As of 6:26 PM

□	Session Manager	Type	Tests Pass	Alarms	Security Module	Service State	Entity Monitoring	Active Call Count	Registrations	Data Replication	User Data Storage Status	License Mode
□	sm70vmpg	Core	✓	0/0/0	Up	Accept New Service	0/3	0	2/2	✓	✓	Normal

The DECT user **7213** should show as being registered as highlighted.



User Registrations

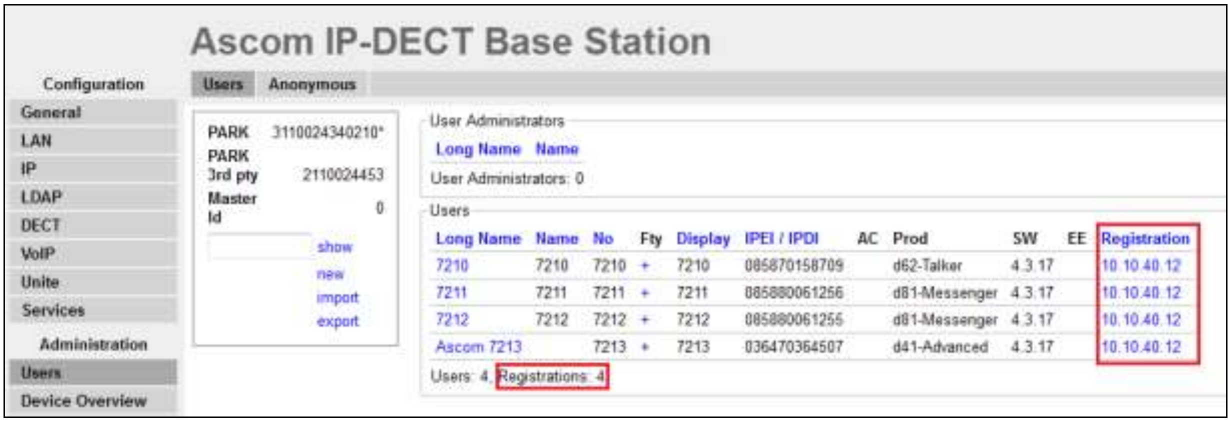
Select rows to send notifications to devices. Click on Details column for complete registration status.

☐	Details	Address	First Name	Last Name	Actual Location	IP Address	Remote Office	Shared Control	Simult. Devices	AST Device	Registered		
											Prim	Sec	Surv
☐	▹ Show	—	Ascom Myco	7221	—	—	☐	☐	0/1	☐	☐	☐	☐
☐	▹ Show	—	Ascom Dect	7212	—	—	☐	☐	0/1	☐	☐	☐	☐
☐	▹ Show	—	Ascom Myco	7220	—	—	☐	☐	0/1	☐	☐	☐	☐
☐	▹ Show	—	SIPExt	7100	—	—	☐	☐	0/1	☐	☐	☐	☐
☐	▹ Show	—	Ascom i62	7203	—	—	☐	☐	0/1	☐	☐	☐	☐
☐	▹ Show	—	Ascom Dect	7211	—	—	☐	☐	0/1	☐	☐	☐	☐
☐	▹ Show	7213 @devconnect.local	Ascom Dect	7213	PGLAB	10.10.40.150	☐	☐	1/1	☐	☑ (AC)	☐	☐
☐	▹ Show	—	Ascom i62	7200	—	—	☐	☐	0/1	☐	☐	☐	☐
☐	▹ Show	—	Ascom Dect	7210	—	—	☐	☐	0/1	☐	☐	☐	☐
☐	▹ Show	—	Ascom Myco	7222	—	—	☐	☐	0/1	☐	☐	☐	☐
☐	▹ Show	—	Ascom i62	7202	—	—	☐	☐	0/1	☐	☐	☐	☐
☐	▹ Show	—	Ascom i62	7201	—	—	☐	☐	0/1	☐	☐	☐	☐
☐	▹ Show	—	Ascom Myco	7223	—	—	☐	☐	0/1	☐	☐	☐	☐
☐	▹ Show	7101@devconnect.local	SIPExt	7101	PGLAB	10.10.40.158	☐	☐	1/1	☑	☑ (AC)	☐	☐

Select : All, None

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**, this displays the DECT handsets that are registered. In the example below, four extensions **7210** to **7213** are registered correctly.



PARK	3110024340210*
PARK 3rd pty	2110024453
Master Id	0

User Administrators

Long Name	Name

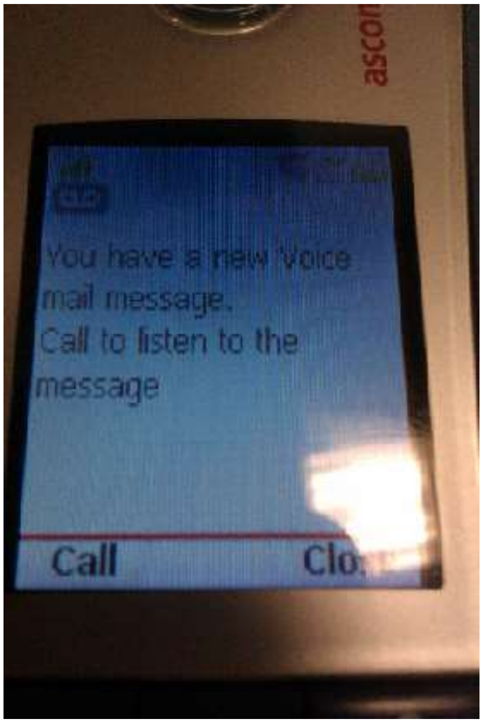
User Administrators: 0

Users

Long Name	Name	No	Fty	Display	IPEI / IPDI	AC	Prod	SW	EE	Registration
7210	7210	7210	+	7210	085870158709		d62-Talker	4.3.17		10.10.40.12
7211	7211	7211	+	7211	085880061256		d81-Messenger	4.3.17		10.10.40.12
7212	7212	7212	+	7212	085880061255		d81-Messenger	4.3.17		10.10.40.12
Ascom 7213		7213	+	7213	036470364507		d41-Advanced	4.3.17		10.10.40.12

Users: 4, Registrations: 4

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.


ascom
You have a new Voice mail message.
Call to listen to the message
Call
Clo

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 R7.0 and Avaya Aura® Session Manager R7.0 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 7.0.x) (TD 92579EN)*

[7] *System Description Ascom IP-DECT System (TD 92375EN)*

[8] *System Planning Ascom IP-DECT System (TD 92422EN)*

[9] *DECT handset user manual*

©2016 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.