



Application Notes for configuring Ascom DECT Handsets and Ascom IPBS2 Access Point with Avaya Aura® Communication Manager and Avaya Aura® Session Manager– 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 attention to **Section 2**, in particular the scope of testing as outlined in **Section 2.1** as well as any 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 and Avaya Aura® Session Manager. 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 9640 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". Refer to **Section 6.3** for configuration details.

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 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.

Avaya recommends our customers implement Avaya solutions using appropriate security and encryption capabilities enabled by our products. The testing referenced in these DevConnect Application Notes included the enablement of supported encryption capabilities in the Avaya products. Readers should consult the appropriate Avaya product documentation for further information regarding security and encryption capabilities supported by those Avaya products.

Support for these security and encryption capabilities in any non-Avaya solution component is the responsibility of each individual vendor. Readers should consult the appropriate vendor-supplied product documentation for more information regarding those products.

For the testing associated with these Application Notes, the interface between Avaya systems and Ascom DECT handsets did not include use of any specific encryption features as requested by Ascom.

Avaya's formal testing and Declaration of Conformity is provided only on the headsets/Smartphones that carry the Avaya brand or logo. Avaya may conduct testing of non-Avaya headset/handset to determine interoperability with Avaya phones. However, Avaya does not conduct the testing of non-Avaya headsets/Smartphones for: Acoustic Pressure, Safety, Hearing Aid Compliance, EMC regulations, or any other tests to ensure conformity with safety, audio quality, long-term reliability or any regulation requirements. As a result, Avaya makes no representations whether a particular non-Avaya headset will work with Avaya's telephones or with a different generation of the same Avaya telephone.

Since there is no industry standard for handset interfaces, different manufacturers utilize different handset/headset interfaces with their telephones. Therefore, any claim made by a headset vendor that its product is compatible with Avaya telephones does not equate to a guarantee that the headset will provide adequate safety protection or audio quality.

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
- Media Shuffling
- Session Refresh Timer
- Long Duration Call
- Hold and Long Hold, Retrieve and Brokering (Toggle)
- Feature Access Code dialing with special characters
- Attended, Semi-attended and Blind Transfer
- Call Forwarding Unconditional, No Reply and Busy
- Call Waiting
- Call Park/Pickup
- EC500, where Avaya deskphone is the primary phone and DECT handset being the EC500 destination
- Conference
- Do Not Disturb
- Calling Line Name/Identification
- Codec Support (G.711, G.729, G.722.2 tested)
- DTMF Support
- Voice Mail, Message Waiting Indication
- Serviceability

Note: Multi-Device Access (MDA) is not supported.

2.2. Test Results

Tests were performed to verify interoperability between Ascom DECT handsets and Communication Manager desk phones. The tests were all functional in nature and performance testing was not included. The following observations/limitations were noted during testing:

1. All compliance testing was done using UDP and TCP (preferred) as the transport protocol.
2. Negotiation of G.722.2 between endpoints, such as the Ascom DECT handset, requires support for the codec to be configured on Communication Manager.
3. A SIP Entity with “Endpoint Concentrator” assigned was set up for both the Master and Standby Base Stations, the corresponding TCP entity links need to be of type “untrusted”.
4. With regard to Shuffling and Direct media is ON - When an Ascom DECT set calls another Ascom DECT set, the media still goes through the Avaya Media Gateway regardless of Direct Media being on. This is obvious when DECT is used as there is only one IP address for both the source and the endpoint.

5. When using local diversion for call forward all calls, no answer and busy on the Ascom DECT handsets, note that for busy the call actually is not forwarded but caller hears a busy tone since the Communication Manager returns a 486 BUSY HERE instead of forwarding the INVITE to the IP-DECT master.
6. When an Avaya endpoint or a DECT handset calls another DECT handset, after the called DECT handset declines the call, the display for the DECT calling party shows busy whereas the Avaya calling party receives the busy tone.
7. In the scenario where an Avaya station calls DECT1 and DECT1 does a semi-attended transfer to DECT2. The DECT2 display shows DECT1 information instead of the Avaya station information until the call is answered.
8. In a scenario where DECT calls PSTN. PSTN does attended transfer to Avaya station and completes transfer. The Avaya station and DECT handset display show PSTN information.
9. As per current design, DECT handsets cannot initiate a conference however are able to join a conference.
10. DECT handsets do not have a redial button. User needs to use “Call List” and redial the numbers.
11. When outgoing calls are restricted for a DECT handset, the display shows “Hung Up” when users attempt to make an outbound call.
12. As per current design, DECT handsets do not support Multi-Device Access (MDA).
13. When using the EC500 (concurrent call) feature, if DECT handset or an Avaya endpoint answers the call before two rings, the call is dropped. This is due to the “Cellular Voice Mail Detection” field default value seen in “off-pbx-telephone configuration-set” form of Communication Manager. The default value for this field is “timed (seconds): 4” which means that if Communication Manager receives an answer within 4 seconds then it will be considered as the cellular voicemail picking up the call, and so call will be dropped and proceed to do Communication Manager coverage processing instead. The workaround is to answer the call after 2 rings, or change the “Cellular Voice Mail Detection” field value to “none” or decrease “timed” value. Note that changing the “off-pbx-telephone configuration-set” affects all users in the same set, so if cellular users are grouped with DECT handset users, calls may be answered by a cellular user’s voicemail instead of following the coverage criteria in Communication Manager.
14. A DECT handset is configured on an Avaya station as EC500. Call Avaya station, both Avaya station and DECT handset rings. Decline the call at DECT handset, Avaya station continues to ring as per normal design.

2.3. Support

Technical support for the Ascom DECT handsets can be obtained through a local Ascom supplier or Ascom global technical support:

- Email: support@ascom.com
- 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. During compliance testing the DECT base stations were configured by accessing it via a web interface using a laptop.

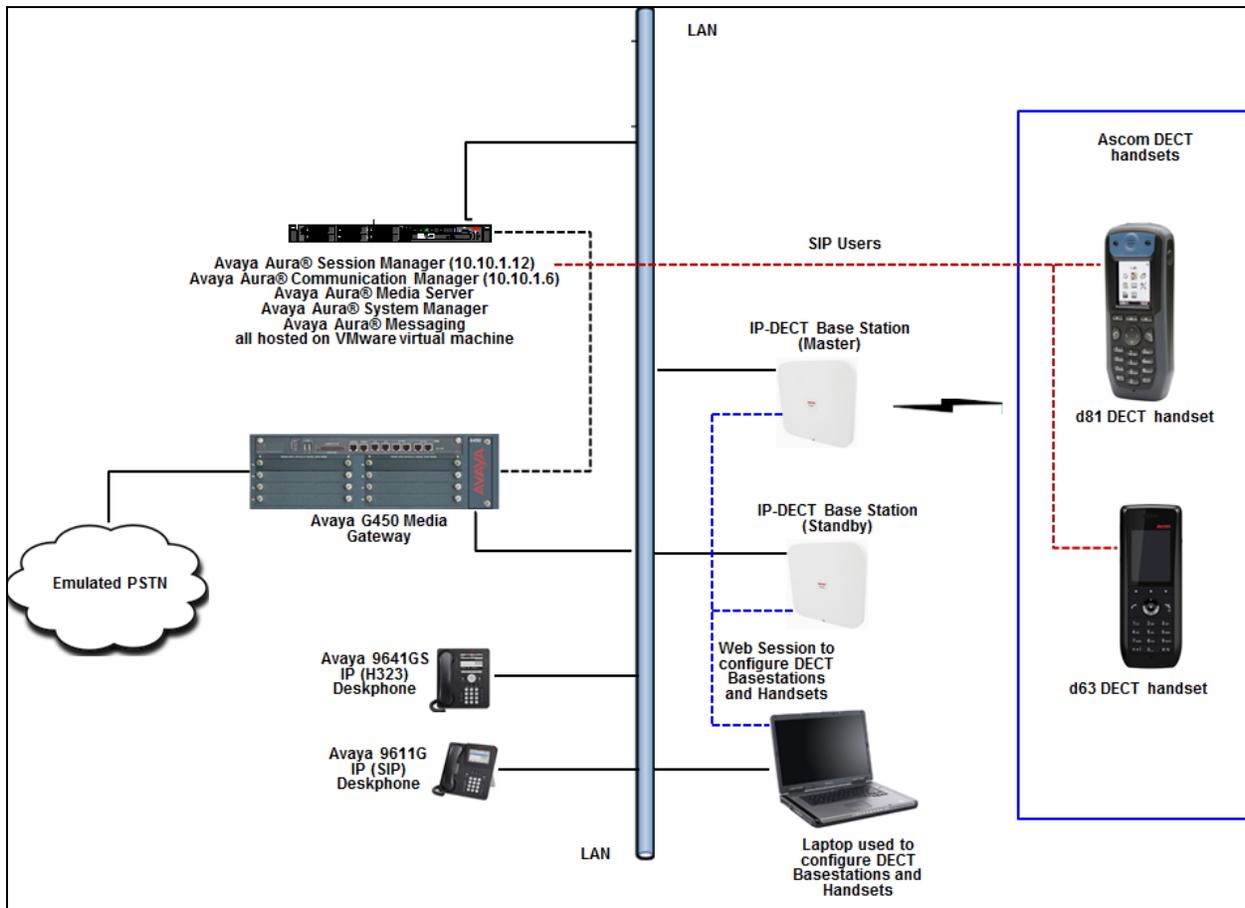


Figure 1: Network Solution of Ascom DECT Handsets with Avaya Aura® Communication Manager and Avaya Aura® Session Manager

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya Aura® Communication Manager running on Virtual Server	7.1.2.0.0-FP2
Avaya Aura® Session Manager running on Virtual Server	7.1.2.0.712004
Avaya Aura® System Manager running on Virtual Server	7.1.2.0 (Feature Pack 2)
Avaya Aura® Messaging running on Virtual Server	07.0.0.0.441
Avaya G450 Gateway	38 .18 .0 /1
Avaya IP Telephones: <ul style="list-style-type: none">• 9641GS (H.323)• 9611G (SIP)	6.6506 7.1.1.0.9
Ascom DECT Master Base Station Ascom DECT Standby Base Station	IPBS2 10.1.4 (update 1)
Ascom DECT Handsets: <ul style="list-style-type: none">• d81• d63	4.6.2 2.2.2

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 10** 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.

Ensure that the SIP endpoints license is valid as shown below by using the command **display system-parameters customer-options**.

```
display system-parameters customer-options                               Page 1 of 12
                                OPTIONAL FEATURES

G3 Version: V17                Software Package: Enterprise
Location: 2                    System ID (SID): 1
Platform: 28                   Module ID (MID): 1

                                USED
Platform Maximum Ports: 48000 168
Maximum Stations: 36000 44
Maximum XMOBILE Stations: 36000 0
Maximum Off-PBX Telephones - EC500: 41000 2
Maximum Off-PBX Telephones - OPS: 41000 20
Maximum Off-PBX Telephones - PBFMC: 41000 0
Maximum Off-PBX Telephones - PVFMC: 41000 0
Maximum Off-PBX Telephones - SCCAN: 0 0
Maximum Survivable Processors: 313 1
```

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 **33** and **34**. Feature Access Codes (**fac**) use digits **8** and **9**. Dial Access Codes (**dac**) use characters ***** or **#**.

```

change dialplan analysis                                     Page 1 of 12
                                                           DIAL PLAN ANALYSIS TABLE
                                                           Location: all                                     Percent Full: 5

```

Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type
33	4	ext						
30	4	aar						
33	4	ext						
8	1	fac						
9	1	fac						
*	3	dac						
#	3	dac						

5.2. Configure Feature Access Codes

Use the **change feature-access-codes** command to configure access codes which can be entered from DECT handsets to initiate Communication Manager Call features. These access codes must be compatible with the dial plan described in **Section 5.1**. Some of the access codes configured during compliance testing are shown below.

```

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: *05
Answer Back Access Code: 007
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: *07 All: *06   Deactivation: *16
Call Forwarding Enhanced Status: Act:               Deactivation:
Call Park Access Code: 008
Call Pickup Access Code: *09
CAS Remote Hold/Answer Hold-Unhold Access Code: *10
CDR Account Code Access Code: *11
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 **bvwddev.com** is used. Note that 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              NR Group: 1
Location: 1           Authoritative Domain: bvwddev.com
  Name: Loc-1         Stub Network Region: n
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? n
  UDP Port Max: 3329
DIFFSERV/TOS PARAMETERS
  Call Control PHB Value: 46
    Audio PHB Value: 46
    Video PHB Value: 26
802.1P/Q PARAMETERS
  Call Control 802.1p Priority: 6
    Audio 802.1p Priority: 6
    Video 802.1p Priority: 5
H.323 IP ENDPOINTS   AUDIO RESOURCE RESERVATION PARAMETERS
  H.323 Link Bounce Recovery? y      RSVP Enabled? n
  Idle Traffic Interval (sec): 20
  Keep-Alive Interval (sec): 5
```

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 DECT Handsets. During compliance testing the codecs **G.711MU**, **G.729**, **G.723** and **G.722-64K (G.722.2)** were tested.

```
change ip-codec-set 1                                     Page 1 of 2

                                IP MEDIA PARAMETERS

Codec Set: 1

Audio      Silence      Frames      Packet
Codec      Suppression  Per Pkt    Size(ms)
1: G.711MU      n           2          20
2: G.729        n           2          20
3: G.722-64K    2           2          20
4:
5:
6:
7:

Media Encryption                               Encrypted SRTCP: enforce-unenc-srtcp
1: none
2:
3:
4:
5:
```

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 **2**: The coverage path will be used after 2 rings.

Point 1 is set to **h4**: Hunt Group 4 is utilised by this coverage path.

```
display coverage path 4
                                COVERAGE PATH
                                Coverage Path Number: 4
                                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: 2
    All?                  n             n
  DND/SAC/Goto Cover?   y             y
  Holiday Coverage?     n             n

COVERAGE POINTS
  Terminate to Coverage Pts. with Bridged Appearances? n
  Point1: h4           Rng:         Point2:
  Point3:                Point4:
  Point5:                Point6:
```

The hunt group used for compliance testing is shown below. Note that on **Page 1** the **Group Extension** is **3333**, which is used to dial for messaging and on **Page 2 Message Center** is set to **sip-adjunct**.

```
display hunt-group 4                                     Page 1 of 60
                                     HUNT GROUP
Group Number: 4                                         ACD? n
Group Name: AMM                                         Queue? n
Group Extension: 3333                                   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:
```

```
display hunt-group 4                                     Page 2 of 60
                                     HUNT GROUP
                                     Message Center: sip-adjunct
Voice Mail Number      Voice Mail Handle      Routing Digits
                       3000                                (e.g., AAR/ARS Access Code)
3000
```

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:

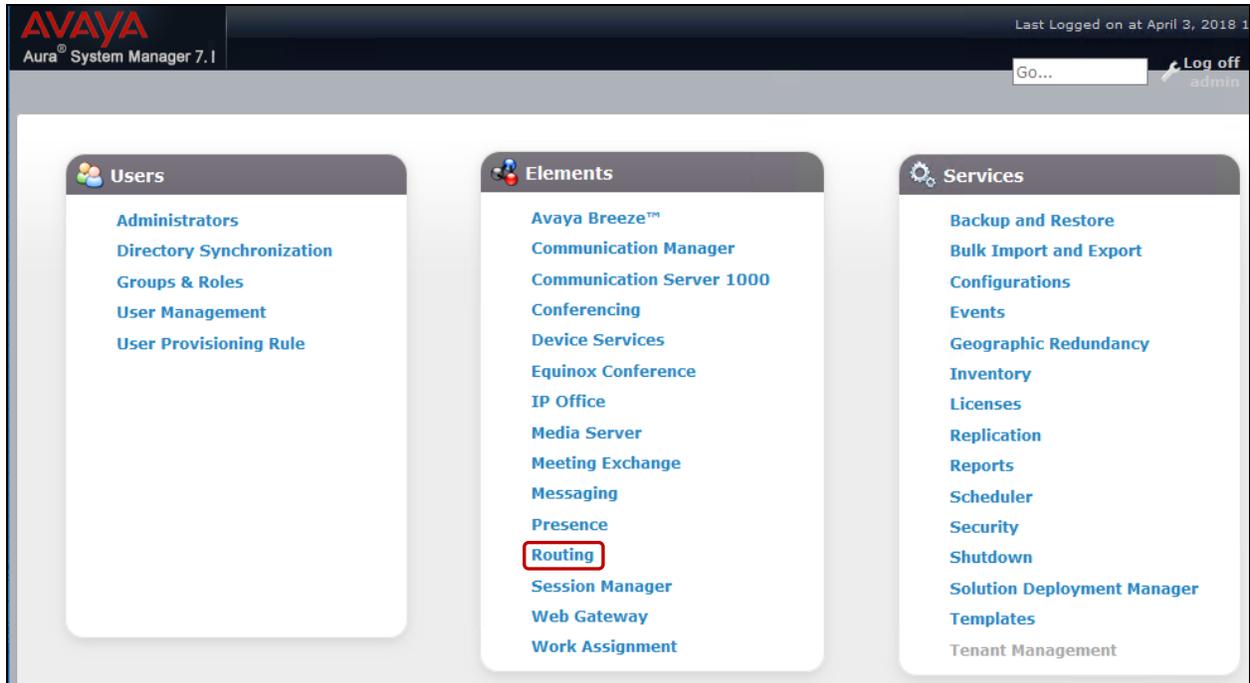
Password:

[Change Password](#)

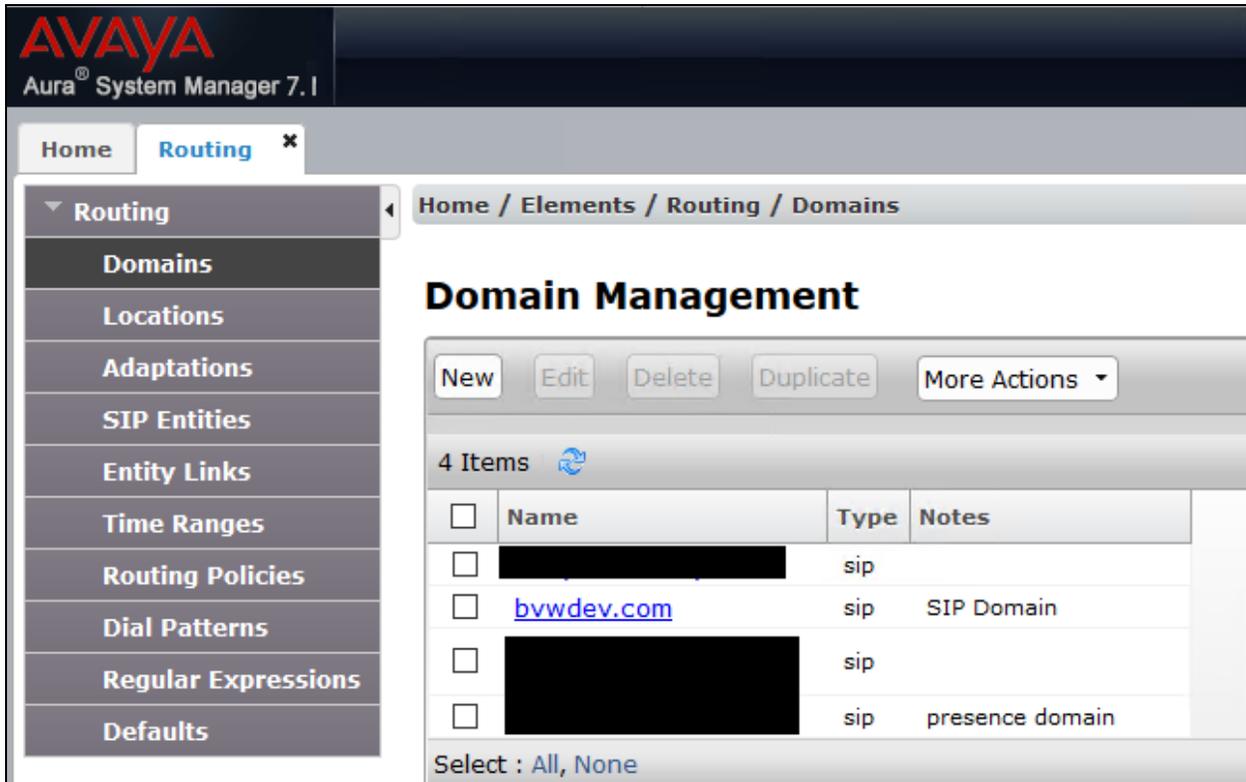
Supported Browsers: Internet Explorer 11.x or Firefox 48.0, 49.0 and 50.0.

6.1. Configuration of a Domain

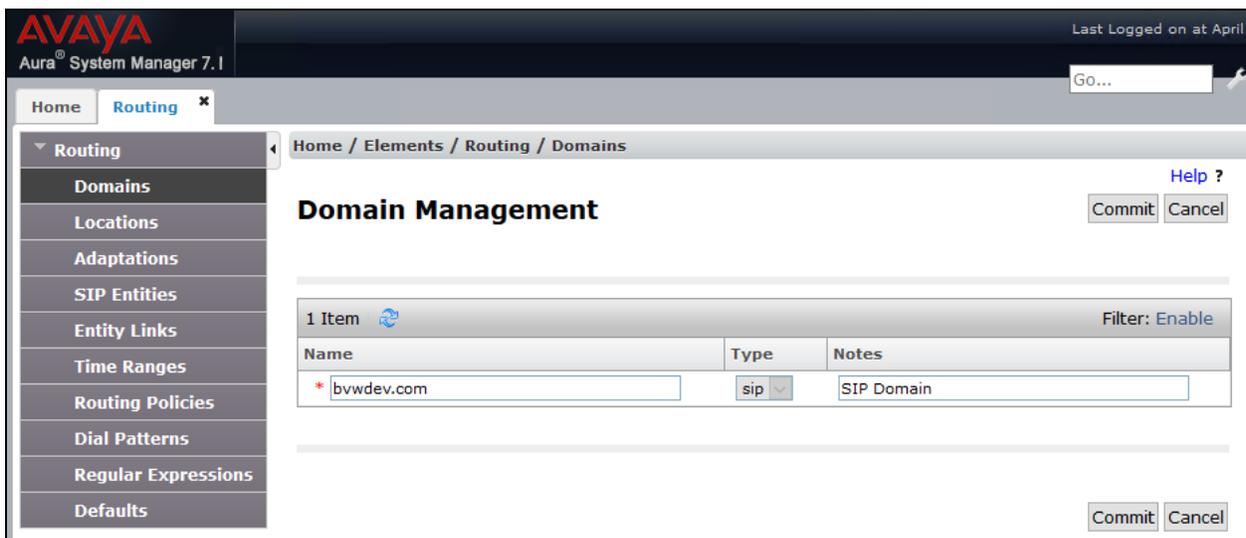
Click on **Routing** highlighted below.



Click on **Domains** in the left window. If there is not a domain already configured click on **New** to create a new domain name with **Type sip**. In the example below, there exists a domain called **bvwdev.com** which has been already configured.



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.



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** to create a new location. However, in the screen below, a location called **CM71** is already setup and click into this to show its contents.

The screenshot shows the Avaya Aura System Manager 7.1 interface. The top left corner displays the Avaya logo and the text 'Aura® System Manager 7.1'. Below this, there are tabs for 'Home' and 'Routing'. The 'Routing' tab is active, and a sidebar on the left lists various configuration options: Routing, Domains, Locations (selected), Adaptations, SIP Entities, Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area is titled 'Location' and features a breadcrumb trail: 'Home / Elements / Routing / Locations'. Below the title, there are buttons for 'New', 'Edit', 'Delete', 'Duplicate', and a 'More Actions' dropdown. A status bar indicates '11 Items' with a refresh icon. A table lists the locations with columns for 'Name', 'Correlation', and 'Notes'. The 'CM71' location is highlighted in blue. At the bottom of the table, there is a 'Select : All, None' option.

<input type="checkbox"/>	Name	Correlation	Notes
<input type="checkbox"/>	[REDACTED]	<input type="checkbox"/>	Aura Messaging Location
<input type="checkbox"/>	[REDACTED]	<input type="checkbox"/>	Simulated as public PSTN
<input type="checkbox"/>	[REDACTED]	<input type="checkbox"/>	Cisco Location
<input type="checkbox"/>	CM71	<input type="checkbox"/>	Interop CM 7.1
<input type="checkbox"/>	[REDACTED]	<input type="checkbox"/>	CS1K Car2 Cores
<input type="checkbox"/>	[REDACTED]	<input type="checkbox"/>	Experience Portal 7.1
<input type="checkbox"/>	[REDACTED]	<input type="checkbox"/>	Genesis Location
<input type="checkbox"/>	[REDACTED]	<input type="checkbox"/>	Avaya IP Office SE
<input type="checkbox"/>	[REDACTED]	<input type="checkbox"/>	IP Phone Location

Select : All, None

The Location below shows **Name** with **Location Pattern** of **10.10.1.6**. Once this is configured, click on **Commit**.

The screenshot displays the Avaya Aura System Manager 7.1 interface. The top navigation bar includes the Avaya logo, the text "Aura System Manager 7.1", and a search box with "Go...". The breadcrumb trail is "Home / Elements / Routing / Locations".

The main content area is titled "Location Details" and includes "Commit" and "Cancel" buttons. It is divided into two sections:

- General:**
 - * Name:
 - Notes:
- Dial Plan Transparency in Survivable Mode:**
 - Enabled:
 - Listed Directory Number:
 - Associated CM SIP Entity:

Below this is the "Location Pattern" section, which includes "Add" and "Remove" buttons. It shows a table with 1 item and a "Filter: Enable" option.

<input type="checkbox"/>	IP Address Pattern	Notes
<input type="checkbox"/>	* 10.10.1.6	

At the bottom of the "Location Pattern" section, it says "Select : All, None".

At the bottom right of the entire form, there are "Commit" and "Cancel" buttons.

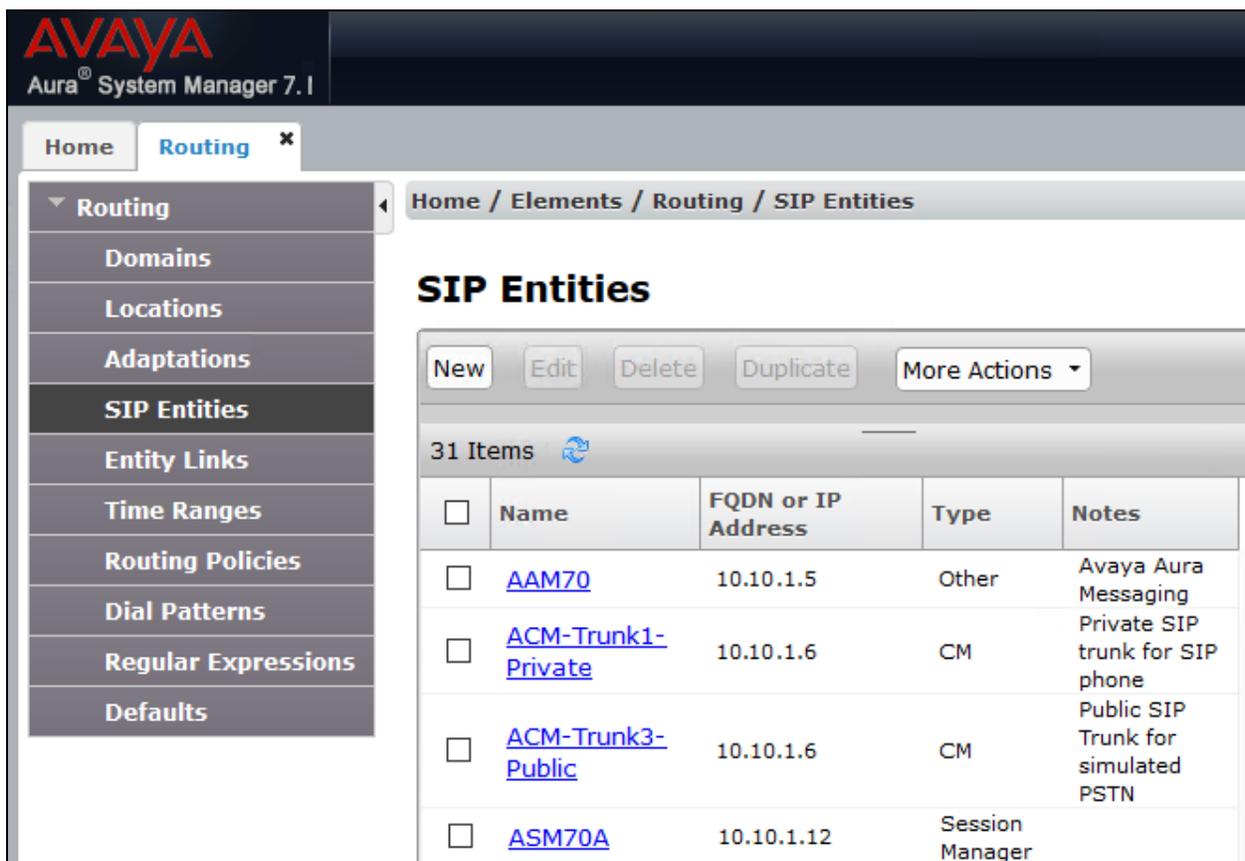
6.3. Configuration of SIP Entities

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 7.3**, 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 IPBS2. Select **SIP Entities** in the left window and click on **New** in the main window.

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



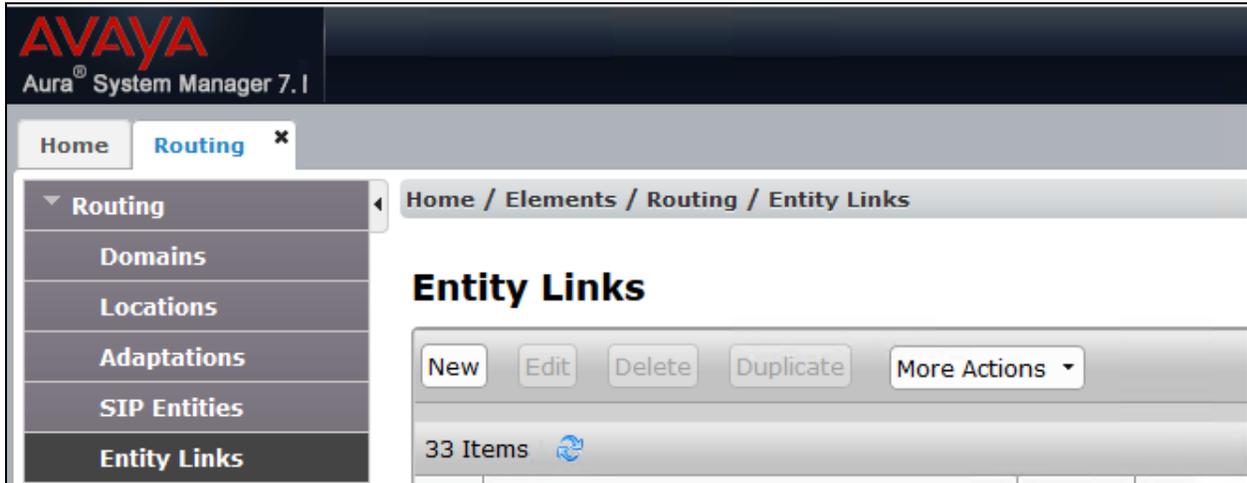
The screenshot shows the Avaya Aura System Manager 7.1 interface. The left sidebar contains a navigation menu with the following items: Routing, Domains, Locations, Adaptations, SIP Entities (highlighted), Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area is titled "SIP Entities" and includes a breadcrumb trail: Home / Elements / Routing / SIP Entities. Below the title, there are buttons for "New", "Edit", "Delete", "Duplicate", and "More Actions". A status bar indicates "31 Items". The main content is a table with the following data:

<input type="checkbox"/>	Name	FQDN or IP Address	Type	Notes
<input type="checkbox"/>	AAM70	10.10.1.5	Other	Avaya Aura Messaging
<input type="checkbox"/>	ACM-Trunk1-Private	10.10.1.6	CM	Private SIP trunk for SIP phone
<input type="checkbox"/>	ACM-Trunk3-Public	10.10.1.6	CM	Public SIP Trunk for simulated PSTN
<input type="checkbox"/>	ASM70A	10.10.1.12	Session Manager	

Enter a suitable **Name** and enter the **IP Address** of the DECT Base Station. Select **Endpoint Concentrator** as the **Type**. Click on **Commit** (not shown) once completed.

The screenshot shows the Avaya Aura System Manager 7.1 web interface. The top navigation bar includes the Avaya logo and the text "Aura System Manager 7.1". Below this, there are tabs for "Home" and "Routing". A left-hand navigation menu is expanded to show "Routing" with sub-items: Domains, Locations, Adaptations, SIP Entities (highlighted), Entity Links, Time Ranges, Routing Policies, and Dial Patterns. The main content area displays the breadcrumb "Home / Elements / Routing / SIP Entities" and the title "SIP Entity Details". Under the "General" section, the following fields are visible: "Name" with the value "MasterBaseStation", "FQDN or IP Address" with the value "10.10.5.206", "Type" with a dropdown menu set to "Endpoint Concentrator", and "Notes" with the value "Master base station for Ascom".

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



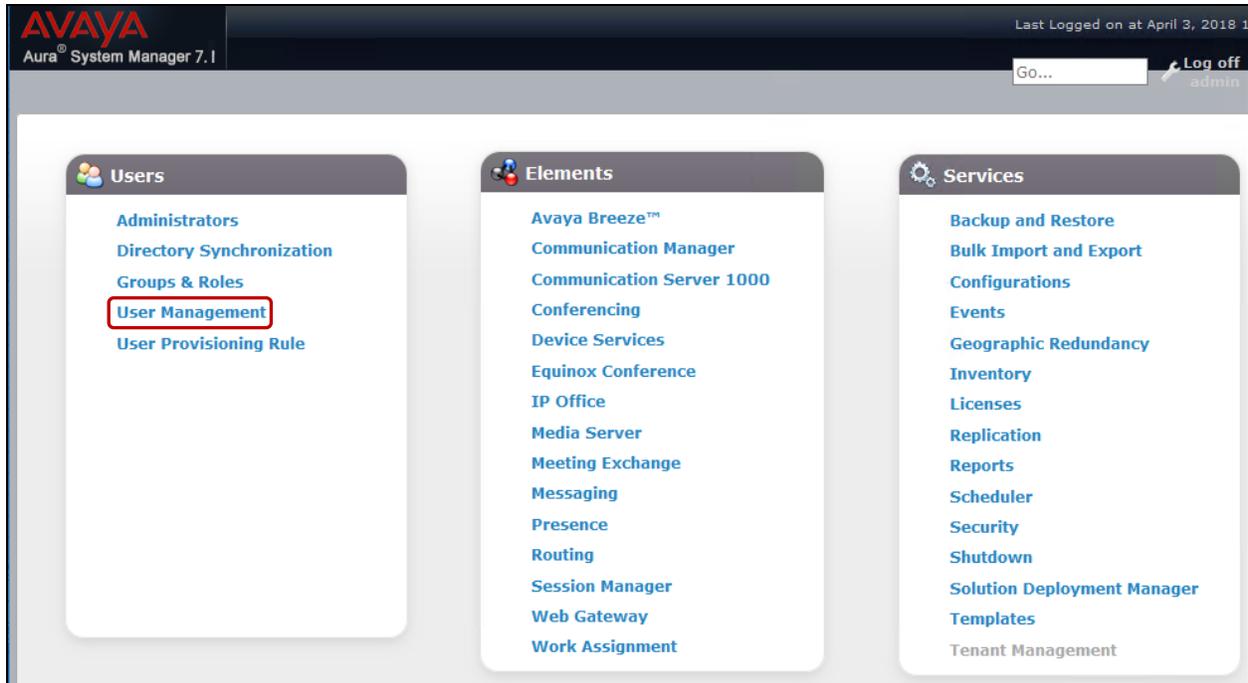
Ensure that **TCP** is selected for the **Protocol** and **5060** for the **Port**. Click on **Commit** once completed.



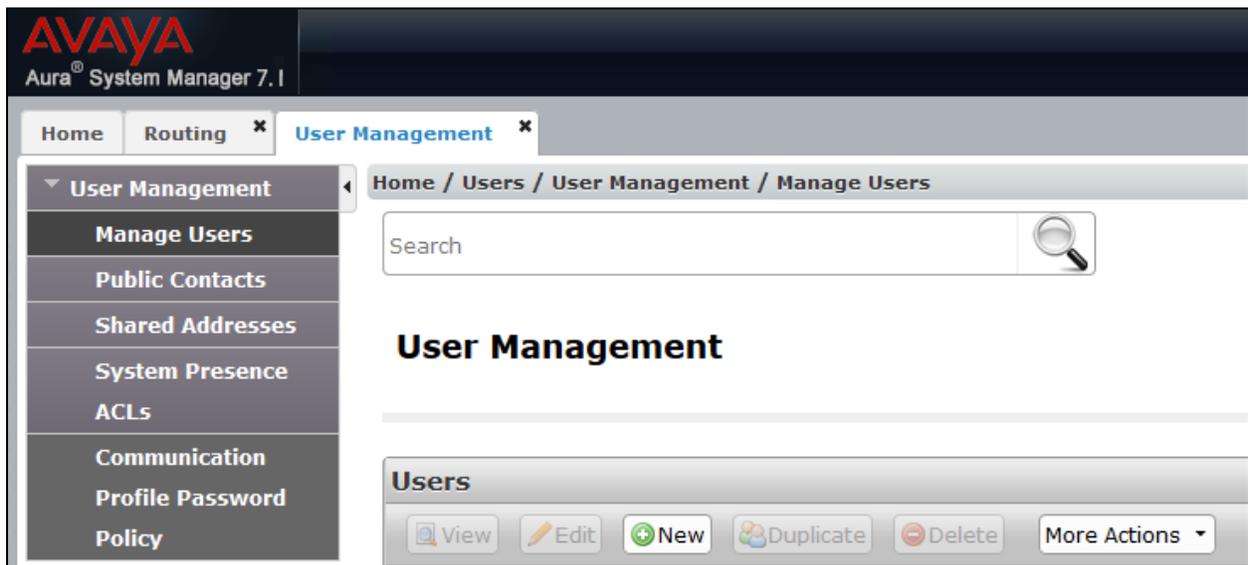
A SIP Entity and Entity link must be added for both the Ascom Master base station and the Ascom Slave (Standby) base station.

6.4. Adding Ascom SIP Users

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



From **Manager Users** section, click on **New** to add a new SIP user.

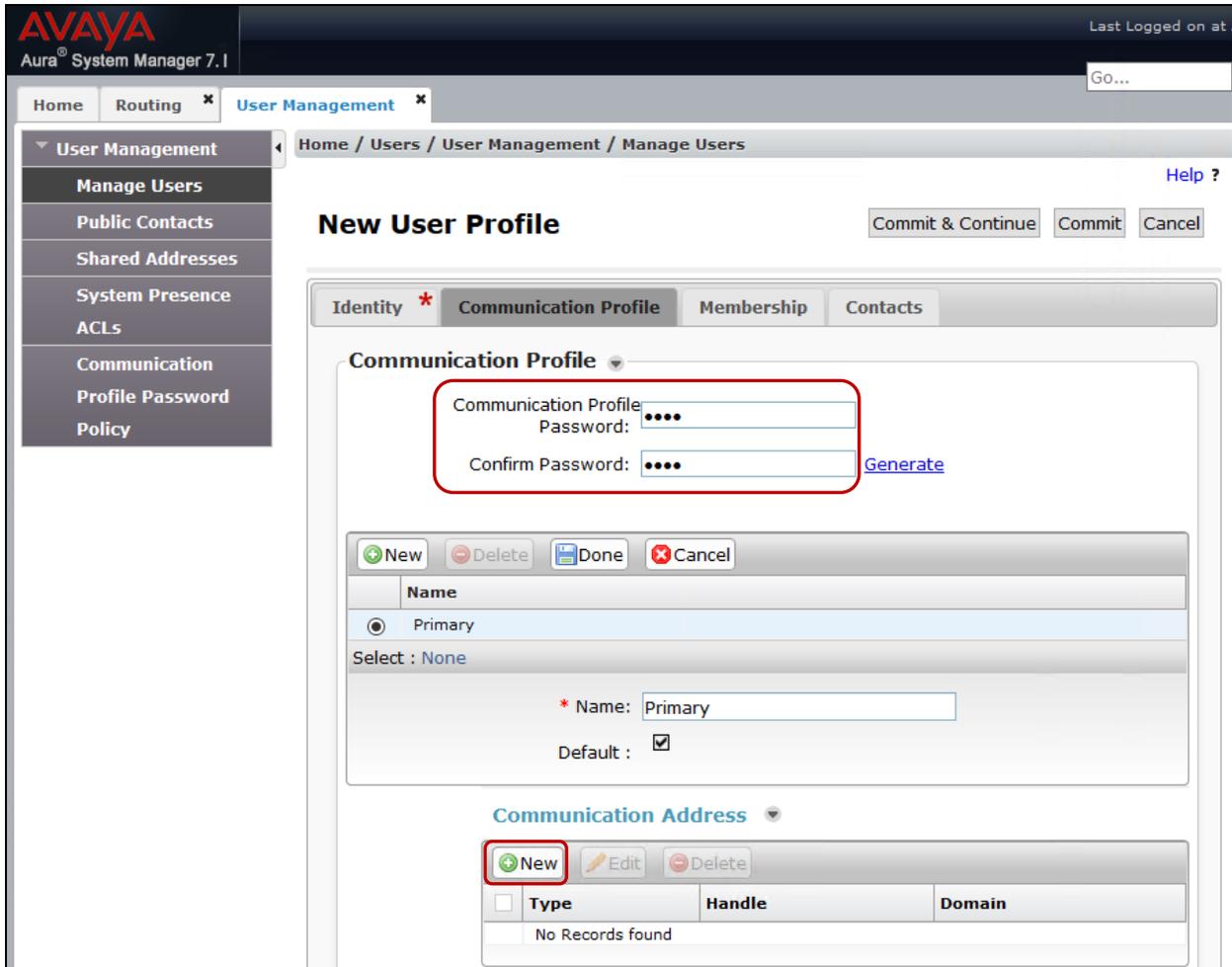


Under the **Identity** tab fill in the user's **Last Name** and **First Name** as shown below. Enter the **Login Name**. The remaining fields can be left as default.

The screenshot shows the Avaya Aura System Manager 7.1 interface. The top navigation bar includes 'Home' and 'User Management'. The left sidebar lists various management options, with 'Manage Users' selected. The main content area is titled 'New User Profile' and features a 'Commit & Continue' button. Below the title are four tabs: 'Identity' (selected), 'Communication Profile', 'Membership', and 'Contacts'. The 'Identity' tab contains a 'User Provisioning Rule' dropdown and an 'Identity' section with the following fields:

- * Last Name: 3418
- Last Name (Latin Translation): 3418
- * First Name: Ascom
- First Name (Latin Translation): Ascom
- Middle Name: (empty)
- Description: (empty text area)
- * Login Name: 3418@bvwdev.com
- Email Address: (empty)
- User Type: Basic

Under the **Communication Profile** tab enter **Communication Profile Password** and **Confirm Password**, note that his password is required when configuring the DECT handset in **Section 7.4**. Click on **New** to add a new **Communication Address**.



Enter the extension number and the domain for the **Fully Qualified Address** and click on **Add** once finished. Ensure **Session Manager Profile** is checked and enter the **Primary Session Manager** details, enter the **Origination Application Sequence** and the **Termination Application Sequence** and the **Home Location** as highlighted below.

Communication Address ▾

New Edit Delete

Type	Handle	Domain
No Records found		

Type: Avaya SIP ▾

* Fully Qualified Address: 3418 @ bvwdev.com ▾

Add Cancel

Session Manager Profile ▾

SIP Registration

* Primary Session Manager

Secondary Session Manager

Survivability Server

Max. Simultaneous Devices

Block New Registration When Maximum Registrations Active?

Primary	Secondary	Maximum
23	0	23

Application Sequences

Origination Sequence

Termination Sequence

Emergency Calling Application Sequences

Emergency Calling Origination Sequence

Emergency Calling Termination Sequence

Call Routing Settings

* Home Location

Ensure that **CM Endpoint Profile** is selected for the **System** and choose the **9640SIP_DEFAULT_CM_7_1** as the **Template**. Click on **Endpoint Editor** to configure the buttons and features for that handset on Communication Manager.

CM Endpoint Profile ▼

* System ▼

* Profile Type ▼

Use Existing Endpoints

* Extension [Display Extension Ranges](#)

* Template ▼

Set Type

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.

Edit Endpoint

[\[Save As Template\]](#)

System	<input type="text" value="interopcm"/>	Extension	<input type="text" value="3418"/>
Template	<input type="text" value="9640SIP_DEFAULT_CM_7_1"/> ▼	Set Type	<input type="text" value="9640SIP"/> 
Port	<input type="text" value="IP"/>	Security Code	<input type="text"/>
Name	<input type="text" value="3418,Ascom"/>		

General Options (G) *	Feature Options (F)	Site Data (S)	Abbreviated Call Dialing (A)
Enhanced Call Fwd (E)	Button Assignment (B)	Group Membership (M)	

* Class of Restriction (COR)	<input type="text" value="1"/>	* Class Of Service (COS)	<input type="text" value="1"/>
* Emergency Location Ext	<input type="text" value="3418"/>	* Message Lamp Ext.	<input type="text" value="3418"/>
* Tenant Number	<input type="text" value="1"/>	Type of 3PCC Enabled	<input type="text" value="None"/> ▼
* SIP Trunk	<input type="text" value="aar"/>	Coverage Path 1	<input type="text" value="4"/>
		Coverage Path 2	<input type="text"/>

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**.

General Options (G) *		Feature Options (F)		Site Data (S)		Abbreviated Call Dialing (A)	
Enhanced Call Fwd (E)		Button Assignment (B)		Group Membership (M)			
Active Station Ringing	single	Auto Answer	none				
MWI Served User Type	sip-adjunct	Coverage After Forwarding					
Per Station CPN - Send Calling Number	None	Display Language	english				
IP Phone Group ID		Hunt-to Station					
Remote Soft Phone Emergency Calls	as-on-local	Loss Group	19				
LWC Reception	spe	Survivable COR	internal				
AUDIX Name	None	Time of Day Lock Table	None				
Speakerphone	2-way	Voice Mail Number	3333				
Short/Prefixed Registration Allowed	default	Music Source					
EC500 State	enabled						

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

The screenshot shows a configuration window with several tabs. The top row contains 'General Options (G) *', 'Feature Options (F)', 'Site Data (S)', and 'Abbreviated Call Dialing (A)'. The second row contains 'Enhanced Call Fwd (E)', 'Button Assignment (B)', and 'Group Membership (M)'. The 'Button Assignment (B)' tab is active. Below this, there are three sub-tabs: 'Main Buttons', 'Feature Buttons', and 'Button Modules'. The 'Main Buttons' sub-tab is selected. It displays a table with four rows and four columns. The first column contains numbers 1 through 4. The second column contains dropdown menus with 'call-appr' for rows 1-3 and 'None' for row 4. The other three columns are empty text input fields.

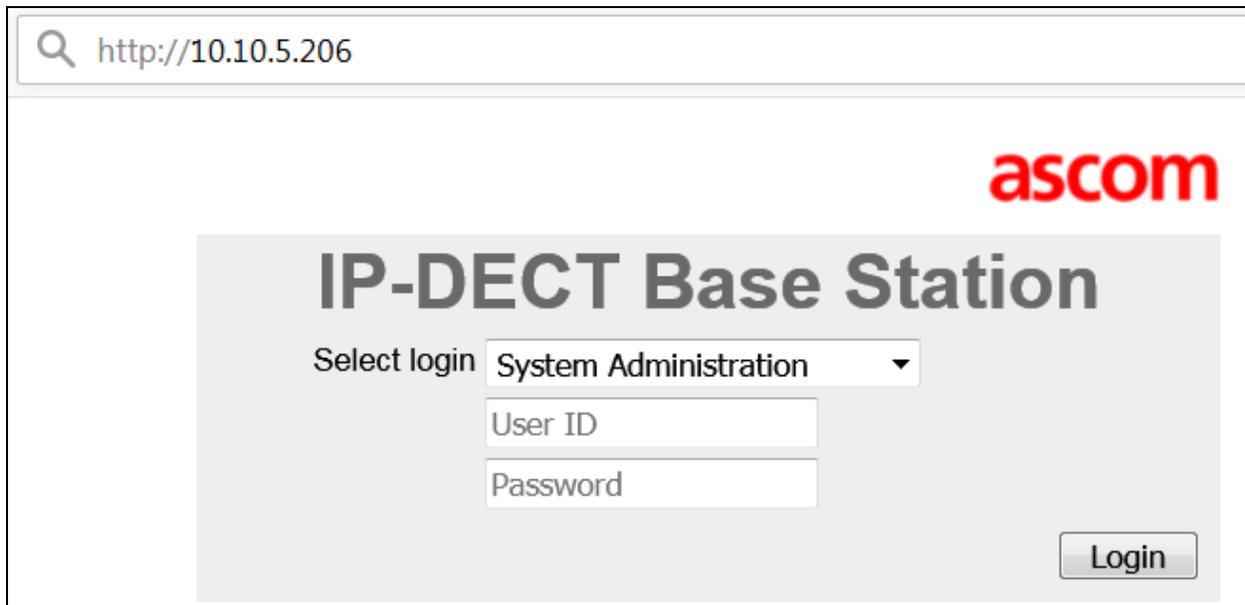
	Main Buttons	Feature Buttons	Button Modules	
1	call-appr			
2	call-appr			
3	call-appr			
4	None			

Once the **CM Endpoint Profile** is completed correctly, click on **Commit** (not shown) to save the new user.

7. Configure Ascom DECT Base Station and Handsets

The configuration of the DECT base station and the DECT handsets are both achieved through an http session to the web interface of the DECT base station acting as Master. Open a web session to the IP address of the DECT base station and select **System administration** as shown below.

Then enter the proper credentials for **User ID** and **Password** and click on **Login** to log in.



The screenshot shows a web browser window with the address bar containing "http://10.10.5.206". The main content area features the "ascom" logo in red in the top right corner. Below the logo, the title "IP-DECT Base Station" is displayed in large, bold, grey text. Underneath the title, there is a login form with the following elements: a "Select login" label followed by a dropdown menu currently set to "System Administration"; a "User ID" text input field; a "Password" text input field; and a "Login" button located in the bottom right corner of the form area.

7.1. 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 **IP4** tab. Enter the **IP Address**, **Network Mask**, **Default Gateway** and **DNS Server** information of the DECT Base Station and click on **OK**. Ensure also that DHCP mode is set to disabled under the **DHCP** tab (not shown).

The screenshot displays the 'IP-DECT Base Station' configuration window. On the left is a navigation menu with categories: Configuration, LAN, IP4, IP6, LDAP, DECT, VoIP, Unite, Services, Administration, Users, Device Overview, and DECT Sync. The 'IP4' tab is selected. The main area shows 'Active Settings' for IP Address (10.10.5.206), Network Mask (255.255.255.0), Default Gateway (10.10.5.1), and DNS Server (10.10.98.60). There is also an 'Alt. DNS Server' field and a 'Check ARP' checkbox. Below this is a 'Static IP Routes' section with columns for Network Destination, Network Mask, and Gateway, each with an empty input field. At the bottom are 'OK' and 'Cancel' buttons.

Please refer to Ascom's documentation listed in **Section 10** of these Application Notes for further information about DECT configuration. The following sections cover specific settings concerning SIP and the connection to Session Manager.

7.2. 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** (this is used in **Section 7.4** to subscribe the DECT handset to the base station). Note that the password seen here is not the password for the SIP users on Session Manager. Select the appropriate country for **Tones**, note for these compliance tests **US** was selected. Select **1920-1930 MHz (North America)** for the **Frequency** and ensure that **Local R-Key Handling** box is checked. For **Coder** select **G722.2/G711u** from the drop-down box; note that this will be the same codec used in **Section 5.4**. Click on **OK** to save the changes.

The screenshot shows the 'IP-DECT Base Station' configuration window, specifically the 'System' tab. The left sidebar contains a 'Configuration' menu with options: General, LAN, IP4, IP6, LDAP, DECT (selected), VoIP, Unite, Services, Administration, Users, Device Overview, DECT Sync, Traffic, Gateway, Backup, Update, Diagnostics, and Reset. The main area displays various configuration fields:

- System Name: DECT3
- Password: [Redacted]
- Confirm Password: [Redacted]
- Subscriptions: With System AC (dropdown)
- Authentication Code: 9999
- Tones: US (dropdown)
- Default Language: English (dropdown)
- Frequency: 1920-1930 MHz (North America) (dropdown)
- Enabled Carriers: 23, 24, 25, 26, 27 (all checked)
- Local R-Key Handling: [checked]
- No Transfer on Hangup: [checked]
- No On-Hold Display: [unchecked]
- Display Original Called: [unchecked]
- Early Encryption: [unchecked]
- RFP Location: [unchecked]
- Disable ICE: [checked]
- Coder: G722.2/G711u (dropdown)
- Frame (ms): 20
- Exclusive: [unchecked]
- SC: [unchecked]
- Secure RTP Key Exchange: No encryption (dropdown)

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

7.3. 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 (preferred) 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** boxes were checked 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**.

The screenshot shows the configuration page for an IP-DECT Base Station, specifically the 'Master' tab. The left sidebar contains a navigation menu with categories like 'Configuration', 'Administration', and 'Services'. The 'DECT' option is selected. The main content area is divided into sections: 'Mirror' (Mode: Mirror, Mirror Master: 10.10.5.205, Mirror Status: Active, Connected to 10.10.5.205), 'Multi-Master' (Master ID: 0, Enable PARI Function: checked, Region Code: empty), and 'IP-PBX' (Protocol: SIP/TCP, Proxy: 10.10.1.12, Alt. Proxy: empty, Domain: empty, Max. Internal Number Length: 4, International CPN Prefix: empty, Registration with system password: unchecked, Enbloc Dialing: checked, Enable Enbloc Send-Key: unchecked, Send Inband DTMF: unchecked, Allow DTMF Through RTP: checked). Red boxes highlight the Protocol, Proxy, Enbloc Dialing, and Allow DTMF Through RTP settings.

Configuration	System	Suppl. Serv.	Master	Crypto Master
General				
LAN				
IP4				
IP6				
LDAP				
DECT				
VoIP				
Unite				
Services				
Administration				
Users				
Device Overview				
DECT Sync				
Traffic				
Gateway				
Backup				
Update				
Diagnostics				
Reset				

IP-DECT Base Station

Mode: Mirror

Mirror Master: 10.10.5.205

Mirror Status: Active
Connected to 10.10.5.205

Multi-Master

Master ID: 0

Enable PARI Function:

Region Code:

IP-PBX

Protocol: SIP/TCP

Proxy: 10.10.1.12

Alt. Proxy:

Alt. Proxy:

Alt. Proxy:

Domain:

Max. Internal Number Length: 4

International CPN Prefix:

Registration with system password:

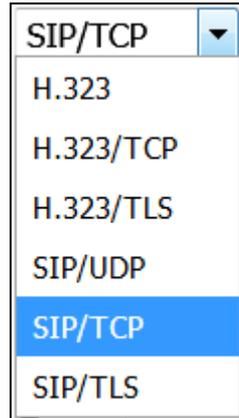
Enbloc Dialing:

Enable Enbloc Send-Key:

Send Inband DTMF:

Allow DTMF Through RTP:

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



Scroll down and click on **OK** (not shown) to save the above new configuration.

Click on the **Suppl. Serv.** tab and ensure that **Enable Supplementary Services** box 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 **3333**.

IP-DECT Base Station

Configuration	System	Suppl. Serv.	Master	Crypto Master	Mobility Master	Radio	Rad
General	<input checked="" type="checkbox"/> Enable Supplementary Services						
LAN							
IP4							
IP6							
LDAP							
DECT							
VoIP							
Unite							
Services							
Administration							
Users							
Device Overview							
DECT Sync							
Traffic							
Gateway							
Backup							
Update							
Diagnostics							
Reset							
		Activate	Deactivate				Disable
	Call Forwarding Unconditional	*21*\$#	#21#				<input type="checkbox"/>
	Call Forwarding Busy	*67*\$#	#67#				<input type="checkbox"/>
	Call Forwarding No Reply	*61*\$#	#61#				<input type="checkbox"/>
	Do Not Disturb	*42#	#42#				<input type="checkbox"/>
	Call Waiting	*43#	#43#				<input type="checkbox"/>
	Call Completion	.	.				<input checked="" type="checkbox"/>
	Call Park	.	.				<input checked="" type="checkbox"/>
	Interception	.	.				<input checked="" type="checkbox"/>
	Call Service URI	.					<input checked="" type="checkbox"/>
	Call Service URI (Argument)	.					<input checked="" type="checkbox"/>
	Soft key	.					<input checked="" type="checkbox"/>
	Logout User	#11*\$#					<input type="checkbox"/>
	Clear Local Setting	*00#					<input type="checkbox"/>
	MWI Mode	User dependent interrogate number					<input type="checkbox"/>
	MWI Notify Number	3333					<input type="checkbox"/>
	Local Clear of MWI	.					<input type="checkbox"/>
	External Idle Display						<input checked="" type="checkbox"/>
	<input type="button" value="OK"/> <input type="button" value="Cancel"/>						

7.4. Adding DECT Users

Click on **Users** in the left column and under the **Users** tab seen on right column, click **new** to add a new DECT user.

The screenshot displays the 'IP-DECT Base Station' configuration interface. On the left, a 'Configuration' sidebar lists various settings: General, LAN, IP4, IP6, LDAP, DECT, VoIP, Unite, Services, Administration, and Users. The 'Users' tab is selected. The main content area shows a list of users with the following details: 'PARK' (name), a redacted phone number, 'PARK' (extension), '3rd' (line), 'pty' (party), a redacted extension, and 'Master Id' (0). Below the list, there is an empty input field, a 'show' button, a 'new' button (highlighted with a red box), an 'import' button, and an 'export' button.

Enter the appropriate information for the new DECT user and once all the information has been correctly filled in click on the **OK** button. The Handset is then registered with the DECT system, according to Ascom's documentation. The Password entered should be the same as that configured in **Section 6.4**.

IP-DECT Base Station

Configuration

- General
- LAN
- IP4
- IP6
- LDAP
- DECT
- VoIP
- Unite
- Services
- Administration**
 - Users**
 - Device Overview
 - DECT Sync
 - Traffic
 - Gateway
 - Backup
 - Update
 - Diagnostics
 - Reset

Users | Anonymous

Edit User - Mozilla Firefox

10.10.5.206/GW-DECT/mod_cmd_login.xml?cmd=sho

User type

User

User Administrator

Long Name: d63 3418

Display Name: d63 3418

Name: 3418

Number: 3418

Auth. Name: (SIP only)

Password: ●●●●●●●●

Confirm Password: ●●●●●●●●

IPEI / IPDI: 110550389538

Idle Display: d63 3418

Auth. Code:

Feature Status

Call Waiting On

OK Apply Delete Unsubs. Cancel

At this point the handset is **Subscribed** to the DECT system; please refer to the DECT Handset user guide (see **Section 10**) 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 and the **Authentication Code** configured in **Section 7.2** is required for the handset to subscribe to the DECT system.

The screenshot shows the 'IP-DECT Base Station' configuration interface. The 'Users' tab is selected. On the left, there is a 'General' sidebar with options like LAN, IP4, IP6, LDAP, DECT, VoIP, Unite, Services, Administration, Users, Device Overview, DECT Sync, and Traffic. The main area shows 'User Administrators' (0) and a table of 'Users'. A 'PARK' field is highlighted in a red box. The table lists users with columns for Long Name, Name, No, Fty, Display, IPEI / IPDI, AC, Prod, SW, EE, and Registration.

Long Name	Name	No	Fty	Display	IPEI / IPDI	AC	Prod	SW	EE	Registration
d41 9923	9923	9923	+	d41 9923	085870140743					Subscribed
d62 9922	9922	9922	+	d62 9922	036470363716					Subscribed
d63 3417	3417	3417	+	d63 3417	110550389613	d63-Talker	2.2.2			Subscribed
d63 3418	3418	3418	+	d63 3418	110550389538	d63-Talker	2.2.2			Subscribed
d81 11128	11128	11128	+	d81 11128	002020909367					Subscribed
d81 3416	3416	3416	+	d81 3416	002020772294	d81-Protector	4.6.2			Subscribed
d81 3419	3419	3419	+	d81 3419	002020909369	d81-Messenger	4.6.2			Subscribed
d81 9916	9916	9916	+	d81 9916	002020909371					Subscribed

Users: 8, Registrations: 0

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

The screenshot shows the same 'IP-DECT Base Station' configuration page, but with a dialog box open over the user table. The dialog box is titled 'Mozilla Firefox' and contains fields for CFU, CFB, and CFNR, and checkboxes for 'Do not Disturb Int.', 'Do not Disturb Ext.', and 'Call Waiting'. The 'Call Waiting' checkbox is checked. The dialog box has 'OK' and 'Cancel' buttons. The user table in the background shows the same data as the previous screenshot, but with a red box around the '+' icon in the 'Fty' column for the user 'd63 3418'. The 'Registration' column for this user now shows '10.10.1.12'. The status at the bottom indicates 'Users: 8, Registrations: 1'.

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 7.3**.

As a final step confirm that DECT handsets have registered successfully with the Avaya Session Manager, note the IP addresses under **Registration**.

IP-DECT Base Station

Configuration

Users Anonymous

General

LAN

IP4

IP6

LDAP

DECT

VoIP

Unite

Services

Administration

Users

Device Overview

DECT Sync

Traffic

Gateway

PARK [REDACTED]

PARK 3rd pty [REDACTED]

Master Id 0

[show](#)
[new](#)
[import](#)
[export](#)

User Administrators

[Long Name](#) [Name](#)

User Administrators: 0

Users

Long Name	Name	No	Fty	Display	IPEI / IPDI	AC	Prod	SW	EE	Registration
d81 3416	3416	3416	+	d81 3416	002020772294		d81-Protector	4.6.2		10.10.1.12
d63 3418	3418	3418	+	d63 3418	110550389538		d63-Talker	2.2.2		10.10.1.12
d81 3419	3419	3419	+	d81 3419	002020909369		d81-Messenger	4.6.2		10.10.1.12
d63 3417	3417	3417	+	d63 3417	110550389613		d63-Talker	2.2.2		10.10.1.12
d62 9922	9922	9922	+	d62 9922	036470363716					Subscribed
d41 9923	9923	9923	+	d41 9923	085870140743					Subscribed
d81 9916	9916	9916	+	d81 9916	002020909371					Subscribed
d81 11128	11128	11128	+	d81 11128	002020909367					Subscribed

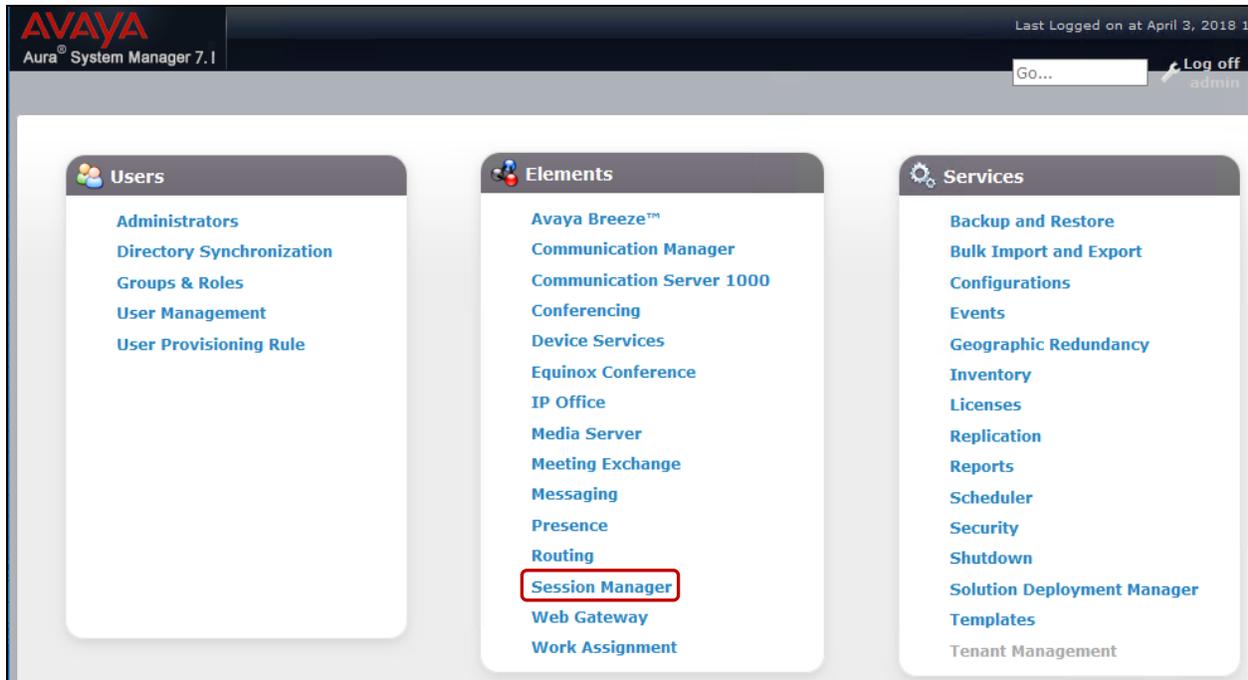
Users: 8, Registrations: 4

8. Verification Steps

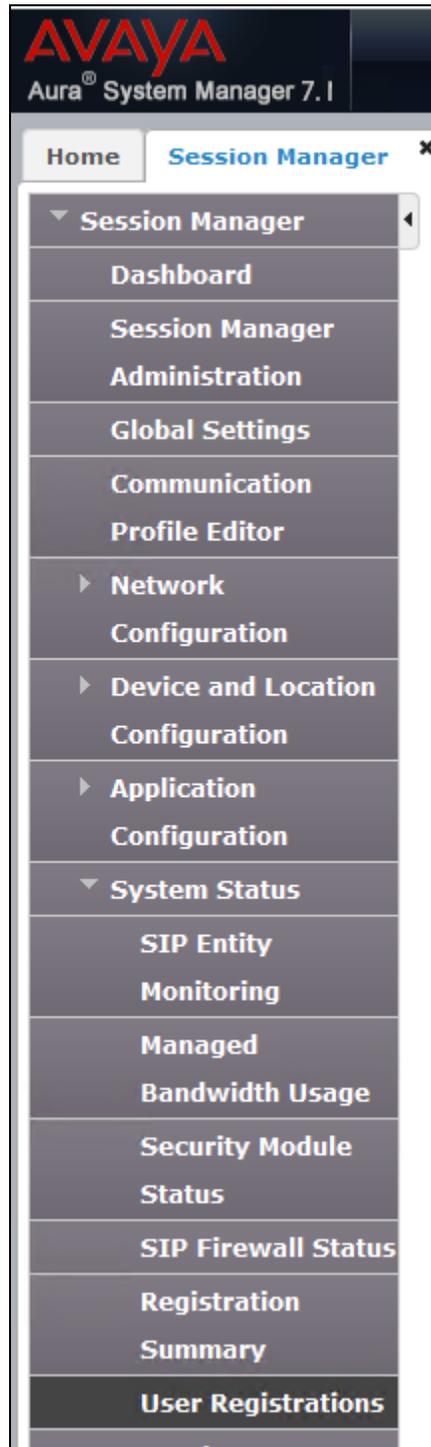
The following steps can be taken to ensure that connections between Ascom DECT handsets and Session Manager and Communication Manager are up.

8.1. Session Manager Registration

Log into System Manager as done previously in **Section 6**, 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.

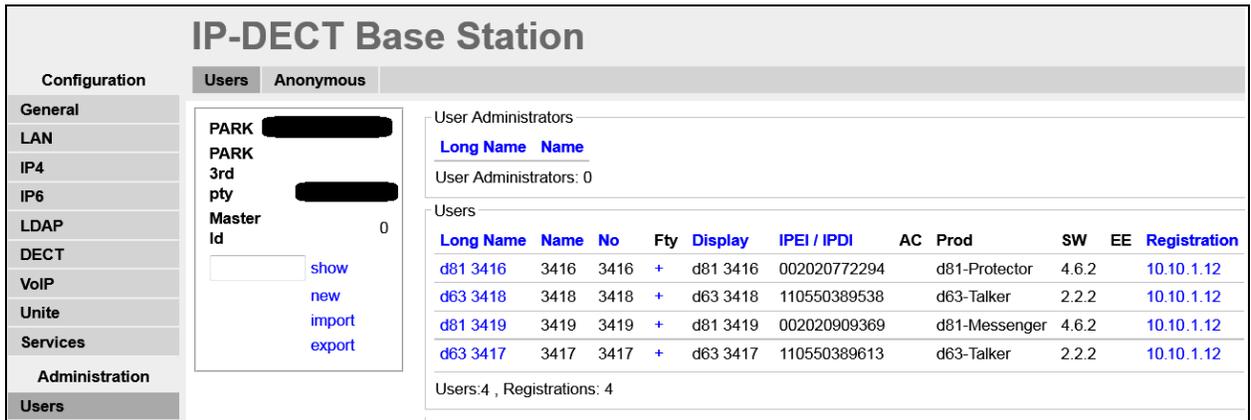


The Ascom DECT user **3418** should show as being registered as seen below.

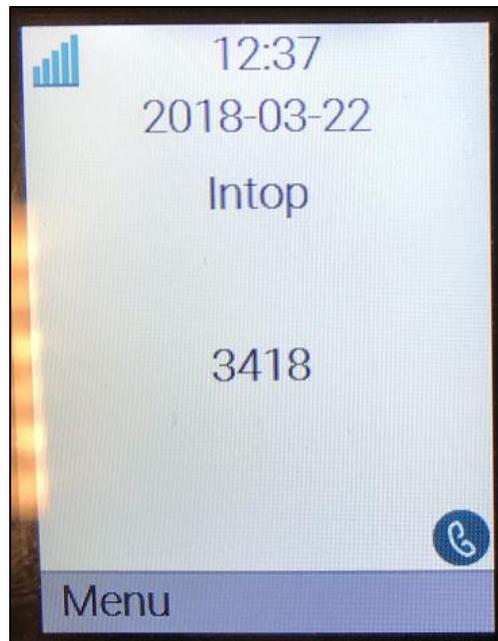


8.2. Ascom DECT Registration

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 **3416** to **3419** are registered correctly.



The Ascom DECT handset connection to Session Manager can also be verified by an absence of an error message on the handset display as shown in the following illustration, (note this is an example from compliance testing).



9. Conclusion

These Application Notes describe the configuration steps required for Ascom's DECT IP Base Station and DECT Handsets to successfully interoperate with Avaya Aura® Communication Manager and Avaya Aura® Session Manager by registering the Ascom Handsets with Session Manager as third-party SIP phones. Please refer to **Section 2.2** for test results and observations.

10. Additional References

This section references the product documentation relevant to these Application Notes.

Product documentation for Avaya products may be found at <http://support.avaya.com>.

1. *Deploying Avaya Aura® Communication Manager*, Release 7.1.2, Issue December 2017
2. *Avaya Aura® Communication Manager Feature Description and Implementation*, Release 7.1.2, Issue 4 January 2018
3. *Deploying Avaya Aura® Session Manager*, Release 7.1.2, Issue 4 December 2017
4. *Administering Avaya Aura® Session Manager*, Release 7.1.2, Issue 4 March 2018
5. *Deploying Avaya Aura® System Manager*, Release 7.1.2, Issue 6 March 2018
6. *Administering Avaya Aura® System Manager for Release 7.1.2*, Release 7.1.2, Issue 11 March 2018
7. *Deploying Avaya Aura® Messaging using VMware® in the Virtualized Environment*, Release 7.0.0, Issue 2 January 2017
8. *Administering Avaya Aura® Messaging*, Release 7.0.0, Issue 3 January 2018

Documentation for Ascom Products can be obtained from an Ascom supplier or may be accessed at <https://www.ascom-ws.com/AscomPartnerWeb/Templates/WebLogin.aspx> (login account for the Ascom Partner Extranet required).

Appendix

Signaling Group

```
display signaling-group 1                               Page 1 of 2
                SIGNALING GROUP

Group Number: 1                Group Type: sip
IMS Enabled? n                Transport Method: tls
    Q-SIP? n
    IP Video? n                Enforce SIPS URI for SRTP? n
Peer Detection Enabled? n Peer Server: SM
Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? y
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? n
Alert Incoming SIP Crisis Calls? n
    Near-end Node Name: procr                Far-end Node Name: interopASM
    Near-end Listen Port: 5061                Far-end Listen Port: 5061
                Far-end Network Region: 1

Far-end Domain: bwvdev.com

Incoming Dialog Loopbacks: eliminate                Bypass If IP Threshold Exceeded? n
                RFC 3389 Comfort Noise? n
    DTMF over IP: rtp-payload                Direct IP-IP Audio Connections? y
Session Establishment Timer(min): 3                IP Audio Hairpinning? n
    Enable Layer 3 Test? y                Initial IP-IP Direct Media? n
H.323 Station Outgoing Direct Media? n                Alternate Route Timer(sec): 6
```

Trunk Group

```
display trunk-group 1                                     Page 1 of 22
                                     TRUNK GROUP
Group Number: 1                Group Type: sip          CDR Reports: y
  Group Name: Private Trunk      COR: 1            TN: 1          TAC: #01
  Direction: two-way            Outgoing Display? n
Dial Access? n                Night Service:
Queue Length: 0
Service Type: tie              Auth Code? n
                                     Member Assignment Method: auto
                                     Signaling Group: 1
                                     Number of Members: 14
```

```
display trunk-group 1                                     Page 2 of 22
  Group Type: sip
TRUNK PARAMETERS
  Unicode Name: auto
                                     Redirect On OPTIM Failure: 5000
  SCCAN? n                      Digital Loss Group: 18
  Preferred Minimum Session Refresh Interval(sec): 90
Disconnect Supervision - In? y Out? y
  XOIP Treatment: auto          Delay Call Setup When Accessed Via IGAR? n
Caller ID for Service Link Call to H.323 1xC: station-extension
```

```
display trunk-group 1                                     Page 3 of 22
TRUNK FEATURES
  ACA Assignment? n              Measured: none
                                     Maintenance Tests? y
  Suppress # Outpulsing? n       Numbering Format: private
                                     UUI Treatment: shared
                                     Maximum Size of UUI Contents: 128
                                     Replace Restricted Numbers? y
                                     Replace Unavailable Numbers? y
                                     Hold/Unhold Notifications? y
  Send UCID? y                  Modify Tandem Calling Number: no
  Show ANSWERED BY on Display? y
```

PROTOCOL VARIATIONS

Mark Users as Phone? n
Prepend '+' to Calling/Alerting/Diverting/Connected Number? n
Send Transferring Party Information? n
Network Call Redirection? y
Build Refer-To URI of REFER From Contact For NCR? n
Send Diversion Header? n
Support Request History? y
Telephone Event Payload Type:

Convert 180 to 183 for Early Media? n
Always Use re-INVITE for Display Updates? n
Identity for Calling Party Display: P-Asserted-Identity
Block Sending Calling Party Location in INVITE? n
Accept Redirect to Blank User Destination? n
Enable Q-SIP? n

Interworking of ISDN Clearing with In-Band Tones: keep-channel-active
Request URI Contents: may-have-extra-digits

©2018 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.