Avaya Solution & Interoperability Test Lab

Application Notes for configuring Ascom IP-DECT with Avaya Aura® Communication Manager and Avaya Aura® Session Manager – Issue 1.0

Abstract

These Application Notes describe the configuration steps for provisioning Ascom IP-DECT R11 (v11.7.2) to interoperate with Avaya Aura® Communication Manager R10.1 and Avaya Aura® Session Manager R10.1.

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 IP-DECT R11 to interoperate with Avaya Aura® Communication Manager R10.1 and Avaya Aura® Session Manager R10.1. Ascom IP -DECT consists of DECT handsets and IP-DECT Access Points (IPBS3), which are also referred to as Base Stations. The DECT handsets are configured to register with Session Manager using SIP signalling and are also subscribed to the IPBS3 Access Points using DECT signalling. Each handset is configured as a SIP user on Communication Manager as Avaya 9620 SIP endpoint. The 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.

- IP (Internet Protocol) – Universal standard for inter-networking that maximizes scalability and interoperability.
- DECT (Digital Enhanced Cordless Telecommunications) - Secure radio communication standard that delivers superior voice quality over reserved radio frequency bands.
- IPBS3 (IP Base Station 3) – This is also referred to as Ascom IP-DECT Access Point or Base Station.

2. General Test Approach and Test Results

The interoperability compliance testing evaluates the ability of DECT handsets to make and receive calls to and from Avaya H.323, SIP and Digital deskphones. Avaya Messaging (Messaging) was used to allow users to leave voicemail messages and to demonstrate Message Waiting Indication working on the DECT 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 6.2** 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's formal testing and Declaration of Conformity is provided only on the headsets/handsets 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/handsets 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.

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.

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, Avaya Digital, Ascom DECT endpoints and PSTN endpoints.

- Basic Calls
- Session Refresh Timer
- Long Duration Call
- Hold, Retrieve and Brokering (Toggle)
- Feature Access Code dialing
- 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

- Do Not Disturb
- Calling Line Name/Identification
- Codec Support (G.711A, G.729A, G.722.2 (AMR-WB) tested)
- DTMF Support
- Voice Mail, Message Waiting Indication
- Serviceability

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

Note: Compliance testing does not include redundancy testing as standard. Where some LAN failures were simulated, and the results observed, there were no redundancy or failover tests performed.

2.2. Test Results

Tests were performed to verify interoperability between Ascom DECT handsets and Communication Manager deskphones. The tests were all functional in nature and performance testing or redundancy testing were not included.

The following observations/limitations were noted during testing.

1. All compliance testing was done using TCP (preferred) and UDP as the transport protocol.
2. Negotiation of G.722.2 (AMR-WB) 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 the Ascom IP-DECT Base Station, the corresponding TCP entity links were setup as type “Endpoint Concentrator”.
4. A call is placed from an Ascom DECT handset to an Avaya phone that has CFNA to voicemail setup and the Ascom phone hangs up once the caller hears the call went to voicemail. When the DECT user then looks at the ‘Call List’, the list shows the last call was made to the Avaya phone, but the number saved was the voicemail number. So, when the DECT user then wants to call back to that phone from the call list, it rings the voicemail number.
5. 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.
6. 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.
7. As per current design, DECT handsets cannot initiate a three-party conference however are able to join a conference.
8. DECT handsets do not have a redial button. User needs to use “Call List” and redial the numbers.
9. As per current design, DECT handsets do not support Multi-Device Access (MDA).

10. 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.
11. 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

Support from Avaya is available by visiting the website http://support.avaya.com and a list of product documentation can be found in **Section 10** of these Application Notes. 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 IP-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, SIP and Digital deskphones on Communication Manager. During compliance testing, the DECT base stations were configured by accessing them via a web interface on a Windows PC.

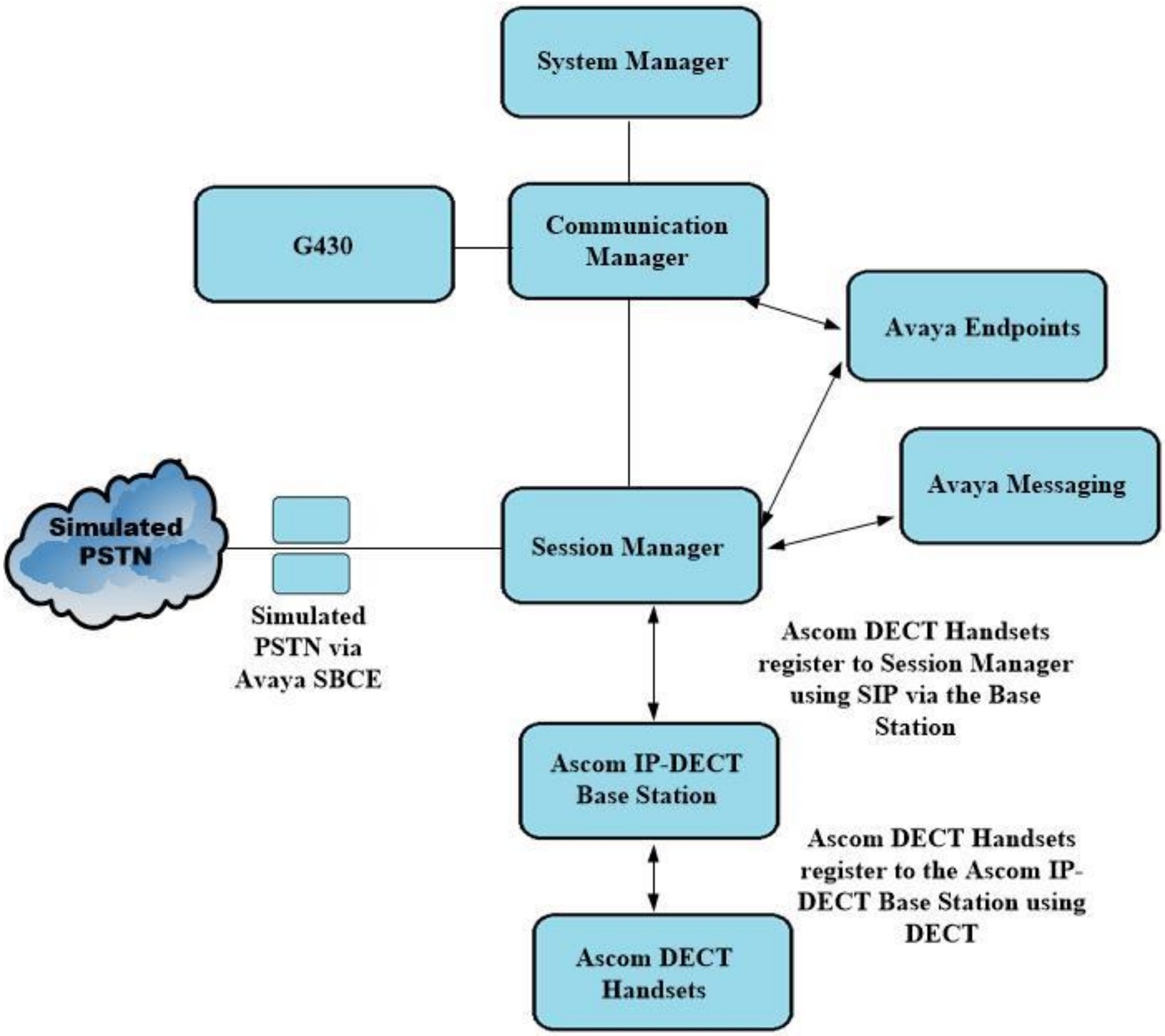


Figure 1: Network Solution of Ascom IP-DECT with Avaya Aura® Communication Manager and Avaya Aura® Session Manager

4. Equipment and Software Validated

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

Avaya Equipment/Software	Release/Version
Avaya Aura® System Manager running on a virtual server	10.1.0.0 Build No. – 10.1.0.0.537353 SW Update Revision No: 10.1.0.0.0614254
Avaya Aura® Session Manager running on a virtual server	10.1 Build No. – 10.1.0.0.1010019
Avaya Aura® Communication Manager running on a virtual server	10.1 Update ID 01.0.974.0-27293
Avaya Messaging running on MS Windows Server 2019	10.8.20.1502
Avaya Session Border Controller for Enterprise	8.1.1.0-26-19214
Avaya G430 Media Gateway	41.16.0/1
Avaya J179 H.323 Deskphone	6.8304
Avaya J159 SIP Deskphone	4.0.7.1.5
Avaya 9408 Digital Phone	2.00
Ascom Equipment/Software	**Release/Version**
Ascom IP-DECT Base Station	IPBS3 v11.7.2
Ascom IP-DECT Handsets D63-Talker	2.12.9

5. Configure Avaya Aura® Communication Manager

It is assumed that a fully functioning Communication Manager is in place with the necessary licensing with SIP trunks in place to Session Manager. For further information on the configuration of Communication Manager please see **Section 10** of these Application Notes.

Note: A printout of the Signalling and Trunk group that were used during compliance testing can be found in the **Appendix** of these Application Notes.

The following sections go through the following.

- System Parameters
- Dial Plan Analysis
- Feature Access Codes
- Network Region
- IP Codec
- Coverage Path and Hunt Group for Voicemail

5.1. Configure System Parameters

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: V20                             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
```

Ascom have asked that the SIP Endpoint Managed Transfer parameter be set to n as an incorrectly set parameter may interfere with attended transfers.

Type **change system-parameters features** and on **Page 19** ensure that the **SIP Endpoint Managed Transfer** parameter is set to **n**.

```
change system-parameters features                             Page  19 of  19
                        FEATURE-RELATED SYSTEM PARAMETERS
IP PARAMETERS
           Direct IP-IP Audio Connections? y         IP Audio Hairpinning? n
                  Synchronization over IP? n Allow SIP-H323 Video in SDES? n
    Initial INVITE with SDP for secure calls? y
               SIP Endpoint Managed Transfer? n

  Expand ISDN Numbers to International for 1XCES? n

CALL PICKUP
  Maximum Number of Digits for Directed Group Call Pickup: 4
                Call Pickup on Intercom Calls? y     Call Pickup Alerting? y
  Temporary Bridged Appearance on Call Pickup? y     Directed Call Pickup? y
                   Extended Group Call Pickup: simple
                Enhanced Call Pickup Alerting? n

   Call Pickup for Call to Coverage Answer Group? y
                        Display Information With Bridged Call? y
  Keep Bridged Information on Multiline Displays During Calls? y
                  PIN Checking for Private Calls? n
```

5.2. 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 **21**. Feature Access Codes (**fac**) use digits **8** and **9** and use characters * or #.

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

    Dialed   Total  Call     Dialed   Total  Call     Dialed   Total  Call
    String   Length Type     String   Length Type     String   Length Type
   1             4  udp
   2             4  udp
   3             4  ext
   4             4  ext
   5             4  udp
   666           4  ext
   8             1  fac
   9             1  fac
   *             3  fac
   *8            4  dac
   #             3  fac
```

Under **aar analysis**, **31** was set to go out over the SIP trunk 11 on **Route Pattern 11**, as shown below. This is used for SIP phones to allow the connection between Session Manager and Communication Manager and would have been setup as part of the initial installation and configuration of the Aura® platform. The configuration of the Signaling and Trunk Group 11 is shown in the **Appendix**.

```
change aar analysis 3                                          Page   1 of   2
                             AAR DIGIT ANALYSIS TABLE
                                   Location: all            Percent Full: 1

          Dialed            Total      Route      Call    Node   ANI
          String           Min  Max   Pattern     Type    Num    Reqd
    31                     4    4      11         lev0           n
    4                      7    7      999        aar            n
    5                      7    7      999        aar            n
    666                    4    4      66         aar            n
    7                      7    7      999        aar            n
    8                      7    7      999        aar            n
    9                      7    7      999        aar            n
                                                                 n
                                                                 n
```

5.3. 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 5.2**. Some of the access codes configured during compliance testing are shown below.

```
change feature-access-codes                                    Page   1 of  12
                               FEATURE ACCESS CODE (FAC)
         Abbreviated Dialing List1 Access Code: *11
         Abbreviated Dialing List2 Access Code: *12
         Abbreviated Dialing List3 Access Code: *13
Abbreviated Dial - Prgm Group List Access Code: *10
                      Announcement Access Code: *27
                       Answer Back Access Code: #02
                         Attendant Access Code:
      Auto Alternate Routing (AAR) Access Code: 8
    Auto Route Selection (ARS) - Access Code 1: 9     Access Code 2:
                 Automatic Callback Activation: *05    Deactivation: #05
Call Forwarding Activation Busy/DA: *03    All: *04    Deactivation: #04
   Call Forwarding Enhanced Status: *73    Act: *74    Deactivation: #74
                         Call Park Access Code: *02
                       Call Pickup Access Code: *09
CAS Remote Hold/Answer Hold-Unhold Access Code:
                  CDR Account Code Access Code: *14
                        Change COR Access Code:
                   Change Coverage Access Code:
            Conditional Call Extend Activation:        Deactivation:
                   Contact Closure   Open Code:          Close Code:
```

5.4. Configure Network Region

Use **change ip-network-region x** (where x is the network region to be configured) to assign an appropriate domain name to be used by Communication Manager, in the example below **greaneyp.sil6.avaya.com** is used. Note that this domain is also configured in **Section 6.1.1**.

```
change ip-network-region 1                                    Page   1 of  20
                               IP NETWORK REGION
  Region: 1       NR Group: 1
Location:         Authoritative Domain: greaneyp.sil6.avaya.com
    Name: PGDefault             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      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                         RSVP Enabled? n
  H.323 Link Bounce Recovery? y
 Idle Traffic Interval (sec): 20
   Keep-Alive Interval (sec): 5
            Keep-Alive Count: 5
```

5.5. Configure IP-Codec

Use the **change ip-codec-set x** (where x is the ip-codec set used) command to designate a codec set compatible with the DECT handsets. During compliance testing the codecs **G.711A**, **G.729A** and **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: OPUS-WB20K                    1        20
 2: G.722-64K                     2        20
 3: G.722.2            n          1        20
 4: G.711A             n          2        20
 5: G.711MU            n          2        20
 6: G.729              n          2        20
 7:

     Media Encryption                   Encrypted SRTCP: best-effort
 1: 1-srtp-aescm128-hmac80
 2: none
 3:
 4:
 5:
```

5.6. Configuration of Coverage Path and Hunt Group for Voicemail

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

Don't' Answer is set to **y:**	The coverage path will be used in the event the phone set is not answered.
Number of Rings is set to **3:**	The coverage path will be used after 3 rings.
Point 1 is set to **h67:**	Hunt Group 67 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: 3
                All?             n               n
 DND/SAC/Goto Cover?             y               y
   Holiday Coverage?             n               n


COVERAGE POINTS
    Terminate to Coverage Pts. with Bridged Appearances? n
Point1: h67                Rng: 3  Point2:
Point3:                            Point4:
Point5:                            Point6:
```

The hunt group used for compliance testing is shown below. Note that on **Page 1** the **Group Extension** is **6667**, which is used to dial for messaging and **Group Type** is set to **ucd-mia**.

```
display hunt-group 67                                       Page   1 of  60
                                  HUNT GROUP

            Group Number: 67                               ACD? n
              Group Name: Messaging                      Queue? n
         Group Extension: 6667                          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:






SIP URI::
```

On **Page 2**, **Message Center** is set to **sip-adjunct**. The **Voice Mail Number** is set to 6667.

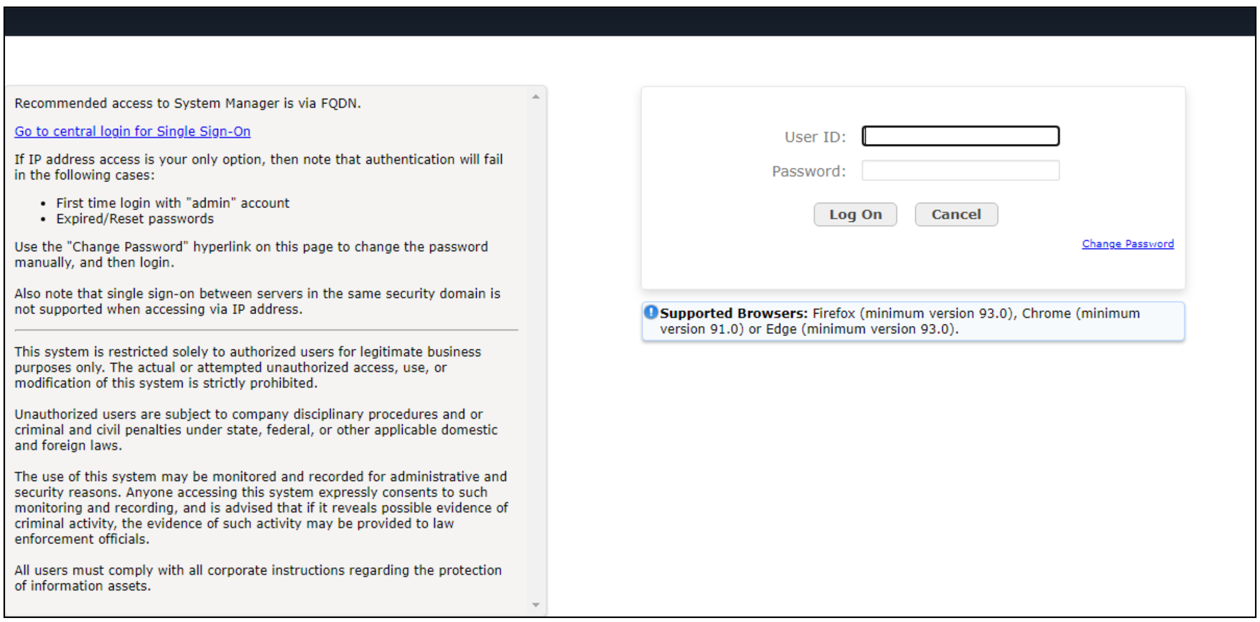
```
display hunt-group 67                                          Page   2 of  60
                                  HUNT GROUP






                      Message Center: sip-adjunct

     Voice Mail Number         Voice Mail Handle         Routing Digits
                                                   (e.g., AAR/ARS Access Code)
     6667                      6667                      8
```

6. Configure Avaya Aura® Session Manager

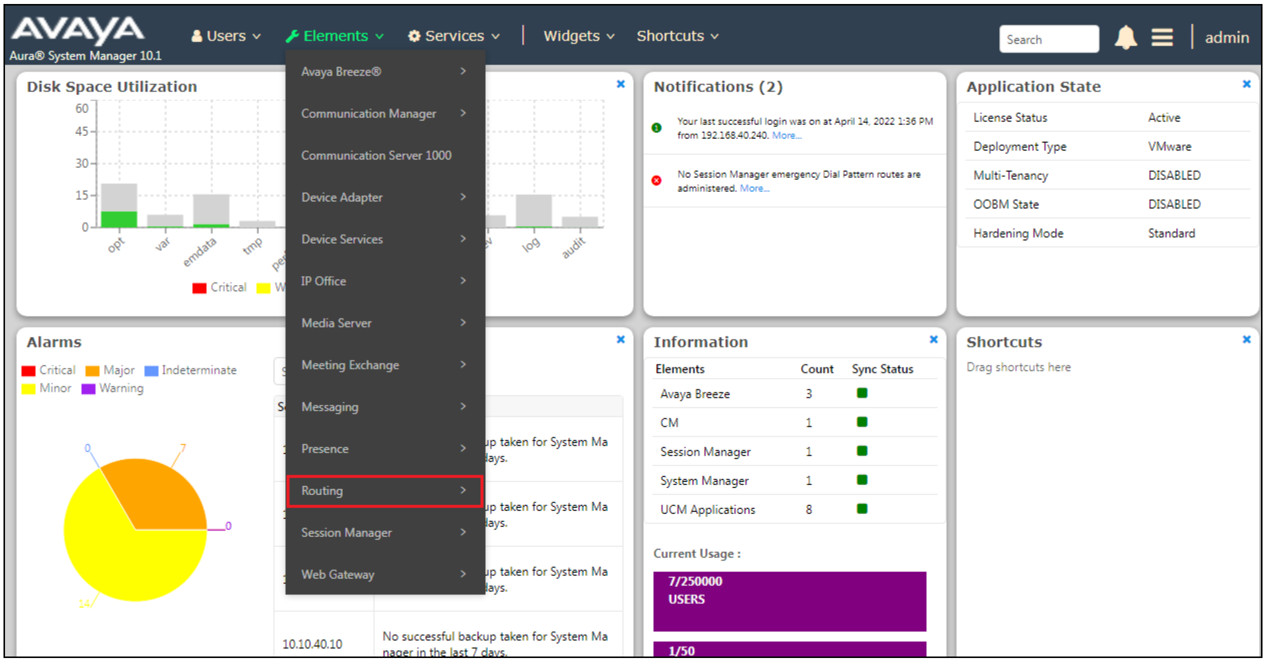
This section provides the procedures for configuring Session Manager. Session Manager is configured via System Manager. The procedures include the following areas:

- Domains and Locations
- Configure SIP Entity and Entity Link
- Adding Ascom SIP Users

To make changes on Session Manager a web session is established to System Manager. Log into System Manager by opening a web browser and navigating to https://<System Manager FQDN>/SMGR. Enter the appropriate credentials for the **User ID** and **Password** and click on **Log On**.



Once logged in navigate to **Elements** and click on **Routing**. This area is where the domain, location and SIP Entities are added.

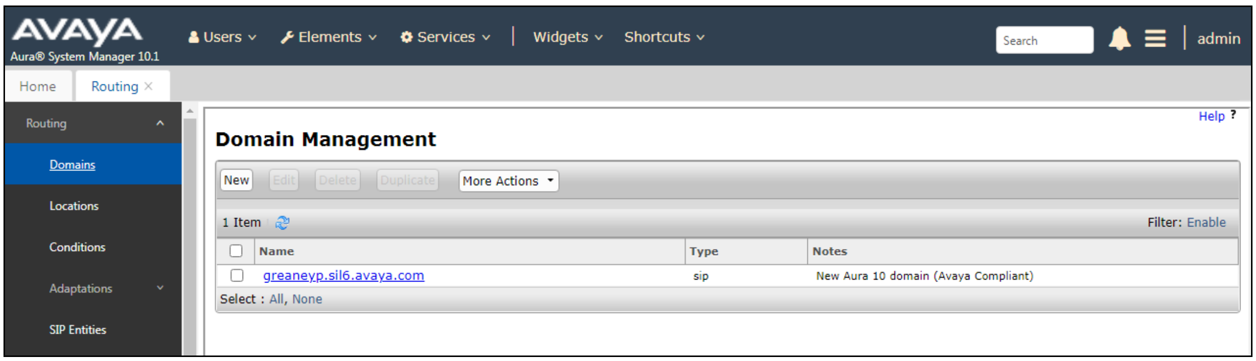


6.1. Domains and Locations

Note: It is assumed that a domain and a location have already been configured, therefore a quick overview of the domain and location that was used in compliance testing is provided here.

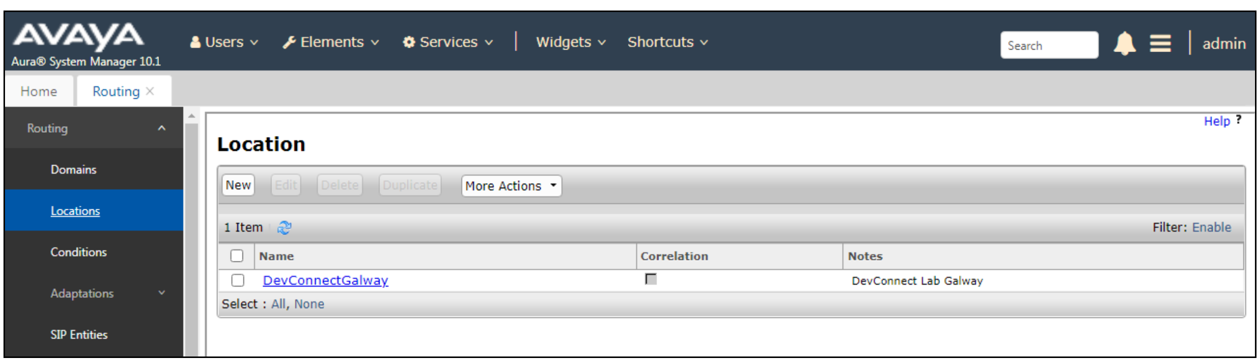
6.1.1. Display the Domain

Select **Domains** from the left window. This will display the domain configured on Session Manager. For compliance testing this domain was **greaneyp.sil6.avaya.com** as shown below. If a domain is not already in place, click on **New**. This will open a new window (not shown) where the domain can be added.



6.1.2. Display the Location

Select **Locations** from the left window and this will display the location setup. The example below shows the location **DevConnectGalway** which was used for compliance testing. If a location is not already in place, then one must be added to include the IP address range of the Avaya solution. Click on **New** to add a new location.



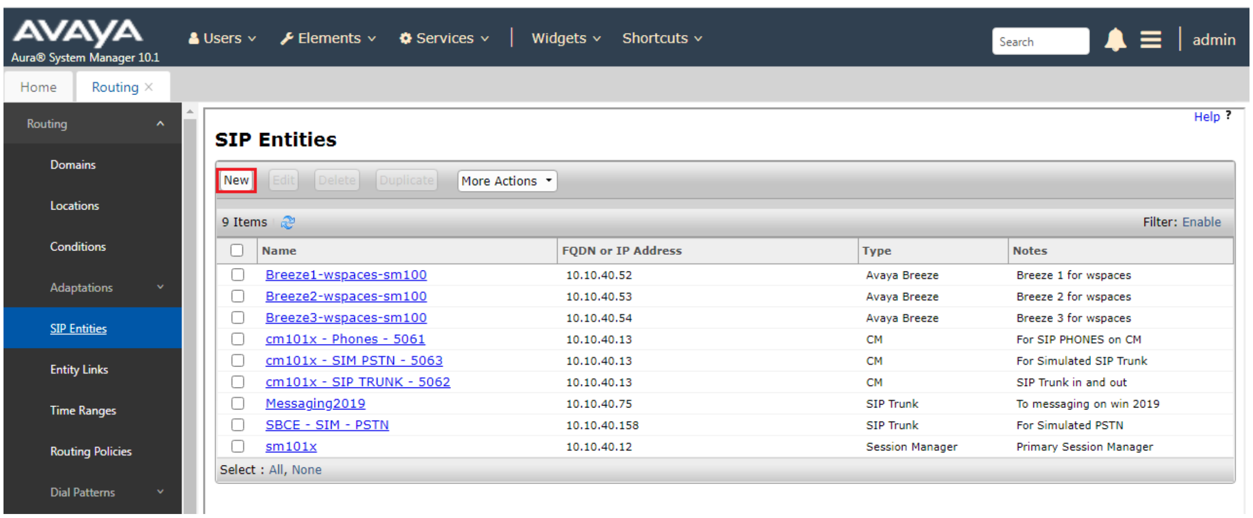
6.2. Configure SIP Entity and Entity Link

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's DECT handsets.

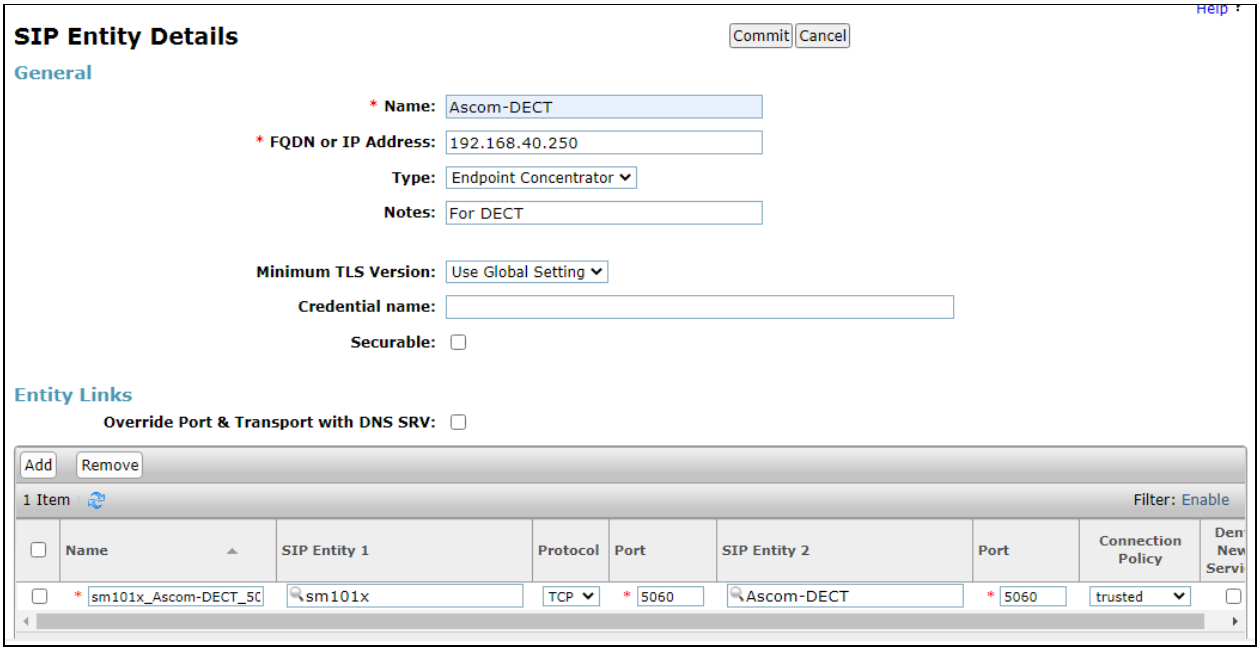
- Communication Manager SIP Entity
- Session Manager SIP Entity
- Messaging2019 SIP Entity

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 IPBS3. Select **SIP Entities** in the left window and click on **New** in the main window.

Note: If there is a Master and Standby base station, then a SIP Entity and Entity link are required for both the Master and Standby base stations.

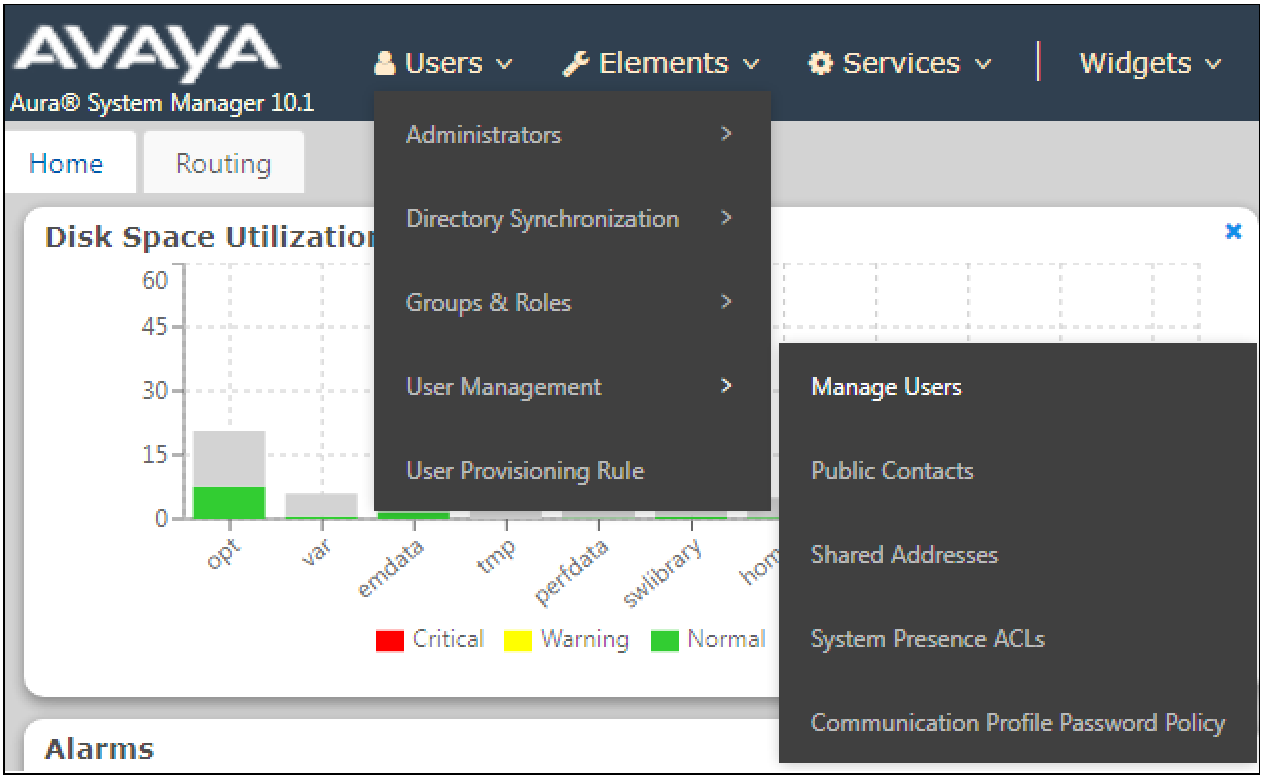


Enter a suitable **Name** and enter the **IP Address** of the DECT Base Station. Select **Endpoint Concentrator** as the **Type**. Under Entity Links, ensure that **TCP** is selected for the **Protocol** and **5060** for the **Port**. Click on **Commit** once completed.

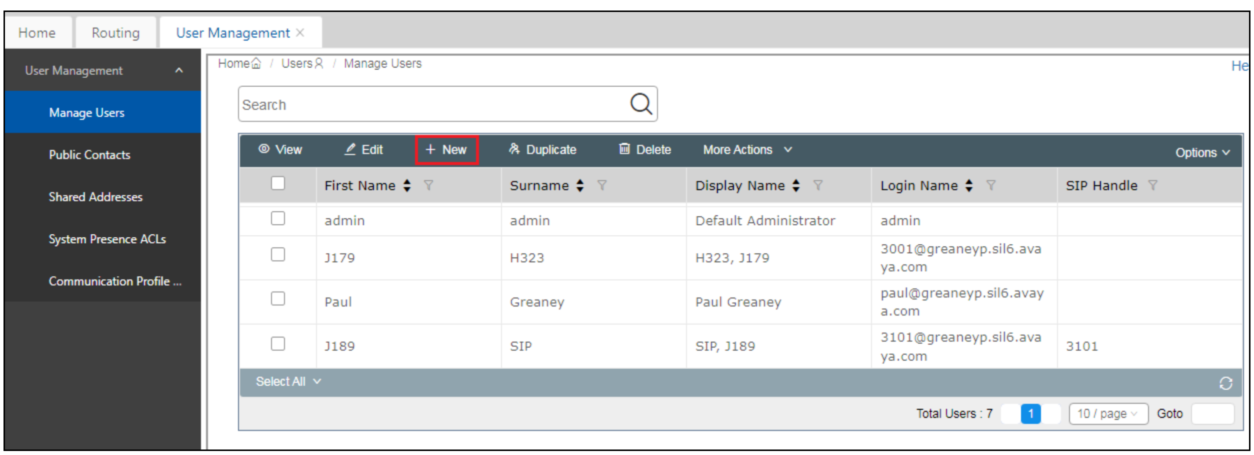


6.3. Adding Ascom SIP Users

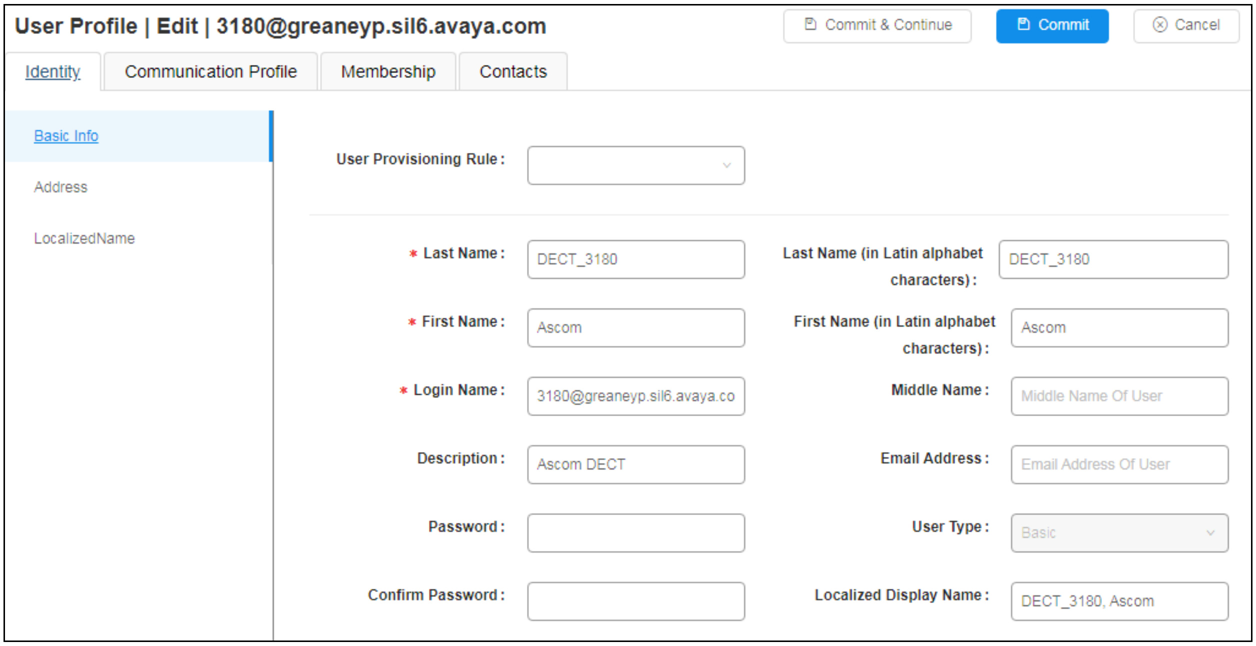
From the home page click on **User Management → Manager Users** shown below.



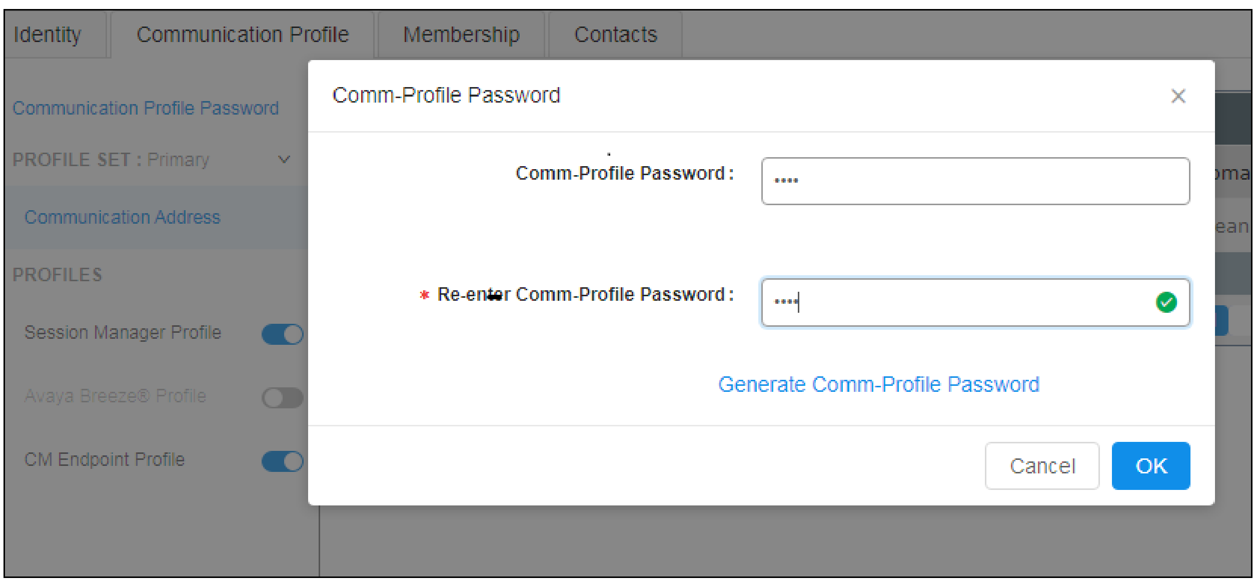
From **Manager Users** section, click on **New** to add a new SIP user.



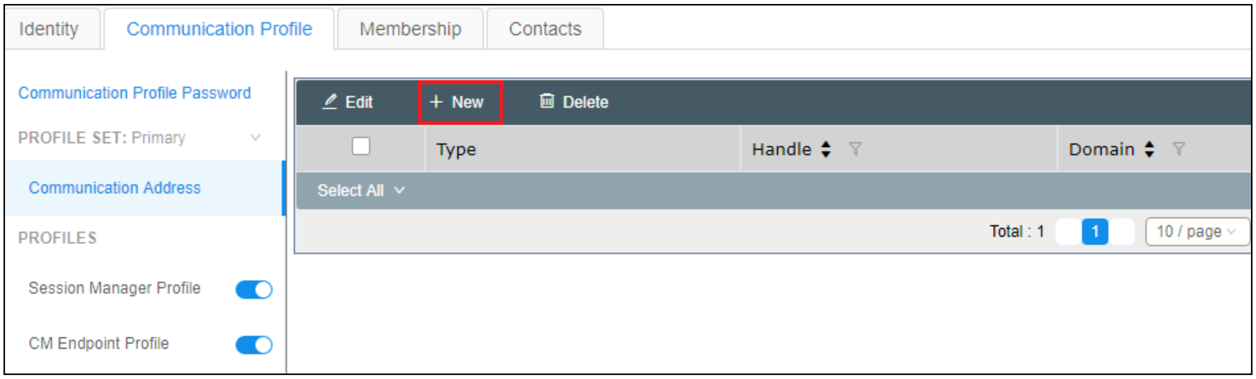
Under the **Identity** tab fill in the user's **Last Name** and **First Name** as shown below. Enter the **Login Name**, following the format of "user id@domain". The remaining fields can be left as default.



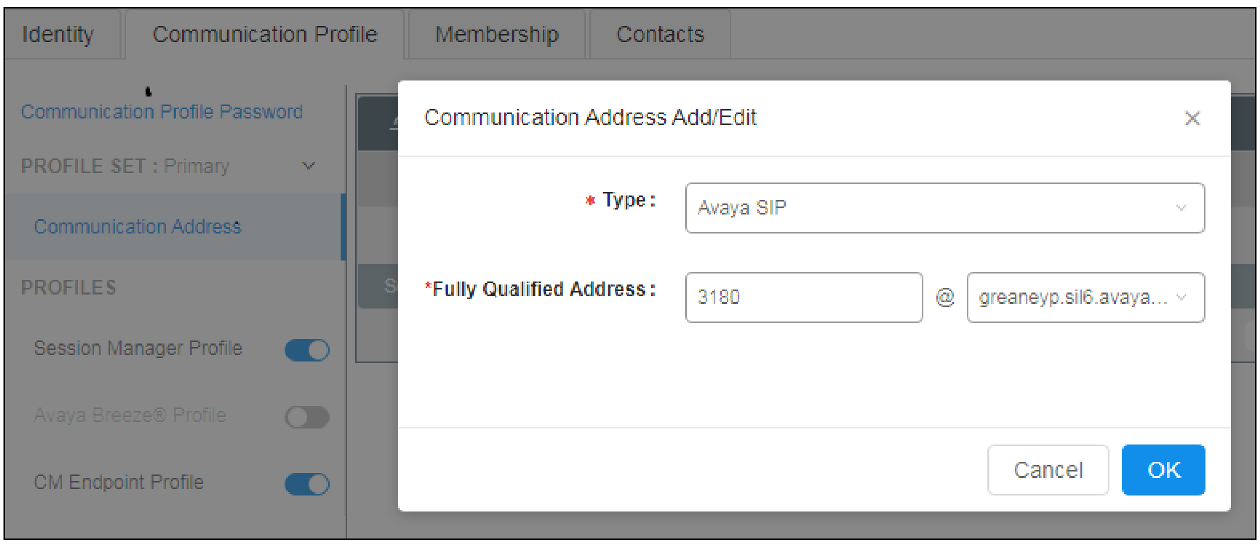
Under the **Communication Profile** tab enter **Communication Profile Password** and **Re-enter Comm-Profile Password**, note that his password is required when configuring the DECT handset in **Section 7.4**.



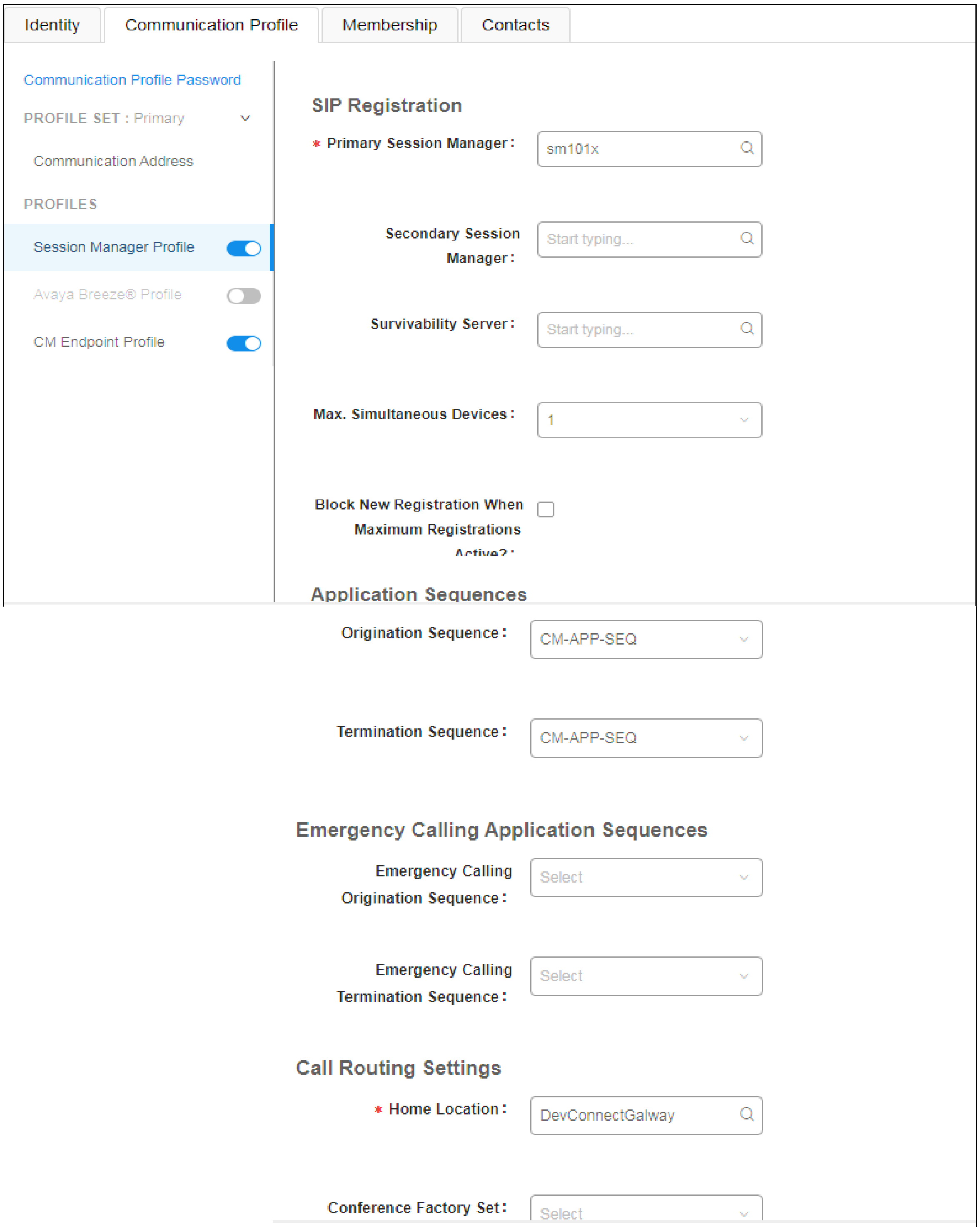
Staying on the **Communication Profile** tab, click on **New** to add a new **Communication Address**.



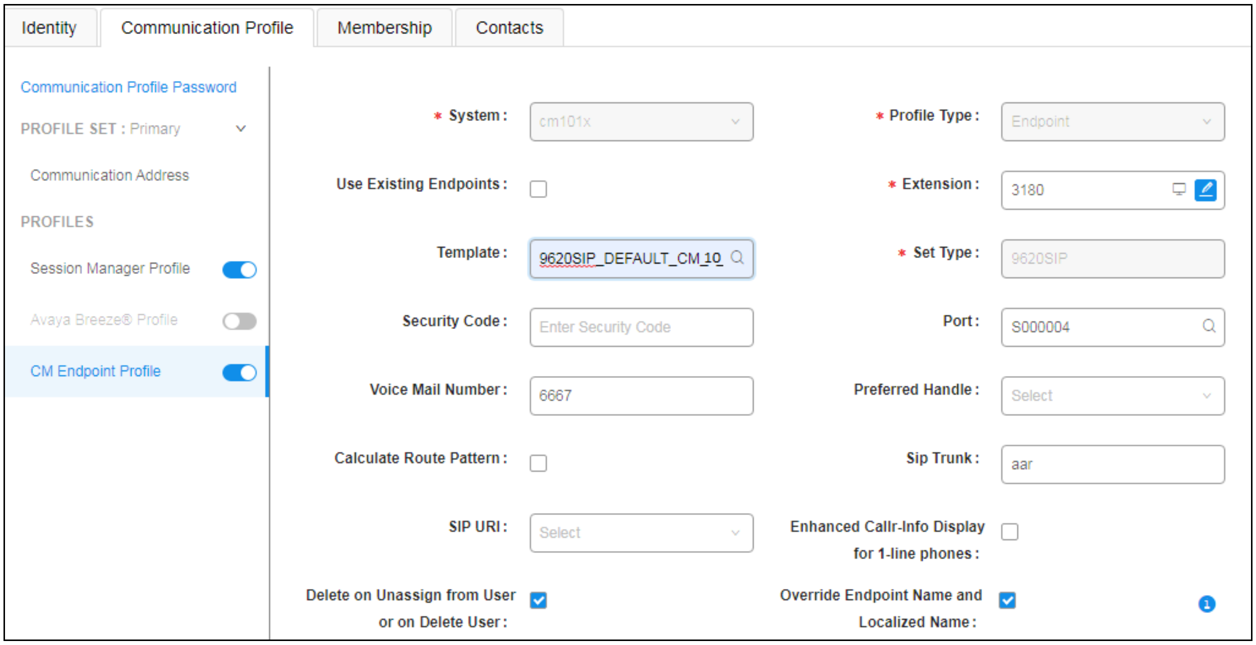
Enter the extension number and the domain for the **Fully Qualified Address** and click on **OK** once finished.



Ensure **Session Manager Profile** is checked and enter the **Primary Session Manager** details, enter the **Origination Sequence** and the **Termination Sequence**. Scroll down to complete the profile. Enter the **Home Location**, this should be the location configured in **Section 6.1.2**. Click on Commit at the top of the page (not shown).

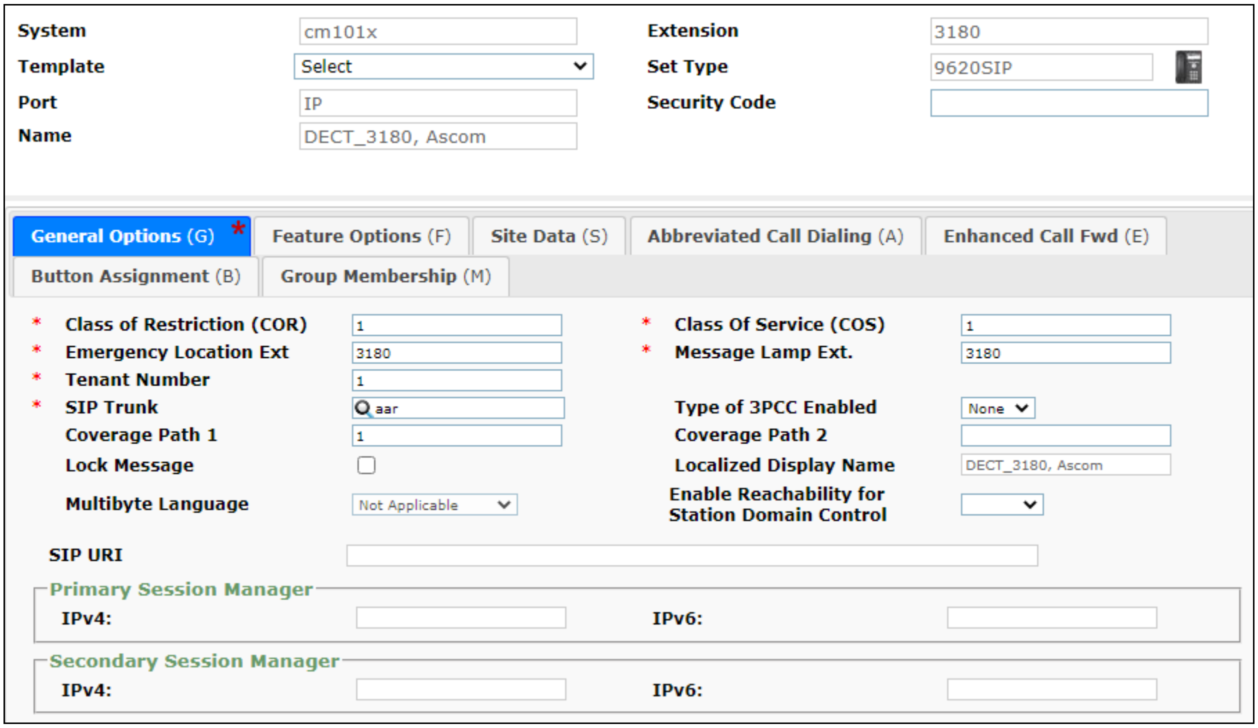


Click on the **CM Endpoint Profile** in the left window. Select the Communication Manager that is configured for the **System** and choose the **9620SIP_DEFAULT_CM_10_1** as the **Template**. Enter the appropriate **Voice Mail Number** and **Sip Trunk** should be set to **aar**, providing that the routing is setup correctly on Communication Manager. The **Profile Type** should be set to **Endpoint** and the **Extension** is the number assigned to the DECT handset. Click on **Endpoint Editor** to configure the buttons and features for that handset on Communication Manager.



Under the **General Options** tab ensure that **Coverage Path 1** is set to that configured in **Section 5.6**. Also ensure that **Message Lamp Ext.** is showing the correct extension number. The **Class of Restriction** and **Class of Service** should be set to the appropriate values for the DECT handset. This may vary depending on what level of access/permissions the handset has been given. Other tabs can be checked but for compliance testing the values were left as default. Click on **Done** (not shown) to complete.

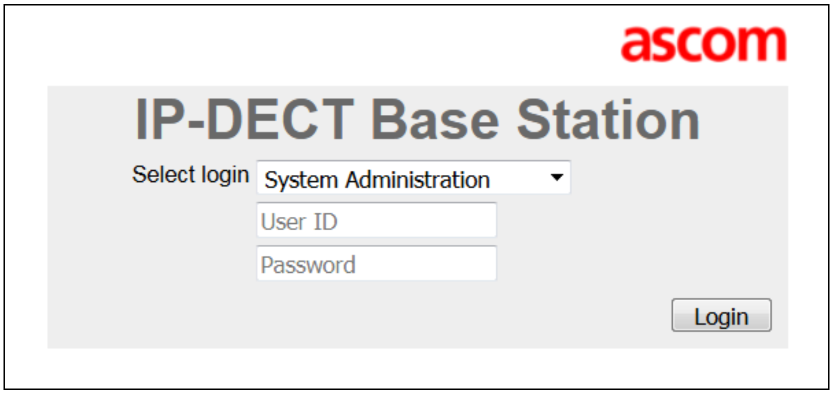
Note: For compliance testing the default value of three call appearance buttons were used. This can be changed under the **Button Assignment** tab.



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

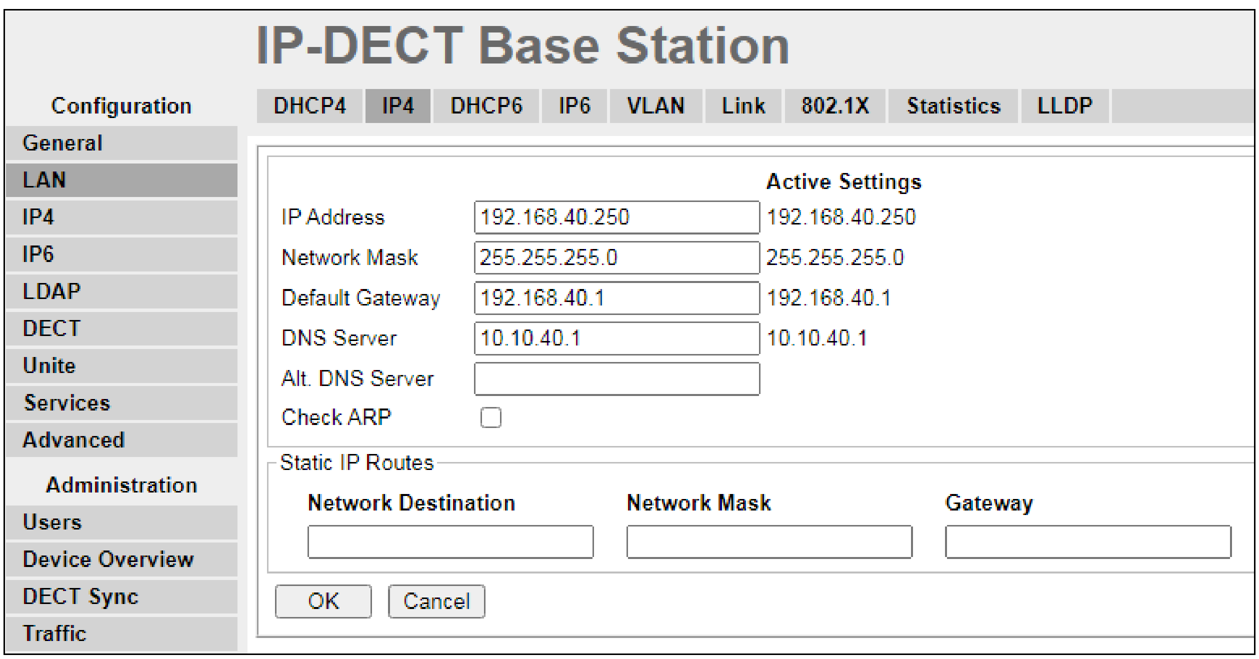
7. Configure Ascom DECT Base Station and Handsets

The configuration of the DECT base station and the DECT handsets is carried out by opening a web browser to 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. Enter the proper credentials for **User ID** and **Password** and click on **Login**.



7.1. Configure DECT Base Station IP address

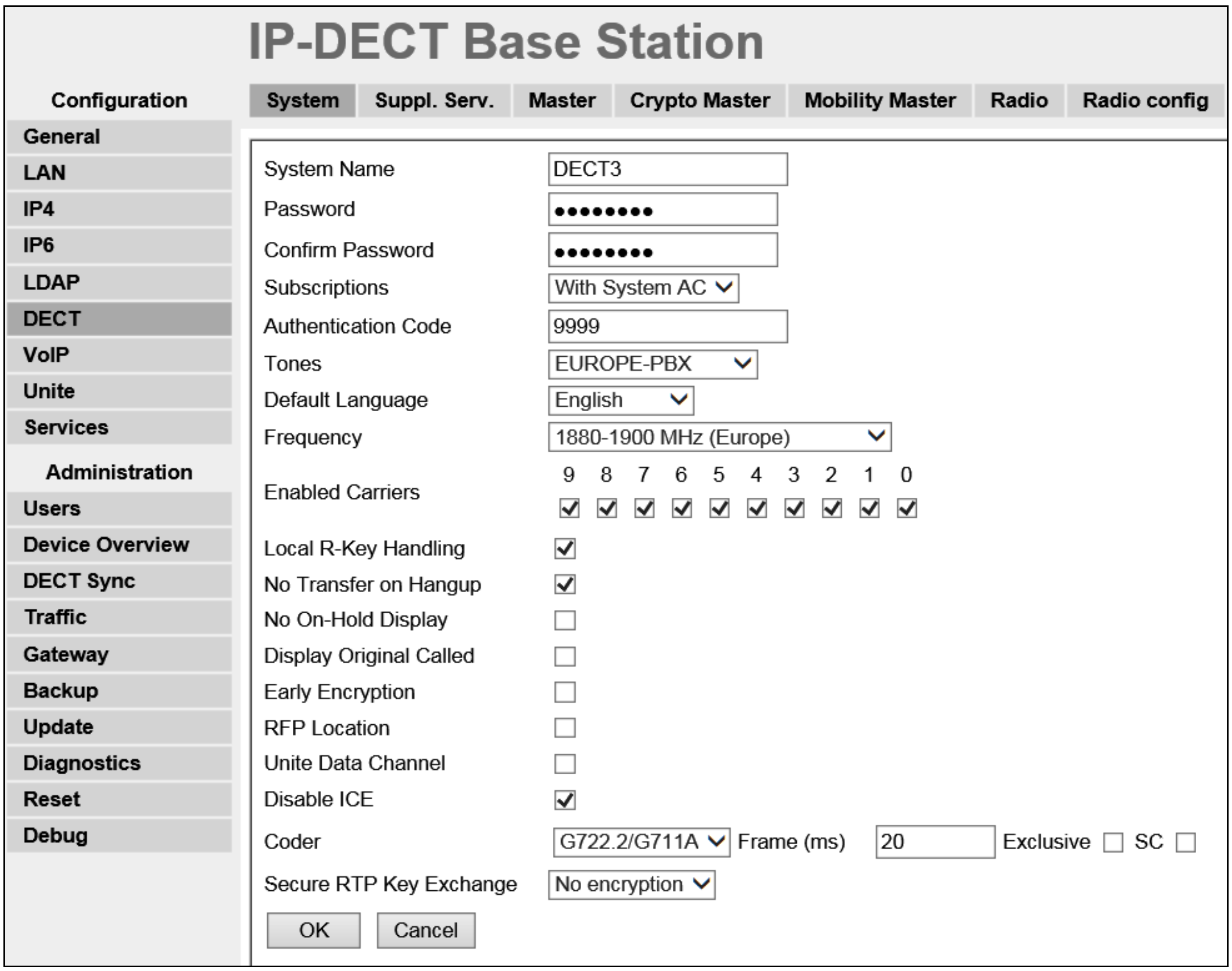
To change the IP Address of the DECT Base Station in order to connect to the local LAN select **LAN** in the left column and click on the **IP4** tab. Enter the **IP Address**, **Network Mask**, **Default Gateway** and **DNS Server** information of the DECT Base Station and click on **OK**. Ensure also that DHCP mode is set to disabled under the **DHCP** tab (not shown).



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

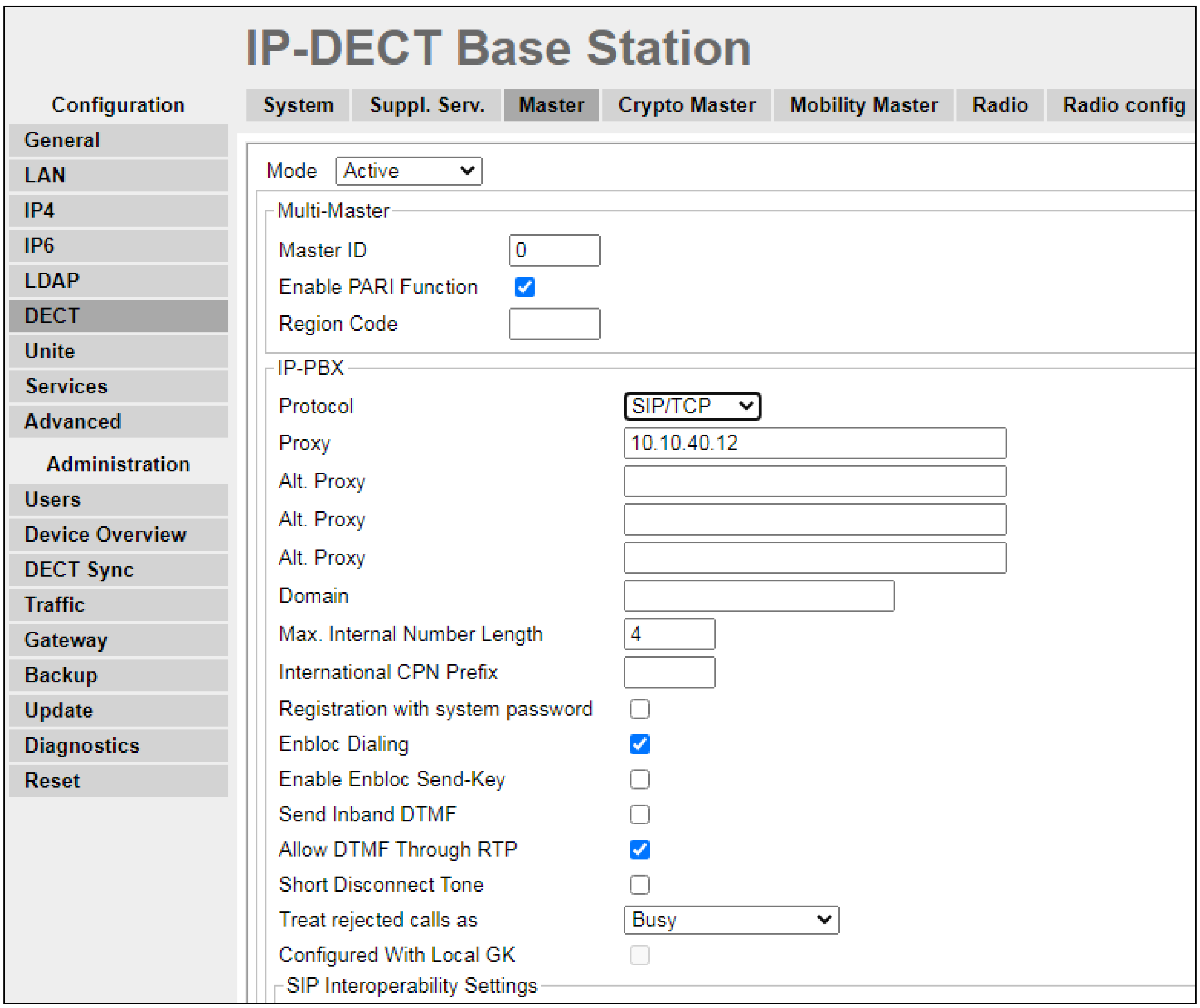
Select **DECT** in the left column and click on the **System** tab in the main window. Ensure that **Subscriptions** is set to **With System AC** and enter an appropriate **Authentication Code** (this is used in **Section 7.4** to subscribe the DECT handset to the base station). Note that the password seen here is not the password for the SIP users on Session Manager. Select the appropriate country for **Tones**, note for these compliance tests **EUROPE-PBX** was selected. Select **1880-1900 MHz (Europe)** for the **Frequency** and ensure that **Local R-Key Handling** box is checked. For **Coder** select **G722.2/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.



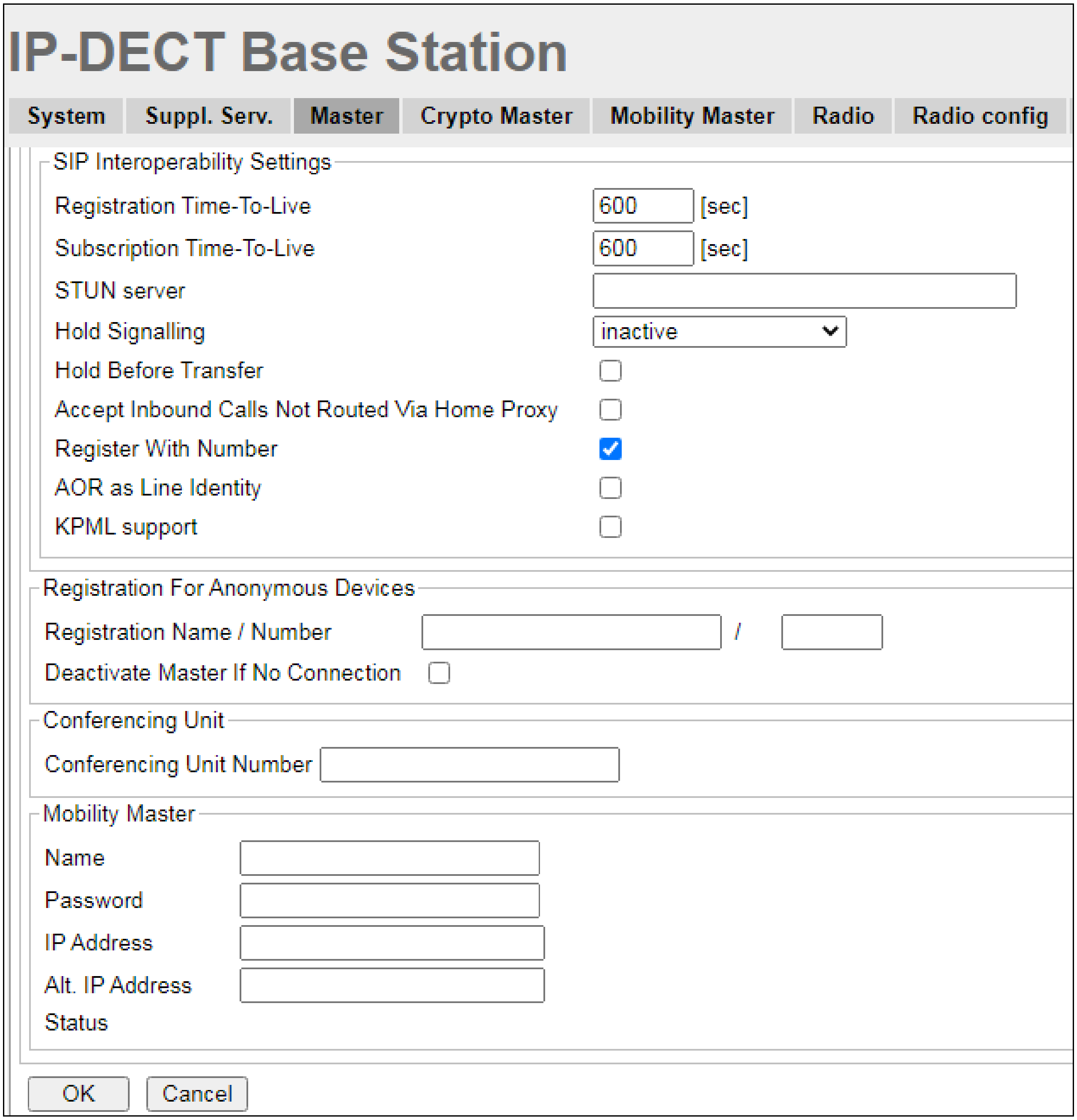
7.3. Configure Session Manager Information

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 6.2**.

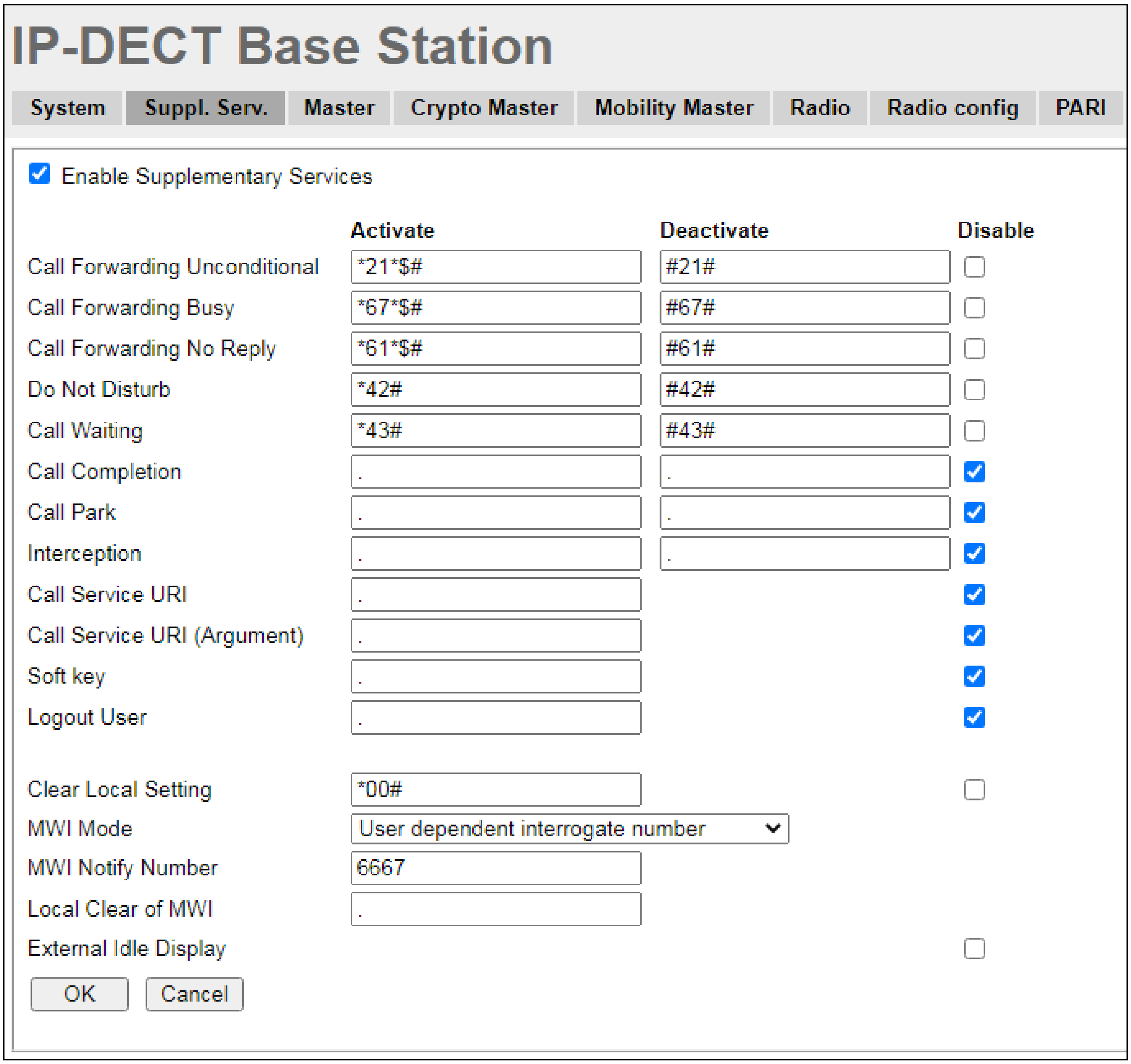


Scrolling down on the same page…., these are the settings that were used for compliance testing.



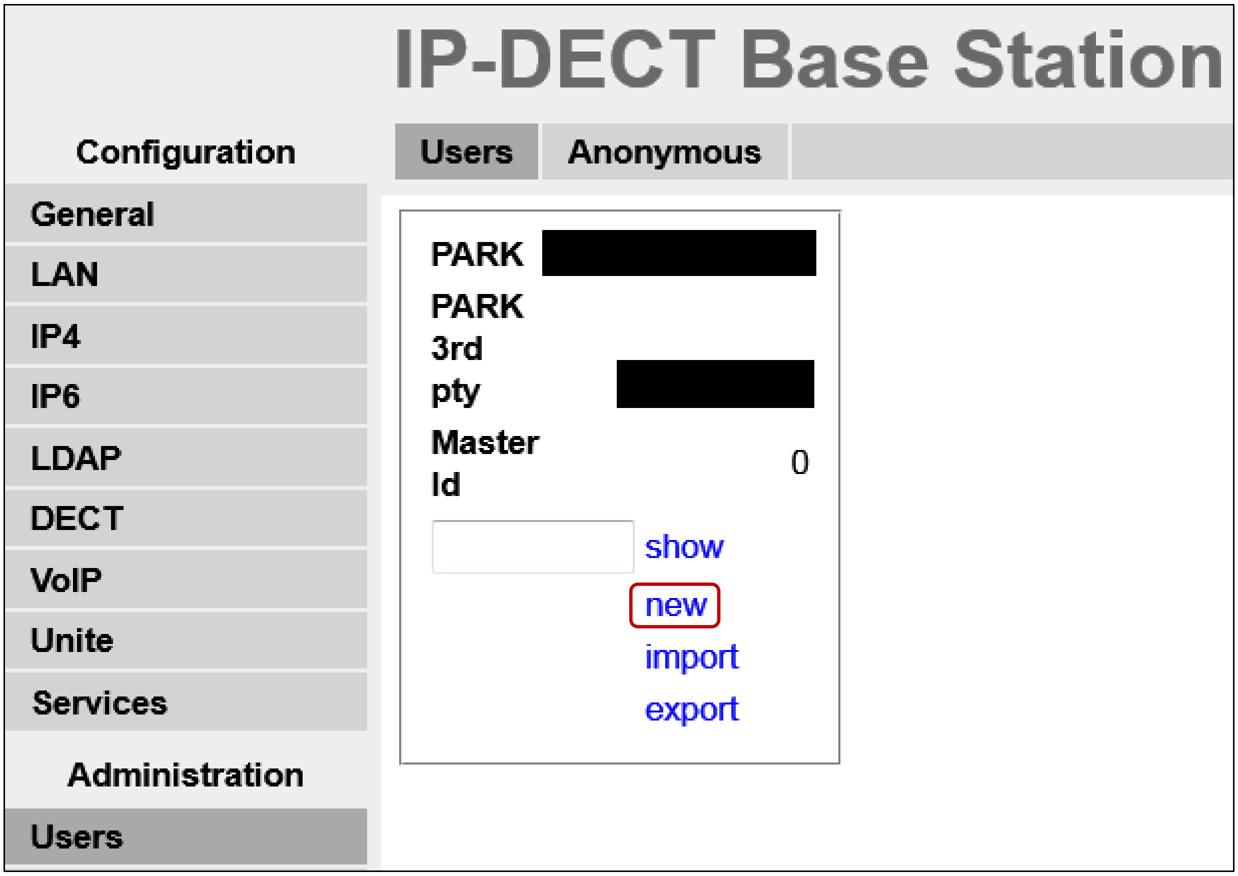
Click on the **Suppl. Serv.** tab and ensure that **Enable Supplementary Services** box is checked. Take note of the activation and deactivation codes for services such as **Call Forwarding**, **Call Waiting** and **Do Not Disturb**. Click on **OK** when finished. These codes are unique to the Ascom 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 **6667**, as per **Section 5.6**.

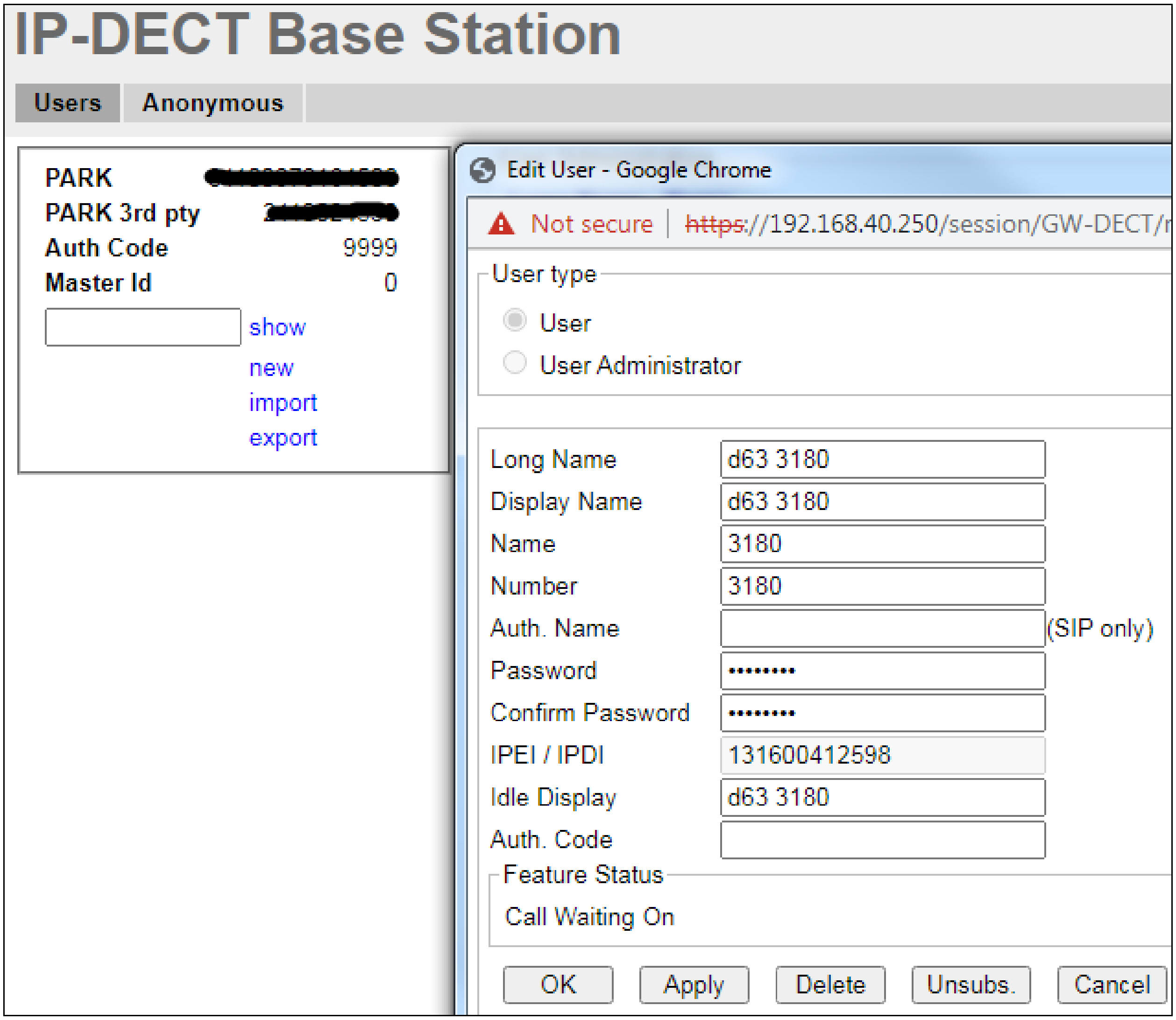


7.4. Adding DECT Users

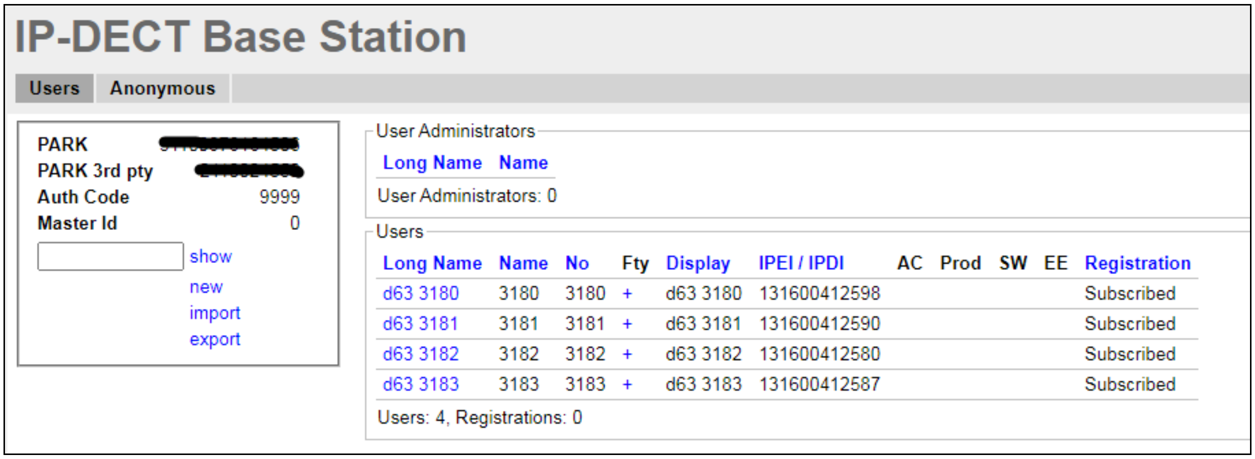
Click on **Users** in the left column and under the **Users** tab seen on right column, click **new** to add a new DECT user.



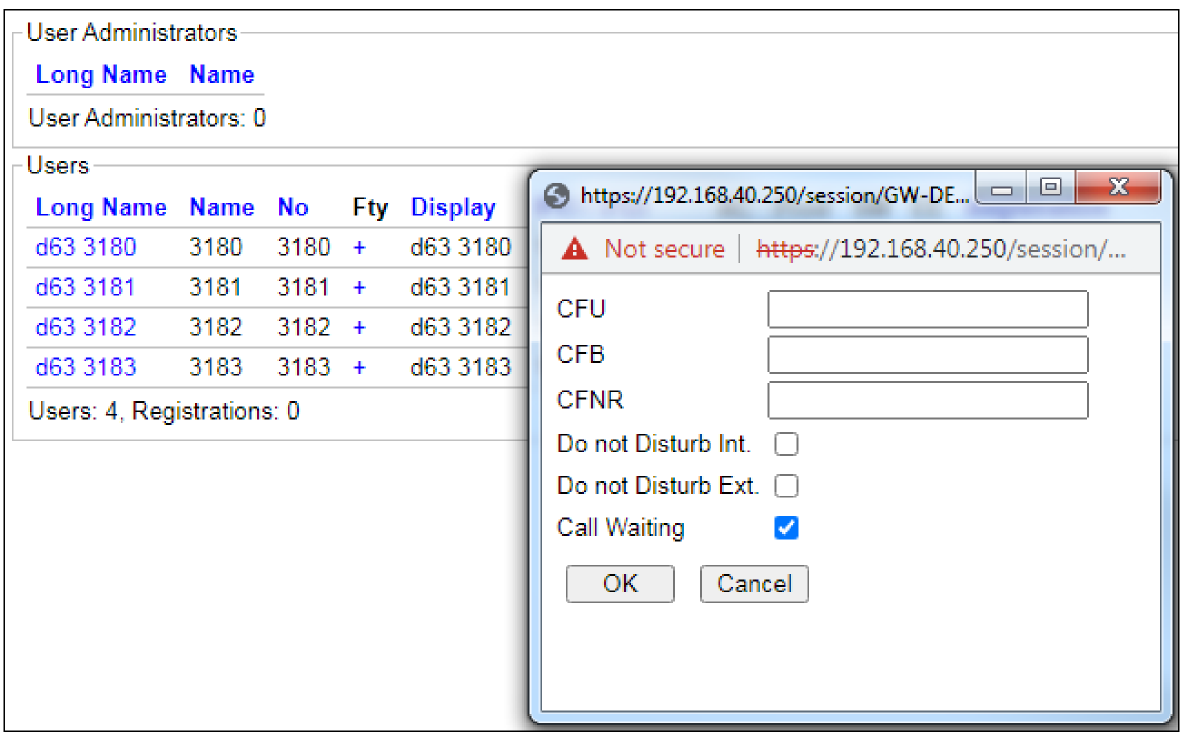
Enter the appropriate information for the new DECT user and once all the information has been correctly filled in click on the **OK** button. The DECT handset is then registered with the DECT system, according to Ascom's documentation. The Password entered should be the same as that configured in **Section 6.3**.



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.

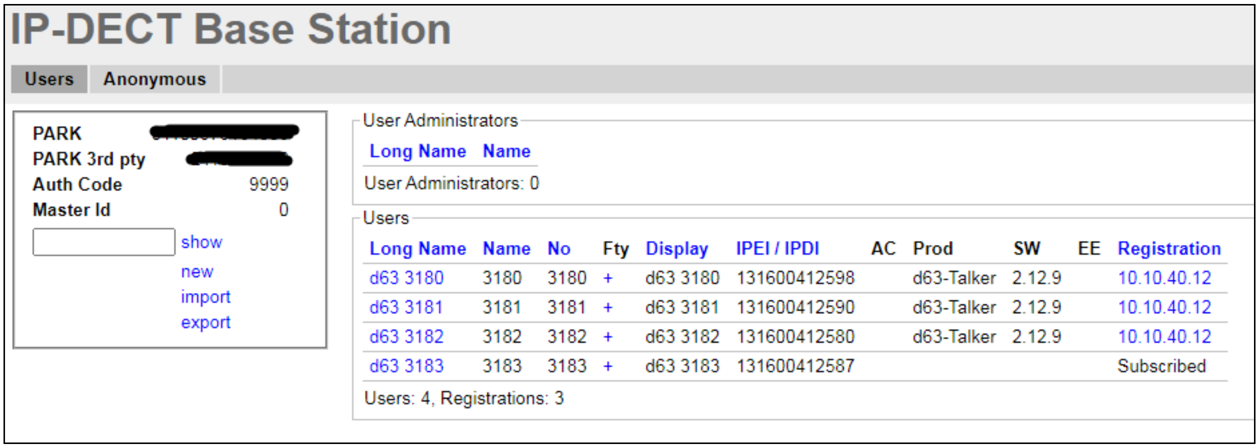


To change features such as **Call Waiting** or **Do not Disturb** click on the **+** icon under **Fty** as highlighted below. This opens a new window where these services can be selected or deselected. Click on **OK** once the appropriate services are selected.

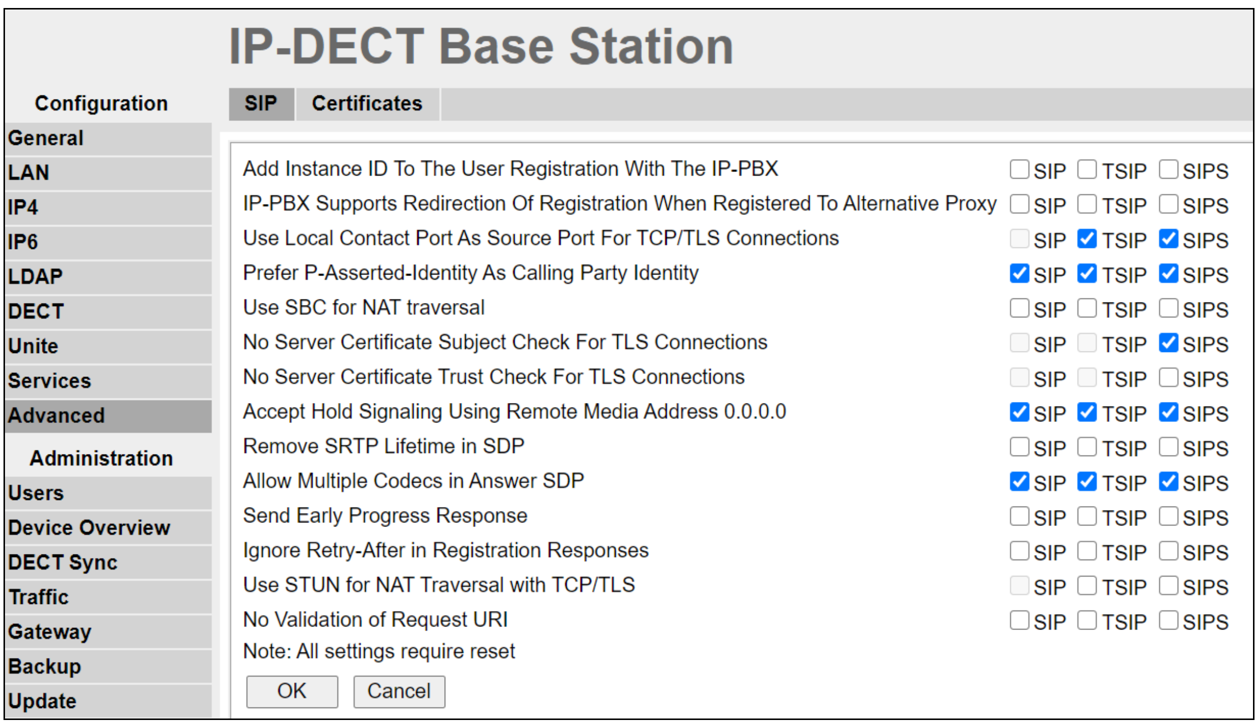


Telephony features, such as Call Waiting and Call Forwarding, can be programmed by entering feature codes on the handset. Please refer to the **Suppl. Serv**. tab in **Section 7.3**.

As a final step, confirm that DECT handsets have registered successfully with Session Manager, noting the IP address should be that of Session Manager, under **Registration**.



These settings were used for compliance testing but can be adjusted to suit each site as required. Please refer to Ascom documentation in **Section 10** for further information.



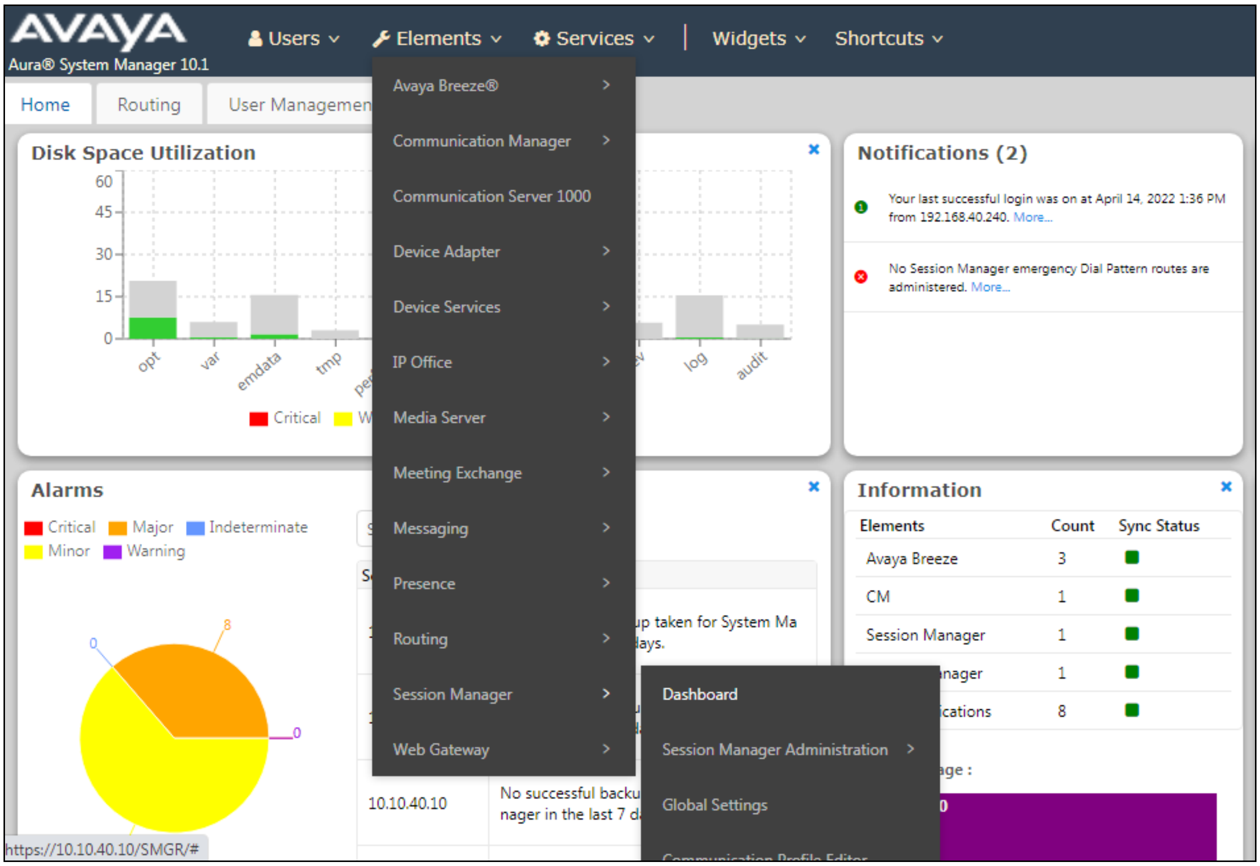
Note: In larger DECT systems where it takes longer (>4s) to reach the DECT handset, it is recommended to enable **Send early progress response** under **VoIP → SIP**.

8. Verification Steps

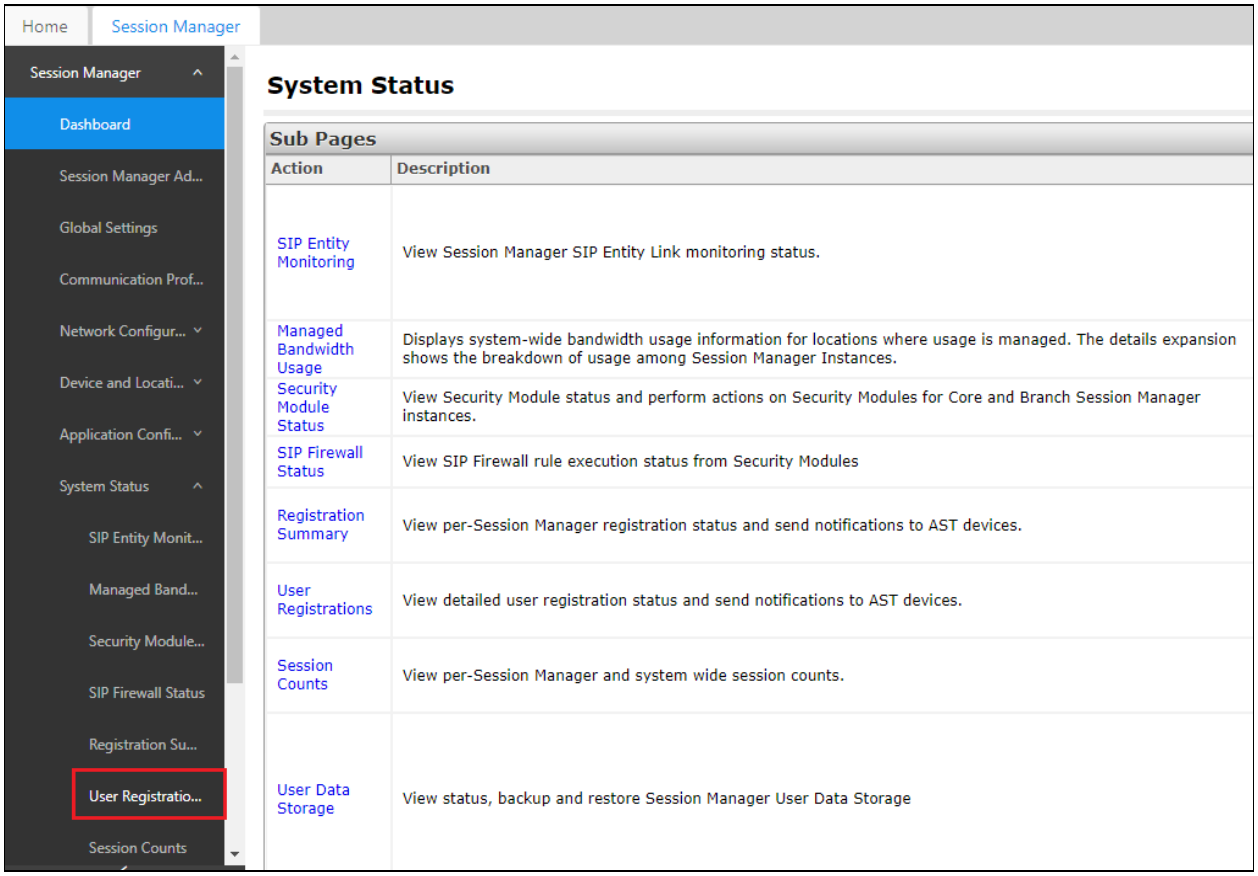
The following steps can be taken to ensure that connections between Ascom DECT handsets and Session Manager and Communication Manager are up.

8.1. Session Manager Registration

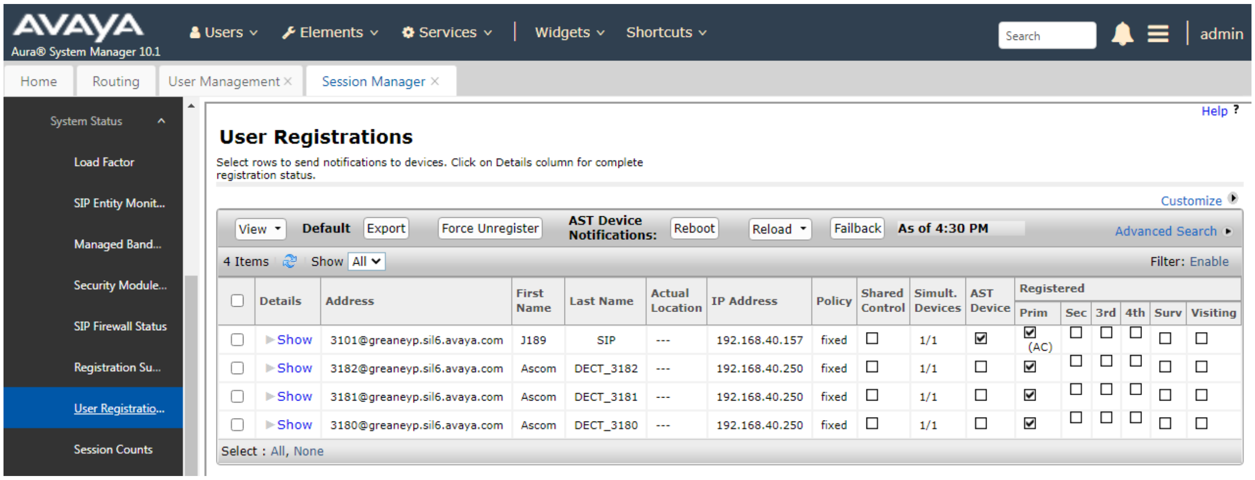
Log into System Manager as done previously in **Section 6**, select **Elements → Session Manager → Dashboard**.



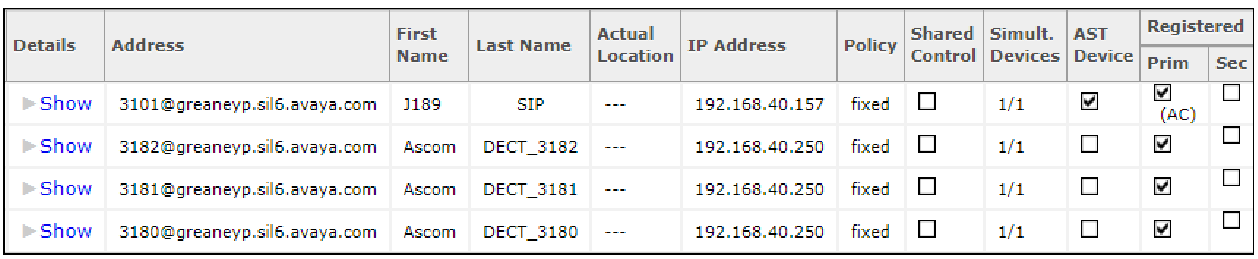
Under **System Status** in the left window, select **User Registrations** to display all the SIP users that are currently registered with Session Manager.



The Ascom DECT users should show as being registered as seen below.



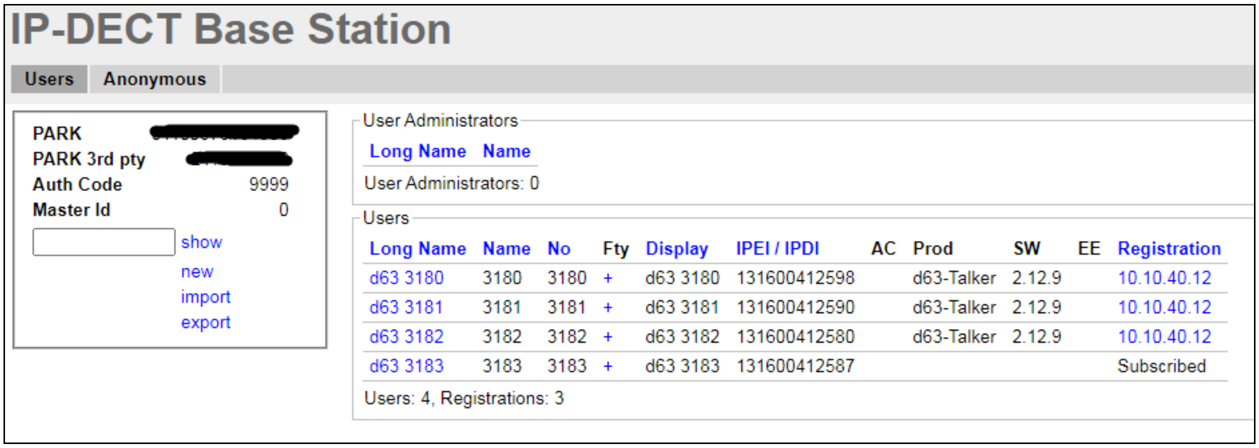
DECT user **3180** is shown as being registered as it has an **IP Address** associated with it and there is a tick in the **Registered Prim** box.



Details	Address	First Name	Last Name	Actual Location	IP Address	Policy	Shared Control	Simult. Devices	AST Device	Registered Prim	Registered Sec
Show	3101@greaneyp.sil6.avaya.com	J189	SIP	---	192.168.40.157	fixed	☐	1/1	☑	☑ (AC)	☐
Show	3182@greaneyp.sil6.avaya.com	Ascom	DECT_3182	---	192.168.40.250	fixed	☐	1/1	☐	☑	☐
Show	3181@greaneyp.sil6.avaya.com	Ascom	DECT_3181	---	192.168.40.250	fixed	☐	1/1	☐	☑	☐
Show	3180@greaneyp.sil6.avaya.com	Ascom	DECT_3180	---	192.168.40.250	fixed	☐	1/1	☐	☑	☐

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, three out of the four extensions **3180** to **3183** are registered correctly.



IP-DECT Base Station

Users | Anonymous

PARK	[redacted]
PARK 3rd pty	[redacted]
Auth Code	9999
Master Id	0

show
new
import
export

User Administrators

Long Name	Name

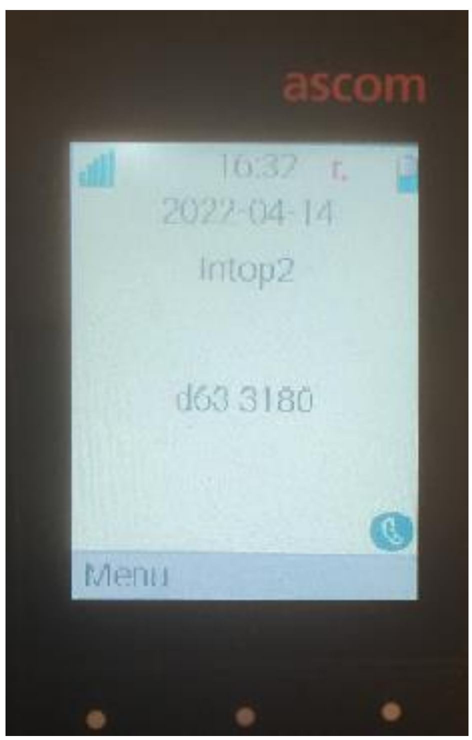
User Administrators: 0

Users

Long Name	Name	No	Fty	Display	IPEI / IPDI	AC	Prod	SW	EE	Registration
d63 3180	3180	3180	+	d63 3180	131600412598		d63-Talker	2.12.9		10.10.40.12
d63 3181	3181	3181	+	d63 3181	131600412590		d63-Talker	2.12.9		10.10.40.12
d63 3182	3182	3182	+	d63 3182	131600412580		d63-Talker	2.12.9		10.10.40.12
d63 3183	3183	3183	+	d63 3183	131600412587					Subscribed

Users: 4, Registrations: 3

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 IP-DECT R11 to successfully interoperate with Avaya Aura® Communication Manager R10.1 and Avaya Aura® Session Manager R10.1 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. *Avaya Aura® Communication Manager Feature Description and Implementation*, Release 10.1
2. *Administering Avaya Aura® Session Manager*, Release 10.1

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 11                                      Page   1 of   3
                                SIGNALING GROUP

 Group Number: 11             Group Type: sip
  IMS Enabled? n        Transport Method: tls
        Q-SIP? n
     IP Video? n                                  Enforce SIPS URI for SRTP? n
  Peer Detection Enabled? y  Peer Server: SM                      Clustered? n
 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: sm101x
 Near-end Listen Port: 5061               Far-end Listen Port: 5061
                                       Far-end Network Region: 1

Far-end Domain: greaneyp.sil6.avaya.com
                                             Bypass If IP Threshold Exceeded? n
Incoming Dialog Loopbacks: eliminate                  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 Page 1

```
display trunk-group 11                                          Page   1 of   5
                                TRUNK GROUP

Group Number: 11                   Group Type: sip           CDR Reports: y
  Group Name: SIP PHONES                  COR: 1        TN: 1        TAC: *811
   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: 11
                                                     Number of Members: 10
```

Page 2

```
display trunk-group 11                                          Page   2 of   5
      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): 600

 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
```

Page 3

```
display trunk-group 11                                          Page   3 of   5
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? n
                                                Replace Unavailable Numbers? n


                               Modify Tandem Calling Number: no
               Send UCID? y




 Show ANSWERED BY on Display? y

 DSN Term? n
```

Page 4

```
display trunk-group 11                                          Page   4 of   5
                           SHARED UUI FEATURE PRIORITIES

                             ASAI: 1

         Universal Call ID (UCID): 2

MULTI SITE ROUTING (MSR)

                      In-VDN Time: 3
                         VDN Name: 4
                 Collected Digits: 5
            Other LAI Information: 6
                   Held Call UCID: 7
                          ECD UUI: 8
```

Page 5

```
display trunk-group 11                                          Page   5 of   5
                              PROTOCOL VARIATIONS

                                       Mark Users as Phone? y
Prepend '+' to Calling/Alerting/Diverting/Connected Number? n
                       Send Transferring Party Information? y
                                  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: 101


                        Convert 180 to 183 for Early Media? n
                  Always Use re-INVITE for Display Updates? n
     Resend Display UPDATE Once on Receipt of 481 Response? n
                        Identity for Calling Party Display: From
            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
```

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.