Avaya Solution & Interoperability Test Lab

Application Notes for configuring Ascom Myco 2 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 Myco 2 smartphone 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 Myco 2 smartphone (Myco) to interoperate with Avaya Aura® Communication Manager R8.0.1 and Avaya Aura® Session Manager R8.0.1. Ascom Myco is a smart phone built for the on-the-job usability, especially suited for nurses and clinicians, as well as the demanding environment of healthcare. It provides reliable communication and access to information at the point of care.

Note: Ascom Myco 2 may be referred to as Myco, Myco handset or Myco smartphone throughout this document. These names all refer to the same product, a smartphone that is connected to Avaya Aura® Communication Manager by registering with Avaya Aura® Session Manager as a third-party SIP extension.

Ascom Myco is configured as a 9620 SIP endpoint on Avaya Aura® Communication Manager which will then register as a SIP endpoint with Avaya Aura® Session Manager. Myco then behaves as a third-party SIP extension on Avaya Aura® Communication Manager able to make/receive internal and PSTN/external calls and utilise telephony facilities available on Avaya Aura® Communication Manager.

2. General Test Approach and Test Results

The interoperability compliance testing evaluates the ability of Ascom Myco smartphone to make and receive calls to and from Avaya H.323, SIP and digital deskphones as well external calls over a simulated SIP PSTN. Avaya Aura® Messaging was used to demonstrate DTMF and Message Waiting Indication (MWI).

Note: The cellular version of the Ascom Myco smartphone can be set up to use Wi-Fi, GSM or both. For compliance testing the Wi-Fi version was used and an Ascom approved wireless access point set up to provide a network connection. This wireless router was considered a part of Ascom's overall solution.

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/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.

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 Myco did not include use of any specific encryption features as requested by Ascom.

Note: Compliance testing was carried out using TCP as the transport for signaling, a selection of basic calls and transfer calls were carried out using UDP.

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 deskphones, Ascom Myco handsets and "PSTN" endpoints.

- Basic Calls
- Session Refresh Timer
- Long Duration Call
- Hold, Retrieve and Brokering (Toggle)
- Feature Access Code dialing
- 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 Myco handset being the EC500 destination.
- Multi-Device Access (MDA)
- Attended Conference (also local three-way calling)
- Calling Line Name/Identification

- Codec Support (G.711, G.729, G.722)
- DTMF Support
- Voice Mail, Message Waiting Indication
- Serviceability

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 Myco and Communication Manager handsets. The tests were all functional in nature and performance testing and redundancy testing were not included. All test cases passed successfully with all issues and observations listed below.

The following is not supported by Myco by design.

- Ascom Myco does not support local call diversion like Call Forward All, Call Forward Busy and Call Forward No Answer.
- When using the EC500 (concurrent call) feature, if an Myco 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 Myco handset users, calls may be answered by a cellular user's voicemail instead of following the coverage criteria in Communication Manager.
- When a Myco handset is configured as an EC500 destination for an Avaya endpoint, an incoming call to the Avaya endpoint will ring both the Avaya endpoint and the Myco handset. When the call is declined on the Myco handset, the Avaya endpoint continues to ring as per normal design.
- All compliance testing was done using TCP (preferred) and UDP as the transport protocol.
- Negotiation of G.722 between endpoints, such as the Ascom Myco, requires support for the codec to be configured on Communication Manager.
- When an Avaya endpoint or a Myco handset calls another Myco handset, after the called Myco handset declines the call, the display for the Myco calling party shows busy whereas the Avaya calling party receives the busy tone.
- Ascom Myco handset supports third party conference, which is, Myco makes two calls simultaneously and conferences the calls locally.

- When multiple voice messages are left for a Myco handset, the handset shows the total number of messages as only "1" in the display even though there are multiple messages. This is because there is no counter information sent in the NOTIFY from Avaya Aura® Messaging.
- For Multi-Device Access (MDA), Myco needs to be configured using and registering through Endpoint ID. Also, the MWI configuration has to be identical on all Myco handsets that are configured for MDA. Refer to **Section 7.3** for details.
- Per design, Myco handsets do not have a redial button. User needs to use "Call List" and redial the numbers.

The following observations/limitations were noted during compliance testing.

- Call forward not being displayed on the Myco when Session Manager sends on the "181 Call is being Forwarded" message. Ascom are investigating this issue (MRS-66).
- Call list – When Myco calls to a diverted Avaya set (coverage to Messaging) and hangs up when the caller hears voicemail, the entry in the "call list" shows that of the dialed Avaya phone but it calls to voicemail which is incorrect, it should also dial the Avaya phone. Ascom are investigating the issue, MRS-295.

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 Myco 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. Ascom Myco handsets connect to an Ascom approved wireless router which is placed on the LAN. Myco registers with Session Manager to be able to make/receive calls to and from the Avaya H.323, SIP and digital deskphones on Communication Manager.

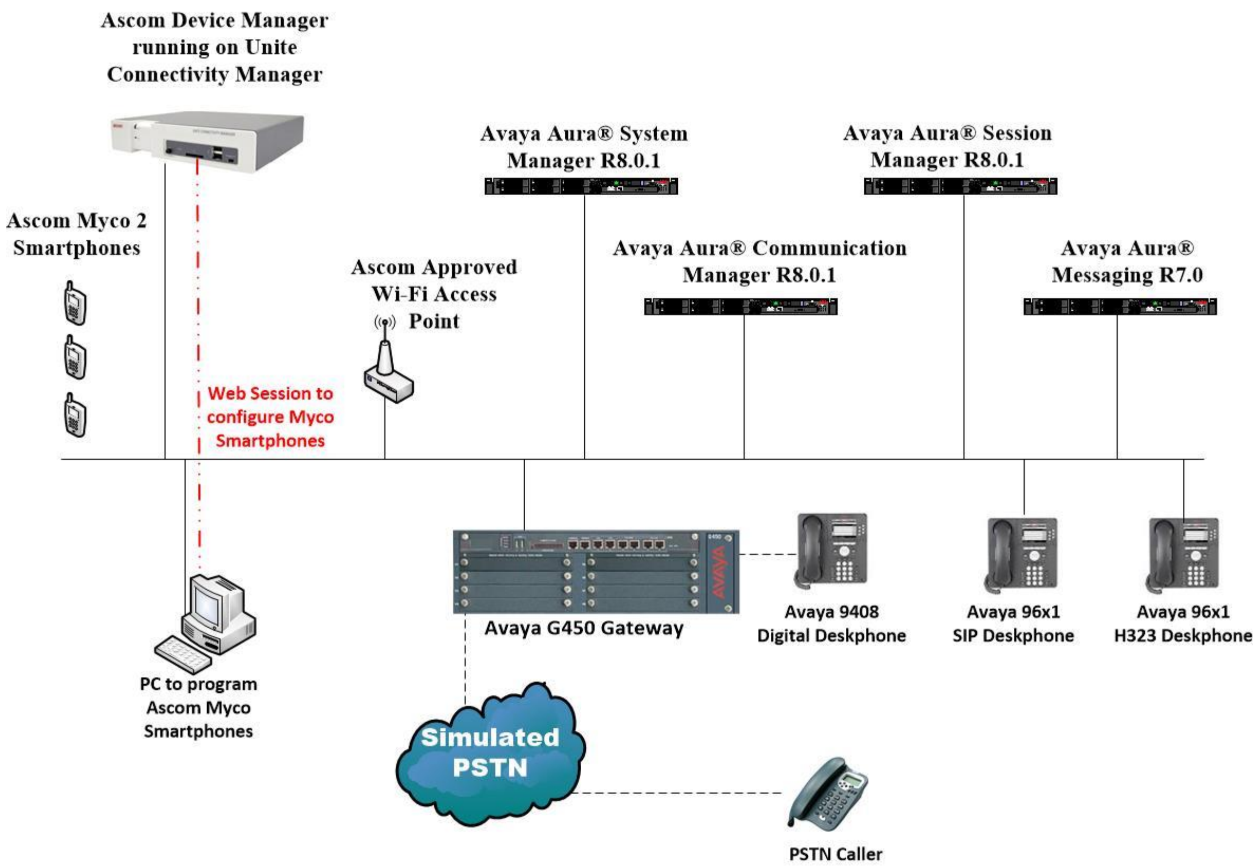


Figure 1: Network Solution of Ascom Myco Smartphone with Avaya Aura® Communication Manager R8.0.1 and Avaya Aura® Session Manager R8.0.1

4. Equipment and Software Validated

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

Avaya Equipment	Software / Firmware Version
Avaya Aura® System Manager running on a virtual server	System Manager 8.0.1.1 Build No. – 8.0.0.0.931077 Software Update Revision No: 8.0.11.039340 Service Pack 1
Avaya Aura® Session Manager running on a virtual server	Session Manager R8.0.1 Build No. – 8.0.1.1.801103
Avaya Aura® Communication Manager running on a virtual server	R8.0.1.1.0 – FP1SP1 R018x.00.0.822.0 Update ID 00.0.822.0-25183
Avaya Aura® Messaging running on a virtual server	7.0 SP0
Avaya Media Gateway G450	40.20.0 /2
Avaya Aura® Media Server	Appliance Version R8.0.0.6 Media Server 8.0.0.150 Element Manager 8.0.0.150
Avaya 96x1 H323 Deskphone	6.6604
Avaya 96x1 SIP Deskphone	7.1.2.0.14
Avaya J179 H323 Deskphone	6.7.002U
Avaya J129 SIP Deskphone	1.0.0.0.0.43
Avaya Equinox running on Vantage	3.4.8.36
Avaya 9408 Digital Deskphone	2.0
Ascom Equipment	**Software / Firmware Version**
Ascom Device Manager running on Unite Connectivity Manager	Unite DM/CM v5.11.2
Ascom Myco Smartphone	Myco 1 & 2, v15.0.0 (SIP App v2.2)
Ascom approved Wi-Fi Access Point	Ascom approved software version

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 groups 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

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: 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
```

5.2. 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
   21          4   ext
   3           4   udp
   8           1   fac
   9           1   fac
   *8          4   dac
   *           3   fac
   #           3   fac
```

5.3. Configure Feature Access Codes

Use the **change feature-access-codes** command to configure access codes which can be entered from Myco 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 the **change ip-network-region x** (where x is the network region to be configured) command to assign an appropriate domain name to be used by Communication Manager, in the example below **devconnect.local** is used. Note this domain is also configured in **Section 6.1.1**.

```
change ip-network-region 1                                  Page   1 of  20
                               IP NETWORK REGION
  Region: 1
Location: 1       Authoritative Domain: devconnect.local
    Name: default NR
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: yes
      Codec Set: 1              Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 2048                      IP Audio Hairpinning? y
   UDP Port Max: 3329
DIFFSERV/TOS PARAMETERS
 Call Control PHB Value: 46
        Audio PHB Value: 46
        Video PHB Value: 26
802.1P/Q PARAMETERS
 Call Control 802.1p Priority: 6
        Audio 802.1p Priority: 6
        Video 802.1p Priority: 5      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                       RSVP Enabled? n
  H.323 Link Bounce Recovery? y
 Idle Traffic Interval (sec): 20
   Keep-Alive Interval (sec): 5
            Keep-Alive Count: 5
```

5.5. Configure IP-Codec

Use the **change ip-codec-set x** (where x is the ip-codec set used) command to designate a codec set compatible with the Myco Handsets. During compliance testing the codecs **G.711A**, **G.729A** and **G.722–64K** 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.711A            n         2        20
 2: G.729A            n         2        20
 3: G.722.2           n         1        20
 4: G.722-64K                   2        20
 5: G.723-5.3K        n         1        30
 6:
     Media Encryption                   Encrypted SRTCP: enforce-unenc-srtcp
 1: 1-srtp-aescm128-hmac80
 2: none
 3:
```

5.6. Configuration of Coverage Path and Hunt Group for voicemail

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

Don't' Answer is set to **y:**	The coverage path will be used in the event the phone set is not answered.
Number of Rings is set to **4:**	The coverage path will be used after 4 rings.
Point 1 is set to **h6**	Hunt Group 6 is utilised by this coverage path.

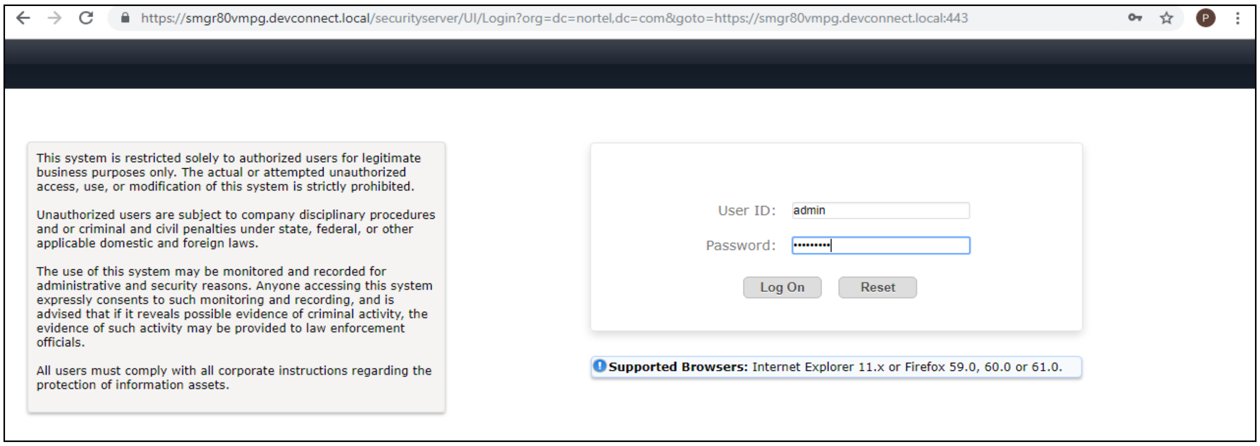
```
display coverage path 1
                                 COVERAGE PATH

                   Coverage Path Number: 1
     Cvg Enabled for VDN Route-To Party? n        Hunt after Coverage? n
                       Next Path Number:          Linkage

COVERAGE CRITERIA
    Station/Group Status    Inside Call     Outside Call
             Active?             n               n
               Busy?             y               y
       Don't Answer?             y               y        Number of Rings: 4
                All?             n               n
 DND/SAC/Goto Cover?             y               y
   Holiday Coverage?             n               n


COVERAGE POINTS
    Terminate to Coverage Pts. with Bridged Appearances? n
  Point1: h6              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 **6666**, which is used to dial for messaging and **Group Type** is set to **ucd-mia**.

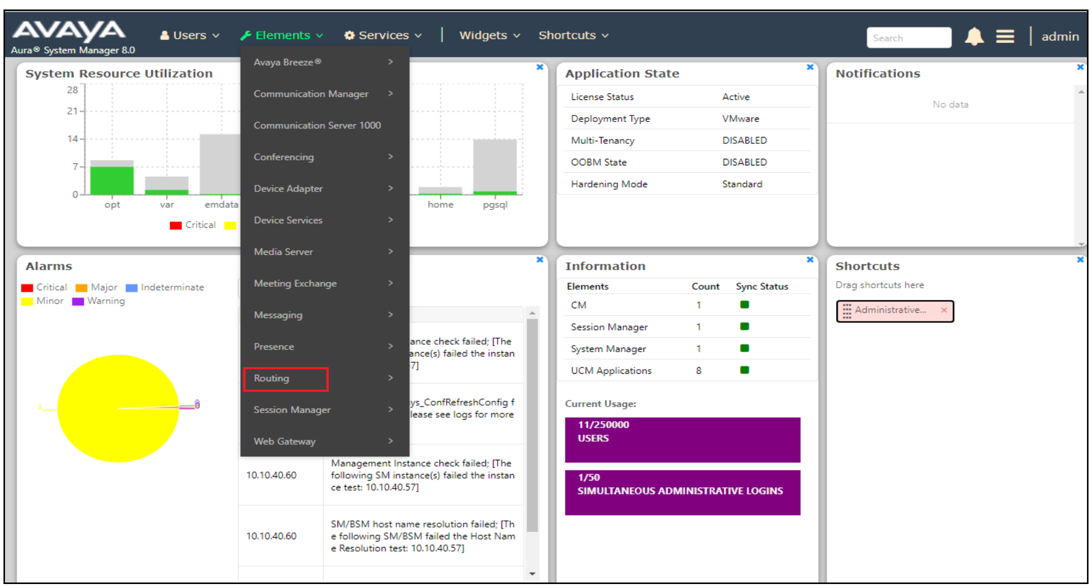
```
display hunt-group 6                                            Page   1 of  60
                                  HUNT GROUP

            Group Number: 6                                 ACD? n
              Group Name: AA Messaging V7                 Queue? n
         Group Extension: 6666                           Vector? n
              Group Type: ucd-mia                 Coverage Path: 1
                      TN: 1          Night Service Destination:
                     COR: 1                     MM Early Answer? n
           Security Code:                Local Agent Preference? n
 ISDN/SIP Caller Display: mbr-name






SIP URI::
```

6. Configure Avaya Aura® Session Manager

The Ascom Myco 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.



Once logged in navigate to **Elements** and click on **Routing** highlighted below.

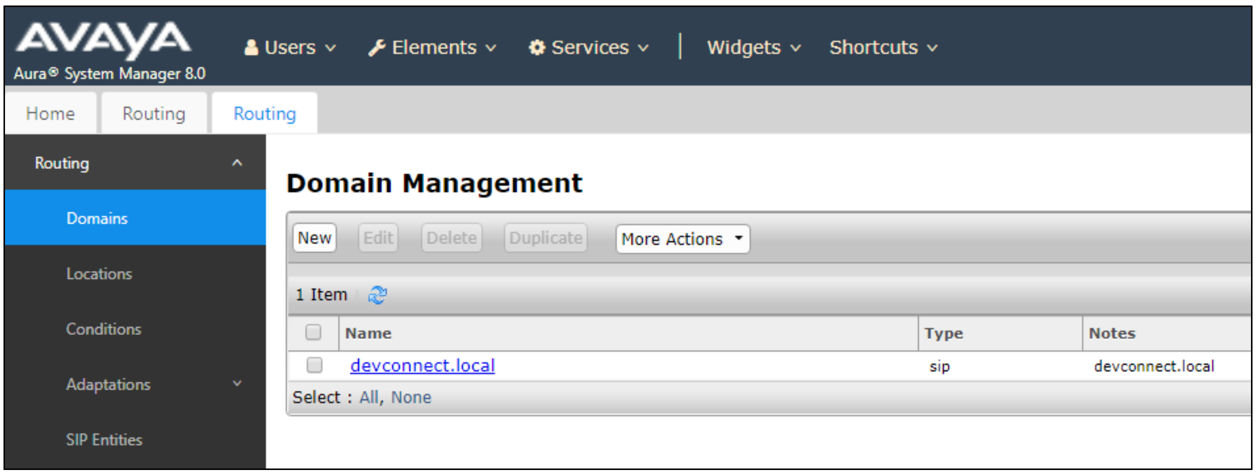


6.1. Domains and Locations

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.

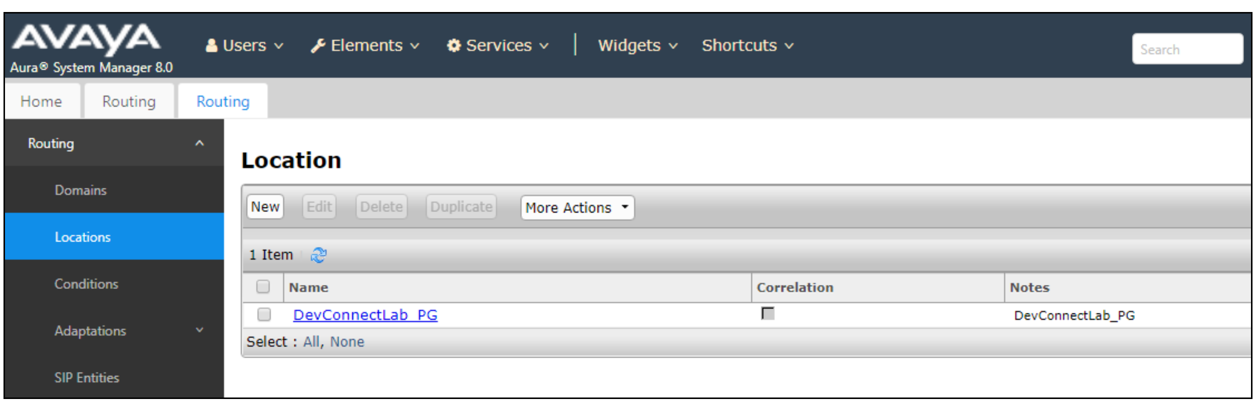
6.1.1. Display the Domain

Select **Domains** from the left window. This will display the domain configured on Session Manager. For compliance testing this domain was **devconnect.local** 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.



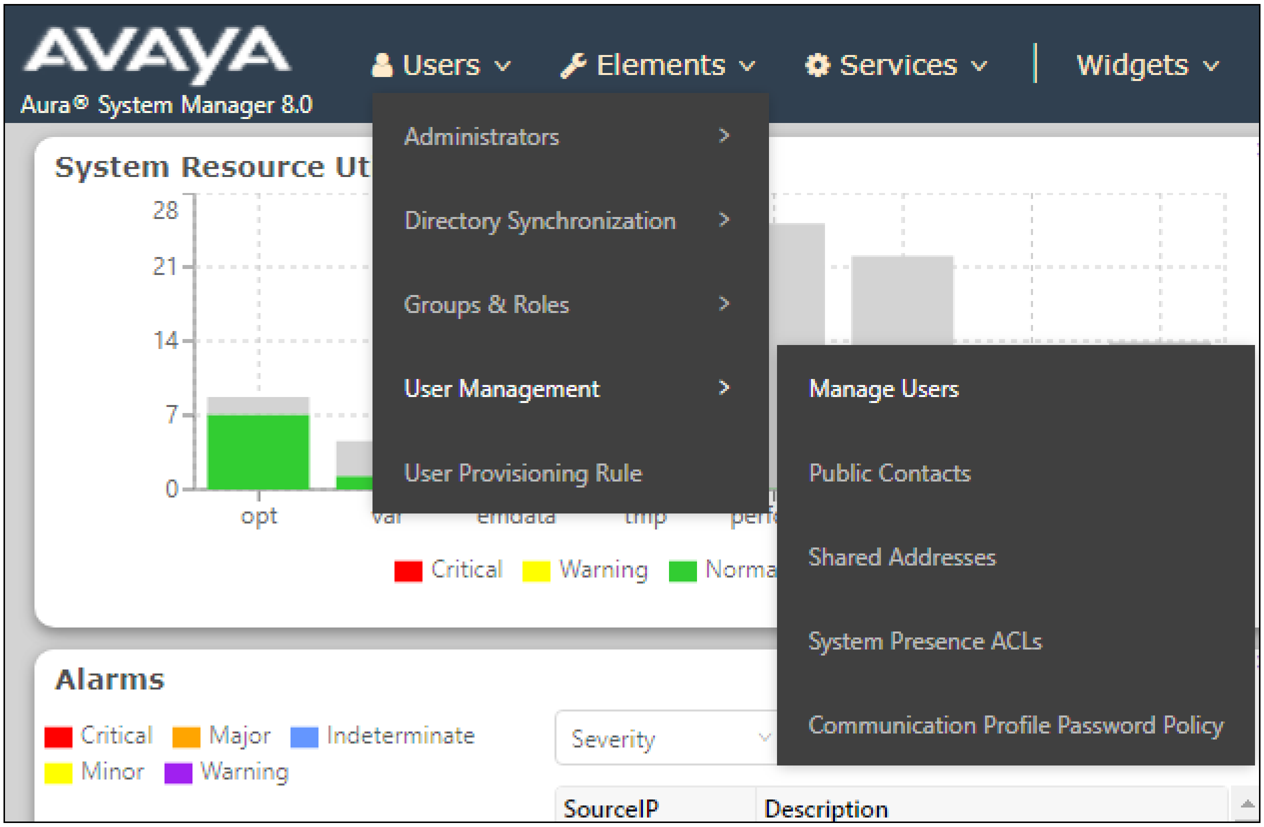
6.1.2. Display the Location

Select **Locations** from the left window and this will display the location setup. The example below shows the location **DevConnectLab_PG** 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.

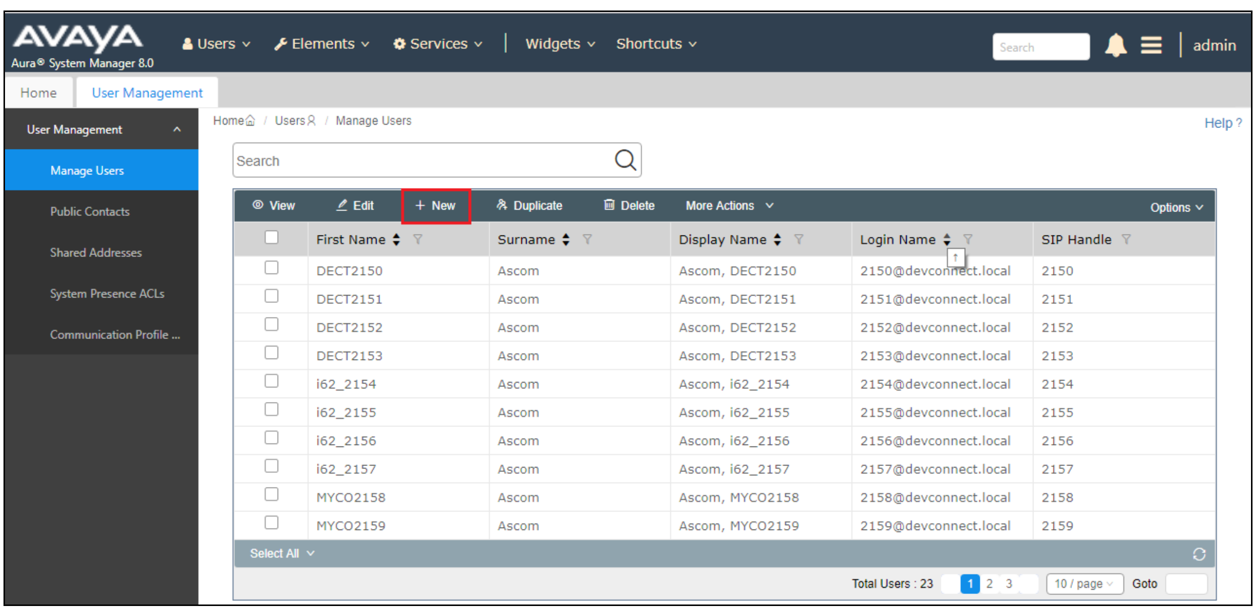


6.2. Adding Ascom Myco SIP User

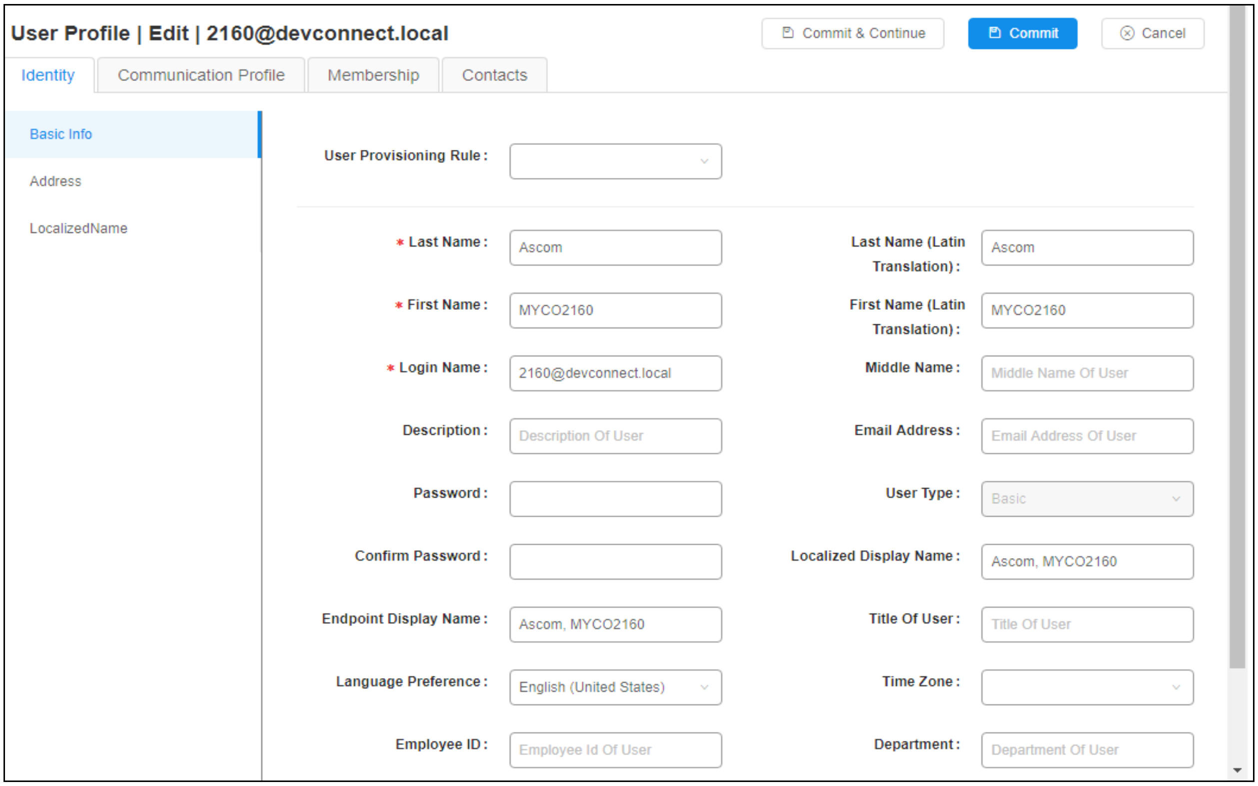
From the home page, click on **User Management → Manager Users** shown below.



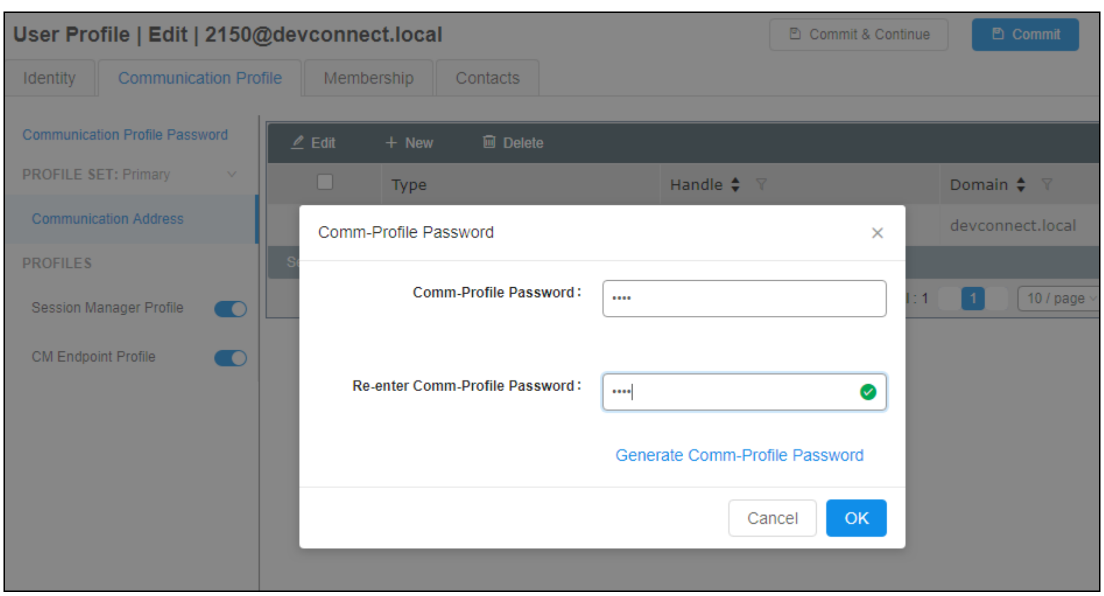
From **Manager Users** section, click on **New** to add a new SIP user.



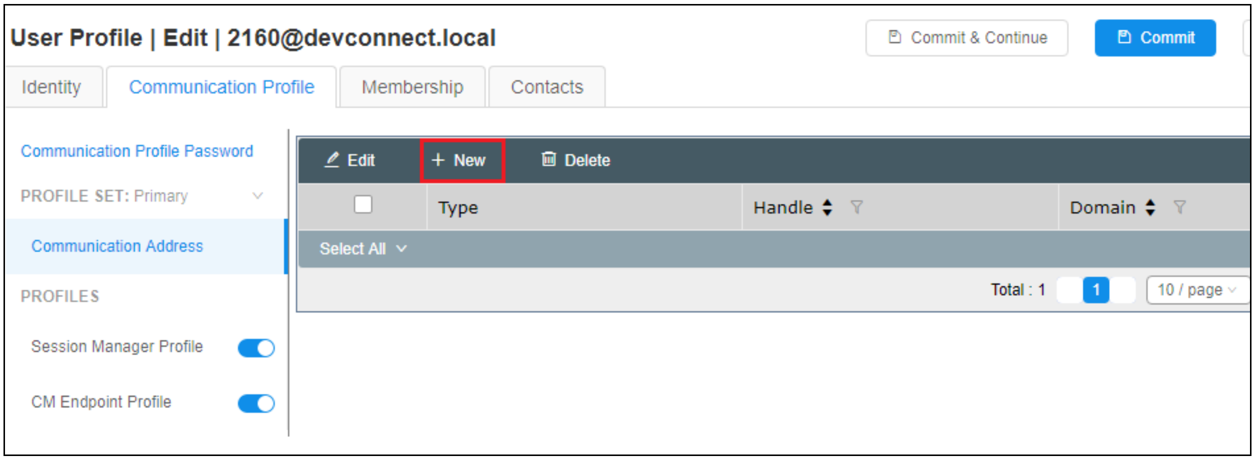
Under the **Identity** tab fill in the user's desired **Last Name** and **First Name** as shown below. Enter the **Login Name** following the format of "user id@domain". The remaining fields can be left as default.



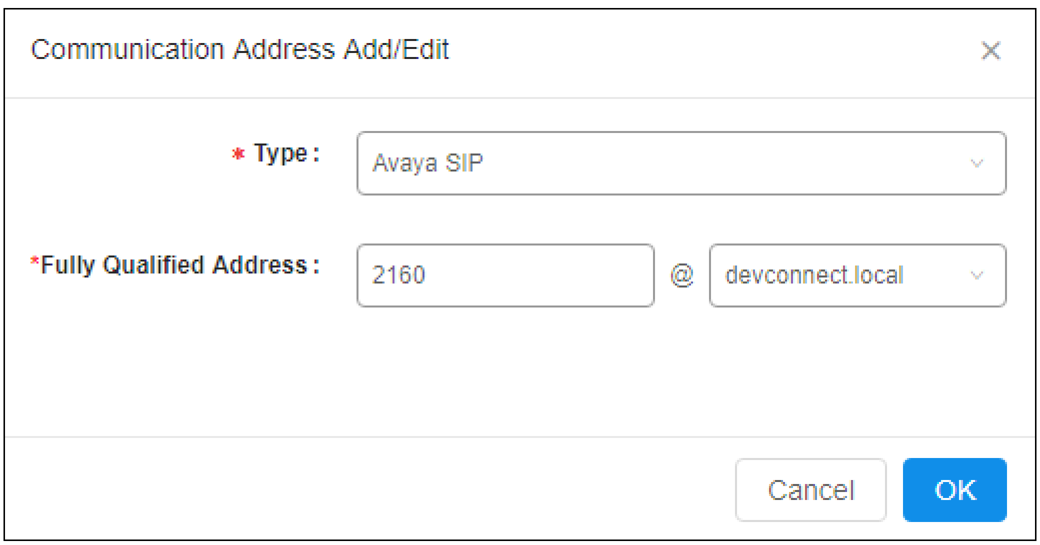
Under the **Communication Profile** tab, enter the **Communication Profile Password** and **Confirm Password**, note that this password is required when configuring the Myco handset in **Section 7.1**.



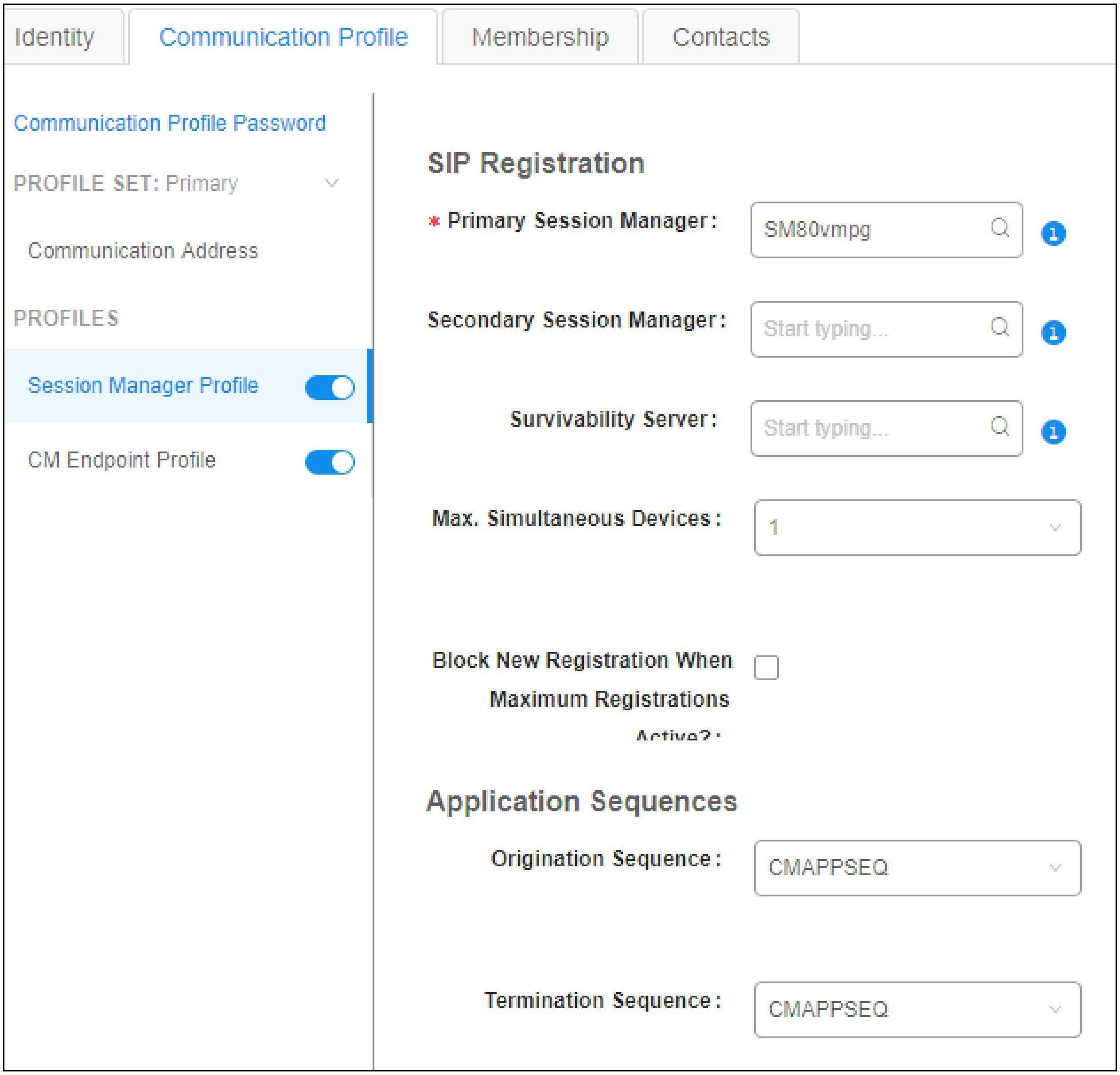
Staying on the **Communication Profile** tab, click on **New** to add a new **Communication Address**.



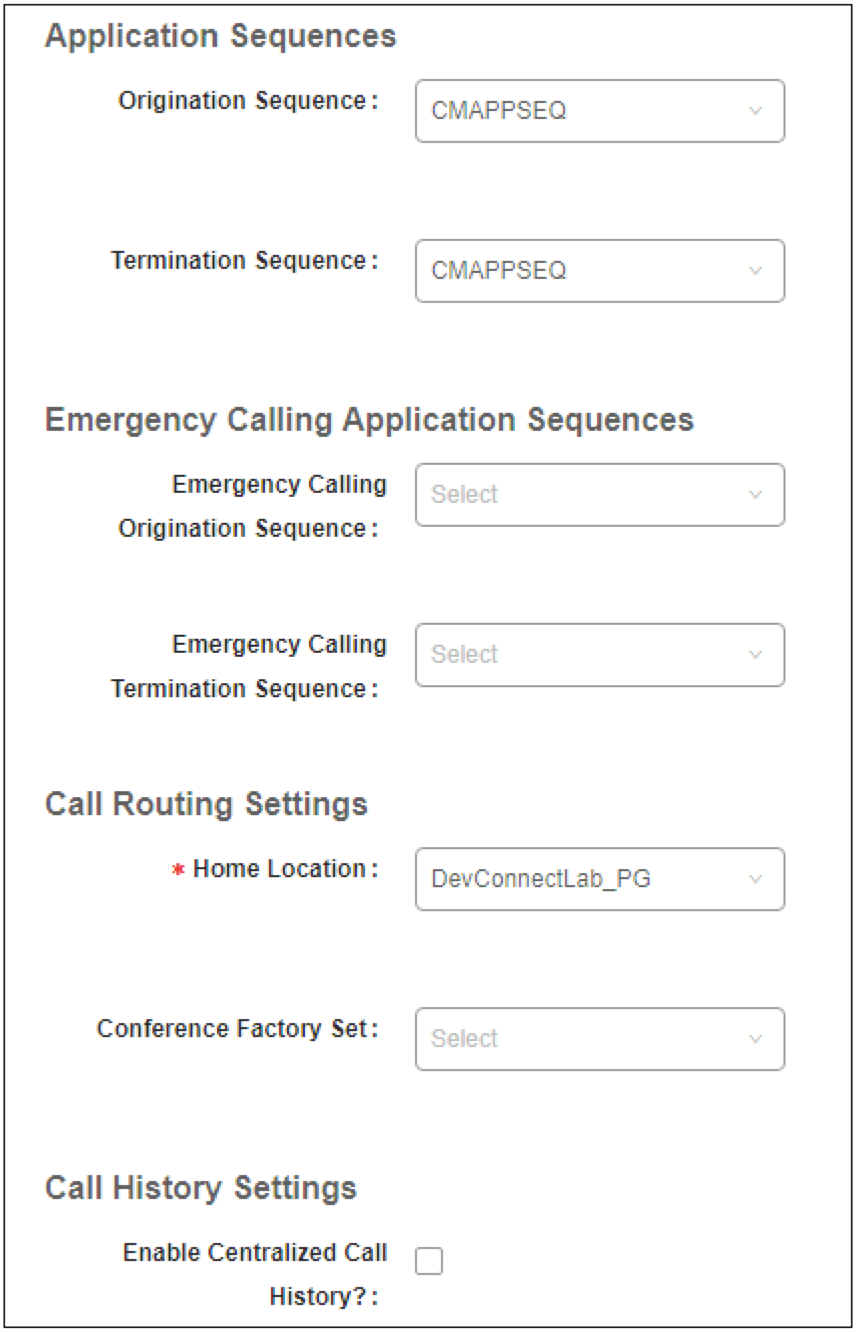
Enter the extension number and the domain for the **Fully Qualified Address** and click on **OK** once finished.



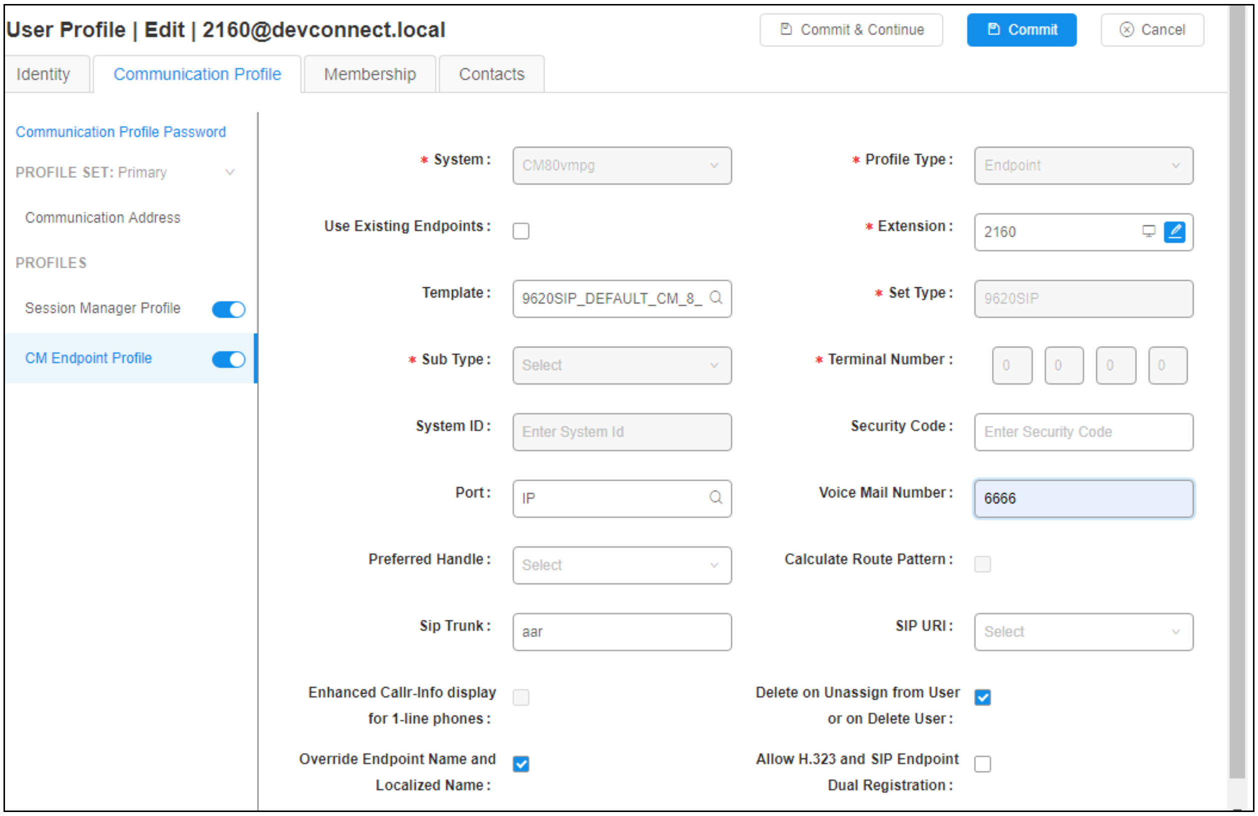
Ensure **Session Manager Profile** is checked and enter the **Primary Session Manager** details, enter the **Origination Sequence** and the **Termination Sequence**. Scroll down to complete the profile.



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).

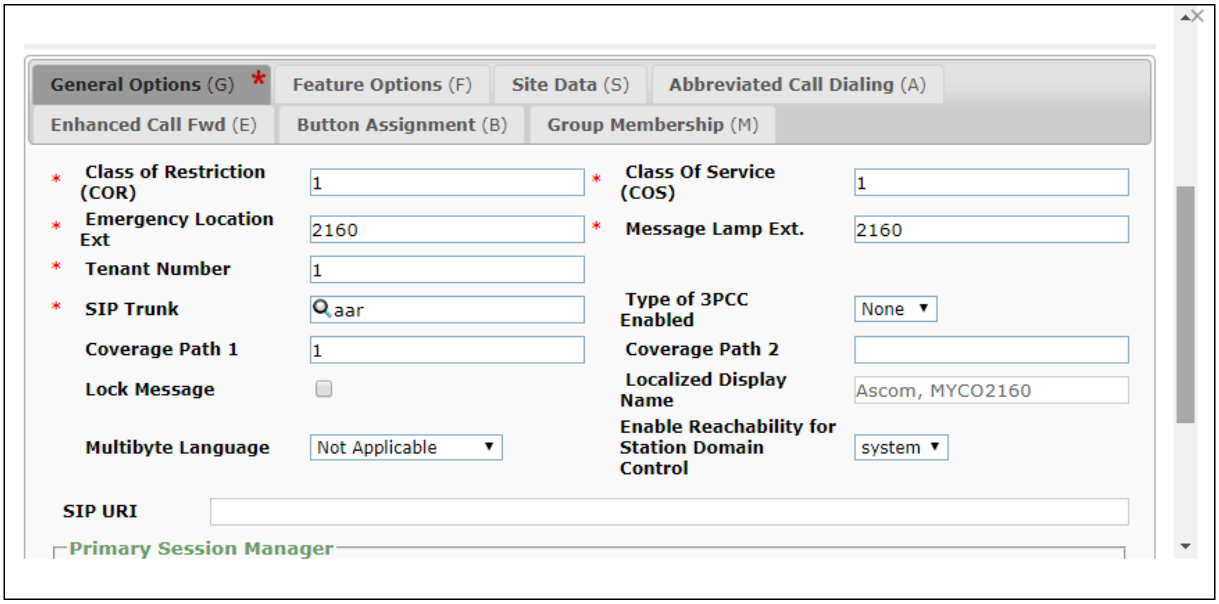


Ensure that **CM Endpoint Profile** is selected in the left window. Select the Communication Manager that is configured for the **System** and choose the **9620SIP_DEFAULT_CM_8_0** as the **Template**. Enter the appropriate **Voice Mail Number** and **Sip Trunk** should be set to **aar**, providing that 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 Myco handset. Click on **Endpoint Editor** to configure the buttons and features for that handset on Communication Manager.

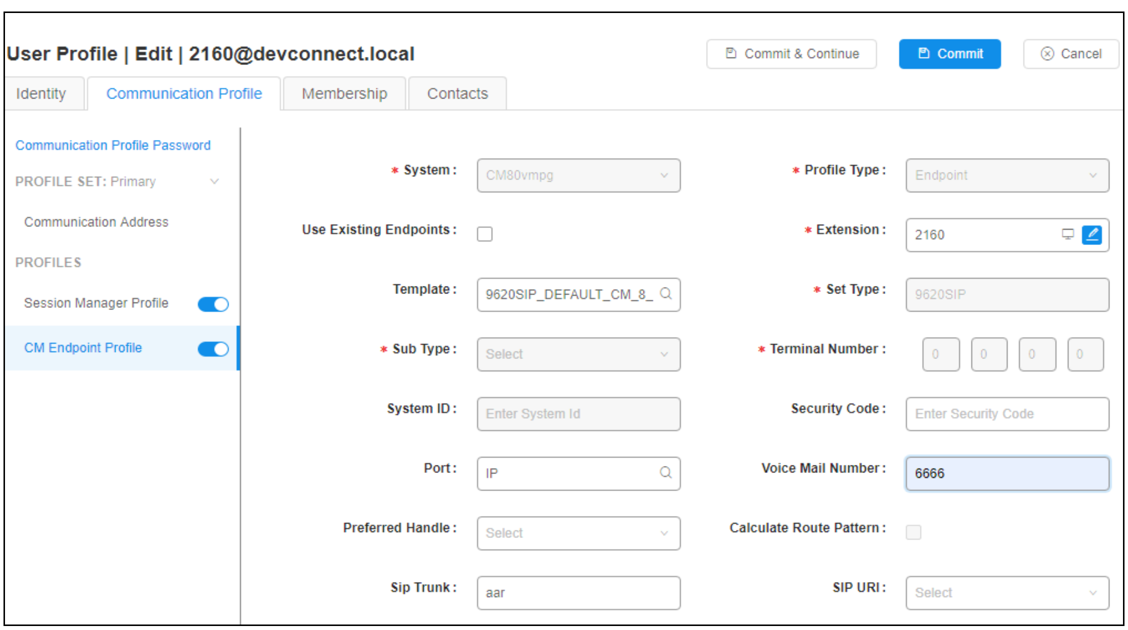


Under the **General Options** tab ensure that **Coverage Path 1** is set to that configured in **Section 5.6**. Also ensure that **Message Lamp Ext.** is showing the correct extension number. The **Class of Restriction** and **Class of Service** should be set to the appropriate values for the Myco handset. 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.

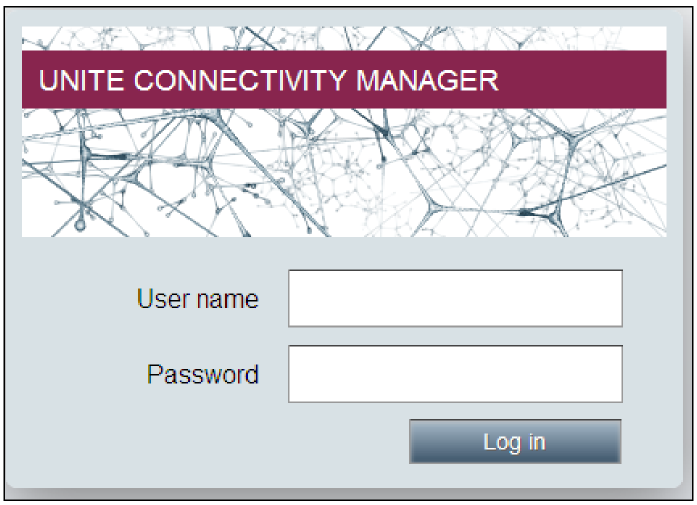


7. Configure Ascom Myco Smartphone

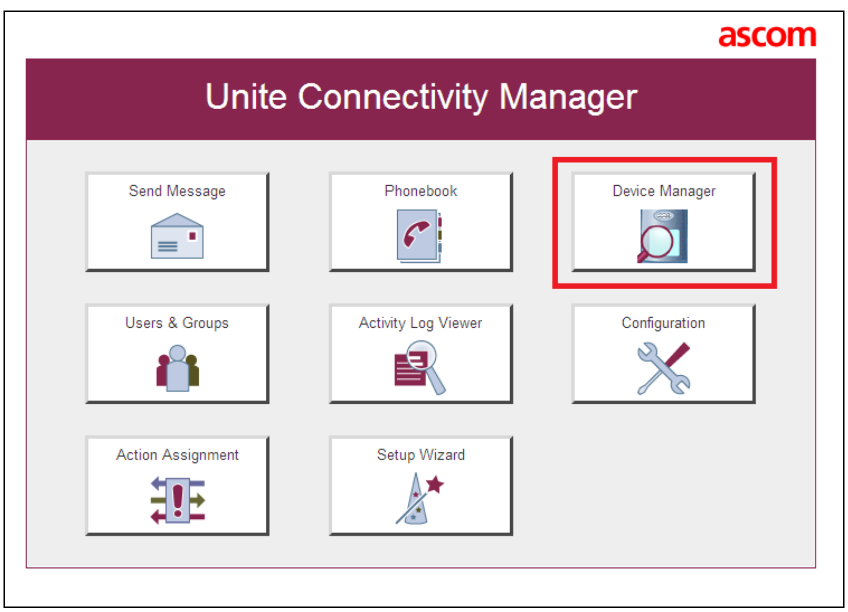
This section describes how to access and configure Myco via the Device Manager. It is implied that the Wi-Fi network has been configured and operational and the Ascom UniteCM box has an IP address assigned.

Note: The Wireless router configuration is outside the scope of these Application Notes.

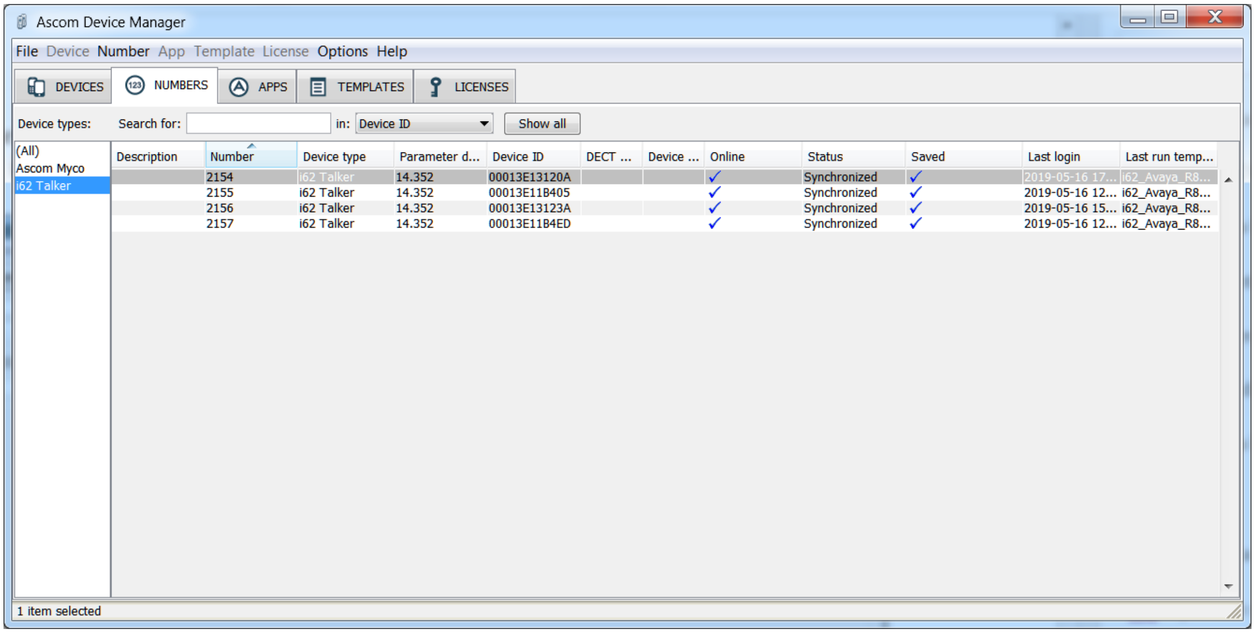
Access the UniteCM box by typing the URL, http://<ip address> in a web browser (not shown). Screen below shows the login screen. Enter the required credentials in the **User name** and **Password** fields and click on **Log in**.



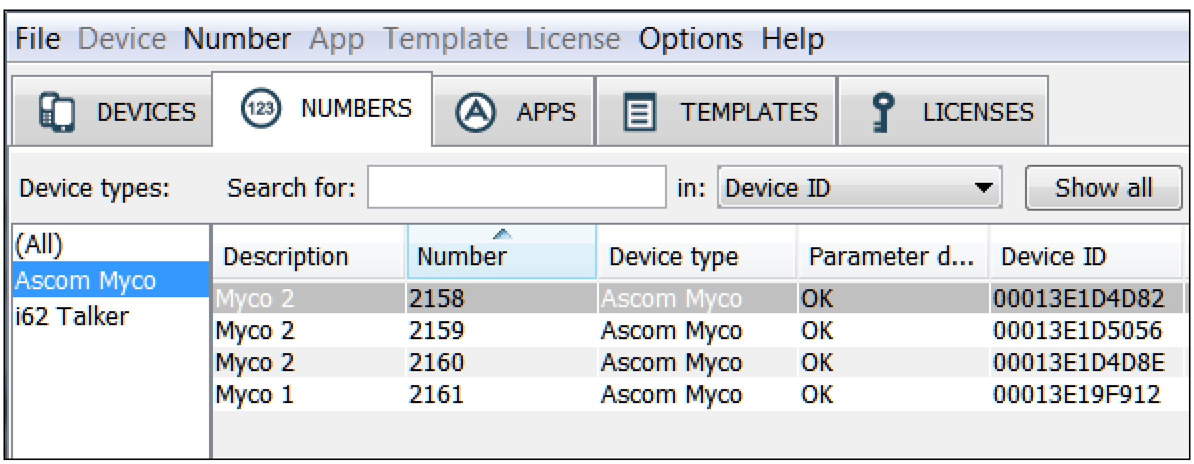
The main screen of **Unite Connectivity Manager** is seen as shown below. Click on the **Device Manager** application.



The **Ascom Device Manager** screen is seen as shown below. In the example below, a device with number **4151** is discovered. Double click on this number.



A close up of the same screen shown above shows that **2158** was selected.

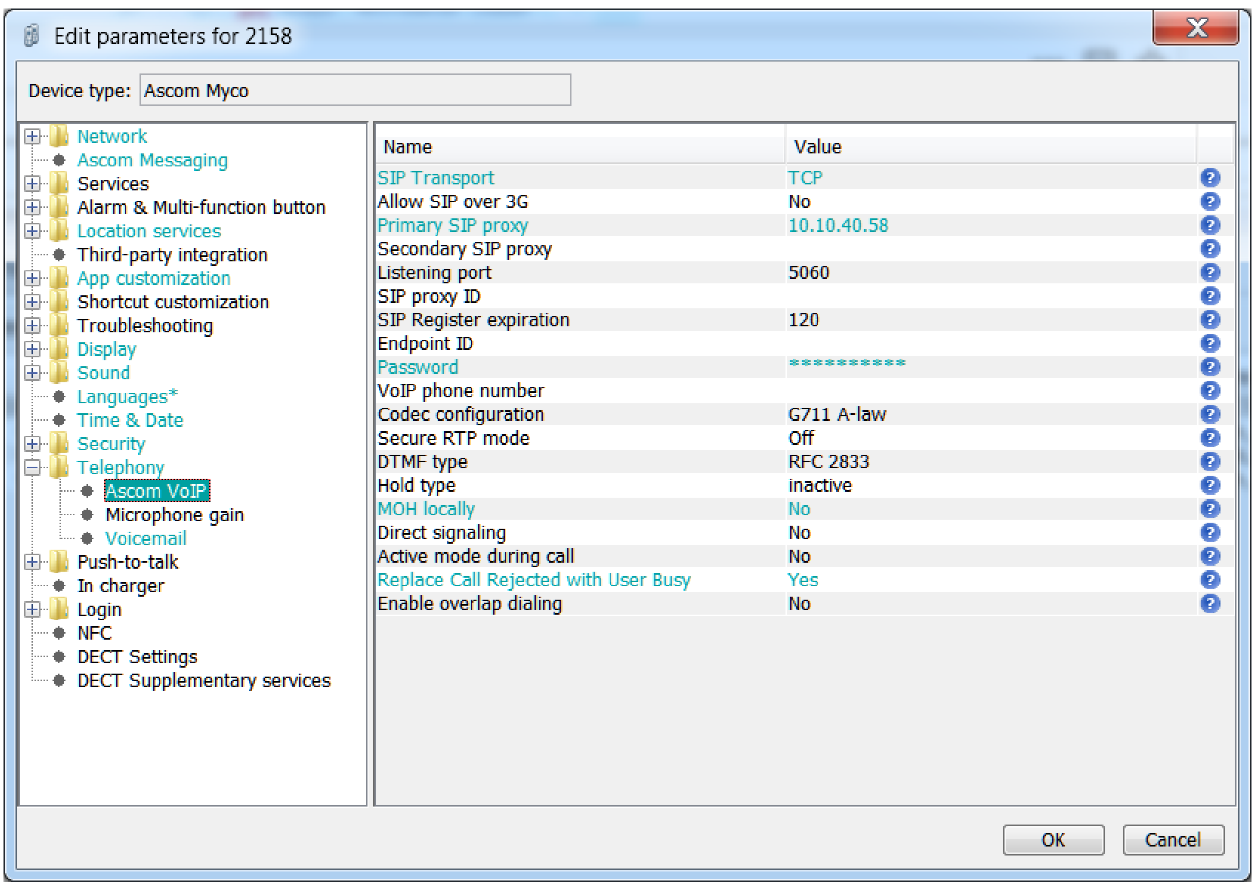


7.1. Configure SIP settings

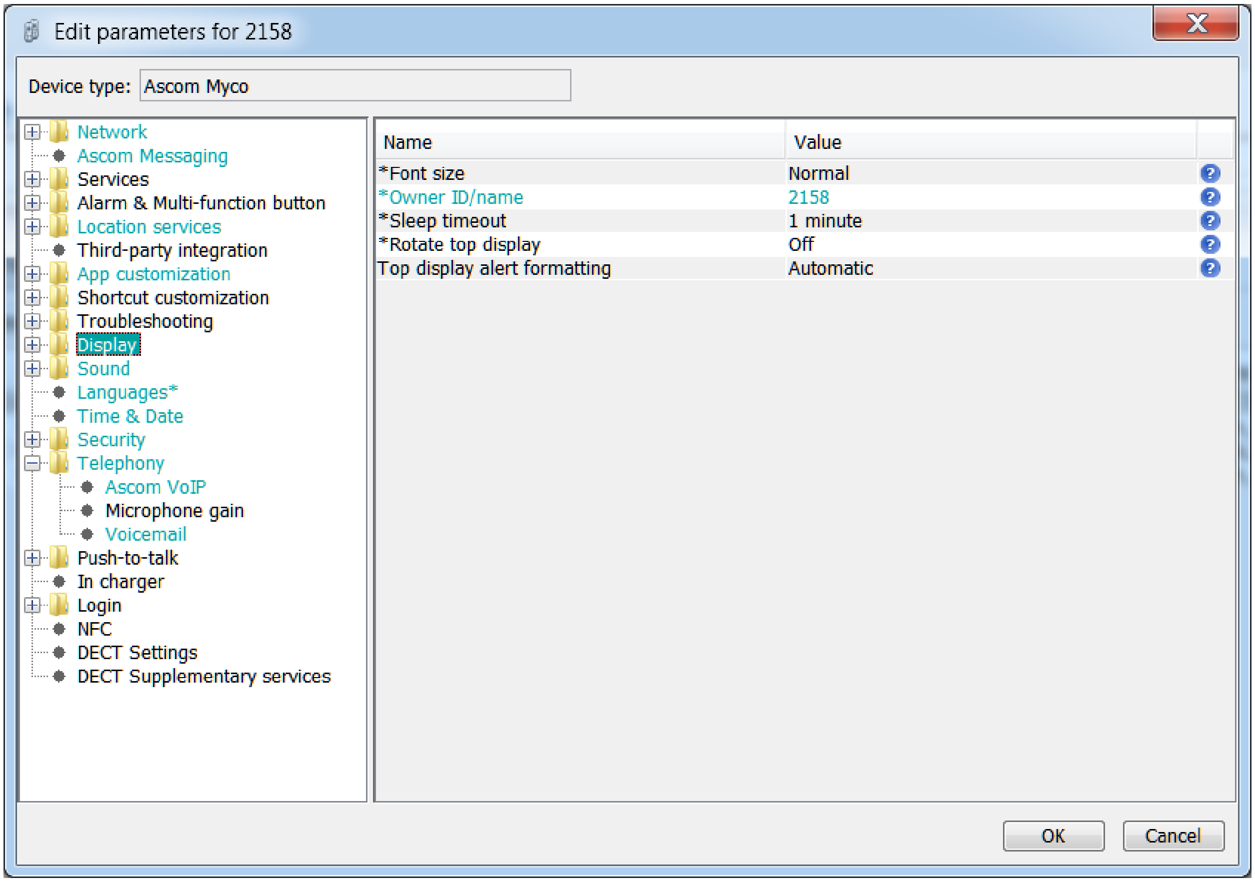
The **Edit parameters for 2158** screen are seen as shown below. Click on **Ascom VoIP** that is seen on the left-hand side and configure the following values.

- **SIP Transport** Set to either **TCP** or **UDP** (for compliance testing TCP was selected as shown below)
- **Primary SIP Proxy** IP address of Session Manager
- **Listening Port** **5060**
- **SIP Register Expiration** **120 (**was simply chosen to refresh every 2 mins)
- **Endpoint ID** This is the extension number
- **Password** Password assigned to the endpoint in **Section 6.2**
- **Codec configuration** This will depend on the country
- **DTMF Type** **RFC 2833** is chosen
- **Direct Signaling** This was left as **No** for compliance testing
- **Replace Call Rejected with User Busy:** This was set to **Yes** for compliance testing

Direct Signaling defines whether calls can be redirected to or accepted from other sources than the configured SIP Proxy. Retain default values for all other fields.

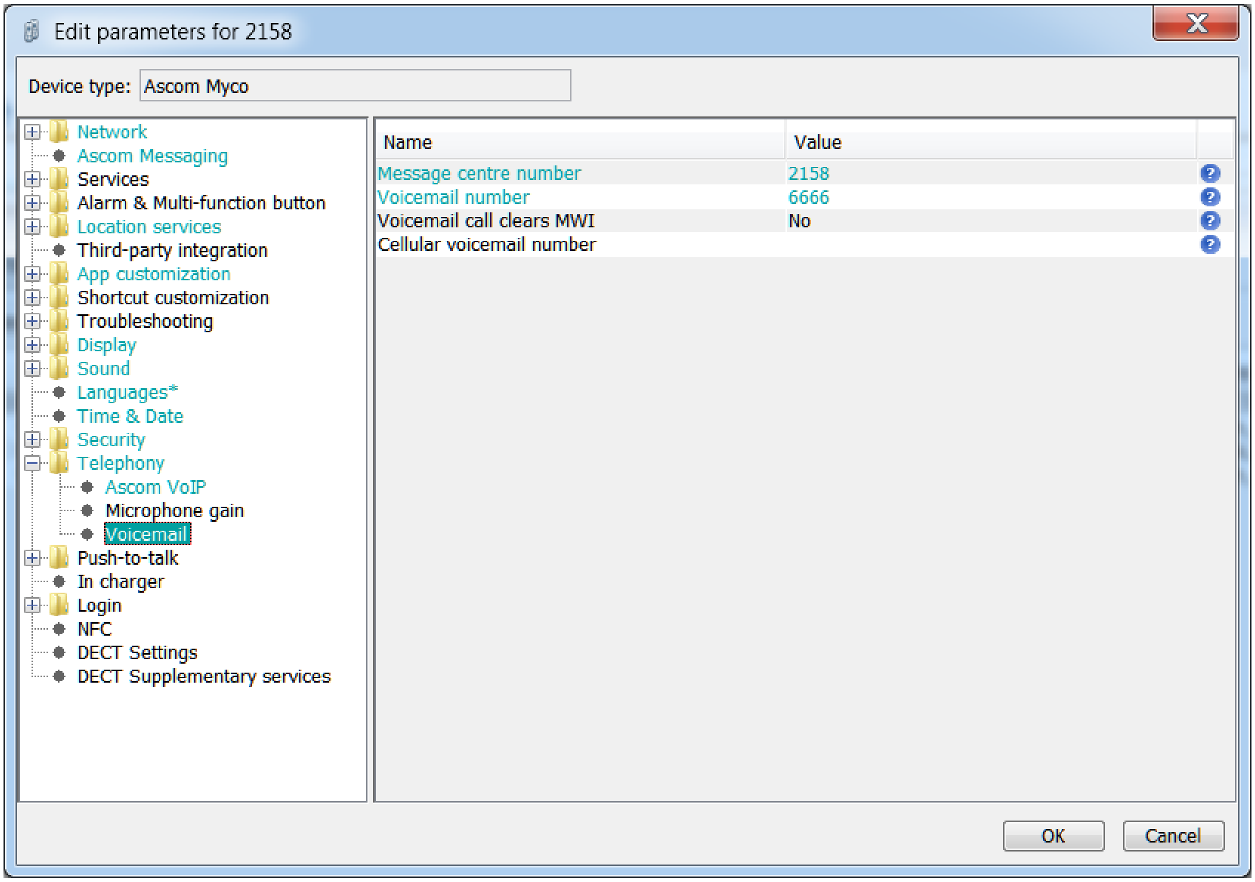


The following step is optional. This field will be displayed on the Myco screen. From the same screen as above, click on **Display** and configure the **Owner ID/name** field with the directory number configured, in this case **2158** as shown below. Retain default values for all other fields and click on **OK** to complete the configuration.



7.2. Configure Message Centre

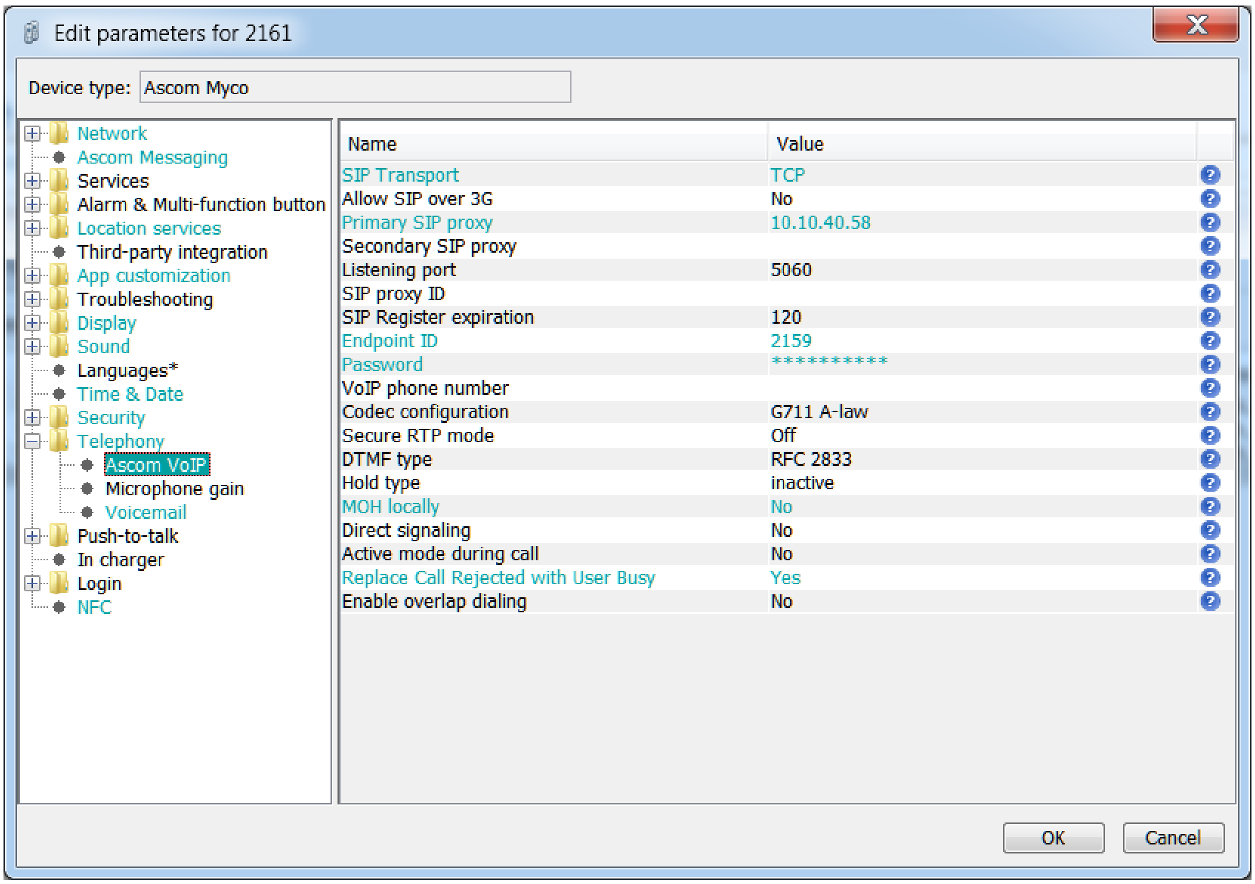
The messaging number can be set as shown below. **6666** is the number that all users dial to access voicemail and retrieve messages, this is the number set for **Voicemail number** below. The **Message centre number** should be set to the Endpoint ID of the extension in question, as in this case **2158**.



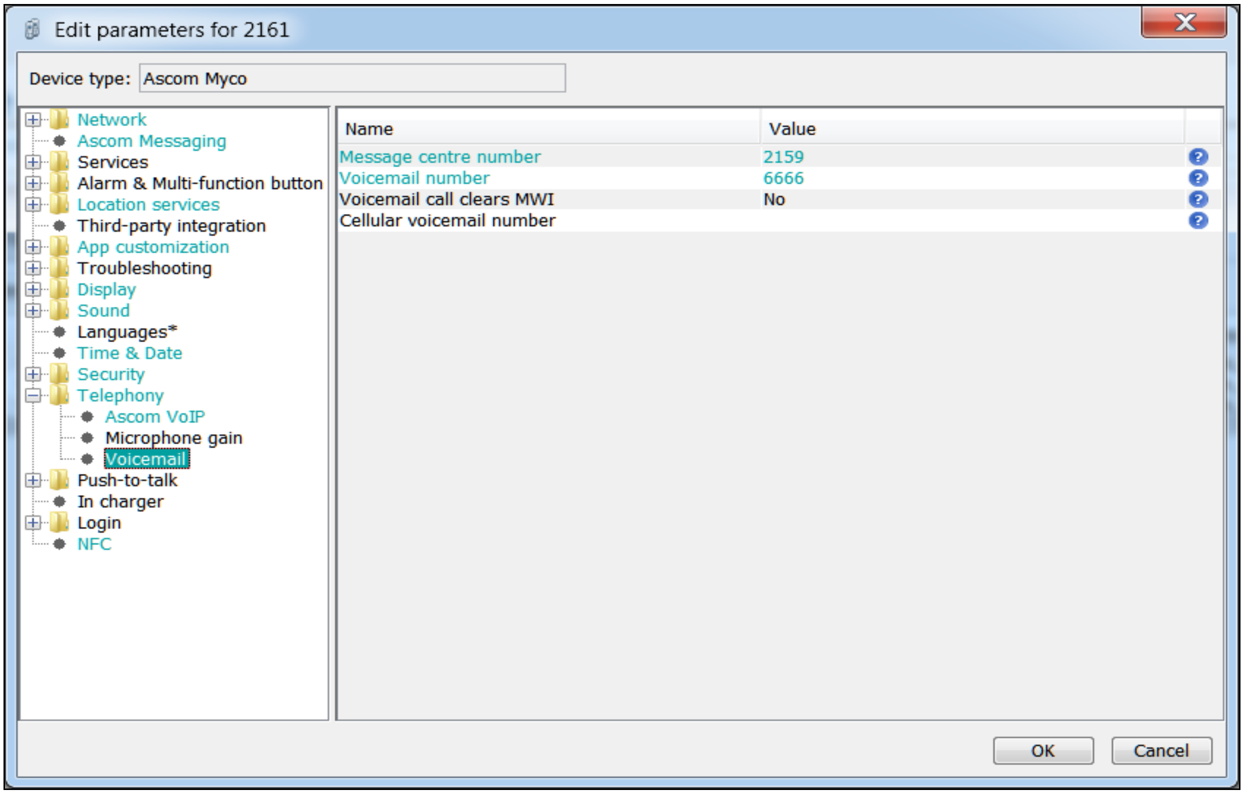
7.3. Configure Multi-Device Access

The MDA feature allows users to leverage multiple devices (endpoints) simultaneously to meet their communication needs. Users can send and receive calls at multiple devices and move calls between devices as needed.

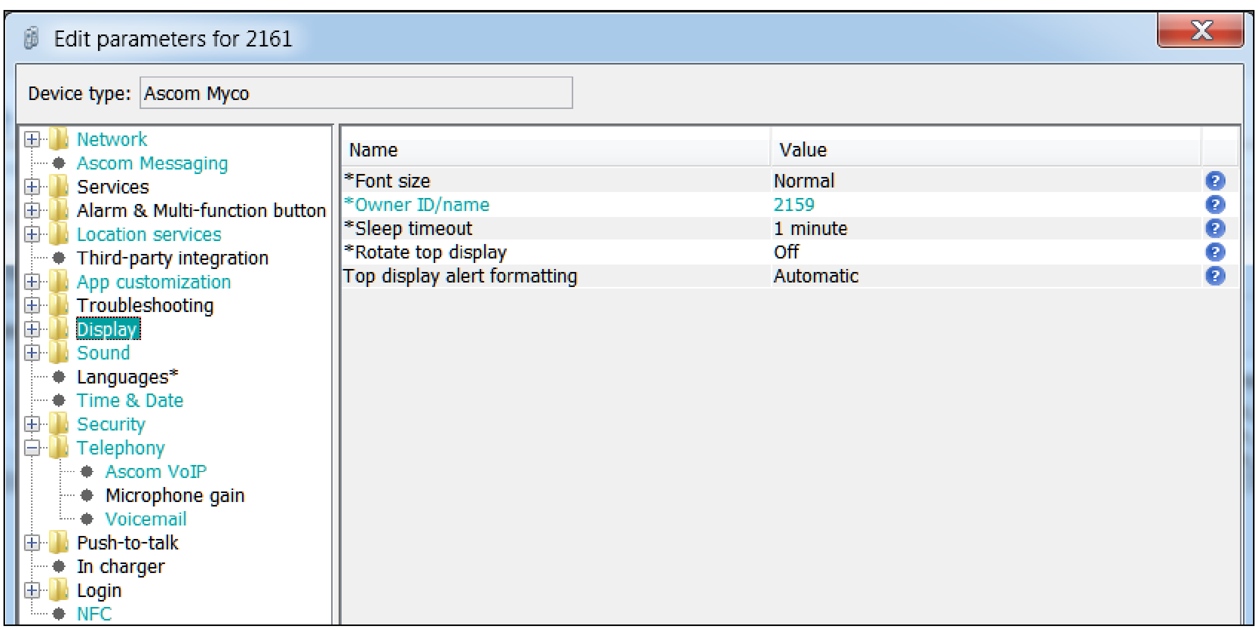
For the Myco smartphone, the MDA feature can be accomplished by configuring and registering the handset using the Endpoint ID parameter. In the example below, handset device with extension number 2161 is configured to register as user 2159. As shown in the screen below, **Endpoint number** is configured as **2161** however **Endpoint ID** is configured as **2159**.



For the **Message Centre number** instead of the extension number of the handset, configure the Endpoint ID which is **2159** in this case.



It is recommended that the **Owner ID/name** is updated to show the registered endpoint ID.

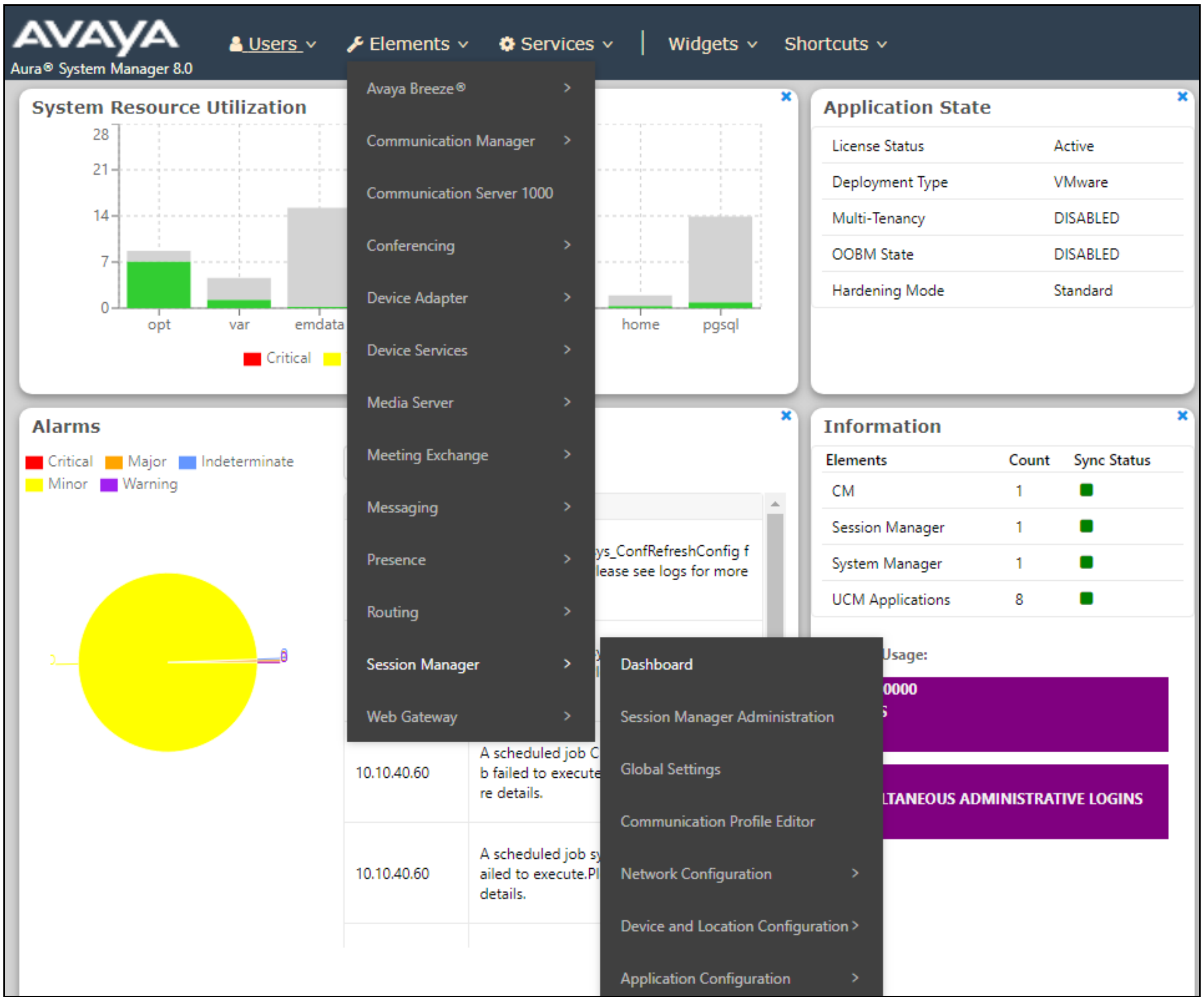


8. Verification Steps

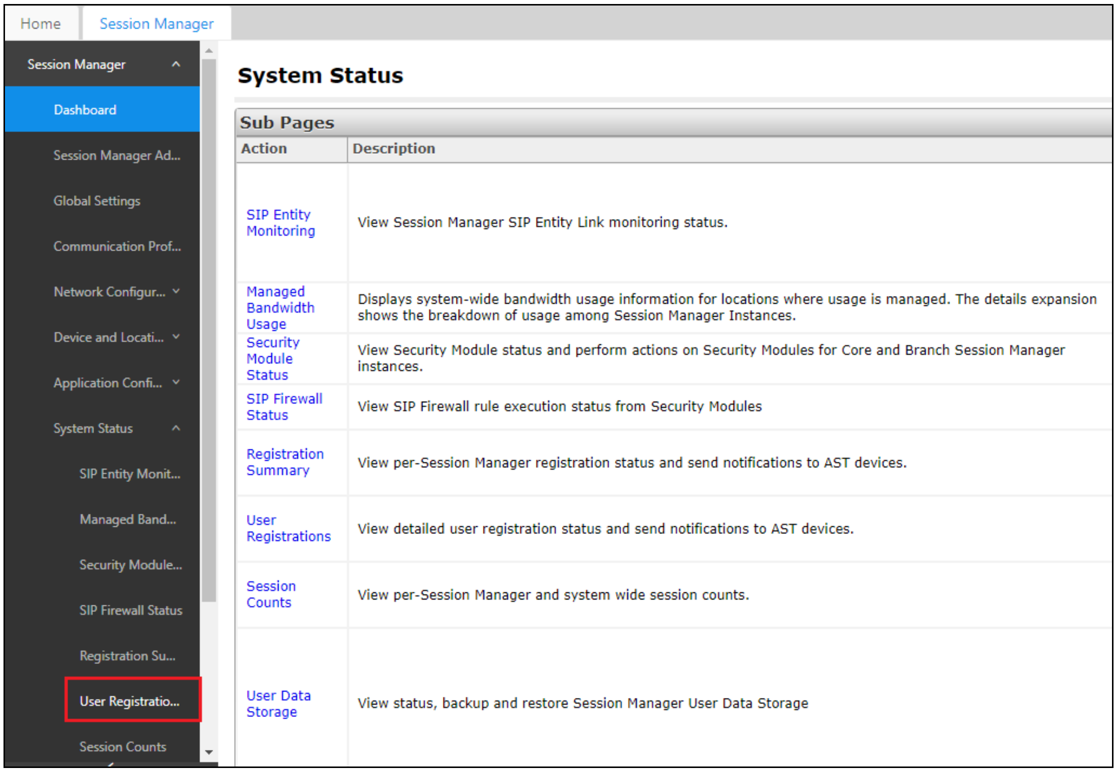
The following steps can be taken to ensure that connections between Myco and Session Manager and Communication Manager are up.

8.1. Session Manager Registration

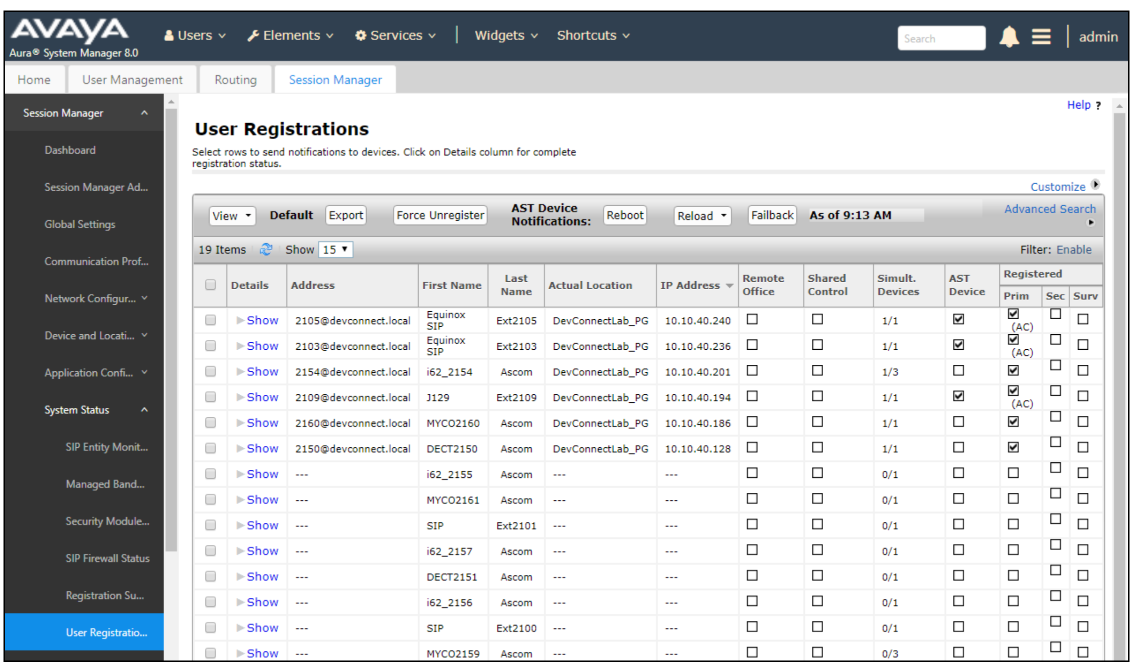
Log into System Manager as done previously in **Section 6**, select **Session Manager → Dashboard**.



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



The Myco users should show as being registered as shown below.

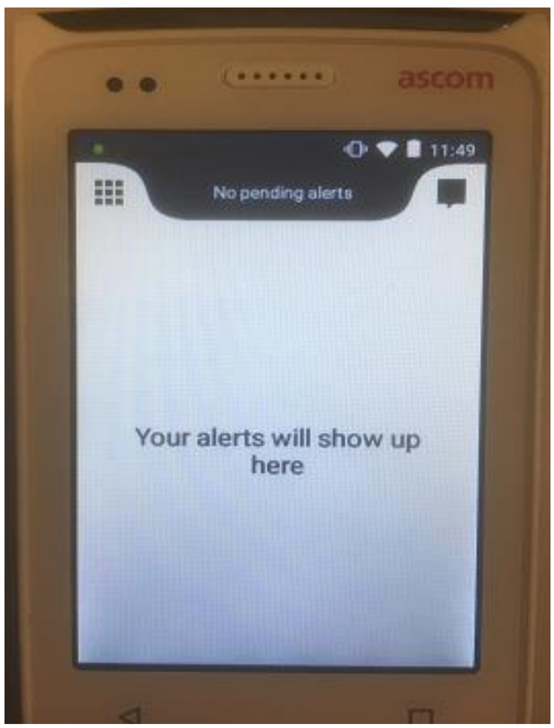


The Ascom Myco user should show as being registered as highlighted. It has an **IP Address** associated with it and there is a tick in the **Registered Prim** box.

☐	Details	Address	First Name	Last Name	Actual Location	IP Address	Remote Office	Shared Control	Simult. Devices	AST Device	Registered Prim	Registered Sec
☐	▶ Show	2105@devconnect.local	Equinox SIP	Ext2105	DevConnectLab_PG	10.10.40.240	☐	☐	1/1	☑	☑ (AC)	☐
☐	▶ Show	2103@devconnect.local	Equinox SIP	Ext2103	DevConnectLab_PG	10.10.40.236	☐	☐	1/1	☑	☑ (AC)	☐
☐	▶ Show	2154@devconnect.local	i62_2154	Ascom	DevConnectLab_PG	10.10.40.201	☐	☐	1/3	☐	☑	☐
☐	▶ Show	2109@devconnect.local	J129	Ext2109	DevConnectLab_PG	10.10.40.194	☐	☐	1/1	☑	☑ (AC)	☐
☐	▶ Show	2160@devconnect.local	MYCO2160	Ascom	DevConnectLab_PG	10.10.40.186	☐	☐	1/1	☐	☑	☐
☐	▶ Show	2150@devconnect.local	DECT2150	Ascom	DevConnectLab_PG	10.10.40.128	☐	☐	1/1	☐	☑	☐
☐	▶ Show	---	i62_2155	Ascom	---	---	☐	☐	0/1	☐	☐	☐

8.2. Ascom Myco Registration

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



9. Conclusion

These Application Notes describe the configuration steps required for Ascom Myco2 to successfully interoperate with Avaya Aura® Communication Manager R8.0.1 and Avaya Aura® Session Manager R8.0.1 by registering Myco with Avaya Aura® Session Manager as a third-party SIP phone. Please refer to **Section 2.2** for test results and observations.

10. Additional References

This section references documentation relevant to these Application Notes. The Avaya product documentation is available at http://support.avaya.com where the following documents can be obtained.

1. *Deploying Avaya Aura® Communication Manager*, Release 8.0
2. *Avaya Aura® Communication Manager Feature Description and Implementation*, Release 8.0
3. *Deploying Avaya Aura® Session Manager*, Release 8.0
4. *Administering Avaya Aura® Session Manager*, Release 8.0
5. *Deploying Avaya Aura® System Manager*, Release 8.0
6. *Administering Avaya Aura® System Manager for Release 8.0*, Release 8.0
7. *Deploying Avaya Aura® Messaging using VMware® in the Virtualized Environment*, Release 7.0.0
8. *Administering Avaya Aura® Messaging*, Release 7.0.0

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 required).

Appendix

Signaling Group

```
display signaling-group 1                                       Page   1 of   3
                                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? 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: SM80vmpg
 Near-end Listen Port: 5061                Far-end Listen Port: 5061
                                        Far-end Network Region: 1

Far-end Domain:
                                             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 1                                           Page   1 of   5
                                TRUNK GROUP

Group Number: 1                   Group Type: sip           CDR Reports: y
  Group Name: SIPTRUNK-SM80              COR: 1        TN: 1        TAC: *801
   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: 10
```

Page 2

```
display trunk-group 1                                                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 1                                                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

                                                 Hold/Unhold Notifications? y
                                Modify Tandem Calling Number: no
               Send UCID? y



 Show ANSWERED BY on Display? y

 DSN Term? n
```

Page 4

```
display trunk-group 1                                          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
```

Page 5

```
trunk-group 1                                                  Page   5 of   5
                              PROTOCOL VARIATIONS

                                       Mark Users as Phone? n
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
                        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
```

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.