



Avaya Solution & Interoperability Test Lab

Application Notes for configuring Ascom Myco V9.2 with Avaya Aura® Communication Manager R7.1 and Avaya Aura® Session Manager R7.1 – Issue 1.0

Abstract

These Application Notes describe the configuration steps for provisioning Ascom's Myco smart device 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 smart device (Ascom Myco) to interoperate with Avaya Aura® Communication Manager R7.1 and Avaya Aura® Session Manager R7.1. Ascom Myco is a smart device built for the on-the-job reality and the methods of working of 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 may be referred to as Myco, Myco handset or Myco smart device throughout this document. These names all refer to the same product, a smart phone 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 smart device 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 Ascom Myco smart device can be set up to use Wi-Fi, GSM or both. For compliance testing only Wi-Fi was used and a wireless router was used to provide a network connection. This wireless router was considered a part of the member'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, Ascom Myco handsets and PSTN endpoints.

- Registration
- Basic Calls
- Hold and Retrieve
- Attended and Blind Transfer
- 3 Party Conference
- Call Forwarding Unconditional, No Reply and Busy
- Call Waiting
- Feature calls (Call Park/Pickup)
- EC500
- Codec Support
- DTMF Support
- Message Waiting Indication (Voicemail)
- Serviceability Testing

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 was not included. All test cases passed successfully but there were some minor issues found surrounding the display on the endpoints and these are described below.

The following observations were noted during testing.

- **Direct Signaling** must be set to **Yes** on the Myco handsets when “Shuffling” is used on Communication Manager. Otherwise there may be issues with transfer. This setting can be found under Telephony → Ascom VoIP on the Device Manager, (see **Section 7**).

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.

The following issue was found 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 (MYCO-2395).

2.3. Support

Support from Avaya is available by visiting the website <http://support.avaya.com> and a list of product documentation can be found in **Section 11** of these Application Notes. Technical support for the Ascom 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 the wireless router which is placed on the LAN. Myco registers 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.

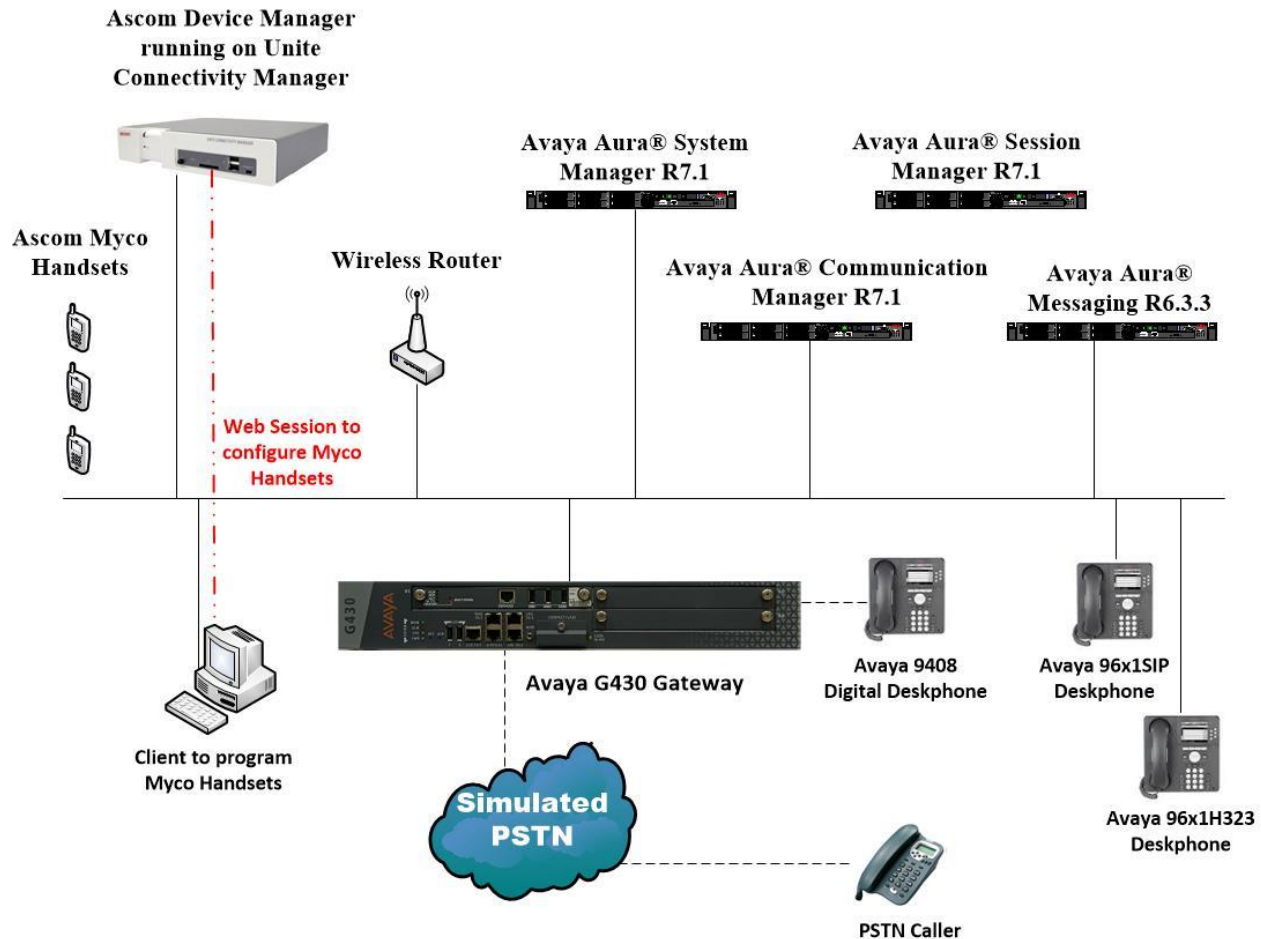


Figure 1: Network Solution of Ascom Myco Smart Device with Avaya Aura® Communication Manager R7.1 and Avaya Aura® Session Manager R7.1

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya Aura® System Manager running on a virtual server	System Manager 7.1.1.0 Build No. - 7.1.0.0.1125193 Software Update Revision No: 7.1.1.0.046931 Feature Pack 1 Service Pack 1
Avaya Aura® Session Manager running on a virtual server	Session Manager R7.1 SP1 Build No. – 7.1.1.0.711008
Avaya Aura® Communication Manager running on Virtual Server	R017x.01.0.532.0 R7.1.1.0.0 - FP1 Update ID 01.0.532.0-23985
Avaya Aura® Messaging running on Virtual Server	R6.3.3
Avaya Aura® Media Server running on Virtual Server	R7.8
Avaya G430 Gateway	37.42.0 /1
Avaya 96x1 H323 Deskphone	96x1 H323 Release 6.6401
Avaya 96x1 SIP Deskphone	96x1 SIP Release 7.1.0.1.1
Avaya 9408 Digital Deskphone	V2
Ascom Device Manager running on Unite Connectivity Manager	Unite DM/CM v5.8.1
Ascom Myco Smart Device	Ascom Myco 1 & 2, v9.2 (SIP App v2.1)

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.

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.

- Dial Plan Analysis
- Feature Access Codes
- Network Region
- IP Codec

5.1. Configure Dial Plan Analysis

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

change dialplan analysis			DIAL PLAN ANALYSIS TABLE			Page 1 of 12		
			Location: all			Percent Full: 1		
Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type
2	4	udp						
3	4	udp						
4	4	ext						
5	4	udp						
5999	4	ext						
6	4	udp						
7	4	udp						
8	1	fac						
9	1	fac						
*	3	fac						
*8	4	dac						
#	3	fac						

5.2. Configure Feature Access Codes

Use the **change feature-access-codes** command to configure access codes which can be entered from Ascom handsets to initiate Communication Manager call features. These access codes must be compatible with the dial plan described in **Section 5.1**. The following access codes need to be setup.

- **Answer Back Access Code** : **#21**
- **Auto Alternate Routing (AAR) Access Code** : **8**
- **Auto Route Selection (ARS) - Access Code 1** : **9**
- **Call Park Access Code** : **#20**

change feature-access-codes		Page 1 of 10
FEATURE ACCESS CODE (FAC)		
Abbreviated Dialing List1 Access Code:		
Abbreviated Dialing List2 Access Code:		
Abbreviated Dialing List3 Access Code:		
Abbreviated Dial - Prgm Group List Access Code:		
Announcement Access Code:		
Answer Back Access Code: #21		
Attendant Access Code:		
Auto Alternate Routing (AAR) Access Code: 8		
Auto Route Selection (ARS) - Access Code 1: 9	Access Code 2:	
Automatic Callback Activation:	Deactivation:	
Call Forwarding Activation Busy/DA:#31 All:#30	Deactivation:#32	
Call Forwarding Enhanced Status: Act:	Deactivation:	
Call Park Access Code: #20		
Call Pickup Access Code: #22		
CAS Remote Hold/Answer Hold-Unhold Access Code:		
CDR Account Code Access Code:		
Change COR Access Code:		
Change Coverage Access Code:		
Conditional Call Extend Activation:	Deactivation:	
Contact Closure Open Code:	Close Code: CDR	
Account Code Access Code:		
Change COR Access Code:		
Change Coverage Access Code:		
Conditional Call Extend Activation:	Deactivation:	
Contact Closure Open Code:	Close Code:	

5.3. Configure Network Region

Use the **change ip-network-region x** (where x is the network region to be configured) command to assign an appropriate domain name to be used by Communication Manager, in the example below **devconnect.local** is used. Note this domain is also configured in **Section 6.1** of these Application Notes.

```
change ip-network-region 1                                     Page 1 of 20
                                                                IP NETWORK REGION
Region: 1
Location: 1           Authoritative Domain: devconnect.local
Name: default NR
MEDIA PARAMETERS
  Codec Set: 1
  UDP Port Min: 2048
  UDP Port Max: 3329
  Intra-region IP-IP Direct Audio: yes
  Inter-region IP-IP Direct Audio: yes
  IP Audio Hairpinning? y
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
  H.323 Link Bounce Recovery? y
  Idle Traffic Interval (sec): 20
  Keep-Alive Interval (sec): 5
  Keep-Alive Count: 5
                                                                AUDIO RESOURCE RESERVATION PARAMETERS
                                                                RSVP Enabled? n
```

5.4. Configure IP-Codec

Use the **change ip-codec-set x** (where x is the ip-codec set used) command to designate a codec set compatible with the Ascom Myco handsets, which supports the Codecs listed below.

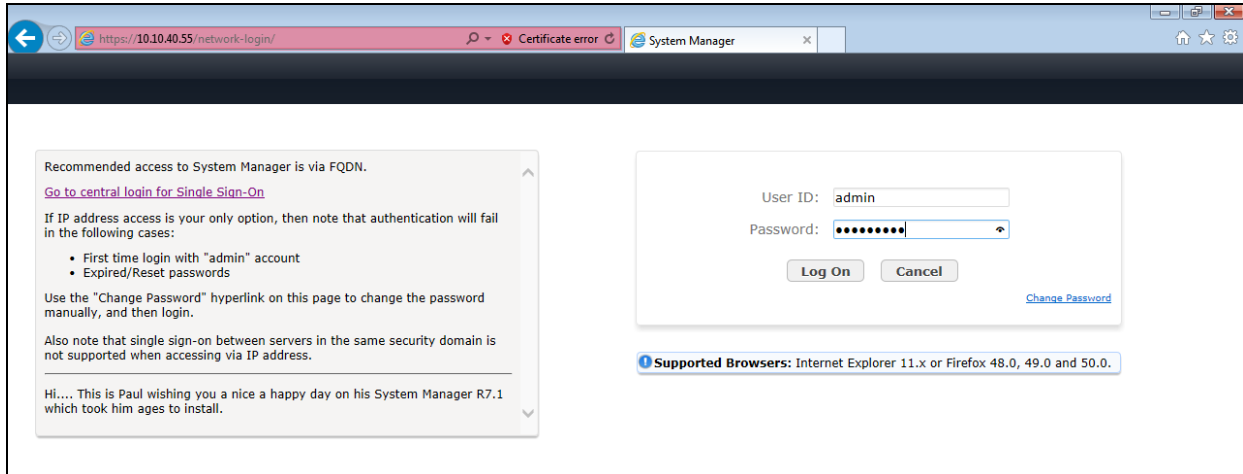
```
change change ip-codec-set 1                                   Page 1 of 2
                                                                IP Codec Set

Codec Set: 1

Audio      Silence      Frames      Packet
Codec      Suppression   Per Pkt     Size (ms)
1: G.711A   n                     2           20
2: G.711MU  n                     2           20
3: G.722-64k 2                     2           20
```

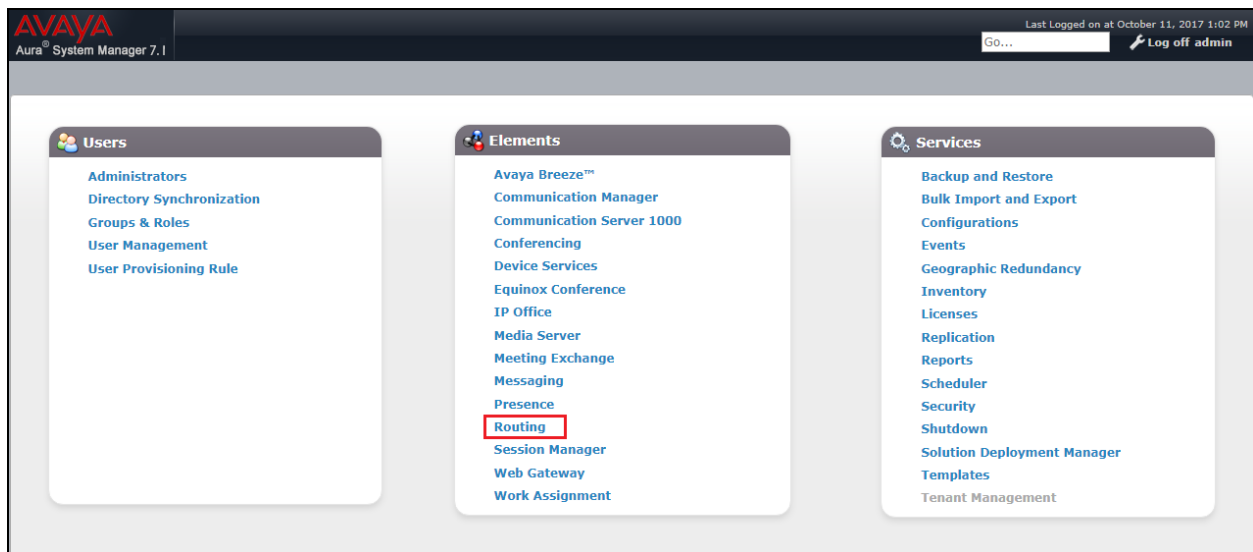
6. Configure Avaya Aura® Session Manager

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.

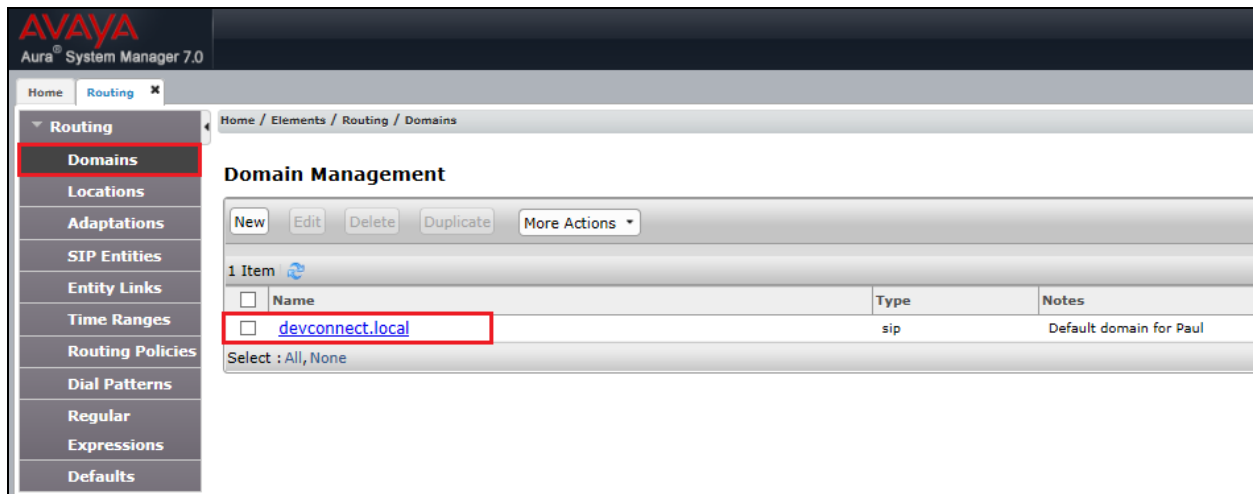


6.1. Display Domain

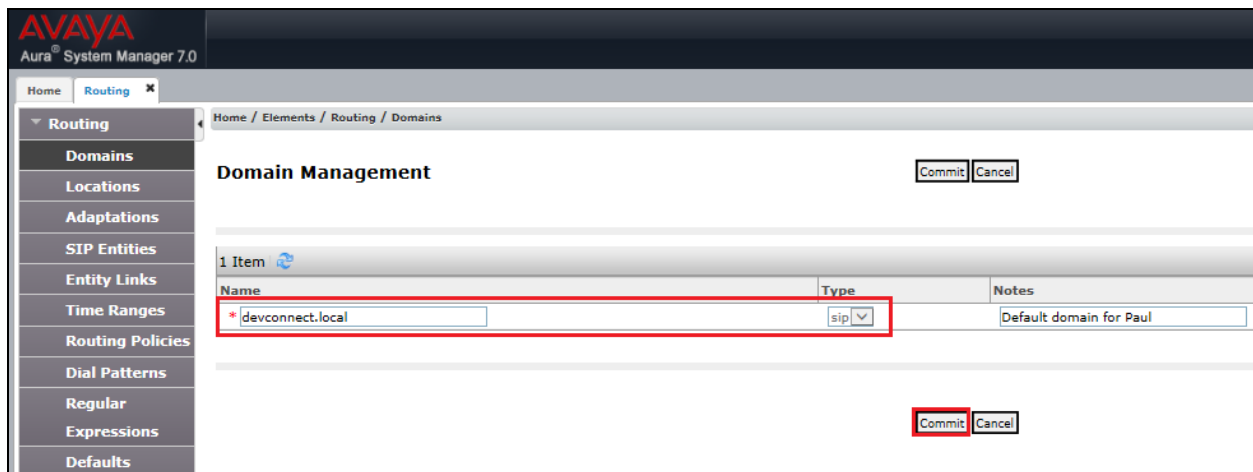
Click on **Routing** highlighted below.



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



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. Display Location

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

The screenshot displays the Avaya Aura System Manager 7.0 interface. The left sidebar contains a navigation menu with the following items: Routing, Domains, **Locations** (highlighted with a red box), Adaptations, SIP Entities, Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area is titled 'Location' and shows a table with one item, 'PGLAB', which is highlighted with a red box. The table has columns for Name, Correlation, and Notes. The 'PGLAB' entry has a correlation of 'Pauls Lab'.

Name	Correlation	Notes
PGLAB	Pauls Lab	

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

AVAYA
Aura® System Manager 7.0

Home / Elements / Routing / Locations

Location Details [Commit] [Cancel]

General

* Name: PGLAB
Notes: Pauls Lab

Dial Plan Transparency in Survivable Mode

Enabled: ☐
Listed Directory Number:
Associated CM SIP Entity:

Overall Managed Bandwidth

Managed Bandwidth Units: Kbit/sec
Total Bandwidth:
Multimedia Bandwidth:
Audio Calls Can Take Multimedia Bandwidth: ☒

Per-Call Bandwidth Parameters

Maximum Multimedia Bandwidth (Intra-Location): 2000 Kbit/Sec
Maximum Multimedia Bandwidth (Inter-Location): 2000 Kbit/Sec
* Minimum Multimedia Bandwidth: 64 Kbit/Sec
* Default Audio Bandwidth: 80 Kbit/sec

Alarm Threshold

Overall Alarm Threshold: 80 %
Multimedia Alarm Threshold: 80 %
* Latency before Overall Alarm Trigger: 5 Minutes
* Latency before Multimedia Alarm Trigger: 5 Minutes

Location Pattern

Add Remove

1 Item

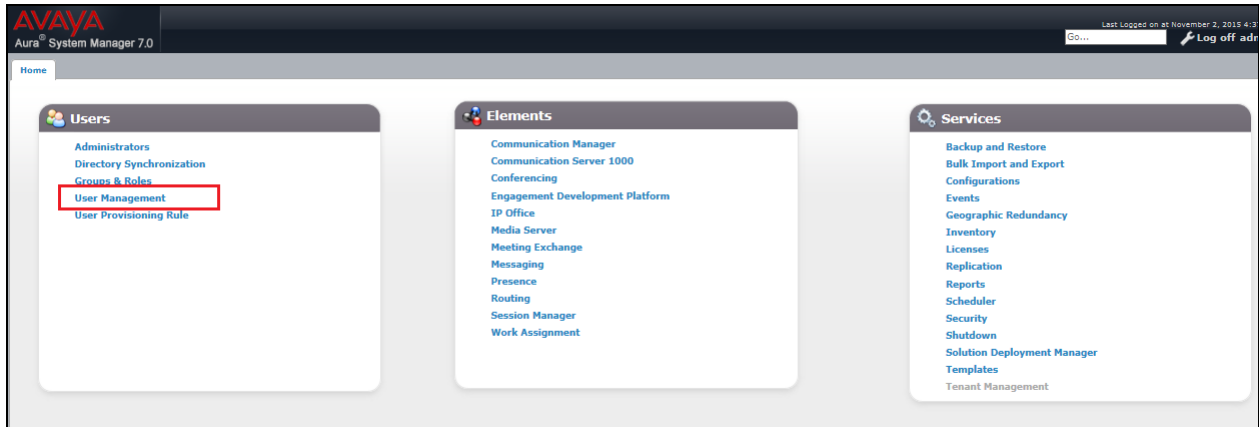
IP Address Pattern	Notes
10.10.40.	Pauls subnet

Select : All, None

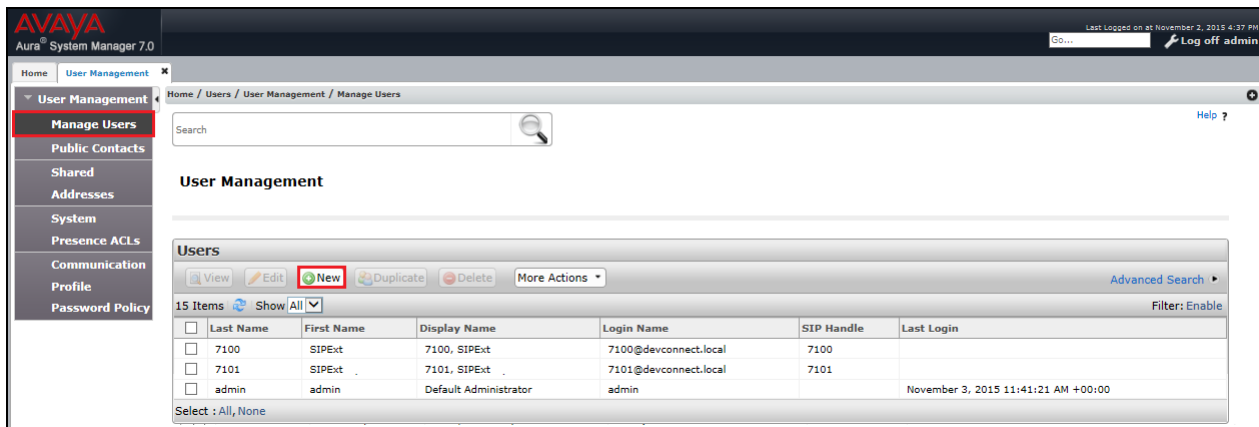
[Commit] [Cancel]

6.3. Adding Ascom Myco SIP User

From the home page shown in **Section 6.1**, click on **User Management** highlighted below.



Click on **New** highlighted 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 or filled in as shown below.

AVAYA
Aura® System Manager 7.1

Last Logged on at October 11, 2017 1:02 PM
GO... Log off admin

Home User Management x

Home / Users / User Management / Manage Users

User Management
Manage Users
Public Contacts
Shared Addresses
System Presence
ACLs
Communication
Profile Password
Policy

User Profile Edit: 4151@devconnect.local

Commit & Continue Commit Cancel

Identity * Communication Profile Membership Contacts

User Provisioning Rule
User Provisioning Rule: [v]

Identity

* Last Name: 4151
Last Name (Latin Translation): 4151
* First Name: AscomMyco
First Name (Latin Translation): AscomMyco
Middle Name: [v]
Description: [v]
Update Time : October 2, 2017 2:40:33
* Login Name: 4151@devconnect.local
Email Address: [v]
User Type: Basic [v]
[Change Password](#)
Source: local
Localized Display Name: 4151, AscomMyco
Endpoint Display Name: 4151, AscomMyco
Title: [v]
Language Preference: English (United Kingdom) [v]
Time Zone: (+1:0)GMT : Dublin, Edinburgh, [v]
Employee ID: [v]
Department: [v]

Under the **Communication Profile** tab enter a suitable **Communication Profile Password** and click on **Done** when added, note that this password is required when configuring the Ascom Myco in **Section 7**.

User Profile Edit: 4151@devconnect.local

Commit & Continue Commit Cancel

Identity * Communication Profile Membership Contacts

Communication Profile

Communication Profile Password: [v]
Confirm Password: [v] [Generate](#) [Cancel](#)

New Delete Done Cancel

Name
Primary
Select : None

* Name: Primary
Default : ☒

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 (not shown). The result is shown below with **4151@devconnect.local** being added.

Communication Address ▼

<input type="checkbox"/>	Type	Handle	Domain
<input type="checkbox"/>	Avaya SIP	4151	devconnect.local

Select : All, None

Ensure **Session Manager Profile** is checked and enter the **Primary Session Manager** details, enter the **Origination Sequence** and the **Termination Sequence** and the **Home Location** as highlighted below.

☒ **Session Manager Profile** ▼

SIP Registration

* Primary Session Manager

Primary	Secondary	Maximum
8	0	8

Secondary Session Manager

Survivability Server

Max. Simultaneous Devices

Block New Registration When Maximum Registrations Active? ☐

Application Sequences

Origination Sequence

Termination Sequence

Emergency Calling Application Sequences

Emergency Calling Origination Sequence

Emergency Calling Termination Sequence

Call Routing Settings

* Home Location

Conference Factory Set

Call History Settings

Enable Centralized Call History? ☐

Ensure that **CM Endpoint Profile** is selected for the **System** and choose the **9620SIP_DEFAULT_CM_7_1** as the **Template**. Enter the **Extension** as required and the **Voice Mail Number**, all of which are shown below. The **Sip Trunk** should be set to **aar** provided that the numbering is configured correctly on Communication Manager for aar. Click on **Endpoint Editor** to configure the buttons and features for that handset on Communication Manager.

☒ **CM Endpoint Profile** ▼

* System

CM71vmpg ▼

* Profile Type

Endpoint ▼

Use Existing Endpoints

☐

* Extension

4151

[Display Extension Ranges](#)

Endpoint Editor

Template

9620SIP_DEFAULT_CM_7_1 ▼

Set Type

9620SIP

Security Code

•••••

Port

500044

Voice Mail Number

5999

Preferred Handle

(None) ▼

Calculate Route Pattern

☐

Sip Trunk

aar

Enhanced Callr-Info display for 1-line phones

☐

Delete Endpoint on Unassign of Endpoint from User or on Delete User.

☒

Override Endpoint Name and Localized Name

☒

Allow H.323 and SIP Endpoint Dual Registration

☐

Under the **General Options** tab the **Coverage Path 1** can be set. This will determine what happens in the event of no answer or busy, for compliance testing Coverage Path “2” was configured on Communication Manager to call to voicemail. Also ensure that **Message Lamp Ext.** is showing the correct extension number. The other fields should be filled in automatically.

Done

Cancel

[Save As Template]

System

CM71vmpg

Extension

4151

Template

9620SIP_DEFAULT_CM_7_1

Set Type

9620SIP

Port

S00044

Security Code

Name

4151, AscomMyco

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)

1

* Class Of Service (COS)

1

* Emergency Location Ext

4151

* Message Lamp Ext.

4151

* Tenant Number

1

* SIP Trunk

Qaar

Type of 3PCC Enabled

None

Coverage Path 1

2

Coverage Path 2

Lock Message

☐

Localized Display Name

4151, AscomMyco

Multibyte Language

Not Applicable

Enable Reachability for Station Domain Control

system

*Required

Under the **Feature Options** tab, ensure that **MWI Served User Type** is set to **sip-adjunct** and the **Voice Mail Number** is set correctly.

General Options (G) *	Feature Options (F)	Site Data (S)	Abbreviated Call Dialing (A)	Enhanced Call Fwd (E)
<div> <div>Button Assignment (B)</div> <div>Group Membership (M)</div> </div>				
Active Station Ringing <input type="text" value="single"/>	Auto Answer <input type="text" value="none"/>			
MWI Served User Type <input type="text" value="sip-adjunct"/>	Coverage After Forwarding <input type="text" value=""/>			
Per Station CPN - Send Calling Number <input type="text" value="None"/>	Display Language <input type="text" value="english"/>			
AUDIX Name <input type="text" value="None"/>	Hunt-to Station <input type="text" value=""/>			
Remote Soft Phone Emergency Calls <input type="text" value="as-on-local"/>	Loss Group <input type="text" value="19"/>			
LWC Reception <input type="text" value="spe"/>	Survivable COR <input type="text" value="internal"/>			
IP Phone Group ID <input type="text" value=""/>	Time of Day Lock Table <input type="text" value="None"/>			
Speakerphone <input type="text" value=""/>				
Short/Prefixed Registration Allowed <input type="text" value="default"/>	Voice Mail Number <input type="text" value="5999"/>			
EC500 State <input type="text" value="enabled"/>	Music Source <input type="text" value=""/>			

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

General Options (G) * Feature Options (F) Site Data (S) Abbreviated Call Dialing (A) Enhanced Call Fwd (E)

Button Assignment (B) Group Membership (M)

	Main Buttons	Feature Buttons			
1	call-appr				
2	call-appr				
3	call-appr				
4	None				
5	None				
6	None				

* Required

Done Cancel

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

☒ CM Endpoint Profile

* System CM71vmpg

* Profile Type Endpoint

Use Existing Endpoints ☐

* Extension 4151 [Display Extension Ranges](#) [Endpoint Editor](#)

Template 9620SIP_DEFAULT_CM_7_1

Set Type 9620SIP

Security Code *****

Port S00044

Voice Mail Number 5999

Preferred Handle (None)

Calculate Route Pattern ☐

Sip Trunk aar

Enhanced Callr-Info display for 1-line phones ☐

Delete Endpoint on Unassign of Endpoint from User or on Delete User. ☒

Override Endpoint Name and Localized Name ☒

Allow H.323 and SIP Endpoint Dual Registration ☐

☐ CS 1000 Endpoint Profile

☐ CallPilot Messaging Profile

* Required

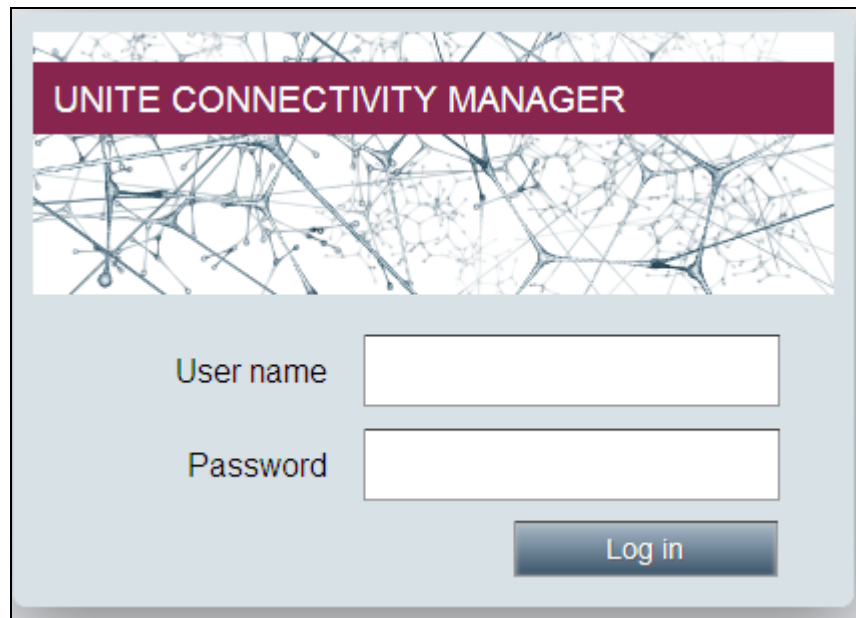
Commit & Continue Commit Cancel

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.

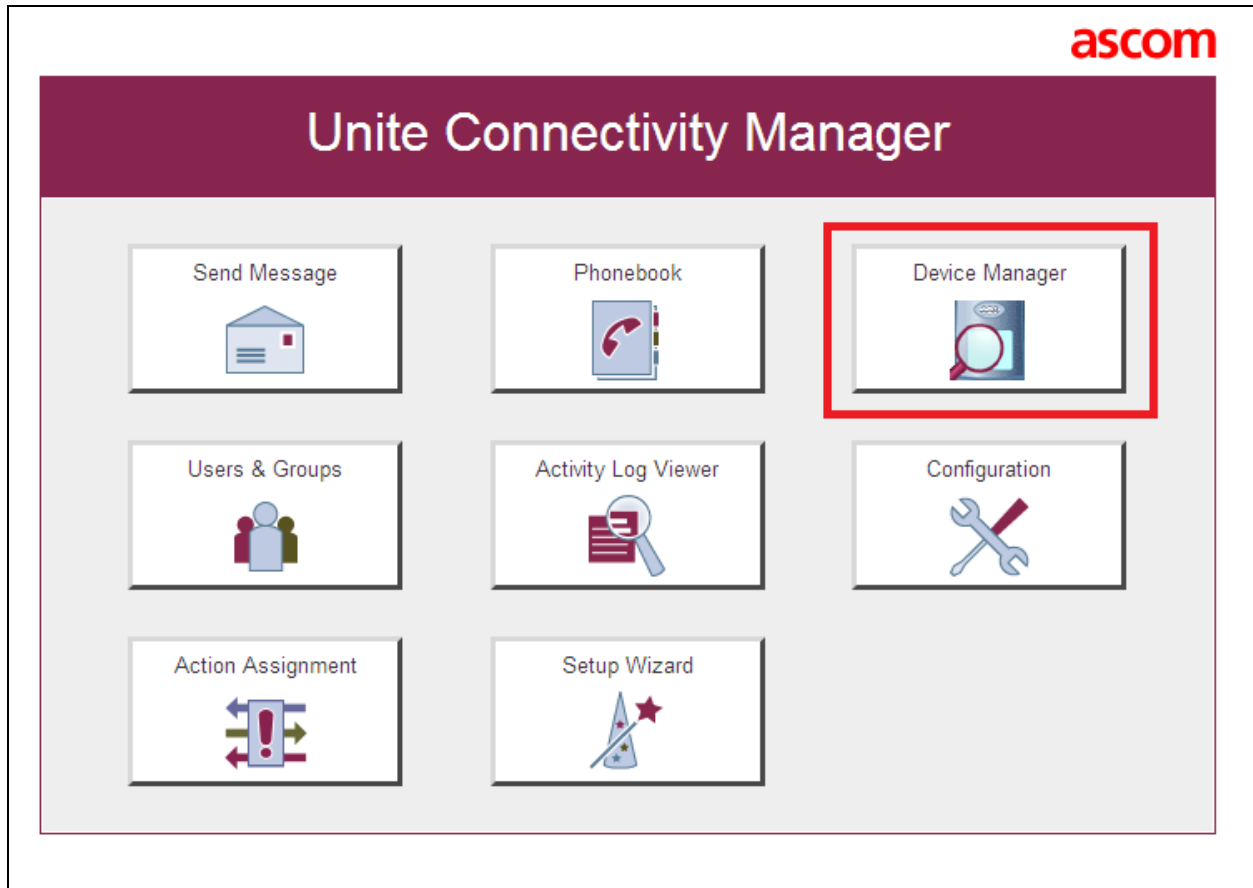
Note: The Wireless router configuration is outside the scope of these Application Notes.

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**.

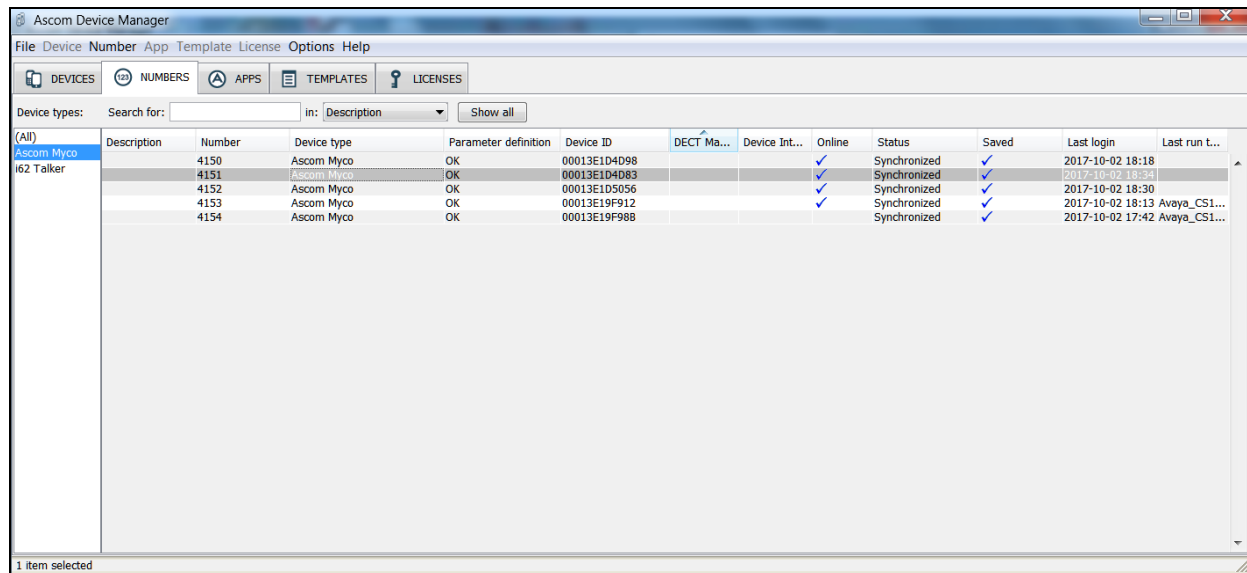


The screenshot shows a web browser window displaying the 'UNITE CONNECTIVITY MANAGER' login interface. The header features the title in white text on a dark red background, with a network diagram background. Below the header, there are two input fields: 'User name' and 'Password', each with a corresponding text label to its left. A 'Log in' button is positioned to the right of the 'Password' field.

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 **4151** was selected.

123	NUMBERS	A	APPS	≡	TEMPLATES	🔑	LICENSES
Search for:		in:	Description	▼	Show all		
Description	Number	Device type	Parameter definition	Device ID			
	4150	Ascom Myco	OK	00013E1D4D98			
	4151	Ascom Myco	OK	00013E1D4D83			
	4152	Ascom Myco	OK	00013E1D5056			
	4153	Ascom Myco	OK	00013E19F912			
	4154	Ascom Myco	OK	00013E19F988			

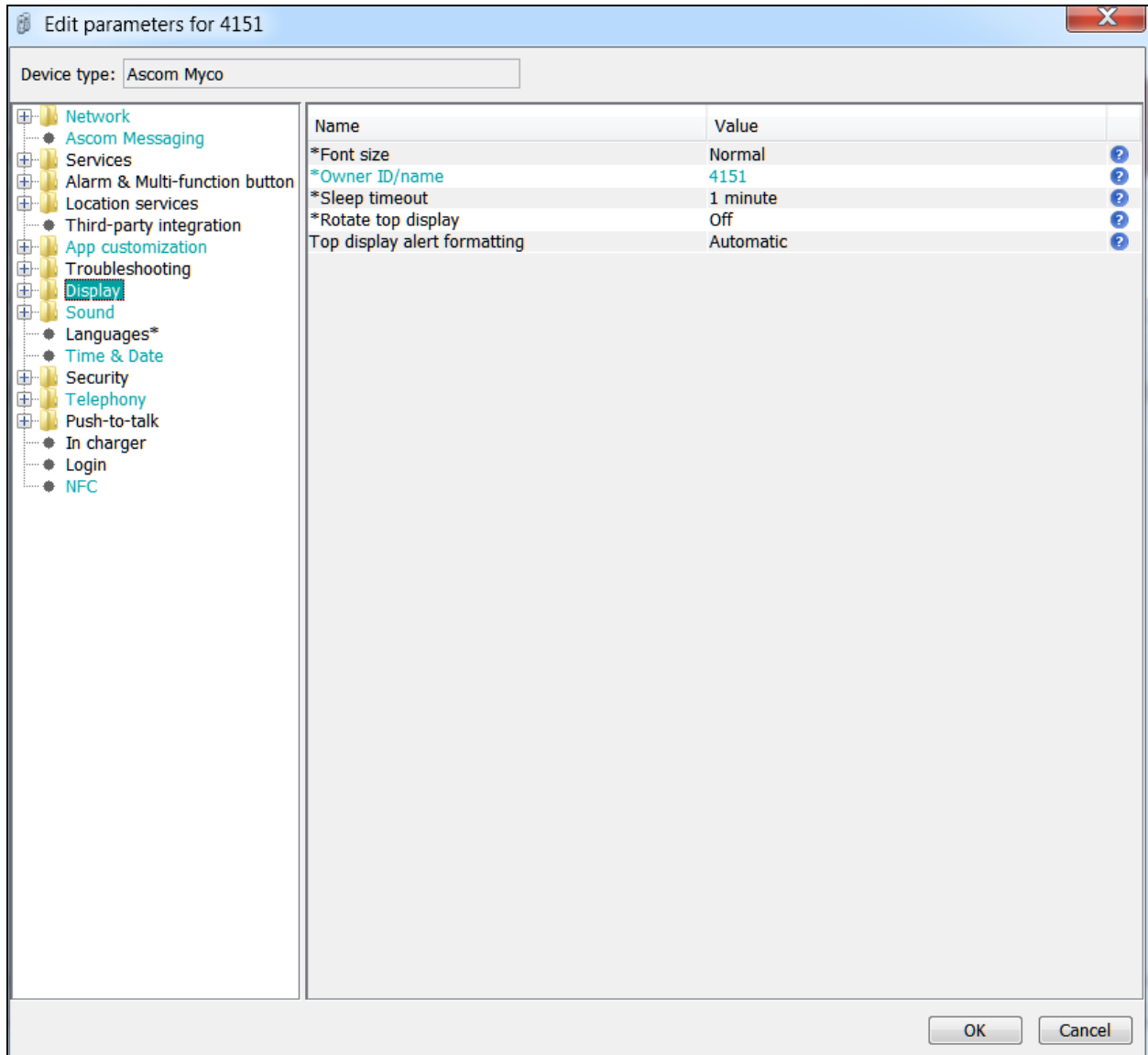
The **Edit parameters for 4151** screen are seen as shown below. Click on **Ascom VoIP** that is seen on the left hand side and configure the following values.

- **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** **300** (was simply chosen to refresh every 5 mins)
- **Endpoint ID** This is the extension number
- **Password** Password assigned to the endpoint in **Section 6.3**
- **Codec configuration** This will depend on the country
- **DTMF Type** **RFC 2833** is chosen
- **Direct Signaling** This must be set to **Yes** if Shuffling is used on Communication Manager

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.

Name	Value
SIP Transport	TCP
Primary SIP proxy	10.10.40.52
Secondary SIP proxy	
Listening port	5060
SIP proxy ID	
SIP Register expiration	300
Endpoint ID	4151
Password	*****
VoIP phone number	
Codec configuration	G711 A-law
Secure RTP mode	Off
DTMF type	RFC 2833
Hold type	inactive
MOH locally	Yes
Direct signaling	Yes
Active mode during call	No
Replace Call Rejected with User Busy	No
Enable overlap dialing	No

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 **4151** as shown below. Retain default values for all other fields and click on **OK** to complete the configuration.



The messaging number can be set as shown below. **5999** is the number that all users dial to access voicemail and retrieve messages, this is the number set for **Voicemail number** below.

Device type:

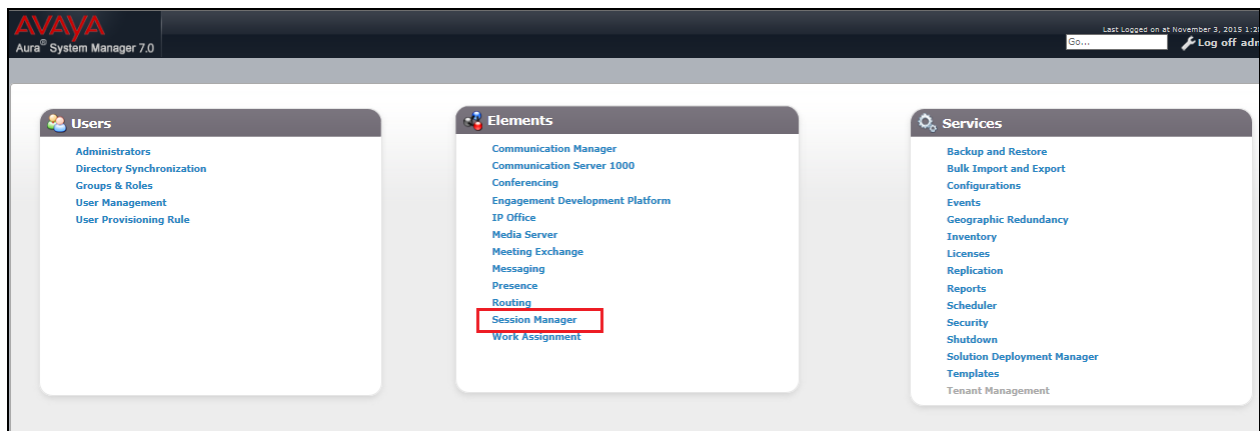
Name	Value	
Message centre number	4151	?
Voicemail number	5999	?
Voicemail call clears MWI	No	?
Cellular voicemail number		?

OK Cancel

8. Verification Steps

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

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 screenshot shows the Session Manager Dashboard. The left sidebar contains a navigation menu with the following items: Dashboard, Session Manager Administration, Communication Profile Editor, Network Configuration, Device and Location Configuration, Application Configuration, System Status (highlighted), SIP Entity Monitoring, Managed Bandwidth Usage, Security Module Status, SIP Firewall Status, Registration Summary, User Registrations (highlighted), and Registrations. The main content area displays the Session Manager Dashboard, which includes a table of Session Manager Instances.

Session Manager Dashboard												
This page provides the overall status and health summary of each administered Session Manager.												
Session Manager Instances												
Service State Shutdown System As of 6:26 PM												
1 Item Show All												
	Session Manager	Type	Tests Pass	Alarms	Security Module	Service State	Entity Monitoring	Active Call Count	Registrations	Data Replication	User Data Storage Status	License Mode
	sm70vmpo	Core	✓	0/0/0	Up	Accept New Service	0/3	0	2/2	✓	✓	Normal

Select : All, None

The Ascom Myco user should show as being registered as highlighted. Note that this is just an example from another compliance test; this is simply shown to illustrate how each endpoint should show once it is registered correctly.

User Registrations

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

View **Default** Force Unregister **AST Device Notifications:** Reboot Reload Failback As of 6:27 PM Customize Advanced Search

14 Items Show All

	Details	Address	First Name	Last Name	Actual Location	IP Address	Remote Office	Shared Control	Simult. Devices	AST Device	Registered		
											Prim	Sec	Surv
<input type="checkbox"/>	Show	---	Ascom Myco	7221	---	---	<input type="checkbox"/>	<input type="checkbox"/>	0/1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	Show	---	Ascom Dect	7212	---	---	<input type="checkbox"/>	<input type="checkbox"/>	0/1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	Show	7220@devconnect.local	Ascom Myco	7220	PGLAB	10.10.40.158	<input type="checkbox"/>	<input type="checkbox"/>	1/1	<input type="checkbox"/>	<input checked="" type="checkbox"/> (AC)	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	Show	7100@devconnect.local	SIPEXt	7100	PGLAB	10.10.40.159	<input type="checkbox"/>	<input type="checkbox"/>	1/1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> (AC)	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	Show	---	Ascom i62	7203	---	---	<input type="checkbox"/>	<input type="checkbox"/>	0/1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	Show	---	Ascom Dect	7211	---	---	<input type="checkbox"/>	<input type="checkbox"/>	0/1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	Show	---	Ascom Dect	7213	---	---	<input type="checkbox"/>	<input type="checkbox"/>	0/1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	Show	---	Ascom i62	7200	---	---	<input type="checkbox"/>	<input type="checkbox"/>	0/1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	Show	---	Ascom Dect	7210	---	---	<input type="checkbox"/>	<input type="checkbox"/>	0/1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	Show	---	Ascom Myco	7222	---	---	<input type="checkbox"/>	<input type="checkbox"/>	0/1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	Show	---	Ascom i62	7202	---	---	<input type="checkbox"/>	<input type="checkbox"/>	0/1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	Show	---	Ascom i62	7201	---	---	<input type="checkbox"/>	<input type="checkbox"/>	0/1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	Show	---	Ascom Myco	7223	---	---	<input type="checkbox"/>	<input type="checkbox"/>	0/1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Select : All, None

9. Conclusion

These Application Notes describe the configuration steps required for Ascom Myco V9.2 to successfully interoperate with Avaya Aura® Communication Manager R7.1 and Avaya Aura® Session Manager R7.1 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] *Administering Avaya Aura® Communication Manager*, Document ID 03-300509
- [2] *Avaya Aura® Communication Manager Feature Description and Implementation*, Document ID 555-245-205
- [3] *Implementing Avaya Aura® Session Manager* Document ID 03-603473
- [4] *Administering Avaya Aura® Session Manager*, Doc ID 03-603324

Product 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

change 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? y	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: SM71vmppg	
Near-end Listen Port: 5061	Far-end Listen Port: 5061	
	Far-end Network Region: 1	
Far-end Domain: devconnect.local		
	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

change trunk-group 1		Page 1 of 21
TRUNK GROUP		
Group Number: 1	Group Type: sip	CDR Reports: y
Group Name: SIPTRUNK	COR: 1	TN: 1 TAC: *801
Direction: two-way	Outgoing Display? n	Night Service:
Dial Access? n		
Queue Length: 0		
Service Type: tie	Auth Code? n	
	Member Assignment Method: auto	
	Signaling Group: 1	
	Number of Members: 10	

change trunk-group 1		Page 2 of 21
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		

```

change trunk-group 1
TRUNK FEATURES
    ACA Assignment? n
    Measured: none
    Maintenance Tests? y

    Suppress # Outpulsing? n
    Numbering Format: private
    UUI Treatment: service-provider

    Replace Restricted Numbers? n
    Replace Unavailable Numbers? n

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

Show ANSWERED BY on Display? y

```

```
change trunk-group 1                                Page    4 of   21
```

```
                        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? y
                        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
```

©2017 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.