



Avaya Solution & Interoperability Test Lab

Application Notes for Ascom Myco 4 with Avaya Aura® Communication Manager R10.1 and Avaya Aura® Session Manager R10.1 - Issue 1.0

Abstract

These Application Notes describe the configuration steps for provisioning Ascom's Myco 4 smartphone to interoperate with Avaya Aura® Communication Manager 10.1 and Avaya Aura® Session Manager 10.1.

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's Myco 4 version A12_065.00 (SW65), including the Ascom Experience app package version 4.0.6, to interoperate with Avaya Aura® Communication Manager R10.1 and Avaya Aura® Session Manager R10.1. Ascom Myco 4 is a smartphone 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 4 may be referred to as Myco 4, Myco 4 handset or Myco 4 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 4 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 4 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 4 smartphone to make and receive calls to and from Avaya H.323, SIP, Workplace and Digital Deskphones as well as external calls over a simulated PSTN. Avaya Messaging was used to demonstrate DTMF and Message Waiting Indication.

Note: The cellular version of the Ascom Myco 4 smartphone can be set up to use Wi-Fi and/or GSM/3G/LTE/5G. 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.

Note: Ascom Myco 4 handsets are 3rd party SIP handsets and as such 3rd party SIP telephone features, beyond basic call handling via Communication Manager, will vary between SIP devices.

DevConnect Compliance Testing is conducted jointly by Avaya and DevConnect members. The jointly defined test plan focuses on exercising APIs and/or standards-based interfaces pertinent to the interoperability of the tested products and their functionalities. DevConnect Compliance Testing is not intended to substitute full product performance or feature testing performed by DevConnect members, nor is it to be construed as an endorsement by Avaya of the suitability or completeness of a DevConnect member's solution.

Avaya recommends our customers implement Avaya solutions using appropriate security and encryption capabilities enabled by our products. The testing referenced in these DevConnect Application Notes included the enablement of supported encryption capabilities in the Avaya

products. Readers should consult the appropriate Avaya product documentation for further information regarding security and encryption capabilities supported by those Avaya products.

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

For the testing associated with these Application Notes, the interface between Avaya systems and Ascom Myco 4 did not include use of any specific encryption features as requested by Ascom.

Avaya's formal testing and Declaration of Conformity is provided only on the headsets/Smartphones that carry the Avaya brand or logo. Avaya may conduct testing of non-Avaya headset/smartphone 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.

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 4 handsets and simulated PSTN endpoints.

- Registration/Invalid Registration
- Basic Calls/PSTN calls
- Multiple Lines (Multiline)
- Session Refresh Timer
- Long Duration Call
- Hold, Retrieve and Brokering (Toggle)
- Feature Access Code dialing
- Attended and Blind Transfer
- Third Party Conference using Myco 4 to host the conference
- Call Forwarding Unconditional, No Reply and Busy (PBX controlled and Locally Controlled)

- Call Waiting
- Call Park/Pickup
- EC500, where Avaya deskphone is the primary phone and Myco 4 handset being the EC500 destination.
- Multi-Device Access (MDA)
- Calling Line Name/Identification
- Codec Support (G.722, G.711, G.729)
- DTMF Support
- Message Waiting Indication and Voicemail
- Serviceability

Note1: 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.

Note2: For 9-1-1 emergency call handling in the USA, Ascom is recommending setting Ascom Settings → Ascom VoIP → “Emergency call location method” to “Register with SIP instance-ID” (RFC5626). **This was not covered in the testing.**

2.2. Test Results

The tests were all functional in nature and performance testing and redundancy testing were not included. All test cases passed successfully with any issues and observations listed below. The following observations were noted.

- During compliance testing, Bluetooth was turned off on all Myco 4 handsets to avoid call quality issues that may be encountered when using 2.4GHz Wi-Fi. There are two places where Bluetooth must be turned off, Android settings → Connected devices → Connection preferences - Bluetooth should be set to off, and Android settings → Location Services → Wi-Fi and Bluetooth scanning - Ensure that both are off.
- Ascom Myco 4 does not support local call diversion like Call Forward Busy and Call Forward No Answer. It does support Call Forward All.
- When using the EC500 (concurrent call) feature, if an Myco 4 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 4 handset users, calls may be answered by a cellular user’s voicemail instead of following the coverage criteria in Communication Manager.

- All compliance testing was done using TCP (preferred) and UDP as the transport protocol.
- Session Manager has a minimum Registration Timer of 600 seconds. If the Myco 4 Registration Timer is set lower than 600 seconds, this will be negotiated to 600 seconds. This appears to be changed from a default value of 120 seconds with previous releases of Session Manager (see **Appendix C**).
- Negotiation of G.722 between endpoints such as the Ascom Myco 4, requires support for the codec to be configured on Communication Manager.
- When multiple voice messages are left for an Myco 4 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 Messaging.
- For Multi-Device Access (MDA), Myco 4 needs to be configured using and registering through Endpoint ID. Refer to **Section 7.3** for details.
- Per design, Myco 4 handsets do not have a redial button. User needs to use “Call List” and redial the numbers.
- PSTN calls were simulated using a SIP trunk routing via an Avaya Session Border Controller. In order to correctly simulate incoming calls from a typical SIP service provider, the Session Border Controller must be setup to present the SIP calls correctly to the Ascom phones. Using Topology Hiding under Configuration Profiles will ensure that the calls are presented to Ascom in the correct format. Please see **Appendix B** for the setup that was used during compliance testing.

2.3. Support

Technical support for the Ascom Myco 4 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 4 handsets register with Session Manager to make/receive calls with the Avaya Digital, H.323, and SIP endpoints on Communication Manager and with a simulated PSTN.

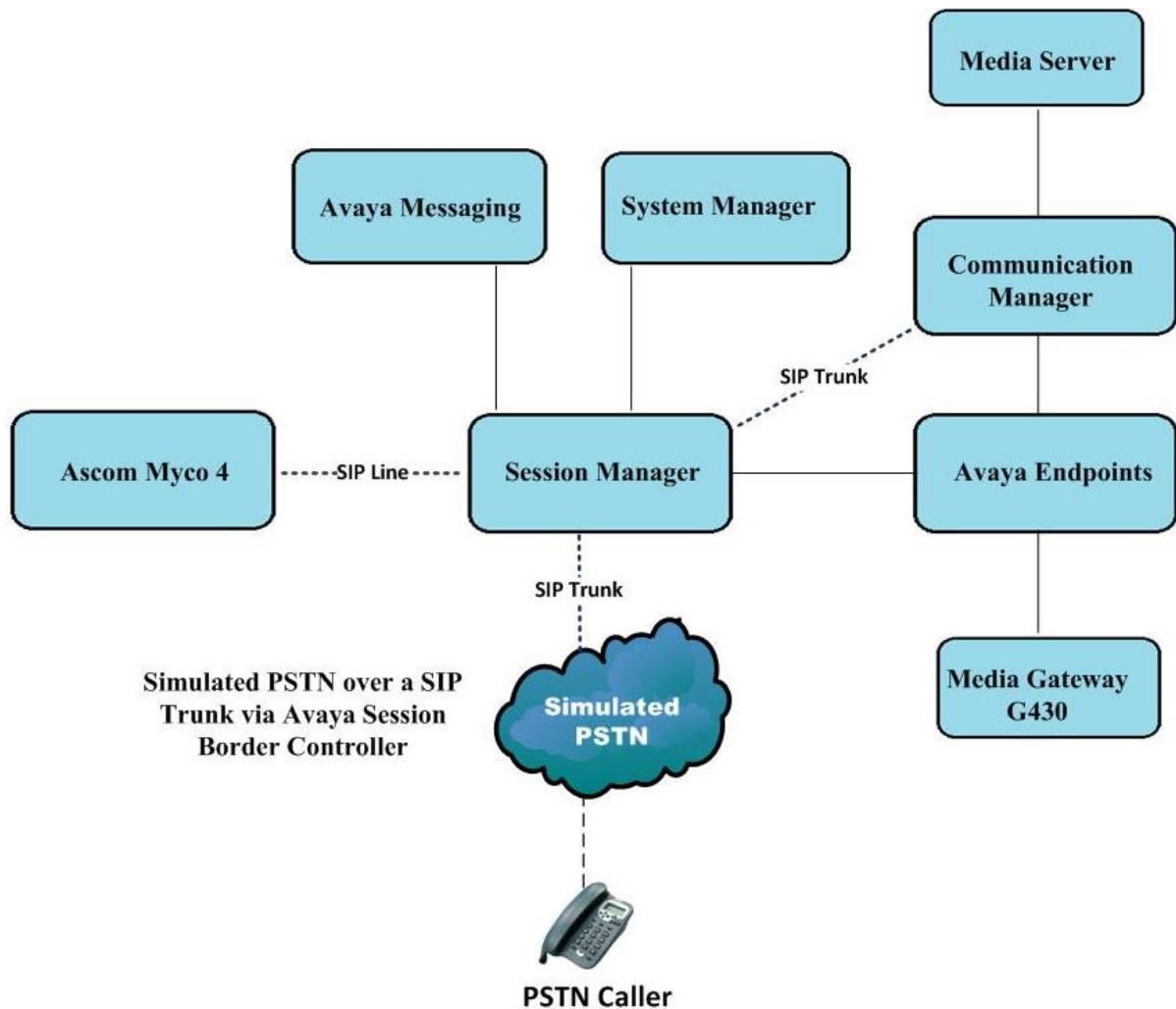


Figure 1: Network Solution of Ascom Myco 4 smartphone with Avaya Aura® Communication Manager R10.1 and Avaya Aura® Session Manager R10.1

4. Equipment and Software Validated

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

Avaya Equipment	Software / Firmware Version
Avaya Aura® System Manager	System Manager 10.1.3.1 Build No. – 10.1.0.0.537353 Software Update Revision No: 10.1.3.1.0716149 (Service Pack 1)
Avaya Aura® Session Manager	Session Manager R10.1 Build No. – 10.1.3.1.1013103
Avaya Aura® Communication Manager	R10.1.3.1 – FP3SP1 R020x.01.0.974.0 Update ID 01.0.974.0-27937
Avaya Messaging	11.0 SP2 Build 11.0.0.324
Avaya Aura® Media Server	10.1.0.154
Avaya Media Gateway G430	42.7.0 /2
Avaya 9404 Digital	17.0
Avaya J100 Series SIP	4.1.1.0.7
Avaya J100 Series H323	6.8.5.4.10
Avaya Session Border Controller (to facilitate simulated PSTN)	10.1.0.0-32-21432
Ascom Equipment	Software / Firmware Version
Ascom Myco 4	A12_065.00 (SW65)
Ascom Experience (AE)*	4.0.6
Ascom approved Wi-Fi Access Point	Ascom approved software version

Note: All Avaya equipment is running on VMware virtual servers.

*Ascom Experience is an application package installed “on top” of Android. It is typically relevant for ascertaining the version of the SIP application used on Ascom Myco 4.

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 A** 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/Hunt Group

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

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 **3**. 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 String	Total Length	Call Type	Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type	
1	4	udp							
2	4	udp							
3	4	ext							
4	4	ext							
5	4	udp							
6	4	ext							
8	1	fac							
9	1	fac							
*8	4	dac							
*	3	fac							
#	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 **Appendix A**.

change aar analysis 3							Page 1 of 2
AAR DIGIT ANALYSIS TABLE							
Location: all					Percent Full: 1		
	Dialed String	Total		Route	Call	Node	ANI
		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 Myco 4 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 **greanep.sil6.avaya.com** 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: greanep.sil6.avaya.com
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 4 handsets. During compliance testing the codecs shown below were offered to the Myco 4 handsets.

```
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-SWB24K                1         20
2: G.722-64K                  2         20
3: G.711A                     n         20
4: G.711MU                   n         20
5:
6:
Media Encryption                               Encrypted SRTCP: best-effort
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 **3**: The coverage path will be used after 3 rings.

Point 1 is set to **h68**: Hunt Group 68 is utilised by this coverage path.

```
display coverage path 3

                                COVERAGE PATH

                                Coverage Path Number: 3
                                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: h68           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 **6668**, which is used to dial for messaging and **Group Type** is set to **ucd-mia**.

```
display hunt-group 68                                     Page 1 of 60

                                HUNT GROUP

                                Group Number: 68                ACD? n
                                Group Name: Messaging             Queue? n
                                Group Extension: 6668            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:

SIP URI::
```

On **Page 2 Message Center** is set to **sip-adjunct**.

display hunt-group 68

HUNT GROUP

Page 2 of 60

Message Center: sip-adjunct

Voice Mail Number	Voice Mail Handle	Routing Digits
		(e.g., AAR/ARS Access Code)
6668	6668	8

6. Configure Avaya Aura® Session Manager

The Ascom Myco 4 handsets are added to Session Manager as SIP users. The procedures include the following areas:

- Domains and Locations
- Adding Ascom SIP Users

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

Recommended access to System Manager is via FQDN.
[Go to central login for Single Sign-On](#)

If IP address access is your only option, then note that authentication will fail in the following cases:

- First time login with "admin" account
- Expired/Reset passwords

Use the "Change Password" hyperlink on this page to change the password manually, and then login.

Also note that single sign-on between servers in the same security domain is not supported when accessing via IP address.

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

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

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

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

User ID:

Password:

[Change Password](#)

Supported Browsers: Firefox (minimum version 93.0), Chrome (minimum version 91.0) or Edge (minimum version 93.0).

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

AVAYA Aura® System Manager 10.1

Users Elements Services Widgets Shortcuts

Search admin

Disk Space Utilization

Avaya Breeze®

Communication Manager

Communication Server 1000

Device Adapter

Device Services

IP Office

Media Server

Meeting Exchange

Messaging

Presence

Routing

Session Manager

Web Gateway

Notifications (2)

Your last successful login was on at April 14, 2022 1:36 PM from 192.168.40.240. [None...](#)

No Session Manager emergency Dial Pattern routes are administered. [None...](#)

Application State

License Status	Active
Deployment Type	VMware
Multi-Tenancy	DISABLED
OOBM State	DISABLED
Hardening Mode	Standard

Information

Elements	Count	Sync Status
Avaya Breeze	3	■
CM	1	■
Session Manager	1	■
System Manager	1	■
UCM Applications	8	■

Current Usage :

7/250000 USERS

1/50

Alarms

Critical Major Indeterminate Minor Warning

Shortcuts

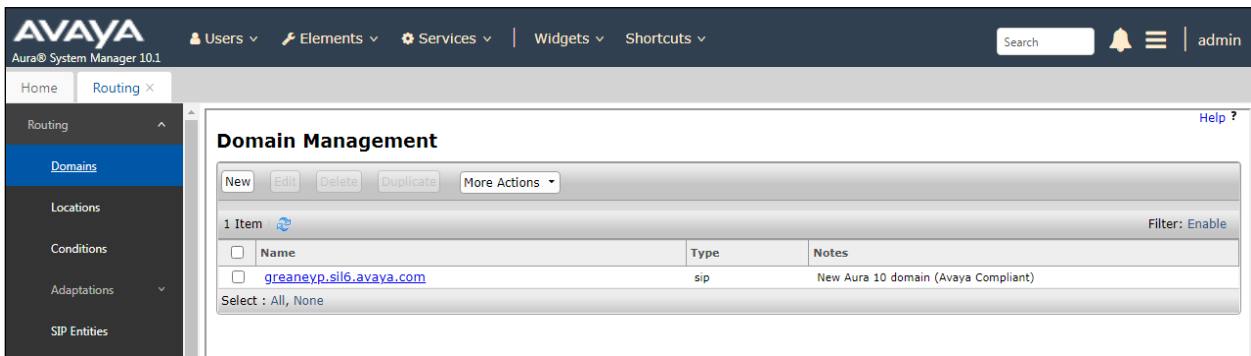
Drag shortcuts here

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.

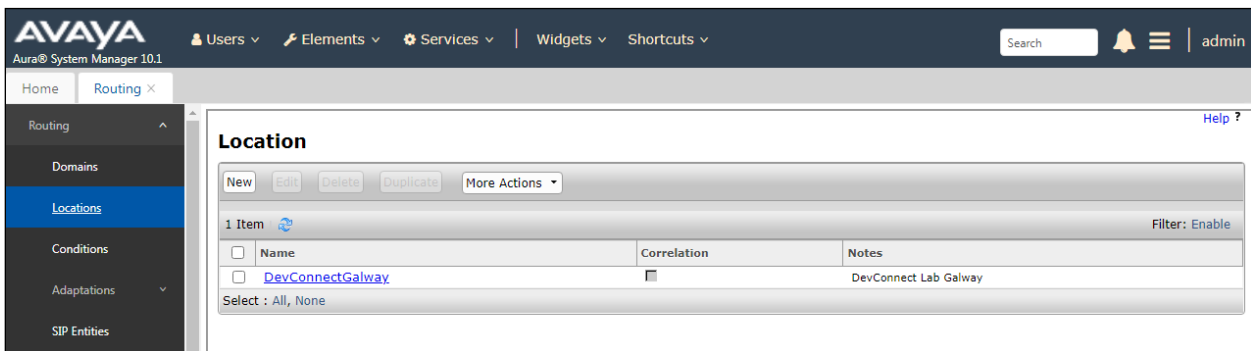
6.1.1. Display the Domain

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



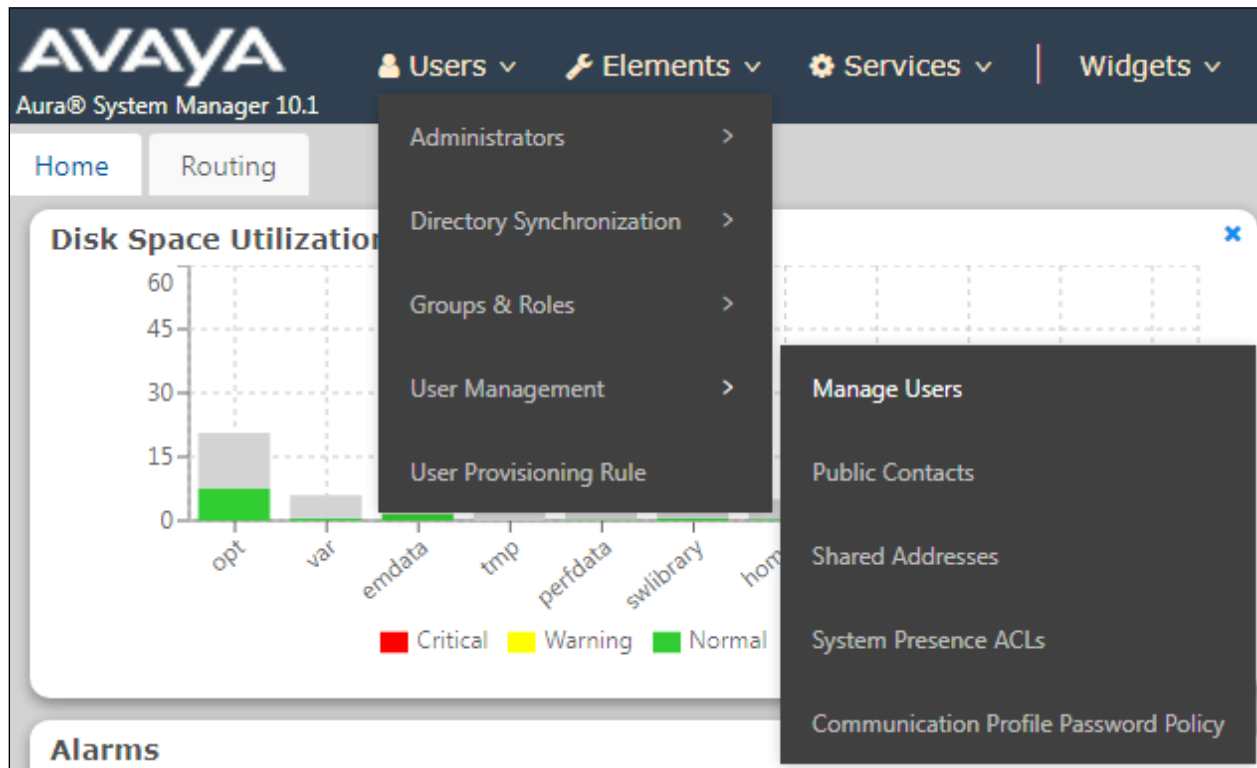
6.1.2. Display the Location

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.

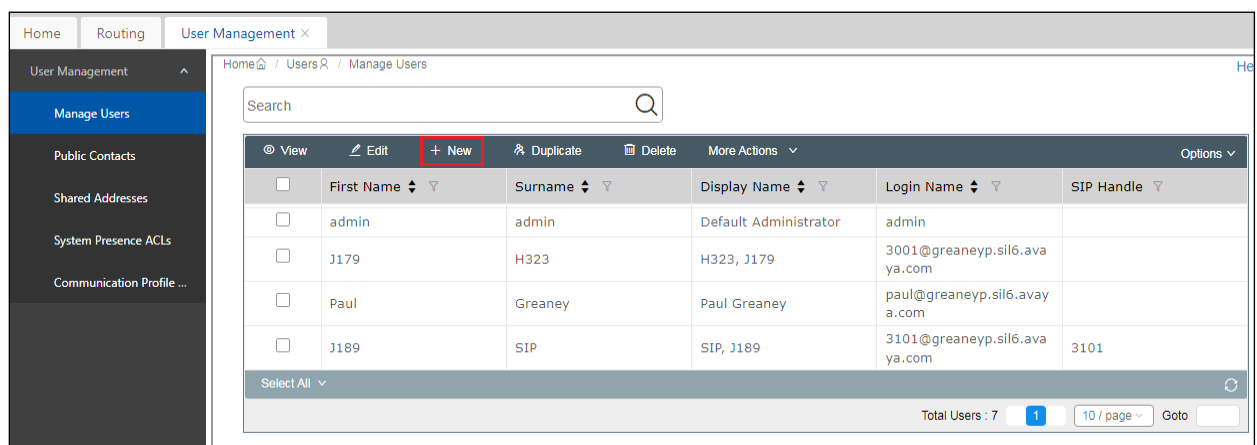


6.2. Adding Ascom SIP Users

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.

The screenshot shows the 'User Management' interface with the 'Identity' tab selected. The left sidebar contains options: 'Manage Users', 'Public Contacts', 'Shared Addresses', 'System Presence ACLs', and 'Communication Profile ...'. The main area displays the 'Basic Info' section with the following fields:

- User Provisioning Rule: (Dropdown)
- * Last Name: 3191
- Last Name (in Latin alphabet characters): 3191
- * First Name: AscomMYCO
- First Name (in Latin alphabet characters): AscomMYCO
- * Login Name: 3191@greanep.sil6.ava
- Middle Name: Middle Name Of User
- Description: AscomMYCO
- Email Address: Email Address Of User
- Password: (Empty)
- User Type: Basic
- Confirm Password: (Empty)
- Localized Display Name: 3191, AscomMYCO
- Endpoint Display Name: 3191, AscomMYCO
- Title Of User: Title Of User
- Language Preference: English (United Sta...)
- Time Zone: (+1:0)GMT : Dublin,...
- Employee ID: Employee Id Of User
- Department: Department Of User
- Company: Company Of User
- Update Time: Oct 23 2023 14:31:20

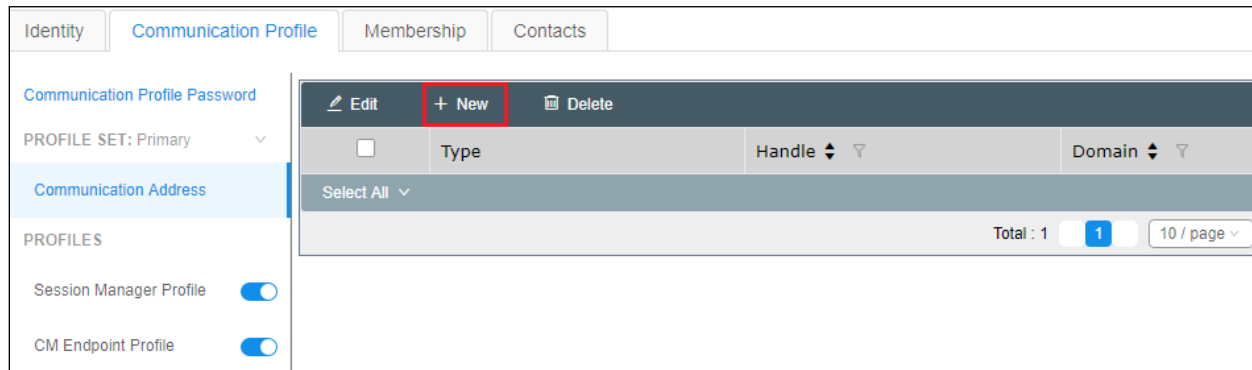
Under the **Communication Profile** tab enter **Communication Profile Password** and **Re-enter Comm-Profile Password**, note that his password is required when configuring the Myco 4 handset in **Section 7.2**.

The screenshot shows the 'Communication Profile' tab selected. A 'Comm-Profile Password' dialog box is open, prompting for a password and its re-entry. The background shows the 'Communication Profile Password' section with 'PROFILE SET : Primary' and 'Communication Address'.

The dialog box contains the following fields:

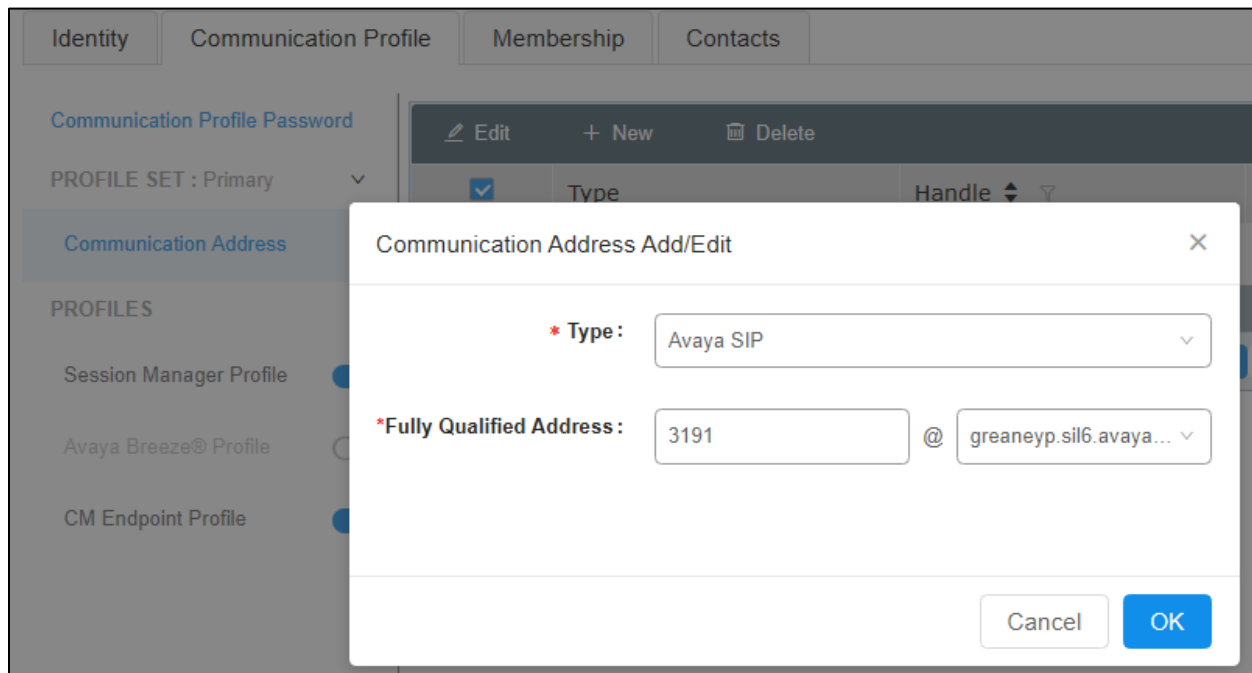
- Comm-Profile Password: (Masked with dots)
- * Re-enter Comm-Profile Password: (Masked with dots, with a green checkmark icon)
- Buttons: Cancel, OK
- Link: Generate Comm-Profile Password

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



The screenshot shows the 'Communication Profile' tab in a web interface. On the left sidebar, 'Communication Address' is selected under the 'PROFILES' section. The main area has a dark header with 'Edit', '+ New' (highlighted with a red box), and 'Delete' buttons. Below this is a table with columns 'Type', 'Handle', and 'Domain'. A 'Select All' dropdown is on the left of the table. At the bottom right of the table area, it says 'Total : 1' and '10 / page'.

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



The screenshot shows the 'Communication Address Add/Edit' dialog box. It has a title bar with a close button. Inside, there are two main fields: '* Type:' with a dropdown menu showing 'Avaya SIP', and '*Fully Qualified Address:' with two input fields. The first input field contains '3191' and the second contains 'greaney.p.sil6.avaya...'. There are 'Cancel' and 'OK' buttons at the bottom right.

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).

Note: Max. Simultaneous Devices will need to be set here when configuring Multi-Device Access in **Section 7.3**, set this to the number of devices that are to be allowed to registered. This will only be set on the SIP user that all devices will be registering as, for compliance testing this SIP user was 3101. So, this will be set on SIP user 3101 to however many devices will be registering as 3101.

Identity

Communication Profile

Membership

Contacts

Communication Profile Password

PROFILE SET : Primary

Communication Address

PROFILES

Session Manager Profile

Avaya Breeze® Profile

CM Endpoint Profile

SIP Registration

* Primary Session Manager :

sm101x

Secondary Session Manager :

Start typing...

Survivability Server :

Start typing...

Max. Simultaneous Devices :

1

Block New Registration When Maximum Registrations Active?

Application Sequences

Origination Sequence :

CM-APP-SEQ

Termination Sequence :

CM-APP-SEQ

Emergency Calling Application Sequences

Emergency Calling Origination Sequence :

Select

Emergency Calling Termination Sequence :

Select

Call Routing Settings

* Home Location :

DevConnectGalway

Conference Factory Set :

Select

PG; Reviewed:
SPOC 11/21/2023

Solution & Interoperability Test Lab Application Notes
©2023 Avaya Inc. All Rights Reserved.

19 of 51
Myco4_CM101

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 Myco 4 handset. Click on **Endpoint Editor** to configure the buttons and features for that handset on Communication Manager.

User Profile | Edit | 3191@greanep.sil6.avaya.com

Commit & Continue

Commit

Cancel

Identity

Communication Profile

Membership

Contacts

Communication Profile Password

PROFILE SET : Primary

Communication Address

PROFILES

Session Manager Profile

Avaya Breeze® Profile

CM Endpoint Profile

* System :

cm101x

* Profile Type :

Endpoint

Use Existing Endpoints :

☐

* Extension :

3191

Template :

9620SIP_DEFAULT_C

* Set Type :

9620SIP

Security Code :

Enter Security Code

Port :

S000010

Voice Mail Number :

6668

Preferred Handle :

Select

Calculate Route Pattern :

☐

Sip Trunk :

aar

SIP URI :

Select

Enhanced Callr-Info Display for 1-line phones :

☐

Delete on Unassign from User or on Delete

☒

Override Endpoint Name and Localized Name :

☒

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.

System	cm101x	Extension	3191
Template	9620SIP_DEFAULT_CM_10_1	Set Type	9620SIP
Port	S000010	Security Code	
Name	3191, 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	3191	* Message Lamp Ext.	3191	
* Tenant Number	1			
* SIP Trunk	Qaar	Type of 3PCC Enabled	None	
Coverage Path 1	3	Coverage Path 2		
Lock Message	<input type="checkbox"/>	Localized Display Name	3191, AscomMYCO	
Multibyte Language	Not Applicable	Enable Reachability for Station Domain Control	system	
SIP URI				
Primary Session Manager				
IPv4:	10.10.40.12	IPv6:		
Secondary Session Manager				
IPv4:		IPv6:		

Call Forwarding can be set from the **Enhanced Call Fwd** tab, as shown below. Other tabs can be checked, but for compliance testing the values were left as default, such as default value of three call appearance buttons that were used, this can be changed under the **Button Assignment** tab.

General Options (G) *	Feature Options (F)	Site Data (S)	Abbreviated Call Dialing (A)	Enhanced Call Fwd (E)
Button Assignment (B) Group Membership (M)				
	Forwarded Destination	Active		
Unconditional For Internal Calls To		<input type="checkbox"/>		
External Calls To		<input type="checkbox"/>		
Busy For Internal Calls To		<input type="checkbox"/>		
External Calls To		<input type="checkbox"/>		
No Reply For Internal Calls To		<input type="checkbox"/>		
External Calls To		<input type="checkbox"/>		
Required				

The **Feature Options** as set as shown below.

General Options (G) *		Feature Options (F)		Site Data (S)		Abbreviated Call Dialing (A)		Enhanced Call Fwd (E)																			
Button Assignment (B)		Group Membership (M)																									
Active Station Ringing		single		Auto Answer		none																					
MWI Served User Type		None		Coverage After Forwarding		system																					
Per Station CPN - Send Calling Number		None		Display Language		english																					
AUDIX Name		None		Hunt-to Station																							
Remote Soft Phone Emergency Calls		as-on-local		Loss Group		19																					
LWC Reception		spe		Survivable COR		internal																					
IP Phone Group ID				Time of Day Lock Table		None																					
Speakerphone				Voice Mail Number		6668																					
Short/Prefixed Registration Allowed		default		Music Source																							
EC500 State		enabled																									
Bridging Tone for This Extension		no																									
Features <table border="0"> <tr> <td><input type="checkbox"/> Always Use</td> <td><input type="checkbox"/> Idle Appearance Preference</td> </tr> <tr> <td><input type="checkbox"/> IP Audio Hairpinning</td> <td><input type="checkbox"/> IP SoftPhone</td> </tr> <tr> <td><input type="checkbox"/> Bridged Call Alerting</td> <td><input checked="" type="checkbox"/> LWC Activation</td> </tr> <tr> <td><input type="checkbox"/> Bridged Idle Line Preference</td> <td><input type="checkbox"/> CDR Privacy</td> </tr> <tr> <td><input checked="" type="checkbox"/> Coverage Message Retrieval</td> <td><input checked="" type="checkbox"/> Precedence Call Waiting</td> </tr> <tr> <td><input type="checkbox"/> Data Restriction</td> <td><input checked="" type="checkbox"/> Direct IP-IP Audio Connections</td> </tr> <tr> <td><input checked="" type="checkbox"/> Survivable Trunk Dest</td> <td><input type="checkbox"/> H.320 Conversion</td> </tr> <tr> <td><input type="checkbox"/> Bridged Appearance Origination Restriction</td> <td><input type="checkbox"/> IP Video</td> </tr> <tr> <td><input checked="" type="checkbox"/> Restrict Last Appearance</td> <td><input type="checkbox"/> Per Button Ring Control</td> </tr> </table>										<input type="checkbox"/> Always Use	<input type="checkbox"/> Idle Appearance Preference	<input type="checkbox"/> IP Audio Hairpinning	<input type="checkbox"/> IP SoftPhone	<input type="checkbox"/> Bridged Call Alerting	<input checked="" type="checkbox"/> LWC Activation	<input type="checkbox"/> Bridged Idle Line Preference	<input type="checkbox"/> CDR Privacy	<input checked="" type="checkbox"/> Coverage Message Retrieval	<input checked="" type="checkbox"/> Precedence Call Waiting	<input type="checkbox"/> Data Restriction	<input checked="" type="checkbox"/> Direct IP-IP Audio Connections	<input checked="" type="checkbox"/> Survivable Trunk Dest	<input type="checkbox"/> H.320 Conversion	<input type="checkbox"/> Bridged Appearance Origination Restriction	<input type="checkbox"/> IP Video	<input checked="" type="checkbox"/> Restrict Last Appearance	<input type="checkbox"/> Per Button Ring Control
<input type="checkbox"/> Always Use	<input type="checkbox"/> Idle Appearance Preference																										
<input type="checkbox"/> IP Audio Hairpinning	<input type="checkbox"/> IP SoftPhone																										
<input type="checkbox"/> Bridged Call Alerting	<input checked="" type="checkbox"/> LWC Activation																										
<input type="checkbox"/> Bridged Idle Line Preference	<input type="checkbox"/> CDR Privacy																										
<input checked="" type="checkbox"/> Coverage Message Retrieval	<input checked="" type="checkbox"/> Precedence Call Waiting																										
<input type="checkbox"/> Data Restriction	<input checked="" type="checkbox"/> Direct IP-IP Audio Connections																										
<input checked="" type="checkbox"/> Survivable Trunk Dest	<input type="checkbox"/> H.320 Conversion																										
<input type="checkbox"/> Bridged Appearance Origination Restriction	<input type="checkbox"/> IP Video																										
<input checked="" type="checkbox"/> Restrict Last Appearance	<input type="checkbox"/> Per Button Ring Control																										

Under **Button Assignment** the number of Call Appearances can be set, for testing the default of three was configured as shown. Once all is configured click on **Done** at the bottom right.

System		cm101x		Extension		3191			
Template		9620SIP_DEFAULT_CM_10_1		Set Type		9620SIP			
Port		S000010		Security Code					
Name		3191, AscomMYCO							
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		Phone View					
1		call-appr							
2		call-appr							
3		call-appr							
4		None							
5		None							
6		None							
*Required									
<div>Done</div>									

Click on **Commit** to save all the user changes.

User Profile | Edit | 3191@greanep.sil6.avaya.com

Commit & ContinueCommitCancel

IdentityCommunication ProfileMembershipContacts

Communication Profile Password

PROFILE SET : Primary

Communication Address

PROFILES

Session Manager Profile

Avaya Breeze® Profile

CM Endpoint Profile

* System :cm101x

* Profile Type :Endpoint

Use Existing Endpoints :☐

* Extension :3191

Template :9620SIP_DEFAULT_C

* Set Type :9620SIP

Security Code :Enter Security Code

Port :S000010

Voice Mail Number :6668

Preferred Handle :Select

Calculate Route Pattern :☐

Sip Trunk :aar

SIP URI :Select

Enhanced Callr-Info Display for 1-line phones :☐

Delete on Unassign from User or on Delete :☒

Override Endpoint Name and Localized Name :☒

Allow H.323 and SIP Endpoint Dual Registration :☐

PG; Reviewed:
SPOC 11/21/2023

Solution & Interoperability Test Lab Application Notes
©2023 Avaya Inc. All Rights Reserved.

23 of 51
Myco4_CM101

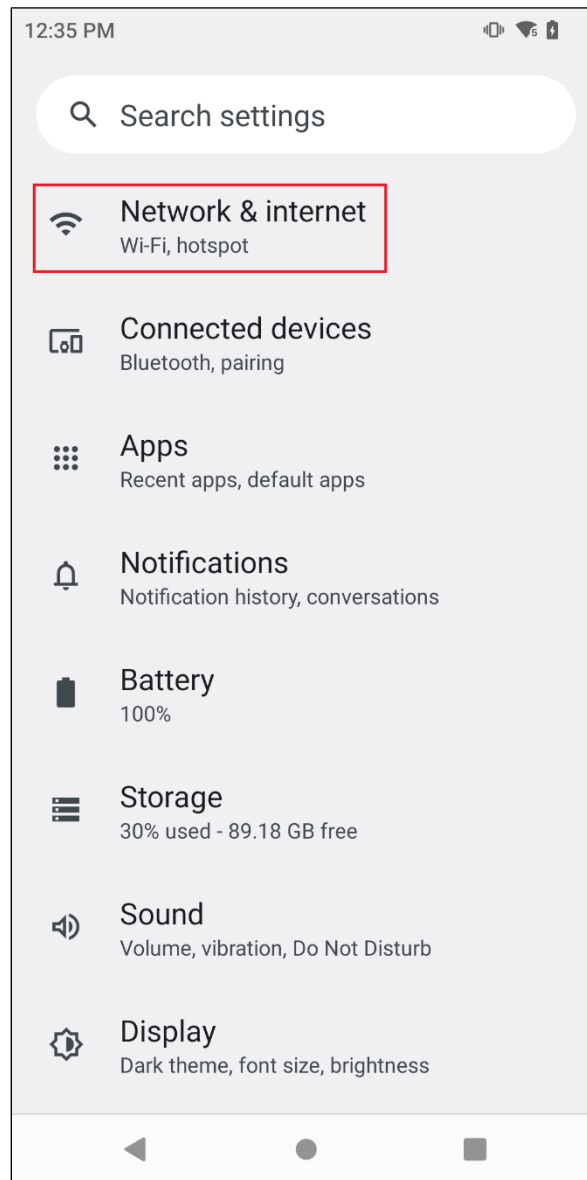
7. Configure Ascom Myco 4 Smartphone

This section describes how to configure the Myco 4 smartphone. It is implied that the Wi-Fi network has been configured and operational.

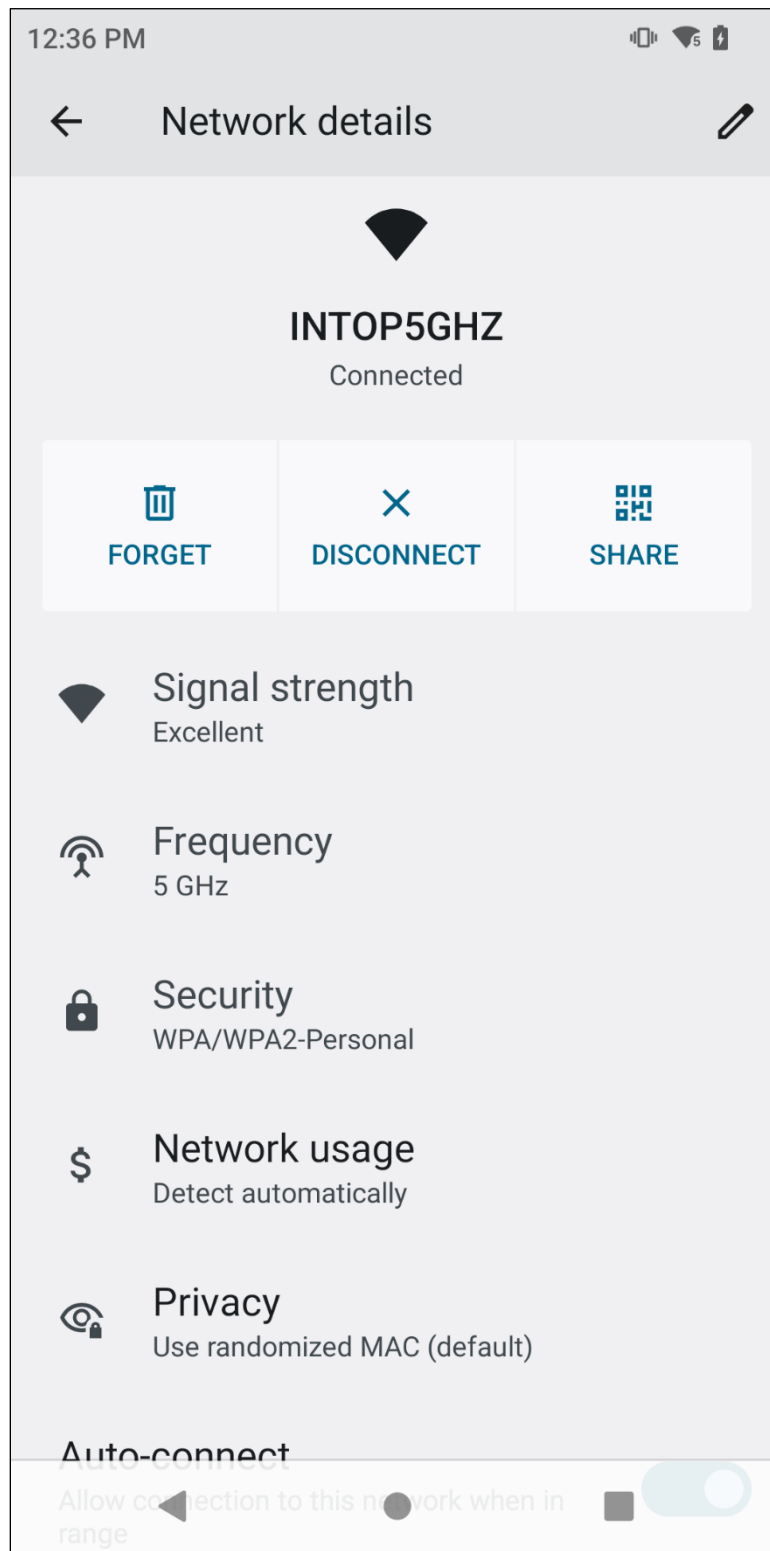
Note: The wireless router configuration is outside the scope of these Application Notes.

7.1. Configure Wi-Fi network on Myco 4

Access to the Myco 4 smartphone is from the smartphone device in question. From the smartphone navigate to **Android Settings** → **Network & Internet** → **Wi-Fi**.

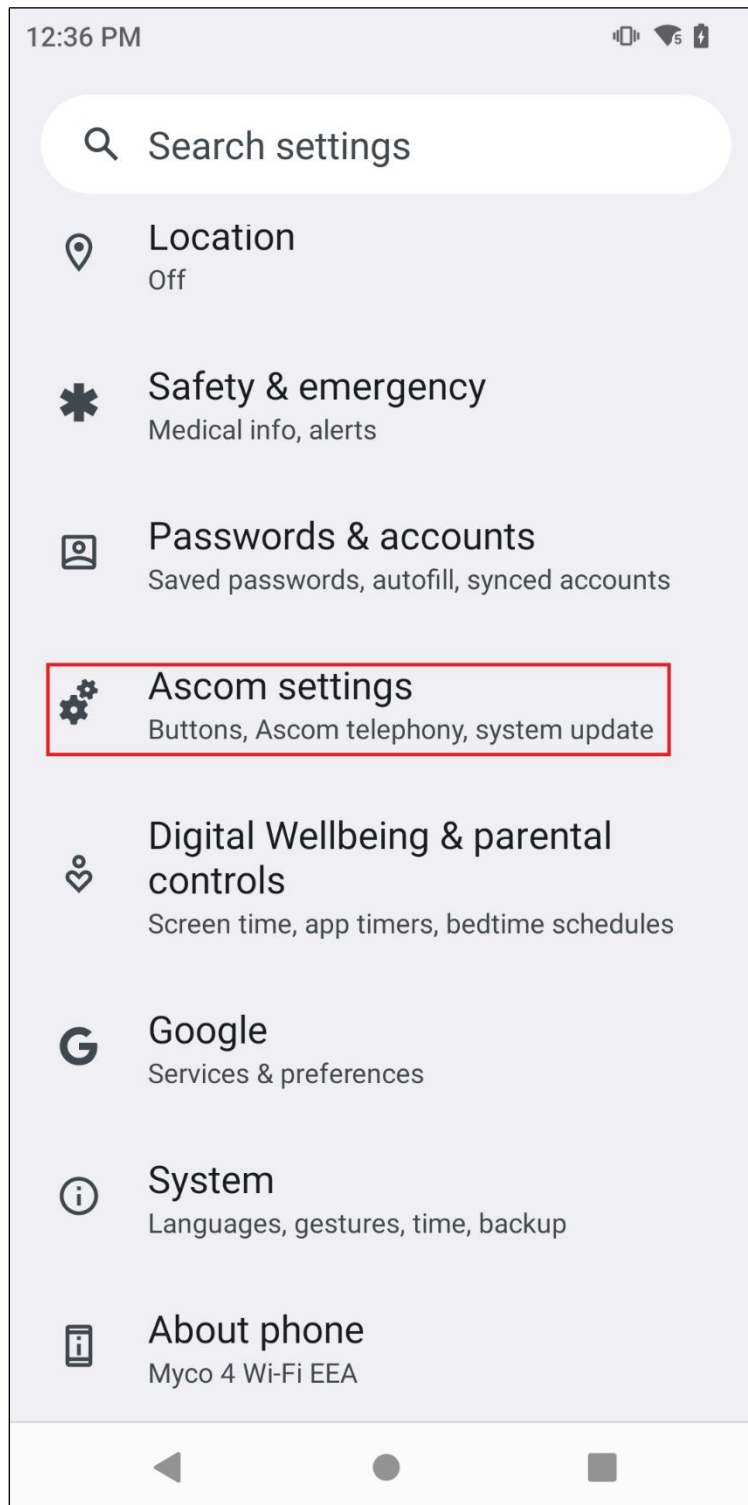


The following screen displays information on the network such as the wireless network that it is connected to.

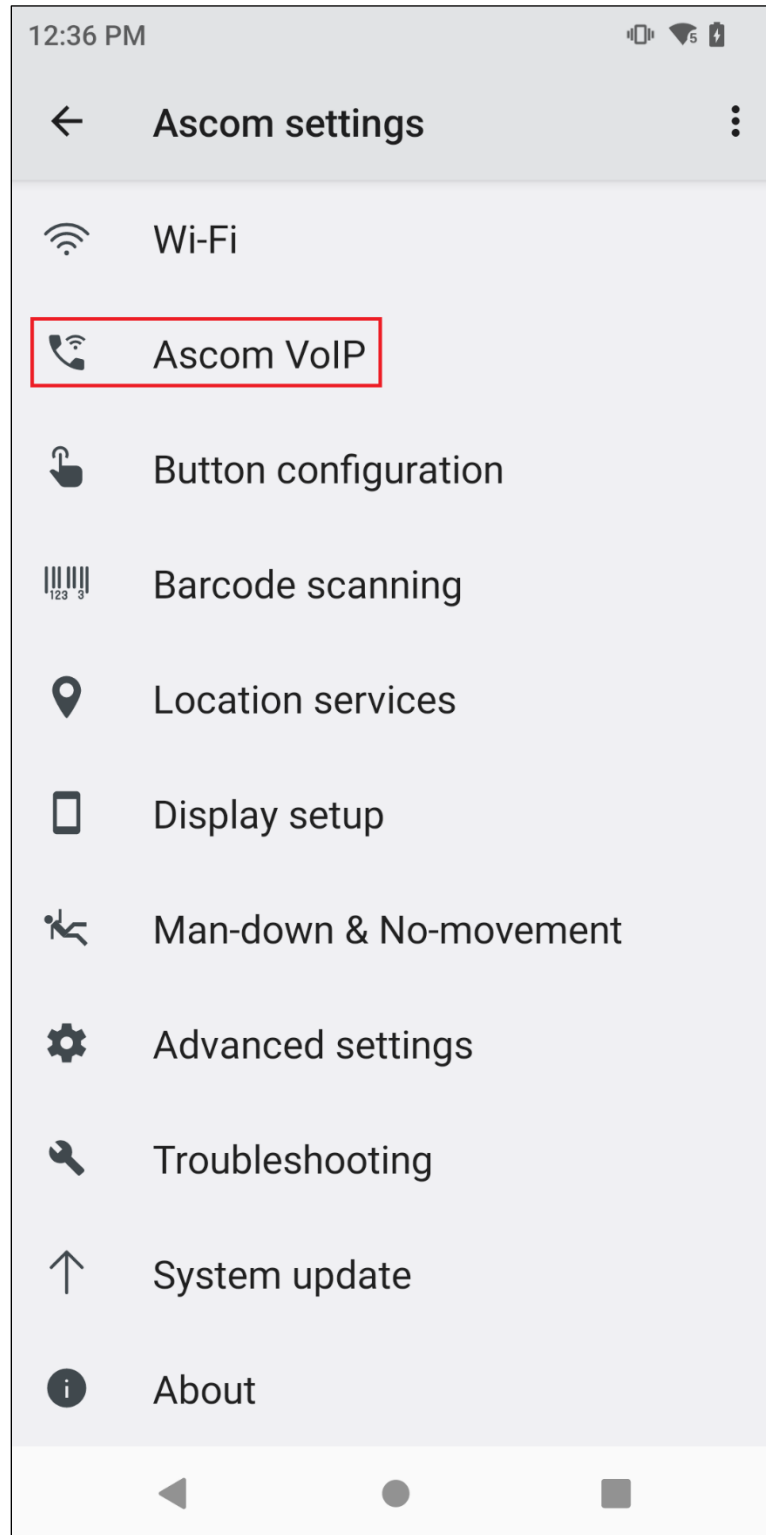


7.2. Configure SIP settings

From the Myco 4 smartphone navigate to **Android Settings** → **Ascom settings**.



Click on **Ascom VoIP**.



Configure the following values.

- **SIP Transport** For compliance testing **TCP** was selected as shown below.
- **Primary SIP Proxy** IP address of Session Manager.
- **Listening port** **5070**.
- **SIP Register expiration** **120** (this will be negotiated with the PBX).
- **Endpoint ID** This is the extension number.

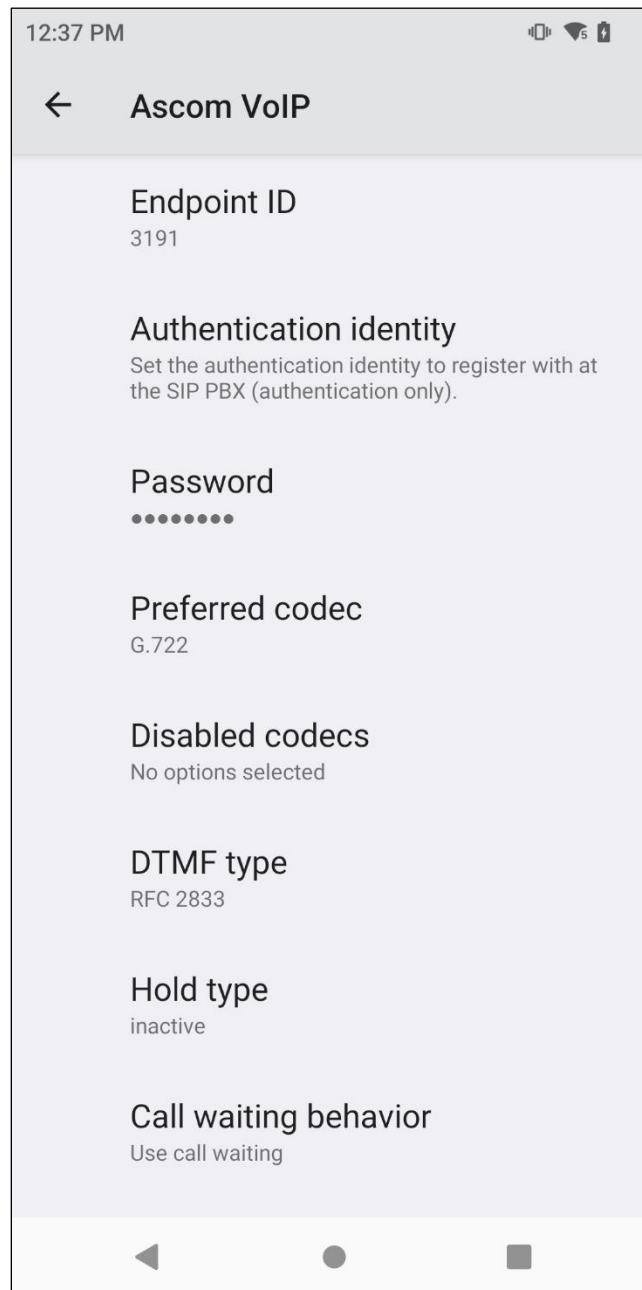
The screenshot shows a mobile application interface for configuring SIP settings. At the top, the status bar displays the time 12:37 PM and icons for signal, Wi-Fi, and battery. Below the status bar is a header with a back arrow and the title "Ascom VoIP". The main content area is a light gray box with several configuration fields, each with a title and a value:

- SIP Transport**: TCP
- Primary SIP proxy**: 10.10.40.12
- Secondary SIP proxy**: Define the optional SIP PBX, if the handset fails to register with the primary SIP PBX. Specify an IP address, a domain name, or an IP address with a port number. Examples of valid formats are: pbx1.mydomain.com or 192.168.1.1:5060
- Listening port**: 5070
- SIP proxy ID**: Define the ID to be used as the Primary/Secondary SIP message headers (optional).
- SIP Register expiration**: 120
- Endpoint ID**: 3191

At the bottom of the screen is a white navigation bar with three icons: a back arrow, a circle, and a square.

Scroll down to display and set the following.

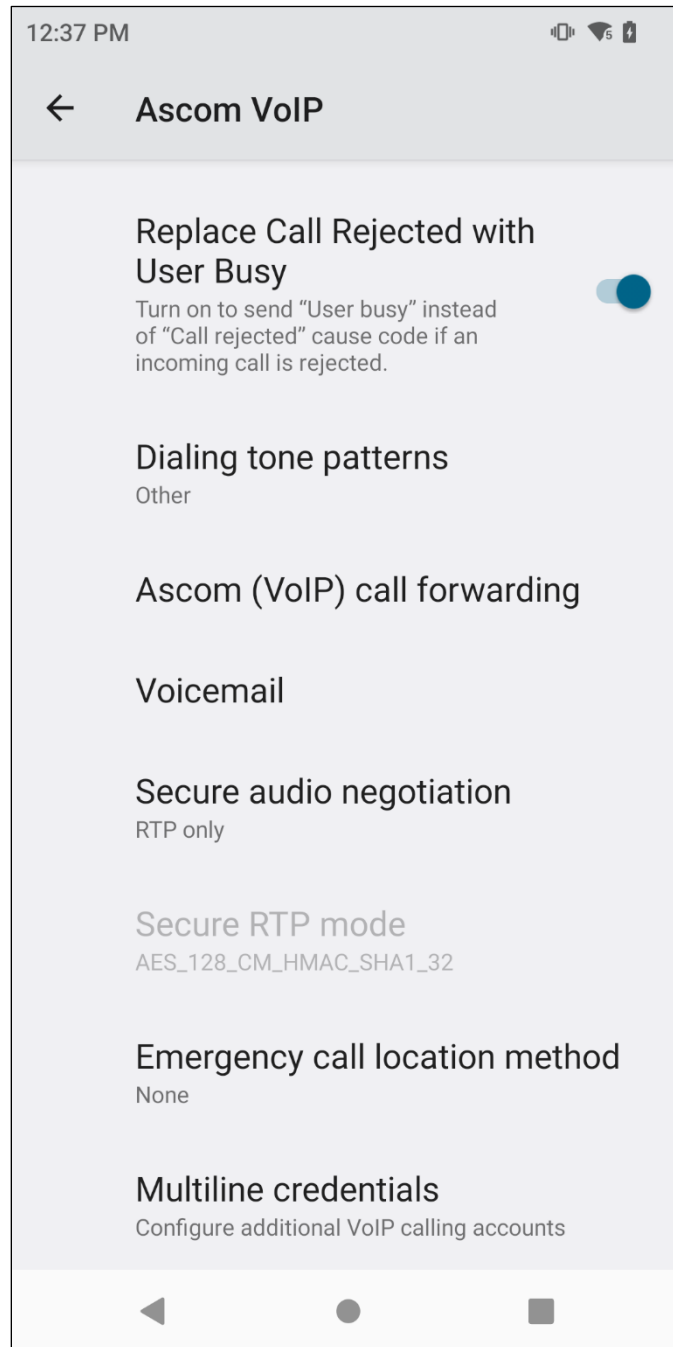
- **Password** Password assigned to the endpoint in **Section 6.2**.
- **Preferred codec** This setting will depend on the country, **G.722** was chosen for compliance testing.
- **DTMF type** **RFC 2833** is chosen, again for this testing.
- **Hold type** Was left as **inactive** for compliance testing.
- **Call waiting behavior** This can be set to **Use call waiting** (preferable) or Reject call.



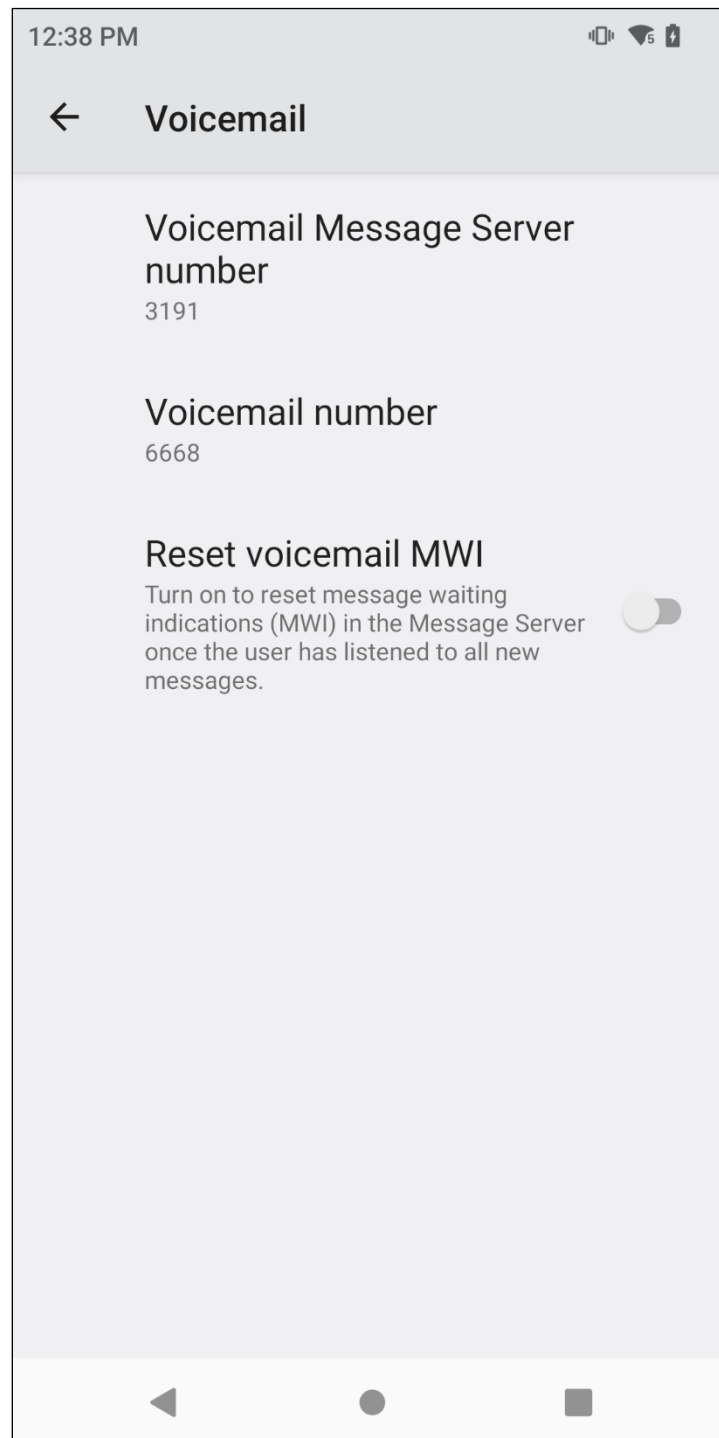
Scroll down to display and set the following.

- **Replace Call Rejected with User Busy** Turn to **on** for compliance testing (preferred setting).
- **Dialing tone patterns** Left as **Other**.

Click on **Voicemail** to enter the details to subscribe for message waiting updates.



Enter the extension number for the **Voicemail Message Server number** and enter the voicemail number to call to voicemail for the **Voicemail number**. The **Reset voicemail MWI** was left as shown below.

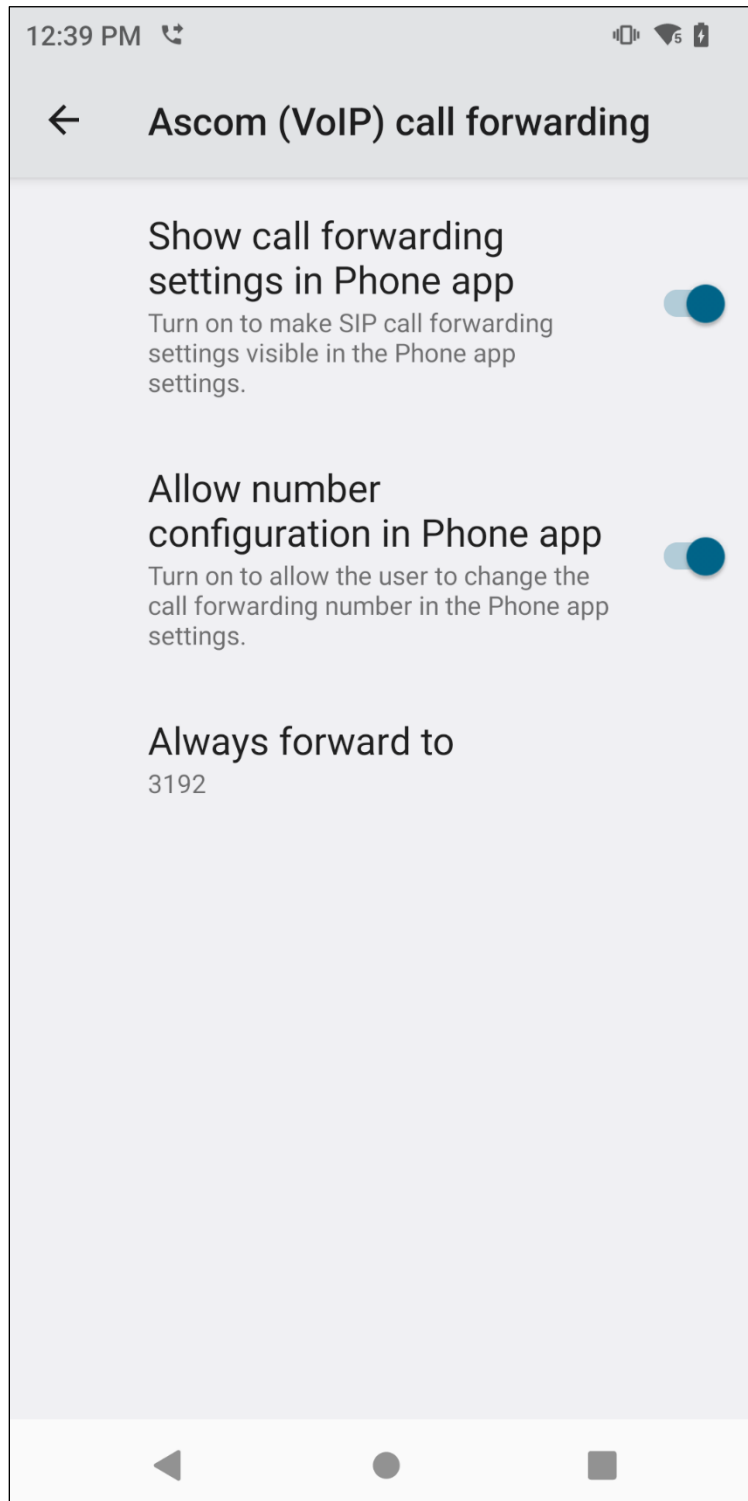


The screenshot shows a mobile application interface for Voicemail settings. At the top, the status bar displays the time 12:38 PM and icons for signal strength, Wi-Fi, and battery. Below the status bar is a header with a back arrow and the title "Voicemail". The main content area has a light gray background and contains three settings:

- Voicemail Message Server number**: The value "3191" is entered in the text field.
- Voicemail number**: The value "6668" is entered in the text field.
- Reset voicemail MWI**: A toggle switch is shown in the "off" position. Below the title is a descriptive text: "Turn on to reset message waiting indications (MWI) in the Message Server once the user has listened to all new messages."

At the bottom of the screen is a white navigation bar with three icons: a back arrow, a home circle, and a recent apps square.

Local Call Forwarding for “call forward all calls” is now available with Myco 4 and this can be accessed by switching on the **Show call forwarding settings in Phone app**, as shown below.



7.3. Configure Multi Device Access

Multi Device Access is used to allow the same user register on multiple devices, this may be all Myco 4 smartphones or a mixture of Avaya endpoints and Myco 4 phones.

The configuration of Multi Device Access for Myco 4 is to change the **Endpoint ID** and **Password** on the bottom of the screen below to that of the user that is to be used on each Myco 4 device. The example below shows this handset being changed to use the **3101** user. Note that the setting for **Max. Simultaneous Devices** will need to be configured accordingly as explained in **Section 6.2**.

12:40 PM

← Ascom VoIP

SIP Transport
TCP

Primary SIP proxy
10.10.40.12

Secondary SIP proxy
Define the optional SIP PBX, if the handset fails to register with the primary SIP PBX. Specify an IP address, a domain name, or an IP address with a port number.

Examples of valid formats are:
pbx1.mydomain.com or 192.168.1.1:5060

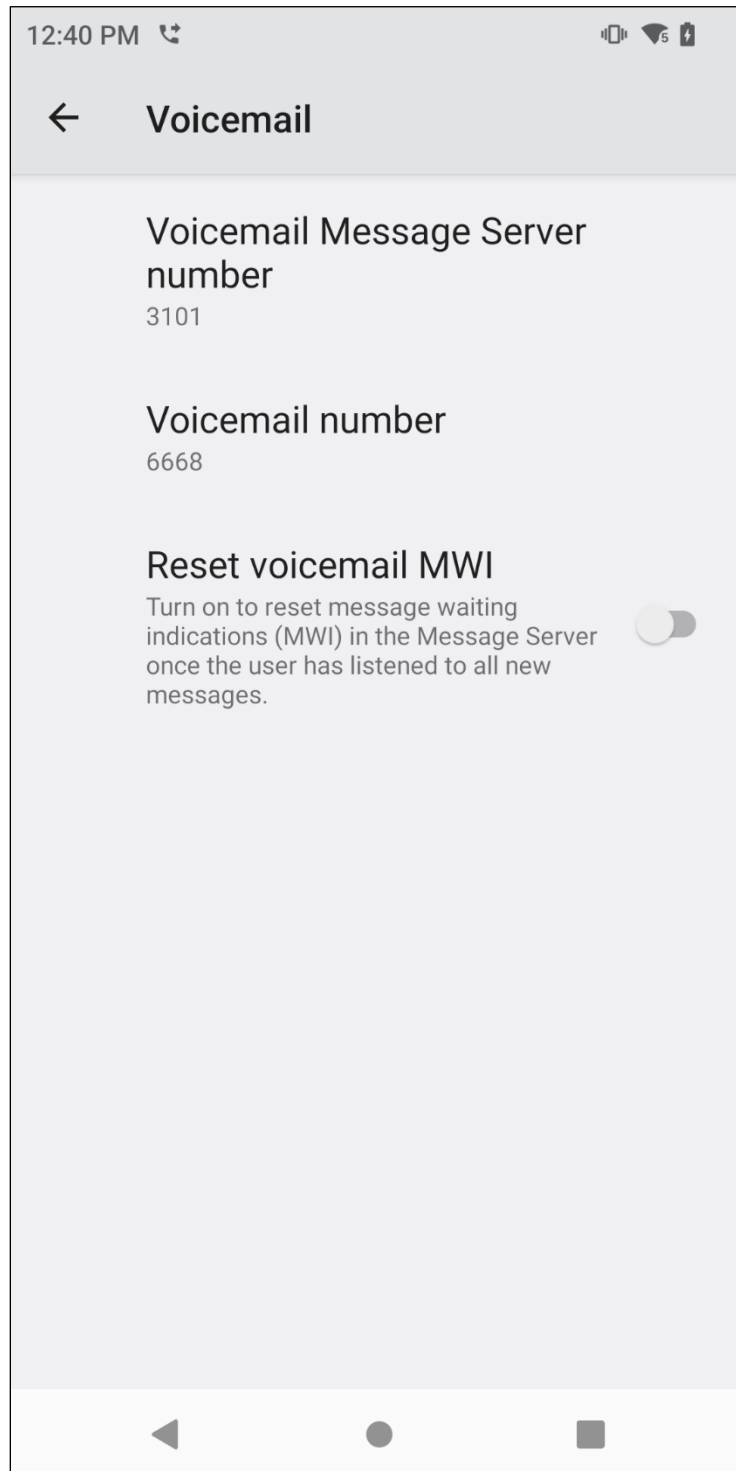
Listening port
5070

SIP proxy ID
Define the ID to be used as the Primary/Secondary SIP message headers (optional).

SIP Register expiration
120

Endpoint ID
3101

The **Voicemail Message Server number** must also be changed to match that of the primary registration device, in this case **3101**.



7.4. Configure Multiline Device

One of the Ascom handsets was configured as a ‘multiline’ device, which means that it is capable of registering multiple SIP users/extensions. A primary line and then up to four additional lines are supported. For compliance testing 3194 was registered as the primary line with 3195 – 3198 as the additional lines.

The primary line is configured the same as any other single line device, as per **Section 7.2**. The Endpoint ID is set to the primary line **3194**.

14:00

← Ascom VoIP

SIP Transport
TCP

Primary SIP proxy
10.10.40.12

Secondary SIP proxy
Define the optional SIP PBX, if the handset fails to register with the primary SIP PBX. Specify an IP address, a domain name, or an IP address with a port number.

Examples of valid formats are:
pbx1.mydomain.com or 192.168.1.1:5060

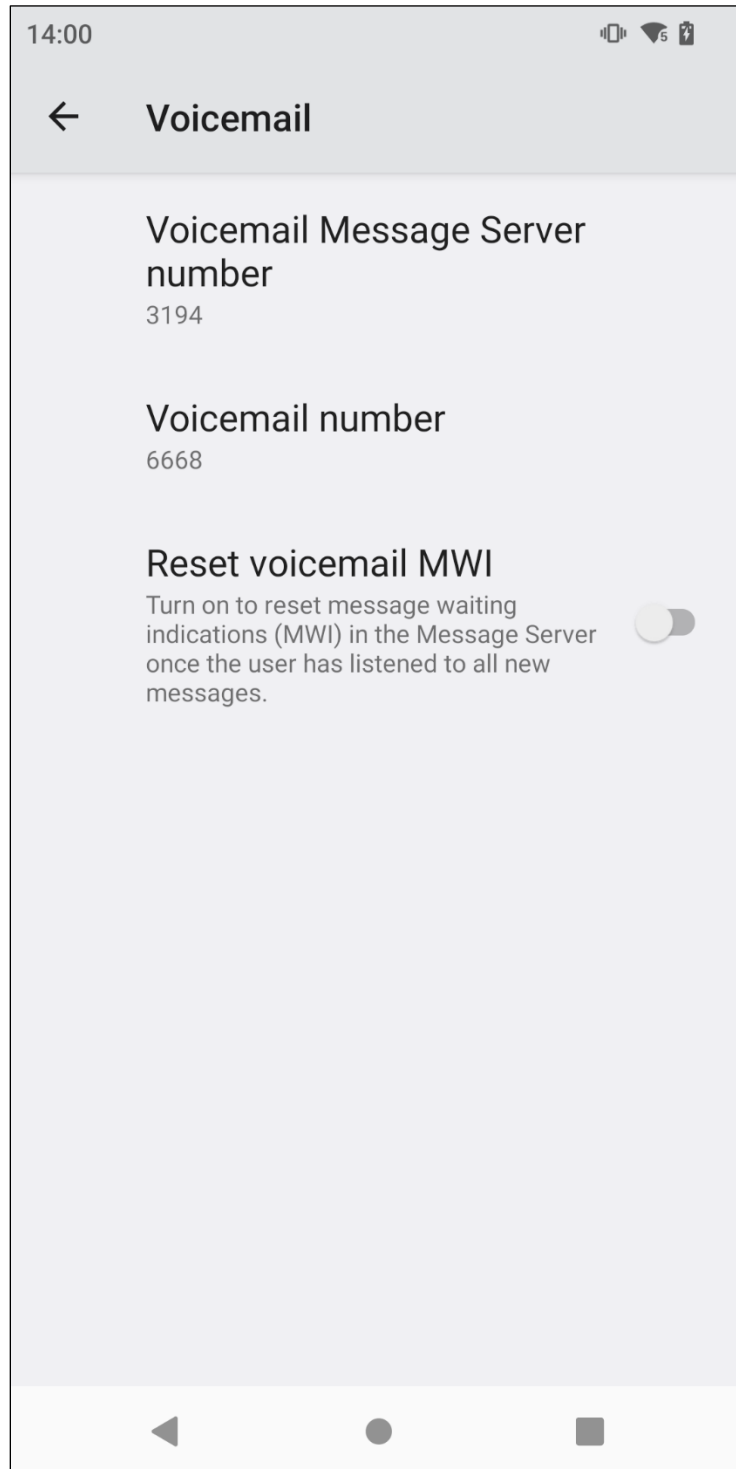
Listening port
5070

SIP proxy ID
Define the ID to be used as the Primary/Secondary SIP message headers (optional).

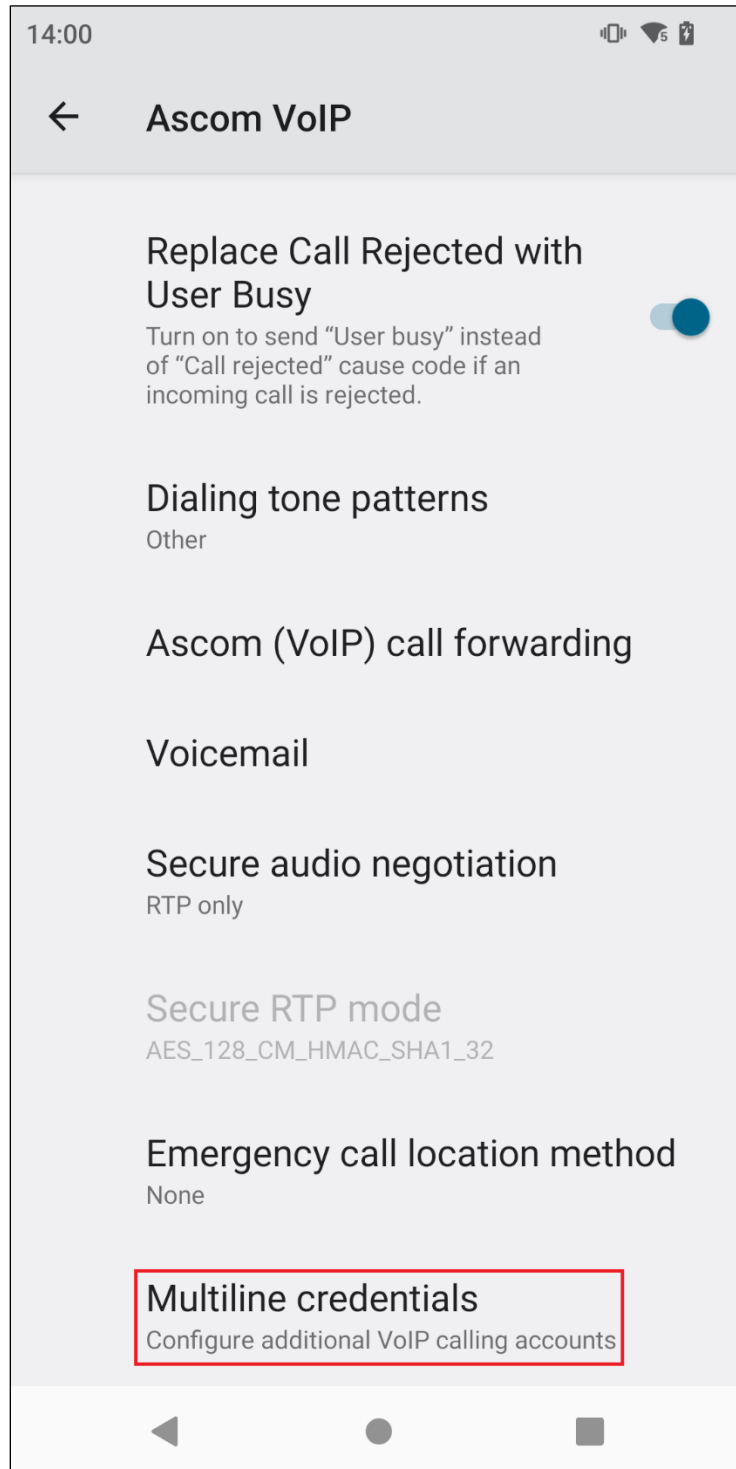
SIP Register expiration
120

Endpoint ID
3194

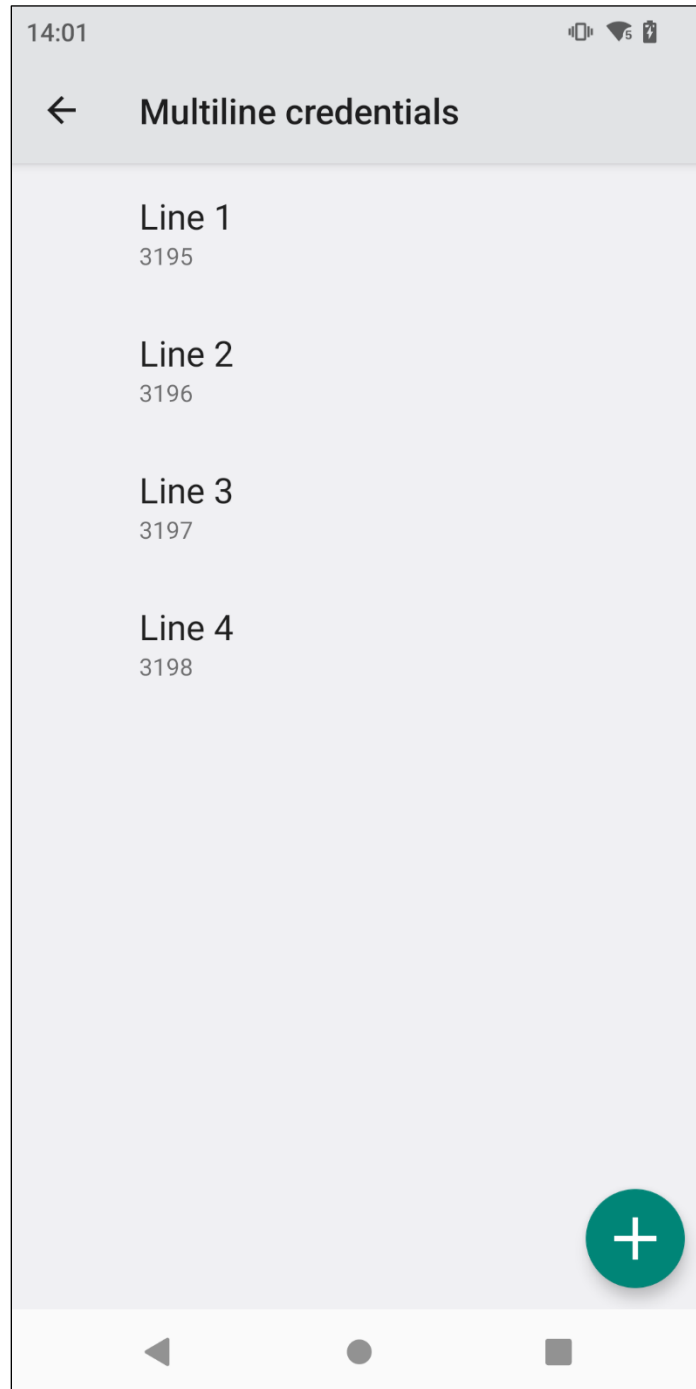
The voicemail is configured for the primary number only, as shown below.



Scroll down to **Multiline credentials** and click on it.



Add the various additional lines, as outlined **3195 – 3198** were assigned as these additional lines.



Each additional line can be configured with the correct **Endpoint ID** and **Display name**, along with the correct **Password** as per what was configured on System Manager under Users.

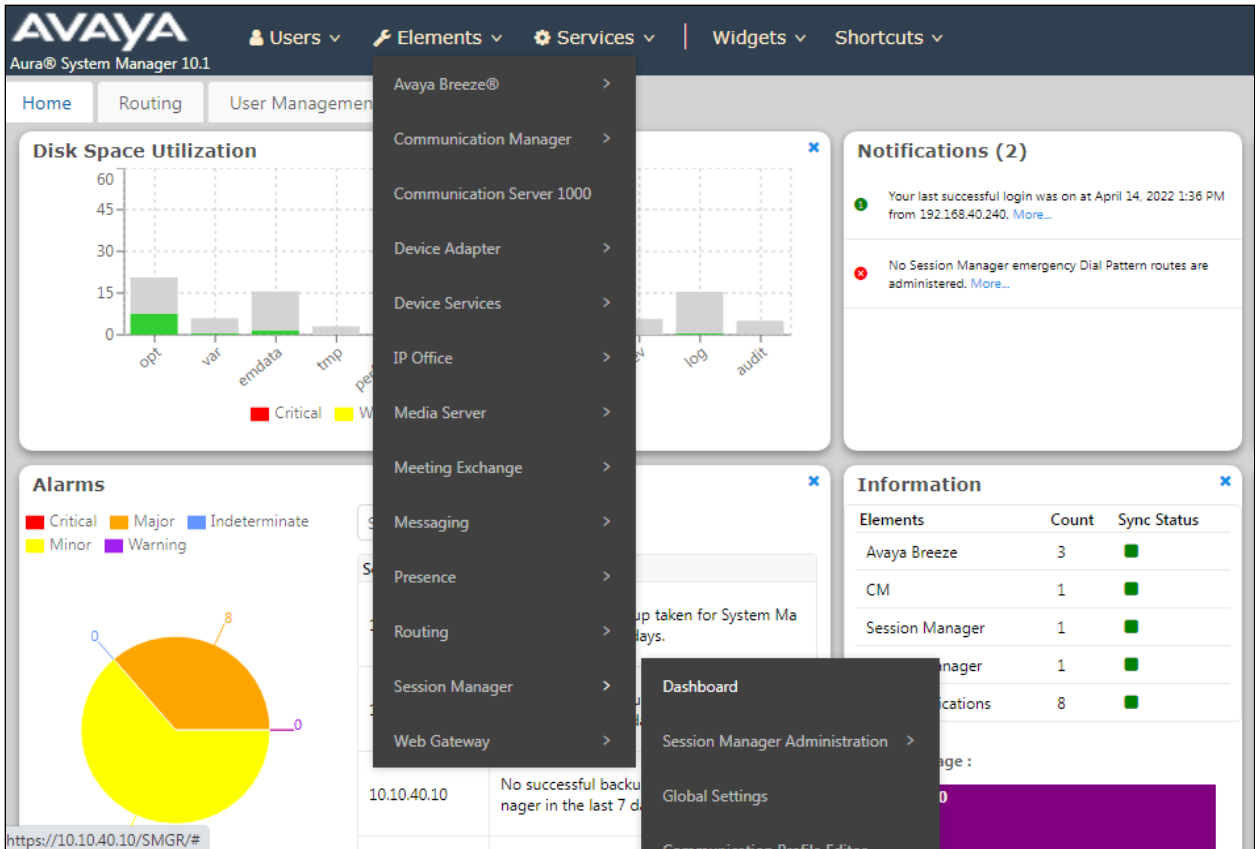
The screenshot shows a mobile application interface for configuring a line. At the top, the status bar displays the time 14:01 and icons for signal, Wi-Fi, and battery. Below the status bar is a header with a back arrow, the text 'Line 1', and a three-dot menu icon. The main content area is light gray and contains four configuration fields: 'Display name' with the value 'Multi 3195', 'Endpoint ID' with the value '3195', 'Authentication identity' (empty), and 'Password' (masked with eight dots). At the bottom of the screen is a white navigation bar with three icons: a back arrow, a circle, and a square.

8. Verification Steps

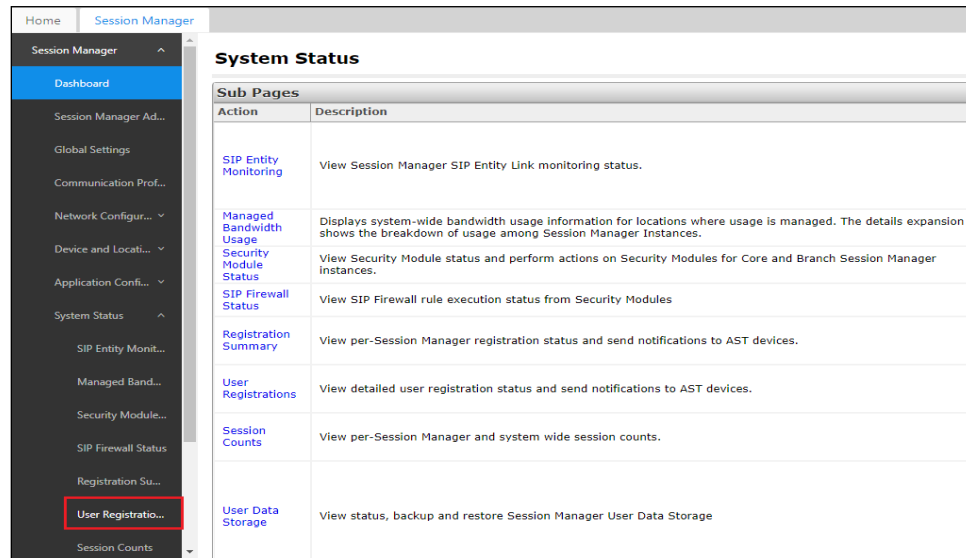
The following steps can be taken to ensure that connections between Myco 4 and Session Manager and Communication Manager are up.

8.1. Session Manager Registration

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

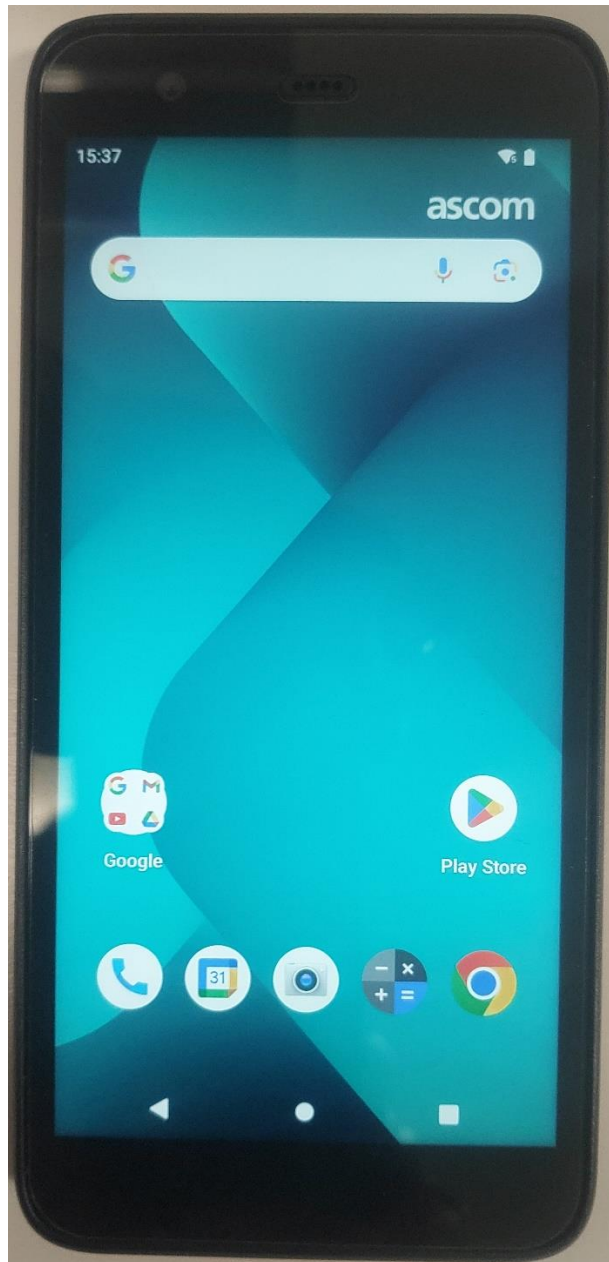


The Ascom Myco 4 handsets should show up as being registered, as shown below. Each Myco handset has an IP Address associated with it and there is a tick in the **Registered Prim** box. Note that there are four separate handsets registered, **3191**, **3192** and **3193**. There is also a multiline endpoint registered which has five extensions associated with it, **3194** (primary), **3195 – 3198** (additional).

User Registrations											
Select rows to send notifications to devices. Click on Details column for complete registration status.											
<div> <div>View ▾</div> <div>Default</div> <div>Export</div> <div>Force Unregister</div> <div>AST Device Notifications:</div> <div>Reboot</div> <div>Reload ▾</div> <div>Failback</div> <div>As of 2:15 PM</div> <div>Advanced Search ▾</div> </div>											
<div> <div>25 Items</div> <div>Show 15 ▾</div> <div>Filter: Enable</div> </div>											
<input type="checkbox"/>	Details	Address ▾	First Name	Last Name	Actual Location	IP Address	Policy	Shared Control	Simult. Devices	AST Device	Registered Prim
<input type="checkbox"/>	Show	3198@greanep.sil6.avaya.com	AscomMYCO	3198	DevConnectGalway	10.10.40.237	fixed	<input type="checkbox"/>	1/1	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Show	3197@greanep.sil6.avaya.com	AscomMYCO	3197	DevConnectGalway	10.10.40.237	fixed	<input type="checkbox"/>	1/1	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Show	3196@greanep.sil6.avaya.com	AscomMYCO	3196	DevConnectGalway	10.10.40.237	fixed	<input type="checkbox"/>	1/1	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Show	3195@greanep.sil6.avaya.com	AscomMYCO	3195	DevConnectGalway	10.10.40.237	fixed	<input type="checkbox"/>	1/1	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Show	3194@greanep.sil6.avaya.com	AscomMYCO	3194	DevConnectGalway	10.10.40.237	fixed	<input type="checkbox"/>	1/1	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Show	3193@greanep.sil6.avaya.com	AscomMYCO	3193	DevConnectGalway	10.10.40.220	fixed	<input type="checkbox"/>	1/1	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Show	3192@greanep.sil6.avaya.com	AscomMYCO	3192	DevConnectGalway	10.10.40.231	fixed	<input type="checkbox"/>	1/1	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Show	3191@greanep.sil6.avaya.com	AscomMYCO	3191	DevConnectGalway	10.10.40.193	fixed	<input type="checkbox"/>	1/1	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Show	3121@greanep.sil6.avaya.com	AgentOne	Wspaces	DevConnectGalway	10.10.40.159	fixed	<input type="checkbox"/>	1/1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> (AC)
<input type="checkbox"/>	Show	3110@greanep.sil6.avaya.com	Workplace	Windows	DevConnectGalway	10.10.40.242	fixed	<input type="checkbox"/>	1/1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> (AC)
<input type="checkbox"/>	Show	3101@greanep.sil6.avaya.com	SIP	Phone	DevConnectGalway	10.10.40.187	fixed	<input type="checkbox"/>	1/3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> (AC)
<input type="checkbox"/>	Show	---	Vantage01	K175	---	---	fixed	<input type="checkbox"/>	0/1	<input type="checkbox"/>	<input type="checkbox"/>

8.2. Ascom Myco 4 Registration

The Ascom Myco 4 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.



9. Conclusion

These Application Notes describe the configuration steps required for Ascom Myco 4 to successfully interoperate with Avaya Aura® Communication Manager R10.1 and Avaya Aura® Session Manager R10.1 by registering Myco 4 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. *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 on the support pages at <https://www.ascom-ws.com/AscomPartnerWeb/Templates/WebLogin.aspx> (login account for the Ascom Partner Extranet required).

Appendix A

Signaling Group

display signaling-group 11	SIGNALING GROUP	Page 1 of 3
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: greaney.sil6.avaya.com		
Incoming Dialog Loopbacks: eliminate	Bypass If IP Threshold Exceeded? n	
DTMF over IP: rtp-payload	RFC 3389 Comfort Noise? n	
Session Establishment Timer(min): 3	Direct IP-IP Audio Connections? y	
Enable Layer 3 Test? y	IP Audio Hairpinning? n	
H.323 Station Outgoing Direct Media? n	Initial IP-IP Direct Media? n	
	Alternate Route Timer(sec): 6	

Trunk Group Page 1

display trunk-group 11	TRUNK GROUP	Page 1 of 5
Group Number: 11	Group Type: sip	CDR Reports: y
Group Name: SIP PHONES	COR: 1	TN: 1
Direction: two-way	Outgoing Display? n	TAC: *811
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): 900

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
                               UII Treatment: shared
                               Maximum Size of UII 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 UI 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 UII: 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
```

Appendix B

Topology Hiding under **Configuration Profiles** can be used to make changes to the SIP messages coming into the enterprise. The **To**, **From** and **Request Line** headers are all overwritten with the SIP realm or domain that was used during compliance testing. This domain was called **greanep.sil6.avaya.com** and it can be seen below as the overwritten value for the **IP/Domain** criteria. It is best to make a copy of the original Topology Hiding profile called **default** and rename it (**sm101x** was chosen as shown in the example below). Once this is created click on **Edit** at the bottom of the screen to make the necessary changes.

Session Border Controller for Enterprise



EMS Dashboard

Software Management

Device Management

Backup/Restore

System Parameters

Configuration Profiles

- Domain DoS
- Server Interworking
- Media Forking
- Routing
- Topology Hiding**
- Signaling Manipulation
- URI Groups
- SNMP Traps
- Time of Day Rules
- FGDN Groups
- Reverse Proxy
- Policy

Topology Hiding Profiles: sm101x

Add

Topology Hiding Profiles

- default
- cisco_th_profile
- Avaya
- Cardeasy
- Bill (PSTN)
- SM8.0
- SM8.1
- sm101x**

RenameCloneDelete

Click here to add a description.

Topology Hiding

Header	Criteria	Replace Action	Overwrite Value
Refer-To	IP/Domain	Auto	---
Referred-By	IP/Domain	Auto	---
Via	IP/Domain	Auto	---
From	IP/Domain	Overwrite	greanep.sil6.avaya.com
SDP	IP/Domain	Auto	---
Request-Line	IP/Domain	Overwrite	greanep.sil6.avaya.com
Record-Route	IP/Domain	Auto	---
To	IP/Domain	Overwrite	greanep.sil6.avaya.com

Edit

PG; Reviewed:
SPOC 11/21/2023

Solution & Interoperability Test Lab Application Notes
©2023 Avaya Inc. All Rights Reserved.

47 of 51
Myco4_CM101

The Topology Hiding profile is then assigned to an **End Point Flow**. Chose the End Point Flow that is coming from the PSTN to the enterprise. This is called **To PSTN PG** below, click in **Edit** as shown to make changes to the Flow.

Manipulation
URI Groups
SNMP Traps
Time of Day Rules
FGDN Groups
Reverse Proxy
Policy
URN Profile
Recording Profile
H248 Profile
▸ Services
▸ Domain Policies
▸ TLS Management
▾ Network & Flows
Network Management
Media Interface
Signaling Interface
End Point Flows
Session Flows
Advanced Options
▸ DMZ Services
▸ Monitoring & Logging

End Point Flows

Subscriber Flows
Server Flows

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
1	From PSTN PG	*	Sig_Int	Sig-EXT-SIM-PSTN	SM-PSTN-RTP	sm101x	View Clone Edit Delete

SIP Server: SMvmpg 8.1

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
1	To PSTN PG from Aura 8.1	*	Sig-EXT-SIM-PSTN	Sig_Int	SM-PSTN-RTP	SM-PSTN-PG	View Clone Edit Delete

SIP Server: sm101x

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
1	To PSTN PG from Aura 10.1	*	Sig-EXT-SIM-PSTN	Sig_Int	SM-PSTN-RTP	SM-PSTN-PG	View Clone Edit Delete

The Topology Hiding Profile created on the previous page is chosen as the **Topology Hiding Profile** for this Flow.

Edit Flow: To PSTN PG from Aura 10.1 X

Flow Name	<input type="text" value="To PSTN PG from Aura 10.1"/>
SIP Server Profile	<input type="text" value="sm101x"/> ▼
URI Group	<input type="text" value="*"/> ▼
Transport	<input type="text" value="*"/> ▼
Remote Subnet	<input type="text" value="*"/>
Received Interface	<input type="text" value="Sig-EXT-SIM-PSTN"/> ▼
Signaling Interface	<input type="text" value="Sig_Int"/> ▼
Media Interface	<input type="text" value="Med_Int"/> ▼
Secondary Media Interface	<input type="text" value="None"/> ▼
End Point Policy Group	<input type="text" value="SM-PSTN-RTP"/> ▼
Routing Profile	<input type="text" value="SM-PSTN-PG"/> ▼
Topology Hiding Profile	<input type="text" value="sm101x"/> ▼
Signaling Manipulation Script	<input type="text" value="None"/> ▼
Remote Branch Office	<input type="text" value="Any"/> ▼
Link Monitoring from Peer	<input type="checkbox"/>
FQDN Support	<input type="checkbox"/>
FQDN	<input type="text"/>

Finish

Appendix C

Registration timers are set under **Session Manager → Device Settings**. These are the values for the **Default Group**. Note that the minimum setting for both **Subscription Expiration Timer** and **Registration Expiration Timer** is **600 (secs)**. This means that if the third-party device is set any lower than 600 secs, Session Manager will return a “session interval is too brief” and negotiate to 600 secs.

The screenshot displays the Avaya Aura System Manager 10.1 web interface. The top navigation bar includes the Avaya logo, user information (Users), and various menu items (Elements, Services, Widgets, Shortcuts). A search bar and a user profile icon are also present. The main content area is titled "Device Settings Group" and features a breadcrumb trail: General | Server Timer | Endpoint Timer | Maintenance Settings | VoIP Monitoring Manager | Volume Settings | VLAN Parameters | DIFFSERV/QoS Parameters | 802.1 P/Q Parameters. Below the breadcrumb trail, there are tabs for "General", "Server Timer", "Endpoint Timer", "Maintenance Settings", and "VoIP Monitoring Manager". The "General" tab is currently selected, showing fields for "Name" (Default Group), "Description" (Default Group), "Group Type" (Location Group selected, Terminal Group unselected), and "Terminal Group Number". The "Server Timer" tab shows "Subscription Expiration Timer (secs)" with a maximum of 86400 and a minimum of 600, and "Registration Expiration Timer (secs)" with a maximum of 3600 and a minimum of 600. The "Endpoint Timer" tab shows "Line Reservation Timer (secs)" (30), "Reactive Monitoring Interval (secs)" (60), and "Timer B (sec)" (4). The "Maintenance Settings" and "VoIP Monitoring Manager" tabs are also visible but not expanded.

©2023 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.