



Avaya Solution & Interoperability Test Lab

Application Notes for configuring Ascom i63 with Avaya Aura® Communication Manager and Avaya Aura® Session Manager – Issue 1.0

Abstract

These Application Notes describe the configuration steps for provisioning Ascom's i63 VoWiFi handsets to interoperate with Avaya Aura® Communication Manager and Avaya Aura® Session Manager.

Readers should pay attention to **Section 2**, in particular the scope of testing as outlined in **Section 2.1** as well as any observations noted in **Section 2.2**, to ensure that their own use cases are adequately covered by this scope and results.

Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

1. Introduction

These Application Notes describe the configuration steps for provisioning Ascom's i63 VoWiFi (i63) handsets to interoperate with Avaya Aura® Communication Manager R8.1 and Avaya Aura® Session Manager R8.1. Ascom's i63 handsets are configured to register with Session Manager and are configured with the 9620 SIP endpoint template. The Ascom i63 handsets then behave as third-party SIP extensions on Communication Manager. The handsets are able to make/receive internal and PSTN/external calls and have full voicemail and other telephony features available on Communication Manager.

2. General Test Approach and Test Results

The interoperability compliance testing evaluates the ability of Ascom i63 handsets to make and receive calls to and from Avaya H.323, Avaya SIP, and PSTN endpoints. Avaya Aura® Messaging was used to allow users leave voicemail messages and to demonstrate Message Waiting Indication and DTMF on the Ascom i63 handsets.

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 i63 VoWiFi handsets did not include use of any specific encryption features as requested by Ascom.

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

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

2.1. Interoperability Compliance Testing

The compliance testing included the test scenarios shown below. Note that when applicable, all tests were performed with Avaya SIP, Avaya H.323, Avaya Digital, Ascom i63 and PSTN endpoints.

- Basic Calls
- Session Refresh Timer
- Long Duration Call
- Hold, Retrieve and Brokering (Toggle)
- Feature Access Code dialing
- Attended and Blind Transfer
- 3-way 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 i63 handset being the EC500 destination
- Multi-Device Access (MDA)
- Do Not Disturb (Locally Controlled)
- Calling Line Name/Identification
- Codec Support (G.711, G.729, G.722)
- DTMF Support
- Voice Mail, Message Waiting Indication
- Serviceability

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

2.2. Test Results

The tests were all functional in nature and performance testing and redundancy testing were not included. All test cases passed successfully with the following observations/limitations noted below:

1. All compliance testing was done using UDP and TCP (preferred) as the transport protocol.
2. In the blind transfer scenario involving three i63 handsets, where A is the calling, B is the called and transfer-from and C is the transfer-to parties. Upon ringing, the display on the

transfer-to party C showed “Redirected x y” where “x” is the extension number of the calling party A and “y” is the name of the transfer-from party B. According to Ascom, transfer-to party C displayed information conveyed by Communication Manager, and “redirected” was displayed because the INVITE included a History-Info header. This was deemed to be ‘as per design’ by Ascom.

3. Ascom i63 handset supports third party conference, which is, i63 makes two calls simultaneously and conferences the calls locally.
4. When using the EC500 (concurrent call) feature, if an i63 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 i63 handset users, calls may be answered by a cellular user’s voicemail instead of following the coverage criteria in Communication Manager.
5. When an i63 handset is configured as an EC500 destination for an Avaya endpoint, an incoming call to the Avaya endpoint will ring both the Avaya endpoint and the i63 handset. When the call is declined on the i63 handset, the Avaya endpoint continues to ring as per normal design.
6. Negotiation of G.722 between endpoints, such as the Ascom i63, requires support for the codec to be configured on Communication Manager.
7. When multiple voice messages are left for an i63 handset, the handset shows the total number of messages as only “1” in the display even though there are multiple messages. This is because there is no counter information sent in the NOTIFY from Avaya Aura® Messaging.
8. For Multi-Device Access (MDA), the i63 needs to be configured using and registering through Endpoint ID. Also, the MWI configuration has to be identical on all i63 handsets that are configured for MDA. Refer to **Section 7.3** for details.
9. Per design, i63 handsets do not have a redial button. User needs to use “Call List” and redial the numbers.
10. When outgoing calls are configured to be restricted for an i63 handset on Communication Manager, the i63 display showed “No Channel Available” when user attempted to make an outbound call.
11. 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

Support from Avaya is available by visiting the website <http://support.avaya.com> and a list of product documentation can be found in **Section 10** of these Application Notes. Technical support for the Ascom i63 wireless handsets can be obtained through a local Ascom supplier or Ascom global technical support:

- Email: support@ascom.com
- Help desk: +46 31 559450

3. Reference Configuration

Figure 1 shows the network topology during compliance testing. The Ascom i63 VoWiFi handsets connect to an Ascom approved wireless access point which is placed on the LAN. The i63 handsets register with Session Manager to be able to make/receive calls with the Avaya H.323, and SIP endpoints on Communication Manager and with the PSTN. The handsets are configured by Ascom Windows Portable Device Manager (WinPDM) using the Ascom Desktop Programmer DP1.

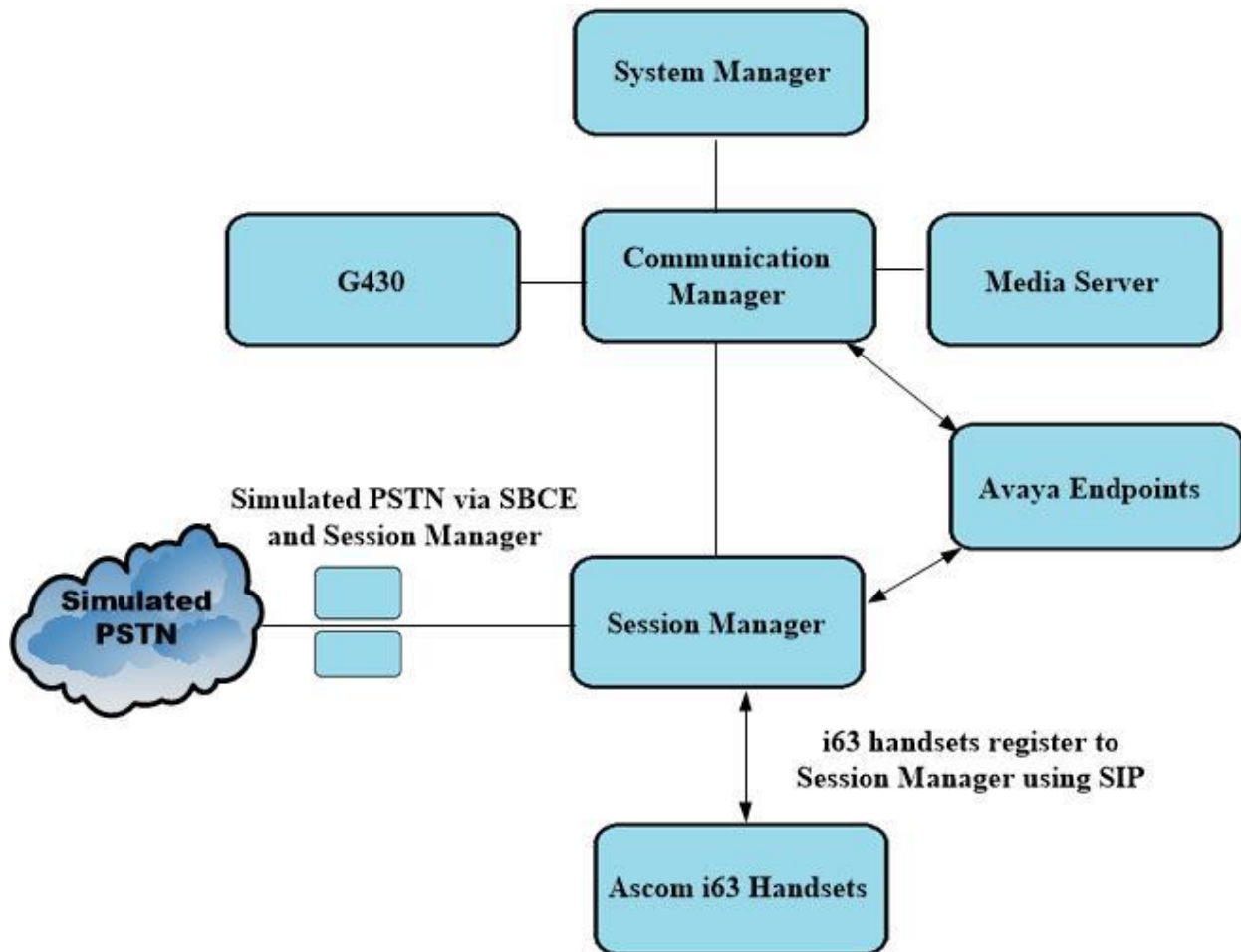


Figure 1: Network Solution of Ascom i63 with Avaya Aura® Communication Manager R8.1 and Avaya Aura® Session Manager R8.1

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 running on a virtual server	System Manager 8.1.2.0 Build No. – 8.1.0.0.733078 Software Update Revision No: 8.1.2.0.0611261 Feature Pack 2
Avaya Aura® Session Manager running on a virtual server	Session Manager R8.1 Build No. – 8.1.2.0.812039
Avaya Aura® Communication Manager running on a virtual server	R8.1.2.0 – FP2 R018x.00.0.890.0 Update ID 01.0.890.0-26095
Avaya Aura® Media Server	8.0.0.169
Avaya Media Gateway G430	41.16.0/1
Avaya 9408 Digital	2.00
Avaya 96x1 SIP Deskphone	7.1.2.0.14
Avaya J179 H323 Deskphone	6.8304
Avaya Session Border Controller for Enterprise (to facilitate simulated PSTN)	8.0.0.0-19-16991
Ascom Equipment	Software / Firmware Version
Ascom Device Manager running on Windows PC (WinPDM)	3.13.4
Ascom i63 Wireless Handset	V2.2.8
Ascom approved Wi-Fi Access Point	Ascom approved software version

5. Configure Avaya Aura® Communication Manager

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

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

The following sections go through the following.

- System Parameters
- Dial Plan Analysis
- Feature Access Codes
- Network Region
- IP Codec
- 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: V17	Software Package: Enterprise	
Location: 2	System ID (SID): 1	
Platform: 28	Module ID (MID): 1	
		USED
Platform Maximum Ports: 48000		168
Maximum Stations: 36000		44
Maximum XMOBILE Stations: 36000		0
Maximum Off-PBX Telephones - EC500: 41000		2
Maximum Off-PBX Telephones - OPS: 41000		20
Maximum Off-PBX Telephones - PBFMC: 41000		0
Maximum Off-PBX Telephones - PVFMC: 41000		0
Maximum Off-PBX Telephones - SCCAN: 0		0
Maximum Survivable Processors: 313		1

5.2. Configure Dial Plan Analysis

Use the **change dialplan analysis** command to configure the dial plan using the parameters shown below. Extension numbers (**ext**) are those beginning with **21**. Feature Access Codes (**fac**) use digits **8** and **9** and use characters ***** or **#**.

change dialplan analysis						Page 1 of 12		
DIAL PLAN ANALYSIS TABLE								
Location: all						Percent Full: 5		
Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type
21	4	ext						
3	4	udp						
8	1	fac						
9	1	fac						
*8	4	dac						
*	3	fac						
#	3	fac						

5.3. Configure Feature Access Codes

Use the **change feature-access-codes** command to configure access codes which can be entered from i63 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	
Call Forwarding Enhanced Status: *73			Act: *74	
			Deactivation: #74	
Call Park Access Code: *02				
Call Pickup Access Code: *09				
CAS Remote Hold/Answer Hold-Unhold Access Code:				
CDR Account Code Access Code: *14				
Change COR Access Code:				
Change Coverage Access Code:				
Conditional Call Extend Activation:			Deactivation:	
Contact Closure			Open Code:	
			Close Code:	

5.4. Configure Network Region

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

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

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 i63 Handsets. During compliance testing the codecs **G.711A**, **G.729A** and **G.722** were tested.

```
change ip-codec-set 1                                         Page 1 of 2
                                                                IP MEDIA PARAMETERS
    Codec Set: 1
    Audio      Silence      Frames      Packet
    Codec      Suppression   Per Pkt   Size (ms)
1: G.711A      n            2         20
2: G.729A      n            2         20
3: G.722.2      n            1         20
4: G.722-64K   2            2         20
5:
6:
7:
    Media Encryption      Encrypted SRTCP: enforce-unenc-srtcp
1: 1-srtp-aescm128-hmac80
2: none
3:
4:
```

5.6. Configuration of Coverage Path and Hunt Group for voicemail

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

Don't Answer is set to **y**: The coverage path will be used in the event the phone set is not answered.

Number of Rings is set to **4**: The coverage path will be used after 4 rings.

Point 1 is set to **h6**: Hunt Group 6 is utilised by this coverage path.

```
display coverage path 1

                                COVERAGE PATH

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

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

COVERAGE POINTS
  Terminate to Coverage Pts. with Bridged Appearances? n
  Point1: h6                Rng:      Point2:
  Point3:                    Point4:
  Point5:                    Point6:
```

The hunt group used for compliance testing is shown below. Note that on **Page 1** the **Group Extension** is **6666**, which is used to dial for messaging and **Group Type** is set to **ucd-mia**.

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

                                HUNT GROUP

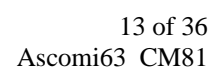
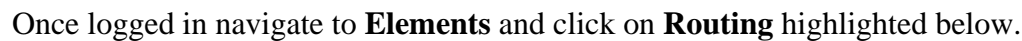
                                Group Number: 6                ACD? n
                                Group Name: AA Messaging V7      Queue? n
                                Group Extension: 6666           Vector? n
                                Group Type: ucd-mia             Coverage Path: 1
                                TN: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

SIP URI::
```

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

display hunt-group 6		Page 2 of 60	
HUNT GROUP			
Message Center: sip-adjunct			
Voice Mail Number	Voice Mail Handle	Routing Digits	
		(e.g., AAR/ARS Access Code)	
6666	6666	9	

The Ascom i63 VoWiFi handsets are added to Session Manager as SIP users. To make changes on Session Manager a web session is established to System Manager. Log into System Manager by opening a web browser and navigating to <https://<System Manager FQDN>/SMGR>. Enter the appropriate credentials for the **User ID** and **Password** and click on **Log On**.



6.1. Domains and Locations

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

6.1.1. Display the Domain

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

The screenshot shows the Avaya Aura System Manager 8.1 interface. The left sidebar has a 'Routing' section with 'Domains' selected. The main panel is titled 'Domain Management' and contains a table with one item: 'devconnect.local' of type 'sip'. The table has columns for Name, Type, and Notes. The Notes column contains 'devconnect.local'.

Name	Type	Notes
devconnect.local	sip	devconnect.local

6.1.2. Display the Location

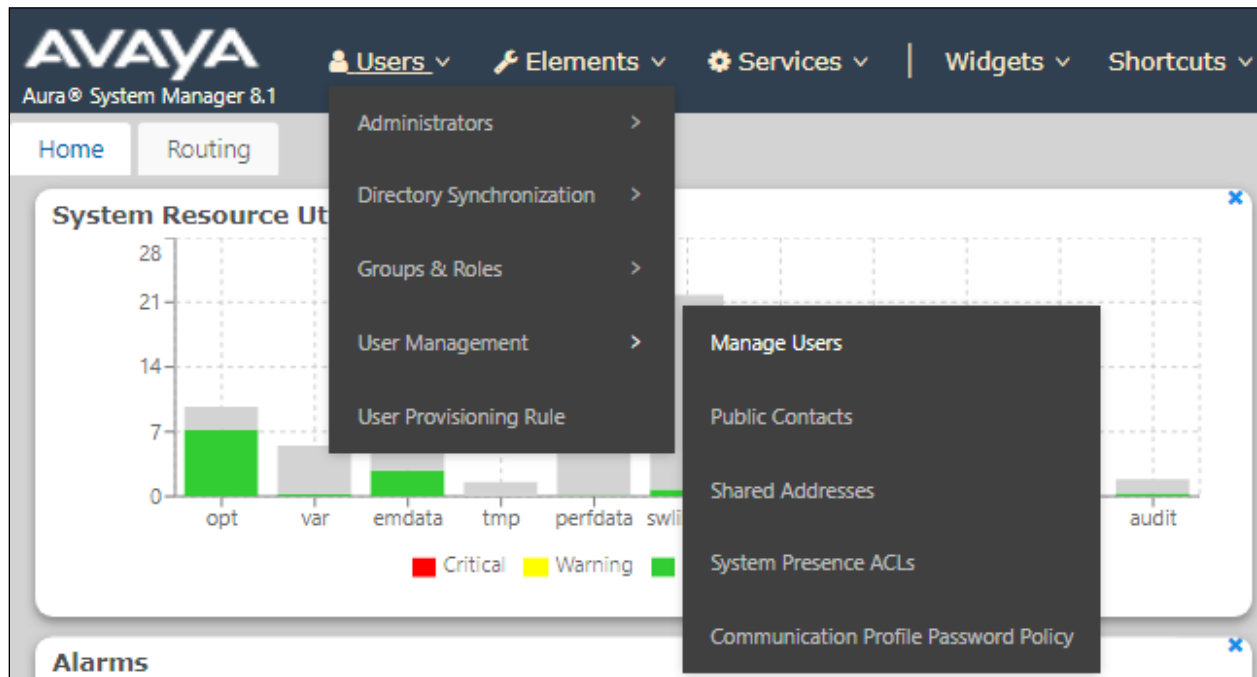
Select **Locations** from the left window and this will display the location setup. The example below shows the location **DevConnectLab** which was used for compliance testing. If a location is not already in place, then one must be added to include the IP address range of the Avaya solution. Click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

The screenshot shows the Avaya Aura System Manager 8.1 interface. The left sidebar has a 'Routing' section with 'Locations' selected. The main panel is titled 'Location' and contains a table with one item: 'DevConnectLab'. The table has columns for Name, Correlation, and Notes. The Notes column contains 'DevConnect Lab in Galway'.

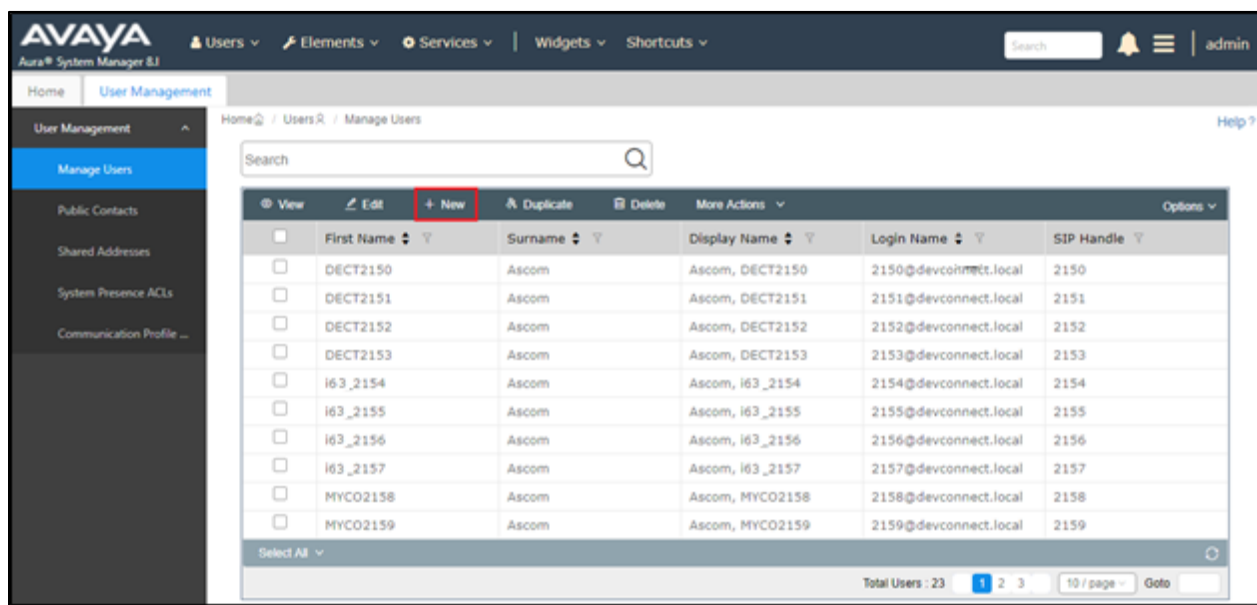
Name	Correlation	Notes
DevConnectLab		DevConnect Lab in Galway

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

The screenshot shows the 'User Profile | Edit | 2154@devconnect.local' interface with the 'Identity' tab selected. The left sidebar has 'Basic Info' selected. The main form contains the following fields:

- User Provisioning Rule: [Dropdown]
- Last Name: [Text: Ascom]
- Last Name (Latin Translation): [Text: Ascom]
- First Name: [Text: i63_2154]
- First Name (Latin Translation): [Text: i63_2154]
- Login Name: [Text: 2154@devconnect.local]
- Middle Name: [Text: Middle Name Of User]
- Description: [Text: Description Of User]
- Email Address: [Text: Email Address Of User]
- Password: [Text]
- User Type: [Dropdown: Basic]
- Confirm Password: [Text]
- Localized Display Name: [Text: Ascom, i63_2154]
- Endpoint Display Name: [Text: Ascom, i63_2154]
- Title Of User: [Text: Title Of User]
- Language Preference: [Dropdown: English (United States)]
- Time Zone: [Dropdown]
- Employee ID: [Text: Employee Id Of User]
- Department: [Text: Department Of User]

Under the **Communication Profile** tab enter **Communication Profile Password** and **Confirm Password**, note that this password is required when configuring the i63 handset in **Section 7.1**.

The screenshot shows the 'User Profile | Edit | 2150@devconnect.local' interface with the 'Communication Profile' tab selected. The left sidebar has 'Communication Profile Password' selected. The main form shows 'PROFILE SET: Primary' and 'Communication Address'. A modal dialog titled 'Comm-Profile Password' is open, containing:

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

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

User Profile | Edit | 2154@devconnect.local

Commit & Continue Commit

Identity Communication Profile Membership Contacts

Communication Profile Password

PROFILE SET: Primary

Communication Address

PROFILES

Session Manager Profile

CM Endpoint Profile

Edit + New Delete

Type Handle Domain

Select All

Total: 1 1 10 / page

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

Communication Address Add/Edit

* Type : Avaya SIP

*Fully Qualified Address : 2154 @ devconnect.local

Cancel OK

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.

Identity	Communication Profile	Membership	Contacts
Communication Profile Password			
PROFILE SET: Primary ▼			
Communication Address			
PROFILES			
Session Manager Profile <input checked="" type="checkbox"/>			
CM Endpoint Profile <input checked="" type="checkbox"/>			
SIP Registration			
* Primary Session Manager :		SM81vmpg	<input type="text"/> ⓘ
Secondary Session Manager :		Start typing...	<input type="text"/> ⓘ
Survivability Server :		Start typing...	<input type="text"/> ⓘ
Max. Simultaneous Devices :		1	▼
Block New Registration When Maximum Registrations		<input type="checkbox"/>	
Active? *			
Application Sequences			
Origination Sequence :		CMAPPSEQ	▼
Termination Sequence :		CMAPPSEQ	▼

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).

Application Sequences

Origination Sequence :

CMAPPSEQ

Termination Sequence :

CMAPPSEQ

Emergency Calling Application Sequences

Emergency Calling Origination Sequence :

Select

Emergency Calling Termination Sequence :

Select

Call Routing Settings

* Home Location :

DevConnectLab

Conference Factory Set :

Select

Call History Settings

Enable Centralized Call History? : ☐

Ensure that **CM Endpoint Profile** is selected in the left window. Select the Communication Manager that is configured for the **System** and choose the **9620SIP_DEFAULT_CM_8_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 i63 handset. Click on **Endpoint Editor** to configure the buttons and features for that handset on Communication Manager.

User Profile | Edit | 2154@devconnect.local

Commit & Continue

Commit

Cancel

Identity

Communication Profile

Membership

Contacts

Communication Profile Password

PROFILE SET: Primary

Communication Address

PROFILES

Session Manager Profile

CM Endpoint Profile

* System :

CM80vmpg

* Profile Type :

Endpoint

Use Existing Endpoints :

☐

* Extension :

2154

Template :

9620SIP_DEFAULT_CM_8_1

* Set Type :

9620SIP

* Sub Type :

Select

* Terminal Number :

0000

System ID :

Enter System Id

Security Code :

Enter Security Code

Port :

IP

Voice Mail Number :

6666

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 User :

☒

Override Endpoint Name and Localized Name :

☒

Allow H.323 and SIP Endpoint Dual Registration :

☐

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 i63 handset. This may vary depending on what level of access/permissions the handset has been given. Other tabs can be checked but for compliance testing the values were left as default. Click on Done (not shown) to complete.

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

The screenshot shows the 'General Options (G)' tab in a configuration window. The window has several tabs: 'General Options (G)', 'Feature Options (F)', 'Site Data (S)', 'Abbreviated Call Dialing (A)', 'Enhanced Call Fwd (E)', 'Button Assignment (B)', and 'Group Membership (M)'. The 'General Options (G)' tab is active. It contains the following fields and values:

- Class of Restriction (COR):** 1
- Emergency Location Ext:** 2154
- Tenant Number:** 1
- SIP Trunk:** Qaar
- Coverage Path 1:** 1
- Lock Message:** ☐
- Multibyte Language:** Not Applicable
- Class Of Service (COS):** 1
- Message Lamp Ext.:** 2154
- Type of 3PCC Enabled:** None
- Coverage Path 2:** (empty)
- Localized Display Name:** Ascom, i62_2154
- Enable Reachability for Station Domain Control:** (empty)
- SIP URI:** (empty)
- Primary Session Manager:** (empty)
- IPv4:** (empty)
- IPv6:** (empty)

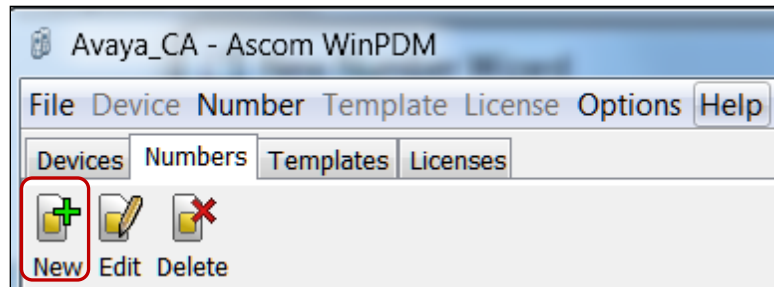
Once the **CM Endpoint Profile** is completed correctly, click on **Commit** to save the new user.

The screenshot shows the 'User Profile | Edit | 2154@devconnect.local' window. It has tabs for 'Identity', 'Communication Profile', 'Membership', and 'Contacts'. The 'Communication Profile' tab is active. It contains the following fields and values:

- Communication Profile Password:** PROFILE SET: Primary
- Communication Address:** (empty)
- PROFILES:**
 - Session Manager Profile: ☐
 - CM Endpoint Profile: ☒
- * System:** CM80vmpg
- * Profile Type:** Endpoint
- Use Existing Endpoints:** ☐
- * Extension:** 2154
- Template:** 9620SIP_DEFAULT_CM_8_
- * Set Type:** 9620SIP
- * Sub Type:** Select
- * Terminal Number:** 0 0 0 0
- System ID:** Enter System Id
- Security Code:** Enter Security Code
- Port:** IP
- Voice Mail Number:** 6666
- Preferred Handle:** Select
- Calculate Route Pattern:** ☐

7. Configure Ascom i63 VoWiFi Handsets

The configuration of the i63 handsets is done using Ascom's WinPDM software installed on a PC. Attach the Ascom DeskTop Programmer DP1 USB cradle to a PC on which the Ascom WinPDM has been installed. Insert the handset to be configured in the DP1 USB Cradle, start the Ascom Device Manager, select the **Numbers** tab and click **New** icon highlighted below.



Place a new i63 to be programmed into the cradle and the following screen should appear automatically. Select **Edit parameters** and click on **Next** as shown below.

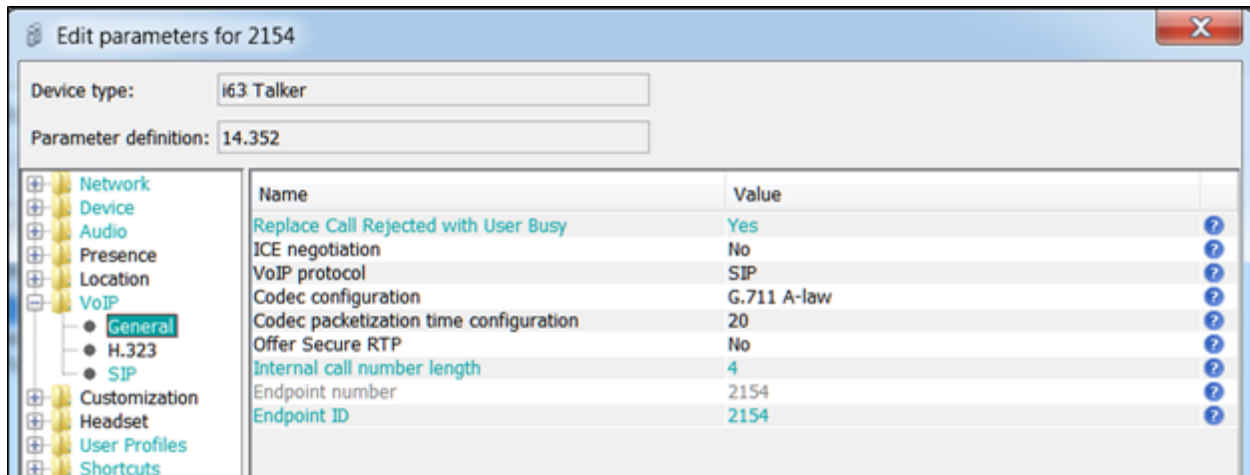


7.1. Configure SIP settings

Select **VoIP → General** from the left window. In the main window ensure the following are set.

- **Replace Call Rejected with User Busy:** **Yes**
- **VoIP Protocol:** **SIP**
- **Codec configuration:** **G.711A-law** (as desired based on **Section 5.5**)
- **Codec packetization time configuration:** **20** (as configured in **Section 5.5**)
- **Internal call number length:** **4** (matches #digits in Endpoint number)
- **Endpoint number:** User extension from **Section 6.2**
- **Endpoint ID:** Can be left blank

Note: The Codec used during compliance testing was G.711A-Law, however other codecs such as G.729 and G.722 are available to use also.



Select the **VoIP→SIP** menu point, and enter the values shown below.

- **Primary SIP proxy:** IP address of Session Manager's signaling interface
- **Listening port:** **5060**
- **SIP proxy password:** Password assigned to the endpoint in **Section 6.2**
- **Registration identity:** Enter **Endpoint number**
- **Authentication identity:** Enter **Endpoint number**
- **SIP Register Expiration:** **120** (recommended value)
- **Direct Signaling** This was left as **No** for compliance testing
- **Disable PRACK** This was set to **Yes** for compliance testing

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

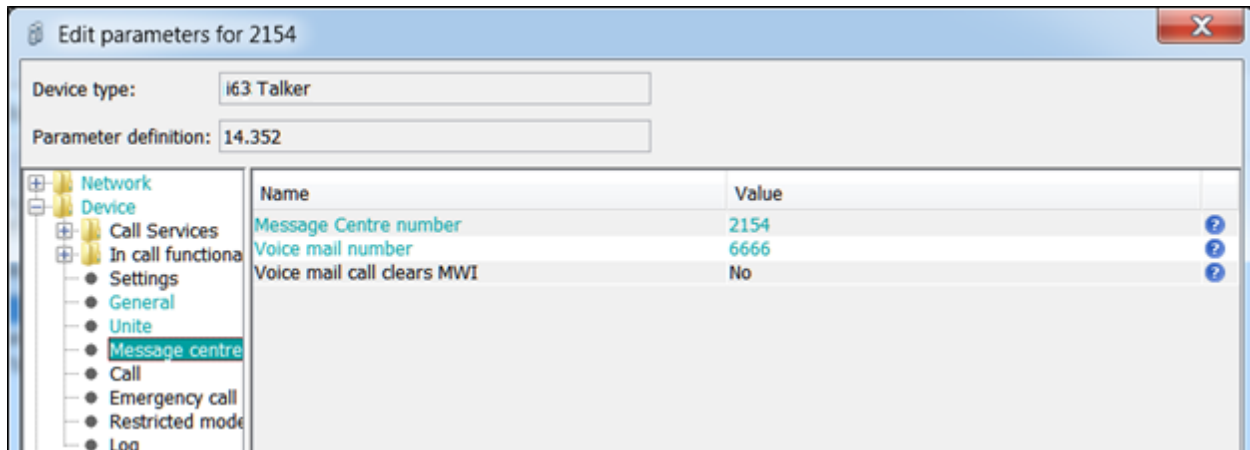
The screenshot shows a window titled "Edit parameters for 2154". At the top, "Device type" is set to "i63 Talker" and "Parameter definition" is set to "14.352". A tree view on the left shows categories: Network, Device, Audio, Presence, Location, VoIP (expanded), Customization, Headset, User Profiles, and Shortcuts. Under VoIP, sub-categories are General, H.323, and SIP (selected). The main area is a table of parameters:

Name	Value
SIP Transport	TCP
Outbound proxy mode	No
Primary SIP proxy	10.10.40.58
Secondary SIP proxy	0.0.0.0
Listening port	5060
SIP proxy ID	
SIP proxy password	*****
Send DTMF using RFC 2833 or SIP INFO	RFC2833
Hold type	Inactive
Registration identity	Endpoint number
Authentication identity	Endpoint number
Call forward locally	Yes
MOH locally	No
Hold on Transfer	No
Direct signaling	No
SIP Register Expiration	120
SIP Message behavior	Ignore
Disable PRACK	Yes
Far-End NAT Traversal	Disabled

For further information about the Ascom i63 handset configurations please refer to Ascom's documentation in **Section 10** of these Application Notes. This section only covers specific settings concerning SIP.

7.2. Configure Message Centre

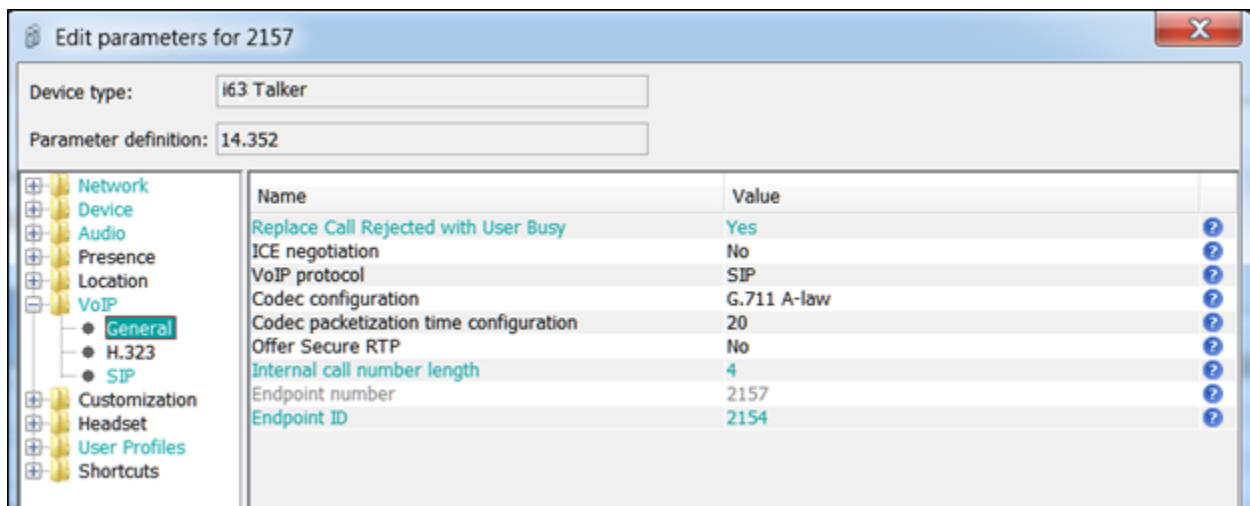
Click on **Device** → **Message centre** in the left window. In the right window, enter the **Voice mail number** as configured in **Section 5.6** and the **Message Centre number** which is the extension number of the handset. Message waiting on/off comes from SIP messages originating from Avaya Aura® Messaging so there is no call to set this value on the Ascom phone.



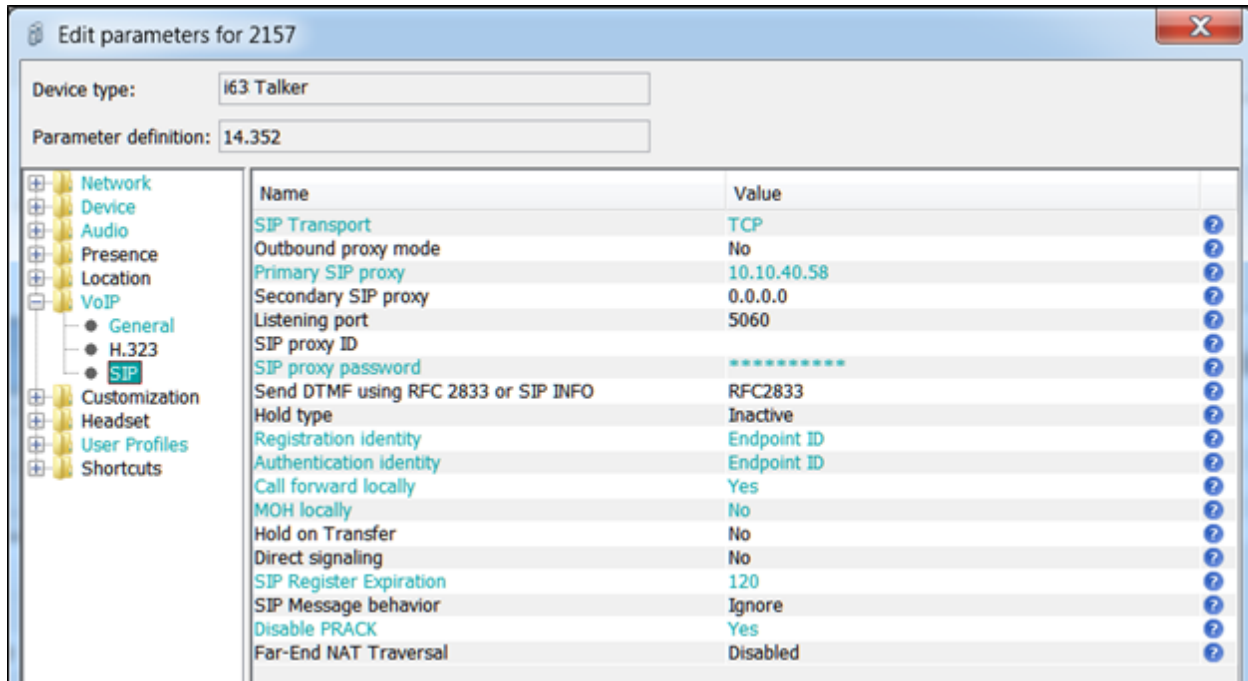
7.3. Configure Multi-Device Access

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

For i63 handset, the MDA feature can be accomplished by configuring and registering the handset using the Endpoint ID parameter. In the example below, handset device with extension number 2157 is configured to register as user 2154. As shown in the screen below, **Endpoint number** is configured as **2157** however **Endpoint ID** is configured as **2154**. As per design, the Endpoint number needs to be unique while configuring the i63 handset via WinPDM.



Also, the **Registration identity** and **Authentication identity** are both configured as **Endpoint ID** as shown below.

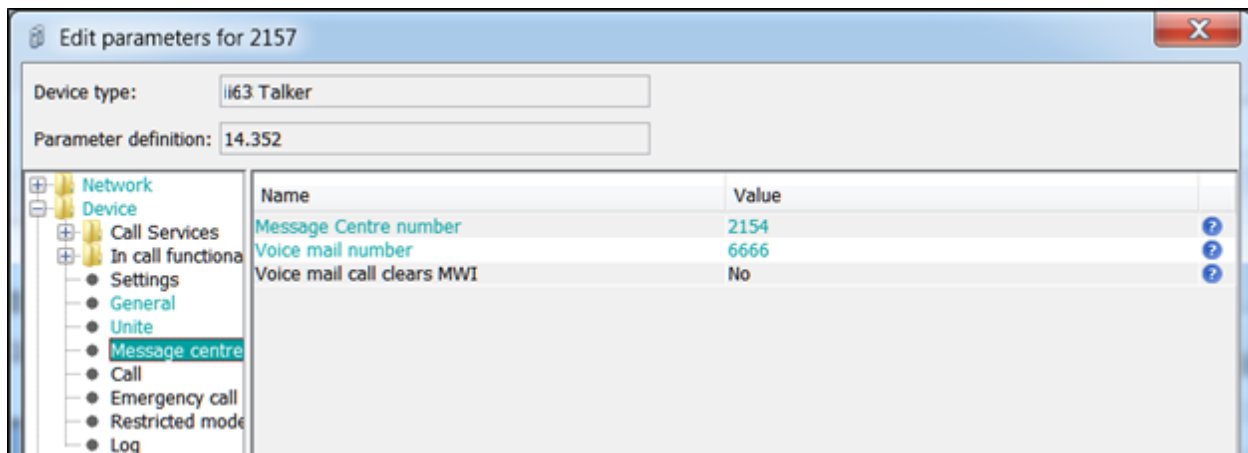


Device type: i63 Talker

Parameter definition: 14.352

Name	Value
SIP Transport	TCP
Outbound proxy mode	No
Primary SIP proxy	10.10.40.58
Secondary SIP proxy	0.0.0.0
Listening port	5060
SIP proxy ID	
SIP proxy password	*****
Send DTMF using RFC 2833 or SIP INFO	RFC2833
Hold type	Inactive
Registration identity	Endpoint ID
Authentication identity	Endpoint ID
Call forward locally	Yes
MOH locally	No
Hold on Transfer	No
Direct signalling	No
SIP Register Expiration	120
SIP Message behavior	Ignore
Disable PRACK	Yes
Far-End NAT Traversal	Disabled

For the **Message Centre number** instead of the extension number of the handset, configure the Endpoint ID which is **2154** in this case.



Device type: i63 Talker

Parameter definition: 14.352

Name	Value
Message Centre number	2154
Voice mail number	6666
Voice mail call clears MWI	No

8. Verification Steps

The following steps can be taken to ensure that connections between Ascom i63 handsets and Session Manager and Communication Manager are up.

8.1. Session Manager Registration

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

The screenshot shows the Avaya Aura System Manager 8.1 interface. The top navigation bar includes 'Users', 'Elements', 'Services', 'Widgets', and 'Shortcuts'. A central menu is open, listing various system components. The 'Session Manager' option is highlighted, and a sub-menu is displayed below it, showing 'Dashboard' as the first option. Other visible dashboard widgets include 'System Resource Utilization' (a bar chart), 'Alarms' (a circular gauge), 'Application State' (a table of system status), and 'Information' (a table of element counts and sync status).

Category	Value
opt	7
var	7
emdata	14

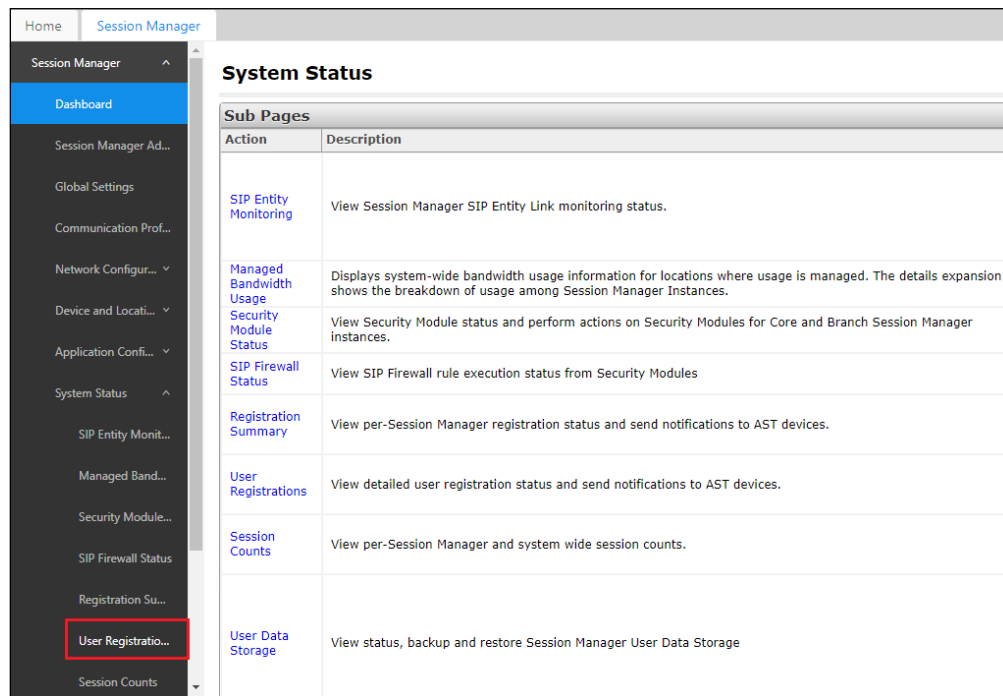
Property	Value
License Status	Active
Deployment Type	VMware
Multi-Tenancy	DISABLED
OOBM State	DISABLED
Hardening Mode	Standard

Elements	Count	Sync Status
CM	1	Green
Session Manager	1	Green
System Manager	1	Green
UCM Applications	8	Green

Severity	Count
Critical	0
Major	0
Indeterminate	0
Minor	0
Warning	0

Item	Link
Dashboard	Dashboard
Session Manager Administration	Session Manager Administration
Global Settings	Global Settings
Communication Profile Editor	Communication Profile Editor
Network Configuration	Network Configuration
Device and Location Configuration	Device and Location Configuration
Application Configuration	Application Configuration

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 i63 user **2154** should show as being registered as shown below. It has an **IP Address** associated with it and there is a tick in the **Registered Prim** box (not shown).

User Registrations							
Select rows to send notifications to devices. Click on Details column for complete registration status.							
<div> View ▾ Default Export Force Unregister AST Device Notifications: Reboot Reload ▾ Failback </div>							
19 Items Show 15 ▾							
<input type="checkbox"/>	Details	Address	First Name	Last Name	Actual Location	IP Address ▾	Remote Office
<input type="checkbox"/>	► Show	2105@devconnect.local	Equinox SIP	Ext2105	DevConnectLab_PG	10.10.40.240	<input type="checkbox"/>
<input type="checkbox"/>	► Show	2103@devconnect.local	Equinox SIP	Ext2103	DevConnectLab_PG	10.10.40.236	<input type="checkbox"/>
<input type="checkbox"/>	► Show	2154@devconnect.local	i63_2154	Ascom	DevConnectLab_PG	10.10.40.201	<input type="checkbox"/>
<input type="checkbox"/>	► Show	2109@devconnect.local	J129	Ext2109	DevConnectLab_PG	10.10.40.194	<input type="checkbox"/>
<input type="checkbox"/>	► Show	2160@devconnect.local	MYCO2160	Ascom	DevConnectLab_PG	10.10.40.186	<input type="checkbox"/>
<input type="checkbox"/>	► Show	2150@devconnect.local	DECT2150	Ascom	DevConnectLab_PG	10.10.40.128	<input type="checkbox"/>

8.2. Ascom i63 Registration

The Ascom i63 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, (note this is an example from compliance testing).



9. Conclusion

These Application Notes describe the configuration steps required for Ascom's i63 VoWiFi handsets to successfully interoperate with Avaya Aura® Communication Manager R8.1 and Avaya Aura® Session Manager R8.1 by registering the Ascom i63 handsets with Avaya Aura® Session Manager as SIP users. Please refer to **Section 2.2** for test results and observations.

10. Additional References

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

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

1. *Deploying Avaya Aura® Communication Manager*, Release 8.1
2. *Avaya Aura® Communication Manager Feature Description and Implementation*, Release 8.1
3. *Deploying Avaya Aura® Session Manager*, Release 8.1
4. *Administering Avaya Aura® Session Manager*, Release 8.1
5. *Deploying Avaya Aura® System Manager*, Release 8.1
6. *Administering Avaya Aura® System Manager for Release 8.1*
7. *Deploying Avaya Aura® Messaging using VMware® in the Virtualized Environment*, Release 7.1
8. *Administering Avaya Aura® Messaging*, Release 7.1

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

Appendix A

Signaling Group

display signaling-group 1	Page 1 of 3
SIGNALING GROUP	
Group Number: 1	Group Type: sip
IMS Enabled? n	Transport Method: tls
Q-SIP? n	
IP Video? n	Enforce SIPS URI for SRTP? n
Peer Detection Enabled? y	Peer Server: SM
	Clustered? n
Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? y	
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? n	
Alert Incoming SIP Crisis Calls? n	
Near-end Node Name: procr	Far-end Node Name: SM80vmppg
Near-end Listen Port: 5061	Far-end Listen Port: 5061
	Far-end Network Region: 1
Far-end Domain:	
	Bypass If IP Threshold Exceeded? n
Incoming Dialog Loopbacks: eliminate	RFC 3389 Comfort Noise? n
DTMF over IP: rtp-payload	Direct IP-IP Audio Connections? y
Session Establishment Timer(min): 3	IP Audio Hairpinning? n
Enable Layer 3 Test? y	Initial IP-IP Direct Media? n
H.323 Station Outgoing Direct Media? n	Alternate Route Timer(sec): 6

Trunk Group Page 1

display trunk-group 1	Page 1 of 4
TRUNK GROUP	
Group Number: 1	Group Type: sip
Group Name: SIPTRUNK-SM80	CDR Reports: y
Direction: two-way	COR: 1
Dial Access? n	TN: 1
Queue Length: 0	TAC: *801
Service Type: tie	Outgoing Display? n
	Night Service:
	Auth Code? n
	Member Assignment Method: auto
	Signaling Group: 1
	Number of Members: 10

Page 2

```
display trunk-group 1                                     Page 2 of 4
  Group Type: sip

TRUNK PARAMETERS

  Unicode Name: auto

                                     Redirect On OPTIM Failure: 5000

  SCCAN? n                                     Digital Loss Group: 18
                                     Preferred Minimum Session Refresh Interval(sec): 600

Disconnect Supervision - In? y Out? y

  XOIP Treatment: auto      Delay Call Setup When Accessed Via IGAR? n

Caller ID for Service Link Call to H.323 1xC: station-extension
```

Page 3

```
display trunk-group 1                                     Page 3 of 4
TRUNK FEATURES

  ACA Assignment? n      Measured: none      Maintenance Tests? y

Suppress # Outpulsing? n  Numbering Format: private
                                     UII 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

DSN Term? n
```


trunk-group 1	Page 4 of 4
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	
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	

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 **devconnect.local** 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 (SM 8.1 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.

The screenshot shows the 'Session Border Controller for Enterprise' interface. On the left is a navigation menu with 'Configuration Profiles' expanded, showing 'Topology Hiding' selected. The main area is titled 'Topology Hiding Profiles: SM8.1'. It includes a list of profiles on the left (default, cisco_th_profile, Avaya, Cardeasy, Bill (PSTN), SM8.0, SM8.1) and a table for the 'Topology Hiding' profile on the right. The table has columns: Header, Criteria, Replace Action, and Overwrite Value. Below the table is an 'Edit' button.

Header	Criteria	Replace Action	Overwrite Value
To	IP/Domain	Overwrite	devconnect.local
Request-Line	IP/Domain	Overwrite	devconnect.local
SDP	IP/Domain	Auto	---
Via	IP/Domain	Auto	---
Record-Route	IP/Domain	Auto	---
Referred-By	IP/Domain	Auto	---
Refer-To	IP/Domain	Auto	---
From	IP/Domain	Overwrite	devconnect.local

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 **From PSTN PG** below, click in **Edit** as shown to make changes to the Flow.

The screenshot shows the 'Session Border Controller for Enterprise' interface. On the left is a navigation menu with 'Network & Flows' expanded, showing 'End Point Flows' selected. The main area is titled 'End Point Flows'. It has tabs for 'Subscriber Flows' and 'Server Flows'. Below the tabs are three tables for different SIP servers. The first table is for 'SIP Server: SM-PSTN-PG' and the second for 'SIP Server: SMvmpg 8.1'. The third table is for 'SIP Server: SMvmpg 8.1' and has an 'Update' button above it. The third table has a red box around the 'Edit' button for the 'From PSTN PG' flow.

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
1	To PSTN Bill	*	Sig_Int	Sig_Ext-Bill	Bill(PSTN)	SM8.1	View Clone Edit Delete

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
1	To PSTN PG	*	Sig_Int	Sig-EXT-PSTN-PG	SM-PSTN-RTP	SM8.1	View Clone Edit Delete

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
1	From PSTN PG	*	Sig-EXT-PSTN-PG	Sig_Int	SM-PSTN-RTP	SM-PSTN-PG	View Clone Edit Delete
2	From PSTN Bill	*	Sig_Ext-Bill	Sig_Int	SM-PSTN-SRTP	Bill (PSTN)	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: From PSTN PGX

Flow Name	From PSTN PG
SIP Server Profile	SMvmpg 8.1
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Sig-EXT-PSTN-PG
Signaling Interface	Sig_Int
Media Interface	Med_Int
Secondary Media Interface	None
End Point Policy Group	SM-PSTN-RTP
Routing Profile	SM-PSTN-PG
Topology Hiding Profile	SM8.1
Signaling Manipulation Script	None
Remote Branch Office	Any
Link Monitoring from Peer	<input type="checkbox"/>

Finish

©2020 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.