



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 v3.1.1 to interoperate with Avaya Aura® Communication Manager R10.1 and Avaya Aura® Session Manager R10.1.

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

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

1. Introduction

These Application Notes describe the configuration steps for provisioning Ascom's i63 VoWiFi (i63) handsets v3.1.1 to interoperate with Avaya Aura® Communication Manager R10.1 and Avaya Aura® Session Manager R10.1. 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, Avaya Digital and simulated PSTN endpoints. Avaya 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 simulated PSTN endpoints.

- Registration/Invalid Registration
- Basic Calls/PSTN calls
- Session Refresh Timer
- Long Duration Call
- Hold, Retrieve and Brokering (Toggle)
- Feature Access Code dialing
- Attended and Blind Transfer
- Third Party Conference using the i63 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 i63 handset being the EC500 destination
- Multi-Device Access (MDA)
- Do Not Disturb (Locally Controlled)
- Calling Line Name/Identification
- Codec Support (OPUS, G.722, G.711, G.729)
- DTMF Support
- Voice Mail, Message Waiting Indication
- 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 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. Session Manager has a minimum Registration Timer of 600 seconds. If the i63 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**).
7. Negotiation of OPUS or G.722 between endpoints, such as the Ascom i63, requires support for the codec to be configured on Communication Manager.
8. 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 Messaging.
9. 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.

10. Per design, i63 handsets do not have a redial button. User needs to use “Call List” and redial the numbers.
11. 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.
12. PSTN calls were simulated using a SIP trunk routing via an Avaya Session Border Controller for Enterprise. In order to correctly simulate incoming calls from a typical SIP service provider, the Session Border Controller for Enterprise 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 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 Digital, H.323, and SIP endpoints on Communication Manager and with a simulated PSTN. The handsets are configured by Ascom Windows Portable Device Manager (WinPDM) using the Ascom Desktop Programmer DPL.

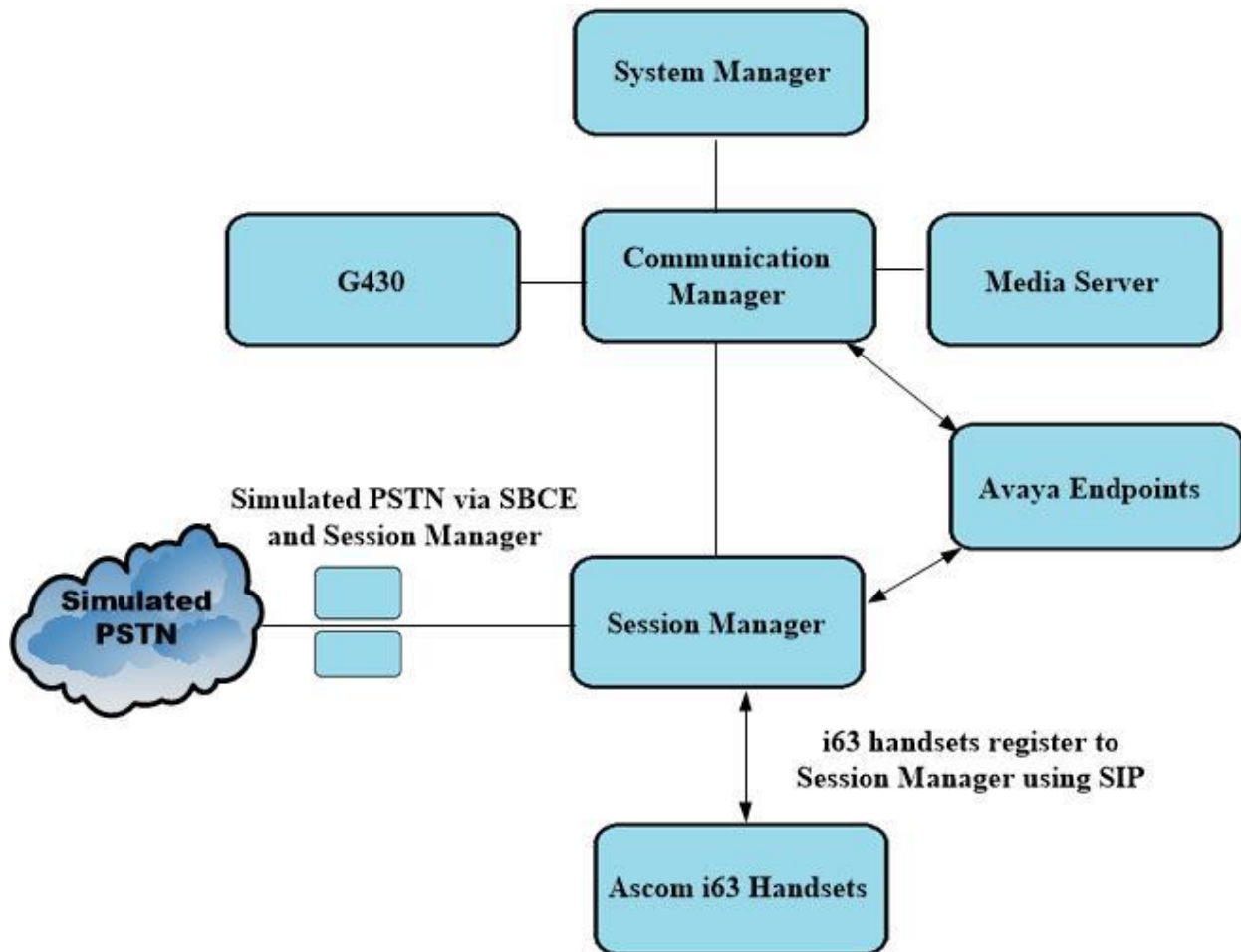


Figure 1: Network Solution of Ascom i63 with Avaya Aura® Communication Manager R10.1 and Avaya Aura® Session Manager R10.1

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 10.1.0.2 Build No. – 10.1.0.0.537353 Software Update Revision No: 10.1.0.2.0715160 Service Pack 2
Avaya Aura® Session Manager	Session Manager R10.1 Build No. – 10.1.0.2.1010219
Avaya Aura® Communication Manager	R10.1.0.2.0 – SP2 R020x.01.0.974.0 Update ID 01.0.974.0-27607
Avaya Messaging	11.0 SP2 Build 11.0.0.324
Avaya Aura® Media Server	10.1.0.101
Avaya Media Gateway G430	42.7.0 /2
Avaya 9404 Digital	17.0
Avaya J100 Series SIP	7.1.2.0.14
Avaya J100 Series H323	7.0.14.0.7
Avaya Session Border Controller for Enterprise (to facilitate simulated PSTN)	8.1.3.0-31-21052
Ascom Equipment	Software / Firmware Version
Ascom Portable Device Manager running on Windows PC	4.1.8
Ascom i63 VoWiFi Handset	V3.1.10
Ascom approved Wi-Fi Access Point	Ascom approved software version

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

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 **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

DIAL PLAN ANALYSIS TABLE

Location: all

Percent Full: 5

Dialed String

Total Length

Call Type

1

4

udp

Dialed String

Total Length

Call Type

2

4

udp

Dialed String

Total Length

Call Type

3

4

ext

Dialed String

Total Length

Call Type

4

4

ext

Dialed String

Total Length

Call Type

5

4

udp

Dialed String

Total Length

Call Type

6

4

ext

Dialed String

Total Length

Call Type

8

1

fac

Dialed String

Total Length

Call Type

9

1

fac

Dialed String

Total Length

Call Type

*8

4

dac

Dialed String

Total Length

Call Type

*

3

fac

Dialed String

Total Length

Call Type

#

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 Req'd	
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 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	Deactivation: #04
Call Forwarding Enhanced Status: *73	Act: *74	Deactivation: #74
Call Park Access Code:	*02	
Call Pickup Access Code:	*09	
CAS Remote Hold/Answer Hold-Unhold Access Code:		
CDR Account Code Access Code:	*14	
Change COR Access Code:		
Change Coverage Access Code:		
Conditional Call Extend Activation:		Deactivation:
Contact Closure Open Code:		Close Code:

5.4. Configure Network Region

Use **change ip-network-region x** (where x is the network region to be configured) to assign an appropriate domain name to be used by Communication Manager, in the example below **greaney.psil6.avaya.com** is used. Note that this domain is also configured in **Section 6.1.1**.

```
change ip-network-region 1                                     Page 1 of 20
                                                                IP NETWORK REGION
    Region: 1          NR Group: 1
    Location: 1        Authoritative Domain: greaney.psil6.avaya.com
        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 shown below were offered to the i63 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           n          20
    3: G.722.2          2          20
    4: G.711A           n          20
    5: G.711MU          n          20
    6: G.729            n          20
    7:
        Media Encryption      Encrypted SRTCP: best-effort
    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 **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

Page 2 of 60

HUNT GROUP

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 i63 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

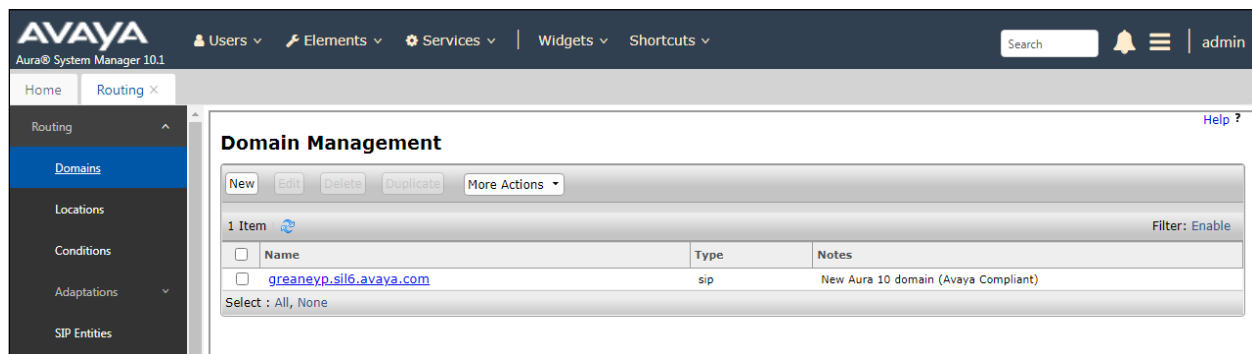
Drag shortcuts here

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.

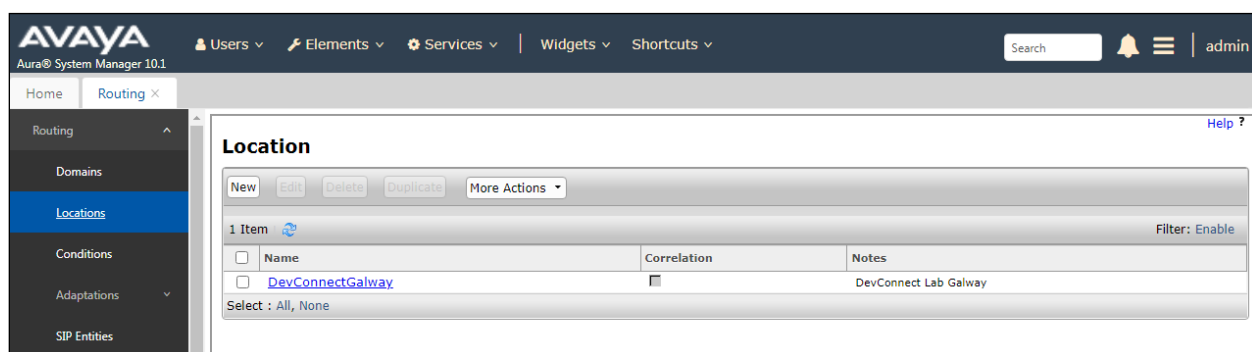
6.1.1. Display the Domain

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.



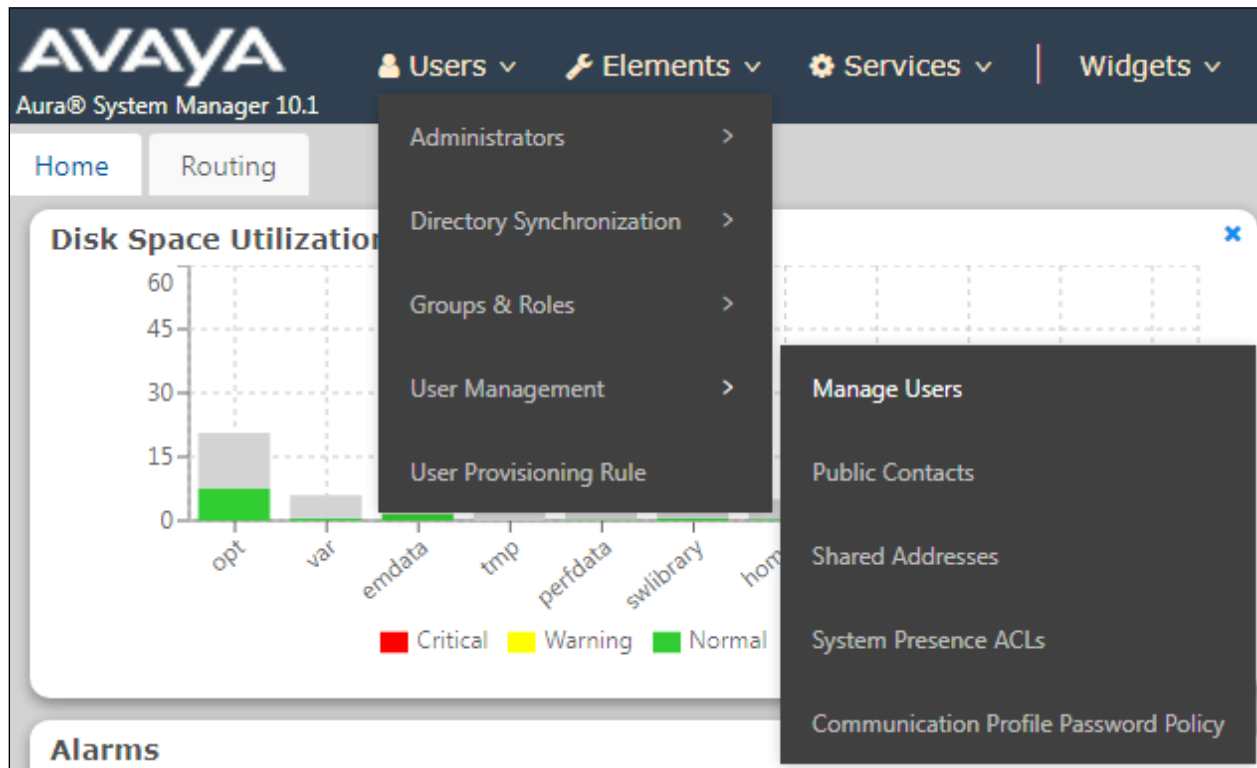
6.1.2. Display the Location

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.

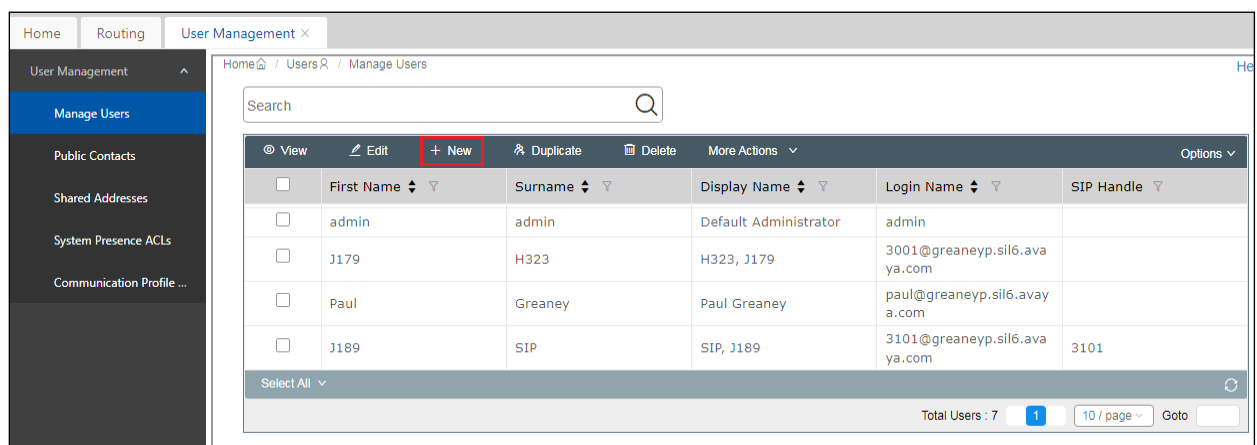


6.2. Adding Ascom SIP Users

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.

User Profile | Edit | 3192@greanep.sil6.avaya.com [Commit & Continue] [Commit] [Cancel]

Identity | Communication Profile | Membership | Contacts

Basic Info

Address

LocalizedName

User Provisioning Rule: [v]

* Last Name: 3192 Last Name (in Latin alphabet characters): 3192

* First Name: Ascom First Name (in Latin alphabet characters): Ascom

* Login Name: 3192@greanep.sil6.ava Middle Name: Middle Name Of User

Description: SIP Phone Email Address: Email Address Of User

Password: [] User Type: Basic [v]

Confirm Password: [] Localized Display Name: 3192, Ascom

Endpoint Display Name: 3192, Ascom Title Of User: Title Of User

Language Preference: English (United Stat... [v] Time Zone: (0:0)GMT : Dublin, ... [v]

Under the **Communication Profile** tab enter **Communication Profile Password** and **Re-enter Comm-Profile Password**, note that his password is required when configuring the i63 handset in **Section Error! Reference source not found.**

Identity | **Communication Profile** | Membership | Contacts

Communication Profile Password

PROFILE SET : Primary [v]

Communication Address

PROFILES

Session Manager Profile [On]

Avaya Breeze® Profile [Off]

CM Endpoint Profile [On]

Comm-Profile Password [x]

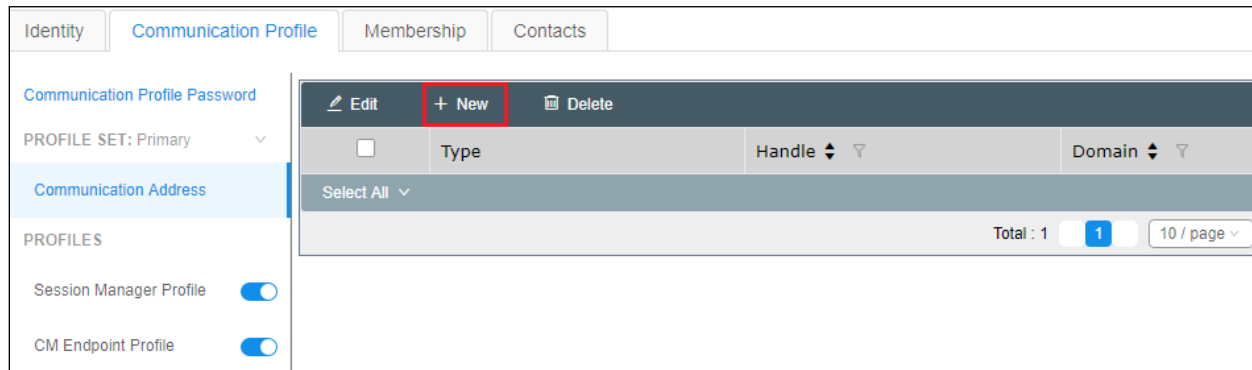
Comm-Profile Password: []

* Re-enter Comm-Profile Password: [] [✓]

[Generate Comm-Profile Password](#)

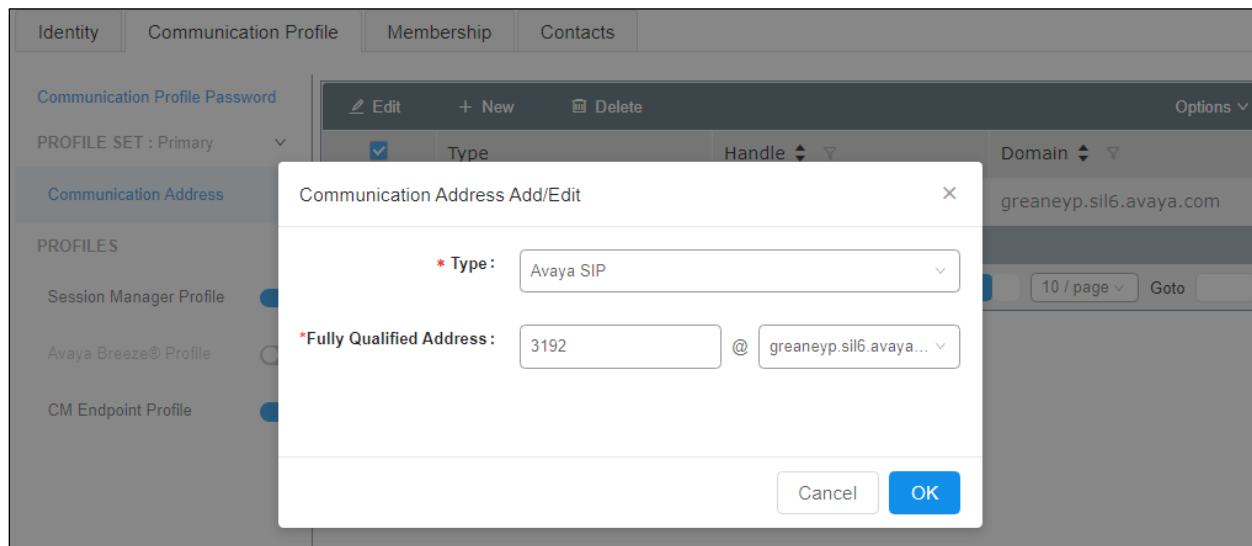
[Cancel] [OK]

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 application. On the left sidebar, 'Communication Address' is selected under the 'PROFILES' section. The main area has a table with columns 'Type', 'Handle', and 'Domain'. Above the table, there are buttons for 'Edit', '+ New' (highlighted with a red box), and 'Delete'. Below the table, there is a 'Total : 1' indicator and a '10 / page' dropdown.

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 two main fields: '* Type:' with a dropdown menu set to 'Avaya SIP', and '* Fully Qualified Address:' with two input fields. The first input field contains '3192' and the second contains 'greanep.sil6.avaya...'. There are 'Cancel' and 'OK' buttons at the bottom right. The background shows the same web application interface as the previous screenshot.

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**. This will only be set on the SIP user that all devices will be registering as, for compliance testing this SIP user was 3101. 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

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 i63 handset. Click on **Endpoint Editor** to configure the buttons and features for that handset on Communication Manager.

User Profile | Edit | 3192@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 :

3192

Template :

9620SIP_DEFAULT_C

* Set Type :

9620SIP

Security Code :

Enter Security Code

Port :

S000011

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 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.

System	cm101x	Extension	3192
Template	9620SIP_DEFAULT_CM_10_1	Set Type	9620SIP
Port	S000011	Security Code	
Name	3192, Ascom		

General Options (G) *	Feature Options (F)	Site Data (S)	Abbreviated Call Dialing (A)	Enhanced Call Fwd
Button Assignment (B) Group Membership (M)				
* Class of Restriction (COR)	1	* Class Of Service (COS)	1	
* Emergency Location Ext	3192	* Message Lamp Ext.	3192	
* 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	3192, Ascom	
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. Click on **Done** (not shown) to complete.

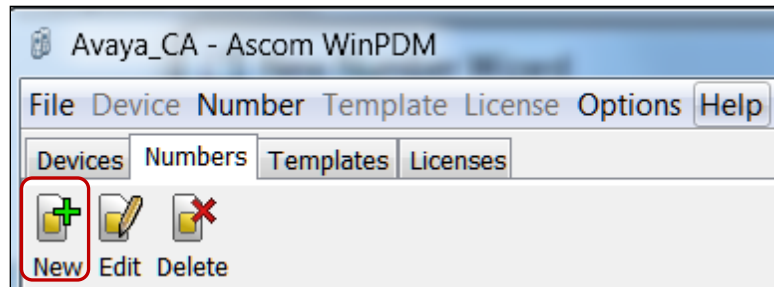
General Options (G) *	Feature Options (F)	Site Data (S)	Abbreviated Call Dialing (A)	Enhanced Call Fwd (E)
Button Assignment (B) Group Membership (M)				
	Forwarded Destination	Active		
Unconditional For Internal Calls To		<input type="checkbox"/>		
External Calls To		<input type="checkbox"/>		
Busy 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

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

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.

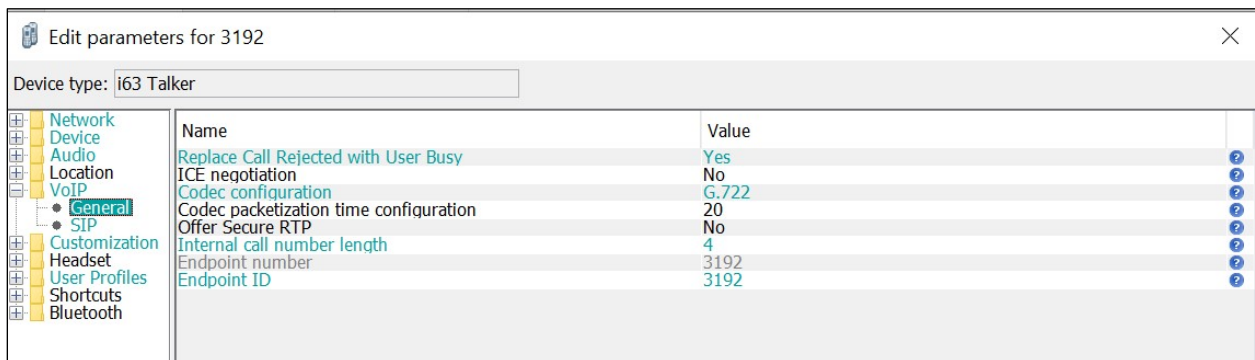


7.1. Configure SIP settings

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

- **Replace Call Rejected with User Busy:** **Yes**
- **Codec configuration:** **G.722** (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:** User extension from **Section 6.2**

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



The screenshot shows a configuration window titled "Edit parameters for 3192". The "Device type" is set to "i63 Talker". The left sidebar shows a tree view with categories: Network, Device, Audio, Location, VoIP, Customization, Headset, User Profiles, Shortcuts, and Bluetooth. The "VoIP" category is expanded, and "General" is selected. The main area displays a table of parameters:

Name	Value
Replace Call Rejected with User Busy	Yes
ICE negotiation	No
Codec configuration	G.722
Codec packetization time configuration	20
Offer Secure RTP	No
Internal call number length	4
Endpoint number	3192
Endpoint ID	3192

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** (this will be negotiated)
- **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 the 'Edit parameters for 3192' window with the 'Device type' set to 'i63 Talker'. The left sidebar shows a tree view with 'VoIP' expanded and 'SIP' selected. The main table lists the following parameters and values:

Name	Value
SIP Transport	TCP
Outbound proxy mode	No
Primary SIP proxy	10.10.40.12
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
Deprecated parameter kept for parameter migration	No
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	No
Emergency call location method	None

To allow call forwarding options to be visible and set locally, the following field needs to be set to “Show”. Under **Customization** in the left window, click on **Visibility** and ensure that **Calls/Call services/Divert calls** is set to **Show**.

The screenshot shows the 'Edit parameters for 3192' window with the 'Device type' set to 'i63 Talker'. The left sidebar shows a tree view with 'Customization' expanded and 'Visibility' selected. The main table lists the following parameters and values:

Name	Value
Connections/Bluetooth	Show
Connections/Headset	Show
Connections/Network	Show
Connections/In Charger	Show
Calls	Show
Calls/Call services	Show
Calls/Call services/Divert calls	Show
Calls/Call services/Do not disturb	Show
Contacts	Show
Contacts/Central Phonebook	Show

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 Messaging so there is no requirement to set this value on the Ascom phone.

The screenshot shows the 'Edit parameters for 3192' window. The 'Device type' is set to 'i63 Talker'. The left sidebar shows a tree view with 'Network' expanded, then 'Device', then 'Call Services', then 'In call functions', then 'Settings', then 'General', then 'SCEP', then 'Unite', then 'Message centre' (highlighted). The main area shows a table with the following parameters:

Name	Value
Message Centre number	3192
Voice mail number	6668
Voice mail call clears MWI	No

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.

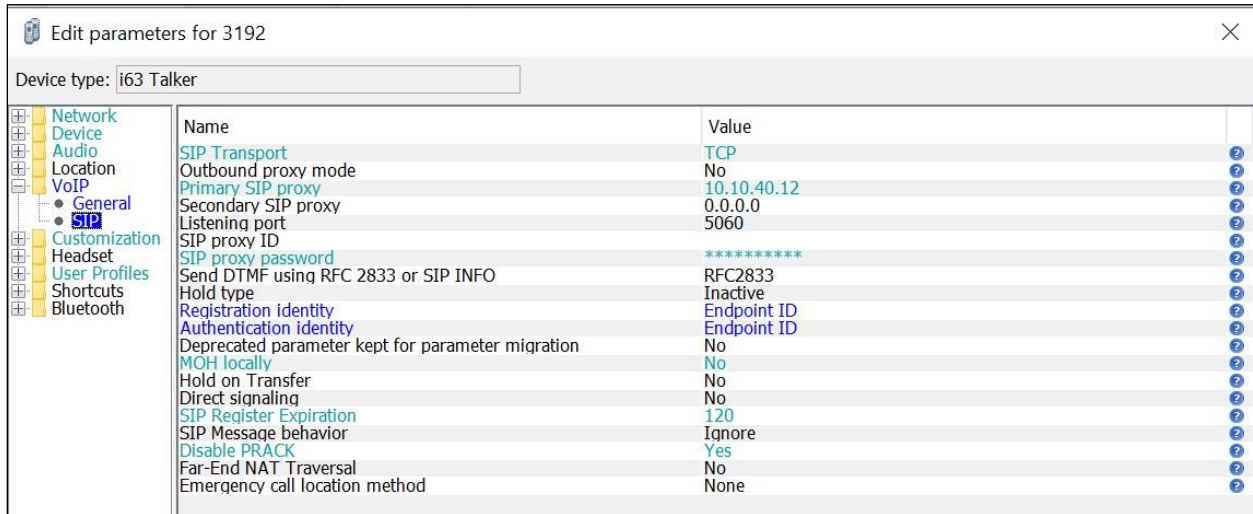
For i63 handset, the MDA feature can be accomplished by configuring and registering the handset using the Endpoint ID parameter. In the example below, handset device with extension number 3192 is configured to register as user 3101. As shown in the screen below, **Endpoint number** is configured as **3192** however **Endpoint ID** is configured as **3101**. As per design, the Endpoint number needs to be unique while configuring the i63 handset via WinPDM.

Note: The number of devices that can be registered to this number depends on the Max. Simultaneous Devices parameter set in **Section 6.2**.

The screenshot shows the 'Edit parameters for 3192' window. The 'Device type' is set to 'i63 Talker'. The left sidebar shows a tree view with 'Network' expanded, then 'Device', then 'Audio', then 'Location', then 'VoIP', then 'General' (highlighted), then 'SIP', then 'Customization', then 'Headset', then 'User Profiles', then 'Shortcuts', then 'Bluetooth'. The main area shows a table with the following parameters:

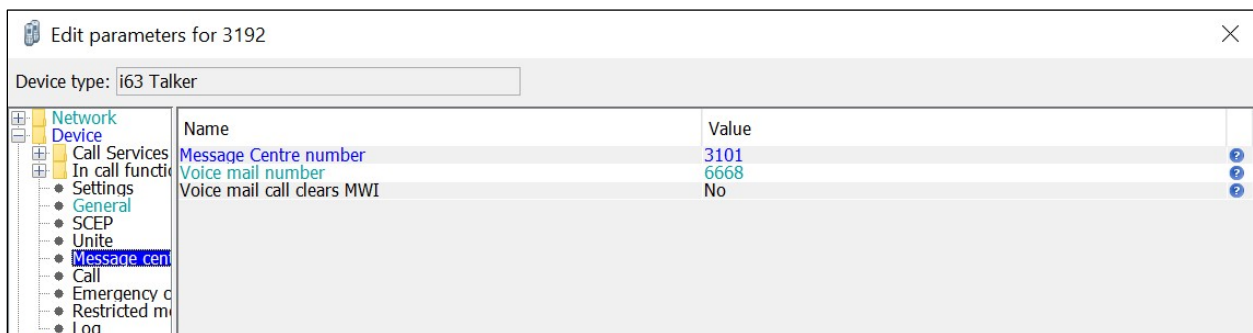
Name	Value
Replace Call Rejected with User Busy	Yes
ICE negotiation	No
Codec configuration	G.722
Codec packetization time configuration	20
Offer Secure RTP	No
Internal call number length	4
Endpoint number	3192
Endpoint ID	3101

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



Name	Value
SIP Transport	TCP
Outbound proxy mode	No
Primary SIP proxy	10.10.40.12
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
Deprecated parameter kept for parameter migration	No
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	No
Emergency call location method	None

For the **Message Centre number**, configure the Endpoint ID, which is **3101** in this case.



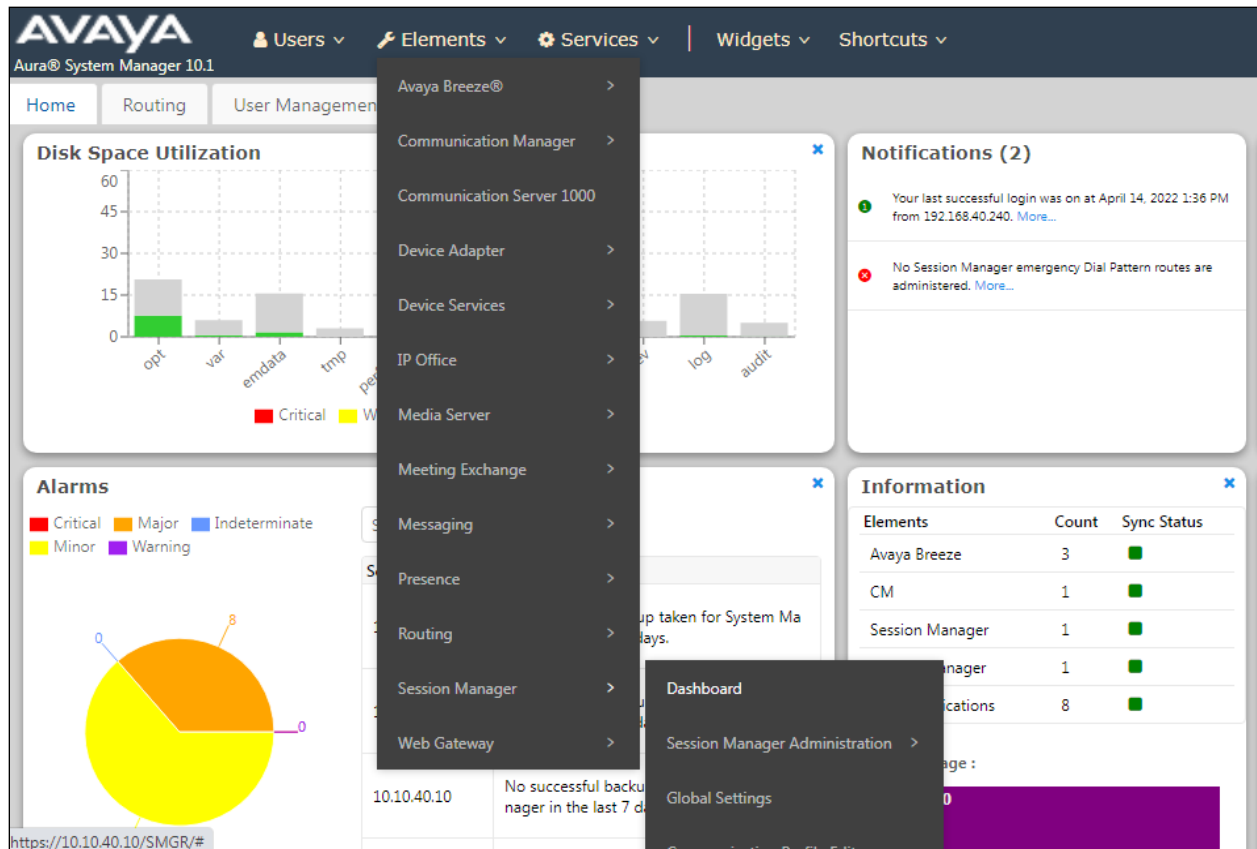
Name	Value
Message Centre number	3101
Voice mail number	6668
Voice mail call clears MWI	No

8. Verification Steps

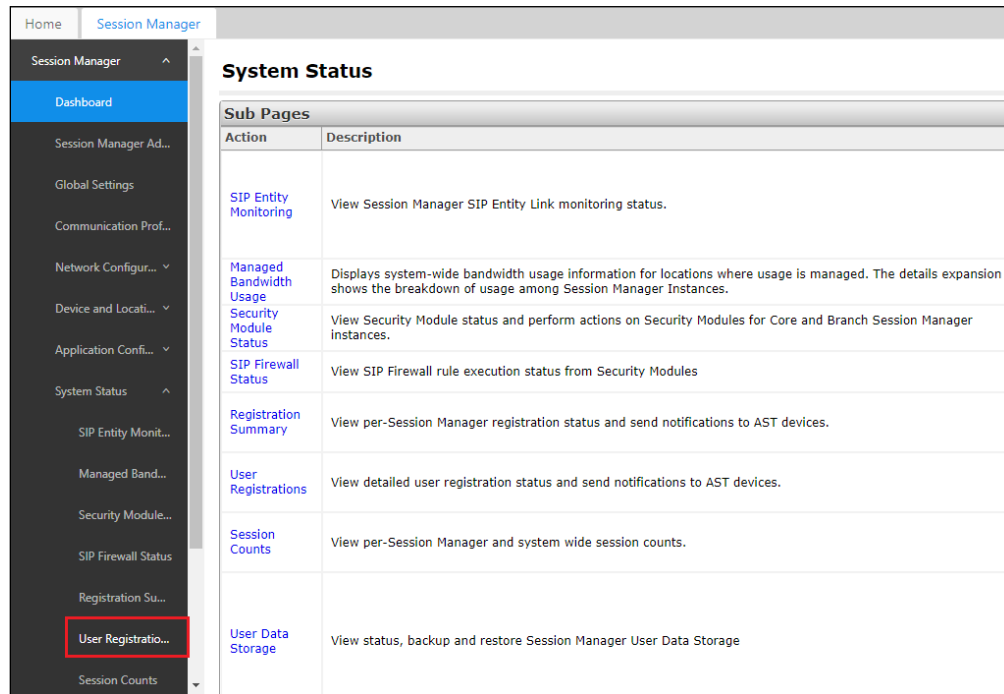
The following steps can be taken to ensure that connections between Ascom i63 handsets and Session Manager and Communication Manager are up.

8.1. Session Manager Registration

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

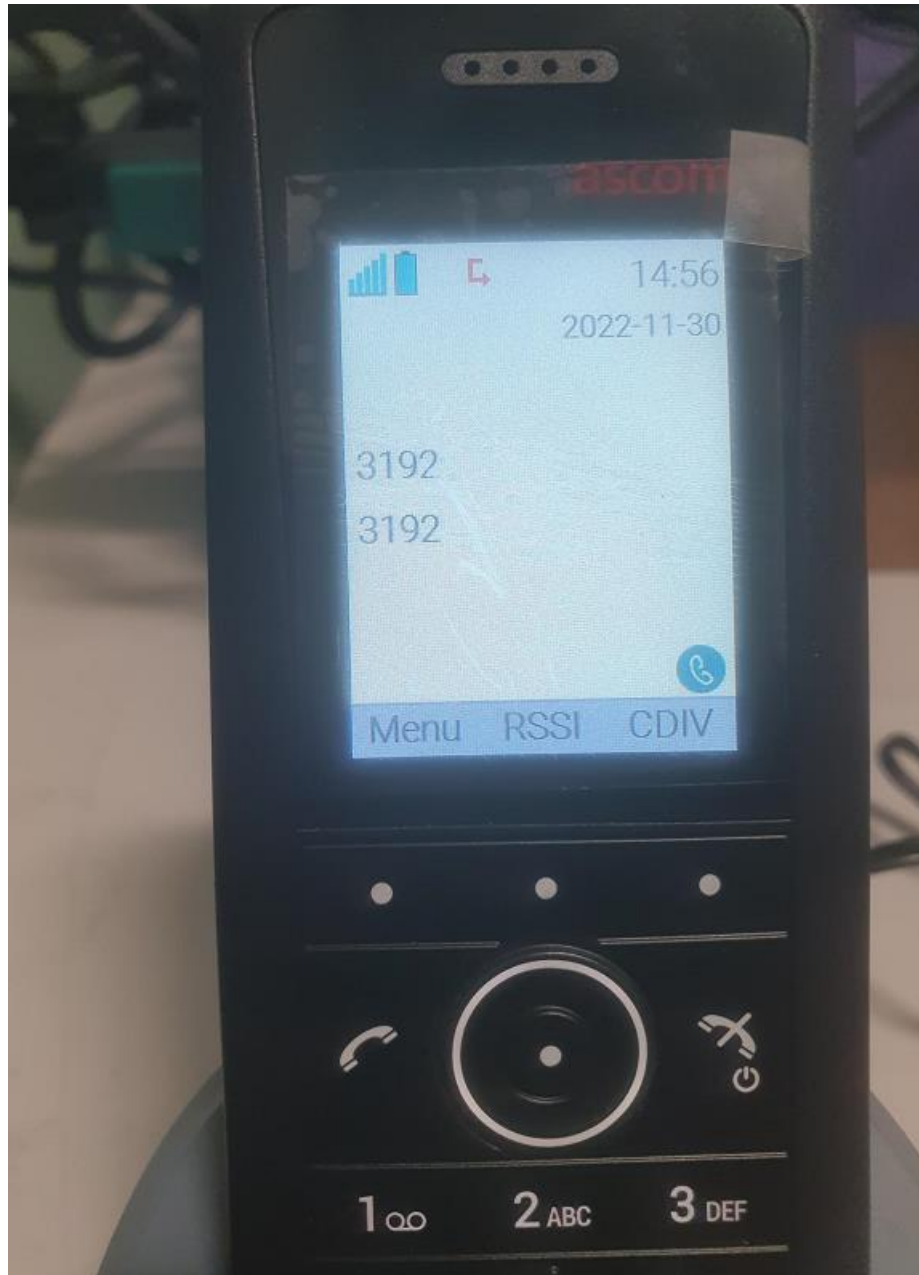


The Ascom i63 user **3192** should show as being registered as shown below. It has an **IP Address** associated with it and there is a tick in the **Registered Prim** box.

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>Fallback</div> <div>As of 2:36 PM</div> <div>Advanced Search</div> </div> <div>14 Items</div> <div>Show All</div> <div>Filter: Enable</div>											
Details	Address	First Name	Last Name	Actual Location	IP Address	Policy	Shared Control	Simult. Devices	AST Device	Registered	
										Prim	Sec
► Show	3194@greanexp.sil6.avaya.com	Ascom	3194	---	10.10.40.219	fixed	<input type="checkbox"/>	1/1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
► Show	3193@greanexp.sil6.avaya.com	Ascom	3193	---	10.10.40.216	fixed	<input type="checkbox"/>	1/1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
► Show	3115@greanexp.sil6.avaya.com	Vantage01	K175	DevConnectGalway	10.10.40.210	fixed	<input type="checkbox"/>	1/1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> (AC)	<input type="checkbox"/>
► Show	3192@greanexp.sil6.avaya.com	Ascom	3192	---	10.10.40.205	fixed	<input type="checkbox"/>	1/1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
► Show	3191@greanexp.sil6.avaya.com	Ascom	3191	---	10.10.40.201	fixed	<input type="checkbox"/>	1/1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
► Show	3101@greanexp.sil6.avaya.com	Agent One	Workspaces	DevConnectGalway	10.10.40.186	fixed	<input type="checkbox"/>	1/3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> (AC)	<input type="checkbox"/>
► Show	---	AAfD - one	SIP	---	---	fixed	<input type="checkbox"/>	0/1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
► Show	---	AAfD - two	SIP	---	---	fixed	<input type="checkbox"/>	0/1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
► Show	---	Workplace	Windows	---	---	fixed	<input type="checkbox"/>	0/1	<input type="checkbox"/>	<input type="checkbox"/>	<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 v3.1.1 to successfully interoperate with Avaya Aura® Communication Manager R10.1 and Avaya Aura® Session Manager R10.1 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. *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): 600

Disconnect Supervision - In? y Out? y

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

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

Page 3

```
display trunk-group 11                                     Page 3 of 5
TRUNK FEATURES

  ACA Assignment? n          Measured: none          Maintenance Tests? y

Suppress # Outpulsing? n    Numbering Format: private
                               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 2/2/2023

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

34 of 38
Ascomi63_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 left sidebar shows a navigation tree with options like Session Manager, Dashboard, Session Manager..., Global Settings, Communication Prof..., Network Configur..., Device and Locati..., Device Settings..., Location Settings, Station Access C..., Application Config..., System Status, System Tools, and Performance. The main content area is titled "Device Settings Group" and includes tabs for General, Server Timer, Endpoint Timer, Maintenance Settings, and VoIP Monitoring Manager. The "General" tab is active, showing fields for Name (Default Group), Description (Default Group), Group Type (Location Group selected), and Terminal Group Number. The "Server Timer" tab shows Subscription Expiration Timer (Maximum: 86400, Minimum: 600) and Registration Expiration Timer (Maximum: 3600, Minimum: 600). The "Endpoint Timer" tab shows Line Reservation Timer (30), Reactive Monitoring Interval (60), and Timer B (4). The "Maintenance Settings" and "VoIP Monitoring Manager" tabs are also visible.

AVAYA
Aura® System Manager 10.1

Users ▾ Elements ▾ Services ▾ | Widgets ▾ Shortcuts ▾

Search 🔍 | admin

Home | User Management | **Session Manager**

Session Manager ▾
Dashboard
Session Manager ... ▾
Global Settings
Communication Prof...
Network Configur... ▾
Device and Locati... ▾
Device Settings ...
Location Settings
Station Access C...
Application Config... ▾
System Status ▾
System Tools ▾
Performance ▾

Device Settings Group [Restore] [Cancel] [Save] [Help ?]

General | Server Timer | Endpoint Timer | Maintenance Settings | VoIP Monitoring Manager | Volume Settings | VLAN Parameters | DIFFSERV/QoS Parameters | 802.1 P/Q Parameters | Expand All | Collapse All

General ▾

*Name: [Default Group]
Description: [Default Group]
Group Type: ☒ Location Group ☐ Terminal Group
Terminal Group Number: []

Server Timer ▾

	Maximum	Minimum
Subscription Expiration Timer (secs):	[86400]	[600]
Registration Expiration Timer (secs):	[3600]	[600]

Endpoint Timer ▾

*Line Reservation Timer (secs): [30]
*Reactive Monitoring Interval (secs): [60]
*Timer B (sec): [4]

Maintenance Settings ▸

VoIP Monitoring Manager ▸

©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.