



Avaya Solution & Interoperability Test Lab

Application Notes for Zenitel IP Operating Room Master with Avaya Aura® Communication Manager and Avaya Aura® Session Manager using TLS – Issue 1.0

Abstract

These Application Notes describe the configuration steps for provisioning Zenitel IP Operating Room Master v6.1.1 to interoperate with Avaya Aura® Communication Manager R8.1 and Avaya Aura® Session Manager R8.1. Zenitel IP Operating Room Master is an IP Intercom that supports voice transmission using Session Initiation Protocol (SIP) and Transport Layer Security (TLS).

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 Zenitel IP Operating Room Master v6.1.1 to interoperate with Avaya Aura® Communication Manager R8.1 and Avaya Aura® Session Manager R8.1. Zenitel IP Operating Room Master is an IP Intercom that supports voice transmission using Session Initiation Protocol (SIP) and Transport Layer Security (TLS).

Transport Layer Security (TLS), is a cryptographic protocol designed to provide communications security over a computer network. Several versions of the protocols are widely used in applications such as email, instant messaging, and voice over IP, but its use as the Security layer in voice over IP is the focus in these Application Notes. The Secure Real-time Transport Protocol (SRTP) is a profile for Real-time Transport Protocol (RTP) intended to provide encryption, message authentication and integrity, and replay attack protection to the RTP data in both unicast and multicast applications. During compliance testing Zenitel IP OR Master phones made use of TLS and SRTP.

The IP Operating Room (OR) Master Station is an intercom station intended for use in operating theatres and clean rooms. The station front plate is totally flat and without any holes to minimize bacteria accumulation. With a large backlit display and Vingtor-Stentofon audio technology the station allows users to read caller ID, listen and talk at a distance. During compliance testing, each IP OR Master station was set up as a SIP user on Session Manager and underwent testing of various call scenarios with other Avaya telephones.

The following models in the Zenitel IP OR Master station family were tested: IP Desk Master V2, IP Master V2, and IP Flush Master. Other models in the IP OR Master family are not covered by this compliance test.

Note: The Zenitel IP Operating Room Master phones may be referred to as ‘IP OR Master station’, ‘IP OR Master Intercom phone’, or ‘IP OR Master’ throughout this document, but they all refer to the same phones that were tested.

2. General Test Approach and Test Results

The general test approach was to place calls to and from the IP OR Master phones and exercise basic telephone operations. For serviceability testing, failures such as LAN cable pulls, and hardware resets were performed.

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

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

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

Avaya recommends our customers implement Avaya solutions using appropriate security and encryption capabilities enabled by our products. The testing referenced in these DevConnect Application Notes included the enablement of supported encryption capabilities in the Avaya products. Readers should consult the appropriate Avaya product documentation for further information regarding security and encryption capabilities supported by those Avaya products.

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

For the testing associated with these Application Notes, the interface between Avaya systems and the Zenitel IP OR Master made use of both TLS and SRTP as requested by Zenitel.

2.1. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability testing. IP Desk Master V2, IP Master V2, and IP Flush Master models were tested. The feature testing was to verify that:

- IP OR Master successfully registers with Session Manager using the TLS protocol.
- IP OR Master successfully establishes audio calls with SRTP audio to Avaya H.323, SIP and digital endpoints.
- IP OR Master successfully establishes audio calls with a simulated PSTN.
- IP OR Master successfully negotiates the appropriate audio codec.
- DTMF tones could be passed successfully to energize relay on the IP OR Master unit to allow a door to be opened from the phone sending the DTMF tone or perhaps to switch audio direction.
- IP OR Master successfully calls multiple Avaya destinations in a hunt group.
- IP OR Master successfully calls a variety of endpoints in its call list set on the IP OR Master phone.

The serviceability testing focused on verifying the ability of IP OR Master to recover from adverse conditions, such as disconnecting/reconnecting the Ethernet cable on Session Manager.

Note: Compliance testing was carried out with the IP OR Master phones set to use TLS/SRTP. Testing was also carried out with IP OR Master phones set to use TCP/RTP and these Application Notes are labelled, *Application Notes for Zenitel IP Operating Room Master with Avaya Aura® Communication Manager and Avaya Aura® Session Manager using TCP*.

2.2. Test Results

All test cases passed successfully with the following observation noted.

1. The Zenitel IP OR Master phones may not support RFC5939, SDP Cap Negotiation, and so only media encryption can be set under the IP Codec associated with these phones. If media encryption is not going to be used for some other phones then a two separate Network Regions must be setup, one with this encryption enabled and the other without any encryption. See **Section 5.3** and **Section 5.4**.
2. Call Park has a different meaning on the IP OR Master functionality than that of the Call Park feature on Communication Manager. When the Call Park function is used on IP OR Master it places multiple calls on hold. For every Direct Access Key (DAK) with Call Park configured, there can be only one active or resumed call.

2.3. Support

Technical support on Zenitel IP OR Master can be obtained through the following:

- **Phone:** +1 816 231 7200 (Americas) +47 4000 2700 (Global)
- **Email:** cs@zenitel.com
- **Web:** <https://www.zenitel.com/customer-service>

3. Reference Configuration

Figure 1 illustrates a test configuration that was used to compliance test the interoperability of IP OR Master with Session Manager and Communication Manager. The configuration consists of H.323 and Digital phones registering directly to Communication Manager and SIP phones registering to Session Manager using the features on Communication Manager. A SIP trunk connects Communication Manager to a simulated PSTN.

Note: The Zenitel IP OR Master phones register to Session Manager the same as the Avaya SIP phones.

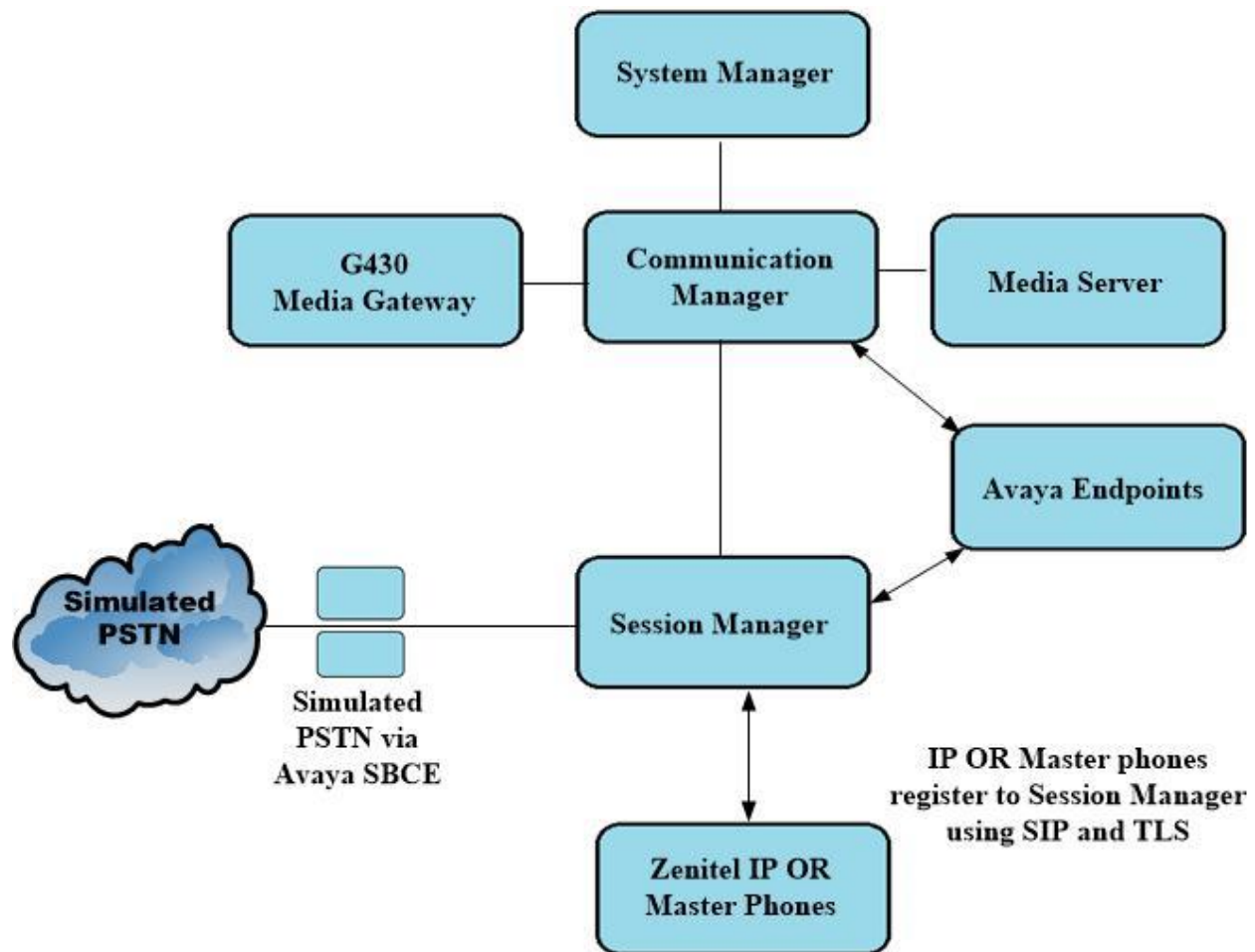


Figure 1: The configuration of Avaya Aura® Communication Manager and Avaya Aura® Session Manager with Zenitel IP Operating Room Master

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	8.1.3.0 Build No. – 8.1.0.0.733078 Software Update Revision No: 8.1.3.0.1011784 Feature Pack 3
Avaya Aura® Session Manager running on a virtual server	8.1.3 Build No. – 8.1.3.0.813014
Avaya Aura® Communication Manager running on a virtual server	8.1.3 – FP3 R018x.01.0.890.0 Update ID 01.0.890.0-26568
Avaya Session Border Controller for Enterprise	8.1.1.0-26-19214
Avaya Aura® Media Server	8.0.2.138
Avaya G430 Media Gateway	41.16.0/1
Avaya J179 H.323 Deskphone	6.8304
Avaya Vantage K175 SIP Deskphone	3.0.0.1.0006
Avaya 9408 Digital Phone	2.00
Zenitel Equipment	Software / Firmware Version
Zenitel IP Operating Room Master - IP Desk Master - IP Master V2 - IP Flush Master	6.1.1.0 6.1.1.0 02.11.3.0

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
- Network Region
- IP Codec

5.1. Configure System Parameters

Ensure that the SIP endpoints license is valid as shown below by using the command **display system-parameters customer-options**.

display system-parameters customer-options		Page	1 of 12
OPTIONAL FEATURES			
G3 Version: V17	Software Package: Enterprise		
Location: 2	System ID (SID): 1		
Platform: 28	Module ID (MID): 1		
		USED	
Platform Maximum Ports:		48000	168
Maximum Stations:		36000	44
Maximum XMOBILE Stations:		36000	0
Maximum Off-PBX Telephones - EC500:		41000	2
Maximum Off-PBX Telephones - OPS:		41000	20
Maximum Off-PBX Telephones - PBFMC:		41000	0
Maximum Off-PBX Telephones - PVFMC:		41000	0
Maximum Off-PBX Telephones - SCCAN:		0	0
Maximum Survivable Processors:		313	1

5.2. Configure Dial Plan Analysis

Use the **change dialplan analysis** command to configure the dial plan using the parameters shown below. Extension numbers (**ext**) are those beginning with **1**. Feature Access Codes (**fac**) use digits **8** and **9** and use characters ***** or **#**.

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

5.3. 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		

5.4. Configure IP-Codec

Use the **change ip-codec-set x** (where x is the ip-codec set used) command to designate a codec set compatible with the IP OR Master phone. During compliance testing the codecs **G.711A**, **G.729A** and **G.722** were tested.

For compliance testing the Avaya phones are set to use Media Encryption as well as the IP OR Master phones. **1-srtp-aescm128-hmac80** was the encryption used and so must be present under **Media Encryption**.

Note: The IP OR Master phones may not support RFC5939, SDP Cap Negotiation, and so only 1-srtp-aescm128-hmac80 encryption can be set under the IP Codec associated with these phones. If media encryption is not going to be used for some other phones then a two separate Network Regions must be setup, one with this encryption enabled and the other without any encryption.

change ip-codec-set 1

Page1 of 2

IP MEDIA PARAMETERS

Codec Set: 1

	Audio	Silence	Frames	Packet
	Codec	Suppression	Per Pkt	Size (ms)
1:	G.711A	n	2	20
2:	G.729A	n	2	20
3:	G.722.2	n	1	20
4:	G.722-64K		2	20
5:				
6:				
7:				

Media Encryption

Encrypted SRTCP: enforce-unenc-srtcp

1:	1-srtp-aescm128-hmac80
2:	
3:	
4:	

6. Configure Avaya Aura® Session Manager

This section provides the procedures for configuring Session Manager. Session Manager is configured via System Manager. The procedures include the following areas:

- Domains and Locations
- Adding Zenitel IP OR Master 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**.

The screenshot displays the login interface for Avaya Aura Session Manager. The browser's address bar shows the URL: `smgr81xvmpg.devconnect.local/securityserver/UI/Login?org=dc=nortel,dc=com&goto=https://smgr81xvmpg.devconnect.local:443`. The login form includes a 'User ID' field with 'admin' entered and a 'Password' field with masked characters. 'Log On' and 'Reset' buttons are positioned below the password field. A disclaimer box on the left contains the following text:

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.

At the bottom right, a blue banner states: **Supported Browsers:** Internet Explorer 11.x or Firefox 65.0, 66.0 or 67.0.

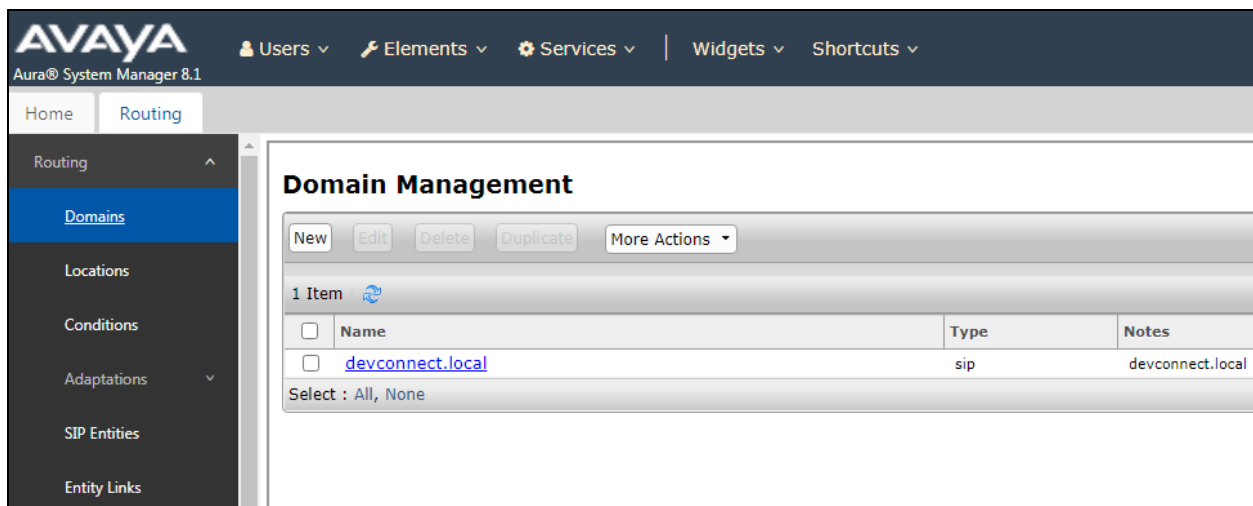
Once logged in navigate to **Elements** and click on **Routing** (not shown).

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.

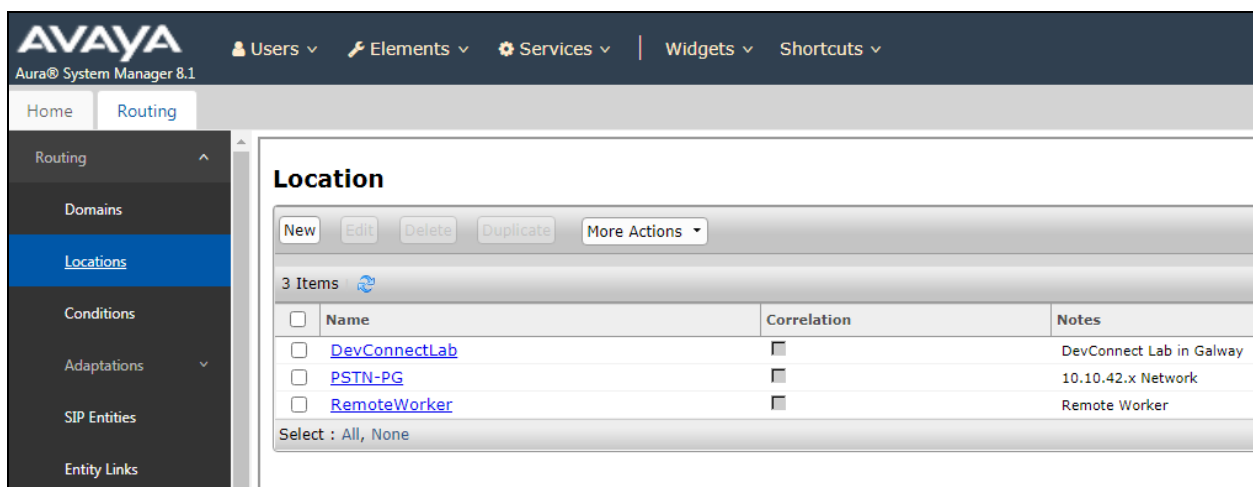


The screenshot shows the Avaya Aura System Manager 8.1 interface. The top navigation bar includes 'Users', 'Elements', 'Services', 'Widgets', and 'Shortcuts'. The left sidebar has 'Routing' selected, and 'Domains' is highlighted. The main content area is titled 'Domain Management' and shows a table with one item: 'devconnect.local' of type 'sip'.

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_PG** which was used for compliance testing. If a location is not already in place, then one must be added to include the IP address range of the Avaya solution. Click on **New** to add a new location.

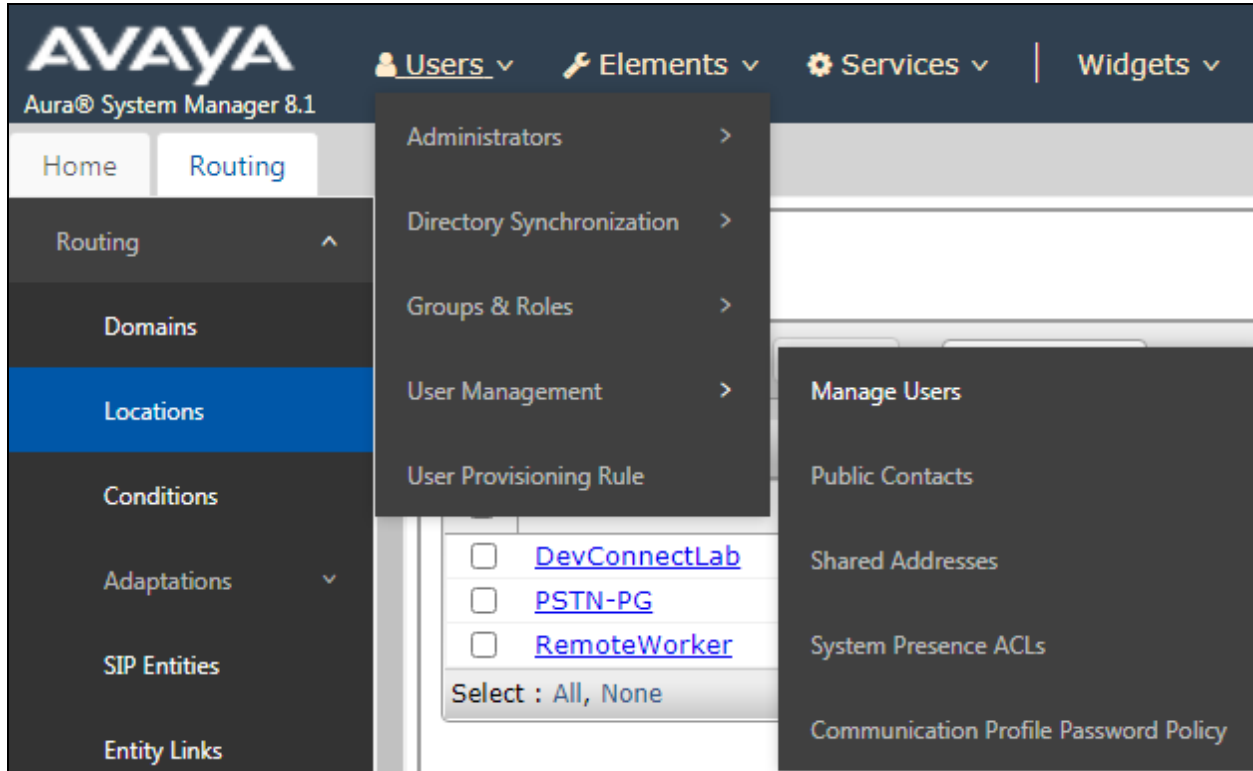


The screenshot shows the Avaya Aura System Manager 8.1 interface. The top navigation bar includes 'Users', 'Elements', 'Services', 'Widgets', and 'Shortcuts'. The left sidebar has 'Routing' selected, and 'Locations' is highlighted. The main content area is titled 'Location' and shows a table with three items: 'DevConnectLab', 'PSTN-PG', and 'RemoteWorker'.

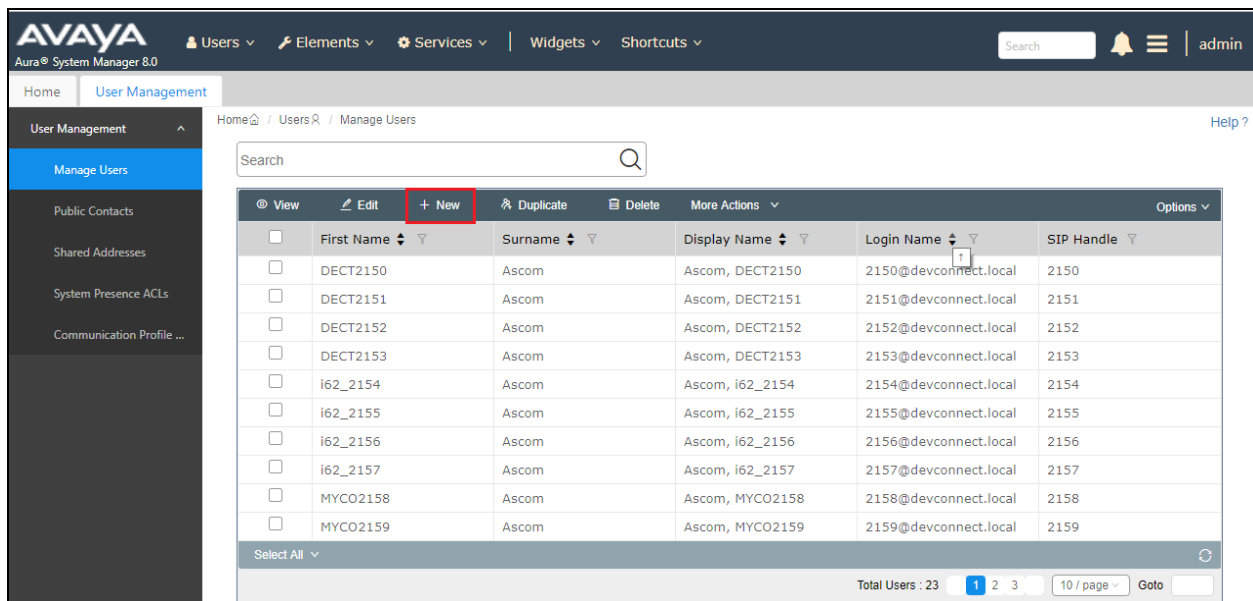
Name	Correlation	Notes
DevConnectLab		DevConnect Lab in Galway
PSTN-PG		10.10.42.x Network
RemoteWorker		Remote Worker

6.2. Adding Zenitel IP Operating Room Master SIP Users

From the top of the home page click on **Users** → **User Management** → **Manager Users** as 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 | 1157@devconnect.local

Commit & Continue Commit Cancel

Identity Communication Profile Membership Contacts

Basic Info

Address

LocalizedName

User Provisioning Rule: [v]

* Last Name: Ext 1157 Last Name (in Latin alphabet characters): Ext 1157

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

* Login Name: 1157@devconnect.local Middle Name: Middle Name Of User

Description: 3rd Party SIP Phone Email Address: Email Address Of User

Password: [] User Type: Basic [v]

Confirm Password: [] Localized Display Name: Ext 1157, SIP

Endpoint Display Name: Ext 1157, SIP Title Of User: Title Of User

Under the **Communication Profile** tab enter **Communication Profile Password** and **Re-enter Comm-Profile Password**, note that his password is required when configuring the IP OR Master phone in **Section 7.2**.

User Profile | Edit | 1157@devconnect.local

Commit

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]

Presence Profile [off]

Comm-Profile Password

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 'User Profile | Edit | 1157@devconnect.local' interface. The 'Communication Profile' tab is selected. On the left, there is a sidebar with 'Communication Profile Password', 'PROFILE SET : Primary', 'Communication Address' (highlighted), and 'PROFILES' (containing 'Session Manager Profile' which is toggled on). The main area shows a table with columns 'Edit', '+ New' (highlighted), and 'Delete'. Below the table, there is a 'Type' dropdown and a 'Select All' button.

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

The screenshot shows the same 'User Profile | Edit | 1157@devconnect.local' interface, but with the 'Communication Address Add/Edit' dialog box open. The dialog box has a title bar with a close button. It contains two fields: '* Type:' with a dropdown menu showing 'Avaya SIP', and '*Fully Qualified Address:' with two input fields: '1157' and '@ devconnect.local' (with a dropdown arrow). At the bottom right of the dialog are 'Cancel' and 'OK' buttons.

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.

User Profile | Edit | 1157@devconnect.local

Identity

Communication Profile

Membership

Contacts

Communication Profile Password

PROFILE SET : Primary

Communication Address

PROFILES

Session Manager Profile

Avaya Breeze® Profile

CM Endpoint Profile

Presence Profile

SIP Registration

* Primary Session Manager :

SM81vmpg

Secondary Session Manager :

Start typing...

Survivability Server :

Start typing...

Max. Simultaneous Devices :

1

Block New Registration When Maximum Registrations Active? :

Application Sequences

Origination Sequence :

CMAPPSEQ

Termination Sequence :

CMAPPSEQ

Emergency Calling Application Sequences

Emergency Calling Origination Sequence :

Select

Emergency Calling Termination Sequence :

Select

PG; Reviewed:
SPOC 9/4/2021

Solution & Interoperability Test Lab Application Notes
©2021 Avaya Inc. All Rights Reserved.

15 of 35
Master_CM81TLS

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_PG

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**. **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 IP OR Master phone. Click on **Endpoint Editor** to configure the buttons and features for that phone on Communication Manager.

The screenshot shows the 'User Profile | Edit | 1157@devconnect.local' interface. The 'Communication Profile' tab is active. On the left, under 'PROFILES', the 'CM Endpoint Profile' is selected with a toggle switch. The main configuration area includes the following fields and options:

- System:** cm81xvmpg
- Profile Type:** Endpoint
- Extension:** 1157
- Set Type:** 9620SIP
- Port:** IP
- Preferred Handle:** Select
- Sip Trunk:** aar
- Template:** 9620SIP_DEFAULT_CM_8_1
- Security Code:** Enter Security Code
- Calculate Route Pattern:** ☒
- SIP URI:** Select
- Delete on Unassign from User or on Delete User:** ☒
- Override Endpoint Name and Localized Name:** ☒
- Allow H.323 and SIP Endpoint Dual Registration:** ☐

Buttons at the top right include 'Commit & Continue', 'Commit', and 'Cancel'.

Under the **Feature Options** tab (not shown), if the IP OR Master phone is capable of video, then IP Video can be ticked. 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.

Active Station Ringing	single	Auto Answer	none
MWI Served User Type	None	Coverage After Forwarding	system
Per Station CPN - Send Calling Number	None	Display Language	english
AUDIX Name	None	Hunt-to Station	
Remote Soft Phone Emergency Calls	as-on-local	Loss Group	19
LWC Reception	spe	Survivable COR	internal
IP Phone Group ID		Time of Day Lock Table	None
Speakerphone	2-way	Voice Mail Number	
Short/Prefixed Registration Allowed	default	Music Source	
EC500 State	enabled		
Bridging Tone for This Extension	None		

Features

<input type="checkbox"/> Always Use <input type="checkbox"/> IP Audio Hairpinning <input type="checkbox"/> Bridged Call Alerting <input type="checkbox"/> Bridged Idle Line Preference <input checked="" type="checkbox"/> Coverage Message Retrieval <input type="checkbox"/> Data Restriction <input checked="" type="checkbox"/> Survivable Trunk Dest <input type="checkbox"/> Bridged Appearance Origination Restriction <input checked="" type="checkbox"/> Restrict Last Appearance <input type="checkbox"/> Turn on mute for remote off-hook attempt <input type="checkbox"/> IP Hoteling	<input type="checkbox"/> Idle Appearance Preference <input type="checkbox"/> IP SoftPhone <input checked="" type="checkbox"/> LWC Activation <input type="checkbox"/> CDR Privacy <input checked="" type="checkbox"/> Precedence Call Waiting <input checked="" type="checkbox"/> Direct IP-IP Audio Connections <input type="checkbox"/> H.320 Conversion <input checked="" type="checkbox"/> IP Video <input type="checkbox"/> Per Button Ring Control
---	--

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

User Profile | Edit | 1157@devconnect.local

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
Presence Profile

* System : cm81xvmpg

Use Existing Endpoints :
Template : 9620SIP_DEFAULT_CM_8_1
Security Code : Enter Security Code
Voice Mail Number :
Calculate Route Pattern :
SIP URI : Select

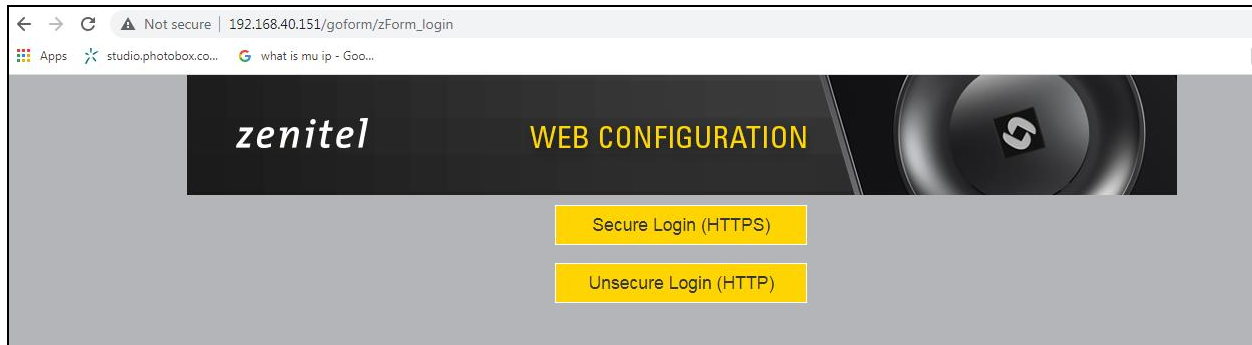
* Profile Type : Endpoint
* Extension : 1157
* Set Type : 9620SIP
Port : IP
Preferred Handle : Select
Sip Trunk : sar

Delete on Unassign from User or on Delete User :
Allow H.323 and SIP Endpoint Dual Registration :

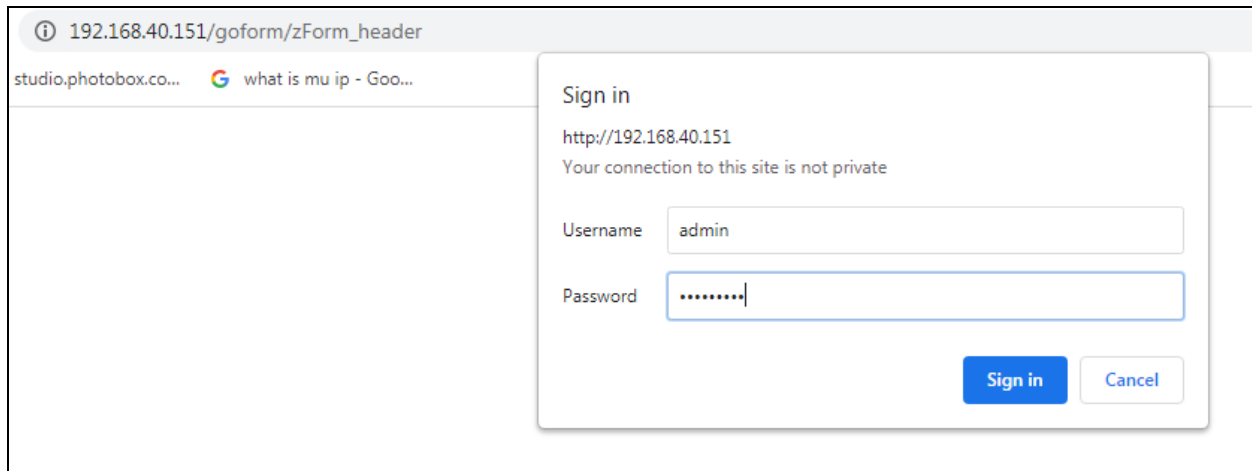
Override Endpoint Name and Localized Name :

7. Configure Zenitel IP Operating Room Master Phone

The following steps detail the configuration for IP OR Master using the web interface. Access the IP OR Master web interface, enter **http://<ipaddress>** in an Internet browser window, where **<ipaddress>** is the IP address of the IP OR Master phone in question. For compliance testing **Unsecure Login (HTTP)** was chosen.



Log in with the appropriate credentials.




Upon logging in, information on that IP OR Master station is displayed. The following settings should be checked.

- Configure Advanced Configuration Mode
- Configure Certificates
- SIP Configuration
- Direct Access Keys
- Audio

ADVANCED

WEB CONFIGURATION

VINGTOR  STENTOFON

MainSIP ConfigurationStation AdministrationAdvanced SIPAdvanced Network

Information

Main Settings

Recovery

Legal Information

IP Master Information

Description	Information
IP Address:	192.168.40.151
Subnet Mask:	255.255.255.0
Default Gateway:	192.168.40.1
DNS Server 1:	192.168.40.1
DNS Server 2:	
MAC Address:	00:13:cb:30:01:b6
Software Version:	6.1.1.0
More Information:	Show/Hide

Status

Description	Status
Mode:	SIP
Uptime:	up 59 minutes
Name:	
Number (SIP ID):	1157
Server Domain (SIP):	devconnect.local, Registered - Tue Apr 20 14:40:46 2021
Backup Domain (SIP):	
Backup Domain 2 (SIP):	
Outbound Proxy:	10.10.40.32:5061

7.1. Configure Advanced Configuration Mode

Select **Recovery** from the left window and under **Preferences** enter the password for **Advanced configuration mode**, this password can be obtained from a Zenitel engineer as per **Section 2.3**.

Main	SIP Configuration	Station Administration
------	-------------------	------------------------

Information

Main Settings

Recovery

Legal Information

Commands

Description	Action
Full reboot	REBOOT
Partial reboot	REBOOT
Factory reset	FACTORY RESET
Factory reset with DHCP	FACTORY RESET

Preferences

Description	Configuration
Advanced configuration mode	<input type="text" value="Type offline password to unlock advanced configuration mode"/>

Once the password is entered the check box will appear as shown and a tick can be placed and click on **Save** to confirm.

Main	SIP Configuration	Station Administration
------	-------------------	------------------------

Information

Main Settings

Recovery

Legal Information

Commands

Description	Action
Full reboot	REBOOT
Partial reboot	REBOOT
Factory reset	FACTORY RESET
Factory reset with DHCP	FACTORY RESET
Rollback	ROLLBACK

Preferences

Description	Configuration
Advanced configuration mode	<input checked="" type="checkbox"/>

SAVE

7.2. Configure Certificates

Click on **Certificates** in the left window and click on **Choose File** in the main window. Locate the Root Certificate required and click on **Upload**. This Certificate must be present to allow the handshake take place for a TLS connection to Session Manager.

Main

SIP Configuration

Station Administration

Advanced SIP

Advanced Network

Account / Call

Audio

Direct Access Keys

Relays / Outputs

Time

Keyboard

RTSP

Audio Messages

Multicast Paging

Language

Certificates

Certificates

	Name	Expiry date	Issuer	Subject	
Certificate 1	turbine_server_sha256.key	Mar 14 2057 15:51 GMT	vs-imx6ul-station	vs-imx6ul-station	DELETE
Certificate 2	turbine_server_sha1.key	Mar 14 2057 15:51 GMT	vs-imx6ul-station	vs-imx6ul-station	DELETE
Certificate 3	RootCertAura81CA.pem	Jul 05 2029 14:54 GMT	System Manager CA	System Manager CA	DELETE

Upload Certificate

Choose File

RootCertAura81CA.pem

UPLOAD

7.3. SIP Configuration

Click on **SIP Configuration** → **SIP** and configure the following in the **Account Settings** section:

- **Name:** Enter the desired name.
- **Number (SIP ID):** Enter a user extension administered from **Section 6.2**.
- **Server Domain (SIP):** Enter the Domain as per **Section 6.1.1**.
- **Authentication User Name:** Enter a user extension administered from **Section 6.2**.
- **Authentication Password:** Enter the **Login Code** from **Section 6.2**.
- **Outbound Proxy (optional):** Enter the IP address of Session Manager and **5061** as the **Port**.
- **Outbound Transport:** Set this to **TLS**.
- **SIP Scheme:** Set this to **sips**.
- **RTP Encryption:** This is set to **srtp_encryption** for testing with SRTP.
- **SRTP Crypto Type:** This is set to the same encryption configured in **Section 5.4**.
- **Use Unencrypted SRTCP:** This was set to the same setting as Communication Manager as per **Section 5.4**.
- **TLS Private Key:** This should be set as shown below. This key was already present and installed by the Zenitel engineer.

Account / Call	Account Settings	
	Description	Configuration
▶ Audio	Name:	<input type="text"/>
▶ Direct Access Keys	Number (SIP ID):	<input type="text" value="1157"/>
▶ Relays / Outputs	Server Domain (SIP):	<input type="text" value="devconnect.local"/>
▶ Time	Backup Domain (SIP):	<input type="text"/>
▶ Keyboard	Backup Domain 2 (SIP):	<input type="text"/>
▶ RTSP	Registration Method:	Parallel <input type="button" value="v"/>
▶ Audio Messages	Authentication User Name:	<input type="text" value="1157"/>
▶ Multicast Paging	Authentication Password:	<input type="text" value="...."/>
▶ Language	Register Interval:	<input type="text" value="100"/> (min. 30 seconds)
▶ Certificates	Register Failure Interval:	<input type="text" value="60"/> (min. 5 seconds)
	Outbound Proxy [optional]:	<input type="text" value="10.10.40.32"/> Port: <input type="text" value="5061"/>
	Outbound Backup Proxy [optional]:	<input type="text"/> Port: <input type="text" value="5060"/>
	Outbound Backup Proxy 2 [optional]:	<input type="text"/> Port: <input type="text" value="5060"/>
	Outbound Transport:	TLS <input type="button" value="v"/>
	SIP Scheme:	sips <input type="button" value="v"/> Using sips forces all proxies to also use TLS
	RTP Encryption:	srtp_encryption <input type="button" value="v"/>
	SRTP Crypto Type:	AES_CM_128_HMAC_SHA1_80 <input type="button" value="v"/>
	Use Unencrypted SRTCP:	<input checked="" type="checkbox"/>
	Verify TLS hostname:	<input type="checkbox"/>
	TLS Private Key:	turbine_server_sha256.key <input type="button" value="v"/>

In the **Call Settings** section, configure as required the **DTMF method** as **RFC 2833** or whatever is set on Communication Manager. Configure other options as required. Click **SAVE** when done and a screen will appear (shown on the next page) to confirm the setting. The **Codec** is also set here, with **g711a** being set with the highest priority, as shown in the example below.

Call Settings	
Description	Configuration
Enable Auto Answer:	<input type="checkbox"/>
Auto Answer Delay:	0 seconds. Max 30 seconds.
Press and Hold Time:	0 seconds. Max 60 seconds. Defines how long a DAK key/Input must be pressed before the call is established.
Max Trying Time:	15 How long to wait on response before hanging up.
Max Ringing Time:	120 How long a call can be ringing before hanging up.
Max Conversation Time:	3600 How long a call can be in conversation before hanging up.
Max MP114 Speech Time:	0 How long between MP114 speech start/end before hanging up.
Max Queued Time:	20 How long a call can be queued before hanging up.
Max Queued Calls:	4 How many incoming calls can be queued. Max 5.
Use NAT Keep Alive:	<input type="checkbox"/>
Dialing Method:	Enbloc Dialing ▾
Enbloc Dialing Timeout:	No Timeout ▾
DTMF method:	RFC 2833 ▾
Conversation Mode:	Duplex ▾
PTT Mode:	Mic and speaker is controlled by PTT button ▾
Resume Call Automatically:	<input type="checkbox"/> Resume Call On-Hold Automatically After Emergency Priority Ends
Remote Controlled Audio Direction:	<input type="checkbox"/> (Received DTMF * to listen, DTMF # to talk, DTMF 0 for open duplex)
SIP Message Controlled Audio Direction:	<input type="checkbox"/> (SIP MESSAGE controls audio direction)
Boost Volume on Push To Talk:	<input type="checkbox"/>
Override Remote Push To Talk:	<input type="checkbox"/>
Force Open Duplex Using DTMF:	- ▾
Send DTMF */# with M key:	<input type="checkbox"/>
RTP Timeout value:	0 seconds. 0 = RTP Timeout Disabled.
SIP OPTIONS Timeout value:	0 seconds. 0 = SIP OPTIONS Timeout Disabled.
Codec g729:	Low Priority ▾
Codec g722:	Low Priority ▾
Codec g711a:	High Priority ▾
Codec g711u:	Low Priority ▾

SAVE

At this point the phone needs to be rebooted in order to save the SIP configuration, however this can be rebooted at a later stage should one wish to proceed with the configuration.

▶ Audio	SIP ID: 1157
▶ Direct Access Keys	SIP Domain: devconnect.local
▶ Relays / Outputs	SIP Backup Domain:
▶ Time	SIP Backup Domain 2:
▶ Keyboard	Registration Method: Parallel
▶ RTSP	SIP Authentication Username: 1157
▶ Audio Messages	SIP Registration Interval updated: 100
▶ Multicast Paging	SIP Registration Fail Interval updated: 60
▶ Language	SIP Outbound Proxy Address: 10.10.40.32
▶ Certificates	SIP Outbound Proxy Port: 5060
	SIP Outbound Proxy Backup Address:
	SIP Outbound Proxy Port: 5060
	SIP Outbound Proxy Backup Address 2:
	SIP Outbound Proxy Port 2: 5060
	Outbound Transport: TCP
	SIP Scheme: sip
	RTP Encryption: disabled
	SRTP Crypto Type: AES_CM_128_HMAC_SHA1_80
	TLS Private Key: turbine_server_sha256.key
	Using Unencrypted SRTCP
	Not using Verify TLS hostname
	RTP timeout value: 0
	SIP OPTIONS timeout value: 0
	Auto answer mode: OFF
	Delay Call Setup: 0
	Max Trying Time: 15
	Max Ringing Time: 120
	Max Conversation Time: 3600
	Max Queued Time: 20
	Max Queued Calls: 4
	Max MP114 Speech Time: 0
	Use NAT keepalive: OFF
	Enbloc Dialing: ON
	Enbloc Dialing Timeout: 0 seconds
	DTMF method: RFC2833
	Default speaking mode: Open Duplex
	Resume Call Automatically: OFF
	Remote Controlled Volume Override Mode: OFF
	Message Controlled Volume Override Mode: OFF
	Not overriding remote Push To Talk
	Not boosting Volume On Push To Talk
	Send DTMF */# using M key: FALSE
	Configuration Saved!
	These changes require a reboot
	REBOOT

7.4. Configure Direct Access Keys

Click on the **Direct Access Keys** in the left window, this will bring up the functions as shown below where an extension to call can be assigned to the call button of the IP OR Master Intercom. This extension was an Avaya telephone, so when the button is pressed this telephone is called. **Button 1** is set to call **Ringlist 1** which is a list of Avaya phones to be called in sequence. **Button 2** is set to call a specific Avaya extension **1003**. In the **Idle** field, select **Call To** from the drop down and enter the extension to be called when the button key is pushed. In the **Call** field, select **Answer/End Call** and **On Key Press**. The buttons can be changed to use Hold or Transfer and other call features should they be required, Buttons 3 and 4 are examples of such.

Main	SIP Configuration	Station Administration	Advanced SIP	Advanced Network																																																									
Account Settings																																																													
<div> <div> Account / Call Audio Direct Access Keys Relays / Outputs Time Keyboard RTSP Audio Messages Multicast Paging Language Certificates </div> <div> <table border="1"> <thead> <tr> <th colspan="5">Function</th> </tr> </thead> <tbody> <tr> <td rowspan="3">Button 1</td> <td>Idle:</td> <td>Call To</td> <td></td> <td>Ringlist 1</td> </tr> <tr> <td>Call:</td> <td>Answer/End Call</td> <td>Filter Dir. No.</td> <td>On Key Press</td> </tr> <tr> <td>Hold:</td> <td>Resume Call</td> <td colspan="2"><input type="checkbox"/> Answer Group Call</td> </tr> <tr> <td rowspan="3">Button 2</td> <td>Idle:</td> <td>Call To</td> <td>1003</td> <td>No Ringlist</td> </tr> <tr> <td>Call:</td> <td>Answer/End Call</td> <td>Filter Dir. No.</td> <td>On Key Press</td> </tr> <tr> <td>Hold:</td> <td>End Call</td> <td colspan="2"><input type="checkbox"/> Answer Group Call</td> </tr> <tr> <td rowspan="3">Button 3</td> <td>Idle:</td> <td>Call To</td> <td></td> <td>No Ringlist</td> </tr> <tr> <td>Call:</td> <td>Transfer Call</td> <td>1050</td> <td></td> </tr> <tr> <td>Hold:</td> <td>End Call</td> <td colspan="2"></td> </tr> <tr> <td rowspan="3">Button 4</td> <td>Idle:</td> <td>Call To</td> <td>1050</td> <td>No Ringlist</td> </tr> <tr> <td>Call:</td> <td>Send DTMF</td> <td>DTMF 0</td> <td>DTMF 0</td> </tr> <tr> <td>Hold:</td> <td>End Call</td> <td colspan="2"></td> </tr> </tbody> </table> </div> </div>					Function					Button 1	Idle:	Call To		Ringlist 1	Call:	Answer/End Call	Filter Dir. No.	On Key Press	Hold:	Resume Call	<input type="checkbox"/> Answer Group Call		Button 2	Idle:	Call To	1003	No Ringlist	Call:	Answer/End Call	Filter Dir. No.	On Key Press	Hold:	End Call	<input type="checkbox"/> Answer Group Call		Button 3	Idle:	Call To		No Ringlist	Call:	Transfer Call	1050		Hold:	End Call			Button 4	Idle:	Call To	1050	No Ringlist	Call:	Send DTMF	DTMF 0	DTMF 0	Hold:	End Call		
Function																																																													
Button 1	Idle:	Call To		Ringlist 1																																																									
	Call:	Answer/End Call	Filter Dir. No.	On Key Press																																																									
	Hold:	Resume Call	<input type="checkbox"/> Answer Group Call																																																										
Button 2	Idle:	Call To	1003	No Ringlist																																																									
	Call:	Answer/End Call	Filter Dir. No.	On Key Press																																																									
	Hold:	End Call	<input type="checkbox"/> Answer Group Call																																																										
Button 3	Idle:	Call To		No Ringlist																																																									
	Call:	Transfer Call	1050																																																										
	Hold:	End Call																																																											
Button 4	Idle:	Call To	1050	No Ringlist																																																									
	Call:	Send DTMF	DTMF 0	DTMF 0																																																									
	Hold:	End Call																																																											

7.5. Configure Audio

Click on **Audio** in the left window, the volume of the speaker can be changed here.

Account / Call	Audio Settings	
Audio		
Direct Access Keys		
Relays / Outputs		
Time		
Keyboard		
RTSP		
Audio Messages		
Multicast Paging		
Language		
Certificates		

Description	Configuration	
Speaker Volume:	4	
Volume Override Level:	7	Sets the volume during volume override. Volume and handset override happens during Emergency Group calls.
External Speaker Volume:	0	(0 = Disable the external speaker)
External Speaker Volume Override Level:	0	Sets the external speaker volume during volume override. Volume and handset override happens during Emergency Group calls. (0 = Disabled)
Handset/Headset Microphone Sensitivity:	3	Offset gain in decibels relative to active accessory type (Handset w/Electret, Headset w/Electret or Headset w/Dynamic Mic). Default value 0dB.
Noise Reduction Level:	0	0 = disabled.
Force loudspeaker ringing:	<input checked="" type="checkbox"/>	Ringing is now always done on loudspeaker when ringing on headphones or handset.
Tone Volume:	0	(-1)=disabled, 0=default, [1..4]=[-22..-1]dB
Automatic Gain Control (AGC):	<input type="checkbox"/>	Automatic Gain Control. If speech level and environmental noise are very unstable it may be turned on.
Far-End Audio Squelch:	Disabled	Audio Squelch on Far-End Signal (suppress audio on low signal levels)
Squelch Threshold:	-60	Threshold level for suppressing audio signal Valid range: [-92..0] dBm0
Squelch Activate Delay:	100	Delay time with signal below threshold level before squelch is activated. Valid range: [0..10000] ms

SAVE

If the phone was not rebooted earlier during the SIP configuration then click the **Main** tab and then click on **Recovery** as shown below. The telephone can be rebooted from this page.

Main	SIP Configuration	Station Administration	Advanced SIP	Advanced Network
------	-------------------	------------------------	--------------	------------------

Information	Commands
Main Settings	
Recovery	

Description	Action
Full reboot	REBOOT
Partial reboot	REBOOT
Factory reset	FACTORY RESET
Factory reset with DHCP	FACTORY RESET

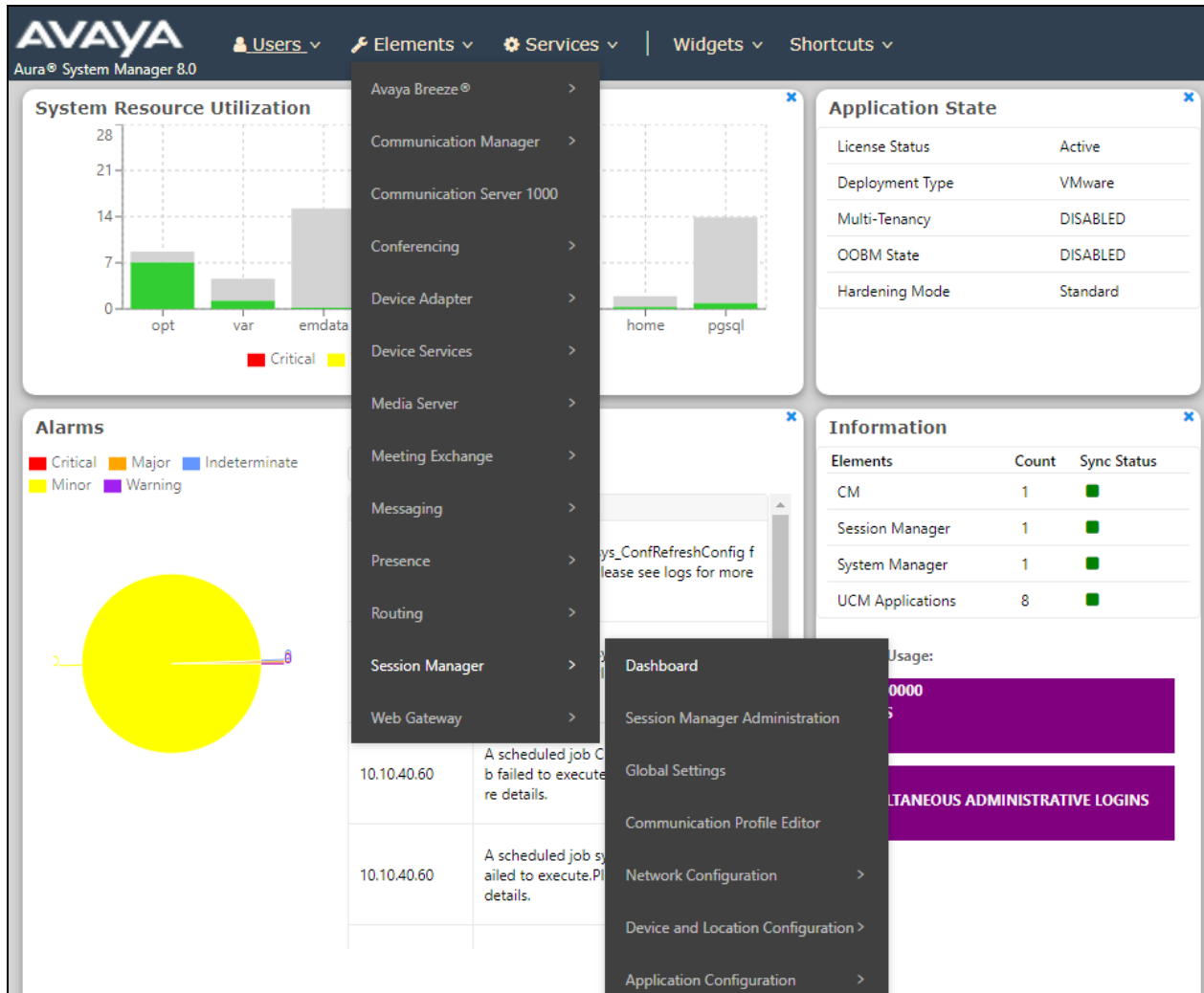
Preferences

8. Verification Steps

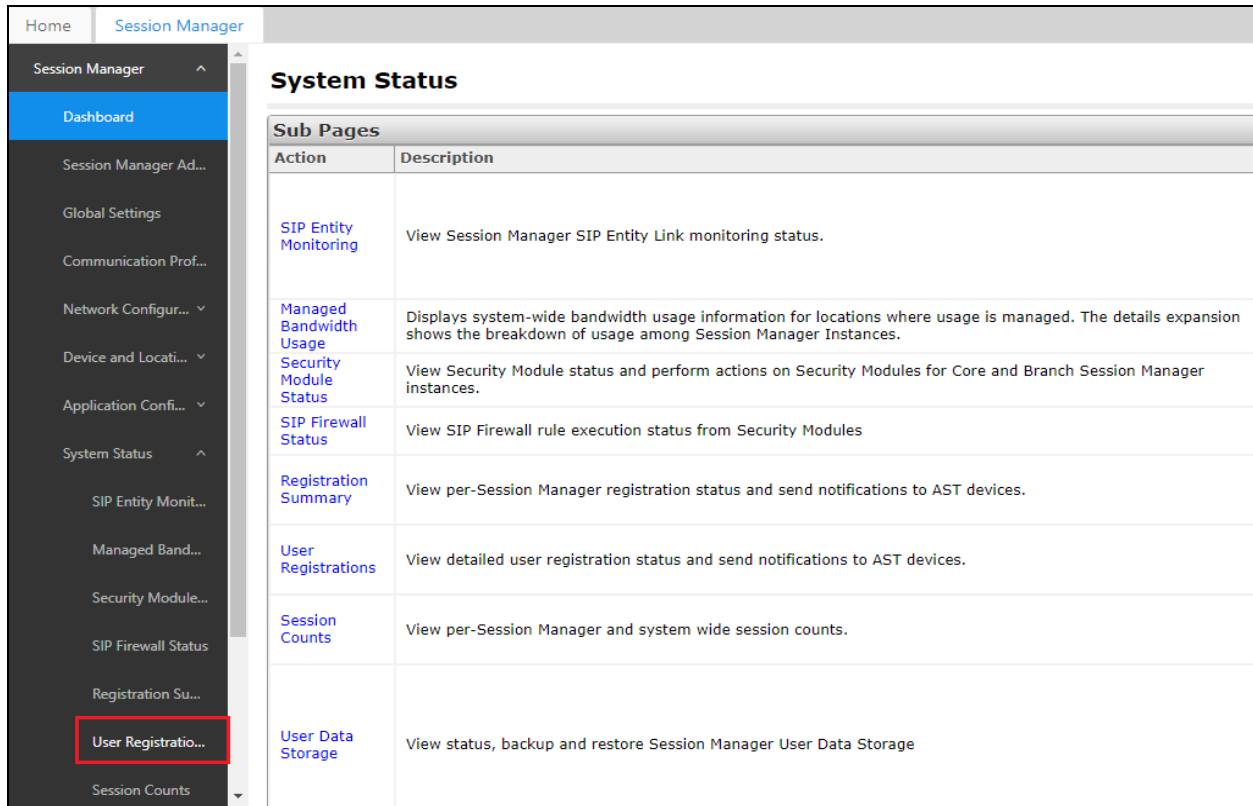
The following steps can be taken to ensure that connections between IP OR Master phones and Session Manager are up.

8.1. Session Manager Registration

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



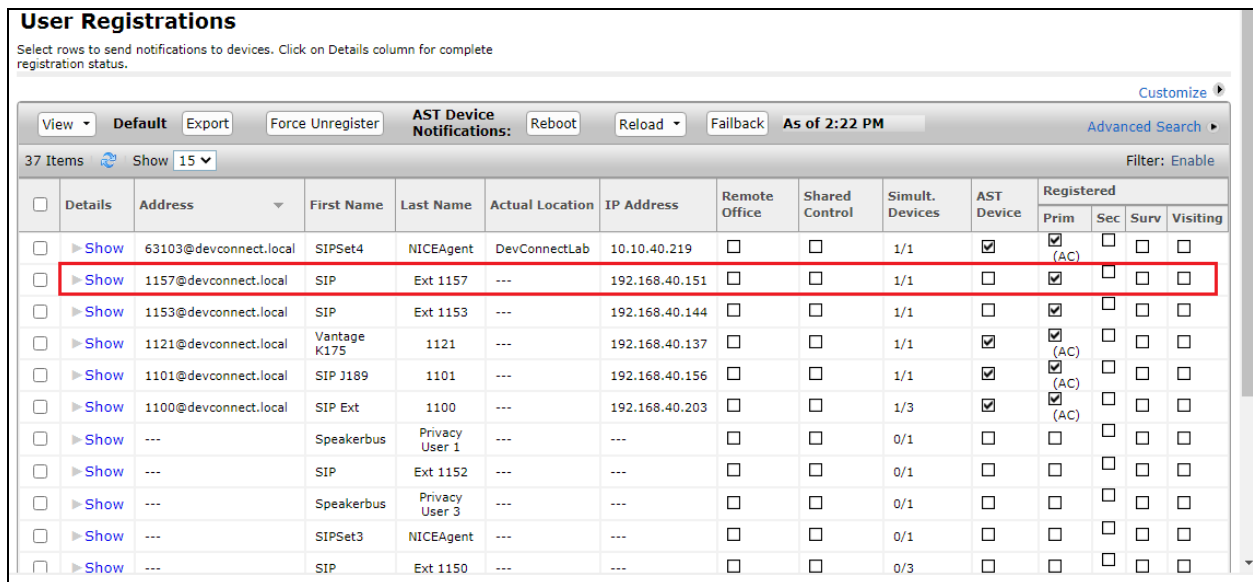
Under **System Status** in the left window, select **User Registrations** to display all the SIP users that are currently registered with Session Manager.



System Status

Action	Description
SIP Entity Monitoring	View Session Manager SIP Entity Link monitoring status.
Managed Bandwidth Usage	Displays system-wide bandwidth usage information for locations where usage is managed. The details expansion shows the breakdown of usage among Session Manager Instances.
Security Module Status	View Security Module status and perform actions on Security Modules for Core and Branch Session Manager Instances.
SIP Firewall Status	View SIP Firewall rule execution status from Security Modules
Registration Summary	View per-Session Manager registration status and send notifications to AST devices.
User Registrations	View detailed user registration status and send notifications to AST devices.
Session Counts	View per-Session Manager and system wide session counts.
User Data Storage	View status, backup and restore Session Manager User Data Storage

The user(s) should show as being registered as seen below.



User Registrations

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

View: Default Export Force Unregister AST Device Notifications: Reboot Reload Fallback As of 2:22 PM Advanced Search Customize

37 Items Show 15 Filter: Enable

	Details	Address	First Name	Last Name	Actual Location	IP Address	Remote Office	Shared Control	Simult. Devices	AST Device	Registered			
											Prim	Sec	Surv	Visiting
<input type="checkbox"/>	Show	63103@devconnect.local	SIPSet4	NICEAgent	DevConnectLab	10.10.40.219	<input type="checkbox"/>	<input type="checkbox"/>	1/1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> (AC)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	Show	1157@devconnect.local	SIP	Ext 1157	---	192.168.40.151	<input type="checkbox"/>	<input type="checkbox"/>	1/1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	Show	1153@devconnect.local	SIP	Ext 1153	---	192.168.40.144	<input type="checkbox"/>	<input type="checkbox"/>	1/1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	Show	1121@devconnect.local	Vantage K175	1121	---	192.168.40.137	<input type="checkbox"/>	<input type="checkbox"/>	1/1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> (AC)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	Show	1101@devconnect.local	SIP J189	1101	---	192.168.40.156	<input type="checkbox"/>	<input type="checkbox"/>	1/1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> (AC)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	Show	1100@devconnect.local	SIP Ext	1100	---	192.168.40.203	<input type="checkbox"/>	<input type="checkbox"/>	1/3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> (AC)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	Show	---	Speakerbus	Privacy User 1	---	---	<input type="checkbox"/>	<input type="checkbox"/>	0/1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	Show	---	SIP	Ext 1152	---	---	<input type="checkbox"/>	<input type="checkbox"/>	0/1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	Show	---	Speakerbus	Privacy User 3	---	---	<input type="checkbox"/>	<input type="checkbox"/>	0/1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	Show	---	SIPSet3	NICEAgent	---	---	<input type="checkbox"/>	<input type="checkbox"/>	0/1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	Show	---	SIP	Ext 1150	---	---	<input type="checkbox"/>	<input type="checkbox"/>	0/3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

8.2. Turbine Registration

To verify that the IP OR Master phone is registered correctly, log into the phone as per **Section 7**, the home page will show the following information where it can be seen if the phone is **Registered**.

IP Master Information	
Description	Information
IP Address:	192.168.40.151
Subnet Mask:	255.255.255.0
Default Gateway:	192.168.40.1
DNS Server 1:	192.168.40.1
DNS Server 2:	
MAC Address:	00:13:cb:30:01:b6
Software Version:	6.1.1.0
More Information:	Show/Hide
Status	
Description	Status
Mode:	SIP
Uptime:	up 59 minutes
Name:	
Number (SIP ID):	1157
Server Domain (SIP):	devconnect.local, Registered - Tue Apr 20 14:40:46 2021
Backup Domain (SIP):	
Backup Domain 2 (SIP):	
Outbound Proxy:	10.10.40.32:5061

9. Conclusion

These Application Notes describe the configuration steps required for Zenitel IP Operating Room Master to successfully interoperate with Avaya Aura® Communication Manager R8.1 and Avaya Aura® Session Manager R8.1 over TLS by registering the IP Operating Room Master phones with Session Manager as third-party SIP phones. 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 8.1.x
2. *Administering Avaya Aura® Session Manager*, Release 8.1.x

The Zenitel IP Operating Room Master documentation can be found by contacting Zenitel at <http://www.zenitel.com>.

Appendix

Signaling Group

display signaling-group 1	Page 1 of 3
SIGNALING GROUP	
Group Number: 1	Group Type: sip
IMS Enabled? n	Transport Method: tls
Q-SIP? n	
IP Video? y	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: SM81vmppg
Near-end Listen Port: 5061	Far-end Listen Port: 5061
	Far-end Network Region: 1
Far-end Domain:	
	Bypass If IP Threshold Exceeded? n
Incoming Dialog Loopbacks: eliminate	RFC 3389 Comfort Noise? n
DTMF over IP: rtp-payload	Direct IP-IP Audio Connections? y
Session Establishment Timer(min): 3	IP Audio Hairpinning? n
Enable Layer 3 Test? y	Initial IP-IP Direct Media? n
H.323 Station Outgoing Direct Media? n	Alternate Route Timer(sec): 6

Trunk Group Page 1

display trunk-group 1	Page 1 of 5
TRUNK GROUP	
Group Number: 1	Group Type: sip
Group Name: SIP PHONES	CDR Reports: y
Direction: two-way	COR: 1
Dial Access? n	TN: 1
Queue Length: 0	TAC: *801
Service Type: tie	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 5
  Group Type: sip

TRUNK PARAMETERS

  Unicode Name: auto

                                         Redirect On OPTIM Failure: 5000

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

Disconnect Supervision - In? y Out? y

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

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

Page 3

```
display trunk-group 1                                     Page 3 of 5
TRUNK FEATURES

  ACA Assignment? n          Measured: none          Maintenance Tests? y

Suppress # Outpulsing? n    Numbering Format: private
                               UII Treatment: shared
                               Maximum Size of UII Contents: 128
                               Replace Restricted Numbers? n
                               Replace Unavailable Numbers? n

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

  Send UCID? y

Show ANSWERED BY on Display? y

DSN Term? n
```

Page 4

```
display trunk-group 1                                     Page 4 of 5
                                     SHARED 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
```

Page 5

```
trunk-group 1                                           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
        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
```

©2021 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.