



Avaya Solution & Interoperability Test Lab

Application Notes for LifeSize Passport Connect with Avaya Aura® Session Manager and Avaya Aura® Communication Manager - Issue 1.0

Abstract

These Application Notes describe the steps required to integrate the LifeSize Passport Connect video system with Avaya Aura® Session Manager and Avaya Aura® Communication Manager using a SIP interface. LifeSize Passport Connect supports HD video and consists of the following components: LifeSize camera, codec device, and remote control. It also requires a 3rd party monitor display, preferably one that supports HD video and has an HDMI interface.

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 steps required to integrate the LifeSize Passport Connect video system with Avaya Aura® Session Manager and Avaya Aura® Communication Manager using a SIP interface. LifeSize Passport Connect supports HD video and consists of the following components: LifeSize camera, codec device, and remote control. It also requires a 3rd party monitor display, preferably one that supports HD video and has an HDMI interface.

2. General Test Approach and Test Results

To verify interoperability of the LifeSize Passport Connect video system with Communication Manager and Session Manager, voice and video calls were made between LifeSize Passport Connect, other LifeSize video systems (see **Section 4**), Avaya one-X® Communicator (SIP and H.323 versions), and the Avaya Desktop Video Device. Additional features were exercised on the Passport Connect, including auto-answer, Do Not Disturb, and audio mute.

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.

2.1 Interoperability Compliance Testing

Interoperability compliance testing covered the following features and functionality:

- Successful registration of LifeSize Passport Connect video system with Session Manager.
- Video calls between LifeSize Passport Connect and other LifeSize video systems, Avaya one-X® Communicator (SIP and H.323 versions), and the Avaya Desktop Video Device.
- Voice calls between LifeSize Passport Connect and other LifeSize video systems, Avaya one-X® Communicator (SIP and H.323 versions), and the Avaya Desktop Video Device.
- G.711 codec support.
- Caller ID display on Avaya and LifeSize endpoints.
- Auto-answer and Do Not Disturb on Passport Connect for incoming video calls.
- Audio mute on Passport Connect and Avaya endpoints for video and voice calls.
- Voice call transfer from an Avaya endpoint to another endpoint while a voice call is active with Passport Connect.
- Video mute from Avaya endpoints to Passport Connect. Initiating video mute from Passport Connect is currently not supported.
- Video call transfer from Avaya endpoints to Passport Connect. Initiating a call transfer from Passport Connect is currently not supported.
- Proper system recovery after a restart of Passport Connect and loss of IP connectivity.

2.2 Test Results

All test cases passed with the following observations:

- If Avaya one-X Communicator places a video call on hold with a LifeSize video system, only the audio portion of the video call is restored after taking the call off hold. Video is no longer available after the hold/resume. In addition to simple hold/resume scenarios, this issue also impacts other call scenarios where a call is placed on hold, such as transfers and conferences. This issue has been fixed in LifeSize firmware version 4.11.6 (2).
- If Avaya one-X Communicator places a video call on hold with a LifeSize video system, a “Call Status” screen appears in the middle of the LifeSize monitor display (blocking the view of the video call behind it). The “Call Status” screen cannot be removed until the call is terminated. This issue has been fixed in LifeSize firmware version 4.11.6 (2).

2.3 Support

For technical support on the Passport Connect video system, contact LifeSize Support via phone or website.

- **Phone:** (877) LIFESIZE or (512) 347-9300
- **Web:** http://www.lifesize.com/Support/Get_support.aspx

3. Reference Configuration

Figure 1 illustrates a sample configuration with an Avaya SIP-based network that includes the following Avaya products:

- Avaya Aura® Communication Manager running on an Avaya S8300D Server with a G450 Media Gateway. Communication Manager was configured as an Evolution Server.
- Avaya Aura® Session Manager connected to Communication Manager via a SIP trunk and acting as a Registrar/Proxy for SIP telephones and video endpoints.
- Avaya Aura® System Manager used to configure Session Manager.

In addition, a LifeSize Passport Connect video system, other LifeSize video systems (see **Section 4**), Avaya one-X Communicator (SIP and H.323 versions), and an Avaya Desktop Video Device were used for video calls. All SIP devices registered with Session Manager and were configured as Off-PBX Stations (OPS) on Communication Manager.

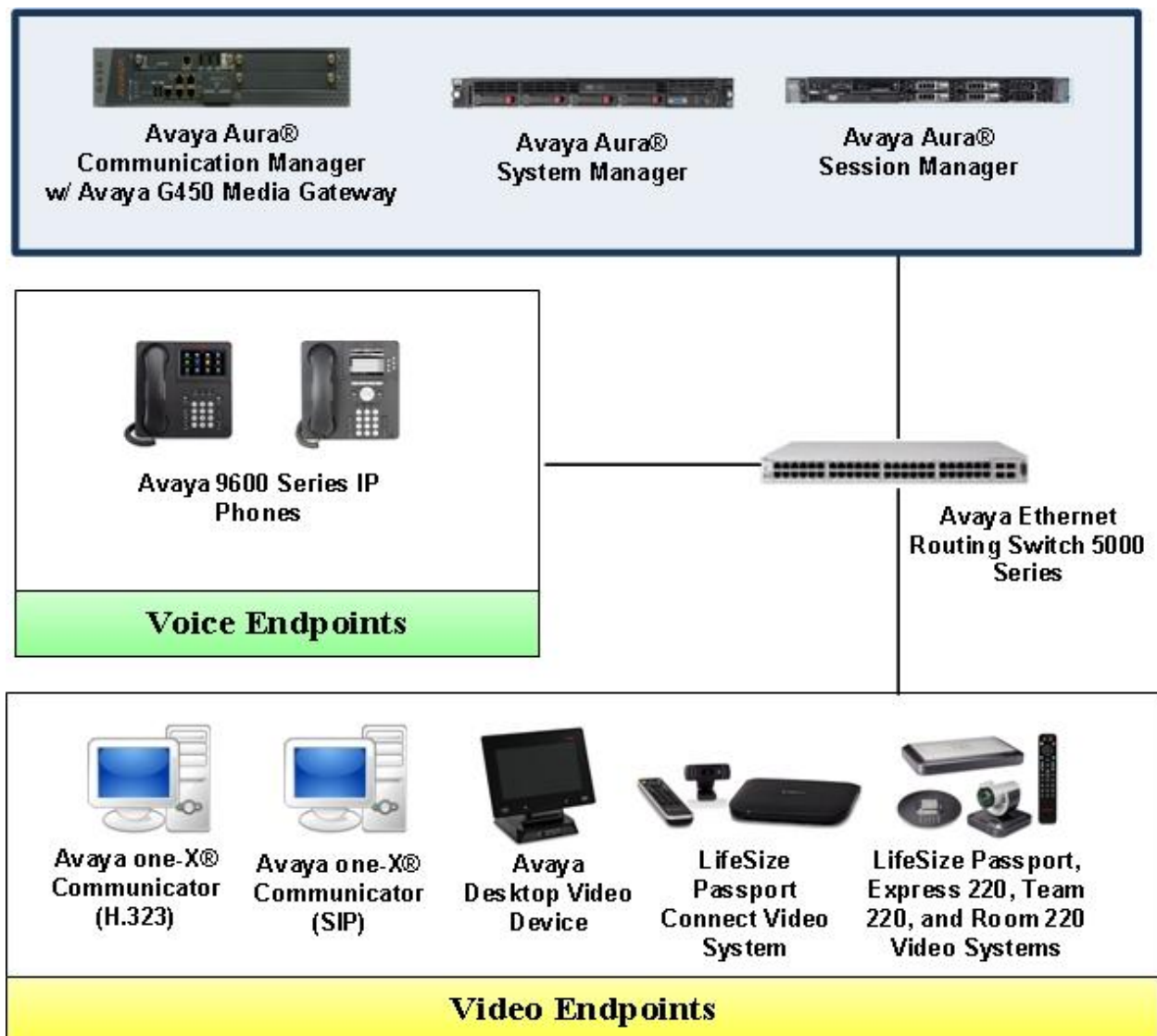


Figure 1: Avaya SIP Network with the LifeSize Passport Connect Video System

4. Equipment and Software Validated

The following equipment and software were used for the sample configuration provided:

Equipment/Software	Release/Version
HP ProLiant DL360 G7 Server	Avaya Aura® Session Manager 6.1 SP7
Dell™ PowerEdge™ R610 Server	Avaya Aura® System Manager 6.1 SP8
Avaya S8300D Server with an Avaya G450 Media Gateway	Avaya Aura® Communication Manager 6.0.1 (R016x.00.1.510.1-19736)
Avaya one-X® Communicator	6.1.3.09-SP3-Patch3-35953
Avaya 9600 Series IP Telephones <ul style="list-style-type: none">• 96x0 (SIP)• 96x1 (SIP)	Avaya one-X® Deskphone Edition SIP 2.6.7 Avaya one-X® Deskphone Edition SIP 6.1
Avaya Desktop Video Device	1.1.1
LifeSize Passport	4.11.1 (16)
LifeSize Passport Connect	4.11.1 (16)
LifeSize Express 220	4.11.1 (16)
LifeSize Team 220	4.11.1 (16)
LifeSize Room 220	4.11.1 (16)

5. Configure Avaya Aura® Communication Manager

This section provides the procedures for configuring Communication Manager. The procedures include the following areas:

- Verify Communication Manager license
- Configure Passport Connect as an Off-PBX Station (OPS)
- Configure a SIP trunk between Communication Manager and Session Manager

Use the System Access Terminal (SAT) to configure Communication Manager and log in with the appropriate credentials.

5.1 Verify OPS and SIP Trunk Capacity

Using the SAT, verify that the Off-PBX Telephones (OPS), video capable endpoints, and SIP Trunk options are enabled on the **system-parameters customer-options** form. The license file installed on the system controls these options. If a required feature is not enabled, contact an authorized Avaya sales representative.

On **Page 1**, verify that the number of OPS stations allowed in the system is sufficient for the number of SIP endpoints that will be deployed.

```
display system-parameters customer-options                               Page 1 of 11
                                OPTIONAL FEATURES

G3 Version: V16                                     Software Package: Enterprise
Location: 2                                           System ID (SID): 1
Platform: 28                                          Module ID (MID): 1

                                USED
Platform Maximum Ports: 65000 409
Maximum Stations: 41000 51
Maximum XMOBILE Stations: 41000 0
Maximum Off-PBX Telephones - EC500: 41000 0
Maximum Off-PBX Telephones - OPS: 41000 19
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 0

(NOTE: You must logoff & login to effect the permission changes.)
```

On **Page 2** of the **system-parameters customer-options** form, verify that the number of video capable endpoints and SIP trunks supported by the system is sufficient.

display system-parameters customer-options		Page 2 of 11
OPTIONAL FEATURES		
IP PORT CAPACITIES		USED
Maximum Administered H.323 Trunks:	12000	77
Maximum Concurrently Registered IP Stations:	18000	5
Maximum Administered Remote Office Trunks:	12000	0
Maximum Concurrently Registered Remote Office Stations:	18000	0
Maximum Concurrently Registered IP eCons:	414	0
Max Concur Registered Unauthenticated H.323 Stations:	100	0
Maximum Video Capable Stations:	18000	8
Maximum Video Capable IP Softphones:	18000	3
Maximum Administered SIP Trunks:	24000	180
Maximum Administered Ad-hoc Video Conferencing Ports:	24000	0
Maximum Number of DS1 Boards with Echo Cancellation:	522	0
Maximum TN2501 VAL Boards:	128	0
Maximum Media Gateway VAL Sources:	250	1
Maximum TN2602 Boards with 80 VoIP Channels:	128	0
Maximum TN2602 Boards with 320 VoIP Channels:	128	0
Maximum Number of Expanded Meet-me Conference Ports:	300	0
(NOTE: You must logoff & login to effect the permission changes.)		

5.2 Configure SIP Trunk

In the **IP Node Names** form, assign a host name and IP address for the Session Manager SIP interface. Note the processor host name of Communication Manager. The host names will be used throughout the other configuration screens of Communication Manager.

change node-names ip		Page 1 of 2
IP NODE NAMES		
Name	IP Address	
SM_21_31	10.64.21.31	
default	0.0.0.0	
msgserver	10.64.21.41	
procr	10.64.21.41	
procr6	::	

(14 of 14 administered node-names were displayed)
Use 'list node-names' command to see all the administered node-names
Use 'change node-names ip xxx' to change a node-name 'xxx' or add a node-name

In the **IP Network Region** form, the **Authoritative Domain** field is configured to match the domain name configured on Session Manager. In this configuration, the domain name is *avaya.com*. By default, **IP-IP Direct Audio** (shuffling) is enabled to allow audio traffic to be sent directly between IP endpoints without using media resources in the Avaya G450 Media Gateway. The **IP Network Region** form also specifies the **IP Codec Set** to be used for calls routed over the SIP trunk to Session Manager. This codec set is used when its corresponding network region (i.e., IP Network Region '1') is specified in the SIP signaling group.

change ip-network-region 1		Page 1 of 20
IP NETWORK REGION		
Region: 1		
Location:	Authoritative Domain: avaya.com	
Name:		
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		
Keep-Alive Count: 5		

In the **IP Codec Set** form, select the audio codec type supported for calls routed over the SIP trunk to the LifeSize Passport Connect endpoint. The form is accessed via the **change ip-codec-set 1** command. Note that IP codec set '1' was specified in IP Network Region '1' shown above. The default settings of the **IP Codec Set** form are shown below.

```
change ip-codec-set 1
```

Page 1 of 2

IP Codec Set

Codec Set: 1

Audio Codec	Silence Suppression	Frames Per Pkt	Packet Size (ms)
1: G.711MU	n	2	20
2:			

Configure **Page 2** of the **IP Codec Set** form as follows (note that other values are possible for the maximum call rates).

```
change ip-codec-set 1
```

Page 2 of 2

IP Codec Set

Allow Direct-IP Multimedia? y

Maximum Call Rate for Direct-IP Multimedia: 10240:Kbits

Maximum Call Rate for Priority Direct-IP Multimedia: 10240:Kbits

	Mode	Redundancy
FAX	t.38-standard	0
Modem	off	0
TDD/TTY	US	3
Clear-channel	n	0

Prior to configuring a SIP trunk group for communication with Session Manager, a SIP signaling group must be configured. Configure the Signaling Group form as follows:

- Set the **Group Type** field to *sip*.
- Set the **IMS Enabled** field to *n*.
- Set the **Transport Method** field to *tls*.
- Set the **IP Video** field to *y*. This is an important setting required for video calls.
- Specify the processor of Communication Manager and the Session Manager SIP interface as the two ends of the signaling group in the **Near-end Node Name** field and the **Far-end Node Name** field, respectively. These field values were taken from the **IP Node Names** form.
- Ensure that the TLS port value of *5061* is configured in the **Near-end Listen Port** and the **Far-end Listen Port** fields.
- The preferred codec for the call will be selected from the IP codec set assigned to the IP network region specified in the **Far-end Network Region** field.
- The **DTMF over IP** field should be set to the default value of *rtp-payload*. Communication Manager supports DTMF transmission using RFC 2833.
- The **Direct IP-IP Audio Connections** field was enabled on this form.
- Set the **Initial IP-IP Direct Media** field to *y*.
- The default values for the other fields may be used.

add signaling-group 1		Page 1 of 1
SIGNALING GROUP		
Group Number: 1	Group Type: sip	
IMS Enabled? n	Transport Method: tls	
Q-SIP? n	SIP Enabled LSP? n	
IP Video? y	Priority Video? n	Enforce SIPS URI for SRTP? y
Peer Detection Enabled? y Peer Server: SM		
Near-end Node Name: procr	Far-end Node Name: SM_21_31	
Near-end Listen Port: 5061	Far-end Listen Port: 5061	
	Far-end Network Region: 1	
Far-end Domain:		
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? y	
	Alternate Route Timer(sec): 20	

Configure the **Trunk Group** form as shown below. This trunk group is used for calls to SIP endpoints. Set the **Group Type** field to *sip*, set the **Service Type** field to *tie*. Set the **Member Assignment Method** to *auto*. Specify the signaling group associated with this trunk group in the **Signaling Group** field, and specify the **Number of Members** supported by this SIP trunk group. Configure the other fields in bold and accept the default values for the remaining fields.

add trunk-group 1		Page 1 of 21	
TRUNK GROUP			
Group Number: 1	Group Type: sip	CDR Reports: y	
Group Name: to SM_21_31	COR: 1	TN: 1	TAC: 101
Direction: two-way	Outgoing Display? n		
Dial Access? n	Night Service:		
Queue Length: 0			
Service Type: tie	Auth Code? n		
	Member Assignment Method: auto		
	Signaling Group: 1		
	Number of Members: 50		

On **Page 3** of the trunk group form, set the **Numbering Format** field to *unk-pvt* (other configurations are possible). This field specifies the format of the calling party number sent to the far-end.

add trunk-group 1		Page 3 of 21	
TRUNK FEATURES			
ACA Assignment? n	Measured: none	Maintenance Tests? y	
Numbering Format: unk-pvt		UII Treatment: service-provider	
		Replace Restricted Numbers? n	
		Replace Unavailable Numbers? n	
Modify Tandem Calling Number: no			
Show ANSWERED BY on Display? y			

Configure the **Private Numbering Format** form to send the calling party number to the far-end. Add an entry so that local stations with a 5-digit extension beginning with '5' whose calls are routed over any trunk group, including SIP trunk group "1", have the extension sent to the far-end for display purposes.

change private-numbering 0					Page 1 of 2
NUMBERING - PRIVATE FORMAT					
Ext	Ext	Trk	Private	Total	
Len	Code	Grp(s)	Prefix	Len	
5	5			5	Total Administered: 2
					Maximum Entries: 540

5.3 Configure Station for LifeSize Passport Connect

The **station** and **off-pbx-telephone station-mapping** configuration shown in this section was automatically performed by creating the **User** in Session Manager as described in **Section 6.7**. In this section, simply verify the settings. Note that the **User** has to be added in Session Manager first before it can be viewed on Communication Manager. Alternatively, this configuration could have also been performed manually.

Use the **display station** command to view the station created for the LifeSize Passport Connect video system and verify the settings in bold. Note that the **IP Video** field must be set to y.

display station 53169		Page 1 of 6
STATION		
Extension: 53169	Lock Messages? n	BCC: M
Type: 9630SIP	Security Code: 123456	TN: 1
Port: S00006	Coverage Path 1:	COR: 1
Name: 53169, LS Passport Connect	Coverage Path 2:	COS: 1
	Hunt-to Station:	
STATION OPTIONS		
Loss Group: 19		Time of Day Lock Table:
		Message Lamp Ext: 53169
Display Language: english	Button Modules: 0	
Survivable COR: internal		
Survivable Trunk Dest? y	IP SoftPhone? n	
IP Video? y		

Use the **display off-pbx-telephone station-mapping** command to view the mapping of the Communication Manager extensions (e.g., 53169) to the same extension configured in System Manager. Verify the field values shown. For the sample configuration, the **Trunk Selection** field is set to *aar* so that AAR call routing is used to route calls to Session Manager. AAR call routing configuration is not shown in these Application Notes. The **Configuration Set** value can reference a set that has the default settings.

change off-pbx-telephone station-mapping 53169							Page	1	of	3
STATIONS WITH OFF-PBX TELEPHONE INTEGRATION										
Station	Application	Dial	CC	Phone Number	Trunk	Config	Dual			
Extension		Prefix			Selection	Set	Mode			
53169	OPS	-		53169	aar	1				

6. Configure Avaya Aura® Session Manager

This section provides the procedures for configuring Session Manager. The procedures include adding the following items:

- SIP domain
- Logical/physical Locations that can be occupied by SIP Entities
- SIP Entities corresponding to Session Manager and Communication Manager
- Entity Links, which define the SIP trunk parameters used by Session Manager when routing calls to/from SIP Entities
- Define Communication Manager as Administrable Entity (i.e., Managed Element)
- Application Sequence
- Session Manager, corresponding to the Session Manager Server to be managed by System Manager
- Add SIP User

Configuration is accomplished by accessing the browser-based GUI of System Manager using the URL “https://<ip-address>/SMGR”, where <ip-address> is the IP address of System Manager. Log in with the appropriate credentials. The initial screen is displayed as shown below. The configuration in this section will primarily be performed under **Routing** and **Session Manager** listed within the **Elements** box.



Avaya Aura® System Manager 6.1

[Help](#) | [About](#) | [Change Password](#) | [Log off admin](#)

The screenshot displays the Avaya Aura System Manager 6.1 web interface. It features a header with the Avaya logo, the product name 'Avaya Aura® System Manager 6.1', and navigation links: 'Help | About | Change Password | Log off admin'. The main content area is divided into three vertical panels, each with an orange header and a white body containing a list of configuration options.

Users	Elements	Services
Administrators Manage Administrative Users	Application Management Manage applications and application certificates	Backup and Restore Backup and restore System Manager database
Groups & Roles Manage groups, roles and assign roles to users	Communication Manager Manage Communication Manager objects	Configurations Manage system wide configurations
Synchronize and Import Synchronize users with the enterprise directory, import users from file	Conferencing Conferencing	Events Manage alarms, view and harvest logs
User Management Manage users, shared user resources and provision users	Inventory Manage, discover, and navigate to elements, update element software	Licenses View and configure licenses
	Messaging Manage Messaging System objects	Replication Track data replication nodes, repair replication nodes
	Presence Presence	Scheduler Schedule, track, cancel, update and delete jobs
	Routing Network Routing Policy	Security Manage Security Certificates
	Session Manager Session Manager Element Manager	Templates Manage Templates for Communication Manager and Messaging System objects
	SIP AS 8.1 SIP AS 8.1	

6.1 Specify SIP Domain

Add the SIP domain for which the communications infrastructure will be authoritative. Select **Domains** on the left and clicking the **New** button (not shown) on the right. The following screen will then be shown. Fill in the following:

- **Name:** The authoritative domain name (e.g., *avaya.com*)
- **Type:** *sip*
- **Notes:** Descriptive text (optional).

Click **Commit**.

Since the sample configuration does not deal with any other domains, no additional domains need to be added.

The screenshot shows the Avaya Aura System Manager 6.1 web interface. The top navigation bar includes the Avaya logo, the title "Avaya Aura® System Manager 6.1", and links for "Help", "About", "Change Password", and "Log off admin". Below the navigation bar, there are tabs for "Routing" and "Home". The left sidebar contains a tree view with "Routing" expanded, showing sub-items: "Domains", "Locations", "Adaptations", "SIP Entities", "Entity Links", "Time Ranges", "Routing Policies", "Dial Patterns", "Regular Expressions", and "Defaults". The main content area is titled "Domain Management" and shows a table with one item. The table has columns for "Name", "Type", "Default", and "Notes". The "Name" column contains "avaya.com", the "Type" column contains "sip", and the "Default" column contains a checkbox. The "Notes" column is empty. Below the table, there is a red asterisk and the text "* Input Required". At the bottom right of the main content area, there are "Commit" and "Cancel" buttons. A "Help ?" link is also visible in the top right of the main content area.

Name	Type	Default	Notes
avaya.com	sip	<input type="checkbox"/>	

6.2 Add Locations

Locations can be used to identify logical and/or physical locations where SIP Entities reside for purposes of bandwidth management. To add a location, select **Locations** on the left and click on the **New** button (not shown) on the right. The following screen will then be shown. Fill in the following:

Under *General*:

- **Name:** A descriptive name.
- **Notes:** Descriptive text (optional).

Under *Location Pattern*:

- **IP Address Pattern:** A pattern used to logically identify the location.
- **Notes:** Descriptive text (optional).

The screen below shows addition of the *.21 Subnet* location, which includes Communication Manager and Session Manager. Click **Commit** to save the Location definition.



Avaya Aura® System Manager 6.1

[Help](#) | [About](#) | [Change Password](#) | [Log off admin](#)

Routing

Home

Home / Elements / Routing / Locations - Location Details

Location Details

CommitCancelHelp ?

Call Admission Control has been set to ignore SDP. All calls will be counted using the Default Audio Bandwidth.
See Session Manager -> Session Manager Administration -> Global Setting

Routing

Domains

Locations

Adaptations

SIP Entities

Entity Links

Time Ranges

Routing Policies

Dial Patterns

Regular Expressions

Defaults

General

* Name: .21 Subnet

Notes:

Overall Managed Bandwidth

Managed Bandwidth Units: Kbit/sec

Total Bandwidth:

Per-Call Bandwidth Parameters

* Default Audio Bandwidth: 80 Kbit/sec

Location Pattern

AddRemove

1 Item RefreshFilter: Enable

IP Address Pattern	Notes
* 10.64.21.*	

Select : All, None

6.3 Add SIP Entities

In the sample configuration, a SIP Entity is added for Session Manager and Communication Manager.

6.3.1 Session Manager

A SIP Entity must be added for Session Manager. To add a SIP Entity, select **SIP Entities** on the left and click on the **New** button (not shown) on the right. The following screen is displayed. Fill in the following:

Under *General*:

- **Name:** A descriptive name.
- **FQDN or IP Address:** IP address of the signaling interface on Session Manager.
- **Type:** Select *Session Manager*.
- **Location:** Select the location defined previously.
- **Time Zone:** Time zone for this location.

Under *Port*, click **Add**, and then edit the fields in the resulting new row as shown below:

- **Port:** Port number on which the system listens for SIP requests.
- **Protocol:** Transport protocol to be used to send SIP requests.
- **Default Domain** The domain used for the enterprise (e.g., *avaya.com*).

Defaults can be used for the remaining fields. Click **Commit** to save each SIP Entity definition.

[Routing](#) [Home](#)

Routing

- Domains
- Locations
- Adaptations
- SIP Entities**
- Entity Links
- Time Ranges
- Routing Policies
- Dial Patterns
- Regular Expressions
- Defaults

[Home](#) / [Elements](#) / [Routing](#) / [SIP Entities](#) - SIP Entity Details

SIP Entity Details

[Help ?](#)[Commit](#) [Cancel](#)

General

* Name: SM_21_31

* FQDN or IP Address: 10.64.21.31

Type: Session Manager

Notes: local SM (subnet 21)

Location:

Outbound Proxy:

Time Zone: America/Denver

Credential name:

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

Entity Links

[Add](#) [Remove](#)

26 Items [Refresh](#) Filter: Enable

<input type="checkbox"/>	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy
<input type="checkbox"/>	SM_21_31	TCP	* 5060	AAM_21_72	* 5060	Trusted
<input type="checkbox"/>	SM_21_31	TCP	* 5060	Alliance	* 5060	Trusted
<input type="checkbox"/>	SM_21_31	UDP	* 5060	Alliance	* 5060	Trusted
<input type="checkbox"/>	SM_21_31	TCP	* 5060	AASBC_22_112	* 5060	Trusted
<input type="checkbox"/>	SM_21_31	TLS	* 5061	CM_20_72	* 5061	Trusted

Select : All, None < Previous Page 1 of 6 Next >

Port

[Add](#) [Remove](#)

4 Items [Refresh](#) Filter: Enable

<input type="checkbox"/>	Port	Protocol	Default Domain	Notes
<input type="checkbox"/>	5060	UDP	avaya.com	
<input type="checkbox"/>	5060	TCP	avaya.com	
<input type="checkbox"/>	5061	TLS	avaya.com	
<input type="checkbox"/>	5063	TCP	avaya.com	

Select : All, None

* Input Required

[Commit](#) [Cancel](#)

6.3.2 Communication Manager

A SIP Entity must be added for the Communication Manager. To add a SIP Entity, select **SIP Entities** on the left and click on the **New** button (not shown) on the right. The following screen is displayed. Fill in the following:

Under *General*:

- **Name:** A descriptive name.
- **FQDN or IP Address:** IP address of the signaling interface (e.g., C-LAN board) on the telephony system.
- **Type:** Select *CM*.
- **Location:** Select the location defined previously.
- **Time Zone:** Time zone for this location.

Defaults may be used for the remaining fields. Click **Commit** to save the SIP Entity definition.



Avaya Aura® System Manager 6.1

[Help](#) | [About](#) | [Change Password](#) | [Log off admin](#)

[Routing](#) * [Home](#)

[Home](#) / [Elements](#) / [Routing](#) / [SIP Entities](#) - SIP Entity Details

[Help ?](#)

[Commit](#) [Cancel](#)

SIP Entity Details

General

* Name:

* FQDN or IP Address:

Type:

Notes:

Adaptation:

Location:

Time Zone:

Override Port & Transport with DNS SRV: ☐

* SIP Timer B/F (in seconds):

Credential name:

Call Detail Recording:

SIP Link Monitoring

SIP Link Monitoring:

Entity Links

[Add](#) [Remove](#)

1 Item [Refresh](#) Filter: Enable

<input type="checkbox"/>	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy
<input type="checkbox"/>	<input type="text" value="SM_21_31"/>	<input type="text" value="TLS"/>	<input type="text" value="* 5061"/>	<input type="text" value="CM_21_41"/>	<input type="text" value="* 5061"/>	<input type="text" value="Trusted"/>

Select : All, None

* Input Required

[Commit](#) [Cancel](#)

6.4 Add Entity Link

The SIP trunk from Session Manager to Communication Manager is described by an Entity link. To add an Entity Link, select **Entity Links** on the left and click on the **New** button (not shown) on the right. Fill in the following fields in the new row that is displayed:

- **Name:** A descriptive name.
- **SIP Entity 1:** Select the Session Manager.
- **Protocol:** Select the appropriate protocol.
- **Port:** Port number to which the other system sends SIP requests.
- **SIP Entity 2:** Select the name of Communication Manager.
- **Port:** Port number on which the other system receives SIP requests.
- **Connection Policy:** Select **Trusted**. *Note: If **Trusted** is not selected, calls from the associated SIP Entity specified in Section 6.3.2 will be denied.*

Click **Commit** to save the Entity Link definition.

Avaya Aura® System Manager 6.1

Help | About | Change Password | Log off admin

Routing * Home

Home / Elements / Routing / Entity Links - Entity Links

Entity Links

Commit Cancel

1 Item Refresh Filter: Enable

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Notes
* CM_21_41	* SM_21_31	TLS	* 5061	* CM_21_41	* 5061	Trusted	Mike

* Input Required

Commit Cancel

6.5 Define Communication Manager as Managed Element

Before adding SIP users, Communication Manager must be added to System Manager as a managed element. This action allows System Manager to access Communication Manager over its administration interface. Using this administration interface, System Manager will notify Communication Manager when new SIP users are added.

To define Communication Manager as a managed element, select **Elements→Inventory→Manage Elements** on the left and click on the **New** button (not shown) on the right. In the **New Entities Instance** screen (not shown), select **CM** in the **Type** field can click **Commit**.

In the **New CM Instance** screen, fill in the following fields as follows:

In the *Application* tab:

- **Name:** Enter an identifier for Communication Manager.
- **Type:** Select **CM** from the drop-down field.
- **Node:** Enter the IP address of the administration interface for Communication Manager.

The screenshot shows the Avaya Aura System Manager 6.1 interface. The top navigation bar includes the Avaya logo, the title 'Avaya Aura® System Manager 6.1', and links for 'Help | About | Change Password | Log off admin'. Below the navigation bar, there's a breadcrumb trail: 'Home / Elements / Inventory / Manage Elements - New CM Instance'. The left sidebar shows a tree view with 'Inventory' expanded, containing 'Manage Elements', 'Discovered Inventory', 'Discovery Management', and 'Synchronization'. The main content area is titled 'New CM Instance' and has 'Commit' and 'Cancel' buttons. It features two tabs: 'Application' (selected) and 'Attributes'. The 'Application' tab contains several fields: 'Name' (text input with value 'CM_21_41'), 'Type' (dropdown menu with 'CM' selected and a 'Reset' button), 'Description' (text area), and 'Node' (text input with value '10.64.21.41'). Below these fields are sections for 'Access Point' and 'Port', each with a dropdown arrow. At the bottom left, there's a legend indicating that an asterisk (*) denotes a required field. At the bottom right, there are 'Commit' and 'Cancel' buttons.

In the *Attributes* tab:

- **Login / Password:** Enter the login and password used for administration access.
- **Is SSH Connection:** Enable SSH access.
- **Port:** Enter the port number for SSH administration access (5022).

Defaults can be used for the remaining fields. Click **Commit** to save the settings.

AVAYA Avaya Aura® System Manager 6.1 [Help](#) | [About](#) | [Change Password](#) | [Log off admin](#)

[Inventory](#) [Home](#)

[Home](#) / [Elements](#) / [Inventory](#) / [Manage Elements - New CM Instance](#) [Help ?](#)

New CM Instance

[Commit](#) [Cancel](#)

Application **Attributes**

SNMP Attributes

*** Version** ☒ None ☐ V1 ☐ V3

Attributes

*** Login**

Password

Confirm Password

Is SSH Connection ☒

*** Port**

Alternate IP Address

RSA SSH Fingerprint (Primary IP)

RSA SSH Fingerprint (Alternate IP)

Is ASG Enabled ☐

ASG Key

6.6 Add Application Sequence

To define an application for Communication Manager, navigate to **Elements → Session Manager → Application Configuration → Applications** on the left and select **New** button (not shown) on the right. Fill in the following fields:

- **Name:** Enter name for application.
- **SIP Entity:** Select the Communication Manager SIP entity.
- **CM System for SIP Entity** Select the Communication Manager managed element.

Click **Commit** to save the Application definition.

The screenshot shows the Avaya Aura System Manager 6.1 web interface. The top navigation bar includes the Avaya logo, the title "Avaya Aura® System Manager 6.1", and links for "Help | About | Change Password | Log off admin". Below the navigation bar, there are tabs for "Session Manager" and "Home". The left sidebar contains a tree view with the following items: Session Manager, Dashboard, Session Manager, Administration, Communication Profile Editor, Network Configuration, Device and Location Configuration, Application Configuration, Applications (highlighted), Application Sequences, Implicit Users, NRS Proxy Users, System Status, and System Tools. The main content area is titled "Application Editor" and contains the following fields:

- Name:** CM_21_41
- SIP Entity:** CM_21_41
- CM System for SIP Entity:** CM_21_41 (with a Refresh button and a link to View/Add CM Systems)
- Description:** CM Evolution Server

Below these fields is a section titled "Application Attributes (optional)" which contains a table with two columns: Name and Value.

Name	Value
Application Handle	
URI Parameters	

At the bottom of the form, there is a "Commit" button and a "Cancel" button. A legend indicates that fields marked with an asterisk (*) are required.

Next, navigate to **Elements → Session Manager → Application Configuration → Application Sequences** to define the Application Sequence for Communication Manager as shown below. Provide a **Name** for the Application Sequence and under **Available Applications**, click on the plus (+) sign by **CM_21_41** to add it under the **Application in this sequence** section.

Verify a new entry is added to the **Applications in this Sequence** table and the **Mandatory** column is  as shown below.

Note: The Application Sequence defined for Communication Manager Evolution Server can only contain a single Application.



Session Manager

Dashboard

Session Manager

Administration

Communication Profile Editor

Network Configuration

Device and Location Configuration

Application Configuration

Applications

Application Sequences

Implicit Users

NRS Proxy Users

System Status

System Tools

[Home](#) / [Elements](#) / [Session Manager](#) / [Application Configuration](#) / [Application Sequences - Application Sequences](#)

[Help ?](#)

Application Sequence Editor

Application Sequence

***Name**

Description

Applications in this Sequence

1 Item	Sequence Order (first to last)	Name	SIP Entity	Mandatory	Description
<input type="checkbox"/>	<input type="checkbox"/>	CM_21_41	CM_21_41	<input checked="" type="checkbox"/>	CM Evolution Server

Select : All, None

Available Applications

12 Items Refresh
Filter: Enable

	Name	SIP Entity	Description
<input type="checkbox"/>	Call Blocker	FT_21_211	Foundation Toolkit - Call Blocker
<input type="checkbox"/>	Call Director	FT_21_211	Foundation Toolkit - Call Director
<input type="checkbox"/>	Call Screening	FT_21_211	Foundation Toolkit - Screen Incoming Calls

6.7 Add SIP User

Add a SIP user for LifeSize Passport Connect. The following configuration will automatically create the SIP station on Communication Manager Evolution Server.

To add new SIP users, navigate to **Users → User Management → Manage Users** from the left and select **New** button (not shown) on the right.

Enter values for the following required attributes for a new SIP user in the **Identity** tab of the new user form.

- **Last Name:** Enter the last name of the user.
- **First Name:** Enter the first name of the user.
- **Login Name:** Enter <extension>@<sip domain> of the user (e.g., 53169@avaya.com).
- **Authentication Type:** Select *Basic*.
- **Password:** Enter the password which will be used to log into System Manager
- **Confirm Password:** Re-enter the password from above.

The screen below shows the information when adding a new SIP user to the sample configuration.

[User Management](#) * [Home](#)

[Home](#) / [Users](#) / [User Management](#) / [Manage Users - New User Profile](#)

User Management

Manage Users

Public Contacts

Shared Addresses

System Presence ACLs

[Help ?](#)

New User Profile

Identity *
Communication Profile *
Membership
Contacts

Identity ▾
▾

* Last Name:

* First Name:

Middle Name:

Description:

* Login Name:

* Authentication Type:

* Password:

* Confirm Password:

Localized Display Name:

Endpoint Display Name:

Honorific:

Language Preference:

Time Zone:

*Required

Enter values for the following required attributes for a new SIP user in the **Communication Profile** tab of the new user form.

- **Communication Profile Password:** Enter the password which will be used by Passport Connect to register with Session Manager.
- **Confirm Password:** Re-enter the password from above.

Scroll down to the **Communication Address** section and select **New** to define a **Communication Address** for the new SIP user. Enter values for the following required fields:

- **Type:** Select *Avaya SIP*.
- **Fully Qualified Address:** Enter extension number and select SIP domain.

The screen below shows the information when adding a new SIP user to the sample configuration. Click **Add**.

MJH; Reviewed:
SPOC 10/1/2012

Solution & Interoperability Test Lab Application Notes
©2012 Avaya Inc. All Rights Reserved.

26 of 41
LifeSizePPC-SM61



[User Management](#) [Home](#)

Home / Users / User Management / Manage Users - New User Profile [Help ?](#)

New User Profile [Commit](#) [Cancel](#)

User Management

- Manage Users
- Public Contacts
- Shared Addresses
- System Presence ACLs

Identity *

Communication Profile *

Membership

Contacts

Communication Profile

Communication Profile Password:

Confirm Password:

[New](#) [Delete](#) [Done](#) [Cancel](#)

Name
<input checked="" type="radio"/> Primary

Select : None

* Name:

Default : ☒

Communication Address

[New](#) [Edit](#) [Delete](#)

Type	Handle	Domain
No Records found		

Type:

* Fully Qualified Address: @

[Add](#) [Cancel](#)

☐ **Session Manager Profile**

☐ **Endpoint Profile**

☐ **Messaging Profile**

* Required

[Commit](#) [Cancel](#)

In the *Session Manager Profile* section, specify the Session Manager entity from **Section 6.3.1** for **Primary Session Manager** and assign the **Application Sequence** defined in **Section 6.6** to the new SIP user as part of defining the **SIP Communication Profile**. The **Application Sequence** can be used for both the originating and terminating sequence. Set the **Home Location** field to the **Location** configured in **Section 6.2**.

☒ **Session Manager Profile** ▼

* **Primary Session Manager**

SM_21_31 ▼

Primary	Secondary	Maximum
33	0	33

Secondary Session Manager

(None) ▼

Primary	Secondary	Maximum

Origination Application Sequence

CM_21_41 ▼

Termination Application Sequence

CM_21_41 ▼

Survivability Server

(None) ▼

* **Home Location**

.21 Subnet ▼

In the **Endpoint Profile** section, fill in the following fields:

- **System:** Select the managed element corresponding to Communication Manager.
- **Profile Type** Select *Endpoint*.
- **Use Existing Stations:** If field is not selected, the station will automatically be added in Communication Manager.
- **Extension:** Enter extension number of SIP user.
- **Template:** Select template for type of SIP phone.
- **Port:** Enter *IP*.

☒ **Endpoint Profile** ▼

* **System** CM_21_41 ▼

* **Profile Type** Endpoint ▼

Use Existing Endpoints ☐

* **Extension** 53169 Endpoint Editor

* **Template** DEFAULT_9630_CM_6_0 ▼

Set Type 9630

Security Code ●●●●●●

* **Port** IP

Voice Mail Number

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

Next, click on the **Endpoint Editor** button by the **Extension** field. The following screen is displayed. In the **Feature Options** section, select **IP Video Softphone** and click **Done**. The user will be returned to the previous screen. Click the **Commit** button to save the new SIP user profile.

General Options (G) *		Feature Options (F)		Site Data (S)		Abbreviated Call Dialing (A)																	
Enhanced Call Fwd (E)		Button Assignment (B)		Group Membership (M)																			
Active Station Ringing	single	Auto Answer	none																				
MWI Served User Type	Select	Coverage After Forwarding	system																				
Per Station CPN - Send Calling Number	Select	Display Language	english																				
IP Phone Group ID		Hunt-to Station																					
Remote Soft Phone Emergency Calls	Select	Loss Group	19																				
LWC Reception	spe	Survivable COR	internal																				
AUDIX Name		Time of Day Lock Table	Select																				
Speakerphone	Select	Voice Mail Number																					
Short/Prefixed Registration Allowed	Select																						
EC500 State	enabled																						
Features <table border="1"> <tbody> <tr> <td><input type="checkbox"/> Always Use</td> <td><input type="checkbox"/> Idle Appearance Preference</td> </tr> <tr> <td><input type="checkbox"/> IP Audio Hairpinning</td> <td><input type="checkbox"/> IP SoftPhone</td> </tr> <tr> <td><input type="checkbox"/> Bridged Call Alerting</td> <td><input checked="" type="checkbox"/> LWC Activation</td> </tr> <tr> <td><input type="checkbox"/> Bridged Idle Line Preference</td> <td><input type="checkbox"/> CDR Privacy</td> </tr> <tr> <td><input checked="" type="checkbox"/> Coverage Message Retrieval</td> <td><input checked="" type="checkbox"/> Direct IP-IP Auto Connection</td> </tr> <tr> <td><input type="checkbox"/> Data Restriction</td> <td><input type="checkbox"/> H.320 Conversion</td> </tr> <tr> <td><input checked="" type="checkbox"/> Survivable Trunk Dest</td> <td><input checked="" type="checkbox"/> IP Video</td> </tr> <tr> <td><input type="checkbox"/> Bridged Appearance Origination Restriction</td> <td></td> </tr> </tbody> </table>								<input type="checkbox"/> Always Use	<input type="checkbox"/> Idle Appearance Preference	<input type="checkbox"/> IP Audio Hairpinning	<input type="checkbox"/> IP SoftPhone	<input type="checkbox"/> Bridged Call Alerting	<input checked="" type="checkbox"/> LWC Activation	<input type="checkbox"/> Bridged Idle Line Preference	<input type="checkbox"/> CDR Privacy	<input checked="" type="checkbox"/> Coverage Message Retrieval	<input checked="" type="checkbox"/> Direct IP-IP Auto Connection	<input type="checkbox"/> Data Restriction	<input type="checkbox"/> H.320 Conversion	<input checked="" type="checkbox"/> Survivable Trunk Dest	<input checked="" type="checkbox"/> IP Video	<input type="checkbox"/> Bridged Appearance Origination Restriction	
<input type="checkbox"/> Always Use	<input type="checkbox"/> Idle Appearance Preference																						
<input type="checkbox"/> IP Audio Hairpinning	<input type="checkbox"/> IP SoftPhone																						
<input type="checkbox"/> Bridged Call Alerting	<input checked="" type="checkbox"/> LWC Activation																						
<input type="checkbox"/> Bridged Idle Line Preference	<input type="checkbox"/> CDR Privacy																						
<input checked="" type="checkbox"/> Coverage Message Retrieval	<input checked="" type="checkbox"/> Direct IP-IP Auto Connection																						
<input type="checkbox"/> Data Restriction	<input type="checkbox"/> H.320 Conversion																						
<input checked="" type="checkbox"/> Survivable Trunk Dest	<input checked="" type="checkbox"/> IP Video																						
<input type="checkbox"/> Bridged Appearance Origination Restriction																							

*Required

Done Cancel

6.8 Add Session Manager

To complete the configuration, adding the Session Manager will provide the linkage between System Manager and Session Manager. Expand the **Session Manager** menu on the left and select **Session Manager Administration**. Click **Add** (not shown), and fill in the fields as described below and shown in the following screen:

Under *Identity*:

- **SIP Entity Name:** Select the name of the SIP Entity added for Session Manager
- **Description:** Descriptive comment (optional)
- **Management Access Point Host Name/IP:** Enter the IP address of the Session Manager management interface.

Under *Security Module*:

- **Network Mask:** Enter the network mask corresponding to the IP address of Session Manager
- **Default Gateway:** Enter the IP address of the default gateway for Session Manager

Use default values for the remaining fields. Click **Commit** to add this Session Manager.

AVAYA Avaya Aura® System Manager 6.1 [Help](#) | [About](#) | [Change Password](#) | [Log off admin](#)

[Session Manager](#) [Home](#)

Home / Elements / Session Manager / Session Manager Administration - Session Manager Administration [Help ?](#)

Edit Session Manager [Commit](#) [Cancel](#)

General | Security Module | NIC Bonding | Monitoring | CDR | Personal Profile Manager (PPM) - Connection Settings | Event Server |
Expand All | Collapse All

General

SIP Entity Name

Description

*Management Access Point Host Name/IP

*Direct Routing to Endpoints

Security Module

SIP Entity IP Address

*Network Mask

*Default Gateway

*Call Control PHB

*QOS Priority

*Speed & Duplex

VLAN ID

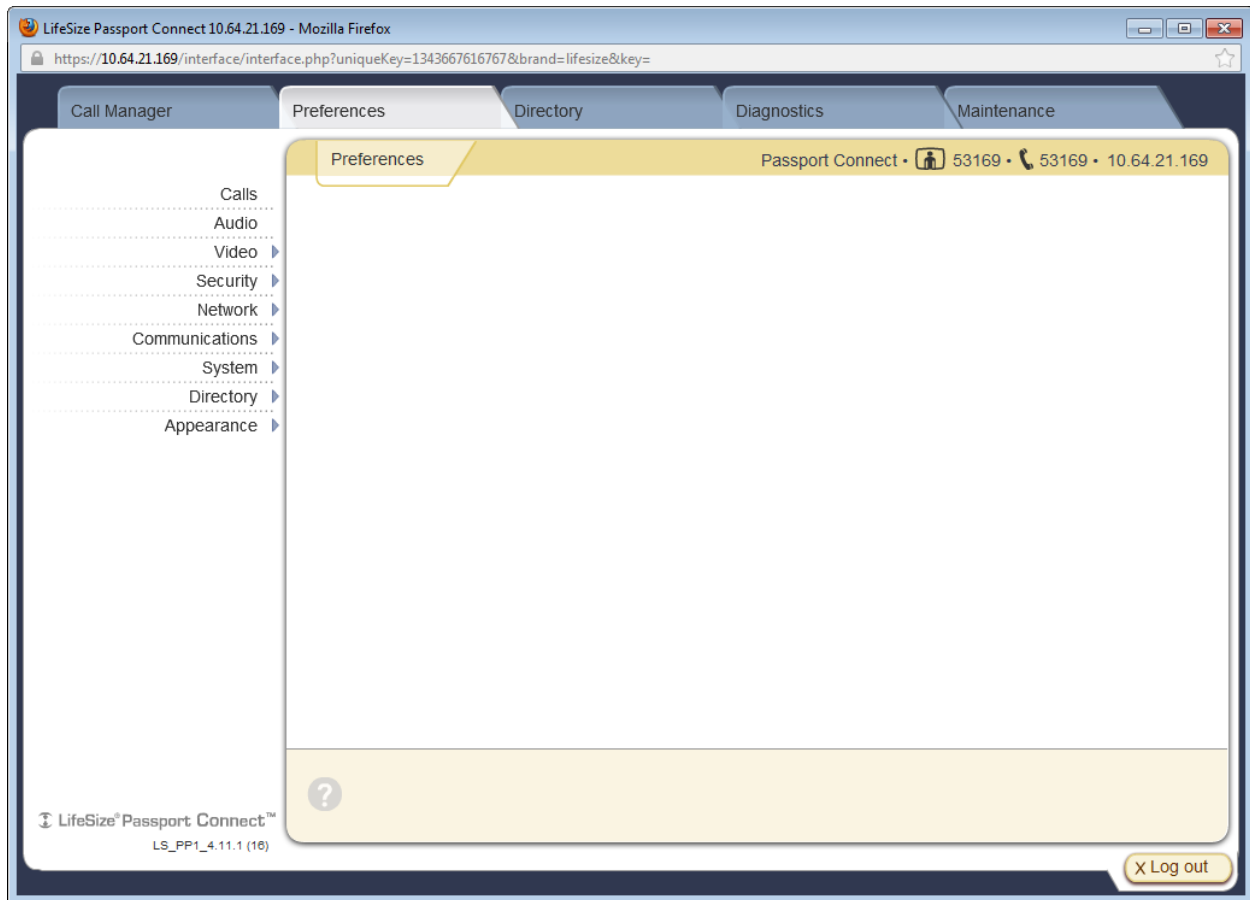
7. Configure LifeSize Passport Connect

The configuration of the LifeSize Passport Connect video system was performed via the Passport Connect's embedded Web interface or user interface on the monitor display using the remote control. However, the Passport Connect's LAN connection interface was initially configured via its monitor using the remote control. To configure the IP parameters for Passport Connect, navigate to the **System Menu** → **Administrator Preferences** and then log in with the appropriate credentials. Next, select **Network** and then select **General** to configure the LAN interface. The LAN configuration will be shown later in this section. The rest of the configuration was performed via the Passport Connect's embedded Web interface as shown in this section. Refer to reference [4] for additional information on configuring the Passport Connect video system.

From an internet browser, enter `https://<ip-addr>` in the URL field, where `<ip-addr>` is the Passport Connect's IP address. The following **Login** screen is displayed. Log in with the appropriate password.



After logging in, the main screen is displayed as shown below.



To view the LAN configuration, navigate to **Network → General**. The following screen is displayed. In this configuration, a static IP address was assigned. As mentioned earlier, the initial IP configuration was performed via the monitor using the remote control.

The screenshot shows the LifeSize Passport Connect web interface in a Mozilla Firefox browser. The address bar displays the URL: `https://10.64.21.169/interface/interface.php?uniqueKey=1343667616767&brand=lifesize&key=`. The interface has a top navigation bar with tabs: Call Manager, Preferences, Directory, Diagnostics, and Maintenance. The 'Preferences' tab is active, and within it, the 'Network • General' sub-tab is selected. A left sidebar lists various configuration categories: Preferences (expanded), General (selected), NAT, Reserved Ports, Network QoS, LifeSize Transit, and 802.1x Authentication. The main content area displays the following configuration fields:

- DHCP: Disabled (dropdown)
- IP Address: 10.64.21.169 (text input)
- Subnet Mask: 255.255.255.0 (text input)
- Default Gateway: 10.64.21.1 (text input)
- Hostname: LifeSize (text input)
- DNS Servers: 205.171.3.65 (text input)
- Name Search Domains: (text input)
- Network Speed: Auto (dropdown)
- VLAN Tag: (text input)
- NTP Server Hostname: (text input)
- 802.1x Authentication: Disabled (dropdown)

At the bottom of the configuration area, there are four buttons: Save Changes, Cancel Changes, Refresh, and Copy. Below these buttons is a yellow informational box with a question mark icon and the text: **IP Address:** Enter the static IP address of the device. The bottom left corner of the interface shows the device name 'LifeSize® Passport Connect™' and the model 'LS_FP1_4.11.1 (16)'. The bottom right corner has a 'Log out' button.

If network QoS is implemented using DiffServ, the **DiffServ Video Priority** may be configured on Passport Connect so that it tags its video RTP packets with the appropriate DiffServ value. To configure DiffServ on Passport Connect, navigate to **Network → Network QoS** to display the screen below. Set the **Network QoS** field to *DiffServ* and set the **DiffServ Video Priority** field to the appropriate value as specified by your network administrator. Click the **Save Changes** button.

The screenshot shows the 'Network • Network QoS' configuration page in the LifeSize Passport Connect web interface. The browser address bar shows the URL: `https://10.64.21.169/interface/interface.php?uniqueKey=1343667616767&brand=lifese&key=`. The page has a navigation bar with tabs: Call Manager, Preferences (selected), Directory, Diagnostics, and Maintenance. A left sidebar lists preferences: General, NAT, Reserved Ports, Network QoS (highlighted), and LifeSize Transit. The main content area is titled 'Network • Network QoS' and shows the following configuration fields:

- Network QoS:
- DiffServ Audio Priority:
- DiffServ Video Priority:
- DiffServ Data Priority:
- IntServ Audio Priority:
- IntServ Video Priority:
- IntServ Data Priority:
- IntServ ToS:

At the bottom of the configuration area are four buttons: 'Save Changes', 'Cancel Changes', 'Refresh', and 'Copy'. Below these buttons is a help section with a question mark icon and the text: 'IntServ ToS: Select the Type of Service (ToS) for IP Precedence (IntServ)'. The footer of the page includes 'LifeSize® Passport Connect™ LS_PP1_4.11.1 (16)' and a 'Log out' button.

Next, configure the Passport Connect's SIP parameters. From the main screen, navigate to **Communications** → **SIP** to display the screen below. Configure the fields as follows:

- **SIP** Set to *Enabled*.
- **SIP Username** Specify the Passport Connect's extension (e.g., 53169).
- **Authorization Name** Specify the Passport Connect's extension, which will be used to register with Session Manager.
- **Authorization Password** Specify the password used by Passport Connect to register with Session Manager
- **SIP Server Type** Set to *Auto*.
- **SIP Registration** Set to *Through Proxy*.
- **SIP Proxy** Set to *Enabled*.
- **Proxy Hostname** Specify the IP address of Session Manager's SIP interface (e.g., 10.64.21.31).
- **SIP Registrar** Set to *Enabled*.

LifeSize Passport Connect 10.64.21.169 - Mozilla Firefox

https://10.64.21.169/interface/interface.php?uniqueKey=1343667616767&brand=lifsize&key=

Call Manager Preferences Directory Diagnostics Maintenance

Communications • SIP Passport Connect • 53169 • 53169 • 10.64.21.169

Registrar Status: Registered

SIP: Enabled

SIP Username: 53169

Authorization Name: 53169

Authorization Password: *****

SIP Server Type: Auto

SIP Registration: Through Proxy

SIP Proxy: Enabled

Proxy Hostname: 10.64.21.31

SIP Registrar: Enabled

Registrar Hostname: sip.smc.com

Save Changes Cancel Changes Refresh Copy

? **Proxy Hostname:**
Enter the hostname or IP address of the SIP proxy server.

LifeSize® Passport Connect™
LS_PP1_4.11.1 (16)

X Log out

On the same **Communications** → **SIP** screen, scroll down to configure the rest of the SIP parameters as follows:

- **Registrar Hostname** Specify the IP address of Session Manager's SIP interface.
- **SIP Registrar** Set to *Enabled*.
- **Registrar Hostname** Set to *avaya.com*.
- **SIP Signaling** Set to *UDP*.
- **UDP Signaling Port** Specify the port used to communicate with Session Manager via UDP.

When the configuration is completed, click the **Save Changes** button.

The screenshot shows the 'LifeSize Passport Connect' web interface in a Mozilla Firefox browser. The address bar shows the URL: `https://10.64.21.169/interface/interface.php?uniqueKey=1343667616767&brand=lifesize&key=`. The interface has a top navigation bar with tabs: 'Call Manager', 'Preferences', 'Directory', 'Diagnostics', and 'Maintenance'. The 'Preferences' tab is active, and within it, the 'Communications • SIP' sub-tab is selected. On the left, a sidebar shows 'Preferences' expanded with 'General', 'LifeSize Connections', and 'SIP' (highlighted in orange). The main content area is titled 'Passport Connect • 53169 • 53169 • 10.64.21.169' and contains the following configuration fields:

- Proxy Hostname:
- SIP Registrar:
- Registrar Hostname:
- Internal Server:
- External Server:
- UVC Video Engine for Lync:
- SIP Signaling:
- UDP Signaling Port:
- TCP Signaling Port:
- TLS Signaling Port:

At the bottom of the configuration area, there are four buttons: 'Save Changes', 'Cancel Changes', 'Refresh', and 'Copy'. Below these buttons is a section titled 'SIP Server Type:' with the instruction 'Select the type of SIP registrar and proxy servers.' and a question mark icon. In the bottom right corner, there is a 'Log out' button.

Lastly, to display the Passport Connect's extension on the top of the monitor, configure the **Identification** screen. From the main screen, navigate to **System → Identification** and set the **Video Number** and **Voice Number** fields to the Passport Connect's extension as shown below. Click **Save Changes** when done.

The screenshot shows the LifeSize Passport Connect web interface in a Mozilla Firefox browser. The address bar displays the URL: `https://10.64.21.169/interface/interface.php?uniqueKey=1343671651430&brand=lifesize&key=`. The interface has a top navigation bar with tabs: Call Manager, Preferences, Directory, Diagnostics, and Maintenance. The 'Preferences' tab is active, and a sub-menu on the left shows 'Identification' selected. The main content area is titled 'System • Identification' and contains the following fields:

- System Name: Passport Connect
- Video Number: 53169
- Voice Number: 53169
- Location: United States (dropdown menu)

At the bottom of the form, there are four buttons: 'Save Changes', 'Cancel Changes', 'Refresh', and 'Copy'. The bottom status bar shows 'LifeSize® Passport Connect™ LS_PP1_4.11.1 (16)' on the left and a 'Log out' button on the right.

8. Verification Steps

This section provides the steps that may be performed to verify proper configuration of the LifeSize Passport Connect video system with Avaya Aura® Communication Manager and Avaya Aura® Session Manager.

1. Verify that the LifeSize system has successfully registered with Session Manager. Navigate to **Communications** → **SIP** and verify that the **Registrar Status** indicates *Registered* as shown below.

The screenshot shows the LifeSize Passport Connect web interface in a Mozilla Firefox browser. The address bar shows the URL: <https://10.64.21.169/interface/interface.php?uniqueKey=1343667616767&brand=lifesize&key=>. The interface has a top navigation bar with tabs: Call Manager, Preferences, Directory, Diagnostics, and Maintenance. The left sidebar shows a tree view with 'Preferences' expanded, containing 'General' and 'LifeSize Connections'. Under 'LifeSize Connections', 'SIP' is selected and highlighted in orange. The main content area is titled 'Communications • SIP' and shows the 'Registrar Status: Registered'. Below this, there are several configuration fields: 'SIP' (Enabled), 'SIP Username' (53169), 'Authorization Name' (53169), 'Authorization Password' (masked with asterisks), 'SIP Server Type' (Auto), 'SIP Registration' (Through Proxy), 'SIP Proxy' (Enabled), 'Proxy Hostname' (10.64.21.31), and 'SIP Registrar' (Enabled). At the bottom of the configuration area, there is a 'Registrar Hostname' field (partially visible as 'sps.com'). Below the configuration fields are buttons for 'Save Changes', 'Cancel Changes', 'Refresh', and 'Copy'. A help section at the bottom left explains the 'Proxy Hostname' field: 'Proxy Hostname: Enter the hostname or IP address of the SIP proxy server.' The bottom right corner has a 'Log out' button.

2. Place an outgoing video call from Passport Connect to another video system registered with Session Manager and verify that the video completes with 2-way audio and video.
3. Place an outgoing voice call from Passport Connect to an Avaya IP telephone and verify that the voice call completes with 2-way audio.

9. Conclusion

These Application Notes have described the administration steps required to integrate the LifeSize Passport Connect video system with Avaya Aura® Communication Manager and Avaya Aura® Session Manager. LifeSize Passport Connect successfully registered with Session Manager and voice and video calls were established with LifeSize Passport Connect, Avaya one-X Communicator and Avaya IP telephones. All test cases passed with observations noted in **Section 2.2**.

10. References

This section references the Avaya documentation relevant to these Application Notes. The following Avaya product documentation is available at <http://support.avaya.com>.

- [1] *Administering Avaya Aura® Communication Manager*, March 2012, Document Number 03-300509.
- [2] *Administering Avaya Aura® Session Manager*, July 2012, Document Number 03-603324.

The following LifeSize product documentation is available at <http://www.lifesize.com>.

- [3] *LifeSize® Video Communication Systems Installation Guide*, February 2011.
- [4] *LifeSize® Video Communication Systems User and Administrator Guide*, February 2011.

©2012 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.