Avaya Solution & Interoperability Test Lab

Application Notes for LifeSize Passport 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 video system with Avaya Aura® Session Manager and Avaya Aura® Communication Manager using a SIP interface. LifeSize Passport supports HD video and consists of the following components: LifeSize camera, codec device, and remote control. It also requires 3rd party speakers and monitor display, preferably one that support HD video and has an HDMI interface. The LifeSize Express 220 video system was also used in this compliance test.

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 video system with Avaya Aura® Session Manager and Avaya Aura® Communication Manager using a SIP interface. LifeSize Passport supports HD video and consists of the following components: LifeSize camera, codec device, and remote control. It also requires 3rd party speakers and monitor display, preferably one that support HD video and has an HDMI interface. The LifeSize Express 220 video system was also used in this compliance test.

2. General Test Approach and Test Results

To verify interoperability of the LifeSize Passport video system with Communication Manager and Session Manager, video calls were made between LifeSize Passport and LifeSize Express 220, and between LifeSize Passport and Avaya one-X® Communicator (SIP and H.323 versions). In addition, voice calls were established from LifeSize Passport to Avaya one-X® Communicator and Avaya IP telephones. Additional features were exercised on the Passport, including auto-answer, Do Not Disturb, and audio mute. See the following sub-section for additional features covered.

2.1 Interoperability Compliance Testing

Interoperability compliance testing covered the following features and functionality:

- Successful registration of LifeSize Passport with Session Manager.
- Video calls between LifeSize Passport, LifeSize Express 220 and Avaya one-X® Communicator with a SIP and H.323 interface.
- Voice calls between LifeSize Passport and Avaya one-X Communicator, Avaya Desktop Video Device, and Avaya IP telephones (SIP and H.323).
- G.711 codec support.
- Caller ID display on Avaya and LifeSize endpoints.
- Auto-answer and Do Not Disturb on Passport for incoming video calls.
- Audio mute on Passport 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.
- Video mute from one-X Communicator to Passport. Initiating video mute from Passport is currently not supported.
- Video call transfer from one-X Communicator to Passport. Initiating a call transfer from Passport is currently not supported.
- Proper system recovery after a restart of Passport and loss of IP connectivity.

2.2 Test Results

All test cases passed with the following observations:

- If Avaya one-X Communicator transfers a video call to LifeSize Passport, only the audio portion of video call is successfully transferred. Video is no longer available on the call after the call transfer.

- Video interoperability with Avaya Desktop Video Device is currently not supported.

2.3 Support

For technical support on the Passport 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 S8800 Server with a G650 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, LifeSize Express 220, and Avaya one-X Communicator (SIP and H.323 versions) were used for video calls. All SIP devices registered with Session Manager and were configured as Off-PBX Stations (OPS) on Communication Manager.

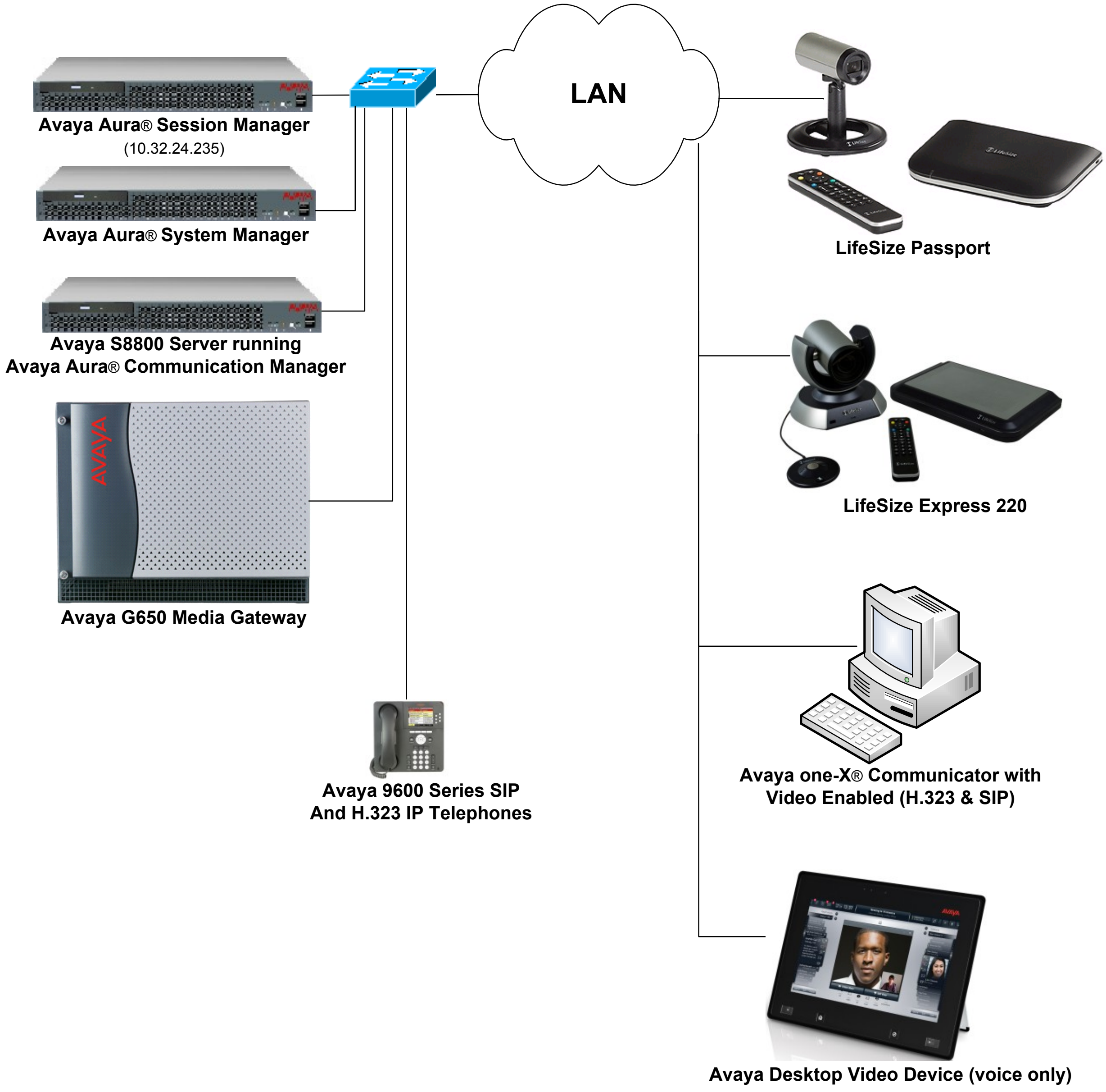

Avaya Aura® Session Manager
(10.32.24.235)
Avaya Aura® System Manager
Avaya S8800 Server running
Avaya Aura® Communication Manager
Avaya G650 Media Gateway
Avaya 9600 Series SIP
And H.323 IP Telephones
LAN
LifeSize Passport
LifeSize Express 220
Avaya one-X® Communicator with
Video Enabled (H.323 & SIP)
Avaya Desktop Video Device (voice only)

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

4. Equipment and Software Validated

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

Hardware Component	Version
Avaya S8800 Servers and G650 Media Gateway	Avaya Aura® Communication Manager 6.1 SP 1.01
Avaya Aura® Session Manager	6.1 SP 1 (6.1.0.0-610023))
Avaya Aura® System Manager	6.1.0 (6.1.0.4.5072-6.1.4.113)
Avaya one-X® Communicator	6.0 SP 1 (6.0.1.16-SP1-25226)
Avaya 9600 Series IP Telephones	3.101 (H.323) 2.6 (SIP)
Avaya Desktop Video Device (for voice calls only)	1.0.2
LifeSize Passport	4.7.0 (19)
LifeSize Express 220	4.7.0 (19)

5. Configure Communication Manager

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

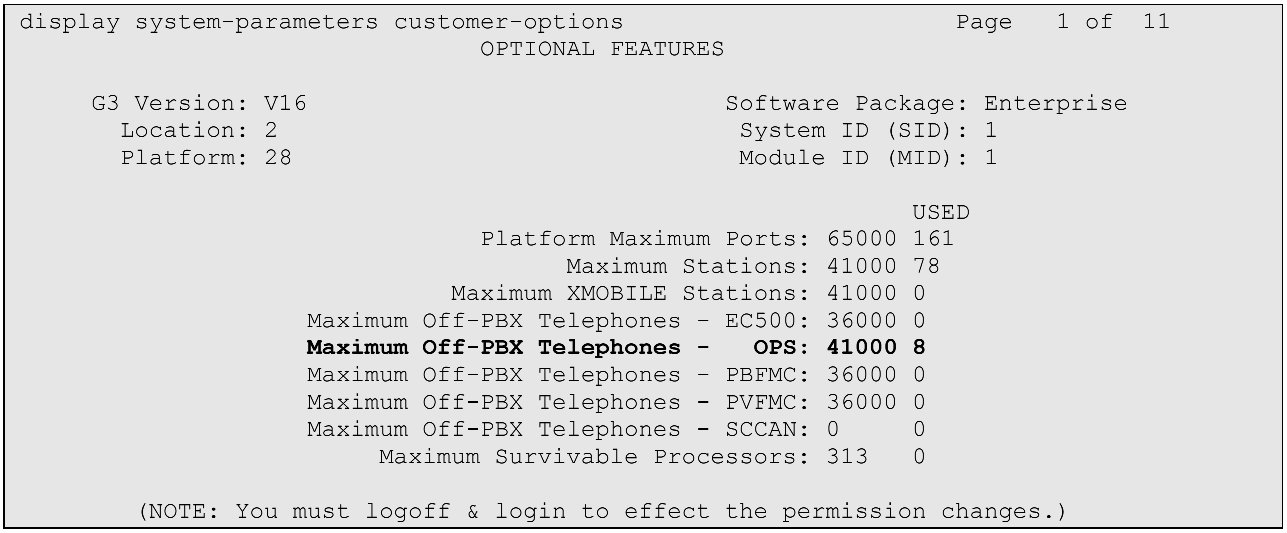
- Verify Communication Manager license
- Configure Passport as an Off-PBX Station (OPS)
- Configure a SIP trunk between Communication Manager and Session Manager

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

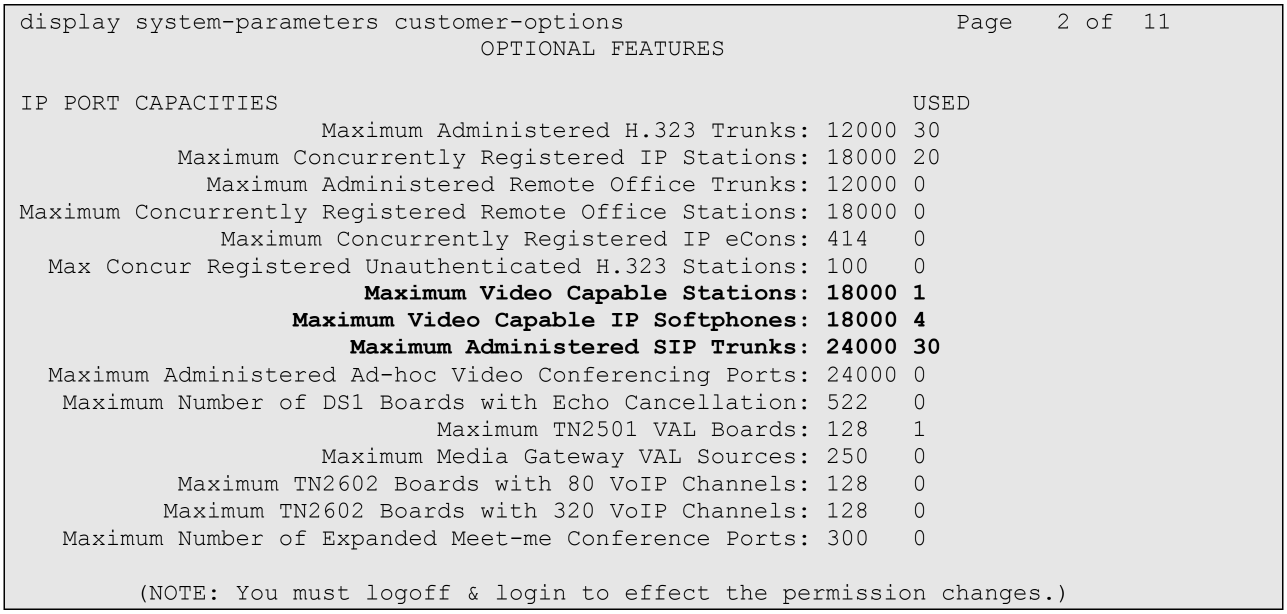
Using the SAT, verify that the Off-PBX Telephones (OPS), video capable endpoints, and SIP Trunk options are enabled on the **system-parameters customer-options** form. The license file installed on the system controls these options. If a required feature is not enabled, contact an authorized Avaya sales 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 161
                                      Maximum Stations: 41000 78
                              Maximum XMOBILE Stations: 41000 0
                    Maximum Off-PBX Telephones - EC500: 36000 0
                    Maximum Off-PBX Telephones -   OPS: 41000 8
                    Maximum Off-PBX Telephones - PBFMC: 36000 0
                    Maximum Off-PBX Telephones - PVFMC: 36000 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 30
           Maximum Concurrently Registered IP Stations: 18000 20
             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 1
                   Maximum Video Capable IP Softphones: 18000 4
                       Maximum Administered SIP Trunks: 24000 30
  Maximum Administered Ad-hoc Video Conferencing Ports: 24000 0
   Maximum Number of DS1 Boards with Echo Cancellation: 522   0
                             Maximum TN2501 VAL Boards: 128   1
                     Maximum Media Gateway VAL Sources: 250   0
           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 an IP address and host name for the C-LAN board in the G650 Media Gateway and the Session Manager SIP interface. 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
Gateway001          10.32.24.1
ModMsg              192.50.10.45
clancrm             10.32.24.20
default             0.0.0.0
devcon-asm          10.32.24.235
medprocrm           10.32.24.21
procr               10.32.24.10
procr6              ::
 ( 8 of 8   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 G650 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: 1       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? y
   UDP Port Max: 3029
DIFFSERV/TOS PARAMETERS
 Call Control PHB Value: 34
        Audio PHB Value: 46
        Video PHB Value: 26
802.1P/Q PARAMETERS
 Call Control 802.1p Priority: 7
        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 Passport. 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        Silence      Frames   Packet
    Codec        Suppression  Per Pkt  Size(ms)
 1: G.711MU          n          2        20
 2:
 3:
 4:
 5:
 6:
 7:
```

Configure **Page 2** of the **IP Codec Set** form as follows.

```
change ip-codec-set 1                                            Page   2 of   2

                          IP Codec Set

                              Allow Direct-IP Multimedia? y
              Maximum Call Rate for Direct-IP Multimedia:  4096:Kbits
     Maximum Call Rate for Priority Direct-IP Multimedia:  4096: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 *tcp*.
- Set the **IP Video** field to *y*. This is an important setting required for video calls.
- Specify the C-LAN board and the Session Manager 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 TCP port value of *5060* 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.
- Enter the domain name of Session Manager in the **Far-end Domain** field. In this configuration, the domain name is *avaya.com*.
- 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 50                                       Page   1 of   1
                                SIGNALING GROUP

 Group Number: 50             Group Type: sip
  IMS Enabled? n        Transport Method: tcp
        Q-SIP? n                                             SIP Enabled LSP? n
     IP Video? Y          Priority Video? y         nforce SIPS URI for SRTP? y
  Peer Detection Enabled? y  Peer Server: SM



   Near-end Node Name: clancrm               Far-end Node Name: devcon-asm
 Near-end Listen Port: 5060                Far-end Listen Port: 5060
                                        Far-end Network Region: 1

Far-end Domain: avaya.com
                                             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? n                   Initial IP-IP Direct Media? y
H.323 Station Outgoing Direct Media? n            Alternate Route Timer(sec): 6
```

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*, 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 50                                          Page   1 of  21
                                TRUNK GROUP

Group Number: 50                   Group Type: sip           CDR Reports: y
  Group Name: To devcon-asm              COR: 1        TN: 1        TAC: 1050
   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: 50
                                                    Number of Members: 10
```

On **Page 3** of the trunk group form, set the **Numbering Format** field to *private*. This field specifies the format of the calling party number sent to the far-end.

```
add trunk-group 50                                          Page   3 of  21
TRUNK FEATURES
          ACA Assignment? n            Measured: none
                                                     Maintenance Tests? y

                     Numbering Format: private
                                               UUI 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 '7' whose calls are routed over any trunk group, including SIP trunk group "50", 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  7                                            5     Total Administered: 1
                                                          Maximum Entries: 540
```

5.3 Configure Station for LifeSize Passport

The **station** and **off-pbx-telephone station-mapping** configuration shown in this section was automatically performed after 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 video system and verify the settings in bold. Note that the **IP Video** field must be set to *y*.

```
add station 78401                                            Page   1 of   6
                                     STATION

Extension: 78401                         Lock Messages? n               BCC: M
     Type: 9630SIP                       Security Code:                  TN: 1
     Port: S00188                      Coverage Path 1:                 COR: 1
     Name: 78401, Passport             Coverage Path 2:                 COS: 1
                                       Hunt-to Station:
STATION OPTIONS
                                           Time of Day Lock Table:
              Loss Group: 19
                                                 Message Lamp Ext: 78401

        Display Language: english                  Button Modules: 0

          Survivable COR: internal
   Survivable Trunk Dest? y                          IP SoftPhone? y

                                                         IP Video? Y
                              Short/Prefixed Registration Allowed: default
```

Use the **display off-pbx-telephone station-mapping** command to view the mapping of the Communication Manager extensions (e.g., 78401) 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.

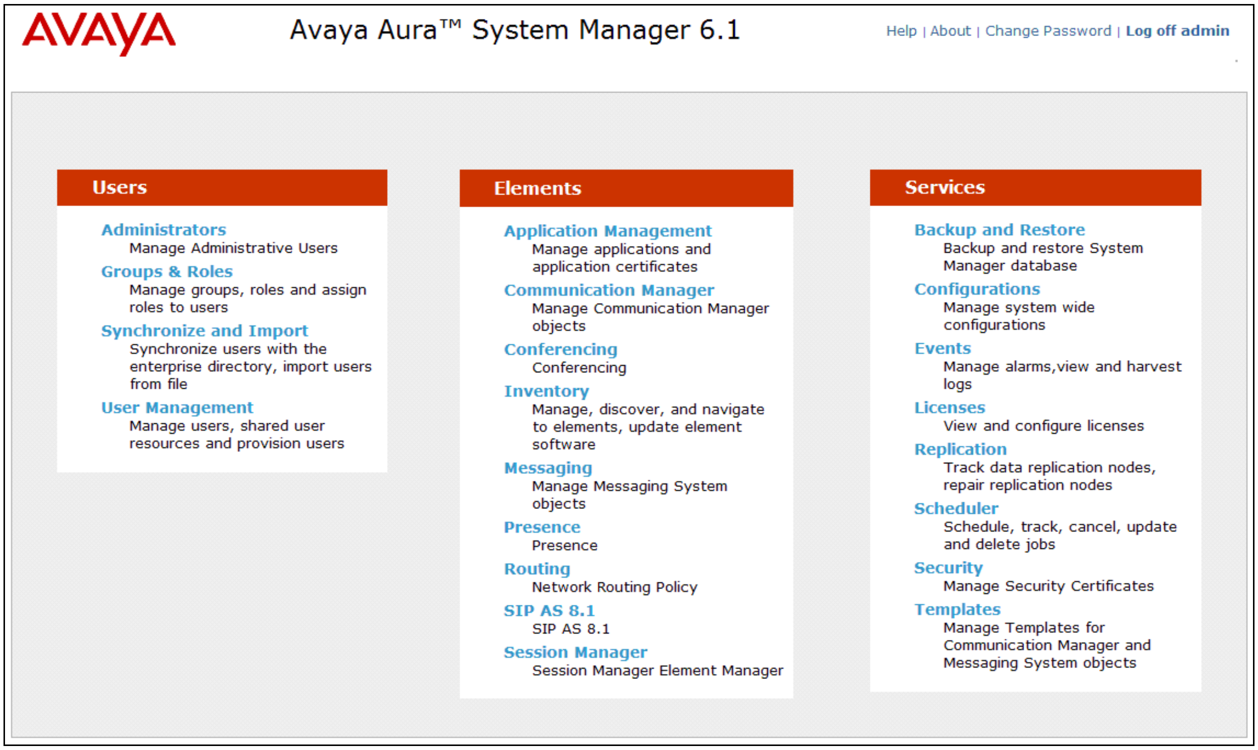
```
change off-pbx-telephone station-mapping 78401                  Page   1 of   3
                  STATIONS WITH OFF-PBX TELEPHONE INTEGRATION

 Station       Application Dial   CC  Phone Number    Trunk       Config  Dual
 Extension                 Prefix                     Selection   Set     Mode
 78401            OPS           -     78401            aar        1
```

6. Configure 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 be performed under **Routing** and **Session Manager** listed within the **Elements** box.



AVAYA Avaya Aura™ System Manager 6.1

Help | About | Change Password | Log off admin

Users

Administrators
Manage Administrative Users

Groups & Roles
Manage groups, roles and assign roles to users

Synchronize and Import
Synchronize users with the enterprise directory, import users from file

User Management
Manage users, shared user resources and provision users

Elements

Application Management
Manage applications and application certificates

Communication Manager
Manage Communication Manager objects

Conferencing
Conferencing

Inventory
Manage, discover, and navigate to elements, update element software

Messaging
Manage Messaging System objects

Presence
Presence

Routing
Network Routing Policy

SIP AS 8.1
SIP AS 8.1

Session Manager
Session Manager Element Manager

Services

Backup and Restore
Backup and restore System Manager database

Configurations
Manage system wide configurations

Events
Manage alarms,view and harvest logs

Licenses
View and configure licenses

Replication
Track data replication nodes, repair replication nodes

Scheduler
Schedule, track, cancel, update and delete jobs

Security
Manage Security Certificates

Templates
Manage Templates for Communication Manager and Messaging System objects

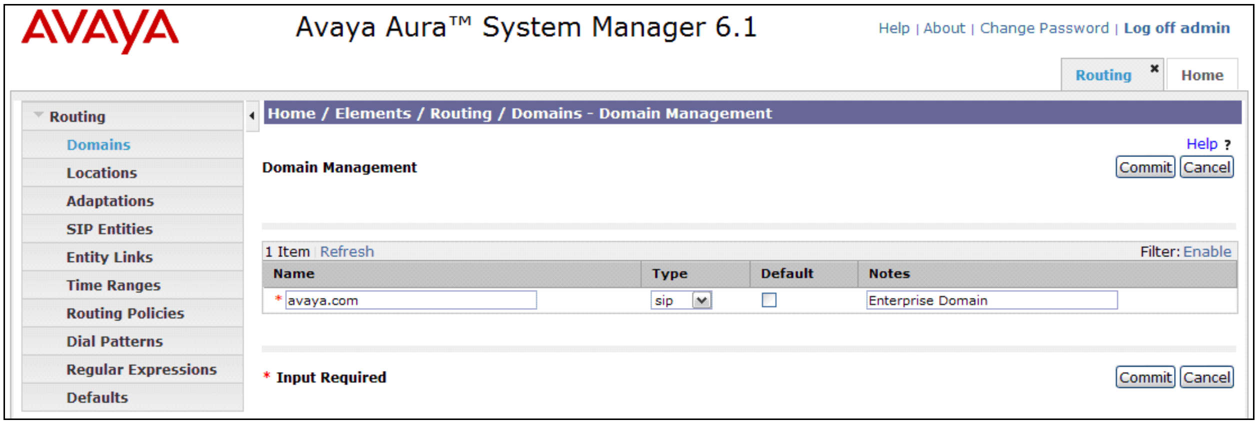
6.1 Specify SIP Domain

Add the SIP domain for which the communications infrastructure will be authoritative. Do this by selecting **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*)
- **Notes:** Descriptive text (optional).

Click **Commit**.

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



Home / Elements / Routing / Domains - Domain Management

Domain Management

1 Item

Name	Type	Default	Notes
* avaya.com	sip	□	Enterprise Domain

* Input Required

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:

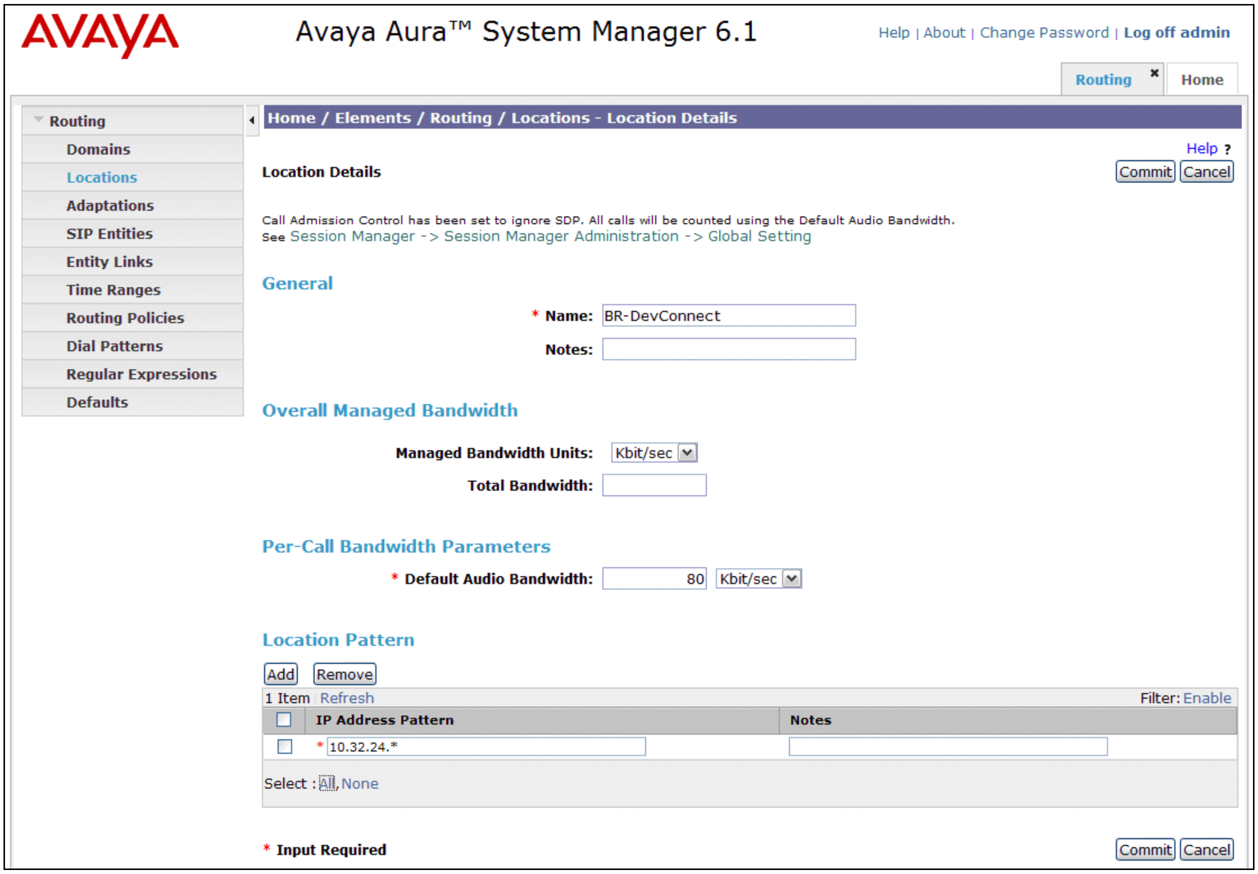
Under *General*:

▪ **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 *BR-DevConnect* location, which includes the Communication Manager and Session Manager. Click **Commit** to save the Location definition.



Home / Elements / Routing / Locations - Location Details

Location Details

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

General

* Name: BR-DevConnect

Notes:

Overall Managed Bandwidth

Managed Bandwidth Units: Kbit/sec

Total Bandwidth:

Per-Call Bandwidth Parameters

* Default Audio Bandwidth: 80 Kbit/sec

Location Pattern

□	IP Address Pattern	Notes
□	* 10.32.24.*	

* Input Required

6.3 Add SIP Entities

In the sample configuration, a SIP Entity is added for Session Manager and the C-LAN in the G650 Media Gateway.

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:

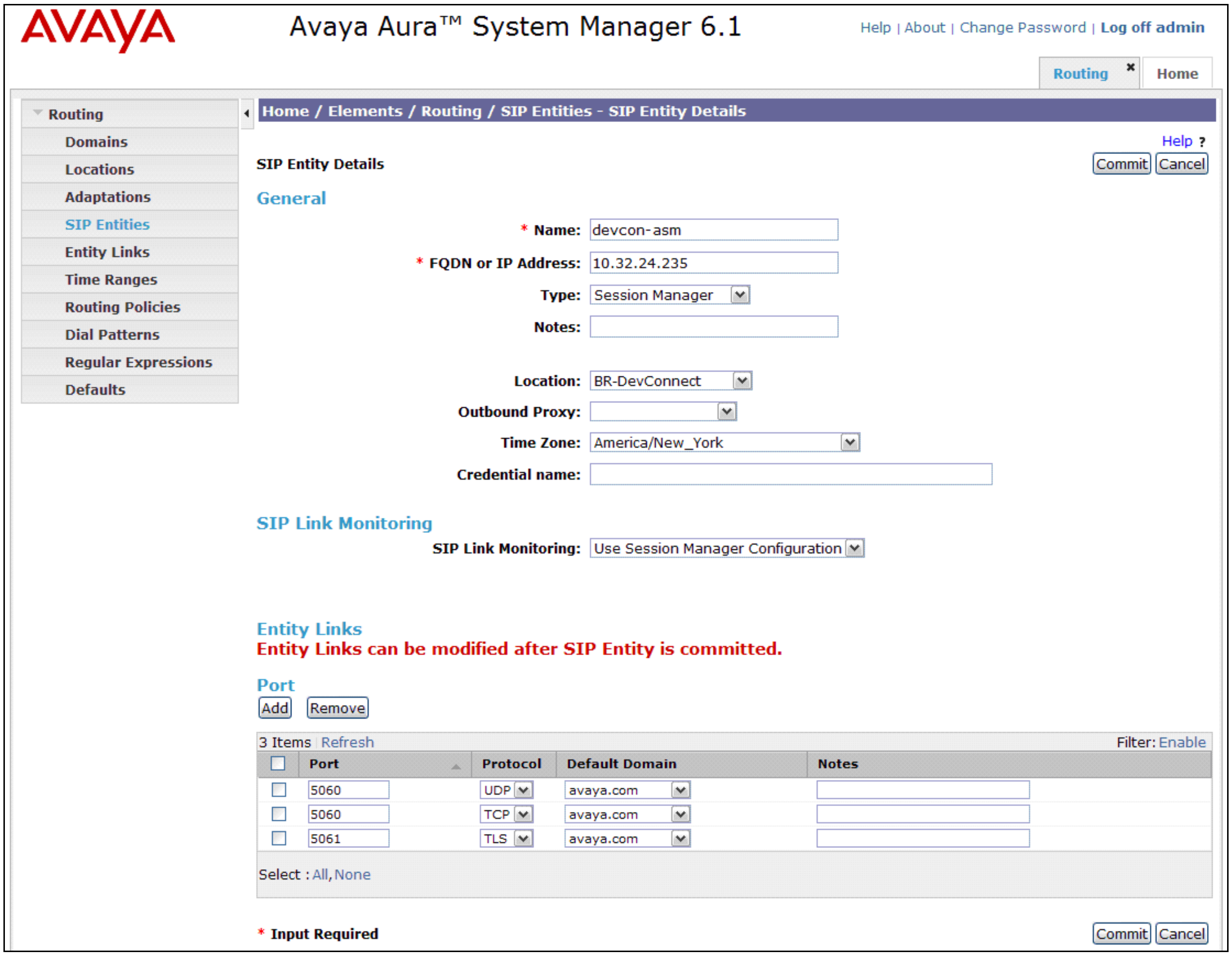
Under *General*:

- **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.



SIP Entity Details

General

* Name:	devcon-asm
* FQDN or IP Address:	10.32.24.235
Type:	Session Manager
Notes:	
Location:	BR-DevConnect
Outbound Proxy:	
Time Zone:	America/New_York
Credential name:	

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

Entity Links

Entity Links can be modified after SIP Entity is committed.

Port

3 Items

□	Port	Protocol	Default Domain	Notes
□	5060	UDP	avaya.com	
□	5060	TCP	avaya.com	
□	5061	TLS	avaya.com	

Select : All, None

* Input Required

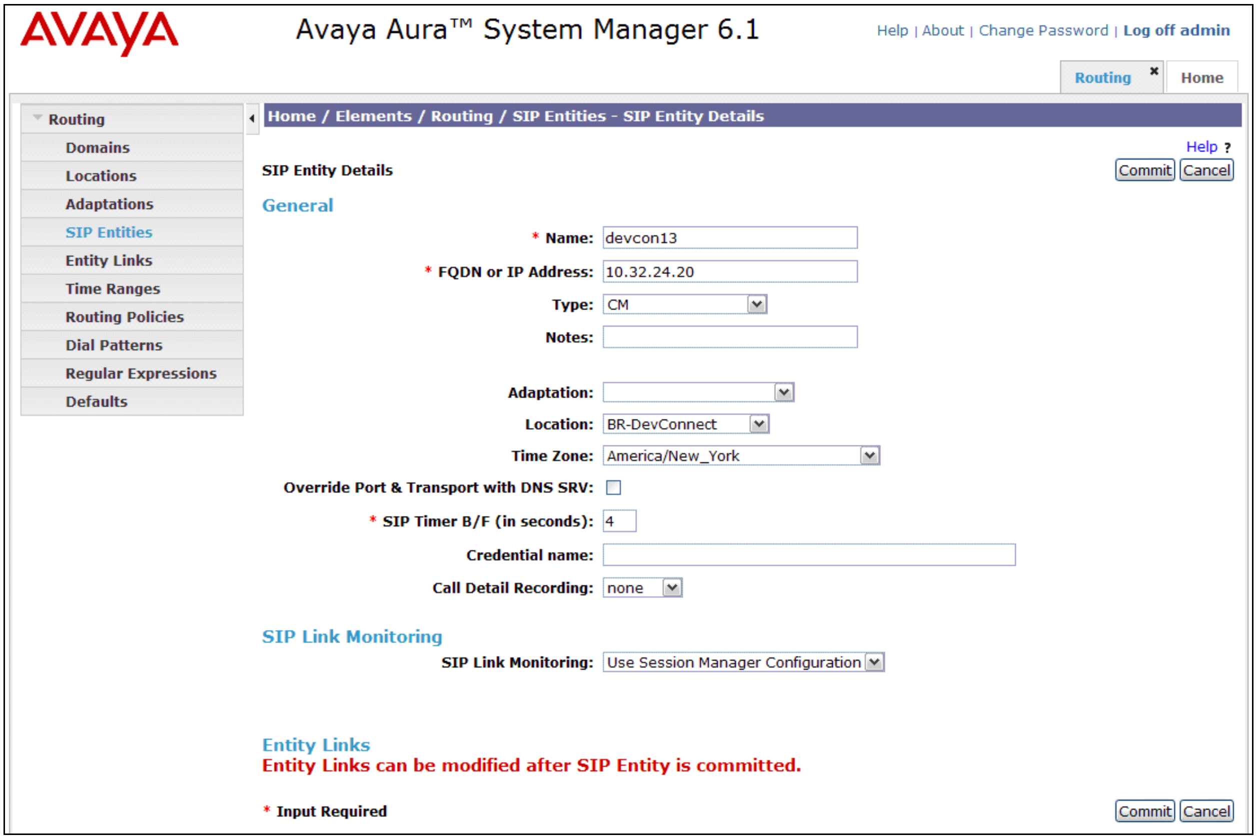
6.3.2 Communication Manager

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.



SIP Entity Details

General

* Name: devcon13

* FQDN or IP Address: 10.32.24.20

Type: CM

Notes:

Adaptation:

Location: BR-DevConnect

Time Zone: America/New_York

Override Port & Transport with DNS SRV: □

* SIP Timer B/F (in seconds): 4

Credential name:

Call Detail Recording: none

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

Entity Links

Entity Links can be modified after SIP Entity is committed.

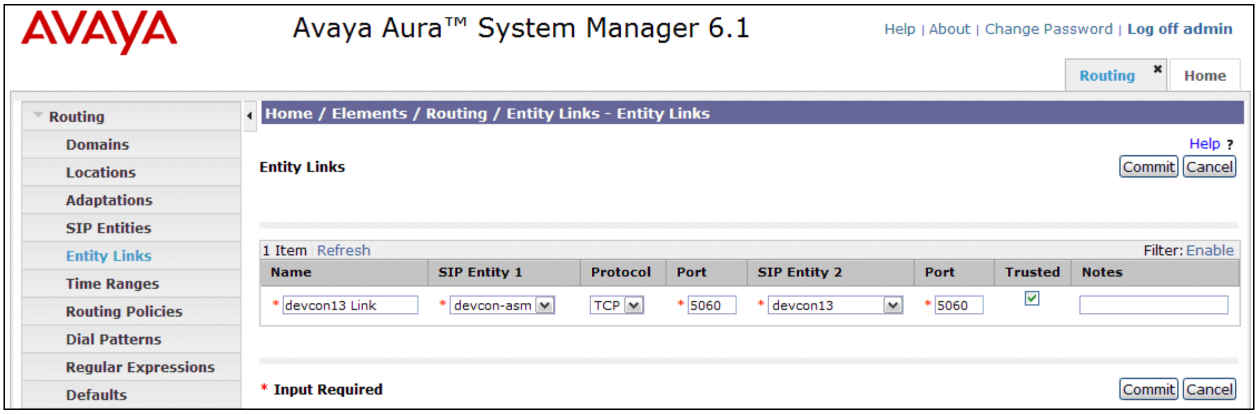
* Input Required

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 (e.g., *devcon13 Link*).
- **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.
- **Trusted:** Check this box. *Note: If this box is not checked, calls from the associated SIP Entity specified in **Section 6.3.2** will be denied.*

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



Entity Links

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted	Notes
* devcon13 Link	* devcon-asm	TCP	* 5060	* devcon13	* 5060	☑	

* Input Required

6.5 Define Communication Manager as Managed Element

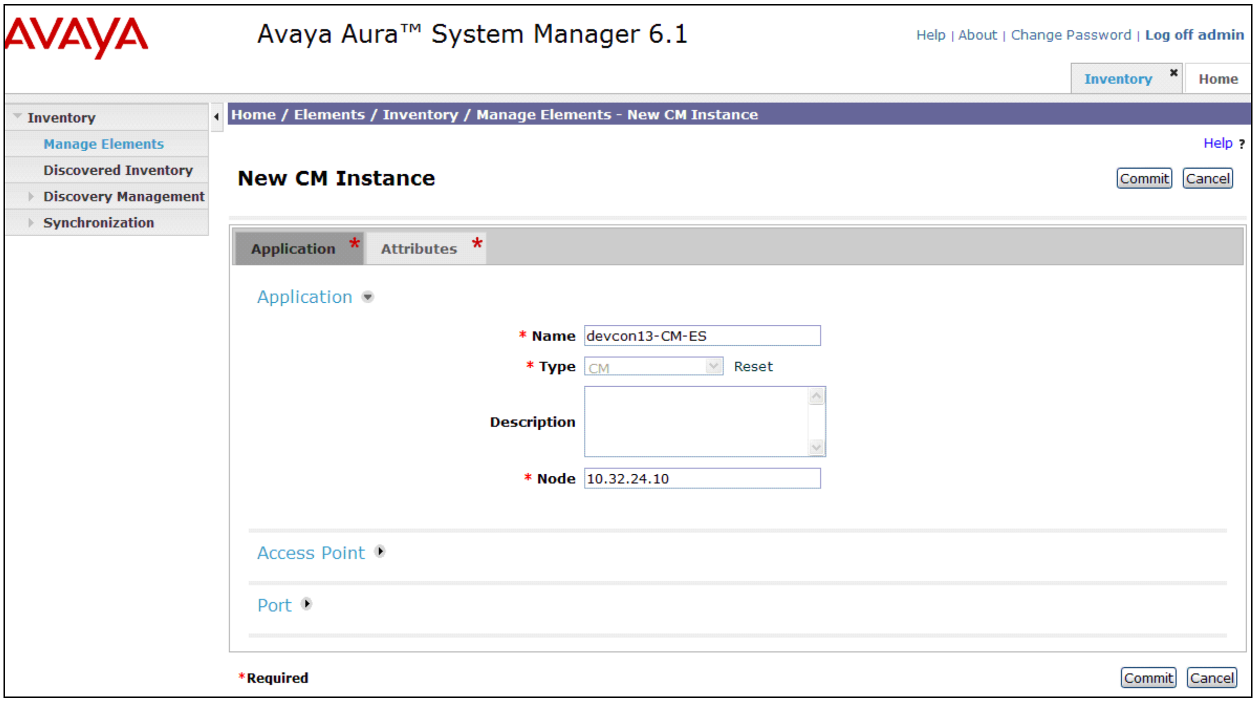
Before adding SIP users, Communication Manager must be added to System Manager as a managed element. This action allows System Manager to access Communication Manager over its administration interface. Using this administration interface, System Manager will notify Communication Manager when new SIP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


AVAYA
Avaya Aura™ System Manager 6.1
Help | About | Change Password | Log off admin
Inventory
Home
Inventory
Manage Elements
Discovered Inventory
Discovery Management
Synchronization
Home / Elements / Inventory / Manage Elements - New CM Instance
Help ?

New CM Instance

* Name: devcon13-CM-ES

* Type: CM

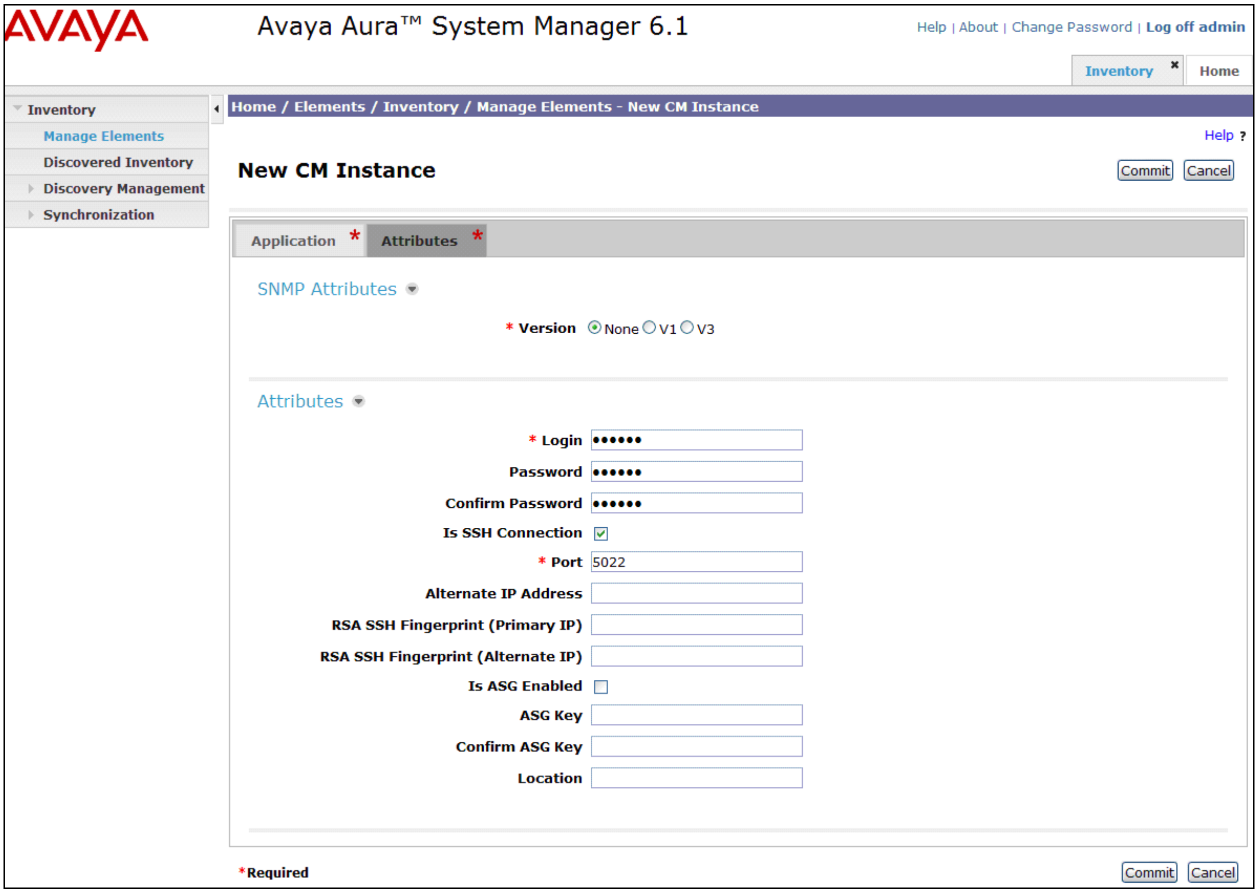
Description:

* Node: 10.32.24.10

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.



New CM Instance

* Version	● None ○ V1 ○ V3
* Login	••••••
Password	••••••
Confirm Password	••••••
Is SSH Connection	☑
* Port	5022
Alternate IP Address	
RSA SSH Fingerprint (Primary IP)	
RSA SSH Fingerprint (Alternate IP)	
Is ASG Enabled	□
ASG Key	
Confirm ASG Key	
Location	

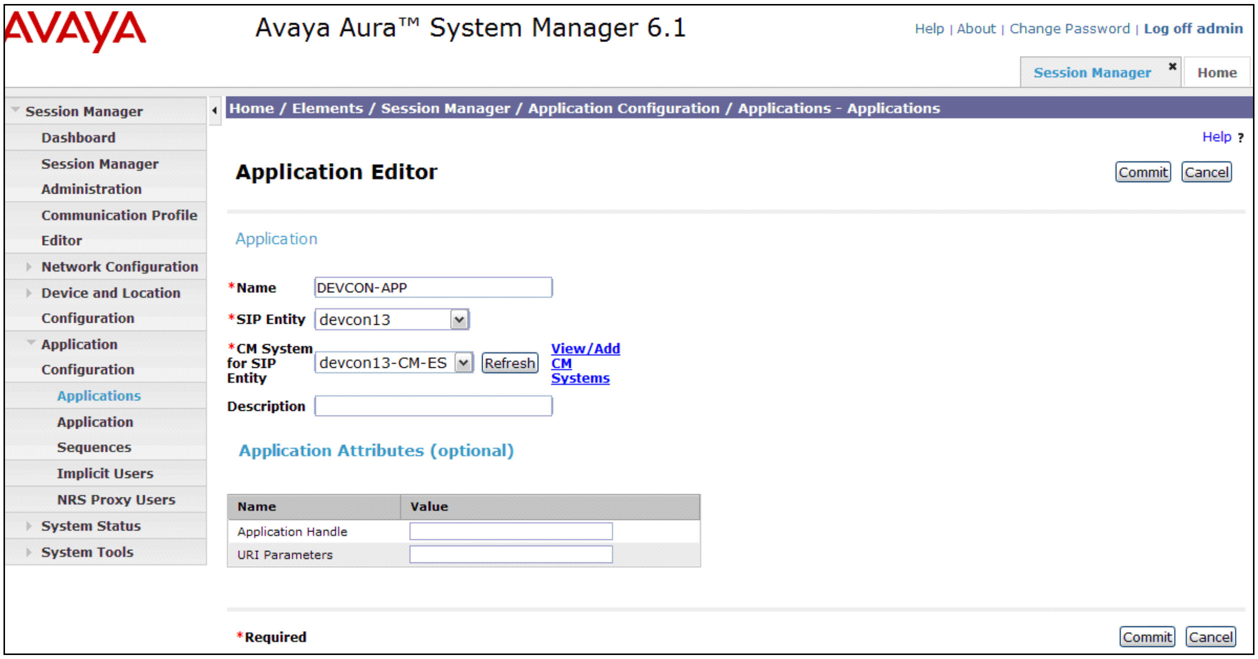
*Required

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.


AVAYA
Avaya Aura™ System Manager 6.1
Help | About | Change Password | Log off admin
Session Manager
Home
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 / Applications - Applications
Help ?
Commit
Cancel
Refresh
View/Add CM Systems
*Required

Application Editor

Application

*Name: DEVCON-APP

*SIP Entity: devcon13

*CM System for SIP Entity: devcon13-CM-ES

Description:

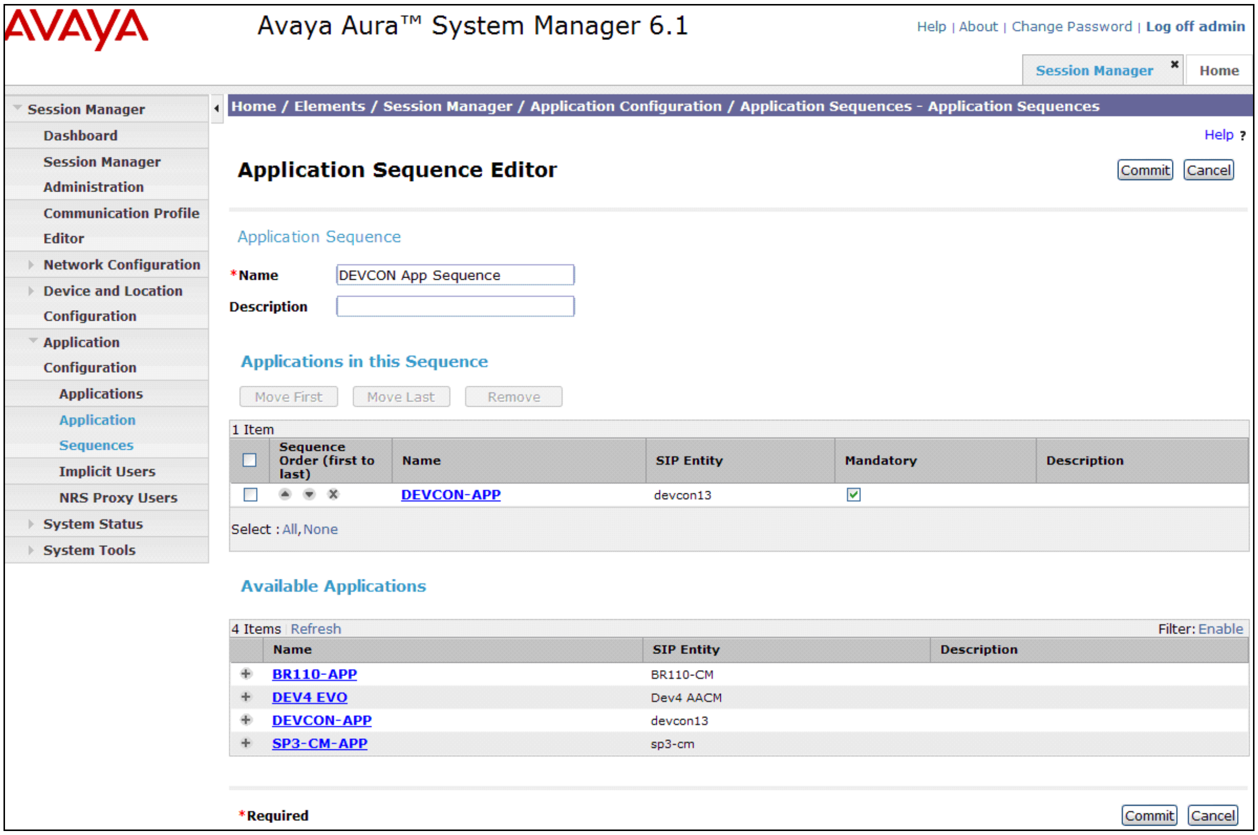
Application Attributes (optional)

Name	Value
Application Handle	
URI Parameters	

Next, navigate to **Elements → Session Manager → Application Configuration → Application Sequences** to define the Application Sequence for Communication Manager as shown below. Provide a **Name** (e.g., *DEVCON App Sequence*) for the Application Sequence and under **Available Applications**, click on the plus (+) sign by *DEVCON-APP* 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.


AVAYA
Avaya Aura™ System Manager 6.1
Help | About | Change Password | Log off admin
Session Manager
Home
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 ?
Commit
Cancel
Move First
Move Last
Remove
Refresh
Filter: Enable
Commit
Cancel

Application Sequence Editor

Application Sequence

*Name: DEVCON App Sequence

Description:

Applications in this Sequence

1 Item

□	Sequence Order (first to last)	Name	SIP Entity	Mandatory	Description
□	▲ ▼ ✕	DEVCON-APP	devcon13	☑	

Select : All, None

Available Applications

4 Items

	Name	SIP Entity	Description
+	BR110-APP	BR110-CM	
+	DEV4 EVO	Dev4 AACM	
+	DEVCON-APP	devcon13	
+	SP3-CM-APP	sp3-cm	

*Required

6.7 Add SIP User

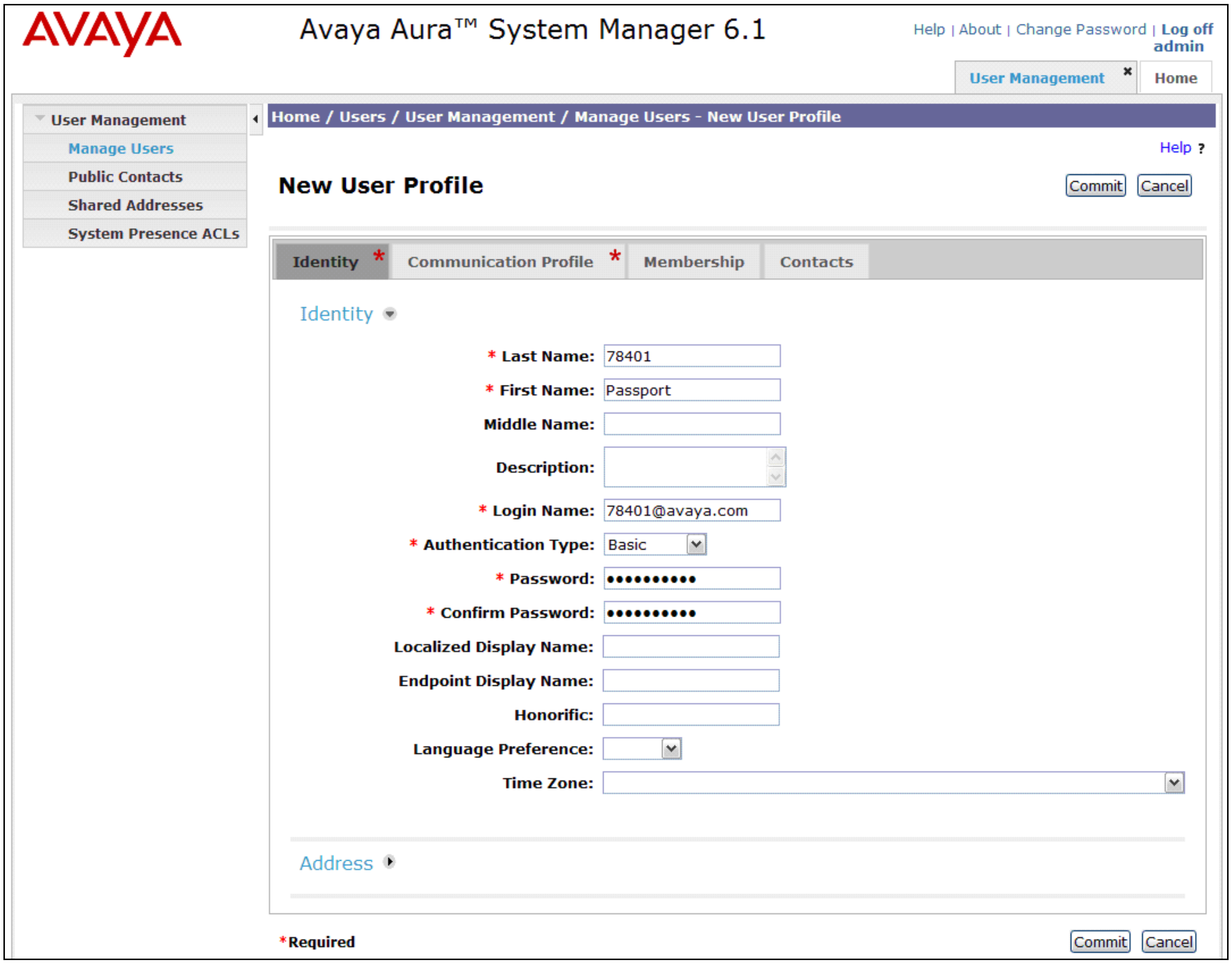
Add a SIP user for LifeSize Passport**.** The following configuration will automatically create the SIP station on Communication Manager Evolution Server.

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., 78401@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.



New User Profile

Identity

* Last Name:	78401
* First Name:	Passport
Middle Name:	
Description:	
* Login Name:	78401@avaya.com
* Authentication Type:	Basic
* Password:	••••••••••
* Confirm Password:	••••••••••
Localized Display Name:	
Endpoint Display Name:	
Honorific:	
Language Preference:	
Time Zone:	

*Required

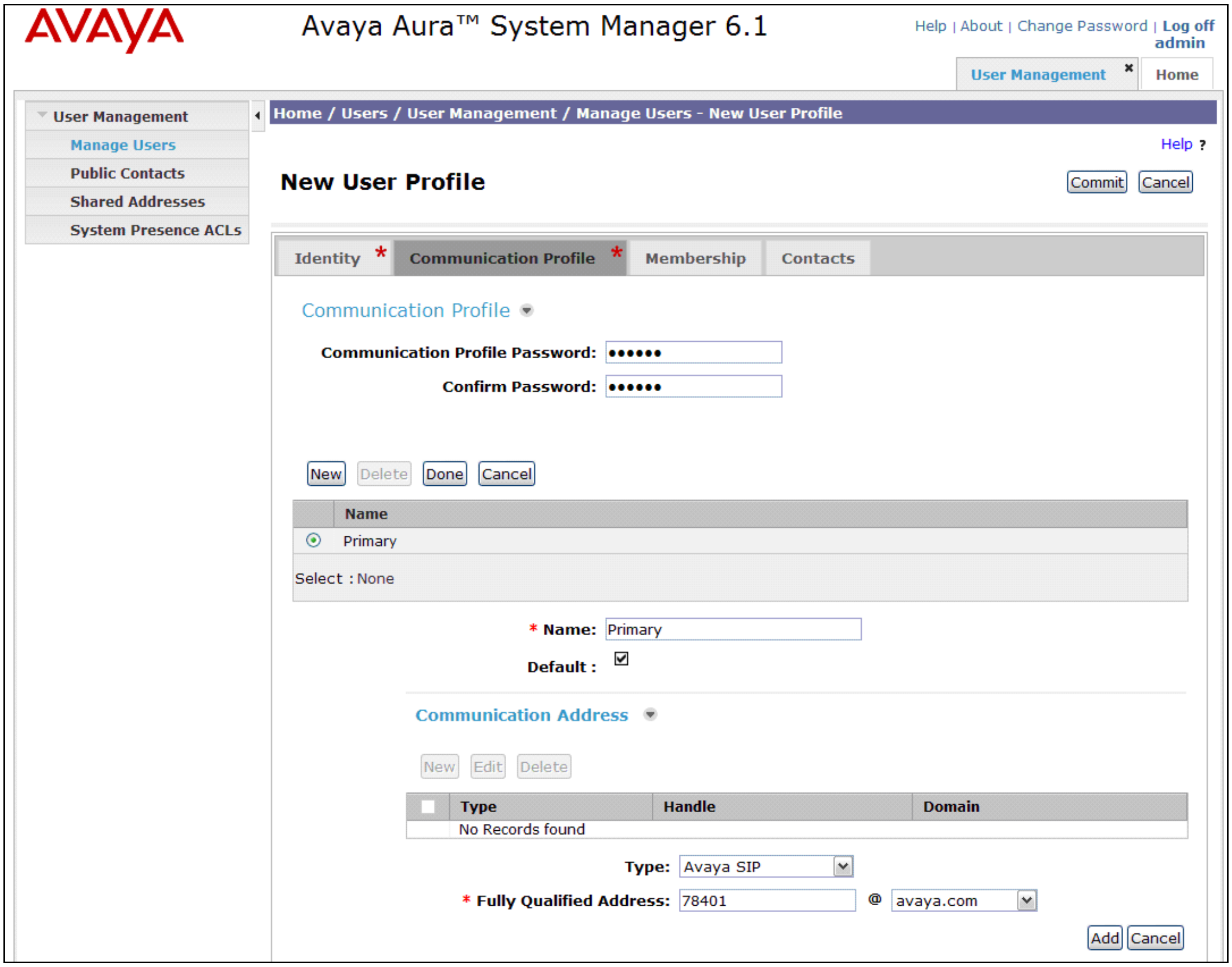
Enter values for the following required attributes for a new SIP user in the **Communication Profile tab** of the new user form.

- **Communication Profile Password:** Enter the password which will be used by Passport 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**.



New User Profile

Communication Profile

Communication Profile Password: ••••••

Confirm Password: ••••••

	Name
●	Primary

Select : None

* Name: Primary

Default : ☑

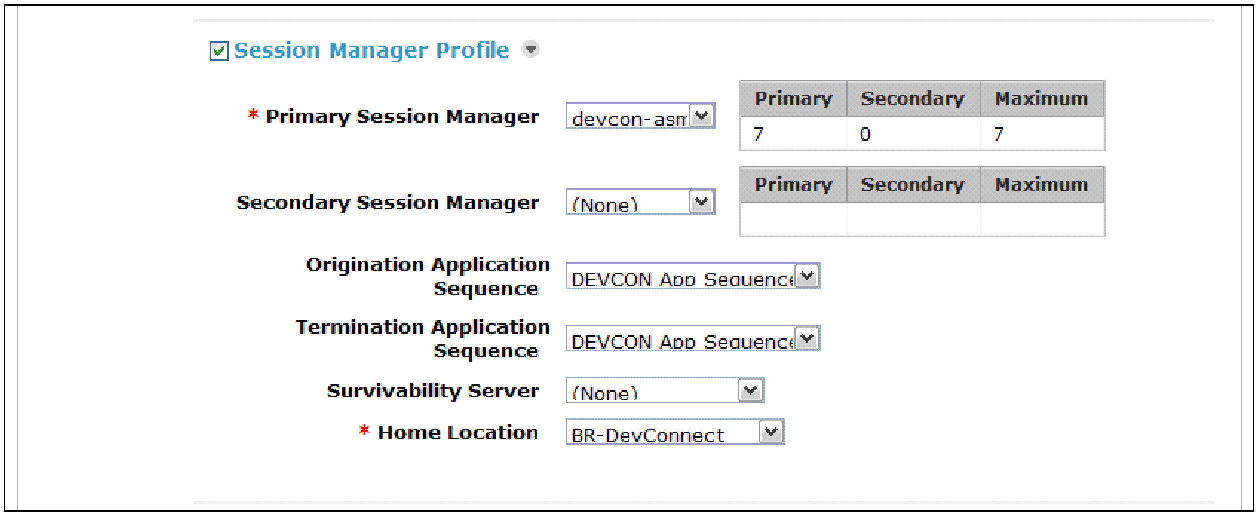
Communication Address

□	Type	Handle	Domain
	No Records found		

Type: Avaya SIP

* Fully Qualified Address: 78401 @ avaya.com

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**.



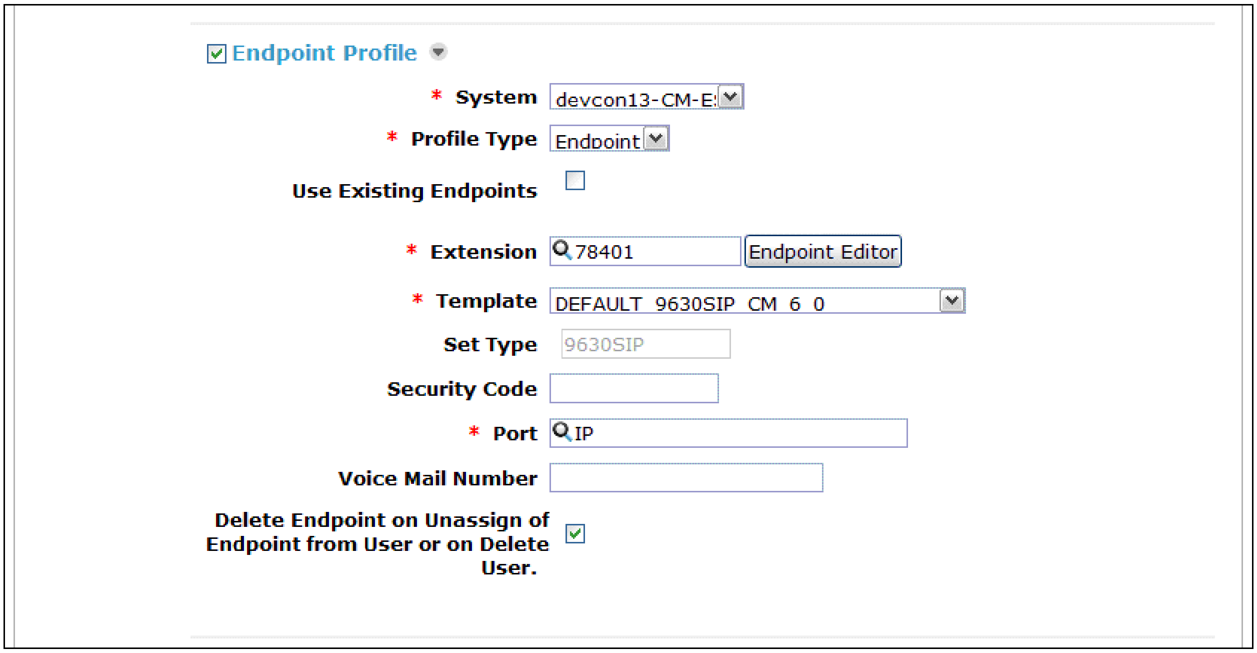
☑ Session Manager Profile

		Primary	Secondary	Maximum
* Primary Session Manager	devcon-asm	7	0	7
Secondary Session Manager	(None)			

Origination Application Sequence	DEVCON App Sequence
Termination Application Sequence	DEVCON App Sequence
Survivability Server	(None)
* Home Location	BR-DevConnect

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

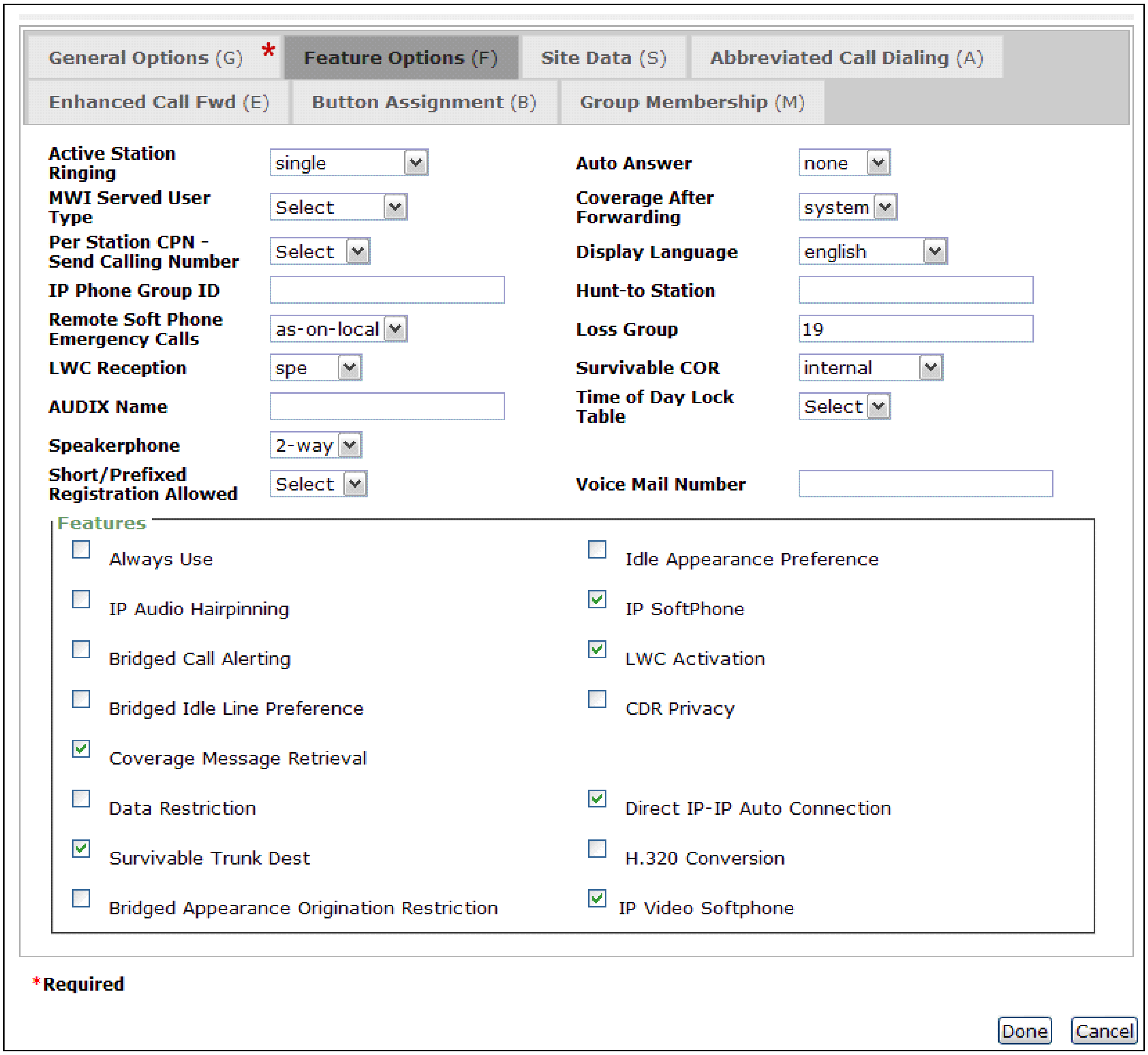
- **System:** Select the managed element corresponding to Communication Manager.
- **Profile Type** Select *Endpoint*.
- **Use Existing Stations:** If field is not selected, the station will automatically be added in Communication Manager.
- **Extension:** Enter extension number of SIP user.
- **Template:**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



☑ Endpoint Profile

* System	devcon13-CM-E:
* Profile Type	Endpoint
Use Existing Endpoints	□
* Extension	78401
* Template	DEFAULT_9630SIP_CM_6_0
Set Type	9630SIP
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 Softphone** and **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.



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	as-on-local	Loss Group	19
LWC Reception	spe	Survivable COR	internal
AUDIX Name		Time of Day Lock Table	Select
Speakerphone	2-way		
Short/Prefixed Registration Allowed	Select	Voice Mail Number	

Features

□ Always Use	□ Idle Appearance Preference
□ IP Audio Hairpinning	☑ IP SoftPhone
□ Bridged Call Alerting	☑ LWC Activation
□ Bridged Idle Line Preference	□ CDR Privacy
☑ Coverage Message Retrieval	
□ Data Restriction	☑ Direct IP-IP Auto Connection
☑ Survivable Trunk Dest	□ H.320 Conversion
□ Bridged Appearance Origination Restriction	☑ IP Video Softphone

*Required

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:

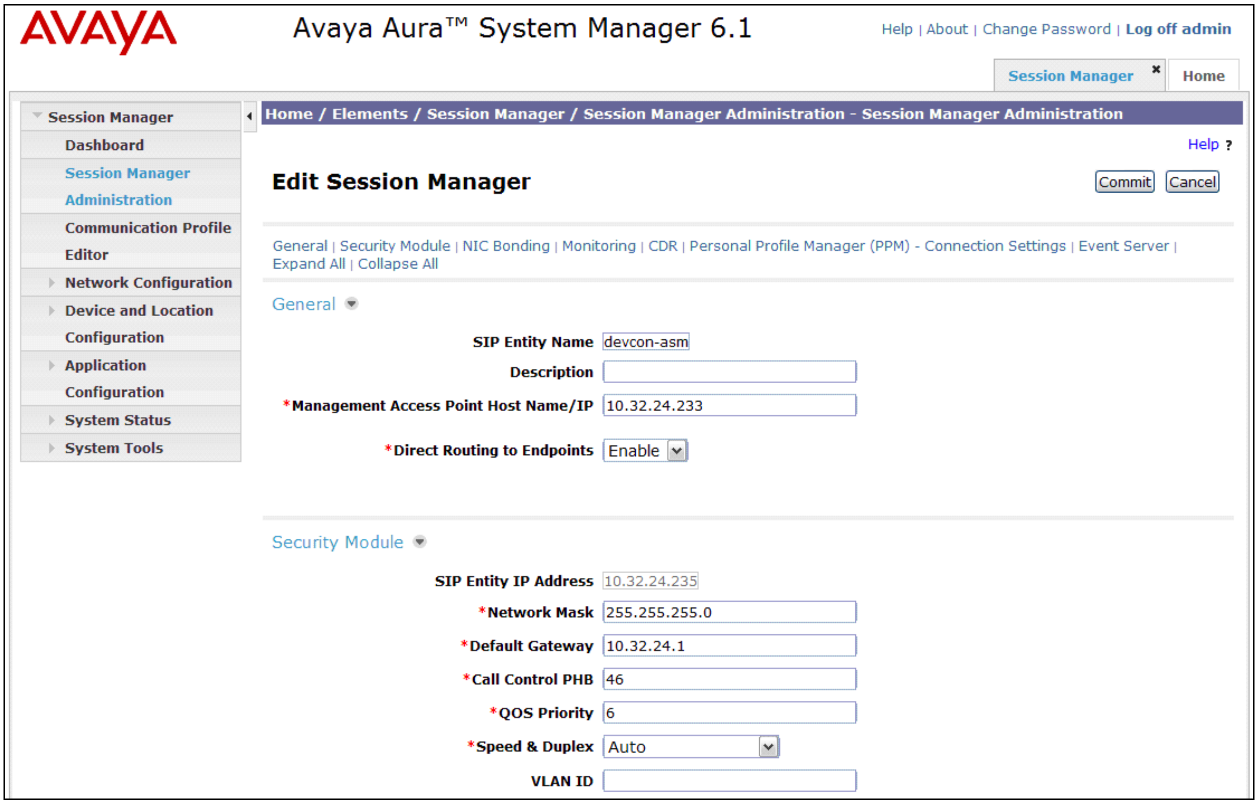
Under *Identity*:

- **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
Session Manager
Dashboard
Session Manager Administration
Communication Profile Editor
Network Configuration
Device and Location Configuration
Application Configuration
System Status
System Tools
Home / Elements / Session Manager / Session Manager Administration - Session Manager Administration
Help ?
Commit
Cancel
General | Security Module | NIC Bonding | Monitoring | CDR | Personal Profile Manager (PPM) - Connection Settings | Event Server | Expand All | Collapse All

Edit Session Manager

General

SIP Entity Name	devcon-asm
Description	
*Management Access Point Host Name/IP	10.32.24.233
*Direct Routing to Endpoints	Enable

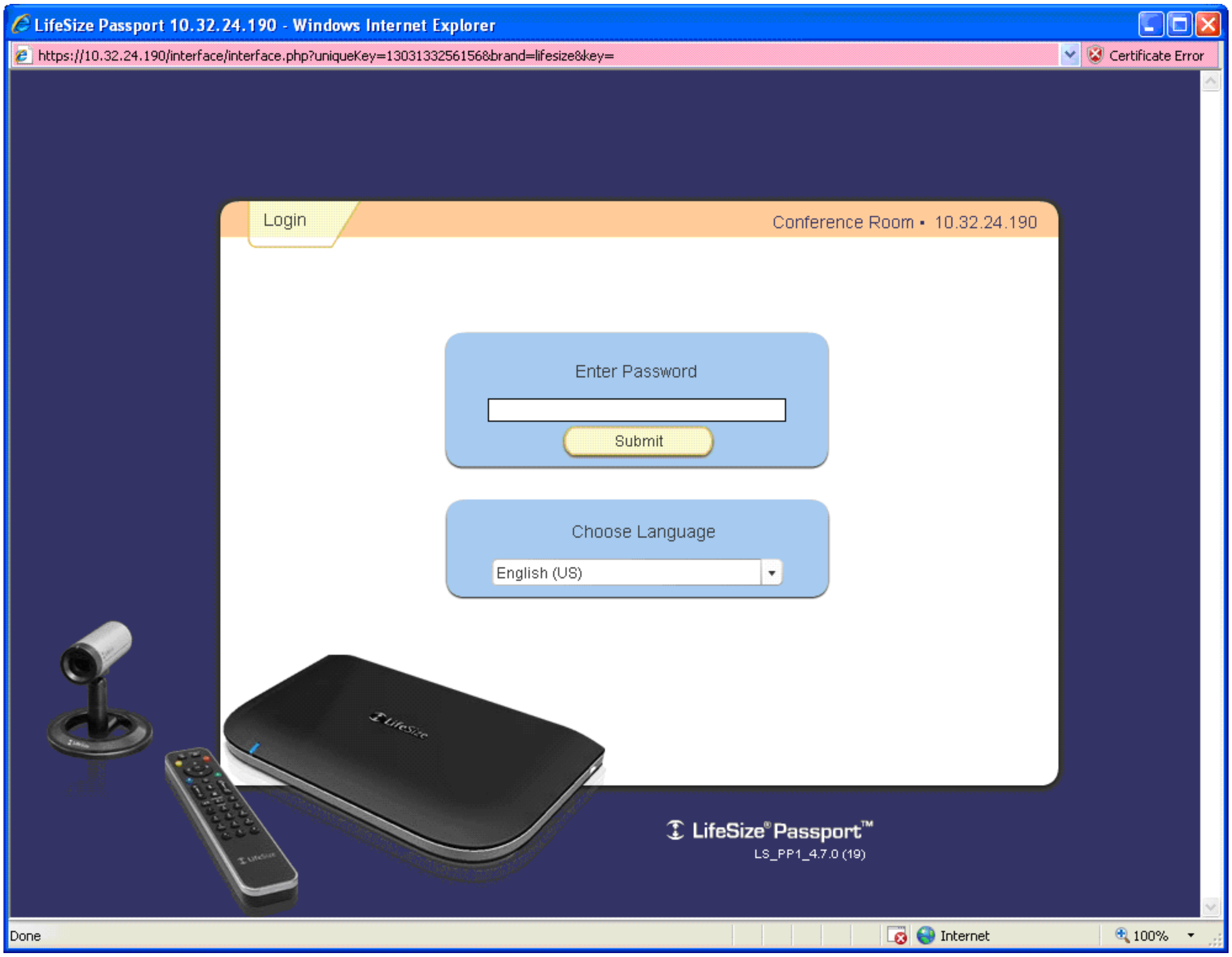
Security Module

SIP Entity IP Address	10.32.24.235
*Network Mask	255.255.255.0
*Default Gateway	10.32.24.1
*Call Control PHB	46
*QOS Priority	6
*Speed & Duplex	Auto
VLAN ID	

7. Configure LifeSize Passport

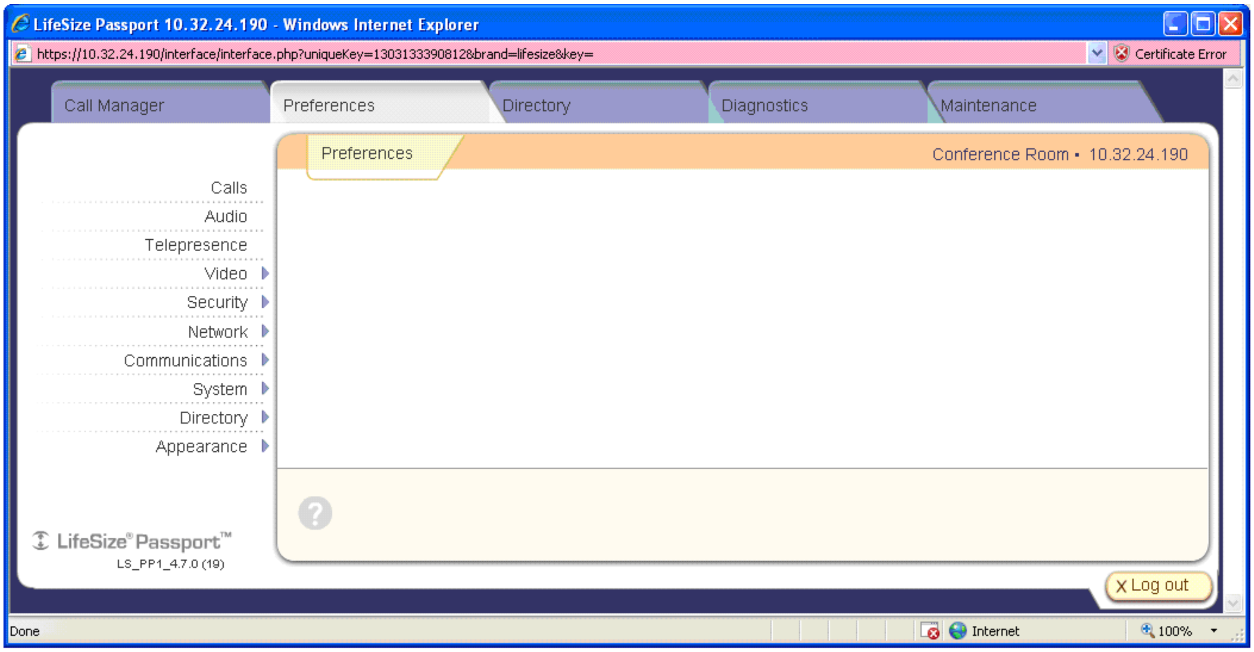
The configuration of the LifeSize Passport video system was performed via the Passport's embedded Web interface or user interface on the monitor display using the remote control. However, the Passport's LAN connection interface was initially configured via its monitor using the remote control. To configure the IP parameters for Passport, 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's embedded Web interface as shown in this section. Refer to [4] for additional information on configuring the Passport video system.

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

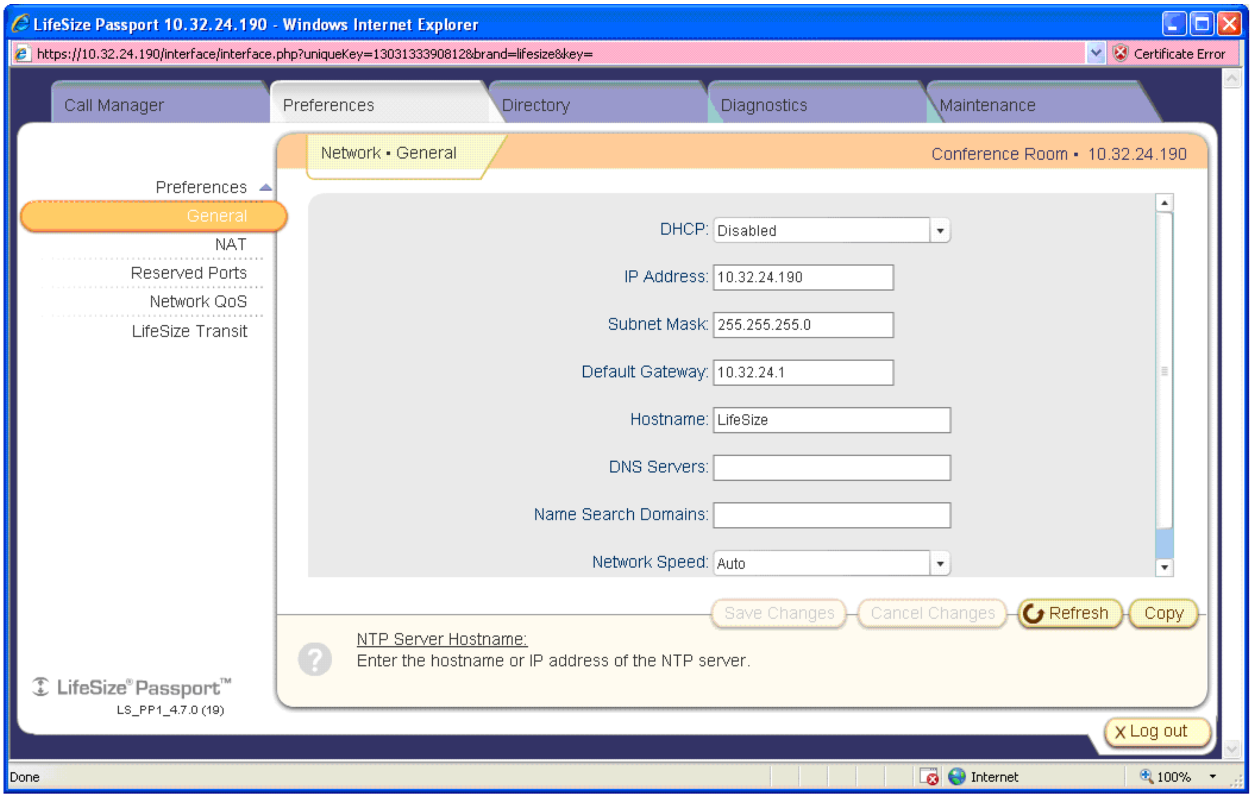

LifeSize Passport 10.32.24.190 - Windows Internet Explorer

https://10.32.24.190/interface/interface.php?uniqueKey=1303133256156&brand=lifesize&key=

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.



DHCP: Disabled

IP Address: 10.32.24.190

Subnet Mask: 255.255.255.0

Default Gateway: 10.32.24.1

Hostname: LifeSize

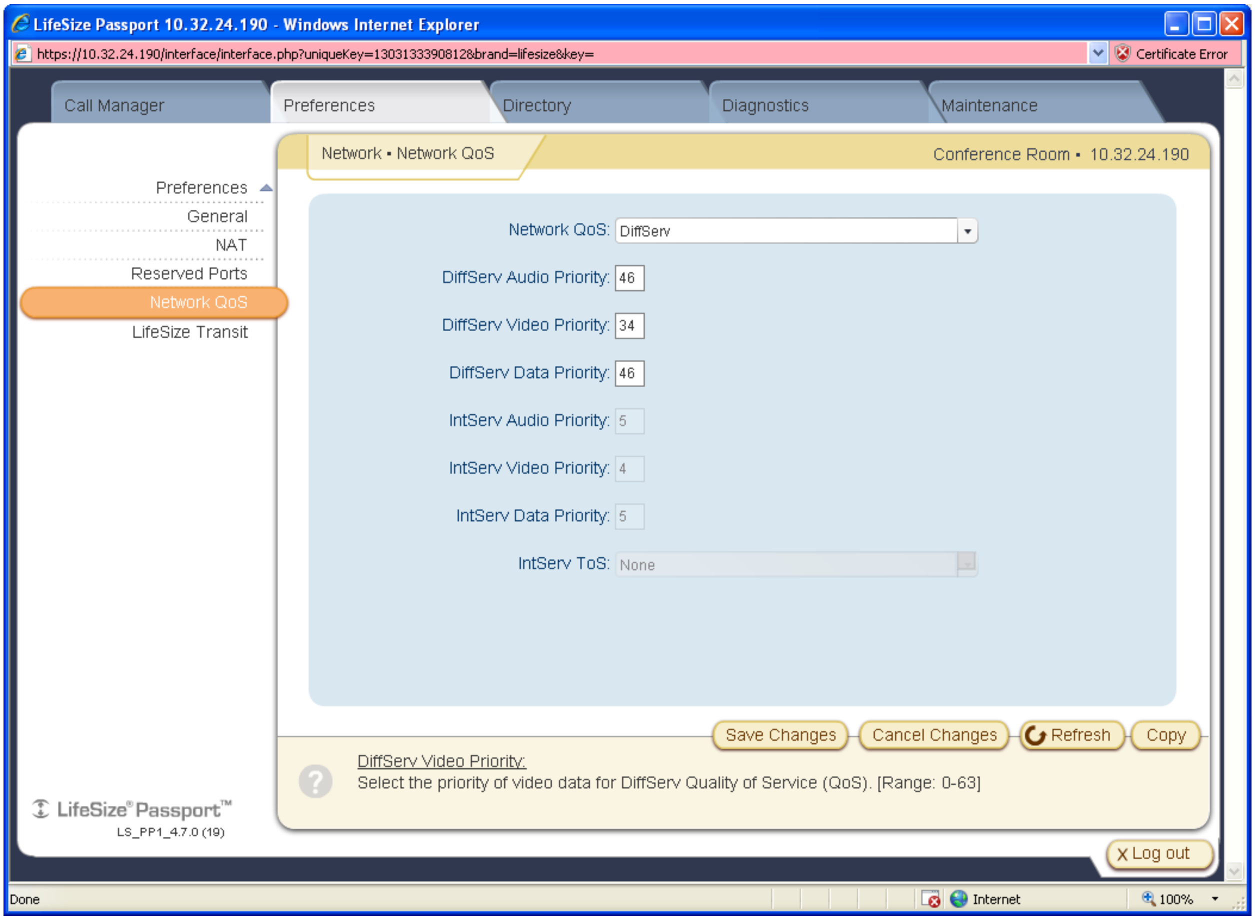
DNS Servers:

Name Search Domains:

Network Speed: Auto

NTP Server Hostname:
Enter the hostname or IP address of the NTP server.

If network QoS is implemented using DiffServ, the **DiffServ Video Priority** may be configured on Passport so that it tags its video RTP packets with the appropriate DiffServ value. To configure DiffServ on Passport, 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.



Network QoS: DiffServ

DiffServ Audio Priority: 46

DiffServ Video Priority: 34

DiffServ Data Priority: 46

IntServ Audio Priority: 5

IntServ Video Priority: 4

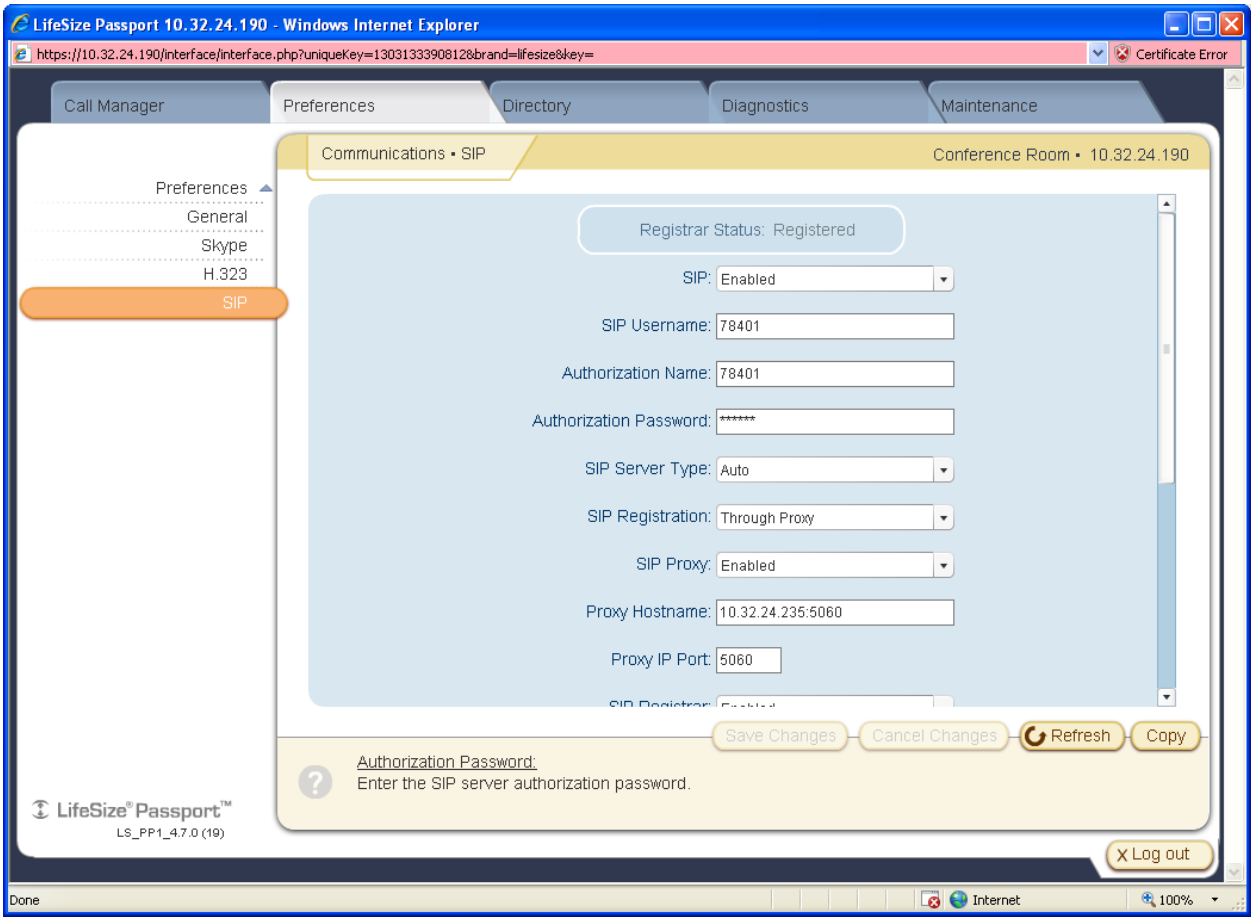
IntServ Data Priority: 5

IntServ ToS: None

DiffServ Video Priority:
Select the priority of video data for DiffServ Quality of Service (QoS). [Range: 0-63]

Next, configure the Passport'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's extension (e.g., 78401).
- **Authorization Name** Specify the Passport's extension, which will be used to register with Session Manager.
- **Authorization Password** Specify the password used by Passport to register with Session Manager.
- **SIP Proxy** Set to *Enabled*.
- **Proxy Hostname** Specify the IP address of Session Manager's SIP interface (e.g., 10.32.24.235).
- **Proxy IP Port** Specify the port used to communication with Session Manager. In this configuration, port *5060* was used.



Registrar Status: Registered

SIP: Enabled

SIP Username: 78401

Authorization Name: 78401

Authorization Password: ******

SIP Server Type: Auto

SIP Registration: Through Proxy

SIP Proxy: Enabled

Proxy Hostname: 10.32.24.235:5060

Proxy IP Port: 5060

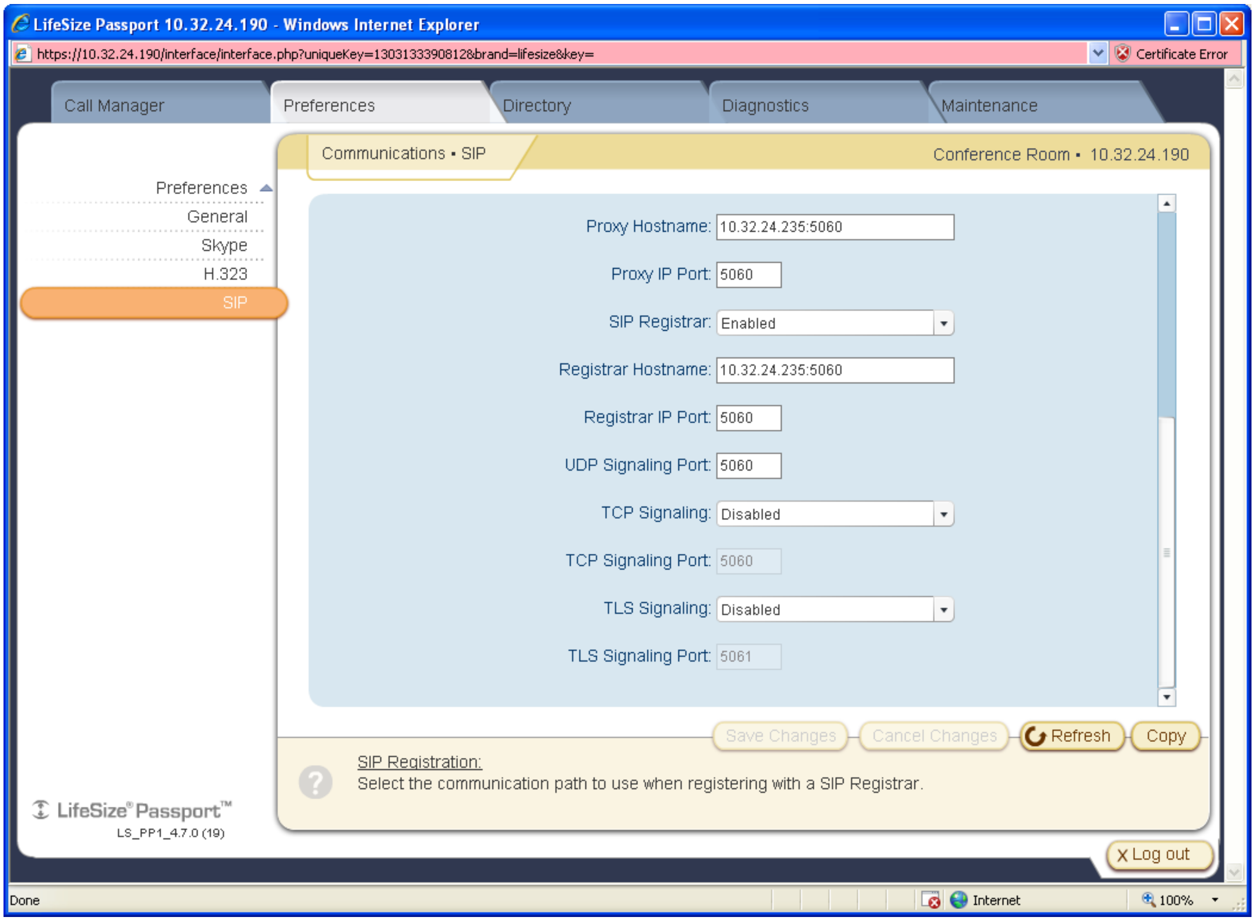
SIP Registrar: Enabled

Authorization Password:
Enter the SIP server authorization password.

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

- **SIP Registrar** Set to *Enabled*.
- **Registrar Hostname** Specify the IP address of Session Manager's SIP interface.
- **Registrar IP Port** Specify the port used to register with Session Manager.
- **UDP Signaling Port** Specify the port used to communicate with Session Manager via UDP.
- **TCP Signaling** Set to *Disabled* since Passport was configured to use UDP.
- **TLS Signaling** Set to *Disabled* since Passport was configured to use UDP.

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



Proxy Hostname: 10.32.24.235:5060

Proxy IP Port: 5060

SIP Registrar: Enabled

Registrar Hostname: 10.32.24.235:5060

Registrar IP Port: 5060

UDP Signaling Port: 5060

TCP Signaling: Disabled

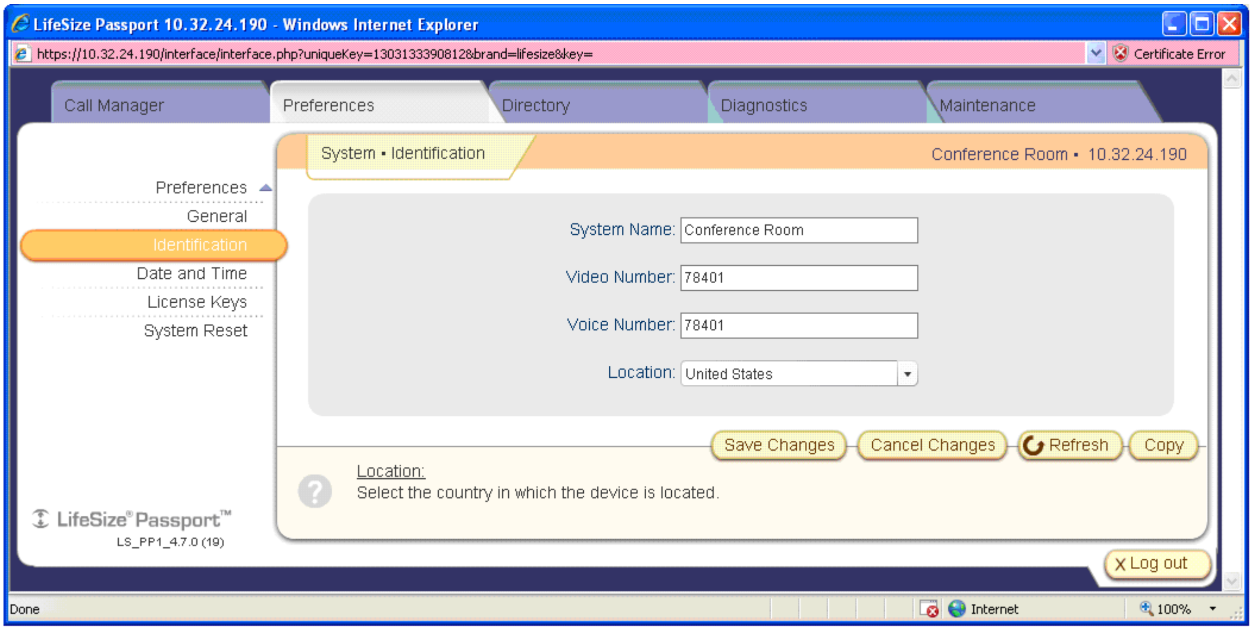
TCP Signaling Port: 5060

TLS Signaling: Disabled

TLS Signaling Port: 5061

SIP Registration:
Select the communication path to use when registering with a SIP Registrar.

Lastly, to display the Passport'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's extension as shown below. Click **Save Changes** when done.



System Name: Conference Room

Video Number: 78401

Voice Number: 78401

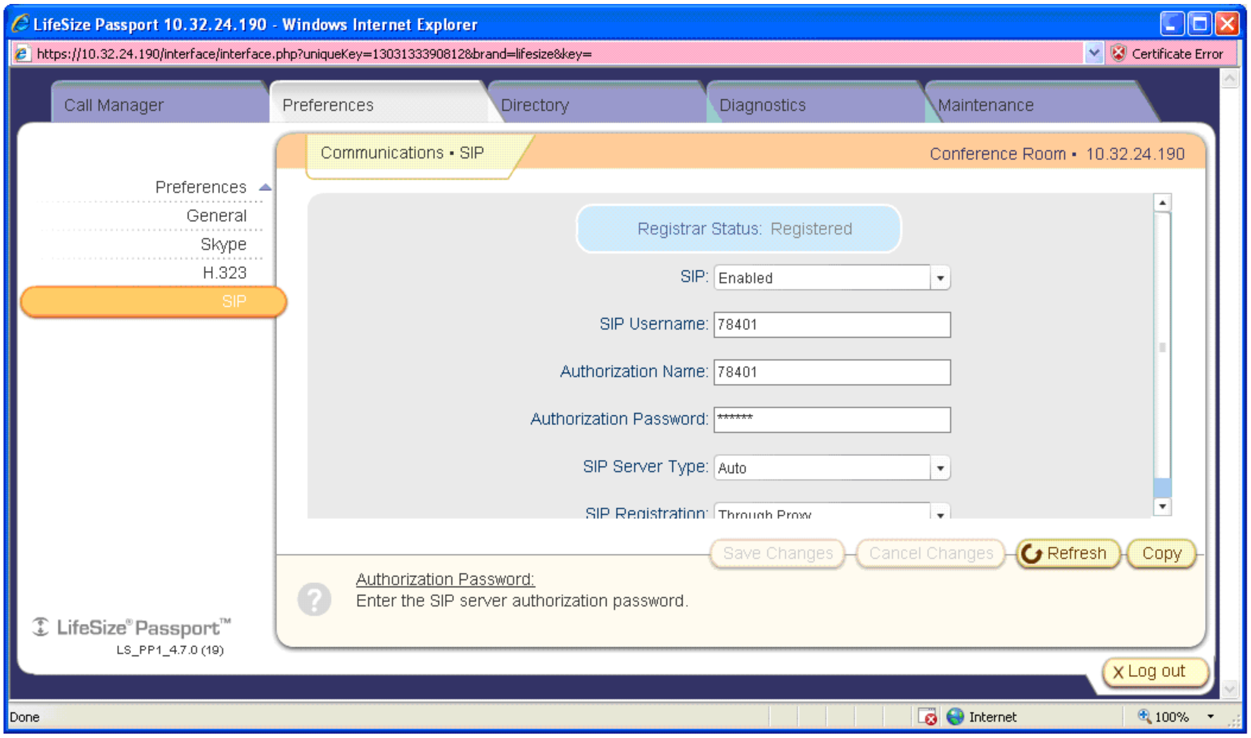
Location: United States

Location:
Select the country in which the device is located.

8. Verification Steps

This section provides the steps that may be performed to verify proper configuration of the LifeSize Passport 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.



LifeSize Passport 10.32.24.190 - Windows Internet Explorer

https://10.32.24.190/interface/interface.php?uniqueKey=1303133390812&brand=lifesize&key=

Communications • SIP

Conference Room • 10.32.24.190

Registrar Status: Registered

SIP: Enabled

SIP Username: 78401

Authorization Name: 78401

Authorization Password: ******

SIP Server Type: Auto

SIP Registration: Through Proxy

Authorization Password:
Enter the SIP server authorization password.

2. Place an outgoing video call from Passport 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 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 video system with Avaya Aura® Communication Manager and Avaya Aura® Session Manager. LifeSize Passport successfully registered with Session Manager and voice and video calls were established with LifeSize Express 220, 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*, August 2010, Release 6.0, Issue 6.0, Document Number 03-300509.

[2] *Administering Avaya Aura® Session Manager*, August 2010, Issue 3, Release 6.0, Document Number 03-603324.

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

[3] *LifeSize Passport Installation Guide*, October 2009.

[4] *LifeSize Passport User Guide*, October 2009.

[5] *LifeSize Express 220 Installation Guide*, November 2009.

[6] *LifeSize Express 220 User Guide*, November 2009.

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.