



Avaya Solution & Interoperability Test Lab

Application Notes for PatientSafe Solutions' PatientTouch Communications with Avaya Aura® Communication Manager and Avaya Aura® Session Manager using SIP Trunks – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for PatientSafe Solutions' PatientTouch Communications to interoperate with Avaya Aura® Communication Manager and Avaya Aura® Session Manager using SIP trunks.

PatientTouch Clinical Communications solution facilitates hospital care team collaboration by combining real-time clinical context with intuitive technology with minimal IT requirements. In the compliance testing, PatientTouch Communications used SIP trunks to Avaya Aura® Session Manager, for PatientTouch users to reach users on Avaya Aura® Communication Manager and on the PSTN.

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

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

1. Introduction

These Application Notes describe the configuration steps required for PatientSafe Solutions' PatientTouch Communications to interoperate with Avaya Aura[®] Communication Manager (Communication Manager) and Avaya Aura[®] Session Manager (Session Manager) using SIP trunks. Transport type of UDP was used for SIP and RTP was used for media.

PatientTouch Communications facilitates hospital care team collaboration by combining real-time clinical context with intuitive technology with minimal IT requirements. By delivering secured texting, voice, alerts, and critical context, PatientTouch Communications provides clinicians with the right information, at the right time, about the right patient, in the right way—to deliver better, safer, Connected Patient Care. In the compliance tests, PatientTouch Communications used SIP trunks to Session Manager allowing PatientTouch users to reach users on Communication Manager and on the PSTN.

2. General Test Approach and Test Results

The feature test cases were performed manually. Calls were manually established among PatientTouch users with Avaya SIP and H.323 endpoints, and/or PSTN users.

The serviceability test cases were performed manually by disconnecting and reconnecting the LAN connection to PatientTouch Communications.

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

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

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

For the testing associated with this Application Note, the interface between Avaya systems and PatientSafe Solutions did not include use of any specific encryption features as requested by PatientSafe Solutions.

2.1. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability testing.

The feature testing included; basic call, display, G.711 Mu-law, hold/reconnect, call forwarding and call transfer.

The serviceability testing focused on verifying the ability of PatientTouch Communications to recover from adverse conditions, such as disconnecting/reconnecting of network connectivity.

2.2. Test Results

All test cases passed with following observations:

- During the compliance test, only G.711 Mu-law was utilized.
- This version of PatientTouch Communications does not support conference feature and hence it was not tested.
- PatientTouch users are not members of voice messaging system and therefore Message Waiting Indicator (MWI) feature testing is not relevant for this compliance testing.
- Forwarding feature for PatientTouch users works in following scenarios, forward on manual decline, forward no answer, forward on busy, and forward on unavailable (i.e. user being logged out).

2.3. Support

Technical support on PatientTouch Communications can be obtained through the following:

- **Phone:** +1 (858) 746-3100
- **Email:** support@patientsafesolutions.com

3. Reference Configuration

Figure 1 illustrates a sample configuration of PatientTouch Communications that consists of PatientTouch servers and clients. SIP trunks are used from PatientTouch VoIP server to Session Manager, to reach users on Communication Manager and on the PSTN.

A variable digit dialing plan was used to facilitate dialing between the Avaya and PatientTouch sites. Unique extension ranges were associated with Communication Manager users (3xxxx), and PatientTouch users (1xxx).

The configuration of Session Manager was performed via the web interface of Avaya Aura® System Manager (System Manager). The configuration of Communication Manager was performed via the SAT interface. The detailed administration of basic connectivity between Communication Manager, System Manager, and Session Manager is not the focus of these Application Notes and will not be described in full detail.

The configuration of PatientTouch Communications and on iOS devices was performed by a PatientSafe Solutions engineer prior to the solution testing. During compliance testing the PatientTouch Server was installed as a virtual machine on a VMware host server.

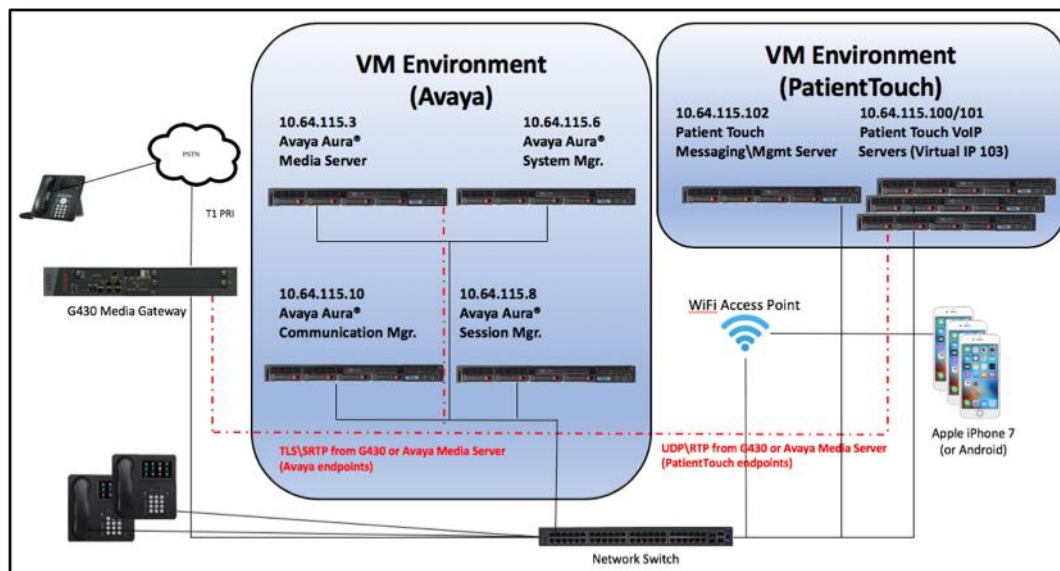


Figure 1: Avaya SIP Network with PatientSafe Solutions

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya Aura® Communication Manager running on virtualized environment	7.1.3.1.0.532.24811
Avaya Aura® Session Manager running on virtualized environment	7.1.3.0.713014
Avaya Aura® System Manager running on virtualized environment	7.1.3.0.037763
Avaya Aura® Media Server running on virtualized environment	7.8.0.333
Avaya G430 Media Gateway	39.12.0 /1
Avaya 96x1 Series IP Telephone <ul style="list-style-type: none">• 9611 (H.323)• 9641G (SIP)	6.6506 7.1.1.0.9
PatientSafe Solutions <ul style="list-style-type: none">• PatientTouch® Communications (Server/App) running on virtualized environment• iPhone 7 (MNAC2LL/A)	4.3/4.2.1 11.4.1

5. Configure Avaya Aura® Communication Manager

Configuration and verification operations on the Communication Manager illustrated in this section were all performed using an SSH System Access Terminal (SAT) session. The information provided in this section describes the configuration of the Communication Manager for this solution. For all other provisioning information such as initial installation and configuration, please refer to the product documentation in **Section 10**.

It is implied a working system is already in place. The configuration operations described in this section can be summarized as follows:

- Verify License
- Administer SIP Trunk Group
- Administer SIP Signaling Group
- Administer SIP Trunk Group Members
- Administer IP Network Region
- Administer IP Codec Set
- Administer Route Pattern
- Administer Private Numbering
- Administer Dial Plan
- Administer Uniform Dial Plan
- Administer AAR Analysis

5.1. Verify License

Verify that the Communication Manager license has proper permissions for features illustrated in these Application Notes. Use the “**display system-parameters customer-options**” command. Navigate to **Page 2** and verify that there is sufficient remaining capacity for SIP trunks by comparing the **Maximum Administered SIP Trunks** field value with the corresponding value in the **USED** column.

display system-parameters customer-options		Page 2 of 12
OPTIONAL FEATURES		
IP PORT CAPACITIES		USED
Maximum Administered H.323 Trunks:	4000	0
Maximum Concurrently Registered IP Stations:	2400	10
Maximum Administered Remote Office Trunks:	4000	0
Maximum Concurrently Registered Remote Office Stations:	2400	0
Maximum Concurrently Registered IP eCons:	68	0
Max Concur Registered Unauthenticated H.323 Stations:	100	0
Maximum Video Capable Stations:	2400	0
Maximum Video Capable IP Softphones:	2400	0
Maximum Administered SIP Trunks:	4000	55
Maximum Administered Ad-hoc Video Conferencing Ports:	4000	0
Maximum Number of DS1 Boards with Echo Cancellation:	80	0

5.2. Administer SIP Trunk Group

An existing SIP Trunk was used for this testing, the following values demonstrate the settings.

- **Group Type:** *sip*
- **Group Name:** A descriptive name.
- **TAC:** An available trunk access code.
- **Service Type:** *tie*

display trunk-group 10		Page 1 of 21
TRUNK GROUP		
Group Number: 10	Group Type: sip	CDR Reports: y
Group Name: toSM1	COR: 1	TN: 1 TAC: 110
Direction: two-way	Outgoing Display? n	Night Service:
Dial Access? n		
Queue Length: 0		
Service Type: tie	Auth Code? n	
	Member Assignment Method: auto	
	Signaling Group: 10	
	Number of Members: 25	

Navigate to **Page 3** and enter *private* for **Numbering Format**.

```
display trunk-group 10                                     Page 3 of 21
TRUNK FEATURES
    ACA Assignment? n                                     Measured: none
                                                         Maintenance Tests? y

    Suppress # Outpulsing? n   Numbering Format: private
                                                         UUI Treatment: service-provider
                                                         Replace Restricted Numbers? n
                                                         Replace Unavailable Numbers? n
                                                         Hold/Unhold Notifications? y
    Modify Tandem Calling Number: no

    Show ANSWERED BY on Display? y

    DSN Term? n
```


5.3. Administer SIP Signaling Group

An existing SIP Signaling Group was used for this testing, the following values demonstrate the settings.

- **Group Type:** *sip*
- **Transport Method:** *tls*
- **Near-end Node Name:** An existing C-LAN node name or *procr*
- **Far-end Node Name:** The existing node name for Session Manager
- **Near-end Listen Port:** An available port for integration with Session Manager
- **Far-end Listen Port:** The same port number as used in **Section 6.5.2**
- **Far-end Network Region:** An existing network region to use with Session Manager
- **Far-end Domain:** The applicable domain name for the network
- **Direct IP-IP Audio Connections:** *y*

```
display signaling-group 10                                     Page 1 of 3

                                SIGNALING GROUP

Group Number: 10                      Group Type: sip
IMS Enabled? n                      Transport Method: tls
Q-SIP? n
IP Video? n                      Enforce SIPS URI for SRTP? y
Peer Detection Enabled? y Peer Server: SM
Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? y
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? n
Alert Incoming SIP Crisis Calls? n
Near-end Node Name: procr                      Far-end Node Name: sildvsm1
Near-end Listen Port: 5061                      Far-end Listen Port: 5061
                                                Far-end Network Region: 1

Far-end Domain: sildenver.org

Bypass If IP Threshold Exceeded? n
Incoming Dialog Loopbacks: eliminate                      RFC 3389 Comfort Noise? n
DTMF over IP: rtp-payload                      Direct IP-IP Audio Connections? y
Session Establishment Timer(min): 3                      IP Audio Hairpinning? n
Enable Layer 3 Test? y                      Initial IP-IP Direct Media? n
H.323 Station Outgoing Direct Media? n                      Alternate Route Timer(sec): 6
```

5.4. Administer SIP Trunk Group Members

Use the “**change trunk-group n**” command, where “**n**” is the trunk group number from **Section 5.2**. Enter the following values for the specified fields and retain the default values for the remaining fields.

- **Signaling Group:** The signaling group number from **Section 5.3**.
- **Number of Members:** The desired number of members, in this case 25.

change trunk-group 10			Page 1 of 21	
TRUNK GROUP				
Group Number: 10		Group Type: sip		CDR Reports: y
Group Name: toSM1		COR: 1	TN: 1	TAC: 110
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: 10		
		Number of Members: 25		

5.5. Administer IP Network Region

Use the “**change ip-network-region n**” command, where “**n**” is the existing Far-end Network Region number used by the SIP signaling group from **Section 5.3**.

For **Authoritative Domain**, enter the applicable domain for the network as configured in **Section 6.2**. Enter a descriptive **Name**. Enter **yes** for **Intra-region IP-IP Direct Audio** and **Inter-region IP-IP Direct Audio**, as shown below. For **Codec Set**, enter an available codec set number for integration with PatientTouch Communications.

change ip-network-region 1		Page	1 of	20
IP NETWORK REGION				
Region: 1				
Location: Authoritative Domain: sildenvr.org				
Name: Region1 Stub Network Region: n				
MEDIA PARAMETERS Intra-region IP-IP Direct Audio: yes				
Codec Set: 1 Inter-region IP-IP Direct Audio: yes				
UDP Port Min: 2048 IP Audio Hairpinning? n				
UDP Port Max: 3329				
DIFFSERV/TOS PARAMETERS				
Call Control PHB Value: 46				
Audio PHB Value: 46				
Video PHB Value: 26				

Navigate to **Page 4**, and specify this codec set to be used for calls with network regions used by Avaya endpoints and by the trunk to the PSTN. In the compliance testing, network region *1* was used by the Avaya endpoints and by the trunk to the PSTN.

change ip-network-region 1		Page	4 of	20
Source Region: 1 Inter Network Region Connection Management				
dst codec direct WAN-BW-limits Video Intervening Dyn A G t				
rgn set WAN Units Total Norm Prio Shr Regions CAC R L e				
1 1 all				
2				

5.6. Administer IP Codec Set

Use the “**change ip-codec-set n**” command, where “**n**” is the codec set number from **Section 5.5**. Update the audio codec types in the **Audio Codec** fields as necessary. The codec shown below was used in the compliance testing.

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

                                IP MEDIA PARAMETERS

Codec Set: 1

Audio      Silence      Frames      Packet
Codec      Suppression  Per Pkt    Size (ms)
1: G.711MU      n          2          20
2:
3:

Media Encryption                                Encrypted SRTCP: enforce-unenc-srtcp
1: 1-srtp-aescm128-hmac80
2: 2-srtp-aescm128-hmac32
3: none
4:
```

5.7. Administer Route Pattern

Use the “**change route-pattern n**” command, where “**n**” is an existing route pattern number to be used to reach PatientTouch Communications, in this case “1”. Enter the following values for the specified fields and retain the default values for the remaining fields.

- **Pattern Name:** A descriptive name.
- **Grp No:** The SIP trunk group number from **Section 0**.
- **FRL:** A level that allows access to this trunk, with 0 being least restrictive.
- **Numbering Format:** lev0-pvt (private numbering) was used to ensure 4 and 5-digit extensions appeared on both ends.

```
change route-pattern 10                                   Page 1 of 3

                                Pattern Number: 1      Pattern Name: To SM on VM
SCCAN? n      Secure SIP? n      Used for SIP stations? n

Grp FRL NPA Pfx Hop Toll No. Inserted      DCS/ IXC
No      Mrk Lmt List Del Digits      QSIG
                                Dgts      Intw
1: 1      0                                n      user
2:                                n      user
3:                                n      user
4:                                n      user
5:                                n      user
6:                                n      user

BCC VALUE      TSC CA-TSC      ITC BCIE Service/Feature PARM Sub      Numbering LAR
0 1 2 M 4 W      Request      rest      Dgts      Format
1: y y y y y n      n      rest      lev0-pvt      none
```

5.8. Administer Private Numbering

Use the “**change private-numbering 0**” command, to define the calling party number to send to PatientTouch Communications. Add an entry for the trunk group defined in **Section 0**. In the example shown below, all calls originating from a 5-digit extension beginning with 3 and routed to any trunk group will result in a 5-digit calling number. The calling party number will be in the SIP “From” header.

change private-numbering 0					Page 1 of 2
NUMBERING - PRIVATE FORMAT					
Ext Len	Ext Code	Trk Grp(s)	Private Prefix	Total Len	
5	3			5	Total Administered: 4 Maximum Entries: 540

5.9. Administer Dial Plan

This section provides a sample dial plan used for routing calls with dialed digits 1xxx to PatientTouch Communications. Use the “**change dialplan analysis 0**” command, and add an entry to specify the use of digits pattern 1, as shown below

change dialplan analysis										Page 1 of 12
DIAL PLAN ANALYSIS TABLE										
Location: all					Percent Full: 2					
Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type		
0	1	attd								
1	3	dac								
1	11	udp								
3	5	ext								
4	5	ext								
5	5	ext								
8	1	fac								
9	1	fac								
*	3	fac								
#	3	fac								
1	4	udp								

5.10. Administer Uniform Dial Plan

This section provides a sample AAR routing used for routing calls with dialed digits 1xxx to PatientTouch Communications. Note that other routing methods may be used. Use the “**change uniform-dialplan 0**” command and add an entry to specify the use of AAR for routing of digits 1xxx, as shown below.

change uniform-dialplan 0									Page 1 of 2
UNIFORM DIAL PLAN TABLE									
									Percent Full: 0
Matching Pattern	Len	Del	Insert Digits	Net	Conv	Node Num			
1	11	0		ars	n				
1	4	0		aar	n				

5.11. Administer AAR Analysis

Use the “**change aar analysis 0**” command and add an entry to specify how to route calls to 1xxx. In the example shown below, calls with digits 1xxx will be routed as an AAR call using route pattern *10* from **Section 5.7**.

change aar analysis 0							Page 1 of 2	
AAR DIGIT ANALYSIS TABLE								
Location: all							Percent Full: 2	
Dialed String		Total Min Max		Route Pattern	Call Type	Node Num	ANI Req'd	
3		5 5		10	aar		n	
<u>1</u>		<u>4 4</u>		<u>10</u>	<u>aar</u>	<u></u>	<u>n</u>	

6. Configure Avaya Aura® Session Manager

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

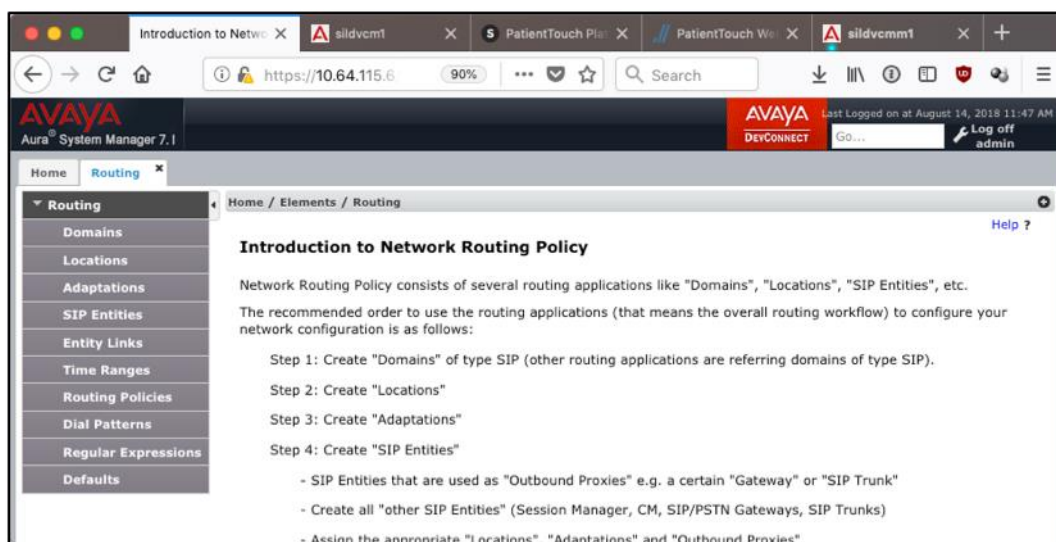
- Launch System Manager
- Administer Domain
- Administer Locations
- Administer Adaptation
- Administer SIP Entities
- Administer Routing Policies
- Administer Dial Patterns

6.1. Launch System Manager

Access the System Manager web interface by using the URL “https://ip-address” in an Internet browser window, where “ip-address” is the IP address of System Manager. Log in using the appropriate credentials.

6.2. Administer Domain

In the subsequent screen (not shown), select **Elements** → **Routing** to display the **Introduction to Network Routing Policy** screen below. Select **Routing** → **Domains** from the left pane, and click **New** in the subsequent screen (not shown) to add a new domain



The **Domain Management** screen is displayed. In the **Name** field enter the domain name, select *sip* from the **Type** drop down menu and provide any optional **Notes**.

Domain Management

Commit Cancel

1 Item Filter: Enable

Name	Type	Notes
*sldenver.org	sip	

Commit Cancel

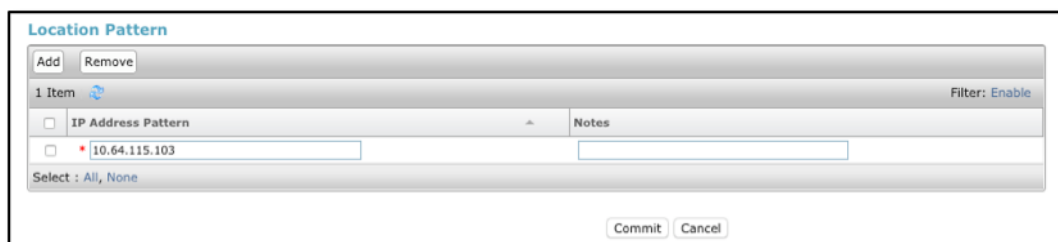
6.3. Administer Locations

Select **Routing** → **Locations** from the left pane and click **New** in the subsequent screen (not shown) to add a new location for PatientTouch Communications.

The **Location Details** screen is displayed. In the **General** sub-section, enter a descriptive **Name** and optional **Notes**. Retain the default values in the remaining fields.



Scroll down to the **Location Pattern** sub-section, click **Add** and enter the IP address of all devices involved in the compliance testing in **IP Address Pattern**, as shown below. In this case, the Virtual IP server is the only address Session Manager will see.



6.4. Administer Adaptation

During compliance test, in order to make the call from and to Communication Manager via Session Manager, an Adaptation to translate IP address into domain name and vice-a-versa, is used for PatientTouch Communications SIP entity. Select **Adaptations** on the left panel menu and then click on the **New** button in the main window (not shown).

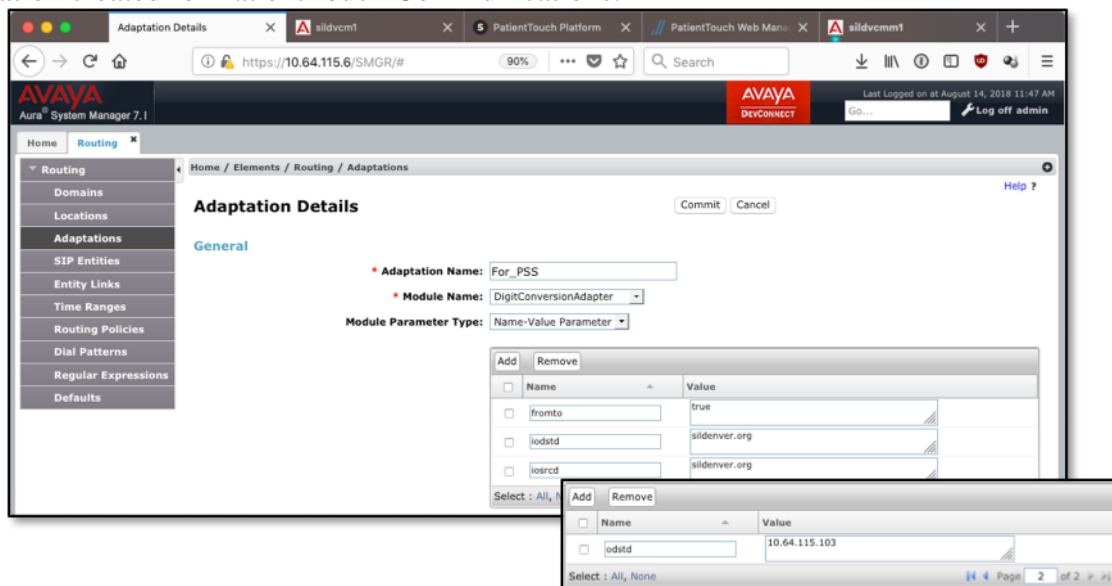
Enter the following for the PatientTouch Communications Adaptation.

- **Adaptation Name** An informative name (e.g., *For_PSS*)
- **Module Name** Select *DigitConversionAdapter*
- **Module Parameter Type** Select *Name-Value Parameter*

Click **Add** to add a new row for the following values as shown below table:

Name	Value
fromto	true
iodstd	Enter the domain name of system, example <i>sildenver.org</i>
iosrcd	Enter the domain name of system, example <i>sildenver.org</i>
odstd	Enter IP address of PatientTouch Communications, <i>10.64.115.103</i>

Once the correct information is entered click the **Commit** button. Below screen shows the Adaptation created for PatientTouch Communications.



6.5. Administer SIP Entities

Add two new SIP entities, one for PatientTouch Communications and one for the new SIP trunks with Communication Manager.

6.5.1. SIP Entity for PatientTouch Communications

Select **Routing** → **SIP Entities** from the left pane and click **New** in the subsequent screen (not shown) to add a new SIP entity for PatientTouch Communications.

The **SIP Entity Details** screen is displayed. Enter the following values for the specified fields and retain the default values for the remaining fields.

- **Name:** A descriptive name.
- **FQDN or IP Address:** The IP address of PatientTouch Communications server.
- **Type:** *Other*
- **Notes:** Any desired notes.
- **Adaptation:** Select the adaptation configured in **Section 6.4**.
- **Location:** Select the PatientTouch Communications location name from **Section 6.3**.
- **Time Zone:** Select the applicable time zone.

The screenshot shows the 'SIP Entity Details' web form in a browser. The left sidebar has a menu with 'Routing' selected, and 'SIP Entities' is highlighted under it. The main content area is titled 'SIP Entity Details' and has 'General' selected. The form contains the following fields and values:

- Name:** PatientSafe
- FQDN or IP Address:** 10.64.115.103
- Type:** Other
- Notes:** (empty)
- Adaptation:** For_PSS
- Location:** PatientSafe
- Time Zone:** America/Denver
- SIP Timer B/F (in seconds):** 4
- Minimum TLS Version:** Use Global Setting
- Credential name:** (empty)
- Securable:** ☐
- Call Detail Recording:** none
- CommProfile Type Preference:** (empty)
- Loop Detection:**
 - Loop Detection Mode:** On
 - Loop Count Threshold:** 5
 - Loop Detection Interval (in msec):** 200
- Monitoring:**
 - SIP Link Monitoring:** Link Monitoring Enabled

Buttons for 'Commit' and 'Cancel' are at the top right of the form area.

Scroll down to the **Entity Links** sub-section and click **Add** to add an entity link. Enter the following values for the specified fields and retain the default values for the remaining fields.

- **Name:** A descriptive name.
- **SIP Entity 1:** The Session Manager entity name, in this case *sildvsm1*.
- **Protocol:** *UDP*
- **Port:** *5060*
- **SIP Entity 2:** The PatientTouch Communications entity name from this section.
- **Port:** *5060*
- **Connection Policy:** *trusted*

Note that only UDP protocol was tested.

Entity Links

Override Port & Transport with DNS SRV: ☐

Add Remove

1 Item Filter: Enable

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Deny New Service
* sildvsm1_PatientSafe	sildvsm1	UDP	* 5060	PatientSafe	* 5060	trusted	<input type="checkbox"/>

Select: All, None

6.5.2. SIP Entity for Communication Manager

Select **Routing** → **SIP Entities** from the left pane and click **New** in the subsequent screen (not shown) to add a new SIP entity for Communication Manager.

The **SIP Entity Details** screen is displayed. Enter the following values for the specified fields and retain the default values for the remaining fields.

- **Name:** A descriptive name.
- **FQDN or IP Address:** The IP address of an existing CLAN or the processor interface.
- **Type:** *CM*
- **Notes:** Any desired notes.
- **Location:** Select the applicable location for Communication Manager.
- **Time Zone:** Select the applicable time zone.

The screenshot shows the Avaya Aura System Manager 7.1 interface. The left-hand navigation pane is expanded, showing the 'Routing' section with 'SIP Entities' selected. The main content area displays the 'SIP Entity Details' form for a new entity named 'sildvcm1'. The form includes fields for Name, FQDN or IP Address (10.64.115.10), Type (CM), Notes, Adaptation, Location (Data Center), Time Zone (America/Denver), SIP Timer B/F (4), Minimum TLS Version (Use Global Setting), Credential name, Securable (unchecked), Call Detail Recording (both), Loop Detection Mode (On), Loop Count Threshold (5), Loop Detection Interval (200), SIP Link Monitoring (Use Session Manager Configuration), CRLF Keep Alive Monitoring (Use Session Manager Configuration), Supports Call Admission Control (unchecked), Shared Bandwidth Manager (unchecked), Primary Session Manager Bandwidth Association, and Backup Session Manager Bandwidth Association. The 'Commit' and 'Cancel' buttons are visible at the top right of the form.

Scroll down to the **Entity Links** sub-section and click **Add** to add an entity link. Enter the following values for the specified fields and retain the default values for the remaining fields.

- **Name:** A descriptive name.
- **SIP Entity 1:** The Session Manager entity name, in this case *sildvsm1*.
- **Protocol:** The signaling group transport (*TLS*) method from **Section 5.3**.
- **Port:** The signaling group listen port (*5061*) number from **Section 5.3**.
- **SIP Entity 2:** The Communication Manager entity name from this section.
- **Port:** The signaling group listen port (*5061*) number from **Section 5.3**.
- **Connection Policy:** *trusted*

Entity Links

Override Port & Transport with DNS SRV: ☐

Add Remove

1 Item Filter: Enable

<input type="checkbox"/>	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Deny New Service
<input type="checkbox"/>	* sildvsm1_sildvcm1	sildvsm1	TLS	* 5061	sildvcm1	* 5061	trusted	<input type="checkbox"/>

Select : All, None

6.6. Administer Routing Policies

Add two new routing policies, one for PatientTouch Communications and one for the new SIP trunks with Communication Manager.

6.6.1. Routing Policy for PatientTouch Communications

Select **Routing** → **Routing Policies** from the left pane and click **New** in the subsequent screen (not shown) to add a new routing policy for PatientTouch Communications.

The **Routing Policy Details** screen is displayed. In the **General** sub-section, enter a descriptive **Name**, and retain the default values in the remaining fields.

In the **SIP Entity as Destination** sub-section, click **Select** and select the PatientTouch Communications entity name from **Section 6.5.1**. The screen below shows the result of the selection.

The screenshot shows the Avaya Aura System Manager 7.1 interface. The left navigation pane is expanded to 'Routing' > 'Routing Policies'. The main content area is titled 'Routing Policy Details' and has 'Commit' and 'Cancel' buttons. The 'General' section contains the following fields:

- Name:** Route_to_PatientSafe
- Disabled:** ☐
- Retries:** 0
- Notes:** (empty text area)

The 'SIP Entity as Destination' section features a 'Select' button and a table with the following data:

Name	FQDN or IP Address	Type	Notes
PatientSafe	10.64.115.103	Other	

6.6.2. Routing Policy for Communication Manager

Select **Routing** → **Routing Policies** from the left pane and click **New** in the subsequent screen (not shown) to add a new routing policy for Communication Manager.

The **Routing Policy Details** screen is displayed. In the **General** sub-section, enter a descriptive **Name**, and retain the default values in the remaining fields.

In the **SIP Entity as Destination** sub-section, click **Select** and select the Communication Manager entity name from **Section 6.5.2**. The screen below shows the result of the selection.

The screenshot displays the 'Routing Policy Details' configuration page in the Avaya Aura System Manager 7.1 interface. The left-hand navigation pane shows the 'Routing' menu expanded, with 'Routing Policies' selected. The main content area is titled 'Routing Policy Details' and includes 'Commit' and 'Cancel' buttons. The 'General' tab is active, showing the following fields:

- Name:** sildvcm1
- Disabled:** ☐
- Retries:** 0
- Notes:** (empty text area)

Below the 'General' tab is the 'SIP Entity as Destination' section. It features a 'Select' button and a table with the following data:

Name	FQDN or IP Address	Type	Notes
sildvcm1	10.64.115.10	CM	

6.7. Administer Dial Patterns

Add a new dial pattern for PatientTouch Communications and Communication Manager.

6.7.1. Dial Pattern for PatientTouch Communications

Select **Routing** → **Dial Patterns** from the left pane and click **New** in the subsequent screen (not shown) to add a new dial pattern to reach PatientTouch Communications. The **Dial Pattern Details** screen is displayed. In the **General** sub-section, enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Pattern:** A dial pattern to match, in this case *1*.
- **Min:** The minimum number of digits to match.
- **Max:** The maximum number of digits to match.
- **SIP Domain:** The domain name from **Section 6.2**.

In the **Originating Locations and Routing Policies** sub-section, click **Add** and create an entry for reaching PatientTouch Communications. In the compliance testing, the entry allowed for call originations from all Communication Manager endpoints in all locations. The PatientTouch Communications routing policy from **Section 6.6.1** was selected as shown below.

The screenshot shows the 'Dial Pattern Details' screen in the Avaya Aura System Manager 7.1. The left sidebar shows the 'Routing' menu with 'Dial Patterns' selected. The main content area is divided into two sections: 'General' and 'Originating Locations and Routing Policies'.

General Section:

- Pattern:** 1
- Min:** 4
- Max:** 4
- Emergency Call:** ☐
- Emergency Priority:** 1
- Emergency Type:**
- SIP Domain:** sildenver.org
- Notes:**

Originating Locations and Routing Policies Section:

Buttons: Add, Remove

1 Item

Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/> -ALL-	Route_to_PatientSafe		0	<input type="checkbox"/>	PatientSafe	

Select : All, None

6.7.2. Dial Pattern for Communication Manager

Select **Routing** → **Dial Patterns** from the left pane and click **New** in the subsequent screen (not shown) to add a new dial pattern to reach Communication Manager. The **Dial Pattern Details** screen is displayed. In the **General** sub-section, enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Pattern:** A dial pattern to match, in this case 3.
- **Min:** The minimum number of digits to match.
- **Max:** The maximum number of digits to match.
- **SIP Domain:** The signaling group domain name from **Section 6.2**.

In the **Originating Locations and Routing Policies** sub-section, click **Add** and create an entry for reaching Communication Manager. In the compliance testing, the entry allowed for call originations from all PatientTouch Communications endpoints in all locations. The Communication Manager routing policy from **Section 6.6.2** was selected as shown below.

Follow the procedures in this section to make similar changes to the applicable Communication Manager dial pattern to reach the PSTN (not shown).

The screenshot displays the Avaya Aura System Manager 7.1 web interface. The left navigation pane shows the 'Routing' menu expanded, with 'Dial Patterns' selected. The main content area is titled 'Dial Pattern Details' and includes 'Commit' and 'Cancel' buttons. The 'General' tab is active, showing the following fields:

- Pattern:** 3
- Min:** 5
- Max:** 5
- Emergency Call:** ☐
- Emergency Priority:** 1
- Emergency Type:**
- SIP Domain:** sildcnr.org
- Notes:**

Below the 'General' section is the 'Originating Locations and Routing Policies' section, which includes an 'Add' button and a table with one item:

Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
-ALL-		sildcnr1	0	<input type="checkbox"/>	sildcnr1	

Below this table is the 'Denied Originating Locations' section, which includes an 'Add' button and a table with zero items:

Originating Location	Notes
----------------------	-------

The interface also shows a 'Log off admin' button in the top right corner.

7. Configure PatientSafe Solutions' PatientTouch Communications

PatientSafe engineer installs, configures, and customizes the PatientTouch applications for their end customers. By PatientSafe Solutions request, installation/configuration steps were not included in these Application Notes. To acquire above information, please contact PatientSafe Solutions.

8. Verification Steps

This section provides the tests that can be performed to verify proper configuration of the solution.

8.1. Verify Avaya Aura® Session Manager

From the System Manager home page, select **Elements** → **Session Manager** to display the **Session Manager Dashboard** screen (not shown). Select **Session Manager** → **System Status** → **SIP Entity Monitoring** from the left pane to display the **SIP Entity Link Monitoring Status Summary** screen. Click on the PatientTouch entity name from **Section 6.5.1**.

The screenshot shows the Avaya Aura Session Manager interface. The left navigation pane is expanded to 'System Status' > 'SIP Entity Monitoring'. The main content area displays the 'SIP Entity Link Monitoring Status Summary' page. It includes a 'Run Monitor' button and a table titled 'SIP Entities Status for All Monitoring Session Manager Instances'. The table has columns for Session Manager, Type, Monitored Entities (Down, Partially Up, Up, Not Monitored), Deny, and Total. One item, 'sildvsm1', is listed with a 'Core' type and 4 'Up' entities. Below this is a section for 'All Monitored SIP Entities' with a 'Run Monitor' button and a list of 4 items: 'sildvsm1Agents', 'sildvcmm', 'PatientSafe', and 'sildvcm1'. A 'Filter: Enable' button is visible on the right of both tables.

Session Manager	Type	Monitored Entities	Down	Partially Up	Up	Not Monitored	Deny	Total
sildvsm1	Core		0	0	4	0	0	4

SIP Entity Name
sildvsm1Agents
sildvcmm
PatientSafe
sildvcm1

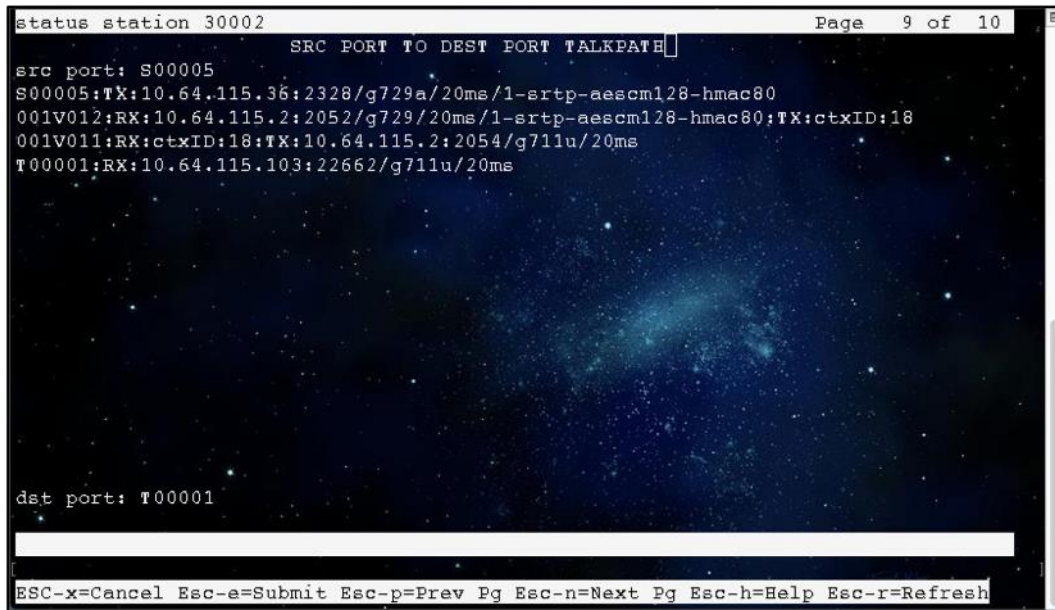
The **SIP Entity, Entity Link Connection Status** screen is displayed. Verify that **Conn. Status** and **Link Status** are *Up*, as shown below.

The screenshot shows the Avaya Aura Session Manager interface. The left navigation pane is expanded to 'System Status' > 'SIP Entity Monitoring'. The main content area displays the 'SIP Entity, Entity Link Connection Status' page. It includes a 'Status Details for the selected Session Manager:' section and a table titled 'All Entity Links to SIP Entity: PatientSafe'. The table has columns for Session Manager Name, IP Address Family, SIP Entity Resolved IP, Port, Proto., Deny, Conn. Status, Reason Code, and Link Status. One item, 'sildvsm1', is listed with IP Address Family 'IPv4', SIP Entity Resolved IP '10.64.115.103', Port '5060', Proto. 'UDP', Deny 'FALSE', Conn. Status 'UP', Reason Code '200 OK', and Link Status 'UP'. A 'Filter: Enable' button is visible on the right of the table.

Session Manager Name	IP Address Family	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
sildvsm1	IPv4	10.64.115.103	5060	UDP	FALSE	UP	200 OK	UP

8.2. Verify Avaya Aura® Communication Manager

With an active call in progress, use the **status station** command and change page to the talkpath page to view codecs used in the call. In the example below, the Avaya H.323 phone and G430 are connected with g729a with SRTP, while the G430 connection to the PatientSafe server is g711mulaw with no encryption.



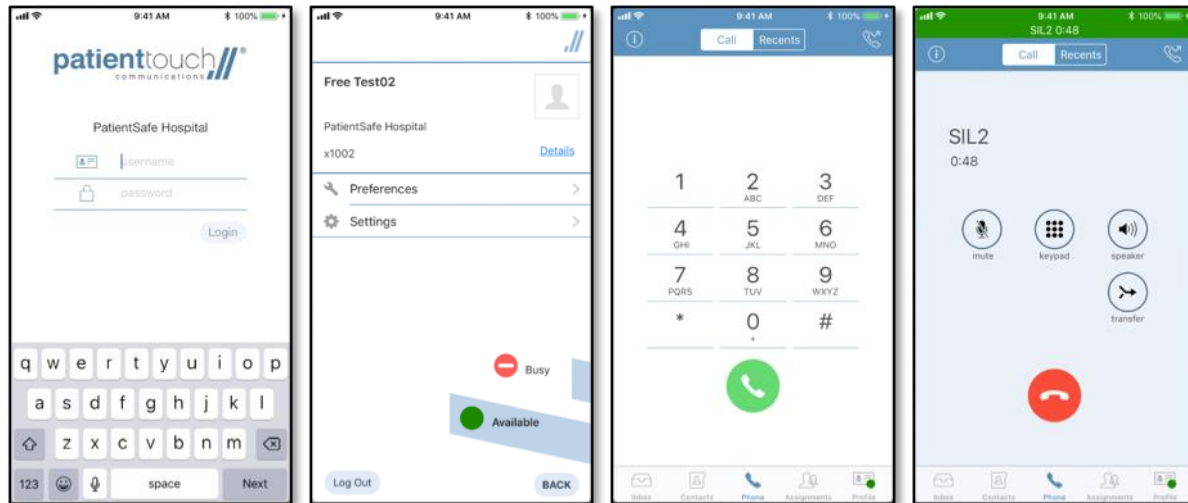
```
status station 30002                                     Page 9 of 10
SRC PORT TO DEST PORT TALKPATH
src port: S00005
S00005:TX:10.64.115.36:2328/g729a/20ms/1-srtp-aescm128-hmac80
001V012:RX:10.64.115.2:2052/g729/20ms/1-srtp-aescm128-hmac80;TX:ctxID:18
001V011:RX:ctxID:18;TX:10.64.115.2:2054/g711u/20ms
T00001:RX:10.64.115.103:22662/g711u/20ms

dst port: T00001

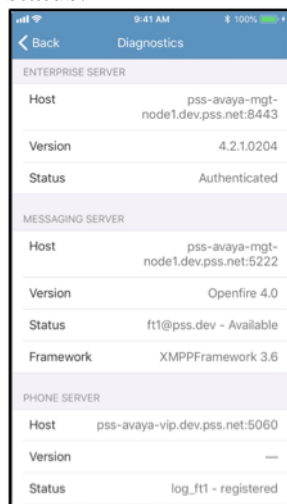
ESC-x=Cancel ESC-e=Submit ESC-p=Prev Pg ESC-n=Next Pg ESC-h=Help ESC-r=Refresh
```

8.3. Verify PatientSafe Solutions' PatientTouch Communications

From one of the PatientTouch softphones, login a user and navigate to the phone screen and place a test call to an Avaya phone.



Also, navigating to the diagnostics screen will confirm Enterprise, messaging and phone login status:



Please contact PatientSafe Solutions for further information.

9. Conclusion

These Application Notes describe the configuration steps required for PatientSafe's PatientTouch Communications to successfully interoperate with Avaya Aura® Communication Manager and Avaya Aura® Session Manager using SIP trunks. All feature and serviceability test cases were completed with observations noted in **Section 2.2**.

10. Additional References

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

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

1. *Administering Avaya Aura® Session Manager*, Release 7.1.3, Issue 5 July 2018
2. *Administering Avaya Aura® System Manager for Release 7.1.3*, Release 7.1.3, Issue 18 September 2018
3. *Administering Avaya Aura® Communication Manager*, Release 7.1.3 Issue 7 May 2018
4. *Avaya Aura® Communication Manager Feature Description and Implementation*, Release 7.1.3, Issue 6 May 2018

For PatientTouch Communications product documents, please contact PatientSafe Solutions.

©2018 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.