



Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Avaya Aura® Session Manager and Avaya Aura® Communication Manager with Khomp Kmedia 6400 for E1 access - Issue 1.0

Abstract

These Application Notes describe the procedure for configuring the Khomp Kmedia 6400 Gateway to interoperate with Avaya Aura® Session Manager and Avaya Aura® Communication Manager using SIP trunking along with E1 access to a simulated PSTN.

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

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

Table of Contents

1.	Introduction.....	4
2.	General Test Approach and Test Results.....	4
2.1.	Interoperability Compliance Testing.....	5
2.2.	Test Results	5
2.3.	Support	5
3.	Reference Configuration.....	6
4.	Equipment and Software Validated	7
5.	Configure Avaya Aura® Communication Manager.....	8
5.1.	Verify Avaya Aura® Communication Manager License.....	9
5.2.	Administer System Parameters Features	10
5.3.	Administer IP Node Names.....	11
5.4.	Administer IP Network Region and Codec Set.....	12
5.5.	Administer SIP Trunks with Avaya Aura® Session Manager	14
5.5.1.	Add SIP Signaling Group.....	14
5.5.2.	Add Trunk Group.....	15
5.6.	Configure Route Patterns	16
5.6.1.	Route Pattern for reaching Session Manager and Simulated PSTN Endpoints.....	16
5.7.	Administer Public Numbering	17
5.8.	Administer Dial Plan and AAR analysis	18
5.9.	Administer ARS Analysis	18
5.10.	Administer Feature Access Code.....	19
5.11.	Save Changes.....	19
6.	Configure Avaya Aura® Session Manager.....	20
6.1.	Specify SIP Domain	21
6.2.	Add Locations	22
6.3.	Add Adaptations.....	23
6.4.	Add SIP Entities and SIP Entity Links	24
6.4.1.	Adding Avaya Aura® Communication Manager SIP Entity and SIP Entity Link	24
6.4.2.	Adding Kmedia Gateway SIP Entity	26
6.5.	Add Routing Policies.....	28
6.6.	Add Dial Patterns	31
6.7.	Add Users for SIP Phones	33
6.7.1.	Identity	33
6.7.2.	Communication Profile.....	34
7.	Kmedia Configuration.....	36
7.1.	Log Into Kmedia	36
7.2.	Configure NAP.....	38
7.3.	Configure Route	39
8.	Verification Steps	42
8.1.	Verify Avaya Aura® Communication Manager Trunk Status.....	42
8.2.	SIP Monitoring on Avaya Aura® Session Manager.....	43
8.3.	Kmedia Web Interface to Observe Status	44

9.	Conclusion	45
10.	Additional References.....	45

1. Introduction

These Application Notes describe the procedure for configuring the Khomp Kmedia 6400 (Kmedia) to interoperate with Avaya Aura® Session Manager and Avaya Aura® Communication Manager using SIP trunking for E1 access to a simulated PSTN.

These Application Notes present a sample configuration for an enterprise network consisting of Avaya Aura® Session Manager and Avaya Aura® Communication Manager, integrated with an Kmedia Gateway using SIP trunk and providing E1 access to a simulated PSTN.

Kmedia is a media gateway carrier grade, for converging applications in digital communication platforms (E1/T1, STM-1 or SIP), replacing several signaling and connectivity devices by a single item of equipment.

With hardware designed to work in heavy traffic environments, the Kmedia has the main protocols for NGN 's (Next Generation Networks) and universal codecs for all the channels, besides high performance and processing capacity of calls per second.

The Kmedia-6400 is expandable up to 64 E1/T1 trunks in only 2 Us, without the use of separate servers for signaling management and processing. Each trunk can be managed for maximum use of its capacity by means of the traffic distribution system, which can comply with criteria pre-established by the user, as prioritizing routes of lower cost and re-route (configuration of the waiting time in the response of the operator ahead), etc. Furthermore, the Kmedia allows the partitioning of calls in all the routes determined by the user, simultaneously.

Offering the highest density of ports and processing of the sector and the lowest operating cost for a media gateway, the Kmedia presents an average energy consumption two thirds lower than other products of similar capacity, besides occupying less space in the Data Center, aiding to reduce rental costs and contributing to reducing the environmental impact.

The Kmedia is revolutionary in the gateways market, bringing a new reality in availability, reliability, flexibility of growth and management, and also reduced physical size.

2. General Test Approach and Test Results

The general test approach was to make calls, verify codecs, and exercise common PBX features, between endpoints located in the enterprise and the simulated PSTN.

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

2.1. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability. The feature testing focused on verifying the following:

- Simulated PSTN calls from and to Avaya endpoints
- Calling with various Avaya Deskphone models
- Support for G.711A, G.711MU, G.729, G.729AB, G722 and G.726 codecs
- SIP transport using TCP
- Codec negotiation
- Telephony supplementary features, such as Hold, Call Transfer, Conference Calling and Call Forwarding
- DTMF Tone Support
- Voicemail Coverage and Retrieval
- Direct IP-to-IP Media (also known as “Shuffling”) over SIP Trunk. Direct IP-to-IP media allows compatible phones to reconfigure the RTP path after call establishment directly between the Avaya phones and the Kmedia Gateway and release media processing resources on the Avaya Media Gateway

2.2. Test Results

The Kmedia passed compliance testing.

2.3. Support

For technical support, contact Kmedia via www.khomp.com.

3. Reference Configuration

As shown in **Figure 1**, the Avaya enterprise network uses SIP trunking for call signaling internally, and with the Kmedia Gateway in order to access the simulated PSTN. The Kmedia is managed by using the web interface. Session Manager, with its SM-100 (Security Module) network interface, routes calls between the different entities using SIP Trunks. All inter-system calls are carried over these SIP trunks. Session Manager supports flexible inter-system call routing based on the dialed number, the calling number and the system location; it can also provide protocol adaptation to allow multi-vendor systems to interoperate. Session Manager is managed by Avaya Aura® System Manager via the management network interface.

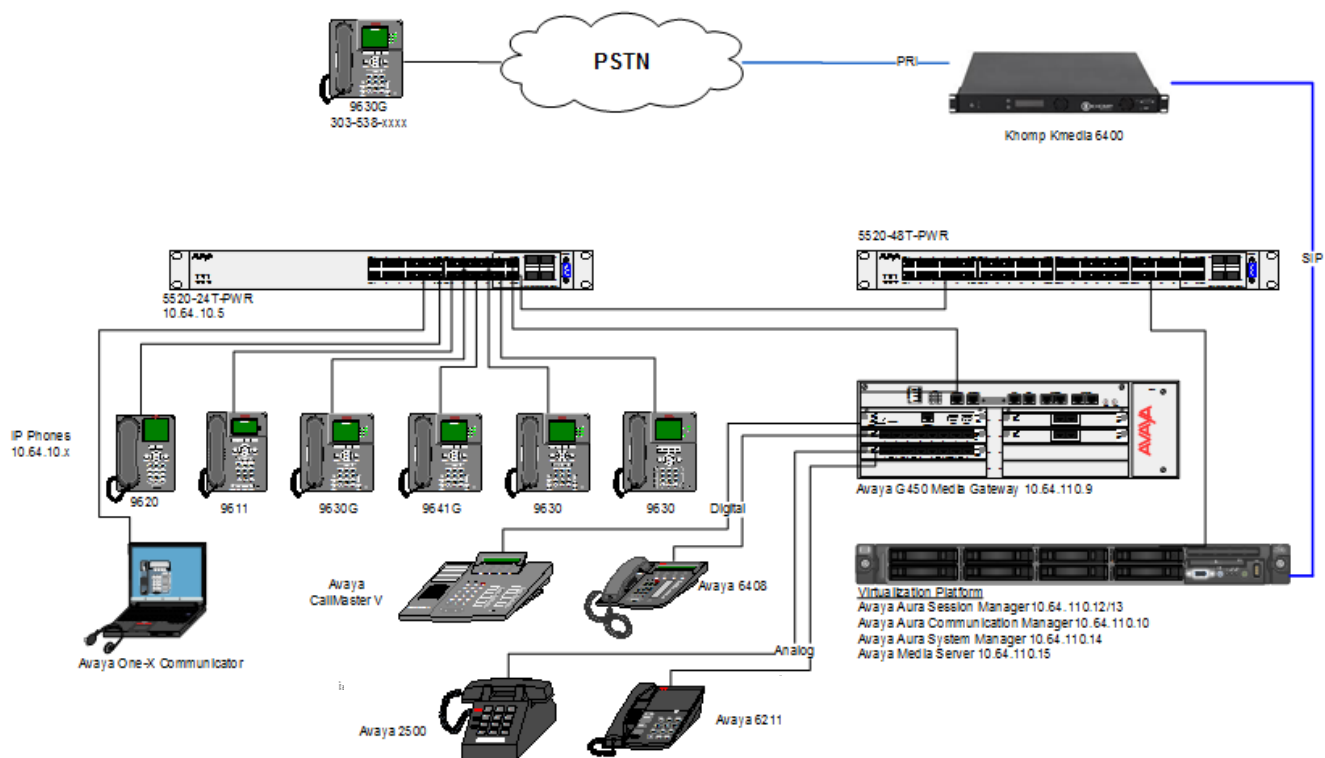


Figure 1: Compliance Test Reference Configuration

For the sample configuration shown in **Figure 1**, Session Manager, System Manager, Communication Manager, and Media Server all run in a virtual environment . These Application Notes focus on the configuration of the SIP trunks and call routing.

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya Aura® Communication Manager in a Virtual Environment	7.0 SP3
Avaya Aura® Session Manager in a Virtual Environment	7.0 SP2
Avaya Aura® System Manager in a Virtual Environment	7.0 SP2
Avaya Aura® Media Server in a Virtual Environment	7.7.0.226
Avaya 96x1 Deskphone	SIP 7.0, H.323 6.6
Avaya 6211 and 6221 Analog Phone	-
Khomp Kmedia	2.9.47

5. Configure Avaya Aura® Communication Manager

This section shows the configuration in Communication Manager. All configurations in this section are administered using the System Access Terminal (SAT). These Application Notes assumed that the basic configuration has already been administered. For further information on Communication Manager, please consult with **Reference [1]**. The procedures include the following areas:

- Verify Communication Manager License
- Administer System Parameters Features
- Administer IP Node Names
- Administer IP Network Region and Codec set
- Administer SIP Signaling Group and Trunk Group
- Administer Route Pattern
- Administer Private Numbering
- Administer Dial Plan and AAR analysis
- Administer ARS analysis
- Administer Feature Access Codes
- Save Changes

5.1. Verify Avaya Aura® Communication Manager License

Use the **display system-parameter customer options** command to verify whether the **Maximum Administered SIP Trunks** field value with the corresponding value in the **USED** column. The difference between the two values needs to be greater than or equal to the desired number of simultaneous SIP trunk connections.

Note: The license file installed on the system controls the maximum features permitted. If there is insufficient capacity or a required feature is not enabled, contact an authorized Avaya sales representative to make the appropriate changes.

change system-parameters customer-options		Page	2 of	12
OPTIONAL FEATURES				
IP PORT CAPACITIES		USED		
Maximum Administered H.323 Trunks:		4000	20	
Maximum Concurrently Registered IP Stations:		2400	1	
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	15	
Maximum Administered SIP Trunks:		4000	10	
Maximum Administered Ad-hoc Video Conferencing Ports:		4000	0	
Maximum Number of DS1 Boards with Echo Cancellation:		80	0	

5.2. Administer System Parameters Features

Use the **change system-parameters features** command to allow for trunk-to-trunk transfers. This feature is needed to allow for transferring an incoming/outgoing call from/to a remote switch back out to the same or different switch. For simplicity, the **Trunk-to-Trunk Transfer** field was set to **all** to enable all trunk-to-trunk transfers on a system wide basis.

```
change system-parameters features                               Page 1 of 19
      FEATURE-RELATED SYSTEM PARAMETERS
      Self Station Display Enabled? n
      Trunk-to-Trunk Transfer: all
      Automatic Callback with Called Party Queuing? n
      Automatic Callback - No Answer Timeout Interval (rings): 3
      Call Park Timeout Interval (minutes): 10
      Off-Premises Tone Detect Timeout Interval (seconds): 20
      AAR/ARS Dial Tone Required? y

      Music (or Silence) on Transferred Trunk Calls? all
      DID/Tie/ISDN/SIP Intercept Treatment: attendant
      Internal Auto-Answer of Attd-Extended/Transferred Calls: transferred
      Automatic Circuit Assurance (ACA) Enabled? n

      Abbreviated Dial Programming by Assigned Lists? n
      Auto Abbreviated/Delayed Transition Interval (rings): 2
      Protocol for Caller ID Analog Terminals: Bellcore
      Display Calling Number for Room to Room Caller ID Calls? y
```

5.3. Administer IP Node Names

Use the **change node-names ip** command to add entries for Communication Manager and Session Manager that will be used for connectivity. In the sample network, the processor Ethernet interface **procr** and **10.64.110.10** are entered as **Name** and **IP Address** for the signaling in Communication Manager running in a virtual environment. In addition, **asm** and **10.64.110.13** are entered for Session Manager.

change node-names ip		Page 1 of 2	
		IP NODE NAMES	
Name	IP Address		
acms	10.64.110.18		
aes	10.64.110.15		
ams	10.64.110.16		
asm	10.64.110.13		
procr	10.64.110.10		
procr6	::		

5.4. Administer IP Network Region and Codec Set

Use the **change ip-network-region n** command, where **n** is the network region number, to configure the network region being used. In the sample network ip-network-region **1** is used. For the **Authoritative Domain** field, enter the SIP domain name configured for this enterprise and a descriptive **Name** for this ip-network-region. Set **Intra-region IP-IP Direct Audio** and **Inter-region IP-IP Direct Audio** to **yes** to allow for direct media between endpoints. Set the **Codec Set** to **1** to use ip-codec-set 1.

```
change ip-network-region 1                                     Page 1 of 20
                                                                IP NETWORK REGION
    Region: 1
    Location: 1          Authoritative Domain: avaya.com
        Name: Main          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? y
        UDP Port Max: 3329
    DIFFSERV/TOS PARAMETERS
        Call Control PHB Value: 46
        Audio PHB Value: 46
        Video PHB Value: 26
    802.1P/Q PARAMETERS
        Call Control 802.1p Priority: 6
        Audio 802.1p Priority: 6
        Video 802.1p Priority: 5      AUDIO RESOURCE RESERVATION PARAMETERS
    H.323 IP ENDPOINTS          RSVP Enabled? n
        H.323 Link Bounce Recovery? y
        Idle Traffic Interval (sec): 20
        Keep-Alive Interval (sec): 5
        Keep-Alive Count: 5
```

Use the **change ip-codec-set n** command where **n** is codec set used in the configuration. The codecs used in the compliance test are shown here. Configure the IP Codec Set as shown in the screen below.

Retain the default values for the remaining fields.

```
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: G.711A      n          2       20
  3: G.729AB     n          2       20
  4:
  5:
  6:
  7:

    Media Encryption                                Encrypted SRTCP: enforce-unenc-srtcp
  1: none
  2:
  3:
  4:
  5:
```

5.5. Administer SIP Trunks with Avaya Aura® Session Manager

In the test configuration, a SIP trunk was configured between Communication Manager and Session Manager for enterprise calling between Communication Manager and Session Manager registered endpoints. Additionally a SIP trunk was configured between Session Manager and the Kmedia in order to communicate between the enterprise and the simulated PSTN. To administer a SIP Trunk on Communication Manager, two steps are required: the creation of a signaling group and a trunk group.

5.5.1. Add SIP Signaling Group

Use the **add signaling-group n** command, where **n** is an available signaling group number, for one of the SIP trunks to the Session Manager, and fill in the indicated fields. Default values can be used for the remaining fields:

- **Group Type:** sip
- **Transport Method:** tcp
- **Near-end Node Name:** procr
- **Far-end Node Name:** Session Manager node name from **Section 5.3**
i.e., asm
- **Near-end Listen Port:** 5061
- **Far-end Listen Port:** 5061
- **Far-end Network Region:** 1
- **DTMF over IP:** rtp-payload
- **Direct IP-IP Audio Connections:** y

```
add signaling-group 1                                     Page 1 of 3
                                     SIGNALING GROUP

Group Number: 1                      Group Type: sip
IMS Enabled? n                      Transport Method: tls
Q-SIP? n
IP Video? n                        Enforce SIPS URI for SRTP? n
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? y
Near-end Node Name: procr              Far-end Node Name: asm
Near-end Listen Port: 5061             Far-end Listen Port: 5061
                                     Far-end Network Region: 1

Far-end Domain: avaya.com

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

5.5.2. Add Trunk Group

Add the corresponding trunk group controlled by this signaling group via the **add trunk-group n** command, where **n** is an available trunk group number and fill in the indicated fields.

- **Group Type:** sip
- **Group Name:** A descriptive name (i.e., **asm**)
- **TAC:** An available trunk access code (i.e., **101**)
- **Service Type:** **public-ntwrk**
- **Signaling Group:** The number of the signaling group associated (i.e., **1**)
- **Number of Members:** The number of SIP trunks to be allocated to calls routed to **Session Manager** (must be within the limits of the total trunks available from license verified in **Section 5.1**)

```
change trunk-group 1                                     Page 1 of 22
                                     TRUNK GROUP
Group Number: 1                      Group Type: sip      CDR Reports: y
  Group Name: asm                    COR: 1              TN: 1      TAC: 101
  Direction: two-way                Outgoing Display? n
  Dial Access? n                    Night Service:
Queue Length: 0
Service Type: public-ntwrk        Auth Code? n
                                     Member Assignment Method: auto
                                     Signaling Group: 1
                                     Number of Members: 10
```

Navigate to **Page 3** and change **Numbering Format** to **public**. Use default values for all other fields.

```
add trunk-group 1                                         Page 3 of 21
TRUNK FEATURES
  ACA Assignment? n                      Measured: none
                                           Maintenance Tests? y

                                     Numbering Format: public
                                           UI 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
```

5.6. Configure Route Patterns

Configure route patterns to correspond to the newly added SIP trunk group. Use the **change route pattern n** command, where **n** is an available route pattern.

The route pattern, as shown below, was configured to route calls to Session Manager and simulated PSTN endpoints.

5.6.1. Route Pattern for reaching Session Manager and Simulated PSTN Endpoints

When changing the route pattern, enter the following values for the specified fields and retain the default values for the remaining fields.

- **Pattern Name:** A descriptive name (i.e., **asm**)
- **Grp No:** The trunk group number from **Section 5.5.2**
- **FRL:** Enter a level that allows access to this trunk, with **0** being least restrictive
- **No. Del Dgts:** **0** was entered to delete zero digits

change route-pattern 1													Page 1 of 3			
Pattern Number: 1													Pattern Name:asm			
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						
										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								Dgts	Format	
1:		Y Y		Y Y		Y n		n		rest						none
2:		Y Y		Y Y		Y n		n		rest						none
3:		Y Y		Y Y		Y n		n		rest						none
4:		Y Y		Y Y		Y n		n		rest						none
5:		Y Y		Y Y		Y n		n		rest						none
6:		Y Y		Y Y		Y n		n		rest						none

5.7. Administer Public Numbering

Use the **change public-numbering** command to define the calling party number to be sent out through the SIP trunk. In the sample network configuration below, all calls originating from a **5**-digit extension (**Ext Len**) beginning with **1** (**Ext Code**) and routed through any trunk will result in a **5**-digit calling number (**Total Len**). The calling party number will be in the SIP "From" header.

change public-unknown-numbering 0					Page	1 of	2
NUMBERING - PUBLIC/UNKNOWN FORMAT							
Ext	Ext	Trk	CPN	Total			
Len	Code	Grp(s)	Prefix	CPN			
				Len			
5	1			5	Total Administered: 1		
					Maximum Entries: 240		
					Note: If an entry applies to a SIP connection to Avaya Aura(R) Session Manager, the resulting number must be a complete E.164 number.		
					Communication Manager automatically inserts a '+' digit in this case.		

5.8. Administer Dial Plan and AAR analysis

Configure the dial plan for dialing 5-digit extensions beginning with **111** to stations registered with Session Manager.

Use the **change aar analysis n** command, where **n** is the dial string pattern to configure an **aar** entry for **Dialed String 111** (Extensions on Session Manager) to use **Route Pattern 1** (defined in Section 5.6). The **Call Type** was set to **lev0**.

change aar analysis 111							Page	1 of	2
AAR DIGIT ANALYSIS TABLE									
Location: all							Percent Full: 0		
	Dialed	Total		Route	Call	Node	ANI		
	String	Min	Max	Pattern	Type	Num	Reqd		
111		5	5	1	lev0		n		

5.9. Administer ARS Analysis

This section provides sample Auto Route Selection (ARS) used for routing calls with dialed digits beginning with **1** which correspond to numbers accessible via the Kmedia. Use the **change ars analysis 1** command and add an entry to specify how to route calls. Enter the following values for the specified fields and retain the default values for the remaining fields.

- **Dialed String:** Dialed digits to match on
- **Total Min:** Minimum number of digits, in this case **11**
- **Total Max:** Maximum number of digits, in this case **11**
- **Route Pattern:** The route pattern number from **Section 5.6**, i.e., **1**
- **Call Type:** hnpa

Note: The additional entries may be added for different number destinations.

change ars analysis 1							Page	1 of	2
ARS DIGIT ANALYSIS TABLE									
Location: all							Percent Full: 0		
	Dialed	Total		Route	Call	Node	ANI		
	String	Min	Max	Pattern	Type	Num	Reqd		
1		11	11	1	nat1		n		

5.10. Administer Feature Access Code

Configure a feature access code to use for AAR and ARS routing. Use the **change feature access code** command to define **Access Code** for **Auto Alternate Routing (AAR)** and for **Auto Route Selection (ARS)**. In the test configuration, **8** and **9** were used respectively.

change feature-access-codes	Page 1 of 10
FEATURE ACCESS CODE (FAC)	
Abbreviated Dialing List1 Access Code:	
Abbreviated Dialing List2 Access Code:	
Abbreviated Dialing List3 Access Code:	
Abbreviated Dial - Prgm Group List Access Code:	
Announcement Access Code:	
Answer Back Access Code:	
Attendant Access Code:	
Auto Alternate Routing (AAR) Access Code: 8	
Auto Route Selection (ARS) - Access Code 1: 9	Access Code 2:
Automatic Callback Activation:	Deactivation:

5.11. Save Changes

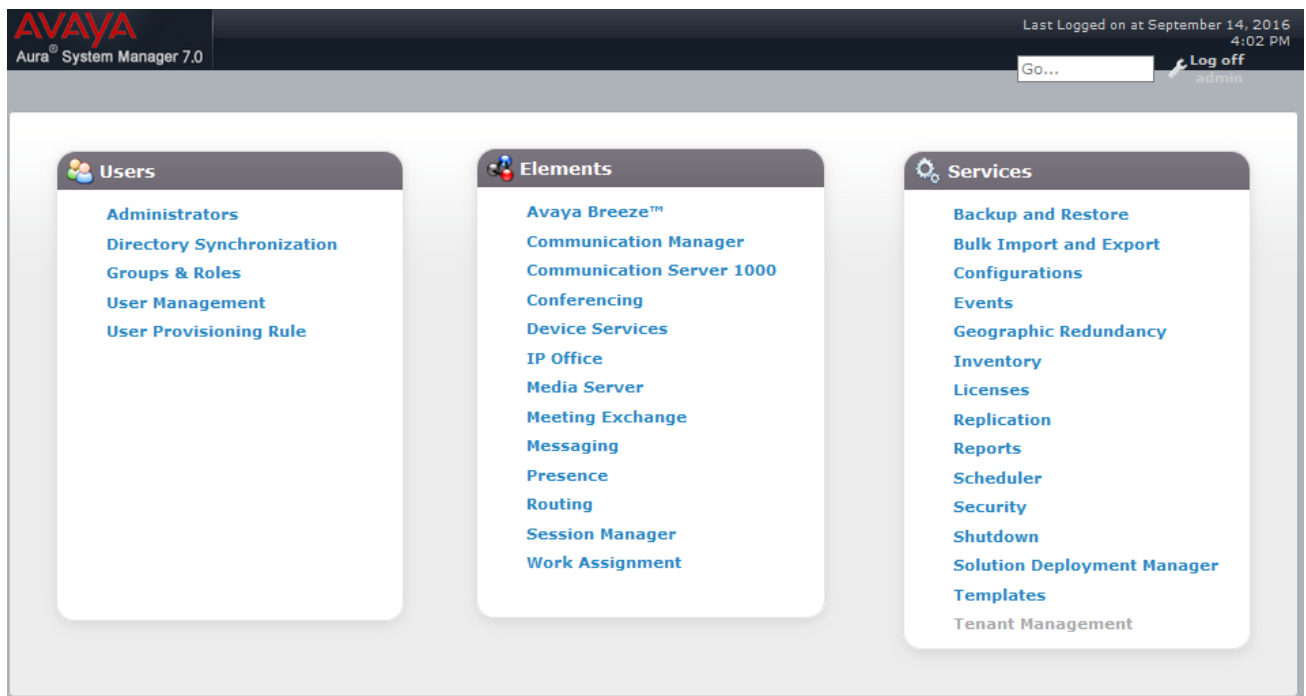
Use the **save translation** command to save all changes.

6. Configure Avaya Aura® Session Manager

This section provides the procedures for configuring Session Manager, assuming it has been installed and licensed as described in **Reference [2]**. The procedures include adding the following items:

- Specify SIP Domain
- Add Locations
- Add Adaptations
- Add SIP Entities and Entity Links
- Add Routing Policies
- Add Dial Patterns
- Add Users for SIP Phones

Configuration is accomplished by accessing the browser-based GUI of System Manager, using the URL **http://<ip-address>/SMGR**, where **<ip-address>** is the IP address of System Manager. Log in with the appropriate credentials. The home screen as shown below is displayed. Expand the **Routing** Link under **Elements**.



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 on the right (not shown). The following screen will then be shown. Fill in the following fields and click **Commit**.

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

The screenshot shows the Avaya Aura System Manager 7.0 interface. The top header includes the Avaya logo, 'Aura System Manager 7.0', and a 'Last Logged on at September 14, 2016 4:02 PM' timestamp. A 'Go...' search bar and a 'Log off' button are also present. The left sidebar contains a navigation menu with 'Routing' selected, and a sub-menu showing 'Domains', 'Locations', 'Adaptations', 'SIP Entities', 'Entity Links', 'Time Ranges', 'Routing Policies', 'Dial Patterns', 'Regular Expressions', and 'Defaults'. The main content area is titled 'Domain Management' and shows a breadcrumb trail: 'Home / Elements / Routing / Domains'. There are 'Commit' and 'Cancel' buttons at the top right. Below the title, there is a table with one item, 'avaya.com', of type 'sip'. The table has columns for 'Name', 'Type', and 'Notes'. At the bottom right, there are 'Commit' and 'Cancel' buttons.

Name	Type	Notes
* avaya.com	sip	

6.2. Add Locations

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

Under **General**:

- **Name:** A descriptive name

Under **Location Pattern**:

- **IP Address Pattern:** A pattern used to logically identify the location (optional). In these Application Notes, no pattern was defined.

Defaults can be used for the remaining fields. The screen below shows addition of the **Lab** location, which includes all the components of the compliance test environment. Click **Commit** to save.

AVAYA
Aura® System Manager 7.0

Last Logged on at September 14, 2016 4:02 PM

Go... Log off admin

Home Routing

Home / Elements / Routing / Locations

Location Details

Commit Cancel

General

* Name: DevConnect-Lab

Notes:

Dial Plan Transparency in Survivable Mode

Enabled: ☐

Listed Directory Number:

Associated CM SIP Entity:

Location Pattern

Add Remove

2 Items Filter: Enable

<input type="checkbox"/>	IP Address Pattern	Notes
<input type="checkbox"/>	*10.64.10.*	
<input type="checkbox"/>	*10.64.101.*	

Select : All, None

Commit Cancel

6.3. Add Adaptations

In order to maintain digit manipulation centrally on Session Manager, an adaptation module can be configured with a numbering plan offered from the PSTN Service Provider. To add an adaptation, select **Adaptations** on the left and click on the **New** button on the right. The following screen will then be shown. Fill in the following:

Under **General**:

- **Adaptation Name:** A descriptive name i.e., **kmedia**
- **Module Name:** From the dropdown list select **DigitConversionAdapter**
- **Module Parameter Type:** Configured as shown in the screen capture below.

The module parameters configured in the Screen capture overrides the domain avaya.com with the IP Address of Kmedia in SIP messages.

The screen below is the Adaptation detail page. Click **Commit** to save the changes.

AVAYA
Aura® System Manager 7.0

Last Logged on at October 24, 2016 2:43 PM

GO... Log off

Home Routing

Home / Elements / Routing / Adaptations

Adaptation Details

Commit Cancel

Help ?

General

* Adaptation Name: kmedia

* Module Name: DigitConversionAdapter

Module Parameter Type: Name-Value Parameter

Name	Value
fromto	true
ingressOverrideDestinationDomain	avaya.com
ingressOverrideSourceDomain	avaya.com
overrideDestinationDomain	10.64.10.132

Select : All, None

Page 1 of 2

Egress URI Parameters:

Notes:

6.4. Add SIP Entities and SIP Entity Links

A SIP Entity is required for each SIP-based telephony system wishing to communicate with Session Manager for call routing. In the sample configuration, a SIP Entity and SIP Entity Link is added for Communication Manager, and the Kmedia.

6.4.1. Adding Avaya Aura® Communication Manager SIP Entity and SIP Entity Link

Navigate to **Network Routing Policy → SIP Entities** on the left and click on the **New** button on the right (not shown).

Under **General**:

- **Name:** A descriptive name, i.e., **acm**
- **FQDN or IP Address:** IP address of the Communication Manager i.e., **10.64.110.10**
- **Type:** Select **CM**
- **Adaptation:** Select CM Adapter
- **Location:** Select one of the locations defined previously
- **Time Zone:** Time zone for this entity

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

- **Name:** Will be populated automatically
- **SIP Entity 2:** Will be populated automatically with the name of this SIP Entity.
- **SIP Entity 1:** Select Session Manager from the pull down box
- **Protocol:** Select the desired Protocol from the pull down box
- **Port:** Enter the desired port number for the Entity Link
- **Policy:** Select the appropriate Connection Policy from the pull down box

Defaults can be used for the remaining fields. Click **Commit** to save each SIP Entity definition. The following screen shows the addition of the SIP Entity for Communication Manager.

SIP Entity Details

Commit Cancel

General

* Name:

* FQDN or IP Address:

Type:

Notes:

Adaptation:

Location:

Time Zone:

* SIP Timer B/F (in seconds):

Credential name:

Securable: ☐

Call Detail Recording:

Loop Detection

Loop Detection Mode:

Loop Count Threshold:

Loop Detection Interval (in msec):

SIP Link Monitoring

SIP Link Monitoring:

Supports Call Admission Control: ☐

Shared Bandwidth Manager: ☐

Primary Session Manager Bandwidth Association:

Backup Session Manager Bandwidth Association:

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"/>	* asm_acm_5061_TLS	asm	TLS	* 5061	acm	* 5061	trusted	<input type="checkbox"/>
Select : All, None								

6.4.2. Adding Kmedia Gateway SIP Entity

Navigate to **Network Routing Policy → SIP Entities** on the left and click on the **New** button on the right (not shown).

Under **General**:

- **Name:** A descriptive name, i.e., **kmedia**
- **FQDN or IP Address:** IP address of the Kmedia i.e., **10.64.10.132**
- **Type:** Select **Gateway**
- **Adaptation:** Select **kmedia**. This was configured in **Section 6.3**
- **Location:** Select one of the locations defined previously
- **Time Zone:** Time zone for this entity
- **SIP Link Monitoring:** Use **Session Manager Configuration**

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

- **Name:** Will be populated automatically
- **SIP Entity 2:** Will be populated automatically with the name of this SIP Entity.
- **SIP Entity 1:** Select Session Manager from the pull down box
- **Protocol:** Select the desired Protocol from the pull down box
- **Port:** Enter the desired port number for the Entity Link
- **Policy:** Select the appropriate Connection Policy from the pull down box

Defaults can be used for the remaining fields. Click **Commit** to save each SIP Entity definition. The following screen shows the addition of the SIP Entity for Kmedia.

SIP Entity Details

Commit Cancel

General

* Name:

* FQDN or IP Address:

Type:

Notes:

Adaptation:

Location:

Time Zone:

* SIP Timer B/F (in seconds):

Credential name:

Securable: ☐

Call Detail Recording:

Loop Detection

Loop Detection Mode:

Loop Count Threshold:

Loop Detection Interval (in msec):

SIP Link Monitoring

SIP Link Monitoring:

Supports Call Admission Control: ☐

Shared Bandwidth Manager: ☐

Primary Session Manager Bandwidth Association:

Backup Session Manager Bandwidth Association:

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"/>	* asm_khomp_5060_TC?	asm	TCP	* 5060	kmedia	* 5060	trusted	<input type="checkbox"/>
Select : All, None								

6.5. Add Routing Policies

Routing policies describe the condition under which calls will be routed to the SIP Entities specified in **Section 6.4**. A routing policy must be added for Communication Manager and the Kmedia Gateway. To add a routing policy, select **Routing Policies** on the left and click on the **New** button on the right (not shown). The following screen is displayed. Fill in the following:

Under **General**

- Enter a descriptive **Name**

Under **SIP Entity as Destination**

- Click **Select**, and then select the appropriate SIP entity to which this routing policy applies

Under **Time of Day:**

- Click **Add**, and select the time range configured. In these Application Notes, the predefined **24/7** Time Range is used

Defaults can be used for the remaining fields. Click **Commit** to save each Routing Policy definition. The following screens show the Routing Policies for Communication Manager and the Kmedia. Note that **Dial Patterns** (to be configured in **Section 6.6**), when configured, will be automatically displayed in the **Routing Policy Details** page.

Routing Policy Details

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

General

* Name:

Disabled: ☐

* Retries:

Notes:

SIP Entity as Destination

Select			
Name	FQDN or IP Address	Type	Notes
acm	10.64.110.10	CM	

Time of Day

Add Remove View Gaps/Overlaps												
1 Item												Filter: Enable
<input type="checkbox"/>	Ranking	Name	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
<input type="checkbox"/>	3	24/7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	00:00	23:59	
Select : All , None												

Dial Patterns

Add Remove							
4 Items							Filter: Enable
<input type="checkbox"/>	Pattern	Min	Max	Emergency Call	SIP Domain	Originating Location	Notes
<input type="checkbox"/>	110	4	5	<input type="checkbox"/>	-ALL-	DevConnect-Lab	
<input type="checkbox"/>	112	5	5	<input type="checkbox"/>	-ALL-	DevConnect-Lab	
<input type="checkbox"/>	17209772872	11	11	<input type="checkbox"/>	-ALL-	-ALL-	
<input type="checkbox"/>	9	11	12	<input type="checkbox"/>	-ALL-	DevConnect-Lab	
Select : All , None							

Routing Policy Details

Commit Cancel

General

* Name:

Disabled: ☐

* Retries:

Notes:

SIP Entity as Destination

Select			
Name	FQDN or IP Address	Type	Notes
kmedia	10.64.10.132	Gateway	

Time of Day

Add Remove View Gaps/Overlaps												
1 Item												Filter: Enable
<input type="checkbox"/>	Ranking	Name	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
<input type="checkbox"/>	0	24/7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	00:00	23:59	
Select : All, None												

Dial Patterns

Add Remove							
0 Items							Filter: Enable
<input type="checkbox"/>	Pattern	Min	Max	Emergency Call	SIP Domain	Originating Location	Notes

Regular Expressions

Add Remove			
0 Items			Filter: Enable
<input type="checkbox"/>	Pattern	Rank Order	Deny Notes

6.6. Add Dial Patterns

Dial patterns must be defined that will direct calls to the appropriate SIP Entity. In the sample configuration numbers beginning with **5** with 5-digit length reside in the Enterprise network. To add a dial pattern, select **Dial Patterns** on the left and click on the **New** button on the right (not shown). Fill in the following, as shown in the screen below, which corresponds to the dial pattern for routing calls to Communication Manager.

Under **General**:

- **Pattern:** Dialed number or prefix i.e., **110**
- **Min:** Minimum length of dialed number i.e., **4**
- **Max:** Maximum length of dialed number i.e., **5**
- **SIP Domain:** Select **ALL**

Under **Originating Locations and Routing Policies**, click **Add**, and then select the appropriate location and routing policy from the list. Default values can be used for the remaining fields. Click **Commit** to save this dial pattern.

The following screen shows the dial pattern definition for calls within the Enterprise.

Dial Pattern Details

Commit Cancel

General

* **Pattern:**

* **Min:**

* **Max:**

Emergency Call: ☐

Emergency Priority:

Emergency Type:

SIP Domain: ▼

Notes:

Originating Locations and Routing Policies

Add Remove							
1 Item		Filter: Enable					
<input type="checkbox"/>	Originating Location Name ▲	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	DevConnect-Lab		acm	3	<input type="checkbox"/>	acm	
Select : All, None							

The following screen shows the dial pattern definition for calls destined for the Kmedia.

Dial Pattern Details

General

* Pattern:


* Min:

* Max:

Emergency Call: ☐



Emergency Priority:

Emergency Type:

SIP Domain: 

Notes:

Originating Locations and Routing Policies

<input type="button" value="Add"/> <input type="button" value="Remove"/>							
1 Item 		Filter: Enable					
<input type="checkbox"/>	Originating Location Name 	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	-ALL-		kmedia	0	<input type="checkbox"/>	kmedia	
Select : All , None							

6.7. Add Users for SIP Phones

From the home screen select **Users** → **User Management** → **Manage Users** to display the **User Management** screen (not shown). Click **New** to add a user.

6.7.1. Identity

The **New User Profile** screen is displayed. Enter desired **Last Name** and **First Name**. For **Login Name**, enter “n@z”, where “n” is the user extension and “z” is the domain name, in this case “avaya.com” used for compliance testing. Retain the default values in the remaining fields.

User Profile Edit: 11101@avaya.com Commit & Continue Commit Cancel

Identity *

Communication Profile

Membership

Contacts

User Provisioning Rule ▼

User Provisioning Rule:

Identity ▼

* Last Name:

Last Name (Latin Translation):

* First Name:

First Name (Latin Translation):

Middle Name:

Description:

Update Time:

* Login Name:

User Type:

[Change Password](#)

Source:

Localized Display Name:

Endpoint Display Name:

Title:

Language Preference:

Time Zone:

Employee ID:

Department:

Company:

Address ▶

Localized Names ▶

6.7.2. Communication Profile

Select the **Communication Profile** tab. For **Communication Profile Password** and **Confirm Password**, enter the desired password for the SIP user to use for registration. Scroll down to the **Communication Address** sub-section, and click **New** to add a new address.

For **Type**, retain “Avaya SIP”. For **Fully Qualified Address**, enter and select the SIP user extension and domain configured in **Section 6.7.1**. Click **Add**.

Scroll down to check and expand **Session Manager Profile**. For **Primary Session Manager**, **Origination Application Sequence**, **Termination Application Sequence**, and **Home Location**, select the values corresponding to the applicable Session Manager. Retain the default values in the remaining fields. These settings are configured during the initial setup of Session Manager.

Scroll down to check and expand **CM Endpoint Profile**. For **System**, select the value corresponding to the applicable Communication Manager. For **Extension**, enter or select the SIP user extension configured in **Section 6.7.1**. For **Template**, select corresponding Telephone type. Retain the default values in the remaining fields.

Click **Commit** to complete the creation of the new user.

Identity

Communication Profile

Membership

Contacts

Communication Profile

Communication Profile Password: [Edit](#)

New

Delete

Done

Cancel

Name

Primary

Select: None

Name: Primary

Default: ☒

Communication Address

New

Edit

Delete

Type	Handle	Domain
<input type="checkbox"/> Avaya SIP	11101	avaya.com

Select: All, None

☒ Session Manager Profile

SIP Registration

Primary Session Manager

Primary	Secondary	Maximum
8	0	8

Secondary Session Manager

Survivability Server

Max. Simultaneous Devices

Block New Registration When Maximum Registrations Active?

☐

Application Sequences

Origination Sequence

Termination Sequence

Call Routing Settings

Home Location

Conference Factory Set

Call History Settings

Enable Centralized Call History?

☐

☐ Avaya Breeze Profile

☒ CM Endpoint Profile

System

Profile Type

Use Existing Endpoints

☐

Extension

Endpoint Editor

Template

Set Type

7. Kmedia Configuration

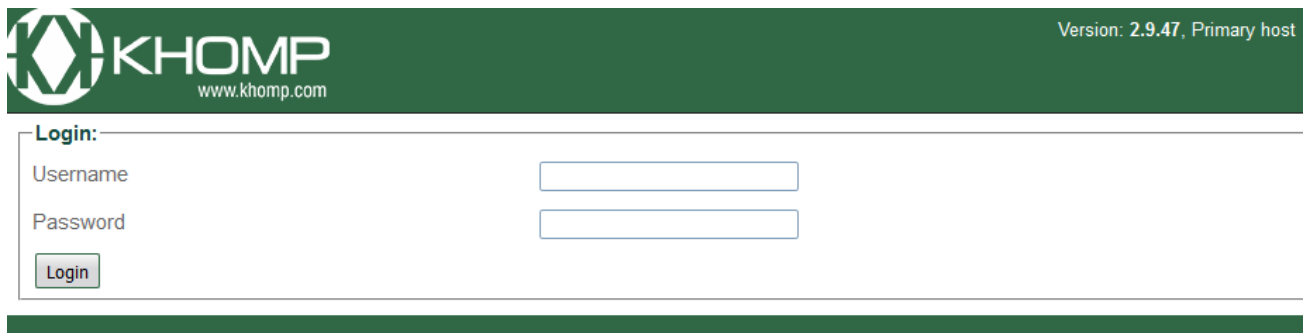
This section describes the configuration for enabling the Kmedia to interoperate with Session Manager.

7.1. Log Into Kmedia

The configuration of the Kmedia Gateway is done via a Web browser. To access the device, enter the **IP address** of the Kmedia in the **Address** field of the web browser. The IP address was provisioned during initial installation.


Login credentials

The following window will appear. Log in with the proper credentials.



The screenshot shows the login interface for KHOMP. The header bar is dark green and contains the KHOMP logo and website URL (www.khomp.com) on the left, and the version information (Version: 2.9.47, Primary host) on the right. Below the header, there is a white login form. The form has a 'Login:' label, followed by 'Username' and 'Password' labels, each with a corresponding text input field. A 'Login' button is located at the bottom left of the form.

Once logged in the following home page is displayed.

**KHOMP**
www.khomp.com

Version: 2.9.47, Primary host
Logged as root | Logout

Welcome

- Status
- Backups
- System
- Configurations

Avaya_20160906 ▾

- Hardware Units
- IP Interfaces
- TB017495 ▾**
 - TDM Line Interfaces
 - TDM Signaling**
 - ISDN
 - CAS
 - MTP2
 - Sigtran
 - SCTP
 - M2PA
 - M2UA
 - IUA
 - SS7**
 - Point Codes
 - MTP3
 - M3UA
 - ISUP
 - SCCP
 - TCAP
 - SIP
 - Clocking
 - Profiles
 - NAPs
 - Advanced Networking

Main

Welcome to Khomp' Toolpack™ Web Portal

You are connected to the **Primary** host of this Toolpack system

System

Info	
Name	system_1
System Date	2016-09-09 13:00:05
Up Time	11m 22s
Boot Time	September 09 2016, 12:48:43
Package	Running from package '2.9.47'

Call legs	Current	Highest	Cumulative
Answered	0 (0/s)	0	0
Total	0 (0/s)	0	0

Configuration

Name	Is active	Validation status	Validation status desc
Avaya_20160906	Yes	Successful	TB017495.gateway: Success TB017495.logtrace: Success TB017495.stream_server: Success TB017495.tbcam_app: Success TB017495.tbctwriter: Success TB017495.toolpack_engine: Success TB017495.toolpack_sys_mgr: Success TB017495.web_server: Success

Database toolpack_2_9 (v 0.564.0)

7.2. Configure NAP

To configure a NAP for Session Manager, navigate to **Configuration → NAPs → Create New NAP**.

- Type in a desired name in **Name**
- Type in the Session Managers' SM100 IP Address and Port in **Proxy Address** and **Proxy Port**.
- Set **Proxy Port** to **TCP**

Once done select **Save** to save changes.

Similarly, based on the E1 carrier add a NAP for PSTN (not shown).

KxHOMP www.khomp.com Version: 2.9.47, Primary host Logged as root | Logout

Welcome

- Status
- Backups
- System
- Configurations
 - Avaya_20160906
 - Hardware Units
 - IP Interfaces
 - TB017495
 - TDM Line Interfaces
 - TDM Signaling
 - ISDN
 - CAS
 - MTP2
 - Sigtran
 - SCTP
 - M2PA
 - M2UA
 - IUA
 - SS7
 - Point Codes
 - MTP3
 - M3UA
 - ISUP
 - SCCP
 - TCAP
 - SIP
 - Clocking

Configuration **Status**

[List](#)

Editing NAP:

Name: AVAYA_SM

Default Profile: default

Proxy address: 10.64.110.13

Proxy port type: TCP

Proxy port: 5060

Poll Remote Proxy? ☒

[Filtering Parameters](#)

[Registration Parameters](#)

[Authentication Parameters](#)

[Network Address Translation \(NAT\)](#)

[SIP-I Parameters](#)

[Advanced Parameters](#)

Save

7.3. Configure Route

To add a route, navigate to **Configuration → Gateway → Routes**. Select **Create New Static Route** to add a new route.

Version: 2.9.47, Primary host
Logged as root | Logout

Welcome

- Status
- Backups
- System
- Configurations
 - Avaya_20160906
 - Hardware Units
 - IP Interfaces
 - TB017495
 - TDM Line Interfaces
 - TDM Signaling
 - ISDN
 - CAS
 - MTP2
 - Sigtran

Configuration

Listing Routes:

List static routes only ☐

[Create New Static Route](#)
[Create New Route Column](#)

Name	Routeset	Incoming Attributes	Outgoing Attributes	Actions			
Name	Name	Called	NAP	Remapped Called	Remapped NAP	Remapped Profile	
PSTN --> SM			PSTN		AVAYA_SM		Delete
SM --> PSTN			AVAYA_SM	/*(*)\$/9/1/	PSTN		Delete

The following screen capture shows the route that was added to route call from PSTN to Session Manager.

Version: 2.9.47, Primary host
Logged as root | Logout

Welcome

- Status
- Backups
- System
- Configurations
 - Avaya_20160906
 - Hardware Units
 - IP Interfaces
 - TB017495
 - TDM Line Interfaces
 - TDM Signaling
 - ISDN
 - CAS
 - MTP2
 - Sigtran
 - SCTP
 - M2PA
 - M2UA
 - IUA
 - SS7
 - Point Codes
 - MTP3
 - M3UA
 - ISUP
 - SCCP
 - TRAP

Configuration

[List](#)

Editing Route:

Name: PSTN --> SM

Routeset Name:

Called: [Help](#)

Calling: [Help](#)

NAP: PSTN

Remapped Called: [Help](#)

Remapped Calling: [Help](#)

Remapped NAP: AVAYA_SM


Source call leg remapped Profile: (same as NAP)

Destination call leg remapped Profile: (same as NAP)

[Custom Parameters](#)

[Save](#)

The following screen capture shows the route that was added to route calls from Session Manager to PSTN.

 **KHOMP**
www.khomp.com

Version: 2.9.47, Primary host
Logged as root | Logout

Welcome

- Status
- Backups
- System
- Configurations
 - Avaya_20160906**
 - Hardware Units
 - IP Interfaces
 - TB017495**
 - TDM Line Interfaces
 - TDM Signaling
 - ISDN
 - CAS
 - MTP2
 - Sigtran
 - SCTP
 - M2PA
 - M2UA
 - IUA
 - SS7
 - Point Codes
 - MTP3
 - M3UA
 - ISUP
 - SCCP
 - TCAP

Configuration

[List](#)
Editing Route:

Name	SM --> PSTN
Routeset Name	
Called	<input type="text"/> Help
Calling	<input type="text"/> Help
NAP	AVAYA_SM
Remapped Called	/^(.*)\$/9\1/ Help
Remapped Calling	/^(.*)\$/\1/ Help
Remapped NAP	PSTN
Source call leg remapped Profile	(same as NAP)
Destination call leg remapped Profile	(same as NAP)

Custom Parameters

Save

7.4. Configure Profile

To configure a profile, navigate to **Configuration → Profiles**. During the compliance test, **default** profile was used. Profile is used to configure audio parameters. Select **Edit** to configure audio parameters.

The screenshot shows the KxHOMP web interface. The top header is green with the KxHOMP logo and website URL on the left, and version information and user status on the right. A left sidebar contains a 'Welcome' section and a tree of configuration options. The main content area is titled 'Profiles' and shows the 'Editing Profile' form for the 'default' profile. The form includes a 'Name' field, a 'VOIP' section with an 'SDP' sub-section containing a text area for the 'Profile SDP Description', and a checkbox for 'Force FAX tones as telephony-event'.

Version: 2.9.47, Primary host
Logged as root | Logout

Welcome

- Status
- Backups
- System
- Configurations
 - Avaya_20160906
 - Hardware Units
 - IP Interfaces
 - TB017495
 - TDM Line Interfaces
 - TDM Signaling
 - ISDN
 - CAS
 - MTP2
 - Sigtran
 - SCTP
 - M2PA
 - M2UA
 - IUA

SS7

Profiles

[List](#)

Editing Profile:

Name: default

VOIP

SDP

Profile SDP Description

```
m=audio 0 RTP/AVP 8 0 18 9 101
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15,32-36
```

Force FAX tones as telephony-event ☐

8. Verification Steps

This section provides the verification steps that may be performed to verify the configuration.

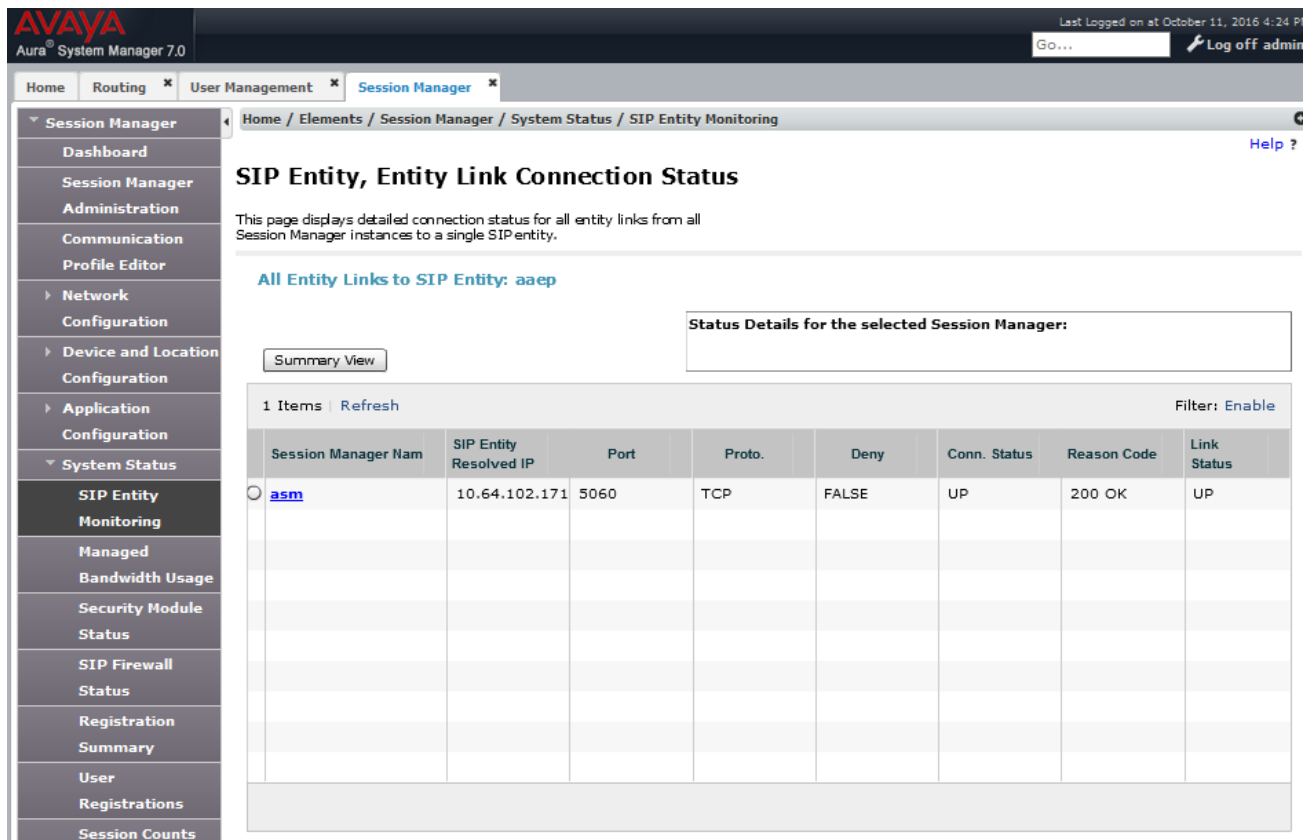
8.1. Verify Avaya Aura® Communication Manager Trunk Status

On Communication Manager, ensure that all the signalling groups are in service by issuing the command status **signalling-group n** where **n** is the signalling group number.

```
status signaling-group 1
                        STATUS
SIGNALING GROUP
    Group ID: 1
    Group Type: sip
    Group State: in-service
```

8.2. SIP Monitoring on Avaya Aura® Session Manager

From System Manager's Home screen, navigate to **Elements → Session Manager → System Status → SIP Entity Monitoring**. Verify that none of the links to the defined SIP entities are down, indicating that they are all reachable for call routing. The screen below shows the link status between Session Manager and the Kmedia.



AVAYA
Aura® System Manager 7.0

Last Logged on at October 11, 2016 4:24 PM
Go... Log off admin

Home Routing * User Management * Session Manager *

Session Manager
Dashboard
Session Manager Administration
Communication Profile Editor
Network Configuration
Device and Location Configuration
Application Configuration
System Status
SIP Entity Monitoring
Managed Bandwidth Usage
Security Module Status
SIP Firewall Status
Registration Summary
User Registrations
Session Counts

Home / Elements / Session Manager / System Status / SIP Entity Monitoring

SIP Entity, Entity Link Connection Status

This page displays detailed connection status for all entity links from all Session Manager instances to a single SIP entity.

All Entity Links to SIP Entity: aaep

Summary View

Status Details for the selected Session Manager:

1 Items | Refresh Filter: Enable

Session Manager Nam	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
<input type="radio"/> asm	10.64.102.171	5060	TCP	FALSE	UP	200 OK	UP

8.3. Kmedia Web Interface to Observe Status

To view the status of the SIP trunk between Kmedia and Session Manager, navigate to **Status** → **Nap**. Select the NAP that was added for Session Manager from the **value** column.

The screenshot shows the Kmedia web interface. On the left is a navigation tree with categories like TDM Line Interfaces, TDM Signaling, Sigtran, and SS7. The 'Sigtran' category is expanded, and 'Nap' is selected. The main content area displays the 'Naps status' for the selected interface 'TB017495'. It includes a table with the following data:

name	value
Available nap cnt	1
Partially available nap cnt	0
Unavailable nap cnt	1
Available nap list	AVAYA_SM
Unavailable nap list	PSTN

The NAP added for Session Manager shows 100% Availability.

The screenshot shows the Kmedia web interface with the 'Status' tab selected. The 'Network Access Point Status' section displays a table with the following data:

Name	Type	Availability %	Available Count	Unavailable Count	In ASR % (24h)	Out ASR % (24h)	Usage %	Shared usage %	In calls
AVAYA_SM	SIP	100	512	0	0	0	0	0	0
PSTN	ISDN	0	0	23	0	0	0	0	0

9. Conclusion

These Application Notes describe the procedures required to configure the Kmedia Gateway to interoperate with Avaya Aura® Session Manager and Avaya Aura® Communication Manager. The Kmedia Gateway successfully passed compliance testing.

10. Additional References

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

- [1] *Administering Avaya Aura® Communication Manager*, Document 03-300509
- [2] *Administering Avaya Aura® Session Manager*, Document 03-603324
- [3] Kmedia Manual

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

Product documentation for Khomp products may be found at <http://www.khomp.com>.

©2016 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.