

Avaya Solution & Interoperability Test Lab

Application Notes for Prism-IPX Systems PriMega Messaging Gateway with Avaya Aura® Communication Manager and Avaya Aura® Session Manager - Issue 1.0

Abstract

These Application Notes describe the configuration steps required for PriMega Messaging Gateway to interoperate with Avaya Aura® Communication Manager and Avaya Aura® Session Manager.

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 outline the steps necessary to configure PriMega Messaging Gateway from Prism-IPX Systems to interoperate with Avaya Aura® Communication Manager (Communication Manager) and Avaya Aura® Session Manager (Session Manager). PriMega Messaging Gateway (hereafter referred to as PriMega) is a server-based application running on Linux platform. PriMega SIP User Agent Interfaces for Linux platforms. Interfaces are used for allowing callers to enter numeric digits for sending to pagers on PriMega platform.

PriMega connects to Communication Manager using a SIP trunk via the Session Manager. PriMega is supplied with all prerequisite software. Communication Manager also connects to PriMega when it is being used as a Paging adjunct for Meet-Me Paging features by initiating a TCP/IP connection. In this case PriMega sends TAP (Telocator Alphanumeric Protocol) messages which is an outbound protocol to pagers on the PSTN.

2. General Test Approach and Test Results

The general test approach was to configure a simulated enterprise voice network using Communication Manager. PriMega communicates with Communication Manager using a SIP trunk through the Session Manager. See **Figure 1** for a network diagram. A dial plan was configured on the Communication Manager to route calls to PriMega. Calls are placed to PriMega and the digits required to be sent to the pager by PriMega are entered by the caller after which PriMega automatically disconnects the call.

For the Meet-Me Paging feature, SA8312 is enabled in Communication Manager which allows a Page Line (station that is administered with the Paging station type) to interface (using TCP/IP) with paging equipment, in this case PriMega. When a Page Line is called, MultiVantage sends a TAP formatted paging message (described in document mentioned in **Section 10**) to the PriMega Paging Adjunct, which in turn, alerts the pager associated with the called page line.

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 these DevConnect Application Notes included the enablement of supported encryption capabilities in the Avaya products. Readers should consult the appropriate Avaya product documentation for further information regarding security and encryption capabilities supported by those Avaya products.

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

For the testing associated with these Application Notes, the interface between Avaya systems and PriMega did not include use of any specific encryption features as requested by Prism-IPX Systems.

2.1. Interoperability Compliance Testing

The interoperability compliance testing included feature and serviceability testing. The serviceability testing introduced failure scenarios to see if PriMega could resume after a link failure with Communication Manager/Session Manager. The testing included:

- Call PriMega using both internal and external users.
- Detection and confirmation by PriMega of digits entered by users.
- Termination of calls by PriMega after receiving digits from users.
- Termination of calls by PriMega if there is no activity by user within the configured time limit.
- Multiple simultaneous calls to PriMega.
- Internal and external users call the paging station and PriMega detects and acknowledges the same using the Meet-Me Paging feature.

2.2. Test Results

Tests were performed to insure full interoperability between PriMega and Communication Manager via Session Manager. The tests were all functional in nature and performance testing was not included. All test cases passed successfully.

2.3. Support

For technical support for Prism-IPX Systems products, please use the following web link. <u>https://prism-ipx.com/</u>.

Prism-IPX Systems can also be contacted as follows: Phone: +1 678 242 5266 Fax: +1 678 242 5201 Web: <u>https://prism-ipx.com/contact-us/</u> Email: prism-harktech_support@prism-ipx.com

3. Reference Configuration

Figure 1 illustrates the network topology used during compliance testing. The Avaya solution consists of a Communication Manager, which has a SIP Trunk connection to PriMega Messaging Gateway via the Session Manager. SIP and H.323 stations were configured on the Communication Manager to generate outbound calls to PriMega. For PSTN users calling PriMega, both PRI and SIP trunks were configured. For the Meet-Me Paging feature SA8312, connection between Communication Manager and PriMega is accomplished via TCP/IP.



PriMega was installed on a Linux OS platform.

Figure 1: Avaya and PriMega Reference Configuration

4. Equipment and Software Validated

The following equipment and version were used in the reference configuration described above:

Equipment/Software	Release/Version
Avaya Aura® Communication Manager	7.1.3.0.0-FP3
running on virtualized environment	
Avaya Aura® Session Manager running on	7.1.3.0.713014
virtualized environment	
Avaya Aura® System Manager running on	7.1.3.0
virtualized environment	
Avaya Aura® Media Server	7.8.0.384
Avaya G450 Media Gateway	39.12.0/1
Avaya IP Deskphones:	
• 9611G (H.323)	6.6401
• 4610 (H.323)	2.800
• 9641GS (SIP)	7.0.1.2.9
Avaya 9404 Digital Deskphone	18.0
Avaya Analog Deskphone	N/A
PriMega Messaging Gateway running on Linux	V9
OS	
PriMega Linux OS	Centos 7.4

5. Configure Avaya Aura® Communication Manager

Configuration and verification operations on the Communication Manager illustrated in this section were all performed using Avaya Site Administrator Emulation Mode. 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: (Note: During Compliance Testing all inputs not highlighted in Bold were left as Default)

- 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 dial plan
- Administer uniform dial plan
- Administer AAR analysis
- Enable special application 8312
- Configure node names
- Configure IP services
- Configure paging station type

5.1. Verify License

Log in to the System Access Terminal to verify that the Communication Manager license has proper permissions for features illustrated in these Application Notes. Use the "display systemparameters 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:	12000	10		
Maximum Concurrently Registered IP Stations:	18000	5		
Maximum Administered Remote Office Trunks:	12000	0		
Maximum Concurrently Registered Remote Office Stations:	18000	0		
Maximum Concurrently Registered IP eCons:	414	0		
Max Concur Registered Unauthenticated H.323 Stations:	100	0		
Maximum Video Capable Stations:	41000	0		
Maximum Video Capable IP Softphones:	18000	1		
Maximum Administered SIP Trunks:	24000	34		

5.2. Administer SIP Trunk Group

Use the "add trunk-group n" command, where "n" is an available trunk group number, in this case "1". Enter the following values for the specified fields and retain the default values for the remaining fields.

- Group Type: Enter "sip".
 Group Name: Enter a descriptive name.
 TAC: Enter an available trunk access code.
- Service Type: Enter "tie".

add trunk-group 1		Page 1 of 22
	TRUNK GROUP	
Group Number: 1	Group Type: sip	CDR Reports: y
Group Name: Trunk to SM or	COR: 1	TN: 1 TAC: #001
Direction: two-way	Outgoing Display? y	
Dial Access? n	Nigh	nt Service:
Queue Length: 0		
Service Type: tie	Auth Code? n	
	Member A	Assignment Method: auto
		Signaling Group: 1
	Ν	Number of Members: 24

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

display trunk-group 1 TRUNK FEATURES	Page 3 of 22
ACA Assignment? n Mea	asured: internal Maintenance Tests? v
Suppress # Outpuising? n Numbering For	mat: private
	UUI Treatment: shared
	Maximum Size of UUI Contents: 128
	Poplaco Postrictod Numbers? n
	Replace Restlicted Numbers: II
	Replace Unavailable Numbers? n
	Hold/Unhold Notifications? W
	Hold/official Notifications? y
Modify Tar	idem Calling Number: no
Send UCID? y	
Show ANSWERED BY on Display? y	
DSN Term? N	

5.3. Administer SIP Signaling Group

Use the "add signaling-group n" command, where "n" is an available signaling group number, in this case "1". Enter the following values for the specified fields and retain the default values for the remaining fields.

• Group Type:	Enter "sip".
Transport Method:	Enter "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 in Near-end Listen Port.
 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?:	Enter "y".

• Initial IP-IP Direct Media?:

Enter "y". Enter "y".

add at was lines as a second		Dama 1 af 2	
add signaling-group i		Page 1 01 Z	
	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? y	7
Peer Detection Enable	d? y Peer Server:	SM	
Prepend '+' to Outgoin	g Calling/Alerting,	/Diverting/Connected Public Numbers? y	7
Remove '+' from Incomin	g Called/Calling/Al	lerting/Diverting/Connected Numbers? r	1
Alert Incoming SIP Cris	is Calls? n		
Near-end Node Name:	procr	Far-end Node Name: SM-VM	
Near-end Node Name: Near-end Listen Port:	procr 5061	Far-end Node Name: SM-VM Far-end Listen Port: 5061	
Near-end Node Name: Near-end Listen Port:	procr 5061 Fa	Far-end Node Name: SM-VM Far-end Listen Port: 5061 ar-end Network Region: 1	
Near-end Node Name: Near-end Listen Port:	procr 5061 Fa	Far-end Node Name: SM-VM Far-end Listen Port: 5061 ar-end Network Region: 1	
Near-end Node Name: Near-end Listen Port: Far-end Domain: bvwdev.	procr 5061 Fa	Far-end Node Name: SM-VM Far-end Listen Port: 5061 ar-end Network Region: 1	
Near-end Node Name: ; Near-end Listen Port: Far-end Domain: bvwdev.	procr 5061 Fa	Far-end Node Name: SM-VM Far-end Listen Port: 5061 ar-end Network Region: 1 Bypass If IP Threshold Exceeded? r	1
Near-end Node Name: ; Near-end Listen Port: Far-end Domain: bvwdev. Incoming Dialog Loopbac	procr 5061 Fa com ks: eliminate	Far-end Node Name: SM-VM Far-end Listen Port: 5061 ar-end Network Region: 1 Bypass If IP Threshold Exceeded? r RFC 3389 Comfort Noise? r	1
Near-end Node Name: Near-end Listen Port: Far-end Domain: bvwdev. Incoming Dialog Loopbac DTMF over IP:	procr 5061 Fa com ks: eliminate rtp-payload	Far-end Node Name: SM-VM Far-end Listen Port: 5061 ar-end Network Region: 1 Bypass If IP Threshold Exceeded? r RFC 3389 Comfort Noise? r Direct IP-IP Audio Connections? y	1
Near-end Node Name: Near-end Listen Port: Far-end Domain: bvwdev. Incoming Dialog Loopbac DTMF over IP: Session Establishment T	procr 5061 Fa com ks: eliminate rtp-payload imer(min): 3	Far-end Node Name: SM-VM Far-end Listen Port: 5061 ar-end Network Region: 1 Bypass If IP Threshold Exceeded? r RFC 3389 Comfort Noise? r Direct IP-IP Audio Connections? y IP Audio Hairpinning? y	1 1 7
Near-end Node Name: Near-end Listen Port: Far-end Domain: bvwdev. Incoming Dialog Loopbac DTMF over IP: Session Establishment T Enable Layer 3	procr 5061 Fa com ks: eliminate rtp-payload imer(min): 3 Test? y	Far-end Node Name: SM-VM Far-end Listen Port: 5061 ar-end Network Region: 1 Bypass If IP Threshold Exceeded? r RFC 3389 Comfort Noise? r Direct IP-IP Audio Connections? y IP Audio Hairpinning? y Initial IP-IP Direct Media? y	1 1 7
Near-end Node Name: Near-end Listen Port: Far-end Domain: bvwdev. Incoming Dialog Loopbac DTMF over IP: Session Establishment T Enable Layer 3 H.323 Station Outgoing	procr 5061 Fa com ks: eliminate rtp-payload imer(min): 3 Test? y Direct Media? n	Far-end Node Name: SM-VM Far-end Listen Port: 5061 ar-end Network Region: 1 Bypass If IP Threshold Exceeded? r RFC 3389 Comfort Noise? r Direct IP-IP Audio Connections? y IP Audio Hairpinning? y Initial IP-IP Direct Media? y Alternate Route Timer(sec): 6	1 1 7 7

5.4. Administer SIP Trunk Group Members

Use the "change trunk-group n" command, where "n" is the trunk group number from **Section 5.22**. 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 5.33**.
- Number of Members: The desired number of members, in this case "24".

change trunk-o	group 1			Page	1 of 22	
	5	TRUNK GROUP		5		
Group Number:	1	Group Typ	e: sip	CDR Rep	orts: y	
Group Name:	Trunk to SM on	VM CO	R: 1	TN: 1	TAC: #001	
Direction:	two-way	Outgoing Displa	у? у			
Dial Access?	n		Night	Service:		
Queue Length:	0					
Service Type:	tie	Auth Cod	le? n			
			Member As	signment Meth	od: auto	
				Signaling Gro	up: 1	
			Nu	mber of Membe	rs: 24	

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 5.33**.

For Authoritative Domain, enter the applicable domain for the network. 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 PriMega.

```
change ip-network-region 1
                                                                  Page 1 of 20
                                IP NETWORK REGION
Region: 1 NR Group: 1
Location: 1 Authoritative Domain: bvwdev.com
   Name: Region1
                                Stub Network Region: n
MEDIA PARAMETERS
Codec Set: 1
                                Intra-region IP-IP Direct Audio: yes
                                Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 2048
                                            IP Audio Hairpinning? y
   UDP Port Max: 8001
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	4 of	20
Source Region: 1 Inter Network Region Connection Management		I	7	M
		G	А	τ
dst codec direct WAN-BW-limits Video Intervening	Dyn	А	G	С
rgn set WAN Units Total Norm Prio Shr Regions	CAC	R	L	е
1 1		ć	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 5.55**. Update the audio codec types in the **Audio Codec** fields as necessary. The codec shown below was used in the compliance testing.

```
display ip-codec-set 1
                                                                             Page
                                                                                     1 of
                                                                                             2
                               IP MEDIA PARAMETERS
    Codec Set: 1
Audio<br/>CodecSilence<br/>SuppressionFrames<br/>Per PktPacket<br/>Size(ms)1: G.711MUn2202: G.711An2203: G.729n220
                        n 2
3: G.729
                                              20
 4:
 5:
 6:
 7:
     Media Encryption
                                               Encrypted SRTCP: enforce-unenc-srtcp
 1: 1-srtp-aescm128-hmac80
 2: 2-srtp-aescm128-hmac32
 3: none
```

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 PriMega, 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 5.2**.
- **FRL:** A level that allows access to this trunk, with 0 being least restrictive.

change route-pattern 1 Page 1 of З Pattern Name: To SM on VM Pattern Number: 1 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 Ō n user 2: n user user 3: n 4: user n 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 lev0-pvt none 1: yyyyyn n rest

5.8. Administer Dial Plan

This section provides a sample dial plan used for routing calls with dialed digits 71xxx to PriMega. Use the "change dialplan analysis 0" command and add an entry to specify the use of digits pattern 71, as shown below.

```
change dialplan analysis

DIAL PLAN ANALYSIS TABLE

Location: all Percent Full: 2

Dialed Total Call

String Length Type

1 4 ext

71 5 udp
```

5.9. Administer Uniform Dial Plan

This section provides a sample AAR routing used for routing calls with dialed digits 71xxx to PriMega. 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 71xxx, as shown below.

```
change uniform-dialplan 0

UNIFORM DIAL PLAN TABLE

Matching Insert Node

Pattern Len Del Digits Net Conv Num

71 5 0 aar n
```

5.10. Administer AAR Analysis

Use the "change aar analysis 0" command and add an entry to specify how to route calls to 71xxx. In the example shown below, calls with digits 71xxx will be routed as an AAR call using route pattern "1" from **Section 5.77**.

change aar analysis O				Page 1 of 2
	AAR D	IGIT ANALYS	SIS TABLE	
		Location:	all	Percent Full: 2
Dialed	Total	Route	Call Node	ANI
String	Min Max	Pattern	Type Num	Reqd
71	5	5 1	aar	n

5.11. Enable Special Applications 8312

For the Meet-Me Paging feature to be activated the Special Applications 8312 (SA8312) needs to be enabled. To enable this feature, use the "change system-parameters special-applications" command and in **Page 3**, enable the (SA8312) - Meet-Me Paging? by entering "y" as shown below.

5.12. Configure Node Names

Prior to administering PAGEx Service type, the user would have to administer all the relevant node names and their respective IP addresses by using the "change node-names ip" command. During compliance testing since PAGE1 and PAGE2 were configured, two node-names pointing to the same hardware, in this case PriMega was configured as shown below. Also, the node name for the Communication Manager is shown below. All these node names configured will be used in the next **Section 5.13**. Run the command "change node-names ip" and enter the following:

- Name: Enter descriptive names. For PriMega "PrismIPX1" and "PrismIPX2" were configured. For Communication Manager "procr" was configured.
- IP Address: Enter the IP Address of PriMega and Communication Manager.

change node-names	ip			Page	1 of	2	
		IP NODE	NAMES				
Name	IP Address						
PrismIPX1	10.10.98.72						
PrismIPX2	10.10.98.72						
procr	10.10.97.222						

5.13. Configure IP Services

The "change ip-services" command is to administer typical asynchronous adjuncts, e.g., PMS, CDR etc., that MultiVantage supports. The paging adjunct is in the same category of such adjuncts.

The PAGE1 and PAGE2 are considered as two separate page links when communicating with the paging adjunct. There is no priority indication when the links are assigned as PAGE1 or PAGE2. It is not required that both PAGE1 and PAGE2 are administered in the system however during compliance testing both were used. Run the "change ip-services" command and configure the following:

- Service Type: Enter "PAGE1" and "PAGE2".
- Enabled: Enter "y".
- Local Node: Enter "procr" which is the node name for Communication Manager as explained in Section 5.12.
- **Remote Node:** Enter "PrismIPX1" and "PrismIPX2" which is the node name for PriMega as explained in **Section 5.12**.
- **Remote Port:** During compliance testing "10004" and "20004" were used.

change ip-s	services				Page	1 of	4	
			IP SERVICE	S				
Service	Enabled	Local	Local	Remote	Remote			
Туре		Node	Port	Node	Port			
PAGE1	y :	procr	0	PrismIPX1	10004			
PAGE2	y :	procr	0	PrismIPX2	20004			

5.14. Configure Paging Station Type

SA8312 will support the page line through a station type - "PAGING", in the station administration. When the station is administered as "PAGING" type, the port field will become a display only field with the value of 'X' displayed, i.e., administered without hardware (AWOH). The new station type keyword "PAGING" is displayed regardless whether the system "MeetMe Paging" option is enabled or not.

The PAGING station type is administrable only when the "Meet-Me Page" system option is enabled. However, SA8312 will not require the stations with "PAGING" type to be removed before the Meet-Me Paging (MMP) option can be disabled. To add this station type, run the "add station x" command, where "x" is an available extension and configure the following:

- Type: Enter "PAGING".
- Name: Enter a
 Sond MMP Mossage: Ensure

Enter a descriptive name. Ensure that this is set to "y".

• Send MMP Message:

add station 56503 Page 1 of 4 STATION Lock Messages? n Security Code: Coverage Path 1: Coverage Path 2: Hunt-to Station: Extension: 56503 BCC: 0 Type: PAGING TN: 1 COR: 1 Port: X Name: 56503, PrismIPX COS: 1 Tests? n STATION OPTIONS Time of Day Lock Table: Loss Group: 1 Message Waiting Indicator: none Off Premises Station? n Survivable COR: internal Survivable Trunk Dest? y Send MMP Message: y

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.

Recommended access to System Manager is via FODN	
Co to control login for Single Sign On	
	User ID:
If IP address access is your only option, then note that authentication will fail in the following cases:	Password:
 First time login with "admin" account Expired/Reset passwords 	Log On Cancel
Use the "Change Password" hyperlink on this page to change the password manually, and then login.	Change Password

6.2. Administer Domain

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

AVAYA Aura [®] System Manager 7. I	Configuratio*
Home Routing ×	
Routing	Home / Elements / Routing / Domains
Domains	Introduction to Notwork Douting Doligy
Locations	Introduction to Network Routing Policy

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**.

	Configuratio ×			Last Logged on at July 30
Home Routing ×			0	Go
▼ Routing	Home / Elements / Routing / D	omains		
Domains				Help ?
Locations	Domain Manageme	ent		Commit Cancel
Adaptations				
SIP Entities				
Entity Links	1 Item 🖓			Filter: Enable
Time Ranges	Name	Туре	Notes	
Routing Policies	* bvwdev.com	sip 🗸	Primary Domain	

6.3. Administer Locations

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

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.

AVAVA			Last Logged on at July (
Aura [®] System Manager 7. I	Configuratio*		Go
Home Routing X		Ð	00
Routing	Home / Elements / Routing / Location	15	
Domains			Help ?
Locations	Location Details		Commit Cancel
Adaptations	General		
SIP Entities	* Name	Della: ille	
Entity Links	Name:	Belleville	
Time Ranges	Notes:	Belleville DevConnect Lab	

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. Retain the default values in the remaining fields.

4 Items 🛛 😂			Filter: Enable
IP Address Pattern	*	Notes	
* 10.10.5.*			
* 10.10.97.*			
* 10.10.98.*			
*			
Select : All, None			

6.4. Administer Adaptation

During compliance test, to make the call from Communication Manager via Session Manager to PriMega, adaptation to translate IP address into domain name is used for PriMega SIP entity. Here is step on how to create Adaptation. 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 PriMega Adaptation.

- Adaptation Name An informative name (e.g.," For_Prism").
- 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,
	ex: "bvwdev.com"
iosrcd	Enter the domain name of system,
	ex: "bvwdev.com"
odstd	Enter IP address of PriMega, ex:
	"10.10.98.72"
osrcd	Enter IP Address of Session
	Manager, ex: "10.10.97.228"

Once the correct information is entered click the **Commit** button.

Here is the screenshot show Adaptation created for PriMega.

Aura [®] System Manager 7.1 C Configuratio	Last Logged on at July
Routing Home / Ele Domains Adapta Locations Adapta	ements / Routing / Adaptations Help ? ation Details Commit Cancel
Adaptations SIP Entities Entity Links Time Ranges Routing Policies Dial Patterns Reputar Expressions	* Adaptation Name: For_Prism DigitConversionAdapter v Name-Value Parameter v
Defaults	Add Remove Name Value
	fromto true
	iodstd bywdey.com
	iosrcd byggey.com
	Select : All, None II 4 4 Page 1 of 2 🕨

(Continue) the screenshot show Adaptation created for PriMega:

AVAVA		Last Logged on at July
Aura [®] System Manager 7. I	Configuratio*	Go
Home Routing *		
▼ Routing	Home / Elements / Routing / Adaptations	
Domains	Adambakian Dabaila	Help ?
Locations	Adaptation Details	Commit Cancel
Adaptations	General	
SIP Entities	* Adaptation Name: For Prism	
Entity Links	* Modulo	
Time Ranges	Name: DigitConversionAdapter v	
Routing Policies	Module	
Dial Patterns	Type:	
Regular Expressions		
Defaults	Add Remove	
	Name Value	
	odstd 10.10.98.72	
	osrcd 10.10.97.228	
	Select : All, None	4 Page 2 of 2 ▶

6.5. Administer SIP Entity for PriMega

Add a new SIP entity for PriMega. Select **Routing** \rightarrow **SIP Entities** from the left pane and click **New** in the subsequent screen (not shown) to add a new SIP entity for PriMega.

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 the PriMega server.
- **Type:** Select "Other" from the drop-down menu.
- Notes: Any desired notes.
- Adaptation: Select he adaptation configured in Section 6.4
- Location: Select the PriMega location name from Section 6.3.
- **Time Zone:** Select the applicable time zone.
- SIP Link Monitoring: Select "Link Monitoring Disabled" from the drop-down menu.

AVAVA				Last Logged on at July 3
Aura [®] System Manager 7. I 💽	Configuratio*			Go
Home Routing ×			O	00
▼ Routing	Home / Elements / Routing / SIP Ent	ities		
Domains				Help ?
Locations	SIP Entity Details			Commit Cancel
Adaptations	General			
SIP Entities	* Name:	PrismIPX		
Entity Links	* FQDN or IP Address:	10.10.98.72		
Time Ranges	Туре:	Other 🗸		
Routing Policies	Notes:	SIP trunk for PrismIPX		
Dial Patterns				
Regular Expressions	Adaptation:	For_Prism ~		
Defaults	Location:	Belleville 🗸		
	Time Zone:	America/Fortaleza	~	
	* SIP Timer B/F (in seconds):	4		
	Use Global Setting 🗸			
	Credential name:			
	Securable:			
	Call Detail Recording:	none 🗸		
	CommProfile Type Preference:			
	Loop Detection			
	Loop Detection Mode:	On 🗸		
	Loop Count Threshold:	5		
	Loop Detection Interval (in msec):	200		
	Monitoring			
	SIP Link Monitoring:	Link Monitoring Disabled	~	
		· · · · · · · · · · · · · · · · · · ·		

Solution & Interoperability Test Lab Application Notes ©2018 Avaya Inc. All Rights Reserved.

22 of 37 Prism_CM-SM71

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.
- The Session Manager entity name, in this case "DevvmSM". • SIP Entity 1:
- Select "UDP" and "TCP". • Protocol:
- Enter "5060". • Port:
- SIP Entity 2: The PriMega entity name configured in the beginning of this section. Enter "5060".
- Port:
- Connection Policy: Select "trusted".

Entit	Entity Links Override Port & Transport with DNS SRV:							
Add	Remove							
2 Ite	ms 🛛 🍣						Filter	r: Enable
	Name 🔺	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Deny New Service
	* DevvmSM_PrismIPX_	DevvmSM 🗸	UDP 🗸	* 5060	PrismIPX ~	* 5060	trusted \lor	
	* PrismIPX_PrismIPX_5	DevvmSM 🗸	TCP 🗸	* 5060	PrismIPX v	* 5060	trusted 🗸	
Selec	t : All, None							

6.6. Administer Routing Policies

A new routing policy is to be added for calls to reach PriMega from the Communication Manager.

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

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

In the **SIP Entity as Destination** sub-section, click **Select** and select the PriMega entity name from **Section 6.5**. The screen below shows the result of the selection.

AVAYA						Last Logged on at July
Aura [®] System Manager 7. I	Configuratio*	_	_	_		Go
Home Routing ×						
Routing	Home / Elements	/ Routing / Routing	Policies			
Domains	. _					Help ?
Locations	Routing Po	licy Details				Commit Cancel
Adaptations	General					
SIP Entities	General	* Namo:	Route To Drigg	aIDV		
Entity Links		Disable de		шРХ		
Time Ranges		Disabled:				
Routing Policies	* Retries: 0					
Dial Patterns		Notes:	Routing to Pris	mIPX		
Regular Expressions	SIP Entity as	Destination				
Defaults	Colort	Destinution				
	Select			-		
	Name	FQDN or IP Addres	is	Туре	Notes	
	PrismIPX	10.10.98.72		Other	SIP trunk for PrismIP	X

6.7. Administer Dial Patterns

Add a new dial pattern for PriMega by navigating to **Routing** \rightarrow **Dial Patterns** from the left pane and click **New** in the subsequent screen (not shown) to add a new dial pattern to reach PriMega. 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 "71".
- 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 5.33**.

In the **Originating Locations and Routing Policies** sub-section, click **Add** and create an entry for reaching PriMega. In the compliance testing, the entry allowed for call originations from all Communication Manager endpoints in locations "Belleville" is selected under **Originating Location Name**. The PriMega routing policy from **Section 6.6** was selected under **Routing Policy Name** as shown below.

AVAVA			Last Logged on at July 30,
Aura [®] System Manager 7. I	onfiguratio*		Go
Home Routing *		v	a ta
▼ Routing ◀	Home / Elements / Routing / Dial Patterns		
Domains			Help ?
Locations	Dial Pattern Details		Commit Cancel
Adaptations	General		
SIP Entities	* Dattern: 71]
Entity Links]
Time Ranges	* Min: 5		
Routing Policies	* Max: 36		
Dial Patterns	Emergency Call:		
Regular Expressions	Emergency Priority: 1		
Defaults	Emergency Type:		
	SIP Domain: bvwdev.com	\sim	
	Notes: Dialing patter	m to reach PrismIPX]
	Originating Locations and Routing Policies		
	Add Remove		
	1 Item 💝		Filter: Enable
	Originating Location Name A Originating Location Name A Notes Na	uting Policy me Rank Routing Policy Disabled	Routing Routing Policy Policy Destination Notes
	Belleville DevConnect Ro Lab	oute_To_PrismIPX 0	PrismIPX to PrismIPX
	Select : All, None		

7. Configure PriMega Messaging Gateway

PriMega Messaging Gateway is typically configured for customers by Prism-IPX Systems. For details on how to configure PriMega Messaging Gateway, contact Prism-IPX Systems by referring to **Section 2.3**. This section provides a "snapshot" of PriMega Messaging Gateway configuration used during this compliance testing. The screen shots and partial configuration shown below, supplied by Prism-IPX Systems, are provided only for reference. It does not show how to configure pagers or pager output. The PriMega software must be installed with the pika add on.

7.1. Confirm Pika configuration

Edit /etc/pika/pikagp.cfg and ensure IP address matches the IP that is going to be used on the server.

and confirm codecs:

..... codecs=g711u|g711a

7.2. Set up virthost entry in Primega

Set up a **virthost** entry for **5060** on the IP to which the Communication Manager is pointing (all fields default except Name and Host).



7.3. Change default FCOS setting

This section shows the FCOS1 setting used during the compliance testing.

FCOS 1				
Number	1			
Name	Default			
Allow login				
Allow voice messages				
Allow numeric messages				
Allow text messages				
Enable voice greeting				
Allow playing of messages marked deleted				
Play messages first-in-first-out				
Allow subscriber to keep/delete messages				
Enable overdial				
Enable clearing message with ***				
Allow subscriber to modify their recorded name				
Allow subscriber to modify their custom greeting				
Allow subscriber to change their passcode				
Numeric prompt filename	prompts/beep_1700_60_60_30.wav			
Overdial prompt filename	prompts/beep_1400_630ms.wav			
End prompt filename	prompts/beep_100_100_8.wav			
Urgent text				
Urgent function	Select One (ONLY if urgent) \vee			
Comment				
Update				

7.4. Create a SIP Input Service

This section shows the three screen shots of the SIP Input Service configured during compliance testing.

Screen below shows the configuration of the input port of 5060.

messagefilt modemtype outputgroup service servisource smppemail smppprofile smtpprofile							
tappassword tapprofile throttle thppprofile thpproute useraccess virthost wotpprofile							
Service 600							
Name	SIP input						
Port type	Network (TCP or UDP)						
	Remote TCP/IP host						
	TCP/IP port (listen or connect to)	5060					
	Socket domain	INET 🗡					
	Socket type	TCP 🗸					
	Socket bind IP (0.0.0.=any)	0.0.00					
	Socket bind port	0					
	Initial read timeout	5000					
	Secondary read timeout	500					
	Network connect timeout	0					
	IP filter	0					
	Max connections (from same IP address)	0					
	SSL Certificate	Select One 🗸					
	Minimum SSL protocol version	TLS v1.2 🗠					
	Maximum SSL protocol version	Latest supported in installed OpenSSL 🖂					
Port status		Dn-line 🗸					
Backup service	0						
Backup interval	0						
Retry count	0						
Retry interval	0						

Depends on service (typically 0)						0							
Hostname (typically empty)													
Direction						Input		~]				
		Maximum reci	ipients							50			
	Enable lookup			Subscr	iber ge ID (t	wo-		olock urce add	ress (two-	⊠ Virthost	Alias		
		Translate inco (see idma	ming ID ap)										
		Input grou	up						1	- Default	~		
	Input rate (0=don't limit)							C)				
	Duplicate detection time (in sec)						0						
	Duplicate detection message length (0=entire message)						80						
		Duplicate check	subjec	ţ									
		Use opag	le										
		Append dor	main										
Protocol						PIKA	~						
		Options											
		Profile						1 -	- Default	\sim			
	⊡Logging ⊡Locks	Functions	□ Not	used 🛛	🛛 Qu 🖾 Rei	ieues ad							
Debug level	Write Protocol Template Not used	Events Shared memory Zero read bin2str	Pro	mpts eads og used	Tel	lephony cense cssage data t used							

Screen below shows the configuration of the input section and protocol details.

Screen below shows the configuration of the debug level, send fields and logging.

	Database Pa	rse IPC	Not used			
		rbose 🗀 Very v				
Packet Size			1024 (TAP, IN	PF)		
Buffer size			16384			
Send fields	🗹 From (email add	r) 📃 From (real nam	e) 🗹 Subject 🗹 Bod	y 🔲 Wordcount 🔲 Timestamp	Recipient 🔲 MDN	
Header fields	From	Subject	Timestamp	Recipient	MDN	
Maximum message length			240			
Maximum length per page			240			
Enable auto-create						
Auto template	Select One 🗸					
Over length service			Select One	~		
Enable datamon						
Error action			Log and Noti	fy 🖂		
Log type	Both 🛩					
Log profile			2 - Telephon	у 🖌		
Outgoing source address (for SMPP or GSM SCA)			ANI			
Update						

Solution & Interoperability Test Lab Application Notes ©2018 Avaya Inc. All Rights Reserved.

7.5. Create TAP Input Services (10004 and 20004)

This section explains the two TAP input services ports 10004 and 20004 created during compliance testing. Example below only shows configuration for 10004. Similarly, port 20004 can be created.

Screen below shows the configuration of the input port.

messagefilt modemtype outputgroup service service smppemail smppprofile smtpprofile								
tappassword tapprofile throttle thppprofile thppproute useraccess virthost wctpprofile								
Service 701								
Name	TAP Input from Avaya							
Port type	Network (TCP or UDP) 🗸							
	Remote TCP/IP host							
	TCP/IP port (listen or connect to)	10004						
	Socket domain	INET 🚩						
	Socket type	TCP 🗸						
	Socket bind IP (0.0.0=any) 0.0.0.0							
	Socket bind port 0							
	Initial read timeout	30000						
	Secondary read timeout	1000						
	Network connect timeout	0						
	IP filter	0						
	Max connections (from same IP address)	0						
	SSL Certificate	Select One 🗸						
	Minimum SSL protocol version TLS v1.2 ~							
	Maximum SSL protocol version	Latest supported in installed OpenSSL 🖂						
Port status		On-line 🗸						
Backup service	0							
Backup interval	0							
Retry count	0							
Retry interval	0							

Retry count	
Retry interval	
Depends on service (typically 0)	0
Hostname (typically empty)	
Direction	Input
	Maximum recipients 10
	Enable lookup Enable lookup Message ID (two- Way) Way) Message ID (two- Way) Kenable lookup Kenable look
	Translate incoming ID (see idmap)
	Input group 1 - Default
	Input rate (0=don't limit) 0
	Duplicate detection time (in sec) 0
	Duplicate detection message length (0=entire 80
	Duplicate check subject
	Use opage
	Append domain
Protocol	
	Options Transparent Extended Disable 1.6+ Response Allow Manual DID Net Even Image: Constraint of the second sec
	Profile 1-Default V
	Password
	Logging Functions Not used Queues

Screen below shows the configuration of the input section and protocol details.

Screen below shows the configuration of the debug level, send fields and logging.

Debug level	Write Protocol Template Not used	Events Shared memory Zero read bin2str Parse	Prompts Prompts Threads Do log Not used IPC	Telephony License Message data Not used Not used				
Packet size		L. Verboac	very verb	1024 (TAP;	TNPP) ~			
Buffer size				16384				
Send fields	🔲 From (en	nail addr) 🛛 🔲 Fro	m (real name)	🗌 Subject 🗹 E	ody 🔲 Wordcount	Timestamp	Recipient	
Header fields	From	🗌 Subjec	t	Timestamp	🗌 Re	cipient	MDN	
Maximum message length	240							
Maximum length per page	240							
Enable auto-create								
Auto template		Select One 🗡						
Over length service	Select One 🗸							
Enable datamon								
Error action	Log and Notify 🛩							
Log type	Both 🗸							
Log profile	1 - Default 🗸							
Outgoing source address (for SMPP or GSM SCA)								
			Update	2				

RS; Reviewed: SPOC 9/5/2018 Solution & Interoperability Test Lab Application Notes ©2018 Avaya Inc. All Rights Reserved. 32 of 37 Prism_CM-SM71

Block 1 5 digit numbers					
Name	5 digit numbers				
Enabled					
ID start	10000				
ID end	99999				
Output group	351 - SNPP to localhost 🗸				
Output rate	0				
Allow sources	GCP HTTP SMPP SMTP SNPP TAP TNPP WCTP TEL				
Allow input group	All groups 🖂				
Match domain (%=any)	%				
Send fields	🗖 From 🗖 To 🗖 Timestamp 🗖 MDN 🗹 Subject 🗹 Body				
Timezone offset (e.g. EST is -500)	-500				
Daylight saving observed					
Update					

Screen below shows the configuration of valid subscribers (that accept SIP and TAP input) with pagers or use an ID Block.

Note: Subscribers and ID Blocks will need valid destinations and services to which to send the messages, with the connection(s) to the destination(s) working. Failure to do so will result in failure status being returned to Communication Manager.

8. Verification Steps

This section provides the tests that can be performed to verify correct configuration of the Avaya and PriMega solution.

8.1. Verify Avaya Aura® Communication Manager Page-Link State

The following step can ensure that the communication between Communication Manager paging adjunct and PriMega is functioning correctly. Using SAT, connect to Communication Manager and check the page link status with PriMega by using the command "status page-link". Verify that the **Status** of the CTI link is **up** as shown below.

```
status page-link
PAGE LINK STATUS
PAGE1 Link Status: up
PAGE2 Link Status: up
```

8.2. Verify Page-Link Data

The following step can ensure that the data is being sent and received over the page links. To accomplish this, initiate a call to the paging station mentioned in **Section 5.14** and run the command "list trace page-links". Screen below shows the page being sent and received. It also shows the sent and receive of the heartbeat message.

```
list trace page-links
                                                                               1
                                                                        Page
                                LIST TRACE
time
                data
09:07:25 TRACE STARTED 08/01/2018 CM Release String cold-01.0.532.0-24515
09:07:36 PAGE2 Sent: <STX>56503<CR><CR><ETX>122<CR>
09:07:37 PAGE2 Received: <ACK><CR>
09:07:43 PAGE1 Sent: Heartbeat Message
09:07:43 PAGE1 Received: Heartbeat Message
09:07:43 PAGE1 Received: PAGE EXCHANGE DISCONNECT<CR><EOT><CR>
09:07:45 PAGE1 Sent: <CR>
09:07:47 PAGE1 Sent: <CR>
09:07:47 PAGE1 Received: ID=<CR><LF>
09:07:47 PAGE1 Sent: <ESC>PG1<CR>
09:07:47 PAGE1 Received: <ACK><CR>
09:07:47 PAGE1 Received: <ESC>[p<CR>
09:08:29 PAGE1 Sent: <STX>56503<CR><CR><ETX>122<CR>
09:08:30 PAGE1 Received: <ACK><CR>
09:08:43 PAGE2 Sent: Heartbeat Message
```

8.3. Verify PriMega Logs

The screen below shows excerpts of logs from PriMega when a paging call is made and when the paging station is called.

```
07/19 09:51:18 Received connection from 127.0.0.1
rcvd 'CALL 56204@10.10.97.228'
sent '250 OK'
rcvd 'PAGE 71072'
sent '250 Pager ID accepted'
rcvd 'MESS 1234567890'
sent '250 Message OK'
rcvd 'SEND'
sent '250 Message sent OK'
rcvd 'QUIT'
07/19 11:43:51 Received connection from 127.0.0.1
rcvd 'CALL 15149626014@10.10.97.228'
sent '250 OK'
rcvd 'PAGE 71071'
sent '250 Pager ID accepted'
rcvd 'MESS 1234567890'
sent '250 Message OK'
rcvd 'SEND'
sent '250 Message sent OK'
rcvd 'QUIT'
12:17:27.380 recv returned 13
12:17:27.380 NetRead(fd=11,rsin=): read 9 '[02]56503[0D][0D][03]'
12:17:27.380 in
NetRead(fd=11,max=4,init=99999999,sec=500,btr=4,rt=1,option=0x00000000,rsin= terms=)
12:17:27.380 NetRead(fd=11, rsin=): read 4 '122[0D]'
12:17:27.380 in process_tap(id=56503,data=)
12:17:27.380 in parse_emailaddr(buff=56503,maxname=0,maxaddr=128,maxdomain=80)
12:17:27.380 parse emailaddr returning name='(null)' addr='56503' domain=''
12:17:27.380 in
check id(id=56503,domain=,callpass=****),tnppdest=,source=0x00000020,lookup=0x0000000
3,flags=0x0000001)
12:17:27.380 in sql run buff vp(sqlbuff=select * from subscriber where subscriberid =
'56503')
12:17:27.382 checking idblock 1 name='5 digit numbers' domain='%' allowingroup=0
allowsource=0x00000272 (inputsource=0x00000020)
12:17:27.382 have matching idblock 1 name='5 digit numbers' domain='%'
allowsource=0x00000272
12:17:27.382 in sql_run_buff_vp(sqlbuff=select * from outputgroup where groupnum =
351)
12:17:27.383 leaving check id(found flags=0x00000000) retval=0
12:17:27.383 in sql_vp_copy(srcvp=
                                              (nil))
12:17:27.383 in sql vp copy(srcvp=0x007f481c02ef00)
12:17:27.383 in
send egroup(subvp=(nil),source=0x00000020,max recip=10,smpacket=0x007f481c03de70,reqin
dex=1)
12:17:27.383 in
send notification(smpacket=0x007f481c03de70,useraccess=(nil),service=0,regindex=0,prot
ocol=tap,from=,to=56503,subj=,cid=,bin=N,vce=N,msg=)
12:17:27.383 in insert message record (protocol=TAP, messageid=, capcode=)
12:17:27.383 in NetGetConnInfo(ti=, si=, TCP, server=Y)
12:17:27.383 in NetGetHostDomain(hostmax=81,domainmax=65)
12:17:27.383 NetGetHostDomain: (host='PIKA Test' domain='')
```

Solution & Interoperability Test Lab Application Notes ©2018 Avaya Inc. All Rights Reserved.

9. Conclusion

A full and comprehensive set of feature and functional test cases were performed during Compliance Testing. PriMega Messaging Gateway is considered compliant with Avaya Aura® Communication Manager and Avaya Aura® Session Manager. All test cases have passed and met all the objectives.

10. Additional References

These documents form part of the Avaya official technical reference documentation suite. Further information may be had from <u>http://support.avaya.com</u> or from the local Avaya representative.

- 1. Deploying Avaya Aura® Session Manager, Release 7.1.3. Issue 5. May 2018.
- 2. Administering Avaya Aura® Session Manager, Release 7.1.3. Issue 5. May 2018.
- 3. Deploying Avaya Aura® System Manager, 7.1.3. Issue 8. July 2018.
- 4. Administering Avaya Aura® System Manager for Release 7.1.3, Release 7.1.3. Issue 15. July 2018.
- 5. Deploying Avaya Aura® Communication Manager, Release 7.1.3. Issue 5. May 2018.
- 6. Administering Avaya Aura® Communication Manager, Release 7.1.3. Issue 7. May 2018.
- 7. Avaya Aura® Communication Manager Feature Description and Implementation, Release 7.1.3. Issue 6. May 2018.
- 8. *MultiVantage*® *Requirements/Feature Spec: SA8312*. COMPAS ID: 92212 Issue: 1.1. Date: June 19, 2013

Product Documentation for PriMega Messaging Gateway can be obtained in the installed software or at <u>https://wiki.harktech.com:8443/wiki/index.php</u> (this requires registration).

©2018 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by [®] and TM 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 <u>devconnect@avaya.com</u>.