



Avaya Solution Interoperability Lab

Configuring Avaya Aura™ Session Manager 5.2 with Avaya Aura™ Communication Manager Access Element, Avaya Voice Portal and Avaya Aura™ Communication Manager Feature Server – Issue 1.0

Abstract

These Application Notes describe the configuration of Avaya Aura™ Session Manager R5.2, Avaya Aura™ Communication Manager Access Element R5.2.1 with an Avaya G650 Media Gateway, Avaya Aura™ Communication Manager operating as a Feature Server, and Avaya Voice Portal R5 to support a Voice Portal First (VP 1st) solution.

- Avaya Aura™ Session Manager provides SIP proxy/routing functionality, routing SIP sessions across a TCP/IP network with centralized routing policies and registrations for SIP endpoints.
- Avaya Aura™ Communication Manager operates as a Feature Server to support SIP endpoints which communicate with Avaya Aura™ Session Manager over SIP trunks.
- Avaya G650 Media Gateway consolidates PSTN facilities by concentrating and routing the calls to Avaya Aura™ Communication Manager Access Element which communicates with Avaya Aura™ Session Manager and Avaya Voice Portal over SIP trunks.
- Avaya Voice Portal is a Web services based, speech enabled interactive voice response system that can accept traditional DTMF touch tone inputs and prerecorded audio files for output, as well as VoiceXML2.0 compliant speech applications to guide callers through call flows.

These Application Notes provide information for the setup, configuration, and verification of the call flows tested on the Voice Portal First (VP 1st) solution.

Table of Contents:

1.	Introduction	5
1.1.	Voice Portal First Solution Overview.....	6
1.1.1.	Avaya Aura™ Communication Manager Access Element	6
1.1.2.	Avaya G650 Media Gateway (G650).....	6
1.1.3.	Avaya Aura™ Session Manager (SM).....	6
1.1.4.	Avaya Aura™ Communication Manager Feature Server	7
1.1.5.	Avaya Voice Portal (VP)	7
1.2.	Network Topology.....	8
1.3.	Equipment and Software Validated.....	9
1.4.	Call Flow — SIP Trunk to Avaya Aura™ Communication Manager.....	10
2.	Configuring Avaya Aura™ Communication Manager Access Element.....	11
2.1.	Verify System Capabilities and Licensing	11
2.1.1.	SIP Trunk Capacity Check	11
2.1.2.	AAR/ARS Routing Check	12
2.1.3.	Configure Trunk-to-Trunk Transfers	12
2.1.4.	Configure Codec Type	12
2.2.	Set IP Network Region	13
2.3.	Add Node Names and IP Addresses	13
2.4.	Configure SIP Signaling Group and Trunk Group.....	15
2.4.1.	Create a Signaling Group for SIP Trunk to Avaya Aura™ Session Manager ...	15
2.4.2.	Add a SIP Trunk Group to Connect to Avaya Aura™ Session Manager	16
2.5.	Configure Route Pattern.....	18
2.6.	Administer Numbering Plan	18
2.6.1.	Administer dial plan	18
2.6.2.	Administer ARS analysis	19
2.7.	Administer Hunt-Group, VDN and Vector for calls transferred from VP application	19
2.7.1.	Define Hunt-Group	19
2.7.2.	Administer Vector	21
3.	Configure the Avaya Aura™ Communication Manager Feature Server	21
3.1.	Enable Private Numbering.....	21
3.2.	Configure Private Numbering Plan	22
4.	Configure Avaya Aura™ Session Manager	23
4.1.	Administer SIP Domains.....	24

4.2. Define Locations	24
4.3. Add Avaya Aura™ Communication Manager Access Element.....	25
4.3.1. Define SIP Entity for the Communication Manager Access Element.....	25
4.3.2. Define an Entity Link for Communication Manager Access Element.....	26
4.3.3. Define Routing Policy for Communication Manager Access Element	27
4.3.4. Define Dial Plan for calls to Communication Manager Access Element.....	29
4.4. Add Voice Portal System	31
4.4.1. Define SIP Entity for Voice Portal.....	31
4.4.2. Define the Entity Links for Voice Portal	32
4.4.3. Define Routing Policies for Voice Portal	32
4.4.4. Define Dial Plan to Route Calls to Voice Portal	34
4.5. Administration of Avaya Aura™ Communication Manager Feature Server	35
4.5.1. Define SIP Entity	35
4.5.2. Define the Entity Link	37
4.5.3. Define the Routing Policy	37
4.5.4. Define Application Sequence	38
4.5.5. Verify Registrations of SIP Endpoints.....	39
5. Configure the Voice Portal.....	41
5.1. System Configuration	41
5.1.1. MPP Servers	41
5.1.1. Verify MPP is in Service	41
5.2. Configure the Speech Server	42
5.2.1. Add the Automated Speech Recognition Server (ASR)	43
5.3. Add the Text-To-Speech Server (TTS)	44
5.4. Add a SIP Connection for Session Manager	45
5.5. Setup Self Service Applications	46
6. Verification Steps.....	47
6.1. Verify Avaya Aura™ Session Manager Configuration.....	47
6.2. Verify Voice Portal Configuration	49
6.3. Verify Avaya Aura™ Communication Manager Access Element Configuration....	51
6.4. Verification Scenarios	52
6.4.1. Call Scenarios Verified	52
6.4.2. Verify status on Communication Manager Access Element	53
6.4.3. Verify status on Voice Portal	54

6.4.4. Verify status on Session Manager	54
7. Acronyms.....	55
8. Conclusion.....	56
9. Additional References.....	56

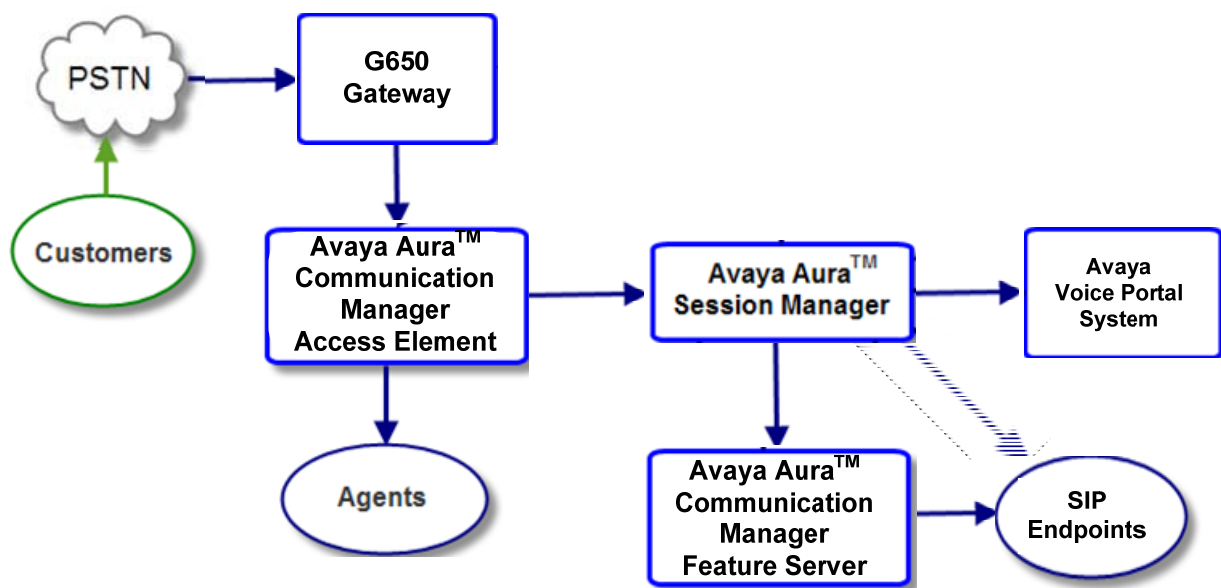
1. Introduction

The Voice Portal First solution in the sample configuration is comprised of five Avaya products – Avaya Aura™ Communication Manager Access Element with an Avaya G650 Media Gateway, Avaya Aura™ Communication Manager Feature Server, Avaya Aura™ Session Manager, and Avaya Voice Portal.

In a typical scenario, a customer call enters an Avaya G650 Media Gateway through the Public Switched Telephone Network (PSTN) over a DS1 trunk. The Avaya G650 Media Gateway delivers the call to the Avaya Aura™ Communication Manager Access Element. Communication Manager routes the calls to the Session Manager over a network connection using a SIP trunk.

The Session Manager routes the call to the Voice Portal system where the customer interacts with a self service application. After completing the self service application, the customer may opt to speak to a contact center agent. If so, the Voice Portal system delivers the call back to Session Manager, which then routes the call back to the Communication Manager Access Element. After arriving at a Communication Manager, the caller is connected to an agent. Alternatively, the call can originate from a SIP endpoint registered to the Session Manager. In this scenario, the Communication Manager Feature Server routes the call to the Session Manager over a SIP trunk.

The figure provides an overview of a typical Voice Portal First solution.



Voice Portal First Solution Overview

These Application Notes describe the administrative steps required for configuring the Avaya products that comprise the Voice Portal First solution.

1.1. Voice Portal First Solution Overview

The following section describes the components of the Voice Portal First Solution.

Core Site

1.1.1. Avaya Aura™ Communication Manager Access Element

Avaya Aura™ Communication Manager provides Call Center Software functionality when a customer elects to talk with an agent. Calls from VP application are delivered to Communication Manager Access Element via direct SIP trunks through Session Manager.

1.1.2. Avaya G650 Media Gateway (G650)

The Avaya G650 Media Gateway provides consolidation of PSTN facilities into SIP.

Data Center

1.1.3. Avaya Aura™ Session Manager (SM)

Avaya Aura™ Session Manager is a SIP proxy/routing engine that is capable of routing SIP requests throughout a network. The Avaya Aura™ System Manager (SMGR) provides administration. Session Manager provides the following functionality:

User Relation Element (URE)

The User Relation Element provides a mapping for all devices associated with a user, acting as a registrar and location server. It also provides origination and termination routing for a user based on their configured and registered features by routing sessions in progress to appropriate feature servers or delivery platforms for featured services. There may be multiple User Relation Elements – all share the same configuration data and real time data.

SIP Routing Element (SRE)

The SIP Routing Element provides site to site routing services including number/name resolution, richly manages network ingress and egress including carrier selection for least cost, time of day, load balancing, and media preferences. There may be multiple SIP Routing Elements – all share the same configuration data and some real time data.

Session Manager does the following:

- Routes SIP sessions across the network with centralized routing policies

- Centralizes SIP registrations and location services
- Scales to support up to 25,000 locations and up to 250,000 users¹
- Enables applications to be decomposed and distributed across the enterprise network
- Introduces application sequencing preparing for applications to run alongside Communication Manager.
- Provides the gateway for the enterprise for external SIP adjuncts.
- Is available with geographically dispersed redundancy, that is, the Session Manager instances can be spread across distance (WAN) but in the event of loss of one Session Manager instance, service still continues to operate normally.
- All the Session Manager instances in an enterprise function as a whole, providing continuous service to all users in the event of Session Manager one instance failures.
- Each Session Manager instance operating in the “active” mode, processes INVITE, REGISTER, SUBSCRIBE and other SIP messages
- Each user in the enterprise is assigned two Session Manager instances to support that user’s proxy, registrar, application sequencer, and event-handler.

1.1.4. Avaya Aura™ Communication Manager Feature Server

Avaya Aura™ Communication Manager operating as a Feature Server supports IP Multimedia Subsystem (IMS)-SIP users that are registered to Avaya Session Manager. The Communication Manager server is connected to Session Manager via an IMS-enabled SIP signaling group.

1.1.5. Avaya Voice Portal (VP)

VP is a Web based speech enabled interactive voice response system that can accept traditional DTMF touch tone inputs and prerecorded audio files for output. It uses VoiceXML2.0 compliant speech applications to guide callers through self service call flows.

Avaya Voice Portal is comprised of a Voice Portal Management System (VPMS) server, a Media Processing Platform (MPP) server, a Web Application Server, and a Speech Processing server. Avaya Dialog Designer (DD) application is deployed on a web application server to perform a custom self service workflow.

Voice Portal Management System (VPMS) manages the MPPs and provides a web interface for administering VP.

Media Processing Platform (MPP) provides the main processing for self service applications. Details are described below:

- Uses H.323, SIP, and RTP protocols to communicate with external services, such as Session Manager.

¹ If there are “N” Session Manager instances in an enterprise, then the total capacity of users that can be supported is = (N-1) X 50,000.

- Runs the Avaya VoiceXML browser to interpret VoiceXML2.0 compliant speech applications.
- Provides proxy interfaces to communicate with the TTS (Text To Speech) servers and ASR (Automatic Speech Recognition) servers. The MPP uses Media Resource Control Protocol (MRCP) to control ASR and TTS servers.

Web Application Server – The web application server utilizes a workflow defined in Dialog Designer to provide the self service application. The MPP calls the application server and coordinates media resources available for processing the call.

Speech Server – The speech server provides Automatic Speech Recognition (ASR) and Text To Speech (TTS) capabilities.

1.2. Network Topology

As shown in **Figure 1**, the Avaya 9600-Series IP Telephone (H.323) and 2420 Digital Telephone are supported by Avaya Aura™ Communication Manager Access Element. The Communication Manager Access Element is connected over a SIP trunk to the Avaya Aura™ Session Manager, using its SM-100 (Security Module) network interface. All inter-system calls are carried over these SIP trunks.

Avaya Aura™ Session Manager is managed by a separate Avaya Aura™ System Manager. Avaya 9620 IP Telephones configured as SIP users utilize the Avaya Aura™ Session Manager User Registration feature and require a Communication Manager operating as a Feature Server.

For the sample configuration, Avaya Aura™ Session Manager runs on an Avaya S8510 Server, and Avaya Aura™ Communication Manager 5.2.1 runs on an Avaya S8730 Server with Avaya G650 Media Gateway. Two Avaya Aura™ Session Managers are deployed as a pair of active-active redundant servers. The results in these Application Notes should be applicable to other Avaya servers and media gateways that support Avaya Aura™ Communication Manager 5.2.1.

These Application Notes will focus on the configuration of the SIP trunks and call routing. Detailed administration of Communication Manager Feature Server and the endpoint telephones will not be described (see the appropriate documentation listed in **Section 9**).

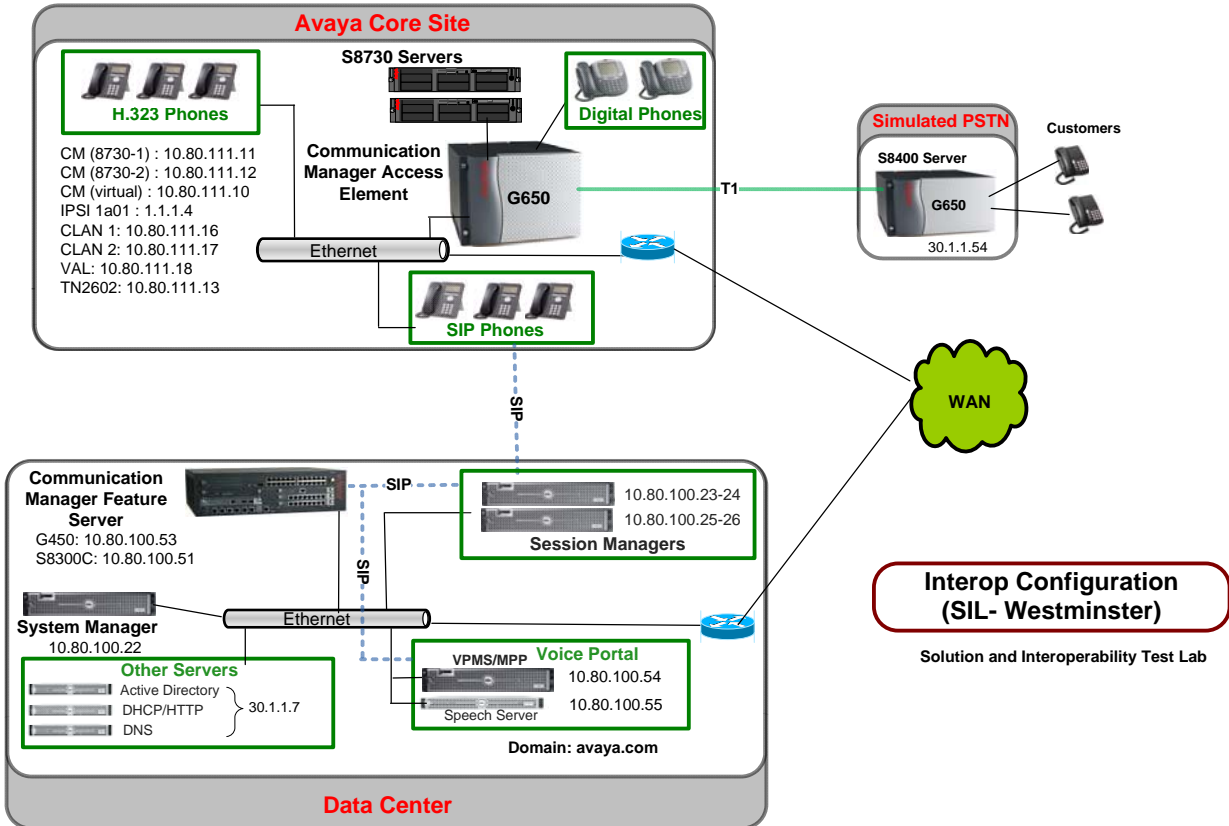


Figure 1: Voice Portal First - Sample Configuration

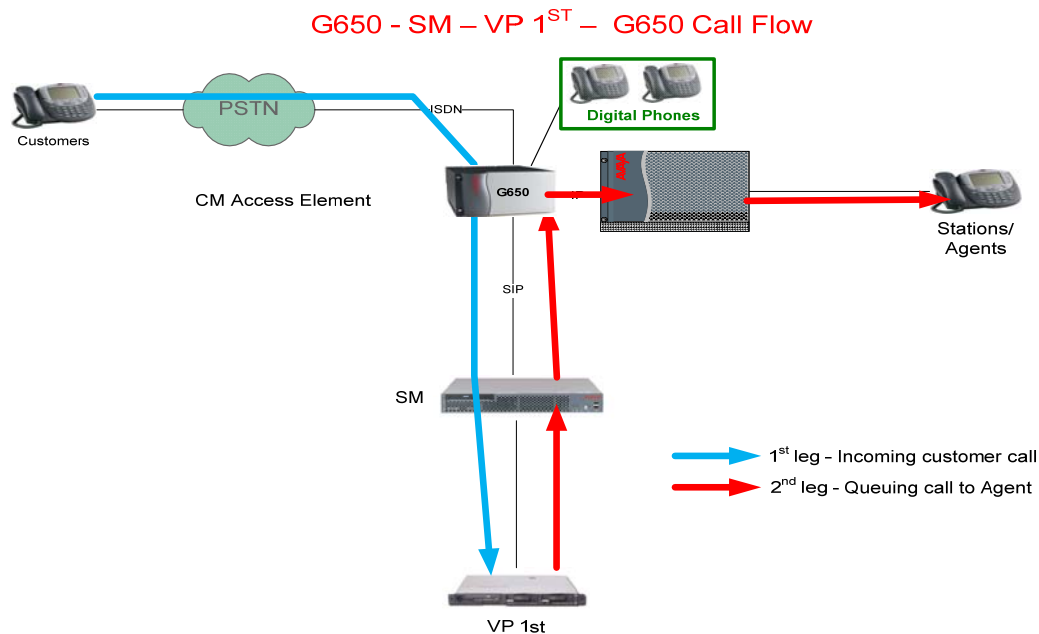
1.3. Equipment and Software Validated

The following equipment and software were used for the sample configuration.

Component	Software Version
Avaya Aura™ Session Manager on Avaya S8510 server	Release 5.2.0.1.520017-11-18-2009
Avaya Voice Portal <ul style="list-style-type: none"> Voice Portal Management System Media Processing Platform Nuance Speech Server Tomcat Application Server 	5.0.0.2.0104 5.0.0.0.4106 NSS05.0.2 Tomcat 5.5
Avaya Aura™ Communication Manager Access Element <ul style="list-style-type: none"> Avaya S8730 Server 	5.2.1 R015x.02.1.016.4
Avaya Aura™ Communication Manager Feature Server <ul style="list-style-type: none"> Avaya S8300 Server 	5.2.1 R015x.02.1.016.4
Avaya G650 Media Gateway <ul style="list-style-type: none"> IPSI (TN2312BP) C-LAN (TN799DP) 	TN2312BP HW14 FW040 TN799DP HW01 FW034

Component	Software Version
<ul style="list-style-type: none"> IP Media Resource 320 (TN2602AP) DS1 Interface (TN464F) 	TN2602AP HW02 FW051 TN464F 000020
Avaya IP Telephones: <ul style="list-style-type: none"> 9650 9630 9620 	FW: 2.0 FW:1.50 FW:1.5
Avaya SIP Phones <ul style="list-style-type: none"> 9650 	FW: 2.5.5.16
Avaya Digital Telephones (2420D)	-

1.4. Call Flow — SIP Trunk to Avaya Aura™ Communication Manager



Scenario: Customer calls VP for self service and selects option to talk to an Agent.

1. Customer calls VP application using either PSTN phone or internal Avaya telephone and is handled by Avaya Aura™ Communication Manager Access Element.
2. Avaya Aura™ Communication Manager routes the call to the Session Manager via SIP trunk.
3. Avaya Aura™ Session Manager routes the call to an MPP on Voice Portal System.
4. The MPP maps the DNIS (Dialed Number Identification Service) number to a speech application and begins the self service workflow.
5. Customer decides to talk to an agent and selects the appropriate option from the workflow.

6. The MPP places an outbound call to Avaya Aura™ Session Manager as part of a SIP REFER method.
7. Session Manager forwards the REFER destination to the Avaya Aura™ Communication Manager.
8. The Avaya Aura™ Communication Manager accepts the REFER message and then delivers the call to an agent².

2. Configuring Avaya Aura™ Communication Manager Access Element

This section describes configuring Avaya Aura™ Communication Manager Access Element using Avaya Site Administrator. These instructions assume a CLAN and Media Processor board are already installed and configured on the Communication Manager Access Element. Some administration screens have been abbreviated for clarity.

- Verify System Capabilities and Communication Manager Licensing
- Administer IP codec set and network region
- Administer IP node names
- Administer IP interface
- Administer SIP trunk group and signaling group
- Administer route patterns
- Administer numbering plan
- Administer VDN for calls transferred from VP application

After completing these steps, the “**save translations**” command should be performed.

2.1. Verify System Capabilities and Licensing

This section describes the procedures to verify the correct system capabilities and licensing have been configured. If there is insufficient capacity or a required feature is not available, contact an authorized Avaya sales representative to make the appropriate changes.

2.1.1. SIP Trunk Capacity Check

Issue the **display system-parameters customer-options** command to verify that an adequate number of SIP trunk members are administered for the system as shown below:

² Note that resulting communication path is from customer, through the G650, to Communication Manager, thereby freeing resources on Voice Portal.

display system-parameters customer-options		Page	2 of 11
OPTIONAL FEATURES			
IP PORT CAPACITIES		USED	
Maximum Administered H.323 Trunks:		500	0
Maximum Concurrently Registered IP Stations:		18000	4
Maximum Administered Remote Office Trunks:		0	0
Maximum Concurrently Registered Remote Office Stations:		0	0
Maximum Concurrently Registered IP eCons:		0	0
Max Concur Registered Unauthenticated H.323 Stations:		100	0
Maximum Video Capable Stations:		0	0
Maximum Video Capable IP Softphones:		0	0
Maximum Administered SIP Trunks:		50	20

2.1.2. AAR/ARS Routing Check

Verify that **ARS** is enabled (on page 3 of system-parameters customer options).

display system-parameters customer-options		Page	3 of 11
OPTIONAL FEATURES			
Abbreviated Dialing Enhanced List? n		Audible Message Waiting? n	
Access Security Gateway (ASG)? n		Authorization Codes? n	
Analog Trunk Incoming Call ID? n		CAS Branch? n	
A/D Grp/Sys List Dialing Start at 01? n		CAS Main? n	
Answer Supervision by Call Classifier? n		Change COR by FAC? n	
ARS? y		Computer Telephony Adjunct Links? y	
ARS/AAR Partitioning? y		Cvg Of Calls Redirected Off-net? y	
ARS/AAR Dialing without FAC? y		DCS (Basic)? y	
ASAI Link Core Capabilities? y		DCS Call Coverage? y	
: 18000		0	

2.1.3. Configure Trunk-to-Trunk Transfers

Use the “**change system-parameters features**” command to enable trunk-to-trunk transfers.

This feature is needed to transfer an incoming/outgoing call from/to the remote switch back out to the same or another 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. Note that this feature poses significant security risk, and must be used with caution.

change system-parameters features		Page	1 of 18
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			

2.1.4. Configure Codec Type

Issue the **change ip-codec-set n** command where **n** is the next available number. Enter the following values:

- Enter “**G.711MU**” for type of Audio Codec

The value administered here will be used in Voice Portal configuration.

- Silence Suppression: Retain the default value “n”.
- Frames Per Pkt: Enter “2”.
- Packet Size (ms): Enter “20”.
- Media Encryption: Enter the value based on the system requirement. For the sample configuration, “none” was used.

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.729	n	2	20
3:			

Media Encryption

1: none

2.2. Set IP Network Region

Using the **change ip-network-region 1** command, set the **Intra-region IP-IP Direct Audio**, and **Inter-region IP-IP Direct Audio** fields to “yes”. For the **Codec Set** enter the corresponding audio codec set configured in **Section 2.1**. Set the **Authoritative Domain** to the correct SIP domain for the configuration.

change ip-network-region 1		Page	1 of	19
IP NETWORK REGION				
Region: 1				
Location:		Authoritative Domain: avaya.com		
Name:				
MEDIA PARAMETERS		Intra-region IP-IP Direct Audio: yes		
Codec Set: 1		Inter-region IP-IP Direct Audio: yes		
UDP Port Min: 2048		IP Audio Hairpinning? n		
UDP Port Max: 16585				

2.3. Add Node Names and IP Addresses

Using the **change node-names ip** command, add the node-name and IP for the CLANs and the Session Manager, if not already previously added. Note the node names of the CLANs which will later be used to configure the SIP trunks between the Avaya G650 and the Session Manager.

Node names for other SIP entities in the solution such as Voice Portal do not have to be administered on the Communication Manager Access Element since the Access Element does not directly connect to these entities.

*Note that these may have been already created and do not need to be re-created if the names are already present in the node-names list.

change node-names ip		Page 1 of 2
Name IP Address		IP NODE NAMES
8730-1	10.80.111.11	
8730-2	10.80.111.12	
ASM1	10.80.100.24	
ASM2	10.80.100.26	
CLAN-1	10.80.111.16	
CLAN-2	10.80.111.17	

2.4. Configure SIP Signaling Group and Trunk Group

2.4.1. Create a Signaling Group for SIP Trunk to Avaya Aura™ Session Manager

In the sample configuration, trunk group “20” and signaling group “20” were used to connect to Avaya Aura™ Session Manager. Issue the **add signaling-group n** command, where “n” is an available signaling group number to create a SIP trunk to the Session Manager. Fill in the indicated fields as shown below. Default values can be used for the remaining fields.

- **Group Type:** “sip”
- **Transport Method:** “tcp”³
- **Near-end Node Name:** C-LAN node name from **Section 2.3**.
- **Far-end Node Name:** Session Manager node name from **Section 2.3**.
- **Near-end Listen Port:** “5060”
- **Far-end Listen Port:** “5060”
- **Far-end Domain:** this field should be left blank⁴
- **DTMF over IP:** “rtp-payload”
- **Session Establishment Timer:** “3”⁵

display signaling-group 20		Page	1 of	1
SIGNALING GROUP				
Group Number: 20		Group Type: sip		
		Transport Method: tcp		
IMS Enabled? n				
IP Video? n				
Near-end Node Name: CLAN-2		Far-end Node Name: ASM1		
Near-end Listen Port: 5060		Far-end Listen Port: 5060		
Far-end Domain:		Far-end Network Region:		
		Bypass If IP Threshold Exceeded? n		
DTMF over IP: rtp-payload		Direct IP-IP Audio Connections? y		
Session Establishment Timer(min): 3		IP Audio Hairpinning? n		
Enable Layer 3 Test? n		Direct IP-IP Early Media? n		
H.323 Station Outgoing Direct Media? n		Alternate Route Timer(sec): 6		

³ TCP was used for the sample configuration. However, TLS would typically be used in production environments.

⁴ To support the ability for the Voice Portal application to transfer calls back to agents logged into Communication Manager, the name of the far-end domain should be left blank.

⁵ If agents are not expected to answer the transferred call from the VP application within 3 minutes, this value may need to be increased.

2.4.2. Add a SIP Trunk Group to Connect to Avaya Aura™ Session Manager

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.

*Note that the number of members determines how many simultaneous calls can be processed by the trunk through Session Manager.

- **Group Type:** “sip”
- **Group Name:** A descriptive name.
- **TAC:** An available trunk access code.
- **Service Type:** “tie”
- **Signaling Group:** The number of the signaling group added in **Section 2.4.1**
- **Number of Members:** The number of members in the SIP trunk to be allocated to calls routed to Session Manager (must be within the limits of the total number of trunks configured in **Section 2.1.1**).

One the add command is completed, trunk members will be automatically generated based on the value in the **Number of Members** field.

add trunk-group 20		Page 1 of 21	
TRUNK GROUP			
Group Number: 20	Group Type: sip	CDR Reports: y	
Group Name: SIP to ASM1 for VP app	COR: 1	TN: 1	TAC: #20
Direction: two-way	Outgoing Display? n	Night Service:	
Dial Access? n			
Queue Length: 0			
Service Type: tie	Auth Code? n		
		Signaling Group: 20	
		Number of Members: 10	

On page 2, set the **Preferred Minimum Session Refresh Interval** to 1200. Note: to avoid extra SIP messages, all SIP trunks connected to Session Manager should be configured with a minimum value of 1200.

add trunk-group 20		Page 2 of 21	
Group Type: sip			
TRUNK PARAMETERS			
Unicode Name: auto			
Redirect On OPTIM Failure: 5000			
SCCAN? n		Digital Loss Group: 18	
Preferred Minimum Session Refresh Interval(sec): 1200			

On page 3, set **Numbering Format** to be *public*. Use default values for all other fields.

add trunk-group 20		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		
Show ANSWERED BY on Display? y		

2.5. Configure Route Pattern

Use the “**change route-pattern n**” command, when n is an available number to define a route pattern for routing calls to the VP application over the SIP trunk group defined in **Section 2.4.2**. In the sample configuration, route pattern 20 was created as shown below:

change route-pattern 20										Page 1 of 3	
Pattern Number: 20 Pattern Name: to VP via ASM											
SCCAN? n Secure SIP? n											
Grp	FRL	NPA	Pfx	Hop	Toll	No.	Inserted	DCS/ IXC			
No			Mrk	Lmt	List	Del	Digits	QSIG			
								Intw			
1: 20	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 No. Numbering LAR											
0	1	2	M	4	W	Request		Dgts Format		Subaddress	
1:	y	y	y	y	y	n	n	rest		none	

2.6. Administer Numbering Plan

2.6.1. Administer dial plan

Use the “**change dialplan analysis**” command, to define any extension numbers associated with the VP application.

In the sample configuration, VDN “522-1000” is used for agents supporting the VP application.

change dialplan analysis										Page 1 of 12	
DIAL PLAN ANALYSIS TABLE											
Location: all										Percent Full: 1	
Dialed	Total	Call	Dialed	Total	Call	Dialed	Total	Call			
String	Length	Type	String	Length	Type	String	Length	Type			
0	1	attd									
1	2	dac									
2	6	aar									
400	7	ext									
500	5	ext									
522	7	ext									
666	7	ext									

2.6.2. Administer ARS analysis

This section provides the configuration of the Automatic Route Selection (ARS) pattern used in the sample configuration for routing “522-2000” calls to the VP application.

Note that other methods of routing may be used.

Use the “**change ars analysis n**” command where **n** is a valid number defined in the dialplan to add an entry for routing the dialed number of “522-2000” to Voice Portal application over the route pattern defined in **Section 2.5**.

change ars analysis 2							Page 1 of 2
ARS DIGIT ANALYSIS TABLE							
Location: all							Percent Full: 1
	Dialed String	Total Min	Total Max	Route Pattern	Call Type	Node Num	ANI Reqd
222		7	7	1	hnpa		n
255		7	7	1	hnpa		n
303		10	10	10	hnpa		n
333		7	7	999	hnpa		n
4		7	7	1	hnpa		n
411		3	3	deny	svcl		n
5		7	7	999	hnpa		n
511		7	7	999	hnpa		n
522		7	7	20	hnpa		n
555		7	7	deny	hnpa		n
611		3	3	1	svcl		n
666		7	7	10	hnpa		n
7		7	7	2	hnpa		n
8		7	7	999	hnpa		n
811		3	3	1	svcl		n

2.7. Administer Hunt-Group, VDN and Vector for calls transferred from VP application

2.7.1. Define Hunt-Group

Use “**add hunt-group x**” command where **x** is an available number to define a hunt-group (skill) for the agents who will receive calls from the VP application.

For the sample configuration, skill 522 was created. Since the Voice Portal application can support multiple, simultaneous calls, set the Queue and Queue Limit fields on page 1 to support queuing.

```
add hunt-group 522
```

Page 1 of 3

HUNT GROUP

```
Group Number: 522                      ACD? y
Group Name: VP Agents                  Queue? y
Group Extension: 522-2222              Vector? y
Group Type: ucd-mia
TN: 1
COR: 1                                MM Early Answer? n
Security Code:                        Local Agent Preference? n
ISDN/SIP Caller Display:

Queue Limit: unlimited
Calls Warning Threshold: 100 Port:
Time Warning Threshold: 100 Port:
```

On page 2, optionally set **Measured** field to “internal” to enable BCMS to monitor agent and queue status. If another reporting product such as Avaya Call Management System is available, this field should be set to either “external” or “both”.

```
add hunt-group 522
```

Page 2 of 3

HUNT GROUP

```
Skill? y      Expected Call Handling Time (sec): 180
AAS? n        Service Level Target (% in sec): 80 in 20
Measured: internal
Supervisor Extension:
```

Use “**add vdn xxx**” command where **xxx** is a valid extension number to define a VDN as the number the VP application will use to transfer calls to an agent.

For the sample configuration, VDN “522-1000” was created. Optionally, set **Measured** field to “internal” to enable BCMS to monitor agent and queue status.

```
add vdn 5221000
```

Page 1 of 2
VECTOR DIRECTORY NUMBER

```
Extension: 522-1000
Name*: Sample VP application
Destination: Vector Number      1000

Meet-me Conferencing? n
Allow VDN Override? n
COR: 1
TN*: 1
Measured: internal
Acceptable Service Level (sec): 20
```

2.7.2. Administer Vector

Use “**change vector xxx**” command where **xxx** is an available vector to define a vector for processing calls from the VP application.

For the sample configuration, vector 1000 was created. Since the Voice Portal application can support multiple, simultaneous calls, define the first step in the vector to queue to the skill (hunt-group) defined in **Section 2.7.1**.

change vector 1000				Page 1 of 6	
CALL VECTOR					
Number: 1000		Name: Sample VP app			
Multimedia? n				Meet-me Conf? n	Lock? n
Basic? y	EAS? y	G3V4 Enhanced? y	ANI/II-Digits? n	ASAI Routing? y	
Prompting? n	LAI? y	G3V4 Adv Route? y	CINFO? n	BSR? y	Holidays? n
Variables? n	3.0 Enhanced? N				
01 queue-to		skill 522 pri h			

3. Configure the Avaya Aura™ Communication Manager Feature Server

Assuming the Avaya Aura™ Communication Manager Feature Server was already installed and configured, this section provides the procedures for any additional configuration needed when an Avaya Aura™ Communication Manager Feature Server is part of the Voice Portal First solution.

3.1. Enable Private Numbering

SIP Users registered to Session Manager need to be added to either the private or public numbering table on the Communication Manager Feature Server. For the sample configuration, private numbering was used.

Use the “**change system-parameters customer-options**” command to verify that Private Networking is enabled as shown below:

display system-parameters customer-options		Page	5 of 11
OPTIONAL FEATURES			
Multinational Locations?	y	Station and Trunk MSP?	y
Multiple Level Precedence & Preemption?	n	Station as Virtual Extension?	y
Multiple Locations?	y	System Management Data Transfer?	n
Personal Station Access (PSA)?	y	Tenant Partitioning?	n
PNC Duplication?	n	Terminal Trans. Init. (TTI)?	y
Port Network Support?	n	Time of Day Routing?	n
Posted Messages?	n	TN2501 VAL Maximum Capacity?	y
Private Networking?	y	Uniform Dialing Plan?	y
Processor and System MSP?	y	Usage Allocation Enhancements?	y
Processor Ethernet?	y	Wideband Switching?	n

3.2. Configure Private Numbering Plan

To enable SIP endpoints to dial extensions defined in the Communication Manager Access Element, use the “**change private-numbering x**” command, where x is the number used to identify the private number plan to create entries for any extension numbers assigned in the Communication Manager Access Element. For the sample configuration, extension numbers starting with 522-XXXX will be used to access the Voice Portal application.

- **Ext Len:** Enter the extension length allowed by the dial plan
- **Ext Code:** Enter leading digit (s) from extension number
- **Trunk Grp:** Enter the SIP Trunk Group number for the SIP trunk between the Feature Server and Session Manager
- **Private Prefix:** Leave blank unless an enterprise canonical numbering scheme is defined in Session Manager. If so, enter the appropriate prefix.

change private-numbering 1		Page	1 of 2
NUMBERING - PRIVATE FORMAT			
Ext Len	Ext Code	Trk Grp(s)	Private Prefix
7	5	10	7
7	6	10	7
		Total Administered: 2	
		Maximum Entries: 540	

Note: After a change on Communication Manager Feature Server which alters the dial plan, synchronization between Communication Manager Feature Server and Session Manager needs to be completed and SIP phones must be re-registered. To request an on demand synchronization, log into the System Manager console and use the **Synchronize CM Data** feature under the Communication System Management menu.

4. Configure Avaya Aura™ Session Manager

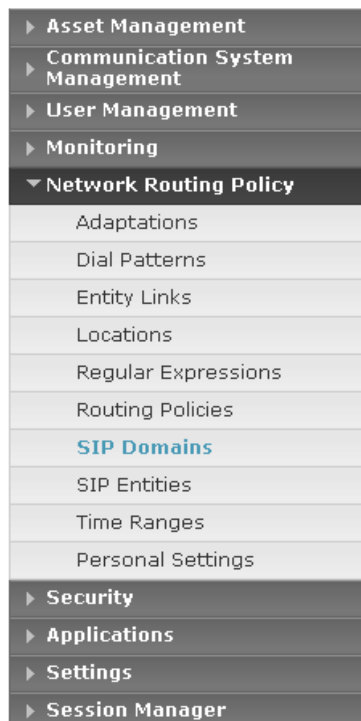
This section provides the procedures for configuring Avaya Aura™ Session Manager. The procedures include adding the following items:

- Administer SIP domain
- Define Logical/physical Locations that can be occupied by SIP Entities
- For each SIP entity in the sample configuration:
 - Define SIP Entity
 - Define Entity Links, which define the SIP trunk parameters used by Avaya Aura™ Session Manager when routing calls to/from SIP Entities
 - Define Routing Policies, which control call routing between the SIP Entities
 - Define Dial Patterns, which govern to which SIP Entity a call is routed

Configuration is accomplished by accessing the browser-based GUI of Avaya Aura™ System Manager, using the URL “http://<ip-address>/SMGR”, where “<ip-address>” is the IP address of Avaya Aura™ System Manager.

Log in with the appropriate credentials and accept the Copyright Notice.

Expand the **Network Routing Policy** Link on the left side of Navigation Menu. Select a specific item such as SIP Domains. When the specific item is selected, the color of the item will change to blue as shown below:



4.1. Administer SIP Domains

- Expand Network Routing Policy and select **SIP Domains**.
 - Click **New**
 - In the *General* Section, under *Name* add a descriptive name. Under *Notes* add a brief description.
 - Click **Commit** to save.

The screen below shows the information for sample configuration.

The screenshot shows the Avaya Aura System Manager 5.2 web interface. The top navigation bar includes the Avaya logo, the product name 'Avaya Aura™ System Manager 5.2', and a user status message: 'Welcome, admin Last Logged on at Dec. 16, 2009 10:07 AM'. Below this is a red breadcrumb trail: 'Home / Network Routing Policy / SIP Domains'. On the left is a sidebar menu with categories: Asset Management, Communication, System Management, User Management, Monitoring, and Network Routing Policy (which is expanded). Under Network Routing Policy, the following items are listed: Adaptations, Dial Patterns, Entity Links, Locations, Regular Expressions, Routing Policies, SIP Domains (highlighted in blue), and SIP Entities. The main content area is titled 'Domain Management' and contains a table with one item. The table has columns for Name, Type, Default, and Notes. The single row shows 'lavaya.com' as the Name, 'sip' as the Type, an unchecked checkbox for Default, and an empty Notes field. Above the table is a 'Filter: Enable' link. Below the table is a red asterisk and the text '* Input Required'. At the top right and bottom right of the main content area are 'Commit' and 'Cancel' buttons.

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

4.2. Define Locations

- Expand Network Routing Policy and select **Locations**. Locations are used to identify logical and/or physical locations where SIP Entities reside, for purposes of bandwidth management or location-based routing.
 - Click **New**
 - In the *General* Section, under *Name* add a descriptive name.
 - Under *Notes* add a brief description.
 - In the *Location Pattern* Section, under IP Address Pattern enter pattern used to logically identify the location. Under *Notes* add a brief description.
 - Click **Commit** to save.

The screen below shows the information for Communication Manager Access Element in the sample configuration.

Home / Network Routing Policy / Locations / **Location Details**

- ▶ Asset Management
- ▶ Communication System Management
- ▶ User Management
- ▶ Monitoring
- ▼ Network Routing Policy
 - Adaptations
 - Dial Patterns
 - Entity Links
 - Locations
 - Regular Expressions
 - Routing Policies
 - SIP Domains
 - SIP Entities
 - Time Ranges
 - Personal Settings
- ▶ Security
- ▶ Applications
- ▶ Settings
- ▶ Session Manager

Location Details

General

* Name:

Notes:

Managed Bandwidth:

* Average Bandwidth per Call: Kbit/sec

* Time to Live (secs):

Location Pattern

1 Item	Refresh	Filter: Enable
<input type="checkbox"/>		<div style="display: flex; justify-content: space-between;"> <div>IP Address Pattern</div> <div>Notes</div> </div> <div style="display: flex; justify-content: space-between;"> <div>* <input type="text" value="10.80.111.*"/></div> <div><input type="text"/></div> </div>

Select : All, None (0 of 1 Selected)

* Input Required

4.3. Add Avaya Aura™ Communication Manager Access Element

4.3.1. Define SIP Entity for the Communication Manager Access Element

- Expand Network Routing Policy
 - Select SIP Entities
 - Click **New**
 - In the *General* Section, under *Name* add an identifier for the Communication Manager. Under *FQDN or IP Address* enter the IP Address of the Communication Manager. Under *Type* select CM. Under *Notes* add a brief description.
 - *Location*: From the drop-down select the Location added in **Section 4.2**. Note: since location-based routing was not used in the sample configuration, selecting a value for location field is optional.
 - Click **Commit** to save.

In the sample configuration, a SIP entity was defined for each of the CLAN boards in the Avaya G650 Media Gateway. The following screen shows addition of one of the SIP entities for the Communication Manager Access Element. The IP address used is that of the C-LAN board in the Avaya G650 Media Gateway.

Home / Network Routing Policy / SIP Entities / SIP Entity Details

Asset Management

Communication System Management

User Management

Monitoring

Network Routing Policy

Adaptations

Dial Patterns

Entity Links

Locations

Regular Expressions

Routing Policies

SIP Domains

SIP Entities

Time Ranges

Personal Settings

Security

Applications

Settings

Session Manager

SIP Entity Details

General

* Name:

* FQDN or IP Address:

Type:

Notes:

Adaptation:

Location:

Time Zone:

Override Port & Transport with DNS SRV: ☐

* SIP Timer B/F (in seconds):

Credential name:

Call Detail Recording:

SIP Link Monitoring

SIP Link Monitoring:

Entity Links

1 Item		Refresh		Filter: Enable		
<input type="checkbox"/>	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted
<input type="checkbox"/>	ASM1-DR	TCP	* 5060	S8730-2	* 5060	<input checked="" type="checkbox"/>

Select : All, None (0 of 1 Selected)

4.3.2. Define an Entity Link for Communication Manager Access Element

- Network Routing Policy
 - Entity Links
 - Click **New**
 - Under *Name*, enter an identifier for the Communication Manager Access Element.
 - Under *SIP Entity 1* drop-down select the appropriate Session Manager. Under *Port* dropdown select the correct port for the Session Manager.
 - Under *SIP Entity 2* drop-down select the SIP Entity added in **Section 4.3.1** for the Communication Manager Access Element. Under *Port* dropdown select the correct port for the Communication Manager. Select it as a *Trusted* host. Under *Protocol* dropdown select the required protocol.
 - Under *Notes* add a brief description.
 - Click **Commit** to save.

The following screen shows the entity link defined for the Communication Manager Access Element.

AVAYA Avaya Aura™ System Manager 5.2

Welcome, **admin** Last Logged on at Dec. 15, 2009 2:03 PM [Help](#) [Log off](#)

Home / Network Routing Policy / Entity Links

Entity Links Commit Cancel

1 Item Refresh Filter: Enable

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted	Notes
* ADM1 to S8730-2	* ASM1-DR	TCP	* 5060	* S8730-2	* 5060	<input checked="" type="checkbox"/>	

* Input Required Commit Cancel

4.3.3. Define Routing Policy for Communication Manager Access Element

- Network Routing Policy
 - Routing Policies
 - Click **New**
 - In the 'General' section, under Name add an identifier to define the routing policy for the Communication Manager. Under *Notes* add a brief description.
 - In the 'SIP Entity as Destination' section, click on **Select**.
 - The SIP Entity List page opens.
 - Select one of the SIP entries for the Communication Manager added in **Section 4.3.1** and click on **Select**
 - The selected SIP Entity displays on the Routing Policy Details page.
 - Click on **Commit** to save.

Shown below is the updated screen for the sample configuration.

- ▶ Asset Management
- ▶ Communication System Management
- ▶ User Management
- ▶ Monitoring
- ▼ Network Routing Policy
 - Adaptations
 - Dial Patterns
 - Entity Links
 - Locations
 - Regular Expressions
 - Routing Policies**
 - SIP Domains
 - SIP Entities
 - Time Ranges
 - Personal Settings
- ▶ Security
- ▶ Applications
- ▶ Settings
- ▶ Session Manager

Shortcuts

- Change Password
- Help for Routing Policy Details fields
- Help for SIP Entity List
- Help for Time Range List
- Help for Pattern List
- Help for Regular Expressions List
- Help for Committing configuration changes

Routing Policy Details[Commit](#) [Cancel](#)**General*** Name: Disabled: ☐Notes: **SIP Entity as Destination**[Select](#)

Name	FQDN or IP Address	Type	Notes
S8730-1	10.80.111.16	CM	S8730 Pair CLAN-1

Time of Day[Add](#)[Remove](#)[View Gaps/Overlaps](#)1 Item [Refresh](#)Filter: [Enable](#)

<input type="checkbox"/>	Ranking 1 ▲	Name 2 ▲	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	Time Range 24/7

Select : All, None (0 of 1 Selected)

Dial Patterns[Add](#)[Remove](#)4 Items [Refresh](#)Filter: [Enable](#)

<input type="checkbox"/>	Pattern ▲	Min	Max	Emergency Call	SIP Domain	Originating Location	Notes
<input type="checkbox"/>	400	7	7	<input type="checkbox"/>	-ALL-	-ALL-	
<input type="checkbox"/>	5221	7	7	<input type="checkbox"/>	-ALL-	-ALL-	to S8730 Agents
<input type="checkbox"/>	5223	7	7	<input type="checkbox"/>	-ALL-	-ALL-	direct call to VP VDN on S8730
<input type="checkbox"/>	6664	7	7	<input type="checkbox"/>	-ALL-	-ALL-	to S8730 CM

Select : All, None (0 of 4 Selected)

4.3.4. Define Dial Plan for calls to Communication Manager Access Element

- Expand Network Routing Policy
 - Dial Patterns
 - Click **New**
 - In the 'General' section, under *Pattern* add the number that the Voice Portal will dial-out to reach an agent on Communication Manager. Under *Min* enter the minimum number digits that must be dialed. Under *Max* enter the maximum number digits that may be dialed.
 - Under SIP Domain drop-down, select the SIP Domain added in **Section 4.1** or select "All" if the system can accept incoming call from all SIP domains
 - Under *Notes* add a brief description.
 - In the 'Originating Locations and Routing Policies' section click on **Add**
 - The 'Locations and Routing Policy List' page opens.
 - Under Locations, select the desired location.
 - Under Routing Policies, select the one defined for Avaya Communication Manager in **Section 4.3.3** and click on **Select**.

Shown below is the updated screen for the sample configuration.

[Home](#) / [Network Routing Policy](#) / [Dial Patterns](#) / **Dial Pattern Details**

- ▶ Asset Management
- ▶ Communication System Management
- ▶ User Management
- ▶ Monitoring
- ▼ **Network Routing Policy**
 - Adaptations
 - Dial Patterns**
 - Entity Links
 - Locations
 - Regular Expressions
 - Routing Policies
 - SIP Domains
 - SIP Entities
 - Time Ranges
 - Personal Settings
- ▶ Security
- ▶ Applications
- ▶ Settings
- ▶ Session Manager

Shortcuts

[Change Password](#)
[Help for Dial Pattern Details fields](#)
[Help for Location and Routing Policy Lists](#)
[Help for Denied Location fields](#)
[Help for Committing](#)

Dial Pattern Details[Commit](#) [Cancel](#)**General**

* **Pattern:**

* **Min:**

* **Max:**

Emergency Call: ☐

SIP Domain:

Notes:

Originating Locations and Routing Policies[Add](#) [Remove](#)

1 Item Refresh		Filter: Enable					
<input type="checkbox"/>	Originating Location Name 1 ▲	Originating Location Notes	Routing Policy Name	Rank 2 ▲	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	-ALL-	Any Locations	to S8730 CM	0	<input type="checkbox"/>	S8730-1	
Select : All, None (0 of 1 Selected)							

Denied Originating Locations[Add](#) [Remove](#)


0 Items Refresh		Filter: Enable	
<input type="checkbox"/>	Originating Location	Notes	

* **Input Required**[Commit](#) [Cancel](#)

4.4. Add Voice Portal System

4.4.1. Define SIP Entity for Voice Portal

- Expand Network Routing Policy
 - Select SIP Entities
 - Click **New**
 - In the *General* Section, under *Name* add an identifier for the Voice Portal. Under *FQDN or IP Address* enter the Host Name or IP address of the Voice Portal server⁶. Under *Type* select VP. Under *Notes* add a brief description.
 - Click **Commit** to save.

 Avaya Aura™ System Manager 5.2

Welcome, **admin** Last Logged on at Dec. 15, 2009 2:03 PM

[Help](#) | [Log off](#)

Home / Network Routing Policy / SIP Entities / SIP Entity Details

Asset Management

Communication System Management

User Management

Monitoring

Network Routing Policy

Adaptations

Dial Patterns

Entity Links

Locations

Regular Expressions

Routing Policies

SIP Domains

SIP Entities

Time Ranges

Personal Settings

Security

Applications

Settings

Session Manager

Shortcuts

Change Password

Help for SIP Entity Details fields

Help for Committing configuration changes

SIP Entity Details

Commit Cancel

General

* Name: VPMS

* FQDN or IP Address: 10.80.100.54

Type: Voice Portal

Notes: VP in SIL Westminster Lab

Adaptation:

Location:

Time Zone: America/Denver

Override Port & Transport with DNS SRV:

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

Credential name:

Call Detail Recording: none

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

Entity Links

Add Remove

1 Item | Refresh

Filter: Enable

	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted
<input type="checkbox"/>	ASM1-DR	TCP	* 5060	VPMS	* 5060	<input checked="" type="checkbox"/>

Select : All, None (0 of 1 Selected)

⁶ Note: in the sample configuration, the MPP is running on the same server as the VPMS. In configurations with multiple MPPs, a SIP entity would need to be defined for each MPP.

4.4.2. Define the Entity Links for Voice Portal

- Expand Network Routing Policy
 - Select Entity Links
 - Click **New**
 - Under *Name* enter an identifier for the Avaya Voice Portal.
 - Under *SIP Entity 1* drop-down select the appropriate Session Manager. Under *Port* dropdown select the correct port for the Session Manager.
 - Under *SIP Entity 2* drop-down select the SIP Entity added in **Section 4.4.1** for the Avaya Voice Portal. Under *Port* drop-down select the correct port for the Avaya Voice Portal. Select it as a *Trusted* host. Under *Protocol* dropdown select the required protocol. Under *Notes* add a brief description.
 - Click **Commit** to save.

Shown below is the updated screen for the sample configuration.

The screenshot shows the Avaya Aura System Manager 5.2 interface. The top navigation bar includes the Avaya logo, the system name 'Avaya Aura™ System Manager 5.2', and a welcome message for the 'admin' user. The sidebar menu on the left lists various management options, with 'Network Routing Policy' expanded to show 'Entity Links'. The main content area displays the 'Entity Links' configuration page, which includes a table with columns for Name, SIP Entity 1, Protocol, Port, SIP Entity 2, Port, Trusted, and Notes. A single entity link is shown in the table, with fields for Name, SIP Entity 1, Protocol, Port, SIP Entity 2, Port, Trusted, and Notes. The 'Trusted' checkbox is checked. Below the table, there is a 'Commit' button and a 'Cancel' button. The page also includes a 'Filter: Enable' option and a 'Refresh' button.


Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted	Notes
* ASM1 to VP	* ASM1-DR	TCP	* 5060	* VPMS	* 5060	<input checked="" type="checkbox"/>	

4.4.3. Define Routing Policies for Voice Portal

- Network Routing Policy
 - Routing Policies
 - Click **New**

- In the 'General' section, under Name add an identifier to define the routing policy for the Avaya Voice Portal. Under *Notes* add a brief description.
- In the 'SIP Entity as Destination' section, click on **Select**
- The SIP Entity List page opens.
Select the entry of the Avaya Voice Portal added in the above steps, and click **Select**.
- The selected SIP Entity displays on the Routing Policy Details page.
- Click on **Commit** to save.

Shown below is the updated screen for the sample configuration.


Avaya Aura™ System Manager 5.2
Welcome, **admin** Last Logged on at Dec. 15, 2009 2:03 PM
[Help](#) | [Log off](#)

Home / Network Routing Policy / Routing Policies / Routing Policy Details

▶ Asset Management
▶ Communication System Management
▶ User Management
▶ Monitoring
▼ Network Routing Policy
Adaptations
Dial Patterns
Entity Links
Locations
Regular Expressions
Routing Policies
SIP Domains
SIP Entities
Time Ranges
Personal Settings
▶ Security
▶ Applications
▶ Settings
▶ Session Manager

Routing Policy Details

Commit Cancel

General

* Name:

Disabled: ☐

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
VPMS	10.80.100.54	Voice Portal	VP in SIL Westminster Lab

Time of Day

Add Remove View Gaps/Overlaps

1 Item Refresh
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	Time Range 24/7

Select : All, None (0 of 1 Selected)

Dial Patterns

Add Remove

1 Item Refresh
Filter: Enable

<input type="checkbox"/>	Pattern	Min	Max	Emergency Call	SIP Domain	Originating Location	Notes
<input type="checkbox"/>	5222	7	7	<input type="checkbox"/>	-ALL-	-ALL-	to Voice Portal Apps

Select : All, None (0 of 1 Selected)

Shortcuts

- Change Password
- Help for Routing Policy Details fields
- Help for SIP Entity List
- Help for Time Range List
- Help for Pattern List
- Help for Regular Expressions List
- Help for Committing

4.4.4. Define Dial Plan to Route Calls to Voice Portal

- Expand Network Routing Policy
 - Select Dial Patterns
 - Click **New**
 - In the 'General' section under Pattern, add the dialed string of the number associated with the Voice Portal application. Under Min, enter the minimum number digits that must be dialed. Under Max, enter the maximum number digits that may be dialed.
 - Under SIP Domain drop-down, select the appropriate SIP Domain.
 - Under *Notes* add a brief description.
 - In the 'Originating Locations and Routing Policies' section click on **Add**
 - The 'Locations and Routing Policy List' page opens.
 - Under Locations, select the desired location or select the ALL options
 - Under Routing Policies select the one defined for the Voice Portal in **Section 4.4.3** and click on **Select**.

Shown below is the updated screen for the sample configuration.

Dial Pattern Details

General

* Pattern:

* Min:

* Max:

Emergency Call: ☐

SIP Domain:

Notes:
Originating Locations and Routing Policies

1 Item		Refresh		Filter: Enable			
<input type="checkbox"/>	Originating Location Name 1 ▲	Originating Location Notes	Routing Policy Name	Rank 2 ▲	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	-ALL-	Any Locations	to Voice Portal	0	<input type="checkbox"/>	VPMS	
Select : All, None (0 of 1 Selected)							

Denied Originating Locations

0 Items		Refresh	Filter: Enable	
<input type="checkbox"/>	Originating Location	Notes		

* Input Required

4.5. Administration of Avaya Aura™ Communication Manager Feature Server

Detailed administration of Communication Manager Feature Server and the endpoint telephones will not be described (see the appropriate documentation listed in **Section 9**). The following section captures relevant screens for Communication Manager Feature Server applicable for these Application Notes.

4.5.1. Define SIP Entity

The following screen shows addition of Communication Manager Feature Server. The IP address used is that of the S8300C server.



- ▶ Asset Management
- ▶ Communication System Management
- ▶ User Management
- ▶ Monitoring
- ▼ Network Routing Policy
 - Adaptations
 - Dial Patterns
 - Entity Links
 - Locations
 - Regular Expressions
 - Routing Policies
 - SIP Domains
 - SIP Entities**
 - Time Ranges
 - Personal Settings
- ▶ Security
- ▶ Applications
- ▶ Settings
- ▶ Session Manager

Shortcuts

[Change Password](#)
[Help for SIP Entity Details fields](#)
[Help for Committing configuration changes](#)

SIP Entity Details

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

General

* Name:

* FQDN or IP Address:

Type:

Notes:

Adaptation:

Location:

Time Zone:

Override Port & Transport with DNS SRV: ☐

* SIP Timer B/F (in seconds):

Credential name:

Call Detail Recording:

SIP Link Monitoring

SIP Link Monitoring:

* Proactive Monitoring Interval (in seconds):

* Reactive Monitoring Interval (in seconds):

* Number of Retries:

Entity Links

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

1 Item Refresh		Filter: Enable				
<input type="checkbox"/>	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted
<input type="checkbox"/>	ASM1-DR	TCP	* 5060	S8300-G450-FS	* 5060	<input checked="" type="checkbox"/>
Select : All, None (0 of 1 Selected)						

4.5.2. Define the Entity Link

The following screen shows the entity link defined for the Communication Manager Feature Server.

AVAYAAvaya Aura™ System Manager 5.2Welcome, **admin** Last Logged on at Dec. 16, 2009 10:07 AMHelp | [Log off](#)

Home / Network Routing Policy / Entity Links

▶ Asset Management

▶ Communication System Management

▶ User Management

▶ Monitoring

▼ Network Routing Policy

Adaptations

Dial Patterns

Entity Links

Locations

Regular Expressions

Routing Policies

SIP Domains

SIP Entities

Time Ranges

Entity Links

CommitCancel

1 Item RefreshFilter: Enable

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted	Notes
* ASM-to-S8300-2	* ASM1-DR	TCP	* 5060	* S8300-G450-FS	* 5060	<input checked="" type="checkbox"/>	

< >

* Input Required

CommitCancel

4.5.3. Define the Routing Policy

Since the SIP users are registered on Session Manager, the routing policy defined for the Communication Manager Feature Server does not need to include any dial patterns as shown below:

AVAYAAvaya Aura™ System Manager 5.2Welcome, **admin** Last Logged on at Dec. 15, 2009 3:30 PMHelp | [Log off](#)

Home / Network Routing Policy / Routing Policies / Routing Policy Details

▶ Asset Management

▶ Communication System Management

▶ User Management

▶ Monitoring

▼ Network Routing Policy

Adaptations

Dial Patterns

Entity Links

Locations

Regular Expressions

Routing Policies

SIP Domains

SIP Entities

Time Ranges

Personal Settings

Routing Policy Details

CommitCancel

General

* Name: to CM FS

Disabled: ☒

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
S8300-G450-FS	10.80.100.51	CM	CM 5.2.1

Time of Day

AddRemoveView Gaps/Overlaps

1 Item RefreshFilter: Enable

<input type="checkbox"/>	Ranking 1 ▲	Name 2 ▲	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	Time Range 24/7

Select: All, None (0 of 1 Selected)

Dial Patterns

AddRemove

0 Items RefreshFilter: Enable

<input type="checkbox"/>	Pattern	Min	Max	Emergency Call	SIP Domain	Originating Location	Notes
--------------------------	---------	-----	-----	----------------	------------	----------------------	-------

4.5.4. Define Application Sequence

First, verify an application has been defined for the Communication Manager Feature Server as shown below:

AVAYA

Avaya Aura™ System Manager 5.2

Welcome, **admin** Last Logged on at Dec. 15, 2009 2:03 PM
[Help](#) [Log off](#)

Home / Session Manager / Application Configuration / Application Editor

▶ Asset Management

▶ Communication System Management

▶ User Management

▶ Monitoring

▶ Network Routing Policy

▶ Security

▶ Applications

▶ Settings

▼ Session Manager

Session Manager Administration

▶ Network Configuration

▶ Device and Location Configuration

▼ Application Configuration

■ Applications

■ Application Sequences

■ Implicit Users

▶ System Status

▶ System Tools

Application Editor

Commit

Cancel

Application Editor

Name

* SIP Entity

Description

Application Attributes (optional)

Name	Value
Application Handle	<input type="text"/>
URI Parameters	<input type="text"/>

*Required

Commit

Cancel

Second, define an application sequence for the Communication Manager Feature Server as shown below:

AVAYA

Avaya Aura™ System Manager 5.2

Welcome, **admin** Last Logged on at Dec. 15, 2009 2:03 PM
[Help](#) [Log off](#)

Home / Session Manager / Application Configuration / Application Sequence Editor

▶ Asset Management

▶ Communication System Management

▶ User Management

▶ Monitoring

▶ Network Routing Policy

▶ Security

▶ Applications

▶ Settings

▼ Session Manager

Session Manager Administration

▶ Network Configuration

▶ Device and Location Configuration

▼ Application Configuration

■ Applications

■ Application Sequences

■ Implicit Users

▶ System Status

▶ System Tools

Application Sequence Editor

Commit

Cancel

Sequence Name

Name

Description

Applications in this Sequence

Move First

Move Last

Remove

1 Item

<input type="checkbox"/>	Sequence Order (first to last)	Name	SIP Entity	Mandatory	Description
<input type="checkbox"/>	▲ ▼ ✕	S8300-G450-APP	S8300-G450-FS	<input checked="" type="checkbox"/>	CM as FS only

Select : All, None (0 of 1 Selected)

Available Applications

2 Items Refresh

Filter: Enable

	Name	SIP Entity	Description
+	S8300-G450-APP	S8300-G450-FS	CM as FS only
+	Voice Portal	VPMS	VMPS/MPP Server running VP app

*Required

Commit

Cancel

4.5.5. Verify Registrations of SIP Endpoints

Verify SIP users have been created in the Session Manager. In the sample configuration, two SIP users were created as shown in the highlighted area below:

AVAYA

Avaya Aura™ System Manager 5.2

Welcome, **admin** Last Logged on at Dec. 15, 2009 2:03 PM
Help : [Log off](#)

Home / User Management / User Management

Asset Management

Communication System Management

User Management

Manage Roles

User Management

Global User Settings

Group Management

Monitoring

Network Routing Policy

Security

Applications

Settings

Session Manager

Shortcuts

Change Password

Help for View Users

User Management

Users

View Edit New Duplicate Delete More Actions

Advanced Search

5 Items Refresh Filter: Enable

<input type="checkbox"/>	Status	Name	User Name	Handle	Last Login
<input type="checkbox"/>		Administrator	administrator@avaya.com		December 7, 2009 7:19:23 PM -06:00
<input type="checkbox"/>		Default Administrator	admin		December 15, 2009 10:30:29 PM -06:00
<input type="checkbox"/>		John Smith	6663000@avaya.com	6663000	
<input type="checkbox"/>		Jones, Paul	6663001@avaya.com	6663001	
<input type="checkbox"/>		System User	system		

Select : All, None (0 of 5 Selected)

Verify the application sequence defined in **Section 4.5.4** is assigned to the SIP users by assigning the appropriate SIP communication profile as shown below:

AVAYA

Avaya Aura™ System Manager 5.2

Welcome, **admin** Last Logged on at Dec. 15, 2009 2:03 PM
Help : [Log off](#)

Home / User Management / User Management / User Edit

Asset Management

Communication System Management

User Management

Manage Roles

User Management

Global User Settings

Group Management

Monitoring

Network Routing Policy

Security

Applications

Settings

Session Manager

Shortcuts

Change Password

Help for Edit User

Help for New Private Contact

Help for Edit Private Contact

Help for Delete Private Contact

Help for adding contact into contact list

Help for editing contact from contact list

Help for deleting contact from contact list

User Profile Edit: 6663000@avaya.com

Commit Cancel

General | Identity | Communication Profile | Roles | Override Permissions | Group Membership | Attribute Sets | Default Contact List | Private Contacts |
Expand All | Collapse All

General

Identity

Communication Profile

New Delete Done Cancel

Name
Primary

Select : None

* Name: Primary

Default: ☒

Communication Address

New Edit Delete

<input type="checkbox"/>	Type	SubType	Handle	Domain
<input type="checkbox"/>	sip	username	6663000	avaya.com

Select : All, None (0 of 1 Selected)

☒ Session Manager

Verify the SIP endpoints have successfully registered with the Session Manager as shown below:



- ▶ Asset Management
- ▶ Communication System Management
- ▶ User Management
- ▶ Monitoring
- ▶ Network Routing Policy
- ▶ Security
- ▶ Applications
- ▶ Settings
- ▼ Session Manager
 - Session Manager Administration
 - ▶ Network Configuration
 - ▶ Device and Location Configuration
 - ▶ Application Configuration
 - ▼ System Status
 - System State Administration
 - System State Monitoring
 - Managed Bandwidth Usage
 - Security Module Status
 - Data Replication Status
 - RegistrationSummary
 - User Registrations**
 - ▶ System Tools

Shortcuts

- [Change Password](#)
- [Help for User Registrations](#)
- [Help for Page Fields](#)

User Registrations

Select to send notifications to AST devices. Click on row to display registration detail.

[Refresh](#) **AST Device Notifications:** [Reboot](#) [Reload](#)

3 Items Refresh		Filter: Enable					
<input type="checkbox"/>	Registered	Address	Login Name	First Name	Last Name	Session Manager	AST Device
<input type="checkbox"/>	true	6663000@avaya.com	6663000@avaya.com	John	Smith	ASM1-DR	true
<input checked="" type="checkbox"/>	true	6663001@avaya.com	6663001@avaya.com	Paul	Jones	ASM1-DR	true
<input type="checkbox"/>	false	Administrator@avaya.com	administrator@avaya.com	SIL	Administrator	ASM1-DR	false
Select : All, None (1 of 3 Selected)							

Registration Detail

Login Name:	6663001@avaya.com					
Registration Address:	6663001@avaya.com					
Registration Time:	Mon Dec 14 11:07:57 MST 2009					
Event Subscriptions:	<table><tr><td>avaya-cm-feature-status</td></tr><tr><td>avaya-ccs-profile</td></tr><tr><td>dialog</td></tr><tr><td>reg</td></tr><tr><td>message-summary</td></tr></table>	avaya-cm-feature-status	avaya-ccs-profile	dialog	reg	message-summary
avaya-cm-feature-status						
avaya-ccs-profile						
dialog						
reg						
message-summary						
User Communication Profile Addresses:	6663001@avaya.com					

5. Configure the Voice Portal

Log in to the Web Administration page of Voice Portal with Administrative rights.

5.1. System Configuration

5.1.1. MPP Servers

Add the installed MPP with details of the appropriate IP addresses, maximum simultaneous calls, etc. For the sample configuration, the MPP server is located at IP address 10.80.100.54.

Refer to Voice Portal documentation for additional details in **Section 9**.

AVAYA

Welcome, administrator
Last logged in yesterday at 3:39:38 PM MST

Voice Portal 5.0 (VoicePortal)

Expand All | Collapse All

- ▼ User Management
 - Roles
 - Users
- ▼ Real-Time Monitoring
 - Login Options
 - System Monitor
 - Active Calls
 - Port Distribution
- ▼ System Maintenance
 - Audit Log Viewer
 - Trace Viewer
 - Log Viewer
 - Alarm Manager
- ▼ System Management
 - MPP Manager
 - Software Upgrade
 - System Backup
- ▼ System Configuration
 - Alarm Codes
 - Alarm/Log Options
 - Applications
 - MPP Servers
 - Report Data
 - SNMP
 - Speech Servers
 - VoIP Connections
 - VPMS Servers
- ▼ Security
 - Certificates
 - Licensing
- ▼ Reports
 - Standard
 - Custom
 - Scheduled

You are here: [Home](#) > [System Configuration](#) > [MPP Servers](#) > [Change MPP Server](#)

Change MPP Server

Use this page to change the configuration of an MPP. Take care when changing the MPP Trace Logging Thresholds. Do not set Trace Levels to Finest if your Voice Portal system has heavy call traffic. The system might experience performance issues if Trace Levels are set to Finest. Set Trace Levels to Finest only when you are troubleshooting the system.

Name: MPP1

Host Address: 10.80.100.54

Network Address (VoIP): <Default>

Network Address (MRCP): <Default>

Network Address (AppSvr): <Default>

Maximum Simultaneous Calls: 10

Restart Automatically: ☒ Yes ☐ No

MPP Certificate

Owner: CN=VPMS, O=Avaya, OU=VPMS
Issuer: CN=VPMS, O=Avaya, OU=VPMS
Serial Number: 80d16a0dd06e111f
Valid from: Fri Dec 04 12:54:19 MST 2009 until: Mon Dec 02 12:54:19 MST 2019
Certificate fingerprints
MD5: 86:23:e4:c0:3a:87:e6:4e:3a:73:5b:34:bb:a4:24:c7
SHA: dd:ac:c7:9f:45:0c:ab:23:72:ad:81:9b:be:00:c3:b9:dd:de:72:6a

Categories and Trace Levels ▶

[Save](#) [Apply](#) [Cancel](#) [Help](#)

5.1.1. Verify MPP is in Service

Under System Management select MPP Manager, on the left hand side. This will list all the administered MPPs. To place a MPP in service, check the box to the left of the server name and click on Start.

The screen shot below shows the MPP is Online and in the Running State.

Welcome, administrator
Last logged in yesterday at 3:39:38 PM MS

Voice Portal 5.0 (VoicePortal)
Home Help Logoff

Expand All Collapse All

User Management
Roles
Users
Login Options

Real-Time Monitoring
System Monitor
Active Calls
Port Distribution

System Maintenance
Audit Log Viewer
Trace Viewer
Log Viewer
Alarm Manager

System Management
MPP Manager
Software Upgrade
System Backup

System Configuration
Alarm Codes
Alarm/Log Options
Applications
MPP Servers
Report Data
SNMP
Speech Servers
VoIP Connections
VPMS Servers

Security
Certificates
Licensing

Reports
Standard
Custom
Scheduled

You are here: [Home](#) > System Management > MPP Manager

MPP Manager (12/15/09 2:13:38 PM MST)

[Refresh](#)

This page displays the current state of each MPP in the Voice Portal system. To enable the state and mode commands, select one or more MPPs. To enable the mode commands, the selected MPPs must also be stopped.

Last Poll: 12/15/09 2:13:38 PM MST

	Server Name	Mode	State	Config	Auto Restart	Restart Schedule		Active Calls	
						Today	Recurring	In	Out
<input type="checkbox"/>	MPP1	Online	Running	OK	Yes	No	None	0	0

State Commands
Start Stop Restart Reboot Halt Cancel

Mode Commands
Offline Test Online

[Help](#)

Restart/Reboot Options
☐ One server at a time
☒ All selected servers at the same time

5.2. Configure the Speech Server

Under System Configuration, Select Speech Servers. Verify the Speech Server is correctly configured with the IP address of the host machine running the application server and speech server. The configuration of the Speech Server for the sample configuration is shown below:

Welcome, administrator
Last logged in yesterday at 3:39:38 PM MST

Voice Portal 5.0 (VoicePortal)
Home Help Logoff

Expand All Collapse All

User Management
Roles
Users
Login Options

Real-Time Monitoring
System Monitor
Active Calls
Port Distribution

System Maintenance
Audit Log Viewer
Trace Viewer
Log Viewer
Alarm Manager

System Management
MPP Manager
Software Upgrade
System Backup

System Configuration
Alarm Codes
Alarm/Log Options
Applications
MPP Servers
Report Data
SNMP
Speech Servers
VoIP Connections
VPMS Servers

Security
Certificates
Licensing

Reports
Standard
Custom
Scheduled

You are here: [Home](#) > System Configuration > Speech Servers

Speech Servers

This page displays the list of Automated Speech Recognition (ASR) and Text-to-Speech (TTS) servers that Voice Portal communicates with.

ASR TTS

	Name	Enable	Network Address	Engine Type	MRCP	Base Port	Total Number of Licensed ASR Resources	Languages
<input type="checkbox"/>	SpeechSvr	Yes	10.80.100.55	Nuance	MRCP V1	4900	100	English(USA) en-us

Add Delete

Customize Help

5.2.1. Add the Automated Speech Recognition Server (ASR)

On the Speech Servers page when the ASR tab is highlighted, select the Add button at the bottom of the page and enter the required details such as the IP address of the speech server host machine, Engine Type such as Nuance, etc.

Below is a screen after ASR is added for the sample configuration.

AVAYA Welcome, administrator
Last logged in yesterday at 3:39:38 PM MST

Voice Portal 5.0 (VoicePortal) Home ? Help Logoff

Expand All | Collapse All

You are here: [Home](#) > [System Configuration](#) > [Speech Servers](#) > [Change ASR Server](#)

Change ASR Server

Use this page to change the configuration of an ASR server.

Name: SpeechSvr

Enable: ☒ Yes ☐ No

Engine Type: Nuance

Network Address: 10.80.100.55

Base Port: 4900

Total Number of Licensed ASR Resources: 100

New Connection per Session: ☐ Yes ☒ No

Languages: Dutch(Netherlands) nl-nl
English(Australia) en-au
English(UK) en-gb
English(India) en-in
English(Singapore) en-SG
English(USA) en-us

MRCP

Ping Interval: 15 second(s)

Response Timeout: 4 second(s)

Protocol: MRCP V1

RTSP URL: 10.80.100.55/media/speechrecognizer

Save Apply Cancel Help

5.3. Add the Text-To-Speech Server (TTS)

On the Speech Servers page, select the TTS tab and enter the required details such as the IP address of the TTS host machine, Engine Type such as Nuance, etc.

Below is the screen after TTS is added for the sample configuration.

AVAYA Welcome, administrator
Last logged in yesterday at 3:39:38 PM MST

Voice Portal 5.0 (VoicePortal) Home Help Logoff

Expand All | Collapse All

- ▼ **User Management**
 - Roles
 - Users
- ▼ **Real-Time Monitoring**
 - Login Options
 - System Monitor
 - Active Calls
 - Port Distribution
- ▼ **System Maintenance**
 - Audit Log Viewer
 - Trace Viewer
 - Log Viewer
 - Alarm Manager
- ▼ **System Management**
 - MPP Manager
 - Software Upgrade
 - System Backup
- ▼ **System Configuration**
 - Alarm Codes
 - Alarm/Log Options
 - Applications
 - MPP Servers
 - Report Data
 - SNMP
 - Speech Servers
 - VoIP Connections
 - VPMS Servers
- ▼ **Security**
 - Certificates
 - Licensing
- ▼ **Reports**
 - Standard
 - Custom
 - Scheduled

You are here: [Home](#) > [System Configuration](#) > [Speech Servers](#) > [Change TTS Server](#)

Change TTS Server

Use this page to change the configuration of a TTS server.

Name: TextServer

Enable: ☒ Yes ☐ No

Engine Type:

Network Address:

Base Port:

Total Number of Licensed TTS Resources:

New Connection per Session: ☐ Yes ☒ No

Voices:

English(Irish) en-El Moira F
English(South_African) af-ZA Tessa F
English(Scottish) en-SC Fiona F
English(USA) en-US Donna F
English(USA) en-US Erica F
English(USA) en-US Jennifer F

MRCP

Ping Interval: second(s)

Response Timeout: second(s)

Protocol:

RTSP URL:

Save Apply Cancel Help

5.4. Add a SIP Connection for Session Manager

Under System Configuration, select VoIP Connections. Select the SIP tab and Click on New. Add the SIP connection details which would contain details of the SIP interface to Session Manager. Enter IP address of the Session Manager Security Module (SM 100) under Proxy Servers. Verify the port number matches the port number defined in **Section 4.4.1** for the Voice Portal SIP entity. Finally, verify the SIP domain matches the SIP domains defined in Session Manager.

Below is a screen after the SIP Connection is added for the sample configuration.

The screenshot shows the Avaya Voice Portal 5.0 (VoicePortal) interface. The top navigation bar includes the Avaya logo, a welcome message for the administrator, and links for Home, Help, and Logoff. The left sidebar contains a tree view of system configuration options, with 'System Configuration' expanded. The main content area is titled 'Change SIP Connection' and contains the following fields and sections:

- Name:** sm100-silasm1
- Enable:** ☒ Yes ☐ No
- Proxy Transport:** TCP
- Proxy Servers:** A table with columns Address, Port, Administration, and an action column. The first row shows Address: 10.80.100.24, Port: 5060, Administration: Administration, and a Remove button.
- Additional Proxy Server:** A link to add more proxy servers.
- Listener Port:** 5060
- SIP Domain:** avaya.com
- P-Asserted-Identity:** (empty field)
- Call Capacity:** Maximum Simultaneous Calls: 10. Radio buttons for 'All Calls can be either inbound or outbound' (selected) and 'Configure number of inbound and outbound calls allowed'.
- Buttons:** Save, Apply, Cancel, Help.

Address	Port	Administration	
10.80.100.24	5060	Administration	Remove

5.5. Setup Self Service Applications

Under System Configuration → Applications, add the Application URL, the Speech Servers configured, and the DNIS number to access the application that will be used in the sample configuration.

As shown below for the sample configuration, the following values were entered:

- url to the VP Bank application:
http://10.80.100.55:8080/VPBank/Start
- DNIS of 5222000

AVAYA Welcome, administrator
Last logged in yesterday at 3:39:38 PM MST

Voice Portal 5.0 (VoicePortal) Home ? Help Logoff

Expand All | Collapse All

You are here: [Home](#) > [System Configuration](#) > [Applications](#) > [Change Application](#)

Change Application

Use this page to change the configuration of a VoiceXML or CCXML application.

Name: VP_Bank
Enable: ☒ Yes ☐ No
MIME Type: VoiceXML
VoiceXML URL: **Verify**

Speech Servers

ASR: <input type="text" value="Nuance"/>	TTS: <input type="text" value="Nuance"/>
Languages: <input type="text" value="English(USA) en-us"/>	Voices: <input type="text" value="English(USA) en-US Jennifer F"/>

Application Launch

Type: ☒ Inbound ☐ Inbound Default ☐ Outbound

☒ Number ☐ Number Range ☐ URI

Called Number: **Add** **Remove**

Speech Parameters

Reporting Parameters

Advanced Parameters


Save **Apply** **Cancel** **Help**

6. Verification Steps

This section provides the tests that can be performed on Voice Portal, Communication Manager and Session Manager to verify proper configuration of these systems.

6.1. Verify Avaya Aura™ Session Manager Configuration

Expand the Session Manager menu on the left and click SIP Entity Monitoring. Verify all SIP Entity Links are operational as shown below:

Avaya Aura™ System Manager 5.2

Welcome, **admin** Last Logged on at Dec. 14, 2009 1:45 PM[Help](#) [Log off](#)

Home / Session Manager / System Status / SIP Entity Monitoring

Asset Management

Communication System Management

User Management

Monitoring

Network Routing Policy

Security

Applications

Settings

Session Manager

- Session Manager Administration
- Network Configuration
- Device and Location Configuration
- Application Configuration
- System Status
 - System State Administration
 - SIP Entity Monitoring
 - Managed Bandwidth Usage
 - Security Module Status
 - Data Replication Status
 - RegistrationSummary
 - User Registrations
- System Tools

SIP Entity Link Monitoring Status Summary

This page provides a summary of Session Manager SIP entity link monitoring status.

Entity Link Status for All Session Manager Instances

[Refresh](#)

Session Manager Name	Entity Links Down/Total	Entity Links Partially Down	SIP Entities - Monitoring Not Started	SIP Entities - Not Monitored
ASM1-DR	0/7	0	0	0
ASM2-DR	0/0	0	0	0


All Monitored SIP Entities

[Refresh](#)

7 ItemsFilter: [Enable](#)

SIP Entity Name
IPO 500
Nortel-Node_Server
SB300-G450-FS
SB730-1
SB730-2
SIL-DR-MAS1
VPMS

Select the corresponding SIP Entity for the VP system and verify the link is up as shown below:

Avaya Aura™ System Manager 5.2

Welcome, **admin** Last Logged on at Dec. 15, 2009 2:03 PM[Help](#) [Log off](#)

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

Asset Management

Communication System Management

User Management

Monitoring

Network Routing Policy

Security

Applications

Settings

Session Manager

- Session Manager Administration
- Network Configuration
- Device and Location Configuration
- Application Configuration
- System Status
 - System State Administration
 - SIP Entity Monitoring
 - Managed Bandwidth Usage
 - Security Module Status
 - Data Replication Status
 - RegistrationSummary
 - User Registrations
- System Tools

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: [VPMS](#)

[Refresh](#) [Summary View](#)

1 ItemFilter: [Enable](#)

Details	Session Manager Name	SIP Entity Resolved IP	Port	Proto.	Conn. Status	Reason Code	Link Status
<input type="checkbox"/> Show	ASM1-DR	10.80.100.54	5060	TCP	Up	200 OK	Up

DH Reviewed:
SPOC 01/18/2010

Solution Interoperability Lab Application Notes
©2010 Avaya Inc. All Rights Reserved.

47 of 57
SM5-2wVP-CM.doc

Verify the overall system status for the specific Session Manager as shown below:

AVAYA

Avaya Aura™ System Manager 5.2

Welcome, **admin** Last Logged on at Dec. 15, 2009 2:03 PM
[Help](#) [Log off](#)

Home / Session Manager / System Status / System State Administration

Asset Management

Communication System Management

User Management

Monitoring

Network Routing Policy

Security

Applications

Settings

Session Manager

Session Manager Administration

Network Configuration

Device and Location Configuration

Application Configuration

System Status

System State

System State Administration

This page shows the current service and management state of configured Session Managers. You can use this page to make state changes in the context of an upgrade or necessary maintenance.

Session Manager Instances

[Refresh](#) [Management State](#) [Service State](#) [Shutdown System](#)

2 Items

<input type="checkbox"/>	Session Manager	Management State	Service State	Last Service State Change	Active Call Count	Version
<input type="checkbox"/>	ASM1-DR	Management Enabled	Accept New Service	No last service state change	1	Development Patch on Version 5.2.0.0 05-Nov-09 14:55
<input type="checkbox"/>	ASM2-DR	Management Enabled	Accept New Service	Wed Nov 18 15:13:46 MST 2009	0	5.2.0.1.520017 - 11-18-2009

Select : All, None (0 of 2 Selected)

Verify the status of the Security Module (SM 100 card) for the specific Session Manager as shown below:

AVAYA

Avaya Aura™ System Manager 5.2

Welcome, **admin** Last Logged on at Jan. 04, 2010 1:38 PM
[Help](#) [Log off](#)

Home / Session Manager / System Status / Security Module Status

Asset Management

Communication System Management

User Management

Monitoring

Network Routing Policy

Security

Applications

Settings

Session Manager

Session Manager Administration

Network Configuration

Device and Location Configuration

Application Configuration

System Status

System State Administration

SIP Entity Monitoring

Managed Bandwidth Usage

Security Module Status

Data Replication Status

RegistrationSummary

User Registrations

System Tools

Security Module Status

This page allows you to view the status of each Session Manager's Security Module and to perform certain actions.

Security Module Statistics

[Refresh](#)

Stat Name	ASM1-DR	ASM2-DR
Security Module Deployment	Up	Up
IP Address	10.80.100.24	10.80.100.26
Network Mask	255.255.255.0	255.255.255.0
Default Gateway	10.80.100.1	10.80.100.1
Interface Name	eth0	eth0
Name Servers	192.11.13.2	192.11.13.2
DNS Search	---	---
Call Control PHB	46	46
Speed & Duplex	Auto	Auto
VLAN	---	---
QOS	---	---
Certificate Used	Default Certificate (Issued By SIP CA)	Default Certificate (Issued By SIP CA)
Trusted Hosts (expected/actual)	8/8	0/0

Security Module Actions

[Security Module Reset](#) [Synchronize Security Module](#) [Security Module Certificate](#)

System Name
<input type="radio"/> ASM1-DR
<input type="radio"/> ASM2-DR

Select : None

Finally, verify the data replication status as shown below:



- ▶ Asset Management
- ▶ Communication System Management
- ▶ User Management
- ▶ Monitoring
- ▶ Network Routing Policy
- ▶ Security
- ▶ Applications
- ▶ Settings
- ▼ Session Manager
 - Session Manager Administration
 - ▶ Network Configuration
 - ▶ Device and Location Configuration
 - ▶ Application Configuration
- ▼ System Status
 - System State Administration
 - SIP Entity Monitoring
 - Managed Bandwidth Usage
 - Security Module Status
 - Data Replication Status**
 - RegistrationSummary
 - User Registrations
- ▶ System Tools

Shortcuts

- [Change Password](#)
- [Help for Data Replication](#)

Session Manager Downward Data Replication Status

This page allows you to view Session Manager downward data replication statistics and run tests.

Master Database and Session Manager Replica Database Statistics

Stat Name	Master	ASM1-DR (replica)	ASM2-DR (replica)
Records Currently in Database	1062	1062	1062
Records Pending Update	0	0	0
Modifications	1080	44	15962
Modifications Resulting from Audits	1939	0	0
Failed Modifications (replica only)	N/A	0	0
Failed Modifications Resulting from Audit (replica only)	N/A	0	0
Elapsed Time Since Last Update/Audit (Days H:M:S)	00:00:00	00:06:35	00:04:28
Elapsed Time Since Last Update/Audit Requiring Modifications (Days H:M:S)	00:03:00	01:51:52	26 23:44:45
Last JMS Message Sent (master) / Received (replica)	Dec 15, 2009 2:43:56 PM MST	Dec 15, 2009 2:43:56 PM MST	Dec 15, 2009 2:43:56 PM MST
Last JMS Message Received (master) / Sent (replica)	Dec 15, 2009 2:42:28 PM MST	Dec 15, 2009 2:40:21 PM MST	Dec 15, 2009 2:42:28 PM MST
JMS Connection Status	OK	OK	OK
Test String Value	545454	545454	545454
Test String Last Update Time	Nov 12, 2009 10:25:59 AM MST	Nov 12, 2009 10:25:59 AM MST	Nov 12, 2009 10:25:59 AM MST

New Master Test String Value

6.2. Verify Voice Portal Configuration

Verify the correct licenses for the VP system by accessing the Licensing link as shown below:

Welcome, administrator
Last logged in yesterday at 3:39:38 PM MST

Voice Portal 5.0 (VoicePortal)

Home
Help
Logoff

Expand All | Collapse All

User Management
Roles
Users
Login Options

Real-Time Monitoring
System Monitor
Active Calls
Port Distribution

System Maintenance
Audit Log Viewer
Trace Viewer
Log Viewer
Alarm Manager

System Management
MPP Manager
Software Upgrade
System Backup

System Configuration
Alarm Codes
Alarm/Log Options
Applications
MPP Servers
Report Data
SNMP
Speech Servers
VoIP Connections
VPMS Servers

Security
Certificates
Licensing

Reports
Standard
Custom
Scheduled

You are here: [Home](#) > Security > Licensing

Licensing

This page displays the Voice Portal license information that is currently in effect. Voice Portal uses Avaya License Manager (WebLM) to control the number of telephony ports that are used.

License Information

License Server URL:	https://10.80.100.54:8443/WebLM/LicenseServer
Telephony Ports:	100
Non Media Ports:	0
Announcement Ports:	0
ASR Connections:	100
TTS Connections:	100
Video Server Connections:	100
Version:	5
Last Changed:	12/7/09 9:53:46 AM MST
Last Successful Poll:	12/15/09 2:18:43 PM MST

License Settings

License Server URL:

	Minimum	Maximum
Telephony Ports:	<input type="text" value="0"/>	<input type="text" value="5,000"/>
Non Media Ports:	<input type="text" value="0"/>	<input type="text" value="0"/>
Announcement Ports:	<input type="text" value="0"/>	<input type="text" value="0"/>

Verify the application has been correctly configured by selecting the sample VP bank application and selecting the “Verify” option. If the system has been correctly configured, a separate window should be displayed as shown below:

Starting application : VPbank

Application Startup Parameters

AAI	<input type="text"/>
ANI	<input type="text"/>
DNIS	<input type="text"/>
Protocol Name	<input type="text"/>
Protocol Version	<input type="text"/>
UUI	<input type="text"/>
Call Tag	<input type="text"/>
Channel	<input type="text"/>
VP-Called Extension	<input type="text"/>
VP-Coverage Reason	<input type="text"/>
VP-Coverage Type	<input type="text"/>
VP-RDNIS	<input type="text"/>
Redirect URI	<input type="text"/>
Redirect Presentation Info	<input type="text"/>
Redirect Screening Info	<input type="text"/>

Use the **Real-Time Monitoring → System Monitor** or **System Management → MPP Manager** to ensure MPPs are online, running and receiving calls as shown below:

AVAYA Welcome, administrator
Last logged in yesterday at 3:39:38 PM MS

Voice Portal 5.0 (VoicePortal) Home ? Help Logoff

Expand All | Collapse All

User Management
Roles
Users
Login Options

Real-Time Monitoring
System Monitor
Active Calls

System Maintenance
Port Distribution
Audit Log Viewer
Trace Viewer
Log Viewer
Alarm Manager

System Management
MPP Manager
Software Upgrade
System Backup

System Configuration
Alarm Codes
Alarm/Log Options
Applications
MPP Servers
Report Data
SNMP
Speech Servers
VoIP Connections
VPMS Servers

Security
Certificates
Licensing

Reports
Standard
Custom
Scheduled

You are here: [Home](#) > System Management > MPP Manager

MPP Manager (12/15/09 2:13:38 PM MST) Refresh

This page displays the current state of each MPP in the Voice Portal system. To enable the state and mode commands, select one or more MPPs. To enable the mode commands, the selected MPPs must also be stopped.

Last Poll: 12/15/09 2:13:38 PM MST

	Server Name	Mode	State	Config	Auto Restart	Restart Schedule		Active Calls	
						Today	Recurring	In	Out
<input type="checkbox"/>	MPP1	Online	Running	OK	Yes	No	None	0	0

State Commands
Start Stop Restart Reboot Halt Cancel

Restart/Reboot Options
☐ One server at a time
☒ All selected servers at the same time

Mode Commands
Offline Test Online

Help

6.3. Verify Avaya Aura™ Communication Manager Access Element Configuration

Verify the status of the SIP trunk group by using the “**status trunk n**” command, where “**n**” is the trunk group number administered in **Section 2.4.2**. Verify that all trunks are in the “in-service/idle” state as shown below:

```
status trunk 20
```

TRUNK GROUP STATUS			
Member	Port	Service State	Mtce Connected Ports
			Busy0020/001 T00057 in-service/idle
no			
0020/002	T00058	in-service/idle	no
0020/003	T00059	in-service/idle	no
0020/004	T00060	in-service/idle	no
0020/005	T00061	in-service/idle	no
0020/006	T00062	in-service/idle	no
0020/007	T00063	in-service/idle	no
0020/008	T00064	in-service/idle	no
0020/009	T00065	in-service/idle	no
0020/010	T00066	in-service/idle	no

Verify the status of the SIP signaling groups by using the “**status signaling-group n**” command, where “**n**” is the signaling group number administered in **Section 2.4.1**.

Verify the signaling group is “in-service” as indicated in the **Group State** field shown below:

```
status signaling-group 20
                        STATUS SIGNALING GROUP

      Group ID: 20
      Group Type: sip
      Signaling Type: facility associated signaling
      Group State: in-service

Active NCA-TSC Count: 0
Active CA-TSC Count: 0
```

6.4. Verification Scenarios

For all scenarios, perform the following steps:

- Step 1: Log in an agent on the Communication Manager Access Element.
- Step 2: Verify caller is able to hear the appropriate prompts in the VP application.
- Step 3: Select the option to talk to an agent and verify call is delivered to the agent.

6.4.1. Call Scenarios Verified

- Basic Call flow from external PSTN phone
 - Verify Communication Manager is able to route external call to VP application through the Session Manager.
 - Verify call is successfully transferred to the agent
- Basic Call flow from internal Avaya phones (includes both digital and IP stations)
 - Verify Communication Manager is able to route internal call to VP application through the Session Manager.
 - Verify call is successfully transferred to the agent
- Basic Call flow from SIP endpoints registered to Session Manager
 - Verify Communication Manager is able to route call from SIP endpoint to VP application through the Session Manager.
 - Verify call is successfully transferred to the agent
- Multiple Calls
 - Verify VP application is able to support multiple, simultaneous calls.
 - Verify first call can still be successfully transferred to the agent
 - Verify other calls are queued
- Queuing
 - Place multiple, simultaneous calls to VP application
 - Verify first call is successfully transferred to the agent
 - Verify calls queued for > 5 minutes are delivered to agent once agent becomes available

6.4.2. Verify status on Communication Manager Access Element

Use the Communication Manager SAT command, '**list trace tac #**', where **tac #** is the trunk access code defined in **Section 2.4.2** to trace trunk group activity for the SIP trunk between the Session Manager and Communication Manager as shown below:

list trace tac #20		Page 1
LIST TRACE		
time	data	
17:35:44	dial 5222000 route:UDP HNPA ARS	
17:35:44	term trunk-group 20 cid 0x200	
17:35:44	dial 5222000 route:UDP HNPA ARS	
17:35:44	route-pattern 20 preference 1 cid 0x200	
17:35:44	seize trunk-group 20 member 10 cid 0x200	
17:35:44	Setup digits 5222000	
17:35:44	Calling Number & Name NO-CPNumber H.323 4621 IP	
17:35:44	Proceed trunk-group 20 member 10 cid 0x200	
17:35:44	G711MU ss:off ps:20	
	rgn:1 [10.80.100.54]:23374	
	rgn:1 [10.80.111.13]:9660	
17:35:44	xoip options: fax:Relay modem:off tty:US uid:0x50042	
	xoip ip: [10.80.111.13]:9660	
17:35:44	active trunk-group 20 member 10 cid 0x200	
17:35:44	G711MU ss:off ps:20	

Use the Communication Manager SAT command, '**list trace vdn**' where **vdn** is the VDN number defined in **Section 2.7.1** to trace calls from the VP Application are correctly processed on the Communication Manager Access Element as shown below:

list trace vdn 5221000	
LIST TRACE VDN	
time	vec prt st data
17:36:57	0 0 ENTERING TRACE cid 515
17:36:57	1000 1 vdn e5221000 bsr appl 0 strategy 1st-found override n
17:36:57	1000 1 queue-to
17:36:57	1000 1 queueing to skill 522 pri h
17:36:57	1000 1 Local Agent Preference=n
17:36:57	1000 1 Agent Login ID: 50001 Logged in at station: 4001000
17:36:57	1000 1 LEAVING VECTOR PROCESSING cid 515
17:36:57	1000 1 TRACE COMPLETE cid 515

Use the Communication Manager SAT command, "**mon bcms system**" to verify calls are in queue or delivered to agents as shown by screen below.

monitor bcms system										
BCMS SYSTEM STATUS										
Date: 13:33 THU DEC 10 2009										
SKILL NAME	CALLS WAIT	OLDEST CALL	AUG SPEED ANS	AVAIL AGENT	ABAND CALLS	AUG ABAND TIME	ACD CALLS	AUG TALK TIME	AUG AFTER CALL	% IN SERV LEVL
UP Agents	2	0:09	0:00	0	0	0:00	3	0:26	0:00	67

6.4.3. Verify status on Voice Portal

- Verify the prompts from the application can be heard.
- Go to the VPMS webpage “Real-Time Monitoring → System Monitor → Active Calls” to ensure MPPs are online, running and receiving calls as shown below:

Active Calls (12/10/09 11:09:33 AM MST)



This page displays the status of all the active calls being handled by the Voice Portal system.

Total Active Calls: 3									Last Poll: 12/10/09 11:09:33 AM MST		
Port ↕	Port Group ↕	Protocol ↕	Call Type ↕	MPP Server ↕	Start Time ↕	Calling Number/URI ↕	Called Number/URI ↕	Application ↕	ASR Server ↕	TTS Server ↕	
1	sm100-silasm1	SIP_Trunk	Inbound	MPP1	12/10/09 11:08:52 AM MST	anonymous	tel:5222000	VP_Bank	SpeechSvr	TextServer	
2	sm100-silasm1	SIP_Trunk	Inbound	MPP1	12/10/09 11:09:09 AM MST	tel:6663000	tel:5222000	VP_Bank	SpeechSvr	TextServer	
3	sm100-silasm1	SIP_Trunk	Inbound	MPP1	12/10/09 11:09:26 AM MST	anonymous	tel:5222000	VP_Bank	SpeechSvr	TextServer	

6.4.4. Verify status on Session Manager

The SIP Tracing Viewer on System Manager can be used to display SIP message traces between Session Manager and SIP entities, based on configurable filters. For more information on how to configure SIP tracing, see Maintaining and Troubleshooting Avaya Aura™ Session Manager, Doc ID 03-603325.

7. Acronyms

ARS	Automatic Route Selection (Routing on Communication Manager)
ASR	Automatic Speech Recognition
BCMS	Basic Call Management System (used for monitoring ACD calls)
CLAN	Control LAN (Control Card in Communication Manager)
DCP	Digital Communications Protocol
DD	Avaya Voice Portal Dialog Designer
DNIS	Dialed Number identification Service
DTMF	Dual Tone Multi Frequency
FQDN	Fully Qualified Domain Name (hostname for Domain Naming Resolution)
IMS	IP Multimedia Subsystem
IP	Internet Protocol
IPSI	IP-services interface (Control Card in Communication Manager)
IVR	Interactive Voice Response
LAN	Local Area Network
MPP	Media Processing Platform (Voice Portal Server)
MRCP	Media Resource Control Protocol
PSTN	Public Switched Telephone Network
RTP	Real Time Protocol
SAT	System Access Terminal
SIL	Solution Interoperability Lab
SIP	Session Initiation Protocol
SM	Avaya Aura™ Session Manager
SMGR	Avaya Aura™ System Manager
SNMP	Simple Network Management Protocol
SRE	SIP Routing Element
SSH	Secure Shell
SSL	Secure Socket Layer
TAC	Trunk Access Code (Communication Manager Trunk Access)
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TLS	Transport Layer Security
TTS	Text To Speech
URE	User Relation Element
URL	Uniform Resource Locator
VDN	Vector Directory Number
VP	Voice Portal
VP 1 st	Voice Portal First
VPMS	Voice Portal Management Server
WAN	Wide Area Network
XML	eXtensible Markup Language

8. Conclusion

These Application Notes describe how to configure the Avaya Aura™ Session Manager, Avaya Aura™ Communication Manager Access Element, Avaya Aura™ Communication Manager operating as a Feature Server, Avaya G650 Media Gateway, and Avaya Voice Portal (VP) to support a Voice Portal First (VP 1st) solution.

Interoperability testing included verification of basic calls to the VP application from several types of endpoints including ability to transfer call to an agent on Communication Manager.

9. Additional References

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

Session Manager

- 1) Avaya Aura™ Session Manager Overview, Doc ID 03-603323, available at <http://support.avaya.com>.
- 2) Installing and Administering Avaya Aura™ Session Manager, Doc ID 03-603324, available at <http://support.avaya.com>.
- 3) Maintaining and Troubleshooting Avaya Aura™ Session Manager, Doc ID 03-603325, available at <http://support.avaya.com>.

Communication Manager

- 4) Hardware Description and Reference for Avaya Aura™ Communication Manager (COMCODE 555-245-207) http://support.avaya.com/elmodocs2/comm_mgr/r4_0/avayadoc/03_300151_6/245207_6/245207_6.pdf
- 5) SIP Support in Avaya Aura™ Communication Manager Running on Avaya S8xxx Servers, Doc ID 555-245-206, May 2009, available at <http://support.avaya.com>.
- 6) Administering Avaya Aura™ Communication Manager, Doc ID 03-300509, May 2009, available at <http://support.avaya.com>.
- 7) Administering Avaya Aura™ Communication Manager as a Feature Server, Doc ID 03-603479, November 2009, available at <http://support.avaya.com>

Voice Portal

- 8) Administering Voice Portal, available at <http://support.avaya.com>
- 9) Configuring Avaya Voice Portal with Avaya Communication Manager and Designing a Sample Speech Application using Dialog Designer – Issue 1.0 : <http://www.avaya.com/master-usa/en-us/resource/assets/applicationnotes/voiceportal.pdf>

Avaya Application Notes

- 1) Voice Portal First Solution: Configuring Avaya Aura™ Session Manager with Avaya G860 High Density Trunk Gateway, Avaya Aura™ Communication Manager and Avaya Voice Portal – Issue 1.0, available at <http://www.avaya.com>
- 2) Configuring 9600-Series SIP Phones on Avaya Aura™ Session Manager Release 5.2, available at <http://www.avaya.com>.

©2010 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 Solution & Interoperability Test Lab at interoplabinotes@list.avaya.com