



## **Avaya Solution & Interoperability Test Lab**

---

# **Application Notes for DuVoice DV2000 7.2 with Avaya Aura® Communication Manager 10.1 and Avaya Aura® Session Manager 10.1 – Issue 1.0**

### **Abstract**

These Application Notes describe the configuration steps required for the DuVoice DV2000 7.2 to interoperate with Avaya Aura® Communication Manager 10.1 and Avaya Aura® Session Manager 10.1. DuVoice DV2000 is a hospitality messaging system.

In the compliance testing, DuVoice DV2000 used the Property Management System interface from Avaya Aura® Communication Manager and the SIP trunk interface from Avaya Aura® Session Manager to support hospitality operations.

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

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

# 1. Introduction

These Application Notes describe the configuration steps required for the DuVoice DV2000 7.2 to interoperate with Avaya Aura® Communication Manager 10.1 and Avaya Aura® Session Manager 10.1. DV2000 is a hospitality system.

In the compliance testing, DV2000 used the Property Management System (PMS) interface from Communication Manager and the SIP trunk interface from Session Manager to support hospitality operations.

DV2000 is typically installed onsite at the customer hotel premise and uses a local third-party PMS system to initiate hospitality functions. In the compliance testing, the DuVoice Hospitality Tester tool on DV2000 was used in place of a real PMS system to initiate hospitality requests.

The PMS interface is used by DV2000 to provide check-in, check-out, room move, controlled restriction, guest information change, and housekeeping status. The Hospitality Tester tool is used to initiate all PMS exchanges from DV2000 except housekeeping status. Updates on housekeeping status are initiated by hotel personnel by dialing pertinent feature access codes from the guest telephones, and with Communication Manager notifying DV2000 via PMS.

The SIP trunk interface is used by DV2000 to provide automated attendant, voicemail, wakeup call, and Message Waiting Indicator (MWI). Incoming calls to DV2000 are delivered over the SIP trunk to DV2000. DV2000 uses the SIP packets to determine type of call and hence the service to provide, such as automated attendant for incoming calls, voicemail coverage for redirected calls, voicemail retrieval by subscribers, scheduling of wakeup calls from guest and/or staff telephones. The activation and deactivation of MWI for voicemail users are accomplished by DV2000 via use of SIP NOTIFY. All SIP communications on DV2000 are supported using the Dialogic Host Media Processing SIP stack.

For the automated attendant feature, incoming calls to DV2000 are routed via SIP trunk to DV2000. DV2000 played appropriate greeting announcement and used the input DTMF digits along with the SIP REFER method to perform unsupervised transfer of calls to appropriate staff destinations on Communication Manager.

In the compliance testing, subscribers of DV2000 voicemail consisted of all staff and guest users on Communication Manager. DV2000 is configured as a SIP message center and the Call Coverage feature from Communication Manager is used to redirect calls to DV2000 via SIP trunk.

Upon guest manually making a request to staff for do not disturb, the Hospitality Tester tool is used in the compliance testing to set controlled restriction for the guest telephone to termination, thus preventing all calls terminating to the guest telephone.

## 2. General Test Approach and Test Results

The feature test cases were performed manually. Calls were made from the PSTN and from local users to DV2000, for various hospitality features such as automated attendant, voicemail retrieval, etc. The Hospitality Tester tool was used to manually initiate check-in, check-out, controlled restriction, room moves, guest information change, do not disturb, and for monitoring of housekeeping status.

The serviceability test cases were performed manually by disconnecting and reconnecting the Ethernet connection to DV2000 and disrupting the PMS link.

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

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

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

For the testing associated with these Application Notes, the interfaces between Avaya and DuVoice did not include use of any specific encryption features as requested by DuVoice.

## 2.1. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability testing.

The feature testing focused on verifying the following on DV2000:

- Proper handling of SIP message exchanges including OPTIONS, G.711 codec, media shuffling, session refresh, DTMF, REFER, and NOTIFY.
- Proper handling of PMS operations including check-in, check-out, room move, guest information change, housekeeping status, and controlled restriction including termination setting for do not disturb.
- Automated attendant navigation for incoming trunk calls, such as transfer to staff.
- Voicemail recording and retrieval, with proper MWI activation/deactivation for users with analog, digital, H.323, and SIP telephone types.
- Scheduling and delivering of wake-up call requests, including retried attempts.

The serviceability testing focused on verifying the ability of DV2000 to recover from adverse conditions, such as disconnecting and reconnecting the Ethernet connection to DV2000 and disrupting the PMS connection.

## 2.2. Test Results

All test cases were executed, and the following were observations on DV2000:

- DV2000 does not support swap of two occupied rooms.
- The Hospitality Tester tool did not send the right restriction value for restriction levels 5-7 therefore reflection of these restriction levels was not able to be verified on Communication Manager. This should not occur in customer environments with use of actual third-party PMS system.
- The Hospitality Tester tool can send the wrong restriction value to Communication Manager for do not disturb activation/deactivation depending on the guest current restriction level. The workaround used in testing was to set guest restriction to the no restriction level prior to activating do not disturb.

## 2.3. Support

Technical support on DV2000 can be obtained through the following:

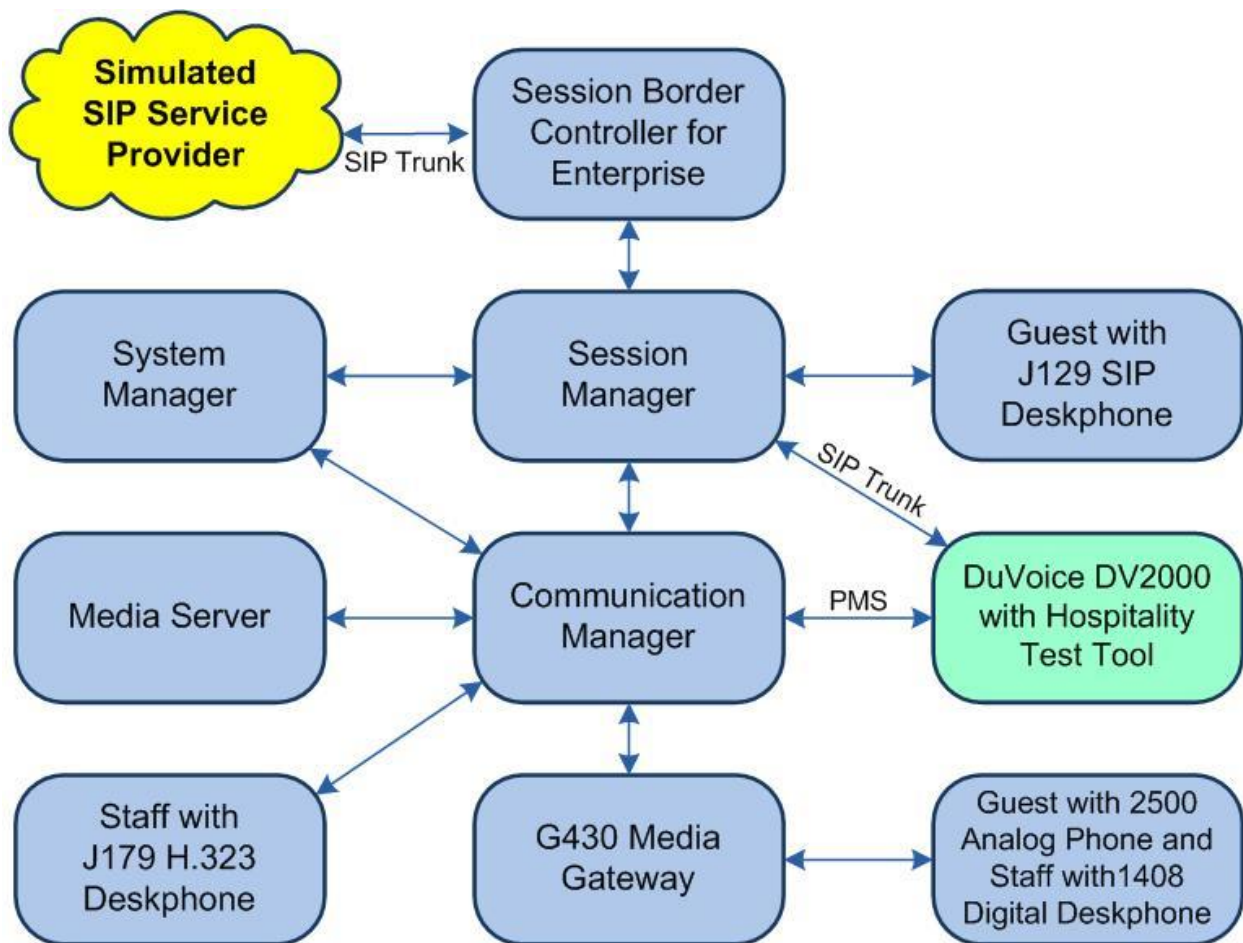
- **Phone:** (425) 250-2393
- **Email:** <mailto:support@communicado-inc.comsupport@duvoice.com>

### 3. Reference Configuration

The configuration used for the compliance testing is shown in **Figure 1**. In the compliance testing, the number **53000** is assigned as main number for DV2000, and the pertinent domain name for the network is **dr220.com**.

The Communication Manager resources used in the compliance testing are shown in the table below.

Device Type	Extension
Staff Station	65001 (H.323), 64001 (Digital)
Guest Station	66001 (SIP), 63001 (Analog)



**Figure 1: Compliance Testing Configuration**

## 4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya Aura® Communication Manager in Virtual Environment	10.1 (10.1.0.1.0.974.27372)
Avaya G430 Media Gateway	42.8.0
Avaya Aura® Media Server in Virtual Environment	10.1.0.77
Avaya Aura® Session Manager in Virtual Environment	10.1 (10.1.0.1.1010105)
Avaya Aura® System Manager in Virtual Environment	10.1 (10.1.0.1.0614394)
Avaya J179 IP Deskphone (H.323)	6.8.5.3.2
Avaya J129 IP Deskphone (SIP)	4.0.13.0.6
Avaya 1408 Digital Deskphone (Digital)	48.02
2500YMGK Analog Phone	NA
DuVoice DV2000 on Microsoft Windows 10 <ul style="list-style-type: none"><li>• Dialogic PowerMedia HMP</li><li>• Hospitality Tester</li></ul>	7.2.33 Pro 3.0.533 7.2.33

## 5. Configure Avaya Aura® Communication Manager

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

- Verify license
- Administer node names
- Administer IP services
- Administer system parameters hospitality
- Administer feature access codes
- Administer class of service
- Administer codec set
- Administer network region
- Administer SIP trunk group
- Administer SIP signaling group
- Administer SIP trunk group members
- Administer route pattern
- Administer private numbering
- Administer uniform dial plan
- Administer AAR analysis
- Administer hunt group
- Administer coverage path
- Administer stations

In the compliance testing, the Avaya endpoints used encrypted signaling connections and encrypted media wherever applicable. A separate set of codec set, network region, trunk group, and signaling group was created for integration with DV2000.

## 5.1. Verify License

Log into the System Access Terminal (SAT) to verify that the Communication Manager license has proper permissions for features illustrated in these Application Notes. Use the **display system-parameters customer-options** command.

Navigate to **Page 2** and verify that there is sufficient capacity for SIP trunks by comparing the **Maximum Administered SIP Trunks** field value with the corresponding value in the **USED** column.

The license file installed on the system controls the maximum permitted. If there is insufficient capacity, contact an authorized Avaya sales representative to make the appropriate changes.

display system-parameters customer-options		Page	2 of 12
OPTIONAL FEATURES			
IP PORT CAPACITIES		USED	
Maximum Administered H.323 Trunks:		12000	10
Maximum Concurrently Registered IP Stations:		18000	1
Maximum Administered Remote Office Trunks:		12000	0
Max Concurrently Registered Remote Office Stations:		18000	0
Maximum Concurrently Registered IP eCons:		414	0
Max Concur Reg Unauthenticated H.323 Stations:		100	0
Maximum Video Capable Stations:		41000	1
Maximum Video Capable IP Softphones:		18000	2
<b>Maximum Administered SIP Trunks:</b>		<b>40000</b>	<b>50</b>
Max Administered Ad-hoc Video Conferencing Ports:		24000	0
Max Number of DS1 Boards with Echo Cancellation:		999	0

Navigate to **Page 5** and verify that the **Hospitality (Basic)** and **Hospitality (G3V3 Enhancements)** customer option are set to **y**. If the options are not set to **y**, then contact the Avaya sales team or business partner for a proper license file.

display system-parameters customer-options		Page	5 of 12
OPTIONAL FEATURES			
Emergency Access to Attendant? y		IP Stations? y	
Enable 'dadmin' Login? y			
Enhanced Conferencing? y		ISDN Feature Plus? n	
Enhanced EC500? y		ISDN/SIP Network Call Redirection? y	
Enterprise Survivable Server? n		ISDN-BRI Trunks? y	
Enterprise Wide Licensing? n		ISDN-PRI? y	
ESS Administration? y		Local Survivable Processor? n	
Extended Cvg/Fwd Admin? y		Malicious Call Trace? y	
External Device Alarm Admin? y		Media Encryption Over IP? y	
Five Port Networks Max Per MCC? n		Mode Code for Centralized Voice Mail? n	
Flexible Billing? n			
Forced Entry of Account Codes? y		Multifrequency Signaling? y	
Global Call Classification? y		Multimedia Call Handling (Basic)? y	
<b>Hospitality (Basic)? y</b>		Multimedia Call Handling (Enhanced)? y	
<b>Hospitality (G3V3 Enhancements)? y</b>		Multimedia IP SIP Trunking? y	
IP Trunks? y			



## 5.2. Administer Node Names

Use the **change node-names ip** command to add an entry for DV2000. In this case, **DV2000** and **10.64.101.208** are entered as **Name** and **IP Address**. The actual node name and IP address may vary.

Note the **Name** and **IP Address** of the processor or an existing C-LAN circuit pack that will be used for PMS connectivity with DV2000, in this case **procr** and **10.64.101.236**.

Also note the **Name** and **IP Address** of the existing entry for Session Manager that will be used for SIP trunk connectivity with DV2000, in this case **sm7-sig** and **10.64.101.238**.

change node-names ip		Page 1 of 2
		IP NODE NAMES
Name	IP Address	
G430	192.168.200.43	
aes7	10.64.101.239	
clan	10.64.125.32	
default	0.0.0.0	
gateway	10.64.125.1	
ms7	10.64.101.233	
<b>procr</b>	<b>10.64.101.236</b>	
procr6	::	
<b>sm7-sig</b>	<b>10.64.101.238</b>	
<b>DV2000</b>	<b>10.64.101.208</b>	

## 5.3. Administer IP Services

Use the **change ip-services** command to add an entry for PMS connectivity with DV2000. Enter the following values for the specified fields and retain the default values for the remaining fields.

- **Service Type:** “PMS”
- **Local Code:** Node name of the processor or C-LAN circuit pack from **Section 5.2**.
- **Local Port:** “0”
- **Remote Node:** Node name of DV2000 from **Section 5.2**.
- **Remote Port:** An available port in the range of 5000-64500, in this case “5000”.

change ip-services					Page	1 of	3
			IP SERVICES				
Service Type	Enabled	Local Node	Local Port	Remote Node	Remote Port		
AESVCS	y	procr	8765				
PMS		procr	0	DV2000	5000		

## 5.4. Administer System Parameters Hospitality

Enter the **change system-parameters hospitality** command to modify hospitality related system parameters. Enter all values as shown below.

```
change system-parameters hospitality                                     Page 1 of 3
                                HOSPITALITY

                                Message Waiting Configuration: act-pms
                                Controlled Restrictions Configuration: act-pms
                                Housekeeper Information Configuration: act-pms
                                Number of Housekeeper ID Digits: 0
                                PMS Log Endpoint:
                                Journal/Schedule Endpoint:
                                Client Room Coverage Path Configuration: act-nopms
                                Default Coverage Path for Client Rooms:
                                Forward PMS Messages to Intuity Lodging? n

                                PMS LINK PARAMETERS
                                PMS Endpoint: PMS
                                PMS Protocol Mode: transparent ASCII mode? y
                                Seconds before PMS Link Idle Timeout: 20
                                Milliseconds before PMS Link Acknowledgement Timeout: 1500
                                PMS Link Maximum Retransmissions: 3
                                PMS Link Maximum Retransmission Requests: 3
                                Take Down Link for Lost Messages? n
```

Navigate to **Page 3** and set the desired definitions for all room states as shown below.

```
change system-parameters hospitality                                     Page 3 of 3
                                ROOM STATES                                HOSPITALITY

                                Definition for Rooms in State 1: Clean
                                Definition for Rooms in State 2: Dirty
                                Definition for Rooms in State 3: Clean and Checked
                                Definition for Rooms in State 4: Dirty and Checked
                                Definition for Rooms in State 5: Cleanest
                                Definition for Rooms in State 6: Dirtiest

                                HOSPITALITY FEATURES
                                Suite Check-in? n
                                Cancel Do-Not-Disturb for Wakeup Calls? y
```

## 5.5. Administer Feature Access Codes

Enter the **change feature-access-codes** command and navigate to **Page 8**. Set the housekeeping status access codes for client room to available codes. These codes are dialed by the hotel personnel to update the housekeeping status for guest rooms.

change feature-access-codes		Page 8 of 10
FEATURE ACCESS CODE (FAC)		
Hospitality Features		
Automatic Wakeup Call Access Code:		
Housekeeping Status (Client Room)	Access Code: 151	
Housekeeping Status (Client Room)	Access Code: 152	
Housekeeping Status (Client Room)	Access Code: 153	
Housekeeping Status (Client Room)	Access Code: 154	
Housekeeping Status (Client Room)	Access Code: 155	
Housekeeping Status (Client Room)	Access Code: 156	
Housekeeping Status (Station)	Access Code:	
Housekeeping Status (Station)	Access Code:	
Housekeeping Status (Station)	Access Code:	
Housekeeping Status (Station)	Access Code:	
Verify Wakeup Announcement	Access Code:	
Voice Do Not Disturb	Access Code:	

## 5.6. Administer Class of Service

Enter the **change cos** command. For customer systems with enablement of Tenant Partitioning customer option, the pertinent command is **change cos-group n** where **n** is the applicable tenant number. Locate the desired class of service number to be used for integration with DV2000, in this case **3**, and set the corresponding **Client Room** parameter to **y**, as shown below.

This setting enables stations with class of service **3** to support hospitality functions such as check-in and check-out. This class of service will be assigned to all guest stations in **Section 5.18**.

change cos-group 1										Page		1 of		2			
CLASS OF SERVICE		COS Group: 1			COS Name:												
		0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Auto Callback		n	n	y	n	y	n	y	n	y	n	y	n	y	n	y	n
Call Fwd-All Calls		n	y	n	y	y	n	n	y	y	n	n	y	y	n	n	y
Data Privacy		n	y	n	n	n	y	y	y	y	n	n	n	n	y	y	y
Priority Calling		n	y	n	n	n	n	n	n	n	y	y	y	y	y	y	y
Console Permissions		y	y	n	n	n	n	n	n	n	n	n	n	n	n	n	n
Off-hook Alert		n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n
Client Room		n	n	n	y	n	n	n	n	n	n	n	n	n	n	n	n
Restrict Call Fwd-Off Net		y	y	y	y	y	y	y	y	y	y	y	y	y	y	y	y
Call Forwarding Busy/DA		n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n
Personal Station Access (PSA)		n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n
Extended Forwarding All		n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n

## 5.7. Administer Codec Set

Administer a codec set for integration with DV2000. Use the **change ip-codec-set n** command, where **n** is an existing codec set number to use for integration with DV2000.

For **Audio Codec**, enter the pertinent G.711 variant as shown below. Note that G.711 is the only codec type supported by DV2000.

For customer systems with **Media Encryption Over IP** customer option enabled, the **Media Encryption** and **Encrypted SRTCP** parameters will also appear. Retain the default values of **none** and **enforce-unenc-srtcp** as shown below.

change ip-codec-set 3

Page1 of 2

IP MEDIA PARAMETERS

Codec Set: 3

Audio Codec	Silence Suppression	Frames Per Pkt	Packet Size(ms)
1: G.711MU	n	2	20
2:			
3:			
4:			
5:			
6:			
7:			

Media Encryption

Encrypted SRTCP: enforce-unenc-srtcp

1: none

## 5.8. Administer Network Region

Administer a network region for integration with DV2000. Use the **change ip-network-region n** command, where **n** is an existing network region number to use for integration with DV2000.

Enter the following values for the specified fields and retain the default values for the remaining fields.

- **Authoritative Domain:** The SIP domain from **Section 3**.
- **Name:** A descriptive name.
- **Codec Set:** The codec set number from **Section 5.7**.

```
change ip-network-region 3                                     Page 1 of 20
                                     IP NETWORK REGION
Region: 3              NR Group: 3
Location:              Authoritative Domain: dr220.com
Name: DV2000           Stub Network Region: n
MEDIA PARAMETERS      Intra-region IP-IP Direct Audio: yes
Codec Set: 3           Inter-region IP-IP Direct Audio: yes
                      IP Audio Hairpinning? n
UDP Port Min: 2048
UDP Port Max: 3329
DIFFSERV/TOS PARAMETERS
Call Control PHB Value: 46
Audio PHB Value: 46
Video PHB Value: 26
```

Navigate to **Page 4**, and specify the same codec set number to be used for calls with network regions used by guest and staff stations and by the trunk with the PSTN. In the compliance testing, network region **1** was used by the guest and staff stations and by the trunk with the PSTN.

```
change ip-network-region 3                                     Page 4 of 20

Source Region: 3      Inter Network Region Connection Management      I      M
                                                                G      A      t
dst codec direct      WAN-BW-limits      Video      Intervening      Dyn      A      G      c
rgn set      WAN      Units      Total Norm      Prio Shr      Regions      CAC      R      L      e
1      3      y      NoLimit
2
3      3
4
5
6
7
8
```

## 5.9. Administer SIP Trunk Group

Use the **add trunk-group n** command, where **n** is an available trunk group number, in this case **53**. Enter the following values for the specified fields and retain the default values for the remaining fields.

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

<b>add trunk-group 53</b>		Page 1 of 21	
TRUNK GROUP			
Group Number: 53	<b>Group Type: sip</b>	CDR Reports: y	
<b>Group Name: SIP trunk to DV2000</b>	COR: 1	TN: 1	<b>TAC: 1053</b>
Direction: two-way	Outgoing Display? n	Night Service:	
Dial Access? n			
Queue Length: 0			
<b>Service Type: tie</b>	Auth Code? n		
	Member Assignment Method: auto		
	Signaling Group:		
	Number of Members: 0		

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

<b>add trunk-group 53</b>		Page 3 of 4	
TRUNK FEATURES			
ACA Assignment? n	Measured: none	Maintenance Tests? y	
Suppress # Outpulsing? n	<b>Numbering Format: private</b>	UUI Treatment: service-provider	
	Replace Restricted Numbers? n		
	Replace Unavailable Numbers? n		
	Hold/Unhold Notifications? y		
	Modify Tandem Calling Number: no		
Show ANSWERED BY on Display? y			

## 5.10. Administer SIP Signaling Group

Use the **add signaling-group n** command, where **n** is an available signaling group number, in this case **53**. Enter the following values for the specified fields and retain the default values for the remaining fields.

- **Group Type:** “sip”
- **Transport Method:** “tcp”
- **Near-end Node Name:** The C-LAN or “procr” node name from **Section 5.2**.
- **Far-end Node Name:** The node name for Session Manager from **Section 5.2**.
- **Near-end Listen Port:** An available port for integration with DV2000.
- **Far-end Listen Port:** The same port number as in **Near-end Listen Port**.
- **Far-end Network Region:** The network region number from **Section 5.8**.
- **Far-end Domain:** The domain name from **Section 3**.

<b>add signaling-group 53</b>		Page 1 of 2
SIGNALING GROUP		
Group Number: 53	Group Type: sip	
IMS Enabled? n	Transport Method: tcp	
Q-SIP? n		
IP Video? n	Enforce SIPS URI for SRTP? y	
Peer Detection Enabled? y	Peer Server: Others	Clustered? n
Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? n		
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? y		
Near-end Node Name: procr		Far-end Node Name: sm7-sig
Near-end Listen Port: 5053		Far-end Listen Port: 5053
		Far-end Network Region: 3
Far-end Domain: dr220.com		
Incoming Dialog Loopbacks: eliminate		Bypass If IP Threshold Exceeded? n
DTMF over IP: rtp-payload		RFC 3389 Comfort Noise? n
Session Establishment Timer(min): 3		Direct IP-IP Audio Connections? y
Enable Layer 3 Test? n		IP Audio Hairpinning? n
H.323 Station Outgoing Direct Media? n		Initial IP-IP Direct Media? n
		Alternate Route Timer(sec): 6

## 5.11. Administer SIP Trunk Group Members

Use the **change trunk-group n** command, where **n** is the trunk group number from **Section 5.9**. Enter the following values for the specified fields and retain the default values for the remaining fields.

- **Signaling Group:** The signaling group number from **Section 5.10**.
- **Number of Members:** The desired number of members, in this case **4**.

change trunk-group 53			Page 1 of 4		
TRUNK GROUP					
Group Number: 53		Group Type: sip		CDR Reports: y	
Group Name: SIP Trunk to DV2000		COR: 1		TN: 1 TAC: 1053	
Direction: two-way		Outgoing Display? n			
Dial Access? n		Night Service:			
Queue Length: 0					
Service Type: tie		Auth Code? n			
Member Assignment Method: auto					
Signaling Group: 53					
Number of Members: 4					

## 5.12. Administer Route Pattern

Use the **change route-pattern n** command, where **n** is an existing route pattern number to be used to reach DV2000, in this case **53**. Enter the following values for the specified fields and retain the default values for the remaining fields.

- **Pattern Name:** A descriptive name.
- **Grp No:** The SIP trunk group number from **Section 5.9**.
- **FRL:** A level that allows access to this trunk, with 0 being least restrictive.
- **Numbering Format:** "lev0-pvt"

change route-pattern 53													Page 1 of 3	
Pattern Number: 53    Pattern Name: DV2000														
SCCAN? n    Secure SIP? n														
Grp	FRL	NPA	Pfx	Hop	Toll	No.	Inserted						DCS/	IXC
No			Mrk	Lmt	List	Del	Digits						QSIG	
Dgts													Intw	
1:	53	0											n	user
2:												n	user	
3:												n	user	
4:												n	user	
5:												n	user	
6:												n	user	
BCC VALUE		TSC	CA-TSC		ITC BCIE Service/Feature			PARM Sub	Numbering		LAR			
0 1 2 M 4 W		Request							Dgts	Format				
1:	y	y	y	y	y	n	n	rest			lev0-pvt		none	



### 5.13. Administer Private Numbering

Use the **change private-numbering 0** command, to define the calling party number to send to DV2000. Add an entry for the trunk group defined in **Section 5.9**. In the example shown below, all calls originating from a 5-digit extension beginning with **6** and routed to trunk group **53** will result in a 5-digit calling number. The calling party number will be in the SIP “From” header.

change private-numbering 0					Page 1 of 2
NUMBERING - PRIVATE FORMAT					
Ext	Ext	Trk	Private	Total	
Len	Code	Grp(s)	Prefix	Len	
5	6	66		5	Total Administered: 3
5	6	212	30353	10	Maximum Entries: 540
5	6	431	30353	10	
<b>5</b>	<b>6</b>	<b>53</b>		<b>5</b>	

### 5.14. Administer Uniform Dial Plan

This section provides a sample AAR routing used for routing calls with dialed digits **53000** to DV2000. Note that other routing methods may be used. Use the **change uniform-dialplan 0** command and add an entry to specify the use of AAR for routing of digits **53000**, as shown below.

change uniform-dialplan 0					Page 1 of 2
UNIFORM DIAL PLAN TABLE					
					Percent Full: 0
Matching			Insert	Node	
Pattern	Len	Del	Digits	Net Conv	Num
<b>53000</b>	<b>5</b>	<b>0</b>		<b>aar</b>	<b>n</b>

### 5.15. Administer AAR Analysis

Use the **change aar analysis 0** command and add an entry to specify how to route calls to **53000**. In the example shown below, calls with digits **53000** will be routed as call type **lev0** using route pattern **53** from **Section 5.12**.

change aar analysis 0					Page 1 of 2
AAR DIGIT ANALYSIS TABLE					
Location: all					Percent Full: 2
Dialed	Total	Route	Call	Node	ANI
String	Min Max	Pattern	Type	Num	Reqd
<b>53000</b>	<b>5 5</b>	<b>53</b>	<b>lev0</b>		<b>n</b>

## 5.16. Administer Hunt Group

Use the **add hunt-group n** command, where **n** is an available hunt group number. This hunt group will be used for DV2000 voicemail. Enter the following values for the specified fields and retain the default values for the remaining fields.

- **Group Number:** The available group number.
- **Group Name:** A descriptive name.
- **Group Extension:** The DV2000 main number from **Section 3**.

add hunt-group 53		Page 1 of 60
HUNT GROUP		
Group Number: 53	ACD? n	
Group Name: DV2000 Voicemail	Queue? n	
Group Extension: 53000	Vector? n	
Group Type: ucd-mia	Coverage Path:	
TN: 1	Night Service Destination:	
COR: 1	MM Early Answer? n	
Security Code:	Local Agent Preference? n	
ISDN/SIP Caller Display:		

Navigate to **Page 2**. Enter the following values for the specified fields and retain the default values for the remaining fields.

- **Message Center:** “sip-adjunct”
- **Voice Mail Number:** The DV2000 main number from **Section 3**.
- **Voice Mail Handle:** The DV2000 main number from **Section 3**.
- **Routing Digits:** The pertinent access code for routing to DV2000, in this case “8”.

add hunt-group 53		Page 2 of 60
HUNT GROUP		
Message Center: sip-adjunct		
Voice Mail Number	Voice Mail Handle	Routing Digits
		(e.g., AAR/ARS Access Code)
53000	53000	8

## 5.17. Administer Coverage Path

Add a coverage path using the **add coverage path n** command where **n** is an available coverage path number. This coverage path is used for redirecting calls to DV2000 for voicemail and will be assigned to all guest and staff stations in **Section 5.18**.

For the **Point1** field, enter **h53** to designate the first coverage point where **53** is the hunt group number from **Section 5.16**. Retain the default values in the remaining fields.

add coverage path 3		Page 1 of 1	
COVERAGE PATH			
Coverage Path Number: 3			
Cvg Enabled for VDN Route-To Party? n		Hunt after Coverage? n	
Next Path Number:		Linkage	
COVERAGE CRITERIA			
Station/Group Status	Inside Call	Outside Call	
Active?	n	n	
Busy?	y	y	
Don't Answer?	y	y	Number of Rings: 2
All?	n	n	
DND/SAC/Goto Cover?	y	y	
Holiday Coverage?	n	n	
COVERAGE POINTS			
Terminate to Coverage Pts. with Bridged Appearances? n			
Point1: h53	Rng:	Point2:	
Point3:		Point4:	
Point5:		Point6:	

## 5.18. Administer Stations

Use the **change station n** command, where **n** is the first non-SIP station resource from **Section 3**. Note that configuration for SIP stations is performed from System Manager in **Section 6.7**.

For guest station resources, set **COS** to the class of service number from **Section 5.6**, and set **Coverage Path 1** to the coverage path number from **Section 5.17**.

For staff station resources, only set **Coverage Path 1** to the coverage path number from **Section 5.17**.

For station resources that are analog, the **Message Waiting Indicator** parameter may need modification depending on the type of analog telephone. In the compliance testing, one analog guest station with phone **Type** of **2500** was required to have the **Message Waiting Indicator** set to **led** for interoperability.

change station 63001		Page 1 of 4
STATION		
Extension: 67001	Lock Messages? n	BCC: 0
<b>Type: 2500</b>	Security Code:	TN: 1
Port: 001V201	<b>Coverage Path 1: 3</b>	COR: 1
Name: Avaya, Analog 1	Coverage Path 2:	<b>COS: 3</b>
Unicode Name? n	Hunt-to Station:	Tests? y
STATION OPTIONS		
XOIP Endpoint type: auto	Time of Day Lock Table:	
Loss Group: 1	<b>Message Waiting Indicator: led</b>	
Off Premises Station? n	Message Lamp Ext: 63001	

Repeat this section and **Section 6.7** to administer all guest and staff station resources from **Section 3**. In the compliance testing, two staff stations with extensions **64001** and **65001**, and two guest stations with extensions **63001** and **66001** were configured as shown below.

list station 63001 count 4							Page	1
STATIONS								
Ext/ Hunt-to	Port/ Type	Name/ Surv GK NN	Move	Cable	Room/ Jack	Cv1/ Cv2	COR/ COS	TN
63001	001V101	Analog Guest				3	1	
	2500		no				3	1
64001	001V101	Digital Staff				3	1	
	1408		no				1	1
65001	S000118	H323 Staff				3	1	
	1608		no				1	1
66001	S000172	Avaya, SIP 1				3	1	
	J129		no				3	1

## 6. Configure Avaya Aura® Session Manager

This section provides the procedures for configuring Session Manager, which is performed via the web interface of System Manager. The procedures include the following areas:

- Launch System Manager
- Administer locations
- Administer adaptations
- Administer SIP entities
- Administer routing policies
- Administer dial patterns
- Administer SIP users

### 6.1. Launch System Manager

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

Recommended access to System Manager is via FQDN.  
[Go to central login for Single Sign-On](#)

If IP address access is your only option, then note that authentication will fail in the following cases:

- First time login with "admin" account
- Expired/Reset passwords

Use the "Change Password" hyperlink on this page to change the password manually, and then login.

Also note that single sign-on between servers in the same security domain is

User ID:

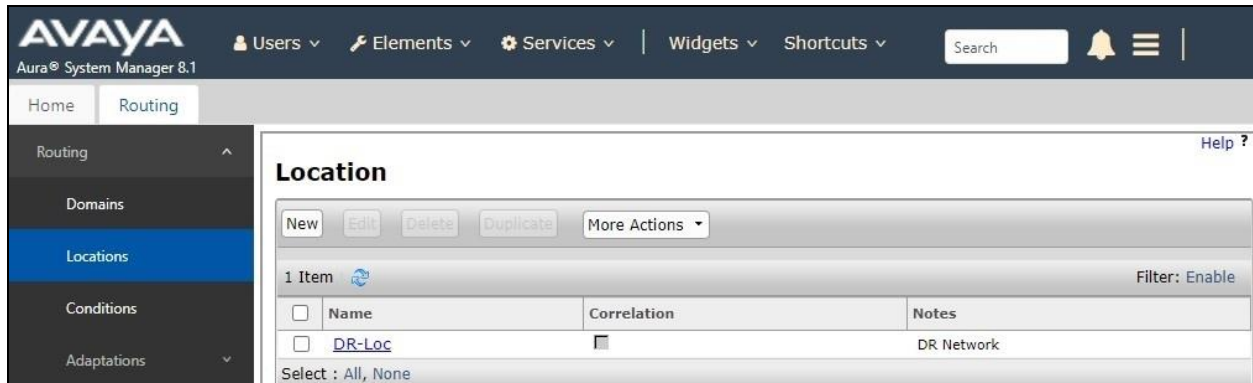
Password:

The screen below is displayed next.



## 6.2. Administer Locations

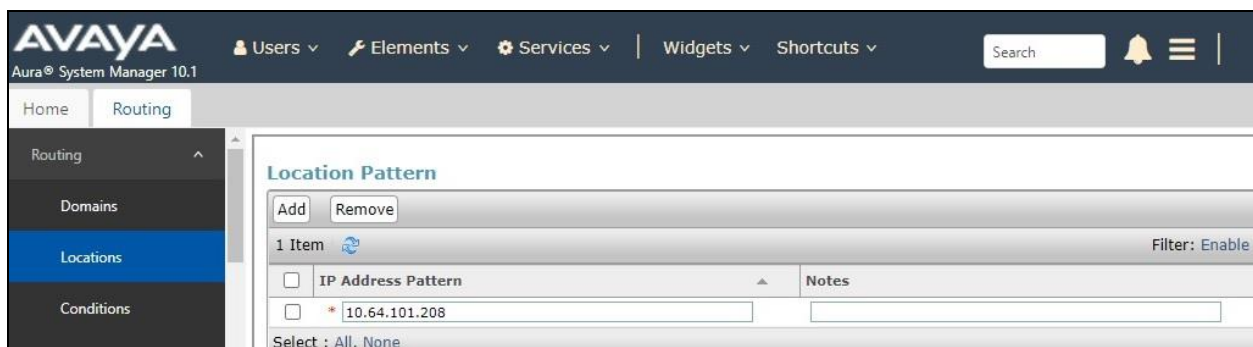
Select **Elements** → **Routing** → **Locations** from the top menu to display the **Location** screen below. Select **New** to add a new location for DV2000.



The **Location Details** screen is displayed next. In the **General** sub-section, enter a descriptive **Name** and optional **Notes**.



Scroll down to the **Location Pattern** sub-section and click **Add**. For **IP Address Pattern**, enter the IP address of DV2000 as shown below. Retain the default values in the remaining fields.



## 6.3. Administer Adaptations

Select **Routing** → **Adaptations** from the left pane and click **New** in the subsequent screen (not shown) to add a new adaptation for DV2000. **The Adaptation Details** screen is displayed.

In the **General** sub-section, enter the following values for the specified fields and retain the default values for the remaining fields.

- **Adaptation Name:** A descriptive name.
- **Notes:** Optional notes.
- **Module Name:** “DomainAdapter”
- **Module Parameter Type:** “Name-Value Parameter”

Select **Add** to add an entry. Enter **odstd** for **Name** and the IP address of DV2000 for **Value** as shown below.

This adaptation will set the destination domain for outgoing calls from Session Manager to the IP address of DV2000, as required by DV2000.

**AVAYA**  
Aura® System Manager 10.1

Users ▾ Elements ▾ Services ▾ | Widgets ▾ Shortcuts ▾ Search 🔍

Home Routing

Routing ▾  
Domains  
Locations  
Conditions  
Adaptations ▾  
Adaptations  
Regular Expressi...  
Device Mappings  
SIP Entities  
Entity Links

**Adaptation Details** Commit Cancel

**General**

\* **Adaptation Name:** DV2000 Outgoing

**Notes:** replace outgoing domain with IP

\* **Module Name:** DomainAdapter ▾

**Type:** digit

**State:** enabled ▾

**Module Parameter Type:** Name-Value Parameter ▾

Add Remove	
<input type="checkbox"/> Name	Value
<input type="checkbox"/> odstd	10.64.101.208

Select : All, None

**Egress URI Parameters:**

## 6.4. Administer SIP Entities

Add two SIP entities, one for DV2000 and one for the new SIP trunk with Communication Manager.

### 6.4.1. SIP Entity for DV2000

Select **Routing** → **SIP Entities** from the left menu and click **New** in the subsequent screen (not shown) to add a new SIP entity for DV2000.

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

- **Name:** A descriptive name.
- **FQDN or IP Address:** The IP address of DV2000.
- **Type:** “SIP Trunk”
- **Adaptation:** Select the DV2000 adaptation name from **Section 6.3**.
- **Location:** Select the DV2000 location name from **Section 6.2**.
- **Time Zone:** Select the applicable time zone.

The screenshot displays the Avaya Aura System Manager 8.1 web interface. The top navigation bar includes the Avaya logo, the version number '8.1', and several menu items: 'Users', 'Elements', 'Services', 'Widgets', and 'Shortcuts'. A search bar and notification icons are also present. The left sidebar shows a tree view with 'Routing' selected, and 'SIP Entities' highlighted. The main content area is titled 'SIP Entity Details' and contains a 'General' tab. The form fields are as follows:

- Name:** DV2000
- FQDN or IP Address:** 10.64.101.208
- Type:** SIP Trunk (dropdown)
- Notes:** (empty text area)
- Adaptation:** DV2000 Outgoing (dropdown)
- Location:** DV-Loc (dropdown)
- Time Zone:** America/New\_York (dropdown)
- SIP Timer B/F (in seconds):** 4
- Minimum TLS Version:** Use Global Setting (dropdown)
- Credential name:** (empty text area)
- Securable:** ☐
- Call Detail Recording:** egress (dropdown)

At the bottom of the form, there is a 'Loop Detection' section which is currently collapsed. 'Commit' and 'Cancel' buttons are located at the top right of the form area.



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

- **Name:** A descriptive name.
- **SIP Entity 1:** The Session Manager entity name, in this case “DR-SM”.
- **Protocol:** “UDP”
- **Port:** “5060”
- **SIP Entity 2:** The DV2000 entity name from this section.
- **Port:** “5060”
- **Connection Policy:** “trusted”

Note that DV2000 can support UDP and TCP, and the compliance testing used the UDP protocol.

### Entity Links

Override Port & Transport with DNS SRV: ☐

Add Remove

1 Item
Filter: Enable

<input type="checkbox"/>	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy
<input type="checkbox"/>	* SM-DV2000	DR-SM	UDP	* 5060	DV2000	* 5060	trusted

Select : All, None

### SIP Responses to an OPTIONS Request

Add Remove

0 Items
Filter: Enable

<input type="checkbox"/>	Response Code & Reason Phrase	Mark Entity Up/Down	Notes
--------------------------	-------------------------------	---------------------	-------

Commit Cancel

### 6.4.2. SIP Entity for Communication Manager

Select **Routing** → **SIP Entities** from the left menu and click **New** in the subsequent screen (not shown) to add a new SIP entity for Communication Manager. Note that this SIP entity is used for integration with DV2000.

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

- **Name:** A descriptive name.
- **FQDN or IP Address:** The C-LAN or “procr” IP address from **Section 5.2**.
- **Type:** “CM”
- **Location:** Select the applicable location for Communication Manager.
- **Time Zone:** Select the applicable time zone.

The screenshot shows the Avaya Aura System Manager 8.1 interface. The left sidebar contains a navigation menu with the following items: Routing, Domains, Locations, Conditions, Adaptations, SIP Entities (selected), Entity Links, Time Ranges, Routing Policies, Dial Patterns, and Regular Expressions. The main content area displays the 'SIP Entity Details' form. The form has a 'General' tab selected and a 'Commit' button. The fields and their values are as follows:

Field	Value
Name	DR-CM-5053
FQDN or IP Address	10.64.101.236
Type	CM
Notes	
Adaptation	
Location	DR-Loc
Time Zone	America/New_York
SIP Timer B/F (in seconds)	4
Minimum TLS Version	Use Global Setting
Credential name	
Securable	<input type="checkbox"/>
Call Detail Recording	none

The 'Loop Detection' tab is visible at the bottom of the form.

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

- **Name:** A descriptive name, in this case the entity name from above was used.
- **SIP Entity 1:** The Session Manager entity name, in this case “DR-SM”.
- **Protocol:** The signaling group transport method from **Section 5.10**.
- **Port:** The signaling group far-end listen port number from **Section 5.10**.
- **SIP Entity 2:** The Communication Manager entity name from this section.
- **Port:** The signaling group near-end listen port number from **Section 5.10**.
- **Connection Policy:** “trusted”

### Entity Links

Override Port & Transport with DNS SRV: ☐

Add Remove

1 Item
Filter: Enable

<input type="checkbox"/>	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy
<input type="checkbox"/>	* DR-CM-5053	DR-SM	TCP	* 5053	DR-CM-5053	* 5053	trusted

Select : All, None

### SIP Responses to an OPTIONS Request

Add Remove

0 Items
Filter: Enable

<input type="checkbox"/>	Response Code & Reason Phrase	Mark Entity Up/Down	Notes
--------------------------	-------------------------------	---------------------	-------

Commit Cancel

## 6.5. Administer Routing Policies

Add two routing policies, one for DV2000 and one for the new SIP trunk with Communication Manager.

### 6.5.1. Routing Policy for DV2000

Select **Routing** → **Routing Policies** from the left pane and click **New** in the subsequent screen (not shown) to add a new routing policy for DV2000. The **Routing Policy Details** screen is displayed.

In the **General** sub-section, enter a descriptive **Name**. Enter optional **Notes** and retain the default values in the remaining fields.

In the **SIP Entity as Destination** sub-section, click **Select** and select the DV2000 entity name from **Section 6.4.1**. The screen below shows the result of the selection.

**AVAYA** Aura® System Manager 8.1

Users ▾ Elements ▾ Services ▾ | Widgets ▾ Shortcuts ▾ Search 🔍 🔔 ☰

Home Routing

Routing Policy Details Commit Cancel Help ?

**General**

\* Name:

Disabled: ☐

\* Retries:

Notes:

**SIP Entity as Destination**

Select

Name	FQDN or IP Address	Type	Notes
DV2000	10.64.101.208	SIP Trunk	

**Time of Day**

### 6.5.2. Routing Policy for Communication Manager

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

In the **General** sub-section, enter a descriptive **Name**. Enter optional **Notes** and retain the default values in the remaining fields.

In the **SIP Entity as Destination** sub-section, click **Select** and select the Communication Manager entity name from **Section 6.4.2**. The screen below shows the result of the selection.

**AVAYA**  
Aura® System Manager 10.1

Users ▾ Elements ▾ Services ▾ | Widgets ▾ Shortcuts ▾

Search 🔍 🔔 ☰

Home Routing

Routing Policy Details Commit Cancel [Help ?](#)

**General**

\* Name:

Disabled: ☐

\* Retries:

Notes:

**SIP Entity as Destination**

Select

Name	FQDN or IP Address	Type	Notes
DR-CM-5053	10.64.101.236	CM	

**Time of Day**

## 6.6. Administer Dial Patterns

Add a new dial pattern for DV2000 and update existing dial patterns for Communication Manager to allow calls from DV2000.

### 6.6.1. Dial Pattern for DV2000

Select **Routing** → **Dial Patterns** from the left pane and click **New** in the subsequent screen (not shown) to add a new dial pattern to reach DV2000. The **Dial Pattern Details** screen is displayed.

In the **General** sub-section, enter the following values for the specified fields and retain the default values for the remaining fields.

- **Pattern:** The DV2000 main number from **Section 3**.
- **Min:** The minimum number of digits to match.
- **Max:** The maximum number of digits to match.

In the **Originating Locations and Routing Policies** sub-section, click **Add** and create an entry for reaching DV2000. In the compliance testing, the entry allowed for call origination from Communication Manager endpoints in locations **DR-Loc**. The DV2000 routing policy from **Section 6.5.1** was selected as shown below.

The screenshot displays the Avaya Aura System Manager 10.1 interface. The left navigation pane shows the 'Routing' menu expanded, with 'Dial Patterns' selected. The main content area is titled 'Dial Pattern Details' and includes 'Commit' and 'Cancel' buttons. The 'General' section contains the following fields:

- \* Pattern: 53000
- \* Min: 5
- \* Max: 5
- Emergency Call: ☐
- SIP Domain: -ALL-
- Notes:

The 'Originating Locations and Routing Policies' section features an 'Add' button and a table with one item:

	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	DR-Loc	DR Network	To-DV2000	0	<input type="checkbox"/>	DV2000	

Below the table, it says 'Select : All, None'.

### 6.6.2. Dial Pattern for Communication Manager

Select **Routing** → **Dial Patterns** from the left pane and click on the applicable dial pattern for Communication Manager in the subsequent screen, in this case dial pattern **6** (not shown). The **Dial Pattern Details** screen is displayed.

In the **Originating Locations and Routing Policies** sub-section, click **Add** and create a new policy as necessary for calls from DV2000. In the compliance testing, the new policy allowed for call origination from the DV2000 location from **Section 6.2** and the Communication Manager routing policy from **Section 6.5.2** were selected as shown below. Retain the default values in the remaining fields.

**AVAYA**  
Aura® System Manager 10.1

Users ▾ Elements ▾ Services ▾ | Widgets ▾ Shortcuts ▾ Search 🔍 🔔 ☰

Home Routing

Routing ▾  
Domains  
Locations  
Conditions  
Adaptations ▾  
SIP Entities  
Entity Links  
Time Ranges  
Routing Policies  
Dial Patterns ▾  
Dial Patterns  
Origination Dial...

**Dial Pattern Details** Commit Cancel [Help ?](#)

**General**

\* Pattern: 6

\* Min: 5

\* Max: 5

Emergency Call: ☐

SIP Domain: -ALL- ▾

Notes: To CM

**Originating Locations and Routing Policies**

Add Remove

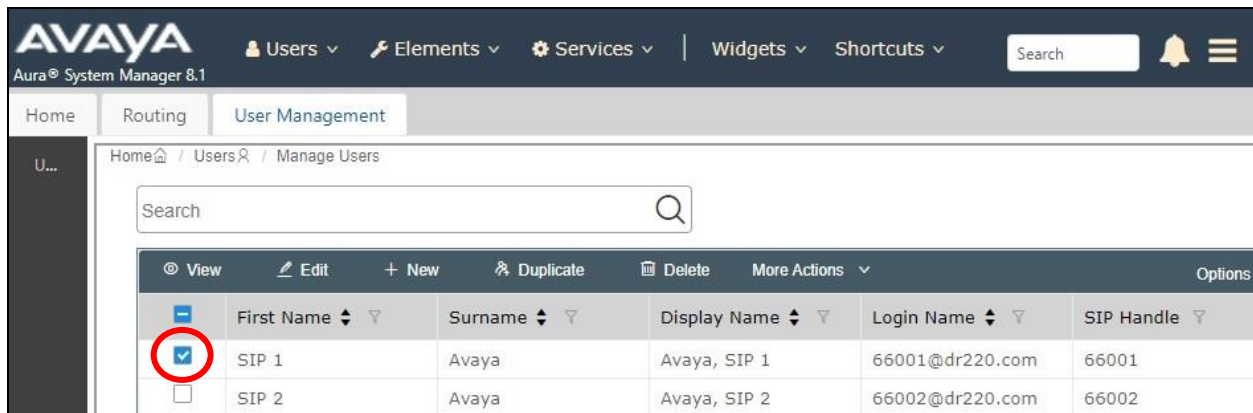
2 Items

<input type="checkbox"/>	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	DR-Loc	DR Network	To-CM	0	<input type="checkbox"/>	DR-CM	
<input type="checkbox"/>	DV-Loc	DV2000	To-CM-5053	0	<input type="checkbox"/>	DR-CM-5053	

Select : All, None

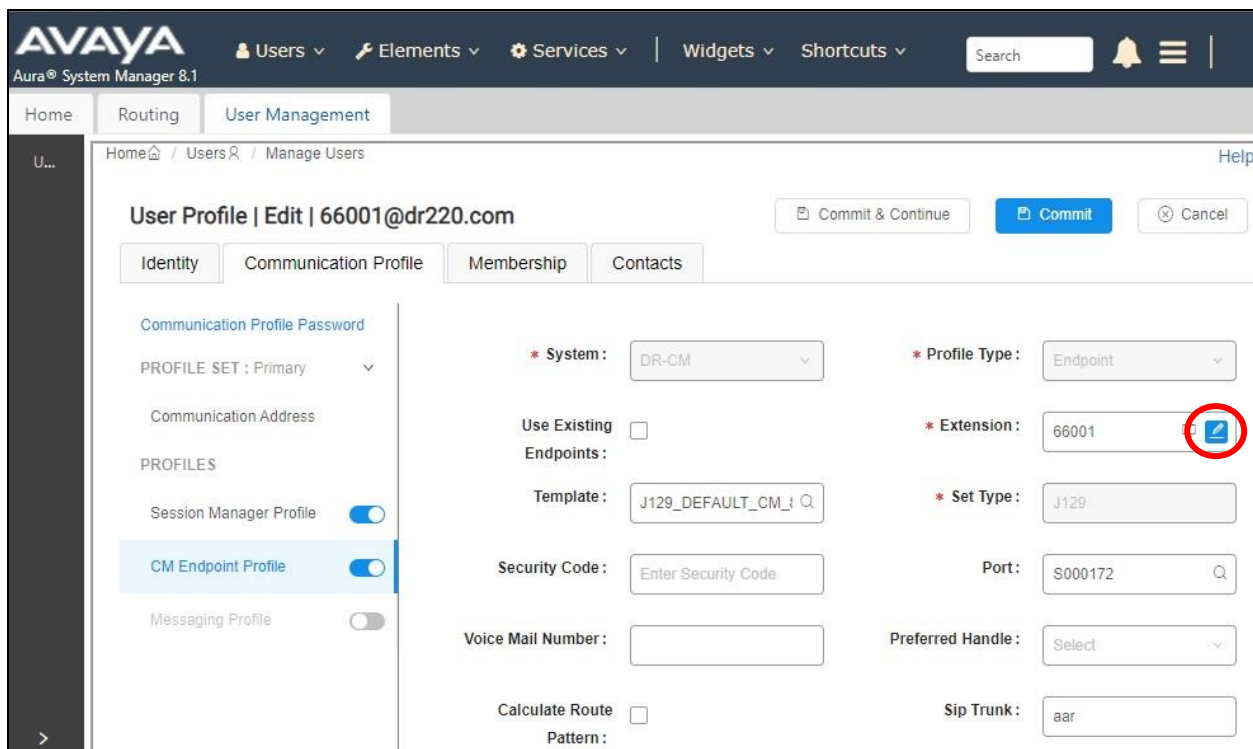
## 6.7. Administer SIP Users

Select **Users** → **User Management** from the top menu. Select **User Management** → **Manage Users** (not shown) from the left pane to display the screen below. Select the entry associated with the first SIP station resource from **Section 3**, in this case **66001**, and click **Edit**.



The **User Profile | Edit** screen is displayed. Select the **Communication Profile** tab, followed by **CM Endpoint Profile** to display the screen below.

Click on the **Editor** icon shown below.





The popped-up screen below is displayed.

For guest station resource, set **Class of Service (COS)** to the class of service number from **Section 5.6**, and set **Coverage Path 1** to the coverage path number from **Section 5.17**.

For staff station resource, only set **Coverage Path 1** to the coverage path number from **Section 5.17**.

Repeat this section to administer all SIP station resources from **Section 3**. In the compliance testing, one SIP guest with extension **66001** was configured as shown below.

The screenshot displays the Avaya Aura System Manager 8.1 User Management interface. The top navigation bar includes 'Users', 'Elements', 'Services', 'Widgets', and 'Shortcuts'. The main content area is titled 'User Management' and shows configuration details for a user with extension 66001. The 'System' field is set to 'DR-CM', 'Template' to 'J129\_DEFAULT\_CM\_8\_1', 'Port' to 'S000172', and 'Name' to 'Avaya, SIP 1'. The 'Extension' field is '66001' and 'Set Type' is 'J129'. Below these fields are tabs for 'General Options (G)', 'Feature Options (F)', 'Site Data (S)', 'Abbreviated Call Dialing (A)', and 'Button Assignment (B)'. The 'General Options (G)' tab is active, showing 'Profile Settings (P)' and 'Group Membership (M)'. Under 'Profile Settings (P)', the following fields are visible: 'Class of Restriction (COR)' set to '1', 'Emergency Location Ext' set to '66001', 'Tenant Number' set to '1', 'SIP Trunk' set to 'Qaar', 'Coverage Path 1' set to '3', 'Lock Message' (unchecked), 'Multibyte Language' set to 'Not Applicable', and 'SIP URI' (empty). Under 'Group Membership (M)', the following fields are visible: 'Class Of Service (COS)' set to '3', 'Message Lamp Ext.' set to '66001', 'Type of 3PCC Enabled' set to 'None', 'Coverage Path 2' (empty), 'Localized Display Name' set to 'Avaya, SIP 1', and 'Enable Reachability for Station Domain Control' set to 'system'. Red boxes highlight the 'Coverage Path 1' and 'Class Of Service (COS)' fields.

Field	Value
System	DR-CM
Extension	66001
Template	J129_DEFAULT_CM_8_1
Set Type	J129
Port	S000172
Security Code	
Name	Avaya, SIP 1
Class of Restriction (COR)	1
Emergency Location Ext	66001
Tenant Number	1
SIP Trunk	Qaar
Coverage Path 1	3
Lock Message	<input type="checkbox"/>
Multibyte Language	Not Applicable
SIP URI	
Class Of Service (COS)	3
Message Lamp Ext.	66001
Type of 3PCC Enabled	None
Coverage Path 2	
Localized Display Name	Avaya, SIP 1
Enable Reachability for Station Domain Control	system

## 7. Configure DuVoice DV2000

This section provides the procedures for configuring DV2000. The procedures include the following areas:

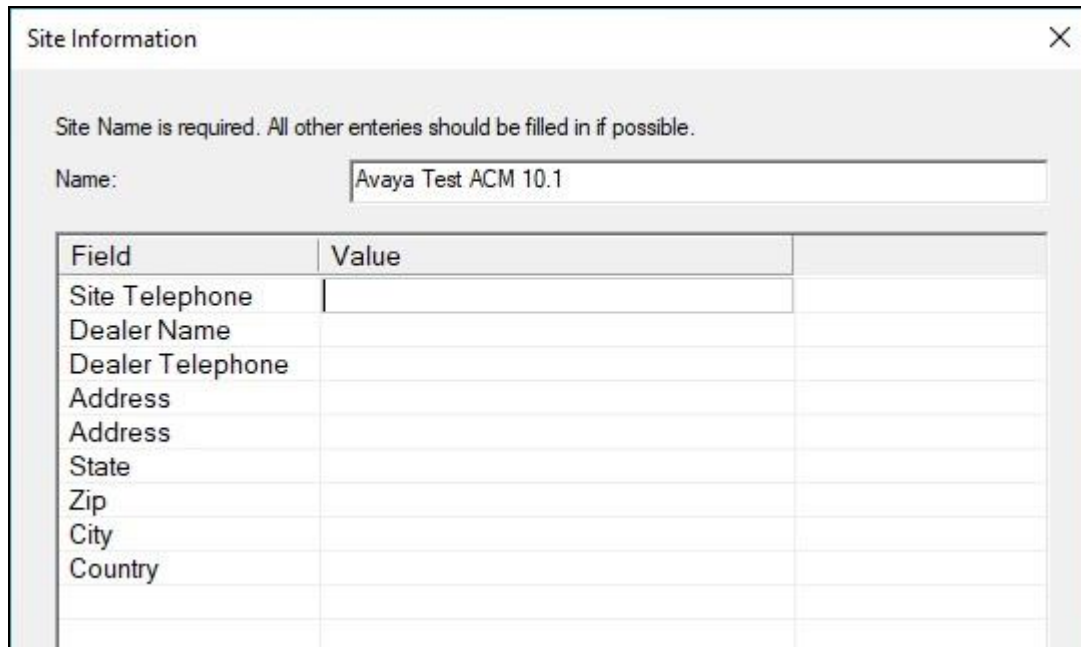
- Administer PBX configuration
- Administer profile configuration
- Administer SIP configuration
- Administer hospitality configuration
- Administer mailboxes
- Start service

## 7.1. Administer PBX Configuration

At the conclusion of DV2000 installation, the Setup Wizard auto launches and displays the **Production Activation** screen below. Follow reference [3] to download the pertinent license and activate the system.

[illegible]

The **Site Information** screen is displayed next. Enter a descriptive **Name** and pertinent values in the remaining fields.



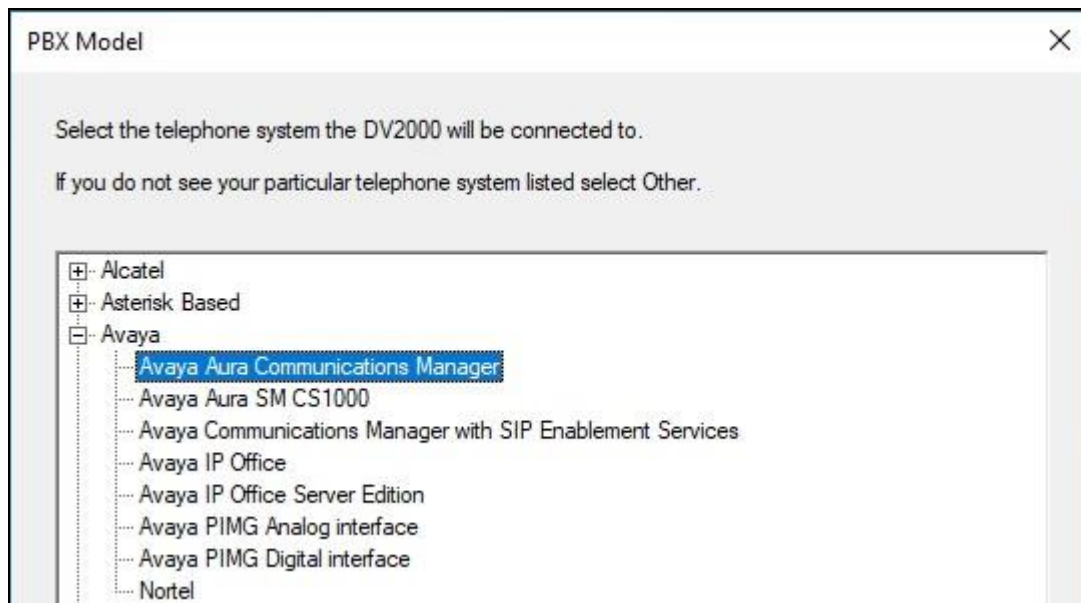
Site Information

Site Name is required. All other entries should be filled in if possible.

Name:

Field	Value
Site Telephone	
Dealer Name	
Dealer Telephone	
Address	
Address	
State	
Zip	
City	
Country	

Continue the configuration in subsequent screens with default values unless otherwise indicated. When the **PBX Model** screen appears, select **Avaya → Avaya Aura Communications Manager**, as shown below. Retain the default values in all subsequent screens to complete the Setup Wizard.



PBX Model

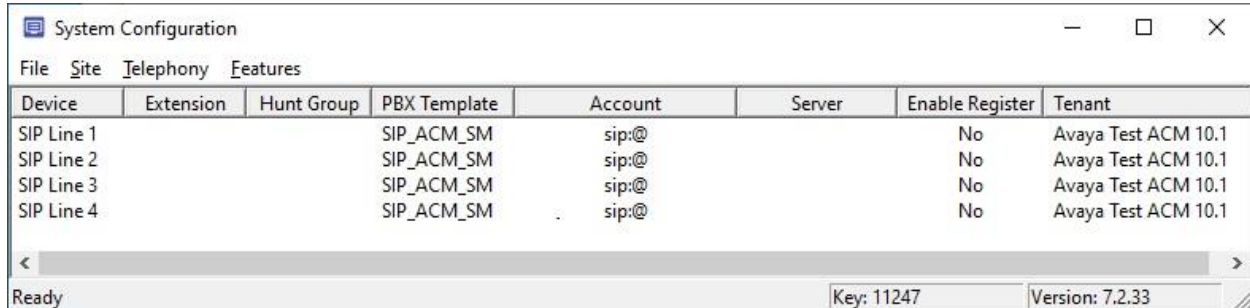
Select the telephone system the DV2000 will be connected to.

If you do not see your particular telephone system listed select Other.

- + Alcatel
- + Asterisk Based
- Avaya
  - Avaya Aura Communications Manager
  - Avaya Aura SM CS1000
  - Avaya Communications Manager with SIP Enablement Services
  - Avaya IP Office
  - Avaya IP Office Server Edition
  - Avaya PIMG Analog interface
  - Avaya PIMG Digital interface
- ... Nortel

## 7.2. Administer Profile Configuration

At the conclusion of the Setup Wizard, the **System Configuration** screen below is displayed. Select **Site** → **Profiles** from the top menu.



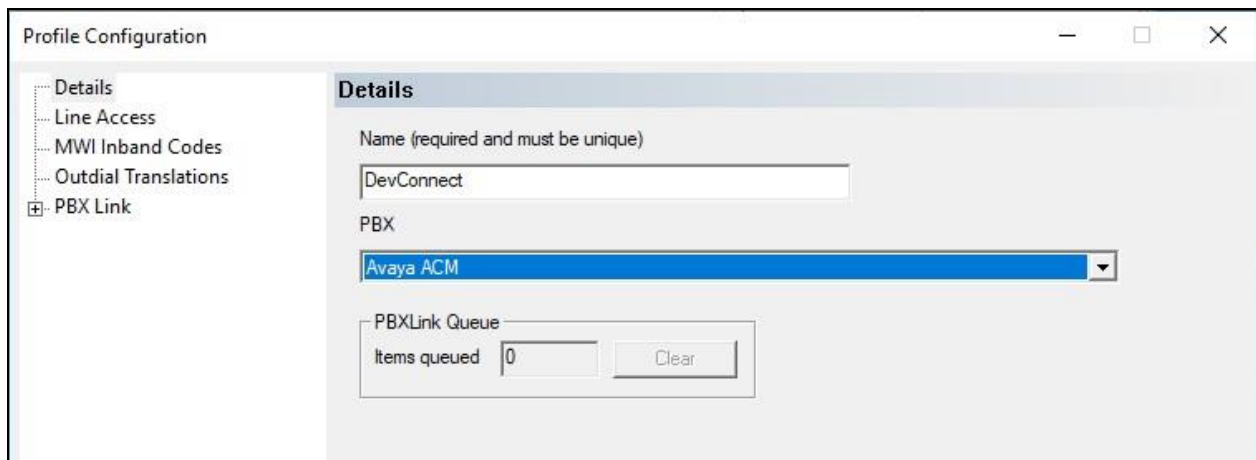
The screenshot shows the 'System Configuration' window with a menu bar (File, Site, Telephony, Features) and a table of SIP lines. The table has columns for Device, Extension, Hunt Group, PBX Template, Account, Server, Enable Register, and Tenant. There are four rows for SIP Line 1 through 4, all using the SIP\_ACM\_SM template and sip:@ accounts, with 'No' for Enable Register and 'Avaya Test ACM 10.1' for Tenant. A status bar at the bottom shows 'Ready', 'Key: 11247', and 'Version: 7.2.33'.

Device	Extension	Hunt Group	PBX Template	Account	Server	Enable Register	Tenant
SIP Line 1			SIP_ACM_SM	sip:@		No	Avaya Test ACM 10.1
SIP Line 2			SIP_ACM_SM	sip:@		No	Avaya Test ACM 10.1
SIP Line 3			SIP_ACM_SM	sip:@		No	Avaya Test ACM 10.1
SIP Line 4			SIP_ACM_SM	sip:@		No	Avaya Test ACM 10.1

The **Profile Selection** (not shown) screen is displayed. Select the default entry and click **Edit** (not shown).

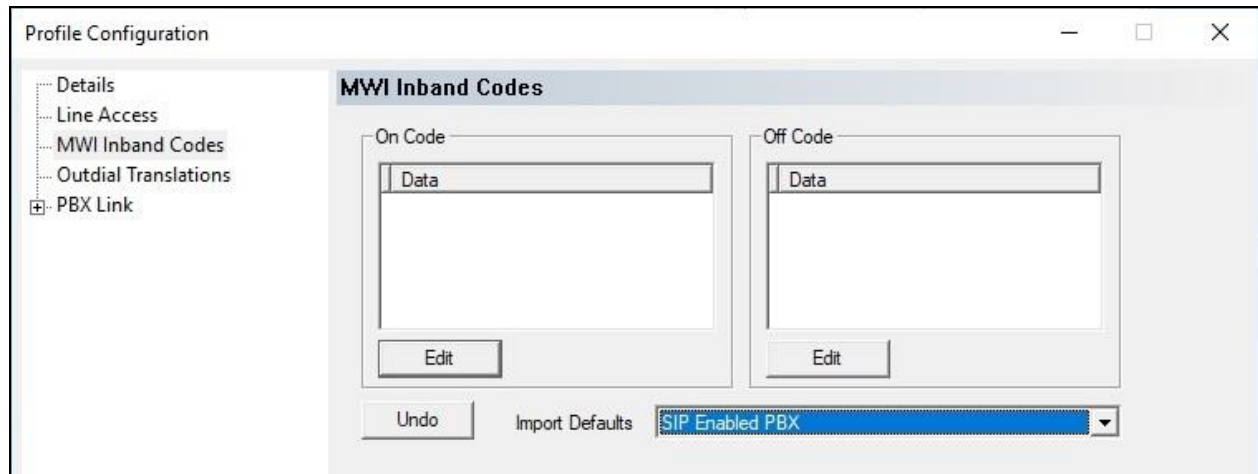
The **Profile Configuration** screen is displayed next. Select **Details** in the left pane. Enter the following values for the specified fields and retain the default values for the remaining fields.

- **Name:** A descriptive name.
- **PBX:** “Avaya ACM”



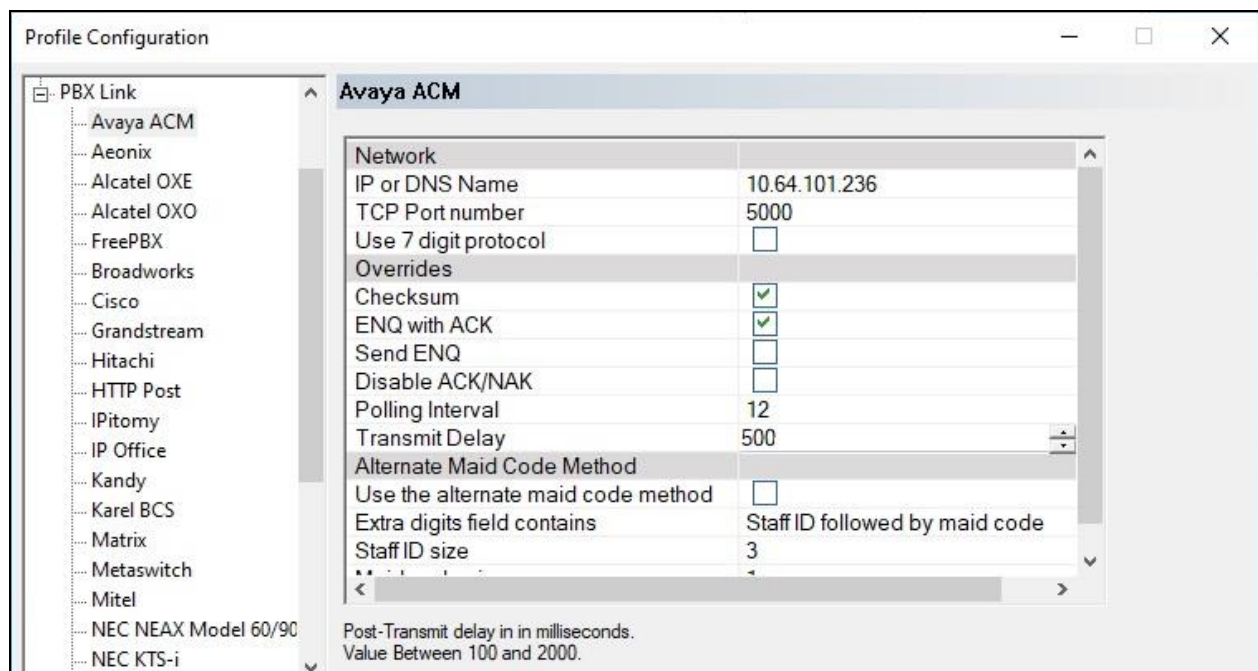
The screenshot shows the 'Profile Configuration' window with a left sidebar containing 'Details', 'Line Access', 'MWI Inband Codes', 'Outdial Translations', and 'PBX Link'. The 'Details' tab is selected, showing a 'Name (required and must be unique)' field with 'DevConnect', a 'PBX' dropdown menu with 'Avaya ACM' selected, and a 'PBXLink Queue' section with 'Items queued' set to 0 and a 'Clear' button.

Select **MWI Inband Codes** in the left pane. For **Import Defaults**, select **SIP Enabled PBX** as shown below.



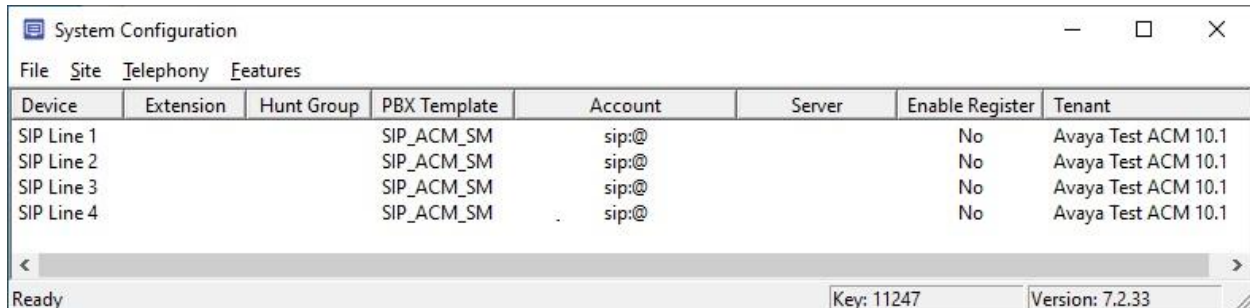
Expand **PBX Link** in the left pane, and select **Avaya ACM**. Enter the following values for the specified fields and retain the default values for the remaining fields.

- **IP or DNS Name:** IP address of the C-LAN or “procr” node name from **Section 5.2**.
- **Checksum:** Check this parameter.
- **ENQ with ACK:** Check this parameter.
- **Polling Interval:** “12”
- **Polling Interval:** “500”



### 7.3. Administer SIP Configuration

The **System Configuration** screen below is displayed again. Select **Telephony → SIP Configuration** from the top menu.

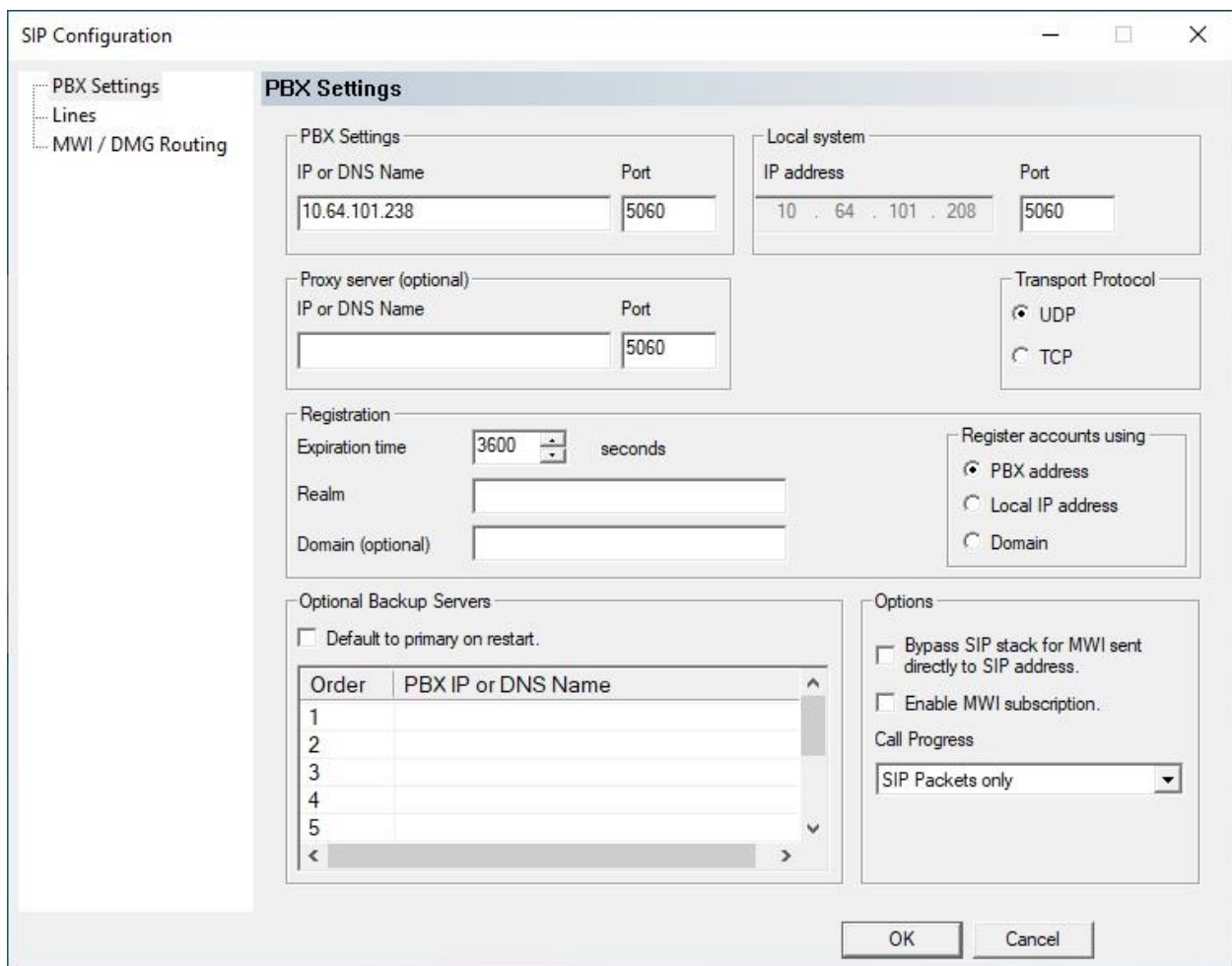


The screenshot shows the 'System Configuration' window with the 'Telephony' tab selected. It displays a table with the following data:

Device	Extension	Hunt Group	PBX Template	Account	Server	Enable Register	Tenant
SIP Line 1			SIP_ACM_SM	sip:@		No	Avaya Test ACM 10.1
SIP Line 2			SIP_ACM_SM	sip:@		No	Avaya Test ACM 10.1
SIP Line 3			SIP_ACM_SM	sip:@		No	Avaya Test ACM 10.1
SIP Line 4			SIP_ACM_SM	sip:@		No	Avaya Test ACM 10.1

At the bottom of the window, it shows 'Key: 11247' and 'Version: 7.2.33'.

The **SIP Configuration** screen is displayed. Select **PBX Settings** from the left pane. For **IP or DNS Name**, enter the IP address of Session Manager from **Section 5.2**. Retain the default values in the remaining fields.



The screenshot shows the 'SIP Configuration' window with the 'PBX Settings' tab selected. The left pane shows a tree view with 'PBX Settings', 'Lines', and 'MWI / DMG Routing'. The main area contains the following settings:

- PBX Settings:**
  - IP or DNS Name: 10.64.101.238
  - Port: 5060
- Local system:**
  - IP address: 10 . 64 . 101 . 208
  - Port: 5060
- Proxy server (optional):**
  - IP or DNS Name: (empty)
  - Port: 5060
- Transport Protocol:**
  - ☒ UDP
  - ☐ TCP
- Registration:**
  - Expiration time: 3600 seconds
  - Realm: (empty)
  - Domain (optional): (empty)
- Register accounts using:**
  - ☒ PBX address
  - ☐ Local IP address
  - ☐ Domain
- Optional Backup Servers:**
  - ☐ Default to primary on restart.
  - Table with 2 columns: Order, PBX IP or DNS Name
- Options:**
  - ☐ Bypass SIP stack for MWI sent directly to SIP address.
  - ☐ Enable MWI subscription.
  - Call Progress: SIP Packets only

At the bottom, there are 'OK' and 'Cancel' buttons.



The **System Configuration** screen below is displayed again and updated with **Account** and **Server** values shown below. Double click on the **SIP Line 1** entry.

System Configuration							
File Site Telephony Features							
Device	Extension	Hunt Group	PBX Template	Account	Server	Enable Register	Tenant
SIP Line 1			SIP_ACM_SM	sip:53000@10.64.101.238	10.64.101.238	No	Avaya Test ACM 10.1
SIP Line 2			SIP_ACM_SM	sip:53000@10.64.101.238	10.64.101.238	No	Avaya Test ACM 10.1
SIP Line 3			SIP_ACM_SM	sip:53000@10.64.101.238	10.64.101.238	No	Avaya Test ACM 10.1
SIP Line 4			SIP_ACM_SM	sip:53000@10.64.101.238	10.64.101.238	No	Avaya Test ACM 10.1

Ready Key: 11247 Version: 7.2.33

The **SIP Line 1** screen is displayed. For **Extension number**, enter the DV2000 main number from **Section 3**. Retain the default values in the remaining fields.

SIP Line 1

Line Configuration

PBX Integration

Extension number

53000

Hunt group extension is a member of

Integration:

SIP\_ACM\_SM

Serial Integration

None

Details

Advanced...

Line Application

External IVR filename

(Optional, default is blank)

Application:

Default

Default tenant:

Avaya Test ACM 10.1

OK

Cancel

Apply

Help

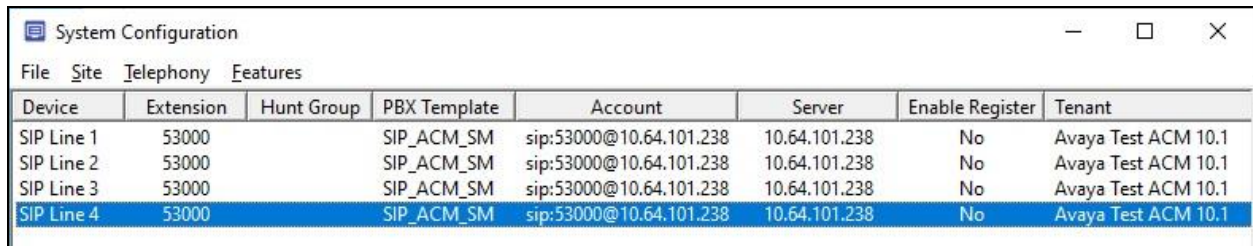
Repeat the last procedure to update **Extension** for all SIP Line entries as shown below.

System Configuration							
File Site Telephony Features							
Device	Extension	Hunt Group	PBX Template	Account	Server	Enable Register	Tenant
SIP Line 1	53000		SIP_ACM_SM	sip:53000@10.64.101.238	10.64.101.238	No	Avaya Test ACM 10.1
SIP Line 2	53000		SIP_ACM_SM	sip:53000@10.64.101.238	10.64.101.238	No	Avaya Test ACM 10.1
SIP Line 3	53000		SIP_ACM_SM	sip:53000@10.64.101.238	10.64.101.238	No	Avaya Test ACM 10.1
SIP Line 4	53000		SIP_ACM_SM	sip:53000@10.64.101.238	10.64.101.238	No	Avaya Test ACM 10.1

Ready Key: 11247 Version: 7.2.33

## 7.4. Administer Hospitality Configuration

Select **Features** → **Hospitality** from the top menu.

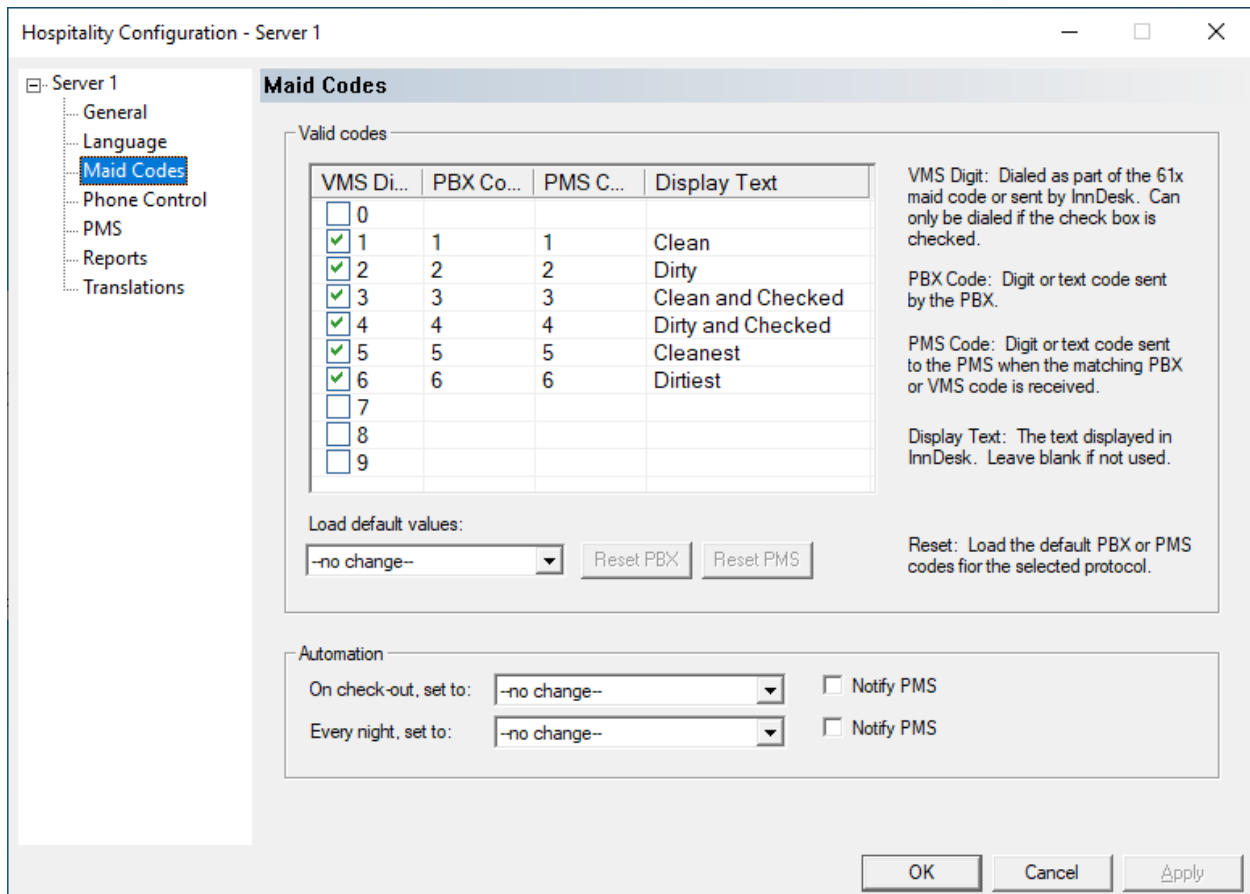


Device	Extension	Hunt Group	PBX Template	Account	Server	Enable Register	Tenant
SIP Line 1	53000		SIP_ACM_SM	sip:53000@10.64.101.238	10.64.101.238	No	Avaya Test ACM 10.1
SIP Line 2	53000		SIP_ACM_SM	sip:53000@10.64.101.238	10.64.101.238	No	Avaya Test ACM 10.1
SIP Line 3	53000		SIP_ACM_SM	sip:53000@10.64.101.238	10.64.101.238	No	Avaya Test ACM 10.1
SIP Line 4	53000		SIP_ACM_SM	sip:53000@10.64.101.238	10.64.101.238	No	Avaya Test ACM 10.1

The **Hospitality Selection** (not shown) screen is displayed. Click **Add** (not shown).

The **Hospitality Configuration – Server 1** screen is displayed next. Select **Maid Codes** from the left pane, to display the **Maid Codes** screen in the right pane.

Follow reference [3] to set maid codes to match definitions for room states and values in **Section 5.4**. The settings used in the compliance testing are shown below.



**Hospitality Configuration - Server 1**

Server 1

- General
- Language
- Maid Codes**
- Phone Control
- PMS
- Reports
- Translations

**Maid Codes**

Valid codes

VMS Di...	PBX Co...	PMS C...	Display Text
<input type="checkbox"/> 0			
<input checked="" type="checkbox"/> 1	1	1	Clean
<input checked="" type="checkbox"/> 2	2	2	Dirty
<input checked="" type="checkbox"/> 3	3	3	Clean and Checked
<input checked="" type="checkbox"/> 4	4	4	Dirty and Checked
<input checked="" type="checkbox"/> 5	5	5	Cleanest
<input checked="" type="checkbox"/> 6	6	6	Dirtiest
<input type="checkbox"/> 7			
<input type="checkbox"/> 8			
<input type="checkbox"/> 9			

VMS Digit: Dialed as part of the 61x maid code or sent by InnDesk. Can only be dialed if the check box is checked.

PBX Code: Digit or text code sent by the PBX.

PMS Code: Digit or text code sent to the PMS when the matching PBX or VMS code is received.

Display Text: The text displayed in InnDesk. Leave blank if not used.

Load default values:

--no change--

Reset: Load the default PBX or PMS codes for the selected protocol.

Automation

On check-out, set to: --no change-- ☐ Notify PMS

Every night, set to: --no change-- ☐ Notify PMS



Select **Phone Control** from the left pane.

Follow reference [3] to set phone state and create restriction entries as appropriate for the customer. The settings used in the compliance testing are shown below.

Hospitality Configuration - Server 1

Server 1

- General
- Language
- Maid Codes
- Phone Control**
- PMS
- Reports
- Translations

### Phone Control

Auto-set phone state on

☒ Check-in: No restriction

☒ Check-out: Outward + Toll

Call accounting

Type: -none--

Enabled: -no change--

Disabled: -no change--

User group restrictions / call restriction values

To edit an entry, left-click on it. For all other actions, right-click any row to display a menu.

Reset restrictions to defaults for: - No Change -

Display Text	PBX Value	PMS Value
No restriction	0	0
Outward + Termination	6	6
Outward + Toll	3	3
Outward Restriction	1	1
Termination restriction	5	5
Toll + termination	7	7
Toll restriction	2	2

Active PMS: Static

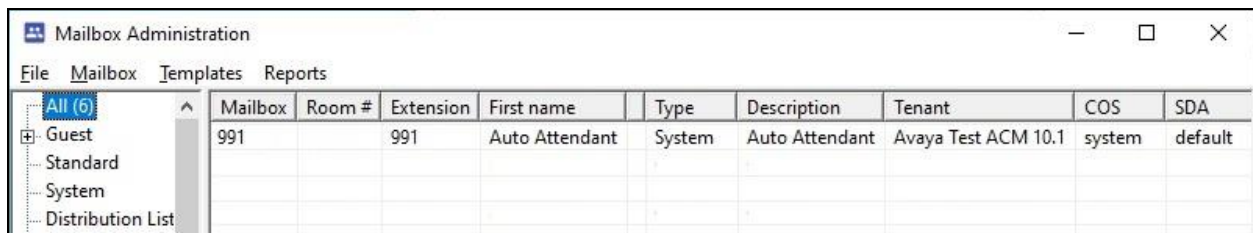
OK Cancel Apply

## 7.5. Administer Mailboxes

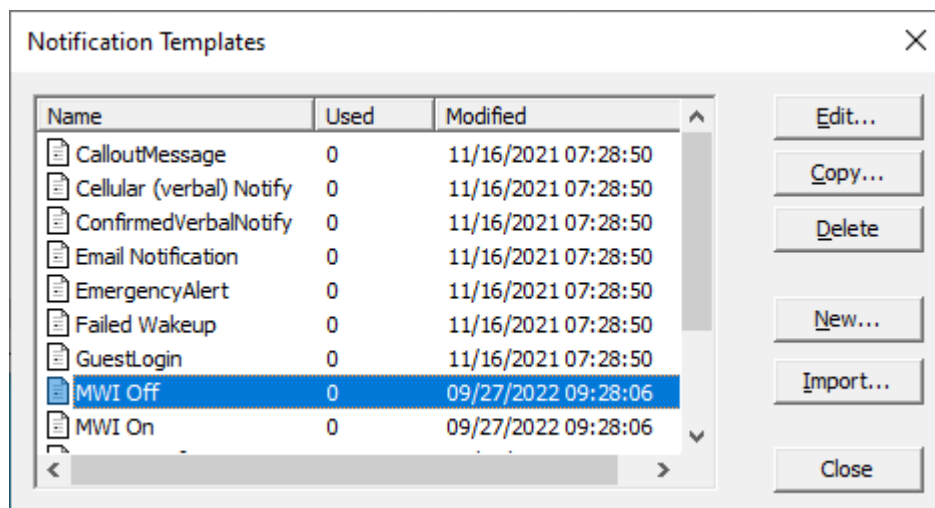
From the DV2000 server, double-click on the **Mailbox Administration** icon on the desktop, which was created as part of DV2000 installation.



The **Mailbox Administration** screen is displayed. Select **Templates** → **Notifications** from the top menu.



In the **Notification Templates** pop-up screen, select **MWI Off** and click **Edit**.



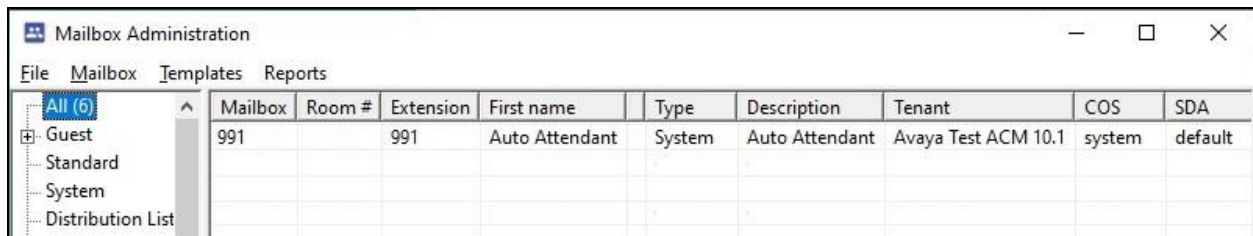
The **MWI Off** screen is displayed. For **Method**, select **SIP** as shown below and retain the default values in the remaining fields.

The screenshot shows the 'MWI Off' dialog box with the 'Notification' tab selected. The 'Definition' section on the left contains the following settings: 'Event' is 'retrieve new messages', 'Address' is 'MWI' with 'ALL' selected in the secondary dropdown, 'Technique' is 'Message Waiting Indicator Of', the checkbox 'Light for every message' is checked, 'Method' is 'SIP', 'Initial Delay' is 0 minutes, 'Retry Interval' is 1 minute, and 'Do not exceed' is 5 attempts. The 'Schedule' section on the right shows 'Days of the week this template is active' with all days (Su, M, Tu, W, Th, F, Sa) selected, and 'Time period during which this notification is active' with 'Starting at' and 'Ending at' both set to 12:00 AM. 'OK' and 'Cancel' buttons are at the bottom.

Repeat the same procedure for **MWI On**.

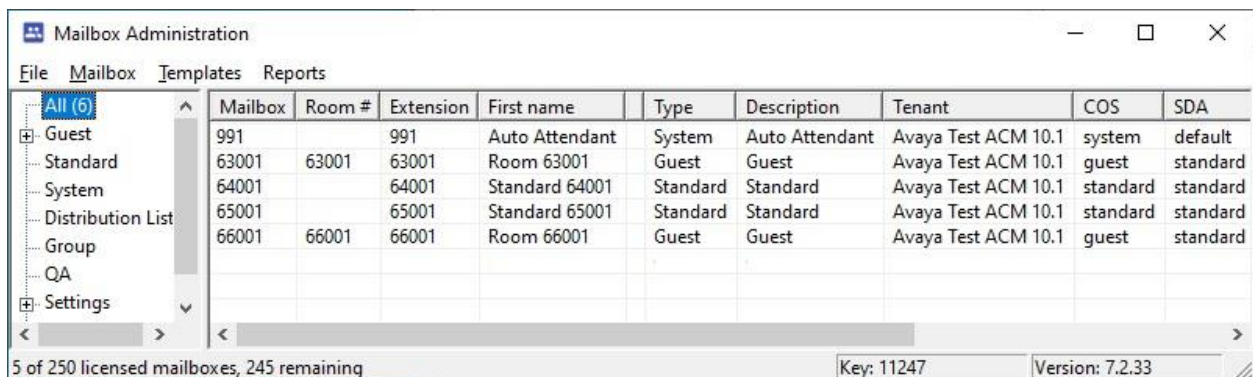
The screenshot shows the 'MWI On' dialog box with the 'Notification' tab selected. The 'Definition' section on the left contains the following settings: 'Event' is 'all messages', 'Address' is 'MWI' with 'ALL' selected in the secondary dropdown, 'Technique' is 'Message Waiting Indicator Of', the checkbox 'Light for every message' is checked, 'Method' is 'SIP', 'Initial Delay' is 0 minutes, 'Retry Interval' is 1 minute, and 'Do not exceed' is 5 attempts. The 'Schedule' section on the right shows 'Days of the week this template is active' with all days (Su, M, Tu, W, Th, F, Sa) selected, and 'Time period during which this notification is active' with 'Starting at' and 'Ending at' both set to 12:00 AM. 'OK' and 'Cancel' buttons are at the bottom.

The **Mailbox Administration** screen is displayed again. Select **Mailbox → Create** from the top menu and follow reference [3] to create a mailbox for each guest and staff on Communication Manager that will be using DV2000 for voicemail.



Mailbox	Room #	Extension	First name	Type	Description	Tenant	COS	SDA
991		991	Auto Attendant	System	Auto Attendant	Avaya Test ACM 10.1	system	default

In the compliance testing, mailboxes for two guests and two staff were configured as shown below.

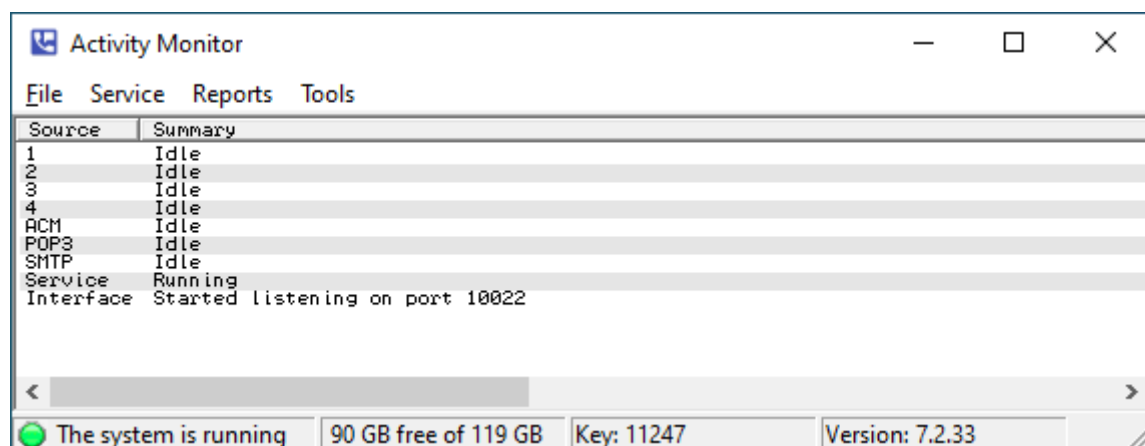


Mailbox	Room #	Extension	First name	Type	Description	Tenant	COS	SDA
991		991	Auto Attendant	System	Auto Attendant	Avaya Test ACM 10.1	system	default
63001	63001	63001	Room 63001	Guest	Guest	Avaya Test ACM 10.1	guest	standard
64001		64001	Standard 64001	Standard	Standard	Avaya Test ACM 10.1	standard	standard
65001		65001	Standard 65001	Standard	Standard	Avaya Test ACM 10.1	standard	standard
66001	66001	66001	Room 66001	Guest	Guest	Avaya Test ACM 10.1	guest	standard


5 of 250 licensed mailboxes, 245 remaining      Key: 11247      Version: 7.2.33

## 7.6. Start Service

From the DV2000 server, select **Start → DV2000 → Activity Monitor** to launch Activity Monitor. Select **Service → Start** from the top menu to start the application.



Source	Summary
1	Idle
2	Idle
3	Idle
4	Idle
ACM	Idle
POP3	Idle
SMTP	Idle
Service	Running
Interface	Started listening on port 10022

 The system is running      90 GB free of 119 GB      Key: 11247      Version: 7.2.33

## 8. Verification Steps

This section provides the tests that can be performed to verify proper configuration of Communication Manager, Session Manager, and DV2000.

### 8.1. Verify PMS Integration

On Communication Manager, verify status of the PMS link by using the **status pms-link** command. Verify that the **Physical Link State** and **Protocol State** are **up**, as shown below.

```
status pms-link

PMS LINK STATUS

Physical Link State: up
Protocol State: up

Maintenance Busy? no
Data Base Swapping? no
```

From the DV2000 server, select **Start → DV2000 Testing → Hospitality Tester** to launch the tool. The **Hospitality Tester** screen is displayed. For **Rooms**, select a guest extension, in this case **63001**. Enter the desired **First name** and **Last name**, and click **Check in**.

The screenshot shows the 'Hospitality Tester' application window. At the top, there's a 'Rooms' section with a dropdown menu set to '63001' and buttons for 'Reload', 'Update All', 'Check Out All', and 'Check In All'. Below this is a form for entering guest information: 'First name' (Apple), 'Last name' (Applebee), and 'Title'. There's also a 'Tenant' dropdown set to 'Avaya Test ACM 10.1', a 'Language' dropdown set to 'Default', a 'Maid status' dropdown, and a 'Phone COS' dropdown. Checkboxes for 'VIP', 'DND', 'Set arrival', and 'Set departure' are present, along with a 'Text count' field set to '0'. Dates for 'Set arrival' and 'Set departure' are both set to '9/27/2022'. A 'Group ID' field is also visible. On the right side, there's a 'Current state' section with a 'Refresh' button. It contains fields for 'Extension' (63001), 'Tenant' (Avaya Test ACM 10.1), 'Language' (Default), 'Maid status', 'Phone COS', 'Guest ID', 'Text count' (0), 'Arrival date', 'Departure date', 'Checked in', and 'Checked out'. At the bottom, there's a table with columns: 'Wakeup Call', 'Scheduled', 'Actor', 'Attempts', 'Result', 'Last attempt', and 'Created'. A 'Delete' button is next to the 'Wakeup Call' column. The table is currently empty, with a message 'There are no items to show in this view.'

On Communication Manager, use the **display station n** command, where **n** is the guest station extension. Verify that the station **Name** reflects the name from above.

```

display station 63001
                                STATION
Extension: 63001                Lock Messages? n                BCC: 0
Type: 2500                     Security Code:                  TN: 1
Port: 001V201                 Coverage Path 1: 3                COR: 1
Name: Applebee, Apple          Coverage Path 2:                COS: 3
Unicode Name? n                Hunt-to Station:                Tests? y
STATION OPTIONS
    XOIP Endpoint type: auto    Time of Day Lock Table:
    Loss Group: 1               Message Waiting Indicator: led
    Off Premises Station? n     Message Lamp Ext: 63001

    Survivable COR: internal
    Survivable Trunk Dest? y

                                Remote Office Phone? n

```

Use the **status station n** command, where **n** is the guest station extension. Verify that **Room Status** is **occupied**, and that **User Cntrl Restr** is **none** as shown below.

```

status station 63001
                                GENERAL STATUS
Administered Type: 2500          Service State: in-srv/on-hook or disc
    Connected Type: N/A
        Extension: 63001          Network Region: 1
            Port: 001V201        Parameter Download: not-applicable
                Call Parked? no   SAC Activated? no
                    Ring Cut Off Act? no
Active Coverage Option: 1        one-X Server Status: N/A

                                EC500 Status: N/A    Off-PBX Service State: N/A
Message Waiting:
Connected Ports:

Limit Incoming Calls? no

User Cntrl Restr: none
Group Cntrl Restr: none

                                HOSPITALITY STATUS
                                Awaken at:
                                User DND: not activated
                                Group DND: not activated
                                Room Status: occupied

```

## 8.2. Verify SIP Trunk Integration

On Communication Manager, verify status of the SIP trunk group by using the **status trunk n** command, where **n** is the trunk group number administered in **Section 5.9**. Verify that all trunks are in the **in-service/idle** state as shown below.

```
status trunk 53
```

TRUNK GROUP STATUS			
Member	Port	Service State	Mtce Connected Ports Busy
0053/001	T00087	in-service/idle	no
0053/002	T00113	in-service/idle	no
0053/003	T00114	in-service/idle	no
0053/004	T00115	in-service/idle	no

Verify status of the SIP signaling group by using the **status signaling-group n** command, where **n** is the signaling group number administered in **Section 5.10**. Verify that the **Group State** is **in-service**, as shown below.

```
status signaling-group 53
```

STATUS SIGNALING GROUP	
Group ID:	53
Group Type:	sip
<b>Group State:</b>	<b>in-service</b>

From the System Manager home page (not shown), select **Elements** → **Session Manager** from the top menu to display the **Session Manager Dashboard** screen (not shown).

Select **Session Manager** → **System Status** → **SIP Entity Monitoring** from the left pane to display the **SIP Entity Link Monitoring Status Summary** screen (name not shown). Click on the DV2000 entity name from **Section 6.4.1**.

**AVAYA** Aura® System Manager 10.1

Users ▾ Elements ▾ Services ▾ Widgets ▾ Shortcuts ▾ Search [ ] [ ] [ ]

Home Session Manager

Global Settings  
Communication Prof...  
Network Configur... ▾  
Device and Locati... ▾  
Application Confi... ▾  
System Status ^  
Load Factor  
**SIP Entity Monit...**  
Managed Band...

**All Monitored SIP Entities**

Run Monitor

10 Items Filter: Enable

<input type="checkbox"/>	SIP Entity Name
<input type="checkbox"/>	<a href="#">DR-CM</a>
<input type="checkbox"/>	<a href="#">IPO2-IPOSE</a>
<input type="checkbox"/>	<a href="#">DR-CM-5212</a>
<input type="checkbox"/>	<a href="#">DR-CM-5077</a>
<input type="checkbox"/>	<a href="#">AACC-VMCS</a>
<input type="checkbox"/>	<a href="#">EP-MPP</a>
<input type="checkbox"/>	<a href="#">SBCE</a>
<input type="checkbox"/>	<a href="#">DR-IXM</a>
<input type="checkbox"/>	<a href="#">DR-CM-5053</a>
<input checked="" type="checkbox"/>	<a href="#">DV2000</a>

Select : All, None

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

**AVAYA** Aura® System Manager 10.1

Users ▾ Elements ▾ Services ▾ Widgets ▾ Shortcuts ▾ Search [ ] [ ] [ ]

Home Session Manager

S...

**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.

Status Details for the selected Session Manager:

**All Entity Links to SIP Entity: DV2000**

Summary View

1 Item Filter: Enable

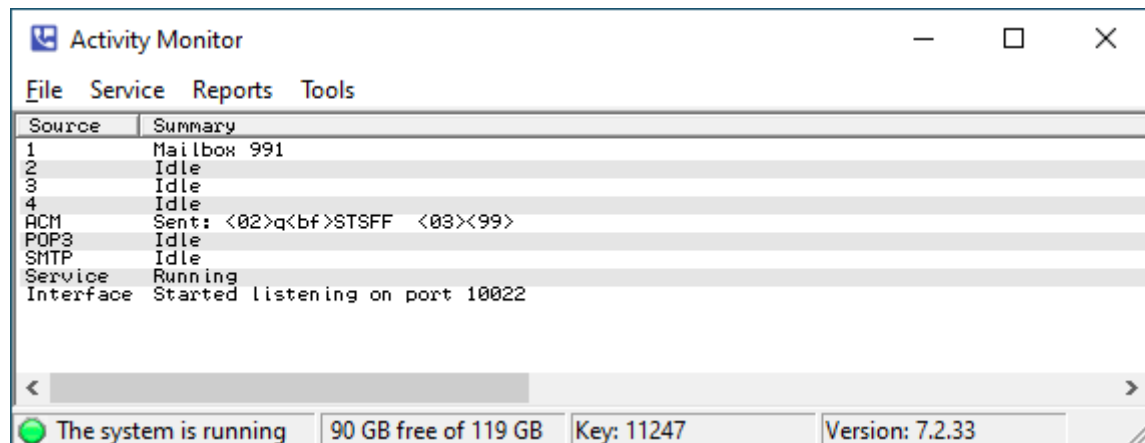
	Session Manager Name	Session Manager IP Address	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
<input type="radio"/>	<a href="#">DR-SM</a>	IPv4	10.64.101.208	5060	UDP	FALSE	UP	200 OK	UP

Select : None



From the DV2000 server, select **Start → DV2000 → Activity Monitor** to launch Activity Monitor.

Place an incoming call from the PSTN to reach the DV2000 main number in **Section 3**. Verify that the calling party hears the greeting announcement from DV2000, and that the **Activity Monitor** screen reflects an active connection with **Mailbox 991**, which is the default mailbox for auto attendant.



## 9. Conclusion

These Application Notes describe the configuration steps required for DuVoice DV2000 7.2 to successfully interoperate with Avaya Aura® Communication Manager 10.1 and Avaya Aura® Session Manager 10.1. All feature and serviceability test cases were completed with observations noted in **Section 2.2**.

## 10. Additional References

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

1. *Administering Avaya Aura® Communication Manager*, Release 10.1.x, Issue 2, September 2022 available at <http://support.avaya.com>.
2. *Administering Avaya Aura® Session Manager*, Release 10.1, Issue 4, September 2022, available at <http://support.avaya.com>.
3. *DV2000 System Reference Guide*, available at <https://support.duvoice.com/product/vs7/manual/home>.

---

**©2022 Avaya Inc. All Rights Reserved.**

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya DevConnect Program at [devconnect@avaya.com](mailto:devconnect@avaya.com).