



Avaya Solution & Interoperability Test Lab

Application Notes for DiVitas Mobile Unified Communications with Avaya AuraTM Communication Manager and Avaya AuraTM Session Manager – Issue 1.0

Abstract

These Application Notes describe the configuration steps required to integrate the DiVitas Mobile Unified Communications solution with Avaya AuraTM Communication Manager and Avaya AuraTM Session Manager. DiVitas consists of two key components: the DiVitas Client and the DiVitas Server. The DiVitas Client is installed on a mobile handset, such as the Nokia E- and N-Series, and provides access to DiVitas mobile communications features. The DiVitas Server monitors connections with DiVitas Clients and proactively identifies the optimal network connection for each call. The DiVitas solution provides the seamless convergence of WiFi and cellular networks enabling roaming (back and forth) between the two networks. The DiVitas Client increases user's accessibility by extending their office phone to the WiFi and cellular networks. This is accomplished by mapping the DiVitas Client to a desktop phone on Avaya AuraTM Communication Manager. Incoming calls can then ring at both phones simultaneously and the call can be answered at either phone. In addition, Avaya AuraTM Communication Manager and Avaya AuraTM Session Manager provide DiVitas Clients with access to the PSTN and to other local stations in the enterprise through a SIP trunk integration.

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 to integrate the DiVitas Mobile Unified Communications solution with Avaya Aura™ Communication Manager and Avaya Aura™ Session Manager. DiVitas consists of two key components: the DiVitas Client and the DiVitas Server. The DiVitas Client is installed on a mobile handset, such as the Nokia E- and N-Series, and provides access to DiVitas mobile communications features. The DiVitas Server monitors connections with DiVitas Clients and proactively identifies the optimal network connection for each call. The DiVitas solution provides the seamless convergence of WiFi and cellular networks enabling roaming (back and forth) between the two networks. The DiVitas Client increases user's accessibility by extending their office phone to the WiFi and cellular networks. This is accomplished by mapping the DiVitas Client to a desktop phone on Avaya Aura™ Communication Manager. Incoming calls can then ring at both phones simultaneously and the call can be answered at either phone. In addition, Avaya Aura™ Communication Manager and Avaya Aura™ Session Manager provide DiVitas Clients with access to the PSTN and to other local stations in the enterprise through a SIP trunk integration.

To provide voicemail coverage for the DiVitas Clients using Avaya Modular Messaging, see [4] *Application Notes for DiVitas Mobile Unified Communications with Avaya Modular Messaging*.

1.1. Interoperability Compliance Testing

The focus of the interoperability compliance test was to verify call establishment and basic telephony features between DiVitas Clients registered to the DiVitas Mobile UC Server, telephones on Avaya Aura™ Communication Manager, and the PSTN. The DiVitas Client was installed on Nokia E51 and N95 mobile handsets and mapped to an H.323 IP station on Avaya Aura™ Communication Manager. The general test approach was to verify the following functionality:

- Establishing calls between DiVitas Clients and H.323, digital, and analog stations on Avaya Aura™ Communication Manager.
- Establishing calls between the DiVitas Clients and the PSTN.
- Establishing calls with the DiVitas Clients while they were in WiFi and Cellular modes.
- Ability to hold a call, transfer a call, and establish a conference.
- Conferencing using the DiVitas Bridge.
- Conferencing initiated by a station on Avaya Aura™ Communication Manager.
- Displaying the calling party number on the DiVitas Clients.
- Simultaneous ringing on a desktop IP phone and DiVitas Client when an incoming call is received.
- Ability of DiVitas Clients to roam between the WiFi and Cellular networks.
- Call establishment using G.711mu-law codec.

The serviceability testing focused on verifying the ability of the DiVitas Mobile UC Server to recover from adverse conditions, such as power failures and disconnecting cables to the IP network. In addition, the ability of the DiVitas Mobile UC Server to recover from Avaya S8730 Server interchange and from cycling power on Session Manager was also verified.

1.2. Support

For technical support on the DiVitas Mobile Unified Communications Solution and how to configure dual mode handsets connected to it, consult the support pages at <http://www.divitas.com/support.html> or contact technical support at:

- Telephone: (866) 857-6087
- E-Mail: support@divitas.com

2. Reference Configuration

Figure 1 illustrates a sample configuration consisting of a pair of Avaya S8730 Servers running Avaya AuraTM Communication Manager, an Avaya G650 Media Gateway, Avaya AuraTM Session Manager, and dual-mode wireless telephones registered with DiVitas Mobile Unified Communications. Each DiVitas Client was paired with an H.323 IP telephone on Avaya AuraTM Communication Manager. The solution described herein is also applicable to other Avaya Servers and Media Gateways. Avaya 9600 Series H.323 IP Telephones and Avaya analog and digital telephones were included in the configuration to verify calls with the SIP-based DiVitas Mobile UC Server and DiVitas Clients. Calls were also routed from the DiVitas Clients to the PSTN through Avaya AuraTM Communication Manager and Avaya AuraTM Session Manager. A SIP trunk was established between the DiVitas Mobile UC Server and Avaya AuraTM Session Manager. The Avaya G650 Media Gateway connected to the PSTN via an ISDN-PRI trunk. Avaya AuraTM System Manager was used to configure Avaya AuraTM Session Manager.

Note: While a DiVitas Client is in Cellular mode, it communicates with the DiVitas Mobile UC Server through a Cellular Voice Channel (CVC). When in Cellular mode, the DiVitas Client places a call using a PSTN number assigned to the DiVitas Mobile UC Server. CVC enables the client to make and receive voice calls and use voice features such as hold and resume. CVC supports multiple simultaneous calls and is used when the Cellular Data Channel (CDC) is not available, which requires a public IP address assigned to the DiVitas Mobile UC Server. In this configuration, CVC was used.

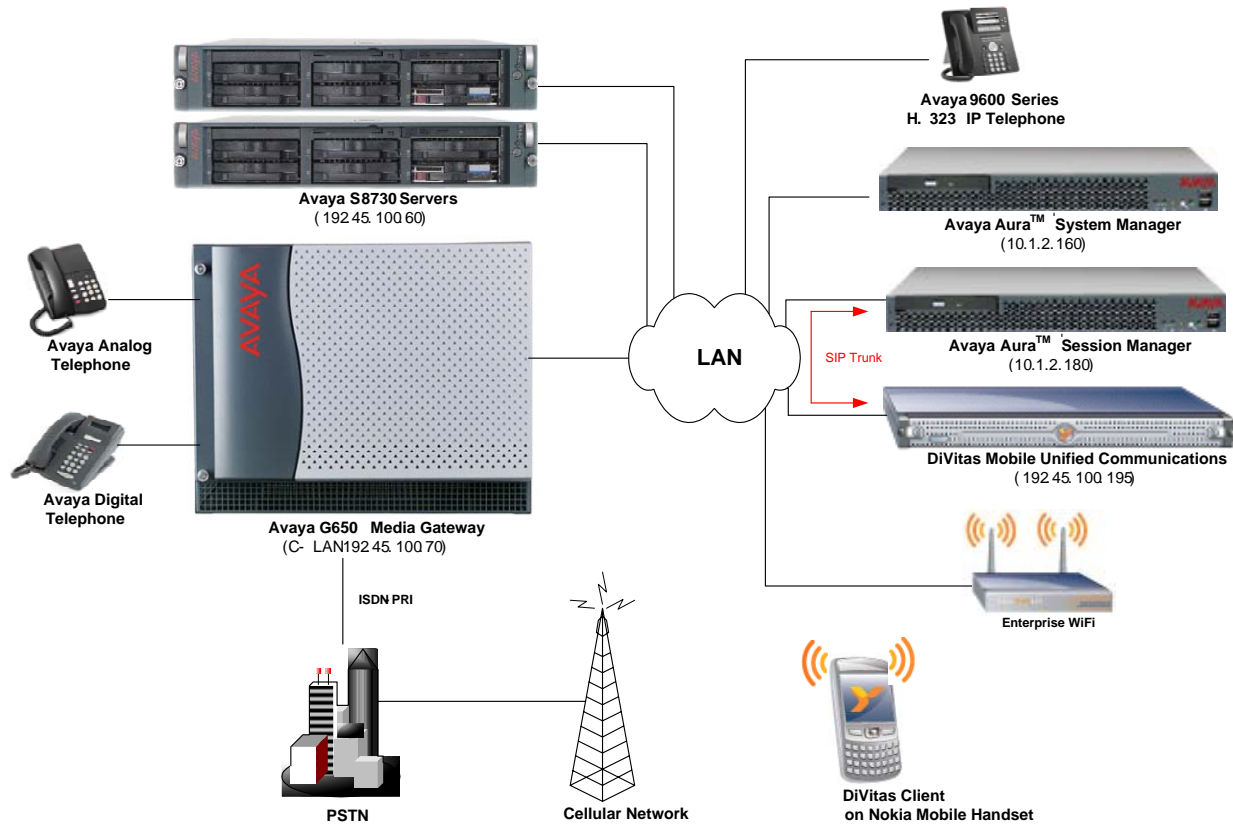


Figure 1: DiVitas Mobile Unified Communications with Avaya SIP-based Network

3. Equipment and Software Validated

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

Equipment	Software/Firmware
Avaya S8730 Server with G650 Media Gateway	Avaya Aura™ Communication Manager 5.2 (R015x.02.0.947.3) with Service Pack 1 (Patch 17294)
Avaya Aura™ Session Manager	1.1.3.1.18022
Avaya Aura™ System Manager	1.0
Avaya 9600 Series IP Telephones	3.0 (H.323)
Avaya 6400 Series Digital Telephones	--
Avaya Analog Telephones	--
DiVitas Mobile Unified Communications	2.7.2.0 Build 39
DiVitas Client on Nokia E51 and N95	2.7.2.0 Build 39

Table 1: Equipment and Software Validated

4. Configure Avaya Aura™ Communication Manager

This section describes the procedure for configuring a SIP trunk to Avaya Aura™ Session Manager, a local station mapped to a DiVitas Client, and call routing. In addition, the required customer software options are checked and the dial plan is configured. Avaya Aura™ Communication Manager was configured using the System Access Terminal (SAT). Refer to [1] and [3] for additional details.

4.1. Check Customer Options

Prior to configuring the SIP trunk and stations, verify that the required customer software options are available. Enter the **display system-parameters customer-options** command to verify that the number of EC500 telephones and SIP trunks supported by the system are sufficient. If not, contact an authorized Avaya account representative to obtain additional licenses. The EC500 license also enables CSP (Cellular Service Provider) which is used in this configuration.

display system-parameters customer-options		Page 1 of 11
OPTIONAL FEATURES		
G3 Version: V15	Software Package: Standard	
Location: 1	RFA System ID (SID): 1	
Platform: 6	RFA Module ID (MID): 1	
	USED	
Platform Maximum Ports:	48000	779
Maximum Stations:	36000	261
Maximum XMOBILE Stations:	0	0
Maximum Off-PBX Telephones - EC500:	50	2
Maximum Off-PBX Telephones - OPS:	50	33
Maximum Off-PBX Telephones - PBFMC:	0	0
Maximum Off-PBX Telephones - PVFMC:	0	0
Maximum Off-PBX Telephones - SCCAN:	0	0
(NOTE: You must logoff & login to effect the permission changes.)		

Figure 2: System-Parameters Customer-Options Form – EC500

display system-parameters customer-options		Page 2 of 11
OPTIONAL FEATURES		
IP PORT CAPACITIES		USED
Maximum Administered H.323 Trunks:	5000	258
Maximum Concurrently Registered IP Stations:	18000	6
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:	10	0
Maximum Video Capable H.323 Stations:	0	0
Maximum Video Capable IP Softphones:	0	0
Maximum Administered SIP Trunks:	555	80
Maximum Administered Ad-hoc Video Conferencing Ports:	0	0
Maximum Number of DS1 Boards with Echo Cancellation:	0	0
Maximum TN2501 VAL Boards:	128	1
Maximum Media Gateway VAL Sources:	0	0
Maximum TN2602 Boards with 80 VoIP Channels:	128	0
Maximum TN2602 Boards with 320 VoIP Channels:	128	0
Maximum Number of Expanded Meet-me Conference Ports:	0	0
(NOTE: You must logoff & login to effect the permission changes.)		

Figure 3: System-Parameters Customer-Options Form – SIP Trunks

4.2. Configure Dial Plan

In the **Dial Plan Analysis Table**, a dialed string beginning with '2' was configured as extensions for the local stations mapped to DiVitas Clients and for other H.323, digital, and analog telephones in this configuration. The other entries in bold are used for trunk access codes and the AAR/ARS features access codes. In this configuration, the AAR access code is '8' and the ARS access code is '9'.

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

Figure 4: Dial Plan Analysis

4.3. Configure SIP Trunk

This section covers the configuration of the SIP trunk between Communication Manager and Session Manager, including the IP node names, IP network region, and IP codec set.

In the **IP Node Names** form, associate a name with the IP addresses of Session Manager and the C-LAN board in the Avaya G650 Media Gateway.

change node-names ip		IP NODE NAMES		Page 1 of 2	
Name	IP Address				
clan2	192.45.100.70				
default	0.0.0.0				
medpro2	192.45.100.71				
SessMgr	10.1.2.180				

Figure 5: IP Nodes Names

In the **IP Network Region** form, the **Authoritative Domain** field is configured to match the domain name configured on Session Manager. In this configuration, the domain name is *avaya.com*. By default, **IP-IP Direct Audio** (shuffling) is enabled to allow audio traffic to be sent directly between SIP endpoints without using media resources in the Avaya G650 Media Gateway. The **IP Network Region** form also specifies the **IP Codec Set** to be used for local calls and calls routed over the SIP trunk to Session Manager. This codec set is used when its corresponding network region (i.e., IP Network Region '1') is specified in the SIP signaling group as shown in **Figure 8**. The IP network region for local and outgoing trunk calls may be different.

```

change ip-network-region 1                                     Page 1 of 19
                                IP NETWORK REGION
    Region: 1
    Location: 1      Authoritative Domain: avaya.com
    Name: Avaya region
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: 65531
DIFFSERV/TOS PARAMETERS                                RTCP Reporting Enabled? n
    Call Control PHB Value: 34
    Audio PHB Value: 46
    Video PHB Value: 26
802.1P/Q PARAMETERS
    Call Control 802.1p Priority: 7
    Audio 802.1p Priority: 6
    Video 802.1p Priority: 5      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                RSVP Enabled? n
    H.323 Link Bounce Recovery? y
    Idle Traffic Interval (sec): 20
    Keep-Alive Interval (sec): 5
    Keep-Alive Count: 5

```

Figure 6: IP Network Region

In the **IP Codec Set** form, select the audio codec type supported for calls routed over the SIP trunk to the DiVitas Clients. The form is accessed via the **change ip-codec-set 1** command. Note that IP codec set '1' was specified in IP Network Region '1' shown in **Figure 6**. The default settings of the **ip-codec-set** form are shown below. Currently, the DiVitas Mobile UC solution supports the G.711 codec.

```

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:
3:

```

Figure 7: IP Codec Set

Prior to configuring a SIP trunk group for communication with Session Manager, a SIP signaling group must be configured. Configure the **Signaling Group** form as shown in **Figure 8** with the following parameters:

- Set the **Group Type** field to *sip*.
- The **Transport Method** field will default to *tls* (Transport Layer Security).
- Specify the C-LAN board in the G650 Media Gateway and Session Manager as the two ends of the signaling group in the **Near-end Node Name** field and the **Far-end Node Name** field, respectively. These field values are taken from the **IP Node Names** form shown in **Figure 5**.
- Ensure that the recommended TLS port value of *5061* is configured in the **Near-end Listen Port** and the **Far-end Listen Port** fields.
- Specify the IP network region to be used for outgoing calls that use this signaling group in **Far-end Network Region** field. The codec type for the outgoing call is derived from the IP codec set specified in the IP network region. In this configuration, IP network region '1' and IP codec set '1' is used which allows the G.711mu-law codec for the call.
- Enter the domain name of Session Manager in the **Far-end Domain** field. In this configuration, the domain name is *avaya.com*. This domain is specified in the Uniform Resource Identifier (URI) of the "SIP To Address" in the INVITE message. Misconfiguring this field may prevent calls from being successfully established over the SIP trunk.
- If calls to/from SIP endpoints are to be shuffled, then the **Direct IP-IP Audio Connections** field must be set to 'y'.
- The **DTMF over IP** field should be set to the default value of *rtp-payload*. Communication Manager supports DTMF transmission using RFC 2833. Setting the field to *rtp-payload* implies RFC 2833. The default values for the other fields may be used.

change signaling-group 702		Page 1 of 1
SIGNALING GROUP		
Group Number: 702	Group Type: sip	
	Transport Method: tls	
IMS Enabled? n		
Near-end Node Name: clan2	Far-end Node Name: SessMgr	
Near-end Listen Port: 5061	Far-end Listen Port: 5061	
	Far-end Network Region: 1	
Far-end Domain: avaya.com		
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? y	
Enable Layer 3 Test? n	Direct IP-IP Early Media? n	
H.323 Station Outgoing Direct Media? n	Alternate Route Timer(sec): 6	

Figure 8: Signaling Group

Configure the **Trunk Group** form as shown in **Figure 9**. Set the **Group Type** field to *sip*, set the **Service Type** field to *tie*, specify the signaling group associated with this trunk group in the **Signaling Group** field, and specify the **Number of Members** supported by this SIP trunk group. Configure the other fields in bold and accept the default values for the remaining fields.

change trunk-group 702		Page 1 of 21	
TRUNK GROUP			
Group Number: 702	Group Type: sip	CDR Reports: y	
Group Name: To SessMgr	COR: 1	TN: 1	TAC: 176
Direction: two-way	Outgoing Display? n		
Dial Access? n	Night Service:		
Queue Length: 0			
Service Type: tie	Auth Code? n		
Signaling Group: 702 Number of Members: 20			

Figure 9: Trunk Group – Page 1

On Page 3 of the trunk group form, set the **Format** field to *public*. This field specifies the format of the calling party number sent to the far-end.

change trunk-group 702		Page 3 of 21	
TRUNK FEATURES			
ACA Assignment? n	Measured: none	Maintenance Tests? y	
Numbering Format: public			
UUI Treatment: service-provider			
Replace Restricted Numbers? n			
Replace Unavailable Numbers? n			
Show ANSWERED BY on Display? y			

Figure 10: Trunk Group – Page 3

Configure the **Public/Unknown Numbering Format** form to send the calling party number to the far-end. Add an entry so that local stations with a 5-digit extension beginning with '2' and whose calls are routed over PSTN trunk group '6' or SIP trunk group '702' have their number sent to the far-end for display purposes. The PSTN trunk group is discussed in Section 4.4. In the example shown in **Figure 11**, the **CPN Prefix** field is left blank and the **CPN Len** field is set to '5' indicating that the 5-digit extension corresponding to the calling party will be sent to the far-end. Additional entries may be included to cover other extensions.

change public-unknown-numbering 2		Page 1 of 2	
NUMBERING - PUBLIC/UNKNOWN FORMAT			
Ext	Ext	Trk	Total
Len	Code	Grp(s)	CPN
		Prefix	Len
5	2	6	5
5	2	702	5
Total Administered: 22			
Maximum Entries: 9999			

Figure 11: Public Unknown Numbering Format

To allow a call to the H.323 IP phone to be delivered to the DiVitas Client at the same time, the **Stations with Off-PBX Telephone Integration** form must be configured. On this form, specify the extension of the H.323 IP phone in the **Station Extension** field and set the **Application** field to *CSP*, which stands for Cellular Service Provider. The **Phone Number** field is set to the digits to be sent over the SIP trunk. In this case, the 5-digit extension of the DiVitas Client is specified and delivered to the DiVitas Mobile UC server. Finally, the **Trunk Selection** field is set to '702', the SIP trunk group number. This field specifies the trunk group used to route the call. Another option for routing a call over a SIP trunk group is to use Auto Alternate Routing (AAR) or Auto Route Selection (ARS) routing instead. In this case, the **Trunk Selection** field would be set to *aar* or *ars*. Configuration of other AAR or ARS forms would also be required. Refer to [1] for information on routing calls using AAR or ARS. Repeat this step for each DiVitas Client associated with a desk phone.

change off-pbx-telephone station-mapping 24511						Page	1 of	2
STATIONS WITH OFF-PBX TELEPHONE INTEGRATION								
Station	Application	Dial	CC	Phone Number	Trunk	Config		
Extension		Prefix			Selection	Set		
24511	CSP	-		24511	702	1		

Figure 13: Stations with Off-PBX Telephone Integration

4.6. Call Routing

This section describes how to configure call routing on Communication Manager for calls to the PSTN and for establishing a CVC from the DiVitas Clients in Cellular mode to the DiVitas Server.

4.6.1. Call Routing from DiVitas Clients to the PSTN

To call the PSTN, DiVitas Clients dial the ARS feature access code '9' followed by the 11-digit number. On Communication Manager, the call is steered to the **ARS Digit Analysis Table** where the call is routed based on the dialed 11-digit number. In this configuration, routing for calls to the 408 and 732 area codes was configured. Configure the **ARS Digit Analysis Table** as shown in **Figure 14**. In this example, calls are routed over route pattern '732'.

change ars analysis 14						Page	1 of	2
ARS DIGIT ANALYSIS TABLE								
Location: all						Percent Full:	1	
	Dialed	Total	Route	Call	Node	ANI		
	String	Min Max	Pattern	Type	Num	Reqd		
1408		11 11	732	fnpa		n		
1732		11 11	732	fnpa		n		

Figure 14: ARS Digit Analysis Table

change route-pattern 732													Page	1 of	3
Pattern Number: 732 Pattern Name: To PSTN															
SCCAN? n Secure SIP? n															
Grp	FRL	NPA	Pfx	Hop	Toll	No.	Inserted						DCS/	IXC	
No			Mrk	Lmt	List	Del	Digits						QSIG		
													Intw		
1:	6	0		1									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			Dgts	Format	
										Subaddress
1:	y	y	y	y	y	n	n		rest	none
2:	y	y	y	y	y	n	n		rest	none
3:	y	y	y	y	y	n	n		rest	none
4:	y	y	y	y	y	n	n		rest	none
5:	y	y	y	y	y	n	n		rest	none
6:	y	y	y	y	y	n	n		rest	none

4.6.2. Call Routing from the PSTN to the DiVitas Clients or CVC

4.6.3. Call Routing for CVC on DiVitas Mobile UC Server

change uniform-dialplan 2						Page	1 of	2
UNIFORM DIAL PLAN TABLE								
						Percent Full: 0		
Matching			Insert		Node			
Pattern	Len	Del	Digits	Net	Conv	Num		
24555	5	0		aar	n			

12 of 45
DiVitasMUCv272

In the **AAR Digit Analysis Table**, an entry is added for dialed string “24555”, which routes that call over route pattern ‘702’.

change aar analysis 24						Page	1 of	2
AAR DIGIT ANALYSIS TABLE								
Location: all						Percent Full:	1	
Dialed	Total	Route	Call	Node	ANI			
String	Min Max	Pattern	Type	Num	Reqd			
24555	5 5	702	aar		n			

Figure 17: AAR Analysis

In **Route Pattern ‘702’**, calls are routed over SIP trunk group ‘702’ with no digit manipulation being performed. The exact dial string is sent to Session Manager, which routes the call based on the 5-digit extension.

change route-pattern 702						Page	1 of	3
Pattern Number: 702 Pattern Name: To SessMgr								
SCCAN? n Secure SIP? n								
Grp FRL NPA Pfx Hop Toll No. Inserted	DCS/ IXC							
No Mrk Lmt List Del Digits	QSIG							
	Intw							
1: 702 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 next							
2: y y y y y n n	rest none							
3: y y y y y n n	rest none							
4: y y y y y n n	rest none							
5: y y y y y n n	rest none							
6: y y y y y n n	rest none							

Figure 18: Route Pattern

5. Configure Avaya Aura™ Session Manager

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

- SIP domain
- Logical/physical Locations that can be occupied by SIP Entities
- Adaptations to perform digit conversion
- SIP Entities corresponding to Avaya Aura™ Session Manager and DiVitas MUC
- Entity Links, which define the SIP trunk parameters used by Avaya Aura™ Session Manager when routing calls to/from SIP Entities
- Time Ranges during which routing policies are active
- Routing Policies, which control call routing between the SIP Entities
- Dial Patterns, which govern to which SIP Entity a call is routed
- Session Manager, corresponding to the Avaya Aura™ Session Manager Server to be managed by Avaya Aura™ System Manager.

Configuration is accomplished by accessing the browser-based GUI of Avaya Aura™ System Manager using the URL “http://<ip-address>/IMSM”, where <ip-address> is the IP address of Avaya Aura™ System Manager. Log in with the appropriate credentials and accept the Copyright Notice. The menu shown below is displayed. Expand the **Network Routing Policy** Link on the left side as shown. The sub-menus displayed in the left column below will be used to configure all but the last of the above items (**Sections 5.1** through **5.8**).

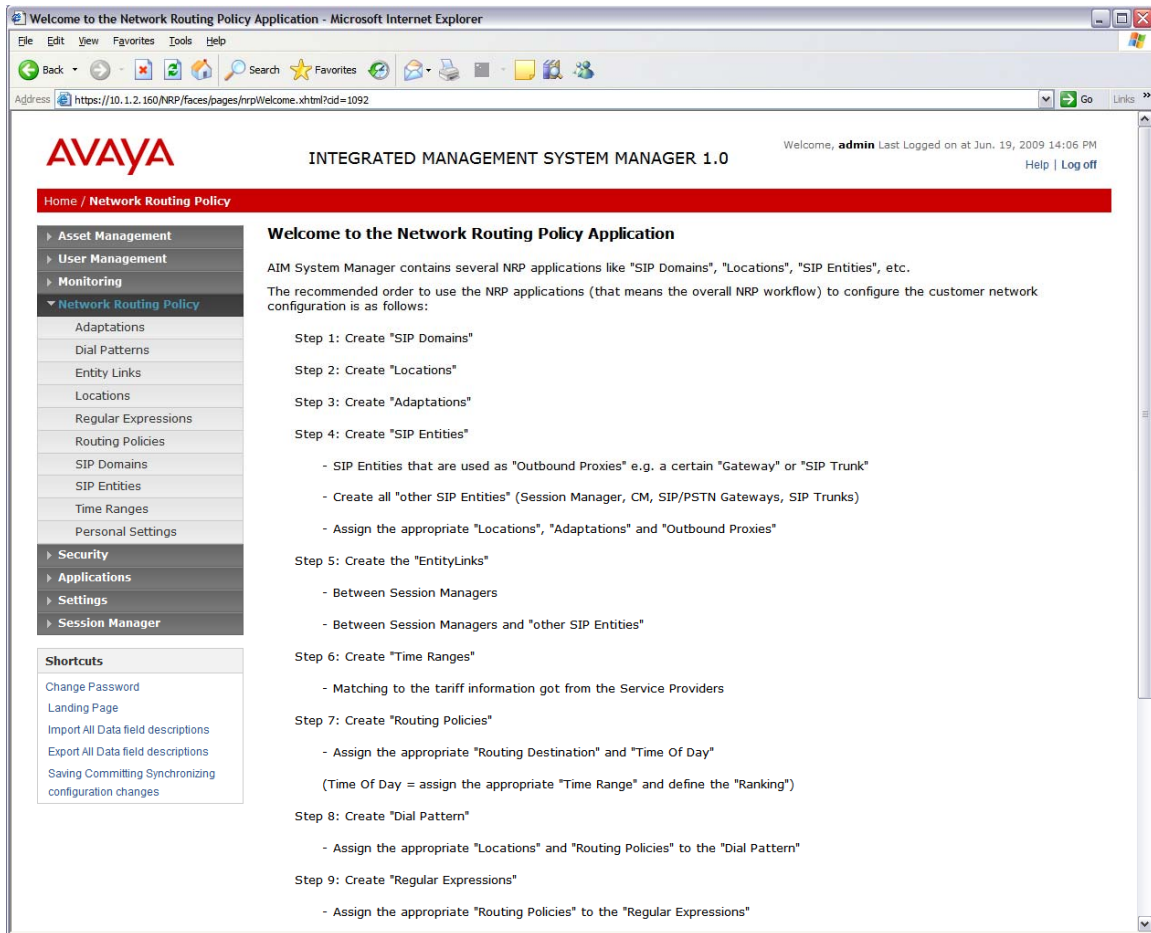


Figure 19: Session Manager

5.1. Specify SIP Domain

Add the SIP domain for which the communications infrastructure will be authoritative. Do this by selecting **SIP Domains** on the left and clicking the **New** button on the right. The following screen will then be shown. Fill in the following:

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

Click **Commit**.

Since the sample configuration does not deal with any other domains, no additional domains need to be added.

The screenshot shows the Avaya Integrated Management System Manager 1.0 interface. The top header includes the Avaya logo, the title "INTEGRATED MANAGEMENT SYSTEM MANAGER 1.0", and a welcome message for user "admin" with the last login time "Jun. 23, 2009 14:27 PM". There are links for "Help" and "Log off".

The left sidebar contains a navigation menu with the following items: Asset Management, User Management, Monitoring, Network Routing Policy (expanded), Adaptations, Dial Patterns, Entity Links, Locations, Regular Expressions, Routing Policies, SIP Domains (highlighted), SIP Entities, Time Ranges, Personal Settings, Security, Applications, Settings, and Session Manager.

The main content area is titled "SIP Domains" and includes "Commit" and "Cancel" buttons. Below the title, there is a table with one item:

Name	Notes
avaya.com	

Below the table, there is a red asterisk and the text "Input Required", followed by "Commit" and "Cancel" buttons.

Figure 20: SIP Domain

5.2. Add Locations

Locations can be used to identify logical and/or physical locations where SIP Entities reside for purposes of bandwidth management. A Location is added for the Avaya and the DiVitas environments. To add a location, select **Locations** on the left and click on the **New** button on the right. The following screen will then be shown. Fill in the following:

Under *General*:

- **Name:** A descriptive name.
- **Notes:** Descriptive text (optional).

Under *Location Pattern*:

- **IP Address Pattern:** A pattern used to logically identify the location.
- **Notes:** Descriptive text (optional).

The screen below shows addition of the *Lincroft* location, which includes Avaya Aura™ Communication Manager and Avaya Aura™ Session Manager. Click **Commit** to save each Location definition.

AVAYA INTEGRATED MANAGEMENT SYSTEM MANAGER 1.0 Welcome, **admin** Last Logged on at Jun. 19, 2009 09:38 AM Help | Log off

Home / Network Routing Policy / Locations / Location Details

Location Details [Commit] [Cancel]

General

Name	Notes
* Lincroft	Session Manager and ACM

Managed Bandwidth: [] Kbit/sec

*** Average Bandwidth per Call:** [80] Kbit/sec

*** Time to Live (secs):** [3600]

Location Pattern [Add] [Remove]

3 Items | Refresh Filter: Enable

IP Address Pattern	Notes
<input type="checkbox"/> * 192.45.100.*	ACM
<input type="checkbox"/> * 10.1.2.*	Session Manager

Select: All, None (0 of 3 Selected)

*** Input Required** [Commit] [Cancel]

Shortcuts

- Change Password
- Locations Details field descriptions
- Saving Committing Synchronizing configuration changes

Figure 21: Location

The screen below shows addition of the *Lincroft-Mobile* location, which includes DiVitas Mobile UC Server. Click **Commit** to save each Location definition.

INTEGRATED MANAGEMENT SYSTEM MANAGER 1.0

Welcome, **admin** Last Logged on at Jun. 23, 2009 14:27 PM
[Help](#) | [Log off](#)

Home / Network Routing Policy / Locations / Location Details

Asset 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
Locations Details field descriptions
Saving Committing Synchronizing configuration changes

Location Details

CommitCancel

General

Name	Notes
Lincroft-Mobile	DiVitas

Managed Bandwidth:
Kbit/sec

Average Bandwidth per Call:
 80
Kbit/sec

Time to Live (secs):
 3600

Location Pattern

AddRemove

1 Item Refresh
Filter: Enable

IP Address Pattern	Notes
192.45.100.195	DiVitas MUC

Select: All, None (0 of 1 Selected)

Input Required

CommitCancel

The fields under *General* can be filled in to specify bandwidth management parameters between Avaya Aura™ Session Manager and this location. These were not used in the sample configuration, and reflect default values. Note also that although not implemented in the sample configuration, routing policies can be defined based on location.

5.3. Add Adaptations

Adaptations are used to modify SIP messages which are leaving Session Manager (egress adaptation) and which are entering Session Manager (ingress adaptation). One reason to use an adaptation is to convert strings containing calling and called party numbers from the local dial plan of a SIP entity to the dial plan administered on the Session Manager, and vice versa. Session Manager is installed with a module called *DigitConversionAdapter*, which can convert digit strings in various message headers.

In this example, an ingress adaptation is used to convert 5-digit extensions to 7-digit numbers when routing calls from DiVitas Clients to local stations on Communication Manager. This allows Session Manager to use a 7-digit string to route the call. As the call is routed to Communication Manager, an egress adaptation converts the 7-digit number back to a 5-digit extension. No adaptations were used for calls routed from Communication Manager to DiVitas Clients (i.e., 5-digit extensions were used end-to-end). This digit conversion was required to properly route calls to the desktop phones paired with a DiVitas Client because both devices were assigned the same extension.

To add an Adaptation, select **Adaptations** on the left and click on the **New** button on the right. The following screen is displayed. Fill in the following:

Under *General*:

- **Name:** A descriptive name.
- **Adaptation Module:** Specify the appropriate adaptation module.

Under *Digit Conversion for Incoming Calls* and *Digit Conversion for Outgoing Calls*, click **Add**, and then edit the fields in the resulting new row as shown below:

- **Matching Pattern:** Dialed number or prefix.
- **Min:** Minimum length of dialed number.
- **Max:** Maximum length of dialed number.
- **Delete Digits:** Number of digits to delete.
- **Address to modify:** A setting of both looks for adaptations on both origination and destination type headers.

Defaults can be used for the remaining fields. Click **Commit** to save each SIP Entity definition.

The following screen shows the ingress adaptation that converts a 5-digit extension starting with “2” to a 7-digit number starting with “852”.

AVAYA INTEGRATED MANAGEMENT SYSTEM MANAGER 1.0 Welcome, **admin** Last Logged on at Jun. 23, 2009 14:27 PM Help | Log off

Home / Network Routing Policy / Adaptations / Adaptation Details

Adaptation Details [Commit] [Cancel]

General

Name	Adaptation Module	Egress URI Parameters	Notes
• DiVitas	DigitConversionAdapter		

Digit Conversion for Incoming Calls

[Add] [Remove]

1 Item | Refresh Filter: Enable

<input type="checkbox"/>	Matching Pattern	Min	Max	Delete Digits	Insert Digits	Address to modify	Notes
<input type="checkbox"/>	• 2	• 5	• 5	• 0	85	both	

Select: All, None (0 of 1 Selected)

Digit Conversion for Outgoing Calls

[Add] [Remove]

0 Items | Refresh Filter: Enable

<input type="checkbox"/>	Matching Pattern	Min	Max	Delete Digits	Insert Digits	Address to modify	Notes
--------------------------	------------------	-----	-----	---------------	---------------	-------------------	-------

* Input Required [Commit] [Cancel]

Figure 22: Adaptation for DiVitas Mobile UC Server

The following screen shows the egress adaptation that converts a 7-digit number starting with “852” back to a 5-digit extension adhering to the dial plan of Communication Manager.

AVAYA INTEGRATED MANAGEMENT SYSTEM MANAGER 1.0 Welcome, **admin** Last Logged on at Jun. 23, 2009 14:27 PM Help | Log off

Home / Network Routing Policy / Adaptations / Adaptation Details

Adaptation Details [Commit] [Cancel]

General

Name	Adaptation Module	Egress URI Parameters	Notes
• devcon31	DigitConversionAdapter		

Digit Conversion for Incoming Calls

[Add] [Remove]

0 Items | Refresh Filter: Enable

<input type="checkbox"/>	Matching Pattern	Min	Max	Delete Digits	Insert Digits	Address to modify	Notes
--------------------------	------------------	-----	-----	---------------	---------------	-------------------	-------

Digit Conversion for Outgoing Calls

[Add] [Remove]

1 Item | Refresh Filter: Enable

<input type="checkbox"/>	Matching Pattern	Min	Max	Delete Digits	Insert Digits	Address to modify	Notes
<input type="checkbox"/>	• 852	• 7	• 7	• 2		both	

Select: All, None (0 of 1 Selected)

* Input Required [Commit] [Cancel]

Figure 23: Adaptation for Avaya Aura™ Communication Manager

5.4. Add SIP Entities

A SIP Entity must be added for Avaya Aura™ Session Manager, Avaya Aura™ Communication Manager, and the DiVitas MUC Server. In the sample configuration, a SIP Entity is added for the ASM, the C-LAN board in the Avaya G650 Media Gateway, and the DiVitas MUC Server. To add a SIP Entity, select **SIP Entities** on the left and click on the **New** button on the right. The following screen is displayed. Fill in the following:

Under *General*:

- **Name:** A descriptive name.
- **FQDN or IP Address:** IP address of the ASM or the signaling interface on the telephony system.
- **Type:** “Session Manager” for Avaya Aura™ Session Manager,
“CM” for Avaya Communication Manager, and
“Other” for DiVitas MUC Server.
- **Location:** Select one of the locations defined previously.
- **Time Zone:** Time zone for this location.

Under *Port*¹, click **Add**, and then edit the fields in the resulting new row as shown below:

- **Port:** Port number on which the system listens for SIP requests.
- **Protocol:** Transport protocol to be used to send SIP requests.
- **Default Domain** The domain used for the enterprise (e.g., “avaya.com”).

Defaults can be used for the remaining fields. Click **Commit** to save each SIP Entity definition.

¹ Although not tested, the **Ports** section of the “SM2” **SIP Entity** shown in **Figure 24** could have also included an entry to assign the *avaya.com* default domain to messages arriving on port 5060 and using the UDP transport protocol when no domain is specified.

The following screen shows addition of Avaya Aura™ Session Manager. The IP address used is that of the SM-100 Security Module.

AVAYA INTEGRATED MANAGEMENT SYSTEM MANAGER 1.0 Welcome, **admin** Last Logged on at Jun. 19, 2009 09:38 AM Help | Log off

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

SIP Entity Details [Commit] [Cancel]

General

Name	FQDN or IP Address	Type	Notes
SM2	10.1.2.180	Session Manager	

Entity Links

Adaptation: [dropdown]
 Location: [Lincroft] [dropdown]
 Outbound Proxy: [dropdown]
 Time Zone: [America/New_York] [dropdown]
 Override Port & Transport with DNS SRV: ☐
 SIP Timer B/F (secs): * 4
 Credential name: [text field]

Monitoring

Monitoring on/off: [Use Session Manager configuration] [dropdown]

Port

[Add] [Remove]

2 Items | Refresh Filter: Enable

Port	Protocol	Default Domain	Notes
5060	TCP	avaya.com	
5061	TLS	avaya.com	

Select: All, None (0 of 2 Selected)

Figure 24: SIP Entity – Session Manager

The following screen shows addition of Avaya Aura™ Communication Manager. The IP address used is that of the C-LAN board in the Avaya G650 Media gateway. Note that the egress adaptation was assigned to this SIP entity.

AVAYA INTEGRATED MANAGEMENT SYSTEM MANAGER 1.0 Welcome, **admin** Last Logged on at Jun. 23, 2009 14:27 PM Help | Log off

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

SIP Entity Details [Commit] [Cancel]

General

Name	FQDN or IP Address	Type	Notes
devcon31	192.45.100.70	CM	

Entity Links

Adaptation: [devcon31] [dropdown]
 Location: [Lincroft] [dropdown]
 Time Zone: [America/New_York] [dropdown]
 Override Port & Transport with DNS SRV: ☐
 SIP Timer B/F (secs): * 4
 Credential name: [text field]
 Call Detail Recording: [egress] [dropdown]

Monitoring

Monitoring on/off: [Use Session Manager configuration] [dropdown]

* Input Required [Commit] [Cancel]

Figure 25: SIP Entity – Avaya Aura™ Communication Manager

The following screen shows addition of DiVitas Mobile UC Server. Note that the ingress adaptation was assigned to this SIP entity.

The screenshot displays the Avaya Integrated Management System Manager 1.0 web interface. The top navigation bar includes the Avaya logo, the system name, a welcome message for user 'admin', and a 'Log off' link. A red breadcrumb trail shows the path: Home / Network Routing Policy / SIP Entities / SIP Entity Details.

On the left is a sidebar menu with categories: Asset Management, User Management, Monitoring, Network Routing Policy (expanded), Security, Applications, Settings, and Session Manager. Under 'Network Routing Policy', options include Adaptations, Dial Patterns, Entity Links, Locations, Regular Expressions, Routing Policies, SIP Domains, SIP Entities (highlighted), Time Ranges, and Personal Settings.

The main content area is titled 'SIP Entity Details' and contains two tabs: 'General' and 'Monitoring'. The 'General' tab is active and shows a table with one entry:

Name	FQDN or IP Address	Type	Notes
* DiVitas MUC Server	* 192.45.100.195	Other	

Below the table, the 'Entity Links' section includes:

- Adaptation:** A dropdown menu set to 'DiVitas'.
- Location:** A dropdown menu set to 'Lincroft-Mobile'.
- Time Zone:** A dropdown menu set to 'America/New_York'.
- Override Port & Transport with DNS SRV:** An unchecked checkbox.
- SIP Timer B/F (secs):** A text input field containing '4'.
- Credential name:** An empty text input field.
- Call Detail Recording:** A dropdown menu set to 'egress'.

The 'Monitoring' tab is also visible and shows a 'Monitoring on/off' dropdown set to 'Use Session Manager configuration'. At the bottom of the form, there is a red asterisk and the text '* Input Required', along with 'Commit' and 'Cancel' buttons.

Figure 26: SIP Entity – DiVitas Mobile UC Server

5.5. Add Entity Links

SIP trunks from Avaya Aura™ Session Manager to Avaya Aura™ Communication Manager and DiVitas Mobile UC Server are described by Entity links. To add an Entity Link, select **Entity Links** on the left and click on the **New** button on the right. Fill in the following fields in the new row that is displayed:

- **Name:** A descriptive name.
- **SIP Entity 1:** Select the Avaya Aura™ Session Manager.
- **Port:** Port number to which the other system sends SIP requests.
- **SIP Entity 2:** Select the name of the other system.
- **Port:** Port number on which the other system receives SIP requests.
- **Trusted:** Check this box. *Note: If this box is not checked, calls from the associated SIP Entity specified in Section 4.3 will be denied.*

Click **Commit** to save each Entity Link definition. The following screens illustrate adding the two Entity Links for Avaya Aura™ Communication Manager and DiVitas MUC Server.

The screenshot shows the Avaya Integrated Management System Manager 1.0 interface. The left sidebar contains a navigation menu with options: Asset Management, User Management, Monitoring, and Network Routing Policy. Under Network Routing Policy, the following options are listed: Adaptations, Dial Patterns, Entity Links (highlighted), Locations, Regular Expressions, Routing Policies, SIP Domains, and SIP Entities. The main content area is titled 'Entity Links' and contains a table with the following columns: Name, SIP Entity 1, Port, SIP Entity 2, Port, Trusted, Protocol, and Notes. The table contains one row with the following values: Name: SM2 devcon31, SIP Entity 1: SM2, Port: 5061, SIP Entity 2: devcon31, Port: 5061, Trusted: checked, Protocol: TLS, Notes: (empty). Above the table, there is a 'Filter: Enable' dropdown and a 'Refresh' button. Below the table, there is a '* Input Required' message and 'Commit' and 'Cancel' buttons.

Figure 27: Entity Link – Avaya Aura™ Communication Manager

The screenshot shows the Avaya Integrated Management System Manager 1.0 interface. The left sidebar contains a navigation menu with options: Asset Management, User Management, Monitoring, and Network Routing Policy. Under Network Routing Policy, the following options are listed: Adaptations, Dial Patterns, Entity Links (highlighted), Locations, Regular Expressions, Routing Policies, SIP Domains, and SIP Entities. The main content area is titled 'Entity Links' and contains a table with the following columns: Name, SIP Entity 1, Port, SIP Entity 2, Port, Trusted, Protocol, and Notes. The table contains one row with the following values: Name: SM2 DiVitasMUC, SIP Entity 1: SM2, Port: 5060, SIP Entity 2: DiVitas MUC Server, Port: 5060, Trusted: checked, Protocol: UDP, Notes: (empty). Above the table, there is a 'Filter: Enable' dropdown and a 'Refresh' button. Below the table, there is a '* Input Required' message and 'Commit' and 'Cancel' buttons.

Figure 28: Entity Link – DiVitas Mobile UC Server

5.6. Add Time Ranges

Before adding routing policies (see next section), time ranges must be defined during which the policies will be active. In the sample configuration, one policy was defined that would allow routing to occur at anytime. To add this time range, select **Time Ranges**, and click on the left and click on the **New** button on the right. Fill in the following:

- **Name:** A descriptive name (e.g., “Anytime”).
- **Mo through Su** Check the box under each of these headings.
- **Start Time** Enter 00:00.
- **End Time** Enter 23:59.

Click **Commit** to save this time range.

The screenshot shows the Avaya Integrated Management System Manager 1.0 interface. The top header includes the Avaya logo, the title 'INTEGRATED MANAGEMENT SYSTEM MANAGER 1.0', and a welcome message for user 'admin' last logged on at Jun. 23, 2009 14:27 PM. The breadcrumb trail is 'Home / Network Routing Policy / Time Ranges'. The left sidebar contains a tree view with categories: Asset Management, User Management, Monitoring, Network Routing Policy (expanded), Security, Applications, Settings, and Session Manager. Under Network Routing Policy, the options are Adaptations, Dial Patterns, Entity Links, Locations, Regular Expressions, Routing Policies, SIP Domains, SIP Entities, Time Ranges (selected), and Personal Settings. The main content area is titled 'Time Ranges' and has 'Commit' and 'Cancel' buttons. It shows a table with 1 item, a 'Refresh' link, and a 'Filter: Enable' option. The table has columns: Name, Mo, Tu, We, Th, Fr, Sa, Su, Start Time, End Time, and Notes. The row shows 'Anytime' with checkboxes for all days (Mo-Su) checked, Start Time '00:00', and End Time '23:59'. Below the table, there is a red asterisk and the text '* Input Required', followed by 'Commit' and 'Cancel' buttons.

Name	Mo	Tu	We	Th	Fr	Sa	Su	Start Time	End Time	Notes
Anytime	<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	

Figure 29: Time Range

5.7. Add Routing Policies

Routing policies describe the conditions under which calls will be routed to the SIP Entities specified in **Section 4.3**. Two routing policies must be added – one for Avaya Aura™ Communication Manager 5.2 and one for DiVitas MUC. To add a routing policy, select **Routing Policies** on the left and click on the **New** button on the right. The following screen is displayed. Fill in the following:

Under *General*:

Enter a descriptive name in **Name**.

Under *SIP Entity as Destination*:

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

Under *Time of Day*:

Click **Add**, and select the time range configured in the previous section.

Defaults can be used for the remaining fields. Click **Commit** to save each Routing Policy definition. The following screen shows the Routing Policy for Avaya Aura™ Communication Manager.

The screenshot displays the Avaya Integrated Management System Manager 1.0 interface. The top navigation bar includes the Avaya logo, the title 'INTEGRATED MANAGEMENT SYSTEM MANAGER 1.0', and a welcome message for 'admin' last logged in on Jun. 23, 2009 at 14:27 PM. A breadcrumb trail shows the path: Home / Network Routing Policy / Routing Policies / Routing Policy Details. The left sidebar contains a menu with categories: Asset Management, User Management, Monitoring, Network Routing Policy (selected), Security, Applications, Settings, and Session Manager. Under Network Routing Policy, sub-items include Adaptations, Dial Patterns, Entity Links, Locations, Regular Expressions, Routing Policies (selected), SIP Domains, SIP Entities, Time Ranges, and Personal Settings. The main content area is titled 'Routing Policy Details' and includes 'Commit' and 'Cancel' buttons. It is divided into four sections: 1. General: A table with columns 'Name', 'Disabled', and 'Notes'. The first row shows 'To devcon31' with the 'Disabled' checkbox unchecked. 2. SIP Entity as Destination: A 'Select' button and a table with columns 'Name', 'FQDN or IP Address', 'Type', and 'Notes'. The first row shows 'devcon31' with FQDN '192.45.100.70' and Type 'CM'. 3. Time of Day: 'Add', 'Remove', and 'View Gaps/Overlaps' buttons. A table with 1 item shows a time range from 00:00 to 23:59, labeled 'Anytime'. 4. Dial Patterns: 'Add' and 'Remove' buttons. A table with 0 items is shown. 5. Regular Expressions: 'Add' and 'Remove' buttons.

Figure 30: Routing Policy for Calls from DiVitas Clients to Communication Manager

The following screen shows the Routing Policy for the DiVitas Mobile UC Server.

INTEGRATED MANAGEMENT SYSTEM MANAGER 1.0

Welcome, **admin** Last Logged on at Jun. 23, 2009 14:27 PM
[Help](#) | [Log off](#)

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

Asset 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

Routing Policy Details field descriptions

SIP Entity List field descriptions

Time Range List field descriptions

Pattern List field descriptions

Regular Expressions List field descriptions

Saving Committing Synchronizing configuration changes

Commit

Cancel

Routing Policy Details

General

Name	Disabled	Notes
To DiVitas	<input type="checkbox"/>	

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
DiVitas MUC Server	192.45.100.195	Other	

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	Anytime	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	00:00	23:59	

Select: All, None (0 of 1 Selected)

Dial Patterns

Add

Remove

0 Items

Refresh

Filter: Enable

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

Regular Expressions

Add

Remove

Figure 31: Routing Policy for Calls from Communication Manager to a DiVitas Client

5.8. Add Dial Patterns

Dial patterns must be defined that will direct calls to the appropriate SIP Entity. In the sample configuration, 5-digit extensions beginning with “2” reside on Communication Manager and 12-digit numbers beginning with ‘9’, which corresponds to the ARS feature access code, were used to route calls to the PSTN through Communication Manager.. To add a dial pattern, select **Dial Patterns** on the left and click on the **New** button on the right. Fill in the following, as shown in the screen below, which corresponds to the dial pattern for routing calls to Avaya Aura™ Communication Manager:

Under *General*:

- **Pattern:** Dialed number or prefix.
- **Min** Minimum length of dialed number.
- **Max** Maximum length of dialed number.
- **Notes** Comment on purpose of dial pattern.

Under *Originating Locations and Routing Policies*:

Click **Add**, and then select the appropriate location and routing policy from the list.

Default values can be used for the remaining fields. Click **Commit** to save this dial pattern. The following screens show the dial pattern definitions for Avaya Aura™ Communication Manager and DiVitas Mobile UC Server.

AVAYA INTEGRATED MANAGEMENT SYSTEM MANAGER 1.0 Welcome, **admin** Last Logged on at Jun. 23, 2009 14:27 PM Help | Log off

Home / Network Routing Policy / Dial Patterns / Dial Pattern Details

Dial Pattern Details [Commit] [Cancel]

General

Pattern	Min	Max	Emergency Call	SIP Domain	Notes
2	5	5	<input type="checkbox"/>	avaya.com	

Originating Locations and Routing Policies

[Add] [Remove]

1 Item | Refresh Filter: Enable

<input type="checkbox"/>	Originating Location Name	Originating Location Notes	Routing Policy Name	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	-ALL-	Any Locations	To DiVitas	<input type="checkbox"/>	DiVitas MUC Server	

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]

Figure 32: Dial Pattern for Local Extension Calls

AVAYA

INTEGRATED MANAGEMENT SYSTEM MANAGER 1.0

Welcome, **admin** Last Logged on at Jun. 23, 2009 14:27 PM
[Help](#) | [Log off](#)

Home / Network Routing Policy / Dial Patterns / Dial Pattern Details

Asset 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

Dial Pattern Details field descriptions

Location and Routing Policy List field descriptions

Denied Location field descriptions

Saving Committing Synchronizing configuration changes

Dial Pattern Details

Commit

Cancel

General

Pattern	Min	Max	Emergency Call	SIP Domain	Notes
* 91	* 12	* 12	<input type="checkbox"/>	avaya.com	To PSTN

Originating Locations and Routing Policies

AddRemove

1 Item RefreshFilter: Enable

<input type="checkbox"/>	Originating Location Name	Originating Location Notes	Routing Policy Name	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	-ALL-	Any Locations	To devcon31	<input type="checkbox"/>	devcon31	

Select: All, None (0 of 1 Selected)

Denied Originating Locations

AddRemove

0 Items RefreshFilter: Enable

<input type="checkbox"/>	Originating Location	Notes
--------------------------	----------------------	-------

* Input Required

Commit

Cancel

Figure 33: Dial Pattern for PSTN Calls

5.9. Add Session Manager

To complete the configuration, adding the Session Manager will provide the linkage between Avaya Aura™ System Manager and Avaya Aura™ Session Manager. Expand the **Session Manager** menu on the left and select **Session Manager Administration**. Then click **Add**, and fill in the fields as described below and shown in the following screen:

Under *Identity*:

- **SIP Entity Name:** Select the name of the SIP Entity added for Avaya Aura™ Session Manager
- **Description:** Descriptive comment (optional)
- **Management Access Point Host Name/IP:** Enter the IP address of the Avaya Aura™ Session Manager management interface.

Under *Security Module*:

- **Network Mask:** Enter the network mask corresponding to the IP address of Avaya Aura™ Session Manager
- **Default Gateway:** Enter the IP address of the default gateway for Avaya Aura™ Session Manager

Use default values for the remaining fields. Click **Save** to add this Session Manager.

The screenshot displays the Avaya Integrated Management System Manager 1.0 web interface. The top header includes the Avaya logo, the system name, and a user status bar showing 'Welcome, admin' and 'Last Logged on at Jun. 19, 2009 09:38 AM'. A navigation menu on the left lists various system management functions, with 'Session Manager' expanded to show 'Session Manager Administration'. The main content area is titled 'Edit Session Manager' and contains three tabs: 'General', 'Security Module', and 'Monitoring'. The 'General' tab is active, showing fields for 'SIP Entity Name' (SM2), 'Description' (ASM2), and 'Management Access Point Host Name/IP' (10.1.2.181). The 'Security Module' tab is also visible, showing fields for 'SIP Entity IP Address' (10.1.2.180), 'Network Mask' (255.255.255.0), 'Default Gateway' (10.1.2.1), 'Call Control PHB' (46), 'VLAN ID', and 'QOS Priority' (6). The 'Monitoring' tab is partially visible at the bottom, showing 'Enable Monitoring' (checked), 'Proactive cycle time (secs)' (900), and 'Reactive cycle time (secs)' (120). Buttons for 'Cancel' and 'Save' are located at the top right of the configuration area.

Figure 34: Session Manager Administration

6. Configure DiVitas Mobile Unified Communications

This section describes the steps for configuring the DiVitas Mobile Unified Communications Server (Mobile UC Server) which supports a variety of dual mode (WiFi/Cellular) telephones including Nokia E- and N-Series DiVitas Clients. Refer to [5] for additional configuration information.

All DiVitas Mobile UC Server configuration and management features are accessed from a Web-based interface. From an Internet browser, enter the IP address of the DiVitas Mobile UC Server in the URL field and log in using the appropriate credentials. The screen shown in **Figure 35** is displayed.

The screenshot displays the DiVitas Mobile UC Server Web Interface. At the top, there is a navigation bar with tabs for Server, Clients, Voice, Monitoring, Reporting, and Tools. The 'Server' tab is active, showing sub-tabs for Status, Network Status, IP Config, Admin Users, Images, Licensing, Time, Voice Config, Backup/Restore, and Email. The 'Status' sub-tab is selected. Below the navigation bar, a message indicates the user is logged in as 'admin' from IP '192.45.60.62' at '9:20 am EDT'. A 'Logout' link is visible in the top right corner. The main content area is divided into three sections: 'Server Information', 'Active Server Image', and 'License Information'. Each section contains a table of system details.

Server Information	
Serial Number	D27LCC1
Kernel Version	2.6.25.10-47.DV3.fc8
Kernel Build Date	#1 SMP Tue Jul 22 13:59:41 EDT 2008
System Memory	1034596 kB
System Uptime	0 days, 23:38
DVOS Uptime	0 days, 0:09
DVOS Status	System Normal
CPU Usage	1%

Active Server Image	
Platform	U1000
Version	2.7.2.0
Build	39
Build Timestamp	May 27 2009, 12:25:28

License Information	
Customer Name	Avaya Test lab
Customer ID	AVA001
Expiration	Tue Mar 16 19:59:59 2010

At the bottom of the interface, the DVOS Version is 2.7.2.0.39, and the copyright notice reads: © 2009 DiVitas Networks. All Rights Reserved.

Figure 35: DiVitas Mobile UC Server Web Interface

In the **Server→IP Config** webpage, configure the IP network parameters of the DiVitas Mobile UC Server corresponding to the customer's network as shown in **Figure 36**. The remaining fields on this webpage (not shown) may be left at the default values. Click **Submit**.

The screenshot displays the DiVitas Networks management interface. At the top, the DiVitas Networks logo is on the left, and a navigation bar contains tabs for 'Server', 'Clients', 'Voice', 'Monitoring', 'Reporting', and 'Tools'. The 'Server' tab is active, showing a sub-menu with 'Status', 'Network Status', 'IP Config' (highlighted), 'Admin Users', 'Images', 'Licensing', 'Time', 'Voice Config', 'Backup/Restore', and 'Email'. A 'Logout' link is also present. Below the navigation bar, a status bar indicates the user is logged in as 'admin' from '192.45.60.62' at '9:20 am EDT' and provides a 'Click link for documentation.' link. The main content area is titled 'Server Network Configuration' and features a 'Host Configuration' section. This section contains six input fields: 'IP Address' (192.45.100.195), 'Subnet Mask' (255.255.255.0), 'IP Gateway' (192.45.100.1), 'Internal Hostname' (localhost), 'Primary DNS Server Address' (0.0.0.0), and 'Secondary DNS Server Address' (0.0.0.0). At the bottom of this section are 'Submit' and 'Clear' buttons.

Figure 36: Server IP Configuration

The DiVitas Server and Avaya Aura™ Session Manager communicate over a SIP trunk. All calls from a DiVitas Client are routed over this SIP trunk to Avaya Aura™ Communication Manager. The SIP trunk is also used to route calls to DiVitas Clients operating in Cellular mode. To configure the SIP trunk on the DiVitas Server, navigate to **Voice→Configuration** and then click on **Trunks→Add Trunk**. The following example shows the SIP trunk after it has been configured.

In the SIP trunk configuration, specify a descriptive name for the **Trunk Name** field. For the **Dial Rules**, specify the format of the dial patterns that are allowed to be routed over this SIP trunk. In this example, the DiVitas Clients are allowed to dial 10 and 11-digit numbers preceded by a '9'. The '9' corresponds to the ARS feature access code on Communication Manager.

Figure 37 shows the first half of the SIP trunk configuration.

The screenshot displays the DiVitas Networks web interface for configuring a SIP trunk. The top navigation bar includes tabs for Server, Clients, Voice, Monitoring, Reporting, and Tools. The 'Voice' tab is active, and the 'Configuration' sub-tab is selected. A sidebar on the left lists various configuration options, with 'Trunks' highlighted. The main content area is titled 'Edit SIP Trunk' and shows the configuration for a trunk named 'To_SM'. The 'General Settings' section includes fields for 'Trunk Name' (To_SM), 'Outbound Caller ID', and 'Maximum channels'. The 'Outgoing Dial Rules' section includes fields for 'Outbound Dial Prefix', 'Dial rules wizards' (a dropdown menu), and 'Dial Rules' (a text area containing two rules: '9+1NXXNXXXXXX' and '9+NXXNXXXXXX'). A 'Clean & Remove duplicates' button is located at the bottom of the 'Dial Rules' section. A 'Logout' link is visible in the top right corner.

Figure 37: SIP Trunk - Top

Figure 38 displays the second half of the SIP trunk configuration webpage. The **Host Address** field should be set to the SIP domain, the **Port** field should be set to *5060* since UDP transport is used for the SIP trunk, and *rfc2833* should be used for the **DTMF Mode**. The other fields should be configured as shown below. Click **Submit Changes**.

Note: The SIP domain (Avaya.com) needs to be resolved to the IP address of Session Manager. If DNS is not available, an entry should be added to the *Hosts* file in the DiVitas Mobile UC Server. For the compliance testing, an entry was added to the *Hosts* file.

The screenshot shows the DiVitas Networks web interface for SIP Trunk configuration. The top navigation bar includes tabs for Server, Clients, Voice (selected), Monitoring, Reporting, and Tools. Below this is a sub-navigation bar with Configuration (selected), Conferencing, Voicemail, and Ring Groups. The main content area is titled 'PEER Details' and contains the following fields and options:

- Connection Type:** Radio buttons for 'Advanced' (selected) and 'Basic', with a 'Change View' button.
- Host Address:** Text input field containing 'avaya.com'.
- Port:** Text input field containing '5060'.
- User Name:** Empty text input field.
- Secret:** Empty text input field.
- Type:** Dropdown menu set to 'peer'.
- Context:** Dropdown menu set to 'shared-pbx-extensions'.
- NAT:** Radio buttons for 'yes' and 'no' (selected).
- Insecure:** Dropdown menu set to 'port and invite'.
- DTMF Mode:** Dropdown menu set to 'rfc2833'.
- Reinvite:** Radio buttons for 'yes' and 'no' (selected).

Below these fields is a text area containing the following configuration parameters:

```
canreinvite=no
context=shared-pbx-extensions
dtmfmode=rfc2833
fromdomain=avaya.com
host=avaya.com
insecure=port,invite
nat=no
port=5060
secret=
type=peer
username=
```

Below the text area are sections for 'Incoming Settings' and 'Registration':

- Incoming Settings:** Includes a 'USER Context' dropdown and a 'USER Details' text input field.
- Registration:** Includes a 'Register String' text input field.

At the bottom right of the form is a 'Submit Changes' button.

Figure 38: SIP Trunk – Bottom

A route was defined for routing calls to the PSTN by navigating to **Voice→Configuration** and then clicking on **Outbound Routing→Add Route**. The **Route Name** was set to a descriptive name. The **Dial Patterns** field specified the dial string format of calls routed over the SIP trunk. The **Trunk Sequence** specifies the trunk(s) for routing outbound calls to the PSTN. In this example, the calls are routed over the SIP trunk configured in **Figure 37** and **Figure 38**.

The screenshot shows the 'Edit Route' configuration page in the Divitas Networks web interface. The page is titled 'Edit Route' and has a sub-header 'Delete Route outbound_dialing'. The main configuration area includes fields for 'Route Name' (set to 'outbound_dialing'), 'Route Password', 'Intra Company Route' (checkbox), 'Use P-Asserted-Identity Headers' (checkbox), and 'Select Privacy Headers' (checkboxes for Header, ID, Session, User, Critical). The 'Dial Patterns' field contains a list of patterns: 1NXXXXXXXX, 91NXXXXXXXX, 9NXXXXXXXX, NXXXXXXXX, and NXXXXXX. Below this is a 'Clean & Remove duplicates' button and a 'Pick pre-defined patterns' dropdown. The 'Trunk Sequence' section shows a list with one entry: '0 SIP/To_SM'. At the bottom right is a 'Submit Changes' button.

Server	Clients	Voice	Monitoring	Reporting	Tools	Logout
Configuration	Conferencing	Voicemail	Ring Groups			

Incoming Calls
Extensions
Digital Receptionist
Trunks
Trunk Profile
Show Registry
Inbound Routing
Outbound Routing
System Recordings
General Settings

Edit Route

[Delete Route outbound_dialing](#)

Route Name: outbound_dialing [Rename](#)

Route Password:

Intra Company Route: ☐

Use P-Asserted-Identity Headers: ☐

Select Privacy Headers: ☐ Header ☐ ID ☐ Session ☐ User ☐ Critical

Dial Patterns

1NXXXXXXXX
91NXXXXXXXX
9NXXXXXXXX
NXXXXXXXX
NXXXXXX

[Clean & Remove duplicates](#)

Insert: [Pick pre-defined patterns](#)

Trunk Sequence

0	SIP/To_SM	
	<input type="text"/>	<input type="button" value="Add"/>

[Submit Changes](#)

[Add Route](#)
0 outbound_dialing
1 internal_station_dialing

Figure 39: Outbound Routing for PSTN Calls

Another route was defined for routing calls to stations on Communication Manager. The **Route Name** was set to a descriptive name. The **Dial Patterns** field specified the format of local extensions. In this example, local extensions were 5-digits starting with '2'. The **Trunk Sequence** specifies the trunk(s) for routing outbound calls to Communication Manager. In this example, the calls are routed over the SIP trunk configured in **Figure 37** and **Figure 38**.

Divitas Networks

Server Clients **Voice** Monitoring Reporting Tools [Logout](#)

Configuration Conferencing Voicemail Ring Groups

Edit Route

[Delete Route internal_station_dialing](#)

Route Name: internal_station_dialing [Rename](#)

Route Password:

Intra Company Route: ☒

Use P-Asserted-Identity Headers: ☐

Select Privacy Headers: ☐ Header ☐ ID ☐ Session ☐ User ☐ Critical


Dial Patterns

2XXXXX

[Clean & Remove duplicates](#)

Insert: [Pick pre-defined patterns](#) ▼

Trunk Sequence

0 SIP/To_SM 


[Add](#)

[Submit Changes](#)

Left Sidebar:

- Incoming Calls
- Extensions
- Digital Receptionist
- Trunks
- Trunk Profile
- Show Registry
- Inbound Routing
- Outbound Routing**
- System Recordings
- General Settings

Right Sidebar:

- Add Route
- 0 outbound_dialing ▼
- 1 internal_station_dialing 

In the **Server → Voice Config** webpage, configure the CVC. In the **Server CVC Configuration** section, set the **CVC Operational Mode** field to *Allowed* and configure the external and internal CVC numbers. Enable **Share PBX Extensions** to allow the desktop phone and DiVitas clients to have the same extension. Click **Submit**.

Server Clients Voice Monitoring Reporting Tools [Logout](#)
 Status Network Status IP Config Admin Users Images Licensing Time **Voice Config** Backup/Restore Email

Logged in as: admin from 192.45.60.62 at 9:20 am EDT [Click link for documentation.](#)

➔ **Server CVC Configuration**

Server CVC Configuration

CVC Operational Mode ☒ Allowed ☐ Disabled
 External CVC Number
 Internal CVC Number
You must configure both Internal and External CVC numbers to use CVC calling.
 The Internal CVC number must not conflict with configured extensions, scheduled conferences, or ring groups.

➔ **Server Caller ID Configuration**

Server Caller ID Configuration

Caller ID 1
 Caller ID 2
 Caller ID 3
 Caller ID 4
 Caller ID 5
 Caller ID 6
 Caller ID 7
 Caller ID 8
 Caller ID 9
 Caller ID 10

➔ **Server Call Configuration**

Server Call Configuration

Process calls with unknown callerid as server calls ☒ Enable ☐ Disable
 Process calls with private callerid as server calls ☐ Enable ☒ Disable

➔ **Share PBX Extension Configuration**

Share PBX Extension Configuration

Share PBX Extensions ☒ Enable ☐ Disable
Configure outbound routes properly before enabling this feature.

Figure 40: Server CVC Configuration

To view and add users to the DiVitas Server, navigate to **Clients→Users**. To add a **User**, click on the **Add** button under **Add User Account**. To view the details of a configured user account, select **Modify** in the **Action** field and click **Submit** under the **User Accounts** section.

Logged in as: admin from 192.45.60.62 at 9:20 am EDT [Click link for documentation.](#)

➔ Add User Account

Add User Account

➔ Delete User Accounts

Delete User Accounts

➔ User Accounts

Name	Action	Full Name	Group	Extension	Devices	Active Calls	Status
24511	None <input type="button" value="Submit"/>	David Wells	default	24511	357663010613226	0	Active
24513	None <input type="button" value="Submit"/>	John Smith	default	24513	357676011245400	0	Active

Figure 41: User Accounts

When adding a **User**, specify the user's **Full Name** and **Extension** as shown in **Figure 42**. The figure below shows the user account after it has been configured. The **Add User Account** webpage will appear slightly different, but contain similar fields.

DIVITAS NETWORKS

Server **Clients** Voice Monitoring Reporting Tools [Logout](#)

Users User Groups User Config Devices Device Groups Device Config Bulk Load

Logged in as: admin from 192.45.60.62 at 9:20 am EDT [Click link for documentation.](#)

Modify User Account

Account

Extension

Divitas Client User Password

SIP Device User Password

If SIP device user password is left blank, it will be defaulted to the Divitas Client password.

Full Name

Outbound CID

Email

SMS Email Address

Paired Deskphone ☐ Internal ☒ External

Group Name

Voicemail

Mailbox

The following fields are only used when voicemail is enabled.

Mailbox Password

Play Caller ID ☐ Yes ☒ No

Play Envelope(Date/Time) ☐ Yes ☒ No

Access Number

Redirect Number

The redirect number is only used when voicemail redirect is selected.

IMAP Configuration

Enable IMAP ☐ Yes ☒ No

IMAP Username

IMAP User Password

Figure 42: User

7. General Test Approach and Test Results

The focus of the interoperability compliance testing was to verify call establishment between the DiVitas Clients in WiFi and Cellular modes, the PSTN, and local stations on Communication Manager and Session Manager. The DiVitas Clients were paired with an H.323 IP station on Communication Manager. In addition, basic telephony features were exercised.

The serviceability testing focused on verifying the ability of the DiVitas Server to recover from adverse conditions, such as power failures and disconnecting cables to the IP network. In addition, the ability of the solution to recover from Avaya S8730 Server interchange and from cycling power on Session Manager was also verified.

All tests passed successfully.

8. Verification Steps

This section provides the verification steps that may be performed to verify that DiVitas Clients registered with the DiVitas Mobile UC server can establish calls to the PSTN or stations on Communication Manager.

1. From the Communication Manager SAT, verify that the SIP signaling group and trunk group are in-service using the **status signaling-group** and **status trunk** commands, respectively.
2. From the DiVitas web interface, navigate to the **Clients→Devices** webpage and verify that the DiVitas Clients are registered with the DiVitas Mobile UC Server and that their status is active.

Logged in as: admin from 192.45.60.62 at 9:20 am EDT [Click link for documentation.](#)

➔ Add Client Device

Add Client Device

➔ Delete Client Devices

Delete Client Devices

➔ Client Devices

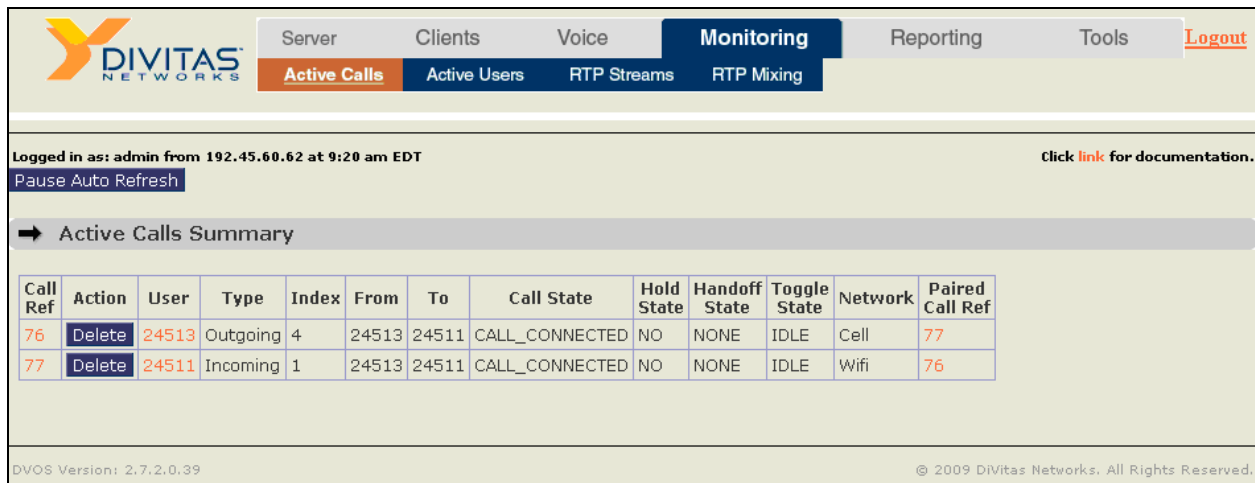
Serial Number/ Name	Action	Group	Image	IP:Port	User	Active Calls	Status
357663010613226	None <input type="button" value="Submit"/>	default	2.7.2.0.37	192.45.100.191:5064	24511	0	Active
357676011245400	None <input type="button" value="Submit"/>	default	2.7.2.0.37	192.45.100.228:5064	24513	0	Active

➔ Other SIP Devices

Name	IP:Port	User	Active Calls	Status
------	---------	------	-----------------	--------

Figure 43: Status of Client Devices

- Place a call between two DiVitas Clients routed through Communication Manager. Verify that the call completes successfully. From the DiVitas Web interface, navigate to **Monitoring→Active Calls** to view the call summary as shown in **Figure 44**.



The screenshot shows the DiVitas Networks web interface. The top navigation bar includes 'Server', 'Clients', 'Voice', 'Monitoring' (selected), 'Reporting', and 'Tools'. Under 'Monitoring', there are sub-tabs: 'Active Calls' (selected), 'Active Users', 'RTP Streams', and 'RTP Mixing'. The user is logged in as 'admin' from '192.45.60.62' at '9:20 am EDT'. A 'Pause Auto Refresh' button is visible. The main section is titled 'Active Calls Summary' and contains a table with the following data:

Call Ref	Action	User	Type	Index	From	To	Call State	Hold State	Handoff State	Toggle State	Network	Paired Call Ref
76	Delete	24513	Outgoing	4	24513	24511	CALL_CONNECTED	NO	NONE	IDLE	Cell	77
77	Delete	24511	Incoming	1	24513	24511	CALL_CONNECTED	NO	NONE	IDLE	Wifi	76

At the bottom, it shows 'DVOS Version: 2.7.2.0.39' and '© 2009 DiVitas Networks. All Rights Reserved.'

Figure 44: Call Summary – Call between Two DiVitas Clients

- While a call is active on a Nokia E51 with the DiVitas Client, the connected number is shown on the phone's display as shown in **Figure 45** and **Figure 46**.

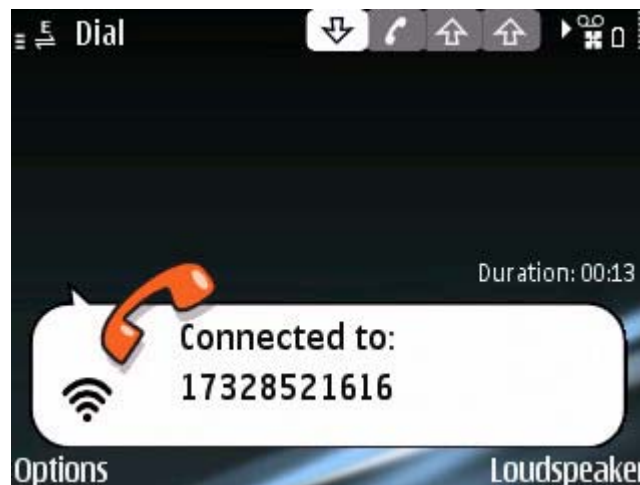


Figure 45: Active Call to DiVitas Client in WiFi Mode

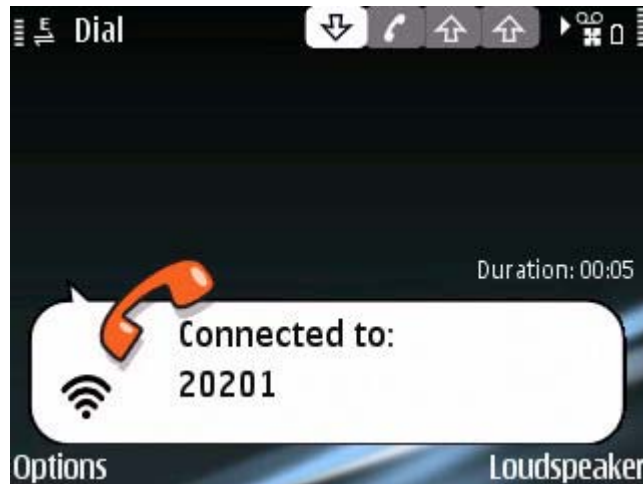


Figure 46: Active Call to an Avaya H.323 IP Telephone

After the call is completed, calls are maintained in the phone's call log as shown in **Figure 47**.



Figure 47: Call Log

9. Conclusion

These Application Notes describe the configuration steps required to integrate the DiVitas Mobile Unified Communications solution with Avaya AuraTM Communication Manager and Avaya AuraTM Session Manager. The DiVitas Clients were able to register with the DiVitas Server and originate and terminate calls to/from the PSTN and stations on Communication Manager.

10. Additional References

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

- [1] *Administrator Guide for Avaya AuraTM Communication Manager*, Document 03-300509, Issue 5, May 2009, available at <http://support.avaya.com>.
- [2] *Avaya AuraTM Communication Manager Feature Description and Implementation*, Document 555-245-205, Issue 7, May 2009, available at <http://support.avaya.com>.
- [3] *SIP Support in Avaya AuraTM Communication Manager Running on Avaya S8xxx Servers*, Issue 9, May 2009, Document Number 555-245-206, available at <http://support.avaya.com>.
- [4] *Application Notes for DiVitas Mobile Unified Communications with Avaya Modular Messaging*, Issue 1.0, available at <http://support.avaya.com>.
- [5] *DiVitas Server Administration Guide*, Version 2.7, Part Number: DOC-DVOS-AG-206.

©2009 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.