



Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Avaya Aura® Communication Manager R6.2 as an Evolution Server, Avaya Aura® Session Manager R6.3 and Avaya Aura® Session Border Controller to support Udata SIP Trunking service - Issue 1.0

Abstract

These Application Notes describe the steps used to configure Session Initiation Protocol (SIP) trunking between Udata SIP Trunking service and an Avaya SIP enabled Enterprise Solution. The Avaya solution consists of Avaya Aura® Session Border Controller, Avaya Aura® Session Manager and Avaya Aura® Communication Manager as an Evolution Server. Udata is a member of the DevConnect Service Provider program.

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 steps used to configure Session Initiation Protocol (SIP) trunking between Udata SIP Trunking service and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Aura® Session Border Controller (SBC), Avaya Aura® Session Manager and Avaya Aura® Communication Manager Evolution Server. Customers using this Avaya SIP-enabled enterprise solution with the Udata SIP Trunking service are able to place and receive PSTN calls via a dedicated Internet connection and the SIP protocol. This converged network solution is an alternative to traditional PSTN trunks. This approach generally results in lower cost for the enterprise customer.

2. General Test Approach and Test Results

The general test approach was to configure a simulated enterprise site using an Avaya SIP telephony solution consisting of Communication Manager, Session Manager and SBC. The enterprise site was configured to use the SIP Trunking service provided by Udata.

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

2.1. Interoperability Compliance Testing

The interoperability test included the following:

- Incoming calls to the enterprise site from mobile phones using the SIP Trunk provided by Udata, calls made to SIP and H.323 telephones at the enterprise
- Outgoing fixed and mobile calls from the enterprise site completed via Udata to PSTN and mobile destinations, calls made from SIP and H.323 telephones
- Calls using the G.711A, G.711MU and G.729 codecs
- Fax calls to/from a group 3 fax machine to a PSTN connected fax machine using T.38
- DTMF transmission using RFC 2833 with successful Voice Mail/Vector navigation for inbound and outbound calls
- User features such as hold and resume, transfer, conference, call forwarding, etc
- Caller ID Presentation and Caller ID Restriction
- Direct IP-to-IP media with SIP and H.323 telephones
- No initial direct IP to IP media so that media is established to the G430 Media Gateway initially then converted to a direct connection after call set-up (shuffling)
- Call coverage and call forwarding for endpoints at the enterprise site
- Transmission and response of SIP OPTIONS messages sent by Udata requiring Avaya response and sent by Avaya requiring Udata response

2.2. Test Results

Interoperability testing of the sample configuration was completed with successful results for the Udata SIP Trunking service with the following observations:

- Shuffling was delayed on outgoing calls from the 9620 SIP phone and media was routed via the Media Gateway – this was end-point specific as shuffling worked effectively from the Flare and SIP soft client
- Although codec G.729 is supported, it was observed during test that annex B is not supported
- When making incoming calls with no matching codec available, CM sends a 488 “Not Acceptable Here”. The network responds to this with several re-attempts resulting in a delay before a tone is heard by the caller.
- When testing DTMF voicemail menu navigation from the Flare, an upgrade was required to the latest Flare firmware for navigation to work effectively.
- Incoming Toll-Free access was not available for test
- No test call was booked with Emergency Services Operator
- When incoming faxes are received, the network attempts to change back to the original codec once the fax is completed. The re-INVITE is rejected by CM with a 488 “Not Acceptable Here”. During test the fax machine indicated an intermittent failure even though the faxes were sent successfully.
- When all trunks are busy and the Communication Manager sends 500 “Service Unavailable”, the network re-attempts the call and there is a delay before the caller hears the call failure treatment.
- When the signalling is unavailable and the Session Manager sends 500 “Server Link Monitor Status Down”, the network re-attempts the call and there is a delay before the caller hears the call failure treatment.

2.3. Support

For technical support on Udata products please visit the website at www.udata.net or contact an authorized Udata representative.

3. Reference Configuration

Figure 1 illustrates the test configuration. The test configuration shows an Enterprise site connected to the Udata SIP Trunking service. Located at the Enterprise site is an Avaya Aura® Session Border Controller, Session Manager and Communication Manager. Endpoints are Avaya 96x0 series and Avaya 96x1 series IP telephones (with SIP and H.323 firmware), Avaya 46xx series IP telephones (with H.323 firmware), Avaya 16xx series IP telephones (with H.323 firmware), Avaya A175 Desktop Video Device running Flare Experience (audio only), Avaya analogue telephones and an analogue fax machine. Also included in the test configuration was an Avaya one-X® Communicator soft phone running on a laptop PC configured for SIP.

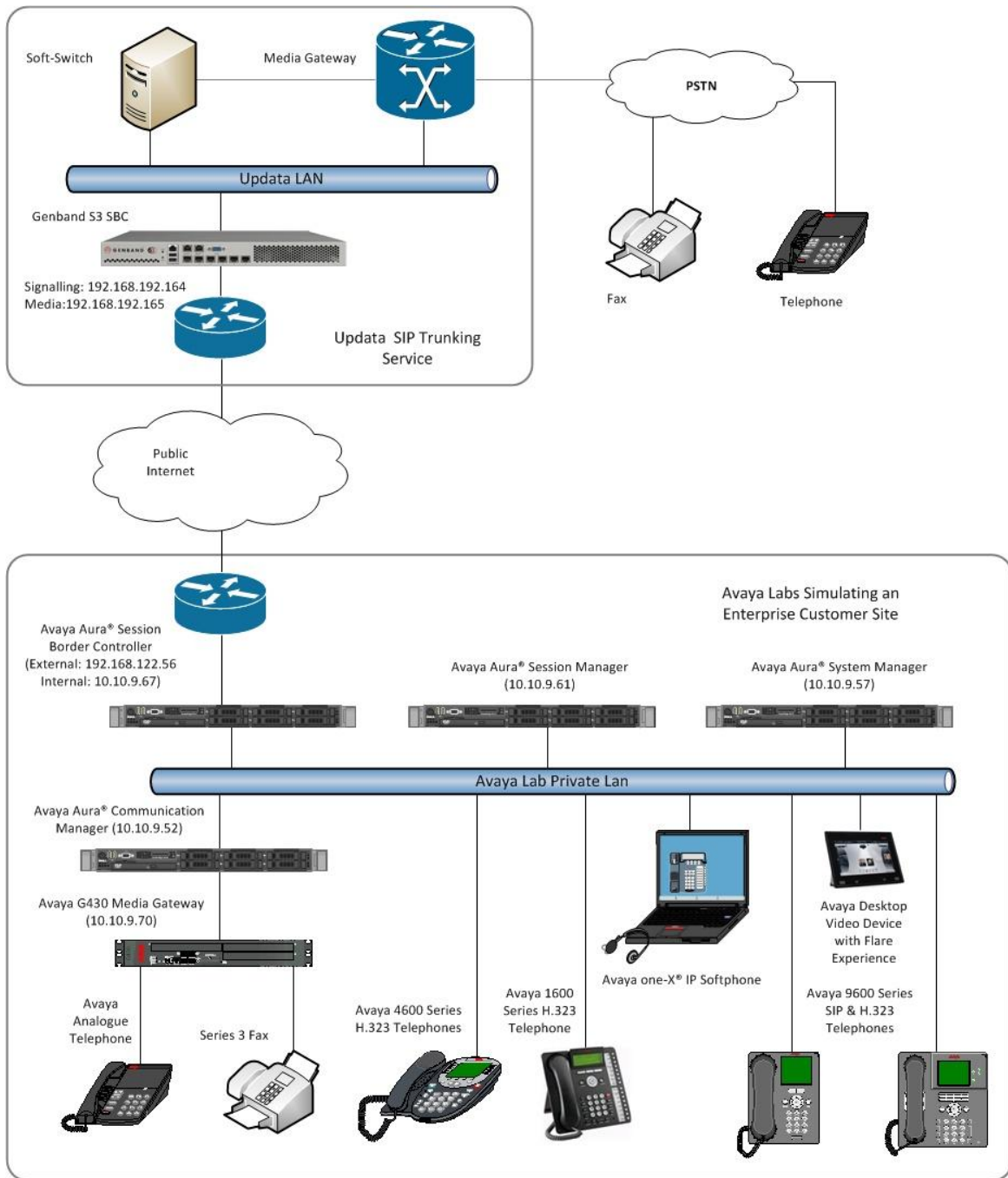


Figure 1: Test Setup Updata SIP Trunking to Avaya Enterprise

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya	
Avaya S8800 Server running Session Manager	R6.3 - 6.3.0.0.630039
Avaya S8800 Server running System Manager	R6.3 - Build No. - 6.3.0.8.5682-6.3.8.818 Software Update Revision No: 6.3.0.8.923
Avaya S8800 Server running Communication Manager	R016x.02.0.823.0 Patch 20396 (SP5)
Avaya S8800 Server running Session Border Controller	Version E3.6.2.M1P2 – Build No. 50293
Avaya 1616 Phone (H.323)	1.301
Avaya 4621 Phone (H.323)	2.902
Avaya 9630 Phone (H.323)	3.103
Avaya A175 Desktop Video Device (SIP)	Flare Experience Release 1.1.2
Avaya 9620 Phone (SIP)	R2.6 SP9
Avaya one-X® Communicator (H.323) on Lenovo T510 Laptop PC	6.1.7.04-SP7-39506
Analogue Handset	NA
Analogue Fax	NA
Udata	
Genband S3 THN (Annapolis)	7.1
Genband S3 LD5 (Annapolis)	7.1

5. Configure Avaya Aura® Communication Manager

This section describes the steps for configuring Communication Manager for SIP Trunking. SIP trunks are established between Communication Manager and Session Manager. These SIP trunks will carry SIP signalling associated with the Udata SIP Trunking service. For incoming calls, the Session Manager receives SIP messages from the Avaya Aura® Session Border Controller (SBC) and directs the incoming SIP messages to Communication Manager. Once the message arrives at Communication Manager, further incoming call treatment, such as incoming digit translations and class of service restrictions may be performed. All outgoing calls to the PSTN are processed within Communication Manager and may be first subject to outbound features such as automatic route selection, digit manipulation and class of service restrictions. Once Communication Manager selects a SIP trunk, the SIP signalling is routed to the Session Manager. The Session Manager directs the outbound SIP messages to the SBC at the enterprise site that then sends the SIP messages to the Udata network. Communication Manager Configuration was performed using the System Access Terminal (SAT). Some screens in this section have been abridged and highlighted for brevity and clarity in presentation. The general

installation of the Avaya S8800 Servers and Avaya G430 Media Gateway is presumed to have been previously completed and is not discussed here.

5.1. Confirm System Features

The license file installed on the system controls the maximum values for these attributes. If a required feature is not enabled or there is insufficient capacity, contact an authorized Avaya sales representative to add additional capacity. Use the **display system-parameters customer-options** command and on **Page 2**, verify that the **Maximum Administered SIP Trunks** supported by the system is sufficient for the combination of trunks to the Updata network, and any other SIP trunks used.

display system-parameters customer-options		Page 2 of 11
OPTIONAL FEATURES		
IP PORT CAPACITIES	USED	
Maximum Administered H.323 Trunks:	12000	0
Maximum Concurrently Registered IP Stations:	18000	3
Maximum Administered Remote Office Trunks:	12000	0
Maximum Concurrently Registered Remote Office Stations:	18000	0
Maximum Concurrently Registered IP eCons:	414	0
Max Concur Registered Unauthenticated H.323 Stations:	100	0
Maximum Video Capable Stations:	18000	0
Maximum Video Capable IP Softphones:	18000	0
Maximum Administered SIP Trunks:	24000	20
Maximum Administered Ad-hoc Video Conferencing Ports:	24000	0
Maximum Number of DS1 Boards with Echo Cancellation:	522	0
Maximum TN2501 VAL Boards:	128	0
Maximum Media Gateway VAL Sources:	250	1
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:	300	0

On **Page 4**, verify that **IP Trunks** field is set to **y**.

display system-parameters customer-options		Page 4 of 11
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? n	
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	
Hospitality (Basic)? y	Multimedia Call Handling (Enhanced)? y	
Hospitality (G3V3 Enhancements)? y	Multimedia IP SIP Trunking? y	
IP Trunks? y		
IP Attendant Consoles? y		

5.2. Administer IP Node Names

The node names defined here will be used in other configuration screens to define a SIP signalling group between Communication Manager and Session Manager. In the **IP Node Names** form, assign the node **Name** and **IP Address** for the Session Manager. In this case, **SM100** and **10.10.9.61** are the **Name** and **IP Address** for the Session Manager SIP interface. Also note the **procr** name as this is the processor interface that Communication Manager will use as the SIP signalling interface to Session Manager.

display node-names ip		IP NODE NAMES
Name	IP Address	
SM100	10.10.9.61	
Sipera-SBC	10.10.9.71	
default	0.0.0.0	
procr	10.10.9.52	
procr6	::	

5.3. Administer IP Network Region

Use the **change ip-network-region 1** command to set the following values:

- 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** (both **Intra-** and **Inter-Region**) is enabled (**yes**) to allow audio traffic to be sent directly between endpoints without using gateway VoIP resources. When a PSTN call is shuffled, the media stream is established directly between the enterprise end-point and the internal media interface of the SBC.
- The **Codec Set** is set to the number of the IP codec set to be used for calls within the IP network region. In this case, codec set **1** is used.

```
change ip-network-region 1                                     Page 1 of 20
                                                                IP NETWORK REGION
Region: 1
Location: 1           Authoritative Domain: avaya.com
Name: default
MEDIA PARAMETERS
  Codec Set: 1
  Intra-region IP-IP Direct Audio: yes
  Inter-region IP-IP Direct Audio: yes
  UDP Port Min: 2048
  UDP Port Max: 3329
  IP Audio Hairpinning? n
DIFFSERV/TOS PARAMETERS
  Call Control PHB Value: 46
  Audio PHB Value: 46
  Video PHB Value: 26
802.1P/Q PARAMETERS
  Call Control 802.1p Priority: 6
  Audio 802.1p Priority: 6
  Video 802.1p Priority: 5
  AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS
  RSVP Enabled? n
  H.323 Link Bounce Recovery? y
  Idle Traffic Interval (sec): 20
  Keep-Alive Interval (sec): 5
  Keep-Alive Count: 5
```


5.4. Administer IP Codec Set

Open the **IP Codec Set** form for the codec set specified in the IP Network Region form in **Section 5.3**. Enter the list of audio codec's eligible to be used in order of preference. For the interoperability test the codec's supported by Updata were configured, namely **G.711A**, **G.729** and **G.711MU**.

change ip-codec-set 1				Page 1 of 2
IP Codec Set				
Codec Set: 1				
Audio Codec	Silence Suppression	Frames Per Pkt	Packet Size (ms)	
1: G.711A	n	2	20	
2: G.729A	n	2	20	
3: G.711MU	n	2	20	

Note: G.729A is shown here. In fact, Updata supports G.729 and both annexes A and B were tested. While annex A was tested successfully, annex B was not fully supported.

The Updata SIP Trunking service supports T.38 for transmission of fax. Navigate to **Page 2** to configure T.38 by setting the **FAX - Mode** to **t.38-standard** as shown below

change ip-codec-set 1			Page 2 of 2
IP Codec Set			
Allow Direct-IP Multimedia? n			
FAX	Mode	Redundancy	
	t.38-standard	0	
Modem	off	0	
TDD/TTY	US	3	
Clear-channel	n	0	

5.5. Administer SIP Signaling Groups

This signalling group (and trunk group) will be used for inbound and outbound PSTN calls to the Udata SIP Trunking service. During test, this was configured to use **TCP** and port **5060** to facilitate tracing and fault analysis. It is recommended however, to use TLS (Transport Layer Security) and the default TLS port of **5061** for security. Configure the **Signaling Group** using the **add signaling-group x** command as follows:

- Set **Group Type** to **sip**
- Set **Transport Method** to **tcp**
- Set **Peer Detection Enabled** to **y** allowing the Communication Manager to automatically detect if the peer server is a Session Manager
- Set **Near-end Node Name** to the processor interface (node name **procr** as defined in the **IP Node Names** form shown in **Section 5.2**)
- Set **Far-end Node Name** to the Session Manager (node name **SM100** as defined in the **IP Node Names** form shown in **Section 5.2**)
- Set **Near-end Listen Port** and **Far-end Listen Port** to **5060** (Commonly used TCP port value)
- Set **Far-end Network Region** to the IP Network Region configured in **Section 5.3**. (logically establishes the far-end for calls using this signalling group as network region **1**)
- Leave **Far-end Domain** blank (allows the CM to accept calls from any SIP domain on the associated trunk)
- Set **Direct IP-IP Audio Connections** to **y**
- Leave **DTMF over IP** at default value of **rtp-payload** (Enables **RFC2833** for DTMF transmission from the Communication Manager)

The default values for the other fields may be used.

change signaling-group 1		Page 1 of 2
SIGNALING GROUP		
Group Number: 1	Group Type: sip	
IMS Enabled? n	Transport Method: tcp	
Q-SIP? n		
IP Video? n	Enforce SIPS URI for SRTP? n	
Peer Detection Enabled? y	Peer Server: SM	
Near-end Node Name: procr	Far-end Node Name: SM100	
Near-end Listen Port: 5060	Far-end Listen Port: 5060	
	Far-end Network Region: 1	
Far-end Domain:		
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? y	IP Audio Hairpinning? n	
H.323 Station Outgoing Direct Media? n	Initial IP-IP Direct Media? n	
	Alternate Route Timer(sec): 6	

5.6. Administer SIP Trunk Group

A trunk group is associated with the signaling group described in **Section 5.5**. Configure the trunk group using the **add trunk-group x** command, where **x** is an available trunk group. On **Page 1** of this form:

- Set the **Group Type** field to **sip**
- Choose a descriptive **Group Name**
- Specify a trunk access code (**TAC**) consistent with the dial plan
- The **Direction** is set to **two-way** to allow incoming and outgoing calls
- Set the **Service Type** field to **public-ntwrk**
- Specify the signalling group associated with this trunk group in the **Signaling Group** field as previously configured in **Section 5.5**
- Specify the **Number of Members** supported by this SIP trunk group

add trunk-group 1		Page 1 of 21	
TRUNK GROUP			
Group Number: 1	Group Type: sip	CDR Reports: y	
Group Name: Group 1	COR: 1	TN: 1	TAC: 101
Direction: two-way	Outgoing Display? y		
Dial Access? n	Night Service:		
Queue Length: 0			
Service Type: public-ntwrk	Auth Code? n		
		Member Assignment Method: auto	
		Signaling Group: 1	
		Number of Members: 10	

On **Page 2** of the trunk-group form, the Preferred **Minimum Session Refresh Interval (sec)** field should be set to a value mutually agreed with Updata to prevent unnecessary SIP messages during call setup.

Add trunk-group 1		Page 2 of 21	
Group Type: sip			
TRUNK PARAMETERS			
Unicode Name: auto			
Redirect On OPTIM Failure: 5000			
SCCAN? n		Digital Loss Group: 18	
Preferred Minimum Session Refresh Interval(sec): 300			
Disconnect Supervision - In? y Out? y			

On **Page 3**, set the **Numbering Format** field to **private**. This allows delivery of CLI with leading zeros.

add trunk-group 1		Page 3 of 21
TRUNK FEATURES		
ACA Assignment? n	Measured: none	Maintenance Tests? y
Numbering Format: private		
UUI Treatment: service-provider		
Replace Restricted Numbers? n		
Replace Unavailable Numbers? n		

Note: The **Numbering Format** setting of **private** is only effective with non-international numbering formats specified in the route pattern.

On **Page 4** of this form:

- Set **Support Request History** to **y**
- Set the **Telephone Event Payload Type** to **101** to match the value preferred by Updata (this Payload Type is not applied to calls from SIP end-points)
- Set **Always Use re-INVITE for Display Updates** to **y**
- Set the **Identity for Calling Party Display** to **From** to ensure that where CLI for incoming calls is withheld, it is not displayed on the Communication Manager extension

add trunk-group 1		Page 4 of 21
PROTOCOL VARIATIONS		
Mark Users as Phone? n		
Prepend '+' to Calling Number? n		
Send Transferring Party Information? n		
Network Call Redirection? n		
Send Diversion Header? n		
Support Request History? y		
Telephone Event Payload Type: 101		
Convert 180 to 183 for Early Media? n		
Always Use re-INVITE for Display Updates? y		
Identity for Calling Party Display: From		
Block Sending Calling Party Location in INVITE? n		
Enable Q-SIP? n		

5.7. Administer Calling Party Number Information

Use the **change private-unknown-numbering** command to configure Communication Manager to send the calling party number with leading zeros. As with the public numbering table, individual stations were mapped to send numbers allocated from the Udata DDI range supplied.

change public-unknown-numbering 0					Page 1 of 2
NUMBERING - PUBLIC/UNKNOWN FORMAT					
Ext Len	Ext Code	Trk Grp(s)	CPN Prefix	Total CPN Len	
4	2000	1	01737nnnnn3	11	Total Administered: 8
4	2291	1	01737nnnnn5	11	Total Administered: 9
4	2296	1	01737nnnnn6	11	Maximum Entries: 540
4	2316	1	01737nnnnn3	11	
4	2346	1	01737nnnnn5	11	
4	2396	1	01737nnnnn4	11	
4	2400	1	01737nnnnn4	11	
4	2401	1	01737nnnnn7	11	
4	2601	1	01737nnnnn7	11	

Note: The private numbering table is used when **private** is specified in the trunk settings described in **Section 5.6** and when a non-international number format is specified in the route pattern settings specified in **Section 5.8** for example **unk-unk**.

5.8. Administer Route Selection for Outbound Calls

In the test environment, the Automatic Route Selection (ARS) feature was used to route outbound calls via the SIP trunk to the Udata SIP Trunking service. The single digit **9** was used as the ARS access code providing a facility for telephone users to dial 9 to reach an outside line. Use the **change feature-access-codes** command to configure a digit as the **Auto Route Selection (ARS) - Access Code 1**.

change feature-access-codes		Page 1 of 10
FEATURE ACCESS CODE (FAC)		
Abbreviated Dialing List1 Access Code:		
Abbreviated Dialing List2 Access Code:		
Abbreviated Dialing List3 Access Code:		
Abbreviated Dial - Prgm Group List Access Code:		
Announcement Access Code: *69		
Answer Back Access Code:		
Attendant Access Code:		
Auto Alternate Routing (AAR) Access Code: 7		
Auto Route Selection (ARS) - Access Code 1: 9		Access Code 2:

Use the **change ars analysis** command to configure the routing of dialled digits following the first digit 9. A small sample of dial patterns are shown here as an example. Further administration of ARS is beyond the scope of this document. The example entries shown will match outgoing calls to numbers beginning 0 or 00. Note that exact maximum number lengths should be used where possible to reduce post-dial delay. Calls are sent to **Route Pattern 1**.

change ars analysis 0							Page 1 of 2
ARS DIGIT ANALYSIS TABLE							
Location: all							Percent Full: 0
	Dialed String	Total Min	Total Max	Route Pattern	Call Type	Node Num	ANI Req'd
	0	8	14	1	pubu		n
	00	13	17	1	pubu		n
	00353	10	14	1	pubu		n
	0044	12	14	1	pubu		n
	0800	11	11	1	pubu		n
	118	5	6	1	pubu		n

Use the **change route-pattern x** command, where **x** is an available route pattern, to add the SIP trunk group to the route pattern that ARS selects. In this configuration, route pattern **1** is used to route calls to trunk group **1**. Set the **Numbering Format** to **unk-unk** to allow sending of national format CLI.

change route-pattern 1													Page	1 of	3						
Pattern Number: 1													Pattern Name: all calls								
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:	1	0											n	user							
2:													n	user							
3:													n	user							
4:													n	user							
5:													n	user							
6:													n	user							
BCC VALUE													TSC	CA-TSC	ITC	BCIE	Service/Feature	PARM	No.	Numbering	LAR
0 1 2 M 4 W													Request						Dgts Format		
																			Subaddress		
1:	y	y	y	y	y	n	n	rest					unk-unk		none						
2:	y	y	y	y	y	n	n	rest							none						
3:	y	y	y	y	y	n	n	rest							none						
4:	y	y	y	y	y	n	n	rest							none						
5:	y	y	y	y	y	n	n	rest							none						
6:	y	y	y	y	y	n	n	rest							none						

5.9. Administer Incoming Digit Translation

This step configures the settings necessary to map incoming DDI calls to the proper Communication Manager extension(s). The incoming digits sent in the INVITE message from Updata can be manipulated as necessary to route calls to the desired extension. In the example, the incoming DDI numbers provided by Updata for testing are assigned to the internal extensions of the test equipment configured within the Communication Manager. The **change inc-call-handling-trmt trunk-group x** command is used to translate numbers **01737nnnnn3** to **01737nnnnn7** to the 4 digit extension by deleting all (**11**) of the incoming digits and inserting the extension number. Note that the significant digits beyond the area code have been obscured.

change inc-call-handling-trmt trunk-group 1					Page	1 of 30
INCOMING CALL HANDLING TREATMENT						
Service/ Feature	Number Len	Number Digits	Del	Insert		
public-ntwrk	11	01737nnnnn3	11	2000		
public-ntwrk	11	01737nnnnn4	11	2396		
public-ntwrk	11	01737nnnnn5	11	2346		
public-ntwrk	11	01737nnnnn6	11	2296		
public-ntwrk	11	01737nnnnn7	11	2401		

5.10. EC500 Configuration

When EC500 is enabled on the Communication Manager station, a call to that station will generate a new outbound call from Communication Manager to the configured EC500 destination, typically a mobile phone. The following screen shows an example EC500 configuration for the user with station extension 2396. Use the command **change off-pbx-telephone station-mapping x** where **x** is the Communication Manager station.

- The **Station Extension** field will automatically populate with station extension
- For **Application** enter **EC500**
- Enter a **Dial Prefix** (e.g., 9) if required by the routing configuration
- For the **Phone Number** enter the phone that will also be called (e.g. **0035386nnnnnnnn**)
- Set the **Trunk Selection** to **1** so that Trunk Group 1 will be used for routing
- Set the **Config Set** to **1**

change off-pbx-telephone station-mapping 2396						Page	1 of	3
STATIONS WITH OFF-PBX TELEPHONE INTEGRATION								
Station	Application	Dial	CC	Phone Number	Trunk	Config	Dual	
Extension		Prefix			Selection	Set	Mode	
2396	EC500	-		0035386nnnnnnnn	1	1		
		-						

Save Communication Manager configuration changes by entering **save translation** to make them permanent.

6. Configuring Avaya Aura® Session Manager

This section provides the procedures for configuring Session Manager. The Session Manager is configured via the System Manager. The procedures include the following areas:

- Log in to Avaya Aura® System Manager
- Administer SIP domain
- Administer Locations
- Administer SIP Entities
- Administer Entity Links
- Administer Routing Policies
- Administer Dial Patterns
- Administer Application for Avaya Aura® Communication Manager
- Administer Application Sequence for Avaya Aura® Communication Manager
- Administer SIP Extensions

6.1. Log in to Avaya Aura® System Manager

Access the System Manager using a Web Browser by entering **http://<FQDN>/SMGR**, where **<FQDN>** is the fully qualified domain name of System Manager. Log in using appropriate credentials (not shown) and the **Home** tab will be presented with menu options shown below.



6.2. Administer SIP Domain

To add the SIP domain that will be used with Session Manager, select **Routing** from the **Home** tab menu and in the resulting tab select **Domains** from left hand menu. Click the **New** button to create a new SIP domain entry. In the **Name** field enter the domain name agreed with Updata; this will be the same as specified in the Authoritative Domain specified in the IP Network Region on the Communication Manager. Refer to **Section 5.3** for details. In test, **avaya.com** was used. Optionally, a description for the domain can be entered in the Notes field. Click **Commit** to save changes.

The screenshot shows a web interface for 'Domain Management'. At the top, there is a breadcrumb trail: 'Home / Elements / Routing / Domains'. Below this, the title 'Domain Management' is displayed. To the right of the title is a 'Help ?' link. Below the title, there are several action buttons: 'New', 'Edit', 'Delete', 'Duplicate', and 'More Actions' (which is a dropdown menu). Below the buttons, there is a table with the following structure:

1 Item Refresh			Filter: Enable
<input type="checkbox"/>	Name	Type	Notes
<input type="checkbox"/>	avaya.com	sip	

Below the table, there is a 'Select : All, None' option.

6.3. Administer Locations

Locations can be used to identify logical and/or physical locations where SIP Entities reside, for the purposes of bandwidth management. One location is added to the sample configuration for all of the enterprise SIP entities. On the **Routing** tab select **Locations** from the left hand menu. Under **General**, in the **Name** field, enter an informative name for the location. Scroll to the bottom of the page and under **Location Pattern** click **Add**, then enter an **IP Address Pattern** in the resulting new row (* is used to specify any number of allowed characters at the end of the string). Below is the location configuration used for the test enterprise.

Home / Elements / Routing / Locations

Location Details

Help ?

Commit

Cancel

General

* Name:

Galway

Notes:

Overall Managed Bandwidth

Managed Bandwidth Units:

Kbit/sec

Total Bandwidth:

Multimedia Bandwidth:

Audio Calls Can Take Multimedia Bandwidth:

☒

Per-Call Bandwidth Parameters

Maximum Multimedia Bandwidth (Intra-Location):

1000

Kbit/Sec

Maximum Multimedia Bandwidth (Inter-Location):

1000

Kbit/Sec

* Minimum Multimedia Bandwidth:

64

Kbit/Sec

* Default Audio Bandwidth:

80

Kbit/sec

Alarm Threshold

Overall Alarm Threshold:

80

%

Multimedia Alarm Threshold:

80

%

* Latency before Overall Alarm Trigger:

5

Minutes

* Latency before Multimedia Alarm Trigger:

5

Minutes

Location Pattern

Add

Remove

2 Items

Refresh

Filter: Enable

<input type="checkbox"/>	IP Address Pattern	Notes
<input type="checkbox"/>	* 10.10.9.*	
<input type="checkbox"/>	* 10.10.3.*	

6.4. Administer SIP Entities

A SIP Entity must be added for each SIP-based telephony system, supported by a SIP connection to the Session Manager. To add a SIP Entity, select **SIP Entities** on the left panel menu, and then click on the **New** button (not shown). The following will need to be entered for each SIP Entity.

Under **General**:

- In the **Name** field enter an informative name
- In the **FQDN or IP Address** field enter the IP address of the Session Manager or the signalling interface on the connecting system
- In the **Type** field use **Session Manager** for a Session Manager SIP entity, **Other** for a Communication Manager SIP entity and **SIP Trunk** for the SBC SIP entity
- In the **Location** field select the appropriate location from the drop down menu
- In the **Time Zone** field enter the time zone for the SIP Entity

In this configuration there are three SIP Entities:

- Avaya Aura® Session Manager SIP Entity
- Avaya Aura® Communication Manager SIP Entity
- Avaya Aura® Session Border Controller (SBC) SIP Entity

6.4.1. Avaya Aura® Session Manager SIP Entity

The following screens show the SIP entity for Session Manager. The **FQDN or IP Address** field is set to the IP address of the Session Manager SIP signalling interface.

The screenshot shows the 'SIP Entity Details' configuration page. The breadcrumb trail at the top is 'Home / Elements / Routing / SIP Entities'. The page title is 'SIP Entity Details' with a 'Help ?' link. There are 'Commit' and 'Cancel' buttons in the top right. The 'General' tab is selected. The form contains the following fields:

- Name:** Session Manager
- FQDN or IP Address:** 10.10.9.61
- Type:** Session Manager (dropdown menu)
- Notes:** (empty text area)
- Location:** Galway (dropdown menu)
- Outbound Proxy:** (empty dropdown menu)
- Time Zone:** Europe/Dublin (dropdown menu)
- Credential name:** (empty text area)

Below the 'General' tab is the 'SIP Link Monitoring' section, which contains a dropdown menu set to 'Use Session Manager Configuration'.

The Session Manager must be configured with the port numbers on the protocols that will be used by the other SIP entities. To configure these scroll to the bottom of the page and under **Port**, click **Add**, then edit the fields in the resulting new row.

- In the **Port** field enter the port number on which the system listens for SIP requests
- In the **Protocol** field enter the transport protocol to be used for SIP requests
- In the **Default Domain** field, from the drop down menu select the domain added in **Section 6.2** as the default domain

Port

TCP Failover port:

TLS Failover port:

3 Items Refresh Filter: Enable

<input type="checkbox"/>	Port	Protocol	Default Domain	Notes
<input type="checkbox"/>	5060	TCP	avaya.com	<input type="text"/>
<input type="checkbox"/>	5060	UDP	avaya.com	<input type="text"/>
<input type="checkbox"/>	5061	TLS	avaya.com	<input type="text"/>

Select : All, None

6.4.2. Avaya Aura® Communication Manager SIP Entity

The following screen shows the SIP entity for Communication Manager which is configured as an Evolution Server. The **FQDN or IP Address** field is set to the IP address of the interface on Communication Manager that will be providing SIP signalling. Set the location to that defined in **Section 6.3** and the **Time Zone** to the appropriate time zone.

Home / Elements / Routing / SIP Entities Help ?

SIP Entity Details

General

* Name: Communication Manager

* FQDN or IP Address: 10.10.9.52

Type: CM

Notes:

Adaptation:

Location: Galway

Time Zone: Europe/Dublin

Override Port & Transport with DNS SRV: ☐

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

Credential name:

Call Detail Recording: none

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

6.4.3. Avaya Aura® Session Border Controller (SBC) SIP Entity

The following screen shows the SIP Entity for the SBC. The **FQDN or IP Address** field is set to the IP address of the SBC private network interface (see **Figure 1**). Set the location to that defined in **Section 6.3** and the **Time Zone** to the appropriate time zone.

Home / Elements / Routing / SIP Entities Help ?

SIP Entity Details Commit Cancel

General

* Name: AASBC

* FQDN or IP Address: 10.10.9.67

Type: SIP Trunk

Notes:

Adaptation:

Location: Galway

Time Zone: Europe/Dublin

Override Port & Transport with DNS SRV: ☐

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

Credential name:

Call Detail Recording: egress

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

6.5. Administer Entity Links

A SIP trunk between a Session Manager and another system is described by an Entity Link. To add an Entity Link, select **Entity Links** on the left panel menu and click on the **New** button (not shown). Fill in the following fields in the new row that is displayed.

- In the **Name** field enter an informative name
- In the **SIP Entity 1** field select **Session Manager**
- In the **Port** field enter the port number to which the other system sends its SIP requests
- In the **SIP Entity 2** field enter the other SIP Entity for this link, created in **Section 6.4**
- In the **Port** field enter the port number to which the other system expects to receive SIP requests
- Select the **Trusted** tick box to make the other system trusted
- In the **Protocol** field enter the transport protocol to be used to send SIP requests

Click **Commit** to save changes. The following screen shows the Entity Links used in this configuration.

Home / Elements / Routing / Entity Links Help ?

Entity Links

5 Items Refresh Filter: Enable

<input type="checkbox"/>	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Deny New Service	Notes
<input type="checkbox"/>	AASBC Link	Session Manager	TCP	5060	AASBC	5060	Trusted	<input type="checkbox"/>	
<input type="checkbox"/>	ASBCE Link	Session Manager	TCP	5060	ASBCE	5060	Trusted	<input type="checkbox"/>	
<input type="checkbox"/>	CS1K Link	Session Manager	TCP	5060	CS1K	5060	Trusted	<input type="checkbox"/>	
<input type="checkbox"/>	Msg Link	Session Manager	TCP	5060	Messaging	5060	Trusted	<input type="checkbox"/>	
<input type="checkbox"/>	Session Manager Communication Manager 5061 TLS	Session Manager	TCP	5060	Communication Manager	5060	Trusted	<input type="checkbox"/>	

Select : All, None

6.6. Administer Routing Policies

Routing policies must be created to direct how calls will be routed to a system. To add a routing policy, select **Routing Policies** on the left panel menu and then click on the **New** button (not shown).

Under **General**:

- Enter an informative name in the **Name** field
- 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 then select the time range

The following screen shows the routing policy for Communication Manager.

Home / Elements / Routing / Routing Policies Help ?

Routing Policy Details Commit Cancel

General

* Name:

Disabled: ☐

* Retries:

Notes:

SIP Entity as Destination

Name	FQDN or IP Address	Type	Notes
Communication Manager	10.10.9.52	CM	

Time of Day

1 Item Refresh Filter: Enable

Ranking	Name	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
<input type="checkbox"/> 0	24/7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	00:00	23:59	Time Range 24/7

The following screen shows the routing policy for the SBC.

Home / Elements / Routing / Routing Policies Help ?

Routing Policy Details Commit Cancel

General

* Name:

Disabled: ☐

* Retries:

Notes:

SIP Entity as Destination

Name	FQDN or IP Address	Type	Notes
AASBC	10.10.9.67	SIP Trunk	

Time of Day

1 Item Refresh Filter: Enable

Ranking	Name	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
<input type="checkbox"/> 0	24/7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	00:00	23:59	Time Range 24/7

6.7. Administer Dial Patterns

A dial pattern must be defined to direct calls to the appropriate telephony system. To configure a dial pattern select **Dial Patterns** on the left panel menu and then click on the **New** button (not shown).

Under **General**:

- In the **Pattern** field enter a dialled number or prefix to be matched
- In the **Min** field enter the minimum length of the dialled number
- In the **Max** field enter the maximum length of the dialled number
- In the **SIP Domain** field select **ALL** or alternatively one of those configured in **Section 6.2**

Configuration is continued on the next page.

Under **Originating Locations and Routing Policies**. Click **Add**, in the resulting screen (not shown), under **Originating Location** select the location defined in **Section 6.3** or **ALL** and under **Routing Policies** select one of the routing policies defined in **Section 6.6**. Click **Select** button to save. The following screen shows an example dial pattern configured for the SBC which will route the calls out to the Updata Business Trunk service.

Home / Elements / Routing / Dial Patterns Help ?

Dial Pattern Details Commit Cancel

General

* Pattern: 00

* Min: 8

* Max: 14

Emergency Call: ☐

Emergency Priority: 1

Emergency Type:

SIP Domain: -ALL- v

Notes:

Originating Locations and Routing Policies

Add Remove

1 Item Refresh Filter: Enable

<input type="checkbox"/>	Originating Location Name 1	Originating Location Notes	Routing Policy Name	Rank 2	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	Galway		External	0	<input type="checkbox"/>	AASBC	

The following screen shows the test dial pattern configured for Communication Manager.

Home / Elements / Routing / Dial Patterns Help ?

Dial Pattern Details Commit Cancel

General

* Pattern: 01737nnnnn

* Min: 10

* Max: 11

Emergency Call: ☐

Emergency Priority: 1

Emergency Type:

SIP Domain: -ALL- v

Notes:

Originating Locations and Routing Policies

Add Remove

1 Item Refresh Filter: Enable

<input type="checkbox"/>	Originating Location Name 1	Originating Location Notes	Routing Policy Name	Rank 2	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	Galway		Internal	0	<input type="checkbox"/>	Communication Manager	

Note: The pattern to be matched has been obscured.

6.8. Administer Application for Avaya Aura® Communication Manager

From the **Home** tab select **Session Manager** from the menu. In the resulting tab from the left panel menu select **Application Configuration** → **Applications** and click **New**.

- In the **Name** field enter a name for the application
- In the **SIP Entity** field select the SIP entity for the Communication Manager
- In the **CM System for SIP Entity** field select the SIP entity for the Communication Manager and select **Commit** to save the configuration.

The screenshot shows the 'Application Editor' window. The breadcrumb path is 'Home / Elements / Session Manager / Application Configuration / Applications'. The window has 'Commit' and 'Cancel' buttons. The 'Application' section contains the following fields:

- *Name**: Text field with 'cm-app' entered.
- *SIP Entity**: Dropdown menu with 'Communication Manager' selected.
- *CM System for SIP Entity**: Dropdown menu with 'Communication Manager' selected, followed by a 'Refresh' button and a link 'View/Add CM Systems'.
- Description**: Empty text field.

6.9. Administer Application Sequence for Avaya Aura® Communication Manager

From the left panel navigate to **Session Manager** → **Application Configuration** → **Application Sequences** and click on **New**.

- In the **Name** field enter a descriptive name
- Under **Available Applications**, click the + sign in front of the appropriate application instance. When the screen refreshes the application should be displayed under the **Applications in this Sequence** heading. Select **Commit**.

The screenshot shows the 'Application Sequence Editor' window. The breadcrumb path is 'Home / Elements / Session Manager / Application Configuration / Application Sequences'. The window has 'Commit' and 'Cancel' buttons and a 'Help ?' link. The 'Application Sequence' section contains:

- *Name**: Text field with 'cm-app-seq' entered.
- Description**: Empty text field.

The 'Applications in this Sequence' section includes 'Move First', 'Move Last', and 'Remove' buttons. Below is a table with 1 item:

<input type="checkbox"/>	Sequence Order (first to last)	Name	SIP Entity	Mandatory	Description
<input type="checkbox"/>	1	cm-app	Communication Manager	<input checked="" type="checkbox"/>	

Below the table is a 'Select : All, None' option.

The 'Available Applications' section includes a 'Refresh' button and a table with 1 item:

<input checked="" type="checkbox"/>	Name	SIP Entity	Description
<input checked="" type="checkbox"/>	cm-app	Communication Manager	

At the bottom right of the 'Available Applications' section is a 'Filter: Enable' link.

6.10. Administer SIP Extensions

SIP extensions are registered with the Session Manager and use Communication Manager for their feature and configuration settings. From the **Home** tab select **User Management** from the menu. Then select **Manage Users** and click **New** (not shown).

On the **Identity** tab:

- Enter the user's name in the **Last Name** and **First Name** fields
- In the **Login Name** field enter a unique system login name in the form of user@domain (e.g. **2402@avaya.com**) which is used to create the user's primary handle
- The **Authentication Type** should be **Basic**
- In the **Password/Confirm Password** fields enter an alphanumeric password
- Set the **Language Preference** and **Time Zone** as required

Home / Users / User Management / Manage Users Help ?

New User Profile

Commit & Continue Commit Cancel

Identity * **Communication Profile** * **Membership** **Contacts**

Identity ▾

* Last Name:

* First Name:

Middle Name:

Description:

* Login Name:

* Authentication Type:

Password:

Confirm Password:

Localized Display Name:

Endpoint Display Name:

Title:

Language Preference:

Time Zone:

On the **Communication Profile** tab, enter a numeric **Communication Profile Password** and confirm it, then expand the **Communication Address** section and click **New**. For the **Type** field select **Avaya SIP** from the drop-down menu. In the **Fully Qualified Address** field, enter an extension number and select the relevant domain from the drop-down menu. Click the **Add** button (not shown).

The screenshot shows the 'Communication Profile' tab in a web interface. At the top, there are tabs for 'Identity', 'Communication Profile', 'Membership', and 'Contacts'. The 'Communication Profile' tab is active. Below the tabs, there is a section titled 'Communication Profile' with a dropdown arrow. It contains two password fields: 'Communication Profile Password' and 'Confirm Password', both with masked characters (dots). Below these fields are buttons for 'New', 'Delete', 'Done', and 'Cancel'. A table with the header 'Name' shows a single entry 'Primary' with a green circle icon. Below the table, it says 'Select : None'. There is a field for '* Name:' with the value 'Primary' and a 'Default:' checkbox which is checked. Below this is a section titled 'Communication Address' with a dropdown arrow. It contains buttons for 'New', 'Edit', and 'Delete'. Below these buttons is a table with the header 'Type', 'Handle', and 'Domain'. The table is empty, with the text 'No Records found' below it. Below the table, there is a form for adding a new address. It has a 'Type:' dropdown menu with 'Avaya SIP' selected. Below it is a field for '* Fully Qualified Address:' with the value '2402' and a domain dropdown menu with 'avaya.com' selected.

Identity * Communication Profile * Membership Contacts

Communication Profile ▾

Communication Profile Password:
Confirm Password:

New Delete Done Cancel

Name
Primary

Select : None

* Name: Primary
Default : ☒

Communication Address ▾

New Edit Delete

Type	Handle	Domain
No Records found		

Type: Avaya SIP ▾
* Fully Qualified Address: 2402 @ avaya.com ▾

Expand the **Session Manager Profile** section.

- Make sure the **Session Manager Profile** check box is checked
- Select the appropriate Session Manager instance from the drop-down menu in the **Primary Session Manager** field
- Select the appropriate application sequence from the drop-down menu in the **Origination Application Sequence** field configured in **Section 6.9**
- Select the appropriate application sequence from the drop-down menu in the **Termination Application Sequence** field configured in **Section 6.9**
- Select the appropriate location from the drop-down menu in the **Home Location** field

☒ Session Manager Profile

SIP Registration

* Primary Session Manager

Session Manager

Primary	Secondary	Maximum
5	0	5

Secondary Session Manager

(None)

Survivability Server

(None)

Application Sequences

Origination Sequence

cm-app-seq

Termination Sequence

cm-app-seq

Call Routing Settings

* Home Location

Galway

Conference Factory Set

(None)

Expand the **Endpoint Profile** section.

- Select the Communication Manager SIP Entity from the **System** drop-down menu
- Select **Endpoint** from the drop-down menu for **Profile Type**
- Enter the extension in the **Extension** field
- Select the desired template from the **Template** drop-down menu
- For the **Port** field select **IP**
- Select the **Delete Endpoint on Unassign of Endpoint from User or on Delete User** check box
- Select **Commit** (Not Shown) to save changes and the System Manager will add the Communication Manager user configuration automatically

The screenshot shows the 'CM Endpoint Profile' configuration form. It includes fields for System (Communication Manager), Profile Type (Endpoint), Extension (2402), Template (9630SIP_DEFAULT_CM_6_2), Set Type (9630SIP), Security Code, Port (IP), Voice Mail Number, Preferred Handle (None), and checkboxes for 'Delete Endpoint on Unassign of Endpoint from User or on Delete User' and 'Override Endpoint Name'. A 'Use Existing Endpoints' checkbox is also present. A red box highlights the 'Delete Endpoint on Unassign of Endpoint from User or on Delete User' checkbox, which is checked.

☒ CM Endpoint Profile

* System: Communication Manager

* Profile Type: Endpoint

Use Existing Endpoints: ☐

* Extension: 2402 [Endpoint Editor]

* Template: 9630SIP_DEFAULT_CM_6_2

Set Type: 9630SIP

Security Code:

Port: IP

Voice Mail Number:

Preferred Handle: (None)

Enhanced Callr-Info display for 1-line phones: ☐

Delete Endpoint on Unassign of Endpoint from User or on Delete User: ☒

Override Endpoint Name: ☒

7. Configure Avaya Aura® Session Border Controller

This section provides the procedures for configuring the SBC to receive and route calls over the SIP trunk between Communication Manager and Udata SIP Trunking. These instructions assume other administration activities have already been completed such as the default configuration. This section will cover the configuration that was put in place specifically for Udata.

7.1. Access Avaya Aura® Session Border Controller

Access the SBC using a web browser by entering the URL **https://<ip-address>**, where **<ip-address>** is the private IP address configured.

Acme Packet Net-Net OS-E

To access the NNOS-E management interface, you must first log in. Please provide your user name and password.

Username:	<input type="text"/>
Password:	<input type="password"/>
	<input type="button" value="Login"/>

7.2. Verify Outside Interface was configured at installation

An IP address was given to the outside interface that is on the public internet. The IP address is modified in the screenshot below for security purposes. Click on the **Configuration** tab and browse to **cluster → interface eth2 → ip outside**.

Configuration: all

Configuration | Setup | View

cluster

- box sbcv9.avaya.com
 - interface eth0
 - interface eth2
 - ip outside**
 - sip
 - media-ports
 - routing
 - route Default
 - route external-sip-med
 - kernel-filter
 - allow-rule allow-sip-udc
 - cli
- vsp
 - default-session-config
 - tls
 - session-config-pool
 - dial-plan

general:

* name	outside
admin	enabled (Resource is active)
* ip-address	<div>* type: static (static IP address)</div> <div>* address/mask: 192.168.122.56/25 (n.n.n.n/n)</div>
geolocation	0
security-domain	enter or select from <Not configured>
address-scope	enter or select from <Not configured>
filter-intf	disabled (Resource is inactive)
media-ports	Delete

7.3. Configure External Interface

7.3.1. Configure SIP Port

For the outside interface a transport protocol needs to be configured. In the compliance testing UDP was used for the SIP messaging. Click on the Configuration tab and browse to **cluster** → **interface eth2** → **ip outside** → **sip**.

- **Port** Port number to be used for SIP messaging, default is **5060**

Configuration: all

Configuration Setup View

cluster

- box sbcv9.avaya.com
 - interface eth0
 - interface eth2
 - ip outside
 - sip**
 - media-ports
 - routing
 - route Default
 - route external-sip-med
 - kernel-filter
 - allow-rule allow-sip-udp

vsp

Configure cluster\box sbcv9.avaya.com\interface eth2\ip outside\sip\udp-port 5060

Set Reset Back Copy Delete

* port 5060 (at minimum 1,default=5060)

from-server

to-server

transport any (All protocol types)

remote-port 0 (from 0 to 65,535)

certificate

The newly created UDP port is shown below

Configuration: all

Configuration Setup View

cluster

- box sbcv9.avaya.com
 - interface eth0
 - interface eth2
 - ip outside
 - sip**
 - media-ports
 - routing
 - route Default
 - route external-sip-med
 - kernel-filter
 - allow-rule allow-sip-udp

admin enabled (Resource is active)

nat-translation disabled (Resource is inactive)

nat-add-received-from disabled (Resource is inactive)

nat-add-X-Remote-Info enabled (Resource is active)

load-balance-head-end false

udp-port

	udp-port	from-server	to-server	transport	remote-port	certificate
Edit Delete	udp-port 5060	Edit	Edit	any	0	Edit

Add udp-port

7.3.2. Configure Routing

Configure routing on the outside interface to correctly route the SIP traffic from the interface to Updata's network. The IP address is modified in the screenshot below for security purposes. Click on the Configuration tab and browse to **cluster** → **interface eth2** → **ip outside** → **routing** → **add route**.

The following values need to be added for the new route that is being created:

- **Admin** Enables or disables this route configuration
- **route name** Enter a name for the route
- **destination type** Use **default** as the network route
- **destination address/mask** The destination address is the subnet used by the service provider and mask
- **gateway** Sets the gateway or next hop IP address for the packet
- **metric** Associates a cost for the route, default is 1

Configuration: all

Configuration Setup View

- cluster
 - box sbcv9.avaya.com
 - interface eth0
 - interface eth2
 - ip outside
 - sip
 - media-ports
 - routing
 - route Default
 - route external-sip-med
 - kernel-filter
 - allow-rule allow-sip-udp

cli

Configure cluster\box sbcv9.avaya.com\interface eth2\ip outside\routing\route Default

Set Reset Back Copy Delete

admin	enabled (Resource is active)
* route-name	Default
* destination	* type default (default route)
* gateway	192.168.122.51 (n.n.n.n)
metric	1 (from 0 to 1,000, default=1)

Note: Default routing is used so that all IP packets not recognised as being destined for the enterprise will be routed to the network via the external interface. This will apply to both signalling and media. The gateway address is the next hop router, the address has been modified for security purposes. Note also that a route is configured for external media on the test equipment. This route isn't used, however, and media is routed by the **Default** route along with signalling.

7.3.3. Kernel Filter

The kernel filter was not used during test and configuration is not covered in this document. It is important to check, however, as previous configuration may block IP traffic from the new SIP trunk. To check, browse to **cluster** → **interface eth2** → **ip outside** → **kernel-filter**. Ensure that no filter is configured and enabled that would disallow traffic from the network.

7.4. Configure VSP

7.4.1. Configure Session-Config-Pool Entry ToTelco

During test, the default action with regard to uri modification for signalling going out to the network was used. This replaces domain names and internal IP addresses with external IP addresses only. If modification of the “To” uri is required, expand **vsp** → **session-config pool** → **entry ToTelco** → **to-uri-specification**. The screenshot below shows the default settings.

Configuration: all

Configuration Setup View

- cluster
 - box sbcv9.avaya.com
 - interface eth0
 - interface eth2
 - ip outside
 - sip
 - media-ports
 - routing
 - route Default
 - route external-sip-media-1
 - kernel-filter
 - allow-rule allow-sip-udp-from
- vsp
 - default-session-config
 - tls
 - session-config-pool
 - entry ToTelco
 - to-uri-specification**
 - from-uri-specification
 - request-uri-specification
 - p-asserted-identity-uri-specification
 - entry ToPBX

Configure vsp\session-config-pool\entry ToTelco\to-uri-specification Help Index

Set Reset Back Delete

user	enter request-uri or select from request-uri (Net-N URI.)
host	enter next-hop or select from next-hop (Net-Net OS-E)
port	enter to-uri or select from to-uri (Net-Net OS-E)
display	enter to-uri or select from to-uri (Net-Net OS-E)
transport	to-uri (Net-Net OS-E uses the value from the incoming TO URI.)
user-param	omit
user-truncate-non-digits	disabled (Resource is inactive)
uri-parameter	Add uri-parameter
header-parameter	

If modification of the “From” uri is required, expand **vsp** → **session-config pool** → **entry ToTelco** → **from-uri-specification**. If modification of the “P-Asserted-ID” uri is required, expand **vsp** → **session-config pool** → **entry ToTelco** → **p-asserted-identity-uri-specification**. Screenshots are not shown for the above settings as default values were used..

7.4.2. Configure Session-Config-Pool Entry ToPBX

During test, the default action with regard to uri modification for signalling going in to the PBX was used. This replaces domain names and external IP addresses with internal IP addresses only. If modification is required, expand **vsp** → **session-config pool** → **entry ToPBX** → **to-uri-specification**.

The screenshot below shows the default settings for modification of the “To” uri for signalling going in to the PBX.

Configuration: all

Configuration Setup View

- cluster
 - box sbcv9.avaya.com
 - interface eth0
 - interface eth2
 - ip outside
 - sip
 - media-ports
 - routing
 - route Default
 - route external-sip-media-1
 - kernel-filter
 - allow-rule allow-sip-udp-from
 - cli
- vsp
 - default-session-config
 - tls
 - session-config-pool
 - entry ToTelco
 - entry ToPBX
 - to-uri-specification
 - request-uri-specification

Configure vsp\session-config-pool\entry ToPBX\to-uri-specification [Help](#) [Index](#)

Set Reset Back Delete

user	enter	to-uri	or select from	to-uri	(Net-N)
host	enter	next-hop-domain	or select from	next-hop-domain	(Net-Net)
port	enter	to-uri	or select from	to-uri	(Net-Net OS-E)
display	enter	to-uri	or select from	to-uri	(Net-Net OS-E)
transport		to-uri			(Net-Net OS-E uses the value from the incoming TO URI.)
user-param		omit			
user-truncate-non-digits		disabled			(Resource is inactive)
uri-parameter		Add uri-parameter			
header-parameter					

7.4.3. Configure Enterprise

To add the additional IP addresses for the Updata Network SBC click on the Configuration tab and browse to **vsp** → **enterprise** → **servers** → **sip-gateway Telco** → **server-pool**. A list of the IP addresses already configured in the server pool is displayed in the right hand pane. Either edit an existing server (not shown) or click the **Add server** link (not shown) as required.

In the resulting page enter a name for the server in the **server-name** field and an IP address in the **host** field. Ensure the **transport** and **port** fields are configured as required. The IP address in the screenshot below has been modified for security purposes. Click the **Set** button (not shown).

Configuration: all

Configuration Setup View

- cluster
 - box sbcv9.avaya.com
- vsp
 - default-session-config
 - tls
 - session-config-pool
 - dial-plan
 - enterprise
 - servers
 - sip-gateway PBX
 - sip-gateway Telco
 - vsp\session-config-pool\entry ToTelco
 - server-pool
 - server Telco1
 - dns
 - settings

General:

* server-name	Telco1
admin	enabled (Resource is active)
* host	192.168.192.164 (host name or n.n.n.n)
transport	transport UDP (User Datagram Protocol)
port	5060 (at minimum 1,default=5060)

Policy:

outbound-normalization	Add outbound-normalization
inbound-normalization	Add inbound-normalization

In the resulting page verify the details entered and edit if necessary.

Configuration: all

Configuration Setup View

- cluster
 - box sbcv9.avaya.com
- vsp
 - default-session-config
 - tls
 - session-config-pool
 - dial-plan
 - enterprise
 - servers
 - sip-gateway PBX
 - vsp\session-config-pool\entry ToPBX
 - server-pool
 - server PBX1
 - sip-gateway Telco
 - vsp\session-config-pool\entry ToTelco
 - server-pool
 - server Telco1

general:

* name: Telco

admin: enabled (Resource is active)

domain:

failover-detection: ping (Use OPTIONS to detect failures)

servers:

server-pool (Delete)

	server	admin	host	transport	port
Edit Delete	server Telco1	enabled	192.168.192.164	UDP	5060

Add server

Repeat these steps for each additional IP address that needs to be added to the Session Border Controller server pool.

7.5. Save the Configuration

To save the configuration, click on **Configuration** in the left pane to display the configuration menu. Next, select **Update and save configuration**.

Configuration: all

Configuration Setup View

- Update and save configuration
- Reload configuration
- Validate configuration
- Analyze configuration
- Search configuration
- Save as XML
- Load from XML

Update and save the current configuration.

8. Configure Udata Equipment

The configuration of the Udata equipment used to support the Udata SIP Trunking service is outside of the scope of these Application Notes and will not be covered. To obtain further information on Udata equipment and system configuration please contact an authorised Udata representative.

9. Verification Steps

This section provides steps that may be performed to verify that the solution is configured correctly.

1. From System Manager **Home** tab click on **Session Manager** and navigate to **Session Manager → System Status → SIP Entity Monitoring**. Select the relevant SIP Entity from the list and observe if the **Conn Status** and **Link Status** are showing as **up**.

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

Help ?

SIP Entity, Entity Link Connection Status

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

All Entity Links to SIP Entity: AASBC

Summary View

Status Details for the selected Session Manager:

1 Items | Refresh

Filter: Enable

Session Manager Name	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
<input checked="" type="radio"/> Session Manager	10.10.9.67	5060	TCP	FALSE	UP	200 OK	UP

2. From the Communication Manager SAT interface run the command **status trunk n** where **n** is a previously configured SIP trunk. Observe if all channels on the trunk group display **in-service/idle**.

```
status trunk 1
```

TRUNK GROUP STATUS			
Member	Port	Service State	Mtce Connected Ports Busy
0001/001	T00001	in-service/idle	no
0001/002	T00002	in-service/idle	no
0001/003	T00003	in-service/idle	no
0001/004	T00004	in-service/idle	no
0001/005	T00005	in-service/idle	no
0001/006	T00006	in-service/idle	no
0001/007	T00007	in-service/idle	no
0001/008	T00008	in-service/idle	no
0001/009	T00009	in-service/idle	no
0001/010	T00010	in-service/idle	no

3. Verify that endpoints at the enterprise site can place calls to the PSTN and that the call remains active.
4. Verify that endpoints at the enterprise site can receive calls from the PSTN and that the call can remain active.
5. Verify that the user on the PSTN can end an active call by hanging up.
6. Verify that an endpoint at the enterprise site can end an active call by hanging up.

10. Conclusion

These Application Notes describe the configuration necessary to connect Avaya Aura® Communication Manager R6.2 as an Evolution Server, Avaya Aura® Session Manager R6.3 and Avaya Aura® Session Border Controller to the Updata SIP Trunking service. Updata SIP Trunking is a SIP-based Voice over IP solution providing businesses a flexible, cost-saving alternative to traditional hardwired telephony trunks. The service was successfully tested with a number of observations listed in **Section 2.2**.

11. Additional References

This section references the documentation relevant to these Application Notes. Additional Avaya product documentation is available at <http://support.avaya.com>.

- [1] *Installing and Configuring Avaya Aura® System Platform*, Release 6.2.2, December 2012.
- [2] *Administering Avaya Aura® System Platform*, Release 6.2.1, July 2012.
- [3] *Administering Avaya Aura® Communication Manager*, Release 6.2, December 2012.
- [4] *Avaya Aura® Communication Manager Feature Description and Implementation*, December 2012, Document Number 555-245-205.
- [5] *Implementing Avaya Aura® System Manager* Release 6.3, December 2012
- [6] *Upgrading Avaya Aura® System Manager to 6.3*, January 2013.
- [7] *Administering Avaya Aura® System Manager* Release 6.3, December 2012
- [8] *Implementing Avaya Aura® Session Manager* Release 6.3, December 2012
- [9] *Upgrading Avaya Aura® Session Manager* Release 6.3, December 2012
- [10] *Administering Avaya Aura® Session Manager* Release 6.3, December 2012,
- [11] *Installing and Configurinnng Avaya Aura® Sesion Border Controller* Release 6.0.1, November 2010
- [12] *RFC 3261 SIP: Session Initiation Protocol*, <http://www.ietf.org/>

©2013 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.