



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

---

# **Application Notes for configuring Capita Secure Information Solutions DS3000 with Avaya Aura® Session Manager R7.0.1 and Avaya Aura® Communication Manager R7.0.1 using SIP Trunks - Issue 1.0**

## **Abstract**

These Application Notes describe the configuration steps for provisioning Capita Secure Information Solutions DS3000 to interoperate with Avaya Aura® Session Manager R7.0.1 and Avaya Aura® Communication Manager R7.0.1.

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

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

# 1. Introduction

These Application Notes describe the configuration steps for provisioning DS3000 from Capita Secure Information Solutions to interoperate with Avaya Aura® Session Manager R7.0.1 connecting to Avaya Aura® Communication Manager R7.0.1. The DS3000 is an Integrated Communication Control System that is used by emergency service customers for answering 999/112 calls and then from the same application using radio communication (TETRA digital radio or analogue PMR) to pass details to mobile resources.

As a radio dispatch deployment with basic PTN/PSTN the DS3000 acts as an end Private Branch Exchange (PBX) and performs call prioritisation and distribution to DS3000 operators as defined by the profile in which they have logged in to the DS3000 application. In this type of configuration the DS3000 has one primary connection to the Avaya Solution, a SIP connection to Avaya Aura® Session Manager. The DS3000 supports basic call control including hold and transfer.

## 2. General Test Approach and Test Results

The interoperability compliance testing evaluates the ability of the DS3000 application to make and receive calls to and from Communication Manager endpoints. All calls destined for the DS3000 both locally and from the PSTN are routed to the DS3000 over SIP trunks using Session Manager to route the calls.

**Note:** A UDP Entity Link was setup in order to make calls between Session Manager and the DS3000.

**Note:** The link between CM and SM had to be setup as TCP, if this was setup as TLS there was an issue with the Session Manager being unable to send on any ACK due to an error in the Contact Header from the DS3000, the Contact Header contains SIPS instead of SIP. Changing the SM – CM link forces the DS3000 to use SIP instead of SIPS but this is not normal behaviour from the DS3000

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 compliance testing focuses on various technical testing scenarios to verify the usage of DS3000 with the Avaya solution. In addition, serviceability tests were also performed to assess the reliability and accuracy of the joint solution. The testing focused on the following types of calls:

- **Calls to Communication Manager endpoints** – Ensure that calls can be made to Communication Manager extensions from DS3000.
- **Calls to DS3000 Operators**– Ensure that calls can be made to DS3000 operators from Communication Manager extensions.
- **Calls to PSTN from DS3000 Operators** – Ensure that calls can be made from DS3000 to PSTN across the SIP trunk through Communication Manager.
- **Calls from PSTN into DS3000 Operators** – Ensure that calls can be made to DS3000 from the PSTN by calling into Communication Manager and across the SIP trunk to the DS3000.
- **Hold/transfer and conference functionality**– Verify that calls can be placed on hold and transferred and conferenced.
- **Caller information is preserved on all calls to/from DS3000** – Ensure that the correct CLID information is preserved.
- **Failover testing** – Verify the behaviour of DS3000 application under different simulated LAN failure conditions on the Avaya platform.

**Note:** All test cases were performed with the following set on the signalling group.

- Direct IP-IP Audio Connections set to Y and Initial Direct IP-IP Media set to N.
- Direct IP-IP Audio Connections set to Y and Initial Direct IP-IP Media set to Y.

## 2.2. Test Results

Most test cases passed except for the following issues observed.

- DTMF does not work with Avaya Aura® Messaging; DS3000 uses in-band DTMF that is not compatible with Messaging.
- When the operator recalls to the original caller and then hangs up the call the original PSTN caller is transferred to the voicemail and that is because the line to the voicemail is still active.
- Music on Hold is never heard although the signalling looks correct and the call is held properly the DS3000 seems to receive the RTP from the Media but the hold music is not played. This is due to the DS3000 playing their own hold music when they are on hold.

**Note:** The link between CM and SM had to be setup as TCP, if this was setup as TLS there was an issue with the Session Manager being unable to send on any ACK due to an error in the Contact Header from the DS3000, the Contact Header contains SIPS instead of SIP. Changing the SM – CM link forces the DS3000 to use SIP instead of SIPS but this is not normal behaviour from the DS3000.

Issues observed with Direct IP-IP Audio Connections set to Y and Initial Direct IP-IP Media set to N:

1. Communication Manager SIP phone transferring DS3000 to DS3000 fails ONLY for Supervised transfer. The DS3000 does not seem to be handling the REFER messages from the Communication Manager correctly and to stop sending REFER messages

setting “Network Call Redirection” to “N” on the Communication Manager Trunk Group seemed to solve this issue.

2. CLID is not being updated correctly upon transfer when Communication Manager has completed the transfer from one DS3000 to another. The DS3000 display was not updated with the new CLID once the transfer was completed. The DS3000 is either not updating its own GUI correctly or it is not taking the updates for the display information from the “Contact” or the “P-Asserted-Identity” headers.
3. Blind transfer does not work when the DS3000 is making the blind transfer for any call being transferred into a H323 phone. This can be from another H323 phone, A SIP or a Digital Phone. Two things observed, 1) The DS3000 is not performing the Blind Transfer as we would expect as the transfer does not complete until party C answers the call. Typically ringback would be heard on party A as A and C would be connected before C answers the call. 2) The issue here occurs when the Communication Manager sends an empty INVITE (for shuffling) to the DS3000, this creates a situation on the DS3000 that stops them sending a new INVITE and subsequent REFER back to Communication Manager.

Issues observed with Direct IP-IP Audio Connections set to Y and Initial Direct IP-IP Media set to Y:

1. Communication Manager SIP phone transferring DS3000 to DS3000 fails for both Supervised and Blind. The DS3000 does not seem to be handling the REFER messages from the Communication Manager correctly and to stop sending REFER messages setting “Network Call Redirection” to “N” on the Communication Manager Trunk Group seemed to solve this issue.
2. CLID is not being updated correctly upon transfer when Communication Manager has completed the transfer from one DS3000 to another. The DS3000 display was not updated with the new CLID once the transfer was completed. The DS3000 is either not updating its own GUI correctly or it is not taking the updates for the display information from the “Contact” or the “P-Asserted-Identity” headers.

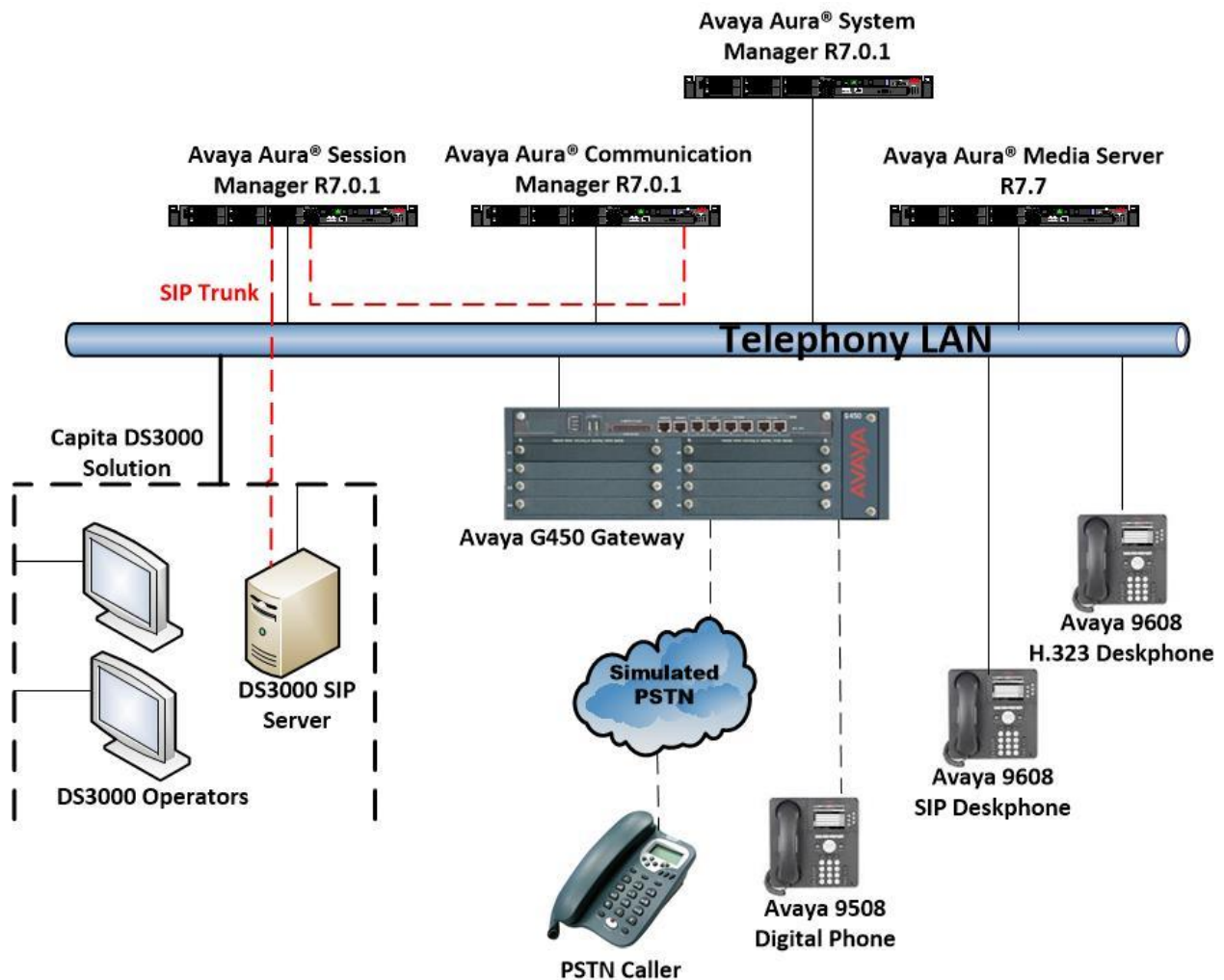
## 2.3. Support

Support from Avaya is available by visiting the website <http://support.avaya.com> and a list of product documentation can be found in **Section 10** of these Application Notes. Technical support for the Capita DS3000 product can be obtained as follows.

- Tel : + 44 (0) 8456 041999
- Email: [csis.info@capita.co.uk](mailto:csis.info@capita.co.uk)

### 3. Reference Configuration

**Figure 1** shows the setup for compliance testing Capita's DS3000 with Communication Manager using SIP signalling over a SIP trunk to pass callers from Communication Manager to the DS3000 Operators.



**Figure 1: Connection of Capita DS3000 with Avaya Aura® Communication Manager R7.0.1 and Avaya Aura® Session Manager R7.0.1**

## 4. Equipment and Software Validated

The following equipment and software was used for the compliance test.

Equipment/Software	Release/Version
Avaya Aura® System Manager running on a virtual server	System Manager 7.0.1.2 Build No. - 7.0.0.0.16266 Software Update Revision No: 7.0.1.2.086007 Service Pack 2
Avaya Aura® Session Manager running on a virtual server	Session Manager R7.0 SP2 Build No. – 7.0.1.2.701230
Avaya Aura® Communication Manager running on a virtual server	R7.0.1 R017x.00.0.441.0 00.0.441.0-23523
Avaya Media Server running on a virtual server	Media Server SYSTEM R7.7.0.21 Media Server R7.7.0.350
Avaya Aura® Messaging running on a virtual server	R7.0.0.0.441
Avaya 9608 H323 Deskphone	Release 6.6.028
Avaya 9608 SIP Deskphone	Release 7.0.0.39
Avaya 9508 Digital Phone	V2.0
Capita DS3000 Solution Kit (DSX Converged Versions 2017 R1 and later) - Aculab Dual Redundant SIP Server	Release 33x Series V6.6.4

## 5. Configure Avaya Aura® Communication Manager

It is assumed that a fully functioning Communication Manager is in place with the necessary licensing and with SIP trunks in place, to Session Manager. The configuration and verification operations illustrated in this section were all performed using Communication Manager System Administration Terminal (SAT). The information provided in this section describes the configuration of Communication Manager for this solution. For all other provisioning information such as initial installation and configuration, please refer to the product documentation in **Section 10**.

The configuration operations described in this section can be summarized as follows:

- Verify System Parameters Customer Options.
- System Features and Access Codes.
- Administer Dial Plan.
- Administer Route Selection for DS3000 calls.
- Configure SIP Trunk.

**Note:** The configuration of PSTN trunks and routes are outside the scope of these Application Notes.

### 5.1. Verify System Parameters Customer Options

The license file installed on the system controls these attributes. If a required feature is not enabled or there is insufficient capacity, contact an authorized Avaya sales representative. Use the **display system-parameters customer-options** command to determine these values. On **Page 2**, verify that **Maximum Administered SIP Trunks** has sufficient capacity. Each call that receives IVR treatment from Communications Portal uses a minimum of one SIP trunk. Calls that are routed back to stations commissioned on Communication Manager, or calls that are routed back to Communication Manager to access the PSTN, use 2 SIP trunks.

display system-parameters customer-options		Page	2 of 11
OPTIONAL FEATURES			
IP PORT CAPACITIES	USED		
Maximum Administered H.323 Trunks:	12000	250	
Maximum Concurrently Registered IP Stations:	18000	2	
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	
<b>Maximum Administered SIP Trunks:</b>	<b>24000</b>	<b>319</b>	
Maximum Administered Ad-hoc Video Conferencing Ports:	24000	0	

On **Page 3**, ensure that both **ARS** and **ARS/AAR Partitioning** are set to **y**.

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

On **Page 5**, ensure that **Uniform Dialing Plan** is set to **y**.

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



## 5.2. System Features and Access Codes

For the testing, **Trunk-to Trunk Transfer** was set to **all** on **page 1** of the **system-parameters features** page. This is a system wide setting that allows calls to be routed from one trunk to another and is usually turned off to help prevent toll fraud. An alternative to enabling this feature on a system wide basis is to control it using COR (Class of Restriction). See **Section 10** for supporting documentation.

```
display system-parameters features                                     Page 1 of 19
      FEATURE-RELATED SYSTEM PARAMETERS
      Self Station Display Enabled? n
      Trunk-to-Trunk Transfer: all
      Automatic Callback with Called Party Queuing? n
      Automatic Callback - No Answer Timeout Interval (rings): 3
      Call Park Timeout Interval (minutes): 10
      Off-Premises Tone Detect Timeout Interval (seconds): 20
      AAR/ARS Dial Tone Required? y

      Music (or Silence) on Transferred Trunk Calls? no
      DID/Tie/ISDN/SIP Intercept Treatment: attd
      Internal Auto-Answer of AttD-Extended/Transferred Calls: transferred
      Automatic Circuit Assurance (ACA) Enabled? n

      Abbreviated Dial Programming by Assigned Lists? n
      Auto Abbreviated/Delayed Transition Interval (rings): 2
      Protocol for Caller ID Analog Terminals: Bellcore
      Display Calling Number for Room to Room Caller ID Calls? n
```

Use the **display feature-access-codes** command to verify that a FAC (feature access code) has been defined for both AAR and ARS. Note that **8** is used for AAR and **9** for ARS routing.

```
display 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:
      Answer Back Access Code:
      Attendant Access Code:
      Auto Alternate Routing (AAR) Access Code: 8
      Auto Route Selection (ARS) - Access Code 1: 9      Access Code 2:
      Automatic Callback Activation: *25      Deactivation: #25
```

### 5.3. Administer Dial Plan

It was decided for compliance testing that all calls beginning with 500xx with a total length of 5 digits were to be sent across the SIP trunk to the DS3000 via Session Manager. In order to achieve this, automatic alternate routing (aar) would be used to route the calls. The dial plan and aar routing analysis need to be changed to allow this.

Type **change dialplan analysis** in order to make changes to the dial plan. Ensure that **5** is added with a **Total Length** of **5** and a **Call Type** of **udp**.

change dialplan analysis			Page 1 of 12		
			DIAL PLAN ANALYSIS TABLE		
			Location: all		
			Percent Full: 2		
Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type
2	4	ext			
3	4	ext			
4	4	udp			
<b>5</b>	<b>5</b>	<b>udp</b>			
6	4	ext			
9	1	fac			
*	3	fac			
#	3	fac			

### 5.4. Administer Route Selection for Communications Portal Calls

As digits **5** were defined in the dial plan as udp (**Section 5.3**) use the **change uniform-dialplan** command to configure the routing of the dialed digits. In the example below calls to numbers beginning with **500xx** that are **5** digits in length will be matched. No further digits are deleted or inserted. Calls are sent to **aar** for further processing.

change uniform-dialplan 5			Page 1 of 2		
			UNIFORM DIAL PLAN TABLE		
			Percent Full: 0		
Matching Pattern	Len Del	Insert Digits	Net Conv	Node Num	
500	5 0		aar n	n	

Use the **change aar analysis x** command to further configure the routing of the dialed digits. Calls to Communications Portal begin with **500xx** and are matched with the AAR entry shown below. Calls are sent to **Route Pattern 1**, which contains the outbound SIP Trunk Group.

change aar analysis 5			Page 1 of 2		
			AAR DIGIT ANALYSIS TABLE		
			Location: all		
			Percent Full: 1		
Dialed String	Total Min Max	Route Pattern	Call Type	Node Num	ANI Req'd
500	5 5	<b>1</b>	unku		n

Use the **change route-pattern *n*** command to add the SIP trunk group to the route pattern that AAR selects. In this configuration, **Route Pattern Number 1** is used to route calls to trunk group (**Grp No**) **1**, this is the SIP Trunk configured in **Section 5.5**.

change route-pattern 1											Page 1 of 3			
Pattern Number: 1    Pattern Name: SIPTRK														
SCCAN? n    Secure SIP? n														
Grp	FRL	NPA	Pfx	Hop	Toll	No.	Inserted					DCS/	IXC	
No				Mrk	Lmt	List	Del	Digits					QSIG	
											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	unre				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		
6:	y	y	y	y	y	n	n	rest				none		

## 5.5. Configure SIP Trunk

In the Node Names IP form, note the IP Address of the **procr** and the Session Manager (**SM70vmpg**). The host names will be used throughout the other configuration screens of Communication Manager and Session Manager. Type **display node-names ip** to show all the necessary node names.

display node-names ip		Page 1 of 2
IP NODE NAMES		
Name	IP Address	
AES63VMPG	10.10.40.30	
PGDECT	10.10.40.50	
SM70vmpg	10.10.40.12	
default	0.0.0.0	
<b>procr</b>	10.10.40.31	
procr6	::	

In the **IP Network Region** form, the **Authoritative Domain** field is configured to match the domain name configured on Session Manager in **Section 6.1**. In this configuration, the domain name is **devconnect.local**. The **IP Network Region** form also specifies the **IP Codec Set** to be used. This codec set will be used for calls routed over the SIP trunk to Session manager as **ip-network region 1** is specified in the SIP signaling group.

display ip-network-region 1		Page 1 of 20
IP NETWORK REGION		
Region: 1		
Location: 1	<b>Authoritative Domain: devconnect.local</b>	
Name: Default region		
MEDIA PARAMETERS	Intra-region IP-IP Direct Audio: yes	
<b>Codec Set: 1</b>	Inter-region IP-IP Direct Audio: yes	
UDP Port Min: 2048	IP Audio Hairpinning? n	
UDP Port Max: 3329		
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		

In the **IP Codec Set** form, select the audio codec's supported for calls routed over the SIP trunk to Communications Portal. The form is accessed via the **change ip-codec-set n** command. Note that IP codec set 1 was specified in IP Network Region 1 shown above. Multiple codecs may be specified in the **IP Codec Set** form in order of preference; the example below includes **G.729**, **G.711MU** (mu-law) and **G.711A** (a-law), which are supported by Communications Portal.

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:	<b>G.729</b>	<b>n</b>	<b>2</b>	<b>20</b>
2:	<b>G.711MU</b>	<b>n</b>	<b>2</b>	<b>20</b>
3:	<b>G.711A</b>	<b>n</b>	<b>2</b>	<b>20</b>
4:				
5:				

Prior to configuring a SIP trunk group for communication with Session Manager, a SIP signaling group must be configured. Configure the Signaling Group form shown below as follows:

- Set the **Group Type** field to **sip**.
- Set the **Transport Method** to the desired transport method, for compliance testing this was set to **tcp**.
- The **Peer Detection Enabled** field should be set to **y** allowing the Communication Manager to automatically detect if the peer server is a Session Manager.
- Specify the node names for the procr and the Session Manager node name as the two ends of the signaling group in the **Near-end Node Name** field and the **Far-end Node Name** field, respectively. These values are taken from the **IP Node Names** form shown above.
- Set the **Near-end Node Name** to **procr**. This value is taken from the **IP Node Names** form shown above.
- Set the **Far-end Node Name** to the node name defined for the Session Manager (node name **SM70vmpg**), as per **Section 5.5**.
- Ensure that the recommended TCP port value of **5060** is configured in the **Near-end Listen Port** and the **Far-end Listen Port** fields.
- In the **Far-end Network Region** field, enter the IP Network Region configured above. This field logically establishes the **far-end** for calls using this signaling group as network region 1.
- Leave the **Far-end Domain** field blank to allow Communication Manager to accept any domain.
- The **Direct IP-IP Audio Connections** field is set to **y**.
- The **Initial IP-IP Direct Media** field is set to **y**.
- The default values for the other fields may be used.

**Note:** Compliance testing was carried out with the **Initial IP-IP Direct Media** field set to both **y** and to **n**. This was to allow testing for shuffling both on and off.

change signaling-group 1		Page 1 of 2
SIGNALING GROUP		
<b>Group Number:</b> 1	<b>Group Type:</b> sip	
IMS Enabled? n	<b>Transport Method:</b> tcp	
Q-SIP? n		
IP Video? n	Enforce SIPS URI for SRTP? y	
<b>Peer Detection Enabled?</b> y	<b>Peer Server:</b> SM	
<b>Near-end Node Name:</b> procr	<b>Far-end Node Name:</b> SM70vmpg	
<b>Near-end Listen Port:</b> 5060	<b>Far-end Listen Port:</b> 5060	
	<b>Far-end Network Region:</b> 1	
<b>Far-end Domain:</b>		
Incoming Dialog Loopbacks: eliminate	Bypass If IP Threshold Exceeded? n	
<b>DTMF over IP:</b> rtp-payload	RFC 3389 Comfort Noise? n	
Session Establishment Timer(min): 3	<b>Direct IP-IP Audio Connections?</b> y	
Enable Layer 3 Test? y	IP Audio Hairpinning? n	
H.323 Station Outgoing Direct Media? n	<b>Initial IP-IP Direct Media?</b> y	
	Alternate Route Timer(sec): 6	

Configure the **Trunk Group** form as shown below. This trunk group is used for calls to and from Communications Portal. Enter a descriptive name in the **Group Name** field. Set the **Group Type** field to **sip**. Enter a **TAC** code compatible with the Communication Manager dial plan. Set the **Service Type** field to **public-ntwrk**. 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. Accept the default values for the remaining fields.

change trunk-group 1		Page 1 of 21	
TRUNK GROUP			
Group Number: 1	<b>Group Type: sip</b>	CDR Reports: y	
<b>Group Name: SIP TRK</b>	COR: 1	TN: 1	<b>TAC: *11</b>
Direction: two-way	Outgoing Display? y	Night Service:	
Dial Access? n			
Queue Length: 0			
<b>Service Type: public-ntwrk</b>	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 Presence to prevent unnecessary SIP messages during call setup. Session refresh is used throughout the duration of the call, to check the other side has not gone away, for the compliance test a value of **1800** was used.

change 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		
	<b>Preferred Minimum Session Refresh Interval(sec): 1800</b>		
Disconnect Supervision - In? y Out? y			
XOIP Treatment: auto Delay Call Setup When Accessed Via IGAR? N			

Settings on **Page 3** can be left as shown below.

change trunk-group 1	Page 3 of 21
TRUNK FEATURES	
ACA Assignment? n	Measured: none
	Maintenance Tests? y
Numbering Format: private	UI Treatment: shared
	Replace Restricted Numbers? n
	Replace Unavailable Numbers? n
Modify Tandem Calling Number: no	
Show ANSWERED BY on Display? y	

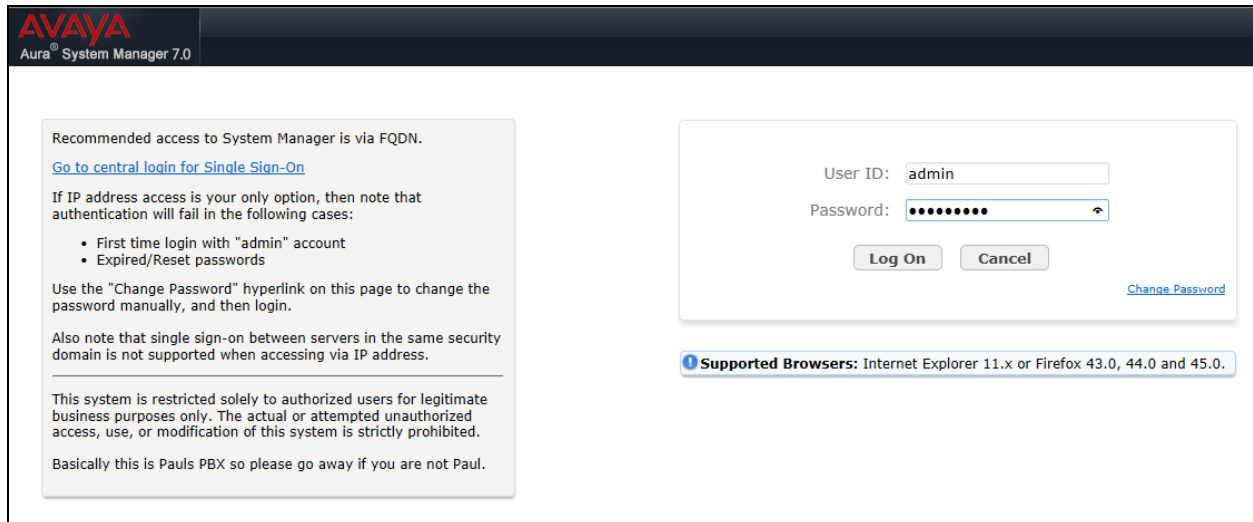
Settings on **Page 5** are as follows. Please note that an issue was observed with ‘Transfer’ see **Section 2.2**. When a Communication Manager SIP phone is transferring DS3000 to DS3000 the transfer fails for both Supervised and Blind transfer. The DS3000 does not seem to be handling the REFER messages from the Communication Manager correctly and to stop sending REFER messages setting “Network Call Redirection” to “N” on the Communication Manager Trunk Group seemed to solve this issue. Please note that the testing was carried out with **Network Call Redirection** set to y.

change trunk-group 1	Page 5 of 22
PROTOCOL VARIATIONS	
Mark Users as Phone? y	
Prepend '+' to Calling/Alerting/Diverting/Connected Number? n	
Send Transferring Party Information? y	
<b>Network Call Redirection? y</b>	
Build Refer-To URI of REFER From Contact For NCR? n	
Send Diversion Header? y	
Support Request History? y	
Telephone Event Payload Type: 101	
Convert 180 to 183 for Early Media? n	
Always Use re-INVITE for Display Updates? n	
Identity for Calling Party Display: P-Asserted-Identity	
Block Sending Calling Party Location in INVITE? n	
Accept Redirect to Blank User Destination? n	
Enable Q-SIP? n	
Interworking of ISDN Clearing with In-Band Tones: keep-channel-active	
Request URI Contents: may-have-extra-digits	



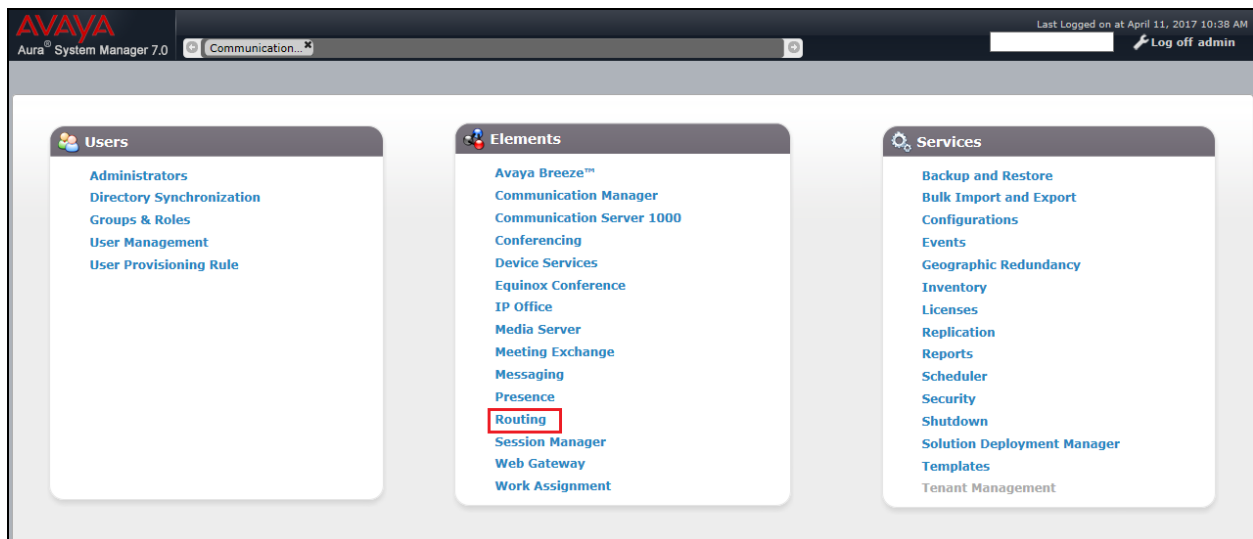
## 6. Configure Avaya Aura® Session Manager

In order to make changes in Session Manager a web session is established to System Manager. Log into System Manager by opening a web browser and navigating to <http://<System Manager IP Address>/SMGR>. Enter the appropriate credentials for the **User ID** and **Password** and click on **Log On** highlighted below.



The screenshot shows the Avaya Aura System Manager 7.0 login interface. On the left, a text box provides instructions: "Recommended access to System Manager is via FQDN. Go to central login for Single Sign-On. If IP address access is your only option, then note that authentication will fail in the following cases: First time login with 'admin' account, Expired/Reset passwords. Use the 'Change Password' hyperlink on this page to change the password manually, and then login. Also note that single sign-on between servers in the same security domain is not supported when accessing via IP address. This system is restricted solely to authorized users for legitimate business purposes only. The actual or attempted unauthorized access, use, or modification of this system is strictly prohibited. Basically this is Pauls PBX so please go away if you are not Paul." On the right, a login form contains fields for "User ID" (with "admin" entered) and "Password" (masked with dots), and "Log On" and "Cancel" buttons. A "Change Password" link is also present. At the bottom, a banner states "Supported Browsers: Internet Explorer 11.x or Firefox 43.0, 44.0 and 45.0."

Once logged in click on **Routing** highlighted below.

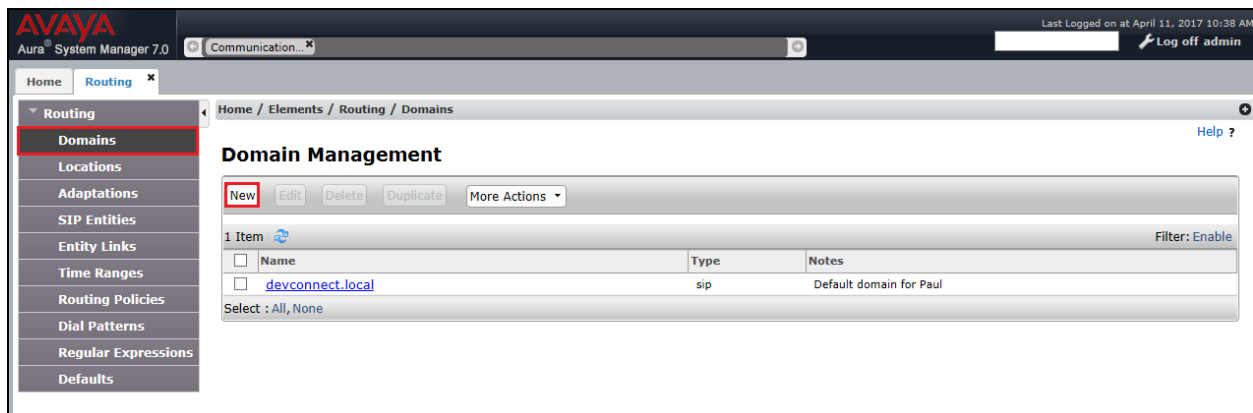


## 6.1. Domains and Locations

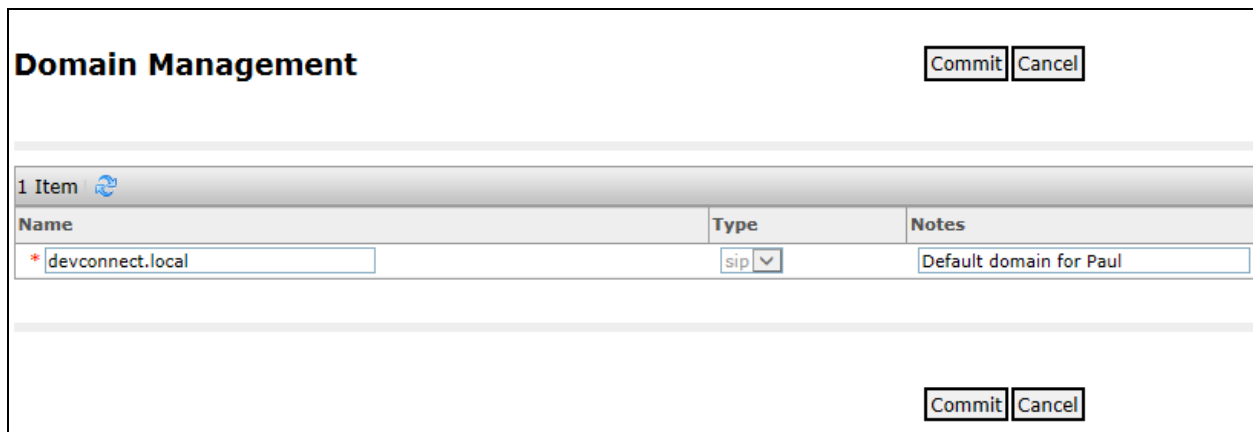
**Note:** It is assumed that a domain and a location have already been setup, therefore a quick overview of the domain and location that was used in compliance testing is only provided here.

### 6.1.1. Add a new Domain

If a domain is not already in place then click on **New** as is highlighted below.

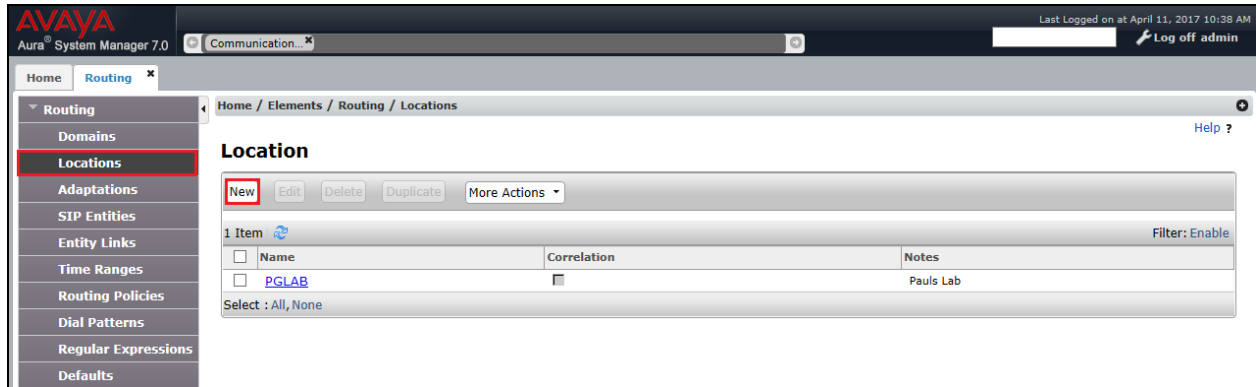


Enter the domain **Name**, note this will be the same as that domain configured in **Section 5.5**, and ensure the **Type** is set to **SIP**. Click on **Commit** once done.




### 6.1.2. Add a new Location

If a location is not already in place then one must be added to include the IP address range of the Avaya solution. Click on **New** as is highlighted below to add a new location.



The screenshot displays the Avaya Aura System Manager 7.0 interface. The left sidebar shows the navigation menu with 'Locations' highlighted. The main content area is titled 'Location' and shows a table with one item, 'PGLAB'. The 'New' button in the top action bar is highlighted.

Name	Correlation	Notes
<input type="checkbox"/> PGLAB		Pauls Lab

Select : All, None

Enter a suitable **Name** and add the IP address ranges at the bottom of the screen under **Location Pattern** and click on **Commit** once this is done.

### Location Details Commit Cancel

#### General

**\* Name:**

**Notes:**

#### Dial Plan Transparency in Survivable Mode

**Enabled:** ☐

**Listed Directory Number:**

**Associated CM SIP Entity:**

#### Overall Managed Bandwidth

**Managed Bandwidth Units:**

**Total Bandwidth:**

**Multimedia Bandwidth:**

**Audio Calls Can Take Multimedia Bandwidth:** ☒

#### Per-Call Bandwidth Parameters

**Maximum Multimedia Bandwidth (Intra-Location):**  **Kbit/Sec**

**Maximum Multimedia Bandwidth (Inter-Location):**  **Kbit/Sec**

**\* Minimum Multimedia Bandwidth:**  **Kbit/Sec**

**\* Default Audio Bandwidth:**

#### Alarm Threshold

**Overall Alarm Threshold:**  %

**Multimedia Alarm Threshold:**  %

**\* Latency before Overall Alarm Trigger:**  **Minutes**

**\* Latency before Multimedia Alarm Trigger:**  **Minutes**

#### Location Pattern

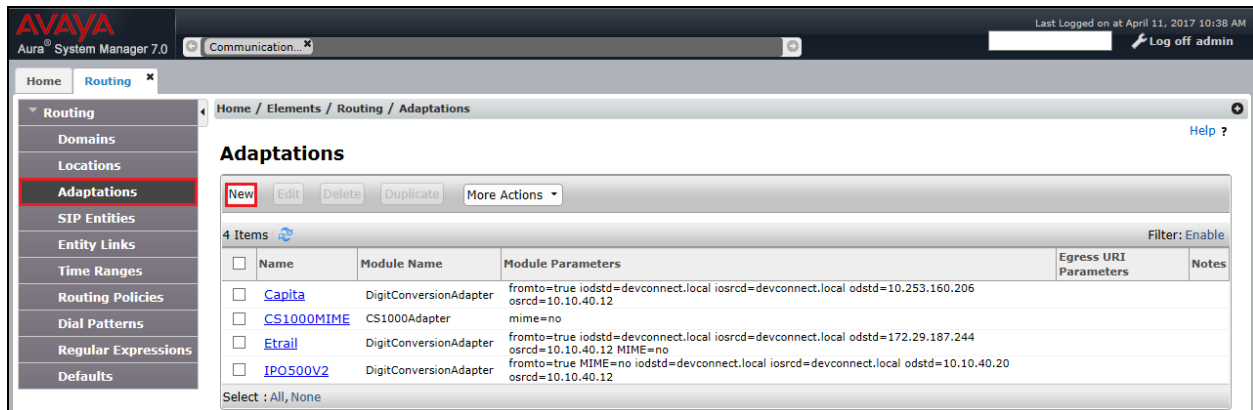
2 Items

	IP Address Pattern	Notes
<input type="checkbox"/>	* 10.10.40.*	Pauls subnet
<input type="checkbox"/>	* 10.253.160.* <span style="float: right;">x</span>	subnet

Select : All, None

## 6.2. Creating an Adaptation for the DS3000

An adaptation can allow the altering of SIP Message. An adaptation is created to convert domain names to IP addresses. Select **Adaptations** from the left window and click on **New** in the main window.



Enter a suitable **Adaptation Name**, select **DigitConversionAdapter** for the **Module Name**. The **Module Parameter Type** should be set to **Name-Value Parameter**. Add the following module parameters:

- **Fromto**            **true**
- **Iodstd**           **devconnect.local**
- **Iosrcd**           **devconnect.local**

The screenshot shows the 'Adaptation Details' form. The 'General' tab is active. The form contains the following fields:

- Adaptation Name:** Capita
- Module Name:** DigitConversionAdapter
- Module Parameter Type:** Name-Value Parameter

Below these fields is a table for adding parameters:

Name	Value
fromto	true
iodstd	devconnect.local
iosrcd	devconnect.local

At the bottom of the form are fields for 'Egress URI Parameters' and 'Notes'.

Add the following module parameters:

- **odstd=10.253.144.206**
- **osrcd=10.10.40.34**

In this example 10.253.160.206 is the DS3000 SIP Gateway and 10.10.40.12 is the Session Manager SM100 IP Address, these IP addresses may need to be changed to suit accordingly. **devconnect.local** is the domain name as per **Section 7.1**. Click on **Commit** once completed

**Adaptation Details**

CommitCancel

General

\* Adaptation Name: Capita

\* Module Name: DigitConversionAdapter

Module Parameter Type: Name-Value Parameter

AddRemove

<input type="checkbox"/>	Name	Value
<input type="checkbox"/>	odstd	10.253.160.206
<input type="checkbox"/>	osrcd	10.10.40.12

Select : All, NonePage 2 of 2

Egress URI Parameters:

Notes:

### 6.3. Adding DS3000 as a SIP Entity

Click on **SIP Entities** in the left column and select **New** in the right window.

The screenshot shows the Avaya Aura System Manager 7.0 interface. The left navigation pane has 'SIP Entities' highlighted. The main pane shows the 'SIP Entities' list with 19 items. The 'New' button is highlighted in the top toolbar.

Name	FQDN or IP Address	Type	Notes
aacc64SIPvmg	10.10.40.55	SIP Trunk	
AACC70vmg	10.10.40.80	SIP Trunk	AACC70vmg
ASBCE_PG	10.10.40.151	SIP Trunk	Session Boarder Controller
Capita	10.253.160.206	SIP Trunk	Capita
cm63vmg	10.10.40.31	CM	R6.3 CM
CM70Redundancy	10.10.40.165	CM	
cm70vmg	10.10.40.13	CM	
CPE	10.10.40.251	SIP Trunk	For Stephen Wilson
CS1000E	10.10.40.111	Other	CS1KPG1

Enter a suitable **Name** for the new SIP Entity and the **IP Address** of the DS3000, which is the floating IP address of the DS3000 SIP Server. Enter the correct **Time Zone** and **Location** and click on **Commit**.

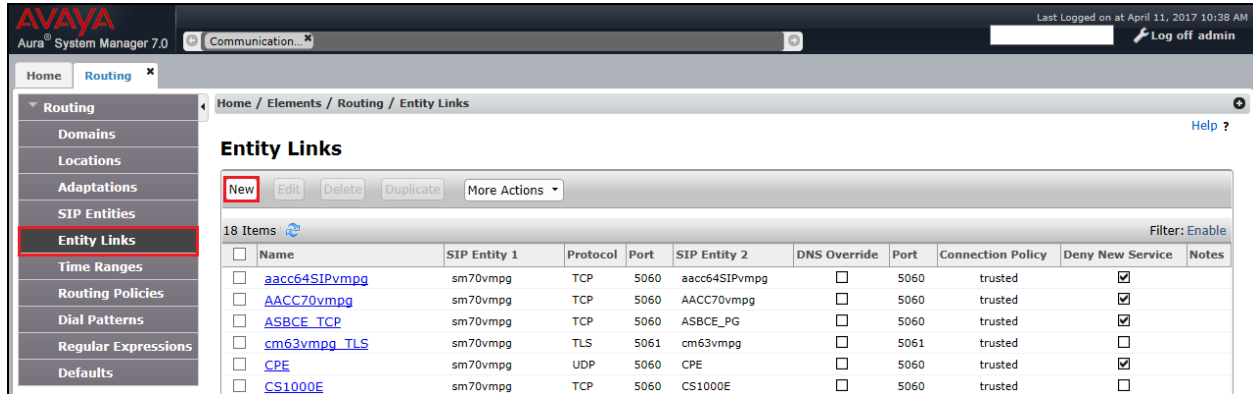
The screenshot shows the 'SIP Entity Details' form. The 'General' tab is selected. The form contains the following fields:

- Name:** Capita
- FQDN or IP Address:** 10.253.160.206
- Type:** SIP Trunk
- Notes:** Capita
- Adaptation:** Capita
- Location:** PGLAB
- Time Zone:** Europe/Dublin
- SIP Timer B/F (in seconds):** 4
- Credential name:**
- Securable:** ☐
- Call Detail Recording:** egress

Buttons: Commit, Cancel

## 6.4. Adding the DS3000 Entity Link

A UDP Entity links was added for the DS3000. Click on **Entity Links** in the left column and select **New** in the main window.

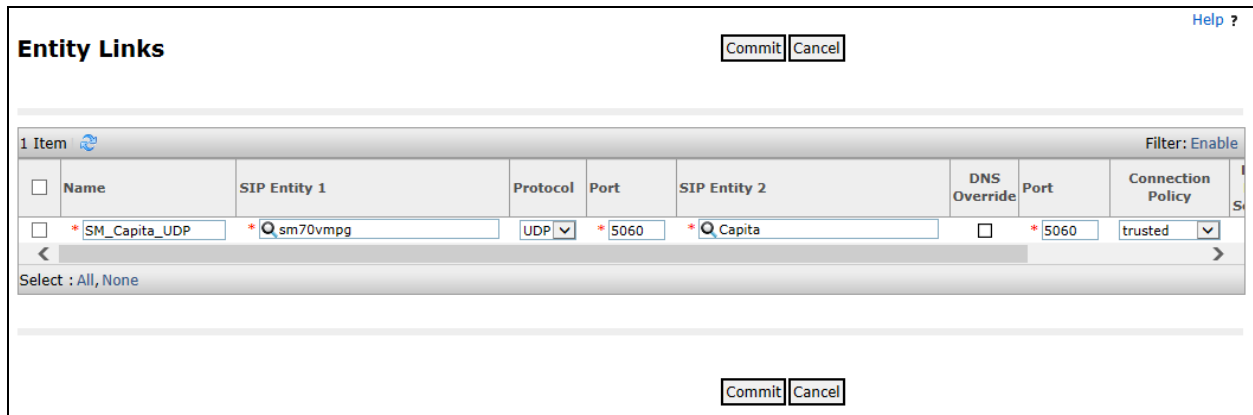


Entity Links

18 Items

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	DNS Override	Port	Connection Policy	Deny New Service	Notes
<a href="#">aacc64SIPvmg</a>	sm70vmg	TCP	5060	aacc64SIPvmg	<input type="checkbox"/>	5060	trusted	<input checked="" type="checkbox"/>	
<a href="#">AACC70vmg</a>	sm70vmg	TCP	5060	AACC70vmg	<input type="checkbox"/>	5060	trusted	<input checked="" type="checkbox"/>	
<a href="#">ASBCE_TCP</a>	sm70vmg	TCP	5060	ASBCE_PG	<input type="checkbox"/>	5060	trusted	<input checked="" type="checkbox"/>	
<a href="#">cm63vmg_TLS</a>	sm70vmg	TLS	5061	cm63vmg	<input type="checkbox"/>	5061	trusted	<input type="checkbox"/>	
<a href="#">CPE</a>	sm70vmg	UDP	5060	CPE	<input type="checkbox"/>	5060	trusted	<input checked="" type="checkbox"/>	
<a href="#">CS1000E</a>	sm70vmg	TCP	5060	CS1000E	<input type="checkbox"/>	5060	trusted	<input type="checkbox"/>	

Enter a suitable **Name** for the Entity Link and select the **Session Manager** SIP Entity for **SIP Entity 1** and the newly created DS3000 Entity called **Capita** for **SIP Entity 2**. Ensure that **UDP** is selected for the **Protocol** and that **Port 5060** is used. Click on **Commit** once finished to save the new Entity Link.



Entity Links

Commit Cancel

1 Item

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	DNS Override	Port	Connection Policy
* SM_Capita_UDP	* sm70vmg	UDP	* 5060	* Capita	<input type="checkbox"/>	* 5060	trusted

Select : All, None

Commit Cancel



## 6.5. Adding the DS3000 Routing Policy

Click on **Routing Policies** in the left window and select **New** in the main window.

The screenshot shows the Avaya Aura System Manager 7.0 interface. The left sidebar has a menu with 'Routing Policies' highlighted. The main window displays the 'Routing Policies' page with a 'New' button highlighted in red. Below the buttons is a table with 15 items. The table has columns: Name, Disabled, Retries, Destination, and Notes. The 'Name' column contains links to various policies, and the 'Destination' column contains their respective destinations.

Name	Disabled	Retries	Destination	Notes
<a href="#">To_aacc64SIPvmg</a>	<input type="checkbox"/>	0	aacc64SIPvmg	aacc64SIPvmg
<a href="#">To_AACC70vmg</a>	<input type="checkbox"/>	0	AACC70vmg	To_AACC70vmg
<a href="#">To ASBCE</a>	<input type="checkbox"/>	0	ASBCE_PG	Calls to ASBCE
<a href="#">To Capita</a>	<input type="checkbox"/>	0	Capita	To Capita
<a href="#">To_cm63vmg</a>	<input type="checkbox"/>	0	cm63vmg	Routing to CM63
<a href="#">To_CM70_Redundancy</a>	<input type="checkbox"/>	0	CM70Redundancy	To CM70 Redundancy
<a href="#">To_cm70vmg</a>	<input type="checkbox"/>	0	cm70vmg	
<a href="#">To_CPE</a>	<input type="checkbox"/>	0	CPE	For Stephen
<a href="#">To_CS1000E</a>	<input type="checkbox"/>	0	CS1000E	Routing to CS1KPG1

Enter a suitable **Name** for the Routing Policy and click on **Select** under **SIP Entity as Destination**, highlighted below.

The screenshot shows the 'Routing Policy Details' form. The 'General' section has fields for 'Name' (To\_Capita), 'Disabled' (checkbox), 'Retries' (0), and 'Notes' (To Capita). The 'SIP Entity as Destination' section has a 'Select' button highlighted in red. Below the button is a table with columns: Name, FQDN or IP Address, Type, and Notes.

Name	FQDN or IP Address	Type	Notes
------	--------------------	------	-------

Select the **Capita** SIP Entity as shown below and click on **Select**.

**SIP Entities**Help ?

Select Cancel

**SIP Entities**

19 Items Filter: Enable

	Name	FQDN or IP Address	Type	Notes
<input type="radio"/>	aacc64SIPvmg	10.10.40.55	SIP Trunk	
<input type="radio"/>	AACC70vmg	10.10.40.80	SIP Trunk	AACC70vmg
<input type="radio"/>	ASBCE_PG	10.10.40.151	SIP Trunk	Session Boarder Controller
<input checked="" type="radio"/>	Capita	10.253.160.206	SIP Trunk	Capita
<input type="radio"/>	cm63vmg	10.10.40.31	CM	R6.3 CM
<input type="radio"/>	CM70Redundancy	10.10.40.165	CM	
<input type="radio"/>	cm70vmg	10.10.40.13	CM	
<input type="radio"/>	CPE	10.10.40.251	SIP Trunk	For Stephen Wilson
<input type="radio"/>	CS1000E	10.10.40.111	Other	CS1KPG1
<input type="radio"/>	EnghouseCP	10.10.40.106	SIP Trunk	EnghouseCP
<input type="radio"/>	EP-POM	10.10.40.135	Voice Portal	EP POM Server

The selected destination is now shown, click on **Commit** to save this.

**Routing Policy Details**Help ?

Commit Cancel

**General**

\* Name:

Disabled: ☐

\* Retries:

Notes:

**SIP Entity as Destination**

Select

Name	FQDN or IP Address	Type	Notes
Capita	10.253.160.206	SIP Trunk	Capita

## 6.6. Adding a Dial Pattern for the DS3000

Select **Dial Patterns** in the left window and select **New** in the main window.

The screenshot shows the Avaya Aura System Manager 7.0 interface. The left sidebar has a 'Routing' section with 'Dial Patterns' highlighted. The main window displays the 'Dial Patterns' page with a 'New' button and a table of 17 items. The table has columns: Pattern, Min, Max, Emergency Call, Emergency Type, Emergency Priority, SIP Domain, and Notes. The table lists various dial patterns and their associated settings.

Pattern	Min	Max	Emergency Call	Emergency Type	Emergency Priority	SIP Domain	Notes
10	4	4	<input type="checkbox"/>			devconnect.local	Ext 10xx on CM63vmpg
2016	4	4	<input type="checkbox"/>			devconnect.local	SIP Trunk to CM63
3	4	4	<input type="checkbox"/>			devconnect.local	To CS1000E
40	4	4	<input type="checkbox"/>			devconnect.local	Calls to SIP exts in CS1000
450	4	4	<input type="checkbox"/>			devconnect.local	To Capita
49	4	4	<input type="checkbox"/>			devconnect.local	To NovaLink 10.10.40.44
51	4	4	<input type="checkbox"/>			devconnect.local	To Etrali
52	4	4	<input type="checkbox"/>			devconnect.local	Was goign to IP Office 500 V2 Now CM70vmpg
5999	4	4	<input type="checkbox"/>			devconnect.local	Messaging (Voicemail)

Enter the required digits for the Pattern, in the example below 5000x is used, which means that 50000 – 50009 will use the Routing Policy that will be selected. **5000** is entered as the **Pattern** and the **Min** and **Max** digit length of **5** is used thus giving 5000x. Ensure that the correct domain is entered for **SIP Domain** in this example the domain created in **Section 7.1** is added. Click on **Add** under **Originating Locations and Routing Policies** in order to select this Routing Policy.

The screenshot shows the 'Dial Pattern Details' form. The 'General' section contains fields for Pattern (5000), Min (5), Max (5), Emergency Call, Emergency Priority (1), Emergency Type, SIP Domain (devconnect.local), and Notes. The 'Originating Locations and Routing Policies' section shows an 'Add' button and a table with 0 items.

**Dial Pattern Details**

**General**

\* Pattern: 5000

\* Min: 5

\* Max: 5

Emergency Call: ☐

Emergency Priority: 1

Emergency Type:

SIP Domain: devconnect.local

Notes:

**Originating Locations and Routing Policies**

Add Remove

0 Items

Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
---------------------------	----------------------------	---------------------	------	-------------------------	----------------------------	----------------------

Select the Originating Location, this will be the location added in **Section 7.1** select the newly created routing policy for the DS3000 created in **Section 7.5** for **Routing Policies**.

**Originating Location**
Select Cancel

---

**Originating Location**

☐ Apply The Selected Routing Policies to All Originating Locations

1 Item
Filter: Enable

<input checked="" type="checkbox"/>	Name	Notes
<input checked="" type="checkbox"/>	PGLAB	Pauls Lab

Select : All, None

---

**Routing Policies**

15 Items
Filter: Enable

<input type="checkbox"/>	Name	Disabled	Destination	Notes
<input type="checkbox"/>	To_aacc64SIPvmg	<input type="checkbox"/>	aacc64SIPvmg	aacc64SIPvmg
<input type="checkbox"/>	To_AACC70vmg	<input type="checkbox"/>	AACC70vmg	To_AACC70vmg
<input type="checkbox"/>	To ASBCE	<input type="checkbox"/>	ASBCE_PG	Calls to ASBCE
<input checked="" type="checkbox"/>	To_Capita	<input type="checkbox"/>	Capita	To Capita
<input type="checkbox"/>	To_cm63vmg	<input type="checkbox"/>	cm63vmg	Routing to CM63
<input type="checkbox"/>	To CM70 Redundancy	<input type="checkbox"/>	CM70Redundancy	To CM70 Redundancy
<input type="checkbox"/>	To_cm70vmg	<input type="checkbox"/>	cm70vmg	

With the Routing Policy selected click on **Commit** to finish adding the **Dial Pattern**.

**Dial Pattern Details**
Commit Cancel
Help ?

---

**General**

\* Pattern: 5000  
\* Min: 5  
\* Max: 5  
Emergency Call: ☐  
Emergency Priority: 1  
Emergency Type:  
SIP Domain: devconnect.local  
Notes:

---

**Originating Locations and Routing Policies**

Add Remove

1 Item
Filter: Enable

<input type="checkbox"/>	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	PGLAB	Pauls Lab	To_Capita	0	<input type="checkbox"/>	Capita	To Capita

Select : All, None

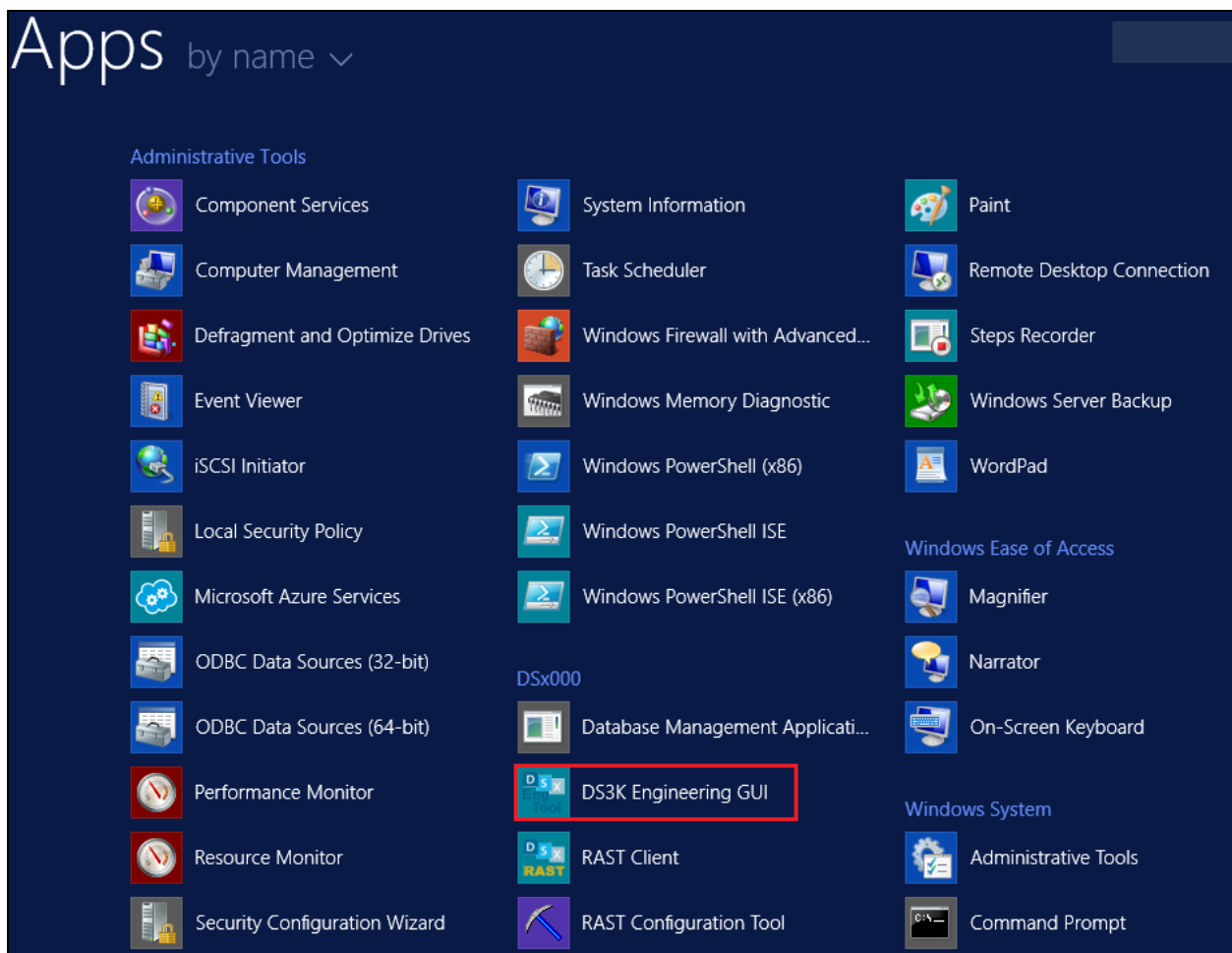
## 7. Configure Capita DS3000 Application

The following sections describe the steps required to configure the DS3000 application in order to connect successfully with Session Manager using SIP trunks.

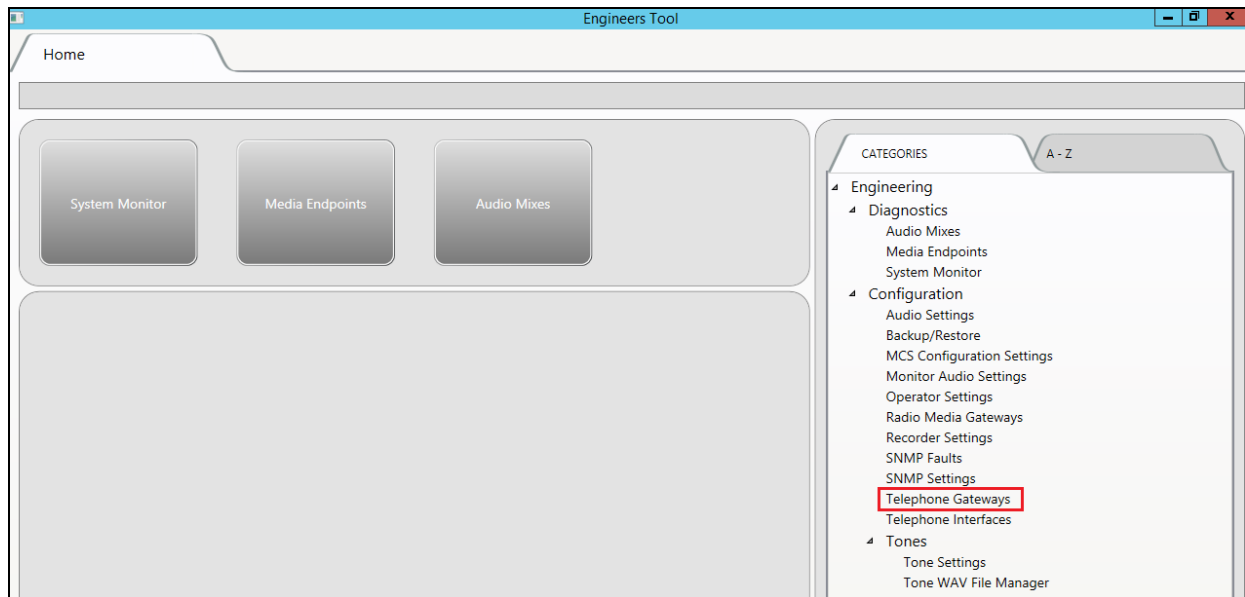
### 7.1. Configure DS3000 connection to Session Manager

The configuration for the connection to Session Manager is performed on the DS3000 SIP Server called RG5FCS.

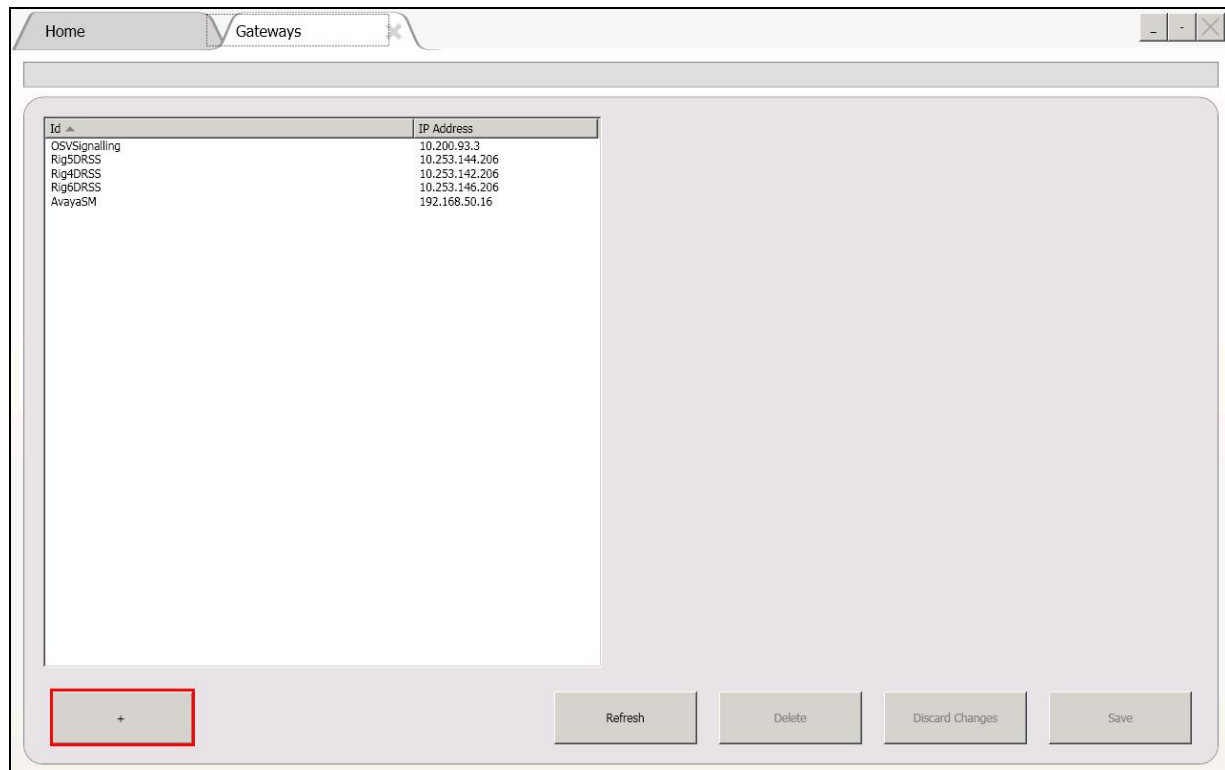
Log into **DS3K Engineering GUI** by clicking on the icon highlighted below on the DS3000 SIP Server.



Once logged in the following screen appears. Select **Telephone Gateways** in the right column, highlighted below.



The **Gateways** tab is opened. Select the + icon at the bottom left of the screen.



Fill in the **Gateway Id** and **Address** information. This will be the IP address of the Session Manager.

The screenshot shows the 'Gateways' tab in the Avaya Session Manager configuration interface. It features a table with two columns: 'Id' and 'IP Address'. The 'AvayaSessionMan' entry is highlighted. To the right of the table, there are input fields for 'Gateway Id' and 'Address'.

Id	IP Address
RG6TMG01	10.253.146.111
RG6TMG02	10.253.146.113
RG6TMG03	10.253.146.115
AudioCodes	10.253.146.235
AudioCodes8FXO	10.253.146.236
Callvision	10.253.146.233
RG4DRSS	10.253.142.206
AudioCodesM1000	10.253.146.110
Asterisk	10.253.100.99
AACC6	10.12.17.14
SIPP	10.253.146.206
RG6CME	10.253.146.230
AudioCodesM2000	10.253.160.125
<b>AvayaSessionMan</b>	<b>10.10.40.12</b>
AvayaIpOffice	10.10.40.20

Gateway Id: AvayaSessionMan

Address: 10.10.40.12

Click on the **Home** tab and select **Telephone Interfaces** in the right column as highlighted below.

The screenshot shows the 'Home' tab in the Avaya Session Manager configuration interface. On the left, there are three buttons: 'System Monitor', 'Media Endpoints', and 'Audio Mixes'. On the right, there is a 'CATEGORIES' sidebar with a tree view. The 'Telephone Interfaces' item under the 'Configuration' category is highlighted with a red box.

System Monitor Media Endpoints Audio Mixes

CATEGORIES A - Z

- Engineering
  - Diagnostics
    - Audio Mixes
    - Media Endpoints
    - System Monitor
  - Configuration
    - Audio Settings
    - Backup/Restore
    - MCS Configuration Settings
    - Monitor Audio Settings
    - Operator Settings
    - Radio Media Gateways
    - Recorder Settings
    - SNMP Faults
    - SNMP Settings
    - Telephone Gateways
    - Telephone Interfaces**
  - Tones
    - Tone Settings
    - Tone WAV File Manager

The **Telephone Interfaces** tab is opened. Select the + icon at the bottom left of the screen to add a new Telephone interface.

Id	Gateway	Interface Number	Type	Group	Start Line	No of Lines	Card Number
Avaya5M	Avaya5M	2	SIP		31	30	N/A
OSV5IP	OSV5signalling	1	SIP		1	30	N/A
RG4	Rig4DRSS	3	SIP		61	10	N/A
RG6	Rig6DRSS	4	SIP		71	10	N/A

All the information in the right column must be filled in. The screen below shows the information used during compliance testing. Click on **Save** at the bottom right of the screen once all the information has been entered correctly. Set the **Operator ringing tone generation** to **generate only when there is no early media**, this will provide ringtone when there is no early media on the PBX.

Id	Gateway	Interface Number	Type	Group	Start Line	No of Lines	Card Number
Asterisk Dir	Asterisk	8	SIP		181	30	N/A
TI 06-02 FXO	AudioCodes8FXO	2	Analog	06	403	4	6
TI 06-01 FXO	AudioCodes8FXO	1	Analog	06	399	4	5
TMG03 Analogue	AudioCodesM1000	3	Analog	04	391	4	4
AACCAgent	AudioCodesM2000	5	DPNSS	03	1	30	N/A
<b>Avaya</b>	<b>AvayaSessionMan</b>	<b>3</b>	<b>SIP</b>		<b>91</b>	<b>30</b>	<b>3</b>
Centricity	Callvision	7	SIP		211	30	N/A
Rig4	RG4DRSS	4	SIP		121	10	N/A
TMG04	RG6CME	2	SIP		61	30	N/A
TMG01	RG6TMG01	0	DPNSS	01	151	30	4
TMG02	RG6TMG02	1	DPNSS	02	31	30	N/A
TMG03 ISDN	RG6TMG03	4	ISDN	05	395	4	4
RG6SIP	SIPP	9	SIP		241	30	N/A

Telephone Interface Id: Avaya

Gateway: AvayaSessionMan

Interface Number: 3

Type: SIP

Group:

Start Line Number: 91

Number of Lines: 30

Operator ringing tone generation: Generate only when there is no early media

Monitor Interface: ☒

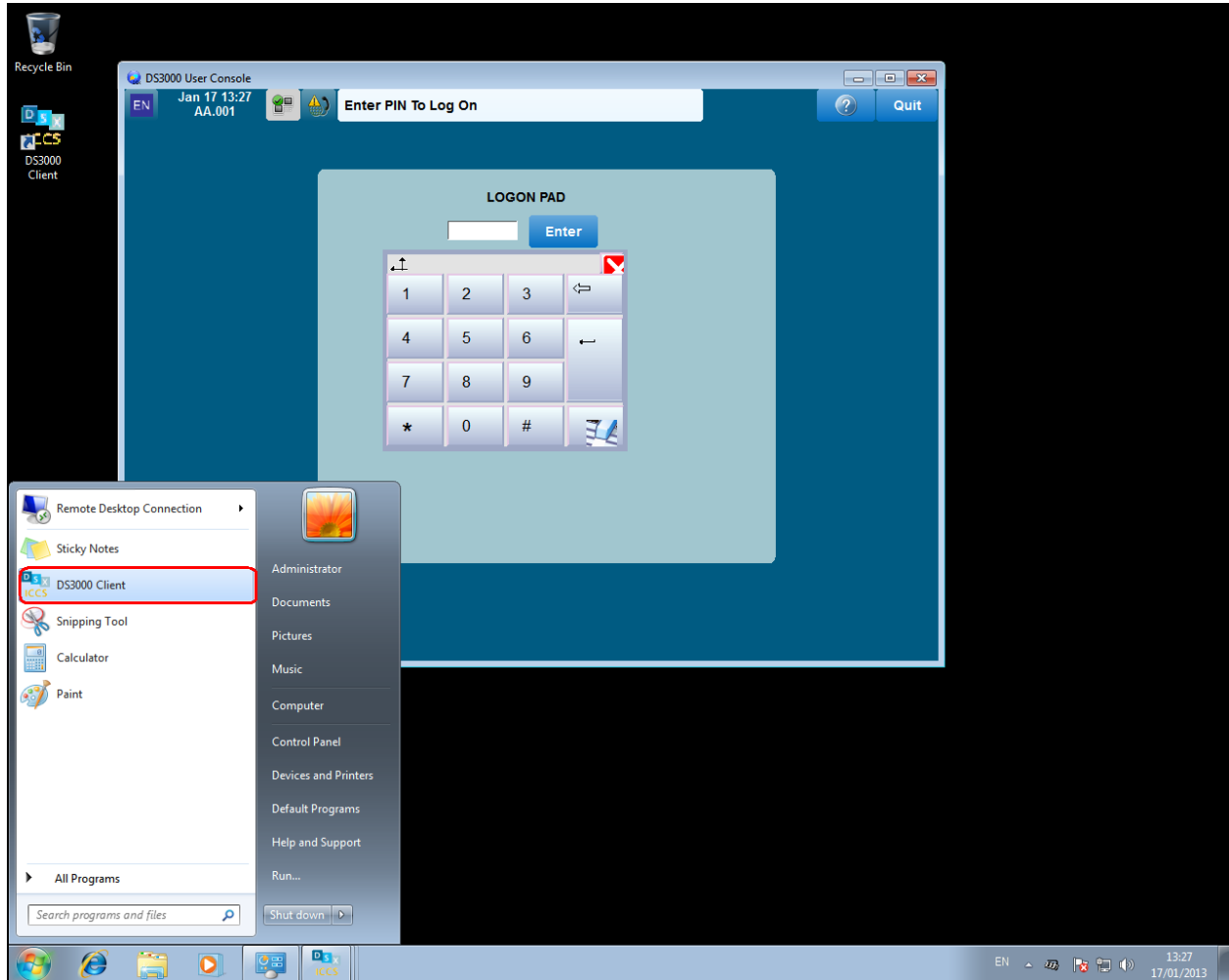
GSIC Number for error reporting: 3

Inter Site: ☐

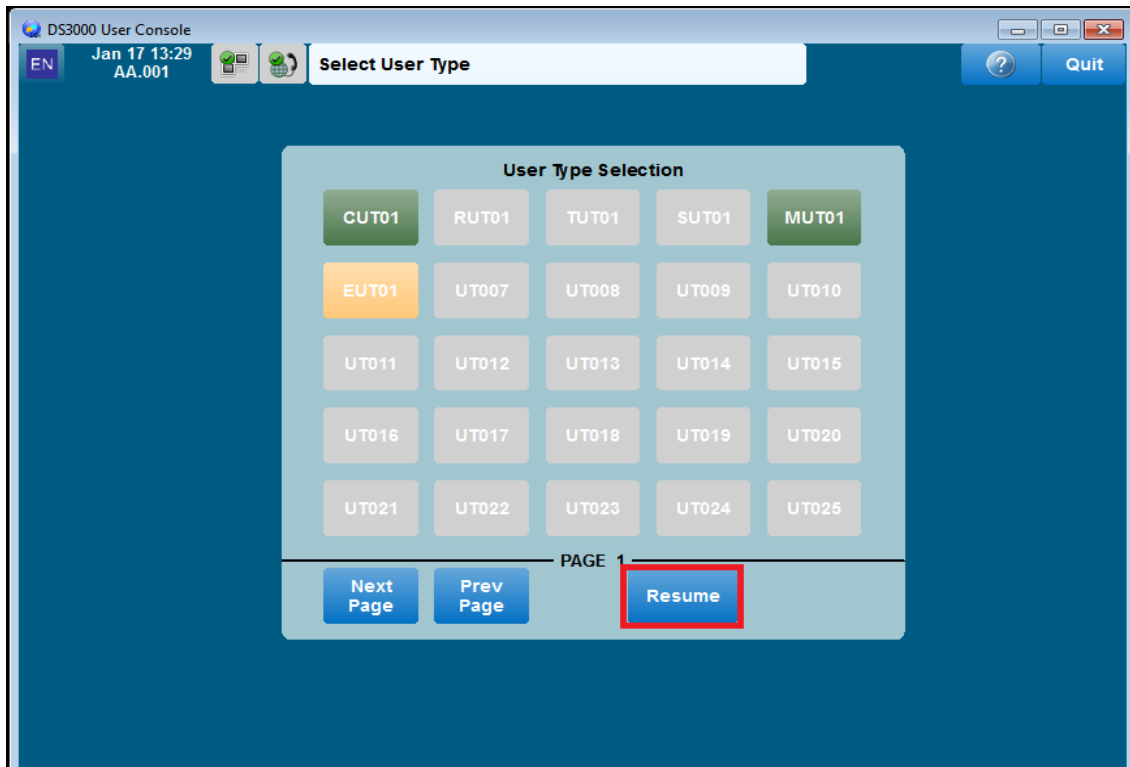


## 7.2. Configure DS3000 extension numbers

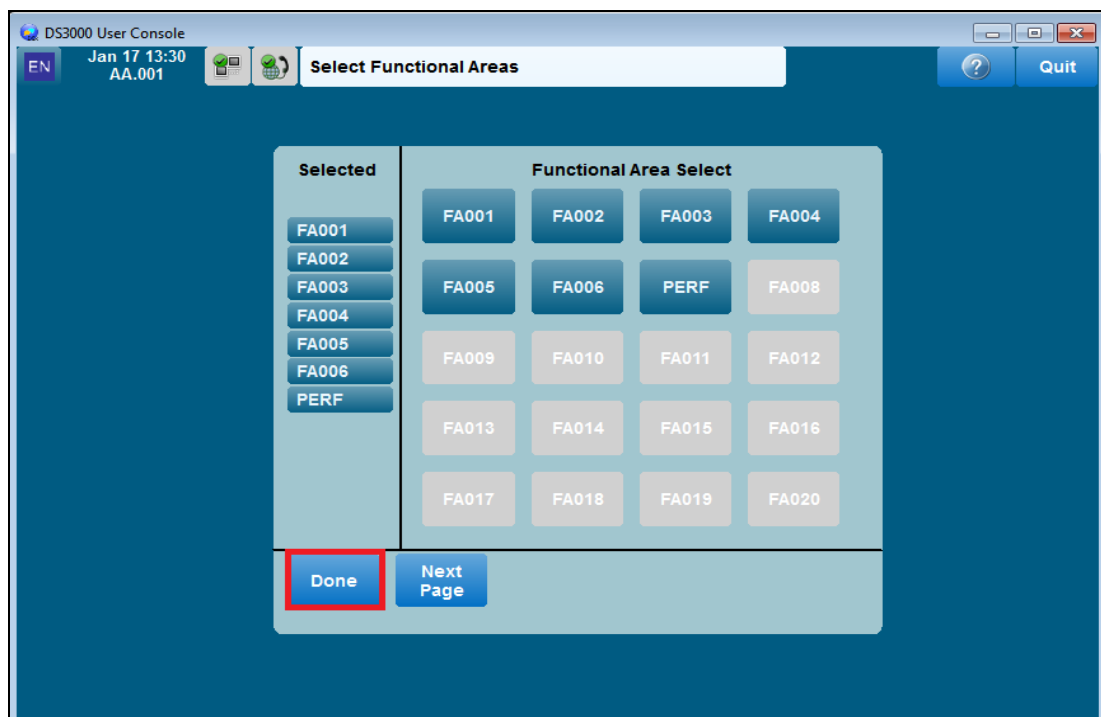
Open the **DS3000 Client** on the DS3000 Client machine. Enter the correct credentials on the **LOGON PAD**.



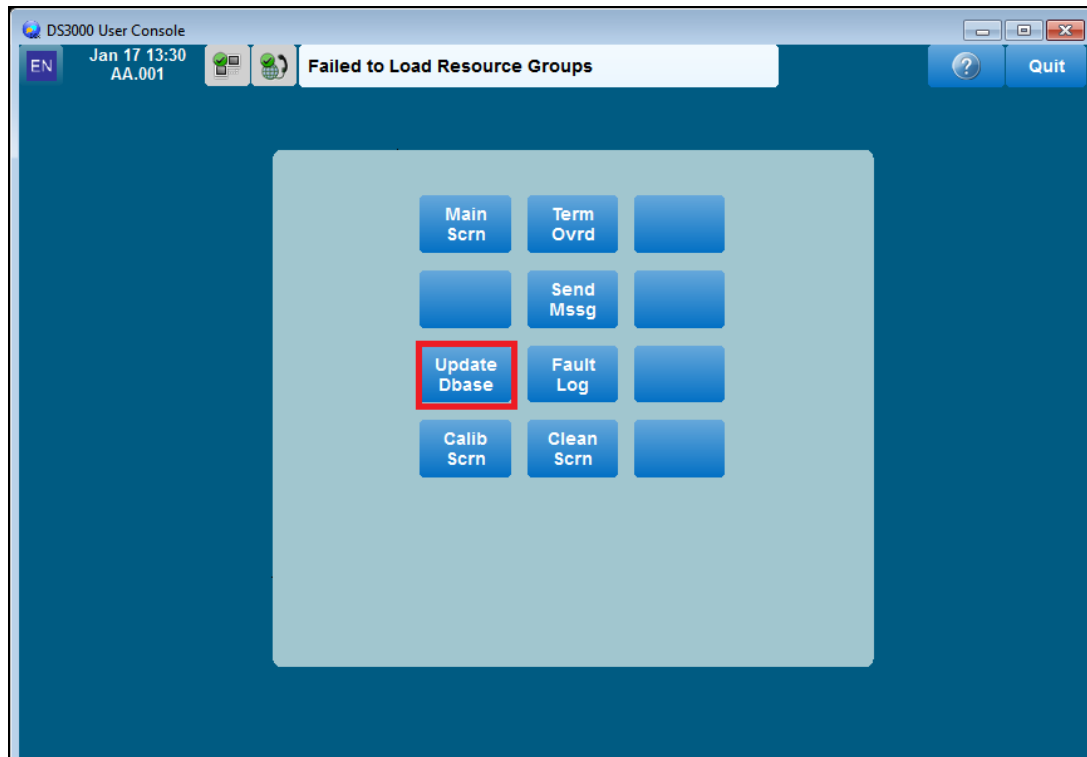
Click on **Resume** at the bottom of the screen as highlighted.



Select **Done** at the bottom of the screen as highlighted.



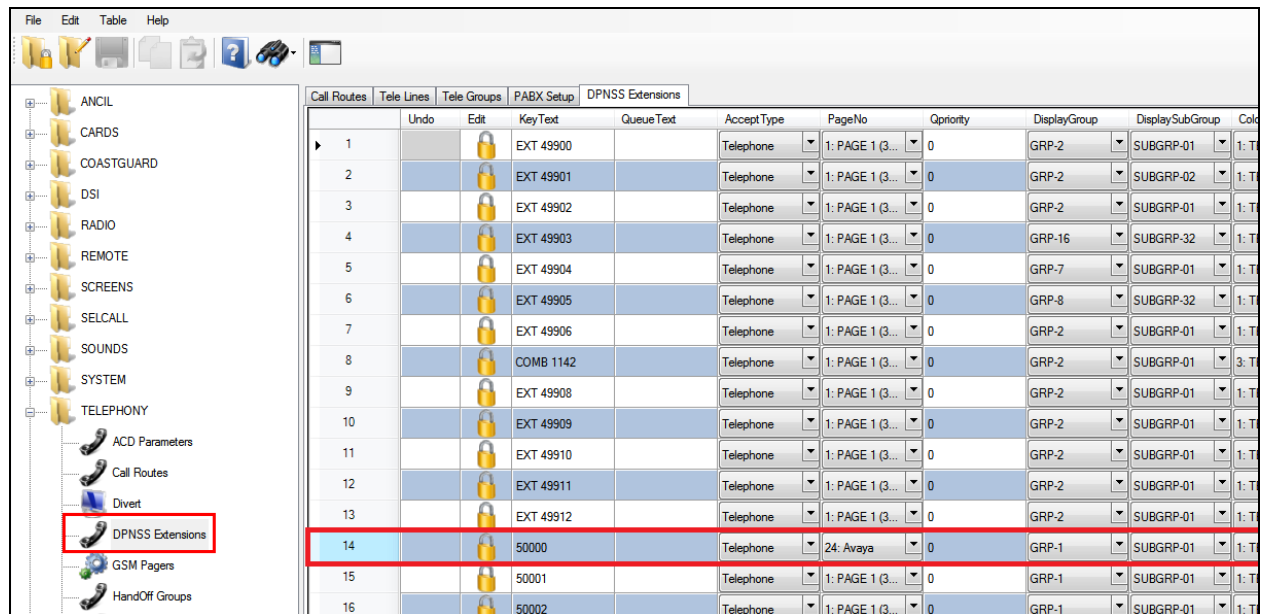
Click on the **UpdateDbase** button highlighted.



Click on the **Call Routes** icon highlighted in the left window. The highlighted row in the right window shows that when 3xxx is dialed, Interface 2 is used. Note: The interface numbers are as defined by the configuration entered in **Section 7.1**.

Call Routes											
	Undo	Edit	DigitsCompare	Leng	Digits	InsertLength	RoutingDigits	GSIC(0)	GSIC(1)	GSIC(2)	GS
1			1	0	0			255	255	255	255
2			1	1	0			0	255	255	255
3			1	2	0			0	255	255	255
4			1	3	0			6	255	255	255
5			1	4	0			1	255	255	255
6			1	5	0			1	255	255	255
7			1	6	0			1	255	255	255
8			1	7	0			1	255	255	255
9			1	8	0			255	255	255	255
10			1	9	0			1	255	255	255
11			2	01	0			255	255	255	255
12			2	22	0			255	255	255	255
13			2	21	0			255	255	255	255
14			2	31	0			255	255	255	255
15			2	4444444	0			255	255	255	255
16			2	51	0			255	255	255	255

Select **DPNSS Extensions** in the left column highlighted. Note the entry highlighted is for DS3000 Extension **50000**. Ensure **Accept Type** is set to **Telephone**.



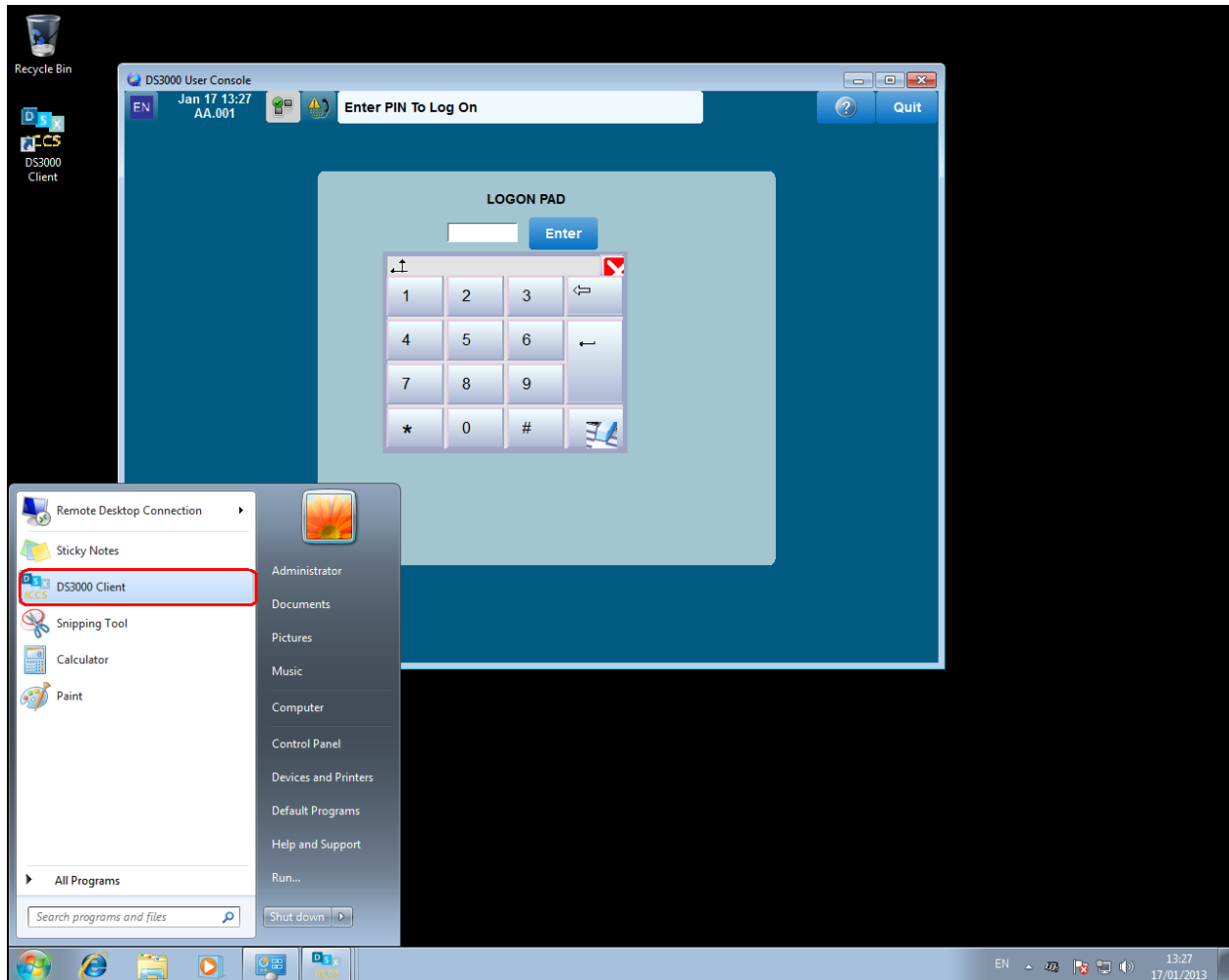
	Undo	Edit	KeyText	QueueText	Accept Type	PageNo	Priority	DisplayGroup	DisplaySubGroup	Col
1			EXT 49900		Telephone	1: PAGE 1 (3...	0	GRP-2	SUBGRP-01	1: T
2			EXT 49901		Telephone	1: PAGE 1 (3...	0	GRP-2	SUBGRP-02	1: T
3			EXT 49902		Telephone	1: PAGE 1 (3...	0	GRP-2	SUBGRP-01	1: T
4			EXT 49903		Telephone	1: PAGE 1 (3...	0	GRP-16	SUBGRP-32	1: T
5			EXT 49904		Telephone	1: PAGE 1 (3...	0	GRP-7	SUBGRP-01	1: T
6			EXT 49905		Telephone	1: PAGE 1 (3...	0	GRP-8	SUBGRP-32	1: T
7			EXT 49906		Telephone	1: PAGE 1 (3...	0	GRP-2	SUBGRP-01	1: T
8			COMB 1142		Telephone	1: PAGE 1 (3...	0	GRP-2	SUBGRP-01	3: T
9			EXT 49908		Telephone	1: PAGE 1 (3...	0	GRP-2	SUBGRP-01	1: T
10			EXT 49909		Telephone	1: PAGE 1 (3...	0	GRP-2	SUBGRP-01	1: T
11			EXT 49910		Telephone	1: PAGE 1 (3...	0	GRP-2	SUBGRP-01	1: T
12			EXT 49911		Telephone	1: PAGE 1 (3...	0	GRP-2	SUBGRP-01	1: T
13			EXT 49912		Telephone	1: PAGE 1 (3...	0	GRP-2	SUBGRP-01	1: T
14			50000		Telephone	24: Avaya	0	GRP-1	SUBGRP-01	1: T
15			50001		Telephone	1: PAGE 1 (3...	0	GRP-1	SUBGRP-01	1: T
16			50002		Telephone	1: PAGE 1 (3...	0	GRP-1	SUBGRP-01	1: T

## 8. Verification Steps

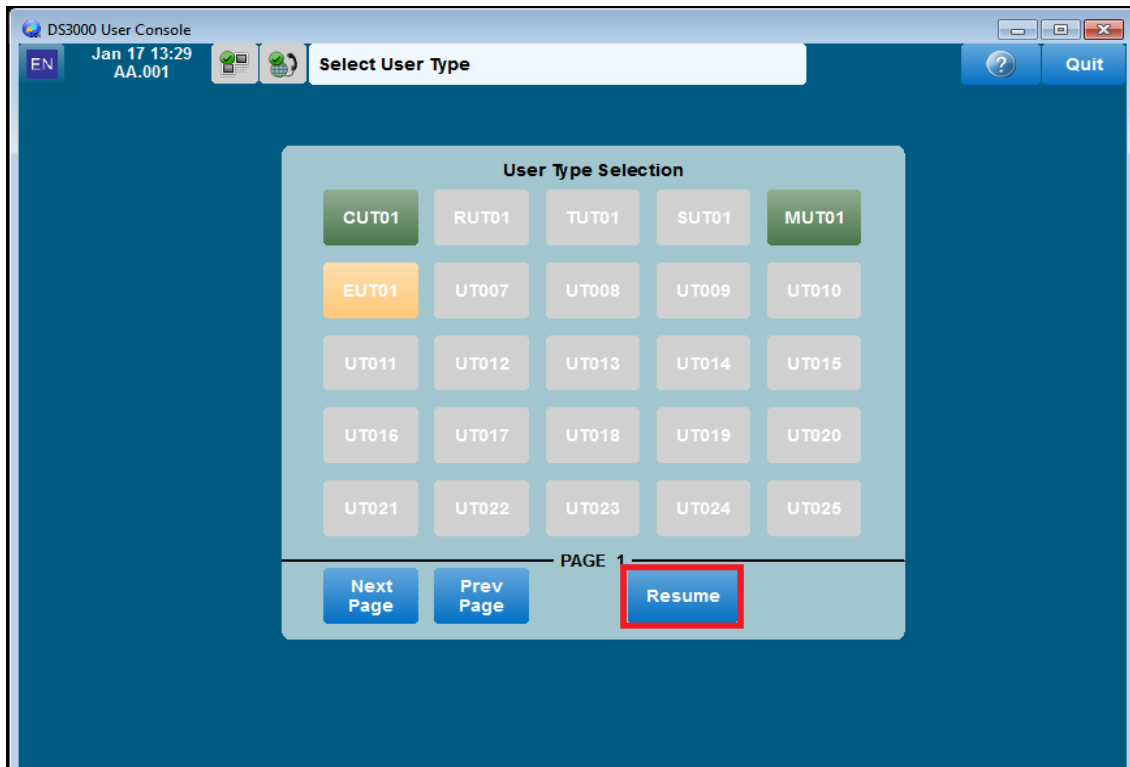
The following steps can be taken to ensure that all connections between Capita's DS3000 Solution and the Avaya solution is configured correctly.

### 8.1. Verify that calls can be made to DS3000

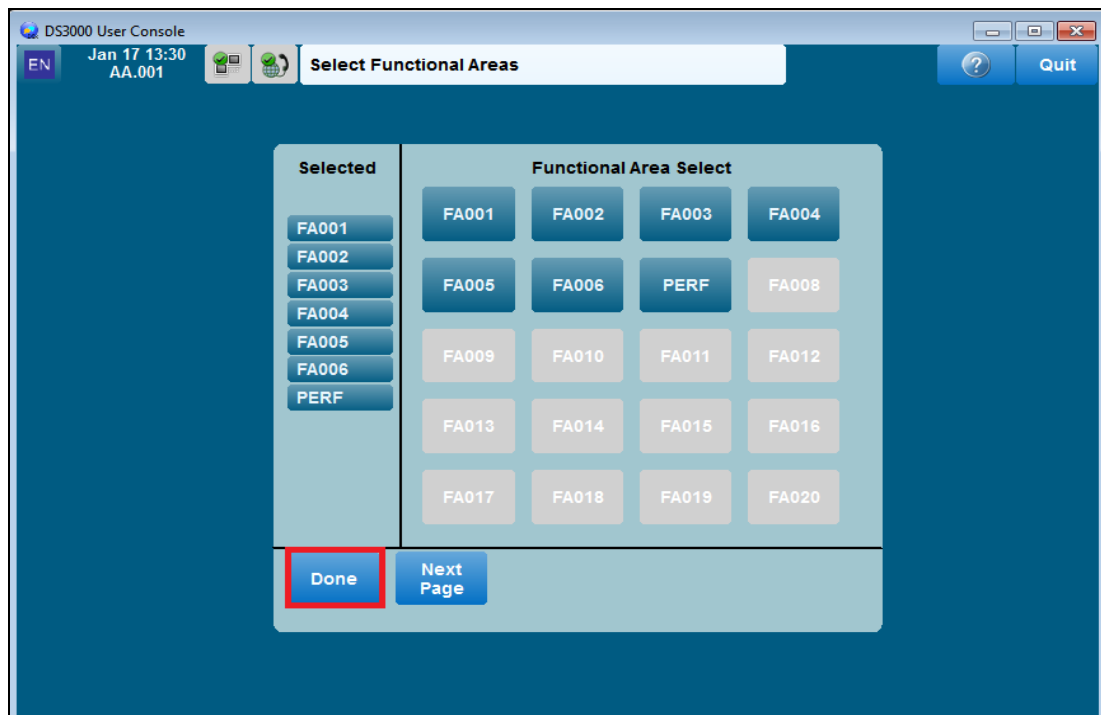
Open the **DS3000 Client** on the DS3000 Client machine. Enter the correct credentials on the **LOGON PAD**.



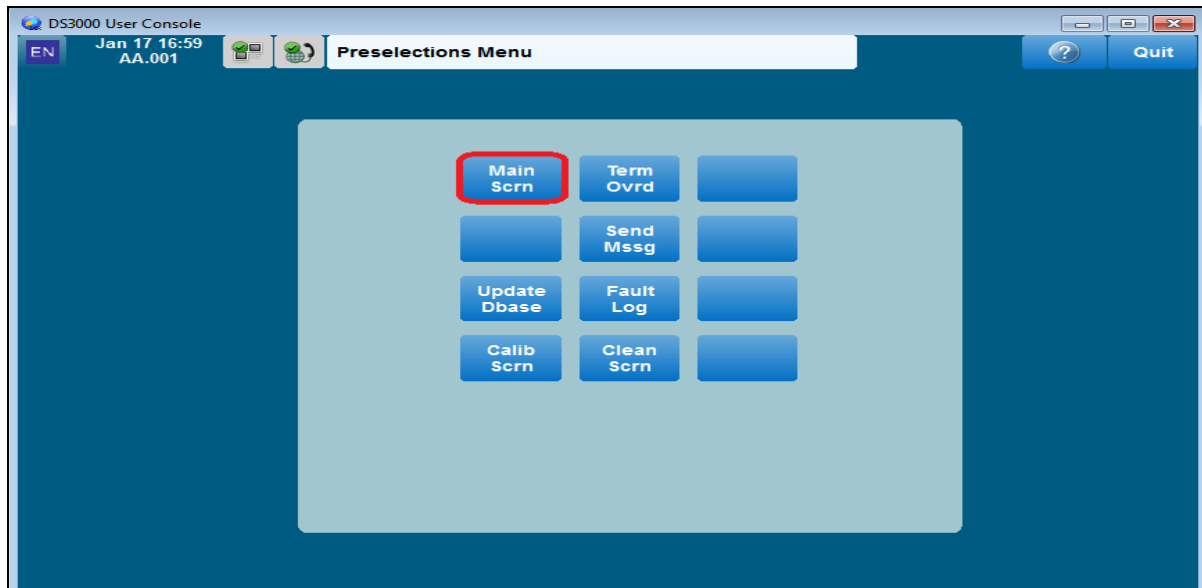
Click on **Resume** at the bottom of the screen as highlight.



Select **Done** at the bottom of the screen as highlighted.



Click on the **Main Scrn** button highlighted below.



Once a call is presented to DS3000, the following screen should appear. Click on the **Take Call** button on the bottom right of the screen to take the call.



## 9. Conclusion

These Application Notes describe the configuration steps required for DS3000 from Capita Secure Information Solutions to successfully interoperate with Avaya Aura® Communication Manager R7.0.1 and Avaya Aura® Session Manager R7.0.1. Please refer to **Section 2.2** for test results and observations.

## 10. Additional References

This section references documentation relevant to these Application Notes. The Avaya product documentation is available at <http://support.avaya.com>, where the following documents can be obtained.

- [1] *Administering Avaya Aura® Communication Manager*, Document ID 03-300509
- [2] *Avaya Aura® Communication Manager Feature Description and Implementation*, Document ID 555-245-205
- [3] *Administering Avaya Aura® Session Manager*, Release 7.0, 03-603324
- [4] *Application Notes for Configuring Capita Secure Information Solutions DS3000 with Avaya Aura® Session Manager R7.0.1 and Avaya Communication Server 1000E R7.6 using SIP Trunks*

Product documentation for DS3000 can be requested from Capita or may be downloaded from <http://www.capitasecureinformationsolutions.co.uk>



---

**©2017 Avaya Inc. All Rights Reserved.**

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

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