



Avaya Solution & Interoperability Test Lab

Application Notes for configuring Capita - Secure Solutions and Services Distinction Media Server R1.0 with Avaya Aura® Communication Manager R8.0.1 and Avaya Aura® Session Manager R8.0.1 and using SIP Trunks - Issue 1.0

Abstract

These Application Notes describe the configuration steps for provisioning Capita - Secure Solutions and Services Distinction Media Server to interoperate with Avaya Aura® Communication Manager R8.0.1 and Avaya Aura® Session Manager R8.0.1.

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 Distinction Media Server from Capita - Secure Solutions and Services to interoperate with Avaya Aura® Communication Manager R8.0.1 using Avaya Aura® Session Manager R8.0.1 to route SIP calls.

In this type of configuration, the Distinction Media Server has a SIP connection to Avaya Aura® Session Manager. The Distinction Media Server supports basic call control including hold, transfer and conference.

2. General Test Approach and Test Results

The interoperability compliance testing evaluates the ability of the Capita - Secure Solutions and Services (Capita) Distinction Media Server (DMS) to make and receive calls to and from Communication Manager endpoints. All calls destined for the DMS both locally and from the PSTN are routed to the DMS over SIP trunks using Session Manager to route the calls.

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

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

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

For the testing associated with these Application Notes, the interface between Session Manager and the DMS did not include use of any specific encryption features as requested by Capita.

2.1. Interoperability Compliance Testing

The interoperability compliance testing focuses on various technical testing scenarios to verify the usage of the DMS 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 the DMS extensions.

- **Calls to DMS extensions**– Ensure that calls can be made to the DMS extensions from Communication Manager extensions.
- **Calls to PSTN from DMS extensions** – Ensure that calls can be made from DMS to PSTN across the SIP trunk through Communication Manager.
- **Calls from PSTN into DMS extensions** – Ensure that calls can be made to DMS from the PSTN by calling into Communication Manager and across the SIP trunk to the DMS.
- **Hold/transfer and conference functionality**– Verify that calls can be placed on hold and transferred and conferenced.
- **Serviceability testing** – Verify the behaviour of DMS 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 to ensure shuffling is off. This will use a DSP resource on the Media Gateway or Media Server for the duration of the call.

- Direct IP-IP Audio Connections set to N, see **Section 5.5**, page 12.

2.2. Test Results

Most test cases passed except for the following issues observed.

- During the compliance test media shuffling was disabled, as shown in **Section 5.5**. This is a per Capita’s request as it was necessary to avoid issues found with media shuffling enabled. With shuffling enabled and a call was placed on hold and resumed the RTP did not re-establish.
- When a DMS phone has Call Forward No Answer set and either a CM extension or another DMS calls to it a “BYE” is sent out by the DMS when the call is forwarded to its CFNA number. This means that CFNA cannot be supported across the DMS system with Communication Manager. Capita are investigating the issue.
- The A-party was not updated after transfers. This may be due to an issue with the DMS picking incorrect contact information. Capita are investigating the issue.

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 DMS product can be obtained as follows.

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

3. Reference Configuration

Figure 1 shows the setup for compliance testing Capita’s DMS with Communication Manager and Session Manager using SIP signalling over a SIP trunk to pass calls between Communication Manager and the DMS extensions.

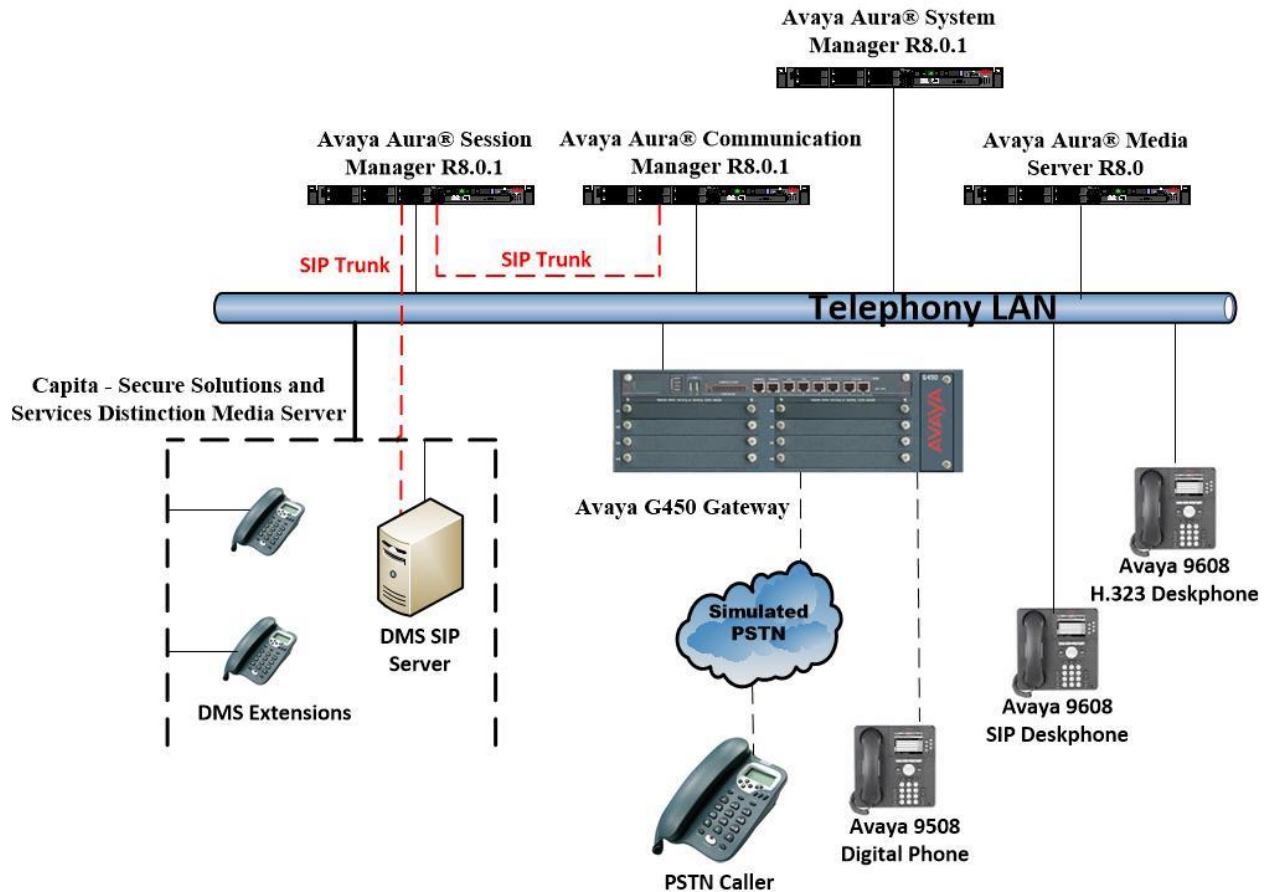


Figure 1: Connection of Capita - Secure Solutions and Services Distinction Media Server with Avaya Aura® Communication Manager R8.0.1 and Avaya Aura® Session Manager R8.0.1

4. Equipment and Software Validated

The following equipment and software were used for compliance testing.

Avaya Equipment	Software / Firmware Version
Avaya Aura® System Manager running on a virtual server	System Manager 8.0.1.1 Build No. – 8.0.0.0.931077 Software Update Revision No: 8.0.11.039340 Service Pack 1
Avaya Aura® Session Manager running on a virtual server	Session Manager R8.0.1 Build No. – 8.0.1.1.801103
Avaya Aura® Communication Manager running on a virtual server	R8.0.1.1.0 – FP1SP1 R018x.00.0.822.0 Update ID 00.0.822.0-25183
Avaya Media Gateway G450	40.20.0 /2
Avaya Aura® Media Server	Appliance Version R8.0.0.6 Media Server 8.0.0.150 Element Manager 8.0.0.150
Avaya 96x1 H323 Deskphone	6.6604
Avaya 96x1 SIP Deskphone	7.1.2.0.14
Avaya J179 H323 Deskphone	6.7.002U
Avaya J129 SIP Deskphone	1.0.0.0.0.43
Avaya Equinox running on Vantage	3.4.8.36
Avaya 9408 Digital Deskphone	V2.0
Capita Equipment	Software / Firmware Version
Capita Distinction Media Server (DMS)	Release 1.0.0.37

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 DMS 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 is answered by a DMS extension 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.

<code>display system-parameters customer-options</code>		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
	Maximum Administered SIP Trunks:	24000	319
	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                               Page 3 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
                                ARS? y                               Computer Telephony Adjunct Links? y
                                ARS/AAR Partitioning? y           Cvg Of Calls Redirected Off-net? y
    ARS/AAR Dialing without FAC? y                                    DCS (Basic)? y
```

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

```
display system-parameters customer-options                               Page 5 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
                                Uniform Dialing Plan? y
    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 7080xx with a total length of 6 digits were to be sent across the SIP trunk to the DMS 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 **7080** is added with a **Total Length** of **6** and a **Call Type** of **udp**.

```

change dialplan analysis                                     Page 1 of 12
                                DIAL PLAN ANALYSIS TABLE
                                Location: all               Percent Full: 2
  Dialed   Total   Call   Dialed   Total   Call   Dialed   Total   Call
  String   Length Type   String   Length Type   String   Length Type
  4         4     udp    4         4     udp    4         4     udp
  5         5     udp    5         5     udp    5         5     udp
  6         4     ext    6         4     ext    6         4     ext
  7         4     udp    7         4     udp    7         4     udp
  7080    6    udp  7080    6    udp  7080    6    udp
  9         1     fac    9         1     fac    9         1     fac
  *         3     fac    *         3     fac    *         3     fac
  
```

5.4. Administer Route Selection for calls to DMS

As digits **7080** 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 **7080xx** that are **6** 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   Len Del   Insert   Node
  Pattern    Len Del   Digits   Net Conv Num
  7080     6 0      aar    n
                                n
  
```


Use the **change aar analysis x** command to further configure the routing of the dialed digits. Calls to DMS begin with **7080xx** 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 7                                     Page 1 of 2
                AAR DIGIT ANALYSIS TABLE
                Location: all                            Percent Full: 1

```

Dialed String	Total Min	Total Max	Route Pattern	Call Type	Node Num	ANI Reqd
7080	6	6	1	aar		n

Use the **change route-pattern n** command to add the SIP trunk group to the route pattern that AAR selects. In this configuration, **Pattern Number 1** is used to route calls to trunk group (**Grp No**) **1**, this is the SIP Trunk configured in **Section 5.5**. Other settings such as **FRL** and **Numbering Format** can be seen below.

```

change route-pattern 1                                   Page 1 of 4
                Pattern Number: 1                       Pattern Name: SIPTrunk
                SCCAN? n      Secure SIP? n      Used for SIP stations? n

```

Grp No	FRL	NPA	Pfx	Hop	Toll	No.	Inserted	DCS/	IXC
			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	Sub	Numbering	LAR
	0 1 2 M 4 W		Request				Dgts		Format	
1:	y y y y y n n			unre					lev0-pvt	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

5.5. Configure SIP Trunk

In the Node Names IP form, note the IP Address of the **procr** and the Session Manager (**SM80vmpg**). 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
                                     IP NODE NAMES
      Name                          IP Address
AMS80vmpg                          10.10.40.61
G450                                10.10.40.14
IPOffice                            10.10.40.25
NRS                                  10.10.40.101
PGDECT                               10.10.40.50
SM80vmpg                          10.10.40.58
SM_Oceana                           10.10.41.26
aes80vmpg                           10.10.40.56
default                             0.0.0.0
procr                              10.10.40.59

( 16 of 18 administered node-names were displayed )
Use 'list node-names' command to see all the administered node-names
Use 'change node-names ip xxx' to change a node-name 'xxx' or add a node-name
```

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 **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                      NR Group: 1
Location: 1                          Authoritative Domain: devconnect.local
      Name: PG Default                Stub Network Region: n
MEDIA PARAMETERS                     Intra-region IP-IP Direct Audio: yes
      Codec Set: 1                  Inter-region IP-IP Direct Audio: yes
      UDP Port Min: 2048              IP Audio Hairpinning? n
      UDP Port Max: 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            Keep-Alive Count: 5
```

In the **IP Media Parameters** form, select the audio codec's supported for calls routed over the SIP trunk to Communications Portal. The form is accessed via the **display ip-codec-set n** command or if a change were needed to be made type change ip-codec-set n. Note that IP codec set 1 was specified in IP Network Region 1 shown on the previous page. Multiple codecs may be specified in the **IP Codec Set** form in order of preference; the example below includes **G.711A** (a-law), which is supported by the DMS.

Media Encryption is used on the Avaya sets where possible these use **srtp-aescm128-hmac80** media encryption. **None** is also present to facilitate the Capita DMS extensions.

```

display ip-codec-set 1                                     Page 1 of 2

                                IP MEDIA PARAMETERS

Codec Set: 1

Audio      Silence      Frames      Packet
Codec      Suppression   Per Pkt    Size(ms)
1: G.711A          n           2           20
2: G.729A          n           2           20
3: G.729           n           2           20
4:
5:
6:
7:

Media Encryption                                Encrypted SRTCP: enforce-unenc-srtcp
1: 1-srtp-aescm128-hmac80
2: none
3:
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 **tls**.
- 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.
- Set the **Near-end Node Name** to **procr**.
- Set the **Far-end Node Name** to the node name defined for the Session Manager (node name **SM80vmpg**), as per **Section 5.5**.
- Ensure that the recommended TLS port value of **5061** is configured in the **Near-end Listen Port** and the **Far-end Listen Port** fields.
- In the **Far-end Network Region** field, enter the IP Network Region configured previously. 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 **n**. This is to turn ‘shuffling’ off in order to facilitate testing with Capita DMS. Issues arose when Shuffling was on.
- The default values for the other fields may be used.

Note: Compliance testing was carried out with the **Direct IP-IP Audio Connections** field is set to **n**. This was to allow testing with shuffling off.

```

change signaling-group 1                                     Page 1 of 3
                                SIGNALING GROUP

Group Number: 1                Group Type: sip
IMS Enabled? n                 Transport Method: tls
Q-SIP? n
IP Video? n                    Enforce SIPS URI for SRTP? n
Peer Detection Enabled? y     Peer Server: SM                Clustered? n
Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? y
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? n
Alert Incoming SIP Crisis Calls? n
Near-end Node Name: procr      Far-end Node Name: SM80vmpg
Near-end Listen Port: 5061     Far-end Listen Port: 5061
                                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? n
Enable Layer 3 Test? y                                     IP Audio Hairpinning? n
                                                                Alternate Route Timer(sec): 6

```

Configure the **Trunk Group** form as shown below. This trunk group is used for all incoming and outgoing SIP calls to Session Manager SIP Entities including Capita's DMS. 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 **tie** (this may vary depending on the site in question). 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 4
                                     TRUNK GROUP
Group Number: 1                                     Group Type: sip           CDR Reports: y
  Group Name: SIPTRUNK-SM80                       COR: 1                 TN: 1           TAC: *801
  Direction: two-way                               Outgoing Display? n
Dial Access? n                                     Night Service:
Queue Length: 0
Service Type: tie                                   Auth Code? n
                                                Member Assignment Method: auto
                                                Signaling Group: 1
                                                Number of Members: 10
  
```

On **Page 2** of the trunk-group form the following values were used for compliance testing.

```

change trunk-group 1                                     Page 2 of 4
  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): 600
Disconnect Supervision - In? y Out? y
  XOIP Treatment: auto   Delay Call Setup When Accessed Via IGAR? n
  Caller ID for Service Link Call to H.323 1xC: station-extension
  
```

On **Page 3** of the trunk-group form the following values were used for compliance testing. The **Numbering Format** was set to **private**.

```
change trunk-group 1                                     Page 3 of 4
TRUNK FEATURES
    ACA Assignment? n          Measured: none
                                Maintenance Tests? y

    Suppress # Outpulsing? n  Numbering Format: private
                                UUI Treatment: service-provider
                                Replace Restricted Numbers? n
                                Replace Unavailable Numbers? n
                                Hold/Unhold Notifications? y
                                Modify Tandem Calling Number: no

    Show ANSWERED BY on Display? y

    DSN Term? n
```

Settings on **Page 4** are as follows. **Network Call Redirection** set to **y**. The other settings should be set as shown below.

```
change trunk-group 1                                     Page 4 of 4
                                PROTOCOL VARIATIONS

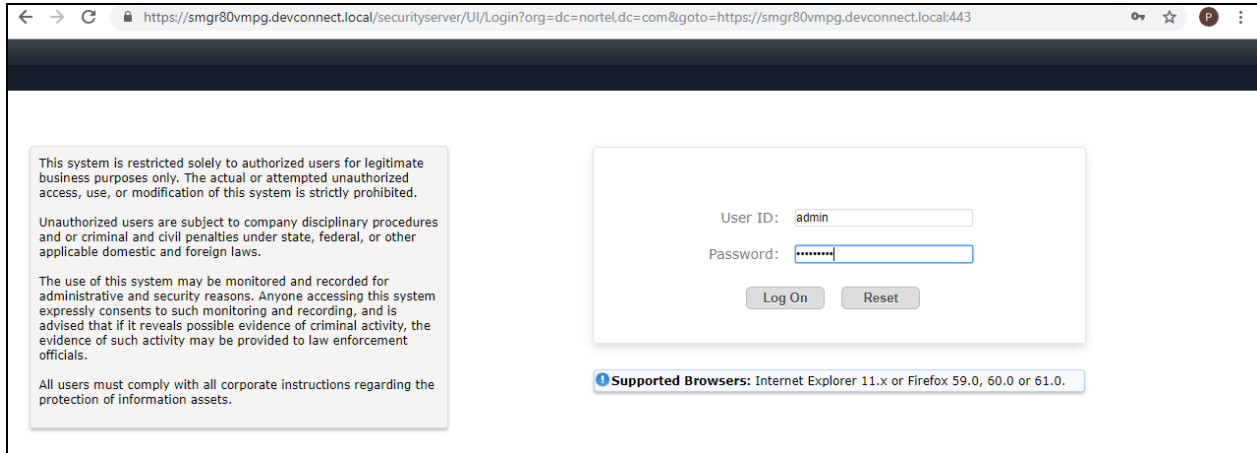
                                Mark Users as Phone? n
    Prepend '+' to Calling/Alerting/Diverting/Connected Number? n
                                Send Transferring Party Information? y
                                Network Call Redirection? y
    Build Refer-To URI of REFER From Contact For NCR? n
                                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? 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

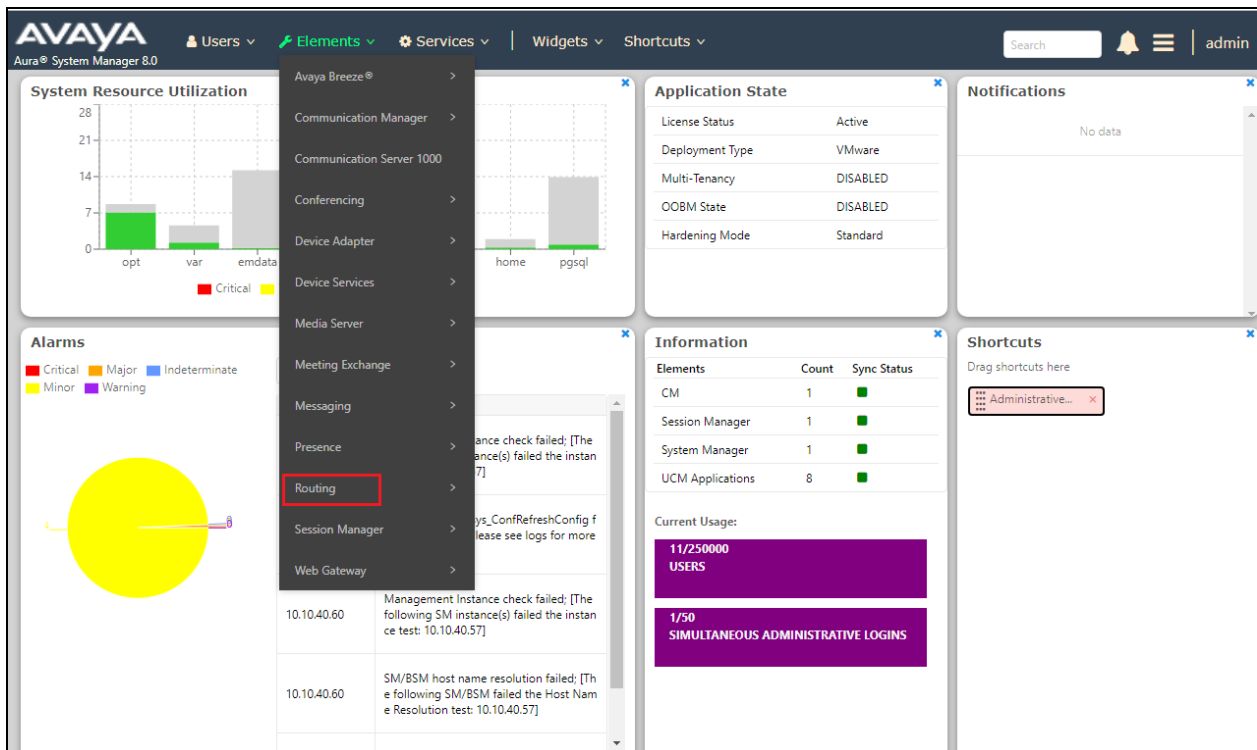
    Interworking of ISDN Clearing with In-Band Tones: keep-channel-active
                                Request URI Contents: may-have-extra-digits
```

6. Configure Avaya Aura® Session Manager

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



Once logged in navigate to **Elements** and click on **Routing** highlighted below.

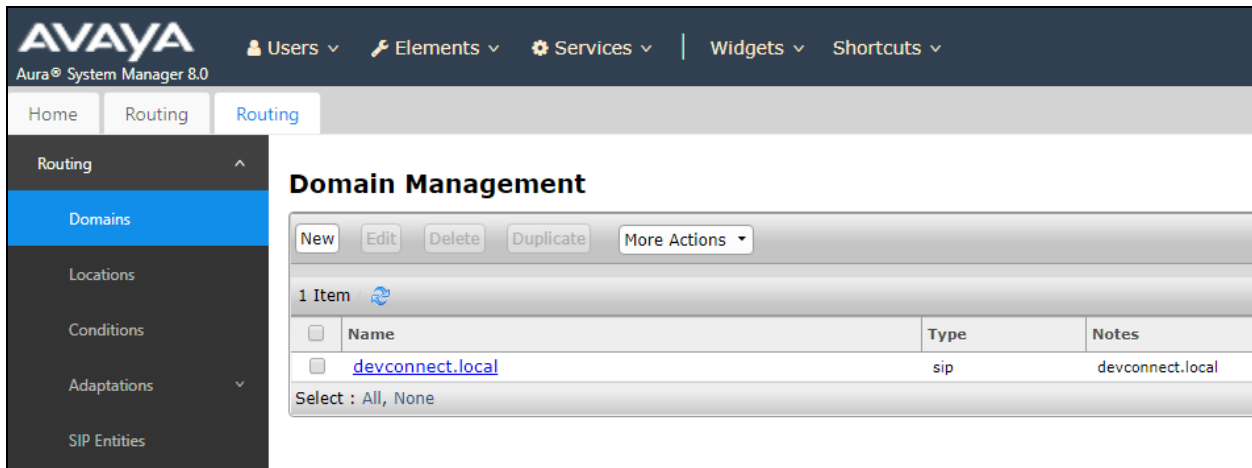


6.1. Domains and Locations

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

6.1.1. Display the Domain

Select **Domains** from the left window. This will display the domain configured on Session Manager. For compliance testing this domain was **devconnect.local** as shown below. If a domain is not already in place, click on **New**. This will open a new window (not shown) where the domain can be added.



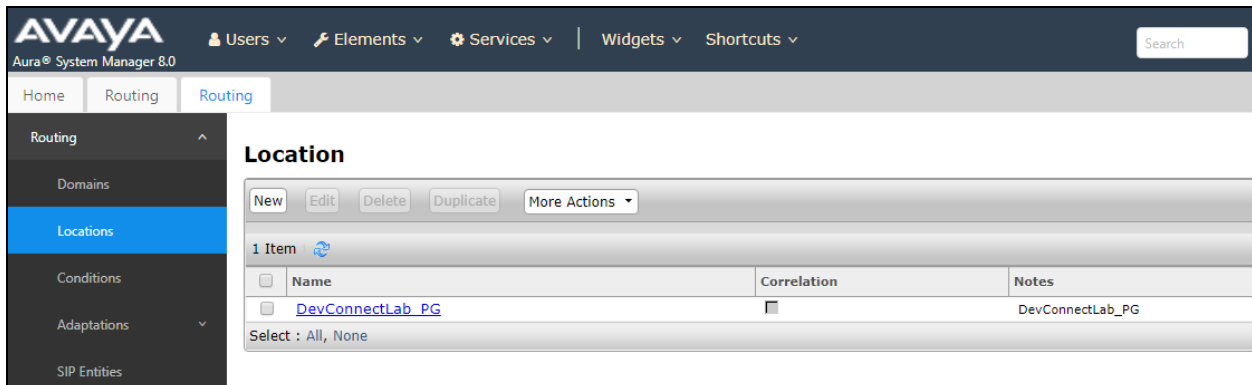
The screenshot shows the Avaya Aura System Manager 8.0 interface. The top navigation bar includes 'Users', 'Elements', 'Services', 'Widgets', and 'Shortcuts'. The left sidebar is expanded to 'Routing', with 'Domains' selected. The main content area is titled 'Domain Management' and features a table with one item:

Name	Type	Notes
devconnect.local	sip	devconnect.local

Buttons for 'New', 'Edit', 'Delete', 'Duplicate', and 'More Actions' are visible above the table. Below the table, it says 'Select : All, None'.

6.1.2. Display the Location

Select **Locations** from the left window and this will display the location setup. The example below shows the location **DevConnectLab_PG** which was used for compliance testing. 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** to add a new location.



The screenshot shows the Avaya Aura System Manager 8.0 interface. The top navigation bar includes 'Users', 'Elements', 'Services', 'Widgets', and 'Shortcuts'. The left sidebar is expanded to 'Routing', with 'Locations' selected. The main content area is titled 'Location' and features a table with one item:

Name	Correlation	Notes
DevConnectLab_PG	<input type="checkbox"/>	DevConnectLab_PG

Buttons for 'New', 'Edit', 'Delete', 'Duplicate', and 'More Actions' are visible above the table. Below the table, it says 'Select : All, None'.

6.2. Adding the Capita Distinction Media Server as a SIP Entity

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

<input type="checkbox"/>	Name	FQDN or IP Address	Type	Notes
<input type="checkbox"/>	AA Messaging V7	10.10.40.23	SIP Trunk	AA Messaging V7
<input type="checkbox"/>	CM71vmppg	10.10.40.47	CM	CM71vmppg
<input type="checkbox"/>	CM80vmppg	10.10.40.59	CM	CM80vmppg
<input type="checkbox"/>	CS1KPG1	10.10.40.111	SIP Trunk	CS1000 (CS1KPG1)
<input type="checkbox"/>	EP72vmppg	10.10.40.63	Voice Portal	EP72vmppg
<input type="checkbox"/>	EP_Oceana	10.10.41.16	Voice Portal	EP_Oceana
<input type="checkbox"/>	SM80vmppg	10.10.40.58	Session Manager	SM80vmppg
<input type="checkbox"/>	StephensCM	10.10.16.23	CM	StephensCM
<input type="checkbox"/>	StevesEP	10.10.16.20	Voice Portal	StevesEP

Enter a suitable **Name** for the new SIP Entity and the **IP Address** of the DMS. Enter the correct **Time Zone** and **Location**. The Entity Link can be added from this page by scrolling down.

SIP Entity Details Commit Cancel

General

* Name:

* FQDN or IP Address:

Type:

Notes:

Adaptation:

Location:

Time Zone:

* SIP Timer B/F (in seconds):

Minimum TLS Version:

Credential name:

Securable:

Call Detail Recording:

Loop Detection

Loop Detection Mode:

Loop Count Threshold:

Loop Detection Interval (in msec):

Monitoring

SIP Link Monitoring:

CRLF Keep Alive Monitoring:

Supports Call Admission Control:

Shared Bandwidth Manager:

6.3. Adding the Distinction Media Server Entity Link

An Entity link can be added from the SIP Entities page. Using the page from the previous page scroll down to Entity Links.

Enter a suitable **Name** for the Entity Link and select the **Session Manager** SIP Entity for **SIP Entity 1** and the newly created Capita DMS Entity 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 and SIP Entity.

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Deny New Service
* SM80vmpg_Capita DMS_	SM80vmpg	UDP	* 5060	Capita DMS	* 5060	trusted	<input type="checkbox"/>

Response Code & Reason Phrase	Mark Entity Up/Down	Notes

6.4. Adding the Distinction Media Server Routing Policy

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

Name	Disabled	Retries	Destination	Notes
To AA Messaging V7	<input type="checkbox"/>	0	AA Messaging V7	To AA Messaging V7
To CM71vmpg	<input type="checkbox"/>	0	CM71vmpg	To CM71vmpg
To CM80vmpg	<input type="checkbox"/>	0	CM80vmpg	To CM80vmpg
To CS1KPG1	<input type="checkbox"/>	0	CS1KPG1	To CS1KPG1
To EP72vmpg	<input type="checkbox"/>	0	EP72vmpg	To EP72vmpg
To EP_Oceana	<input type="checkbox"/>	0	EP_Oceana	To EP Oceana
To Stephens_CM	<input type="checkbox"/>	0	StephensCM	To EP Oceana
To Steves EP	<input type="checkbox"/>	0	StevesEP	To Steves EP

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

Commit Cancel

Routing Policy Details

General

* Name:

Disabled:

* Retries:

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes

Time of Day

Add Remove View Gaps/Overlaps

1 Item 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

Select : All, None

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

Select Cancel

SIP Entities

SIP Entities

10 Items Filter: Enable

Name	FQDN or IP Address	Type	Notes
<input type="radio"/> AA Messaging V7	10.10.40.23	SIP Trunk	AA Messaging V7
<input checked="" type="radio"/> Capita DMS	10.10.40.122	SIP Trunk	Capita DMS
<input type="radio"/> Capita DS3000	10.253.160.206	SIP Trunk	Capita DS3000
<input type="radio"/> CM71vmpg	10.10.40.47	CM	CM71vmpg
<input type="radio"/> CM80vmpg	10.10.40.59	CM	CM80vmpg
<input type="radio"/> CS1KPG1	10.10.40.111	SIP Trunk	CS1000 (CS1KPG1)
<input type="radio"/> EP72vmpg	10.10.40.63	Voice Portal	EP72vmpg
<input type="radio"/> EP_Oceana	10.10.41.16	Voice Portal	EP_Oceana
<input type="radio"/> StephensCM	10.10.16.23	CM	StephensCM
<input type="radio"/> StevesEP	10.10.16.20	Voice Portal	StevesEP

Select : None

Select Cancel

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

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

Routing Policy Details

General

* Name:

Disabled:

* Retries:

Notes:

SIP Entity as Destination

Name	FQDN or IP Address	Type	Notes
Capita DMS	10.10.40.122	SIP Trunk	Capita DMS

6.5. Adding a Dial Pattern for the Distinction Media Server

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

The screenshot shows the Avaya Aura System Manager 8.0 interface. The left sidebar is expanded to show 'Routing Policies' and 'Dial Patterns'. The main content area is titled 'Dial Patterns' and contains a table with 11 items. The table has the following columns: Pattern, Min, Max, Emergency Call, Emergency Type, Emergency Priority, SIP Domain, and Notes. The data rows are as follows:

Pattern	Min	Max	Emergency Call	Emergency Type	Emergency Priority	SIP Domain	Notes
2	4	4	<input type="checkbox"/>			devconnect.local	To CM80vmpg
280	4	4	<input type="checkbox"/>			devconnect.local	To EP72vmpg
290	4	4	<input type="checkbox"/>			devconnect.local	To EP Oceana
30	4	4	<input type="checkbox"/>			devconnect.local	To CS1KPG1
380	4	4	<input type="checkbox"/>			devconnect.local	To Steves EP
4	4	4	<input type="checkbox"/>			devconnect.local	To CM71vmpg
52	4	4	<input type="checkbox"/>			devconnect.local	To CM80Vmpg for simulated PSTN to IPO
6666	4	4	<input type="checkbox"/>			devconnect.local	To AA Messaging V7

Enter the required digits for the Pattern, in the example below 7080xx is used, which means that 708000 – 708099 will use the Routing Policy that will be selected. **7080** is entered as the **Pattern** and the **Min** and **Max** digit length of **6** is used thus giving 7080xx. Ensure that the correct domain is entered for **SIP Domain** in this example the domain created in **Section 6.1.1** is added. Click on **Add** under **Originating Locations and Routing Policies** to select the Routing Policy.

Dial Pattern Details Commit Cancel

General

* Pattern:

* Min:

* Max:

Emergency Call:

SIP Domain:

Notes:

Originating Locations and Routing Policies

Add Remove

1 Item Filter: Enable

	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>							

Select : All, None

Select the **Originating Location**, this will be the location added in **Section 6.1.2** select the newly created routing policy for the DMS.

Originating Location Select Cancel

Originating Location

Apply The Selected Routing Policies to All Originating Locations

1 Item Filter: Enable

	Name	Notes
<input checked="" type="checkbox"/>	DevConnectLab_PG	DevConnectLab_PG

Select : All, None

Routing Policies

10 Items Filter: Enable

	Name	Disabled	Destination	Notes
<input type="checkbox"/>	To AA Messaging V7	<input type="checkbox"/>	AA Messaging V7	To AA Messaging V7
<input checked="" type="checkbox"/>	To Capita DMS	<input type="checkbox"/>	Capita DMS	To Capita DMS
<input type="checkbox"/>	To Capita DS3000	<input type="checkbox"/>	Capita DS3000	To Capita DS3000
<input type="checkbox"/>	To CM71vmpg	<input type="checkbox"/>	CM71vmpg	To CM71vmpg
<input type="checkbox"/>	To CM80vmpg	<input type="checkbox"/>	CM80vmpg	To CM80vmpg
<input type="checkbox"/>	To CS1KPG1	<input type="checkbox"/>	CS1KPG1	To CS1KPG1
<input type="checkbox"/>	To EP72vmpg	<input type="checkbox"/>	EP72vmpg	To EP72vmpg
<input type="checkbox"/>	To EP Oceana	<input type="checkbox"/>	EP_Oceana	To EP Oceana
<input type="checkbox"/>	To Stephens CM	<input type="checkbox"/>	StephensCM	To Stephens CM
<input type="checkbox"/>	To Steves EP	<input type="checkbox"/>	StevesEP	To Steves EP

Select : All, None

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

[Help ?](#)

Dial Pattern Details

General

* **Pattern:**

* **Min:**

* **Max:**

Emergency Call:

SIP Domain:

Notes:

Originating Locations and Routing Policies

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"/>	DevConnectLab_PG	DevConnectLab_PG	To Capita DMS	0	<input type="checkbox"/>	Capita DMS	To Capita DMS

Select : All, None

Denied Originating Locations

0 Items

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

7. Configure Capita - Secure Solutions and Services Distinction Media Server

The installation and configuration of the DMS is carried out by an engineer with sufficient training from Capita as it was for compliance testing. An in-depth knowledge of the DMS is required in order to make configuration changes and such changes should only be made by an engineer with this capability, therefore the setup and configuration of the Capita Distinction Media Server is outside the scope of these Application Notes. For information on the setup and configuration of the DMS, please contact Capita as per **Section 2.3**.

8. Verification Steps

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

8.1. Verify that calls can be made to and from the DMS

From an Avaya extension make a call to a DMS extension and ensure that the call remains active for more than 40 seconds. From a DMS extension make a call to the Avaya extension and again keep the call active for more than 40 seconds. The following steps in **Section 8.2** and **Section 8.3** can be taken if there are any issues with calls being made. This should help verify the links between the products.

8.2. Verify Avaya Aura® Communication Manager

From the SAT interface, verify the status of the SIP trunk groups by using the **status trunk n** command, where "n" is the trunk group number administered in **Section 5.5**. Verify that all trunks are in the **in-service/idle** state as shown below.

```
status trunk 1
```

TRUNK GROUP STATUS			
Member	Port	Service State	Mtce Connected Ports Busy
0001/0001	T00001	in-service/idle	no
0001/0002	T00002	in-service/idle	no
0001/0003	T00003	in-service/idle	no
0001/0004	T00004	in-service/idle	no
0001/0005	T00005	in-service/idle	no
0001/0006	T00006	in-service/idle	no
0001/0007	T00007	in-service/idle	no
0001/0008	T00008	in-service/idle	no
0001/0009	T00009	in-service/idle	no
0001/0010	T00010	in-service/idle	no

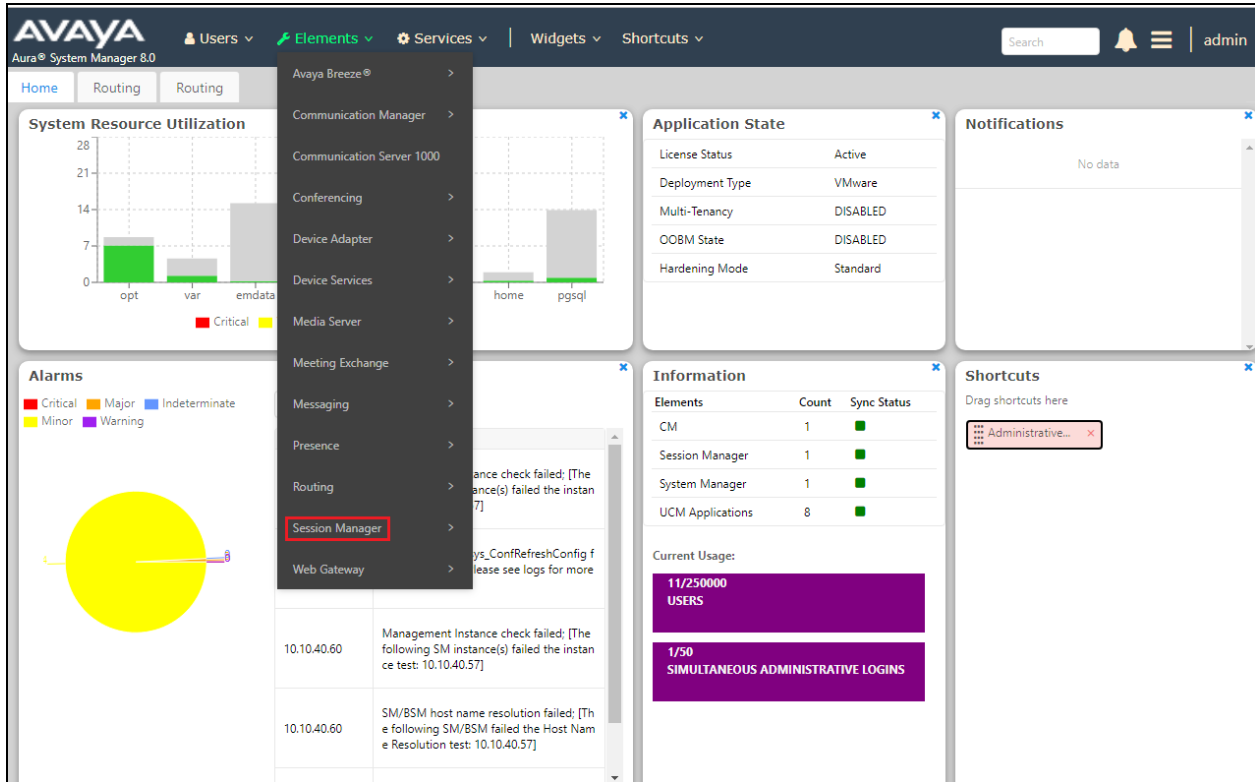
Verify the status of the SIP signaling groups by using the **status signaling-group n** command, where "n" is the signaling group number administered in **Section 5.5**. Verify that the signaling group is **in-service** as indicated in the **Group State** field shown below.

```
status signaling-group 1
```

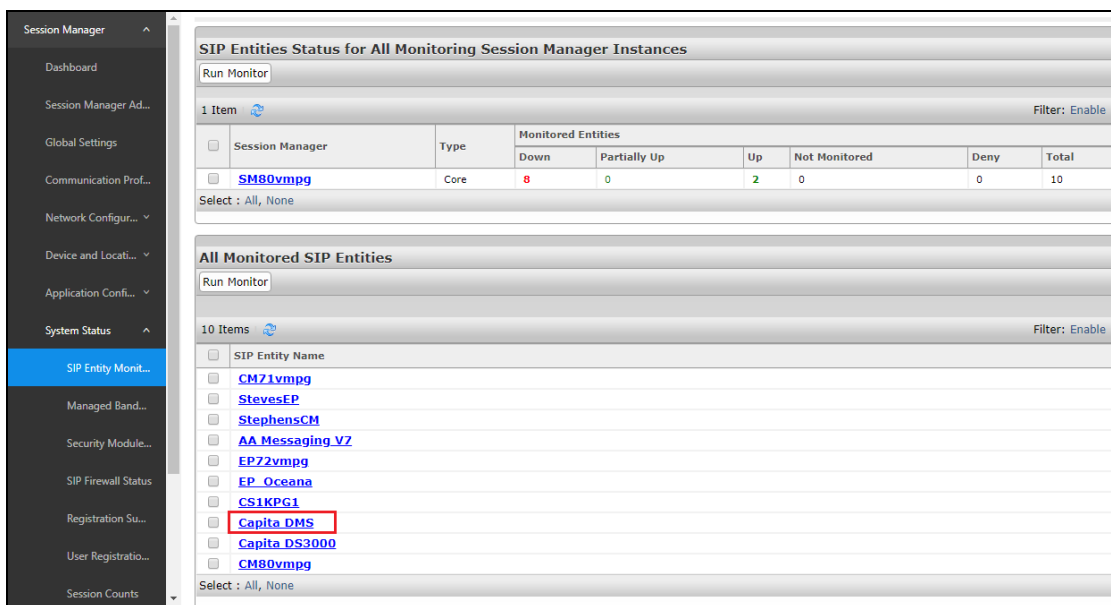
STATUS SIGNALING GROUP	
Group ID:	1
Group Type:	sip
Group State:	in-service

8.3. Verify Capita DMS SIP Entity on Avaya Aura® System Manager

Log into System Manager as per **Section 6.1**. Navigate to **Elements** and click on **Session Manager**.



Select the **Capita DMS** SIP Entity.




The SIP Entity should show as **UP** as it is shown below.

SIP Entity, Entity Link Connection Status
This page displays detailed connection status for all entity links from all Session Manager instances to a single SIP entity.

Status Details for the selected Session Manager:

All Entity Links to SIP Entity: Capita DMS

Summary View

1 Item  Filter: Enable

	Session Manager Name	IP Address Family	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
<input type="radio"/>	SM80vmpg	IPv4	10.10.40.122	5060	UDP	FALSE	UP	200 OK	UP

Select : None

9. Conclusion

These Application Notes describe the configuration steps required for the Distinction Media Server from Capita - Secure Solutions and Services to successfully interoperate with Avaya Aura® Communication Manager R8.0.1 and Avaya Aura® Session Manager R8.0.1. 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*, Release 8.0.1 Issue 3 December 2018
- [2] *Avaya Aura® Communication Manager Feature Description and Implementation*
- [3] *Administering Avaya Aura® System Manager for Release 8.0*
- [4] *Administering Avaya Aura® Session Manager for Release 8.0*

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

©2019 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.