



DevConnect Program

Application Notes for Smoke Customer Intelligence Pty Ltd. Eyerys IVR Connector to interoperate with Avaya Aura® Communication Manager, Avaya Aura® Session Manager and Avaya Aura® Application Enablement Services – Issue 1.0

Abstract

These Application Notes describe the configuration steps for Eyerys IVR Connector R2.2 from Smoke Customer Intelligence Pty Ltd., to successfully interoperate with Avaya Aura® Communication Manager R10.1, Avaya Aura® Session Manager R10.1 and Avaya Aura® Application Enablement Services R10.1. Eyerys is a post call survey which allows callers leave a review in the form of a score from one to five, as well as the option to leave a voice message after a contact center call. Typically the caller is automatically transferred into the survey via SIP trunk once the interaction with the contact center agent is complete. Information on the call and the agent involved is obtained via the Device, Media, and Call Control (DMCC) interface to Avaya Aura® Application Enablement Services.

Readers should pay attention to **Section 2**, in particular the scope of testing as outlined in **Section 2.1** as well as the 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.

1. Introduction

These Application Notes describe the configuration steps for Smoke Customer Intelligence Pty Ltd., Eyerys IVR Connector to successfully interoperate with Avaya Aura® Communication Manager, Avaya Aura® Session Manager and Avaya Aura® Application Enablement Services (AES).

Eyerys IVR Connector v2.2 (Eyerys) from Smoke Customer Intelligence Pty Ltd., integrates with the Avaya platform (Avaya Aura® Communication Manager R10.1, Avaya Aura® Session Manager R10.1 and Avaya Aura® Application Enablement Services R10.1) to allow contact centers to collect customer satisfaction feedback via a telephony survey at the end of a call. The current integration of the Eyerys platform prompts an end customer to provide feedback using their telephones keypad (DTMF).

Eyerys makes use of a SIP trunk connection to Session Manager as well as the Device, Media, and Call Control (DMCC) interface to Application Enablement Services. Typically the caller is automatically transferred into the survey via SIP trunk once the interaction with the contact center agent is complete. Information on the call and the agent involved is obtained via the DMCC interface. Callers use DTMF to leave their review and have the option to leave a voice message on Eyerys which can be played back when analyzing the reports.

2. General Test Approach and Test Results

Compliance testing included validating the operation of Eyerys in a typical contact center environment. Functionality testing included basic telephony operations such as verifying that the call was transferred from Communication Manager to Eyerys correctly and that the information on the call and the agent was passed onto Eyerys. This can be verified by making calls from a simulated PSTN and transferring these calls into Eyerys, where the caller can leave their review using DTMF (pressing 1 to 5) and leaving a voice message and then verifying this review by running various reports on the Eyerys solution. The serviceability test cases were performed manually by disconnecting and reconnecting LAN cables.

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 Avaya systems and Eyerys made use of a secure DMCC connection to Application Enablement Services, but not to Session Manager, using a UDP connection as requested by Smoke Customer Intelligence Pty Ltd.

2.1. Interoperability Compliance Testing

The interoperability compliance test included both feature functionality and serviceability testing. The feature functionality testing focused on verifying Eyerys handling of events from DMCC and using these to create reports on the agents in a contact center, as well as verifying that calls could be transferred successfully from Communication Manager to Eyerys. The serviceability testing focused on verifying the Eyerys ability to recover from adverse conditions, such as disconnecting and reconnecting the Ethernet cable from all the devices in the solution.

The following types of calls were made:

- Calls to agents Automatically transferred to Eyerys Post Call Survey
- Calls to agents Manually transferred to Eyerys Post Call Survey
- Calls to different Eyerys Post Call Surveys
- Testing different Codec and DTMF standards

2.2. Test Results

All test cases were executed successfully. The following observations were noted.

1. A BYE is not being sent correctly to the PSTN; this only happens when the VDN is programmed to automatically send the caller to the survey by configuring “return destination” on Communication Manager. Smoke are investigating this issue.
2. The agents can currently leave their own survey and the events are the same as if the customer left the same survey. This is currently as per design.

2.3. Support

Technical support can be obtained for Smoke Customer Intelligence Pty Ltd. as follows:

- Email: support@smokeci.com
- Website: <https://www.smokeci.com/contact>
- Phone: +1 212 901 5303 or +27 11 462 9881

3. Reference Configuration

Figure 1 shows the setup for compliance testing Eyerys with Communication Manager and Session Manager using SIP signalling over SIP trunks to pass calls from Communication Manager to the Eyerys Post Call Survey.

A second connection to Application Enablement Services is established using DMCC to get call and agent information.

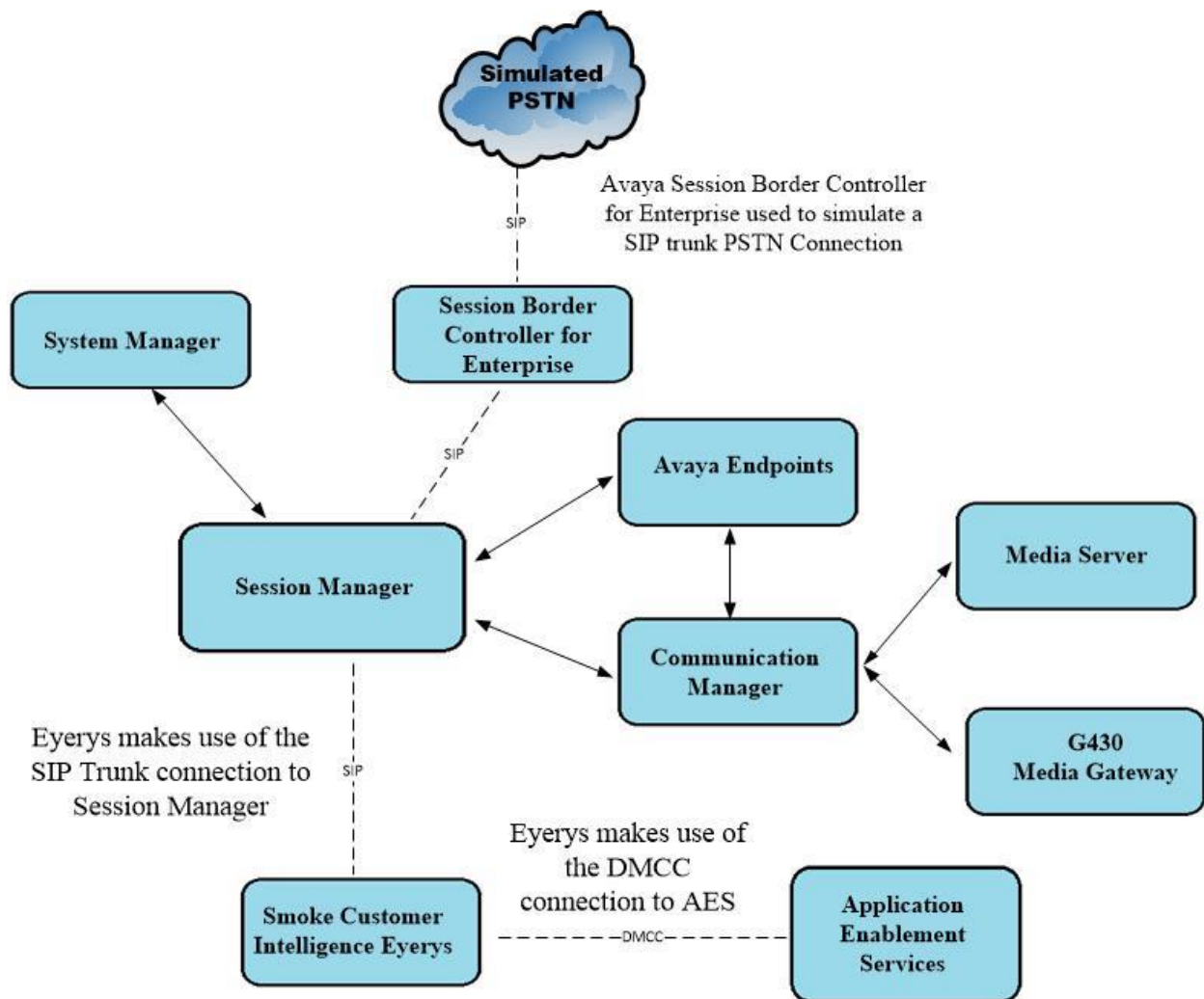


Figure 1: Connection of Smoke Customer Intelligence Pty Ltd. Eyerys IVR Connector v2.2 with Avaya Aura® Communication Manager R10.1, Avaya Aura® Application Enablement Services and Avaya Aura® Session Manager R10.1

4. Equipment and Software Validated

All the hardware and associated software used in the compliance testing is listed below.

Equipment/Software	Release/Version
Avaya Aura® System Manager	System Manager 10.1.0.2 Build No. – 10.1.0.0.537353 Software Update Revision No: 10.1.0.2.0715160 Service Pack 2
Avaya Aura® Session Manager	Session Manager R10.1 Build No. – 10.1.0.2.1010219
Avaya Aura® Communication Manager	R10.1.0.2.0 – SP2 R020x.01.0.974.0 Update ID 01.0.974.0-27607
Avaya Aura® Application Enablement Services	10.1.0 Build 10.1.0.2.0.12-0
Avaya Aura® Media Server	10.1.0.101
Avaya Media Gateway G430	42.7.0 /2
Avaya 9404 Digital	17.0
Avaya J100 Series SIP	7.1.2.0.14
Avaya J100 Series H323	7.0.14.0.7
Avaya Session Border Controller for Enterprise (to facilitate simulated PSTN)	10.1.0
Smoke Customer Intelligence Pty Ltd. Eyerys	2.2.0

All equipment ran on virtual servers on VMware.

5. Configure Avaya Aura® Communication Manager

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 and verification operations illustrated in this section were all performed using Communication Manager System Administration Terminal (SAT).

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

- Verify System Parameters
- Configure SIP Trunk
- Administer Route Selection
- Configure VDN and Vector for Automatic Transfer
- Configure TSAPI link to Avaya Aura® Application Enablement Services

Note: The configuration of the simulated PSTN is outside the scope of these Application Notes.

5.1. Verify System Parameters

Special Applications, Customer Options and Features will all need to be checked under System Parameters to ensure that fields are set to allow the connection to Eyerys to work correctly.

5.1.1. Verify System Parameters Special Applications

(SA8702) - **CDR Enhancements for Network** is recommended to be set to **n**, as setting this to “y” may cause issues with SIP CC phones. Special Application changes the behavior of how Communication Manager handles UCIDs, especially in conference and transfer scenarios. Some call recorders may need to accommodate for this change. Please refer to the "User Scenarios" section in the SA8702 customer document and confirm adjunct applications e.g., call recorders would be compatible with SA8702. Also, SA8702 is not compatible with Avaya IQ and Contact Center SIP agents.

```
change system-parameters special-applications                Page   5 of 11
                        SPECIAL APPLICATIONS

                        (SA8652) - No Hold Consult? n
(SA8654) - Crisis Alert Call Monitoring and Recording? n
                        (SA8661) - Increased Automatic Wakeup Calls? n
                        (SA8662) - Expanded PMS Name & Number? n
                        (SA8684) - PMS Wakeup Message? n
(SA8693) - Connectivity Check for Direct IP Shuffling? n

                        (SA8697) - 3rd Party H.323 Endpoint Support? n
(SA8701) - Net Region Support H.323 Endpoints Behind ALG? n
                        (SA8702) - CDR Enhancements for Network? n
                        (SA8731) - Block Outgoing Bridged Call Display? n
                        (SA8734) - Enhanced Extension Display? n
                        (SA8741) - CDR Identifier for IP Station Calls? n
                        (SA8744) - Block Name for Room to Room Calls? n
                        (SA8747) - Softphone Indication on DCP Terminals? n
```

5.1.2. 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 the **Maximum Administered SIP Trunks** have sufficient capacity. Each call that receives ACD treatment from Eyerys 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 two 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
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 4**, ensure that both **ARS** and **ARS/AAR Partitioning** are set to **y**.

display system-parameters customer-options		Page	4 of 12
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 6**, ensure that **Uniform Dialing Plan** is set to **y**.

display system-parameters customer-options		Page	6 of 12
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

5.1.3. Verify System Parameters Features

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
```


5.2. Configure SIP Trunk

In the **Node Names IP** form, note the IP Address of the **procr** and Session Manager (**sm101x**). These host names will be used throughout the other configuration screens of Communication Manager, Session Manager and Application Enablement Services. Type **display node-names ip** to show all the node names.

```
display node-names ip
```

IP NODE NAMES	
Name	IP Address
sm101x	10.10.40.12
aespri101x	10.10.40.16
aessec101x	10.10.40.46
g450	10.10.40.15
procr	10.10.40.13

(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 **greaney.sil6.avaya.com**. 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 **Authoritative Domain: greaney.sil6.avaya.com**
Name: Default region

MEDIA PARAMETERS Intra-region IP-IP Direct Audio: yes
 Codec Set: 1 Inter-region IP-IP Direct Audio: yes
 UDP Port Min: 2048 IP Audio Hairpinning? n
 UDP Port Max: 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

H.323 IP ENDPOINTS AUDIO RESOURCE RESERVATION PARAMETERS
 H.323 Link Bounce Recovery? y RSVP Enabled? n
 Idle Traffic Interval (sec): 20
 Keep-Alive Interval (sec): 5
 Keep-Alive Count: 5

In the **IP Codec Set** form, select the audio codecs supported for calls routed over the SIP trunk to Eyeris. The form is accessed via the **display 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 the Codecs that Eyeris supports which were all tested.

Media Encryption is used on the Avaya sets where possible these use **srtp-aescm128-hmac80** media encryption. **None** is also present to facilitate any extension not capable of handling encryption.

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: OPUS-SWK24K		1	20	
2: G.711A	n	2	20	
3: G.711MU	n	2	20	
4: G.729	n	2	20	
5:				
Media Encryption			Encrypted SRTCP: best-effort	
1: 1-srtp-aescm128-hmac80				
2: none				
3:				

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, **tls** (Transport Layer Security) should be used for DevConnect testing.
- The **Peer Detection Enabled** field should be set to **y** allowing Communication Manager to automatically detect if the peer server is a Session Manager.
- 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 **sm81xvmpg**), also shown above.
- 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 above. This field logically establishes the **far-end** for calls using this signaling group as network region **1**.
- The **Far-end Domain** field can be set to the domain name specified in the IP Network Region. This was left blank for compliance testing.
- The **DTMF over IP** field should remain set to the default value of **rtp-payload**. This value enables Communication Manager to send DTMF transmissions using RFC 2833.
- The **Direct IP-IP Audio Connections** field is set to **y**.
- The default values for the other fields may be used.

Note: These were the settings for compliance testing, however, this trunk may be setup differently on each customer site depending on the customer's requirements for SIP routing.

change signaling-group 21		Page 1 of 2
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	
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: sm101x	
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? y	
Enable Layer 3 Test? y	IP Audio Hairpinning? n	
H.323 Station Outgoing Direct Media? n	Initial IP-IP Direct Media? n	
	Alternate Route Timer(sec): 6	

Configure the **Trunk Group** form as shown below. This trunk group is used for calls to and from Eyeris. 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 21		Page 1 of 5	
TRUNK GROUP			
Group Number: 1	Group Type: sip	CDR Reports: y	
Group Name: SIPTRUNK	COR: 1	TN: 1	TAC: 821
Direction: two-way	Outgoing Display? n	Night Service:	
Dial Access? n			
Queue Length: 0			
Service Type: public-ntwrk	Auth Code? n		
	Member Assignment Method: auto		
	Signaling Group: 1		
	Number of Members: 10		

On **Page 2** of the trunk-group form the **Preferred Minimum Session Refresh Interval (sec)** field should be set to a value mutually agreed with Smoke Customer Intelligence Pty Ltd., to prevent unnecessary SIP messages during call setup. For the compliance test a value of **600** was used.

change trunk-group 21		Page 2 of 5	
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			

Settings on **Page 3** are as follows. These are the values used during compliance testing. Note that **Numbering Format** was set to **Private**. **UI Treatment** is set to **shared** and **Send UCID** is set to **y**.

change trunk-group 21	Page 3 of 5
TRUNK FEATURES	
ACA Assignment? n	Measured: none
	Maintenance Tests? y
Suppress # Outpulsing? n	
Numbering Format: private	
UI Treatment: shared	
Maximum Size of UI Contents: 128	
Replace Restricted Numbers? n	
Replace Unavailable Numbers? n	
Modify Tandem Calling Number: no	
Send UCID? y	
Show ANSWERED BY on Display? y	

Settings on **Page 5** are as follows.

change trunk-group 21	Page 5 of 5
PROTOCOL VARIATIONS	
Mark Users as Phone? n	
Prepend '+' to Calling/Alerting/Diverting/Connected Number? n	
Send Transferring Party Information? y	
Network Call Redirection? 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	
Resend Display UPDATE Once on Receipt of 481 Response? 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	

5.3. Administer Route Selection for calls to Eyerys

It was decided for compliance testing that all calls to 600x were to be sent across the SIP trunk to Session Manager and routed to Eyerys. To achieve this routing, automatic alternate routing (aar) will be used to route the calls. The dial plan and aar routing analysis need to be changed to allow this routing.

Type **change dialplan analysis** to make changes to the dial plan. Note that **6** is of call type **udp** which means any numbers beginning with 6 are a part of the uniform dial plan.

change dialplan analysis						Page 1 of 12			
DIAL PLAN ANALYSIS TABLE									
Location: all						Percent Full: 3			
Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type	
1	4	udp	#	3	fac				
2	4	udp							
3	4	ext							
4	4	ext							
5	4	udp							
58	5	ext							
5999	4	ext							
6	4	udp							
6666	4	ext							
7	4	udp							
781	5	ext							
8	1	fac							
9	1	fac							
*	3	fac							
*8	4	dac							

Use the **change uniform-dialplan** command to configure the routing of the dialed digits. In the example below calls to **600x** will use Automatic Alternate Routing (aar). No further digits are deleted or inserted. Calls are sent to **aar** for further processing.

change uniform-dialplan 6						Page 1 of 2	
UNIFORM DIAL PLAN TABLE							
Percent Full: 0							
Matching			Insert		Node		
Pattern	Len	Del	Digits	Net	Conv	Num	
600	4	0		aar	n		
65	4	0		aar	n		
					n		
					n		
					n		
					n		
					n		
					n		

Use the **change aar analysis** command to further configure the routing of the dialed digits. Calls to Eyerys are achieved by dialing **600x** and are matched with the AAR entry shown below. Calls are sent to **Route Pattern 21**, which contains the outbound SIP Trunk Group.

change aar analysis 6							Page 1 of 2
AAR DIGIT ANALYSIS TABLE							
				Location: all		Percent Full: 3	
Dialed	Total		Route	Call	Node	ANI	
String	Min	Max	Pattern	Type	Num	Reqd	
6	7	7	254	aar		n	
600	4	4	21	aar		n	
65	4	4	1	aar		n	
7	7	7	254	aar		n	
8	7	7	254	aar		n	
9	7	7	254	aar		n	
						n	
						n	
						n	
						n	
						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 **21** is used to route calls to trunk group (**Grp No**) **21**, this is the SIP Trunk configured in **Section 5.5**. The **Numbering Format** was set to **lev0-pvt**.

change route-pattern 21										Page 1 of 3	
Pattern Number: 1										Pattern Name: SIP TRUNK	
SCCAN? n		Secure SIP? n		Used for SIP stations? n							
Grp		FRL	NPA	Pfx	Hop	Toll	No.	Inserted	DCS/ IXC		
No				Mrk	Lmt	List	Del	Digits	QSIG		
								Dgts	Intw		
1:	21	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

5.4. Configure VDN and Vector for Automatic Transfer

A VDN is created which points to a Vector that is configured to route calls to Eyerys. The idea is that the main VDN will reference this VDN as its Return Destination, so calls will be routed to this VDN when the call leaves the main VDN.

Add a VDN that uses a Vector, in the example below this is **VDN 1902** using **Vector 4**.

change vdn 1902	Page 1 of 3
VECTOR DIRECTORY NUMBER	
Extension: 1902	Unicode
Name? n	
Name*: FOR SMOKE	
Destination: Vector Number	4
Attendant Vectoring? n	
Meet-me Conferencing? n	
Allow VDN Override? n	
COR: 1	
TN*: 1	
Measured: none	Report Adjunct Calls as
ACD*? n	
VDN of Origin Annc. Extension*:	
1st Skill*:	
2nd Skill*:	
3rd Skill*:	
SIP URI:	
* Follows VDN Override Rules	

Vector 4 is changed to route calls to **6003**, which is a service on Eyerys that allows users to take a survey.

change vector 4	Page 1 of 6				
CALL VECTOR					
Number: 4	Name: FOR SMOKE				
Multimedia? n	Attendant Vectoring? n	Meet-me Conf? n	Lock? n		
Basic? y	EAS? y	G3V4 Enhanced? y	ANI/II-Digits? y	ASAI Routing? y	
Prompting? y	LAI? y	G3V4 Adv Route? y	CINFO? y	BSR? y	Holidays? y
Variables? y	3.0 Enhanced? y				
01 route-to	number 6003	cov n if unconditionally			
02					
03					
04					
05					
06					
07					
08					

The main VDN, for compliance testing this was **1900 (Sales)** is amended to set the Return Destination to the VDN created previously.

change vdn 1900	Page 1 of 3
VECTOR DIRECTORY NUMBER	
Extension: 1900	Unicode Name? n
Name*: Sales	
Destination: Vector Number	1
Attendant Vectoring?	n
Meet-me Conferencing?	n
Allow VDN Override?	n
COR:	1
TN*:	1
Measured: none	Report Adjunct Calls as ACD*? n
VDN of Origin Annc. Extension*:	
1st Skill*:	90
2nd Skill*:	
3rd Skill*:	
SIP URI:	
* Follows VDN Override Rules	

On **Page 2**, set the **Return Destination** to **1902**. This should ensure that all calls that come into VDN 1900 will end up being sent onto VDN 1902 once the call is complete.

change vdn 1900	Page 2 of 3
VECTOR DIRECTORY NUMBER	
AUDIX Name:	
Return Destination*: 1902	
VDN Timed ACW Interval*:	After Xfer or Held Call Drops*? n
BSR Application*:	
BSR Available Agent Strategy*:	1st-found Used for BSR Polling? n
BSR Tie Strategy*: system	
Observe on Agent Answer? n	
Send VDN as Called Ringing Name Over QSIG? n	
Display VDN for Route-To DAC*? n	
VDN Override for ASAI Messages*: no	
BSR Local Treatment*? n	
Reporting for PC or POM Calls? n	
Pass Prefixed CPN to VDN/Vector*? system	
* Follows VDN Override Rules	

5.5. Configure TSAPI Link to Avaya Aura® Application Enablement Services

It is assumed that a connection to AES is already in place and that the TSAPI connection and switch connection between Communication Manager and AES is fully working. The following section outlines the connection that was setup for compliance testing.

Display the IP addresses by using the command **display node-names ip** and noting the IP address for the **procr** and the AES.

display node-names ip		Page 1 of 2
		IP NODE NAMES
Name	IP Address	
sm101x	10.10.40.12	
aespri101x	10.10.40.16	
aessec101x	10.10.40.46	
g450	10.10.40.15	
procr	10.10.40.13	

Add a CTI link using the **add cti-link n** command, where n is the n is the cti-link number as shown in the example below this is **1**. Enter an available extension number in the **Extension** field. Enter **ADJ-IP** in the **Type** field, and a descriptive name in the **Name** field. Default values may be used in the remaining fields.

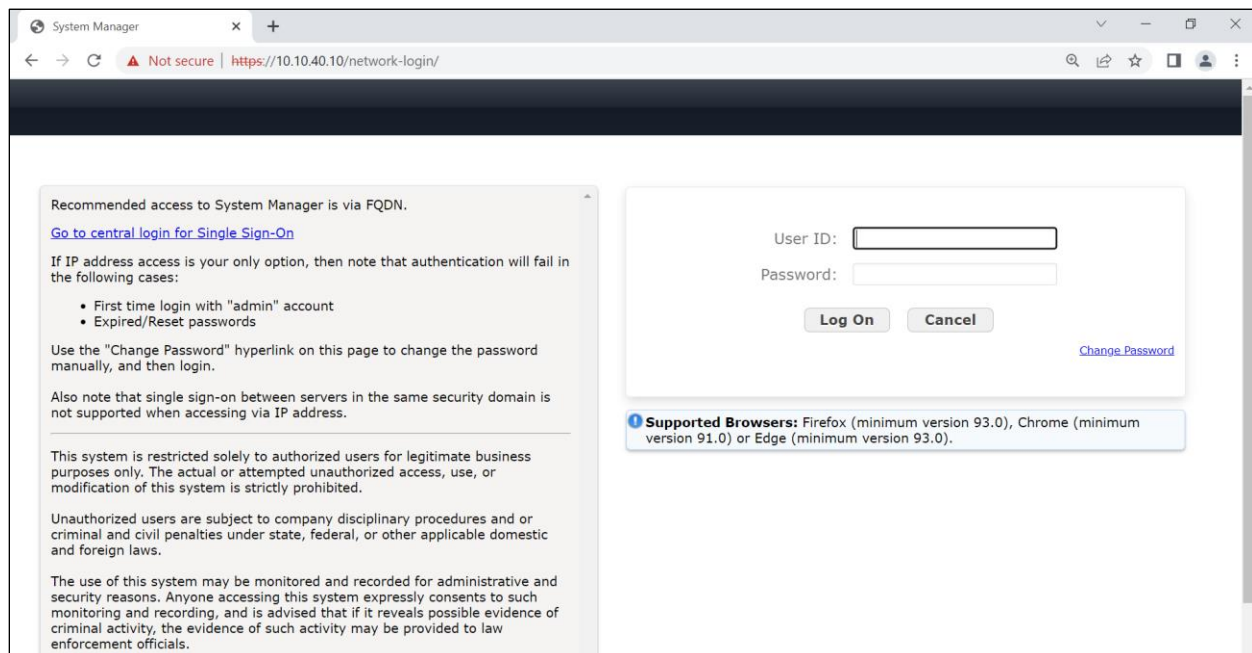
add cti-link 1		Page 1 of 3
		CTI LINK
CTI Link: 1		
Extension: 1990		
Type: ADJ-IP		
		COR: 1
Name: aespri101x		

6. Configuring Avaya Aura® Session Manager

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

- Domains and Locations
- Configure SIP Entity
- Configure Entity Link
- Configure Routing Policy
- Configure Dial Pattern

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**.



The screenshot shows a web browser window with the address bar displaying "https://10.10.40.10/network-login/". The page title is "System Manager". The main content area is divided into two sections. On the left, there is a text block with the following information: "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. Unauthorized users are subject to company disciplinary procedures and or criminal and civil penalties under state, federal, or other applicable domestic and foreign laws. The use of this system may be monitored and recorded for administrative and security reasons. Anyone accessing this system expressly consents to such monitoring and recording, and is advised that if it reveals possible evidence of criminal activity, the evidence of such activity may be provided to law enforcement officials." On the right, there is a login form with fields for "User ID:" and "Password:". Below the fields are "Log On" and "Cancel" buttons. A "Change Password" link is also present. At the bottom of the login form, there is a note about supported browsers: "Supported Browsers: Firefox (minimum version 93.0), Chrome (minimum version 91.0) or Edge (minimum version 93.0)."

Once logged in, navigate to **Elements** and click on **Routing** at the bottom of the screen below.

The screenshot displays the Avaya Aura System Manager 10.1 dashboard. The top navigation bar includes 'Users', 'Elements', 'Services', 'Widgets', and 'Shortcuts'. The 'Elements' menu is open, showing a list of system components. The 'Routing' option is highlighted, and a sub-menu is visible with 'Domains' and 'Locations' options. The background shows various widgets: 'Disk Space Utilization' with a bar chart, 'Alarms' with a gauge, 'Notifications (2)' with two messages, and 'Information' with a table of system elements.

Category	Value
opt	~15
var	~10
emdata	~15
tmp	~5
perdata	~25

Severity	Count
Critical	0
Major	0
Indeterminate	0
Minor	0
Warning	0

1	Your last successful login was on at 10 November 2022 16:08 from 10.10.40.242. More...
2	No Session Manager emergency Dial Pattern routes are administered. More...

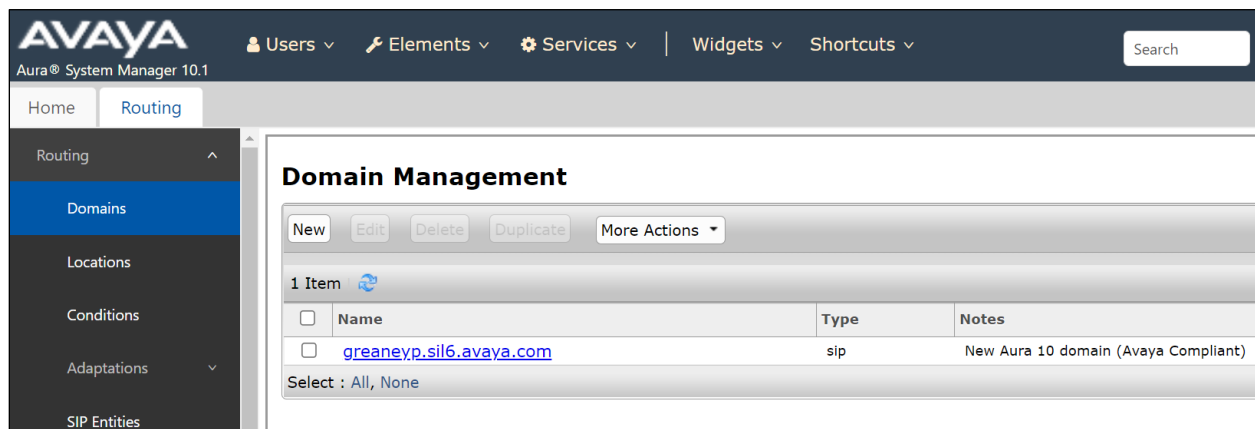
Elements	Count	Sync Statuc
Avaya Breeze	3	■
CM	1	■
Session Manager	1	■
Manager	1	■
Applications	8	■

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.

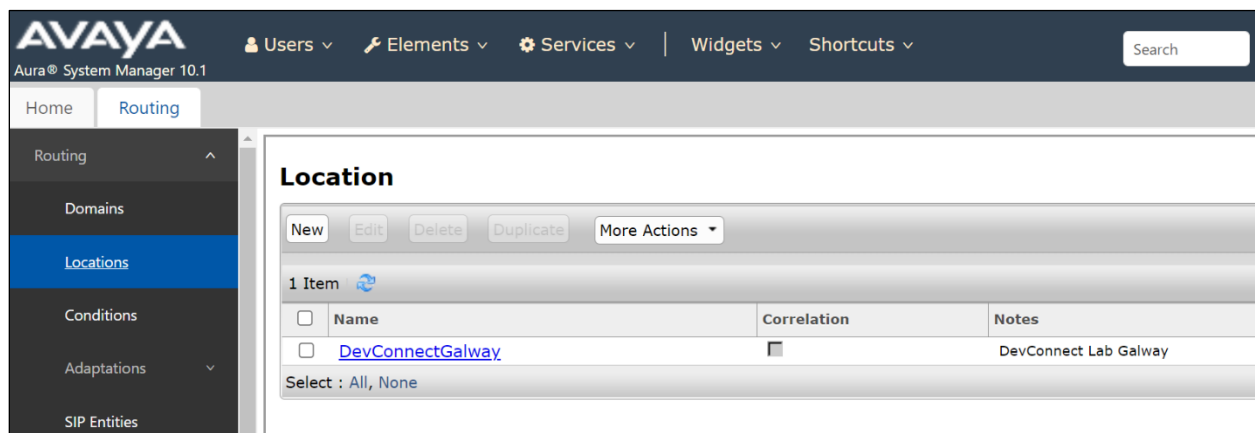
6.1.1. Display the Domain

Select **Domains** from the left window. This will display the domain configured on Session Manager. For compliance testing this domain was **greaney.sil6.avaya.com** 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.



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 **DevConnectGalway** 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.



6.2. Configure Eyerys SIP Entity and Entity Link

Each SIP device (other than Avaya SIP phones) that communicates with Session Manager requires a SIP Entity and Entity Link configuration.

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

The screenshot shows the Avaya Aura System Manager 10.1 interface. The left sidebar has a menu with 'Routing' selected, and 'SIP Entities' is highlighted. The main area displays a table of 11 SIP Entities. The table has columns for Name, FQDN or IP Address, Type, and Notes. The entities listed are: AA Messaging VZ, CM71vmppg, CM80vmppg, CS1KPG1, EP72vmppg, EP_Oceana, SM80vmppg, StephensCM, and StevesEP. The 'Type' column shows various roles like SIP Trunk, CM, Voice Portal, and Session Manager.

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

Enter a suitable **Name** for the new SIP Entity and the **IP Address** of the Eyerys server. Set **Type** to **SIP Trunk**. Enter the correct **Time Zone** and **Location** and scroll down to SIP Entity Links.

The screenshot shows the 'SIP Entity Details' form in the Avaya Aura System Manager 10.1 interface. The form is titled 'SIP Entity Details' and has a 'General' tab. The form fields are: Name (Eyerys), FQDN or IP Address (10.10.40.123), Type (SIP Trunk), Notes (Eyerys - UDP connection), Adaptation (empty), Location (DevConnectGalway), Time Zone (Europe/Dublin), SIP Timer B/F (in seconds) (4), Minimum TLS Version (Use Global Setting), Credential name (empty), Securable (unchecked), and Call Detail Recording (egress). The form also has a 'Loop Detection' section at the bottom.

SIP Entity Details

General

* Name: Eyerys

* FQDN or IP Address: 10.10.40.123

Type: SIP Trunk

Notes: Eyerys - UDP connection

Adaptation:

Location: DevConnectGalway

Time Zone: Europe/Dublin

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

Minimum TLS Version: Use Global Setting

Credential name:

Securable: ☐

Call Detail Recording: egress

Loop Detection

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

Upon scrolling down to **Entity Links**, click on **Add**. Enter a suitable **Name** for the Entity Link and select the Session Manager SIP Entity for **SIP Entity 1** and the newly created Eyerys SIP 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.

Entity Links
Override Port & Transport with DNS SRV: ☐

AddRemove

1 Item

Filter: Enable

<input type="checkbox"/>	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Deny New Service
<input type="checkbox"/>	* sm101x_Eyerys_5060_U	sm101x	UDP	* 5060	Eyerys	* 5060	trusted	<input type="checkbox"/>

Select : All, None

SIP Responses to an OPTIONS Request

AddRemove

0 Items

Filter: Enable

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

CommitCancel

6.3. Configure Routing Policy for Eyerys

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

	Name	Disabled	Retries	Destination	Notes
<input type="checkbox"/>	To AA Messaging VZ	<input type="checkbox"/>	0	AA Messaging V7	To AA Messaging V7
<input type="checkbox"/>	To ASCBE	<input type="checkbox"/>	0	ASBCE8vmppg	To Session Border Controller
<input type="checkbox"/>	To Capita DMS	<input type="checkbox"/>	0	Capita DMS	To Capita DMS
<input type="checkbox"/>	To Capita DS3000	<input type="checkbox"/>	0	Capita DS3000	To Capita DS3000
<input type="checkbox"/>	To CM71vmppg	<input type="checkbox"/>	0	CM71vmppg	To CM71vmppg
<input type="checkbox"/>	To CM80vmppg	<input type="checkbox"/>	0	CM80vmppg	To CM80vmppg
<input type="checkbox"/>	To CS1KPG1	<input type="checkbox"/>	0	CS1KPG1	To CS1KPG1
<input type="checkbox"/>	To EP72vmppg	<input type="checkbox"/>	0	EP72vmppg	To EP72vmppg
<input type="checkbox"/>	To EP Oceana	<input type="checkbox"/>	0	EP_Oceana	To EP Oceana
<input type="checkbox"/>	To Stephens CM	<input type="checkbox"/>	0	StephensCM	To StephensCM
<input type="checkbox"/>	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**, shown below.

Routing Policy Details [Commit] [Cancel]

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
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 the **Eyerys** SIP Entity as shown and click on **Select**.

SIP Entities
Select Cancel

SIP Entities

17 Items
Filter: Enable

	Name	FQDN or IP Address	Type	Notes
<input type="radio"/>	AACC	10.10.40.96	SIP Trunk	
<input type="radio"/>	breeze1wspaces	10.10.40.52	Avaya Breeze	Breeze 1 for wspaces
<input type="radio"/>	breeze2wspaces	10.10.40.53	Avaya Breeze	Breeze 2 for wspaces
<input type="radio"/>	breeze3wspaces	10.10.40.54	Avaya Breeze	Breeze 3 for wspaces
<input type="radio"/>	cm101x - Phones - 5061	10.10.40.13	CM	For SIP PHONES on CM
<input type="radio"/>	cm101x - SIM PSTN - 5063	10.10.40.13	CM	For Simulated SIP Trunk
<input type="radio"/>	cm101x - SIP TRUNK - 5062	10.10.40.13	CM	SIP Trunk in and out
<input type="radio"/>	Experience Portal-MPP	10.10.40.26	Voice Portal	Experience Portal
<input checked="" type="radio"/>	Eyerys	10.10.40.123	SIP Trunk	Eyerys - UDP connection
<input type="radio"/>	InAttend	10.10.40.122	SIP Trunk	Mitel InAttend
<input type="radio"/>	IP Office - SE	10.10.40.19	SIP Trunk	IP Office Server Edition
<input type="radio"/>	Messaging10x	10.10.40.76	SIP Trunk	Messaging R10 on 2016
<input type="radio"/>	Messaging11x	10.10.40.77	SIP Trunk	Messaging R11x on Win 2016 & 2019
<input type="radio"/>	novaalert	10.10.40.120	SIP Trunk	novaalert

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

Routing Policy Details
Commit Cancel

General

*** Name:**

Disabled: ☐

*** Retries:**

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
Eyerys	10.10.40.123	SIP Trunk	Eyerys - UDP connection

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

6.4. Configure Eyerys Dial Patterns

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

Pattern	Min	Max	Emergency Call	Emergency Type	Emergency Priority	SIP Domain	Notes
09173	9	9	<input type="checkbox"/>			-ALL-	To CM80vmpg from Syntec
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
351212455779	12	12	<input type="checkbox"/>			-ALL-	To SBC8 for Syntec
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
7080	4	6	<input type="checkbox"/>			devconnect.local	To Capita DMS
8000	5	5	<input type="checkbox"/>			devconnect.local	To Capita DS3000
823	7	7	<input type="checkbox"/>			devconnect.local	To Stephens CM 823 000x

Enter the required digits for the Routing Pattern, in the example below **600** is used. This ensures that when 600x is dialled it will route to the Eyerys. Enter the appropriate domain for **SIP Domain** in this example the domain created in **Section 6.2** is added. Click on **Add** under **Originating Locations and Routing Policies** to select this Routing Policy.

Dial Pattern Details [Commit] [Cancel]

General

* **Pattern:** 600

* **Min:** 4

* **Max:** 4

Emergency Call: ☐

SIP Domain: greaney.sil6.avaya.com

Notes: 600x to Eyerys

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

Select : All, None

Select the **Originating Location**, this will be the location added in **Section 6.1.2**, then scroll down to select the appropriate Routing Policy for Eyerys. Select the newly created Routing Policy for Eyerys.

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"/>	DevConnectGalway	DevConnect Lab Galway

Select : All, None

Routing Policies

13 Items

Filter: Enable

<input type="checkbox"/>	Name	Disabled	Destination	Notes
<input type="checkbox"/>	To AACC	<input type="checkbox"/>	AACC	To AACC
<input type="checkbox"/>	To cm101x - SIM PSTN	<input type="checkbox"/>	cm101x - SIM PSTN - 5063	Calls from SIM PSTN
<input type="checkbox"/>	To cm101x - SIP Phones	<input type="checkbox"/>	cm101x - Phones - 5061	Route to CM101x - SIP Phones
<input type="checkbox"/>	To cm101x - SIP Trunk	<input type="checkbox"/>	cm101x - SIP TRUNK - 5062	Route to CM101x - SIP Trunk
<input type="checkbox"/>	ToEP810	<input type="checkbox"/>	Experience Portal-MPP	ToEP810
<input checked="" type="checkbox"/>	To Eyerys	<input type="checkbox"/>	Eyerys	Calls to Eyerys SIP Entity
<input type="checkbox"/>	To InAttend	<input type="checkbox"/>	InAttend	To InAttend

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

Dial Pattern Details

Commit Cancel

General

* Pattern: 600

* Min: 4

* Max: 4

Emergency Call: ☐

SIP Domain: greaney.sil6.avaya.com

Notes: 600x to Eyerys

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"/>	DevConnectGalway	DevConnect Lab Galway	To Eyerys	0	<input type="checkbox"/>	Eyerys	Calls to Eyerys SIP Entity

Select : All, None

7. Configure Avaya Aura® Application Enablement Services

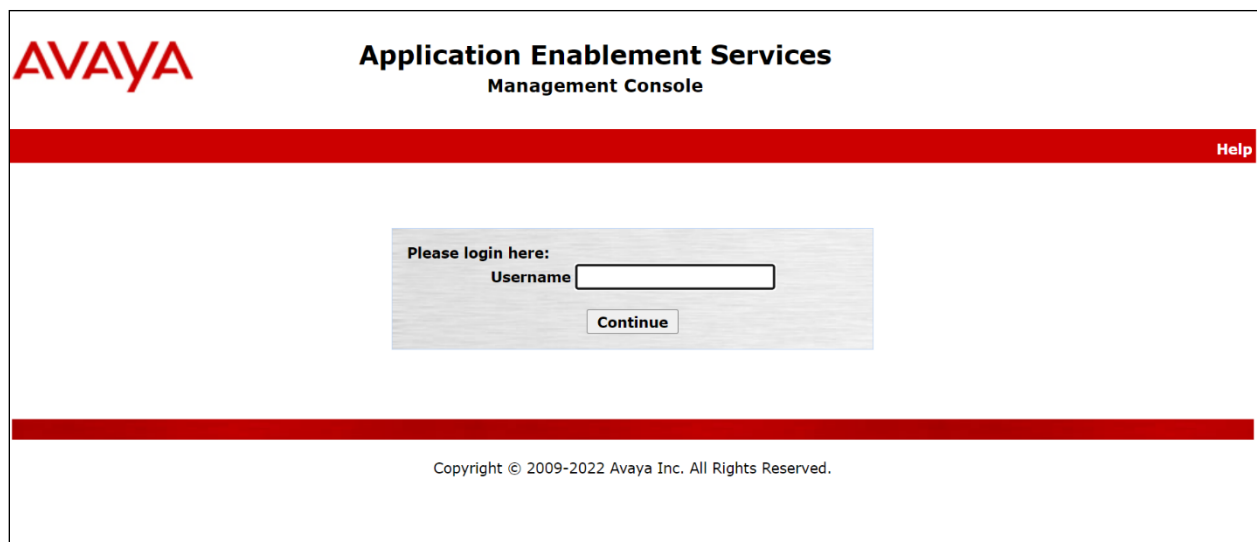
This section provides the procedures for configuring Application Enablement Services. The procedures fall into the following areas:

- Verify Licensing
- Create CTI User
- Enable Unrestricted Access for CTI User
- Configure Networking Ports
- Display Switch Information

Note: It is assumed that a connection between Application Enablement Services and Communication Manager is already in place including the setup of the H.323 Gatekeeper.

7.1. Verify Licensing

To access the maintenance console, enter **https://<ip-addr>** as the URL in an Internet browser, where <ip-addr> is the active IP address of AES. The login screen is displayed, log in with the appropriate credentials and then select the **Login** button.



The screenshot shows the Avaya Application Enablement Services Management Console login interface. At the top left is the Avaya logo. To its right, the text "Application Enablement Services" and "Management Console" is displayed. A red horizontal bar spans the width of the page, with a "Help" link on the right. Below this bar is a central login box with the text "Please login here:" followed by a "Username" label and a text input field. A "Continue" button is positioned below the input field. At the bottom of the page, another red horizontal bar is present, with the copyright notice "Copyright © 2009-2022 Avaya Inc. All Rights Reserved." centered below it.

The Application Enablement Services Management Console appears displaying the **Welcome to OAM** screen (not shown). Select **AE Services** and verify that the **TSAPI Service** and **DMCC Service** are licensed by ensuring that the **License Mode** is showing **NORMAL MODE**.

The screenshot shows the 'AE Services' page in the Application Enablement Services Management Console. The left sidebar contains a navigation menu with options like CVLAN, DLG, DMCC, SMS, TSAPI, TWS, Communication Manager Interface, High Availability, Licensing, Maintenance, Networking, Security, Status, User Management, Utilities, and Help. The 'Licensing' option is highlighted. The main content area displays the 'AE Services' page, which includes a table of services and their license modes.

Service	Status	State	License Mode	Cause*
ASAI Link Manager	N/A	Running	N/A	N/A
CVLAN Service	OFFLINE	Running	N/A	N/A
DLG Service	OFFLINE	Running	N/A	N/A
DMCC Service	ONLINE	Running	NORMAL MODE	N/A
TSAPI Service	ONLINE	Running	NORMAL MODE	N/A
Transport Layer Service	N/A	Running	N/A	N/A
AE Services HA	Not Configured	N/A	N/A	N/A

For status on actual services, please use [Status and Control](#)

* -- For more detail, please mouse over the Cause, you'll see the tooltip, or go to help page.

License Information
You are licensed to run Application Enablement (CTI) release 8.x

The TSAPI and DMCC licenses are user licenses issued by the Web License Manager to which the Application Enablement Services server is pointed to. From the left window open **Licensing** and click on **WebLM Server Access** as shown below.

The screenshot shows the 'Licensing' page in the Application Enablement Services Management Console. The left sidebar contains a navigation menu with options like AE Services, Communication Manager Interface, High Availability, Licensing, WebLM Server Address, WebLM Server Access, Reserved Licenses, Maintenance, Networking, Security, Status, User Management, Utilities, and Help. The 'Licensing' option is highlighted. The main content area displays the 'Licensing' page, which includes instructions on how to set up and maintain the WebLM, and how to import, set up, and maintain the license.

Licensing

If you are setting up and maintaining the WebLM, you need to use the following:

- WebLM Server Address

If you are importing, setting up and maintaining the license, you need to use the following:

- WebLM Server Access

If you want to administer TSAPI Reserved Licenses or DMCC Reserved Licenses, you need to use the following:

- Reserved Licenses

NOTE: Please disable your pop-up blocker if you are having difficulty with opening this page

The following screen shows the available licenses for **TSAPI** and **DMCC** users.

▼ Application_Enablement

View license capacity

View peak usage

ASBCE

▶ Session_Border_Controller_E_AE

AVAYA_OCEANA

▶ Avaya_Oceana

CCTR

▶ ContactCenter

CE

▶ COLLABORATION_ENVIRONMENT

COLLABORATION_DESIGNER

▶ Collaboration_Designer

COLLABORATIVE_BROWSING_SNAP-IN

▶ Collaborative_Browsing_Snap_In

COMMUNICATION_MANAGER

▶ Call_Center

▶ Communication_Manager

License File Host IDs:

Licensed Features

10 Items Show All ▼

Feature (License Keyword)	Expiration date	Licensed capacity
Unified CC API Desktop Edition VALUE_AES_AEC_UNIFIED_CC_DESKTOP	permanent	44
CVLAN ASAI VALUE_AES_CVLAN_ASAI	permanent	44
Device Media and Call Control VALUE_AES_DMCC_DMC	permanent	44
AES ADVANCED SMALL SWITCH VALUE_AES_AEC_SMALL_ADVANCED	permanent	4
DLG VALUE_AES_DLG	permanent	44
TSAPI Simultaneous Users VALUE_AES_TSAPI_USERS	permanent	44
AES ADVANCED LARGE SWITCH VALUE_AES_AEC_LARGE_ADVANCED	permanent	4
CVLAN Proprietary Links VALUE_AES_PROPRIETARY_LINKS	permanent	44

7.2. Create CTI User

A User ID and password needs to be configured for the Eyerys server to communicate with the Application Enablement Services. Navigate to the **User Management** → **User Admin** and choose the **Add User** option (not shown). In the **Add User** screen shown below, enter the following values:

- **User Id** - This will be used by Eyerys in **Section 8**.
- **Common Name** and **Surname** - Descriptive names need to be entered.
- **User Password** and **Confirm Password** - This will be used with the **User Id** in **Section 8**.
- **CT User** - Select **Yes** from the drop-down menu.

Complete the process by choosing **Apply** at the bottom of the screen.

Edit User	
* User Id	<input type="text" value="smoke"/>
* Common Name	<input type="text" value="smoke"/>
* Surname	<input type="text" value="smoke"/>
User Password	<input type="password"/>
Confirm Password	<input type="password"/>
Admin Note	<input type="text"/>
Avaya Role	<input type="text" value="None"/>
Business Category	<input type="text"/>
Car License	<input type="text"/>
CM Home	<input type="text"/>
Css Home	<input type="text"/>
CT User	<input type="text" value="Yes"/>
Department Number	<input type="text"/>
Display Name	<input type="text"/>
Employee Number	<input type="text"/>
Employee Type	<input type="text"/>
Enterprise Handle	<input type="text"/>
Given Name	<input type="text"/>
Home Phone	<input type="text"/>
Home Postal Address	<input type="text"/>

7.3. Enable Unrestricted Access for CTI User

Navigate to the **CTI Users** screen by selecting **Security** → **Security Database** → **CTI Users** → **List All Users**. Select the user that was created in **Section 7.2** and select the **Edit** button.

Maintenance	<input type="radio"/> beta80	beta80	NONE	NONE
Networking	<input type="radio"/> capita	capita	NONE	NONE
Security	<input type="radio"/> emc66x	emc66x	NONE	NONE
Account Management	<input type="radio"/> Enghouse	Enghouse	NONE	NONE
Audit	<input type="radio"/> inisoft	inisoft	NONE	NONE
Certificate Management	<input type="radio"/> messaging	messaging	NONE	NONE
Enterprise Directory	<input type="radio"/> mitel	mitel	NONE	NONE
Host AA	<input type="radio"/> nice	nice	NONE	NONE
PAM	<input type="radio"/> nice1	nice1	NONE	NONE
Security Database	<input type="radio"/> Oceana	Oceana	NONE	NONE
Control	<input type="radio"/> opentextaes	opentextaes	NONE	NONE
CTI Users	<input type="radio"/> paul	Paul	NONE	NONE
List All Users	<input type="radio"/> paul1	paul1	NONE	NONE
Search Users	<input type="radio"/> presence	presence	NONE	NONE
Devices	<input checked="" type="radio"/> smoke	smoke	NONE	NONE
Device Groups	<input type="radio"/> wspaces37	wspaces37	NONE	NONE
Tlinks	<input type="radio"/> wspaces38	wspaces38	NONE	NONE
Tlink Groups				
Worktops				
Session Timeouts				
Standard Reserved Ports				
Tripwire Properties				
Status				
User Management				
Utilities				

The **Edit CTI User** screen appears. Check the **Unrestricted Access** box and **Apply Changes** at the bottom of the screen. Note that DevConnect would not recommend giving unrestricted access as this may be a security risk, but was set specifically for ease of compliance testing.

Edit CTI User

User Profile:

User ID
Common Name
Worktop Name
Unrestricted Access

smoke
smoke
NONE
☒

Call and Device Control:

Call Origination/Termination and Device Status

None

Call and Device Monitoring:

Device Monitoring
Calls On A Device Monitoring
Call Monitoring

None
None
☐

Routing Control:

Allow Routing on Listed Devices

None

Apply Changes

Cancel Changes


7.4. Configure Networking Ports

To ensure that TSAPI and DMCC ports are enabled, navigate to **Networking → Ports**. Ensure that the TSAPI ports are set to **Enabled** as shown below. Ensure that the **DMCC Server Ports** are also **Enabled** and take note of the **Encrypted Port 4722** which will be used later in **Section 8**.

<div>Communication Manager Interface</div> <div>High Availability</div> <div>Licensing</div> <div>Maintenance</div> <div>▼ Networking</div> <div>AE Service IP (Local IP)</div> <div>Network Configure</div> <div>Ports</div> <div>TCP/TLS Settings</div> <div>Security</div> <div>Status</div> <div>User Management</div> <div>Utilities</div> <div>Help</div>	Ports			
	CVLAN Ports		Enabled Disabled	
	Unencrypted TCP Port	9999	<input checked="" type="radio"/>	<input type="radio"/>
	Encrypted TCP Port	<input type="text" value="9998"/>	<input checked="" type="radio"/>	<input type="radio"/>
	<hr/>			
	DLG Port	TCP Port	5678	
	<hr/>			
	TSAPI Ports		Enabled Disabled	
	TSAPI Service Port	450	<input checked="" type="radio"/>	<input type="radio"/>
	Local TLINK Ports			
	TCP Port Min	1024		
	TCP Port Max	1039		
	Unencrypted TLINK Ports			
	TCP Port Min	<input type="text" value="1050"/>		
	TCP Port Max	<input type="text" value="1065"/>		
Encrypted TLINK Ports				
TCP Port Min	<input type="text" value="1066"/>			
TCP Port Max	<input type="text" value="1081"/>			
<hr/>				
DMCC Server Ports		Enabled Disabled		
Unencrypted Port	<input type="text" value="4721"/>	<input checked="" type="radio"/>	<input type="radio"/>	
Encrypted Port	<input type="text" value="4722"/>	<input checked="" type="radio"/>	<input type="radio"/>	
TR/87 Port	<input type="text" value="4723"/>	<input checked="" type="radio"/>	<input type="radio"/>	
<hr/>				
H.323 Ports				
TCP Port Min	<input type="text" value="20000"/>			
TCP Port Max	<input type="text" value="29999"/>			
Local UDP Port Min	<input type="text" value="20000"/>			

7.5. Display Switch Information

The name and IP address of Communication Manager will be needed for the configuration of Eversys in **Section 8**. Navigate to **Communication Manager Interface → Switch Connections** in the left window and note the **Connection Name** in the main window. Selecting the appropriate name and clicking on **Edit PE/CLAN IPs** will open a window for the IP address information.



Application Enablement Services
Management Console

Welcome: User cust
Last login: Fri Sep 9 17:54:25 2022 from 192.168.40.240
Number of prior failed login attempts: 0
HostName/IP: aespri101x/10.10.40.16
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 10.1.0.1.0.7-0
Server Date and Time: Tue Sep 20 15:52:43 IST 2022
HA Status: Not Configured

Communication Manager Interface | Switch Connections

Home | Help | Logout

AE Services

Communication Manager Interface

Switch Connections

Dial Plan

High Availability

Licensing

Maintenance

Networking

Switch Connections

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections
<input checked="" type="radio"/> cm101x	Yes	30	1

The IP address of Communication Manager is displayed below.

Communication Manager Interface | Switch Connections

Home | Help | Logout

AE Services

Communication Manager Interface

Switch Connections

Dial Plan

High Availability

Licensing

Maintenance

Edit Processor Ethernet IP - cm101x

Name or IP Address	Status
10.10.40.13	In Use

Clicking on **Edit Signaling Details** (from the screen at the top of the page) brings up the H.323 Gatekeeper page. The IP address of Communication Manager is set for the **H.323 Gatekeeper**, as shown below.

Communication Manager Interface | Switch Connections

▶ AE Services
▼ **Communication Manager Interface**
Switch Connections
▶ Dial Plan
High Availability
▶ Licensing
▶ Maintenance
▶ Networking

Switch Connections

Edit H.323 Gatekeeper - cm101x

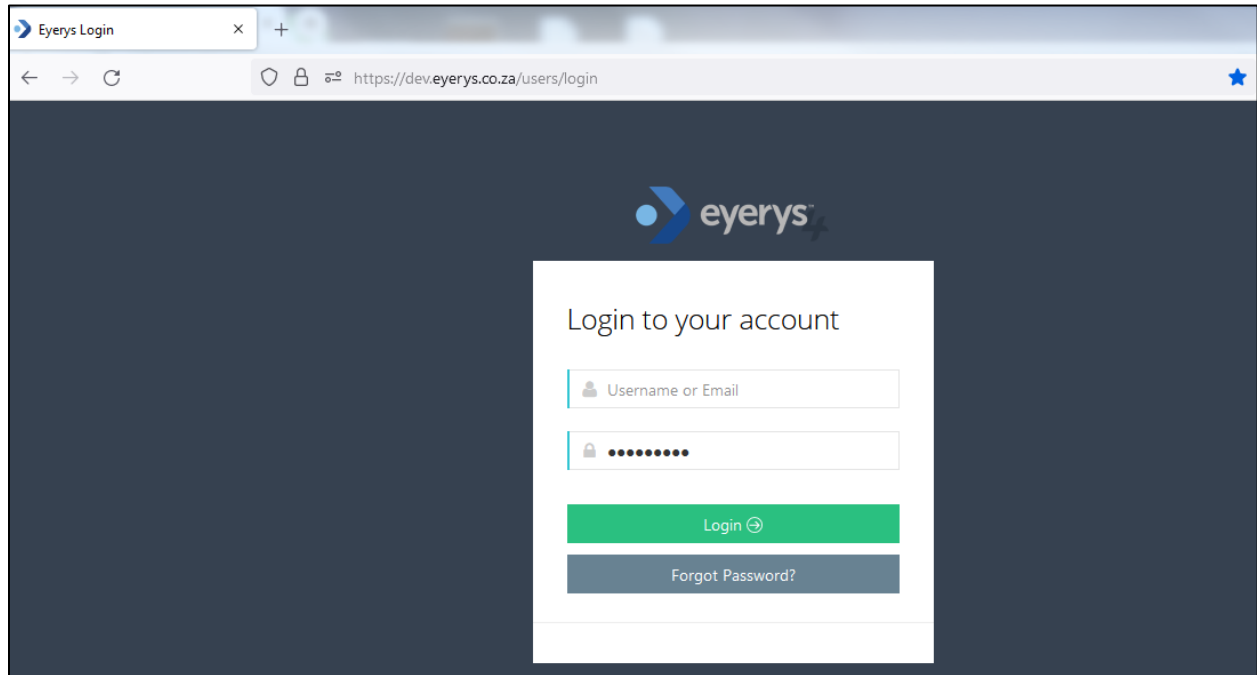
Name or IP Address

☒ 10.10.40.13

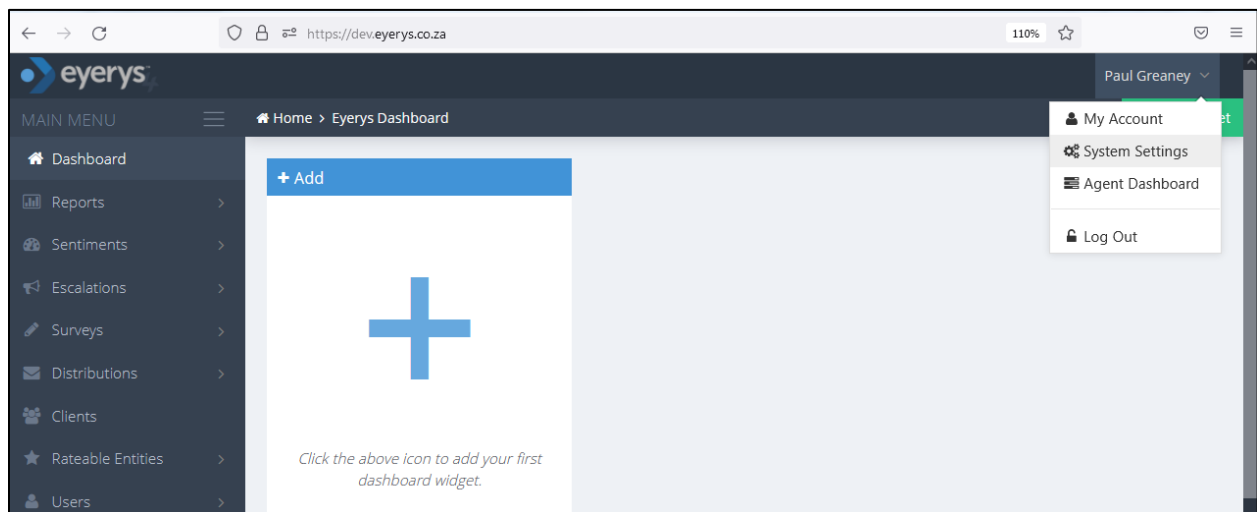
8. Configure Eyerys IVR Connector

The Eyerys server was configured and provided by Smoke Customer Intelligence Pty Ltd. An outline of the configuration relevant to the Avaya solution integration is detailed below.

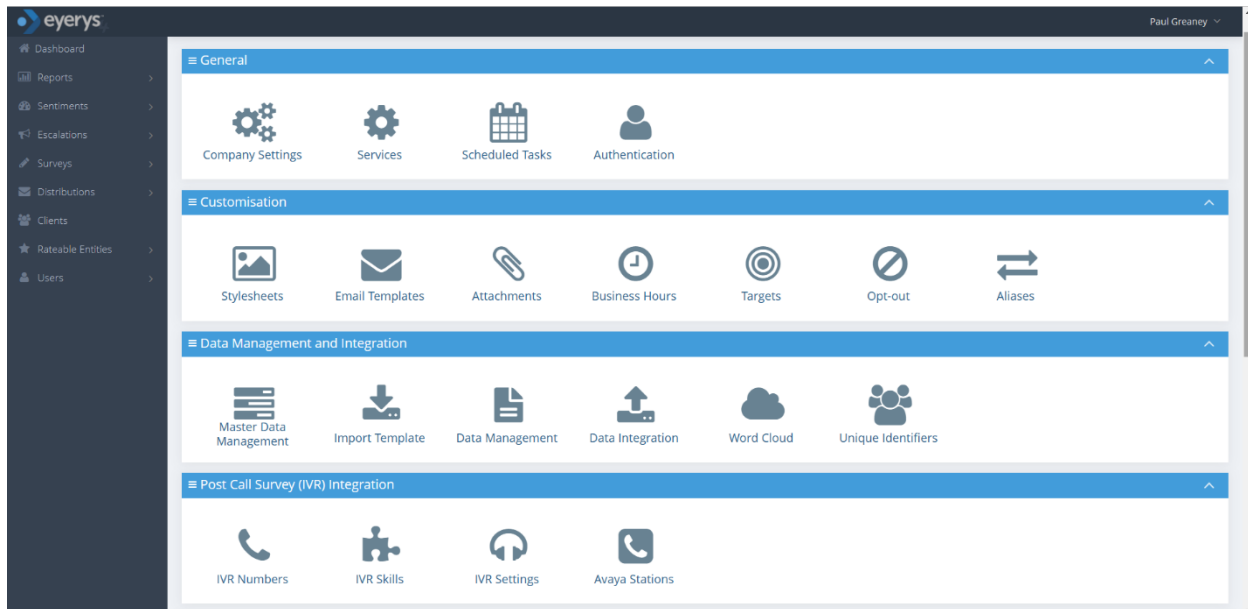
Open a URL to *https://{your_company_name}.eyerys.co.za/users/login* as shown below. Enter the appropriate credentials and click on **Login**.



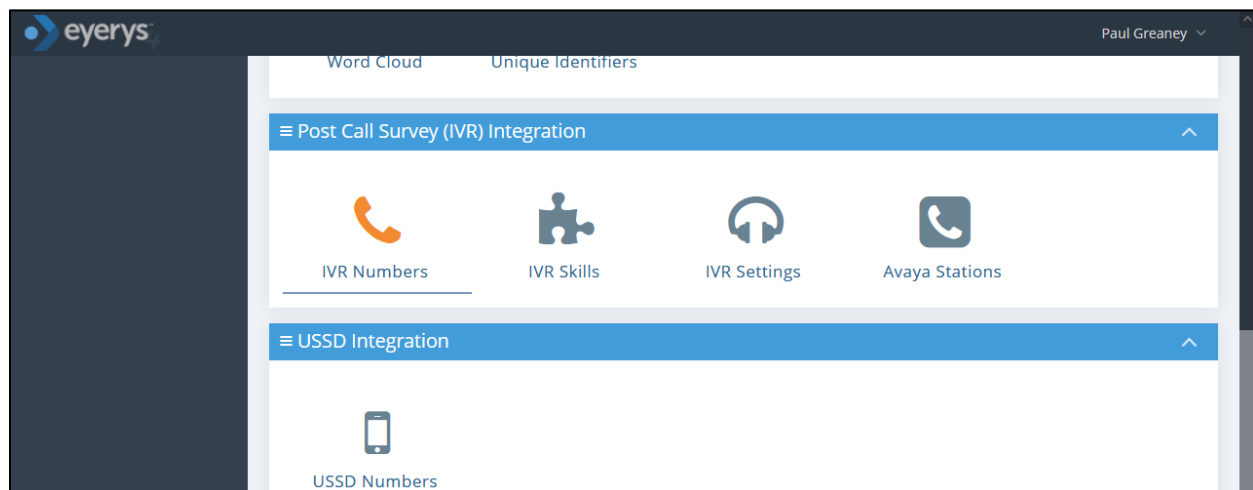
Once logged in, click on **System Settings** (top right of screen) as shown below.



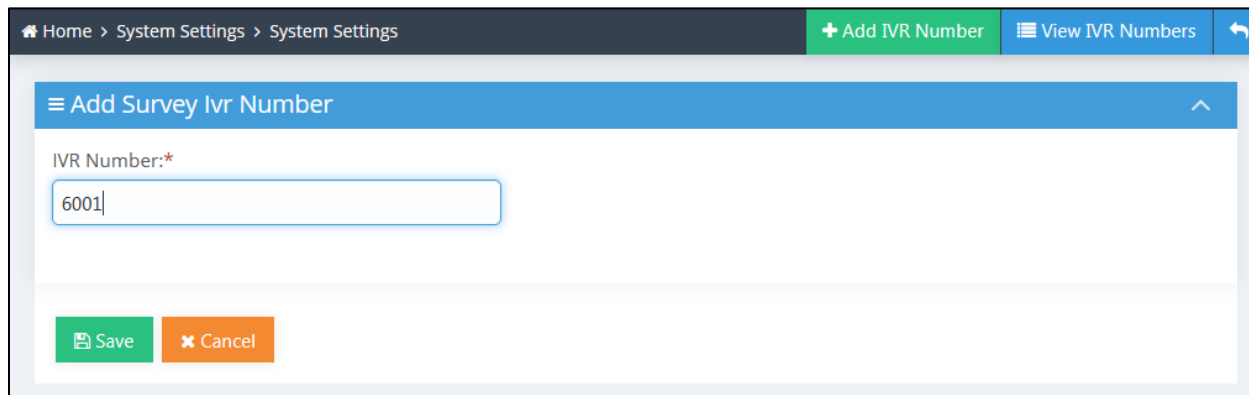
The following screen is displayed where various components can be set.



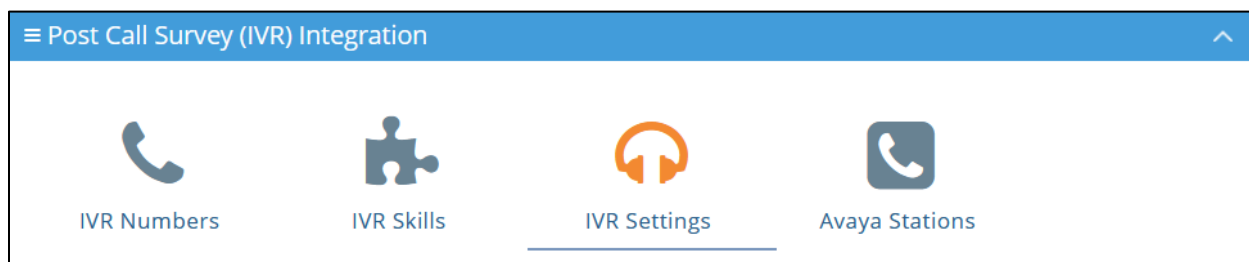
The settings that are relevant to the Avaya connection are all under the **Post Call Survey (IVR) Integration**. Scroll down to these icons, as shown below, **IVR Numbers** can be added for each survey that needs to be run. For compliance testing 6001 to 6004 were used for different surveys that took place.



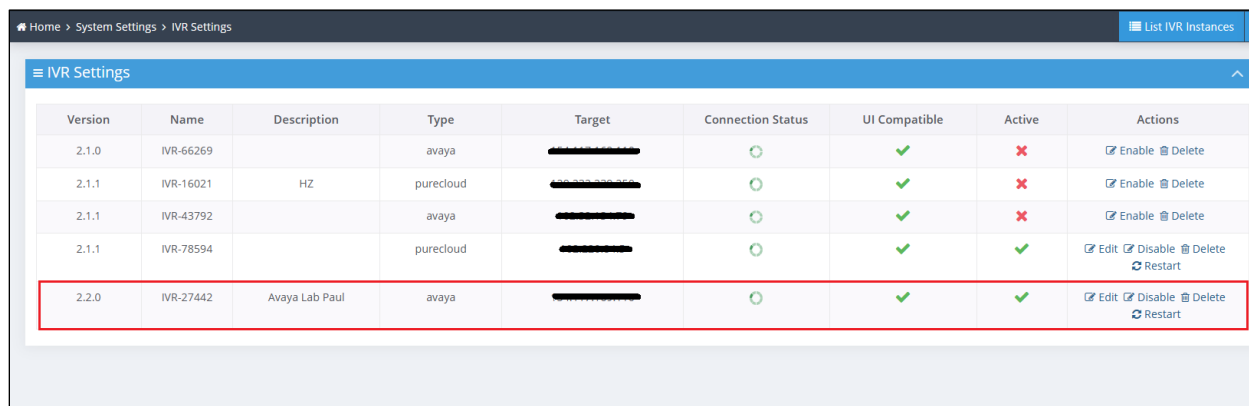
The example below shows the number **6001** being added, simply enter the number and click on **Save**.



The IVR settings contains all the configuration on the connections to both Session Manager and Application Enablement Services. Click on the **IVR Settings** icon as shown below.



There are a number of connections displayed, the IVR connection for compliance testing is highlighted and clicking on **Edit** will display the configuration.



Version	Name	Description	Type	Target	Connection Status	UI Compatible	Active	Actions
2.1.0	IVR-66269		avaya	██████████	🟢	✓	✗	🔗 Enable 🗑 Delete
2.1.1	IVR-16021	HZ	purecloud	██████████	🟢	✓	✗	🔗 Enable 🗑 Delete
2.1.1	IVR-43792		avaya	██████████	🟢	✓	✗	🔗 Enable 🗑 Delete
2.1.1	IVR-78594		purecloud	██████████	🟢	✓	✓	🔗 Edit 🗑 Disable 🗑 Delete 🔄 Restart
2.2.0	IVR-27442	Avaya Lab Paul	avaya	██████████	🟢	✓	✓	🔗 Edit 🗑 Disable 🗑 Delete 🔄 Restart

Under the area named **General**, a **Name** and **Description** can be added, there are a number of configuration details listed on this page but they are viewed by scrolling down through the page.

The **SIP Settings** displays the **Port** and **Protocol** that were used for compliance testing and these will match the SIP Entity information from **Section 6.2**. The **Realm** information will match that of **Section 6.1** and the **DTMF Mode** is set to that of **Section 5.2**.

≡ IVR-27442 v2.2.0

General

Name

IVR-27442

Description

Avaya Lab Paul

Version

2.2.0

IVR Active

✓

URL

154.117.169.110

Restart Connector

SIP Settings

Bind Address ?

0.0.0.0

IVR Connection Server Local Net IP ?

10.10.40.0

IVR Connection Server Local Subnet Mask ?

255.255.255.0

IVR Connection Server External IP ?

10.10.40.123

Bind Port ?

5060

Protocol ?

UDP

NAT ?

No

Realm ?

greanep.sil6.avaya.com

DTMF Mode ?

rfc2833

Scrolling down.... The **Codecs** and order can be chosen. The **Codecs** set here should negotiate with the Codecs in **Section 5.2**.

Codecs ?

Search	Remove all	Search
g729	-	
Opus	-	
Alaw	-	
Ulaw	-	

4 items selected 0 items available

Scrolling down.... The **Survey Pause Times** are displayed, these are the values that were used for compliance testing.

Survey Pause Times

Pause Times are based in milliseconds (ms)

Pre Welcome Message Delay (ms) ?	Pre Error Delay (ms) ?
<input type="text" value="250"/>	<input type="text" value="250"/>
Pre Question Delay (ms) ?	Customer Response Time (ms) ?
<input type="text" value="250"/>	<input type="text" value="10000"/>
Pre Voicemail Delay (ms) ?	2 Digit Input Time (ms) ?
<input type="text" value="250"/>	<input type="text" value="5000"/>
Pre Goodbye Delay (ms) ?	Question Retry Limit ?
<input type="text" value="250"/>	<input type="text" value="5"/>

Save

Scroll down to **Avaya Settings** and the **AES** and **CM Settings** are displayed. The **AES IP Address** as well as the **Username** and **Password** from **Section 7.2**. The **Port** information should match that in **Section 7.4**.

≡ Avaya Settings

Avaya AES Settings

Hostname / IP Address

10.10.40.16

Encrypted Connection

Yes

Port

4722

Username

smoke

Password

Avaya1234%

Session Duration ?

120

Heartbeat Interval ?

73

Heartbeat Retry

2

Cleanup Interval ?

260

Scroll down further to the **Avaya CM Settings**. The **IP Address** and **CM Switch Name** are configured and should match that of **Section 7.5**.

Avaya CM Settings

Hostname / IP Address

10.10.40.13

CM Switch Name

cm101x

Stations Auto Monitor

Enable Station Auto Monitor ?

Yes

! Note:

You must click the Save button in this (Avaya Settings) section after adding or deleting Patterns to save your changes.
An unmonitored station will not be automatically monitored if a call is auto transferred from the unmonitored station.

Scrolling down further, to **SIP Trunks** shows the configuration settings for the connection to Session Manager. There is an existing connection present but a new connection can be made by clicking on **Add New Trunk**.

SIP Trunks				
				+ Add New Trunk
Friendly Name	Avaya Session Manager SIP IP Address	DTMF Mode	Direct Media	Actions
avaya	10.10.40.12	rfc2833	no	Edit Delete

A suitable **Name** is added as well as the **Session Manager SIP IP Address**. **DTMF Mode** and **Direct Media** can be set, the values shown are what were set for compliance testing. This is the final part of the IVR settings page, and **Save** can be clicked on once everything is filled out as required.

Add New SIP Trunk

Friendly Name

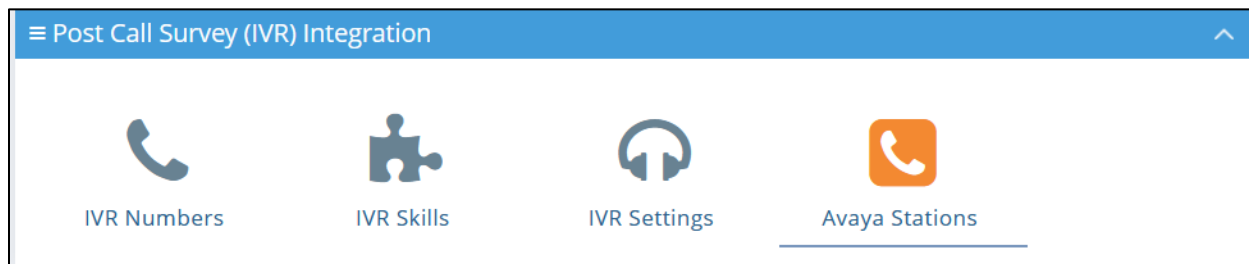
DTMF Mode ?

Avaya Session Manager SIP IP Address

Direct Media ?

[Save](#) [Cancel](#)

From the previous screen the Avaya Stations can be accessed as shown below.



Each station (extension) number can be added here with a brief description of each.

≡ Add Avaya Station

Station*

3050

Description

Digital phone

+ Add

≡ Avaya Stations

Station ID	Description	Created	Actions
3001	Station 3001	2023-02-28 11:22:41	Delete
3060	Station 3060	2023-02-28 11:22:54	Delete
3101	Station 3101	2023-02-28 11:23:06	Delete
50001		2022-10-04 11:16:14	Delete
50002		2022-10-20 12:00:12	Delete
50004		2022-10-19 10:50:12	Delete
50005		2022-10-04 11:16:31	Delete

Page 1 of 1, showing 7 records out of 7 total, starting on record 1, ending on 7

The screen below shows the three Communication Manager extensions that were monitored for compliance testing.

≡ Avaya Stations			
Station ID	Description	Created	Actions
3001	Station 3001	2023-02-28 11:22:41	Delete
3060	Station 3060	2023-02-28 11:22:54	Delete
3101	Station 3101	2023-02-28 11:23:06	Delete

Page 1 of 1, showing 7 records out of 7 total, starting on record 1, ending on 7

9. Verification Steps

This section provides the tests that can be performed to verify correct configuration of Communication Manager, Application Enablement Services and Eyeris.

9.1. Verify Avaya Aura® Application Enablement Services DMCC Connection

The following steps are carried out on AES to validate that the communication link between AES and the Eyeris is functioning correctly. Verify the status of the DMCC service by selecting **Status → Status and Control → DMCC Service Summary**. The **DMCC Service Summary – Session Summary** screen is displayed as shown below. It shows a connection to the Eyeris server, IP address 10.10.40.123. The **Application** is shown as **Eyeris Surveys Connector**, and the **Far-end Identifier** is given as the IP address **10.10.40.123** as expected. The **User** is shown as the user created for the CTI user for Eyeris.

Status | Status and Control | DMCC Service SummaryHome | Help | Logout

AE Services

Communication Manager

Interface

High Availability

Licensing

Maintenance

Networking

Security

Status

Alarm Viewer

Logs

Log Manager

Status and Control

CVLAN Service Summary

DLG Services Summary

DMCC Service Summary

Switch Conn Summary

TSAPI Service Summary

DMCC Service Summary - Session Summary

Please do not use back button

☒ Enable page refresh every 60 seconds

Session Summary [Device Summary](#)

Generated on Wed Feb 23 18:00:37 GMT 2023

Service Uptime: 12 days, 3 hours 34 minutes

Number of Active Sessions: 1

Number of Sessions Created Since Service Boot: 13

Number of Existing Devices: 7

Number of Devices Created Since Service Boot: 24

	Session ID	User	Application	Far-end Identifier	Connection Type	# of Associated Devices
<input type="checkbox"/>	51F454DC7B8F8BD21 D8B26D6A2AC2DF3-12	smoke	Eyeris Surveys Connector	10.10.40.123	XML Encrypted	7

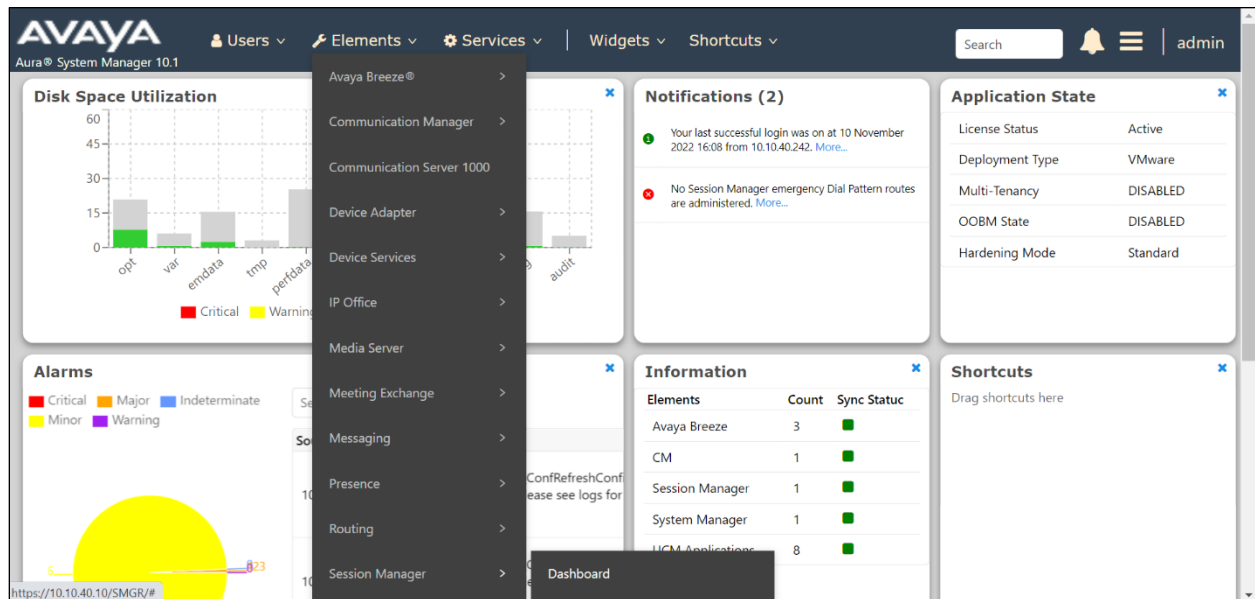
Terminate SessionsShow Terminated Sessions

Item 1-1 of 1

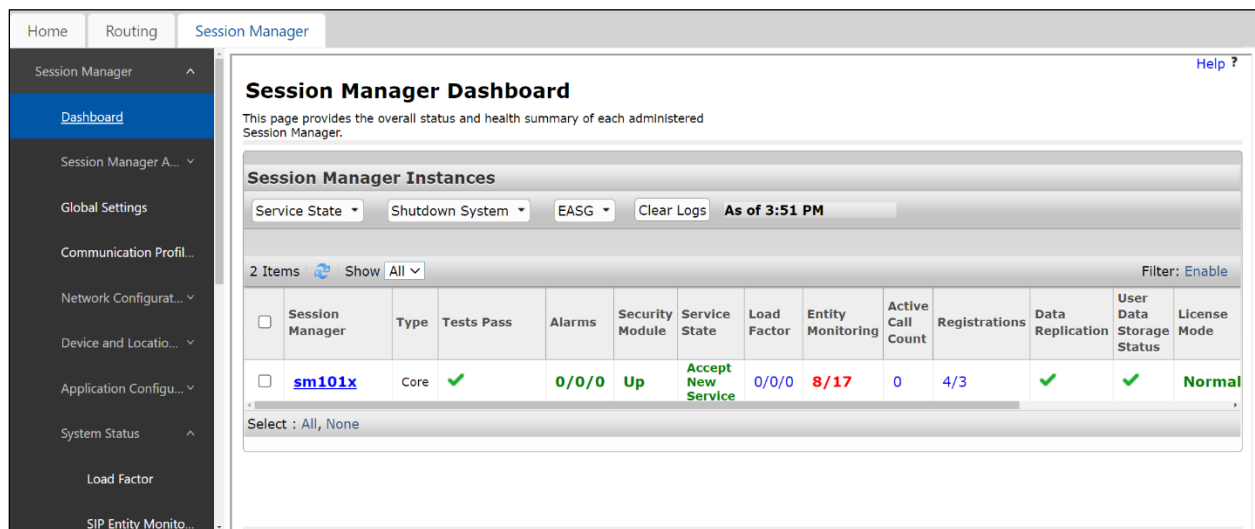
1Go

9.2. Verify Avaya Aura® Session Manager SIP Trunk connection

Log into System Manager as per **Section 6**. Navigate to **Elements** and click on **Session Manager**.



The following screen is displayed, from the left window navigate to **System Status** and select **SIP Entity Monitoring**.



Select the **Eyerys** SIP Entity, as shown below.

The screenshot shows the 'Session Manager' tab in a web interface. On the left is a dark sidebar with navigation links: 'System Status', 'Load Factor', 'SIP Entity Monito...', 'Managed Bandwi...', 'Security Module ...', 'SIP Firewall Status', 'Registration Sum...', 'User Registrations', 'Session Counts', and 'Push Notification...'. The 'SIP Entity Monito...' link is selected. The main panel is titled 'All Monitored SIP Entities' and contains a 'Run Monitor' button. Below this, it says '17 Items' with a refresh icon. A table lists the monitored SIP entities, each with a checkbox and a blue hyperlink name. The 'Eyerys' entry is highlighted with a red rectangular box.

<input type="checkbox"/>	SIP Entity Name
<input type="checkbox"/>	AACC
<input type="checkbox"/>	InAttend
<input type="checkbox"/>	SBCE - InsideRW - 159
<input type="checkbox"/>	novaalert
<input type="checkbox"/>	IP Office - SE
<input type="checkbox"/>	breeze2wspaces
<input type="checkbox"/>	breeze3wspaces
<input type="checkbox"/>	breeze1wspaces
<input type="checkbox"/>	Messaging10x
<input type="checkbox"/>	Messaging11x
<input type="checkbox"/>	Eyerys
<input type="checkbox"/>	SBCE - InsideTrk - 158
<input type="checkbox"/>	SBCE - Loop -Voxtronic
<input type="checkbox"/>	cm101x - SIP TRUNK - 5062
<input type="checkbox"/>	cm101x - Phones - 5061

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: Eyerys

Summary View

1 Item Filter: Enable

	Session Manager Name	Session Manager IP Address Family	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
<input type="radio"/>	sm101x	IPv4	10.10.40.123	5060	UDP	FALSE	UP	200OK	UP

Select : None

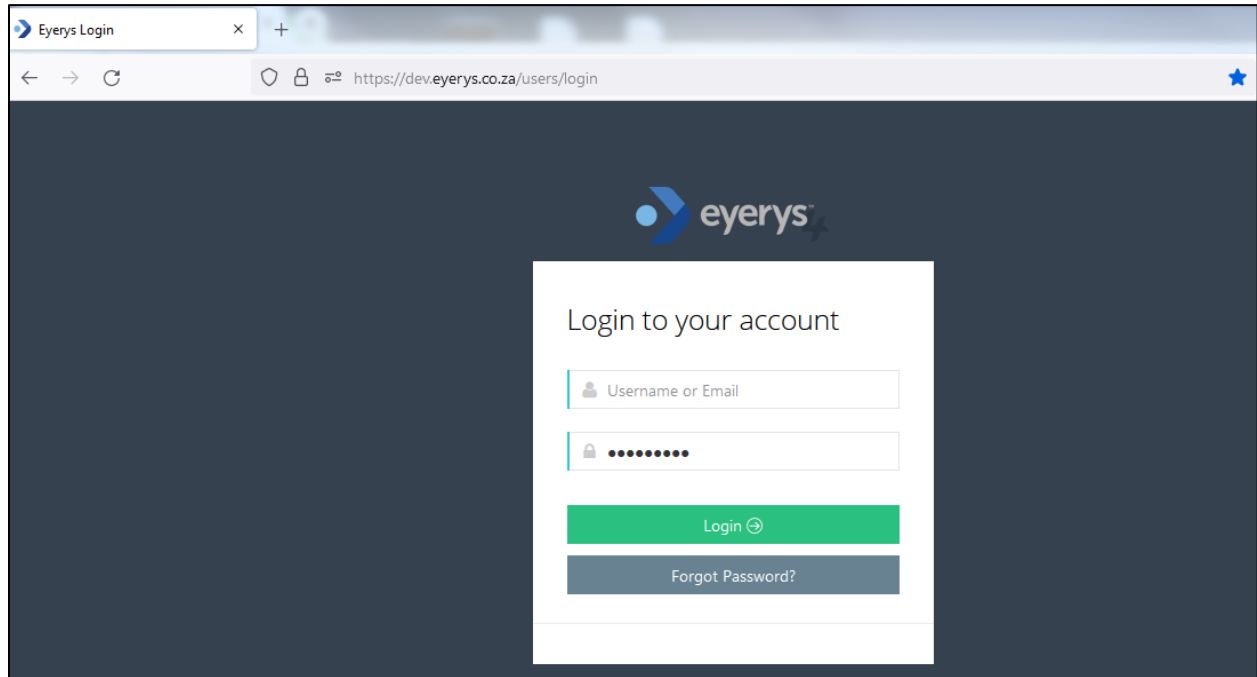
Open “traceSM” on Session Manager. This is achieved by opening a PuTTY connection to Session Manager’s management address and logging in with the appropriate credentials and typing traceSM (not shown). The following window opens which should show something like the call flow below, which can be then scrutinized should that be required.

sm81xvmpg.devconnect.local - traceSM V8.1.3.2.001 - FILTERED - Captured: 10007 Displayed: 404 - MAX NUM PACKETS (10000) EXCEEDED!

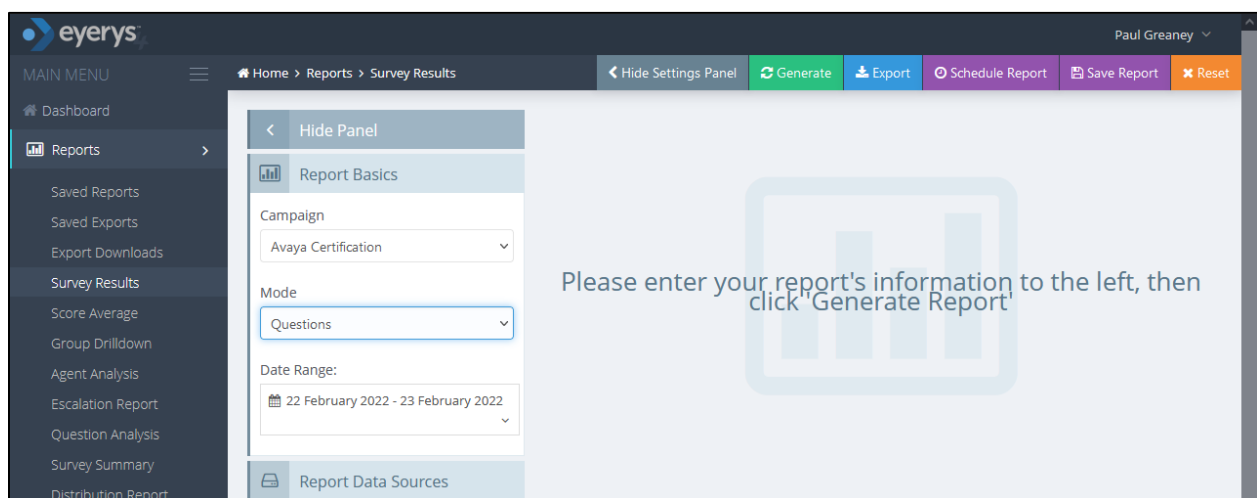
	SM100	10.10.40.39	SBCE8
	Smoke	192.168.40.168	
10:48:18.506	←OPTIONS→		(1334) sip:10.10.40.32
10:48:18.507	→200 OK←		(1334) 200 OK (OPTIONS)
10:48:28.592	←INVITE→		(1340) T:6001 F:1001 U:6001 P:terminating
10:48:28.596	←Trying←		(1340) 100 Trying
10:48:28.797	←200 OK←		(1340) 200 OK (INVITE)
10:48:28.801	→ACK→		(1340) sip:6001@10.10.40.123:5060
10:48:28.901	→reINVIT→		(1340) T:6001 F:1001 U:6001
10:48:28.902	←Trying←		(1340) 100 Trying
10:48:28.902	←200 OK←		(1340) 200 OK (INVITE)
10:48:28.942	→ACK→		(1340) sip:6001@10.10.40.123:5060
10:48:28.942		←G711a→	(1340) RTP 192.168.40.168:3086 <-G711a-> 10.10.40.123:14466
10:48:29.756	→reINVIT→		(1340) T:6001 F:1001 U:6001
10:48:29.757	←Trying←		(1340) 100 Trying
10:48:29.757	←200 OK←		(1340) 200 OK (INVITE)
10:48:29.796	→ACK→		(1340) sip:6001@10.10.40.123:5060
10:48:29.796	←G711a→		(1340) RTP 10.10.40.39:6004 <-G711a-> 10.10.40.123:14466
10:48:29.860	→reINVIT→		(1340) T:6001 F:1001 U:6001
10:48:29.861	←Trying←		(1340) 100 Trying
10:48:29.861	←200 OK←		(1340) 200 OK (INVITE)
10:48:29.861	←200 OK←		(1340) 200 OK (INVITE)
10:48:29.962		←G711a→	(1340) RTP 10.10.40.158:35354 <-G711a-> 10.10.40.123:14466
10:48:30.002	→ACK→		(1340) sip:6001@10.10.40.123:5060
10:48:30.003	→ACK→		(1340) sip:6001@10.10.40.123:5060
10:48:30.003		←G711a→	(1340) RTP 10.10.40.158:35354 <-G711a-> 10.10.40.123:14466
10:48:48.448	←BYE←		(1340) sip:35391847001@10.10.40.37:5061
10:48:48.452	→200 OK←		(1340) 200 OK (BYE)
10:49:18.508	←OPTIONS←		(1373) sip:10.10.40.32
10:49:18.510	→200 OK←		(1373) 200 OK (OPTIONS)

9.3. Verify Reports on Eyerys

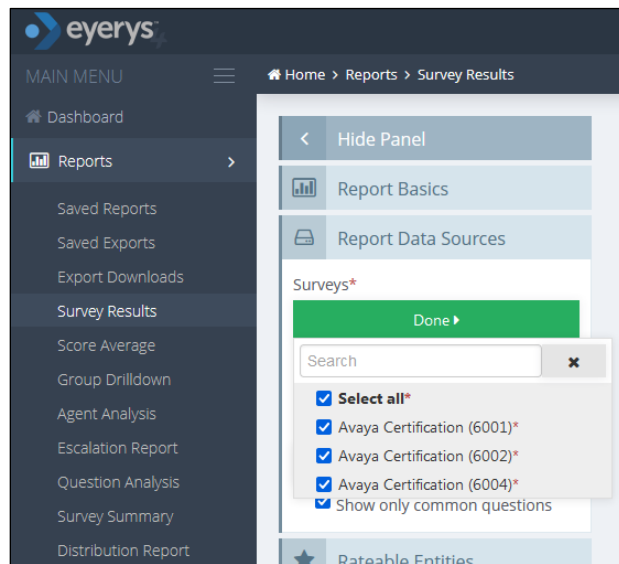
Transferring a caller in the Eyerys application and leaving a review will allow the verification that the correct information is being gathered and reported on. To run such a report on Eyerys open a URL as shown below. Enter the appropriate credentials and click on **Login**.



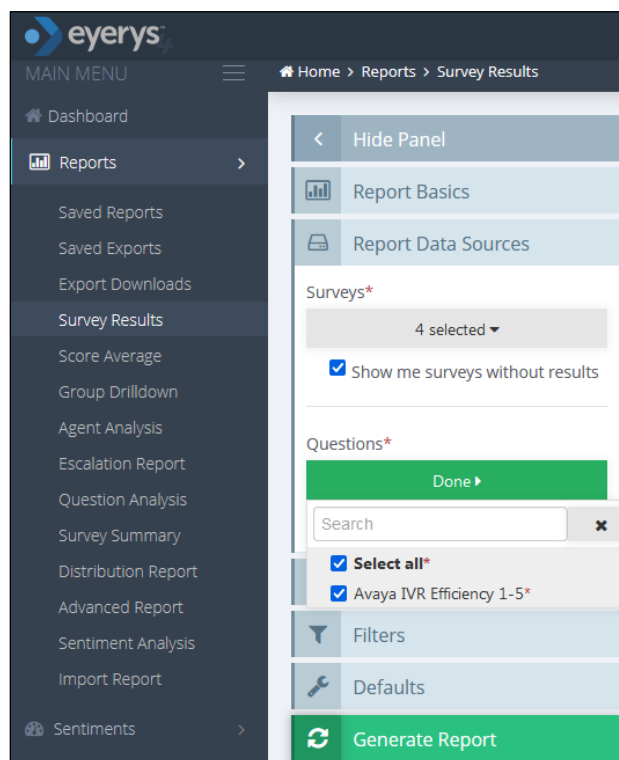
Navigate to **Reports → Survey Results** in the left window, the main window facilitates the creation of this report, where the filters are set, for example the **Campaign** and **Questions** etc. For compliance testing, the **Campaign** used was called **Avaya Certification** and so this will be the campaign chosen to run the report against.



The other filters for this report will need to be set also, for example under **Report Data Sources** the surveys and questions are selected. The example below shows all **Surveys** were selected. Click on **Done** to complete the selection.



All **Questions** were selected. The report can be generated by clicking on the **Generate Report** button at the bottom of the screen.



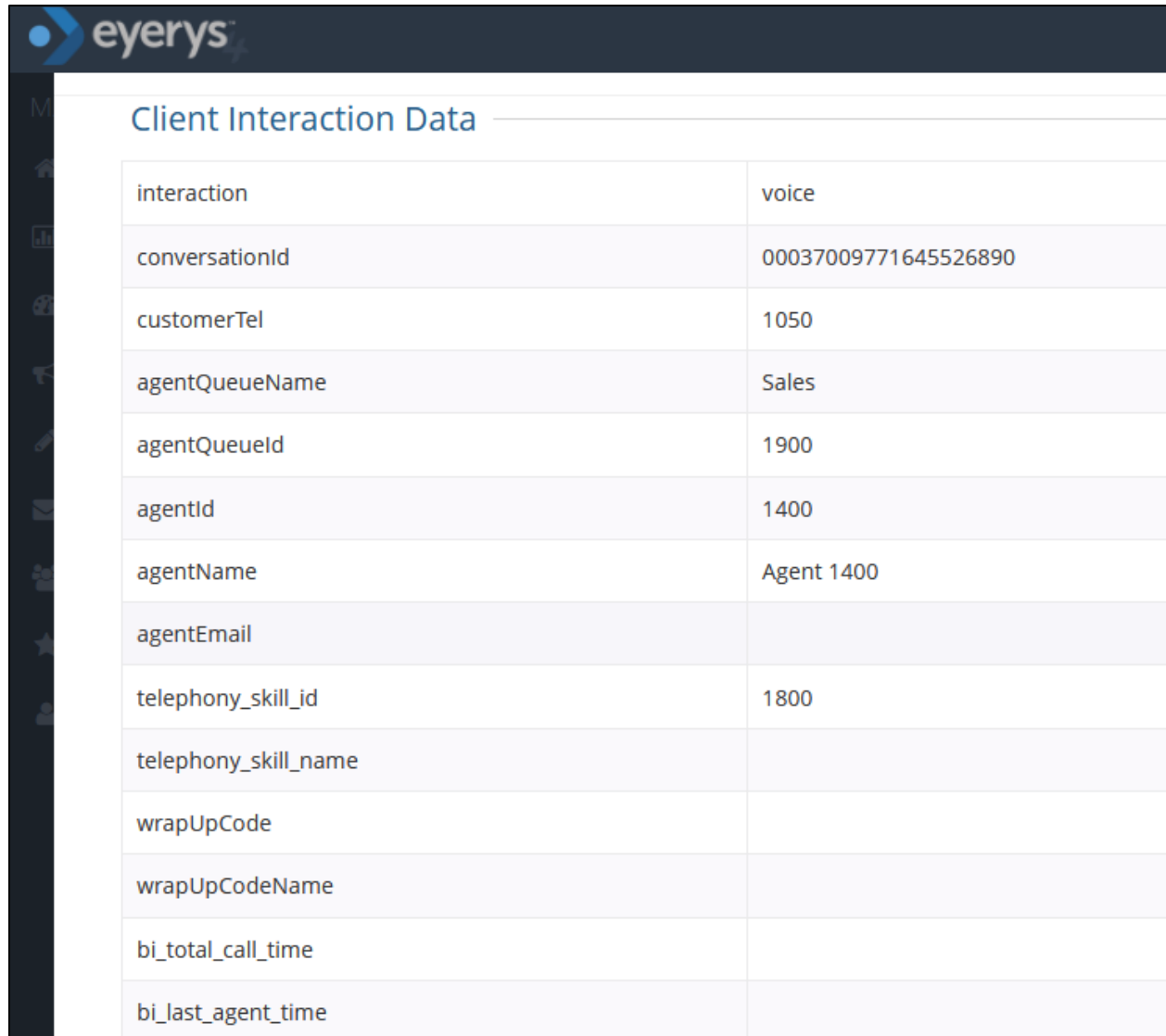
The report shows how many times each choice (1 to 5) was pressed. By clicking on the top of any of these choices (for example **27** for choice **5**) will open yet another window to allow further investigations take place.



The first six of the 27 instances of the ‘DTMF 5 press’ are listed below, a report can be run for each of these by clicking on **Run Report** opposite the desired choice.

Survey Results							
Created	Client	Survey	Rateable Entity	Status	Voicemail	Call Recording	Actions
2022-02-22 10:12:43	Valued Customer	Avaya Certification (6001)	IVR Agent		-	Play Download Listen In PureCloud	Run Report
2022-02-22 11:51:14	Valued Customer	Avaya Certification (6001)	Agent 1400		-	Play Download Listen In PureCloud	Run Report
2022-02-22 12:42:24	Valued Customer	Avaya Certification (6001)	IVR Agent		-	-	Run Report
2022-02-22 12:48:36	Valued Customer	Avaya Certification (6001)	Agent 1400		-	Play Download Listen In PureCloud	Run Report
2022-02-22 12:53:15	Valued Customer	Avaya Certification (6001)	Agent 1400		-	Play Download Listen In PureCloud	Run Report
2022-02-22 13:58:38	Valued Customer	Avaya Certification (6001)	Agent 3		-	Play Download Listen In PureCloud	Run Report

The report below shows that a customer with telephone number **1050**, called to the **Sales** skillset on VDN **1900**, and was answered by agent **1400** with Skillset ID **1800**. This information is coming from Application Enablement Services DMCC. This allows the survey results to be matched against certain calls and agents.



interaction	voice
conversationId	00037009771645526890
customerTel	1050
agentQueueName	Sales
agentQueueId	1900
agentId	1400
agentName	Agent 1400
agentEmail	
telephony_skill_id	1800
telephony_skill_name	
wrapUpCode	
wrapUpCodeName	
bi_total_call_time	
bi_last_agent_time	

10. Conclusion

These Application Notes describe the configuration steps required for Eyerys IVR Connector R2.2 from Smoke Customer Intelligence Pty Ltd., to successfully interoperate with Avaya Aura® Communication Manager R10.1, Avaya Aura® Application Enablement Services R10.1 and Avaya Aura® Session Manager R10.1. All feature functionality and serviceability test cases were completed successfully with any observations noted in **Section 2.2**.

11. Additional References

This section references the Avaya and Smoke Customer Intelligence Pty Ltd., product documentation that are relevant to these Application Notes.

Product documentation for Avaya products may be found at <http://support.avaya.com>.

- [1] *Administering Avaya Aura® Communication Manager, Release 10.1.x, Issue 12, Jul 2021*
- [2] *Administering Avaya Aura® Session Manager, Release 10.1.x, Issue 8, Feb 2021*
- [3] *Avaya Aura® Communication Manager Screen Reference, Release 10.1.x Issue 12 September 2021*
- [4] *Avaya Aura® Communication Manager Feature Description and Implementation, Release 10.1.x Issue 17 August 2021*
- [5] *Avaya Aura® Communication Manager Special Application Features, October 2020*
- [6] *Avaya Aura® Application Enablement Services Administration and Maintenance Guide Release 10.1*

Documentation for Eyerys IVR Connector is available on request from Smoke Customer Intelligence Pty Ltd. at www.smokeci.com/contact.

©2023 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.