AVAYA

Avaya Solution & Interoperability Test Lab

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 R2.0 from Smoke Customer Intelligence Pty Ltd., to successfully interoperate with Avaya Aura® Communication Manager R8.1, Avaya Aura® Session Manager R8.1 and Avaya Aura® Application Enablement Services R8.1. 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 at the Avaya Solution and Interoperability Test Lab.

PG; Reviewed:
SPOC 5/11/2022

Solution & Interoperability Test Lab Application Notes
©2022 Avaya Inc. All Rights Reserved.

1 of 51
Eyerys_SMAES81

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.

Eyerys IVR Connector (Eyerys) from Smoke Customer Intelligence Pty Ltd., integrates with the Avaya platform (Avaya Aura® Communication Manager R8.1.3, Avaya Aura® Session Manager R8.1.3 and Avaya Aura® Application Enablement Services R8.1.3) to allow contact centres 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
- Testing call scenarios with misapplication of the Eyerys Post Call Survey
- Testing different Codec and DTMF standards

2.2. Test Results

All test cases were executed successfully.

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.
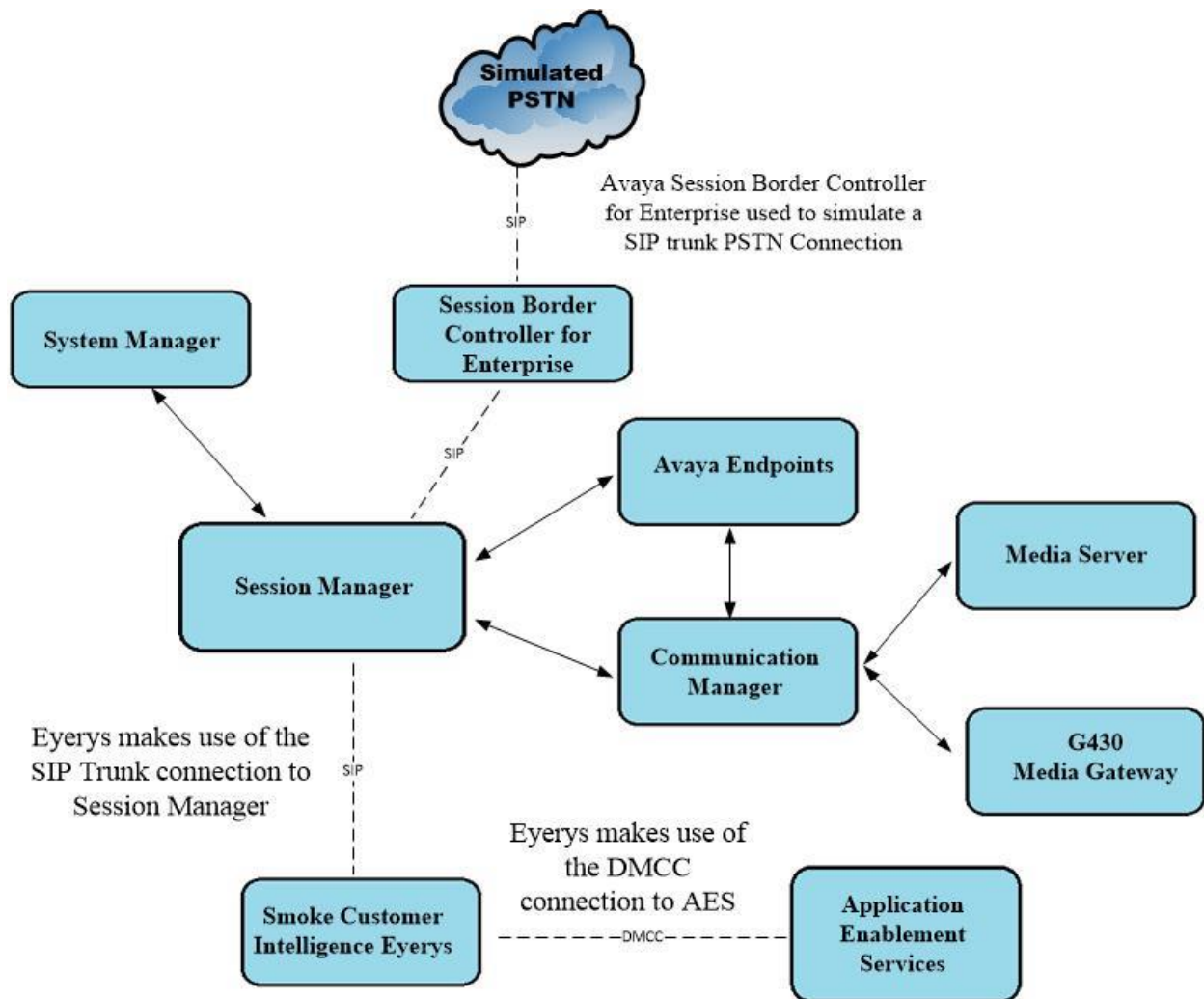
Figure 1: Connection of Smoke Customer Intelligence Pty Ltd. Eyerys IVR Connector with Avaya Aura® Communication Manager R8.1, Avaya Aura® Application Enablement Services and Avaya Aura® Session Manager R8.1

PG; Reviewed:
SPOC 5/11/2022

Solution & Interoperability Test Lab Application Notes
©2022 Avaya Inc. All Rights Reserved.

4 of 51
Eyerys_SMAES81

4. Equipment and Software Validated

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

Avaya Equipment	Software / Firmware Version
Avaya Aura® System Manager running on a virtual server	8.1.3.2 Build No. – 8.1.0.0.733078 Software Update Revision No: 8.1.3.2.1012646 Service Pack 2
Avaya Aura® Session Manager running on a virtual server	8.1.3.2 Build No. – 8.1.3.2.813207
Avaya Aura® Communication Manager running on a virtual server	8.1.3.2 – FP3SP2 R018x.01.0.890.0 Update ID 01.0.890.0-26989
Avaya Aura® Application Enablement Services running on a virtual server	8.1.3.2 Build 8.1.3.2.0.4-0
Avaya Aura® Media Server	8.0.2.184
Avaya G430 Media Gateway	41.16.0/1
Avaya J179 IP Phone (H.323)	6.8502
Avaya J189 IP Phone (SIP)	4.0.10.1.2
Avaya 9408 Digital Deskphone	V2.0
Smoke Customer Intelligence Pty Ltd. Equipment	**Software / Firmware Version**
Eyerys IVR Connector running on Linux	v2.0.0

PG; Reviewed:
SPOC 5/11/2022

Solution & Interoperability Test Lab Application Notes
©2022 Avaya Inc. All Rights Reserved.

5 of 51
Eyerys_SMAES81

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:
- System Parameters
- Administer Dial Plan
- Administer Route Selection
- Configure SIP Trunk
- Configure VDN and Vector for Automatic Transfer

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 certain fields are set correctly to allow the connection to Eyerys to take place and work correctly.

5.1.1. Verify System Parameters Special Applications

(SA8702) - CDR Enhancements for Network may want to be set to **n**, as setting this to y can cause issues with SIP CC phones. Special Application changes the behavior of how CM 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
              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 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. Administer Dial Plan

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    Total  Call     Dialed    Total  Call     Dialed    Total  Call
   String    Length Type     String    Length Type     String    Length Type
   1           4    udp      #            3    fac
   2           4    udp
   3           4    udp
   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
```

5.3. Administer Route Selection for calls to Eyerys

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 SIP Trunk

In the **Node Names IP** form, note the IP Address of the **procr** and Session Manager (**sm81xvmpg**). 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
sm81xvmpg             10.10.40.32
SM_Oceana             10.10.41.26
aes81xvmpg            10.10.40.38
default               0.0.0.0
procr                 10.10.40.37

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

In the **IP Codec Set** form, select the audio codecs supported for calls routed over the SIP trunk to Eyerys. 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 **G.711A** (a-law), **G.711MU** (mu-law) and **G729** which are supported by Eyerys. Eyerys also supports various OPUS Codecs which were also 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: G.711A           n          2        20
 2: G.711MU          n          2        20
 3: G.729            n          2        20
 4:

    Media Encryption                    Encrypted SRTCP: enforce-unenc-srtcp
 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: sm81xvmpg
 Near-end Listen Port: 5061              Far-end Listen Port: 5061
                                       Far-end Network Region: 1


Far-end Domain:
                                         Bypass If IP Threshold Exceeded? n
Incoming Dialog Loopbacks: eliminate            RFC 3389 Comfort Noise? n
       DTMF over IP: rtp-payload         Direct IP-IP Audio Connections? y
Session Establishment Timer(min): 3               IP Audio Hairpinning? n
       Enable Layer 3 Test? y            Initial IP-IP Direct Media? n
H.323 Station Outgoing 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 Eyerys. 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: *801
   Direction: two-way      Outgoing Display? n
 Dial Access? n                                    Night Service:
Queue Length: 0
Service Type: public-ntwrk                   Auth Code? n
                                             Member Assignment Method: auto
                                                   Signaling Group: 1
                                                 Number of Members: 10
```

On **Page 2** of the trunk-group form the **Preferred Minimum Session Refresh Interval (sec)** field should be set to a value mutually agreed with Smoke Customer Intelligence Pty Ltd., to prevent unnecessary SIP messages during call setup. For the compliance test a value of **90** 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): 90

 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 **UUI 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
                                        UUI Treatment: shared
                                     Maximum Size of UUI 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
```

5.5. 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 eth 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
09
10
11
12
```

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
```

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**.

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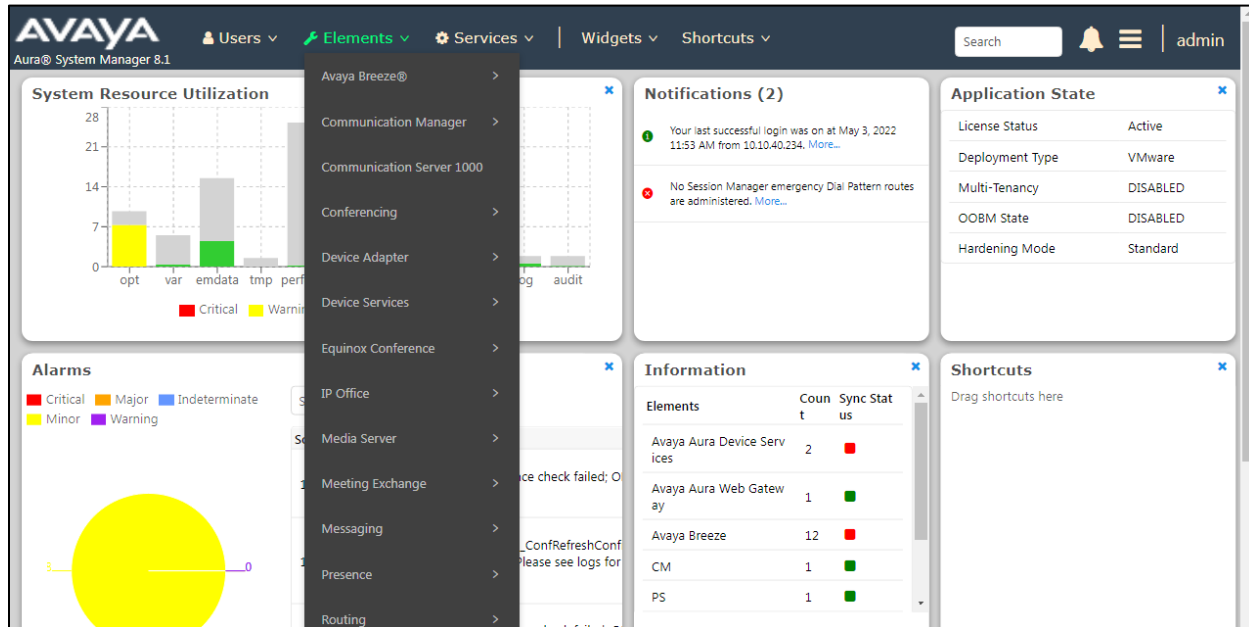
6.1. Domains and Locations

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.
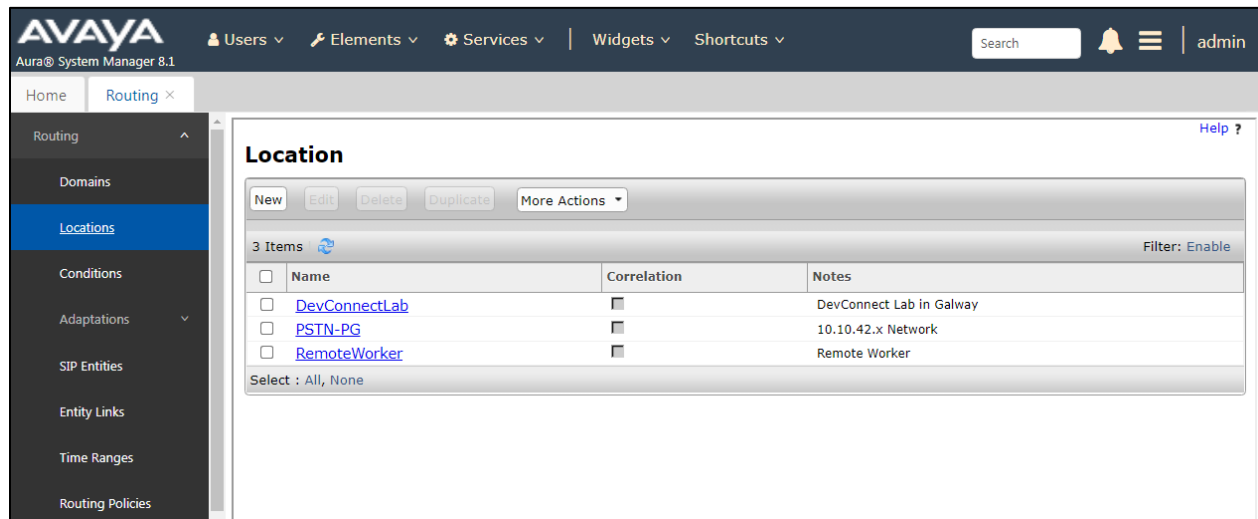
6.1.1. Display the Domain

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.
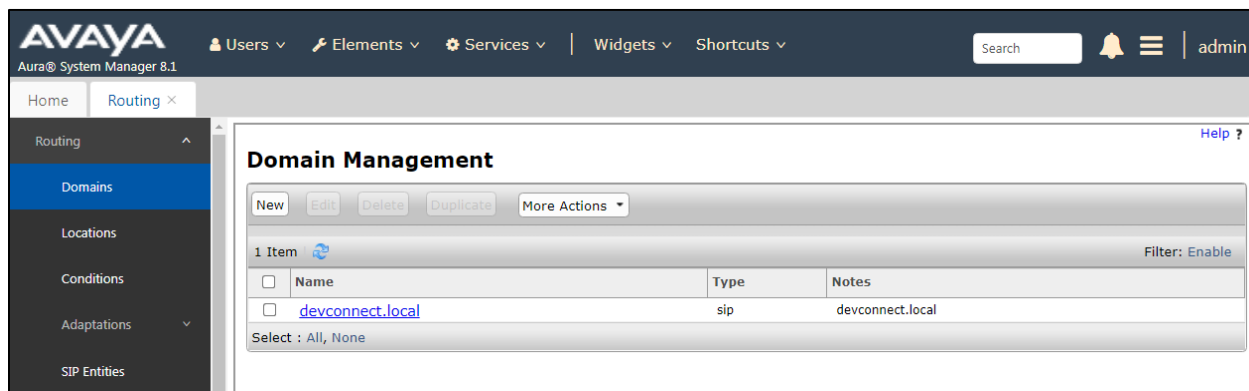
6.1.2. Display the Location

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.
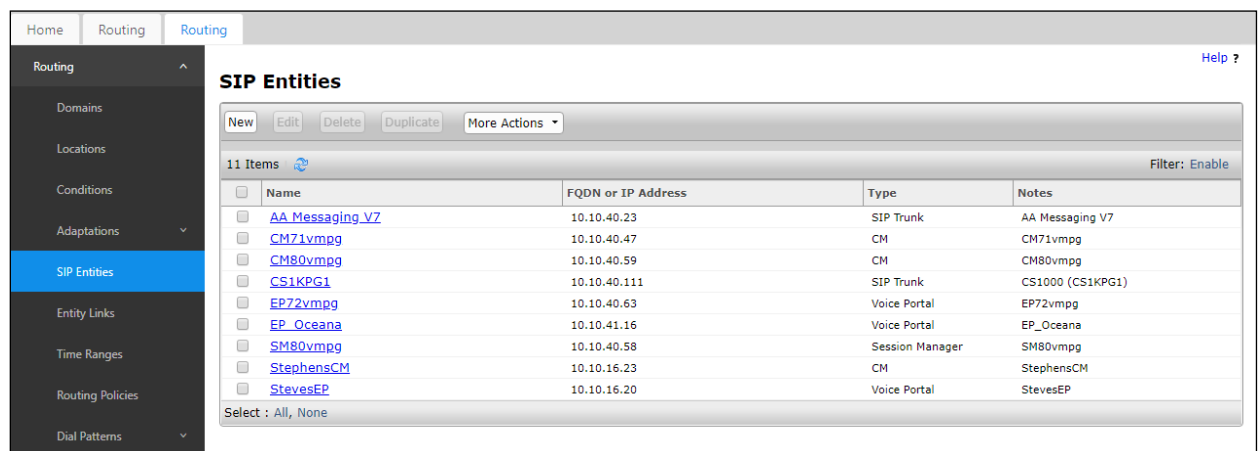
6.2. Configure Eyerys SIP Entity and Entity Link

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.

PG; Reviewed:
SPOC 5/11/2022

Solution & Interoperability Test Lab Application Notes
©2022 Avaya Inc. All Rights Reserved.

20 of 51
Eyerys_SMAES81

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.

PG; Reviewed:
SPOC 5/11/2022

Solution & Interoperability Test Lab Application Notes
©2022 Avaya Inc. All Rights Reserved.

21 of 51
Eyerys_SMAES81

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.

6.3. Configure Routing Policy for Eyerys

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

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

Select the Eyerys SIP Entity as shown below (this was named **Smoke** when added for compliance testing) and click on **Select**.

PG; Reviewed:
SPOC 5/11/2022

Solution & Interoperability Test Lab Application Notes
©2022 Avaya Inc. All Rights Reserved.

23 of 51
Eyerys_SMAES81

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

6.4. Configure Eyerys Dial Patterns

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

PG; Reviewed:
SPOC 5/11/2022

Solution & Interoperability Test Lab Application Notes
©2022 Avaya Inc. All Rights Reserved.

24 of 51
Eyerys_SMAES81

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.

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.

PG; Reviewed:
SPOC 5/11/2022

Solution & Interoperability Test Lab Application Notes
©2022 Avaya Inc. All Rights Reserved.

25 of 51
Eyerys_SMAES81

Select the newly created Routing Policy for Eyerys.

Routing Policies

	Name	Disabled	Destination	Notes
☐	ToAACC71Spare	☐	aacc71spare	ToAACC71Spare
☐	To AACC71x	☐	aacc71x	To AACC71x on Win 2012
☐	To CM80vmpg	☐	cm80vmpg	To CM80vmpg
☐	To cm81xvmpg	☐	cm81vmpg - TRUNK 5063	To cm81xvmpg - 5063
☐	To CM81xvmpg - PHONES	☐	cm81vmpg - SIP PHONES 5061	For SIP Phones
☐	To EP722	☐	EP723(MPP)	To EP722
☐	To EP810 (MPP)	☐	EP810(MPP)	To EP810 (MPP)
☐	To IPOSE11	☐	IPOSE11	To new IPOSE11
☐	To LifeX	☐	LifeX	To LifeX
☐	To Messaging on 2016	☐	MessagingOn2016	To Messaging on 2016
☐	To Messaging on 2019	☐	MessagingOn2019	To Messaging on 2019
☐	To Presence OpenGate	☐	PresenceOG	To Presence OpenGate 6300
☐	To SBCE8	☐	SBCE8	To SBCE8
☐	ToSBCEforLifeX	☐	SBCEforLifeX	ToSBCEforLifeX
☑	To Smoke	☐	Smoke	To Smoke

15 Items   Filter: Enable

Select : All, None

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: devconnect.local ▾
Notes: To Smoke Call Survey

Originating Locations, Origination Dial Pattern Sets, and Routing Policies

Add   Remove

1 Item

	Originating Location Name	Originating Location Notes	Origination Dial Pattern Set Name	Origination Dial Pattern Set Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
☐	DevConnectLab	DevConnect Lab in Galway			To Smoke	0	☐	Smoke	To Smoke

Select : All, None

PG; Reviewed:
SPOC 5/11/2022

Solution & Interoperability Test Lab Application Notes
©2022 Avaya Inc. All Rights Reserved.

26 of 51
Eyerys_SMAES81

7. Configure Avaya Aura® Application Enablement Services Server
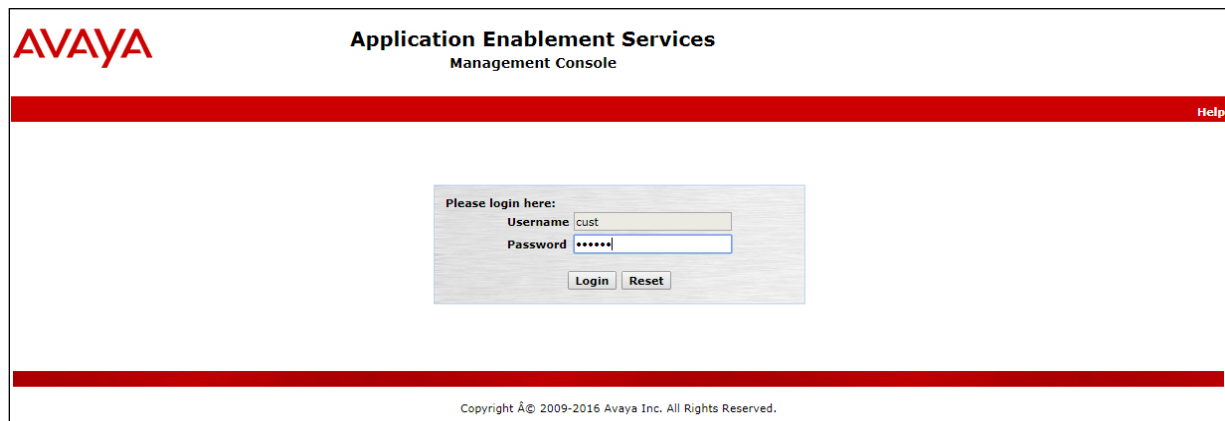
This section provides the procedures for configuring Application Enablement Services. The procedures fall into the following areas:

- 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.

PG; Reviewed:
SPOC 5/11/2022
Solution & Interoperability Test Lab Application Notes
©2022 Avaya Inc. All Rights Reserved.
27 of 51
Eyerys_SMAES81

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 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.

PG; Reviewed:
SPOC 5/11/2022

Solution & Interoperability Test Lab Application Notes
©2022 Avaya Inc. All Rights Reserved.

28 of 51
Eyerys_SMAES81

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

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.

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.

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.

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**.

PG; Reviewed:
SPOC 5/11/2022

Solution & Interoperability Test Lab Application Notes
©2022 Avaya Inc. All Rights Reserved.

32 of 51
Eyerys_SMAES81

7.5. Display Switch Information

The name and IP address of Communication Manager will be needed for the configuration of Eyerys 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.

The IP address of Communication Manager is displayed below.

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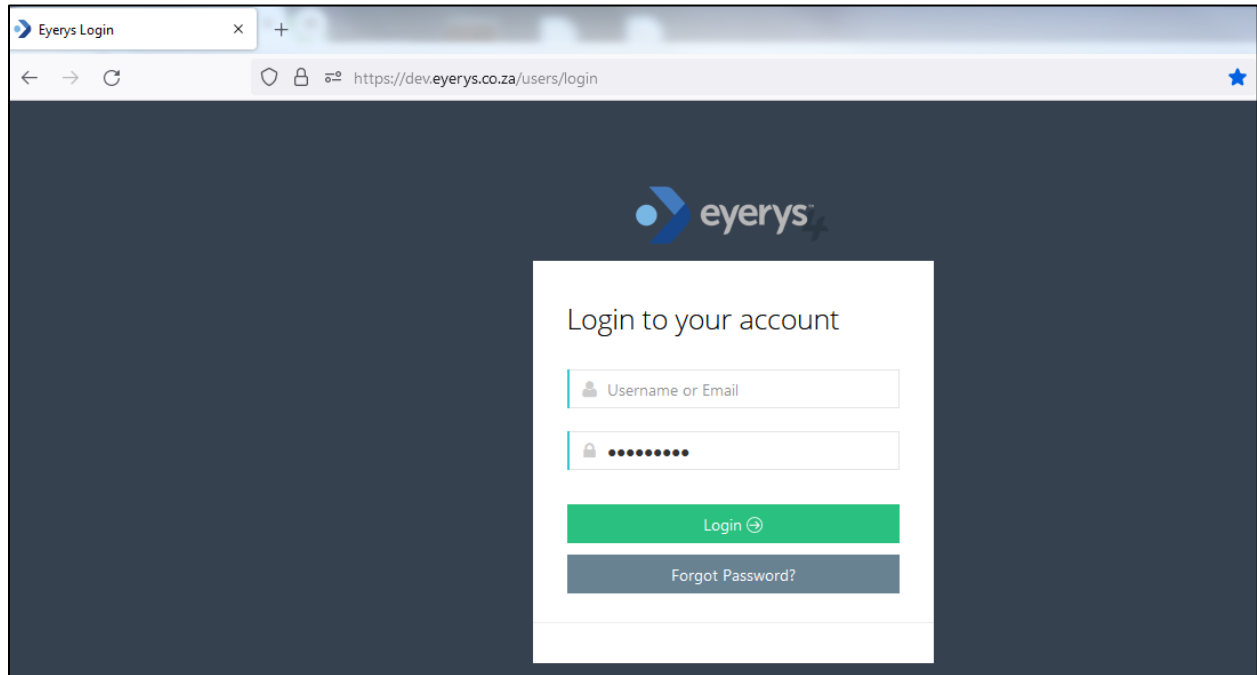
Once logged in, click on **System Settings** (top right of screen) as shown below.

PG; Reviewed:
SPOC 5/11/2022

Solution & Interoperability Test Lab Application Notes
©2022 Avaya Inc. All Rights Reserved.

34 of 51
Eyerys_SMAES81
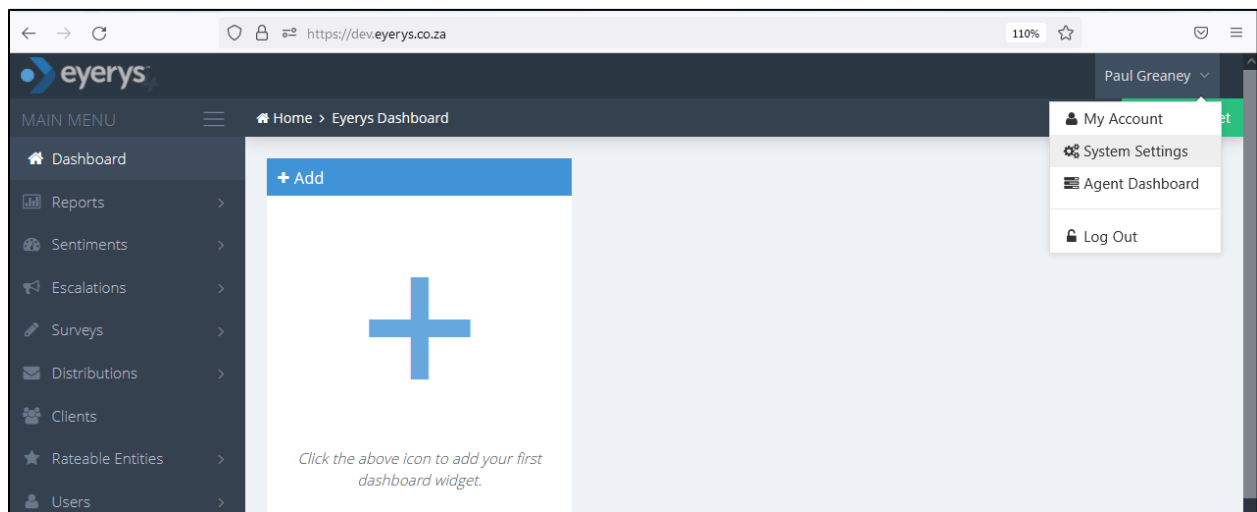
The settings that are relevant to the Avaya connection are all under the **Post Call Survey (IVR) Integration**. Scroll down to these icons, as shown below, **IVR Numbers** can be added for each survey that needs to be run. For compliance testing 6001 to 6004 were used for different surveys that took place.
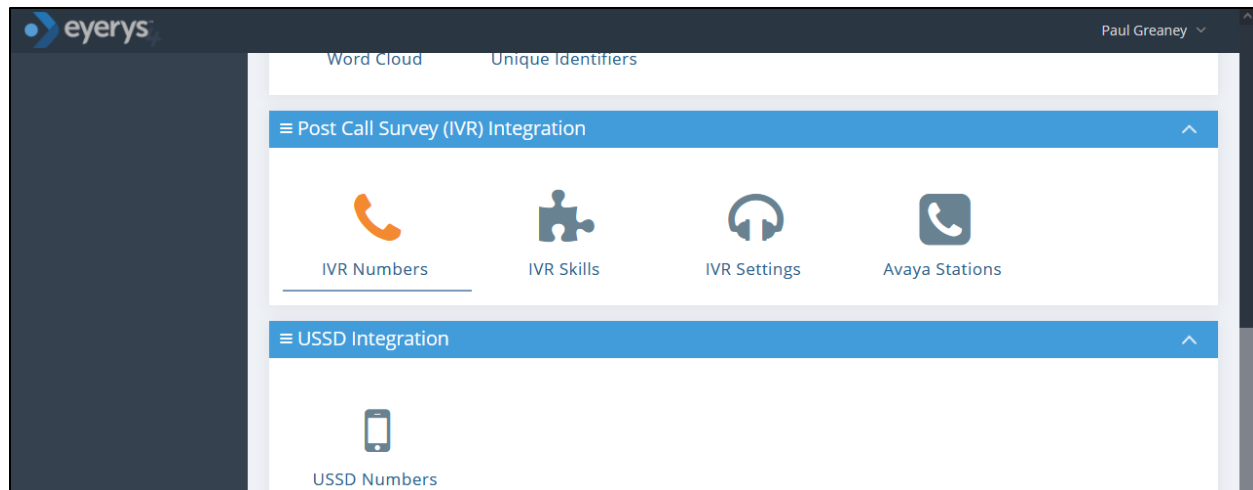
The example below shows the number **6001** being added, simply enter the number and click on **Save**.
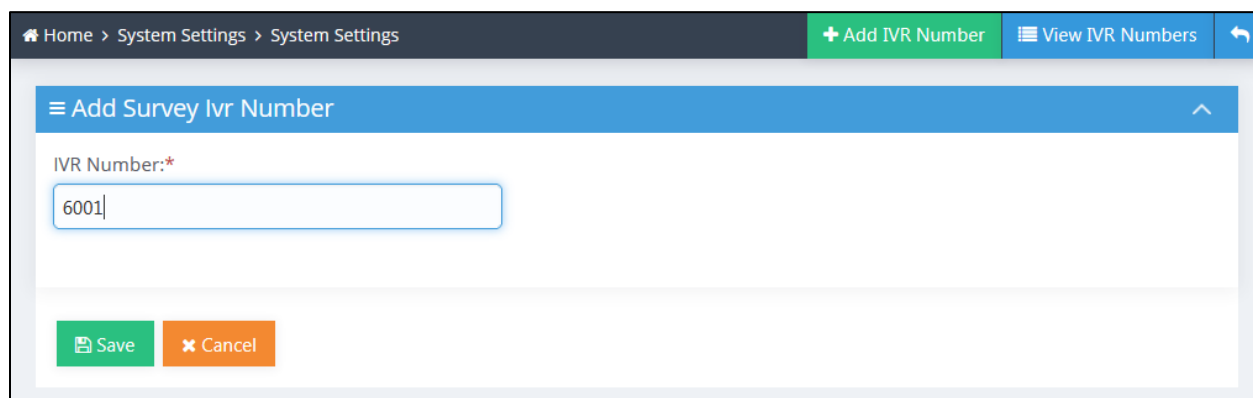
The IVR settings contains all the configuration on the connections to both Session Manager and Application Enablement Services. Click on the **IVR Settings** icon as shown below.
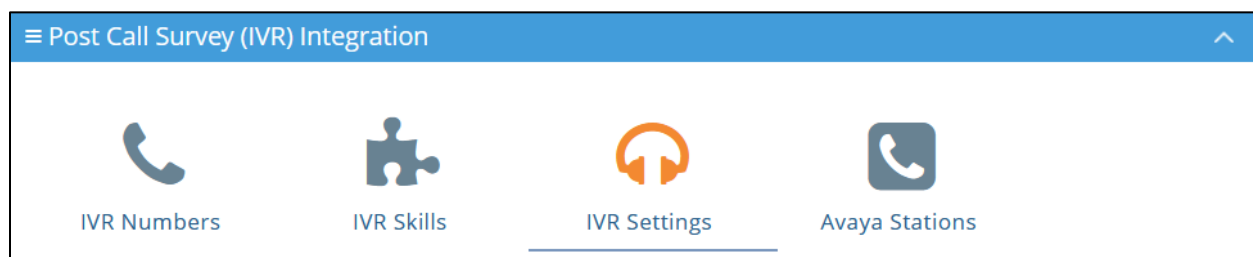
There are a number of connections displayed, the IVR connection for compliance testing is highlighted and clicking on **Edit** will display the configuration.

Here 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 5.4**. The **Codecs** are set here also and should negotiate with the Codecs in **Section 5.4**.

SIP Settings

Bind Address ❓	Bind Port ❓
0.0.0.0	5060

IVR Connection Server Local Net IP ❓	Protocol ❓
10.10.40.0	UDP

IVR Connection Server Local Subnet Mask ❓	NAT ❓
255.255.255.0	No

IVR Connection Server External IP ❓	Realm ❓
10.10.40.123	devconnect.local

DTMF Mode ❓

rfc2833

Codecs ❓

	Remove all		Add all
Alaw	−	g729	+
		Opus	+
		Ulaw	+

PG; Reviewed:
SPOC 5/11/2022
Solution & Interoperability Test Lab Application Notes
©2022 Avaya Inc. All Rights Reserved.
37 of 51
Eyerys_SMAES81

Scroll down the **Survey Pause Times**, 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) ❓
250	250
Pre Question Delay (ms) ❓	Customer Response Time (ms) ❓
250	10000
Pre Voicemail Delay (ms) ❓	2 Digit Input Time (ms) ❓
250	5000
Pre Goodbye Delay (ms) ❓	Question Retry Limit ❓
250	3

💾 Save

☰ Avaya Settings

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**.

PG; Reviewed:
SPOC 5/11/2022

Solution & Interoperability Test Lab Application Notes
©2022 Avaya Inc. All Rights Reserved.

39 of 51
Eyerys_SMAES81

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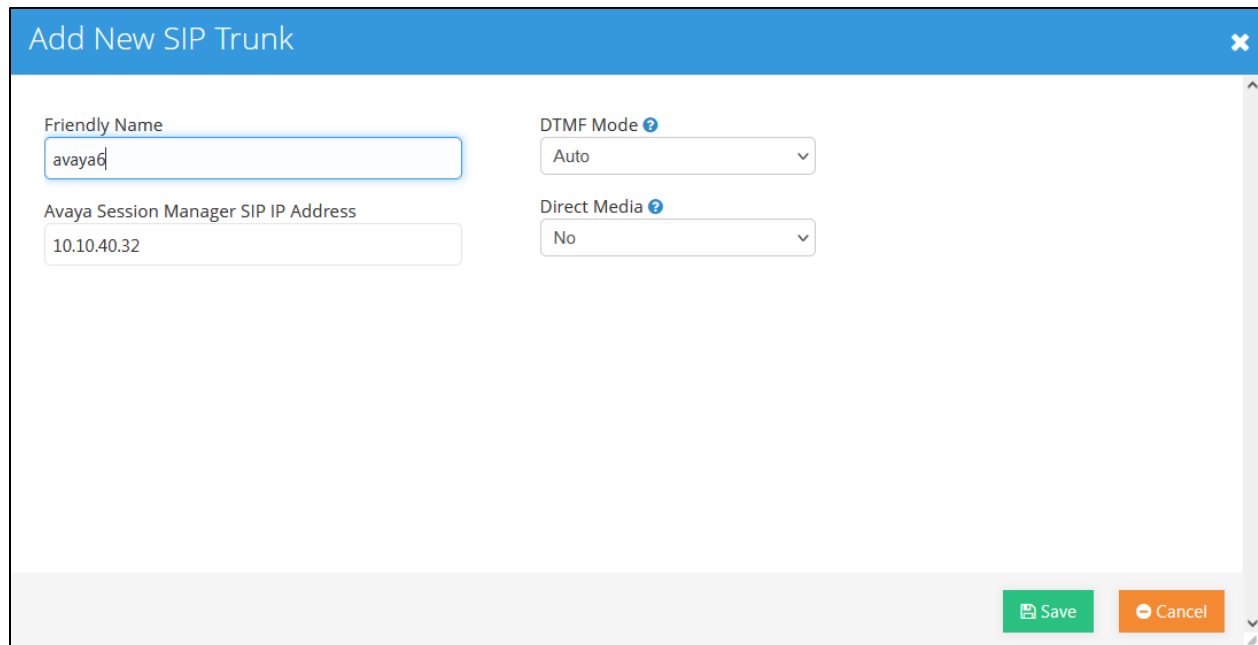
Scrolling down further, to **SIP Trunks** shows the configuration settings for the connection to Session Manager. There is an existing connection present but a new connection can be made by clicking on **Add New Trunk**.

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.

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

PG; Reviewed:
SPOC 5/11/2022

Solution & Interoperability Test Lab Application Notes
©2022 Avaya Inc. All Rights Reserved.

41 of 51
Eyerys_SMAES81
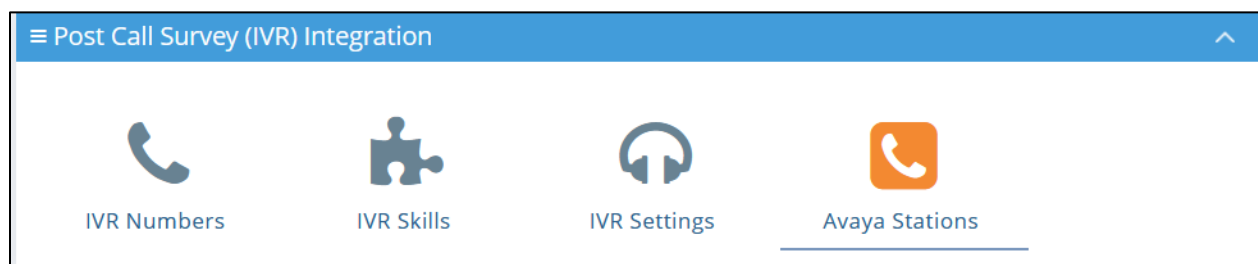
Each station (extension) number can be added here with a brief description of each.

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

9. Verification Steps

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

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 Eyerys 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 Eyerys server, IP address 10.10.40.123. The **Application** is shown as **Eyerys 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 Eyerys.

PG; Reviewed:
SPOC 5/11/2022

Solution & Interoperability Test Lab Application Notes
©2022 Avaya Inc. All Rights Reserved.

43 of 51
Eyerys_SMAES81

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**.

Navigate to **System Status → SIP Entity Monitoring** in the left window, and select the Eyerys SIP Entity, which was named **Smoke** for compliance testing.

PG; Reviewed:
SPOC 5/11/2022

Solution & Interoperability Test Lab Application Notes
©2022 Avaya Inc. All Rights Reserved.

44 of 51
Eyerys_SMAES81

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

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.

PG; Reviewed:
SPOC 5/11/2022

Solution & Interoperability Test Lab Application Notes
©2022 Avaya Inc. All Rights Reserved.

45 of 51
Eyerys_SMAES81

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.**
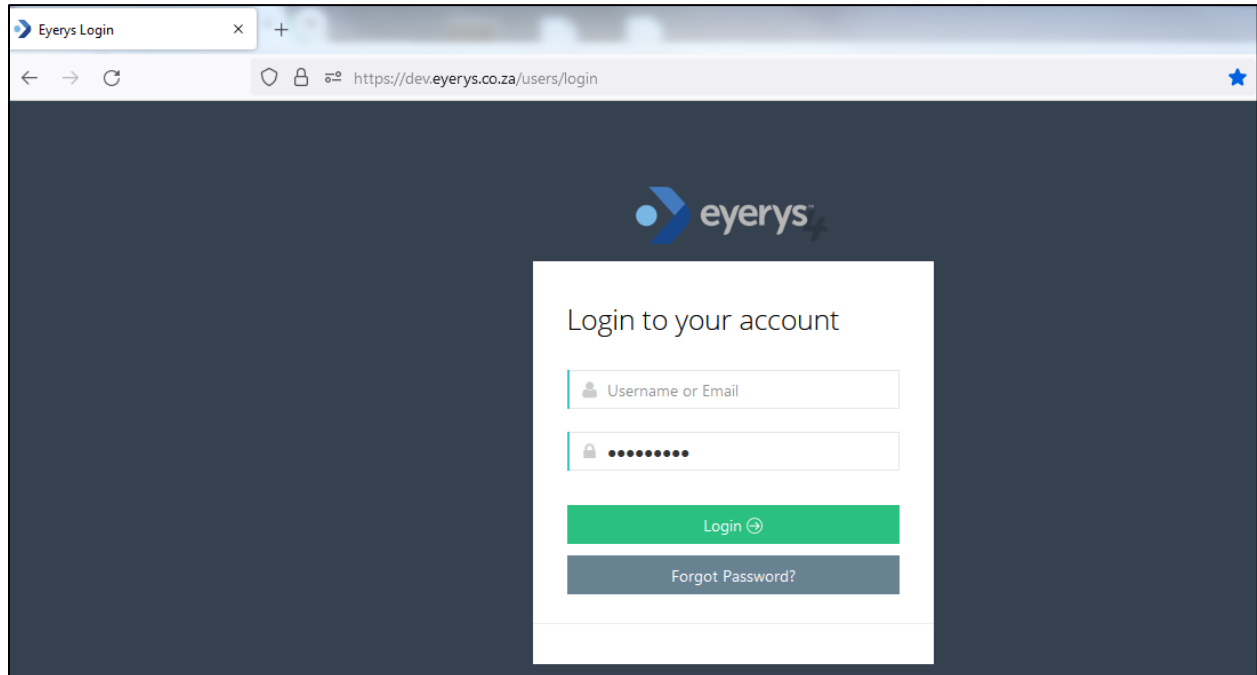

Navigate to **Reports → Survey Results** in the left window, the main window facilitates the creation of this report, where the filters are set, for example the **Campaign** and **Questions** etc. For compliance testing, the **Campaign** used was called **Avaya Certification** and so this will be the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

PG; Reviewed:
SPOC 5/11/2022

Solution & Interoperability Test Lab Application Notes
©2022 Avaya Inc. All Rights Reserved.

46 of 51
Eyerys_SMAES81
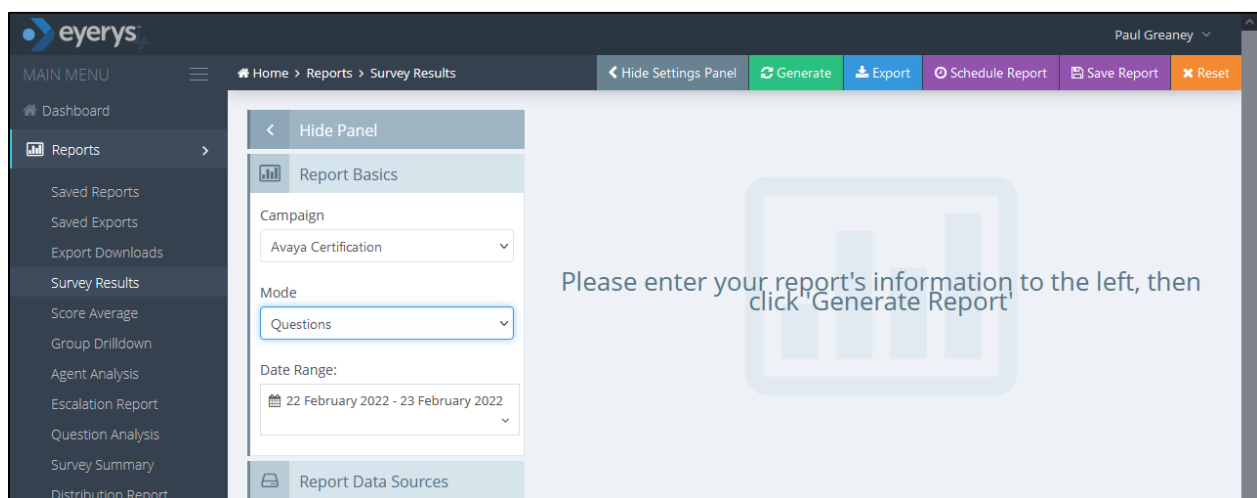
The other filters for this report will need to be set also, for example under **Report Data Sources** the surveys and questions are selected. The example below shows all **Surveys** were selected. Click on **Done** to complete the selection.
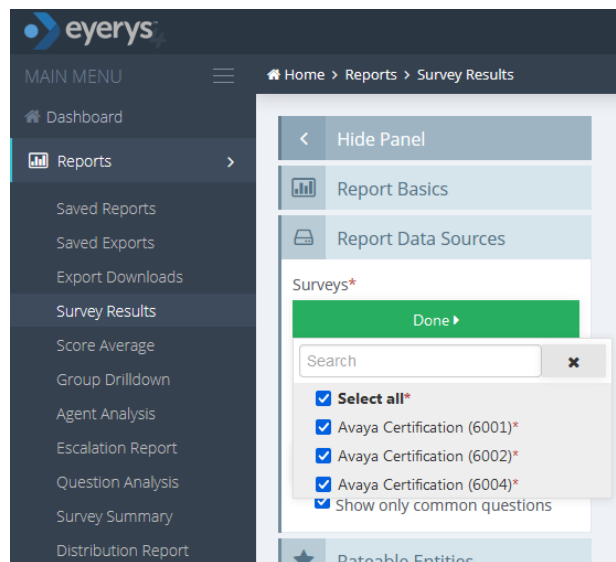
All **Questions** were selected. The report can be generated by clicking on the **Generate Report** button at the bottom of the screen.
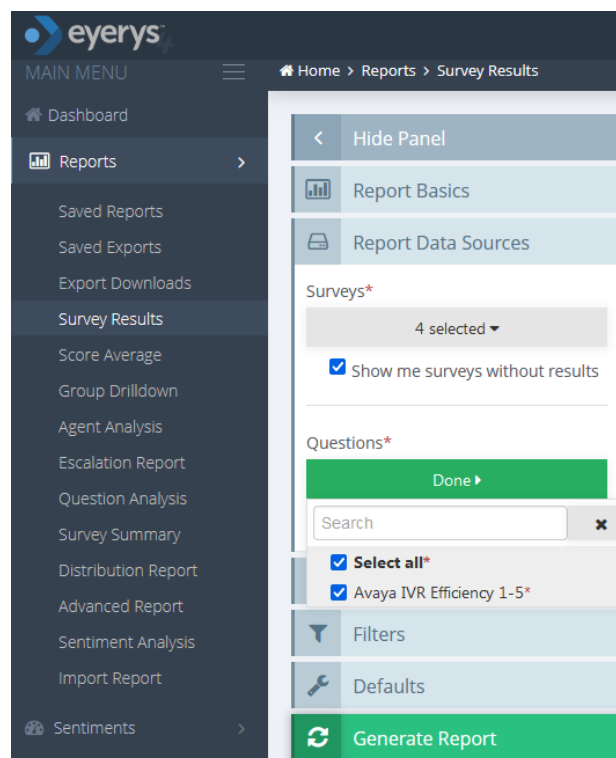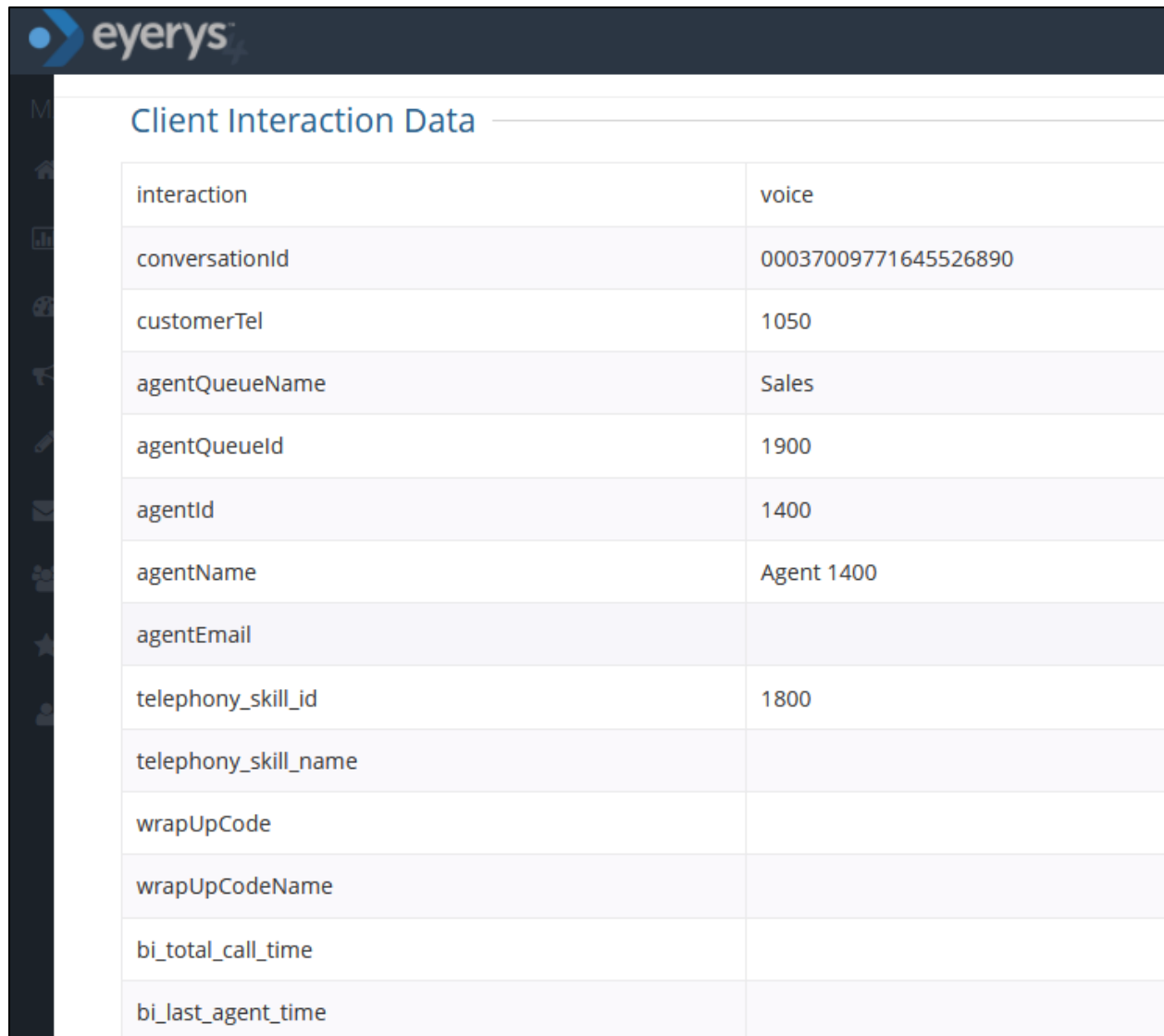
The report shows how many times each choice (1 to 5) was pressed. By clicking on the top of any of these choices (for example **27** for choice **5**) will open yet another window to allow further investigations take place.

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.

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.

● eyerys	
Client Interaction Data	
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 R2.0 from Smoke Customer Intelligence Pty Ltd., to successfully interoperate with Avaya Aura® Communication Manager R8.1, Avaya Aura® Application Enablement Services R8.1 and Avaya Aura® Session Manager R8.1. 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 8.1.x, Issue 12, Jul 2021*
[2] *Administering Avaya Aura® Session Manager, Release 8.1.x, Issue 8, Feb 2021*
[3] *Avaya Aura® Communication Manager Screen Reference, Release 8.1.x Issue 12 September 2021*
[4] *Avaya Aura® Communication Manager Feature Description and Implementation, Release 8.1.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 8.1*

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