Avaya Solution & Interoperability Test Lab

Application Notes for Geomant Desktop Connect 4.2 with Avaya Aura® Application Enablement Services 10.1 and Avaya Proactive Outreach Manager 4.0.2 – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for Geomant Desktop Connect v4.2.0 to interoperate with Avaya Aura® Application Enablement Services 10.1 and Avaya Proactive Outreach Manager 4.0.2. Geomant Desktop Connect provides a connector that links Avaya Aura® platform with cloud-based Customer Relationship Management provider Salesforce.com.

The compliance testing focused on the telephony integration with Avaya Aura® Communication Manager via Avaya Aura® Application Enablement Services Java Telephony Application Programming Interface and the Agent Desktop API on Avaya Proactive Outreach Manager.

Readers should pay attention to **Section 2**, in particular the scope of testing as outlined in **Section 2.1** as well as any observations noted in **Section 0**, to ensure that their own use cases are adequately covered by this scope and results.

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

1. Introduction

These Application Notes describe the configuration steps required for Geomant Desktop Connect 4.2 to interoperate with Avaya Aura® Communication Manager 10.1 by making connects to both Avaya Aura® Application Enablement Services (AES) 10.1 and Avaya Proactive Outreach Manager R4.0.2. Geomant Desktop Connect provides a connector that links Avaya Aura® Communication Manager with cloud-based Customer Relationship Management providers and for compliance testing Salesforce.com was used.

Compliance testing focused on two separate connections, a connection to Avaya Aura® Application Enablement Services using the Java Telephony Application Programming Interface (JTAPI) and a connection to Avaya Proactive Outreach Manager using the Agent Desktop API.

The JTAPI interface is used by Geomant Desktop Connect to monitor contact center devices on Avaya Aura® Communication Manager, and provide login/logout, agent work mode change, screen pop, and click-to-dial via the web-based agent application with Salesforce.com. JTAPI is a client-side interface to the Telephony Services Application Programming Interface (TSAPI) on Avaya Aura® Application Enablement Services. As such, these Application Notes will describe the required configurations for creation and connectivity to the TSAPI service.

The Agent Desktop APIs support the creation of custom desktop applications that enable agents to interact with Avaya Proactive Outreach Manager (POM) for agent-based campaigns. The agent can submit commands to POM via the desktop to, for example, hold, unhold, transfer and conference calls, create callbacks, get contact details, etc.; POM returns responses to the commands and can also send call notifications, agent state change notifications, etc. to the desktop.

2. General Test Approach and Test Results

The general test approach was to validate the ability of Desktop Connect to connect to both Application Enablement Services and POM to handle and control various Communication Manager endpoints in a variety of call scenarios. The feature test cases were performed both automatically and manually. Upon agent log in, the application automatically uses JTAPI to query device information, log the agent in, and request device monitoring. For the manual part of the testing, incoming ACD calls were placed with available agents that have web browser connections to Salesforce.com. Also, Outbound calls were generated using the Campaign Manager on POM. All necessary call actions were initiated from the agent desktop whenever possible, such as answer and drop. The click-to-dial calls were initiated by clicking on the contact phone number displayed on the agent desktop.

Note 1: Currently “agent blending” is not supported on Desktop Connect, compliance testing was carried out by connecting to Application Enablement Services and accepting inbound ACD calls only, and then connection to POM and accepting outbound campaign calls only.

Note 2: For Compliance testing, Desktop Connect was connected to the Salesforce Platform, and only that CRM was used for testing.

The serviceability test cases were performed manually by disconnecting and reconnecting the Ethernet connection to the Desktop Connect server and client, as well as the Application Enablement Services and Proactive Outreach Manager.

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 the Desktop Connect for Salesforce did not include use of any specific encryption features as requested by Geomant.

2.1. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability testing. The feature testing focused on verifying the following on Desktop Connect:

- Use of JTAPI/TSAPI query service to query agent states and device information and to monitor agent stations, skill groups, and VDNs.
- Use of JTAPI/TSAPI set value service to set agent states, including login, logout, and work mode changes.
- Use of JTAPI/TSAPI call control service to support call control and handling of call scenarios involving inbound, outbound, ACD, non-ACD, drop, hold/reconnect, voicemail, transfer, conference, multiple agents, multiple calls, different ANI/DNIS, internal, click-to-dial from contact phone number, pending aux work, and aux work reason codes.
- Use of POM Agent API to allow agents to support call control and handling of call scenarios involving outbound campaigns on POM.
- Serviceability testing.

The serviceability testing focused on verifying the ability of Desktop Connect to recover from adverse conditions, such as disconnecting/reconnecting the Ethernet connection to the Desktop Connect server and client.

2.2. Test Results

All test cases were executed and verified. The following observations were noted from compliance testing.

Note: Currently, “agent blending” is not supported on Desktop Connect, compliance testing was carried out by connecting to Application Enablement Services and accepting inbound ACD calls only, and then connection to POM and accepting outbound campaign calls only

AES Observations.

1. When executing a Supervised transfer, the agent desktop automatically places a 9 in front of the outbound number. However, when executing a Blind transfer, the agent desktop does not place a 9 in front of the outbound number.
2. In general, mixed use of agent desktop and telephone to perform call control actions are supported. For the transfer and conference features, however, all actions need to start and complete from the same source.
3. The application does not support TSAPI user credentials that contained the special character semicolon.

POM Observations.

1. There were less error messages displayed for incorrect logins, extensions and passwords when making mistakes logging into POM as there were for the AES login.
2. When in conference with an external party the agent cannot hang up and come out of the conference as the agent fails to pass ownership to the external party. There is an error message displayed on the agent’s screen to say as much, this is currently as per design.

2.3. Support

Technical support on Desktop Connect can be obtained through the following:

- **Phone:** +44 1789 387900
- **Email:** product_dc@support.geomant.com

3. Reference Configuration

Desktop Connect was deployed on a Windows 2019 server in the DevConnect lab with access to the internet and the ability to connect to the Salesforce platform to allow agents to log into the agent desktop using a web browser. Desktop Connect has two connections to Avaya Aura® platform, that being a JTAPI/TSAPI connection to Application Enablement Services and the Desktop API connection to Proactive Outreach Manager.

The detailed administration of basic connectivity between the Avaya components is not the focus of these Application Notes and will not be described.

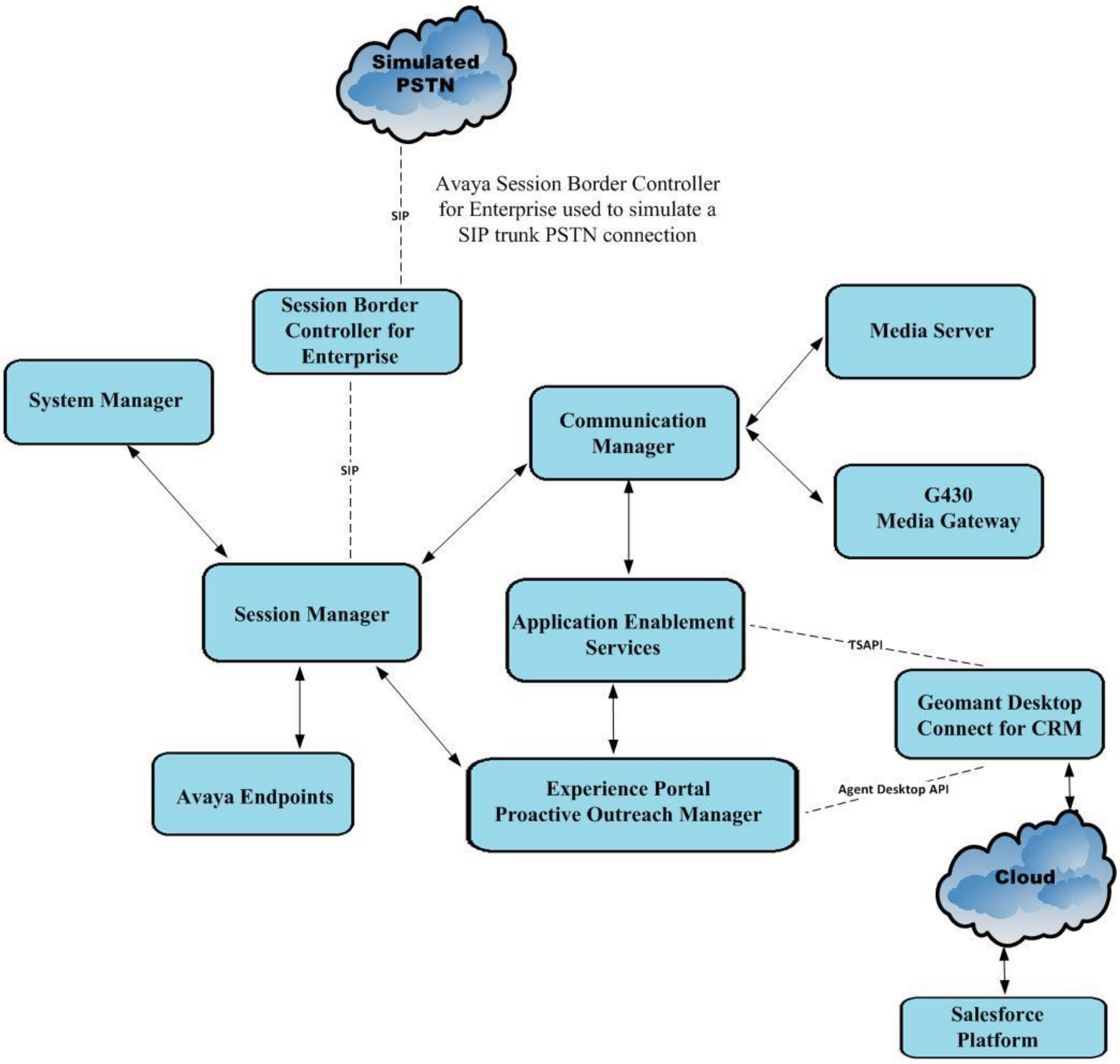


Figure 1: Compliance Testing Configuration

4. Equipment and Software Validated

The following equipment and software versions are used.

Avaya 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 Proactive Outreach Manager On Avaya Experience Portal	4.0.2 8.1.2
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 G450	42.7.0 /2
Avaya 9404 Digital phone	17.0
Avaya J100 Series phone (SIP)	7.1.2.0.14
Avaya J100 Series phone (H.323)	7.0.14.0.7
Avaya Agent for Desktop (SIP)	2.0.6.23.3005
Avaya Session Border Controller for Enterprise (to facilitate simulated PSTN)	10.1.0
Geomant Equipment/Software	**Release/Version**
Geomant Desktop Connect	4.2.0
Chrome Web Browser	111.0.5563.65

All equipment were running on VMware virtual servers.

5. Configure Avaya Aura® Communication Manager

The configuration and verification operations illustrated in this section are performed using the Communication Manager System Access Terminal (SAT). The information provided in this section describes the configuration of Communication Manager for this solution. For all other provisioning information such as initial installation and configuration, please refer to the product documentation as referenced in **Section 11**.

Some screens in this section have been abridged and highlighted for brevity and clarity in presentation. The general installation of the Media servers and G450 Media Gateway is presumed to have been previously completed and is not discussed here.

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

- Configure TSAPI Interface to Avaya Aura® Application Enablement Services
- Configure SIP trunk for Avaya Proactive Outreach Manager
- Configure Call Center Features
- Configure Avaya Endpoints for TSAPI monitoring

5.1. Configure TSAPI Interface to Avaya Aura® Application Enablement Services

The following sections illustrate the steps required to create the TSAPI link between Communication Manager and Application Enablement Services. It is assumed that the switch link (IP Services Interface) between Communication Manager and Application Enablement Services has already been setup as part of the installation of Application Enablement Services.

5.1.1. Verify System Features

Use the **display system-parameters customer-options** command to verify that Communication Manager has permissions for features illustrated in these Application Notes. On **Page 4**, ensure that **Computer Telephony Adjunct Links?** is set to **y** as shown below.

```
display system-parameters customer-options                    Page   4 of  12
                                OPTIONAL FEATURES

    Abbreviated Dialing Enhanced List? y          Audible Message Waiting? y
        Access Security Gateway (ASG)? y              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
          ASAI Link Core Capabilities? y                DCS Call Coverage? y
          ASAI Link Plus Capabilities? y               DCS with Rerouting? y
       Async. Transfer Mode (ATM) PNC? n
  Async. Transfer Mode (ATM) Trunking? n    Digital Loss Plan Modification? y
              ATM WAN Spare Processor? n                          DS1 MSP? y
                                 ATMS? y             DS1 Echo Cancellation? y
       (NOTE: You must logoff & login to effect the permission changes.)
```

5.1.2. Configure CTI Link for TSAPI Service

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
```

5.2. Configuration of the SIP Trunk for Avaya Proactive Outreach Manager

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

- Verify System Parameters Customer Options
- System Features and Access Codes
- Configure SIP Trunk

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

5.2.1. Verify System Parameters Customer Options

The license file installed on the system controls these attributes. If a required feature is not enabled or there is insufficient capacity, contact an authorized Avaya sales representative. Use the **display system-parameters customer-options** command to determine these values. On **Page 2**, verify that the **Maximum Administered SIP Trunks** have sufficient capacity. Each call uses a minimum of one SIP trunk.

```
display system-parameters customer-options                  Page   2 of  12
                                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
```

5.2.2. System Features and Access Codes

For the testing, **Trunk-to Trunk Transfer** was set to **all** on **Page 1** of the **system-parameters features** page. This is a system wide setting that allows calls to be routed from one trunk to another and is usually turned off to help prevent toll fraud. An alternative to enabling this feature on a system wide basis is to control it using COR (Class of Restriction). See **Section 11** 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 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: #2
```

5.2.3. Configure SIP Trunk

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

```
display node-names ip                                         Page   1 of   2
                                  IP NODE NAMES
    Name               IP Address
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
```

In the **IP Network Region** form, the **Authoritative Domain** field is configured to match the domain name configured on Session Manager. In this configuration, the domain name is **greaneyp.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: greaneyp.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      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 Session Manager and POM. The form is accessed via the **change ip-codec-set n** command. Note that IP codec set 1 was specified in IP Network Region 1 shown above. Multiple codecs may be specified in the **IP Codec Set** form in order of preference; the example below includes **G.711A** (a-law), which is supported by POM. Note the **Media Encryption** includes a setting of **none** to allow for unencrypted media.

```
change 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.729A            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 appropriate setting, in this case it was set to **tls**.
- The **Peer Detection Enabled** field should be set to **y** allowing the Communication Manager to automatically detect if the peer server is a Session Manager.
- Specify the node names for the procr and the Session Manager node name as the two ends of the signaling group in the **Near-end Node Name** field and the **Far-end Node Name** field, respectively. These values are taken from the **IP Node Names** form shown above.
- Set the **Near-end Node Name** to **procr**. This value is taken from the **IP Node Names** form shown above.
- Set the **Far-end Node Name** to the node name defined for the Session Manager (node name **sm101x**).
- Ensure that the recommended TLS port value of **5062** 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.
- **Far-end Domain** was set to the domain used during 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**.
- **Initial IP-IP Direct Media** is set to **n**.
- The default values for the other fields may be used.

```
change signaling-group 1                                        Page   1 of   2
                                SIGNALING GROUP

 Group Number: 1             Group Type: sip
  IMS Enabled? n        Transport Method: 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: 5062                 Far-end Listen Port: 5062
                                         Far-end Network Region: 1

Far-end Domain: greaneyp.sil6.avaya.com
                                             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
                                                  Alternate Route Timer(sec): 6
```

Configure the **Trunk Group** form as shown below. This trunk group is used for calls to and from POM via Session Manager. Enter a descriptive name in the **Group Name** field. Set the **Group Type** field to **sip**. Enter a **TAC** code compatible with the Communication Manager dial plan. Set the **Service Type** field to **tie**. Specify the signaling group associated with this trunk group in the **Signaling Group** field and specify the **Number of Members** supported by this SIP trunk group. Accept the default values for the remaining fields.

```
change trunk-group 1                                        Page   1 of  4
                                TRUNK GROUP

Group Number: 1                   Group Type: sip           CDR Reports: y
  Group Name: SIP TRK                    COR: 1        TN: 1     TAC: *801
   Direction: two-way       Outgoing Display? y
 Dial Access? n                                Night Service:
Queue Length: 0
Service Type: tie                 Auth Code? n
                                             Member Assignment Method: auto
                                                      Signaling Group: 1
                                                    Number of Members: 10
```

On **Page 2** of the trunk-group form the **Preferred Minimum Session Refresh Interval (sec)** field should be set to a value mutually agreed with Geomant to prevent unnecessary SIP messages during call setup. Session refresh is used throughout the duration of the call, to check the other side has not gone away, for the compliance test a value of **600** was used.

```
change trunk-group 1                                        Page   2 of  4
      Group Type: sip

TRUNK PARAMETERS

     Unicode Name: auto

                                            Redirect On OPTIM Failure: 5000

            SCCAN? n                                Digital Loss Group: 18
                      Preferred Minimum Session Refresh Interval(sec): 600

 Disconnect Supervision - In? y  Out? y


           XOIP Treatment: auto    Delay Call Setup When Accessed Via IGAR? n
```

Settings on **Page 3** can be left as default. However, the **Numbering Format** in the example below is set to **private**.

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



   Suppress # Outpulsing? n  Numbering Format: private
                                            UUI Treatment: service-provider

                                              Replace Restricted Numbers? n
                                             Replace Unavailable Numbers? n

                                Modify Tandem Calling Number: no




 Show ANSWERED BY on Display? y
```

Settings on **Page 4** are as follows; ensure that the **Telephone Event Payload Type** is set to **101**. Ensure that **Support Request History** is set to **y**.

```
change trunk-group 1                                           Page   4 of  21
                              PROTOCOL VARIATIONS

                                       Mark Users as Phone? n
Prepend '+' to Calling/Alerting/Diverting/Connected Number? n
                       Send Transferring Party Information? y
                                  Network Call Redirection? y
          Build Refer-To URI of REFER From Contact For NCR? n
                                     Send Diversion Header? n
                                   Support Request History? y
                              Telephone Event Payload Type: 101


                      Convert 180 to 183 for Early Media? n
                Always Use re-INVITE for Display Updates? n
                      Identity for Calling Party Display: P-Asserted-Identity
          Block Sending Calling Party Location in INVITE? n
               Accept Redirect to Blank User Destination? n
                                            Enable Q-SIP? n

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

5.3. Configure Call Center Features

The following were set to allow both inbound ACD calls into the Agents and outbound campaign calls delivered to the agents logged into Desktop Connect, specifically Salesforce.

- Configure Hunt Groups
- Configure Vectors
- Configure Vector Directory Number (VDN)
- Configure Agents
- Configure Reason Codes

5.3.1. Configure Hunt Groups

Enter the command **add hunt-group x** where **x** is an appropriate hunt group number and configure as follows:

- **Group Number** – this is the Skill Number when configuring the agent and vector.
- **Group Name** – enter an appropriate name.
- **Group Extension** – enter an extension appropriate to the dialplan.
- **Group Type** – set to **ucd-mia**.
- **ACD?** – set to **y**.
- **Queue?** – set to **y**.
- **Vector?** – set to **y**.

```
add hunt-group 90                                            Page   1 of   4
                                  HUNT GROUP

            Group Number: 90                                    ACD? y
              Group Name: Sales                               Queue? y
         Group Extension: 1800                               Vector? y
              Group Type: ucd-mia
                      TN: 1
                     COR: 1                        MM Early Answer? n
           Security Code:                   Local Agent Preference? n
 ISDN/SIP Caller Display:

             Queue Limit: unlimited
 Calls Warning Threshold:      Port:
  Time Warning Threshold:      Port:
```

On **Page 2**, set **Skill** to **y**.

```
add hunt-group 90                                              Page   2 of   4
                                  HUNT GROUP

                    Skill? y      Expected Call Handling Time (sec): 180
                      AAS? n        Service Level Target (% in sec): 80 in 20
                 Measured: none
     Supervisor Extension:


      Controlling Adjunct: none


        VuStats Objective:

   Multiple Call Handling: none


 Timed ACW Interval (sec):          After Xfer or Held Call Drops? n
```

A hunt group is setup for outbound calls. The outbound hunt group is referenced in **Appendix A** as a Skill in POM. Enter the **add hunt-group n** command where **n** in the example below is **10**. On **Page 1** of the **hunt-group** form, assign a **Group Name** and **Group Extension** valid under the provisioned dial plan. **Group Type** should be set to **ead-mia**. **ACD**, **Queue** and **Vector** set to **y**.

```
add hunt-group 10                                             Page   1 of   4
                                  HUNT GROUP
            Group Number: 10                                ACD? y
              Group Name: Outbound                        Queue? y
         Group Extension: 1801                           Vector? y
              Group Type: ead-mia
                      TN: 1
                     COR: 1                    MM Early Answer? n
           Security Code:               Local Agent Preference? n
 ISDN/SIP Caller Display:

             Queue Limit: unlimited
 Calls Warning Threshold:      Port:
  Time Warning Threshold:      Port:
```

On **Page 2**, set the **Skill** field to **y** as shown below.

```
add hunt-group 10                                               Page   2 of   4
                                  HUNT GROUP

                    Skill? y      Expected Call Handling Time (sec): 180
                      AAS? n
                 Measured: none
     Supervisor Extension:


      Controlling Adjunct: none




   Multiple Call Handling: none


 Timed ACW Interval (sec):          After Xfer or Held Call Drops? n
```

5.3.2. Configure Vectors

Enter the command **change vector x** where **x** is the required vector number. Configure as shown below so that calls **queue-to skill 1st**. Skill 1st is the hunt group configured in the VDN in **Section 5.3.3**.

```
change vector 1                                                 Page   1 of   6
                                  CALL VECTOR

    Number: 1                  Name: Basic Routing
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 wait-time    2   secs hearing ringback
02 queue-to     skill 1st pri m
03 wait-time    100 secs hearing music
04 goto step    3             if unconditionally
05 stop
06
07
08
09
```

5.3.3. Configure Vector Directory Number (VDN)

Enter the command **add vdn x** where **x** is the required VDN number appropriate to the dialplan. Configure the VDN to send calls to the vector configured in the previous section as follows:

- **Extension** – note the VDN extension number which will be used to place calls to the Skill vector and on to the Skill.
- **Name** – enter an appropriate name.
- **Destination** – enter the **Vector Number** configured in the previous section.
- **1st Skill** – enter the hunt group created in **Section 5.3.1**.

```
add vdn 3901                                                 Page   1 of   3
                          VECTOR DIRECTORY NUMBER

                           Extension: 3901                    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
```

5.3.5. Administer Class of Restriction

Enter the **change cor x** command where **x** corresponds to the Class of Restriction to be used for the agent login IDs in **Section 5.3.6**. On **Page 1**, set the **Direct Agent Calling** to **n**, this will allow agents to be called directly once they are logged in and in Aux Work. With Direct Agent Calling set to y, POM could not call the agent to Nail Up the call, the agent would send back a "no answer" as they were in Aux Work. Setting Direct Agent Calling to n solved this issue.

```
change cor 1                                                Page   1 of  23
                              CLASS OF RESTRICTION

               COR Number: 1
          COR Description: DefaultCOR_PG

                      FRL: 0                                APLT? y
  Can Be Service Observed? y          Calling Party Restriction: none
Can Be A Service Observer? y           Called Party Restriction: none
        Time of Day Chart: 1      Forced Entry of Account Codes? n
         Priority Queuing? n               Direct Agent Calling? n
     Restriction Override: none      Facility Access Trunk Test? y
     Restricted Call List? n                Can Change Coverage? n

            Access to MCT? y           Fully Restricted Service? n
Group II Category For MFC: 7           Hear VDN of Origin Annc.? n
         Send ANI for MFE? n            Add/Remove Agent Skills? n
            MF ANI Prefix:             Automatic Charge Display? n
Hear System Music on Hold? y   PASTE (Display PBX Data on Phone)? n
                        Can Be Picked Up By Directed Call Pickup? y
                                    Can Use Directed Call Pickup? y
                                    Group Controlled Restriction: inactive
```

5.3.6. Configure Agents

Agents must be configured with the appropriate Skill Number. Enter the command **add agent-loginID x** where **x** is an agent extension number appropriate to the dialplan and configure as follows:

- **Login ID** – take a note of the configured **Login ID**.
- **Name** – enter an identifying name.
- **Password –** enter a suitable password of the agent.

```
add agent-loginID 3402                                          Page   1 of   2
                                 AGENT LOGINID

                Login ID: 3402                Unicode Name? n   AAS? n
                    Name: Agent two                           AUDIX? n
                      TN: 1        Check skill TNs to match agent TN? n
                     COR: 1
           Coverage Path:                             LWC Reception: spe
           Security Code:                      LWC Log External Calls? n
           Attribute:                        AUDIX Name for Messaging:

                                         LoginID for ISDN/SIP Display? n
                                                           Password:1234
                                             Password (enter again):1234
                                                        Auto Answer: station
 AUX Agent Remains in LOA Queue: system              MIA Across Skills: system
AUX Agent Considered Idle (MIA): system    ACW Agent Considered Idle: system
             Work Mode on Login: system    Aux Work Reason Code Type: system
                                              Logout Reason Code Type: system
                       Maximum time agent in ACW before logout (sec): system
                                             Forced Agent Logout Time:   :
    WARNING:  Agent must log in again before changes take effect
```

On **Page 2**, enter the hunt group number configured in **Section 5.3.1** in the **SN** (Skill Number) column and enter an appropriate **SL** (skill level).

```
add agent-loginID 3402                                          Page   2 of   2
                                 AGENT LOGINID
      Direct Agent Skill: 90                               Service Objective? n
Call Handling Preference: skill-level                  Local Call Preference? n

    SN   RL SL          SN   RL SL
 1: 90      1       16:
 2: 10      1       17:
 3:                 18:
 4:                 19:
 5:                 20:
 6:
 7:
 8:
```

5.3.7. Configure Reason Codes

For contact centers that use reason codes, enter the "change reason-code-names" command to display the configured reason codes. Make a note of the **Aux Work** reason codes, which will be used later to configure Desktop Connect.

Note: Desktop Connect supports up to six reason codes for aux work, and none for log out.

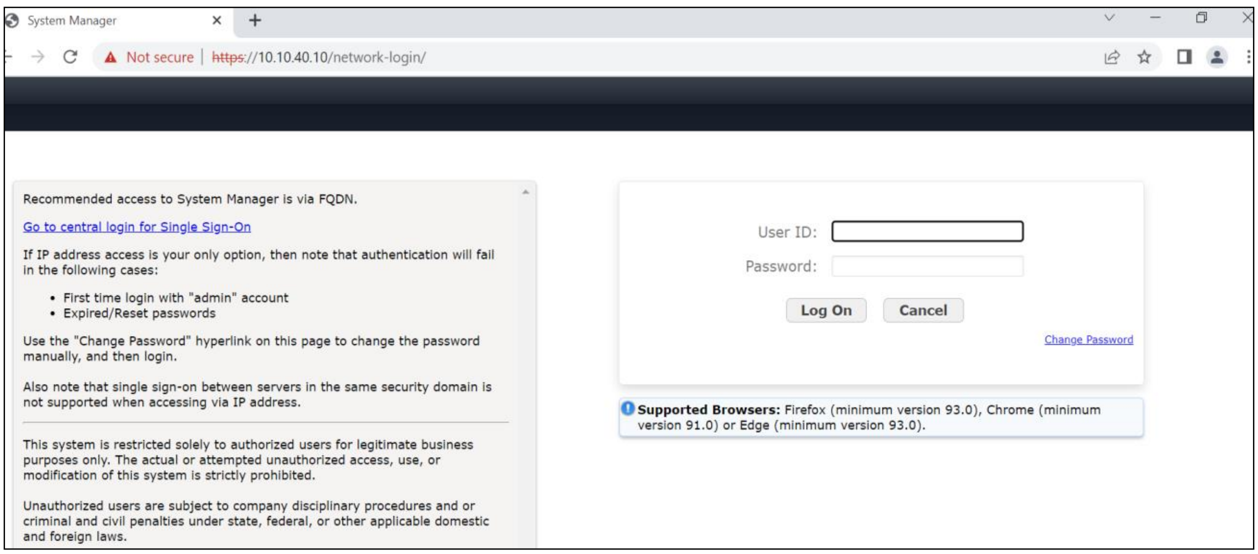
```
change reason-code-names                                        Page   1 of   3

                                REASON CODE NAMES

                           Aux Work/           Logout
                        Interruptible?

        Reason Code 1: Bathroom           /n
        Reason Code 2: Breakfast          /n
        Reason Code 3: Lunch              /n
        Reason Code 4: Meeting            /n
        Reason Code 5: Training           /n
        Reason Code 6: Meeting            /n
        Reason Code 7:                    /n
        Reason Code 8:                    /n
        Reason Code 9:                    /n

  Default Reason Code:
```

5.4. Configure Avaya Endpoints for TSAPI Monitoring

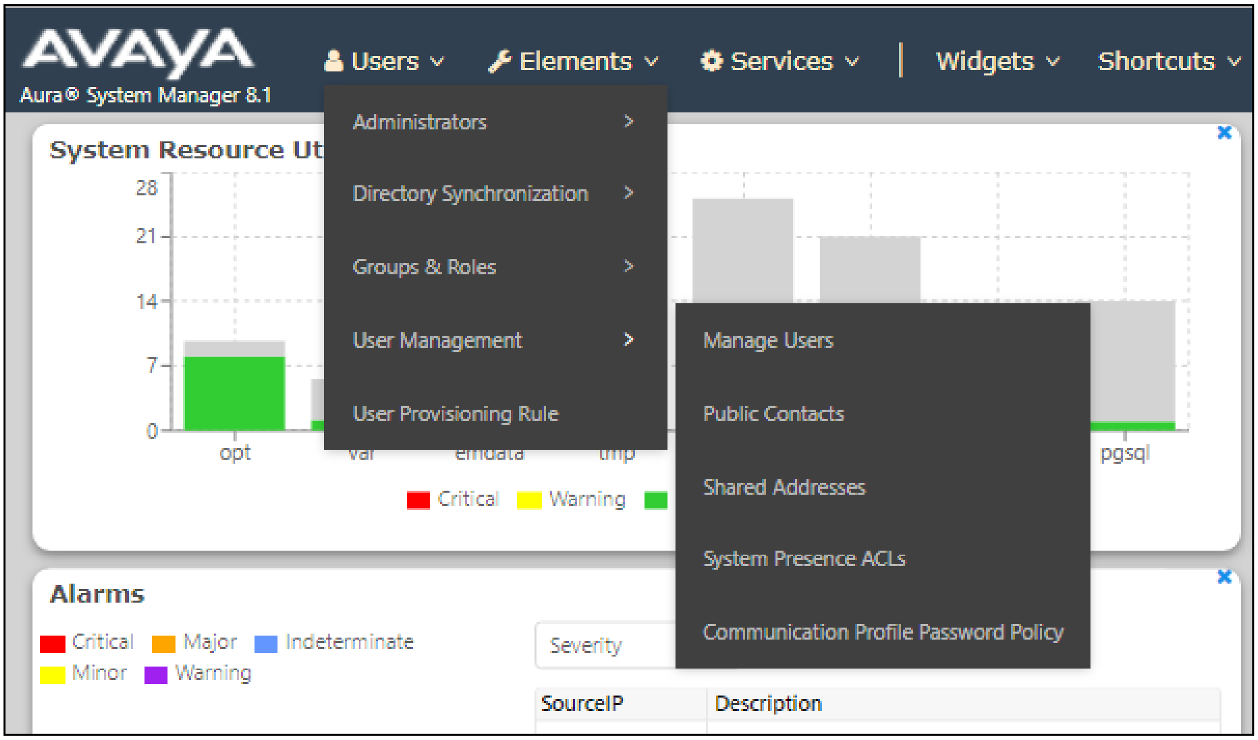
There is no extra configuration needed on the Avaya H.323 or Digital endpoints to allow them to be monitored by TSAPI. However, each Avaya SIP endpoint or station that needs to be monitored and used for 3rd party call control will need to have “Type of 3PCC Enabled” is set to “Avaya”.

Changes to SIP phones on Communication Manager must be carried out by System Manager. Access the System Manager using a Web Browser by entering **http://<FQDN >/network-login**, where **<FQDN>** is the fully qualified domain name of System Manager, or the IP address of System Manager can be used as an alternative to the FQDN. Log in using the appropriate credentials.

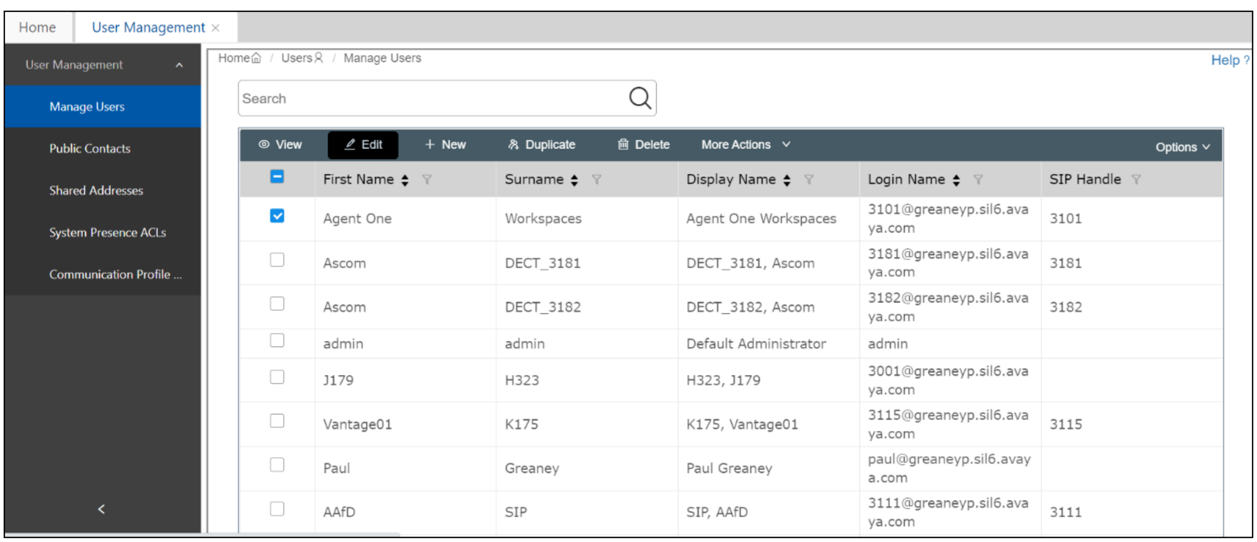
Note: The following shows changes a SIP extension and assumes that the SIP extension has been programmed correctly and is fully functioning.



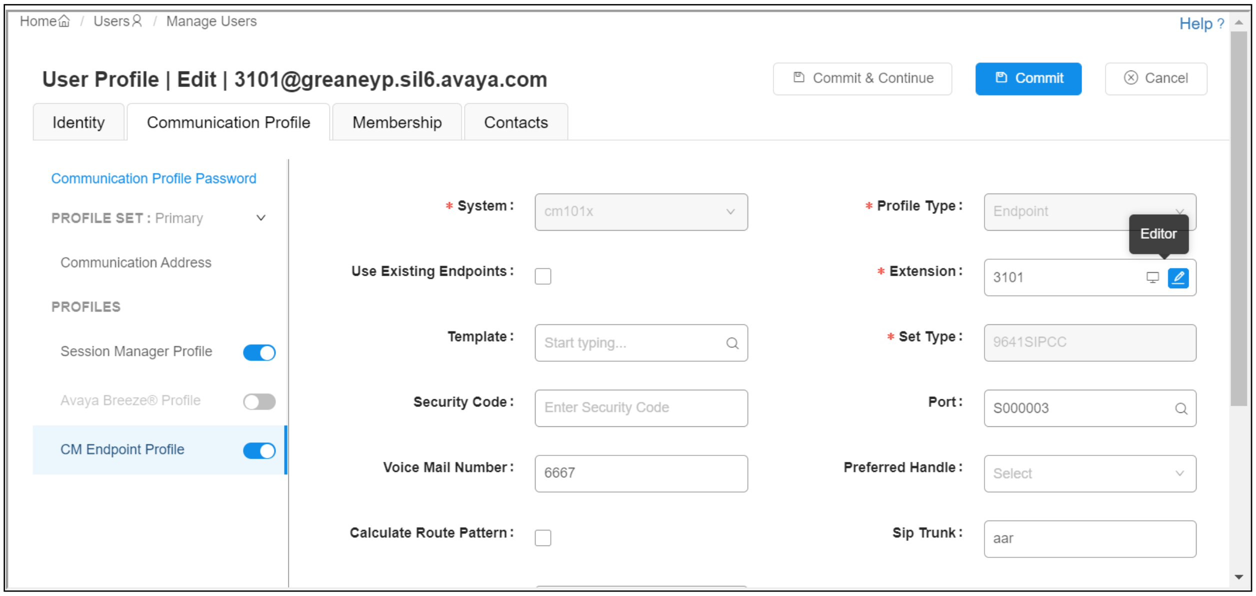
From the home page, click on **Users** → **User Management** → **Manage Users**, as shown below.



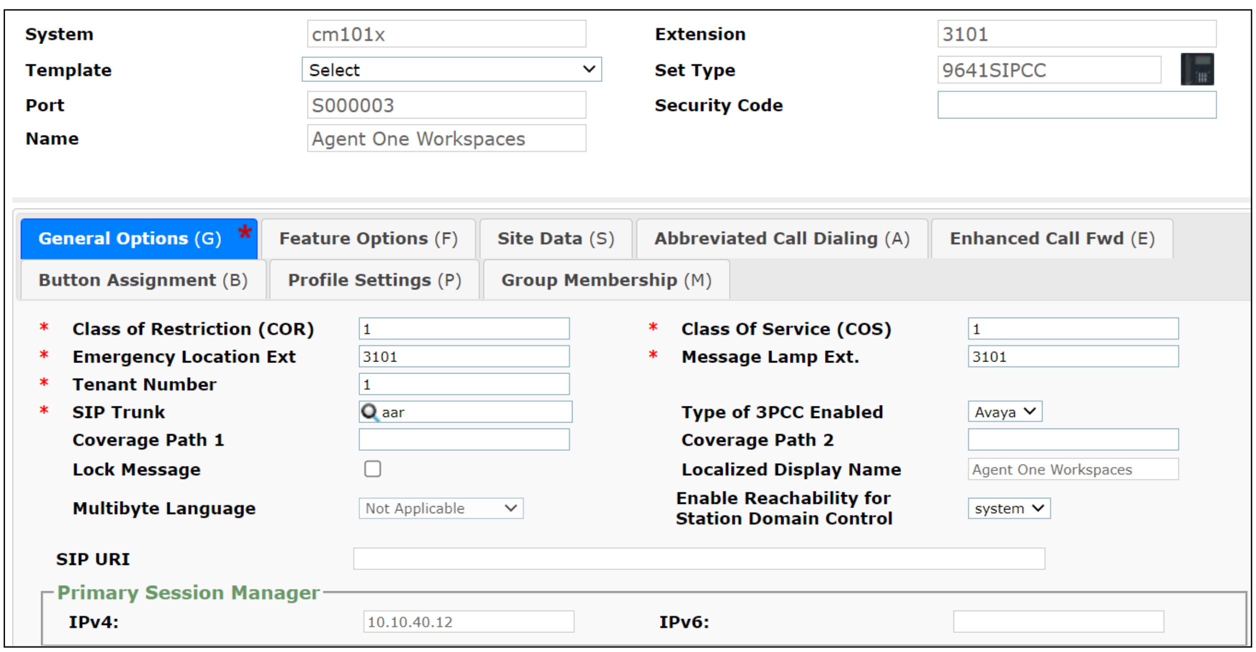
Click on **Manager Users** in the left window. Select the station to be edited and click on **Edit**.



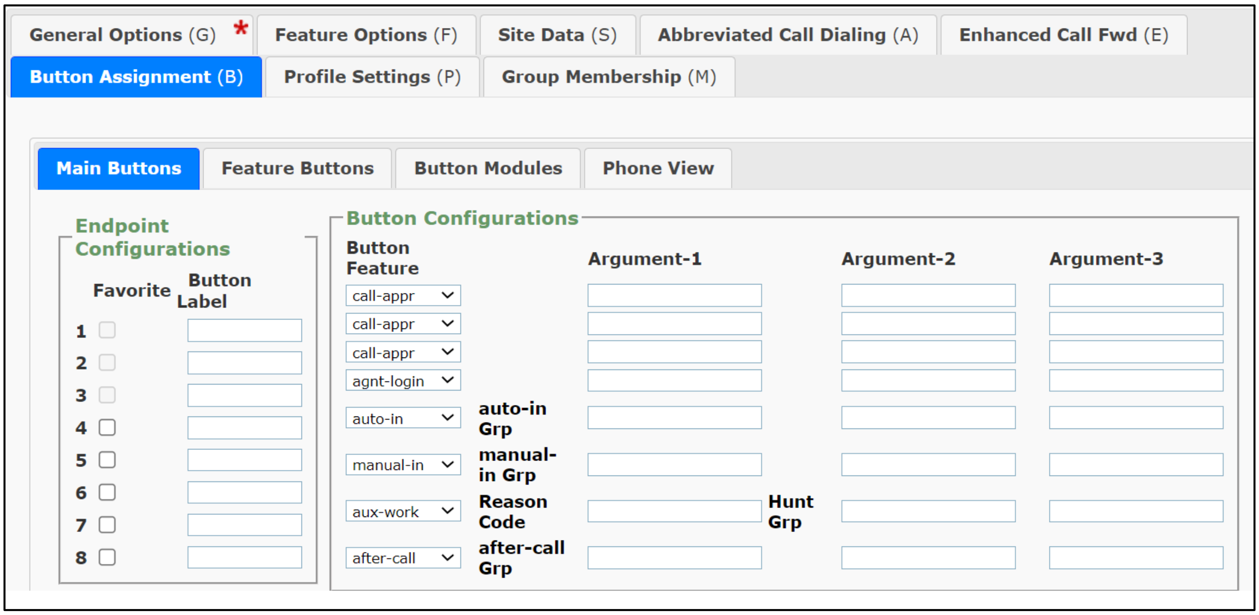
Click on the **CM Endpoint Profile** tab in the left window. Click on **Endpoint Editor** to make changes to the SIP station.



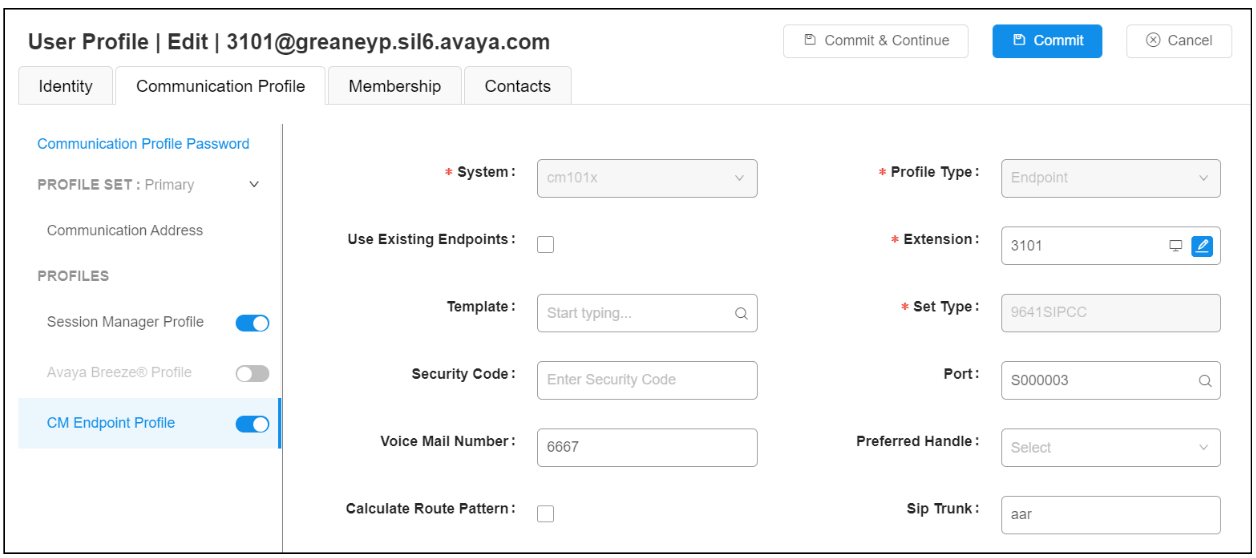
In the **General Options** tab ensure that **Type of 3PCC Enabled** is set to **Avaya** as is shown below.



The buttons were set as shown below but these are not critical to the overall operation of Centricity. Click on **Done** at the bottom of the screen (not shown).



Click on **Commit** once this is done to save the changes.



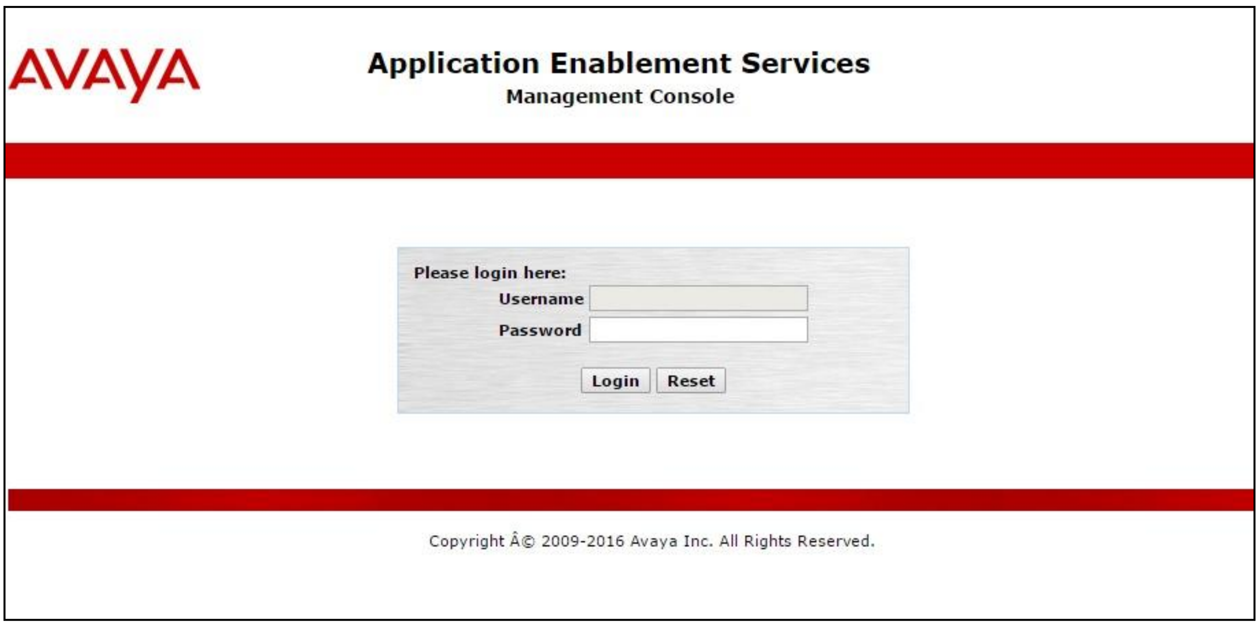
6. Configure Avaya Aura® Application Enablement Services

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

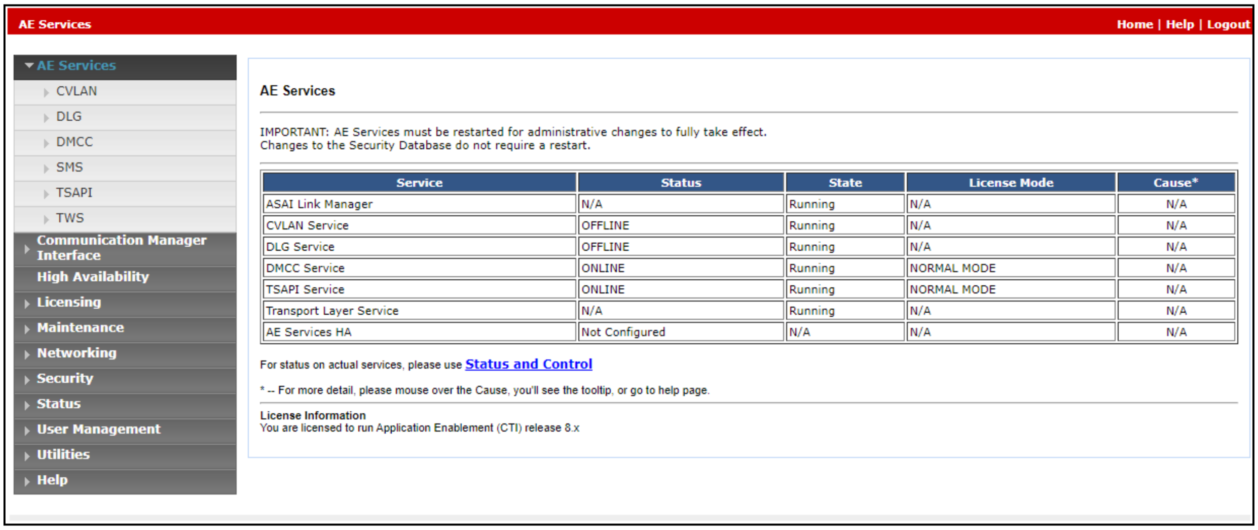
- Verify Licensing
- Administer TSAPI Link
- Identify Tlinks
- Enable TSAPI Ports
- Create CTI User
- Configure Security
- Restart AE Server

6.1. Verify Licensing

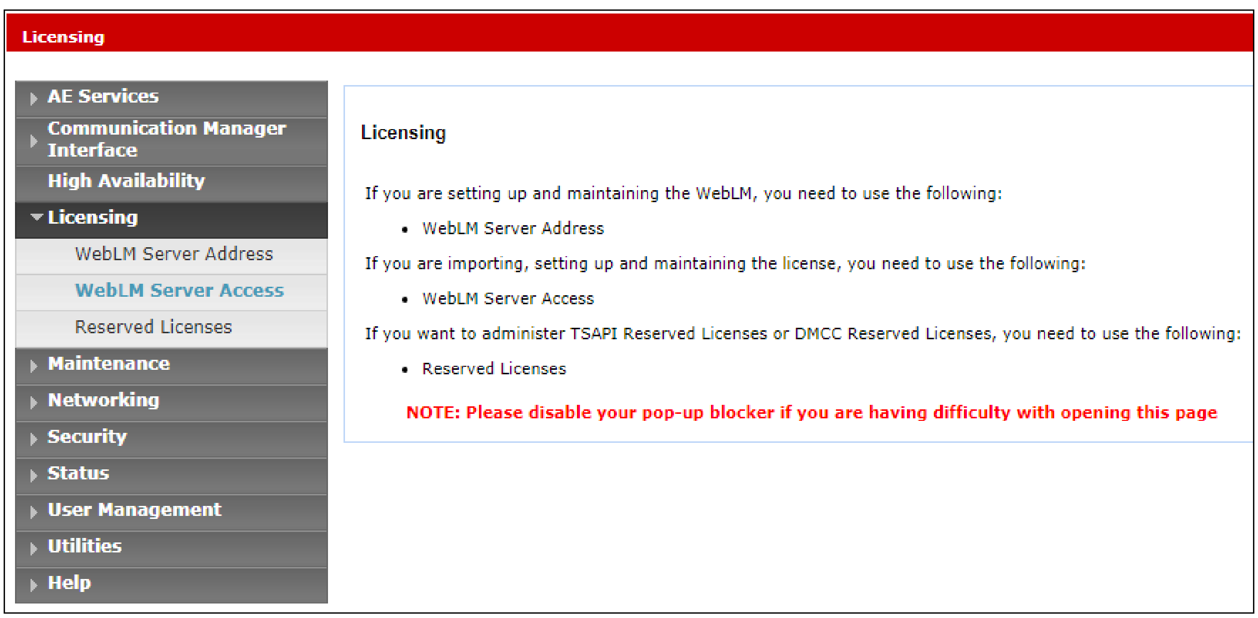
To access the AES Management Console, enter **https://<ip-addr>** as the URL in an Internet browser, where <ip-addr> is the IP address of the AES. At the login screen displayed, log in with the appropriate credentials and then select the **Login** button.



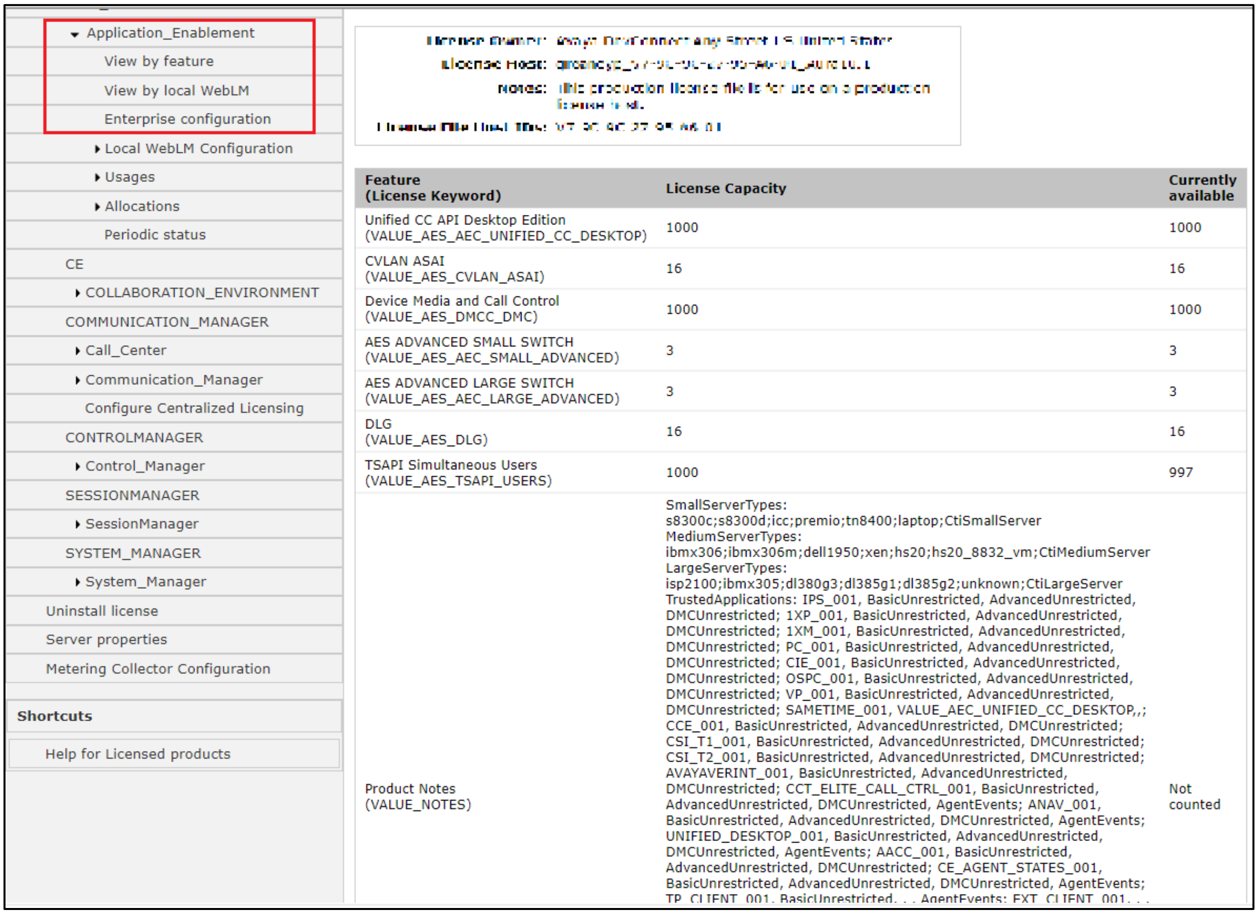
The Application Enablement Services Management Console appears displaying the **Welcome to OAM** screen (not shown). Select **AE Services** and verify that the TSAPI Service is licensed by ensuring that **TSAPI Service** is in the list of **Services** and that the **License Mode** is showing **NORMAL MODE**. If not, contact an Avaya support representative to acquire the appropriate license.



The TSAPI license is a 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.

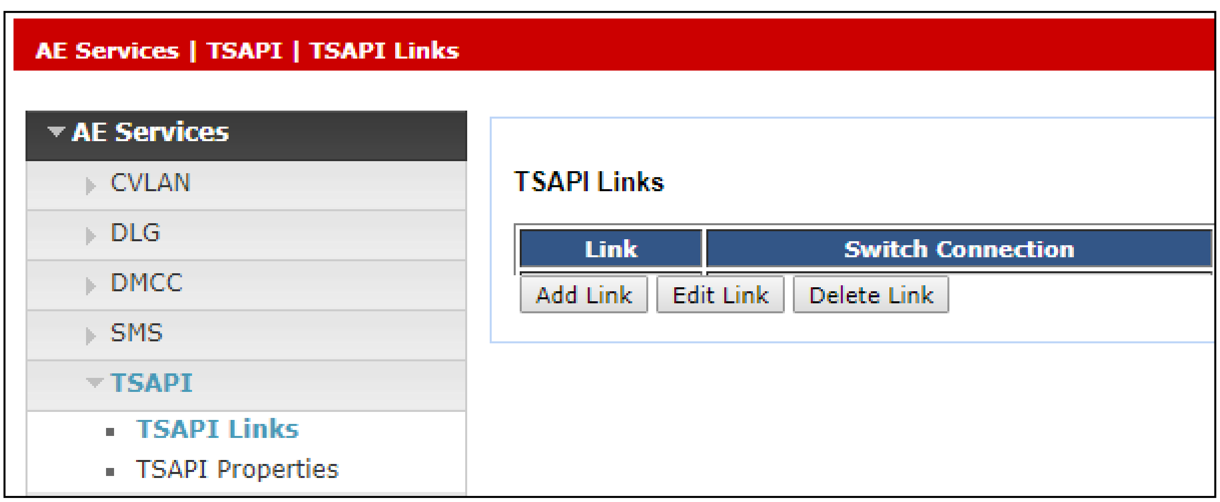


The following screen shows the available licenses for **TSAPI** users.



6.2. Administer TSAPI link

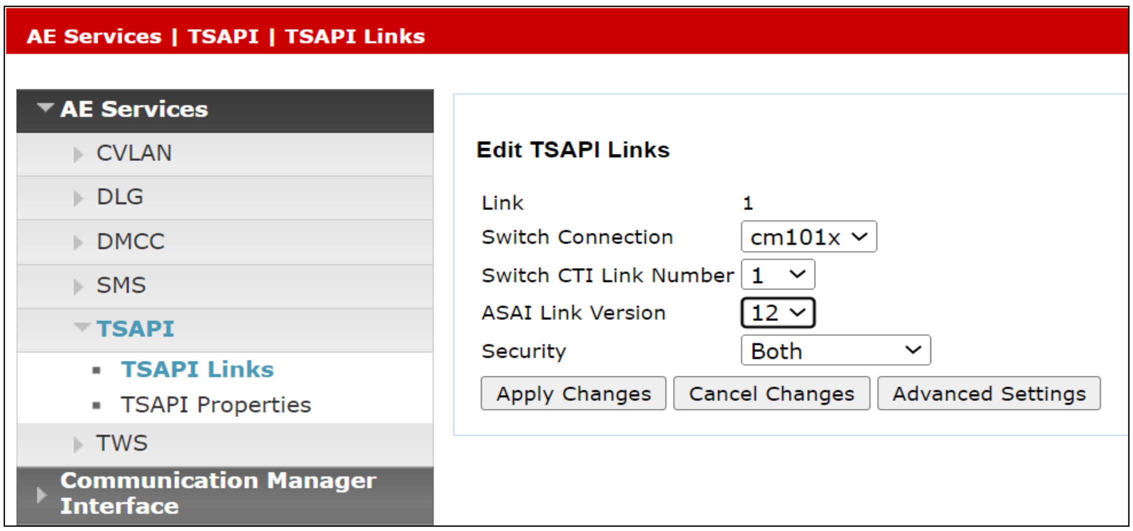
From the Application Enablement Services Management Console, select **AE Services → TSAPI → TSAPI Links**. Select **Add Link** button as shown in the screen below.



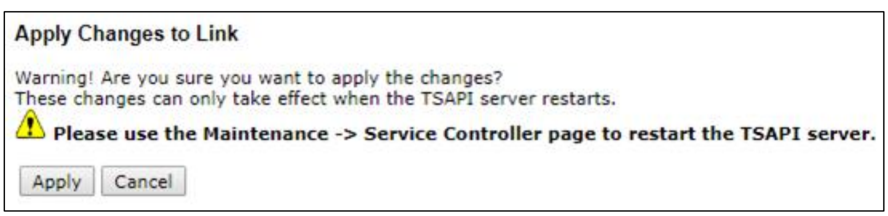
On the **Add TSAPI Links** screen (or the **Edit TSAPI Links** screen to edit a previously configured TSAPI Link as shown below), enter the following values:

- **Link:** Use the drop-down list to select an unused link number.
- **Switch Connection:** Choose the appropriate switch connection **cm101x**, which has already been configured from the drop-down list.
- **Switch CTI Link Number:** Corresponding CTI link number configured in **Section 5.1.2** which is **1**.
- **ASAI Link Version:** This should be set to the highest version available.
- **Security:** This should be set to **Both** allowing both secure and nonsecure connections.

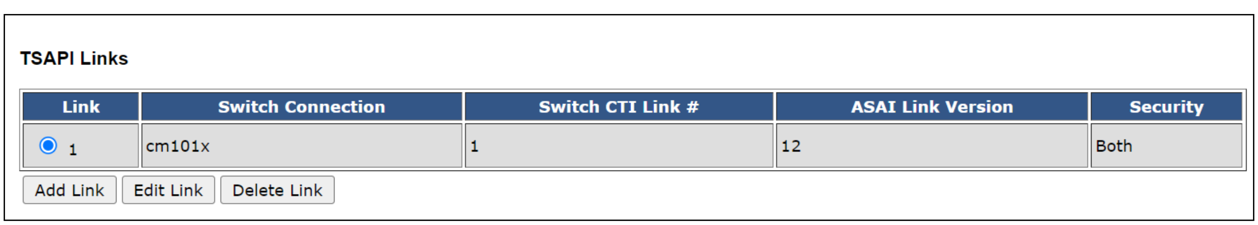
Once completed, select **Apply Changes**.



Another screen appears for confirmation of the changes made. Choose **Apply**.

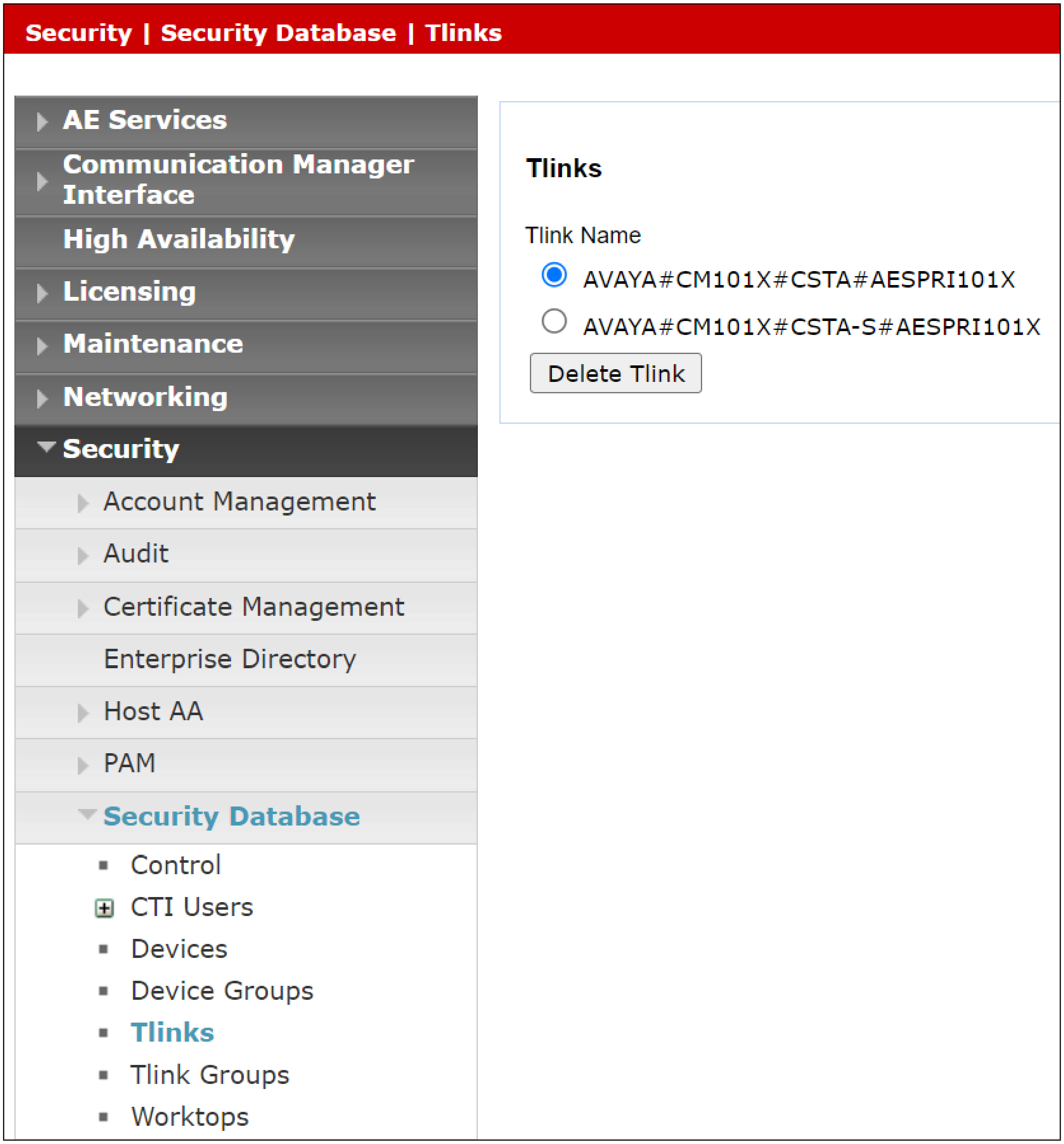


When the TSAPI Link is completed, it should resemble the screen below.



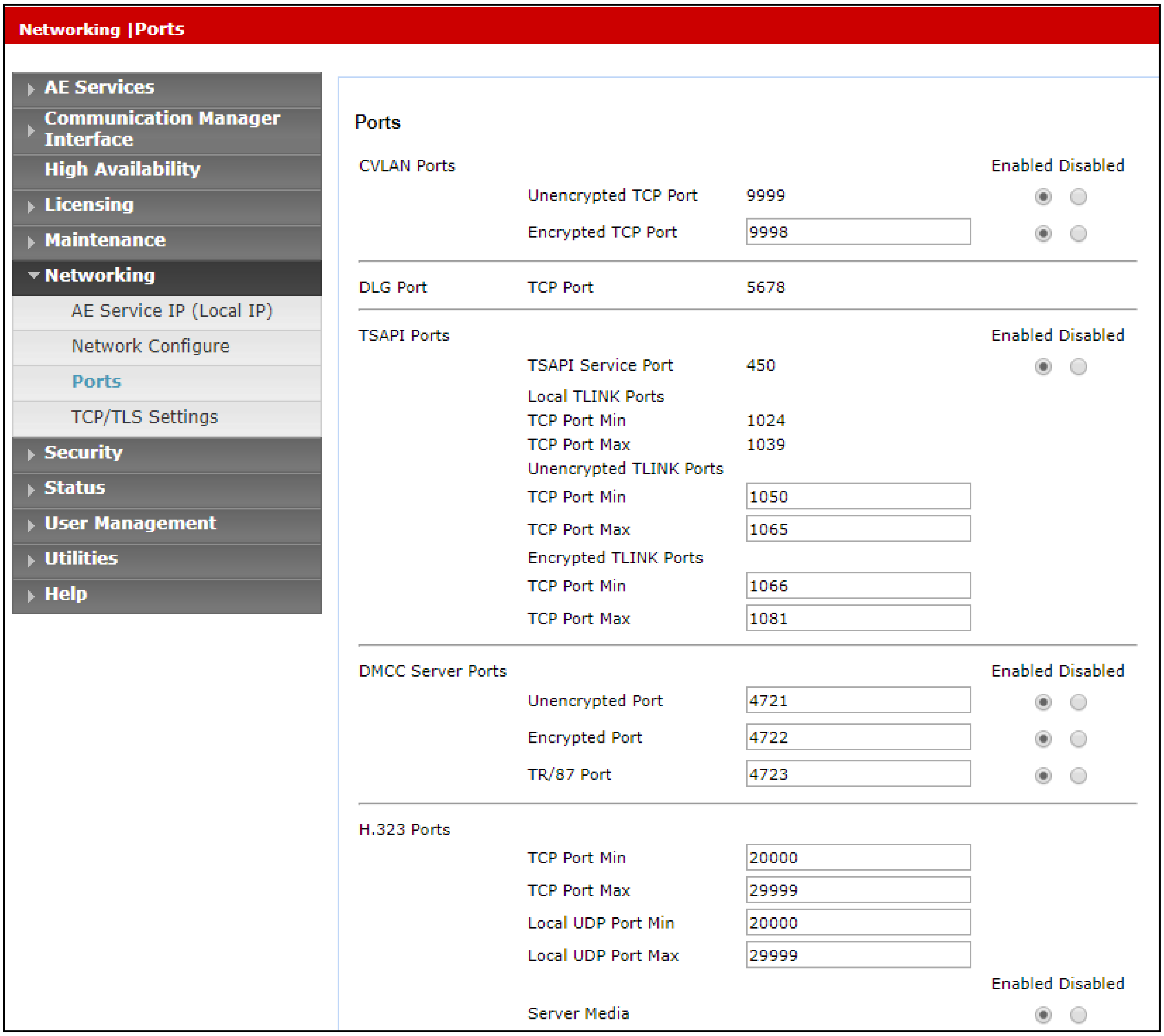
6.3. Identify Tlinks

Navigate to **Security → Security Database → Tlinks**. Verify the value of the **Tlink Name**. This will be needed to configure Desktop Connect.



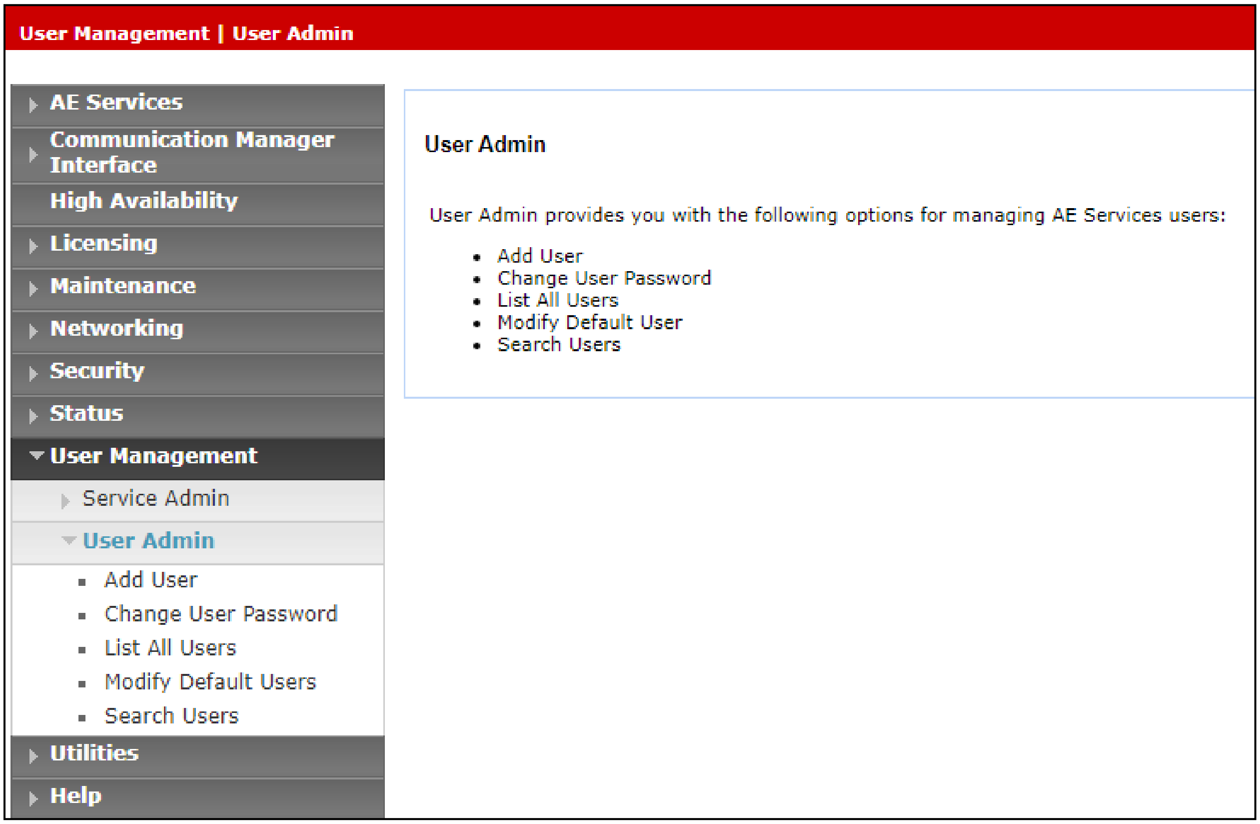
6.4. Enable TSAPI Ports

To ensure that TSAPI ports are enabled, navigate to **Networking → Ports**. Ensure that the TSAPI ports are set to **Enabled** as shown below.



6.5. Create CTI User

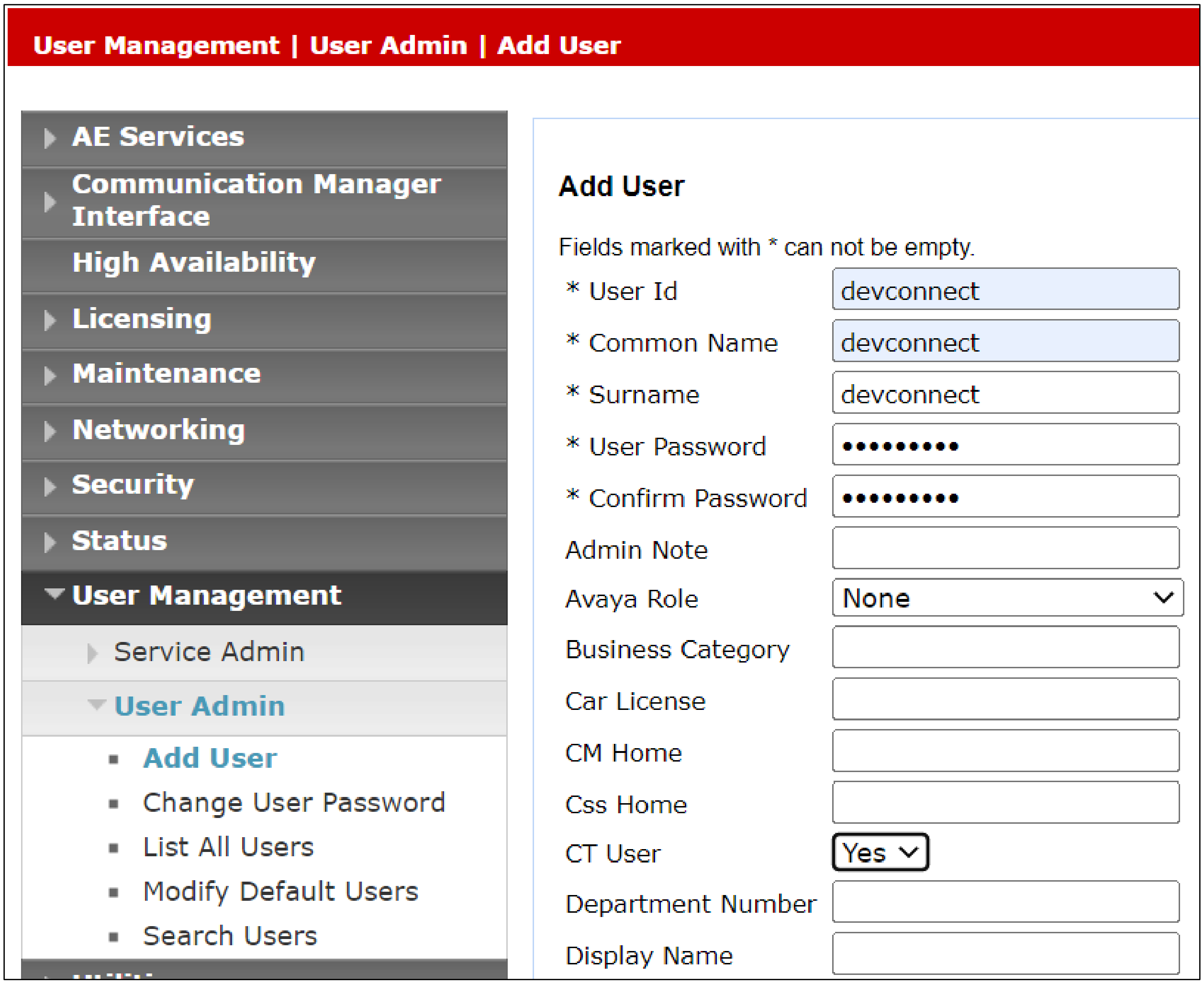
A user ID and password needs to be configured for Desktop Connect to communicate with the Application Enablement Services server. Navigate to the **User Management → User Admin** screen then choose the **Add User** option.



In the **Add User** screen shown below, enter the following values:

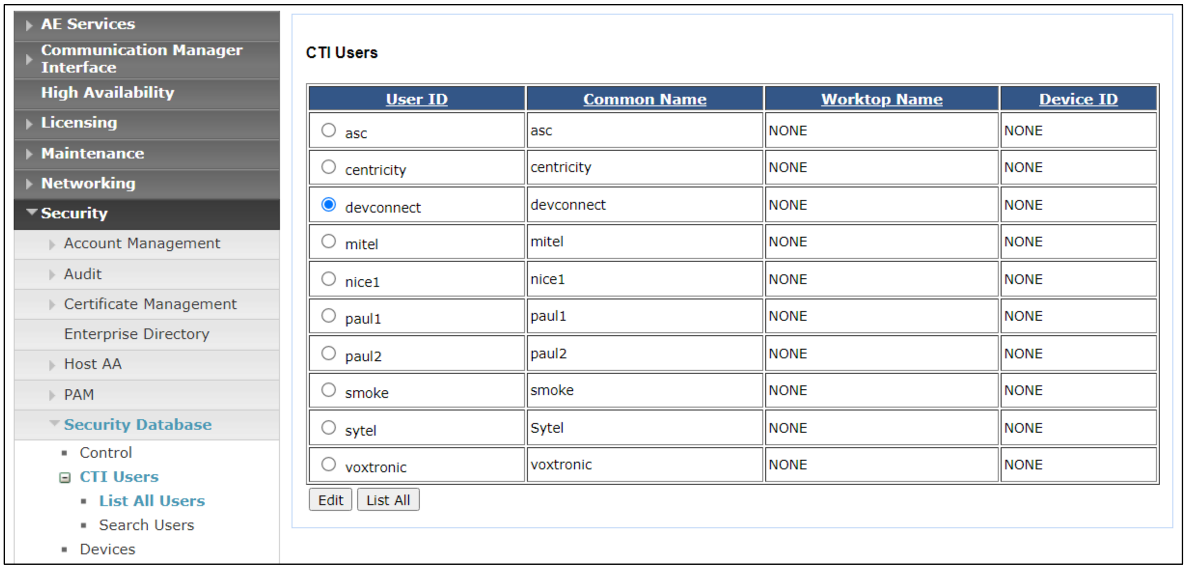
- **User Id -** This will be used by Desktop Connect.
- **Common Name** and **Surname -** Descriptive names need to be entered.
- **User Password** and **Confirm Password -** This will be used by Desktop Connect.
- **CT User -** Select **Yes** from the drop-down menu.

Click on **Apply Changes** at the bottom of the screen.

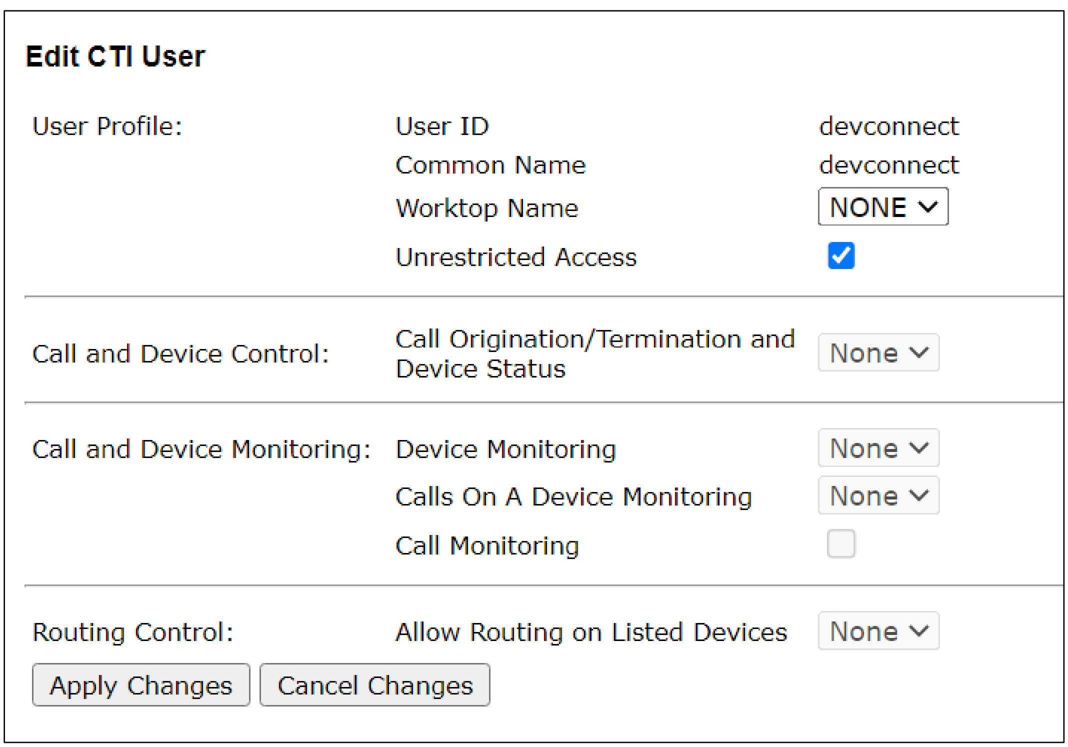


6.6. Associate Devices with CTI User

Navigate to **Security → Security Database → CTI Users → List All Users**. Select the CTI user added in **Section 6.5** and click on **Edit**.



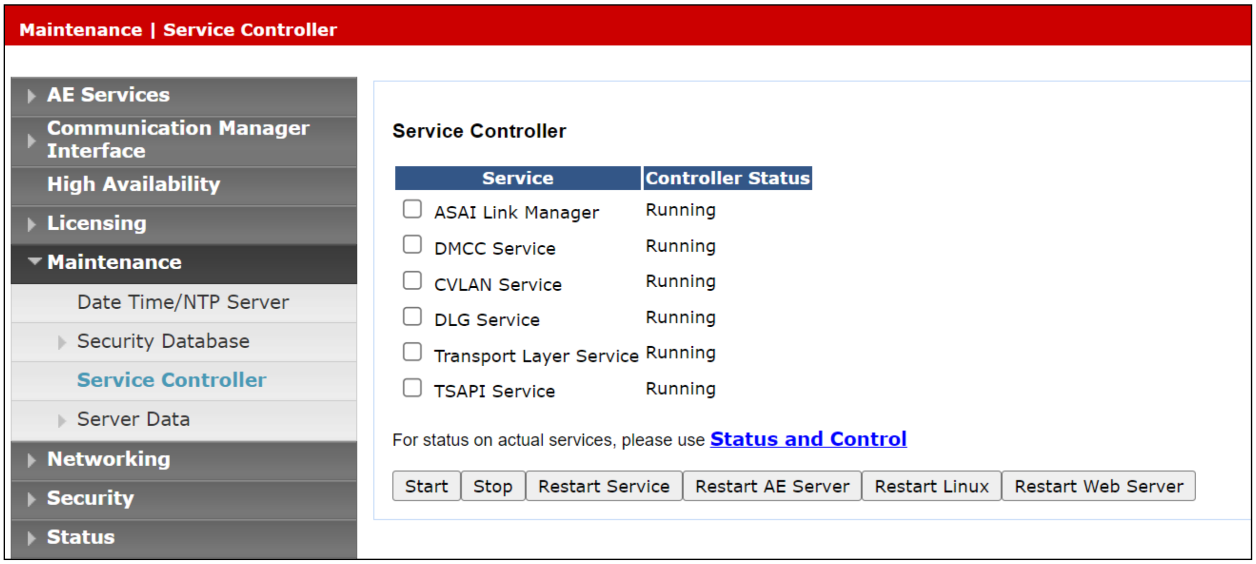
In the main window ensure that **Unrestricted Access** is ticked. Once this is done click on **Apply Changes**.



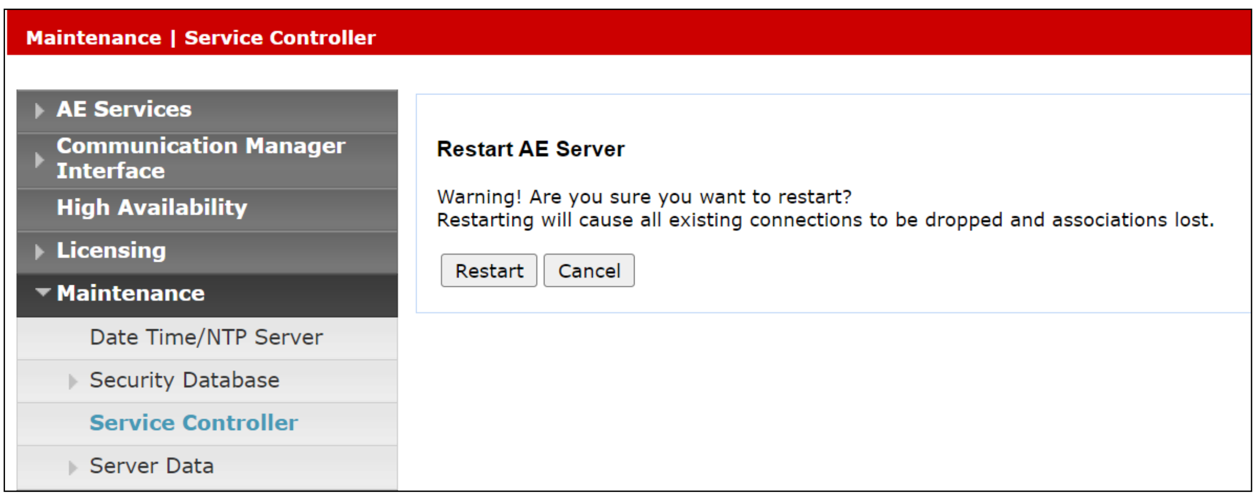
Click on **Apply** when asked again to **Apply Changes** (not shown).

6.7. Restart AE Server

Once everything is configured correctly, it is best practice to restart AE Server (if possible), this will ensure that the new connections are brought up correctly. Click on the **Restart AE Server** button at the bottom of the screen.



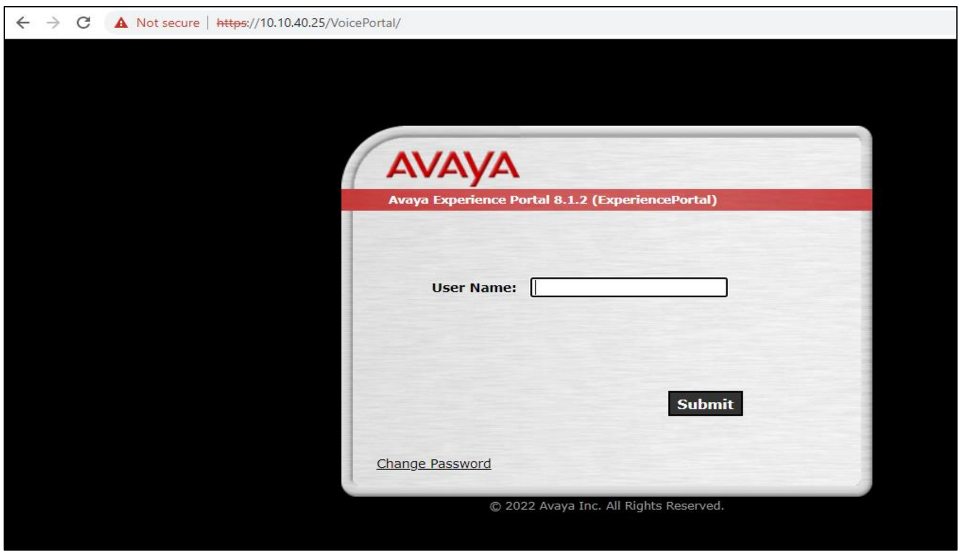
A message confirming the restart will appear, click on **Restart** to proceed.



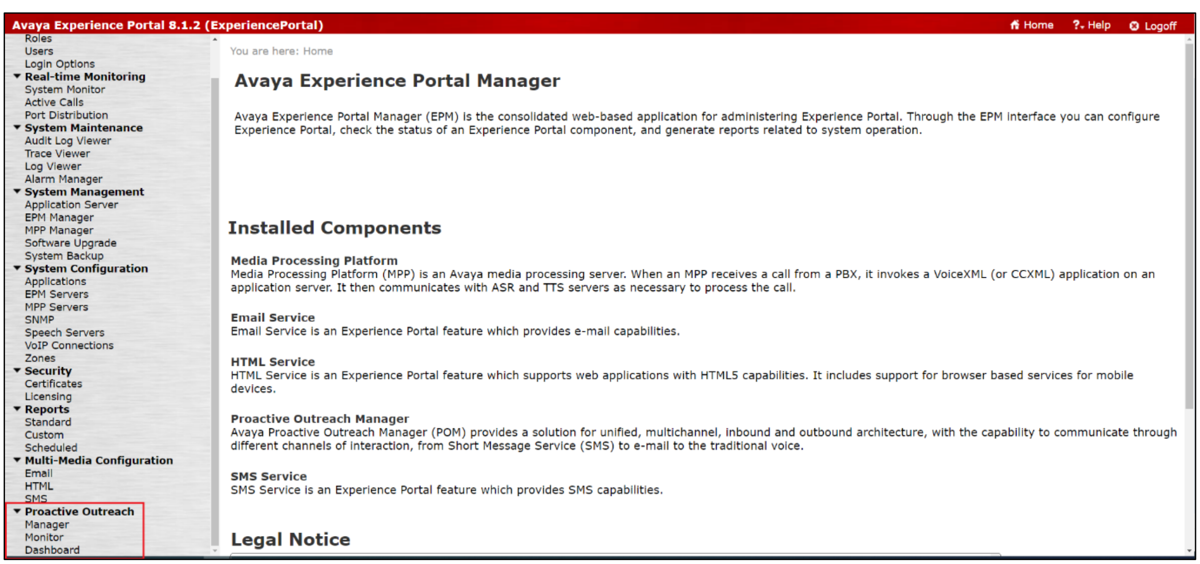
7. Configure Proactive Outreach Manager

There is no specific configuration required on POM to allow Desktop Connect to use the Agent API on POM. The only requirement would be to have a running POM with a running Campaign and CC Elite Agents logged into the outbound skillset associated with that campaign. The following section illustrates how to observe the installed campaigns and how to start them running.

POM is configured via the Experience Portal Manager (EPM) web interface. To access the web interface, enter **https://[IP-Address]/VoicePortal** as the URL in an internet browser, where IP-Address is the IP address of the EPM. Log in using the Administrator user role. The screen shown below is displayed.



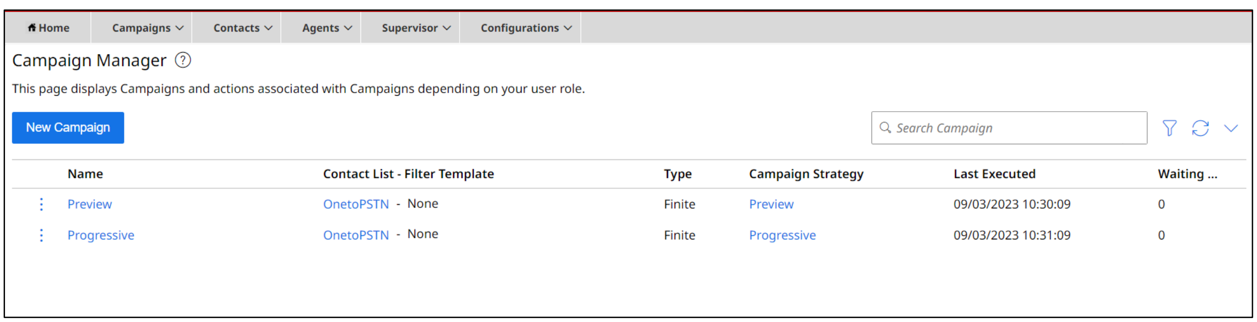
From the left window, navigate to **Proactive Outreach** and select **Manager**.



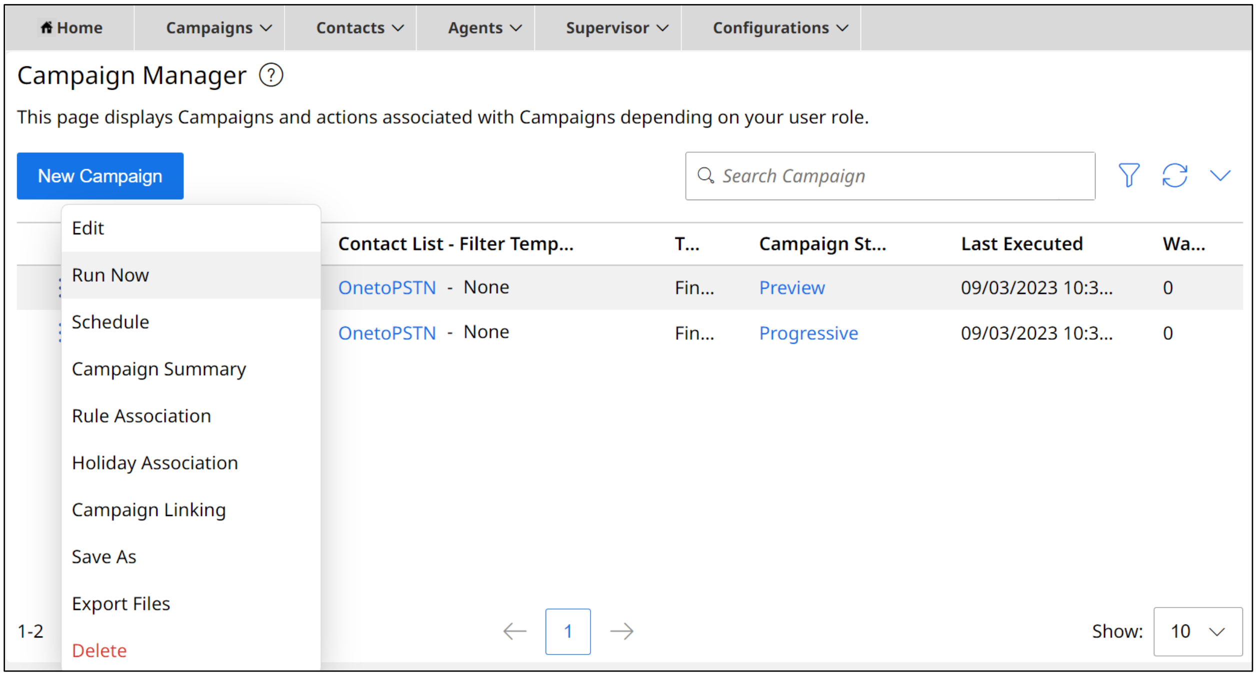
Navigate to **Campaigns → Campaign Manager** from the main window, as shown.

The following two campaigns were setup for compliance testing.

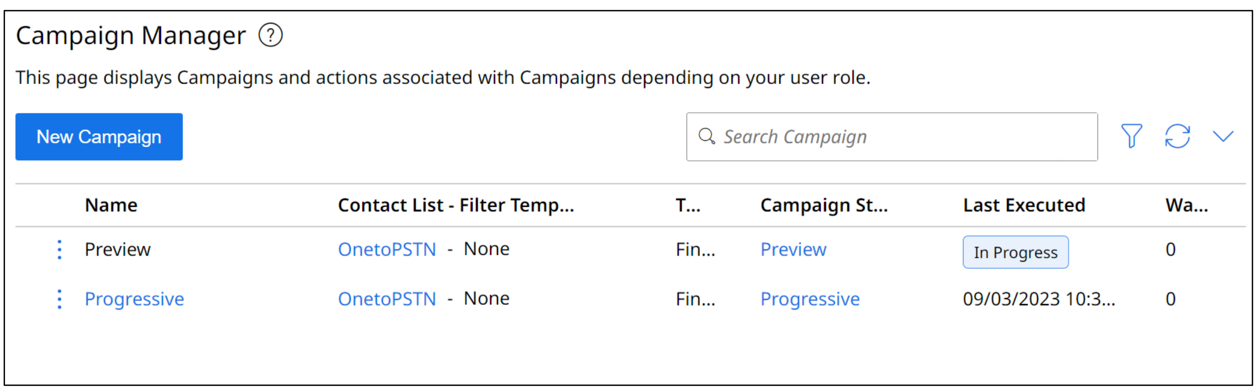
- **Preview** – this campaign allows the agent to make the outbound call by presenting the call information to the agent desktop and allowing the agent click on "preview dial".
- **Progressive** – this campaign makes the call first and then presents the call information to the agent desktop, this effectively forces the call to the agent.



Select the appropriate campaign to run, right click on the three dots to the left of the campaign in question and select **Run Now**.



The campaign should now be displayed as **In Progress**.



8. Configure Geomant Desktop Connect

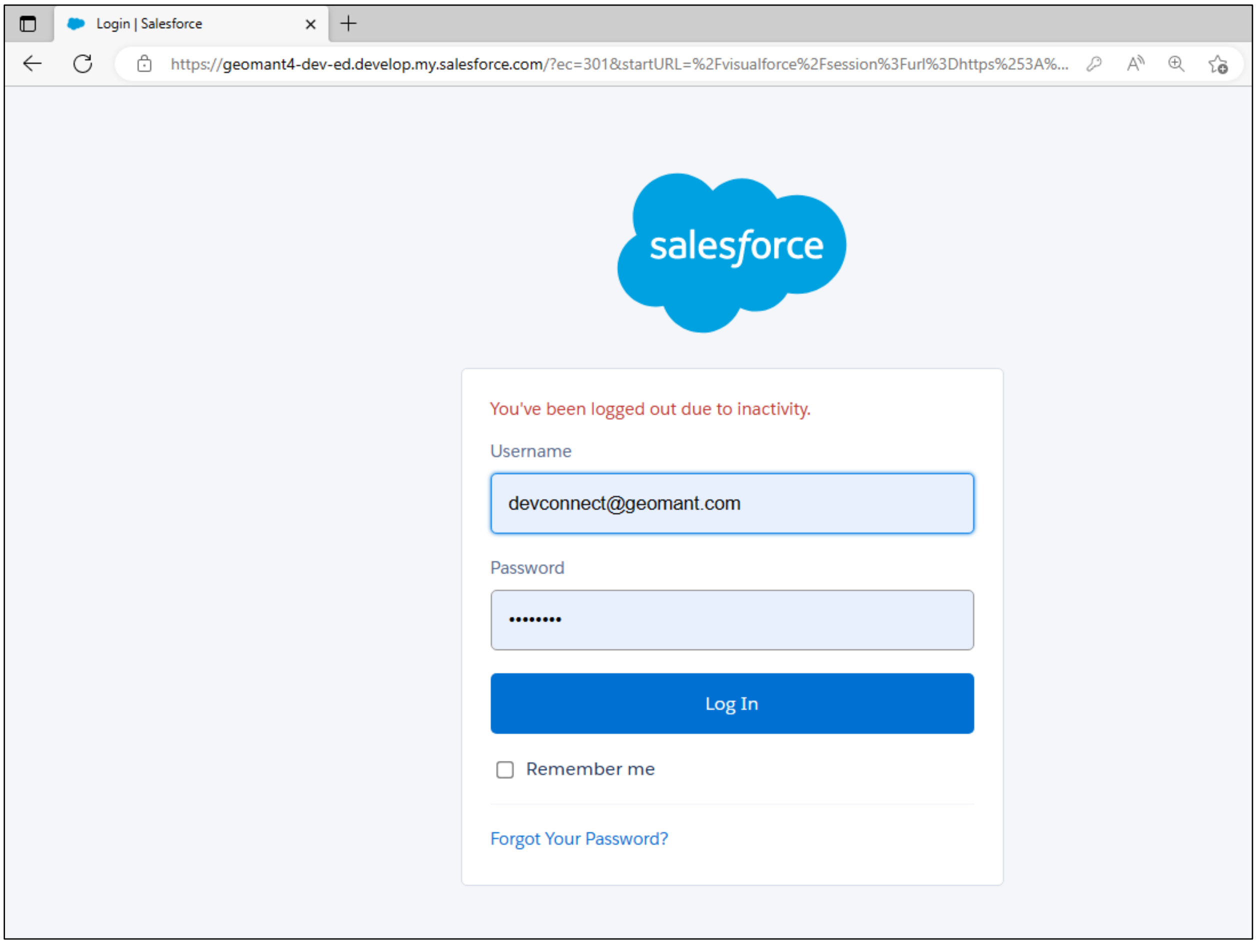
The installation and configuration of Geomant Desktop Connect may vary depending on what CRM is being used. Geomant maintain documentation describing the server configuration at https://docs.geomant.com/, this is what engineers and partners should use to implement the solution.

9. Verification Steps

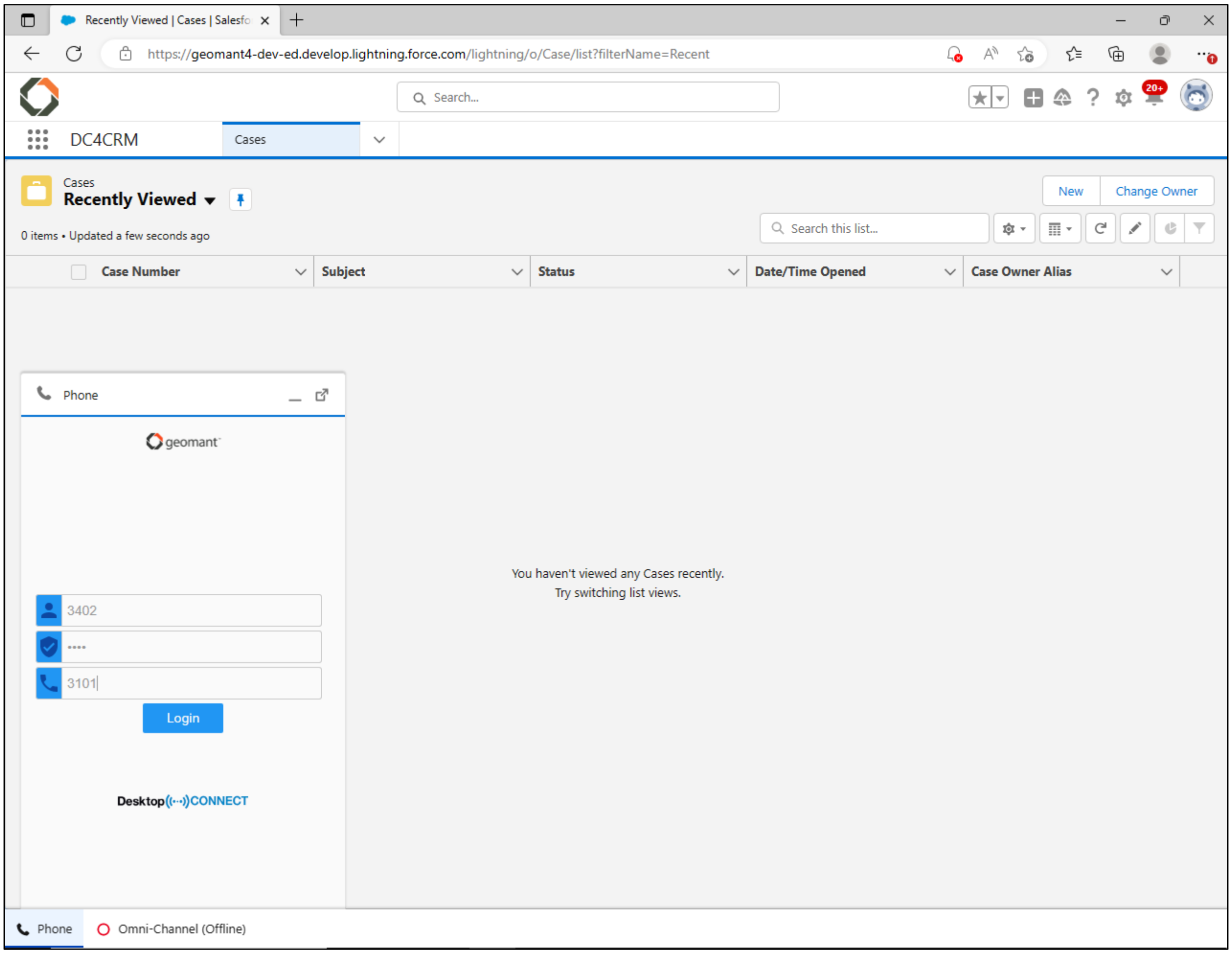
This section provides the tests that can be performed to verify proper configuration of Communication Manager, Proactive Outreach Manager, Application Enablement Services, and Desktop Connect.

9.1. Verify Geomant Desktop Connect

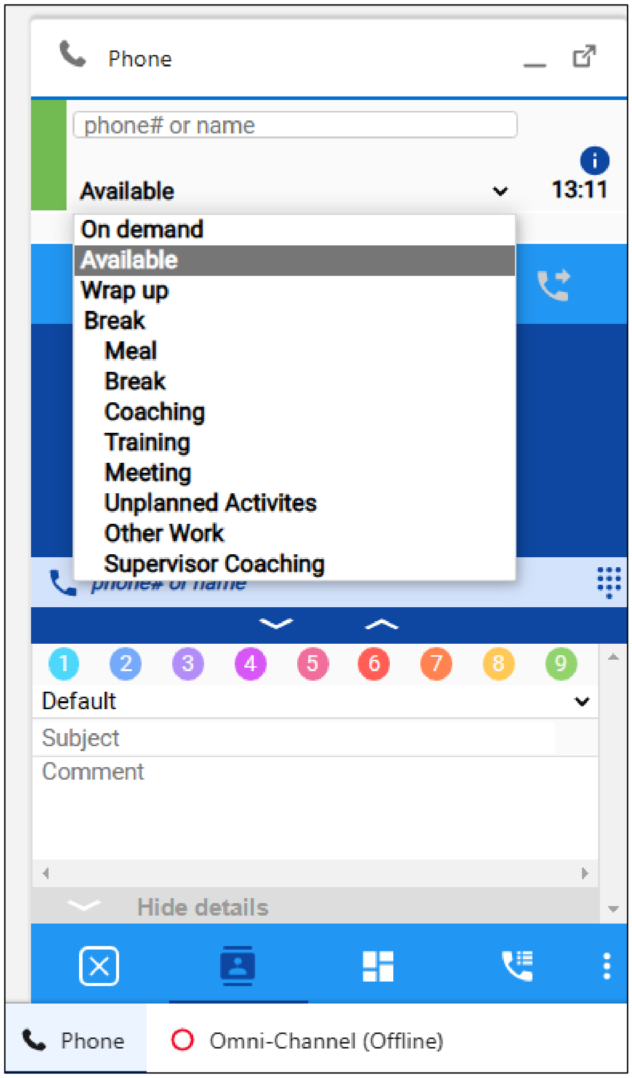
Log into the agent desktop client by opening a browser session to the CRM in question. As Salesforce was the CRM used for compliance testing this is what is shown below.



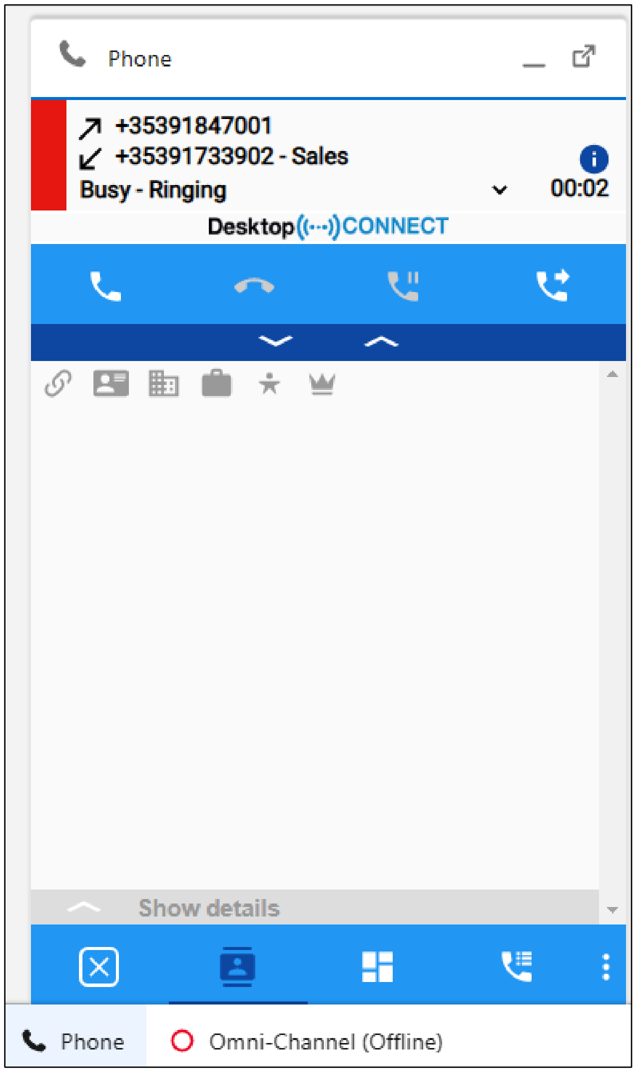
Once logged into Salesforce, click on the **phone** icon at the bottom left of the screen to open the login for telephony. Below agent **3402** was logged into extension **3101**.



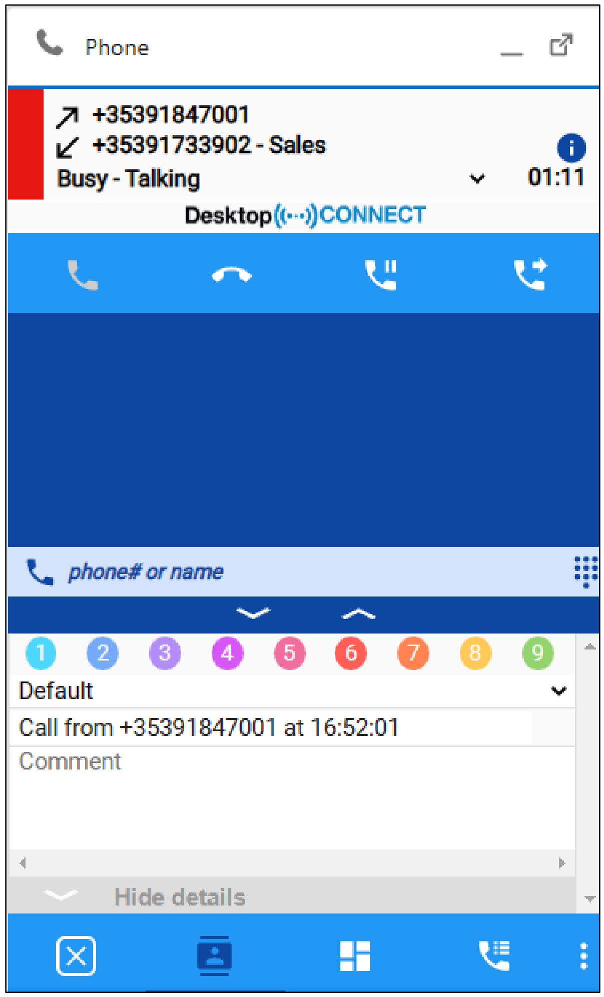
Once logged in the agent can change the status, as shown below.



A call is made to the Sales VDN and appears to be ringing at the agent's desktop.



Once the call is answered, it will show as **Busy – Talking** and the transfer, hold and hang up icons will be available to the agent. The caller's number is shown as well as the skillset name and number.



9.2. Verify connection from Avaya platform

There are a number of checks that can be performed to ensure that a connection is present from the Avaya products. These are some of the key checks that can be performed.

- Verify CTI Service State on Communication Manager.
- Verify TSAPI link and user on Application Enablement Services.
- Verify Avaya Experience Portal is running.
- Verify Avaya Proactive Outreach Manager is running.

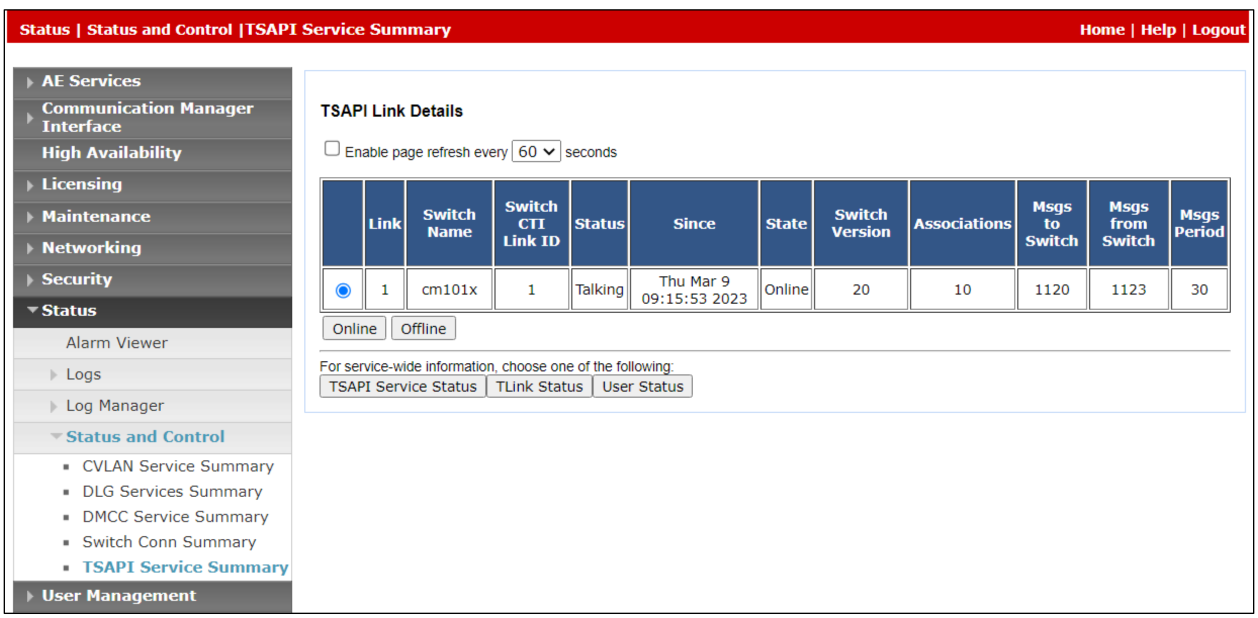
9.2.1. Verify CTI Service State on Communication Manager

Check the connection between Communication Manager and AES. Check the AESVCS link status by using the command **status aesvcs cti-link**. Verify the **Service State** of the CTI link is **established**.

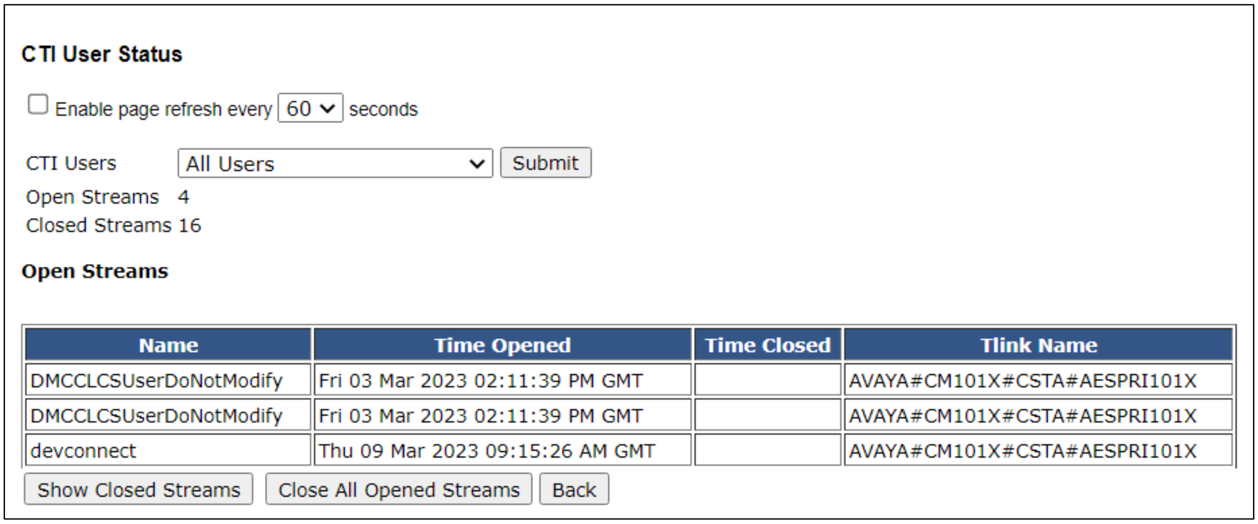
```
status aesvcs cti-link

                              AE SERVICES CTI LINK STATUS

CTI    Version      Mnt   AE Services           Service        Msgs
Link                Busy     Server             State          Sent       Rcvd

1          12       no      aespri101x          established    865        865
```

9.2.2. Verify TSAPI Link

On the AES Management Console, verify the status of the TSAPI link by selecting **Status → Status and Control → TSAPI Service Summary** to display the **TSAPI Link Details** screen. Verify the TSAPI link by checking that the **Status** is **Talking** and the **State** is **Online**.

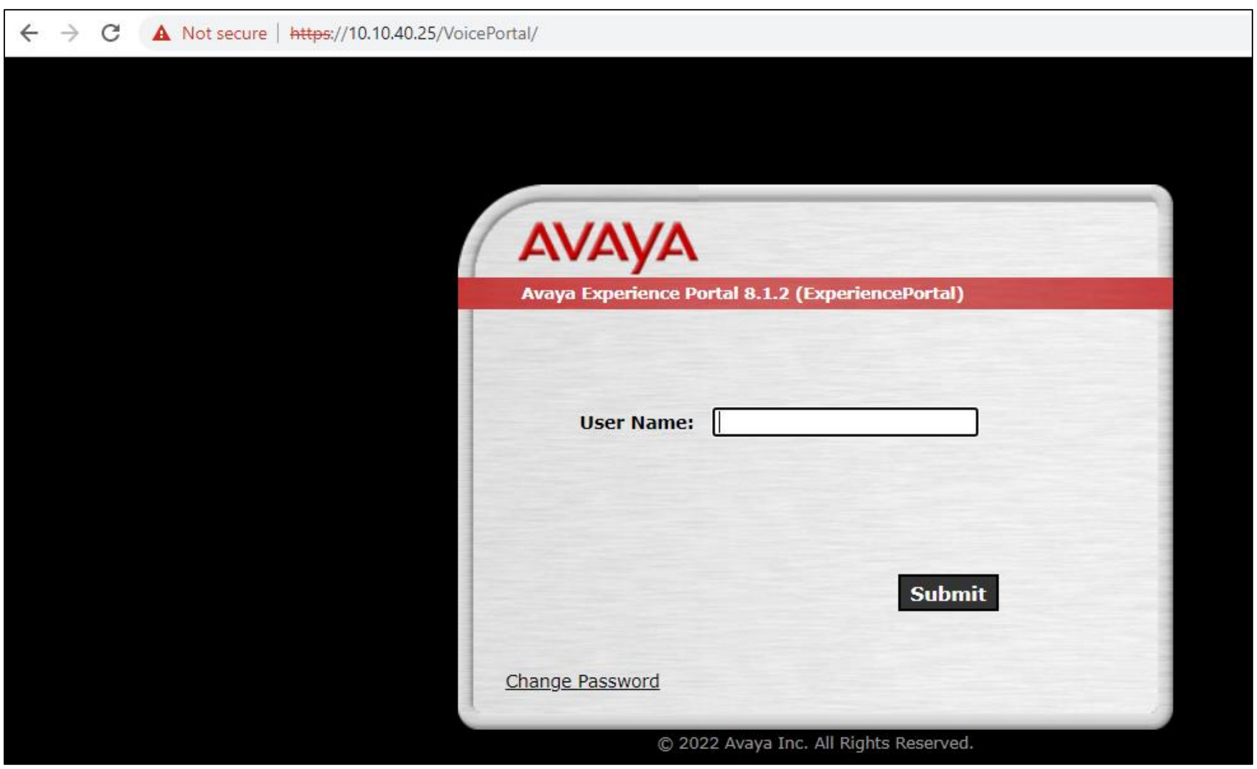


Clicking on **User Status** from the screen on the previous page should display something similar to that shown below, where the **devconnect** user and corresponding **Tlink Name** are shown.

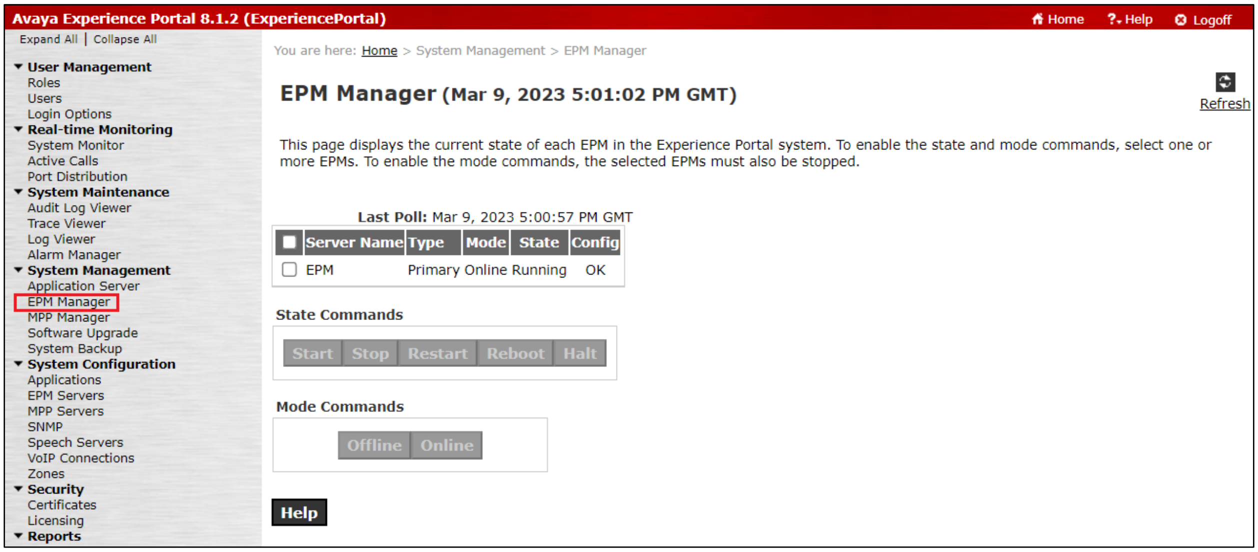


9.2.3. Verify Avaya Experience Portal is running

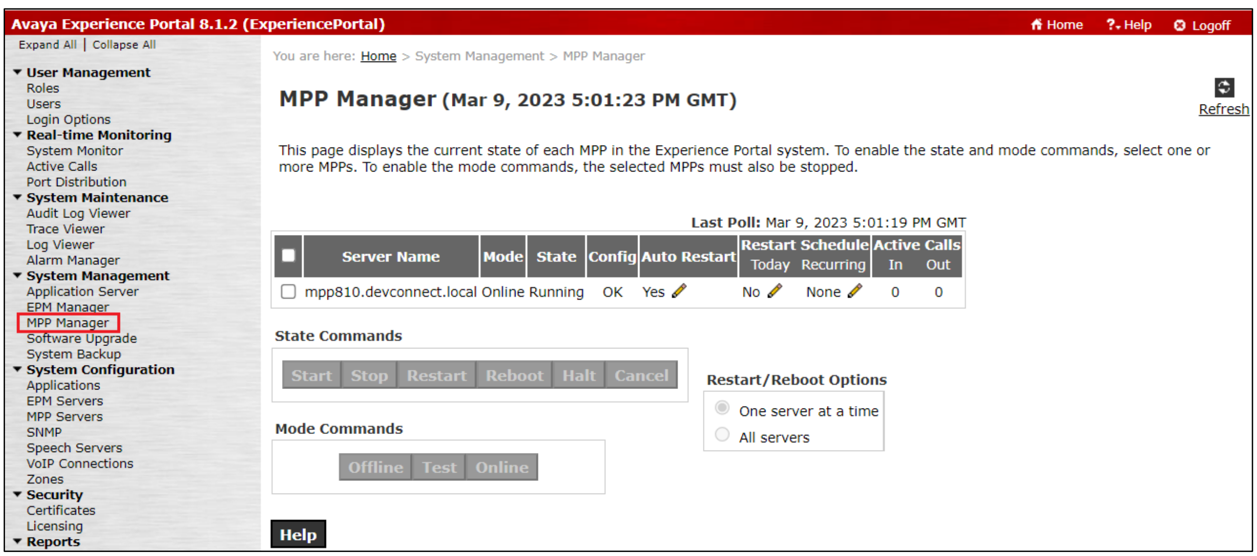
Before checking on Proactive Outreach Manager, check that Experience Portal and Media Processing are running. Log into Experience Portal by opening a browser session to the Experience Portal servers IP address as shown.



Once logged in, navigate to **System Management → EPM Manager** in the left window, and check that the server **Mode** is **Online** and **State** is **Running**, as shown below.

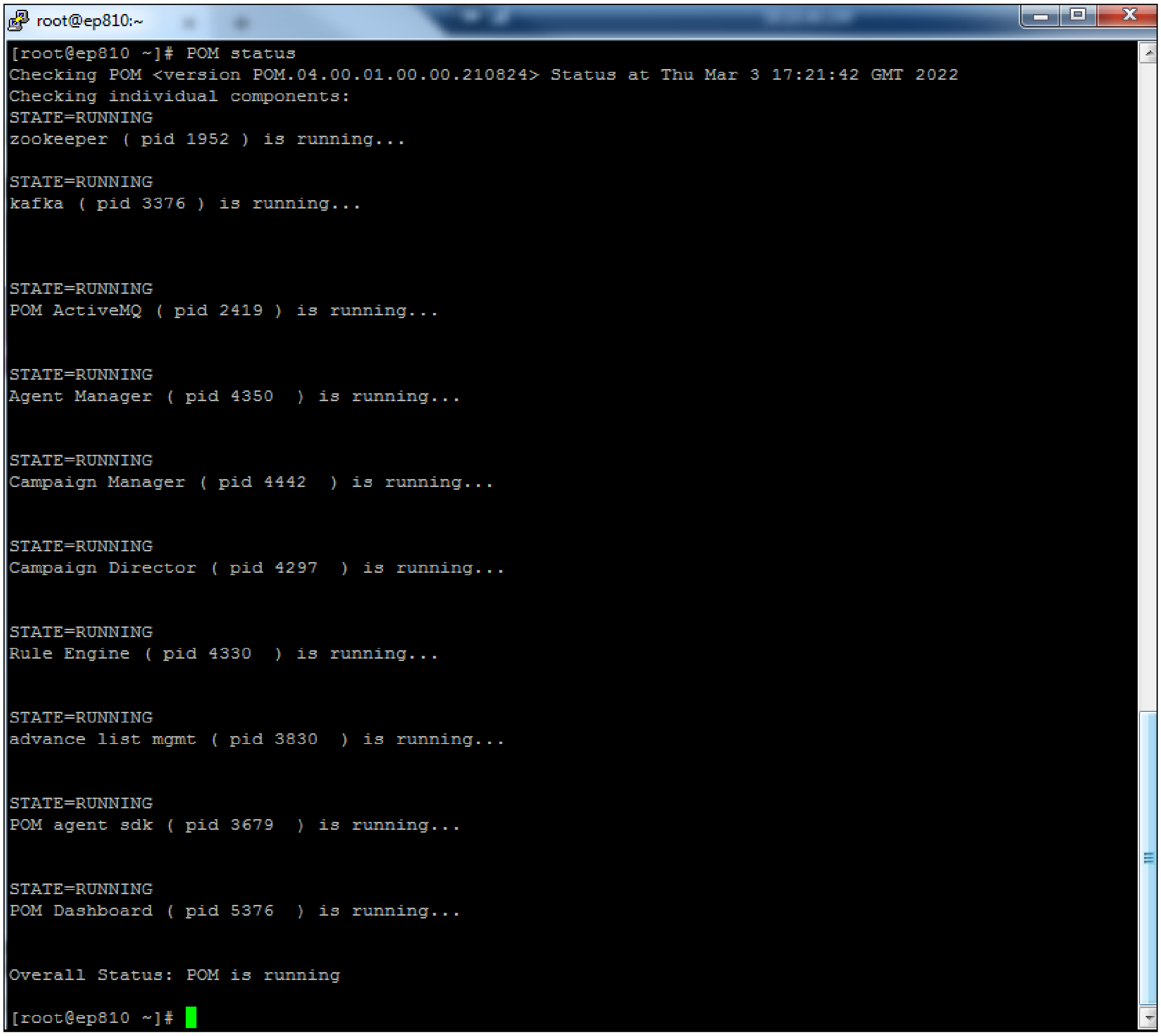


Navigate to **MPP Manager** in the left window and again ensure that **Mode** is **Online**, and **State** is **Running**.



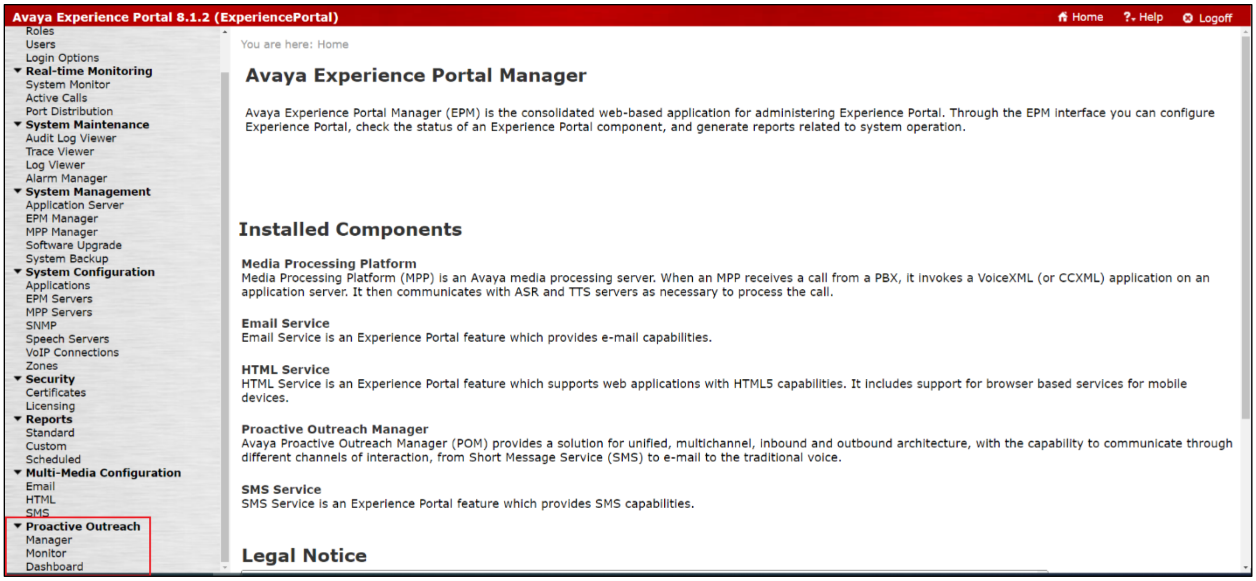
9.2.4. Verify Avaya Proactive Outreach Manager is running

The status of the POM server can be checked from an SSH session to the POM server using something like PuTTY. Open a connection to Experience Portal/POM server and then ensure that the user “root” is used by typing **su – root** (not shown). Type **POM status** and verify that all POM services are **RUNNING**, as shown below.

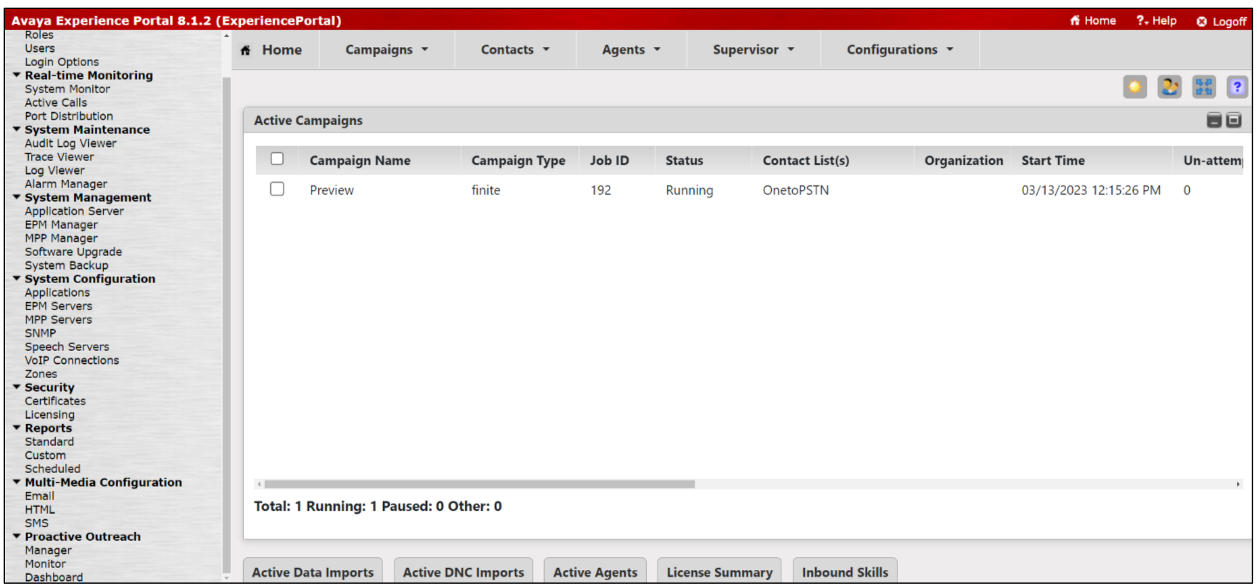


9.2.5. Verify Avaya Proactive Outreach Manager Outbound Campaign is running

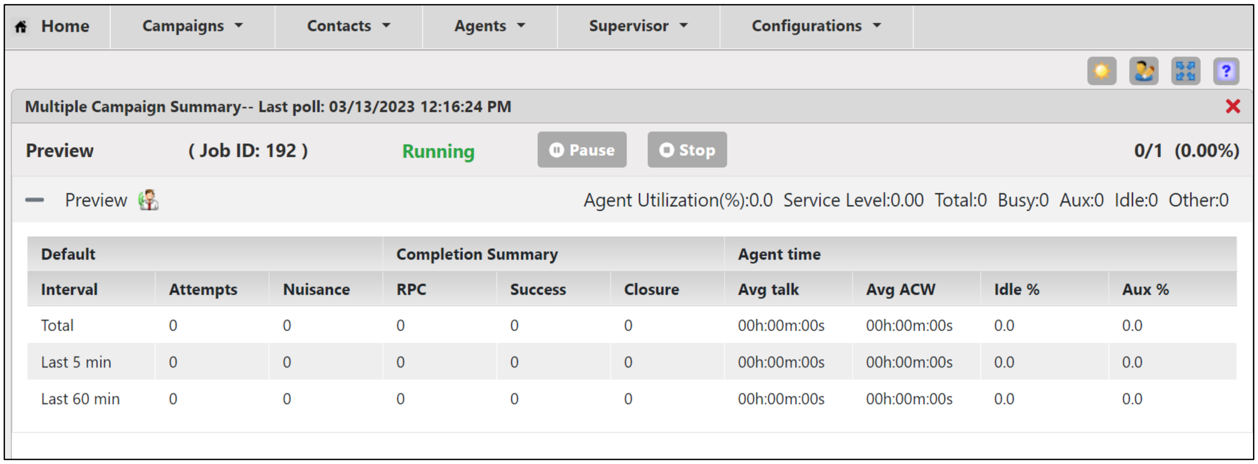
Navigate to **Proactive Outreach → Monitor** in the left window.



If a campaign is running, it will show up here. Clicking on the campaign will show further information on that campaign.



Clicking on the campaign from the previous page results in displaying information on that campaign, as shown below.



Default			Completion Summary			Agent time			
Interval	Attempts	Nuisance	RPC	Success	Closure	Avg talk	Avg ACW	Idle %	Aux %
Total	0	0	0	0	0	00h:00m:00s	00h:00m:00s	0.0	0.0
Last 5 min	0	0	0	0	0	00h:00m:00s	00h:00m:00s	0.0	0.0
Last 60 min	0	0	0	0	0	00h:00m:00s	00h:00m:00s	0.0	0.0

10. Conclusion

These Application Notes describe the configuration steps required for Geomant Desktop Connect 4.2 to successfully interoperate with Avaya Aura® Application Enablement Services 10.1 and Avaya Proactive Outreach Manager 4.0.2. All feature and serviceability test cases were completed with observations noted in **Section 0**.

11. Additional References

This section references the product documentation relevant to these Application Notes.

[1] *Avaya Proactive Outreach Manager Integration. Release 4.0, Issue 1, September 2021.*

[2] *Implementing Avaya Proactive Outreach Manager. Release 4.0.1, Issue 1, September 2021.*

[3] *Administering Avaya Aura® Communication Manager, Release 10.1, Issue 1, December 2021.*

[4] *Administering Avaya Aura® Application Enablement Services, Release 10.1.x, Issue 4, April 2022.*

[5] *Avaya Aura® Communication Manager Feature Description and Implementation, Release 10.1, Issue 8 March 2023.*

[6] *Administering Avaya Aura® Session Manager, Release 10.1, Issue 5 February 2023.*

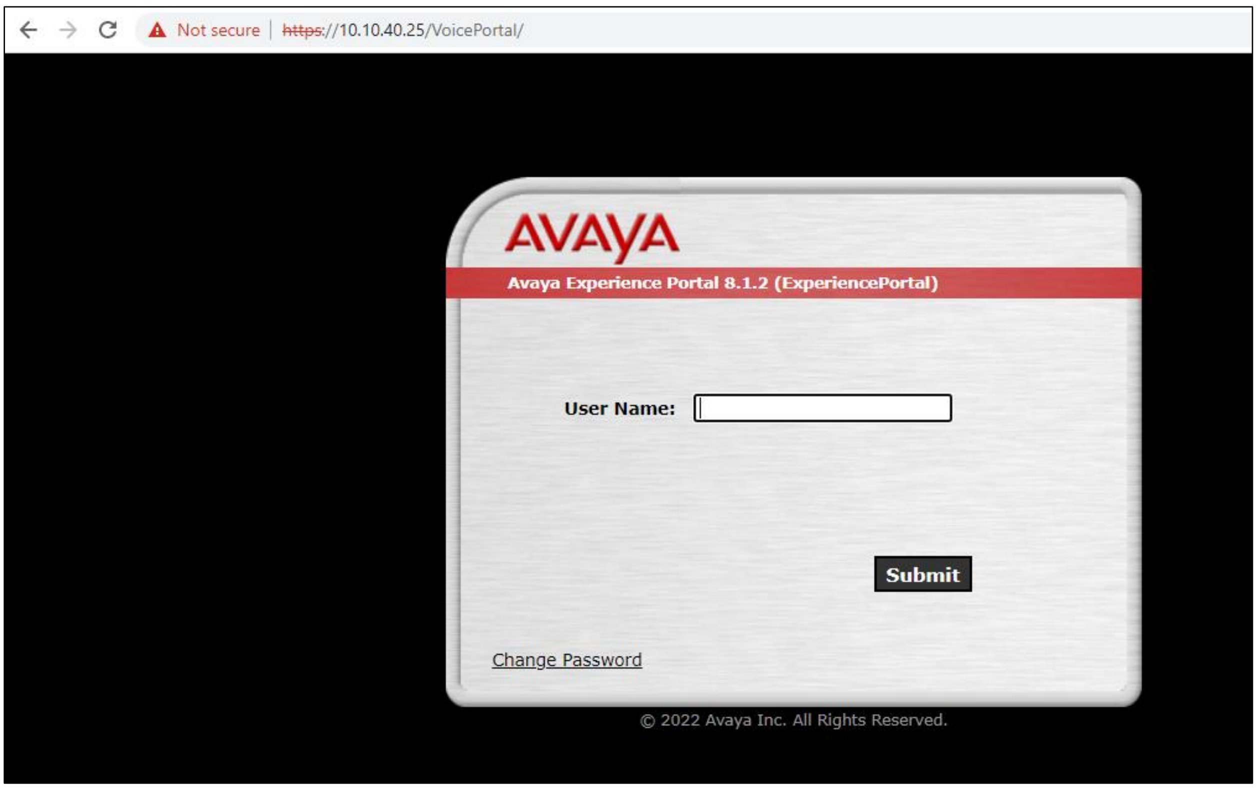
[7] *Desktop Connect Deployment and Configuration Guide*, Version 4.2, available as part of Desktop Connect Knowledge Base at https://docs.geomant.com/dc/index.html.

12. Appendix

There are many configurations that are required for various campaigns to operate, the screen shots displayed here are to serve to display the setup used for compliance testing. This configuration shows the preview campaign that was used, the contact list and strategy associated with that outbound preview campaign.

It is assumed that both POM and Experience Portal are already installed with the connections made to both Session Manager and AES. The setup and configuration of these connections are therefore outside the scope of these Application Notes. **The procedural steps that are presented in this Appendix for informational purposes only**.

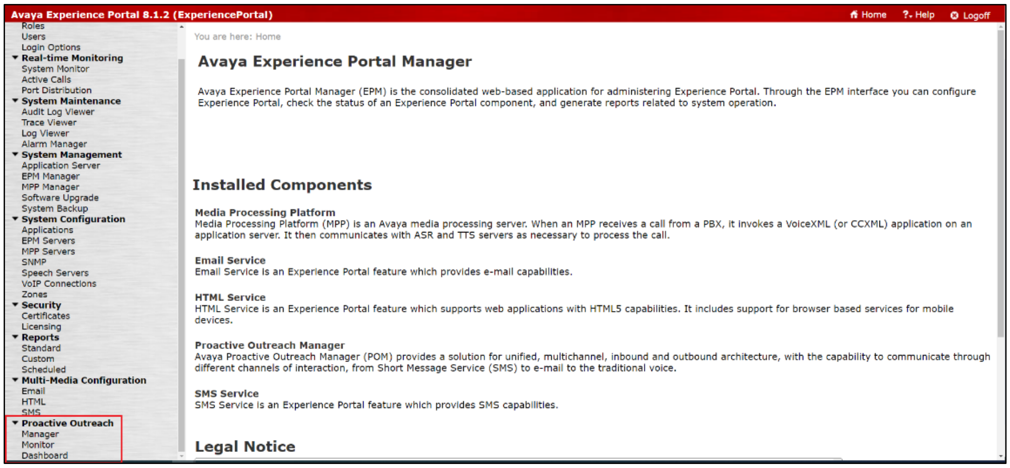
Experience Portal is configured via the Experience Portal Manager (EPM) web interface. To access the web interface, enter **https://[IP-Address]/VoicePortal** as the URL in an internet browser, where IP-Address is the IP address of the EPM. Log in using the Administrator user role. The screen shown below is displayed.



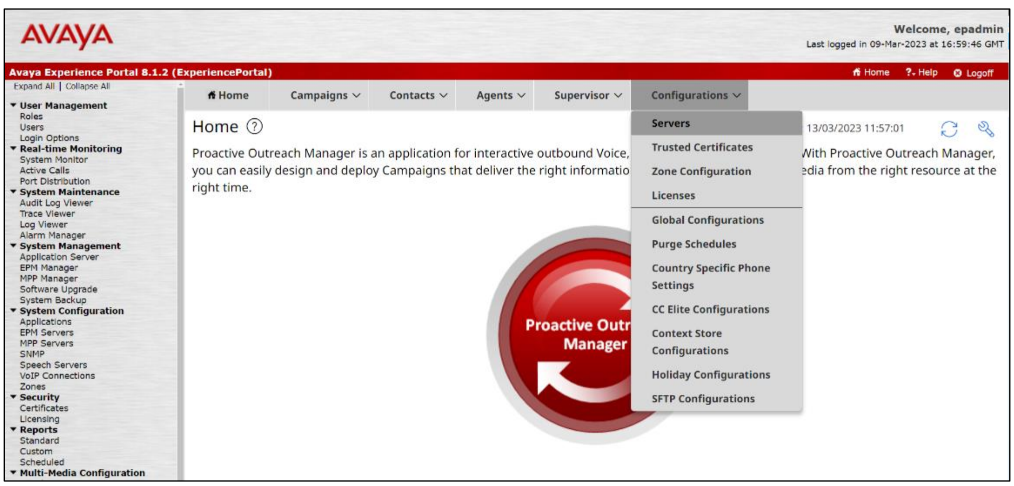
Note: The following sections aim to display the configuration on POM that was used during compliance testing and to help the reader understand the setup of POM that was used. They do not serve as a setup and configuration guide for POM or Experience Portal.

12.2. Display configuration of POM Server

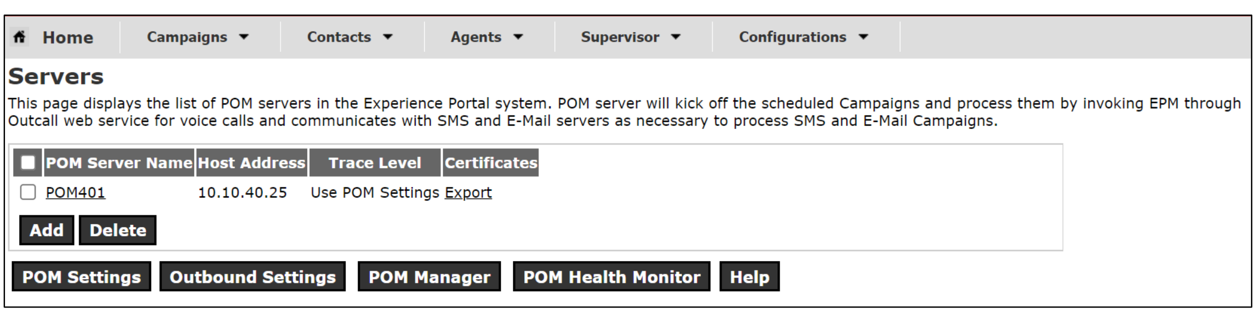
Information on the POM server can be found by navigating to **Proactive Outreach → Manager** in the left window, as shown.



From the main window, select **Configurations → Servers**.

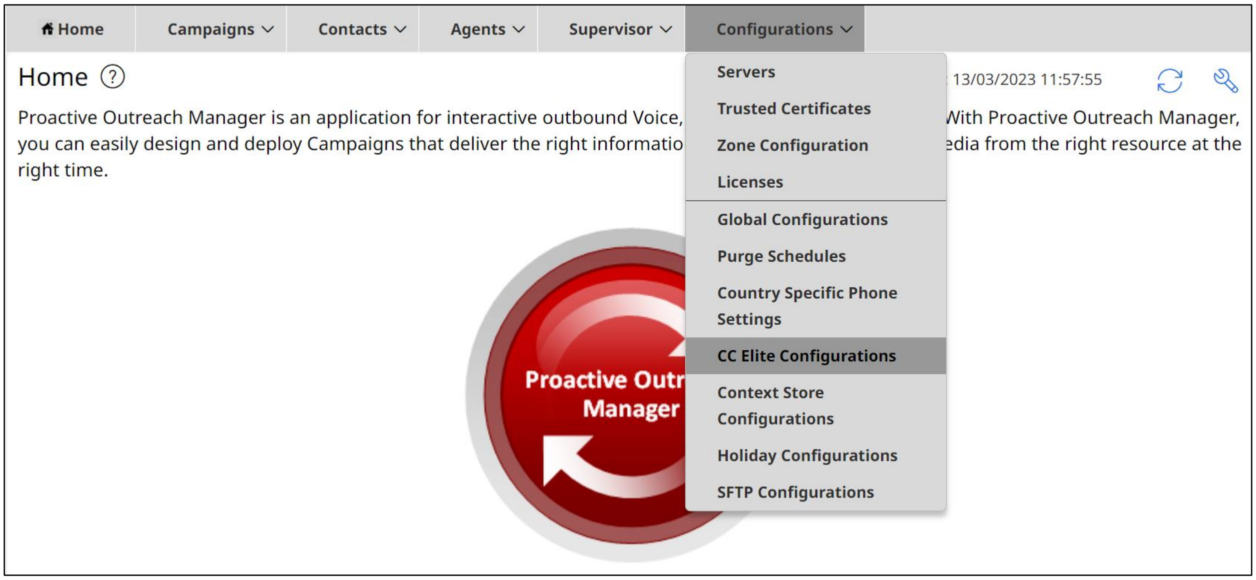


Information on the POM server can be found be either selecting the **POM Server Name** or the various buttons underneath that.

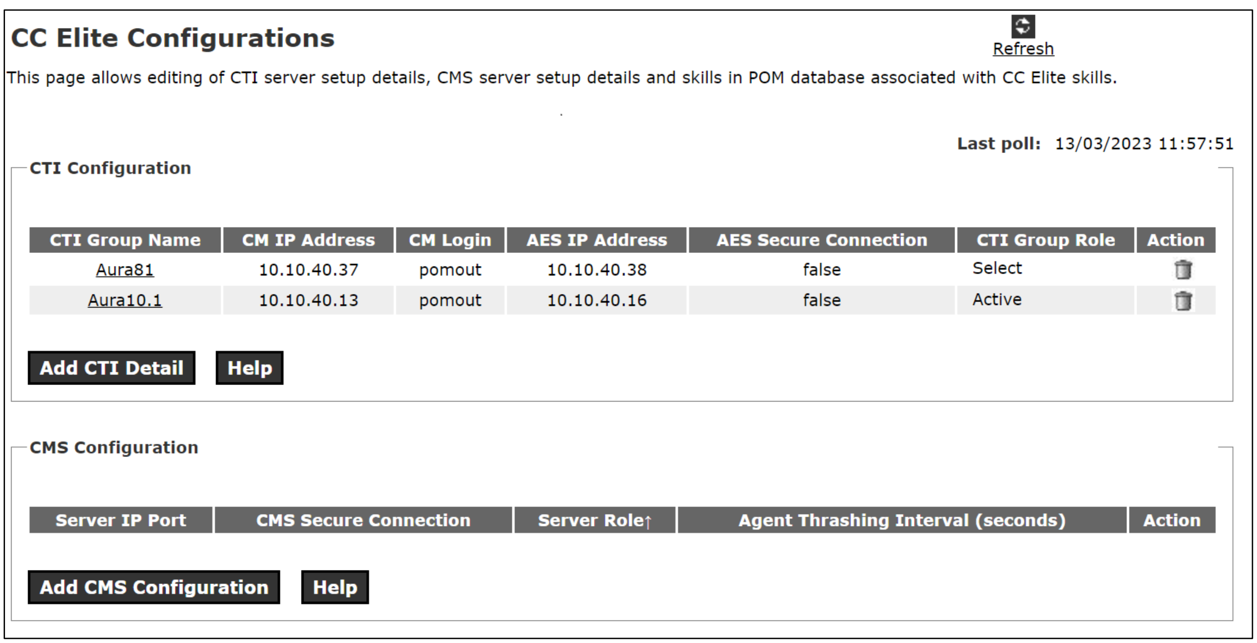


12.3. Display configuration of the CTI connection

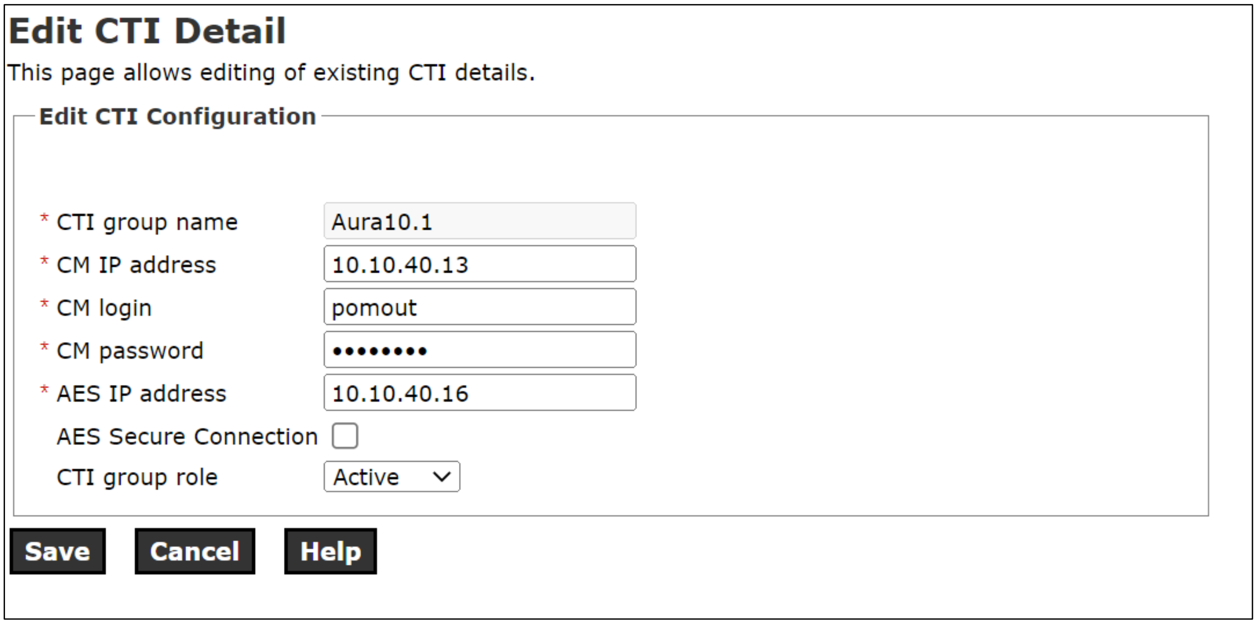
Select **Configuration → CC Elite Configurations** from the main window.



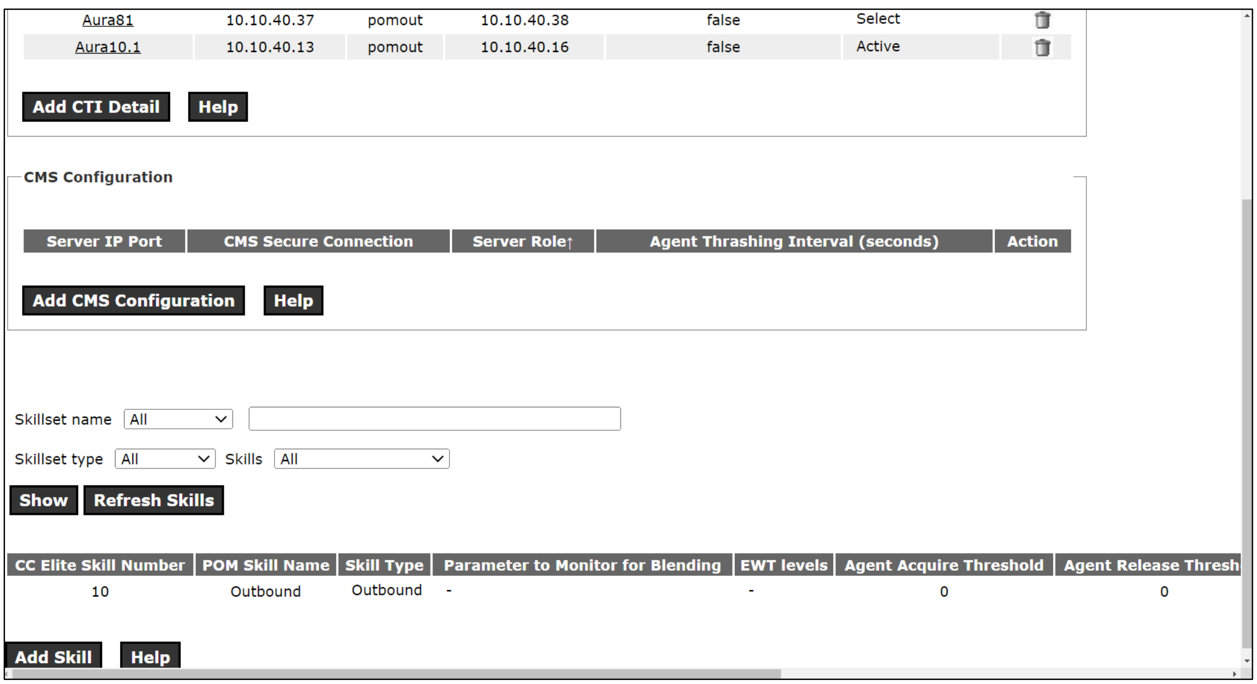
Both the **Aura81** and **Aura 10.1** CTI groups were already in place for compliance testing, clicking on the **Aura 10.1** group will open the connection to show the details.



Information such as the IP Address of Communication Manager and the AES are stored here as well as the Communication Manager user created in **Section 5.2.3**.



From the **Configure CTI setup details, CMS setup and POM Skills** page, the outbound skill must be added. Again, this was already in place but can be added by clicking on **Add Skill**. The skill below matches the outbound hunt group setup in **Section 5.3.1**.



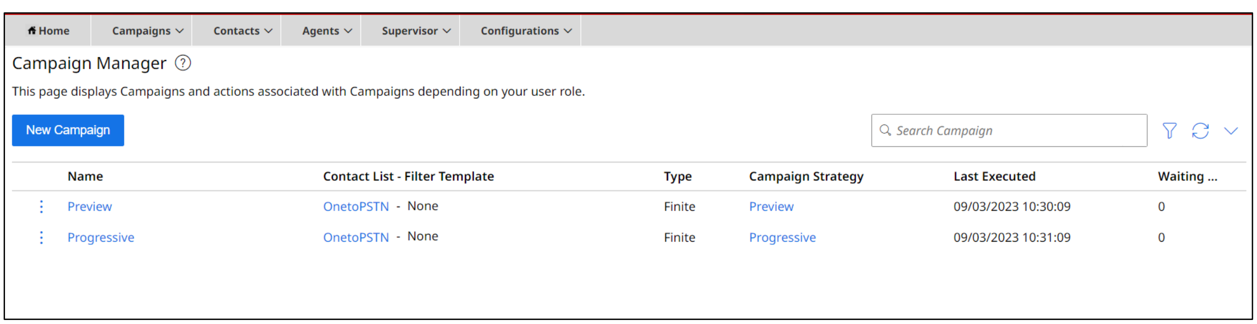
12.4. Display POM Campaigns

It is assumed that the POM campaigns are already setup and running prior to the connection from Desktop Connect. The setup and configuration of the POM Campaign including the Strategies and Contact Lists are outside the scope of these Application Notes. However, an example of the Preview Strategy and Contact List are included in this **Appendix**.

Navigate to **Campaigns → Campaign Manager** from the main window, as shown.

The following two campaigns were setup for compliance testing.

- **Preview** – this campaign allows the agent to make the outbound call by presenting the call information to the agent desktop and allowing the agent click on "preview dial".
- **Progressive** – this campaign makes the call first and then presents the call information to the agent desktop, this effectively forces the call to the agent.

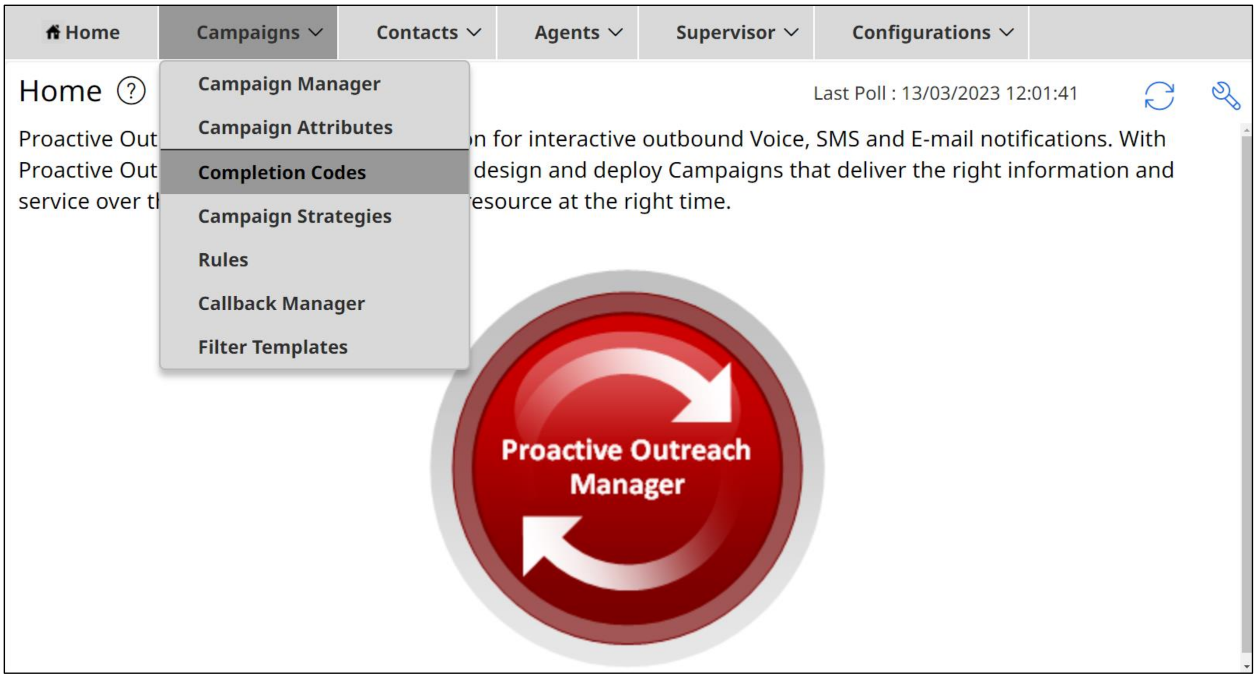


12.5. Display Campaign Components

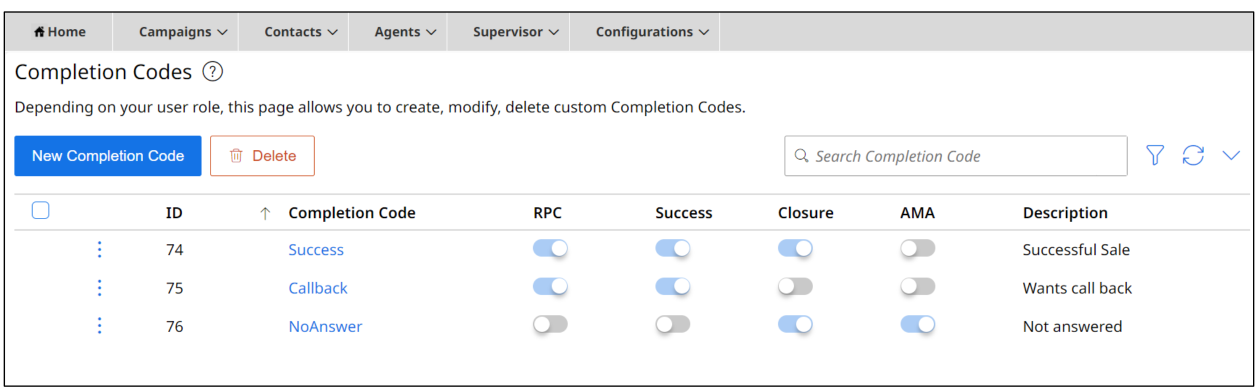
The following section shows the configuration of the various components that contribute to the overall campaign.

12.5.1. Completion Codes

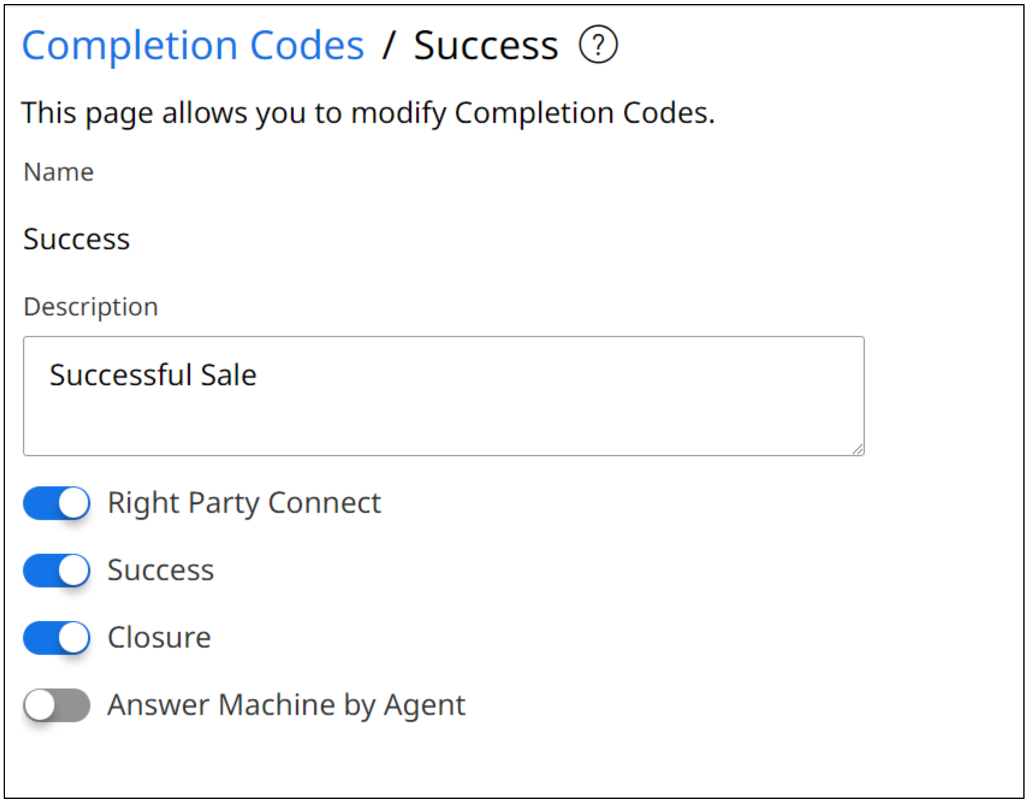
Navigate to **Campaigns → Completion Codes** as shown below.



There are three Completion Codes already present on this POM and each of these can be assigned to the Campaign Strategy. If a new code was to be added, click on **Add** shown below.



The example below shows the **Success** Completion Code which is assigned to the Preview Strategy that is to be displayed below.

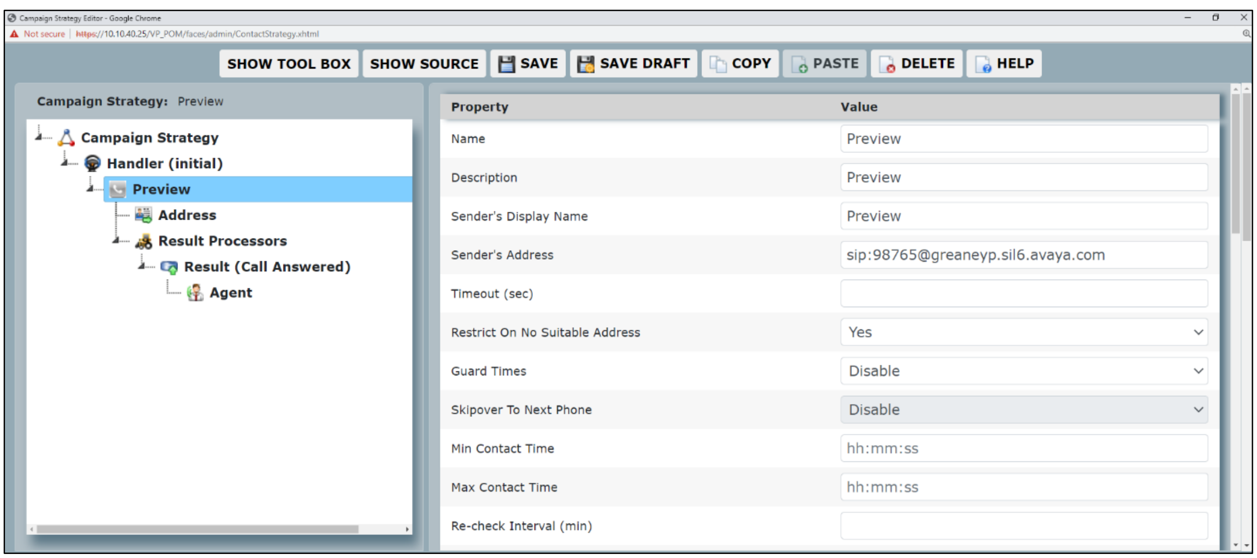


12.5.2. Campaign Strategies

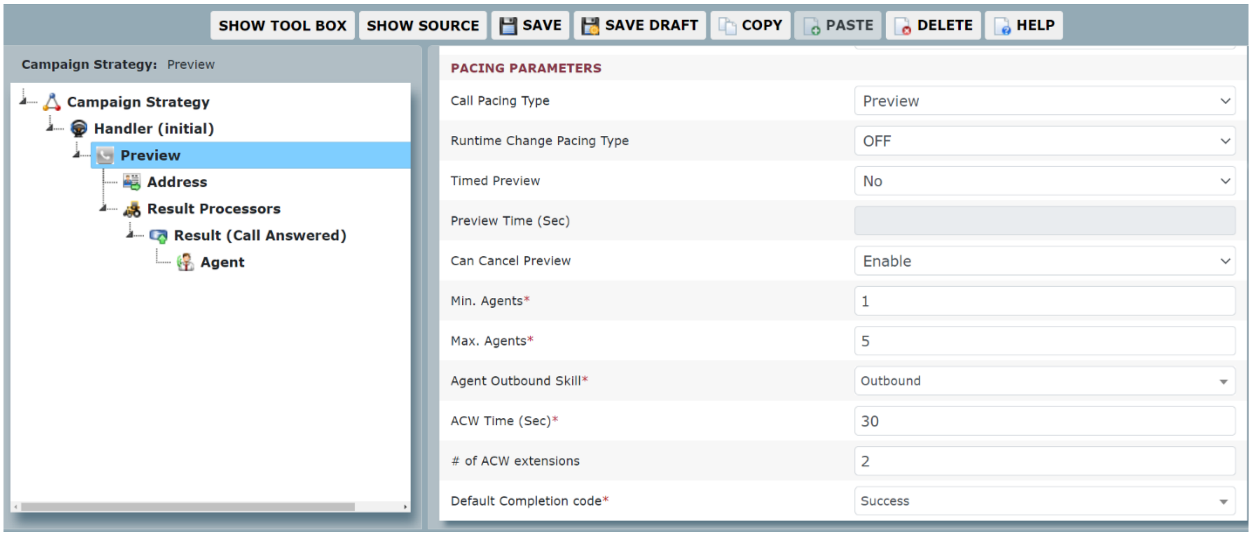
Navigate to **Campaigns → Campaign Strategies** as shown below.

The Campaign Strategies are shown where a new strategy can be added by clicking on **Add** or existing strategies can be viewed by clicking on the **Name** of the strategy displayed.

Clicking on the **Preview** strategy from the screen above will show the **Campaign Strategy** called **Preview** that was created for compliance testing.

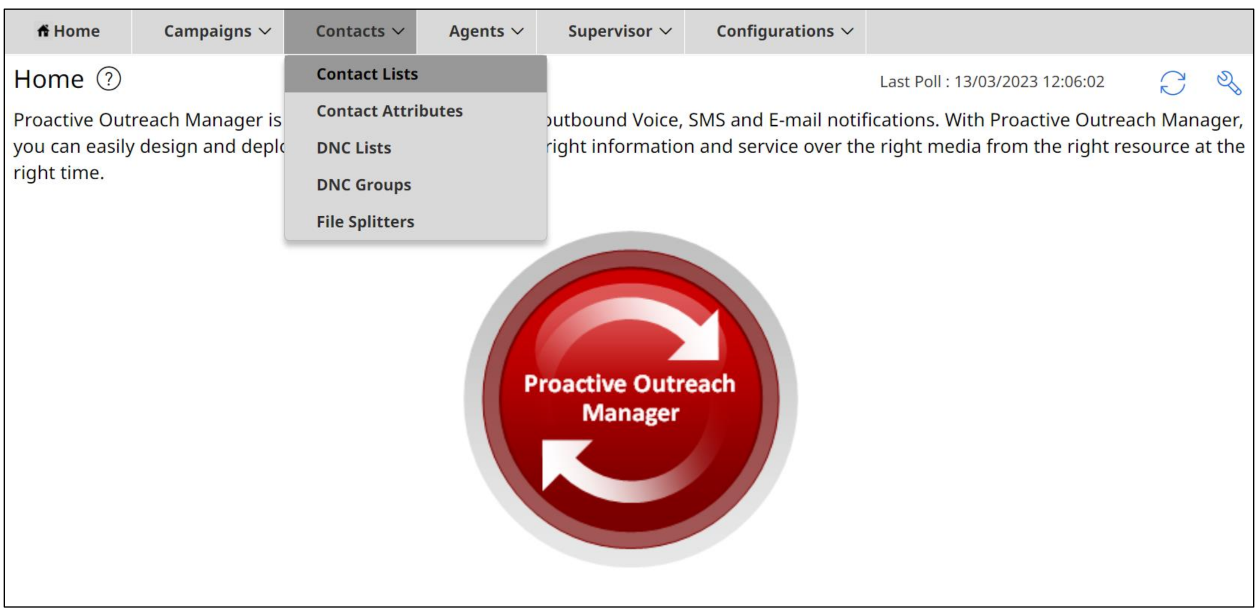


Scrolling down from the screen on the previous page shows the settings that were used for compliance testing.

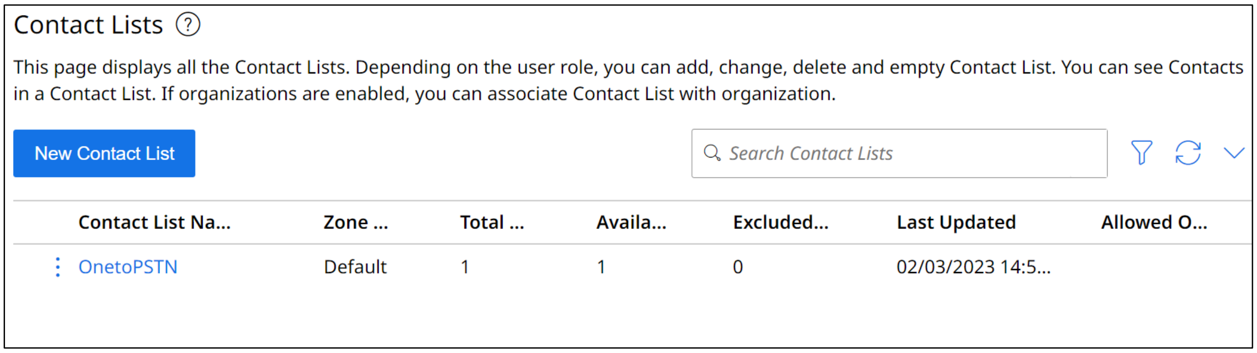


12.5.3. Contact List

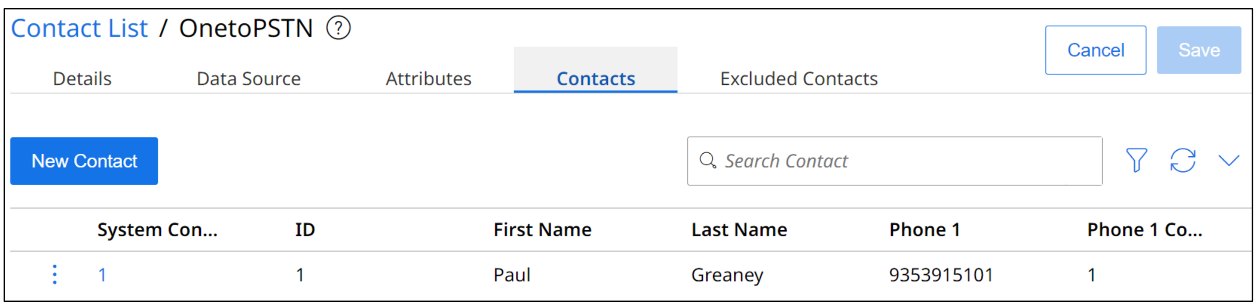
To add or view the Contact Lists, navigate to **Contacts → Contact Lists** as shown below.



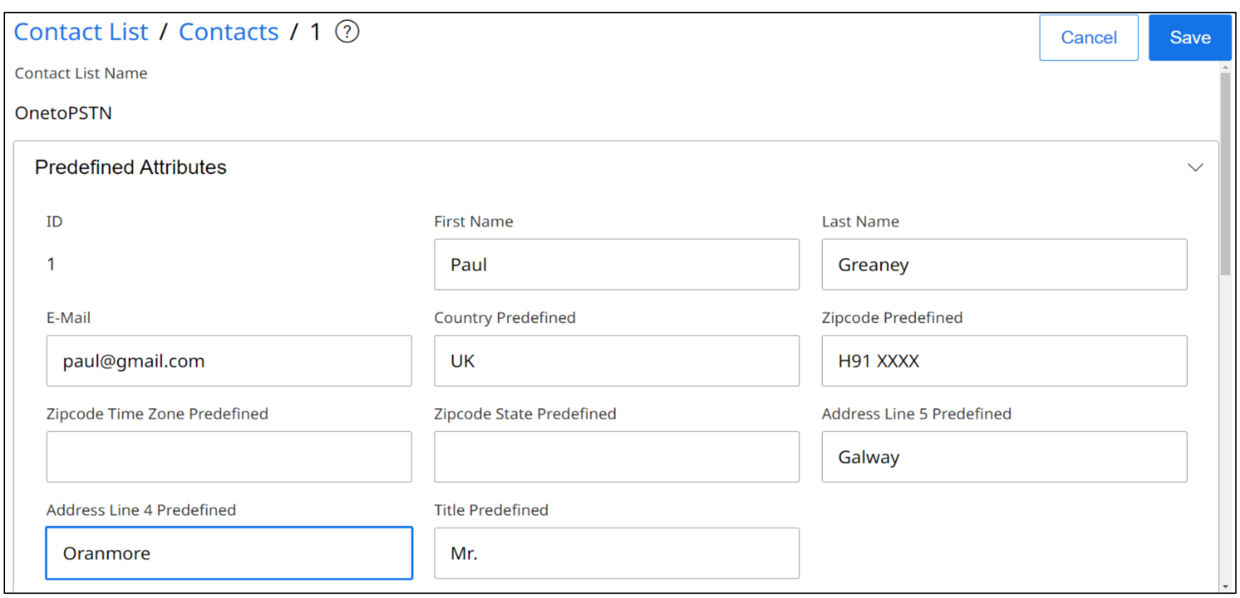
There is a Contact List already configured for the Preview Campaign called **OnetoPSTN**. Details of this Contact List can be viewed by clicking on the **Contact List Name** icon. A new Contact List can be added by clicking on **Add** and uploading the contacts from a file.



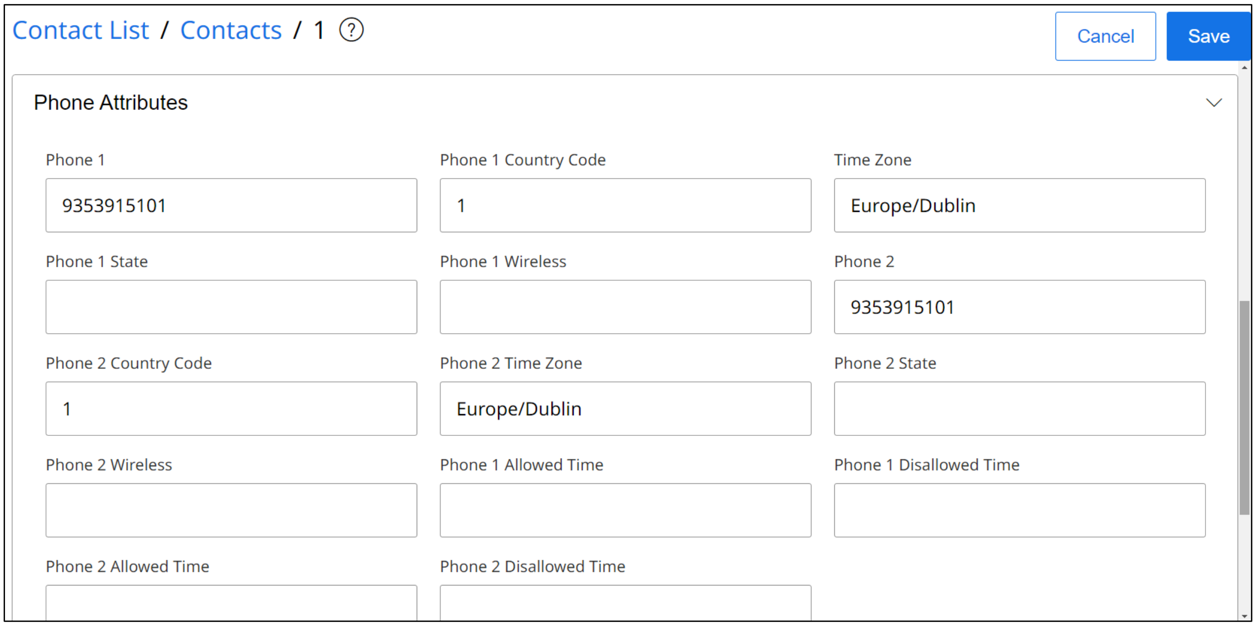
The Contact List shown has just one entry, with some of the details displayed. Clicking on that entry will show further details.



Contact information, such as name and address are shown, and scrolling down will reveal more.



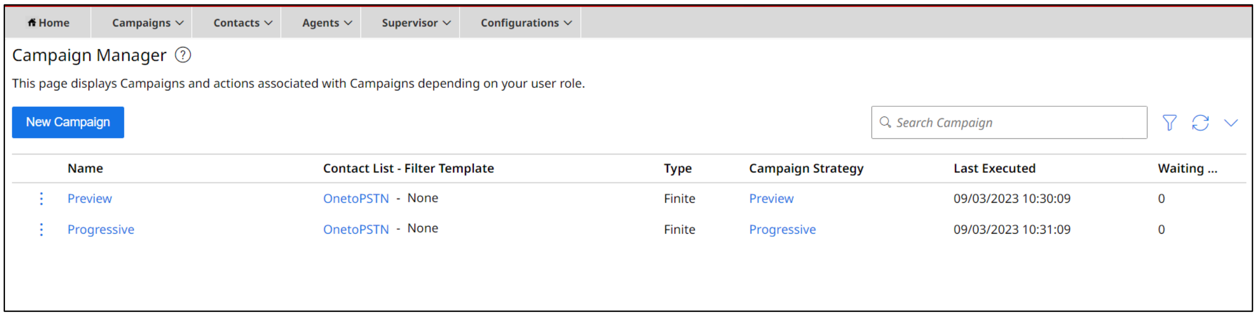
The **Phone 1** and **Phone 2** information is most important for the outbound calls to take place successfully.



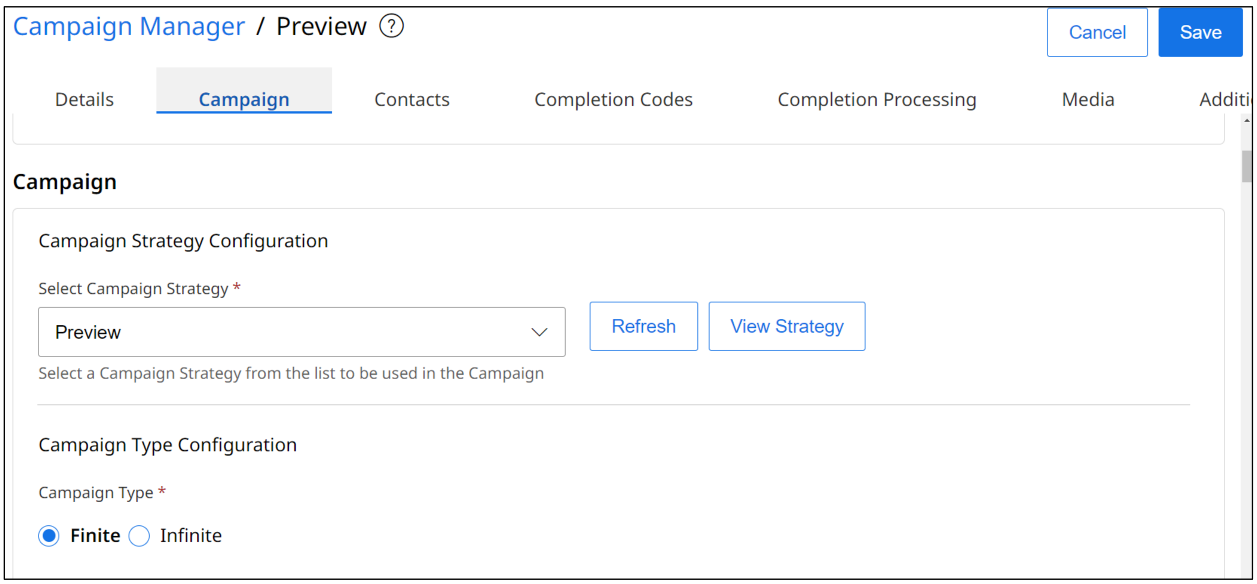
12.6. Display Preview Campaign

Navigate to **Campaigns → Campaign Manager** as shown below.

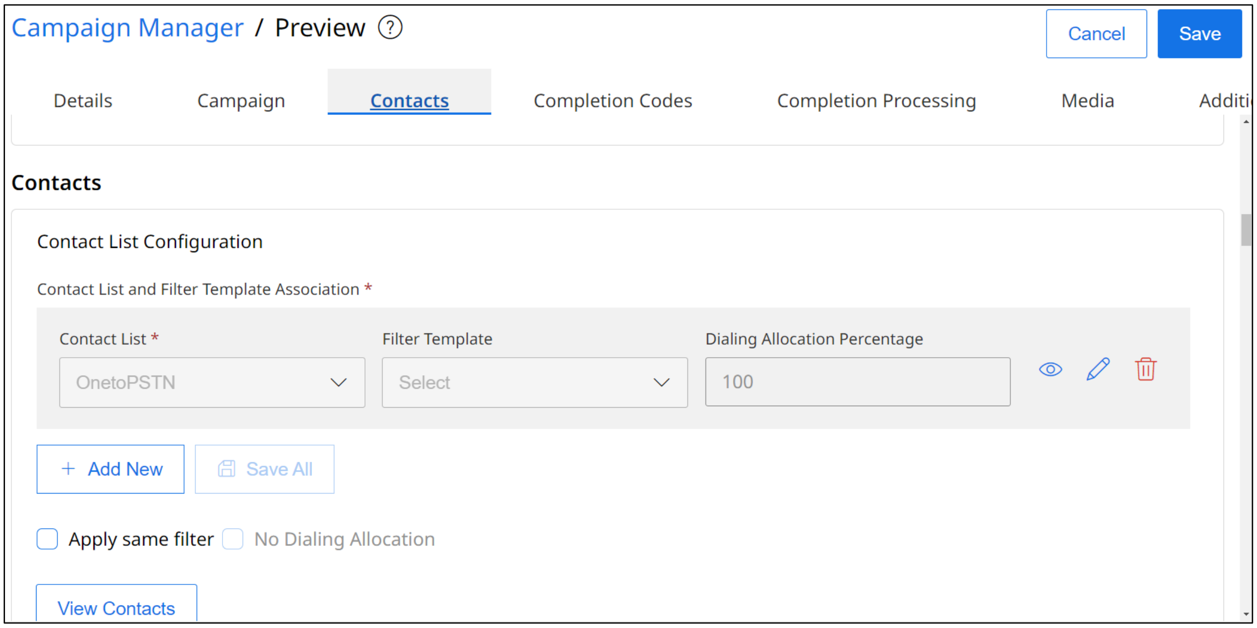
Clicking on **Preview** below to open the campaign and display the various components.



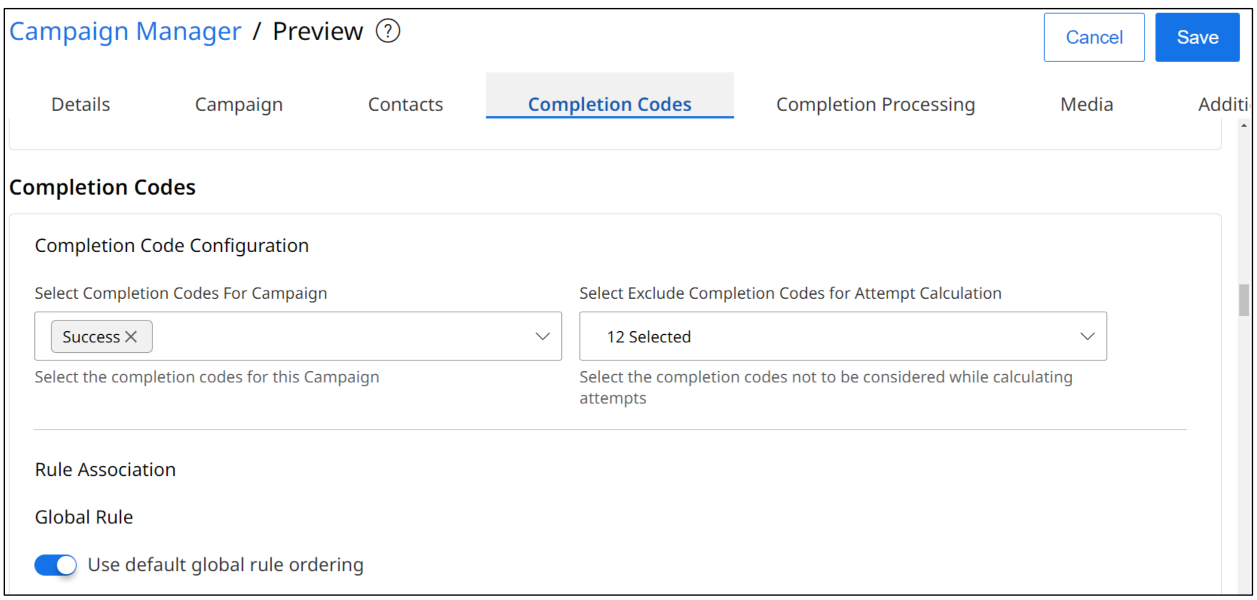
The **Campaign Strategy** that was shown previously is entered in the **Campaign** tab.



The **Contact List** displayed previously is associated with this campaign under the **Contacts** tab.



The **Completion Codes** that were displayed previously are added under the **Completion Codes** tab.



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.