Avaya Solution & Interoperability Test Lab

Application Notes for Altitude Xperience Engagement 8.5 from Altitude Software with Avaya Aura® Communication Manager R8.1, Avaya Aura® Session Manager R8.1 and Avaya Aura® Application Enablement Services R8.1 – Issue 1.0

Abstract

These Application Notes describe the configuration steps for provisioning Altitude Xperience Engagement 8.5 from Altitude Software with Avaya Aura® Session Manager R8.1 and Avaya Aura® Application Enablement Services R8.1 to control agents logged into Avaya Aura® Communication Manager.

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.

1. Introduction

These Application Notes outline the steps necessary to configure Altitude Xperience Engagement 8.5 from Altitude Software to interoperate with Avaya Aura® Session Manager R8.1 and Avaya Aura® Application Enablement Services R8.1 to control agents logged into Avaya Aura® Communication Manager R8.1. These Application Notes focus on two connections from Altitude Xperience Engagement to the Avaya solution.

1. The Telephony Server Application Programming Interface (TSAPI) connection from Altitude Telephony Gateway, a component of Altitude Xperience Engagement Server, to Avaya Aura® Application Enablement Services (AES).
2. The Session Initiation Protocol (SIP) connection from Altitude Communication Server (ACS) to Avaya Aura® Session Manager.

Where the primary focus of these Application Notes is the TSAPI connection to Avaya Aura® Application Enablement Services, the SIP connection to Session Manager, handled by Altitude Communication Server, is an add-on module of Altitude Xperience Engagement, allowing customers call into an IVR system prior to being routed to an Avaya agent. Because Altitude Communication Server serves as an add-on module, it will be included in these Application Notes.

Note: Altitude Xperience Engagement was previously known as Altitude uCI. This is the same product that was tested previously under the newly rebranded name of Altitude Xperience Engagement.

Altitude Xperience Engagement is an IP based contact center management solution, with both predictive dialing and multi-channel inbound capabilities. Altitude uSupervisor is a supervision and management tool that manages, monitors, and allows real-time, as well as historical, reporting of multimedia customer interactions. Altitude uAgent provides a workspace for multimedia contact center customer service representatives in windows and web environment. This tool integrates with business applications to present and manipulate customer data in real time, while offering media handling capabilities for inbound or outbound phone calls, e-mails, or chat requests. The Altitude Telephony Gateway is the component that implements Computer Telephony Integration (CTI) functionality, according to the protocol and specifics of each voice switch. The Altitude Automated Agents enables integrated IVR applications, with seamless transfer of voice and data to the contact center. Altitude Automated Agents uses SIP trunks via Altitude Communication Server to connect to Communication Manager via Session Manager.

Agents can use Altitude uAgent Windows or Altitude uAgent Web, both are totally independent of the telephony functionality using Avaya. The client application is an interface to show information and get requests from the agent. All telephony operations are handled by the Altitude Server using the telephony gateways. For compliance testing Altitude uAgent Windows was used. This may be referred to as Altitude uAgent Windows, or just Altitude uAgent, throughout these Application Notes.

2. General Test Approach and Test Results

The interoperability compliance testing evaluates the ability of Altitude Xperience Engagement to gain telephony functionality on Communication Manager via Application Enablement Services. Testing involved three Altitude Xperience Engagement agents logging in separately onto a H.323, a SIP and a Digital endpoint, going ready, and answering calls as well as being able to make outbound predictive calls from the Altitude uAgent. Agents utilize the telephony functionality on Communication Manager using Altitude uAgent.

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 this DevConnect Application Note 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 Altitude Xperience Engagement did not include use of any specific encryption features as requested by Altitude Software.

2.1. Interoperability Compliance Testing

The interoperability compliance testing included feature and serviceability testing. The feature testing focused on verifying Altitude uAgent and Altitude Automated Agents handling of CTI messages in the areas of call control, event notification and routing. Intra-switch calls as well as simulated PSTN calls were tested. The following call types were tested.

- Agent State Control with Altitude uAgent
- Inbound/Outbound calls
- Hold/Transfer/Conference/DTMF functionality
- Inbound Agent Skillset calls
- VDN routing, with digit collection
- Outbound Power Dial
- Outbound Power Dial, with native classification
- Outbound native Predictive
- Outbound native Predictive, with opt-out on nuisance

- Outbound Predictive with Altitude Call Classifier, via SIP trunk to Session Manager
- Outbound blended with Inbound
- Call Flows with SIP IVR, using Altitude Automated Agents
- Defense/Serviceability testing

2.2. Test Results

All test passed successfully with the following issue reported.

Outbound calls, with 'native' Call Classification enabled, fail with the agent logged into and using a SIP phone. Altitude evokes an outbound call to the simulated PSTN from a specified VDN on Communication Manger. The VDN then calls the agent, logged into a SIP extension, the call should be transferred to the SIP extension but fails to do so. A disconnect happens with a "Denial 1740: No Disconnect Supervision" message given out on the PSTN line. Both Avaya and Altitude Software are investigating the issue separately.

Until a resolution is found, the workaround is to either use Call Classification set to ACC (Altitude Call Classifier), that being where Call Classification is used from the Altitude Communication Server, or in the event that this module is not present, turn Call Classification off. Instructions on how to do these are outlined in **Section 8.1.2**, as part of the outbound campaign setup.

2.3. Support

Support from Avaya is available by visiting the website http://support.avaya.com and a list of product documentation can be found in **Section 11** of these Application Notes. Support from Altitude is available at http://www.altitude.com.

3. Reference Configuration

Figure 1 shows the network topology during compliance testing. The Altitude Xperience Engagement server was placed on the Avaya telephony LAN. Application Enablement Services provides the Altitude Xperience Engagement server CTI capability on Altitude Communication Manager. Altitude uAgent is used to answer/make the calls in a call center environment. SIP trunks between the Altitude Xperience Engagement server and Session Manager connect the Altitude Communication Server (SIP module on Altitude Xperience Engagement) to Communication Manager. The Altitude Communication Server is used both for IVR and predictive dialing. IVR control and scripting is provided by Altitude Automated Agents module using Altitude Communication Server.

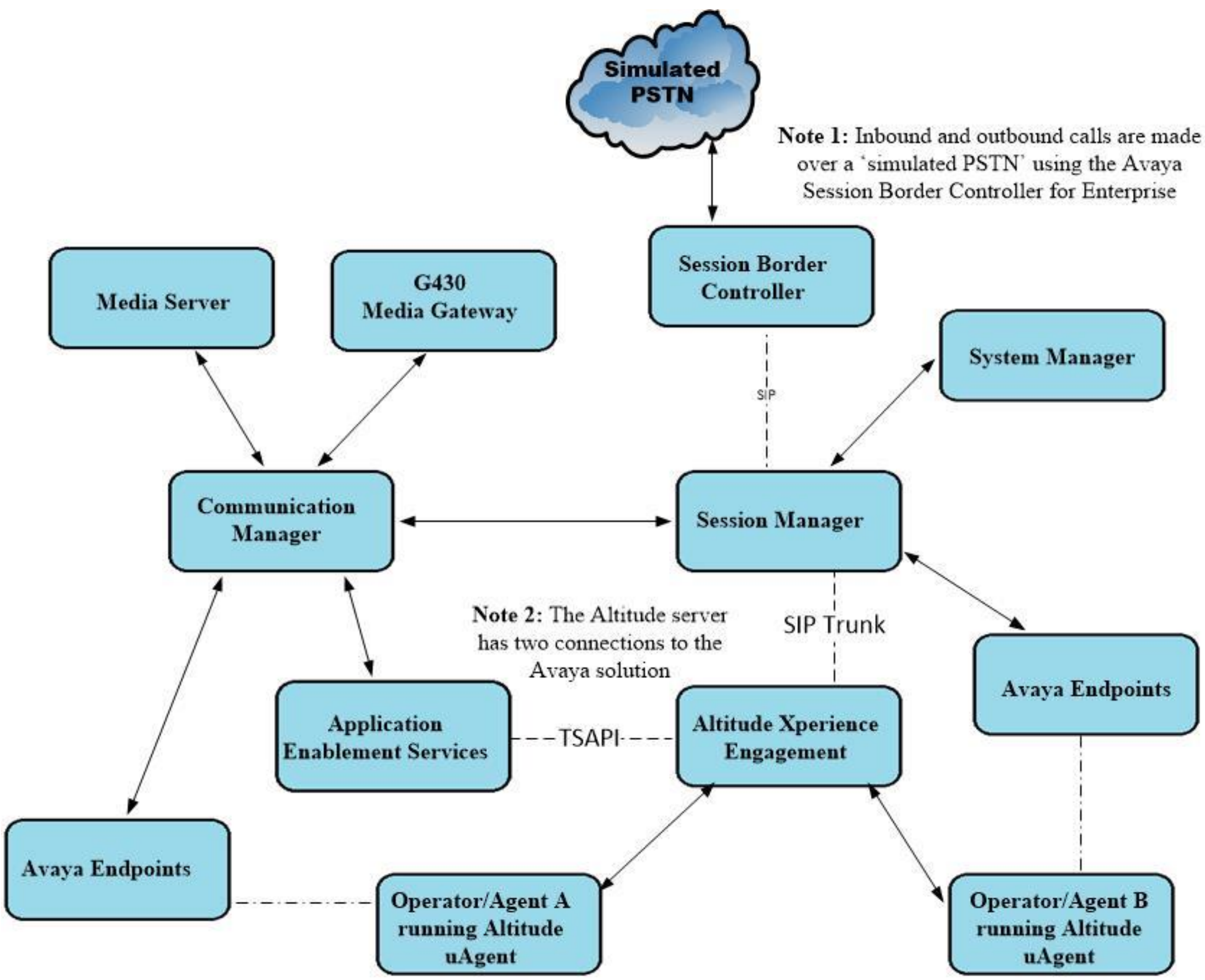


Figure 1: Network solution of Altitude Xperience Engagement 8.5 and Avaya Aura® Communication Manager R8.1 with Avaya Aura® Session Manager R8.1 and Avaya Aura® Application Enablement Services R8.1

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya Aura® System Manager running on a virtual server	8.1.3.0 Build No. – 8.1.0.0.733078 Software Update Revision No: 8.1.3.0.1011784 Feature Pack 3
Avaya Aura® Session Manager running on a virtual server	8.1.3 Build No. – 8.1.3.0.813014
Avaya Aura® Communication Manager running on a virtual server	8.1.3 – FP3 R018x.01.0.890.0 Update ID 01.0.890.0-26568
Avaya Aura® Application Enablement Services running on Virtual Server	8.1.3 Build No – 8.1.3.0.0.25-0
Avaya Aura® Media Server	8.0.2.138
Avaya G430 Media Gateway	41.16.0/1
Avaya J179 H.323 Deskphone	6.8304
Avaya J159 SIP Deskphone	4.0.7.1.5
Avaya 9408 Digital Phone	2.00
Altitude Xperience Engagement running on Windows 2019 Server with MS SQL Server 2017 - Altitude Assisted Server - Altitude Telephony Gateway - Altitude uSupervisor - Altitude uAgent - Altitude Communication Server	8.5

5. Configure Avaya Aura® Communication Manager

It is assumed that a fully functioning Communication Manager is present with the necessary licensing. For further information on the configuration of Communication Manager please see **Section 11** of these Application Notes.

This section can be divided into the following sub sections.

1. Display of System Features and Access Codes
2. Configuration of Call Center Attributes
3. Configure the CTI link to Avaya Aura® Application Enablement Services
4. Configure the SIP trunk to Avaya Aura® Session Manager
5. Configure call routing to Altitude Communication Server (ACS)

5.1. Display of System Features and Access Codes

This section shows the system setup at the time of compliance testing.

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
                  Attendant Vectoring? y



        (NOTE: You must logoff & login to effect the permission changes.)
```

On **Page 7**, verify the following customer options are set to **y** as shown below.

- **ACD?** to **y**
- **Vectoring (Basic)?** to **y**
- **Expert Agent Selection (EAS)?** to **y**

```
display system-parameters customer-options                      Page   7 of  12
                         CALL CENTER OPTIONAL FEATURES

                          Call Center Release: 8.0

                                ACD? y                              Reason Codes? y
                       BCMS (Basic)? y                   Service Level Maximizer? n
         BCMS/VuStats Service Level? y                 Service Observing (Basic)? y
  BSR Local Treatment for IP & ISDN? y         Service Observing (Remote/By FAC)? y
                  Business Advocate? n                 Service Observing (VDNs)? y
                    Call Work Codes? y                                Timed ACW? y
      DTMF Feedback Signals For VRU? y                       Vectoring (Basic)? y
                   Dynamic Advocate? n                   Vectoring (Prompting)? y
       Expert Agent Selection (EAS)? y               Vectoring (G3V4 Enhanced)? y
                            EAS-PHD? y                Vectoring (3.0 Enhanced)? y
                   Forced ACD Calls? n        Vectoring (ANI/II-Digits Routing)? y
               Least Occupied Agent? y        Vectoring (G3V4 Advanced Routing)? y
          Lookahead Interflow (LAI)? y                      Vectoring (CINFO)? y
Multiple Call Handling (On Request)? y         Vectoring (Best Service Routing)? y
    Multiple Call Handling (Forced)? y                   Vectoring (Holidays)? y
  PASTE (Display PBX Data on Phone)? y                  Vectoring (Variables)? Y

        (NOTE: You must logoff & login to effect the permission changes.)
```

5.1.2. Define Feature Access Codes (FAC)

Use the **change feature-access-codes** command to define the required access codes. On **Page 1** observe the **Auto Route Selection (ARS) - Access Code 1** is set to **9**. This will be required again in **Section 8.1.1** when defining the Line Prefix.

```
change feature-access-codes                                     Page   1 of  12
                               FEATURE ACCESS CODE (FAC)
         Abbreviated Dialing List1 Access Code: *11
         Abbreviated Dialing List2 Access Code: *12
         Abbreviated Dialing List3 Access Code: *13
Abbreviated Dial - Prgm Group List Access Code: *10
                      Announcement Access Code: *27
                       Answer Back Access Code: #02
                         Attendant Access Code:
      Auto Alternate Routing (AAR) Access Code: 8
    Auto Route Selection (ARS) - Access Code 1: 9     Access Code 2:
                 Automatic Callback Activation: *05    Deactivation: #05
Call Forwarding Activation Busy/DA: *03    All: *04    Deactivation: #04
   Call Forwarding Enhanced Status: *73    Act: *74    Deactivation: #74
                         Call Park Access Code: *02
                       Call Pickup Access Code: *09
CAS Remote Hold/Answer Hold-Unhold Access Code:
                  CDR Account Code Access Code: *14
                        Change COR Access Code:
                   Change Coverage Access Code:
            Conditional Call Extend Activation:        Deactivation:
                   Contact Closure   Open Code:          Close Code:
```

On **Page 5** define a FAC for each of the following:

- **Aux Work Access Code:** When activated this feature will set the ACD agent to an Auxilary work state, this is the default state for an agent upon first login.
- **After Call Work Access Code:** When activated this feature will set the ACD agent to an ACW or 'not ready' work state, this is the default state for an agent upon call completion when using manual-in.
- **Login Access Code:** This feature allows ACD agents to log in to an extension.
- **Logout Access Code:** This feature allows ACD agents to log out of an extension.
- **Manual-in Access Code:** When activated this feature will set the ACD agent to a state where they are available to handle calls, upon completion of a call the agent will be unavailable until the feature is activated again.

```
change feature-access-codes                                   Page   5 of  12
                               FEATURE ACCESS CODE (FAC)
                                 Call Center Features
  AGENT WORK MODES
                           After Call Work Access Code: *51
                                    Assist Access Code: *55
                                   Auto-In Access Code: *52
                                  Aux Work Access Code: *53
                                     Login Access Code: *50
                                    Logout Access Code: #50
                                 Manual-in Access Code: *54
  SERVICE OBSERVING
             Service Observing Listen Only Access Code: *56
             Service Observing Listen/Talk Access Code: *57
                 Service Observing No Talk Access Code: #57
   Service Observing Next Call Listen Only Access Code:
 Service Observing by Location Listen Only Access Code:
 Service Observing by Location Listen/Talk Access Code:

  AACC CONFERENCE MODES
                    Restrict First Consult Activation:      Deactivation:
                   Restrict Second Consult Activation:      Deactivation:
```

5.1.3. Administer Class of Restriction

Enter the **change cor 1** command where **1** corresponds to the Class of Restriction assigned to the agent login IDs in **Section 5.2.4**. On **Page 1**, set the **Direct Agent Calling** to **y**. This will allow agents to be called directly once they are logged in.

Direct Agent Calling allows a call to be directed to a specific agent logged into a skill. If the agent isn't available, the call will be queued for that agent, waiting for that specific agent to become available. If Direct Agent Calling is disabled, the call to a busy agent isn't queued and treated as any other call.

```
change cor 1                                                Page   1 of  43
                              CLASS OF RESTRICTION

               COR Number: 1
          COR Description: PG Default

                      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? y
     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? y
            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
```

5.2. Configuration of Call Center Attributes

In order for calls to be routed to agents, Hunt Groups (skills) Vectors and Vector Directory Numbers (VDN) must be configured.

5.2.1. Hunt Groups

Enter the **add hunt-group n** command where **n** in the example below is **90**. On **Page 1** of the **hunt group** form, assign a **Group Name** and **Group Extension** valid under the provisioned dial plan. Set the following options to **y** as shown below.

- **ACD** to **y**
- **Queue** to **y**
- **Vector** to **y**

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

            Group Number: 90                                ACD? y
              Group Name: Altitude Inbound                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 the **Skill** field to **y** as shown below.

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

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


      Controlling Adjunct: none



 Timed ACW Interval (sec):
   Multiple Call Handling: none
```

On **Page 3**, **Redirect on No Answer** was set to **3 rings** to allow the call to move onto the other agents logged into the same hunt group if it was not answered after 3 rings at the first agent's phone.

```
change hunt-group 90                                           Page   3 of   4
                                  HUNT GROUP

             Interruptible Aux Threshold: none


   Redirect on No Answer (rings): 3
    Redirect on No Answer to VDN:
Redirect on IP/OPTIM Fail to VDN:
Forced Entry of Stroke Counts or Call Work Codes? n
```

Repeat the steps above to create a hunt group for an outbound service, **hunt group 92** is shown below.

```
add hunt-group 92                                              Page   1 of   4
                                  HUNT GROUP

            Group Number: 92                                ACD? y
              Group Name: Altitude Outbound               Queue? y
         Group Extension: 1802                           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 the **Skill** field to **y** as shown below.

```
add hunt-group 34                                              Page   2 of   4
                                  HUNT GROUP

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


      Controlling Adjunct: none

 Timed ACW Interval (sec):
   Multiple Call Handling: none
```

5.2.2. Vectors

Enter the **add vector n** command, where **n** is the vector number. Enter the vector steps to queue to **1st** as shown below. This will queue to the skillset that is first on the VDN. The first line of the Vector should be the "queue-to skill" without any wait times or adjunct routing.

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

    Number: 3                Name: Altitude Inbound
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 queue-to     skill 1st   pri m
02 wait-time    180 secs hearing ringback
03 stop
```

Another Vector was used for Adjunct Routing, this is where the Altitude Xperience Engagement takes control of the call. The first line should be adjunct routing link x, where x is the CTI link created in **Section 5.3**.

```
add vector 2                                                Page   1 of   6
                                  CALL VECTOR

    Number: 4                Name: Altitude Outbound
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 adjunct      routing link 1
02 wait-time    5   secs hearing silence
03 queue-to     skill 1st   pri m
04 wait-time    180 secs hearing ringback
05 stop
```

5.2.3. Vector Directory Numbers (VDN)

Enter the **add vdn n** command, where **n** is an available extension number. On **Page 1** assign a **Name** for the VDN and set the **Vector Number** to the relevant vector. The hunt group associated with this VDN is added as the **1st Skill**. In the example below, the inbound hunt group is added as this is the VDN that is called for the inbound calls.

```
add vdn 4906                                                Page   1 of   3
                            VECTOR DIRECTORY NUMBER

                             Extension: 4906
                                 Name*: Altitude Inbound
                           Destination: Vector Number        1
                   Attendant Vectoring? n
                  Meet-me Conferencing? n
                    Allow VDN Override? n
                                   COR: 1
                                   TN*: 1
                              Measured: none

        VDN of Origin Annc. Extension*:
                            1st Skill*:90
                            2nd Skill*:
                            3rd Skill*:
```

The above steps may also be used to create a VDN for the outbound service, shown below. In this case the outbound hunt group was added as the **1st Skill**, as this is the VDN associated with the outbound service.

```
add vdn 4908                                                Page   1 of   3
                            VECTOR DIRECTORY NUMBER

                             Extension: 4908
                                 Name*: Altitude Outbound
                           Destination: Vector Number        1
                   Attendant Vectoring? n
                  Meet-me Conferencing? n
                    Allow VDN Override? n
                                   COR: 1
                                   TN*: 1
                              Measured: none

        VDN of Origin Annc. Extension*:
                            1st Skill*:92
                            2nd Skill*:
                            3rd Skill*:
```

Note: Other VDN's were also used during compliance testing, these are listed, along with other Vectors, in the **Appendix** of these Application Notes.

5.2.4. Administer Agent Logins

Enter the **add agent-loginID n** command; where **n** is an available extension number. Enter a descriptive name for the agent in the **Name** field. Ensure the **COR** field is set to **1** which relates to the COR configured in **Section 5.1.3**. The **Auto Answer** field is set to **station**, this setting was also used for the outbound calls.

```
add agent-loginID 1401                                        Page   1 of   2
                                 AGENT LOGINID

                Login ID: 1401                                     AAS? n
                    Name: Altitude Agent1                        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:
                                              Password (enter again):
                                                         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,** assign a skill to the agent by entering the relevant hunt group number created in **Section 5.2.1** for **SN** and entering a skill level of **1** for **SL**. In this case, an agent is able to handle both inbound and outbound calls. Set the **Direct Agent Skill** to the inbound hunt group **90**.

```
change agent-loginID 1401                                     Page   2 of   3
                                 AGENT LOGINID
      Direct Agent Skill: 90                            Service Objective? n
Call Handling Preference: skill-level                 Local Call Preference? n

    SN   RL SL           SN   RL SL           SN   RL SL           SN   RL SL
 1: 90      1            16:                  31:                  46:
 2: 92      1            17:                  32:                  47:
```

5.2.5. Configure Agent Extensions

H.323 extensions are configured on Communication Manager where the SIP extensions are configured using System Manager. Both extension types were setup as follows for the connection with Altitude Xperience Engagement.

5.2.5.1 Configure H.323 Extension

For each station or extension that agents will log in to, enter the command **change station n,** where **n** is the station extension. On **Page 1** the **COR** is set to **1**, as shown below, configure the station password i.e., the **Security Code** and the **Extension** number also.

```
change station 1001                                          Page   1 of   5
                                     STATION

Extension: 1001                         Lock Messages? n             BCC: 0
     Type: J179                         Security Code: *              TN: 1
     Port: S00000                     Coverage Path 1:               COR: 1
     Name: 1001, H323User             Coverage Path 2:               COS: 1
                                      Hunt-to Station:             Tests? n
STATION OPTIONS
                                          Time of Day Lock Table:
              Loss Group: 19        Personalized Ringing Pattern: 1
                                                Message Lamp Ext: 1001
            Speakerphone: 2-way              Mute Button Enabled? y
        Display Language: english                Button Modules: 0
 Survivable GK Node Name:
          Survivable COR: internal             Media Complex Ext:
   Survivable Trunk Dest? y                          IP SoftPhone? y

                                               IP Video Softphone? n
                              Short/Prefixed Registration Allowed: default

                                               Customizable Labels? y
```

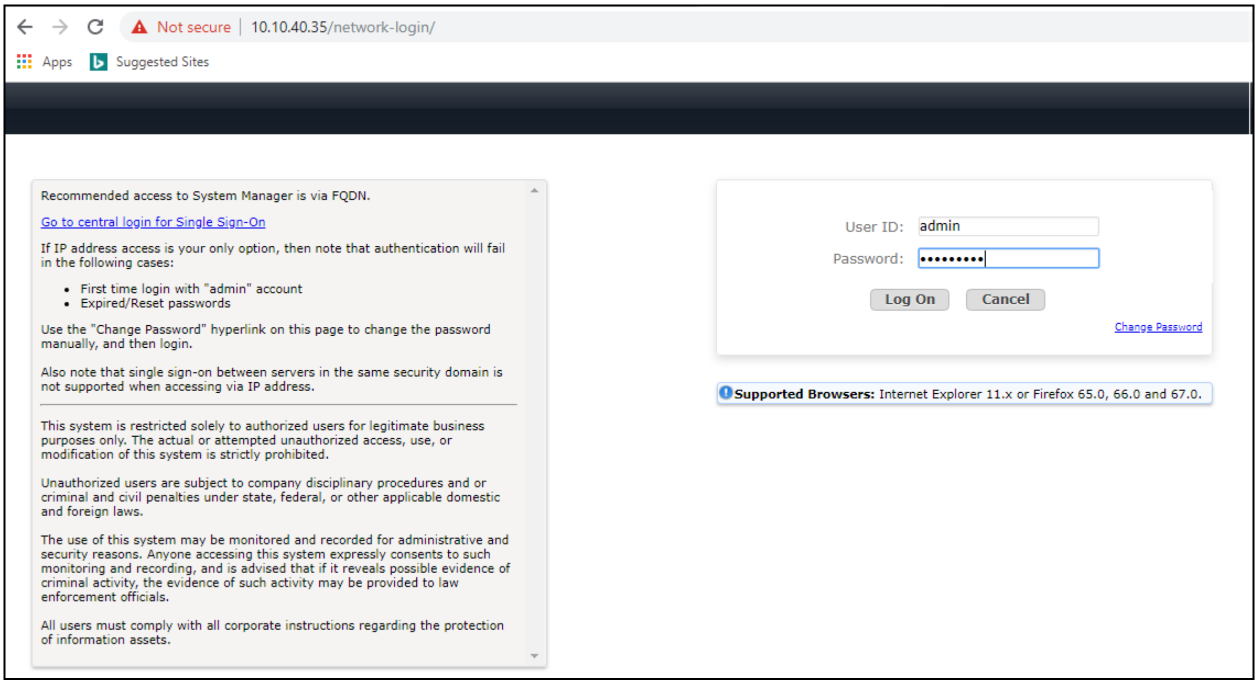
On **Page 4**, three call-appearance buttons were used. There is no requirement to set any other buttons to allow agents login using Altitude.

```
change station 1001                                          Page   4 of   5
                                     STATION
 SITE DATA
       Room:                                         Headset? n
       Jack:                                         Speaker? n
      Cable:                                        Mounting: d
      Floor:                                     Cord Length: 0
   Building:                                       Set Color:

ABBREVIATED DIALING
     List1: system            List2:                  List3:

BUTTON ASSIGNMENTS
 1: call-appr                           5:
 2: call-appr                           6:
 3: call-appr                           7:
 4:                                     8:
    voice-mail
```

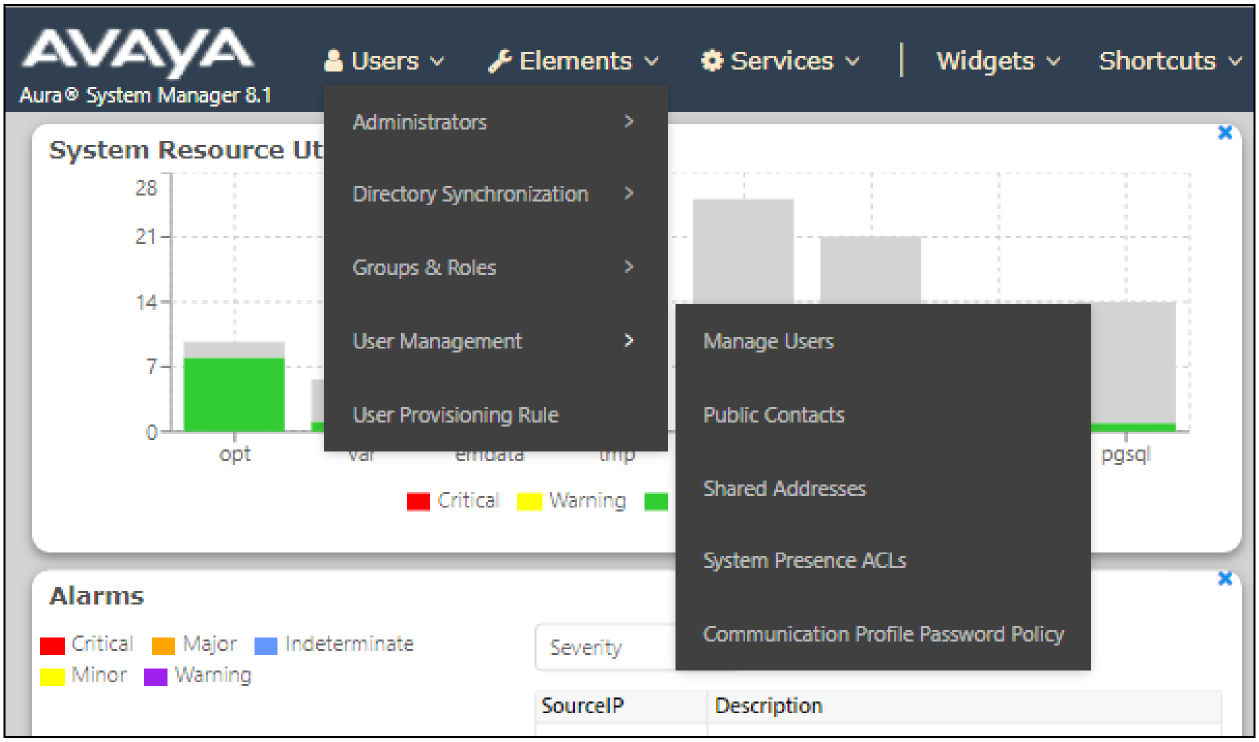
5.2.5.2 Configure SIP Extension

Each Avaya SIP endpoint or extension 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 of SIP phones on Communication Manager must be carried out from 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. Log in using appropriate credentials.

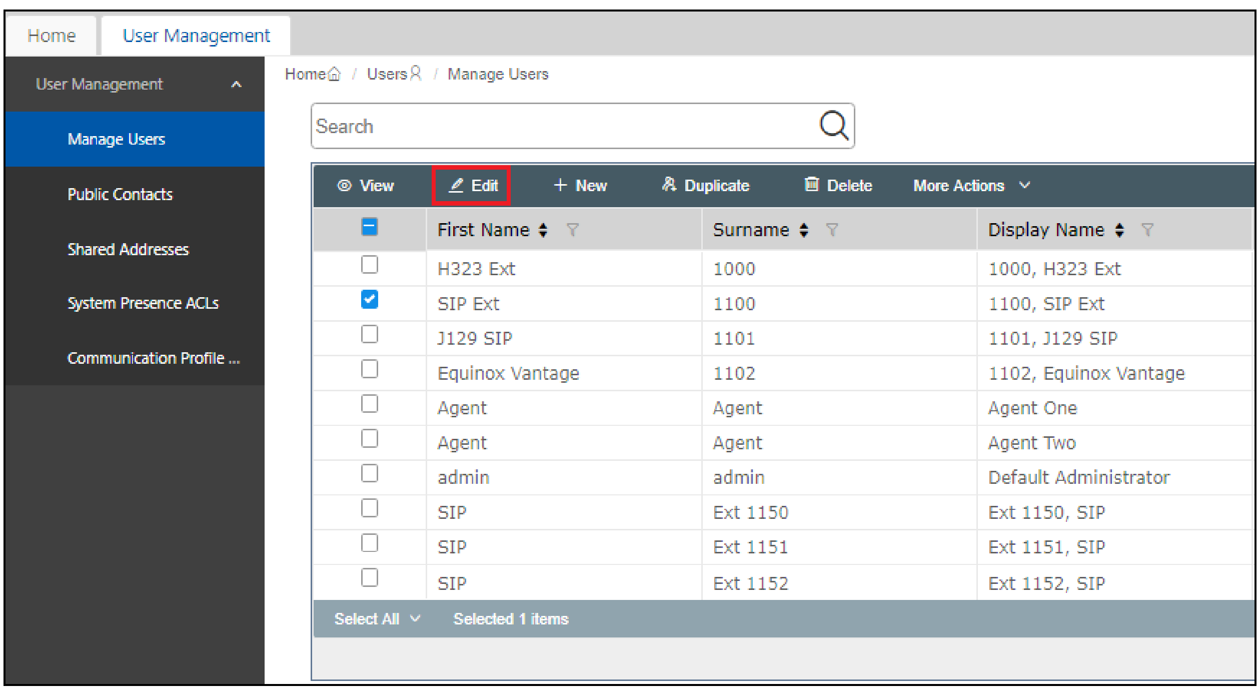
Note: The following shows changes a SIP extension and assumes that the SIP extension has been programmed correctly and is fully functioning.



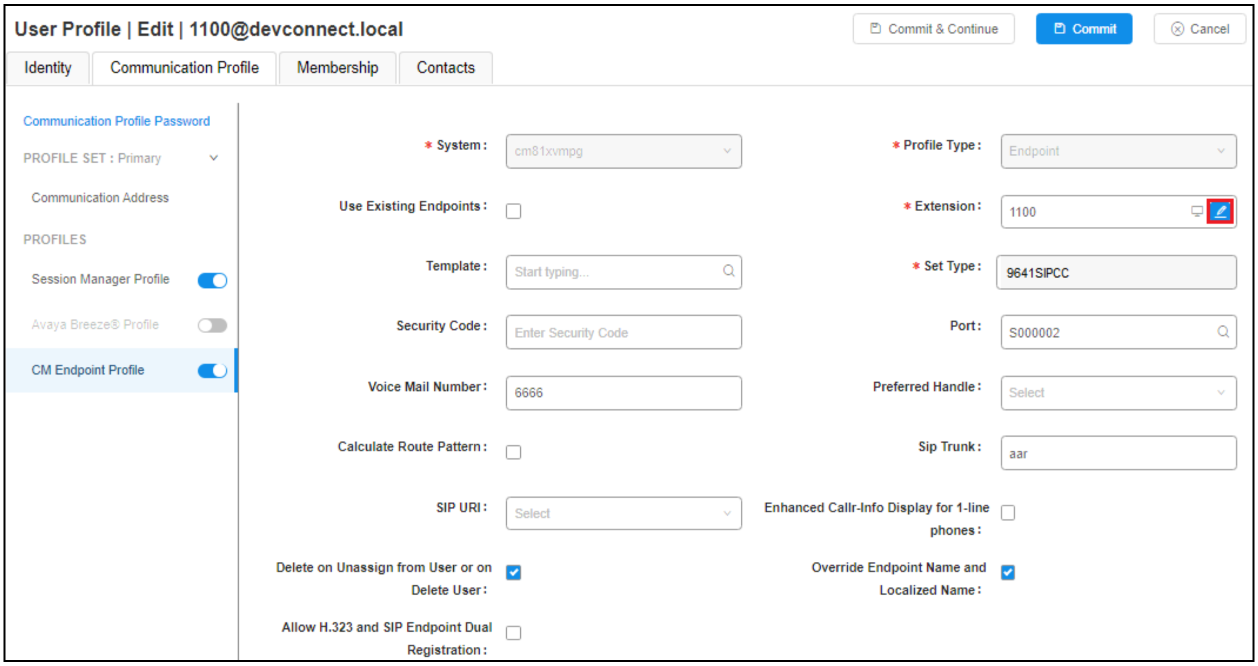
From the home page, click on **Users → User Management → Manage Users**, as shown below.



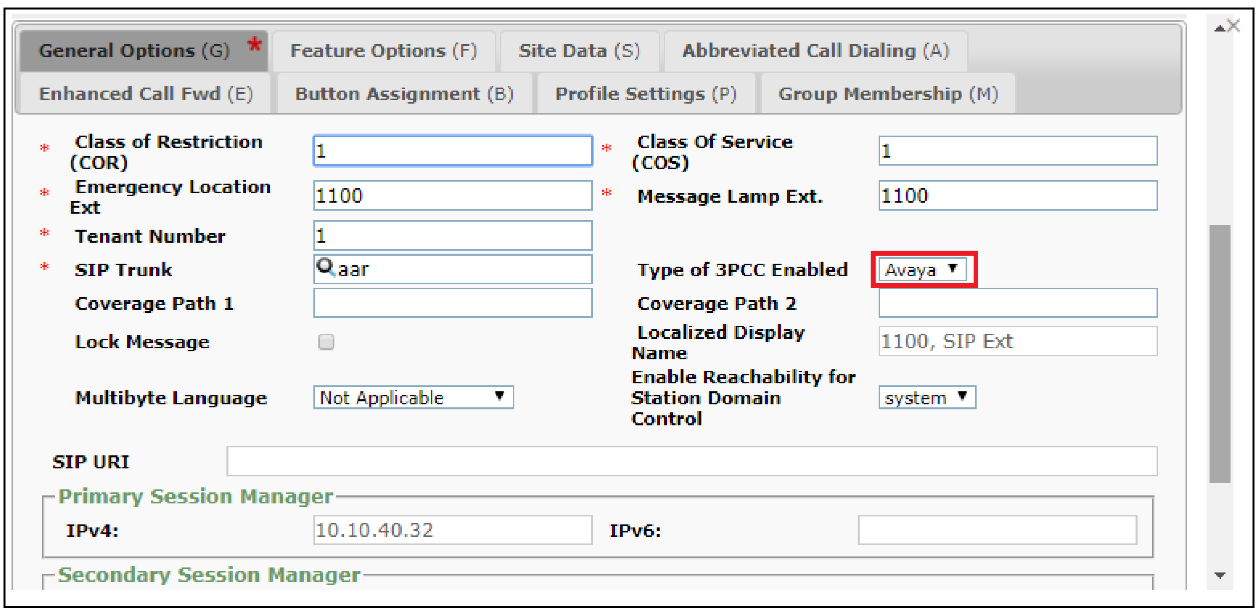
Click on **Manager Users** in the left window. Select the station to be edited and click on **Edit**.



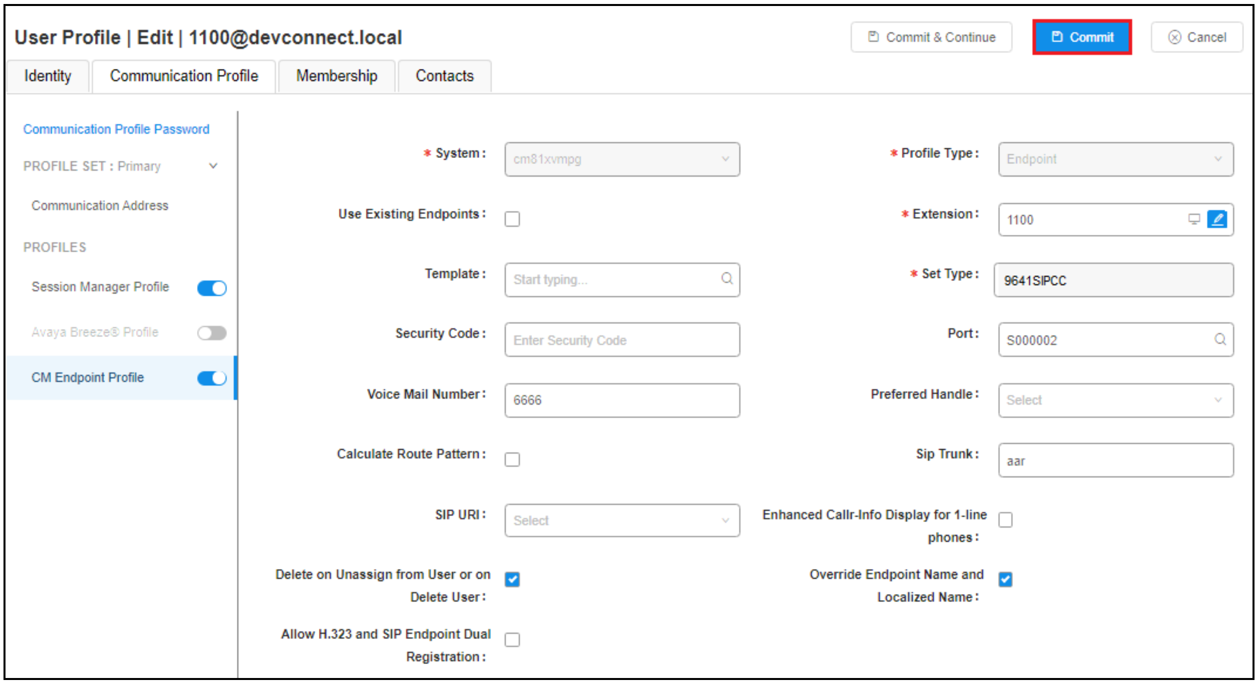
Click on the **CM Endpoint Profile** tab in the left window. Click on **Endpoint Editor** to make changes to the SIP station.



In the **General Options** tab ensure that **Type of 3PCC Enabled** is set to **Avaya** as is shown below. Click on **Done**, at the bottom of the screen, once this is set, (not shown).



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



5.3. Configure the CTI link to Avaya Aura® Application Enablement Services

The following section shows the steps required to setup the CTI link between Communication Manager and Application Enablement Services and will give information on how this link was setup for compliance testing with Altitude Xperience Engagement. Add a CTI link using the **add cti-link n** command. 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: aes81xvmpg
```

5.4. Configure the SIP trunk to Avaya Aura® Session Manager

In the **IP Network Region** form, the **Authoritative Domain** field is configured to match the domain name configured on Session Manager in **Section 7.1.1**. 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 ACS. 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), **G.711MU** (mu-law) and **G729A**, which are supported by ACS.

```
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:
 5:
 6:
 7:
```

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; **tcp** (transport control protocol) or **tls** (Transport Layer Security), TLS was used for compliance 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 IP Node Names (not shown here).
- Set the **Far-end Node Name** to the node name defined for the Session Manager (again taken from the IP Node Names).
- 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 was left blank specifically for this testing with Altitude.
- 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.

```
change signaling-group 21                                       Page   1 of   3
                                SIGNALING GROUP

 Group Number: 21              Group Type: sip
   IMS Enabled? n        Transport Method: tls
         Q-SIP? n
      IP Video? n                                 Enforce SIPS URI for SRTP? y
  Peer Detection Enabled? y  Peer Server: SM                      Clustered? n
 Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? y
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? n
Alert Incoming SIP Crisis Calls? n
   Near-end Node Name: procr                 Far-end Node Name: 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): 66
```

Configure the **Trunk Group** form as shown below. This trunk group is used for calls to and from ACS. 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 to **public-ntwrk**, which was used for compliance testing. 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   4
                                TRUNK GROUP

Group Number: 21                   Group Type: sip           CDR Reports: y
  Group Name: SIP TRUNK OUT              COR: 1        TN: 1        TAC: *821
   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: 21
                                                     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 Altitude Software 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   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): 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: The **UUI Treatment** is currently set to **service-provider**, with this being the case the corresponding setting on the ACS must be set to "Avaya IA5 ASCII" (see **Section 8.2.2**). If **UUI Treatment** is set to **shared** then the corresponding setting on the ACS must be set to "Avaya Shared UUI".

```
change trunk-group 21                                            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

 DSN Term? n
```

Settings on **Page 4** are as follows.

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

                                       Mark Users as Phone? n
Prepend '+' to Calling/Alerting/Diverting/Connected Number? n
                       Send Transferring Party Information? y
                                  Network Call Redirection? 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 call routing to Altitude ACS

The following shows how calls were routed to the Altitude ACS via the SIP trunk created in **Section 5.4**.

5.5.1. Configure Dial Plan

It was decided for compliance testing that all calls to 6300 were to be sent across the SIP trunk to Session Manager to route the call to ACS. To achieve this, automatic alternate routing (aar) was used to route the calls. The dial plan and aar routing analysis need to be changed.

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   ext      #           3   fac
   2           4   udp
   3           4   udp
   4           4   ext
   5           4   udp
   6           4   udp
   6666        4   ext
   7           4   udp
   8           1   fac
   9           1   fac
   *           3   fac
   *8          4   dac
```

5.5.2. Administer Route Selection for ACS Calls

Use the **change uniform-dialplan** command to configure the routing of the dialed digits. In the example below calls to **6300** 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
 6300             4   0                 aar  n
                                             n
                                             n
                                             n
                                             n
```

Use the **change aar analysis** command to further configure the routing of the dialed digits. Calls to Altitude are achieved by dialing **6300** 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
    6300                   4    4      21       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 5.4**. The **Numbering Format** was set to **lev0-pvt**.

```
change route-pattern 21                                            Page   1 of   3
                    Pattern Number: 1      Pattern Name: SIP TRUNK OUT
    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
```

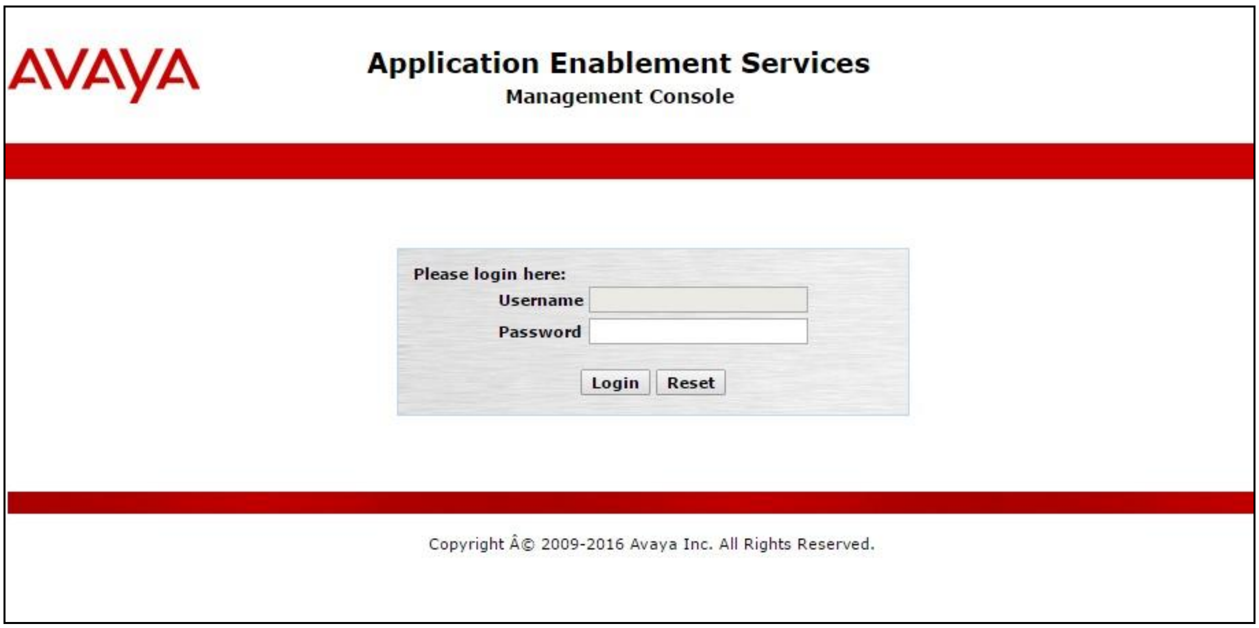
6. Configure Avaya Aura® Application Enablement Services

Application Enablement Services enable Computer Telephony Interface (CTI) applications to control and monitor telephony resources on Communication Manager.

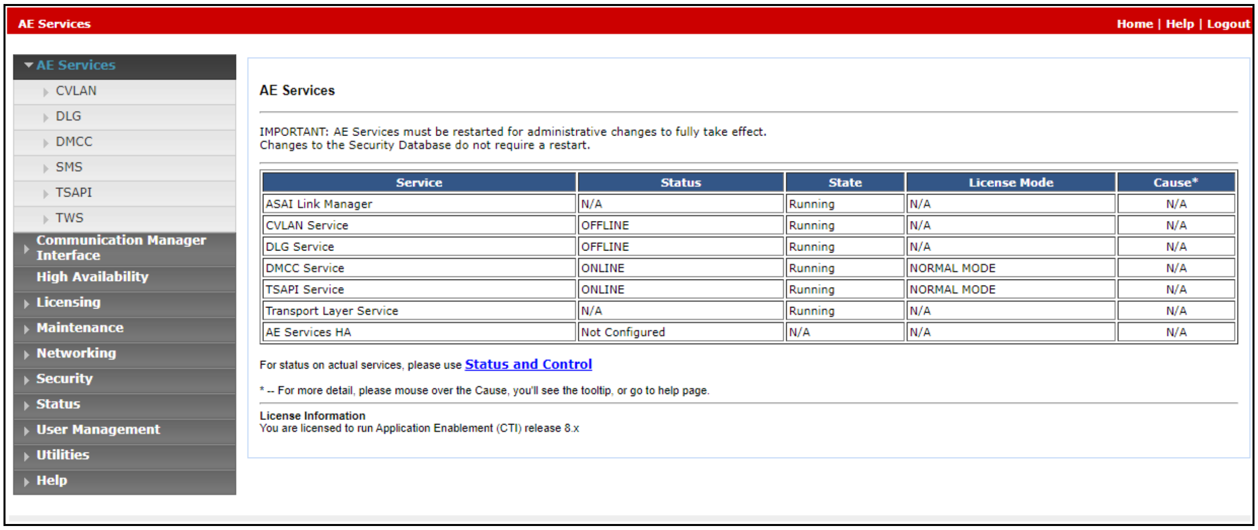
This section assumes that installation and basic administration of the Application Enablement Services server has been performed. The steps in this section describe the configuration of a Switch Connection, creating a CTI link for TSAPI, and a CTI user. For further information on Avaya Application Enablement Services please refer to **Section 11** of these Application Notes.

6.1. Verify Licensing

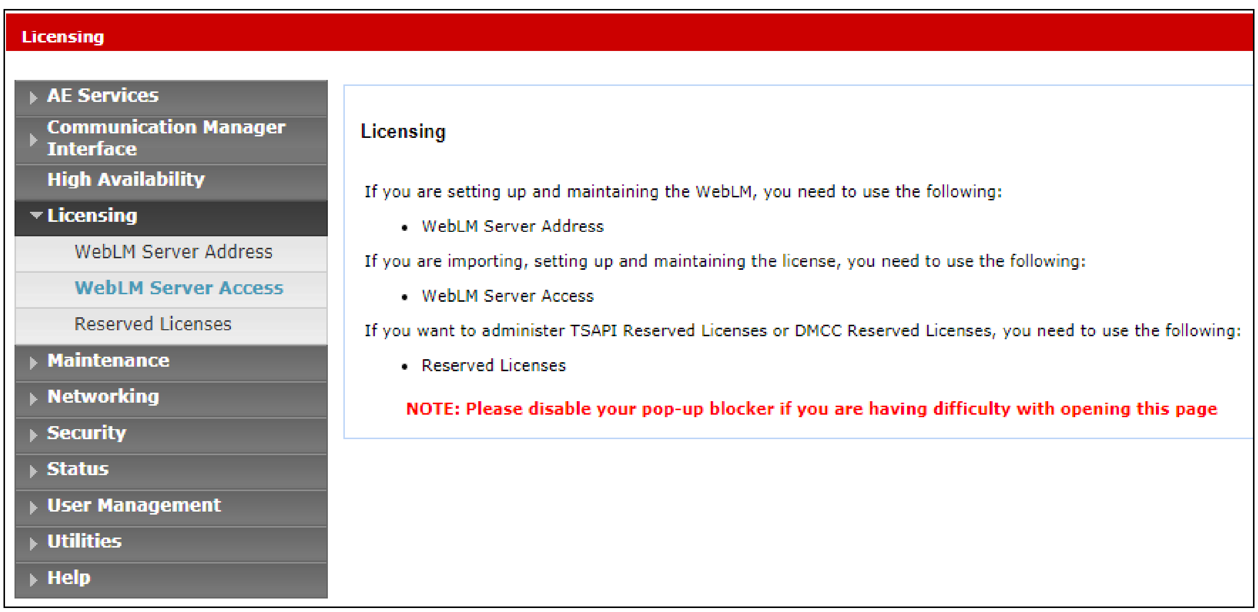
To access the Application Enablement Services Management Console, enter **https://<ip-addr>** as the URL in an Internet browser, where <ip-addr> is the IP address of the Application Enablement Services. At the login screen displayed, log in with the appropriate credentials and then select the **Login**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



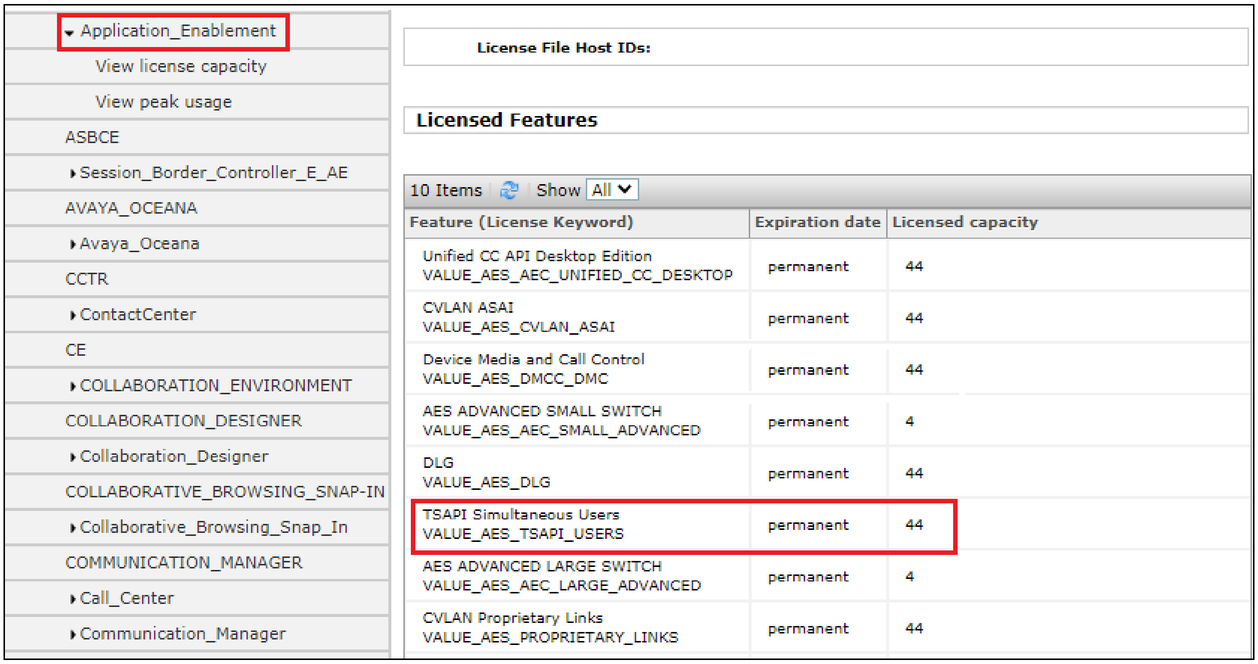
The Application Enablement Services Management Console appears displaying the **Welcome to OAM** screen (not shown). Select **AE Services** and verify that the TSAPI Service is licensed by ensuring that **TSAPI Service** is in the list of **Services** and that the **License Mode** is showing **NORMAL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



The TSAPI licenses are user licenses issues 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.

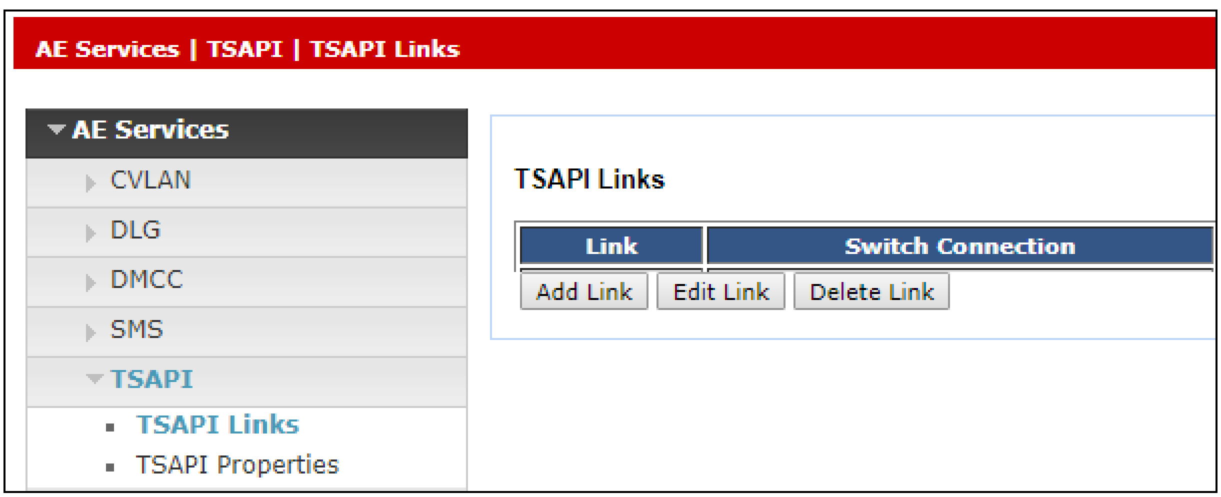


The following screen shows the available licenses for TSAPI users.



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.



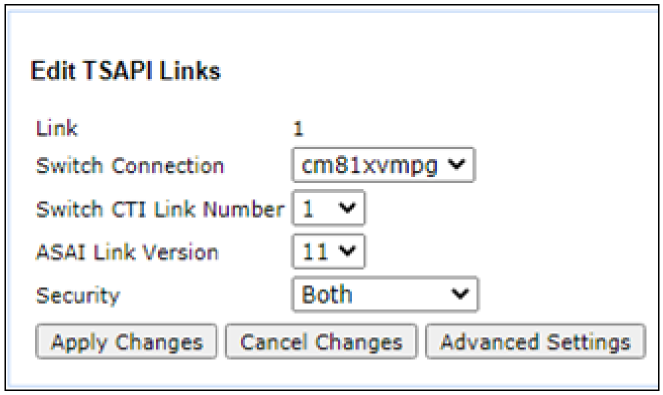
On the **Add TSAPI Links** screen (or the **Edit TSAPI Links** screen to edit a previously configured TSAPI Link as shown below), enter the following values:

- **Link:** Use the drop-down list to select an unused link number.
- **Switch Connection:** Choose the appropriate switch connection **cm81xvmpg**, which has already been configured, from the drop-down list.
- **Switch CTI Link Number:** Corresponding CTI link number configured in **Section 5.3**.

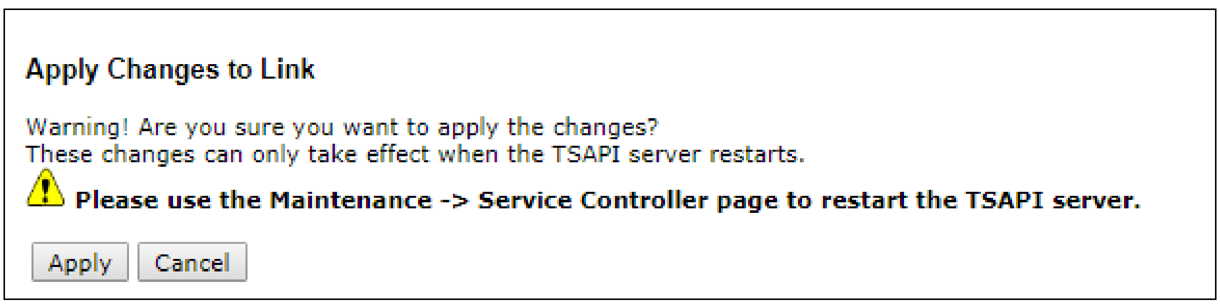
- **ASAI Link Version:** This should be set to the highest version available.
- **Security:** This should be set to **Both** allowing both secure and nonsecure connections.

Once completed, select **Apply Changes**.

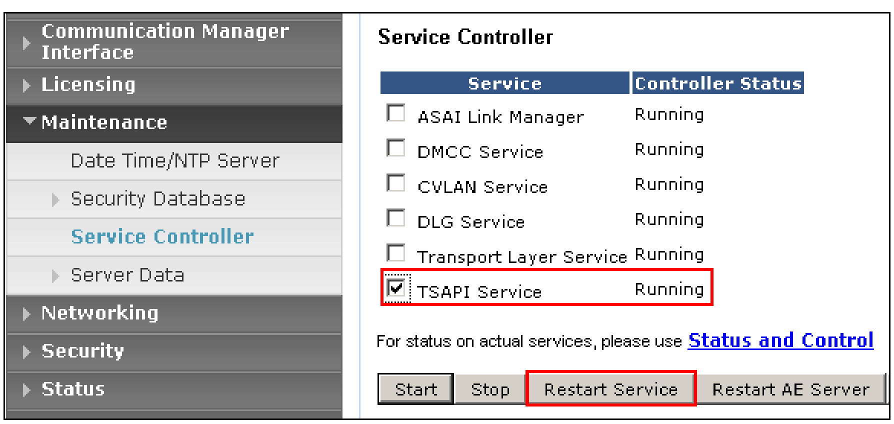
Note: The **Switch Connection** name **cm81xvmpg** should be noted here and given when setting up Altitude Xperience Engagement.



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



The TSAPI Service must be restarted to effect the changes made in this section. From the Management Console menu, navigate to **Maintenance → Service Controller**. On the Service Controller screen, tick the **TSAPI Service** and select **Restart Service**.

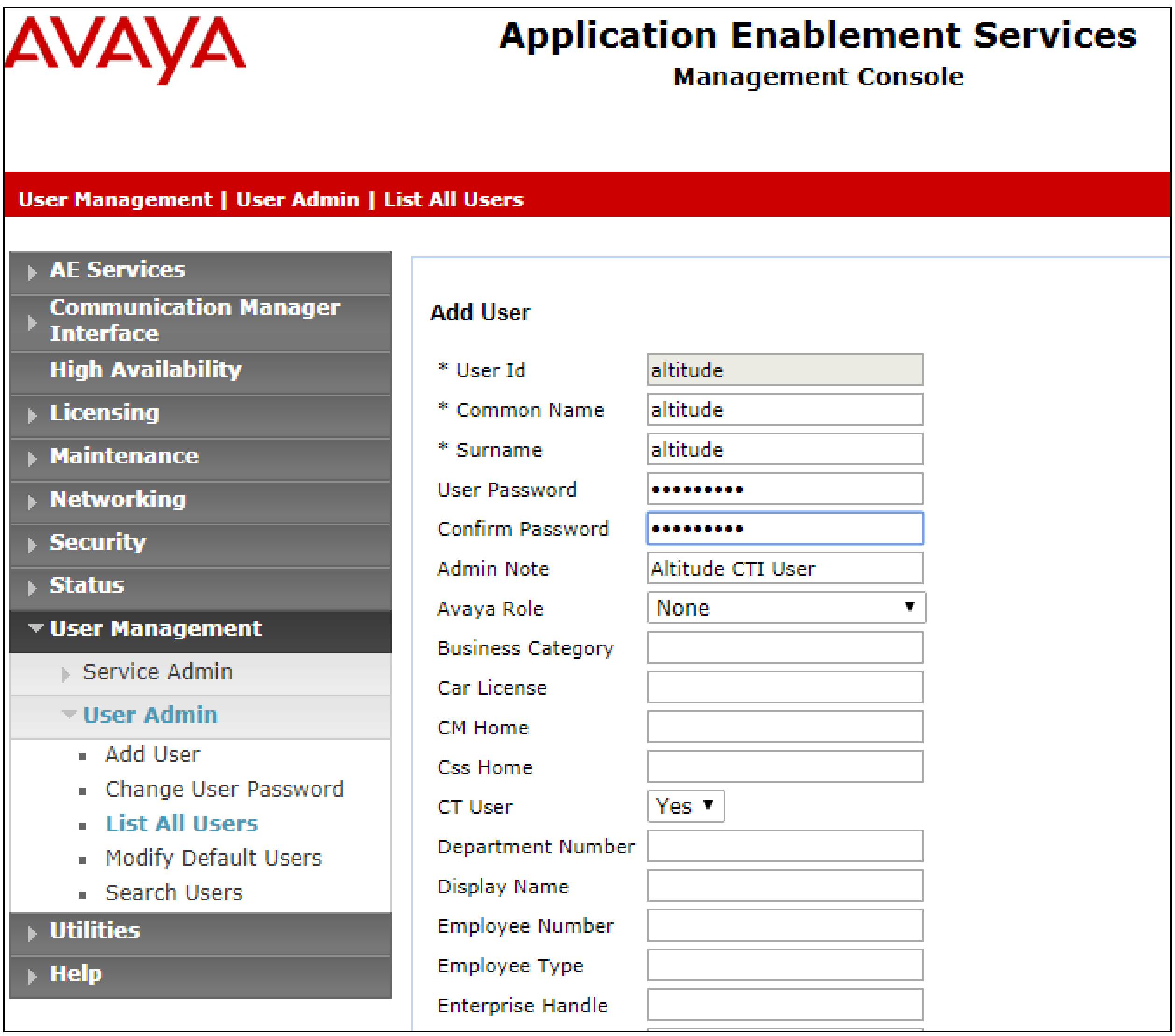


6.3. Create Avaya CTI User

A User ID and password needs to be configured for the Altitude Xperience Engagement server to communicate as a TSAPI client 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.

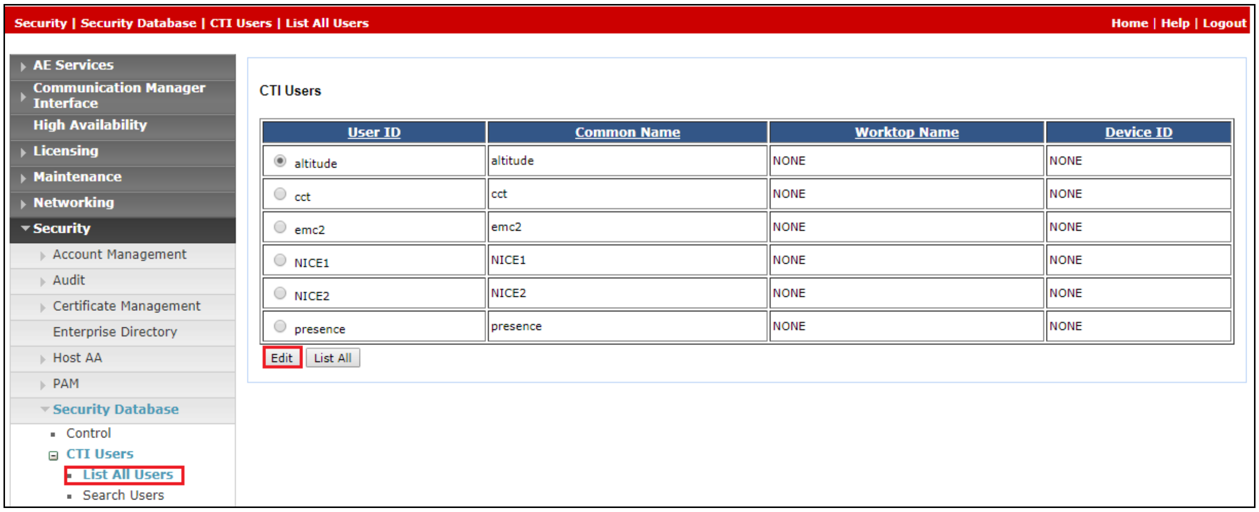
- **User Id -** This will be used by the Altitude Xperience Engagement server in **Section 8.1.1**.
- **Common Name** and **Surname -** Descriptive names need to be entered.
- **User Password** and **Confirm Password -** This will be used with the **User Id** in **Section 8.1.1**.
- **CT User -** Select **Yes** from the drop-down menu.

Complete the process by choosing **Apply** at the bottom of the screen (not shown).

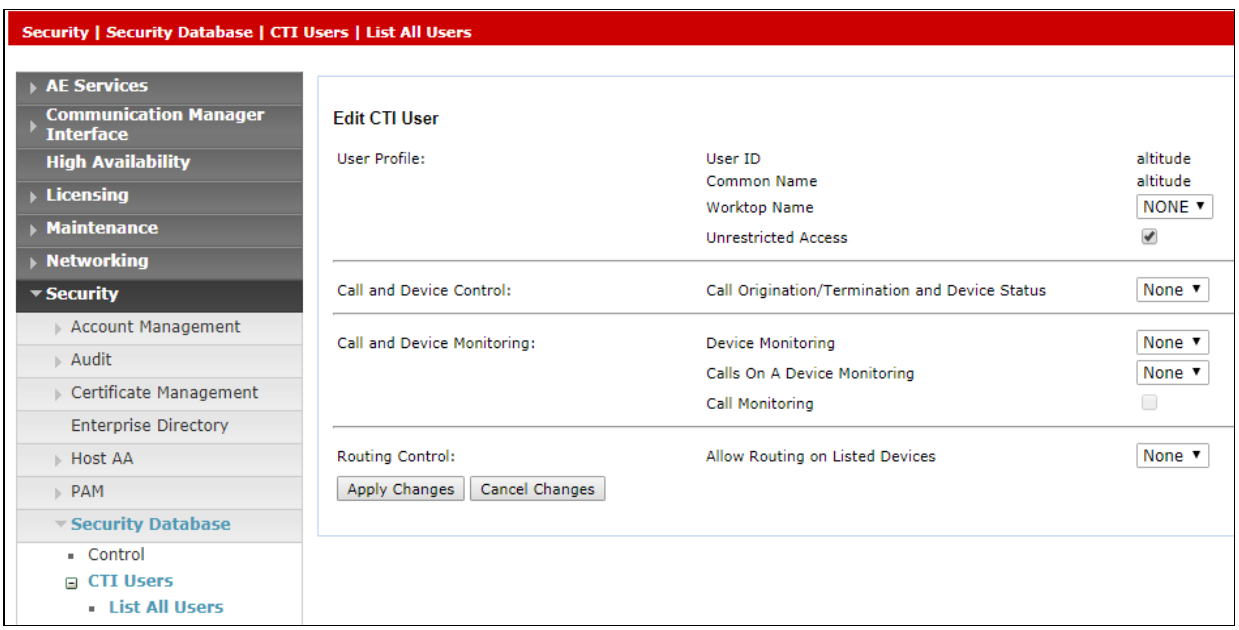


6.4. Enable Unrestricted Access for CTI User

Navigate to the **CTI Users** screen by selecting **Security → Security Database → CTI Users → List All Users**. Select the user that was created in **Section 6.3** and select the **Edit** option.



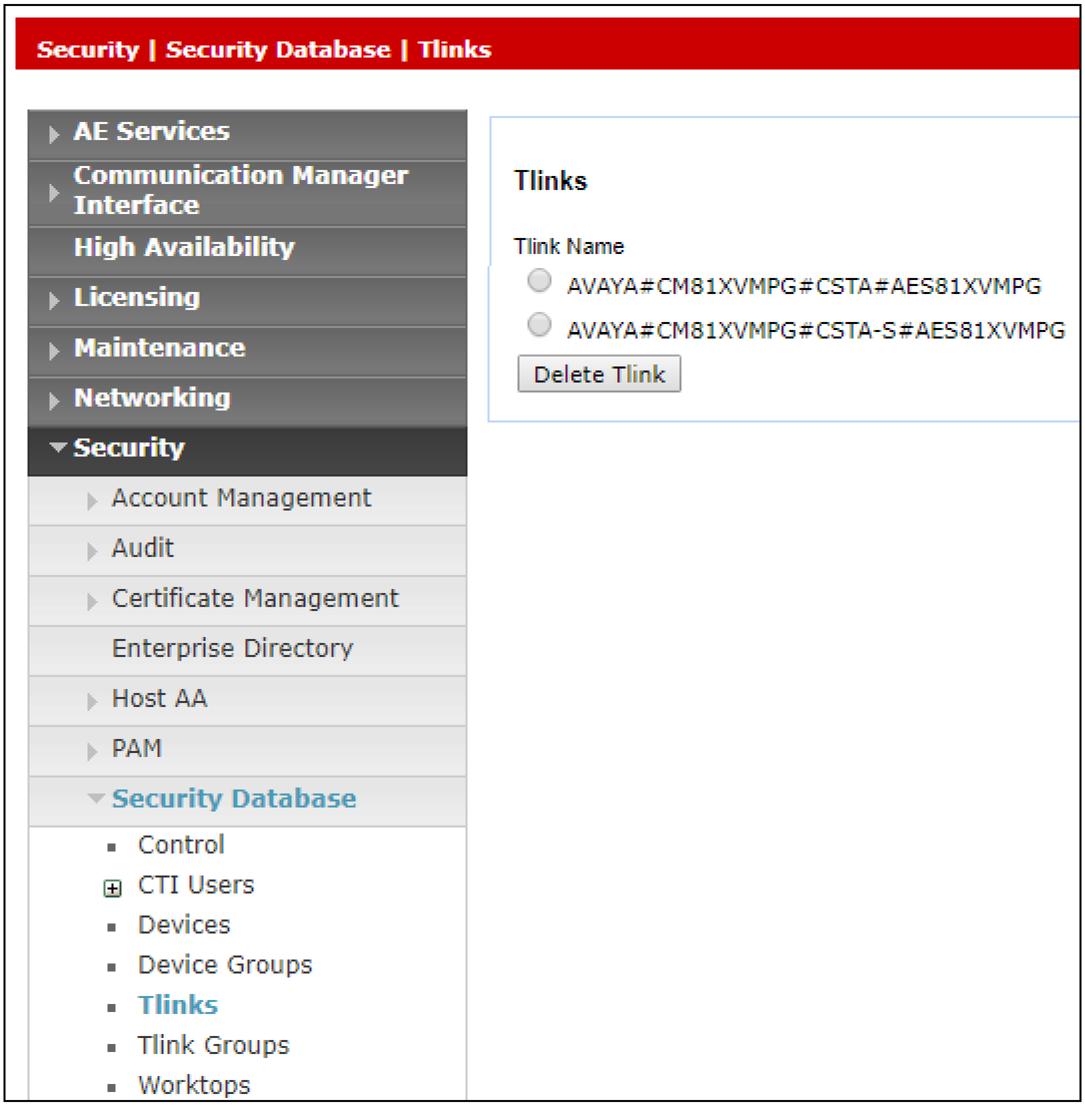
The **Edit CTI User** screen appears. Check the **Unrestricted Access** box and **Apply Changes** at the bottom of the screen.



A screen (not shown) appears to confirm applied changes to CTI User, choose **Apply**. This CTI user should now be enabled.

6.5. Identify Tlinks

Navigate to **Security → Security Database → Tlinks**. Verify the value of the **Tlink Name**. This will be needed to configure Altitude Xperience Engagement in **Section 8.1.1**. The first Tlink (unencrypted) is used.

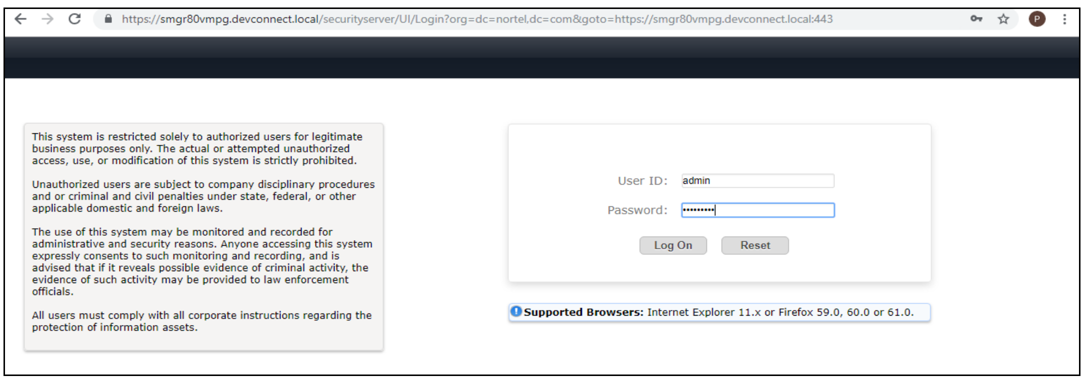


7. Configure Avaya Aura® Session Manager

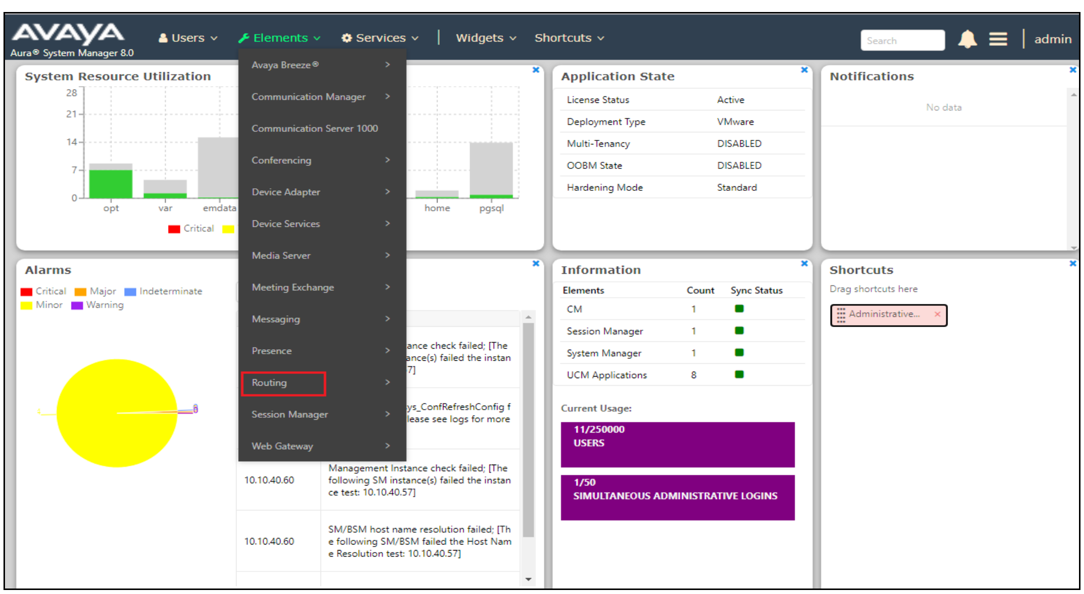
This section provides the procedures for configuring Session Manager to allow Altitude ACS to connect via SIP trunks to pass SIP calls between the ACS and Communication Manager. Session Manager is configured via System Manager. The procedure includes the following.

- 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** highlighted below.

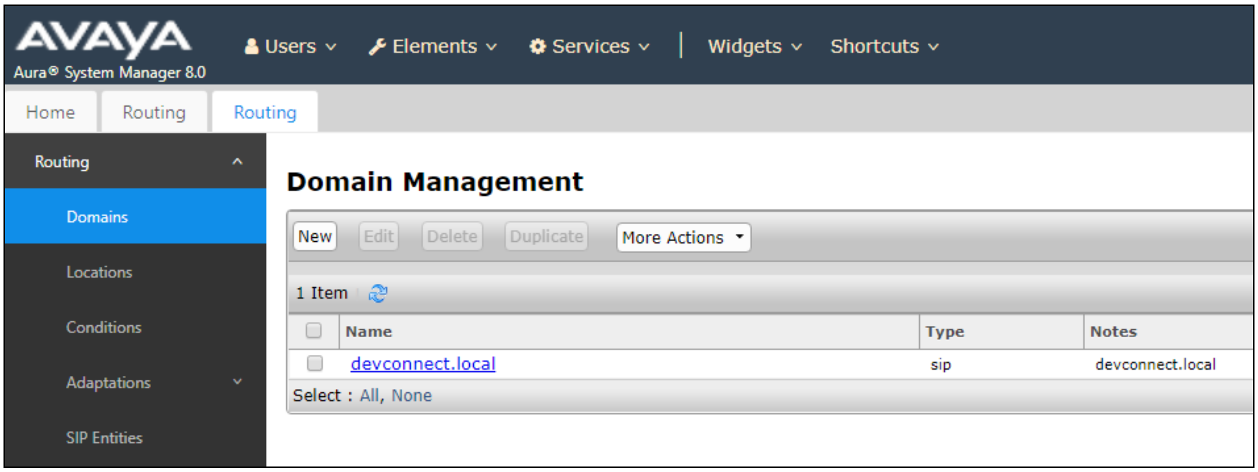


7.1. Domains and Locations

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.

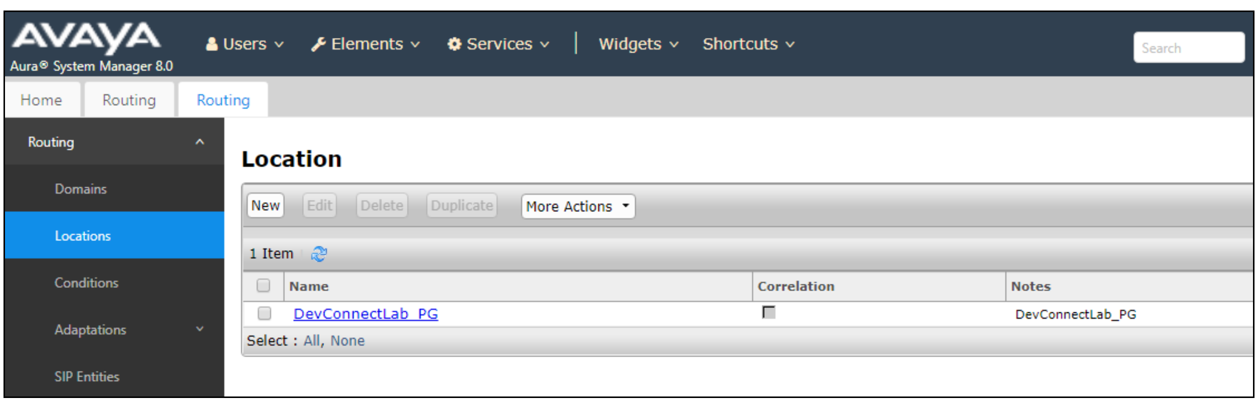
7.1.1. Display the Domain

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.



7.1.2. Display the Location

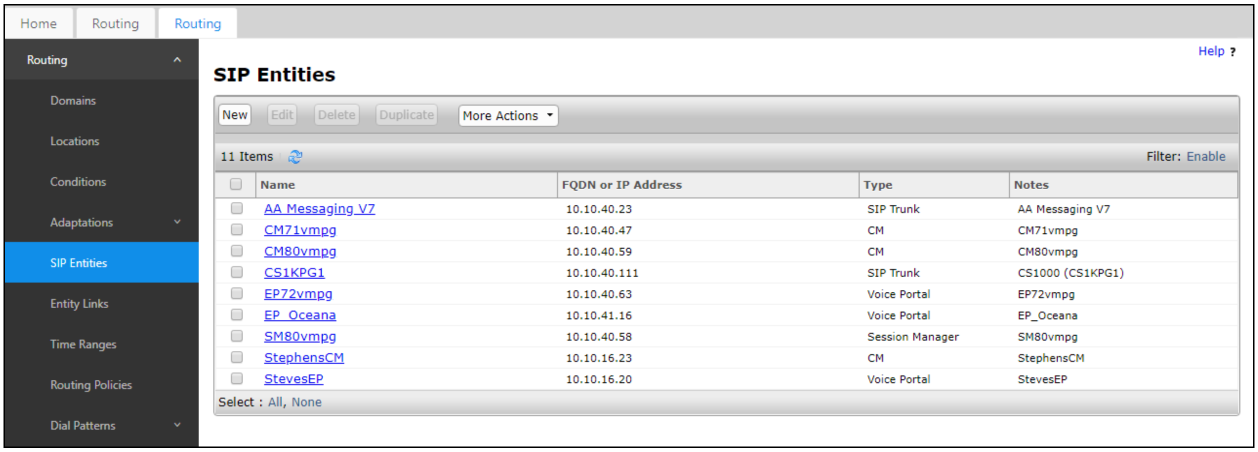
Select **Locations** from the left window and this will display the location setup. The example below shows the location **DevConnectLab_PG** which was used for compliance testing. If a location is not already in place, then one must be added to include the IP address range of the Avaya solution. Click on **New** to add a new location.



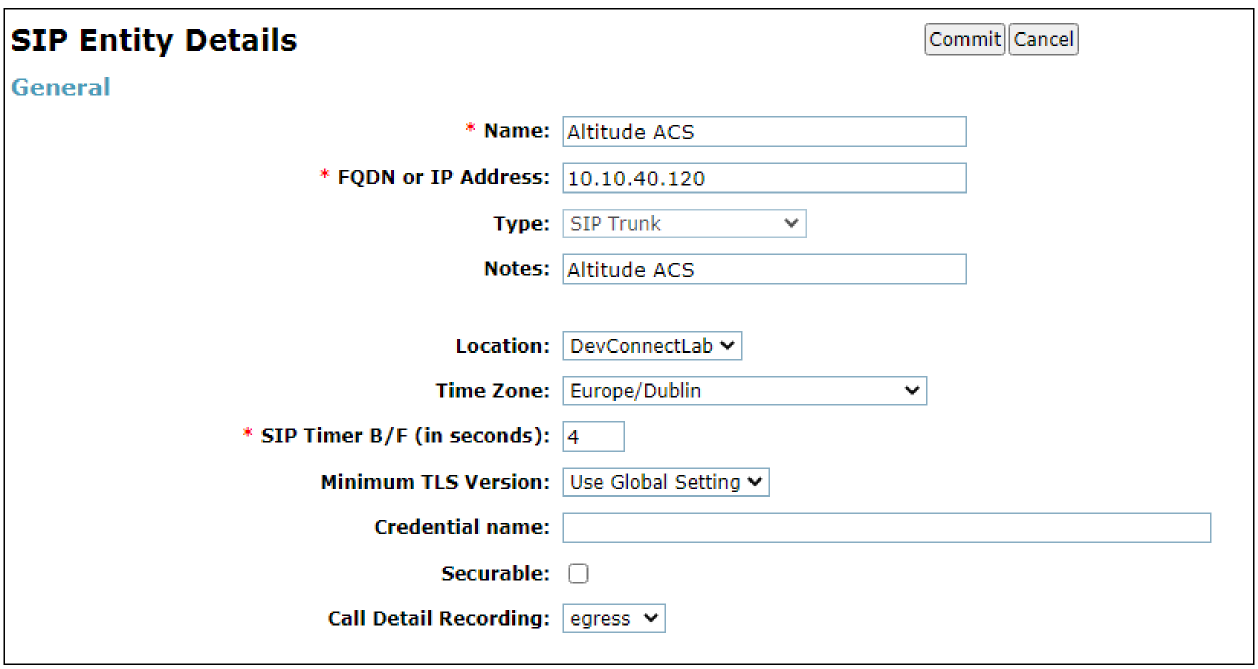
7.2. Configure Altitude ACS SIP Entity

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.



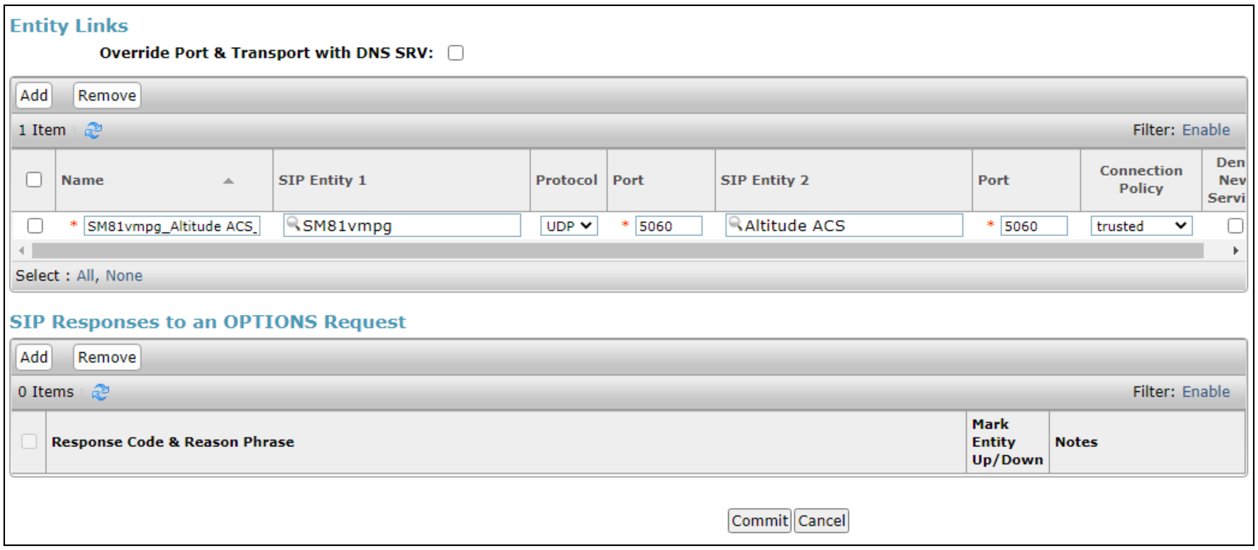
Enter a suitable **Name** for the new SIP Entity and the **IP Address** of the ACS server. Enter the correct **Time Zone** and **Location** and scroll down to SIP Entity Links.



7.3. Configure Altitude ACS SIP Entity Link

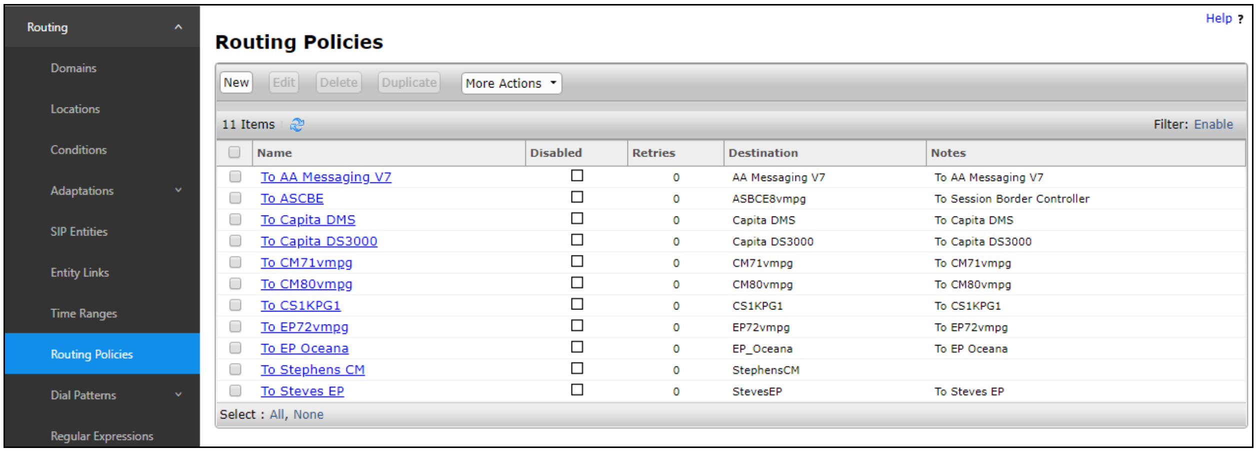
An Entity link can be added from the SIP Entities page. Using the page from the previous page scroll down to Entity Links.

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 ACS 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.

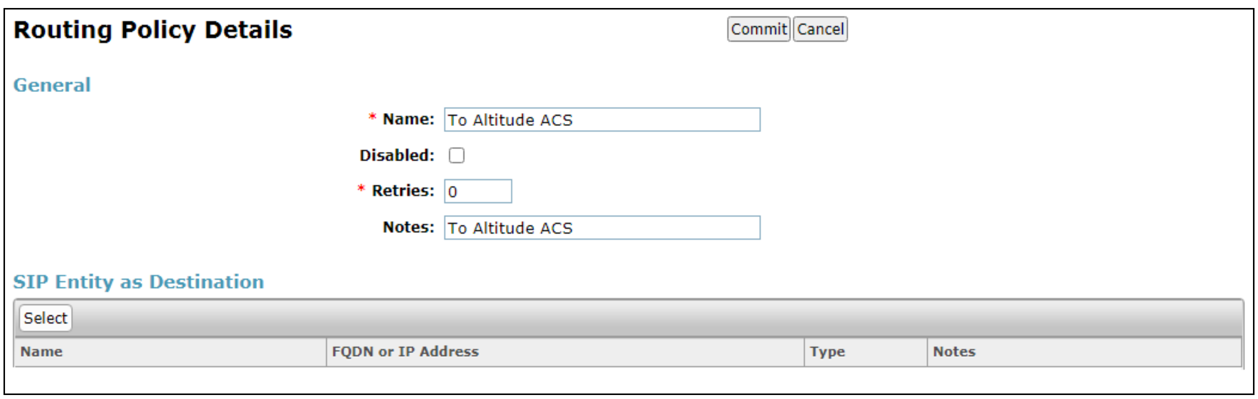


7.4. Configure Routing Policy for Altitude ACS

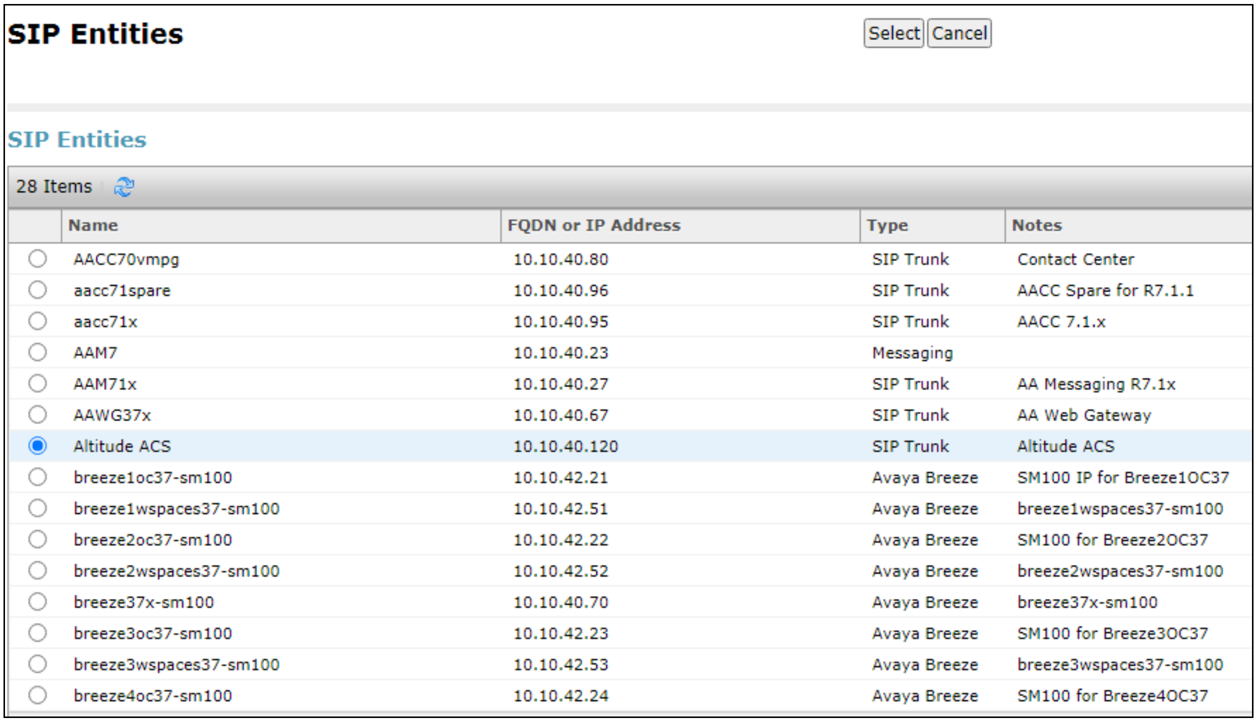
Click on **Routing Policies** in the left window and select **New** in the main window.



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



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



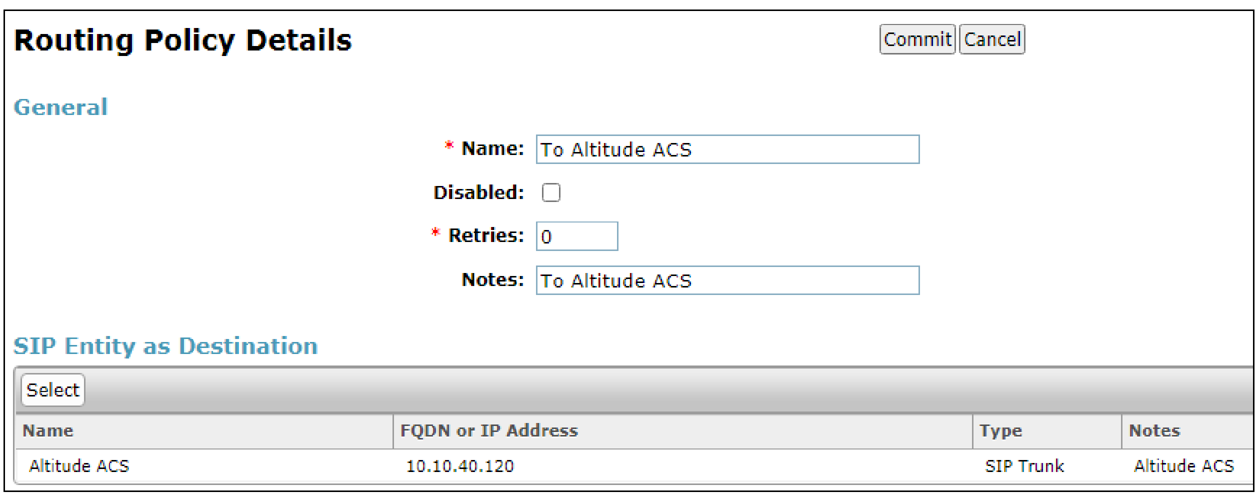
SIP Entities Select Cancel

SIP Entities

28 Items

	Name	FQDN or IP Address	Type	Notes
○	AACC70vmpg	10.10.40.80	SIP Trunk	Contact Center
○	aacc71spare	10.10.40.96	SIP Trunk	AACC Spare for R7.1.1
○	aacc71x	10.10.40.95	SIP Trunk	AACC 7.1.x
○	AAM7	10.10.40.23	Messaging	
○	AAM71x	10.10.40.27	SIP Trunk	AA Messaging R7.1x
○	AAWG37x	10.10.40.67	SIP Trunk	AA Web Gateway
●	Altitude ACS	10.10.40.120	SIP Trunk	Altitude ACS
○	breeze1oc37-sm100	10.10.42.21	Avaya Breeze	SM100 IP for Breeze1OC37
○	breeze1wspaces37-sm100	10.10.42.51	Avaya Breeze	breeze1wspaces37-sm100
○	breeze2oc37-sm100	10.10.42.22	Avaya Breeze	SM100 for Breeze2OC37
○	breeze2wspaces37-sm100	10.10.42.52	Avaya Breeze	breeze2wspaces37-sm100
○	breeze37x-sm100	10.10.40.70	Avaya Breeze	breeze37x-sm100
○	breeze3oc37-sm100	10.10.42.23	Avaya Breeze	SM100 for Breeze3OC37
○	breeze3wspaces37-sm100	10.10.42.53	Avaya Breeze	breeze3wspaces37-sm100
○	breeze4oc37-sm100	10.10.42.24	Avaya Breeze	SM100 for Breeze4OC37

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



Routing Policy Details Commit Cancel

General

* **Name:** To Altitude ACS

Disabled: ☐

* **Retries:** 0

Notes: To Altitude ACS

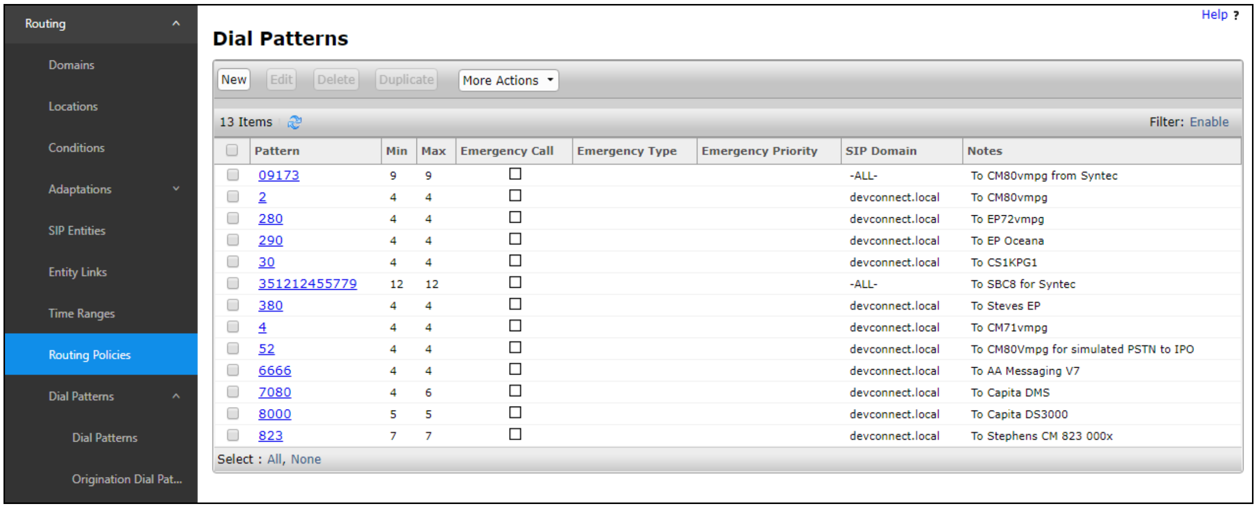
SIP Entity as Destination

Select

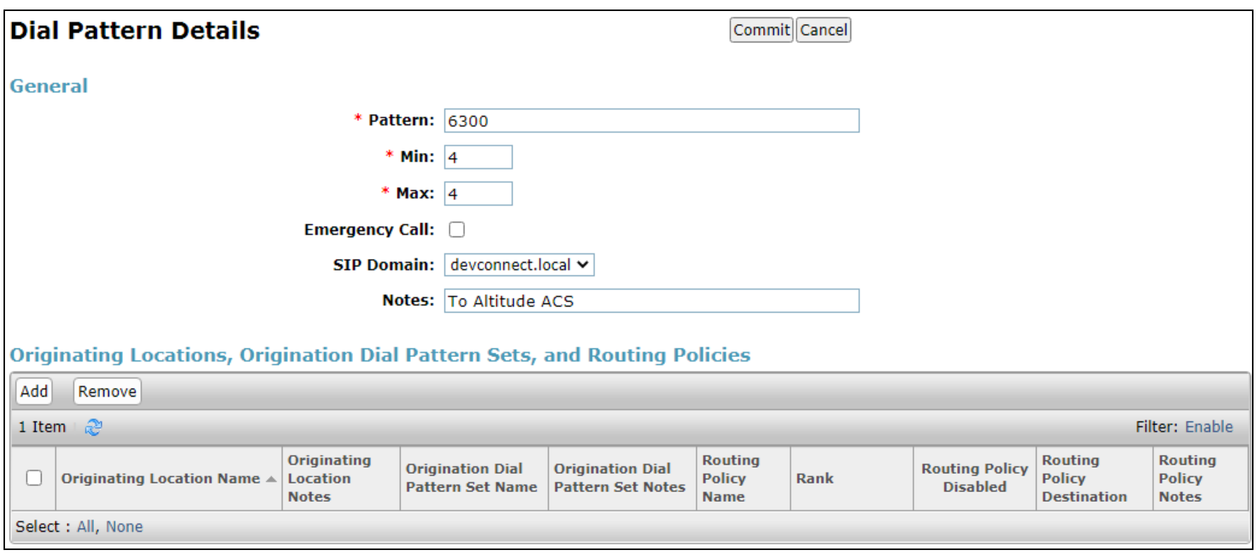
Name	FQDN or IP Address	Type	Notes
Altitude ACS	10.10.40.120	SIP Trunk	Altitude ACS

7.5. Configure Altitude ACS Dial Patterns

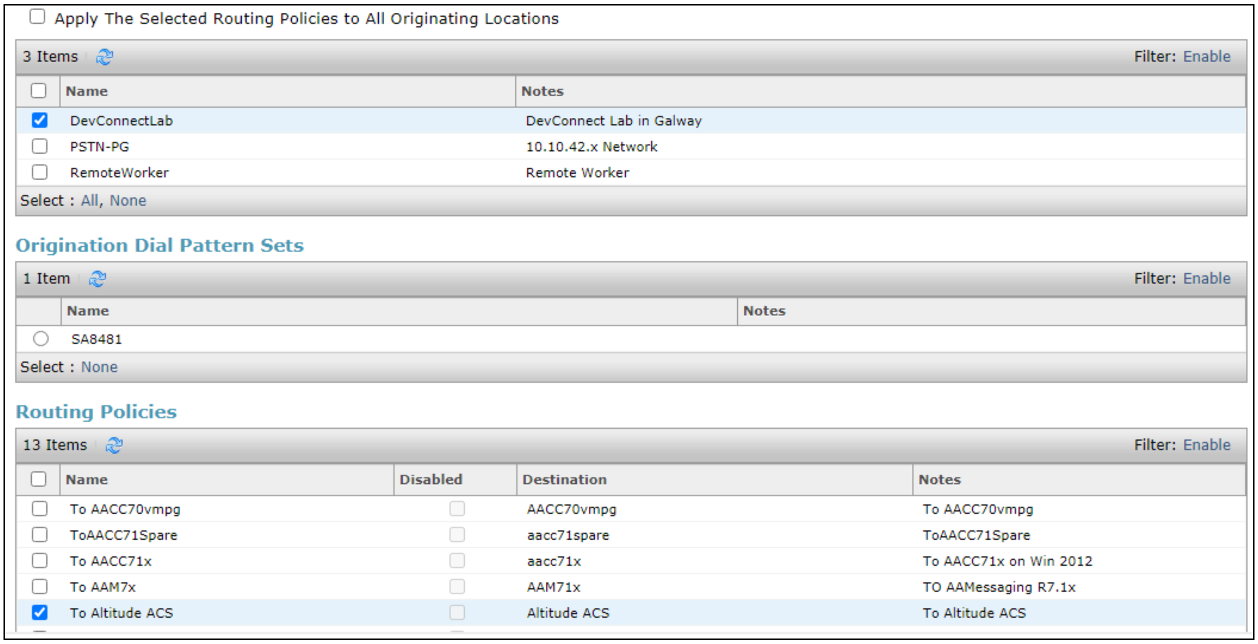
Select **Dial Patterns** in the left window and select **New** in the main window.



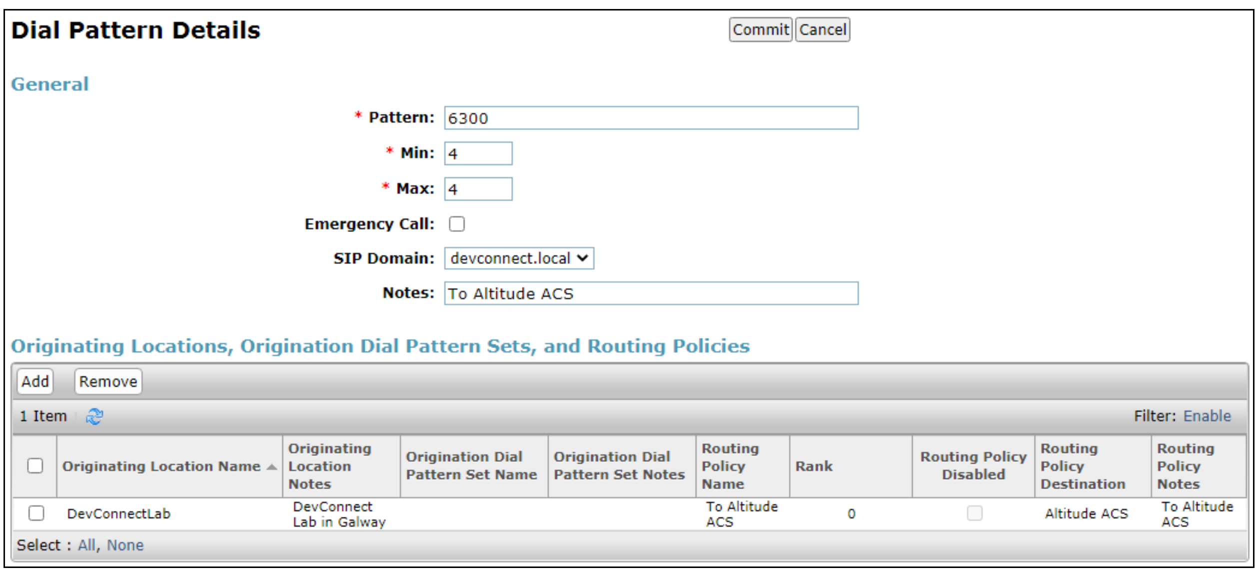
Enter the required digits for the Routing Pattern, in the example below **6300** is used. This ensures that when 6300 is dialled it will route to the ACS server. Enter the appropriate domain for **SIP Domain** in this example the domain created in **Section 7.1.1** is added. Click on **Add** under **Originating Locations and Routing Policies** to select this Routing Policy.



Select the **Originating Location**, this will be the location added in **Section 7.1.2** select the newly created Routing Policy for ACS.



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



8. Configure Altitude Xperience Engagement

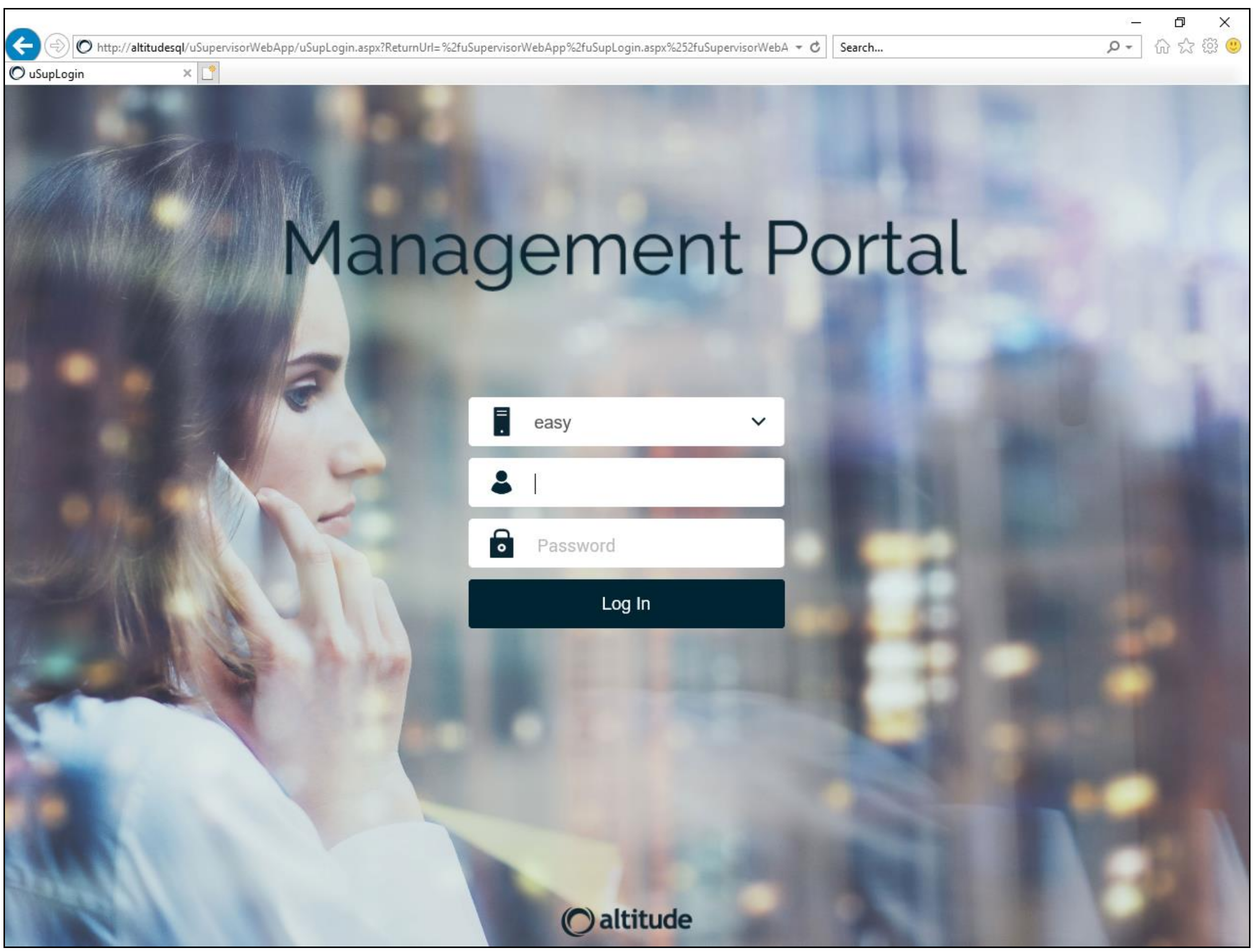
There are two modules to be configured, the Altitude Xperience Engagement server connecting to Application Enablement Services and the Altitude Communication Server (ACS) connecting to Session Manager.

8.1. Configure Altitude Xperience Engagement Server

Note: Windows Internet Explorer R9.0, R10.0 and R11.0, and Firefox 35 or above are the only supported browsers with this release of Altitude Xperience Engagement. Windows Internet Explorer R11.0 was used during compliance testing.

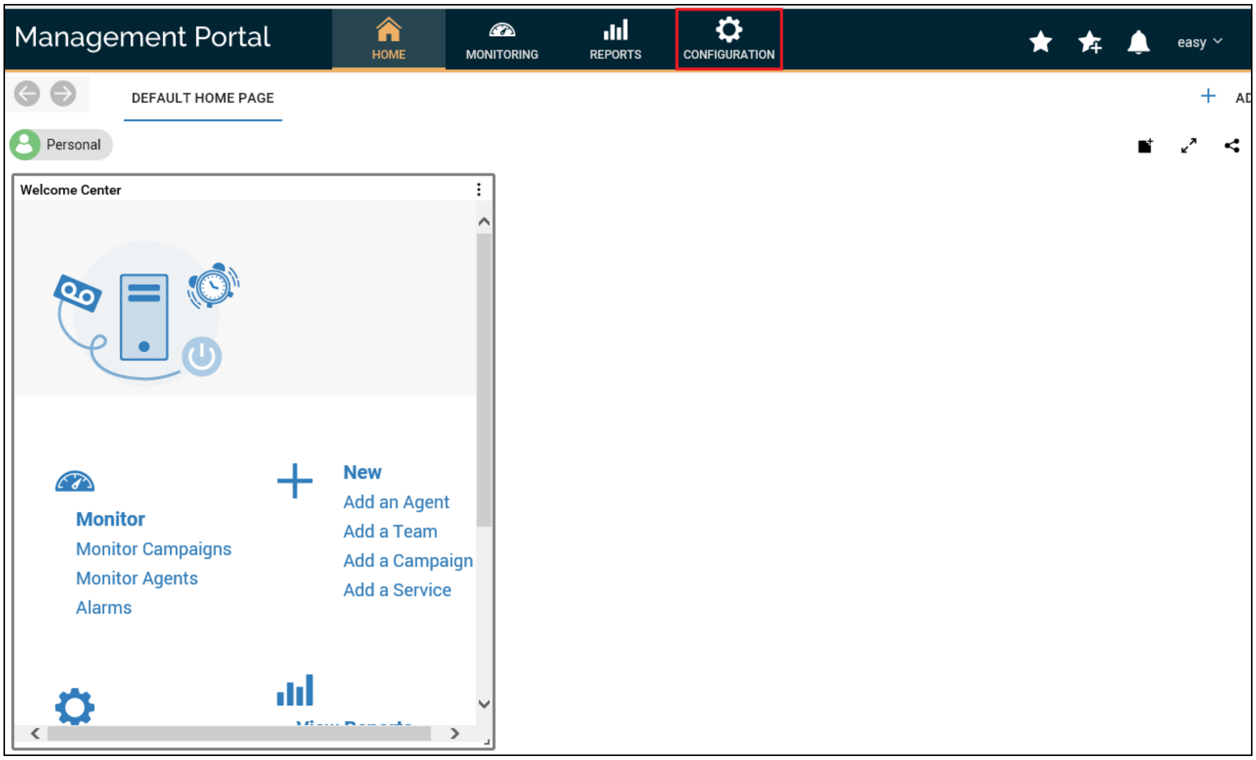
Note: These Application Notes serve as a guide showing the setup present for compliance testing. Therefore, the following sections will highlight the existing setup for both connections to Application Enablement Services and Session Manager and will not illustrate the creation of new connections to both.

Open a web session to **http://<server IP Address>/uSupervisorWebApp**. Enter the appropriate credentials and click on **Log In**.

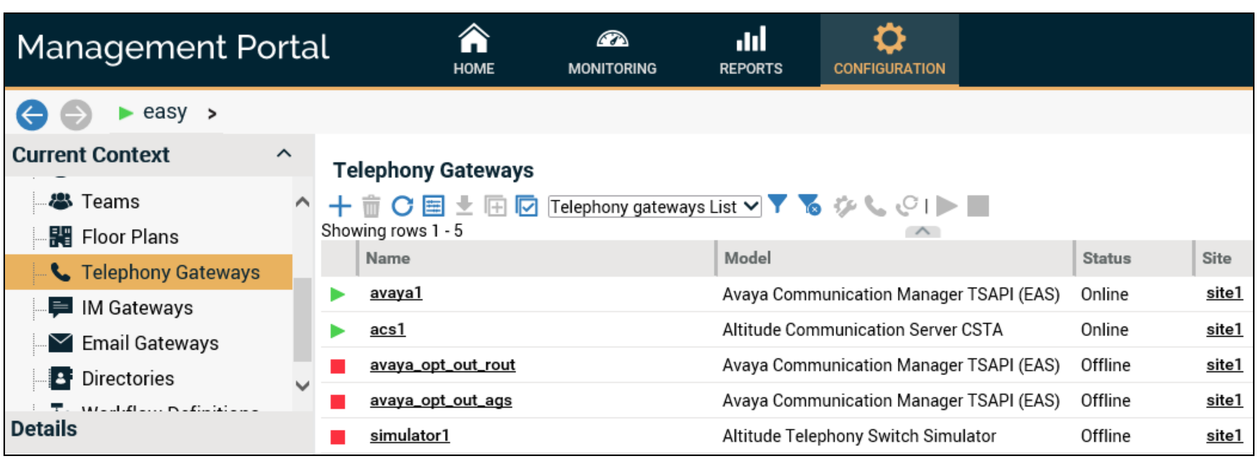


8.1.1. Configure Telephony Gateway

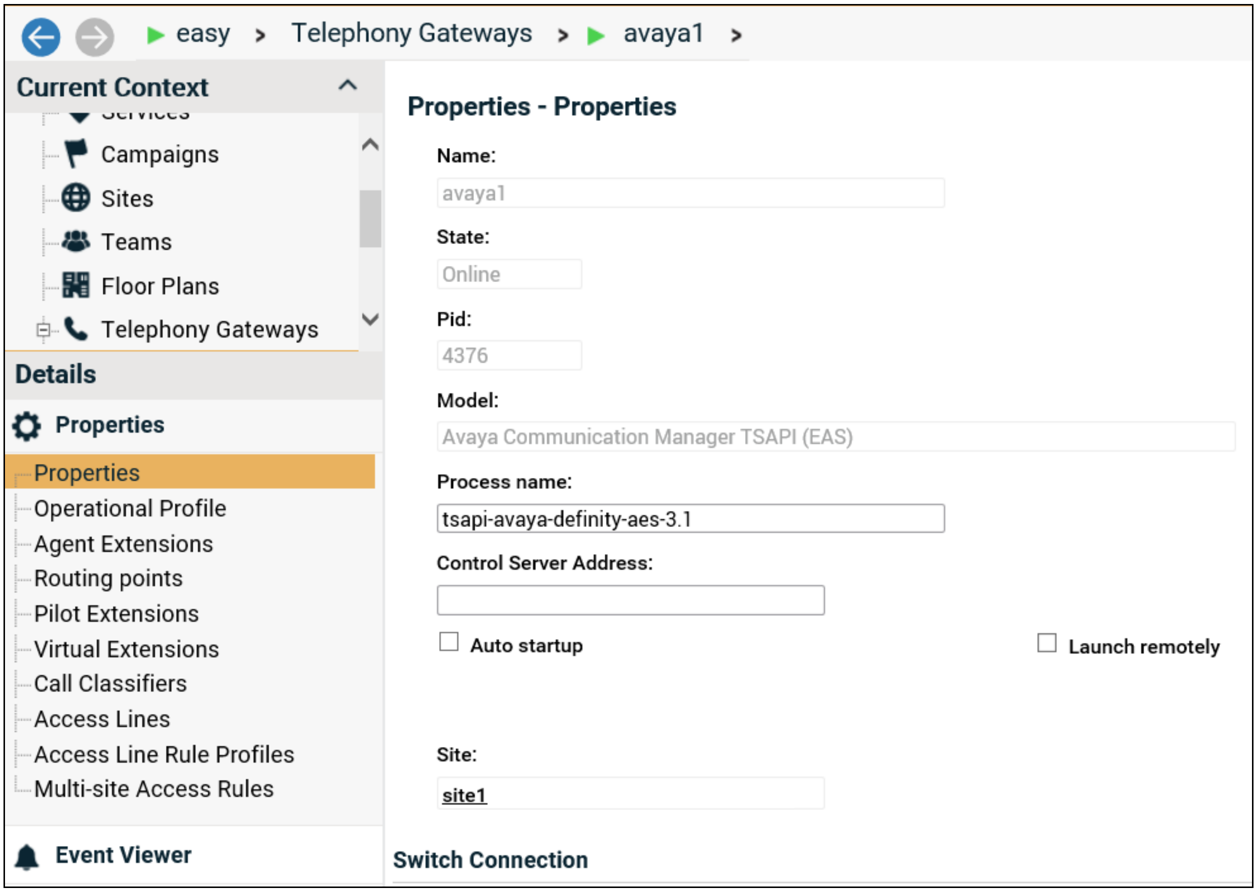
Once logged in select **Configuration** as highlighted below.



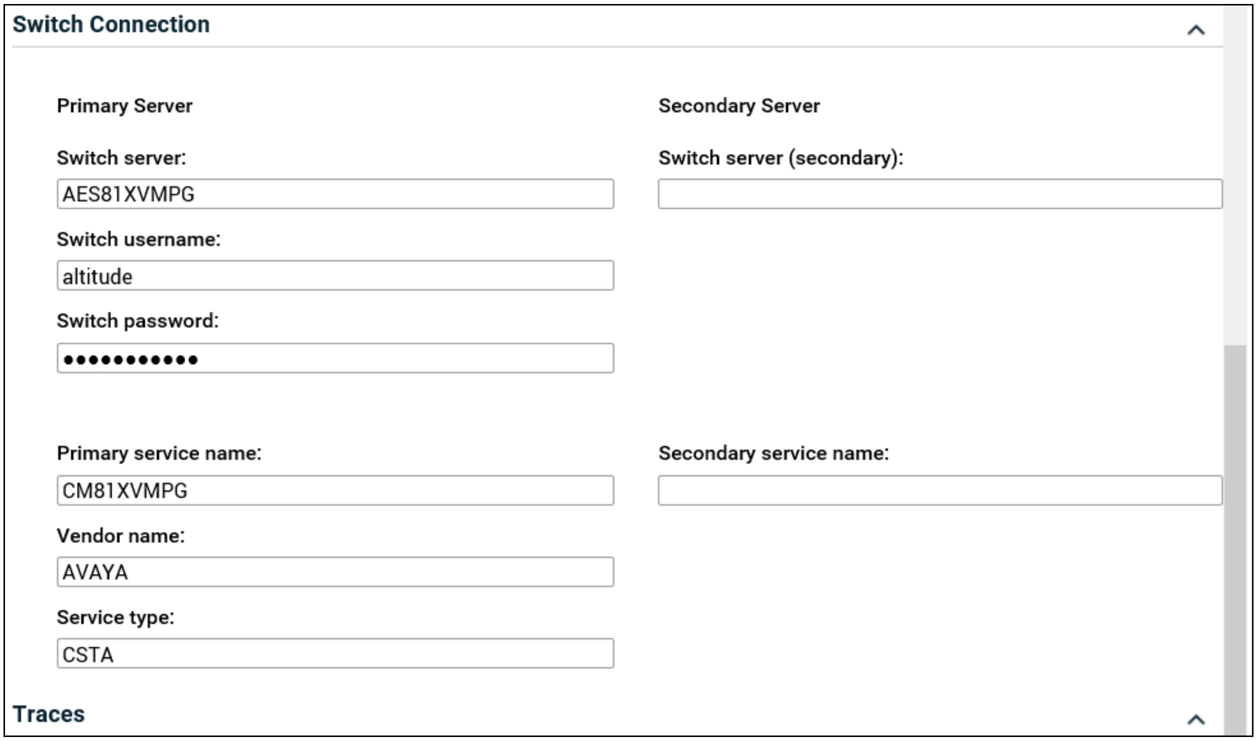
Expand **Current Context** in the left window and select **Telephony Gateways**. A new gateway can be created by clicking on the **+** icon. There are two existing gateways present, one for the TSAPI connection to Application Enablement Services and the other is for the connection to Altitude Communication Server, which for these tests, has a SIP trunk configured to connect to Session Manager. This section shows the TSAPI connection to Application Enablement Services, clicking on **avaya1** below will open this connection. These Application Notes will highlight the important areas of this existing gateway.



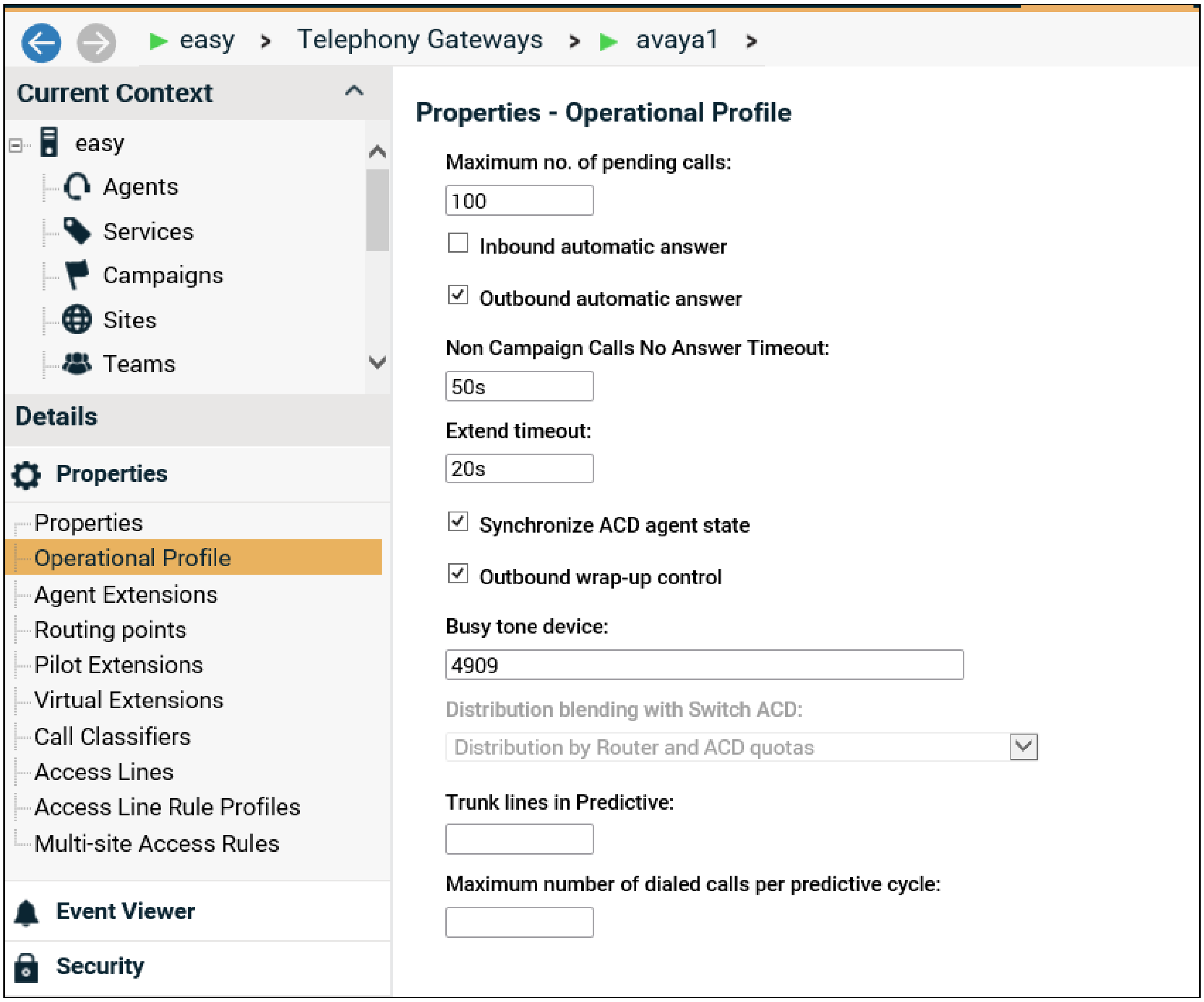
A **Name** for the gateway is mandatory in this case avaya1 was chosen. The **Avaya Communication Manager TSAPI (EAS)** is selected as the **Model** from the drop-down menu.



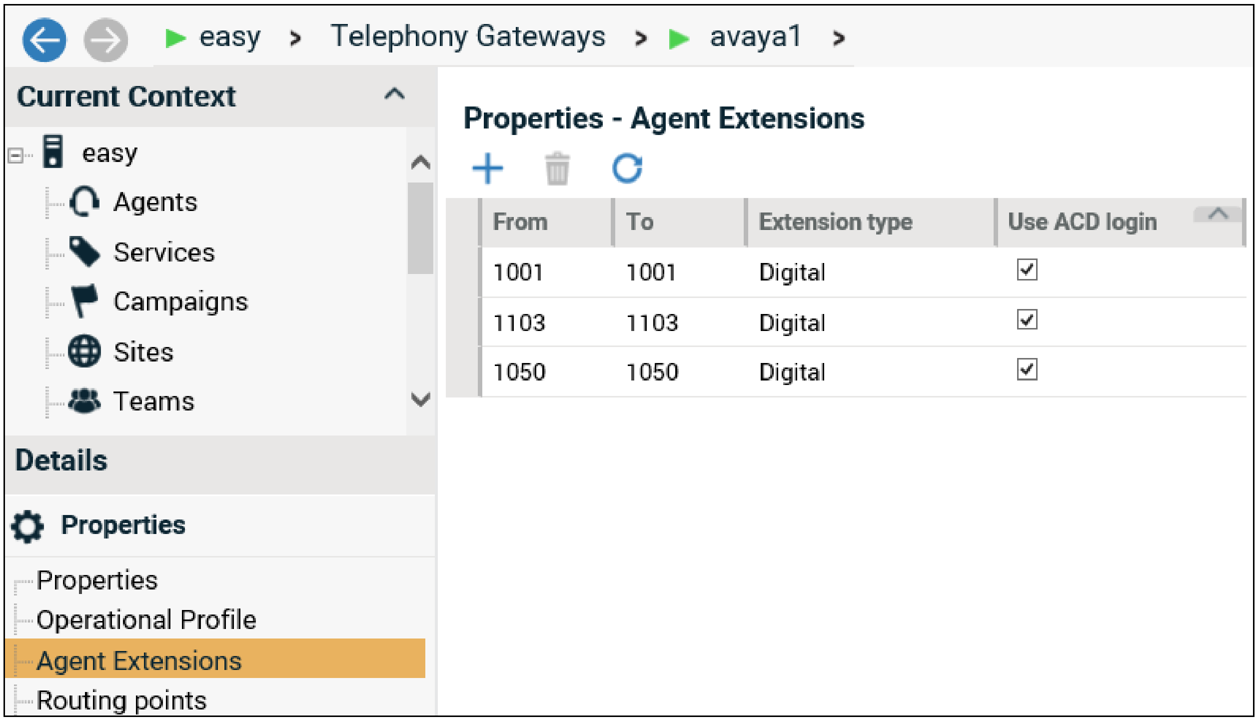
Scroll down to **Switch Connection** and here the information as shown below, is used to connect to Application Enablement Services and can be obtained from the Application Enablement Services Tlink information shown in **Section 6.5**.



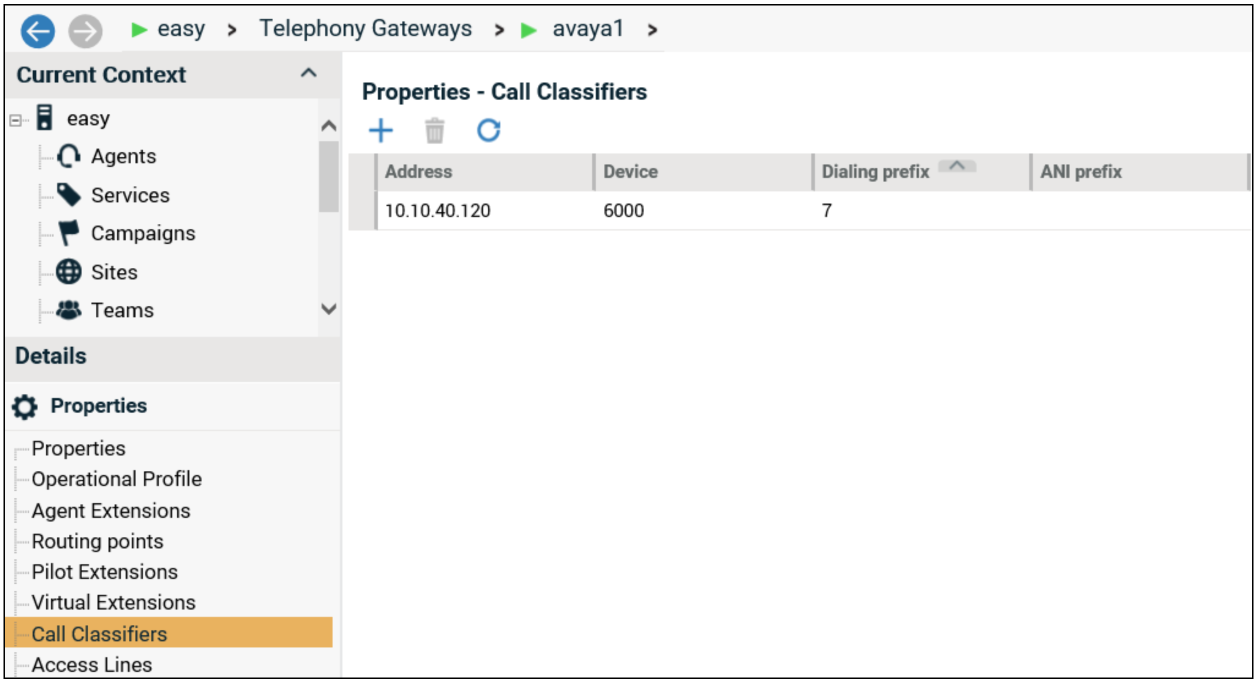
Clicking on **Operational Profile** in the left window shows the **Busy tone device** information and this is the “busy tone” VDN that is created (see **Appendix**).



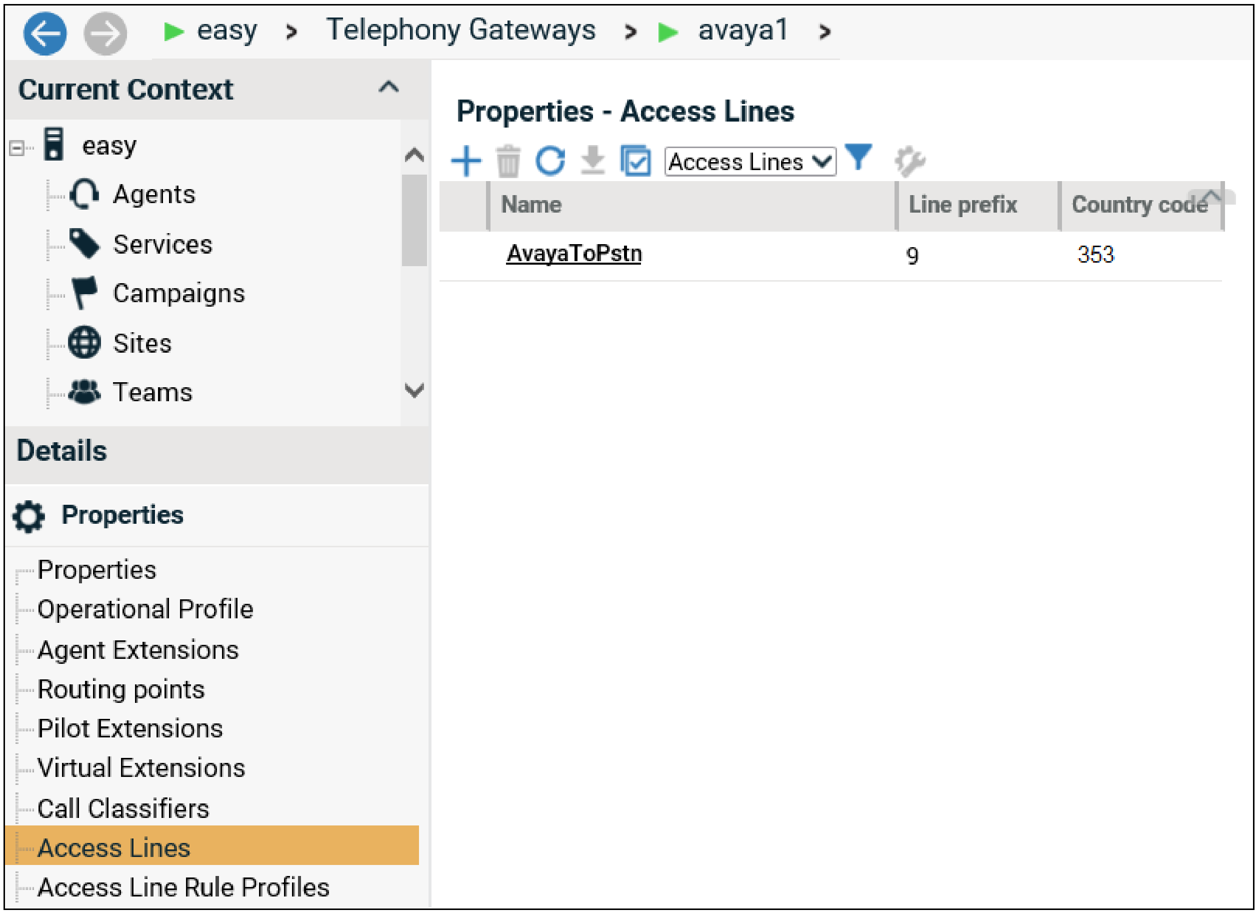
Clicking on **Agent Extensions** in the left window, shows the agents available for use. Adding another agent can be done by clicking on the + icon.



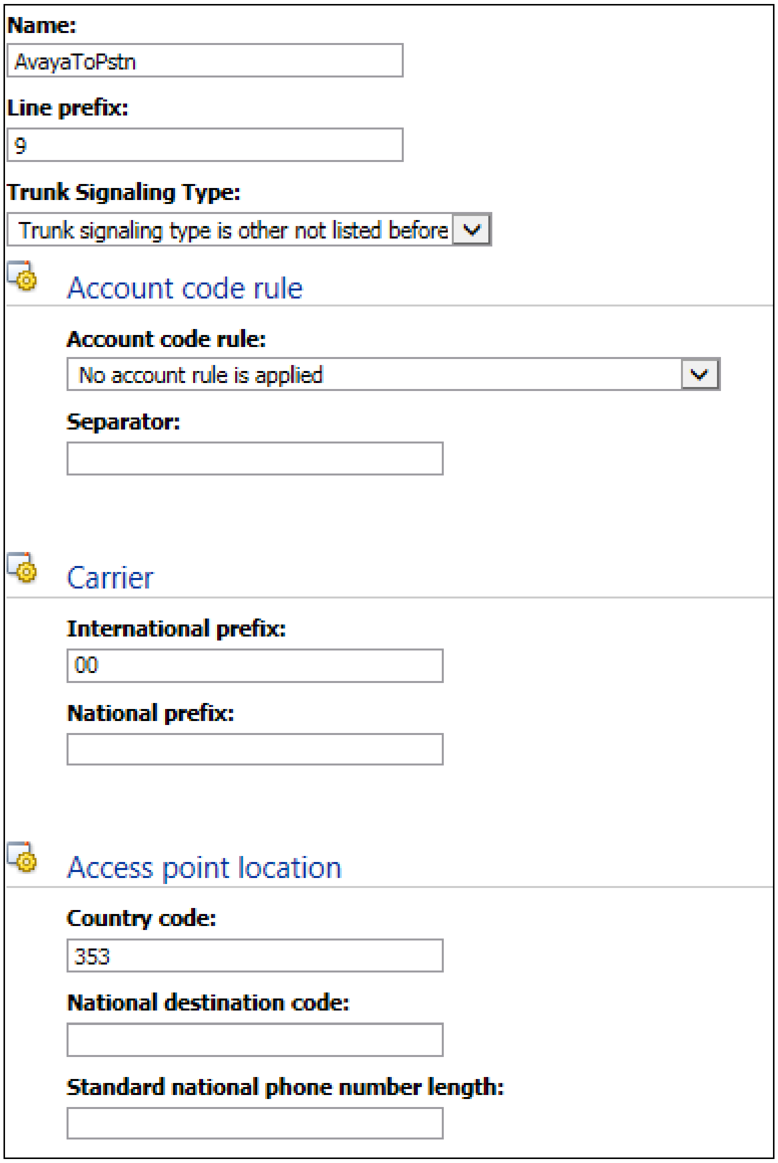
Clicking on **Call Classifiers** in the left window shows the information on Call Classifiers. A call classifier was setup for outbound campaigns for predictive dialing. To add a new Call Classifier, select the **+** icon and enter the IP Address of the Altitude Communication Server (ACS) in this case it will be the same as the Altitude Assisted Server and the **Device** is the number that was created in the Communication Server in **Section 8.2.4**. The **Dialing prefix** is the number used to transfer the calls to the Agents after call classification in **Section 8.2.6**.



Select **Access Lines** from the **Properties** window as shown. From the main window a new access line can be added by clicking on the + icon.

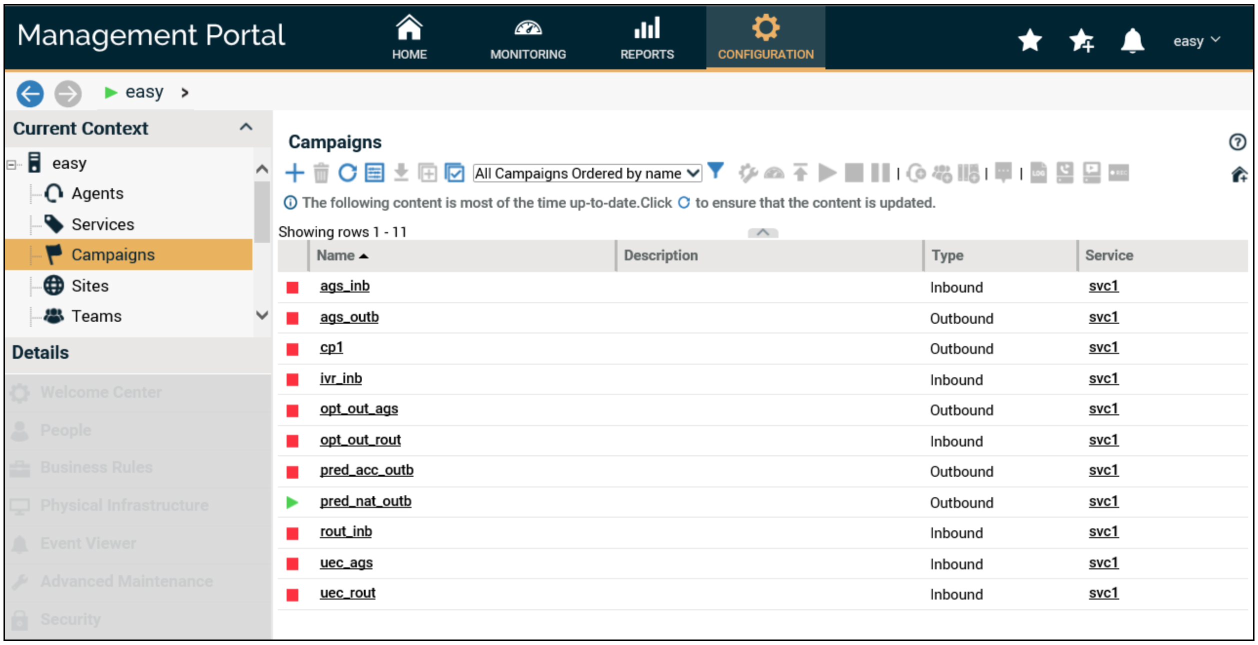


The **Line Prefix** should be set to the Avaya Communication Manager Auto Route Selection (ARS) - Access Code 1 Feature Access Code configured in **Section 5.1.2**. The **Trunk Signaling Type** should be set as shown and the appropriate International and National prefixes, and Country code entered.



8.1.2. Configuring Campaigns

Select **Campaigns** from the left window. The main window displays all the campaigns that were setup for compliance testing, these include a mixture of Inbound, Outbound and Blended scenarios.

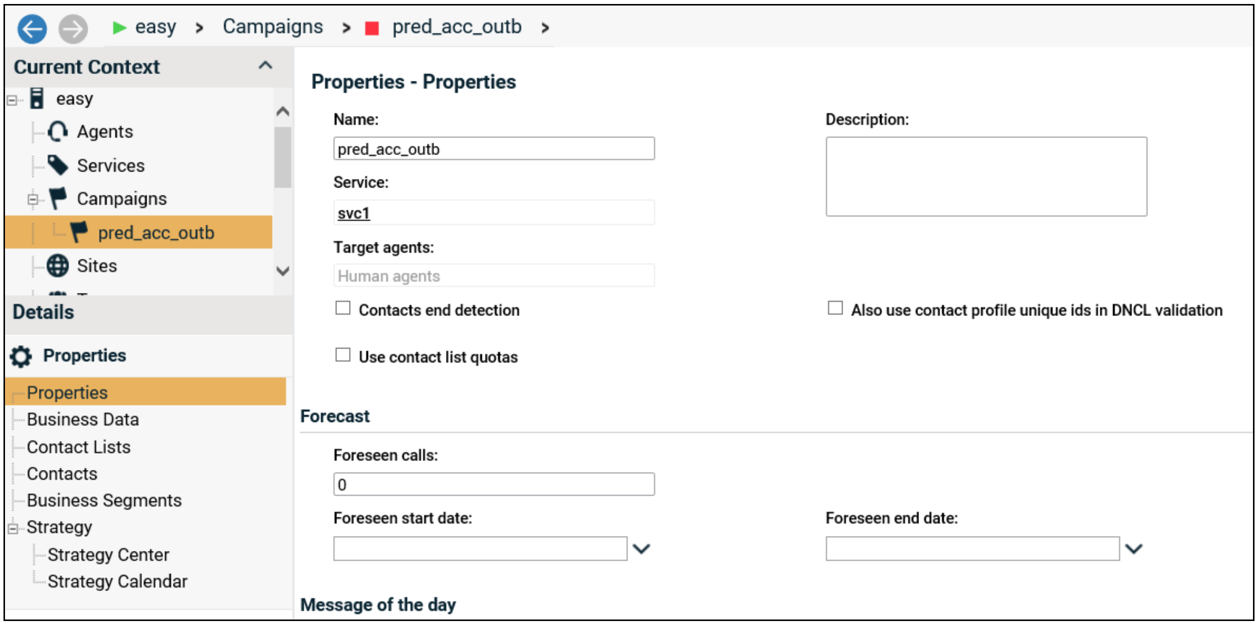


Note: The correct transfer of the customer number to Avaya Call Manager requires using a special configuration option in Altitude Xperience Engagement Server; the following line should be added into AssistedServer.config.

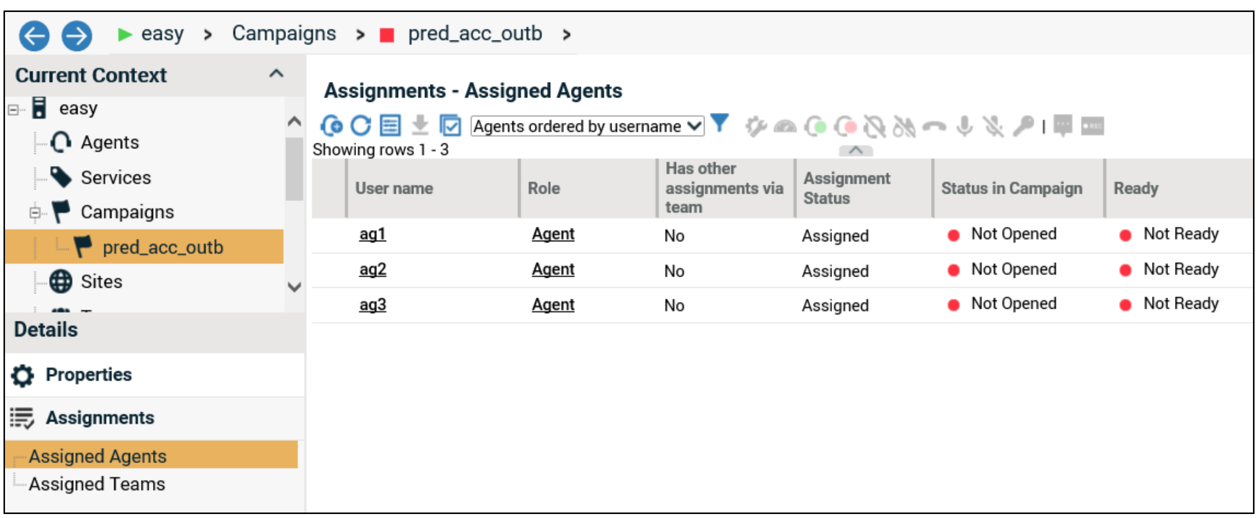
<avaya1_USE_DATA_FORGED_ANI>1</avaya1_USE_DATA_FORGED_ANI>

The following shows the configuration of "Predictive Outbound Dialing using Altitude Call Classifier". In this scenario predictive calls are dialed by Altitude Call Classifier device in Altitude Communication Server to the PSTN via the SIP trunk, then after being successfully classified and answered by a person they are transferred to the Avaya agent.

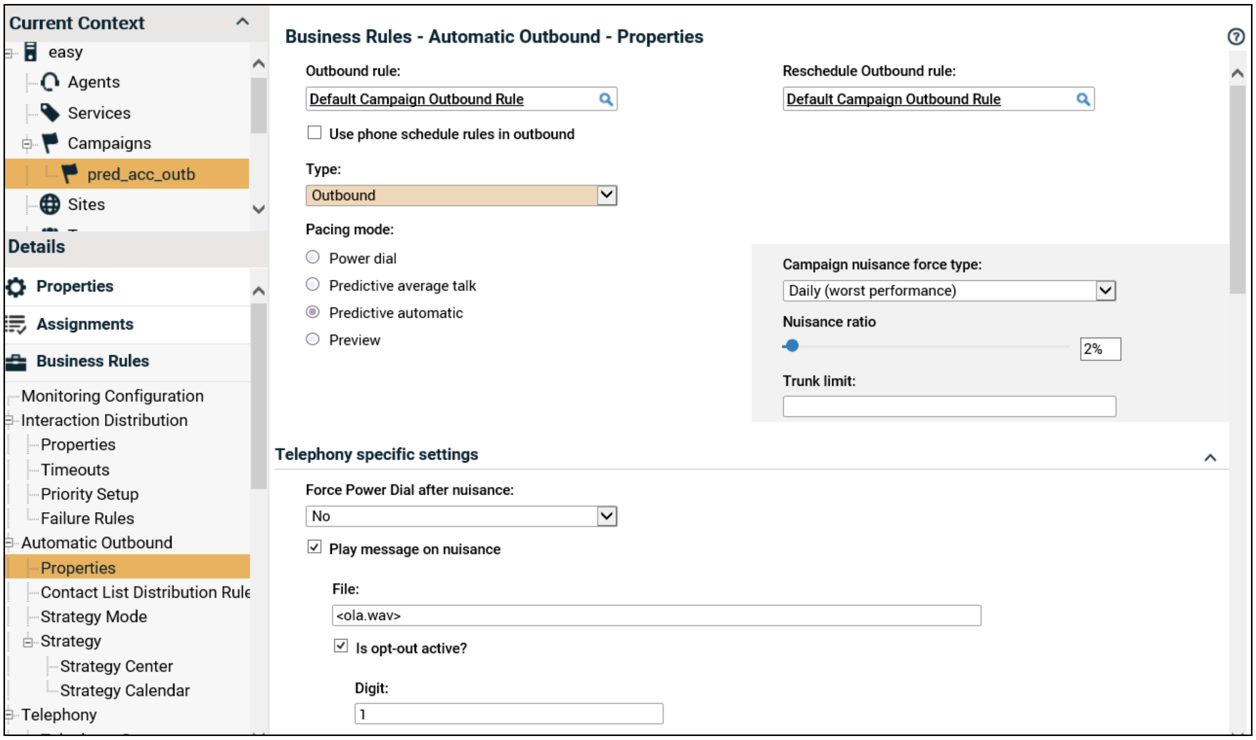
A suitable **Name** is given, and a **Service** is already present.



Click on **Assigned Agents** in the left window, where agents can be assigned to this campaign. The following shows the three agents already assigned and now



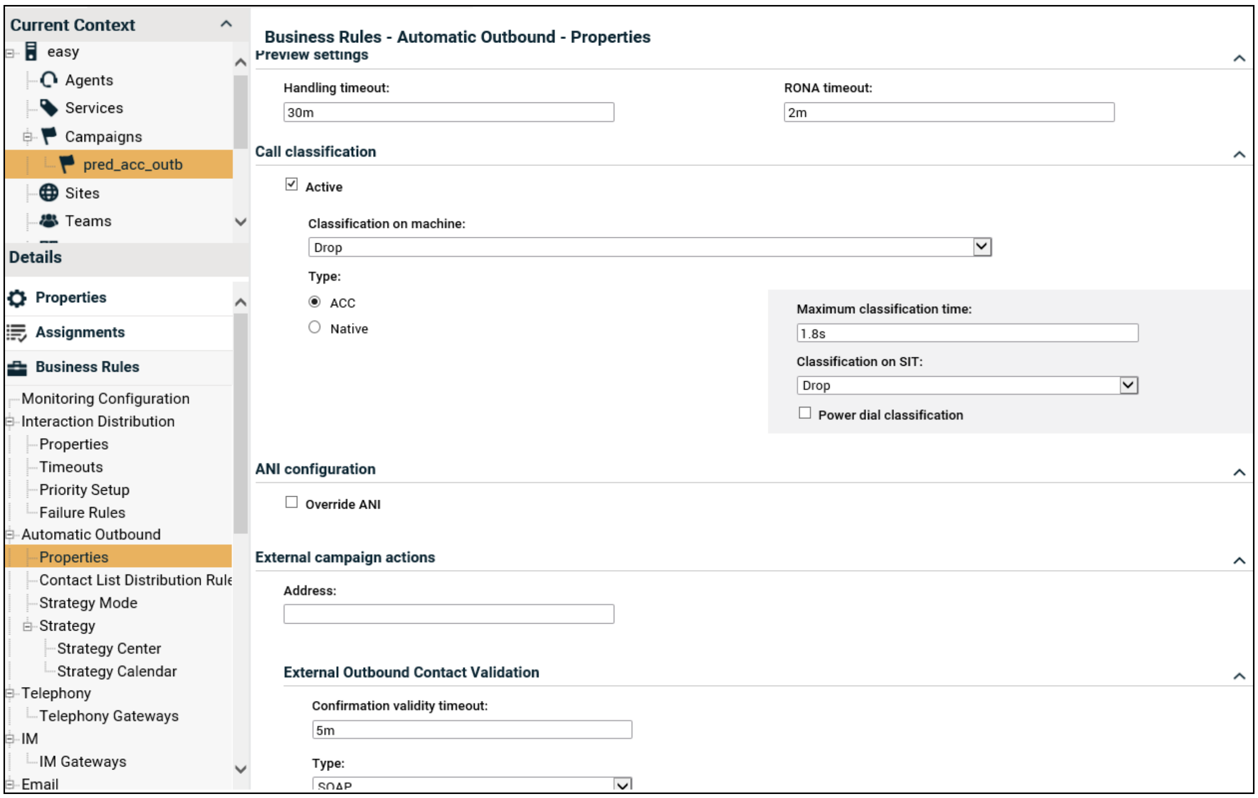
The **Type** should be set to **Outbound** and the **Pacing mode** to **Predictive automatic**, the other fields can be left as default or as shown.



Scroll down and ensure that **Call Classification Active** is ticked and **ACC** (Altitude Call Classifier) is selected as shown below.

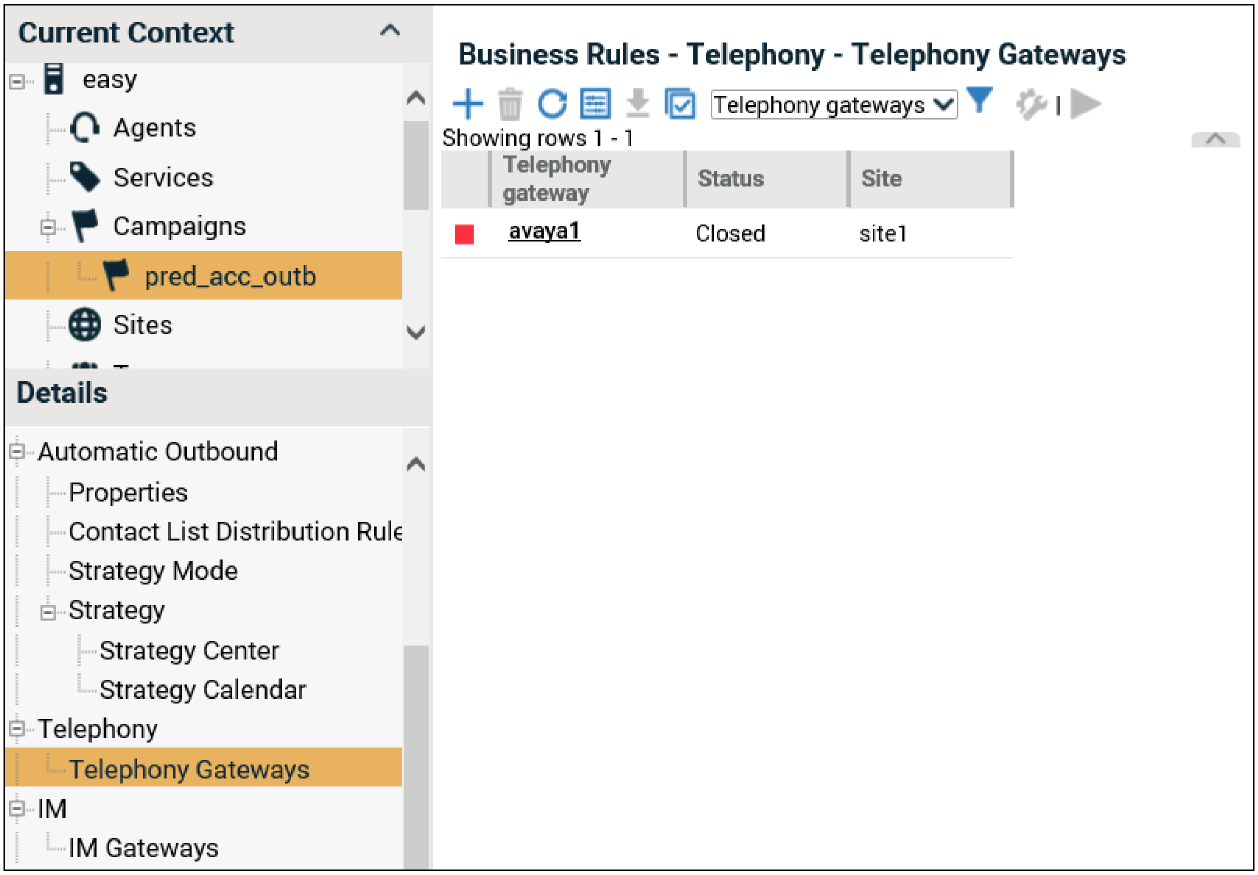
Note that Call Classification can be used on the Avaya Communication Manager by setting **Type** to **Native**, or on the Altitude Communication Server by setting **Type** to **ACC** as is shown.

Call Classification can be turned off by unticking the **Active** box that is currently ticked below. This may be required if an issue is found with outbound calls and SIP phones, as was outlined in **Section 2.2**.

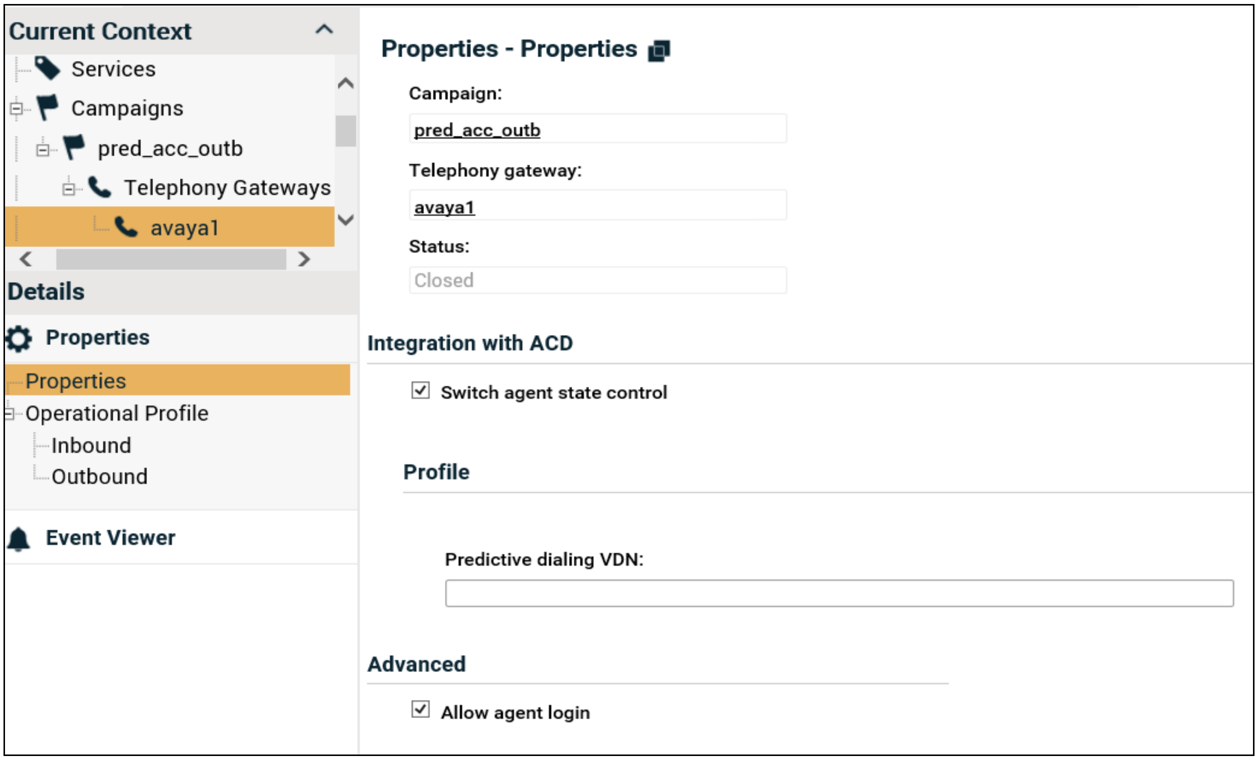


8.1.3. Configure Telephony Gateway in Campaign

Click on **Telephony → Telephony Gateways** in the left window. To add a new gateway, click on + icon. However, the existing gateway is shown and clicking on that.

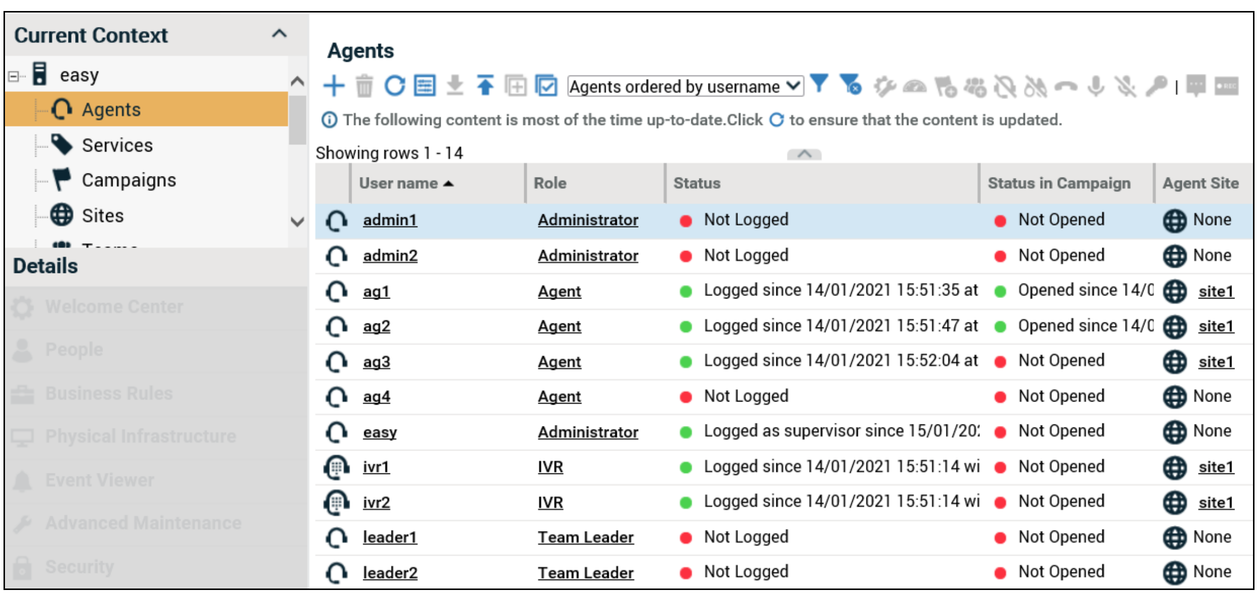


Assign the newly created telephony gateway to this campaign as shown in the screen below and ensure **that Switch agent state control** is **ticked** to allow wrap-up on calls coming to the VDN.

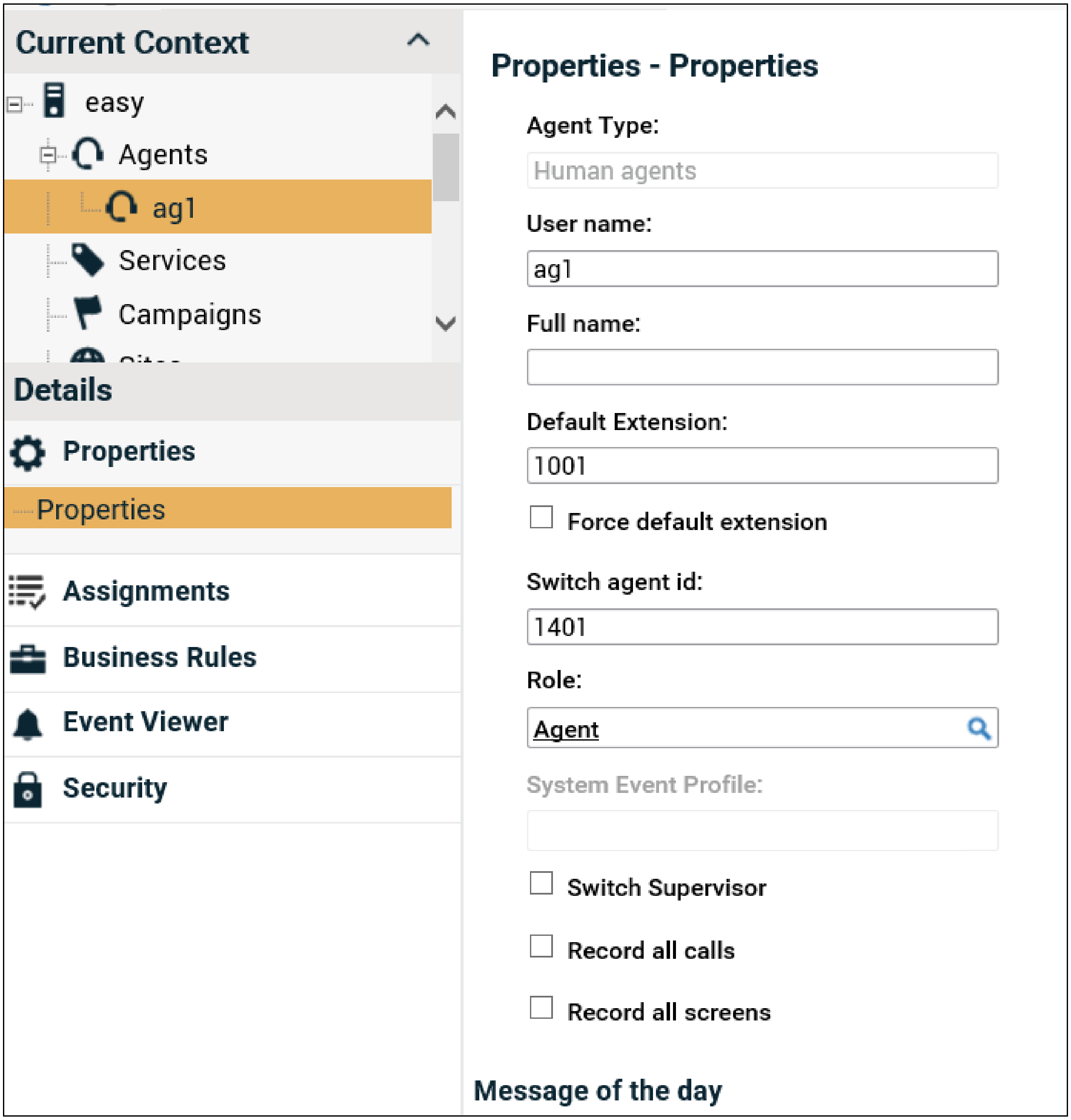


8.1.4. Adding Agents to Assisted Server

Navigate to **Agents** in the left window. In the main window is a list of agents that were configured for compliance testing, these include Human, IVR and Routing agents. To create a new agent, click on the **+** icon or click on an existing agent to view the details.

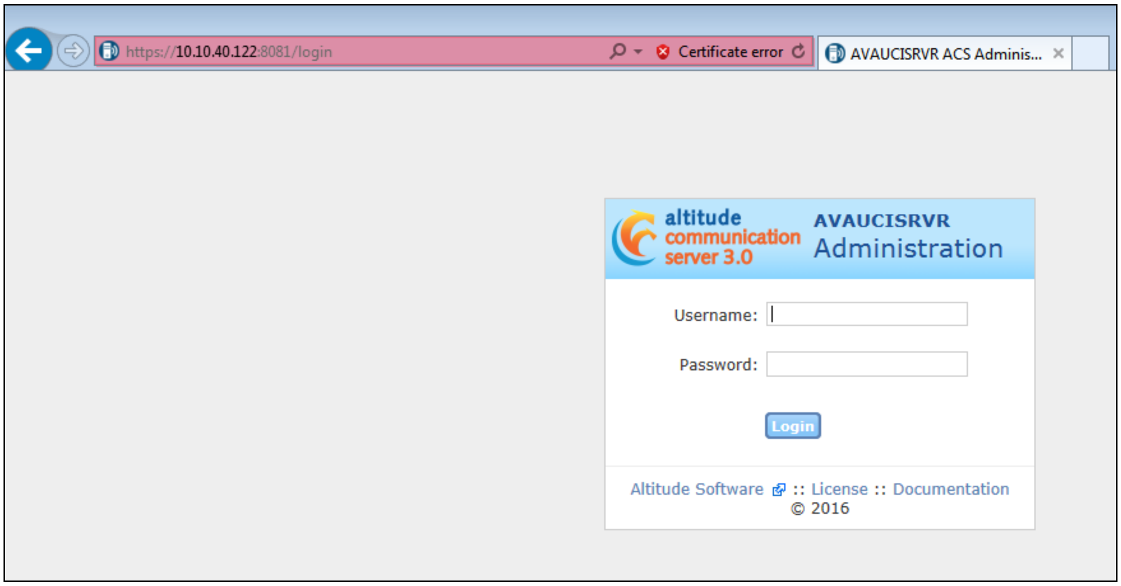


This example shows the creation of a human agent to log into an Avaya desk phone. Enter the suitable credentials noting the **Switch agent id** is **1401** as configured in **Section 5.2.4**. A **Default Extension** is added to avoid having to enter the same extension number when logging in as per **Section 5.2.5**.



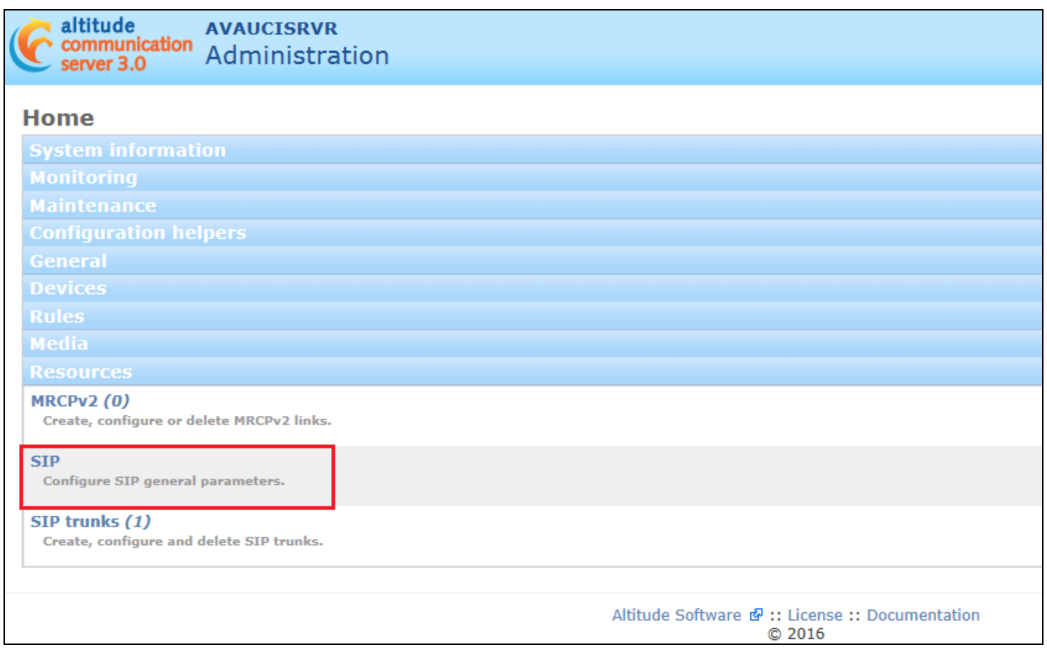
8.2. Configuring Altitude Communication Server

Open a web session to the Communication Server using https://**<Communication Server IP Address>:8081/login**. Enter the proper credentials and click on **Login**.

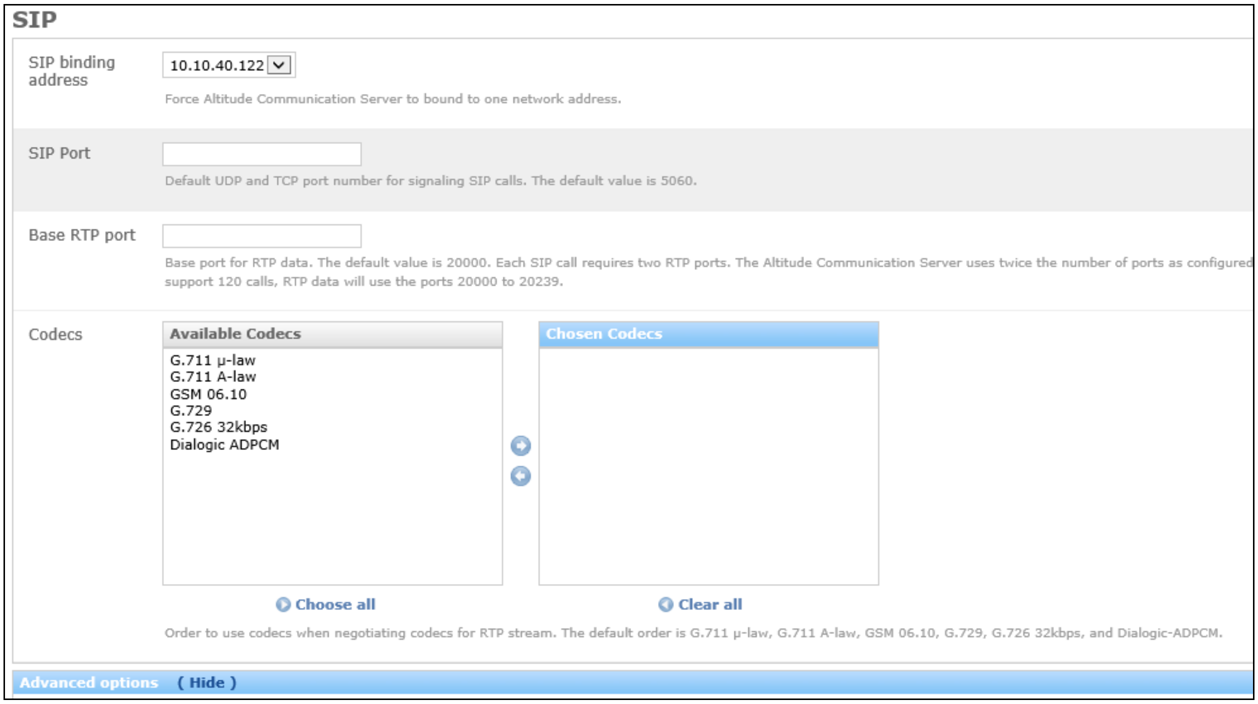


8.2.1. Configure SIP parameters

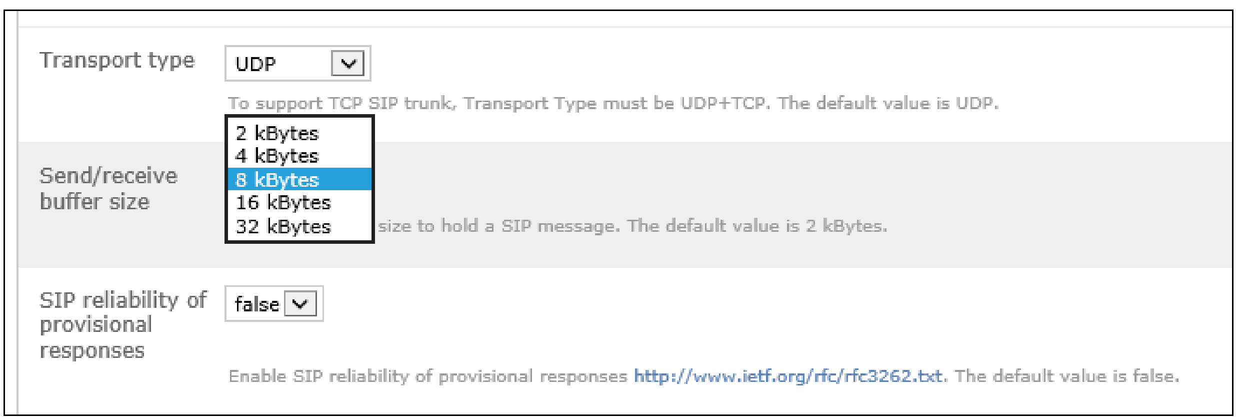
Navigate to **Home** → **Resources** → **SIP**.



The **SIP binding address** is filled in with the ACS IP address.

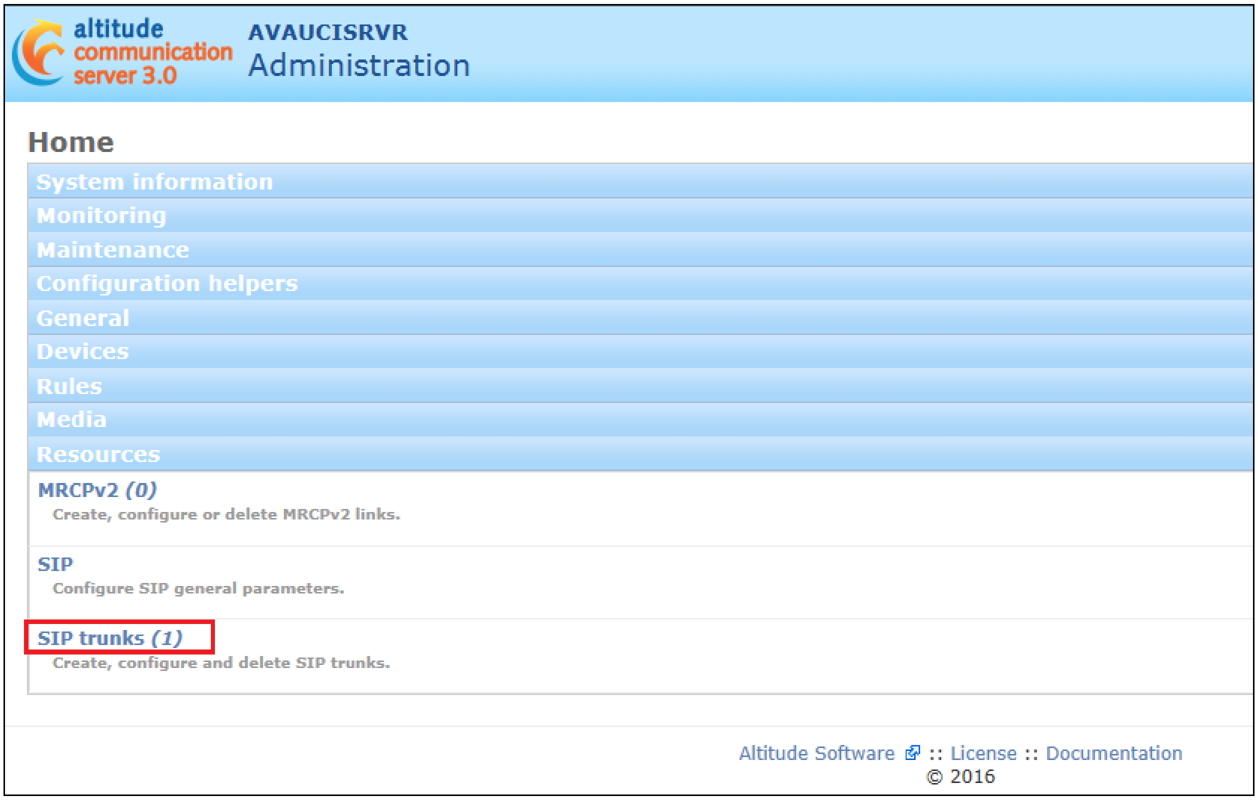


Click on **Advanced options** (shown above) to show other options and scroll down to **Transport type** which by default is set to **UDP**. The **Send/receive buffer size** may need to be increased from the default to **8 kBytes** as shown below.

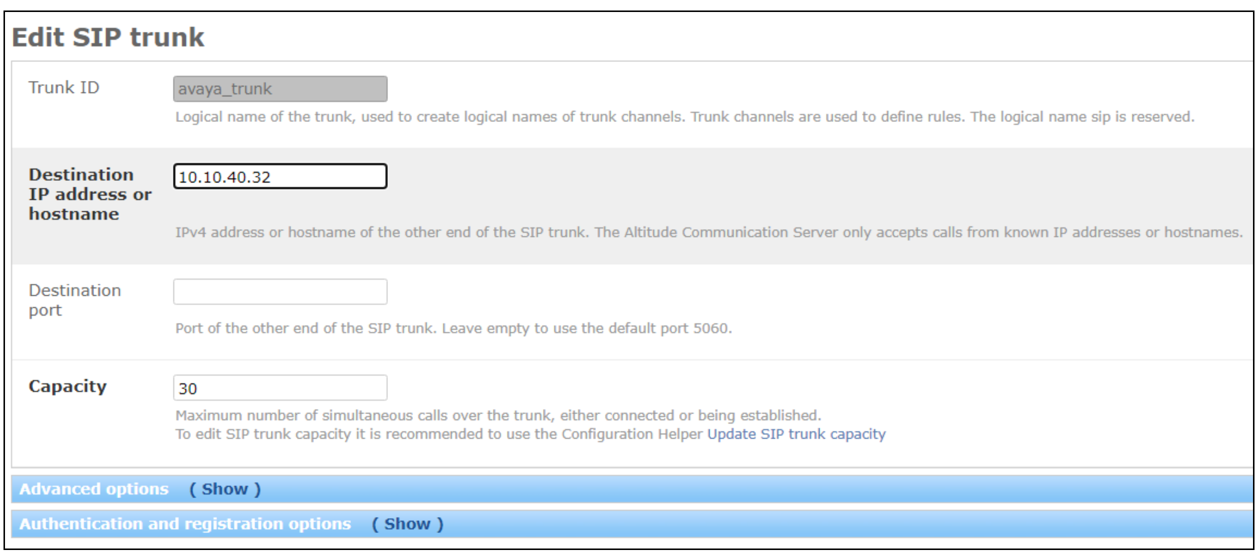


8.2.2. Configure SIP Trunk

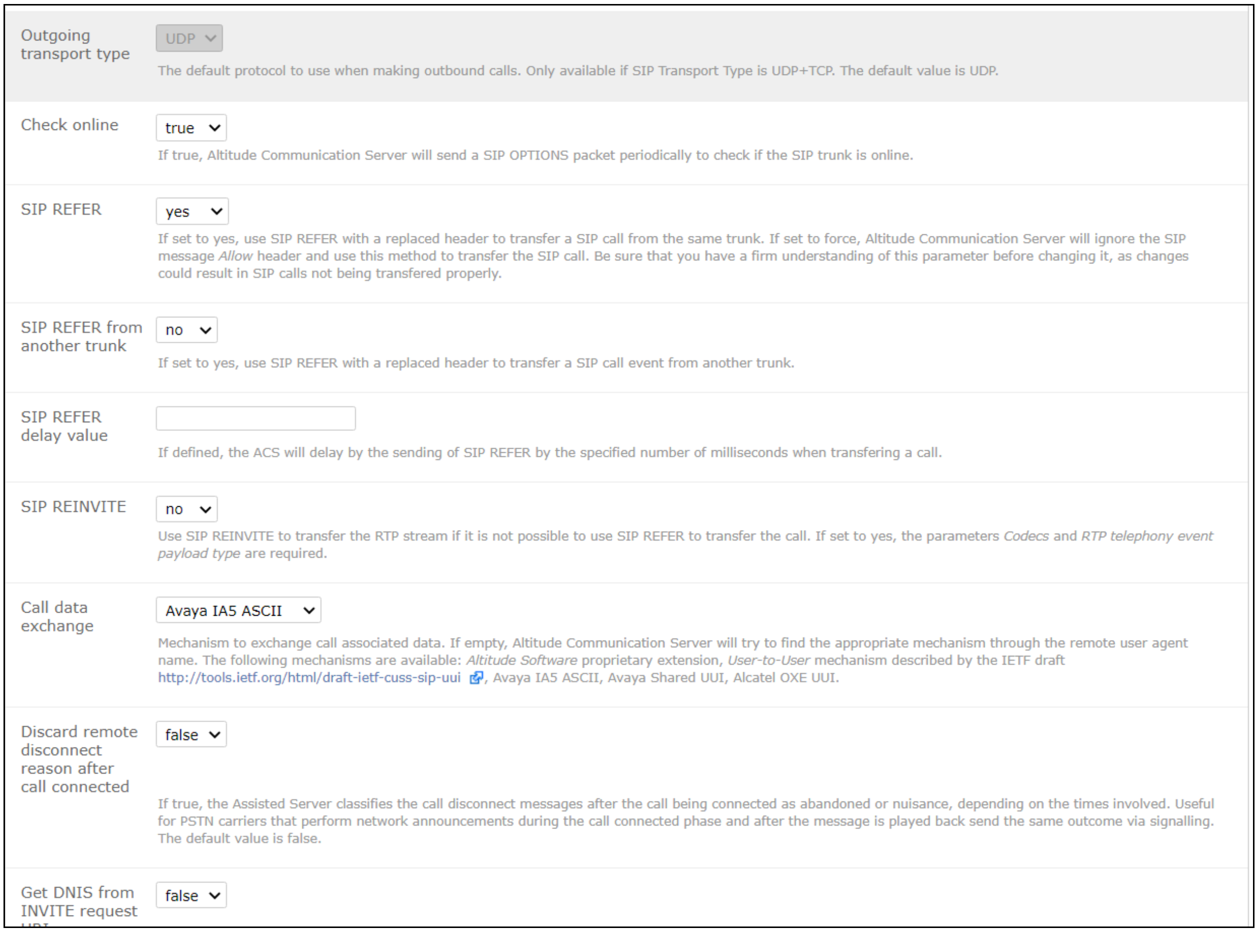
Navigate to **Home → Resources → SIP Trunk**.



Enter the Session Manager IP Address for the **Destination IP address or hostname**. Click on **Advanced options** and scroll down.



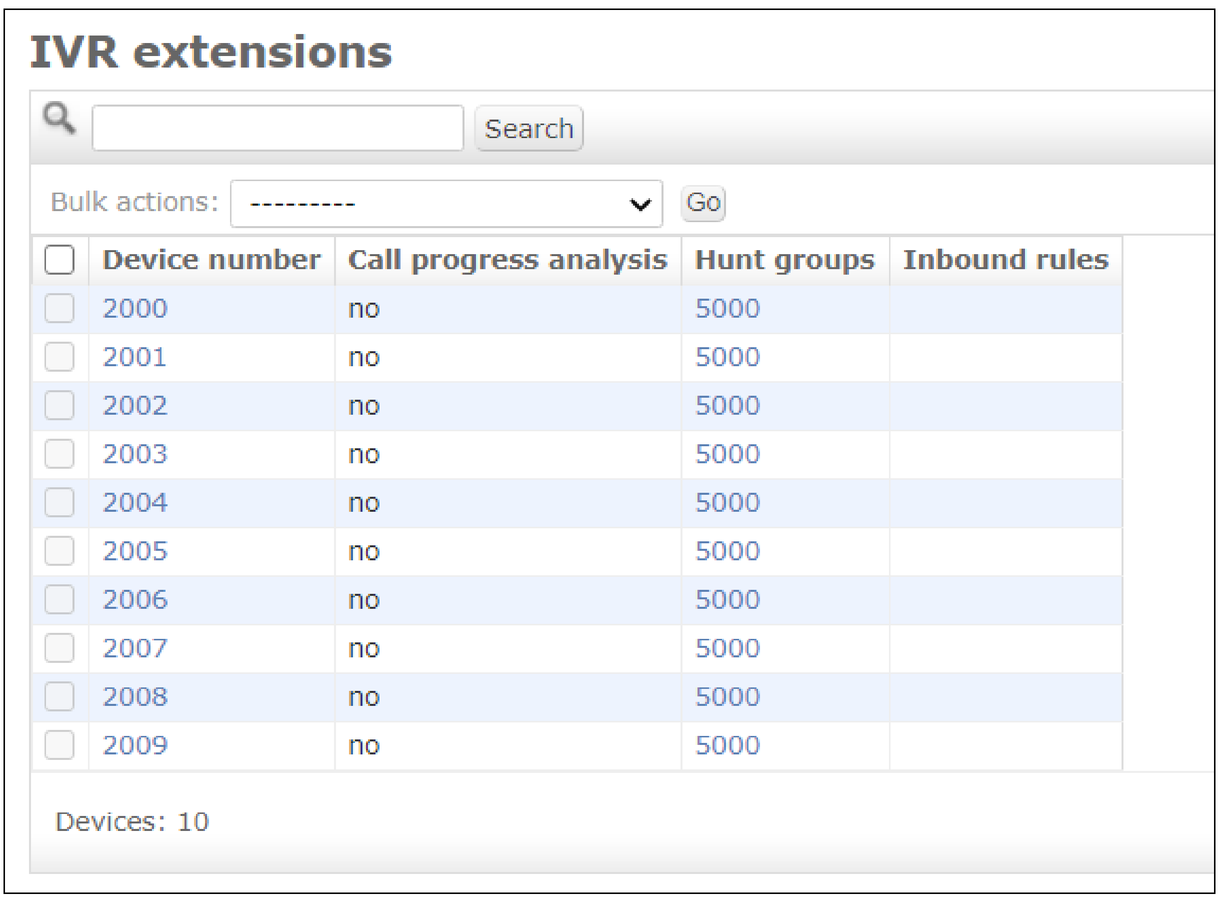
Click on **Advanced options** from the previous screen and scroll down as mentioned above. The **Outgoing Transport** is left as default, set to **UDP**. The **Call data exchange** should be set according to what is configured on the SIP trunk on Avaya Communication Manager. If UUI Treatment is set to "Service Provider" on Communication Manager, then Call data exchange is set to **Avaya IA5 ASCII** on the ACS configuration. If UUI Treatment is set to "Shared" then the below must be set to **Avaya Shared UUI**, (see **Section 5.4**).



8.2.3. Display the IVR Extensions and Hunt Group

Navigate to **Home** → **Devices** → **IVR extensions**.

A list of **IVR extensions** are used internally by ACS to implement the IVR, these are shown as follows.



IVR extensions

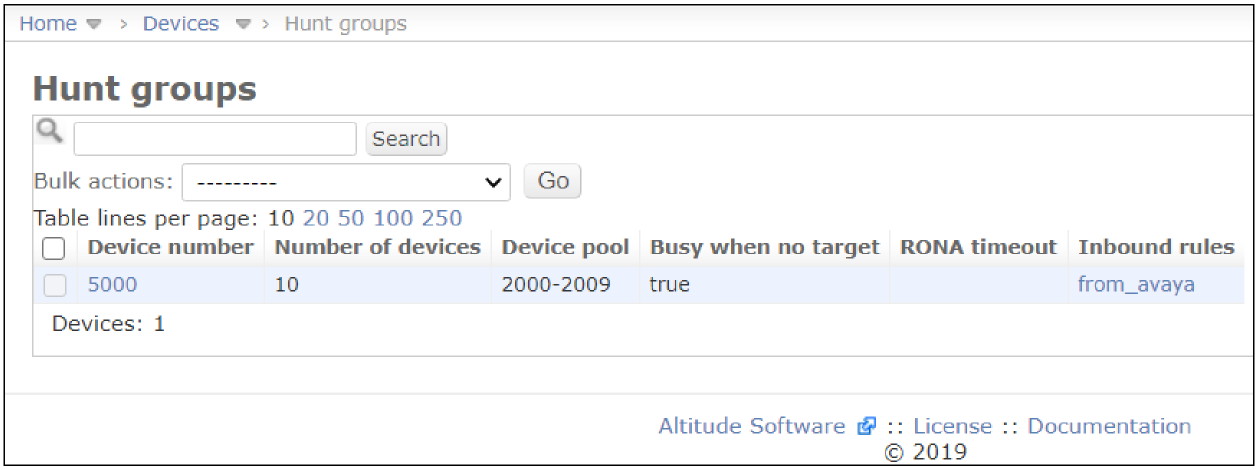
Search

Bulk actions: --------- Go

	Device number	Call progress analysis	Hunt groups	Inbound rules
	2000	no	5000	
	2001	no	5000	
	2002	no	5000	
	2003	no	5000	
	2004	no	5000	
	2005	no	5000	
	2006	no	5000	
	2007	no	5000	
	2008	no	5000	
	2009	no	5000	

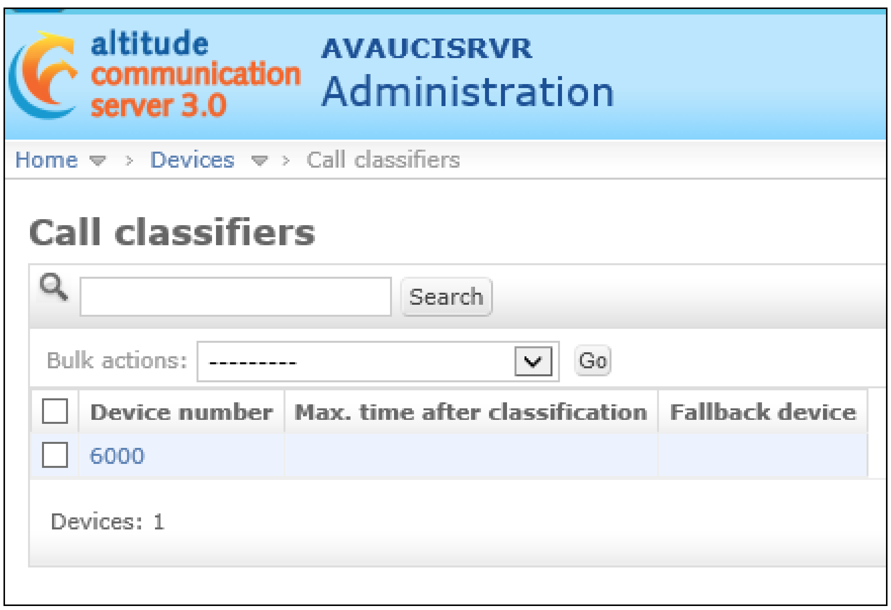
Devices: 10

The hunt group is used to distribute the calls to the IVR extensions. When setting up the hunt group the list of IVR extensions are specified under **Device pool**.



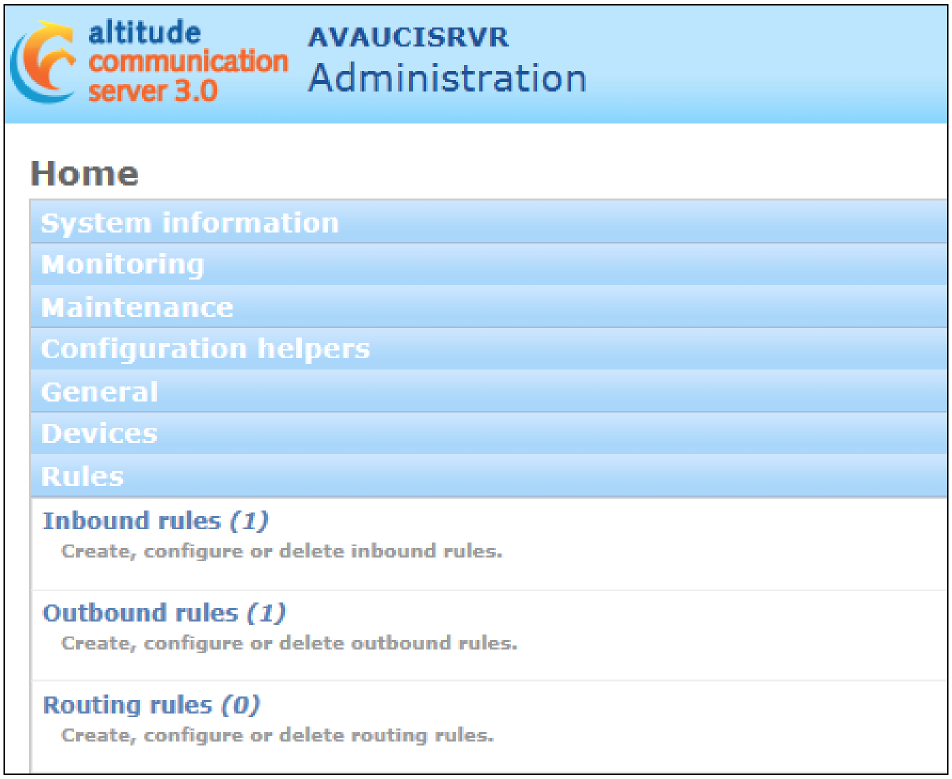
8.2.4. Display Call Classifier Device

The screen below shows the setup of a **Call classifier**, this was used during compliance testing. This value was used on the Telephony Gateway Configuration in **Section 8.1.1**.

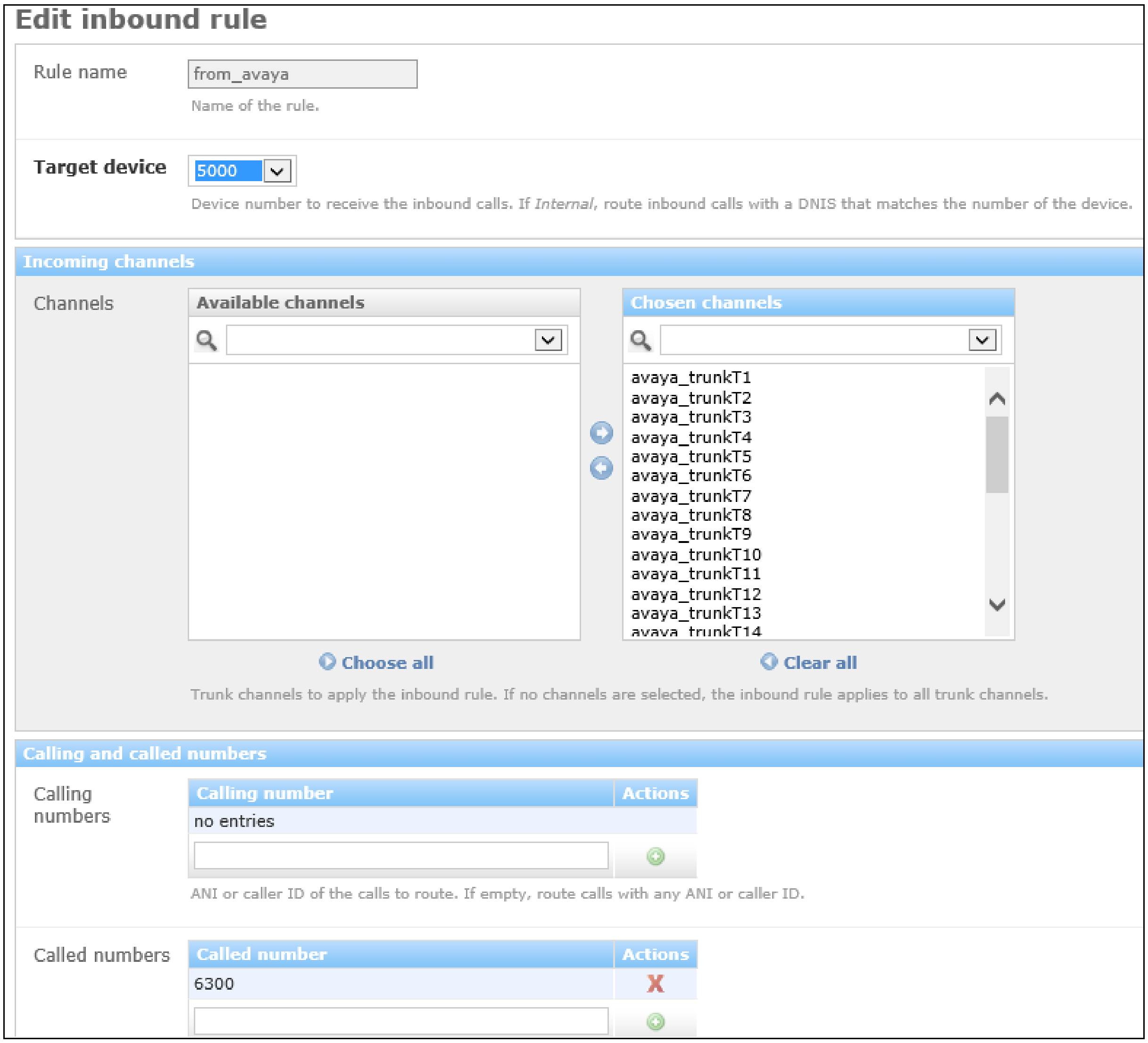


8.2.5. Display Inbound rules

Navigate to **Home → Rules → Inbound Rules**.

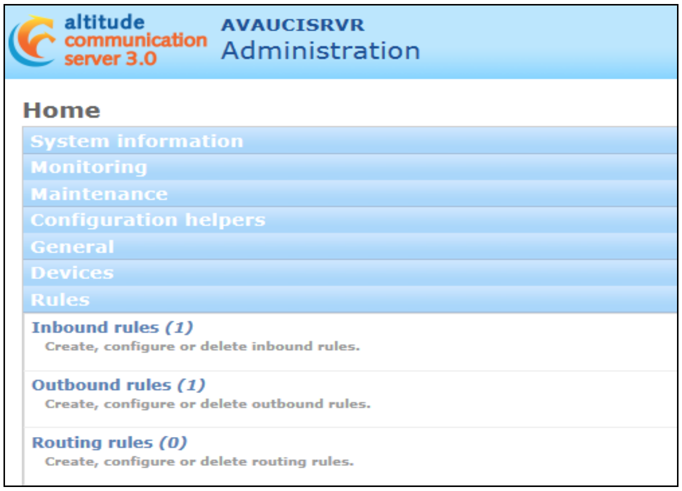


The following shows the setup of the **inbound rule** used for compliance testing. This is the rule for getting the call from the SIP Trunk to the ACS IVR hunt group. Note that **6300** was the number used to route the calls to the ACS via the SIP Trunk using AAR in **Section 5.5** and **Section 7.5**.

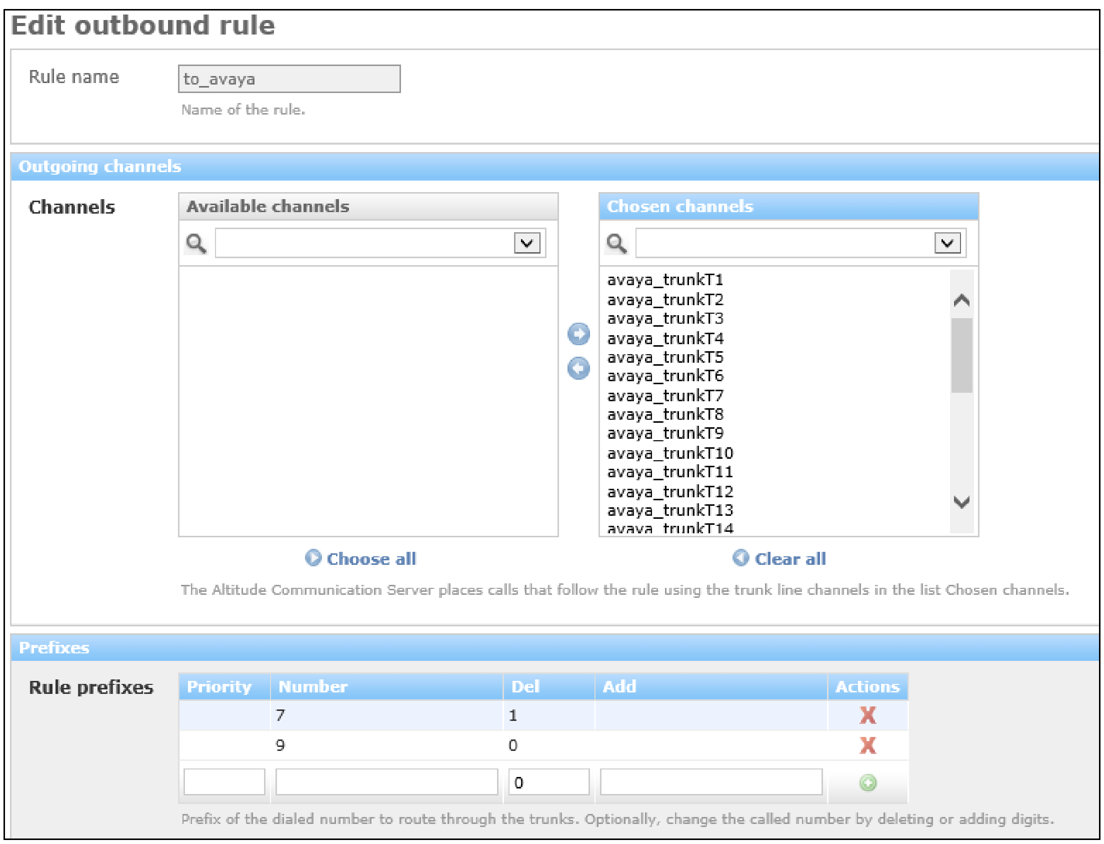


8.2.6. Display Outbound Rule

Navigate to **Home → Rules → Outbound rules**.



The following shows the setup of the **outbound rule** used for compliance testing. This is the rule for placing outbound calls to the PSTN and for transferring calls to Communication Manager. The Rule prefix **9** is added for calls to the PSTN. Rule prefix **7** is added for transferring IVR and Classified calls to the Avaya agents.



9. Verification Steps

The following steps can be taken to ensure that connections between Communication Manager, Application Enablement Services, Session Manager and Altitude Xperience Engagement are configured correctly. The steps described in this section are enough to verify delivery of inbound agent skillset calls. For other features and call flows, consult the technical documentation of both products.

9.1. Verify Avaya Aura® Communication Manager CTI link

Verify the status of the administered CTI link by using the **status aesvcs cti-link** command. Verify the **Service State** is **established** for the CTI link number administered in **Section 5.3**, as shown below.

```
status aesvcs cti-link

                          AE SERVICES CTI LINK STATUS

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

1     11       no    aes81xvmpg       established    87        61
```

By running the **List agent-loginID** command, the list of agents logged in is shown, as highlighted below, agent **1401** is logged into extension **1001**.

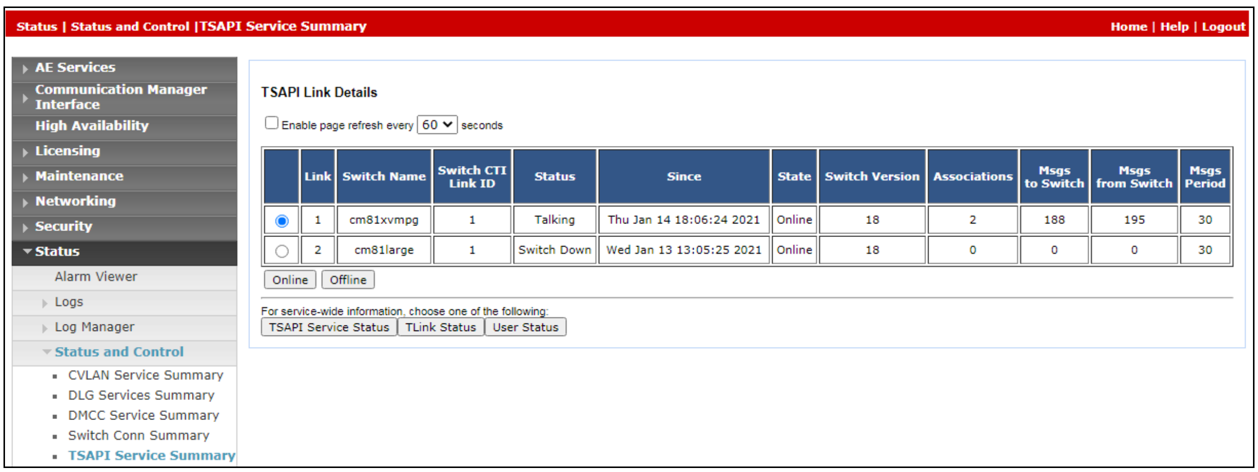
```
list agent-loginID                                                    Page   1
                               AGENT LOGINID
Login ID      Name           Extension      Dir Agt  AAS/AUD    COR AgPr SO
             Skil/Lv Skil/Lv Skil/Lv Skil/Lv Skil/Lv Skil/Lv Skil/Lv Skil/Lv

1400             Wspaces Agent1  unstaffed         90               1    lvl
                 90/01   10/01   37/01     /       /       /       /       /
1401             Altitude Ag1    1001              90               1    lvl
                 90/01   92/01     /       /       /       /       /       /
1402             Altitude Ag2    unstaffed         90               1    lvl
                 90/01   92/01     /       /       /       /       /       /
1403             Altitude Ag3    unstaffed         90               1    lvl
                 90/01   92/01     /       /       /       /       /       /
1410             WSpaces Agent O unstaffed         37               37   lvl
                 37/01   10/01   90/01   91/01     /       /       /       /
1411             WSpaces Supervi unstaffed                          1    lvl
                 37/01     /       /       /       /       /       /       /
60100            NICEAgent1      unstaffed                          1    lvl
                  1/01    2/03    3/03     /       /       /       /       /
60101            NICEAgent2      unstaffed                          1    lvl
                  1/01    3/03   90/02     /       /       /       /       /

                press CANCEL to quit --  press NEXT PAGE to continue
```

Running the command **list monitored-station**, shows all the stations that are currently being monitored via TSAPI and Application Enablement Services.

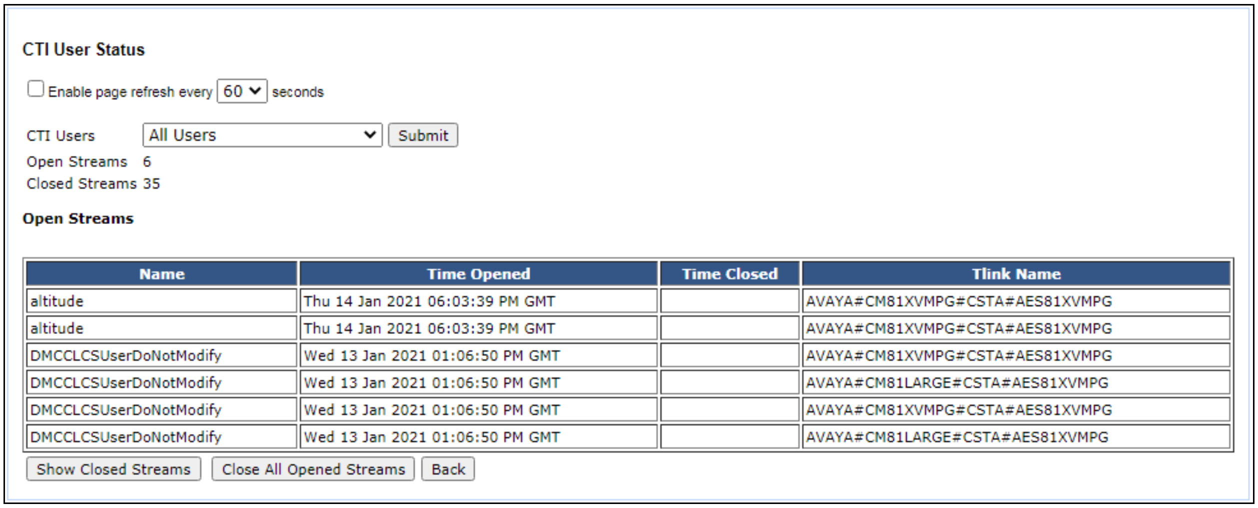
```
list monitored-station

                                   MONITORED STATION

   Associations:     1        2        3        4        5        6        7        8
                   CTI      CTI      CTI      CTI      CTI      CTI      CTI      CTI
Station Ext        Lnk  CRV Lnk  CRV Lnk  CRV Lnk  CRV Lnk  CRV Lnk  CRV Lnk  CRV Lnk  CRV
----------------- ------- ------- ------- ------- ------- ------- ------- -------
1001               1   0100



Command successfully completed
```

9.2. Verify Avaya Aura® Application Enablement Services CTI link

From the Application Enablement Services Status and Control in the left window, both the switch connection and the TSAPI connection can be verified. Click on the **TSAPI Service Summary** and the **State** should show **Online** as shown below.

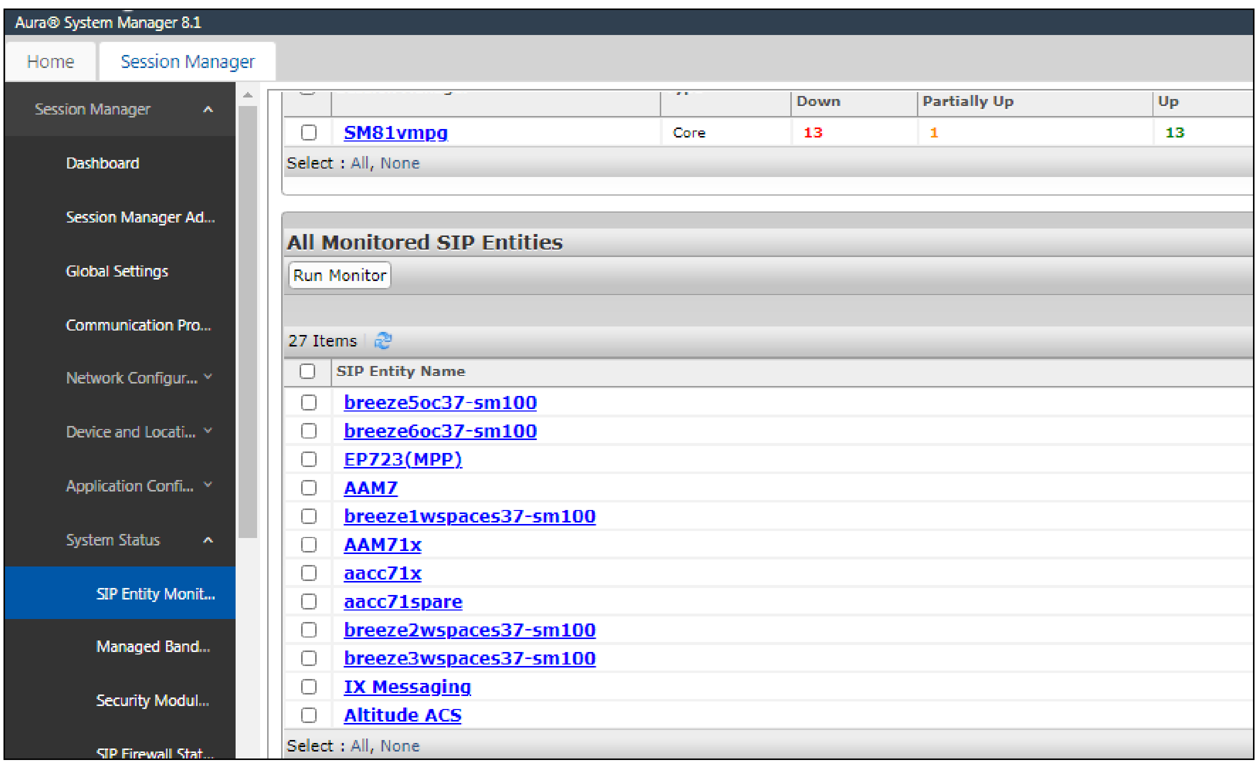


Clicking on the **User Status** from the screen on the previous page will bring up details of the TSAPI users connected, as shown below, the user **altitude** has two connections.

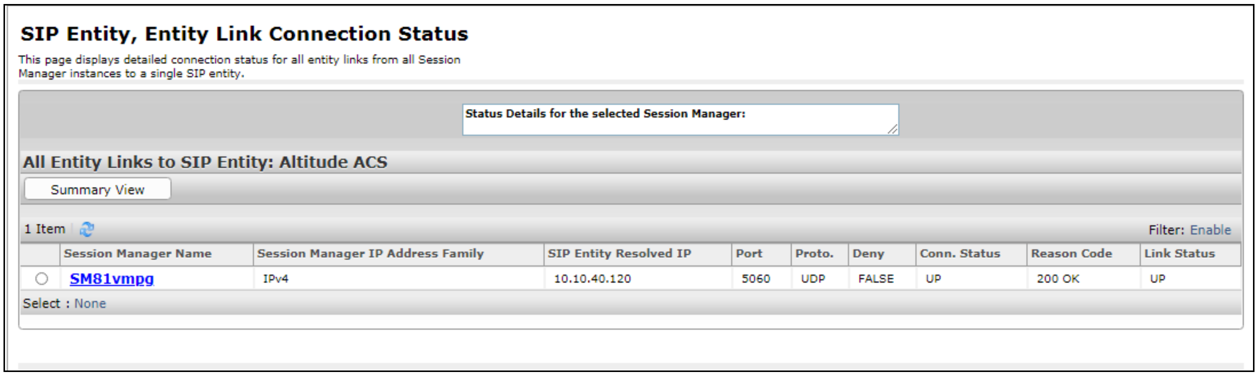


9.3. Verify SIP Entity

From System Manager Home Tab, click on Session Manager and navigate to **Session Manager → System Status → SIP Entity Monitoring**. Select the Altitude SIP Entity from the list.



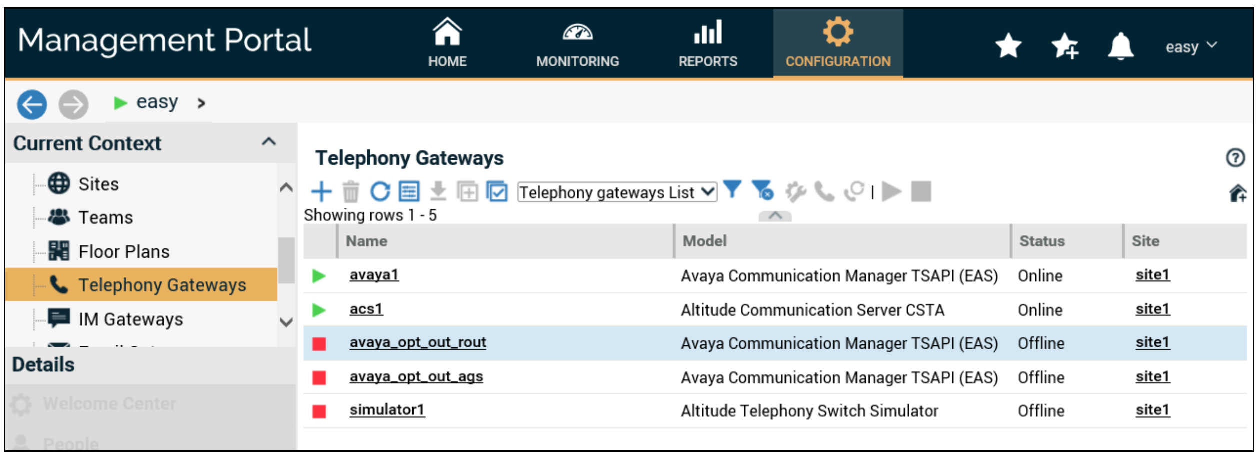
Verify that the **Conn Status** and **Link Status** are showing as **up**, as they are below for the Altitude SIP Entity that was selected from the previous page.



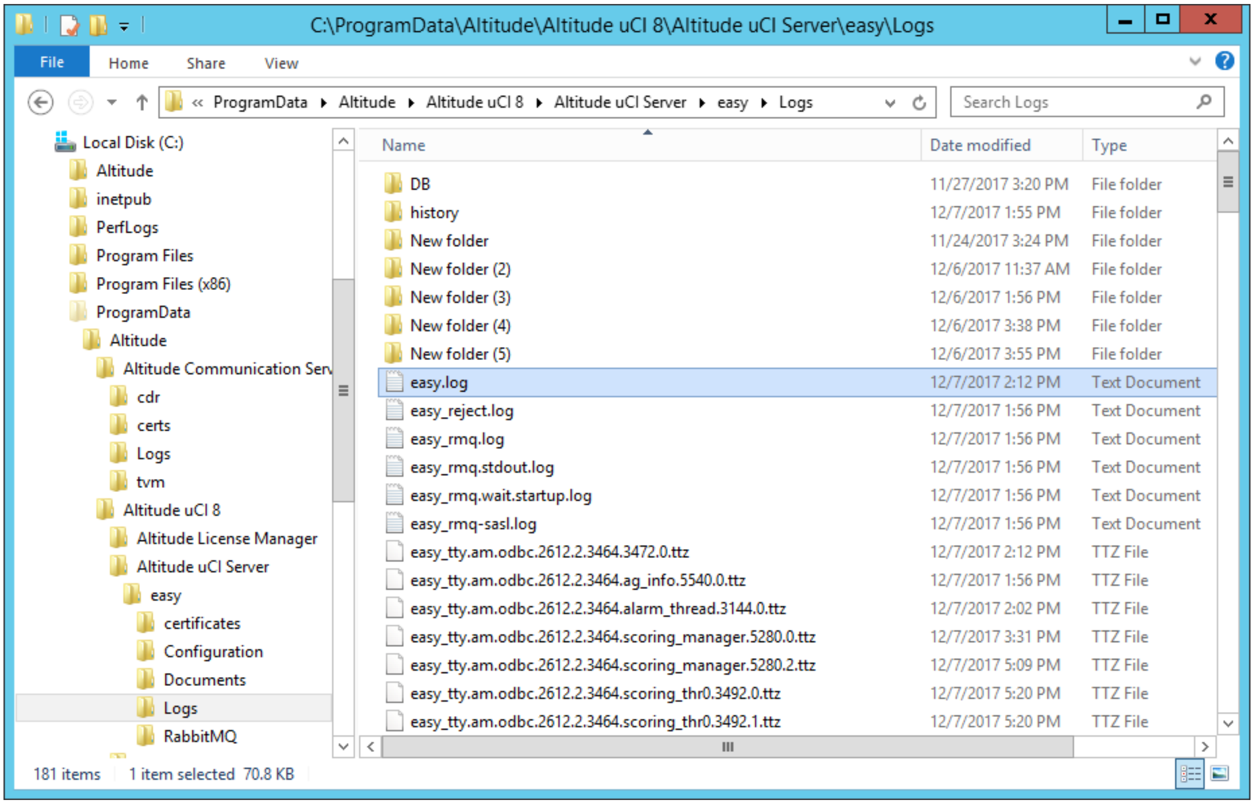
9.4. Verify Altitude Server is running correctly

Log in to the uSupervisor web session as shown in **Section 8**. Select **Current Content → Telephony Gateways** in the left panel.

The following screen shows that two gateways are currently in operation **avaya1** and **acs1**.

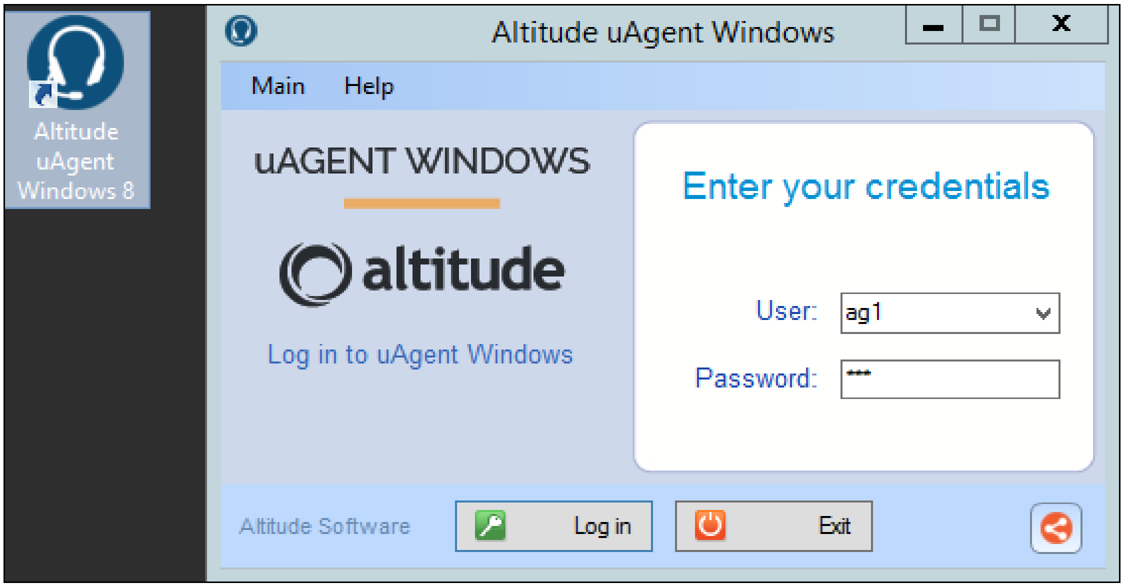


If there are any issues with connecting to the Application Enablement Services then this will be displayed in the easy.log file, located at **C:\ProgramData\Altitude\Altitude uCI 8\Altitude uCI Server\easy\Logs**.

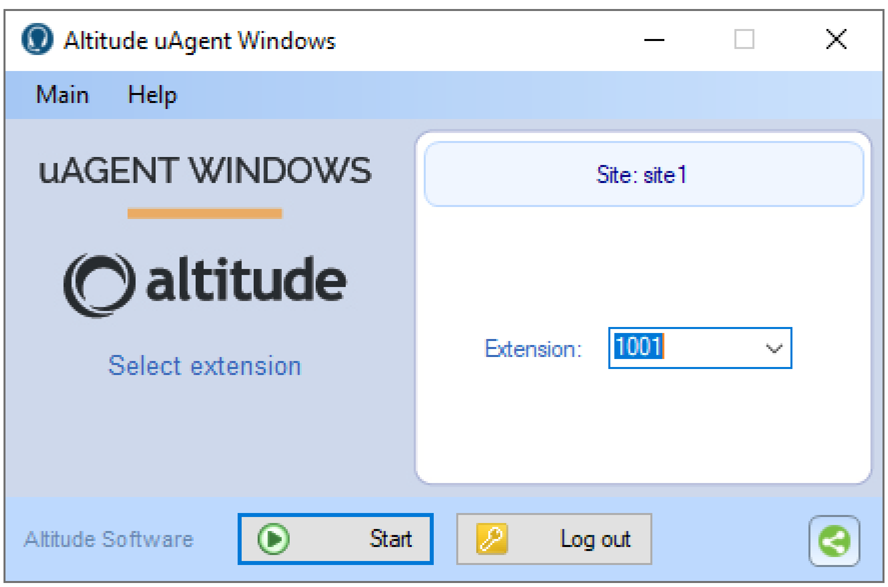


9.5. Verify Altitude uAgent Windows

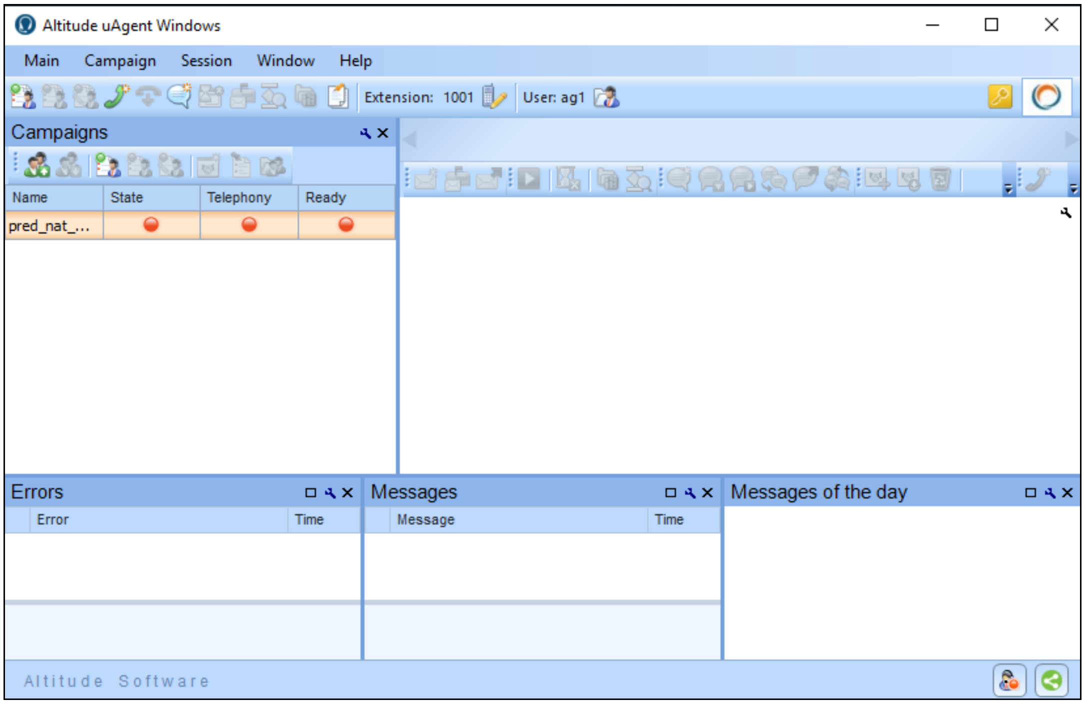
Log in to the Altitude uAgent Windows. Enter the proper credentials and click on **Log in**.



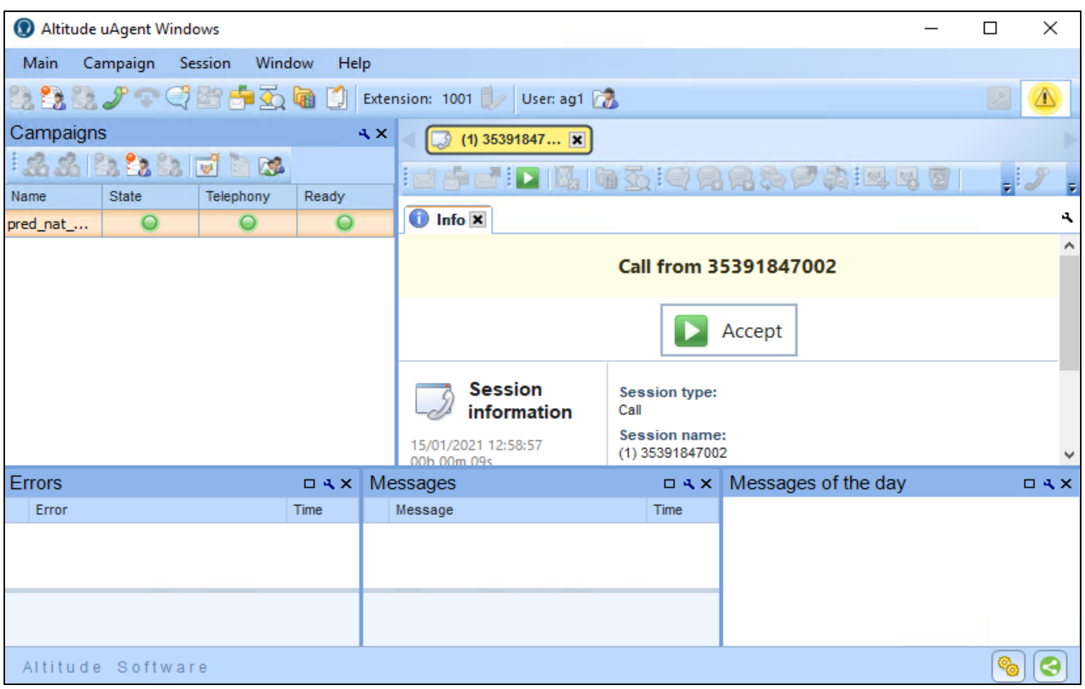
Enter the extension number to be monitored and click on **Start**.



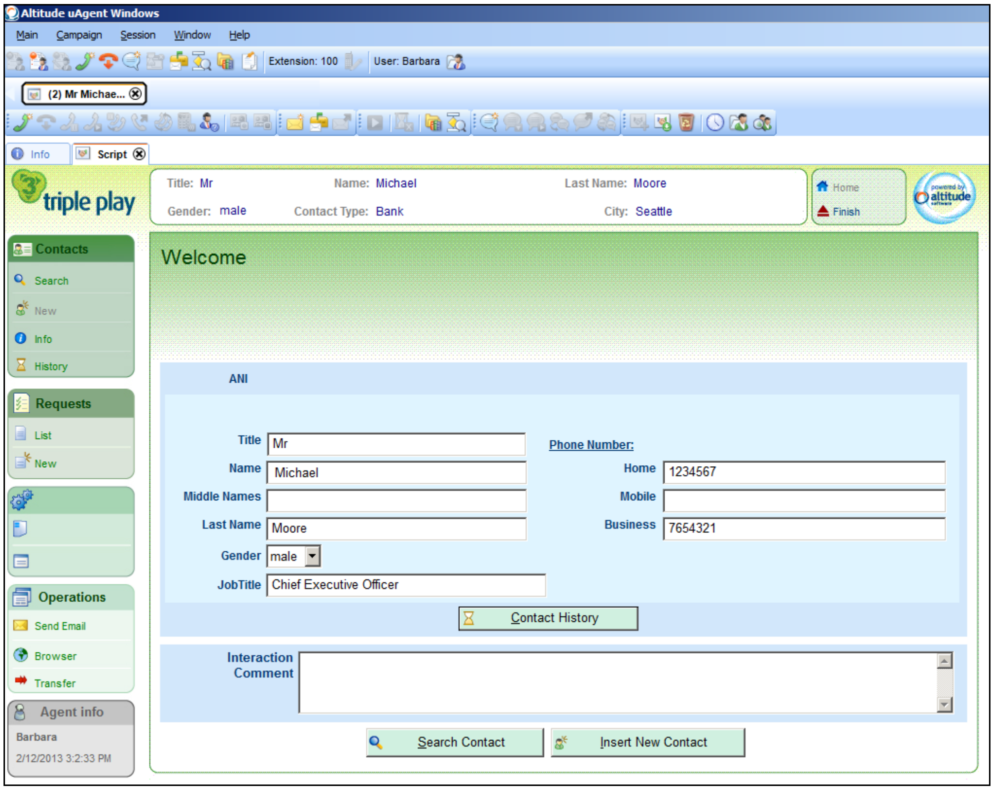
The following screen appears once logged in correctly. In order to open the campaign, double-click on **State** icon and to go ready double-click on **Ready** icon.



The agent is shown as logged in and ready with all lights green in the left window. Once a call is made and presented to the agent, the call can be accepted in the main window by clicking on **Accept**.



Once a call is answered the following screen, or similar, is popped to the agent.



10. Conclusion

These Application Notes describe the configuration steps required for Altitude Xperience Engagement 8.5 from Altitude Software to interoperate with Avaya Aura® Session Manager R8.1 and Avaya Aura® Application Enablement Services R8.1 to control Agents logged into Avaya Aura® Communication Manager R8.1. Please refer to **Section 2.2** for test results and observations.

11. Additional References

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

[1] *Administering Avaya Aura® Communication Manager*, Document ID 03-300509
[2] *Avaya Aura® Communication Manager Feature Description and Implementation,* Document ID 555-245-205
[3] *Avaya Aura® Application Enablement Services Administration and Maintenance Guide* Release 8.1
[4] *Administering Avaya Aura® Session Manager* – Release 8.1

All information on the product installation and configuration of Altitude Xperience Engagement can be found at http://www.altitude.com

Appendix

The following VDN's and Vectors were used during compliance testing. The VDN below was used for the Power Dial and note that **Vector 2** is used as outlined in **Section 5.2.2**, this is used to allow Altitude take control of the call.

```
display vdn 4905                                                 Page   1 of   3
                            VECTOR DIRECTORY NUMBER

                             Extension: 4905                     Unicode Name? n
                                 Name*: Altitude Power Dial
                           Destination: Vector Number        2
                   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*: 92
                            2nd Skill*:
                            3rd Skill*:

SIP URI:

* Follows VDN Override Rules
```

VDN 4907 was used as the 'User Entered Code' service. A special **Vector** was used to collect digits and route the call accordingly, this is shown on the following page.

```
display vdn 4907                                                 Page   1 of   3
                            VECTOR DIRECTORY NUMBER

                             Extension: 4907                     Unicode Name? n
                                 Name*: Altitude User Entered Code
                           Destination: Vector Number        5
                   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 5 was setup to collect digits and route the call to a certain VDN if the correct digit was pressed.

```
change vector 5                                               Page   1 of   6
                                  CALL VECTOR

    Number: 47              Name: Collect Digits
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 collect      1 digit after announcement 1840 for none
02 wait-time    2 secs hearing ringback
03 route-to     number 4908                  cov n if digit = 5
03 stop
04
05
06
07
```

VDN 4909 was used to give busy tone, again a special Vector was setup for this and is displayed below.

```
display vdn 4909                                                Page   1 of   3
                            VECTOR DIRECTORY NUMBER

                             Extension: 4909                    Unicode Name? n
                                 Name*: Altitude BusyTone
                           Destination: Vector Number        3
                   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*:
```

Vector 3 was used to play back busy tone, as shown below.

```
change vector 3                                                Page   1 of   6
                                  CALL VECTOR

    Number: 3               Name: BusyRingtone
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 busy
02
03
```

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.