Avaya Solution & Interoperability Test Lab

Application Notes for Altitude uCI 8 from Altitude Software with Avaya Aura® Communication Manager R7.1, Avaya Aura® Session Manager R7.1 and Avaya Aura® Application Enablement Services R7.1 – Issue 1.0

Abstract

These Application Notes describe the configuration steps for provisioning Altitude uCI 8 from Altitude Software with Avaya Aura® Session Manager R7.1 and Avaya Aura® Application Enablement Services R7.1 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 uCI 8 from Altitude Software to interoperate with Avaya Aura® Session Manager R7.1 and Avaya Aura® Application Enablement Services R7.1 to control agents logged into Avaya Aura® Communication Manager. These Application Notes are focused on two separate connections from Altitude uCI to the Avaya solution.

1. The Telephony Server Application Programming Interface (TSAPI) connection from Altitude Telephony Gateway, a component of Altitude uCI 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 uCI, allowing customers call into an IVR system prior to being routed to an Avaya agent. Because Altitude Communication Server only serves as an add-on module it will be included in these Application Notes.

Altitude uCI (Unified Customer Interaction) is an IP based contact centre 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 centre 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 centre. Altitude Automated Agents uses SIP trunks via Altitude Communication Server to connect to Avaya Aura® Communication Manager via Avaya Aura® Session Manager.

2. General Test Approach and Test Results

The interoperability compliance testing evaluates the ability of Altitude uCI to gain telephony functionality on Communication Manager via AES. Testing involves two Altitude uCI agents logging in going ready and answering calls as well as being able to make outbound predictive calls from the Altitude uAgent Windows. Agents utilize the telephony functionality on Altitude Communication Manager using Altitude uAgent Windows.

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 uCI 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 Windows 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 Windows
- 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 observation. When a call is placed directly to the ACS (via AAR routing and SIP Trunk) and the call is then transferred back into the "incoming VDN" the call data is missing or distorted i.e., the calling number appears as TSAPI Call ID. When a VDN was added that routes the call to the ACS via AAR and SIP Trunk, this issue is resolved. The configuration for this routing point/VDN is added in the **Appendix**.

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 uCI server was placed on the Avaya Telephony LAN. The AES provides the Altitude uCI server CTI capability on Altitude Communication Manager. Altitude uAgent Windows is used to answer/make the calls in a call centre environment. SIP trunks between the Altitude uCI server and Session Manager connect the Altitude Communication Server (SIP module on Altitude uCI) 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.

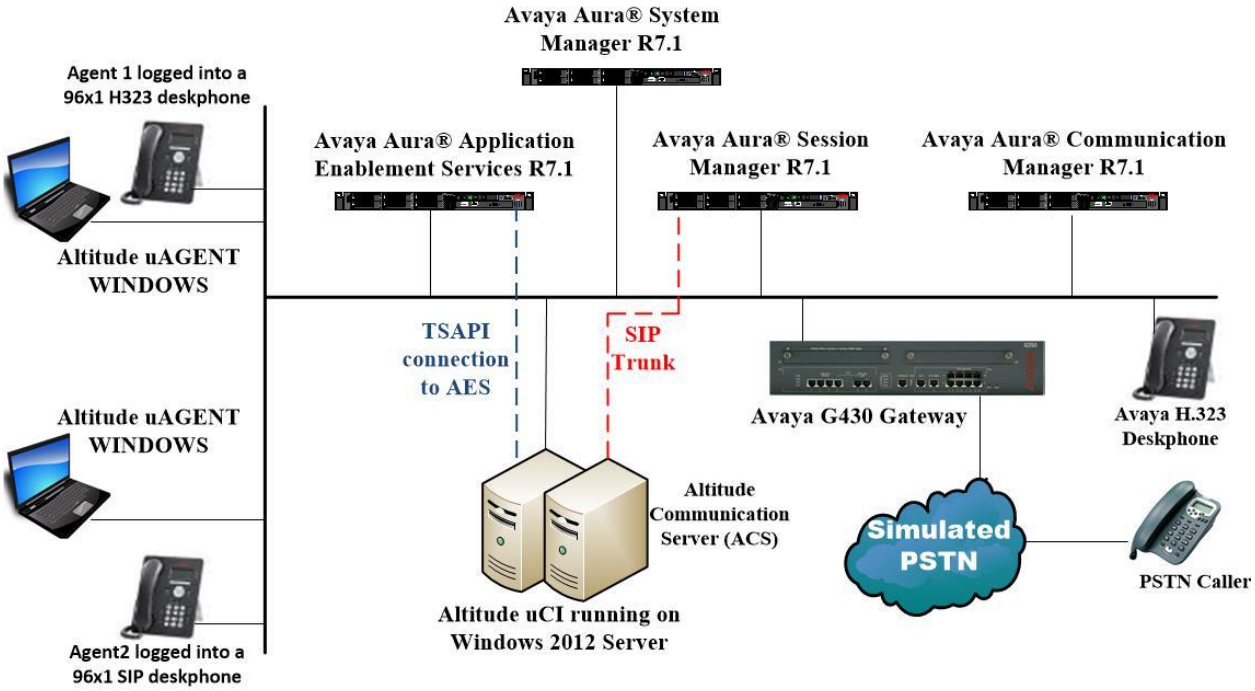


Figure 1: Network solution of Altitude uCI 8 and Avaya Aura® Communication Manager R7.1 with Avaya Aura® Session Manager R7.1 and Avaya Aura® Application Enablement Services R7.1

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya Aura® System Manager running on a virtual server	System Manager 7.1.1.0 Build No. - 7.1.0.0.1125193 Software Update Revision No: 7.1.1.0.046931 Feature Pack 1 Service Pack 1
Avaya Aura® Session Manager running on a virtual server	Session Manager R7.1 SP1 Build No. – 7.1.1.0.711008
Avaya Aura® Communication Manager running on Virtual Server	R017x.01.0.532.0 R7.1.1.0.0 - FP1 Update ID 01.0.532.0-23985
Avaya Aura® Application Enablement Services running on a virtual server	R7.1.0.0.0.17-0
Avaya G430 Gateway	37.42.0 /1
Avaya 96x1 H323 Deskphone	96x1 H323 Release 6.6401
Avaya 96x1 SIP Deskphone	96x1 SIP Release 7.1.0.1.1
Altitude uCI 8 running on a virtual Windows Server 2012 R2 Standard with MS SQL Server 2012 Standard - Altitude uCI Server - Altitude License Manager - Altitude uSupervisor Web - Altitude uAgent Windows - Altitude Automated Agents - Altitude Communication Server	8
Windows Internet Explorer	V11.0

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)? n               Authorization Codes? y
        Analog Trunk Incoming Call ID? y                        CAS Branch? n
 A/D Grp/Sys List Dialing Start at 01? y                          CAS Main? n
Answer Supervision by Call Classifier? y                 Change COR by FAC? n
                                  ARS? y  Computer Telephony Adjunct Links? y
                 ARS/AAR Partitioning? y   Cvg Of Calls Redirected Off-net? y
          ARS/AAR Dialing without FAC? n                       DCS (Basic)? y
          ASAI Link Core Capabilities? n                 DCS Call Coverage? y
          ASAI Link Plus Capabilities? n                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: 7.0

                                 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 8.1.2** when defining the Line Prefix.

```
display feature-access-codes                                    Page   1 of  10
                              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.

```
display feature-access-codes                                          Page   5 of  10
                              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.

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

               COR Number: 1
          COR Description: DefaultCOR_PG

                      FRL: 7                                 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? n
     Restricted Call List? n                 Can Change Coverage? n

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

5.2. 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 **33**. 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 33                                                   Page   1 of   4
                                   HUNT GROUP

            Group Number: 33                                  ACD? y
              Group Name: Altitude Inbound                  Queue? y
         Group Extension: 3330                             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 33                                                   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
```

Repeat the step above to create a hunt group for an outbound service, **hunt group 34** is shown below.

```
add hunt-group 34                                                Page   1 of   4
                                   HUNT GROUP

            Group Number: 34                                 ACD? y
              Group Name: Altitude Outbound                Queue? y
         Group Extension: 3340                           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 **skill 33** as shown below. Skill 33 relates to the skill enabled hunt group configured previously.

```
add vector 3                                                     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 adjunct      routing link 1
02 wait-time    5   secs hearing silence
03 queue-to     skill 33   pri m
04 wait-time    999 secs hearing ringback
```

The above step may also be used to create a Vector for the outbound service, shown below

```
add vector 4                                                    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 34   pri m
04 wait-time    999 secs hearing ringback
```

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.

```
add vdn 3300                                                    Page   1 of   3
                            VECTOR DIRECTORY NUMBER

                             Extension: 3300
                                 Name*: Altitude Inbound
                           Destination: Vector Number        3
                     Attendant Vectoring? n
                   Meet-me Conferencing? n
                     Allow VDN Override? n
                                   COR: 1
                                   TN*: 1
                              Measured: none

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

The above step may also be used to create a VDN for the outbound service, shown below

```
add vdn 3400                                                    Page   1 of   3
                            VECTOR DIRECTORY NUMBER

                             Extension: 3400
                                 Name*: Altitude Outbound
                           Destination: Vector Number        4
                     Attendant Vectoring? n
                   Meet-me Conferencing? n
                     Allow VDN Override? n
                                   COR: 1
                                   TN*: 1
                              Measured: none

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

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** except for those logins that will be used for outbound services. In that case, the field will be set to **all**.

```
add agent-loginID 4405                                          Page   1 of   2
                                  AGENT LOGINID

                Login ID: 4405                                   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 is created. Set the **Direct Agent Skill** to the inbound hunt group **33**.

```
change agent-loginID 4405                                       Page   2 of   3
                                  AGENT LOGINID
      Direct Agent Skill: 33                          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: 33      1           16:                 31:                 46:
 2: 34      1           17:                 32:                 47:
```

5.2.5. Configure Agent Stations

For each station 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 4000                                          Page   1 of   5
                                    STATION

Extension: 4000                        Lock Messages? n               BCC: 0
     Type: 9608                        Security Code: *                TN: 1
     Port: S00000                    Coverage Path 1:                 COR: 1
     Name: 4000, 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: 4000
            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
```

Page 2 was set as follows.

```
change station 4000                                          Page   2 of   5
                                    STATION
FEATURE OPTIONS
           LWC Reception: spe             Auto Select Any Idle Appearance? n
          LWC Activation? y                        Coverage Msg Retrieval? y
  LWC Log External Calls? n                                  Auto Answer: none
             CDR Privacy? n                                Data Restriction? n
   Redirect Notification? y                     Idle Appearance Preference? n
 Per Button Ring Control? n                   Bridged Idle Line Preference? n
   Bridged Call Alerting? n                       Restrict Last Appearance? y
  Active Station Ringing: single
                                                         EMU Login Allowed? n
        H.320 Conversion? n          Per Station CPN - Send Calling Number?
       Service Link Mode: as-needed                     EC500 State: enabled
        Multimedia Mode: enhanced                 Audible Message Waiting? n
    MWI Served User Type:                       Display Client Redirection? n
             AUDIX Name:                       Select Last Used Appearance? n
                                                 Coverage After Forwarding? s
                                                   Multimedia Early Answer? n
 Remote Softphone Emergency Calls: as-on-local Direct IP-IP Audio Connections? y
  Emergency Location Ext: 4000          Always Use? n IP Audio Hairpinning? n
```

On **Page 4**, the following buttons must be assigned as shown below:

- **aux-work** – Agent is logged in to the ACD but is not available to take a call
- **manual-in** – Agent is available to accept ACD calls
- **after-call** – Agent state after the ACD call is completed. The agent is not available
- **release** – State when the call is dropped

```
change station 4000                                          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: manual-in          Grp:
 2: call-appr                            6: after-call         Grp:
 3:                                      7: release
 4: aux-work    RC:    Grp:             8:

    voice-mail
```

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 AES and will give information on how this link was setup for compliance testing with Altitude uCI.

5.3.1. Display Node-Names IP

Display the procr IP Address by using the command **display node-names ip** and noting the IP address for the **procr**, the AES (**AES71vmpg**) and Session Manager (**SM71vmpg**).

```
display node-names ip                                        Page   1 of   2
                                 IP NODE NAMES
    Name              IP Address
AES71vmpg           10.10.40.43
AMS71vmpg           10.10.40.49
GW71vmpg            10.10.40.15
SM70vmpg            10.10.40.12
SM71vmpg            10.10.40.52
default             0.0.0.0
procr               10.10.40.47
```

5.3.2. Configure IP Services

To administer the transport link to AES use the **change ip-services** command. On **Page 1** add an entry with the following values:

- **Service Type:** should be set to **AESVCS**
- **Enabled:** set to **y**
- **Local Node:** set to the node name assigned for the **procr** in **Section 5.3.1**
- **Local Port** Retain the default value of **8765**

```
change ip-services                                                Page   1 of   4

                                    IP SERVICES
 Service      Enabled     Local        Local       Remote      Remote
  Type                    Node         Port        Node        Port
AESVCS         y          procr        8765
```

Go to **Page 4** of the ip-services form and enter the following values:

- **AE Services Server:** Name obtained from the AES server, in this case **AES71vmpg**
- **Password:** Enter a password to be administered on the AES server
- **Enabled:** Set to **y**

Note: The password entered for **Password** field must match the password on the AES server in **Section 6.1**. The **AE Services Server** should match the administered name for the AES server, this is created as part of the AES installation, and can be obtained from the AES server by typing **uname –n** at the Linux command prompt.

```
change ip-services                                                Page   4 of   4
                            AE Services Administration

   Server ID    AE Services       Password          Enabled    Status
                   Server
      1:        AES71vmpg         ********          y          idle
      2:
      3:
```

5.3.3. Configure CTI Link

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: 2002
     Type: ADJ-IP
                                                                        COR: 1
     Name: AES71vmpg
```

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 7.2**. 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 the **IP Node Names** from **Section 5.3.1**.
- Set the **Far-end Node Name** to the node name defined for the Session Manager (node name **SM71vmpg**), from **Section 5.3.1**.
- 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 1                                          Page   1 of   2
                                SIGNALING GROUP

 Group Number: 1              Group Type: sip
  IMS Enabled? n        Transport Method: tls
        Q-SIP? n
     IP Video? n                                    Enforce SIPS URI for SRTP? n
  Peer Detection Enabled? y  Peer Server: SM
 Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? y
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? n
Alert Incoming SIP Crisis Calls? n
   Near-end Node Name: procr                 Far-end Node Name: SM71vmpg
 Near-end Listen Port: 5061                Far-end Listen Port: 5061
                                        Far-end Network Region: 1

Far-end Domain:
                                            Bypass If IP Threshold Exceeded? n
Incoming Dialog Loopbacks: eliminate                RFC 3389 Comfort Noise? n
         DTMF over IP: rtp-payload           Direct IP-IP Audio Connections? y
Session Establishment Timer(min): 3                   IP Audio Hairpinning? n
         Enable Layer 3 Test? y                   Initial IP-IP Direct Media? n
H.323 Station Outgoing Direct Media? n            Alternate Route Timer(sec): 6
```

Configure the **Trunk Group** form as shown below. This trunk group is used for calls to and from 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 **tie**. Specify the signaling group associated with this trunk group in the **Signaling Group** field, and specify the **Number of Members** supported by this SIP trunk group. Accept the default values for the remaining fields.

```
change trunk-group 1                                          Page   1 of  21
                                TRUNK GROUP

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

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

```
change trunk-group 1                                          Page   2 of  21
      Group Type: sip

TRUNK PARAMETERS

     Unicode Name: auto

                                          Redirect On OPTIM Failure: 5000

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

 Disconnect Supervision - In? y  Out? y


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




 Caller ID for Service Link Call to H.323 1xC: station-extension
```

Settings on **Page 3** are as follows. These are the values used during compliance testing.

Note: 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 1                                            Page   3 of  21
TRUNK FEATURES
          ACA Assignment? n            Measured: none
                                                        Maintenance Tests? y



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

                                               Replace Restricted Numbers? n
                                              Replace Unavailable Numbers? n

                                                Hold/Unhold Notifications? y
                                Modify Tandem Calling Number: no




 Show ANSWERED BY on Display? y
```

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

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

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


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

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

5.5. 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 in order to route the call to ACS. In order to achieve this routing, automatic alternate routing (aar) will be used to route the calls. The dial plan and aar routing analysis need to be changed to allow this routing.

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

```
change dialplan analysis                                          Page   1 of  12
                            DIAL PLAN ANALYSIS TABLE
                                  Location: all            Percent Full: 3

    Dialed   Total  Call     Dialed   Total  Call     Dialed   Total  Call
    String   Length Type     String   Length Type     String   Length Type
   1           4   udp      #           3   fac
   2           4   udp
   3           4   udp
   4           4   ext
   5           4   udp
   58          5   ext
   5999        4   ext
   6           4   udp
   6666        4   ext
   7           4   udp
   781         5   ext
   8           1   fac
   9           1   fac
   *           3   fac
   *8          4   dac
```

5.5.2. 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
 65               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 1**, 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     1        aar          n
    65                     4    4     1        aar          n
    7                      7    7     254      aar          n
    8                      7    7     254      aar          n
    9                      7    7     254      aar          n
                                                             n
                                                             n
                                                             n
                                                             n
                                                             n
```

Use the **change route-pattern *n*** command to add the SIP trunk group to the route pattern that AAR selects. In this configuration, Route Pattern Number **1** is used to route calls to trunk group **(Grp No) 1**, this is the SIP Trunk configured in **Section 5.4**. The **Numbering Format** was set to **lev0-pvt**.

```
change route-pattern 1                                         Page   1 of   3
                    Pattern Number: 1      Pattern Name: SIP TRUNK
    SCCAN? n    Secure SIP? n     Used for SIP stations? n

    Grp FRL NPA Pfx Hop Toll No.  Inserted                            DCS/ IXC
    No          Mrk Lmt List Del  Digits                              QSIG
                             Dgts                                     Intw
 1: 1    0                                                            n   user
 2:                                                                   n   user
 3:                                                                   n   user
 4:                                                                   n   user
 5:                                                                   n   user
 6:                                                                   n   user

     BCC VALUE  TSC CA-TSC    ITC BCIE Service/Feature PARM Sub  Numbering LAR
    0 1 2 M 4 W     Request                                Dgts Format
 1: y y y y y n  n           unre                                lev0-pvt  none
 2: y y y y y n  n           rest                                          none
 3: y y y y y n  n           rest                                          none
 4: y y y y y n  n           rest                                          none
 5: y y y y y n  n           rest                                          none
 6: y y y y y n  n           rest                                          none
```

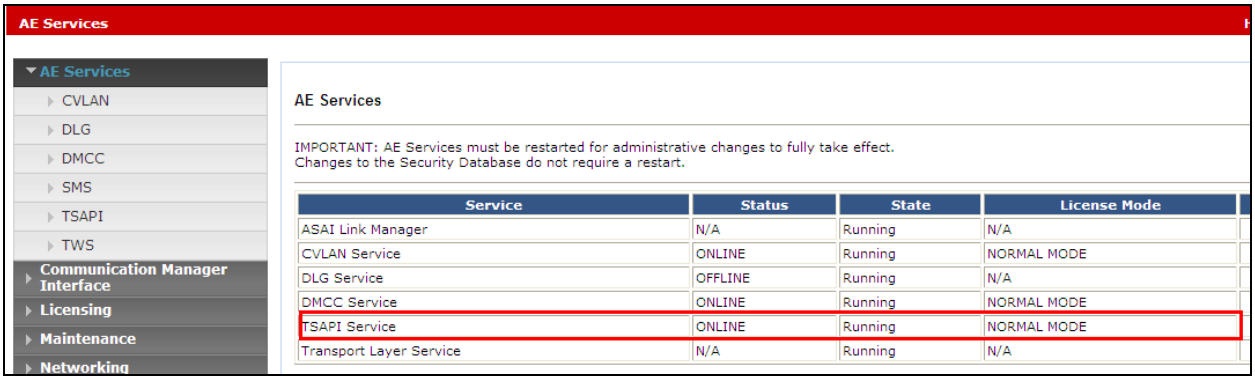
6. Configure Avaya Aura® Application Enablement Services

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.

Launch a web browser, enter **https://<IP address of AES server>** in the URL, and log in with the appropriate credentials for accessing the Application Enablement Services Management Console page.

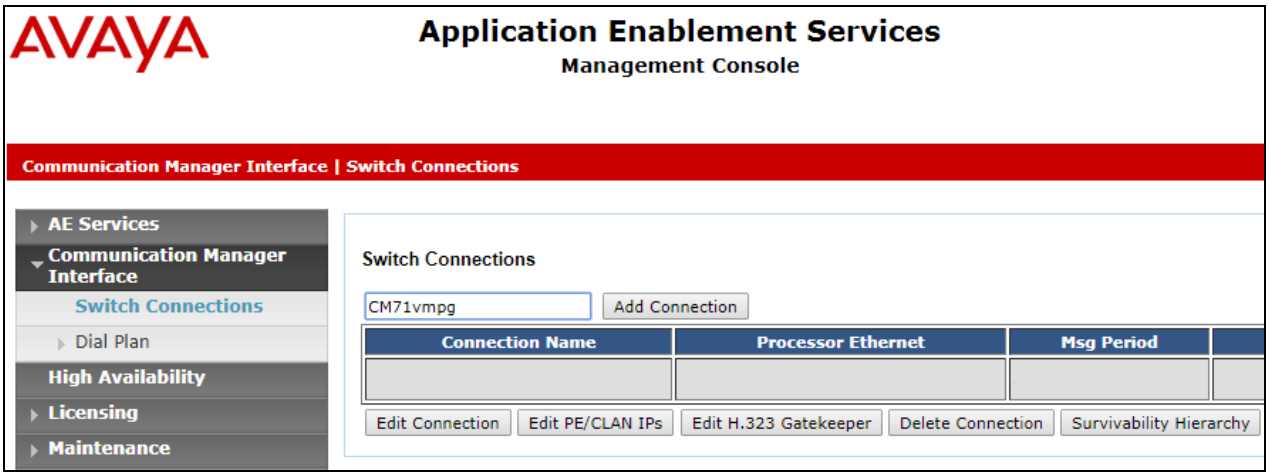
The Application Enablement Services Management Console appears displaying the **Welcome to OAM** screen (not shown). Select **AE Services** and verify that the TSAPI Service is licensed by ensuring that **TSAPI Service** is in the list of services and that the **License Mode** is showing **NORMAL MODE**.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



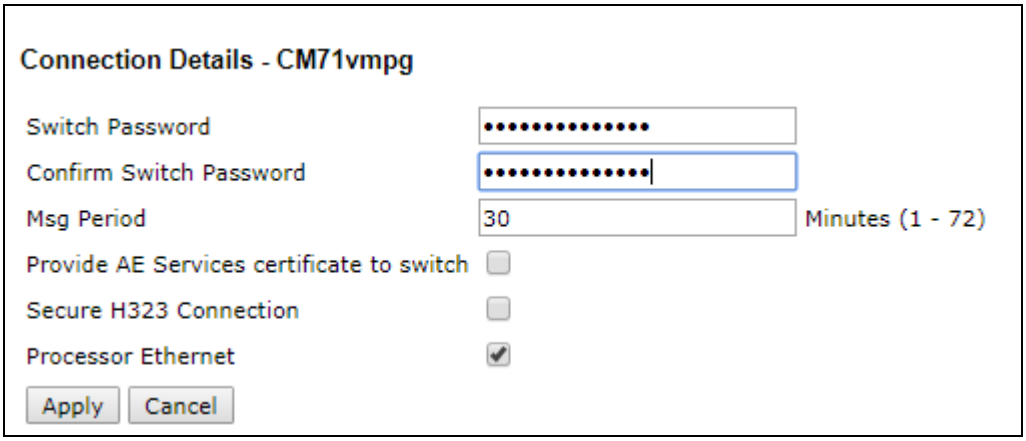
Service	Status	State	License Mode
ASAI Link Manager	N/A	Running	N/A
CVLAN Service	ONLINE	Running	NORMAL MODE
DLG Service	OFFLINE	Running	N/A
DMCC Service	ONLINE	Running	NORMAL MODE
TSAPI Service	ONLINE	Running	NORMAL MODE
Transport Layer Service	N/A	Running	N/A

6.1. Configure Switch Connection

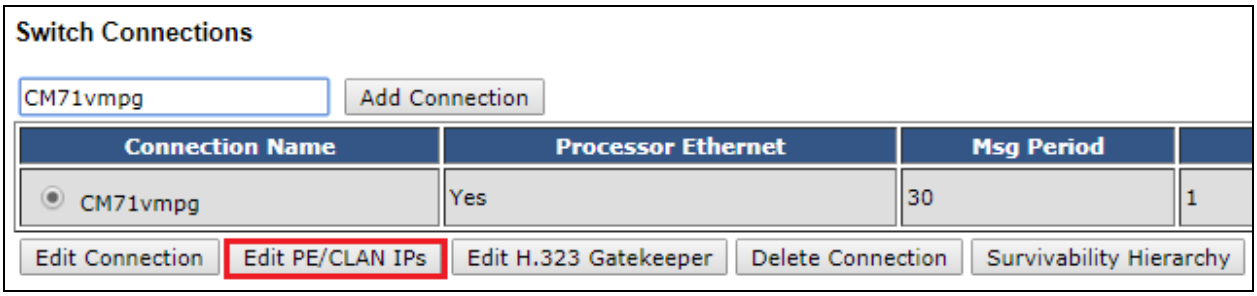
From the AES Management Console navigate to **Communication Manager Interface → Switch Connections** to set up a switch connection. Enter in a name for the Switch Connection to be added and click the **Add Connection** button. A Switch Connection defines a connection between the Application Enablement Services server and Communication Manager.



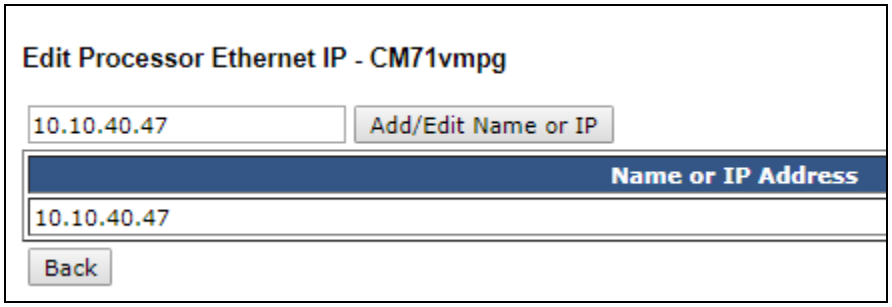
In the resulting screen enter the **Switch Password**, the Switch Password must be the same as that entered into Communication Manager AE Services Administration screen via the **change ip-services** command, described in **Section 5.3.2**. Default values may be accepted for the remaining fields. Click **Apply** to save changes.



From the **Switch Connections** screen, select the radio button for the recently added switch connection and select the **Edit CLAN IPs** button (not shown).

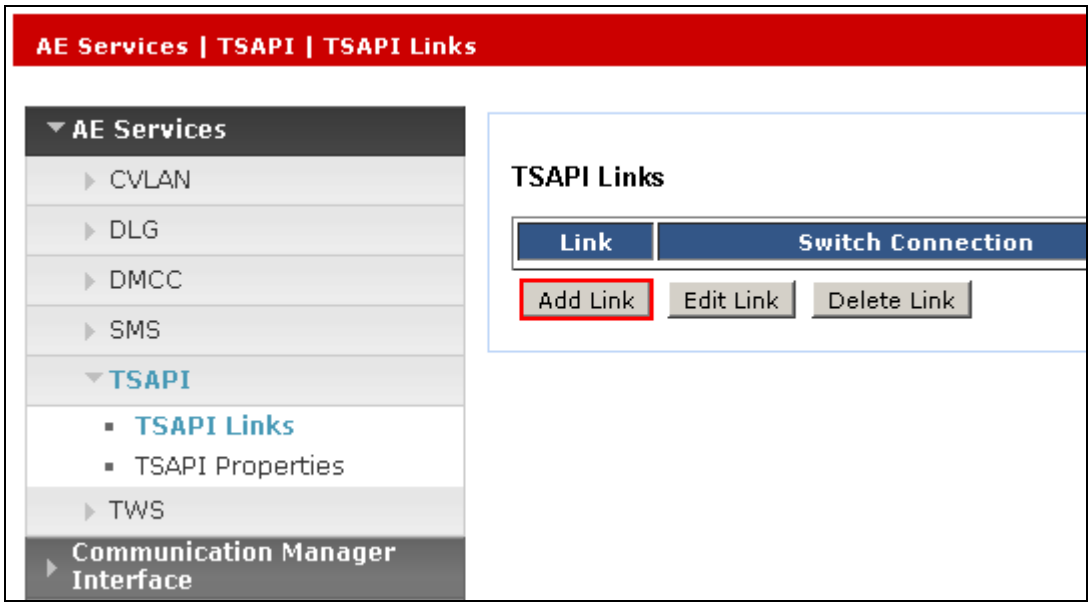


In the resulting screen, enter the IP address of the **procr** as shown in **Section 5.3.1** that will be used for the AES connection and select the **Add/Edit Name or IP** button.



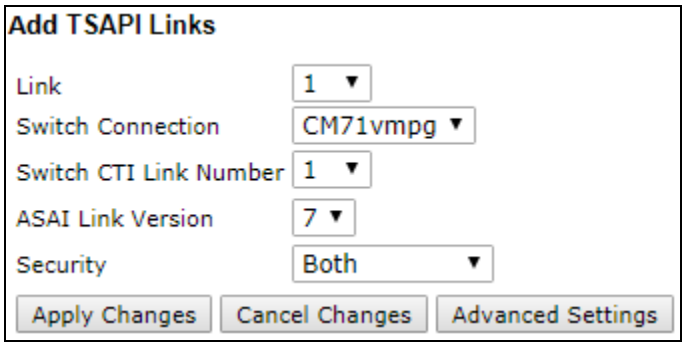
6.2. Configure TSAPI Link

Navigate to **AE Services → TSAPI → TSAPI Links** to configure the TSAPI CTI link. Click the **Add Link** button to start configuring the TSAPI link.

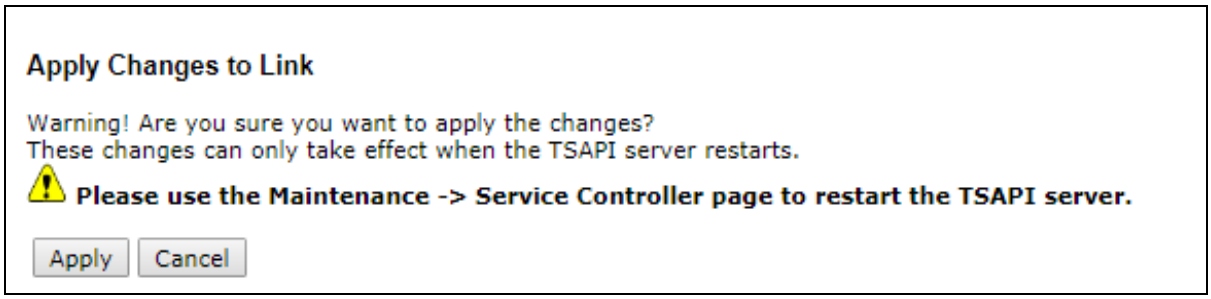


On the **Add TSAPI Links** screen, enter the following values:

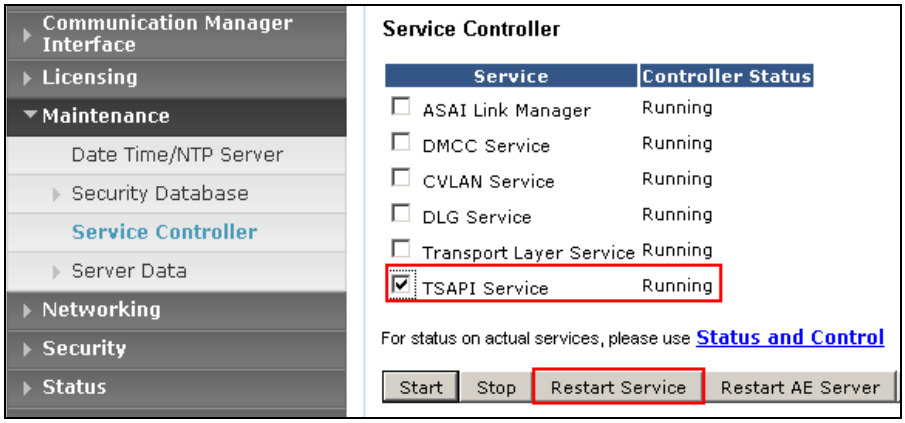
- **Link:** Use the drop-down list to select an unused link number.
- **Switch Connection:** Choose the switch connection **CM71vmpg**, which has already been configured in **Section 6.1**, from the drop-down list.
- **Switch CTI Link Number:** Corresponding CTI link number configured in **Section 5.3.3**.
- **ASAI Link Version:** This can be left at the default value of **7**.
- **Security:** This can be left at the default value. The value **both** was used in this test.
- Once completed, select **Apply Changes**.



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**.

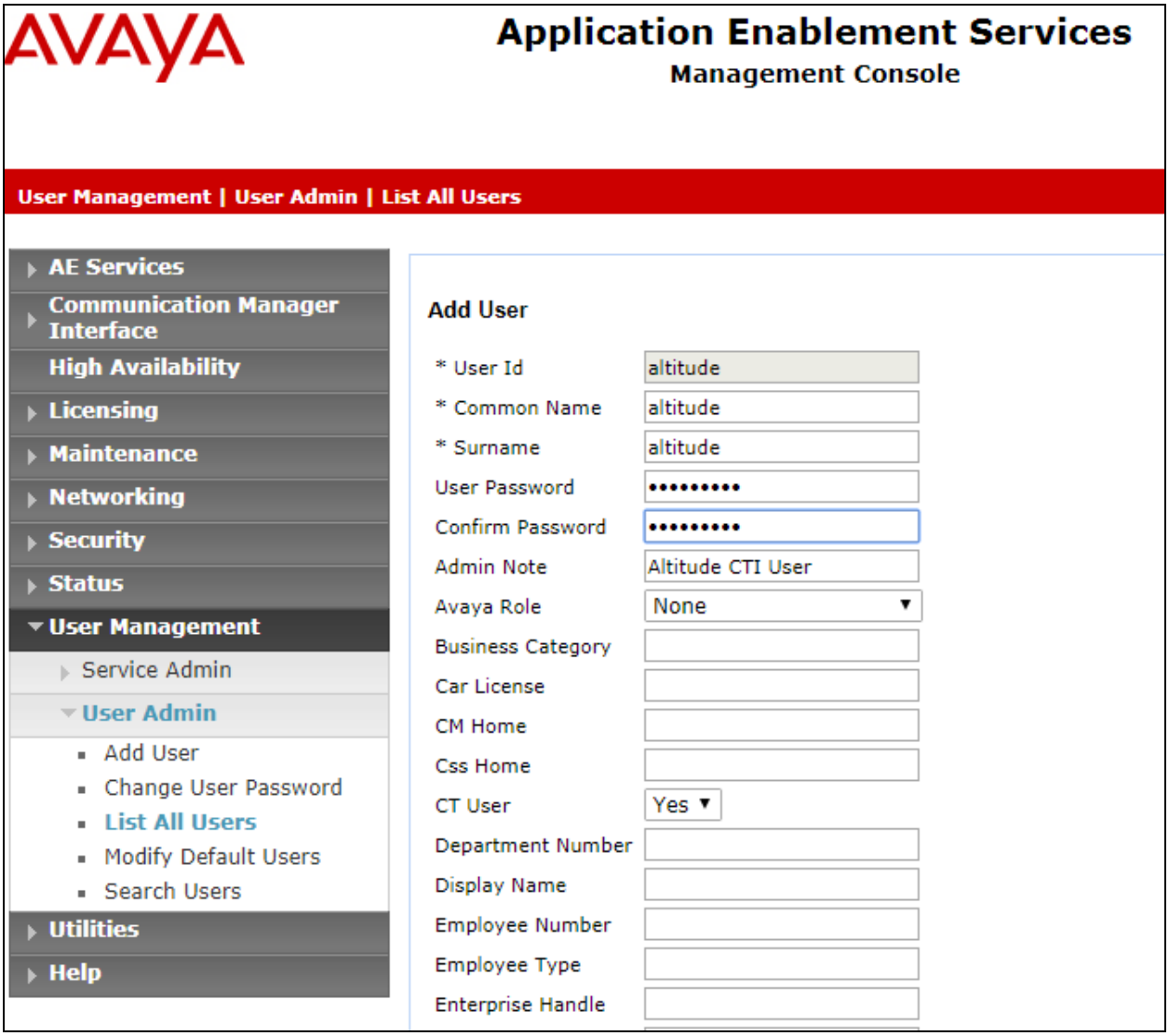


6.3. Create Avaya CTI User

A User ID and password needs to be configured for the Altitude uCI 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:

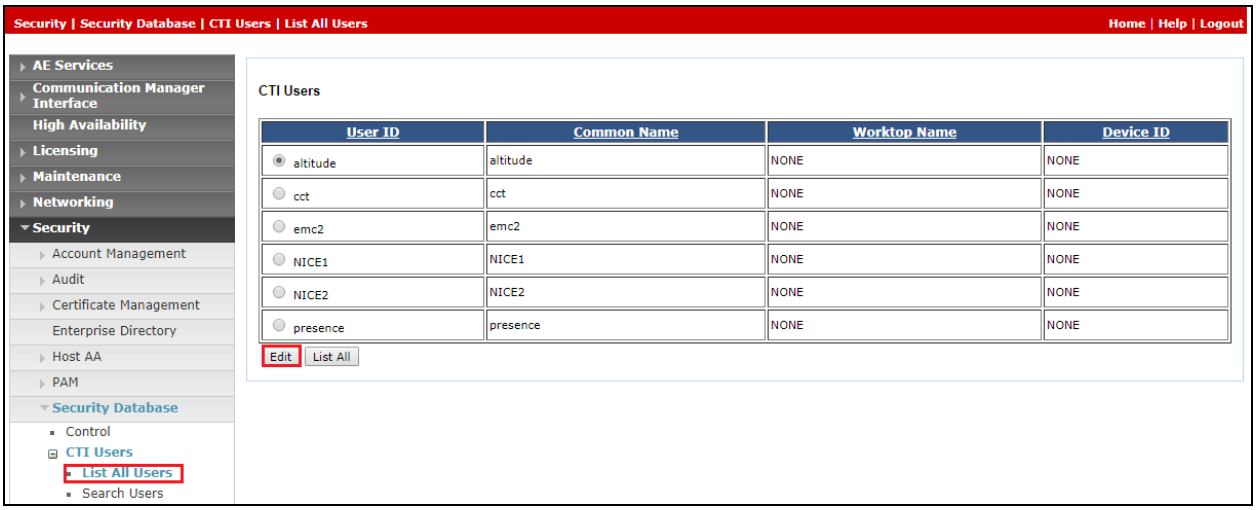
- **User Id** - This will be used by the Altitude uCI server in **Section 8.1.1**.
- **Common Name** and **Surname** - Descriptive names need to be entered.
- **User Password** and **Confirm Password** - This will be used with the **User Id** in **Section 8.1.1**.
- **CT User** - Select **Yes** from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

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

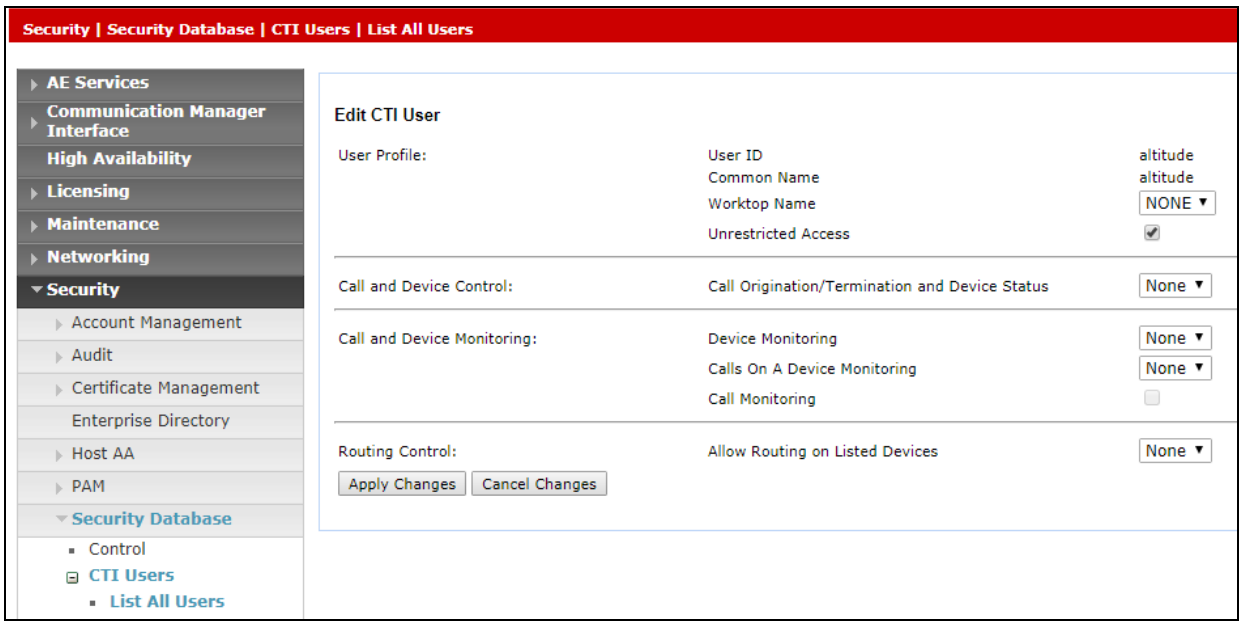


6.4. Enable Unrestricted Access for CTI User

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.



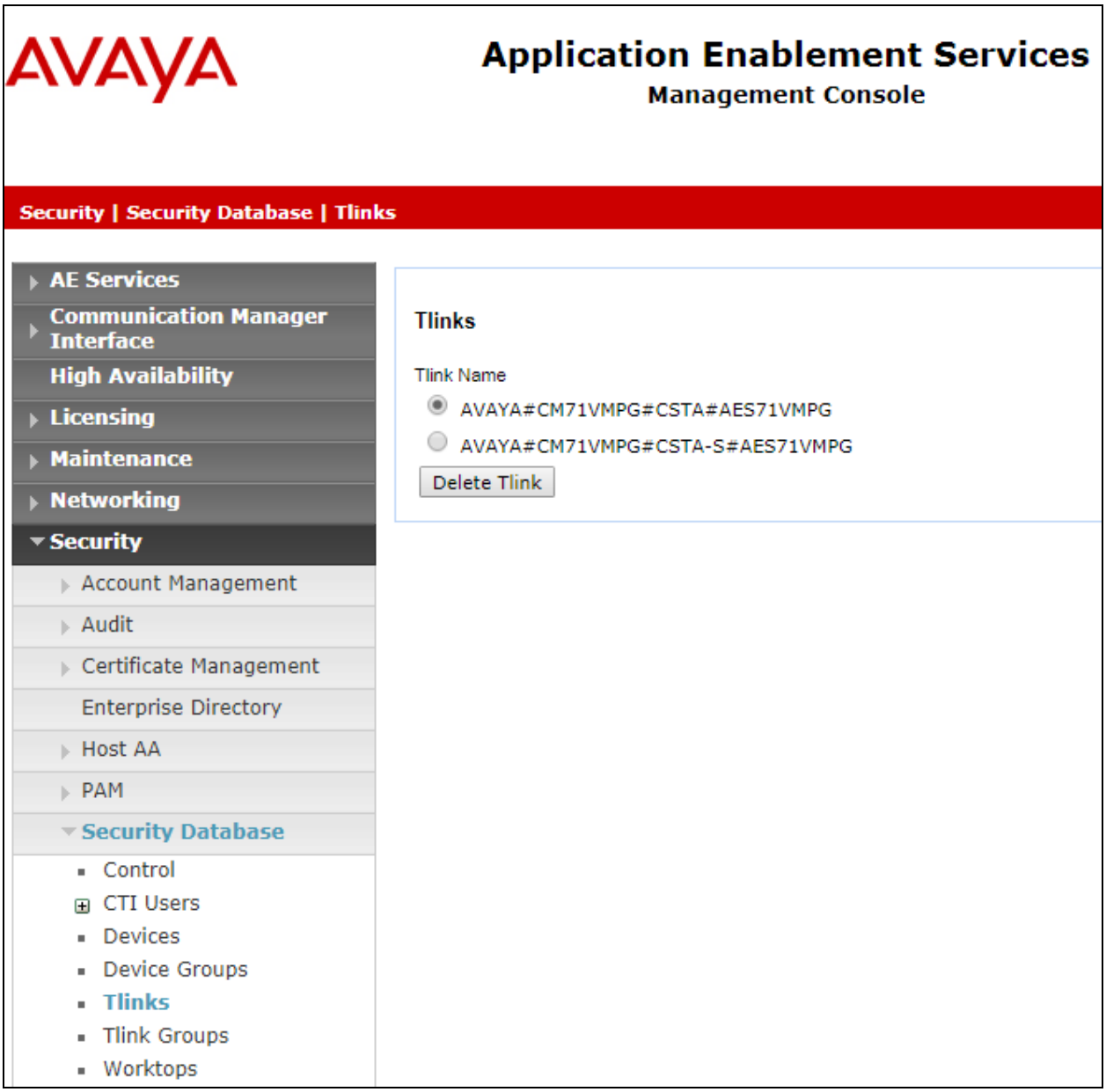
The **Edit CTI User** screen appears. Check the **Unrestricted Access** box and **Apply Changes** at the bottom of the screen.



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 uCI in **Section 8.1.1**.



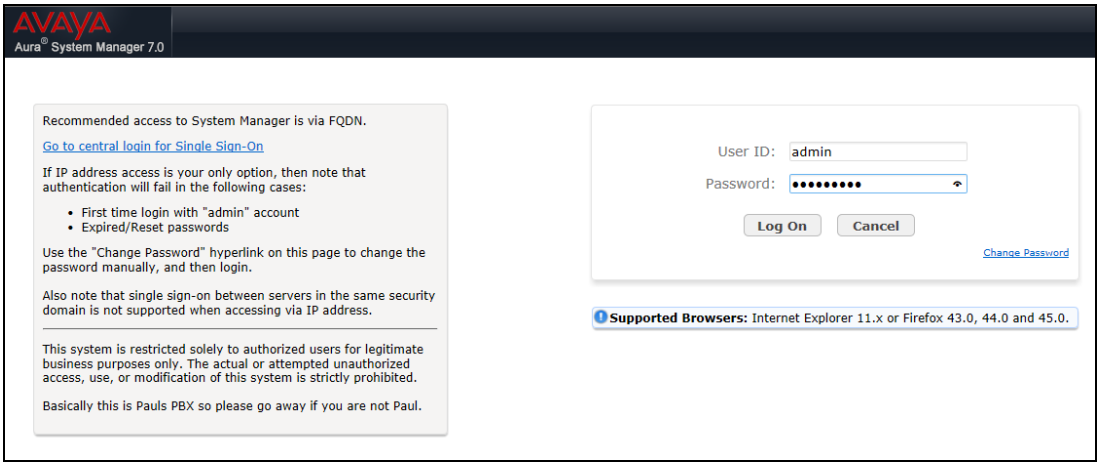
7. Configure Avaya Aura® Session Manager

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

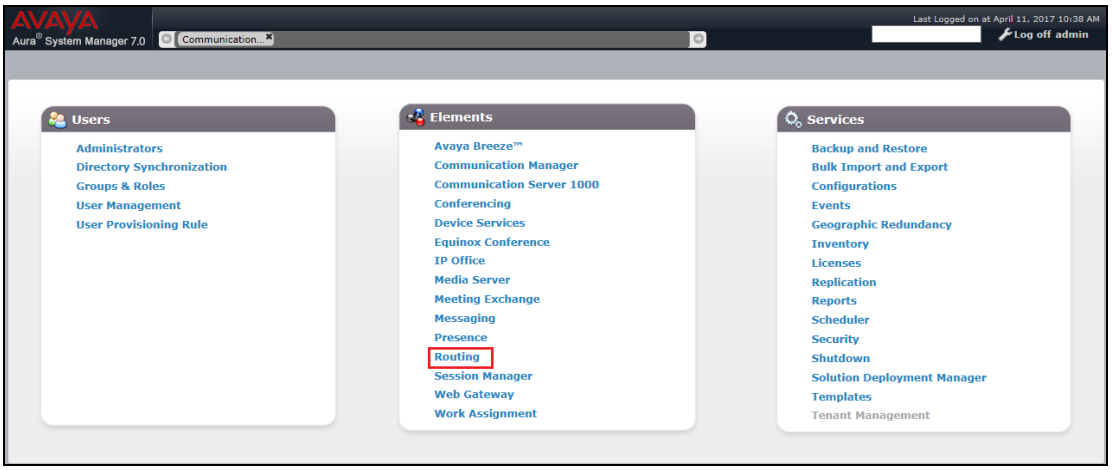
- Log in to Avaya Aura® System Manager
- Administer SIP Domain
- Administer Location
- Administer SIP Entities
- Administer Routing Policies
- Administer Dial Patterns

7.1. Log in to Avaya Aura® System Manager

Access System Manager using a Web Browser by entering **http://<FQDN >/SMGR**, where **<FQDN>** is the fully qualified domain name of System Manager or **http://<IP Adddress >/SMGR**. Log in using appropriate credentials.

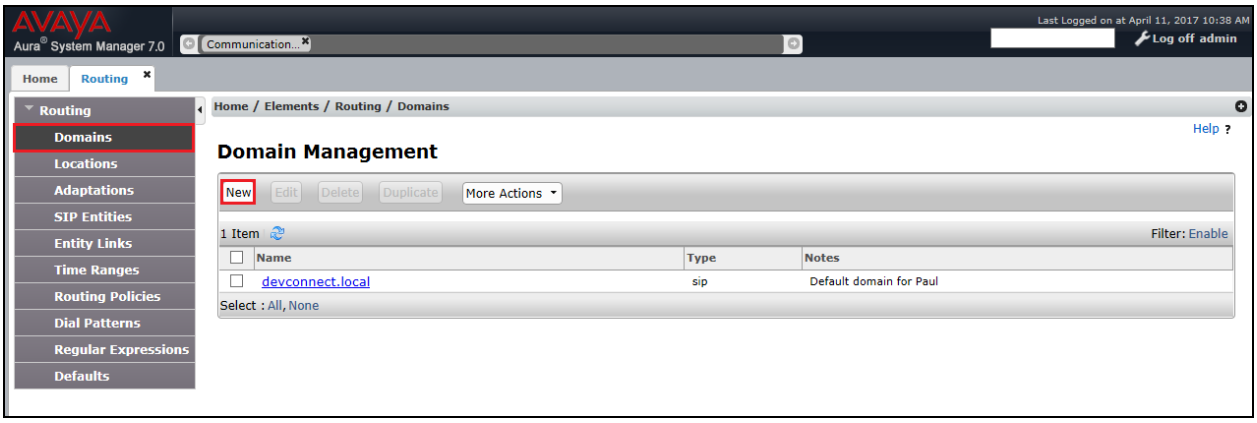


Once logged in click on **Routing** highlighted below.

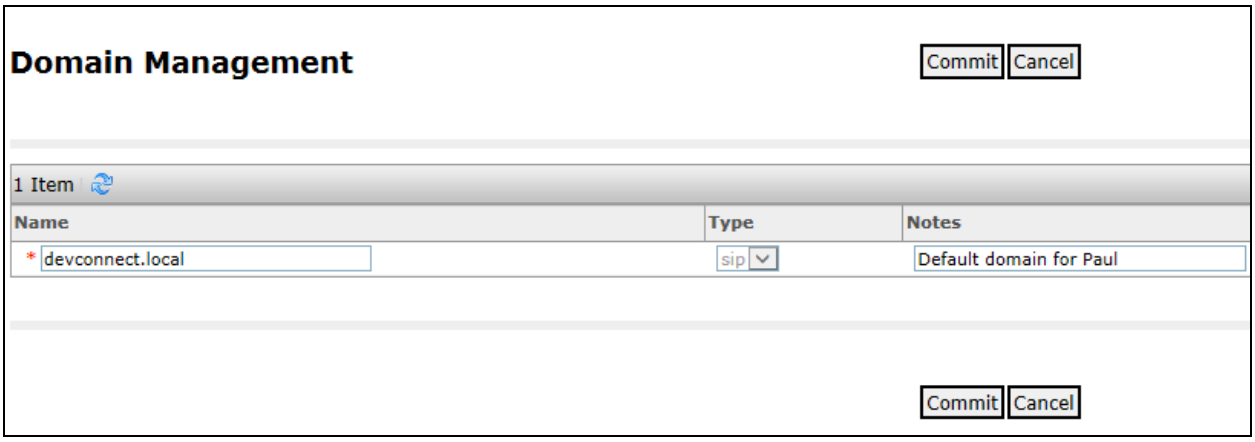


7.2. Administer SIP Domain

Click on **Domains** in the left window. If there is not a domain already configured click on **New** highlighted below.



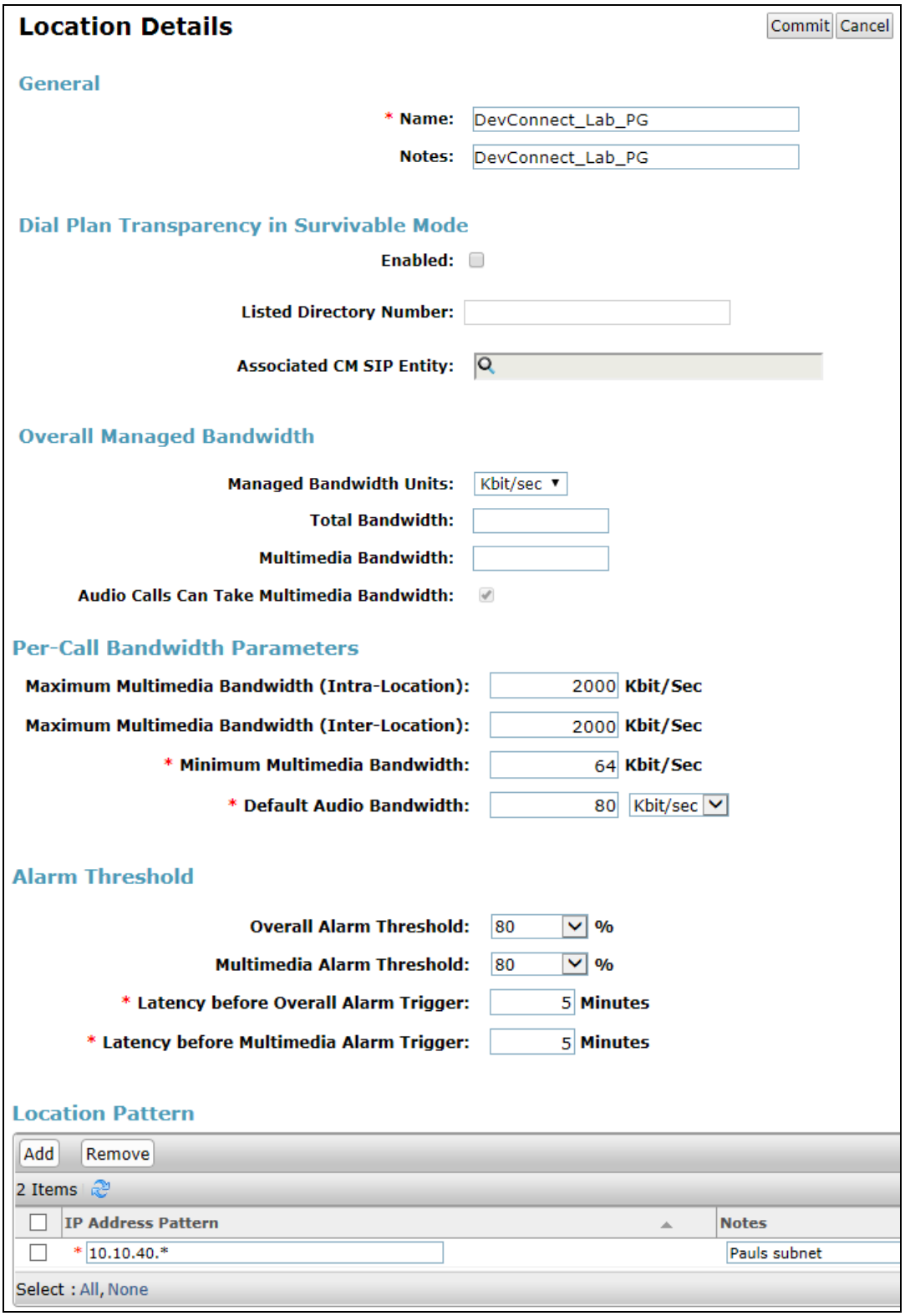
Note the domain **Name** used in the compliance testing was **devconnect.local** and the **Type** should be set to **sip**. This domain is also referenced in **Section 5.4**. Click on **Commit** to save this configuration.



7.3. Administer Location

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** as is highlighted below to add a new location.

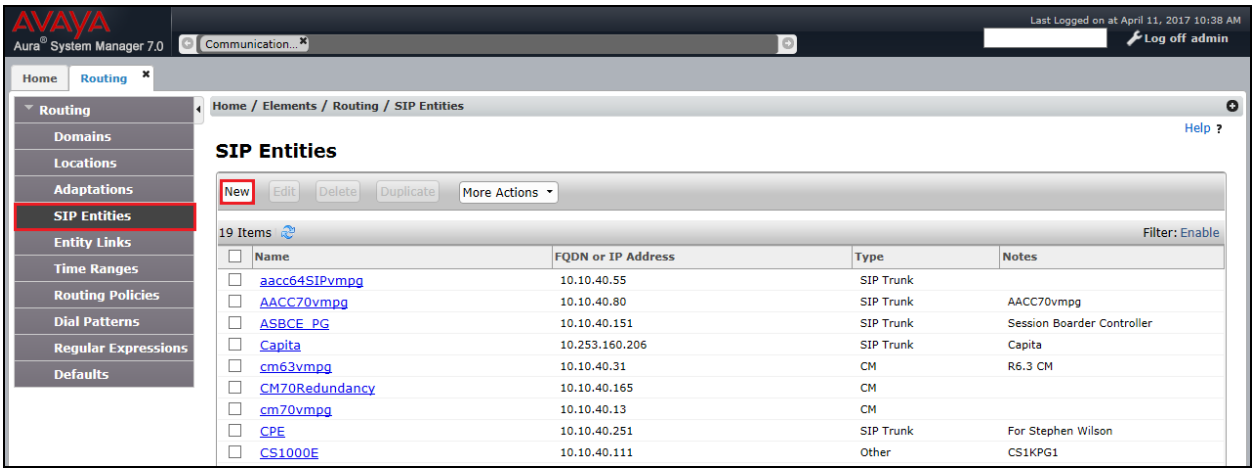
Enter a suitable **Name** and add the IP address ranges at the bottom of the screen under **Location Pattern** and click on **Commit** once this is done.



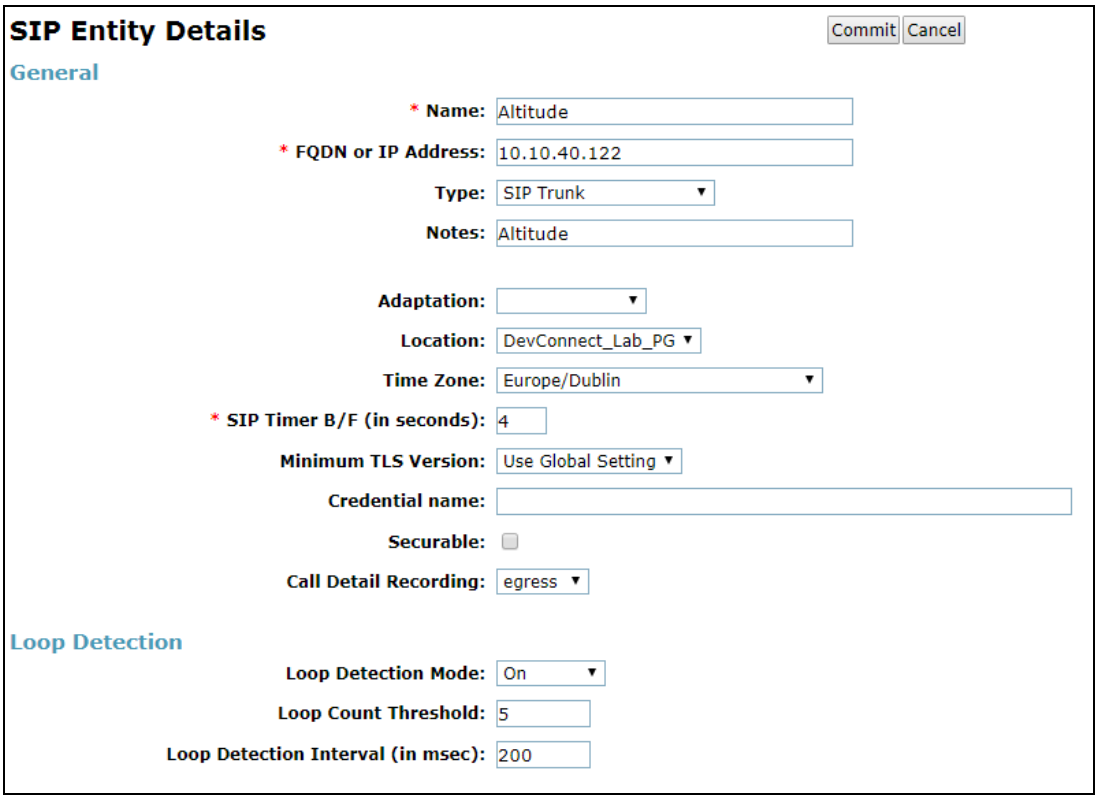
7.4. Configure Altitude Communication Server SIP Entity

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.

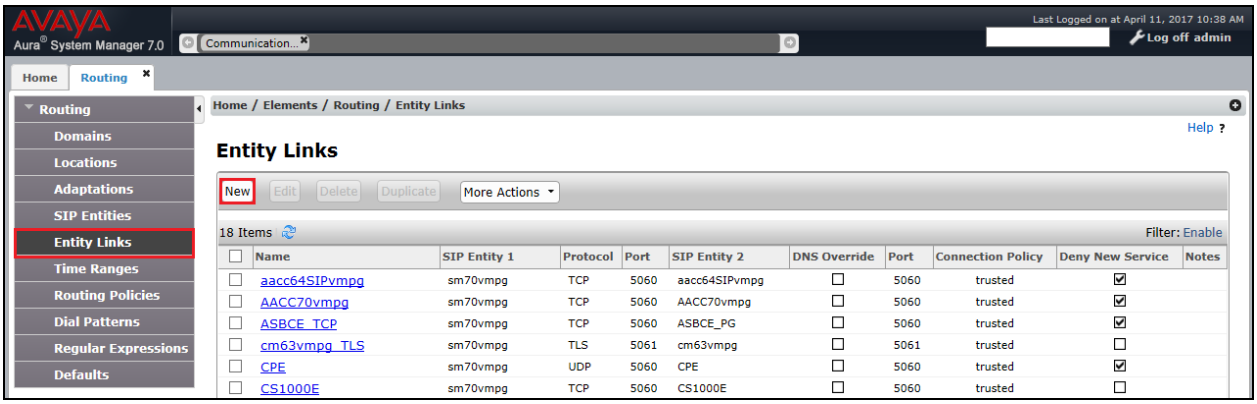


Enter a suitable **Name** for the new SIP Entity and the **IP Address** of the ACS server. **Type** should be set to **SIP Trunk**. Enter the correct **Time Zone** and **Location** and click on **Commit**.

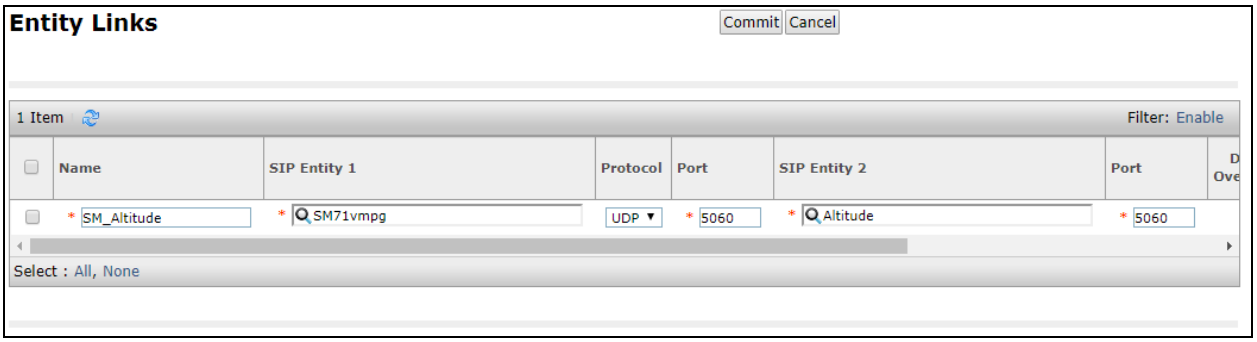


7.5. Configure Altitude Communication Server SIP Entity Link

An Entity Link was added for ACS. Click on **Entity Links** in the left column and select **New** in the main window.

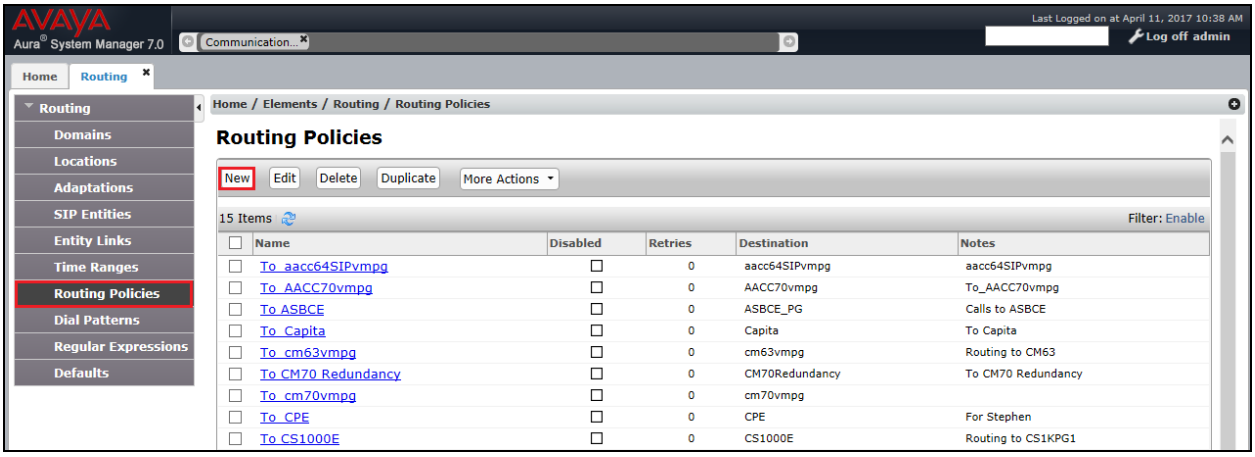


Enter a suitable **Name** for the Entity Link and select the **Session Manager** SIP Entity for **SIP Entity 1** and the newly created ACS SIP Entity for **SIP Entity 2**. Ensure that **UDP** is selected for the **Protocol** and that **Port 5060** is used. Click on **Commit** once finished to save the new Entity Link.

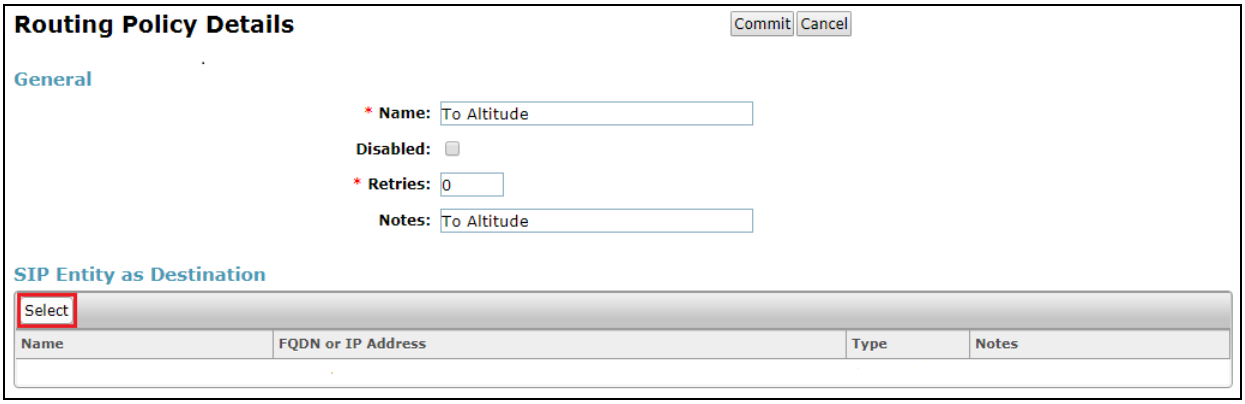


7.6. Configure Routing Policy for Altitude Communication Server

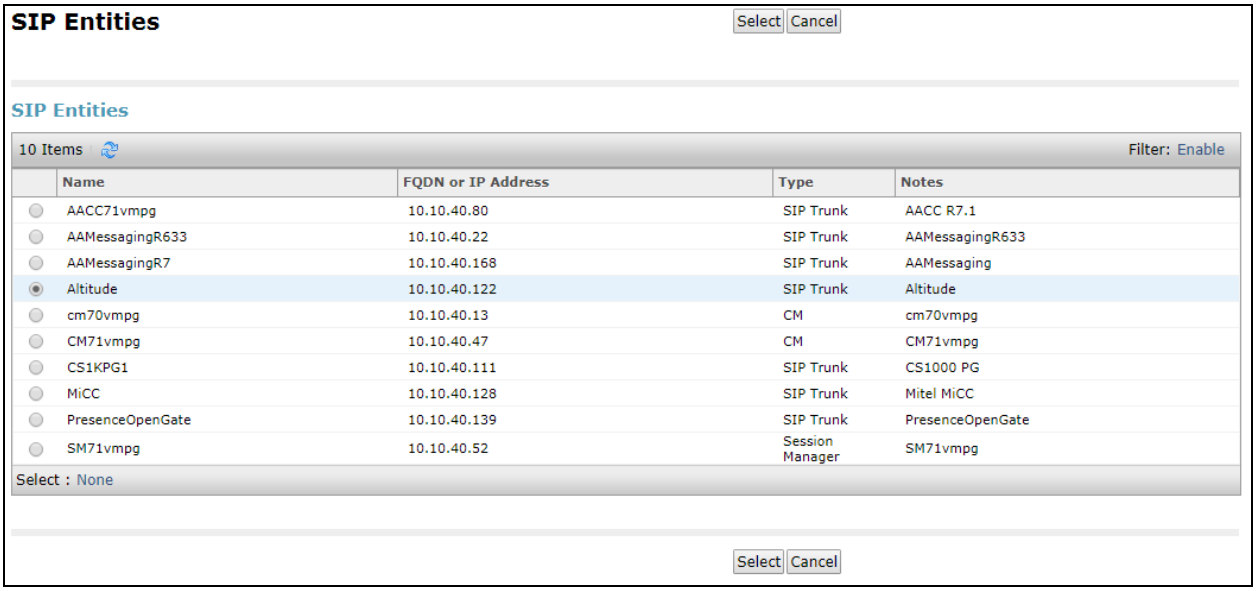
Click on **Routing Policies** in the left window and select **New** in the main window.



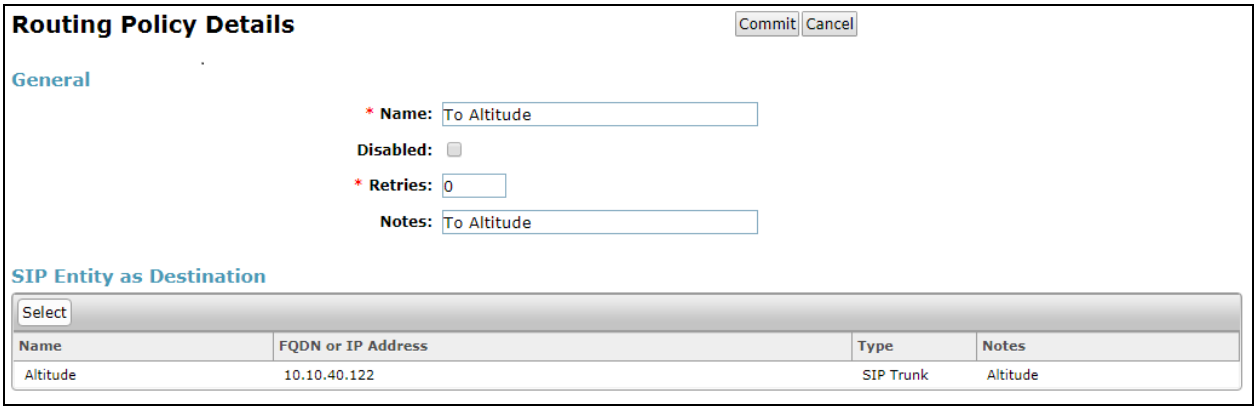
Enter a suitable **Name** for the Routing Policy and click on **Select** under **SIP Entity as Destination**, highlighted below.



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

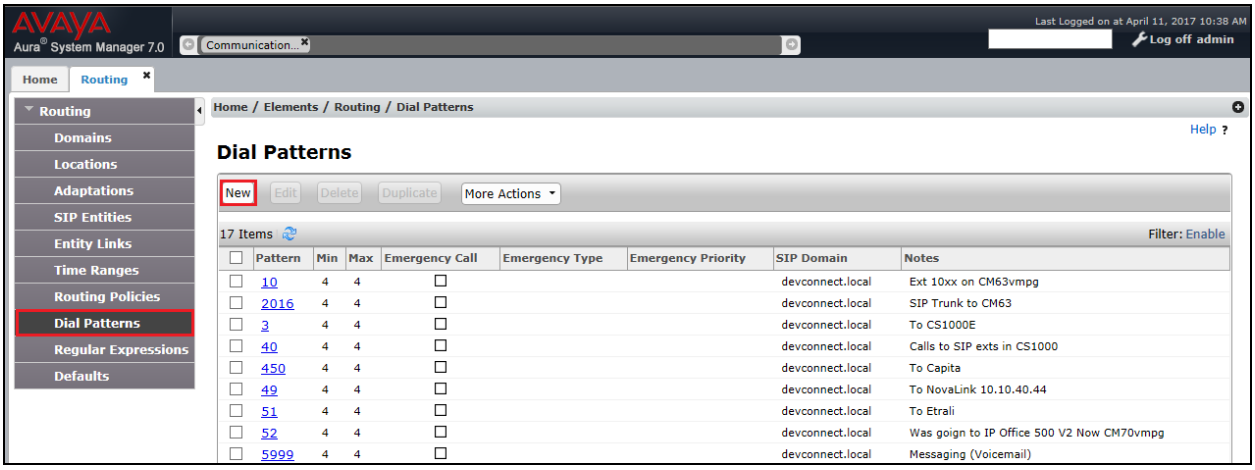


The selected destination is now shown, click on **Commit** to save this.

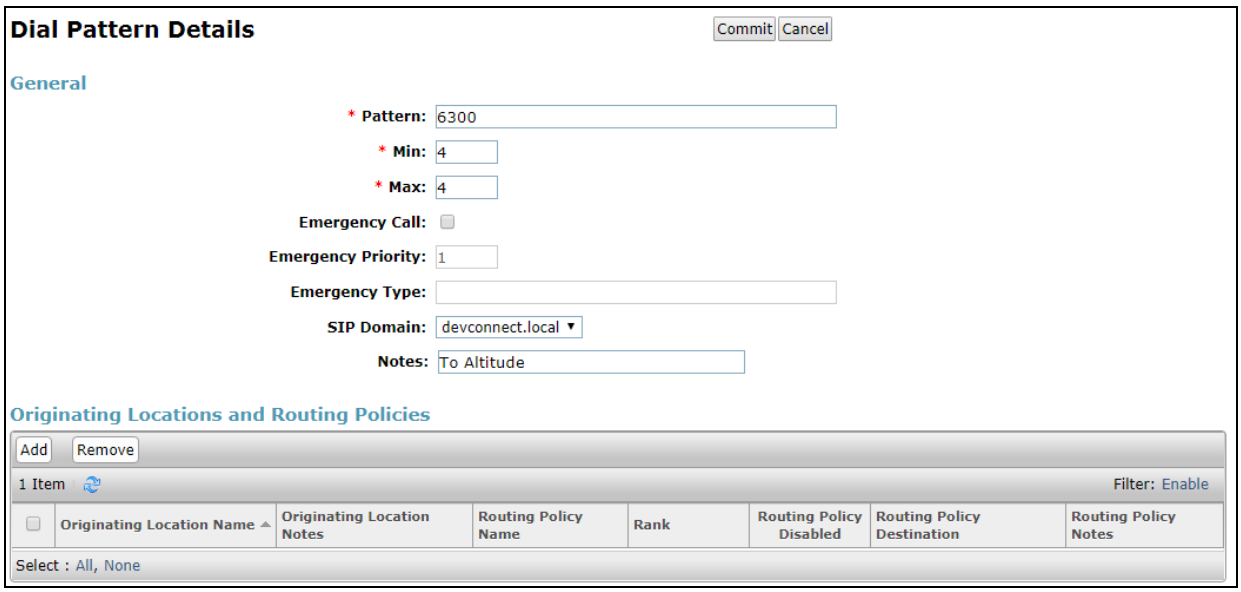


7.7. Configure Dial Pattern for Altitude Communication Server

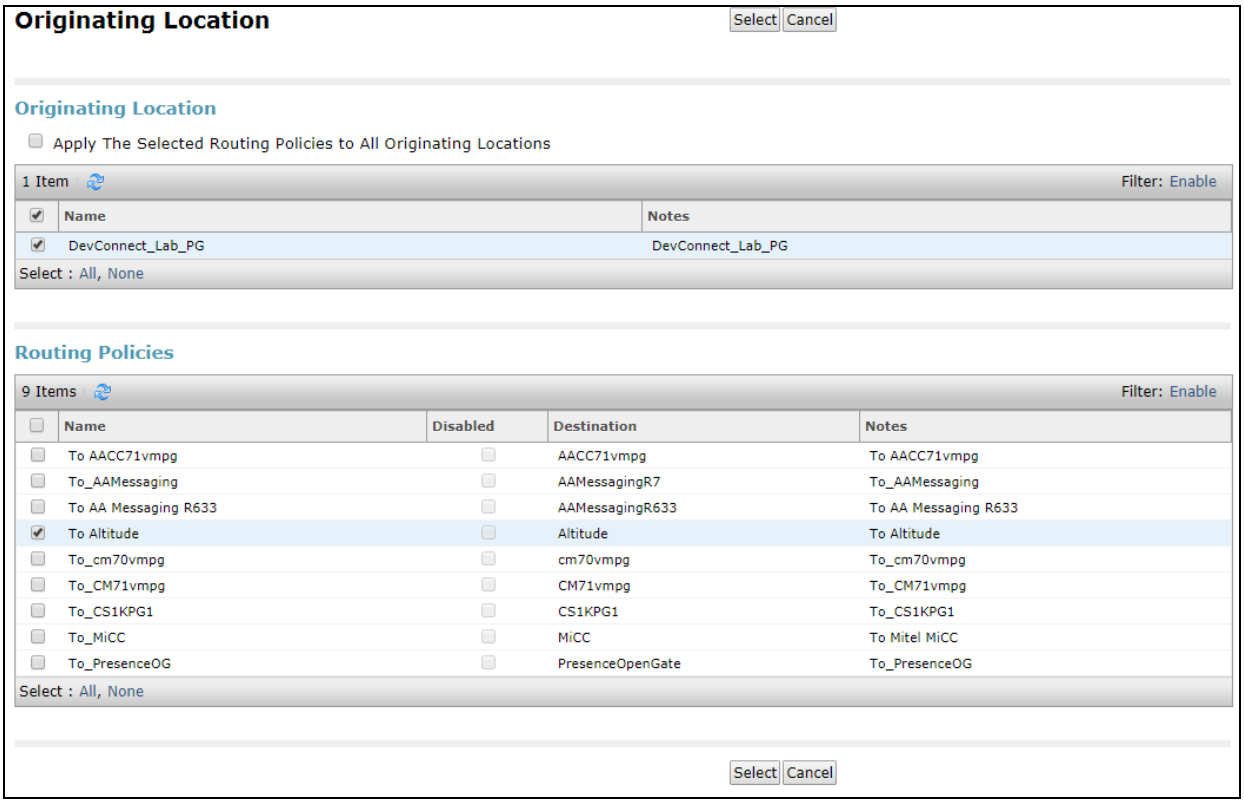
Select **Dial Patterns** in the left window and select **New** in the main window.



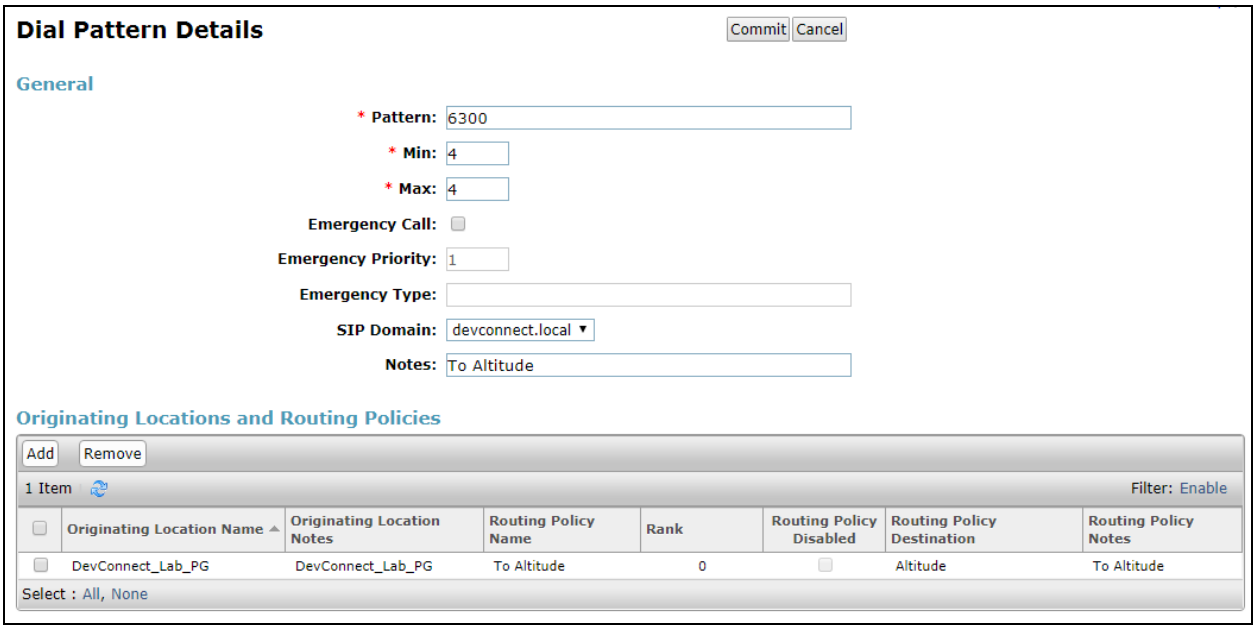
Enter the required digits for the Routing Pattern, in the example below **6300** is used. This ensures that when 6300 is dialled it will route to the ACS. Enter the appropriate domain for **SIP Domain** in this example the domain created in **Section 6.2** is added. Click on **Add** under **Originating Locations and Routing Policies** in order to select this Routing Policy.



Select the Originating Location, this will be the location added in **Section 7.3** and select the newly created Routing Policy for ACS.



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



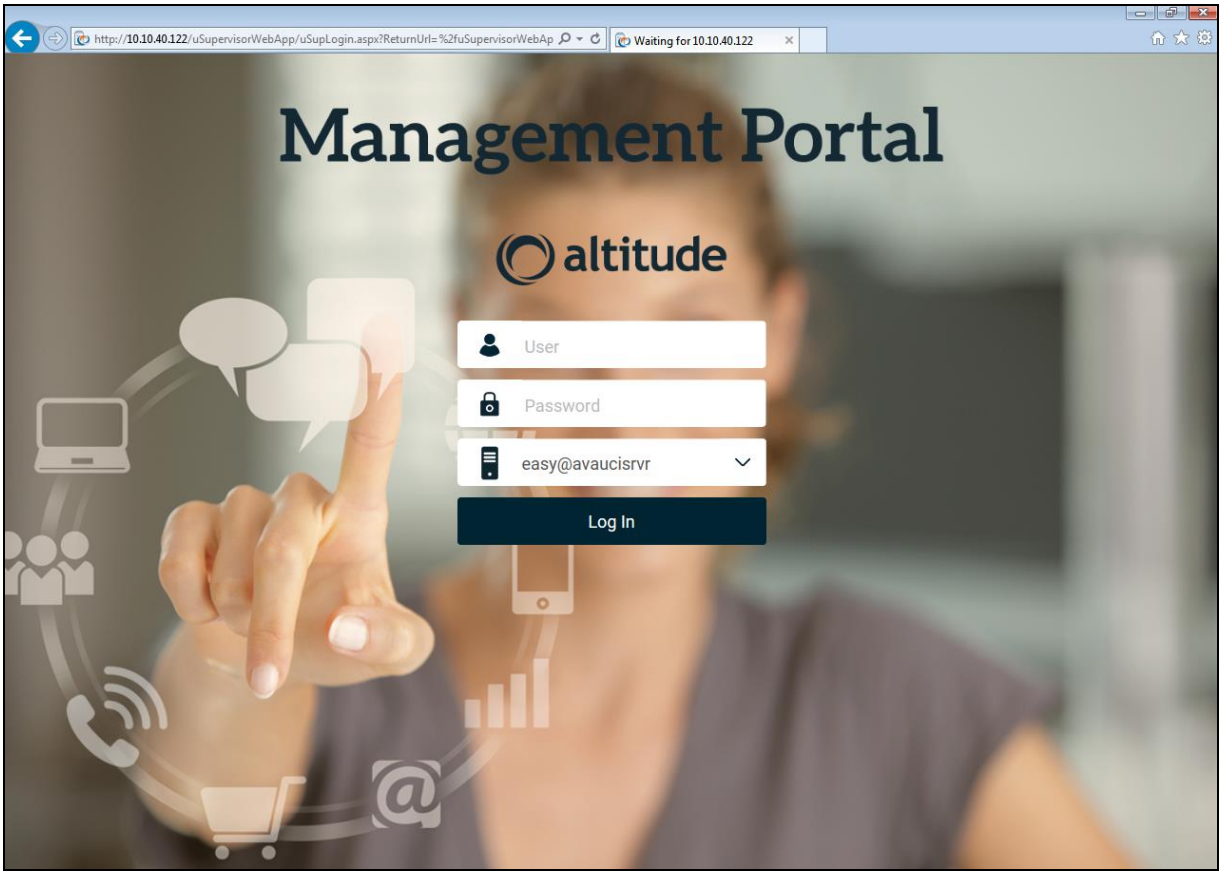
8. Configure Altitude uCI

There are two modules to be configured, the Altitude uCI server connecting to AES and the Altitude Communication Server (ACS) connecting to Session Manager.

8.1. Configure Altitude uCI Server

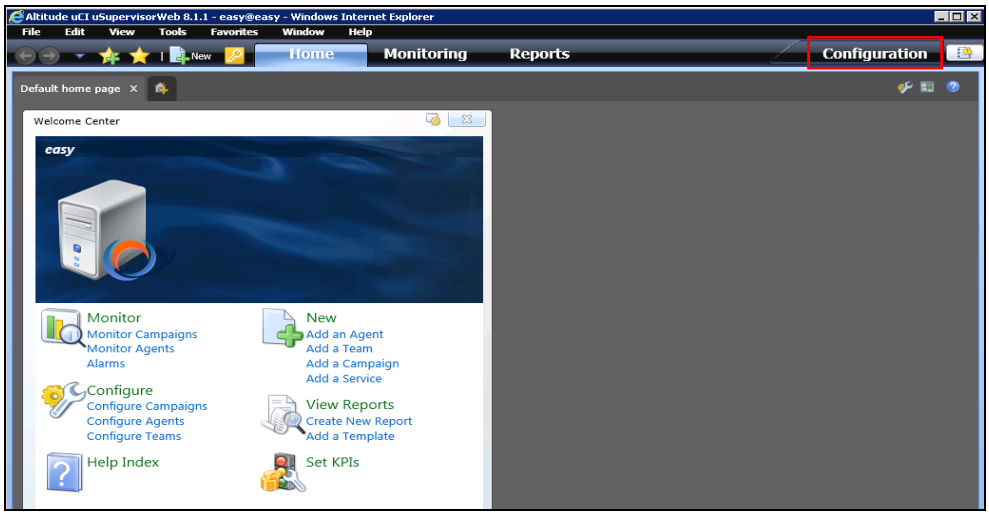
Note: Windows Internet Explorer R9.0, R10.0 and R11.0, and Firefox 35 are the only supported browsers with this release of Altitude uCI. Windows Internet Explorer R11.0 was used during compliance testing.

Open a web session to **http://<server IP Address>/uSupervisorWebApp**. Enter the proper credentials and select the Assisted Server to log into and click on **Login**.

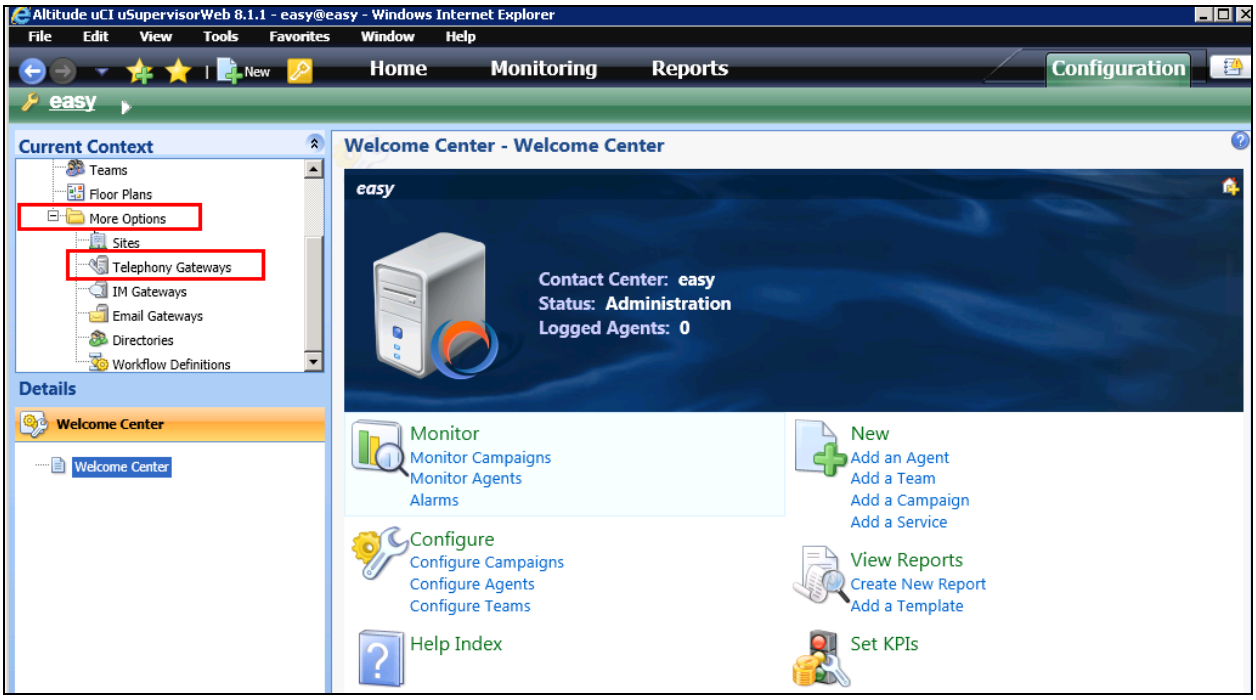


8.1.1. Configure Telephony Gateway

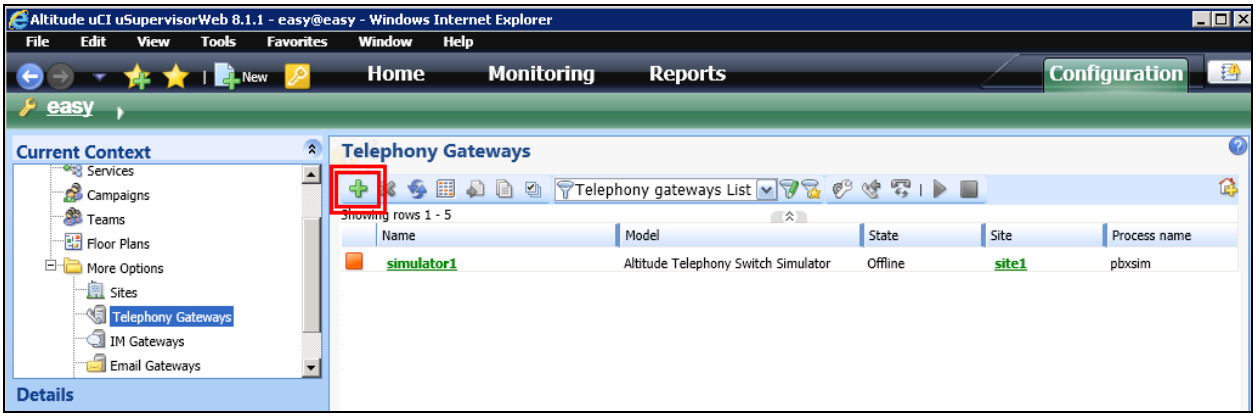
Once logged in select **Configuration** as highlighted below.



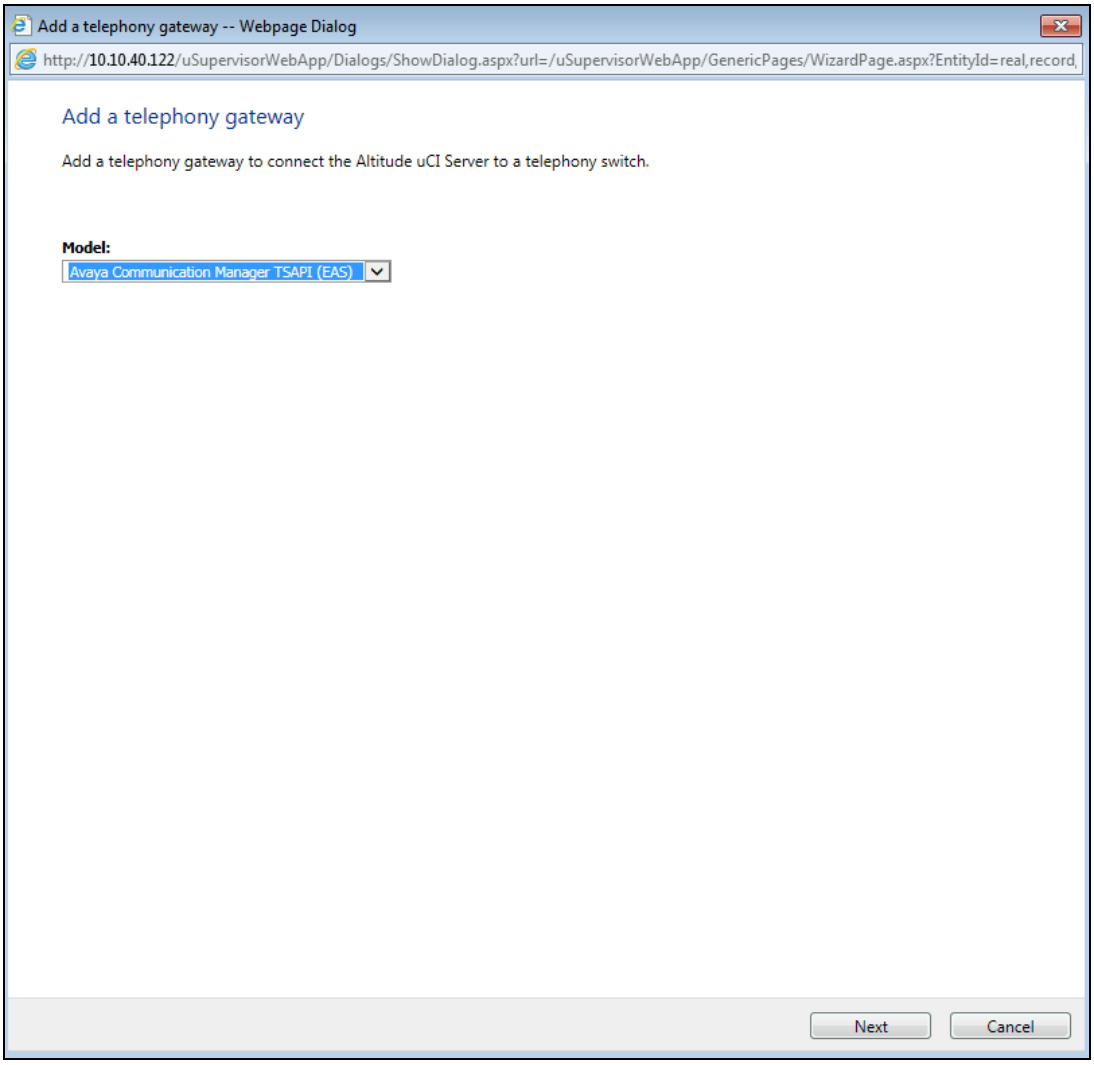
Expand **More Options** in the left window and select **Telephony Gateways**.



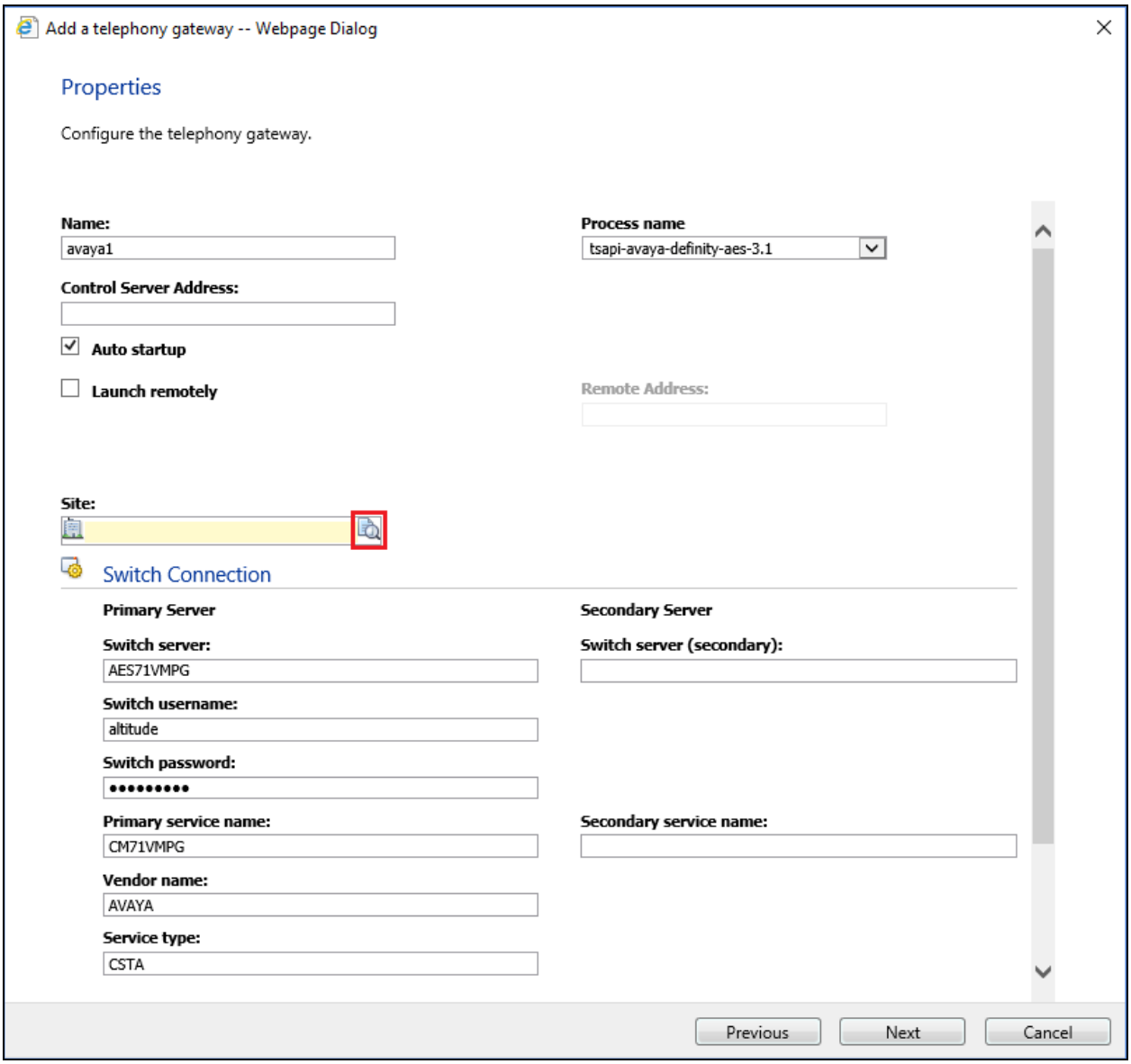
Select the "+" icon that is highlighted below to add the Avaya Telephony Gateway.



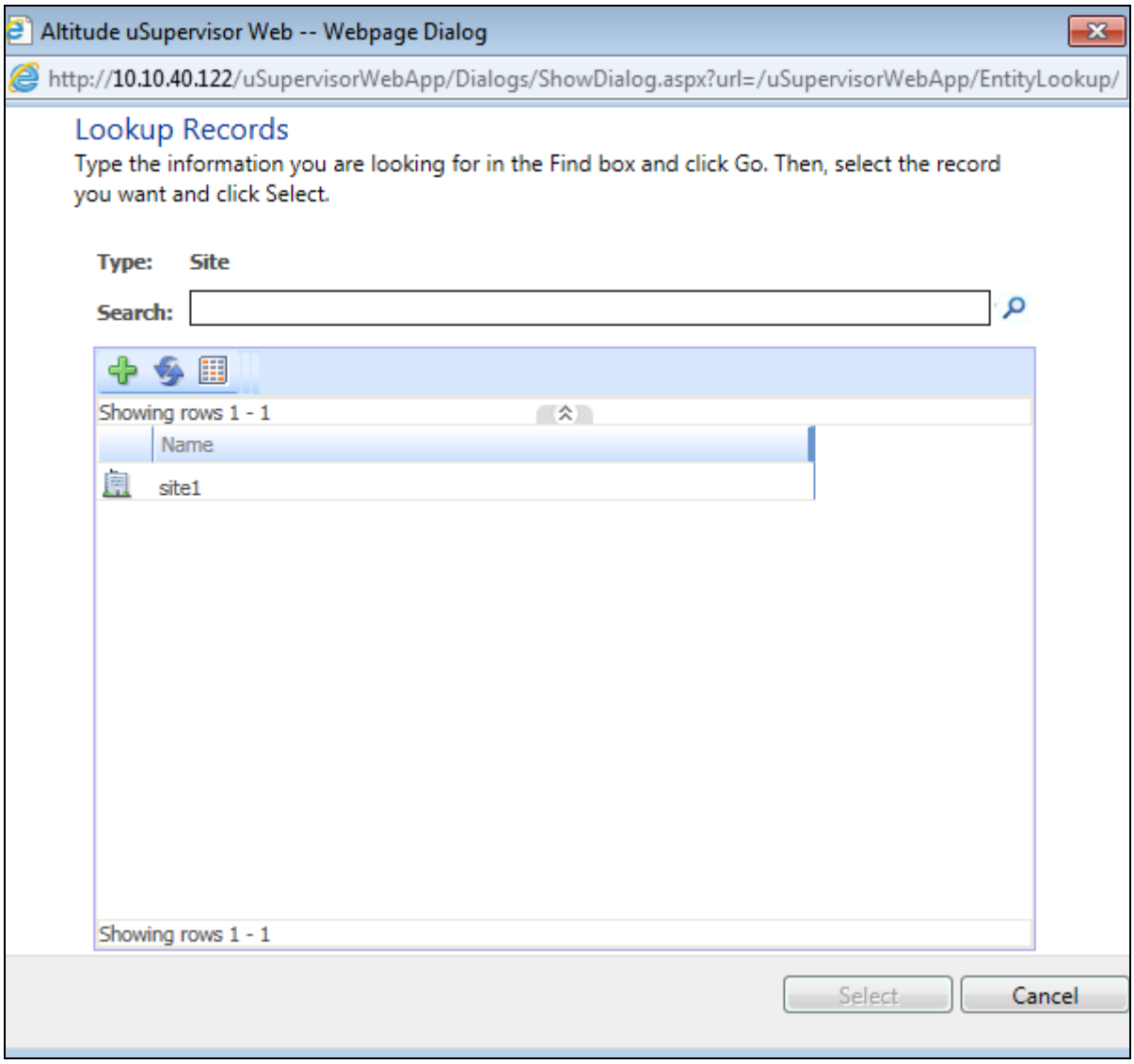
Select **Avaya Communication Manager TSAPI (EAS)** as the **Model** from the drop down menu.



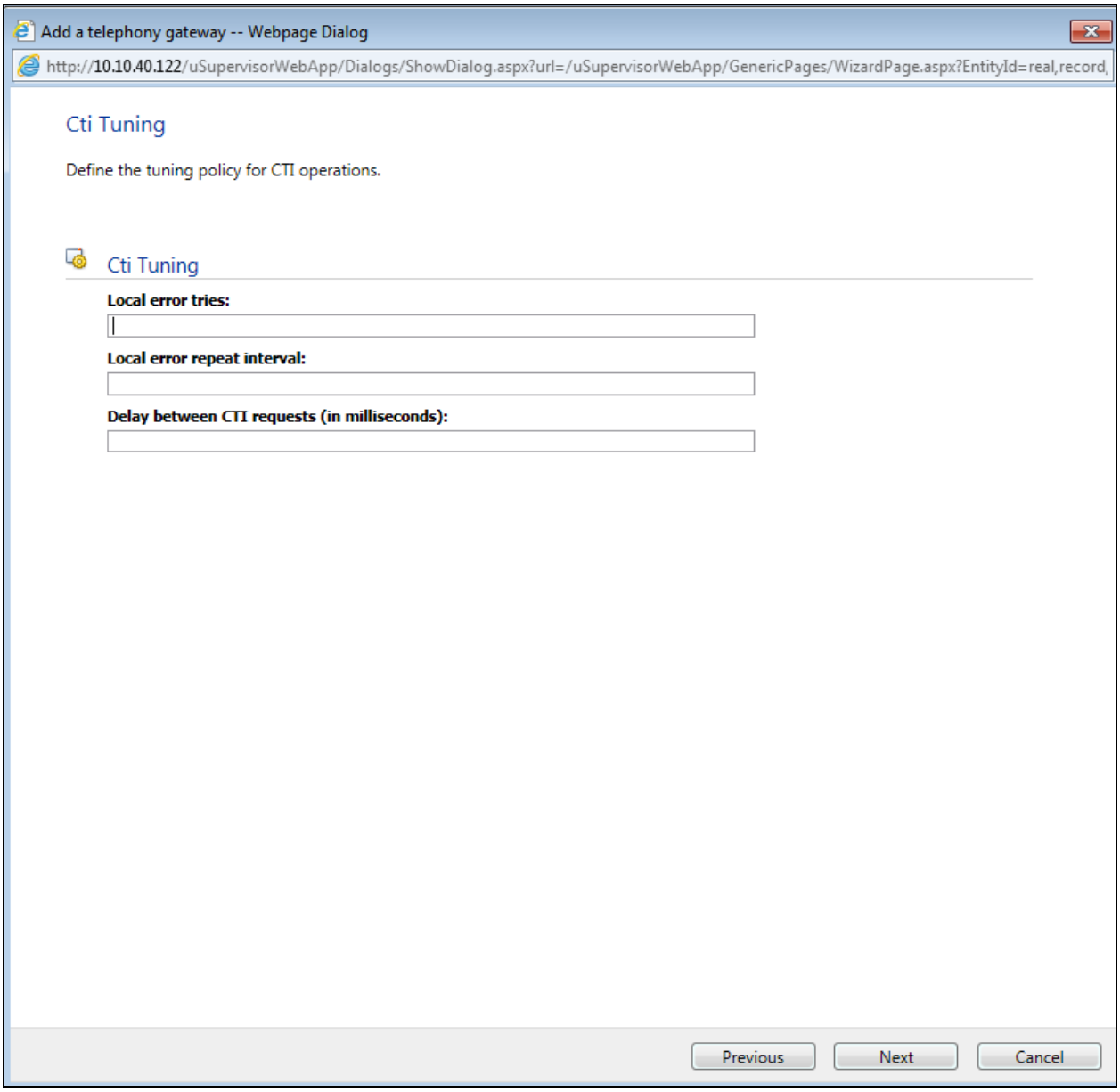
A name for the gateway is mandatory in this case **avaya1** was chosen. The process name is left as the default selection. Under **Switch Connection** enter the information as shown below, this is information that is used to connect to the AES and can be obtained from the AES Tlink information shown in **Section 6.5**. Click on the search icon highlighted beside **Site** to add a new site.



A site may already be configured as was the case for compliance testing, so this **site1** was selected. A new site can be created if there is none already present.

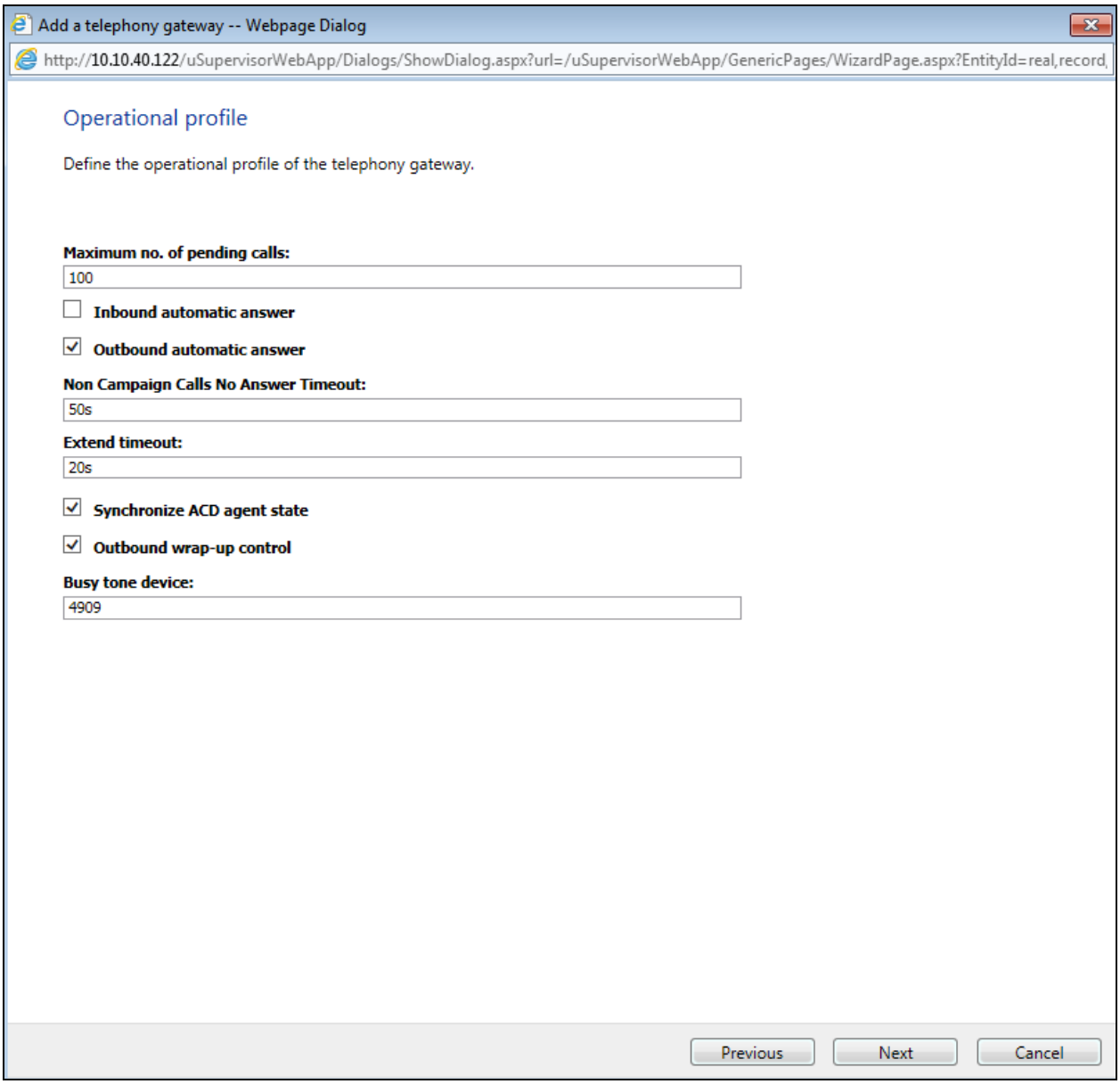


Select **Next** without filling in any information.

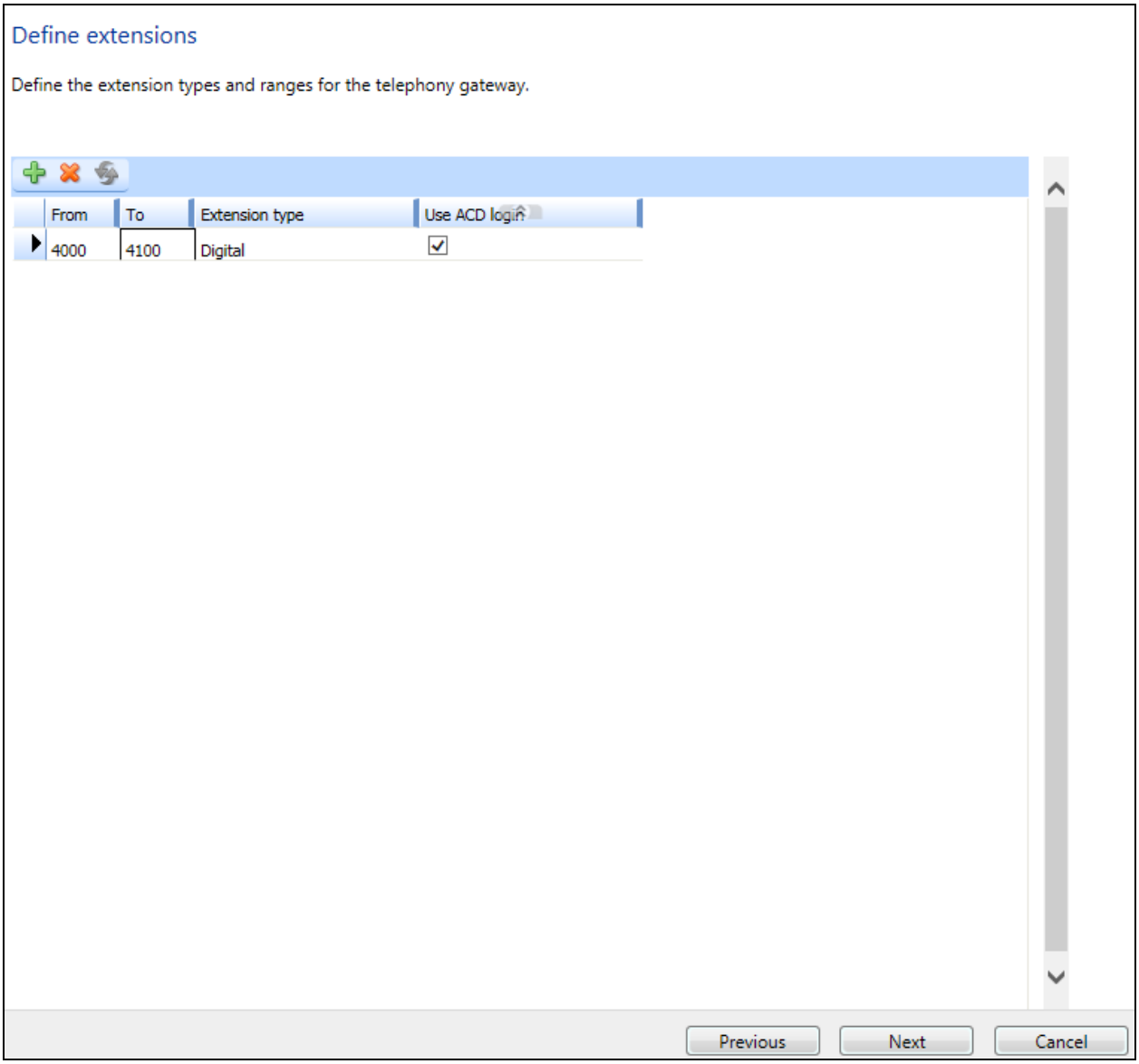


These settings are typical for most Contact Centers but can be changed by the Contact Center administrator at any stage depending on how the agents are to answer the calls. Select **Next**.

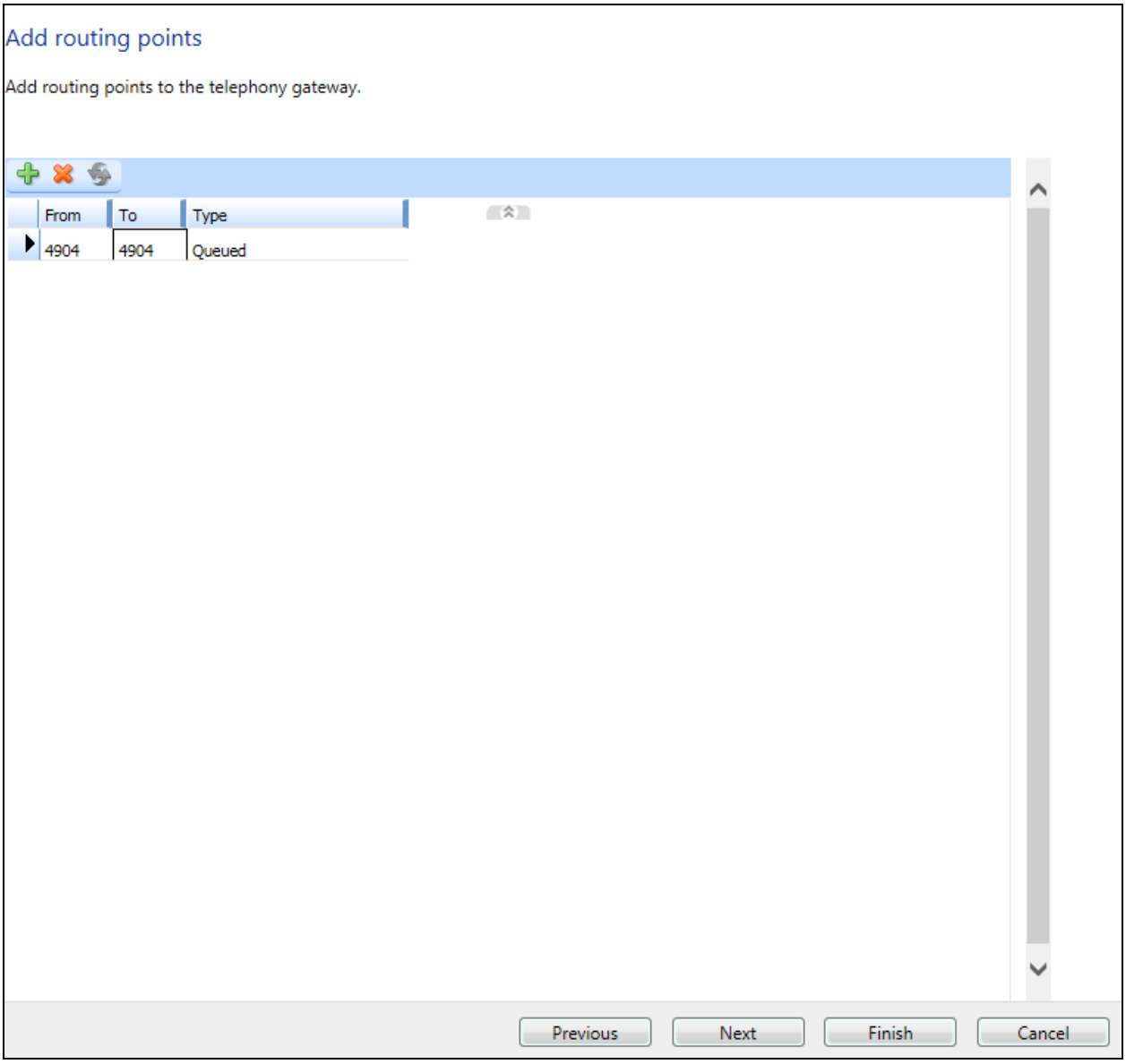
Note: Busy tone device **4909** is a VDN configured to give back a busy tone, used in some of the compliance testing scenarios.



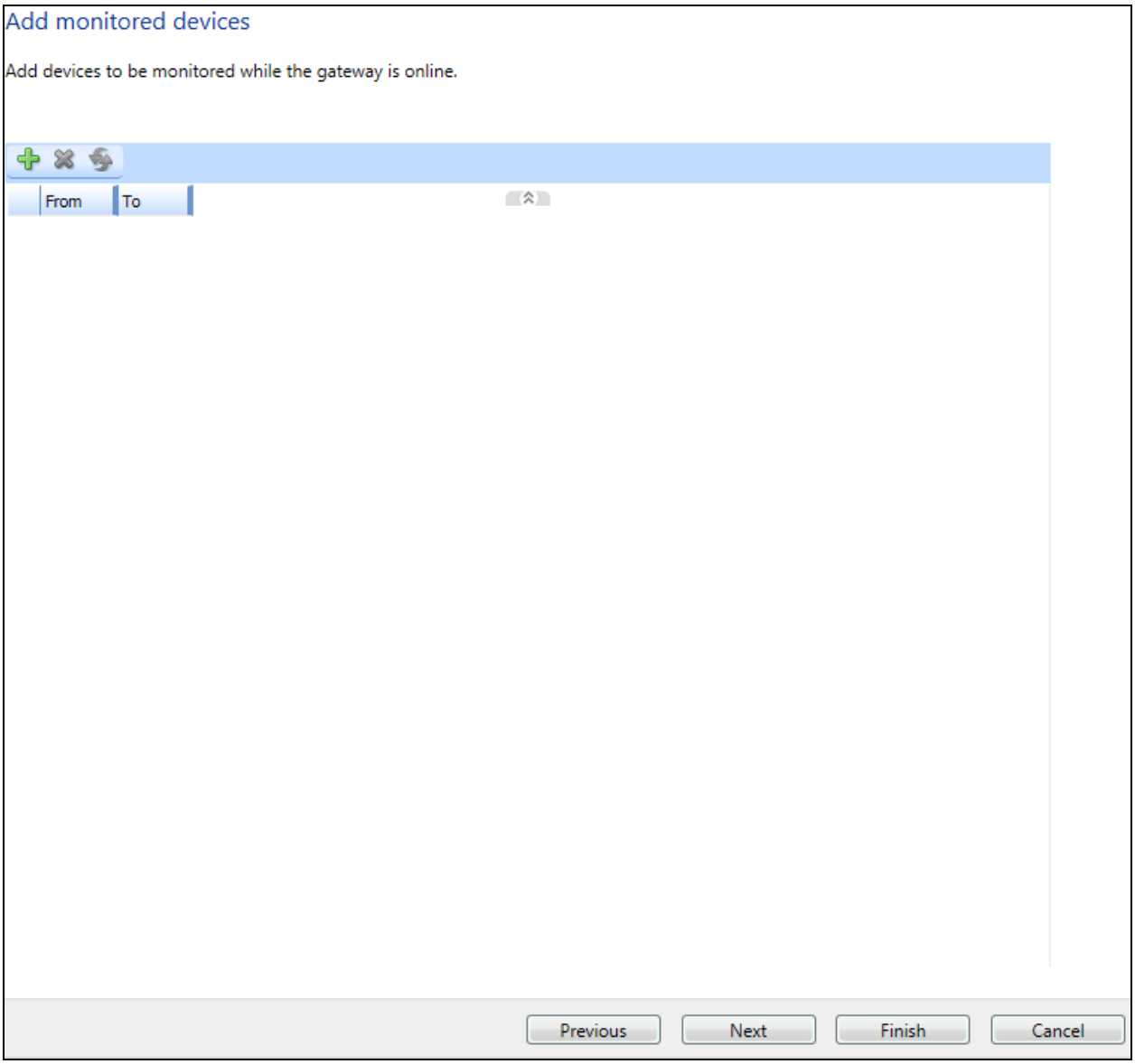
Click on the + icon below. Select the extension range that is to be monitored, using the extensions as configured in **Section 5.2.5**. Tick the **Use ACD login** box as shown below. Click on **Next** once finished.



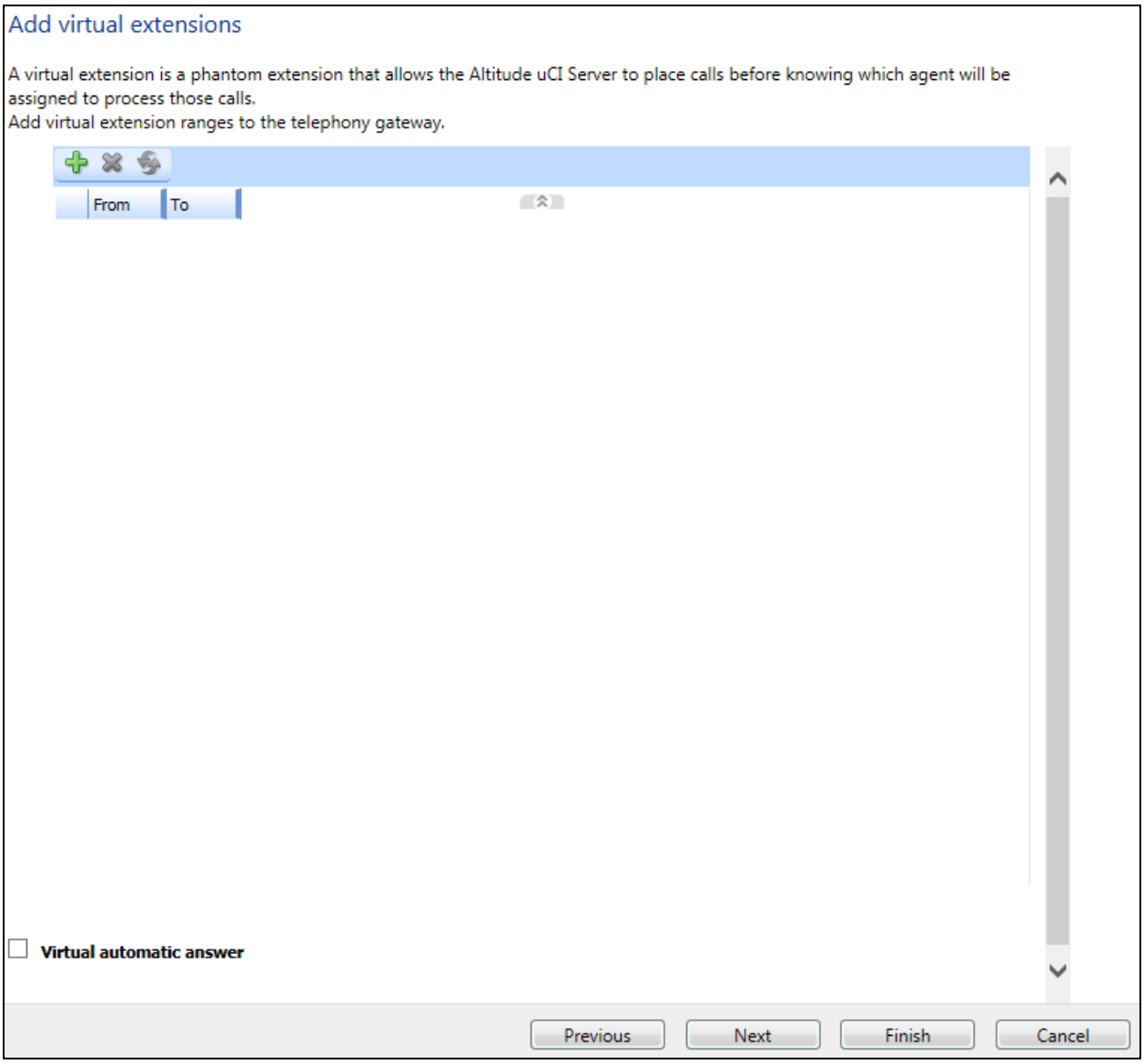
A **routing point** was added (see **Appendix**) to solve an issue found during compliance testing (see **Section 2.2**). When a call is placed directly to the ACS (via aar routing and SIP Trunk) and the call is then transferred back into the "incoming VDN" there is call data missing or distorted. This is the calling number which appears as TSAPI Call ID. When a VDN was added that routes the call to the ACS via aar and SIP Trunk this issue is resolved and this VDN is added below also. Click on **Next** to continue.



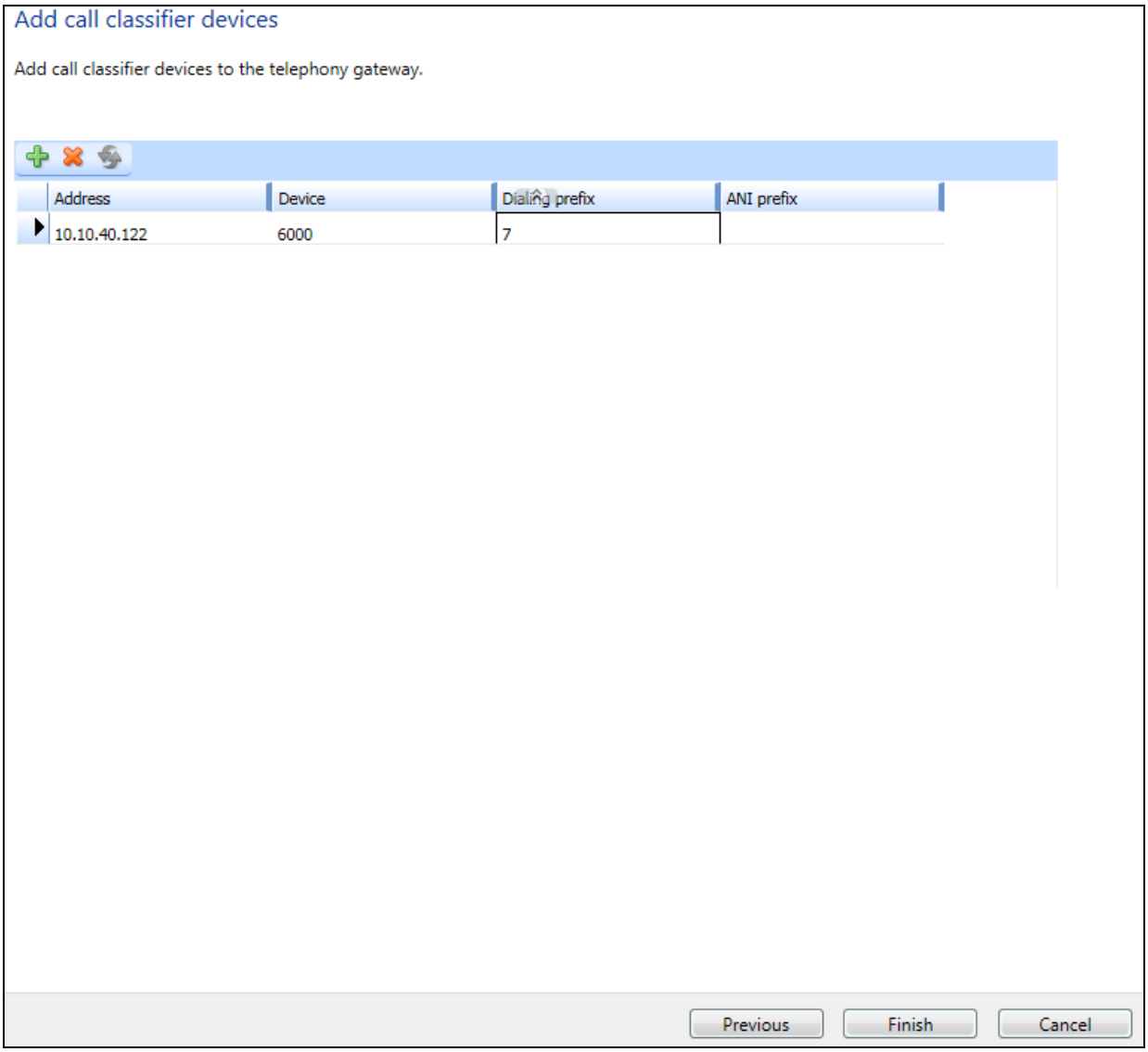
If there are stations or VDN's that need to be permanently monitored regardless of Agent login these are selected below, in this case none were selected. Click **Next** to continue.



If there are virtual stations that are required for predictive outbound campaigns these are added here. Click **Next** to continue.

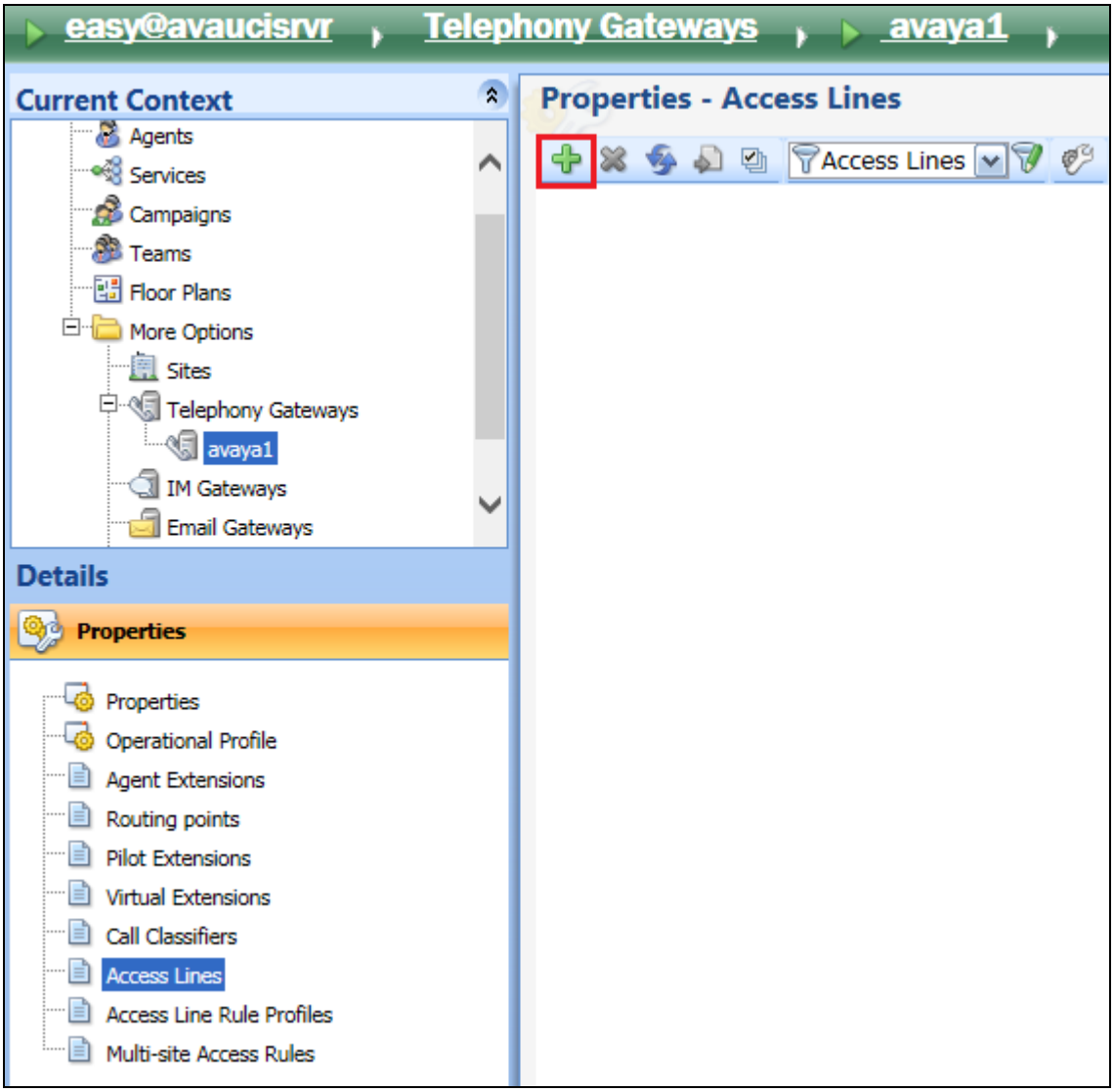


A call classifier was setup for outbound campaigns for predictive dialing. Select the + icon and enter the IP Address of the Altitude Communication Server (ACS) in this case it will be the same as the Altitude Assisted Server and the **Device** is the number that was created in the Communication Server 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**. Click on **Finish** once completed.

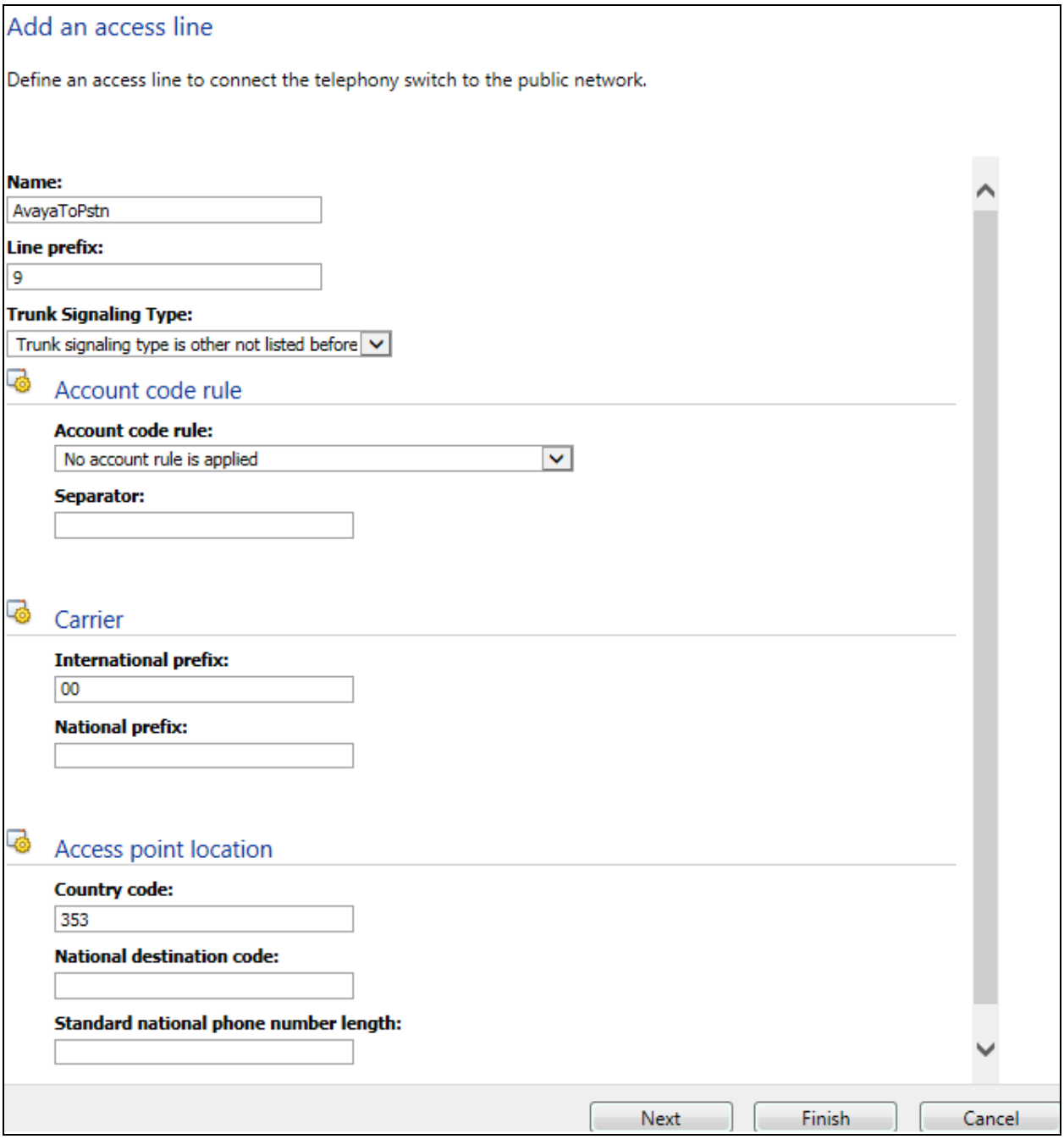


8.1.2. Configure Dialing Prefix

Highlight **Telephony Gateways** → <**Gateway Name**> and select **Access Lines** from the **Properties** window as shown. From the main window click on the add icon.

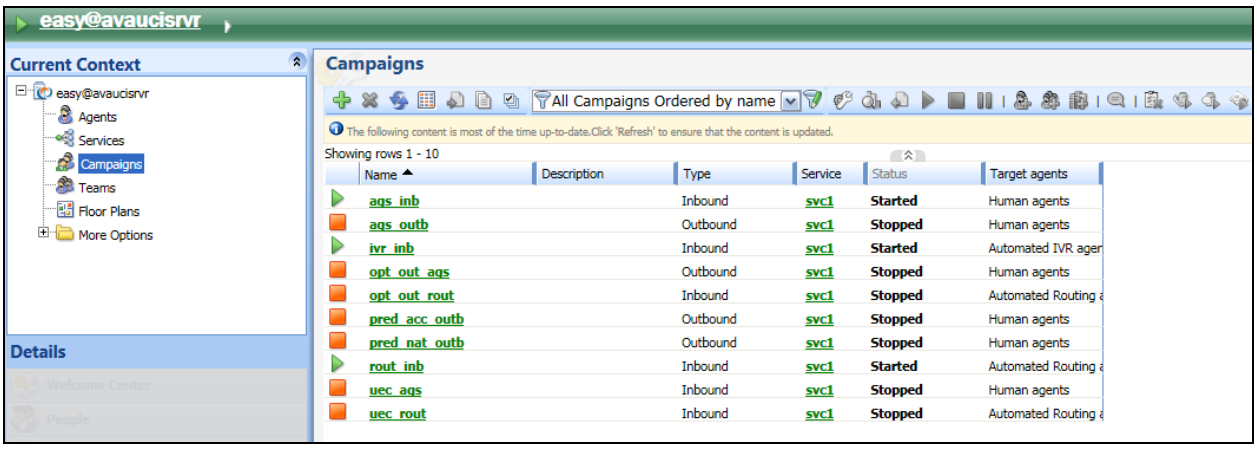


Enter a suitable **Name** and the **Line Prefix** should be set to the Avaya Communication Manager Auto Route Selection (ARS) - Access Code 1 Feature Access Code configured in **Section 5.1.2**. The **Trunk Signaling Type** should be set as shown and the appropriate International and National prefixes, and Country code entered. Click on **Finish** once all is entered correctly.



8.1.3. 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.

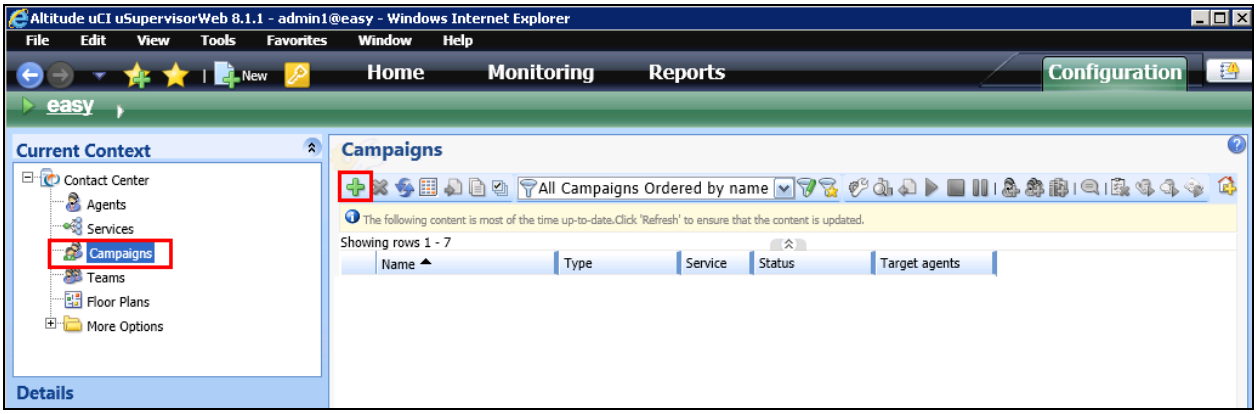


The following shows the setup and configuration of "Predictive Outbound Dialing using Altitude Call Classifier".

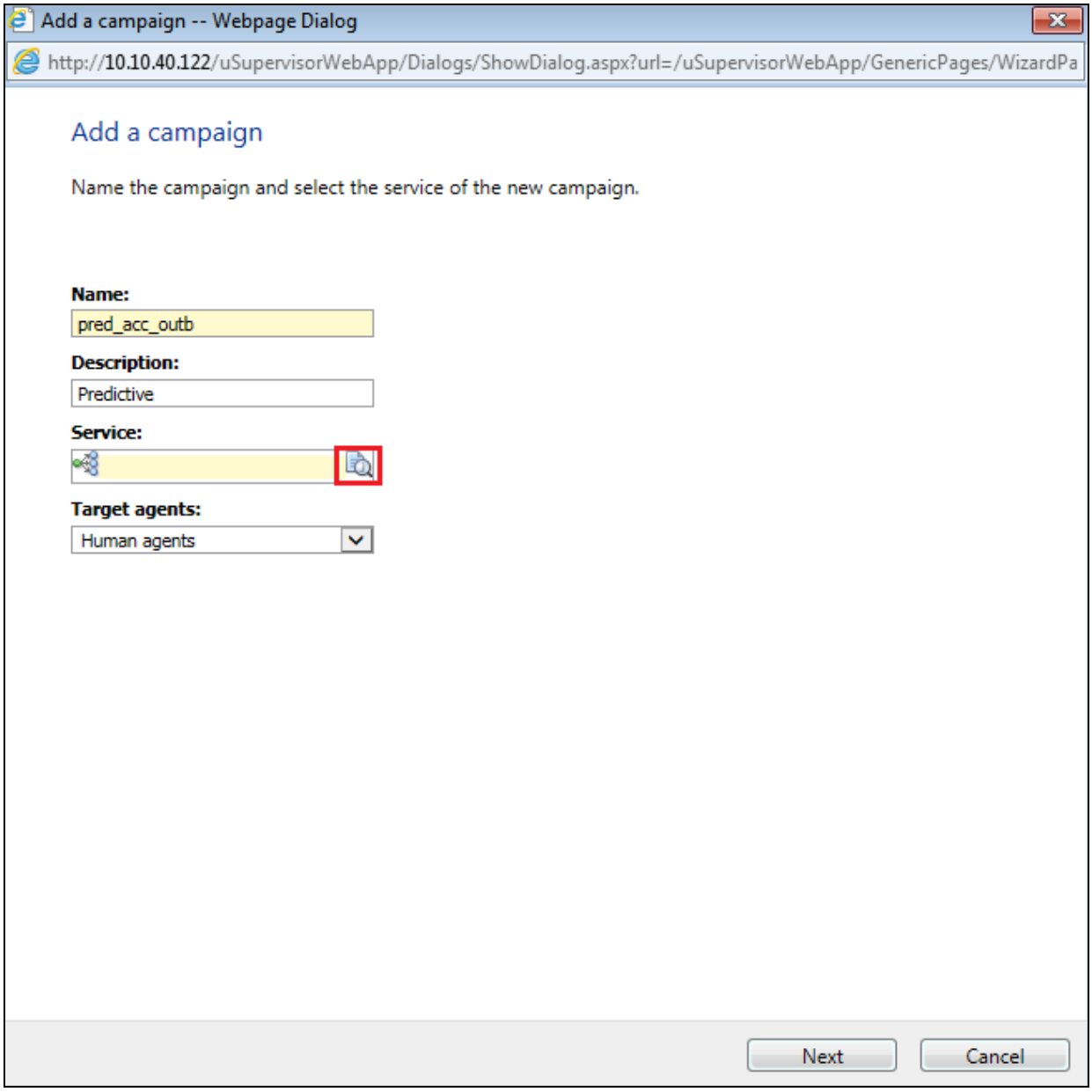
In this scenario predictive calls are dialed by Altitude Call Classifier device in Altitude Communication Server to the PSTN via the SIP trunk, then after being successfully classified and answered by a person they are transferred to the Avaya agent.

Note: The correct transfer of the customer number to Avaya Call Manager requires using a special configuration option in Altitude uCI Server; the following line should be added into AssistedServer.config.
<avaya1_USE_DATA_FORGED_ANI>1</avaya1_USE_DATA_FORGED_ANI>

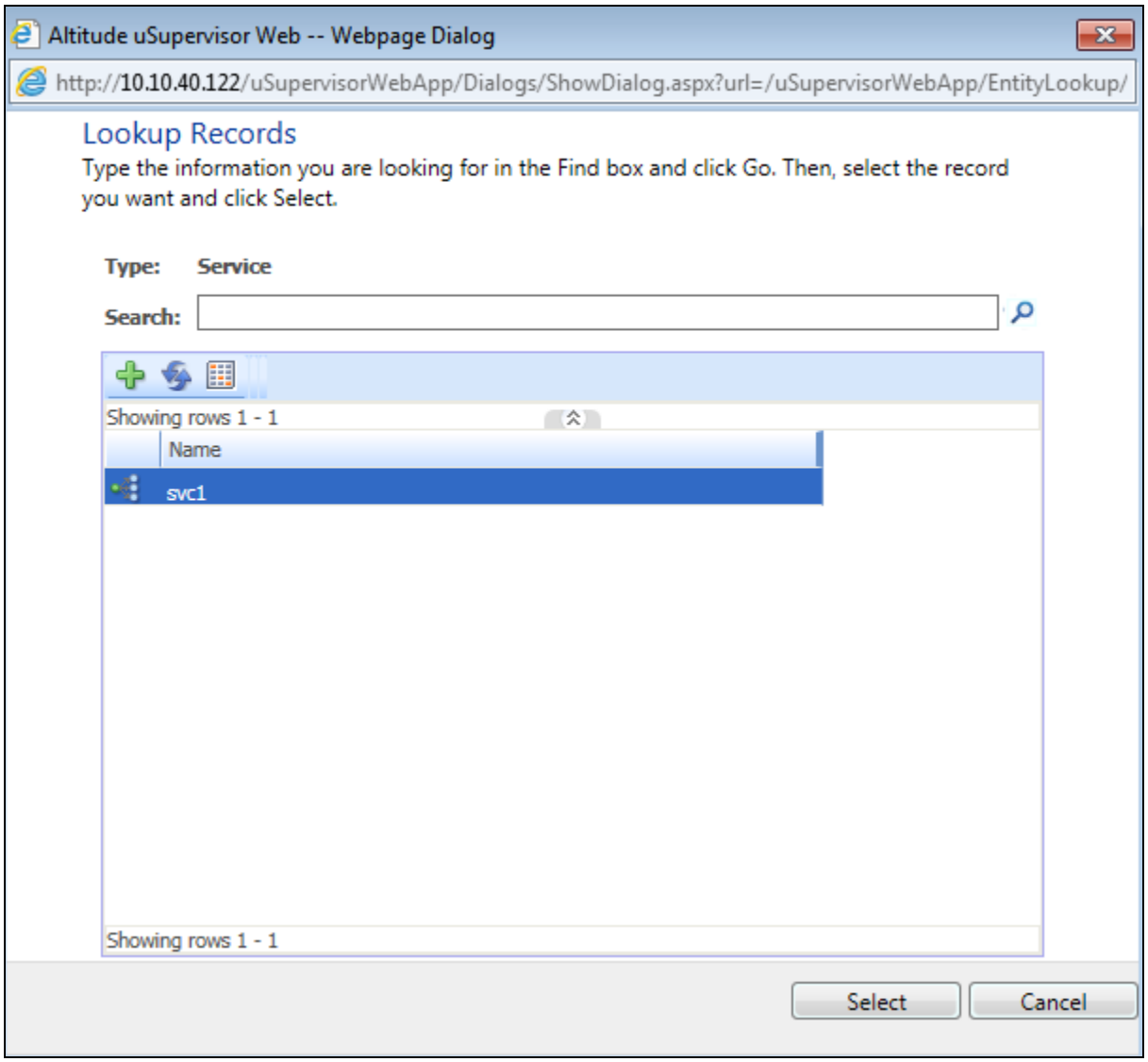
Select **Campaigns** from the left window and select the + icon in the main window.



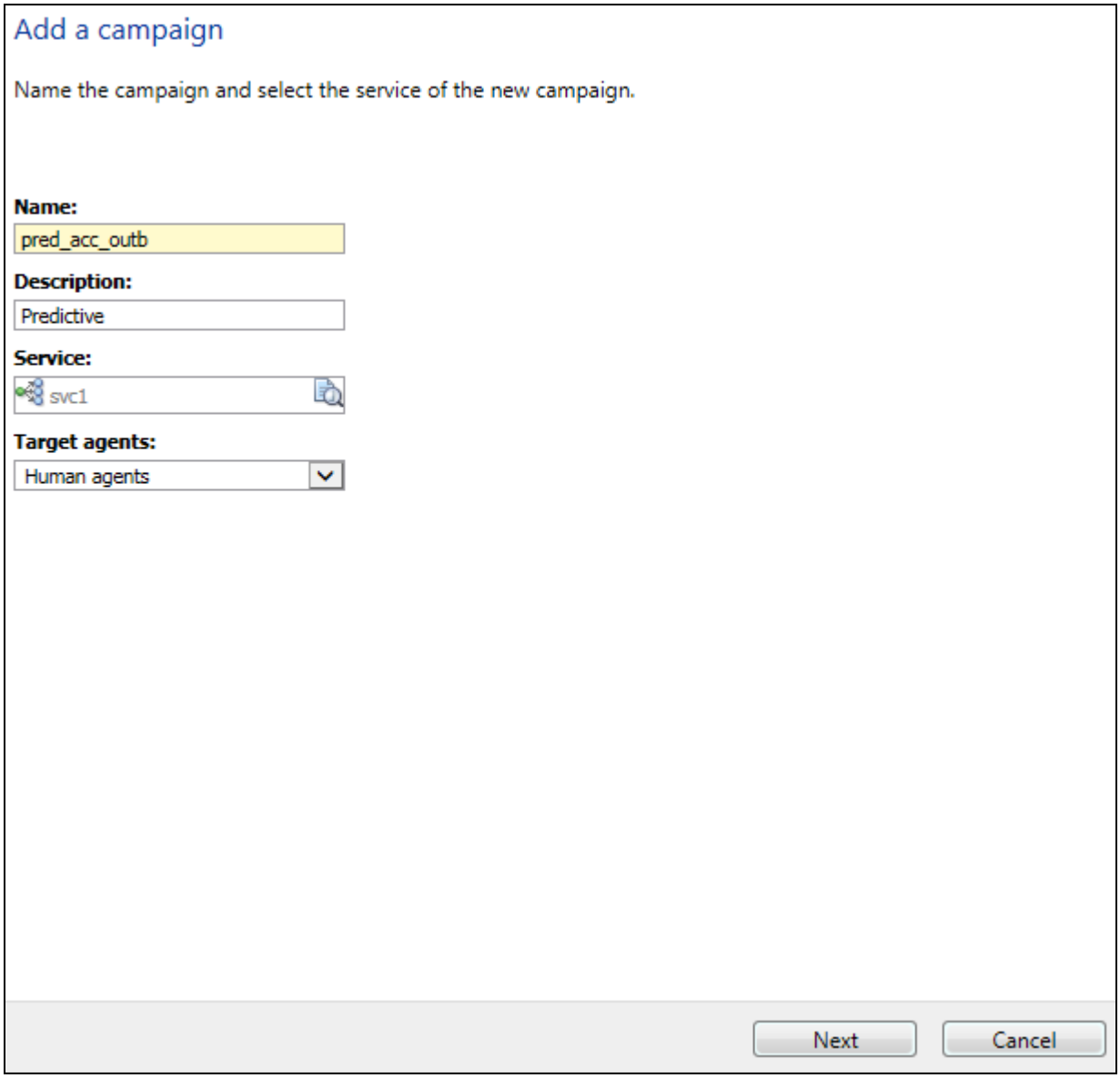
Enter a suitable **Name** for the campaign and click on the search icon highlighted under **Service**.



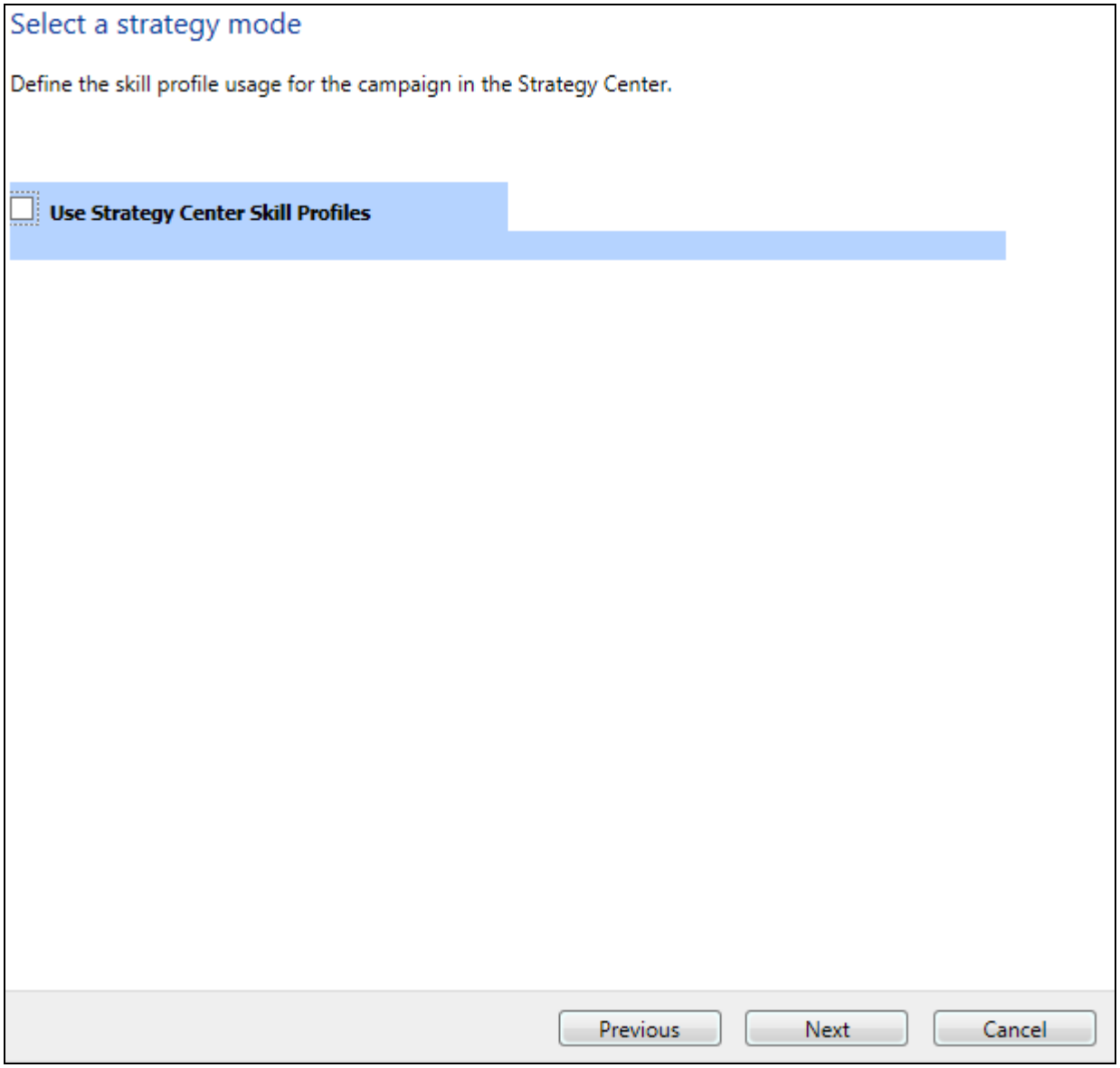
A service may already be configured as was the case for compliance testing, so this **svc1** was selected. A new service can be created if there is none already present.



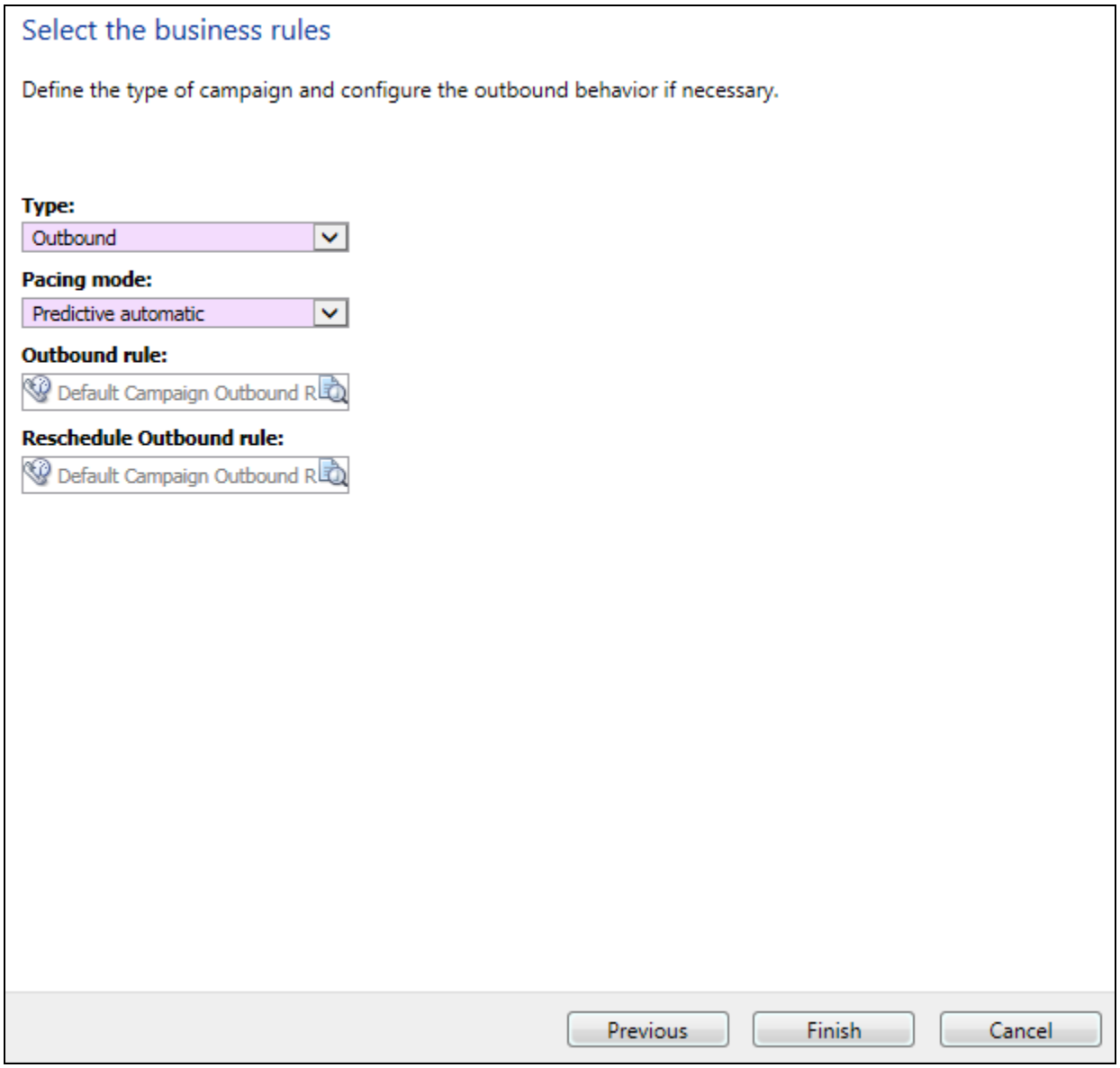
With the **Service** added click on **Next** to continue.



Click on **Next** to continue.

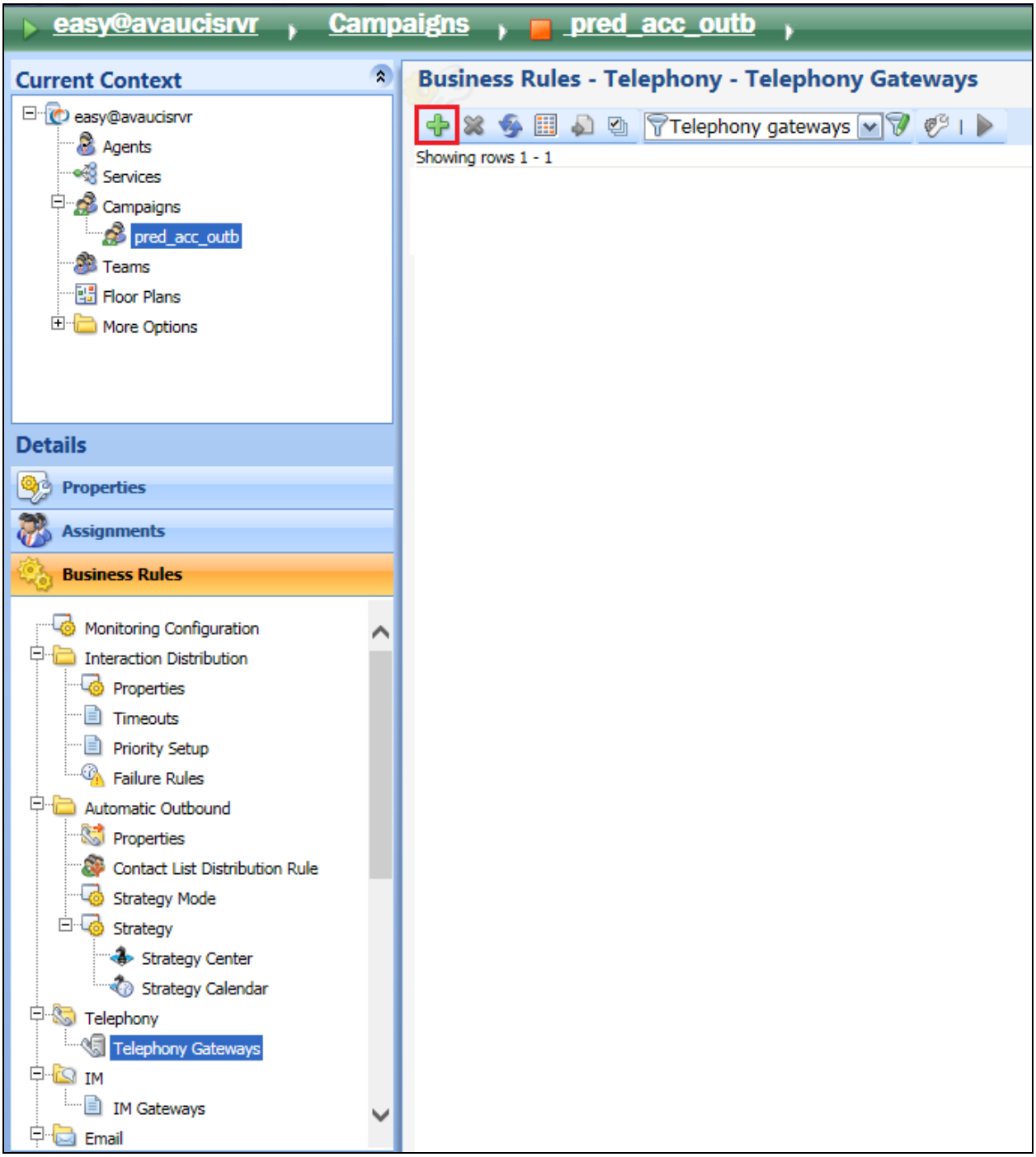


The **Type** should be set to **Outbound** and the **Pacing mode** to **Predictive automatic**, the other fields can be left as default. Click on **Finish** to continue.

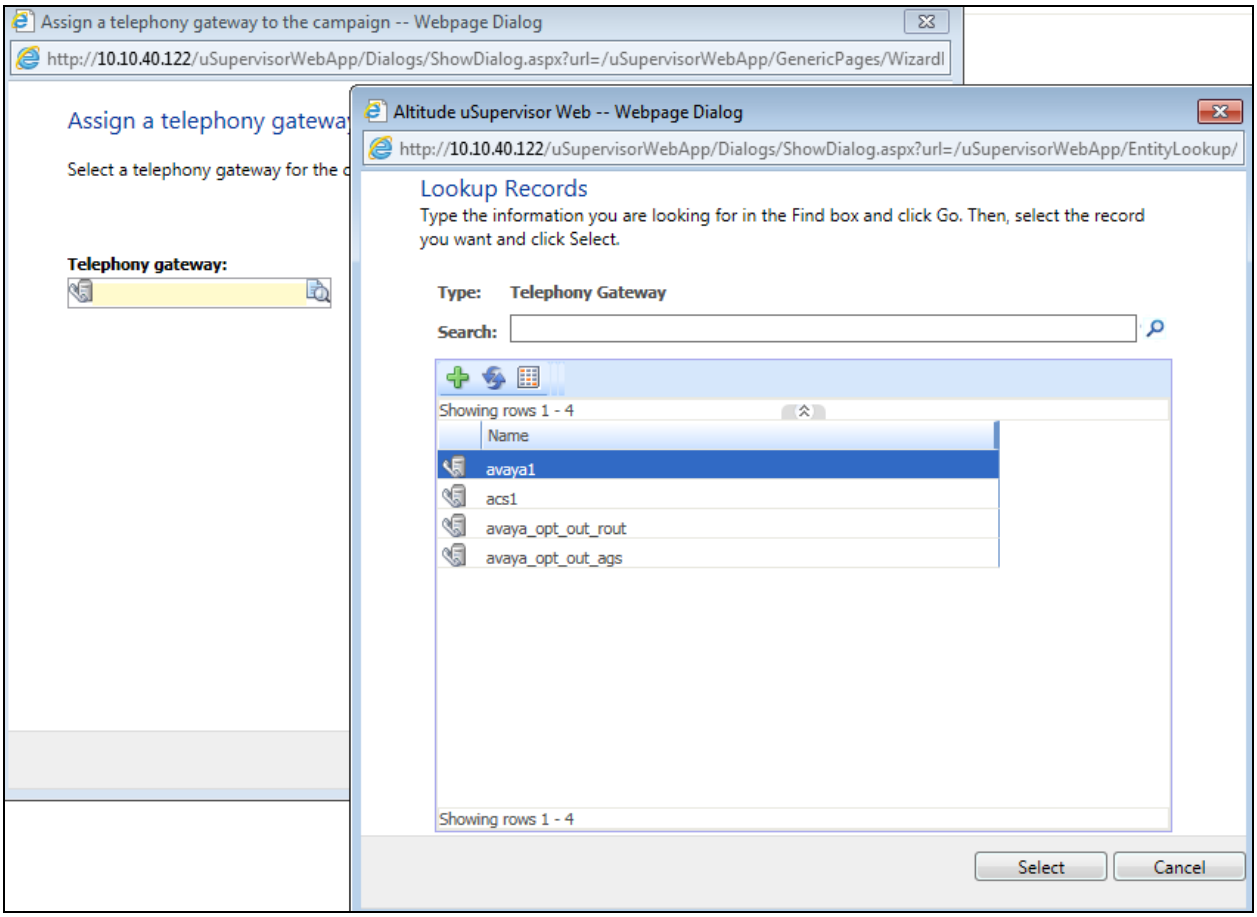


8.1.4. Configure Telephony Gateway in Campaign

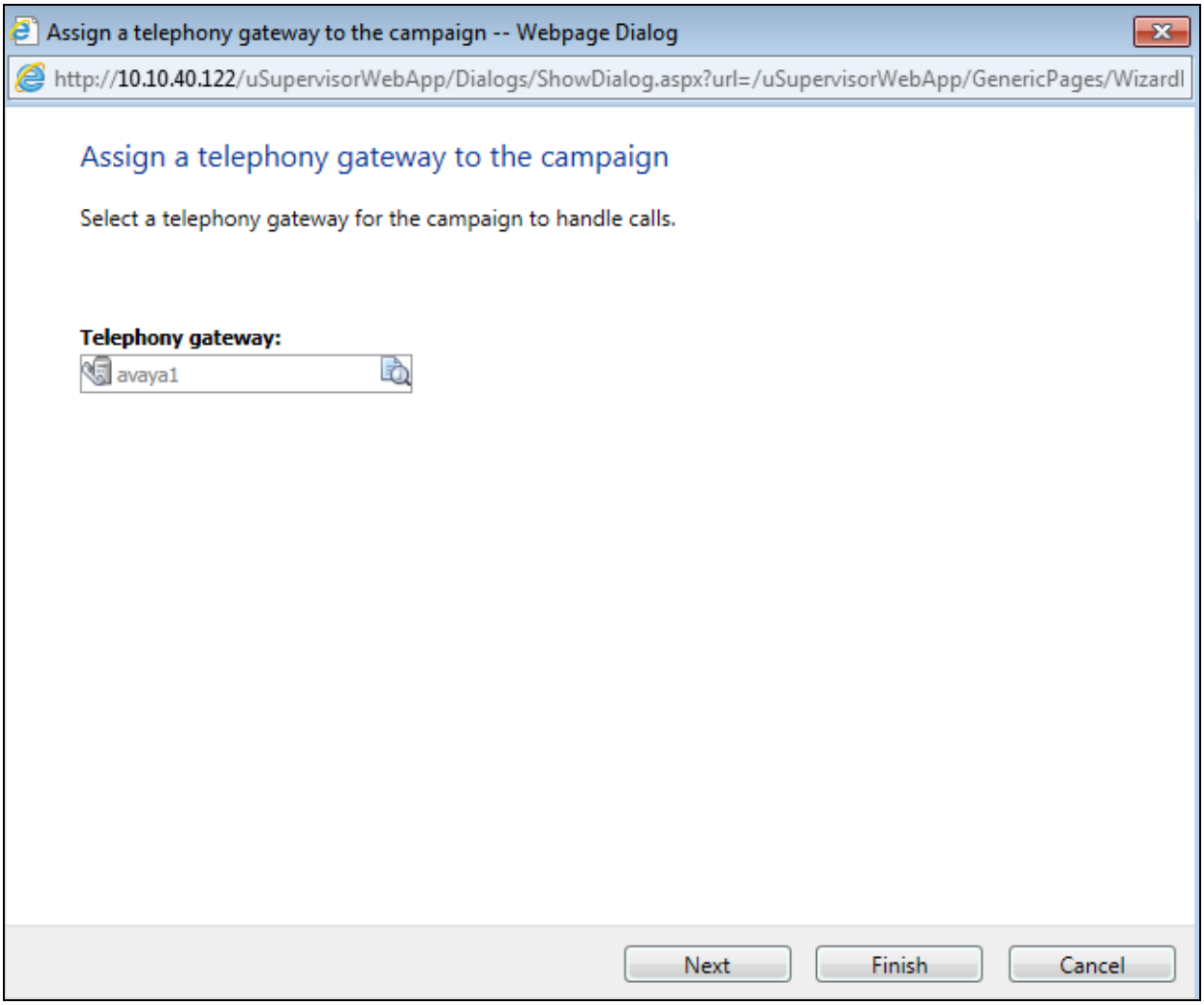
Click on the Campaign configured in **Section 8.1.3**. Select **Business Rules → Telephony → Telephony Gateways**. Click on + icon.



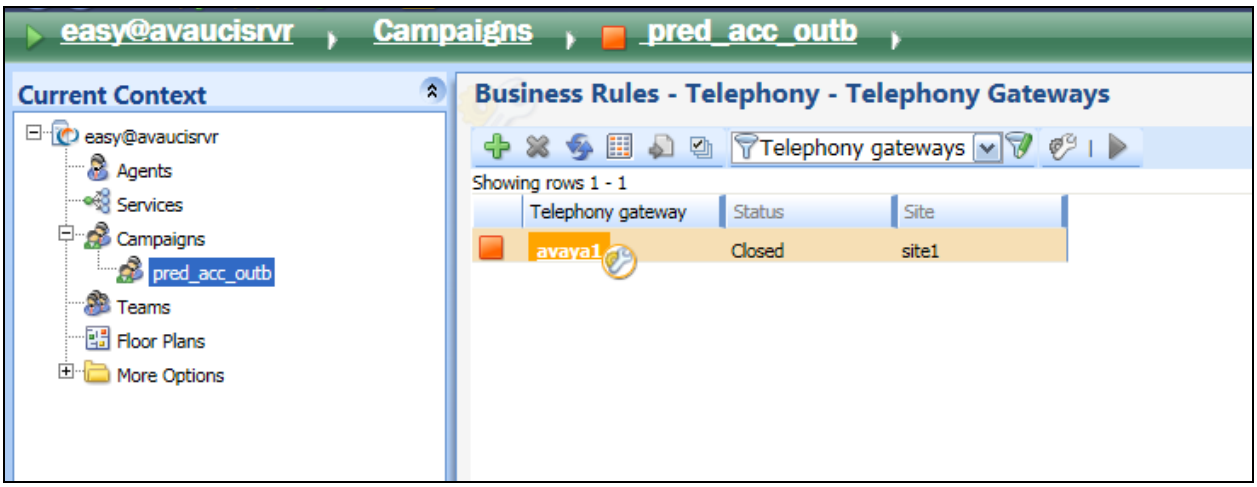
Assign the newly created telephony gateway to this campaign as shown in the screen below and click on **Select**.



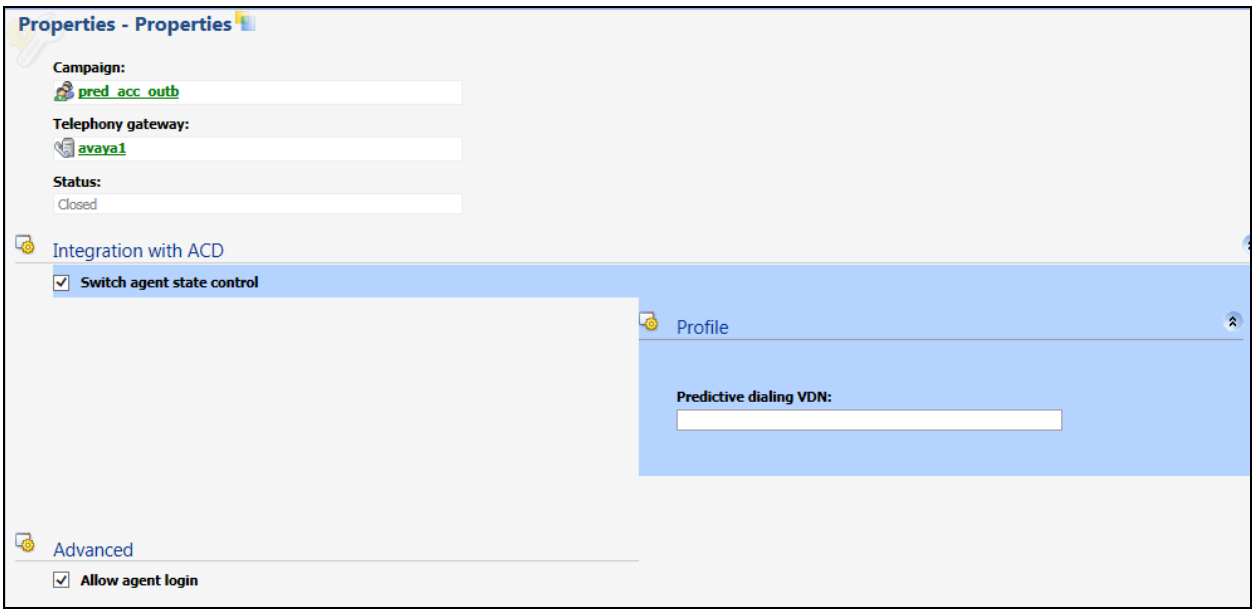
Click on **Finish**.



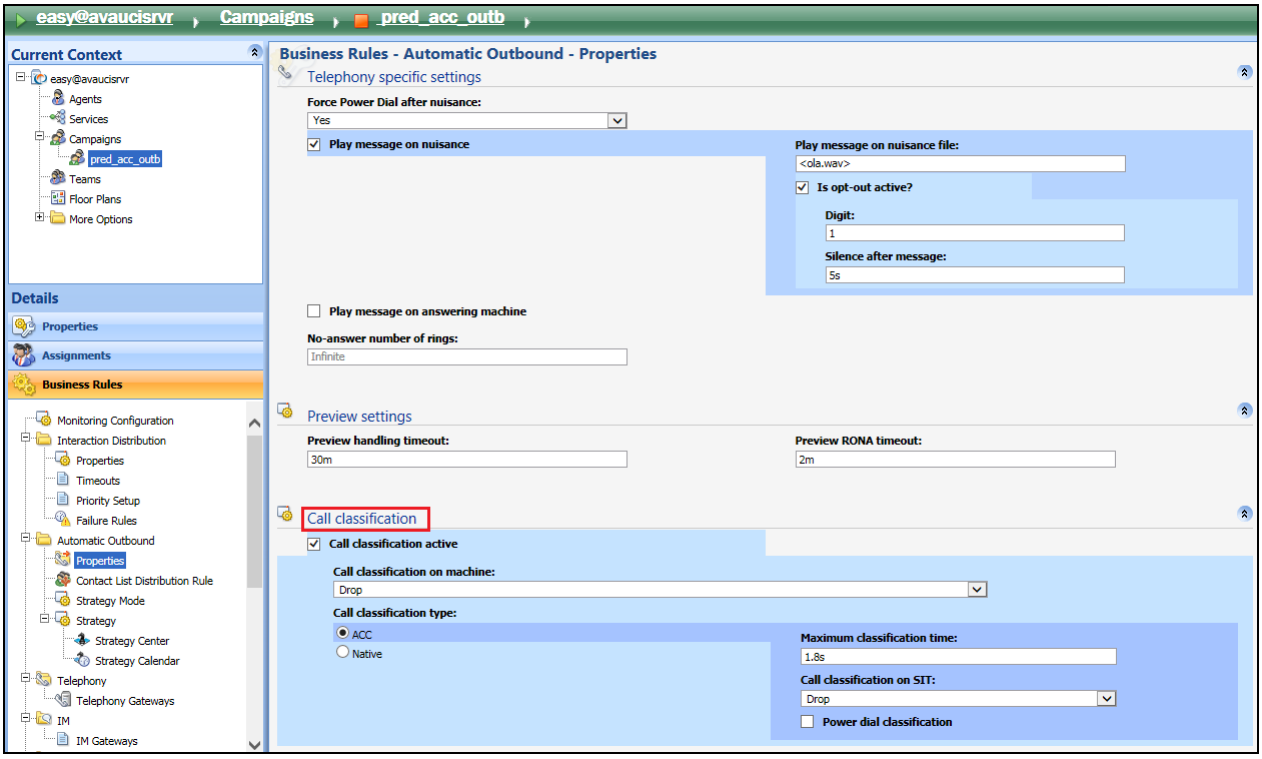
Click on the **Telephony gateway** as shown below.



Ensure that **Switch agent state control** is ticked to allow wrap-up on calls coming to the VDN.

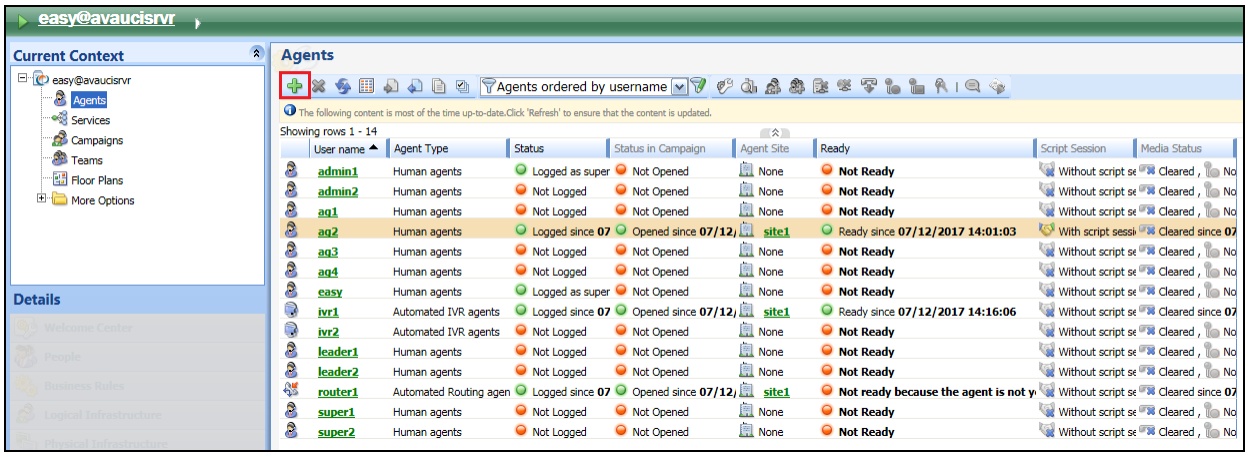


Click on the outbound campaign and navigate to **Business Rules → Automatic Outbound → Properties** in the left window. In the resulting main window, ensure that **Call Classification Active** is ticked and **ACC** (Altitude Call Classifier) is selected as shown below.

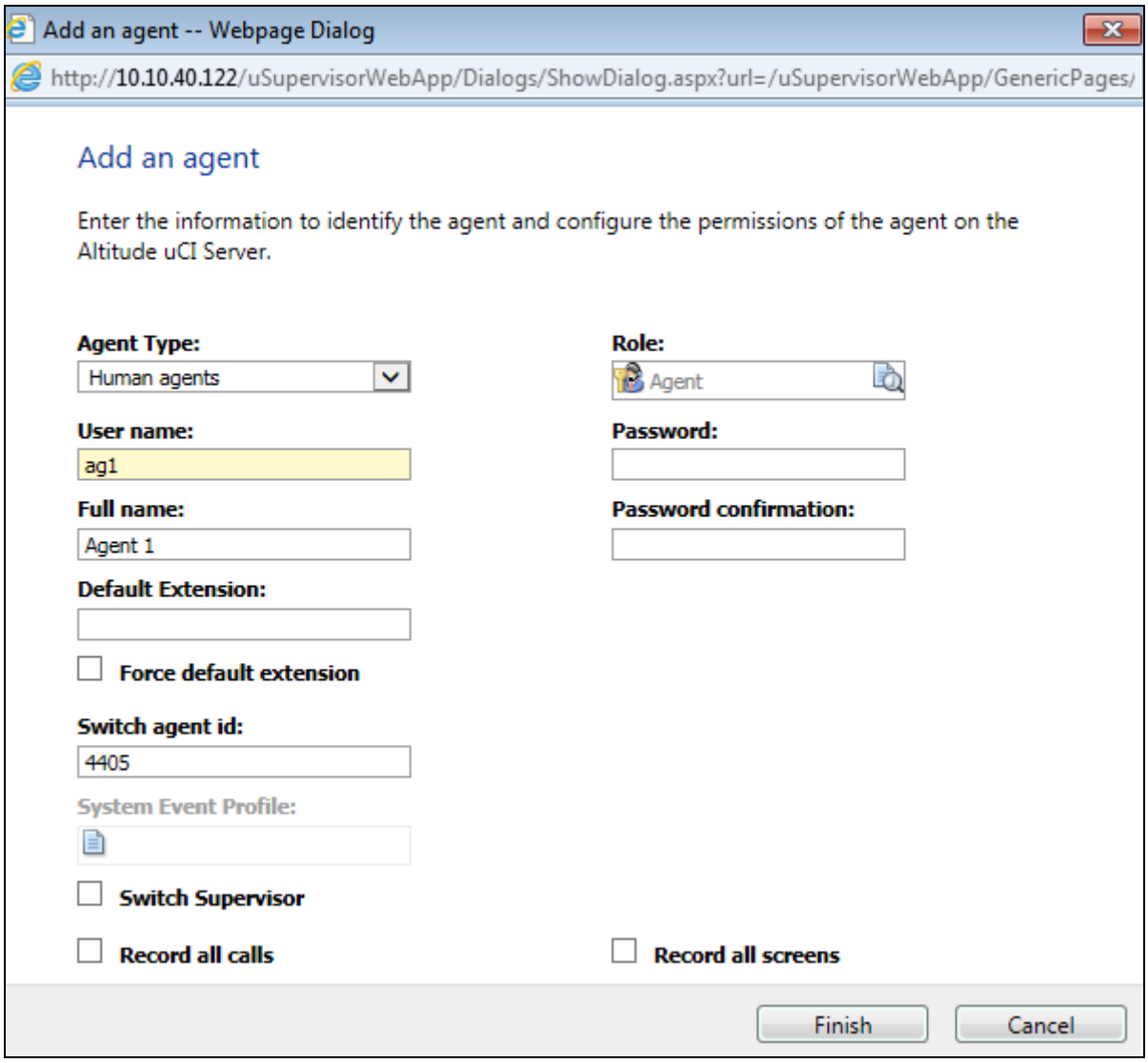


8.1.5. Adding Agents to Assisted Server

Navigate to <**Contact Center Name**>→ **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 highlighted below.

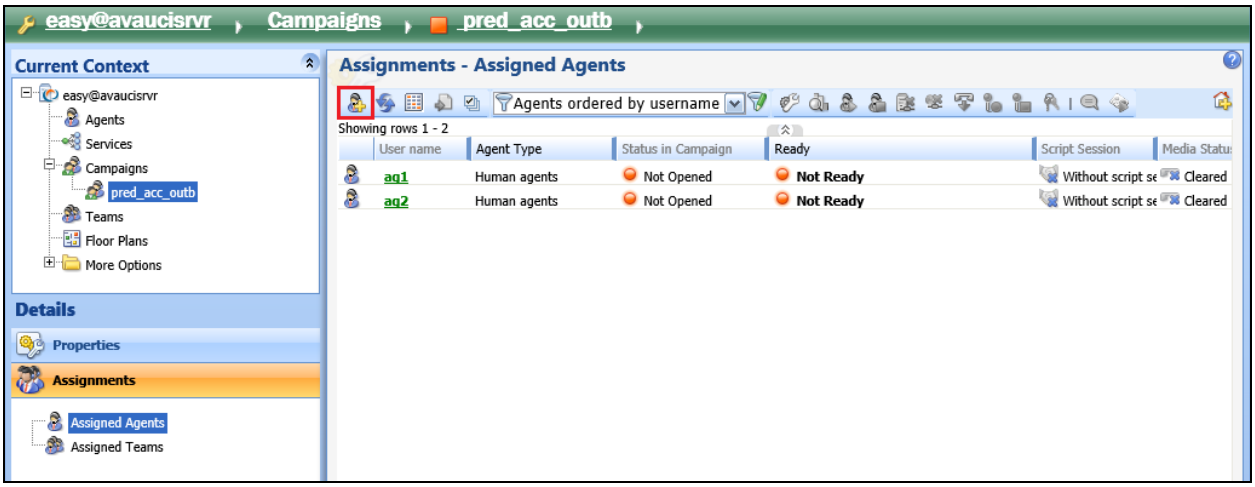


This example shows the creation of a human agent to log into an Avaya desk phone. Enter the suitable credentials noting the **Switch agent id** is **4405** as configured in **Section 5.2.4**.

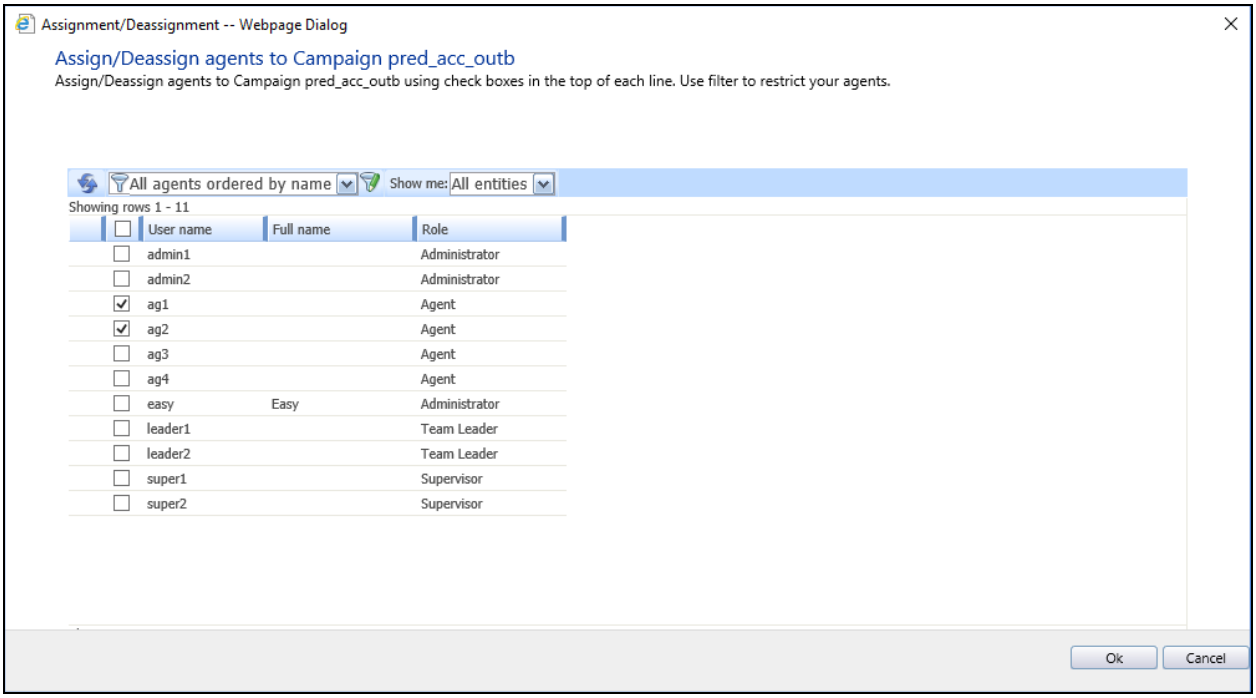


8.1.6. Assigning agents to work in the campaign

Click on the Campaign configured in **Section 8.1.3**. Select **Assignments → Assigned Agents**. In the main window is a list of agents that were assigned to the campaign for compliance testing. To assign agents to the campaign click on the assign icon highlighted below.

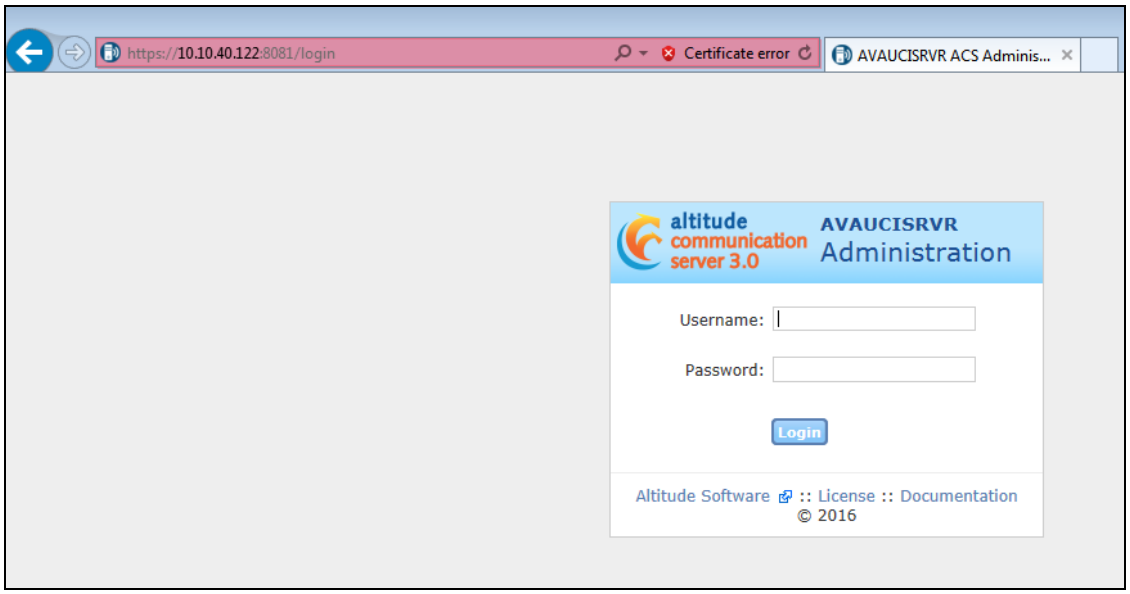


Put a check on the agents that should work in the campaign as shown on the screen below and click on **Ok**.



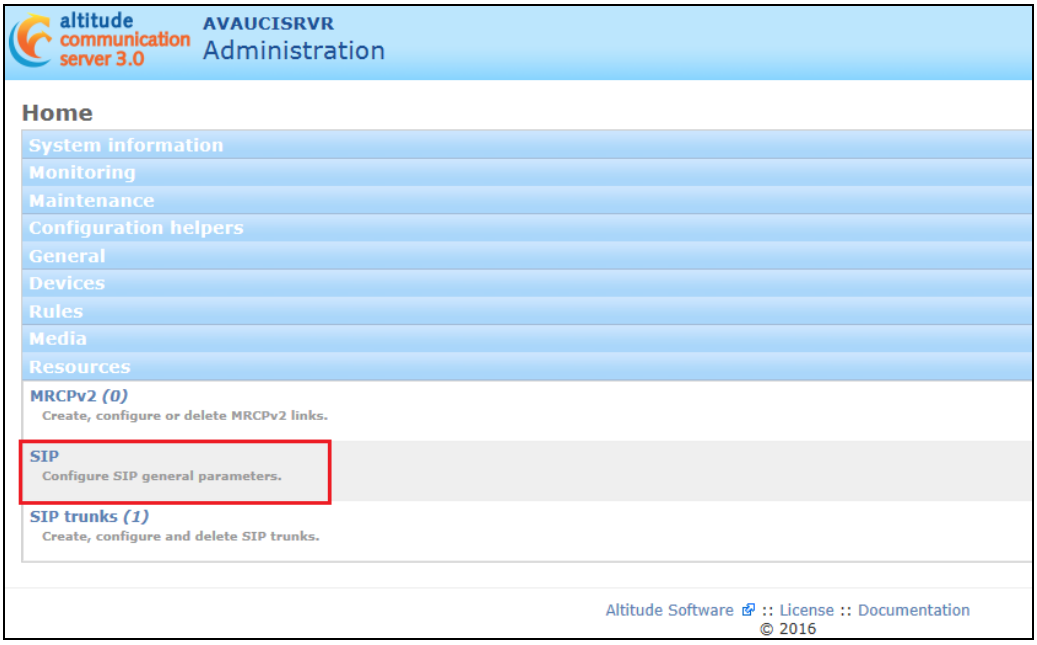
8.2. Configuring Altitude Communication Server

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

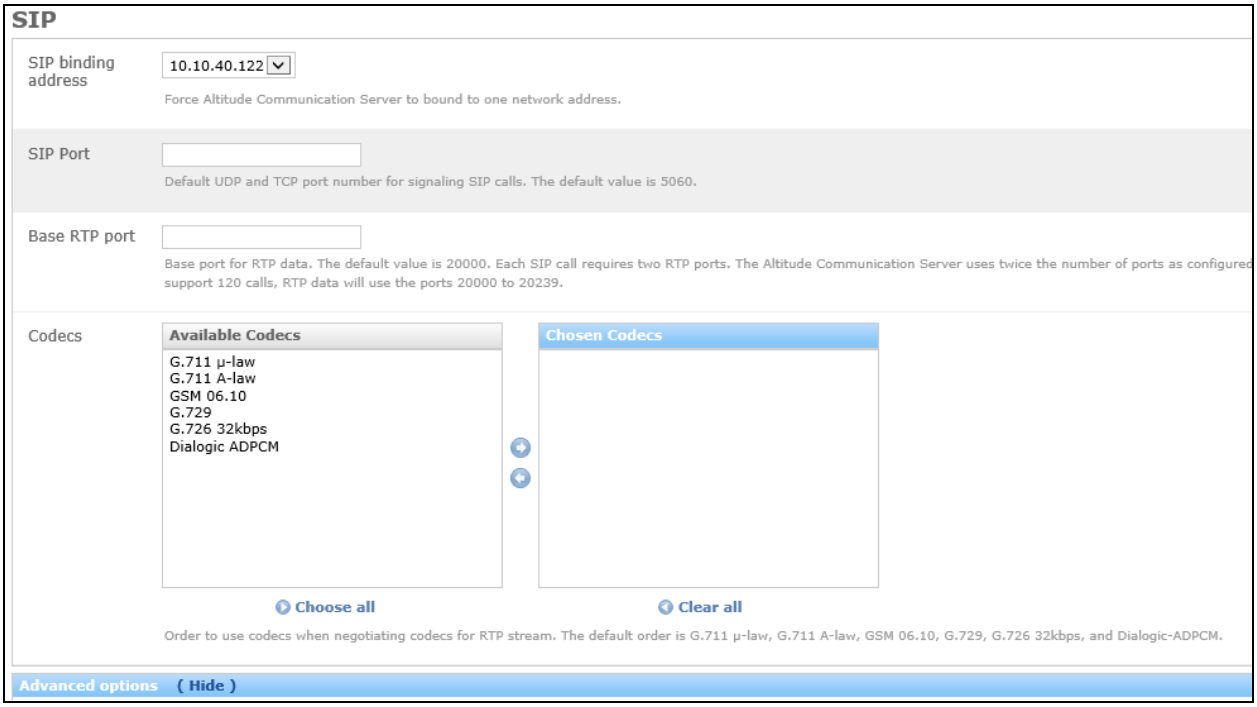


8.2.1. Configure SIP parameters

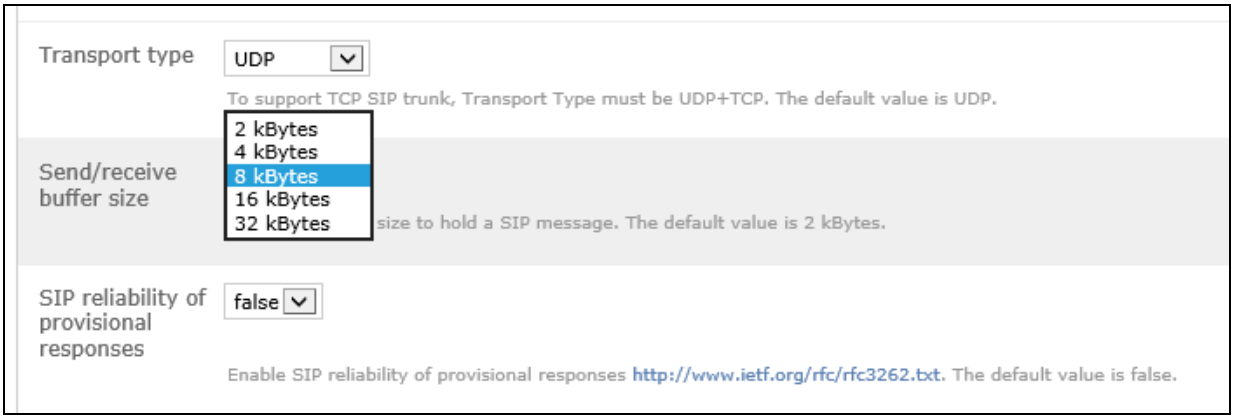
Navigate to **Home → Resources → SIP**.



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

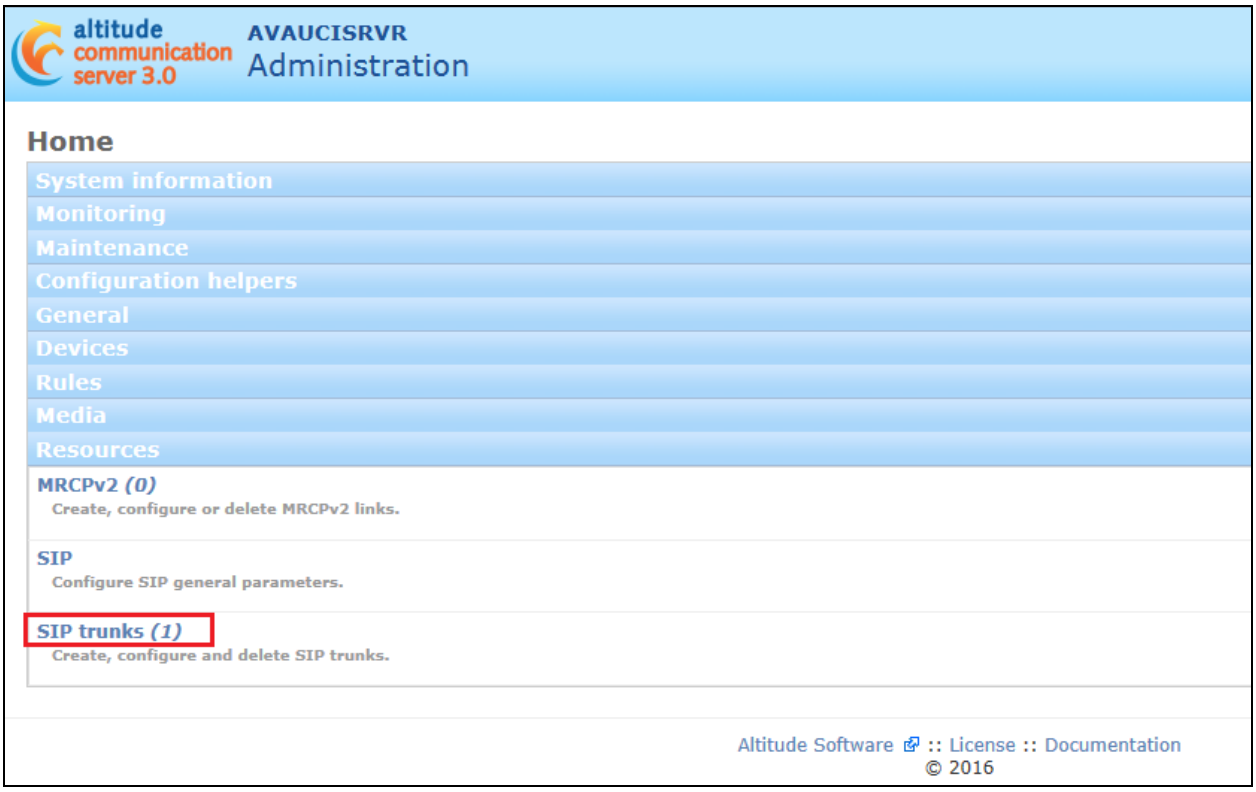


Click on **Advanced options** (shown above) to show other options and scroll down to **Transport type** which by default is set to **UDP**. The **Send/receive buffer size** may need to be increased from the default to **8 kBytes** as shown below.

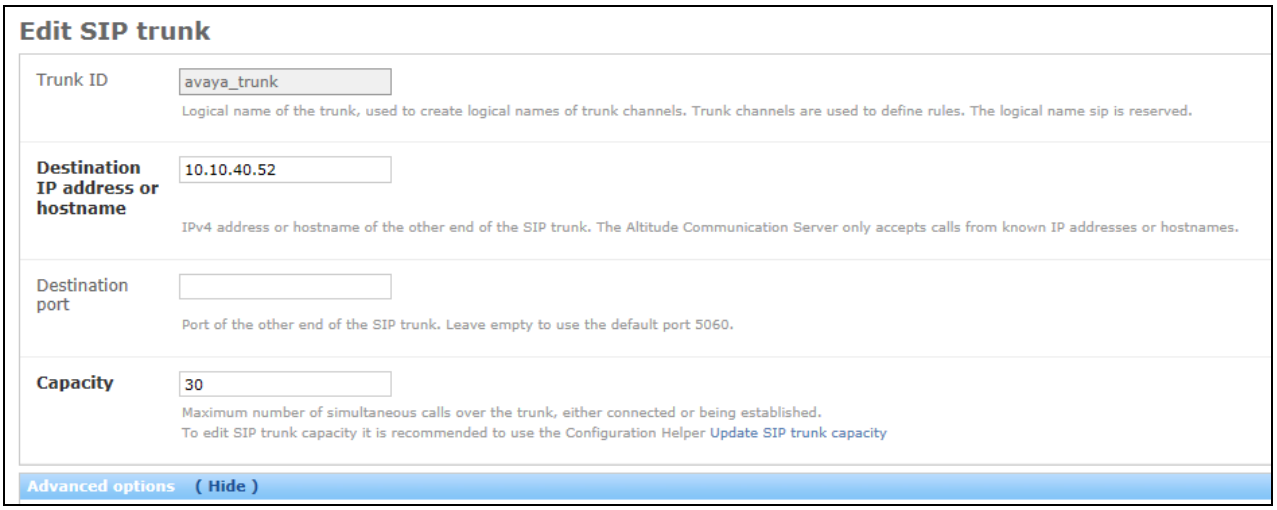


8.2.2. Configure SIP Trunk

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



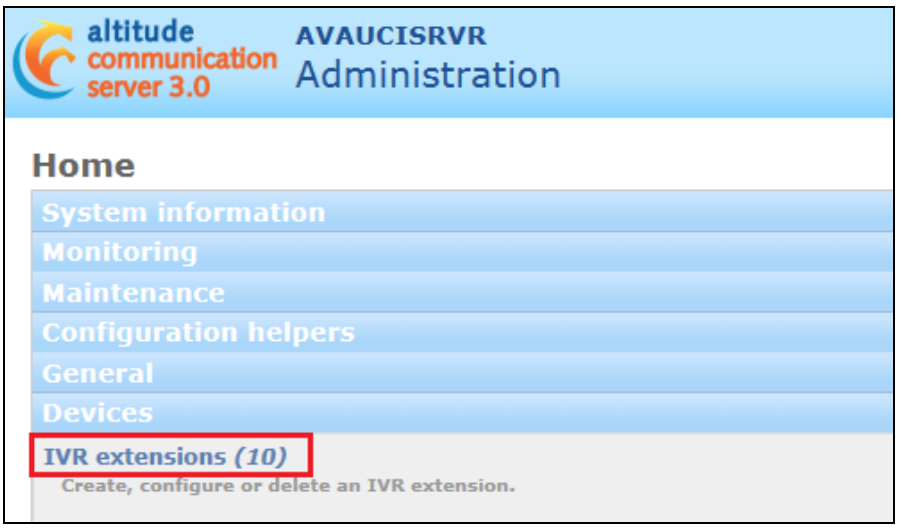
Enter the Session Manager IP Address for the **Destination IP address or hostname**. Click on **Advanced options** and scroll down.



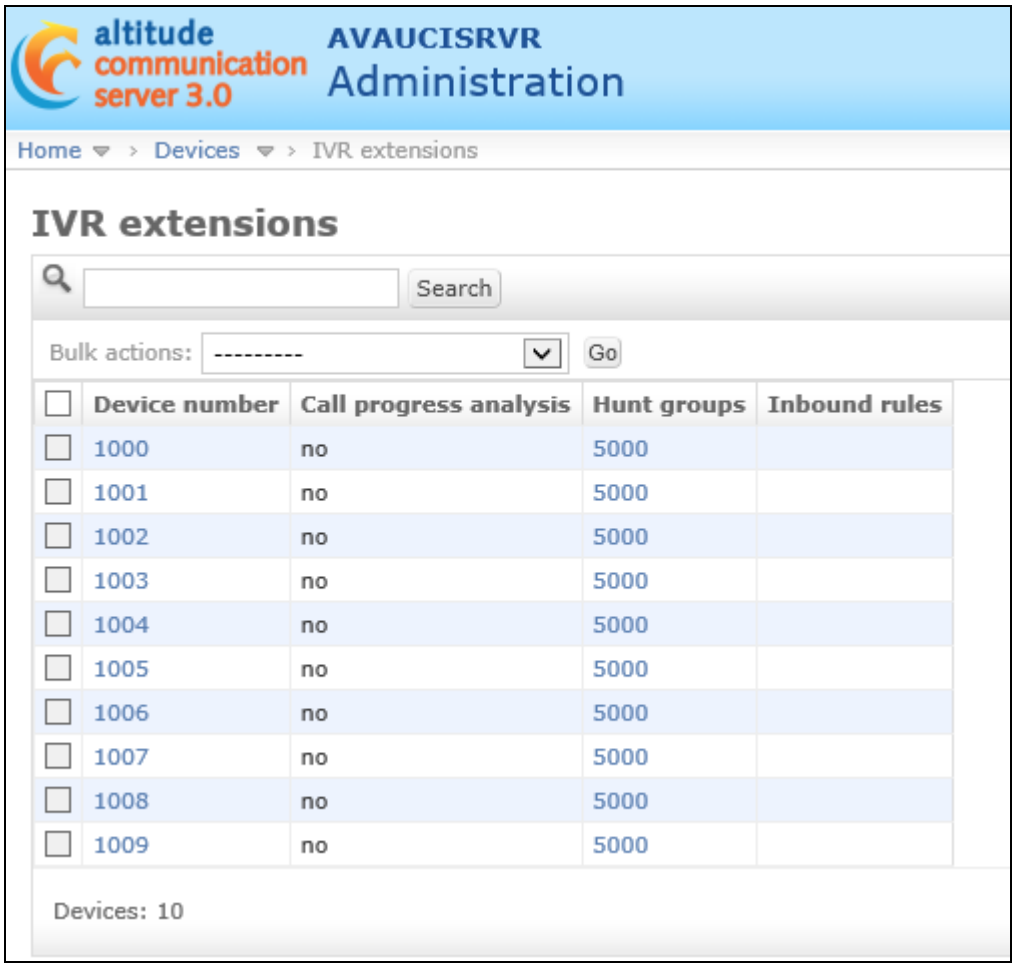
Click on **Advanced options** and scroll down as mentioned above. The **Outgoing Transport** is left as default, set to **UDP**. The **Call data exchange** should be set according to what is configured on the SIP trunk on Avaya Communication Manager. If UUI Treatment is set to "Service Provider" on Communication 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.



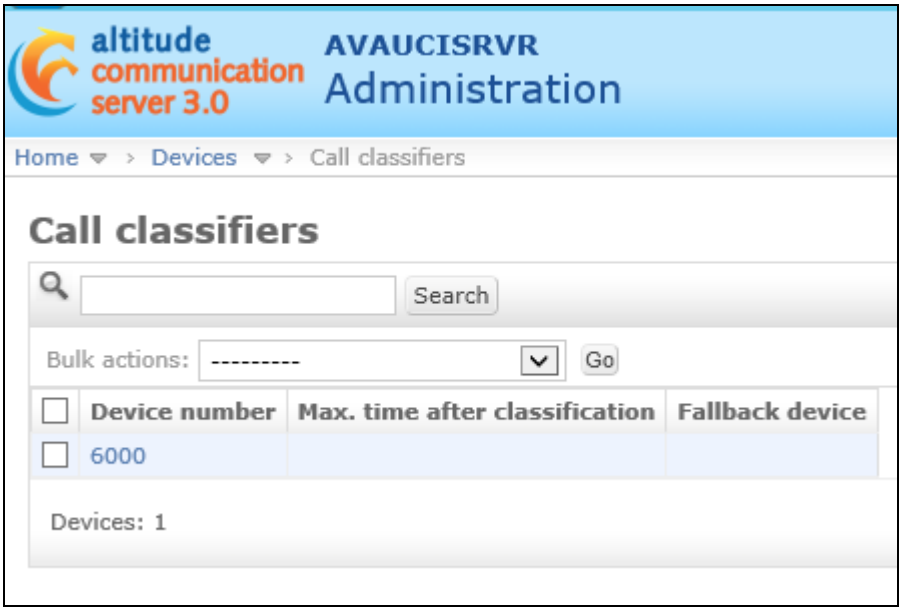
Device number	Call progress analysis	Hunt groups	Inbound rules
1000	no	5000	
1001	no	5000	
1002	no	5000	
1003	no	5000	
1004	no	5000	
1005	no	5000	
1006	no	5000	
1007	no	5000	
1008	no	5000	
1009	no	5000	

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**.

Device number	Number of devices	Device pool	Busy when no target	RONA timeout	Inbound rules
5000	10	1000-1009	true		from_avaya

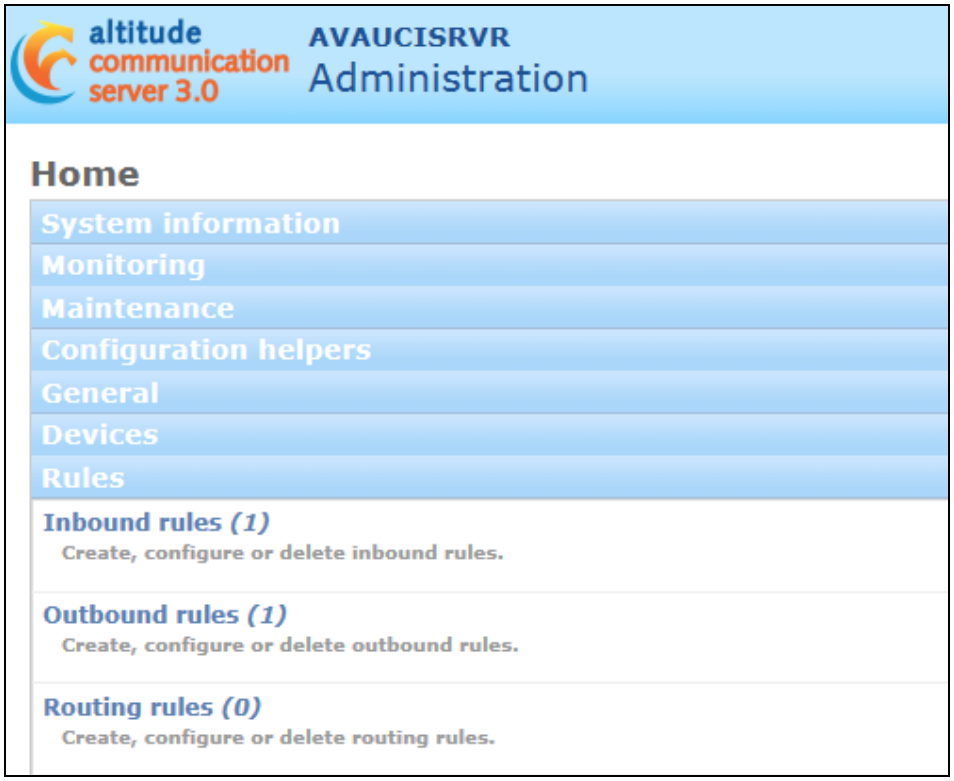
8.2.4. Display Call Classifier Device

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**.

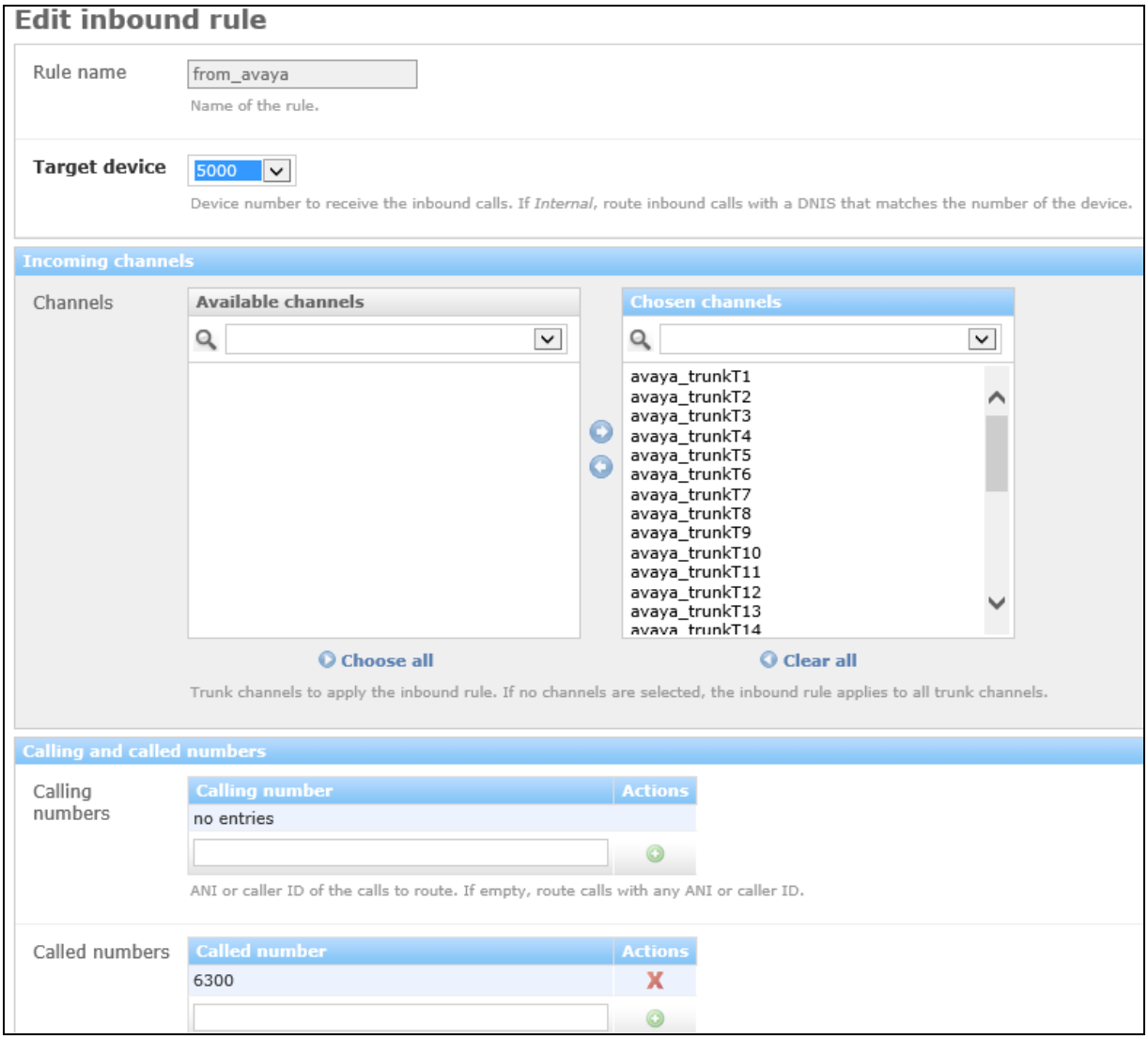


8.2.5. Display Inbound rules

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

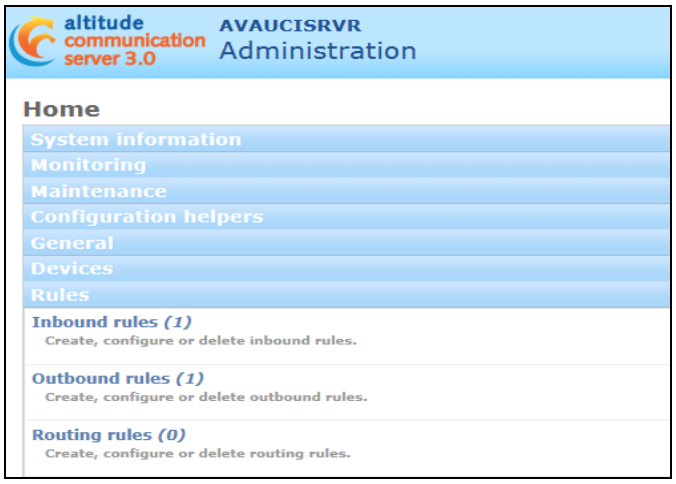


The following shows the setup of the **inbound rule** used for compliance testing. This is the rule for getting the call from the SIP Trunk to the ACS IVR hunt group. Note that **6300** was the number used to route the calls to the ACS via the SIP Trunk using AAR in **Section 5.5** and **Section 7.7**.

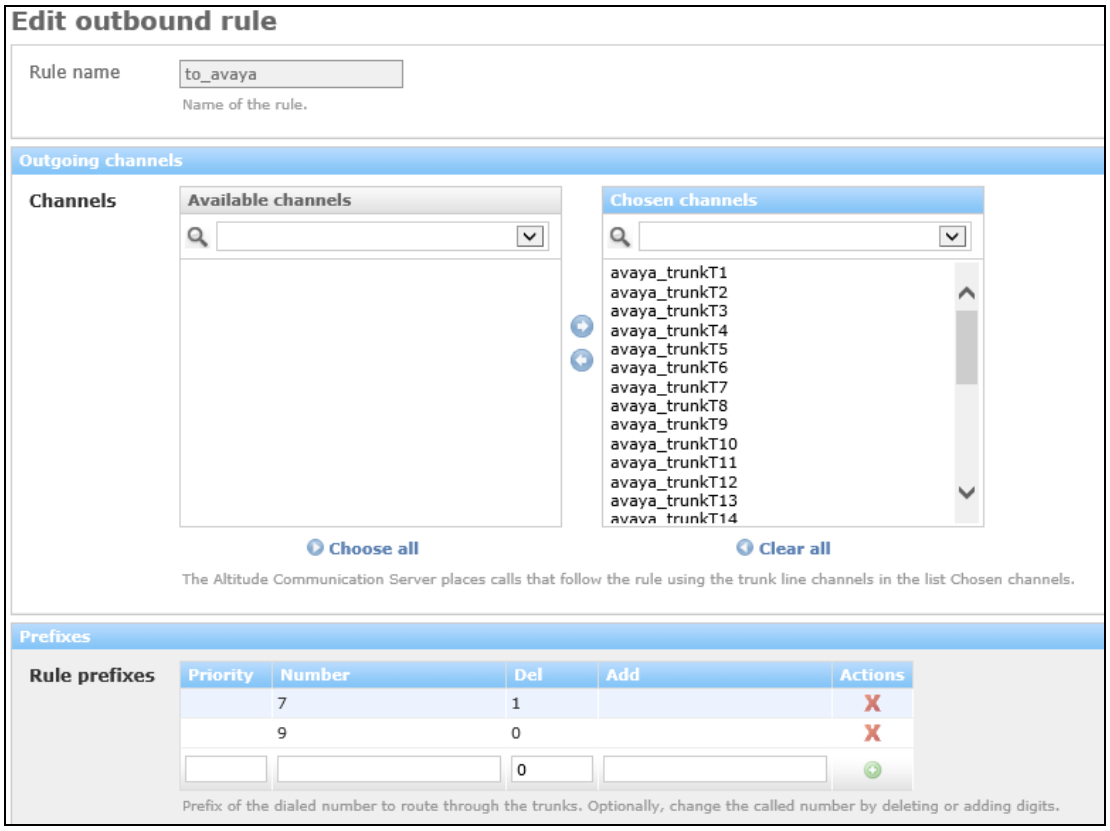


8.2.6. Display Outbound Rule

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, AES, Session Manager and Altitude uCI 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.

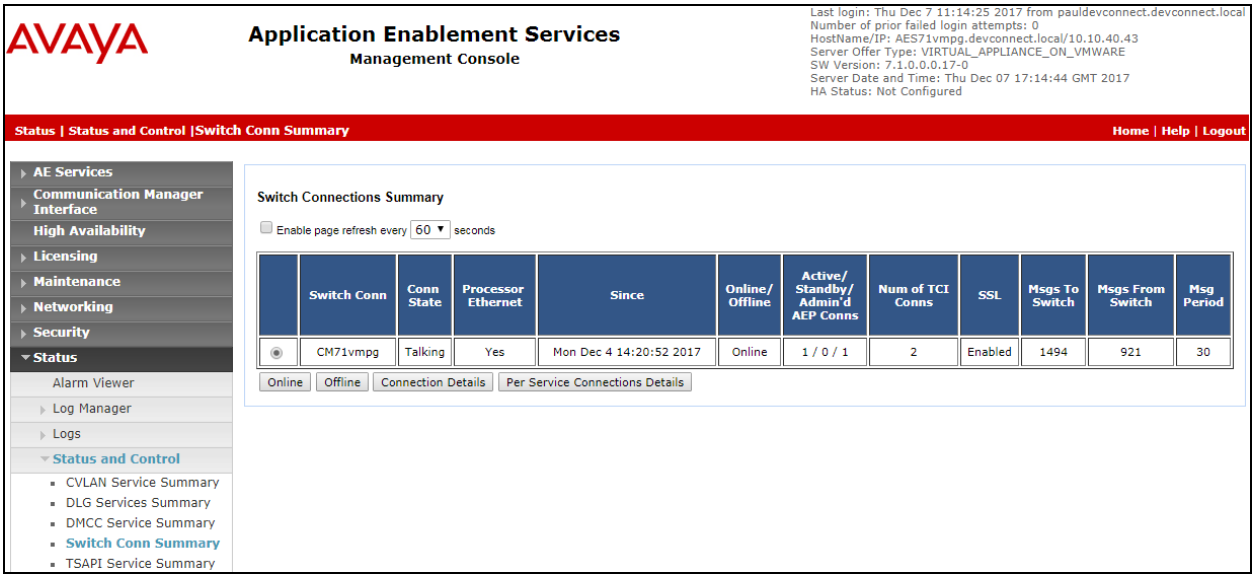
9.1. Verify Avaya Aura® Communication Manager CTI link

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 5.3.3**, as shown below.

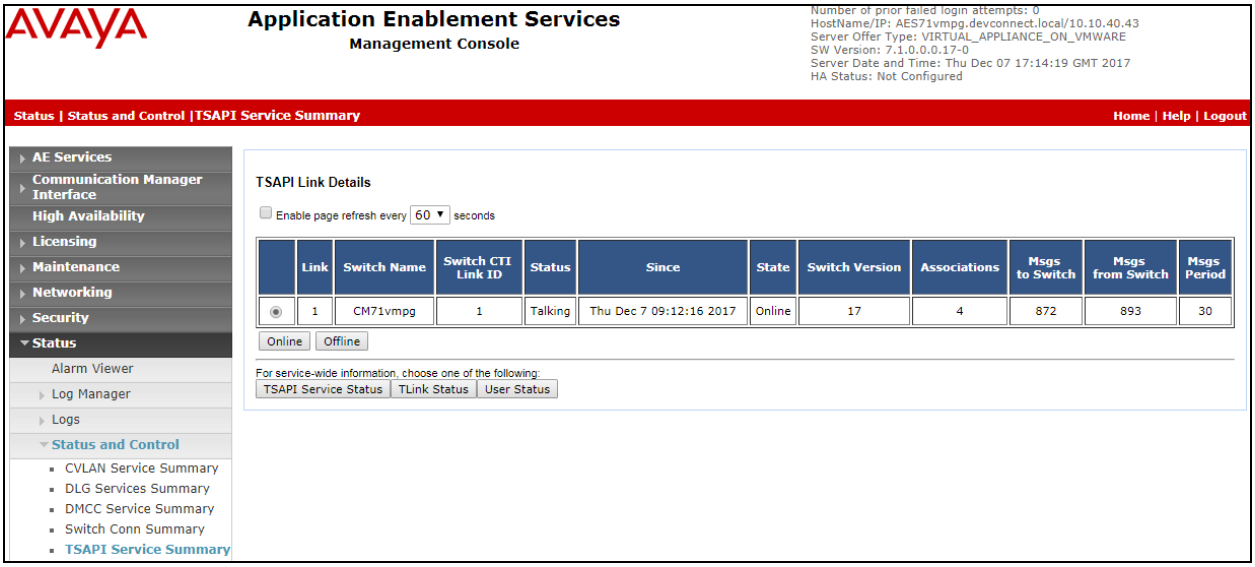
```
status aesvcs cti-link

                         AE SERVICES CTI LINK STATUS

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

1      7        no     AES71vmpg        established   87       61
```

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 **Switch Conn Summary** as shown below and note the **Conn State** is **Talking** and **SSL** is **Enabled**.

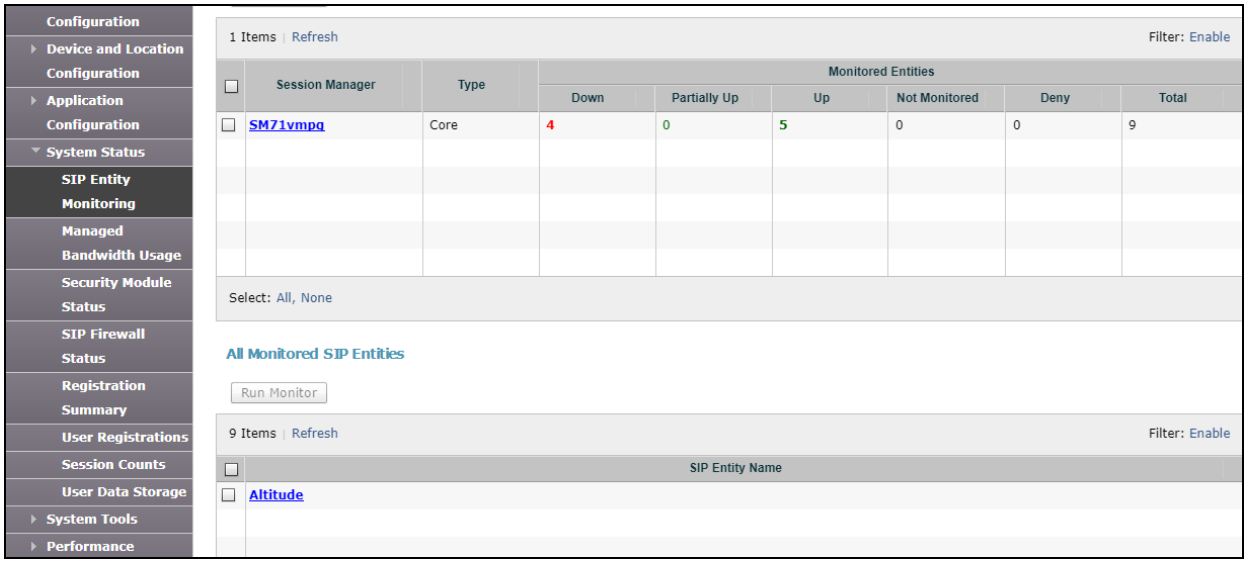


Click on the **TSAPI Service Summary** and the **State** should show **Online** as shown below.

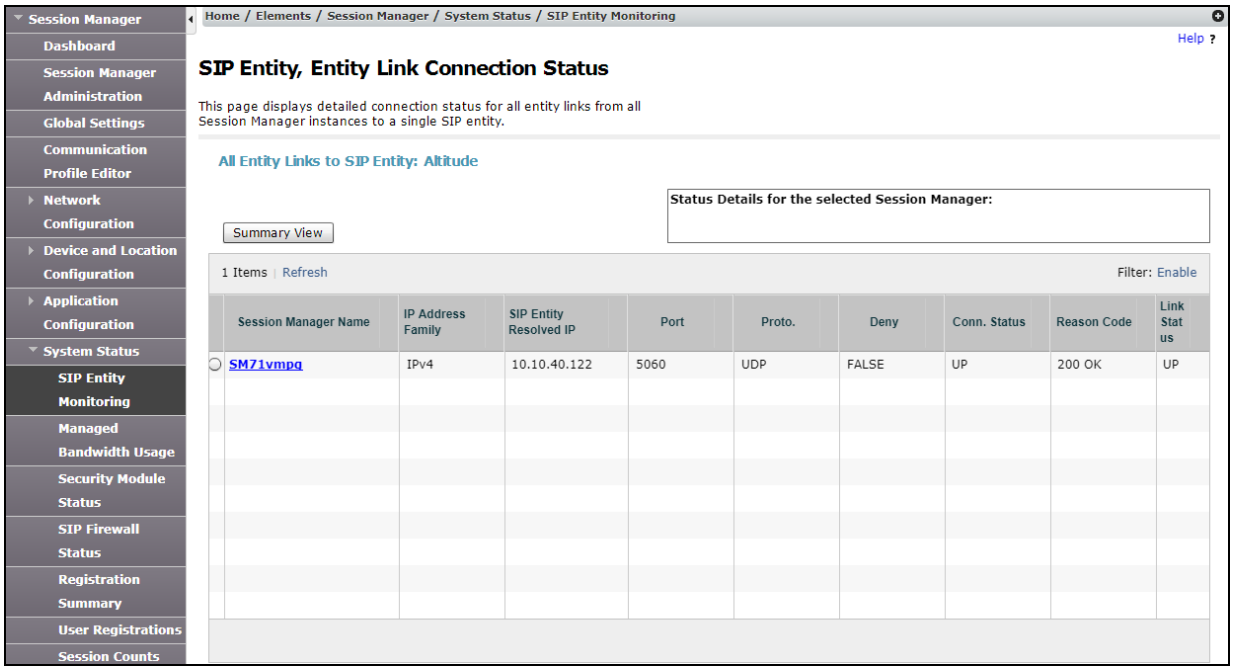


9.3. Verify SIP Entity

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.

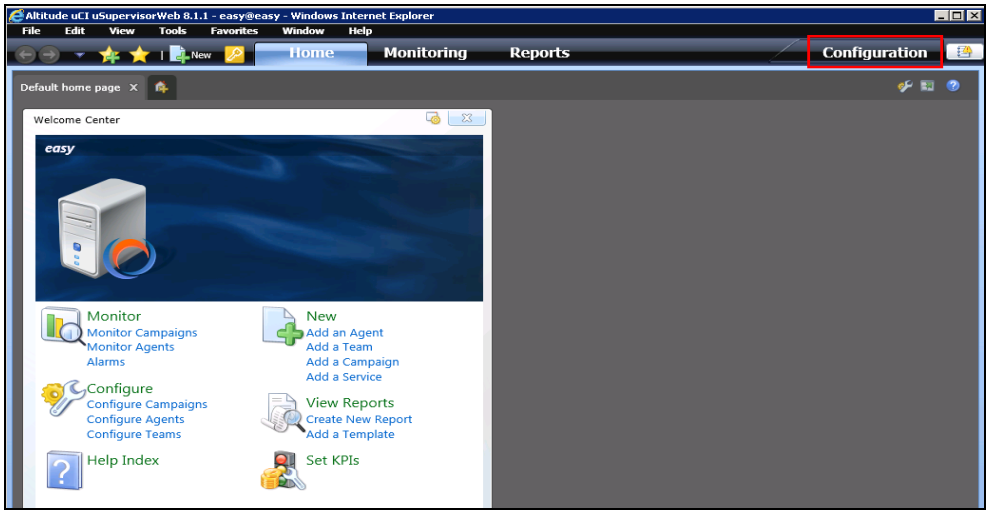


Verify that the **Conn Status** and **Link Status** are showing as **up**, as they are below for the Altitude SIP Entity that was selected from the previous page.

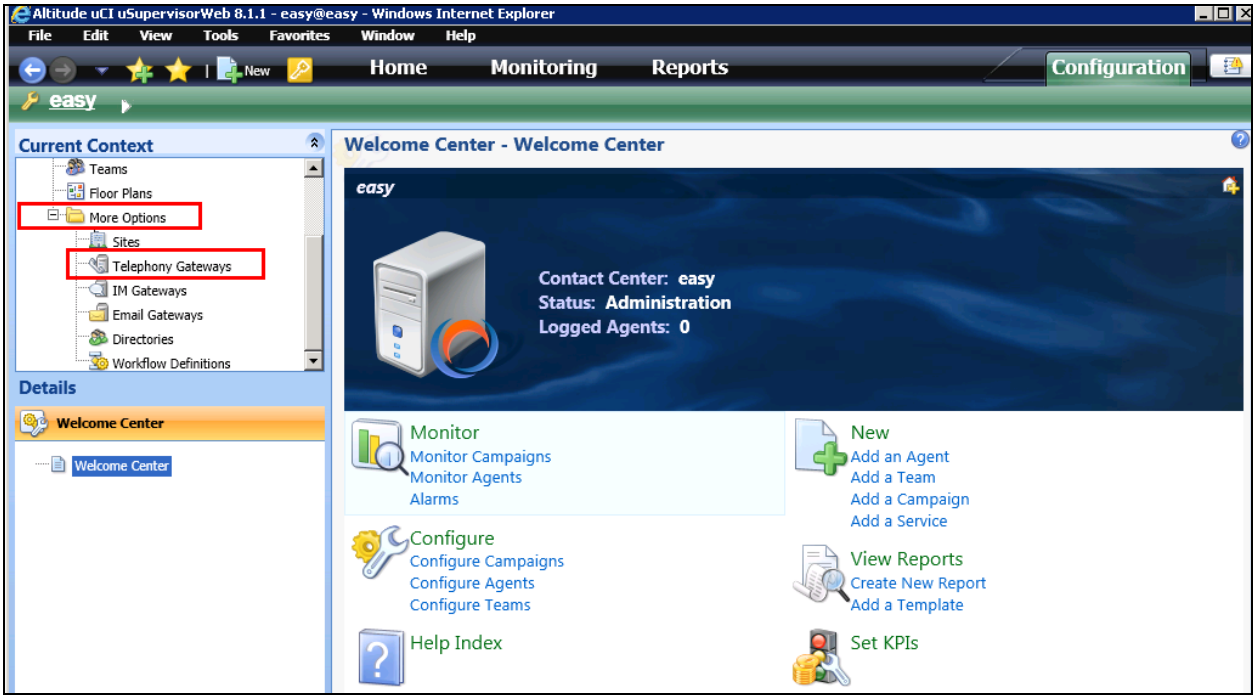


9.4. Verify Altitude Server is running correctly

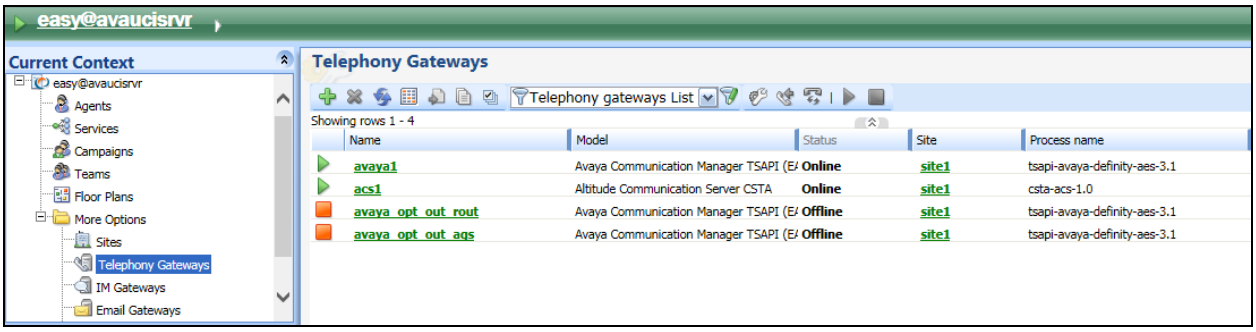
Log in to the uSupervisor web session as shown in **Section 8**. Start the Contact Center, if not already started, by clicking the menu option **Tools → Start contact center…**, (not shown).Once logged in select **Configuration**, highlighted below.



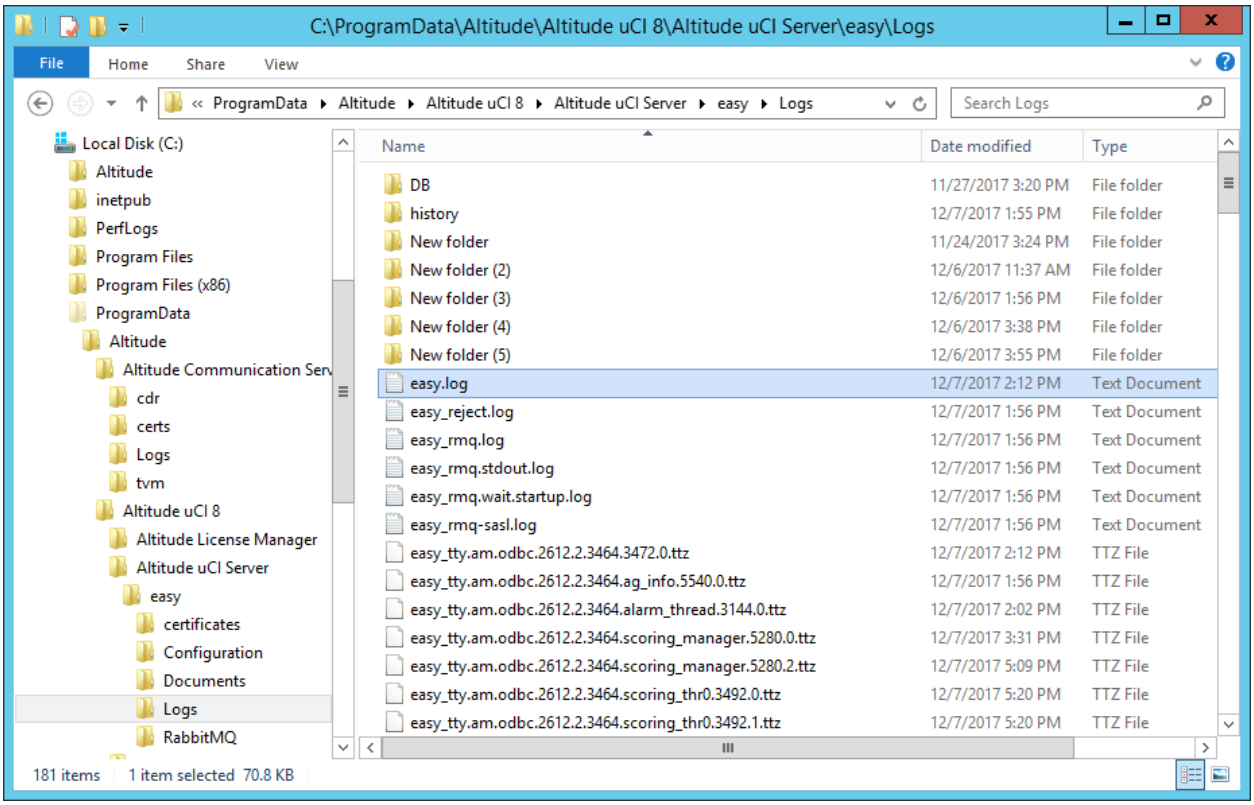
Select **More Options → Telephony Gateways** in the left panel.



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



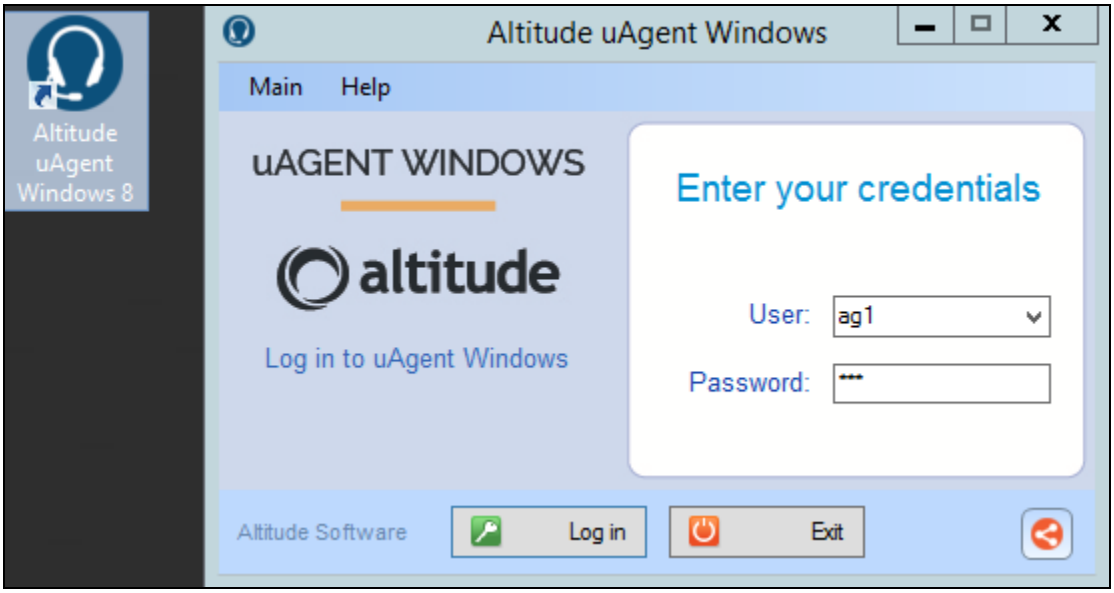
Open **easy.log** file located at **C:\ProgramData\Altitude\Altitude uCI 8\Altitude uCI Server\easy\Logs**.



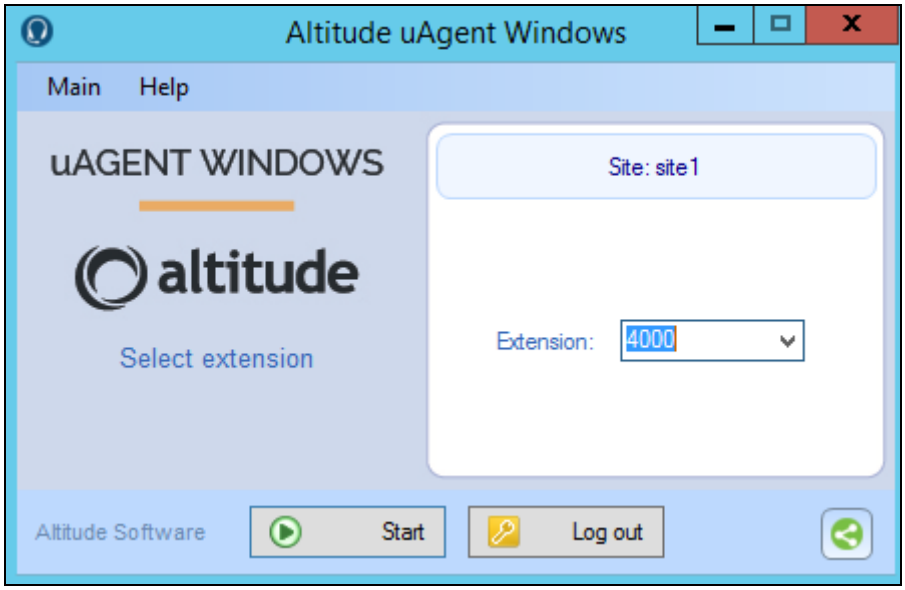
If there are any issues with connecting to the AES server then this will be displayed in the **easy.log** file.

9.5. Verify Altitude uAgent Windows

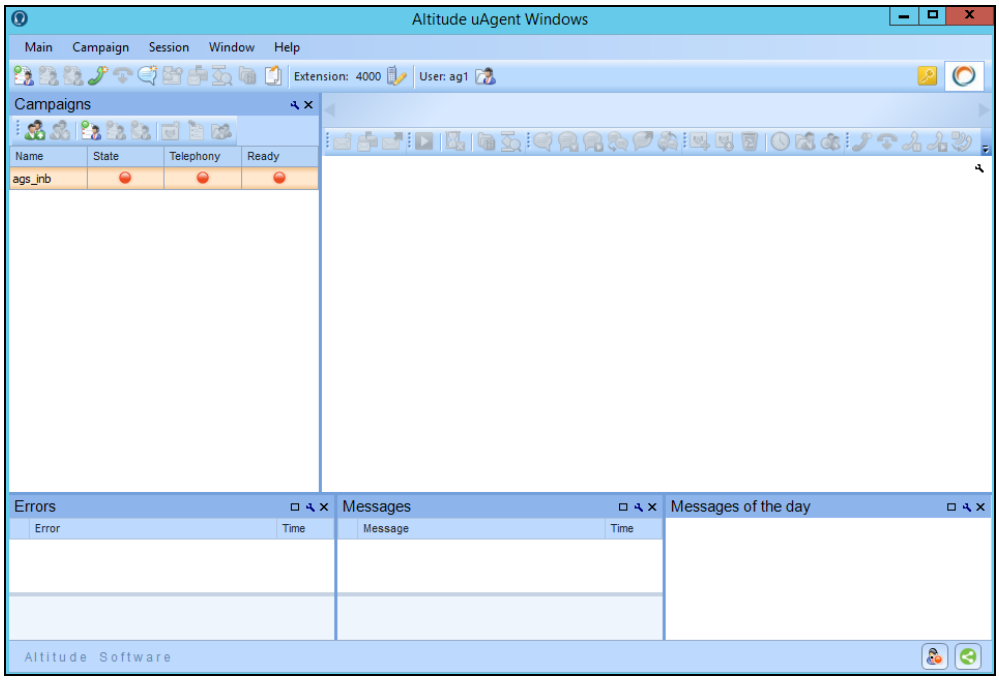
Log in to the Altitude uAgent Windows. Enter the proper credentials and click on **Log in**.



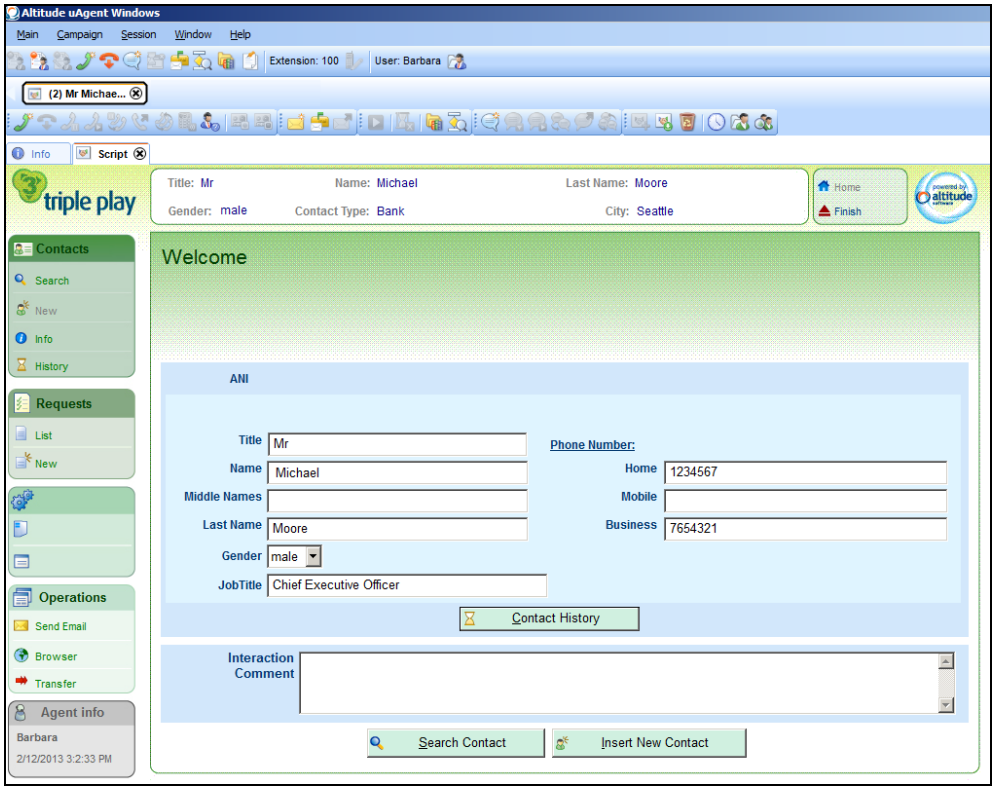
Enter the extension number to be monitored and click on **Start**.



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.



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



10. Conclusion

These Application Notes describe the configuration steps required for Altitude uCI 8 from Altitude Software to interoperate with Avaya Aura® Session Manager R7.1 and Avaya Aura® Application Enablement Services R7.1 to control Agents logged into Avaya Aura® Communication Manager. All test cases were completed successfully. 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 7.1

[4] *Administering Avaya Aura® Session Manager* – Release 7.1

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

Appendix

A routing point/VDN was added to solve an issue found during compliance testing (see **Section 2.2**). When a call is placed directly to the ACS (via aar routing and SIP Trunk) and the call is then transferred back into the "incoming VDN" there is call data missing or distorted. This is the calling number which appears as TSAPI Call ID. When a VDN was added that routes the call to the ACS via aar and SIP Trunk this issue is resolved and the configuration of this VDN and corresponding Vector are shown below.

```
change vdn 4904                                                  Page   1 of   3
                           VECTOR DIRECTORY NUMBER

                            Extension: 4904
                                Name*: Altitude_QRP
                          Destination: Vector Number        47
                   Attendant Vectoring? n
                  Meet-me Conferencing? n
                    Allow VDN Override? y
                                  COR: 1
                                  TN*: 1
                             Measured: none     Report Adjunct Calls as ACD*? n


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



* Follows VDN Override Rules
```

Page 2

```
change vdn 4904                                                  Page   2 of   3
                           VECTOR DIRECTORY NUMBER

                           AUDIX Name:
                   Return Destination*:
               VDN Timed ACW Interval*:      After Xfer or Held Call Drops*? n
                      BSR Application*:
         BSR Available Agent Strategy*: 1st-found      Used for BSR Polling? n
                     BSR Tie Strategy*: system

               Observe on Agent Answer? n

  Send VDN as Called Ringing Name Over QSIG? n

              Display VDN for Route-To DAC*? n
            VDN Override for ASAI Messages*: no

                       BSR Local Treatment*? n

              Reporting for PC or POM Calls? n
           Pass Prefixed CPN to VDN/Vector*? system
* Follows VDN Override Rules
```

Page 3

```
change vdn 4904                                                  Page   3 of   3
                            VECTOR DIRECTORY NUMBER

                                VDN VARIABLES*

                    Var  Description       Assignment
                    V1
                    V2
                    V3
                    V4
                    V5





                    VDN Time-Zone Offset*: + 00:00
                    Daylight Saving Rule*: system
 Use VDN Time Zone For Holiday Vectoring*? n
    Apply Ringback for Auto Answer calls*? y

* Follows VDN Override Rules
```

The corresponding **Vector** shows the call is simply routed to the ACS server via the **Adjunct Routing Link** controlled by a Altitude Automated Agents routing agent in a routing campaign.

```
change vector 47                                                 Page   1 of   6
                                  CALL VECTOR

    Number: 47               Name: Altitude_QRP
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    300 secs hearing ringback
03 stop
04
05
06
07
08
09
10
11
12
```

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.