Avaya Solution & Interoperability Test Lab

A Sample Configuration for Altitude uCI with Avaya Communication Manager and Avaya Application Enablement Services - Issue 1.0

Abstract

These Application Notes describe the configuration steps required for Altitude uCI (Unified Communication Interaction) to successfully interoperate with Avaya Communication Manager and Avaya Application Enablement Services (AES). The objective of the test was to evaluate interoperability of the above-mentioned products in a contact center, handling predictive outbound and inbound calling campaigns, as well as agent blending. Information in these Application Notes has been obtained through interoperability compliance testing and additional technical discussions. Testing was conducted via the Developer*Connection* Program at the Avaya Solution and Interoperability Test Lab.

1. Introduction

These Application Notes describe the compliance-test configuration used to test the Altitude uCI suite with Avaya Communication Manager and Avaya Application Enablement Services (AES). **Figure 1** provides a high level topology.

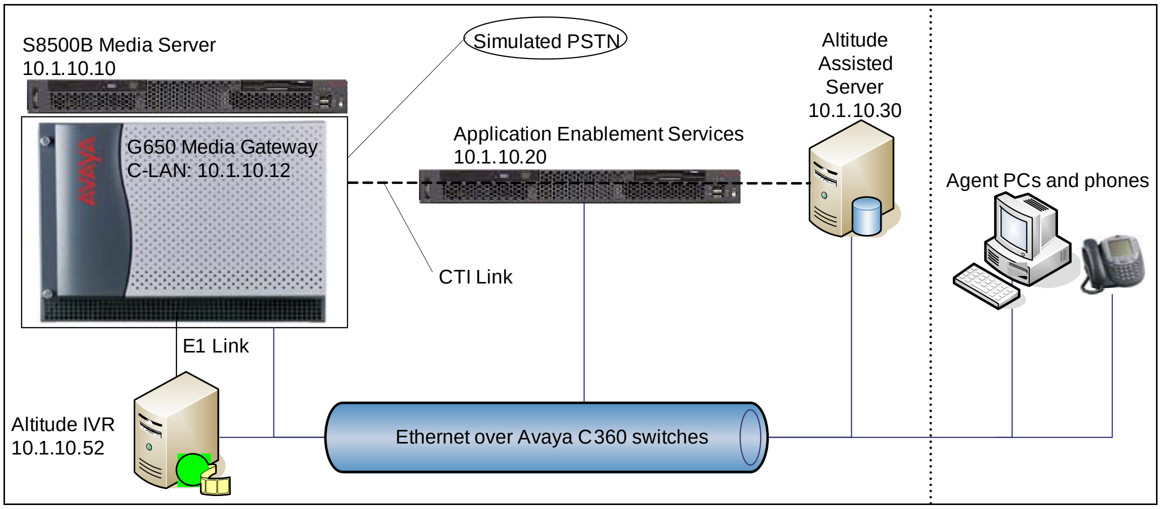


Figure 1: High Level Network Diagram

Altitude uCI is an integrated contact center application suite, focused on the improvement of the overall productivity of contact centers. The Altitude uCI suite includes the following modules, all of which were run on the Altitude Assisted Server except Altitude IVR and Altitude uAgent:

- Altitude uSupervisor is the administration and supervision tool, providing a holistic view of the contact center operation.
- Altitude uAgent is a desktop application for contact center agents, including media handling capabilities and execution of scripts.
- Altitude Voice enables integration of the above tools with the PBX.
- Altitude Voice Outbound is a software dialer with sophisticated contact list management features and support to multiple pacing modes from preview to predictive.
- Altitude uRouter, configured as an add-on to Altitude Voice, is a multi-channel software ACD.
- Altitude IVR is an IVR running on Wintel and Intel Dialogic hardware, connecting to Avaya Communication Manager voice switch using CTI and either CAS or ISDN.

The compliance testing exercised the Altitude uCI modules that rely on integration with Application Enablement Services: Altitude Voice, Altitude Voice Outbound, Altitude IVR, and Altitude uRouter. Altitude uSupervisor and Altitude uAgent were also used to perform configuration tasks and exercise the functionality of the solution.

2. Equipment and Software Validated

The following equipment and software were used for the sample configuration provided:

Equipment	Software
Avaya S8500B Media Server	Avaya Communication Manager 3.1.2
Avaya G650 Media Gateway: • TN799DP C-LAN Circuit Pack • TN2302AP IP Media Processor Circuit Pack • TN2464BP DS-1 Circuit Pack	 HW01/FW017 HW20/FW110 HW05/FW018
Avaya Application Enablement Services	3.1
Avaya 4620 IP Telephones Avaya 4625 IP Telephones	2.4 2.5
Server	Windows Server 2003 Altitude Assisted Server 7.1.A1 - Altitude uSupervisor 7.1.A1 - Altitude Voice 7.1.A1 - Altitude uRouter 7.1.A1 MS SQL Server 2000
Server	Windows Server 2003 Altitude IVR 7.1.A1
PCs	Windows XP Altitude uAgent 7.1.A1

3. Configure Avaya Communication Manager

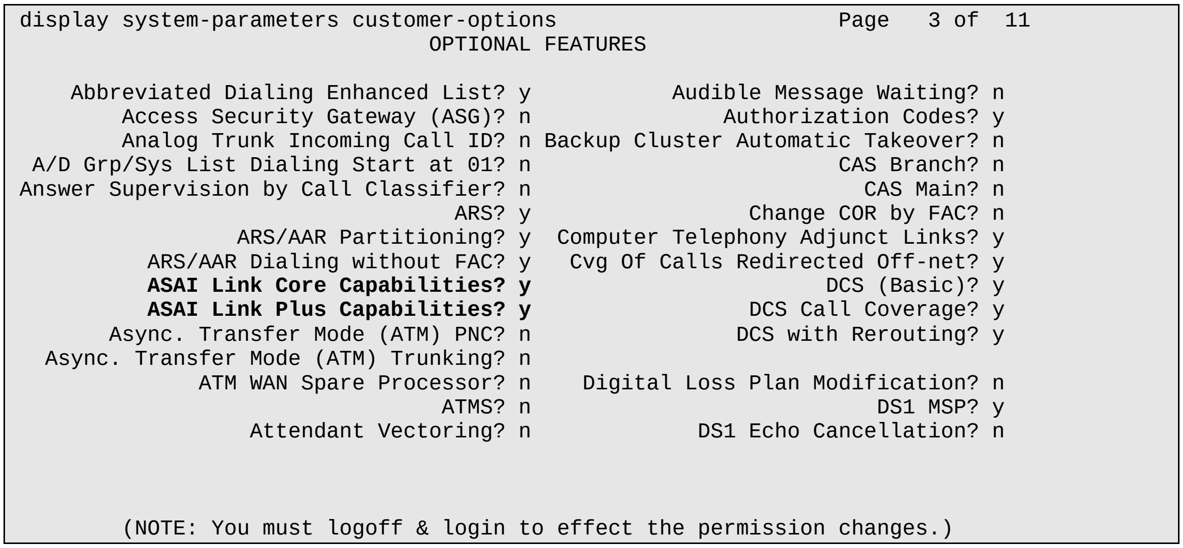
This section provides the procedures for configuring Avaya Communication Manager. The procedures fall into the following areas:

- Administer the C-LAN for AES connectivity.
- Administer the IP service for AES connectivity.
- Administer the CTI-link for the TSAPI service.
- Administer the call vectors for adjunct routing and predictive dialing.
- Administer the DS-1 and stations for the IVR.

3.1. Administer the C-LAN for AES Connectivity

Verify that the **ASAI Link Core Capabilities** customer option is set to “y” on Page 3 using the “display system-parameters customer-options” command, as shown in **Figure 2**. If the **ASAI Link Core Capabilities** is not set to “y”, then contact the Avaya sales team or business partner and request a new license file with this option set.

Also verify that the **ASAI Link Plus Capabilities** customer option is set to “y”, for applications that require it. (Examples include applications that use Adjunct Routing and Switch Classified Outbound Calls amongst others).

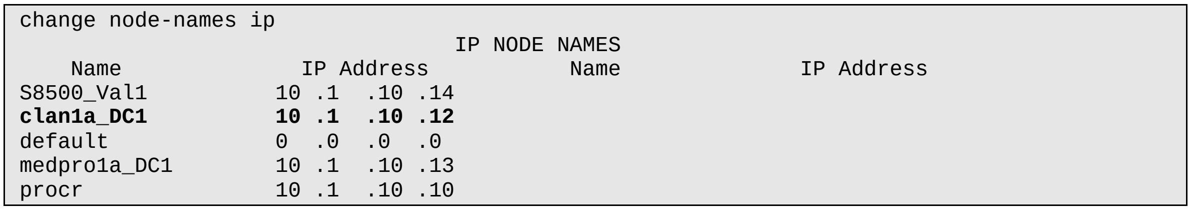


```
display system-parameters customer-options                      Page   3 of  11
                                OPTIONAL FEATURES

    Abbreviated Dialing Enhanced List? y           Audible Message Waiting? n
        Access Security Gateway (ASG)? n               Authorization Codes? y
        Analog Trunk Incoming Call ID? n Backup Cluster Automatic Takeover? n
 A/D Grp/Sys List Dialing Start at 01? n                        CAS Branch? n
Answer Supervision by Call Classifier? n                          CAS Main? n
                                  ARS? y                 Change COR by FAC? n
                 ARS/AAR Partitioning? y  Computer Telephony Adjunct Links? y
          ARS/AAR Dialing without FAC? y   Cvg Of Calls Redirected Off-net? y
          ASAI Link Core Capabilities? y                       DCS (Basic)? y
          ASAI Link Plus Capabilities? y                 DCS Call Coverage? y
       Async. Transfer Mode (ATM) PNC? n                DCS with Rerouting? y
  Async. Transfer Mode (ATM) Trunking? n
              ATM WAN Spare Processor? n    Digital Loss Plan Modification? n
                                 ATMS? n                           DS1 MSP? y
                  Attendant Vectoring? n             DS1 Echo Cancellation? n



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

Figure 2: System-Parameters Customer-Options Form

The C-LAN administration procedure will involve adding an IP node, an IP interface, and a data module.

First, add an entry for the C-LAN in the node-names form. Use the “change node-names ip” command, as shown in **Figure 3**. In this case, “clan1a_DC1” and “10.1.10.12” are entered as the **Name** and **IP Address** for the C-LAN that will be used for connectivity to the AES server. The actual node name and IP address may vary. Submit these changes.

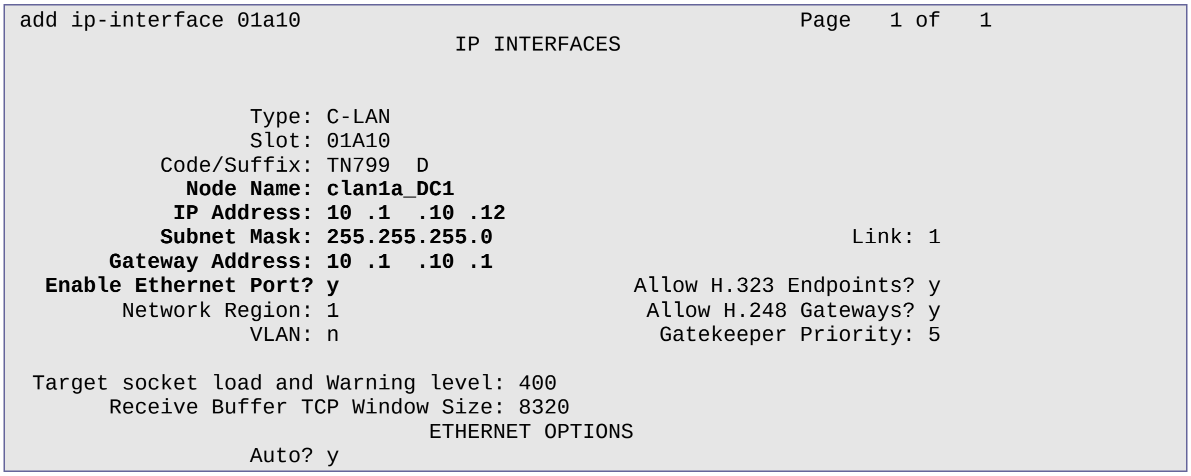


```
change node-names ip
                                  IP NODE NAMES
    Name              IP Address          Name              IP Address
S8500_Val1          10 .1  .10 .14
clan1a_DC1          10 .1  .10 .12
default             0  .0  .0  .0
medpro1a_DC1        10 .1  .10 .13
procr               10 .1  .10 .10
```

Figure 3: IP Node Names Form

Next, add the C-LAN to the system configuration using the “add ip-interface SLOT#” command. Note that the actual slot number may vary. In this case, “01A10” is used as the slot number, as shown in **Figure 4** below. Enter the node name assigned from **Figure 3** above, and the **IP address** field will then be populated automatically. Set the **Enable Ethernet Port** field to “y”.

The values to be entered for the **Subnet Mask** and **Gateway Address** fields will be determined by the network administrator. Submit these changes.

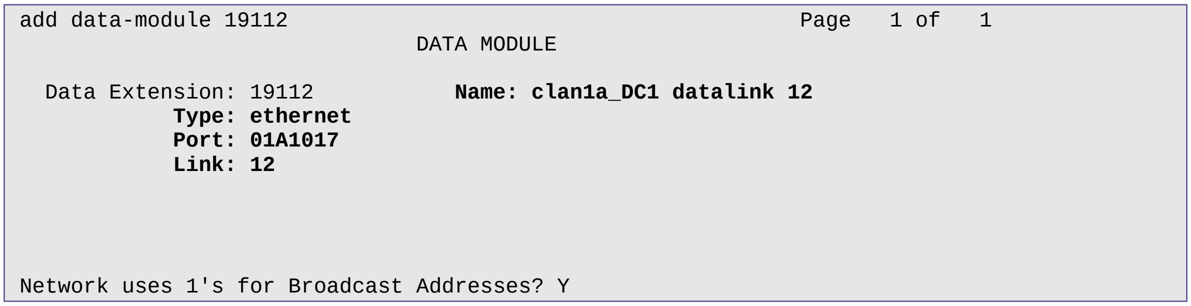


```
add ip-interface 01a10                                       Page   1 of   1
                                  IP INTERFACES


                  Type: C-LAN
                  Slot: 01A10
           Code/Suffix: TN799  D
             Node Name: clan1a_DC1
            IP Address: 10 .1  .10 .12
           Subnet Mask: 255.255.255.0                            Link: 1
       Gateway Address: 10 .1  .10 .1
  Enable Ethernet Port? y                       Allow H.323 Endpoints? y
        Network Region: 1                        Allow H.248 Gateways? y
                  VLAN: n                         Gatekeeper Priority: 5

 Target socket load and Warning level: 400
       Receive Buffer TCP Window Size: 8320
                                ETHERNET OPTIONS
                  Auto? y
```

Figure 4: IP Interface Form

Next, add a new data module using the “add data-module x” command, where “x” is an available extension. Enter the following values as shown in **Figure 5**.

- **Name:** Descriptive name
- **Type:** “ethernet”
- **Port:** Same slot number from **Figure 4** and port “17”
- **Link:** A link number not previously assigned on this switch

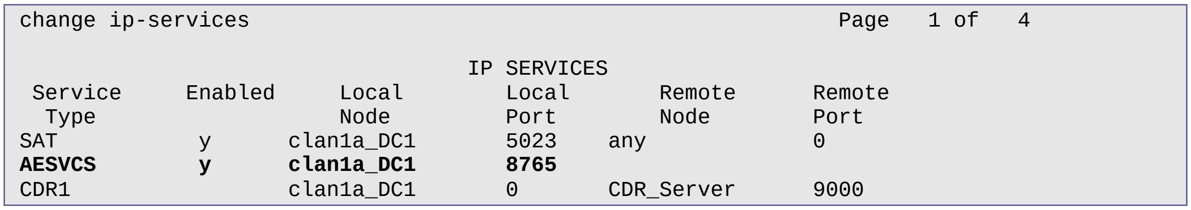


```
add data-module 19112                                        Page   1 of   1
                               DATA MODULE

  Data Extension: 19112           Name: clan1a_DC1 datalink 12
            Type: ethernet
            Port: 01A1017
            Link: 12





Network uses 1's for Broadcast Addresses? Y
```

Figure 5: Data Module Form

3.2. Administer the IP Service for AES Connectivity

Administer the IP Service for Avaya Application Enablement Services (AES) with the “change ip-services” command. Add an entry with the following values for fields on **Page 1** as shown in **Figure 6** below:



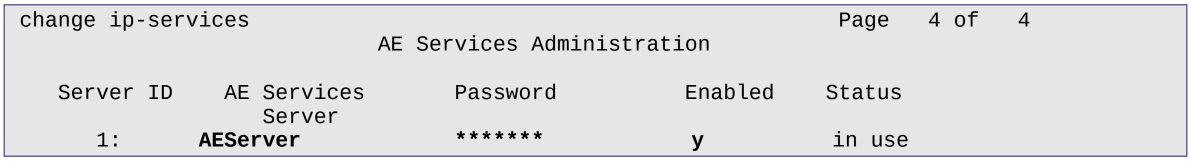
```
change ip-services                                            Page   1 of   4

                                  IP SERVICES
 Service     Enabled     Local        Local       Remote      Remote
  Type                   Node         Port        Node        Port
SAT           y      clan1a_DC1       5023    any             0
AESVCS        y      clan1a_DC1       8765
CDR1                 clan1a_DC1       0       CDR_Server      9000
```

Figure 6: IP Services Form Page 1

Go to **Page 4** of the IP Services form, and enter these values as shown in **Figure 7**:

- **AE Services:** Same name administered on the AES. In this case, “AEServer”.
- **Password:** Same password to be administered on the AES
- **Enabled:** “y”

Note that the name and password entered for the **AE Services Server** and **Password** fields must match the name and password on the AES. The administered name can be obtained from the AES server by typing “uname –n” at the Linux command prompt, and the password is set on the AES server under **Administration** > **Switch Connections** > **Edit Connection** > **Set Password**.

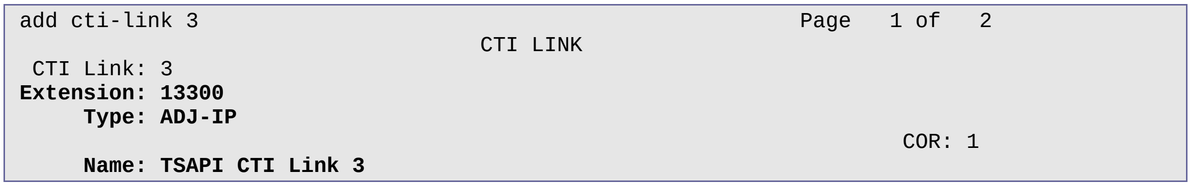


```
change ip-services                                            Page   4 of   4
                            AE Services Administration

   Server ID    AE Services       Password          Enabled    Status
                   Server
      1:      AEServer            *******            y          in use
```

Figure 7: IP-Services Form Page 4

3.3. Administer the CTI Link for the TSAPI Service

Add a CTI link and set the values as shown in **Figure 8** below using the “add cti-link x” command, where “x” is an available CTI link number. Enter a valid extension number in the **Extension** field. Note that the CTI link number and extension number may vary. Enter “ADJ-IP” in the **Type** field, and a descriptive name in the **Name** field. The rest of the values may be left at the defaults. Submit these changes.

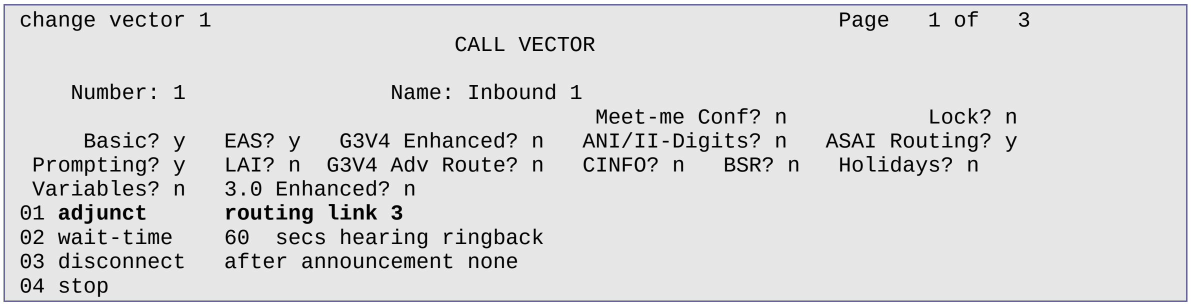


```
add cti-link 3                                               Page   1 of   2
                                    CTI LINK
 CTI Link: 3
Extension: 13300
     Type: ADJ-IP
                                                                     COR: 1
     Name: TSAPI CTI Link 3
```

Figure 8: CTI-Link Form

3.4. Administer Call Vector for Adjunct Routing

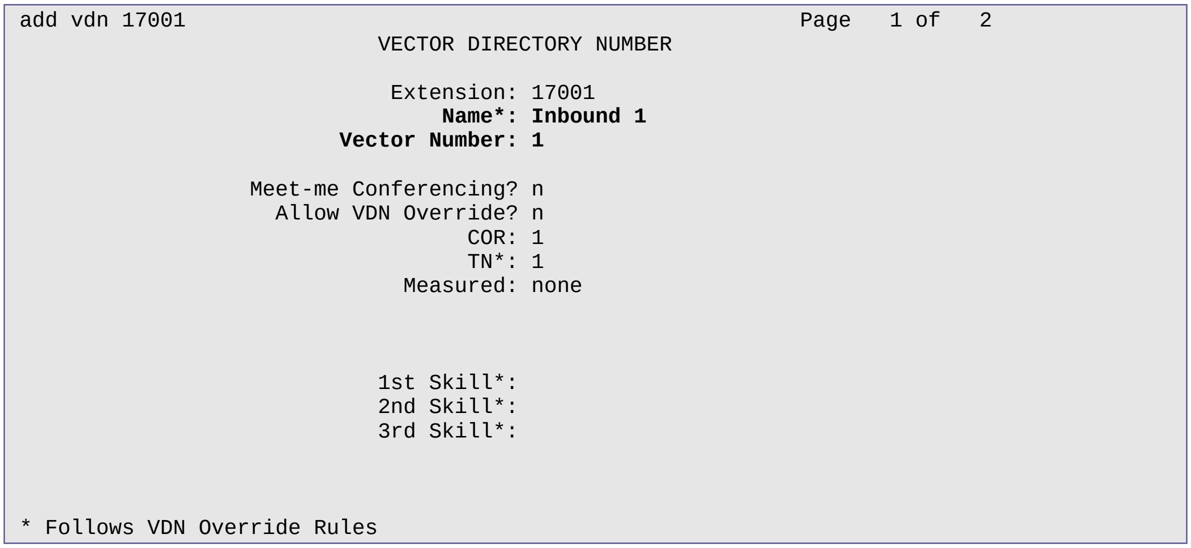
This configuration step is only needed for configurations where the Altitude uRouter module is used to route incoming calls to agents. Modify a vector to send adjunct route requests to the CTI link defined previously in **Figure 8**. Note that the vector in **Figure 9** below is a sample vector only and can be modified as needed for different call treatments.



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

    Number: 1                Name: Inbound 1
                                             Meet-me Conf? n           Lock? n
     Basic? y   EAS? y   G3V4 Enhanced? n   ANI/II-Digits? n   ASAI Routing? y
 Prompting? y   LAI? n  G3V4 Adv Route? n   CINFO? n   BSR? n   Holidays? n
 Variables? n   3.0 Enhanced? n
01 adjunct      routing link 3
02 wait-time    60  secs hearing ringback
03 disconnect   after announcement none
04 stop
```

Figure 9: Vector for Adjunct Routing

Add a Vector Directory Number (VDN) as shown in **Figure 10** below, and set the Vector Number field to the same call vector number assigned in **Figure 9**.

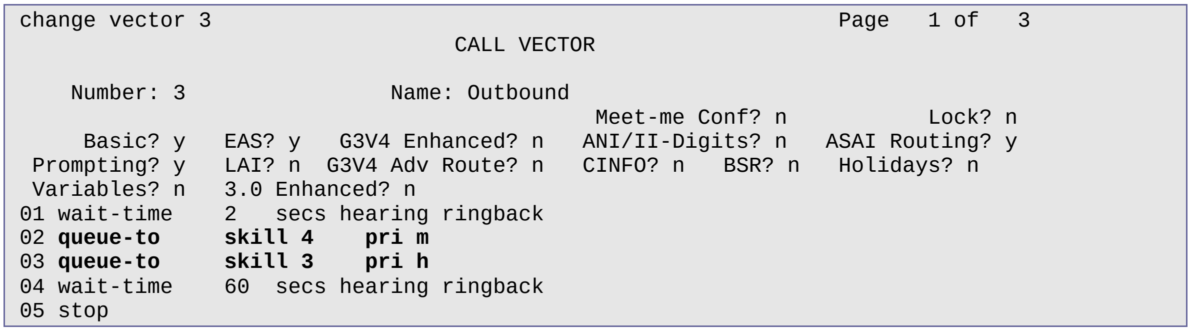


```
add vdn 17001                                                Page   1 of   2
                            VECTOR DIRECTORY NUMBER

                             Extension: 17001
                                 Name*: Inbound 1
                         Vector Number: 1

                  Meet-me Conferencing? n
                    Allow VDN Override? n
                                   COR: 1
                                   TN*: 1
                              Measured: none



                            1st Skill*:
                            2nd Skill*:
                            3rd Skill*:



* Follows VDN Override Rules
```

Figure 10: VDN Form

3.5. Administer Call Vector for Routing Predictive Calls

This configuration step is only needed in predictive dialing configurations where a vector routes outbound calls to a skill. The Altitude system requires that there are 2 queue-to skill steps in the vector, as shown in **Figure 11** below. The first queue-to step is to a skill with no agents and the second is to the skill where the required agents are logged in. This is to stop Avaya Communication Manager from sending out messages too soon for the Altitude system.

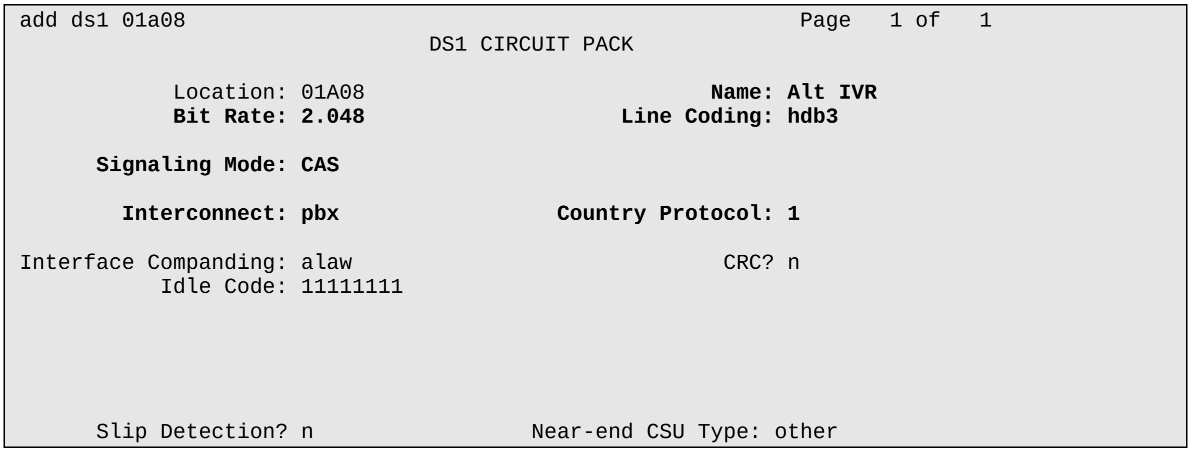


```
change vector 3                                                 Page   1 of   3
                                  CALL VECTOR

    Number: 3                Name: Outbound
                                              Meet-me Conf? n           Lock? n
     Basic? y   EAS? y   G3V4 Enhanced? n   ANI/II-Digits? n   ASAI Routing? y
 Prompting? y   LAI? n  G3V4 Adv Route? n   CINFO? n   BSR? n   Holidays? n
 Variables? n   3.0 Enhanced? n
01 wait-time    2   secs hearing ringback
02 queue-to     skill 4    pri m
03 queue-to     skill 3    pri h
04 wait-time    60  secs hearing ringback
05 stop
```

Figure 11: Vector for Predictive Outbound Dialing

3.6. Administer the DS-1 and stations for the IVR.

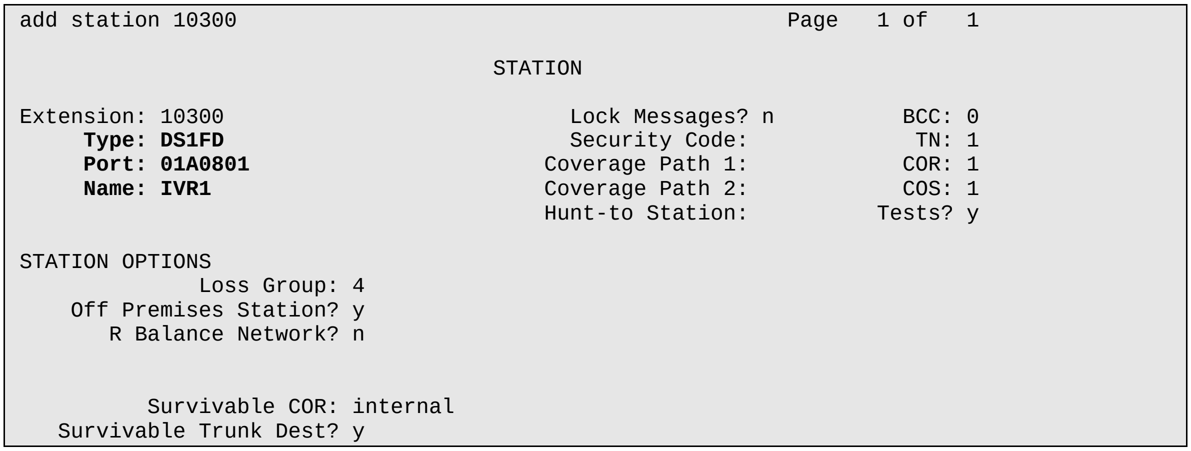
The Altitude IVR module connects to Avaya Communication Manager by means of a DS-1 connection using CAS signaling. The DS-1 is administered as shown in **Figure 12** below.



```
add ds1 01a08                                                Page   1 of   1
                                DS1 CIRCUIT PACK

            Location: 01A08                            Name: Alt IVR
            Bit Rate: 2.048                     Line Coding: hdb3

      Signaling Mode: CAS

        Interconnect: pbx                  Country Protocol: 1

Interface Companding: alaw                             CRC? n
           Idle Code: 11111111





      Slip Detection? n                 Near-end CSU Type: other
```

Figure 12: DS-1 Form

Each port of the DS-1 is terminated by a DS1FD station on the PBX which allows the Altitude IVR virtual agents to log in and answer calls. The DS1FD station is administered as shown in **Figure 13** below.



```
add station 10300                                           Page   1 of   1

                                     STATION

Extension: 10300                          Lock Messages? n          BCC: 0
     Type: DS1FD                          Security Code:             TN: 1
     Port: 01A0801                      Coverage Path 1:            COR: 1
     Name: IVR1                         Coverage Path 2:            COS: 1
                                        Hunt-to Station:          Tests? y

STATION OPTIONS
              Loss Group: 4
    Off Premises Station? y
       R Balance Network? n


          Survivable COR: internal
   Survivable Trunk Dest? y
```

Figure 13: DS1FD Station Form

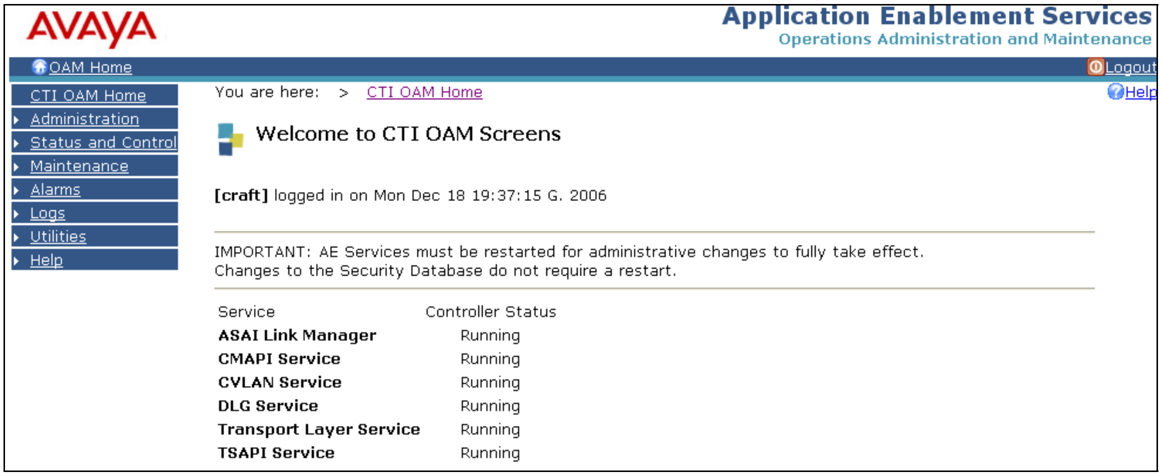
4. Configure Avaya Application Enablement Services

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

- Administer local IP.
- Administer switch connections.
- Administer TSAPI link.
- Add CTI User.

4.1. Administer Local IP

Prior to any administration, verify the TSAPI service has been licensed properly. Log into the AES OAM web interface, select CTI OAM Admin and check to make sure the TSAPI service is licensed as shown in **Figure 14** below. If the TSAPI service is not licensed, then contact the Avaya sales team or business partner for the correct license file.



Welcome to CTI OAM Screens

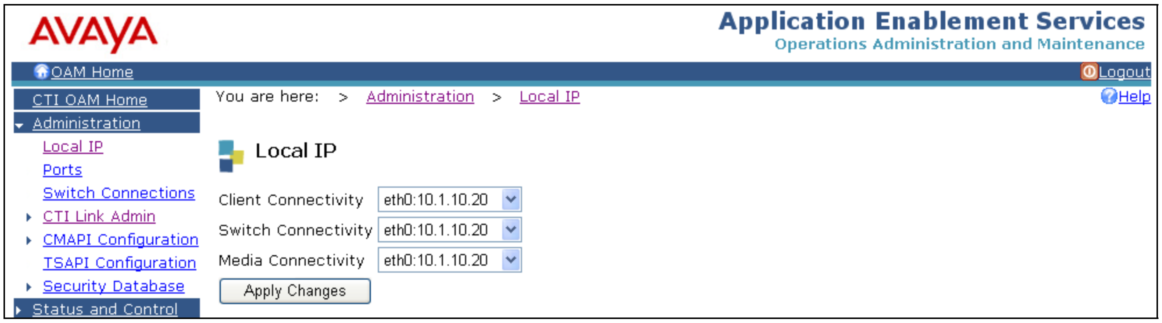
[craft] logged in on Mon Dec 18 19:37:15 G. 2006

IMPORTANT: AE Services must be restarted for administrative changes to fully take effect.
Changes to the Security Database do not require a restart.

Service	Controller Status
ASAI Link Manager	Running
CMAPI Service	Running
CVLAN Service	Running
DLG Service	Running
Transport Layer Service	Running
TSAPI Service	Running

Figure 14: OAM Home License

From the CTI OAM Admin menu, select **Administration > Local IP**. As shown in **Figure 15**, in the **Client Connectivity** field, select the local IP address that the Altitude system will use to connect to the AES server. In the **Switch Connectivity** field, select the local IP address the AES will use to connect to Avaya Communication Manager. Click on **Apply Changes**.



Client Connectivity: eth0:10.1.10.20

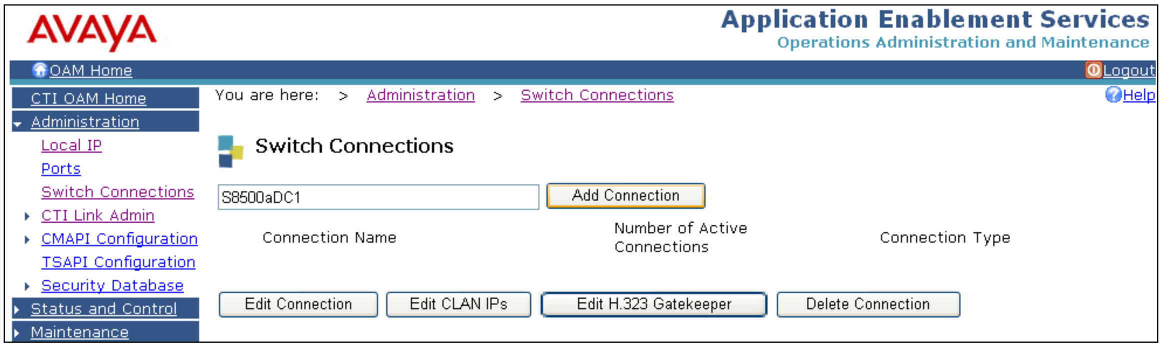
Switch Connectivity: eth0:10.1.10.20

Media Connectivity: eth0:10.1.10.20

Figure 15: Local IP

4.2. Administer Switch Connections

From the CTI OAM Admin menu, select **Administration > Switch Connections**, as shown in **Figure 16**. Enter a descriptive name for the switch connection and click on **Add Connection**. In this case, "S8500aDC1" is used, and the actual switch connection name may vary.

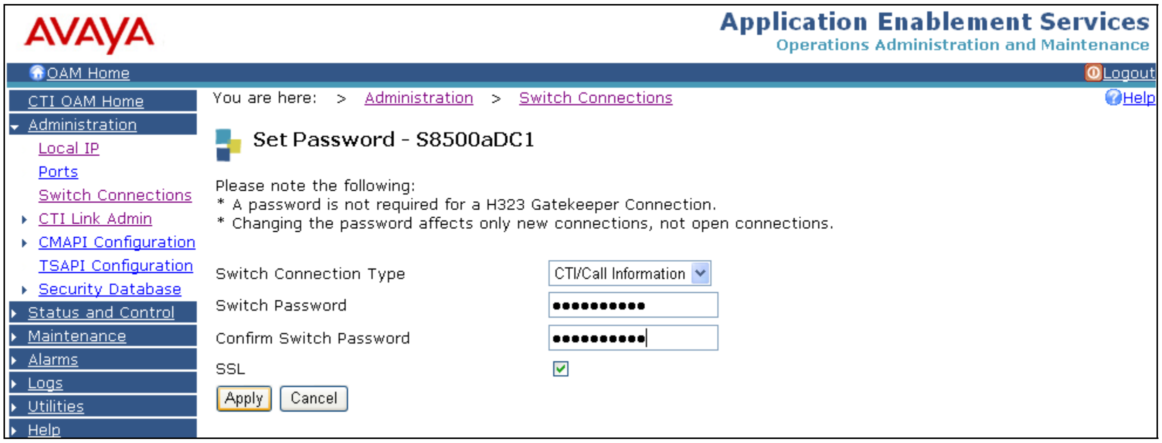


S8500aDC1

Connection Name	Number of Active Connections	Connection Type

Figure 16: Switch Connections

Next, the Set Password screen will be displayed by OAM, as shown in **Figure 17**. Enter the same password that was administered on Avaya Communication Manager on the IP Services form in **Figure 7**. Re-enter the same password in the **Confirm Switch Password** field. Note that the **SSL** field can be left at the default. Click on **Apply**.



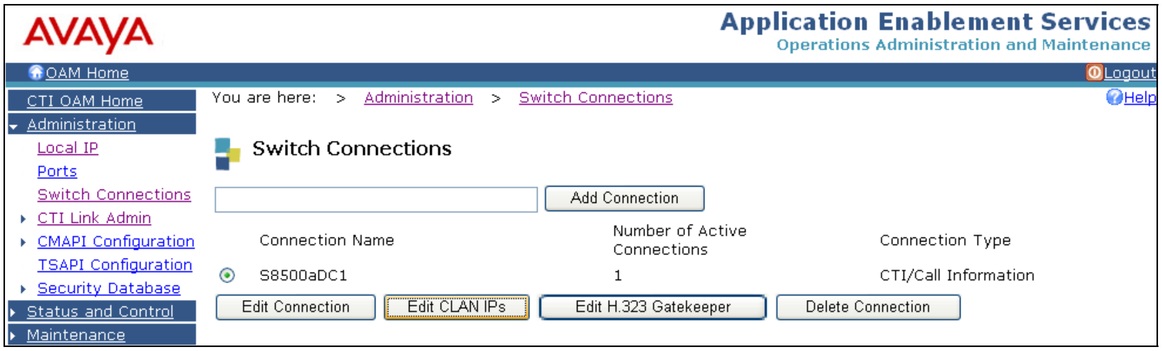
Set Password - S8500aDC1

Please note the following:
* A password is not required for a H323 Gatekeeper Connection.
* Changing the password affects only new connections, not open connections.

Switch Connection Type: CTI/Call Information
Switch Password: ●●●●●●●●●●●
Confirm Switch Password: ●●●●●●●●●●●
SSL: ☑

Figure 17: Set Password

From the Switch Connection page shown in **Figure 18,** select the newly added switch connection name and click on **Edit CLAN IPs**.

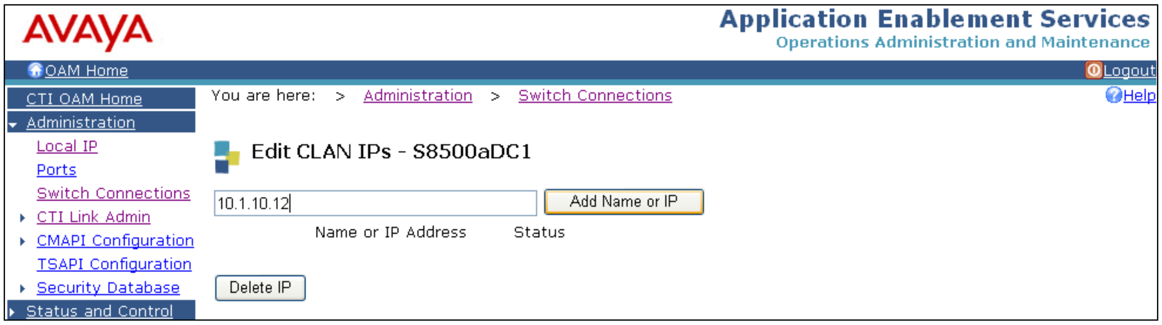


Switch Connections

	Connection Name	Number of Active Connections	Connection Type
●	S8500aDC1	1	CTI/Call Information

Figure 18: Switch Connections

On the Edit CLAN IPs page, enter the host name or IP address of the C-LAN used for AES connectivity as shown in **Figure 19**. In this case, “10.1.10.12” is used, which corresponds to the C-LAN administered on Avaya Communication Manager in **Figure 4**. Click on **Add Name or IP**.



Edit CLAN IPs - S8500aDC1

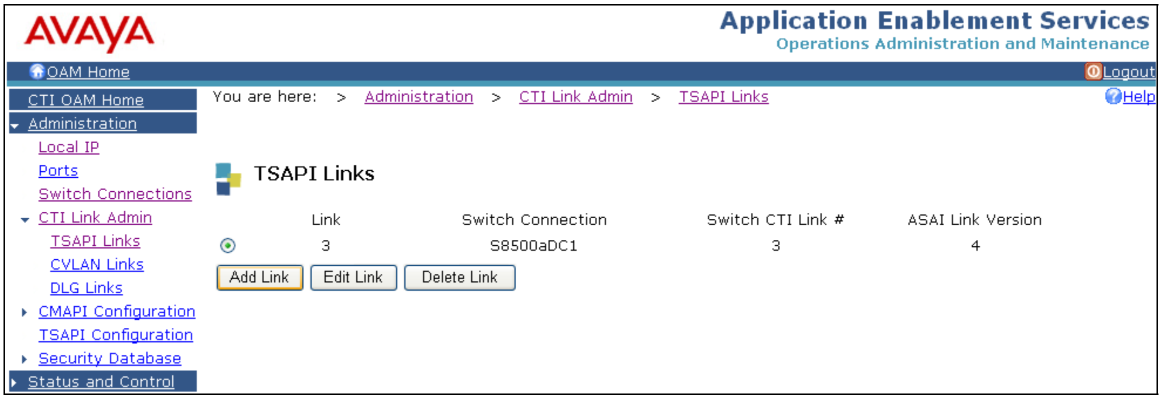
10.1.10.12

Name or IP Address Status

Figure 19: Edit CLAN IPs

4.3. Administer TSAPI Service

To administer a TSAPI link on AES, select **Administration > CTI Link Admin > TSAPI Links** from the CTI OAM Admin menu as shown in **Figure 20** below. Click on **Add Link**.



TSAPI Links

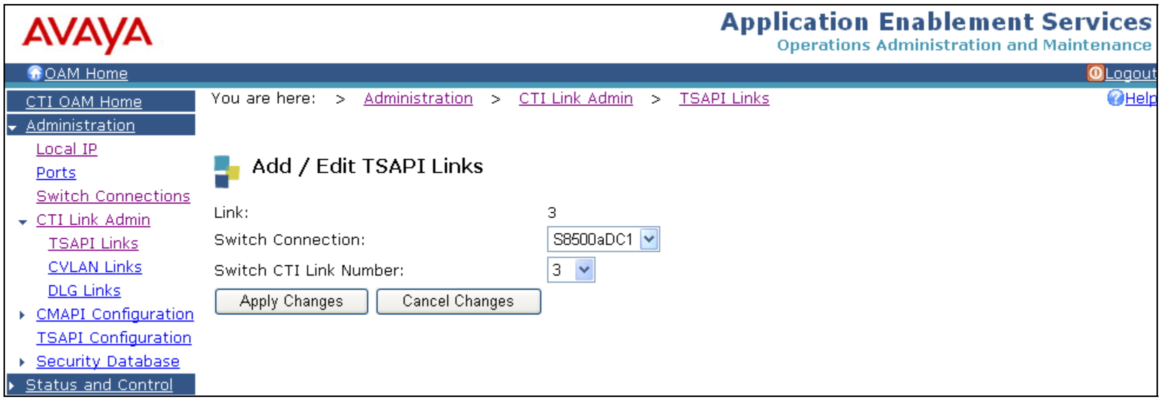
	Link	Switch Connection	Switch CTI Link #	ASAI Link Version
●	3	S8500aDC1	3	4

Figure 20: TSAPI Links

In the Add/Edit TSAPI Links screen, enter the following values as shown in **Figure 21**:

- **Switch Connection:** Administered switch connection configured back in **Figure 16**.
- **Switch CTI Link Number:** Corresponding CTI link number configured in **Figure 8**.

Note that the actual values for both fields may vary. Click on **Apply Changes**.



Add / Edit TSAPI Links

Link: 3

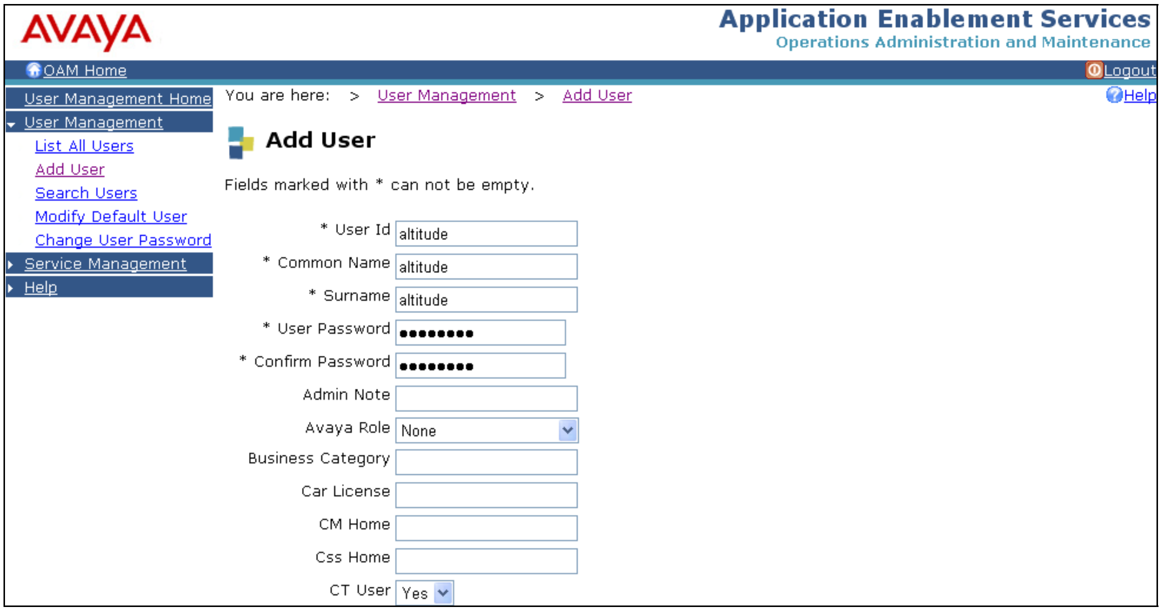
Switch Connection: S8500aDC1

Switch CTI Link Number: 3

Figure 21: Add/Edit TSAPI Links

4.4. Add CTI User.

A username and password is required for the Altitude system to communicate with the AES. This is setup via the User Management main menu as follows in **Figure 22.** All entries with asterisks must be completed and ensure that the **CT User** field is set to "Yes".



Add User

Fields marked with * can not be empty.

* User Id	altitude
* Common Name	altitude
* Surname	altitude
* User Password	●●●●●●●●
* Confirm Password	●●●●●●●●
Admin Note	
Avaya Role	None
Business Category	
Car License	
CM Home	
Css Home	
CT User	Yes

Figure 22: Add CTI User

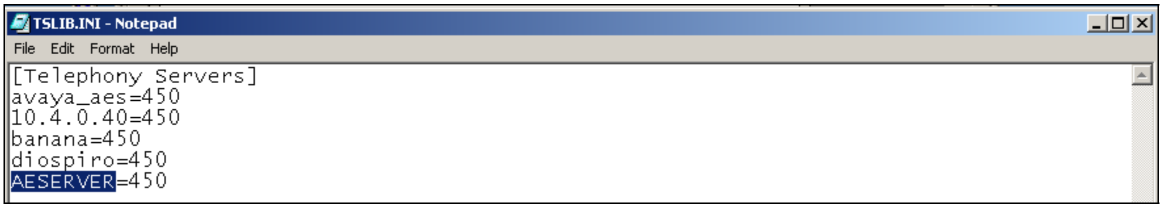
5. Configure the Altitude uCI Suite

This section provides the procedures for configuring Altitude uCI Suite. The procedures fall into the following areas:

- Configure the TSAPI connection to the Avaya AES
- Configure the campaigns
- Configure the agents and assign them to the campaigns
- Install and configure the IVR module

5.1. Configure the TSAPI Connection to the Avaya AES

In the Windows directory (for example, C:\WINNT) of the Altitude Assisted Server, administer the text file “TSLIB.INI” with the host name and the port number of the AES separated by an equal sign (=), as shown highlighted in **Figure 23**. The default port number is 450. The server must be able to resolve the name of the AES server to the relevant IP address either via DNS or the local host file.

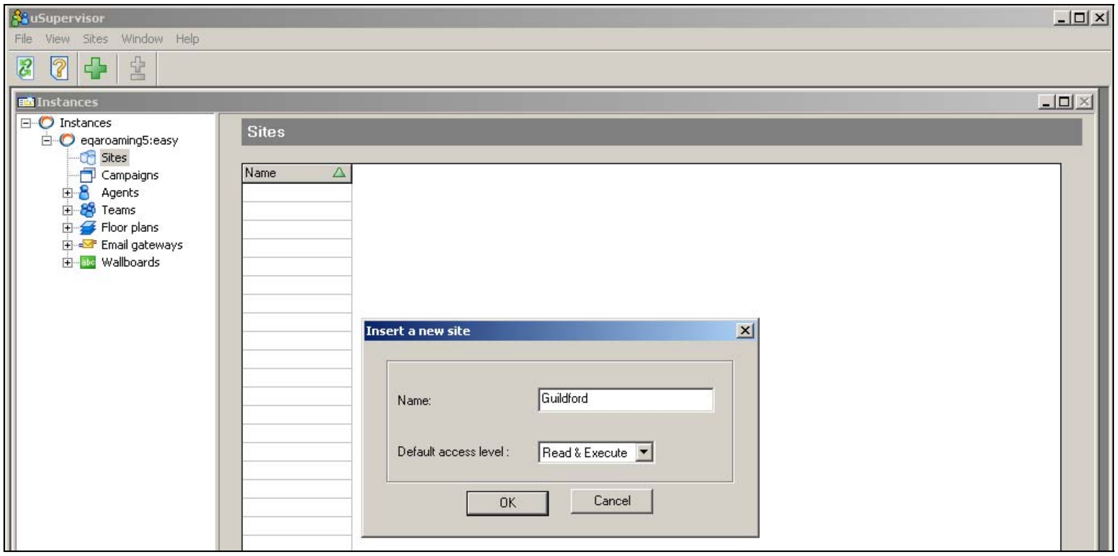


```
[Telephony Servers]
avaya_aes=450
10.4.0.40=450
banana=450
diospiro=450
AESERVER=450
```

Figure 23: Sample TSLIB.INI file

The setup of the Altitude system is done via the uSupervisor application. The first step is to right-click on the hostname in the left pane of uSupervisor and select **Login.**

To create a new site, right-click on **Sites** in the left pane of uSupervisor and select **Insert New**. Give the site a name in the resulting dialog box and click **OK**, as shown in **Figure 24.**

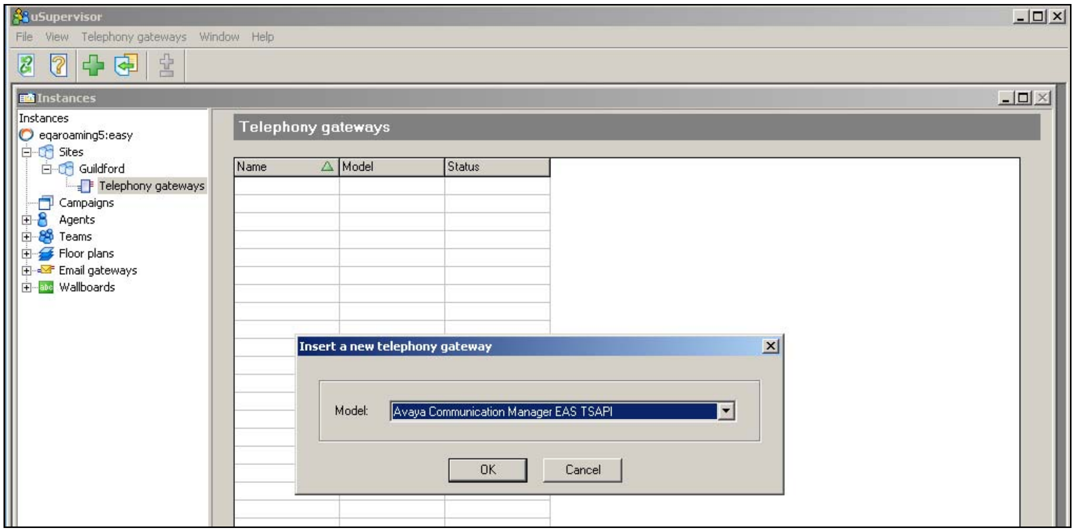


Name: Guildford

Default access level : Read & Execute

Figure 24: Naming the site

To add a telephony gateway to the site go to the left pane and expand **Sites** and expand the site name created in **Figure 24.** Right-click **Telephony Gateway** and select **Insert New.** In the resulting dialog box, choose "Avaya Communication Manager EAS TSAPI" in the **Model** field and click OK, as shown in **Figure 25.**

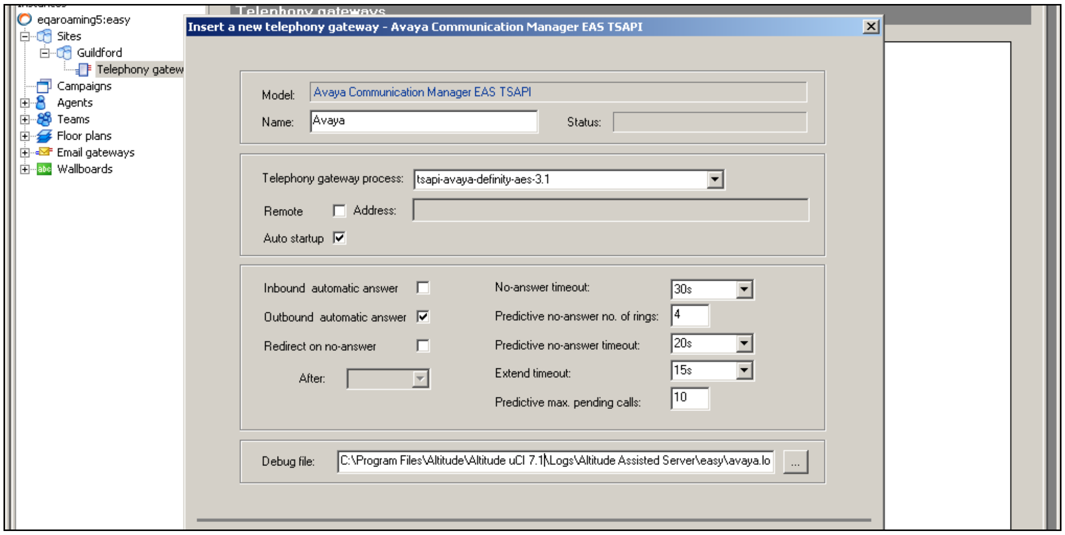


Insert a new telephony gateway

Model: Avaya Communication Manager EAS TSAPI

Figure 25: Choose Telephony Gateway Model

On the next page, give the telephony gateway a name and choose "tsapi-avaya-definity-aes-3.1" in the **Telephony Gateway Process** field, as shown in **Figure 26**. Ensure the **Auto startup** checkbox is ticked and choose a location for the logs in the **Debug file** field, usually this will be "C:\Program Files\Altitude\Altitude uCI 7.1\Logs\Altitude Assisted Server\easy\avaya.log" but can be customised.



Insert a new telephony gateway - Avaya Communication Manager EAS TSAPI

Model: Avaya Communication Manager EAS TSAPI

Name: Avaya

Status:

Telephony gateway process: tsapi-avaya-definity-aes-3.1

Remote □ Address:

Auto startup ☑

Inbound automatic answer □

Outbound automatic answer ☑

Redirect on no-answer □

After:

No-answer timeout: 30s

Predictive no-answer no. of rings: 4

Predictive no-answer timeout: 20s

Extend timeout: 15s

Predictive max. pending calls: 10

Debug file: C:\Program Files\Altitude\Altitude uCI 7.1\Logs\Altitude Assisted Server\easy\avaya.lo

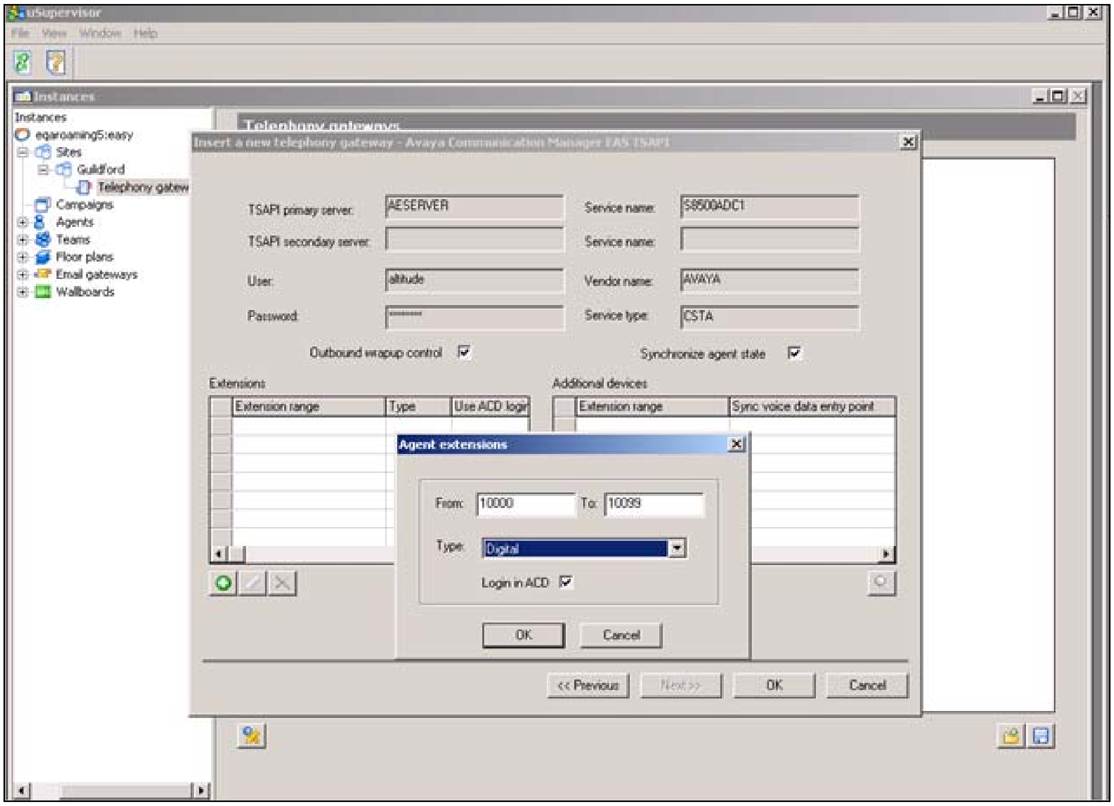
Figure 26: Telephony Gateway – Initial Setup

The next page sets up the CTI link to the AES and adds the extension range for Avaya Communication Manager. Enter the following values as shown in **Figure 27**.

- **TSAPI Primary Server:** This is the hostname of the primary AES server.
- **Service Name:** This is the name of the service to the switch on the AES.
- **User:** This is the user administered on the AES.
- **Password:** This is the password administered on the AES.
- **Vendor Name:** "Avaya"
- **Service Type:** "CSTA"

The checkboxes **Outbound wrapup control** and **Synchronize agent state** should both be ticked.

An extension range is added by clicking on the green "+" button under the **Extensions** box. The **Type** should be "Digital" and **Login in ACD** should be checked. Click OK.



TSAPI primary server: AESERVER
Service name: S8500ADC1
TSAPI secondary server:
Service name:
User: altitude
Vendor name: AVAYA
Password: ********
Service type: CSTA
Outbound wrapup control ☑
Synchronize agent state ☑

Extensions

Extension range	Type	Use ACD login

Additional devices

Extension range	Sync voice data entry point

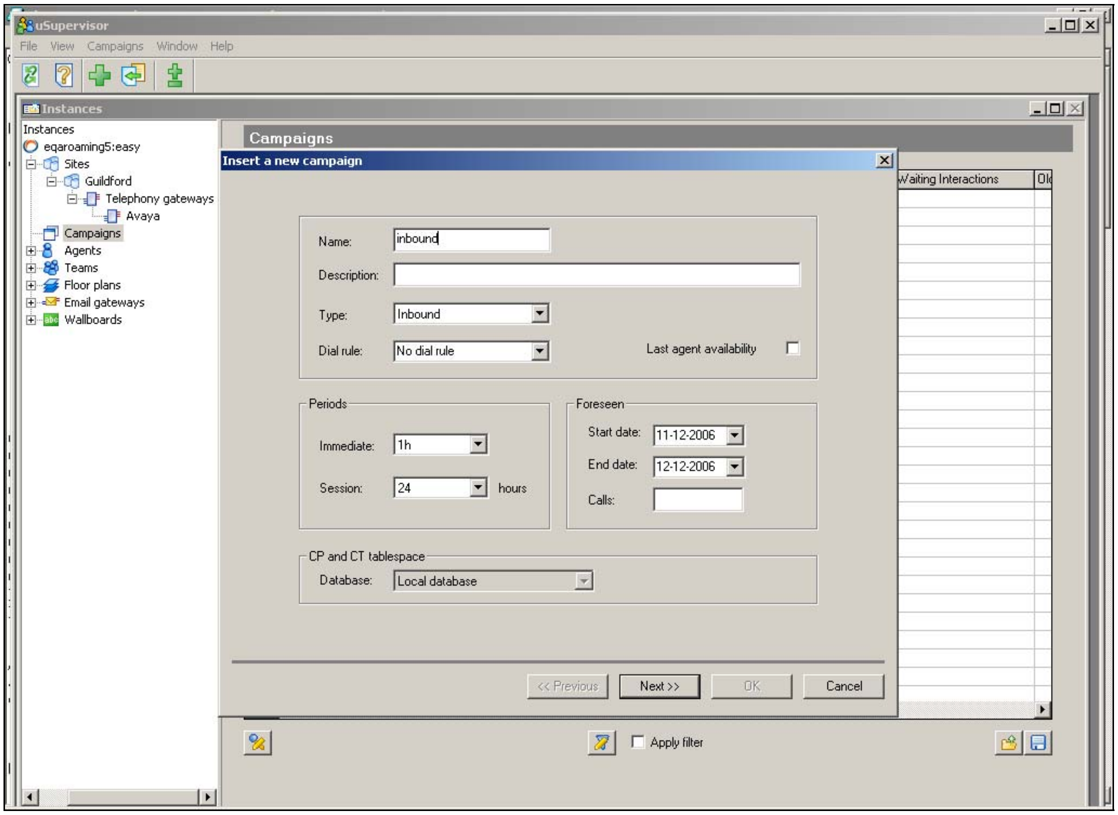
Agent extensions
From: 10000 To: 10099
Type: Digital
Login in ACD ☑
OK Cancel

Figure 27: Telephony Gateway – Switch-Link Setup

5.2. Configure the Campaigns

Altitude uCI supports different campaign configurations. The following section shows the basic steps to configure any campaign. Follow the Altitude uCI Technical Documentation to configure the campaigns according to the configuration required.

To create a campaign right-click on **Campaigns** and select **Insert New**. On the first page, give the campaign a name and set the required campaign type (inbound/outbound/blended) in the **Type** field, as shown in **Figure 28**. Set campaign period according to the call center requirements. Click Next.



Name: inbound

Description:

Type: Inbound

Dial rule: No dial rule

Last agent availability □

Periods

Immediate: 1h

Session: 24 hours

Foreseen

Start date: 11-12-2006

End date: 12-12-2006

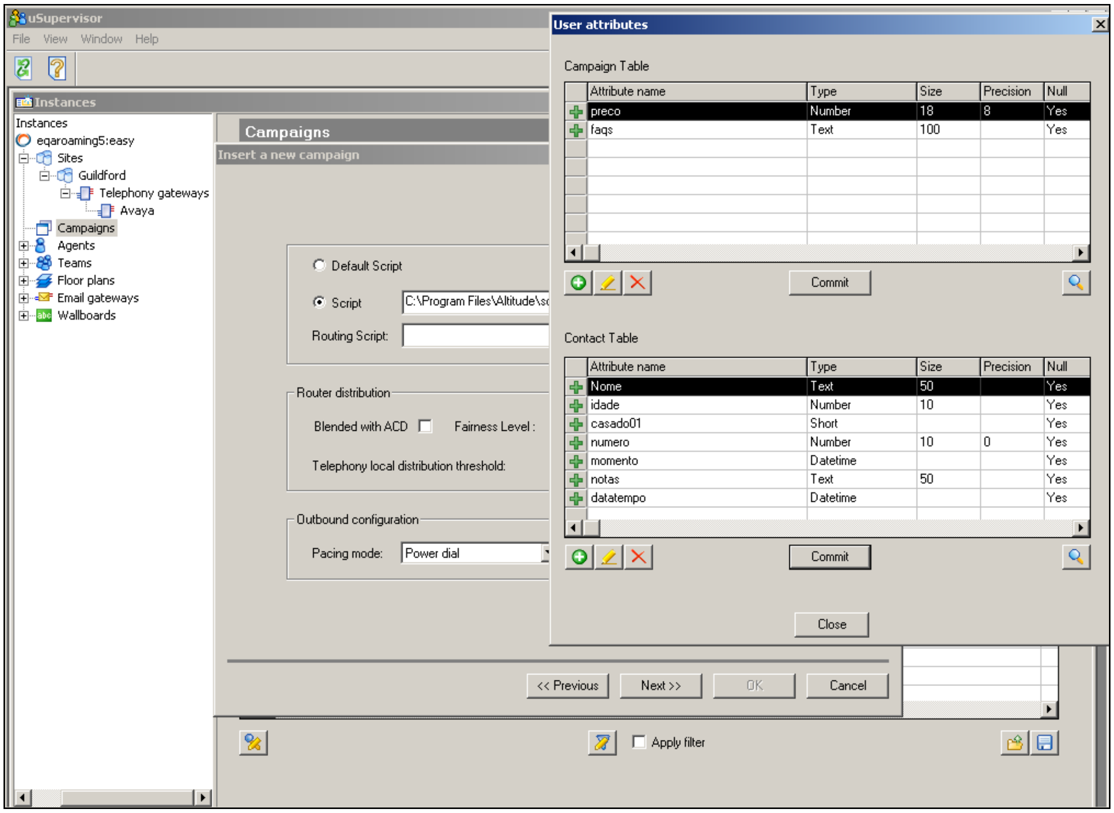
Calls:

CP and CT tablespace

Database: Local database

Figure 28: New Campaign – Initial Setup

On the next page, select a location for the campaign script for agents on call delivery, as shown in **Figure 29**. Once the location has been entered in the **Script** field, click on the tick sign to the right of the script field (not shown in the diagram). In the **User Attributes** window, click on the **Commit** buttons to update the database and click on **Close**. The rest of the page can be left at defaults or used to configure blending and outbound options as required.



○ Default Script

● Script: C:\Program Files\Altitude\sc

Routing Script:

Router distribution

Blended with ACD □ Fairness Level :

Telephony local distribution threshold:

Outbound configuration

Pacing mode: Power dial

Campaign Table

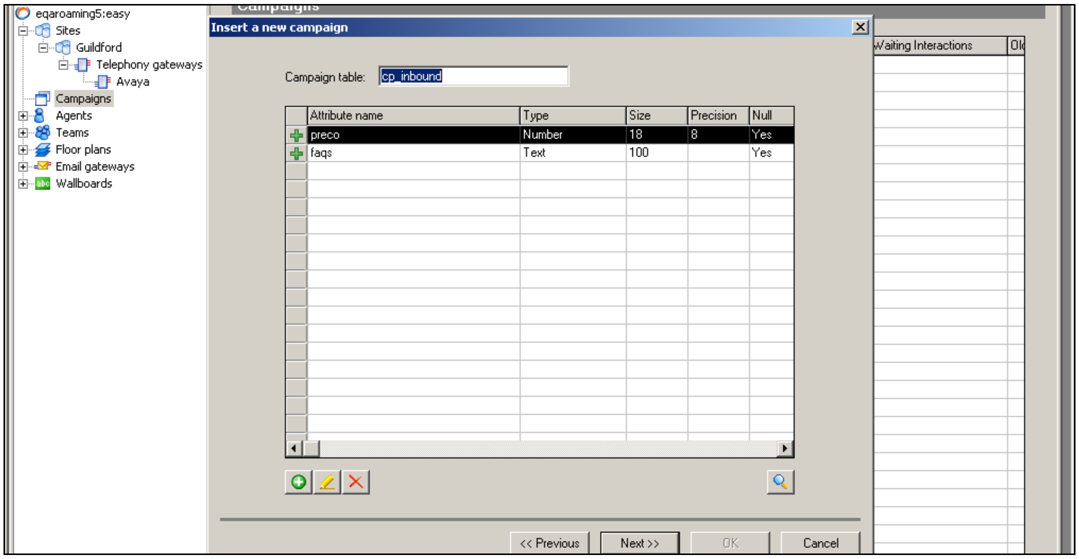
Attribute name	Type	Size	Precision	Null
preco	Number	18	8	Yes
faqs	Text	100		Yes

Contact Table

Attribute name	Type	Size	Precision	Null
Nome	Text	50		Yes
idade	Number	10		Yes
casado01	Short			Yes
numero	Number	10	0	Yes
momento	Datetime			Yes
notas	Text	50		Yes
datatempo	Datetime			Yes

Figure 29: New Campaign – Configure Agent Script

There will then follow a number of screens to allow changes to be made to database attributes. Leave these screens at defaults by clicking the **Next** button. An example is shown in **Figure 30,** below:

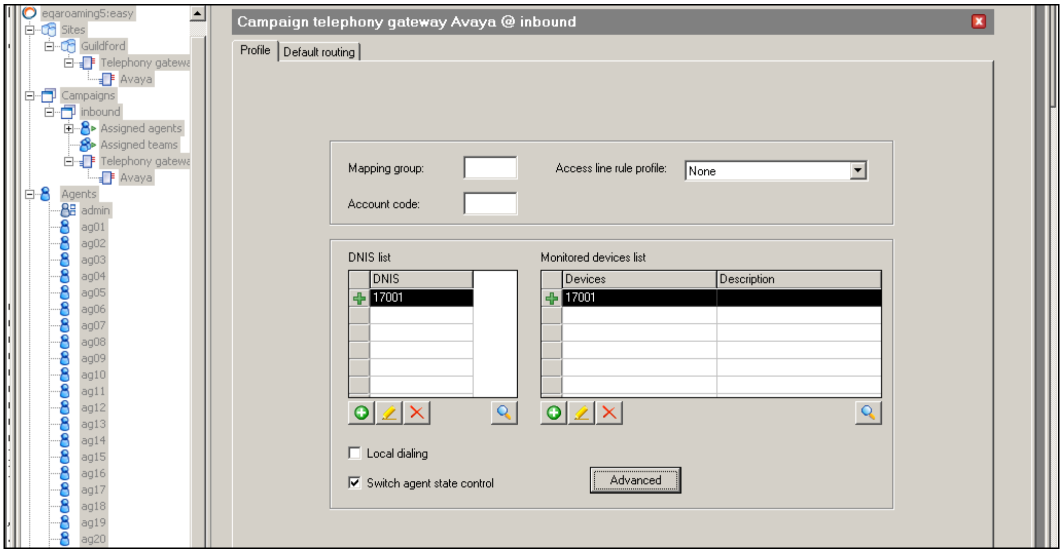


Campaign table: cp_inbound

Attribute name	Type	Size	Precision	Null
preco	Number	18	8	Yes
faqs	Text	100		Yes

Figure 30: Sample Database Configuration Screen

To add the telephony gateway to the campaign, expand **Campaigns** and the required campaign, right-click on **Telephony Gateways** and select **Insert New**. Select the gateway required from the drop-down list and click **OK**. Next, double-click this gateway, go to the **Profile** tab, right-click anywhere in the grey area and select **Update** to allow the fields to be administered. Add the DNIS of the calls to the **DNIS list**, this will be the VDN number for internal calls or the number passed to the PBX for external calls. Add the VDN number to the **Monitored devices list** and click **OK** at the bottom of the screen (not shown in the diagram). See **Figure 31** for an example.



Mapping group:

Account code:

Access line rule profile: None

DNIS list

DNIS
17001

Monitored devices list

Devices	Description
17001	

☐ Local dialing

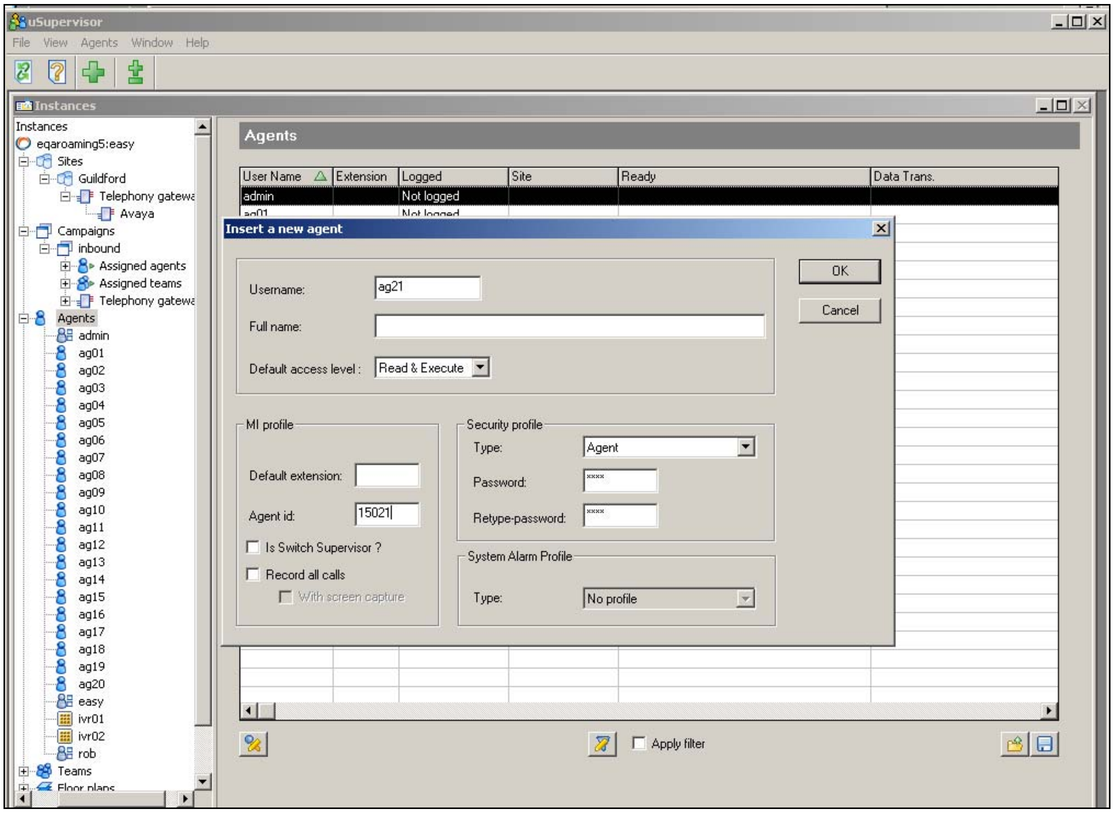
☑ Switch agent state control

Figure 31: Adding DNIS and VDNs to a Campaign

5.3. Configure the Agents and Assign the Agents to Campaigns

These are the basic steps to create agents and assign the agents to a campaign using the Altitude uSupervisor application. If a specific agent configuration is required please refer to the Altitude uCI Technical documentation.

To add an agent, right-click on **Agents** and select **Insert New**. Give the agent an alphanumeric **Username** and **Password**. Enter the Avaya Communication Manager agent ID in the **Agent id** field and the station number in the **Default Extension** field (if using static agents). Set the **Type** field to “Agent” unless setting up an IVR application (set **Type** to “IVR”) or uRouter application (set **Type** to “Routing”). See **Figure 32** for a sample agent configuration. Select **OK** to save the new agent configuration.



Insert a new agent

Username: ag21

Full name:

Default access level : Read & Execute

MI profile

Default extension:

Agent id: 15021

□ Is Switch Supervisor ?

□ Record all calls

□ With screen capture

Security profile

Type: Agent

Password: ****

Retype-password: ****

System Alarm Profile

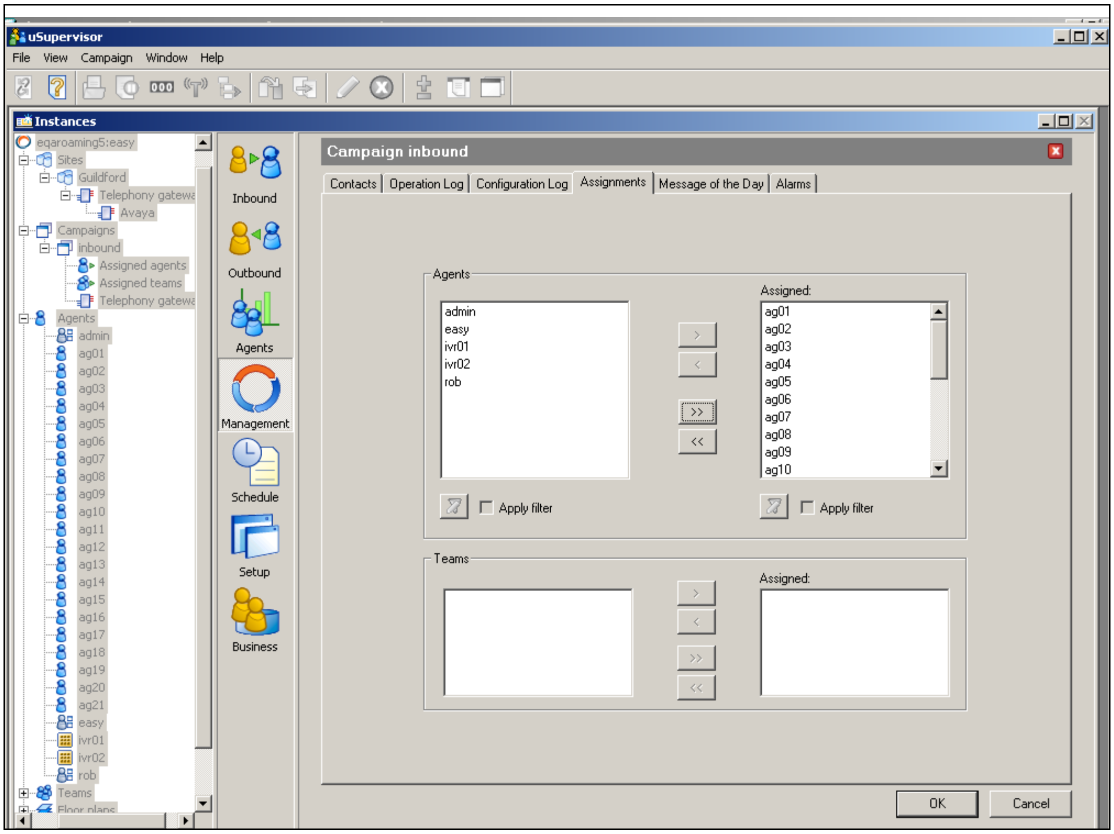
Type: No profile

OK

Cancel

Figure 32: Sample Agent Configuration

To add agents to a campaign; open up the campaign configured in Figure 28 and go to the assignments tab. Right-click anywhere on the grey area and select **Update** and the fields will become available to administer. Select the agents to add to the campaign in the **Agents** box and use the >> button to move them to the **Assigned** box. Click **OK** when finished. This can be seen in **Figure 33.**



Agents: admin, easy, ivr01, ivr02, rob

Assigned: ag01, ag02, ag03, ag04, ag05, ag06, ag07, ag08, ag09, ag10

☐ Apply filter

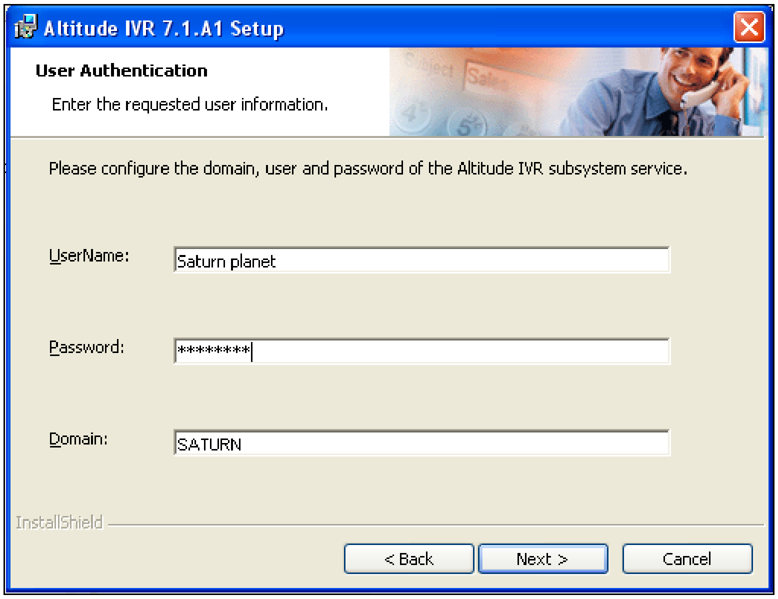
Figure 33: Adding Agents to the Campaign

5.4. Install and Configure the IVR module

The IVR module is installed on a PC or server that has a Dialogic telephony card installed with the default settings.

The installation process for the IVR module asks the user for some information as follows.

On the **User Authentication** screen enter the **Domain**, **UserName** and **Password** of the IVR PC and click **Next** as shown in **Figure 34**.



User Authentication

Enter the requested user information.

Please configure the domain, user and password of the Altitude IVR subsystem service.

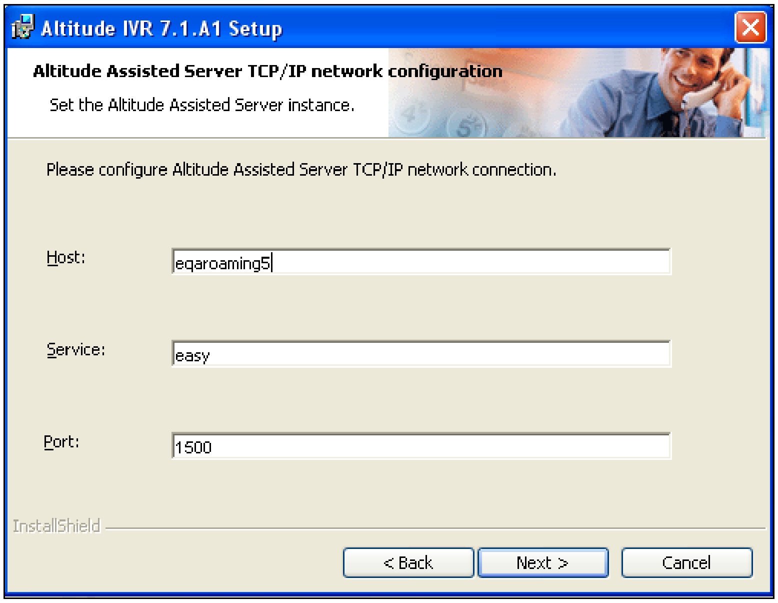
UserName: Saturn planet

Password: *********

Domain: SATURN

Figure 34: User Authentication Screen

On the **Altitude Assisted Server TCP/IP network configuration** screen, enter the hostname of the Altitude core server in the **Host** field. Enter “easy” in the **Service** field and “1500” in the **Port** field and click **Next** as shown in **Figure 35**.



Altitude IVR 7.1.A1 Setup

Altitude Assisted Server TCP/IP network configuration

Set the Altitude Assisted Server instance.

Please configure Altitude Assisted Server TCP/IP network connection.

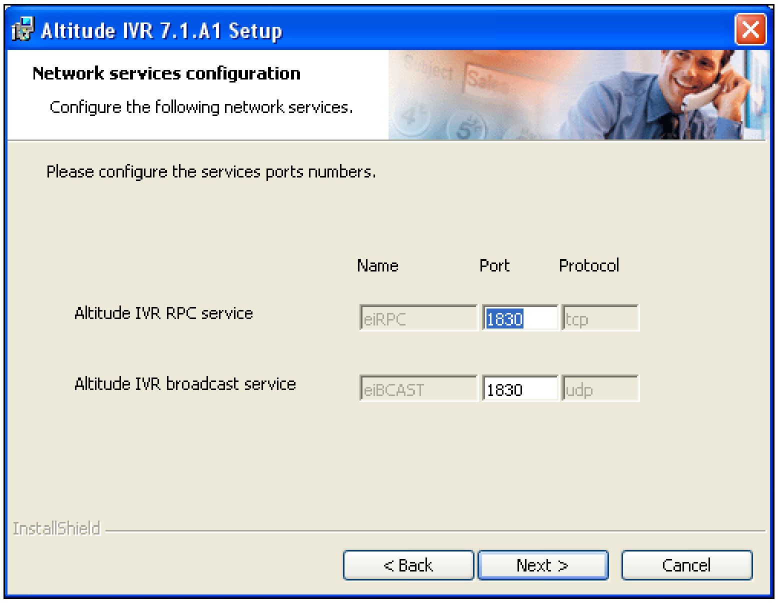
Host: eqaroaming5

Service: easy

Port: 1500

Figure 35: TCP/IP Configuration Screen

On the **Network services configuration** screen accept the default port numbers and click **Next** as shown in **Figure 36**.



Altitude IVR 7.1.A1 Setup

Network services configuration

Configure the following network services.

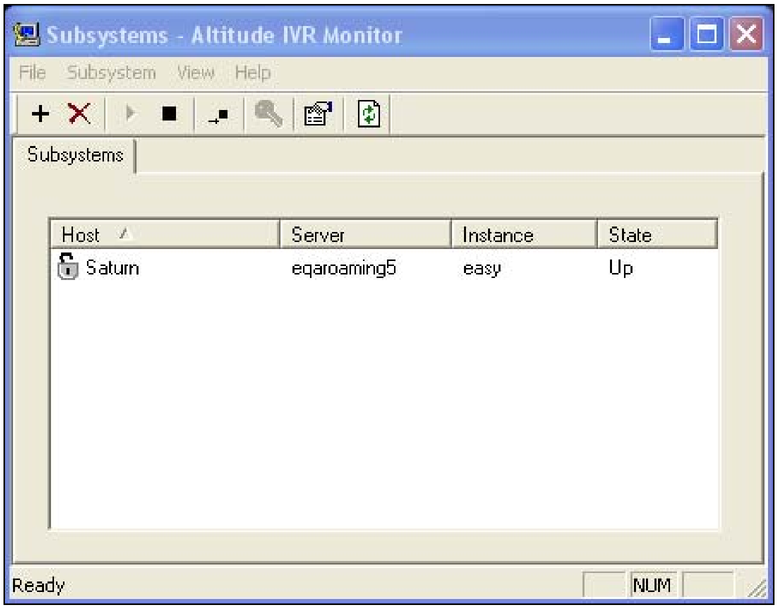
Please configure the services ports numbers.

	Name	Port	Protocol
Altitude IVR RPC service	eiRPC	1830	tcp
Altitude IVR broadcast service	eiBCAST	1830	udp

Figure 36: Network Services Configuration

The installation will now finish and the next step is to configure the subsystem.

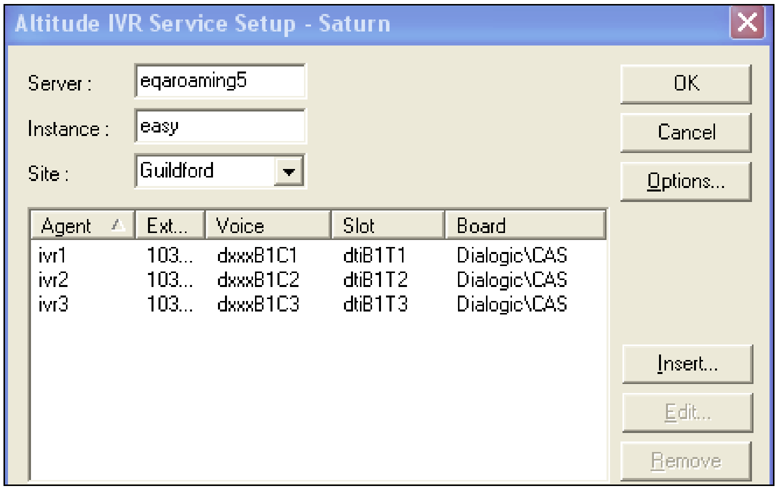
Open the **Altitude IVR Monitor** application. The subsystem was created during the installation and is shown in the **Subsystems** tab, see **Figure 37**.



Host	Server	Instance	State
Saturn	eqaroaming5	easy	Up

Figure 37: Altitude IVR Monitor

Right-click on the subsystem and select **Properties**, this will bring up the **Altitude IVR Service Setup** screen. On this screen, enter the site name configured in **Figure 24** in the **Site** field and use the **Insert** button to configure each IVR agent with a physical DS-1 port, see **Figure 38.**



Server : eqaroaming5

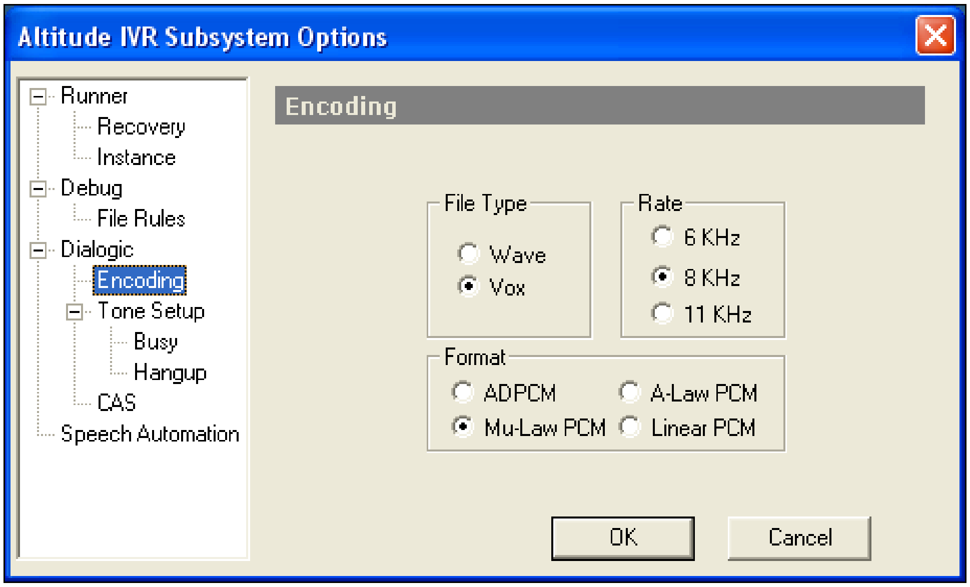
Instance : easy

Site : Guildford

Agent	Ext...	Voice	Slot	Board
ivr1	103...	dxxxB1C1	dtiB1T1	Dialogic\CAS
ivr2	103...	dxxxB1C2	dtiB1T2	Dialogic\CAS
ivr3	103...	dxxxB1C3	dtiB1T3	Dialogic\CAS

Figure 38: Altitude IVR Service Setup

Click on **Options** to bring up the **Altitude IVR Subsystem Options** window and ensure that the **Encoding** and **CAS** screens are configured as shown in **Figures 39** and **40**. Click **OK**.



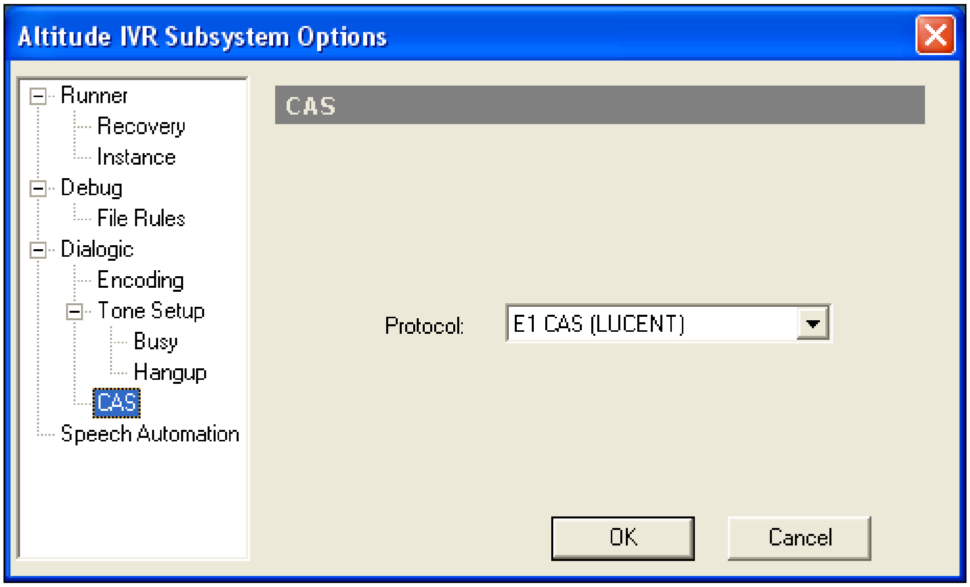
Encoding

File Type
○ Wave
● Vox

Rate
○ 6 KHz
● 8 KHz
○ 11 KHz

Format
○ ADPCM ○ A-Law PCM
● Mu-Law PCM ○ Linear PCM

Figure 39: Altitude IVR Subsystem Options – Encoding Screen



CAS

Protocol: E1 CAS (LUCENT)

Figure 40: Altitude IVR Subsystem Options – CAS Screen

6. Interoperability Compliance Testing

The Interoperability compliance test included both feature functionality and serviceability testing.

The feature functionality testing focused on verifying the Altitude uCI Suite's handling of TSAPI messages to request and respond to the Avaya Communication Manager feature set.

The serviceability testing focused on verifying Altitude uCI Suite's ability to recover from an outage condition, such as busying out the CTI link and disconnecting the Ethernet cable for the CTI link.

6.1. General Test Approach

All feature functionality and serviceability test cases were performed manually. The verification included checking of proper states at the telephone sets, and of capturing TSAPI message traces.

6.2. Test Results

All feature interaction test cases passed successfully. These tests included:

- Initiate, receive, hold, transfer, conference of internal and external calls.
- Handling of the different outbound pacing modes.
- Using the Altitude IVR module in both inbound and outbound campaigns.

All serviceability test cases were completed, with 2 observations.

The first observation is that the uAgent application is unable to recommence monitoring of the extension at recovery if a call remains active during a network outage. The agent must be manually logged out of the phone and the uAgent application must log in again.

The second observation is that, by default, the uAgent application takes 4-5 minutes to recover after a network outage at the client machine. The workaround is to lower the **RAS_RecoverTriesInterval** in the system registry for the uAgent application.

7. Verification Steps

This section provides the tests that can be performed to verify proper configuration of Avaya Communication Manager, Avaya Application Enablement Services, and Altitude uCI Suite.

7.1. Verify Avaya Communication Manager

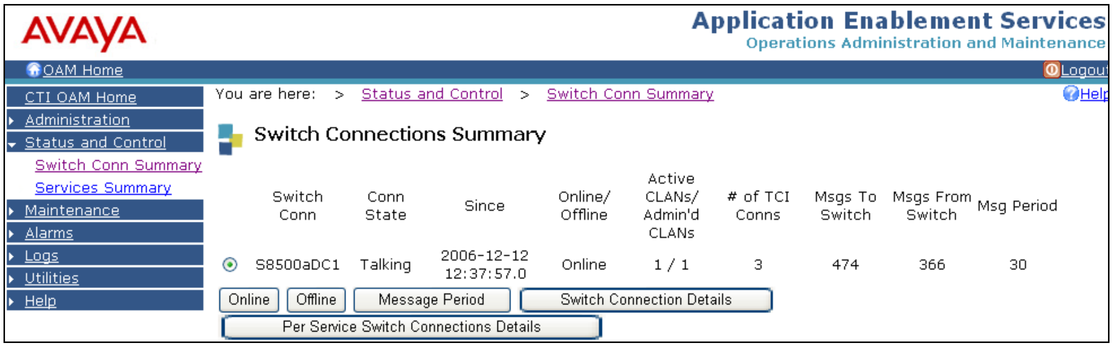
Verify the status of the administered CTI link by using the “status aesvcs cti-link” command as shown in **Figure 41**.

```
status aesvcs cti-link

                           AE SERVICES CTI LINK STATUS

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

1      4         no     AEServer         established   15        15
2                no                      down          0         0
3      4         no     AEServer         established   216       210
```

Figure 41: Status Aesvcs CTI-link

7.2. Verify Avaya Application Enablement Services

From the AES OAM Admin menu, verify the status of the administered CTI link by selecting **Status and Control > Switch Conn Summary**, as shown in **Figure 42**.



You are here: > Status and Control > Switch Conn Summary

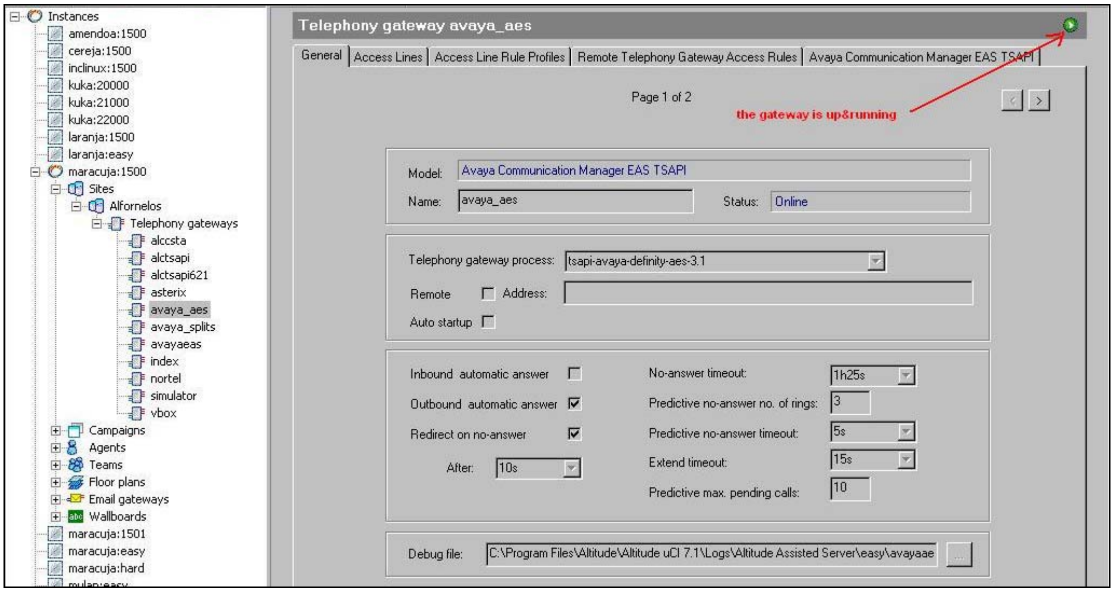
Switch Connections Summary

	Switch Conn	Conn State	Since	Online/ Offline	Active CLANs/ Admin'd CLANs	# of TCI Conns	Msgs To Switch	Msgs From Switch	Msg Period
●	S8500aDC1	Talking	2006-12-12 12:37:57.0	Online	1 / 1	3	474	366	30

Figure 42: Switch Connections Summary

7.3. Verify Altitude Assisted Server

To verify the CTI connection from the uSupervisor application expand **Sites > Alfornelos** (site name) **> Telephony Gateways** and open up the gateway you wish to check. In the top right hand corner there is an icon showing the gateway status. This icon is green when the gateway is up and running, see **Figure 43** (the screenshot was taken from a different server to the one used in the testing).



Telephony gateway avaya_aes

Model: Avaya Communication Manager EAS TSAPI

Name: avaya_aes

Status: Online

Telephony gateway process: tsapi-avaya-definity-aes-3.1

Remote ☐ Address:

Auto startup ☐

Inbound automatic answer ☐

Outbound automatic answer ☑

Redirect on no-answer ☑

After: 10s

No-answer timeout: 1h25s

Predictive no-answer no. of rings: 3

Predictive no-answer timeout: 5s

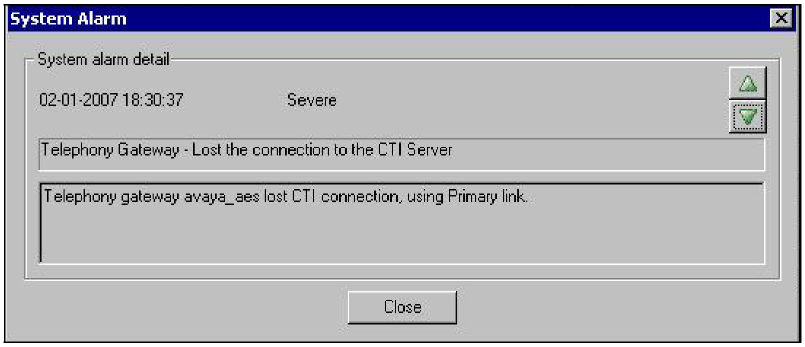
Extend timeout: 15s

Predictive max. pending calls: 10

Debug file: C:\Program Files\Altitude\Altitude uCI 7.1\Logs\Altitude Assisted Server\easy\avayaae

Figure 43: Telephony Gateway Status

If the CTI link drops, then the uSupervisor will get an alarm, which will pop-up on screen, as shown in **Figure 44**.



System Alarm

System alarm detail

02-01-2007 18:30:37 Severe

Telephony Gateway - Lost the connection to the CTI Server

Telephony gateway avaya_aes lost CTI connection, using Primary link.

Figure 44: uSupervisor Alarm Pop-up

8. Support

The Altitude Meeting Point web page is the primary interface of Altitude Software with its customers, who can submit, check and or update tickets through a web interface. For more information, use the email and telephone numbers on the Altitude Meeting Point website at:

http://meetingpoint.altitude.com

9. Conclusion

These Application Notes describe the configuration steps required for the successful interoperability of Altitude uCI with Avaya Communication Manager. All application functionality and serviceability test cases were completed. Two minor observations were made in the failure and recovery testing, see section 6.2 for details.

10. Additional References

This section references the product documentations that are relevant to these Application Notes.

- *Avaya Application Enablement Services 3.1.2 Administration and Maintenance Guide*, Document ID 02-300357, Issue 4, September 2006, available at: http://support.avaya.com

- *Documentation for Avaya Communication Manager(3.1.2), Media Gateways and Servers*, Document ID 03-300151, Issue 5, February 2006, available at: http://support.avaya.com

- *System Administration, Administrator Series*, November 2006, available at: http://meetingpoint.altitude.com

- *How to Create Altitude uCI Campaign on the Avaya, Architect Series*, November 2006, available at: http://meetingpoint.altitude.com

10.1. Glossary

Technical Term	Definition as it pertains to this document.
AES	Application Enablement Services
ASAI	Adjunct Switch Application Interface
CAS	Channel Associated Signaling
CSTA	Computer Supported Telecommunications Applications
CTI	Computer Telephony Integration
ISDN	Integrated Services Digital Network
IVR	Interactive Voice Response
PBX	Private Branch Exchnage
PSTN	Public Switched Telephone Network
TSAPI	Telephony Server Application Program Interface
VDN	Vector Directory Number

The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya Developer*Connection* Program at devconnect@avaya.com.