



Avaya Solution & Interoperability Test Lab

Application Notes for configuring Presence Technology Presence Suite R11.0 to interoperate with Avaya Aura® Communication Manager R7.1 and Avaya Aura® Application Enablement Services R7.1 – Issue 1.0

Abstract

These Application Notes describe the configuration steps for Presence Technology Presence Suite to successfully interoperate with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services. Presence Suite is a multi-channel contact management suite which handles voice, text chat, email and web contact mechanisms. Presence Suite integrates with the Avaya solution by using the Telephony Services Application Programmer Interface (TSAPI) provided by Avaya Aura® Application Enablement Services to monitor and control agent stations, and handle routing of external calls.

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 describe the compliance tested configuration using Presence Suite R11.0 and Avaya Aura® Communication Manager R7.1 with Avaya Aura® Application Enablement Services R7.1. Presence Suite is a multi-channel contact management suite able to handle voice, e-mail and web chat contact mechanisms. The Telephony Services Application Programmer Interface (TSAPI) provided by Avaya Aura® Application Enablement Services is used to monitor and control agent stations, generate phantom calls for non-voice contacts and handle routing of external calls. Presence Suite consists of a number of modules. Only the following modules were tested:

- Presence Voice Outbound
- Presence Voice Inbound
- Presence Mail Interactions
- Presence Web Interactions

Upon starting the Presence Server application, the application automatically queries Avaya Aura® Application Enablement Services for device status and requests monitoring. The Presence Server specifies where to route each call and hence how to handle the calls, based on agent status information that the application tracks from CTI device query results and event reports received from Avaya Aura® Application Enablement Services.

2. General Test Approach and Test Results

Testing included validating the correct operation of typical contact centre functions including, inbound and outbound service calls. Functionality testing included basic telephony operations such as answer, hold/retrieve, transfer, and conference. This was carried out for the inbound and outbound service calls. Email, web call back and web chat were also tested. Additional features such as call capturing, direct agent transfer and malicious calls were tested. The serviceability test cases were performed manually by busying out and releasing the CTI link and by disconnecting and reconnecting LAN cables.

DevConnect Compliance Testing is conducted jointly by Avaya and DevConnect members. The jointly-defined test plan focuses on exercising APIs and/or standards-based interfaces pertinent to the interoperability of the tested products and their functionalities. DevConnect Compliance Testing is not intended to substitute full product performance or feature testing performed by DevConnect members, nor is it to be construed as an endorsement by Avaya of the suitability or completeness of a DevConnect member's solution.

Avaya recommends our customers implement Avaya solutions using appropriate security and encryption capabilities enabled by our products. The testing referenced in 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 Presence Suite did not include use of any specific encryption features as requested by Presence Technology.

2.1 Interoperability Compliance Testing

The interoperability compliance test included both feature functionality and serviceability testing. The feature functionality testing focused on verifying Presence Suite handling of TSAPI messages in the areas of routing, call control and event notification. The serviceability testing focused on verifying the Presence Suite ability to recover from adverse conditions, such as stopping the TSAPI Service, taking the CTI link offline and disconnecting the Ethernet cable from all the devices in the solution.

The following modules were tested.

- Presence Voice Outbound
- Presence Voice Inbound
- Presence Mail Interactions
- Presence Web Interactions

Calls were placed to a VDN to test inbound calls, outbound calls were initiated by the Presence Suite, both email and web chat were tested using phantom calls to route calls to the agent.

2.2 Test Results

All test cases passed successfully.

2.3 Support

Technical support can be obtained for Presence Technology Presence Suite as follows:

- Email: support@presenceco.com
- Website: www.presenceco.com
- Phone: +34 93 10 10 300

3. Reference Configuration

Figure 1 shows the network topology during interoperability testing. A Communication Manager with an Avaya G430 Media Gateway was used as the hosting PBX. Presence Suite, including Presence Agent PC's, are connected to the LAN and controls the Avaya H323 and SIP IP telephones via Application Enablement Services using TSAPI.

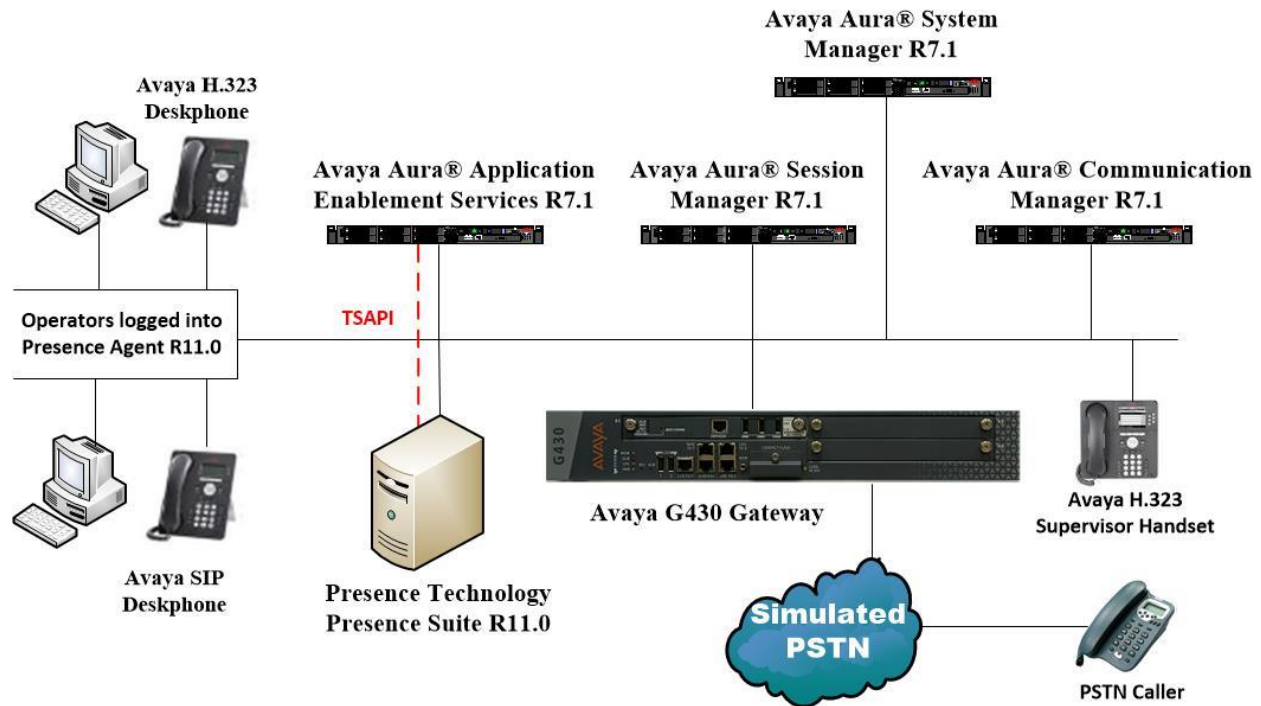


Figure 1: Avaya Aura® Communication Manager R7.1 and Aura® Application Enablement Services R7.1 with Presence Technology Presence Suite Server R11.0 configuration

4. Equipment and Software Validated

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

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	R7.1
Avaya Aura® Media Server running on Virtual Server	R7.8
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
Presence Technology Presence Suite running on Windows Server 2016	R11.0
Presence Technology Presence Client running on Windows 7 SP1	R11.0

5. Configure Avaya Aura® Communication Manager

The information provided in this section describes the configuration of Communication Manager for this solution. For all other provisioning information such as initial installation and configuration, please refer to the product documentation in **Section 10**. The configuration and verification operations illustrated in this section were all performed using Communication Manager System Administration Terminal (SAT). The configuration operations described in this section can be summarized as follows:

- Verify System Features
- Administer SIT Treatment for Call Classification
- Administer Hunt Groups, Vectors and VDN's
- Administer Class of Restriction
- Administer Agent Logins
- Administer Agent Stations
- Administer Phantom Stations
- Note procr IP Address for AES Connectivity
- Configure Transport link for AES Connectivity
- Configure CTI Link for TSAPI Service

5.1 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 3**, ensure that **Computer Telephony Adjunct Links?** is set to **y** and **Answer Supervision by Call Classifier?** is set to **y** as shown below.

display system-parameters customer-options		Page	3 of 11
OPTIONAL FEATURES			
Abbreviated Dialing Enhanced List? y	Audible Message Waiting? y		
Access Security Gateway (ASG)? n	Authorization Codes? y		
Analog Trunk Incoming Call ID? y	CAS Branch? n		
A/D Grp/Sys List Dialing Start at 01? y	CAS Main? n		
Answer Supervision by Call Classifier? y	Change COR by FAC? n		
ARS? y	Computer Telephony Adjunct Links? y		
ARS/AAR Partitioning? y	Cvg Of Calls Redirected Off-net? y		
ARS/AAR Dialing without FAC? y	DCS (Basic)? y		
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			

On **Page 6**, 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 6 of 11
CALL CENTER OPTIONAL FEATURES

Call Center Release: 7.0

ACD? y
BCMS (Basic)? y
BCMS/VuStats Service Level? y
BSR Local Treatment for IP & ISDN? y
Business Advocate? n
Call Work Codes? y
DTMF Feedback Signals For VRU? y
Dynamic Advocate? n
Expert Agent Selection (EAS)? y
EAS-PHD? y
Forced ACD Calls? n
Least Occupied Agent? y
Lookahead Interflow (LAI)? y
Multiple Call Handling (On Request)? y
Multiple Call Handling (Forced)? y
PASTE (Display PBX Data on Phone)? y

Reason Codes? y
Service Level Maximizer? n
Service Observing (Basic)? y
Service Observing (Remote/By FAC)? y
Service Observing (VDNs)? y
Timed ACW? y
Vectoring (Basic)? y
Vectoring (Prompting)? y
Vectoring (G3V4 Enhanced)? y
Vectoring (3.0 Enhanced)? y
Vectoring (ANI/II-Digits Routing)? y
Vectoring (G3V4 Advanced Routing)? y
Vectoring (CINFO)? y
Vectoring (Best Service Routing)? y
Vectoring (Holidays)? y
Vectoring (Variables)? y

```

Use the command **display system-parameters features** and on **Page 1**, verify that the **Trunk-to-Trunk Transfer** option is set to **all** as shown below.

```

display system-parameters features                                     Page 1 of 20
FEATURE-RELATED SYSTEM PARAMETERS
Self Station Display Enabled? n
Trunk-to-Trunk Transfer: all
Automatic Callback with Called Party Queuing? n
Automatic Callback - No Answer Timeout Interval (rings): 3
Call Park Timeout Interval (minutes): 10
Off-Premises Tone Detect Timeout Interval (seconds): 20
AAR/ARS Dial Tone Required? y

Music (or Silence) on Transferred Trunk Calls? no
DID/Tie/ISDN/SIP Intercept Treatment: attendant
Internal Auto-Answer of Attd-Extended/Transferred Calls: transferred
Automatic Circuit Assurance (ACA) Enabled? n

```

On **page 10** ensure that **Station Tone Forward Disconnect** is set to **silence** as shown below.

```
display system-parameters features                                     Page 10 of 20
                                FEATURE-RELATED SYSTEM PARAMETERS

                                Pull Transfer: n                      Update Transferred Ring Pattern? n
                                Outpulse Without Tone? y              Wait Answer Supervision Timer? n
                                Misoperation Alerting? n              Repetitive Call Waiting Tone? n
                                Allow Conference via Flash? y
                                Vector Disconnect Timer (min):        Network Feedback During Tone Detection? y
                                Hear Zip Tone Following VOA? y        System Updates Time On Station Displays? n

                                Station Tone Forward Disconnect: silence
                                Level Of Tone Detection: precise
                                Charge Display Update Frequency (seconds): 30

                                Onhook Dialing on Terminals? n
                                Edit Dialing on 96xx H.323 Terminals? n
                                Allow Crisis Alert Across Tenants? n
                                Send DTMF Over Telecommuter Link? y

ITALIAN DCS PROTOCOL
Italian Protocol Enabled? n
```

Use the command **display system-parameters features** and on **Page 11**, verify that the **Expert Agent Selection (EAS) Enabled?** option is set to **y** as shown below.

```
display system-parameters features                                     Page 11 of 19
                                FEATURE-RELATED SYSTEM PARAMETERS
CALL CENTER SYSTEM PARAMETERS
EAS
    Expert Agent Selection (EAS) Enabled? y
    Minimum Agent-LoginID Password Length:
    Direct Agent Announcement Extension:                               Delay:
    Message Waiting Lamp Indicates Status For: station
```


On page 12 ensure that **ACW Agents Considered Idle** is set to **y**.

```
display system-parameters features                                     Page 12 of 20
      FEATURE-RELATED SYSTEM PARAMETERS

AGENT AND CALL SELECTION
      MIA Across Splits or Skills? n
      ACW Agents Considered Idle? y
      Call Selection Measurement: current-wait-time
Service Level Supervisor Call Selection Override? n
      Auto Reserve Agents: none
      Block Hang-up by Logged-in Auto-Answer Agents? n

CALL MANAGEMENT SYSTEM
REPORTING ADJUNCT RELEASE (determines protocol used by appl link)
      CMS (appl mis):
      AAPC/IQ (appl ccr):

      BCMS/VuStats LoginIDs? y
      BCMS/VuStats Measurement Interval: hour
BCMS/VuStats Abandon Call Timer (seconds):
      Validate BCMS/VuStats Login IDs? n
      Clear VuStats Shift Data: on-login
      Remove Inactive BCMS/VuStats Agents? n
```

On Page 13, verify that **Call Classification After Answer Supervision** option is set to **y** as shown below.

```
display system-parameters features                                     Page 13 of 19
      FEATURE-RELATED SYSTEM PARAMETERS

CALL CENTER MISCELLANEOUS
      Callr-info Display Timer (sec): 10
      Clear Callr-info: next-call
      Allow Ringer-off with Auto-Answer? n

Reporting for PC Non-Predictive Calls? n

      Interruptible Aux Notification Timer (sec): 3

ASAI
      Copy ASAI UUI During Conference/Transfer? y
      Call Classification After Answer Supervision? y
      Send UCID to ASAI? y
      For ASAI Send DTMF Tone to Call Originator? y
```

5.2 Administer Special Information Tones Treatment for Call Classification

This form is used to specify the treatment of Special Information Tones (SIT) used for outbound call management type calls with USA tone characteristics. Enter the **change sit-treatment** command. Set the **Pause Duration** to **0.8** and **Talk Duration** to **3.0**. Please note this may vary depending on the country where the PBX is installed.

change sit-treatment	Page 1 of 1
SIT TREATMENT FOR CALL CLASSIFICATION	
SIT Ineffective Other: dropped	
SIT Intercept: dropped	
SIT No Circuit: dropped	
SIT Reorder: dropped	
SIT Vacant Code: dropped	
SIT Unknown: dropped	
AMD Treatment: dropped	
Pause Duration (seconds): 0.8	
Talk Duration (seconds): 3.0	

5.3 Administer Hunt Groups, Call Vectors and Vector Directory Numbers

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

5.3.1 Hunt Groups

Enter the **add hunt-group n** command where **n** in the example below is **98**. 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 98	Page 1 of 4
HUNT GROUP	
Group Number: 98	ACD? y
Group Name: PresenceInbound	Queue? y
Group Extension: 4808	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 98		Page 2 of 4
HUNT GROUP		
Skill? y	Expected Call Handling Time (sec): 180	
AAS? n		
Measured: none		
Supervisor Extension:		
Controlling Adjunct: none		
Multiple Call Handling: none		
Timed ACW Interval (sec):	After Xfer or Held Call Drops? n	

Repeat the above steps to create a hunt groups for the outbound service, web chat and Email.

5.3.2 Vectors

Enter the **change vector n** command, where **n** is the vector number. The adjunct routing link enables Presenceco Presence Server to specify the destination of a call. The **adjunct routing link** number is defined by the position of the AESVCS link on page three of the ip-services (not shown), in this case Server ID **1**.

The call is then queued to the skill set out on the VDN in the 1st Skill field on the next page.

change vector 44		Page 1 of 6
CALL VECTOR		
Number: 44 Name: DevConnect Vector		
Multimedia? y	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	2 secs hearing ringback	
03 queue-to	skill 1st pri m	
04 wait-time	10 secs hearing music	
05 goto step	3 if unconditionally	
06 stop		
07		
08		
09		
10		
11		
12		

5.3.3 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 4908	Page 1 of 3
VECTOR DIRECTORY NUMBER	
Extension: 4908	
Name* : PresenceInbound	
Destination:	Vector Number 44
Attendant Vectoring? n	
Meet-me Conferencing? n	
Allow VDN Override? n	
COR: 1	
TN*: 1	
Measured: none	Report Adjunct Calls as ACD*? n
VDN of Origin Annc. Extension*:	
1st Skill*: 98	
2nd Skill*:	
3rd Skill*:	
* Follows VDN Override Rules	

5.4 Administer Class of Restriction

Enter the **change cor x** command where **x** corresponds to the Class of Restriction to be used for the agent login IDs in **Section 5.5**. 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

5.5 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 5.4**. 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**. Configure a password as required.

add agent-loginID 4405		Page 1 of 2
AGENT LOGINID		
Login ID: 4405	AAS? n	
Name: PresenceAgent1	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 5.3.1** 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 **98**.

change agent-loginID 4405		Page 2 of 2
AGENT LOGINID		
Direct Agent Skill: 98		Service Objective? n
Call Handling Preference: skill-level		Local Call Preference? n
SN	RL	SL
1: 98	1	16:
2: 96	1	17:
3: 97	1	18:
4:		19:
5:		20:
6:		
7:		

Repeat this task accordingly for any additional inbound or outbound agents required.

5.6 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** ensure that **IP SoftPhone** is set to **y** as shown below.

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: 2	COR: 1
Name: 4000, H323User	Coverage Path 2:	COS: 1
	Hunt-to Station:	Tests? n
STATION OPTIONS		
Loss Group: 19	Time of Day Lock Table:	
	Personalized Ringing Pattern: 1	
Speakerphone: 2-way	Message Lamp Ext: 4000	
Display Language: english	Mute Button Enabled? y	
Survivable GK Node Name:	Button Modules: 0	
Survivable COR: internal	Media Complex Ext:	
Survivable Trunk Dest? y	IP SoftPhone? y	
	IP Video Softphone? n	
	Short/Prefixed Registration Allowed: default	
	Customizable Labels? y	

On **Page 4**, 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:	List2:	List3:
BUTTON ASSIGNMENTS		
1: call-appr	5: manual-in	Grp:
2: call-appr	6: after-call	Grp:
3: call-appr	7: release	
4: aux-work	8: :	
RC:	Grp:	

5.7 Administer Phantom Stations

Presence Suite uses stations via AES to initiate calls on Communication Manager. These stations will be used to place calls to customers for outbound services as well as to place calls to agents in order to reserve an agent to handle the outbound call. Use the command **add station n**, enter a descriptive name for **Name**, the **Type** should be set to **6408D+** and enter **X** for the **Port**.

```
add station 4850                                     Page 1 of 5
                                                    STATION
Extension: 4850                                     Lock Messages? n      BCC: 0
Type: 6408D+                                       Security Code:         TN: 1
Port: X                                           Coverage Path 1:      COR: 1
Name: PresencePhantom                           Coverage Path 2:      COS: 1
                                                    Hunt-to Station:
STATION OPTIONS
                                                    Time of Day Lock Table:
Loss Group: 2                                     Personalized Ringing Pattern: 1
Data Module? n                                   Message Lamp Ext: 4850
Speakerphone: 2-way                             Mute Button Enabled? y
Display Language: english
Survivable COR: internal                         Media Complex Ext:
Survivable Trunk Dest? y                        IP SoftPhone? n
                                                    Remote Office Phone? n
                                                    IP Video? n
```

5.8 Note procr IP Address for Avaya Aura® Application Enablement Services Connectivity

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

```
display node-names ip
                                                    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
procr6    ::
```

5.9 Configure Transport Link for Avaya Aura® Application Enablement Services Connectivity

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 5.8**.
- **Local Port** Retain the default value of **8765**.

change ip-services					Page	1 of 4
IP SERVICES						
Service Type	Enabled	Local Node	Local Port	Remote Node	Remote 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 6.2**. 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 Server	Password	Enabled	Status	
1:	AES71vmpg	*****	y	idle	
2:					
3:					

5.10 Configure CTI Link for TSAPI Service

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: 4499			
Type: ADJ-IP			
		COR: 1	
Name: AES71vmpg			

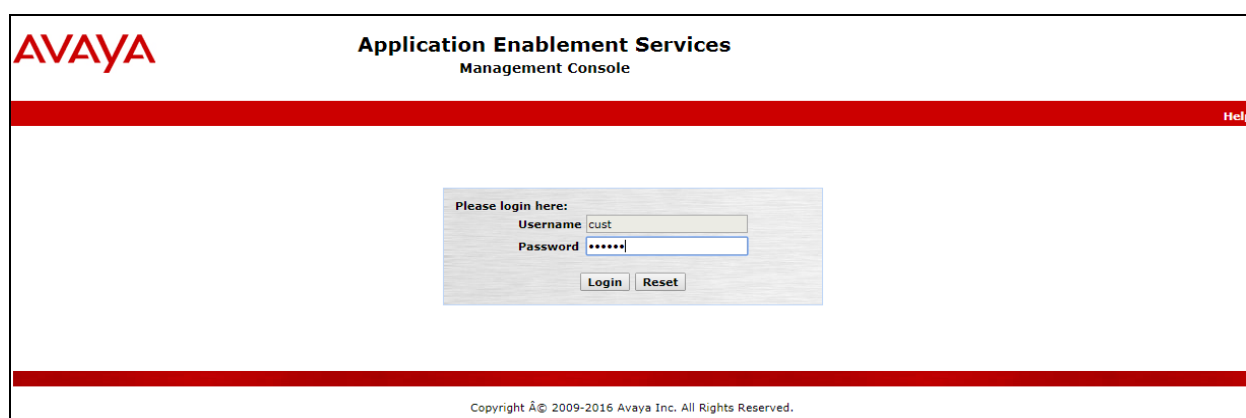
6. Configure Avaya Aura® Application Enablement Services Server

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

- Verify Licensing
- Create Switch Connection
- Administer TSAPI link
- Create CTI User
- Enable CTI Link User
- Identify Tlinks

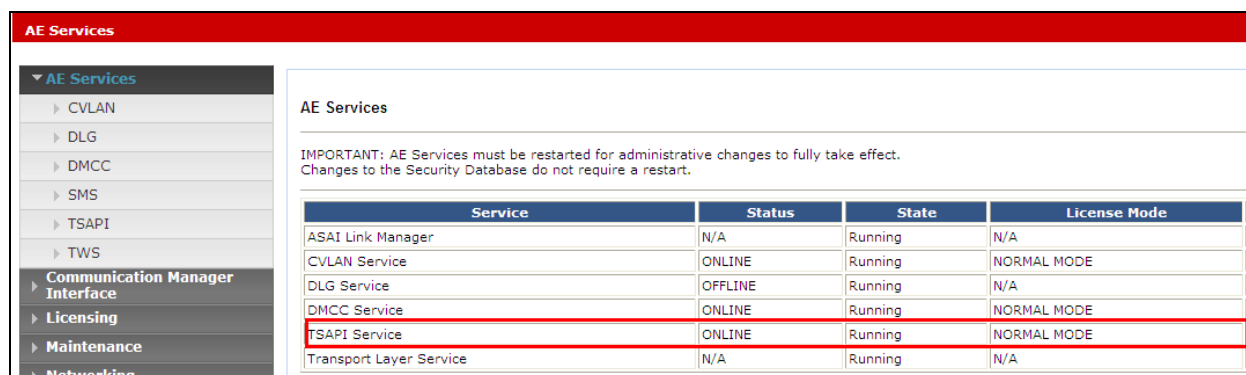
6.1 Verify Licensing

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



The screenshot shows the Avaya Application Enablement Services Management Console login page. At the top left is the Avaya logo. The title is "Application Enablement Services Management Console". A red bar at the top right contains a "Help" link. In the center is a login box with the text "Please login here:". It contains two input fields: "Username" with the value "cust" and "Password" with masked characters "*****". Below the fields are "Login" and "Reset" buttons. At the bottom, a copyright notice reads "Copyright © 2009-2016 Avaya Inc. All Rights Reserved."

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.



The screenshot shows the "AE Services" page in the management console. On the left is a navigation menu with "AE Services" expanded, showing sub-items: CVLAN, DLG, DMCC, SMS, TSAPI, TWS, Communication Manager Interface, Licensing, Maintenance, and Networking. The main content area is titled "AE Services" and includes an important note: "IMPORTANT: AE Services must be restarted for administrative changes to fully take effect. Changes to the Security Database do not require a restart." Below this is a table listing services.

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

6.2 Create 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.

The screenshot shows the Avaya Application Enablement Services Management Console. The left sidebar contains a navigation menu with the following items: AE Services, Communication Manager Interface (selected), Switch Connections (highlighted), Dial Plan, High Availability, Licensing, and Maintenance. The main content area is titled 'Switch Connections' and features a text input field containing 'CM71vmpg' and an 'Add Connection' button. Below this is a table with the following headers: Connection Name, Processor Ethernet, and Msg Period. The table has one empty row. At the bottom of the table are five buttons: Edit Connection, Edit PE/CLAN IPs, Edit H.323 Gatekeeper, Delete Connection, and Survivability Hierarchy.

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 5.9**. Default values may be accepted for the remaining fields. Click **Apply** to save changes.

The screenshot shows the 'Connection Details - CM71vmpg' dialog box. It contains the following fields and options: 'Switch Password' (password field), 'Confirm Switch Password' (password field), 'Msg Period' (text field with '30' and 'Minutes (1 - 72)' label), 'Provide AE Services certificate to switch' (checkbox), 'Secure H323 Connection' (checkbox), and 'Processor Ethernet' (checkbox with a checkmark). At the bottom are 'Apply' and 'Cancel' buttons.

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

Connection Name	Processor Ethernet	Msg Period	
<input checked="" type="radio"/> CM71vmpg	Yes	30	1

Buttons: Edit Connection, **Edit PE/CLAN IPs**, Edit H.323 Gatekeeper, Delete Connection, Survivability Hierarchy

In the resulting screen, enter the IP address of the **procr** as shown in **Section 5.8** that will be used for the AES connection and select the **Add Name or IP** button.

Name or IP Address
10.10.40.47

Buttons: Add/Edit Name or IP, Back

6.3 Administer TSAPI link

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

AVAYA Application Enablement Services Management Console

AE Services | TSAPI | TSAPI Links

TSAPI Links

Link	Switch Connection	Switch CTI Link #

Buttons: **Add Link**, Edit Link, Delete 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 6.2**, from the drop-down list.
- **Switch CTI Link Number:** Corresponding CTI link number configured in **Section 5.10**.
- **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**.

Edit TSAPI Links

Link: 1

Switch Connection: CM71vmpg ▼

Switch CTI Link Number: 1 ▼

ASAI Link Version: 7 ▼

Security: Both ▼

Buttons: Apply Changes, Cancel Changes, Advanced Settings

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

Apply Changes to Link

Warning! Are you sure you want to apply the changes?
These changes can only take effect when the TSAPI server restarts.

⚠ Please use the Maintenance -> Service Controller page to restart the TSAPI server.

Buttons: Apply, Cancel

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**.

Service Controller

Service	Controller Status
<input type="checkbox"/> ASAI Link Manager	Running
<input type="checkbox"/> DMCC Service	Running
<input type="checkbox"/> CVLAN Service	Running
<input type="checkbox"/> DLG Service	Running
<input type="checkbox"/> Transport Layer Service	Running
<input checked="" type="checkbox"/> TSAPI Service	Running

For status on actual services, please use [Status and Control](#)

Buttons: Start, Stop, Restart Service, Restart AE Server

6.4 Create Avaya CTI User

A User ID and password needs to be configured for the Presence Suite 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 (not shown). In the **Add User** screen shown below, enter the following values:

- **User Id** - This will be used by the Presence Suite Server in **Section 7.1**.
- **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 7.1**.
- **CT User** - Select **Yes** from the drop-down menu.

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

The screenshot shows the 'Edit User' form in the 'User Admin' section of the 'User Management' interface. The form contains the following fields:

- * User Id: presence
- * Common Name: presence
- * Surname: presence
- User Password: [empty]
- Confirm Password: [empty]
- Admin Note: [empty]
- Avaya Role: None
- Business Category: [empty]
- Car License: [empty]
- CM Home: [empty]
- Ccs Home: [empty]
- CT User: Yes
- Department Number: [empty]
- Display Name: [empty]
- Employee Number: [empty]
- Employee Type: [empty]

Red boxes highlight the 'User Id', 'Common Name', 'Surname', and 'CT User' fields.

The next screen will show a message indicating that the user was created successfully (not shown).

6.5 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 6.4** and select the **Edit** option (not shown). The **Edit CTI User** screen appears. Check the **Unrestricted Access** box and **Apply Changes** at the bottom of the screen.

The screenshot displays the 'Edit CTI User' interface. On the left, a sidebar menu lists various system components, with 'Security' expanded to show 'Security Database' and 'CTI Users'. The main content area is titled 'Edit CTI User' and contains the following fields and controls:

- User Profile:**
 - User ID: ctiuser
 - Common Name: ctiuser
 - Worktop Name: NONE (dropdown)
 - Unrestricted Access:** ☒ (highlighted with a red box)
- Call and Device Control:**
 - Call Origination/Termination and Device Status: None (dropdown)
- Call and Device Monitoring:**
 - Device Monitoring: None (dropdown)
 - Calls On A Device Monitoring: None (dropdown)
 - Call Monitoring: ☐
- Routing Control:**
 - Allow Routing on Listed Devices: None (dropdown)

At the bottom of the form, there are two buttons: **Apply Changes** (highlighted with a red box) and **Cancel Changes**.

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

6.6 Identify Tlinks

Navigate to **Security** → **Security Database** → **Tlinks**. Verify the value of the **Tlink Name**. This will be needed to configure Presence Suite in **Section 7.1**.

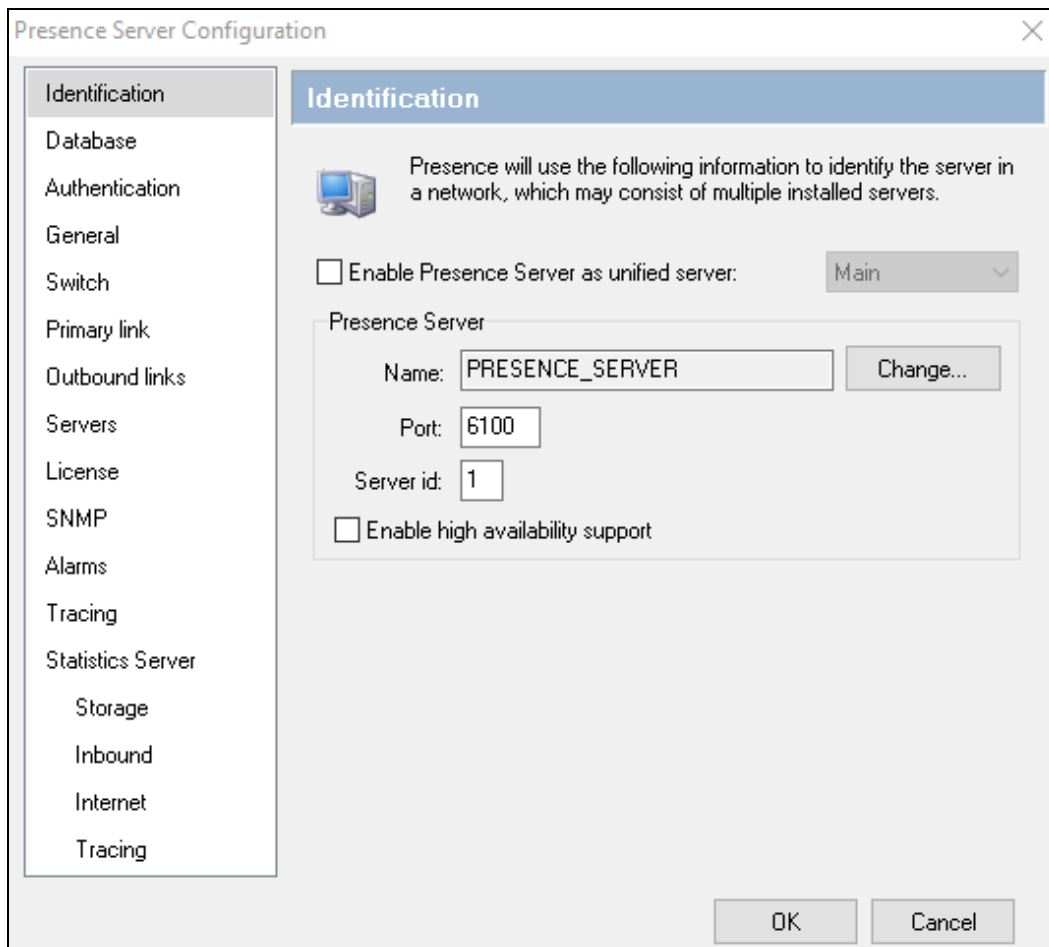
The screenshot displays the Avaya Application Enablement Services Management Console. The top left features the Avaya logo, and the top right shows the title "Application Enablement Services Management Console". A red navigation bar contains the text "Security | Security Database | Tlinks". On the left, a sidebar menu lists various services: AE Services, Communication Manager Interface, High Availability, Licensing, Maintenance, Networking, Security (expanded), Account Management, Audit, Certificate Management, Enterprise Directory, Host AA, PAM, Security Database (expanded), Control, CTI Users, Devices, Device Groups, Tlinks (highlighted), Tlink Groups, and Worktops. The main content area is titled "Tlinks" and shows a "Tlink Name" field with two radio button options: "AVAYA#CM71VMPPG#CSTA#AES71VMPPG" (selected) and "AVAYA#CM71VMPPG#CSTA-S#AES71VMPPG". Below these options is a "Delete Tlink" button.

7. Configure the Presence Suite Server

The Presence Suite includes the Presence Server, Presence Mail Interactions Server, Presence Web Interactions Server, Presence Administrator, Presence Web Supervisor, and Presence Agent. The Presence Server and the Oracle database were pre-installed on the same machine for convenience during the compliance testing. The Presence server was configured and provided by Presence Technology. An outline of the configuration relevant to the Avaya solution integration is detailed below.

7.1 Presence Server Configuration

Launch the Presence Server configuration application by double clicking the **pcoservercfg.exe** located in the pre-installed Presence folder on the Presence Server (not shown). Select the **Identification** option from the menu on the left side of the screen, enter the **Server name** as **PRESENCE_SERVER** as used for the identification of the server. The **Port** can be set to **6100**. Note that the actual value for server port can vary.



The screenshot shows the 'Presence Server Configuration' window. On the left is a vertical menu with options: Identification, Database, Authentication, General, Switch, Primary link, Outbound links, Servers, License, SNMP, Alarms, Tracing, and Statistics Server. The 'Identification' option is selected. The main area is titled 'Identification' and contains the following settings:

- A description: 'Presence will use the following information to identify the server in a network, which may consist of multiple installed servers.' with a computer icon.
- A checkbox 'Enable Presence Server as unified server:' which is unchecked, followed by a dropdown menu set to 'Main'.
- A section titled 'Presence Server' containing:
 - 'Name:' with a text box containing 'PRESENCE_SERVER' and a 'Change...' button.
 - 'Port:' with a text box containing '6100'.
 - 'Server id:' with a text box containing '1'.
 - A checkbox 'Enable high availability support' which is unchecked.

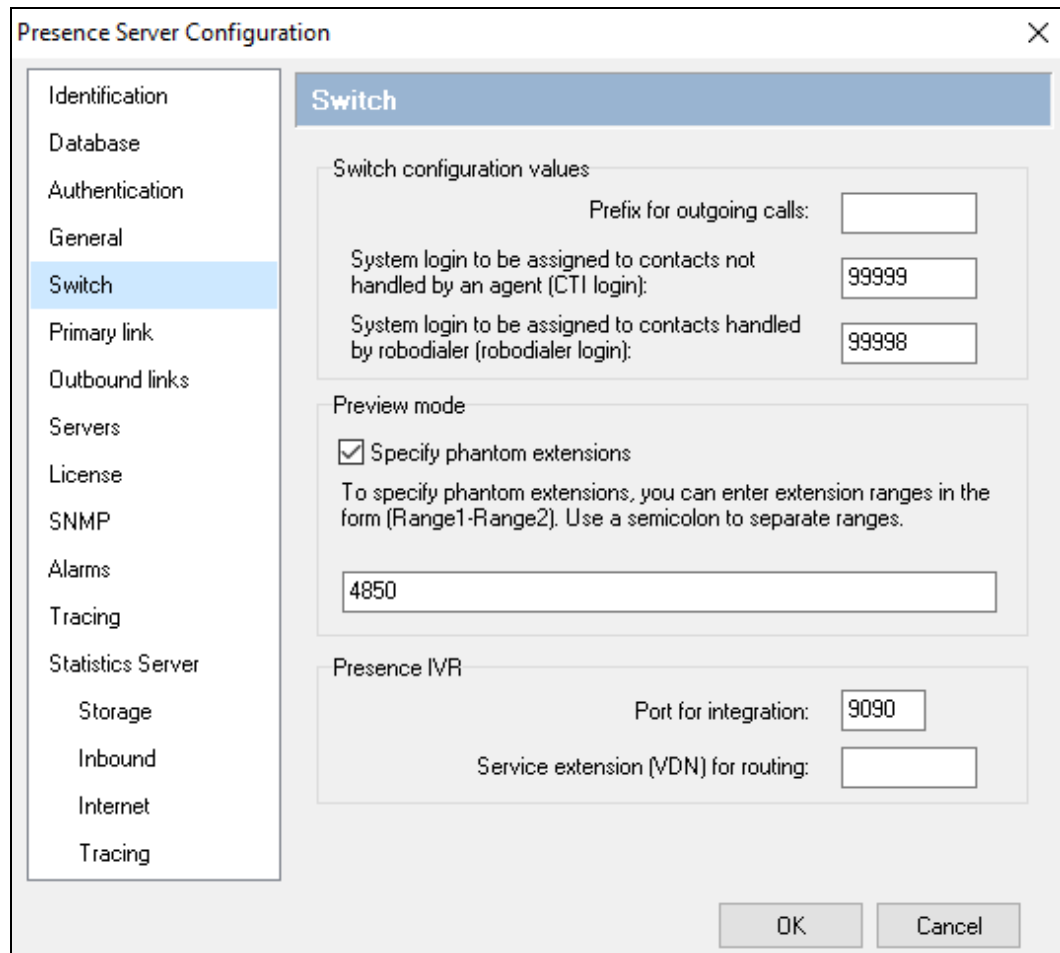
At the bottom right are 'OK' and 'Cancel' buttons.

Select **General** from the menu on the left side of the screen. If desired, the Maintenance configuration values can be altered here, for the compliance test the default values were retained.

The screenshot shows a 'Presence Server Configuration' dialog box with a 'General' tab selected. The left sidebar contains a list of configuration categories: Identification, Database, Authentication, General (highlighted), Switch, Primary link, Outbound links, Servers, License, SNMP, Alarms, Tracing, and Statistics Server. The main area of the dialog is divided into two sections: 'Maintenance configuration values' and 'Other'. The 'Maintenance configuration values' section contains four settings: 'Check for pending outbound calls every' set to 30 seconds, 'Minimum time between queue updates in server (in minutes). If a queue is updated within a shorter interval, a warning will be triggered in server:' set to 15, 'Time for reorganizing queues in server. This is a critical process which may affect the server performance:' set to 03:00, and 'Keep server events from last' set to 15 days. The 'Other' section contains one setting: 'Length of area codes:' set to 6 digits. At the bottom right of the dialog are 'OK' and 'Cancel' buttons.

Configuration Category	Setting	Value	Unit
Maintenance configuration values	Check for pending outbound calls every	30	seconds
	Minimum time between queue updates in server (in minutes). If a queue is updated within a shorter interval, a warning will be triggered in server:	15	minutes
	Time for reorganizing queues in server. This is a critical process which may affect the server performance:	03:00	minutes
	Keep server events from last	15	days
Other	Length of area codes:	6	digits

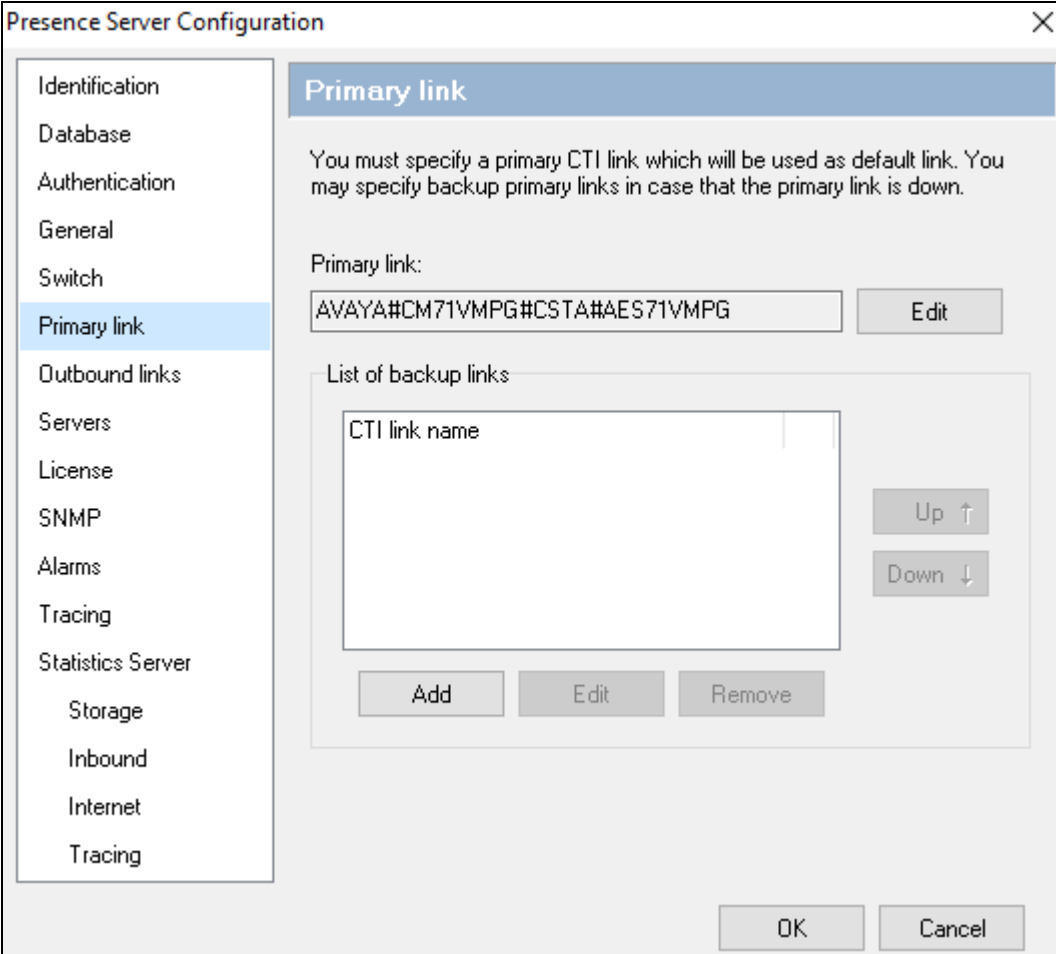
Select the **Switch** option from the menu on the left side of the screen. The **System login to be assigned to contacts not handled by an agent (CTI login)** field should be set to a value supplied by Presence, the value used for this configuration is **99999**. Check the **Specify phantom extension for preview mode** checkbox and enter the phantom extensions configured in **Section 5.9**.



The image shows a 'Presence Server Configuration' dialog box with a sidebar menu on the left and a main configuration area on the right. The 'Switch' option is selected in the sidebar. The main area has a blue header 'Switch' and contains three sections: 'Switch configuration values', 'Preview mode', and 'Presence IVR'. In the 'Switch configuration values' section, there are three text input fields: 'Prefix for outgoing calls' (empty), 'System login to be assigned to contacts not handled by an agent (CTI login):' (containing '99999'), and 'System login to be assigned to contacts handled by robodialer (robodialer login):' (containing '99998'). The 'Preview mode' section has a checked checkbox 'Specify phantom extensions' and a text input field containing '4850'. The 'Presence IVR' section has two text input fields: 'Port for integration:' (containing '9090') and 'Service extension (VDN) for routing:' (empty). At the bottom right are 'OK' and 'Cancel' buttons.

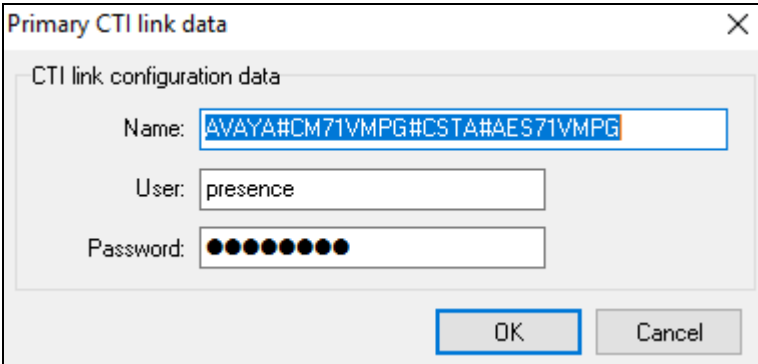
Section	Field	Value
Switch configuration values	Prefix for outgoing calls:	
	System login to be assigned to contacts not handled by an agent (CTI login):	99999
	System login to be assigned to contacts handled by robodialer (robodialer login):	99998
Preview mode	Specify phantom extensions (checkbox)	<input checked="" type="checkbox"/>
	Phantom extensions (text input)	4850
Presence IVR	Port for integration:	9090
	Service extension (VDN) for routing:	

Select the **Primary link** menu on the left side of the screen and choose the **Edit** button to enter a value.



The image shows a 'Presence Server Configuration' dialog box. On the left is a vertical menu with options: Identification, Database, Authentication, General, Switch, **Primary link** (highlighted), Outbound links, Servers, License, SNMP, Alarms, Tracing, and Statistics Server. The main area is titled 'Primary link' and contains the text: 'You must specify a primary CTI link which will be used as default link. You may specify backup primary links in case that the primary link is down.' Below this, there is a 'Primary link:' label followed by a text box containing 'AVAYA#CM71VMPG#CSTA#AES71VMPG' and an 'Edit' button. Further down is a 'List of backup links' section with a large text box labeled 'CTI link name', 'Up' and 'Down' arrow buttons, and 'Add', 'Edit', and 'Remove' buttons. At the bottom right are 'OK' and 'Cancel' buttons.

In the resulting pop-up box enter the Tlink name from **Section 6.6** in the **Name** field. For the **User** and **Password** fields enter the user name and password configured on the Application Enablement Services in **Section 6.4**. Click **OK**.



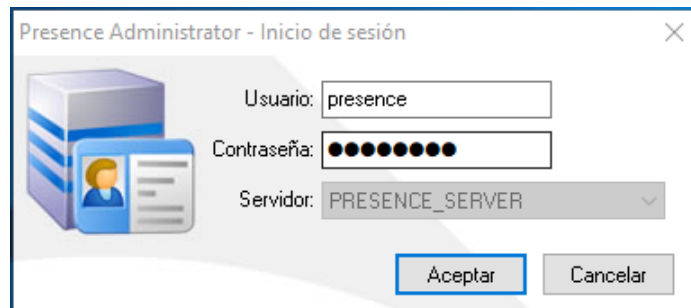
The image shows a 'Primary CTI link data' dialog box. It has a title bar with a close button. The main area is titled 'CTI link configuration data' and contains three fields: 'Name:' with a text box containing 'AVAYA#CM71VMPG#CSTA#AES71VMPG', 'User:' with a text box containing 'presence', and 'Password:' with a text box containing ten black dots. At the bottom right are 'OK' and 'Cancel' buttons.

7.2 Presence Service Configuration

A number of services for inbound, outbound, email and internet were configured via the Presence Administrator. This section covers the basic configuration for each type of service. Please refer to **Section 10** for detailed documentation on configuring Presence Suite services.

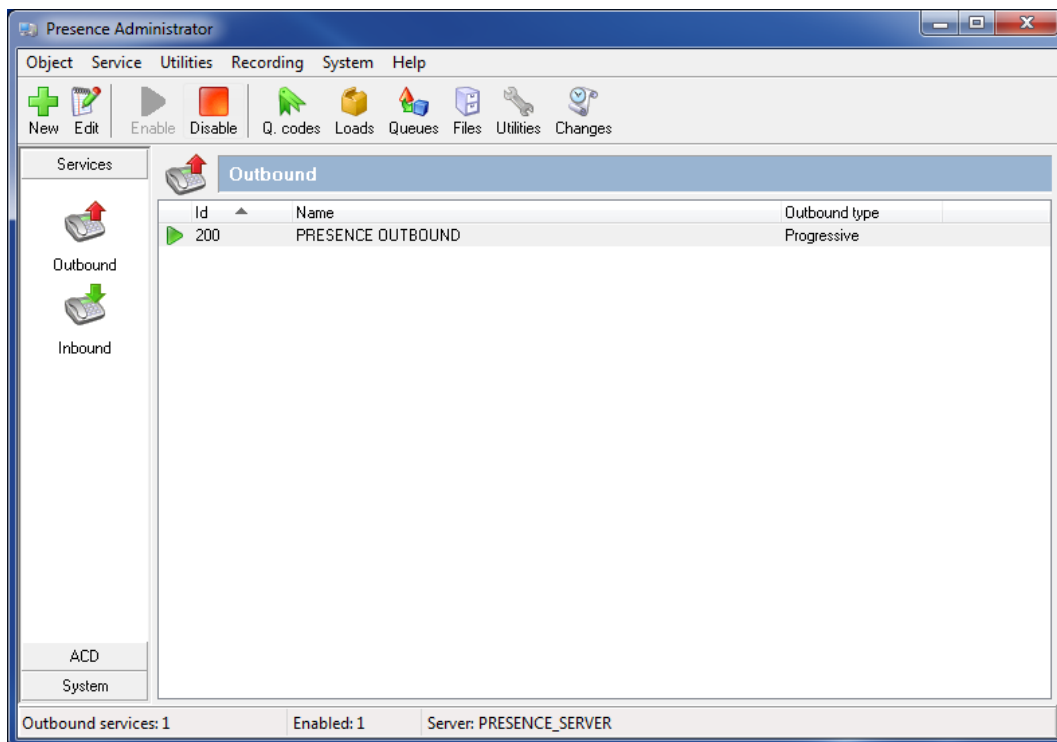
7.2.1 Logging in to Presence Administrator

Launch the **Presence Administrator** application by double clicking the **pcoadmin.exe** located in the Presence folder (not shown). The username and password that appear in the **User** and **Password** fields are created during the Presence Server installation.



7.2.2 Outbound Service

After logging in to Presence Administrator the following screen will be displayed. Select **Services** → **Outbound** from the Presence Administrator main menu on the left hand side. Click the **New** button to configure an outbound service.



In the resulting screen, select **General** from the menu on the left hand side and enter a **Name** for the outbound service. In the **Outbound type** field select the type of outbound service, this specifies the mode in which the outbound service will operate, for further details of the type of outbound service available please refer to documentation in **Section 10**. In the **Calling hours** field set the time range for which the outbound service will be active. All other fields are left with their default values.

The screenshot shows the 'Outbound service' configuration window with the 'General' tab selected. The left sidebar contains a list of configuration categories, with 'General' checked. The main area displays the following fields and values:

- Id:** 200
- Name:** PRESENCE OUTBOUND
- Outbound type:** Progressive
- Resource profile:** General
- Stop reasons:** [All]
- Scheduled calling hours:**
 - Do not schedule records for the last 15 minutes of a time range
 - ☐ Limit date: 14/12/2017
- Outbound calling hours:** 09:00-21:00

At the bottom right, there are 'OK' and 'Cancel' buttons.

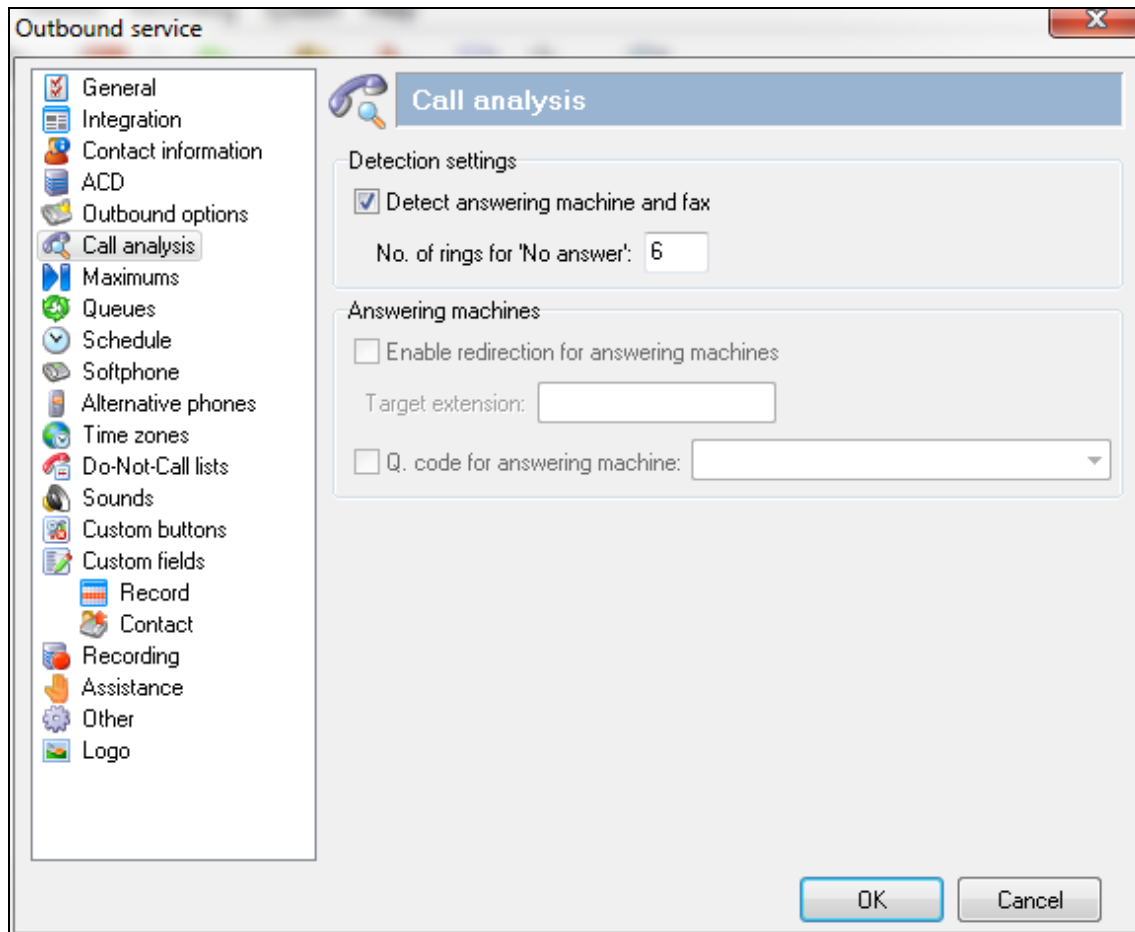
Select **ACD** from the left hand side menu and moving to the right. In the **Extension/Skill** field enter the extension number assigned to the outbound hunt group configured in **Section 5.3.1**. In the **VDN/SE** field enter the VDN number assigned to Outbound calls configured in **Section 5.3.3**. In the test configuration only one CTI link was configured so the **CTI Link** field is set to <<Primary CTI Link>> if multiple CTI links exist on the system then the specific CTI link can be specified. All other field may be left at their default values.

The screenshot shows the 'Outbound service' configuration window. On the left is a sidebar with a tree view containing the following items: General, Integration, Contact information, ACD (selected), Outbound options, Call analysis, Maximums, Queues, Schedule, Softphone, Alternative phones, Time zones, Do-Not-Call lists, Sounds, Custom buttons, Custom fields, Record, Contact, Recording, Assistance, Other, and Logo. The main panel is titled 'ACD' and contains the following fields and options:

- ACD Items**
 - Extension/Skill: 4806
 - VDN/SE: 4906
 - CTI link: <<Primary CTI link>> (dropdown menu)
 - ☒ Use primary CTI link in case that CTI link is not connected
- ☐ Maximum number of concurrent service calls: [text box]
- ☐ Check agent availability
- ☐ Minimum number/percentage of available agents: [text box]

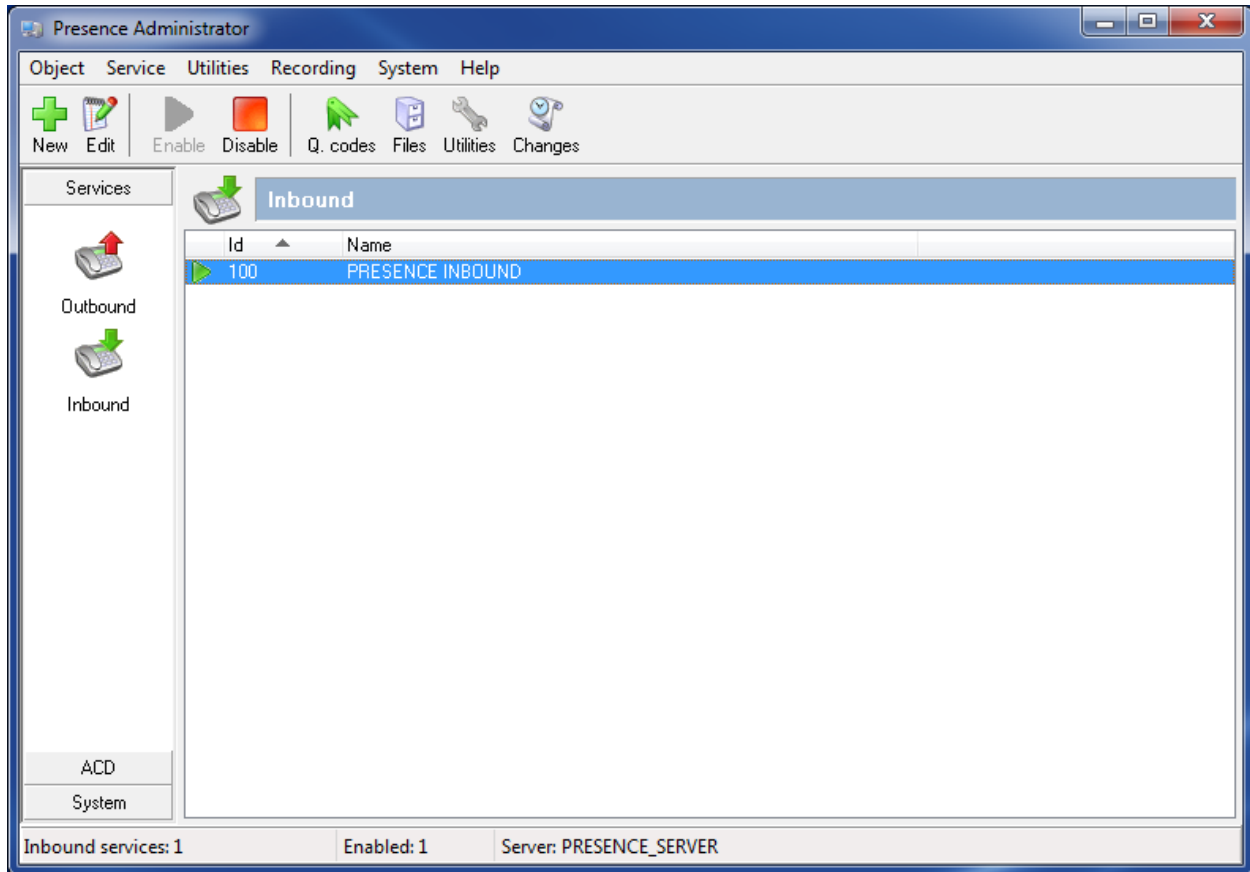
At the bottom right are 'OK' and 'Cancel' buttons.

Select **Call analysis** from the left hand side menu. The fields in the right hand side define how the outbound service should behave following an unsuccessful attempt at contacting the customer. For testing, the **Detect answering machine and fax** box are checked and the **No. of rings for 'No answer'** is set to **6**, as shown in the screen below. Click **OK** to complete the outbound service configuration.



7.2.3 Inbound Service

To configure an inbound service, from the left hand side select **Services** → **Inbound** from the Presence Administrator main menu. Click the **New** button.



In the resulting screen, select **General** from the menu on the left hand side and enter a **Name** for the inbound service. All other fields are left with their default values.

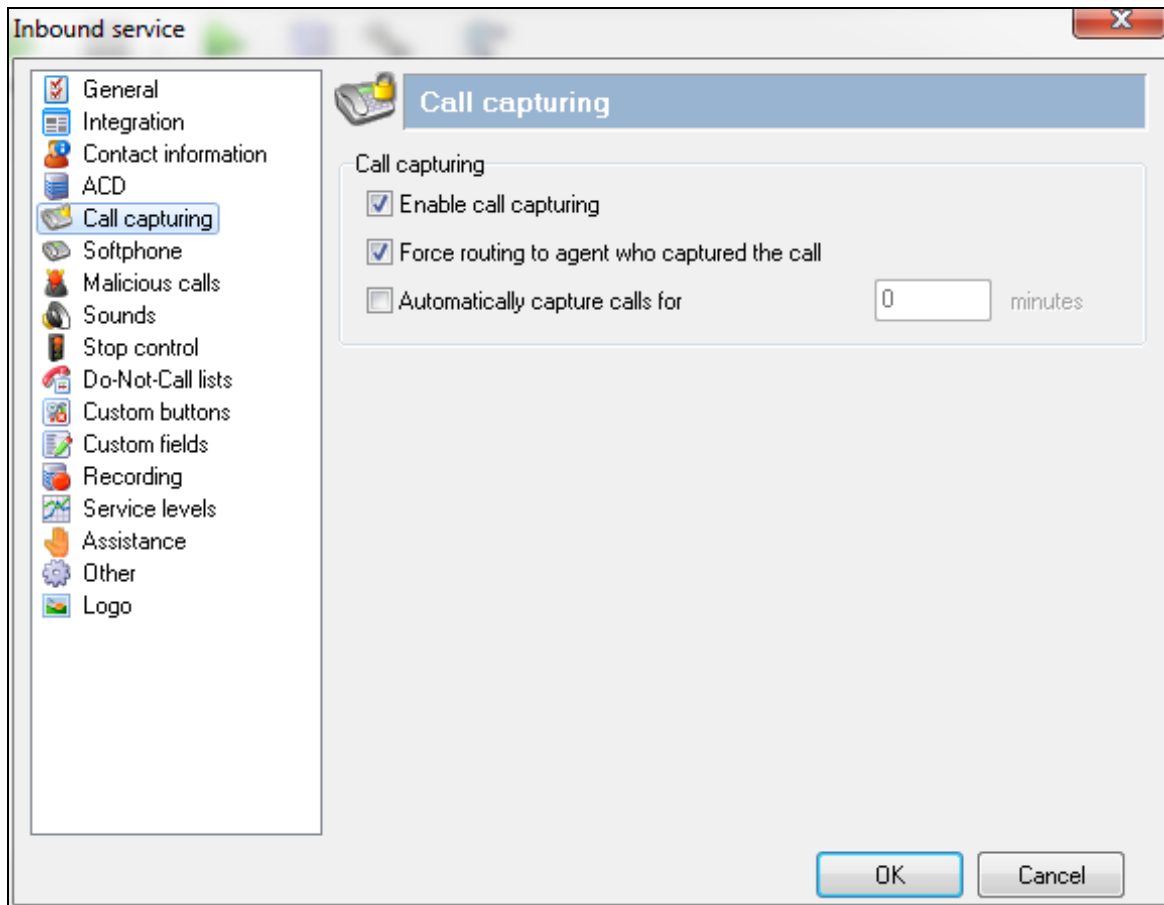
The screenshot shows a window titled "Inbound service" with a close button (X) in the top right corner. On the left is a vertical menu with icons and labels: General (checked), Integration, Contact information, ACD, Call capturing, Softphone, Malicious calls, Sounds, Stop control, Do-Not-Call lists, Custom buttons, Custom fields, Recording, Service levels, Assistance, Other, and Logo. The main area is titled "General" and contains the following fields: "Id:" with a text box containing "100", "Name:" with a text box containing "PRESENCE INBOUND", "Resource profile:" with a dropdown menu showing "General", and "Stop reasons:" with a dropdown menu showing "[All]". At the bottom right are "OK" and "Cancel" buttons.

Field	Value
Id	100
Name	PRESENCE INBOUND
Resource profile	General
Stop reasons	[All]

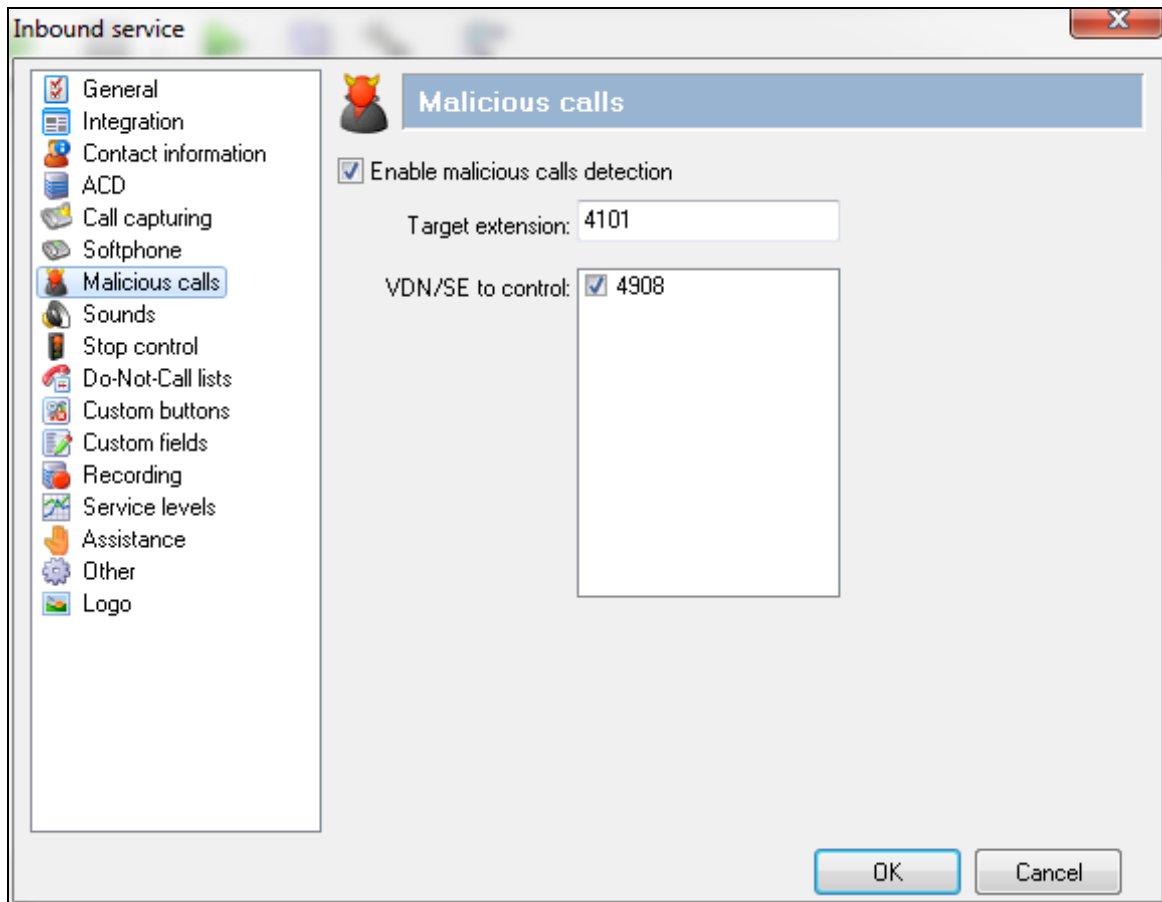
Select **ACD** from the left hand side menu and moving to the right, under the heading **Skills** enter the skill group extensions configured in **Section 5.3.1** that will handle inbound calls in the untitled box (this includes email and web chat call types) and click **Add**. The skill group extensions will then appear to the left in the **Extension/Skill** box. Under the heading **VDN/SE** enter the VDN configured in **Section 5.3.3** that will handle inbound calls in the untitled box and click **Add**. The VDN will then appear to the left in the **VDN/SE** box.

The screenshot shows the 'Inbound service' configuration window with the 'ACD' tab selected. The left sidebar lists various service options, with 'ACD' highlighted. The main area is divided into two sections: 'Skills' and 'VDN/SE'. Each section has a list box on the left and an 'Add' button on the right. In the 'Skills' section, the list box contains '4808'. In the 'VDN/SE' section, the list box contains '4908'. At the bottom right are 'OK' and 'Cancel' buttons.

Select **Call capturing** from the left hand side menu and moving to the right, select the **Enable call capturing**. **Force routing to agent who captured the call** was checked for this compliance testing but is each users preference. These options allow an agent to mark an inbound call so that if the caller rings back while that agent is logged onto the system, the call will be routed again to the agent who tagged the call.



Select **Malicious calls** from the left hand side menu and moving to the right, select the **Enable malicious calls detection** check box. This option allows agents to mark calls as malicious, so that the caller can be directed to another location such as a supervisor position if they call back again. In the **Target extension** field enter the extension that any malicious calls will be re-directed to. In the **VDN/SE to control** field select the VDNs this option will be available on.



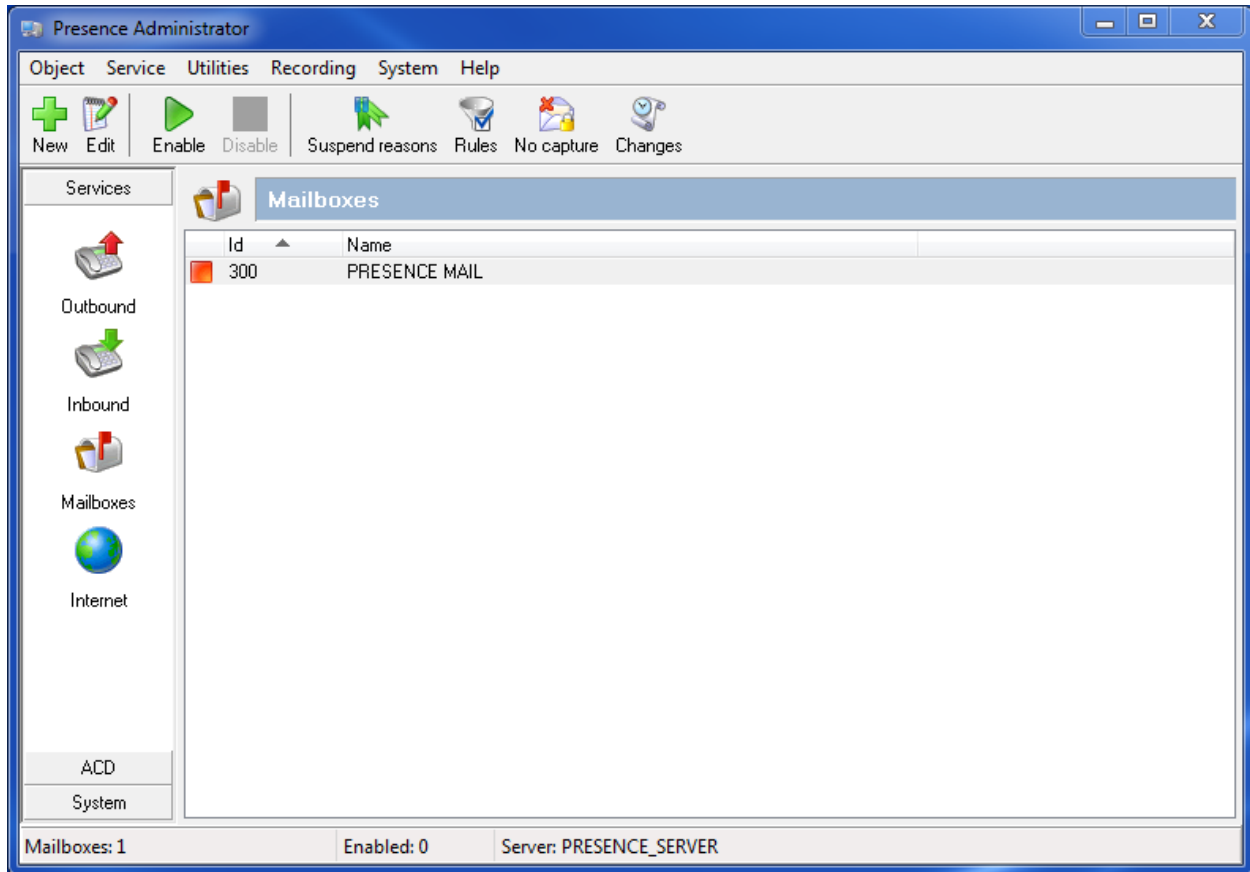
Select **Other** from the left hand side menu and moving to the right, select the **Enable direct transfer to agents of this service** check box. Enter the direct agent transfer VDN assigned in **Section 5.3.3** in the **Use the following VDN/SE for transfer** field. Click **OK** to complete the inbound service configuration.

The screenshot shows the 'Inbound service' configuration window with the 'Other' tab selected. The left sidebar lists various configuration categories, with 'Other' highlighted. The main panel contains three sections: 'After-call work', 'Transfer to agents', and 'Outgoing calls identification'. In the 'Transfer to agents' section, the 'Enable direct transfer to agents of this service' checkbox is checked, and the 'Use the following VDN/SE for transfer' dropdown is set to '4908'. The 'Outgoing calls identification' section has the 'Enable outgoing calls identification' checkbox unchecked. The 'After-call work' section includes checkboxes for 'Minimum after-call work time' and 'Maximum after-call work time', both currently unchecked, and a dropdown for 'Q. code for maximum time'. The window has 'OK' and 'Cancel' buttons at the bottom right.

Section	Option	Value / Status
After-call work	Minimum after-call work time	<input type="checkbox"/> seconds
	Maximum after-call work time	<input type="checkbox"/> seconds
	Q. code for maximum time	[Dropdown]
	Use q. code only if contact has not yet been qualified	<input type="checkbox"/>
Transfer to agents	Enable direct transfer to agents of this service	<input checked="" type="checkbox"/>
	Use the following VDN/SE for transfer	4908
Outgoing calls identification	Enable outgoing calls identification	<input type="checkbox"/>
	Phone no.	[Text Field]

7.2.4 Email Service

To configure an email service, from the left hand side select **Services** → **Mailboxes** from the Presence Administrator main menu. Click the **New** button.



In the resulting screen, select **General** from the menu on the left hand side and enter a **Name** for the email service. Referring to **Section 5.3**, in the **General VDN/SE** field enter the VDN assigned for email and enter the VDN assigned for suspended emails in the **Suspended VDN/SE** field. This is to allow each incoming email to be reported on. When the email arrives the VDN is called and the agent is placed on work.

The image shows a 'Mailboxes' configuration window. On the left is a sidebar with icons and labels: 'General' (checked), 'Incoming mail', 'IMAP', 'Outgoing mail', 'Mail movement', and 'Other'. The main area is titled 'General' and contains two sections: 'Identification' and 'ACD'. In the 'Identification' section, 'Id' is 300, 'Name' is 'PRESENCE MAIL', 'Default priority' is 50, and 'Resource profile' is 'General'. In the 'ACD' section, 'Inbound service' is '100 - PRESENCE INBOUND', 'General VDN/SE' is 4907, 'Suspended VDN/SE' is 4907, and 'Maximum number of concurrent e-mails' is 0. 'OK' and 'Cancel' buttons are at the bottom right.

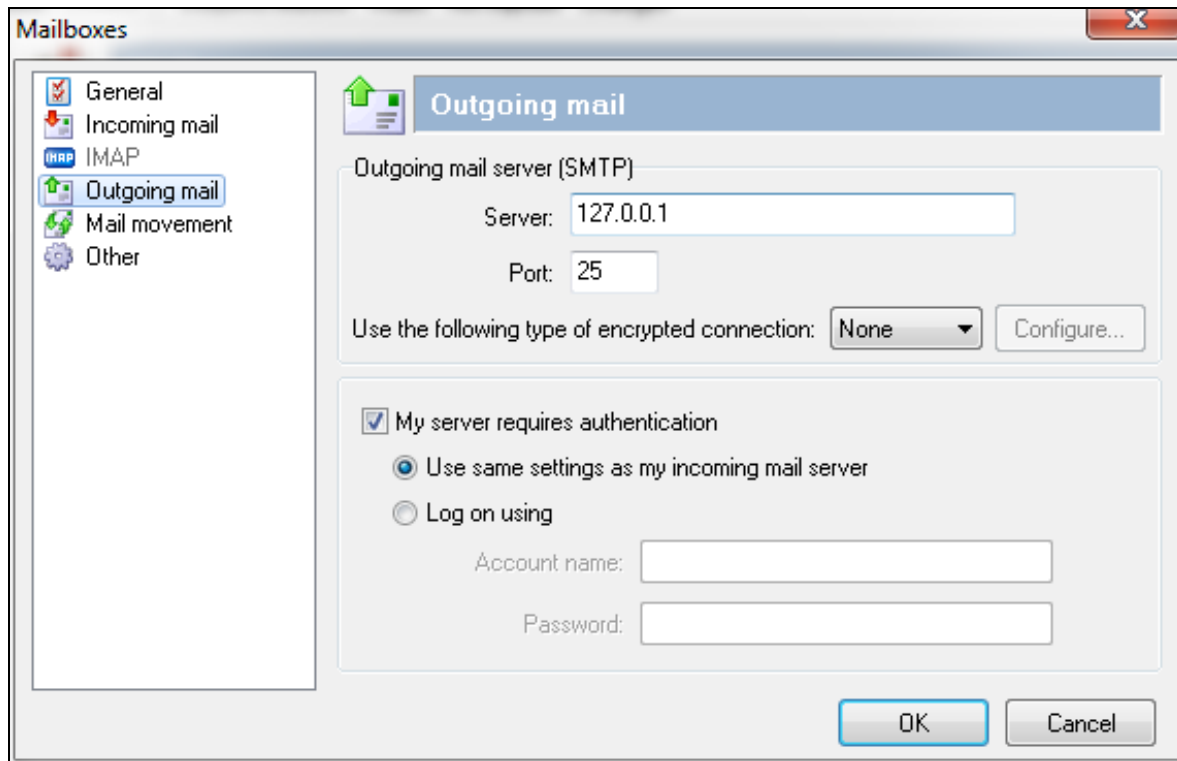
Section	Field	Value
Identification	Id	300
	Name	PRESENCE MAIL
	Default priority	50
	Resource profile	General
ACD	Inbound service	100 - PRESENCE INBOUND
	General VDN/SE	4907
	Suspended VDN/SE	4907
	Maximum number of concurrent e-mails	0

Select **Incoming mail** from the left hand side menu. This window allows administrator to specify the POP3 server and account from which to download incoming mails. In the **Server** field enter the POP3 mail server address. For the interoperability testing this was the same IP address as the Presence Server. The POP3 port of **110** is entered into the **Port** field. Under the **Incoming mail account** heading enter the **Account name**, **Password** and **E-mail address** associated with the POP3 mail account.

The screenshot shows a window titled "Mailboxes" with a sidebar on the left containing icons and labels for "General", "Incoming mail", "IMAP", "Outgoing mail", "Mail movement", and "Other". The "Incoming mail" option is selected. The main area is titled "Incoming mail" and contains two sections. The first section, "Incoming mail server (IMAP/POP3)", has a "Protocol" dropdown set to "POP3", a "Server" text field with "127.0.0.1", a "Port" text field with "110", and a "Use the following type of encrypted connection:" dropdown set to "None" with a "Configure..." button. The second section, "Incoming mail account", has an "Account name" text field with "server", a "Password" text field with masked characters, and an "E-mail address" text field with "server@prstestplans.com". At the bottom right are "OK" and "Cancel" buttons.

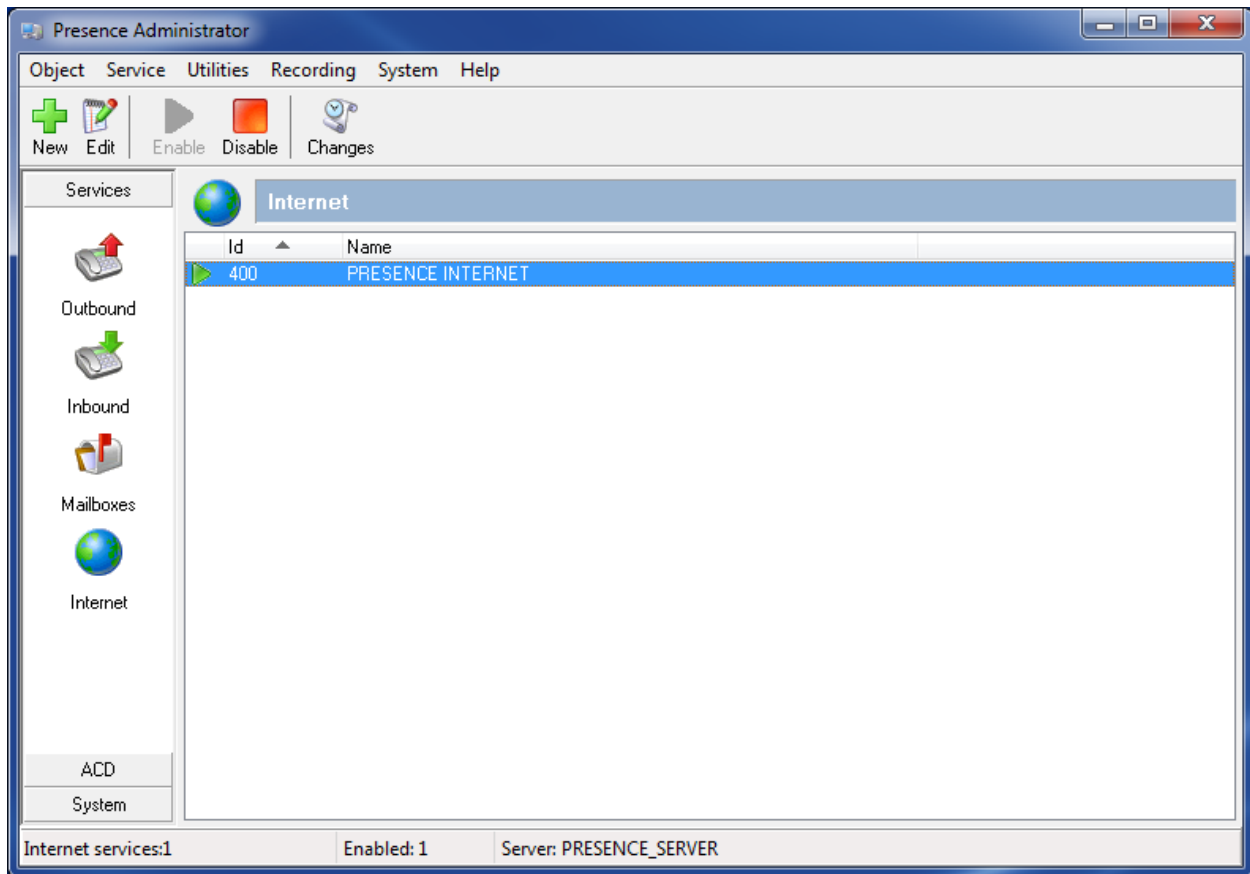
Field	Value
Protocol	POP3
Server	127.0.0.1
Port	110
Use the following type of encrypted connection:	None
Account name	server
Password	••••••••
E-mail address	server@prstestplans.com

Select **Outgoing mail** from the left hand side menu and moving to the right, define the SMTP server that will be used to send response emails from Presence agents. Enter an IP address in the server field. For the interoperability testing this was the same IP address as the Presence Server. The SMTP port of **25** is entered into the **Port** field. Click **OK** to complete the email service configuration.



7.2.5 Web Chat / Web Call Back

To configure a web service, from the left hand side select **Services** → **Internet** from the Presence Administrator main menu. Click the **New** button.



In the resulting screen, select **General** from the menu on the left hand side and enter a **Name** for the web service. The **Enable chat** and **Enable callback** check boxes should be selected and the relevant VDN for each entered into the **VDN/SE** field, click **OK** when done.

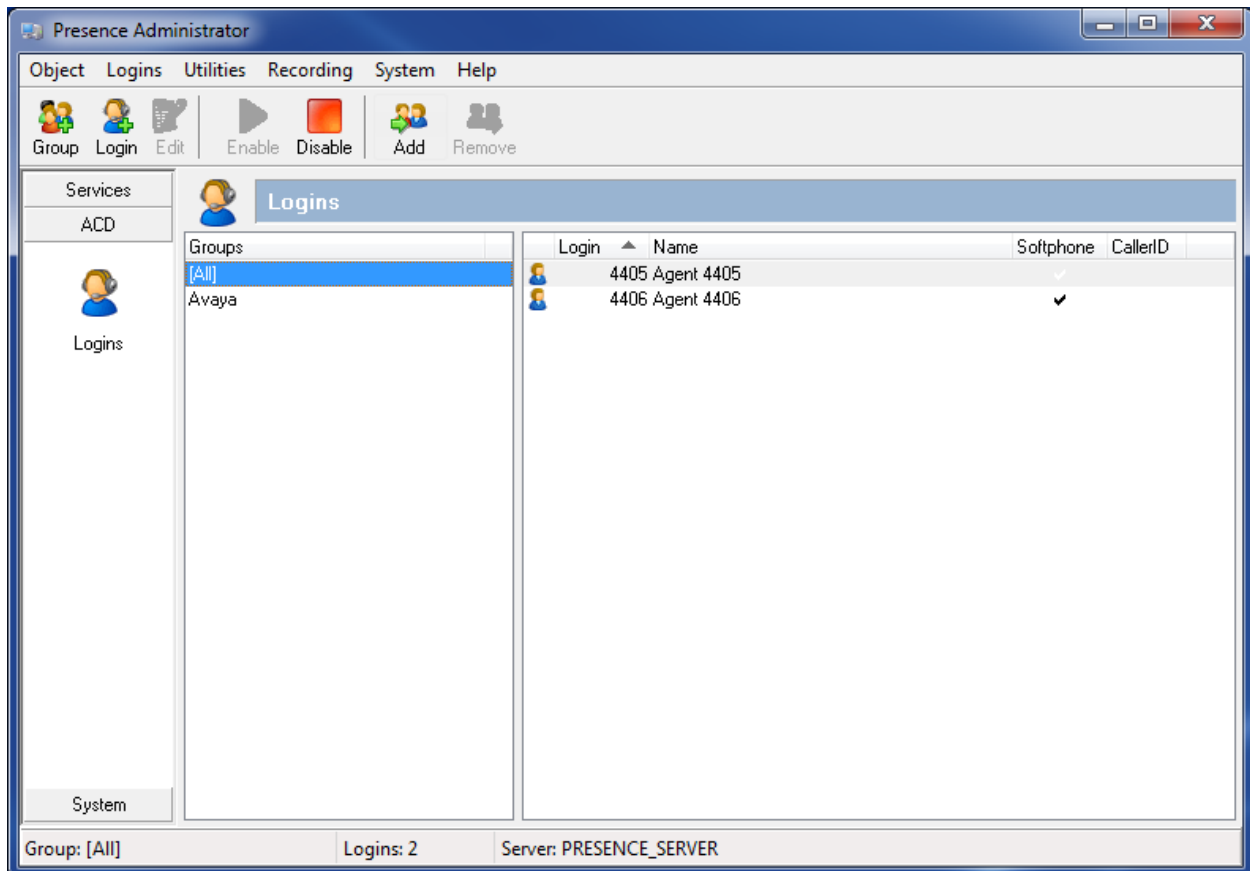
The screenshot shows the 'Internet service' configuration window with the 'General' tab selected. The left sidebar contains a list of categories: General (checked), URL, Interface, Texts, Mail, Service levels, Assistance, and Other. The main area displays the following configuration options:

- Id:** 400
- Name:** PRESENCE INTERNET
- Inbound service:** 100 - PRESENCE INBOUND
- Chat:**
 - ☒ Enable chat
 - VDN/SE:** 4908
- Callback:**
 - ☒ Enable callback
 - VDN/SE:** 4908
- Web collaboration:**
 - ☒ Enable web collaboration
 - Linker:** (empty text field)

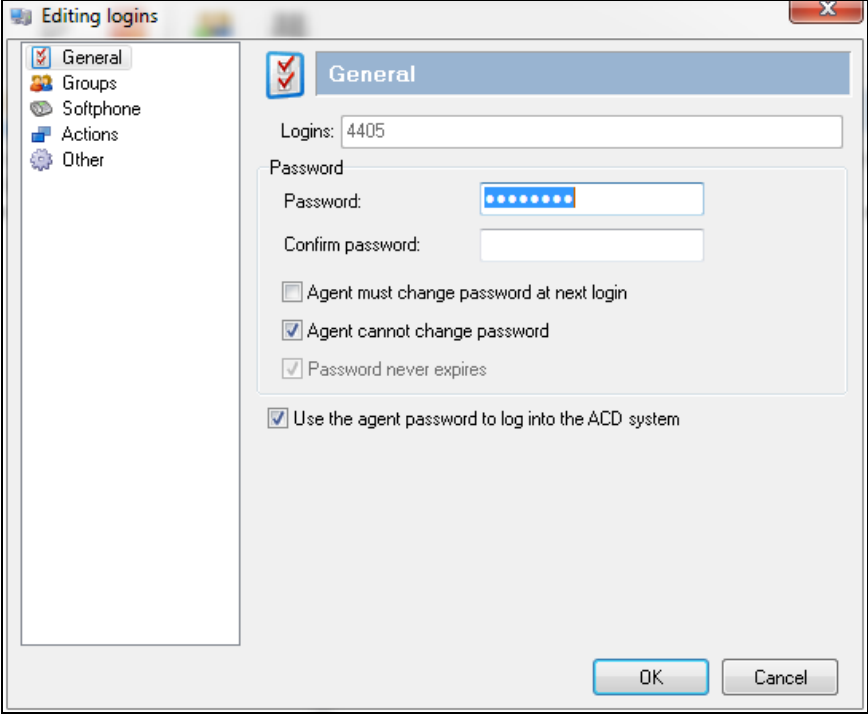
At the bottom right, there are 'OK' and 'Cancel' buttons.

7.2.6 Add ACD Agent Logins

To add the agent logins administered on Communication Manager for use by Presence Suite, from the left hand pane of the Presence Administrator main menu select **ACD** → **Logins** and click the **Login** button.



In the **Logins** field, enter a Communication Manager Agent Login ID and a password, as configured in **Section 5.5**. Best practice is to tick **Agent cannot change password** as shown.



The screenshot shows the 'Editing logins' dialog box with the 'General' tab selected. The 'Logins' field contains the value '4405'. The 'Password' field is masked with dots. The 'Confirm password' field is empty. The 'Agent cannot change password' checkbox is checked. The 'Agent must change password at next login' checkbox is unchecked. The 'Password never expires' checkbox is checked. The 'Use the agent password to log into the ACD system' checkbox is checked. The 'OK' and 'Cancel' buttons are at the bottom right.

Editing logins

General

Logins: 4405

Password

Password: [masked]

Confirm password: [empty]

☐ Agent must change password at next login

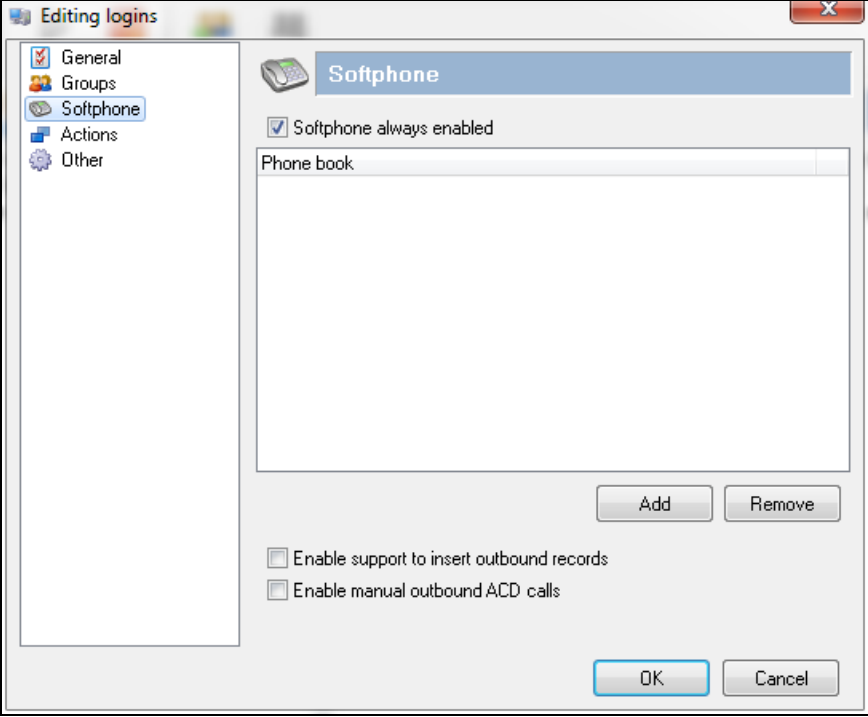
☒ Agent cannot change password

☒ Password never expires

☒ Use the agent password to log into the ACD system

OK Cancel

Click on **Softphone** in the left pane, and place a tick in the **Softphone always enabled** field. Click **OK** when done.



The screenshot shows the 'Editing logins' dialog box with the 'Softphone' tab selected. The 'Softphone always enabled' checkbox is checked. The 'Phone book' field is empty. The 'Add' and 'Remove' buttons are below the 'Phone book' field. The 'Enable support to insert outbound records' checkbox is unchecked. The 'Enable manual outbound ACD calls' checkbox is unchecked. The 'OK' and 'Cancel' buttons are at the bottom right.

Editing logins

Softphone

☒ Softphone always enabled

Phone book

Add Remove

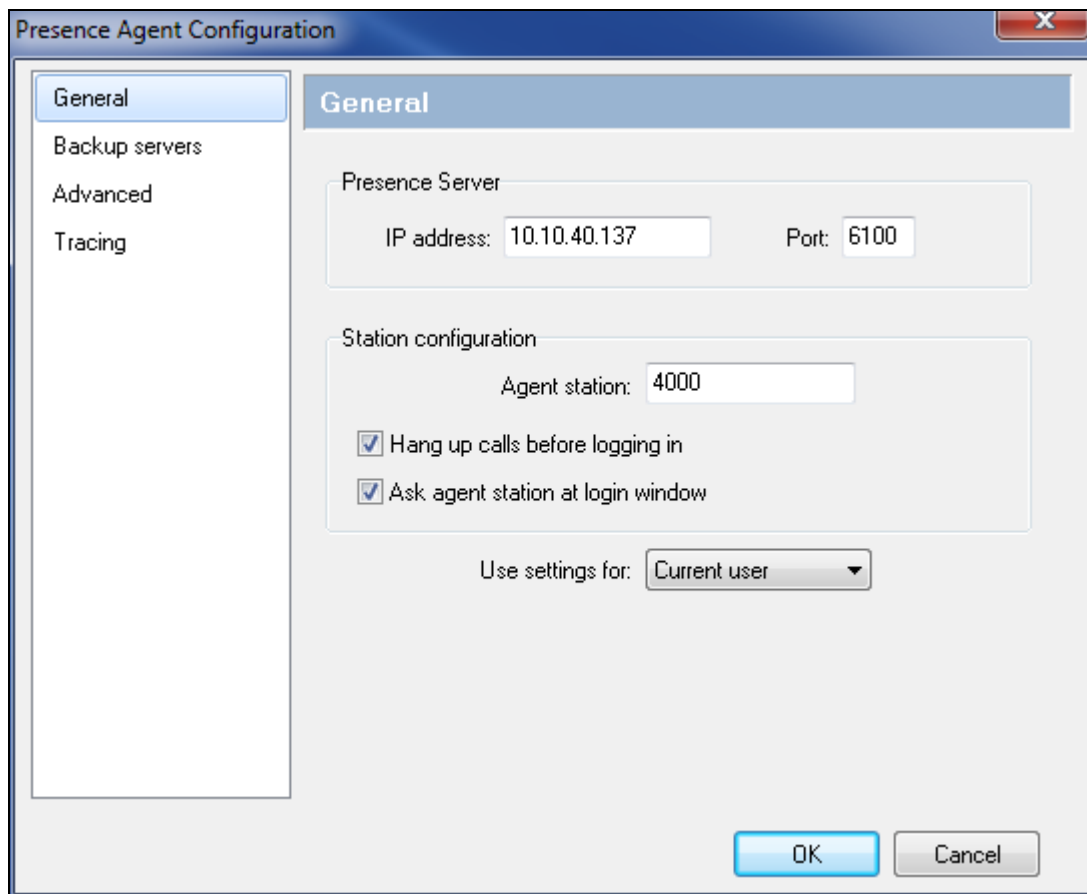
☐ Enable support to insert outbound records

☐ Enable manual outbound ACD calls

OK Cancel

7.3 Presence Agent Configuration

The following steps are carried out on the Presence Suite Agent PC. Prior to installing the Presence agent, ensure that the DBExpress driver (dbexpoda40.dll) is located in the **C:\Windows\System32** directory. The DBExpress driver allows the agent application to communicate with the Oracle database. Installing this driver eliminates the need to install the Oracle client. Launch the Presence agent configuration application by double clicking the **pcoagentcfg.exe** located in the **C: → Presence** folder. Enter the **Presence Server IP:** address as **10.10.40.137**. The **Presence Server port** can be left as the default value of **6100**. Enter the extension of the agent that will be using this workstation in the **Agent station** field. Check both the **Hang up calls before logging in** and the **Ask agent station at login window** check boxes. In the field **Use settings for** choose **Current user** from the drop down menu. Click **OK**. This step is needed for each agent configured; only the agent station field will vary.

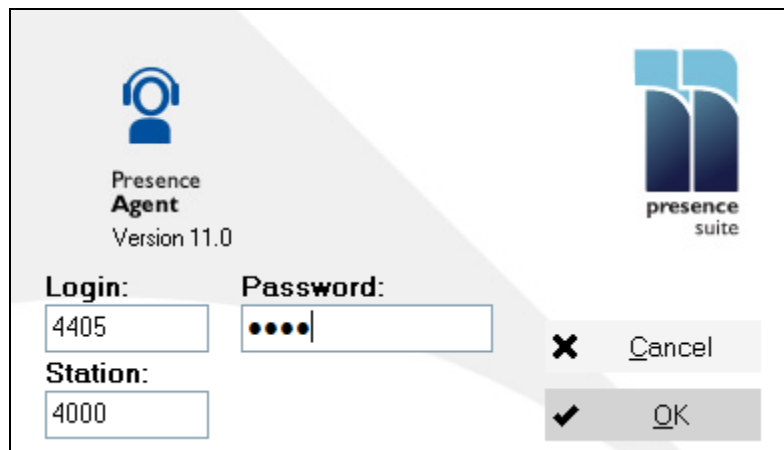


8. Verification Steps

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

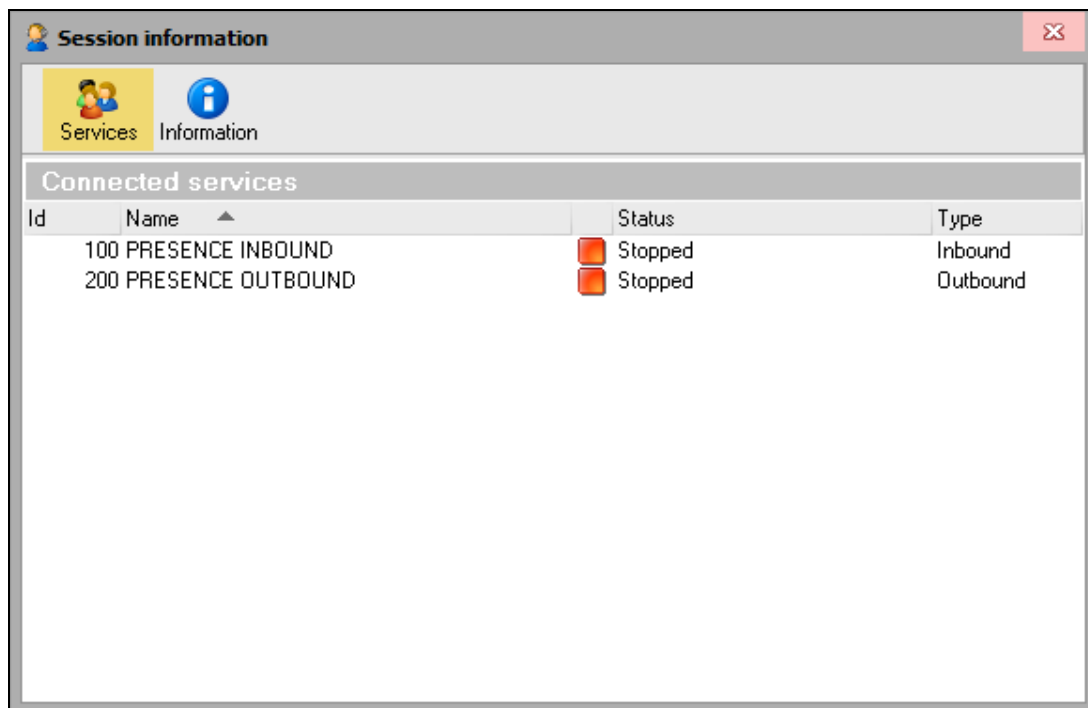
8.1 Verify Presence Suite

Launch the Presence agent configuration application by double clicking the **pcoagent.exe** located in the Presence folder (not shown). Enter the agent **Login** and **Password** configured in **Section 5.5** and click on **OK**.



The image shows the 'Presence Agent Version 11.0' login window. It features a blue headset icon and the 'presence suite' logo. The window contains two text input fields: 'Login:' with the value '4405' and 'Password:' with masked characters '••••'. Below these is a 'Station:' field with the value '4000'. On the right side, there are two buttons: 'Cancel' with a red 'X' icon and 'OK' with a green checkmark icon.

In the next screen, click on the **Services** button in the task bar. The service set up for the agent will be displayed.



The image shows the 'Session information' window. It has a title bar with a close button. Below the title bar, there are two tabs: 'Services' (selected) and 'Information'. The 'Services' tab displays a table of 'Connected services'.

Id	Name	Status	Type
100	PRESENCE INBOUND	Stopped	Inbound
200	PRESENCE OUTBOUND	Stopped	Outbound

A task bar is present at the top of the Agent PC. Click on the green arrow to put the agent in to an available state.



The information status on the task bar goes to available indicating the agent is ready to receive calls.



An outbound call is placed and answered.



8.2 Verify Avaya Aura® Communication Manager CTI Link

The following steps can ensure that the communication between Communication Manager and the Application Enablement Services server is functioning correctly. Check the TSAPI link status with Application Enablement Services by using the command **status aesvcs cti-link**. Verify the **Service State** of the TSAPI link is **established**.

```
status aesvcs cti-link
```

AE SERVICES CTI LINK STATUS						
CTI Link	Version	Mnt Busy	AE Services Server	Service State	Msgs Sent	Msgs Rcvd
1	7	no	AES71vmpg	established	87	61

Use the command **status aesvcs interface** to verify that the status **Local Node** of Application Enablement Services interface is connected and **listening**.

```
status aesvcs interface
```

AE SERVICES INTERFACE STATUS			
Local Node	Enabled?	Number of Connections	Status
procr	yes	1	listening

Verify that there is a link with the Application Enablement Services and that messages are being sent and received by using the command **status aesvcs link**.

```
status aesvcs link
```

AE SERVICES LINK STATUS						
Srvr/ Link	AE Services Server	Remote IP	Remote Port	Local Node	Msgs Sent	Msgs Rcvd
01/01	AES71vmpg	10.10.16.43	57650	procr	683	665

8.3 Verify Avaya Aura® Application Enablement Services CTI Connection

The following steps are carried out on Application Enablement Services to ensure that the communication link between Communication Manager and the Application Enablement Services server is functioning correctly.

8.3.1 TSAPI Link

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

- ▶ AE Services
- ▶ Communication Manager Interface
- High Availability
- ▶ Licensing
- ▶ Maintenance
- ▶ Networking
- ▶ Security
- ▼ Status
 - Alarm Viewer
 - Log Manager
 - ▶ Logs
 - ▼ Status and Control
 - CVLAN Service Summary
 - DLG Services Summary
 - DMCC Service Summary
 - Switch Conn Summary
 - TSAPI Service Summary

TSAPI Link Details

☐ Enable page refresh every 60 seconds

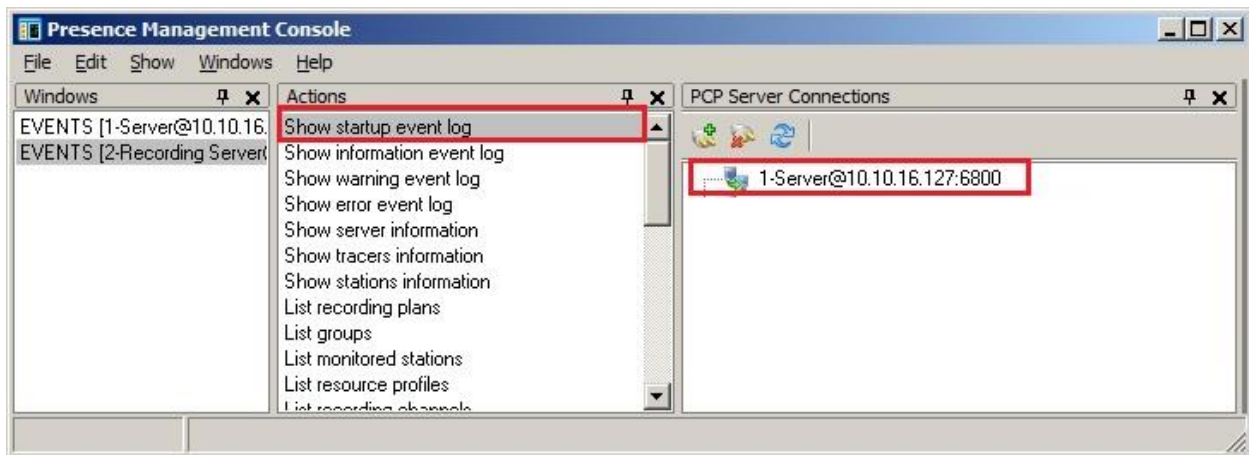
	Link	Switch Name	Switch CTI Link ID	Status	Since	State
	1	CM1627	1	Talking	Mon Nov 16 14:54:50 2015	Online

For service-wide information, choose one of the following:

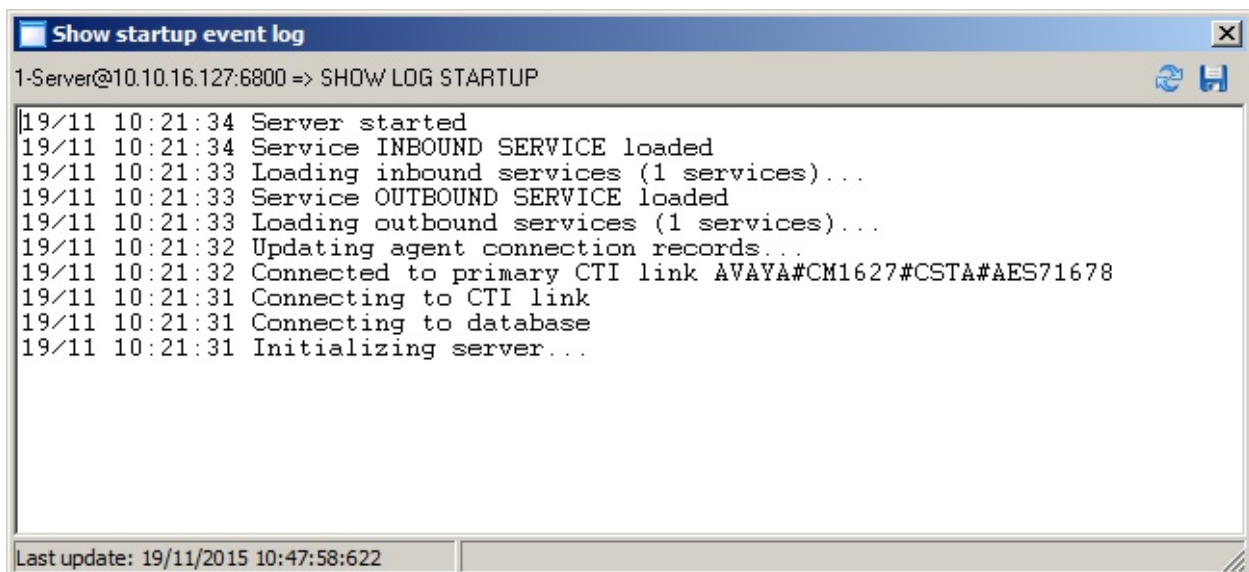
8.4 Verify Presence Suite CTI Connection

One of the available methods to confirm correct startup is a startup log which can be accessed from Presence Management Console. Navigate to **C: → Presence → pmconsole.exe** (not shown). A startup log commences when the Presence Server is trying to load and connect to the Application Enablement Services server. Click on the item named **Server@10.10.16.127:6800** in the **PCP Server Connections** pane of the Management Console. To open the startup event log, double click **Show startup event log** in the **Actions** pane.

Note: The example below shows a connection to another AES server not the server mentioned in this document.



Verify successful CTI connection and service startup.



9. Conclusion

These Application Notes describe the configuration steps required for Presence Suite R11.0 to successfully interoperate with Avaya Aura® Communication Manager R7.1 using Avaya Aura® Application Enablement Services R7.1. All feature functionality and serviceability test cases were completed successfully with observations noted in **Section 2.2**.

10. Additional References

This section references the Avaya and Presence Suite product documentation that are relevant to these Application Notes.

Product documentation for Avaya products may be found at <http://support.avaya.com>.

- [1] *Administering Avaya Aura® Communication Manager*, 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*

The following documentation is available on request from Presence: www.presenceco.com

- [4] *ACD Sys Presence Administrator Manual Presence Suite*, V11.0
- [5] *Presence Installation Guides Presence Software*, V11.0
- [6] *PBX/ACD Requirements Presence Software*, V11.0

©2018 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. 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 DevConnect Program at devconnect@avaya.com.