



## **Avaya Solution & Interoperability Test Lab**

---

# **Application Notes for Presence Technology Presence Suite R9.0 with Avaya Aura® Communication Manager R6.0.1 and Avaya Aura® Application Enablement Services R6.1.1 – 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.

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 and Avaya Aura® Communication Manager with Avaya Aura® Application Enablement Services (AES). 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 Messaging
- Presence Internet

Link Failure\Recovery was also tested to ensure successful reconnection on link failure. 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 campaign calls. Functionality testing included basic telephony operations such as answer, hold/retrieve, transfer, and conference. This was carried out for the inbound and outbound campaign 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.

### 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 for the CLAN.

## 2.2 Test Results

All test cases passed successfully. For link failover, as soon as Presence Server identifies the link is down, it automatically re-starts the service, requiring the agents to login again. This is as expected.

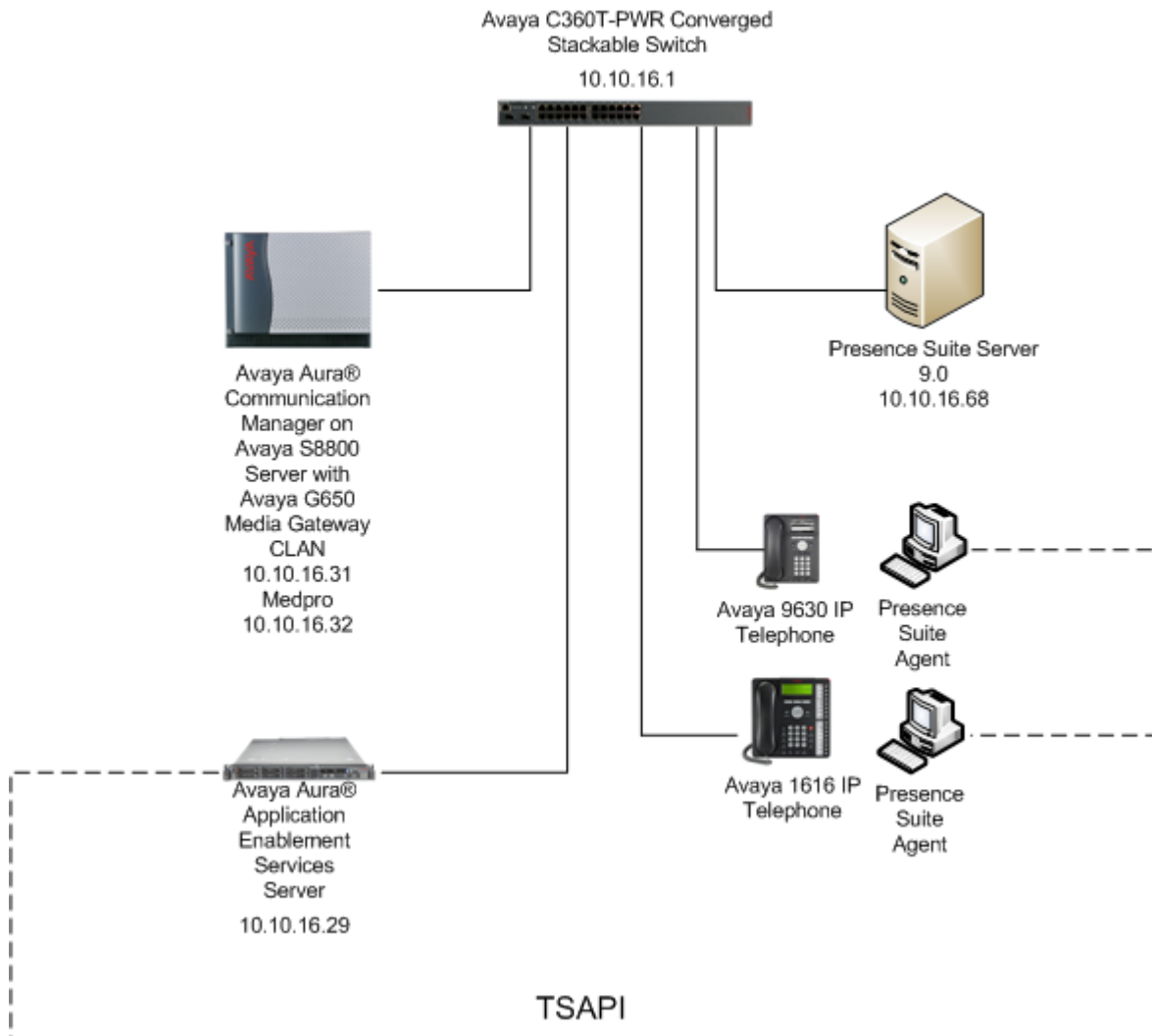
## 2.3 Support

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

- Email: [support@presenceco.com](mailto:support@presenceco.com)
- Website: [www.presenceco.com](http://www.presenceco.com)
- Phone: +34 93 10 10 300

### 3 Reference Configuration

**Figure 1** shows the network topology during interoperability testing. Avaya S8800 Server running Communication Manager with an Avaya G650 Media Gateway was used as the hosting PBX. Presence Suite, including Presence Agent PC's, are connected to the LAN and control the Avaya IP telephones via Application Enablement Services using TSAPI.



**Figure 1: Avaya Aura® Communication Manager with Aura® Application Enablement Server and Presence Technology Presence Suite Server configuration**

## 4 Equipment and Software Validated

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

Equipment	Software
Avaya S8800 Server	Avaya Aura® Communication Manager R6.0.1 Service Pack 04
Avaya G650 Media Gateway CLAN -TN799DP MEDPRO- TN2602AP	HW 01 FW 040 HW 08 FW 061
Avaya S8800 Server	Avaya Aura® Application Enablement Services R6.1.1
Avaya 96xx Telephone (H.323)	3.102S
Avaya 16xx Telephone (H323)	1.301S
Generic Server	VMWare ESXi 4.1.0 Microsoft Windows XP SP3 Presence Suite Server 9.0

**Table 1: Hardware and Software Version Numbers**

## 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
- Define Feature Access Codes (FAC)
- Administer Trunk Group
- Administer Hunt Groups, Vectors and VDN's
- Administer Class of Restriction
- Administer Agent Logins
- Administer Agent Stations
- Administer Phantom Stations
- Configure CLAN 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** 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	<b>Computer Telephony Adjunct Links?</b>	<b>y</b>
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	Digital Loss Plan Modification?	y
Async. Transfer Mode (ATM) Trunking?	n	DS1 MSP?	y
ATM WAN Spare Processor?	n	DS1 Echo Cancellation?	y
ATMS?	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: 6.0			
<b>ACD?</b>	<b>y</b>	Reason Codes?	y
BCMS (Basic)?	y	Service Level Maximizer?	n
BCMS/VuStats Service Level?	y	Service Observing (Basic)?	y
BSR Local Treatment for IP & ISDN?	y	Service Observing (Remote/By FAC)?	y
Business Advocate?	n	Service Observing (VDNs)?	y
Call Work Codes?	y	Timed ACW?	y
DTMF Feedback Signals For VRU?	y	<b>Vectoring (Basic)?</b>	<b>y</b>
Dynamic Advocate?	n	Vectoring (Prompting)?	y
<b>Expert Agent Selection (EAS)?</b>	<b>y</b>	Vectoring (G3V4 Enhanced)?	y
EAS-PHD?	y	Vectoring (3.0 Enhanced)?	y
Forced ACD Calls?	n	Vectoring (ANI/II-Digits Routing)?	y
Least Occupied Agent?	y	Vectoring (G3V4 Advanced Routing)?	y
Lookahead Interflow (LAI)?	y	Vectoring (CINFO)?	y
Multiple Call Handling (On Request)?	y	Vectoring (Best Service Routing)?	y
Multiple Call Handling (Forced)?	y	Vectoring (Holidays)?	y
PASTE (Display PBX Data on Phone)?	y	Vectoring (Variables)?	y

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 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**.

```
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 Define Feature Access Codes (FAC)

Use the **change feature-access-codes** command to define the required access codes. On **Page 5** define a FAC for each of the following:

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

<b>change feature-access-codes</b>	<b>Page 5 of 10</b>
FEATURE ACCESS CODE (FAC)	
Call Center Features	
AGENT WORK MODES	
After Call Work Access Code: *36	
Assist Access Code: *37	
Auto-In Access Code: *38	
Aux Work Access Code: *39	
Login Access Code: *40	
Logout Access Code: *41	
Manual-in Access Code: *42	

## 5.4 Administer Trunk

Use the **change trunk group n** command, where **n** is the trunk group number for the pre-configured ISDN trunk which will be used for inbound and outbound campaign calls. It is assumed that the ISDN trunk and the corresponding signaling group are already configured. The trunk group number used for interoperability testing is **2**. On **Page 1** set the **COR** (class of restriction) to **1**, this is the COR used for the sample configuration.

change trunk-group 1			Page 1 of 22		
TRUNK GROUP					
Group Number: 1		Group Type: isdn		CDR Reports: y	
Group Name: Simulated PSTN		COR: 1		TN: 1	TAC: 701
Direction: two-way		Outgoing Display? y		Carrier Medium: PRI/BRI	
Dial Access? y		Busy Threshold: 255		Night Service:	
Queue Length: 0					
Service Type: public-ntwrk		Auth Code? n		TestCall ITC: rest	
		Far End Test Line No:			
TestCall BCC: 4					

On **Page 3**, set the following values: **UII IE Treatment** to **shared** and **Maximum Size of UII IE Contents** to **32**. Default values may be used in the remaining fields.

change trunk-group 2			Page	3 of	22
TRUNK FEATURES					
ACA Assignment? n	Measured: none	Wideband Support? n			
		Maintenance Tests? y			
	Data Restriction? n	NCA-TSC Trunk Member:			
	Send Name: n	Send Calling Number: n			
Used for DCS? n		Send EMU Visitor CPN? n			
Suppress # Outpulsing? n	Format: public				
Outgoing Channel ID Encoding: preferred	UII IE Treatment: shared				
	Maximum Size of UII IE Contents: 32				
	Replace Restricted Numbers? y				

## 5.5 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.

### 5.5.1 Hunt Groups

Enter the **add hunt-group n** command where **n** is an available hunt group number. 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 8		Page 1 of 4	
HUNT GROUP			
Group Number: 8	ACD? y		
Group Name: Presenceco Inbound	Queue? y		
Group Extension: 4095	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 8		Page 2 of 4	
HUNT GROUP			
Skill? y	Expected Call Handling Time (sec): 180		
AAS? n			
Measured: none			
Supervisor Extension:			
Controlling Adjunct: none			
Timed ACW Interval (sec):			
Multiple Call Handling: none			

Repeat the above steps to create a hunt groups for the outbound service, hunt group **9** is shown below.

<b>add hunt-group 9</b>		<b>Page 1 of 4</b>
HUNT GROUP		
Group Number: 9		ACD? y
Group Name: Presenceco Outbound		Queue? y
Group Extension: 4094		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.

<b>add hunt-group 9</b>		<b>Page 2 of 4</b>
HUNT GROUP		
Skill? y	Expected Call Handling Time (sec): 180	
AAS? n		
Measured: none		
Supervisor Extension:		
Controlling Adjunct: none		
Timed ACW Interval (sec):		
Multiple Call Handling: none		

## 5.5.2 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 3 of the ip-services page, as configured in **Section 5.11**, in this case Server ID **1**. Enter the vector steps to queue to **skill 8** as shown below. Skill 8 relates to the skill enabled hunt group configured previously.

<b>add vector 4</b>		<b>Page 1 of 6</b>
CALL VECTOR		
Number: 4	Name: Presenceco In	
Multimedia? n	Attendant Vectoring? n	Meet-me Conf? n Lock? n
Basic? y	EAS? y G3V4 Enhanced? y	ANI/II-Digits? y ASAI Routing? y
Prompting? y	LAI? y G3V4 Adv Route? y	CINFO? y BSR? y Holidays? y
Variables? y	3.0 Enhanced? y	
01 adjunct	routing link 1	
02 wait-time	5 secs hearing silence	
03 queue-to	skill 8 pri m	
04 wait-time	999 secs hearing ringback	

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

```

add vector 5                                     Page 1 of 6
                                CALL VECTOR

Number: 5                                Name: Presenceco Outb
Multimedia? n      Attendant Vectoring? n      Meet-me Conf? n      Lock? n
Basic? y      EAS? y      G3V4 Enhanced? y      ANI/II-Digits? y      ASAI Routing? y
Prompting? y      LAI? y      G3V4 Adv Route? y      CINFO? y      BSR? y      Holidays? y
Variables? y      3.0 Enhanced? y
01 adjunct      routing link 1
02 wait-time      5 secs hearing silence
03 queue-to      skill 9      pri m
04 wait-time      999 secs hearing ringback

```

### 5.5.3 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 1804                                     Page 1 of 3
                                VECTOR DIRECTORY NUMBER

                                Extension: 1804
                                Name*: Presenceco Inbound
                                Destination: Vector Number      4
                                Attendant Vectoring? n
                                Meet-me Conferencing? n
                                Allow VDN Override? n
                                COR: 1
                                TN*: 1
                                Measured: none

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

```

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

```

add vdn 1805                                     Page 1 of 3
                                VECTOR DIRECTORY NUMBER

                                Extension: 1805
                                Name*: Presenceco Outbound
                                Destination: Vector Number      5
                                Attendant Vectoring? n
                                Meet-me Conferencing? n
                                Allow VDN Override? n
                                COR: 1
                                TN*: 1
                                Measured: none

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

```

## 5.6 Administer Class of Restriction

Enter the **change cor 1** command where **1** corresponds to the Class of Restriction assigned to the trunk group in **Section 5.4** and the agent login IDs in **Section 5.7**. 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: Default			
FRL: 0		APLT? y	
Can Be Service Observed? y	Calling Party Restriction: none		
Can Be A Service Observer? y	Called Party Restriction: none		
Time of Day Chart: 1	Forced Entry of Account Codes? n		
Priority Queuing? n	Direct Agent Calling? y		
Restriction Override: all	Facility Access Trunk Test? n		
Restricted Call List? n	Can Change Coverage? n n		

## 5.7 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 5.6**. 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 201		Page 1 of 3
AGENT LOGINID		
Login ID: 201	AAS? n	
Name: Presenceco Agent 1	AUDIX? n	
TN: 1	LWC Reception: spe	
COR: 1	LWC Log External Calls? n	
Coverage Path:	AUDIX Name for Messaging:	
Security Code:	LoginID for ISDN/SIP Display? n	
	Password:	
	Password (enter again):	
	Auto Answer: station	
	MIA Across Skills: system	

On **Page 2**, assign a skill to the agent by entering the relevant hunt group number created in **Section 5.5.1** 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 **8**.

change agent-loginID 201		Page 2 of 3
AGENT LOGINID		
Direct Agent Skill: 8		Service Objective? n
Call Handling Preference: skill-level		Local Call Preference? n
SN	RL SL	
1: 8	1	
2: 9	1	
SN	RL SL	
16:		
31:		
46:		
SN	RL SL	
32:		
47:		

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

## 5.8 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 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.

<b>change station 4001</b>		<b>Page 4 of 5</b>	
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:		

## 5.9 Administer Phantom Stations

Presence Suite uses stations via the AES to initiate calls on Communication Manager. These stations will be used to place calls to customers for outbound campaigns 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** and enter **X** for the **Port**. Extensions **1500** to **1502** were created.

<b>add station 1500</b>		<b>Page 1 of 5</b>	
STATION			
Extension: 1500	Lock Messages?	n	BCC: 0
Type: 6408D+	Security Code:		TN: 1
Port: X	Coverage Path 1:		COR: 1
Name: Presenceco Phantom	Coverage Path 2:		COS: 1
	Hunt-to Station:		
STATION OPTIONS			
	Time of Day Lock Table:		
Loss Group: 1	Personalized Ringing Pattern:	1	
Data Module? n	Message Lamp Ext:	3500	
Display Module? n			
Survivable COR: internal	Media Complex Ext:		
Survivable Trunk Dest? y			

## 5.10 Configure CLAN for Avaya Aura® Application Enablement Services Connectivity

Define a node name for the CLAN by using the command **change node-names ip** and adding an IP address and node name for the CLAN.

change node-names ip		Page 1 of 2
IP NODE NAMES		
Name	IP Address	
devconaes611	10.10.16.29	
clancm601	10.10.16.31	

Add the CLAN to the system configuration using the **add ip-interface n** command where **n** is the CLAN board location. Enter the CLAN node name assigned in the previous step to the **Node Name** field. Enter values for the **Subnet Mask** and **Gateway Node Name** fields. In this case, **/24** and **Gateway** are used to correspond to the network configuration in these Application Notes. Set the **Enable Interface** field to **y**. Default values may be used in the remaining fields.

add ip-interface 01a02		Page 1 of 3
IP INTERFACES		
Type: C-LAN	Target socket load and Warning level: 400	
Slot: 01A02	Receive Buffer TCP Window Size: 8320	
Code/Suffix: TN799 D	Allow H.323 Endpoints? y	
<b>Enable Interface? y</b>	Allow H.248 Gateways? y	
VLAN: n	Gatekeeper Priority: 5	
Network Region: 1		
IPV4 PARAMETERS		
<b>Node Name: clancm601</b>	IP Address:	
<b>Gateway Node Name: Gateway</b>	IP Address:	
<b>Subnet Mask: /24</b>		
Ethernet Link: 1		
Network uses 1's for Broadcast Addresses? y		

## 5.11 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 CLAN in **Section 5.10**.
- **Local Port** Retain the default value of **8765**.

change ip-services						Page 1 of 3
Service Type	Enabled	Local Node	Local Port	Remote Node	Remote Port	
AESVCS	y	CLAN	8765			

Go to **Page 3** of the ip-services form and enter the following values:

- **AE Services Server:** Name obtained from the AES server, in this case **devconaes611**
- **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 3 of 3
AE Services Administration					
Server ID	AE Services Server	Password	Enabled	Status	
1:	devconaes611	Avayapassword1	y	in use	
2:	:				

## 5.12 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: 4999		
Type: ADJ-IP		
Name: devconaes611	COR: 1	

## 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.



#### Application Enablement Services Management Console


[Help](#)

Please login here:

Username	<input type="text" value="craft"/>
Password	<input type="password" value="*****"/>

© Copyright © 2009-2010 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.



**Application Enablement Services**  
 Management Console

Welcome: User craft  
 Last login: Thu Dec 15 19:28:13 2011 from 10.10.16.62  
 HostName/IP: devconaes611/10.10.16.29  
 Server Offer Type: TURNKEY  
 SW Version: r6-1-1-30-0

AE Services
Home | Help | Logout

▼ AE Services

▶ CVLAN

▶ DLG

▶ DMCC

▶ SMS

▶ TSAPI

▶ TWS

▶ Communication Manager Interface

▶ Licensing

▶ Maintenance

▶ Networking

▶ Security

▶ Status

▶ User Management

▶ Utilities

### AE Services

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

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


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

\* -- For more detail, please mouse over the Cause, you'll see the tooltip, or go to help page.

**License Information**  
 You are licensed to run Application Enablement (CTI) release 6.x

## 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.



**Application Enablement Services**  
 Management Console

Welcome: User craft  
 Last login: Thu Dec 15 19:28:13 2011 from 10.10.16.62  
 HostName/IP: devconaes611/10.10.16.29  
 Server Offer Type: TURNKEY  
 SW Version: r6-1-1-30-0

Communication Manager Interface | Switch Connections
Home | Help | Logout

▶ AE Services

▼ Communication Manager Interface

Switch Connections

▶ Dial Plan

▶ Licensing

▶ Maintenance

▶ Networking

▶ Security

▶ Status

▶ User Management

▶ Utilities

▶ Help

### Switch Connections

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections
<input type="radio"/> CM521	No	30	1
<input checked="" type="radio"/> CM601	No	30	1

Edit Connection
Edit PE/CLAN IPs
Edit H.323 Gatekeeper
Delete Connection
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 5.11**. default values may be accepted for the remaining fields. Click **Apply** to save changes.

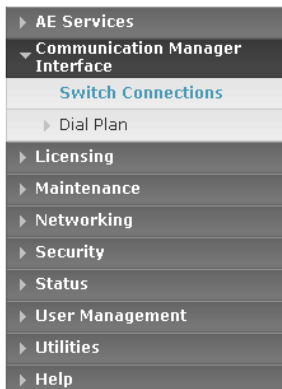


## Application Enablement Services Management Console

Welcome: User craft  
Last login: Thu Dec 15 19:28:13 2011 from 10.10.16.62  
HostName/IP: devconaes611/10.10.16.29  
Server Offer Type: TURNKEY  
SW Version: r6-1-1-30-0

Communication Manager Interface | Switch Connections

[Home](#) | [Help](#) | [Logout](#)



### Connection Details - CM601

Switch Password	<input type="password"/>
Confirm Switch Password	<input type="password"/>
Msg Period	<input type="text" value="30"/> Minutes (1 - 72)
SSL	<input checked="" type="checkbox"/>
Processor Ethernet	<input type="checkbox"/>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

From the **Switch Connections** screen, select the radio button for the recently added switch connection and select the **Edit CLAN IPs** button (not shown). In the resulting screen, enter the IP address of the CLAN that will be used for the AES connection and select the **Add Name or IP** button.

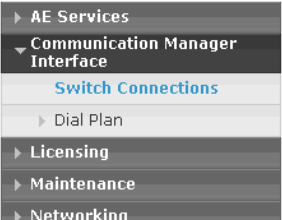


## Application Enablement Services Management Console

Welcome: User craft  
Last login: Thu Dec 15 19:28:13 2011 from 10.10.16.62  
HostName/IP: devconaes611/10.10.16.29  
Server Offer Type: TURNKEY  
SW Version: r6-1-1-30-0

Communication Manager Interface | Switch Connections

[Home](#) | [Help](#) | [Logout](#)




### Edit CLAN IPs - CM

<input type="text" value="10.10.16.31"/>	<input type="button" value="Add Name or IP"/>
Name or IP Address	
	Status
<input type="button" value="Delete IP"/> <input type="button" value="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.

**Application Enablement Services**  
Management Console

Welcome: User craft  
Last login: Thu Dec 15 19:28:13 2011 from 10.10.16.62  
HostName/IP: devconaes611/10.10.16.29  
Server Offer Type: TURNKEY  
SW Version: r6-1-1-30-0

AE Services | TSAPI | TSAPI LinkHome | Help | Logout

▼ AE Services

▶ CVLAN

▶ DLG

▶ DMCC

▶ SMS

▼ TSAPI

▪ TSAPI Links

▪ TSAPI Properties

▶ Communication Manager Interface


TSAPI Links

Link	Switch Connection	Switch CTI Link #	ASAI Link Version	Security
<b>Add Link</b>	<b>Edit Link</b>	<b>Delete Link</b>		

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 **CM**, 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 5.12** which is 1.
- **ASAI Link Version:** This can be left at the default value of 4.
- **Security:** This can be left at the default value of **Unencrypted**.

Once completed, select **Apply Changes**.

**Application Enablement Services**  
Management Console

Welcome: User craft  
Last login: Thu Dec 15 19:28:13 2011 from 10.10.16.62  
HostName/IP: devconaes611/10.10.16.29  
Server Offer Type: TURNKEY  
SW Version: r6-1-1-30-0

AE Services | TSAPI | TSAPI LinkHome | Help | Logout

▼ AE Services

▶ CVLAN

▶ DLG

▶ DMCC

▶ SMS

▼ TSAPI

▪ TSAPI Links

▪ TSAPI Properties

▶ Communication Manager Interface

▶ Licensing

Add TSAPI Links

Link

1

Switch Connection

CM601

Switch CTI Link Number

1

ASAI Link Version

4


Security

Unencrypted

**Apply Changes**

Cancel Changes

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



**Application Enablement Services**  
Management Console

Welcome: User craft  
Last login: Thu Dec 15 19:28:13 2011 from 10.10.16.62  
HostName/IP: devconaes611/10.10.16.29  
Server Offer Type: TURNKEY  
SW Version: r6-1-1-30-0

AE Services | TSAPI | TSAPI Link
Home | Help | Logout


▼ AE Services

- ▶ CVLAN
- ▶ DLG
- ▶ DMCC
- ▶ SMS
- ▼ TSAPI
  - TSAPI Links
  - TSAPI Properties
- ▶ Communication Manager Interface

### 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.

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



**Application Enablement Services**  
Management Console

Welcome: User craft  
Last login: Thu Dec 15 19:28:13 2011 from 10.10.16.62  
HostName/IP: devconaes611/10.10.16.29  
Server Offer Type: TURNKEY  
SW Version: r6-1-1-30-0

AE Services | TSAPI | TSAPI Link
Home | Help | Logout


▼ AE Services

- ▶ CVLAN
- ▶ DLG
- ▶ DMCC
- ▶ SMS
- ▼ TSAPI
  - TSAPI Links

### TSAPI Links

Link	Switch Connection	Switch CTI Link #	ASAI Link Version	Security
1	CM601	1	4	Unencrypted

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**.



**Application Enablement Services**  
Management Console

Welcome: User craft  
Last login: Thu Dec 15 19:28:13 2011 from 10.10.16.62  
HostName/IP: devconaes611/10.10.16.29  
Server Offer Type: TURNKEY  
SW Version: r6-1-1-30-0

Maintenance | Service Controller
Home | Help | Logout

- ▶ AE Services
- ▶ Communication Manager Interface
- ▶ Licensing
- ▼ Maintenance
  - Date Time/NTP Server
  - ▶ Security Database
  - Service Controller
  - ▶ Server Data
- ▶ Networking
- ▶ Security
- ▶ Status
- ▶ User Management

### 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](#)

## 6.4 Create Avaya CTI User

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. 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).

**AVAYA** **Application Enablement Services**  
Management Console

Welcome: User craft  
Last login: Thu Dec 15 19:28:13 2011 from 10.10.16.62  
HostName/IP: devconaes611/10.10.16.29  
Server Offer Type: TURNKEY  
SW Version: r6-1-1-30-0

User Management | User Admin | Add User Home | Help | Logout

▶ AE Services

▶ Communication Manager Interface

▶ Licensing

▶ Maintenance

▶ Networking

▶ Security

▶ Status

▼ User Management

▶ Service Admin

▼ User Admin

▪ Add User

▪ Change User Password

▪ List All Users

▪ Modify Default Users

▪ Search Users

▶ Utilities

**Add User**

Fields marked with \* can not be empty.

\* User Id

Presenceco

\* Common Name

presenceco

\* Surname

Presenceco

\* User Password

.....

\* Confirm Password

.....

Admin Note

Avaya Role

None

Business Category

Car License

CM Home

Css Home

CT User

Yes

Department Number

Display Name

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 set up 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.

**AVAYA** **Application Enablement Services**  
Management Console

Welcome: User craft  
Last login: Thu Dec 15 19:28:13 2011 from 10.10.16.62  
HostName/IP: devconaes611/10.10.16.29  
Server Offer Type: TURNKEY  
SW Version: r6-1-1-30-0

Security | Security Database | CTI Users | List All Users

Home | Help | Logout

▶ AE Services

▶ Communication Manager Interface

▶ Licensing

▶ Maintenance

▶ Networking

▼ Security

▶ Account Management

▶ Audit

▶ Certificate Management

Enterprise Directory

▶ Host AA

▶ PAM

▼ Security Database

▪ Control

▣ CTI Users

**Edit CTI User**

User Profile:

User ID

Common Name

Worktop Name

Unrestricted Access

Presenceco  
presenceco  
NONE

Call and Device Control:

Call Origination/Termination and Device Status

None

Call and Device Monitoring:

Device Monitoring

Calls On A Device Monitoring

Call Monitoring

None

None

Routing Control:

Allow Routing on Listed Devices

None

Apply Changes

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**.

**AVAYA** **Application Enablement Services**  
Management Console

Welcome: User craft  
Last login: Thu Dec 15 19:28:13 2011 from 10.10.16.62  
HostName/IP: devconaes611/10.10.16.29  
Server Offer Type: TURNKEY  
SW Version: r6-1-1-30-0

Security | Security Database | Tlinks

Home | Help | Logout

▶ AE Services

▶ Communication Manager Interface

▶ Licensing

▶ Maintenance

▶ Networking

▼ Security

▶ Account Management

▶ Audit

**Tlinks**

Tlink Name

AVAYA#CM521#CSTA#DEVCONAES611

AVAYA#CM601#CSTA#DEVCONAES611

AVAYA#CM601#CSTA-S#DEVCONAES611

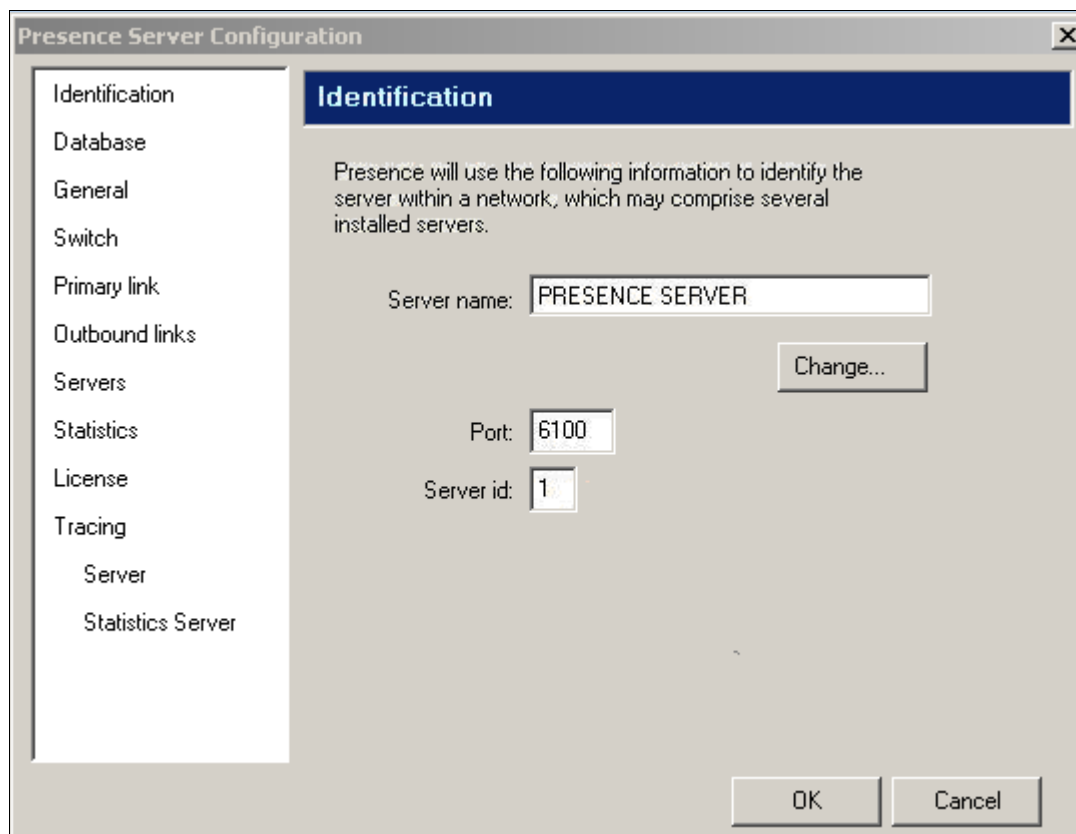
Delete Tlink

## 7 Configure the Presence Suite Server

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. 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. Press **OK** to continue.



The screenshot shows the 'Presence Server Configuration' dialog box with the 'Identification' tab selected. The left sidebar lists various configuration categories: Identification, Database, General, Switch, Primary link, Outbound links, Servers, Statistics, License, Tracing, Server, and Statistics Server. The main area of the dialog is titled 'Identification' and contains the following text: 'Presence will use the following information to identify the server within a network, which may comprise several installed servers.' Below this text are three input fields: 'Server name' with the value 'PRESENCE SERVER', 'Port' with the value '6100', and 'Server id' with the value '1'. A 'Change...' button is located to the right of the 'Server name' field. At the bottom right of the dialog are 'OK' and 'Cancel' buttons.

Field	Value
Server name	PRESENCE SERVER
Port	6100
Server id	1

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 the 'Presence Server Configuration' dialog box with the 'General' tab selected. The left sidebar contains a menu with the following items: Identification, Database, General (highlighted), Switch, Primary link, Outbound links, Servers, Statistics, License, Tracing, Server, and Statistics Server. The main area of the dialog is titled 'General' and contains two sections: 'Maintenance configuration values' and 'Other'. The 'Maintenance configuration values' section includes four settings, each with a red rectangular highlight around the input field: 'Check for pending outbound calls every' with a value of 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:' with a value of 15; 'Time for reorganizing queues in server. This is a critical process which may affect the server performance:' with a value of 03:00; and 'Keep server events from last' with a value of 15 days. The 'Other' section includes one setting with a red rectangular highlight: 'Length of area codes:' with a value of 6 digits. At the bottom right of the dialog are 'OK' and 'Cancel' buttons.

Section	Configuration Item	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

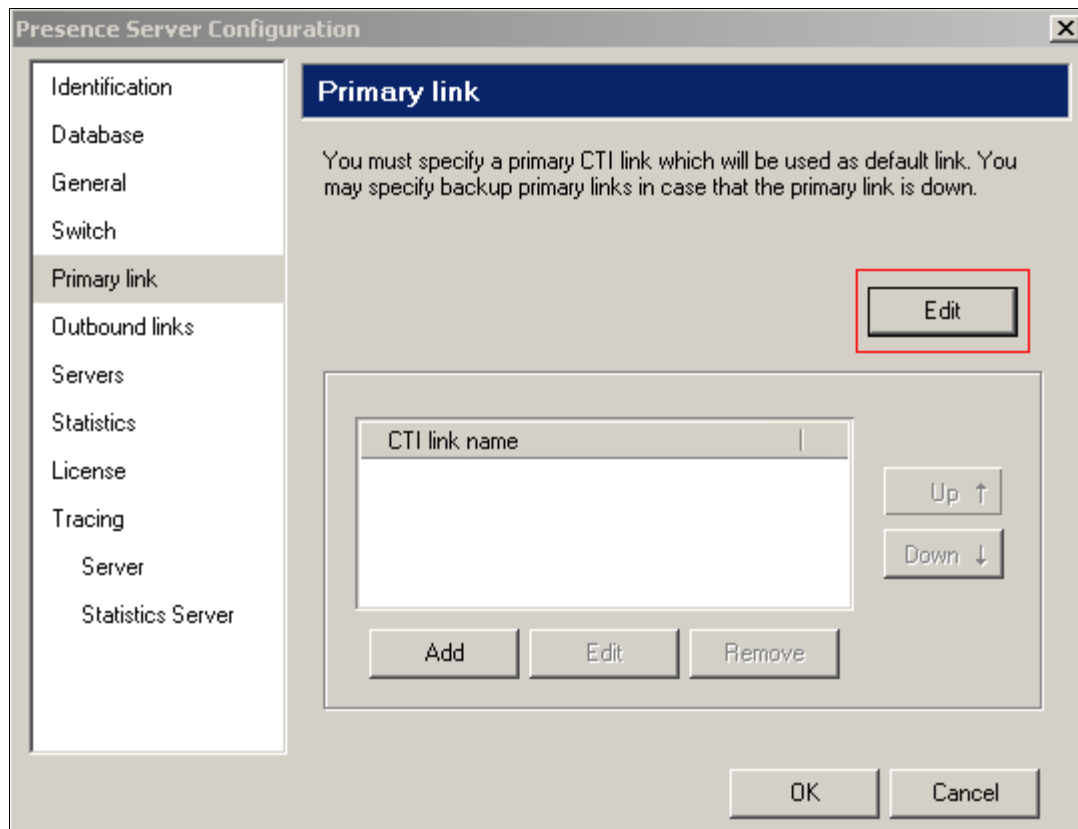
Select the **Switch** option from the menu on the left side of the screen. If required, enter a value in the **Prefix for outgoing calls** field, in this example the ARS feature access code of **9** was used. The **System login to be assigned to contacts not handled by an agent (CTI login)** field should 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 screenshot shows the 'Presence Server Configuration' dialog box with the 'Switch' tab selected. The left sidebar contains a list of configuration categories: Identification, Database, General, Switch (highlighted), Primary link, Outbound links, Servers, Statistics, License, Alarms, Tracing, Server, and Statistics Server. The main area of the dialog is titled 'Switch' and contains the following fields and options:

- Switch configuration values:**
  - Prefix for outgoing calls:** A text box containing the value '9'.
  - System login to be assigned to contacts not handled by an agent (CTI login):** A text box containing the value '99999'.
- ☒ **Specify phantom extensions for preview mode:**
- To specify phantom extensions, you can enter extension ranges in the form (Range1-Range2). Use a semicolon to separate ranges.**
- Phantom extensions:** A text box containing the value '1500-1502', which is highlighted with a red rectangle.

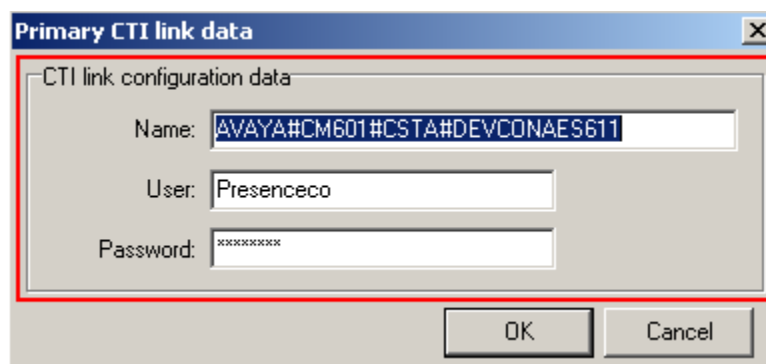
At the bottom right of the dialog are 'OK' and 'Cancel' buttons.

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



The image shows the 'Presence Server Configuration' dialog box. On the left is a vertical menu with options: Identification, Database, General, Switch, Primary link (highlighted), Outbound links, Servers, Statistics, License, Tracing, Server, 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 text is a list box labeled 'CTI link name' which is currently empty. To the right of the list box are 'Up ↑' and 'Down ↓' buttons. Below the list box are 'Add', 'Edit', and 'Remove' buttons. The 'Edit' button is highlighted with a red rectangle. At the bottom right of the dialog 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 the 'Primary CTI link data' dialog box. It has a title bar and a close button. The main area is titled 'CTI link configuration data' and contains three fields: 'Name:' with the value 'AVAYA#CM601#CSTA#DEVCONAES611', 'User:' with the value 'Presenceco', and 'Password:' with a masked value 'xxxxxxxx'. The entire configuration area is highlighted with a red rectangle. At the bottom right are 'OK' and 'Cancel' buttons.

## 7.2 Campaign 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.

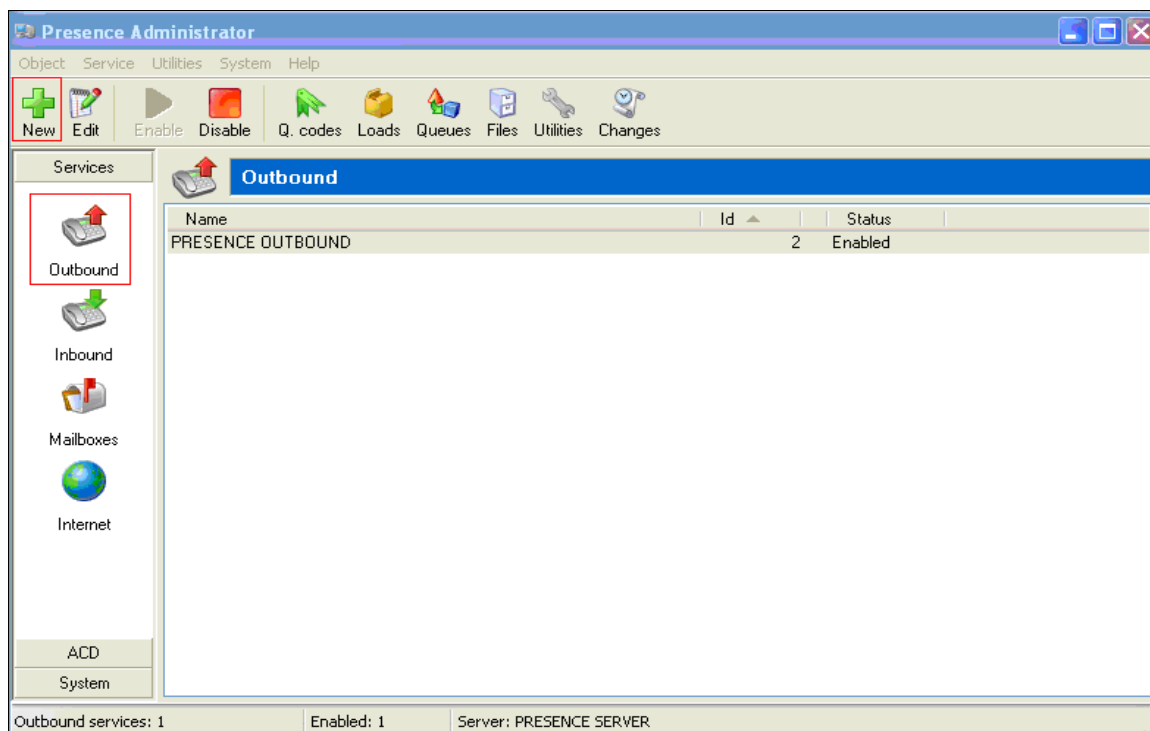
### 7.2.1 Logging in to Presence Administrator

Launch the Presence Administrator application by double clicking the **pcoadmin.exe** located in the Presence folder. The username and password that appear in the **User** and **Password** fields are created during the Presence Server installation.



### 7.2.2 Outbound Campaign

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 campaign.



In the resulting screen, select general from the menu on the left hand side and enter a **Name** for the outbound campaign. In the **Calling hours** field set the time range for which the outbound Campaign will be active. All other fields are left with their default values.

**Outbound service**

**General**

Id: 2

Name: OUTBOUND SERVICE

Resource profile: General

Stop reasons: [All]

Scheduled calling hours

Calling hours: 08:00-22:00

☐ Limit date: 30/12/2011

Outbound calling hours: 08:00-22:00

OK Cancel

Select **Outbound Type** from the left hand side menu and moving to the right, select the **Type** of outbound campaign, this specifies the mode in which the outbound campaign will operate, for further details of the type of outbound campaign available please refer to documentation in **Section 10**. In the **Extension/Skill** field enter the extension number assigned to the outbound hunt group configured in **Section 5.5.1**. In the **VDN/CDN** field enter the VDN number assigned to Outbound calls configured in **Section 5.5.3**. 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.

**Outbound service**

**Outbound type**

Type: Progressive

ACD Items

Extension/Skill: 4094

VDN/CDN: 1805

CTI link: <<Primary CTI link>>

☒ Use primary CTI link in case that CTI link is not connected

☐ Maximum number of concurrent service calls:

☐ Check agent availability

☐ Minimum number/percentage of available agents:

OK Cancel

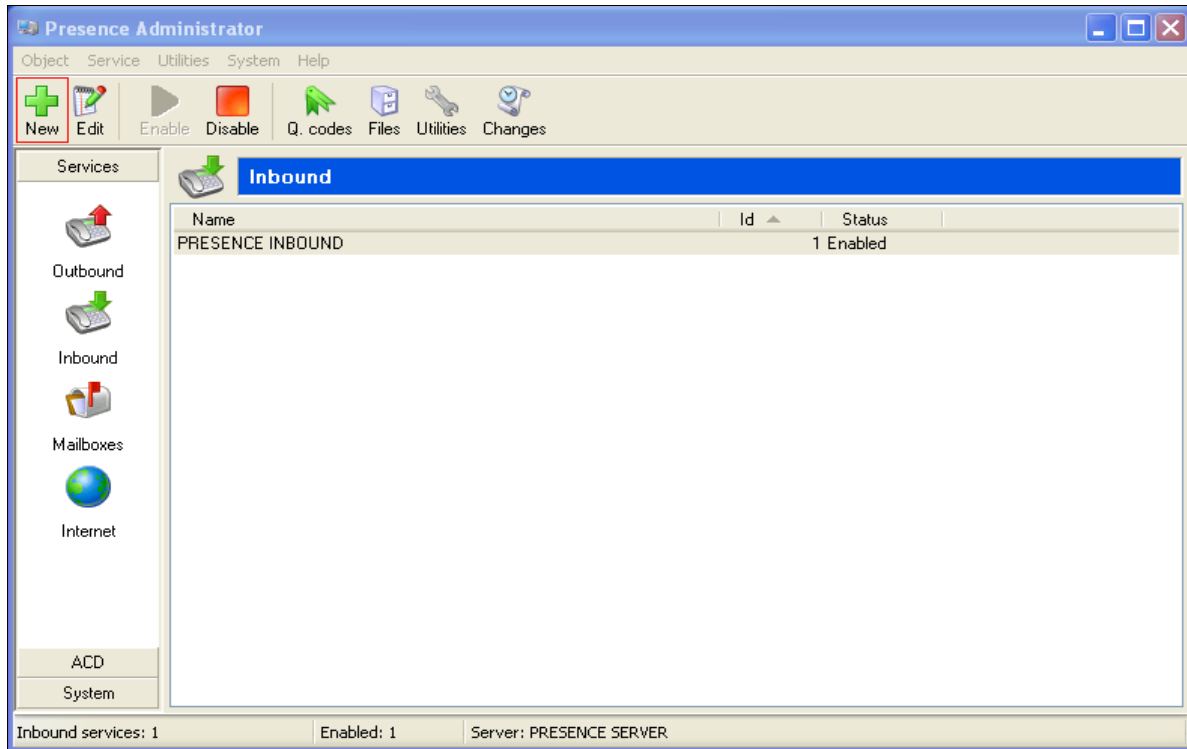
Select **Schedule** from the left hand side menu. The fields in the right hand side define how the outbound campaign should behave following an unsuccessful attempt at contacting the customer. For testing, the **Answering machine** and **Fax** box was checked with default values accepted for all other fields, as shown in the screen below. Click **OK** to complete the outbound campaign configuration.

The screenshot shows the 'Outbound service' dialog box with the 'Schedule' tab selected. The left-hand menu lists various configuration options, with 'Schedule' highlighted. The main area contains two sections: 'Scheduling intervals' and 'Scheduled records'. In the 'Scheduling intervals' section, the 'Answering machine' and 'Fax' fields are highlighted with a red rectangular box. The 'Answering machine' field is set to 0 days, 2 hours, and 0 minutes. The 'Fax' field is set to 60 minutes. Other fields in this section include 'Busy signal' (20 min), 'No answer' (120 min), 'Invalid generic reason' (120 min), 'Phone number does not exist' (0 min), and 'Abandoned call' (0 days, 6 hours, 0 min). The 'Scheduled records' section includes 'Scheduled record expiration' (60 min), 'Maximum consecutive retries for scheduled records' (2), 'Default schedule' (0 days, 0 hours, 0 min), and a checked checkbox for 'Allow the agent to edit the phone number when scheduling record'. At the bottom right are 'OK' and 'Cancel' buttons.

Field	Value	Unit
Busy signal	20	min
No answer	120	min
Answering machine	0 days, 2 hours, 0 min	
Fax	60	min
Invalid generic reason	120	min
Phone number does not exist	0	min
Abandoned call	0 days, 6 hours, 0 min	
Scheduled record expiration	60	min
Maximum consecutive retries for scheduled records	2	
Default schedule	0 days, 0 hours, 0 min	

### 7.2.3 Inbound Campaign

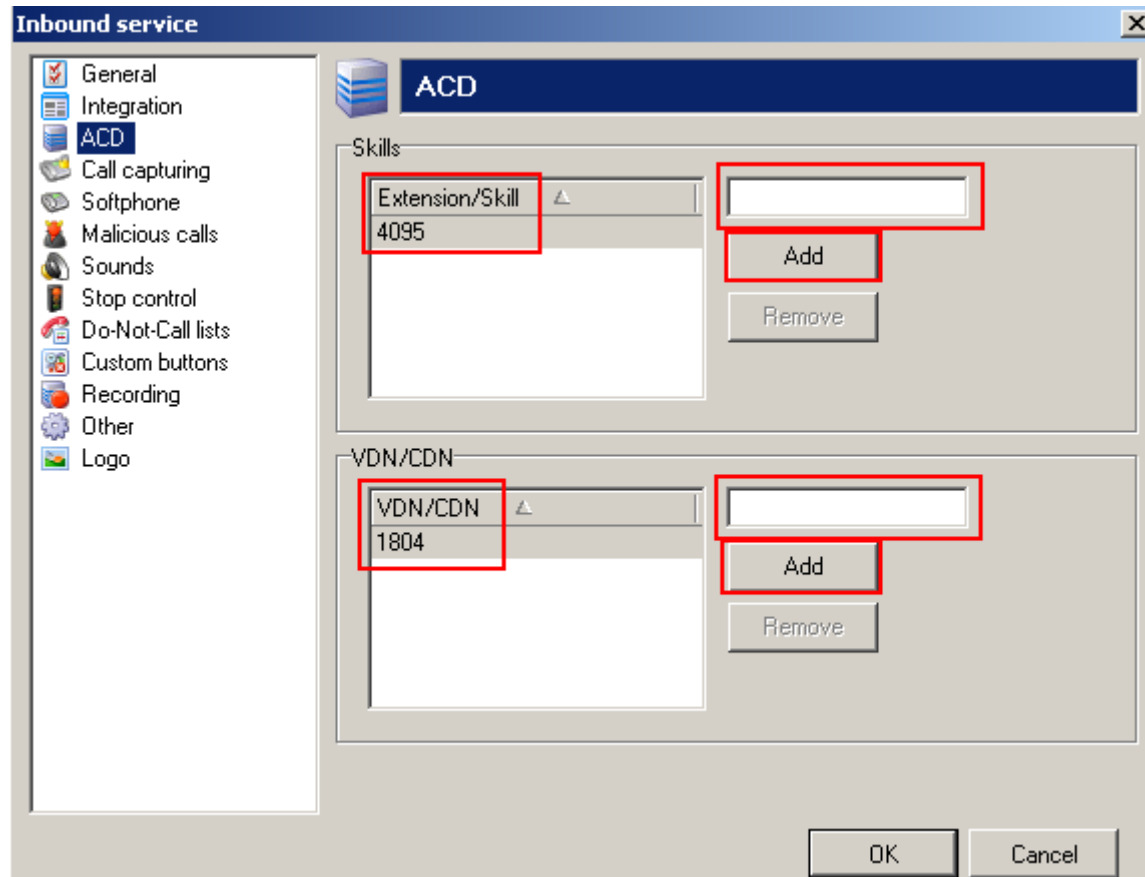
To configure an inbound campaign, from the left hand side select **Services** → **Inbound** from the Presence Administrator main menu. Click the **New** button.



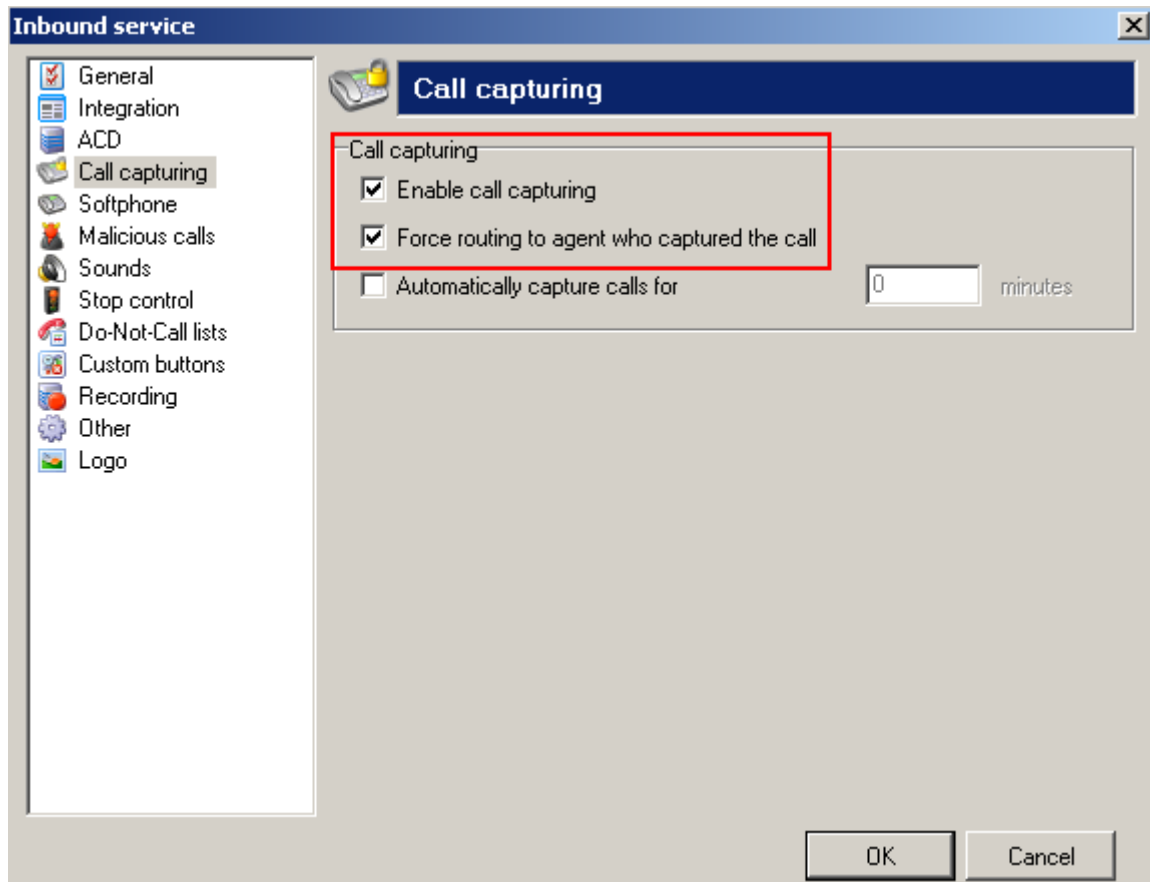
In the resulting screen, select **General** from the menu on the left hand side and enter a **Name** for the inbound campaign. All other fields are left with their default values.

The screenshot shows a software window titled "Inbound service". On the left is a vertical menu with icons and labels: General (checked), Integration, ACD, Call capturing, Softphone, Malicious calls, Sounds, Stop control, Do-Not-Call lists, Custom buttons, Recording, Other, and Logo. The main area of the window has a sub-header "General" with a checked icon. Below this, there are four input fields: "Id:" with the value "1", "Name:" with the value "INBOUND SERVICE" (this field is highlighted with a red border), "Resource profile:" with a dropdown menu showing "General", and "Stop reasons:" with a dropdown menu showing "[All]". At the bottom right of the window are two buttons: "OK" and "Cancel".

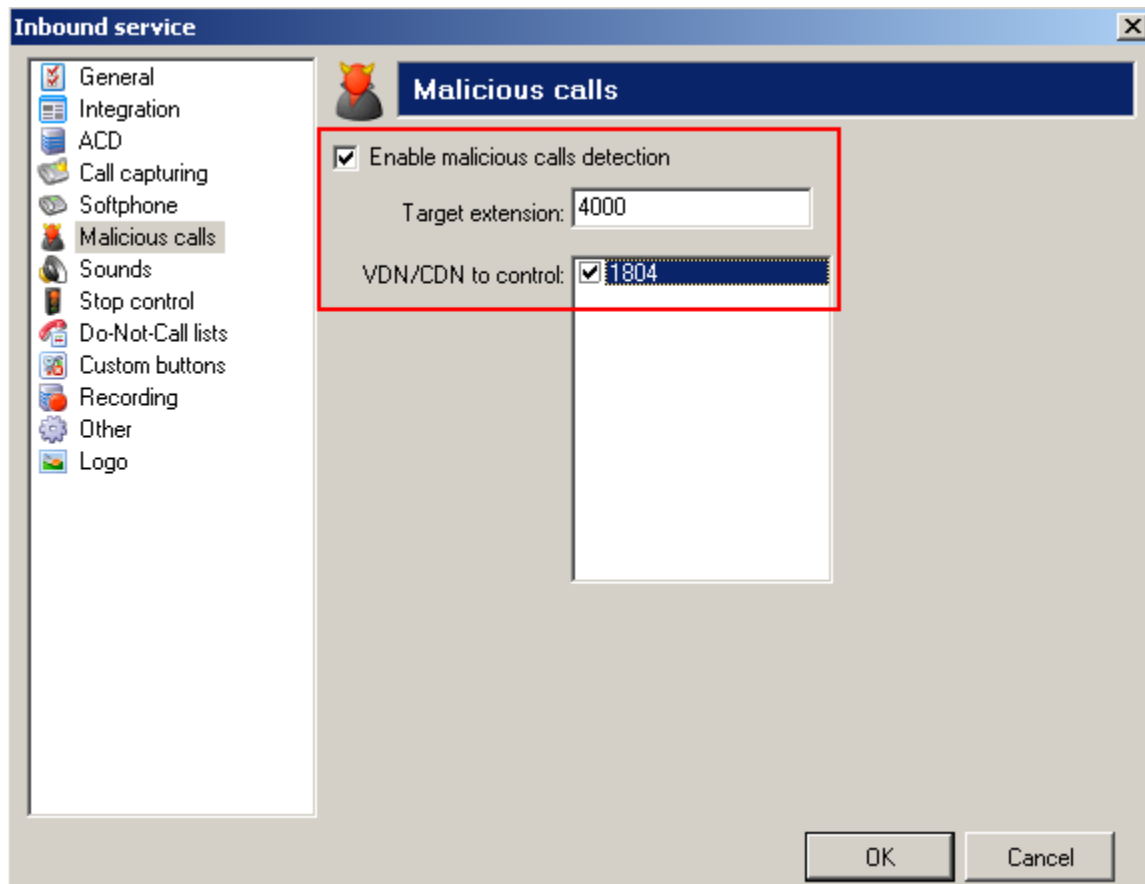
Select **ACD** from the left hand side menu and moving to the right, under the heading **Skills** enter the skill group extensions configured in **Section 5.5.1** that will handle inbound calls in the untitled box (this includes email and web chat call types) and click **Add**. The skill group extensions will then appear to the left in the **Extension/Skill** box. Under the heading **VDN/CDN** enter the VDN configured in **Section 5.5.3** that will handle inbound calls in the untitled box and click **Add**. The VDN will then appear to the left in the **VDN/CDN** box.



Select **Call capturing** from the left hand side menu and moving to the right, select the **Enable call capturing** and **Force routing to agent who captured the call** check box's. These options allow an agent to mark an inbound call so that if the caller rings back while that agent is logged on 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/CDN to control** field select the VDNs this option will be available on.

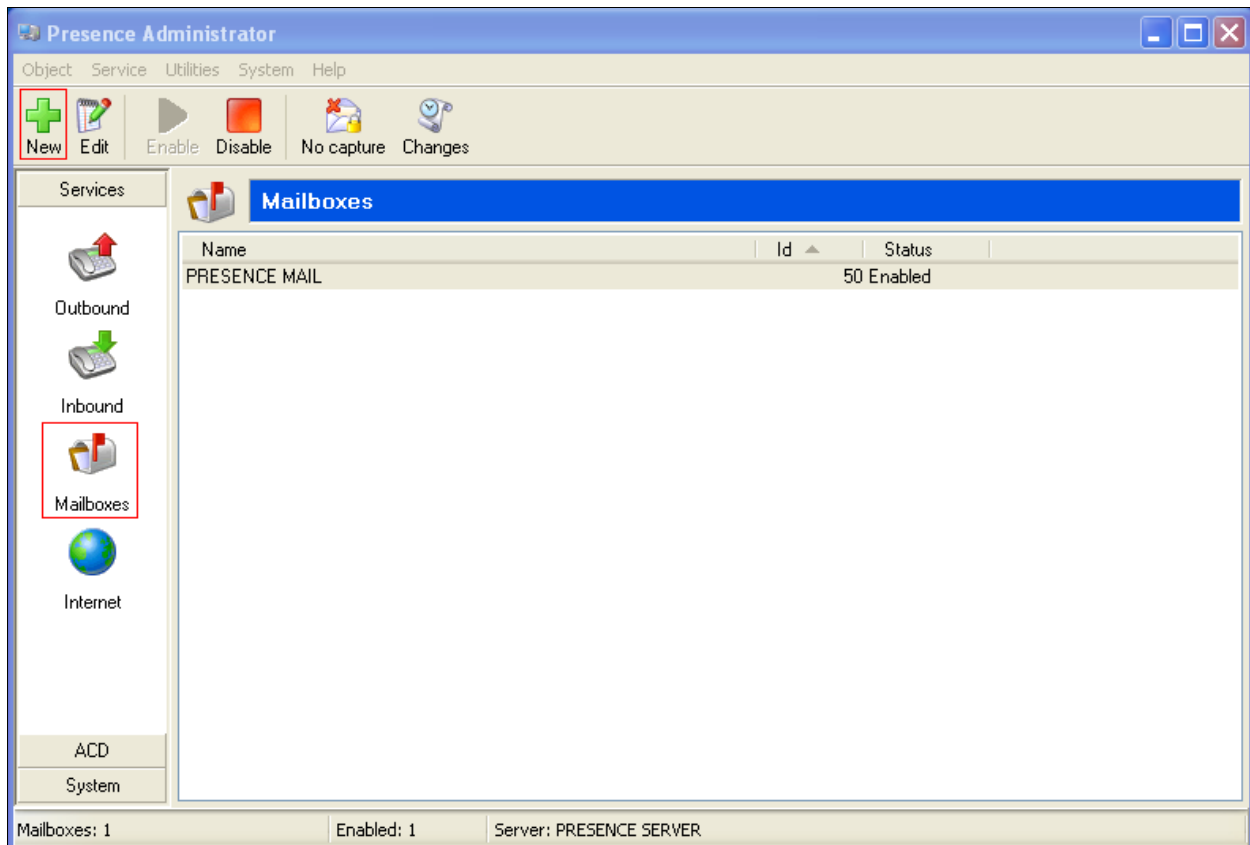


Select **Other** from the left hand side menu and moving to the right, select the **Enable direct transfer to agents of this service** check box. Enter the direct agent transfer VDN assigned in **Section 5.5.3** in the **Use the following VDN/CDN for transfer** field. Click **OK** to complete the inbound campaign configuration.

The screenshot shows the 'Inbound service' configuration window with the 'Other' tab selected. The left sidebar lists various configuration options: General, Integration, ACD, Call capturing, Softphone, Malicious calls, Sounds, Stop control, Do-Not-Call lists, Custom buttons, Recording, Other (selected), and Logo. The main area is divided into sections: 'After-call work' with checkboxes for minimum and maximum after-call work time, a dropdown for 'Q. code for maximum time', and a checkbox for 'Use q. code only if contact has not yet been qualified'; 'Transfer to agents' which is highlighted with a red box, containing a checked checkbox for 'Enable direct transfer to agents of this service' and a dropdown for 'Use the following VDN/CDN for transfer' set to '1804'; and 'Outgoing calls identification' with a checkbox for 'Enable outgoing calls identification' and a 'Phone no.' field. 'OK' and 'Cancel' buttons are at the bottom right.

## 7.2.4 Email Campaign

To configure an email campaign, 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 campaign. Referring to **Table 2, Section 5.5**, under the heading **VDN/CDN** in the **General** field enter the VDN assigned for email and enter the VDN assigned for suspended emails in the **Suspended** field.

The image shows a 'Mailboxes' dialog box with a sidebar on the left containing icons and labels for 'General', 'Incoming mail', 'Outgoing mail', 'Mail movement', and 'Other'. The 'General' option is selected. The main area is titled 'General' and contains the following fields:

- Id:** 50
- Name:** PRESENCE MAIL (highlighted with a red box)
- Resource profile:** General (dropdown menu)
- Priority:** Medium (dropdown menu)
- VDN/CDN** section (highlighted with a red box):
  - General:** 1803
  - Suspended:** 1804
- ☐ Maximum number of concurrent e-mails: 0

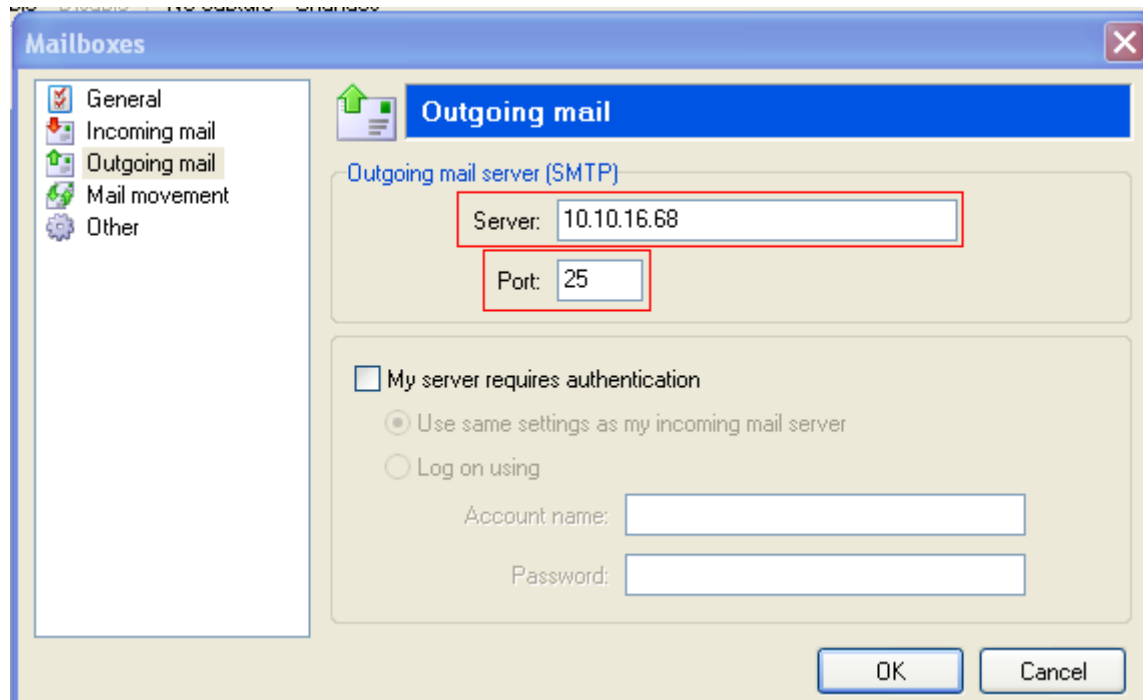
At the bottom right are 'OK' and 'Cancel' buttons.

Select **Incoming mail** from the left hand side menu. This window allows you 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 default 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 four items: "General" (checked), "Incoming mail" (selected), "Outgoing mail", "Mail movement", and "Other". The main area is titled "Incoming mail" and contains two sections. The "Incoming mail server (POP3)" section has a "Server:" field with the value "10.10.16.68" and a "Port:" field with the value "110". The "Incoming mail account" section has three fields: "Account name:" with the value "support", "Password:" with the value "xxxxxxx", and "E-mail address:" with the value "support@test.com". At the bottom right are "OK" and "Cancel" buttons.

Field	Value
Server	10.10.16.68
Port	110
Account name	support
Password	xxxxxxx
E-mail address	support@test.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 default SMTP port of **25** is entered into the **Port** field. Click **OK** to complete the email campaign configuration.



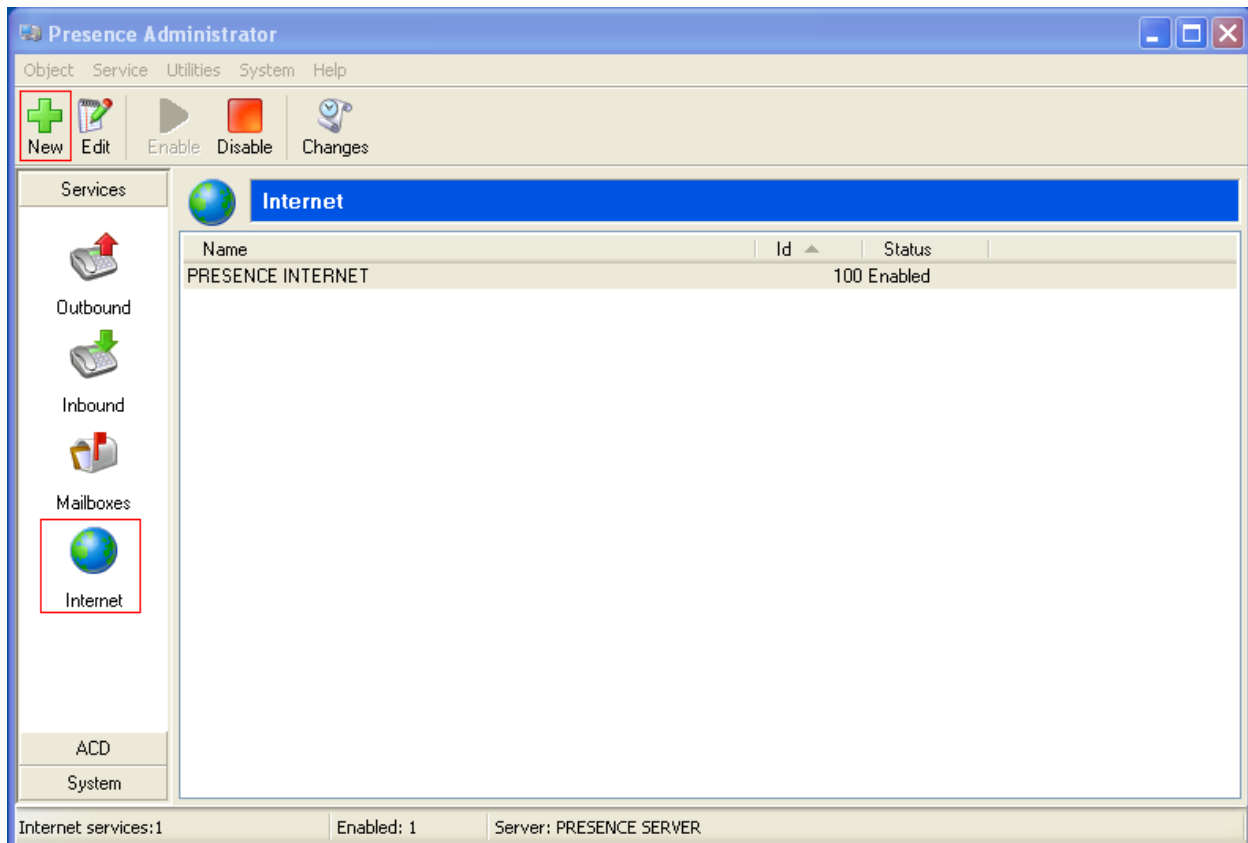
The image shows a 'Mailboxes' configuration window. On the left is a sidebar with a tree view containing: 'General' (checked), 'Incoming mail', 'Outgoing mail' (selected), 'Mail movement', and 'Other'. The main area is titled 'Outgoing mail' and contains the following fields and options:

- Outgoing mail server (SMTP)**
  - Server:** 10.10.16.68
  - Port:** 25
- ☐ **My server requires authentication**
  - ☒ Use same settings as my incoming mail server
  - ☐ Log on using
    - Account name:** [text box]
    - Password:** [text box]

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

## 7.2.5 Web Chat / Web Call Back

To configure a web campaign, 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 campaign. Under the **URL** heading three campaigns are defined:

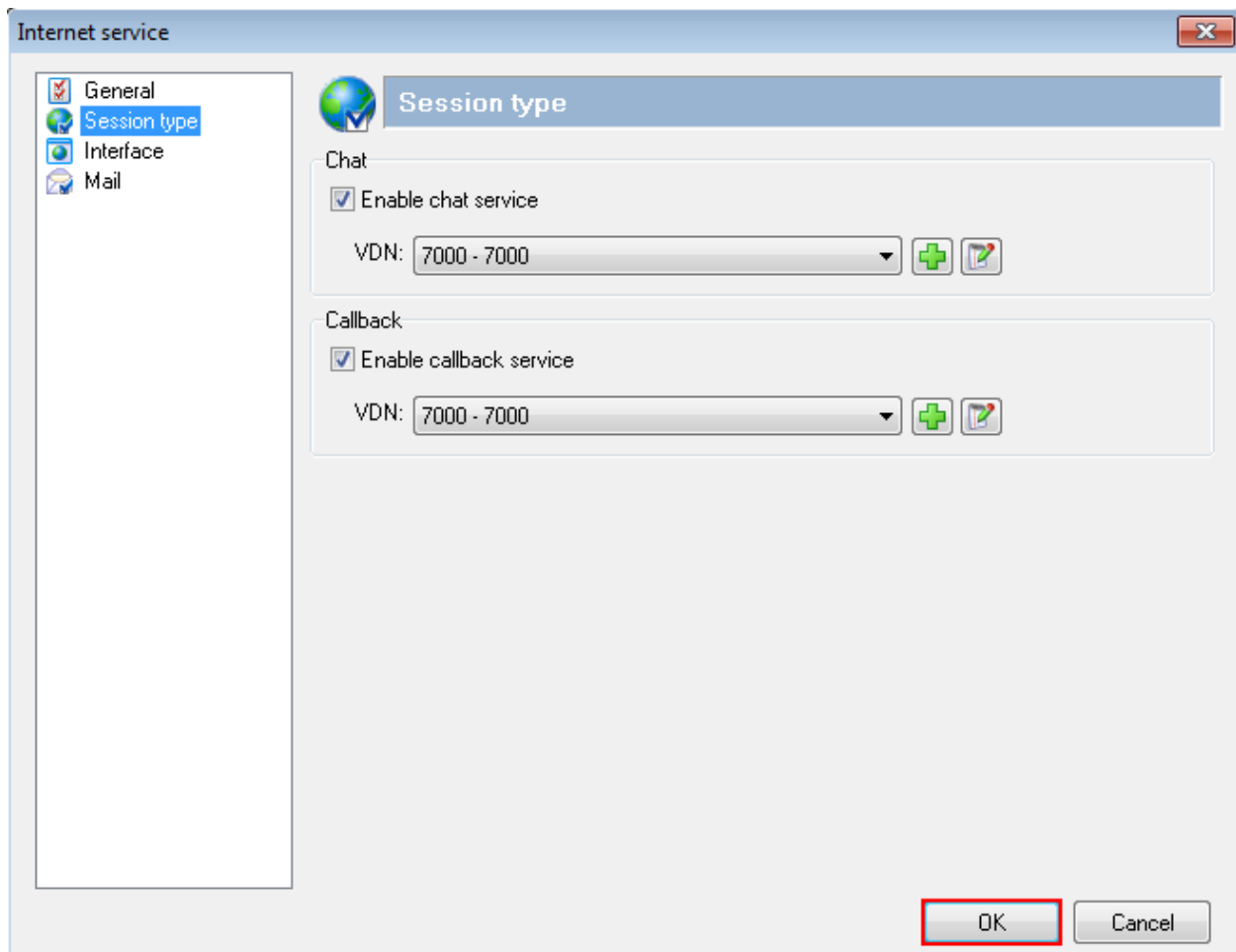
- The **Waiting** URL is the URL that is presented to the customer if no agents are available.
- The **Goodbye** URL is the URL that is presented to the customer when the web callback or web chat session ends.
- The **Service disabled** URL is the URL that is presented to the customer if the service has been disabled for any reason.

The screenshot shows a window titled "Internet service" with a close button in the top right corner. On the left is a vertical menu with four items: "General" (selected with a checkmark icon), "Session type", "Interface", and "Mail". The main area is titled "General" and contains the following fields:

- Id:** 7777
- Name:** PRESENCE INTERNET (This field is highlighted with a red rectangle)
- URL:** (This section is enclosed in a light gray box and contains three sub-fields: "Linker:", "Waiting:", and "Goodbye:", each followed by an empty text input field.)
- ☐ Show in the same window
- Service disabled:** (followed by an empty text input field)
- Custom content:** (followed by an empty text input field)
- Customer template:** (followed by an empty text input field)

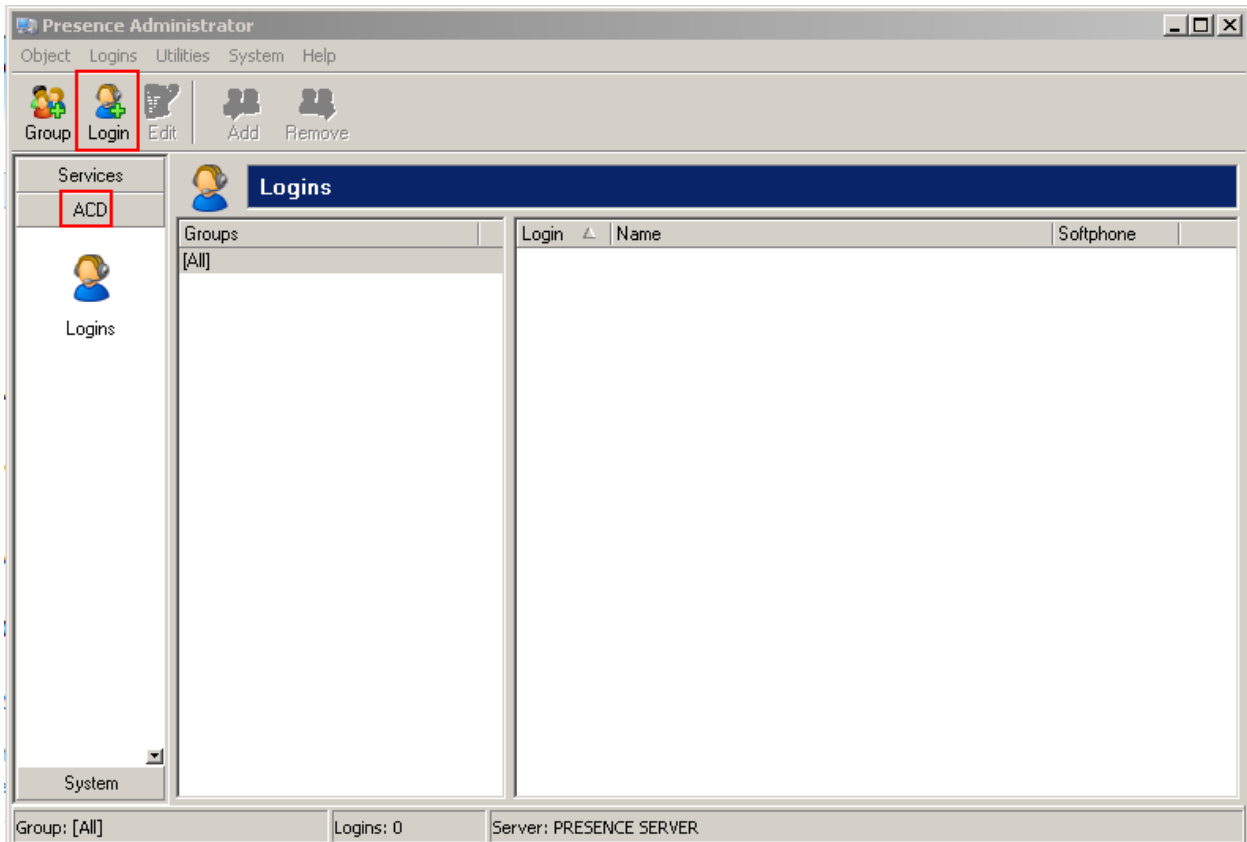
At the bottom right of the window are "OK" and "Cancel" buttons.

Select **Session type** in the left hand pane, the **Chat service** and **Callback service** check boxes should be selected and the relevant VDN for each entered into the **VDN/CDN** field, click **OK** when done.



## 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 5.7**.

The screenshot shows the 'Insert logins' dialog box with the 'General' tab selected. The left pane shows 'General', 'Groups', 'Softphone', and 'Other'. The 'General' tab is active, and the 'Logins' field contains '201'. The 'Password' and 'Confirm password' fields are masked with 'xxxxxxx'. The 'Use as ACD password' checkbox is unchecked. Below these fields are three unchecked checkboxes: 'Change password at next login', 'Synchronize the 'Available' status of the agent', and 'Store outgoing calls of agent'. The 'OK' and 'Cancel' buttons are at the bottom right.

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 'Insert logins' dialog box with the 'Softphone' tab selected. The left pane shows 'General', 'Groups', 'Softphone', and 'Other'. The 'Softphone' tab is active, and the 'Softphone always enabled' checkbox is checked. Below this is a 'Phone book' section with an empty list and 'Add' and 'Remove' buttons. At the bottom, there is an unchecked checkbox for 'Enable manual outbound ACD calls' and 'OK' and 'Cancel' buttons.

### 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 (dbexpoda.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 **10.10.16.68**. 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 the **Hang up calls before logging in** check box. In the field **Use configuration for** choose **Machine** from the drop down menu. Click **OK**. This step is needed for each agent configured; only the agent station field will vary.

The screenshot shows the 'Presence Agent Configuration' dialog box with the 'General' tab selected. The dialog has a sidebar on the left with options: 'General', 'Backup servers', 'Advanced', and 'Tracing'. The main area contains the following fields and controls:

- Presence Server** section:
  - IP address: 10.10.16.68
  - Port: 6100
- Station configuration** section:
  - Agent station: 4001
  - ☒ Hang up calls before logging in
  - ☐ Ask agent station at login window
- Use configuration for:** Machine (selected in the dropdown menu)

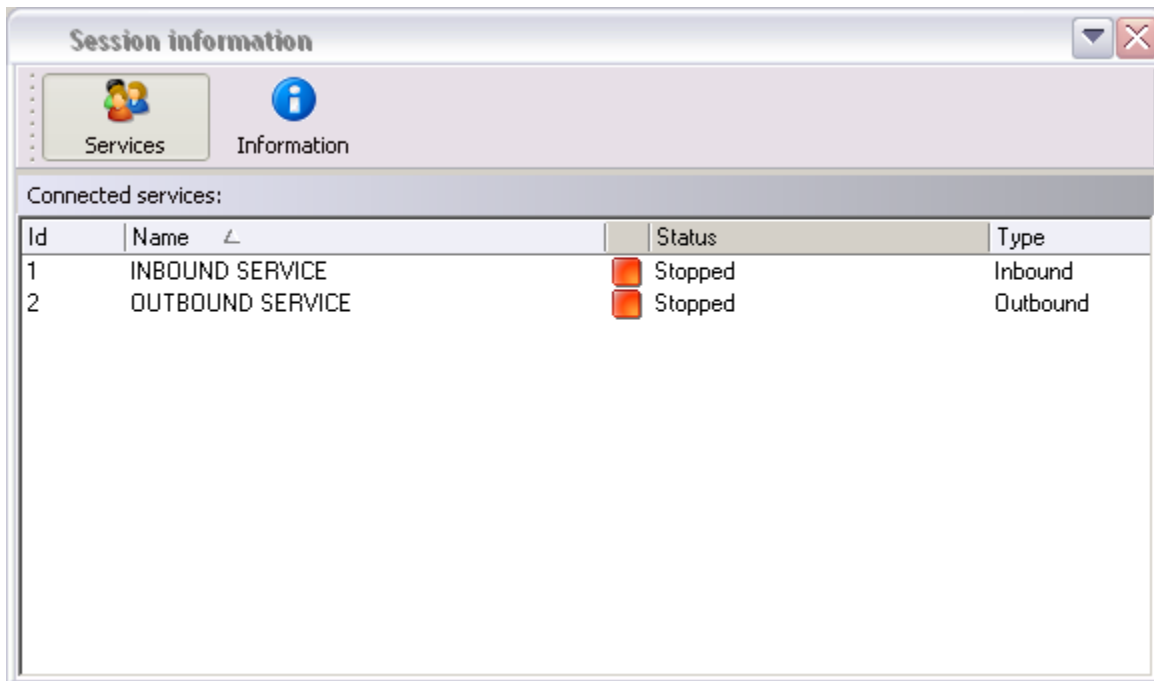
At the bottom right are 'OK' and 'Cancel' buttons. Three red rectangular boxes highlight the 'Presence Server' section, the 'Station configuration' section, and the 'Use configuration for' dropdown menu.

### 7.3.1 Logging in Presence Agent

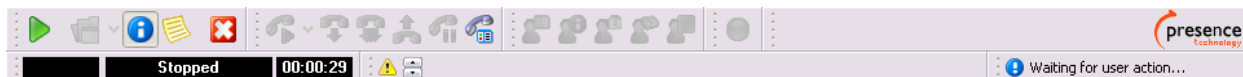
Launch the Presence agent configuration application by double clicking the **pcoagent.exe** located in the Presence folder. Enter the agent **Login** and **Password** configured in **Section 5.7** and click on **OK**.



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



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.



## 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 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	4	no	devconaes611	established	87	61

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

```
status aesvcs interface
```

AE SERVICES INTERFACE STATUS			
Local Node	Enabled?	Number of Connections	Status
clancm601	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	devconaes611	10.10.16.29	45883	clancm601	683	665

## 8.2 Verify Avaya Aura® Application Enablement Services CTI Connection

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

### 8.2.1 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**.



#### Application Enablement Services Management Console

Welcome: User craft  
Last login: Thu Dec 15 19:33:46 2011 from 10.10.16.62  
HostName/IP: devconaes611/10.10.16.29  
Server Offer Type: TURNKEY  
SW Version: r6-1-1-30-0

Status | Status and Control | TSAPI Service Summary

Home | Help | Logout

▶ AE Services
▶ Communication Manager Interface
▶ Licensing
▶ Maintenance
▶ Networking
▶ Security
▼ Status
Alarm Viewer
▶ Logs
▼ Status and Control
▪ CVLAN Service Summary
▪ DLG Services Summary
▪ DMCC Service Summary
▪ Switch Conn Summary
▪ <b>TSAPI Service Summary</b>

#### TSAPI Link Details

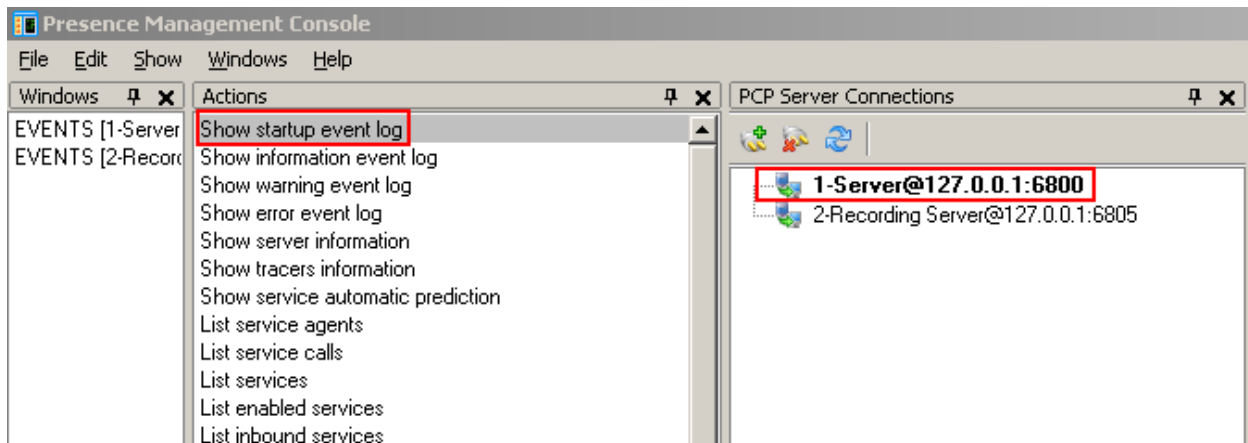
☐ Enable page refresh every  seconds

	Link	Switch Name	Switch CTI Link ID	Status	Since	State	Switch Version	Associations	Msgs to Switch	Msgs from Switch	Msgs Period
<input type="radio"/>	1	CM521	1	Talking	Wed Dec 14 16:03:39 2011	Online	15	0	15	15	30
<input checked="" type="radio"/>	2	CM601	1	Talking	Wed Dec 14 16:10:07 2011	Online	16	8	71	87	30

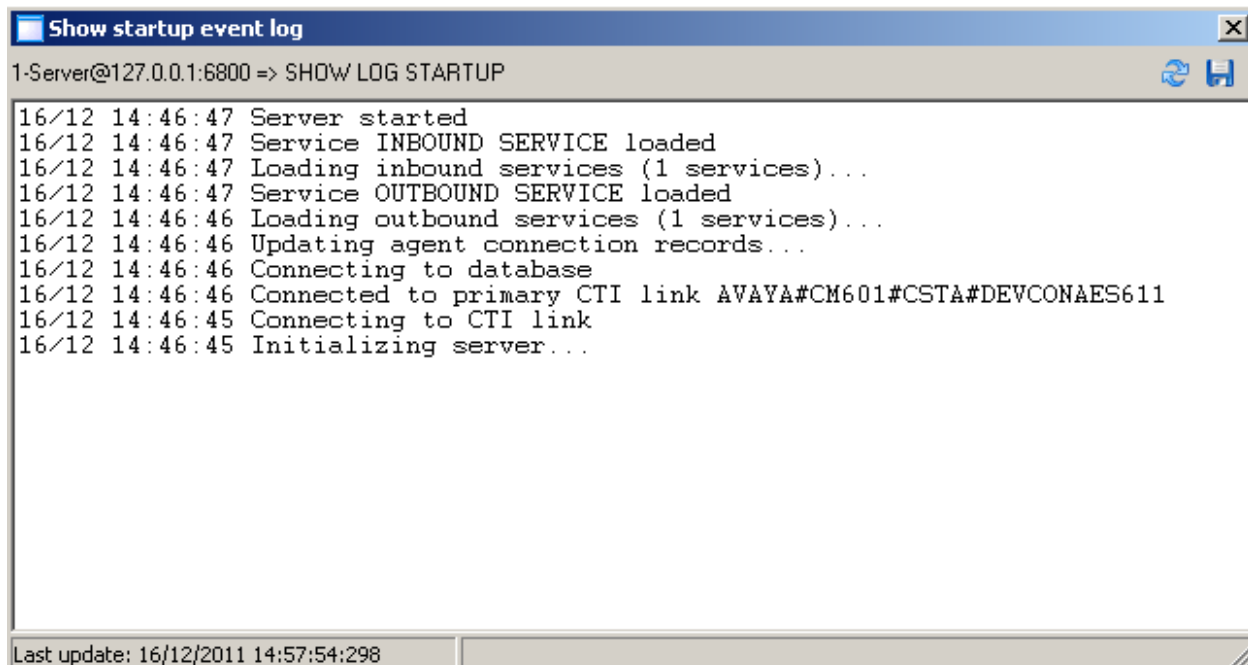
For service-wide information, choose one of the following:

### 8.3 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**. A startup log commences when the Presence Server is trying to load and connect to the Application Enablement Services. Click on the item named **Server@127.0.0.1:6800** 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.



Verify successful CTI connection and service startup.



## 9 Conclusion

These Application Notes describe the configuration steps required for Presence Suite 9 to successfully interoperate with Avaya Aura® Communication Manager R6.0.1 using Avaya Aura® Application Enablement Services R6.1.1. 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>. The following documentation is available on request from Presence:  
[www.presenceco.com](http://www.presenceco.com)

1. Presence Administrator Manual Presence Suite, V9
2. Presence Installation Guides Presence Software, V9
3. PBX/ACD Requirements Presence Software, V9

---

**©2012 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](mailto:devconnect@avaya.com).