



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

---

# **Application Notes for configuring Enghouse Presence Suite R11.1 to interoperate with Avaya Aura® Communication Manager R8.0.1 and Avaya Aura® Application Enablement Services R8.0 – Issue 1.0**

## **Abstract**

These Application Notes describe the configuration steps for Enghouse 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 and call recording 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 and uses single step conferencing implemented via DMCC over TSAPI to record 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.

## Introduction

These Application Notes describe the compliance tested configuration of Enghouse Presence Suite R11.1 to interoperate with Avaya Aura® Communication Manager R8.0.1 using Avaya Aura® Application Enablement Services R8.0. Presence Suite is a multi-channel contact management suite able to handle voice, e-mail, call recording 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. The call recording module uses Avaya Aura® Communication Manager's Single Step Conferencing (SSC) feature via the Device, Media, and Call Control (DMCC) service provided by the Avaya Aura® Application Enablement Services (AES) to capture the audio and call details for recording agent calls.

Device Media Call Control (DMCC) works by allowing software vendors to create soft phones, in memory on a recording server, and use them to monitor and record other phones. This is purely a software solution and does not require telephony boards or any wiring beyond a typical network infrastructure.

Presence Suite consists of a number of modules. The following modules were tested.

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

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.

## General Test Approach and Test Results

Testing included validating the correct operation of typical contact center 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, web chat and call recording 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 Enghouse.

## **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
- Presence Recording

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. Call recording was tested by repeating the inbound and outbound calls specifically for call recording.

## **2.2 Test Results**

All test cases passed successfully.

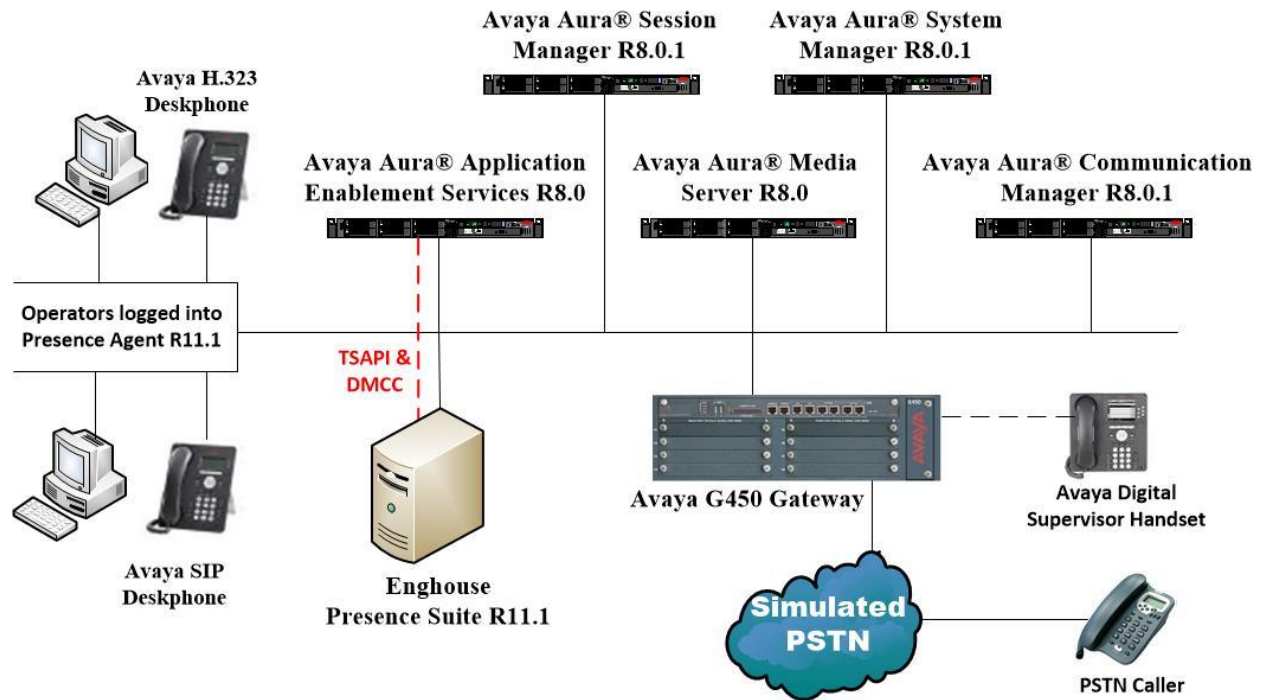
## **2.3 Support**

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

- Email: Presence.Support@enghouse.com
- Website: <https://www.enghouseinteractive.es/en>
- Phone: +34 93 10 10 300

## Reference Configuration

**Figure 1** shows the network topology during interoperability testing. A Communication Manager with an Avaya G450 Media Gateway and Media Server 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 and Presence Recording using DMCC Single Step Conference.



**Figure 1: Avaya Aura® Communication Manager R8.0.1 and Aura® Application Enablement Services R8.0 with Enghouse Presence Suite R11.1 configuration**

## Equipment and Software Validated

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

| Avaya Equipment   | Software / Firmware Version  |
|---|--|
| Avaya Aura® System Manager running on a virtual server                | System Manager 8.0.1.1<br>Build No. – 8.0.0.0.931077<br>Software Update Revision No: 8.0.11.039340<br>Service Pack 1 |
| Avaya Aura® Session Manager running on a virtual server               | Session Manager R8.0.1<br>Build No. – 8.0.1.1.801103   |
| Avaya Aura® Communication Manager running on a virtual server         | R8.0.1.1.0 – FP1SP1<br>R018x.00.0.822.0<br>Update ID 00.0.822.0-25183  |
| Avaya Aura® Application Enablement Services running on Virtual Server | R8.0<br>Build No – 8.0.0.0.0.6-0   |
| Avaya Media Gateway G450  | 41.10.1 /1   |
| Avaya Aura® Media Server  | Appliance Version R8.0.0.6<br>Media Server 8.0.0.150<br>Element Manager 8.0.0.150                                    |
| Avaya 96x1 SIP Deskphone  | 7.1.2.0.14   |
| Avaya J179 H323 Deskphone   | 6.7.002U   |
| Avaya 9408 Digital Deskphone  | V2.0   |
| Enghouse Equipment  | Software / Firmware Version  |
| Enghouse Presence Suite running on Windows Server 2016 Server         | R11.1  |
| Enghouse Presence Client running on Windows 10                        | R11.1  |

## 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
- Configure H323 Stations for Single Step Conference
- Configure SIP Stations for Single Step Conference
- Configure Virtual Stations

### 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 4**, 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 | 4 of 12 |
|---|--|------|---------|
| OPTIONAL FEATURES                               |  |      |         |
| Abbreviated Dialing Enhanced List? y            | Audible Message Waiting? y                 |      |         |
| Access Security Gateway (ASG)? y                | Authorization Codes? y                     |      |         |
| Analog Trunk Incoming Call ID? y                | CAS Branch? n                              |      |         |
| A/D Grp/Sys List Dialing Start at 01? y         | CAS Main? n                                |      |         |
| <b>Answer Supervision by Call Classifier? y</b> | Change COR by FAC? n                       |      |         |
| ARS? y  | <b>Computer Telephony Adjunct Links? 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? y                  | DCS Call Coverage? y                       |      |         |
| ASAI Link Plus Capabilities? y                  | 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 7**, verify the following customer options are set to **y** as shown below.

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

```

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

Call Center Release: 8.0

ACD? y
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 19
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

Abbreviated Dial Programming by Assigned Lists? n
Auto Abbreviated/Delayed Transition Interval (rings): 2
Protocol for Caller ID Analog Terminals: Bellcore
Display Calling Number for Room to Room Caller ID Calls? N

```

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

```
display system-parameters features                                     Page 10 of 19
                                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
                                    Date Format on Terminals: dd/mm/yy
                                    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
```

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
                                    Work Mode On Login: aux

                                VECTORING
                                    Converse First Data Delay: 0          Second Data Delay: 2
                                    Converse Signaling Tone (msec): 100      Pause (msec): 70
                                    Prompting Timeout (secs): 10
                                    Interflow-qpos EWT Threshold: 2
                                    Reverse Star/Pound Digit For Collect Step? n
                                    Available Agent Adjustments for BSR? n
                                    BSR Tie Strategy: 1st-found
                                    Store VDN Name in Station's Local Call Log? n
                                SERVICE OBSERVING
                                    Service Observing: Warning Tone? y      or Conference Tone? n
                                    Allowed with Exclusion: Service Observing? n      SSC? n
                                    Allow Two Observers in Same Call? y
```

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

```
display system-parameters features Page 12 of 19
      FEATURE-RELATED SYSTEM PARAMETERS
AGENT AND CALL SELECTION
      MIA Across Splits or Skills? n
      ACW Agents Considered Idle? y
      AUX Agents Considered Idle (MIA)? n
      AUX Agent Remains in LOA Queue? n
      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

      Agent/Caller Disconnect Tones? n
      Interruptible Aux Notification Timer (sec): 3
      Zip Tone Burst for Callmaster Endpoints: double

ASAI
      Copy ASAI UI During Conference/Transfer? n
      Call Classification After Answer Supervision? y
      Send UCID to ASAI? y
      For ASAI Send DTMF Tone to Call Originator? y
      Send Connect Event to ASAI For Announcement Answer? n
      Prefer H.323 Over SIP For Dual-Reg Station 3PCC Make Call? n
```

## 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.

|                                       |             |
|---------------------------------------|-------------|
| <b>change sit-treatment</b>           | 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                |             |
| <b>Pause Duration (seconds): 0.8</b>  |             |
| <b>Talk Duration (seconds): 3.0</b>   |             |

## 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. Typically a unique VDN and Hunt Group would be setup for each of the following modules which were tested. However for these Application Notes the configuration shows the setup of only the Presence Inbound VDN, Vector and Hunt Group as an example.

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

### 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 Presence Suite 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.

|   |  |
|---|--|
| <b>change cor 1</b>                         | <b>Page 1 of 23</b>                    |
| 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                         | <b>Direct Agent Calling? y</b>         |
| 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.

|   |   |
|---|---|
| <b>add agent-loginID 4405</b>                               | <b>Page 1 of 2</b>                                    |
| AGENT LOGINID   |   |
| Login ID: 4405  | AAS? n  |
| <b>Name:</b> PresenceAgent1                                 | AUDIX? n  |
| TN: 1   | Check skill TNs to match agent TN? n                  |
| <b>COR: 1</b>   |   |
| 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):                               |
|   | <b>Auto Answer: station</b>                           |
| 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 |  | 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 Administer 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              |             |          |  |
|                           |  | Message Lamp Ext: 4000                       |             |          |  |
| Speakerphone: 2-way       |  | Mute Button Enabled? y                       |             |          |  |
| Display Language: english |  | Button Modules: 0                            |             |          |  |
| Survivable GK Node Name:  |  |  |             |          |  |
| Survivable COR: internal  |  | Media Complex Ext:                           |             |          |  |
| Survivable Trunk Dest? y  |  | IP SoftPhone? y                              |             |          |  |
|                           |  | IP Video Softphone? n                        |             |          |  |
|                           |  | Short/Prefixed Registration Allowed: default |             |          |  |
|                           |  | Customizable Labels? y                       |             |          |  |

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: <b>manual-in</b>  | Grp:        |
| 2: call-appr        | 6: <b>after-call</b> | Grp:        |
| 3: call-appr        | 7: <b>release</b>    |             |
| 4: <b>aux-work</b>  | 8::                  |             |
| RC:                 | Grp:                 |             |

**Note:** The same changes should be made on a SIP station. Changes to SIP stations are made using System Manager as shown in **Section 5.12**.

## 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 28800         |                                 | Page 1 of 5 |
|---------------------------|---------------------------------|-------------|
| STATION                   |                                 |             |
| Extension: 28800          | 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           |                                 |             |
| Loss Group: 2             | Time of Day Lock Table:         |             |
| Data Module? n            | Personalized Ringing Pattern: 1 |             |
| Speakerphone: 2-way       | Message Lamp Ext: 4850          |             |
| Display Language: english | Mute Button Enabled? y          |             |
| 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 (**aes80vmpg**).

| display node-names ip |                    | Page 1 of 2 |
|-----------------------|--------------------|-------------|
| IP NODE NAMES         |                    |             |
| Name                  | IP Address         |             |
| SM100                 | 10.10.40.58        |             |
| <b>aes80vmpg</b>      | <b>10.10.40.56</b> |             |
| default               | 0.0.0.0            |             |
| g450                  | 10.10.40.15        |             |
| <b>procr</b>          | <b>10.10.40.59</b> |             |

## 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  |
| AESVCS             | y       | procr       |

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 **aes80vmpg**.
- **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    |
| 1:                         | aes80vmpg          | *****       |
| 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: 2002
Type: ADJ-IP
COR: 1
Name: aes80vmpg
```

## 5.11 Configure H323 Stations for Single Step Conference

No extra specific changes were made during compliance testing for and H.323 stations in order for recording and single step conference to work. The screen below shows an example of a H.323 phone that was tested.

```
diaplay station 2000                               Page 1 of 6
STATION
Extension: 2000                                     Lock Messages? n      BCC: 0
Type: 9608                                           Security Code: 1234    TN: 1
Port: S00101                                         Coverage Path 1:      COR: 1
Name: H323 2000                                     Coverage Path 2:      COS: 1
Hunt-to Station:
STATION OPTIONS
Loss Group: 19                                     Time of Day Lock Table:
Personalized Ringing Pattern: 1
Message Lamp Ext: 2000
Mute Button Enabled? y
Speakerphone: 2-way
Display Language: english
Survivable GK Node Name:
Survivable COR: internal                           Media Complex Ext:
Survivable Trunk Dest? y                           IP SoftPhone? y
IP Video Softphone? n
Short/Prefixed Registration Allowed: default
```

## 5.12 Configure SIP Stations for Single Step Conference

There should be no extra changes required for SIP stations to work using Single Step Conference. Changes of SIP phones on Communication Manager must be carried out from System Manager. Access the System Manager using a web browser by entering **http://<FQDN>/SMGR**, where <FQDN> is the fully qualified domain name of System Manager or **http://<IP Address>/SMGR**. Log in using appropriate credentials.

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

This system is restricted solely to authorized users for legitimate business purposes only. The actual or attempted unauthorized access, use, or modification of this system is strictly prohibited.

Unauthorized users are subject to company disciplinary procedures and or criminal and civil penalties under state, federal, or other applicable domestic and foreign laws.

The use of this system may be monitored and recorded for administrative and security reasons. Anyone accessing this system expressly consents to such monitoring and recording, and is advised that if it reveals possible evidence of criminal activity, the evidence of such activity may be provided to law enforcement officials.

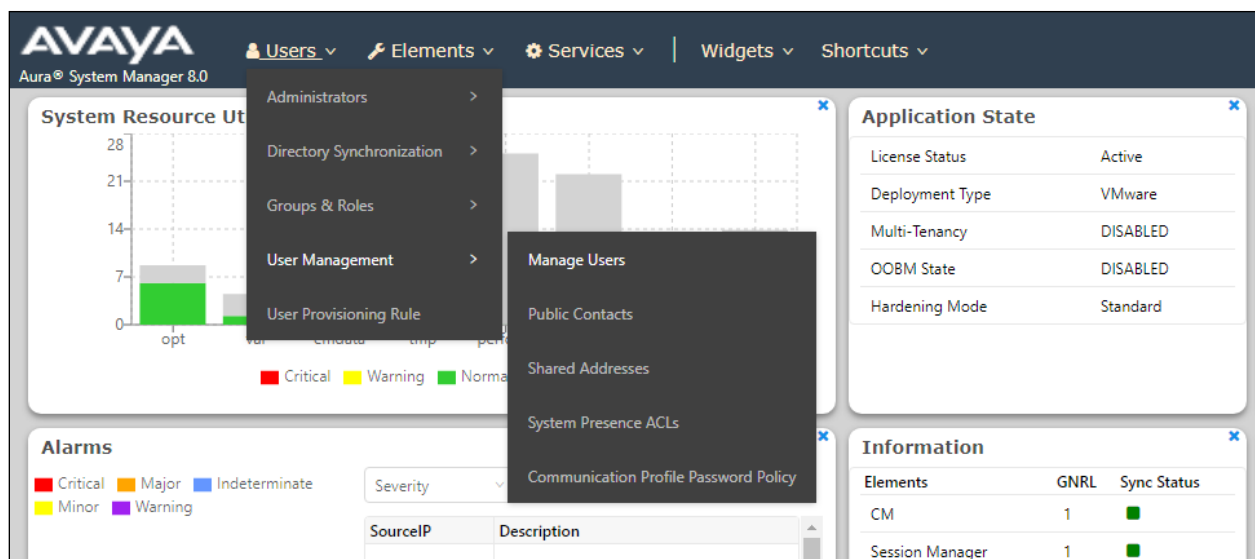
All users must comply with all corporate instructions regarding the protection of information assets.

User ID:

Password:

**Supported Browsers:** Internet Explorer 11.x or Firefox 59.0, 60.0 or 61.0.

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



Select the station to be edited and click on **Edit**. The example below shows that SIP extension **2100** is selected.

| Home                                | User Management |  |                       |                       |            |  |            |         |              |            |            |                          |       |       |                       |       |  |                          |      |         |               |                       |  |                          |      |         |               |                       |  |                          |      |         |               |                       |  |                                     |     |         |              |                       |      |                          |     |         |              |                       |      |                          |             |         |                      |                       |      |                          |             |         |                      |                       |      |                          |             |         |                      |                       |      |                          |             |         |                      |                       |      |
|-------------------------------------|-----------------|--|-----------------------|-----------------------|------------|--|------------|---------|--------------|------------|------------|--------------------------|-------|-------|-----------------------|-------|--|--------------------------|------|---------|---------------|-----------------------|--|--------------------------|------|---------|---------------|-----------------------|--|--------------------------|------|---------|---------------|-----------------------|--|-------------------------------------|-----|---------|--------------|-----------------------|------|--------------------------|-----|---------|--------------|-----------------------|------|--------------------------|-------------|---------|----------------------|-----------------------|------|--------------------------|-------------|---------|----------------------|-----------------------|------|--------------------------|-------------|---------|----------------------|-----------------------|------|--------------------------|-------------|---------|----------------------|-----------------------|------|
| User Management                     |                 | Home / Users / Manage Users  |                       |                       |            |  |            |         |              |            |            |                          |       |       |                       |       |  |                          |      |         |               |                       |  |                          |      |         |               |                       |  |                          |      |         |               |                       |  |                                     |     |         |              |                       |      |                          |     |         |              |                       |      |                          |             |         |                      |                       |      |                          |             |         |                      |                       |      |                          |             |         |                      |                       |      |                          |             |         |                      |                       |      |
| Manage Users                        |                 | Search   |                       |                       |            |  |            |         |              |            |            |                          |       |       |                       |       |  |                          |      |         |               |                       |  |                          |      |         |               |                       |  |                          |      |         |               |                       |  |                                     |     |         |              |                       |      |                          |     |         |              |                       |      |                          |             |         |                      |                       |      |                          |             |         |                      |                       |      |                          |             |         |                      |                       |      |                          |             |         |                      |                       |      |
| Public Contacts                     |                 | <div> <div>View</div> <div>Edit</div> <div>New</div> <div>Duplicate</div> <div>Delete</div> <div>More Actions</div> <div>Options</div> </div>  |                       |                       |            |  |            |         |              |            |            |                          |       |       |                       |       |  |                          |      |         |               |                       |  |                          |      |         |               |                       |  |                          |      |         |               |                       |  |                                     |     |         |              |                       |      |                          |     |         |              |                       |      |                          |             |         |                      |                       |      |                          |             |         |                      |                       |      |                          |             |         |                      |                       |      |                          |             |         |                      |                       |      |
| Shared Addresses                    |                 | <table> <tr> <th></th><th>First Name</th><th>Surname</th><th>Display Name</th><th>Login Name</th><th>SIP Handle</th></tr> <tr> <td><input type="checkbox"/></td><td>admin</td><td>admin</td><td>Default Administrator</td><td>admin</td><td></td></tr> <tr> <td><input type="checkbox"/></td><td>H323</td><td>Ext2000</td><td>Ext2000, H323</td><td>2000@devconnect.local</td><td></td></tr> <tr> <td><input type="checkbox"/></td><td>H323</td><td>Ext2001</td><td>Ext2001, H323</td><td>2001@devconnect.local</td><td></td></tr> <tr> <td><input type="checkbox"/></td><td>H323</td><td>Ext2002</td><td>Ext2002, H323</td><td>2002@devconnect.local</td><td></td></tr> <tr> <td><input checked="" type="checkbox"/></td><td>SIP</td><td>Ext2100</td><td>Ext2100, SIP</td><td>2100@devconnect.local</td><td>2100</td></tr> <tr> <td><input type="checkbox"/></td><td>SIP</td><td>Ext2101</td><td>Ext2101, SIP</td><td>2101@devconnect.local</td><td>2101</td></tr> <tr> <td><input type="checkbox"/></td><td>Equinox SIP</td><td>Ext2102</td><td>Ext2102, Equinox SIP</td><td>2102@devconnect.local</td><td>2102</td></tr> <tr> <td><input type="checkbox"/></td><td>Equinox SIP</td><td>Ext2103</td><td>Ext2103, Equinox SIP</td><td>2103@devconnect.local</td><td>2103</td></tr> <tr> <td><input type="checkbox"/></td><td>Equinox SIP</td><td>Ext2104</td><td>Ext2104, Equinox SIP</td><td>2104@devconnect.local</td><td>2104</td></tr> <tr> <td><input type="checkbox"/></td><td>Equinox SIP</td><td>Ext2105</td><td>Ext2105, Equinox SIP</td><td>2105@devconnect.local</td><td>2105</td></tr> </table> |                       |                       |            |  | First Name | Surname | Display Name | Login Name | SIP Handle | <input type="checkbox"/> | admin | admin | Default Administrator | admin |  | <input type="checkbox"/> | H323 | Ext2000 | Ext2000, H323 | 2000@devconnect.local |  | <input type="checkbox"/> | H323 | Ext2001 | Ext2001, H323 | 2001@devconnect.local |  | <input type="checkbox"/> | H323 | Ext2002 | Ext2002, H323 | 2002@devconnect.local |  | <input checked="" type="checkbox"/> | SIP | Ext2100 | Ext2100, SIP | 2100@devconnect.local | 2100 | <input type="checkbox"/> | SIP | Ext2101 | Ext2101, SIP | 2101@devconnect.local | 2101 | <input type="checkbox"/> | Equinox SIP | Ext2102 | Ext2102, Equinox SIP | 2102@devconnect.local | 2102 | <input type="checkbox"/> | Equinox SIP | Ext2103 | Ext2103, Equinox SIP | 2103@devconnect.local | 2103 | <input type="checkbox"/> | Equinox SIP | Ext2104 | Ext2104, Equinox SIP | 2104@devconnect.local | 2104 | <input type="checkbox"/> | Equinox SIP | Ext2105 | Ext2105, Equinox SIP | 2105@devconnect.local | 2105 |
|                                     | First Name      | Surname  | Display Name          | Login Name            | SIP Handle |  |            |         |              |            |            |                          |       |       |                       |       |  |                          |      |         |               |                       |  |                          |      |         |               |                       |  |                          |      |         |               |                       |  |                                     |     |         |              |                       |      |                          |     |         |              |                       |      |                          |             |         |                      |                       |      |                          |             |         |                      |                       |      |                          |             |         |                      |                       |      |                          |             |         |                      |                       |      |
| <input type="checkbox"/>            | admin           | admin  | Default Administrator | admin                 |            |  |            |         |              |            |            |                          |       |       |                       |       |  |                          |      |         |               |                       |  |                          |      |         |               |                       |  |                          |      |         |               |                       |  |                                     |     |         |              |                       |      |                          |     |         |              |                       |      |                          |             |         |                      |                       |      |                          |             |         |                      |                       |      |                          |             |         |                      |                       |      |                          |             |         |                      |                       |      |
| <input type="checkbox"/>            | H323            | Ext2000  | Ext2000, H323         | 2000@devconnect.local |            |  |            |         |              |            |            |                          |       |       |                       |       |  |                          |      |         |               |                       |  |                          |      |         |               |                       |  |                          |      |         |               |                       |  |                                     |     |         |              |                       |      |                          |     |         |              |                       |      |                          |             |         |                      |                       |      |                          |             |         |                      |                       |      |                          |             |         |                      |                       |      |                          |             |         |                      |                       |      |
| <input type="checkbox"/>            | H323            | Ext2001  | Ext2001, H323         | 2001@devconnect.local |            |  |            |         |              |            |            |                          |       |       |                       |       |  |                          |      |         |               |                       |  |                          |      |         |               |                       |  |                          |      |         |               |                       |  |                                     |     |         |              |                       |      |                          |     |         |              |                       |      |                          |             |         |                      |                       |      |                          |             |         |                      |                       |      |                          |             |         |                      |                       |      |                          |             |         |                      |                       |      |
| <input type="checkbox"/>            | H323            | Ext2002  | Ext2002, H323         | 2002@devconnect.local |            |  |            |         |              |            |            |                          |       |       |                       |       |  |                          |      |         |               |                       |  |                          |      |         |               |                       |  |                          |      |         |               |                       |  |                                     |     |         |              |                       |      |                          |     |         |              |                       |      |                          |             |         |                      |                       |      |                          |             |         |                      |                       |      |                          |             |         |                      |                       |      |                          |             |         |                      |                       |      |
| <input checked="" type="checkbox"/> | SIP             | Ext2100  | Ext2100, SIP          | 2100@devconnect.local | 2100       |  |            |         |              |            |            |                          |       |       |                       |       |  |                          |      |         |               |                       |  |                          |      |         |               |                       |  |                          |      |         |               |                       |  |                                     |     |         |              |                       |      |                          |     |         |              |                       |      |                          |             |         |                      |                       |      |                          |             |         |                      |                       |      |                          |             |         |                      |                       |      |                          |             |         |                      |                       |      |
| <input type="checkbox"/>            | SIP             | Ext2101  | Ext2101, SIP          | 2101@devconnect.local | 2101       |  |            |         |              |            |            |                          |       |       |                       |       |  |                          |      |         |               |                       |  |                          |      |         |               |                       |  |                          |      |         |               |                       |  |                                     |     |         |              |                       |      |                          |     |         |              |                       |      |                          |             |         |                      |                       |      |                          |             |         |                      |                       |      |                          |             |         |                      |                       |      |                          |             |         |                      |                       |      |
| <input type="checkbox"/>            | Equinox SIP     | Ext2102  | Ext2102, Equinox SIP  | 2102@devconnect.local | 2102       |  |            |         |              |            |            |                          |       |       |                       |       |  |                          |      |         |               |                       |  |                          |      |         |               |                       |  |                          |      |         |               |                       |  |                                     |     |         |              |                       |      |                          |     |         |              |                       |      |                          |             |         |                      |                       |      |                          |             |         |                      |                       |      |                          |             |         |                      |                       |      |                          |             |         |                      |                       |      |
| <input type="checkbox"/>            | Equinox SIP     | Ext2103  | Ext2103, Equinox SIP  | 2103@devconnect.local | 2103       |  |            |         |              |            |            |                          |       |       |                       |       |  |                          |      |         |               |                       |  |                          |      |         |               |                       |  |                          |      |         |               |                       |  |                                     |     |         |              |                       |      |                          |     |         |              |                       |      |                          |             |         |                      |                       |      |                          |             |         |                      |                       |      |                          |             |         |                      |                       |      |                          |             |         |                      |                       |      |
| <input type="checkbox"/>            | Equinox SIP     | Ext2104  | Ext2104, Equinox SIP  | 2104@devconnect.local | 2104       |  |            |         |              |            |            |                          |       |       |                       |       |  |                          |      |         |               |                       |  |                          |      |         |               |                       |  |                          |      |         |               |                       |  |                                     |     |         |              |                       |      |                          |     |         |              |                       |      |                          |             |         |                      |                       |      |                          |             |         |                      |                       |      |                          |             |         |                      |                       |      |                          |             |         |                      |                       |      |
| <input type="checkbox"/>            | Equinox SIP     | Ext2105  | Ext2105, Equinox SIP  | 2105@devconnect.local | 2105       |  |            |         |              |            |            |                          |       |       |                       |       |  |                          |      |         |               |                       |  |                          |      |         |               |                       |  |                          |      |         |               |                       |  |                                     |     |         |              |                       |      |                          |     |         |              |                       |      |                          |             |         |                      |                       |      |                          |             |         |                      |                       |      |                          |             |         |                      |                       |      |                          |             |         |                      |                       |      |
| System Presence ACLs                |                 | <div> <div>Select All</div> <div>Selected 1 items</div> </div>   |                       |                       |            |  |            |         |              |            |            |                          |       |       |                       |       |  |                          |      |         |               |                       |  |                          |      |         |               |                       |  |                          |      |         |               |                       |  |                                     |     |         |              |                       |      |                          |     |         |              |                       |      |                          |             |         |                      |                       |      |                          |             |         |                      |                       |      |                          |             |         |                      |                       |      |                          |             |         |                      |                       |      |
| Communication Profile ...           |                 | <div> <div>Total Users : 11</div> <div>1 2</div> <div>10 / page</div> <div>Goto</div> </div>   |                       |                       |            |  |            |         |              |            |            |                          |       |       |                       |       |  |                          |      |         |               |                       |  |                          |      |         |               |                       |  |                          |      |         |               |                       |  |                                     |     |         |              |                       |      |                          |     |         |              |                       |      |                          |             |         |                      |                       |      |                          |             |         |                      |                       |      |                          |             |         |                      |                       |      |                          |             |         |                      |                       |      |

To set the password for the SIP extension click on **Communication Profile Password** in the left window and set the password in the main window (not shown here).

Click on the **CM Endpoint Profile** in the left window. Click on the **Editor** icon in the main window.

User Profile | Edit | 2100@devconnect.local

Commit & Continue

Commit

Cancel

Identity

Communication Profile

Membership

Contacts

Communication Profile Password

PROFILE SET: Primary

Communication Address

PROFILES

Session Manager Profile

CM Endpoint Profile

\* System:

CM80vmpg

\* Profile Type:

Endpoint

Editor

\* Extension:

2100

\* Set Type:

9641SIP

Use Existing Endpoints:

Template:

Start typing...

Security Code:

Enter Security Code

Port:

S00001

Voice Mail Number:

6666

Preferred Handle:

Select

Ensure that **Type of 3PCC Enabled** is set to **Avaya**. Click on the **Feature Options** tab after that. Ensure that both the **Class of Restriction (COR)** and the **Class of Service (COS)** are set correctly. Scroll up or down and click on **Done** (not shown).

The screenshot shows a configuration window with several tabs: General Options (G) \*, Feature Options (F), Site Data (S), Abbreviated Call Dialing (A), Enhanced Call Fwd (E), Button Assignment (B), Profile Settings (P), and Group Membership (M). The 'General Options' tab is active. It contains two columns of settings. On the left: Class of Restriction (COR) is 1, Emergency Location Ext is 2100, Tenant Number is 1, SIP Trunk is 'aar', Coverage Path 1 is empty, Lock Message is unchecked, and Multibyte Language is 'Not Applicable'. On the right: Class of Service (COS) is 1, Message Lamp Ext. is 2100, Type of 3PCC Enabled is 'Avaya' (highlighted with a red box), Coverage Path 2 is empty, Localized Display Name is 'Ext2100, SIP', and Enable Reachability for Station Domain Control is 'system'. At the bottom, there is a SIP URI field.

Click on **Commit**, as shown.

The screenshot shows a 'User Profile | Edit | 2100@devconnect.local' window. At the top right, there are buttons for 'Commit & Continue', 'Commit' (highlighted with a red box), and 'Cancel'. Below the title bar, there are tabs for 'Identity', 'Communication Profile', 'Membership', and 'Contacts'. The 'Communication Profile' tab is active. On the left, there is a sidebar with 'Communication Profile Password', 'PROFILE SET: Primary', 'Communication Address', 'PROFILES', 'Session Manager Profile' (unchecked), and 'CM Endpoint Profile' (checked). The main area contains various configuration fields: System (CM80vmpg), Profile Type (Endpoint), Use Existing Endpoints (unchecked), Extension (2100), Template (Start typing...), Set Type (9641SIP), Security Code (\*\*\*\*), Port (S00001), Voice Mail Number (6666), Preferred Handle (Select), Calculate Route Pattern (unchecked), SIP URI (Select), Sip Trunk (aar), Enhanced Callr-Info display f... (unchecked), 1-line phones ... (unchecked), Delete on Unassign from User or on Delete User (checked), and Override Endpoint Name and Localized Name (checked).

## 5.13 Configure Virtual Stations

Add virtual stations to allow Presence Suite record calls using Single Step Conference. Type **add station x** where x is the extension number of the station to be configured also note this extension number for configuration required in **Section 7.2.1**. Note the **Security Code** and ensure that **IP SoftPhone** is set to **y**.

|                           |  |               |
|---------------------------|--|---------------|
| <b>add station 28903</b>  |  | Page 1 of 6   |
| STATION                   |  |               |
| Extension: 28903          | Lock Messages? n                             | BCC: 0        |
| <b>Type: 4624</b>         | <b>Security Code: 1234</b>                   | TN: 1         |
| Port: S00101              | Coverage Path 1:                             | <b>COR: 1</b> |
| Name: Recorder            | Coverage Path 2:                             | COS: 1        |
|                           | Hunt-to Station:                             |               |
| STATION OPTIONS           |  |               |
|                           | Time of Day Lock Table:                      |               |
| Loss Group: 19            | Personalized Ringing Pattern: 1              |               |
|                           | Message Lamp Ext: 28903                      |               |
| Speakerphone: 2-way       | Mute Button Enabled? y                       |               |
| Display Language: english |  |               |
| Survivable GK Node Name:  |  |               |
| Survivable COR: internal  | Media Complex Ext:                           |               |
| Survivable Trunk Dest? y  | <b>IP SoftPhone? y</b>                       |               |
|                           | IP Video Softphone? n                        |               |
|                           | Short/Prefixed Registration Allowed: default |               |

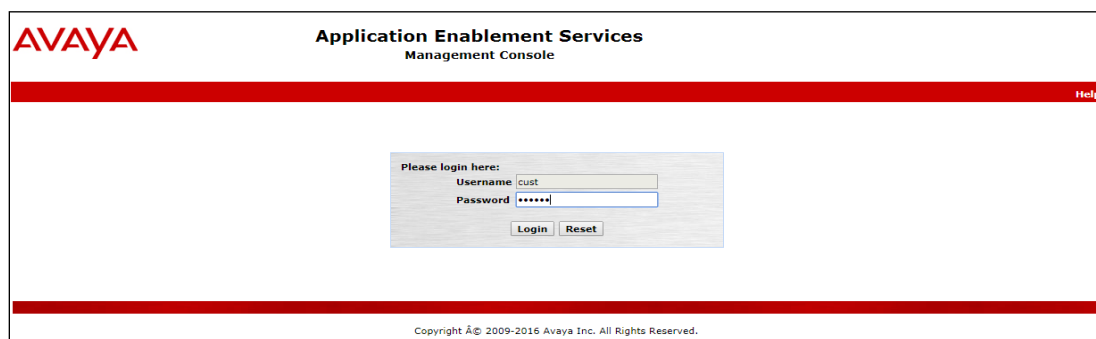
# Configure Avaya Aura® Application Enablement Services Server

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 Unrestricted Access for CTI User
- Identify TLinks
- Configure Networking Ports

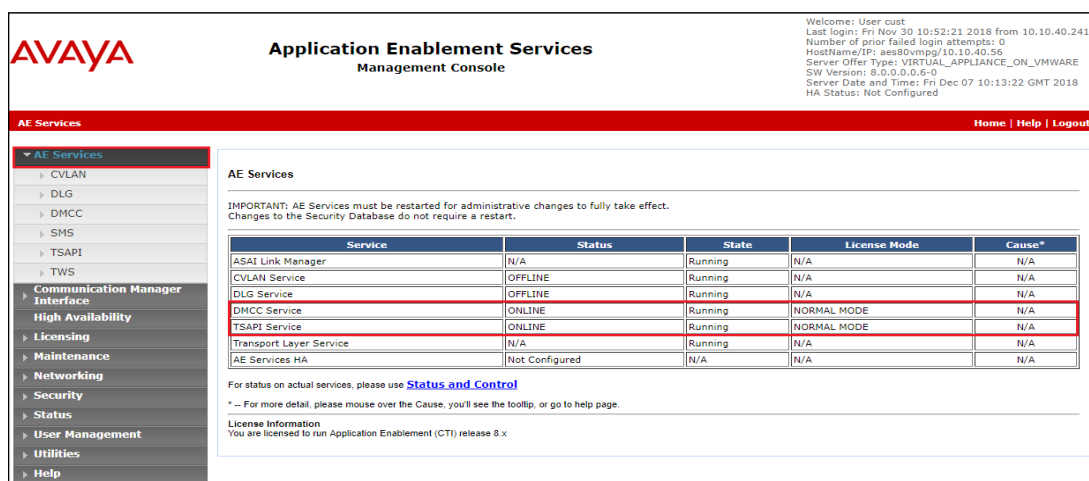
## 6.1 Verify Licensing

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. It features the Avaya logo and the title 'Application Enablement Services Management Console'. A login form is centered on the page with fields for 'Username' (containing 'cust') and 'Password' (masked with dots). Below the fields are 'Login' and 'Reset' buttons. A 'Help' link is in the top right corner. The footer contains the copyright notice: '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** and **DMCC Service** are licensed by ensuring that the **License Mode** is showing **NORMAL MODE**.



The screenshot shows the 'AE Services' page in the Avaya Application Enablement Services Management Console. The left sidebar contains a navigation menu with options like 'AE Services', 'Communication Manager Interface', 'High Availability', 'Licensing', 'Maintenance', 'Networking', 'Security', 'Status', 'User Management', 'Utilities', and 'Help'. The main content area displays the 'AE Services' status. A table lists various services and their status, state, license mode, and cause. The 'DMCC Service' and 'TSAPI Service' are highlighted with red boxes, showing a 'License Mode' of 'NORMAL MODE'. Below the table, there is a note about restarting services for administrative changes and a link to 'Status and Control'. The footer includes license information: 'You are licensed to run Application Enablement (CTI) release 8.x'.

| 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    |
| AE Services HA          | Not Configured | N/A     | N/A          | 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 (expanded), Switch Connections (highlighted with a red box), Dial Plan, High Availability, Licensing, and Maintenance. The main content area is titled 'Switch Connections' and features a text input field containing 'cm80vmppg' and an 'Add Connection' button (highlighted with a red box). Below this is a table with columns: Connection Name, Processor Ethernet, and Msg Period. The table contains one row with the connection name 'cm80vmppg'. Below the table are several action 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 - cm80vmppg' form. It contains the following fields and controls: 'Switch Password' (password field with dots), 'Confirm Switch Password' (password field with dots), 'Msg Period' (text field with '30' and a label 'Minutes (1 - 72)'), 'Provide AE Services certificate to switch' (checkbox, unchecked), 'Secure H323 Connection' (checkbox, unchecked), 'Processor Ethernet' (checkbox, checked), and 'Apply' (button, highlighted with a red box) and 'Cancel' (button).

From the **Switch Connections** screen, select the radio button for the recently added switch connection and select the **Edit CLAN IPs** button.

**Switch Connections**

cm80vmpg Add Connection

| Connection Name | Processor Ethernet      | Msg Period              |
|-----------------|-------------------------|-------------------------|
| Edit Connection | <b>Edit PE/CLAN IPs</b> | 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.

**Edit Processor Ethernet IP - cm80vmpg**

10.10.40.59 Add/Edit Name or IP

| Name or IP Address |
|--------------------|
| 10.10.40.59        |

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

▼ AE Services

- ▶ CVLAN
- ▶ DLG
- ▶ DMCC
- ▶ SMS
- ▼ TSAPI
  - **TSAPI Links**
  - TSAPI Properties
- ▶ TWS

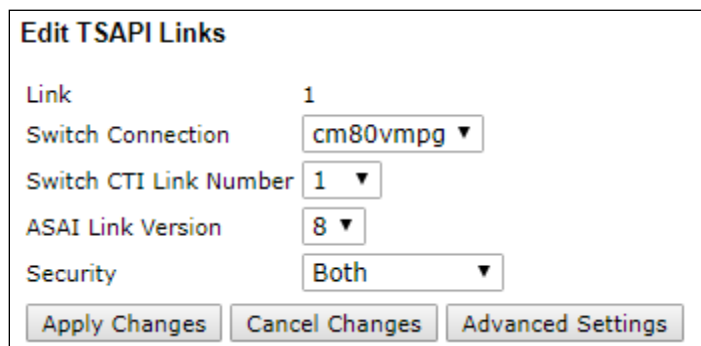
**TSAPI Links**

| Link | Switch Connection | Switch CTI Link # |
|------|-------------------|-------------------|
|      |                   |                   |

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 **cm80vmppg**, 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 **8**.
- **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 cm80vmppg ▼

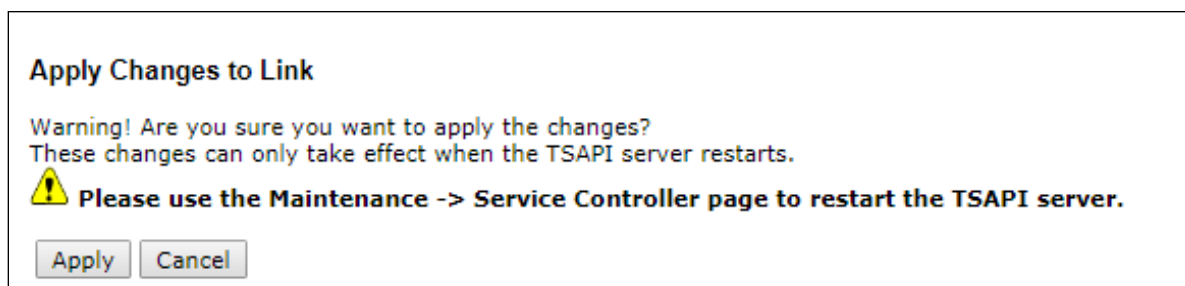
Switch CTI Link Number 1 ▼

ASAI Link Version 8 ▼

Security Both ▼

Apply Changes Cancel Changes Advanced Settings

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



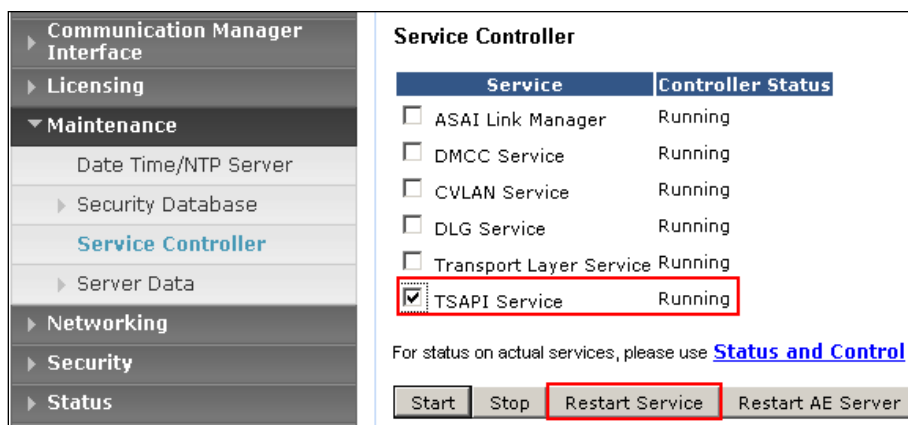
**Apply Changes to Link**

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.

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](#)

Start Stop **Restart Service** Restart AE Server

## 6.4 Create 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. Navigate to the **User Management** → **User Admin** and 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 Presence Suite 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.

The screenshot shows the 'Add User' form within the 'User Management | User Admin | Add User' interface. On the left is a navigation menu with categories: AE Services, Communication Manager Interface, High Availability, Licensing, Maintenance, Networking, Security, Status, User Management (expanded), Service Admin, User Admin (expanded), Add User (selected), Change User Password, List All Users, Modify Default Users, Search Users, Utilities, and Help. The main form area is titled 'Add User' and includes a note: 'Fields marked with \* can not be empty.' The form fields are as follows:

| Field               | Value    |
|---------------------|----------|
| * User Id           | presence |
| * Common Name       | presence |
| * Surname           | presence |
| * User Password     | *****    |
| * Confirm Password  | *****    |
| Admin Note          |          |
| Avaya Role          | None     |
| Business Category   |          |
| Car License         |          |
| CM Home             |          |
| Css Home            |          |
| CT User             | Yes      |
| Department Number   |          |
| Display Name        |          |
| Employee Number     |          |
| Employee Type       |          |
| Enterprise Handle   |          |
| Given Name          |          |
| Home Phone          |          |
| Home Postal Address |          |
| Initials            |          |
| Labeled URI         |          |
| Mail                |          |
| MM Home             |          |
| Mobile              |          |
| Organization        |          |
| Pager               |          |
| Preferred Language  | English  |
| Room Number         |          |
| Telephone Number    |          |

At the bottom of the form are 'Apply' and 'Cancel' buttons.

## 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** button.

| User ID                                   | Common Name | Worktop Name | Device ID |
|---|-------------|--------------|-----------|
| <input type="radio"/> asc                 | asc         | NONE         | NONE      |
| <input type="radio"/> cardeasy            | cardeasy    | NONE         | NONE      |
| <input type="radio"/> NICE                | NICE        | NONE         | NONE      |
| <input type="radio"/> paul                | paul        | NONE         | NONE      |
| <input checked="" type="radio"/> presence | presence    | NONE         | NONE      |

[Edit](#) [List All](#)

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

**Edit CTI User**

User Profile: User ID: presence  
Common Name: presence  
Worktop Name: NONE ▼  
Unrestricted Access: ☒

---

Call and Device Control: Call Origination/Termination and Device Status: None ▼

---

Call and Device Monitoring: Device Monitoring: None ▼  
Calls On A Device Monitoring: None ▼  
Call Monitoring: ☐

---

Routing Control: Allow Routing on Listed Devices: None ▼

[Apply Changes](#) [Cancel Changes](#)

A screen appears to confirm applied changes to CTI User, choose **Apply**. This CTI user should now be enabled.

**Apply Changes to CTI User Properties**

Warning! Are you sure you want to apply the changes?

[Apply](#) [Cancel](#)

## 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 system configuration interface. On the left is a vertical navigation menu with the following items: AE Services, Communication Manager Interface, High Availability, Licensing, Maintenance, Networking, Security (expanded), Account Management, Audit, Certificate Management, Enterprise Directory, Host AA, PAM, and Security Database (expanded). Under Security Database, the following sub-items are listed: Control, CTI Users, Devices, Device Groups, Tlinks (highlighted in blue), Tlink Groups, and Worktops. On the right, the 'Tlinks' configuration page is shown. It has a title 'Tlinks' and a section 'Tlink Name' with two radio button options: 'AVAYA#CM80VMPPG#CSTA#AES80VMPPG' (selected) and 'AVAYA#CM80VMPPG#CSTA-S#AES80VMPPG'. Below these options is a 'Delete Tlink' button.

**Navigation Menu:**

- ▶ AE Services
- ▶ Communication Manager Interface
- ▶ High Availability
- ▶ Licensing
- ▶ Maintenance
- ▶ Networking
- ▼ Security
  - ▶ Account Management
  - ▶ Audit
  - ▶ Certificate Management
  - Enterprise Directory
  - ▶ Host AA
  - ▶ PAM
  - ▼ Security Database
    - Control
    - ⊕ CTI Users
    - Devices
    - Device Groups
    - **Tlinks**
    - Tlink Groups
    - Worktops

**Tlinks Configuration:**

**Tlinks**

**Tlink Name**

- ☒ AVAYA#CM80VMPPG#CSTA#AES80VMPPG
- ☐ AVAYA#CM80VMPPG#CSTA-S#AES80VMPPG

**Delete Tlink**

## 6.7 Configure Networking Ports

To ensure that TSAPI and DMCC ports are enabled, navigate to **Networking → Ports**. Ensure that the TSAPI ports are set to **Enabled** as shown below. Ensure that the **DMCC Server Ports** are also **Enabled** and take note of the **Unencrypted Port 4721** which will be used later in **Section 7.4.1**.

**AVAYA** Application Enablement Services Management Console

**Networking | Ports**

**Ports**

**CVLAN Ports**

|                      |                                   |  | Enabled                          | Disabled              |
|----------------------|-----------------------------------|--|----------------------------------|-----------------------|
| Unencrypted TCP Port | 9999                              |  | <input checked="" type="radio"/> | <input type="radio"/> |
| Encrypted TCP Port   | <input type="text" value="9998"/> |  | <input checked="" type="radio"/> | <input type="radio"/> |

**DLG Port**

|  | TCP Port |  |
|--|----------|--|
|  | 5678     |  |

**TSAPI Ports**

|                         |                                   |  | Enabled                          | Disabled              |
|-------------------------|-----------------------------------|--|----------------------------------|-----------------------|
| TSAPI Service Port      | 450                               |  | <input checked="" type="radio"/> | <input type="radio"/> |
| Local TLINK Ports       |                                   |  |                                  |                       |
| TCP Port Min            | 1024                              |  |                                  |                       |
| TCP Port Max            | 1039                              |  |                                  |                       |
| Unencrypted TLINK Ports |                                   |  |                                  |                       |
| TCP Port Min            | <input type="text" value="1050"/> |  |                                  |                       |
| TCP Port Max            | <input type="text" value="1065"/> |  |                                  |                       |
| Encrypted TLINK Ports   |                                   |  |                                  |                       |
| TCP Port Min            | <input type="text" value="1066"/> |  |                                  |                       |
| TCP Port Max            | <input type="text" value="1081"/> |  |                                  |                       |

**DMCC Server Ports**

|                  |                                   |  | Enabled                          | Disabled              |
|------------------|-----------------------------------|--|----------------------------------|-----------------------|
| Unencrypted Port | <input type="text" value="4721"/> |  | <input checked="" type="radio"/> | <input type="radio"/> |
| Encrypted Port   | <input type="text" value="4722"/> |  | <input checked="" type="radio"/> | <input type="radio"/> |
| TR/87 Port       | <input type="text" value="4723"/> |  | <input checked="" type="radio"/> | <input type="radio"/> |

Once all the necessary changes are made it is a good idea to restart of the AE Server. Navigate to **Maintenance → Service Controller**. In the main screen select **Restart AE Server** highlighted.

**AVAYA** Application Enablement Services Management Console

**Maintenance | Service Controller**

**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 type="checkbox"/> TSAPI Service           | Running           |

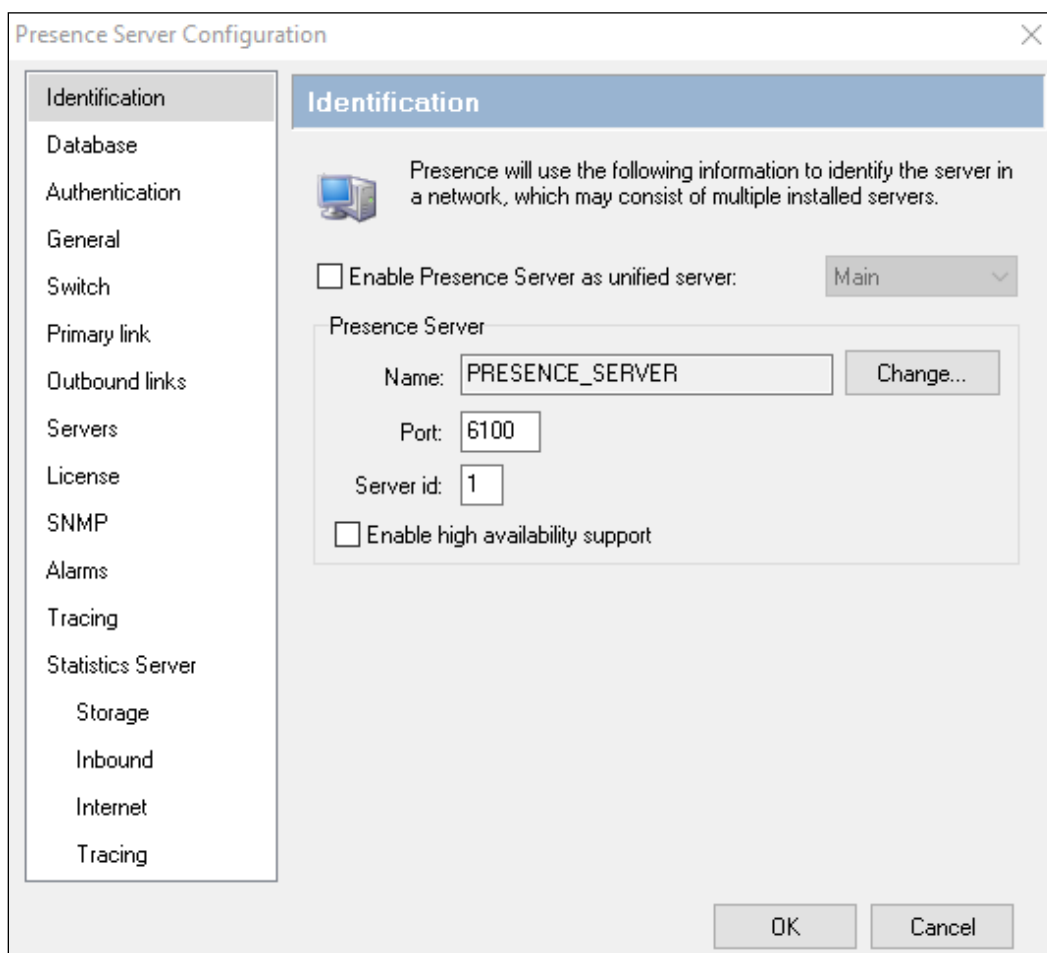
For status on actual services, please use [Status and Control](#)

## ■ Configure Enghouse Presence Suite

The Presence Suite includes the Presence Server, Presence Mail Interactions Server, Presence Web Interactions Server, Presence Recording 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 Enghouse Interactive. 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.

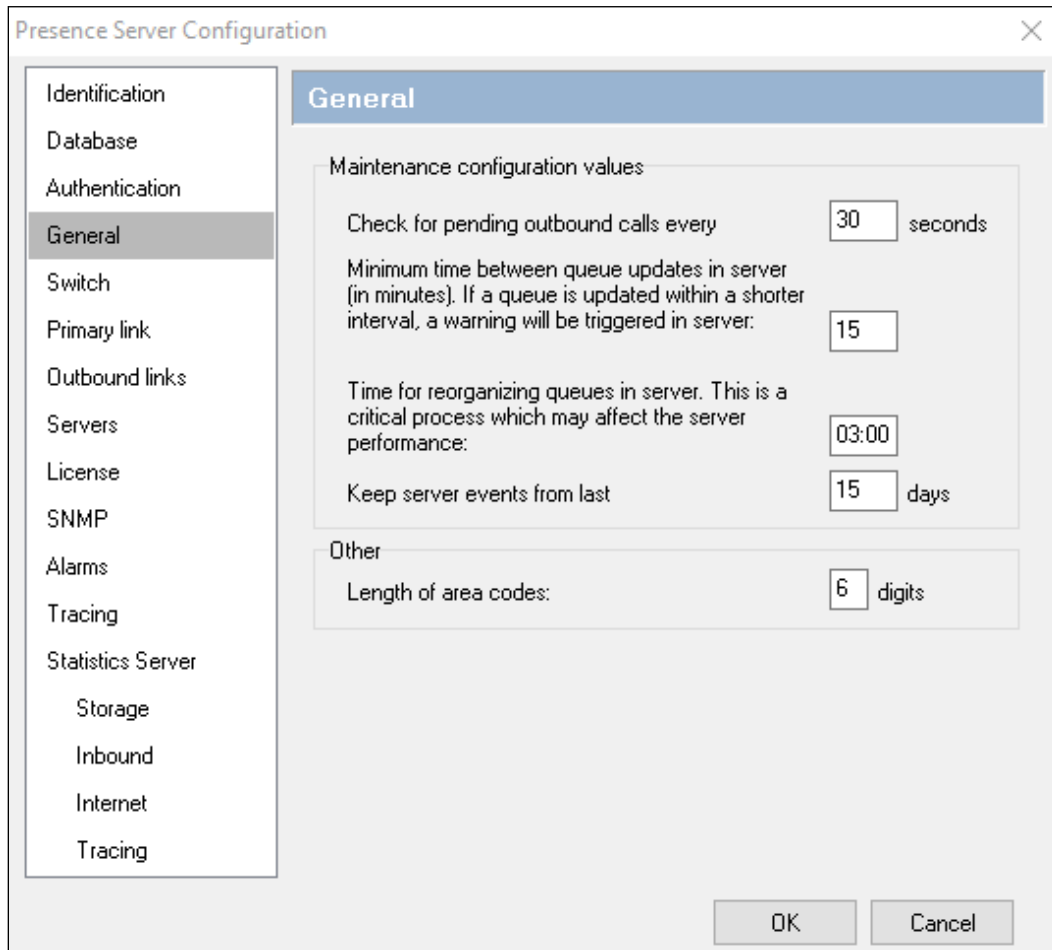


The screenshot shows the 'Presence Server Configuration' window. On the left is a vertical menu with options: Identification, Database, Authentication, General, Switch, Primary link, Outbound links, Servers, License, SNMP, Alarms, Tracing, Statistics Server, Storage, Inbound, Internet, and Tracing. The '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.' accompanied by a computer icon.
- A checkbox 'Enable Presence Server as unified server:' which is unchecked, followed by a dropdown menu currently set to 'Main'.
- A section titled 'Presence Server' containing:
  - 'Name:' field with 'PRESENCE\_SERVER' and a 'Change...' button.
  - 'Port:' field with '6100'.
  - 'Server id:' field with '1'.
  - An unchecked checkbox 'Enable high availability support'.

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

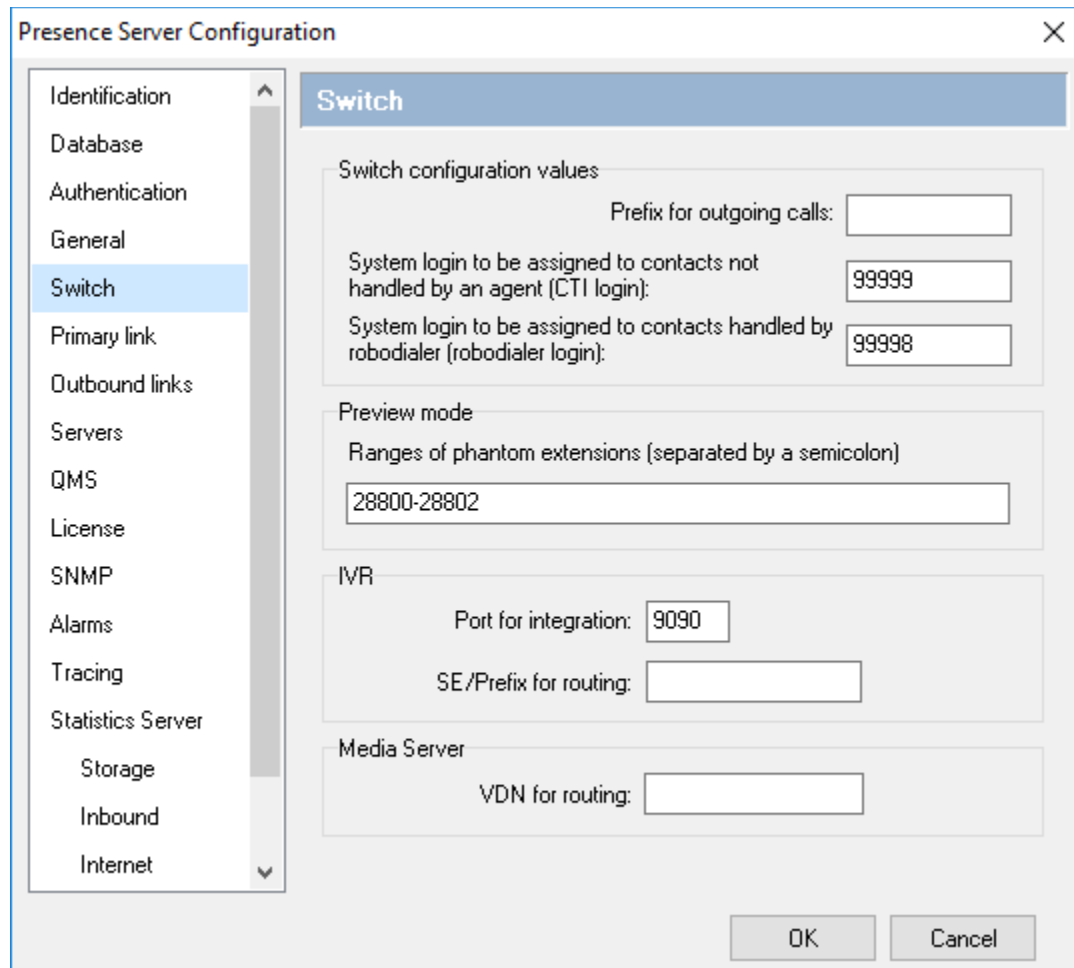
Select **General** from the menu on the left side of the screen. If desired, the Maintenance configuration values can be altered here, for the compliance test the default values were retained.



The image 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, Statistics Server, Storage, Inbound, Internet, and Tracing. 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' (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), 'Time for reorganizing queues in server. This is a critical process which may affect the server performance:' (03:00), and 'Keep server events from last' (15 days). The 'Other' section contains one setting: 'Length of area codes:' (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    |         |
|                                  | Time for reorganizing queues in server. This is a critical process which may affect the server performance:  | 03:00 |         |
|                                  | Keep server events from last   | 15    | days    |
| Other                            | Length of area codes:  | 6     | digits  |

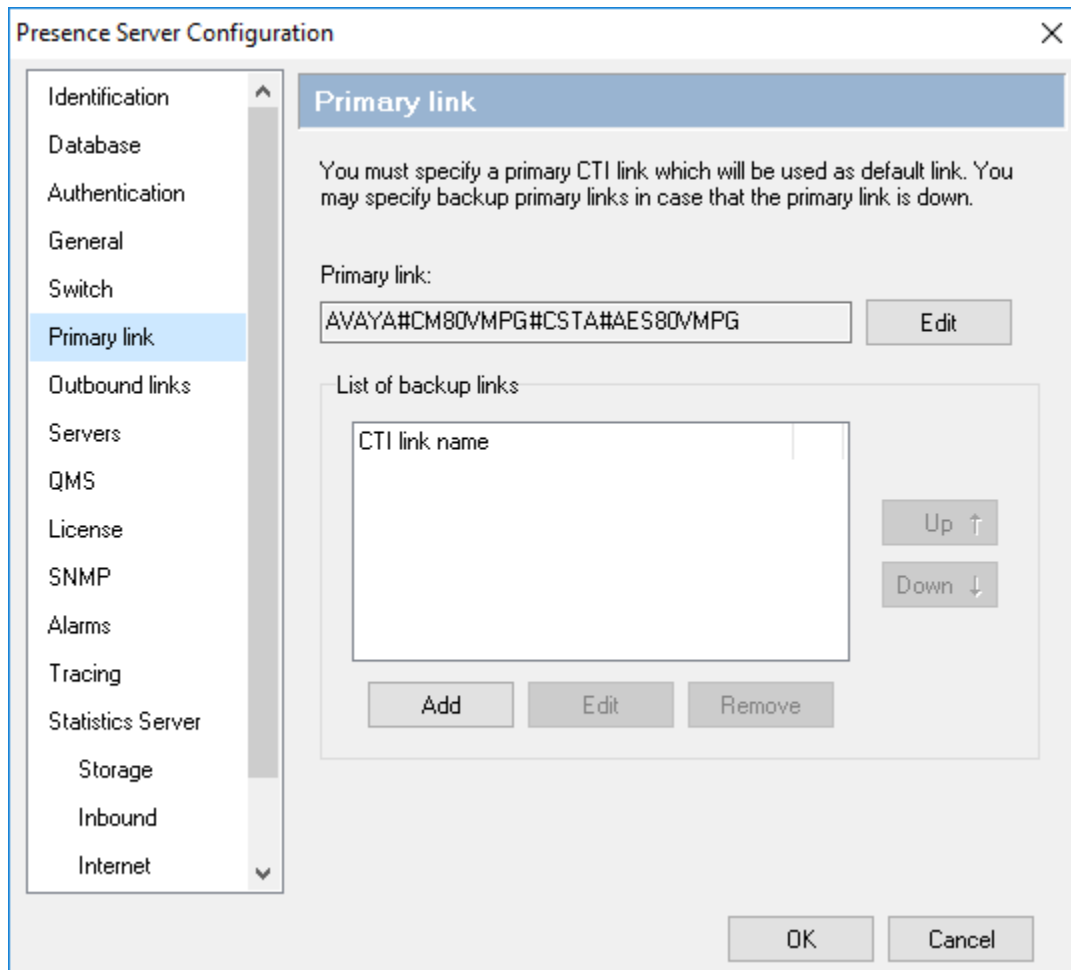
Select the **Switch** option from the menu on the left side of the screen. The **System login to be assigned to contacts not handled by an agent (CTI login)** field should be set to a value supplied by Presence, the value used for this configuration is **99999**. Enter the phantom extensions configured in **Section 5.7** in the **Ranges of phantom extensions** parameter.



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 is titled 'Switch' and contains several sections: 'Switch configuration values' with fields for 'Prefix for outgoing calls', 'System login to be assigned to contacts not handled by an agent (CTI login)' (set to 99999), and 'System login to be assigned to contacts handled by robodialer (robodialer login)' (set to 99998); 'Preview mode' with a field for 'Ranges of phantom extensions (separated by a semicolon)' (set to 28800-28802); 'IVR' with fields for 'Port for integration' (set to 9090) and 'SE/Prefix for routing'; and 'Media Server' with a field for 'VDN for routing'. At the bottom right are 'OK' and 'Cancel' buttons.

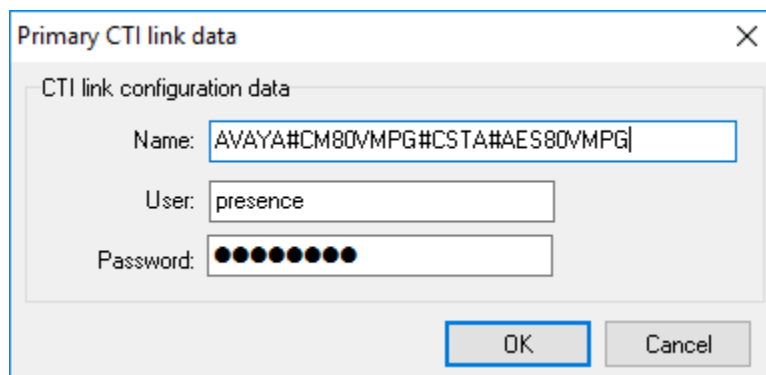
| Section                     | Field  | Value       |
|-----------------------------|--|-------------|
| Switch configuration values | Prefix for outgoing calls  |             |
|                             | System login to be assigned to contacts not handled by an agent (CTI login)      | 99999       |
|                             | System login to be assigned to contacts handled by robodialer (robodialer login) | 99998       |
| Preview mode                | Ranges of phantom extensions (separated by a semicolon)                          | 28800-28802 |
| IVR                         | Port for integration   | 9090        |
|                             | SE/Prefix for routing  |             |
| Media Server                | 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, QMS, License, SNMP, Alarms, Tracing, Statistics Server, Storage, Inbound, and Internet. 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#CM80VMPG#CSTA#AES80VMPG' and an 'Edit' button. Further down is a 'List of backup links' section with a large text box labeled 'CTI link name' and 'Up'/'Down' arrow buttons. At the bottom of this section are 'Add', 'Edit', and 'Remove' buttons. The dialog box has 'OK' and 'Cancel' buttons at the bottom right.

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**.



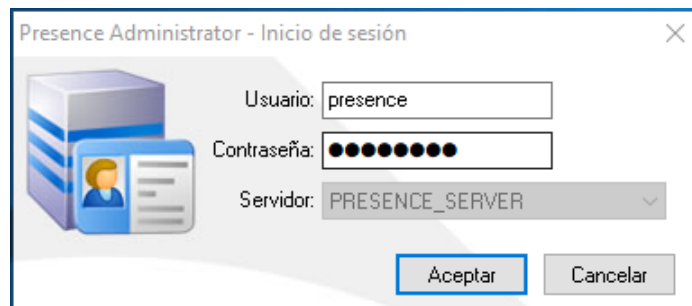
The image shows a 'Primary CTI link data' dialog box. It contains a section titled 'CTI link configuration data' with three fields: 'Name' (containing 'AVAYA#CM80VMPG#CSTA#AES80VMPG'), 'User' (containing 'presence'), and 'Password' (containing a masked password represented by dots). The dialog box has 'OK' and 'Cancel' buttons at the bottom right.

## 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.

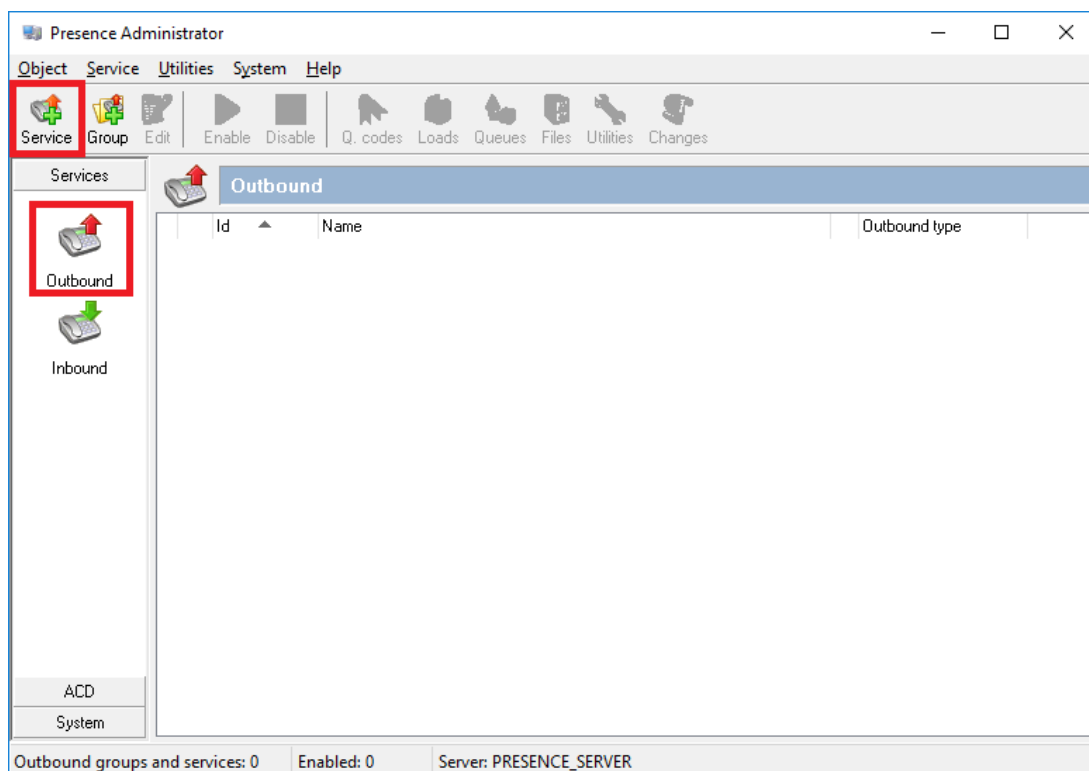
### 7.2.1 Logging in to Presence Administrator

Launch the **Presence Administrator** application by double clicking the **pcadmin.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 **Service** button to configure an outbound service.



In the resulting screen, select **General** from the menu on the left hand side and enter an **Id** and 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 **Outbound calling hours** field set the time range for which the outbound service will be active. All other fields are left with their default values.

**New outbound service**

☒ **General**

☒ **Integration**

☐ **Contact information**

☐ **ACD**

☐ **Outbound options**

☐ **Call analysis**

☐ **Maximums**

☐ **Queues**

☐ **Schedule**

☐ **Softphone**

☐ **Alternative phones**

☐ **Time zones**

☐ **Do-Not-Call lists**

☐ **Sounds**

☐ **Custom buttons**

☐ **Custom fields**

☐ **Record**

☐ **Contact**

☐ **Assistance**

☐ **Other**

☐ **Logo**

**General**

**Identification**

Id: 2

Name: OUTBOUND SERVICE

Outbound type: Progressive

**Resources**

Resource profile: General

Stop reasons: [All]

**Outbound and scheduled calling hours**

Outbound calling hours: 08:00-22:00

Do not schedule records for the last 15 minutes of a time range

☐ Scheduled limit date: 01/05/2019

OK Cancel

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. 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.

**Note:** Typically a unique VDN/Skill would be setup for each module such as Inbound, Outbound, Webchat etc., in these screen shots taken for compliance testing the same VDN may have been used for some of these services.

Outbound service

ACD

ACD Items

Extension/Skill: 4806

VDN/SE: 4906

CTI link: <<Primary CTI link>>

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

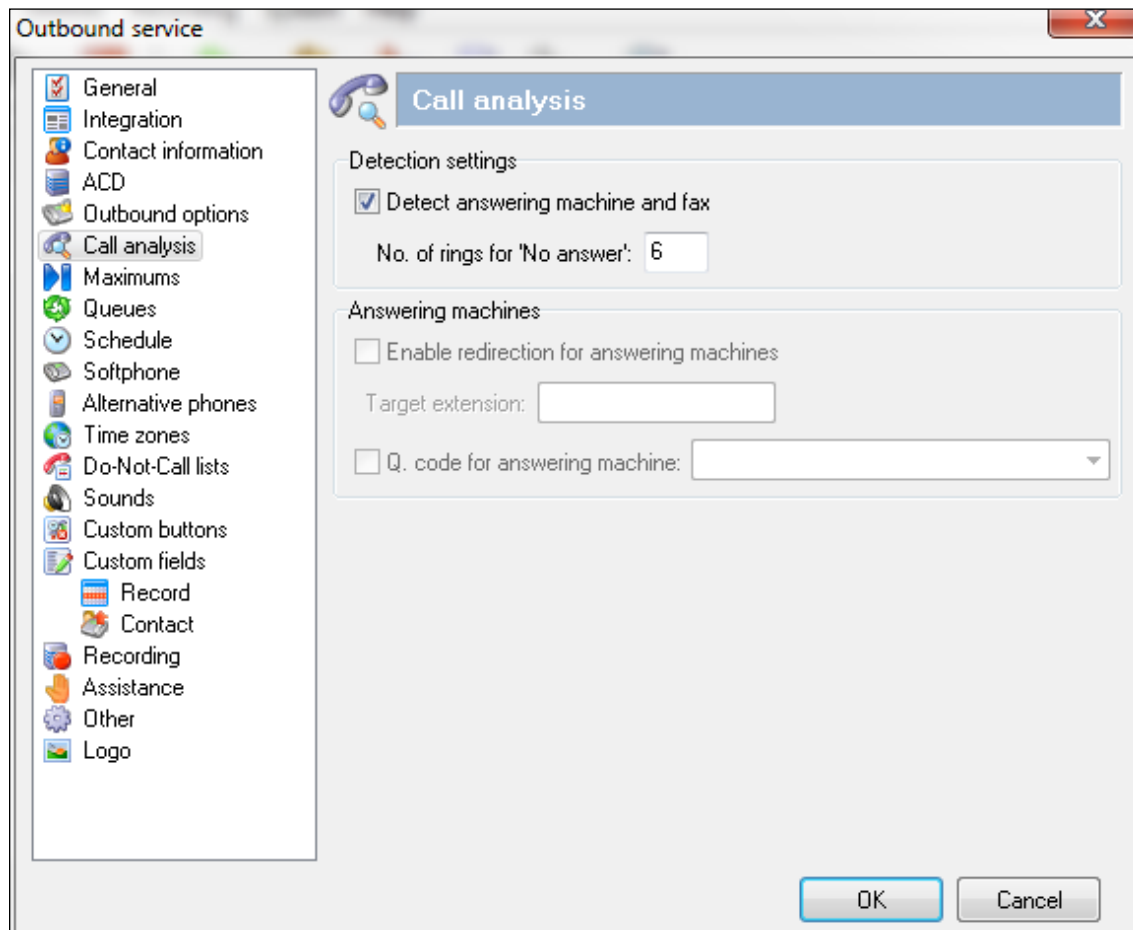
☐ Maximum number of concurrent service calls:

☐ Check agent availability

☐ Minimum number/percentage of available agents:

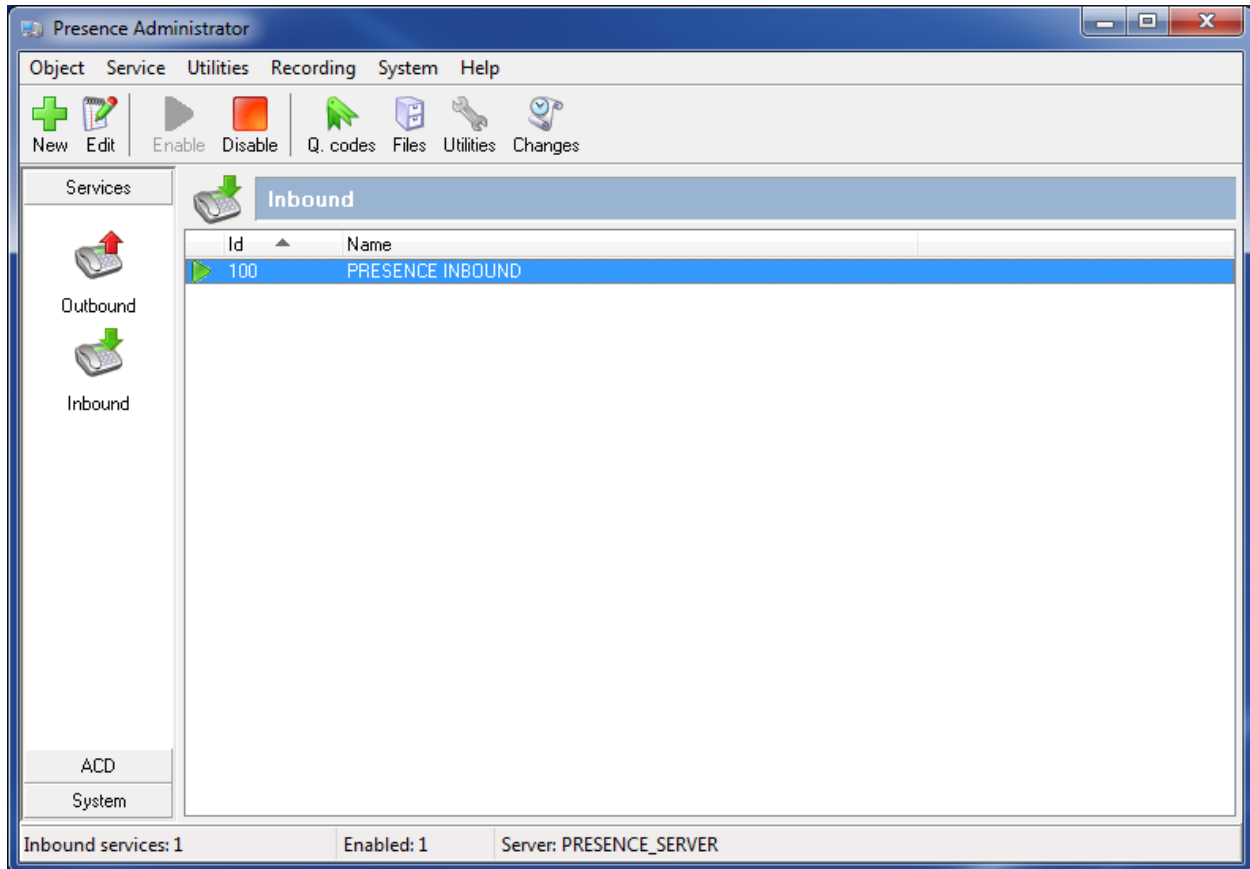
OK Cancel

Select **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

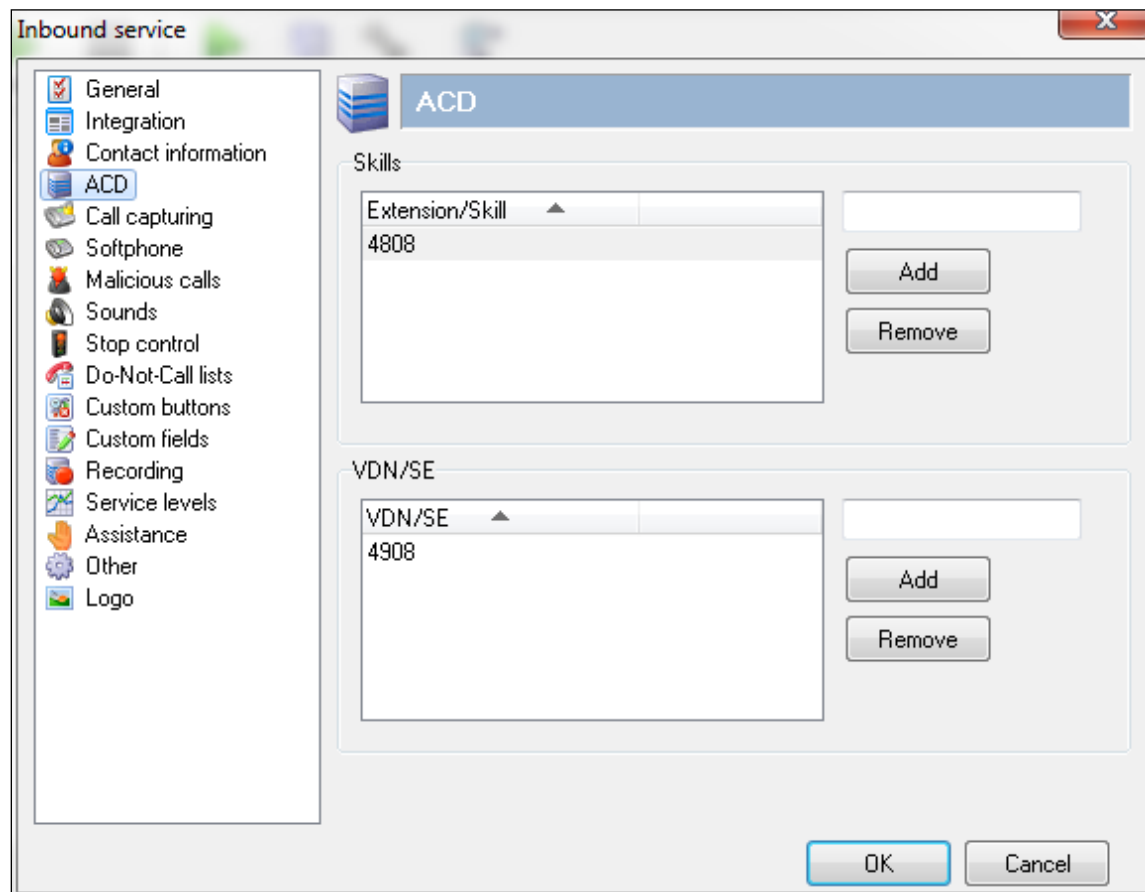
To configure an inbound service, from the left hand side select **Services** → **Inbound** from the Presence Administrator main menu. Click the **New** button.



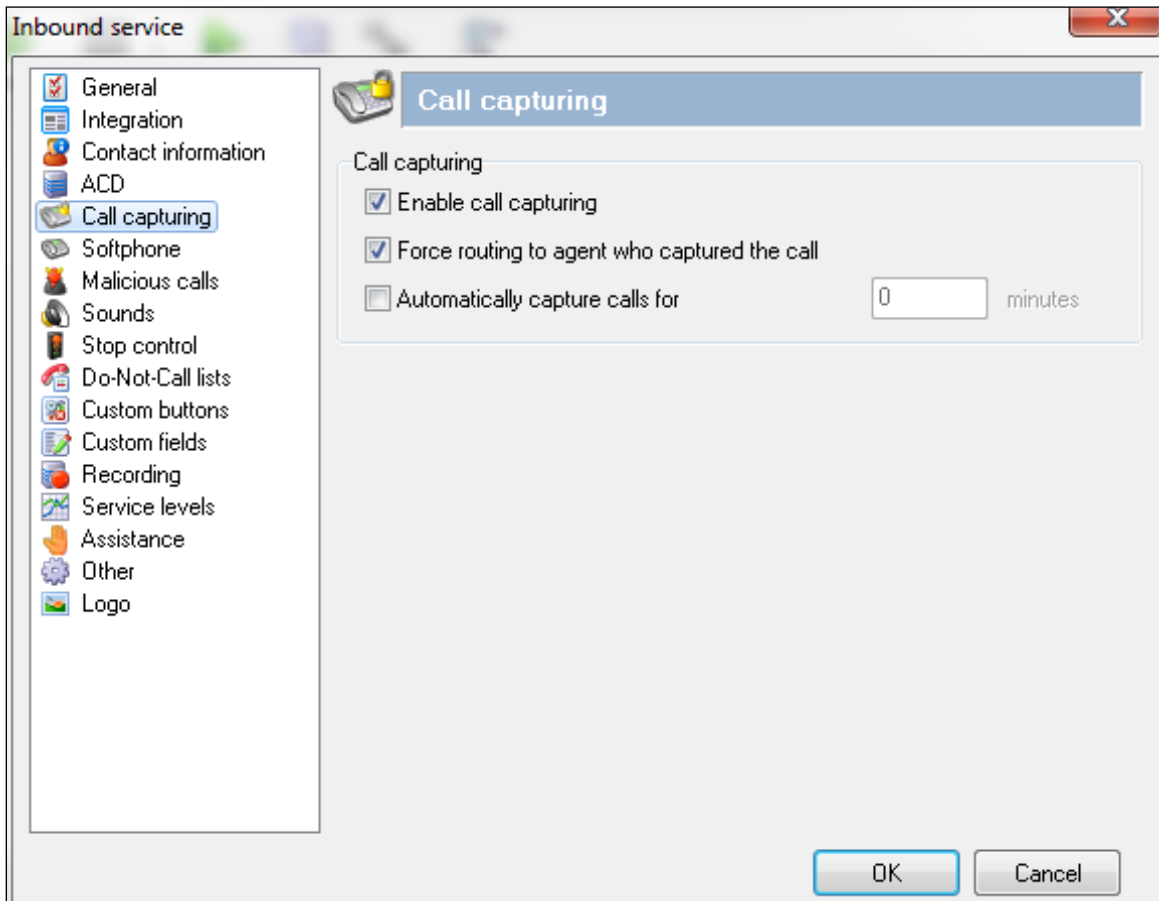
In the resulting screen, select **General** from the menu on the left hand side and enter an **Id** and a **Name** for the inbound service. All other fields are left with their default values.

The screenshot shows a window titled "Inbound service" with a sidebar menu on the left and a main configuration area on the right. The sidebar menu includes the following items: 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 has a "General" tab selected, which contains the following fields: "Id" with the value "100", "Name" with the value "PRESENCE INBOUND", "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 "OK" and "Cancel" buttons.

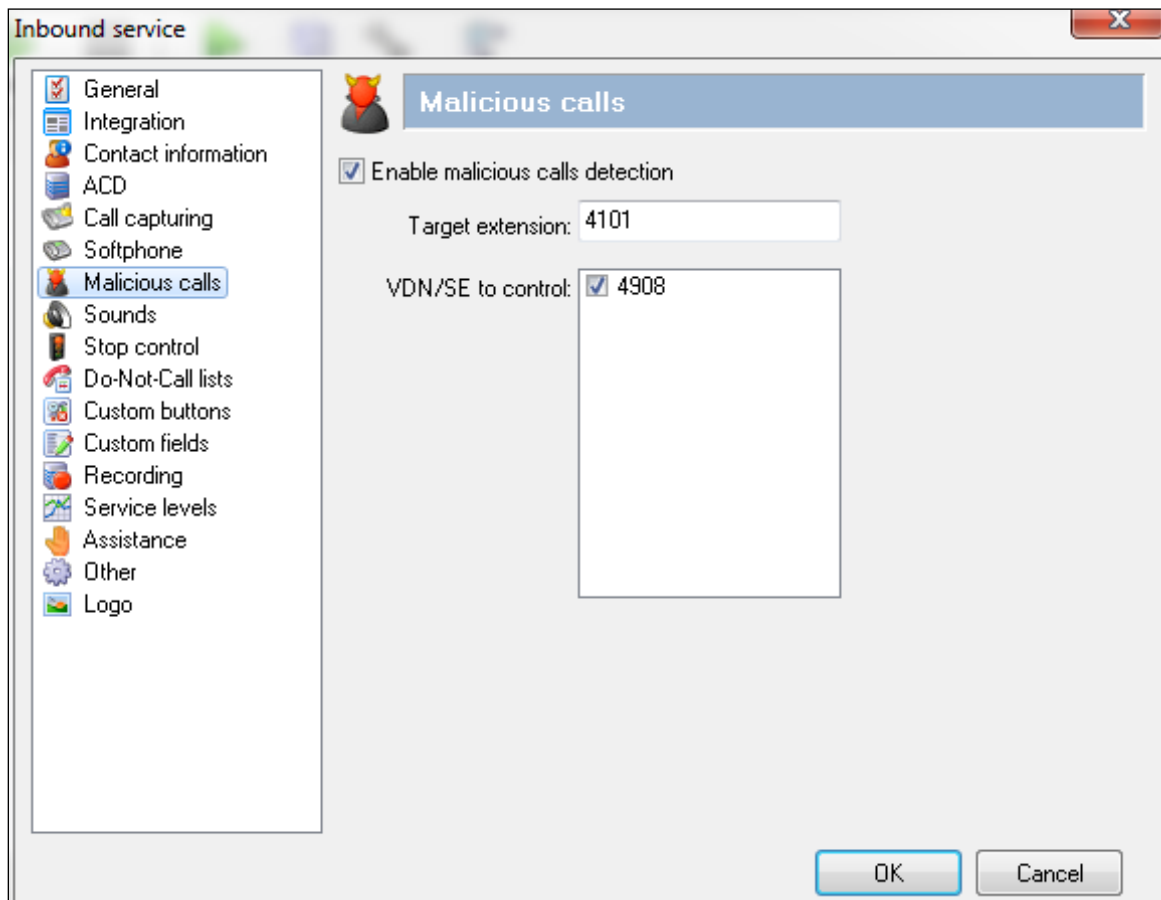
Select **ACD** from the left hand side menu and moving to the right, under the heading **Skills** enter the skill group extensions configured in **Section 5.3.1** that will handle inbound calls in the untitled box (this includes email and web chat call types) and click **Add**. The skill group extensions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



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 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, and the 'Phone no.' field is empty. The 'After-call work' section has checkboxes for 'Minimum after-call work time' and 'Maximum after-call work time', both of which are unchecked, and a dropdown for 'Q. code for maximum time'.

**Inbound service**

**Other**

**After-call work**

☐ Minimum after-call work time:  seconds

☐ Maximum after-call work time:  seconds

Q. code for maximum time:

☐ Use q. code only if contact has not yet been qualified

**Transfer to agents**

☒ Enable direct transfer to agents of this service

Use the following VDN/SE for transfer:

**Outgoing calls identification**

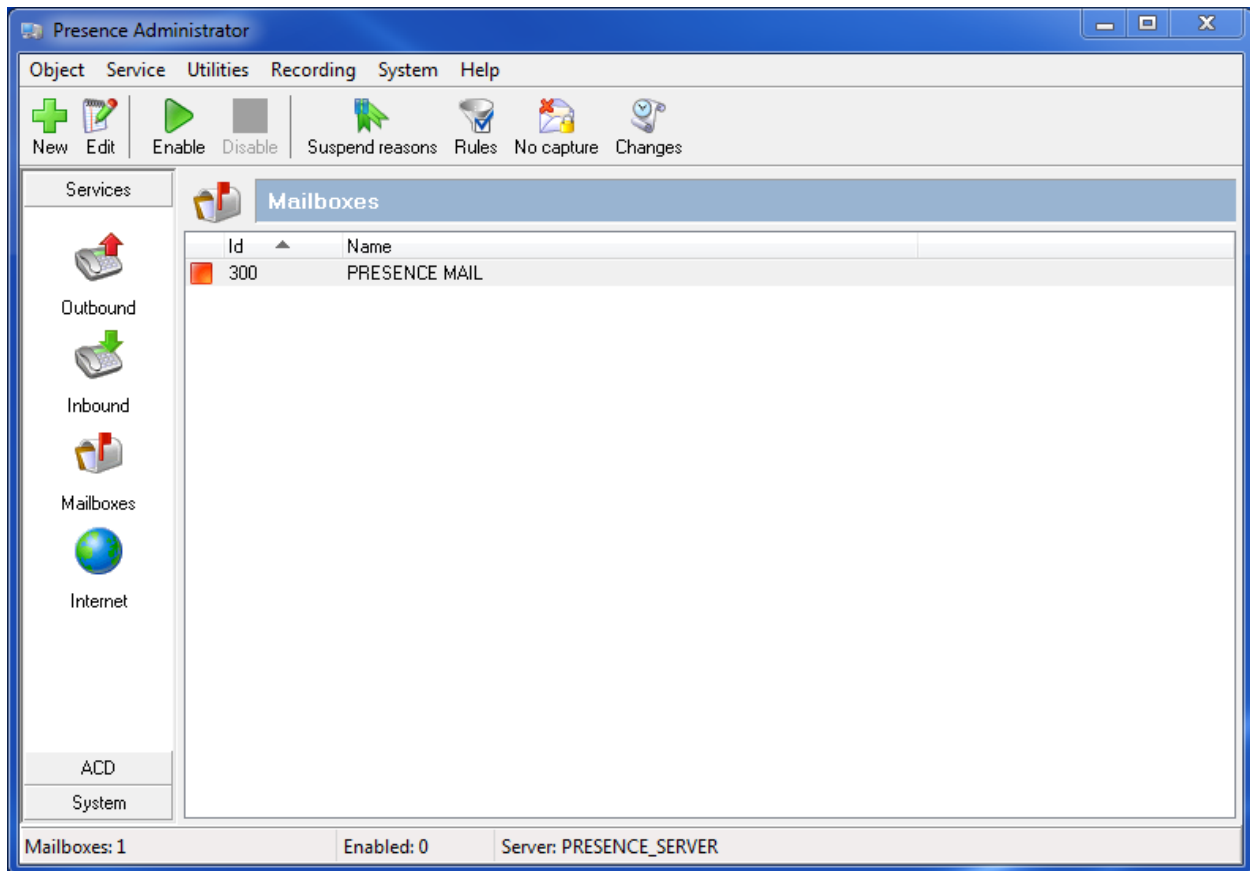
☐ Enable outgoing calls identification

Phone no:

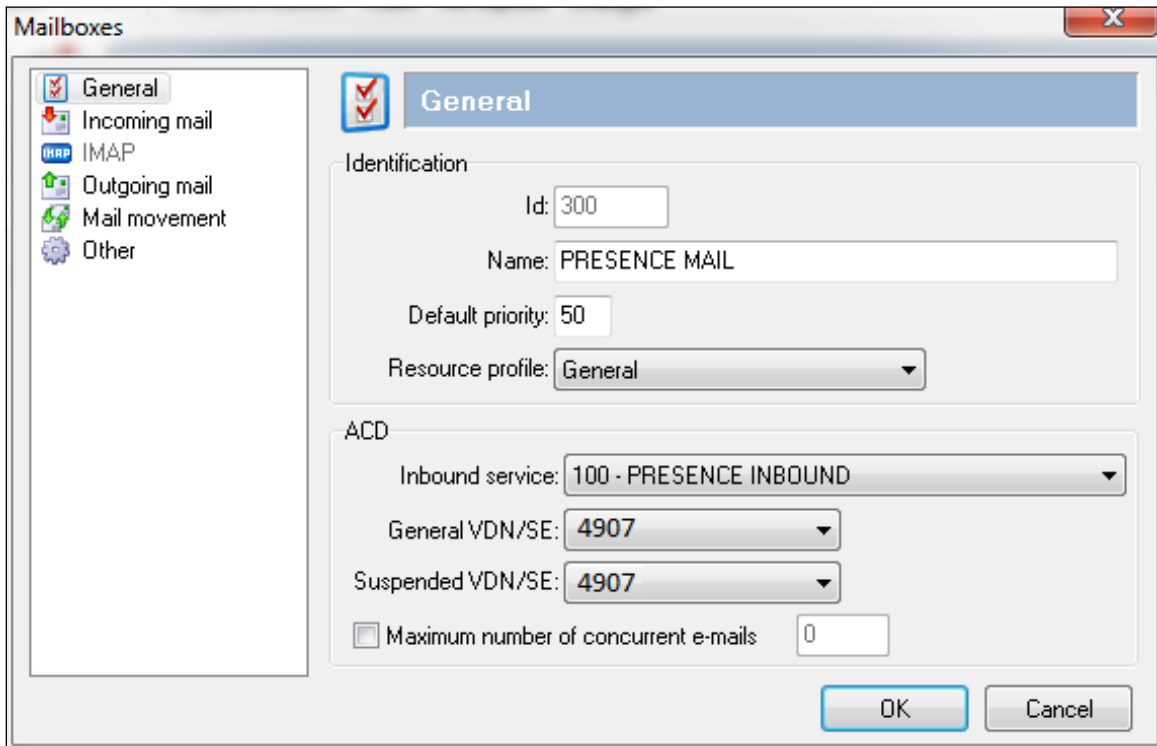
OK Cancel

## 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 an **Id** and 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.



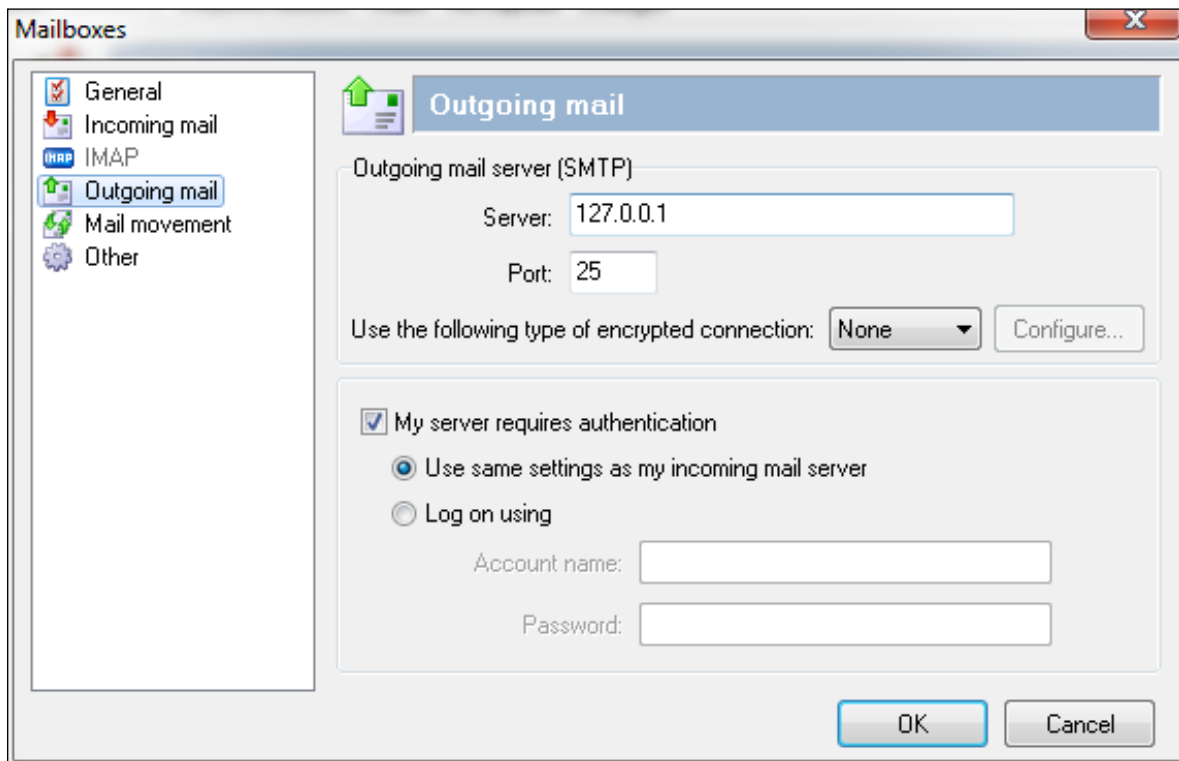
The image shows a 'Mailboxes' configuration window. On the left is a sidebar with a tree view containing: 'General' (checked), 'Incoming mail', 'IMAP', 'Outgoing mail', 'Mail movement', and 'Other'. The main area is titled 'General' and contains two sections: 'Identification' and 'ACD'. In the 'Identification' 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" (selected), "IMAP", "Outgoing mail", "Mail movement", and "Other". 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:" section with a "None" dropdown and 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.

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.



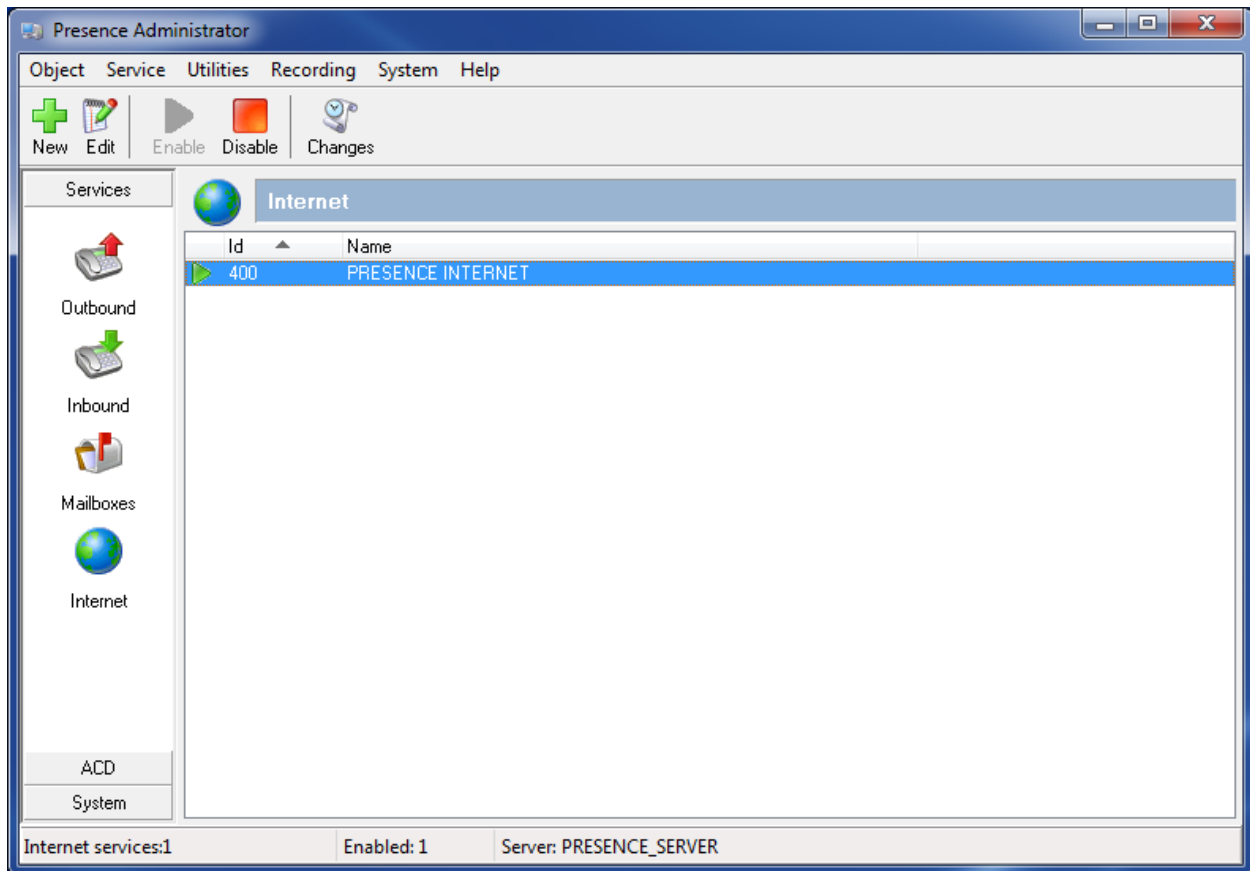
The image shows a Windows-style dialog box titled "Mailboxes" with a close button (X) in the top right corner. On the left is a vertical list of icons and labels: "General" (checkmark), "Incoming mail" (envelope with red arrow), "IMAP" (IMAP icon), "Outgoing mail" (envelope with green arrow, highlighted with a blue selection bar), "Mail movement" (circular arrows), and "Other" (gear). The main area of the dialog is titled "Outgoing mail" with a green arrow icon. It contains the following fields and controls:

- "Outgoing mail server (SMTP)" section:
  - "Server:" text box containing "127.0.0.1"
  - "Port:" text box containing "25"
  - "Use the following type of encrypted connection:" dropdown menu set to "None", with a "Configure..." button to its right.
- Authentication section:
  - Checked checkbox: "My server requires authentication"
  - Radio button (selected): "Use same settings as my incoming mail server"
  - Radio button: "Log on using"
  - Below "Log on using": "Account name:" text box and "Password:" text box.

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

## 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 an **Id** and 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.

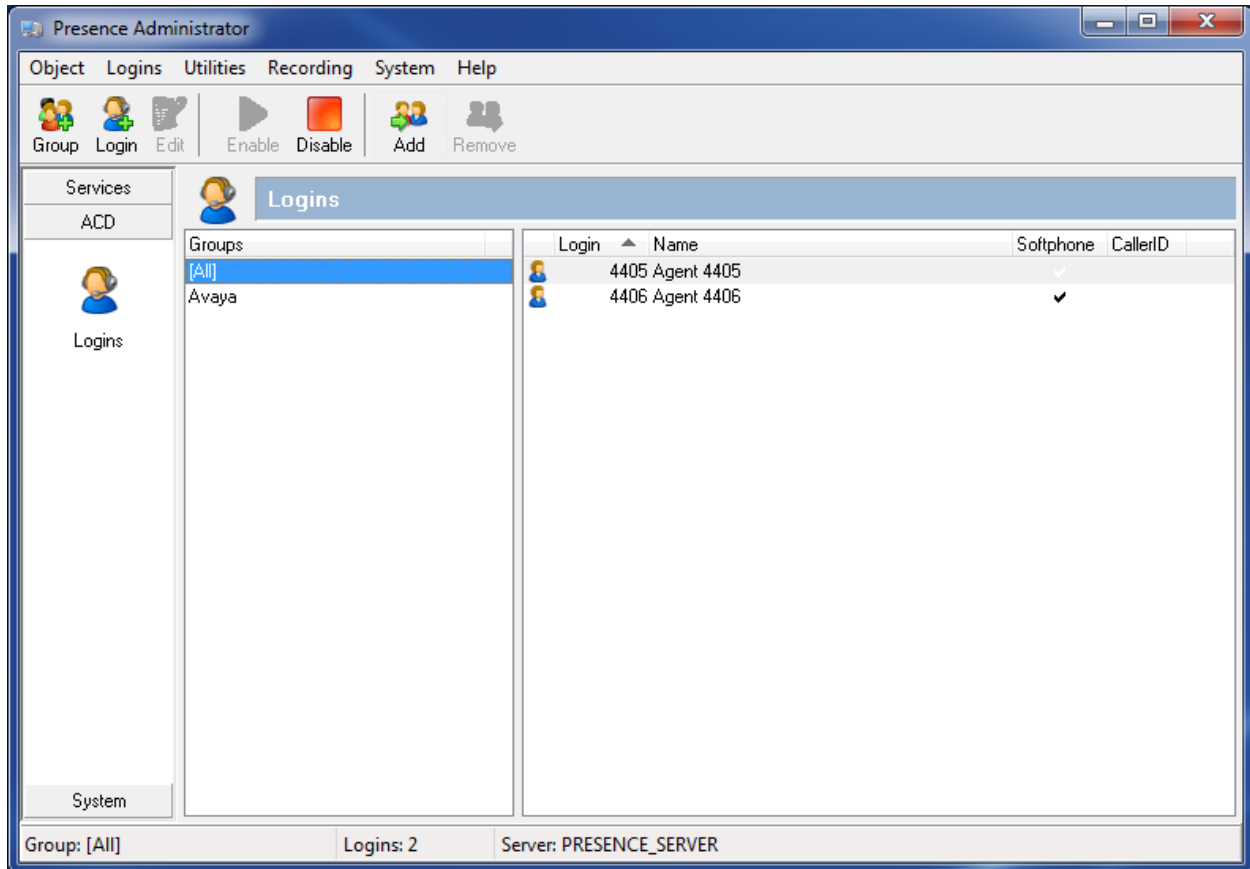
The screenshot shows the 'Internet service' configuration window with the 'General' tab selected. The left sidebar contains a list of categories: General (checked), URL, Interface, Texts, Mail, Service levels, Assistance, and Other. The main area of the window is titled 'General' and contains the following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

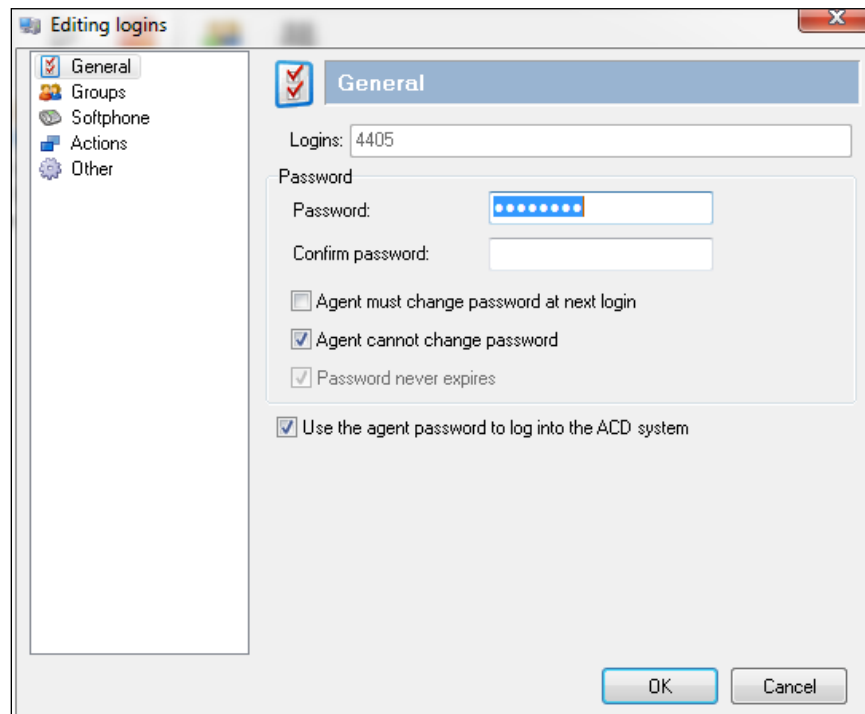
At the bottom right of the window are 'OK' and 'Cancel' buttons.

## 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.

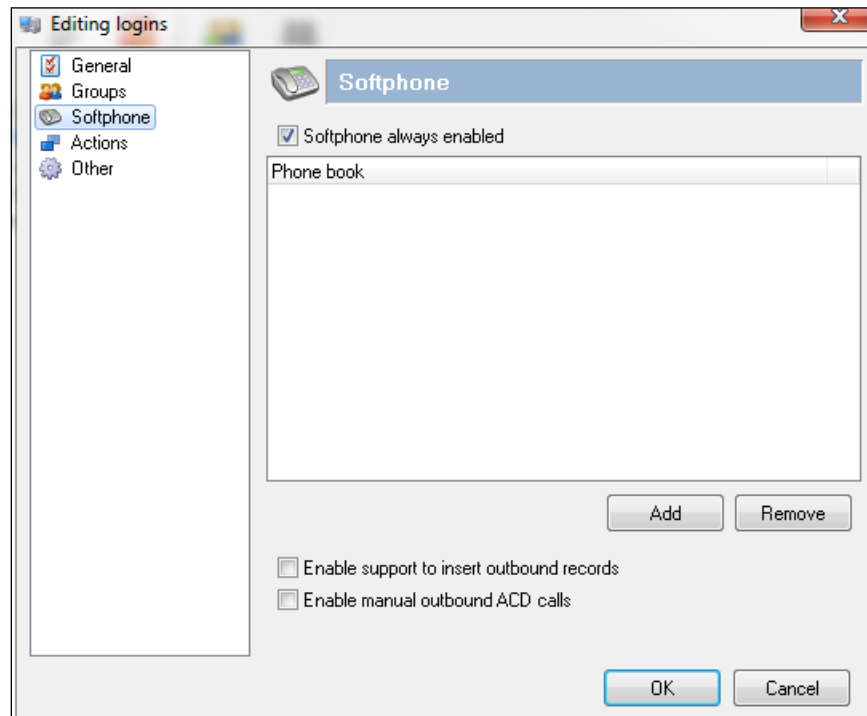


In the **Logins** field, enter a Communication Manager Agent Login ID and a password, as configured in **Section 5.5**. Best practice is to tick **Agent cannot change password** as shown.



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 following checkboxes are visible: 'Agent must change password at next login' (unchecked), 'Agent cannot change password' (checked), 'Password never expires' (checked), and 'Use the agent password to log into the ACD system' (checked). 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 'Editing logins' dialog box with the 'Softphone' tab selected. The 'Softphone always enabled' checkbox is checked. Below it is a 'Phone book' list box. At the bottom right of the list box are 'Add' and 'Remove' buttons. Below these are two unchecked checkboxes: 'Enable support to insert outbound records' and 'Enable manual outbound ACD calls'. The 'OK' and 'Cancel' buttons are at the bottom right.

## 7.3 Configure Presence Recording

Launch the Presence Recording Server configuration application by double clicking the **precservercfg.exe** located in the pre-installed Presence folder on the Presence server (not shown).

### 7.3.1 Presence Recording Server Configuration

Select the **General** option from the menu on the left side of the screen, tick the **Integrated with Presence Server** box and enter the **IP address** of the Presence Server and the port used for connection. Select **DMCC extensions** from the **Channel type** drop-down box.

The screenshot shows the 'Presence Recording Server Configuration' dialog box with the 'General' tab selected. The left sidebar contains a list of configuration categories: General, Backup servers, Storage, Channels, SNMP, Alerts, Tracing, Server, Backup Server, Service, Screen Recording, General, and Tracing. The main area is titled 'General' and contains the following settings:

- ☒ Integrated with Presence Server
- Presence Server**
  - IP address: 10.10.40.128
  - Port: 6100
- Ports**
  - Recording Server: 6111
  - Backup Recording Server: 6120
- Channel type: DMCC extensions (dropdown menu)
- Audio format: G711 (a-Law/u-Law) (dropdown menu)
- Maximum recording duration (in seconds). '0' for unlimited duration: 0
- ☐ Encrypt recording files

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

Click on **Storage** in the left-hand pane and enter an appropriate directory in the **Directory to store recordings** field.

The image shows a 'Presence Recording Server Configuration' dialog box with the 'Storage' tab selected. The left-hand pane contains a tree view with the following items: General, Backup servers, Storage (selected), Channels, SNMP, Alerts, Tracing, Server, Backup Server, Service, Screen Recording, General, and Tracing. The main area of the dialog is titled 'Storage' and contains the following fields and controls:

- 'Time interval of Presence Backup to store recordings on tape (in seconds):' with a text box containing '300'.
- 'Configuration of disk space to store and retrieve recordings' section containing:
  - 'Directory to store recordings:' with a text box containing 'C:\Recordings\rec' and a browse button (...).
  - 'Directory to store retrieved recordings:' with a text box containing 'C:\Recordings\ret' and a browse button (...).
  - 'Alternative directories to search for recordings:' with an empty text box and a browse button (...).
- 'Space for recordings:' with a slider bar set to 80%.
- 'Space for retrieved recordings:' with a value of 10%.
- 'Minimum free space:' with a value of 10%.

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

Click on **Channels** in the left-hand pane. In the **DMCC Server** section enter the IP address of the AES server and the AES user configured for the Presence Suite installation, enter the port configured for connectivity to AES (the default is **4721**). In the **DMCC channel configuration** section, click **Add**.

The screenshot shows the 'Presence Recording Server Configuration' dialog box with the 'Channels' tab selected. The left-hand pane lists various configuration categories, with 'Channels' highlighted. The main area is divided into two sections: 'DMCC Server' and 'DMCC channel configuration'.

**DMCC Server** section:

- IP address: 10.10.40.56
- User: presence
- Password: (masked with dots)
- Port: 4721

**DMCC channel configuration** section:

- Base port to receive RTP packets: 50000
- A table with columns: Extension, Usage, CLAN IP address.
- Buttons: Up ↑, Down ↓, Add, Edit, Remove.

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

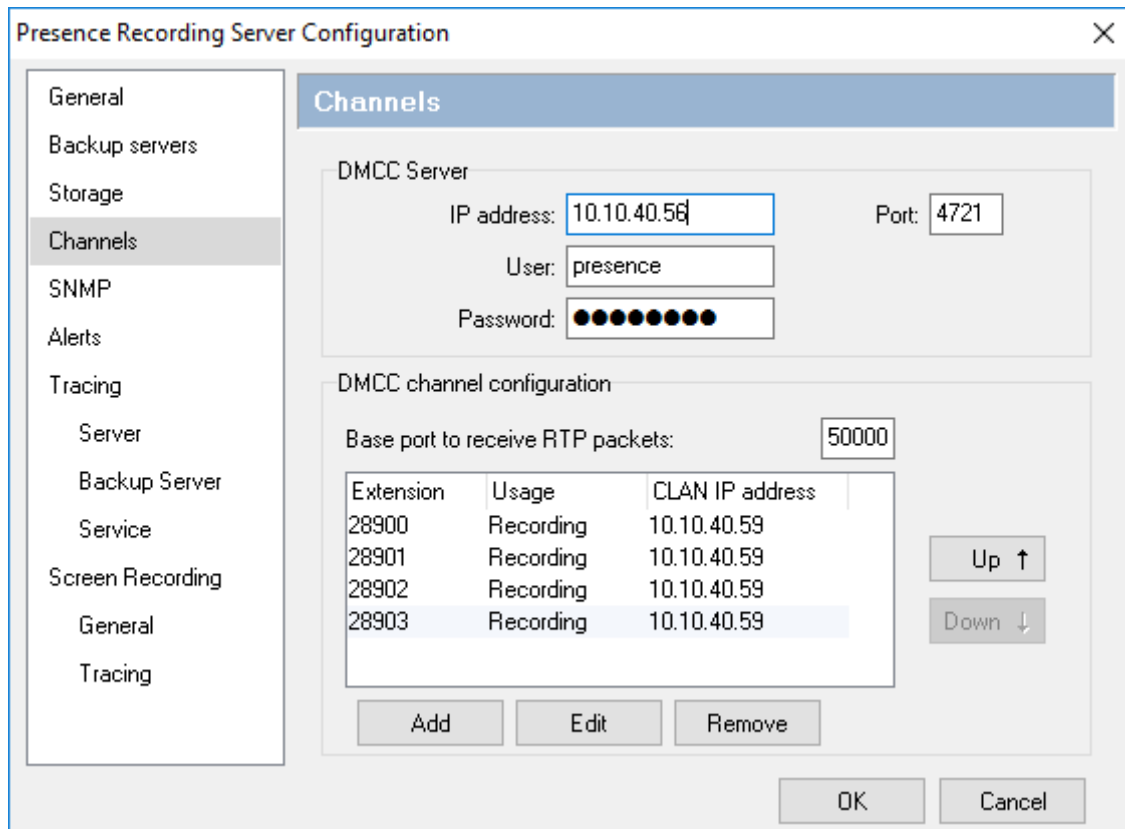
Enter a valid recording channel **Extension** and **Password** as configured in **Section 5.13**. Enter the **CLAN IP address** and select **Recording** from the **Usage** drop-down box. Click **OK** when done. Repeat as necessary. For playback channels, select **Playback** from the **Usage** drop-down box.

The screenshot shows the 'Channel' dialog box with the 'Channel information' tab selected. The fields are as follows:

- Extension: 28903
- Password: (masked with dots)
- Usage: Recording (selected from a drop-down menu)
- CLAN IP address: 10.10.40.59

At the bottom are 'OK', 'Cancel', and 'Apply' buttons.

The screen shown below will appear, displaying all recording and playback channels, click **OK** when done.



The screenshot shows the 'Presence Recording Server Configuration' window with the 'Channels' tab selected. The left sidebar contains a tree view with the following items: General, Backup servers, Storage, Channels (selected), SNMP, Alerts, Tracing, Server, Backup Server, Service, Screen Recording, General, and Tracing. The main area is divided into two sections: 'DMCC Server' and 'DMCC channel configuration'. The 'DMCC Server' section has fields for IP address (10.10.40.56), Port (4721), User (presence), and Password (masked with dots). The 'DMCC channel configuration' section has a field for 'Base port to receive RTP packets' (50000) and a table of channels. The table has three columns: Extension, Usage, and CLAN IP address. It lists four channels: 28900, 28901, 28902, and 28903, all with 'Recording' usage and '10.10.40.59' CLAN IP address. To the right of the table are 'Up' and 'Down' buttons. Below the table are 'Add', 'Edit', and 'Remove' buttons. At the bottom right are 'OK' and 'Cancel' buttons.

**Presence Recording Server Configuration**

**Channels**

DMCC Server

IP address: 10.10.40.56 Port: 4721

User: presence

Password: ●●●●●●●●

DMCC channel configuration

Base port to receive RTP packets: 50000

| Extension | Usage     | CLAN IP address |
|-----------|-----------|-----------------|
| 28900     | Recording | 10.10.40.59     |
| 28901     | Recording | 10.10.40.59     |
| 28902     | Recording | 10.10.40.59     |
| 28903     | Recording | 10.10.40.59     |

Up ↑

Down ↓

Add Edit Remove

OK Cancel

### 7.3.2 Configure Recording Plan for Inbound Service

Recording plans must be configured according to the call recordings required. This plan is created for the inbound calls to agents.

Using the Presence Web Supervisor, click on **Administration** → **Recording** → **Plans** → **New** (not shown). In the displayed window, assign an identifying **Name** and set the **Percentage to record** as required, in this case **100%**. Configure the **Start** and **End** parameters as appropriate.

The screenshot shows the 'Plan INBOUND 100' dialog box with the 'General' tab selected. The left-hand pane shows 'General', 'Services', and 'Groups'. The 'General' tab contains the following fields and options:

- Name:** INBOUND 100
- Resource profile:** General
- Percentage to record:** General, 100 %
- Start:** ☐ Immediate ☒ Date 16/11/2017 16:18
- End:** ☒ Indeterminate ☐ Date
- ☒ Allow the agent to pause recordings
- ☒ Allow the agent to stop recordings

Buttons at the bottom: OK, Cancel, Apply.

Click on **Services** in the left-hand pane, enter the inbound service identifier in the **Service ID** box and click the plus icon.

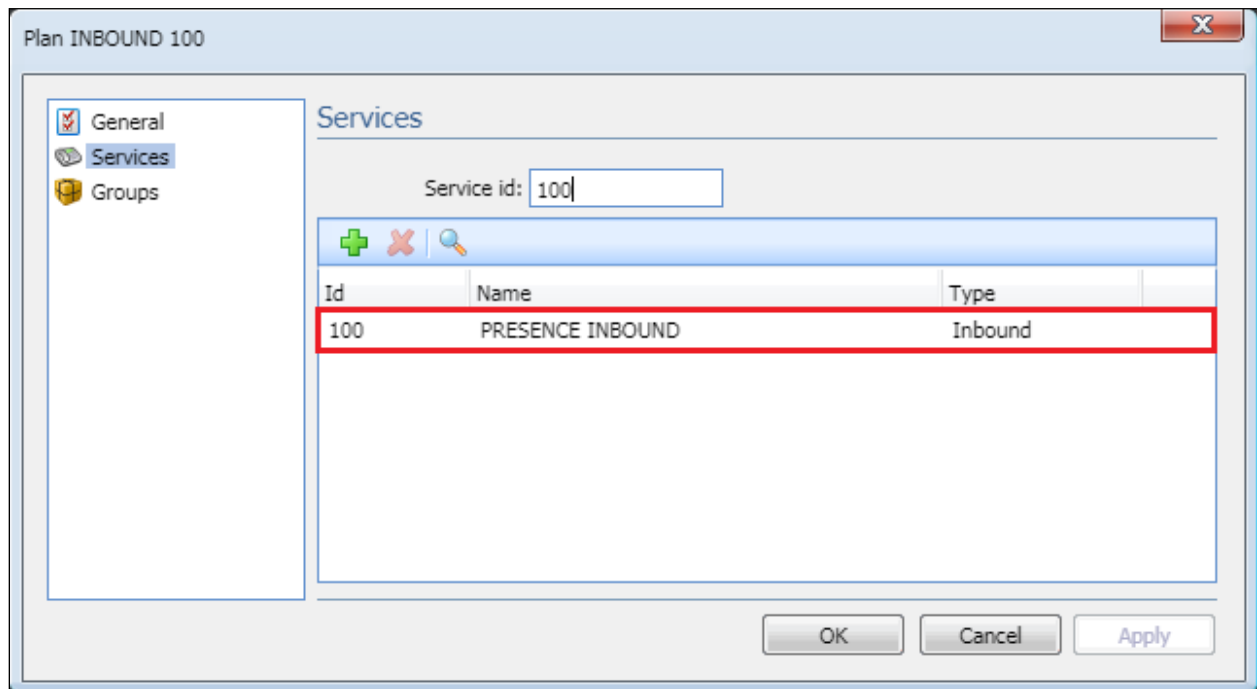
The screenshot shows the 'Plan INBOUND 100' dialog box with the 'Services' tab selected. The left-hand pane shows 'General', 'Services', and 'Groups'. The 'Services' tab contains the following fields and options:

- Service id:** 100
- Buttons:** +, -, 🔍
- Table:**

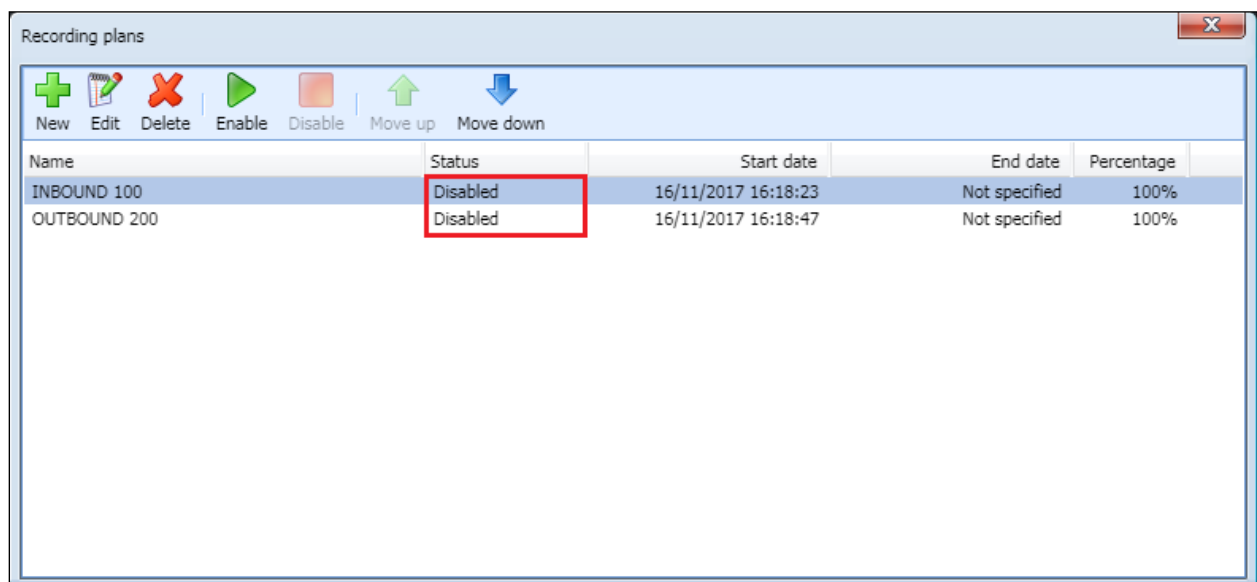
| Id | Name | Type |
|----|------|------|
|----|------|------|

Buttons at the bottom: OK, Cancel, Apply.

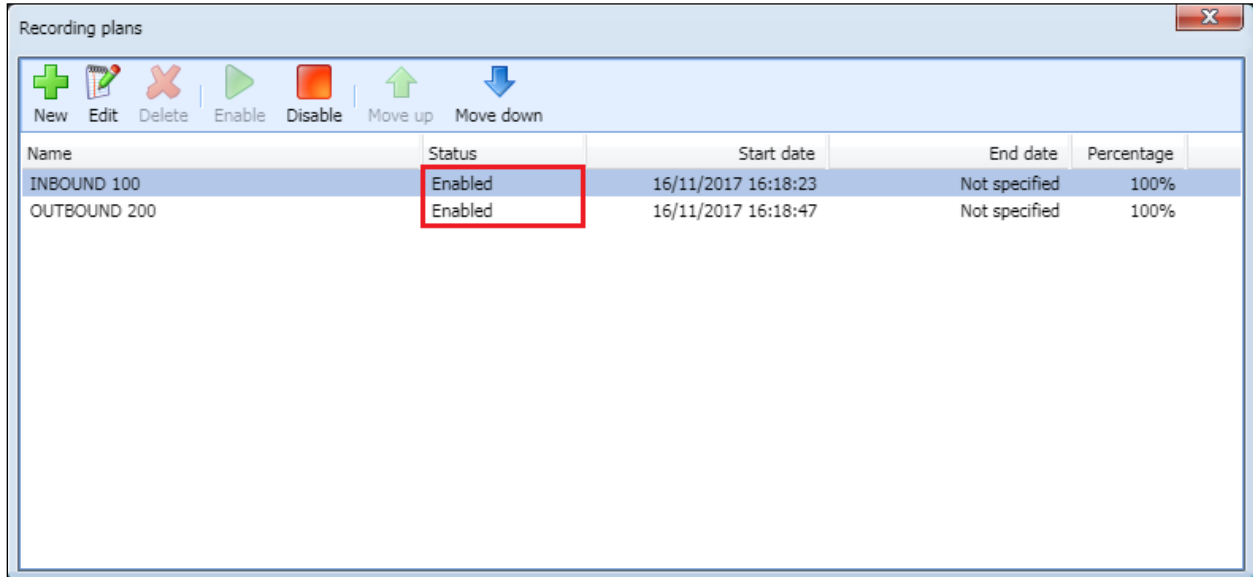
This will add the relevant configured service to the recording plan, in this case **PRESENCE INBOUND**. Click **OK** when done. Repeat as necessary for additional recording plans.



The screen below will be displayed, summarizing the added recording plans. Note that the status shows **Disabled**.



Select each one in turn and click **Enable**, the status will now appear as **Enabled**.



| Name         | Status  | Start date          | End date      | Percentage |
|--------------|---------|---------------------|---------------|------------|
| INBOUND 100  | Enabled | 16/11/2017 16:18:23 | Not specified | 100%       |
| OUTBOUND 200 | Enabled | 16/11/2017 16:18:47 | Not specified | 100%       |

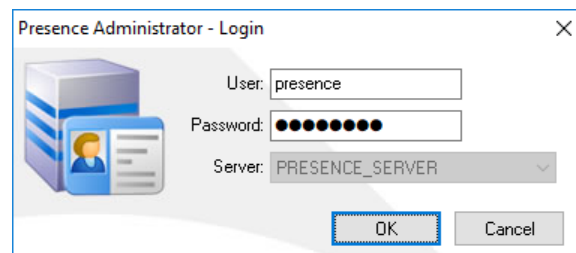
Calls that are placed via either of these services will be recorded according to the recording plan configured above.

### 7.3.3 Add stations to Presence Recording

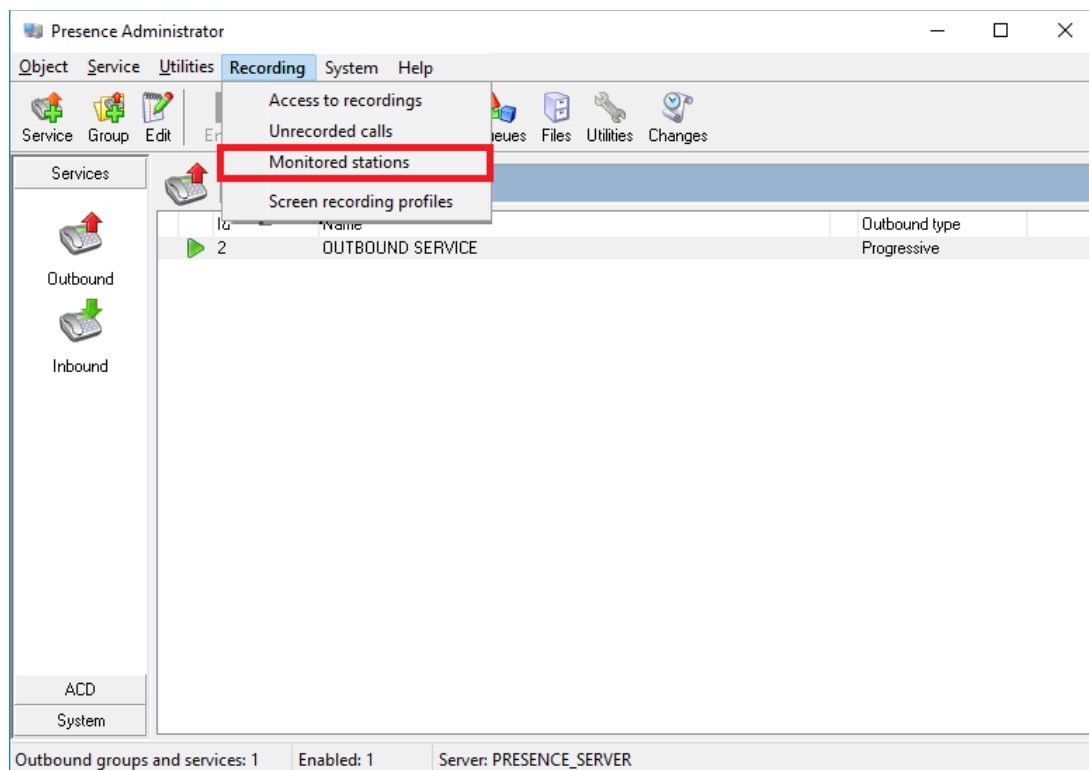
To record non-agent stations, each station that is to be recorded must be added to Presence Recording. Create a recording group adding these stations and finally create a recording plan adding this group.

**Note:** In the example below extensions 8270001 and 8270002 are added to be recorded by Presence Recording.

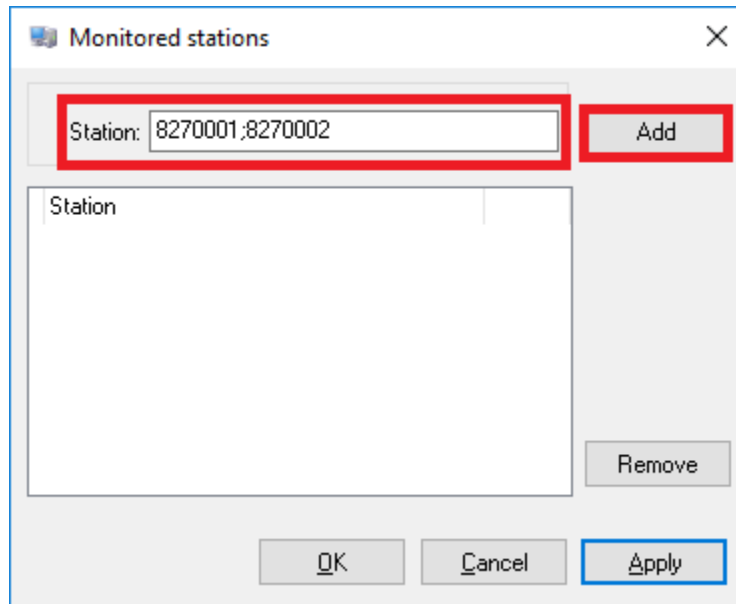
Launch the **Presence Administrator** application by double clicking the **pcoadmin.exe** located in the Presence folder (not shown). The username and password that appear in the **User** and **Password** fields are created during the Presence server installation.



Select **Recording** → **Monitored stations** from the Presence Administrator menu. Calls that are placed via either of these stations will be recorded according to the recording plan configured in **Section 7.3.5**.



In the resulting screen, add both stations in the **Station** field and click **Add**.



Monitored stations

Station: 8270001;8270002

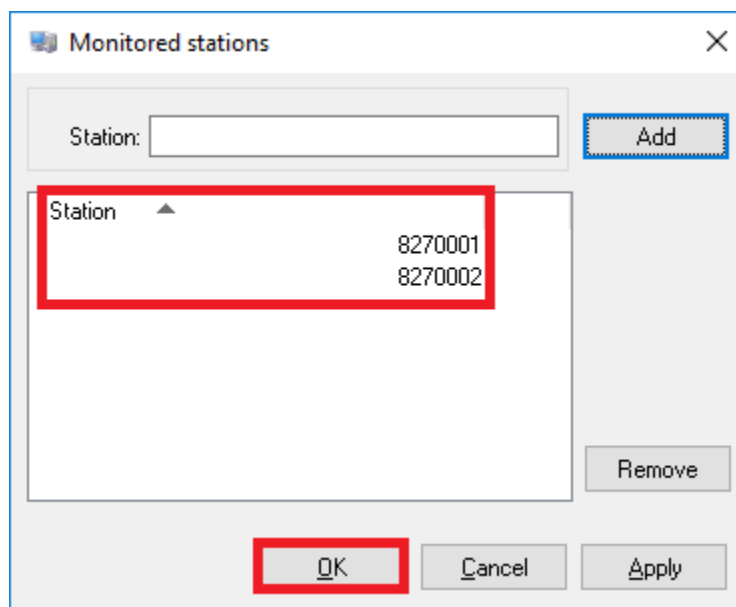
Add

Station

Remove

OK Cancel Apply

Then click **OK** to add the stations into Presence Recording and close the screen.



Monitored stations

Station:

Add

Station ▲

8270001

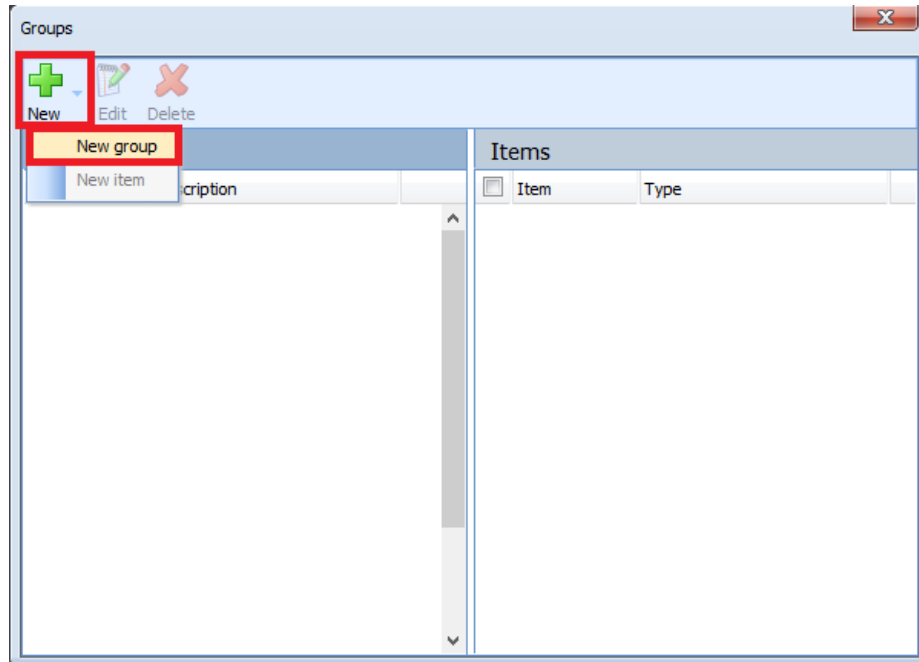
8270002

Remove

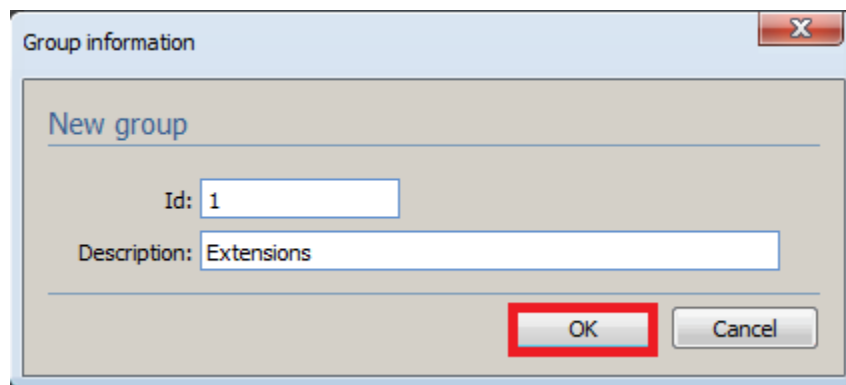
OK Cancel Apply

### 7.3.4 Create a new recording group

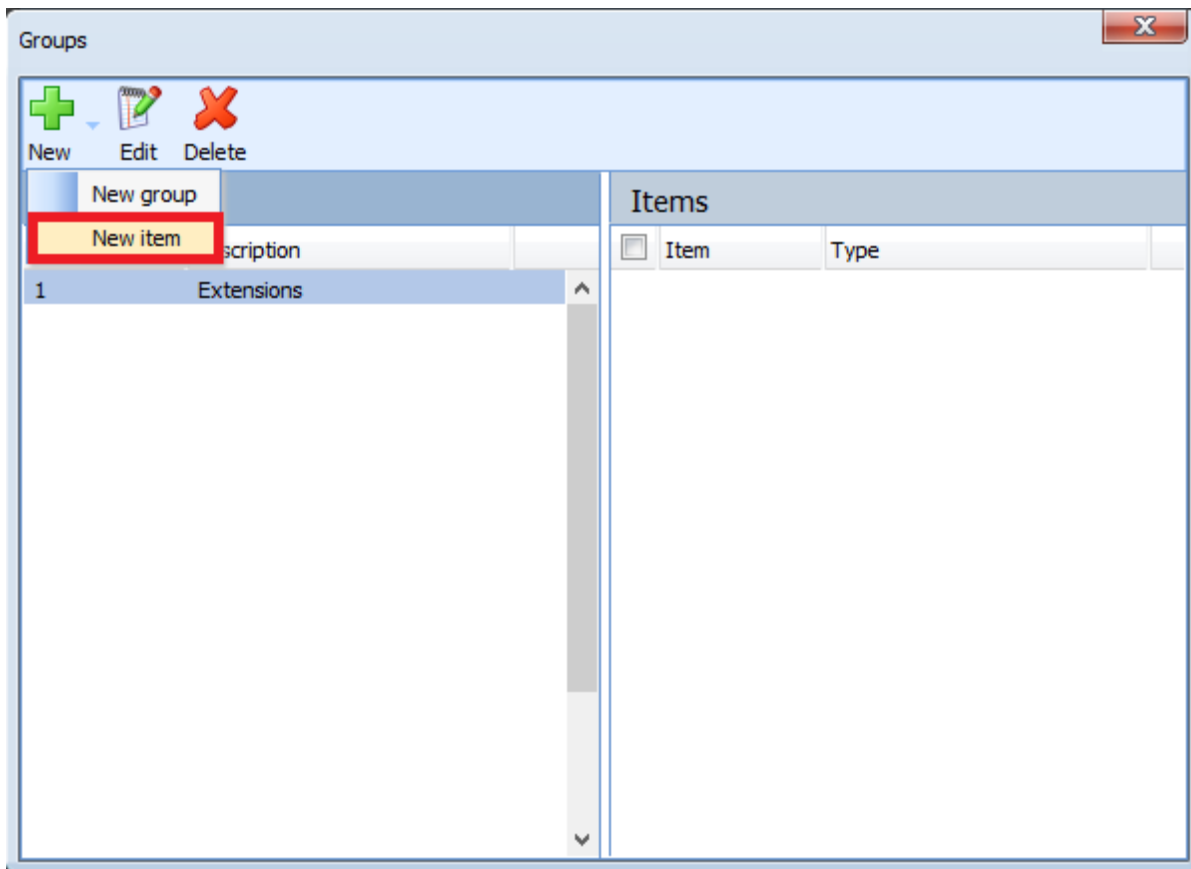
Using the Presence Web Supervisor application, double click on **Administration** → **Recording** → **Groups** and click on **New** (drop-down box) and select **New group**.



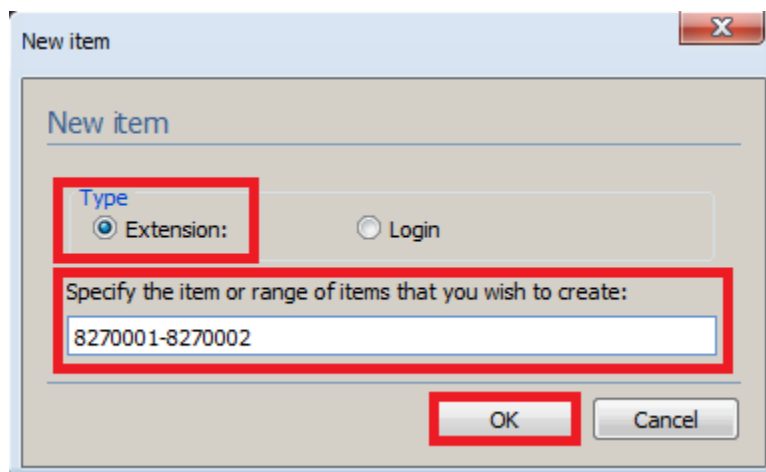
Enter the details for the new group. Note any number is used for code. Click on **OK** when finished.



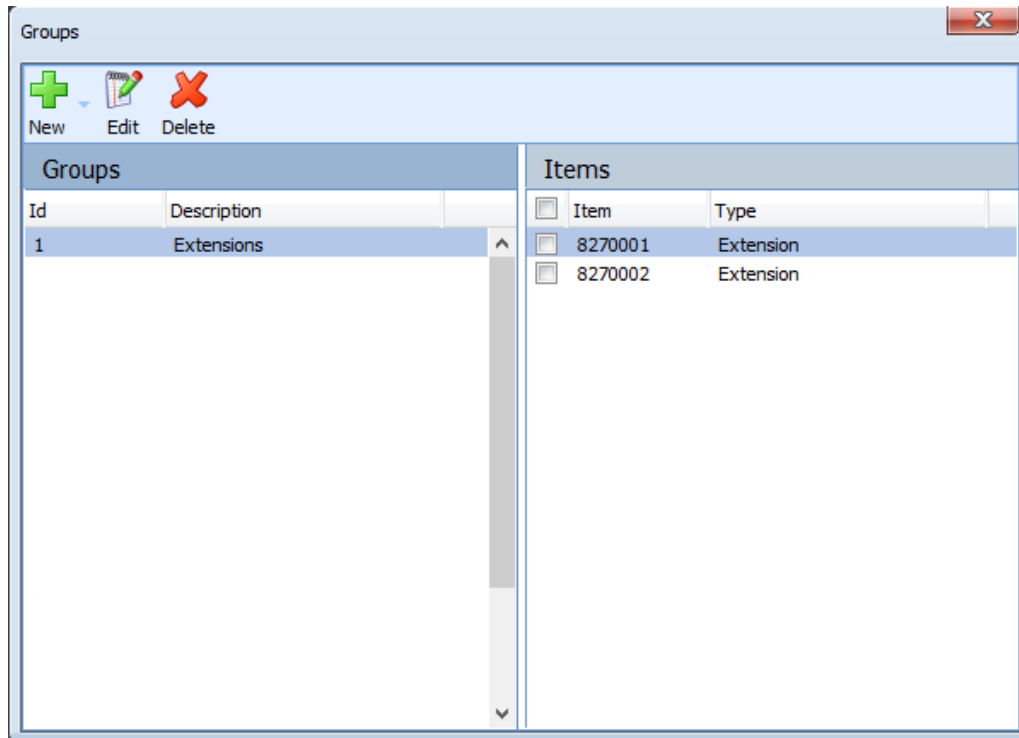
Select the group created and click on **New** (drop-down box) and select **New item**.



Select **Extension** as the **Type** and the extensions to be added. Click on **OK** once done.

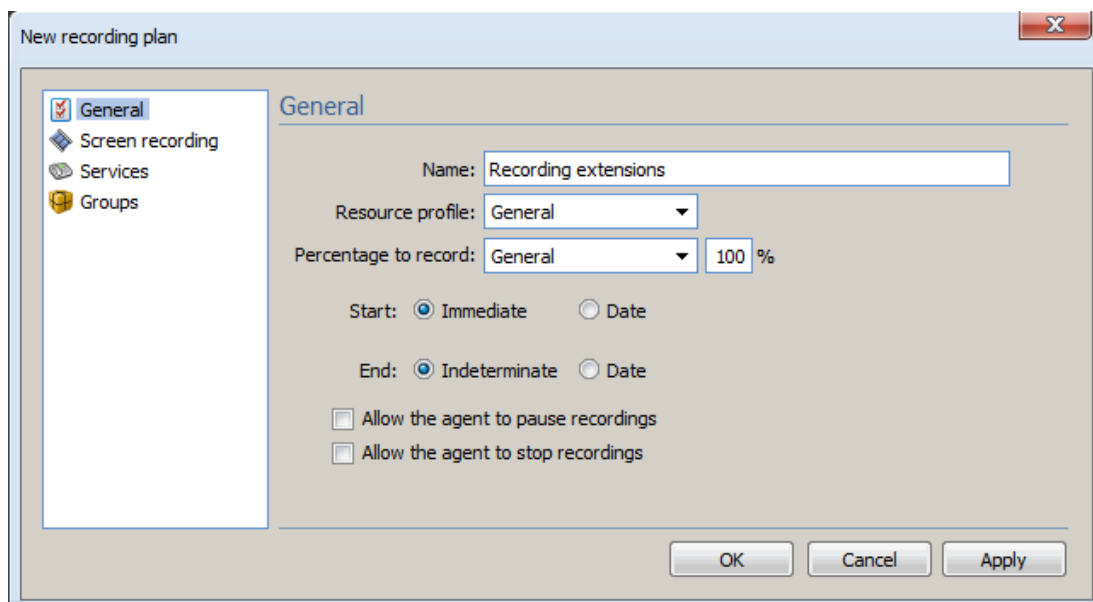


Once **OK** is clicked above the following screen shows the added stations.

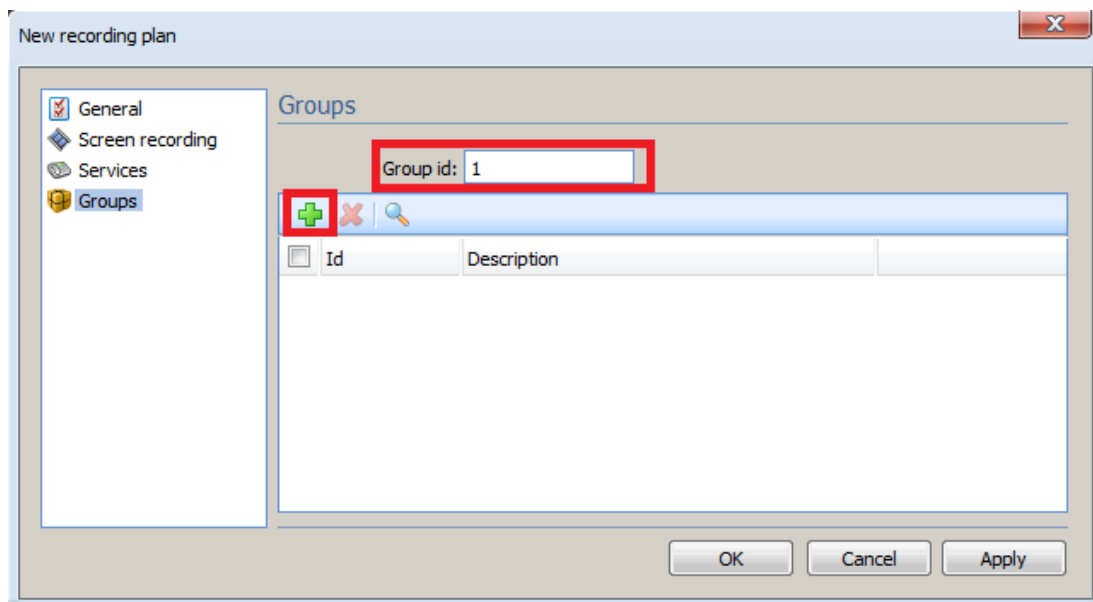


### 7.3.5 Create a recording plan for extensions

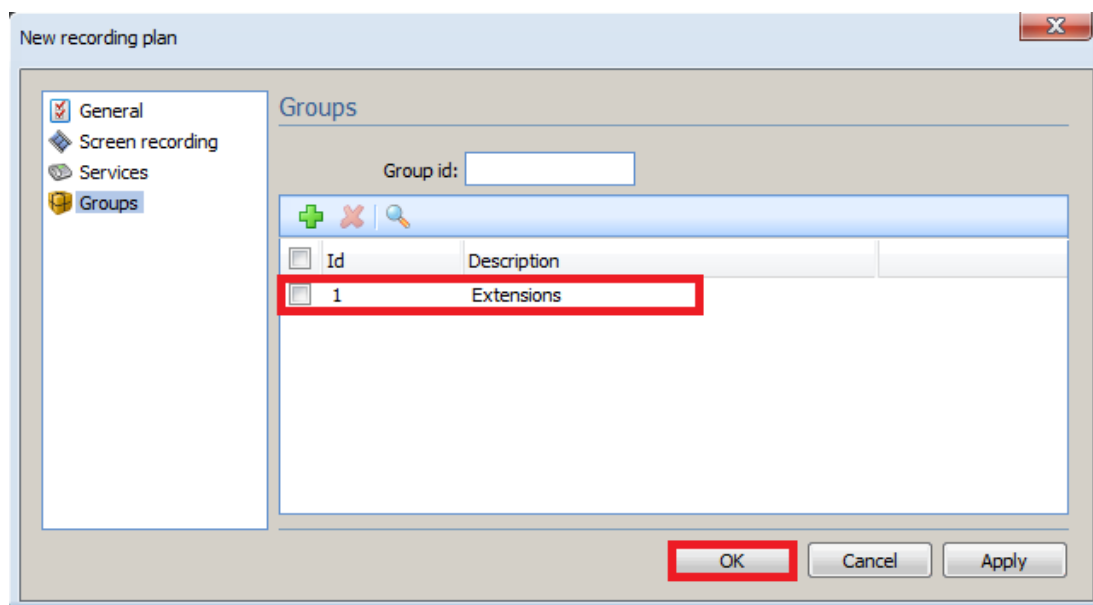
Double click on **Administration** → **Recording** → **Plans** → **New** (not shown). In the displayed **New recording plan** window, enter a **Name**, the **Resource profile** is pre-selected, **Percentage to record** is set to **100%**. **Start** and **End** is set to **Immediately** and **Indeterminate** respectively. Click on **OK** once done.



On the **Groups** window set the **Group id** created click on the Add icon.



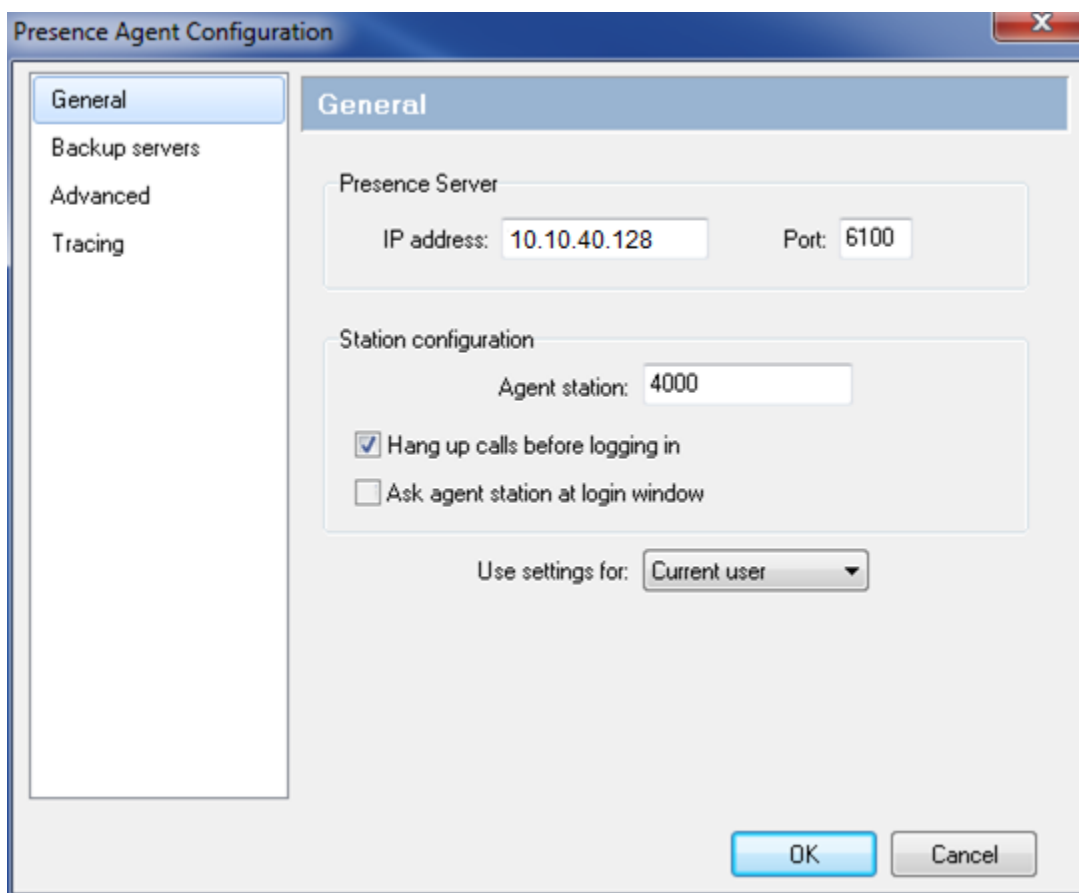
Click on **OK** to create the recording plan.



In the screen that display the added recording plans (not shown), select the recording plan created and click **Enable**, the status will now appear as **Enabled**.

## 7.4 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 **10.10.40.128**. 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** check box. 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.



Presence Agent Configuration

General

Backup servers

Advanced

Tracing

General

Presence Server

IP address: 10.10.40.137 Port: 6100

Station configuration

Agent station: 4000

☒ Hang up calls before logging in

☐ Ask agent station at login window

Use settings for: Current user


OK Cancel

## Verification Steps

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

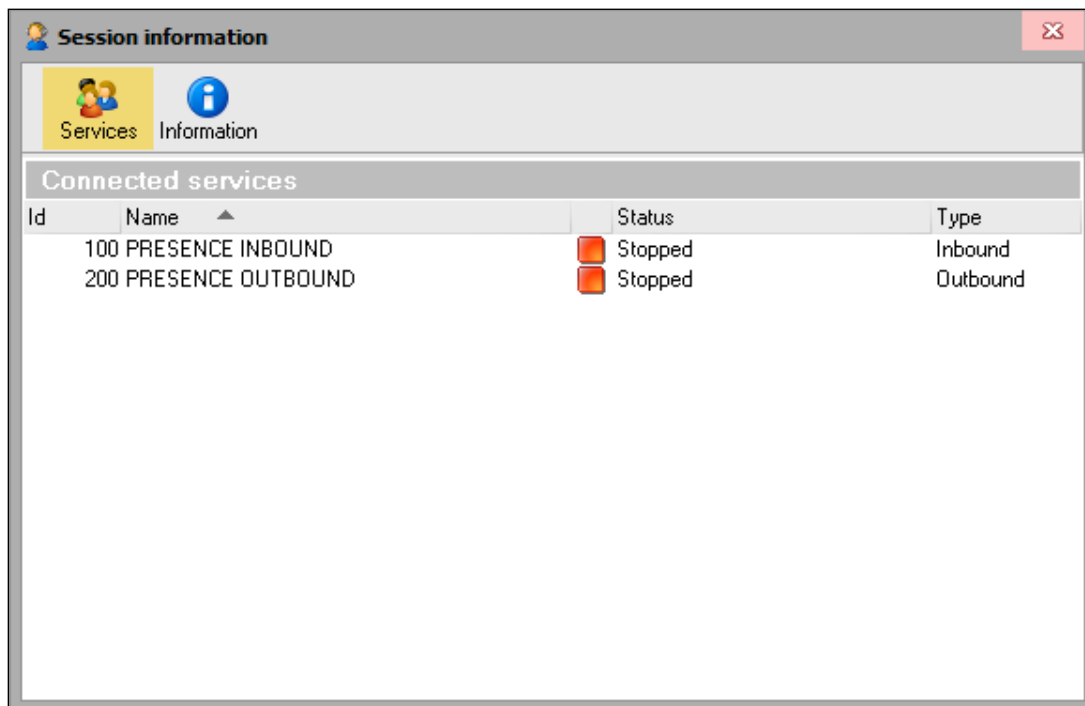
### 8.1 Verify Presence Suite

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 a login dialog box for the Presence Agent. It features the 'Presence Agent Version 11.0' logo on the left and the 'presence suite' logo on the right. The dialog contains three input fields: 'Login:' with the value '4405', 'Password:' with four masked dots, and 'Station:' with the value '4000'. At the bottom right, 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 a 'Session information' window with a tabbed interface. The 'Services' tab is selected, displaying a table of connected services. The 'Information' tab is also visible. The table has columns for Id, Name, Status, and Type.

| 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.

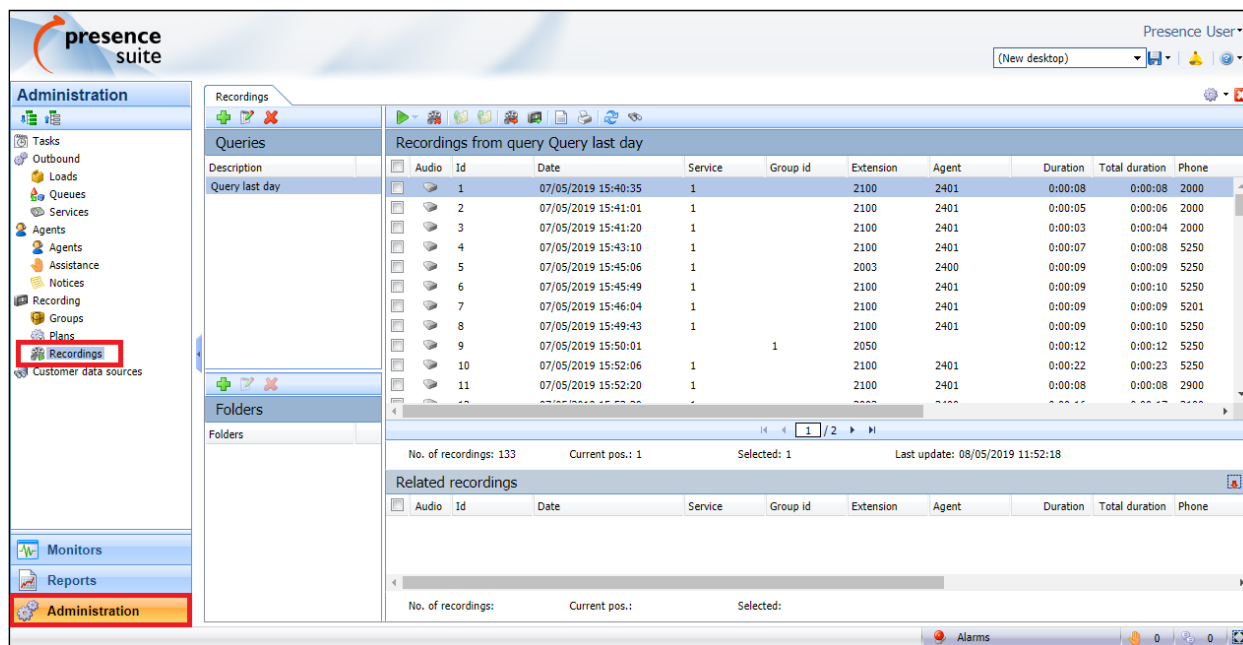


An outbound call is placed and answered.

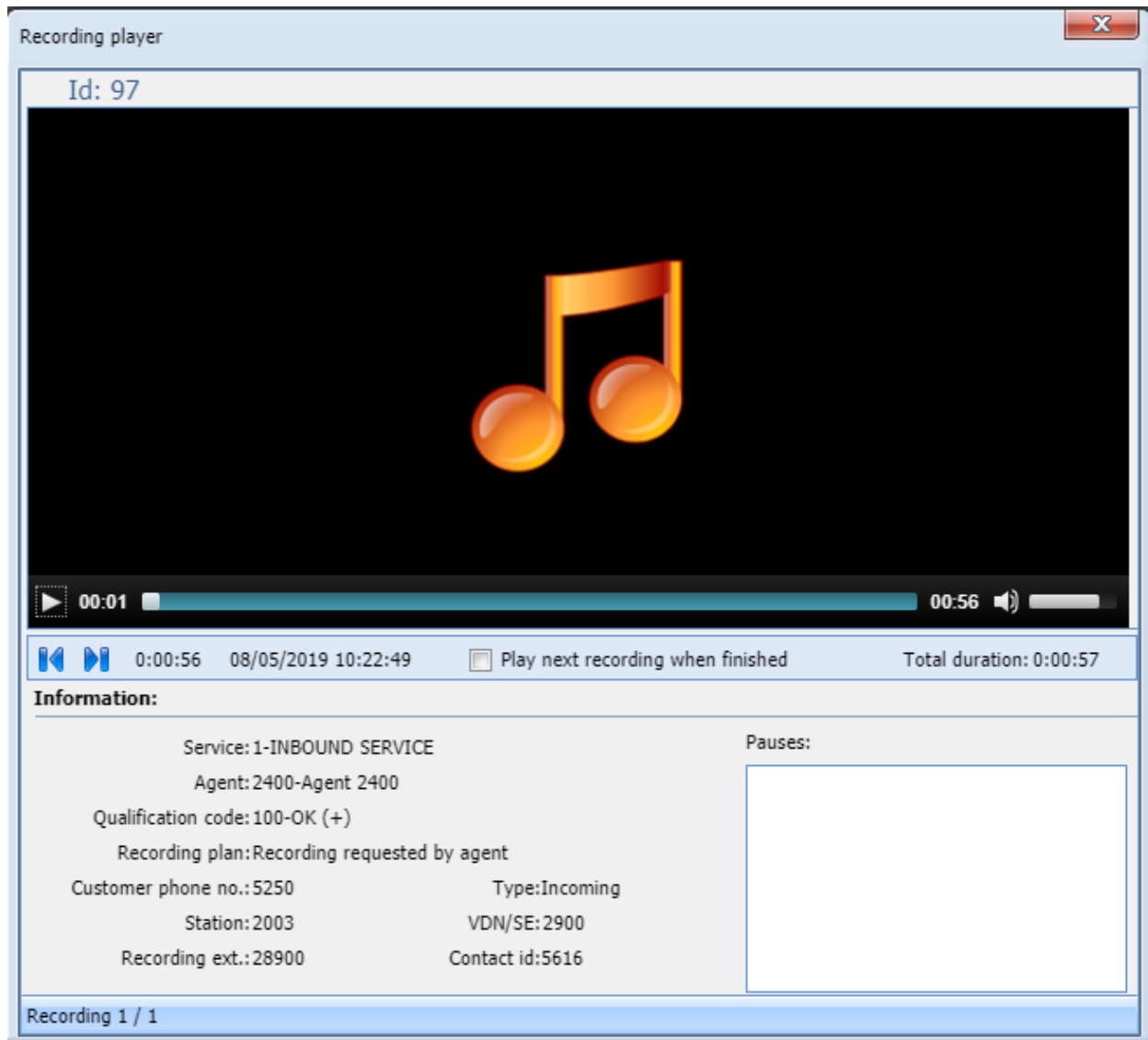


## 8.2 Verify Presence Recording

Using Presence Web Supervisor, click **Administration** → **Recording** → **Recordings**, visually verify correct recording detail as shown below. Select a recording and click on Play audio only in browser to be played, the audio will be played in the computer.



The audio will be played in the computer. The screen below will be displayed allowing playback control.



### 8.3 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**.

|                               |         |          |                    |                      |           |      |
|-------------------------------|---------|----------|--------------------|----------------------|-----------|------|
| <b>status aesvcs cti-link</b> |         |          |                    |                      |           |      |
| AE SERVICES CTI LINK STATUS   |         |          |                    |                      |           |      |
| CTI Link                      | Version | Mnt Busy | AE Services Server | <b>Service State</b> | Msgs Sent | Rcvd |
| 1                             | 8       | no       | aes80vmpg          | <b>established</b>   | 87        | 61   |

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

|                                |          |                       |                  |
|--------------------------------|----------|-----------------------|------------------|
| <b>status aesvcs interface</b> |          |                       |                  |
| AE SERVICES INTERFACE STATUS   |          |                       |                  |
| <b>Local Node</b>              | Enabled? | Number of Connections | Status           |
| procr                          | yes      | 1                     | <b>listening</b> |

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**.

|                           |                    |             |             |              |            |            |
|---------------------------|--------------------|-------------|-------------|--------------|------------|------------|
| <b>status aesvcs link</b> |                    |             |             |              |            |            |
| AE SERVICES LINK STATUS   |                    |             |             |              |            |            |
| Srvr/ Link                | AE Services Server | Remote IP   | Remote Port | Local Node   | Msgs Sent  | Rcvd       |
| 01/01                     | aes80vmpg          | 10.10.40.56 | 57650       | <b>procr</b> | <b>683</b> | <b>665</b> |

## 8.4 Verify TSAPI Link and DMCC

This section will verify both the TAPI and DMCC links.

### 8.4.1 Verify TSAPI Link

On the AES 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**.

**TSAPI Link Details**

☐ Enable page refresh every 60 seconds

|                                  | Link | Switch Name | Switch CTI Link ID | Status  | Since                    | State  | Switch Version | Associations | Msgs to Switch | Msgs from Switch | Msgs Period |
|----------------------------------|------|-------------|--------------------|---------|--------------------------|--------|----------------|--------------|----------------|------------------|-------------|
| <input checked="" type="radio"/> | 1    | cm80vmpg    | 1                  | Talking | Mon Jan 28 11:08:16 2019 | Online | 18             | 11           | 632            | 657              | 30          |

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

### 8.4.2 Verify Avaya Aura® Application Enablement Services DMCC Service

The following steps are carried out on AES to validate that the communication link between AES and the Presence Recording server is functioning correctly. Verify the status of the DMCC service by selecting **Status** → **Status and Control** → **DMCC Service Summary**. The **DMCC Service Summary – Session Summary** screen is displayed as shown below. It shows a connection to the Presence server, IP address **10.10.40.128**. The **Application** is shown as **cmapiApplication**, and the **Far-end Identifier** is given as the IP address **10.10.40.128** as expected. The **User** is shown as the user created for the CTI user for Presence Recording.

**DMCC Service Summary - Session Summary**

Please do not use back button

☐ Enable page refresh every 60 seconds

Session Summary [Device Summary](#)

Generated on Tue Feb 26 10:36:12 GMT 2019

Service Uptime: 28 days, 23 hours 26 minutes

Number of Active Sessions: 1

Number of Sessions Created Since Service Boot: 2

Number of Existing Devices: 10

Number of Devices Created Since Service Boot: 20

|                                     | Session ID                          | User     | Application      | Far-end Identifier | Connection Type | # of Associated Devices |
|-------------------------------------|-------------------------------------|----------|------------------|--------------------|-----------------|-------------------------|
| <input checked="" type="checkbox"/> | AC98198E9ED3A664D-839EC412A13A678-1 | presence | cmapiApplication | 10.10.40.128       | XML Unencrypted | 10                      |

Item 1-1 of 1  
1

Status | Status and Control | DMCC Service Summary

Home | Help | Logout

AE Services

Communication Manager Interface

High Availability

Licensing

Maintenance

Networking

Security

Status

Alarm Viewer

Logs

Log Manager

Status and Control

CVLAN Service Summary

DLG Services Summary

DMCC Service Summary

Switch Conn Summary

TSAPI Service Summary

DMCC Service Summary - Session Summary

Please do not use back button

☐ Enable page refresh every 60 seconds

Session Summary [Device Summary](#)

Generated on Tue Feb 26 10:36:12 GMT 2019

Service Uptime: 28 days, 23 hours 26 minutes

Number of Active Sessions: 1

Number of Sessions Created Since Service Boot: 2

Number of Existing Devices: 10

Number of Devices Created Since Service Boot: 20

|                          | Session ID                          | User     | Application      | Far-end Identifier | Connection Type | # of Associated Devices |
|--------------------------|-------------------------------------|----------|------------------|--------------------|-----------------|-------------------------|
| <input type="checkbox"/> | AC98198E9ED3A664D-839EC412A13A678-1 | presence | cmapiApplication | 10.10.40.121       | XML Unencrypted | 10                      |

Terminate Sessions

Show Terminated Sessions

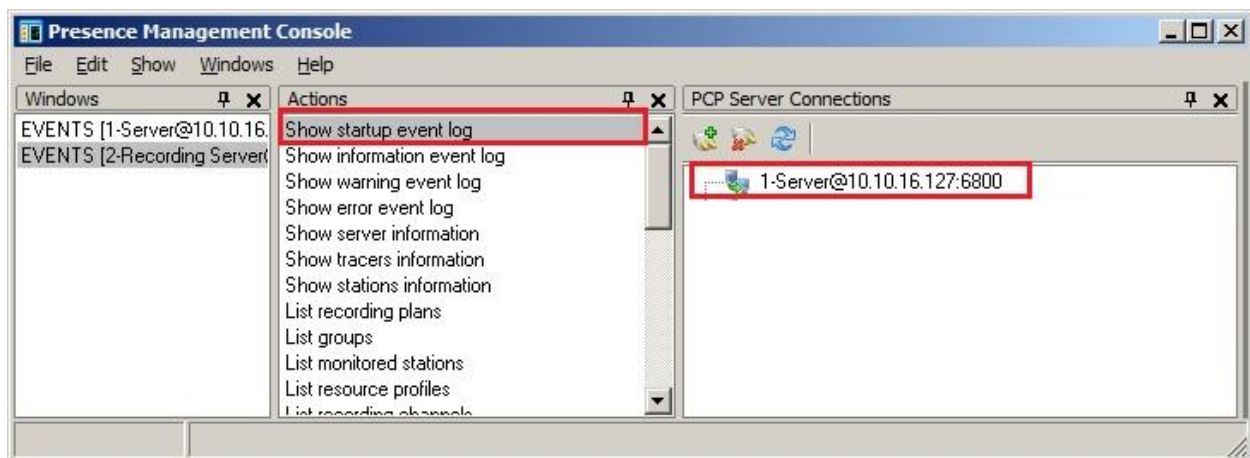
Item 1-1 of 1

1Go

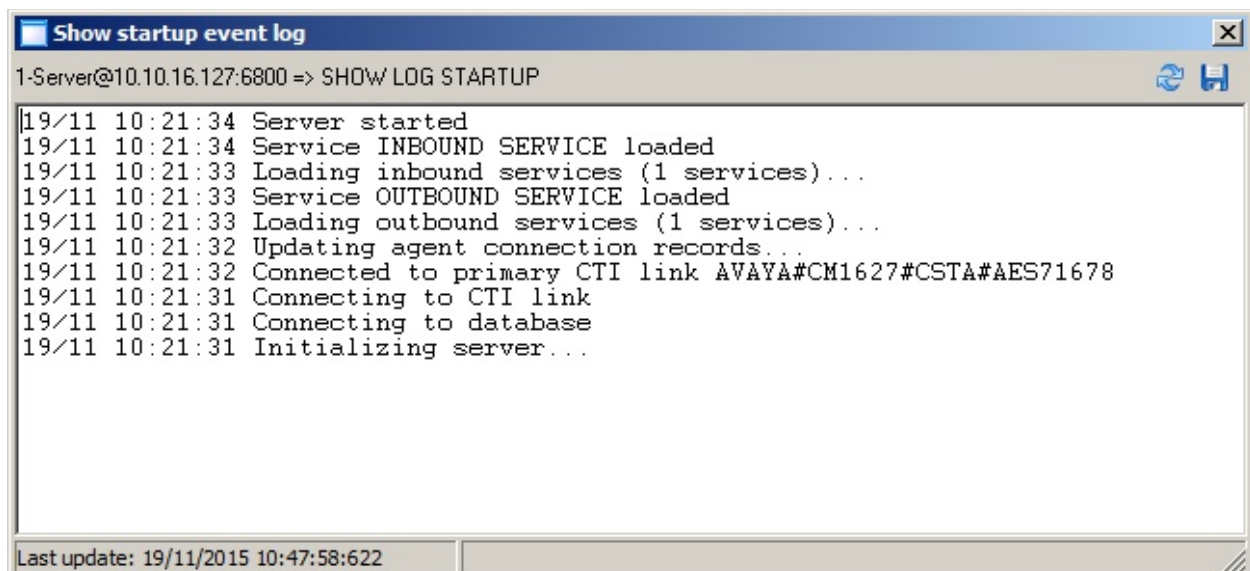
## 8.5 Verify Presence Suite CTI Connection

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.



## Conclusion

These Application Notes describe the configuration steps required for Presence Suite R11.1 to successfully interoperate with Avaya Aura® Communication Manager R8.0.1 using Avaya Aura® Application Enablement Services R8.0. All feature functionality and serviceability test cases were completed successfully with observations noted in **Section 2.2**.

## 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 8.0*

The following documentation is available on request from Enghouse at [www.enghouseinteractive.es/en](http://www.enghouseinteractive.es/en)

- [4] *ACD Sys Presence Administrator Manual Presence Suite*, V11.1
- [5] *Presence Installation Guides Presence Software*, V11.1
- [6] *PBX/ACD Requirements Presence Software*, V11.1

---

**©2019 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).