



Avaya Solution & Interoperability Test Lab

Application Notes for configuring Enghouse Presence Suite R12.1 to interoperate with Avaya Aura® Communication Manager R8.1 and Avaya Aura® Application Enablement Services R8.1 – 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 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 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.

1. Introduction

These Application Notes describe the compliance tested configuration of Enghouse Presence Suite R12.1 to interoperate with Avaya Aura® Communication Manager R8.1 using Avaya Aura® Application Enablement Services R8.1. 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 calls to and from the PSTN. The call recording module uses Avaya Aura® Communication Manager's Single Step Conferencing (SSC) feature via the Device, Media, and Call Control service provided by the Avaya Aura® Application Enablement Services (AES) to capture the audio and call details for recording agent calls.

Each Presence Agent has TSAPI client installed to facilitate its own connection to Application Enablement Services. This Presence Agent makes use of an Avaya phone for audio and controls the phone from Presence Agent using the TSAPI connection. The Presence Agent application uses TSAPI connection to monitor the agent extension to receive CTI events (call received, call established, call cleared, etc.). It also uses the TSAPI connection to make CTI requests, like `cstaMakeCall`, `cstaClearCall`.

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 Suite application, each of the modules or applications connect directly against TSAPI individually querying Avaya Aura® Application Enablement Services for device status and requests monitoring. Presence Suite specifies where to route each call and hence how to handle the calls, based on agent status information that the application tracks from device query results and event reports received from Avaya Aura® Application Enablement Services.

2. General Test Approach and Test Results

Testing included validating the correct operation of typical contact 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 (forwarding of future calls from a specific number to a supervisor) 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. Email and Web Chat services were hosted by the Presence Server and initiated from there.

For compliance testing two VDN's and two hunt groups were setup for Inbound and Outbound. The Email and Web chat services made use of the Inbound VDN/Hunt Group. Two agents were configured, one associated with an Avaya H.323 phone and another to an Avaya SIP phone (which are listed in **Section 4**).

2.2. Test Results

All test cases were executed 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

3. Reference Configuration

Figure 1 shows the network topology during interoperability testing. A Communication Manager with an Avaya G430 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.

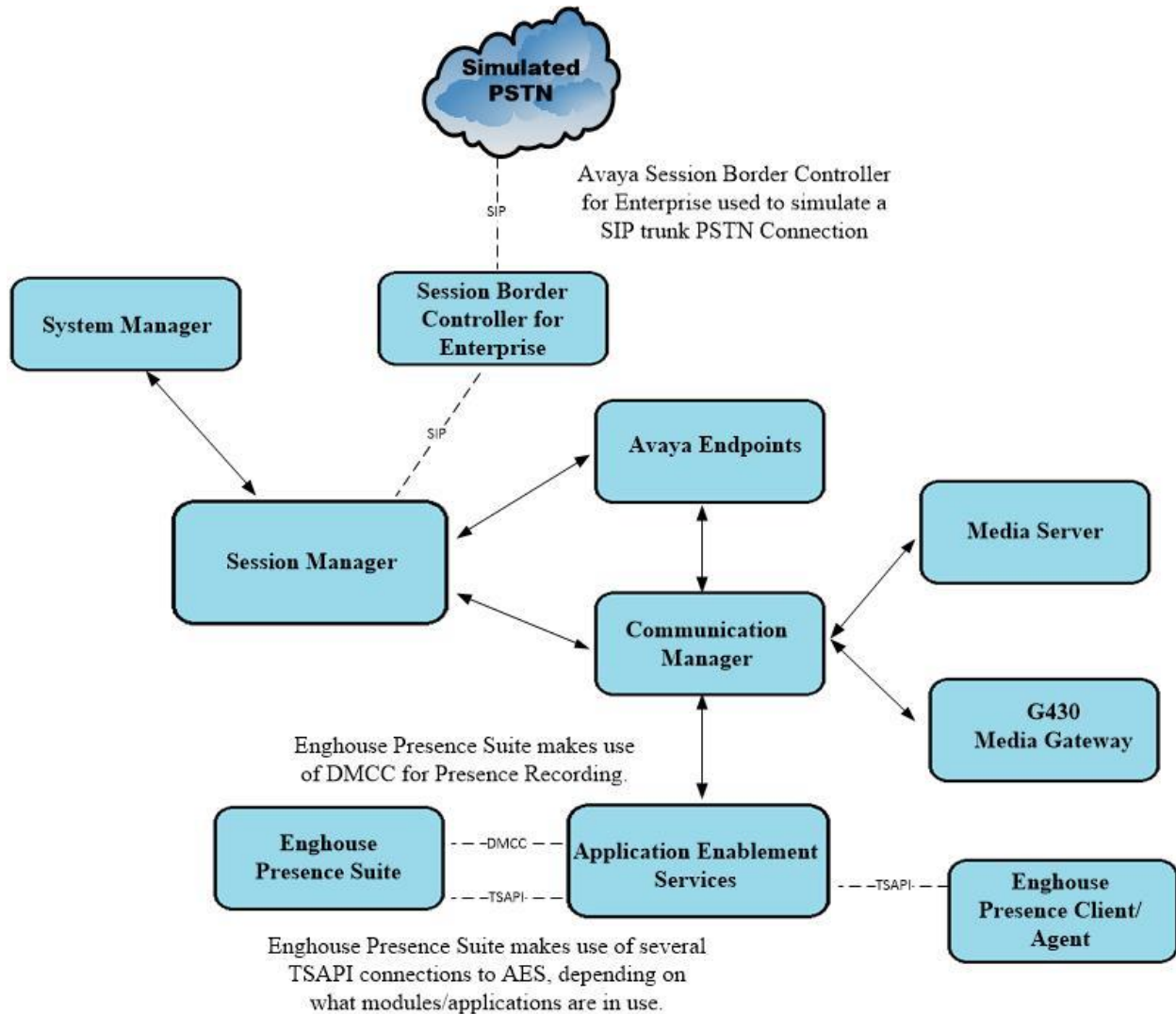


Figure 1: Avaya Aura® Communication Manager R8.1 and Aura® Application Enablement Services R8.1 with Enghouse Presence Suite R12.1 configuration

4. 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	8.1.3.2 Build No. – 8.1.0.0.733078 Software Update Revision No: 8.1.3.2.1012646 Service Pack 2
Avaya Aura® Session Manager running on a virtual server	8.1.3.2 Build No. – 8.1.3.2.813207
Avaya Aura® Communication Manager running on a virtual server	8.1.3.2 – FP3SP2 R018x.01.0.890.0 Update ID 01.0.890.0-26989
Avaya Aura® Application Enablement Services running on a virtual server	8.1.3.2 Build 8.1.3.2.0.4-0
Avaya Aura® Media Server	8.0.2.184
Avaya G430 Media Gateway	41.16.0/1
Avaya J179 IP Phone (H.323)	6.8502
Avaya J189 IP Phone (SIP)	4.0.10.1.2
Avaya 9408 Digital Deskphone	V2.0
Enghouse Equipment	Software / Firmware Version
Enghouse Presence Suite running on Windows Server 2019 Server	R12.1
Enghouse Presence Client running on Windows 10	R12.1

5. Configure Avaya Aura® Communication Manager

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

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

5.1. Verify System Features

Communication Manager is responsible for Call Classification for Outbound calls. 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		
Answer Supervision by Call Classifier? y	Change COR by FAC? n		
ARS? y	Computer Telephony Adjunct Links? y		
ARS/AAR Partitioning? y	Cvg Of Calls Redirected Off-net? y		
ARS/AAR Dialing without FAC? y	DCS (Basic)? y		
ASAI Link Core Capabilities? 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: 8.1			
ACD? y		Reason Codes? y	
BCMS (Basic)? y		Service Level Maximizer? n	
BCMS/VuStats Service Level? y		Service Observing (Basic)? y	
BSR Local Treatment for IP & ISDN? y		Service Observing (Remote/By FAC)? y	
Business Advocate? n		Service Observing (VDNs)? y	
Call Work Codes? y		Timed ACW? y	
DTMF Feedback Signals For VRU? y		Vectoring (Basic)? y	
Dynamic Advocate? n		Vectoring (Prompting)? y	
Expert Agent Selection (EAS)? y		Vectoring (G3V4 Enhanced)? y	
EAS-PHD? y		Vectoring (3.0 Enhanced)? y	
Forced ACD Calls? n		Vectoring (ANI/II-Digits Routing)? y	
Least Occupied Agent? y		Vectoring (G3V4 Advanced Routing)? y	
Lookahead Interflow (LAI)? y		Vectoring (CINFO)? y	
Multiple Call Handling (On Request)? y		Vectoring (Best Service Routing)? y	
Multiple Call Handling (Forced)? y		Vectoring (Holidays)? y	
PASTE (Display PBX Data on Phone)? y		Vectoring (Variables)? y	

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. This is a system wide setting that allows calls to be routed from one trunk to another and is usually turned off to help prevent toll fraud. An alternative to enabling this feature on a system wide basis is to control it using COR (Class of Restriction). See **Section 10** for supporting documentation.

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
VECTORIZING
    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 UII 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.

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

5.3. Administer Hunt Groups, 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

For compliance testing two VDN's were created, one for Voice Outbound and another for Voice Inbound, the Mail and Web Interactions both use the Inbound VDN as shown in Sections **7.2.4** and **7.2.5**. Two Hunt Groups were also created one for Inbound and one for Outbound.

Inbound VDN 1908, uses Hunt Group 98 and Outbound VDN 1909 uses Hunt Group 99. One Vector was used to route the calls to the primary skill.

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: 1808		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, as required, again for compliance testing the Inbound VDN was used for additional services such as direct agent transfer.

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 1908                                     Page 1 of 3

                                VECTOR DIRECTORY NUMBER

                                Extension: 1908
                                Name*: PresenceInbound
                                Destination: Vector Number      44
                                Attendant Vectoring? n
                                Meet-me Conferencing? n
                                Allow VDN Override? n
                                COR: 1
                                TN*: 1
                                Measured: none      Report Adjunct Calls as ACD*? n

VDN of Origin Annc. Extension*:
                                1st Skill*: 98
                                2nd Skill*:
                                3rd Skill*:

* Follows VDN Override Rules
```

5.4. Administer Class of Restriction

Enter the **change cor x** command where **x** corresponds to the Class of Restriction to be used for the agent login IDs in **Section 5.5**. On **Page 1**, set the **Direct Agent Calling** to **y**. This will allow agents to be called directly once they are logged in.

change cor 1	Page 1 of 23
CLASS OF RESTRICTION	
COR Number: 1	
COR Description: DefaultCOR_PG	
FRL: 7	APLT? y
Can Be Service Observed? y	Calling Party Restriction: none
Can Be A Service Observer? y	Called Party Restriction: none
Time of Day Chart: 1	Forced Entry of Account Codes? n
Priority Queuing? n	Direct Agent Calling? y
Restriction Override: none	Facility Access Trunk Test? n
Restricted Call List? n	Can Change Coverage? n
Access to MCT? y	Fully Restricted Service? n
Group II Category For MFC: 7	Hear VDN of Origin Annc.? n
Send ANI for MFE? n	Add/Remove Agent Skills? n
MF ANI Prefix:	Automatic Charge Display? n
Hear System Music on Hold? y	PASTE (Display PBX Data on Phone)? n
Can Be Picked Up By Directed Call Pickup? y	Can Use Directed Call Pickup? y
	Group Controlled Restriction: inactive

5.5. Administer Agent Logins

Enter the **add agent-loginID n** command; where **n** is an available extension number. Enter a descriptive name for the agent in the **Name** field. Ensure the **COR** field is set to **1** which relates to the COR configured in **Section 5.4**. The **Auto Answer** field is set to **station** except for those logins that will be used for outbound services. In that case, the field will be set to **all**. Configure a password as required.

add agent-loginID 1400	Page 1 of 2
AGENT LOGINID	
Login ID: 1400	AAS? n
Name: PresenceAgent1	AUDIX? n
TN: 1	Check skill TNs to match agent TN? n
COR: 1	
Coverage Path:	LWC Reception: spe
Security Code:	LWC Log External Calls? n
Attribute:	AUDIX Name for Messaging:
	LoginID for ISDN/SIP Display? n
	Password:
	Password (enter again):
	Auto Answer: station
AUX Agent Remains in LOA Queue: system	MIA Across Skills: system
AUX Agent Considered Idle (MIA): system	ACW Agent Considered Idle: system
Work Mode on Login: system	Aux Work Reason Code Type: system
	Logout Reason Code Type: system
	Maximum time agent in ACW before logout (sec): system
	Forced Agent Logout Time: :
WARNING: Agent must log in again before changes take effect	

On **Page 2**, assign a skill to the agent by entering the relevant hunt group number created in **Section 5.3.1** for **SN** and entering a skill level of **1** for **SL**. In this case, an agent is able to handle both inbound and outbound calls is created. Set the **Direct Agent Skill** to the Inbound hunt group **98**. Note other skills may already be assigned to an agent.

change agent-loginID 1400										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:	99		1			17:					
3:						18:					
4:						19:					
5:						20:					
6:											
7:											

Repeat this task accordingly for any additional inbound or outbound agents required. For compliance testing two agents were configured one associated with a SIP phone and another a H.323 phone.

5.6. 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**.

Note: For compliance testing six Phantom Stations in total were used, two for OUTBOUND and INBOUND, two for MAIL and two for WEB (internet server).

add station 58101			Page 1 of 5		
STATION					
Extension: 58101		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: 58101			
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			

5.7. 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
Name: aes80vmpg
COR: 1
```

5.8. 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**.

Note: For compliance testing four stations were used (28900 – 28903). The amount of Virtual Stations configured determines the simultaneous calls that can be recorded.

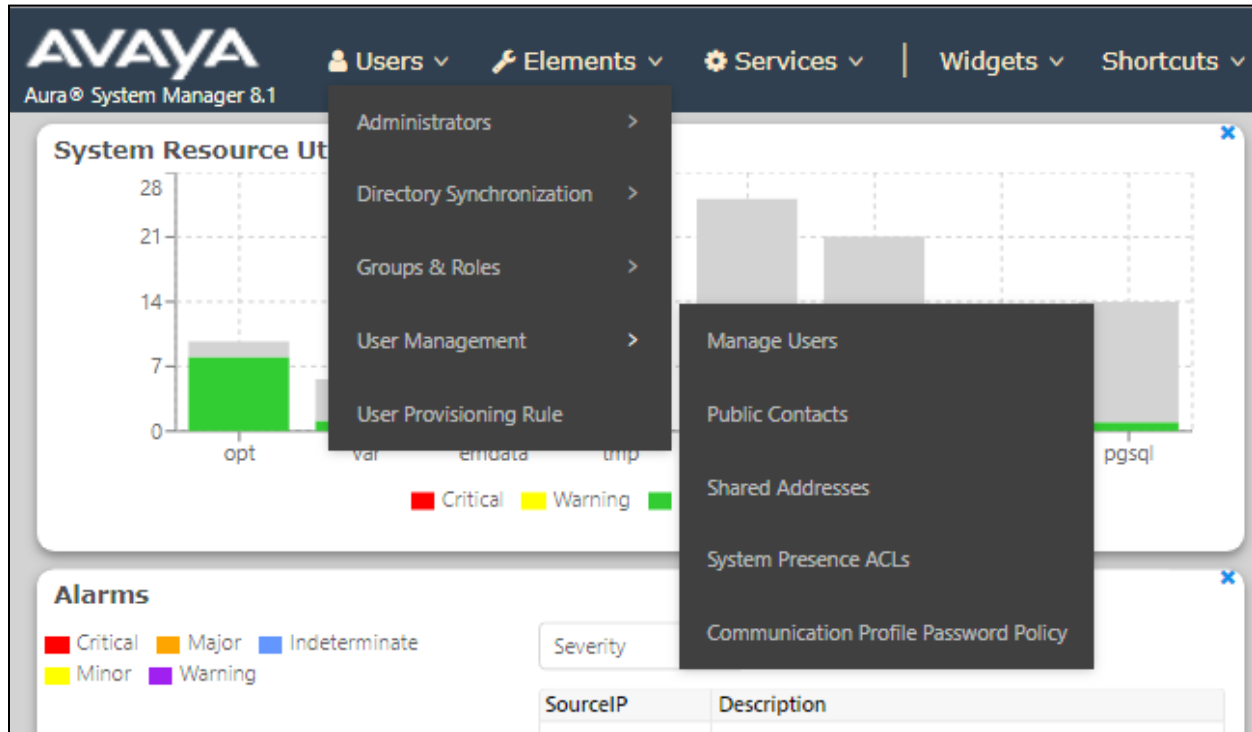
```
add station 28903                                Page 1 of 6
STATION
Extension: 28903      Lock Messages? n      BCC: 0
Type: 4624           Security Code: 1234      TN: 1
Port: S00101         Coverage Path 1:      COR: 1
Name: Recorder       Coverage Path 2:      COS: 1
                    Hunt-to Station:
STATION OPTIONS
Loss Group: 19      Time of Day Lock Table:
                    Personalized Ringing Pattern: 1
                    Message Lamp Ext: 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      IP SoftPhone? y
                    IP Video Softphone? n
                    Short/Prefixed Registration Allowed: default
```


5.9. Configure SIP Agent Stations

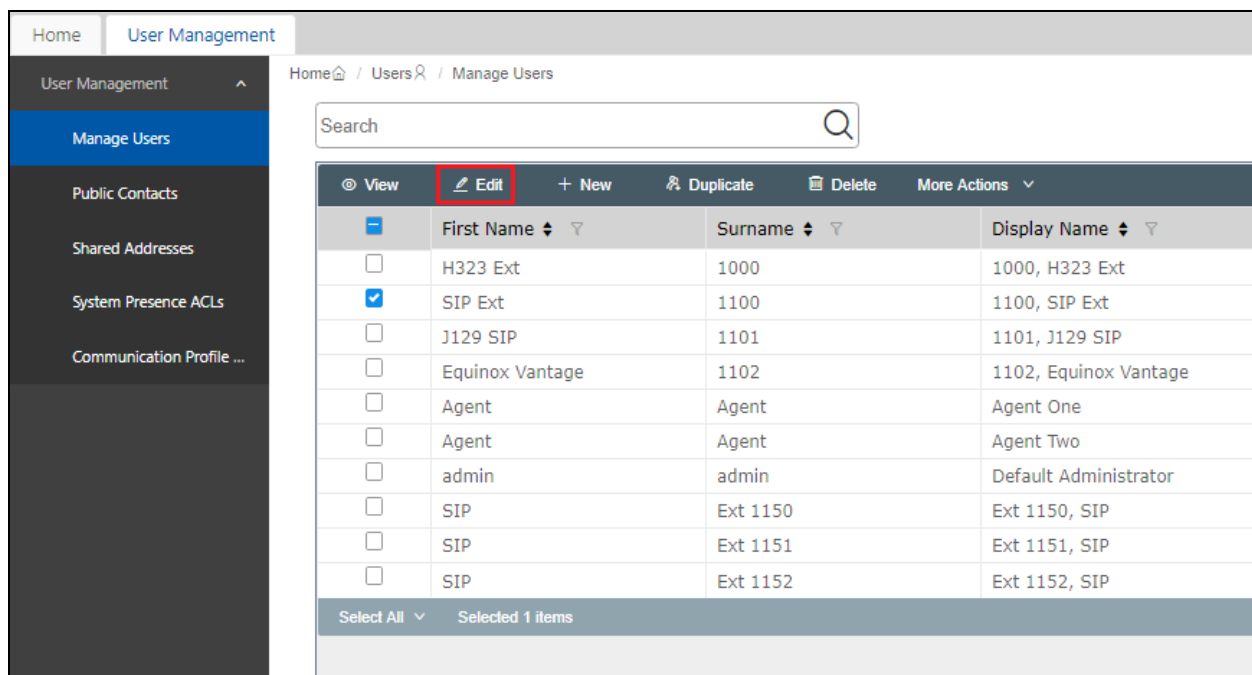
Each Avaya SIP endpoint or station that needs to be monitored will need to have “Type of 3PCC Enabled” set to “Avaya”. Changes to SIP phones on Communication Manager must be carried out from System Manager. Access the System Manager using a Web Browser by entering **http://<FQDN>/network-login**, where <FQDN> is the fully qualified domain name of System Manager or the IP address of System Manager can be used as an alternative to the FQDN. 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.

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



Click on **Manager Users** in the left window. Select the station to be edited and click on **Edit**.



Click on the **CM Endpoint Profile** tab in the left window. Click on **Endpoint Editor** to make changes to the SIP station.

User Profile | Edit | 1100@devconnect.local

Identity | **Communication Profile** | Membership | Contacts

Communication Profile Password

PROFILE SET : Primary

Communication Address

PROFILES

Session Manager Profile ☒

Avaya Breeze® Profile ☐

CM Endpoint Profile ☒

* System: cm\$1xvmpg

* Profile Type: Endpoint

Use Existing Endpoints: ☐

* Extension: 1100

Template: Start typing...

* Set Type: 9641SIPCC

Security Code: Enter Security Code

Port: S000002

Voice Mail Number: 6666

Preferred Handle: Select

Calculate Route Pattern: ☐

Sip Trunk: aar

SIP URI: Select

Enhanced Callr-Info Display for 1-line phones: ☐

Delete on Unassign from User or on Delete User: ☒

Override Endpoint Name and Localized Name: ☒

Allow H.323 and SIP Endpoint Dual Registration: ☐

Commit & Continue | **Commit** | Cancel

In the **General Options** tab ensure that **Type of 3PCC Enabled** is set to **Avaya** as is shown below. Click on **Done**, at the bottom of the screen, once this is set, (not shown).

General Options (G) * | Feature Options (F) | Site Data (S) | Abbreviated Call Dialing (A)

Enhanced Call Fwd (E) | Button Assignment (B) | Profile Settings (P) | Group Membership (M)

* Class of Restriction (COR) 1

* Emergency Location Ext 1100

* Tenant Number 1

* SIP Trunk aar

Coverage Path 1

Lock Message ☐

Multibyte Language Not Applicable

* Class Of Service (COS) 1

* Message Lamp Ext. 1100

Type of 3PCC Enabled Avaya

Coverage Path 2

Localized Display Name 1100, SIP Ext

Enable Reachability for Station Domain Control system

SIP URI

Primary Session Manager

IPv4: 10.10.40.32 | IPv6:

Secondary Session Manager

6. Configure Avaya Aura® Application Enablement Services Server

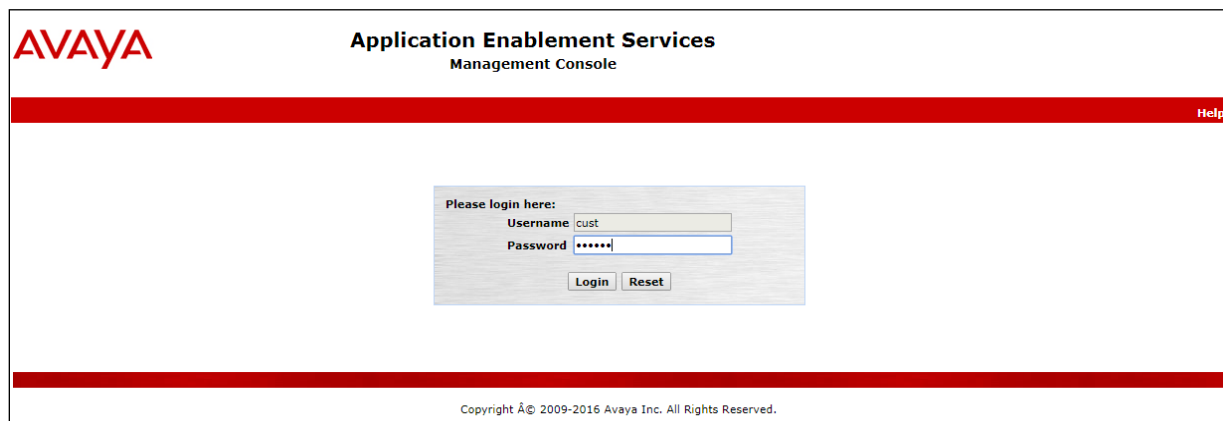
This section provides the procedures for configuring Application Enablement Services. The procedures fall into the following areas:

- Verify Licensing
- Administer TSAPI link
- Create CTI User
- Enable Unrestricted Access for CTI User
- Identify TLinks
- Configure Networking Ports

Note: It is assumed that a connection between Application Enablement Services and Communication Manager is already in place including the setup of the H.323 Gatekeeper.

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 interface. At the top left is the Avaya logo. The title "Application Enablement Services Management Console" is centered at the top. A red horizontal bar spans the width of the page, with a "Help" link on the right. In the center, there is a login box with the text "Please login here:". Below this, there are two input fields: "Username" with the value "cust" and "Password" with masked characters "*****". Below the password field are two buttons: "Login" and "Reset". At the bottom of the page, a red horizontal bar is present, and below it, the copyright notice "Copyright © 2009-2016 Avaya Inc. All Rights Reserved." is displayed.

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**.

Application Enablement Services
Management Console

Welcome: User cust
Last login: Fri Nov 30 10:52:21 2018 from 10.10.40.241
Number of prior failed login attempts: 0
HostName/IP: aes80vmppg/10.10.40.56
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.0.0.0.0.6-0
Server Date and Time: Fri Dec 07 10:13:22 GMT 2018
HA Status: Not Configured

AE Services
Home | Help | Logout

AE Services

CVLAN

DLG

DMCC

SMS

TSAPI

TWS

Communication Manager Interface

High Availability

Licensing

Maintenance

Networking

Security

Status

User Management

Utilities

Help

AE Services

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

Service	Status	State	License Mode	Cause*
ASAI Link Manager	N/A	Running	N/A	N/A
CVLAN Service	OFFLINE	Running	N/A	N/A
DLG Service	OFFLINE	Running	N/A	N/A
DMCC Service	ONLINE	Running	NORMAL MODE	N/A
TSAPI Service	ONLINE	Running	NORMAL MODE	N/A
Transport Layer Service	N/A	Running	N/A	N/A
AE Services HA	Not Configured	N/A	N/A	N/A

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

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

License Information
You are licensed to run Application Enablement (CTI) release 8.x

The TSAPI and DMCC licenses are user licenses issued by the Web License Manager to which the Application Enablement Services server is pointed to. From the left window open **Licensing** and click on **WebLM Server Access** as shown below.

Licensing

AE Services

Communication Manager Interface

High Availability

Licensing

WebLM Server Address

WebLM Server Access

Reserved Licenses

Maintenance

Networking

Security

Status

User Management

Utilities

Help

Licensing

If you are setting up and maintaining the WebLM, you need to use the following:

- WebLM Server Address

If you are importing, setting up and maintaining the license, you need to use the following:

- WebLM Server Access

If you want to administer TSAPI Reserved Licenses or DMCC Reserved Licenses, you need to use the following:

- Reserved Licenses

NOTE: Please disable your pop-up blocker if you are having difficulty with opening this page

The following screen shows the available licenses for **TSAPI** and **DMCC** users.

▼ Application_Enablement

View license capacity

View peak usage

ASBCE

▶ Session_Border_Controller_E_AE

AVAYA_OCEANA

▶ Avaya_Oceana

CCTR

▶ ContactCenter

CE

▶ COLLABORATION_ENVIRONMENT

COLLABORATION_DESIGNER

▶ Collaboration_Designer

COLLABORATIVE_BROWSING_SNAP-IN

▶ Collaborative_Browsing_Snap_In


COMMUNICATION_MANAGER

▶ Call_Center

▶ Communication_Manager

License File Host IDs:

Licensed Features

10 Items  Show All ▼

Feature (License Keyword)	Expiration date	Licensed capacity
Unified CC API Desktop Edition VALUE_AES_AEC_UNIFIED_CC_DESKTOP	permanent	44
CVLAN ASAI VALUE_AES_CVLAN_ASAI	permanent	44
Device Media and Call Control VALUE_AES_DMCC_DMC	permanent	44
AES ADVANCED SMALL SWITCH VALUE_AES_AEC_SMALL_ADVANCED	permanent	4
DLG VALUE_AES_DLG	permanent	44
TSAPI Simultaneous Users VALUE_AES_TSAPI_USERS	permanent	44
AES ADVANCED LARGE SWITCH VALUE_AES_AEC_LARGE_ADVANCED	permanent	4
CVLAN Proprietary Links VALUE_AES_PROPRIETARY_LINKS	permanent	44

6.2. Administer TSAPI link

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

Application Enablement Services

Management Console

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 #

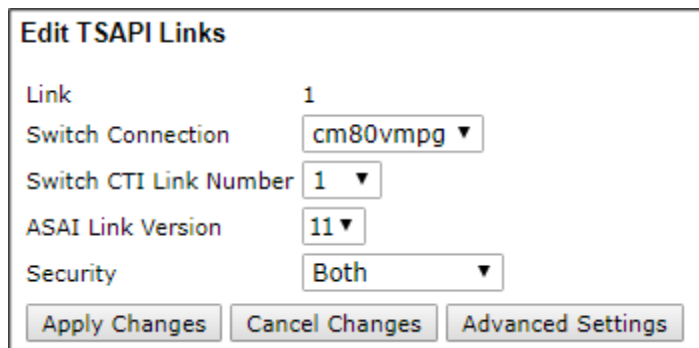
Add Link

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 **cm80vmg**, which has already been configured, from the drop-down list.
- **Switch CTI Link Number:** Corresponding CTI link number configured in **Section 5.10**.
- **ASAI Link Version:** This can be set to the latest version.
- **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: cm80vmg ▼

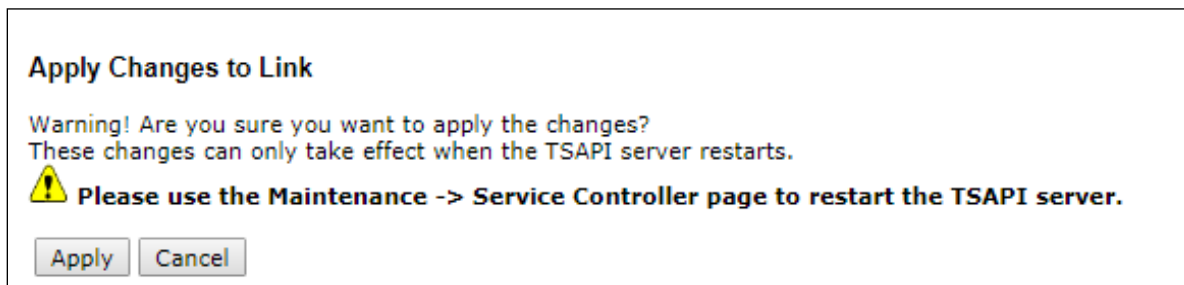
Switch CTI Link Number: 1 ▼

ASAI Link Version: 11 ▼

Security: Both ▼

Buttons: Apply Changes, Cancel Changes, Advanced Settings

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



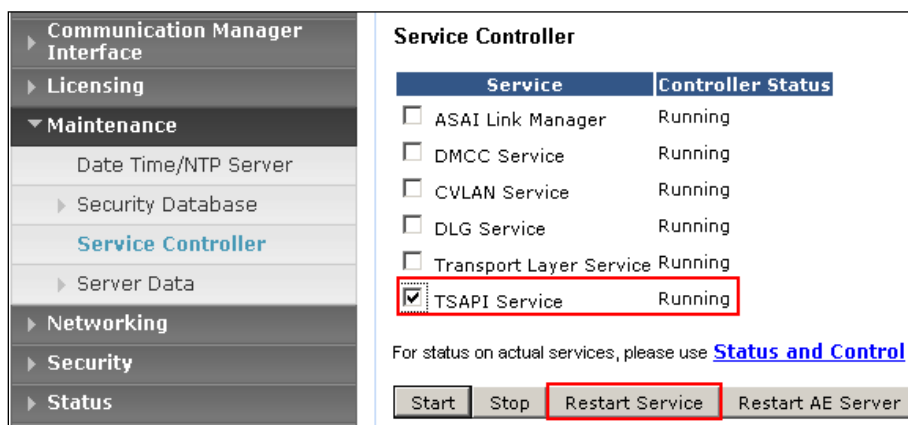
Apply Changes to Link

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

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

Buttons: Apply, Cancel

The TSAPI Service must be restarted to effect the changes made in this section. From the Management Console menu, navigate to **Maintenance → Service Controller**. On the Service Controller screen, tick the **TSAPI Service** and select **Restart Service**.



Service Controller

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

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

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

6.3. Create CTI User

A User ID and password needs to be configured for the Presence Suite server to communicate 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.

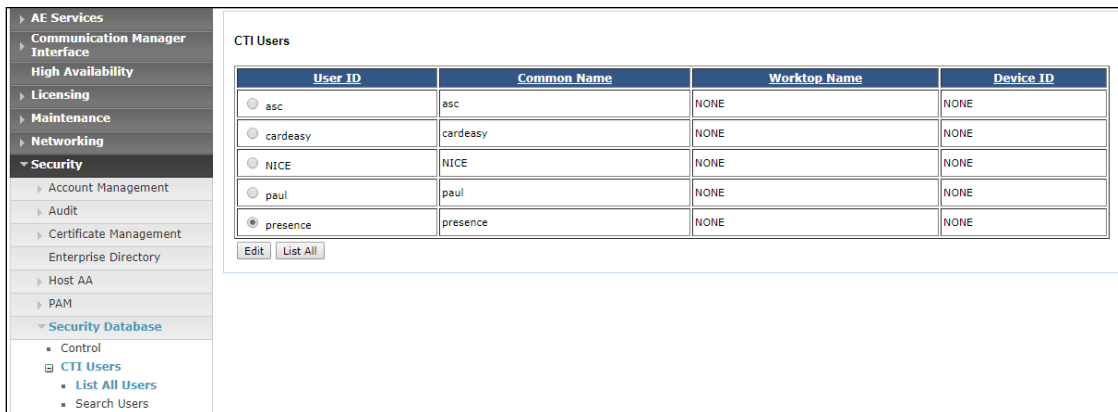
The screenshot shows the 'Add User' form within the 'User Management | User Admin | Add User' interface. On the left is a navigation menu with categories: AE Services, Communication Manager Interface, High Availability, Licensing, Maintenance, Networking, Security, Status, User Management (expanded), 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 two buttons: 'Apply' and 'Cancel'.

6.4. Enable Unrestricted Access for CTI User

Navigate to the **CTI Users** screen by selecting **Security** → **Security Database** → **CTI Users** → **List All Users**. Select the user that was created in **Section 6.3** and select the **Edit** button.

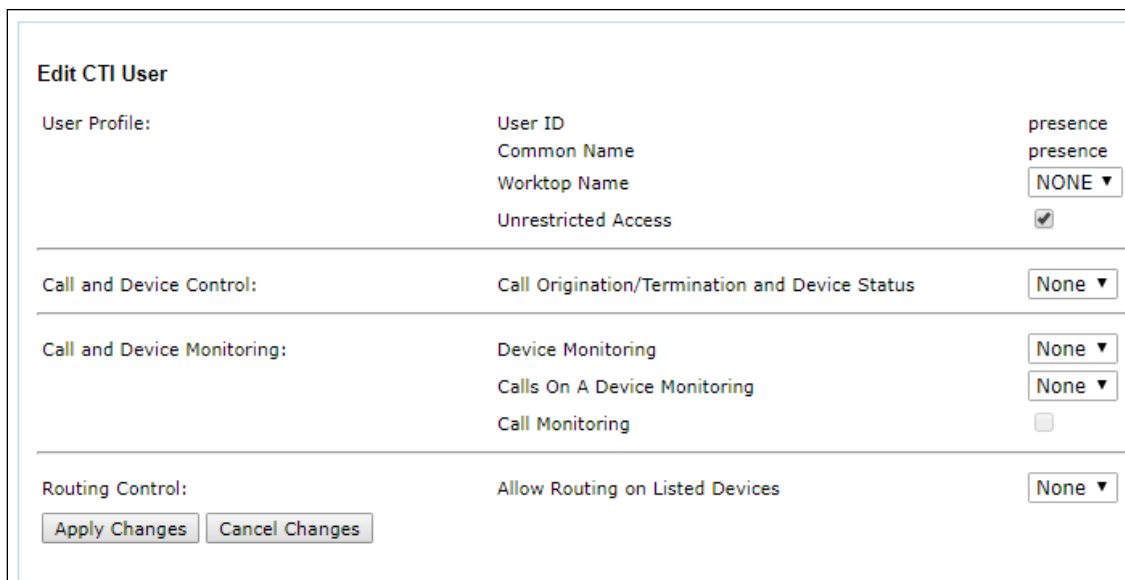


The screenshot shows the 'CTI Users' screen. On the left is a navigation menu with categories: AE Services, Communication Manager Interface, High Availability, Licensing, Maintenance, Networking, Security (expanded), Account Management, Audit, Certificate Management, Enterprise Directory, Host AA, PAM, Security Database (expanded), Control, CTI Users (expanded), List All Users, and Search Users. The main area displays a table of CTI Users.

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

Below the table are buttons for 'Edit' and 'List All'.

The **Edit CTI User** screen appears. Check the **Unrestricted Access** box and **Apply Changes** at the bottom of the screen. Note that DevConnect would not recommend giving unrestricted access as this may be a security risk, but was set specifically for ease of compliance testing.

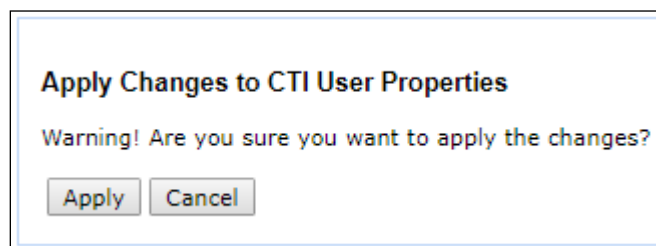


The screenshot shows the 'Edit CTI User' screen. It contains several sections for configuring user properties:

- User Profile:** Fields for User ID (presence), Common Name (presence), Worktop Name (dropdown menu showing NONE), and Unrestricted Access (checkbox checked).
- Call and Device Control:** Field for Call Origination/Termination and Device Status (dropdown menu showing None).
- Call and Device Monitoring:** Fields for Device Monitoring (dropdown menu showing None), Calls On A Device Monitoring (dropdown menu showing None), and Call Monitoring (checkbox unchecked).
- Routing Control:** Field for Allow Routing on Listed Devices (dropdown menu showing None).

At the bottom are buttons for 'Apply Changes' and 'Cancel Changes'.

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



The screenshot shows a dialog box titled 'Apply Changes to CTI User Properties'. It contains a warning message: 'Warning! Are you sure you want to apply the changes?'. At the bottom are buttons for 'Apply' and 'Cancel'.

6.5. 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 top link was used as this was the non-secure link.

The screenshot displays the Avaya system's administrative 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, Security Database (expanded), Control, CTI Users, Devices, Device Groups, Tlinks (highlighted in blue), Tlink Groups, and Worktops. The main content area on the right is titled 'Tlinks'. It contains a section labeled 'Tlink Name' with two radio button options: 'AVAYA#CM80VMPG#CSTA#AES80VMPG' (which is selected) and 'AVAYA#CM80VMPG#CSTA-S#AES80VMPG'. Below these options is a 'Delete Tlink' button.

6.6. 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	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	1050			
TCP Port Max	1065			
Encrypted TLINK Ports				
TCP Port Min	1066			
TCP Port Max	1081			

DMCC Server Ports

			Enabled	Disabled
Unencrypted Port	4721		<input checked="" type="radio"/>	<input type="radio"/>
Encrypted Port	4722		<input checked="" type="radio"/>	<input type="radio"/>
TR/87 Port	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

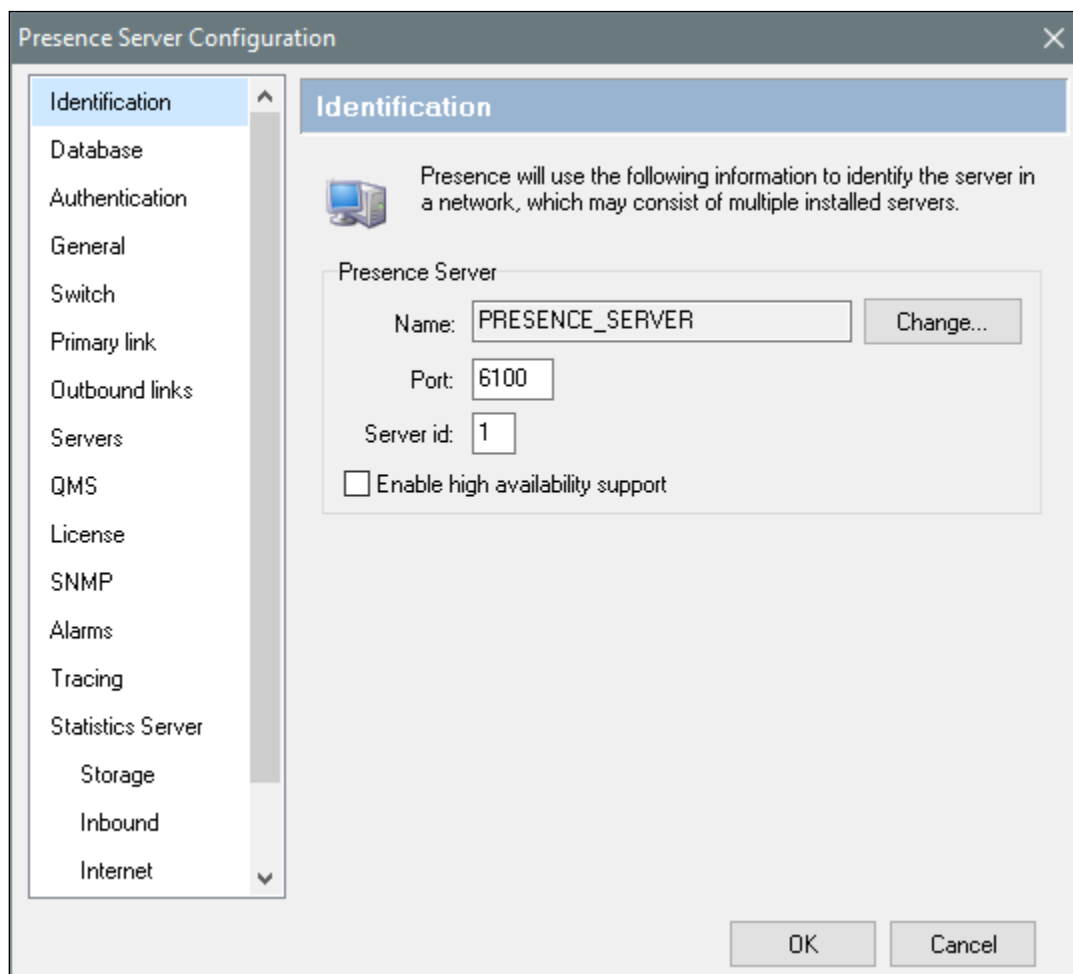
For status on actual services, please use [Status and Control](#)

7. Configure Enghouse Presence Suite


The Presence Suite includes the Presence Server, Presence Mail Interactions Server, Presence Web Interactions Server, Presence Recording Server, Presence Unified Manager, 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 with the 'Identification' tab selected. The left sidebar lists various configuration categories, with 'Identification' at the top. The main area of the window contains the following information:

- Identification** (tab title)
-  Presence will use the following information to identify the server in a network, which may consist of multiple installed servers.
- Presence Server** (section header)
- Name:** PRESENCE_SERVER (text field) with a 'Change...' button.
- Port:** 6100 (text field).
- Server id:** 1 (text field).
- ☐ Enable high availability support (checkbox).
- OK** and **Cancel** buttons at the bottom right.

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

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

Configuration Category	Setting	Value	Unit
Maintenance configuration values	Check for pending outbound calls every	30	seconds
	Minimum time between queue updates in server (in minutes). If a queue is updated within a shorter interval, a warning will be triggered in server:	15	minutes
	Time for reorganizing queues in server. This is a critical process which may affect the server performance:	03:00	hours
	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 5.6** in the **Ranges of phantom extensions** parameter. The two extensions below were used for Inbound.

The screenshot shows the 'Presence Server Configuration' dialog box with the 'Switch' tab selected. The left sidebar contains a list of configuration categories: Identification, Database, Authentication, General, Switch (highlighted), Primary link, Outbound links, Servers, QMS, License, SNMP, Alarms, Tracing, Statistics Server, Storage, Inbound, and Internet. The main area is divided into several sections: 'Switch configuration values' with fields for 'Prefix for outgoing calls' (empty), 'System login to be assigned to contacts not handled by an agent (CTI login):' (99999), and 'System login to be assigned to contacts handled by robodialer (robodialer login):' (99998); 'Preview mode' with a field for 'Ranges of phantom extensions (separated by a semicolon)' containing '58101-58102'; 'IVR' with fields for 'Port for integration:' (9090) and 'SE/Prefix for routing:' (empty); and 'Media Server' with a field for 'VDN for routing:' (empty). 'OK' and 'Cancel' buttons are at the bottom right.

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)	58101-58102
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 the following items: 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 of the dialog is titled 'Primary link' and contains the following text: 'You must specify a primary CTI link which will be used as default link. You may specify backup primary links in case that the primary link is down.' Below this text is a 'Primary link:' label followed by a text input field containing 'AVAYA#CM80XVMPPG#CSTA#AES80XVMPPG' and an 'Edit' button. Below the primary link section is a 'List of backup links' section, which includes a text area labeled 'CTI link name', 'Up' and 'Down' buttons, and 'Add', 'Edit', and 'Remove' buttons. At the bottom right of the dialog are 'OK' and 'Cancel' buttons.

Presence Server Configuration

Primary link

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.

Primary link:

List of backup links

CTI link name

In the resulting pop-up box enter the Tlink name from **Section 6.5** in the **Name** field. For the **User** and **Password** fields enter the user name and password configured on the Application Enablement Services in **Section 6.3**. Click **OK**.

Primary CTI link data

CTI link configuration data

Name:

User:

Password:

Primary CTI link data

CTI link configuration data

Name: AVAYA#CM81XVMGP#CSTA#AES81XVMGP

User: presence

Password: ●●●●●●●●

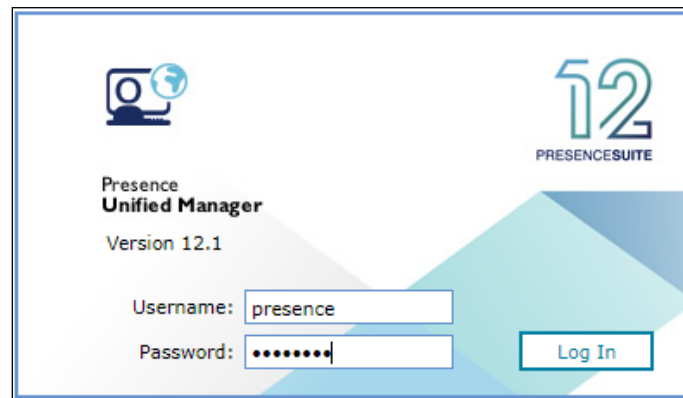
OK Cancel

7.2. Presence Service Configuration

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

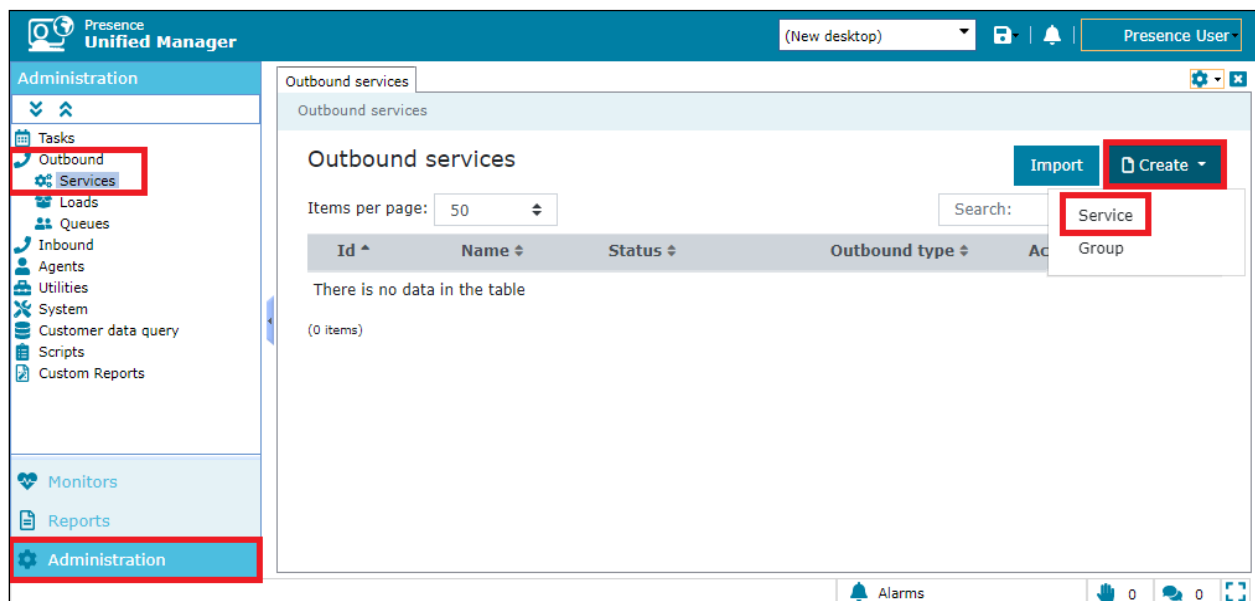
7.2.1. Logging in to Presence Unified Manager

Enter **https://<ip-addr>/websupervisor** (where the ip-addr is the IP address of the Presence Server) as the URL in an Internet browser. 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 Unified Manager the following screen will be displayed. Select **Administration → Outbound → Services** from the main menu on the left hand side. Double click in **Services** to open a new tab showing the list of outbound services, click on **Create** button and then click on the **Service** option to create a new outbound service.



In the resulting tab, in the **General** section, 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.

Presence Unified Manager

(New desktop) Presence User

Outbound services / Create

Configuration

General

Integration

Contact information

ACD

Outbound options

Call analysis

Maximums

Queues

Schedule

Softphone

Alternative phone

Time zones

Do-Not-Call list

Sounds

Custom buttons

Custom fields

Assistance

Other

General

Identification

Select a logo

Id: 2 Name: OUTBOUND SERVICE Outbound type: Predictive

☐ Grouped Weight: 1 ☐ Use the group configuration parameters

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

Save Cancel

Go to **ACD** section. 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.

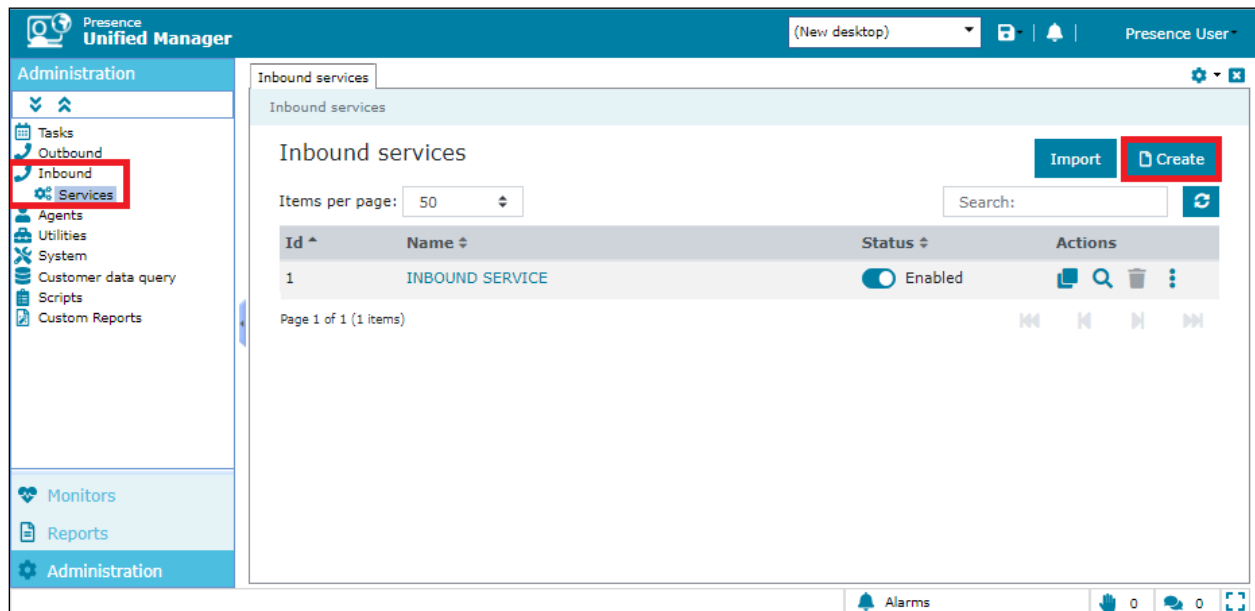
The screenshot shows the 'Presence Unified Manager' interface. The top navigation bar includes the logo, a '(New desktop)' dropdown, and a 'Presence User' profile. The main content area is titled 'Outbound services / Create' and features a 'Configuration' tab. A left-hand sidebar lists various configuration categories: General, Integration, Contact information, ACD, Outbound options, Call analysis, Maximums, Queues, Schedule, Softphone, Alternative phone, Time zones, Do-Not-Call list, Sounds, Custom buttons, Custom fields, Assistance, and Other. The 'ACD' section is currently selected, displaying the following fields: 'Extension/Skill' with the value '1809', 'VDN/SE' with the value '1909', and 'Link CTI' with a dropdown menu showing '<<Primary CTI link>>'. A checkbox labeled 'Use primary CTI link in case that CTI link is not connected' is checked. Below these are sections for 'Calls' (with a checkbox for 'Maximum number of concurrent service calls') and 'Agent availability' (with a checkbox for 'Check agent availability' and a field for 'Minimum number/percentage of available agents'). The 'Outbound options' section is partially visible at the bottom. At the bottom of the configuration area are 'Save' and 'Cancel' buttons. The system status bar at the very bottom shows 'Alarms', a handshake icon with '0', and a speech bubble icon with '0'.

Communication Manager is responsible for Call Classification for Outbound calls. Go to **Call analysis** section. 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 **Save** button to complete the outbound service configuration.

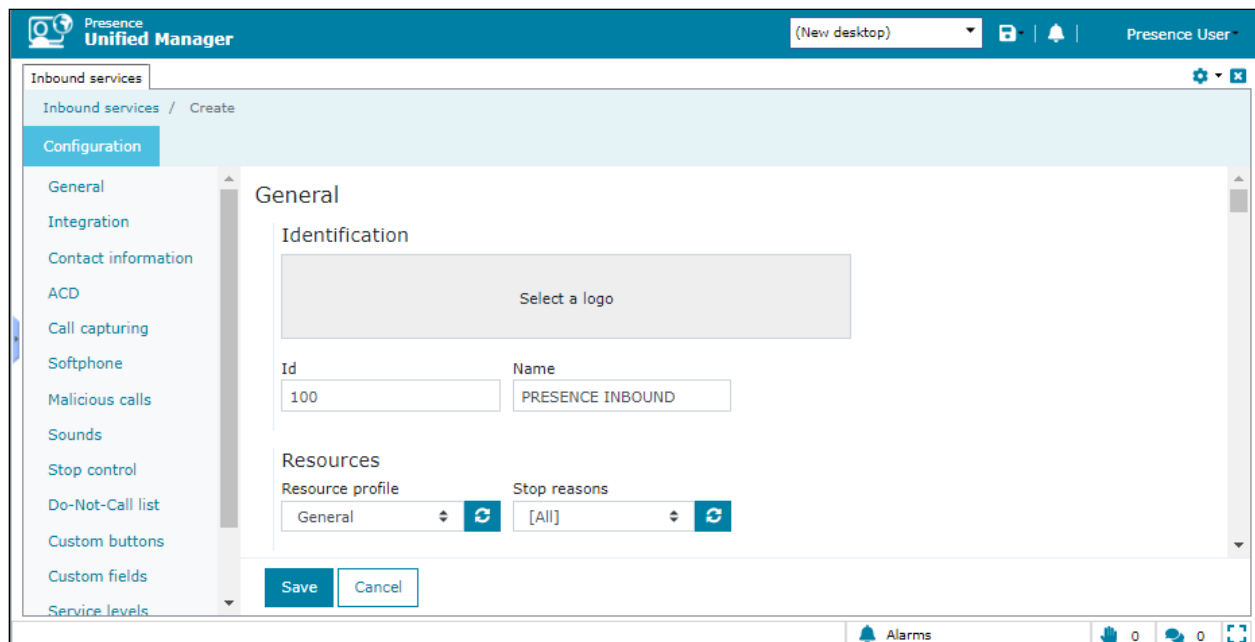
The screenshot shows the 'Presence Unified Manager' interface. The top navigation bar includes the logo, a '(New desktop)' dropdown, and a 'Presence User' profile. The main content area is titled 'Outbound services / Create' and features a 'Configuration' tab. On the left, a sidebar lists various configuration categories: General, Integration, Contact information, ACD, Outbound options, Call analysis (which is currently selected), Maximums, Queues, Schedule, Softphone, and Alternative phone. The 'Call analysis' section is divided into two parts. The 'Detection settings' section contains a checked checkbox for 'Detect answering machine and fax' and a text input field for 'No. of rings for 'No answer'' set to the value '6'. The 'Answering machines' section includes an unchecked checkbox for 'Enable redirection for answering machines', a 'Target extension' text field, a 'Q. code for answering machine' text field, and a 'Select q. code' button. At the bottom of the configuration area are 'Save' and 'Cancel' buttons. The bottom status bar shows 'Alarms' and some system icons.

7.2.3. Inbound Service

To configure an inbound service, from the left hand side select **Administration** → **Inbound** → **Services** from the Presence Unified Manager main menu. Double click in **Services** to open a new tab showing the list of inbound services and click on **Create** button to create a new inbound service.



In the resulting screen, go to **General** section and enter an **Id** and a **Name** for the inbound service. All other fields are left with their default values.



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

The screenshot shows the 'Presence Unified Manager' interface. The top navigation bar includes the logo, 'Presence Unified Manager', a '(New desktop)' dropdown, and user information 'Presence User'. The left sidebar lists various configuration categories: Inbound services, Configuration, General, Integration, Contact information, ACD, Call capturing, Softphone, Malicious calls, Sounds, Stop control, Do-Not-Call list, Custom buttons, Custom fields, Service levels, Assistance, and Other. The main content area is titled 'ACD' and contains two sections: 'Skills' and 'VDN/SE'. Each section has an input field, a '+ Add' button, and a search bar. Below each input field is a table with columns 'Skill ^' or 'VDN/SE ^' and 'Actions'. The 'Skills' table shows one item with the value '1808'. The 'VDN/SE' table shows one item with the value '1908'. At the bottom of the main content area are 'Save' and 'Cancel' buttons. The bottom status bar shows 'Alarms' and some icons.

Skill ^	Actions
1808	—

VDN/SE ^	Actions
1908	—

Go to **Call capturing** section, select the **Enable call capturing. Force routing to agent who captured the call** was checked for this compliance testing but is each user's 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.

The screenshot shows the 'Call capturing' configuration page in the Presence Unified Manager. The left sidebar lists various configuration sections, with 'Call capturing' selected. The main content area has a 'Configuration' tab active, showing three checkboxes: 'Enable call capturing' (checked), 'Force routing to agent who captured the call' (checked), and 'Automatically capture calls for (minutes)' (unchecked). Below these is a text input field for the duration. At the bottom are 'Save' and 'Cancel' buttons. The top of the interface shows the 'Presence Unified Manager' logo, a '(New desktop)' dropdown, and a 'Presence User' profile.

Go to **Malicious calls** section, 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, for compliance testing supervisor extension **1050** was chosen. In the **VDN/SE to control** field select the VDNs this option will be available on.

The screenshot shows the 'Malicious calls' configuration page in the Presence Unified Manager. The left sidebar lists various configuration sections, with 'Malicious calls' selected. The main content area has a 'Configuration' tab active, showing the 'Enable malicious calls detection' checkbox checked. Below it is the 'Target extension' field with the value '1050'. The 'VDN/SE to control' section has a 'Show selected only' checkbox (unchecked) and a search field. Below this is a table with two columns: 'VDN/SE' and 'Description'. The table contains one row with '1908' in the 'VDN/SE' column and '1908' in the 'Description' column. At the bottom are 'Save' and 'Cancel' buttons. The top of the interface shows the 'Presence Unified Manager' logo, a '(New desktop)' dropdown, and a 'Presence User' profile.

VDN/SE	Description
1908	1908

Go to **Other** section, select the **Enable direct transfer to agents of this service** check box. Enter the direct agent transfer VDN assigned in the list. Click **Save** to complete the inbound service configuration.

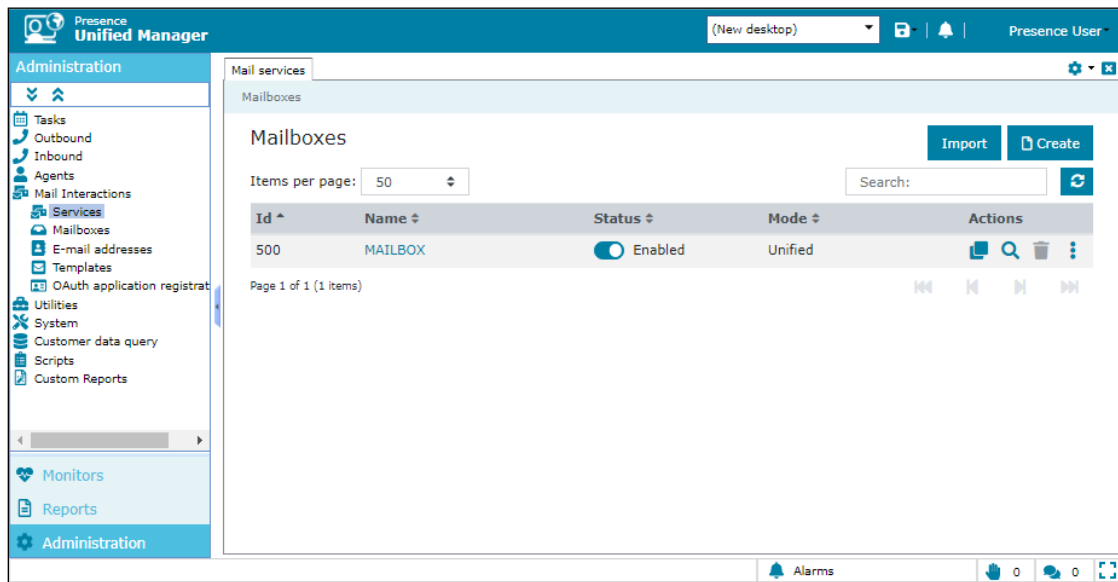
The screenshot shows the 'Presence Unified Manager' interface. The top navigation bar includes the logo, a '(New desktop)' dropdown, and a 'Presence User' profile. The main content area is titled 'Inbound services / Create' and features a 'Configuration' tab. A left sidebar lists various configuration categories: General, Integration, Contact information, ACD, Call capturing, Softphone, Malicious calls, Sounds, Stop control, Do-Not-Call list, Custom buttons, Custom fields, Service levels, Assistance, and Other. The 'Other' section is currently selected and displays the following settings:

- After-call work**
 - ☐ Minimum after-call work time (seconds) [text input field]
 - ☐ Maximum time in after-call work (seconds) [text input field]
 - Q. code for maximum time** [text input field] **Select q. code** [button] ☐ Use q. code only if contact has not yet been qualified
- Transfer to agents**
 - ☒ Enable direct transfer to agents of this service
 - 1908 [dropdown menu]
- Outgoing calls identification**
 - ☐ Enable outgoing calls identification
 - Phone no. [text input field]

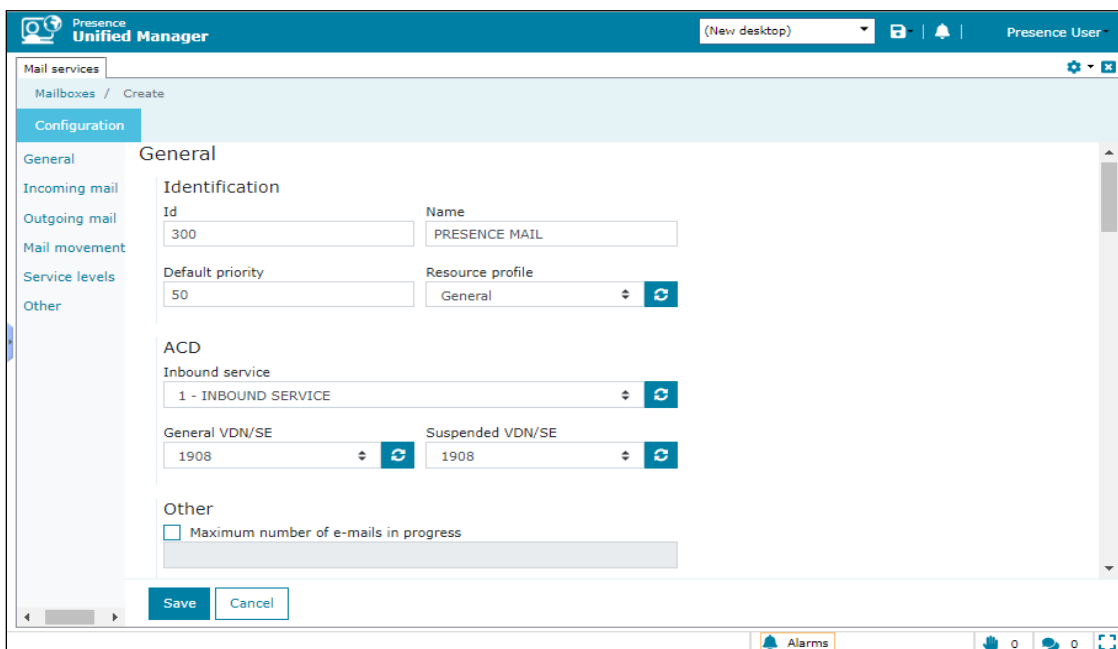
At the bottom of the configuration area are 'Save' and 'Cancel' buttons. The system status bar at the very bottom shows 'Alarms' and resource counts (0 agents, 0 calls).

7.2.4. Email Service

To configure an email service, from the left hand side select **Administration** → **Mail Interactions** → **Services** from the Presence Unified Manager main menu. Double click in **Services** to open a new tab showing the list of mailboxes and click on **Create** button to create a new mailbox.



In the resulting screen, go to **General** section 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.



Go to **Incoming mail** section. 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 the 'Incoming mail' configuration window in the Presence Unified Manager. The left sidebar has a 'Configuration' tab selected. The main area is titled 'Incoming mail' and contains the following fields:

- Incoming mail server (IMAP/POP3)**: Protocol dropdown set to 'POP3'.
- Server**: Text field containing '10.10.40.122'.
- Port**: Text field containing '110'.
- Use the following type of encrypted connection**: Dropdown set to 'None'.
- Incoming mail account**:
 - Account name**: Text field containing 'mailbox1@test.com'.
 - Password**: Text field containing '*****'.
 - E-mail address**: Text field containing 'mailbox1@test.com'.

At the bottom are 'Save' and 'Cancel' buttons. The top bar shows 'Presence Unified Manager' and 'Presence User'.

Go to **Outgoing mail** section, 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 **Save** to complete the email service configuration.

The screenshot shows the 'Outgoing mail' configuration window in the Presence Unified Manager. The left sidebar has a 'Configuration' tab selected. The main area is titled 'Outgoing mail' and contains the following fields:

- Outgoing mail server (SMTP)**:
 - Server**: Text field containing '10.10.40.122'.
 - Port**: Text field containing '25'.
- Use the following type of encrypted connection**: Dropdown set to 'None'.
- Authentication**:
 - ☒ **My server requires authentication**
 - Use same settings as my incoming mail server (dropdown)
 - Account name**: Text field (empty).
 - Password**: Text field (empty).

At the bottom are 'Save' and 'Cancel' buttons. The top bar shows 'Presence Unified Manager' and 'Presence User'.

7.2.5. Web Chat / Web Call Back

To configure a web chat service, from the left hand side select **Administration** → **Web Interactions** → **Services** from the Presence Unified Manager main menu. Double click in **Services** to open a new tab showing the list of internet services and click on **Create** button to create a new service.

The screenshot shows the Presence Unified Manager interface. The left sidebar has a menu with 'Administration' selected, and 'Services' is highlighted under 'Web Interactions'. The main content area is titled 'Internet services' and contains a table with the following data:

Id	Name	Status	Mode	Actions
7777	MYINTERNETSERVICE	Enabled	Unified	[Icons for edit, delete, and other actions]

At the top right of the table area, there are buttons for 'Import' and 'Create'. Below the table, it says 'Page 1 of 1 (1 items)'. The bottom status bar shows 'Alarms' and some counts.

In the resulting screen, go to **General** section 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 'Presence Unified Manager' interface. The top navigation bar includes the logo, a dropdown menu set to '(New desktop)', and a 'Presence User' profile. The main content area is titled 'Internet services' and 'Create'. A left sidebar lists configuration sections: General, URL, Interface, Texts, Mail, Service levels, and Other. The 'General' section is active, showing fields for 'Id' (400) and 'Name' (PRESENCE INTERNET). Below these are 'ACD' settings, including 'Inbound service' (1 - INBOUND SERVICE), 'Enable chat' (checked, with VDN 1908), and 'Enable callback' (checked, with VDN 1908). There is also a 'Web collaboration' section with 'Enable web collaboration' checked and a 'Linker' field. At the bottom are 'Save' and 'Cancel' buttons. The footer shows an 'Alarms' section with a bell icon and two status indicators (0).

Presence Unified Manager

(New desktop) Presence User

Internet services / Create

Configuration

General

URL

Interface

Texts

Mail

Service levels

Other

General

Identification

Id: 400 Name: PRESENCE INTERNET

ACD

Inbound service: 1 - INBOUND SERVICE

☒ Enable chat: 1908

☒ Enable callback: 1908

Web collaboration

☒ Enable web collaboration

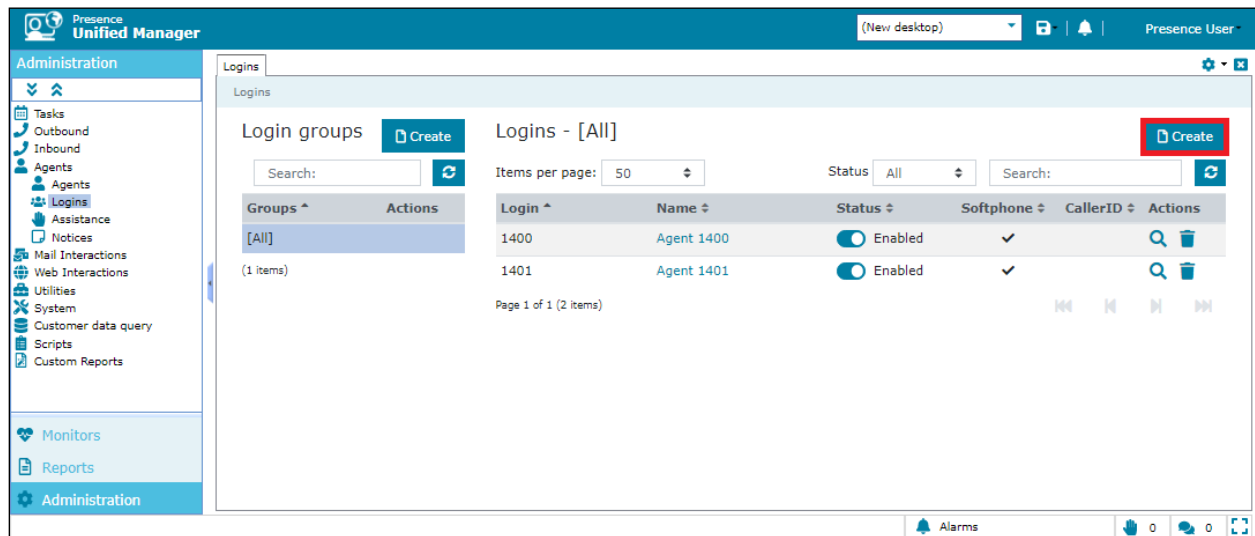
Linker

Save Cancel

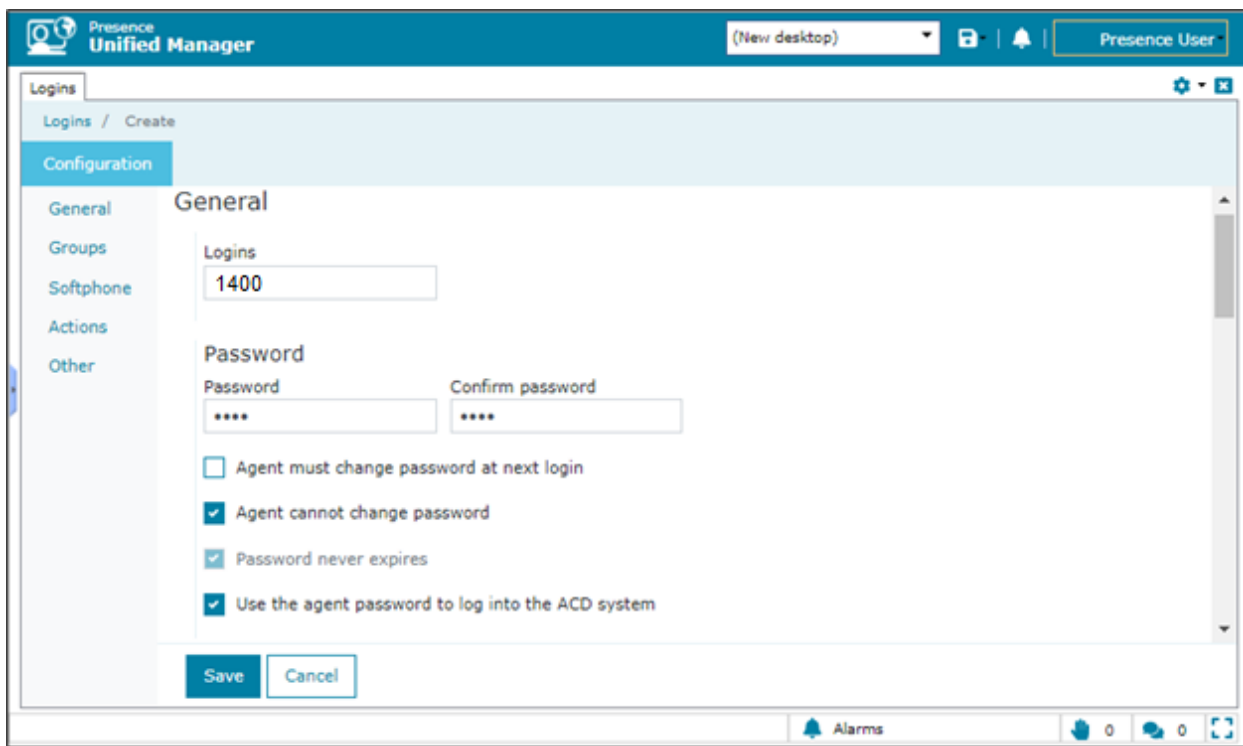
Alarms 0 0

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 Unified Manager main menu select **Administration** → **Agents** → **Logins**. Double click in **Logins** to open a new tab showing the list of login groups and logins and click on **Create** button to create a new login.



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.



Go to **Softphone**, and place a tick in the **Softphone always enabled** field. Click **Save** when done. This is not related to IP Softphone on Communication Manager, this is to enable a toolbar on Presence Agent to allow the agent transfer/conference etc. Also to make outbound calls without having to be on inbound call.

The screenshot shows the 'Softphone' configuration page in the Presence Unified Manager. The page has a blue header with the 'Presence Unified Manager' logo and a user profile 'Presence User'. A left sidebar contains navigation links: 'Logins', 'Configuration', 'General', 'Groups', 'Softphone', 'Actions', and 'Other'. The 'Configuration' section is active, and the 'Softphone' tab is selected. The main content area contains several checkboxes: 'Softphone always enabled' (checked), 'Enable support to insert outbound records' (unchecked), 'Enable manual outbound ACD calls' (unchecked), and 'Show selected only' (unchecked). Below these is a 'Phone book' section with a search bar and a refresh button. A message 'There is no data in the table' is displayed below the search bar, with '(0 items)' underneath. At the bottom of the configuration area are 'Save' and 'Cancel' buttons. The footer of the application shows 'Alarms' and some status icons.

Presence Unified Manager (New desktop) Presence User

Logins / Create

Configuration

General Groups Softphone Actions Other

Softphone

☒ Softphone always enabled

☐ Enable support to insert outbound records

☐ Enable manual outbound ACD calls

☐ Show selected only Search: [refresh]

☐ Phone book

There is no data in the table

(0 items)

Save Cancel

Alarms 0 0

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 tree view with the following items: General (selected), Backup servers, Storage, Channels, SNMP, Alerts, Tracing, Server, Backup Server, Service, Screen Recording, General, and Tracing. The main area of the dialog 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 of the dialog 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, 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 options: 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'. In the 'DMCC Server' section, the 'IP address' is set to '10.10.40.56', the 'Port' is '4721', the 'User' is 'presence', and the 'Password' is masked with dots. In the 'DMCC channel configuration' section, the 'Base port to receive RTP packets' is '50000'. Below this is a table with columns 'Extension', 'Usage', and 'CLAN IP address'. To the right of the table are 'Up' and 'Down' buttons. At the bottom of the 'DMCC channel configuration' section are 'Add', 'Edit', and 'Remove' buttons. At the bottom of the dialog box are 'OK' and 'Cancel' buttons.

Enter a valid recording channel **Extension** and **Password** as configured in **Section 5.10**. Enter the **CLAN IP address** and select **Recording** from the **Usage** drop-down box. Click **OK** when done. Four recording channels were added for compliance testing with none used for playback as these were played back using software and not an Avaya phone. If playback channels are required, select **Playback** from the **Usage** drop-down box.

Note that the CLAN IP address below is the H.323 gatekeeper IP address on AES, which happens to be the IP address of Communication Manager.

The screenshot shows the 'Channel' dialog box with the 'Channel information' tab selected. The 'Extension' is '28903' and there is a '+1' checkbox. The 'Password' is masked with dots. The 'Usage' is set to 'Recording' in a drop-down menu. The 'CLAN IP address' is '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 image shows a 'Presence Recording Server Configuration' dialog box 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 'Base port to receive RTP packets' field (50000) and a table with columns 'Extension', 'Usage', and 'CLAN IP address'. The table contains four rows of data, all with 'Recording' usage and '10.10.40.59' 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.

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

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 Unified Manager, 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 'New recording plan' dialog box with the 'General' tab selected. The left-hand pane contains a tree view with 'General', 'Services', and 'Groups'. The main area is titled 'General' and contains the following fields and options:

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

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

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

The screenshot shows the 'New recording plan' dialog box with the 'Services' tab selected. The left-hand pane contains a tree view with 'General', 'Services', and 'Groups'. The main area is titled 'Services' and contains the following elements:

- Service id:** 100
- Add icon:** A document icon with a plus sign, highlighted with a red box.
- Table:** A table with columns 'Id', 'Name', and 'Type'. The table is currently empty.

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

New recording plan

General
Services
Groups

Services

Service id: 100

Id	Name	Type
100	PRESENCE INBOUND	Inbound

OK Cancel Apply

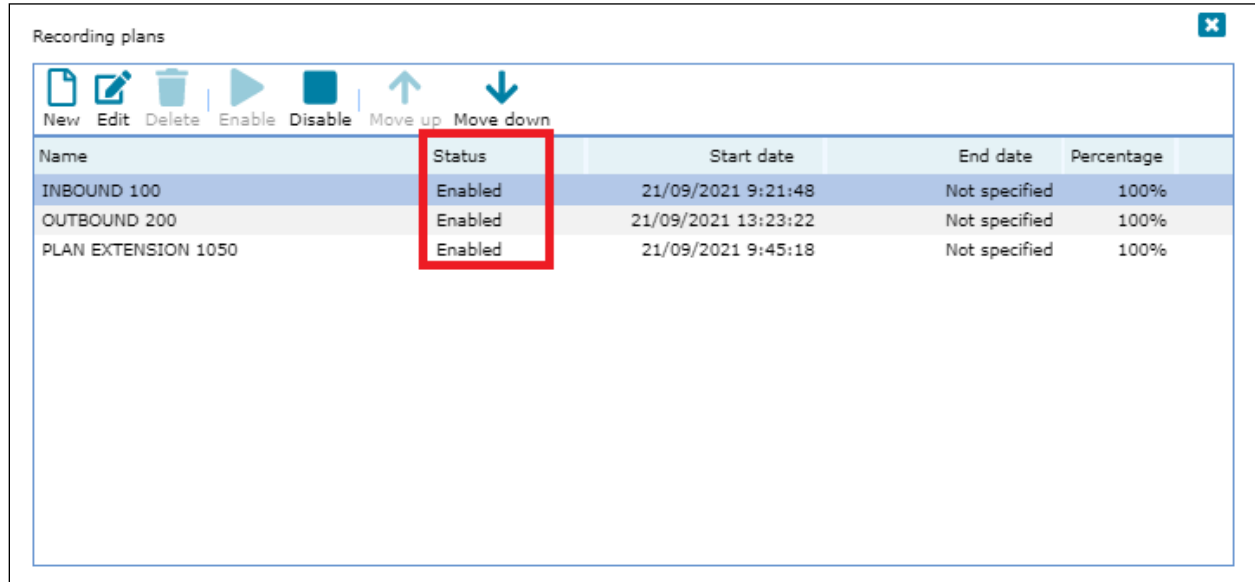
The screen below will be displayed, summarizing the added recording plans. Note that the status shows **Disabled**.

Recording plans

New Edit Delete Enable Disable Move up Move down

Name	Status	Start date	End date	Percentage
INBOUND 100	Disabled	21/09/2021 9:21:48	Not specified	100%
OUTBOUND 200	Disabled	21/09/2021 13:23:22	Not specified	100%
PLAN EXTENSION 1050	Disabled	21/09/2021 9:45:18	Not specified	100%

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



Recording plans

Name	Status	Start date	End date	Percentage
INBOUND 100	Enabled	21/09/2021 9:21:48	Not specified	100%
OUTBOUND 200	Enabled	21/09/2021 13:23:22	Not specified	100%
PLAN EXTENSION 1050	Enabled	21/09/2021 9:45:18	Not specified	100%

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

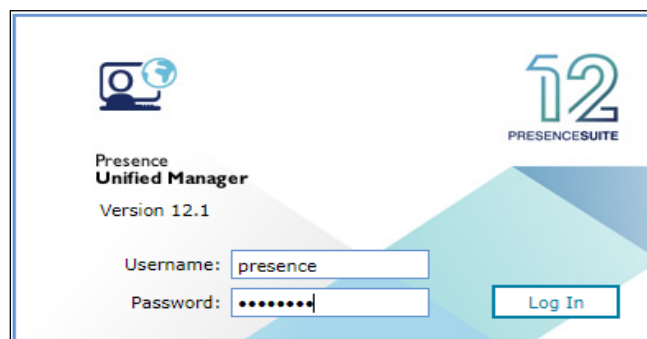
7.3.3. Add stations to Presence Recording

The extensions used for the Presence Agents do not have to be manually added in this section as when an agent is logged into the Presence system, the extension is added in the Presence Recording Server automatically, in case it is necessary to record calls related to a service.

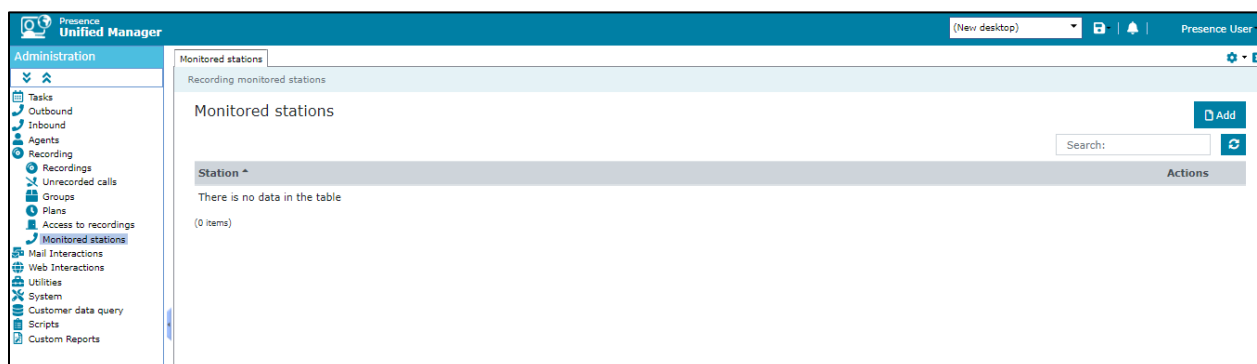
To record non-agent stations, each station that is to be recorded must be added to Presence Recording. Create a recording group adding these stations and finally create a recording plan adding this group.

Note: For compliance testing extension 1050 was used as a Supervisors station/extension. Malicious calls were sent to this supervisor and these calls would need to be recorded. The section below shows the steps necessary to add extension 1050 for call recording.

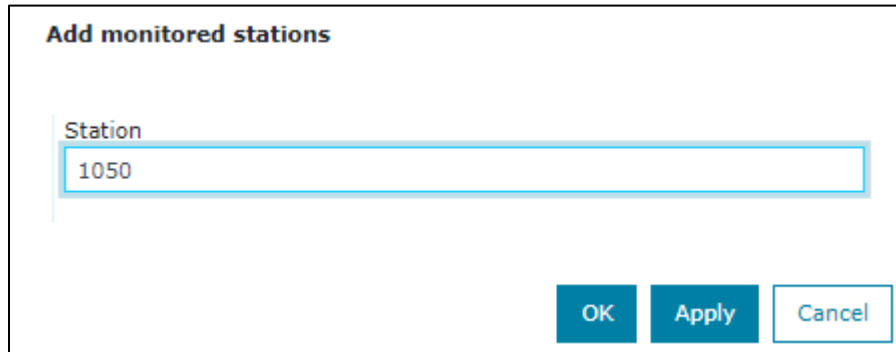
Enter **https://<ip-addr>/websupervisor** as the URL in an Internet browser to logging into Presence Unified Manager. For compliance testing Presence Unified Manager was installed on the same server as the other Presence Suite modules. The username and password that appear in the **User** and **Password** fields are created during the Presence Server installation.



Select **Administration → Recording → Monitored stations**, and click the **Add** button. Calls that are placed via either of these stations will be recorded according to the recording plan configured in **Section 7.3.5**.

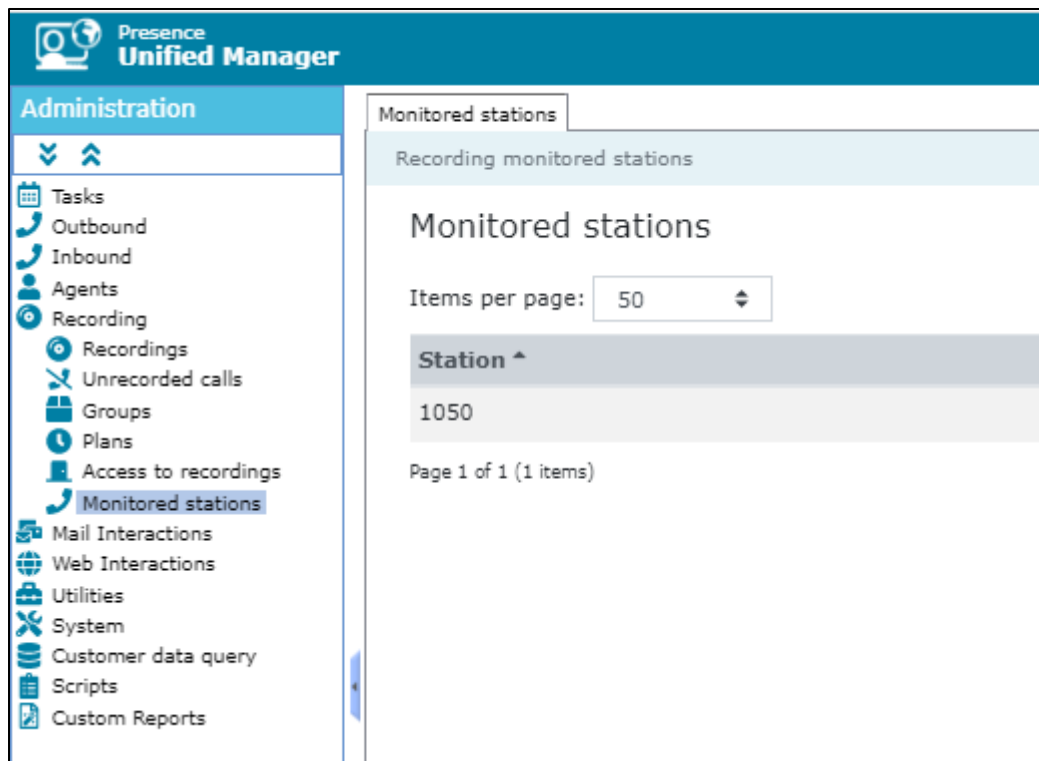


In the resulting screen, add extension **1050** in the **Station** field and click **OK**.



The image shows a dialog box titled "Add monitored stations". It contains a text input field labeled "Station" with the value "1050" entered. At the bottom right, there are three buttons: "OK", "Apply", and "Cancel".

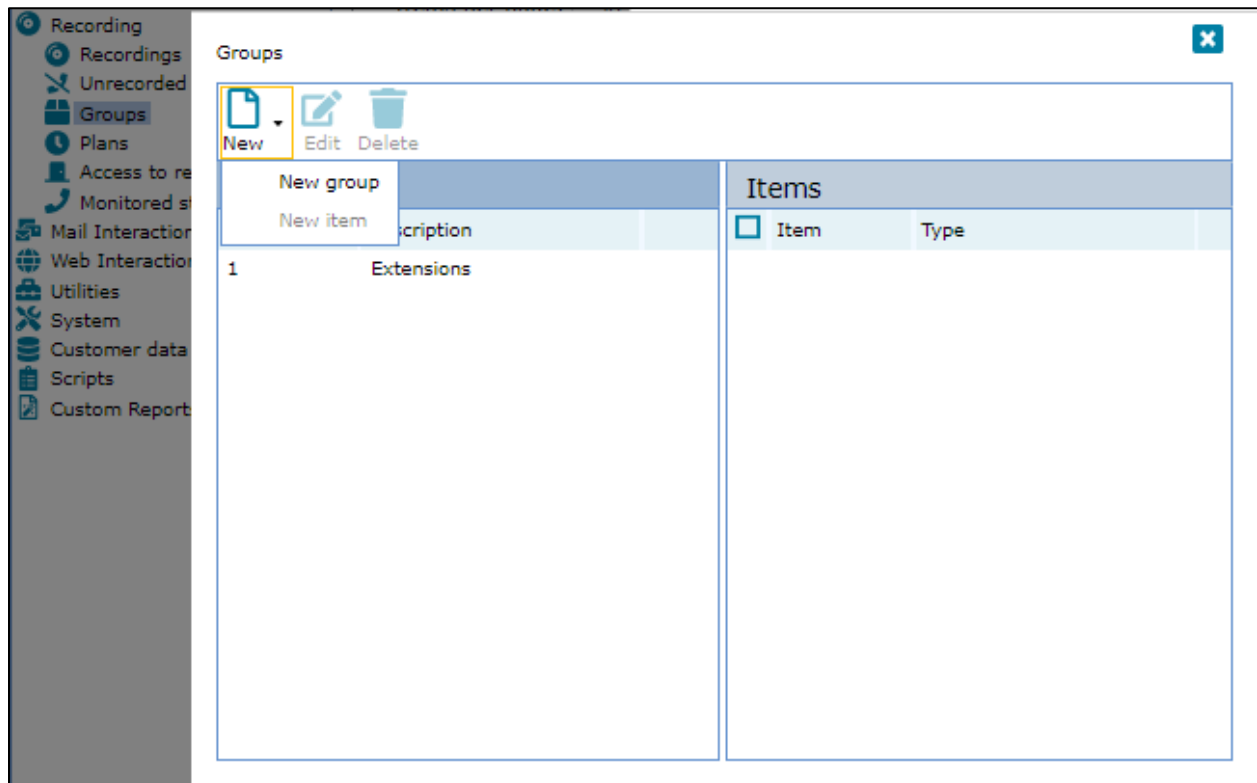
Station **1050** was added into Presence Recording.



The image shows the "Presence Unified Manager" interface. On the left is a navigation menu with options like Tasks, Outbound, Inbound, Agents, Recording, Recordings, Unrecorded calls, Groups, Plans, Access to recordings, Monitored stations (highlighted), Mail Interactions, Web Interactions, Utilities, System, Customer data query, Scripts, and Custom Reports. The main area is titled "Monitored stations" and shows a list of "Recording monitored stations". The list has a header "Station ^" and one item "1050". Below the list, it says "Page 1 of 1 (1 items)".

7.3.4. Create a new recording group

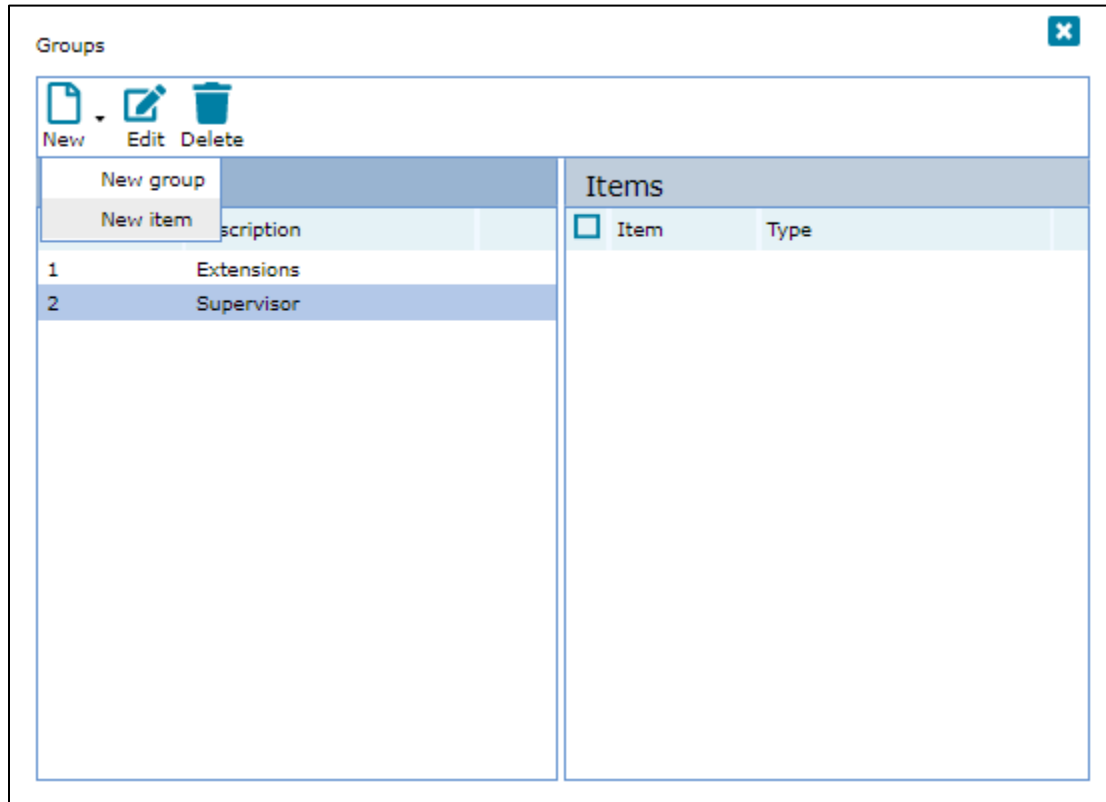
Using the Presence Unified Manager application, double click on **Administration** → **Recording** → **Groups** and click on **New** (drop-down box) and select **New group**.



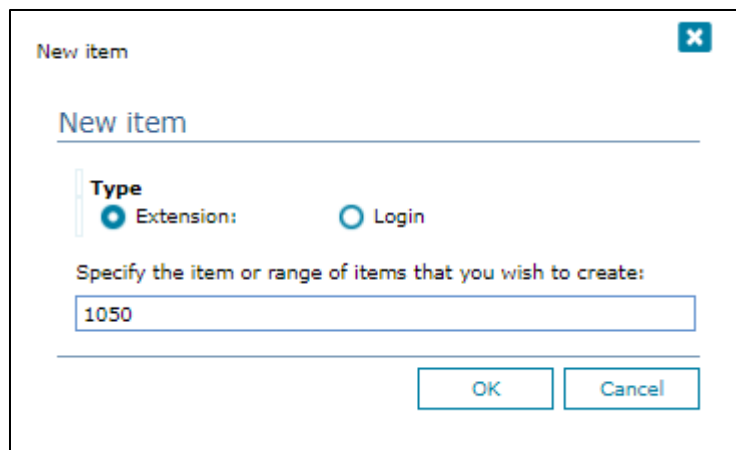
Enter the details for the new group. Note any number is used for code. Click on **OK** when finished.

The 'Group information' dialog box is shown. It has a title bar with a close button. The main content area is titled 'New group'. Below the title, there are two input fields: 'Id:' with the value '2' and 'Description:' with the value 'Supervisor'. At the bottom right, there are two buttons: 'OK' and 'Cancel'.

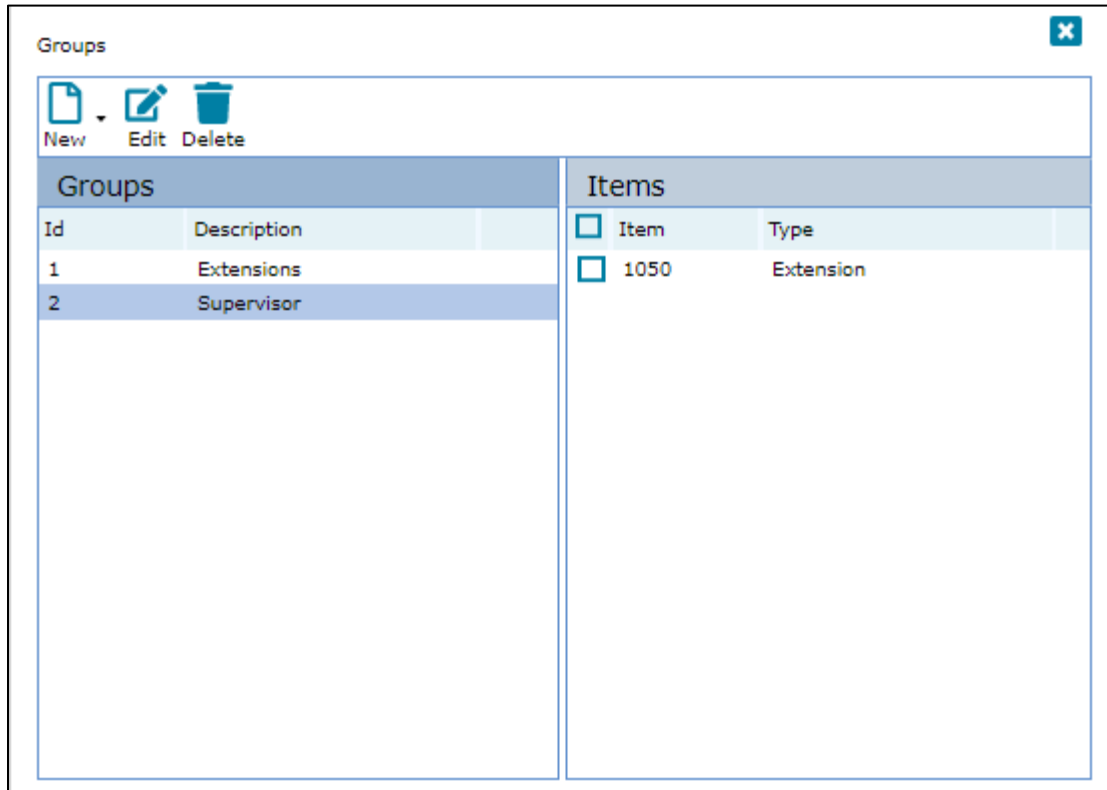
Select the group created and click on **New** (drop-down box) and select **New item**.



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

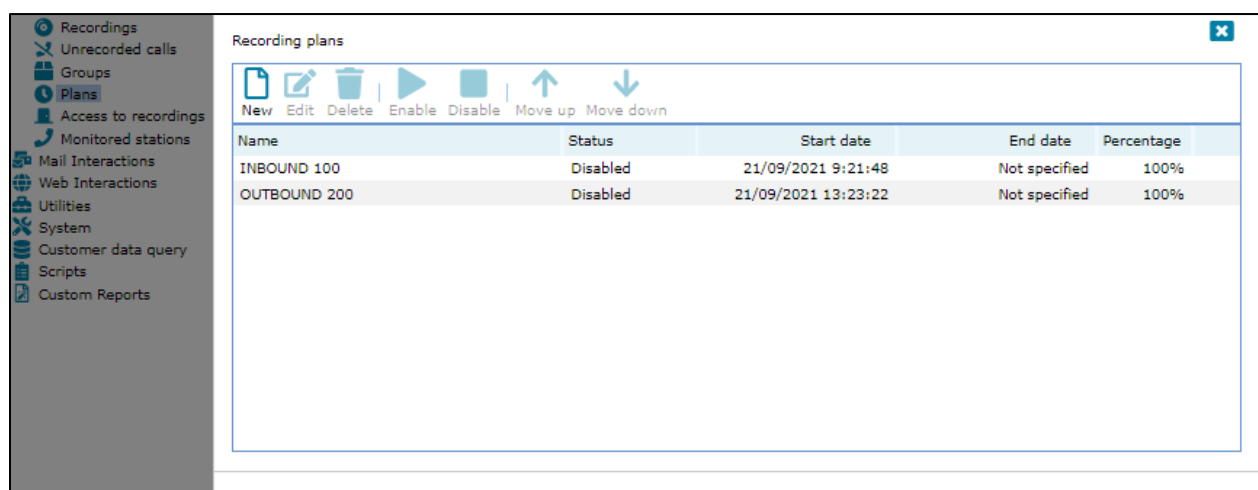


Once **OK** is clicked above the following screen shows the added station.



7.3.5. Create a recording plan for extensions

Double click on **Administration** → **Recording** → **Plans** → **New**.



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.

The screenshot shows a window titled "Plan PLAN EXTENSION 1050" with a sidebar containing "General", "Services", and "Groups". The "General" tab is active. The "Name" field contains "PLAN EXTENSION 1050". The "Resource profile" dropdown is set to "General". The "Percentage to record" dropdown is set to "General" and the percentage value is "100 %". The "Start" section has "Immediate" selected with a radio button, and the "Date" option is also selected with a radio button. The date is "21/09/2021" and the time is "9 :45". The "End" section has "Indeterminate" selected with a radio button, and the "Date" option is also selected with a radio button. There are two checkboxes: "Allow the agent to pause recordings" and "Allow the agent to stop recordings", both of which are unchecked. At the bottom right are "OK", "Cancel", and "Apply" buttons.

On the **Groups** window set the **Group id** created click on the add icon. Click on **OK** to create the recording plan.

The screenshot shows the same window titled "Plan PLAN EXTENSION 1050", but the "Groups" tab is active in the sidebar. The "Group id" field contains "2" and has an information icon. Below the field is a table with columns "Id" and "Description". The table has one row with "1" in the "Id" column and "Extensions" in the "Description" column. At the bottom right are "OK", "Cancel", and "Apply" buttons.

Id	Description
1	Extensions

In the screen that display the added recording plans, select the recording plan created and click **Enable**, the status will now appear as **Enabled**.

Recording plans

New

Edit

Delete

Enable

Disable

Move up

Move down

Name	Status	Start date	End date	Percentage
INBOUND 100	Disabled	21/09/2021 9:21:48	Not specified	100%
OUTBOUND 200	Disabled	21/09/2021 13:23:22	Not specified	100%
PLAN EXTENSION 1050	Disabled	21/09/2021 9:45:18	Not specified	100%

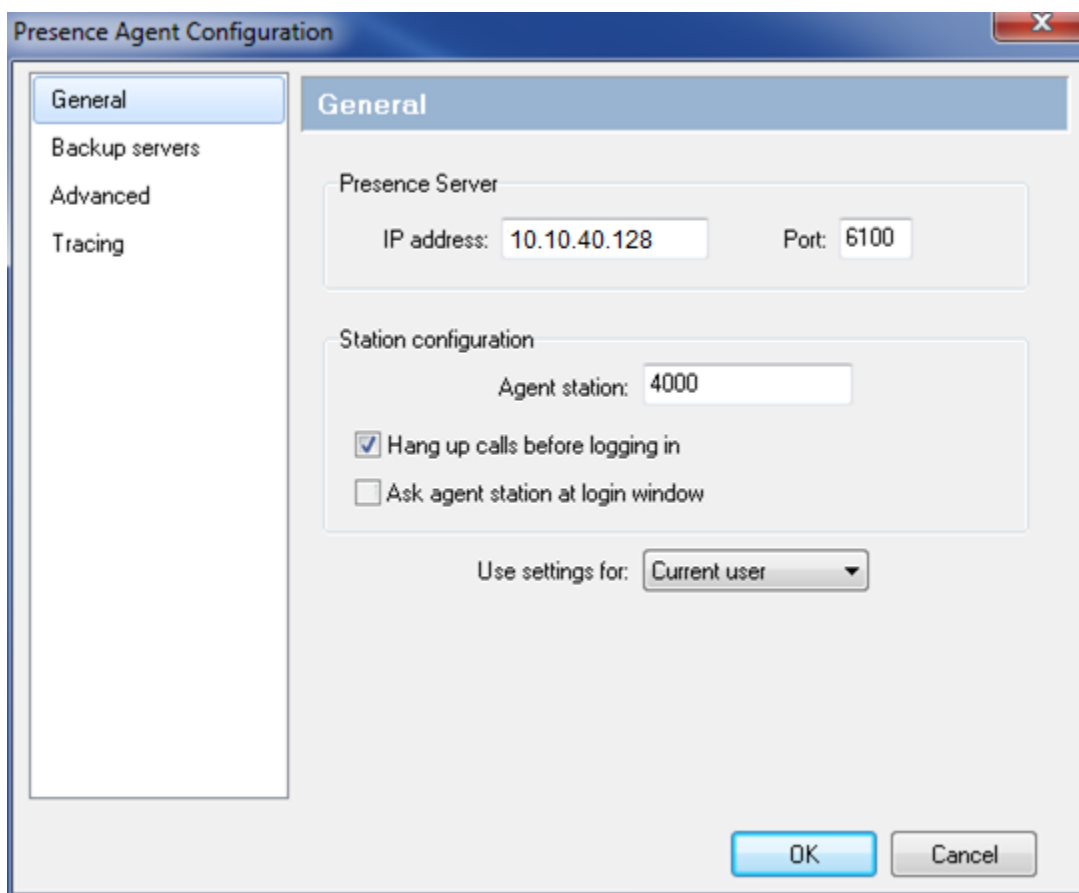
Edit

Enable

Disable

7.4. Presence Agent Configuration

The following steps are carried out on the Presence Suite agent PC. Prior to installing the Presence Client application, ensure that the DBExpress driver (dbexpoda40.dll) is located in the **C:\Windows\SysWOW64** 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.



The screenshot shows the 'Presence Agent Configuration' dialog box with the 'General' tab selected. The 'General' tab is highlighted in the left sidebar and the main content area. The 'Presence Server' section contains two text boxes: 'IP address' with the value '10.10.40.128' and 'Port' with the value '6100'. The 'Station configuration' section contains a text box for 'Agent station' with the value '4000', a checked checkbox for 'Hang up calls before logging in', and an unchecked checkbox for 'Ask agent station at login window'. Below these is a dropdown menu for 'Use settings for' with 'Current user' selected. At the bottom right are 'OK' and 'Cancel' buttons.

Field	Value
IP address	10.10.40.128
Port	6100
Agent station	4000
Hang up calls before logging in	<input checked="" type="checkbox"/>
Ask agent station at login window	<input type="checkbox"/>
Use settings for	Current user

8. Verification Steps

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

8.1. Verify Avaya Aura® Communication Manager CTI Link

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

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

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

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

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

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

8.2. Verify TSAPI Link and DMCC

This section will verify both the TAPI and DMCC links.

8.2.1. 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**.

AVAYA

Application Enablement Services
Management Console

Welcome: User cust
Last login: Mon Jan 10 19:14:39 2022 from 192.168.40.240
Number of prior failed login attempts: 0
HostName/IP: aes81xvmpg/10.10.40.38
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.1.3.2.0.4-0
Server Date and Time: Wed Jan 12 14:28:17 GMT 2022
HA Status: Not Configured

Status | Status and Control | TSAPI Service SummaryHome | 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

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	cm81xvmpg	1	Talking	Mon Jan 10 19:00:29 2022	Online	18	7	19	19	30
<input type="radio"/>	2	cm81large	1	Switch Down	Mon Dec 6 10:45:59 2021	Online	18	0	0	0	30

OnlineOffline

For service-wide information, choose one of the following:
TSAPI Service Status | TLink Status | User Status

Clicking on **User Status** from the previous screen shot reveals the CTI users connected to AES using TSAPI, below shows seven instances of the user Presence connected. These individual connections are due to the fact that the Presence Suite is made of several modules each having their own direct TSAPI connection to AES.

AVAYA

Application Enablement Services
Management Console

Last login: Mon Jan 10 19:14:39 2022 from 192.168.40.240
Number of prior failed login attempts: 0
HostName/IP: aes81xvmpg/10.10.40.38
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.1.3.2.0.4-0
Server Date and Time: Wed Jan 12 14:28:54 GMT 2022
HA Status: Not Configured

Status | Status and Control | TSAPI Service SummaryHome | 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

User Management

Utilities

Help

CTI User Status

☐ Enable page refresh every 60 seconds

CTI UsersAll UsersSubmit

Open Streams 12
Closed Streams 4

Open Streams

Name	Time Opened	Time Closed	Tlink Name
DMCCLCSUserDoNotModify	Mon 06 Dec 2021 10:46:56 AM GMT		AVAYA#CM81XVMPG#CSTA#AES81XVMPG
DMCCLCSUserDoNotModify	Mon 06 Dec 2021 10:46:56 AM GMT		AVAYA#CM81LARGE#CSTA#AES81XVMPG
DMCCLCSUserDoNotModify	Mon 06 Dec 2021 10:46:56 AM GMT		AVAYA#CM81XVMPG#CSTA#AES81XVMPG
DMCCLCSUserDoNotModify	Mon 06 Dec 2021 10:46:57 AM GMT		AVAYA#CM81LARGE#CSTA#AES81XVMPG
nice	Mon 13 Dec 2021 03:14:48 PM GMT		AVAYA#CM81XVMPG#CSTA#AES81XVMPG
presence	Wed 12 Jan 2022 02:12:51 PM GMT		AVAYA#CM81XVMPG#CSTA#AES81XVMPG
presence	Wed 12 Jan 2022 02:12:52 PM GMT		AVAYA#CM81XVMPG#CSTA#AES81XVMPG
presence	Wed 12 Jan 2022 02:12:52 PM GMT		AVAYA#CM81XVMPG#CSTA#AES81XVMPG
presence	Wed 12 Jan 2022 02:12:52 PM GMT		AVAYA#CM81XVMPG#CSTA#AES81XVMPG
presence	Wed 12 Jan 2022 02:12:52 PM GMT		AVAYA#CM81XVMPG#CSTA#AES81XVMPG
presence	Wed 12 Jan 2022 02:12:52 PM GMT		AVAYA#CM81XVMPG#CSTA#AES81XVMPG
presence	Wed 12 Jan 2022 02:12:53 PM GMT		AVAYA#CM81XVMPG#CSTA#AES81XVMPG

Show Closed StreamsClose All Opened StreamsBack

8.2.2. 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 module 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.

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 Thu Jan 13 12:25:14 GMT 2022

Service Uptime: 38 days, 1 hours 38 minutes

Number of Active Sessions: 2

Number of Sessions Created Since Service Boot: 33

Number of Existing Devices: 16

Number of Devices Created Since Service Boot: 63

	Session ID	User	Application	Far-end Identifier	Connection Type	# of Associated Devices
<input type="checkbox"/>	78C035EB7FB96E576 9B1176AA7E19104-15	nice		10.10.40.126	XML Unencrypted	8
<input type="checkbox"/>	95CEFABB6354FBCA6 4D0B4383DA3D80F-32	presence	precsrvr.exe	10.10.40.128	XML Unencrypted	8

Terminate Sessions Show Terminated Sessions

Item 1-2 of 2

1Go

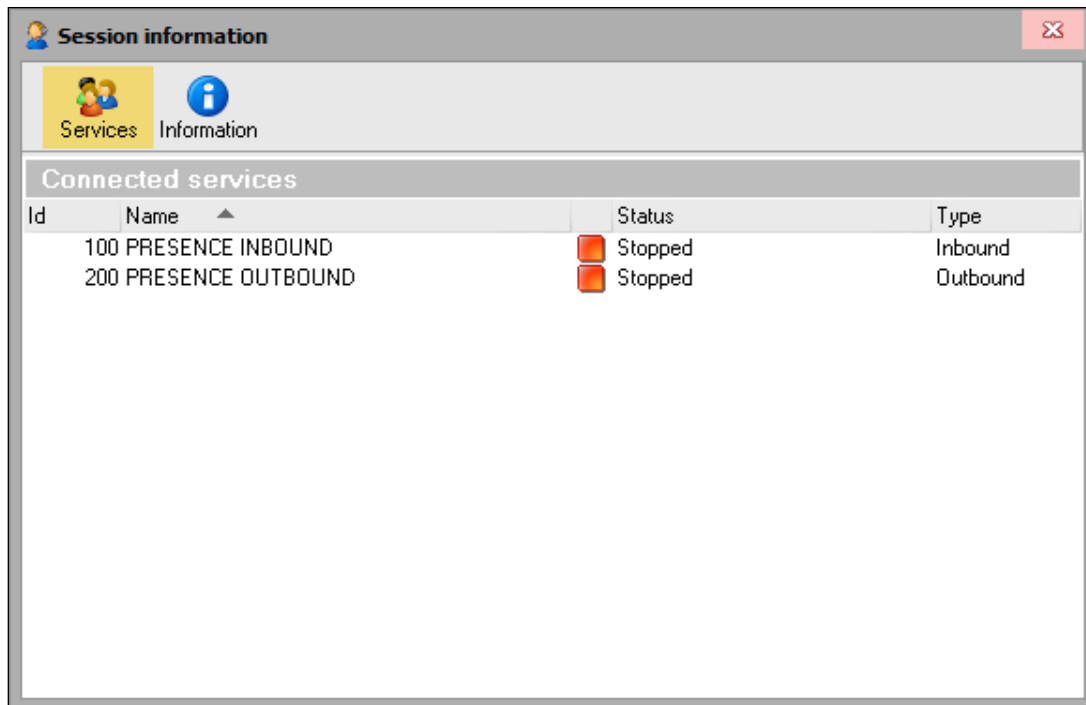
8.3. Verify Presence Suite

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



The image shows the Presence Agent Version 12.1 login dialog box. It features a headset icon and the text 'Presence Agent Version 12.1' on the left, and a large '12' logo with 'PRESENCESUITE' below it on the right. The login fields are: 'Login:' with the value '1400', 'Password:' with four dots, and 'Station:' with the value '1001'. There are 'Cancel' and 'OK' buttons at the bottom right.

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



The image shows the 'Session information' window. It has a 'Services' button (selected) and an 'Information' button. Below the buttons is a table titled 'Connected services'.

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

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



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



An outbound call is placed and answered.



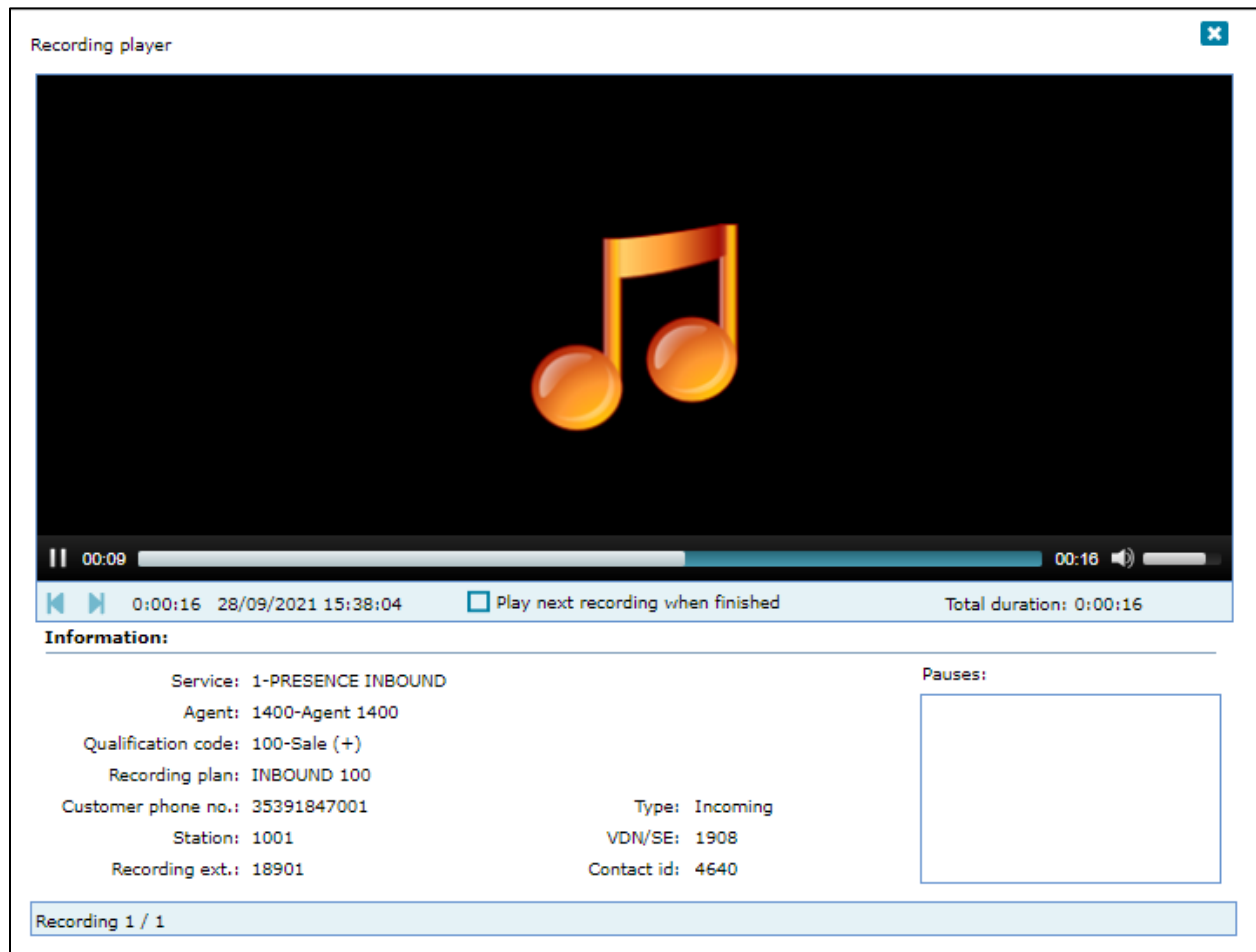
8.4. Verify Presence Recording

Using Presence Unified Manager, 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 screenshot shows the Presence Unified Manager interface. The left sidebar contains a navigation menu with options like Administration, Tasks, Outbound, Inbound, Agents, Recording, Groups, Plans, Access to recordings, Monitored stations, Mail Interactions, Web Interactions, Utilities, System, Customer data query, Scripts, and Custom Reports. The main area is titled 'Recordings from query QUERY INBOUND SERVICE'. It displays a table with columns: Audio, Id, Date, Service, Group id, Extension, Agent, Duration, Total duration, Phone, and Call type. The table lists 19 recordings. Below the table, there is a summary section showing 'No. of recordings: 99', 'Current pos.: 1', 'Selected: 1', and 'Last update: 13/01/2022 14:28:03'. There is also a 'Related recordings' section with a similar table structure. At the bottom, there is a message: 'Activate Windows Go to Settings to activate Windows.'

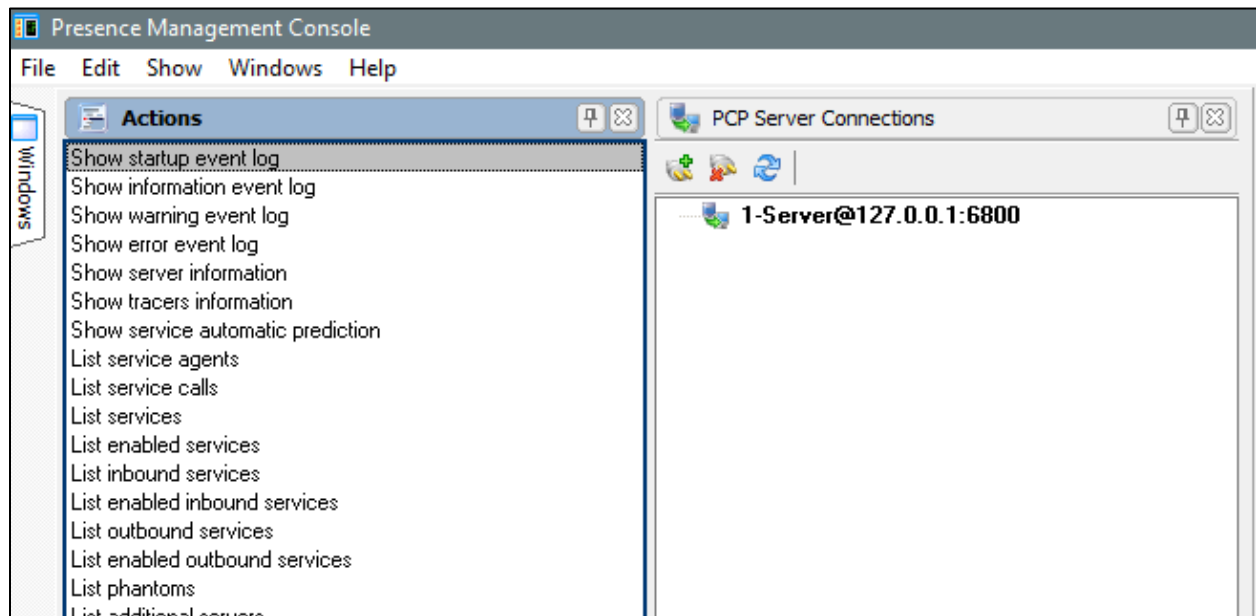
Audio	Id	Date	Service	Group id	Extension	Agent	Duration	Total duration	Phone	Call type
<input type="checkbox"/>	22	28/09/2021 15:38:04	1	1001	1400	1400	0:00:16	0:00:16	35391847001	Incoming
<input type="checkbox"/>	23	28/09/2021 17:30:26	1	1101	1401	1401	0:00:08	0:00:08	35391847001	Incoming
<input type="checkbox"/>	24	28/09/2021 17:30:42	1	1001	1400	1400	0:00:09	0:00:10	35391847001	Incoming
<input type="checkbox"/>	25	28/09/2021 17:31:38	1	1001	1400	1400	0:00:38	0:00:38	35391847001	Incoming
<input type="checkbox"/>	26	28/09/2021 17:32:07	1	1001	1400	1400	0:00:08	0:00:09	1101	Outgoing
<input type="checkbox"/>	27	28/09/2021 17:32:07	1	1101	1401	1401	0:00:17	0:00:18	1001	Incoming
<input type="checkbox"/>	28	28/09/2021 17:32:39	1	1101	1401	1401	0:00:33	0:00:33	35391847001	Incoming
<input type="checkbox"/>	29	28/09/2021 17:33:05	1	1101	1401	1401	0:00:07	0:00:07	1400	Outgoing
<input type="checkbox"/>	30	28/09/2021 17:33:05	1	1001	1400	1400	0:00:13	0:00:14	1101	Incoming
<input type="checkbox"/>	31	28/09/2021 18:00:18	1	1101	1401	1401	0:00:31	0:00:32	35391847001	Incoming
<input type="checkbox"/>	32	28/09/2021 18:00:53	1	1001	1400	1400	0:00:13	0:00:14	35391847001	Incoming
<input type="checkbox"/>	33	28/09/2021 18:01:19	1	1001	1400	1400	0:00:20	0:00:20	35391847001	Incoming
<input type="checkbox"/>	34	28/09/2021 18:01:41	1	1101	1401	1401	0:00:10	0:00:10	35391847001	Incoming
<input type="checkbox"/>	35	28/09/2021 18:16:35	1	1101	1401	1401	0:00:20	0:00:20	35391847001	Incoming
<input type="checkbox"/>	36	28/09/2021 18:16:51	1	1101	1401	1401	0:00:04	0:00:05	5250	Outgoing
<input type="checkbox"/>	37	28/09/2021 18:17:17	1	1001	1400	1400	0:00:17	0:00:18	35391847001	Incoming
<input type="checkbox"/>	38	28/09/2021 18:17:28	1	1001	1400	1400	0:00:06	0:00:06	5250	Outgoing

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



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@127.0.0.1:6800** in the **PCP Server Connections** pane of the Management Console. To open the startup event log, double click **Show startup event log** in the **Actions** pane.



Verify successful CTI connection and service startup.

```
1-Server@127.0.0.1:6800 => SHOW LOG STARTUP
12/01 16:13:42 Server started
12/01 16:13:42 Service INBOUND MAILBOX SERVICE loaded
12/01 16:13:42 Service PRESENCE INBOUND loaded
12/01 16:13:42 Loading inbound services (2 services)...
12/01 16:13:42 Loading inbound groups (0 groups)...
12/01 16:13:42 Service OUTBOUND SERVICE loaded
12/01 16:13:42 Loading outbound services (1 services)...
12/01 16:13:41 Updating agent connection records...
12/01 16:13:41 Connected to primary CTI link AVAYA#CM80XVMFG#CSTA#AES80XVMFG
12/01 16:13:39 Connecting to CTI link
12/01 16:13:36 Connecting to database
12/01 16:13:36 Initializing server...
```

9. Conclusion

These Application Notes describe the configuration steps required for Presence Suite R12.1 to successfully interoperate with Avaya Aura® Communication Manager R8.1 using Avaya Aura® Application Enablement Services R8.1. All feature functionality and serviceability test cases were completed successfully with observations noted in **Section 2.2**.

10. Additional References

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

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

- [1] *Administering Avaya Aura® Communication Manager, Release 8.1.x, Issue 12, Jul 2021*
- [2] *Administering Avaya Aura® Session Manager, Release 8.1.x, Issue 8, Feb 2021*
- [3] *Avaya Aura® Communication Manager Screen Reference, Release 8.1.x Issue 12 September 2021*
- [4] *Avaya Aura® Communication Manager Feature Description and Implementation, Release 8.1.x Issue 17 August 2021*
- [5] *Avaya Aura® Communication Manager Special Application Features, October 2020*
- [6] *Avaya Aura® Application Enablement Services Administration and Maintenance Guide Release 8.1*

The following documentation is available on request from Enghouse at www.enghouseinteractive.es/en

- [7] *ACD Sys Presence Unified Manager Manual Presence Suite, V12.1*
- [8] *Presence Installation Guides Presence Software, V12.1*
- [9] *PBX/ACD Requirements Presence Software, V12.1*

©2022 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.