



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

---

# **Application Notes for Beta 80 Life 1st and emma CAD CTI with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services – Issue 1.0**

### **Abstract**

These Application Notes describe the configuration steps required for Beta 80 Life 1st and emma CAD CTI R4.5 to interoperate with Avaya Aura® Communication Manager R8.1 and Avaya Aura® Application Enablement Services R8.1 using the Device, Media and Call Control Application Programming Interface. The Beta 80 Life 1st and emma CAD CTI platform provides Public Safety Answering Points (PSAP) for emergency service 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 configuration steps required for Beta 80 Life 1st and emma CAD CTI R4.5 to interoperate with Avaya Aura® Communication Manager R8.1 and Avaya Aura® Application Enablement Services R8.1 using the Device, Media and Call Control (DMCC) Application Programming Interface (API) on Avaya Aura® Application Enablement Services (Application Enablement Services).

The Beta 80 Life 1st and emma CAD CTI (CAD CTI) platform integrates with Application Enablement Services and provides Public Safety Answering Points (PSAP) agents with an application interface aimed at managing emergency calls hands-free. Beta 80 CAD platform complements Avaya Aura® solution in providing Public Safety Answering Points using a complete, full featured, Computer Aided Dispatch platform (CAD). CAD helps PSAP professionals to streamline emergency calls processing by automatically retrieving and displaying the caller's position, suggesting standard operating procedures Agents and dispatchers have to follow given the specific call for service (CFS), monitoring dispatched units and providing necessary information for dispatchers to assure a quick and effective engagement of first responders and resources upon the creation of new incidents.

The Application Enablement Services integration allows call takers and dispatchers to benefit from a broader range of integration services between Avaya and the Beta 80 CAD platform. Integration is performed leveraging on the Application Enablement Services DMCC.NET interface.

## 2. General Test Approach and Test Results

The general test approach was to validate the ability of CAD CTI to correctly and successfully connect to Application Enablement Services to handle and control Communication Manager endpoints in a variety of call scenarios. Agents were logged into various Avaya endpoints (outlined in **Section 4**) using the CAD CTI agent desktop provided by Beta 80. Each agent was assigned to a specific Avaya endpoint (SIP, H.323 and Digital). Calls were made to and from these endpoints using the agent desktop to control the Avaya endpoints. The collection of telephony events from Application Enablement Services allowed the agents to be mutually aware of their presence status and to produce advanced reports and statistics.

**Note:** To test the ability of agents handling PSTN calls to various emergency numbers, specific routing on the DevConnect lab had to be created to mimic that found in production on real sites where this solution is being used. Both calls to an ACD queue and calls routed to the CAD CTI using adjunct routing were created by simulating a PSTN using an Avaya Session Border Controller and SIP trunks to Communication Manager via Session Manager. Calls were made to very specific numbers that terminated on various VDN's setup to act as emergency numbers such as, 112 (cross-agency emergency), 113 (police), 115 (fire), 118 (ambulance service). Beta 80 also provide the agents with the ability to cherry pick calls in a queue.

**Note:** See **Appendix** to follow the call routing setup that was used to mimic the 'cherry picking' service that Beta 80 provides to their agents.

CAD CTI makes use of the DMCC API in Application Enablement Services. The DMCC APIs provided by Application Enablement Services enable applications to access the physical device, media and basic third-party call control capabilities provided by Communication Manager. Device control enables applications to manipulate and monitor the physical aspects of devices, such as buttons, lamps, the display and the ringer. Applications can simulate manual actions on devices and obtain the status of their physical elements. Call control makes use of the Telephony Services API (TSAPI) service to provide third-party call control capabilities, such as the ability to place calls, create conferences, transfer calls, reconnect calls, and monitor call control events.

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 these DevConnect Application Notes 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 Beta 80 Life 1st and emma CAD CTI did not include use of any specific encryption features as requested by Beta 80.

## **2.1. Interoperability Compliance Testing**

The interoperability compliance test included both feature functionality and serviceability testing. The feature functionality testing focused on interacting with the CAD CTI platform in different call scenarios. The tests included:

- Agent login
- Agent's status selection
- Agent auto/manual answer mode selection
- Dispatcher/Call Taker presence and chat service
- Make Call
- Call pick up with CLI Import (into the CAD client)
- Call hang up
- Call hold/resume
- Call Transfer (blind or with consultation)
- Conference

- Phone book /with click-to call
- DTMF relay

## 2.2. Test Results

All test cases were executed successfully.

## 2.3. Support

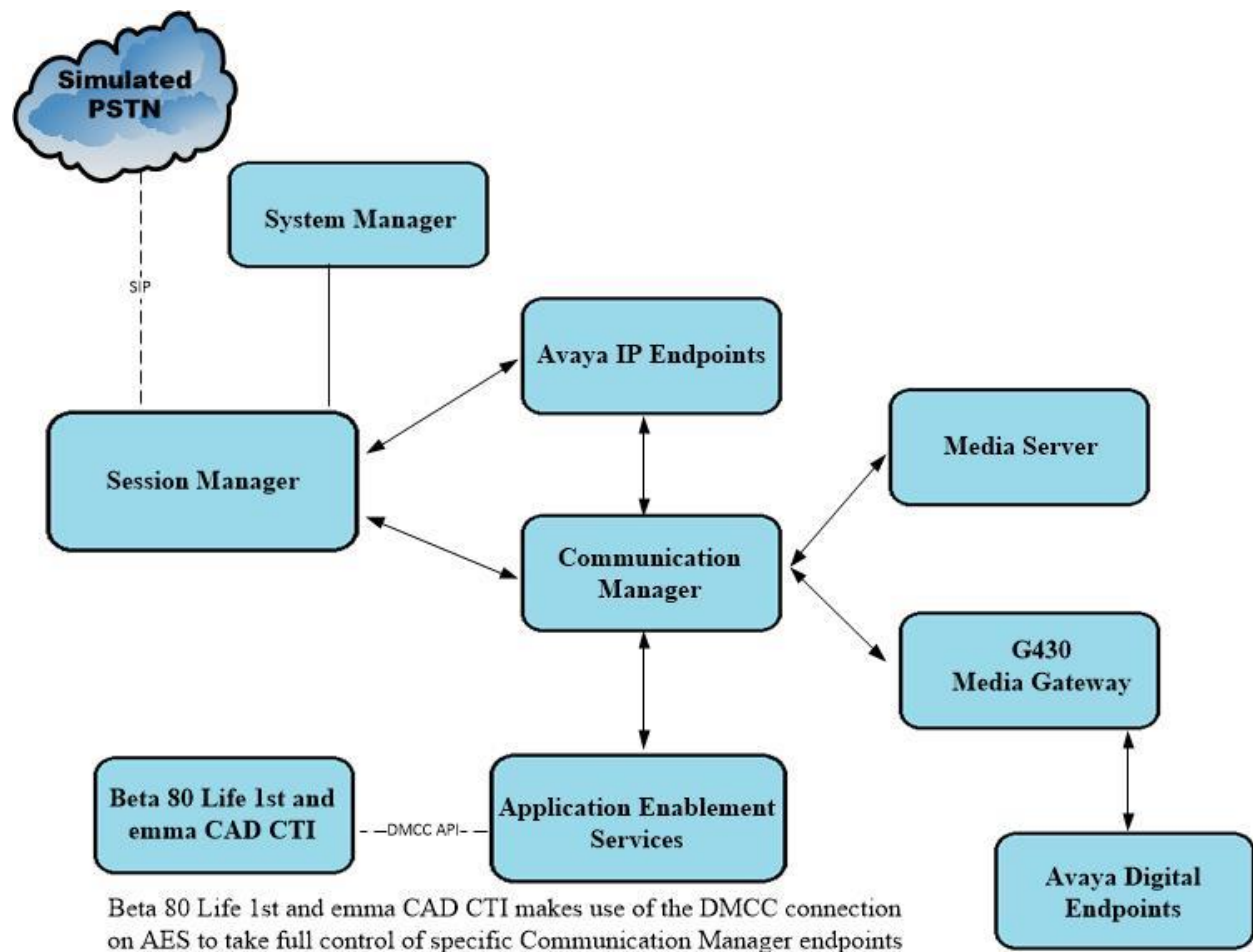
For technical support on Beta 80 Life 1st and emma CAD CTI products, please visit the website at <http://www.capitacontrolsolutions.co.uk/> or contact Beta 80 as follows:

- Web: <https://beta80group.it/en/>
- Email: [sales@beta80group.com](mailto:sales@beta80group.com)

### 3. Reference Configuration

**Figure 1** below shows Avaya Aura® Communication Manager serving Digital, H.323 and SIP endpoints with Avaya Aura® Application Enablement Services providing a DMCC interface to which the Beta 80 Life 1st and emma CAD CTI application connects to. Avaya Aura® Session Manager provides the point of registration for Avaya SIP endpoints. Avaya Aura® System Manager provides a means to manage and configure Session Manager. Calls from the PSTN are simulated using an Avaya Session Border Controller providing calls over a SIP trunk to Session Manager.

**Note:** SIP, H.323 and Digital endpoints were used during compliance testing.



**Figure 1: Connection of Beta 80 Life 1st and emma CAD CTI with Avaya Aura® Communication Manager R8.1 and Avaya Aura® Application Enablement Services R8.1**

## 4. Equipment and Software Validated

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

Avaya Equipment	Software / Firmware Version
Avaya Aura® System Manager running on a virtual server	System Manager 8.1.2.0 Build No. – 8.1.0.0.733078 Software Update Revision No: 8.1.2.0.0611261 Feature Pack 2
Avaya Aura® Session Manager running on a virtual server	Session Manager R8.1 Build No. – 8.1.2.0.812039
Avaya Aura® Communication Manager running on a virtual server	R8.1.2.0 – FP2 R018x.00.0.890.0 Update ID 01.0.890.0-26095
Avaya Aura® Application Enablement Services	R8.1.2 8.1.2.1.0.6-0
Avaya G430 Media Gateway	41.16.0 /1
Avaya Aura® Media Server	Appliance Version R8.0.0.12 Media Server 8.0.0.169 Element Manager 8.0.0.169
Avaya 96x1 SIP Deskphone	7.1.2.0.14
Avaya J179 H323 Deskphone	6.8304
Avaya 9508 Digital Deskphone	2.0
Beta 80 Equipment	Software / Firmware Version
Beta 80 emma/Life 1st CAD	6.11
Beta 80 emma/Life 1st CTI	4.5

## 5. Configure Avaya Aura® Communication Manager

The configuration and verification operations illustrated in this section are performed using the Communication Manager System Access Terminal (SAT). 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 as referenced in **Section 10**. The configuration operations described in this section can be summarized as follows:

- Configure Interface to Avaya Aura® Application Enablement Services
- Configure Avaya Endpoints for Third Party Call Control
- Configure Call Center Routing

### 5.1. Configure Interface to Avaya Aura® Application Enablement Services

The following sections illustrate the steps required to create a link between Communication Manager and Application Enablement Services.

#### 5.1.1. Verify System Features

Use the **display system-parameters customer-options** command to verify that Communication Manager has permissions for features illustrated in these Application Notes. On **Page 4**, ensure that **Answer Supervision by Call Classifier** is set to **y** and that **Computer Telephony Adjunct Links** is set to **y** as shown below.

display system-parameters customer-options		Page	4 of 12
OPTIONAL FEATURES			
Abbreviated Dialing Enhanced List? y	Audible Message Waiting? y		
Access Security Gateway (ASG)? y	Authorization Codes? y		
Analog Trunk Incoming Call ID? y	CAS Branch? n		
A/D Grp/Sys List Dialing Start at 01? y	CAS Main? n		
<b>Answer Supervision by Call Classifier? y</b>	Change COR by FAC? n		
ARS? y	<b>Computer Telephony Adjunct Links? y</b>		
ARS/AAR Partitioning? y	Cvg Of Calls Redirected Off-net? y		
ARS/AAR Dialing without FAC? y	DCS (Basic)? y		
ASAI Link Core Capabilities? y	DCS Call Coverage? y		
ASAI Link Plus Capabilities? y	DCS with Rerouting? y		
Async. Transfer Mode (ATM) PNC? n	Digital Loss Plan Modification? y		
Async. Transfer Mode (ATM) Trunking? n	DS1 MSP? y		
ATM WAN Spare Processor? n	DS1 Echo Cancellation? y		
ATMS? y			
Attendant Vectoring? y			
(NOTE: You must logoff & login to effect the permission changes.)			

### 5.1.2. Configure CTI Link for DMCC Service

Add a CTI link using the **add cti-link n** command, where n is the n is the cti-link number as shown in the example below this is **1**. 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: 1990		
Type: ADJ-IP		
Name: aes81xvmpg		COR: 1

## 5.2. Configure Avaya Endpoints for Third Party Call Control

Avaya H.323, Digital and SIP endpoints need to be configured correctly to allow third party call control. The H.323 and Digital endpoints can be configured directly on Communication Manager, where the SIP endpoints must be configured using System Manager.

### 5.2.1. Configure Avaya H.323 Endpoints

Each Avaya H.323 endpoint or station that needs to be monitored and used for 3rd party call control will need to have “IP Softphone” set to “Y”. To make changes to a H.323 station, from Communication Manager type **change station x**, where x is the extension number of the station to be changed. Ensure that **IP Softphone** is set to **y**, as shown below.

change station 1001		Page 1 of 5
STATION		
Extension: 1001	Lock Messages? n	BCC: 0
Type: 9608	Security Code: *	TN: 1
Port: S000040	Coverage Path 1:	COR: 1
Name: J179 H323	Coverage Path 2:	COS: 1
Unicode Name? n	Hunt-to Station:	Tests? y
STATION OPTIONS		
Time of Day Lock Table:		
Loss Group: 19	Personalized Ringing Pattern: 1	
Speakerphone: 2-way	Message Lamp Ext: 1001	
Display Language: english	Mute Button Enabled? y	
Survivable GK Node Name:	Button Modules: 0	
Survivable COR: internal	Media Complex Ext:	
Survivable Trunk Dest? y	<b>IP SoftPhone? y</b>	
IP Video Softphone? n		
Short/Prefixed Registration Allowed: default		
Customizable Labels? y		



## 5.2.2. Configure Avaya SIP Endpoints

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

Recommended access to System Manager is via FQDN.  
[Go to central login for Single Sign-On](#)

If IP address access is your only option, then note that authentication will fail in the following cases:

- First time login with "admin" account
- Expired/Reset passwords

Use the "Change Password" hyperlink on this page to change the password manually, and then login.

Also note that single sign-on between servers in the same security domain is not supported when accessing via IP address.

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

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

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

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

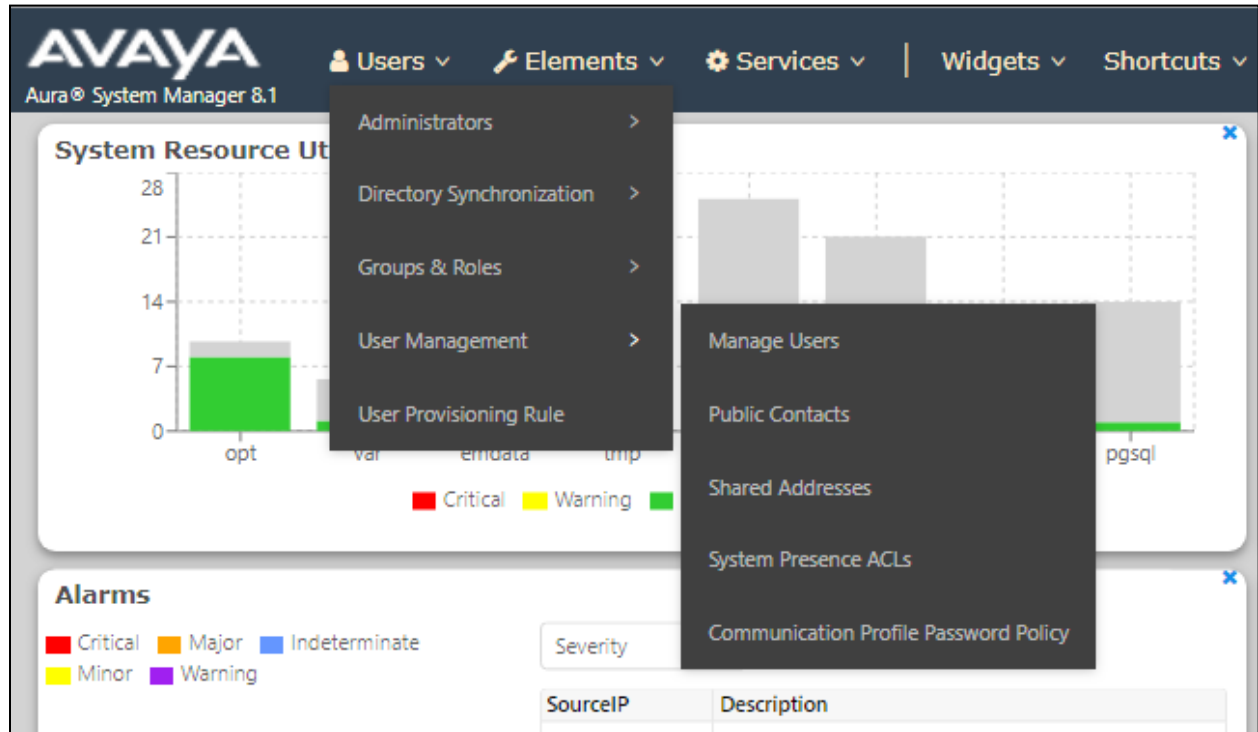
User ID:

Password:

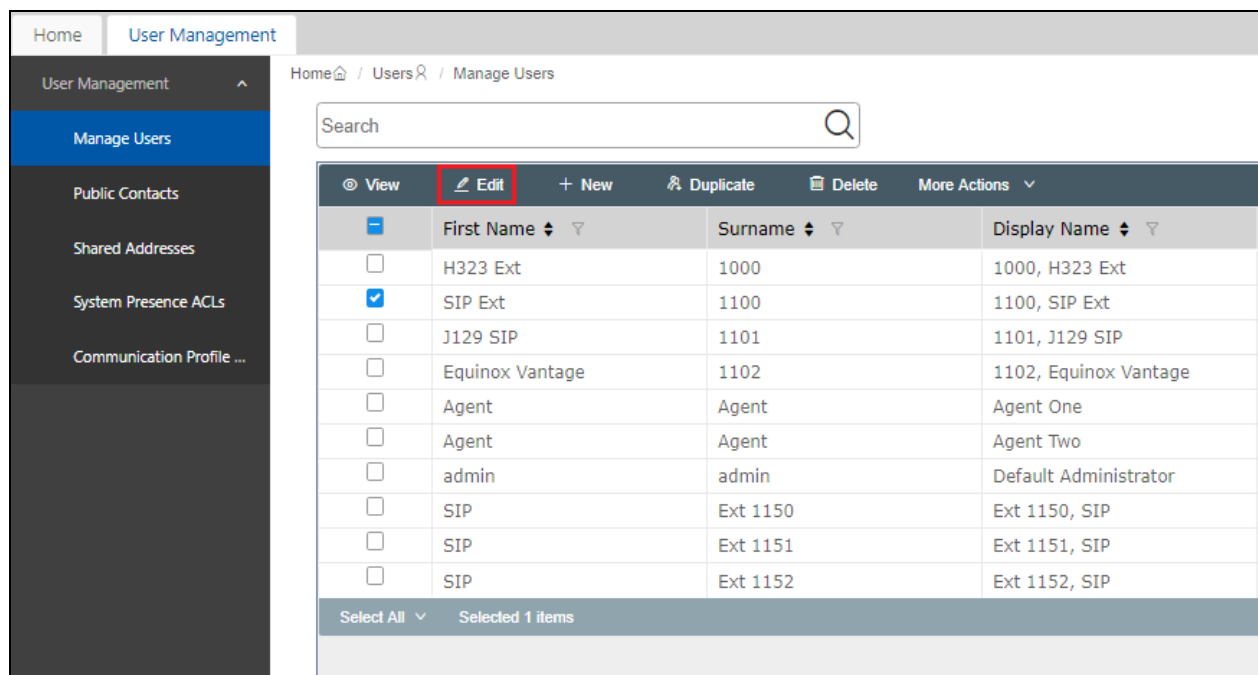
[Change Password](#)

**Supported Browsers:** Internet Explorer 11.x or Firefox 65.0, 66.0 and 67.0.

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



Click on **Manage 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.

**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

\* Class Of Service (COS) : 1

\* Emergency Location Ext : 1100

\* Message Lamp Ext. : 1100

\* Tenant Number : 1

\* SIP Trunk : aar

Type of 3PCC Enabled : **Avaya**

Coverage Path 1

Coverage Path 2

Localized Display Name : 1100, SIP Ext

Lock Message : ☐

Enable Reachability for Station Domain Control : system

Multibyte Language : Not Applicable

SIP URI

**Primary Session Manager**

IPv4 : 10.10.40.32 | IPv6 :

**Secondary Session Manager**

Under the **Feature Options** tab, ensure that **IP Softphone** is ticked, as 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)																
<b>Active Station Ringing</b> single ▼ <b>MWI Served User Type</b> sip-adjunct ▼ <b>Per Station CPN - Send Calling Number</b> None ▼ <b>IP Phone Group ID</b> <input type="text"/> <b>Remote Soft Phone Emergency Calls</b> as-on-local ▼ <b>LWC Reception</b> spe ▼ <b>AUDIX Name</b> None ▼ <b>Short/Prefixed Registration Allowed</b> default ▼ <b>Voice Mail Number</b> 6111 <b>Bridging Tone for This Extension</b> no ▼	<b>Auto Answer</b> none ▼ <b>Coverage After Forwarding</b> ▼ <b>Display Language</b> english ▼ <b>Hunt-to Station</b> <input type="text"/> <b>Loss Group</b> 19 <b>Survivable COR</b> internal ▼ <b>Time of Day Lock Table</b> None ▼ <b>Music Source</b> <input type="text"/>																	
<b>Features</b> <table border="0"> <tr> <td><input type="checkbox"/> Always Use</td> <td><input type="checkbox"/> Idle Appearance Preference</td> </tr> <tr> <td><input type="checkbox"/> IP Audio Hairpinning</td> <td><input checked="" type="checkbox"/> IP SoftPhone</td> </tr> <tr> <td><input checked="" type="checkbox"/> Bridged Call Alerting</td> <td><input checked="" type="checkbox"/> LWC Activation</td> </tr> <tr> <td><input type="checkbox"/> Bridged Idle Line Preference</td> <td><input type="checkbox"/> CDR Privacy</td> </tr> <tr> <td><input checked="" type="checkbox"/> Coverage Message Retrieval</td> <td><input checked="" type="checkbox"/> Precedence Call Waiting</td> </tr> <tr> <td><input type="checkbox"/> Data Restriction</td> <td><input checked="" type="checkbox"/> Direct IP-IP Audio Connections</td> </tr> <tr> <td><input checked="" type="checkbox"/> Survivable Trunk Dest</td> <td><input type="checkbox"/> H.320 Conversion</td> </tr> </table>					<input type="checkbox"/> Always Use	<input type="checkbox"/> Idle Appearance Preference	<input type="checkbox"/> IP Audio Hairpinning	<input checked="" type="checkbox"/> IP SoftPhone	<input checked="" type="checkbox"/> Bridged Call Alerting	<input checked="" type="checkbox"/> LWC Activation	<input type="checkbox"/> Bridged Idle Line Preference	<input type="checkbox"/> CDR Privacy	<input checked="" type="checkbox"/> Coverage Message Retrieval	<input checked="" type="checkbox"/> Precedence Call Waiting	<input type="checkbox"/> Data Restriction	<input checked="" type="checkbox"/> Direct IP-IP Audio Connections	<input checked="" type="checkbox"/> Survivable Trunk Dest	<input type="checkbox"/> H.320 Conversion
<input type="checkbox"/> Always Use	<input type="checkbox"/> Idle Appearance Preference																	
<input type="checkbox"/> IP Audio Hairpinning	<input checked="" type="checkbox"/> IP SoftPhone																	
<input checked="" type="checkbox"/> Bridged Call Alerting	<input checked="" type="checkbox"/> LWC Activation																	
<input type="checkbox"/> Bridged Idle Line Preference	<input type="checkbox"/> CDR Privacy																	
<input checked="" type="checkbox"/> Coverage Message Retrieval	<input checked="" type="checkbox"/> Precedence Call Waiting																	
<input type="checkbox"/> Data Restriction	<input checked="" type="checkbox"/> Direct IP-IP Audio Connections																	
<input checked="" type="checkbox"/> Survivable Trunk Dest	<input type="checkbox"/> H.320 Conversion																	

Click on **Commit** once this is done to save the changes.

User Profile | Edit | 1100@devconnect.local

Commit & Continue

Commit

Cancel

Identity	Communication Profile	Membership	Contacts
<b>Communication Profile Password</b> PROFILE SET : Primary ▼ Communication Address PROFILES Session Manager Profile <input checked="" type="checkbox"/> Avaya Breeze® Profile <input type="checkbox"/> CM Endpoint Profile <input checked="" type="checkbox"/>	<b>* System :</b> cm\$1xvmpg ▼ <b>* Profile Type :</b> Endpoint ▼ <b>* Extension :</b> 1100 <b>* Set Type :</b> 9641SIPCC <b>Port :</b> S000002 <b>Preferred Handle :</b> Select ▼ <b>Sip Trunk :</b> aar <b>Enhanced Callr-Info Display for 1-line phones :</b> <input type="checkbox"/> <b>Override Endpoint Name and Localized Name :</b> <input checked="" type="checkbox"/> <b>Use Existing Endpoints :</b> <input type="checkbox"/> <b>Template :</b> Start typing... <b>Security Code :</b> Enter Security Code <b>Voice Mail Number :</b> 6666 <b>Calculate Route Pattern :</b> <input type="checkbox"/> <b>SIP URI :</b> Select ▼ <b>Delete on Unassign from User or on Delete User :</b> <input checked="" type="checkbox"/> <b>Allow H.323 and SIP Endpoint Dual Registration :</b> <input type="checkbox"/>		

## 5.3. Configure Call Center Routing

The following was set to allow inbound ACD calls to the agents logged into the CAD CTI agent desktop.

- Configure Hunt Group
- Configure Vector
- Configure Vector Directory Number (VDN)
- Configure Agents
- Configure Adjunct Routing for CAD CTI

### 5.3.1. Configure Hunt Group

Enter the command **add hunt-group x** where **x** is an appropriate hunt group number and configure as follows:

- **Group Number** – this is the skill number when configuring the agent and vector.
- **Group Name** – enter an appropriate name.
- **Group Extension** – enter an extension appropriate to the dialplan.
- **Group Type** – set to **ucd-mia**.
- **ACD?** – set to **y**.
- **Queue?** – set to **y**.
- **Vector?** – set to **y**.

<b>add hunt-group 90</b>		Page 1 of 4
HUNT GROUP		
Group Number: 90	ACD? y	
Group Name: Sales	Queue? y	
Group Extension: 1800	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 **Skill** to **y**.

add hunt-group 90		Page 2 of 4
HUNT GROUP		
Skill? y	Expected Call Handling Time (sec): 180	
AAS? n	Service Level Target (% in sec): 80 in 20	
Measured: none		
Supervisor Extension:		
Controlling Adjunct: none		
VuStats Objective:		
Multiple Call Handling: none		
Timed ACW Interval (sec):	After Xfer or Held Call Drops? n	

### 5.3.2. Configure Vector

Enter the command **change vector x** where **x** is the required vector number. Configure as shown below so that calls **queue-to skill 1st**. Skill 1st the hunt group configured in the VDN in **Section 5.3.3**.

change vector 1		Page 1 of 6
CALL VECTOR		
Number: 1	Name: Basic Routing	
Multimedia? n	Attendant Vectoring? n	Meet-me Conf? n Lock? n
Basic? y	EAS? y G3V4 Enhanced? y	ANI/II-Digits? y ASAI Routing? y
Prompting? y	LAI? y G3V4 Adv Route? y	CINFO? y BSR? y Holidays? y
Variables? y	3.0 Enhanced? y	
01 wait-time	2 secs hearing ringback	
02 <b>queue-to</b>	<b>skill 1st</b> pri m	
03 wait-time	100 secs hearing music	
04 goto step	3 if unconditionally	
05 stop		
06		
07		
08		
09		

### 5.3.3. Configure Vector Directory Number (VDN)

Enter the command **add vdn x** where **x** is the required VDN number appropriate to the dialplan. Configure the VDN to send calls to the vector configured in the previous section as follows:

- **Extension** – note the VDN extension number which will be used to place calls to the Skill vector and on to the Skill.
- **Name** – enter an appropriate name.
- **Destination** – enter the **Vector Number** configured in the previous section.
- **1<sup>st</sup> Skill** – enter the hunt group created in **Section 5.3.1**

<b>add vdn 1900</b>	Page 1 of 3
VECTOR DIRECTORY NUMBER	
<b>Extension: 1900</b>	Unicode Name? n
<b>Name*: Sales</b>	
<b>Destination: Vector Number</b>	<b>1</b>
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*:	
	<b>1st Skill*: 90</b>
	2nd Skill*:
	3rd Skill*:
SIP URI:	
* Follows VDN Override Rules	

### 5.3.4. Configure Agents

Agents must be configured with the appropriate Skill Number. Enter the command **add agent-loginID x** where **x** is an agent extension number appropriate to the dialplan and configure as follows:

- **Login ID** – take a note of the configured **Login ID**.
- **Name** – enter an identifying name.
- **Password** – enter a suitable password of the agent.

<b>add agent-loginID 5001</b>		Page 1 of 2
AGENT LOGINID		
<b>Login ID: 5001</b>		Unicode Name? n AAS? n
<b>Name: Agent One</b>		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		
<b>Password:1234</b>		
Password (enter again):1234		
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**, enter the hunt group number configured in **Section 5.3.1** in the **SN** (Skill Number) column and enter an appropriate **SL** (skill level).

<b>add agent-loginID 5001</b>		<b>Page 2 of 2</b>
AGENT LOGINID		
Direct Agent Skill: 90		Service Objective? n
Call Handling Preference: skill-level		Local Call Preference? n
<b>SN</b>	<b>RL</b>	<b>SL</b>
1: 90	1	16:
2:		17:
3:		18:
4:		19:
5:		20:
6:		
7:		
8:		



### 5.3.5. Configure Adjunct Routing for CAD CTI

The following setup is specific to this solution to allow CAD CTI to correctly and successfully places calls on hold and to use transfer and conference successfully. The VDN is used to direct the call to the CAD CTI application using Adjunct Routing. VDN **4001** was added specifically for agent 5001 and this was used to call on Vector **51**.

**Note:** Similar VDN's and Vectors were used for all other agents.

add vdn <b>4001</b>	Page 1 of 3
VECTOR DIRECTORY NUMBER	
Extension: <b>4001</b>	Unicode Name? n
Name*: Personal Code <b>5001</b>	
Destination: Vector Number <b>51</b>	
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*:	
2nd Skill*:	
3rd Skill*:	
SIP URI:	
* Follows VDN Override Rules	

**Vector 51** is used to route the call to CAD CTI using Adjunct Routing. The command **adjunct routing link 1** will use the CTI link created in **Section 5.1.2** to route the call to the CAD CTI. Once the call is routed the user hears whatever announcement is set before the call can be sent on to a backup skill should this be required.

change <b>vector 51</b>	Page 1 of 6
CALL VECTOR	
Number: 51	Name: Personal Code 5001
Multimedia? n	Attendant Vectoring? n
Basic? y	Meet-me Conf? n
EAS? y	Lock? n
G3V4 Enhanced? y	ANI/II-Digits? y
ASAI Routing? y	CINFO? y
Prompting? y	BSR? y
Holidays? y	Variables? y
3.0 Enhanced? y	
01 adjunct	routing link 1
02 wait-time	50 secs hearing 1844 then continue
03 queue-to	skill 90 pri m
04 wait-time	15 secs hearing 1843 then silence
05 stop	
06	
07	

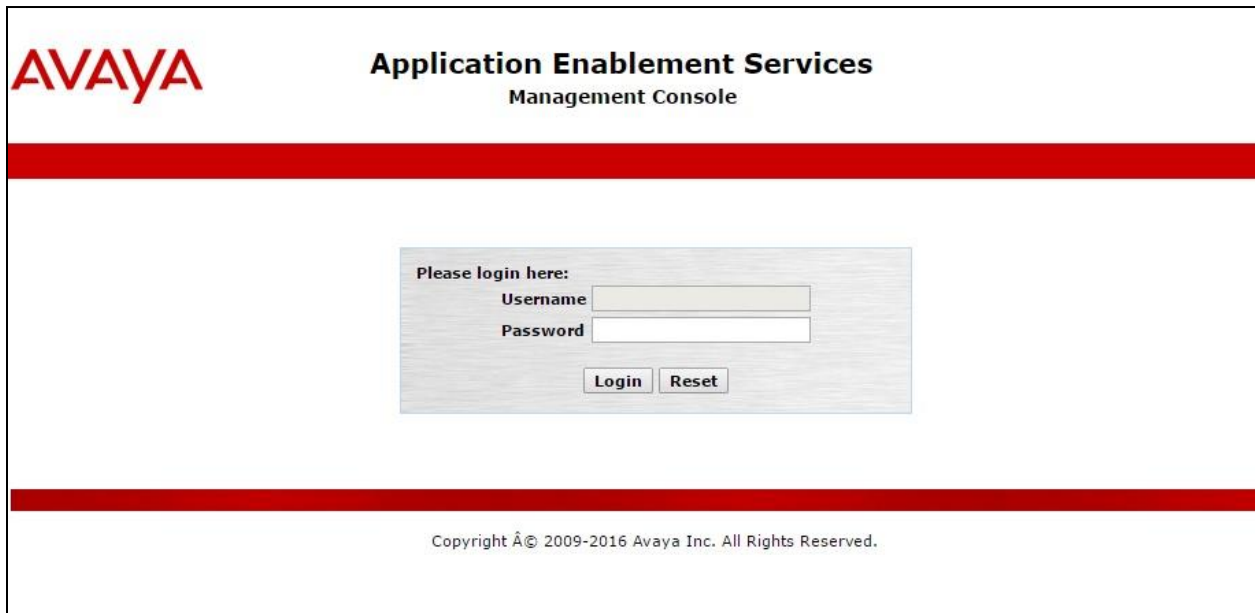
## 6. Configure Avaya Aura® Application Enablement Services

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

- Verify Licensing
- Administer TSAPI link
- Enable DMCC Ports
- Create CTI User
- Associate Devices with CTI User

### 6.1. Verify Licensing

To access the Application Enablement Services Management Console, enter **https://<ip-addr>** as the URL in an Internet browser, where <ip-addr> is the IP address of the Application Enablement Services. At the login screen displayed, log in with the appropriate credentials and then select the **Login** button.



The screenshot shows the login interface for the Avaya Application Enablement Services Management Console. At the top left is the Avaya logo. To its right, the text "Application Enablement Services" is displayed in a large, bold font, with "Management Console" in a smaller font below it. A thick red horizontal bar spans the width of the page. In the center, there is a light gray rectangular box containing the login form. The form includes the text "Please login here:" followed by "Username" and "Password" labels, each next to a text input field. Below these fields are two buttons: "Login" and "Reset". Another thick red horizontal bar is located below the login box. At the bottom of the page, centered, is the copyright notice: "Copyright © 2009-2016 Avaya Inc. All Rights Reserved."

The Application Enablement Services Management Console appears displaying the **Welcome to OAM** screen (not shown). Select **AE Services** and verify that the TSAPI Service is licensed by ensuring that **TSAPI Service** is in the list of **Services** and that the **License Mode** is showing **NORMAL MODE**. If not, contact an Avaya support representative to acquire the proper license.

The screenshot shows the 'AE Services' management console. On the left is a navigation menu with options like CVLAN, DLG, DMCC, SMS, TSAPI, TWS, Communication Manager Interface, High Availability, Licensing, Maintenance, Networking, Security, Status, User Management, Utilities, and Help. The main area displays a table of services with columns for Service, Status, State, License Mode, and Cause\*.

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

Below the table, there is a note: 'For status on actual services, please use [Status and Control](#)'. Another note says: '\* -- For more detail, please mouse over the Cause, you'll see the tooltip, or go to help page.' At the bottom, 'License Information' states: 'You are licensed to run Application Enablement (CTI) release 8.x'.

The TSAPI and DMCC licenses are user licenses issues by the Web License Manager to which the Application Enablement Services server is pointed to. The following screen shows the available licenses for both DMCC and TSAPI users.

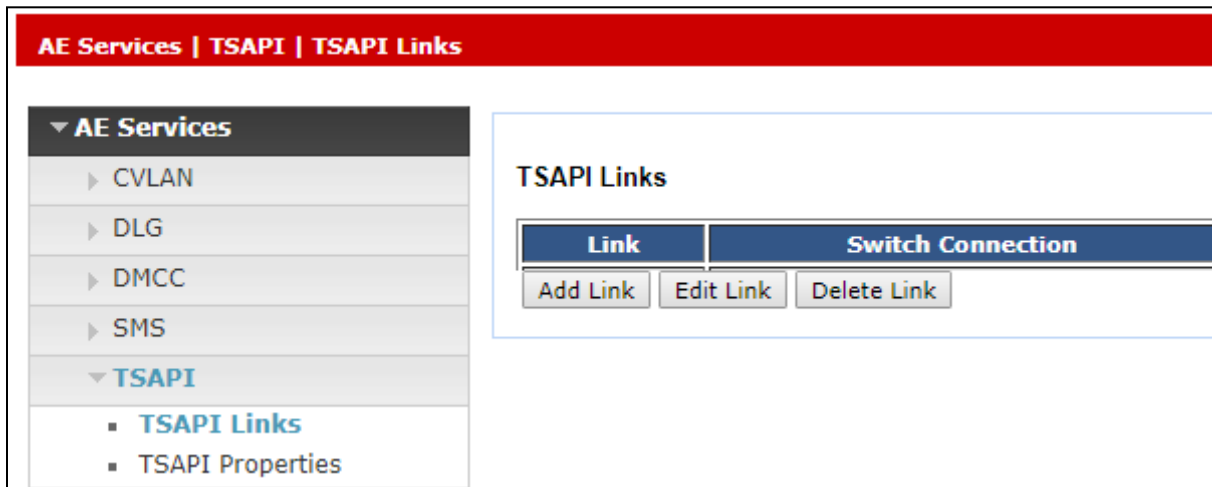
The screenshot shows the 'Application\_Enablement' section of the Web License Manager. It lists various license features with columns for Feature (License Keyword), Expiration date, and Licensed capacity. Two features are highlighted with red boxes: 'Device Media and Call Control' and 'TSAPI Simultaneous Users'.

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

At the bottom right, there is a section for 'SmallServerTypes' and 'MediumServerTypes' with various hardware configurations listed.

## 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.



On the **Add TSAPI Links** screen (or the **Edit TSAPI Links** screen to edit a previously configured TSAPI Link as shown below), enter the following values:

- **Link:** Use the drop-down list to select an unused link number.
- **Switch Connection:** Choose the appropriate switch connection **cm81xvmpg**, which has already been configured from the drop-down list.
- **Switch CTI Link Number:** Corresponding CTI link number configured in **Section 5.1.2** which is **1**.
- **ASAI Link Version:** This should be set to the highest version available.
- **Security:** This should be set to **Both** allowing both secure and nonsecure connections.

Once completed, select **Apply Changes**.


**Note:** The **Switch Connection** name **cm81xvmpg** will be used during the configuration of the CAD CTI server, this name should be noted here and given to the Beta 80 engineers.

The screenshot shows the 'Edit TSAPI Links' configuration form. It contains the following fields and values:

Field	Value
Link	1
Switch Connection	cm81xvmpg
Switch CTI Link Number	1
ASAI Link Version	11
Security	Both

At the bottom of the form are three buttons: 'Apply Changes', 'Cancel Changes', and 'Advanced Settings'.


Another screen appears for confirmation of the changes made. 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.**

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

TSAPI Links				
Link	Switch Connection	Switch CTI Link #	ASAI Link Version	Security
<input checked="" type="radio"/> 1	cm81xvmpg	1	11	Both
<input type="button" value="Add Link"/> <input type="button" value="Edit Link"/> <input type="button" value="Delete Link"/>				

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



**Application Enablement Services**  
Management Console

Maintenance | Service Controller

▶ AE Services

▶ Communication Manager Interface

High Availability

▶ Licensing

▼ Maintenance

Date Time/NTP Server

▶ Security Database

**Service Controller**

▶ Server Data

▶ Networking

▶ Security

▶ Status

▶ User Management

▶ Utilities

▶ Help

Service Controller

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

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

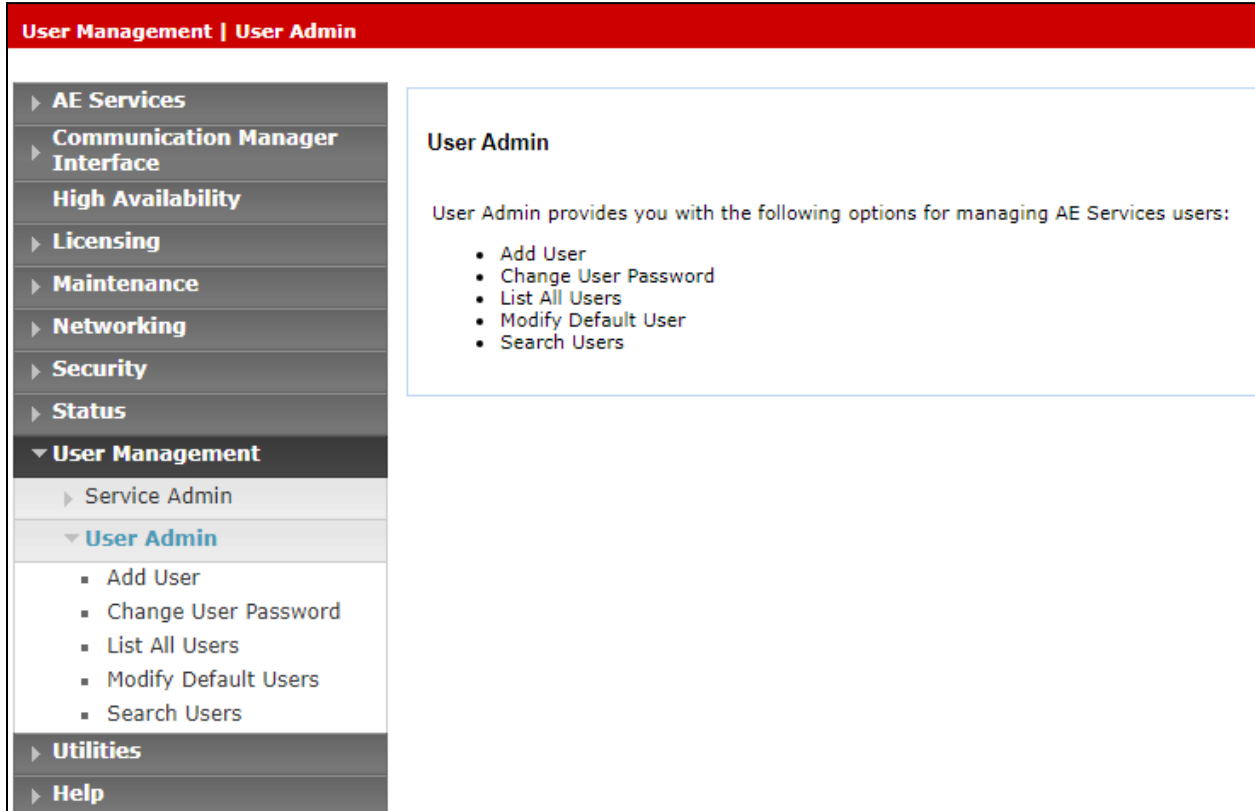
### 6.3. Enable DMCC Ports

To ensure that TSAPI and DMCC ports are enabled, navigate to **Networking** → **Ports**. Ensure that the DMCC ports are set to **Enabled** as shown below. Note that port **4721** was used for compliance testing.

Networking   Ports				
<ul style="list-style-type: none"> <li>AE Services</li> <li>Communication Manager Interface</li> <li>High Availability</li> <li>Licensing</li> <li>Maintenance</li> <li><b>Networking</b></li> <li>AE Service IP (Local IP)</li> <li>Network Configure</li> <li><b>Ports</b></li> <li>TCP/TLS Settings</li> <li>Security</li> <li>Status</li> <li>User Management</li> <li>Utilities</li> <li>Help</li> </ul>	<b>Ports</b>			
	CVLAN Ports			Enabled Disabled
	Unencrypted TCP Port	9999	<input checked="" type="radio"/>	<input type="radio"/>
	Encrypted TCP Port	<input type="text" value="9998"/>	<input checked="" type="radio"/>	<input type="radio"/>
	DLG Port	TCP Port	5678	
	TSAPI Ports			Enabled Disabled
	TSAPI Service Port	450	<input checked="" type="radio"/>	<input type="radio"/>
	Local TLINK Ports			
	TCP Port Min	1024		
TCP Port Max	1039			
Unencrypted TLINK Ports				
TCP Port Min	<input type="text" value="1050"/>			
TCP Port Max	<input type="text" value="1065"/>			
Encrypted TLINK Ports				
TCP Port Min	<input type="text" value="1066"/>			
TCP Port Max	<input type="text" value="1081"/>			
DMCC Server Ports			Enabled Disabled	
Unencrypted Port	<input type="text" value="4721"/>	<input checked="" type="radio"/>	<input type="radio"/>	
Encrypted Port	<input type="text" value="4722"/>	<input checked="" type="radio"/>	<input type="radio"/>	
TR/87 Port	<input type="text" value="4723"/>	<input checked="" type="radio"/>	<input type="radio"/>	
H.323 Ports				
TCP Port Min	<input type="text" value="20000"/>			
TCP Port Max	<input type="text" value="29999"/>			
Local UDP Port Min	<input type="text" value="20000"/>			
Local UDP Port Max	<input type="text" value="29999"/>			
Server Media			Enabled Disabled	
		<input checked="" type="radio"/>	<input type="radio"/>	

## 6.4. Create CTI User

A user ID and password needs to be configured for the Beta 80 to communicate with the Application Enablement Services server. Navigate to the **User Management** → **User Admin** screen then choose the **Add User** option.



**User Management | User Admin**

**User Admin**

User Admin provides you with the following options for managing AE Services users:

- Add User
- Change User Password
- List All Users
- Modify Default User
- Search Users

In the **Add User** screen shown below, enter the following values:

- **User Id** - This will be used by the CAD CTI setup in **Section 7.1**.
- **Common Name** and **Surname** - Descriptive names need to be entered.
- **User Password** and **Confirm Password** - This will be used with CAD CTI setup in **Section 7.1**.
- **CT User** - Select **Yes** from the drop-down menu.

Click on **Apply Changes** at the bottom of the screen (not shown).

<ul style="list-style-type: none"><li>▶ <b>AE Services</b></li><li>▶ <b>Communication Manager Interface</b></li><li>▶ <b>High Availability</b></li><li>▶ <b>Licensing</b></li><li>▶ <b>Maintenance</b></li><li>▶ <b>Networking</b></li><li>▶ <b>Security</b></li><li>▶ <b>Status</b></li><li>▼ <b>User Management</b><ul style="list-style-type: none"><li>▶ Service Admin</li><li>▼ <b>User Admin</b><ul style="list-style-type: none"><li>■ <b>Add User</b></li><li>■ Change User Password</li><li>■ List All Users</li><li>■ Modify Default Users</li><li>■ Search Users</li></ul></li></ul></li><li>▶ <b>Utilities</b></li><li>▶ <b>Help</b></li></ul>	<h3>Add User</h3> <p>Fields marked with * can not be empty.</p> <table><tr><td>* User Id</td><td><input type="text" value="beta80"/></td></tr><tr><td>* Common Name</td><td><input type="text" value="beta80"/></td></tr><tr><td>* Surname</td><td><input type="text" value="beta80"/></td></tr><tr><td>* User Password</td><td><input type="password" value="....."/></td></tr><tr><td>* Confirm Password</td><td><input type="password" value="....."/></td></tr><tr><td>Admin Note</td><td><input type="text"/></td></tr><tr><td>Avaya Role</td><td><input type="text" value="None"/></td></tr><tr><td>Business Category</td><td><input type="text"/></td></tr><tr><td>Car License</td><td><input type="text"/></td></tr><tr><td>CM Home</td><td><input type="text"/></td></tr><tr><td>Css Home</td><td><input type="text"/></td></tr><tr><td>CT User</td><td><input type="text" value="Yes"/></td></tr><tr><td>Department Number</td><td><input type="text"/></td></tr><tr><td>Display Name</td><td><input type="text"/></td></tr><tr><td>Employee Number</td><td><input type="text"/></td></tr><tr><td>Employee Type</td><td><input type="text"/></td></tr></table>	* User Id	<input type="text" value="beta80"/>	* Common Name	<input type="text" value="beta80"/>	* Surname	<input type="text" value="beta80"/>	* User Password	<input type="password" value="....."/>	* Confirm Password	<input type="password" value="....."/>	Admin Note	<input type="text"/>	Avaya Role	<input type="text" value="None"/>	Business Category	<input type="text"/>	Car License	<input type="text"/>	CM Home	<input type="text"/>	Css Home	<input type="text"/>	CT User	<input type="text" value="Yes"/>	Department Number	<input type="text"/>	Display Name	<input type="text"/>	Employee Number	<input type="text"/>	Employee Type	<input type="text"/>
* User Id	<input type="text" value="beta80"/>																																
* Common Name	<input type="text" value="beta80"/>																																
* Surname	<input type="text" value="beta80"/>																																
* User Password	<input type="password" value="....."/>																																
* Confirm Password	<input type="password" value="....."/>																																
Admin Note	<input type="text"/>																																
Avaya Role	<input type="text" value="None"/>																																
Business Category	<input type="text"/>																																
Car License	<input type="text"/>																																
CM Home	<input type="text"/>																																
Css Home	<input type="text"/>																																
CT User	<input type="text" value="Yes"/>																																
Department Number	<input type="text"/>																																
Display Name	<input type="text"/>																																
Employee Number	<input type="text"/>																																
Employee Type	<input type="text"/>																																



## 6.5. Associate Devices with CTI User

Navigate to **Security** → **Security Database** → **CTI Users** → **List All Users**. Select the CTI user added in **Section 6.4** and click on **Edit**.

Security   Security Database   CTI Users   List All Users				Home   Help   Logout
<ul style="list-style-type: none"><li>AE Services</li><li>Communication Manager Interface</li><li>High Availability</li><li>Licensing</li><li>Maintenance</li><li>Networking</li><li>Security<ul style="list-style-type: none"><li>Account Management</li><li>Audit</li><li>Certificate Management</li><li>Enterprise Directory</li><li>Host AA</li><li>PAM</li><li>Security Database<ul style="list-style-type: none"><li>Control</li><li>CTI Users<ul style="list-style-type: none"><li>List All Users</li><li>Search Users</li><li>Devices</li><li>Device Groups</li></ul></li></ul></li></ul></li></ul>	CTI Users			
	User ID	Common Name	Worktop Name	Device ID
	<input checked="" type="radio"/> beta80	beta80	NONE	NONE
	<input type="radio"/> capita	capita	NONE	NONE
	<input type="radio"/> Enghouse	Enghouse	NONE	NONE
	<input type="radio"/> inisoft	inisoft	NONE	NONE
	<input type="radio"/> mitel	mitel	NONE	NONE
	<input type="radio"/> nice	nice	NONE	NONE
	<input type="radio"/> Oceana	Oceana	NONE	NONE
	<input type="radio"/> opentextaes	opentextaes	NONE	NONE
	<input type="radio"/> paul	Paul	NONE	NONE
	<input type="radio"/> paul1	paul1	NONE	NONE
	<input type="radio"/> wspaces37	wspaces37	NONE	NONE
	<input type="button" value="Edit"/> <input type="button" value="List All"/>			

In the main window ensure that **Unrestricted Access** is ticked. Once this is done click on **Apply Changes**.

<b>Edit CTI User</b>		
User Profile:	User ID	beta80
	Common Name	beta80
	Worktop Name	NONE ▾
	Unrestricted Access	<input checked="" type="checkbox"/>
Call and Device Control:	Call Origination/Termination and Device Status	None ▾
Call and Device Monitoring:	Device Monitoring	None ▾
	Calls On A Device Monitoring	None ▾
	Call Monitoring	<input type="checkbox"/>
Routing Control:	Allow Routing on Listed Devices	None ▾
<input type="button" value="Apply Changes"/> <input type="button" value="Cancel Changes"/>		

Click on **Apply** when asked again to **Apply Changes** (not shown).

## 7. Configure Beta 80 Life 1st and emma CAD CTI

This section describes the steps required for Beta 80 CAD CTI to interoperate with Application Enablement Services in an ACD environment.

### 7.1. Add CTI link to Avaya Aura® Application Enablement Services

In order to correctly establish the CTI link between emma / Life 1st CAD and Application Enablement Services, “PABXConverter.exe.config” file has to be accessed and the following configuration steps have to be carried out.

- AES IP address and port configuration, as per **Section 6** (note the IP addresses of the AES and Communication Manager servers should be already known, however, these can be found using ifconfig command from each Linux server)
- DMCC login parameters configuration, as per **Section 6.4**
- CM IP address configuration, as per **Section 6.2**
- ACD agent’s login and status exchange from the CTI server and Application Enablement Services

```
<configuration>
  <appSettings>
    <add key="PBXIP" value="10.10.40.38"/>
    <add key="PBXPort" value="4721"/>

    <add key="PBXLoginName" value="beta80"/>
    <add key="PBXLoginPassword" value="Bet@1234"/>

    <add key="CMSwitchName" value="cm81xvmpg"/>
    <add key="CMSwitchAddressIp" value="10.10.40.37"/>

    <add key="LocalIP" value="192.168.15.18"/>
    <add key="LocalReceivePort" value="1041"/>

    <add key="AutoAgentLoginLogout" value="True"/>
    <add key="ACDModeEnabled" value="True"/>
```

The “PABXConverter.exe.config” file is normally stored in the “PABXConverter” folder. emma / Life 1st CTI client can be configured to work in either Auto Answer Mode or Manual Answer Mode or Mixed Mode. The third option represents the default setting and allows each agent to dynamically set their own answer mode into auto or manual.

The configuration string follows which allows the client-level answer mode configuration:

```
<add key="ACDMode_ACDEnabled" value="1"/>
<add key="ACDMode_AnswerMode" value="SetByOperator"/>
```

The “value” field can be filled as follows:

*SetByOperator*: (default) allows each agent to dynamically set his own answer mode

*AutoAnswerOnly*: Auto answer only

*ManualOnly*: Manual answer only

emma / Life 1st CTI administration interface gives the opportunity to define the whole set of elements which constitute the CTI environment from the agent point of view; these elements are:

- Icons
- Ringing tones
- Personal queues
- Positions
- Agents

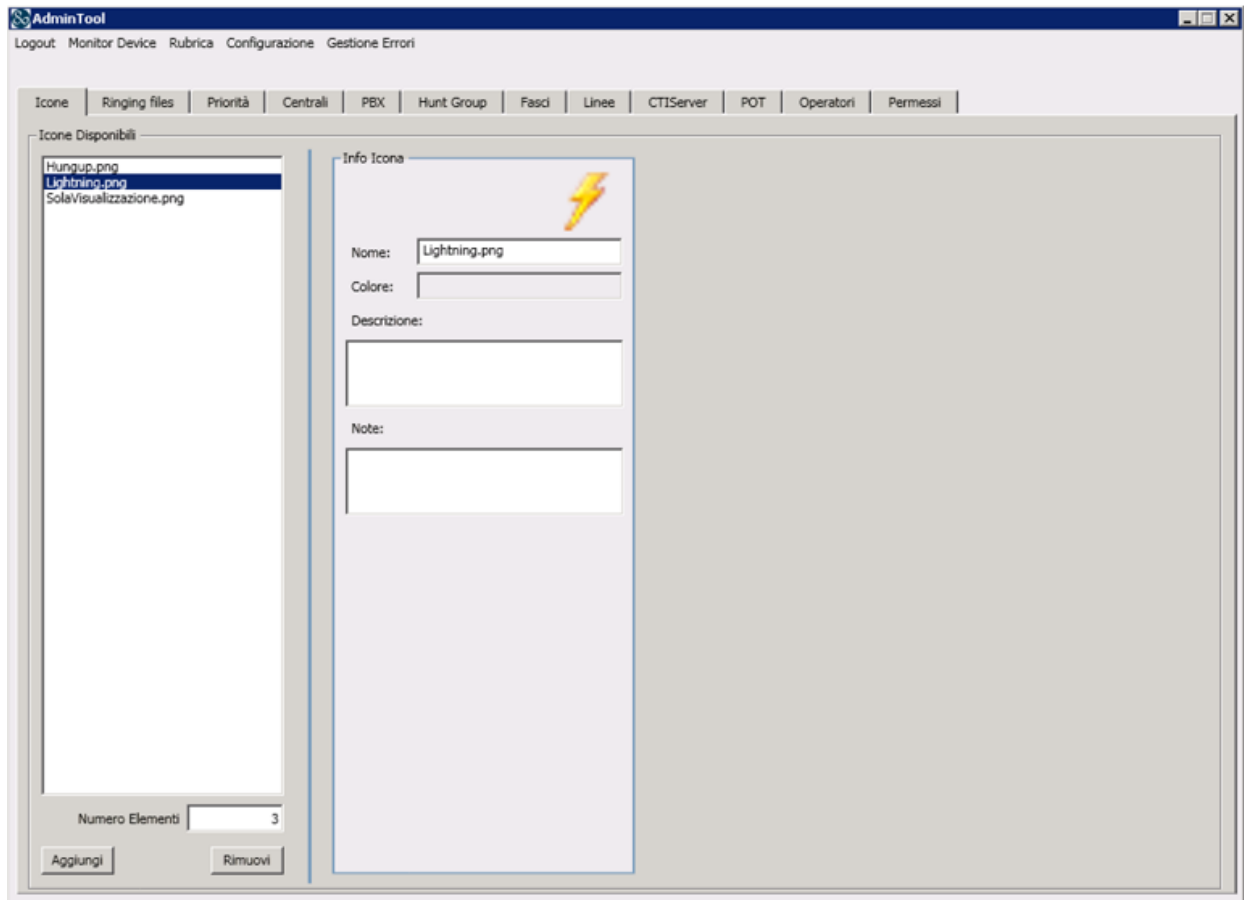
To access the CTI admin tool a valid user/password must be used; once logged in, the “Configuration” menu provides administrators with all relevant functionalities to complete the CTI setup.



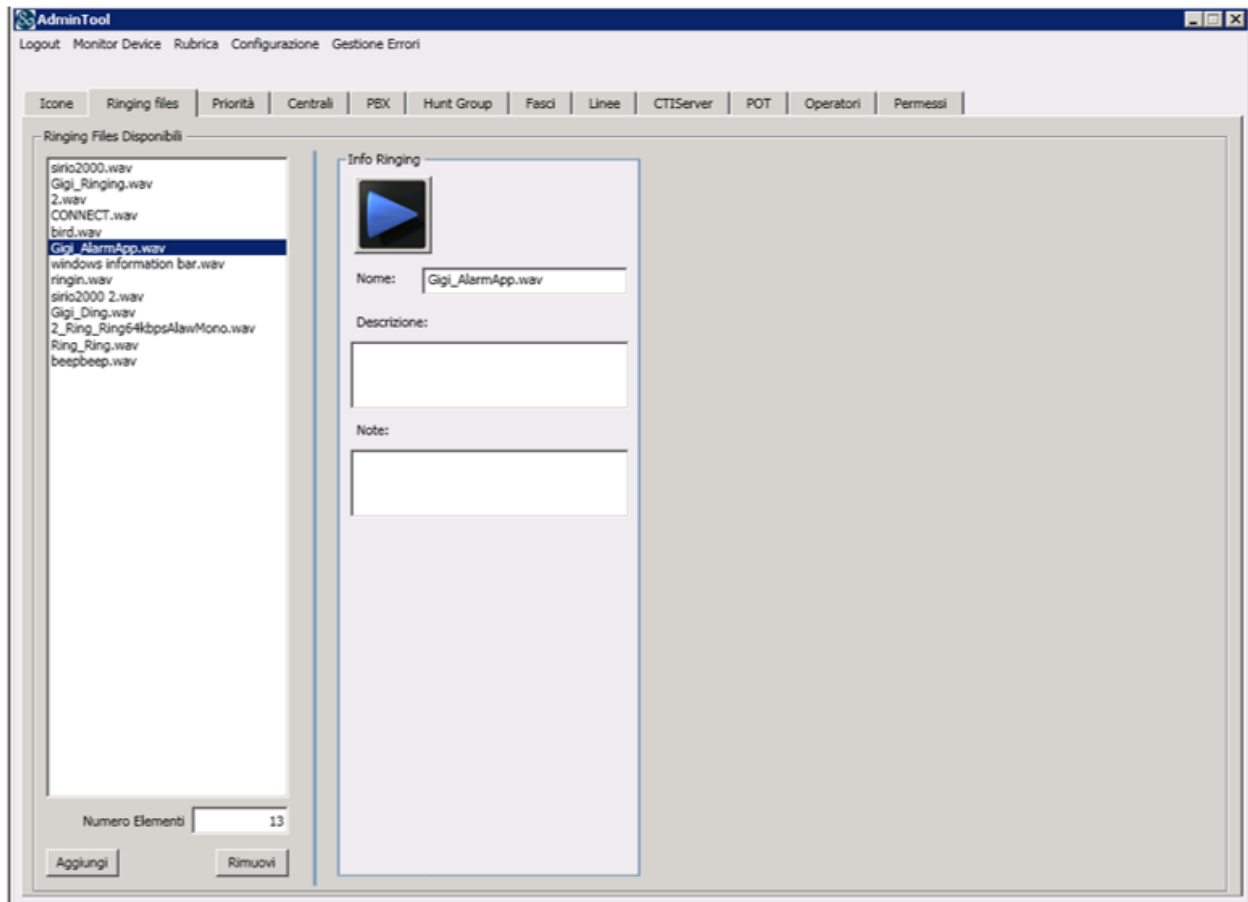
The screenshot shows a web browser window titled "AdminTool". The address bar displays the URL "http://192.168.1.100:8080/". The page features a navigation menu at the top with links: "Logout", "Monitor Device", "Rubrica", "Configurazione", and "Gestione Errori". In the center, there is a large logo for "BETA 80 GROUP" consisting of a blue circle with a white infinity symbol inside, and the text "BETA 80 GROUP" below it. Below the logo is a "Login" section with a white border. It contains two input fields: "Username:" and "Password:". The "Password:" field is masked with six dots. Below the input fields are two buttons: "Accedi" (Login) and "Annulla" (Cancel).

## 7.2. Configuration of Icons and Ringing Tones

PSAP admins can define incoming calls icons and ringing tones; the configuration is performed via the relevant tabs of emma / Life 1st CTI admin interface. The incoming call icon is defined in the **Icone** tab, as shown below, a **Lightning** icon was chosen.



The incoming call tone is defined in the **Ringing files** tab, where a suitable **.wav** file is chosen to represent the incoming call.



### 7.3. Personal Queues Configuration

Agents' personal queues are configured under the **Hunt Group** tab. Where a specific queue is assigned to the agent at hand. Each queue is associated with the monitored VDN configured on Communication Manager.

AdminTool

Logout Monitor Device Rubrica Configurazione Gestione Errori

Icone Ringing files Priorità Centrali PBX Hunt Group Fasci Linee CTIServer POT Operatori Permessi

Hunt Group Disponibili

- 113 attesa
- Ritorni
- CUG NUE
- 113
- 118 attesa
- Chiamate Urbane
- 115
- 112
- 115 attesa
- PSAP 2 NON Urgente
- 112 attesa
- PSAP 2 Urgente
- 118
- Coda Personale 02
- Coda personale 06
- Coda personale 07
- Coda Personale 01
- Coda Personale 03
- Coda personale 04
- Coda personale 09
- Coda personale 08
- Coda personale 10
- Coda personale 05
- Operatore 07
- Operatore 08
- Operatore 05
- Operatore 06
- Operatore 01
- Operatore 04
- Operatore 03
- Operatore 09
- Operatore 10
- Operatore 02

Numero Elementi 33

Aggiungi Modifica Rimuovi

Info Hunt Group

PBX: PBX Avaya Catania

Codice: 1112

Nome: 112

Tipo: HG

Priorità: Very High - Urgent

Centrale: NUE CT

Public Code: 1112

Codice HG Supplier: 1112

HG Prompt:

HG Prompt Timeout: sec.

Descrizione:

Coda di Centrale x 112

Note:

## 7.4. Positions Configuration

The **POT** tab is where to configure PSAP positions within the CTI admin tool; this configuration also includes the definition of the agent's personal queue.

The screenshot shows the AdminTool interface with the POT tab selected. The interface includes a menu bar at the top with options: Logout, Monitor Device, Rubrica, Configurazione, and Gestione Errori. Below the menu bar is a tabbed interface with tabs: Icone, Ringing files, Priorità, Centrali, PBX, Hunt Group, Fasci, Linee, CTIServer, POT, Operatori, and Permessi. The POT tab is active, displaying a list of available positions on the left and a configuration form on the right.

**POT Disponibili**

- Post. 01 - 192.168.15.51
- Post. 02 - 192.168.15.52
- Post. 03 - 192.168.15.53
- Post. 04 - 192.168.15.54

Numero Elementi: 4

**Info POT**

Centrale: NUE CT

Interno: Operatore 04

Coda Personale: Coda personale 04

IP: 192.168.15.54

MAC:

Nome Host: Post. 04

Note:

Buttons: Aggiungi, Modifica, Rimuovi



The screenshot shows the Modifica POT (Modify POT) configuration window. It contains two main sections: 'Info Interno Selezionato' and 'Info Coda Personale Selezionata'.

**Info Interno Selezionato**

PBX: PBX Avaya Catania

Centrale: NUE CT

Codice: 3004

Nome: Operatore 04

Tipo: HG OPERATOR

**Info Coda Personale Selezionata**

PBX: PBX Avaya Catania

Centrale: NUE CT

Codice: 4004

Nome: Coda personale 04

Tipo: HG PERSONAL

Buttons: Modifica, Annulla

## 7.5. Phone Bar Users Definition

Each agent is registered in the system as a named user, this is done in the **Operators** tab as shown below.

The screenshot shows the 'AdminTool' interface with the 'Operatori' tab selected. On the left, a list titled 'Operatori Disponibili' contains names like NOTAR, beta80, OperMI2, etc. Below the list is a 'Numero Elementi' field showing 14 and buttons for 'Aggiungi', 'Modifica', and 'Rimuovi'. On the right, the 'Info Operatore' form is displayed with the following fields: Centrale (NUE CT), Context (2), Gruppo (1025), User (2057), Username (OperMI4), Nome (NomeOpMI4), Cognome (CognomeOpMI4), Interno (empty), Coda Personale (empty), and a Note text area.



The 'Modifica Operatore' dialog box shows the same fields as the 'Info Operatore' form, but with additional options. The 'Interno' and 'Coda Personale' fields now have dropdown arrows and red 'X' icons. To the right, there are two sections: 'Info Interno Selezionato' and 'Info Coda Personale Selezionata', each containing fields for PBX, Centrale, Codice, Nome, and Tipo. At the bottom are 'Modifica' and 'Annulla' buttons.



## 7.6. Agents Profiling

Each agent or position is assigned a personal queue, a ringing tone and an incoming call icon. This is done in the **Permessi** tab, as shown below.

The screenshot shows the 'AdminTool' application window with the 'Permessi' tab selected. The interface is divided into several sections:

- Genera Nuovi Permessi:** This section contains dropdown menus for 'Centrale' (set to 'NUE CT'), 'Operatore' (set to 'IVAN'), 'Interno' (set to 'Coda Personale 01'), and 'Postazione' (set to 'Tutti'). There are also buttons for 'Rimuovi', 'Audio' (with a play icon), 'Pulisci', and 'Genera Permessi'.
- Info Interno Selezionato:** This section displays details for the selected internal extension, including 'PBX' (PBX Avaya Catania), 'Centrale' (NUE CT), 'Codice' (4001), 'Nome' (Coda Personale 01), and 'Tipo' (HG PERSONAL).
- Permessi Disponibili:** This section contains a table with the following columns: Operatore, POT, Hunt Group, Permessi, Priorità, Icona, and Audio. The table lists the permissions for the selected agent 'IVAN'.

Operatore	POT	Hunt Group	Permessi	Priorità	Icona	Audio
IVAN	192.168.15.51	Coda Personale 01	Completa gestione	High	Hungup.png	Ring_Ring.wav

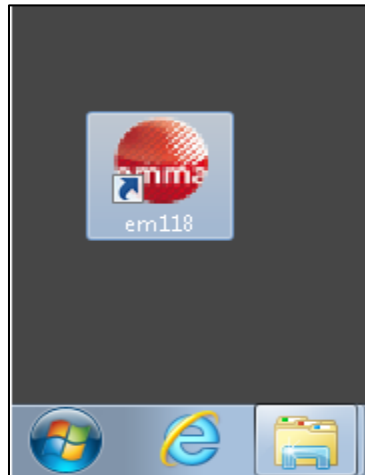
At the bottom of the window, there are buttons for 'Salva Permessi' and 'Rimuovi Selezionati', and a 'Numero Elementi' field showing '1'.

## 8. Verification Steps

The correct configuration of the solution can be verified as follows.

### 8.1. Verify Beta 80 Life 1st and emma CAD CTI

Open the agent desktop as shown below, by clicking on the desktop shortcut.



Enter the appropriate credentials for the agent (not shown) and the following screen will be displayed showing the agent **Available** to take calls.

Hr.	Inc.	Address	Operator	Hr. Disp.	Ope
17:43	000038	MILANO	NOTAR		
17:38	000036	MILANO	ANDREA		
16:42	000013	MILANO	NOTAR		
16:35	000012	MILANO	NOTAR		
09:43	000063	MILANO	NOTAR		
16:38	036808	MILANO	ANDREA		
16:33	036807	MILANO	ANDREA		
16:29	036806	MILANO	ANDREA		
15:12	036805	MILANO	ANDREA		
15:10	036804	MILANO	ANDREA		
15:02	036803	MILANO	ANDREA		
11:50	036799	MILANO	IVAN		
11:49	036788	MILANO	NOTAR		
11:42	036785	MILANO	ISOCRATE		
11:15	036774	MILANO	ISOCRATE		
12:35	036718	MILANO	NOTAR		
12:01	036717	MILANO	ISOCRATE		
11:11	036712	MILANO	LENCI		
10:53	036711	MILANO	SOCRATE		
16:53	036705	MILANO	MMMMM		
16:22	036700	MILANO	MMMMM		
17:01	036699	MILANO	NOTAR		
14:24	036688	MILANO	NOTAR		
12:29	036686	MILANO	MMMMM		
08:40	036680	MILANO	LENCI		
08:19	036660	MILANO	MMMMM		

Once a call is placed to the emergency queue (**112**), the agent can answer this by either pressing the **Answer** button highlighted or double clicking on the call waiting as highlighted.

Phone Station Operator - V. 4.5.4.0

**System state and Info**

Cristiano Notargiacomo  
 Station : 3001  
 Personal : 4001  
 Workplace : Post. 01  
 Address : 192.168.15.51

**Available**

**14:28:55**  
 09/23/2020

**Active Calls**

Number	Description
--------	-------------

**Phone Operations**

Call HangUp **Answer** Cons. DTMF

Resume Trasfer Conf. Park

**Short text messages**

[ Isola Call Taking ]

**List of calls in parking queue**

Waiting time	Source	Description	Trunk
--------------	--------	-------------	-------

**List of calls in personal queue**

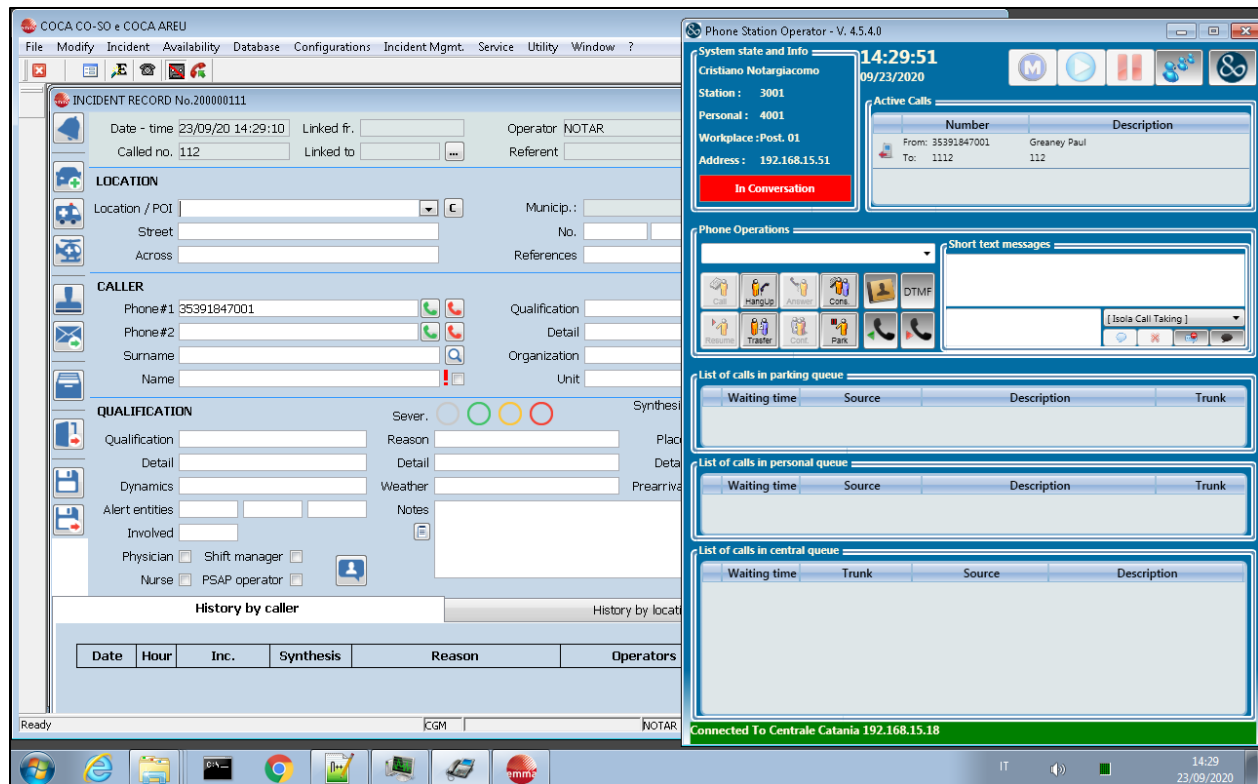
Waiting time	Source	Description	Trunk
--------------	--------	-------------	-------

**List of calls in central queue**

Waiting time	Trunk	Source	Description
00:00:00	112	35391847001	Greaney Paul

**Connected To Centrale Catania 192.168.15.18**

Once a call answered the caller's information is populated in the left side of the screen along with other important information such as their location (not used in testing). The call is then controlled from the window located on right side of the screen where the call can be transferred, conference or parked.



## 8.2. Verify Avaya Aura® Application Enablement Services DMCC

Using the Application Enablement Services web interface, click **Status** → **Status and Control** → **DMCC Service Summary**. The CAD CTI User (as configured in **Section 6.4**) should be present along with the appropriate number of **Associated Devices**.

**DMCC Service Summary - Session Summary**

Please do not use back button

☐ Enable page refresh every 60 seconds

Session Summary [Device Summary](#)  
Generated on Wed Sep 23 11:51:35 IST 2020  
Service Uptime: 1 days, 3 hours 33 minutes  
Number of Active Sessions: 4  
Number of Sessions Created Since Service Boot: 6  
Number of Existing Devices: 29  
Number of Devices Created Since Service Boot: 121

	Session ID	User	Application	Far-end Identifier	Connection Type	# of Associated Devices
<input type="checkbox"/>	0BACF96AAAE931A6 0854BA24F9A0986-6	beta80	CTI	192.168.15.18	XML Unencrypted	21
<input type="checkbox"/>	ADDEC832E0FFD996B D0E5CB7A1A06015-3	nice	DmccInterface	10.10.40.129	XML Unencrypted	8
<input type="checkbox"/>	5AE6EDED18628D128 C77D7DB0822FCE5-0	wspaces37	Khepri Call Server Connector	10.10.42.51	XML Encrypted	0
<input type="checkbox"/>	BE33C6B065EFEFFD3 7BA7F95CC8959BF-1	wspaces37	Khepri Call Server Connector	10.10.42.53	XML Encrypted	0

[Terminate Sessions](#) [Show Terminated Sessions](#)

## 8.3. Verify monitoring from Communication Manager

There are commands that can be used to show that certain stations are being monitored. The **List Monitor** command can be used to display any stations are being currently monitored.

```
list monitored-station
```

```
MONITORED STATION
```

```
Associations:      1      2      3      4      5      6      7      8
```

```
                  CTI      CTI      CTI      CTI      CTI      CTI      CTI      CTI
```

```
Station Ext      Lnk CRV Lnk CRV Lnk CRV Lnk CRV Lnk CRV Lnk CRV Lnk CRV Lnk CRV
```

```
-----
```

```
3001              1  0003
```

```
3002              1  0001
```

```
3003              1  0004
```

```
1000              1  0004
```

```
1100              1  0002
```

```
1105              1  0005
```

```
1106              1  0006
```

```
18911             1  001C
```

```
18912             1  001D
```

```
18913             1  001E
```

```
-----
```

```
Command successfully completed
```

## 9. Conclusion

These Application Notes describe the compliance testing of Beta 80 Life 1st and emma CAD CTI with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services. All test cases were executed successfully.

## 10. Additional References

This section references the product documentations 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
- [2] *Avaya Aura® Communication Manager Feature Description and Implementation*, Release 8.1
- [3] *Avaya Aura® Application Enablement Services Administration and Maintenance Guide*, Release 8.1
- [4] *Administering Avaya Aura® Session Manager*, Release 8.1

Product documentation for Life 1st and emma CAD CTI can be found by contacting Beta 80 as per **Section 2.3**.

# Appendix

The following shows the setup on Communication Manager to facilitate the ‘cherry picking’ of calls for the CAD CTI agents. Calls are routed to a VDN and then using Adjunct Routing the call is the routed to the CAD CTI. To ensure that the call is routed correctly there are a number of VDN’s and Vectors used, this will ensure that the call is routed correctly to the CAD CTI and also gives a backup should this call be unable to be received by the CAD CTI application.

The call is initially routed to the 91112 VDN where Vector 112 is called upon.

```
display vdn 91112                                     Page 1 of 3
                                         VECTOR DIRECTORY NUMBER
                                         Extension: 91112          Unicode Name? n
                                         Name*: 112 Entry
                                         Destination: Vector Number 112
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*:
2nd Skill*:
3rd Skill*:

SIP URI:

* Follows VDN Override Rules
```

Vector 112 then routes the call to another VDN 1112.

```
display vector 112                                     Page 1 of 6
                                         CALL VECTOR
Number: 112      Name: 112 Entry
Multimedia? n    Attendant Vectoring? n    Meet-me Conf? n    Lock? n
Basic? y    EAS? y    G3V4 Enhanced? y    ANI/II-Digits? y    ASAI Routing? y
Prompting? y    LAI? y    G3V4 Adv Route? y    CINFO? y    BSR? y    Holidays? y
Variables? y    3.0 Enhanced? y
01 wait-time    0    secs hearing ringback
02 route-to    number 1112      cov n if unconditionally
03 stop
04
05
06
07
08
09
10
11
12
```

VDN 1112 then calls upon Vector 212.

```
display vdn 1112                                     Page 1 of 3
                                                    VECTOR DIRECTORY NUMBER

      Extension: 1112                                Unicode Name? n
      Name*: 112 route to adj
      Destination: Vector Number 212
      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*:
      2nd Skill*:
      3rd Skill*:

SIP URI:

* Follows VDN Override Rules
```

Vector 212 then routes the call to the CAD CTI application using Adjunct Routing. If the call is not routed to the CAD CTI then the call proceeds to VDN 81112.

```
display vector 212                                   Page 1 of 6
                                                    CALL VECTOR

      Number: 212      Name: 112 route adj
Multimedia? n      Attendant Vectoring? n      Meet-me Conf? n      Lock? n
      Basic? y      EAS? y      G3V4 Enhanced? y      ANI/II-Digits? y      ASAI Routing? y
      Prompting? y      LAI? y      G3V4 Adv Route? y      CINFO? y      BSR? y      Holidays? y
      Variables? y      3.0 Enhanced? y
01 wait-time      0      secs hearing silence
02 adjunct      routing link 1
03 wait-time      1      mins hearing 1842      then continue
04 route-to      number 81112      cov n if unconditionally
05 stop
06
07
08
09
10
11
12
```



VDN 81112 calls upon Vector 231.

```
display vdn 81112                                     Page 1 of 3
                                         VECTOR DIRECTORY NUMBER

      Extension: 81112                                Unicode Name? n
      Name*: 112 loop
      Destination: Vector Number 231
      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*:
      2nd Skill*:
      3rd Skill*:

SIP URI:

* Follows VDN Override Rules
```

Vector 231 makes a second attempt at Adjunct Routing and again if this is not possible the call is routed on to 71112.

```
display vector 231                                     Page 1 of 6
                                         CALL VECTOR

      Number: 231      Name: 112 loop
Multimedia? n      Attendant Vectoring? n      Meet-me Conf? n      Lock? n
      Basic? y      EAS? y      G3V4 Enhanced? y      ANI/II-Digits? y      ASAI Routing? y
      Prompting? y      LAI? y      G3V4 Adv Route? y      CINFO? y      BSR? y      Holidays? y
      Variables? y      3.0 Enhanced? y
01 adjunct      routing link 1
02 wait-time      2      secs hearing 1842      then continue
03 route-to      number 71112      cov n if unconditionally
04 stop
05
06
07
08
09
10
11
12
```

VDN 71112 calls upon Vector 12.

```
display vdn 71112                                     Page 1 of 3
                                         VECTOR DIRECTORY NUMBER

      Extension: 71112                                Unicode Name? n
      Name*: 112 ACD no CTI
      Destination: Vector Number 12
      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*:
      2nd Skill*:
      3rd Skill*:

SIP URI:

* Follows VDN Override Rules
```

Vector 12 then routes the call to a skill which the agents would be associated with. This will act as a 'fall back' should the two previous Adjunct Routing attempts fail.

```
display vector 12                                     Page 1 of 6
                                         CALL VECTOR

      Number: 12      Name: 112 ACD
Multimedia? n      Attendant Vectoring? n      Meet-me Conf? n      Lock? n
      Basic? y      EAS? y      G3V4 Enhanced? y      ANI/II-Digits? y      ASAI Routing? y
      Prompting? y      LAI? y      G3V4 Adv Route? y      CINFO? y      BSR? y      Holidays? y
      Variables? y      3.0 Enhanced? y
01 wait-time      0      secs hearing silence
02 queue-to      skill 19      pri m
03 wait-time      15      secs hearing 1843      then continue
04 goto step      3      if unconditionally
05 stop
06
07
08
09
10
11
12
```

---

**©2020 Avaya Inc. All Rights Reserved.**

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya DevConnect Program at [devconnect@avaya.com](mailto:devconnect@avaya.com).