



DevConnect Program

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 R5.6 to interoperate with Avaya Aura® Communication Manager R10.1 and Avaya Aura® Application Enablement Services R10.1 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 R5.6 to interoperate with Avaya Aura® Communication Manager R10.1 and Avaya Aura® Application Enablement Services R10.1 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 Avaya Aura® 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 Avaya Aura® 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 Avaya Aura® 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, this was achieved using Adjunct Routing.

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. The DMCC API makes use of Telephony Services API (TSAPI) 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.

Several new VDNs and Vectors were setup as per the unique specifications of Beta 80 to allow the adjunct routing to work correctly and to ensure that the backup ACD was in place. VDN 91112 using Vector 112 → routing to 1112, VDN 1112 using Vector 212 → routing to 81112, VDN 81112 using Vector 231 → routing to 71112, VDN 71112 using Vector 12 → routing to backup ACD hunt group, as outlined in **Section 5.3**.

This same setup was put in place for VDNs 91113, 91115 and 91118, which all emulate different services such as Fire, Police and Personal Numbers.

For compliance testing three agents were logged into three different Avaya endpoints. Each of these endpoints were controlled by the CAD CTI platform.

- Agent 3401 logged into H.323 extension 3001
- Agent 3402 logged into SIP extension 3101
- Agent 3403 logged into Digital extension 3063

The primary focus of the compliance test was to ensure that the CAD CTI platform had total control of both call routing and the Avaya endpoint answering the call. To ensure this was the case, the following test scenarios were carried out.

- Agent login
- Agent's status selection
- Dispatcher/Call Taker presence
- 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
- Automatic recovery of the CTI channel
- Queue assignment to agents
- Voice communications statistics

2.2. Test Results

All test cases were executed successfully. Note that there was a specific setup using the VDN's and Vectors to allow Adjunct Routing to occur successfully. This setup can be found in **Section 5.3.3**.

2.3. Support

Technical support from Beta 80 is provided to customers after a contract has been signed. There is no support web site available for the Public at large. Beta 80 can be contacted as follows.

- Web: <https://content.beta80group.it/en/contact-us>

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.

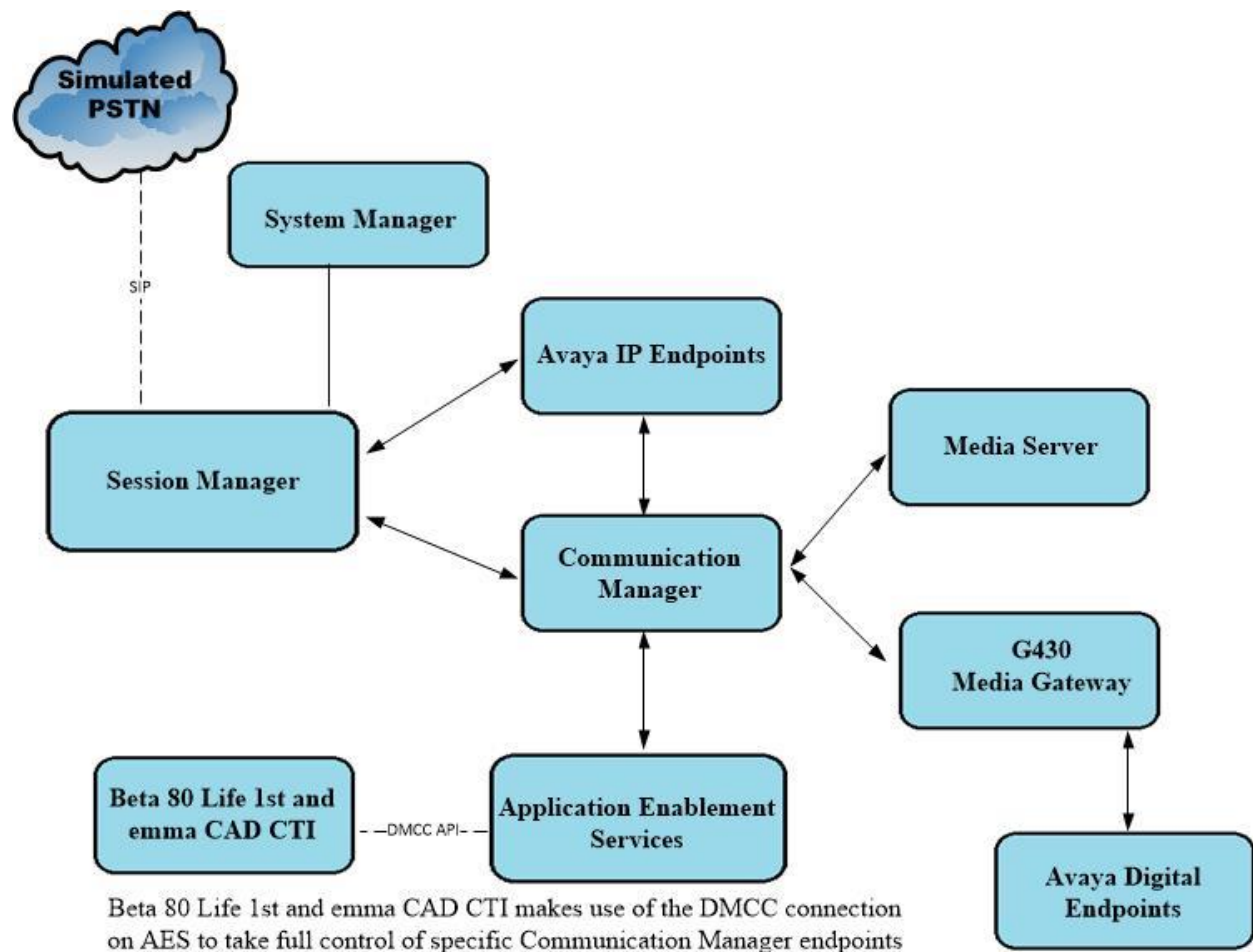


Figure 1: Connection of Beta 80 Life 1st and emma CAD CTI with Avaya Aura® Communication Manager R10.1 and Avaya Aura® Application Enablement Services R10.1

4. Equipment and Software Validated

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

Avaya Equipment/Software	Release/Version
Avaya Aura® System Manager	System Manager 10.1.3.0 Feature Pack 3 Build No. – 10.1.0.0.537353 Software Update Revision No: 10.1.3.0.0715713
Avaya Aura® Session Manager	Session Manager R10.1 Build No. – 10.1.3.0.1013007
Avaya Aura® Communication Manager	R10.1.3.0 – FP3 R020x.01.0.974.0 Update ID 01.0.974.0-27893
Avaya Aura® Application Enablement Services	R10.1 10.1.0.2.0.12-0
Avaya Aura® Media Server	10.1.0.101
Avaya Media Gateway G430	42.7.0 /2
Avaya J100 Series (H323) Deskphone	6.8.5.3.2
Avaya J100 Series (SIP) Deskphone	4.0.14.0.7
Avaya 96x1 Series (SIP) Deskphone	7.1.2.0.14
Avaya 9404 Digital Deskphone	17.0
Beta 80 Equipment/Software	Release/Version
Beta 80 emma/Life 1st CAD	1.5.0.0
Beta 80 emma/Life 1st CTI	5.6.1.3

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). Some screens in this section have been abridged and highlighted for brevity and clarity in presentation. The general installation of the servers and Media Gateways is presumed to have been previously completed and is not discussed here. 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 the Interface to Avaya Aura® Application Enablement Services
- Configure Avaya Endpoints for Third Party Call Control
- Configure Call Center Routing

5.1. Configure the 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
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		
(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		
COR: 1		
Name: aespri101x		

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

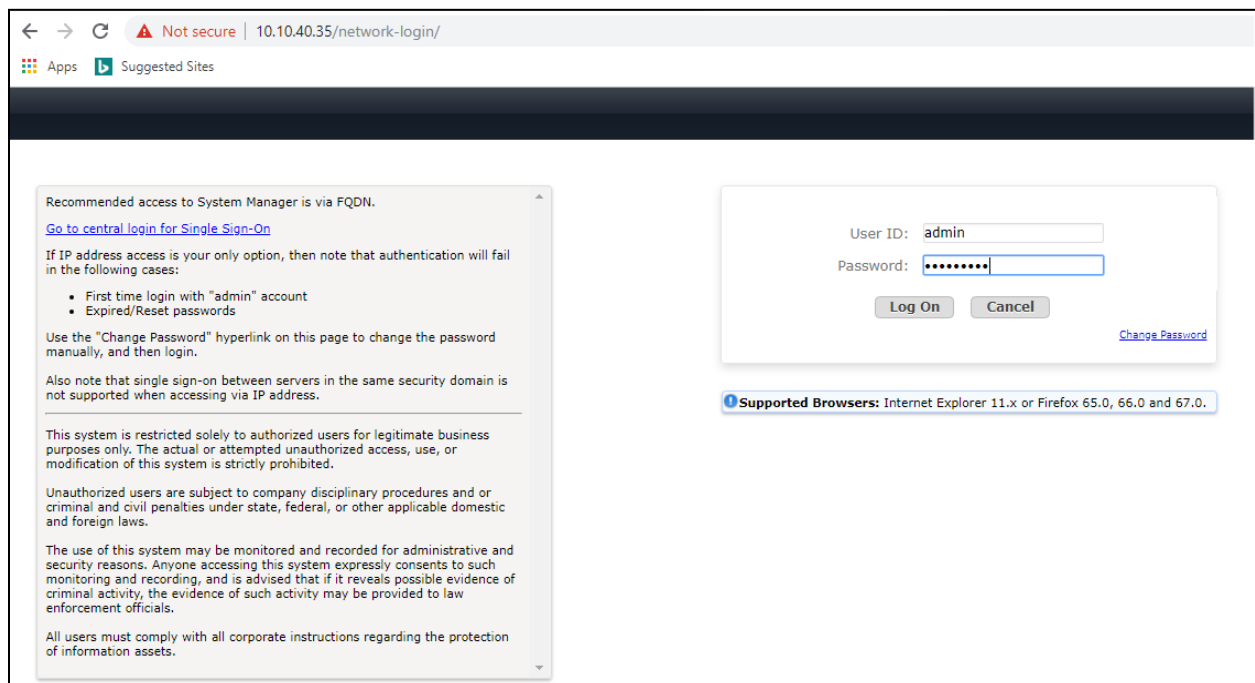
Each Avaya H.323 endpoint or station that needs to be monitored and used for 3rd party call control will need to have “IP Softphone” set to “y”. To make changes to a H.323 station, from Communication Manager type **change station x**, where x is the extension number of the station to be changed. Ensure 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	
	Message Lamp Ext: 1001	
Speakerphone: 2-way	Mute Button Enabled? y	
Display Language: english	Button Modules: 0	
Survivable GK Node Name:		
Survivable COR: internal	Media Complex Ext:	
Survivable Trunk Dest? y	IP SoftPhone? y	
	IP Video Softphone? n	
	Short/Prefixed Registration Allowed: default	
	Customizable Labels? y	

5.2.2. Configure Avaya SIP Endpoints

Each Avaya SIP endpoint or station that needs to be monitored and used for 3rd 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 **Error! Hyperlink reference not valid. 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.

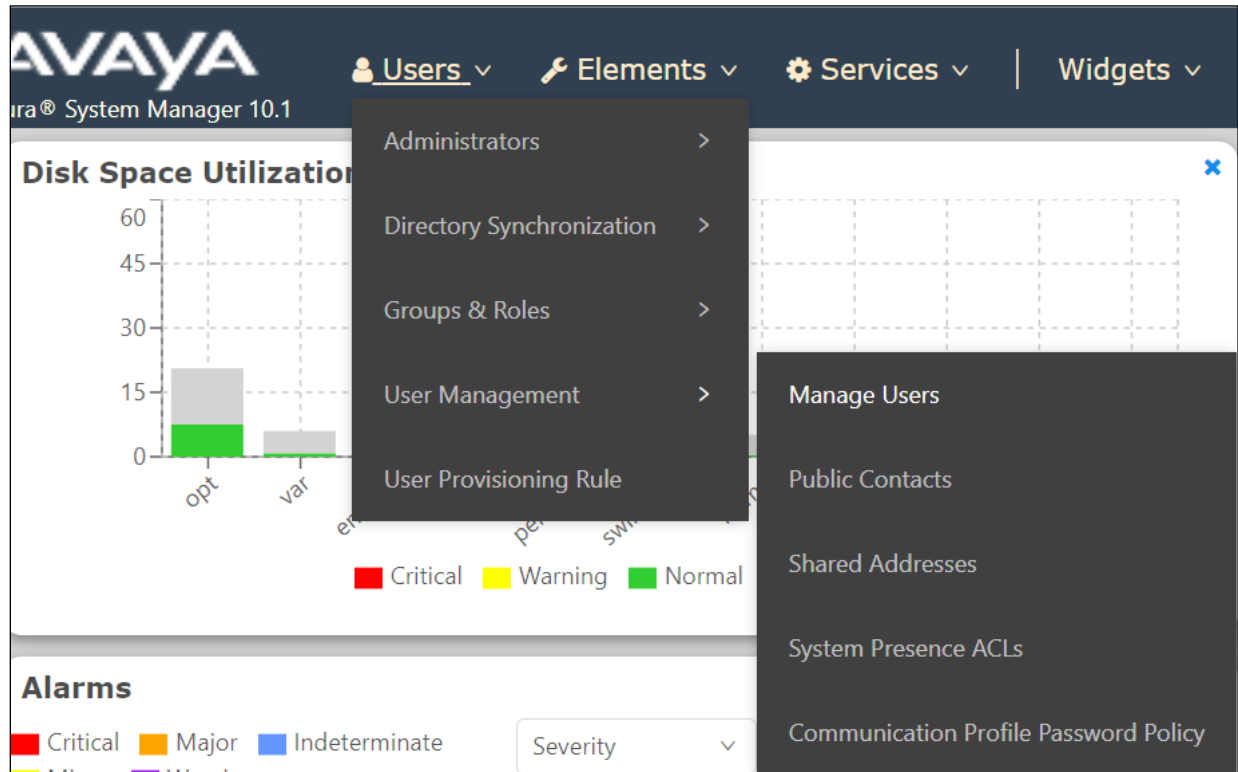
User ID:

Password:

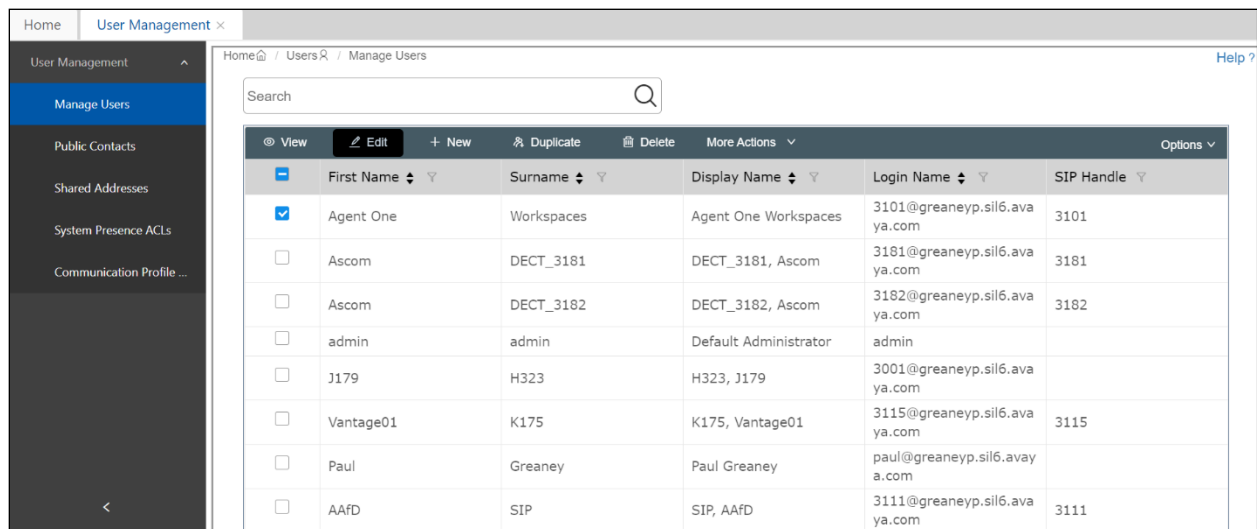
[Change Password](#)

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 **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.

In the **General Options** tab ensure that **Type of 3PCC Enabled** is set to **Avaya** as is shown below.

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)																
Active Station Ringing	single		Auto Answer	none														
MWI Served User Type	sip-adjunct		Coverage After Forwarding															
Per Station CPN - Send Calling Number	None		Display Language	english														
IP Phone Group ID			Hunt-to Station															
Remote Soft Phone Emergency Calls	as-on-local		Loss Group	19														
LWC Reception	spe		Survivable COR	internal														
AUDIX Name	None		Time of Day Lock Table	None														
Short/Prefixed Registration Allowed	default		Music Source															
Voice Mail Number	6111																	
Bridging Tone for This Extension	no																	
Features <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 | 3101@greanep.sil6.avaya.com

Commit & Continue

Commit

Cancel

Identity

Communication Profile

Membership

Contacts

Communication Profile Password

PROFILE SET : Primary

Communication Address

PROFILES

Session Manager Profile

Avaya Breeze® Profile

CM Endpoint Profile

* System : cm101x

* Profile Type : Endpoint

Use Existing Endpoints : ☐

* Extension : 3101

Template : Start typing...

* Set Type : 9641SIPCC

Security Code : Enter Security Code

Port : S000003

Voice Mail Number : 6667

Preferred Handle : Select

Calculate Route Pattern : ☐

Sip Trunk : aar

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 Backup ACD.
- Configure Agents.
- Configure Adjunct Routing for Cherry Picking.

5.3.1. Configure Backup ACD

In the event that the CAD CTI platform fails, the call should still get routed to the agent's phone. To allow this to happen the 'backup ACD' skill/hunt group is used, and the agents are logged into this skill.

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**.

add hunt-group 90		Page	1 of	4
HUNT GROUP				
Group Number:	90	ACD?	y	
Group Name:	Backup ACD	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 Agents

Agents are configured to use the skill group setup in **Section 5.3.1**. Enter the command **change agent-loginID x** where **x** is an agent ID 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.

change agent-loginID 3401		Page 1 of 2
AGENT LOGINID		
Login ID: 3401	Unicode Name? n	AAS? n
Name: Agent One	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:1234		
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).

add agent-loginID 5001				Page 2 of 2			
				AGENT LOGINID			
Direct Agent Skill: 90				Service Objective? n			
Call Handling Preference: skill-level				Local Call Preference? n			
SN	RL	SL		SN	RL	SL	
1:	90	1		16:			
2:				17:			
3:				18:			
4:				19:			

5.3.3. Configure Adjunct Routing for CAD CTI

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 VDNs and Vectors used, this will ensure that the call is routed correctly to the CAD CTI and gives a backup routing option should the CAD CTI application become inoperable. The following shows the setup for just one “service” for example ‘Police Service 1112’.

Note: The same structure will need to be repeated for each service and each personal VDN that are added.

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
```

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**. Note the key entry here is **adjunct routing link 1**, as 1 is the CTI link created in **Section 5.1.2**.

```

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

```

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
```

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. Note that this skill number **90** is that ‘ACD backup’ hunt group created in **Section 5.3.1**.

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 90 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

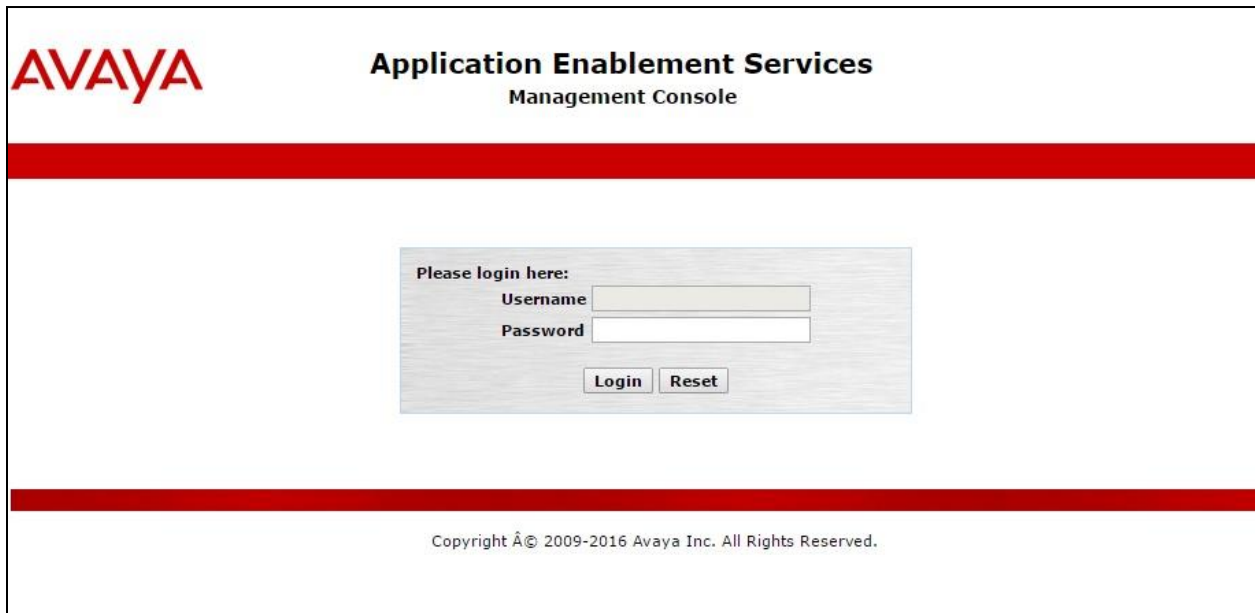
6. Configure Avaya Aura® Application Enablement Services

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 two input fields: "Username" and "Password". 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 **DMCC Service** and **TSAPI Service** are licensed by ensuring that **DMCC Service** and **TSAPI Service** are both 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.

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

DLG does not support Encrypted link. In case of GDPR (Data Privacy) enabled systems, use of DLG service will be site responsibility. By default DLG will be in running state

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 10.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. Navigate to **Licensing → WebLM Server Access** to observe these licenses.

Licensing | WebLM Server Access

Home | Help | Logout

▶ AE Services

▶ Communication Manager Interface

▶ High Availability

▼ Licensing

WebLM Server Address

WebLM Server Access

Reserved Licenses

▶ Maintenance

WebLM Server Access

WebLM Server Access helps you to access the WebLM server specified on the WebLM Server Address page.

- If you are using a local Avaya WebLM server, the AE Services management console redirects you to the Web License Manager page for WebLM configuration.
- If you are using a standalone WebLM server, you must manually log in to the WebLM server for WebLM configuration.

PG; Reviewed:
SPOC 8/23/2023

Avaya DevConnect Application Notes
©2023 Avaya Inc. All Rights Reserved.

21 of 42
Beta80_AES101

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

WebLM Home

Install license

Licensed products

APPL_ENAB

▼ Application_Enablement

View by feature

View by local WebLM

Enterprise configuration

► Local WebLM Configuration

► Usages

► Allocations

Periodic status

COLLABORATION_ENVIRONMENT

► COLLABORATION_ENVIRONMENT

COMMUNICATION_MANAGER

► Call_Center

► Communication_Manager

Configure Centralized Licensing

CONTROLMANAGER

► Control_Manager

MEDIA_SERVER

► Media_Server

OL

► OL

SYSTEM_MANAGER

► System_Manager

Application Enablement (CTI) - Release: 10 - SID: 11 (Enterprise license file)

You are here: Licensed Products > Application_Enablement > View by Feature

License installed on: January 12, 2023 12:55:41 PM +01:00

License Owner: Avaya DevConnect Any Street US United States

License Host: qreareys_V7-9C-9C-27-93-A6-01_Aura19.L

Notes: This production license file is for use on a production license host.

License File Host IDs: V7-9C-9C-27-93-A6-01, V7-9C-9C-27-93-A6-01

Feature (License Keyword)	Expiration date	License Capacity
Unified CC API Desktop Edition (VALUE_AES_AEC_UNIFIED_CC_DESKTOP)	March 1, 2024	1000
CVLAN ASAI (VALUE_AES_CVLAN_ASAI)	March 1, 2024	16
High Availability Medium (VALUE_AES_HA_MEDIUM)	March 1, 2024	8
Device Media and Call Control (VALUE_AES_DMCC_DMC)	March 1, 2024	1000
AES ADVANCED SMALL SWITCH (VALUE_AES_AEC_SMALL_ADVANCED)	March 1, 2024	3
AES ADVANCED LARGE SWITCH (VALUE_AES_AEC_LARGE_ADVANCED)	March 1, 2024	3
DLG (VALUE_AES_DLG)	March 1, 2024	16
TSAPI Simultaneous Users (VALUE_AES_TSAPI_USERS)	March 1, 2024	1000
High Availability Large (VALUE_AES_HA_LARGE)	March 1, 2024	3

SmallServerTypes: s8300c;s8300d;icc;premio;tn8400;laptop;CtiS
MediumServerTypes: ibmx306;ibmx306m;dell1950;xen;hs20;hs20_1

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.

AE Services | TSAPI | TSAPI Links

▼ AE Services

► CVLAN

► DLG

► DMCC

► SMS

▼ TSAPI

■ TSAPI Links

■ TSAPI Properties

TSAPI Links

Link	Switch Connection
Add Link	Edit Link Delete Link

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 **cm101x**, 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 **cm101x** will be used during the configuration of the CAD CTI server, this name should be noted here and given to the Beta 80 engineers.

AE Services | TSAPI | TSAPI Links

AE Services

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

Communication Manager Interface

▶

Edit TSAPI Links

Link 1

Switch Connection cm101x ▼


Switch CTI Link Number 1 ▼

ASAI Link Version 12 ▼

Security Both ▼

Apply Changes Cancel Changes 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	cm101x	1	12	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.

▶ AE Services			
▶ Communication Manager Interface			
High Availability			
▶ Licensing			
▶ Maintenance			
▼ Networking			
AE Service IP (Local IP)			
Network Configure			
Ports			
TCP/TLS Settings			
▶ Security			
▶ Status			
▶ User Management			
▶ Utilities			
▶ Help			

Ports

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

DLG Port	TCP Port	5678	
----------	----------	------	--

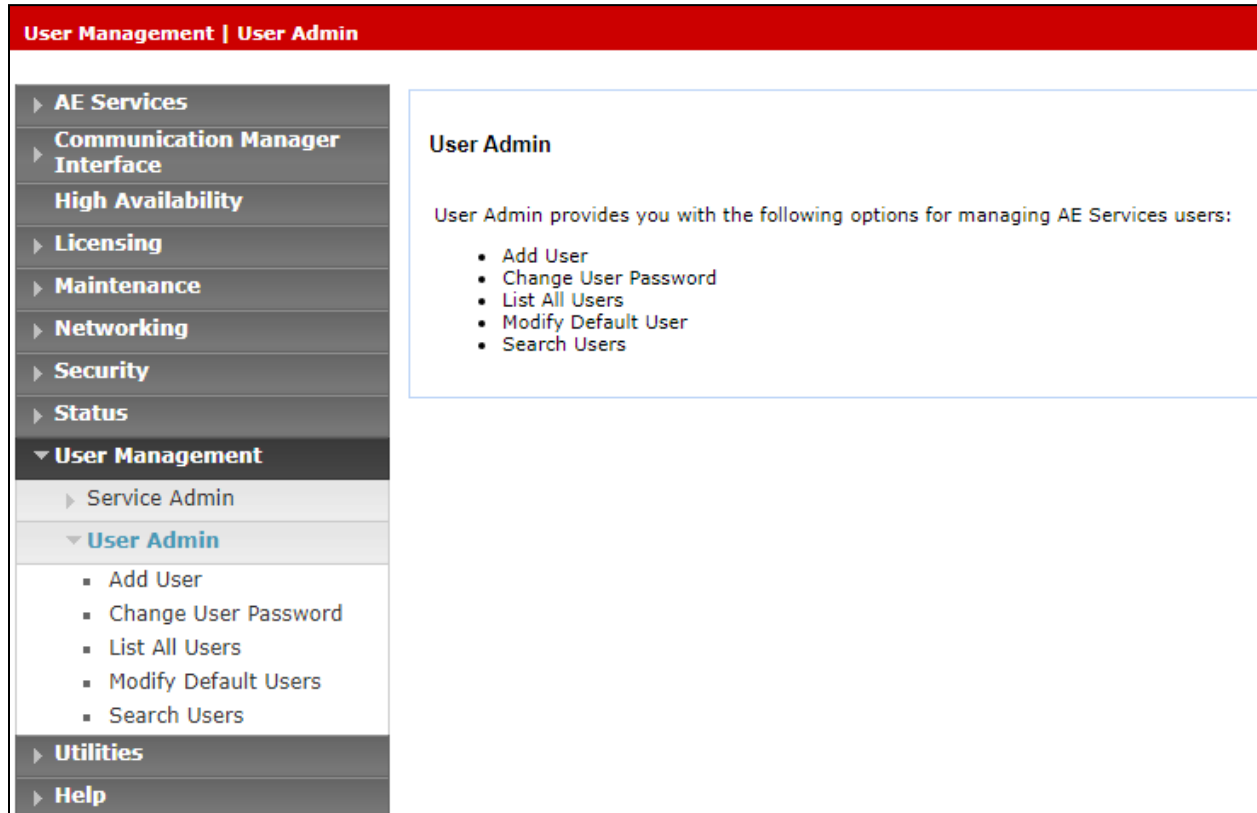
TSAPI Ports			Enabled Disabled
TSAPI Service Port	450		<input checked="" type="radio"/> <input type="radio"/>
Local TLINK Ports			
TCP Port Min	1024		
TCP Port Max	1039		
Unencrypted TLINK Ports			
TCP Port Min	<input type="text" value="1050"/>		
TCP Port Max	<input type="text" value="1065"/>		
Encrypted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

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

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"/>		
			Enabled Disabled
Server Media			<input checked="" type="radio"/> <input type="radio"/>
RTP Local UDP Port Min*	<input type="text" value="30000"/>		
RTP Local UDP Port Max*	<input type="text" value="49999"/>		

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.



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

- **User Id** - This will be used by the CAD CTI setup in **Section 0**.
- **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 0**.
- **CT User** - Select **Yes** from the drop-down menu.

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

<div><div>▶ AE Services</div><div>▶ Communication Manager Interface</div><div>High Availability</div><div>▶ Licensing</div><div>▶ Maintenance</div><div>▶ Networking</div><div>▶ Security</div><div>▶ Status</div><div>▼ User Management</div><div>▶ Service Admin</div><div>▼ User Admin</div><div>▪ Add User</div><div>▪ Change User Password</div><div>▪ List All Users</div><div>▪ Modify Default Users</div><div>▪ Search Users</div><div>▶ Utilities</div><div>▶ Help</div></div>	<div><h3>Edit User</h3><div>* User Id<div>devconnect</div></div><div>* Common Name<div>devconnect</div></div><div>* Surname<div>devconnect</div></div><div>User Password<div>.....</div></div><div>Confirm Password<div>.....</div></div><div>Admin Note<div></div></div><div>Avaya Role<div>None</div></div><div>Business Category<div></div></div><div>Car License<div></div></div><div>CM Home<div></div></div><div>Css Home<div></div></div><div>CT User<div>Yes</div></div><div>Department Number<div></div></div><div>Display Name<div></div></div><div>Employee Number<div></div></div><div>Employee Type<div></div></div><div>Enterprise Handle<div></div></div><div>Given Name<div></div></div><div>Home Phone<div></div></div><div>Home Postal Address<div></div></div><div>Initials<div></div></div><div>Labeled URI<div></div></div></div>
---	--

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

▶ AE Services

▶ Communication Manager Interface

▶ High Availability

▶ Licensing

▶ Maintenance

▶ Networking

▼ Security

▶ Account Management

▶ Audit

▶ Certificate Management

▶ Enterprise Directory

▶ Host AA

▶ PAM

▼ Security Database

▪ Control

▪ CTI Users

▪ List All Users

▪ Search Users

▪ Devices

▪ Device Groups

CTI Users

User ID	Common Name	Worktop Name	Device ID
<input type="radio"/> asc	asc	NONE	NONE
<input type="radio"/> centricity	centricity	NONE	NONE
<input checked="" type="radio"/> devconnect	devconnect	NONE	NONE
<input type="radio"/> mitel	mitel	NONE	NONE
<input type="radio"/> nice1	nice1	NONE	NONE
<input type="radio"/> paul1	paul1	NONE	NONE
<input type="radio"/> paul2	paul2	NONE	NONE
<input type="radio"/> qfiniti	qfiniti	NONE	NONE
<input type="radio"/> smoke	smoke	NONE	NONE
<input type="radio"/> sytel	Sytel	NONE	NONE
<input type="radio"/> voxtronic	voxtronic	NONE	NONE

Edit List All

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

Edit CTI User

User Profile:

User ID
Common Name
Worktop Name
Unrestricted Access

devconnect
devconnect
NONE ▼
☒

Call and Device Control:

Call Origination/Termination and Device Status

None ▼

Call and Device Monitoring:

Device Monitoring
Calls On A Device Monitoring
Call Monitoring

None ▼
None ▼
☐

Routing Control:

Allow Routing on Listed Devices

None ▼

Apply Changes

Cancel Changes

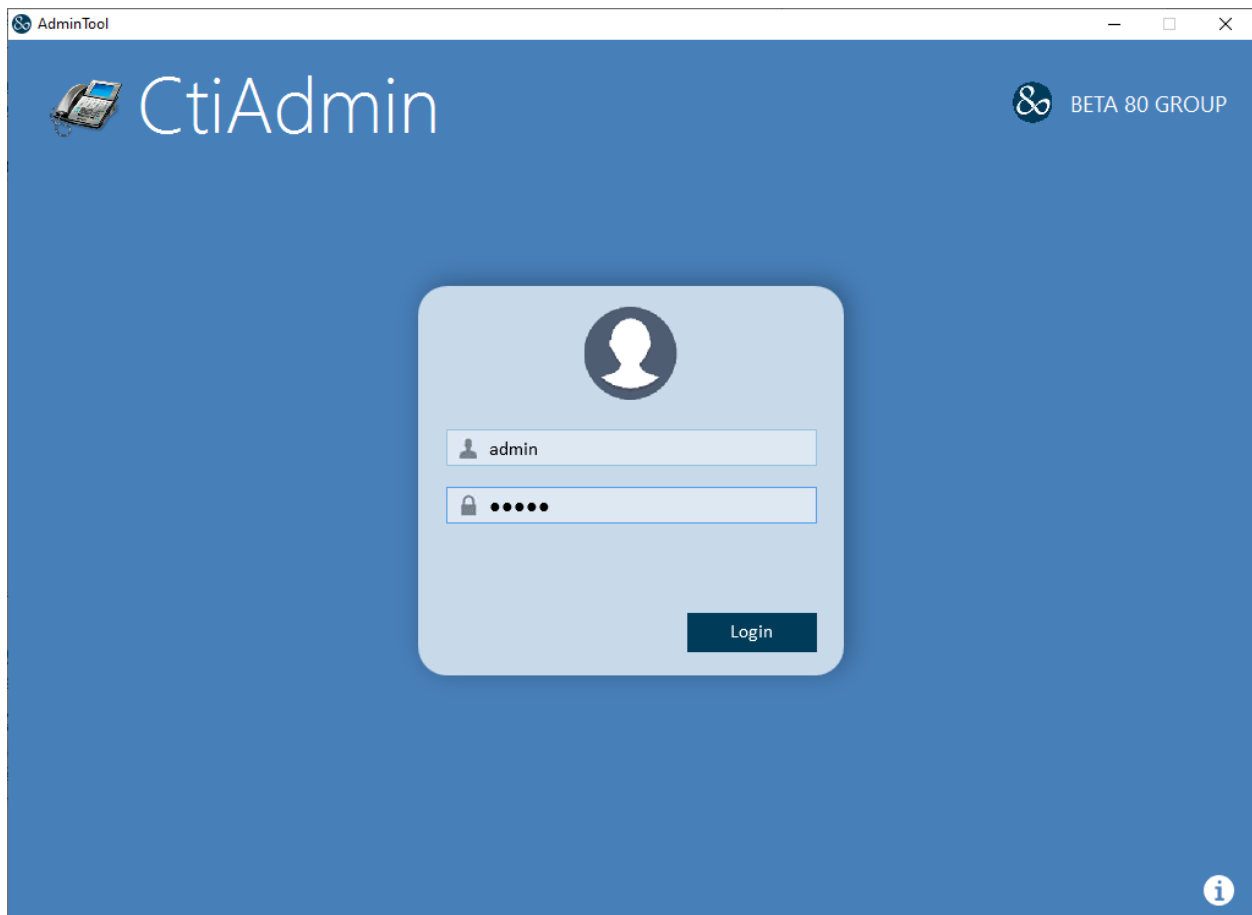
Click on **Apply** when asked again to **Apply Changes** (not shown).

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. 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:

- PBX (CTI link to Avaya Aura® Application Enablement Services)
- 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.



7.1. Configuration of PBX (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, PSAP admins can define the relevant info regarding the CTI link in the “PBX” tab of the configurator. The system can support multiple PBXs and the configuration is performed mainly editing the **Informazioni aggiuntive** field which is a JSON with the following properties.

EndpointConfiguration: list of AES endpoints. For this setup we only used 1 AES. Each object is made of the following:

- **Primary:** boolean value indicating if the object is to be considered as primary (true) or as backup (false).
- **PBXConfiguration:** it contains the AES info.
- **Ip:** This corresponds to the AES IP address (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).
- **Port:** This corresponds to the DMCC port number, as per **Section 6.3**.
- **Username:** This corresponds to the CTI user configured in **Section 6.4**.
- **Password:** This corresponds to the CTI user’s password (it needs to be obfuscated using a proprietary tool), as per **Section 6.4**.
- **CMConfiguration:** it contains the CM info.
- **Ip:** This corresponds to the IP address of Communication Manager.
- **SwitchName:** This corresponds to the Communication Manager Switch name, as per **Section 6.2**.

```
"EndpointConfiguration": [{
  "Primary": true,
  "PBXConfiguration": {
    "Ip": "10.10.40.16",
    "Port": 4721,
    "Username": "devconnect",
    "Password": "6U7xxU79xUdUd5ddd65c"
  },
  "CMConfiguration": {
    "Ip": "10.10.40.13",
    "SwitchName": "cml01x"
  }
},
]
```

AdminTool
Logout Monitor Device Rubrica Configurazione Gestione Errori

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

PBX Avaya Certification
PBX Avaya Lab Beta

Nome: PBX Avaya Certification
IP: 10.10.40.16
MAC:
Porta: 4721
Nome Host:
Supplier: Avaya
Codice PBX Supplier: Avaya v10.x.y.t
IP Backup:
MAC Backup:
Porta Backup: 0
Nome Host Backup:
Descrizione: PBX Avaya AES - v10.x.y.t
Note:
Informazioni Aggiuntive:

```

"PluginSpecific": {
  "EndpointConfiguration": [{
    "Primary": true,
    "PBXConfiguration": {
      "Ip": "10.10.40.16",
      "Port": 4721,
      "Username": "devconnect",
      "Password": "6U7xxU79xUdUd5ddd65c"
    },
    "CMConfiguration": {
      "Ip": "10.10.40.13",
      "SwitchName": "cm101x"
    }
  ]
}

```

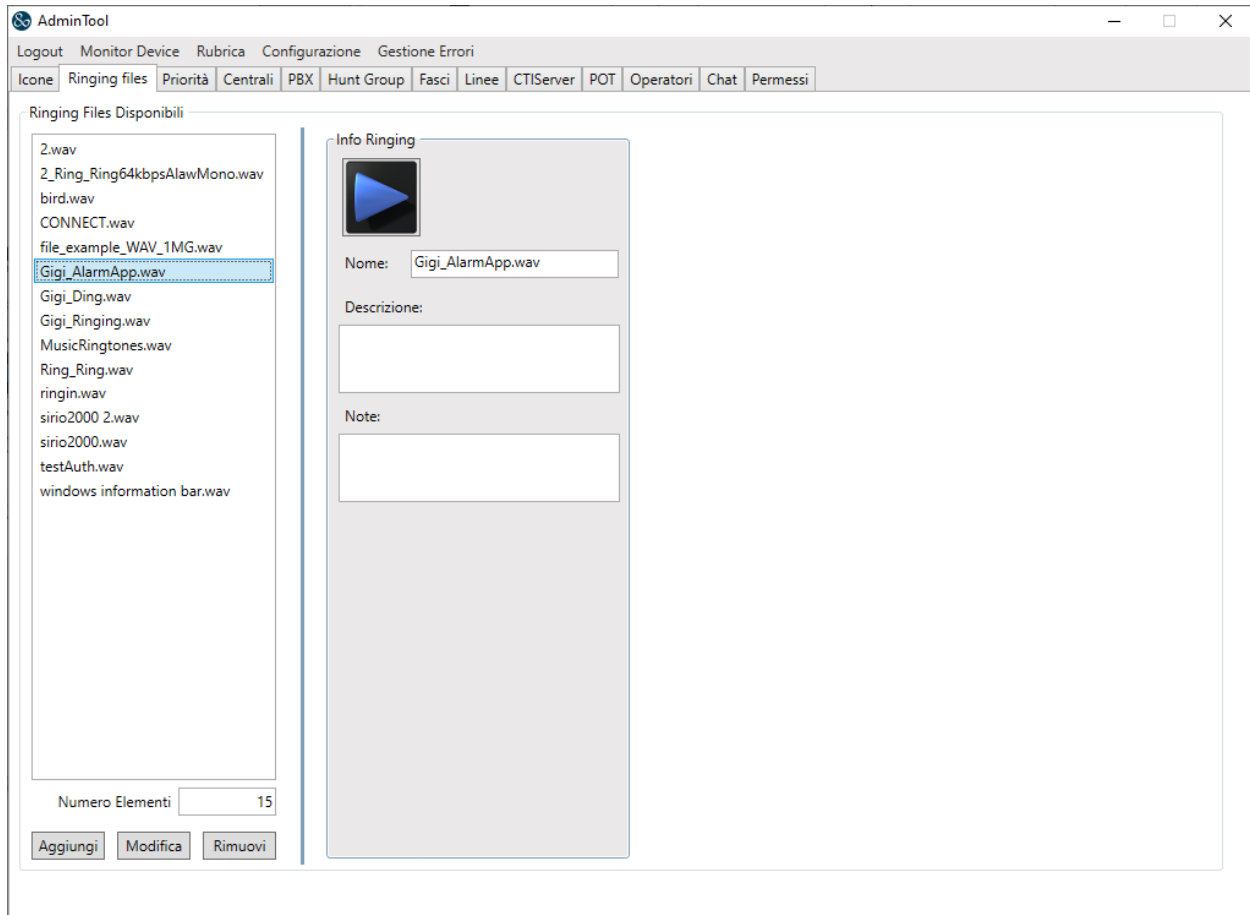
Rimuovi Modifica Aggiungi

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 screenshot displays the 'AdminTool' web application interface. At the top, there is a navigation bar with links: Logout, Monitor Device, Rubrica, Configurazione, and Gestione Errori. Below this is a tabbed interface with the following tabs: Icone, Ringing files, Priorità, Centrali, PBX, Hunt Group, Fasci, Linee, CTIServer, POT, Operatori, Chat, and Permessi. The 'Icone' tab is currently selected. The main content area is divided into two panels. The left panel, titled 'Icone Disponibili', lists four available icons: Hungup.png, Lightning.png (which is highlighted with a blue dashed border), SolaVisualizzazione.png, and test-icon.jpg. Below this list is a 'Numero Elementi' field set to '4' and three buttons: 'Aggiungi', 'Modifica', and 'Rimuovi'. The right panel, titled 'Info Icona', shows the configuration for the selected 'Lightning.png' icon. It includes a visual preview of a yellow lightning bolt icon, a 'Nome' field containing 'Lightning.png', a 'Colore' field with a red color swatch, a 'Descrizione' text area, and a 'Note' text area.

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



7.3. Personal Queues Configuration

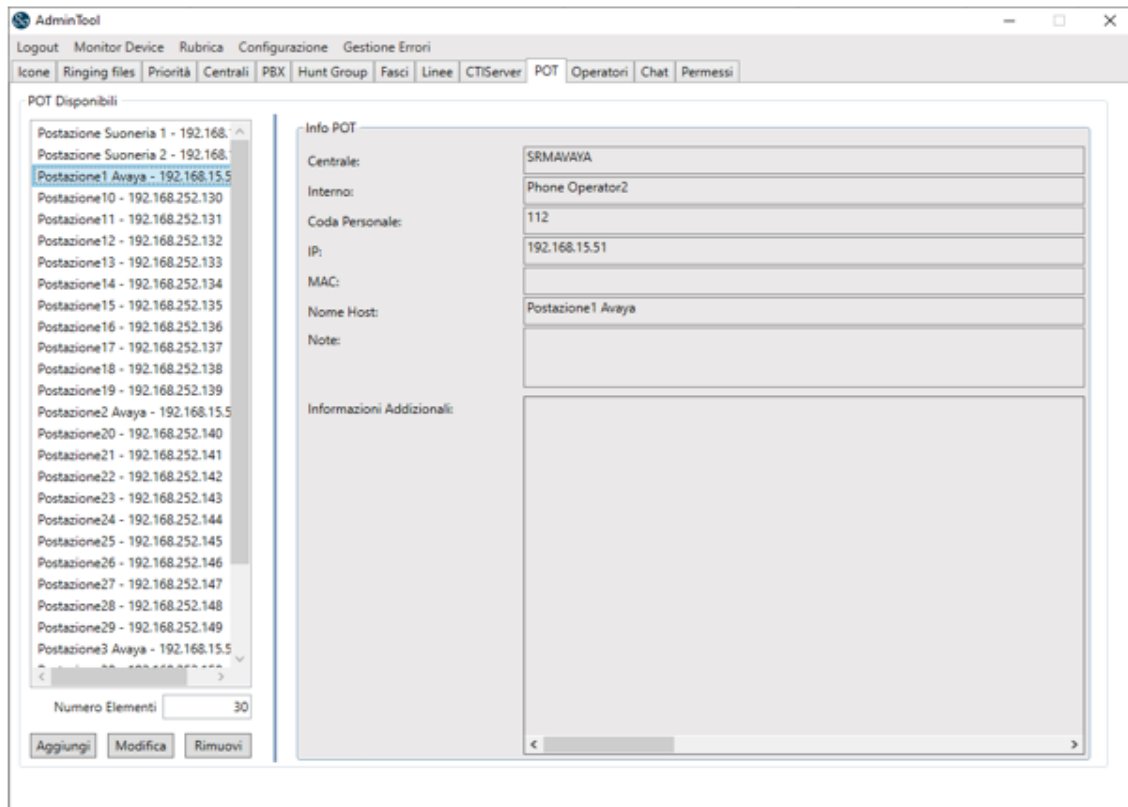
Agents' personal queues are configured under the **Hunt Group** tab. Where a specific queue is assigned to the agent at hand. Each queue is associated with the monitored VDN configured on Communication Manager.

The screenshot displays the AdminTool web interface. The top navigation bar includes links for Logout, Monitor Device, Rubrica, Configurazione, and Gestione Errori. Below this is a tabbed menu with options: Icone, Ringing files, Priorità, Centrali, PBX, Hunt Group (selected), Fasci, Linee, CTIServer, POT, Operatori, Chat, and Permessi. The main content area is titled 'Hunt Group Disponibili' and features a list of available hunt groups. The group '112' is selected and highlighted. Below the list, there are buttons for 'Aggiungi', 'Modifica', and 'Rimuovi', along with a 'Numero Elementi' field showing '72'. To the right of the list is the 'Info Hunt Group' configuration panel for group 112. This panel contains various fields: Icona (empty), Audio (play button icon), PBX (PBX Avaya Certification), Codice (C1112), Nome (112), Tipo (HG PERSONAL), Priorità (Very High - Urgent), Centrale (SRMAVAYA), Public Code (empty), Codice HG Supplier (1112), HG Prompt (empty), HG Prompt Timeout (empty), Descrizione (empty), Note (empty), and Informazioni Aggiuntive (a JSON object: { "Common": { "SendPresenceOnAnswer": true } }).

Info Hunt Group	
Icona:	
Audio:	
PBX:	PBX Avaya Certification
Codice:	C1112
Nome:	112
Tipo:	HG PERSONAL
Priorità:	Very High - Urgent
Centrale:	SRMAVAYA
Public Code:	
Codice HG Supplier:	1112
HG Prompt:	
HG Prompt Timeout:	
Descrizione:	
Note:	
Informazioni Aggiuntive:	<pre>{ "Common": { "SendPresenceOnAnswer": true } }</pre>

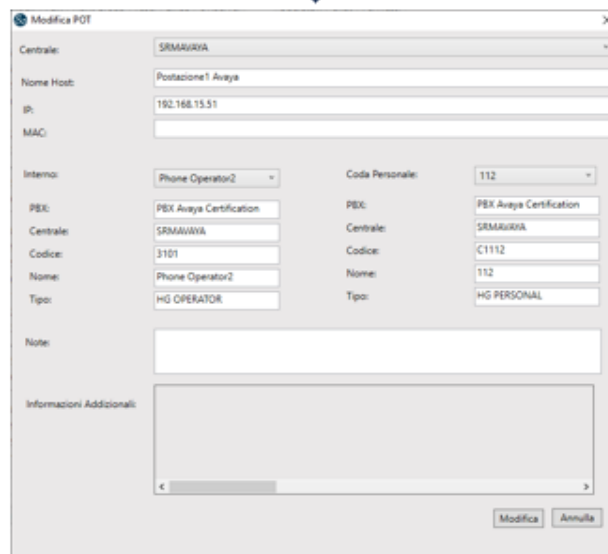
7.4. Positions Configuration

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 left pane, titled 'POT Disponibili', lists various positions. The right pane, titled 'Info POT', shows the configuration details for the selected position.

Field	Value
Centrale:	SRMAVAYA
Interno:	Phone Operator2
Coda Personale:	112
IP:	192.168.15.51
MAC:	
Nome Host:	Postazione1 Avaya
Note:	
Informazioni Aggiuntive:	



The screenshot shows the 'Modifica POT' (Modify POT) screen. It contains the same fields as the 'Info POT' screen, but with additional fields for editing the position's details.

Field	Value
Centrale:	SRMAVAYA
Nome Host:	Postazione1 Avaya
IP:	192.168.15.51
MAC:	
Interno:	Phone Operator2
Coda Personale:	112
PEX:	PEX Avaya Certification
Centrale:	SRMAVAYA
Codice:	3101
Nome:	Phone Operator2
Tipo:	HG OPERATOR
Note:	
Informazioni Aggiuntive:	

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 of operators is displayed, including 'ANDREA - Rossini Andrea', 'NOTAR - Notargiacomo Cristiano', and 'Oper1 - CognomeOper1 NomeO'. The 'Oper1' operator is selected. On the right, the 'Info Operatore' form is shown with the following fields:

- Icona: ☐
- Audio: ☐
- Centrale: SRMAVAYA
- Context: 0
- Gruppo: 0
- User: 0
- Username: Oper1
- Nome: NomeOper1
- Cognome: CognomeOper1
- Interno:
- Coda Personale:
- Note:
- Informazioni Aggiuntive:

At the bottom of the list, there are buttons for 'Aggiungi', 'Modifica', and 'Rimuovi', and a 'Numero Elementi' field showing 31.



The screenshot shows the 'Modifica Operatore' form. It contains the same fields as the 'Info Operatore' form, but with additional fields for permissions and personal code:

- Centrale: SRMAVAYA
- Context: 0
- Gruppo: 0
- User: 0
- Username: Oper1
- Nome: NomeOper1
- Cognome: CognomeOper1
- Interno:
- Coda Personale:
- Note:
- Informazioni Aggiuntive:
- Info permesso selezionato:
- Info Coda Personale Selezionata:

At the bottom right, there are buttons for 'Modifica' and 'Annulla'.

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.

AdminTool

Logout Monitor Device Rubrica Configurazione Gestione Errori

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

Genera Nuovi Permessi

Seleziona un operatore

Centrale: SRMAVAYA Operatore: Oper1 Tutti

Interno: Tutti Postazione: Postazione1 Avaya - 192.168.1 Tutti

Priorità: Permessi:

Icona:

Rimuovi

Audio:

Rimuovi

Pulisci

Genera Permessi

Info permesso selezionato

PBX: PBX Avaya Certification

Centrale: SRMAVAYA

Codice: C1112

Nome: 112

Tipo: HG PERSONAL

Permessi Disponibili

Operatore	POT	Hunt Group	Permessi	Priorità	Icona	Audio			
Oper1	192.168.15.51	112	Completa gestione	Very High	Hungup.png	Gigi_Ringing.wa		Modifica	Rimuovi
Oper1	192.168.15.51	113	Completa gestione	Medium	Hungup.png	Gigi_Ringing.wa		Modifica	Rimuovi
Oper1	192.168.15.51	118	Completa gestione	Very High	Hungup.png	Gigi_Ringing.wa		Modifica	Rimuovi

Salva Permessi

Rimuovi Selezionati

Copia autorizzazioni

Numero Elementi 3

PG; Reviewed:
SPOC 8/23/2023

Avaya DevConnect Application Notes
©2023 Avaya Inc. All Rights Reserved.

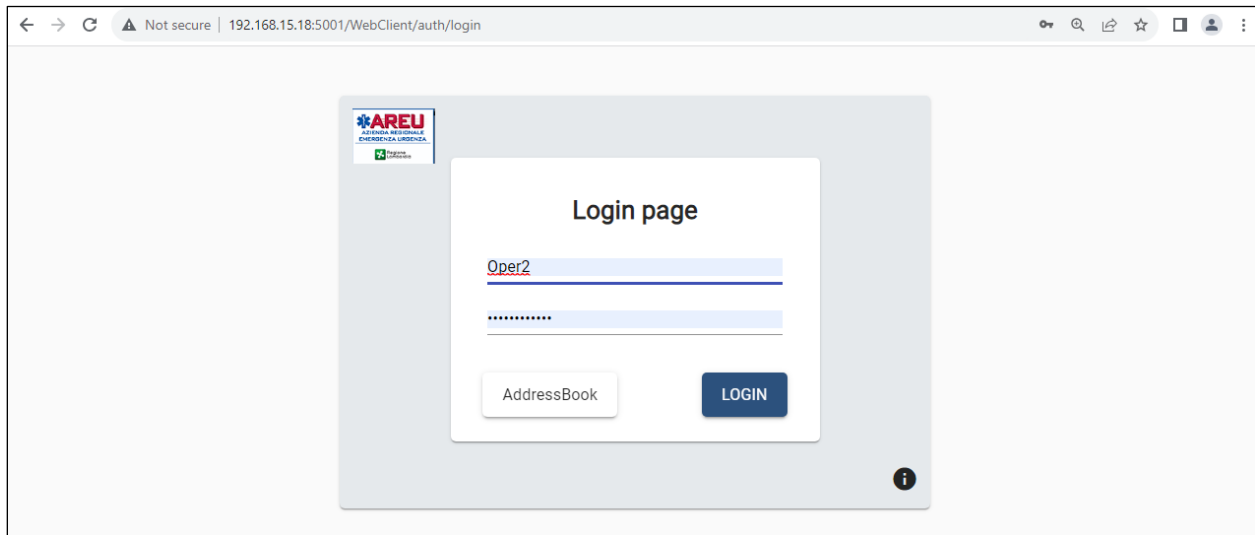
37 of 42
Beta80_AES101

8. Verification Steps

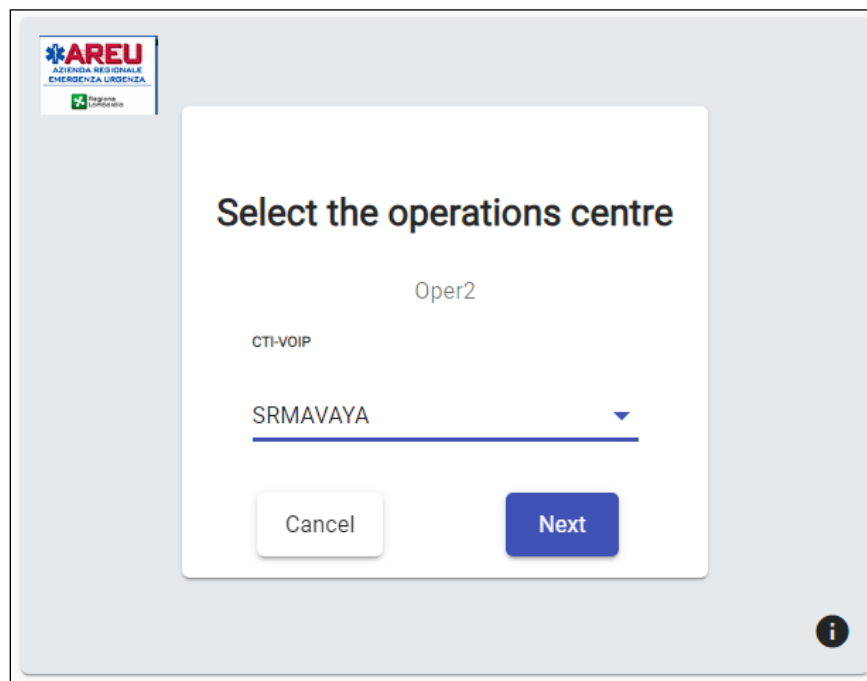
The correct configuration of the solution can be verified as follows.

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

Open the agent desktop using a suitable browser to connect to the URL **http://ServerIP:5001**. Enter the appropriate Agent/Operator ID and Password and click on **LOGIN**.



Select the appropriate **operations centre** and click on **Next**.



The following screen will be displayed showing the agent **Available** to take calls.

Connected to SRMAVAYA

General information

Available

Wednesday 07/26/2023 16:36:51

Available

No active call

Phone

Name or number to be called...

Call Answer Addressbook

Highlights

EMS FIRE LAW

Resume Park Call Call history

Consult Transfer Presence

Conference DTMF Chat

Personal queue

Waiting	Line	Caller	Description
---------	------	--------	-------------

Global queue

Waiting	Line	Caller	Description
---------	------	--------	-------------

Operator2 - NomeOper2 CognomeOper2

Operators presence

Available 2 Busy 0 Pause 0 Not Connected 0

Status	Workplace	Name	Phone	Queue	Workplace status	Operator status
🕒	Postazione1	Oper1 - NomeOper1 Cog...	3101	C1112	00:12	00:06
🟢	Postazione2	Oper2 - NomeOper2 Cog...	3180	C1115	00:11	00:08

Once a call is placed to the emergency queue (**1113**), the agent can answer this by either pressing the **Answer** button highlighted or double clicking on the call waiting.

Connected to SRMAVAYA

General information

Available

Wednesday 07/26/2023 16:37:39

Available

No active call

Phone

Name or number to be called...

Call **Answer** Addressbook

Highlights

EMS FIRE LAW

Resume Park Call Call history

Consult Transfer Presence

Conference DTMF Chat

Personal queue

Waiting	Line	Caller	Description
---------	------	--------	-------------

Global queue

Waiting	Line	Caller	Description
📞	00:22	1113	35391847001 EMS

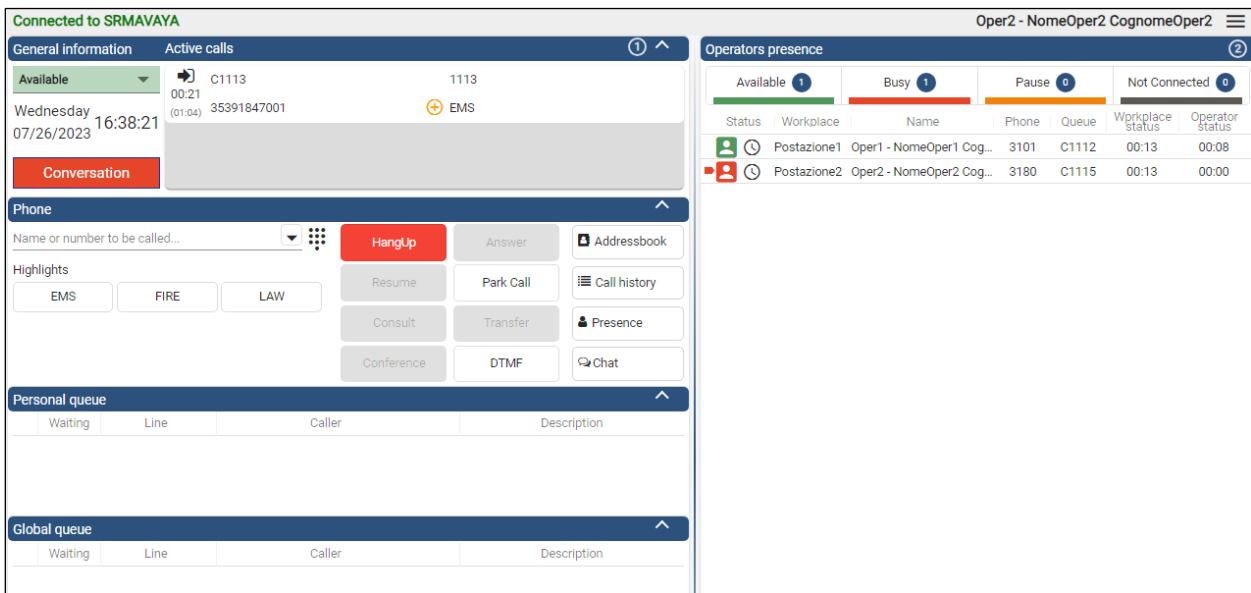
Operator2 - NomeOper2 CognomeOper2

Operators presence

Available 2 Busy 0 Pause 0 Not Connected 0

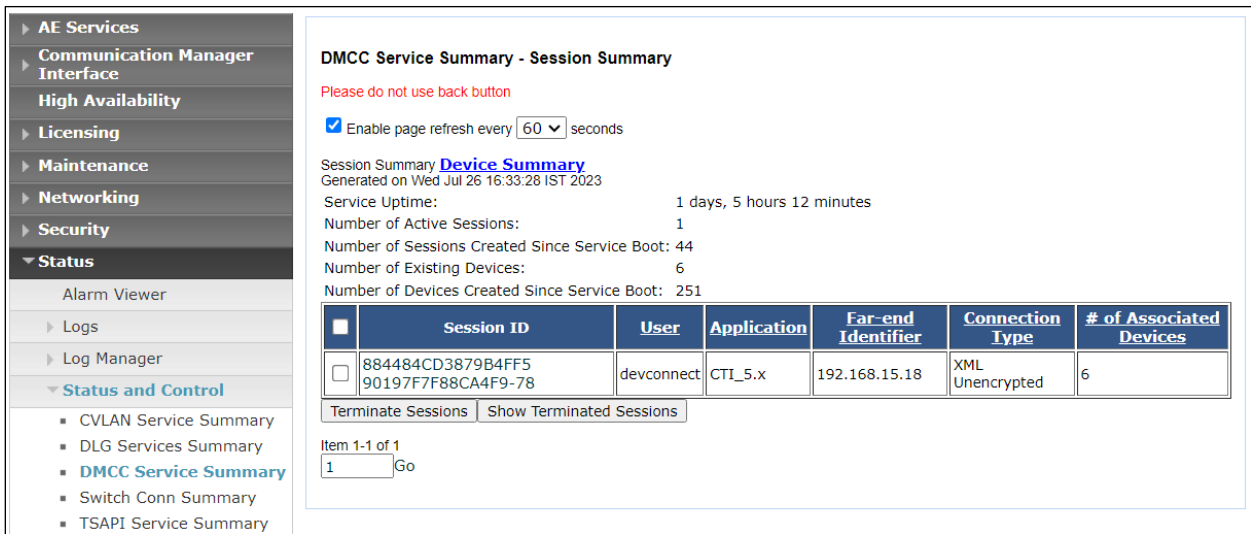
Status	Workplace	Name	Phone	Queue	Workplace status	Operator status
🕒	Postazione1	Oper1 - NomeOper1 Cog...	3101	C1112	00:13	00:07
🟢	Postazione2	Oper2 - NomeOper2 Cog...	3180	C1115	00:12	00:09

Once a call answered the caller’s information is populated at the top of the screen. The call is then controlled from the middle window located on left 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**.



9. Conclusion

These Application Notes describe the compliance testing of Beta 80 Life 1st and emma CAD CTI with Avaya Aura® Communication Manager R10.1 and Avaya Aura® Application Enablement Services R10.1. 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 10.1 Issue 6 June 2023
- [2] *Avaya Aura® Communication Manager Feature Description and Implementation*, Release 10.1 Issue 9 May 2023
- [3] *Avaya Aura® Application Enablement Services Administration and Maintenance Guide*, Release 10.1 Issue 8 May 2023
- [4] *Administering Avaya Aura® Session Manager*, Release 10.1 Issue 6 May 2023

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

©2023 Avaya LLC All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya LLC. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya LLC. 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.