



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

---

# **Application Notes for Beta80 IO and Emma CAD CTI with Avaya Aura® Communication Manager R7.0 using Avaya Aura® Application Enablement Services 7.0 – Issue 1.0**

## **Abstract**

These Application Notes describe the configuration steps required to integrate Beta80 IO and emma CAD CTI Integration with Avaya Aura® Communication Manager R7.0 using Avaya Aura® Application Enablement Services 7.0. Beta 80 IO and emma CAD CTI platform Provides a Graphical User Interface with Avaya Aura providing Public Safety Answering Points 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 any 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 to integrate Beta80 IO and emma CAD CTI Integration with Avaya Aura® Communication Manager R7.0 using Avaya Aura® Application Enablement Services 7.0. The Beta 80 IO and emma CAD CTI platform provides a Graphical User Interface with Avaya Aura® Application Enablement Services providing Public Safety Answering Points (PSAP) for emergency service calls. Beta 80 CAD platform complements Avaya Aura in providing Public Safety Answering Points (PSAP) using a complete, full featured, Computer Aided Dispatch platform; 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.

## 2. General Test Approach and Test Results

The general test approach was to configure the IO and emma CAD CTI platform to communicate with Communication manager using the Application Enablement Services Device, Media and Call Control API. This allows CAD platform to take control of Avaya Aura® Communication Manager extensions.

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 the Beta 80 CAD CTI did not include use of any specific encryption features as requested by Beta80.

## **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:

- Call queues monitoring
- CLI Import (into the CAD client)
- Dispatcher/Call Taker presence and chat service
- Make Call
- Call pick up
- Call hang up
- Call park/Resume
- Call hold/Resume
- Call Transfer (blind or with consultation)
- Conference
- Phone book /w click-to call
- DTMF relay Test Results

## **2.2. Test Results**

All test cases were passed with the following observations.

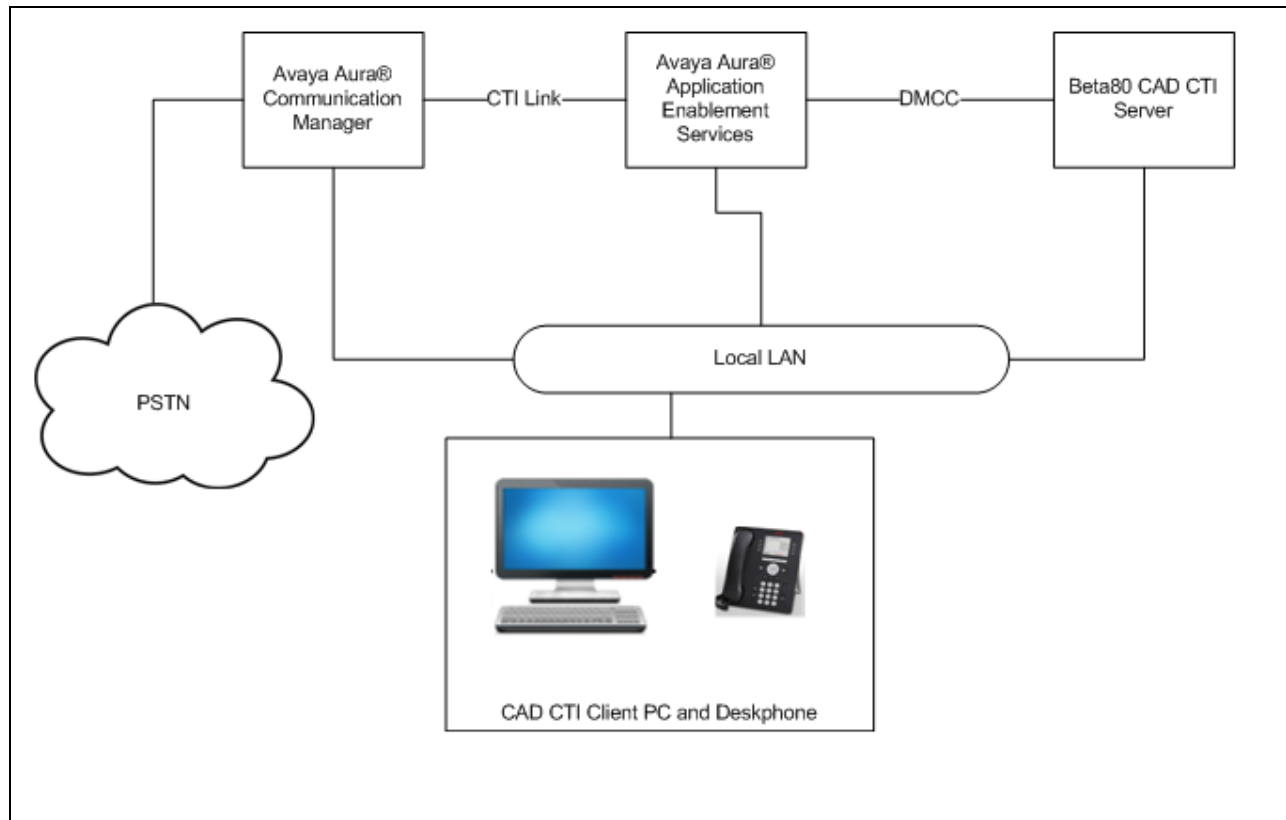
## **2.3. Support**

E-Mail: [sales@beta80group.com](mailto:sales@beta80group.com)

Internet: [www.beta80group.com](http://www.beta80group.com)

### 3. Reference Configuration

The configuration shown in Figure 1 was used during the compliance test of Beta 80 CAD CTI, with Communication Manager using Application Enablement Services. Beta 80 CAD CTI uses DMCC to control Communication Manager extensions.



**Figure 1: Beta80 CAD CTI with Application Enablement Services**

### 4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya Aura® Communication Manager running on a VMware Virtual Machine	7.0.1.2.0-FP1SP2
Avaya Aura® Application Enablement Services	7.0.1.0.4.15-0
Beta 80 EMMA/iO CAD	6.4.0.0
Beta 80 EMMA/iO CTI	4.0.0.0

## 5. Configure Avaya Aura® Communication Manager

The information provided in this section describes the configuration of Communication Manager relevant to this solution. For all other provisioning information such as initial installation and configuration, please refer to the product documentation in **Section 10**.

The configuration illustrated in this section was performed using Communication Manager System Administration Terminal (SAT).

### 5.1. Verify System Features

Use the **display system-parameters customer-options** command to verify that Communication Manager has permissions for features illustrated in these Application Notes. On **Page 3**, ensure that **Answer Supervision by Call Classifier?** is set to **y** and **Computer Telephony Adjunct Links?** is set to **y** as shown below.

display system-parameters customer-options		Page	3 of 11
OPTIONAL FEATURES			
Abbreviated Dialing Enhanced List?	y	Audible Message Waiting?	y
Access Security Gateway (ASG)?	n	Authorization Codes?	y
Analog Trunk Incoming Call ID?	y	CAS Branch?	n
A/D Grp/Sys List Dialing Start at 01?	y	CAS Main?	n
<b>Answer Supervision by Call Classifier?</b>	<b>y</b>	Change COR by FAC?	n
ARS?	y	<b>Computer Telephony Adjunct Links?</b>	<b>y</b>
ARS/AAR Partitioning?	y	Cvg Of Calls Redirected Off-net?	y
ARS/AAR Dialing without FAC?	y	DCS (Basic)?	y
ASAI Link Core Capabilities?	n	DCS Call Coverage?	y
ASAI Link Plus Capabilities?	n	DCS with Rerouting?	y
Async. Transfer Mode (ATM) PNC?	n		
Async. Transfer Mode (ATM) Trunking?	n	Digital Loss Plan Modification?	y
ATM WAN Spare Processor?	n	DS1 MSP?	y
ATMS?	y	DS1 Echo Cancellation?	y
Attendant Vectoring?	y		

## 5.2. Display Node Names for Avaya Aura® Application Enablement Services Connectivity

Display the **procr** IP Address by using the command **display node-names ip** and noting the IP address for the **procr** and AES (**Aes71678**).

display node-names ip		Page 1 of 2
IP NODE NAMES		
Name	IP Address	
SM100	10.10.40.34	
<b>Aes71678</b>	10.10.16.78	
default	0.0.0.0	
g430	10.10.40.15	
<b>procr</b>	10.10.16.27	

## 5.3. Configure AE service for Avaya Aura® Application Enablement Services Connectivity

To administer the transport link to AES use the **change ip-services** command. On **Page 1** add an entry with the following values:

- **Service Type:** should be set to **AESVCS**.
- **Enabled:** set to **y**.
- **Local Node:** set to the node name assigned for the **procr** in **Section 5.2**
- **Local Port:** retain the default value of **8765**.

change ip-services		Page 1 of 4
IP SERVICES		
Service Type	Enabled	Local Node
AESVCS	y	procr

Go to **Page 4** of the **ip-services** form and enter the following values:

- **AE Services Server:** Name obtained from the AES server, in this case **aes63vmppg**.
- **Password:** Enter a password to be administered on the AES server.
- **Enabled:** Set to **y**.

**Note:** The password entered for **Password** field must match the password on the AES server in **Section 6.2**. The **AE Services Server** should match the administered name for the AES server, that is created as part of the AES installation, and can be obtained from the AES server by typing **uname -n** at the Linux command prompt.

change ip-services		Page 4 of 4
AE Services Administration		
Server ID	AE Services Server	Password
1:	aes71678	*****
2:		
3:		

## 5.4. Configure CTI Link for TSAPI Service

Add a CTI link using the **add cti-link n** command. Enter an available extension number in the **Extension** field. Enter **ADJ-IP** in the **Type** field, and a descriptive name in the **Name** field. Default values may be used in the remaining fields.

<b>add cti-link 1</b>	Page 1 of 3
CTI Link: 1	CTI LINK
<b>Extension:</b> 2002	
<b>Type:</b> ADJ-IP	
<b>Name:</b> aes71678	COR: 1

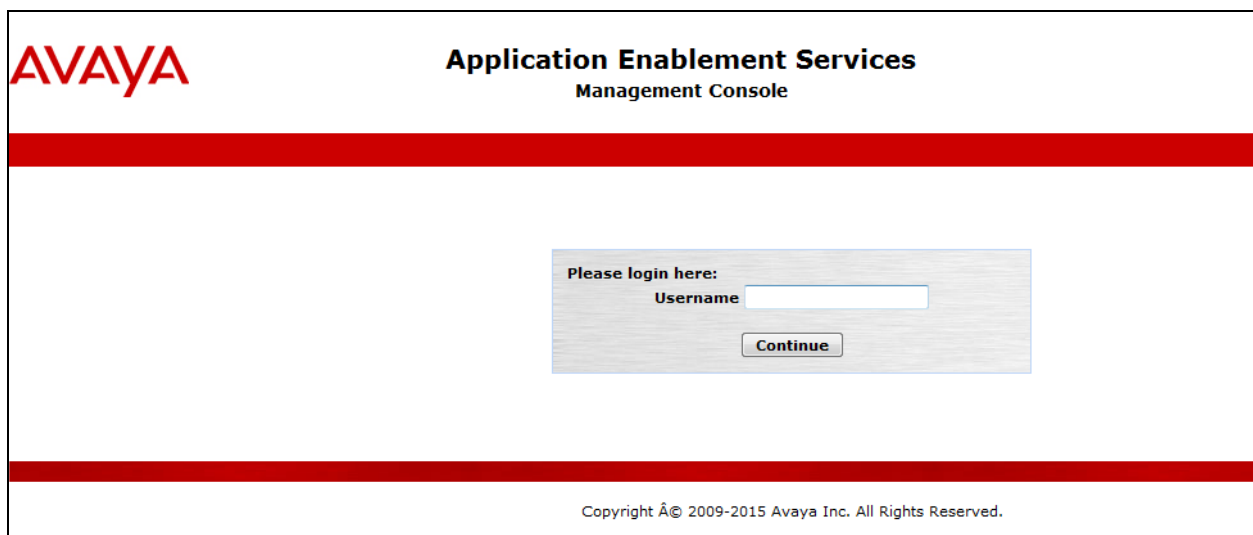
## 6. Configure Avaya Aura® Application Enablement Services

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

- Verify Licensing.
- Create Switch Connection.
- Administer TSAPI link.
- Create CTI User.
- Enable CTI Link User.
- Identify Tlinks.
- Enable DMCC ports.

### 6.1. Verify Licensing

To access the maintenance console, enter **https://<ip-addr>** as the URL in an Internet browser, where <ip-addr> is the active IP address of AES. The login screen is displayed, enter the appropriate credentials and then select the **Login** button.



The screenshot shows the Avaya Application Enablement Services Management Console login interface. At the top left is the Avaya logo. To its right, the text "Application Enablement Services" and "Management Console" is displayed. A thick red horizontal bar spans the width of the page below the header. In the center of the page is a login box with a light gray background. Inside this box, the text "Please login here:" is followed by a label "Username" and a text input field. Below the input field is a button labeled "Continue". At the bottom of the page, another thick red horizontal bar is present, and below it, the copyright notice "Copyright © 2009-2015 Avaya Inc. All Rights Reserved." is displayed.



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

The screenshot shows the 'AE Services' management console. The left sidebar contains a navigation menu with options like CVLAN, DLG, DMCC, SMS, TSAPI, TWS, Communication Manager Interface, High Availability, Licensing, Maintenance, Networking, Security, Status, User Management, and Utilities. The main content area displays the 'AE Services' status. A red warning message states: 'This AE Services server is using a default installed server certificate. Default installed certificates should not be used in a production environment. It is highly recommended to replace all default installed certificates.' Below this, an important note says: 'IMPORTANT: AE Services must be restarted for administrative changes to fully take effect. Changes to the Security Database do not require a restart.' A table lists the services and their status:

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, a note says: 'For status on actual services, please use [Status and Control](#)'. A footnote at the bottom states: '\* -- For more detail, please mouse over the Cause, you'll see the tooltip, or go to help page.'

## 6.2. Create Switch Connection

From the AES Management Console navigate to **Communication Manager Interface** → **Switch Connections** to set up a switch connection. Enter in a name for the Switch Connection to be added and click the **Add Connection** button.

The screenshot shows the 'Switch Connections' page within the 'Communication Manager Interface'. The left sidebar has a navigation menu with options like AE Services, Communication Manager Interface, Switch Connections, and Dial Plan. The main content area has a title 'Switch Connections' and a form with a text input field containing 'CM1627' and an 'Add Connection' button. Below the form is a table with two columns: 'Connection Name' and 'Processor Ethernet'.

Connection Name	Processor Ethernet
CM1627	

In the resulting screen enter the **Switch Password**, the Switch Password must be the same as that entered into Communication Manager AE Services Administration screen via the **change ip-services** command, described in **Section 5.3** Default values may be accepted for the remaining fields. Click **Apply** to save changes.

**Connection Details - CM1627**

Switch Password: [Masked]

Confirm Switch Password: [Masked]

Msg Period: 30 Minutes (1 - 72)

Provide AE Services certificate to switch: ☒

Secure H323 Connection: ☐

Processor Ethernet: ☒

Apply Cancel

From the **Switch Connections** screen, select the radio button for the recently added switch connection and select the **Edit CLAN IPs** button (not shown). In the resulting screen, enter the IP address of the **procr** as shown in **Section 5.2** that will be used for the AES connection and select the **Add/Edit Name or IP** button.

**Edit Processor Ethernet IP - CM1627**

10.10.16.27 Add/Edit Name or IP

Name or IP Address
--------------------

Back

### 6.3. Administer TSAPI link

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

The screenshot shows the 'AE Services' sidebar on the left with 'TSAPI' selected. The main panel is titled 'TSAPI Links' and contains a table with two columns: 'Link' and 'Switch Connection'. Below the table are three buttons: 'Add Link', 'Edit Link', and 'Delete Link'.

On the **Add TSAPI Links** screen, enter the following values:

- **Link:** Use the drop-down list to select an unused link number.
- **Switch Connection:** Choose the switch connection **CM1627**, which has already been configured in **Section 6.2**, from the drop-down list.
- **Switch CTI Link Number:** Corresponding CTI link number configured in **Section 5.4** which is **1**.
- **ASAI Link Version:** This can be left at the default value of **7**.
- **Security:** select **Both** from the drop down.

Once completed, select **Apply Changes**.

The screenshot shows the 'Edit TSAPI Links' screen. The sidebar on the left shows 'TSAPI Links' selected under 'TSAPI'. The main panel has the following fields and values: 'Link' is 1, 'Switch Connection' is CM1627, 'Switch CTI Link Number' is 1, 'ASAI Link Version' is 7, and 'Security' is Both. At the bottom are three buttons: 'Apply Changes', 'Cancel Changes', and 'Advanced Settings'.

Another screen appears for confirmation of the changes. Choose **Apply** (not shown).

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**.

The screenshot shows the 'Service Controller' management console. On the left is a navigation menu with the following items: 'AE Services', 'Communication Manager Interface', 'High Availability', 'Licensing', 'Maintenance' (expanded), 'Date Time/NTP Server', 'Security Database', 'Service Controller' (highlighted in blue), 'Server Data', 'Networking', and 'Security'. The main panel is titled 'Service Controller' and contains a table with two columns: 'Service' and 'Controller Status'. The table lists six services: ASAI Link Manager, DMCC Service, CVLAN Service, DLG Service, Transport Layer Service, and TSAPI Service. Each service has a checkbox to its left. The checkboxes for ASAI Link Manager, DMCC Service, CVLAN Service, DLG Service, and Transport Layer Service are unchecked. The checkbox for TSAPI Service is checked. All services are listed with a status of 'Running'. Below the table, there is a text prompt: 'For status on actual services, please use [Status and Control](#)'. At the bottom of the panel are four buttons: 'Start', 'Stop', 'Restart Service', and 'Restart AE Server'.

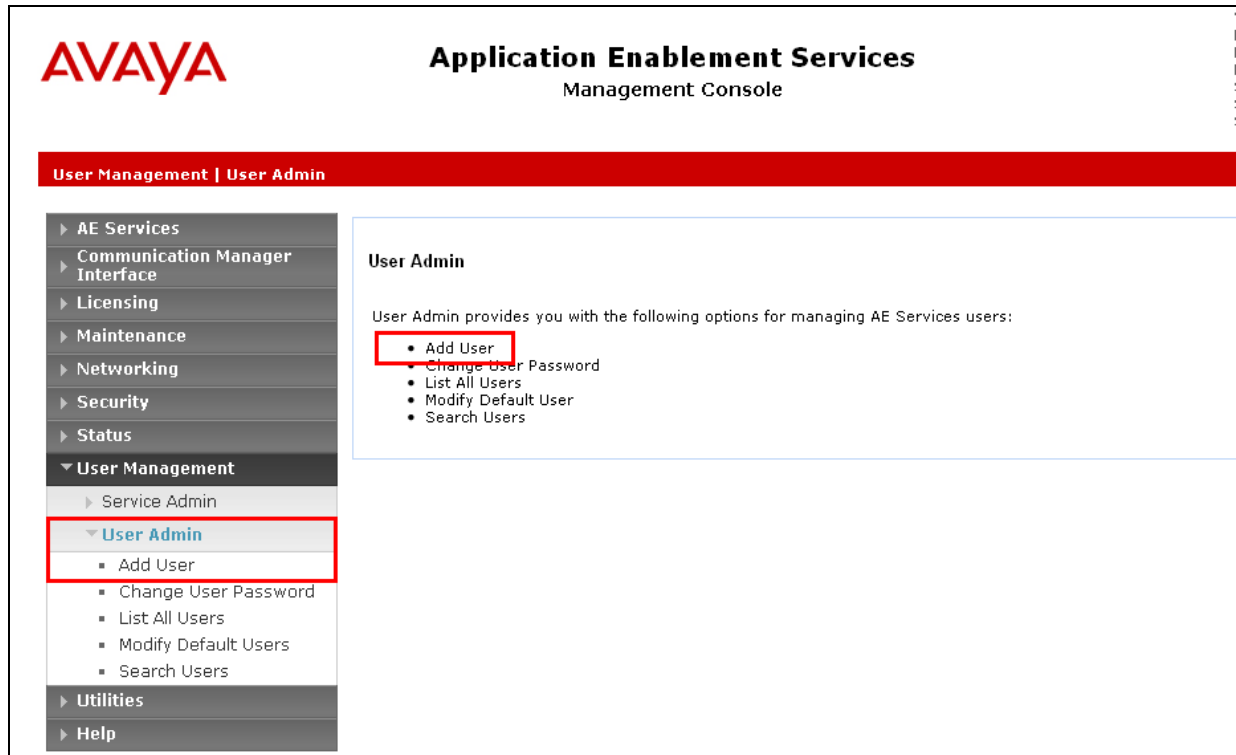
Service	Controller Status
<input type="checkbox"/> ASAI Link Manager	Running
<input type="checkbox"/> DMCC Service	Running
<input type="checkbox"/> CVLAN Service	Running
<input type="checkbox"/> DLG Service	Running
<input type="checkbox"/> Transport Layer Service	Running
<input checked="" type="checkbox"/>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

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

Start Stop Restart Service Restart AE Server

## 6.4. Create Avaya CTI User

A User ID and password needs to be configured for the Beta80 CAD CTI to communicate as a TSAPI client with the Application Enablement Services server. Navigate to the **User Management** → **User Admin** screen then choose the **Add User** option.



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

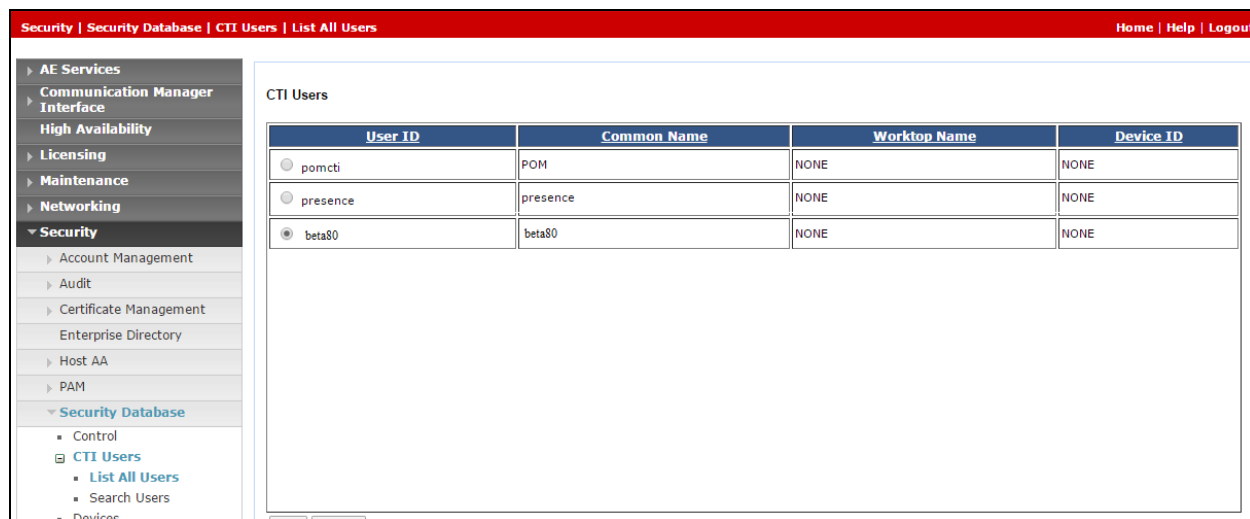
- **User Id** - This will be used by the CAD CTI Server to connect.
- **Common Name** and **Surname** - Descriptive names need to be entered.
- **User Password** and **Confirm Password** - This will be used with the **User Id** to connect.
- **CT User** - Select **Yes** from the drop-down menu.

The screenshot shows the 'Add User' screen within a web application. The top navigation bar is red and contains the text 'User Management | User Admin | Add User' on the left and 'Home | Help | Logout' on the right. A left-hand sidebar menu lists various categories: 'AE Services', 'Communication Manager Interface', 'High Availability', 'Licensing', 'Maintenance', 'Networking', 'Security', 'Status', 'User Management' (expanded), 'Service Admin', and 'User Admin' (expanded). Under 'User Admin', the options are 'Add User' (highlighted), 'Change User Password', and 'List All Users'. The main content area is titled 'Add User' and includes a note: 'Fields marked with \* can not be empty.' Below this, there are several input fields: '\* User Id' (containing 'beta80'), '\* Common Name' (containing 'beta80'), '\* Surname' (containing 'CAD CTI'), '\* User Password' (containing '\*\*\*\*\*'), '\* Confirm Password' (containing '\*\*\*\*\*'), 'Admin Note' (empty), 'Avaya Role' (a dropdown menu showing 'None'), 'Business Category' (empty), 'Car License' (empty), 'CM Home' (empty), 'Css Home' (empty), and 'CT User' (a dropdown menu showing 'Yes').

Complete the process by choosing **Apply** at the bottom of the screen (not shown). The next screen will show a message indicating that the user was created successfully (not shown).

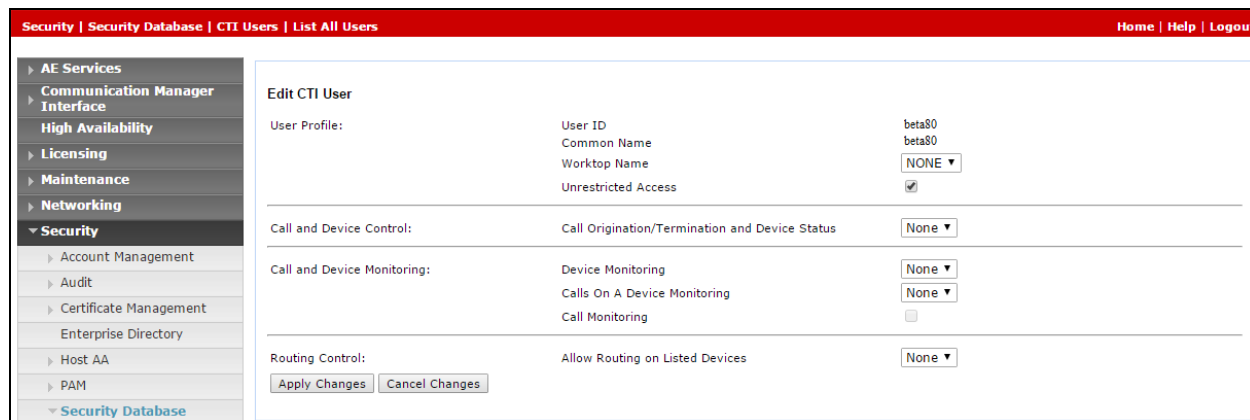
## 6.5. Enable Unrestricted Access for CTI User

Navigate to the **CTI Users** screen by selecting **Security** → **Security Database** → **CTI Users** → **List All Users**. Select the user that was created in **Section 6.4** and select the **Edit** option (not shown).



User ID	Common Name	Worktop Name	Device ID
<input type="radio"/> pomcti	POM	NONE	NONE
<input type="radio"/> presence	presence	NONE	NONE
<input checked="" type="radio"/> beta80	beta80	NONE	NONE

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



Edit CTI User		
User Profile:	User ID	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"/>		

A screen (not shown) appears to confirm applied changes to CTI User, choose **Apply**. This CTI user should now be enabled.

## 6.6. Enable DMCC ports

In order to enable DMCC for call recording navigate to **Networking → Ports → DMCC Server Ports**.

- Enable DMCC **Unencrypted Port**
- Enable DMCC **Encrypted Port**
- Enable DMCC **TR/87 Port**

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

**Networking | Ports**

**Ports**

CVLAN Ports

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

DLG Port

TCP Port	
5678	

TSAPI Ports

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

**DMCC Server Ports**

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



Once this change is made a restart of the AE Server is required. Navigate to **Maintenance** → **Service Controller**. In the main screen select **Restart AE Server** highlighted.

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

**Maintenance | Service Controller**

Left Sidebar:

- ▶ AE Services
- ▶ Communication Manager Interface
- ▶ 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 type="checkbox"/> TSAPI Service	Running

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

Buttons: Start Stop Restart Service **Restart AE Server** Restart Linux Restart Web Server

## 7. Configure Beta 80 CAD CTI

This section describes the steps required for Beta80 CAD CTI to interoperate with Application Enablement Services. In order to correctly establish the CTI link between emma / iO CAD and Aura “PABXConverter.exe.config” file has to be accessed and the following configuration steps have to be carried out:

- AES IP address and port configuration
- DMCC login parameters configuration
- CM IP address configuration

These steps are displayed in the following picture:

```
<configuration>
  <appSettings>
    <add key="PBXIP" value="192.168.15.101"/>
    <add key="PBXPort" value="4721"/>

    <add key="PBXLoginName" value="CTI01"/>
    <add key="PBXLoginPassword" value="CTI01"/>

    <add key="CMSwitchName" value="CM"/>
    <add key="CMSwitchAddressIp" value="192.168.15.22"/>
```

“PABXConverter.exe.config” file is normally stored in the “PABXConverter” folder.

emma/iO 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:

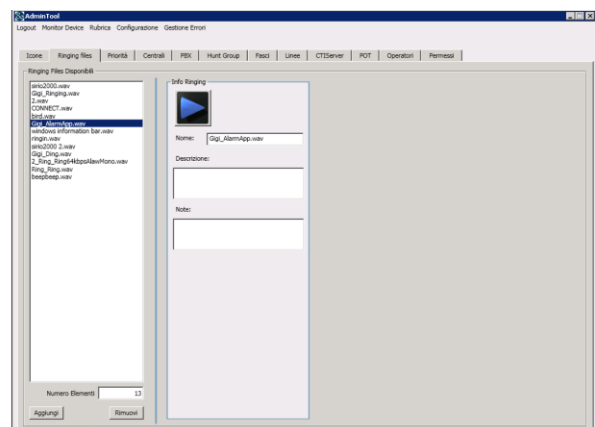
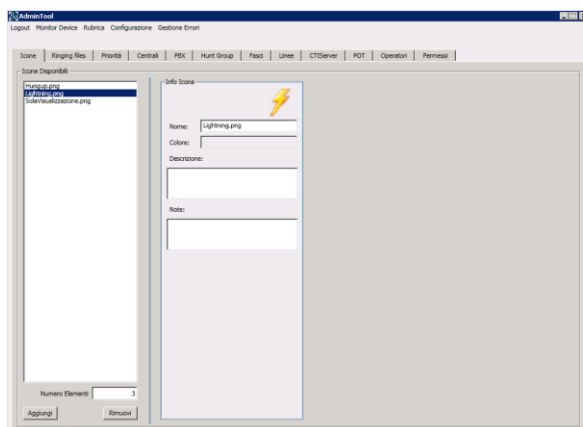
- icons
- ringing tones
- calls priority
- queues
- positions
- agents

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 icons and ringing tones

PSAP admins can apply specific icons and ringing tones to different queues; the configuration is performed via the relevant tab of emma / iO CTI admin interface



## 7.2. Configuration of call priorities

Different priority levels can be created according to PSAP operating procedures and business rules

The screenshot shows the 'AdminTool' application window. The title bar includes 'Logout', 'Monitor Device', 'Rubrica', 'Configurazione', and 'Gestione Errori'. The main menu bar contains 'Icone', 'Ringing files', 'Priorità', 'Centrali', 'PBX', 'Hunt Group', 'Fasci', 'Linee', 'CTIServer', 'POT', 'Operatori', and 'Permessi'. The 'Priorità' tab is active, displaying a list of available priorities on the left and a detailed configuration form on the right. The list on the left includes 'Very High - Urgent', 'Low', 'Very Low', 'Medium', and 'High'. The configuration form on the right has fields for 'Codice' (set to 3), 'Descrizione' (set to Medium), and 'Note'. At the bottom left, there is a 'Numero Elementi' field set to 5 and buttons for 'Aggiungi', 'Modifica', and 'Rimuovi'.

Priorità Disponibili
Very High - Urgent
Low
Very Low
Medium
High

Info Priorità
Codice: 3
Descrizione: Medium
Note:

Numero Elementi: 5

Aggiungi Modifica Rimuovi

### 7.3. Queues configuration

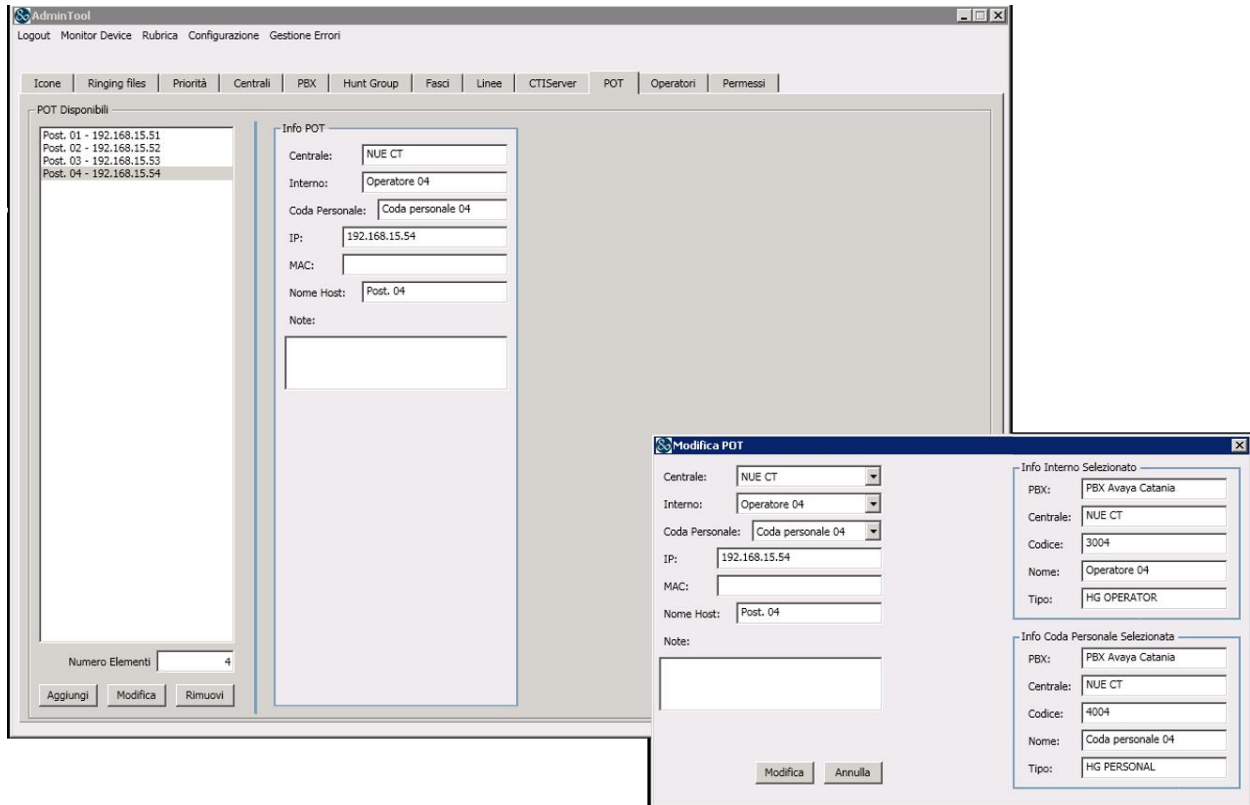
PSAP queues and agents' personal queues are configured as follows:

The screenshot displays the AdminTool application window. The top menu bar includes 'Logout', 'Monitor Device', 'Rubrica', 'Configurazione', and 'Gestione Errori'. Below this is a navigation bar with tabs: 'Icone', 'Ringing files', 'Priorità', 'Centrali', 'PBX', 'Hunt Group', 'Fasci', 'Linee', 'CTIServer', 'POT', 'Operatori', and 'Permessi'. The 'Hunt Group' tab is selected. The main area is divided into two panes. The left pane, titled 'Hunt Group Disponibili', contains a list of available hunt groups, including '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', and 'Operatore 02'. The right pane, titled 'Info Hunt Group', contains a form for configuring a selected hunt group. The form includes fields for 'PBX' (set to 'PBX Avaya Catania'), 'Codice' (set to '1112'), 'Nome' (set to '112'), 'Tipo' (set to 'HG'), 'Priorità' (set to 'Very High - Urgent'), 'Centrale' (set to 'NUE CT'), 'Public Code' (set to '1112'), 'Codice HG Supplier' (set to '1112'), 'HG Prompt' (empty), 'HG Prompt Timeout' (empty), 'Descrizione' (set to 'Coda di Centrale x 112'), and 'Note' (empty). At the bottom of the left pane, there is a 'Numero Elementi' field showing '33' and three buttons: 'Aggiungi', 'Modifica', and 'Rimuovi'.

Each queue is associated with the priority and the monitored VDN or device Configured on Communication Manager.

## 7.4. Positions configuration

The following picture presents how to configure PSAP positions within the CTI admin tool; this configuration also includes the definition of the agent's personal queue.



## 7.5. Phone bar users definition

Each agent is registered in the system as a named user.

The screenshot displays the 'Admin Tool' interface with the 'Operatori Disponibili' list on the left and the 'Modifica Operatore' dialog box open on the right. The 'Operatori Disponibili' list contains the following entries:

- NOTAR - Notargiacomo Cristiano
- beta80 - beta80cognome beta80nome
- OperM12 - CognomeOperM12 NomeOperM12
- OperM16 - CognomeOperM16 NomeOperM16
- SEN - Tamburilla Semi
- OperM18 - CognomeOperM18 NomeOperM18
- OperM13 - CognomeOperM13 NomeOperM13
- alpi's username - alpi's surname alpi's
- Administrator - Cognome Administrator
- OperM11 - CognomeOperM11 NomeOperM11
- ANDREA - Rosini Andrea
- OperM15 - CognomeOperM15 NomeOperM15
- TUARI - Tinsacco Ivan
- PARADISO - Paradiso Carlo

The 'Modifica Operatore' dialog box shows the following fields:

- Centrale: NUJE CT
- Contesto: 2
- Gruppo: 1025
- User: 2057
- Username: OperM14
- Nome: NomeOperM14
- Cognome: CognomeOperM14
- Interno: [Redacted]
- Nota: [Redacted]

The 'Info Interno Selezionato' section shows:

- PEX: [Redacted]
- Centrale: [Redacted]
- Codice: [Redacted]
- Nome: [Redacted]
- Tipo: [Redacted]

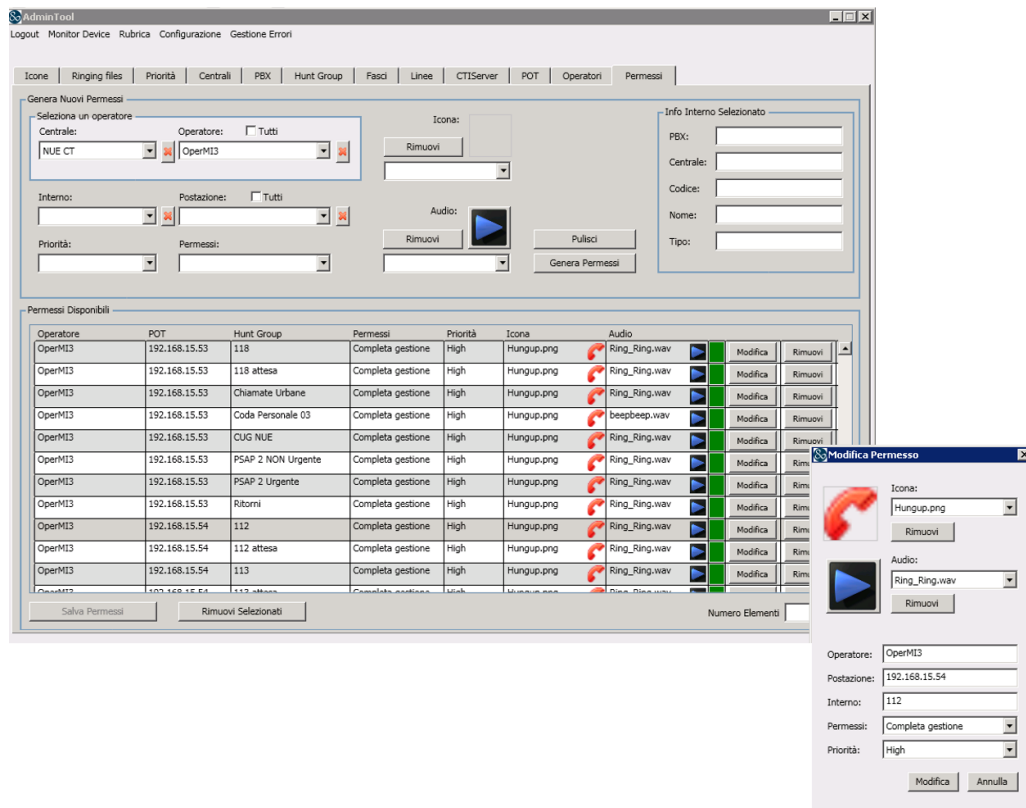
The 'Info Codice Personale Selezionato' section shows:

- PEX: [Redacted]
- Centrale: [Redacted]
- Codice: [Redacted]
- Nome: [Redacted]
- Tipo: [Redacted]

Buttons at the bottom of the dialog include 'Modifica' and 'Annulla'.

## 7.6. Agents profiling

Each agent is assigned permissions and grants according to the PSAP business rules; permissions and grants can be configured on a per named user basis or given a named user which position is logging in (e.g. an agent inherits a certain set of permissions if they log into position n.1 and another set of permissions if they log into position n.5).



Any of the previously parameters can be applied to each agent or agent/position couple, e.g. queues they are entitled to monitor, queue priorities, ring tones



## 8. Verification Steps

This section provides the tests that can be performed to verify correct configuration of the Avaya and the Beta80 CAD CTI solution.

### 8.1. Verify Avaya Aura® Communication Manager CTI Service State

The following steps can validate that the communication between Communication Manager and AES is functioning correctly. Check the AESVCS link status with AES by using the command **status aesvcs cti-link**. Verify the **Service State** of the CTI link is **established**.

status aesvcs cti-link						
AE SERVICES CTI LINK STATUS						
CTI Link	Version	Mnt Busy	AE Services Server	Service State	Msgs Sent	Msgs Rcvd
1	4	no	aes71678	established	18	18

### 8.2. Verify TSAPI Link and DMCC

This section will verify both the TAPI and DMCC links between the AES and Communication Manager.

#### 8.2.1. Verify TSAPI Link

On the AES Management Console verify the status of the TSAPI link by selecting **Status** → **Status and Control** → **TSAPI Service Summary** to display the **TSAPI Link Details** screen. Verify the status of the TSAPI link by checking that the **Status** is **Talking** and the **State** is **Online**.

AE Services

Communication Manager Interface

High Availability

Licensing

Maintenance

Networking

Security

Status

Alarm Viewer

Log Manager

Logs

Status and Control

CVLAN Service Summary

DLG Services Summary

DMCC Service Summary

Switch Conn Summary

TSAPI Service Summary

TSAPI Link Details

☐ Enable page refresh every 60 seconds

Link	Switch Name	Switch CTI Link ID	Status	Since	State	Switch Version	Associations	Msgs to Switch	Msgs from Switch	Msgs Period
1	CM1627	1	Talking	Tue Jul 26 10:03:32 2016	Online	17	9	15	15	30

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

### 8.2.2. Verify Avaya Aura® Application Enablement Services DMCC Service

The following steps are carried out on AES to validate that the communication link between AES and the CCP server is functioning correctly. Verify the status of the DMCC service by selecting **Status → Status and Control → DMCC Service Summary**. The **DMCC Service Summary – Session Summary** screen is displayed as shown below. It shows a connection to the CCP server, IP address **10.10.16.95**. The **Application** is shown as **cmapiApplication**, and the **Far-end Identifier** is given as the IP address **10.10.16.95** as expected.

AE Services

Communication Manager Interface

High Availability

Licensing

Maintenance

Networking

Security

Status

Alarm Viewer

Log Manager

Logs

Status and Control

CVLAN Service Summary

DLG Services Summary

DMCC Service Summary

DMCC Service Summary - Session Summary

Please do not use back button

☐ Enable page refresh every 60 seconds

Session Summary [Device Summary](#)

Generated on Thu Jul 28 08:13:30 IST 2016

Service Uptime: 1 days, 22 hours 9 minutes

Number of Active Sessions: 1

Number of Sessions Created Since Service Boot: 4

Number of Existing Devices: 6

Number of Devices Created Since Service Boot: 18

	Session ID	User	Application	Far-end Identifier	Connection Type	# of Associated Devices
<input type="checkbox"/>	55BB86290F3297363 1BAEC2FCC9517F9-3		cmapiApplication	10.10.16.95	XML Unencrypted	6

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

Item 1-1 of 1  
1 Go

### 8.3. Verify Beta 80 CAD CTI

The following shows that the CAD CTI Client is logged in and a call has been made and answered showing that the agent is **In Conversation**.

Phone Station Operator - V. 4.0.0.0

System state and Info

Cristiano Notargiacomo

Telephone : 3004

Queue : 4004

Workplace : Post. 04

Address : 192.168.15.54

**In Conversation**

14:31:38

06/12/2017

Active Calls

Number	Description
From: 03922579528	Beta80 Resources
To: 1118	118

Phone Operations

Short text messages

[ Isola Call Taking ]

List of calls in parking queue

Waiting time	Source	Description	Trunk
00:02:14	0225202		118

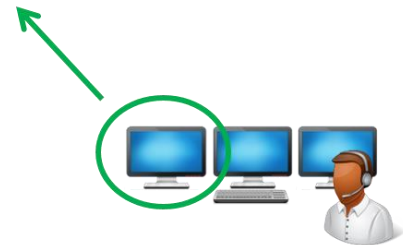
List of calls in personal queue

Waiting time	Source	Description	Trunk
00:02:38	3003	Andrea Rossini	

List of calls in central queue

Waiting time	Trunk	Source	Description
00:02:15	118	0225202	

Connected To Centrale Catania 192.168.15.18



## 9. Conclusion

These Application Notes describe the configuration steps required for Beta80 CAD CTI to successfully interoperate with Avaya Aura® Communication Manager R7.0 using Avaya Aura® Application Enablement Services R7.0. All feature functionality and serviceability test cases were completed successfully as outlined in **Section 2.2**.

## 10. Additional References

This section references the Avaya and Beta80 product documentation that are relevant to these Application Notes.

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

[1] *Administering Avaya Aura® Communication Manager*, Document ID 03-300509

[2] *Avaya Aura® Communication Manager Feature Description and Implementation*, Document ID 555-245-205

*Avaya Aura® Application Enablement Services Administration and Maintenance Guide Release 7.0*

Product documentation for Beta80 can be obtained as follows:

- Email: [sales@beta80group.com](mailto:sales@beta80group.com)
- Website: [www.beta80group.com](http://www.beta80group.com)

---

**©2017 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).