



Avaya Solution & Interoperability Test Lab

Application Notes for trinityRESPOND Emergency Response Management Solution 4.0 with Avaya Aura® Communication Manager 8.1 and Avaya Aura® Application Enablement Services 8.1 – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for trinityRESPOND – Emergency Response Management Solution to interoperate with Avaya Aura® Communication Manager 8.1 and Avaya Aura® Application Enablement Services 8.1.

The compliance testing focused on the voice integration with Avaya Aura® Communication Manager via the Avaya Aura® Application Enablement Services Telephony Application Programming Interface.

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.

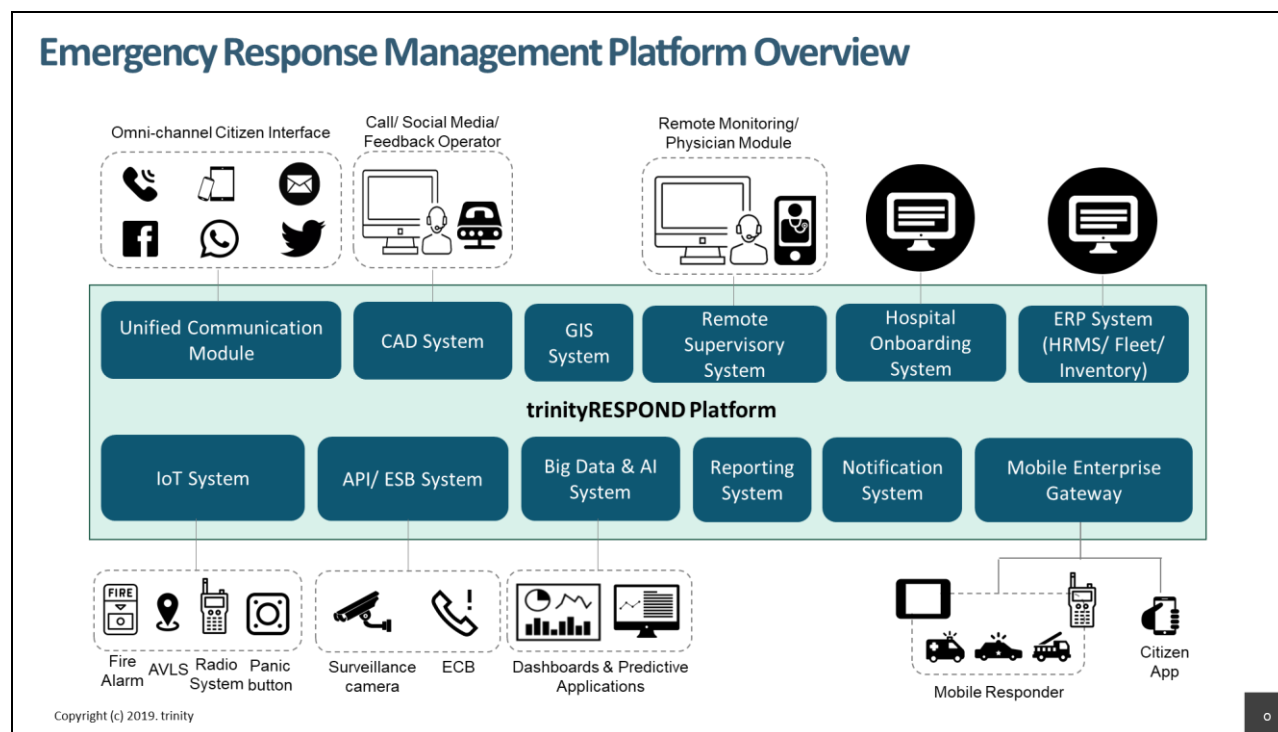
1. Introduction

These Application Notes describe the configuration steps required for trinityRESPOND – Emergency Response Management Solution to interoperate with Avaya Aura® Communication Manager 8.1 using Avaya Aura® Application Enablement Services 8.1.

trinityRESPOND - Emergency Response Management Solution has an intelligent computer aided dispatch application where in a CTI Integration with Avaya Aura® Communication Manager is established using Avaya Aura® Application Enablement Services.

The Computer Aided Dispatch (CAD) application together with Avaya Aura® will enable Public Safety Answering Points (PSAP). CAD application helps the PSAP professionals to streamline emergency calls processing by automatically retrieving and displaying the caller information such as number, address and other details. It also suggests the standard operating procedures for the call takers and dispatchers to follow based on the call for service (CFS) request. The dispatcher can monitor the dispatched units and provide necessary information for the field responders to ensure quick and effective engagement upon the creation of new incidents.

The Computer Aided Dispatch (CAD) CTI Platform will communicate with Communication Manager using the Application Enablement Services Java Telephony API (JTAPI) allowing the CAD platform to take control of Communication Manager extensions.



2. General Test Approach and Test Results

The general test approach was to validate successful handling of inbound calls using trinityRESPOND - Emergency Response Management Solution. This was performed by calling inbound and/or outbound from the elite call center using Computer Aided Dispatch (CAD) application to answer calls. Where applicable, agent actions were performed using the trinityRESPOND – Call Taker.

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 trinityRESPOND - Emergency Response Management Solution used TLS.

2.1. Interoperability Compliance Testing

The testing focused on the following areas:

- **Change Agent state** – Login, Ready, AUX, Operator using CAD Call Taker.
- **Inbound Calls** – Answer calls using CAD Call Taker.
- **Outbound Calls** – Make calls using CAD Call Taker.
- **Hold/Transfer** – Place callers on hold and transfer using CAD Call Taker.
- **Conference** – Make Conference using CAD Call Taker.
- **Serviceability** - Verify the ability of CAD to recover from disconnection and reconnection to the Avaya solution.

2.2. Test Results

All test cases were executed. The following observation was noted during the compliance testing.

- CAD Call Taker software required select extension number to execute Hold/Resume.

2.3. Support

Technical support can be obtained for the trinityRESPOND - Emergency Response Management Solution as follows:

- Email: helpdesk@trinitymobility.com
- Website: <https://www.trinitymobility.com/>
- Phone: +91 08042060604

3. Reference Configuration

The configuration used for the compliance testing is shown in **Figure 1**. The detailed administration of basic connectivity between Communication Manager and Application Enablement Services.

The devices used in the compliance testing are shown in the table below.

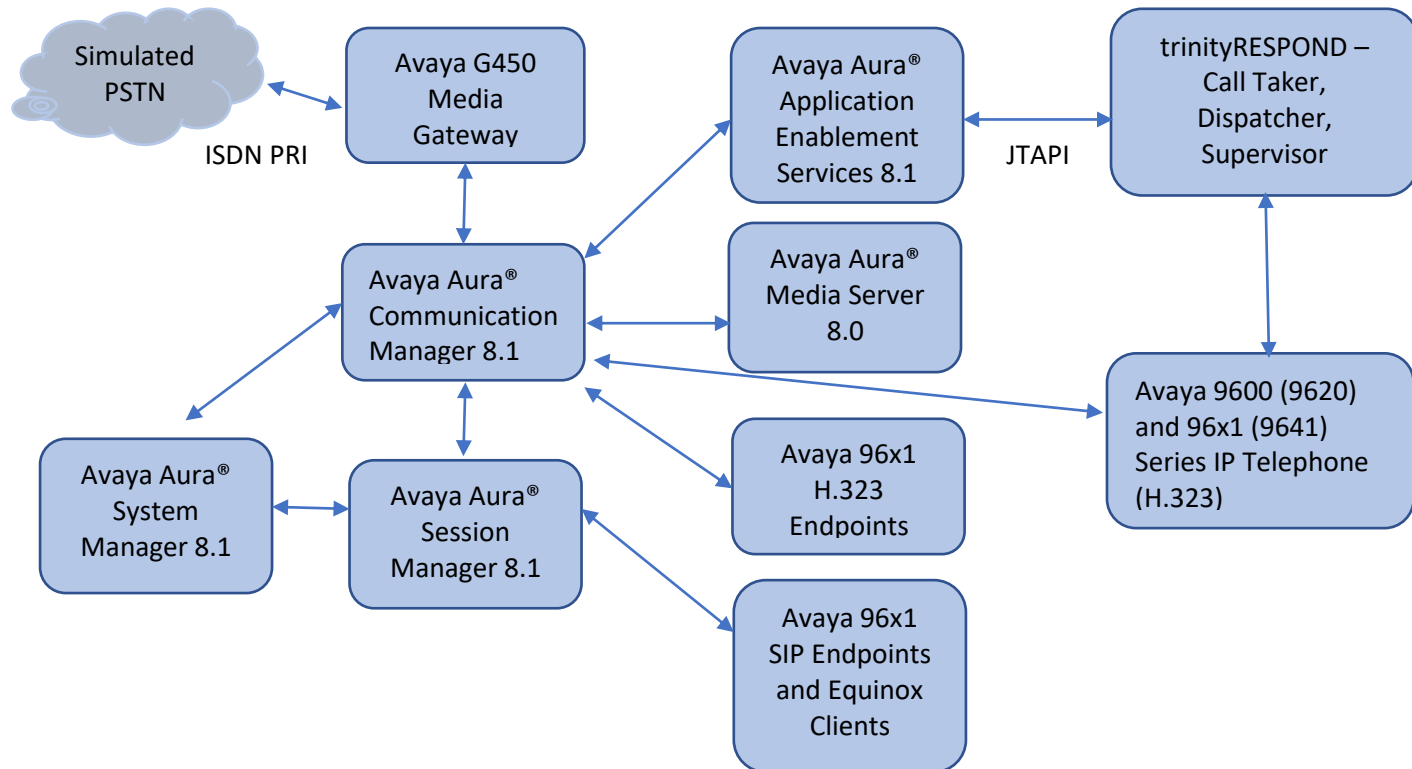


Figure 1: Compliance Testing Configuration

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 in Virtual Environment	8.1.0.1.0-SP1
Avaya G450 Media Gateway	41.9.0
Avaya Aura® Media Server in Virtual Environment	8.0 SP2
Avaya Aura® Application Enablement Services in Virtual Environment	8.1.0.0.9-1
Avaya 9620L IP Deskphone (H.323)	3.2.8A
Avaya 9608G & 9641G IP Deskphone (H.323)	6.8
Avaya 9641G IP Deskphone (SIP)	7.1.6
Avaya One-X® Communicator on Desktop PC	6.2.12.22
trinityRESPOND – Call Taker	V4.0
trinityRESPOND – Dispatcher	V4.0
trinityRESPOND - Supervisor	V4.0

5. Configure Avaya Aura® Communication Manager

This section provides the procedures for configuring Communication Manager. The procedures include the following areas:

- Verify license
- Administer CTI link
- Administer Hunt Group and Agent

5.1. Verify License

Log into the System Access Terminal to verify that the Communication Manager license has proper permissions for features illustrated in these Application Notes. Use the “display system-parameters customer-options” command to verify that the **Computer Telephony Adjunct Links** customer option is set to “y” on **Page 4**. If this option is not set to “y”, then contact the Avaya sales team or business partner for a proper license file.

display system-parameters customer-options		Page	4 of 12
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
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		
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		
(NOTE: You must logoff & login to effect the permission changes.)			

5.2. Administer CTI Link

Add a CTI link using the **add cti-link n** command, where **n** is an available CTI link number. Enter an available extension number in the **Extension** field. Note that the CTI link number and extension number may vary. 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: 79999		
Type: ADJ-IP		
COR: 1		
Name: aes8		

5.3. Administer Hunt Group and Agent

This section shows the steps required to add a new service or skill on Communication Manager. Services are accessed by calling a Hunt Group associated with agents. . The following sections give step by step instructions on how to add the following.

- Hunt Group
- Agent

5.3.1. Add Hunt Group

To add a new skillset or hunt group type, **add hunt-group x**, where **x** is the new hunt group number. For example, hunt group **100** is added for the **Voice Service** queue. Ensure that **ACD**, **Queue** and **Vector** are all set to **y**. Also, that **Group Type** is set to **ucd-mia**.

add hunt-group 2		Page 1 of 4
HUNT GROUP		
Group Number: 2		ACD? y
Group Name: Voice Service		Queue? y
Group Extension: 88100		Vector? y
Group Type: ucd-mia		
TN: 1		
COR: 1		
Security Code:		MM Early Answer? n
ISDN/SIP Caller Display:		Local Agent Preference? n
Queue Limit: unlimited		
Calls Warning Threshold:		Port:
Time Warning Threshold:		Port:

On **Page 2** ensure that **Skill** is set to **y** as shown below.

add hunt-group 2	HUNT GROUP	Page 2 of 4
Skill? y	Expected Call Handling Time (sec): 180	
AAS? n		
Measured: none		
Supervisor Extension:		
Controlling Adjunct:		
Multiple Call Handling: none		
Timed ACW Interval (sec):	After Xfer or Held Call Drops? n	

5.3.2. Add Agent

To add a new agent, type **add agent-loginID x**, where x is the login id for the new agent.

add agent-loginID 80000	AGENT LOGINID	Page 1 of 3
Login ID: 80000	AAS? n	
Name: Voice Agent	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	
	AUDIX Name for Messaging:	
	LoginID for ISDN/SIP Display? n	
	Password:	
	Password (enter again):	
	Auto Answer: station	
	MIA Across Skills: system	
	ACW Agent Considered Idle: 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**, add the required skills. Note that the skill **2** is added to this agent so when a call for **Voice Service** is initiated, the call is routed correctly to this agent.

add agent-loginID 80000												Page 2 of 3		
AGENT LOGINID														
Direct Agent Skill:												Service Objective? n		
Call Handling Preference: skill-level												Local Call Preference? n		
SN	RL	SL	SN	RL	SL	SN	RL	SL	SN	RL	SL			
1: 2		1	16:			31:			46:					
2:			17:			32:			47:					
3:			18:			33:			48:					
4:			19:			34:			49:					
5:			20:			35:			50:					
6:			21:			36:			51:					
7:			22:			37:			52:					
8:			23:			38:			53:					
9:			24:			39:			54:					
10:			25:			40:			55:					
11:			26:			41:			56:					
12:			27:			42:			57:					
13:			28:			43:			58:					
14:			29:			44:			59:					
15:			30:			45:			60:					

6. Configure Avaya Aura® Application Enablement Services

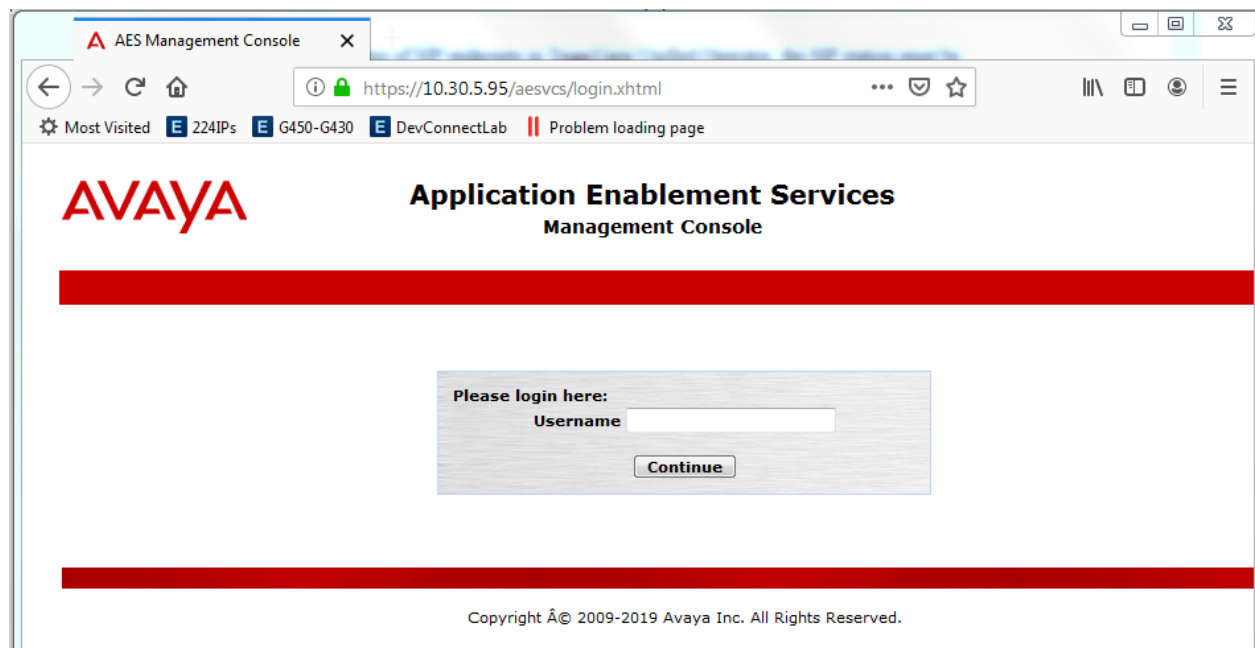
This section provides the procedures for configuring Application Enablement Services. It is assumed that configuration steps for Switch Connection to Communication Manager and H323 Gatekeeper have been performed. The procedures include the following areas:

- Launch OAM interface
- Verify License
- Administer TSAPI link
- Administer Trinity User
- Restart Services
- Obtain Tlink name


6.1. Launch OAM Interface

Access the OAM web-based interface by using the URL “https://ip-address” in an Internet browser window, where **ip-address** is the IP address of the Application Enablement Services server.

The **Please login here** screen is displayed. Log in using the appropriate credentials.



The **Welcome to OAM** screen is displayed next.

 **Application Enablement Services**
Management Console

Welcome: User cust
Last login: Thu Aug 15 15:41:45 2019 from 10.128.224.59
Number of prior failed login attempts: 0
HostName/IP: aes95/10.30.5.95
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.1.0.0.0.9-1
Server Date and Time: Fri Aug 16 13:19:44 IST 2019
HA Status: Not Configured

Home

Home | Help | Logout

- ▶ AE Services
- ▶ Communication Manager Interface
- ▶ High Availability
- ▶ Licensing
- ▶ Maintenance
- ▶ Networking
- ▶ Security
- ▶ Status
- ▶ User Management
- ▶ Utilities
- ▶ Help

Welcome to OAM

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.

The AE Services Operations, Administration, and Management (OAM) Web provides you with tools for managing the AE Server. OAM spans the following administrative domains:


- AE Services - Use AE Services to manage all AE Services that you are licensed to use on the AE Server.
- Communication Manager Interface - Use Communication Manager Interface to manage switch connection and dialplan.
- High Availability - Use High Availability to manage AE Services HA.
- Licensing - Use Licensing to manage the license server.
- Maintenance - Use Maintenance to manage the routine maintenance tasks.
- Networking - Use Networking to manage the network interfaces and ports.
- Security - Use Security to manage Linux user accounts, certificate, host authentication and authorization, configure Linux-PAM (Pluggable Authentication Modules for Linux) and so on.
- Status - Use Status to obtain server status informations.
- User Management - Use User Management to manage AE Services users and AE Services user-related resources.
- Utilities - Use Utilities to carry out basic connectivity tests.
- Help - Use Help to obtain a few tips for using the OAM Help system

Depending on your business requirements, these administrative domains can be served by one administrator for all domains, or a separate administrator for each domain.

Copyright © 2009-2019 Avaya Inc. All Rights Reserved.

6.2. Verify License

Select **Licensing → WebLM Server Access** in the left pane, to display the applicable WebLM server log in screen (not shown). Log in using the appropriate credentials and navigate to display installed licenses (not shown).

 **Application Enablement Services**
Management Console

Welcome: User cust
Last login: Thu Aug 15 15:41:45 2019 from 10.128.224.59
Number of prior failed login attempts: 0
HostName/IP: aes95/10.30.5.95
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.1.0.0.0.9-1
Server Date and Time: Fri Aug 16 13:20:56 IST 2019
HA Status: Not Configured

Licensing

Home | Help | Logout

- ▶ AE Services
- ▶ Communication Manager Interface
- ▶ High Availability
- ▼ Licensing
 - WebLM Server Address
 - WebLM Server Access**
 - Reserved Licenses
- ▶ Maintenance
- ▶ Networking

Licensing

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

- WebLM Server Address

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

- WebLM Server Access

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

- Reserved Licenses

Select **Licensed products** → **APPL_ENAB** → **Application_Enablement** in the left pane, to display the **Licensed Features** screen in the right pane.

Verify that there are sufficient licenses for **TSAPI Simultaneous Users**, as shown below. Also verify that there is an applicable advanced switch license, in this case **AES ADVANCED LARGE SWITCH**, which is needed for adjunct routing.

The screenshot shows the Avaya Aura System Manager 8.0 interface. The left sidebar contains a tree view with 'Licenses' expanded. The main content area displays the 'View License Capacity' page for 'APPL_ENAB' under 'Application_Enablement'. The page shows the license installed on December 28, 2018, at 11:22:53 AM +07:00, with host IDs V0-55-3B-33-B4-26-01. A table titled 'Licensed Features' lists 13 items, including various switch licenses (AES) and TSAPI Simultaneous Users.

Feature (License Keyword)	Expiration date	Licensed capacity
Device Media and Call Control VALUE_AES_DMCC_DMC	permanent	1000
AES ADVANCED LARGE SWITCH VALUE_AES_AEC_LARGE_ADVANCED	permanent	1000
AES HA LARGE VALUE_AES_HA_LARGE	permanent	1000
AES ADVANCED MEDIUM SWITCH VALUE_AES_AEC_MEDIUM_ADVANCED	permanent	1000
Unified CC API Desktop Edition VALUE_AES_AEC_UNIFIED_CC_DESKTOP	permanent	1000
CVLAN ASAI VALUE_AES_CVLAN_ASAI	permanent	1000
AES HA MEDIUM VALUE_AES_HA_MEDIUM	permanent	1000
AES ADVANCED SMALL SWITCH VALUE_AES_AEC_SMALL_ADVANCED	permanent	1000
DLG VALUE_AES_DLG	permanent	1000
TSAPI Simultaneous Users VALUE_AES_TSAPI_USERS	permanent	1000
CVLAN Proprietary Links VALUE_AES_PROPRIETARY_LINKS	permanent	1000

6.3. Administer TSAPI Link

Select **AE Services** → **TSAPI** → **TSAPI Links** from the left pane of the **Management Console**, to administer a TSAPI link. The **TSAPI Links** screen is displayed, as shown below. Click **Add Link**.

The screenshot shows the AVAYA Application Enablement Services Management Console. The top right corner displays user information: "Welcome: User cust", "Last login: Fri Aug 16 13:18:49 2019 from 10.128.224.59", "Number of prior failed login attempts: 0", "HostName/IP: aes95/10.30.5.95", "Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE", "SW Version: 8.1.0.0.9-1", "Server Date and Time: Fri Aug 16 13:40:32 IST 2019", and "HA Status: Not Configured". The main navigation bar includes "AE Services | TSAPI | TSAPI Links" and "Home | Help | Logout". The left sidebar shows the "AE Services" tree with "TSAPI Links" selected. The main content area, titled "TSAPI Links", contains a table with columns: "Link", "Switch Connection", "Switch CTI Link #", "ASAI Link Version", and "Security". Below the table are buttons for "Add Link", "Edit Link", and "Delete Link".

The **Add TSAPI Links** screen is displayed next.


The **Link** field is only local to the Application Enablement Services server and may be set to any available number. For **Switch Connection**, select the relevant switch connection from the drop-down list. In this case, the existing switch connection **CM8** is selected. For **Switch CTI Link Number**, select the CTI link number from **Section 5.2**. Select **Encrypted** for Security field. **ASAI Link Version 9** was used for compliance testing.

The screenshot shows the AVAYA Application Enablement Services Management Console with the "Edit TSAPI Links" screen. The top right corner displays user information: "Welcome: User cust", "Last login: Mon Oct 7 08:43:49 2019 from 10.128.224.59", "Number of prior failed login attempts: 0", "HostName/IP: aes95/10.30.5.95", "Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE", "SW Version: 8.1.0.0.9-1", "Server Date and Time: Mon Oct 07 08:59:03 IST 2019", and "HA Status: Not Configured". The main navigation bar includes "AE Services | TSAPI | TSAPI Links" and "Home | Help | Logout". The left sidebar shows the "AE Services" tree with "TSAPI Links" selected. The main content area, titled "Edit TSAPI Links", contains form fields for "Link" (value: 1), "Switch Connection" (dropdown: CM8), "Switch CTI Link Number" (dropdown: 1), "ASAI Link Version" (dropdown: 9), and "Security" (dropdown: Encrypted). Below the fields are buttons for "Apply Changes", "Cancel Changes", and "Advanced Settings".

6.4. Administer Trinity User

Select **User Management** → **User Admin** → **Add User** from the left pane, to display the **Add User** screen in the right pane.

Enter desired values for **User Id**, **Common Name**, **Surname**, **User Password**, and **Confirm Password**. For **CT User**, select **Yes** from the drop-down list. Retain the default value in the remaining fields.

 **Application Enablement Services**
Management Console

Welcome: User cust
Last login: Wed Oct 2 14:23:12 2019 from 10.128.224.59
Number of prior failed login attempts: 0
HostName/IP: aes95/10.30.5.95
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.1.0.0.9-1
Server Date and Time: Wed Oct 02 15:04:42 IST 2019
HA Status: Not Configured

User Management | User Admin | Add UserHome | Help | Logout

▶ AE Services

▶ Communication Manager Interface

▶ High Availability

▶ Licensing

▶ Maintenance

▶ Networking

▶ Security

▶ Status

▼ User Management

▶ Service Admin

▼ User Admin

▪ Add User

▪ Change User Password

▪ List All Users

▪ Modify Default Users

▪ Search Users

▶ Utilities

▶ Help

Add User

Fields marked with * can not be empty.

* User Idtrinity

* Common Nametrinity

* Surnametrinity

* User Password••••••

* Confirm Password••••••

Admin Note

Avaya RoleNone

Business Category

Car License

CM Home

Css Home

CT UserYes

Department Number

Display Name

Employee Number

Employee Type

6.5. Restart Services

Select **Maintenance** → **Service Controller** from the left pane, to display the **Service Controller** screen in the right pane. Check **TSAPI Service** and click **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](#)

6.6. Obtain Tlink Name

Select **Security** → **Security Database** → **Tlinks** from the left pane. The **Tlinks** screen shows a listing of the Tlink names. A new Tlink name is automatically generated for the TSAPI service. Locate the Tlink name associated with the relevant switch connection, which would use the name of the switch connection as part of the Tlink name. Make a note of the associated Tlink name, to be used later for configuring Trinity.

In this case, the associated Tlink name is **AVAYA#CM8#CSTA-S#AES8**. Note the use of the switch connection **CM8** from **Section 6.3** as part of the Tlink name.

**Application Enablement Services**
Management Console

Welcome: User cust
Last login: Mon Oct 7 13:30:12 2019 from 10.128.224.59
Number of prior failed login attempts: 0
HostName/IP: aes95/10.30.5.95
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.1.0.0.9-1
Server Date and Time: Mon Oct 07 13:38:49 IST 2019
HA Status: Not Configured

Security | Security Database | TlinksHome | 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

Tlinks

Tlink Name

☒ AVAYA#CM8#CSTA-S#AES8

Delete Tlink

7. Configure trinityRESPOND Emergency Response Management Solution

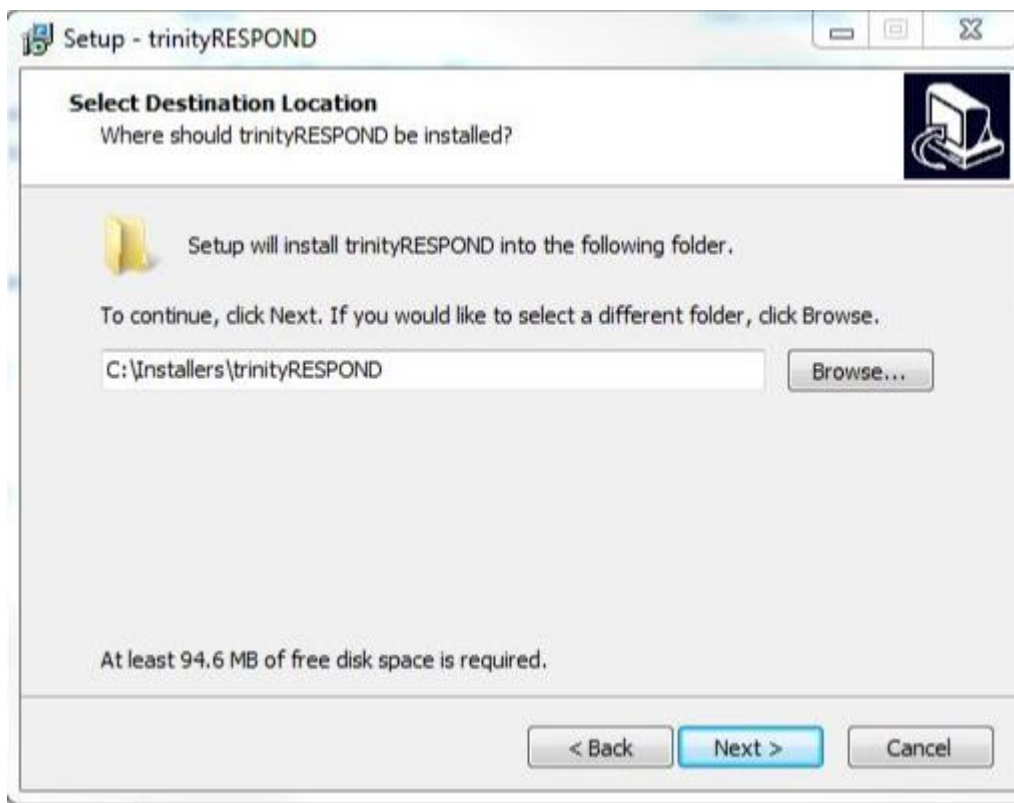
This section provides the procedures for configuring trinityRESPOND Server and CAD workstation CTI telephone with Avaya AES.

- Configure trinityRESPOND CAD CTI
- Configure CAD Taker

7.1. Configure trinityRESPOND CAD CTI

This section describes the steps required for trinityRESPOND CAD CTI to interoperate with Application Enablement Services. the following configuration steps have to be carried out.

Step 1: Double click the CADWorkstation.exe.config in workstation desktop
Add PBX information into appconfix.xml file and enable secured connections using TLS.

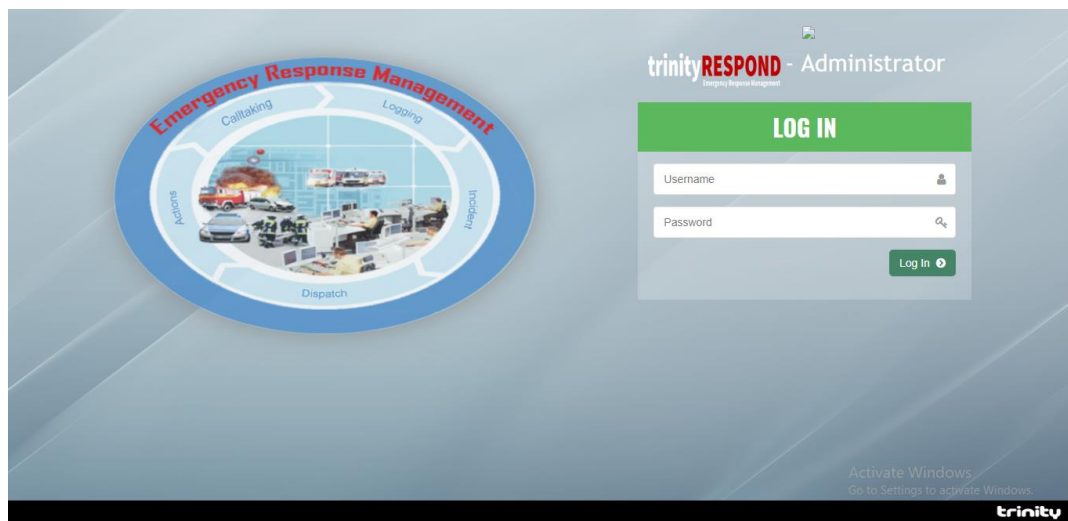


```

<Configuration>
<PBXSetings>
  <Add key="PBXIP" value="10.30.5.95"/>
  <Add key="PBXPort" value="450"/>
  <Add key="PBXUsername" value="trinity"/>
  <Add key="PBXPassword" value=" trinity "/>
</PBXSetings>
</Configuration>

```

Step 2: Access the trinityRESPOND admin tool using HTTP link provide a valid user/password must be used.



Once logged in, the “User Management” menu provides administrators with all relevant functionalities to complete the add new user.

trinityRESPOND - Administrator

ADMIN

User Management -

Resource Configuration -

Remodeling -

Run Card Config -

SOP Modeling -

Management -

Enquiry -

Approvals -

Cameras and Sensors -

Telephone Data -

Response Matrix -

Application configuration -

Workstation

+ Add Workstation Delete Reset Status Reset All Reset Activation Upload Excel Download Template

Show 10 entries

	SL No	Edit	Component id	User	User Type	Workstation Name	Login Status
<input type="checkbox"/>	1		102	ctws1	COMMUNICATION OFFICER		
<input type="checkbox"/>	2		240	dws1	DISPATCH OFFICER		
<input type="checkbox"/>	3		300	abhi	DISPATCH OFFICER		
<input type="checkbox"/>	4		622	dcabhi	DOCTOR CONSOLE		
<input type="checkbox"/>	5		402	abhicdws	CALL DISPATCHER		
<input type="checkbox"/>	6		100	NGCT	COMMUNICATION OFFICER		
<input type="checkbox"/>	7		2010	ramdws	DISPATCH OFFICER	RAMDWS	
<input type="checkbox"/>	8		3010	ramsws	SUPERVISOR	RAMSWWS	
<input type="checkbox"/>	9		3600		DOCTOR CONSOLE		
<input type="checkbox"/>	10		4010		CALL DISPATCHER	RAMCDWS	

Showing 1 to 10 of 48 entries

Previous 1 2 3 4 5 Next

Select the option for **Add Workstation** for telephone registration.

trinityRESPOND - Administrator ADMIN

Workstation

+ Add Workstation Delete Reset Status Reset All Reset Activation Upload Excel Download Template

Add Workstation

Component Id *: ENTER COMPONENT ID

Workstation Name: ENTER WORKSTATION NAME

User Type *: SELECT USER TYPE

Save Clear Cancel

Show 10 entries

SL No	Edit	Component Id	User	User Type	Workstation Name	Login Status
1		102	ctws1	COMMUNICATION OFFICER		
2		240	dws1	DISPATCH OFFICER		
3		300	abhi	DISPATCH OFFICER		
4		622	dcabhi	DOCTOR CONSOLE		
5		402	abhidws	CALL DISPATCHER		
6		100	NGCT	COMMUNICATION OFFICER		

Step 3: Create telephone extension and agent Ids and map to user ID.

trinityRESPOND - Administrator ADMIN

Workstation

+ Add Workstation Delete Reset Status Reset All Reset Activation Upload Excel Download Template

Add Workstation

Component Id *: 1002

Workstation Name: CTWS1

User Type *: COMMUNICATION OFFICER

Save Clear Cancel

Show 10 entries

trinityRESPOND - Administrator ADMIN

Active Users

+ Add User Block User Delete User

Add User

User Id *: CTWS1

Name *: ENTER NAME

Password *: *****

Contact Number: ENTER CONTACT NUMBER

User Type *: COMMUNICATION OFFICER

Email Id: ENTER EMAIL ID

Department *: ALL

Agent Id: ENTER AGENT ID

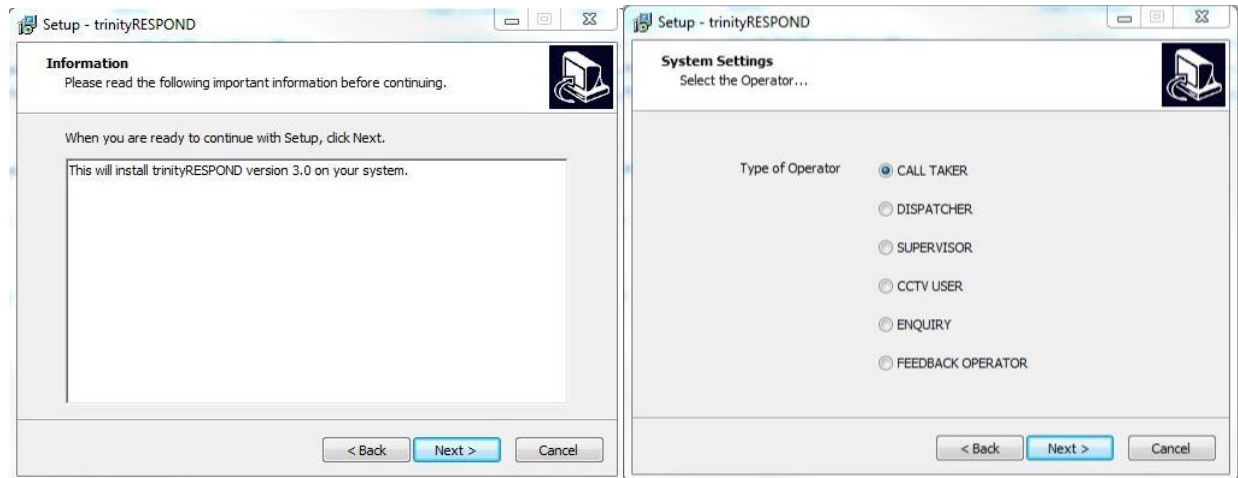
Save Clear Cancel

Show 10 entries

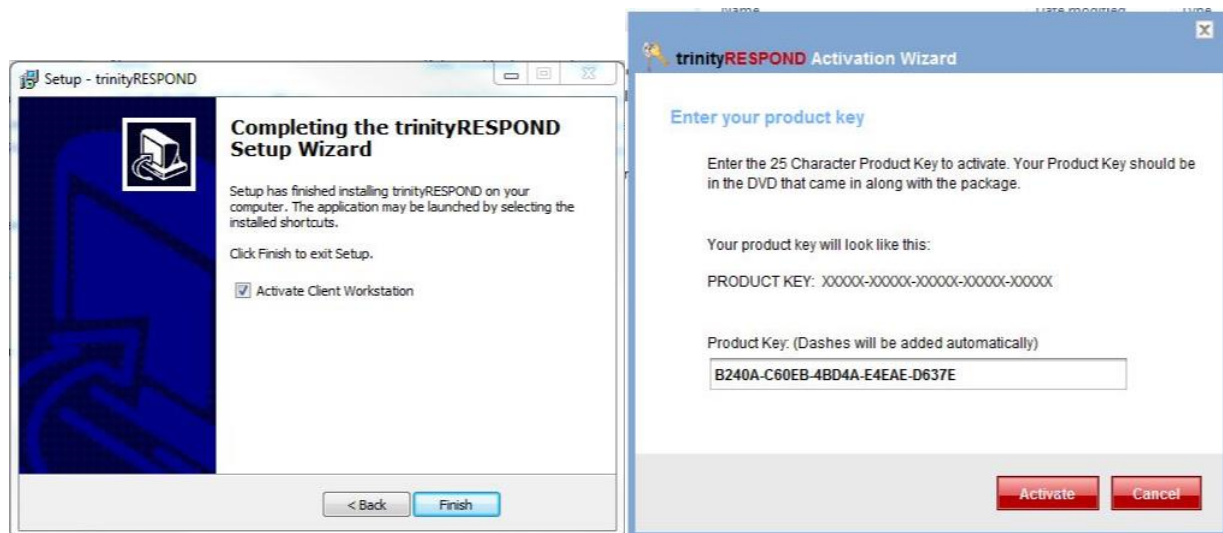
SL NO	Edit User	Name	User Id	User Type	Agent Id	Department
-------	-----------	------	---------	-----------	----------	------------

7.2. Configure CAD Taker

These Application Notes assume that the default installation of CAD Taker software is performed as below.



When the **trinityRESPOND Activation Wizard** screen is displayed, enter the **Product Key** provided by Trinity:



Launch the CAD Taker application from the Windows Start menu, enter **User ID** and **Password**, administered in **Section 7.1** and the **Station ID** you wish the operator to use, as shown below.

Click **Login** to log in CAD Taker. Once successfully logged in, the details are clearly displayed User ID (**ctws1**) and Agent ID (**80000**) as below.

8. Verification Steps

This section provides the tests that can be performed to verify correct configuration of Communication Manager, Application Enablement Services, and trinityRESPOND – Emergency Response Management Solution.

8.1. Verify Avaya Aura® Communication Manager

On Communication Manager, verify status of the administered CTI link by using the “status aesvcs cti-link” command. Verify that the **Service State** is “established” for the CTI link number administered in **Section 5.2**, as shown below.

```
status aesvcs cti-link
```

AE SERVICES CTI LINK STATUS						
CTI Link	Version	Mnt Busy	AE Services Server	Service State	Msgs Sent	Msgs Rcvd
1	9	no	aes8	established	14	14

Enter the command **list agent-loginID** verify that extension 70010 is logged into agent **80000** shown in **Section 5.3.2**.

```
list agent-loginID
```

AGENT LOGINID									
Login ID	Name	Extension	Dir	Agt	AAS/AUD	COR	Ag	Pr	SO
	Skil/Lv	Skil/Lv	Skil/Lv	Skil/Lv	Skil/Lv	Skil/Lv	Skil/Lv	Skil/Lv	Skil/Lv
80000	Voice Agent	70009					1	lvl	
	2/01	/	/	/	/	/	/	/	

Enter the command **status station 70009** and on **Page 7** verify that the agent is logged-in to the appropriate skill.

```
status station 70009
```

ACD STATUS							Page 7 of 7
Grp/Mod	Grp/Mod	Grp/Mod	Grp/Mod	Grp/Mod	Grp/Mod	Grp/Mod	
2/AI	/	/	/	/	/	/	On ACD Call? no

8.2. Verify Avaya Aura® Application Enablement Services

On Application Enablement Services, verify the status of the TSAPI link by selecting **Status** → **Status and Control** → **TSAPI Service Summary** from the left pane. The **TSAPI Link Details** screen is displayed.

Verify the **Status** is “Talking” for the TSAPI link administered in **Section 6.3**, and that the **Associations** column reflects the total number of agent, in this case “1”.

Status | Status and Control | TSAPI Service Summary

Home | Help | Logout

▶ AE Services

▶ Communication Manager Interface

High Availability

▶ Licensing

▶ Maintenance

▶ Networking

▶ Security

▼ Status

Alarm Viewer

▶ Logs

▶ Log Manager

▼ Status and Control

▪ CVLAN Service Summary

▪ DLG Services Summary

▪ DMCC Service Summary

▪ Switch Conn Summary

▪ TSAPI Service Summary

TSAPI Link Details


☐ Enable page refresh every 60 seconds

	Link	Switch Name	Switch CTI Link ID	Status	Since	State	Switch Version	Associations	Msgs to Switch	Msgs from Switch	Msgs Period
<input checked="" type="radio"/>	1	CM8	1	Talking	Mon May 20 18:12:03 2019	Online	18	1	6450	6461	30

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

8.3. Verify Avaya Aura® Application Enablement Services TSAPI Service

The following steps are carried out on the Application Enablement Services to ensure that the communication link between Communication Manager and the Application Enablement Services server is functioning correctly. Verify the status of the TSAPI service by selecting **Status → Status and Control → TSAPI Service Summary → User Status**. The **Open Streams** section of this page displays open stream created by the **trinity** user with the **Tlink**.



Application Enablement Services
Management Console

Welcome: User cust
Last login: Fri Oct 4 16:14:50 2019 from 10.128.224.59
Number of prior failed login attempts: 0
HostName/IP: aes95/10.30.5.95
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.1.0.0.9-1
Server Date and Time: Mon Oct 07 08:48:54 IST 2019
HA Status: Not Configured

Status | Status and Control | TSAPI Service SummaryHome | Help | Logout

▶ AE Services

▶ Communication Manager Interface

▶ High Availability

▶ Licensing

▶ Maintenance

▶ Networking

▶ Security

▼ Status

Alarm Viewer

▶ Logs

▶ Log Manager

▼ Status and Control

▪ CVLAN Service Summary

▪ DLG Services Summary

▪ DMCC Service Summary

▪ Switch Conn Summary

▪ TSAPI Service Summary

CTI User Status

☐ Enable page refresh every 60 seconds

CTI Users All Users Submit

Open Streams 1

Closed Streams 42

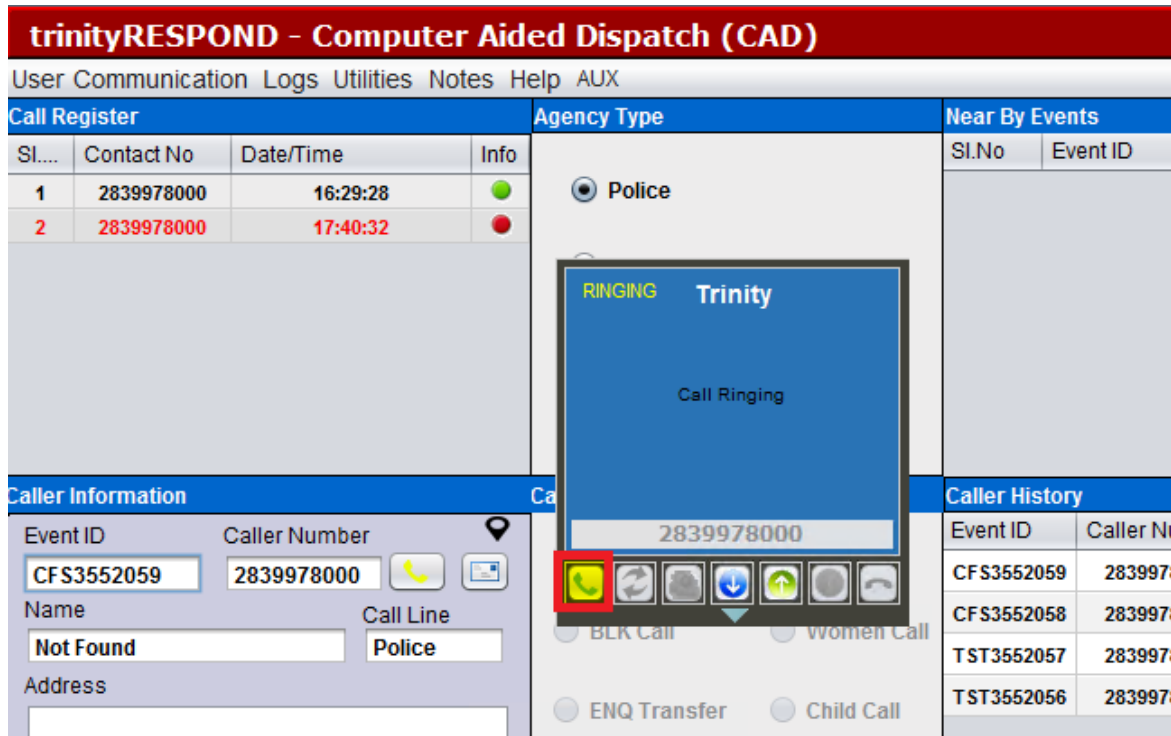
Open Streams

Name	Time Opened	Time Closed	Tlink Name
trinity	Mon 07 Oct 2019 08:41:33 AM IST		AVAYA#CM93#CSTA-S#AES95

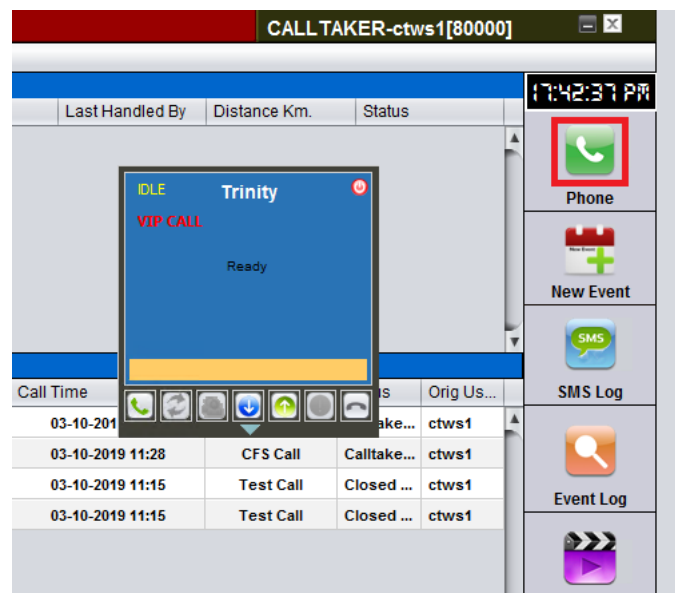
Show Closed StreamsClose All Opened StreamsBack

8.4. Verify trinityRESPOND CAD Call Taker

Make an incoming call from PSTN to a general routing hunt group in **Section 5.3.1**. Verify that the CAD Taker can receive incoming call. Answer incoming calls with the **Answer** button.



Make an outbound call with **Phone** button:



The phone call status is shown as below:

trinityRESPOND - Computer Aided Dispatch (CAD) CALLTAKER-vip1[6447]

User Communication Logs Utilities Notes Help AUX

Call Register

Sl...	Contact No	Date/Time	Info
1	08801917380...	22:44:04	

Agency Type

☒ Police

☐ Fire Force

☐ Traffic Police

☐ Ambulance

Near By Events

Sl.No	Event ID	Phone No	Call Time	Last Handled By	Distance Km.	Status

Caller Information

Event ID: CFS13722577
 Caller Number: 01917380856
 Name: farhaan
 Call Line: Police
 Address: 6/3,flat g-8,segunbagicha,Dhaka
 Identity: Update

Call Type

☒ CFS Call ☐ CRK Call

☐ BLK Call ☐ Women Call

☐ ENQ Transfer ☐ Child Call

☐ Test Call ☐ DEP Call

☐ Repeat Call

Call Answer

Caller History

Event ID	Caller Address	Call Time	Call Type	Status	Orig Us...
CFS13722...	,flat g-8,segunb...	02-10-2019 22:44	CFS Call	Calltake...	vip1
TST13722...	,flat g-8,segunb...	02-10-2019 22:39	Test Call	Closed ...	vip1

Distress Information

Name: ☐ Same as Caller's Data

Address:

Place:

Land Mark:

Phone No: 08801917380856

District: -Select- Event Ty: -Select-

Nearest Station: -Select- Event SubType: -Select-

Additional Details:

Services

☐ Police ☐ Fire ☐ Ambulance ☐ Other

Priority

☒ H ☐ M ☐ L

Call List

088019173... 00:00:07

Phone Status

ON_TALK Trinity

In Talk

00:00:19

8801917380856

Send SMS

Dispatch

Similar Events

Hand Over

Hot Dispatch

trinity

Go to Settings to activate W

00:04

9. Conclusion

These Application Notes describe the configuration steps required for the trinityRESPOND - Emergency Response Management Solution to successfully interoperate with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services. All feature and serviceability test cases were completed with observations noted in **Section 2.2**.

10. Additional References

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

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

1. *Administering Avaya Aura® Communication Manager, Release 8, Issue 2.0, Nov 2018*
2. *Administering Avaya Aura® Session Manager, Release 8, Issue 2, August 2018*
3. *Administering Avaya Aura® System Manager, Release 8, Issue 4, September 2018*
4. *Administering Avaya Aura® Application Enablement Services, Release 8.0.1, Issue 2, December 2018*

Product Documentation for trinityRESPOND - Emergency Response Management Solution can be requested from Trinity Mobility found at: <http://trinitymobility.com/>.

©2019 Avaya Inc. All Rights Reserved.

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

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