



Avaya Solution & Interoperability Test Lab

Application Notes for TriTech Inform 911™ R5.5 with Avaya Aura® Communication Manager R7.1 and Avaya Aura® Application Enablement Services R7.1 – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for the TriTech Inform 911™ R5.5 solution to interoperate with Avaya Aura® Communication Manager R7.1 and Avaya Aura® Application Enablement Services R7.1.

TriTech is a desktop application that is used to answer emergency calls in a PSAP. Trittech Inform 911™ uses the Avaya Aura® Application Enablement Services' Telephony Services Application Program Interface (TSAPI) and Device, Media and Call Control (DMCC) Interface from Avaya Aura® Communication Manager to receive phone activity for agents and control Avaya IP Deskphones.

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

TriTech Inform 911™ (Inform 911) is a Public Safety Answering Point (PSAP) solution used for handling Emergency Calls. Inform 911 uses the TSAPI interface provided by Avaya Aura® Application Enablement Services (AES) for call control. Inform 911 also uses the DMCC interface provided by AES for monitoring, sending DTMF and hook flash.

Inform 911 consists of Inform 911 server and Inform 911 workstations. All configuration related to AES is performed on Inform 911 server. Inform 911 workstations connect to AES via Inform 911 server. Inform 911 workstation runs the Inform 911 PSAP call taking application.

2. General Test Approach and Test Results

The compliance test included feature and serviceability testing as mentioned in **Section 2.1**.

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 this Application Note, the interface between Avaya systems and Inform 911 did not include use of any specific encryption features as requested by TriTech.

2.1. Interoperability Compliance Testing

The compliance test validated the ability of Inform 911 to perform the following:

- Answering incoming Emergency Calls.
- Agent log-in and logout.
- Agent work modes such as Auto-In, ACW, etc.
- Answer and place calls to/from PSTN and internal Avaya endpoints.
- Call hold, mute, transfer, conference and DTMF.

Additionally, serviceability testing was performed to confirm the ability for Inform 911 to recover from common outages such as network outages and server reboots.

2.2. Test Results

All test cases passed.

2.3. Support

Technical support on Inform 911 can be obtained through the following:

- **Phone:** 800-987-0911
- **Email:** support@tritech.com

3. Reference Configuration

Figure 1 illustrates the compliance test configuration consisting of Avaya environment and, Inform 911 server and Inform 911 workstations. The Inform 911 controlled Avaya 9600 Series IP H.323 Deskphones via Inform 911 server. Incoming simulated Emergency Calls to Avaya were routed via Inform 911 server, simulating a Central Office (CO). During the compliance test, TriTech products were deployed in TriTech labs, and connected to Avaya DevConnect labs via a VPN connection.

Note: Though incoming Emergency Calls to Avaya were routed via Inform 911 (SIP), the scope of this compliance test was to verify AES interoperability. It was suggested by TriTech to have simulated Emergency Calls routed via a CO simulator (SIP Trunks) because such is their typical deployment.

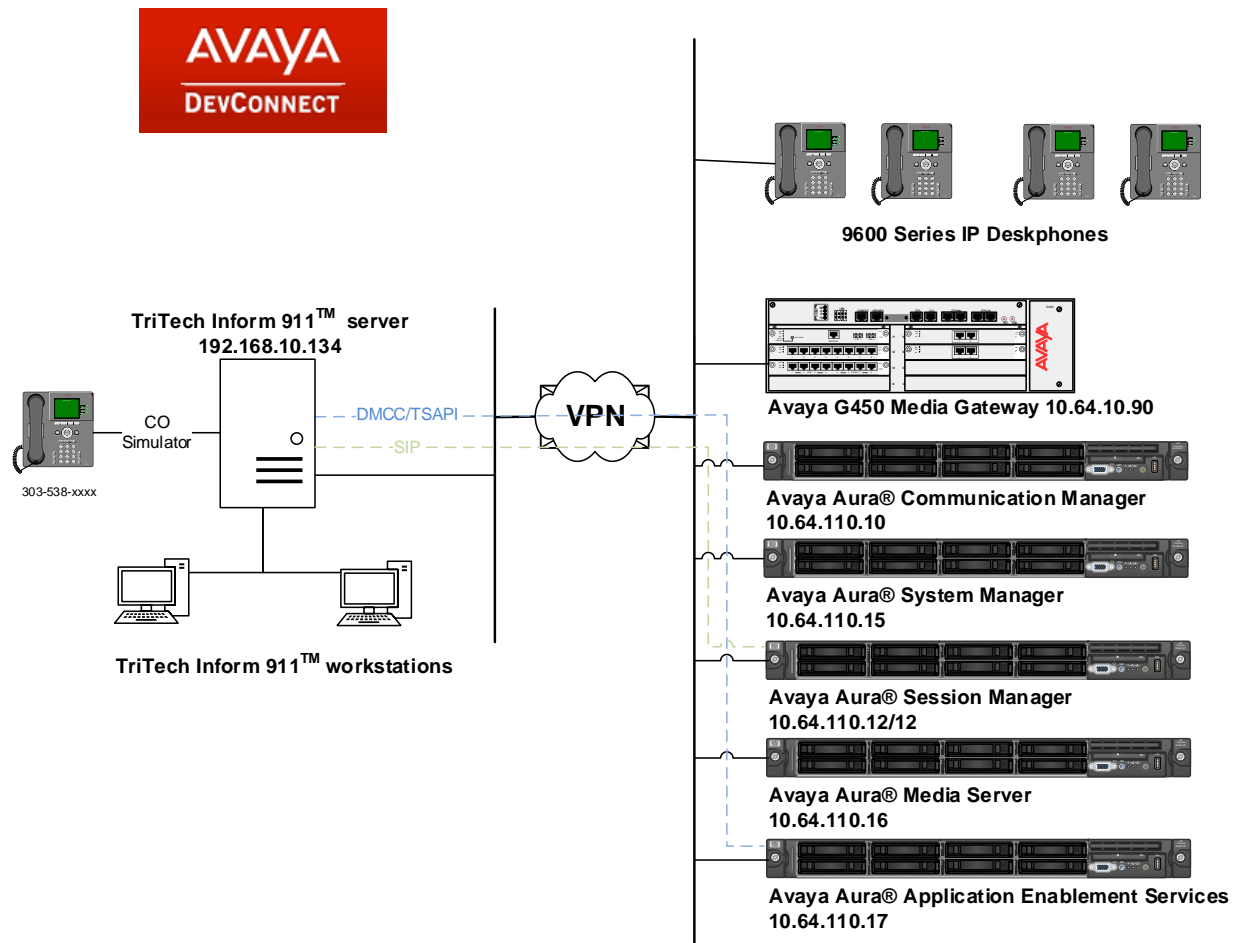


Figure 1 – Inform 911 Compliance Test Configuration

4. Equipment and Software Validated

The following equipment and version were used in the reference configuration described above:

Equipment/Software	Release/Version
Avaya Aura® Communication Manager running on virtualized environment	7.1.2 R017x.01.0.532.0 Build 24184
Avaya Aura® Application Enablement Services running on virtualized environment	7.1.2
Avaya Aura® System Manager running on virtualized environment	7.1.2
Avaya Aura® Session Manager running on virtualized environment	7.1.2
Avaya Aura® Media Server running on virtualized environment	7.8.0.309
Avaya G450 Media Gateway	FW 39.17.0/1
Avaya 9600 Series IP Deskphone <ul style="list-style-type: none">• 96x1 H.323• 96x1 SIP• 96x0 H.323	6.6.6 7.1.1.0 3.2.6
TriTech Inform 911™	5.500.9.5

Note: Inform 911 used Avaya TSAPI Client version 6.3.3 and Avaya DMCC SDK version 6.3.3.

5. Configure Avaya Aura® Communication Manager

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

- Verify Feature and License for the integration
- Administer Communication Manager System Features
- Administer IP Services for Application Enablement Services
- Administer Computer Telephony Integration (CTI) Link
- Add Station Extension
- Add Agent Login
- Add VDN
- Administer Skill
- Administer Vector

All the configuration changes in this section for Communication Manager are performed through the System Access Terminal (SAT) interface. For more details on configuring Communication Manager, refer to the Avaya product documentation in **Section 10**.

5.1. Verify Feature

Enter the **display system-parameters customer-options** command and ensure that **Computer Telephony Adjunct Links** is set to **y**. If this option is not set to **y**, 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? 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
```

(NOTE: You must logoff & login to effect the permission changes.)

5.2. Administer Communication Manager System Features

Enter the **change system-parameters features** command and ensure that on Page 5 **Create Universal Call ID (UCID)** is enabled and a relevant **UCID Network Node ID** (1 was used in the test) is defined. Also ensure that on Page 13 that **Send UCID to ASAI** is set to **y**. Inform 911 relies on UCID to track complex calls (Transfers and Conferences).

```
change system-parameters features                               Page  5 of  19
                        FEATURE-RELATED SYSTEM PARAMETERS

SYSTEM PRINTER PARAMETERS
  Endpoint:                Lines Per Page: 60

SYSTEM-WIDE PARAMETERS
                        Switch Name:
  Emergency Extension Forwarding (min): 10
  Enable Inter-Gateway Alternate Routing? n
  Enable Dial Plan Transparency in Survivable Mode? n
                        COR to Use for DPT: station
                        EC500 Routing in Survivable Mode: dpt-then-ec500
MALICIOUS CALL TRACE PARAMETERS
  Apply MCT Warning Tone? n    MCT Voice Recorder Trunk Group:
  Delay Sending RElease (seconds): 0
SEND ALL CALLS OPTIONS
  Send All Calls Applies to: station    Auto Inspect on Send All Calls? n
  Preserve previous AUX Work button states after deactivation? n
UNIVERSAL CALL ID
  Create Universal Call ID (UCID)? y    UCID Network Node ID: 1
```

```
change system-parameters features                               Page 13 of  19
                        FEATURE-RELATED SYSTEM PARAMETERS

CALL CENTER MISCELLANEOUS
  Callr-info Display Timer (sec): 10
                        Clear Callr-info: next-call
  Allow Ringer-off with Auto-Answer? n

  Reporting for PC Non-Predictive Calls? n

  Agent/Caller Disconnect Tones? n
  Interruptible Aux Notification Timer (sec): 3
  Zip Tone Burst for Callmaster Endpoints: double

ASAI
  Copy ASAI UUI During Conference/Transfer? n
  Call Classification After Answer Supervision? n
                        Send UCID to ASAI? y
  For ASAI Send DTMF Tone to Call Originator? y
  Send Connect Event to ASAI For Announcement Answer? n
  Prefer H.323 Over SIP For Dual-Reg Station 3PCC Make Call? n
```

5.3. Administer IP-Services for Application Enablement Services

Add an IP-Services entry for Application Enablement Services as described below:

- Enter the **change ip-services** command.
- In the **Service Type** field, type **AESVCS**.
- In the **Enabled** field, type **y**.
- In the **Local Node** field, type the Node name **procr** for the Processor Ethernet Interface.
- In the **Local Port** field, use the default of **8765**.
- Note that in installations using CLAN connectivity, each CLAN interface would require similar configuration.

change ip-services					Page	1 of	3
IP SERVICES							
Service Type	Enabled	Local Node	Local Port	Remote Node	Remote Port		
AESVCS	y	procr	8765				

On Page 3 of the IP Services form, enter the following values:

- In the **AE Services Server** field, type the host name of the Application Enablement Services server.
- In the **Password** field, type the same password to be administered on the Application Enablement Services server in **Section 6.1**.
- In the **Enabled** field, type **y**.

change ip-services				Page	3 of	3
AE Services Administration						
Server ID	AE Services Server	Password	Enabled	Status		
1:	aes	*	y	in use		

Add an entry in node-names table for AES using **change node-names ip** command. Note that the **Name** should match the actual host name of AES. Type in the IP Address of AES in **IP Address** as shown below.

change node-names ip		Page 1 of 2
IP NODE NAMES		
Name	IP Address	
aes	10.64.110.17	
ams	10.64.110.13	
asm	10.64.110.12	
cms	10.64.110.18	
default	0.0.0.0	
procr	10.64.110.10	
procr6	::	

5.4. Administer Computer Telephony Integration (CTI) Link

Enter the **add cti-link <link number>** command, where **<link number>** is an available CTI link number.

- In the **Extension** field, type a valid station extension.
- In the **Type** field, type **ADJ-IP**.
- In the **Name** field, type a descriptive name.

add cti-link 1	Page 1 of 3
CTI Link: 1	CTI LINK
Extension: 69999	
Type: ADJ-IP	
	COR: 1
Name: AES CTI Link	

5.5. Add Station Extensions

A station extension needs to be added for PSAP call taker. Inform 911 uses this station for call control and monitoring. To add a station, enter the **add station <number>** command, where **<number>** is an available extension. Ensure that the station has **IP Softphone** enabled, and the Inform 911 application needs to know the **Security Code** in order to successfully register. Note that the **Security Code** configured should be same for all the stations that will be used by Inform 911. Configure other information as desired. During the compliance test two stations were configured, 50001 and 50002.

```
add station 50001                                     Page 1 of 5

                                STATION

Extension: 50001                                Lock Messages? n                BCC: 0
Type: 9630                                      Security Code: *                TN: 1
Port: S00002                                Coverage Path 1:                COR: 1
Name: H.323 Station 1                       Coverage Path 2:                COS: 1
                                           Hunt-to Station:                Tests? y

STATION OPTIONS

                                Time of Day Lock Table:
                                Personalized Ringing Pattern: 1
                                Message Lamp Ext: 50001
                                Mute Button Enabled? y
                                Display Language: english        Button Modules: 0
                                Speakerphone: 2-way
                                Survivable GK Node Name:
                                Survivable COR: internal
                                Survivable Trunk Dest? y
                                Media Complex Ext:
                                IP SoftPhone? y
                                IP Video Softphone? n
                                Short/Prefixed Registration Allowed: default
                                Customizable Labels? y
```

5.6. Add Agent Login

An agent login needs to be added for PSAP call taker. To add an agent login, enter the **add agent-loginID <number>** command, where **<number>** is and available agent ID. During the compliance test two agent logins were created, 5001 and 5002.

```
add agent-loginID 5001                               Page 1 of 2

                                AGENT LOGINID

                                Login ID: 5001
                                Name: CC Agent 1
                                TN: 1
                                COR: 1
                                Coverage Path:
                                Security Code:
                                Attribute:
                                AAS? n
                                AUDIX? n
                                Check skill TNs to match agent TN? n
                                LWC Reception: spe
                                LWC Log External Calls? n
                                AUDIX Name for Messaging:
                                LoginID for ISDN/SIP Display? n
                                Password:*
                                Password (enter again):*
                                Auto Answer: station
```

On Page 2, configure the skill of the agent. The skill used here is as configured in **Section 5.8**.

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

5.7. Add VDN

A VDN needs to be added that will be used to route incoming Emergency Calls to PSAP call takers via vector programming. To add a VDN, enter the **add vdn <number>** command, where **<number>** is an available extension number. Enter a **Vector Number** to be used for the compliance test. Inform 911 monitors this VDN.

add vdn 55501						Page 1 of 3	
VECTOR DIRECTORY NUMBER							
Extension: 55501							
Name*: Trittech VDN 1							
Destination: Vector Number						1	
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							

5.8. Administer Skill

To add a skill, Enter the **add hunt-group <number>**, where <number> is an available hunt group number. Configure a **Group Extension**, and set **ACD**, **Queue** and **Vector** to **y**.

add hunt-group 1		Page 1 of 4	
HUNT GROUP			
Group Number: 1		ACD? y	
Group Name: Skill 1		Queue? y	
Group Extension: 23001		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 1		Page 2 of 4	
HUNT GROUP			
Skill? y		Expected Call Handling Time (sec): 10	
AAS? n		Service Level Target (% in sec): 80 in 20	
Measured: both			
Supervisor Extension:			

5.9. Administer Vector

Enter the **change vector <number>** command to configure the vector, where <number> is the value configured in **Section 5.7**. During compliance test, the following vector configuration was used.

change vector 1		Page 1 of 6	
CALL VECTOR			
Number: 1	Name: Vector 1		
Multimedia? n	Attendant Vectoring? n	Meet-me Conf? n	Lock? n
Basic? y	EAS? y	G3V4 Enhanced? y	ANI/II-Digits? y
Prompting? y	LAI? y	G3V4 Adv Route? y	ASAI Routing? y
Variables? y	3.0 Enhanced? y	CINFO? y	BSR? y
01 wait-time	2	secs hearing ringback	
02 queue-to	skill 1	pri m	
03 wait-time	30	secs hearing ringback	
04 goto step	2	if unconditionally	
05 stop			

6. Configure Avaya Aura® Application Enablement Services

All administration of AES is performed via a web browser. Enter <https://<ip-addr>> in the URL field of a web browser where <ip-addr> is the IP address of the AES server. After a login step, the **Welcome to OAM** page is displayed. Note that all navigation is performed by clicking links in the Navigation Panel on the left side of the screen, context panels will then appear on the right side of the screen.

The procedures fall into the following areas:

- Configure Communication Manager Switch Connections
- Configure TSAPI Link
- Configure Inform 911 User
- Obtain Tlink
- Confirm TSAPI and DMCC Licenses

AVAYA Application Enablement Services Management Console

Welcome: User cust
Last login: Fri Apr 20 16:53:07 2018 from 10.64.10.202
Number of prior failed login attempts: 0
HostName/IP: aes/10.64.110.17
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.1.2.0.0.5-0
Server Date and Time: Thu May 03 13:18:33 MDT 2018
HA Status: Not Configured

Home Home | Help | Logout

Navigation Panel:

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

Welcome to OAM

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.

6.1. Configure Communication Manager Switch Connections

To add links to Communication Manager, navigate to the **Communication Manager Interface** → **Switch Connections** page and enter a name for the new switch connection (e.g. **cm71**) and click the **Add Connection** button (not shown). The **Connection Details** screen is shown. Enter the **Switch Password** configured in **Section 5.3** and check the **Processor Ethernet** box if using the **procr** interface. Click **Apply**.

Communication Manager Interface | Switch Connections Home | Help | Logout

AE Services
Communication Manager Interface
Switch Connections
Dial Plan
High Availability
Licensing
Maintenance
Networking
Security
Status

Connection Details - cm71

Switch Password

Confirm Switch Password

Msg Period Minutes (1 - 72)

Provide AE Services certificate to switch ☐

Secure H323 Connection ☐

Processor Ethernet ☒

The display returns to the **Switch Connections** screen which shows that the **cm71** switch connection has been added.

Communication Manager Interface | Switch Connections Home | Help | Logout

AE Services
Communication Manager Interface
Switch Connections
Dial Plan
High Availability
Licensing
Maintenance

Switch Connections

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections
<input checked="" type="radio"/> cm71	Yes	30	1

Click the **Edit PE/CLAN IPs** button on the **Switch Connections** screen to configure the **procr** or **CLAN** IP Address(es) for TSAPI message traffic. The **Edit Processor Ethernet IP** screen is displayed. Enter the IP address of the **procr** interface and click the **Add/Edit Name or IP** button.

Communication Manager Interface | Switch Connections Home | Help | Logout

AE Services
 Communication Manager Interface
 Switch Connections
 Dial Plan
 High Availability
 Licensing
 Maintenance

Edit Processor Ethernet IP - cm71

10.64.110.10

Name or IP Address	Status
10.64.110.10	In Use

Click the **Edit H.323 Gatekeeper** button on the **Switch Connections** screen to configure the **procr** or **CLAN** IP Address(es) for DMCC registrations. The **Edit H.323 Gatekeeper** screen is displayed. Enter the IP address of the **procr** interface and click the **Add Name or IP** button.

Communication Manager Interface | Switch Connections Home | Help | Logout

AE Services
 Communication Manager Interface
 Switch Connections
 Dial Plan
 High Availability
 Licensing
 Maintenance

Edit H.323 Gatekeeper - cm71

10.64.110.10

Name or IP Address

☒ 10.64.110.10

6.2. Configure TSAPI Link

In the Navigation Panel, select **AE Service → TSAPI → TSAPI Link → Add Link**. Select the **Switch Connection** configured in previous section. Select the **Switch CTI Link Number** configured in **Section 5.4**. For **Security**, select **Both**.

Select **Apply Changes** once done. Note that once added, the TSAPI Service needs to be restarted. To restart TSAPI Service, navigate to **Maintenance → Service Controller**, check box for **TSAPI Service**, and select **Restart Service** (not shown).

The screenshot shows the 'Add TSAPI Links' configuration page. The left navigation pane is expanded to 'TSAPI Links'. The main content area has the following fields:

- Link: 1
- Switch Connection: cm71
- Switch CTI Link Number: 1
- ASAI Link Version: 8
- Security: Both

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

6.3. Configure a Inform 911 User

In the Navigation Panel, select **User Management → User Admin → Add User**. The **Add User** panel will display as shown below. Enter an appropriate **User Id**, **Common Name**, **Surname**, and **User Password**. Select **Yes** from the **CT User** dropdown list.

Click **Apply** (not shown) at the bottom of the pages to save the entries.

The screenshot shows the 'Add User' configuration page. The left navigation pane is expanded to 'User Admin'. The main content area has the following fields:

- * User Id: tritech
- * Common Name: tritech
- * Surname: tritech
- * User Password: [masked]
- * Confirm Password: [masked]
- Admin Note: [empty]
- Avaya Role: None
- Business Category: [empty]
- Car License: [empty]
- CM Home: [empty]
- Css Home: [empty]
- CT User: Yes
- Department Number: [empty]
- Display Name: [empty]

At the bottom is an 'Apply' button.

If the Security Database (SDB) is enabled on Application Enablement Services, set the Inform 911 user account to Unrestricted Access to enable any device (station, ACD extension, DMCC virtual station) to be used implicitly. This step avoids the need to duplicate administration.

Navigate to **Security → Security Database → CTI Users → List All Users** and select the **Inform 911** user and click **Edit**.

Security | Security Database | CTI Users | List All Users Home | Help | Logout

CTI Users

User ID	Common Name	Worktop Name	Device ID
<input type="radio"/> intranext	intranext	NONE	NONE
<input type="radio"/> oceana	oceana	NONE	NONE
<input type="radio"/> spokaes	spok	NONE	NONE
<input checked="" type="radio"/> tritech	tritech	NONE	NONE

[Edit](#) [List All](#)

On the **Edit CTI User** panel, check the **Unrestricted Access** box and click the **Apply Changes** button. Click **Apply** when asked to confirm the change on the **Apply Changes to CTI User Properties** dialog (not shown).

Security | Security Database | CTI Users | List All Users Home | Help | Logout

Edit CTI User

User Profile:

User ID: tritech
Common Name: tritech
Worktop Name:
Unrestricted Access: ☒

Call and Device Control:

Call Origination/Termination and Device Status:

Call and Device Monitoring:

Device Monitoring:
Calls On A Device Monitoring:
Call Monitoring: ☐

Routing Control:

Allow Routing on Listed Devices:

[Apply Changes](#) [Cancel Changes](#)

6.4. Obtain Tlink

To obtain the Tlink that will be used by Inform 911 to connect to AES, navigate to **Security** → **Security Database** → **Tlink**. During the compliance test, the select Tlink below was used.

Tlinks

Tlink Name

☒ AVAYA#CM71#CSTA#AES

☐ AVAYA#CM71#CSTA-S#AES

Delete Tlink

6.5. Confirm TSAPI and DMCC Licenses

A DMCC license is normally a **VALUE_AES_DMCC_DMC** from AE Services' WebLM. As a fall back, when a **VALUE_AES_DMCC_DMC** license is not available, an **IP_API_A** license from Communication Manager can be utilized in place of **VALUE_AES_DMCC_DMC**. Please consult product offer documentation for more details. If the licensed quantities are not sufficient for the implementation, contact the Avaya sales team or business partner for a proper license file.

From the left pane menu on Application Enablement Services Management Console, click **Licensing → WebLM Server Access**. A **Web License Manager** login window is displayed. Enter proper credentials to log in. Click **Licensed products → APPL_ENAB → Application Enablement** from the left pane. The Application Enablement Services license is displayed in the right pane. Ensure that there are enough **VALUE_AES_DMCC_DMC** and **VALUE_AES_TSAPI_USERS** licenses available.

WebLM Home

Install license

Licensed products

APPL_ENAB

▼ Application_Enablement

View license capacity

View peak usage

AVAYA_OCEANA

► Avaya_Oceana

Avaya_Aura_Web_Gateway

► Avaya_Aura_Web_Gateway

CE

► COLLABORATION_ENVIRONMENT

CMM

► Communication_Manager_Messaging

Configure Centralized Licensing

COLLABORATION_DESIGNER

► Collaboration_Designer

COMMUNICATION_MANAGER

► Call_Center

► Communication_Manager

Application Enablement (CTI) - Release: 7 - SID: 10503000 **Standard**

You are here: Licensed Products > Application_Enablement > View License Capacity

License installed on: July 11, 2017 5:33:16 PM +00:00

License File Host IDs: V4-3C-72-CC-66-1C-01

Licensed Features

10 Items Show **All** ▼

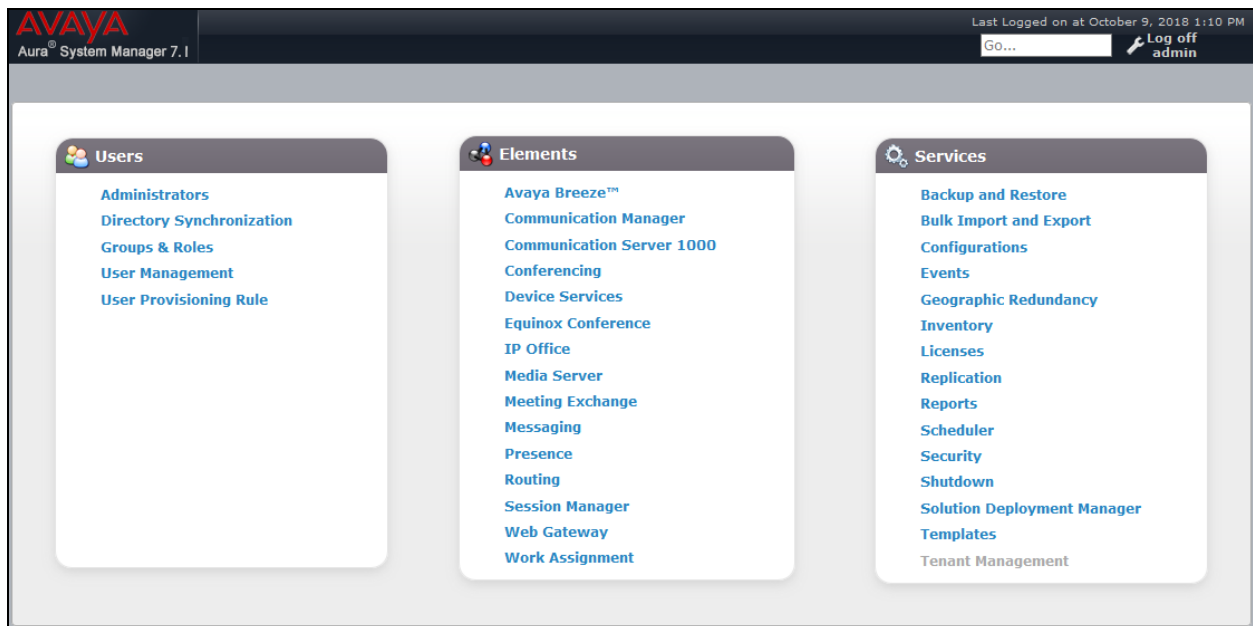
Feature (License Keyword)	Expiration date	Licensed capacity
Unified CC API Desktop Edition VALUE_AES_AEC_UNIFIED_CC_DESKTOP	permanent	1000
CVLAN ASAI VALUE_AES_CVLAN_ASAI	permanent	16
Device Media and Call Control VALUE_AES_DMCC_DMC	permanent	1000
AES ADVANCED SMALL SWITCH VALUE_AES_AEC_SMALL_ADVANCED	permanent	3
DLG VALUE_AES_DLG	permanent	16
TSAPI Simultaneous Users VALUE_AES_TSAPI_USERS	permanent	1000
AES ADVANCED LARGE SWITCH	permanent	3

7. Configure Avaya Aura® Session Manager

During the compliance test, incoming Emergency Calls to Session manager were routed via SIP from Inform 911 server. Though SIP interoperability was not the scope of this test, this section details the configuration performed for SIP connectivity to Inform 911 server. A SIP trunk was created on Session Manager to communicate to Inform 911 server.

Configuration for Session Manager is performed via System Manager. Log on the System Manager web console via a web browser; <https://<IP-Address>> where IP-Address is the IP Address of System Manager.

Once logged on, select **Routing** under **Elements** sub-section.



On the left pane, select **SIP Entities** and select **New** (not shown) to create a SIP Entity for Inform 911 server. Screen capture below displays the SIP Entity and SIP Entity Link that was created during the compliance test.

AVAYA
Aura® System Manager 7.1

Last Logged on at October 9, 2018 1:10 PM

Go... Log off admin

Home Routing

Home / Elements / Routing / SIP Entities

SIP Entity Details

Commit Cancel

General

* Name: Tritech

* FQDN or IP Address: 192.168.120.44

Type: SIP Trunk

Notes:

Adaptation:

Location:

Time Zone: America/Denver

* SIP Timer B/F (in seconds): 4

Minimum TLS Version: Use Global Setting

Credential name:

Securable: ☐

Call Detail Recording: egress

Entity Links

Override Port & Transport with DNS SRV: ☐

Add Remove

1 Item Filter: Enable

	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Deny New Service
<input type="checkbox"/>	*asm_Tritech_5060_TCP	asm	TCP	*5060	Tritech	*5060	trusted	<input type="checkbox"/>

Select : All, None

SIP Responses to an OPTIONS Request

Add Remove

0 Items Filter: Enable

	Response Code & Reason Phrase	Mark Entity Up/Down	Notes
--	-------------------------------	---------------------	-------

Commit Cancel

Continuing from above, select **Dial Patterns** and select **New** to add a new dial pattern. This dial pattern was used to route calls from Inform 911 server to Communication Manager. During the compliance test, the VDN configured in **Section 5.7** was dialed by CO emulator on Inform 911 server. The screen capture below displays the dial pattern that was used during the test.

AVAYA
Aura® System Manager 7.1

Last Logged on at October 9, 2018 1:10 PM

Home / Elements / Routing / Dial Patterns

Dial Pattern Details [Commit](#) [Cancel](#) [Help ?](#)

General

* Pattern:

* Min:

* Max:

Emergency Call: ☐

Emergency Priority:

Emergency Type:

SIP Domain:

Notes:

Originating Locations and Routing Policies

[Add](#) [Remove](#)

1 Item [Filter: Enable](#)

<input type="checkbox"/>	Originating Location Name ▲	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	DevConnect		cm71	0	<input type="checkbox"/>	acm71	

Select : All, None

8. Configure TriTech Inform 911™

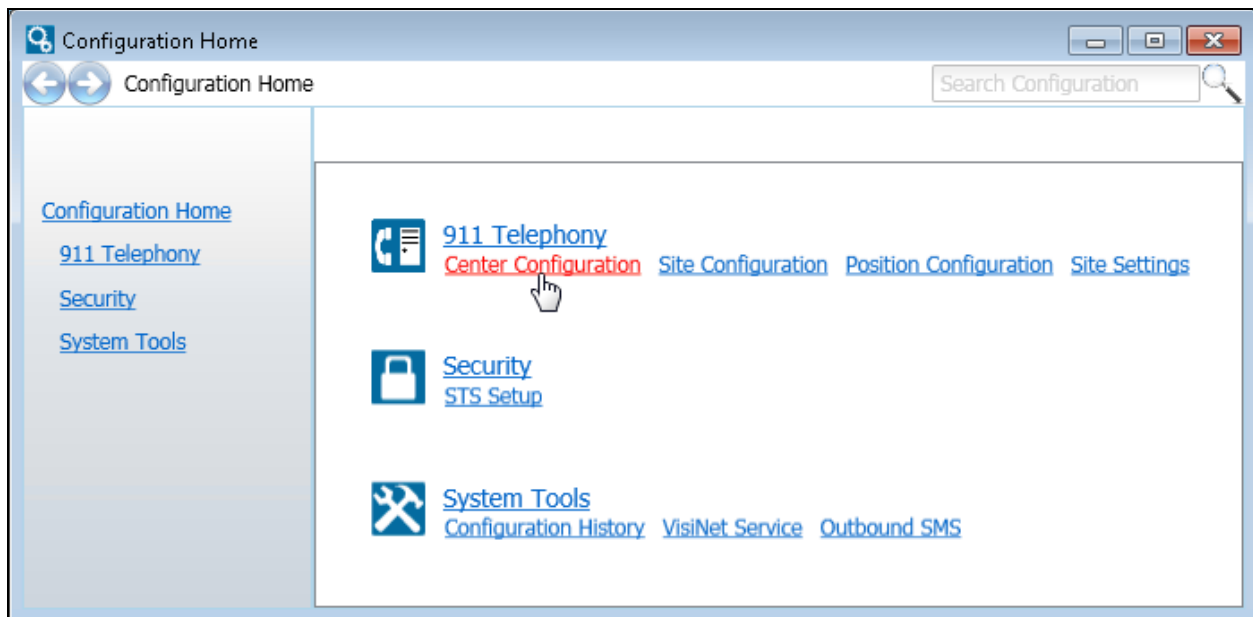
Configuration in this section is performed by TriTech engineers. Following information is for informational and reference purposes only. Configuration information in this section does not necessarily match the compliance tested configuration.

Note: The configuration in this section was provided by TriTech.

8.1. Configure Test Center

To Configure Centers, Sites, Connections and Positions information, start one of the installed Inform 911 workstations. From the **Tools** menu, select **Configuration Utility** (not shown).

The Configuration Home application will appear and display the menu of configuration options.



Select **Center Configuration** from the menu. Enter a center **Identity** and **Name**. The identifier will be used in other configurations. The name is for descriptive use. The center is not controlled in the server applications so these values can contain any values.

The screenshot shows a web browser window titled "Telephony Center Configuration". The breadcrumb navigation at the top reads "Configuration Home > 911 Telephony > Center Configuration". A search bar labeled "Search Configuration" is in the top right corner. On the left, a sidebar contains a list of links: "Configuration Home", "911 Telephony", "Center Configuration" (which is highlighted), "Position Configuration", "Site Configuration", "Site Settings", "Security", and "System Tools". The main content area is titled "911 Telephony Center Configuration" and includes the instruction "Use this utility to configure the telephony centers." Below this, it says "Select a center to edit or create a new center by entering the values below." A dropdown menu currently shows "Inform911". Below the dropdown, there are two text input fields: "Identify this center as" with the value "Inform911" and "Name this center as" with the value "Inform911 Name". At the bottom right of the form are three buttons: "Delete", "Save", and "Cancel".

8.2. Configure Test Site

Select **Site Configuration** from the menu. Select the **Center** configured above and type an **Identity** and **Name**. This must be done before configuring QRConnect. QRConnect is an internal component of Inform 911 that is used for connectivity to AES.

The screenshot shows a web application window titled "Telephony Site Configuration". The breadcrumb navigation at the top reads "Configuration Home > 911 Telephony > Site Configuration". A search bar on the right is labeled "Search Configuration".

On the left is a sidebar menu with the following links: [Configuration Home](#), [911 Telephony](#), [Center Configuration](#), [Position Configuration](#), [Site Configuration](#) (which is highlighted), [Site Settings](#), [Security](#), and [System Tools](#).

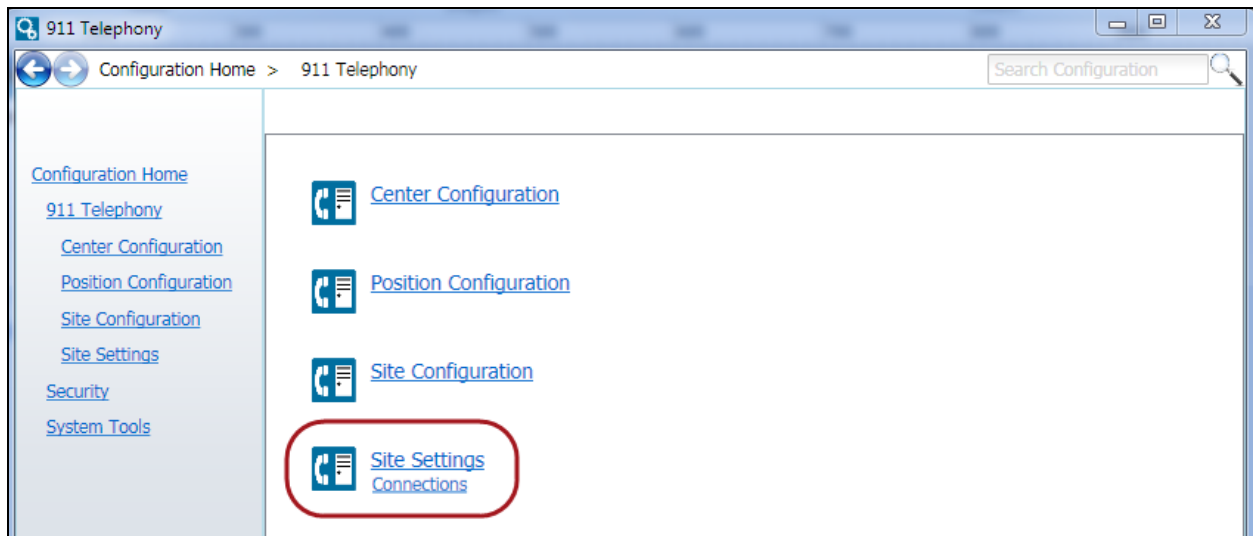
The main content area is titled "911 Telephony Site Configuration" and contains the following text: "Use this utility to configure the telephony sites. Select a site to edit or create a new site by entering the values below." Below this text is a dropdown menu currently showing "Inform911".

There are two text input fields: "Identify this site as" with the value "SDLab41" and "Name this site as" with the value "SDLab41 Name".

At the bottom right of the main area are three buttons: "Delete", "Save", and "Cancel".

8.3. Configure Site Connections

From the **Configuration Home**, select **Site Settings Connections**.



Select the **Center** and **Site** from the dropdown lists or click on the applicable item in the grid.

Configuration Home > 911 Telephony > Site Settings > Connections

Search Configuration

[Configuration Home](#)
[911 Telephony](#)
[Center Configuration](#)
[Position Configuration](#)
[Site Configuration](#)
[Site Settings](#)
[Connections](#)
[Security](#)
[System Tools](#)

911 Telephony Connections Configuration

Use this utility to configure the site connections to the telephony system. Enter the connection address and port for each center and site.

Center	Site	Remote Machine	Port	Interface
Inform911	AgSite	192.168.17.15	911	Asterisk
Inform911	TritechSD	192.168.17.201	911	Asterisk
Inform911	SDLab41	192.168.17.201	911	Avaya
Inform911	SidDev	192.168.100.141	911	Asterisk
Inform911	KentDev	10.99.3.120	911	Asterisk
Inform911	ENGINEERING	10.99.17.122	911	Asterisk
Inform911	ControlMain	192.168.17.15	911	Asterisk

Center: Inform911 Name

Site: SDLab41 Name

Remote Machine: 192.168.17.201

Port: 911

Telephony System Interface:
☒ Avaya ☐ SoftSwitch

New Connection Delete Connection Save Cancel

Continuing from above, select the option for the applicable **Telephony System Interface** type, **Avaya** in this case. This should match the value as configured in **Section 8.5.1** in the QRConnect application.

911 Telephony Connections Configuration

Use this utility to configure the site connections to the telephony system. Enter the connection address and port for each center and site.

Center	Site	Remote Machine	Port	Interface
Inform911	AgSite	192.168.17.15	911	Asterisk
Inform911	TritechSD	192.168.17.201	911	Asterisk
Inform911	SDLab41	192.168.17.201	911	Avaya
Inform911	SidDev	192.168.100.141	911	Asterisk
Inform911	KentDev	10.99.3.120	911	Asterisk
Inform911	ENGINEERING	10.99.17.122	911	Asterisk
Inform911	ControlMain	192.168.17.15	911	Asterisk

Center: Inform911 Name

Site: SDLab41 Name

Remote Machine: 192.168.17.201

Port: 911

Telephony System Interface:
☒ Avaya ☐ SoftSwitch

New Connection Delete Connection Save Cancel

From the **Configuration Home**, select **System Tools → Options** (not shown).

- Enter the Inform 911 server IP Address in the **Bind Listening TCP/IP address**.
- Enter the **Listening Port** as configured on Inform 911 server.

Options

General | System | ALI Formats | ALI Steering | Timers | Clocks | Interface Ports | Positions | Wireless | Alarms

Site Settings
Global Settings

Display Options

Activity Log Color Scheme: ☐ Black On White ☒ Green On Black

Workstation Clients

Listening Port: 911

Bind Listening TCP/IP address: 192.168.17.201

CTI API Clients

Listening Port: 1088

Bind Listening TCP/IP address: 192.168.17.201

Call Options

☒ Server manages auto abandoned clearing

☐ Apply dialplan rules at server (for all sites)

Reporting

☒ Create IQSubmit report files

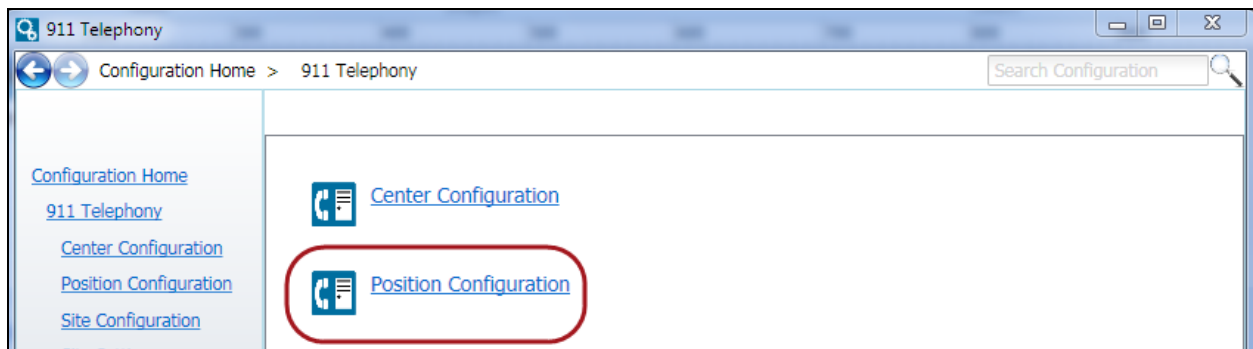
SMS

☐ Create a CallNote for each SMS

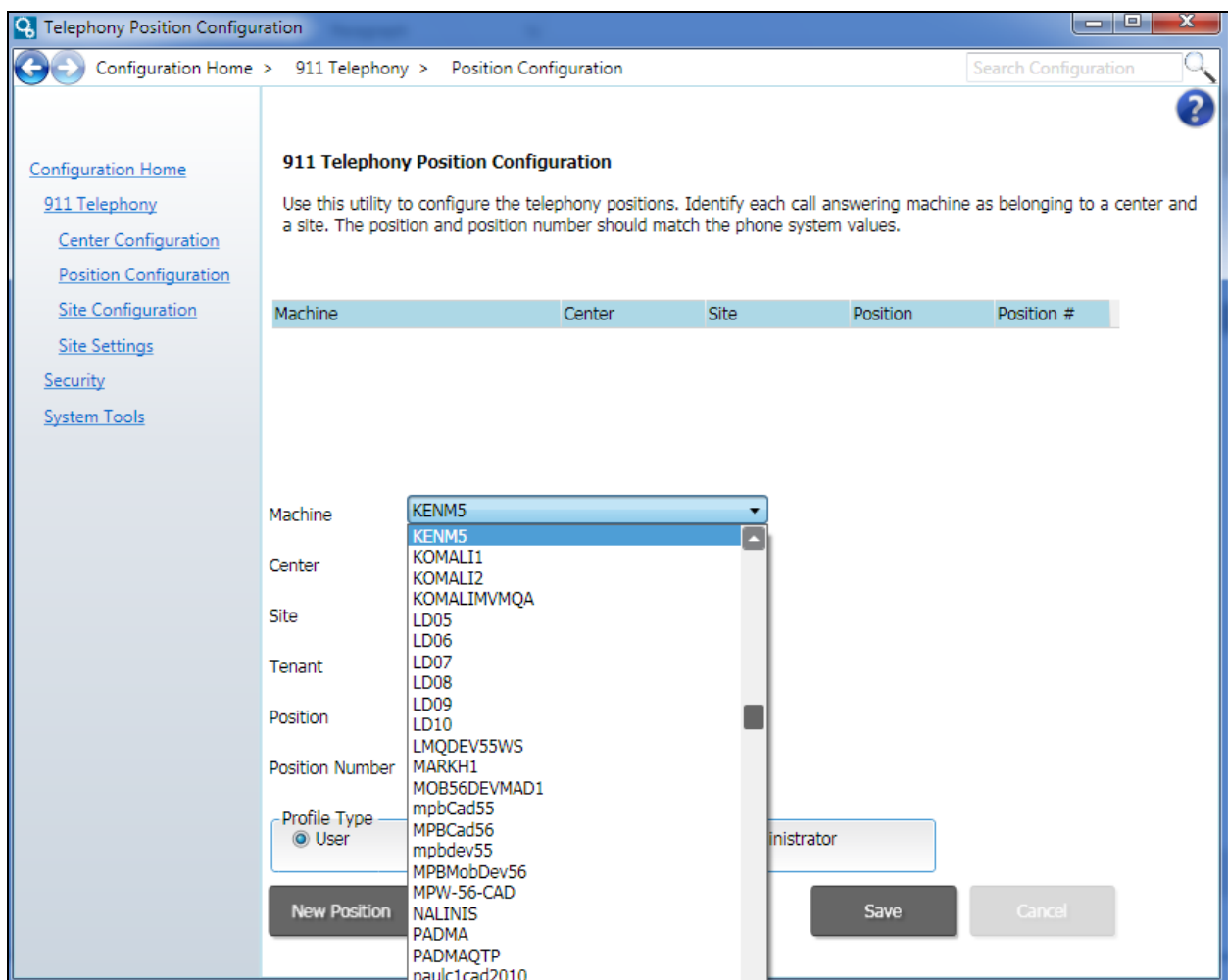
OK Cancel

8.4. Configure Positions

To configure positions, select **Position Configuration** from **Configuration Home**.



Select the workstation machine ID, which is the hostname of the workstation, from the **Machine** drop-down list.



Continuing from above, select the position's **Center** and **Site** values from the drop-down lists, as configured in **Section 8.1** and **Section 8.2**, respectively.

Telephony Position Configuration

Configuration Home > 911 Telephony > Position Configuration

Search Configuration

[Configuration Home](#)

[911 Telephony](#)

[Center Configuration](#)

[Position Configuration](#)

[Site Configuration](#)

[Site Settings](#)

[Security](#)

[System Tools](#)

911 Telephony Position Configuration

Use this utility to configure the telephony positions. Identify each call answering machine as belonging to a center and a site. The position and position number should match the phone system values.

Machine	Center	Site	Position	Position #
---------	--------	------	----------	------------

Machine: KENM5

Center: Inform911

Site: SDLab41

Tenant: TriTech

Enter the **Tenant**. This identifier represents a group where the site resides and can be any value.

Tenant: TriTech

Position: 1001

Position Number: 1

Enter the **Position Number** identifier. This must match the station's **Pos #** value as configured in **Section 8.5.4**, in QRConnect application. **Profile Type** is left to its default value.

Position: 1001

Position Number: 1

Profile Type: ☒ User ☐ Supervisor ☐ Administrator

8.5. Configure QRConnect

QRConnect is an internal component of Inform 911 that is used for connectivity to AES. It runs on Inform 911 server. Open the QRConnect application to configure as mentioned in this section.

8.5.1. Setup TSAPI and DMCC Connections

To configure TSAPI and DMCC connectivity to AES, select the **Connections** tab. Configure as follows:

- **TSAPI CTI Link # 1:** Tlink obtained from **Section 6.4**.
- **AES IP Addr #1:** IP Address of AES.
- **Tsapi Login** and **Tsapi Password:** As configured in **Section 6.3**.
- **CM IP Addr:** IP Address of Communication Manager.
- Check box for **Enable DMCC Caller ID** to enable DMCC connections.
- **DMCC Port:** Default DMCC port 4721.
- **DMCC Login** and **DMCC Password:** As configured in **Section 6.3**.
- **Phone System → Type:** Set to **Avaya**.
- **Station Password:** As configured in **Section 5.5**.

Note: If using a dual-AES setup, check the box for a second AES and enter its TSAPI server name. All enabled AES connections will maintain a constant connection, sending and receiving TSAPI events and requests.

The screenshot shows the 'QRConnect Options' dialog box with the 'Connections' tab selected. The 'AES Connections' section contains fields for 'TSAPI CTI Link #1' (AVAYA#GLYCERIN#CSTARLABAES), 'AES IP Addr #1' (192.168.17.6), 'Use TSAPI CTI Link #2' (unchecked), 'TSAPI Login' (e911), 'TSAPI Password' (masked), 'CM IP Addr' (192.168.17.11), 'DMCC Port' (4721), 'DMCC Login' (e911), 'DMCC Password' (masked), 'DMCC Instance' (0), and 'Station Password' (1234). The 'Phone System' section shows 'Type' set to 'Avaya' and 'Auto-Start Phone Service' checked. The 'Server Connections' section includes 'Server Listener' (checked), 'IP Address' (10.1.10.162), 'Port' (5038), 'Proxy #2' (unchecked), 'Proxy Username' (admin), 'Proxy Password' (masked), 'Send Error after no connection for' (120), 'Secs (60-3600)', 'Call-Taker TDD Volume (%)' (50), 'Bind all Socket connections to this IP' (10.1.10.31), and 'TDD volume only applies to internal trunks identified to the right for Avaya'. The 'Internal Trunks' section is empty. The 'Cancel' and 'Save' buttons are at the bottom right.

8.5.2. Configure the Site

To configure Site, select the **Site** tab. The site entered here must match the site that was configured in **Section 8.2**. The **Add** button will add a site to the site table.

- **Site Name:** Enter the name of the site.
- **Call Distribution Type:** Select **ACD**.
- **Default Call Distribution:** Select **Bridge**.
- Keep the defaults for the remaining options.

The screenshot shows the 'QRConnect Options' dialog box with the 'Site' tab selected. The 'Site specific settings' table lists two sites: 'SDLab41' and 'SDLab41_2', both with 'ACD' as the 'Call Distribution Type'. The 'ACD' value for 'SDLab41' is highlighted in blue. To the right, the 'Settings for all sites' section shows 'Default Call Distribution' set to 'Bridge' and 'Default DTMF type' set to 'Audiocodes'. Below this, the 'Greetings' section shows 'Record Extension' as 5551 and 'Playback Extension' as 5552. The 'Optional Features' section has several checked options: 'Abandoned Call if hangup while Park, Held', 'Disconnect if CTI requests for State=None event', 'Dmcc Logoff notification - by Dependent mode regi', 'Incoming call if extension calls VDN', 'Retry Failed Park on different Park Extension', and 'Transfer CallerId with Admin transfers'. The 'Add' and 'Delete' buttons are at the bottom left of the site table.

Site Name	Call Distribution Type
SDLab41	ACD
SDLab41_2	ACD

Settings for all sites

Defaults

Default Call Distribution: Bridge

Default DTMF type: Audiocodes

Greetings

Record Extension: 5551

Playback Extension: 5552

Optional Features

- ☒ Abandoned Call if hangup while Park, Held
- ☒ Disconnect if CTI requests for State=None event
- ☒ Dmcc Logoff notification - by Dependent mode regi
- ☒ Incoming call if extension calls VDN
- ☐ Park, BlindXfer use SingleStepXfer (not recommend
- ☒ Retry Failed Park on different Park Extension
- ☐ Transfer CallerId with Admin transfers

Add Delete

8.5.3. Configure the VDN

The VDN screen is where one configures an incoming VDN for monitoring. The VDN number entered here must match the VDN number that was configured on Communication Manager. The site name selected here must also match the site name that was configured in **Section 8.2** of this document.

- **VDN:** Enter the VDN number as configured in **Section 5.7**.
- **Monitor:** Check the box.
- **Desc:** Enter a text description of the VDN.
- **Site:** Select the site created in **Section 8.5.2** of this document.
- **EmergT:** Select **911**.
- **SourceT:** Select **Land**.
- **HF Type:** Select **AudioCodes**.
- **DTMF Type:** Select **Tsapi**.

VDN	Monit	Desc	Site	EmergT	SourceT	HF Type	DTMF T	Line Type	OutgAnyDis	IncomNoneDis	BrdgSta	TG	Mbr	Routing VDN	Routin
4100	<input checked="" type="checkbox"/>	4.1 911 SCD	SidDev	911	Land	AudioCodes	Tsapi	Other	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>					

VDN: The extension of this VDN. For true VDN, must use actual extension.
For unmonitored Trunk Groups can use any number not in use.

Only VDN's renamed from 0000 will be saved.

8.5.4. Configure the Stations

The stations screen is where station extensions are configured for monitoring. The station numbers entered here must match the station extension numbers that were configured in Communication Manager, **Section 5.4**. Each station must be entered on a separate line. Use the **Add** button to add additional stations. The station descriptions entered here must match the position names entered in **Section 8.4** of this document.

- **Station:** Enter station extension as configured in Communication Manager, **Section 5.5**.
- **Monitor:** Check the box.
- **Dmcc:** Check the box.
- **Desc:** Enter the station description.
- **Site:** Select the site created in **Section 8.5.2** of this document.
- **Pos #:** Enter station extension as configured in Communication Manager, **Section 5.5**.

QRConnect Options

Connections VDN Stations Site ACD Timing SMS Options Call Prioritization

Station	Monit	Dmcc	Desc	Site	Pos #
4003	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Lab Station	AgSite	4003
4004	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	4004	AgSite	4004
4201	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Console 1	SidDev	4201
4202	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Console 2	SidDev	4202
4203	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Console 3	SidDev	4203
4204	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Console 4	SidDev	4204

Dmcc: Register this station on DMCC. This uses a DMCC license.
If you do not register with DMCC you cannot get enhanced caller ID (admin calls), and you will not be able to issue Hookflash on admin lines (only CAMA trunks), an

Add Delete Only monitored Stations will be saved. If you do not monitor them, they last only for the current session.

Add Positions and half positions, not Bridge stations.

Cancel Save

9. Verification Steps

The following steps may be used to verify the configuration:

9.1. Verify Avaya Aura® Communication Manager

Log on to SAT interface:

- Verify that the interface on Communication Manager to Application Enablement Services is enabled and in **listening** status (use the **status aesvcs interface** command on the Communication Manager SAT).
- Verify that the link between Communication Manager and Application Enablement Services is transmitting and receiving messages (use the **status aesvcs link** command on the SAT).

9.2. Verify Avaya Aura® Application Enablement Services

Via the AES OAM Web interface:

- Verify that the **conn state** of the Switch Connection is **talking** (on Application Enablement Services web page, navigate to **Status → Status and Control → Switch Conn Summary**).
- Verify that the **service state** of the CTI link is **established** (use the **status aesvcs cti-link** command on the SAT).
- Verify that the Inform 911 recording ports are registered as **IP_API_A** stations in Communication Manager (use the **list registered-ip-stations** command on the SAT).
- Verify the Inform 911 server has successfully monitored the stations using TSAPI (use the **list monitored-stations** command on the SAT).
- Verify that calls may be successfully completed to and from stations and VDN. Verify that Inform 911 is able to monitor the VDN.

9.3. Verify TriTech Inform 911™

- Verify the correct version number of the Workstation via the About box in the Tools menu.
- Verify that the status bubbles in the lower right-hand corner of the Workstation GUI are all Green.
- Verify that the Status bubbles at the bottom of the QRConnect window are all Green.

10. Conclusion

These Application Notes describe the procedures for configuring TriTech Inform 911 with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services. All feature and serviceability test cases were completed and passed.

11. Additional References

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

1. *Administering Avaya Aura® Communication Manager*, Release 7.1.2, Issue 5, July 2018.
2. *Administering and Maintaining Avaya Aura® Application Enablement Services*, Release 7.1.2, Issue 4, December 2017.

Product documentation related to Inform 911 can be obtained directly from TriTech.

©2018 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.