



DevConnect Program

Application Notes for SSS Public Safety Limited Centricity with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for SSS Public Safety Limited Centricity 3.4.2 to interoperate with Avaya Aura® Communication Manager R10.1 and Avaya Aura® Application Enablement Services R10.1 using the TSAPI and SMS interface. SSS Public Safety Centricity is a CTI middleware platform that provides call control and monitoring functionality through various application programming interfaces to end user applications.

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.

1. Introduction

These Application Notes describe the configuration steps required for SSS Public Safety Centricity 3.4.2 to interoperate with Avaya Aura® Communication Manager R10.1 and Avaya Aura® Application Enablement Services R10.1 using the Telephony Service Application Programming Interface (TSAPI) and the System Management Service (SMS) Web Service. Centricity is a CTI Middleware server used by the SSS Public Safety portfolio of products to interface with Avaya telephony solutions via Avaya Aura® Application Enablement Services (AES).

SSS Public Safety Centricity implements TSAPI to provide Computer Telephony Integration (CTI) call control and monitoring functionality and application programming interfaces to end user business applications. Centricity also uses the SMS connection to obtain information from Avaya Aura® Communication Manager such as a list of agents, VDNs, extensions and other information to store in its database. For compliance testing a freeware test harness called Postman was used in the absence of any specific client. Postman is an API platform for building and using APIs. Postman connects to the Centricity server to obtain all the caller information.

Centricity is an integrator system that enables telephony integration for simple monitoring of agent and call control at a supported handset or endpoint device. The Centricity server connects to the AES using the SMS connection and the TSAPI TLink on a dedicated user account. It monitors VDN's, endpoint devices and skills in order to receive real time events for call activity as well as obtaining agent information. Deployed as a server, it becomes a centralized data hub for the unified communications platform making real time information available to listening connections and facilitating control requests from connected systems. Deployed as a client, it provides a CTI bridge from the SSS Public Safety desktop client onto the AES to allow an Agent to log on, change state, and exercise call control.

Centricity along with other SSS Public Safety products make up a solution set that can be deployed in various designs and architectures to suit the customer contact enterprise. The SSS Public Safety Centricity solution has been in extensive use in Emergency Service Contact Centers since 2006 handling mission critical data for critical front-line systems supporting patients in 999 and 111 services. The system comes with a variety of tools that provide audit and analysis of the data captured and handled by the Centricity system that is held in its database.

2. General Test Approach and Test Results

The general test approach was to validate the ability of Centricity to connect to Application Enablement Services and handle and control various Communication Manager endpoints in a variety of call scenarios. Agents were logged into an agent desktop, in this case 'Postman' provided by SSS Public Safety for testing the Centricity product. Each agent was assigned to a specific Avaya endpoint, a SIP and H.323 endpoint was used during compliance testing. Calls were made to and from these endpoints using Postman to make and receive calls.

Centricity makes use of the TSAPI protocol in AES and the AES requires 'Basic licensing' to support basic features and call monitoring supported methods.

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 SSS Public Safety Centricity did not include use of any specific encryption features as requested by SSS Public Safety.

2.1. Interoperability Compliance Testing

Interoperability compliance testing consisted of using Centricity to verify successful handling and control of a variety of endpoints as follows:

- Assign and un-assign on devices and call monitor channels
- Agent Log In/Log Out using Postman
- Set Status for ACD Agents
- Agent State Synchronization with Agent Telephones
- Hold/Unhold
- Transfers: Blind and Supervised
- Conferencing: Blind and Supervised
- Calls from Agent to Agent
- Calls from Agent to Non-Agent
- Serviceability Testing

2.2. Test Results

All test cases were executed successfully, with the following observations:

1. Postman was used instead of a specific client. This is a "test harness" that executed the TSAPI commands in the similar manner to that of any client.
2. There were some intermittent SMS connection errors that surfaced when the Centricity services were restarted or when the Centricity server was rebooted. An SMS connection error showed "Connection Failed: All available connections are in use. Try again later." Avaya has identified the issue and a fix will be included in the next release of Application Enablement Services.

2.3. Support

For resolution of technical issues on SSS Public Safety telephony products, please email the SSS Public Safety service desk, sss.servicedesk@sss-publicsafety.com. For general enquiries, please speak with your dedicated Service Line Manager.

3. Reference Configuration

Figure 1 below shows Avaya Aura® Communication Manager serving both SIP and H.323 endpoints with Avaya Aura® Application Enablement Services providing a TSAPI interface to which the SSS Public Safety Centricity application connects to. Avaya Aura® Session Manager provides the point of registration for Avaya SIP endpoints. Avaya Aura® System Manager provides a means to manage and configure Session Manager. An SMS connection to AES provides the means to list various components on Avaya Aura® Communication Manager.

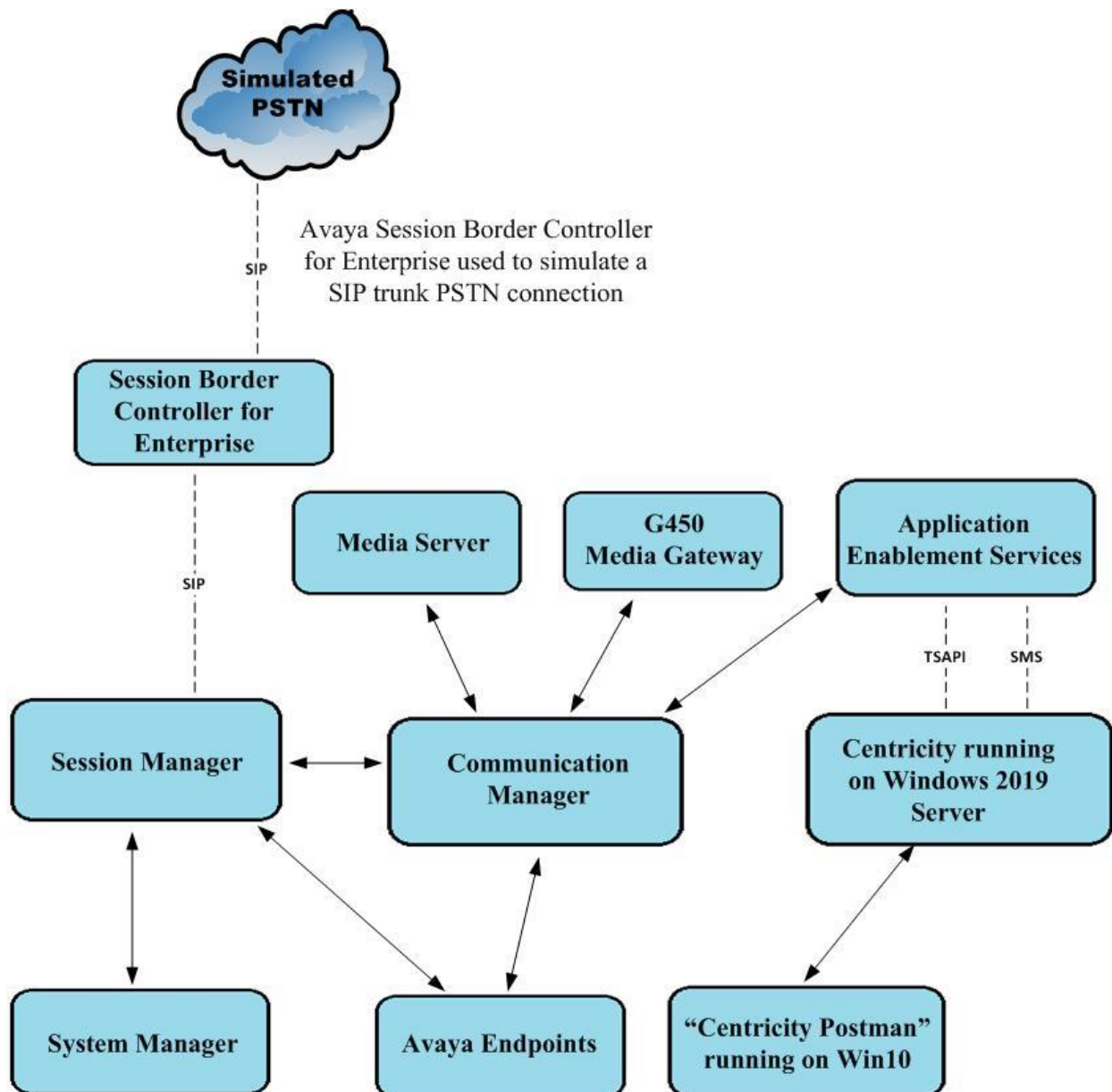


Figure 1: Connection of SSS Public Safety Centricity with Avaya Aura® Communication Manager R10.1 and Avaya Aura® Application Enablement Services R10.1

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya Aura® System Manager	System Manager 10.1.0.2 Build No. – 10.1.0.0.537353 Software Update Revision No: 10.1.0.2.0715160 Service Pack 2
Avaya Aura® Session Manager	Session Manager R10.1 Build No. – 10.1.0.2.1010219
Avaya Aura® Communication Manager	R10.1.0.2.0 – SP2 R020x.01.0.974.0 Update ID 01.0.974.0-27607
Avaya Aura® Application Enablement Services	10.1.0 Build 10.1.0.2.0.12-0
Avaya Aura® Media Server	10.1.0.101
Avaya Media Gateway G430	42.7.0 /2
Avaya 9404 Digital	17.0
Avaya J100 Series SIP	7.1.2.0.14
Avaya J100 Series H323	7.0.14.0.7
Avaya Session Border Controller for Enterprise (to facilitate simulated PSTN)	10.1.0
SSS Public Safety Equipment	Release/Version
SSS Public Safety Centricity	V3.4.2
SSS Public Safety Postman TSAPI Client	V10.1.2 V8.1

All equipment are virtual servers running on VMware.

5. Configure Avaya Aura® Communication Manager

The configuration and verification operations illustrated in this section are performed using the Communication Manager System Access Terminal (SAT). The information provided in this section describes the configuration of Communication Manager for this solution. For all other provisioning information such as initial installation and configuration, please refer to the product documentation as referenced in **Section 10**. The configuration operations described in this section can be summarized as follows:

- Configure TSAPI Interface to Avaya Aura® Application Enablement Services
- Configure Call Center Features
- Configure Avaya SIP Endpoints for Third Party Call Control
- Configure Avaya Aura® Communication Manager user for SMS

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

The following sections illustrate the steps required to create the TSAPI link between Communication Manager and Application Enablement Services. It is assumed that the switch link (IP Services Interface) between Communication Manager and Application Enablement Services has already been setup as part of the installation of Application Enablement Services.

5.1.1. Verify System Features

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

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

5.1.2. Configure CTI Link for TSAPI Service

Add a CTI link using the **add cti-link n** command, where n is the n is the cti-link number as shown in the example below this is **1**. Enter an available extension number in the **Extension** field. Enter **ADJ-IP** in the **Type** field, and a descriptive name in the **Name** field. Default values may be used in the remaining fields.

add cti-link 1		Page 1 of 3
CTI LINK		
CTI Link: 1		
Extension: 1990		
Type: ADJ-IP		
Name: aespri101x		
		COR: 1

5.2. Configure Call Center Features

The following were set to allow inbound ACD calls to the Agents logged into Centricity.

- Configure Hunt Group
- Configure Vector
- Configure Vector Directory Number (VDN)
- Configure Agents

5.2.1. Configure Hunt Group

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

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

add hunt-group 90		Page 1 of 4
HUNT GROUP		
Group Number: 90		
Group Name: Sales		
Group Extension: 1800		
Group Type: ucd-mia		
TN: 1		
COR: 1		
Security Code:		
ISDN/SIP Caller Display:		
Queue Limit: unlimited		
Calls Warning Threshold: Port:		
Time Warning Threshold: Port:		
		ACD? y
		Queue? y
		Vector? y
		MM Early Answer? n
		Local Agent Preference? n

On **Page 2**, set **Skill** to **y**.

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

5.2.2. Configure Vector

Enter the command **change vector x** where **x** is the required vector number. Configure as shown below so that calls **queue-to skill 1st**. Skill 1st is the hunt group configured in the VDN in **Section 5.2.3**.

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

5.2.3. Configure Vector Directory Number (VDN)

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

- **Extension** – note the VDN extension number which will be used to place calls to the Skill vector and on to the Skill.
- **Name** – enter an appropriate name.
- **Destination** – enter the **Vector Number** configured in the previous section.
- **1st Skill** – enter the hunt group created in **Section 5.2.1**.

add vdn 1900	Page 1 of 3
VECTOR DIRECTORY NUMBER	
Extension: 1900	Unicode Name? n
Name*: Sales	
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*: 90
	2nd Skill*:
	3rd Skill*:
SIP URI:	
* Follows VDN Override Rules	

5.2.4. Configure Agents

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

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

add agent-loginID 1401		Page 1 of 2
AGENT LOGINID		
Login ID: 1401		Unicode Name? n AAS? n
Name: Agent One		AUDIX? n
TN: 1	Check skill TNs to match agent TN? n	
COR: 1		
Coverage Path:	LWC Reception: spe	
Security Code:	LWC Log External Calls? n	
Attribute:	AUDIX Name for Messaging:	
LoginID for ISDN/SIP Display? n		
Password:1234		
Password (enter again):1234		
Auto Answer: station		
AUX Agent Remains in LOA Queue: system		MIA Across Skills: system
AUX Agent Considered Idle (MIA): system		ACW Agent Considered Idle: system
Work Mode on Login: system		Aux Work Reason Code Type: system
		Logout Reason Code Type: system
Maximum time agent in ACW before logout (sec): system		
Forced Agent Logout Time: :		
WARNING: Agent must log in again before changes take effect		

On **Page 2**, enter the hunt group number configured in **Section 5.2.1** in the **SN** (Skill Number) column and enter an appropriate **SL** (skill level).

add agent-loginID 1401		Page 2 of 2
AGENT LOGINID		
Direct Agent Skill: 90		Service Objective? n
Call Handling Preference: skill-level		Local Call Preference? n
SN	RL SL	SN RL SL
1: 90	1	16:
2:		17:
3:		18:
4:		19:
5:		20:
6:		
7:		
8:		

5.3. Configure Avaya SIP Endpoints for Third Party Call Control

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

Note: The following shows changes a SIP extension and assumes that the SIP extension has been programmed correctly and is fully functioning.

System Manager

Not secure | <https://10.10.40.10/network-login/>

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

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

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

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

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

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

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

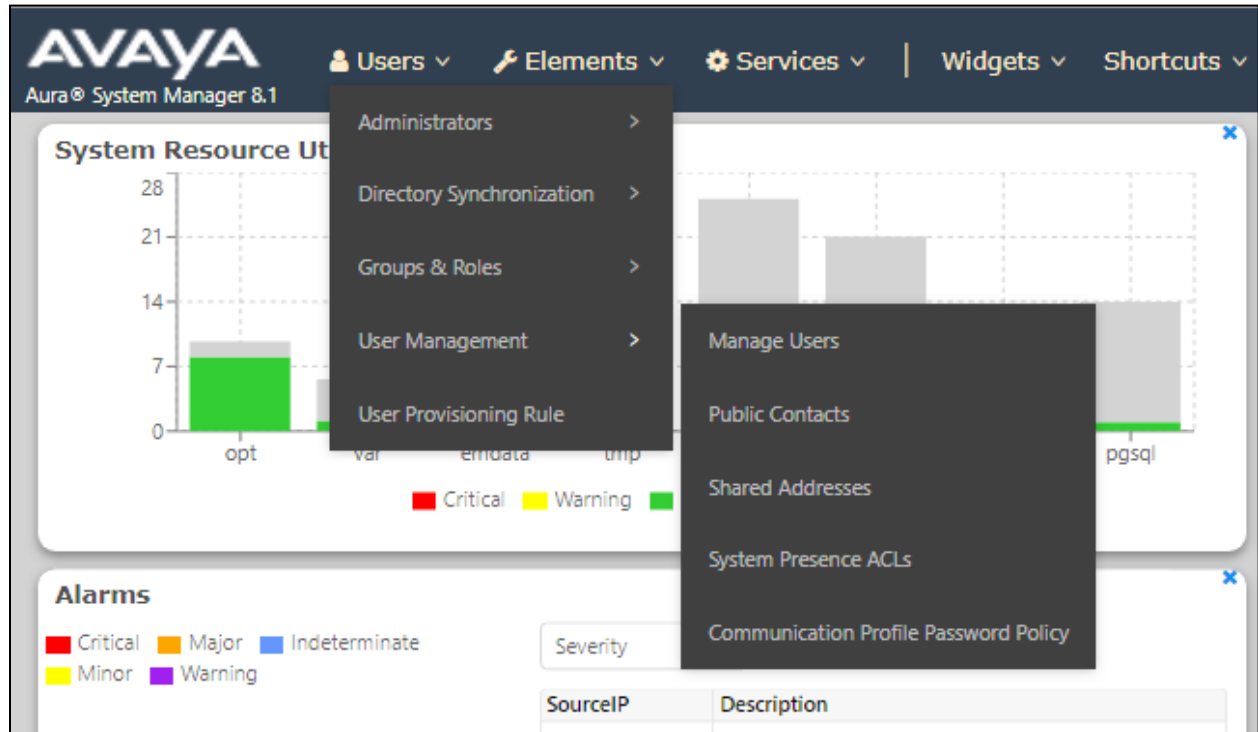
User ID:

Password:

[Change Password](#)

Supported Browsers: Firefox (minimum version 93.0), Chrome (minimum version 91.0) or Edge (minimum version 93.0).

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



Click on **Manage Users** in the left window. Select the station to be edited and click on **Edit**.

Home

User Management x

User Management

Manage Users

Public Contacts

Shared Addresses

System Presence ACLs

Communication Profile ...

Home / Users / Manage Users

Help ?

Search

View

Edit

+ New

Duplicate

Delete

More Actions

Options

	First Name	Surname	Display Name	Login Name	SIP Handle
<input checked="" type="checkbox"/>	Agent One	Workspaces	Agent One Workspaces	3101@greanep.sil6.ava ya.com	3101
<input type="checkbox"/>	Ascom	DECT_3181	DECT_3181, Ascom	3181@greanep.sil6.ava ya.com	3181
<input type="checkbox"/>	Ascom	DECT_3182	DECT_3182, Ascom	3182@greanep.sil6.ava ya.com	3182
<input type="checkbox"/>	admin	admin	Default Administrator	admin	
<input type="checkbox"/>	J179	H323	H323, J179	3001@greanep.sil6.ava ya.com	
<input type="checkbox"/>	Vantage01	K175	K175, Vantage01	3115@greanep.sil6.ava ya.com	3115
<input type="checkbox"/>	Paul	Greaney	Paul Greaney	paul@greanep.sil6.ava ya.com	
<input type="checkbox"/>	AAFD	SIP	SIP, AAFD	3111@greanep.sil6.ava ya.com	3111

Click on the **CM Endpoint Profile** tab in the left window. Click on **Endpoint Editor** to make changes to the SIP station.

Home / Users / Manage Users

User Profile | Edit | 3101@greanep.sil6.avaya.com

Commit & Continue Commit Cancel

Identity Communication Profile Membership Contacts

Communication Profile Password

PROFILE SET : Primary

Communication Address

PROFILES

Session Manager Profile ☒

Avaya Breeze® Profile ☐

CM Endpoint Profile ☒

* System : cm101x

* Profile Type : Endpoint

Use Existing Endpoints : ☐

* Extension : 3101

Template : Start typing...

* Set Type : 9641SIPCC

Security Code : Enter Security Code

Port : S000003

Voice Mail Number : 6667

Preferred Handle : Select

Calculate Route Pattern : ☐

Sip Trunk : aar

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

System cm101x

Extension 3101

Template Select

Set Type 9641SIPCC

Port S000003

Security Code

Name Agent One Workspaces

General Options (G) Feature Options (F) Site Data (S) Abbreviated Call Dialing (A) Enhanced Call Fwd (E)

Button Assignment (B) Profile Settings (P) Group Membership (M)

* Class of Restriction (COR) 1

* Emergency Location Ext 3101

* Tenant Number 1

* SIP Trunk aar

Coverage Path 1

Lock Message ☐

Multibyte Language Not Applicable

* Class Of Service (COS) 1

* Message Lamp Ext. 3101

Type of 3PCC Enabled Avaya

Coverage Path 2

Localized Display Name Agent One Workspaces

Enable Reachability for Station Domain Control system

SIP URI

Primary Session Manager

IPv4: 10.10.40.12

IPv6:

The buttons were set as shown below but these are not critical to the overall operation of Centricity. Click on **Done** at the bottom of the screen (not shown).

General Options (G) *	Feature Options (F)	Site Data (S)	Abbreviated Call Dialing (A)	Enhanced Call Fwd (E)
Button Assignment (B)	Profile Settings (P)	Group Membership (M)		

Main Buttons	Feature Buttons	Button Modules	Phone View
---------------------	-----------------	----------------	------------

Endpoint Configurations

Favorite	Button Label
1 <input type="checkbox"/>	
2 <input type="checkbox"/>	
3 <input type="checkbox"/>	
4 <input type="checkbox"/>	
5 <input type="checkbox"/>	
6 <input type="checkbox"/>	
7 <input type="checkbox"/>	
8 <input type="checkbox"/>	

Button Configurations

Button Feature	Argument-1	Argument-2	Argument-3
call-appr <input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
call-appr <input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
call-appr <input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
agnt-login <input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
auto-in <input type="text"/> auto-in Grp	<input type="text"/>	<input type="text"/>	<input type="text"/>
manual-in <input type="text"/> manual-in Grp	<input type="text"/>	<input type="text"/>	<input type="text"/>
aux-work <input type="text"/> Reason Code	<input type="text"/>	Hunt Grp <input type="text"/>	<input type="text"/>
after-call <input type="text"/> after-call Grp	<input type="text"/>	<input type="text"/>	<input type="text"/>

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

User Profile | Edit | 3101@greanep.sil6.avaya.com

Commit & Continue
Commit
Cancel

Identity
Communication Profile
Membership
Contacts

Communication Profile Password
PROFILE SET: Primary
Communication Address
PROFILES
Session Manager Profile ☒
Avaya Breeze® Profile ☐
CM Endpoint Profile ☒

* System: cm101x
* Profile Type: Endpoint

Use Existing Endpoints: ☐
* Extension: 3101

Template: Start typing...
* Set Type: 9641SIPCC

Security Code: Enter Security Code
Port: S000003

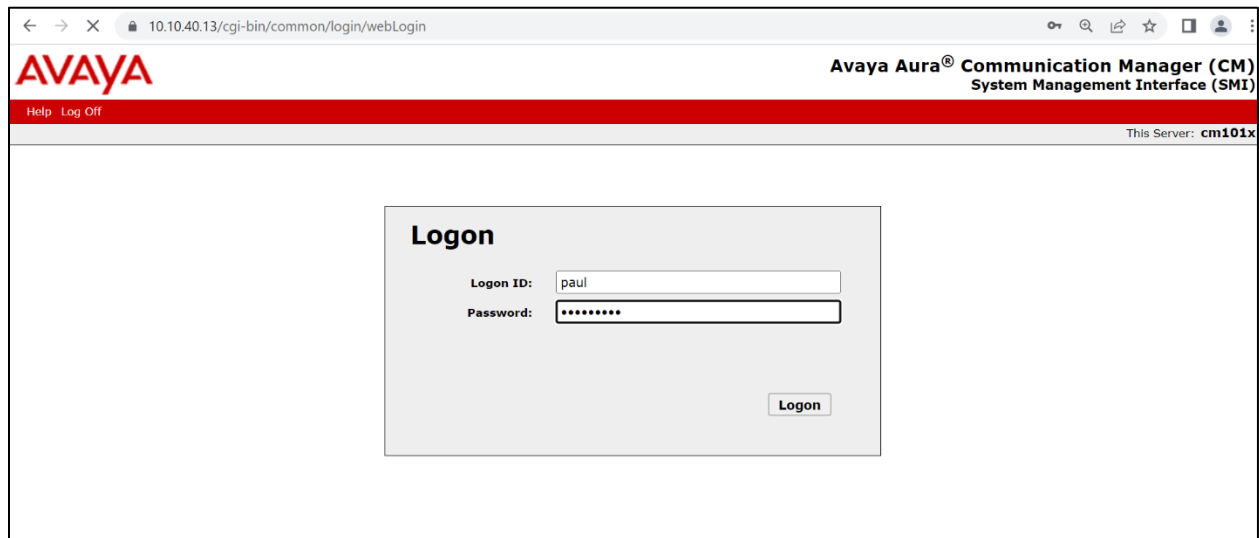
Voice Mail Number: 6667
Preferred Handle: Select

Calculate Route Pattern: ☐
Sip Trunk: aar

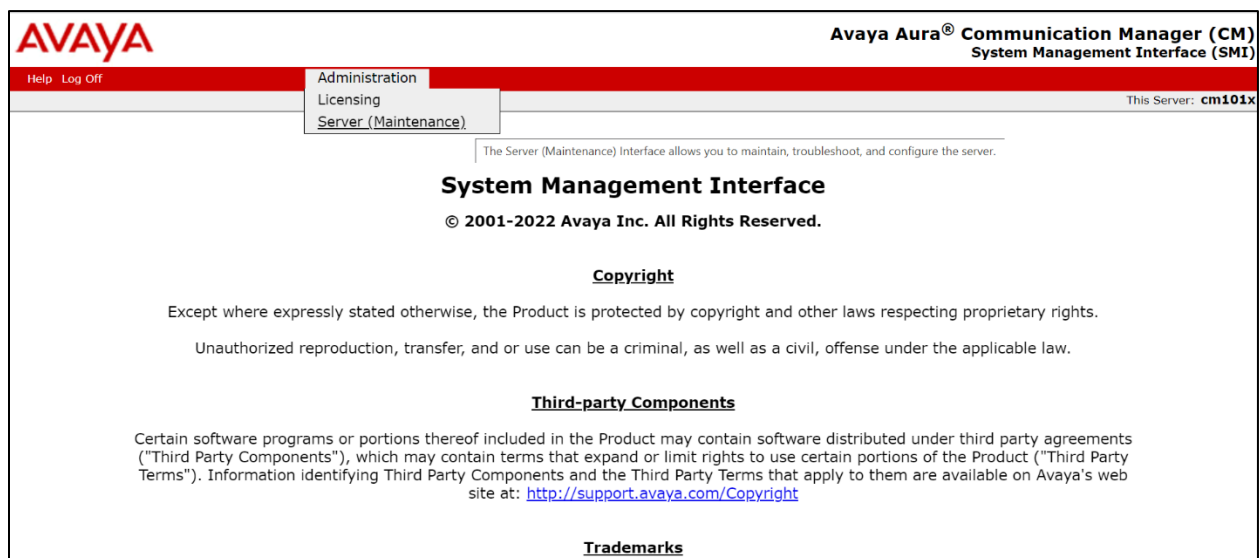
5.4. Adding a user on Avaya Aura® Communication Manager for SMS

A user on Communication Manager must be added to allow Centricity to log onto Communication Manager and list the various components. This is facilitated using a connection to the SMS on AES.

Open the web browser to Communication Manager and log in using the appropriate credentials.



Once logged in, navigate to **Server (Maintenance)** as shown below.



Navigate to **Security** → **Administrator Accounts** in the left window and select **Add Login**. For compliance testing a **Privileged Administrator** was added. Click on **Submit**.

Help Log Off

Administration

Administration / Server (Maintenance)

Alarms

Current Alarms

SNMP

Agent Status

Access

Incoming Traps

FP Traps

FP Trap Test

FP Filters

Diagnostics

Restarts

System Logs

Ping

Traceroute

Netstat

Server

Status Summary

Process Status

Shutdown Server

Server Date/Time

Software Version

Server Configuration

Server Role

Network Configuration

Static Routes

Display Configuration

Time Zone Configuration

NTP Configuration

Server Upgrades

Manage Updates

IPSI Firmware Upgrades

IPSI Version

Download IPSI Firmware

Administrator Accounts

The Administrator Accounts SMI pages allow you to add, delete, or change

Select Action:

☒ Add Login

☒ Privileged Administrator

☐ Unprivileged Administrator

☐ SAT Access Only

☐ Web Access Only

☐ CDR Access Only

☐ Business Partner Login (dadmin)

☐ Business Partner Craft Login

☐ Custom Login

☐ Change Login

Select Login

▼

☐ Remove Login

Select Login

▼

☐ Lock/Unlock Login

Select Login

▼

☐ Add Group

☐ Remove Group

Select Group

▼


Submit

Help

Enter a suitable **Login name** and the rest can be left as default. Enter a new **password** and click on **Submit** to finish.

Administrator Accounts -- Add Login: Privileged Administrator

This page allows you to add a login that is a member of the **SUSERS** group. This login has the greatest access privileges in the system next to root.

Login name	<input type="text" value="centricity"/>
Primary group	<input type="text" value="susers"/>
Additional groups (profile)	<input type="text" value="prof18"/> ▼
Linux shell	<input type="text" value="/bin/bash"/>
Home directory	<input type="text" value="/var/home/centricity"/>
Lock this account	<input type="checkbox"/>
SAT Limit	<input type="text" value="none"/> ▼
Date after which account is disabled-blank to ignore (YYYY-MM-DD)	<input type="text"/>
Enter password	<input type="password" value="....."/>
Re-enter password	<input type="password" value="....."/> 
Force password change on next login	<input type="radio"/> Yes <input checked="" type="radio"/> No

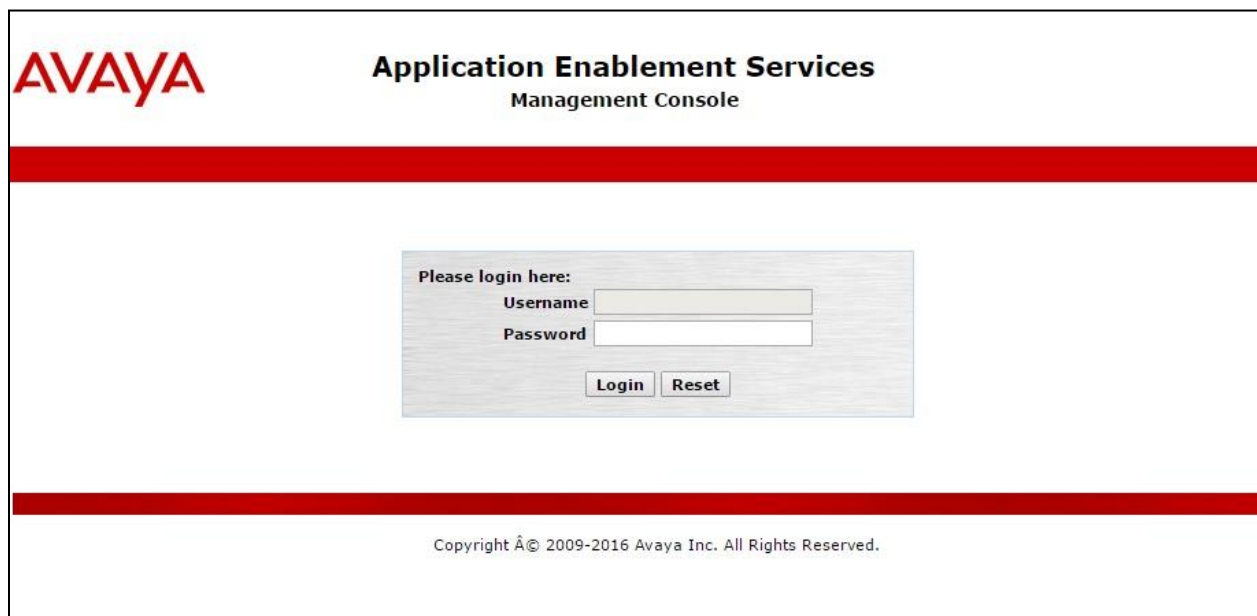
6. Configure Avaya Aura® Application Enablement Services

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

- Verify Licensing
- Administer TSAPI Link
- Identify Tlinks
- Enable TSAPI Ports
- Create CTI User
- Associate Devices with CTI User
- Configure System Management Service (SMS)
- Restart AE Server

6.1. Verify Licensing

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



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

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

The screenshot shows the 'AE Services' management console. On the left is a navigation menu with options like CVLAN, DLG, DMCC, SMS, TSAPI, TWS, Communication Manager Interface, High Availability, Licensing, Maintenance, Networking, Security, Status, User Management, Utilities, and Help. The 'Licensing' option is selected. The main content area displays the 'AE Services' status. It includes an important note: 'IMPORTANT: AE Services must be restarted for administrative changes to fully take effect. Changes to the Security Database do not require a restart.' Below this is a table with columns: Service, Status, State, License Mode, and Cause*. The table lists several services, including ASAI Link Manager, CVLAN Service, DLG Service, DMCC Service, TSAPI Service, Transport Layer Service, and AE Services HA. The TSAPI Service is shown with a status of 'ONLINE', a state of 'Running', and a license mode of 'NORMAL MODE'. Below the table, there is a link to 'Status and Control' and a note about the license information: 'You are licensed to run Application Enablement (CTI) release 8.x'.

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

The TSAPI license is a user licenses issued by the Web License Manager to which the Application Enablement Services server is pointed to. From the left window open **Licensing** and click on **WebLM Server Access** as shown below.

The screenshot shows the 'Licensing' management console. On the left is a navigation menu with options like AE Services, Communication Manager Interface, High Availability, Licensing, WebLM Server Address, WebLM Server Access, Reserved Licenses, Maintenance, Networking, Security, Status, User Management, Utilities, and Help. The 'Licensing' option is selected. The main content area displays the 'Licensing' page. It includes instructions on how to set up and maintain the WebLM, and how to import, set up, and maintain the license. It also provides information on how to administer TSAPI Reserved Licenses or DMCC Reserved Licenses. A note at the bottom states: 'NOTE: Please disable your pop-up blocker if you are having difficulty with opening this page'.

The following screen shows the available licenses for **TSAPI** users.

Application_Enablement

View by feature

View by local WebLM

Enterprise configuration

Local WebLM Configuration

Usages

Allocations

Periodic status

CE

COLLABORATION_ENVIRONMENT

COMMUNICATION_MANAGER

Call_Center

Communication_Manager

Configure Centralized Licensing

CONTROLMANAGER

Control_Manager

SESSIONMANAGER

SessionManager

SYSTEM_MANAGER

System_Manager

Uninstall license

Server properties

Metering Collector Configuration

Shortcuts

Help for Licensed products

License Summary: Avaya DevConnect Any Edition 1.5 (United States)

License Host: 00000000000000000000000000000000

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

License File Path: /etc/opt/avaya/

Feature (License Keyword)	License Capacity	Currently available
Unified CC API Desktop Edition (VALUE_AES_AEC_UNIFIED_CC_DESKTOP)	1000	1000
CVLAN ASAI (VALUE_AES_CVLAN_ASAI)	16	16
Device Media and Call Control (VALUE_AES_DMCC_DMC)	1000	1000
AES ADVANCED SMALL SWITCH (VALUE_AES_AEC_SMALL_ADVANCED)	3	3
AES ADVANCED LARGE SWITCH (VALUE_AES_AEC_LARGE_ADVANCED)	3	3
DLG (VALUE_AES_DLG)	16	16
TSAPI Simultaneous Users (VALUE_AES_TSAPI_USERS)	1000	997
Product Notes (VALUE_NOTES)	SmallServerTypes: s8300c;s8300d;icc;premio;tn8400;laptop;CtiSmallServer MediumServerTypes: ibmx306;ibmx306m;dell1950;xen;hs20;hs20_8832_vm;CtiMediumServer LargeServerTypes: isp2100;ibmx305;dl380g3;dl385g1;dl385g2;unknown;CtiLargeServer TrustedApplications: IPS_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; 1XP_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; 1XM_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; PC_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; CIE_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; OSCP_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; VP_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; SAMETIME_001, VALUE_AES_UNIFIED_CC_DESKTOP,,; CCE_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; CSI_T1_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; CSI_T2_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; AVAYAVERINT_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; CCT_ELITE_CALL_CTRL_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted, AgentEvents; ANAV_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted, AgentEvents; UNIFIED_DESKTOP_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted, AgentEvents; AACC_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; CE_AGENT_STATES_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted, AgentEvents; TP_CITFNT_001, BasicUnrestricted, . . . AgentEvents: EXT_CITFNT_001, . . .	Not counted

6.2. Administer TSAPI link

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

The screenshot shows the 'AE Services | TSAPI | TSAPI Links' interface. On the left, a sidebar lists 'AE Services' with sub-items: CVLAN, DLG, DMCC, SMS, TSAPI (expanded), TSAPI Links (selected), and TSAPI Properties. The main area 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 (or the **Edit TSAPI Links** screen to edit a previously configured TSAPI Link as shown below), enter the following values:

- **Link:** Use the drop-down list to select an unused link number.
- **Switch Connection:** Choose the appropriate switch connection **cm101x**, which has already been configured from the drop-down list.
- **Switch CTI Link Number:** Corresponding CTI link number configured in **Section 5.1.2** which is **1**.
- **ASAI Link Version:** This should be set to the highest version available.
- **Security:** This should be set to **Both** allowing both secure and nonsecure connections.


Once completed, select **Apply Changes**.

The screenshot shows the 'AE Services | TSAPI | TSAPI Links' interface. On the left, a sidebar lists 'AE Services' with sub-items: CVLAN, DLG, DMCC, SMS, TSAPI (expanded), TSAPI Links (selected), TSAPI Properties, TWS, and Communication Manager Interface. The main area is titled 'Edit TSAPI Links' and contains the following fields:

- Link: 1
- Switch Connection: cm101x (dropdown)
- Switch CTI Link Number: 1 (dropdown)
- ASAI Link Version: 12 (dropdown)
- Security: Both (dropdown)

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

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

Apply Changes to Link
Warning! Are you sure you want to apply the changes?
These changes can only take effect when the TSAPI server restarts.
 **Please use the Maintenance -> Service Controller page to restart the TSAPI server.**

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

TSAPI Links				
Link	Switch Connection	Switch CTI Link #	ASAI Link Version	Security
<input checked="" type="radio"/> 1	cm101x	1	12	Both
<input type="button" value="Add Link"/> <input type="button" value="Edit Link"/> <input type="button" value="Delete Link"/>				

6.3. Identify Tlinks

Navigate to **Security** → **Security Database** → **Tlinks**. Verify the value of the **Tlink Name**. This will be needed to configure SSS Public Safety in **Section** Error! Reference source not found..

Security | Security Database | Tlinks

▶ **AE Services**

▶ **Communication Manager Interface**

High Availability

▶ **Licensing**

▶ **Maintenance**

▶ **Networking**

▼ **Security**

▶ Account Management

▶ Audit

▶ Certificate Management

Enterprise Directory

▶ Host AA

▶ PAM

▼ **Security Database**

▪ Control

⊕ CTI Users

▪ Devices

▪ Device Groups

▪ **Tlinks**

▪ Tlink Groups

▪ Worktops

Tlinks

Tlink Name

☒ AVAYA#CM101X#CSTA#AESPRI101X

☐ AVAYA#CM101X#CSTA-S#AESPRI101X

Delete Tlink

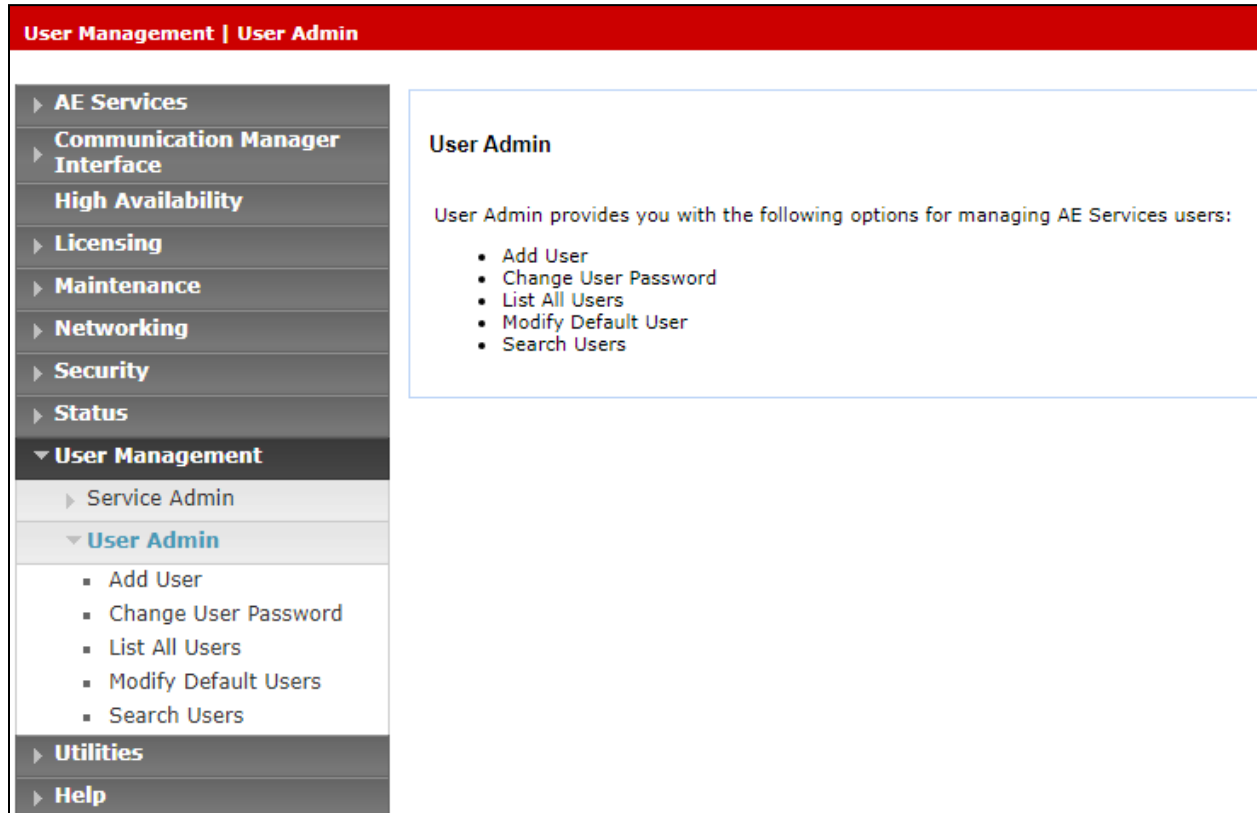
6.4. Enable TSAPI Ports

To ensure that TSAPI ports are enabled, navigate to **Networking → Ports**. Ensure that the TSAPI ports are set to **Enabled** as shown below.

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

6.5. Create CTI User

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



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

- **User Id** - This will be used by the SSS Public Safety setup in **Section** Error! Reference source not found..
- **Common Name** and **Surname** - Descriptive names need to be entered.
- **User Password** and **Confirm Password** - This will be used with SSS Public Safety setup in **Section** Error! Reference source not found..
- **CT User** - Select **Yes** from the drop-down menu.

Click on **Apply Changes** at the bottom of the screen.

User Management | User Admin | List All Users

▶ **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

Edit User

* User Id

centricity

* Common Name

centricity

* Surname

centricity

User Password

.....

Confirm Password

.....

Admin Note

Avaya Role

None ▼

Business Category

Car License

CM Home

Css Home

CT User

Yes ▼

Department Number

Display Name

6.6. Associate Devices with CTI User

Navigate to **Security** → **Security Database** → **CTI Users** → **List All Users**. Select the CTI user added in **Section 6.5** and click on **Edit**.

AE Services

Communication Manager Interface

High Availability

Licensing

Maintenance

Networking

Security

Account Management

Audit

Certificate Management

Enterprise Directory

Host AA

PAM

Security Database

Control

CTI Users

List All Users

Search Users

CTI Users

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

EditList All

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

Edit CTI User

User Profile:

User IDcentricity

Common Namecentricity

Worktop NameNONE ▾

Unrestricted Access☒

Call and Device Control:

Call Origination/Termination and Device StatusNone ▾

Call and Device Monitoring:

Device MonitoringNone ▾

Calls On A Device MonitoringNone ▾

Call Monitoring☐

Routing Control:

Allow Routing on Listed DevicesNone ▾

Apply Changes

Cancel Changes

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

6.7. Configure System Management Service (SMS)

Navigate to **AE Services** → **SMS** → **SMS Properties**. The only change that should be necessary is the value set in the **Default CM Host Address**, this should be set to the IP address of Communication Manager. Everything else should be as default, or as shown below. Click on **Apply Changes** to ensure that all is saved correctly.

AE Services | SMS | SMS Properties

▼ **AE Services**

▶ CVLAN

▶ DLG

▶ DMCC

▼ **SMS**

▪ **SMS Properties**

▶ TSAPI

▶ TWS

▶ **Communication Manager Interface**

▶ **High Availability**

▶ **Licensing**

▶ **Maintenance**

▶ **Networking**

SMS Properties

Default CM Host Address

Default CM Admin Port

CM Connection Protocol

SMS Logging

SMS Log Destination

CM Proxy Trace Logging

Max Sessions per CM

Proxy Shutdown Timer seconds

SAT Login Keepalive seconds

CM Terminal Type

Proxy Log Destination

6.8. Restart AE Server

Once everything is configured correctly, it is best practice to restart AE Server (if possible), this will ensure that the new connections are brought up correctly. Click on the **Restart AE Server** button at the bottom of the screen.

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

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](#)

StartStopRestart ServiceRestart AE ServerRestart LinuxRestart Web Server

A message confirming the restart will appear, click on **Restart** to proceed.

Maintenance | Service Controller

▶ AE Services

▶ Communication Manager Interface

High Availability

▶ Licensing

▼ Maintenance

Date Time/NTP Server

▶ Security Database

Service Controller

▶ Server Data

Restart AE Server

Warning! Are you sure you want to restart?
Restarting will cause all existing connections to be dropped and associations lost.

RestartCancel

7. Configure SSS Public Safety Centricity

This section provides the procedures for configuring Centricity. The file **ProgramData** → **CV2** → **configv2.xml** may need to be amended to connect successfully to AES. These are highlighted below and can be edited using Notepad.

Find the section `<module type="AES TSAPI CONTROLLER">`

```
<module type="AES TSAPI CONTROLLER"
    guid="b0a8810e-2c2d-4eab-9c6e-f874675de9e2"
    path="AESTSAPIController.dll" updated="False" deleted="False" paused="False >
  <param name="inputTags" datatype="string" value="UciToAes,UciNaq" />
  <param name="outputTags" datatype="string" value="AesTsapiController" />
  <param name="port" datatype="int" value="450" />
  <param name="serverid" datatype="string" value="AVAYA#CM101#CSTA#AESPRI101X" />
  <param name="monitors" datatype="string" value="" />
  <param name="acdmonitors" datatype="string" value="" />
  <param name="vdnmonitors" datatype="string" value="" />
  <param name="registerNonAcdQueues" datatype="string" value="" />
  <param name="username" datatype="string" value="ctiuser" />
  <param name="site" datatype="string" value="1" />
  <param name="password" datatype="string" value="Password_01" />
  <param name="reconnecttimeout" datatype="int" value="5000" />
  <param name="pollinginterval" datatype="int" value="10" />
  <param name="featurecode" datatype="string" value="*26" />
  <param name="pollagents" datatype="bool" value="true" />
  <param name="agentmode" datatype="Boolean" value="false" />
  <param name="SmsUrl" datatype="string"
    value="https://aespri101x/smsxml/SystemManagementService.php" />
  <param name="SmsUsername" datatype="string" value="smsuser@10.10.40.13" />
  <param name="SmsPassword" datatype="string" value="Password_02" />
  <param name="SmsCertificateValid" datatype="boolean" value="false" />
  <param name="SmsCallTimeoutSeconds" datatype="int" value="30" />
  <param name="AgentDiscoveryIntervalSeconds" datatype="int" value="1800" />
  <param name="EndpointDiscoveryIntervalSeconds" datatype="int" value="1800" />
  <param name="SkillDiscoveryIntervalSeconds" datatype="int" value="1800" />
  <param name="VdnDiscoveryIntervalSeconds" datatype="int" value="1800" />
  <param name="ReasonCodeDiscoveryIntervalSeconds" datatype="int" value="3600" />
  <param name="PollAgentIntervalMilliseconds" datatype="int" value="500" />
  <param name="AutomaticallyUnmonitor" datatype="boolean" value="false" />
</module>
```

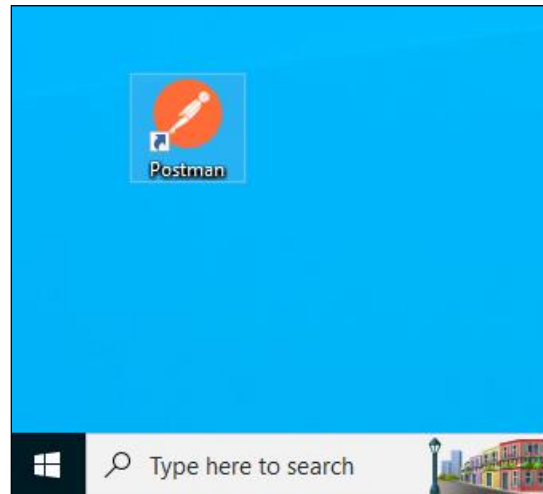
Highlighted in bold above show the AES details from **Section 0** along with others required for the connection to be set up correctly.

8. Verification Steps

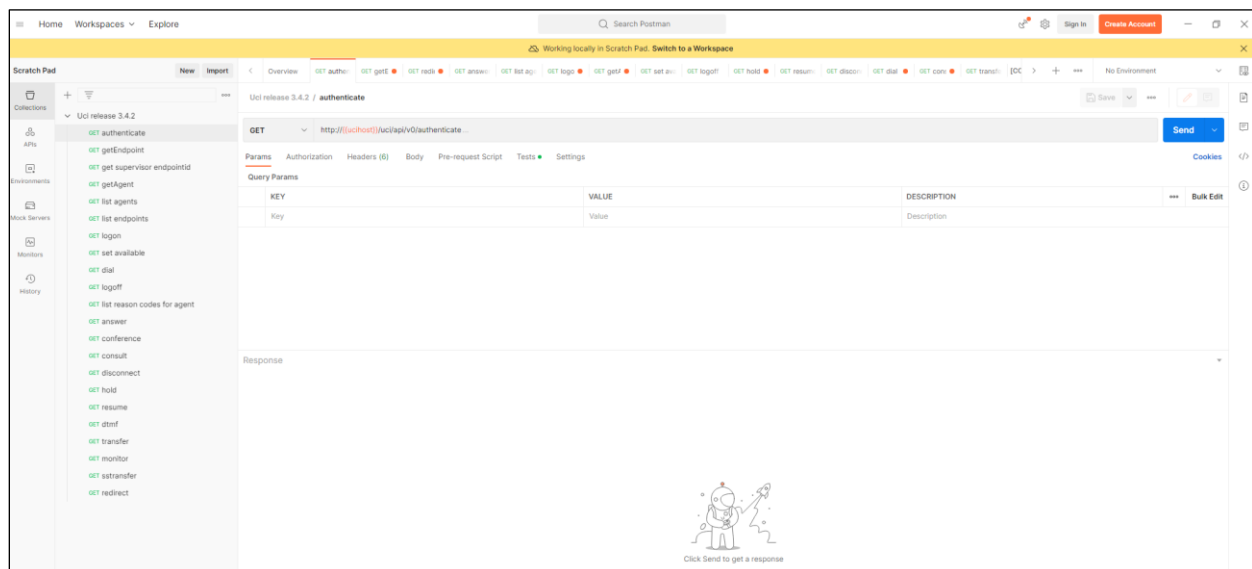
The correct configuration of the solution can be verified as follows.

8.1. Verify SSS Public Safety Centricity

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



Once opened the screen shown below should be automatically displayed. The initial step is to click on **GET authenticate** in the left window.



Once **GET authenticate** has been pressed, the **uciInstanceId** should be returned in the main window.

The screenshot displays a REST client interface with a sidebar on the left listing various endpoints under 'Uci release 3.4.2'. The 'GET authenticate' endpoint is selected. The main panel shows the request details for a GET request to 'http://{{ucihost}}/uci/api/v0/authenticate ...'. The 'Params' tab is active, showing a table with one entry: 'Key' with a value of 'Value'. Below this, the 'Body' tab is active, showing a JSON response in 'Pretty' format. The response contains an 'id' and a 'uciInstanceId'.

KEY	VALUE
Key	Value

```
1 {
2   "id": "428BD702-B6B8-40D3-B393-9A01D0F97CCE",
3   "uciInstanceId": "Centricity-01"
4 }
```

Clicking on **Get getEndpoint** in the left window should return something like is shown below. Note that the **VALUE** for the **KEY extension** must be manually filled in, for compliance testing extension **3001** was used.

The screenshot shows the Postman interface with a collection named 'Uci release 3.4.2'. The 'getEndpoint' endpoint is selected. The request is a GET to `http://{{ucihost}}/uci/api/v0/endpoint?extension=3001`. The 'Query Params' section shows 'extension' with a value of '3001'. The response body is a JSON object with the following structure:

```

{
  "associatedConnections": [
    {
      "id": "55db556e-9ab1-487d-86f6-b4d2c1ee3112",
      "direction": "out",
      "sender": "35391847001",
      "target": "35391733001",
      "senderDomain": "AES",
      "targetDomain": "AES",
      "endpointId": "d9a6b001-fbaf-4ffa-b831-e2e2b17dcaa7",
      "extension": "35391847001",
      "callId": "20230208_331",
      "state": "alerting",
      "targetType": "other",
      "holdStartTime": null,
      "startTime": "2023-02-08T18:18:42.6336741Z",
      "monitoring": null,
      "lastError": "",
      "associatedConnections": [],
      "canEnd": true,
      "canAccept": false,
      "canHold": false,
      "canResume": false,
      "canTransfer": false,
      "canSSTransfer": false,
      "canConsult": false,
      "canDtmf": false,
      "canBarge": false,
      "canConference": false,
      "canRedirect": false
    }
  ]
}

```

8.1. Verify connection from Avaya platform

There are a number of checks that can be performed to ensure that a connection is present from the Avaya products. These are some of the key checks that can be performed.

- Verify CTI Service State on Communication Manager
- Verify TSAPI link and user on Application Enablement Services
- Verify SMS on Application Enablement Services

8.1.1. Verify Avaya Aura® Communication Manager CTI Service State

Check the connection between Communication Manager and AES. Check the AESVCS link status by using the command **status aescvcs cti-link**. Verify the **Service State** of the CTI link is **established**.

status aescvcs cti-link						
AE SERVICES CTI LINK STATUS						
CTI Link	Version	Mnt Busy	AE Services Server	Service State	Msgs Sent	Msgs Rcvd
1	12	no	aespri101x	established	865	865

8.1.2. 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 TSAPI link by checking that the **Status** is **Talking** and the **State** is **Online**.

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

User Management

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	cm101x	1	Talking	Tue Feb 7 10:38:49 2023	Online	20	42	6689	6689	30

OnlineOffline

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

TSAPI Service StatusTLink StatusUser Status

Clicking on **User Status** from the screen on the previous page should display something similar to that shown below, where the **centricity** user and corresponding **Tlink Name** are shown.

CTI User Status

☐ Enable page refresh every seconds

CTI Users

Open Streams 4

Closed Streams 4

Open Streams

Name	Time Opened	Time Closed	Tlink Name
DMCCLCSUserDoNotModify	Thu 02 Feb 2023 06:15:13 PM GMT		AVAYA#CM101X#CSTA#AESPRI101X
DMCCLCSUserDoNotModify	Thu 02 Feb 2023 07:15:14 PM GMT		AVAYA#CM101X#CSTA#AESPRI101X
centricity	Tue 07 Feb 2023 10:38:52 AM GMT		AVAYA#CM101X#CSTA#AESPRI101X

8.1.3. Verify SMS link

Open a web page to **https://<AESIP>/sms/sms-test.php**, as shown below. Enter the Communication Manager login details and a **Request**, such as List Agent, is entered as shown below, this should return a **Response** as shown.

The screenshot displays the 'SMS Interactive Test' web application in a browser. The address bar shows the URL 'https://10.10.40.16/sms/sms_test.php' with a 'Not secure' warning. The application header features the 'AVAYA' logo and the title 'String Based - Web Service Request Form'.

SMS Resources

- [Model Documentation](#)
- [Model Doc \(No-Frames\)](#)
- [SMS WSDL](#)

Connection Information

CM Login ID: login@<[IPv6]:port|hostname:port>
Password:
SOAP Request Timeout (Seconds):

Request Parameters

Model: ...
Operation:
Objectname:
Qualifier:
Fields:

Session Recording

☐ Record SMS Request
☐ Record Result Data
[Get Record](#) [Clear Record](#)

Submit Request **Release**

Last Request Response

Session ID: [Duplicate Session](#)

Response

```
Response {
  var $result_code = 0
  var $result_data = 'Login_ID[0]=3401|Login_ID[1]=3402|Name[0]=Agent One
Workspaces|Name[1]=Agent Two
Workspaces|Extension[0]=unstaffed|Extension[1]=unstaffed|Direct_Agent_Skill[0]=
Direct_Agent_Skill[1]=|AAS[0]=n|AAS[1]=n|AUDIX[0]=n|AUDIX[1]=n|COR[0]=1|COR[1]=1
|Call_Handling_Preference[0]=skill-level|Call_Handling_Preference[1]=skill-
level|Service_Objective[0]=n|Service_Objective[1]=n|SN[0]=|SN[1]=|SL[0]=|SL[1]=''
```

9. Conclusion

These Application Notes describe the compliance testing of SSS Public Safety Centricity with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services. All test cases were executed successfully with any observations noted in **Section 2.2**.

10. Additional References

This section references the product documentations that are relevant to these Application Notes.

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

- [1] *Administering Avaya Aura® Communication Manager, Release 10.1.x, Issue 5, March 2023.*
- [2] *Administering Avaya Aura® Application Enablement Services, Release 10.1.x, Issue 6, Feb 2023.*
- [3] *Avaya Aura® Communication Manager Feature Description and Implementation, Release 10.1.x, Issue 8, March 2023.*
- [4] *Administering Avaya Aura® Session Manager, Release 10.1.x Issue 5, Feb 2023.*

Product documentation for Centricity can be found by contacting SSS Public Safety as per **Section 2.3**.

©2023 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.