



Avaya Solution & Interoperability Test Lab

Application Notes for Trio Enterprise to interoperate with Avaya Aura® Communication Manager, Avaya Aura® Session Manager and Avaya Aura® Application Enablement Services - Issue 1.0

Abstract

These Application Notes describe the configuration steps required for Trio Enterprise to interoperate with Avaya Aura® Communication Manager, Avaya Aura® Session Manager and Avaya Aura® Application Enablement Services.

Readers should pay attention to **Section 2**, in particular the scope of testing as outlined in **Section 2.1** as well as the observations noted in **Section 2.2**, to ensure that their own use cases are adequately covered by this scope and results.

Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

1. Introduction

These Application Notes outline the steps necessary to configure Trio Enterprise from Enghouse Interactive AB to interoperate with Avaya Aura® Communication Manager R7.0 (Communication Manager), Avaya Aura® Session Manager R7.0 (Session Manager) and Avaya Aura® Application Enablement Services R7.0 (AES). Trio Enterprise is a client/server based application running on Windows Server operating systems. Trio Enterprise provides users with an attendant answering position for Communication Manager, as well as a call referral function that provides spoken information about the status of the extension called, it also includes its own built-in voice mail called Trio VoiceMail. The Trio Enterprise Attendant client provides a view of contacts, schedules, and communication tasks and was installed on the same server as the Trio Server, but can be installed on a separate platform if required.

Trio Enterprise connects to the Communication Manager using a SIP trunk via the Session Manager. A TSAPI connection on AES enables the Trio Enterprise Absence integration. Trio Enterprise is supplied with all prerequisite software.

2. General Test Approach and Test Results

The general test approach was to configure a simulated enterprise voice network using Communication Manager. The Trio Enterprise server Communicates with the Communication Manager using a SIP trunk through the Session Manager. See **Figure 1** for a network diagram. A Dial plan was configured on the Communication Manager to route calls to Trio Enterprise. Calls placed to the Trio Enterprise server automatically places a call to the telephone the Attendant is using for answering purposes. When the attendant answers the call the Trio Enterprise server bridges the two calls. When the attendant extends the call to another telephone, Trio Enterprise server performs a SIP Refer method, and the caller and the called user are now directly connected.

It is possible to have multiple Trio attendant positions on a Communication Manager system. A variety of Avaya telephones were installed and configured on the Communication Manager.

Note: During compliance testing an Avaya SIP station was used as the attendant's telephone.

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.

2.1. Interoperability Compliance Testing

The interoperability compliance testing included feature and serviceability testing. The serviceability testing introduced failure scenarios to see if Trio Enterprise could resume after a link failure with Communication Manager/AES. The testing included:

- Incoming internal and external calls
- Outgoing internal and external calls
- Supervised and unsupervised transfer with answer
- Directing calls to busy extensions
- Call queuing and retrieval
- Loop detection for busy and unanswered extensions
- Absence detection
- Message Waiting lamb

2.2. Test Results

Tests were performed to insure full interoperability between Trio Enterprise and Avaya Communication Manager. The tests were all functional in nature and performance testing was not included. All test cases passed successfully with the following observation,

- Trio Enterprise is designed to work in Europe therefore codec G.711Alaw is used as first priority. If ip-codec-set form in Communication Manager is configured with different codec than G.711Alaw the Avaya 96x1 SIP deskphone could not hear early media from Trio Enterprise. To overcome this issue, the codec G.711Alaw was configured as first priority in the ip-codec-set form as mentioned in **Section 5.6**.

2.3. Support

For technical support for Enghouse Interactive AB products, please use the following web link.
<http://www.trio.com/web/Support.aspx>

Enghouse Interactive AB can also be contacted as follows.

Phone: +46 (0)8 457 30 00

Fax: +46 (0)8 31 87 00

E-mail: triosupport@enghouse.com

3. Reference Configuration

Figure 1 illustrates the network topology used during compliance testing. The Avaya solution consists of a Communication Manager, which has a SIP Trunk connection to the Trio Enterprise server via the Session Manager. TSAPI is configured on the Trio Enterprise server which enables the Trio Enterprise to interact with telephone on the Communication Manager to act as the Attendant telephone via the AES. An Avaya SIP station was used as the Trio Enterprise Attendant telephone during compliance testing. SIP and H.323 stations were configured on the Communication Manager to generate outbound/inbound calls to/from the PSTN. A PRI/T1 trunk on Media Gateway G450 was configured to connect to the simulated PSTN.

Note: The Trio Enterprise Attendant (client) was installed on the same server as the Trio Enterprise Server, but can be installed on a separate platform if required.

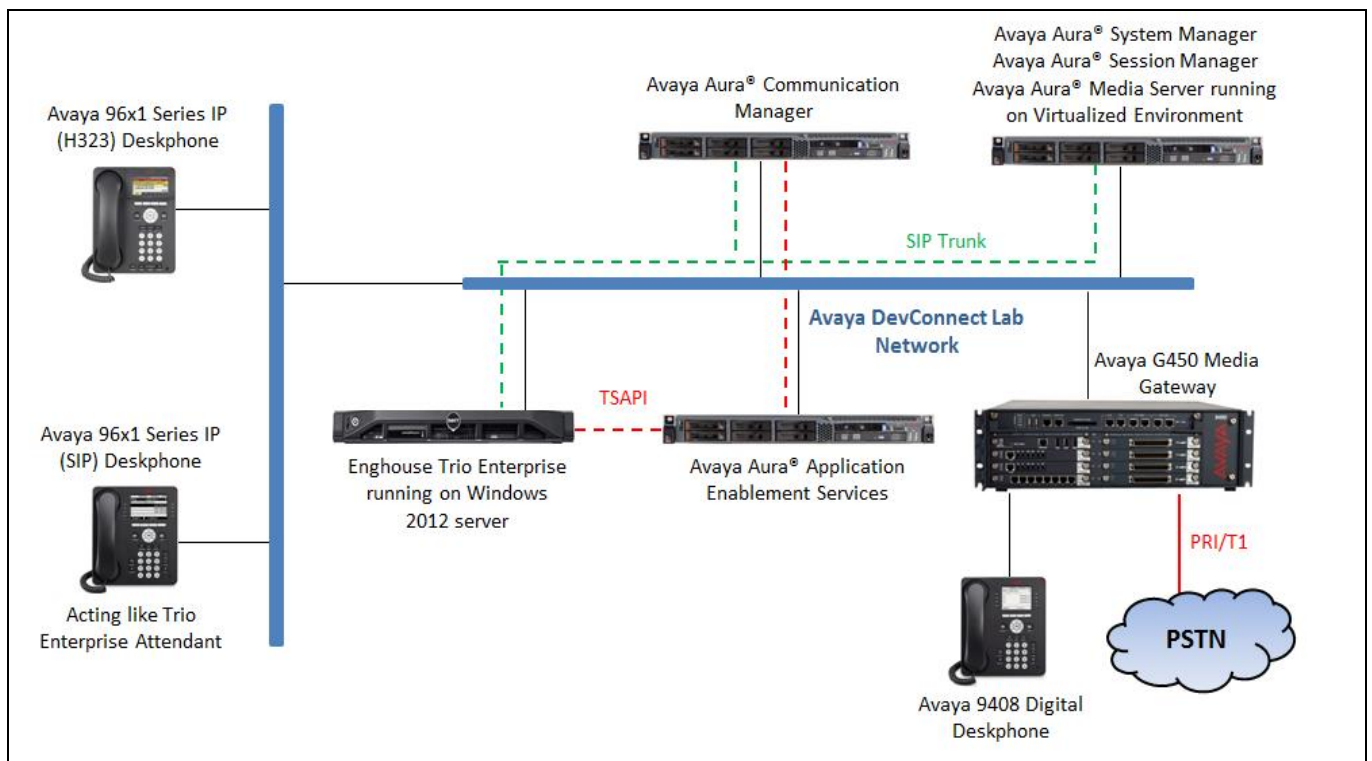


Figure 1: Avaya and Trio Enterprise Reference Configuration

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	7.0.1.2.0-FP1SP2
Avaya Aura® Application Enablement Services running on virtualized environment	7.0.1.0.4.15-0
Avaya Aura® Session Manager running on virtualized environment	7.0.1.2.701230
Avaya Aura® System Manager	7.0.1.2.086007
Avaya Aura® Media Server	7.7.0.359
Avaya G450 Media Gateway	FW 39.19.0/1
Avaya 96x1 Series IP Telephone <ul style="list-style-type: none">• 96x1 (H.323)• 96x1 (SIP)	6.6401 7.0.1.4
Avaya 9408 Digital Telephone	2.0 SP8 (R18)
Trio Enterprise Server and Client running on Microsoft Windows 2012 R2 Server	7.0

5. Configure Avaya Aura® Communication Manager

Configuration and verification operations on the Communication Manager illustrated in this section were all performed using Avaya Site Administrator Emulation Mode. The information provided in this section describes the configuration of the Communication Manager for this solution. For all other provisioning information such as initial installation and configuration, please refer to the product documentation in **Section 11**.

It is implied a working system is already in place. The configuration operations described in this section can be summarized as follows: (Note: During Compliance Testing all inputs not highlighted in Bold were left as Default)

- Verify License
- Administer System Parameters Features
- Administer SIP signaling group
- Administer SIP trunk group
- Administer IP network region
- Administer IP codec set
- Administer route pattern
- Administer private numbering
- Administer dial plan
- Administer uniform dial plan
- Administer AAR analysis
- Configure interface to Application Enablement Services
- Create a CTI Link to the Application Enablement Services
- Configure Absence diversion

5.1. Verify License

Log in to the System Access Terminal to verify that the Communication Manager license has proper permissions for features illustrated in these Application Notes. Use the “display system-parameters customer-options” command. Navigate to **Page 2**, and verify that there is sufficient remaining capacity for SIP trunks by comparing the **Maximum Administered SIP Trunks** field value with the corresponding value in the **USED** column.

Verify that the **Computer Telephony Adjunct Links** customer option is set to “y” on **Page 4**. If this option is not set to “y”, then contact the Avaya sales team or business partner for a proper license file.

display system-parameters customer-options		Page	2 of	12
OPTIONAL FEATURES				
IP PORT CAPACITIES		USED		
Maximum Administered H.323 Trunks:		12000	20	
Maximum Concurrently Registered IP Stations:		18000	3	
Maximum Administered Remote Office Trunks:		12000	0	
Maximum Concurrently Registered Remote Office Stations:		18000	0	
Maximum Concurrently Registered IP eCons:		128	0	
Max Concur Registered Unauthenticated H.323 Stations:		100	0	
Maximum Video Capable Stations:		36000	3	
Maximum Video Capable IP Softphones:		18000	3	
Maximum Administered SIP Trunks:		12000	58	
Maximum Administered Ad-hoc Video Conferencing Ports:		12000	0	
Maximum Number of DS1 Boards with Echo Cancellation:		522	0	

display system-parameters customer-options		Page	4 of	12
OPTIONAL FEATURES				
Abbreviated Dialing Enhanced List? y		Audible Message Waiting? y		
Access Security Gateway (ASG)? n		Authorization Codes? y		
Analog Trunk Incoming Call ID? y		CAS Branch? n		
A/D Grp/Sys List Dialing Start at 01? y		CAS Main? n		
Answer Supervision by Call Classifier? y		Change COR by FAC? n		
ARS? y		Computer Telephony Adjunct Links? y		
ARS/AAR Partitioning? y		Cvg Of Calls Redirected Off-net? y		
ARS/AAR Dialing without FAC? y		DCS (Basic)? y		
ASAI Link Core Capabilities? y		DCS Call Coverage? y		
ASAI Link Plus Capabilities? y		DCS with Rerouting? y		
Async. Transfer Mode (ATM) PNC? n		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				

5.2. Administer System Parameter Features

During compliance testing Trio Enterprise suggested that the Station Call Transfer Recall Timer was set to be 20 seconds. Use the “change system-parameters features” command to change the **Station Call Transfer Recall Timer** on **page 6**.

```
change system-parameters features                                     Page 6 of 19
      FEATURE-RELATED SYSTEM PARAMETERS
Public Network Trunks on Conference Call: 5                        Auto Start? n
Conference Parties with Public Network Trunks: 6                  Auto Hold? n
Conference Parties without Public Network Trunks: 6                Attendant Tone? y
Night Service Disconnect Timer (seconds): 180                     Bridging Tone? n
Short Interdigit Timer (seconds): 3                               Conference Tone? n
Unanswered DID Call Timer (seconds):                               Intrusion Tone? n
Line Intercept Tone Timer (seconds): 30                           Mode Code Interface? n
Long Hold Recall Timer (seconds): 0
Reset Shift Timer (seconds): 0
Station Call Transfer Recall Timer (seconds): 20                 Recall from VDN? n
Trunk Alerting Tone Interval (seconds): 15
      DID Busy Treatment: tone
Allow AAR/ARS Access from DID/DIOD? n
Allow ANI Restriction on AAR/ARS? n
Use Trunk COR for Outgoing Trunk Disconnect/Alert? n
      7405ND Numeric Terminal Display? n                          7434ND? n
DISTINCTIVE AUDIBLE ALERTING
Internal: 1 External: 2 Priority: 3
      Attendant Originated Calls: external
DTMF Tone Feedback Signal to VRU - Connection:                   Disconnection:
```

Enable **Create Universal Call ID (UCID)**, which is located on **Page 5**. For **UCID Network Node ID**, enter an available node ID.

```
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
Copy UCID for Station Conference/Transfer? y
```


Navigate to **Page 13**, and enable **Send UCID to ASAI**. This parameter allows for the universal call ID to be sent to Trio Enterprise.

```
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 UII 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? y
      Prefer H.323 Over SIP For Dual-Reg Station 3PCC Make Call? n
```

5.3. Administer SIP Signaling Group

Use the “add signaling-group n” command, where “n” is an available signaling group number, in this case “1”. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Group Type:** “sip”
- **Transport Method:** “tls”
- **Near-end Node Name:** An existing C-LAN node name or “procr”.
- **Far-end Node Name:** The existing node name for Session Manager.
- **Near-end Listen Port:** An available port for integration with Parlance.
- **Far-end Listen Port:** The same port number as in **Near-end Listen Port**.
- **Far-end Network Region:** An existing network region to use with Parlance.
- **Far-end Domain:** The applicable domain name for the network.
- **Direct IP-IP Audio Connections:** “y”

change signaling-group 1		Page 1 of 3	
SIGNALING GROUP			
Group Number: 1	Group Type: sip		
IMS Enabled? n	Transport Method: tls		
Q-SIP? n			
IP Video? n	Enforce SIPS URI for SRTP? n		
Peer Detection Enabled? n	Peer Server: SM		
Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? y			
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? n			
Alert Incoming SIP Crisis Calls? n			
Near-end Node Name: procr		Far-end Node Name: interopASM	
Near-end Listen Port: 5061		Far-end Listen Port: 5061	
		Far-end Network Region: 1	
Far-end Domain: bvwdev.com			
		Bypass If IP Threshold Exceeded? n	
Incoming Dialog Loopbacks: eliminate		RFC 3389 Comfort Noise? n	
DTMF over IP: rtp-payload		Direct IP-IP Audio Connections? y	
Session Establishment Timer(min): 3		IP Audio Hairpinning? n	
Enable Layer 3 Test? y		Initial IP-IP Direct Media? n	
H.323 Station Outgoing Direct Media? n		Alternate Route Timer(sec): 6	

5.4. Administer SIP Trunk Group

Use the “add trunk-group n” command, where “n” is an available trunk group number, in this case “1”. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Group Type:** “sip”
- **Group Name:** A descriptive name.
- **TAC:** An available trunk access code.
- **Service Type:** “tie”
- **Signaling Group:** The signaling group number from **Section 5.3**.
- **Number of Members:** The desired number of members, in this case “14”.

```
change trunk-group 1                                     Page 1 of 22
                                     TRUNK GROUP
Group Number: 1
  Group Name: Private Trunk          Group Type: sip      CDR Reports: y
    Direction: two-way              COR: 1              TN: 1      TAC: #01
  Dial Access? n                    Outgoing Display? n
Queue Length: 0                      Night Service:
Service Type: tie                    Auth Code? n
                                     Member Assignment Method: auto
                                     Signaling Group: 1
                                     Number of Members: 14
```

Navigate to **Page 3**, and enter “private” for **Numbering Format**.

```
change trunk-group 1                                     Page 3 of 22
TRUNK FEATURES
  ACA Assignment? n                      Measured: none
                                           Maintenance Tests? y

  Suppress # Outpulsing? n  Numbering Format: private
                                           UI Treatment: shared
                                           Maximum Size of UI Contents: 128
                                           Replace Restricted Numbers? y
                                           Replace Unavailable Numbers? y

                                           Hold/Unhold Notifications? y
                                           Modify Tandem Calling Number: no
  Send UCID? n

  Show ANSWERED BY on Display? y

  DSN Term? n                      SIP ANAT Supported? n
```

5.5. Administer IP Network Region

Use the “change ip-network-region n” command, where “n” is the existing far-end network region number used by the SIP signaling group from **Section 5.3**.

For **Authoritative Domain**, enter the applicable domain for the network. Enter a descriptive **Name**. Enter “yes” for **Intra-region IP-IP Direct Audio** and **Inter-region IP-IP Direct Audio**, as shown below. For **Codec Set**, enter an available codec set number for integration with Trio Enterprise.

change ip-network-region 1		Page 1 of 20
IP NETWORK REGION		
Region: 1		
Location: 1	Authoritative Domain: bvwdev.com	
Name: Loc-1	Stub Network Region: n	
MEDIA PARAMETERS	Intra-region IP-IP Direct Audio: yes	
Codec Set: 1	Inter-region IP-IP Direct Audio: yes	
UDP Port Min: 2048	IP Audio Hairpinning? n	
UDP Port Max: 3329		
DIFFSERV/TOS PARAMETERS		
Call Control PHB Value: 46		
Audio PHB Value: 46		
Video PHB Value: 26		

Navigate to **Page 4**, and specify this codec set to be used for calls with network regions used by Avaya endpoints and by the trunk to the PSTN. In the compliance testing, network region “1” was used by the Avaya endpoints and by the trunk to the PSTN.

change ip-network-region 1		Page 4 of 20
Source Region: 1	Inter Network Region Connection Management	I M
		G A t
dst codec direct WAN-BW-limits Video Intervening	Dyn	A G c
rgn set WAN Units Total Norm Prio Shr Regions	CAC	R L e
1 1		n all
2 2 y NoLimit		n t

5.6. Administer IP Codec Set

Use the “change ip-codec-set n” command, where “n” is the codec set number from **Section 5.5**. Update the audio codec types in the **Audio Codec** fields as necessary. As per the observation noted in **Section 2.2**, Trio Enterprise is designed to work in Europe they use the codec G.711A therefore it should be set as first priority so that Avaya 96x1 SIP phone can hear the early media when it connects to Trio. The codec shown below was used in the compliance testing.

```
change ip-codec-set 1                                     Page 1 of 2

                                IP CODEC SET

Codec Set: 1

Audio      Silence      Frames      Packet
Codec      Suppression   Per Pkt    Size(ms)
1: G.711A   n                 2         20
2: G.711MU n                 2         20
3: G.729    n                 2         20
4:
5:

Media Encryption                               Encrypted SRTP: best-effort
1: 1-srtp-aescm128-hmac80
2: 2-srtp-aescm128-hmac32
3: none
```

5.7. Administer Route Pattern

Use the “change route-pattern n” command, where “n” is an existing route pattern number to be used to reach Trio Enterprise, in this case “1”. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Pattern Name:** A descriptive name.
- **Grp No:** The SIP trunk group number from **Section 5.4**.
- **FRL:** A level that allows access to this trunk, with 0 being least restrictive.

```
change route-pattern 1                                     Page 1 of 3

                                Pattern Number: 1      Pattern Name: SIP-TLS-To-SM
SCCAN? n      Secure SIP? n      Used for SIP stations? n

Grp FRL NPA Pfx Hop Toll No.  Inserted      DCS/  IXC
No      Mrk Lmt List Del  Digits      QSIG
                                Dgts      Intw
1: 1      0                                     n      user
2:                                     n      user
3:                                     n      user
4:                                     n      user

BCC VALUE  TSC CA-TSC      ITC BCIE Service/Feature PARM Sub  Numbering LAR
0 1 2 M 4 W      Request      Dgts Format
1: y y y y y n  n      rest      lev0-pvt next
```

5.8. Administer Private Numbering

Use the “change private-numbering 0” command, to define the calling party number to send to Trio Enterprise. Add an entry for the trunk group defined in **Section 5.4**. In the example shown below, all calls originating from a 4-digit extension beginning with 3 and routed to trunk group 1 will result in a 4-digit calling number. The calling party number will be in the SIP “From” header.

change private-numbering 0					Page 1 of 2
NUMBERING - PRIVATE FORMAT					
Ext Len	Ext Code	Trk Grp(s)	Private Prefix	Total Len	
4	3	1		4	Total Administered: 5
4	3	4	417967	10	Maximum Entries: 540

5.9. Administer Dial Plan

This section provides a sample dial plan used for routing calls with dialed digits 47xx to Trio Enterprise. Use the “change dialplan analysis 0” command, and add an entry to specify the use of digits pattern 47, as shown below.

change dialplan analysis									Page 1 of 12
DIAL PLAN ANALYSIS TABLE									
Location: all					Percent Full: 4				
Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type	
0	3	fac	43	4	aar				
1	4	ext	47	4	udp				
13	5	aar	46	4	aar				
28	5	aar	9	1	fac				
30	4	aar	*	3	dac				
33	4	ext	#	3	dac				

5.10. Administer Uniform Dial Plan

This section provides a sample AAR routing used for routing calls with dialed digits 47xx to Trio Enterprise. Note that other routing methods may be used. Use the “change uniform-dialplan 0” command, and add an entry to specify the use of AAR for routing of digits 47xx, as shown below.

change uniform-dialplan 0							Page 1 of 2
UNIFORM DIAL PLAN TABLE							
							Percent Full: 0
Matching Pattern	Len	Del	Insert Digits	Net	Conv	Node Num	
47	4	0		aar	n		
56	5	0		aar	n		

5.11. Administer AAR Analysis

Use the “change aar analysis 0” command, and add an entry to specify how to route calls to 45xx. In the example shown below, calls with digits 47xx will be routed as an AAR call using route pattern “1” from **Section 5.7**.

change aar analysis 47							Page	1	of	2
AAR DIGIT ANALYSIS TABLE										
Location: all							Percent Full: 2			
	Dialed	Total		Route	Call	Node	ANI			
	String	Min	Max	Pattern	Type	Num	Reqd			
47		4	4	1	aar		n			
48		4	4	1	aar		n			

5.12. Configure interface to Avaya Aura® Application Enablement Services

To configure the AES link use the “change ip-services” command and enter the following:

Page 1

- **Type:** Enter AESVCS
- **Enabled:** Enter y
- **Local Node:** Enter procr
- **Port:** Enter 8765

change ip-services							Page	1	of	4
IP SERVICES										
Service	Enabled	Local	Local	Remote	Remote					
Type		Node	Port	Node	Port					
AESVCS	y	procr	8765							

Navigate to **Page 4** and enter the following:

- **Server ID** Enter 1
- **AE Services** Enter aes70 (note that the name entered in this field should be matched with the host name of AES server)
- **Password** Enter a password. This password will be used later in **Section 6.3** to enable the AES to communicate with the Communication Manager.
- **Enabled** Enter y

change ip-services					Page	4	of	4
AE Services Administration								
Server ID	AE Services	Password	Enabled	Status				
	Server							
1:	aes70	*	y	in use				

5.13. Create a CTI Link to the Aura® Application Enablement Services

A CTI Link needs to be created to enable the Communication Manager to interoperate with the AES. Use the **add cti-link next** command and enter the following:

- **Extension:** Enter any unused **Extension** (i.e. 3332)
- **Type:** Enter **ADJ-IP**
- **Name:** Enter a descriptive name (i.e. AES70)

(Note, during compliance testing cti link 1 was added)

```
change cti-link 1                                     Page 1 of 3
CTI LINK
CTI Link: 1
Extension: 3332
Type: ADJ-IP
Name: AES70
COR: 1
```

5.14. Configure Absence diversion

A VDN extension followed by a reason code (list of reason code 1 to 9 is managed on Trio Enterprise) and # can be dialled by users to initiate a diversion for specific reasons. An absence diversion can be cancelled by dialing the VDN extension followed by # #. The following steps are needed to configure Absence diversions:

- Configure VDN 1
- Configure Vector 1
- Configure VDN 2
- Configure Vector 2

5.14.1. Configure VDN 1

During compliance testing VDN 56007 was used. Use the “add vdn x” command, (where **x** is the VDN) and configure the following:

- **Name*:** Enter an informative name (i.e. Phone diversion)
- **Destination:** Enter **Vector Number 7**

```
change vdn 3346                                     Page 1 of 3
VECTOR DIRECTORY NUMBER
Extension: 3346
Name*: Absence Diversion
Destination: Vector Number 7
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*:
```


5.14.2. Configure Vector 7

Configure the Vector that was used as the **Vector Number** in **Section 5.14.1** Use the “add vector 7” command, and configure the following:

- **Name:** Enter an informative name (i.e. Phone diversion)
- **Line 01:** Enter **wait-time 1 secs hearing silence**
- **Line 02:** Enter **collect 9 digits after announcement none for none**
- **Line 03:** Enter **route-to number 3347 with cov n if unconditionally**

In this example, using monitored phone dial 3346 + reason code + #, call is routed to 3347 which will trigger Trio Enterprise to set the phone absence with appropriate reason announcement.

```
change vector 7                                     Page 1 of 6
                                                    CALL VECTOR

Number: 7                                           Name: Absence-Diver
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      1      secs hearing silence
02 collect      9      digits after announcement none      for none
03 route-to      number 3347      with cov n if unconditionally
04
```

5.14.3. Configure VDN 2

Configure a VDN using the **route-to number** as used in **Section 5.14.2**. This VDN is used for activating referrals from the phone set. Use the “add vdn 3347” command, and configure the following:

- **Name*:** Enter an informative name (i.e. Trio Route Number)
- **Destination:** Enter **Vector Number 8**

```
change vdn 3347                                     Page 1 of 3
                                                    VECTOR DIRECTORY NUMBER

Extension: 3347
Name*: Trio Route Number
Destination: Vector Number      8
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*:
```

5.14.4. Configure Vector 8

Configure the Vector that was used as the **Vector Number** in **Section 5.14.3**. Use the “add vector 8” command, and configure the following:

- **Name:** Enter an informative name (i.e. Diversion)
- **Line 01** Enter **wait-time 100 secs hearing ringback**
- **Line 02** Enter **stop**

change vector 8		Page 1 of 6	
CALL VECTOR			
Number: 8		Name: Diversion	
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	100 secs hearing silence		
02 stop			

6. Configuration of Avaya Aura® Application Enablement Services

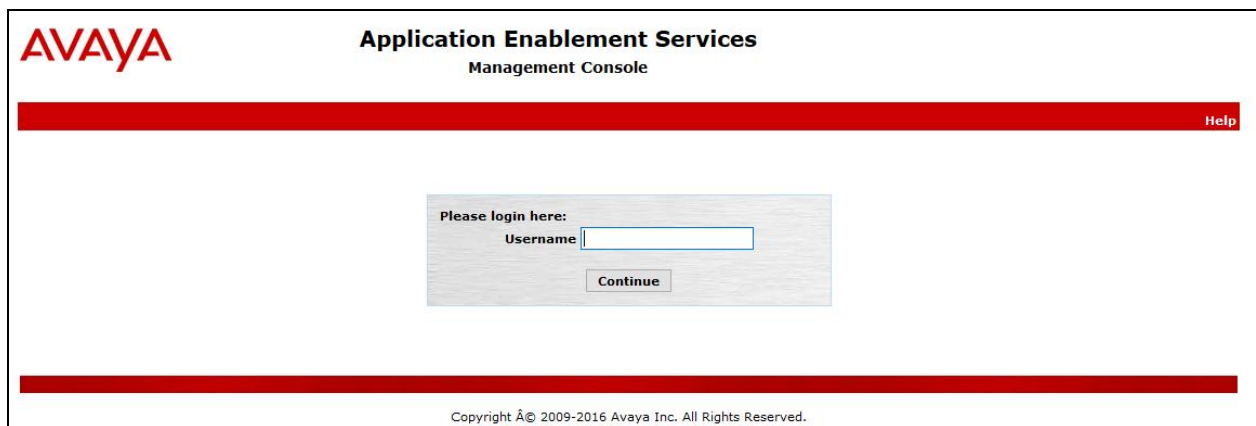
This section provides the procedures for configuring Avaya Application Enablement Services. It is implied a working AES is already in place and the Security Database (SDB) is configured. For all other provisioning information such as initial installation and configuration, please refer to the product documentation in **Section 11**. The configuration operations described in this section can be summarized as follows:

- Logging into Avaya Aura® Application Enablement Services
- Verify Avaya Aura® Application Enablement Services License
- Create a Avaya Aura® Communication Manager Switch Connection
- Create a TSAPI Link
- Create CTI User
- Configure Security Database
- Obtain Tlink Name
- Disable Security Database
- Enable Ports
- Restart TSAPI Service

6.1. Logging into the Avaya Aura® Application Enablement Services

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

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



The screenshot shows the Avaya Application Enablement Services Management Console login interface. At the top left is the Avaya logo. To its right, the text "Application Enablement Services" and "Management Console" is displayed. A red horizontal bar spans the width of the page, with a "Help" link on the right. In the center, there is a login box with the text "Please login here:" followed by a "Username" label and a text input field. Below the input field is a "Continue" button. At the bottom of the page, a red horizontal bar is present, and below it, the copyright notice "Copyright © 2009-2016 Avaya Inc. All Rights Reserved." is displayed.

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

The screenshot shows the Avaya Application Enablement Services Management Console. The top header is red with the Avaya logo and the text "Application Enablement Services Management Console". On the right, a welcome message displays user information: "Welcome: User cust", "Last login: Thu May 18 11:27:06 2017 from 135.10.98.86", "Number of prior failed login attempts: 0", "HostName/IP: aes70/10.33.1.4", "Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE", "SW Version: 7.0.1.0.4.15-0", "Server Date and Time: Tue May 23 15:43:46 EDT 2017", and "HA Status: Not Configured". Below the header is a red navigation bar with "Home | Help | Logout". The left sidebar contains a list of menu items: AE Services, Communication Manager Interface, High Availability, Licensing, Maintenance, Networking, Security, Status, User Management, Utilities, and Help. The main content area is titled "Welcome to OAM" and contains a paragraph: "The AE Services Operations, Administration, and Management (OAM) Web provides you with tools for managing the AE Server. OAM spans the following administrative domains:". This is followed by a bulleted list of domains and their functions: AE Services (manage all AE Services), Communication Manager Interface (manage switch connection and dialplan), High Availability (manage AE Services HA), Licensing (manage the license server), Maintenance (manage routine maintenance tasks), Networking (manage network interfaces and ports), Security (manage Linux user accounts, certificate, host authentication and authorization, configure Linux-PAM), Status (obtain server status informations), User Management (manage AE Services users and AE Services user-related resources), and Utilities (carry out basic connectivity tests).

6.2. Verify Avaya Aura® Application Enablement Services License

Select **Licensing** → **WebLM Server Access** in the left pane, to display the **Web License Manager** pop-up screen (not shown), and log in using the appropriate credentials.

The screenshot shows the Licensing page in the Avaya Application Enablement Services Management Console. The top header is red with the text "Licensing" and "Home | Help | Logout". The left sidebar contains a list of menu items: 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 main content area is titled "Licensing" and contains three paragraphs of instructions: "If you are setting up and maintaining the WebLM, you need to use the following:" followed by a bulleted list containing "WebLM Server Address"; "If you are importing, setting up and maintaining the license, you need to use the following:" followed by a bulleted list containing "WebLM Server Access"; and "If you want to administer TSAPI Reserved Licenses or DMCC Reserved Licenses, you need to use the following:" followed by a bulleted list containing "Reserved Licenses". A red note at the bottom states: "NOTE: Please disable your pop-up blocker if you are having difficulty with opening this page".

The **Web License Manager** screen below is displayed. Select **Licensed products** → **APPL_ENAB** → **Application_Enablement** in the left pane, to display the **Application Enablement (CTI)** screen in the right pane.

Verify that there are sufficient licenses for **TSAPI Simultaneous Users** as shown below. Note that the TSAPI license is required for Telephony Web Service.

APPL_ENAB
Application_Enablement
View license capacity
View peak usage
CCTR
ContactCenter
CIE
CIE
COMMUNICATION_MANAGER
Call_Center
Communication_Manager
Configure Centralized Licensing
MESSAGING
Messaging
SessionManager
SessionManager

License installed on: October 13, 2015 8:25:48 AM 04.0

License File Host IDs: [REDACTED]

Licensed Features

10 Items Show All

Feature (License Keyword)	Expiration date	Licen
Unified CC API Desktop Edition VALUE_AES_AEC_UNIFIED_CC_DESKTOP	permanent	100
CVLAN ASAI VALUE_AES_CVLAN_ASAI	permanent	16
Device Media and Call Control VALUE_AES_DMCC_DMC	permanent	100
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	100

6.3. Create a Avaya Aura® Communication Manager Switch Connection

A Communication Manager Switch Connection needs to be created to enable the AES to communicate with the Communication Manager. Navigate to **Communication Manager Interface → Switch Connections**. In the **Switch Connections** page, enter an informative name for the Communication Manager (i.e. DevvmCM). Click on the **Add Connection** button.



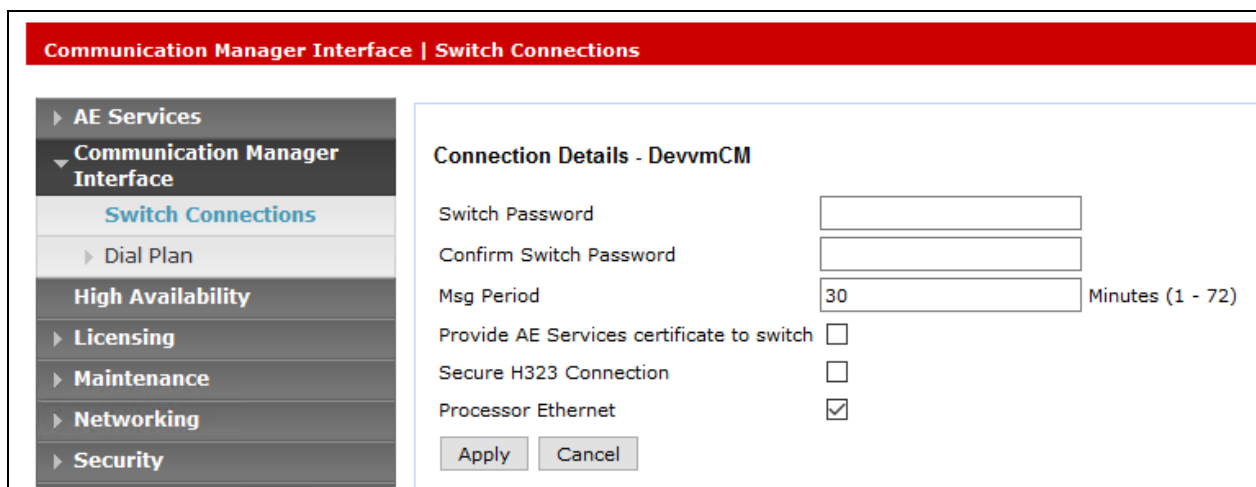
Communication Manager Interface | Switch Connections

AE Services
Communication Manager Interface
Switch Connections

Switch Connections

Add Connection

In the **Connection Details** window opens enter the **Switch Password** as was configured in **Section 5.12** and **Confirm Switch Password**. Click on the **Apply** button.



Communication Manager Interface | Switch Connections

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

Connection Details - DevvmCM

Switch Password

Confirm Switch Password

Msg Period Minutes (1 - 72)

Provide AE Services certificate to switch ☐

Secure H323 Connection ☐

Processor Ethernet ☒

Apply Cancel

Select **Communication Manager Interface** → **Switch Connections** from the left pane. The **Switch Connections** screen shows a listing of the existing switch connections.

Locate the connection name associated with the relevant Communication Manager, in this case “interopCM”, and select the corresponding radio button. Click **Edit PE/CLAN IPs**.

Communication Manager Interface | Switch Connections Home | Help

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

Switch Connections

Add Connection

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections
<input type="radio"/> CLAN1	No	30	1
<input checked="" type="radio"/> interopCM	Yes	30	1
<input type="radio"/> server1	Yes	30	0

Edit Connection Edit PE/CLAN IPs Edit H.323 Gatekeeper Delete Connection Survivability Hiera

The **Edit Processor Ethernet IP** screen is displayed. Enter the IP address of a C-LAN circuit pack or the Processor on Communication Manager to be used, in this case “10.33.1.6” as shown below, which is the Processor on Communication Manager. Click **Add/Edit Name or IP**. Screen below shows the already added IP.

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 - interopCM

10.33.1.6 Add/Edit Name or IP

Name or IP Address	Status
10.33.1.6	In Use

Back

6.4. Create a TSAPI Link

A TSAPI Link needs to be created to interoperate with Trio Enterprise. Navigate to **AE Services** → **TSAPI** → **TSAPI Links** and click on the **Add Link** button.

The screenshot shows the 'TSAPI Links' management page. On the left is a navigation menu with 'AE Services' expanded, showing 'CVLAN', 'DLG', 'DMCC', 'SMS', and 'TSAPI'. Under 'TSAPI', 'TSAPI Links' is selected. The main area is titled 'TSAPI Links' and contains a table with the following headers: 'Link', 'Switch Connection', 'Switch CTI Link #', 'ASAI Link Version', and 'Security'. Below the table are three buttons: 'Add Link', 'Edit Link', and 'Delete Link'.

Once the **Add TSAPI Links** window opens enter the following:

- **Link:** Select the next available Link from the dropdown box
- **Switch Connection:** Select **interopCM** from the dropdown box. (The Switch connection as created in **Section 6.3**)
- **Switch CTI Link Number:** Select **1** from the dropdown box. (The CTI link as created in **Section 5.1313**)
- **ASAI Link Version:** **7**
- **Security:** Select **Both** from the dropdown box

Click on the Apply Changes button.

The screenshot shows the 'Edit TSAPI Links' window. The left navigation menu is the same as the previous screenshot. The main area is titled 'Edit TSAPI Links' and contains the following fields and buttons:

- Link:** 1
- Switch Connection:** interopCM
- Switch CTI Link Number:** 1
- ASAI Link Version:** 7
- Security:** Both

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

6.5. Create CTI User

Navigate to **User Manager** → **User Admin**, and select **Add User**. On the **Add User** screen enter the following:

- **User Id:** Enter an informative name (i.e. trio). This ID is required for the Trio Enterprise installation
- **Common Name:** Enter a Common Name (i.e. **Trio**)
- **Surname:** Enter a Surname (i.e. **Trio**)
- **User Password:** Enter a password. This password is be required for the Trio Enterprise Installation
- **Confirm Password:** Confirm the password
- **Avaya Role** Select **userservice.useradmin** from the dropdown box
- **CT User:** Select **Yes** from the dropdown box

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

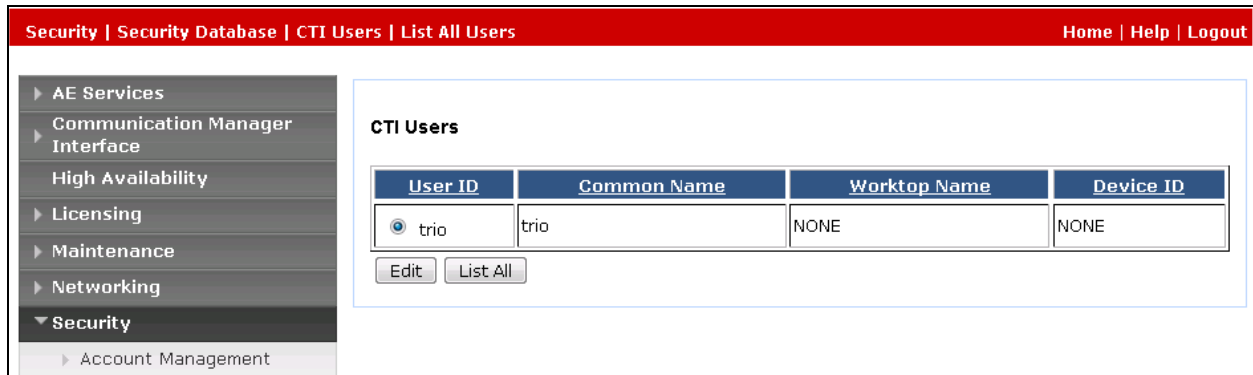
User Management | User Admin | List All Users Home | Help | Logout

Edit User

* User Id	<input type="text" value="trio"/>
* Common Name	<input type="text" value="trio"/>
* Surname	<input type="text" value="trio"/>
User Password	<input type="password"/>
Confirm Password	<input type="password"/>
Admin Note	<input type="text"/>
Avaya Role	<input type="text" value="userservice.useradmin"/>
Business Category	<input type="text"/>
Car License	<input type="text"/>
CM Home	<input type="text"/>
Cms Home	<input type="text"/>
CT User	<input type="text" value="Yes"/>
Department Number	<input type="text"/>
Display Name	<input type="text"/>
Employee Number	<input type="text"/>
Employee Type	<input type="text"/>

6.6. Configure Security Database

Navigate to the users screen by selecting **Security** → **Security Database** → **CTI Users** → **List All Users**. In the **CTI Users** window, select the radio button relating to the CTI user created in **Section 6.5** (trio) and click on the **Edit** button.



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

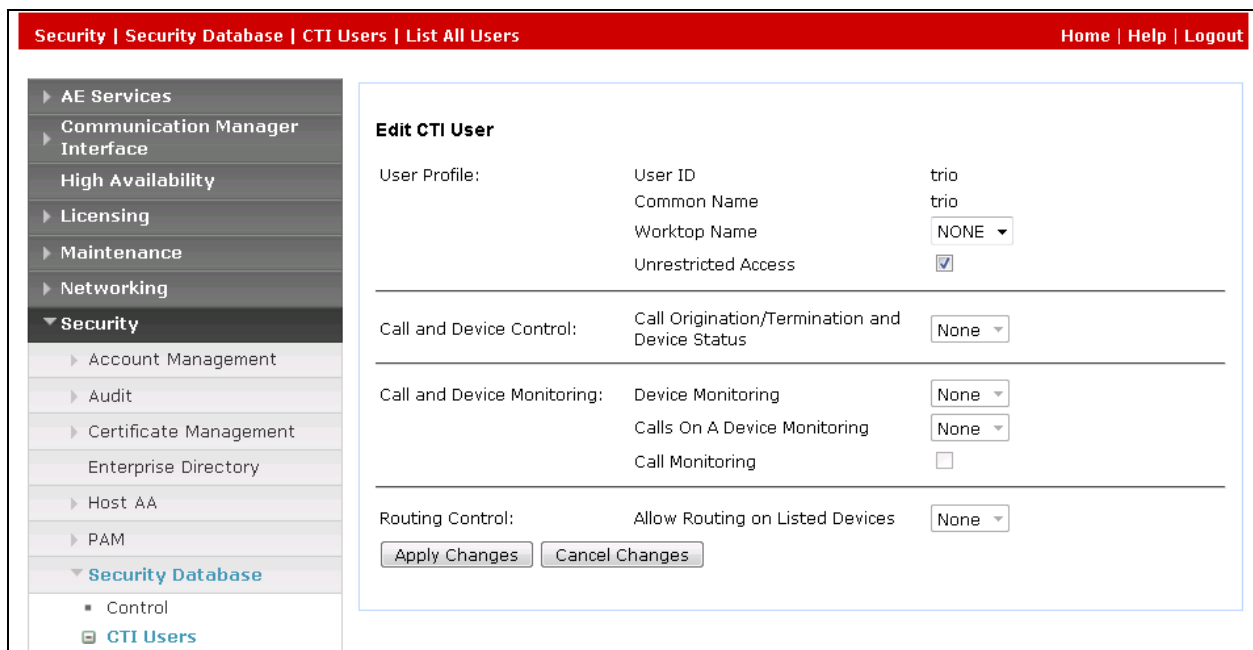
AE Services
Communication Manager Interface
High Availability
Licensing
Maintenance
Networking
Security
Account Management

CTI Users

User ID	Common Name	Worktop Name	Device ID
<input checked="" type="radio"/> trio	trio	NONE	NONE

Edit List All

Once the **Edit CTI User** page appears, tick the **Unrestricted Access** check box and **Apply Changes** at the bottom of the screen.



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

AE Services
Communication Manager Interface
High Availability
Licensing
Maintenance
Networking
Security
Account Management
Audit
Certificate Management
Enterprise Directory
Host AA
PAM
Security Database
Control
CTI Users

Edit CTI User

User Profile: User ID: trio
Common Name: trio
Worktop Name: NONE
Unrestricted Access: ☒

Call and Device Control: Call Origination/Termination and Device Status: None

Call and Device Monitoring: Device Monitoring: None
Calls On A Device Monitoring: None
Call Monitoring: ☐

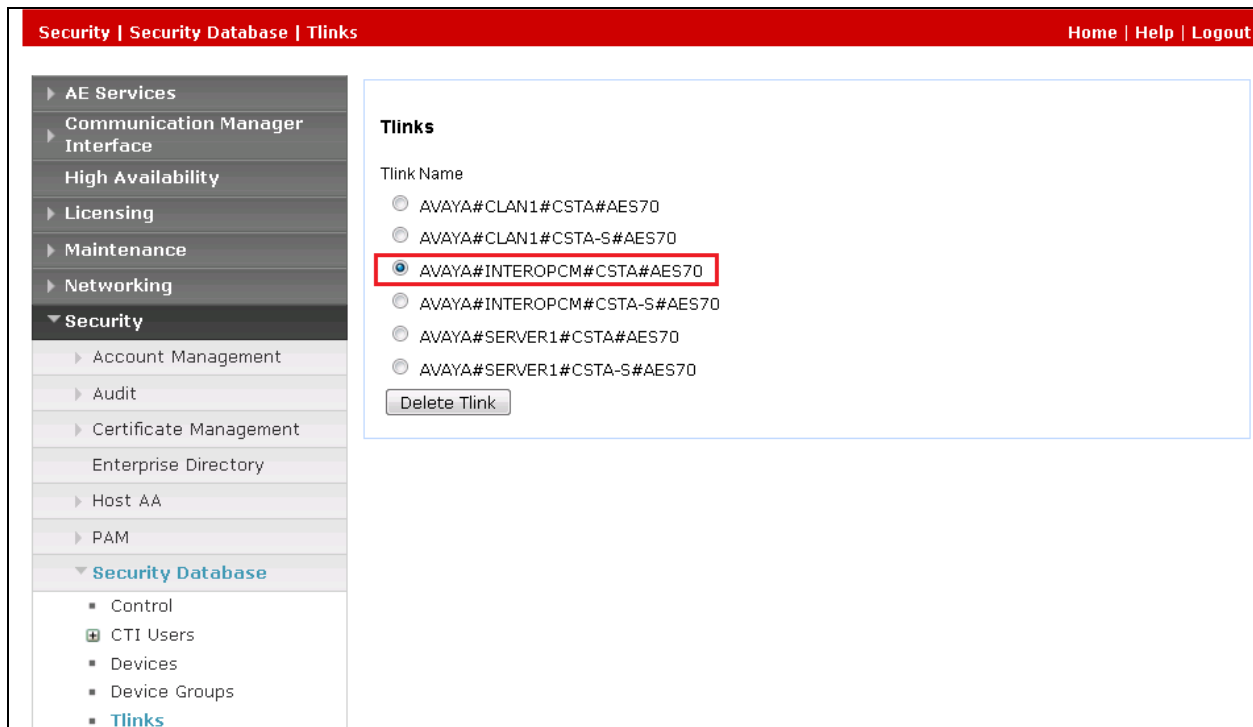
Routing Control: Allow Routing on Listed Devices: None

Apply Changes Cancel Changes

6.7. Obtain Tlink Name

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

In this case, the associated Tlink name is “AVAYA#INTEROPCM#CSTA#AES70”. Note the use of the switch connection “interopCM” from **Section 6.3** as part of the Tlink name.



6.8. Disable Security Database

Select **Security** → **Security Database** → **Control** from the left pane, to display the **SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services** screen in the right pane. Uncheck both fields below.

Security | Security Database | Control

▶ AE Services
▶ Communication Manager Interface
▶ High Availability
▶ Licensing
▶ Maintenance
▶ Networking
▼ **Security**
▶ Account Management
▶ Audit
▶ Certificate Management
Enterprise Directory
▶ Host AA
▶ PAM
▼ **Security Database**
▪ **Control**

SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services

☐ Enable SDB for DMCC Service
☐ Enable SDB for TSAPI Service, JTAPI and Telephony Web Services

Apply Changes

6.9. Enable Ports

Select **Networking** → **Ports** from the left pane, to display the **Ports** screen in the right pane.

In the **TSAPI Ports** section, select the radio button for **TSAPI Service Port** under the **Enabled** column, as shown below. Retain the default values in the remaining fields.

Networking | Ports

▶ 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

Unencrypted TCP Port9999

Enabled Disabled

☒ ☐

Encrypted TCP Port

9998

☒ ☐

DLG Port

TCP Port

5678

TSAPI Ports

TSAPI Service Port450

Enabled Disabled

☒ ☐

Local TLINK Ports

TCP Port Min1024

TCP Port Max1039

Unencrypted TLINK Ports

TCP Port Min1050

TCP Port Max1065

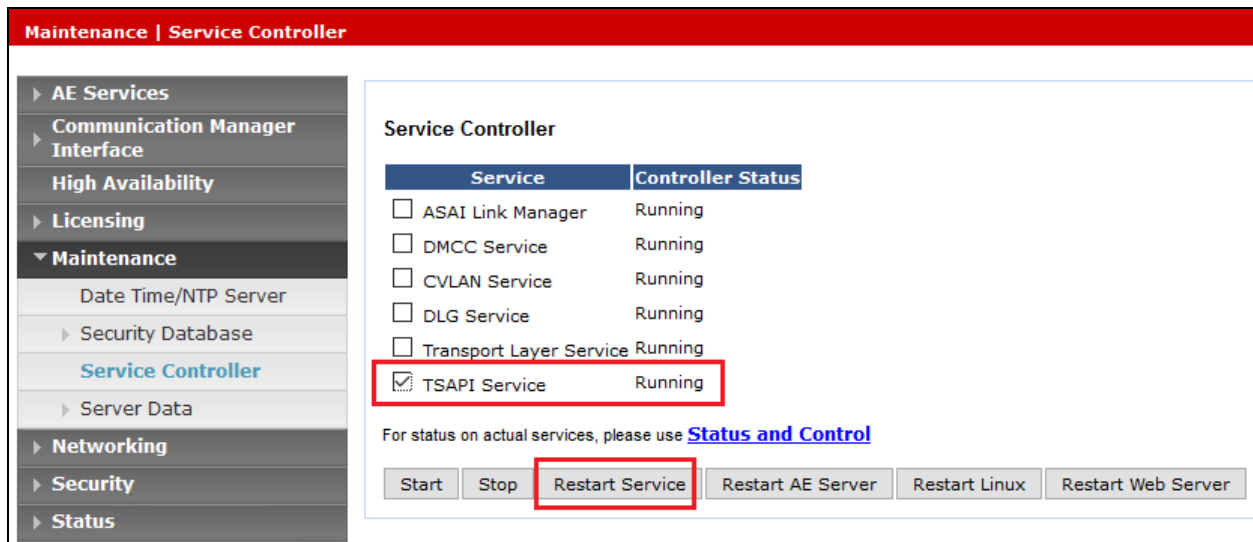
Encrypted TLINK Ports

TCP Port Min1066

TCP Port Max1081

6.10. Restart TSAPI Service

After the AES configuration is completed the TSAPI service needs to be restarted. To restart navigate to **Maintenance** → **Service Controller**. Check the **TSAPI Service** check box and click on the **Restart Service** button.



The screenshot shows the 'Maintenance | Service Controller' interface. On the left is a navigation menu with options: AE Services, Communication Manager Interface, High Availability, Licensing, Maintenance (selected), Date Time/NTP Server, Security Database, Service Controller (highlighted), Server Data, Networking, Security, and Status. The main area is titled 'Service Controller' and contains a table with two columns: 'Service' and 'Controller Status'. The table lists several services, with 'TSAPI Service' checked and highlighted by a red box. Below the table, there is a link 'Status and Control' and a row of buttons: Start, Stop, Restart Service (highlighted with a red box), Restart AE Server, Restart Linux, and Restart Web Server.

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

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

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

When the Restart page opens click on the **Restart button** (not shown).

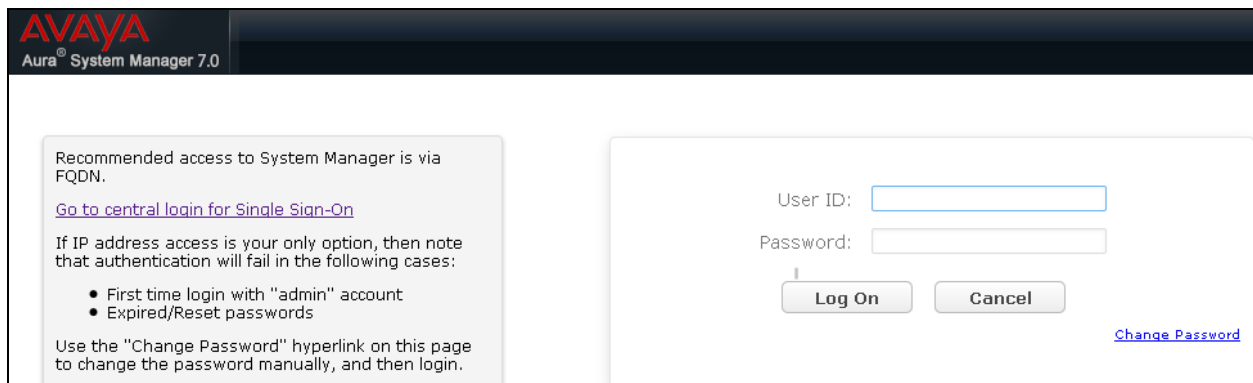
7. Configure Avaya Aura® Session Manager

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

- Launch System Manager
- Administer Domain
- Administer locations
- Administer Adaptation
- Administer SIP entities
- Administer routing policies
- Administer dial patterns

7.1. Launch System Manager

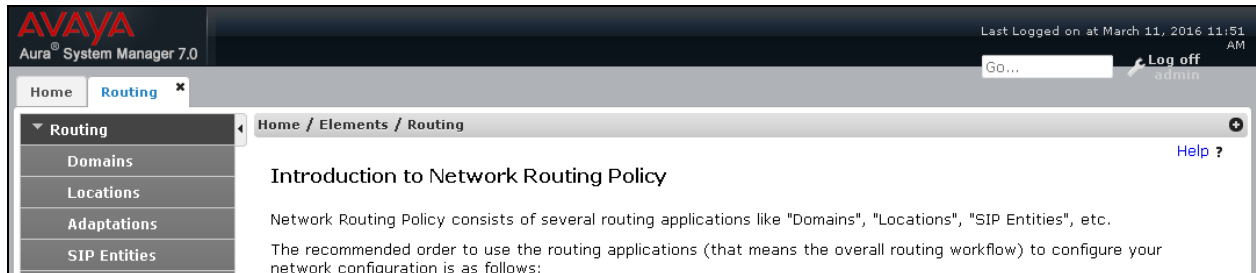
Access the System Manager web interface by using the URL “https://ip-address” in an Internet browser window, where “ip-address” is the IP address of System Manager. Log in using the appropriate credentials.



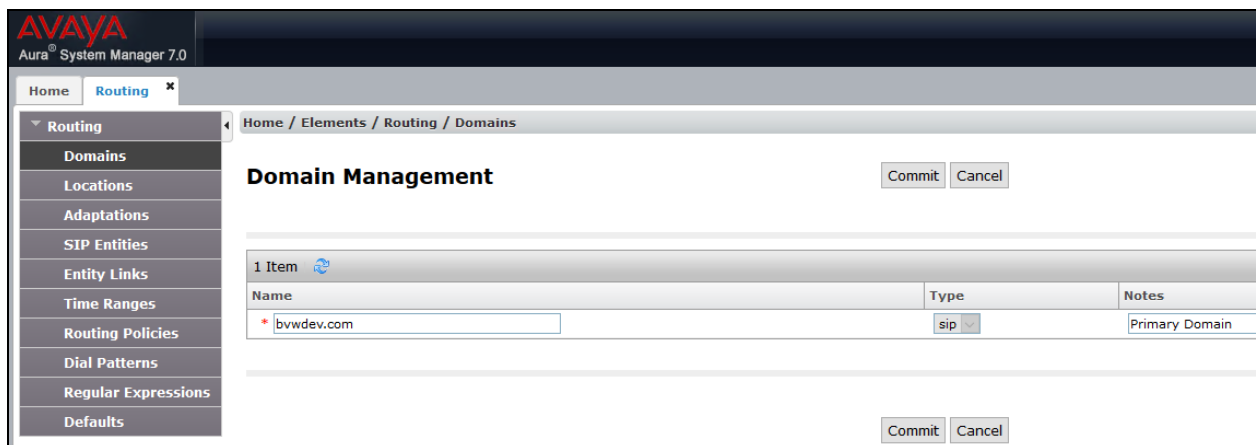
The screenshot shows the Avaya Aura System Manager 7.0 login interface. The header features the Avaya logo and the text "Aura® System Manager 7.0". The main content area is divided into two sections. The left section contains a message: "Recommended access to System Manager is via FQDN." followed by a link "Go to central login for Single Sign-On". Below this, it states: "If IP address access is your only option, then note that authentication will fail in the following cases:" and lists two bullet points: "• First time login with 'admin' account" and "• Expired/Reset passwords". It also includes a note: "Use the 'Change Password' hyperlink on this page to change the password manually, and then login." The right section contains the login form with fields for "User ID:" and "Password:", and buttons for "Log On" and "Cancel". A "Change Password" link is located at the bottom right of the login form.

7.2. Administer Domain

In the subsequent screen (not shown), select **Elements → Routing** to display the **Introduction to Network Routing Policy** screen below. Select **Routing → Domains** from the left pane, and click **New** in the subsequent screen (not shown) to add a new domain



The **Domain Management** screen is displayed. In the **Name** field enter the domain name, select *sip* from the **Type** drop down menu and provide any optional **Notes**.



7.3. Administer Locations

Select **Routing** → **Locations** from the left pane, and click **New** in the subsequent screen (not shown) to add a new location for Trio Enterprise.

The **Location Details** screen is displayed. In the **General** sub-section, enter a descriptive **Name** and optional **Notes**. Retain the default values in the remaining fields.

AVAYA
Aura® System Manager 7.0

Last Logged on at May 23, 201

Home Routing

Home / Elements / Routing / Locations

Location Details

Commit Cancel

General

* Name: BvwDevSIL

Notes:

Scroll down to the **Location Pattern** sub-section, click **Add** and enter the IP address of all devices involved in the compliance testing in **IP Address Pattern**, as shown below. Retain the default values in the remaining fields.

Location Pattern

Add Remove

4 Items Filter: Enable

IP Address Pattern	Notes
* 10.10.5.*	
* 10.10.97.*	
* 10.10.98.*	
*	

Select : All, None

Commit Cancel

7.4. Administer Adaptation

During compliance test, in order to make the call from and to Communication Manager via Session Manager, Adaptation to translate IP address into domain name is used for Trio SIP entity. Here is step on how to create Adaptation. Select **Adaptations** on the left panel menu and then click on the **New** button in the main window (not shown). Enter the following for the Trio Adaptation.

- **Adaptation Name** An informative name (e.g., **change IP to Domain Trio**)
- **Module Name** Select **DigitConversionAdapter**
- **Module Parameter Type** Select Name-Value Parameter

Click **Add** to add a new row for the following values as shown below table:

Name	Value
fromto	true
iodstd	Enter the domain name of system, ex: bvwddev.com
iosrcd	Enter the domain name of system, ex: bvwddev.com
odstd	Enter IP address of Trio, ex: 10.10.98.9
osrcd	Enter IP Address of Session Manager, ex: 10.33.1.12

Once the correct information is entered click the **Commit** button. Here is the screenshot show Adaptation created for Trio.

AVAYA
Aura® System Manager 7.0

Last Logged on at May 23, 2017

Home / Elements / Routing / Adaptations

Adaptation Details

Commit Cancel

General

* Adaptation Name: Trio Adapt

* Module Name: DigitConversionAdapter

Module Parameter Type: Name-Value Parameter

Add Remove

Name	Value
fromto	true
iodstd	bvwddev.com
iosrcd	bvwddev.com

(Continue) the screenshot show Adaptation created for Trio:

The screenshot displays the Avaya Aura System Manager 7.0 interface. The top header shows the Avaya logo and 'Aura® System Manager 7.0'. The left sidebar contains a navigation menu with 'Routing' selected, showing sub-items like Domains, Locations, Adaptations, SIP Entities, Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area is titled 'Adaptation Details' and shows the 'General' tab. The 'Adaptation Name' is 'Trio Adapt', the 'Module Name' is 'DigitConversionAdapter', and the 'Module Parameter Type' is 'Name-Value Parameter'. Below this is a table with two rows: 'odstd' with value '10.10.98.9' and 'osrcd' with value '10.33.1.12'. The bottom of the page shows 'Page 2 of 2'.

AVAYA
Aura® System Manager 7.0

Home / Elements / Routing / Adaptations

Adaptation Details

Commit Cancel

General

* Adaptation Name: Trio Adapt

* Module Name: DigitConversionAdapter

Module Parameter Type: Name-Value Parameter

Name	Value
odstd	10.10.98.9
osrcd	10.33.1.12

Select : All, None Page 2 of 2

7.5. Administer SIP Entities

A SIP Entity must be added for Session Manager and for each SIP telephony system connected to it, which includes Communication Manager and Trio Enterprise.

7.5.1. SIP Entity for Session Manager

Navigate to **Routing** → **SIP Entities** in the left navigation pane and click on the **New** button in the right pane (not shown). In the **General** section, enter the following values. Use default values for all remaining fields:

- **Name:** Enter a descriptive name.
- **FQDN or IP Address:** Enter the FQDN or IP address of the SIP Entity that is used for SIP signaling.
- **Type:** Select *Session Manager* for Session Manager.
- **Adaptation:** This field is only present if **Type** is not set to **Session Manager** if Adaptations were to be created, here is where they would be applied to the entity.
- **Location:** Select the location that applies to the SIP Entity being created, defined in **Section 7.3**.
- **Time Zone:** Select the time zone for the location above.

The following screen shows the addition of the *Session Manager* SIP Entity for Session Manager. The IP address of the Session Manager Security Module is entered in the **FQDN or IP Address** field.

The screenshot displays the Avaya Aura System Manager 7.0 web interface. The top navigation bar includes the Avaya logo, the text 'Aura System Manager 7.0', and a 'Last Logged on at May 23, 2017' status. The main navigation pane on the left lists various configuration areas: Home, Session Manager, Routing, Domains, Locations, Adaptations, SIP Entities (selected), Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area is titled 'SIP Entity Details' and shows the 'General' tab. The form contains the following fields: 'Name' (required, value: ASM70A), 'FQDN or IP Address' (required, value: 10.33.1.12), 'Type' (dropdown menu, value: Session Manager), 'Notes' (text area), 'Location' (dropdown menu, value: BvwDevSIL), 'Outbound Proxy' (dropdown menu), 'Time Zone' (dropdown menu, value: America/Toronto), and 'Credential name' (text field). At the bottom, there is a 'SIP Link Monitoring' section with a dropdown menu set to 'Use Session Manager Configuration'. 'Commit' and 'Cancel' buttons are located at the top right of the form area.

7.5.2. SIP Entity for Communication Manager

Select **Routing** → **SIP Entities** from the left pane, and click **New** in the subsequent screen (not shown) to add a new SIP entity for Communication Manager. Note that this SIP entity is used for integration with Trio Enterprise.

The **SIP Entity Details** screen is displayed. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Name:** A descriptive name.
- **FQDN or IP Address:** The IP address of an existing CLAN or the processor interface.
- **Type:** Select “CM” in the dropdown list.
- **Notes:** Any desired notes.
- **Location:** Select the applicable location for Communication Manager.
- **Time Zone:** Select the applicable time zone.

AVAYA
Aura® System Manager 7.0

Last Logged on at May 23, 201

Go... Log out

Home / Elements / Routing / SIP Entities

SIP Entity Details

Commit Cancel

General

* Name: ACM-Trunk1-Private

* FQDN or IP Address: 10.33.1.6

Type: CM

Notes:

Adaptation:

Location: BvwDevSIL

Time Zone: America/Toronto

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

Credential name:

Securable: ☐

Call Detail Recording: none

7.5.3. SIP Entity for Trio Enterprise

Select **Routing** → **SIP Entities** from the left pane, and click **New** in the subsequent screen (not shown) to add a new SIP entity for Trio Enterprise.

The **SIP Entity Details** screen is displayed. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Name:** A descriptive name.
- **FQDN or IP Address:** The IP address of the Trio Enterprise server.
- **Type:** Select “SIP Trunk” in the dropdown list.
- **Notes:** Any desired notes.
- **Adaptation:** Select the adaptation configured in **Section 7.4**
- **Location:** Select the applicable location from **Section 7.3**.
- **Time Zone:** Select the applicable time zone.

AVAYA
Aura® System Manager 7.0

Last Logged on at May 23, 2017

Home / Elements / Routing / SIP Entities

SIP Entity Details

Commit Cancel

General

* Name: Trio

* FQDN or IP Address: 10.10.98.9

Type: SIP Trunk

Notes:

Adaptation: Trio Adapt

Location: BvwDevSIL

Time Zone: America/Toronto

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

Credential name:

Securable: ☐

Call Detail Recording: none

7.6. Administer Entity Links

A SIP trunk between Session Manager and a telephony system is described by an Entity Link. Two Entity Links were created; one to the Communication Manager and one to Trio Enterprise. To add an Entity Link, select to **Routing** → **Entity Links** in the left navigation pane and click on the **New** button in the right pane (not shown). Fill in the following fields in the new row that is displayed:

- **Name:** Enter a descriptive name.
- **SIP Entity 1:** Select the Session Manager from the drop-down menu.
- **Protocol:** Select applicable transport protocol.
- **Port:** Port number on which Session Manager will receive SIP requests from the far-end.
- **SIP Entity 2:** Select the name of the other systems from the drop-down menu.
- **Port:** Port number on which the other system receives SIP requests from Session Manager.
- **Connection Policy:** Select **Trusted** to allow calls from the associated SIP Entity.

The screens below show the Entity Link to Communication Manager and Trio Enterprise. During the compliance test, **TLS** transport with port **5061** was used between Session Manager and Communication Manager.

The screenshot shows the 'Entity Links' configuration page. The breadcrumb is 'Home / Elements / Routing / Entity Links'. There are 'Commit' and 'Cancel' buttons. Below the title, there is a table with one item. The table has columns: Name, SIP Entity 1, Protocol, Port, SIP Entity 2, DNS Override, and Port. The data row shows: Name: *ASM70_ACM_Trunk1_50, SIP Entity 1: *ASM70A, Protocol: TLS, Port: *5061, SIP Entity 2: *ACM-Trunk1-Private, DNS Override: ☐, Port: *5061. At the bottom, there is a 'Select : All, None' dropdown.

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	DNS Override	Port
*ASM70_ACM_Trunk1_50	*ASM70A	TLS	*5061	*ACM-Trunk1-Private	<input type="checkbox"/>	*5061

The Entity Link to Trio Enterprise is shown below; **TCP** transport and port **5060** were used.

The screenshot shows the 'Entity Links' configuration page. The breadcrumb is 'Home / Elements / Routing / Entity Links'. There are 'Commit' and 'Cancel' buttons. Below the title, there is a table with one item. The table has columns: Name, SIP Entity 1, Protocol, Port, SIP Entity 2, DNS Override, and Port. The data row shows: Name: *ASM70A_Trio_5060_TCF, SIP Entity 1: *ASM70A, Protocol: TCP, Port: *5060, SIP Entity 2: *Trio, DNS Override: ☐, Port: *5060. At the bottom, there is a 'Select : All, None' dropdown.

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	DNS Override	Port
*ASM70A_Trio_5060_TCF	*ASM70A	TCP	*5060	*Trio	<input type="checkbox"/>	*5060

7.7. Administer Routing Policies

Routing policies describe the conditions under which calls will be routed to the SIP Entities specified in **Section 7.5**. Two routing policies were added: an incoming policy with Communication Manager as the destination, and an incoming policy to Trio Enterprise. To add a routing policy, select to **Routing → Routing Policies** in the left navigation pane and click on the **New** button in the right pane (not shown). The following screen is displayed:

- In the **General** section, enter a descriptive **Name** and add a brief description under **Notes** (optional).
- In the **SIP Entity as Destination** section, click **Select**. The **SIP Entity List** page opens (not shown). Choose the appropriate SIP entity to which this routing policy applies (**Section 6.5**) and click **Select**. The selected SIP Entity displays on the **Routing Policy Details** page as shown below.
- Use default values for remaining fields.
- Click **Commit** to save.

The following screens show the Routing Policy for Communication Manager.

The screenshot shows the Avaya Aura System Manager 7.0 interface. The left navigation pane is expanded to 'Routing', and 'Routing Policies' is selected. The main content area displays the 'Routing Policy Details' for a policy named 'To-CM-Trunk1'. The 'General' section includes fields for 'Name' (To-CM-Trunk1), 'Disabled' (unchecked), 'Retries' (0), and 'Notes'. The 'SIP Entity as Destination' section shows a 'Select' button and a table with the selected entity 'ACM-Trunk1-Private' with FQDN '10.33.1.6' and Type 'CM'. The interface includes a 'Commit' button and a 'Cancel' button.

Name	FQDN or IP Address	Type	Notes
ACM-Trunk1-Private	10.33.1.6	CM	

The following screens show the Routing Policy for Trio Enterprise.

The screenshot displays the Avaya Aura System Manager 7.0 web interface. The top navigation bar includes the Avaya logo, the text 'Aura® System Manager 7.0', and a 'Last Logged on at May 23, 2017' timestamp. Below this, a breadcrumb trail reads 'Home / Elements / Routing / Routing Policies'. The left sidebar contains a tree view with 'Routing' expanded, showing sub-items like Domains, Locations, Adaptations, SIP Entities, Entity Links, Time Ranges, Routing Policies (selected), Dial Patterns, Regular Expressions, and Defaults. The main content area is titled 'Routing Policy Details' and includes 'Commit' and 'Cancel' buttons. Under the 'General' tab, the 'Name' field is set to 'To-Trio', 'Disabled' is unchecked, 'Retries' is set to 0, and there is a 'Notes' field. Below this, the 'SIP Entity as Destination' section features a 'Select' button and a table with one entry: 'Trio' with FQDN or IP Address '10.10.98.9' and Type 'SIP Trunk'.

Routing Policy Details

General

* Name:

Disabled: ☐

* Retries:

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
Trio	10.10.98.9	SIP Trunk	

7.8. Administer Dial Patterns

Dial Patterns are needed to route specific calls through Session Manager. For the compliance test, dial patterns were needed to route calls from Communication Manager to Trio Enterprise and vice versa. Dial Patterns define which route policy will be selected for a particular call based on the dialed digits, destination domain and originating location.

7.8.1. Dial Pattern for Trio Enterprise

Select **Routing** → **Dial Patterns** from the left pane, and click **New** in the subsequent screen (not shown) to add a new dial pattern to reach Trio Enterprise. The **Dial Pattern Details** screen is displayed. In the **General** sub-section, enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Pattern:** A dial pattern to match, in this case “47”.
- **Min:** The minimum number of digits to match.
- **Max:** The maximum number of digits to match.
- **SIP Domain:** The signaling group domain name from **Section 7.2**.

In the **Originating Locations and Routing Policies** sub-section, click **Add** and create an entry for reaching Trio Enterprise. In the compliance testing, the entry allowed for call originations from Communication Manager endpoints in the location “BvwDevSIL”. The Trio Enterprise routing policy from **Section 7.5.3** was selected as shown below.

The screenshot displays the 'Dial Pattern Details' configuration page in Session Manager. The left sidebar shows the navigation menu with 'Dial Patterns' selected. The main content area is divided into two sections: 'General' and 'Originating Locations and Routing Policies'.

General Section:

- Pattern:** 47
- Min:** 4
- Max:** 4
- Emergency Call:** ☐
- Emergency Priority:** 1
- Emergency Type:** (empty)
- SIP Domain:** bwvdev.com
- Notes:** Dial pattern to Trio Enterprise

Originating Locations and Routing Policies Section:

Buttons: Add, Remove

1 Item

Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/> BvwDevSIL		To-Trio	0	<input type="checkbox"/>	Trio	

7.8.2. Dial Pattern for Communication Manager

Select **Routing** → **Dial Patterns** from the left pane, and click **New** in the subsequent screen (not shown) to add a new dial pattern to reach Communication Manager. The **Dial Pattern Details** screen is displayed. In the **General** sub-section, enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Pattern:** A dial pattern to match, in this case “33”.
- **Min:** The minimum number of digits to match.
- **Max:** The maximum number of digits to match.
- **SIP Domain:** The signaling group domain name from **Section 7.2**.

In the **Originating Locations and Routing Policies** sub-section, click **Add** and create an entry for reaching Communication Manager. In the compliance testing, the entry allowed for call originations from all Trio Enterprise endpoints in locations “BvwDevSIL”. The Communication Manager routing policy from **Section 7.5.2** was selected as shown below.

Home / Elements / Routing / Dial Patterns

Dial Pattern Details

Commit Cancel

General

* Pattern: 33

* Min: 4

* Max: 4

Emergency Call: ☐

Emergency Priority: 1

Emergency Type:

SIP Domain: bvwddev.com

Notes:

Originating Locations and Routing Policies

Add Remove

1 Item Filter: En

<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"/>	BvwDevSIL		To-CM-Trunk1	0	<input type="checkbox"/>	ACM-Trunk1-Private	

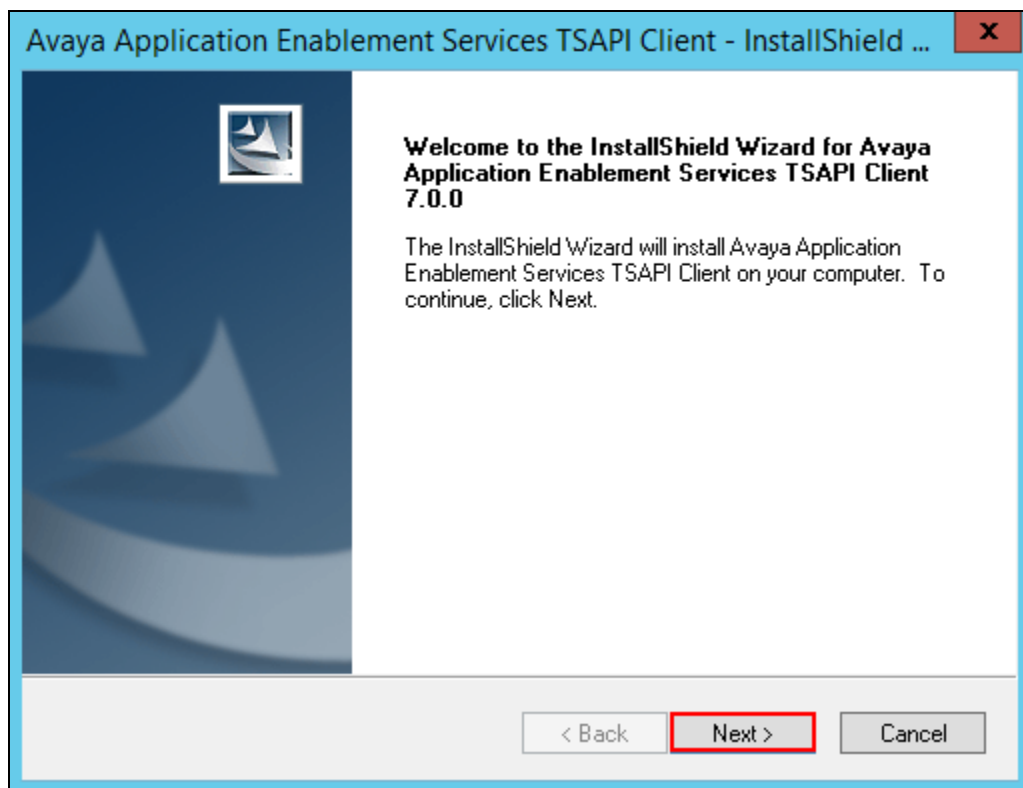
8. Configure Trio Enterprise

This section shows how to configure Trio Enterprise to successfully connect to Communication/AES. The installation of the Trio Enterprise software is assumed to be completed and the Trio Enterprise services are up and. The steps to configure SIP Trunks are as follows:

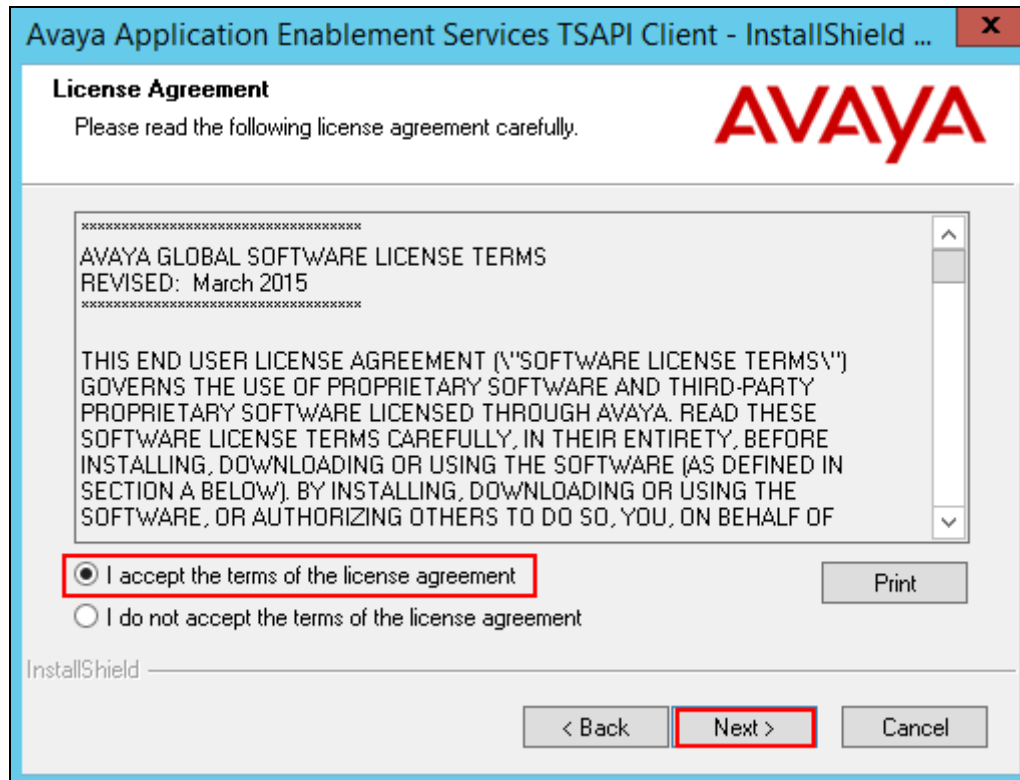
- Install Avaya Application Enablement Services TSAPI Client
- Configure Trio Enterprise to use SIP Trunks
- Configure Absence
- Configure Trio Enterprise Attendant

8.1. Install Avaya Application Enablement Services TSAPI Client

An InstallShield Wizard is used to install the Avaya Application Enablement Services TSAPI Client. Locate the InstallShield Wizard and once opened click on **Next**.



Accept the license agreement as shown below and click on **Next**.



In the subsequent window, enter the following:

- **Host Name or IP Address:** Enter the IP address of the AES
- **Port Number:** Enter **450**

Click on the **Next** button to continue.

Avaya Application Enablement Services TSAPI Client - InstallShield ...

AE Services Server Configuration
Configure your PC for AE Services TSAPI access.

AVAYA

For each AE Services server that you wish to use, enter the server's host name or IP address (for example, aeserver.mydomain.com or 198.51.100.24) and the TSAPI Service port number.

The configured AE Services servers will be saved in the TSLIB.INI file.

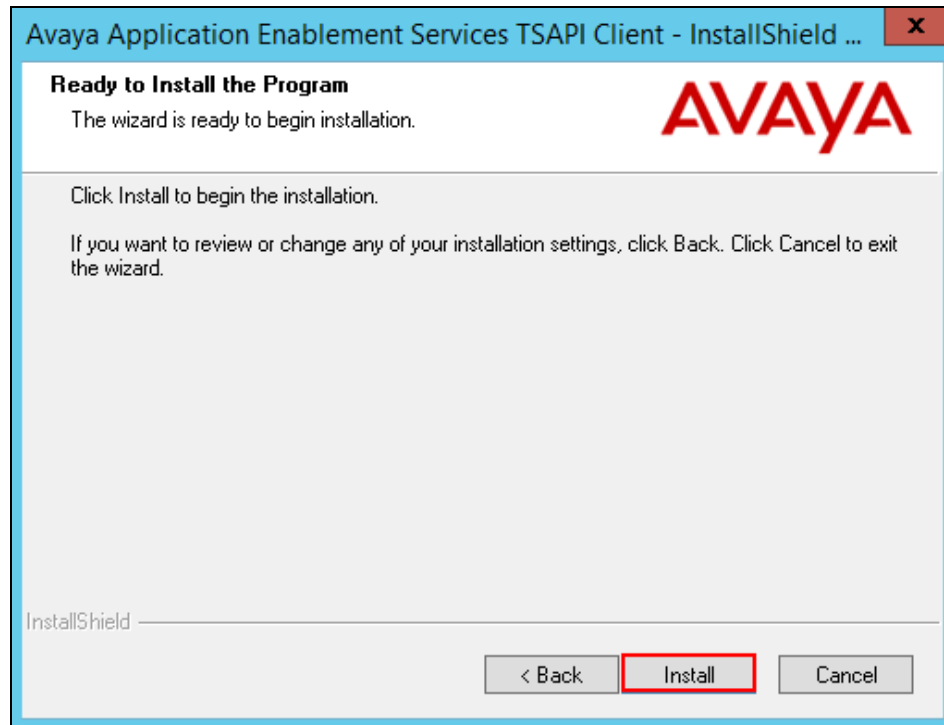
Host Name or IP Address: Port Number:

Configured AE Services Servers:

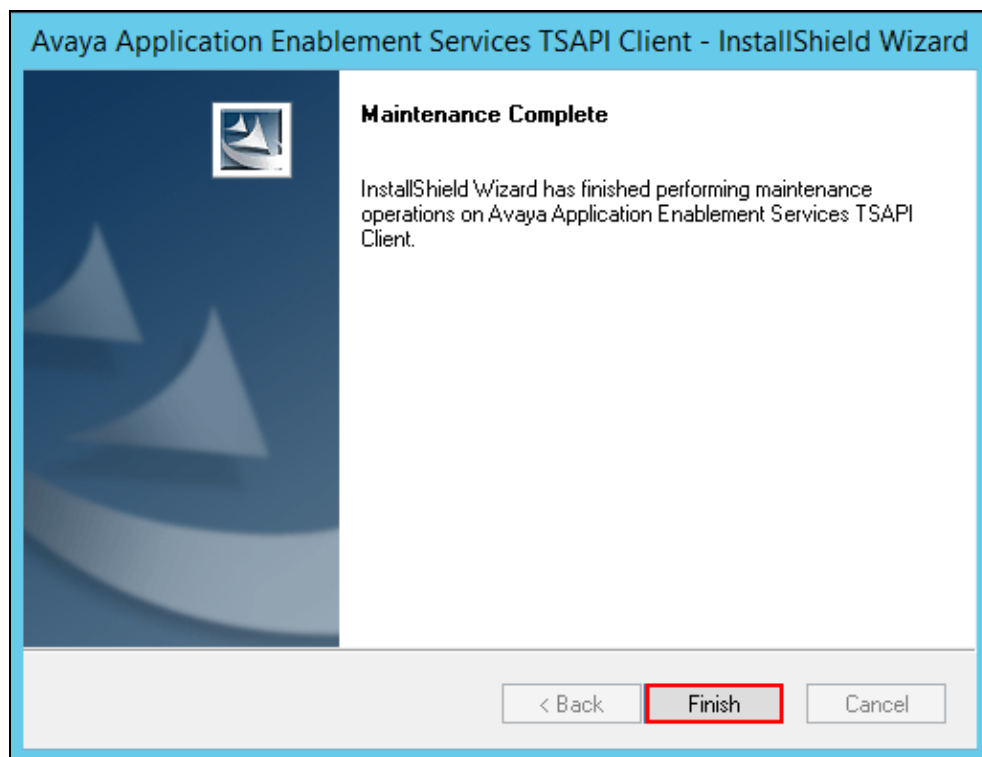
InstallShield

< Back **Next >** Cancel

In the subsequent window shown below, click on the **Install** button.



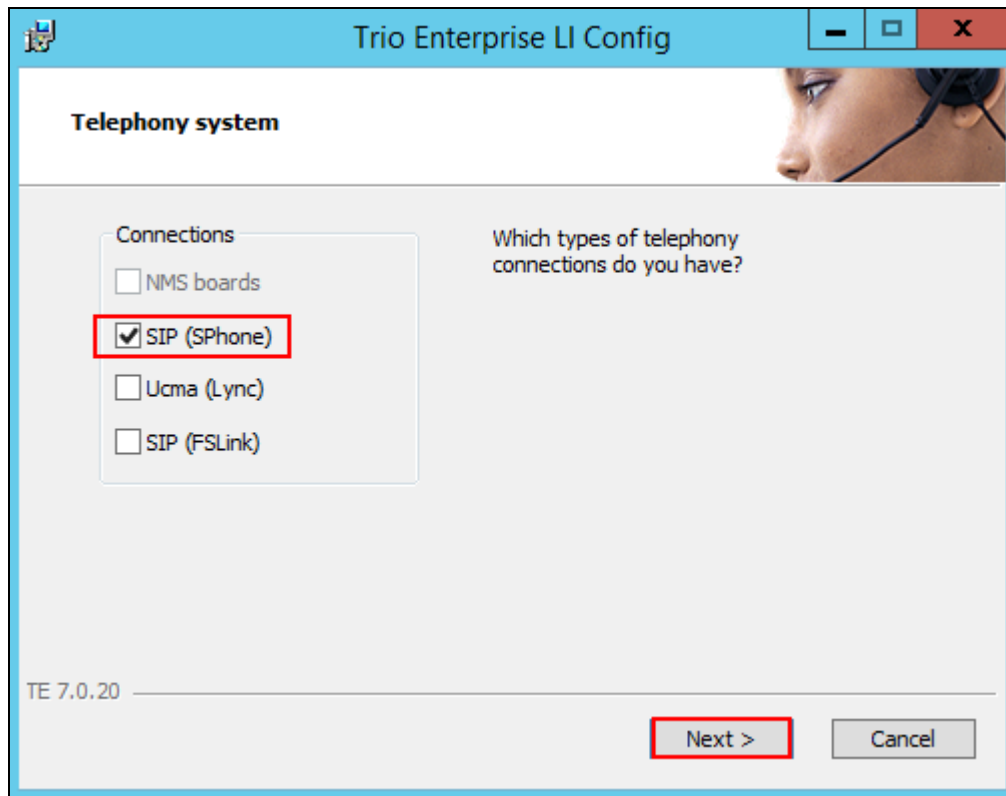
When the InstallShield Wizard Complete window appears click on the **Finish** button.



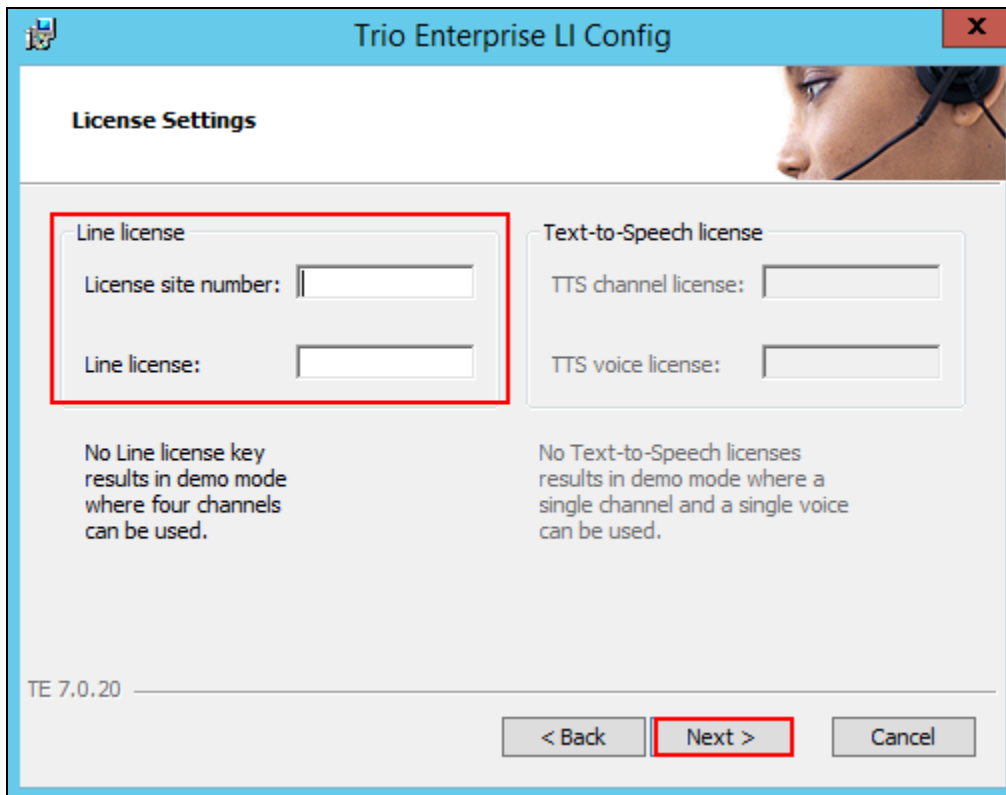
8.2. Configure Trio Enterprise to use SIP Trunks

Access Windows services. Select Start → Run, then type **services.msc** into the command line and press return (not shown). When the services window opens, locate the **Trio Televoice service**, right click and select **stop** to stop the service (not shown).

Launch the Trio configuration application. Select **Start → Programs → Trio Enterprise → TeleVoice Config** (not shown). The configuration of the application starts, and when the new window opens, check the **SIP** check box followed by the **Next** button.



In the subsequent window, enter the **License site number:** and **Line licence:** as supplied directly by Enghouse Interactive AB or the Trio Enterprise reseller. Click on the **Next** button to continue.



Trio Enterprise LI Config

License Settings

Line license

License site number:

Line license:

Text-to-Speech license

TTS channel license:

TTS voice license:

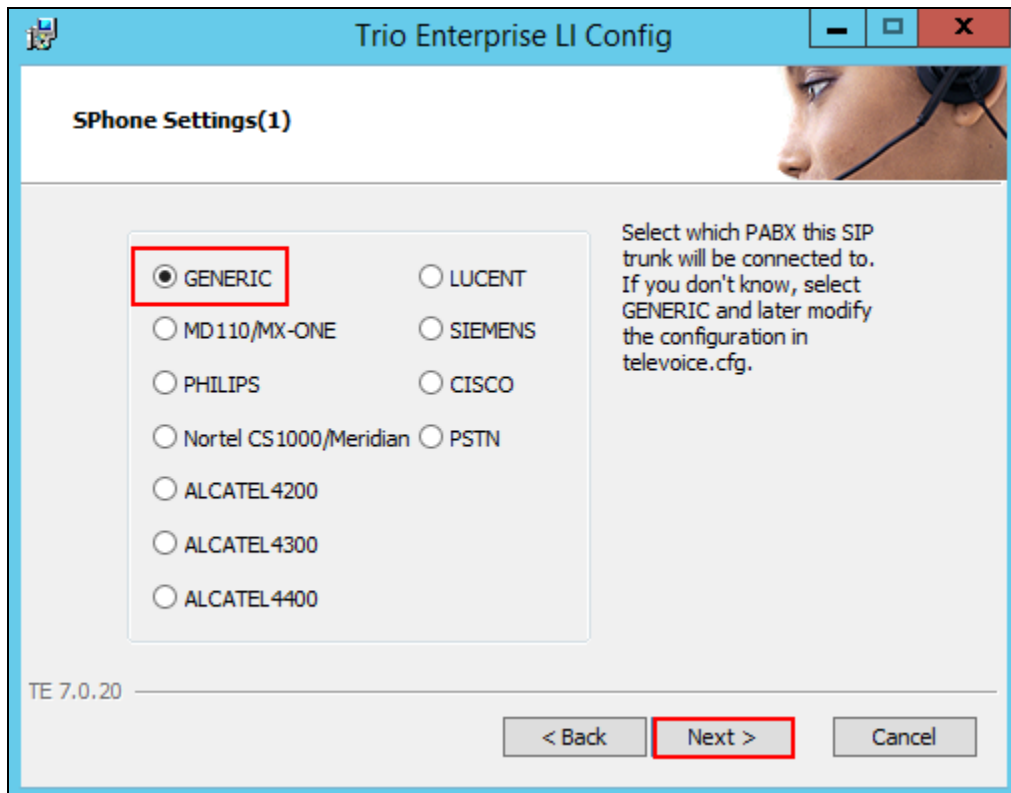
No Line license key results in demo mode where four channels can be used.

No Text-to-Speech licenses results in demo mode where a single channel and a single voice can be used.

TE 7.0.20

< Back **Next >** Cancel

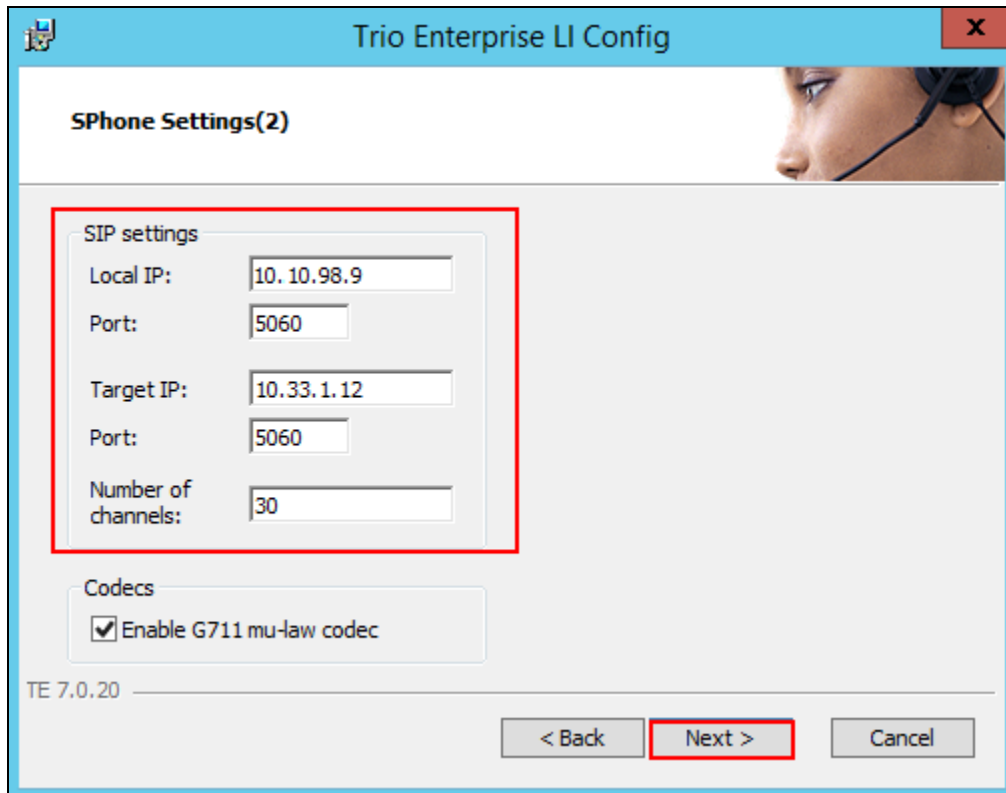
In the subsequent window, select on the **GENERIC** radio button followed by the **Next** button to continue.



In the subsequent window enter the following settings:

- **Local IP** Enter the local IP address of the Trio Enterprise server
- **Port** Enter the SIP Port 5060
- **Target IP** Enter the IP address of the Communication Manager (process IP address)
- **Port** Enter the SIP Port 5060
- **Number of channels** Enter **30** as the number of channels

Click on the **Next** button to continue.



The screenshot shows the 'Trio Enterprise LI Config' window. The title bar is blue with a close button (X) on the right. Below the title bar is a header area with the text 'SPhone Settings(2)' and a small image of a person wearing a headset. The main content area is light gray and contains a 'SIP settings' section highlighted with a red border. This section includes five input fields: 'Local IP' with the value '10.10.98.9', 'Port' with the value '5060', 'Target IP' with the value '10.33.1.12', 'Port' with the value '5060', and 'Number of channels' with the value '30'. Below the 'SIP settings' section is a 'Codecs' section with a checkbox labeled 'Enable G711 mu-law codec' which is checked. At the bottom left of the window, the text 'TE 7.0.20' is displayed. At the bottom right, there are three buttons: '< Back', 'Next >' (highlighted with a red border), and 'Cancel'.

In the subsequent window enter the following settings:

- **Use LI Address Space** Click on the radio button
- **Enable IP routing** Check the box
- **UPDATE support** Check the box

Click on the **Next** button to continue.

Trio Enterprise LI Config

SPhone Settings(3)

Address Space (AS)

☒ Use LI Address Space

☐ AS Name:

☐ No Address Space

Sip Options

☒ UPDATE support

Routing

☒ Enable IP routing

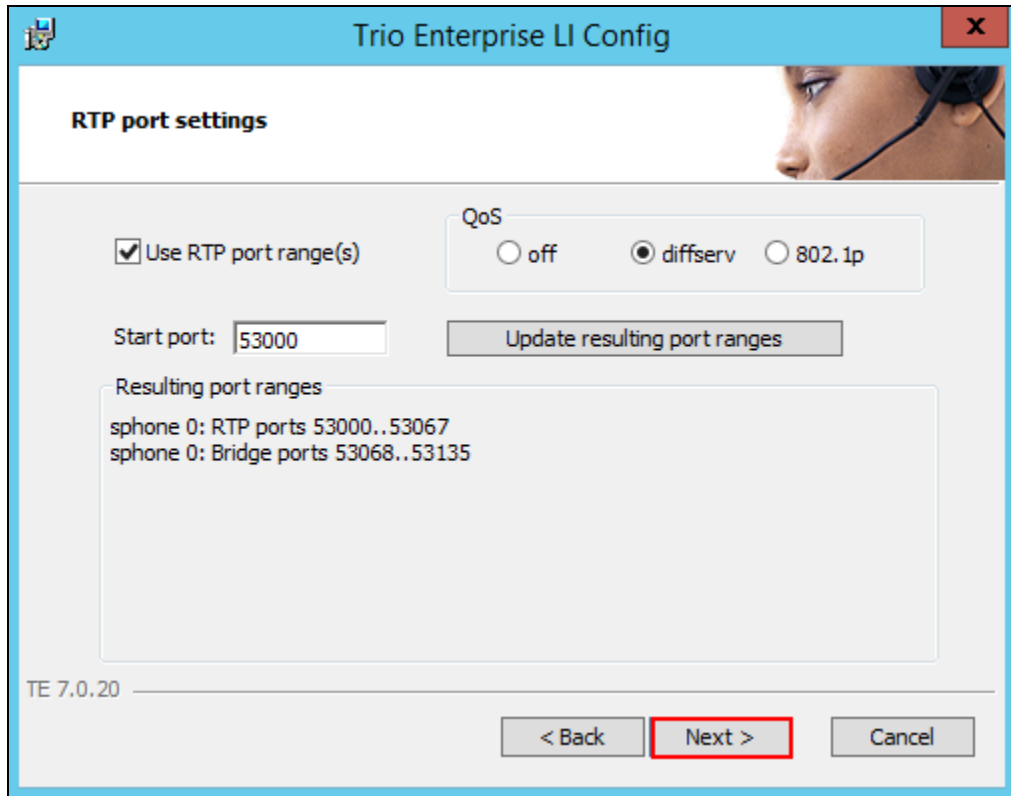
TE 7.0.20

Additional SIP Trunk < Back **Next >** Cancel

In the subsequent window enter the following settings:

- **Use RPT port range(s)** Check the box
- **diffserv** Click on the radio button
- **Start port** Enter **53000**

Click on the **Next** button to continue.



The screenshot shows the 'Trio Enterprise LI Config' window with the 'RTP port settings' tab selected. The 'Use RTP port range(s)' checkbox is checked. The 'QoS' section has three radio buttons: 'off', 'diffserv' (which is selected), and '802.1p'. The 'Start port' field is set to '53000'. An 'Update resulting port ranges' button is located to the right of the 'Start port' field. Below this, a text box displays the 'Resulting port ranges' for 'sphone 0': RTP ports 53000..53067 and Bridge ports 53068..53135. At the bottom of the window, there are three buttons: '< Back', 'Next >' (which is highlighted with a red border), and 'Cancel'. The version 'TE 7.0.20' is displayed in the bottom left corner.

Trio Enterprise LI Config

RTP port settings

☒ Use RTP port range(s)

QoS
☐ off ☒ diffserv ☐ 802.1p

Start port:

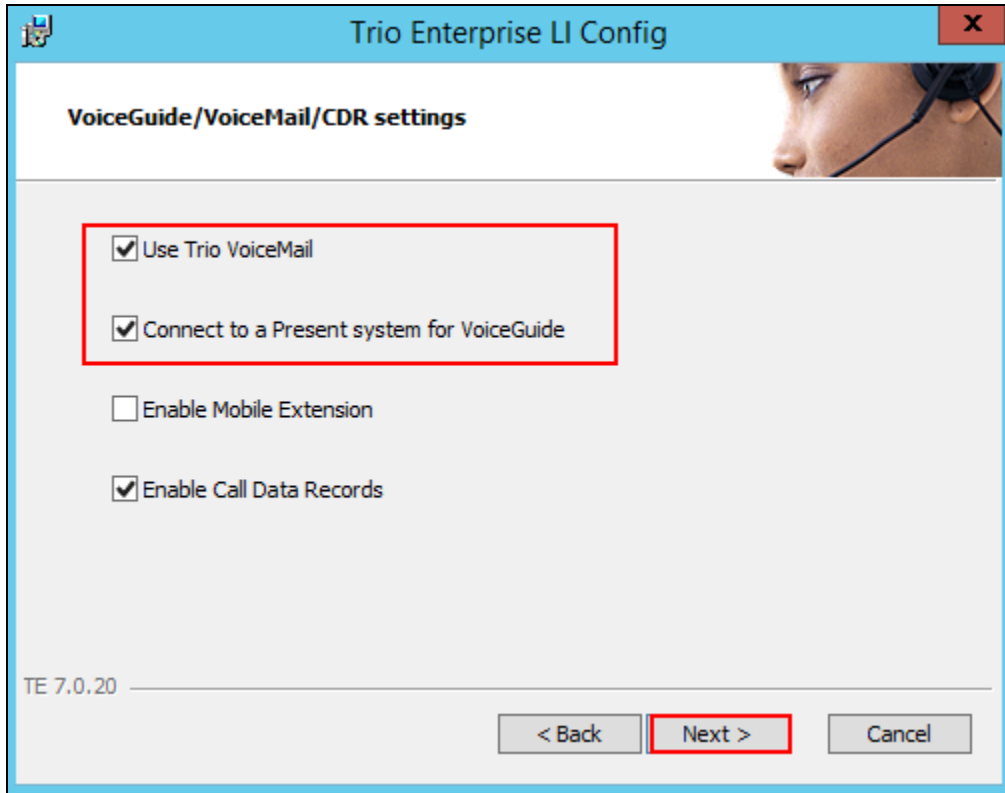
Resulting port ranges
sphone 0: RTP ports 53000..53067
sphone 0: Bridge ports 53068..53135

TE 7.0.20

In the subsequent window enter the following settings:

- **Use Trio VoiceMail** Check the box.
- **Connect to a Present system for VoiceGuide** Check the box.

Click on the **Next** button to continue.

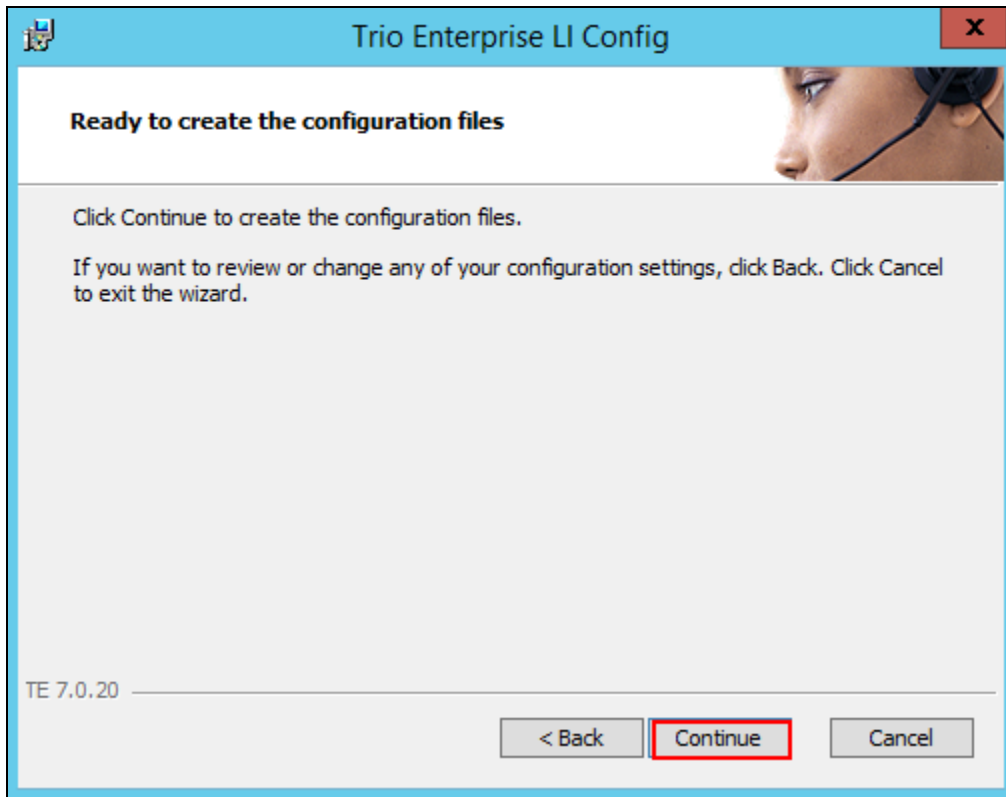


The screenshot shows a window titled "Trio Enterprise LI Config" with a close button (X) in the top right corner. The window contains a section titled "VoiceGuide/VoiceMail/CDR settings" with a background image of a person wearing a headset. Below the title, there are four checkboxes:

- ☒ Use Trio VoiceMail
- ☒ Connect to a Present system for VoiceGuide
- ☐ Enable Mobile Extension
- ☒ Enable Call Data Records

At the bottom left, the text "TE 7.0.20" is displayed. At the bottom right, there are three buttons: "< Back", "Next >", and "Cancel". The "Next >" button is highlighted with a red border.

In the subsequent window shown below, click on **Continue** button.



On the **Wizard Completed** page check the **Start TeleVoice service when finished** check box, followed by the **Finish** button.



8.3. Special Configuration for Avaya Aura® Session Manager

Access the template for televoice.cfg. This is typically found in \TE\ProgramData\LI\templates folder.

Find the [sip_x] section and add the row 'usetcp=1' as shown below,

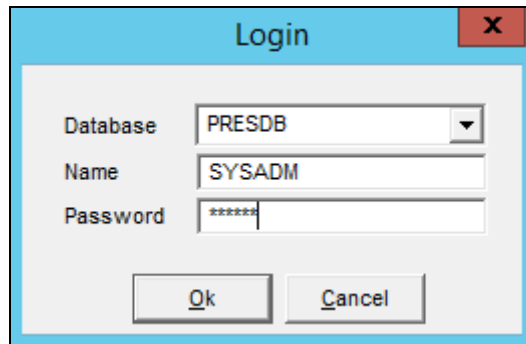
```
[sip_1]
signallingprotocol=sip
localhost=10.10.98.9
targetHost=10.33.1.12
uriScheme=1
transferPoint=afterAnswer
update=1
usetcp=1
```

Find the [device_0] section and set the autype records as shown in the example below, this will prioritize G.711A-Law

```
[device_0]
type=sphone
access=127.0.0.1:33109
voiceserver_1=localhost:33813
sphone=0
localip=10.10.98.9
mf=SipGw_QSIG=0x3ff
rtpsendlog=f=127.0.0.1:33109
autype_1=sdp=pcma
autype_2=sdp=telephone-event,payload=101
autype_3=sdp=pcmu
rtpportrange=53000..53067,dscp
rtpbridgeportrange=53068..53135,dscp
```

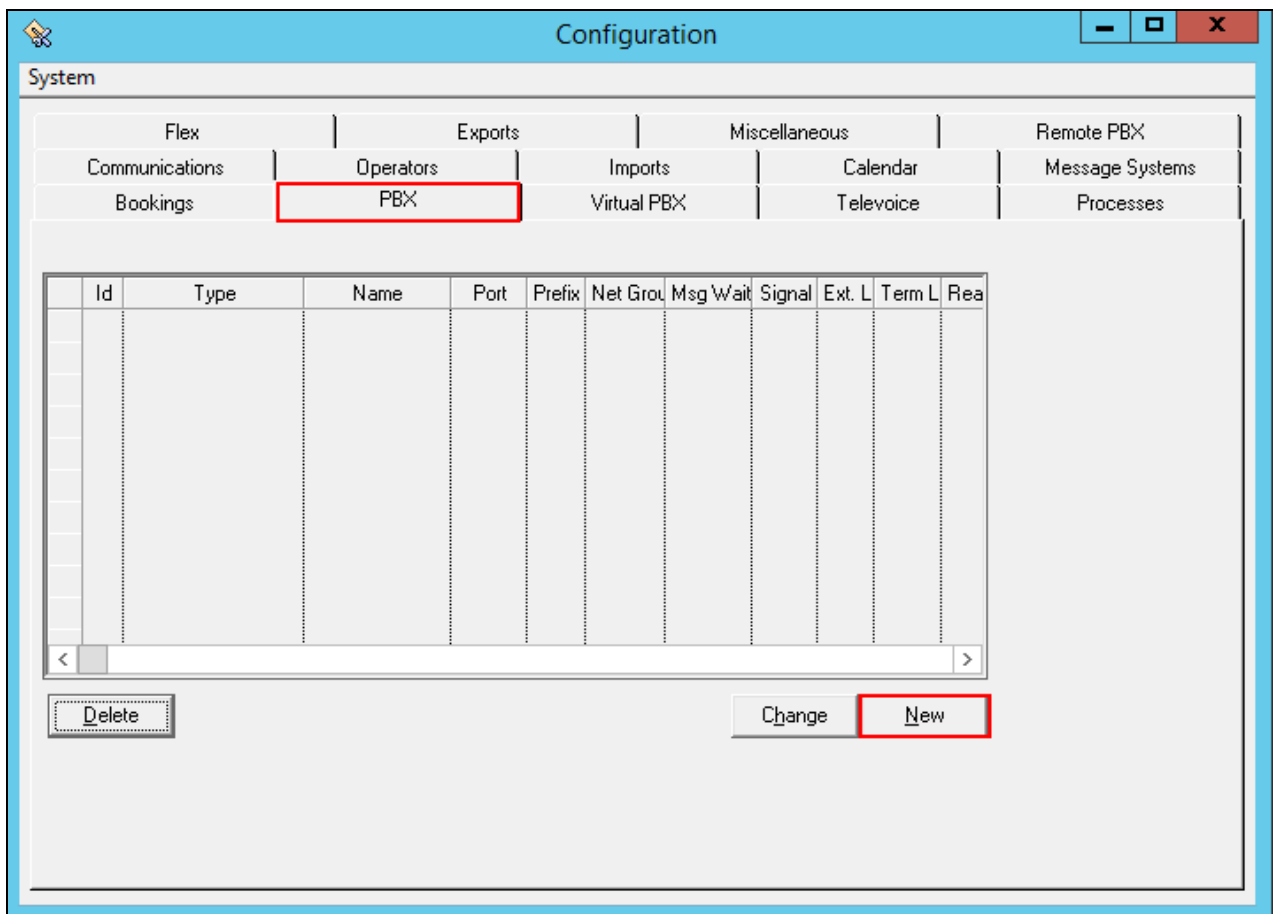
8.4. Configure Absence connection

To configure the Absence connect; navigate to **Start → Programs → Trio Enterprise → Trio Present Setup** (not shown). Use the correct credentials to login as shown below.



A login dialog box titled "Login" with a close button (X) in the top right corner. It contains three input fields: "Database" with a dropdown menu showing "PRESDB", "Name" with the text "SYSADM", and "Password" with masked characters "*****". At the bottom are "Ok" and "Cancel" buttons.

From the screen shown below, select **PBX** and then click on **New**.



A configuration window titled "Configuration" with a close button (X) in the top right corner. It features a tabbed interface with the following tabs: Flex, Exports, Miscellaneous, Remote PBX, Communications, Operators, Imports, Calendar, Message Systems, Bookings, PBX, Virtual PBX, Televoice, and Processes. The "PBX" tab is selected and highlighted with a red border. Below the tabs is a table with the following columns: Id, Type, Name, Port, Prefix, Net Grou, Msg Wait, Signal, Ext. L, Term L, and Rea. The table is currently empty. At the bottom of the window are three buttons: "Delete", "Change", and "New". The "New" button is highlighted with a red border.

Id	Type	Name	Port	Prefix	Net Grou	Msg Wait	Signal	Ext. L	Term L	Rea
----	------	------	------	--------	----------	----------	--------	--------	--------	-----

Configure the **PBX** window as shown below.

- **Type** Click on the **Avaya CM** radio button.
- **PbxName** Enter an informative name.
- **CSTA server** Enter the appropriate Tlink name as seen in **Section 6.77**.
- **PBX login name** Enter the CTI Username as configured in **Section 6.5**.
- **PBX password** Enter the CTI password as configured in **Section 6.5**.
- **Reason code length** Enter **1**
- **Routing device** Enter the extension assigned to the diversion VDN used for activating referrals from the phone set as configured in **Section 5.14.1** and **5.14.3**.
- **Referral destination** Enter the number 4703 that the extensions should be forwarded to when a referral is activated. This number is configured on the Trio Enterprise server for absence treatment.

Click on the **OK** button.

The screenshot shows the PBX configuration window. The 'Type' section has the 'Avaya CM' radio button selected. The 'Virtual' section has the 'MCX' radio button selected. The 'CSTA server' field contains 'AVAYA#INTEROPCM#CSTA#AES70'. The 'PBX login name' field contains 'trio'. The 'PBX password' field contains 'trio'. The 'Reason code length' field contains '1'. The 'Routing device' field contains '3347'. The 'Referral destination' field contains '4703'.

8.5. Configure Trio Enterprise Attendant

Trio Enterprise Attendant is a separate application to Trio Enterprise server and can run concurrently on the same platform. The attendant uses a regular Communication Manager telephone to make and receive calls, which are directed to the telephone by Trio Enterprise server. The steps to configure Trio Attendant are to click on **Start → Programs → Trio Enterprise → Agent Client** (not shown).

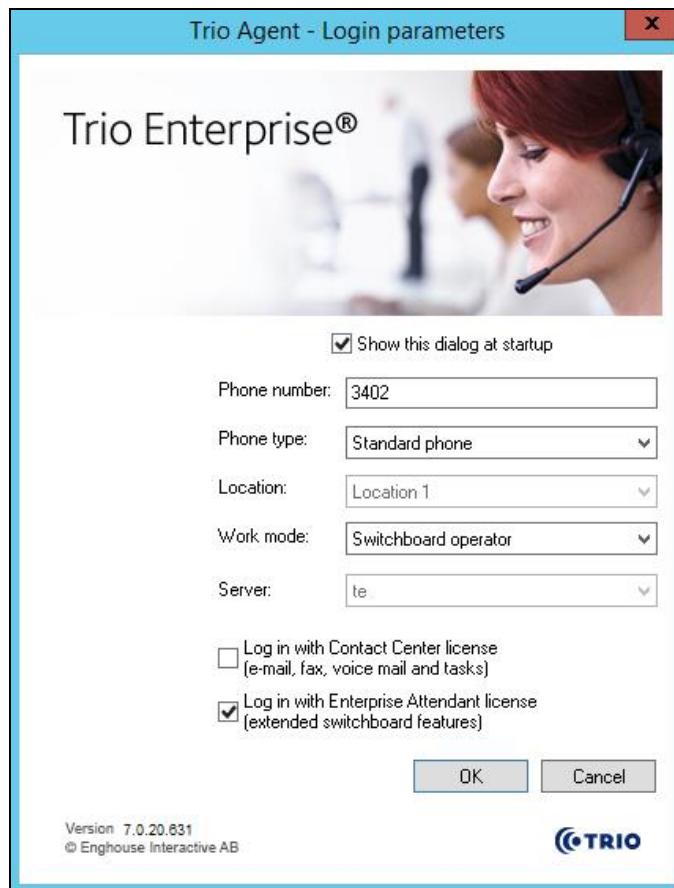
When the Trio Agent window opens enter the following:

- **User ID** Enter a valid user ID
- **Password** Enter a valid Password

Note this user ID and password is created during the installation of Trio Enterprise Server.

- **Extension** Select the Communication Manager telephone number that will be used as the agent's audio device (number 3402 in this example).
- **Phone type** Select **Standard phone** from the dropdown menu
- **Server** Select the correct Trio Enterprise server (default is the current Trio server).

Click on the **OK** button to continue with log in.



Trio Agent - Login parameters

Trio Enterprise®

☒ Show this dialog at startup

Phone number: 3402

Phone type: Standard phone

Location: Location 1

Work mode: Switchboard operator

Server: te

☐ Log in with Contact Center license
(e-mail, fax, voice mail and tasks)

☒ Log in with Enterprise Attendant license
(extended switchboard features)

OK Cancel

Version 7.0.20.631
© Enghouse Interactive AB

TRIO

9. Verification Steps

This section provides the tests that can be performed to verify correct configuration of the Avaya and Trio Enterprise solution.

9.1. Verify Avaya Aura® Communication Manager CTI Service State

The following steps can ensure that the communication between Communication Manager and the Application Enablement Services server is functioning correctly. Using SAT, connect to Communication Manager and check the AESVCS link status with Application Enablement Services by using the command “status aesvcs cti-link”. The CTI Link is 1. Verify that the **Service State** of the CTI link is **established**.

```
status aesvcs cti-link
```

AE SERVICES CTI LINK STATUS						
CTI Link	Version	Mnt Busy	AE Services Server	Service State	Msgs Sent	Msgs Rcvd
1	7	no	aes70	established	15	15

9.2. Verify Session Manager

Log in to System Manager. Under the **Elements** section, navigate to **Session Manager** → **System Status** → **SIP Entity Monitoring**. Click the Session Manager instance (*Session Manager* in the example below).

The screenshot shows the Avaya Aura System Manager 7.0 interface. The left sidebar contains a navigation menu with options like Session Manager, Dashboard, Session Manager Administration, Communication Profile Editor, Network Configuration, Device and Location Configuration, Application Configuration, System Status, SIP Entity Monitoring, Managed Bandwidth Usage, and Security Module Status. The main content area is titled "SIP Entity Link Monitoring Status Summary" and includes a "Run Monitor" button. Below this, a table displays the status of monitored entities for three Session Manager instances: ASM70A, ASM70B, and Branch-ASM70. The table has columns for Session Manager, Type, and Monitored Entities (Down, Partially Up, Up, Not Monitored, Deny, Total). The ASM70A instance shows 15 Down, 0 Partially Up, 10 Up, 1 Not Monitored, 1 Deny, and a Total of 27. The ASM70B instance shows 0 Down, 0 Partially Up, 4 Up, 0 Not Monitored, 1 Deny, and a Total of 5. The Branch-ASM70 instance shows all zeros for the monitored entities and a Total of 0.

Session Manager	Type	Monitored Entities					
		Down	Partially Up	Up	Not Monitored	Deny	Total
<input type="checkbox"/> ASM70A	Core	15	0	10	1	1	27
<input type="checkbox"/> ASM70B	Core	0	0	4	0	1	5
<input type="checkbox"/> Branch-ASM70	BSM	---	---	---	---	---	---

Verify that the state of the Session Manager links to Communication Manager and Trio under the **Conn. Status** and **Link Status** columns is **UP**, like shown on the screen below.

Session Manager Entity Link Connection Status

This page displays detailed connection status for all entity links from a Session Manager.

All Entity Links for Session Manager: ASM70A

Status Details for the selected Session Manager:

Summary View

27 Items Refresh Filter: Enable

	SIP Entity Name	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
<input type="radio"/>	ACM-Trunk3-Public	10.33.1.6	5067	TLS	FALSE	UP	200 OK	UP
<input type="radio"/>	Trio	10.10.98.9	5060	TCP	FALSE	UP	200 OK	UP
<input type="radio"/>	Breeze	10.33.1.16	5061	TLS	FALSE	UP	200 OK	UP
<input type="radio"/>	Interop-AAM63	10.33.1.5	5060	TCP	FALSE	UP	200 OK	UP
<input type="radio"/>	Presence70	10.33.1.16	5061	TLS	FALSE	UP	200 OK	UP
<input type="radio"/>	ACM-Trunk1-Private	10.33.1.6	5061	TLS	FALSE	UP	200 OK	UP
<input type="radio"/>	Avaya-SBCE-A1	10.33.1.51	5061	TLS	FALSE	UP	200 OK	UP
<input type="radio"/>	Car2-cores	10.10.97.170	5061	TLS	FALSE	UP	200 OK	UP

Other Session Manager useful verification and troubleshooting tools include:

- **traceSM** – Session Manager command line tool for traffic analysis. Login to the Session Manager command line management interface to run this command.
- **Call Routing Test** - The Call Routing Test verifies the routing for a particular source and destination. To run the routing test, from the System Manager Home screen navigate to **Elements** → **Session Manager** → **System Tools** → **Call Routing Test**. Enter the requested data to run the test.

10. Conclusion

A full and comprehensive set of feature and functional test cases were performed during Compliance testing. Trio Enterprise from Enghouse Interactive AB is considered compliant with Avaya Aura® Communication Manager, Avaya Aura® Session Manager and Avaya Aura® Application Enablement Services. All test cases have passed and met the all objectives with any observation/s note in **Section 2.2**.

11. Additional References

These documents form part of the Avaya official technical reference documentation suite. Further information may be had from <http://support.avaya.com> or from the local Avaya representative.

1. *Implementing Avaya Aura® Session Manager* Document ID 03-603473.
2. *Administering Avaya Aura® Session Manager*, Doc ID 03-603324.
3. *Deploying Avaya Aura® System Manager*, Release 7.0.
4. *Administering Avaya Aura® System Manager for Release 7.0*, Release 7.0.
5. *Quick Start Guide to Using the Avaya Aura® Media Server with Avaya Aura® Communication Manager*.
6. *Deploying and Updating Avaya Aura® Media Server Appliance*, Release 7.7.
7. *Administering Avaya Aura® Communication Manager*, Release 7.0, 03-300509.
8. *Avaya Aura® Communication Manager Feature Description and Implementation*, Release 7.0, 555-245-205.
9. *Deploying Avaya Aura® Application Enablement Services in Virtualized Environment*, Release 7.0
10. *Administering and Maintaining Avaya Aura® Application Enablement Services*, Release 7.0

Product Documentation for Enghouse Interactive AB can be obtained in the installed software or at: <http://enghouseinteractive.com>

©2017 Avaya Inc. All Rights Reserved.

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

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