



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 (Communication Manager), Avaya Aura® Session Manager (Session Manager) and Avaya Aura® Application Enablement Services (Application Enablement Services). 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 Application Enablement Services 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 digital 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.

For the testing associated with these Application Notes, the interface between Avaya systems and Trio Enterprise did not include use of any specific encryption features as requested by Enghouse Interactive AB.

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/Application Enablement Services. The testing included:

- Incoming internal and external calls
- Outgoing internal and external calls
- Supervised and unsupervised transfer with answer
- Directing calls from busy extensions and extensions that do not answer
- Call queuing and retrieval
- Loop detection for busy and unanswered extensions
- Absence detection
- Message Waiting Indicator

2.2. Test Results

Tests were performed to ensure 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,

- The Codec Set List in Communication Manager cannot have both G.711MU and G.711A together. In case they are present together, then the Codec priority must be configured on the Trio Enterprise Server. Failing to do so, will cause Avaya SIP and digital stations to not hear early media (any pre-recorded audio) from the attendant. Refer to **Sections 5.8** and **8.3**.

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 Application Enablement Services. An Avaya digital 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.

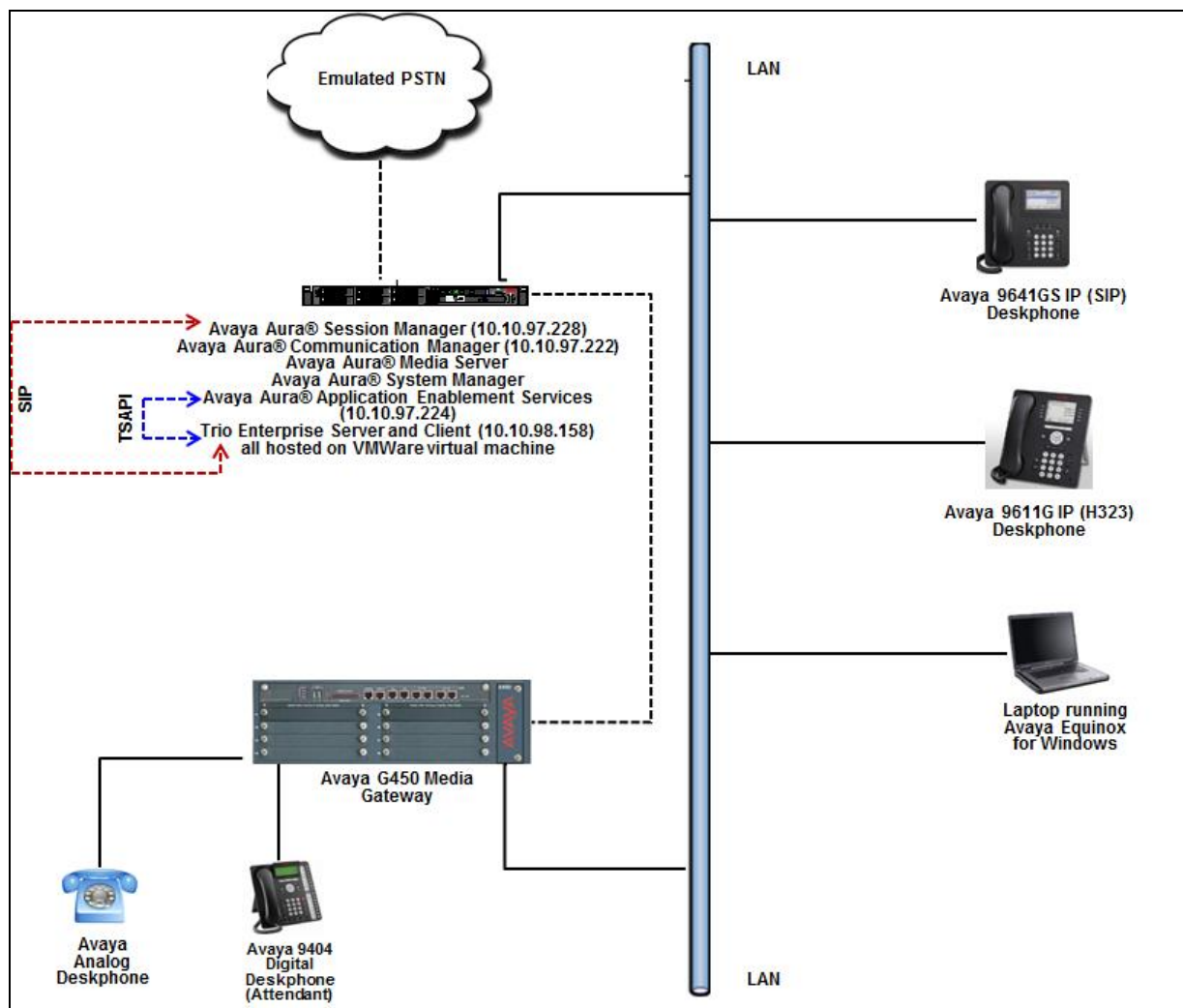


Figure 1: Avaya and Trio Enterprise Reference Configuration

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	08.0.0.0.822
Avaya Aura® Application Enablement Services running on virtualized environment	8.0.0.0.6-0
Avaya Aura® Session Manager running on virtualized environment	8.0.0.0.800035
Avaya Aura® System Manager	8.0.0.0.931077
Avaya Aura® Media Server	8.0.0.117
Avaya G450 Media Gateway	40.10.0/1
Avaya IP Deskphones - 9641GS (SIP) - 9611G (H.323)	7.1.3.0.8 6.6604
Avaya Equinox for Windows	3.4.0.152.46-ACW- INTEGRATIONNEXUS1
Avaya 9404 Digital Telephone	R18
Avaya Analog Telephone	N/A
Trio Enterprise Server and Client running on Microsoft Windows 2012 R2 Server	7.1
TSAPI Client for Windows	8.0.0-38

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 IP Node Names
- Administer SIP trunk group
- Administer SIP signalling group
- Administer SIP Trunk Group Members
- 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				
Async. Transfer Mode (ATM) Trunking? n		Digital Loss Plan Modification? y		
ATM WAN Spare Processor? n		DS1 MSP? y		
ATMS? y		DS1 Echo Cancellation? y		
Attendant Vectoring? y				

5.2. 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 IP Node Names

Use the “change node-names ip” command (not shown) and add an entry for Session Manager. In this case, **SM-VM** and **10.10.97.228** are entered as **Name** and **IP Address**. Note the **procr** and **10.10.97.222** entry, which is the node **Name** and **IP Address** for the processor board. These values will be used later to configure the SIP trunk to Session Manager in **Section 5.5**. The node **Name** and **IP Address** for Application Enablement Services is **10.10.97.224**, which will be used later in the Application Enablement Services configuration as shown in **Section 5.14**.

```
change node-names ip
                                IP NODE NAMES
    Name                IP Address
    SM-VM                10.10.97.228
    procr                10.10.97.222
    devvmaes            10.10.97.224
```

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”.

add trunk-group 1		Page 1 of 22	
TRUNK GROUP			
Group Number: 1	Group Type: sip	CDR Reports: y	
Group Name: Trunk to SM on VM	COR: 1	TN: 1	TAC: #001
Direction: two-way	Outgoing Display? y	Night Service:	
Dial Access? n			
Queue Length: 0			
Service Type: tie	Auth Code? n		
Member Assignment Method: auto			
Signaling Group: 1			
Number of Members: 24			

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

add trunk-group 1		Page 3 of 22	
TRUNK FEATURES			
ACA Assignment? n	Measured: none	Maintenance Tests? y	
Numbering Format: private			
UI Treatment: shared			
Maximum Size of UI Contents: 128			
Replace Restricted Numbers? n			
Replace Unavailable Numbers? n			
Hold/Unhold Notifications? y			
Modify Tandem Calling Number: no			

5.5. Administer SIP Signalling Group

Use the “add signaling-group n” command, where “n” is an available signalling 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” from **Section 5.3**.
- **Far-end Node Name:** The existing node name for Session Manager from **Section 5.3**.
- **Near-end Listen Port:** An available port for integration with Session Manager.
- **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 Session Manager.
- **Far-end Domain:** The applicable domain name for the network.
- **Direct IP-IP Audio Connections?:** “y”.
- **Initial IP-IP Direct Media?:** “y”. This can be set to “n” or “y”.

```
display signaling-group 1                                     Page 1 of 2

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? y
Peer Detection Enabled? y 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: SM-VM
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? y
Enable Layer 3 Test? y              Initial IP-IP Direct Media? y
H.323 Station Outgoing Direct Media? n Alternate Route Timer(sec): 6
```

5.6. Administer SIP Trunk Group Members

Use the “change trunk-group n” command, where “n” is the trunk group number from **Section 5.4**. Enter the following values for the specified fields and retain the default values for the remaining fields.

- **Signalling Group:** The signalling group number from **Section 5.5**.
- **Number of Members:** The desired number of members, in this case “24”.

```
change trunk-group 1                                     Page 1 of 22
                                                         TRUNK GROUP

Group Number: 1                      Group Type: sip          CDR Reports: y
Group Name: Trunk to SM on VM        COR: 1                TN: 1          TAC: #001
Direction: two-way                  Outgoing Display? y
Dial Access? n                      Night Service:
Queue Length: 0
Service Type: tie                    Auth Code? n
                                     Member Assignment Method: auto
                                     Signaling Group: 1
                                     Number of Members: 24
```

5.7. 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 signalling group from **Section 5.5**.

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: Authoritative Domain: bvwdev.com
Name: Region1
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										all	
2												

5.8. Administer IP Codec Set

Use the “change ip-codec-set n” command, where “n” is the codec set number from **Section 5.7**. Update the audio codec types in the **Audio Codec** fields as necessary. As per the observation noted in **Section 2.2** only configure either G.711MU or G.711A. The codec shown below was used in the compliance testing since Trio Enterprise had made the codec priority changes to accommodate both G.711MU and G.711A.

display ip-codec-set 1

Page1 of 2

IP CODEC SET

Codec Set: 1

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

Media Encryption

Encrypted SRTCP: enforce-unenc-srtcp

1: 1-srtp-aescm128-hmac80

2: 2-srtp-aescm128-hmac32

3: none

5.9. 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: To SM on VM									
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					0	n	user
2:								n	user
3:								n	user
4:								n	user
5:								n	user
6:								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 none

5.10. 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 5-digit extension beginning with “56” and routed to trunk group “1” will result in a 5-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	Ext	Trk	Private	Total
Len	Code	Grp(s)	Prefix	Len
5	56	1		5
				Total Administered: 4
				Maximum Entries: 540

5.11. Administer Dial Plan

This section provides a sample dial plan used for routing calls with dialed digits 71xxx to Trio Enterprise. Use the “change dialplan analysis 0” command and add an entry to specify the use of digits pattern “71”, as shown below.

display dialplan analysis								
DIAL PLAN ANALYSIS TABLE								
Location: all								
Percent Full: 2								
Dialed	Total	Call	Dialed	Total	Call	Dialed	Total	Call
String	Length	Type	String	Length	Type	String	Length	Type
1	4	ext						
71	5	udp						

5.12. Administer Uniform Dial Plan

This section provides a sample AAR routing used for routing calls with dialled digits 71xxx 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 71xxx, as shown below.

change uniform-dialplan 0								
UNIFORM DIAL PLAN TABLE								
Percent Full: 0								
Matching			Insert			Node		
Pattern	Len	Del	Digits	Net	Conv	Num		
71	5	0		aar	n			

5.13. Administer AAR Analysis

Use the “change aar analysis 0” command and add an entry to specify how to route calls to 71xxx. In the example shown below, calls with digits 71xxx will be routed as an AAR call using route pattern “1” from **Section 5.9**.

change aar analysis 0								
AAR DIGIT ANALYSIS TABLE								
Location: all								
Percent Full: 2								
Dialed	Total	Route	Call	Node	ANI			
String	Min	Max	Pattern	Type	Num	Reqd		
71	5	5	1	aar		n		

5.14. Configure Interface to Avaya Aura® Application Enablement Services

To configure the Application Enablement Services link, use the “change ip-services” command and enter the following in **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 Type	Enabled	Local Node	Local Port	Remote Node	Remote Port		
AESVCS	y	procr	8765				

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

- **Server ID:** Enter “1”
- **AE Services:** Enter “devvmaes” (The node created in **Section 5.3**. Also note that the name entered in this field should be matched with the host name of Application Enablement Services server)
- **Password:** Enter a password. This password will be used in **Section 6.3** to enable the Application Enablement Services to communicate with the Communication Manager.
- **Enabled:** Enter “y”

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

5.15. 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 Application Enablement Services. Use the “add cti-link next” command (Note, during compliance testing cti link 1 was added) and enter the following:

- **Extension:** Enter any unused Extension (i.e. 56000).
- **Type:** Enter “ADJ-IP”.
- **Name:** Enter a descriptive name (i.e. DevvmAES)

```
add cti-link 1                                     Page 1 of 3
CTI Link: 1                                         CTI LINK
Extension: 56000
Type: ADJ-IP
Name: DevvmAES                                     COR: 1
```

5.16. 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 dialed 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

5.16.1. 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”.

add vdn 56007	Page 1 of 3
VECTOR DIRECTORY NUMBER	
Extension: 56007	
Name*: Phone 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*:	

5.16.2. Configure Vector 7

Configure the Vector that was used as the **Vector Number** in **Section 5.16.1**. 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 56008 with cov n if unconditionally”.

In this example, using monitored phone dial 56007 + reason code + #, call is routed to 56008 which will trigger Trio Enterprise to set the phone absence with appropriate reason announcement.

```
add vector 7                                     Page 1 of 6
                                         CALL VECTOR
Number: 7                                     Name: Phone 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      1      secs hearing silence
02 collect      9      digits after announcement none      for none
03 route-to      number 56008      with cov n if unconditionally
04
```

5.16.3. Configure VDN 2

Configure a VDN using the “route-to number” as used in **Section 5.16.2**. This VDN is used for activating referrals from the phone set. Use the “add vdn 56008” command, and configure the following:

- **Name*:** Enter an informative name (i.e. diversion).
- **Destination:** Enter “Vector Number 8”.

```
display vdn 56008                               Page 1 of 3
                                         VECTOR DIRECTORY NUMBER
Extension: 56008
Name*: Diversion
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*:
```

5.16.4. Configure Vector 8

Configure the Vector that was used as the “Vector Number” in **Section 5.16.3**. 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”.

```
display 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 ringback
02 stop
03
```

6. Configuration of Avaya Aura® Application Enablement Services

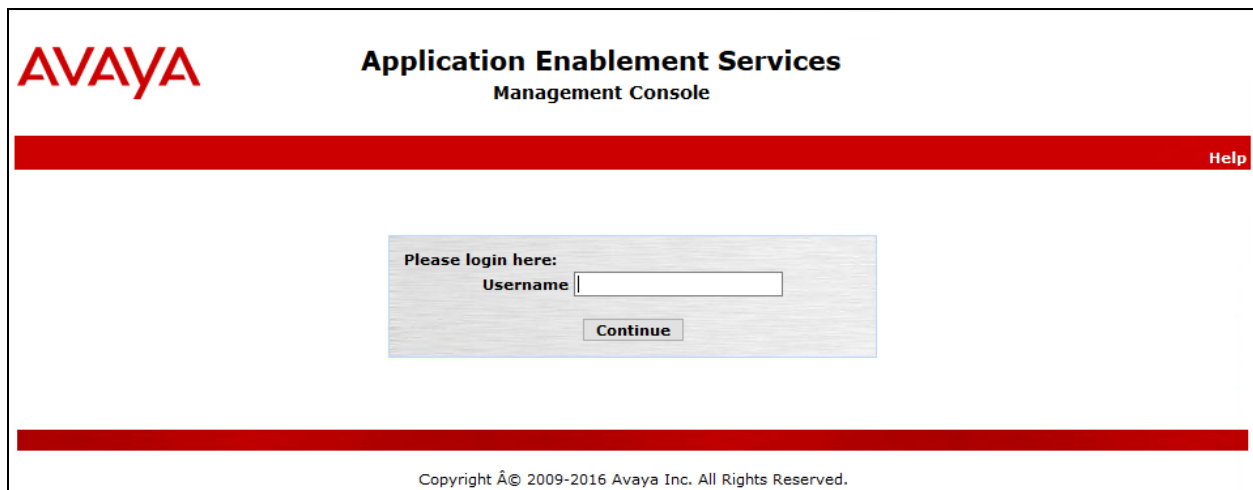
This section provides the procedures for configuring Application Enablement Services. It is implied a working Application Enablement Services is already in place and the Security Database (SDB) is configured. For all other provisioning information such as initial installation and configuration, please 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 an 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 Aura® 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. Below this bar is a login box with the text "Please login here:" and a "Username" label next to a text input field. A "Continue" button is located below the input field. 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 includes 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: Wed Nov 14 10:20:40 2018 from [redacted]", "Number of prior failed login attempts: 0", "HostName/IP: devvmaes/[redacted]", "Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE", "SW Version: 8.0.0.0.0.6-0", "Server Date and Time: Wed Nov 14 11:36:09 EST 2018", 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 explaining the OAM Web's purpose. It lists administrative domains and their functions: AE Services, Communication Manager Interface, High Availability, Licensing, Maintenance, Networking, Security, Status, User Management, Utilities, and Help. A note at the bottom states: "Depending on your business requirements, these administrative domains can be served by one administrator for all domains, or a separate administrator for each domain." The footer displays "Copyright © 2009-2016 Avaya Inc. All Rights Reserved."

Welcome: User cust
Last login: Wed Nov 14 10:20:40 2018 from [redacted]
Number of prior failed login attempts: 0
HostName/IP: devvmaes/[redacted]
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.0.0.0.0.6-0
Server Date and Time: Wed Nov 14 11:36:09 EST 2018
HA Status: Not Configured

Home | Help | Logout

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

Welcome to OAM

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

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

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

Copyright © 2009-2016 Avaya Inc. All Rights Reserved.

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 Avaya Application Enablement Services Management Console with the "Licensing" menu item selected in the left sidebar. The top header includes 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: Wed Nov 14 10:20:40 2018 from [redacted]", "Number of prior failed login attempts: 0", "HostName/IP: devvmaes/[redacted]", "Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE", "SW Version: 8.0.0.0.0.6-0", "Server Date and Time: Wed Nov 14 11:36:09 EST 2018", 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 "Licensing" and contains a paragraph explaining the WebLM. It lists the following information: "WebLM Server Address", "WebLM Server Access", and "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 footer displays "Copyright © 2009-2016 Avaya Inc. All Rights Reserved."

Welcome: User cust
Last login: Wed Nov 14 10:20:40 2018 from [redacted]
Number of prior failed login attempts: 0
HostName/IP: devvmaes/[redacted]
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.0.0.0.0.6-0
Server Date and Time: Wed Nov 14 11:36:09 EST 2018
HA Status: Not Configured

Home | Help | Logout

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

Licensing

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

- WebLM Server Address

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

- WebLM Server Access

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

- Reserved Licenses

NOTE: Please disable your pop-up blocker if you are having difficulty with opening this page

Copyright © 2009-2016 Avaya Inc. All Rights Reserved.

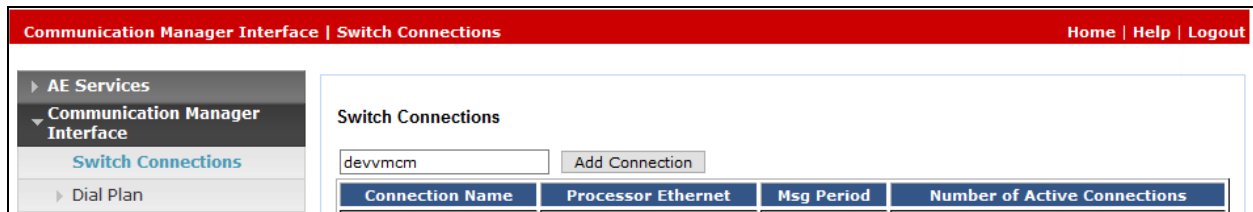
The **Web License Manager** screen below is displayed. Select **Licensed products** → **APPL_ENAB** → **Application_Enablement** in the left pane, to display the **Application Enablement (CTI)** screen in the right pane.

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

WebLM Home	Application Enablement (CTI) - Release: 8 - SID:		
Install license	You are here: Licensed Products > Application_Enablement > View License Capacity		
Licensed products	License installed on: September 13, 2018 2:50:26 PM +00:00		
APPL_ENAB	License File Host IDs:		
▼ Application_Enablement			
View license capacity	Licensed Features		
View peak usage	13 Items Show All		
CCTR	Feature (License Keyword)	Expiration date	Licensed capacity
►ContactCenter	Device Media and Call Control VALUE_AES_DMCC_DMC	permanent	100
Configure Centralized Licensing	AES ADVANCED LARGE SWITCH VALUE_AES_AEC_LARGE_ADVANCED	permanent	100
CE	AES HA LARGE VALUE_AES_HA_LARGE	permanent	100
►COLLABORATION_ENVIRONMENT	AES ADVANCED MEDIUM SWITCH VALUE_AES_AEC_MEDIUM_ADVANCED	permanent	100
COMMUNICATION_MANAGER	Unified CC API Desktop Edition VALUE_AES_AEC_UNIFIED_CC_DESKTOP	permanent	100
►Call_Center	CVLAN ASAI VALUE_AES_CVLAN_ASAI	permanent	100
►Communication_Manager	AES HA MEDIUM VALUE_AES_HA_MEDIUM	permanent	100
Configure Centralized Licensing	AES ADVANCED SMALL SWITCH VALUE_AES_AEC_SMALL_ADVANCED	permanent	100
MSR	DLG VALUE_AES_DLG	permanent	100
►Media_Server	TSAPI Simultaneous Users VALUE_AES_TSAPI_USERS	permanent	100
PRESENCE_SERVICES			
►Presence_Services			
SYSTEM_MANAGER			
►System_Manager			
SessionManager			
►SessionManager			
Uninstall license			

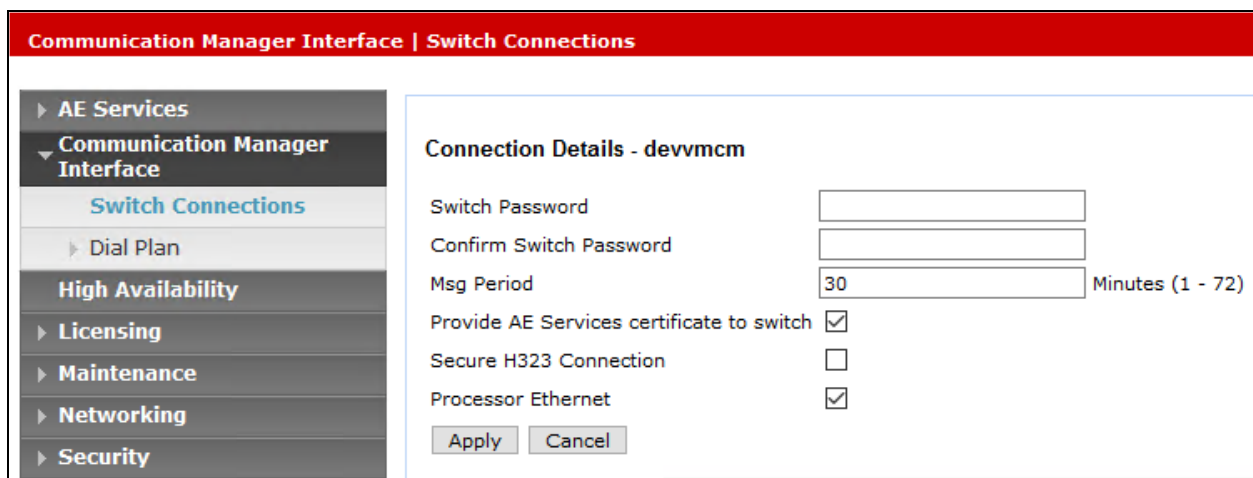
6.3. Create an Avaya Aura® Communication Manager Switch Connection

A Communication Manager Switch Connection needs to be created to enable the Application Enablement Services 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.



Connection Name	Processor Ethernet	Msg Period	Number of Active Connections
-----------------	--------------------	------------	------------------------------

In the **Connection Details** window, enter the **Switch Password** as was configured in **Section 5.14** and **Confirm Switch Password**. Click on the **Apply** button.



Connection Details - devvmcm

Switch Password

Confirm Switch Password

Msg Period Minutes (1 - 72)

Provide AE Services certificate to switch ☒

Secure H323 Connection ☐

Processor Ethernet ☒

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 “devvmcm”, and select the corresponding radio button. Click **Edit PE/CLAN IPs**.

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

The **Edit Processor Ethernet IP** screen is displayed. Enter the IP address of a C-LAN circuit pack or the Processor C-LAN on Communication Manager to be used, in this case “10.10.97.222” as shown below, which is the Processor C-LAN on Communication Manager. Click **Add/Edit Name or IP**.

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

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 a web interface with a red header bar containing "AE Services | TSAPI | TSAPI Links" and "Home | Help | Logout". On the left is a sidebar menu with "AE Services" expanded, showing options like CVLAN, DLG, DMCC, SMS, and "TSAPI" (which is further expanded to show "TSAPI Links" and "TSAPI Properties"). The main content area is titled "TSAPI Links" and contains a table with five columns: "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 drop-down box
- **Switch Connection:** Select "devvmcm" from the drop-down box. (The Switch connection as created in **Section 6.3**)
- **Switch CTI Link Number:** Select "1" from the drop-down box. (The CTI link as created in **Section 5.15**)
- **ASAI Link Version:** Select "8" from the drop-down box.
- **Security:** Select "Both" from the drop-down box

Click on the **Apply Changes** button.

The screenshot shows the "Add TSAPI Links" form. It has the same header and sidebar as the previous screenshot. The form contains five fields, each with a dropdown menu: "Link" (set to "1"), "Switch Connection" (set to "devvmcm"), "Switch CTI Link Number" (set to "1"), "ASAI Link Version" (set to "8"), and "Security" (set to "Both"). At the bottom of the form are two buttons: "Apply Changes" and "Cancel Changes".

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 being required for the Trio Enterprise Installation
- **Confirm Password:** Confirm the password
- **Avaya Role** Select “userservice.useradmin” from the drop-down box
- **CT User:** Select “Yes” from the drop-down box

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

The screenshot shows the 'Add User' form within the 'User Management' section. The left sidebar contains a navigation menu with options like 'AE Services', 'Communication Manager Interface', 'High Availability', 'Licensing', 'Maintenance', 'Networking', 'Security', 'Status', 'User Management', 'Service Admin', and 'User Admin'. The 'User Admin' section is expanded, showing 'Add User' as the selected option. The main form area is titled 'Add User' and includes a note: 'Fields marked with * can not be empty.' The form fields are as follows:

Field	Value
* User Id	Trio
* Common Name	Trio
* Surname	Trio
* User Password
* Confirm Password
Admin Note	
Avaya Role	userservice.useradmin
Business Category	
Car License	
CM Home	
Css Home	
CT User	Yes
Department Number	
Display Name	

6.6. Configure Security Database

Navigate to the All 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

▶ 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 checked="" type="radio"/> Trio	Trio	NONE	NONE

Edit List All

Once the **Edit CTI User** page appears, select the **Unrestricted Access** check box and click on the **Apply Changes** button.

Security | Security Database | CTI Users | List All UsersHome | 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

▪ List All Users

▪ Search Users

Edit CTI User

User Profile:

User ID

Common Name

Worktop Name

Unrestricted Access

Trio

Trio

NONE ▾

☒

Call and Device Control:

Call Origination/Termination and Device Status

None ▾

Call and Device Monitoring:

Device Monitoring

Calls On A Device Monitoring

Call Monitoring

None ▾

None ▾

☐

Routing Control:

Allow Routing on Listed Devices

None ▾

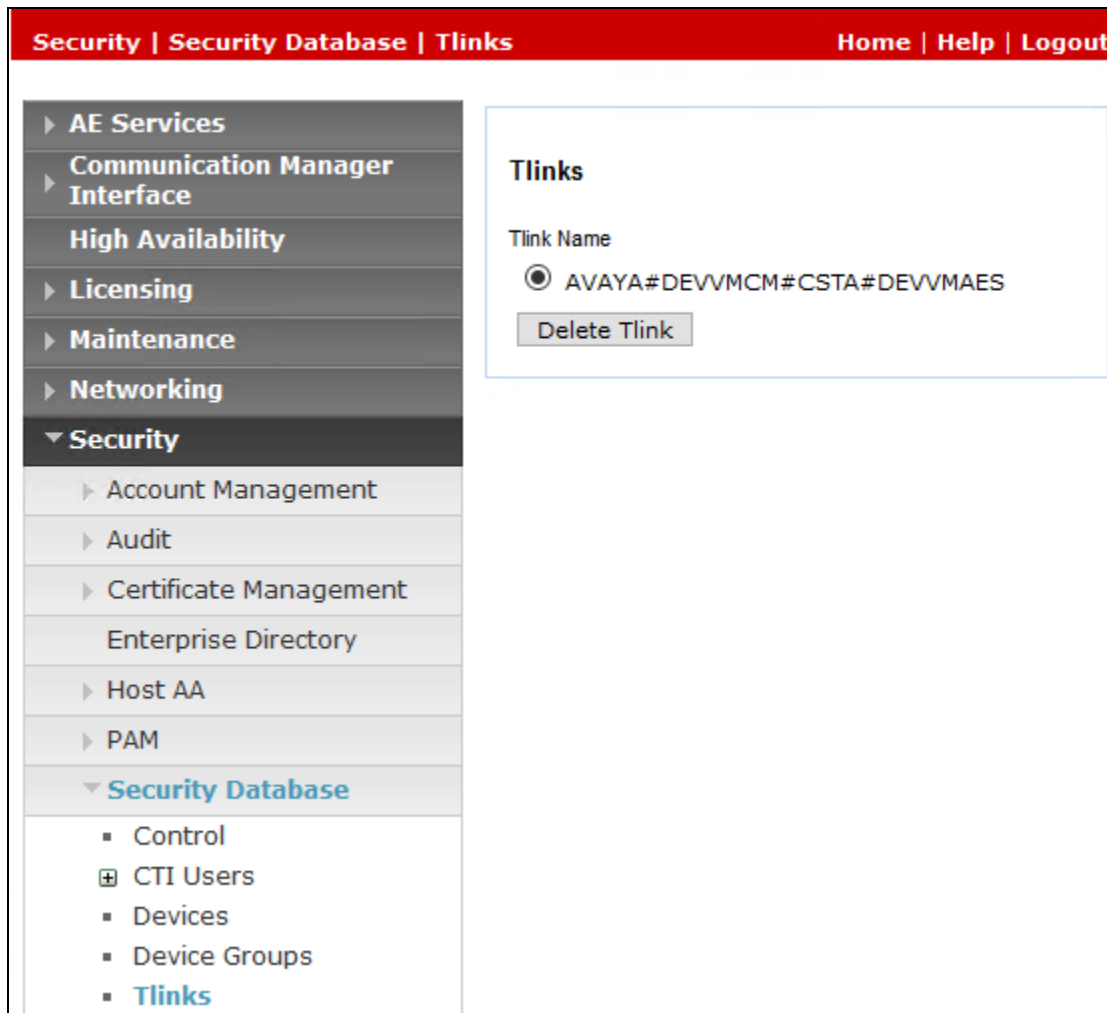
Apply Changes

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#DEVVMCM#CSTA#DEVVMAES”. Note the use of the switch connection “devvmcm” 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.

The screenshot shows a web application interface with a red header bar. The header contains the breadcrumb 'Security | Security Database | Control' on the left and navigation links 'Home | Help | Logout' on the right. A left-hand navigation pane lists various system components: AE Services, Communication Manager Interface, High Availability, Licensing, Maintenance, Networking, Security (expanded), Account Management, Audit, Certificate Management, Enterprise Directory, Host AA, PAM, Security Database (expanded), and Control (selected). The main content area on the right is titled 'SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services'. It contains two unchecked checkboxes: 'Enable SDB for DMCC Service' and 'Enable SDB for TSAPI Service, JTAPI and Telephony Web Services'. Below these checkboxes is a button labeled 'Apply Changes'.

Security Security Database Control		Home Help Logout
▶ AE Services	<div>SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services</div> <div><input type="checkbox"/> Enable SDB for DMCC Service</div> <div><input type="checkbox"/> Enable SDB for TSAPI Service, JTAPI and Telephony Web Services</div> <div>Apply Changes</div>	
▶ Communication Manager Interface		
High Availability		
▶ Licensing		
▶ Maintenance		
▶ Networking		
▼ Security		
▶ Account Management		
▶ Audit		
▶ Certificate Management		
Enterprise Directory		
▶ Host AA		
▶ PAM		
▼ Security Database		
▪ Control		

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

Home | Help | Logout

▶ 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

Encrypted TCP Port9998

DLG PortTCP Port5678

TSAPI Ports

TSAPI Service Port450

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

Enabled Disabled

☒ ☐

☒ ☐

☒ ☐

☒ ☐

☒ ☐

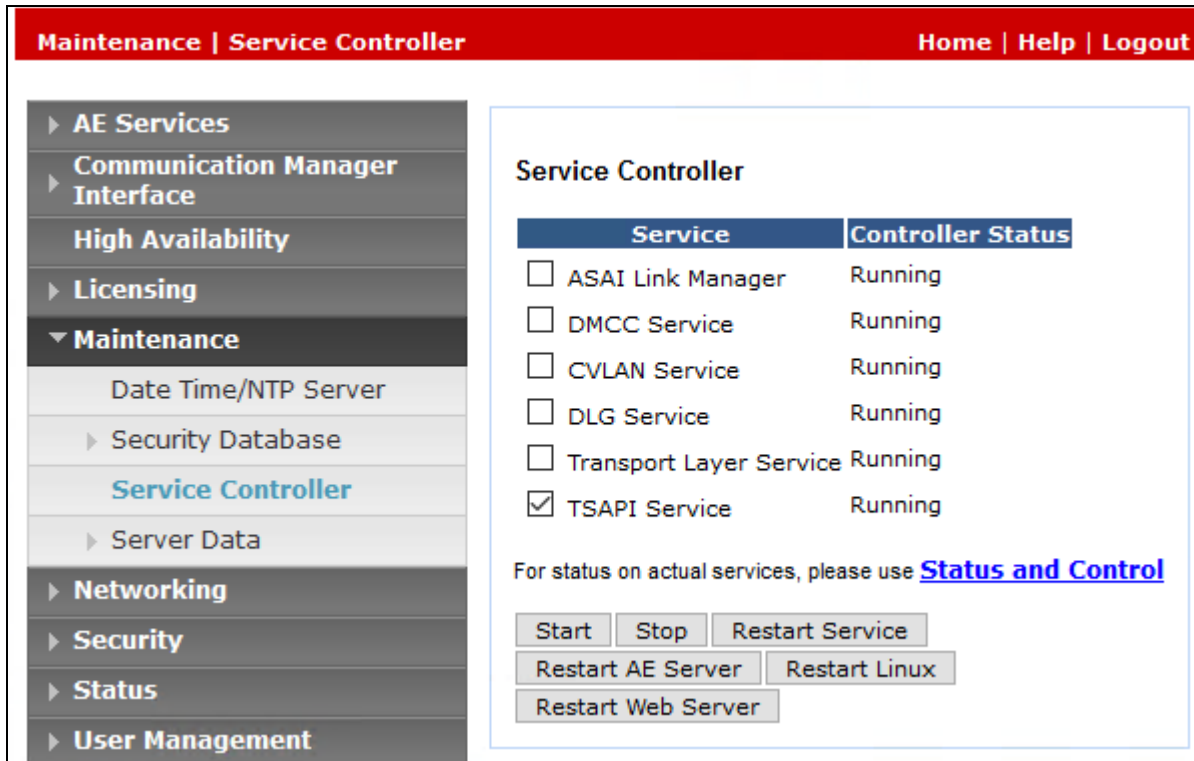
☒ ☐

☒ ☐

☒ ☐

6.10. Restart TSAPI Service

After the Application Enablement Services 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.



Maintenance | Service Controller **Home | Help | Logout**

- ▶ AE Services
- ▶ Communication Manager Interface
- High Availability
- ▶ Licensing
- ▼ **Maintenance**
 - Date Time/NTP Server
 - ▶ Security Database
 - Service Controller**
 - ▶ Server Data
- ▶ Networking
- ▶ Security
- ▶ Status
- ▶ User Management

Service Controller

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

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

Start

Stop

Restart Service

Restart AE Server

Restart Linux

Restart Web Server

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

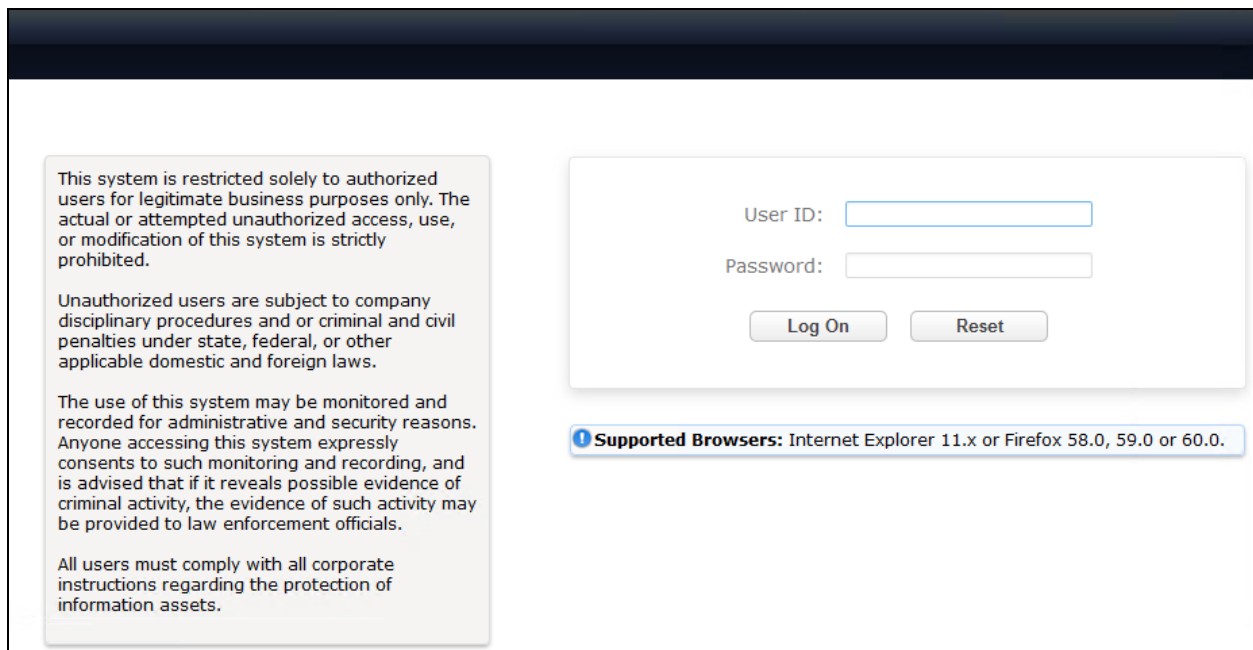
7. Configure Avaya Aura® Session Manager

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.



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.

The use of this system may be monitored and recorded for administrative and security reasons. Anyone accessing this system expressly consents to such monitoring and recording, and is advised that if it reveals possible evidence of criminal activity, the evidence of such activity may be provided to law enforcement officials.

All users must comply with all corporate instructions regarding the protection of information assets.

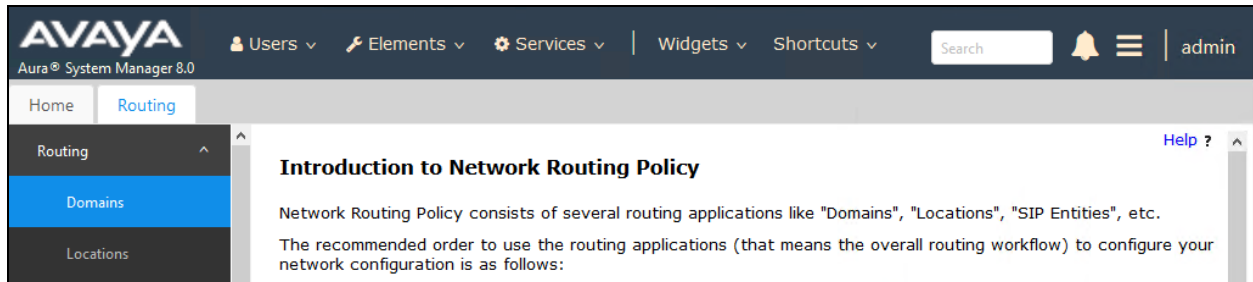
User ID:

Password:

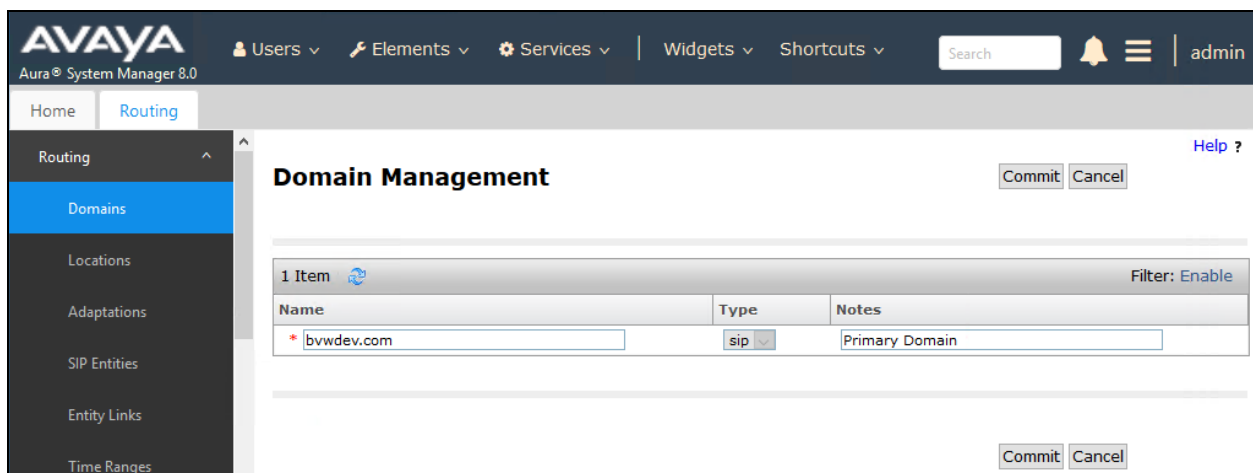
Supported Browsers: Internet Explorer 11.x or Firefox 58.0, 59.0 or 60.0.

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 8.0

Users ▾ Elements ▾ Services ▾ | Widgets ▾ Shortcuts ▾ Search 🔍 🔔 ☰

Home Routing

Routing Domains Locations Adaptations

Location Details

Commit Cancel

General

* Name: Belleville

Notes: Belleville DevConnect Lab

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

<input type="checkbox"/>	IP Address Pattern	Notes
<input type="checkbox"/>	* 10.33.5.*	
<input type="checkbox"/>	* 10.10.97.*	
<input type="checkbox"/>	* 10.10.98.*	
<input type="checkbox"/>	*	

Select : All, None

Commit Cancel

7.4. Administer Adaptation

During compliance test, to make the call from and to Communication Manager via Session Manager, Adaptation to translate IP address into domain name is used for Trio Enterprise SIP entity. Below are the steps that were used during compliance testing to create the needed 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 Enterprise Adaptation.

- **Adaptation Name:** An informative name (e.g., change IP to Domain of Trio Enterprise).
- **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, e.g.: bvwdev.com
iosrcd	Enter the domain name of system, e.g.: bvwdev.com
odstd	Enter IP address of Trio Enterprise SIP Server, e.g.: 10.10.98.158
osrcd	Enter IP address of Session Manager Server, e.g.: 10.10.97.228

Once the correct information is entered click the **Commit** button. Below is the screenshot showing the Adaptation created for Trio Enterprise.

The screenshot shows the Avaya Aura System Manager 8.0 interface. The left sidebar is expanded to 'Routing' > 'Adaptations'. The main panel is titled 'Adaptation Details' with 'Commit' and 'Cancel' buttons. Under the 'General' tab, the 'Adaptation Name' is 'For_Trio', the 'Module Name' is 'DigitConversionAdapter', and the 'Module Parameter Type' is 'Name-Value Parameter'. A table lists parameters: 'fromto' (true), 'iodstd' (bvwdev.com), and 'iosrcd' (bvwdev.com). The bottom of the table shows 'Select : All, None' and 'Page 1 of 2'.

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

The screenshot showing the continuation of the Adaptation values configured for Trio Enterprise.

This screenshot shows the continuation of the 'Adaptation Details' for 'For_Trio'. The table lists parameters: 'odstd' (10.10.98.158) and 'osrcd' (10.10.97.228). The bottom of the table shows 'Select : All, None' and 'Page 2 of 2'.

Name	Value
odstd	10.10.98.158
osrcd	10.10.97.228

7.5. Administer SIP Entities

Add two new SIP entities, one for Trio Enterprise and one for the new SIP trunks with Communication Manager.

7.5.1. 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 Trio Enterprise SIP Server.
- **Type:** “Other”
- **Notes:** Any desired notes.
- **Adaptation:** Select the adaptation configured in **Section 7.4**
- **Location:** Select the Trio Enterprise location name from **Section 7.3**.
- **Time Zone:** Select the applicable time zone.
- **SIP Link Monitoring:** Select “Use Session Manager Configuration”.

AVAYA
Aura® System Manager 8.0

Users ▾ Elements ▾ Services ▾ | Widgets ▾ Shortcuts ▾ Search 🔍

Home Routing

SIP Entity Details Commit Cancel

General

* Name: TrioATT

* FQDN or IP Address: 10.10.98.158

Type: Other ▾

Notes: SIP entity for a partner testing

Adaptation: For_Trio ▾

Location: Belleville ▾

Time Zone: America/Fortaleza ▾

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

Minimum TLS Version: Use Global Setting ▾

Credential name:

Securable: ☐

Call Detail Recording: none ▾

CommProfile Type Preference: ▾

Loop Detection

Loop Detection Mode: On ▾

Loop Count Threshold: 5

Loop Detection Interval (in msec): 200

Monitoring

SIP Link Monitoring: Use Session Manager Configuration ▾

Scroll down to the **Entity Links** sub-section and click **Add** to add an entity link. Enter the following values for the specified fields and retain the default values for the remaining fields.

- **Name:** A descriptive name.
- **SIP Entity 1:** The Session Manager entity name, in this case “DevvmSM”.
- **Protocol:** “TCP”.
- **Port:** “5060”.
- **SIP Entity 2:** The Trio Enterprise entity name from this section.
- **Port:** “5060”.
- **Connection Policy:** “trusted”.

Note that only TCP protocol was tested.

Entity Links

Override Port & Transport with DNS SRV: ☐

Add Remove

1 Item Filter: Enable

<input type="checkbox"/>	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Deny New Service
<input type="checkbox"/>	* DevvmSM_TrioATT_5060	DevvmSM	TCP	* 5060	TrioATT	* 5060	trusted	<input type="checkbox"/>

Select : All, None

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:** “CM”
- **Notes:** Any desired notes.
- **Location:** Select the applicable location for Communication Manager.
- **Time Zone:** Select the applicable time zone.

The screenshot displays the Avaya Aura System Manager 8.0 interface. The top navigation bar includes 'Users', 'Elements', 'Services', 'Widgets', and 'Shortcuts'. The left sidebar shows the 'Routing' menu with 'SIP Entities' selected. The main content area is titled 'SIP Entity Details' and contains the following sections:

- General**
 - Name:** DevvmCM
 - FQDN or IP Address:** 10.10.97.222
 - Type:** CM
 - Notes:** VM CM
 - Adaptation:** (empty dropdown)
 - Location:** Belleville
 - Time Zone:** America/Fortaleza
 - SIP Timer B/F (in seconds):** 4
 - Minimum TLS Version:** Use Global Setting
 - Credential name:** (empty text field)
 - Securable:** ☐
 - Call Detail Recording:** both
- Loop Detection**
 - Loop Detection Mode:** On
 - Loop Count Threshold:** 5
 - Loop Detection Interval (in msec):** 200
- Monitoring**
 - SIP Link Monitoring:** Use Session Manager Configuration

Buttons for 'Commit' and 'Cancel' are located at the top right of the configuration area.

Scroll down to the **Entity Links** sub-section and click **Add** to add an entity link. Enter the following values for the specified fields and retain the default values for the remaining fields.

- **Name:** A descriptive name.
- **SIP Entity 1:** The Session Manager entity name, in this case “DevvmSM”.
- **Protocol:** The signalling group transport (TLS) method from **Section 5.5**.
- **Port:** The signalling group listen port (5061) number from **Section 5.5**.
- **SIP Entity 2:** The Communication Manager entity name from this section.
- **Port:** The signalling group listen port (5061) number from **Section 5.5**.
- **Connection Policy:** “trusted”

Entity Links

Override Port & Transport with DNS SRV: ☐

Add Remove

1 Item [Filter: Enable](#)

<input type="checkbox"/>	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Deny New Service
<input type="checkbox"/>	* LinktoDevvmCM_TLS	DevvmSM	TLS	* 5061	DevvmCM	* 5061	trusted	<input type="checkbox"/>

Select : All, None

7.6. Administer Routing Policies

Add two new routing policies, one for Trio Enterprise and one for the new SIP trunks with Communication Manager.

7.6.1. Routing Policy for Trio Enterprise

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

The **Routing Policy Details** screen is displayed. In the **General** sub-section, enter a descriptive **Name**, and retain the default values in the remaining fields.

In the **SIP Entity as Destination** sub-section, click **Select** and select the Trio Enterprise entity name from **Section 7.5.1**. The screen below shows the result of the selection.

AVAYA
Aura® System Manager 8.0

Users ▾ Elements ▾ Services ▾ | Widgets ▾ Shortcuts ▾ Search 🔍

Home Routing

Routing Policies

Routing Policy Details

Commit Cancel

General

* **Name:**

Disabled: ☐

* **Retries:**

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
TrioATT	10.10.98.158	Other	SIP entity for a partner testing

7.6.2. Routing Policy for Communication Manager

Select **Routing** → **Routing Policies** from the left pane and click **New** in the subsequent screen (not shown) to add a new routing policy for Communication Manager.

The **Routing Policy Details** screen is displayed. In the **General** sub-section, enter a descriptive **Name**, and retain the default values in the remaining fields.

In the **SIP Entity as Destination** sub-section, click **Select** and select the Communication Manager entity name from **Section 7.5.2**. The screen below shows the result of the selection.

AVAYA
Aura® System Manager 8.0

Users ▾ Elements ▾ Services ▾ | Widgets ▾ Shortcuts ▾ Search 🔍

Home Routing

Routing Policy Details [Commit] [Cancel]

General

* Name: RouteToDevvmCM

Disabled: ☐

* Retries: 0

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
DevvmCM	10.10.97.222	CM	VM CM

7.7. Administer Dial Patterns

Add a new dial pattern for Trio Enterprise and Communication Manager.

7.7.1. 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 “71”.
- **Min:** The minimum number of digits to match.
- **Max:** The maximum number of digits to match.
- **SIP Domain:** The signalling 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 all Communication Manager endpoints in locations “Belleville”. The Trio Enterprise routing policy from **Section 7.6.1** was selected as shown below.

AVAYA

Aura® System Manager 8.0

Users

Elements

Services

Widgets

Shortcuts

Search

admin

Home

Routing

Domains

Locations

Adaptations

SIP Entities

Entity Links

Time Ranges

Routing Policies

Dial Patterns

Regular Expressions

Defaults

Dial Pattern Details

Commit

Cancel

General

* Pattern:

71

* Min:

5

* Max:

36

Emergency Call:

☐

SIP Domain:

bvwdev.com

Notes:

Dialing pattern to reach Trio Server

1 Item

Filter: Enable

<input type="checkbox"/>	Originating Location Name ▲	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	Belleville	Belleville DevConnect Lab	Route_to_Trio	0	<input type="checkbox"/>	TrioATT	Routing policy for Trio Server

Select : All, None

7.7.2. 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 “56” and “6190842”.
- **Min:** The minimum number of digits to match.
- **Max:** The maximum number of digits to match.
- **SIP Domain:** The signalling 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 “Belleville”. The Communication Manager routing policy from **Section 7.6.2** was selected as shown below.

AVAYA

Aura® System Manager 8.0

Users

Elements

Services

Widgets

Shortcuts

Search

admin

Home

Routing

Domains

Locations

Adaptations

SIP Entities

Entity Links

Time Ranges

Routing Policies

Dial Patterns

Regular Expressions

Defaults

Dial Pattern Details

CommitCancel

General

* Pattern: 56

* Min: 5

* Max: 5

Emergency Call: ☐

SIP Domain: bvwddev.com

Notes: Dial Pattern to VM CM

Originating Locations and Routing Policies

AddRemove

1 Item

Filter: Enable

<input type="checkbox"/>	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	Belleville	Belleville DevConnect Lab	RouteToDevvmCM	0	<input type="checkbox"/>	DevvmCM	

Select : All, None

AVAYA

[Users](#) |
 [Elements](#) |
 [Services](#) |
 [Widgets](#) |
 [Shortcuts](#) |
 Search |

 |
[adm](#)

Home |
 Routing

Routing ^

- Domains
- Locations
- Adaptations
- SIP Entities
- Entity Links
- Time Ranges
- Routing Policies
- Dial Patterns**
- Regular Expressions
- Defaults

Dial Pattern Details

General

* **Pattern:**

* **Min:**

* **Max:**

Emergency Call: ☐

SIP Domain: ▼

Notes:

Originating Locations and Routing Policies

1 Item
Filter: Enable

<input type="checkbox"/>	Originating Location Name ▲	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	Belleville	Belleville DevConnect Lab	RouteToDevvmCM	0	<input type="checkbox"/>	DevvmCM	

Select : All, None

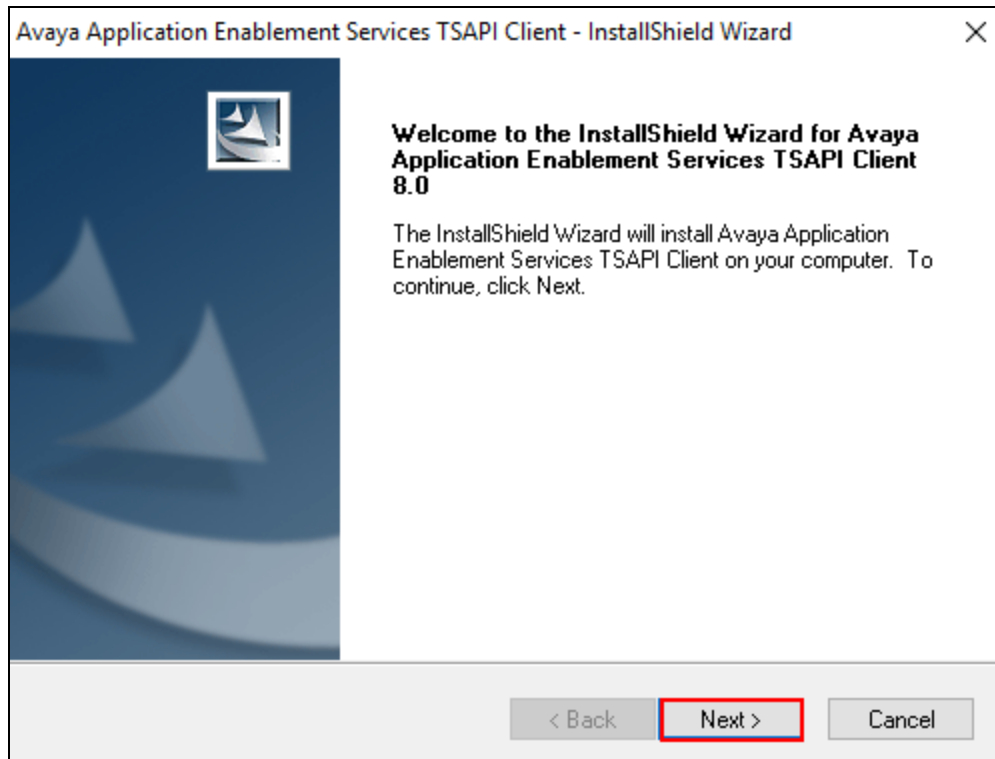
8. Configure Trio Enterprise

This section shows how to configure Trio Enterprise to successfully connect to Communication/Application Enablement Services. 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:

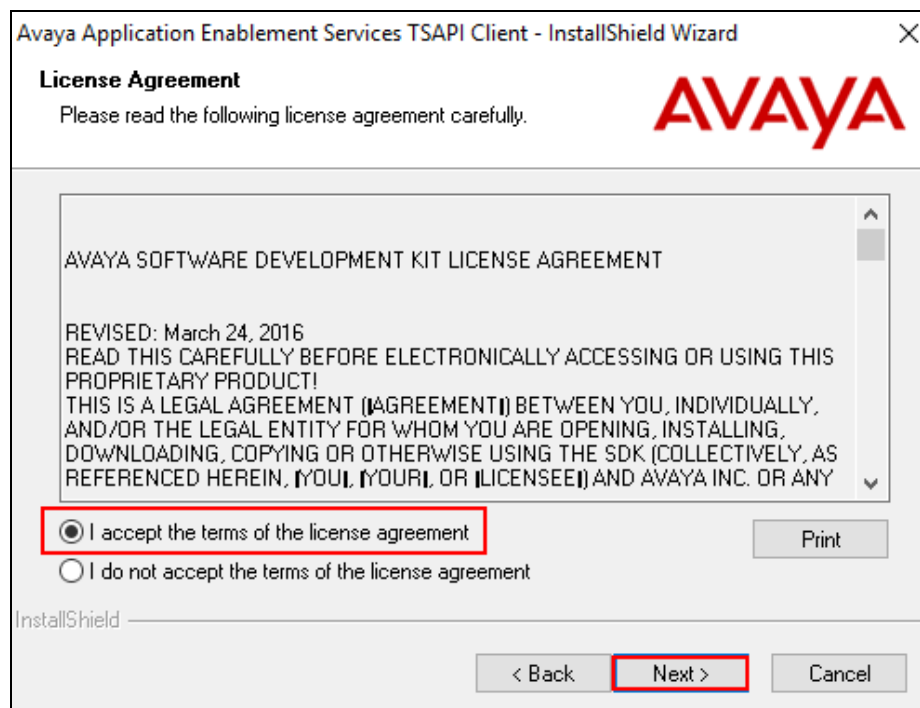
- Install Avaya Application Enablement Services TSAPI Client
- Configure Trio Enterprise to use SIP Trunks
- Configure Absence
- Configure Trio Enterprise Attendant

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 and select **Add to List**:

- **Host Name or IP Address:** Enter the IP address of the Application Enablement Services
- **Port Number:** Enter **450**

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

Avaya Application Enablement Services TSAPI Client - InstallShield Wizard

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

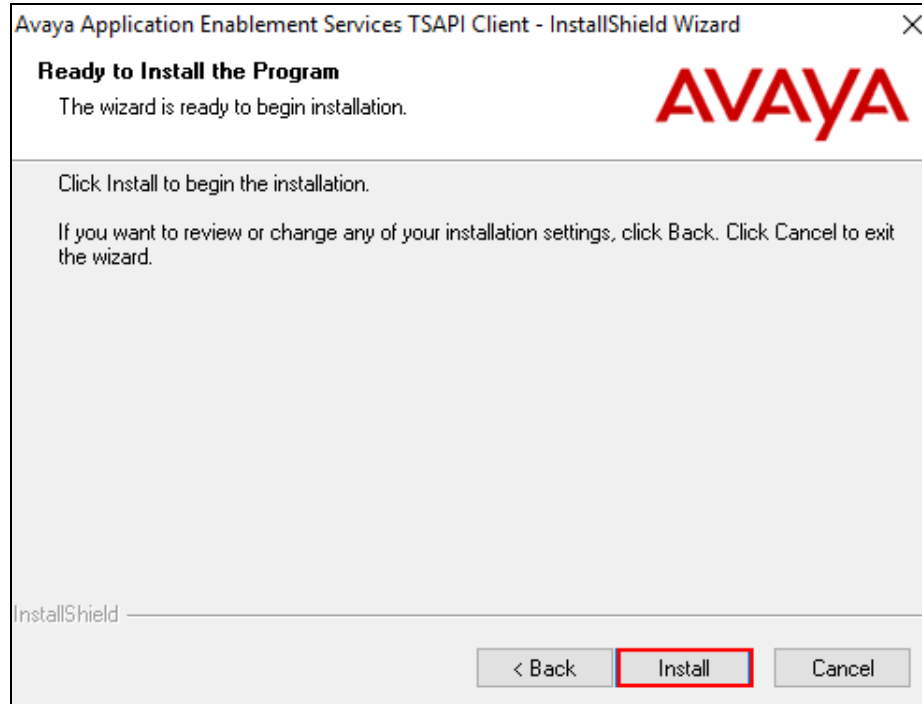
For each AE Services server that you wish to use, enter the server's host name or IP address (for example, aeserver.mydomain.com or 198.51.100.24) and the TSAPI Service port number.
The configured AE Services servers will be saved in the TSLIB.INI file.

Host Name or IP Address: Port Number:

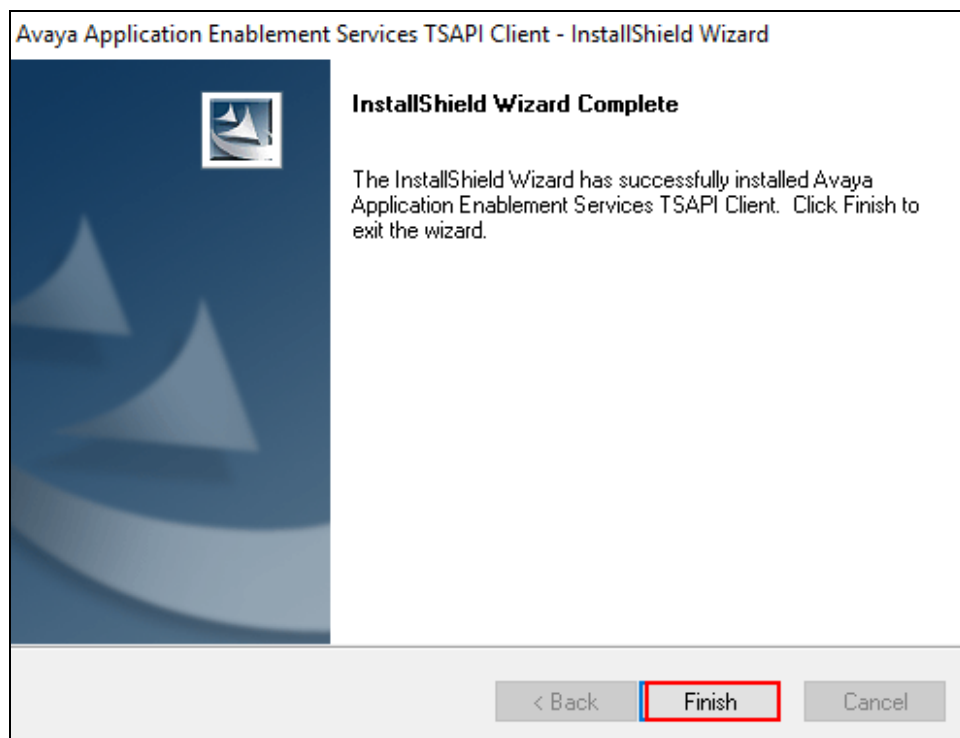
Configured AE Services Servers:

InstallShield

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



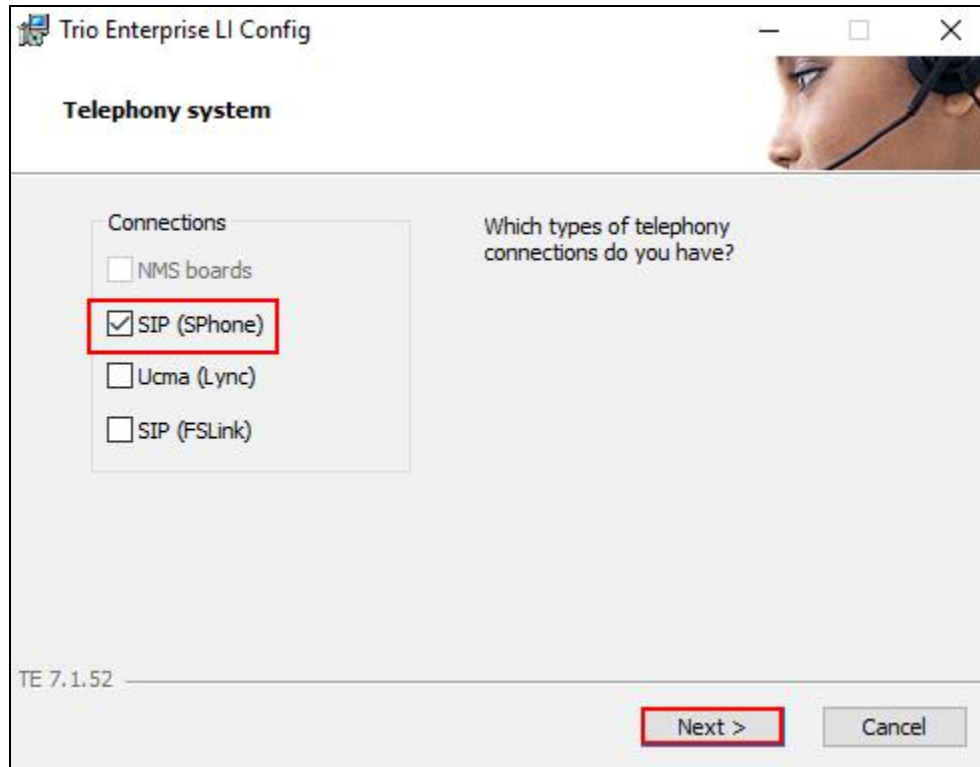
When the **InstallShield Wizard Complete** window appears click on the **Finish** button.



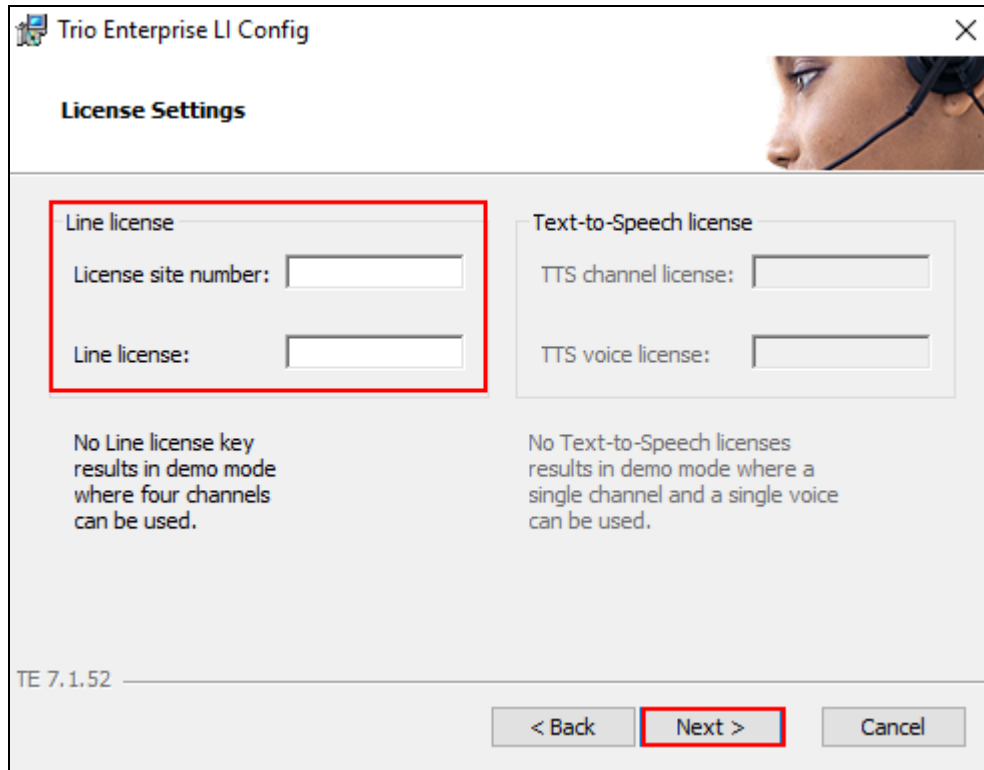
8.2. Configure Trio Enterprise to use SIP Trunks

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 license:** 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:

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

Text-to-Speech license

TTS channel license:

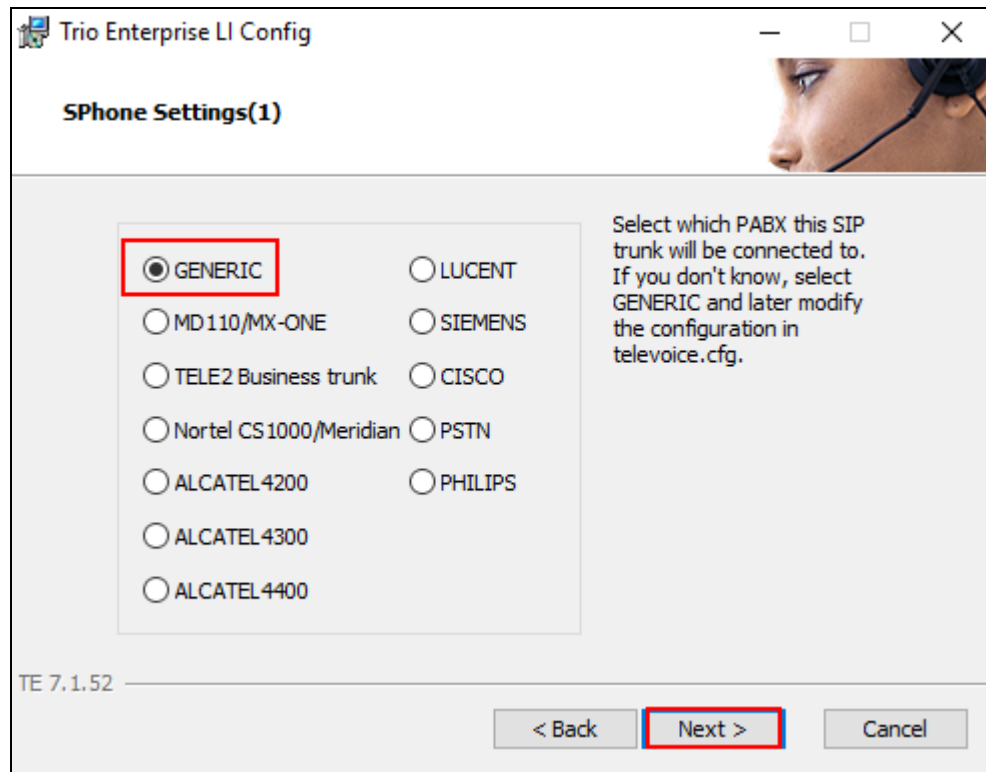
TTS voice license:

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

TE 7.1.52

< Back Next > Cancel

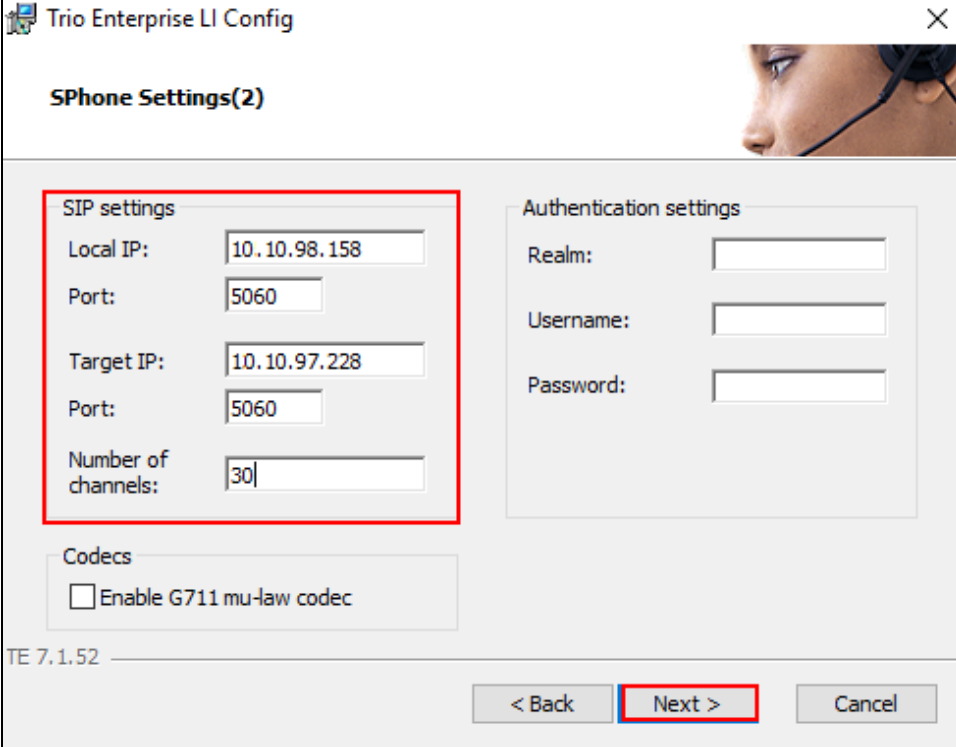
In the subsequent window, select on the **GENERIC** radio button followed by the **Next** button to continue.



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 with the 'SPhone Settings(2)' tab selected. The 'SIP settings' section is highlighted with a red box and contains the following fields:

- Local IP: 10.10.98.158
- Port: 5060
- Target IP: 10.10.97.228
- Port: 5060
- Number of channels: 30

The 'Authentication settings' section contains the following fields:

- Realm: [empty]
- Username: [empty]
- Password: [empty]

Below these sections is a 'Codecs' section with a checkbox labeled 'Enable G711 mu-law codec' which is currently unchecked. At the bottom of the window, the version 'TE 7.1.52' is displayed. The navigation buttons at the bottom are '< Back', 'Next >' (highlighted with a red box), 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 7.1.52

Additional SIP Trunk

< Back

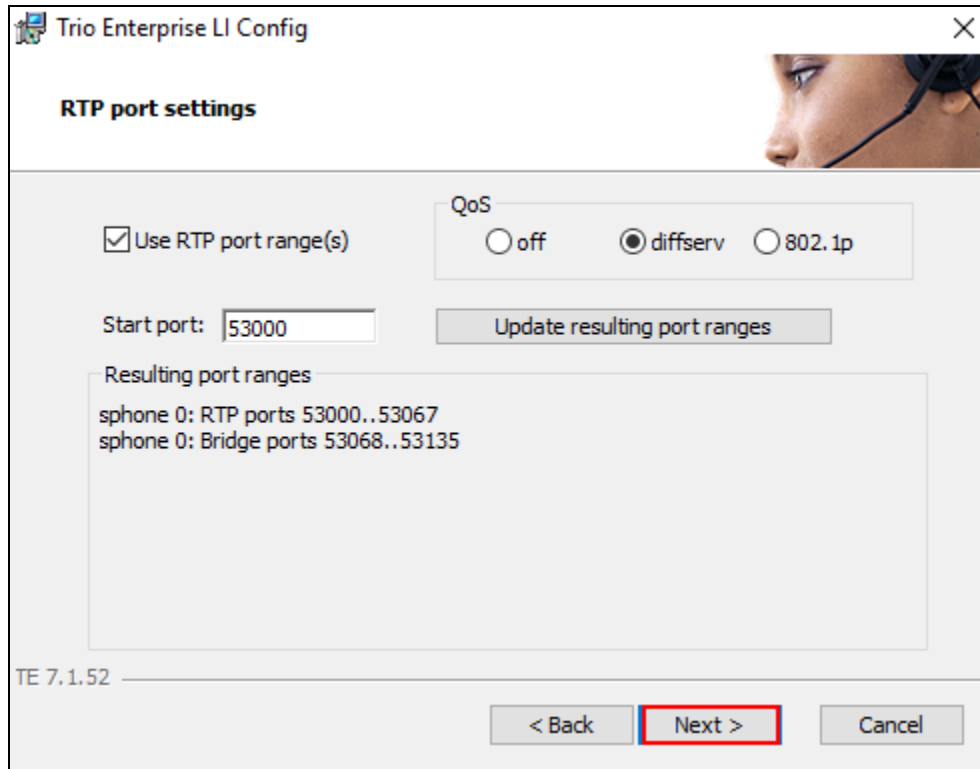
Next >

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.

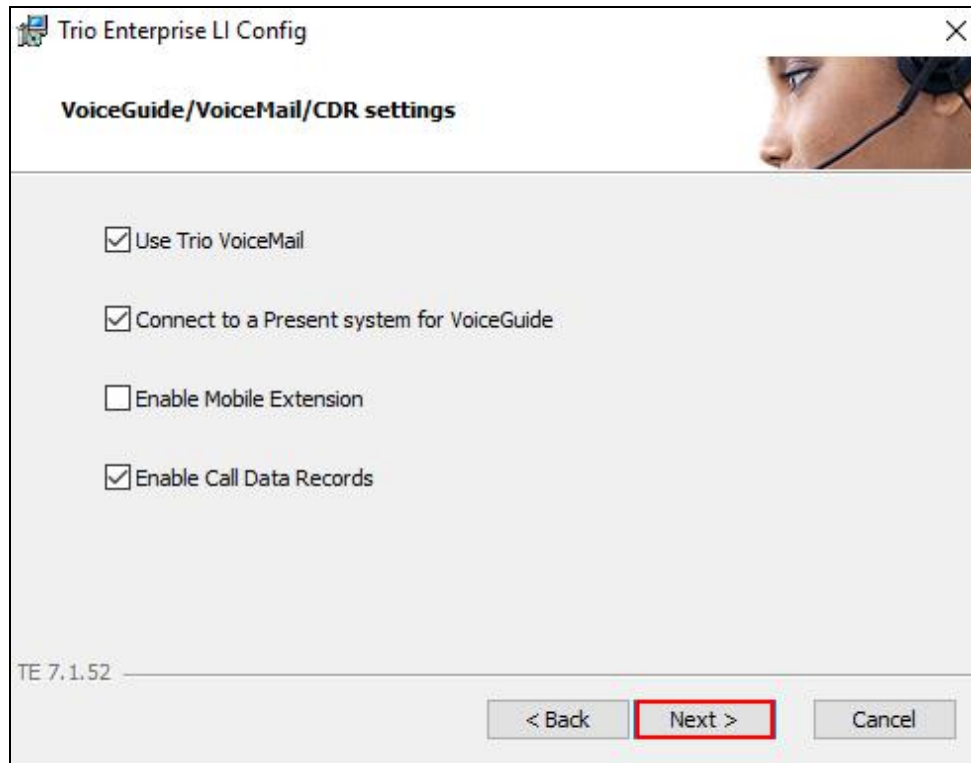


The screenshot shows the 'Trio Enterprise LI Config' window with the 'RTP port settings' tab selected. The 'Use RTP port range(s)' checkbox is checked. The 'QoS' section has three radio buttons: 'off', 'diffserv' (which is selected), and '802.1p'. The 'Start port' field contains the value '53000'. An '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 7.1.52' is displayed in the bottom left corner.

In the subsequent window enter the following settings:

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

Retain default values for other fields and click on the **Next** button to continue.

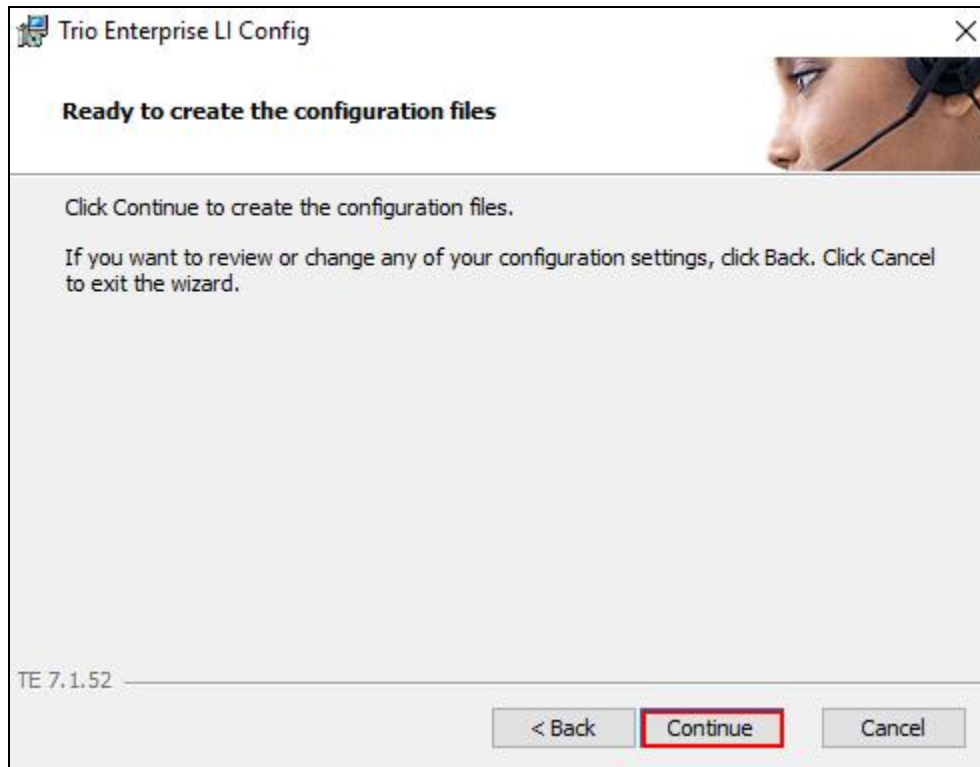


The screenshot shows a window titled "Trio Enterprise LI Config" with a close button in the top right corner. Below the title bar, there is a header area with the text "VoiceGuide/VoiceMail/CDR settings" and a small image of a person wearing a headset. The main area of the window contains four checkboxes:

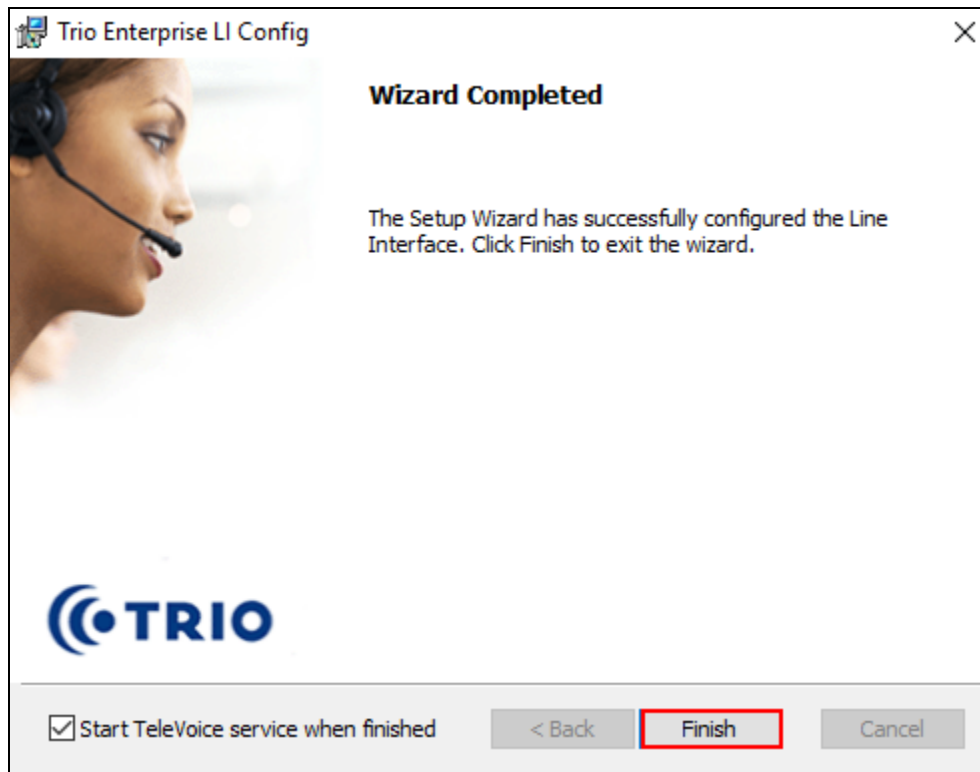
- ☒ Use Trio VoiceMail
- ☒ Connect to a Present system for VoiceGuide
- ☐ Enable Mobile Extension
- ☒ Enable Call Data Records

At the bottom left of the window, the text "TE 7.1.52" is displayed. At the bottom right, there are three buttons: "< Back", "Next >" (which is highlighted with a red border), and "Cancel".

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,

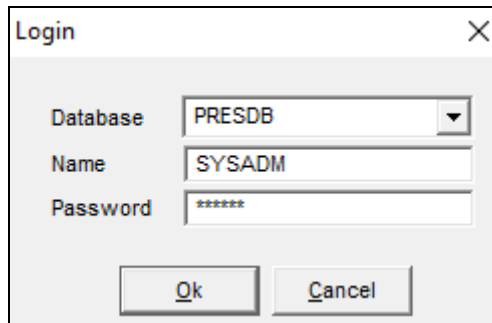
```
[sip_1]
signallingprotocol=sip
localHost=10.10.98.158
targetHost=10.10.97.228
uriScheme=1
transferPoint=afterAnswer
update=1
mwiMethod=unsolicited
rel100=false
allowTransferMedia=false
usetcp=1
```

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

```
[device_0]
type=sphone
access=127.0.0.1:33109
voiceserver_1=localhost:33813
sphone=0
localip=10.10.98.158
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
```

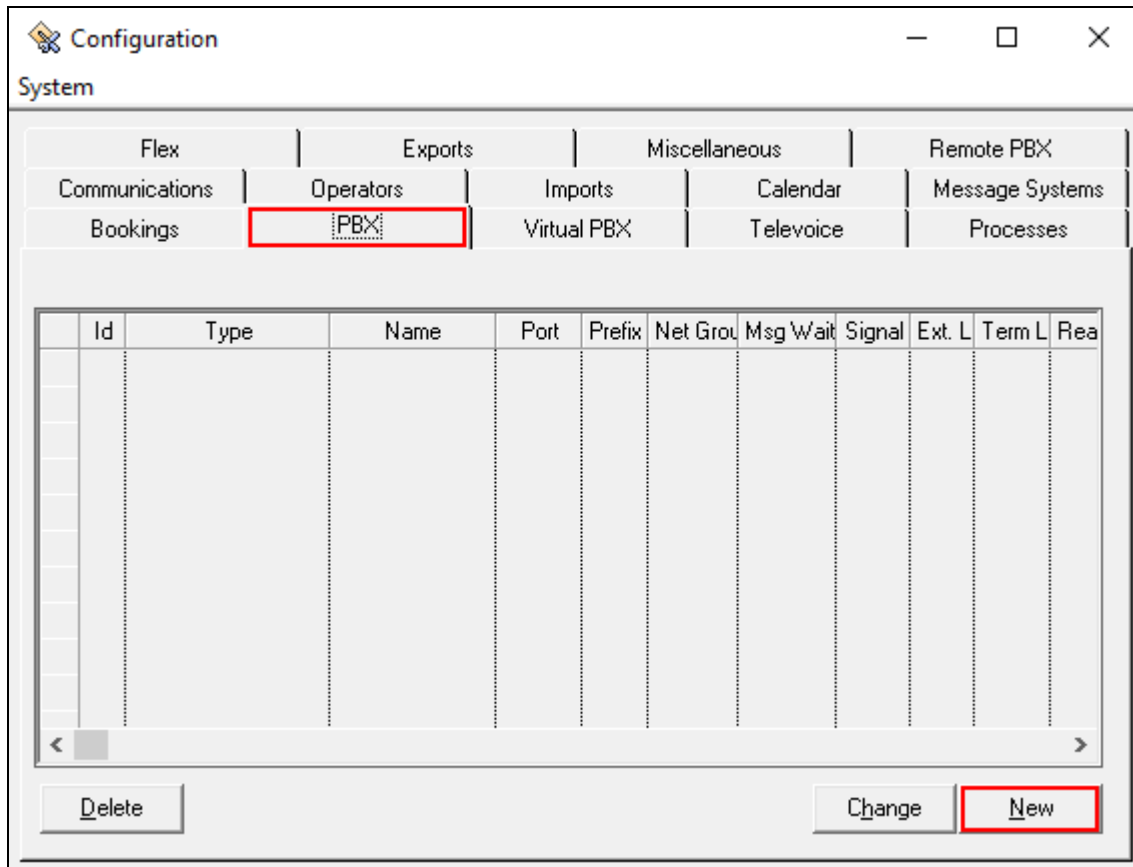
8.4. Configure Absence connection

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 a text box containing "SYSADM", and "Password" with a text box containing "*****". At the bottom are "Ok" and "Cancel" buttons.

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



A "Configuration" window titled "System" 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.

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 6.7**.
- **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 5.16.3**.
- **Referral destination:** Enter the number “71002” 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. On the left, under the 'Type' section, the 'Avaya CM' radio button is selected and highlighted with a red box. Below it, under the 'Virtual' section, several other options are listed. On the right, a red box highlights the main configuration area. This area includes the 'PbxName' field with the value 'Belleville', a 'Prefix' field, and several other fields: 'CSTA server' (AVAYA#DEVVMCM#CSTA#DEVVMAES), 'PBX login name' (Trio), 'PBX password' (password), 'Reason code length' (1), 'Routing device' (56008), and 'Referral destination' (71002). A checkbox labeled 'Monitor line state for all extensions' is checked. At the bottom left, the 'OK' button is highlighted with a red box, and the 'Cancel' button is next to it.

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 56402 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: 56402

Phone type: Standard phone

Location: Location 1

Work mode: Switchboard operator

Server: teipo

☐ 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 7.1.52.717
© 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	devvmaes	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 (DevvmSM in the example below).

The screenshot shows the Avaya Aura System Manager 8.0 interface. The left sidebar contains navigation links: Home, Session Manager, Session Manager Ad..., Global Settings, Communication Pro..., Network Configur..., Device and Locati..., Application Confi..., and System Status. The main content area is titled "SIP Entity Link Monitoring Status Summary" and includes a "Run Monitor" button. Below this, a table shows the status of monitored entities for the DevvmSM instance.

SIP Entities Status for All Monitoring Session Manager Instances								
Run Monitor								
1 Item Filter: Enable								
<input type="checkbox"/>	Session Manager	Type	Monitored Entities					
			Down	Partially Up	Up	Not Monitored	Deny	Total
<input type="checkbox"/>	DevvmSM	Core	9	1	16	1	0	27

Select : All, None

Below the table, there is a section titled "All Monitored SIP Entities" with a "Run Monitor" button.

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

AVAYA Aura® System Manager 8.0

Users ▾ Elements ▾ Services ▾ | Widgets ▾ Shortcuts ▾ Search 🔍 🔔 ☰ | adm

Home Session Manager

Session Manager ^

- Dashboard
- Session Manager Ad...
- Global Settings
- Communication Pro...
- Network Configur... ▾
- Device and Locati... ▾
- Application Confi... ▾
- System Status ^
- SIP Entity Monit...

Session Manager Entity Link Connection Status

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

Status Details for the selected Session Manager:

All Entity Links for Session Manager: DevvmSM

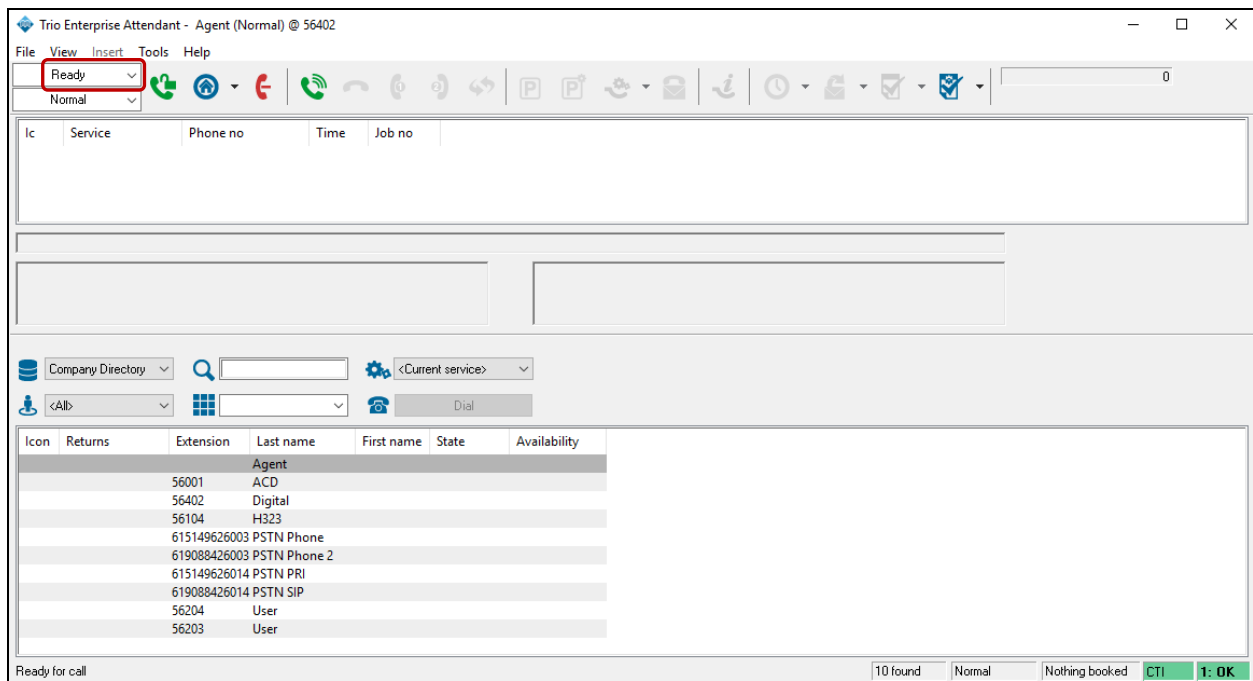
Summary View

30 Items 🔁 Filter: Enable

	SIP Entity Name	IP Address Family	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
<input type="radio"/>	DevvmCM	IPv4	10.10.97.222	5061	TLS	FALSE	UP	200 OK	UP
<input type="radio"/>	TrioATT	IPv4	10.10.98.158	5060	TCP	FALSE	UP	200 OK	UP
<input type="radio"/>									
<input type="radio"/>									
<input type="radio"/>									
<input type="radio"/>									

9.3. Verify Trio Enterprise Attendant

To verify that Trio Enterprise is connected to Communication Manager via Session Manager, log in to the Trio Enterprise Attendant at **Start → Programs → Trio Enterprise → Contact Centre → Agent Client** (not shown) or launch the shortcut mentioned in **Section 8.5**. Complete log in with the appropriate credentials as shown in **Section 8.5**. The Trio Enterprise Attendant window appears as shown below. Select **Ready** from the drop-down box.



The following scenarios were also tested:

- Incoming internal and external calls
- Outgoing internal and external calls
- Supervised and unsupervised transfer with answer
- Directing calls from busy extensions and extensions that do not answer
- Call queuing and retrieval
- Loop detection for busy and unanswered extensions
- Absence detection
- Message Waiting Indicator

10. Conclusion

These Application Notes describe the procedures required to configure Trio Enterprise from Enghouse Interactive AB to interoperate with Avaya Aura® Communication Manager, Avaya Aura® Application Enablement Services and Avaya Aura® Session Manager using SIP Trunks and TSAPI.

All feature functionality test cases described in **Section 2.1** were passed with the observations pointed in **Section 2.2**.

11. Additional References

This section references the product documentation relevant to these Application Notes.

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

1. *Deploying Avaya Aura® Communication Manager in Virtual Appliance*, Release 8.0, Issue 3 September 2018.
2. *Avaya Aura® Communication Manager Feature Description and Implementation*, Release 8.0, Issue 1 July 2018.
3. *Administering Avaya Aura® Communication Manager*, Release 8.0, Issue 1 July 2018.
4. *Avaya Aura® Communication Manager Screen Reference*, Release 8.0, Issue 2 August 2018.
5. *Deploying Avaya Aura® Session Manager in Virtual Appliance*, Release 8.0, Issue 2 September 2018.
6. *Administering Avaya Aura® Session Manager*, Release 8.0, Issue 2 August 2018.
7. *Deploying Avaya Aura® System Manager in Virtualized Environment*, Release 8.0, Issue 2 September 2018.
8. *Administering Avaya Aura® System Manager for Release 8.0*, Release 8.0, Issue 4 September 2018.
9. *Deploying and Updating Avaya Aura® Media Server Appliance*, Release 8.0, Issue 2 July 2018.
10. *Implementing and Administering Avaya Aura® Media Server*, Release 8.0, Issue 2 July 2018.

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

©2019 Avaya Inc. All Rights Reserved.

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

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