



Avaya Solution & Interoperability Test Lab

Application Notes for Trio Enterprise from Enghouse Interactive AB 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 Session Manager. A TSAPI connection on Application Enablement Services enables the Trio Enterprise Absence and Voicemail 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 Communication Manager using a SIP trunk through Session Manager. See **Figure 1** for a network diagram. A dial plan was configured on 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 performs a transfer using the SIP Refer method, and the caller and the called user are now directly connected.

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

Note: During compliance testing Avaya SIP and H.323 endpoints were used as the attendant's telephones.

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
- Re-directing calls to 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 Communication Manager, Session Manager and Application Enablement Services. The tests were all functional in nature and performance testing was not included. All test cases passed.

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 Session Manager. TSAPI is configured on the Trio Enterprise server which enables Trio Enterprise to interact with telephones on Communication Manager to enable call forwarding and Voicemail via 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 Communication Manager to generate outbound/inbound calls to/from the PSTN. An ISDN-PRI/T1 trunk on Avaya G450 Media Gateway was configured to connect to the simulated PSTN.

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

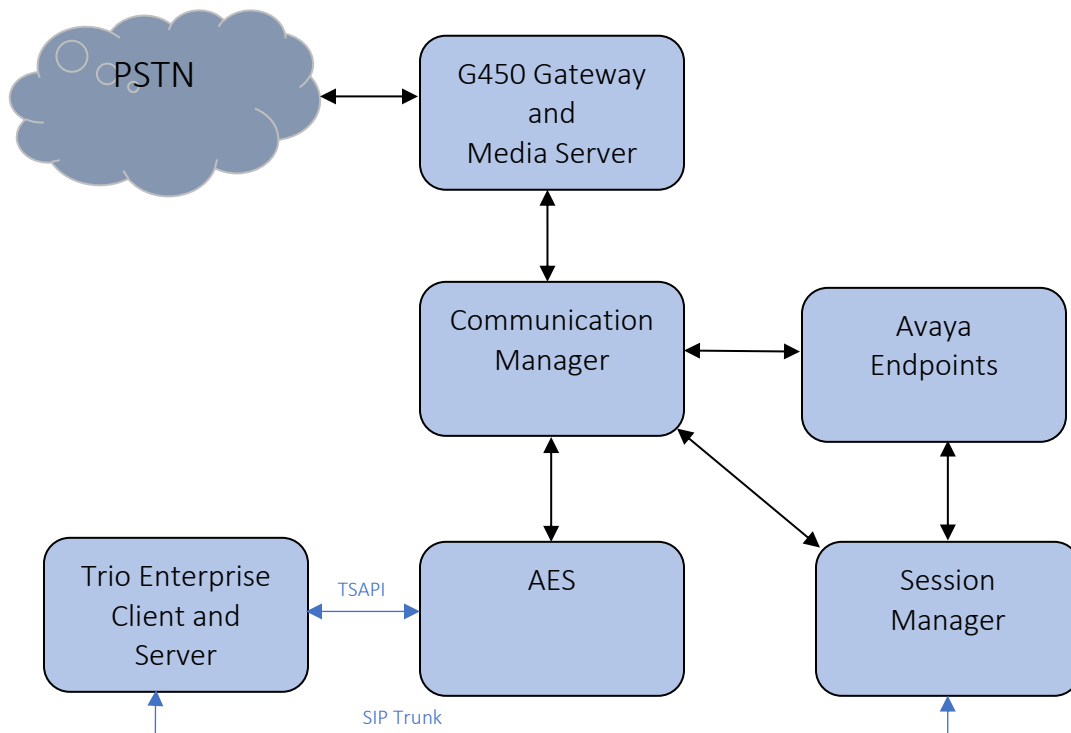


Figure 1: Avaya and Trio Enterprise Reference Configuration

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	8.1.0.1.1.890.25517
Avaya Aura® Application Enablement Services	8.1.0.0.9-1
Avaya Aura® Session Manager	8.1.0.0.810007
Avaya Aura® System Manager	8.1.0.0.733078
Avaya Aura® Media Server	8.0.1.121
Avaya G450 Media Gateway	40.10.0/1
Avaya IP Deskphones	
- 9641GS (SIP)	7.1.6
- 9608 (H.323)	6.8.2
Avaya one-X® Communicator	6.2.10
Trio Enterprise Server and Client running on Microsoft Windows 2012 R2 Server	8.0
Avaya TSAPI Client for Windows	8.1

5. Configure Avaya Aura® Communication Manager

Configuration and verification operations on Communication Manager illustrated in this section were all performed using System Access Terminal (SAT). The information provided in this section describes the configuration of Communication Manager for this solution. For all other provisioning information, such as initial installation and configuration, please refer to the product documentation 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 AAR analysis
- Configure interface to Application Enablement Services
- Create a CTI Link to Application Enablement Services
- Administer COS

5.1. Verify License

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

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

display system-parameters customer-options		Page	2 of 12
OPTIONAL FEATURES			
IP PORT CAPACITIES		USED	
Maximum Administered H.323 Trunks:		12000	20
Maximum Concurrently Registered IP Stations:		18000	3
Maximum Administered Remote Office Trunks:		12000	0
Maximum Concurrently Registered Remote Office Stations:		18000	0
Maximum Concurrently Registered IP eCons:		128	0
Max Concur Registered Unauthenticated H.323 Stations:		100	0
Maximum Video Capable Stations:		36000	3
Maximum Video Capable IP Softphones:		18000	3
Maximum Administered SIP Trunks:		12000	58
Maximum Administered Ad-hoc Video Conferencing Ports:		12000	0
Maximum Number of DS1 Boards with Echo Cancellation:		522	0
display system-parameters customer-options		Page	4 of 12
OPTIONAL FEATURES			
Abbreviated Dialing Enhanced List?	y	Audible Message Waiting?	y
Access Security Gateway (ASG)?	n	Authorization Codes?	y
Analog Trunk Incoming Call ID?	y	CAS Branch?	n
A/D Grp/Sys List Dialing Start at 01?	y	CAS Main?	n
Answer Supervision by Call Classifier?	y	Change COR by FAC?	n
ARS?	y	Computer Telephony Adjunct Links?	y
ARS/AAR Partitioning?	y	Cvg Of Calls Redirected Off-net?	y
ARS/AAR Dialing without FAC?	y	DCS (Basic)?	y
ASAI Link Core Capabilities?	y	DCS Call Coverage?	y
ASAI Link Plus Capabilities?	y	DCS with Rerouting?	y
Async. Transfer Mode (ATM) PNC?	n	Digital Loss Plan Modification?	y
Async. Transfer Mode (ATM) Trunking?	n	DS1 MSP?	y
ATM WAN Spare Processor?	n	DS1 Echo Cancellation?	y
ATMS?	y		
Attendant Vectoring?	y		

5.2. Administer System Parameter Features

During compliance testing, Trio Enterprise suggested that the Station Call Transfer Recall Timer be set to 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? y

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
```


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

5.3. Administer IP Node Names

Use the “change node-names ip” command and add an entry for Session Manager. In this case, “sm81” and “10.64.110.212” are entered as **Name** and **IP Address**. Note the “procr” and “10.64.110.213” 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 “aes81” and “10.64.110.215”, respectively, which will be used later in the Application Enablement Services configuration as shown in **Section 5.14**.

change node-names ip		Page 1 of 2
IP NODE NAMES		
Name	IP Address	
aes81	10.64.110.215	
ams81	10.64.110.214	
procr	10.64.110.213	
sm81	10.64.110.212	

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 5	
TRUNK GROUP			
Group Number: 1	Group Type: sip	CDR Reports: y	
Group Name: SM Trunk	COR: 1	TN: 1	TAC: 101
Direction: two-way	Outgoing Display? n	Night Service:	
Dial Access? n			
Queue Length: 0			
Service Type: tie	Auth Code? n		
Member Assignment Method: auto			
Signaling Group: 1			
Number of Members: 10			

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

add trunk-group 1		Page 3 of 5	
TRUNK FEATURES			
ACA Assignment? n	Measured: both	Maintenance Tests? y	
Suppress # Outpulsing? n	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			
Send UCID? y			
Show ANSWERED BY on Display? y			

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.
- **Direct IP-IP Audio Connections?:** “y”.

add 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	Clustered? n
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: sm81
Near-end Listen Port: 5061		Far-end Listen Port: 5061
		Far-end Network Region: 1
Far-end Domain:		
Incoming Dialog Loopbacks: eliminate		Bypass If IP Threshold Exceeded? n
DTMF over IP: rtp-payload		RFC 3389 Comfort Noise? n
Session Establishment Timer(min): 3		Direct IP-IP Audio Connections? y
Enable Layer 3 Test? y		IP Audio Hairpinning? n
H.323 Station Outgoing Direct Media? n		Initial IP-IP 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 “10”.

```
change trunk-group 1                                     Page 1 of 5
                                                         TRUNK GROUP

Group Number: 1                Group Type: sip           CDR Reports: y
Group Name: SM Trunk           COR: 1                   TN: 1           TAC: 101
Direction: two-way            Outgoing Display? n
Dial Access? n                Night Service:
Queue Length: 0
Service Type: tie              Auth Code? n
                               Member Assignment Method: auto
                               Signaling Group: 1
                               Number of Members: 10
```

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: avaya.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
```

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. Configure the codec as shown below.

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

                                IP CODEC SET

    Codec Set: 1

    Audio      Silence      Frames      Packet
    Codec      Suppression  Per Pkt    Size(ms)
1: G.711A      n           2          20
2:
Media Encryption                               Encrypted SRTCP: enforce-unenc-srtcp
1: none
2:
3:
4:
5:
```

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									
No Mrk Lmt List Del Digits									
DCS/ IXC									
QSIG									
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 “7” and routed to trunk group all trunks 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	5				5	Total Administered: 2			
5	7				5	Maximum Entries: 540			

5.12.Administer AAR Analysis

Use the “change aar analysis 51” command and add an entry to specify how to route calls to 51xxx. In the example shown below, calls with digits 51 will be routed as an AAR call using route pattern “1” from **Section 5.9**.

change aar analysis 51						Page 1 of 2	
AAR DIGIT ANALYSIS TABLE							
Location: all						Percent Full: 0	
	Dialed	Total		Route	Call	Node	ANI
	String	Min	Max	Pattern	Type	Num	Reqd
51		5	5	1	aar		n

5.13. 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

5.13.1.Configure VDN 1

During compliance testing VDN 78201 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 21”.

change vdn 78201		Page 1 of 3	
VECTOR DIRECTORY NUMBER			
Extension: 78201		Unicode Name? n	
Name*: Phone Diversion			
Destination: Vector Number		21	
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*:			

5.13.2. Configure Vector 7

Configure the Vector that was used as the **Vector Number** in **Section 5.13.1**. Use the “change vector 21” command, and configure the following:

- **Name:** Enter an informative name (i.e. Phone diversion).
- **Line 01:** Enter “wait-time 2 secs hearing silence”.
- **Line 02:** Enter “collect 9 digits after announcement none for none”.
- **Line 03:** Enter “route-to number 78202 with cov n if unconditionally”.

In this example, using monitored phone dial 78201 + reason code + #, call is routed to 78202 which will trigger Trio Enterprise to set the phone absence with appropriate reason announcement.

```
change vector 21                                     Page 1 of 6

                                CALL VECTOR

Number: 21                                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      2      secs hearing silence
02 collect      9      digits after announcement none      for none
03 route-to      number 78202      cov n if unconditionally
```

5.13.3. Configure VDN 2

Configure a VDN using the “route-to number” as used in **Section 5.13.2**. This VDN is used for activating referrals from the phone set. Use the “add vdn 78202” command, and configure the following:

- **Name*:** Enter an informative name (i.e. Diversion).
- **Destination:** Enter “Vector Number 22”.

```
change vdn 78202                                     Page 1 of 3

                                VECTOR DIRECTORY NUMBER

                                Extension: 78202                                Unicode Name? n
                                Name*: Diversion
                                Destination: Vector Number      22
                                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*:
```


5.13.4.Configure Vector 8

Configure the Vector that was used as the “Vector Number” in **Section 5.13.3**. Use the “change vector 22” command, and configure the following:

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

change vector 22	CALL VECTOR	Page 1 of 6
Number: 22	Name: Diversion	
Multimedia? n	Attendant Vectoring? n	Meet-me Conf? n
Basic? y	EAS? y	G3V4 Enhanced? y
Prompting? y	LAI? y	G3V4 Adv Route? y
Variables? y	3.0 Enhanced? y	CINFO? y
		BSR? y
		Holidays? y
01 wait-time	100 secs hearing ringback	
02 stop		
03		

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 “aes81” (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 Application Enablement Services to communicate with Communication Manager.
- **Enabled:** Enter “y”

change ip-services				Page	3 of	3
AE Services Administration						
Server ID	AE Services Server	Password	Enabled	Status		
1:	aes81	*	y	in use		

5.15. Create a CTI Link to Avaya Aura® Application Enablement Services

A CTI Link needs to be created to enable Communication Manager to interoperate with 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. 77777).
- **Type:** Enter “ADJ-IP”.
- **Name:** Enter a descriptive name (i.e. CTI Link 1)

```
add cti-link 1                                     Page 1 of 3
CTI LINK
CTI Link: 1
Extension: 77777
Type: ADJ-IP
Name: CTI Link 1
Unicode Name? n
COR: 1
```

5.16. Administer COS

In order for a CTI application to set transfer destination, **Restrict Call Fwd-Off Net** needs to be disabled. In this case, this option was disabled for this COS 1.

change cos-group 1										Page 1 of 2						
CLASS OF SERVICE	COS Group: 1				COS Name:											
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Auto Callback	n	y	y	n	y	n	y	n	y	n	y	n	y	n	y	n
Call Fwd-All Calls	n	y	n	y	y	n	n	y	y	n	n	y	y	n	n	y
Data Privacy	n	y	n	n	n	y	y	y	y	n	n	n	n	y	y	y
Priority Calling	n	y	n	n	n	n	n	n	n	y	y	y	y	y	y	y
Console Permissions	n	y	n	n	n	n	n	n	n	n	n	n	n	n	n	n
Off-hook Alert	n	y	n	n	n	n	n	n	n	n	n	n	n	n	n	n
Client Room	n	y	n	n	n	n	n	n	n	n	n	n	n	n	n	n
Restrict Call Fwd-Off Net	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n
Call Forwarding Busy/DA	n	y	n	n	n	n	n	n	n	n	n	n	n	n	n	n
Personal Station Access (PSA)	n	y	n	n	n	n	n	n	n	n	n	n	n	n	n	n
Extended Forwarding All	n	y	n	n	n	n	n	n	n	n	n	n	n	n	n	n
Extended Forwarding B/DA	n	y	n	n	n	n	n	n	n	n	n	n	n	n	n	n
Trk-to-Trk Transfer Override	n	y	n	n	n	n	n	n	n	n	n	n	n	n	n	n
QSIG Call Offer Originations	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n
Contact Closure Activation	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n

6. Configuration of Avaya Aura® Application Enablement Services

This section provides the procedures for configuring Application Enablement Services. 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 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.



Application Enablement Services Management Console


Help

Please login here:

Username

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

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



Application Enablement Services
Management Console

Welcome: User cust
Last login: Tue Nov 19 12:30:52 2019 from 10.64.10.47
Number of prior failed login attempts: 0
HostName/IP: aes81/10.64.110.215
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.1.0.0.0.9-1
Server Date and Time: Tue Nov 19 12:31:45 MST 2019
HA Status: Not Configured

Home

Home | Help | Logout

▶ AE Services

▶ Communication Manager Interface

▶ High Availability

▶ Licensing

▶ Maintenance

▶ Networking

▶ Security

▶ Status

▶ User Management

▶ Utilities

▶ Help

Welcome to OAM

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

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

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

6.2. 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.

Licensing

Home | Help | Logout

▶ AE Services

▶ Communication Manager Interface

▶ High Availability

▼ Licensing

WebLM Server Address

WebLM Server Access

Reserved Licenses

▶ Maintenance

▶ Networking

▶ Security

▶ Status

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

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
Install license
Licensed products
APPL_ENAB
▼ Application_Enablement
View license capacity
View peak usage
ASBCE
▶ Session_Border_Controller_E_AE
CE
▶ COLLABORATION_ENVIRONMENT
COMMUNICATION_MANAGER
▶ Call_Center
▶ Communication_Manager
▶ Dialog_Designer
MESSAGING
▶ Messaging
MSR
▶ Media_Server
ORCHESTRATION_DESIGNER_IDE
▶ Orchestration_Designer_IDE
POM
▶ POM
PRESENCE_SERVICES
▶ Presence_Services
SYSTEM_MANAGER
▶ System_Manager
SessionManager
▶ SessionManager

Application Enablement (CTI) - Release: 8 - SID: 10503000

Standard

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

License installed on: July 18, 2019 2:10:38 PM -07:00

License File Host IDs:

Licensed Features

13 Items
Show All

Feature (License Keyword)	Expiration date	Licensed capacity
Device Media and Call Control VALUE_AES_DMCC_DMC	permanent	100
AES ADVANCED LARGE SWITCH VALUE_AES_AEC_LARGE_ADVANCED	permanent	100
AES HA LARGE VALUE_AES_HA_LARGE	permanent	100
AES ADVANCED MEDIUM SWITCH VALUE_AES_AEC_MEDIUM_ADVANCED	permanent	100
Unified CC API Desktop Edition VALUE_AES_AEC_UNIFIED_CC_DESKTOP	permanent	100
CVLAN ASAI VALUE_AES_CVLAN_ASAI	permanent	100
AES HA MEDIUM VALUE_AES_HA_MEDIUM	permanent	100
AES ADVANCED SMALL SWITCH VALUE_AES_AEC_SMALL_ADVANCED	permanent	100
DLG VALUE_AES_DLG	permanent	100
TSAPI Simultaneous Users VALUE_AES_TSAPI_USERS	permanent	100
CVLAN Proprietary Links VALUE_AES_PROPRIETARY_LINKS	permanent	100
		SmallServerTypes: s8300c;s8300d;icc;premio;tn8400;laptop;CtiS MediumServerTypes: ibmx306;ibmx306m;dell1950;xen;hs20;hs20 LargeServerTypes:

6.3. Create an Avaya Aura® Communication Manager Switch Connection

A Communication Manager Switch Connection needs to be created to enable Application Enablement Services to communicate with Communication Manager. Navigate to **Communication Manager Interface** → **Switch Connections**. In the **Switch Connections** page, enter an informative name for Communication Manager (i.e. cm81). Click on the **Add Connection** button.

Communication Manager Interface | Switch Connections Home | Help | Logout

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

Switch Connections

cm81 Add Connection

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections
cm81	Yes	30	1

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

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

Communication Manager Interface | Switch Connections Home | Help | Logout

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

Connection Details - cm81

Switch Password
Confirm Switch Password
Msg Period 30 Minutes (1 - 72)
Provide AE Services certificate to switch ☐
Secure H323 Connection ☐
Processor Ethernet ☒
Apply Cancel

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

Locate the connection name associated with the relevant Communication Manager, in this case “cm81”, and select the corresponding radio button. Click **Edit PE/CLAN IPs**.

Communication Manager Interface | Switch Connections Home | Help | Logout

Switch Connections

Add Connection

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections
<input checked="" type="radio"/> cm81	Yes	30	1

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

The **Edit Processor Ethernet IP** screen is displayed. Enter the IP address of a C-LAN circuit pack or the Processor on Communication Manager to be used, in this case “10.64.110.213” as shown below, which is the Processor on Communication Manager. Click **Add/Edit Name or IP**.

Communication Manager Interface | Switch Connections Home | Help | Logout

Edit Processor Ethernet IP - cm81

10.64.110.213 Add/Edit Name or IP

Name or IP Address	Status
10.64.110.213	In Use

Back

6.4. Create a TSAPI Link

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

The screenshot shows the 'TSAPI Links' management page. On the left is a sidebar with a tree view under 'AE Services' containing 'CVLAN', 'DLG', 'DMCC', 'SMS', 'TSAPI' (expanded), 'TSAPI Links' (selected), and 'TSAPI Properties'. The main content area is titled 'TSAPI Links' and contains a table with the following data:

Link	Switch Connection	Switch CTI Link #	ASAI Link Version	Security
<input checked="" type="radio"/> 1	cm81	1	10	Both

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 “cm81” 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 5.13**)
- **ASAI Link Version:** Select “10” from the drop-down box.
- **Security:** Select “Both” from the drop-down box

Click on the **Apply Changes** button.

The screenshot shows the 'Edit TSAPI Links' window. The left sidebar is identical to the previous screenshot. The main content area is titled 'Edit TSAPI Links' and contains the following fields:

- Link: 1
- Switch Connection: cm81 (dropdown)
- Switch CTI Link Number: 1 (dropdown)
- ASAI Link Version: 10 (dropdown)
- Security: Both (dropdown)

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

6.5. Create CTI User

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

- **User Id:** Enter an informative name (i.e. trio). This ID is required for the Trio Enterprise installation
- **Common Name:** Enter a Common Name (i.e. trio)
- **Surname:** Enter a Surname (i.e. trio)
- **User Password:** Enter a password. This password is being required for the Trio Enterprise Installation
- **Confirm Password:** Confirm the password
- **CT User:** Select “Yes” from the drop-down box

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

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

▶ AE Services

▶ Communication Manager Interface

▶ High Availability

▶ Licensing

▶ Maintenance

▶ Networking

▶ Security

▶ Status

▼ **User Management**

▶ Service Admin

▼ **User Admin**

▪ **Add User**

▪ Change User Password

▪ List All Users

▪ Modify Default Users

▪ Search Users

▶ Utilities

▶ Help

Add User

Fields marked with * can not be empty.

* User Id

trio

* Common Name

trio

* Surname

trio

* User Password

••••••••

* Confirm Password

••••••••

Admin Note

Avaya Role

None ▼

Business Category

Car License

CM Home

Css Home

CT User

Yes ▼

Department Number

Display Name

Employee Number

Employee Type

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

CTI Users

User ID	Common Name	Worktop Name	Device ID
<input type="radio"/> calabrio	calabrio	NONE	NONE
<input type="radio"/> interop	interop	NONE	NONE
<input type="radio"/> intradiem	intradiem	NONE	NONE
<input type="radio"/> intranext	intranext	NONE	NONE
<input type="radio"/> rtirdrouter1	rtirdrouter1	NONE	NONE
<input type="radio"/> rtirouter1	rtirouter1	NONE	NONE
<input type="radio"/> rtitele1	rtitele1	NONE	NONE
<input checked="" type="radio"/> trio	trio	NONE	NONE

EditList 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 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

Edit CTI User

User Profile:

User ID

trio

Common Name

trio

Worktop Name

NONE ▾

Unrestricted Access

☒

Call and Device Control:

Call Origination/Termination and Device Status

None ▾

Call and Device Monitoring:

Device Monitoring

None ▾

Calls On A Device Monitoring

None ▾

Call Monitoring

☐

Routing Control:

Allow Routing on Listed Devices

None ▾

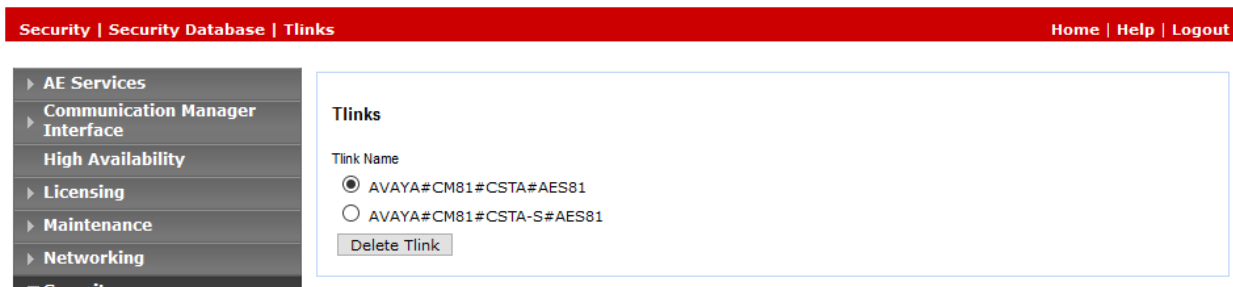
Apply Changes

Cancel Changes

6.7. Obtain Tlink Name

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

In this case, the associated Tlink name is “AVAYA#CM81#CSTA#AES81”. Note the use of the switch connection “cm81” from **Section 6.3** as part of the Tlink name.



The screenshot shows the 'Tlinks' configuration page. On the left is a navigation pane with a tree structure containing 'AE Services', 'Communication Manager Interface', 'High Availability', 'Licensing', 'Maintenance', 'Networking', and 'Security'. The 'Security' item is expanded, showing 'Security Database' and 'Tlinks'. The 'Tlinks' item is selected. The main content area is titled 'Tlinks' and contains a 'Tlink Name' section with two radio button options: 'AVAYA#CM81#CSTA#AES81' (which is selected) and 'AVAYA#CM81#CSTA-S#AES81'. Below these options is a 'Delete Tlink' button. At the top of the page is a red header bar with the text 'Security | Security Database | Tlinks' on the left and 'Home | Help | Logout' on the right.

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 | PortsHome | Help | Logout

▶ AE Services

▶ Communication Manager Interface

High Availability

▶ Licensing

▶ Maintenance

▼ **Networking**

AE Service IP (Local IP)

Network Configure

Ports

TCP/TLS Settings

▶ Security

Ports

CVLAN Ports

Unencrypted TCP Port9999

Enabled Disabled

Encrypted TCP Port9998

Enabled Disabled

DLG Port

TCP Port

5678

TSAPI Ports

TSAPI Service Port450

Local TLINK Ports

TCP Port Min1024

TCP Port Max1039

Unencrypted TLINK Ports

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.

The screenshot shows a web interface with a red header bar containing 'Maintenance | Service Controller' and 'Home | Help | Logout'. On the left is a navigation menu with categories like AE Services, Communication Manager Interface, High Availability, Licensing, Maintenance (selected), Date Time/NTP Server, Security Database, Service Controller (highlighted), Server Data, Networking, Security, and Status. The main content area is titled 'Service Controller' and contains a table with two columns: 'Service' and 'Controller Status'. The table lists several services, with 'TSAPI Service' checked and its status 'Running'. Below the table is a link 'Status and Control' and a row of buttons: 'Start', 'Stop', 'Restart Service', 'Restart AE Server', 'Restart Linux', and 'Restart Web Server'.

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

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

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

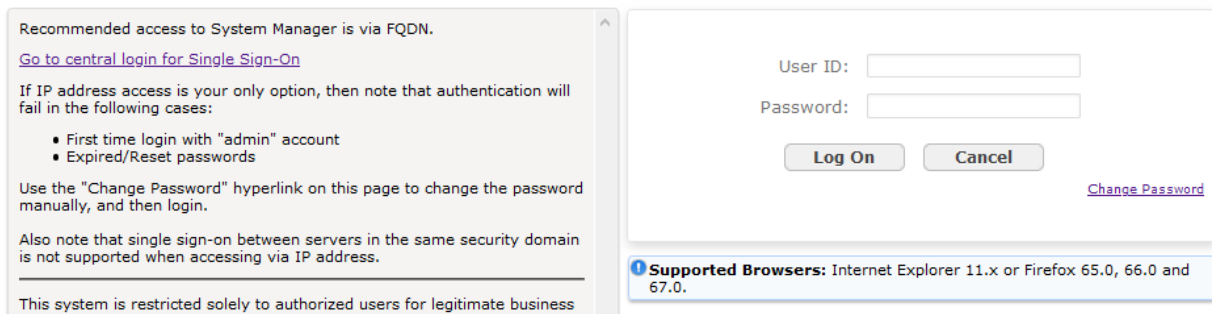
7. Configure Avaya Aura® Session Manager

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/SMGR” in an Internet browser window, where “ip-address” is the IP address of System Manager. Log in using the appropriate credentials.



Recommended access to System Manager is via FQDN.

[Go to central login for Single Sign-On](#)

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

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

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

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

This system is restricted solely to authorized users for legitimate business purposes only. The actual system restrictions may vary.

User ID:

Password:

[Change Password](#)

Supported Browsers: Internet Explorer 11.x or Firefox 65.0, 66.0 and 67.0.

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 to add a new domain.



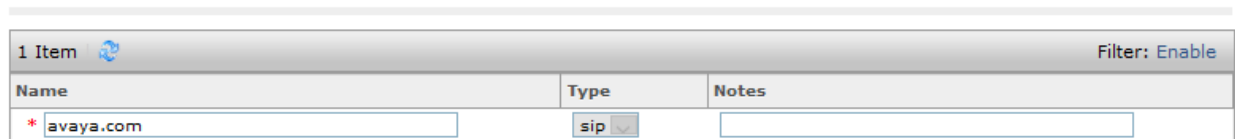
The screenshot shows the 'Domain Management' interface. On the left is a navigation pane with 'Routing' selected, and 'Domains' highlighted. The main area has a title 'Domain Management' and a 'Help ?' link. Below the title are buttons: 'New', 'Edit', 'Delete', 'Duplicate', and 'More Actions'. A table shows '1 Item' with a refresh icon and a 'Filter: Enable' link. The table has columns 'Name', 'Type', and 'Notes'. One row is visible with 'Name' 'avaya.com', 'Type' 'sip', and an empty 'Notes' field. At the bottom, it says 'Select : All, None'.

Name	Type	Notes
avaya.com	sip	

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**.

Domain Management

Commit Cancel



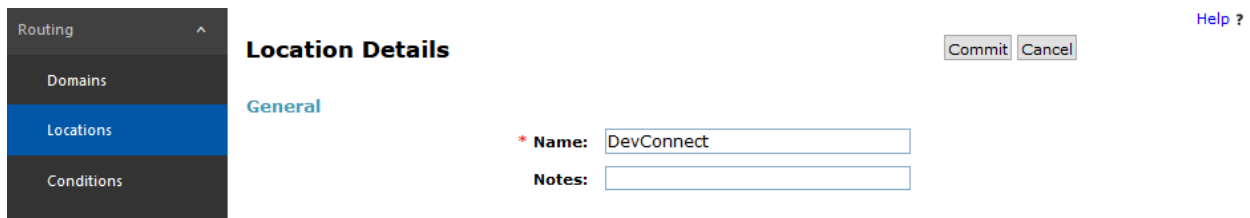
This screenshot shows the 'Domain Management' form. It has a table with '1 Item' and a 'Filter: Enable' link. The table has columns 'Name', 'Type', and 'Notes'. The 'Name' field contains 'avaya.com' with a red asterisk indicating a required field. The 'Type' field is a dropdown menu with 'sip' selected. The 'Notes' field is empty. At the bottom, there are 'Commit' and 'Cancel' buttons.

Name	Type	Notes
* avaya.com	sip	

7.3. Administer Locations

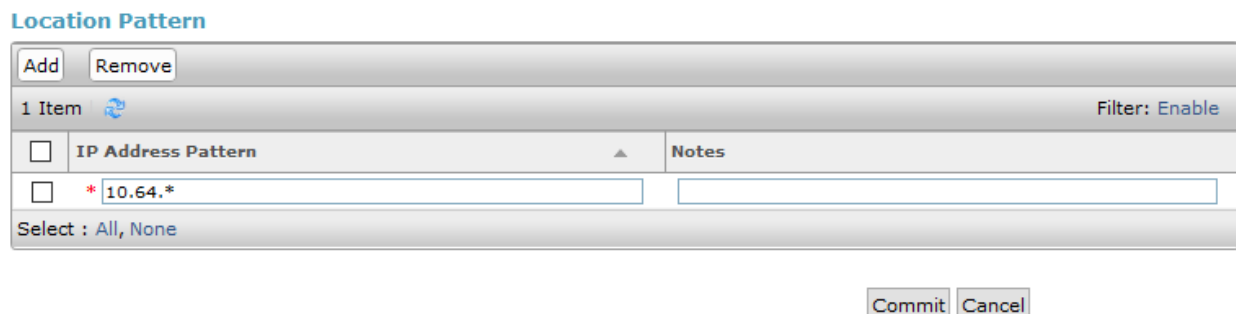
Select **Routing** → **Locations** from the left pane and click **New** in the subsequent screen (not shown) to add a new location for Trio Enterprise.

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.



The screenshot shows the 'Location Details' screen with the 'General' sub-section selected. On the left is a navigation pane with 'Routing', 'Domains', 'Locations' (highlighted), and 'Conditions'. The main area has a 'Name' field with the value 'DevConnect' and an empty 'Notes' field. At the top right are 'Commit' and 'Cancel' buttons, and a 'Help ?' link.

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.



The screenshot shows the 'Location Pattern' sub-section. It has an 'Add' button and a 'Remove' button. Below them is a table with one item. The table has columns for 'IP Address Pattern' and 'Notes'. The 'IP Address Pattern' column contains the value '* 10.64.*'. At the bottom right are 'Commit' and 'Cancel' buttons.

IP Address Pattern	Notes
* 10.64.*	

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.: avaya.com
iosrcd	Enter the domain name of system, e.g.: avaya.com
odstd	Enter IP address of Trio Enterprise SIP Server, e.g.: 10.64.10.112
osrcd	Enter IP address of Session Manager Server, e.g.: 10.64.110.212

Once the correct information is entered click the **Commit** button. Below is the screenshot showing the Adaptation created for Trio Enterprise. Select next to see the 2nd page to view rest of the adaptations.

Routing ^

- Domains
- Locations
- Conditions
- Adaptations ^
- Adaptations**
- Regular Expressio...
- SIP Entities
- Entity Links
- Time Ranges
- Routing Policies

Adaptation Details

[Help ?](#)

[Commit](#) [Cancel](#)

General

* **Adaptation Name:**

* **Module Name:**

Module Parameter Type:

	Name	Value
<input type="checkbox"/>	fromto	true
<input type="checkbox"/>	iodstd	avaya.com
<input type="checkbox"/>	iosrcd	avaya.com

Select : All, None

Page 1 of 2

7.5. Administer SIP Entities

Add two new SIP entities, one for Trio Enterprise and one for the new SIP trunk 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 Server.
- **Type:** “SIP Trunk”
- **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 Entity Details [Help ?](#)

General

* **Name:**

* **FQDN or IP Address:**

Type:

Notes:

Adaptation:

Location:

Time Zone:

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 “sm81”.
- **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: ☐

<input type="checkbox"/>	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy
<input type="checkbox"/>	* sm81_trio_5060_TCP	sm81	TCP	* 5060	trio	* 5060	trusted

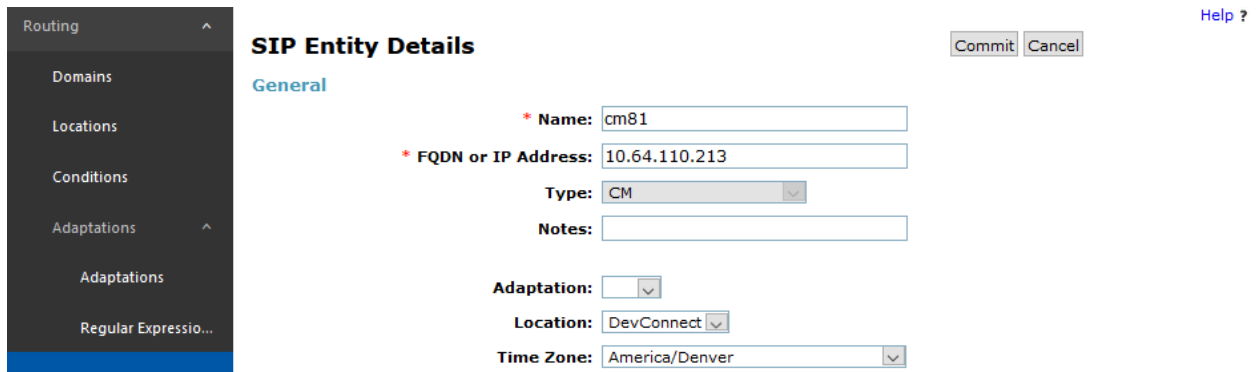
Select : All, None

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 C-LAN or the processor interface.
- **Type:** “CM”
- **Location:** Select the applicable location for Communication Manager.
- **Time Zone:** Select the applicable time zone.



The screenshot displays the 'SIP Entity Details' configuration screen. On the left is a dark sidebar menu with 'Routing' selected at the top, followed by 'Domains', 'Locations', 'Conditions', 'Adaptations', and 'Regular Expressio...'. The main area is titled 'SIP Entity Details' and has a 'General' tab selected. In the top right corner of the main area are 'Commit' and 'Cancel' buttons, and a 'Help ?' link. The form contains the following fields:

- Name:** A text input field containing 'cm81'.
- FQDN or IP Address:** A text input field containing '10.64.110.213'.
- Type:** A dropdown menu with 'CM' selected.
- Notes:** A text input field.
- Adaptation:** A dropdown menu.
- Location:** A dropdown menu with 'DevConnect' selected.
- Time Zone:** A dropdown menu with 'America/Denver' selected.

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 “sm81”.
- **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	
<input type="checkbox"/>	* sm81_cm81_5061_TLS	sm81	TLS	* 5061	cm81	* 5061	trusted	

Select : All, None

7.6. Administer Routing Policies

Add two new routing policies, one for Trio Enterprise and one for the new SIP trunk 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.

Routing Policy Details [Help ?](#)

General

* **Name:**

Disabled: ☐

* **Retries:**

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
trio	10.64.10.112	SIP Trunk	

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.

Routing Policy Details [Help ?](#)

General

* **Name:**

Disabled: ☐

* **Retries:**

Notes:

SIP Entity as Destination

Name	FQDN or IP Address	Type	Notes
cm81	10.64.110.213	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 “51”.
- **Min:** The minimum number of digits to match.
- **Max:** The maximum number of digits to match.

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 “-ALL-”. The Trio Enterprise routing policy from **Section 7.6.1** was selected as shown below.

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

General

* **Pattern:**

* **Min:**

* **Max:**

Emergency Call: ☐

SIP Domain:

Notes:

Originating Locations and Routing Policies

Add Remove

1 Item [Filter: Enable](#)

<input type="checkbox"/>	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	-ALL-		trio	0	<input type="checkbox"/>	trio	

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 “7” and “9”.
- **Min:** The minimum number of digits to match.
- **Max:** The maximum number of digits to match.

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 “-ALL-”. The Communication Manager routing policy from **Section 7.6.2** was selected as shown below.

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

General

* **Pattern:**

* **Min:**

* **Max:**

Emergency Call: ☐

SIP Domain:

Notes:

Originating Locations and Routing Policies

Add Remove

1 Item [Filter: Enable](#)

<input type="checkbox"/>	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	-ALL-		cm81	0	<input type="checkbox"/>	cm81	

Select : All, None

Dial Pattern Details

Commit Cancel

Help ?

General

* Pattern: 9

* Min: 11

* Max: 12

Emergency Call:

SIP Domain: -ALL-

Notes:

Originating Locations and Routing Policies

Add Remove							
1 Item		Filter: Enable					
<input type="checkbox"/>	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	-ALL-		cm81	0	<input type="checkbox"/>	cm81	
Select : All, None							

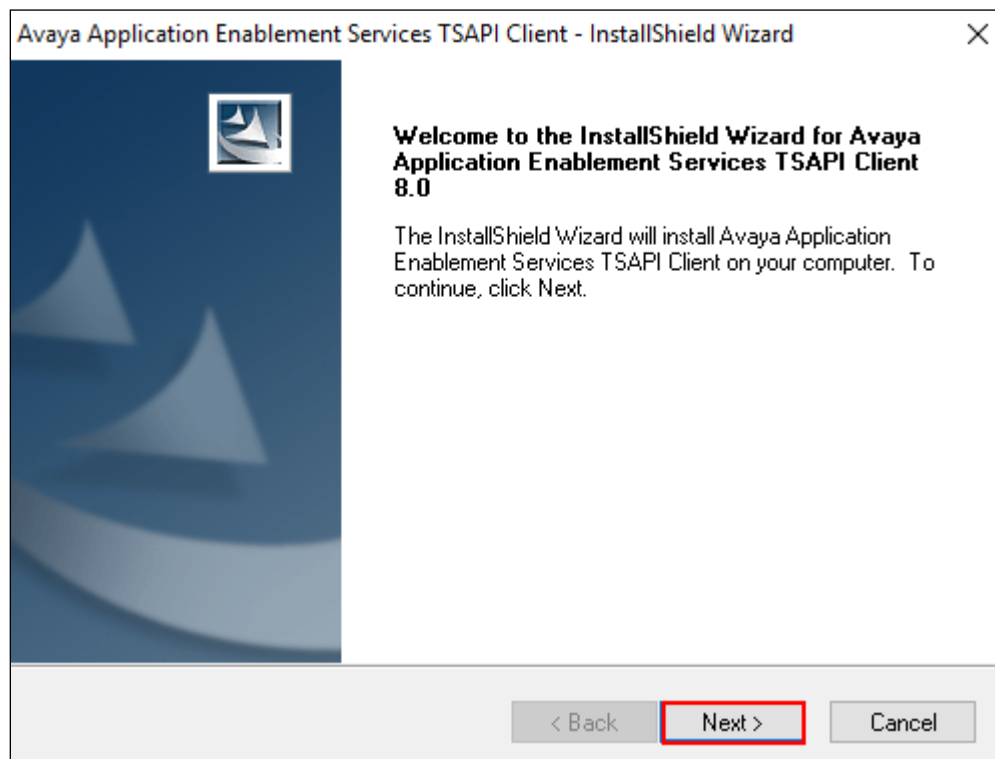
8. Configure Trio Enterprise from Enghouse Interactive AB

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 running. The steps to configure SIP Trunks are as follows:

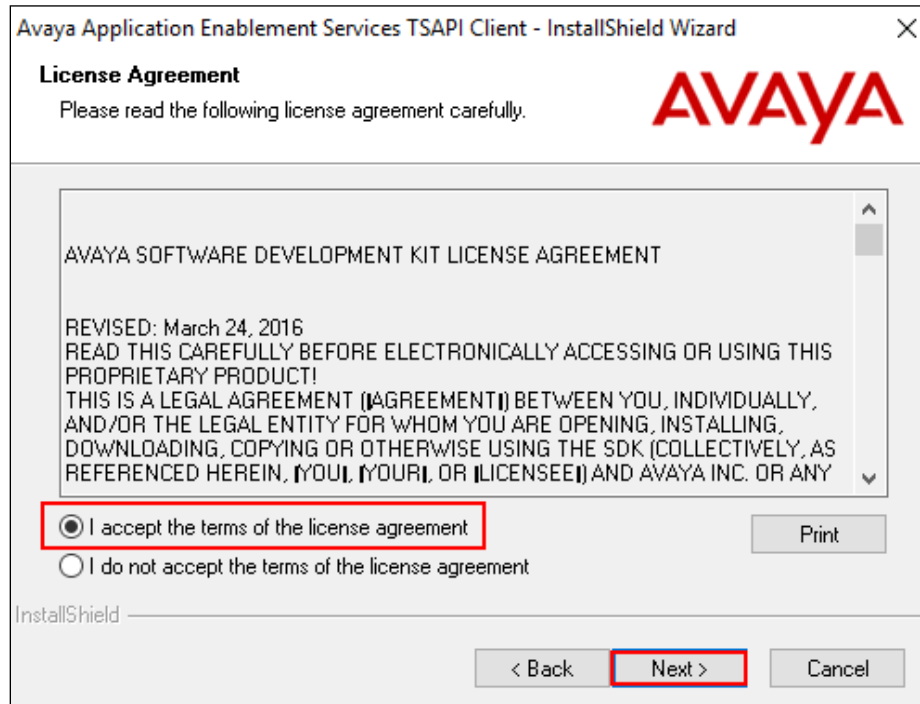
- Install Avaya Application Enablement Services TSAPI Client
- Configure Trio Enterprise to use SIP Trunks
- Configure Absence
- Configure Trio Enterprise Attendant

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.

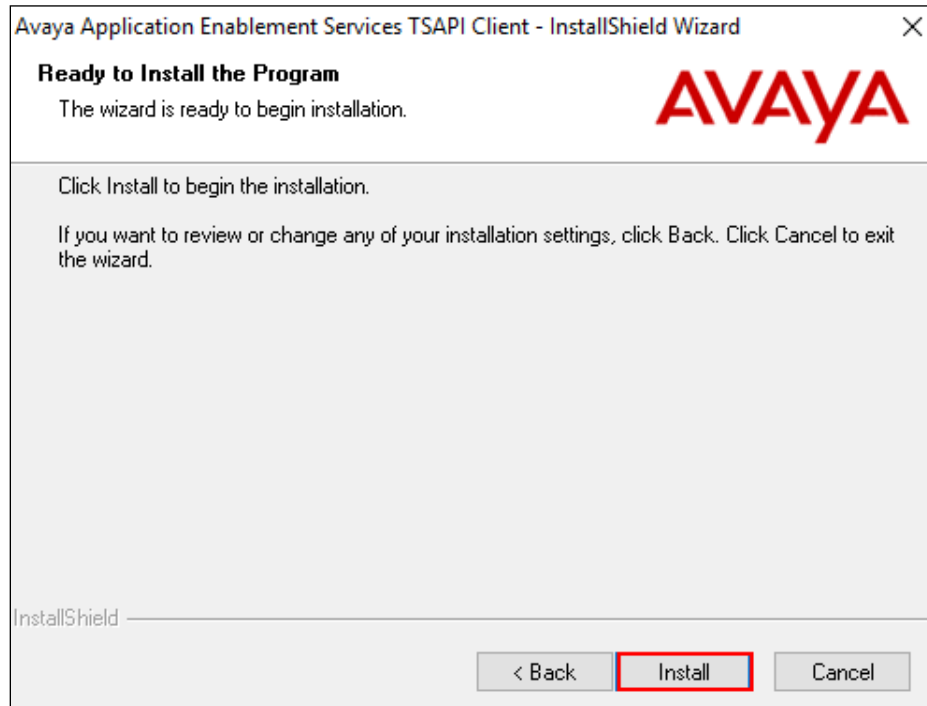
Host Name or IP Address: Port Number:

Configured AE Services Servers:

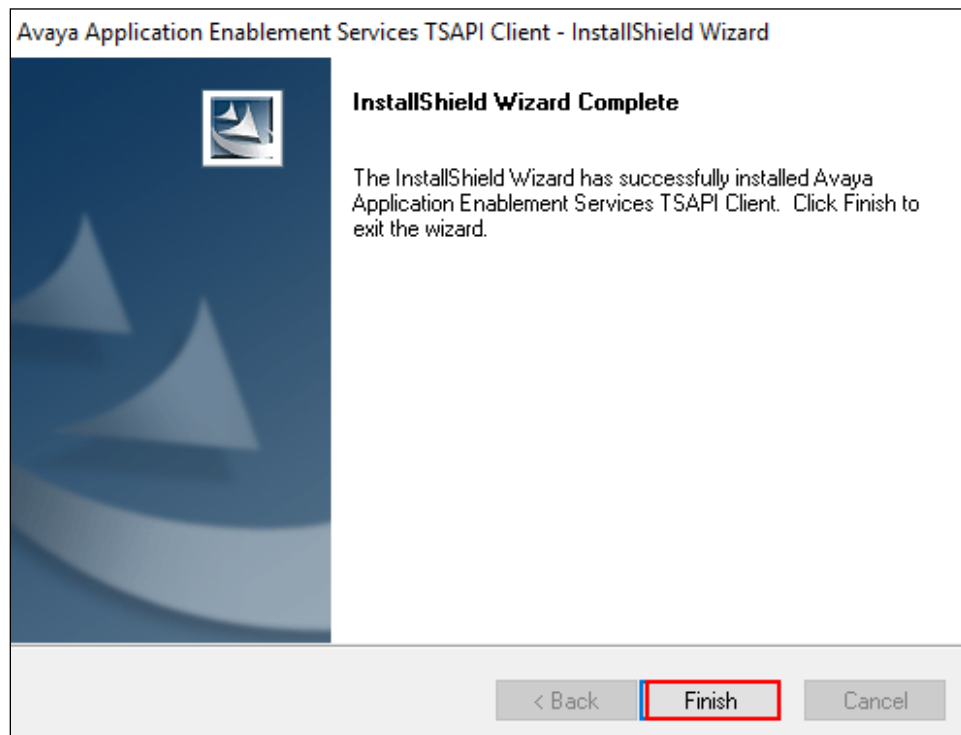
InstallShield

< Back **Next >** Cancel

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



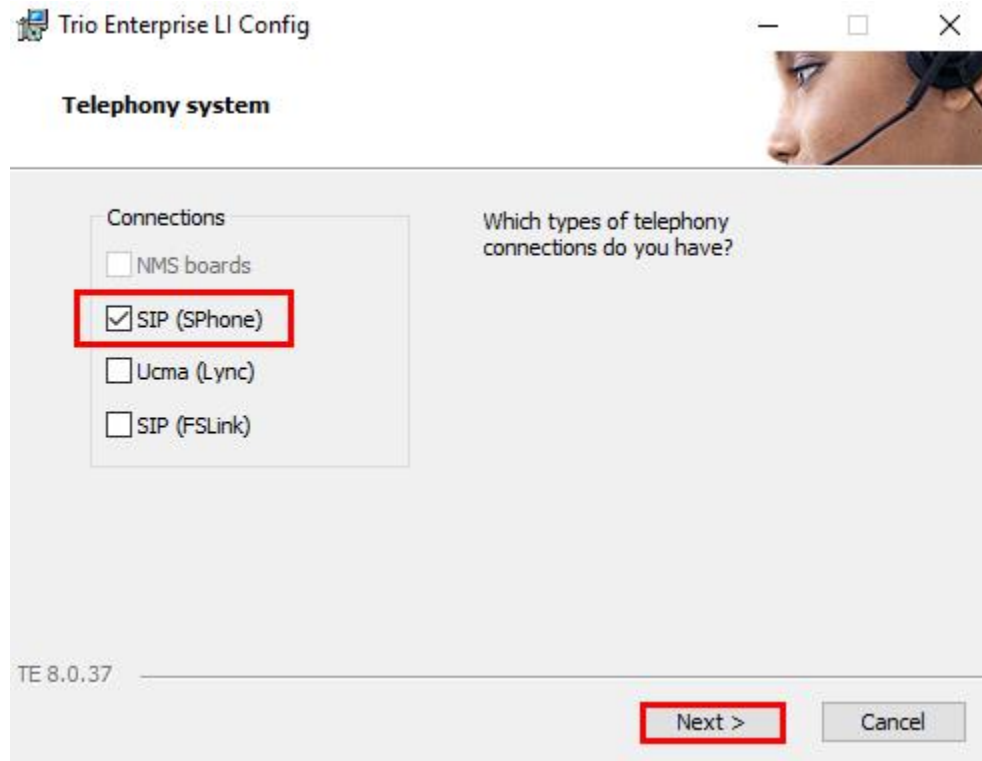
When the **InstallShield Wizard Complete** window appears click on the **Finish** button.



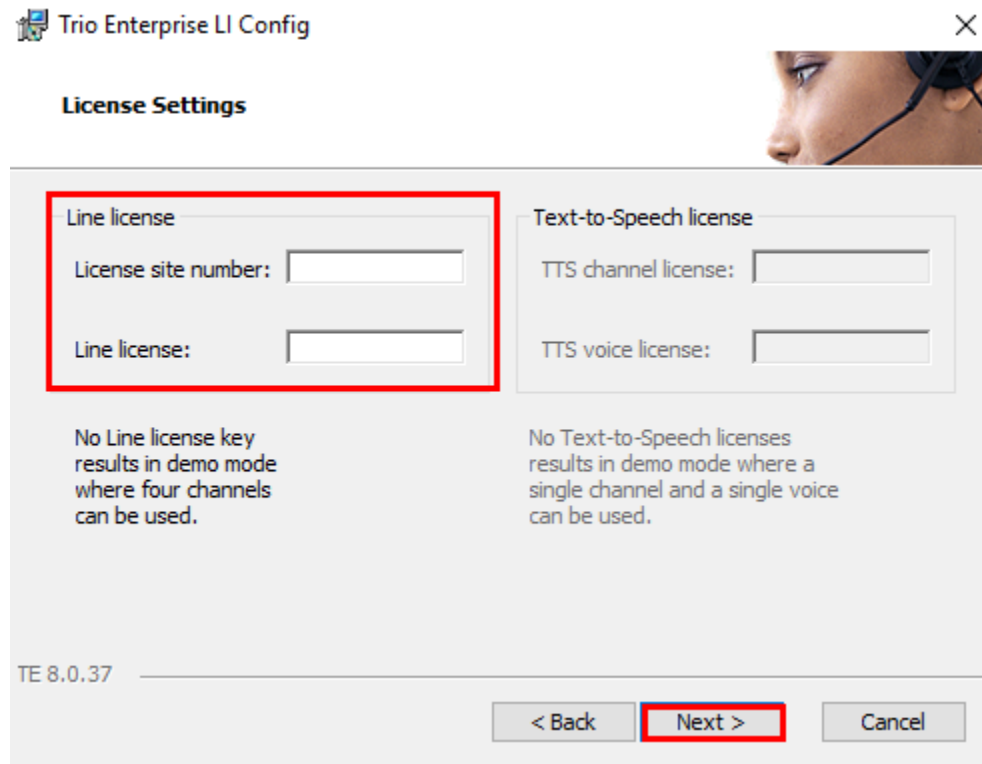
8.2. Configure Trio Enterprise to use SIP Trunk

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 8.0.37

< Back Next > Cancel

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

Trio Enterprise LI Config

SPhone Settings(1)

Select which PABX this SIP trunk will be connected to. If you don't know, select GENERIC and later modify the configuration in televoice.cfg.

☒ GENERIC ☐ LUCENT

☐ MD 110/MX-ONE ☐ SIEMENS

☐ TELE2 Business trunk ☐ CISCO

☐ Nortel CS1000/Meridian ☐ PSTN

☐ ALCATEL 4200 ☐ PHILIPS

☐ ALCATEL 4300

☐ ALCATEL 4400

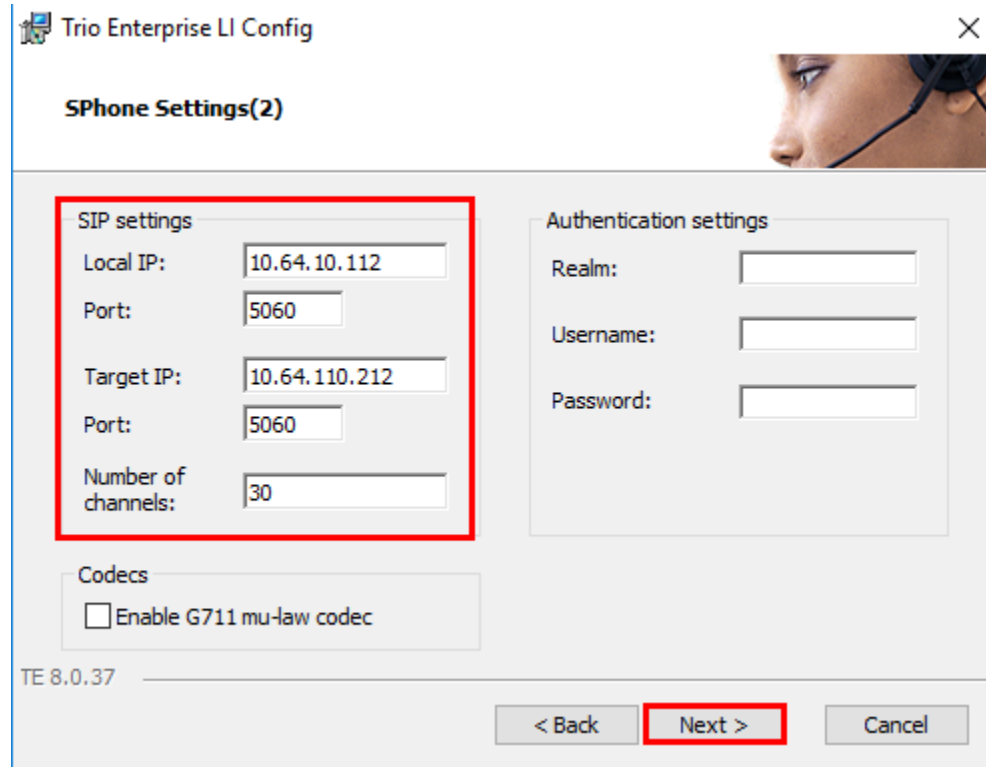
TE 8.0.37

< Back Next > Cancel

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 Session Manager
- **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. The 'Authentication settings' section is also visible. The 'Codecs' section has an unchecked checkbox for 'Enable G711 mu-law codec'. The version 'TE 8.0.37' is displayed at the bottom left. The 'Next >' button is highlighted with a red box.

SIP settings	
Local IP:	10.64.10.112
Port:	5060
Target IP:	10.64.110.212
Port:	5060
Number of channels:	30

Authentication settings	
Realm:	
Username:	
Password:	

Codecs

☐ Enable G711 mu-law codec

TE 8.0.37

< Back **Next >** 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 8.0.37

Additional SIP Trunk

< Back

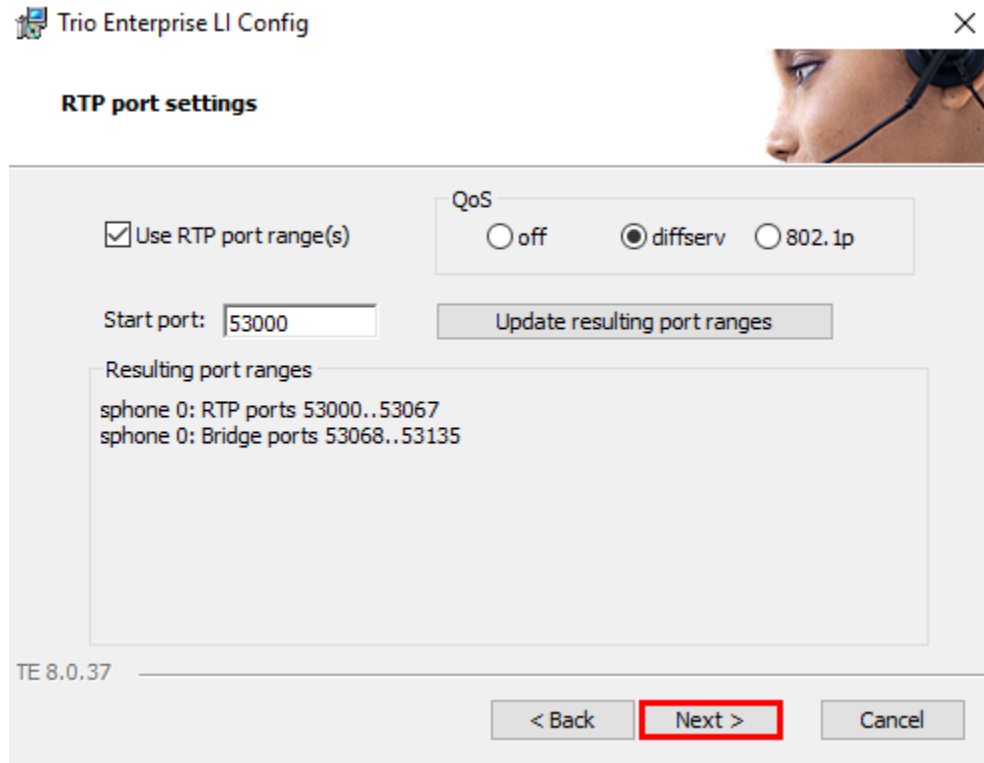
Next >

Cancel

In the subsequent window enter the following settings:

- **Use RPT port range(s):** Check the box
- **QoS:** Select “diffserv”
- **Start port:** Enter “53000”

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



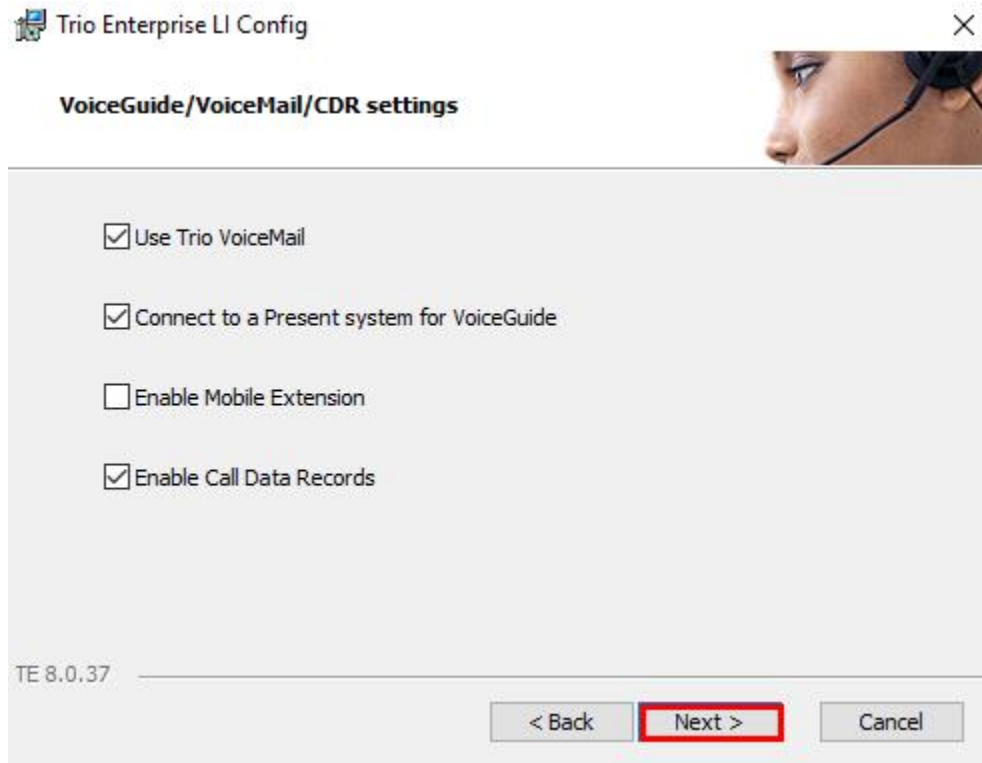
The screenshot shows the 'RTP port settings' window in the Trio Enterprise LI Config application. The window has a title bar with the application name and a close button. The main content area is titled 'RTP port settings' and contains the following elements:

- A checkbox labeled 'Use RTP port range(s)' which is checked.
- A 'QoS' section with three radio buttons: 'off', 'diffserv' (which is selected), and '802.1p'.
- A 'Start port' text box containing the value '53000'.
- An 'Update resulting port ranges' button.
- A 'Resulting port ranges' section with a text area displaying:
 - sphone 0: RTP ports 53000..53067
 - sphone 0: Bridge ports 53068..53135
- A status bar at the bottom left showing 'TE 8.0.37'.
- A navigation bar at the bottom right with three buttons: '< Back', 'Next >' (which is highlighted with a red border), and 'Cancel'.

In the subsequent window enter the following settings:

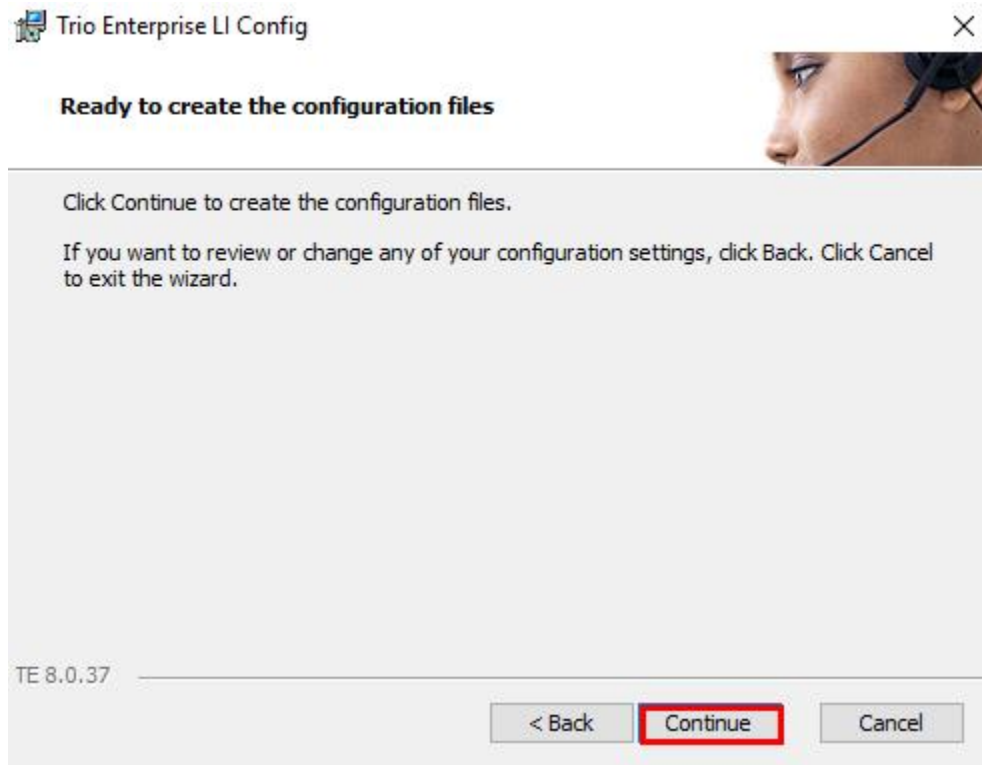
- **Use Trio VoiceMail:** Check the box.
- **Connect to a Present system for VoiceGuide:** Check the box.
- **Enable Call Data Records:** Check the box.

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

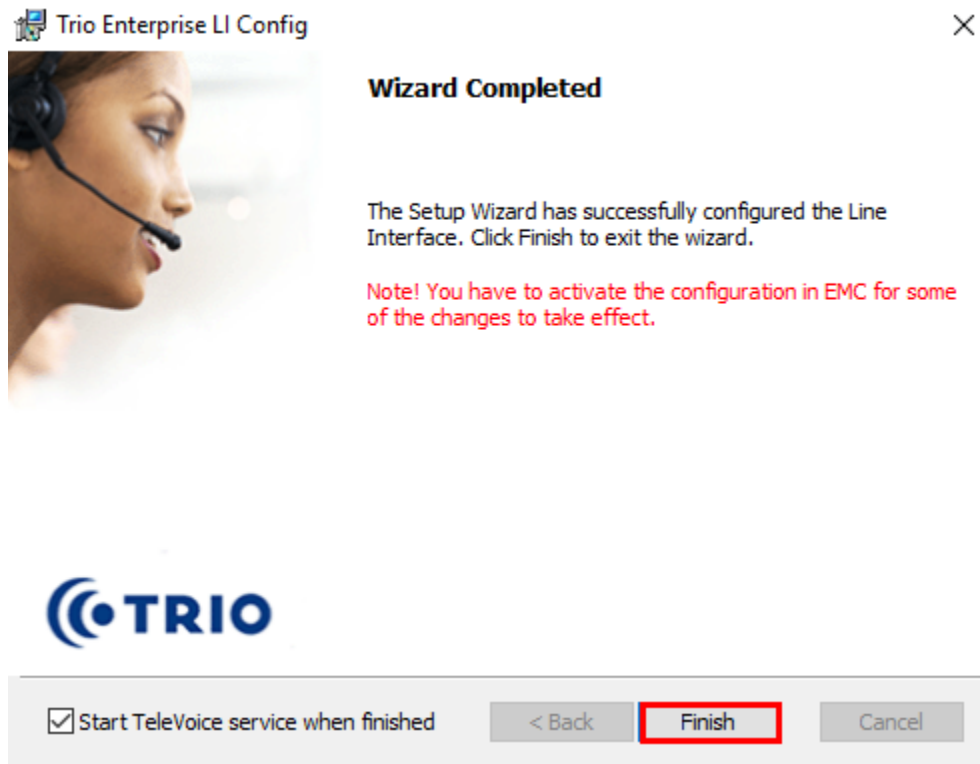


The screenshot shows a window titled "Trio Enterprise LI Config" with a close button (X) in the top right corner. Below the title bar, the text "VoiceGuide/VoiceMail/CDR settings" is displayed. The main area contains four checkboxes: "Use Trio VoiceMail" (checked), "Connect to a Present system for VoiceGuide" (checked), "Enable Mobile Extension" (unchecked), and "Enable Call Data Records" (checked). At the bottom left, the version "TE 8.0.37" is shown. At the bottom right, there are three buttons: "< Back", "Next >" (highlighted with a red border), and "Cancel". A small image of a person wearing a headset is visible on the right side of the window.

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

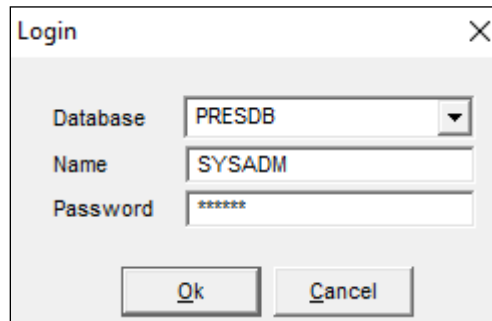
Access the template for televoice.cfg. This is typically found in \TE\ProgramData\LI\templates folder.

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
```

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 screenshot of a 'Login' dialog box. The dialog has a title bar with 'Login' and a close button (X). 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, there are two buttons: 'Ok' and 'Cancel'.

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

[illegible]

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 5.13.3**.
- **Referral destination:** Enter the number “851000” 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.

PBX

Type

- ☐ MXOne/MD110
- ☐ Nortel
- ☐ Alcatel
- ☐ Philips
- ☐ Cisco AXL
- ☐ Tapi Generic
- ☐ Telia Centrex
- ☒ Avaya CM
- ☐ Broadworks
- ☐ Alcatel Open Touch

PbxName: Avaya CM

Prefix:

CSTA server: AVAYA#CM81#CSTA#AES81

PBX login name: trio

PBX password: Interop123!

Reason code length: 1

Routing device: 78202

Referral destination: 851000

☒ Monitor line state for all extensions

Address Space: 1

Virtual

- ☐ MCX
- ☐ Microsoft Lync
- ☐ Telenor MB
- ☐ Generic Linestate
- ☐ MiCloud

OK Cancel

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. Start agent login by browsing to <https://<te server>/cc1/triowebagent>

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

Note this user ID and password is created during the user creation

Go to the setup tab:

- **Phone number:** Select the Communication Manager telephone number that will be used as the agent's audio device (number 70101 in this example).
- **Phone type:** Select "Standard phone" from the dropdown menu

Click on the **SAVE** button to save settings.

The screenshot displays the Trio Web Agent settings interface. The top navigation bar includes the 'Trio Web Agent' logo, a search bar, and a 'LOG OUT' button. The left sidebar shows the user's current status as 'Agent 70101', 'LOGGED OFF', and 'NORMAL'. Below this are icons for Search, Queue, Agents, and Services. The main content area is titled 'Settings' and features a 'Login' section. This section contains two dropdown menus: 'Phone type' set to 'Standard phone' and 'Location' set to 'Default'. The 'Phone number' field is populated with '70101'. There is also a toggle switch for 'Use Contact Center license' which is currently turned off. A 'SAVE' button is located at the bottom of the settings form.

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	10	no	aes81	established	15	15

9.2. Verify Avaya Aura® Session Manager

Log into System Manager. Under the **Elements** section, navigate to **Session Manager** → **System Status** → **SIP Entity Monitoring**.

Session Manager

Dashboard

Session Manager ...

Global Settings

Communication Pr...

Network Config... ▾

Device and Loca... ▾

Application Con... ▾

SIP Entity Link Monitoring Status Summary

This page provides a summary of Session Manager SIP entity link monitoring status.

SIP Entities Status for All Monitoring Session Manager Instances

Run Monitor As of 1:11 PM

1 Item Filter: Enable


	Session Manager	Type	Monitored Entities					
			Down	Partially Up	Up	Not Monitored	Deny	Total
<input type="checkbox"/>	sm81	Core	4	0	6	0	0	10

Select : All, None

Verify that the state of the Session Manager links to Communication Manager and Trio Enterprise by selecting the SIP Entity names.


SIP Entity, Entity Link Connection Status

This page displays detailed connection status for all entity links from all Session Manager instances to a single SIP entity.

Status Details for the selected Session Manager:									
All Entity Links to SIP Entity: trio									
Summary View									
1 Item  Filter: Enable									
	Session Manager Name	IP Address Family	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
<input type="radio"/>	sm81	IPv4	10.64.10.112	5060	TCP	FALSE	UP	200 OK	UP
Select : None									

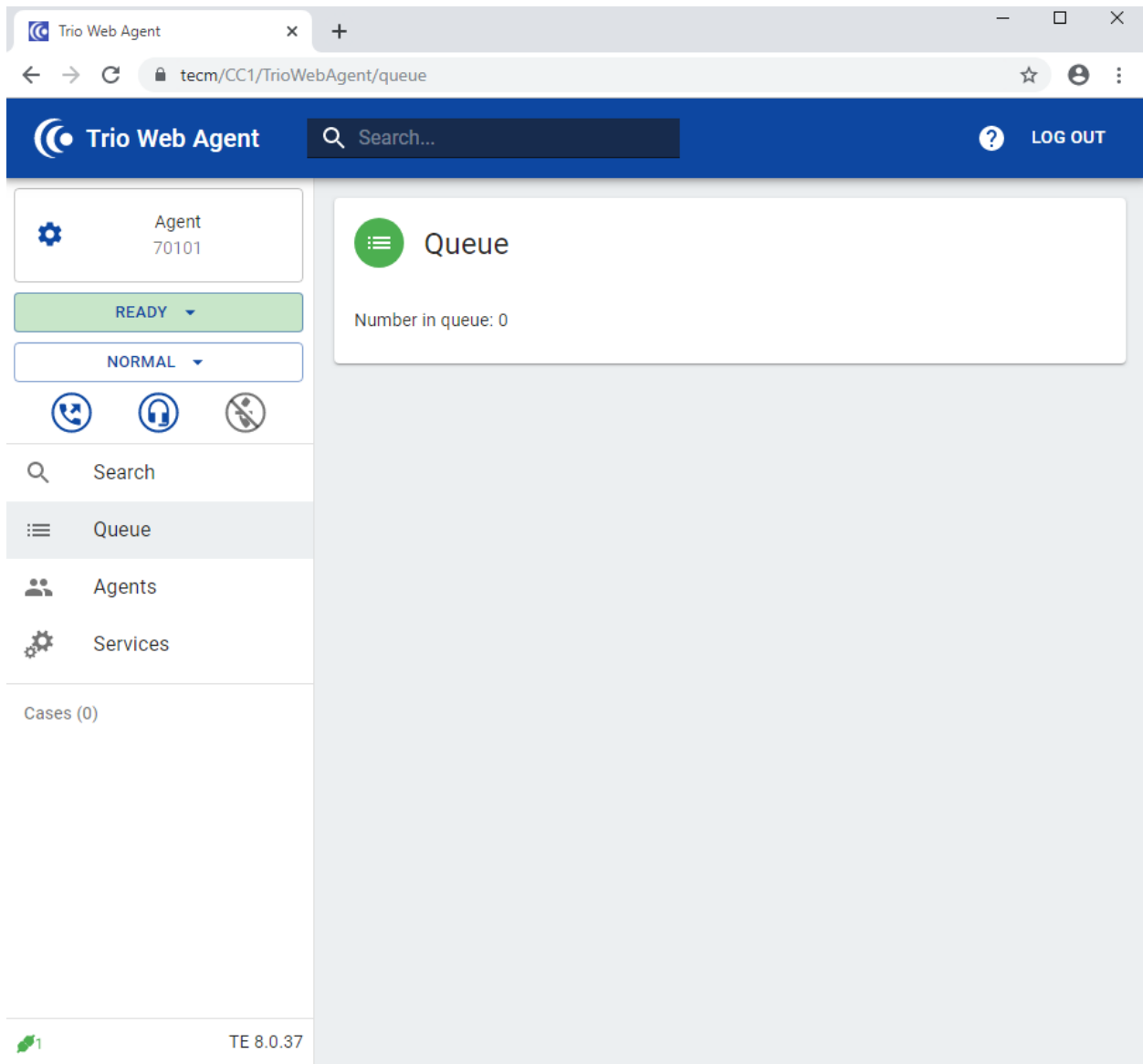
SIP Entity, Entity Link Connection Status

This page displays detailed connection status for all entity links from all Session Manager instances to a single SIP entity.

Status Details for the selected Session Manager:									
All Entity Links to SIP Entity: cm81									
Summary View									
1 Item  Filter: Enable									
	Session Manager Name	IP Address Family	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
<input type="radio"/>	sm81	IPv4	10.64.110.213	5061	TLS	FALSE	UP	200 OK	UP
Select : None									

9.3. Verify Trio Enterprise Attendant

To verify that Trio Enterprise is connected to Communication Manager via Session Manager, log into the Trio Enterprise Attendant at <https://<te server>/cc1/triowebagent>. 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 can be 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 noted 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] Administering Avaya Aura® Communication Manager, Release 8.1.x, Issue 4, November 2019.
- [2] Administering Avaya Aura® Application Enablement Services, Release 8.1.x, Issue 3, October 2019
- [3] Administering Avaya Aura® Session Manager, Release 8.1.1, Issue 2, October 2019

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

©2020 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.