Avaya Solution & Interoperability Test Lab

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

Abstract

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

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

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

1. Introduction

These Application Notes outline the steps necessary to configure Trio Enterprise from Enghouse Interactive AB to interoperate with Avaya Aura® Communication Manager R7.0 (Communication Manager), Avaya Aura® Session Manager R7.0 (Session Manager) and Avaya Aura® Application Enablement Services R7.0 (AES). Trio Enterprise is a client/server based application running on Windows Server operating system. 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 Communication Manager using a SIP trunk via the Session Manager. A TSAPI connection on AES enables the Trio Enterprise Absence integration. Trio Enterprise is supplied with all prerequisite software.

2. General Test Approach and Test Results

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

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

Note: During compliance testing an Avaya H.323 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.

2.1. Interoperability Compliance Testing

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

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

2.2. Test Results

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

- 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 has to be configured on the Trio Enterprise Server. Failing to do so, will cause Avaya SIP stations to not hear any pre-recorded audio from the attendant. Refer to **Sections 5.7** 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 AES. An Avaya H.323 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. Another SIP trunk on the Session Manager was configured to connect to the simulated PSTN.

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

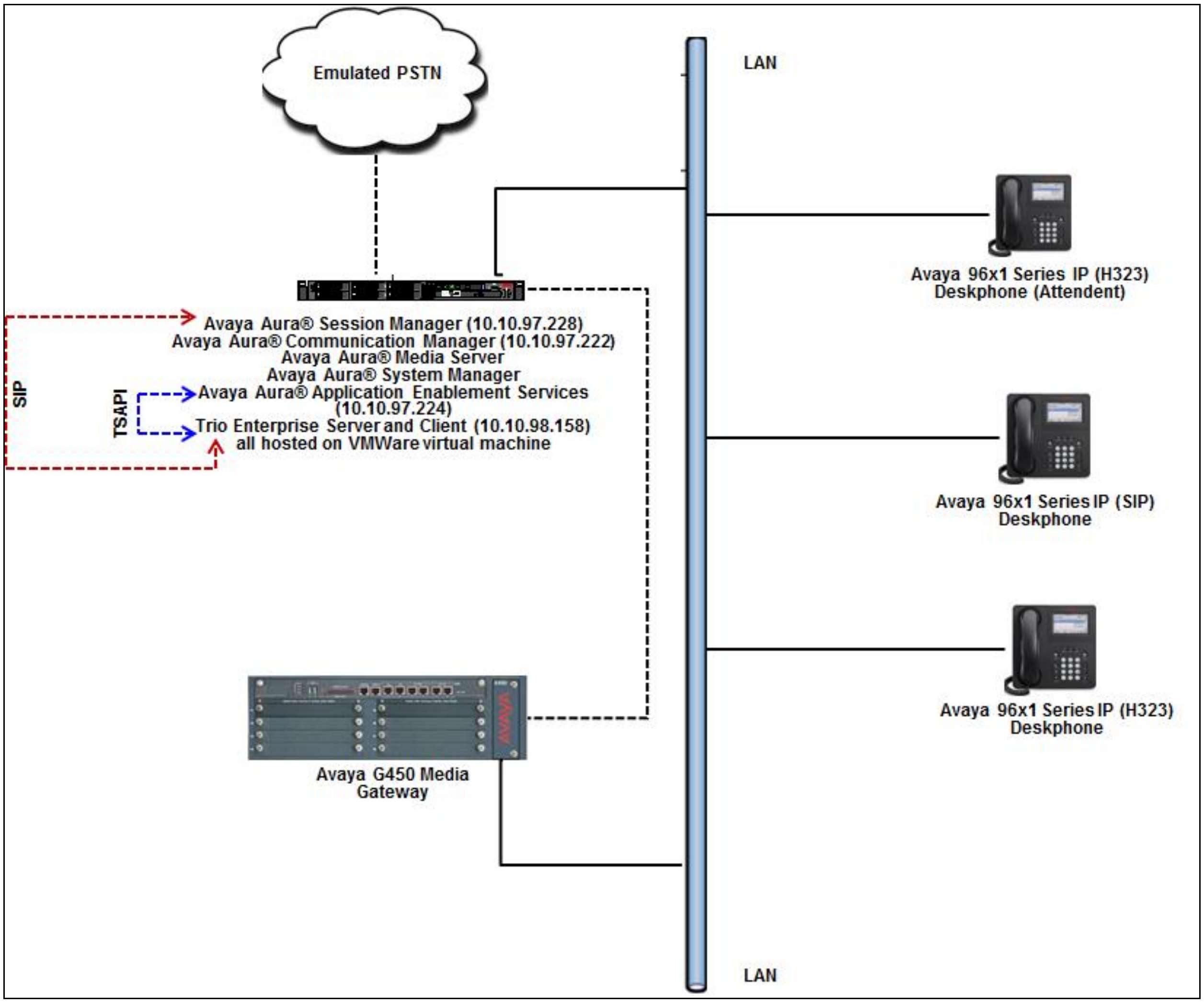


Figure 1: Avaya and Trio Enterprise Reference Configuration

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya Aura® Communication Manager running on virtualized environment	7.0.1.1.0-FP1SP1
Avaya Aura® Application Enablement Services running on virtualized environment	7.0.1.0.2.15-0
Avaya Aura® Session Manager running on virtualized environment	7.0.1.1.701114
Avaya Aura® System Manager	7.0.1.1 SP1
Avaya Aura® Media Server	7.7.0.359
Avaya G450 Media Gateway	FW 37.19.0/1
Avaya 96x1 Series IP Telephone • 96x1 (H.323) • 96x1 (SIP)	 6.6229 7.0.1.1.5
Trio Enterprise Server and Client running on Microsoft Windows 2012 R2 Server	6.2

5. Configure Avaya Aura® Communication Manager

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

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

- Verify License
- Administer System Parameters Features
- Administer SIP trunk group
- Administer SIP signaling 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 Application Enablement Services Node
- 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: 4000  10
           Maximum Concurrently Registered IP Stations: 2400  7
             Maximum Administered Remote Office Trunks: 4000  0
Maximum Concurrently Registered Remote Office Stations: 2400  0
              Maximum Concurrently Registered IP eCons: 68    0
  Max Concur Registered Unauthenticated H.323 Stations: 100   0
                        Maximum Video Capable Stations: 2400  1
                   Maximum Video Capable IP Softphones: 2400  1
                       Maximum Administered SIP Trunks: 4000  24
  Maximum Administered Ad-hoc Video Conferencing Ports: 4000  0
   Maximum Number of DS1 Boards with Echo Cancellation: 80    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? n                       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



    DTMF Tone Feedback Signal to VRU - Connection:          Disconnection:n
```

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.

```
display system-parameters features                              Page  13 of  19
                        FEATURE-RELATED SYSTEM PARAMETERS
 CALL CENTER MISCELLANEOUS
           Callr-info Display Timer (sec): 10
                         Clear Callr-info: next-call
        Allow Ringer-off with Auto-Answer? n

    Reporting for PC Non-Predictive Calls? n

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

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

5.3. Administer 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
 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
```

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
                                                UUI Treatment: shared
                                              Maximum Size of UUI Contents: 128
                                                 Replace Restricted Numbers? n
                                                Replace Unavailable Numbers? n

                                                  Hold/Unhold Notifications? y
                                Modify Tandem Calling Number: no
```

5.4. Administer SIP Signaling Group

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

- **Group Type:** "sip"
- **Transport Method:** "tcp"
- **Near-end Node Name:** An existing C-LAN node name or "procr"
- **Far-end Node Name:** The existing node name for Session Manager
- **Near-end Listen Port:** An available port for integration with 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"

```
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? n
H.323 Station Outgoing Direct Media? n              Alternate Route Timer(sec): 6
```

5.5. Administer SIP Trunk Group Members

Use the "change trunk-group n" command, where "n" is the trunk group number from **Section 5.3**. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Signaling Group:** The signaling group number from **Section 5.4**.
- **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
```

5.6. Administer IP Network Region

Use the “change ip-network-region n” command, where “n” is the existing far-end network region number used by the SIP signaling group from **Section 5.4**.

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
```

5.7. Administer IP Codec Set

Use the “change ip-codec-set n” command, where “n” is the codec set number from **Section 5.6**. 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                                          Page   1 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: G.722-64K                     2         20
 3: G.729              n          2         20
 4: G.711A             n          2         20
```

5.8. 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 5.3**.
- **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
```

5.9. 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 5.3**. 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
```

5.10. 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                                           Page   1 of  12
                             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
```

5.11. Administer Uniform Dial Plan

This section provides a sample AAR routing used for routing calls with dialed 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                                           Page   1 of   2
                       UNIFORM DIAL PLAN TABLE
                                                              Percent Full: 0

  Matching                    Insert             Node
  Pattern          Len Del    Digits      Net Conv Num
 71                 5   0                 aar  n
```

5.12. 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 5.8**.

```
change aar analysis 0                                          Page   1 of   2
                             AAR DIGIT ANALYSIS TABLE
                                   Location: all            Percent Full: 2

          Dialed            Total      Route     Call   Node  ANI
          String          Min  Max  Pattern    Type   Num   Reqd
        71                   5    5      1         aar          n
```

5.13. Configure Avaya Aura® Application Enablement Services Node

A Node Name needs to be created to associate the Communication Manager with AES. Use the "change node-names ip" command and enter an informative name (i.e. **devvmaes**) and the IP address of the AES (10.10.97.224)

```
change node-names ip
                                                                  IP NODE NAMES
    Name                 IP Address
DevvmAMS               10.10.97.232
GW-G450                10.10.97.223
SM-VM                  10.10.97.228
devvmaes               10.10.97.224
procr                  10.10.97.222
```

5.14. Configure interface to Avaya Aura® Application Enablement Services

To configure the AES link use the "change ip-services" command and enter the following:
Page 1

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

```
change ip-services                                              Page   1 of   4

                                   IP SERVICES
 Service      Enabled      Local        Local        Remote       Remote
  Type                     Node         Port         Node         Port
AESVCS          y        procr          8765
```

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

- **Server ID** Enter **1**
- **AE Services** Enter **devvmaes** (The node created in **Section 5.13**)
- **Password** Enter a password. This password will be used in **Section 6.3** to enable the AES to communicate with the Communication Manager.
- **Enabled** Enter **y**

```
change ip-services                                              Page   4 of   4
                            AE Services Administration

   Server ID    AE Services         Password           Enabled    Status
                     Server
      1:       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 AES. Use the **add cti-link next** command and enter the following:

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

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

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

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 dialled by users to initiate a diversion for specific reasons. An absence diversion can be cancelled by dialing the VDN extension followed by # #. The following steps are needed to configure Absence diversions:

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

5.16.1. 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

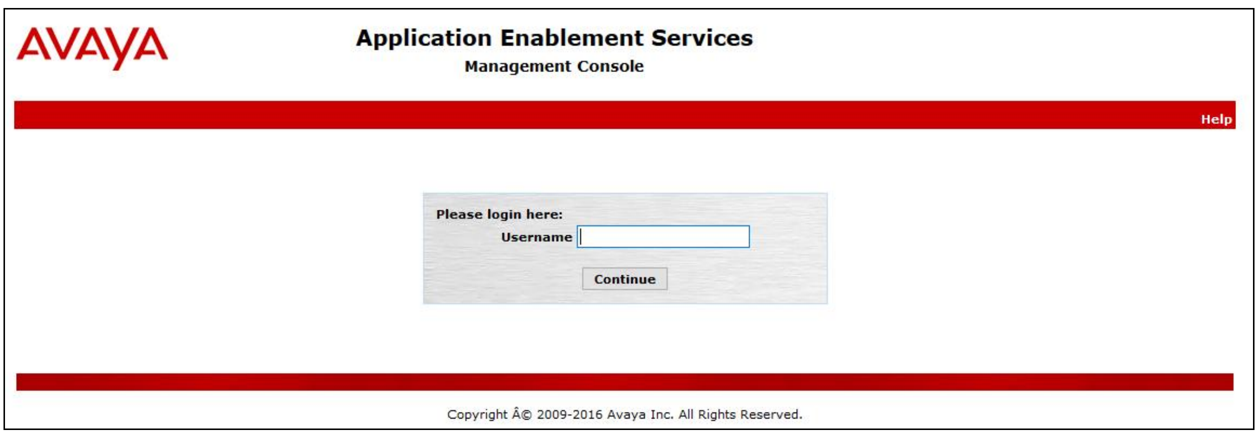
This section provides the procedures for configuring AES. It is implied a working AES is already in place and the Security Database (SDB) is configured. For all other provisioning information such as initial installation and configuration, please refer to the product documentation in **Section 11**.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

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

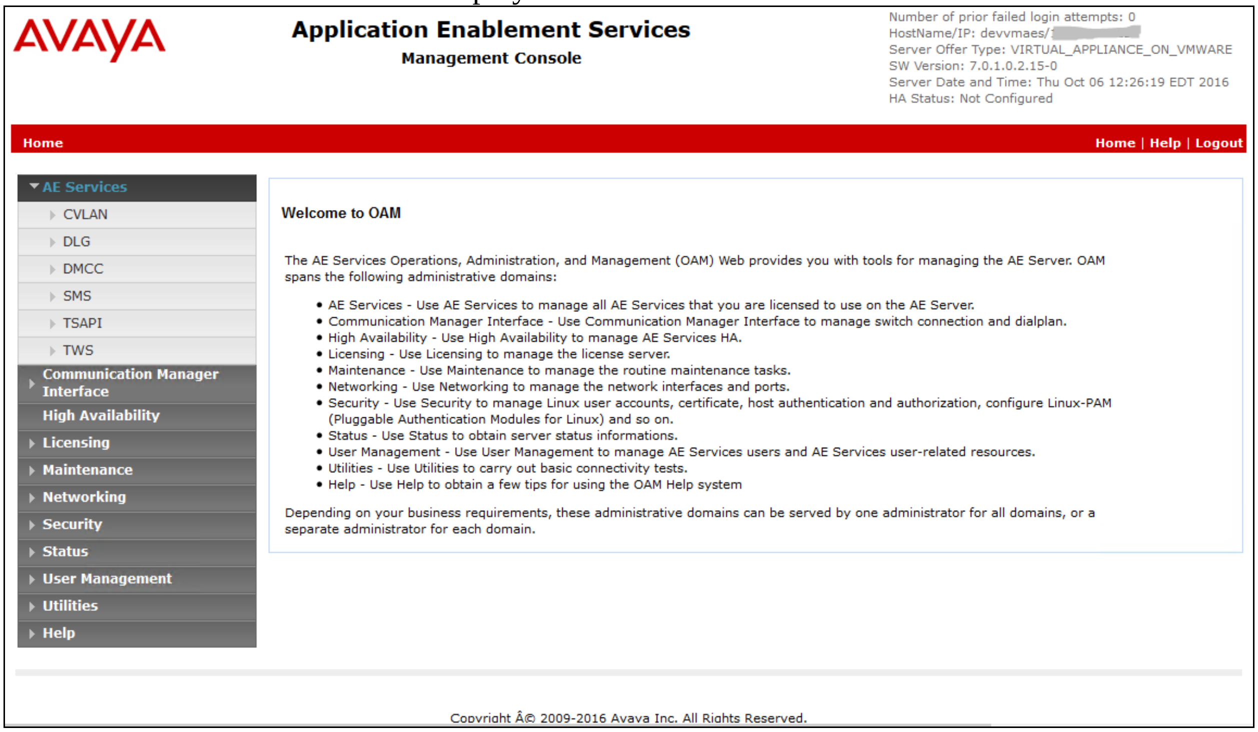
6.1. Logging into the Avaya Aura® Application Enablement Services

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

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

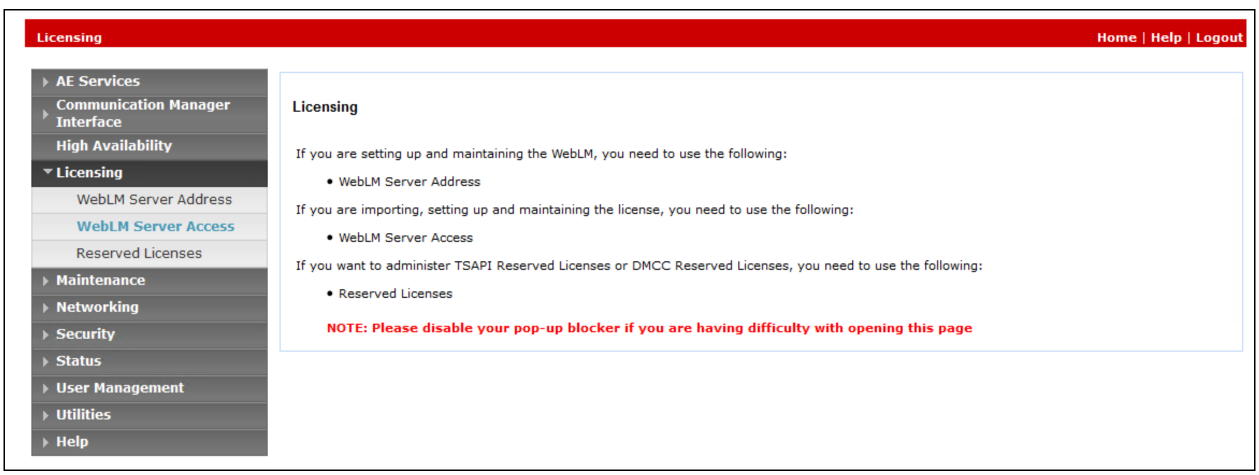


The **Welcome to OAM** screen is displayed next.



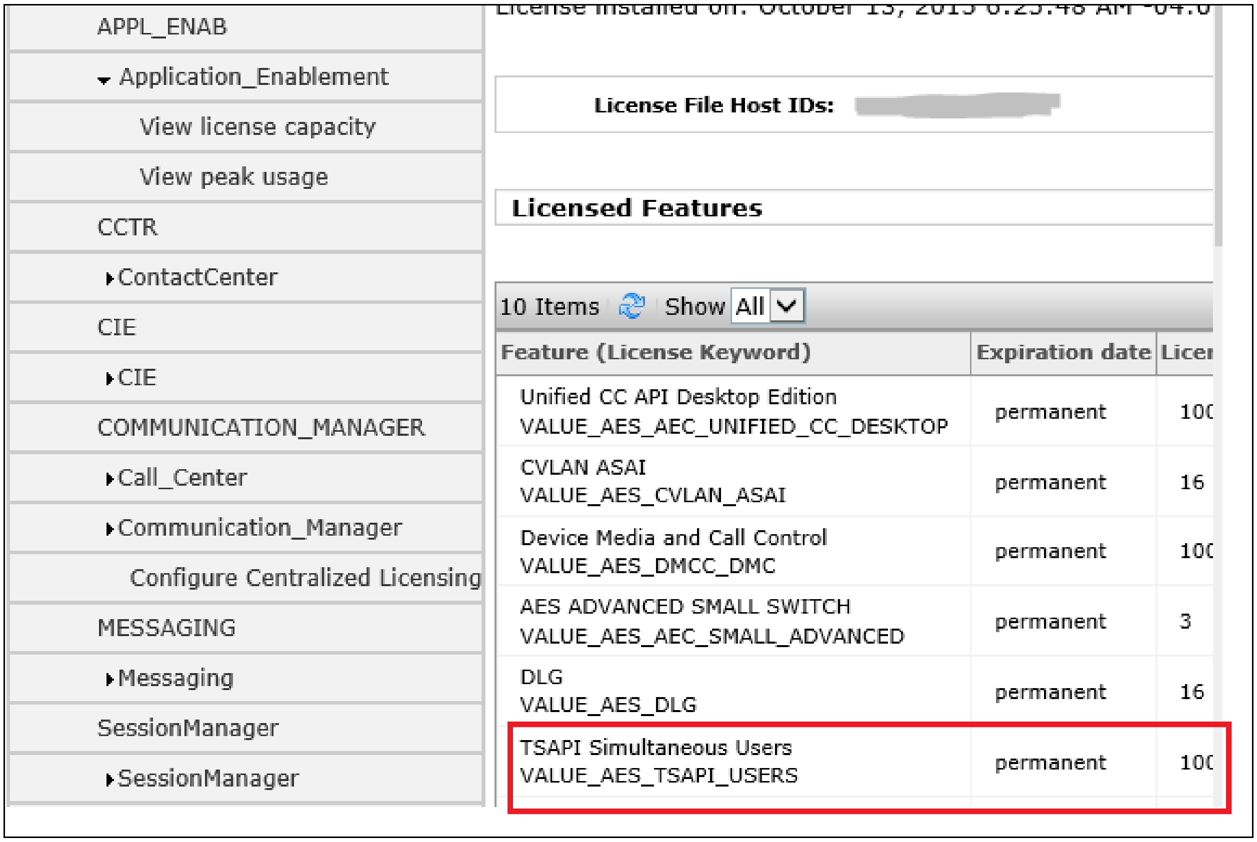
6.2. Verify Avaya Aura® Application Enablement Services License

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.



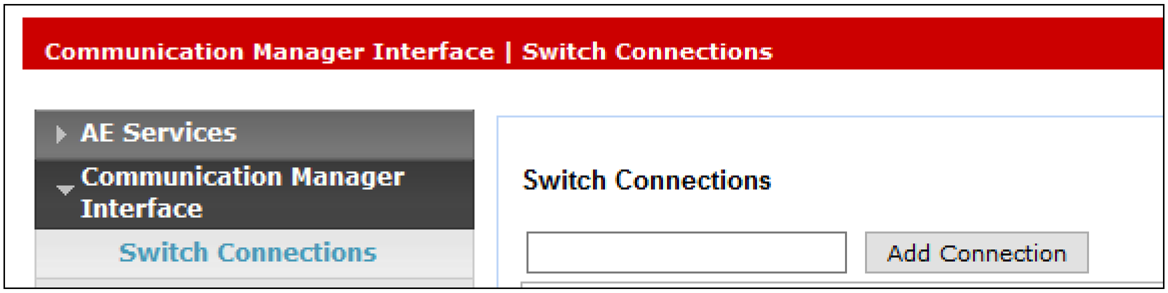
The **Web License Manager** screen below is displayed. Select **Licensed products → APPL_ENAB → Application_Enablement** in the left pane, to display the **Application Enablement (CTI)** screen in the right pane.

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

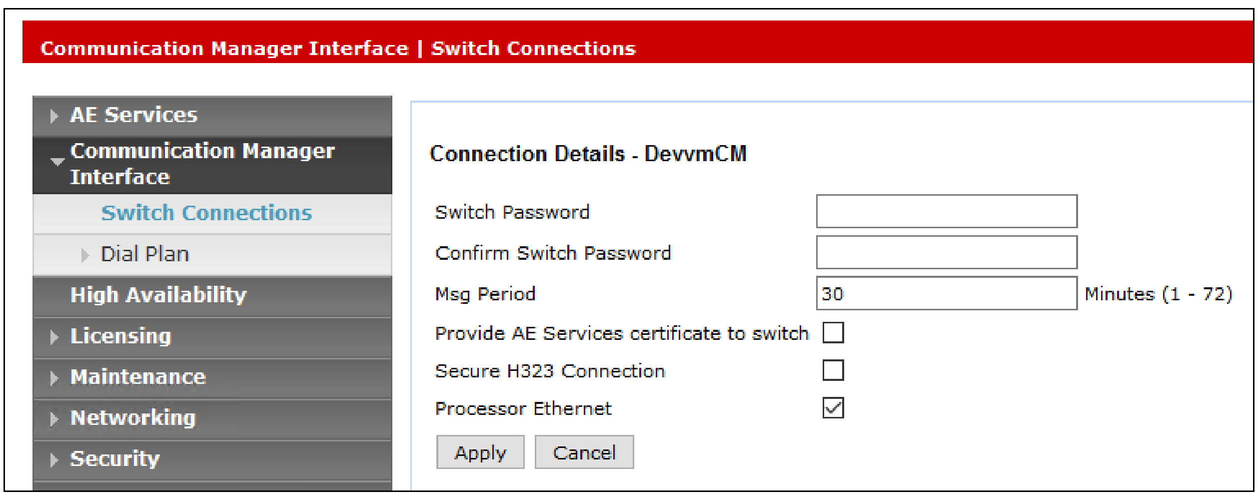


6.3. Create a Avaya Aura® Communication Manager Switch Connection

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

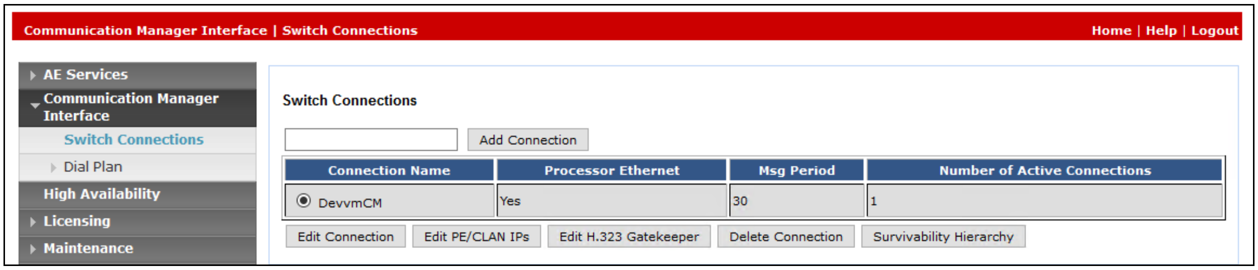


In the **Connection Details** window opens enter the **Switch Password** as was configured in **Section 5.14** and **Confirm Switch Password**. Click on the **Apply** button.

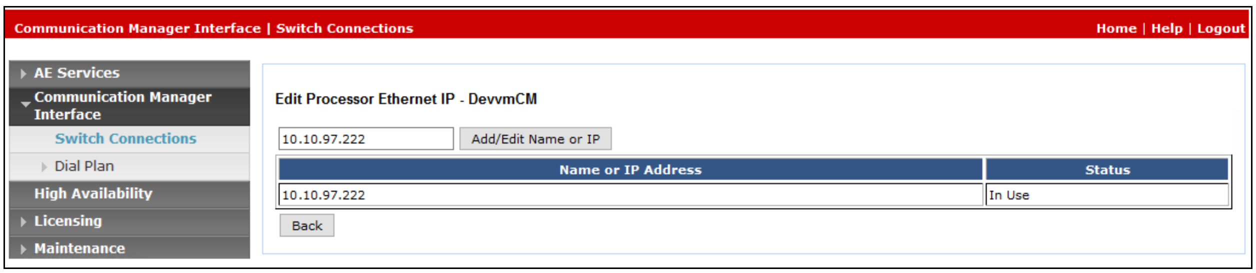


Select **Communication Manager Interface → Switch Connections** from the left pane. The **Switch Connections** screen shows a listing of the existing switch connections.

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**.

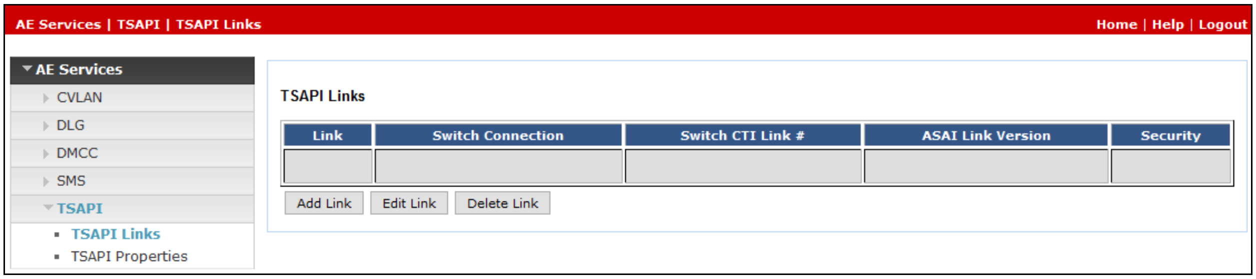


The **Edit Processor Ethernet IP** screen is displayed. Enter the IP address of a C-LAN circuit pack or the Processor C-LAN on Communication Manager to be used, in this case “10.10.97.222” as shown below, which is the Processor C-LAN on Communication Manager. Click **Add/Edit Name or IP**. Screen below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



6.4. Create a TSAPI Link

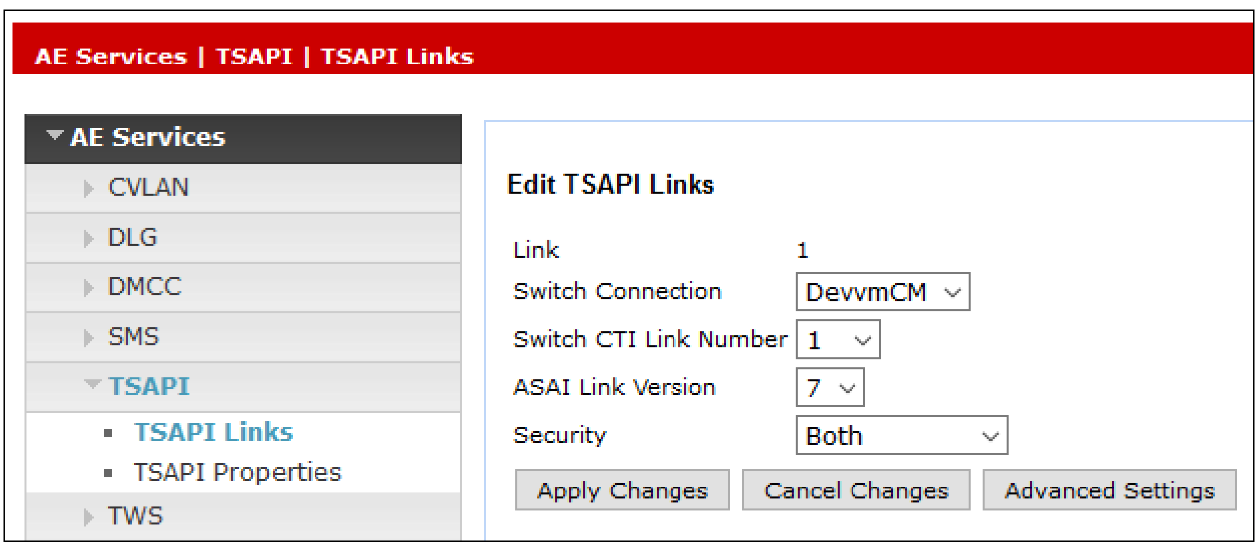
A TSAPI Link needs to be created to interoperate with Trio Enterprise. Navigate to **AE Services → TSAPI → TSAPI Links** and click on the **Add Link** button.



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

- **Link:** Select the next available Link from the dropdown box
- **Switch Connection:** Select **DevvmCM** from the dropdown box. (The Switch connection as created in **Section 6.3**)
- **Switch CTI Link Number:** Select **1** from the dropdown box. (The CTI link as created in **Section 5.1515**)
- **ASAI Link Version:** **7**
- **Security:** Select **Both** from the dropdown box

Click on the **Apply Changes** button.

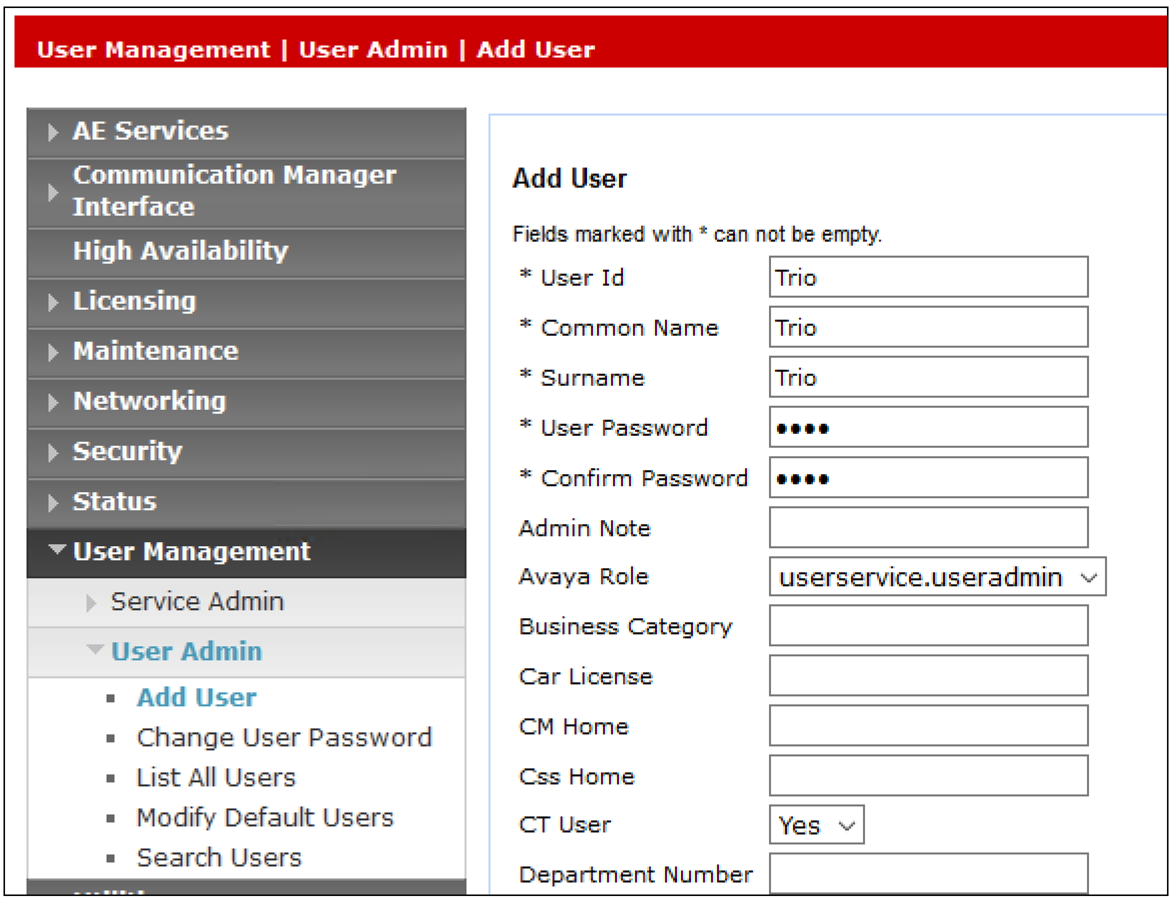


6.5. Create CTI User

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

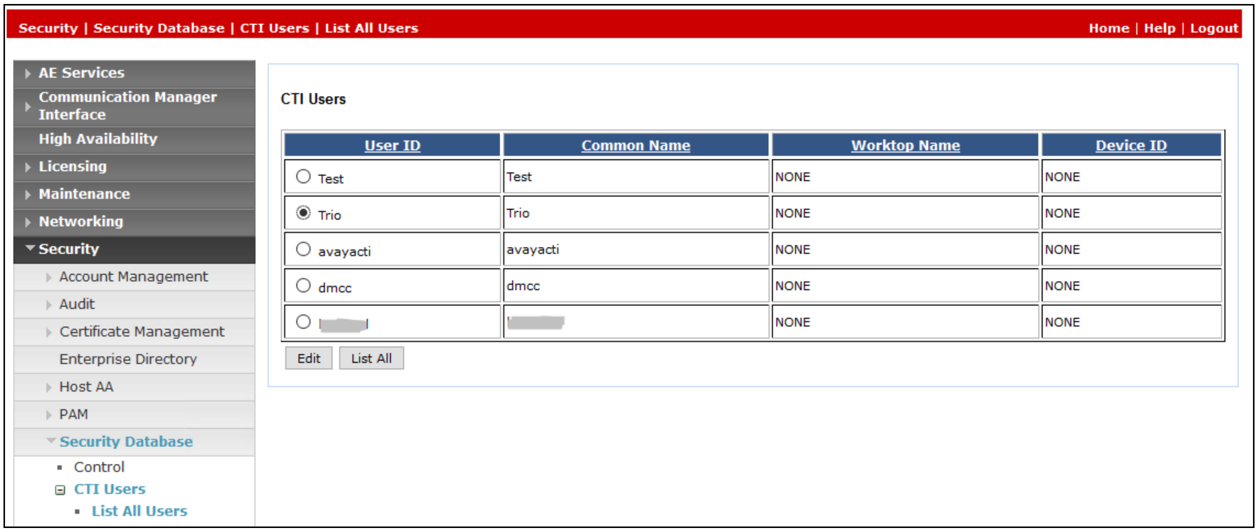
- **User Id**: Enter an informative name (i.e. T**rio**. This ID is required for the Trio Enterprise installation
- **Common Name**: Enter a Common Name (i.e. T**rio**)
- **Surname**: Enter a Surname (i.e. T**rio**)
- **User Password:** Enter a password. This password is be required for the Trio Enterprise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

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

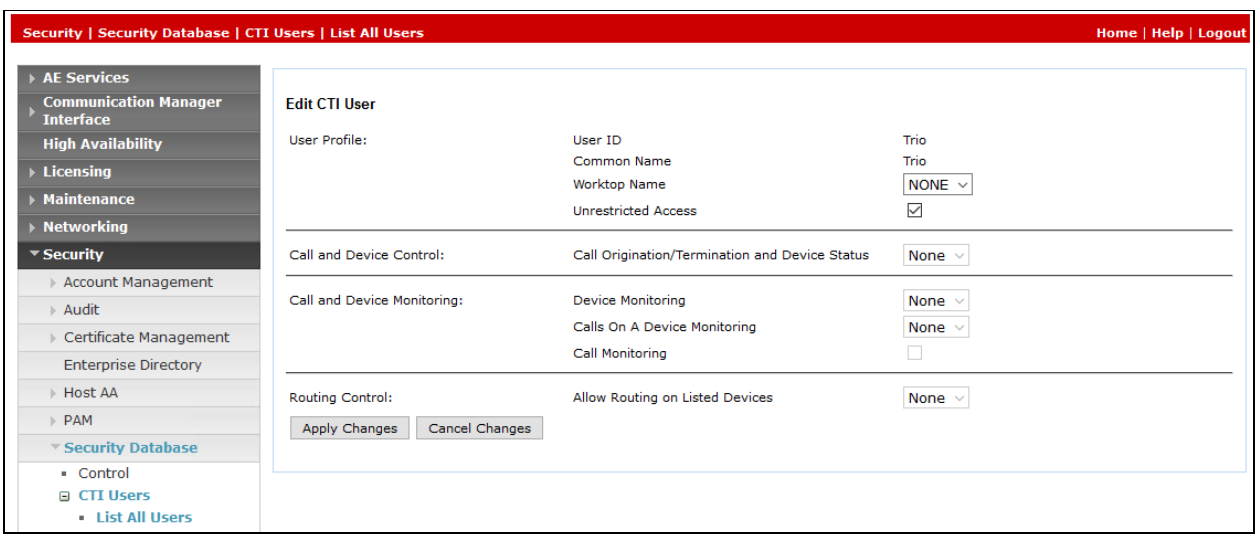


6.6. Configure Security Database

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



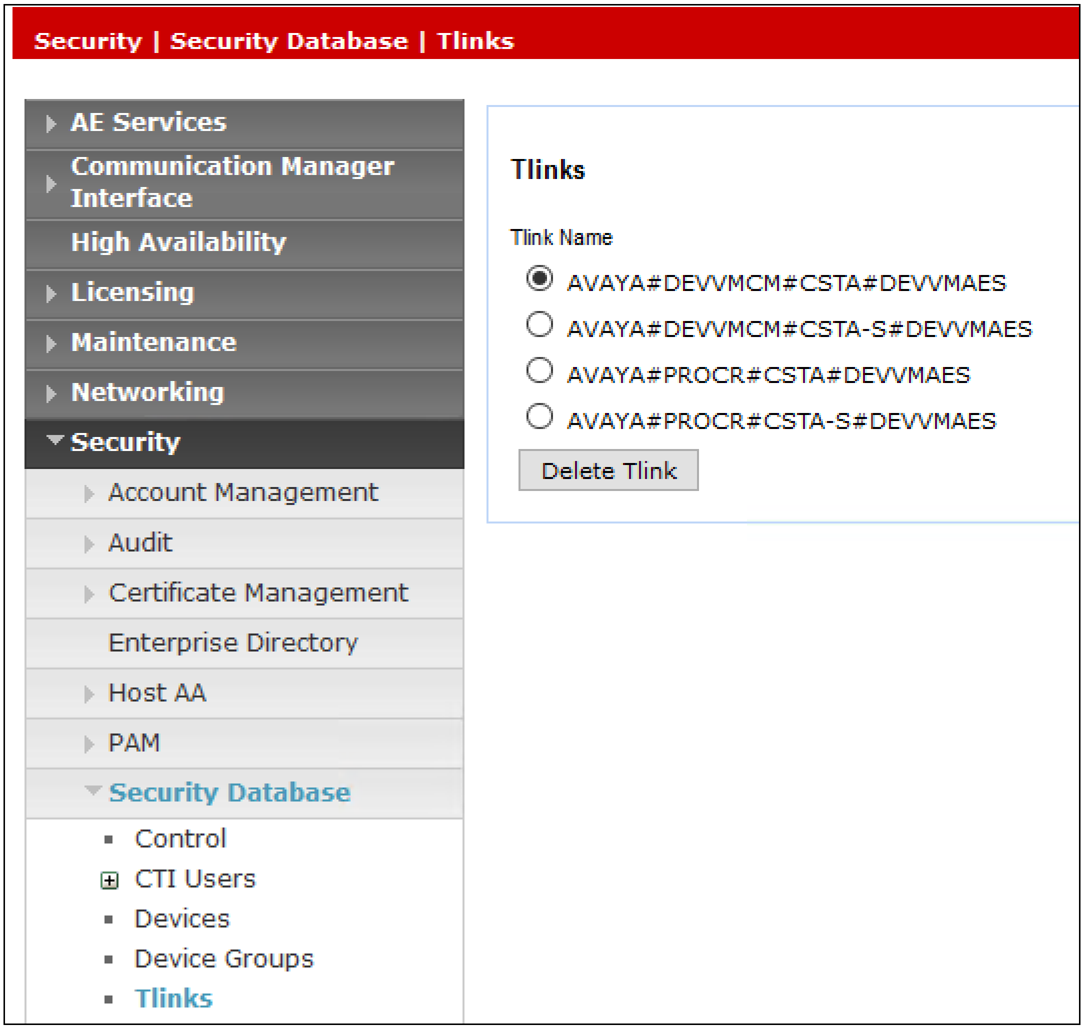
Once the **Edit CTI User** page appears, tick the **Unrestricted Access** check box and **Apply Changes** at the bottom of the screen.



6.7. Obtain Tlink Name

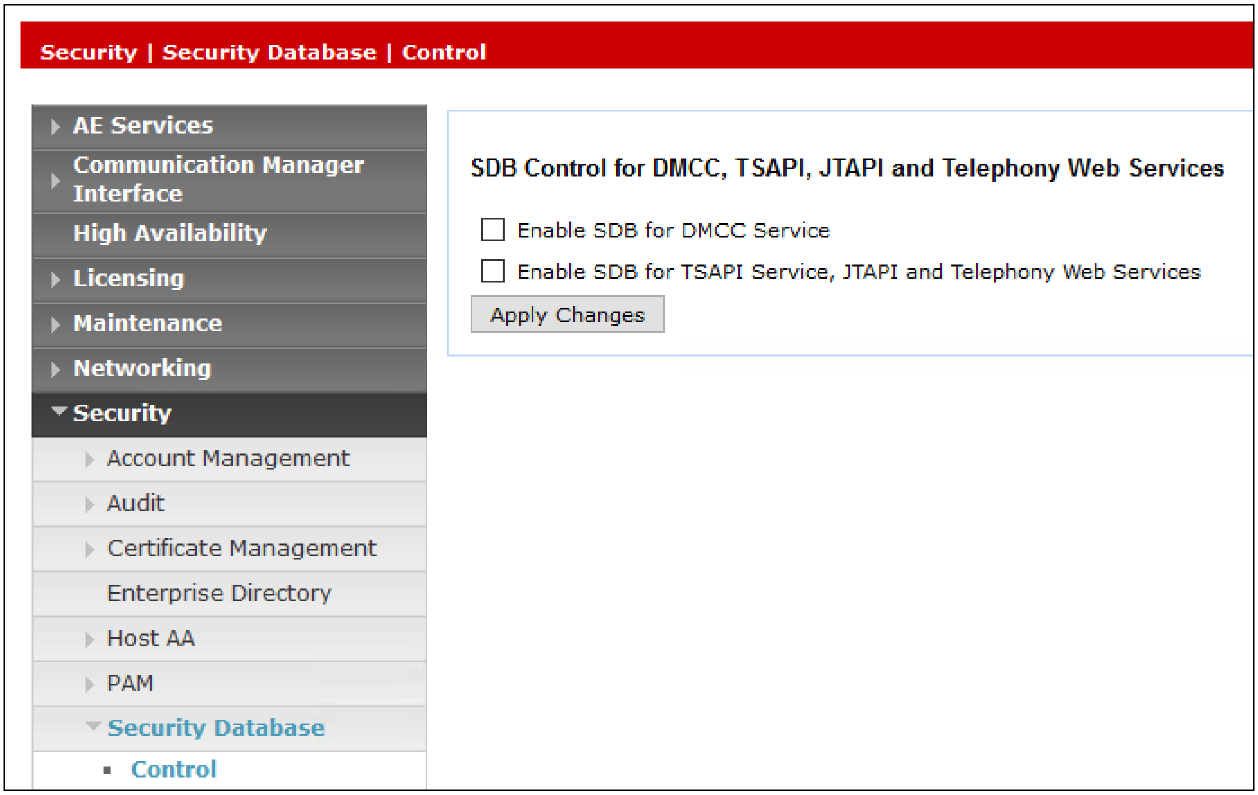
Select **Security → Security Database → Tlinks** from the left pane. The **Tlinks** screen shows a listing of the Tlink names. A new Tlink name is automatically generated for the TSAPI service. Locate the Tlink name associated with the relevant switch connection, which would use the name of the switch 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

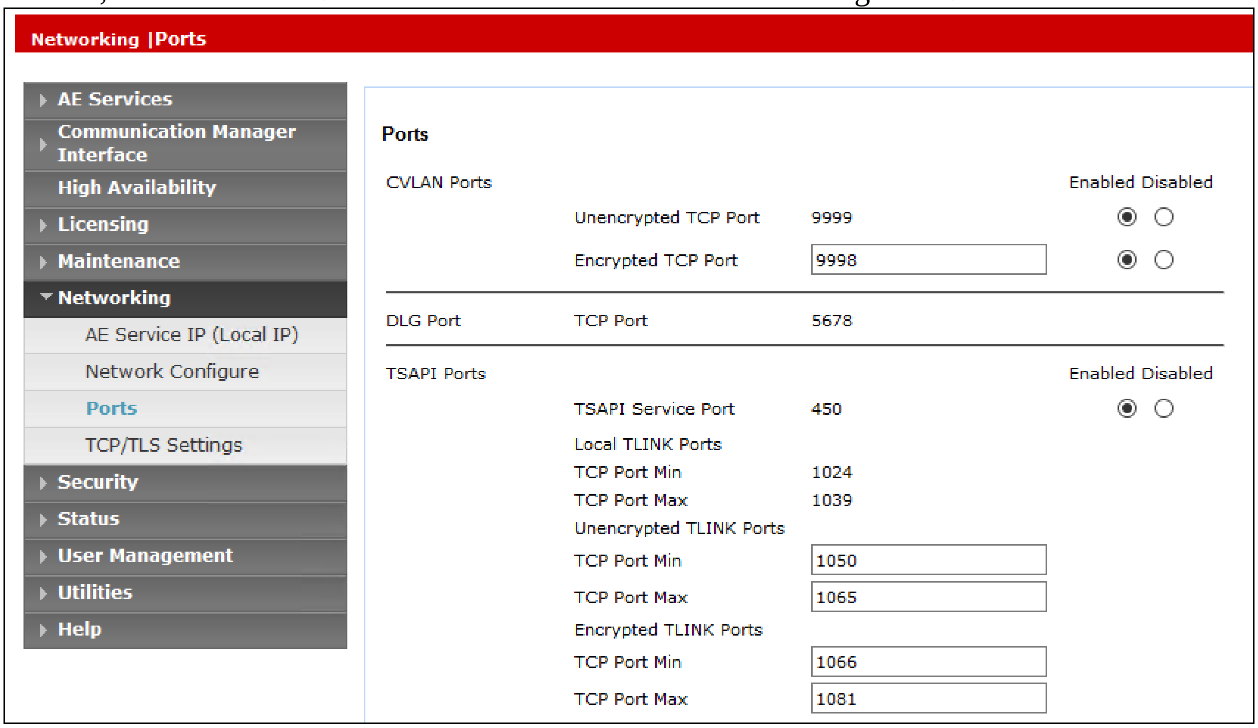
Select **Security → Security Database → Control** from the left pane, to display the **SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services** screen in the right pane. Uncheck both fields below.



6.9. Enable Ports

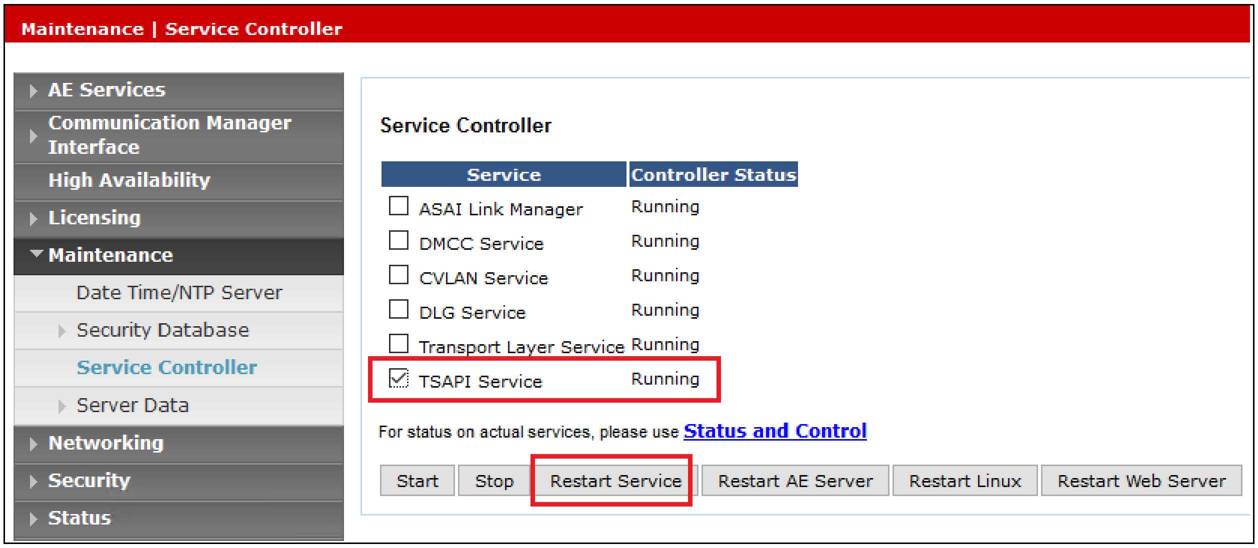
Select **Networking → Ports** from the left pane, to display the **Ports** screen in the right pane.

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.



6.10. Restart TSAPI Service

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



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

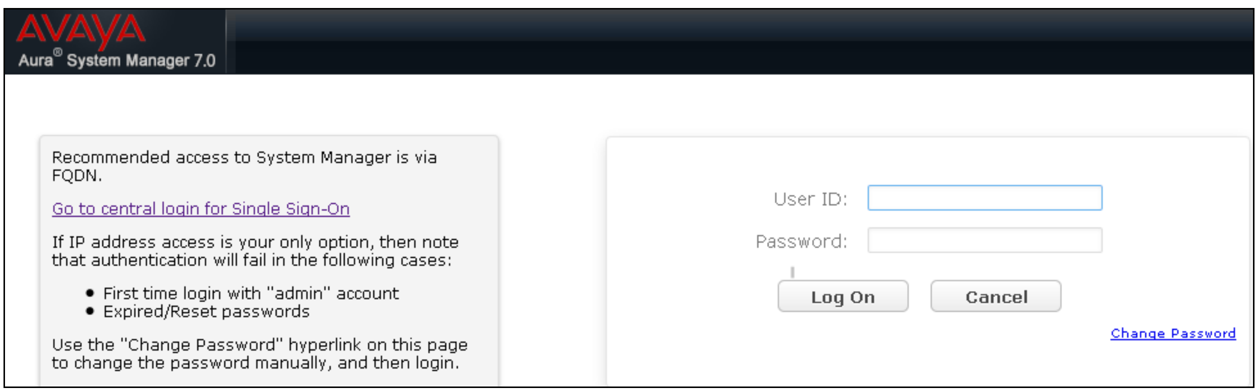
7. Configure Avaya Aura® Session Manager

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

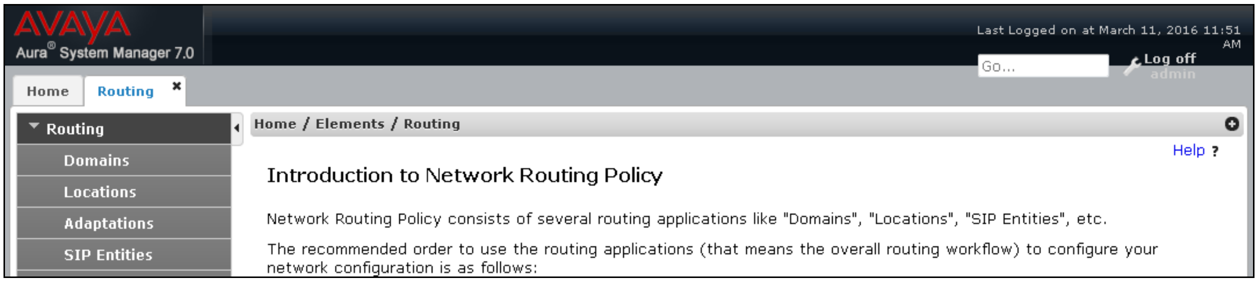
7.1. Launch System Manager

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.

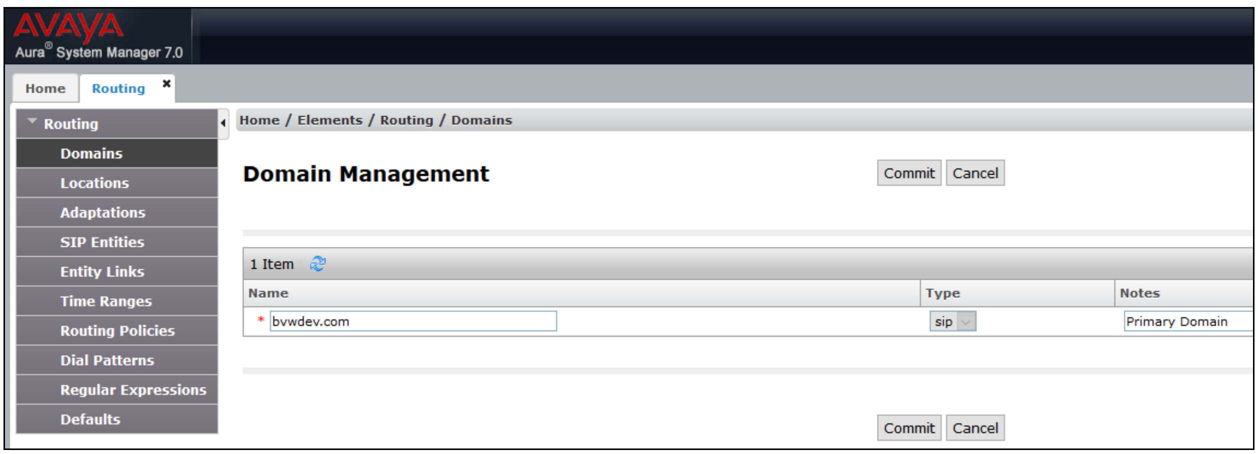


7.2. Administer Domain

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



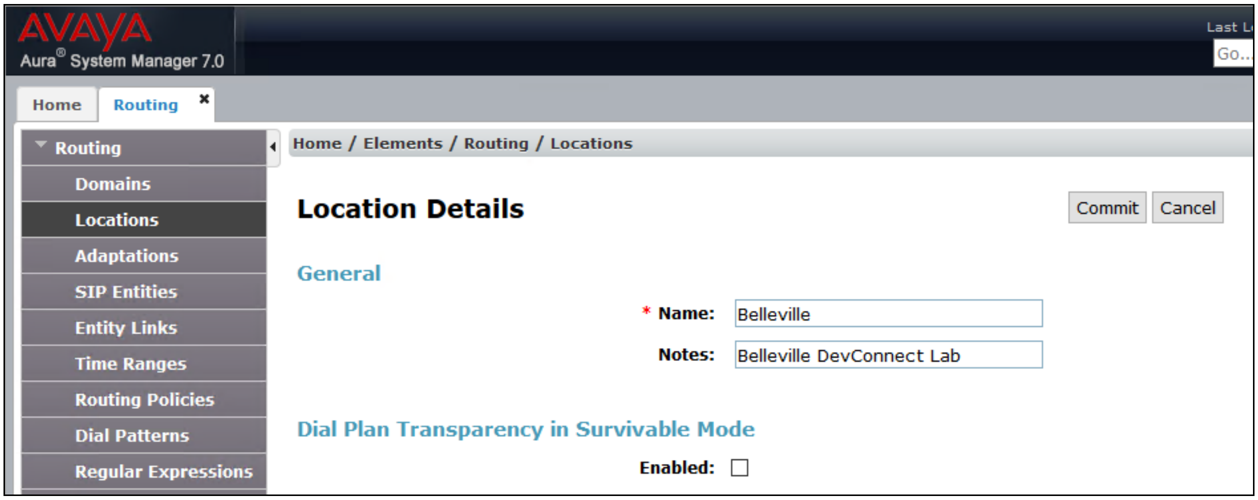
The **Domain Management** screen is displayed. In the **Name** field enter the domain name, select *sip* from the **Type** drop down menu and provide any optional **Notes**.



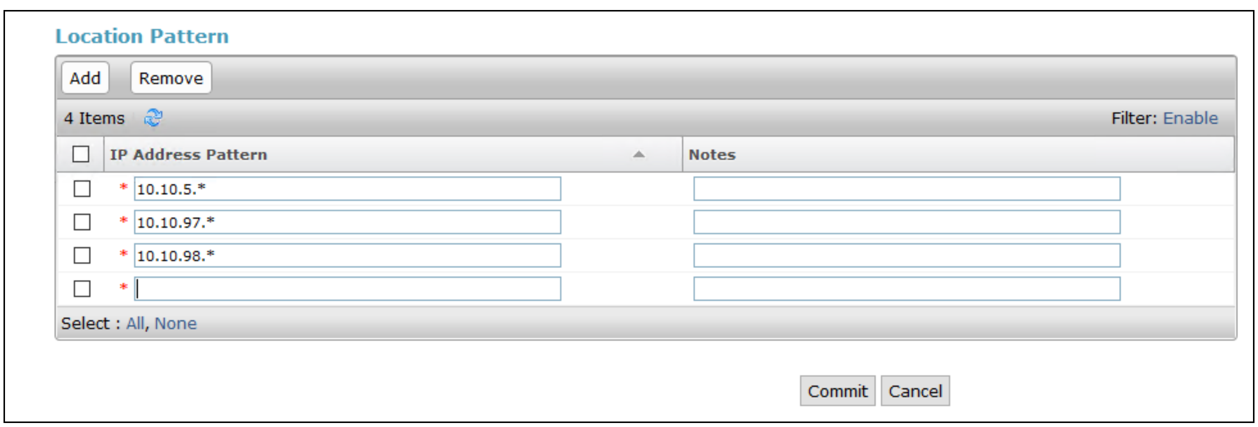
7.3. Administer Locations

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.



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.



7.4. Administer Adaptation

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

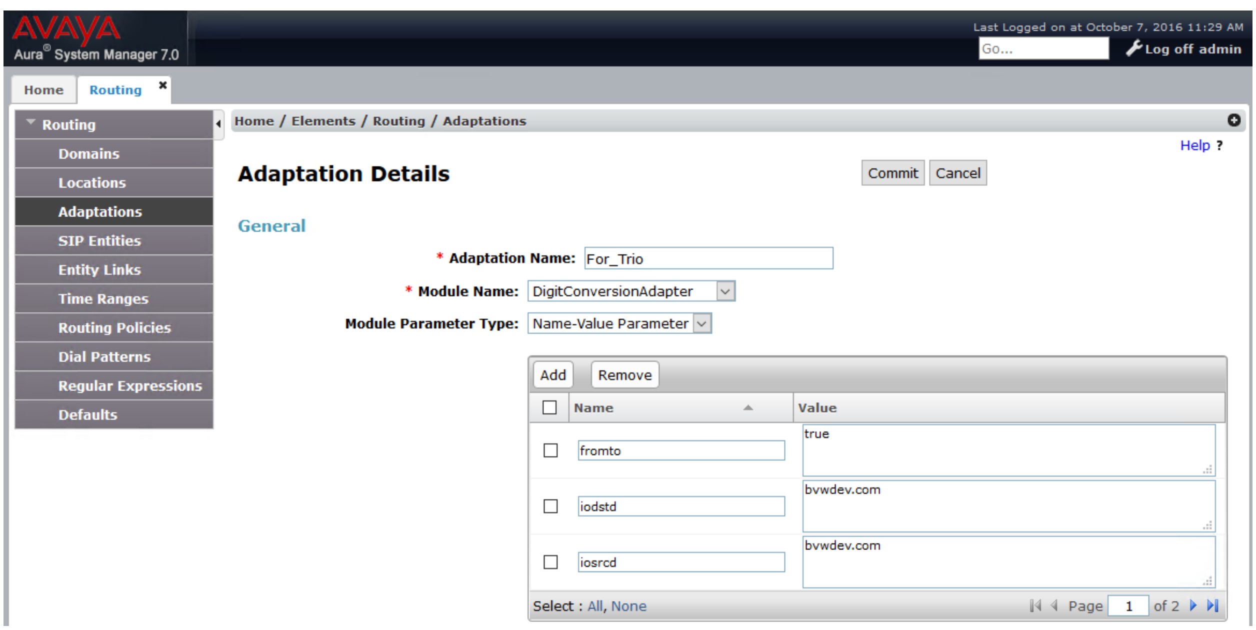
Enter the following for the Trio Adaptation.

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

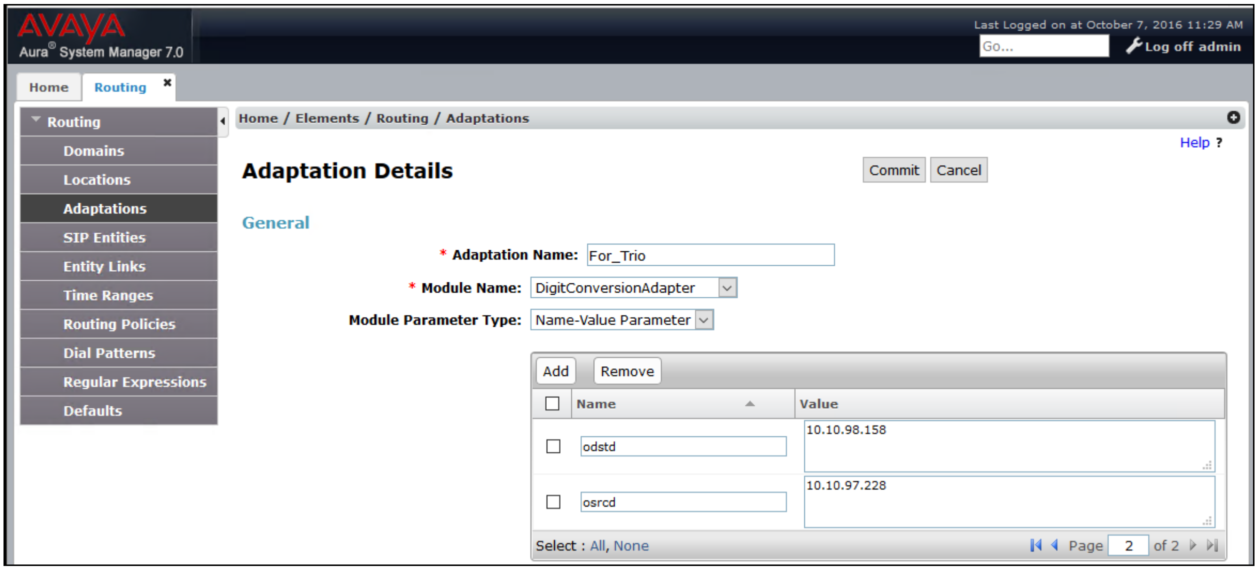
Click **Add** to add a new row for the following values as shown below table:

Name	Value
fromto	true
iodstd	Enter the domain name of system, ex: **bvwdev.com**
iosrcd	Enter the domain name of system, ex: **bvwdev.com**
odstd	Enter IP address of Trio, ex: **10.10.98.158**
osrcd	Enter IP Address of Session Manager, ex: **10.10.97.228**

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



(Continue) the screenshot show Adaptation created for Trio:



7.5. Administer SIP Entities

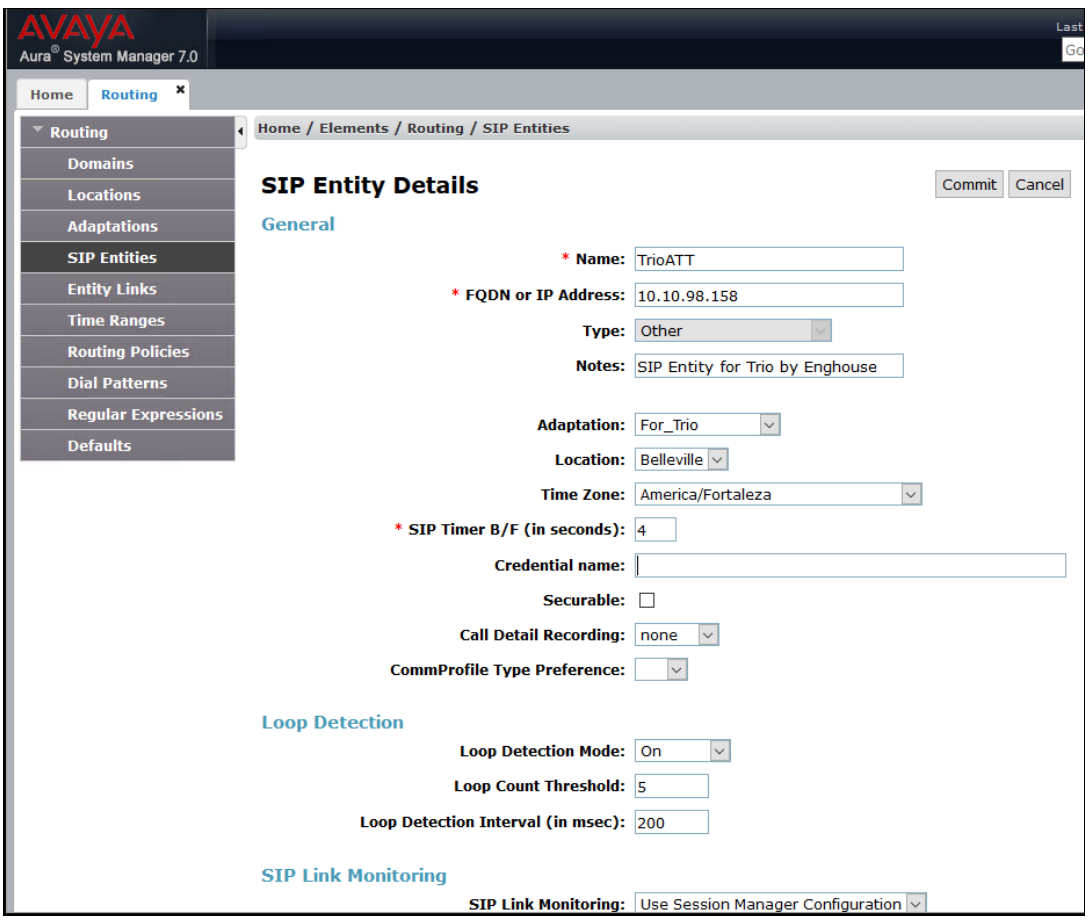
Add two new SIP entities, one for Trio Enterprise and one for the new SIP trunks with Communication Manager.

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.

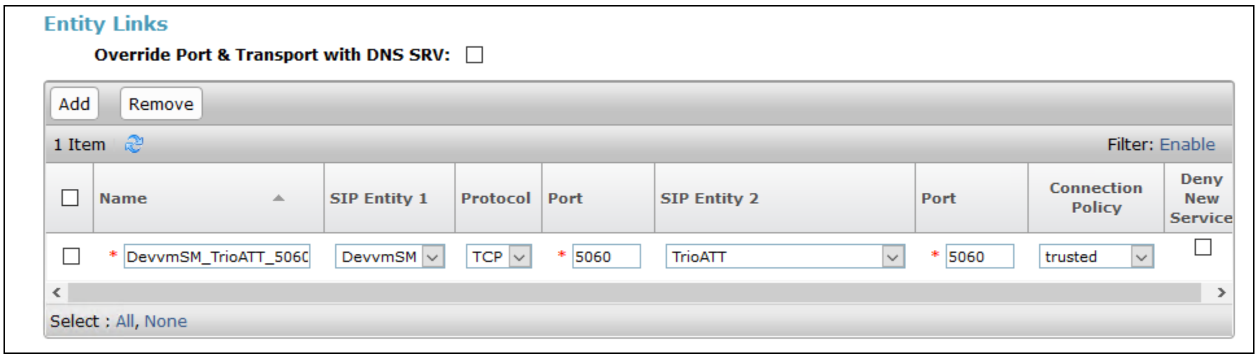
- **Name:** A descriptive name.
- **FQDN or IP Address:** The IP address of the Trio Enterprise server.
- **Type:** "Other"
- **Notes:** Any desired notes.
- **Adaptation:** Select he adaptation configured in **Section 7.4**
- **Location:** Select the Trio Enterprise location name from **Section 7.3**.
- **Time Zone:** Select the applicable 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 "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.

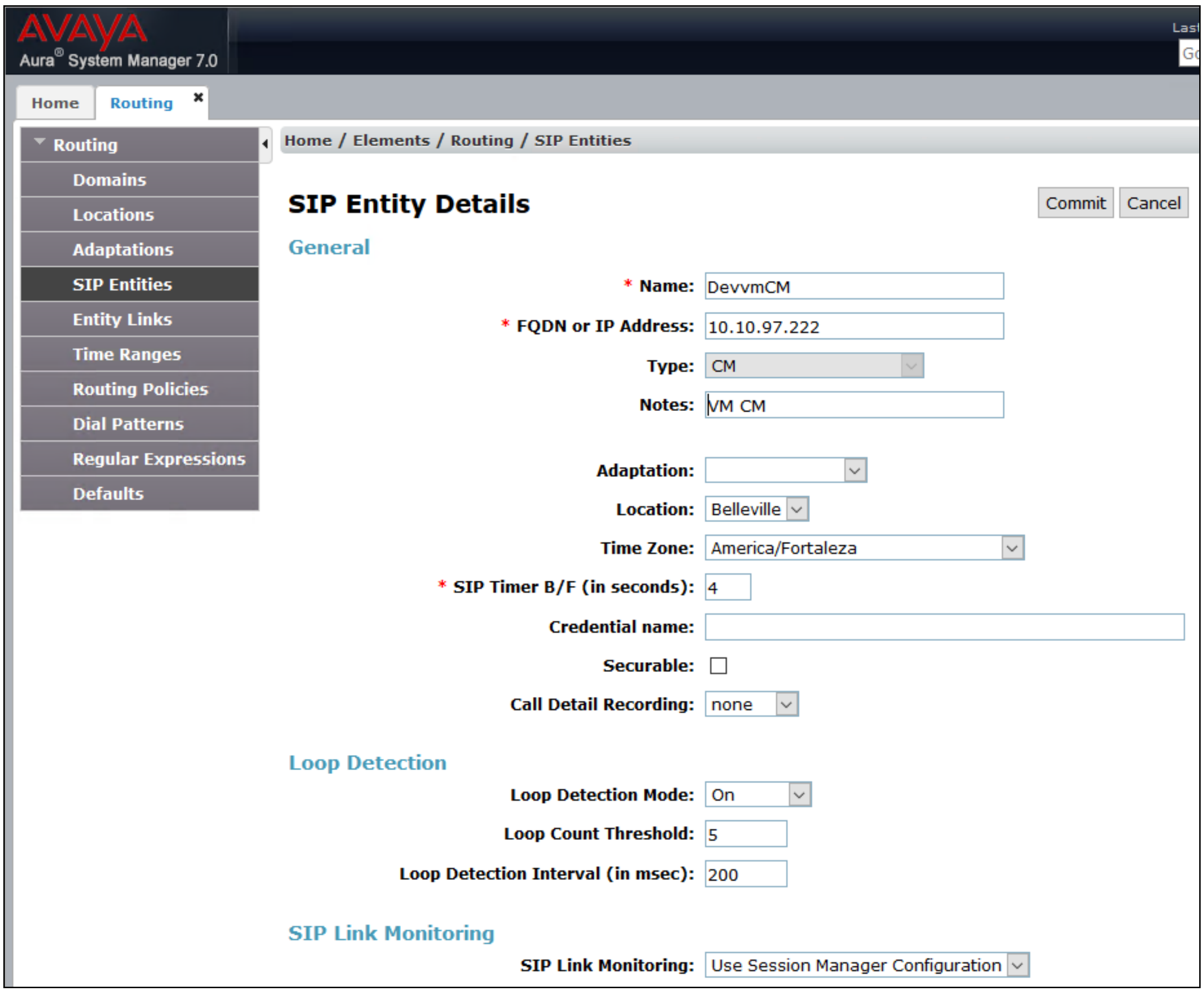


7.5.2. SIP Entity for Communication Manager

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.

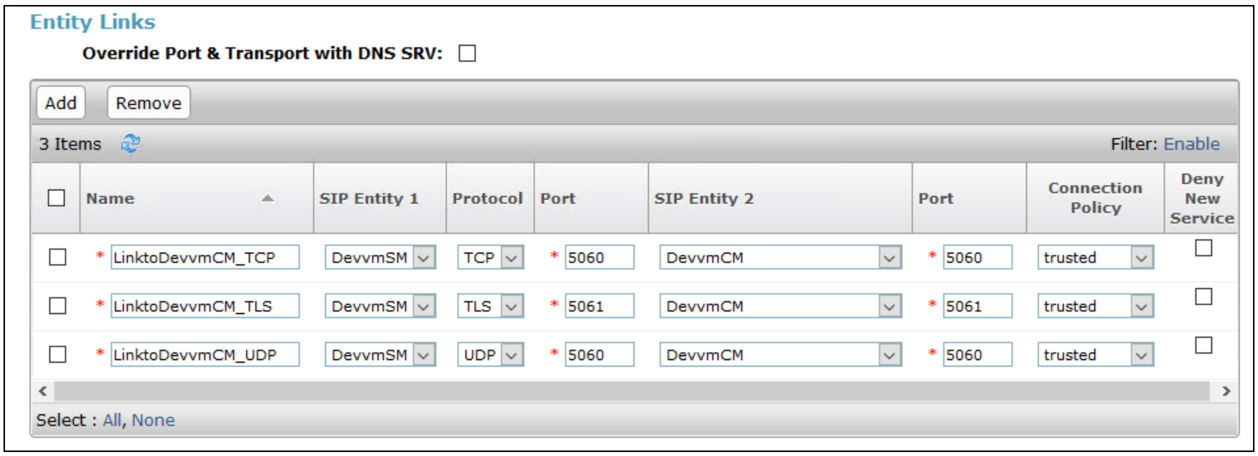
The **SIP Entity Details** screen is displayed. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **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.



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 signaling group transport (TLS) method from **Section 5.4**.
- **Port:** The signaling group listen port (5061) number from **Section 5.4**.
- **SIP Entity 2:** The Communication Manager entity name from this section.
- **Port:** The signaling group listen port (5061) number from **Section 5.4**.
- **Connection Policy:** "trusted"



7.6. Administer Routing Policies

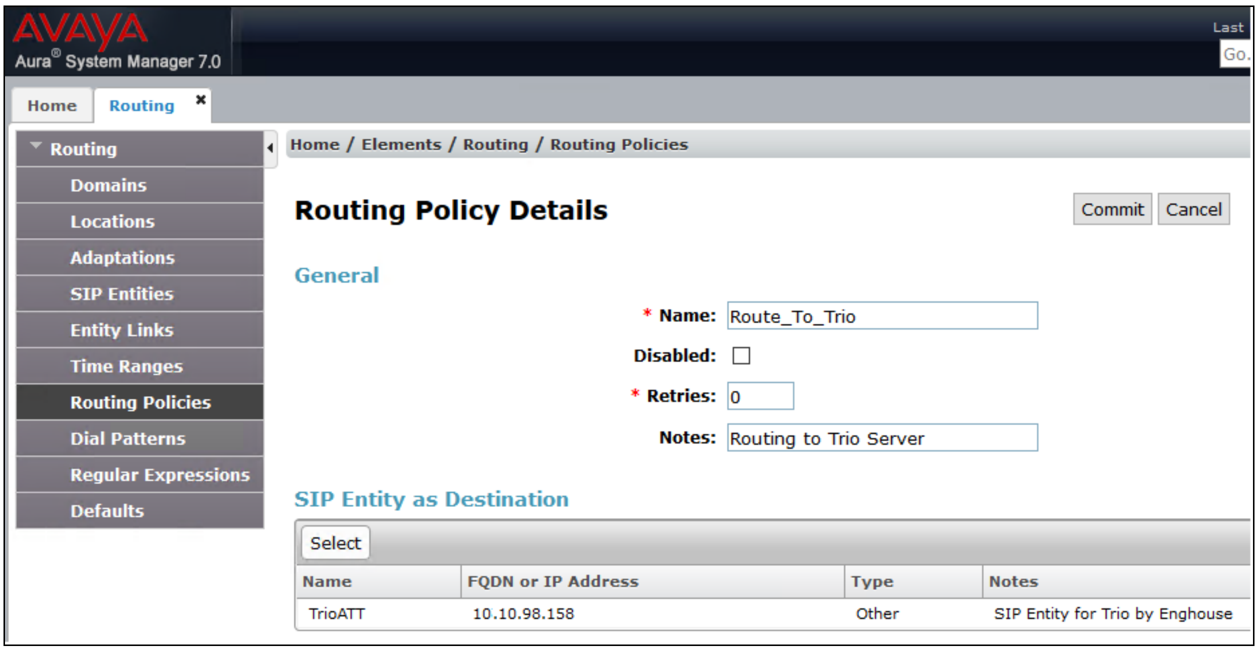
Add two new routing policies, one for Trio Enterprise and one for the new SIP trunks with Communication Manager.

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.

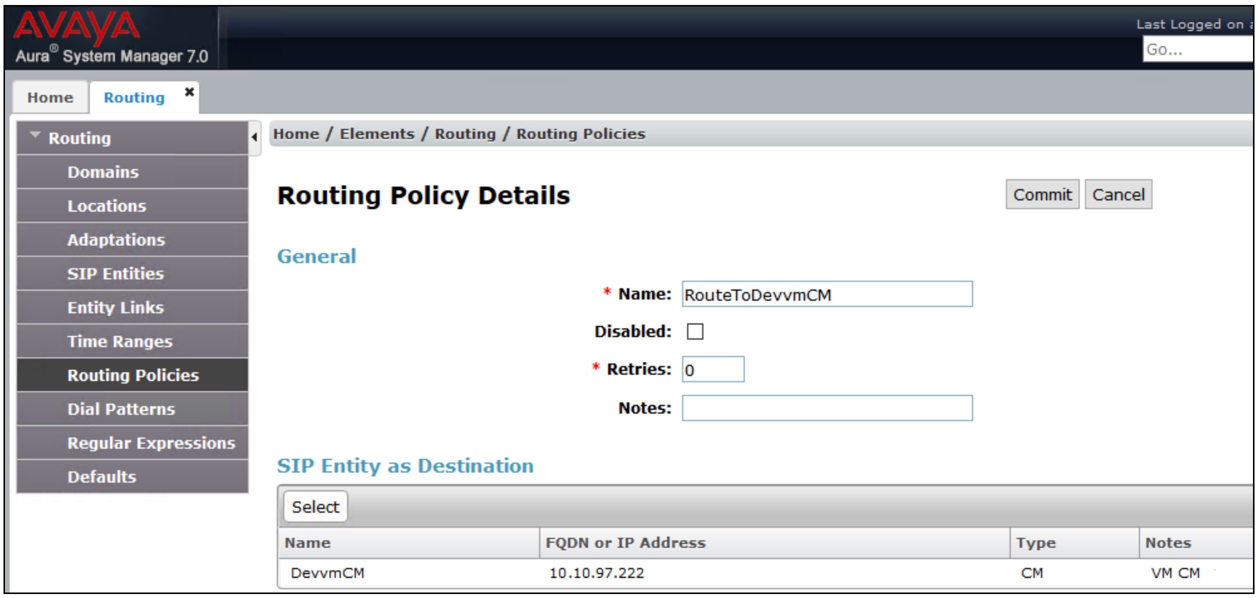


7.6.2. Routing Policy for Communication Manager

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.



7.7. Administer Dial Patterns

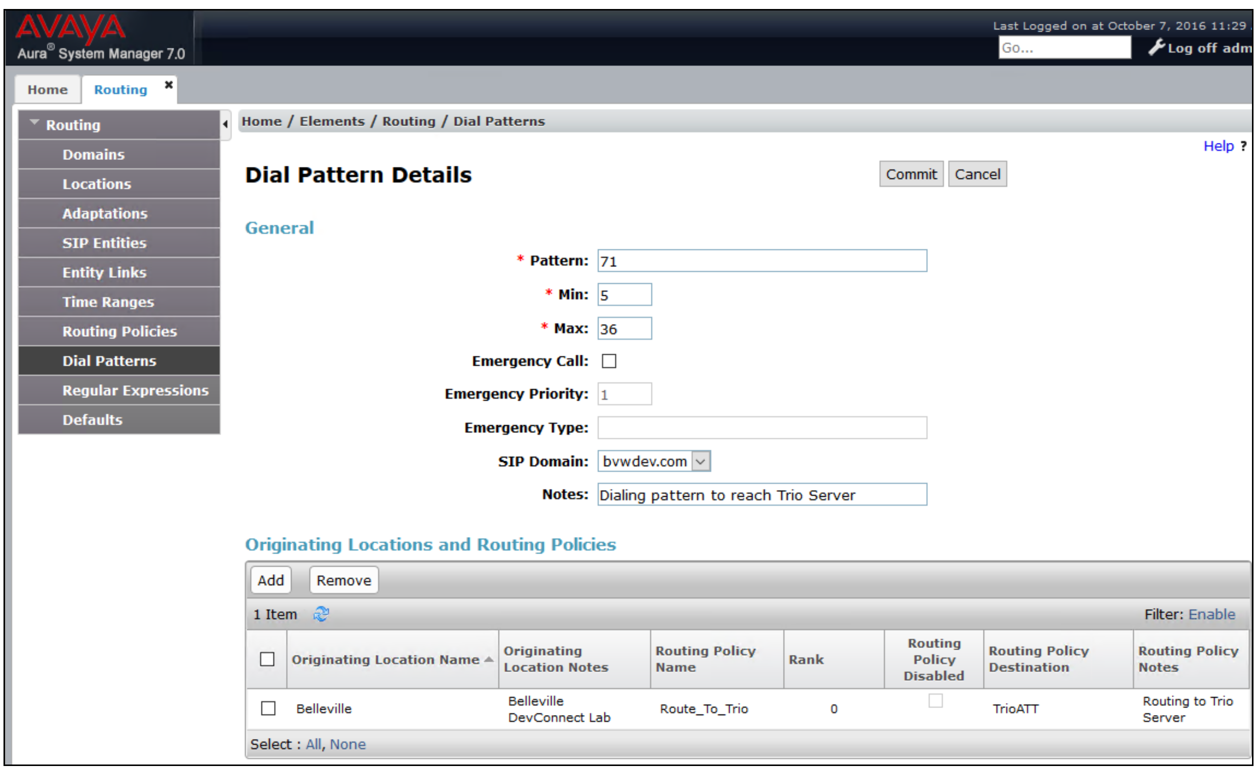
Add a new dial pattern for Trio Enterprise, and update existing dial patterns for Communication Manager.

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 signaling group domain name from **Section 5.4**.

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.



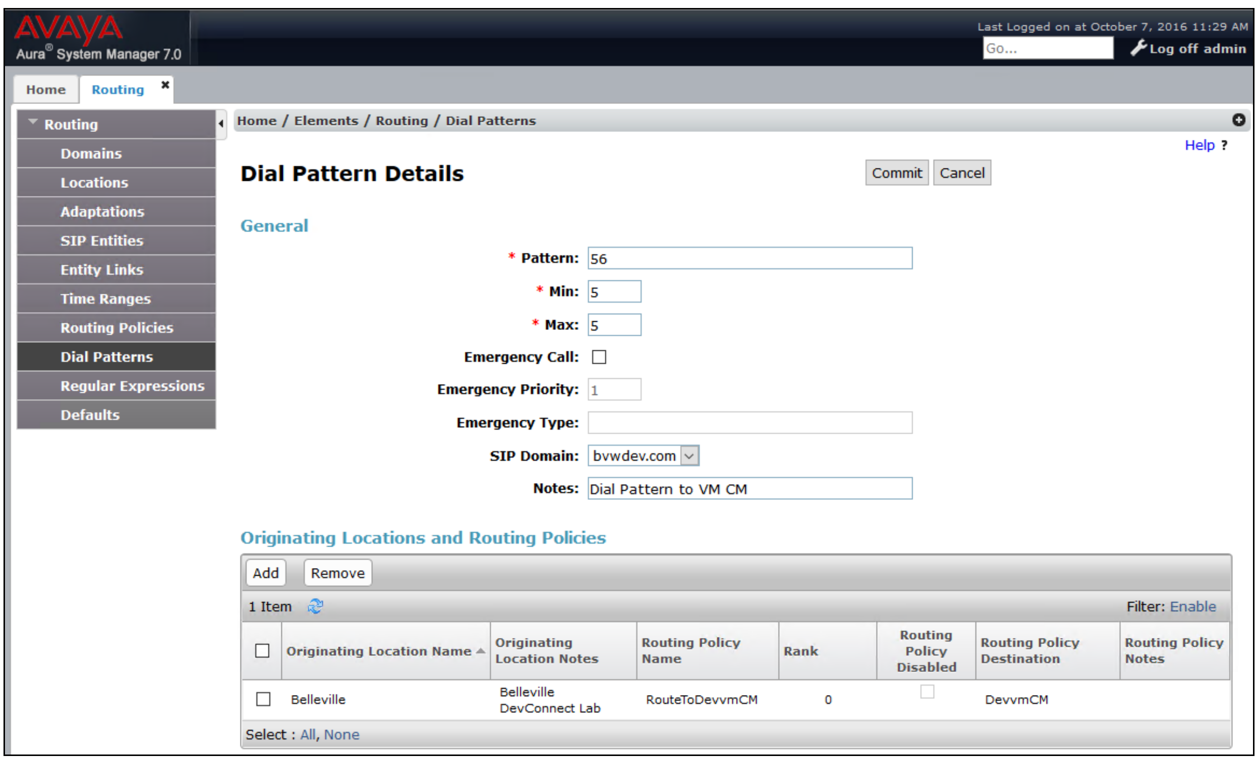
7.7.2. Dial Pattern for Communication Manager

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”.
- **Min:** The minimum number of digits to match.
- **Max:** The maximum number of digits to match.
- **SIP Domain:** The signaling group domain name from **Section 5.4**.

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.

Follow the procedures in this section to make similar changes to the applicable Communication Manager dial pattern to reach the PSTN (not shown).



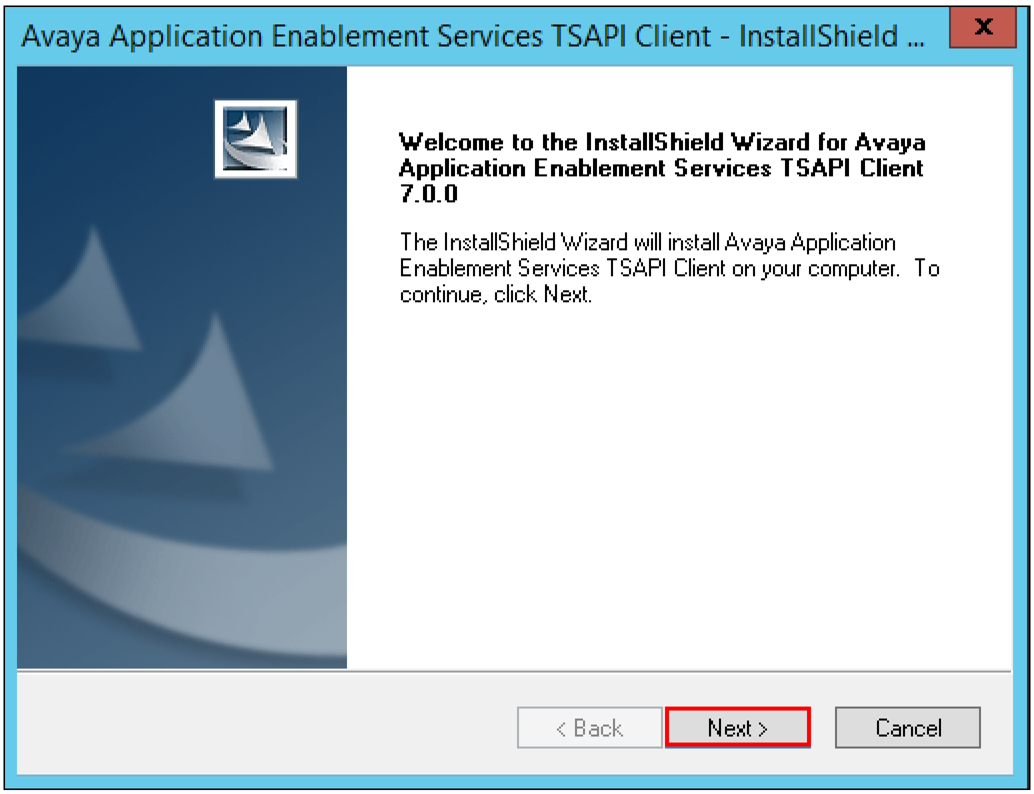
8. Configure Trio Enterprise

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

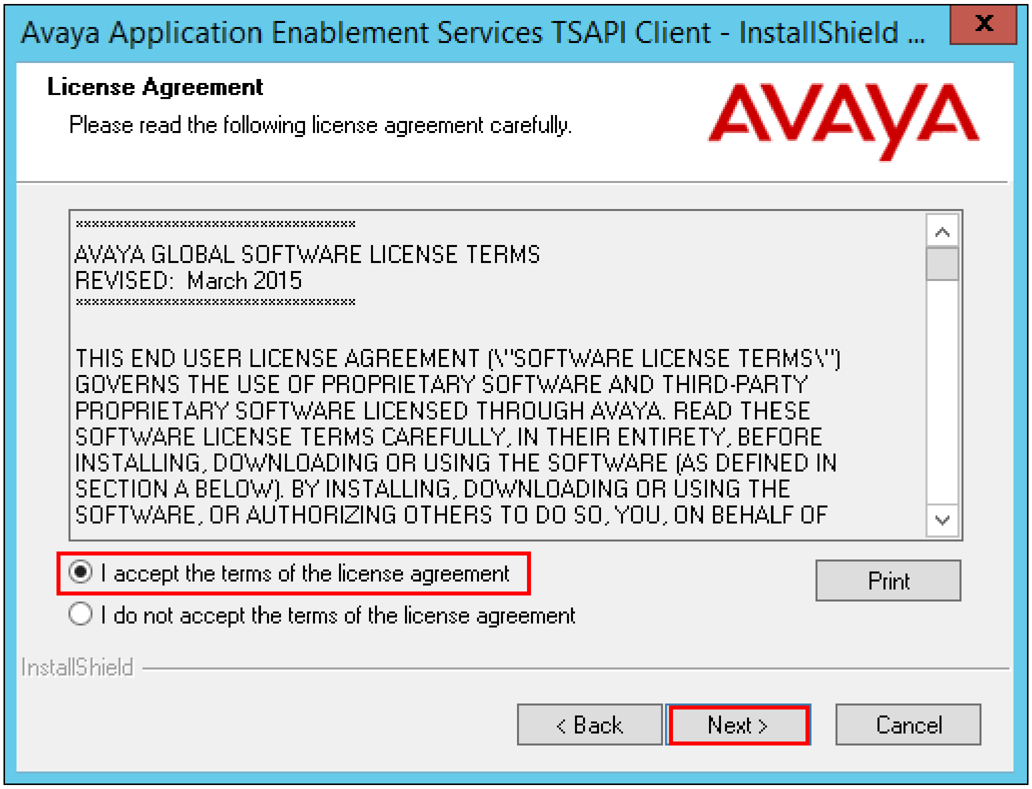
- Install Avaya Application Enablement Services TSAPI Client
- Configure Trio Enterprise to use SIP Trunks
- Configure Absence
- Configure Trio Enterprise Attendant

8.1. Install Avaya Application Enablement Services TSAPI Client

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



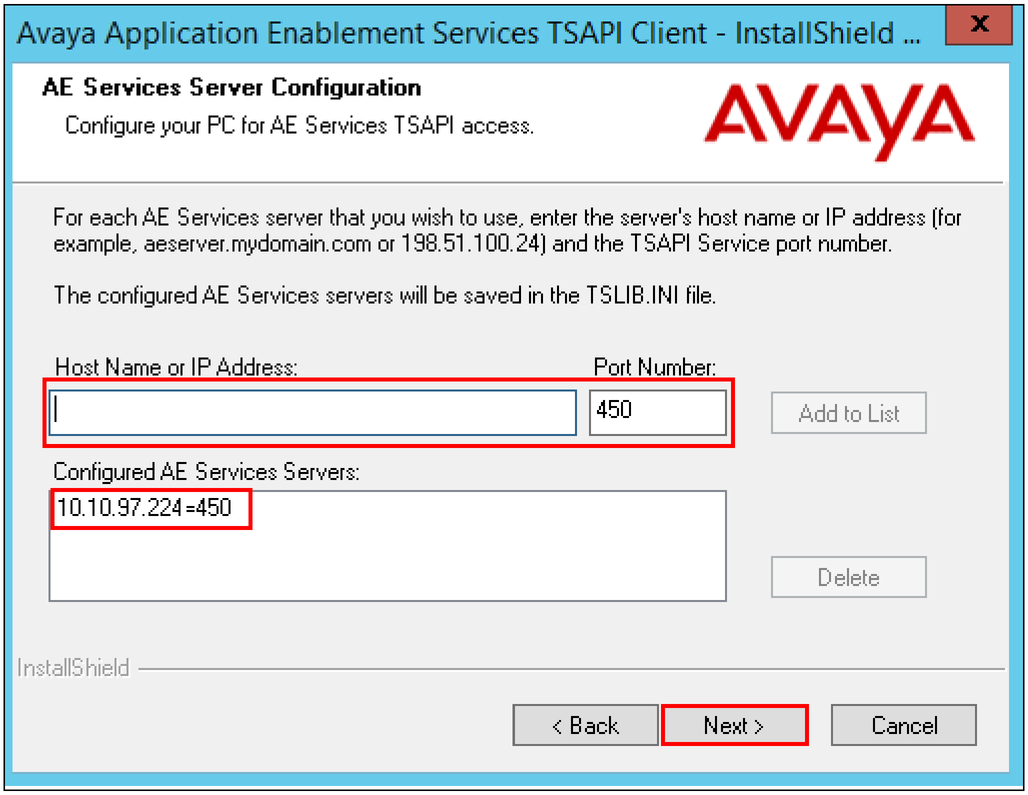
Accept the license agreement as shown below and click on **Next**.



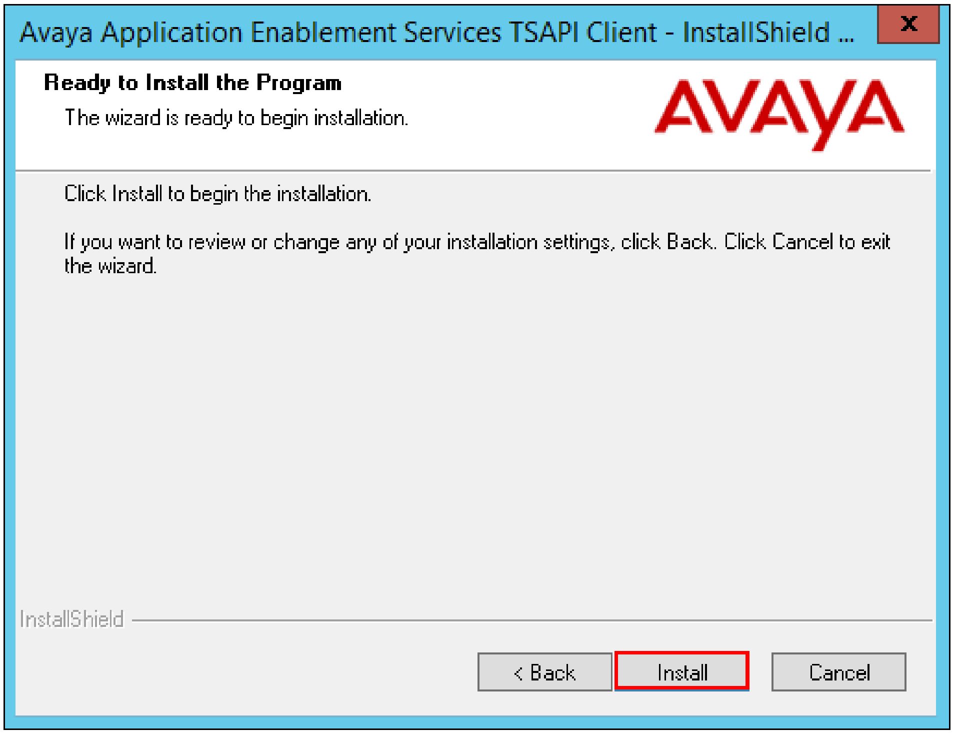
In the subsequent window, enter the following and select **Add to List**:

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

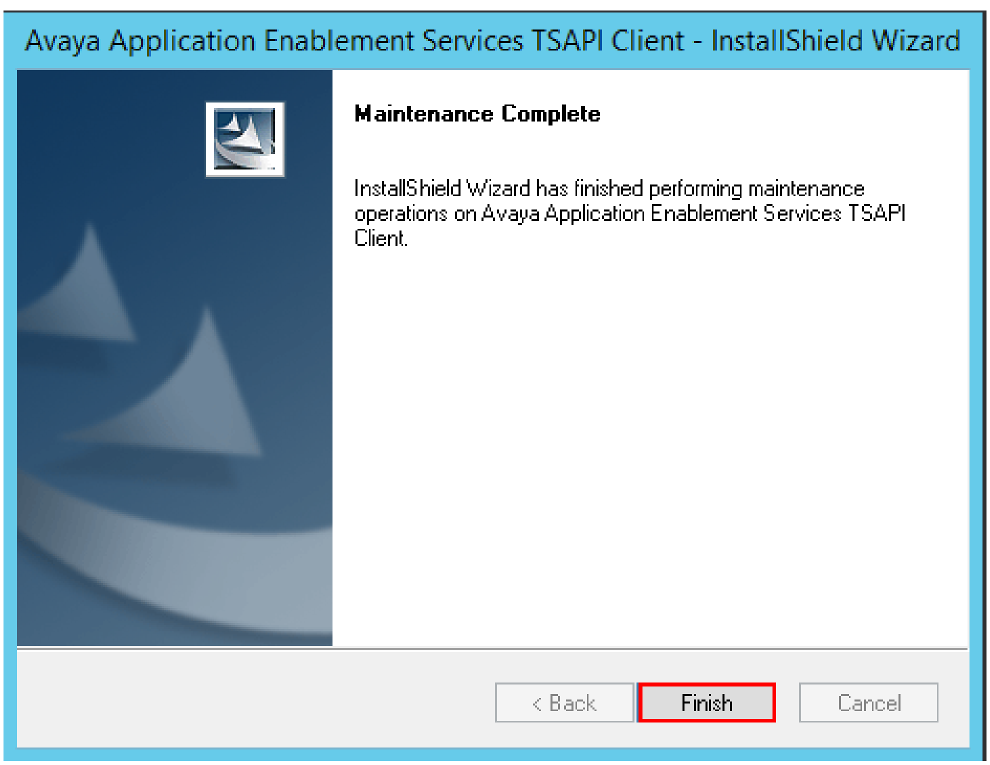
Click on the **Next** button to continue.



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



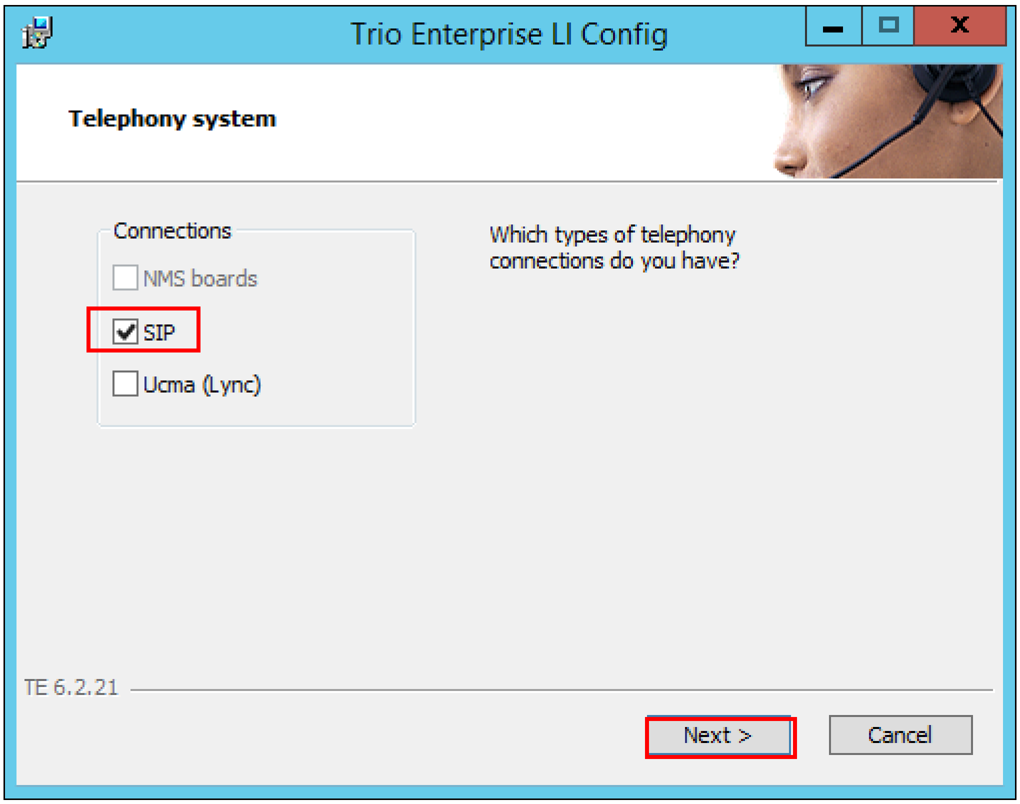
When the InstallShield Wizard Complete window appears click on the **Finish** button.



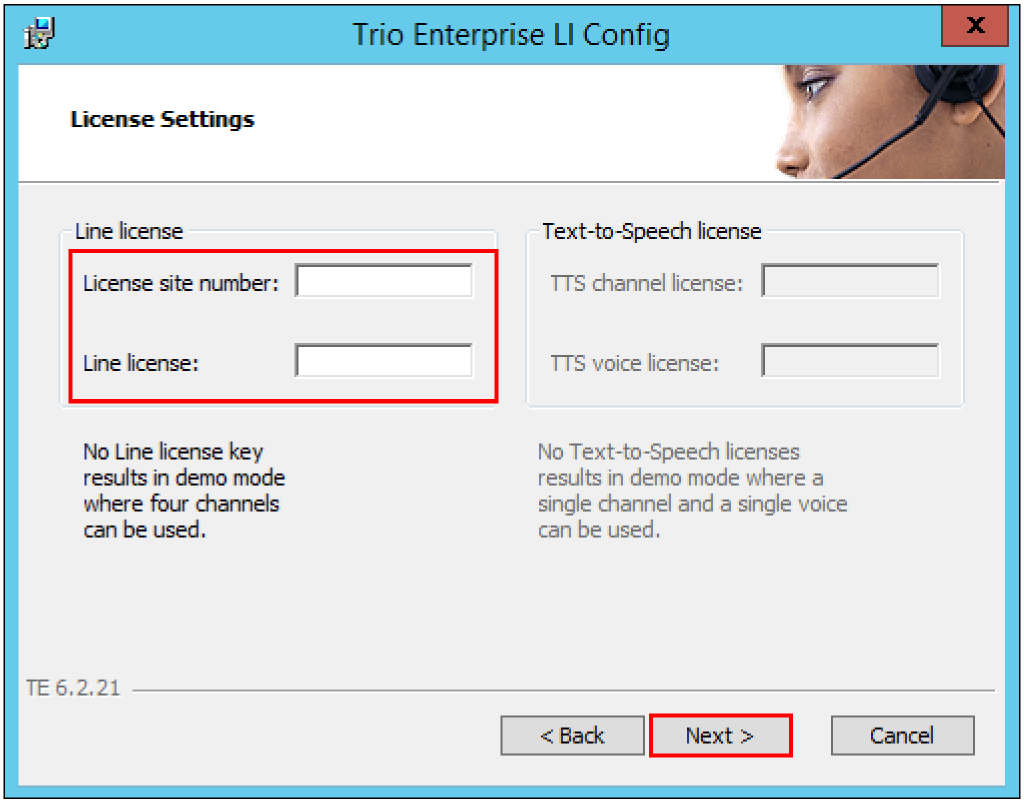
8.2. Configure Trio Enterprise to use SIP Trunks

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

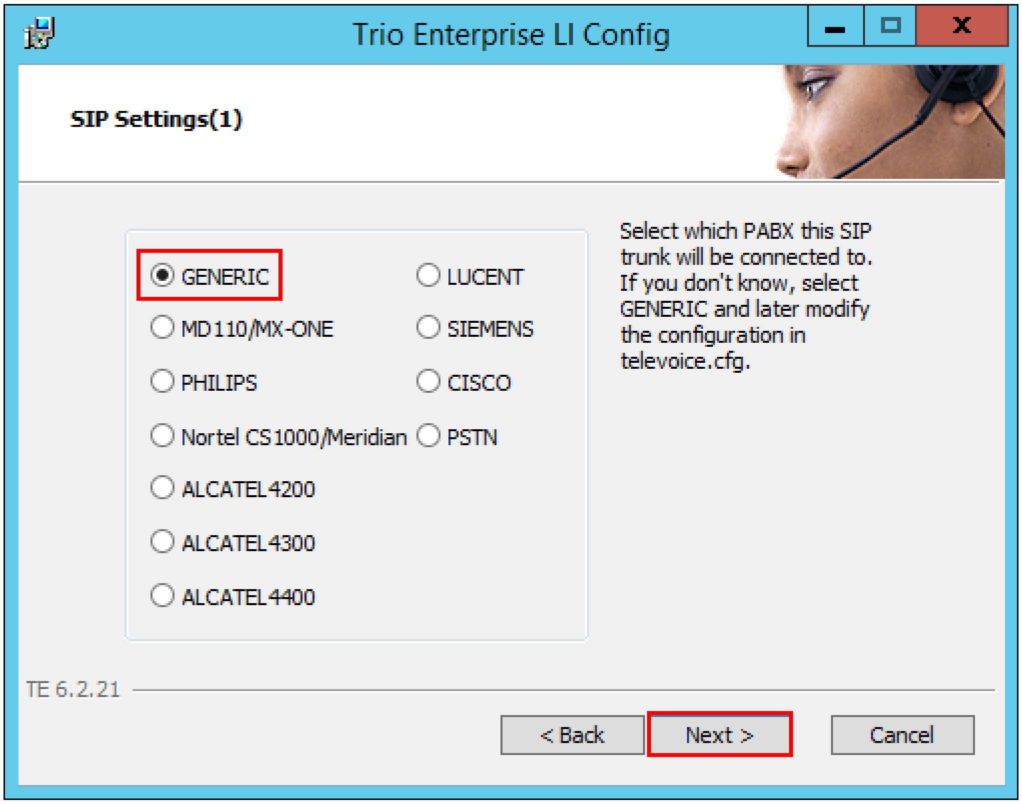
Launch the Trio configuration application. Select **Start → Programs → Trio Enterprise → TeleVoice Config** (not shown). The configuration of the application starts, and when the new window opens, check the **SIP** check box followed by the **Next** button.



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



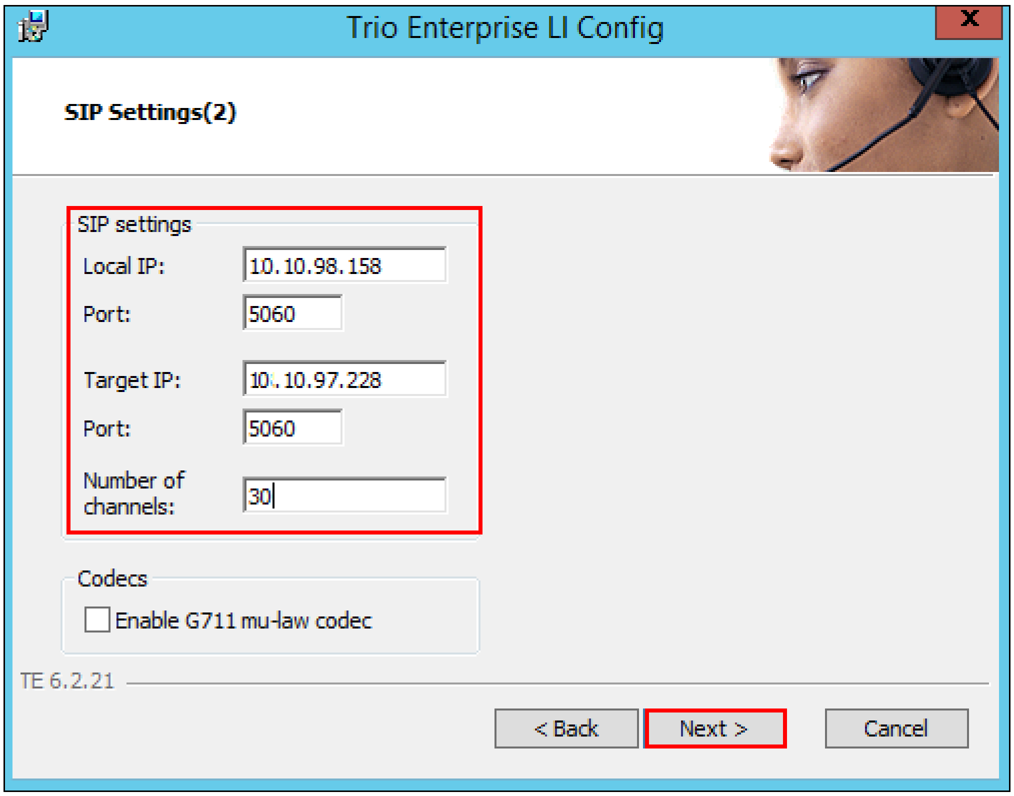
In the subsequent window click on the **GENERIC** radio button followed by the **Next** button to continue.



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 Session Manager (procr IP address)
- **Port** Enter the SIP Port 5060
- **Number of channels** Enter **30** as the number of channels

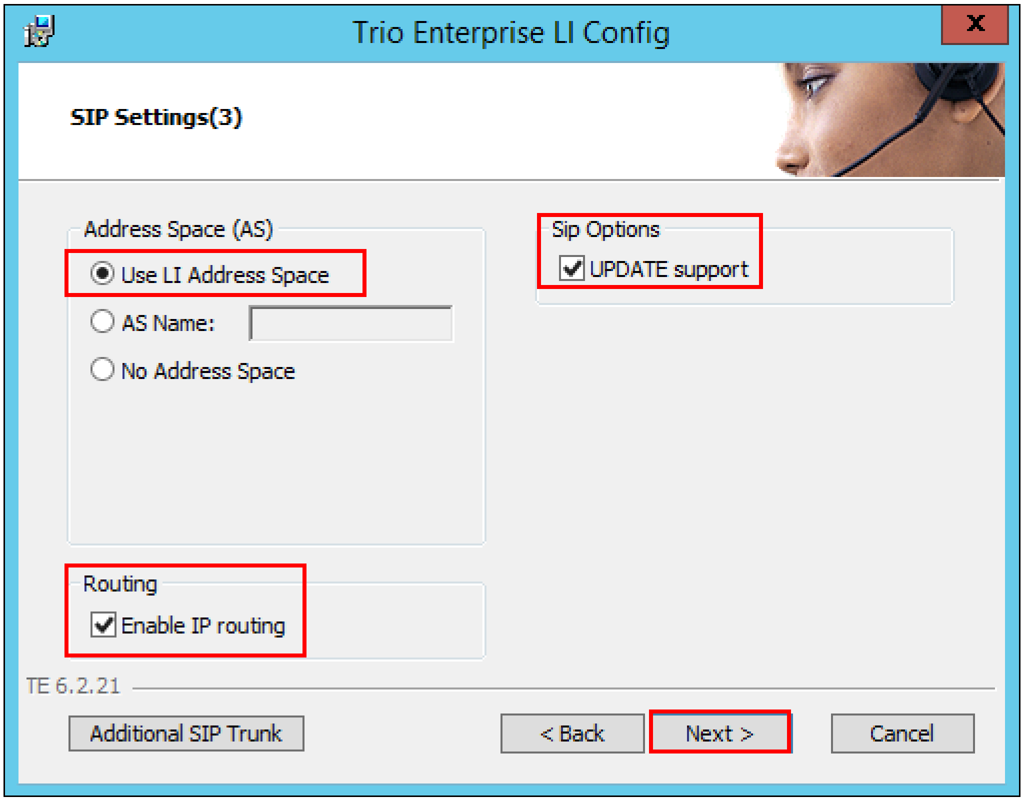
Click on the **Next** button to continue.



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

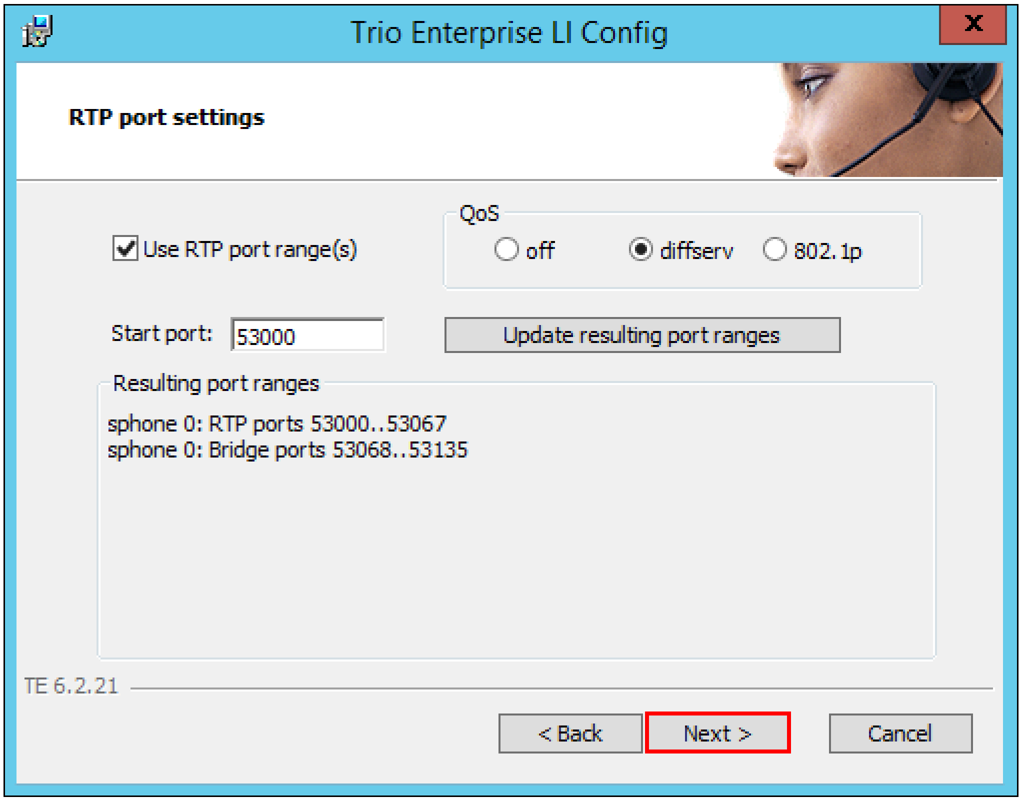
Click on the **Next** button to continue.



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**

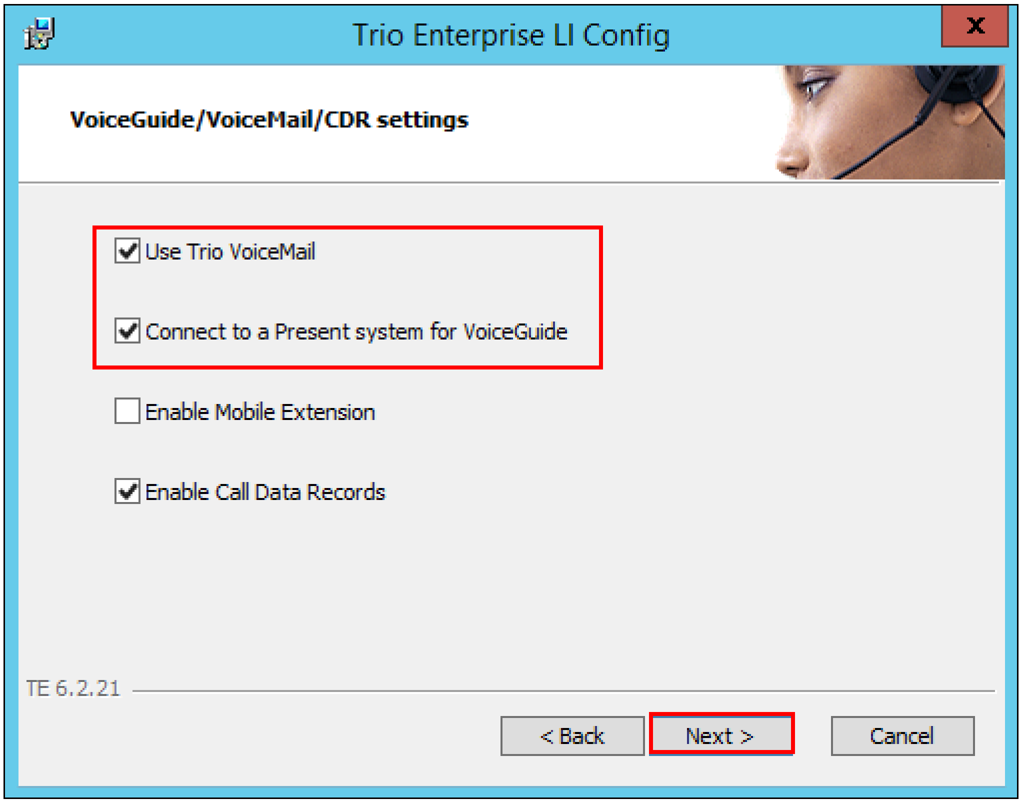
Click on the **Next** button to continue.



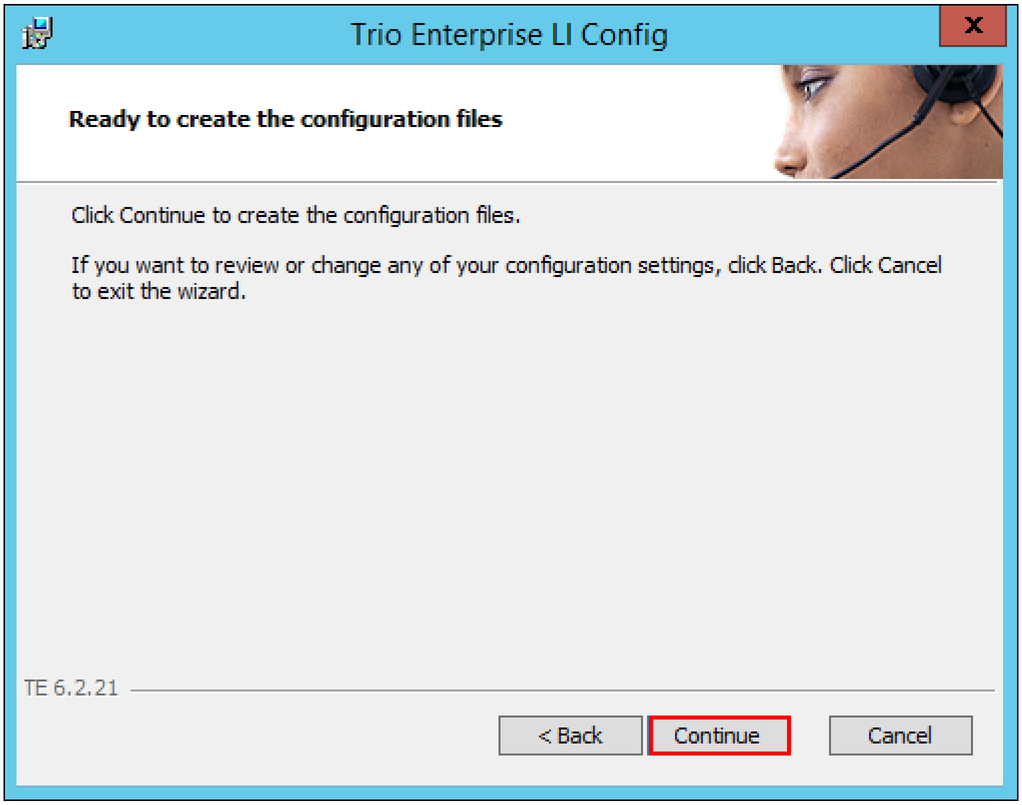
In the subsequent window enter the following settings:

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

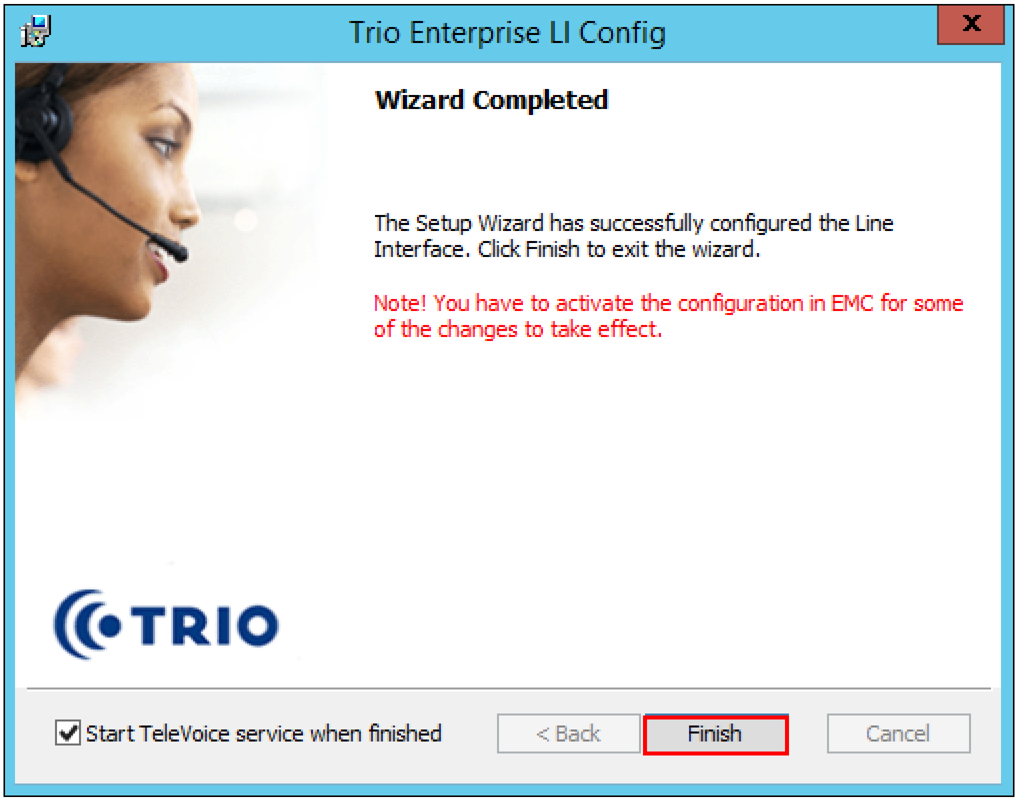
Click on the **Next** button to continue.



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 C:\TE\ProgramData\LI\templates folder.

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

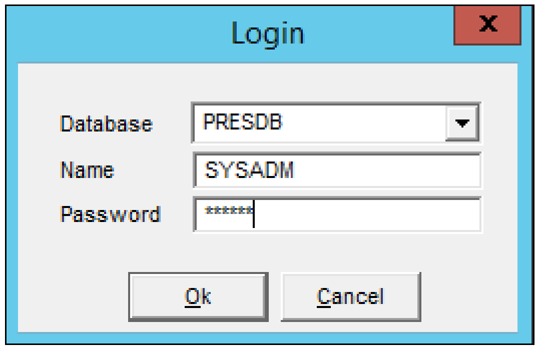
```
[sip_1]
                              signallingprotocol=sip
                              localHost=10.10.98.158
                              targetHost=10.10.97.228
                              uriScheme=1
                              transferPoint=afterAnswer
                              update=1
                              usetcp=1
```

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

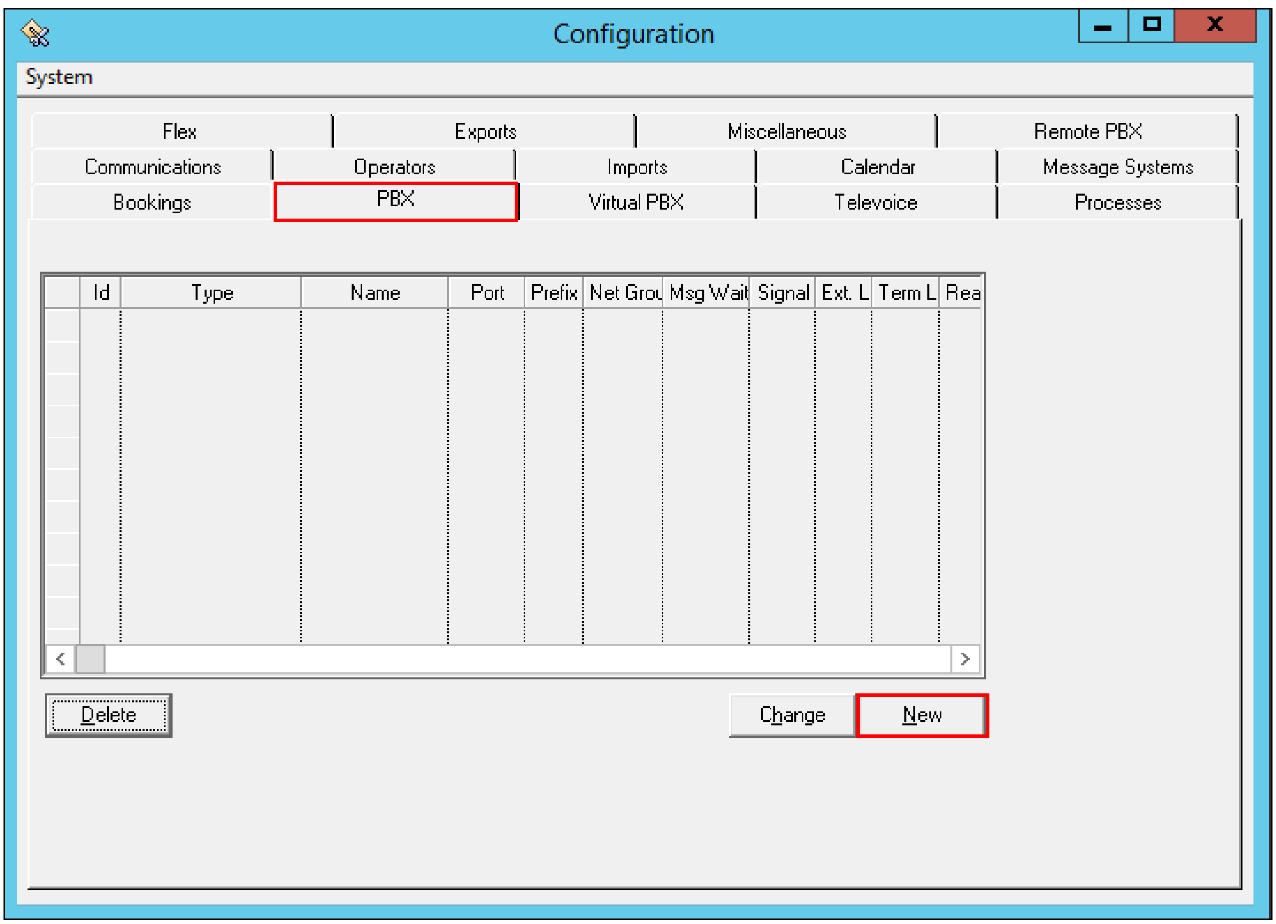
```
[device_0]
                              type=sphone
                              access=127.0.0.1:33109
                              voiceserver_1=localhost:33813
                              sphone=0
                              localip=10.10.98.158
                              mf=SipGw_QSIG=0x3ff
                              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.



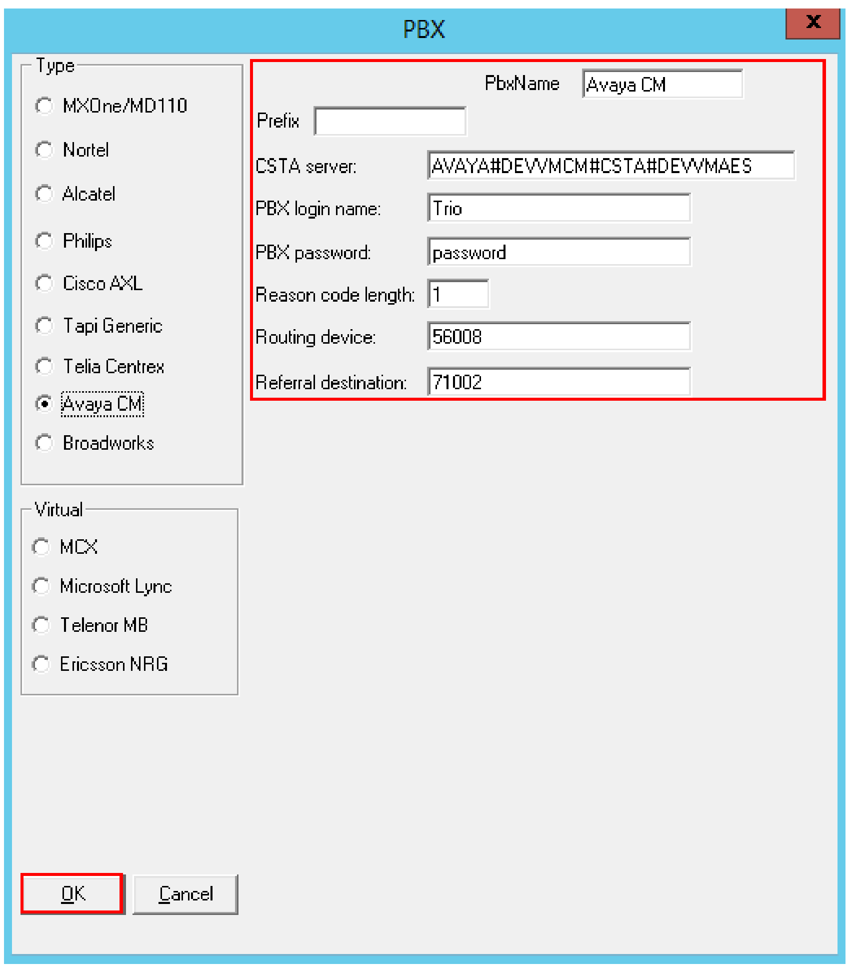
From the screen shown below, select **PBX** and then click on **New**.



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

- **Type** Click on the **Avaya CM** radio button
- **PbxName** Enter an informative name
- **CSTA server** Enter the appropriate Tlink name as seen in **Section 6.77**.
- **PBX login name** Enter the CTI Username as configured in **Section 6.5**
- **PBX password** Enter the CTI password as configured in **Section 6.5**
- **Reason code length** Enter **1**
- **Routing device** Enter the extension assigned to the diversion VDN used for activating referrals from the phone set as configured in **Section 5.16.2** and **5.16.3**.
- **Referral destination** Enter the number 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.



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).

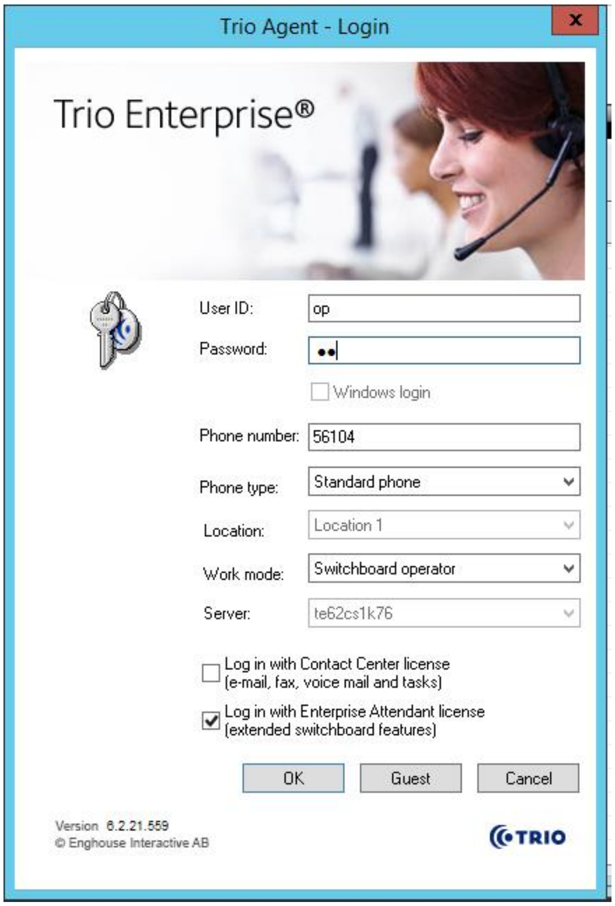
When the Trio Agent window opens enter the following:

- **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** Enter the Communication Manager extension number that will be used as the agent's audio device (number 56104 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.



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

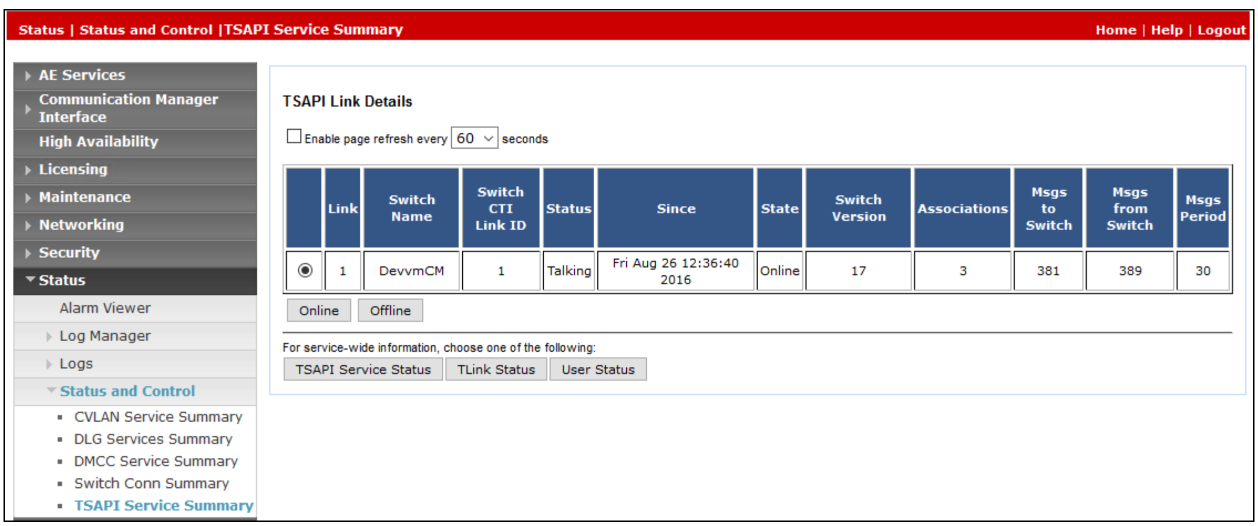
The following steps can ensure that the communication between Communication Manager and the Application Enablement Services server is functioning correctly. Using SAT, connect to Communication Manager and check the AESVCS link status with Application Enablement Services by using the command “status aesvcs 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   Version  Mnt   AE Services      Service       Msgs     Msgs
Link           Busy  Server           State         Sent     Rcvd

1     7        no    devvmaes         established   388      379
```

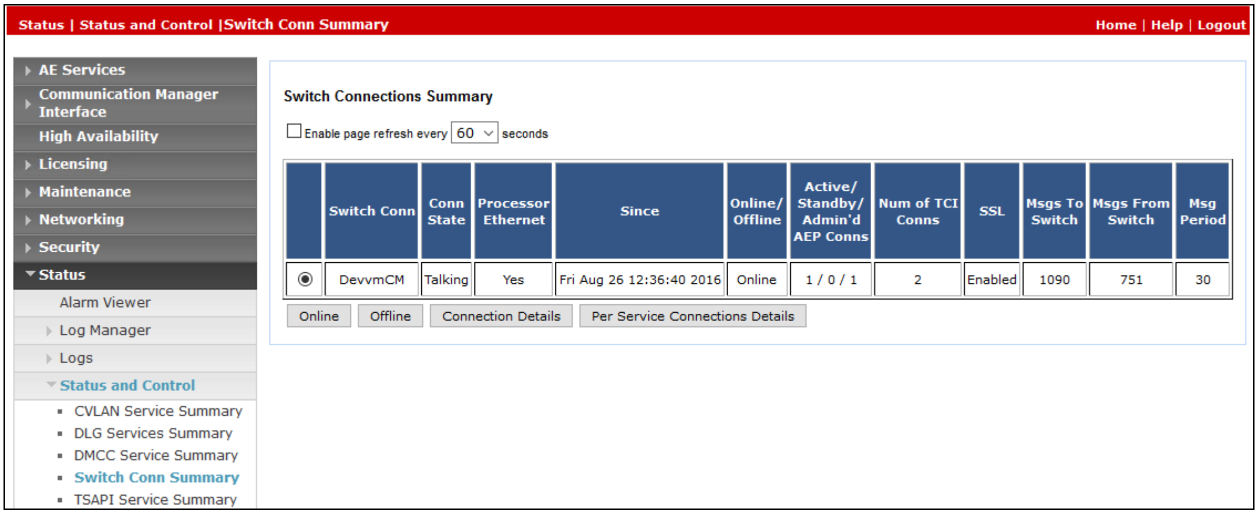
9.2. Verify Avaya Aura® Application Enablement Services

On Application Enablement Services, verify the status of the TSAPI link by selecting **Status → Status and Control → TSAPI Service Summary** from the left pane. The **TSAPI Link Details** screen is displayed.

Verify the **Status** is “Talking” for the TSAPI link administered in **Section** Error! Reference source not found.**4**.



Navigate to **Status → Status and Control → Switch Conn Summary**. Verify that **Conn State** is **Talking** and **Online/Offline** is **Online**.



10. Conclusion

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

11. Additional References

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

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

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

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.