DevConnect Program

Application Notes for Enghouse Intuition Advanced Console Version 7 to interoperate with Avaya Aura® Communication Manager Release 10.1, Avaya Aura® Session Manager Release 10.1 – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for Intuition Advanced Console 7 to interoperate with Avaya Aura® Communication Manager and Avaya Aura® Session Manager.

Readers should pay attention to **Section 2**, in particular the scope of testing as outlined in **Section 2.1** as well as any 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 Avaya DevConnect Program.

1. Introduction

These Application Notes outline the steps necessary to configure Intuition Advanced Console (IAC) from Enghouse Interactive AB to interoperate with Avaya Aura® Communication Manager (Communication Manager) and Avaya Aura® Session Manager (Session Manager). IAC is a client/server-based application running on Windows Server operating systems. IAC 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. The IAC Attendant client provides a view of contacts, schedules, and communication tasks and was installed on the same server as the IAC server but can be installed on a separate platform if required. IAC connects to the Communication Manager using a SIP trunk via Session Manager.

2. General Test Approach and Test Results

The general test approach was to configure a simulated enterprise voice network using Communication Manager. The IAC 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 IAC. Calls placed to the IAC server automatically places a call to the telephone the Attendant is using for answering purposes. When the attendant answers the call the IAC server bridges the two calls. When the attendant extends the call to another telephone, IAC server performs a SIP Refer method, and the caller and the called user are now directly connected.

It is possible to have multiple IAC 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 IAC did not include use of any specific encryption features as requested by Enghouse.

2.1. Interoperability Compliance Testing

The interoperability compliance testing included feature and serviceability testing. The serviceability testing introduced failure scenarios to see if the IAC server could resume after a link failure with Communication Manager. The testing included:

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

2.2. Test Results

The tests were all functional in nature and performance testing was not included. All test cases passed successfully.

2.3. Support

For technical support for Enghouse Intuition Advanced Console product, please use the following web link. https://enghouseinteractive.com/about-us/customer-support/

Enghouse Interactive AB can also be contacted as follows.
Phone: +1 800-513-2810
Fax: +46 (0)8 31 87 00
E-mail: Hello@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 IAC server via Session Manager. Avaya H.323 and SIP stations were used as the IAC Attendant telephones during compliance testing. SIP and H.323 stations were configured on Communication Manager to generate outbound/inbound calls to/from the PSTN. The simulated enterprise voice has SIP trunk to PSTN through Avaya Session Border Controller.

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

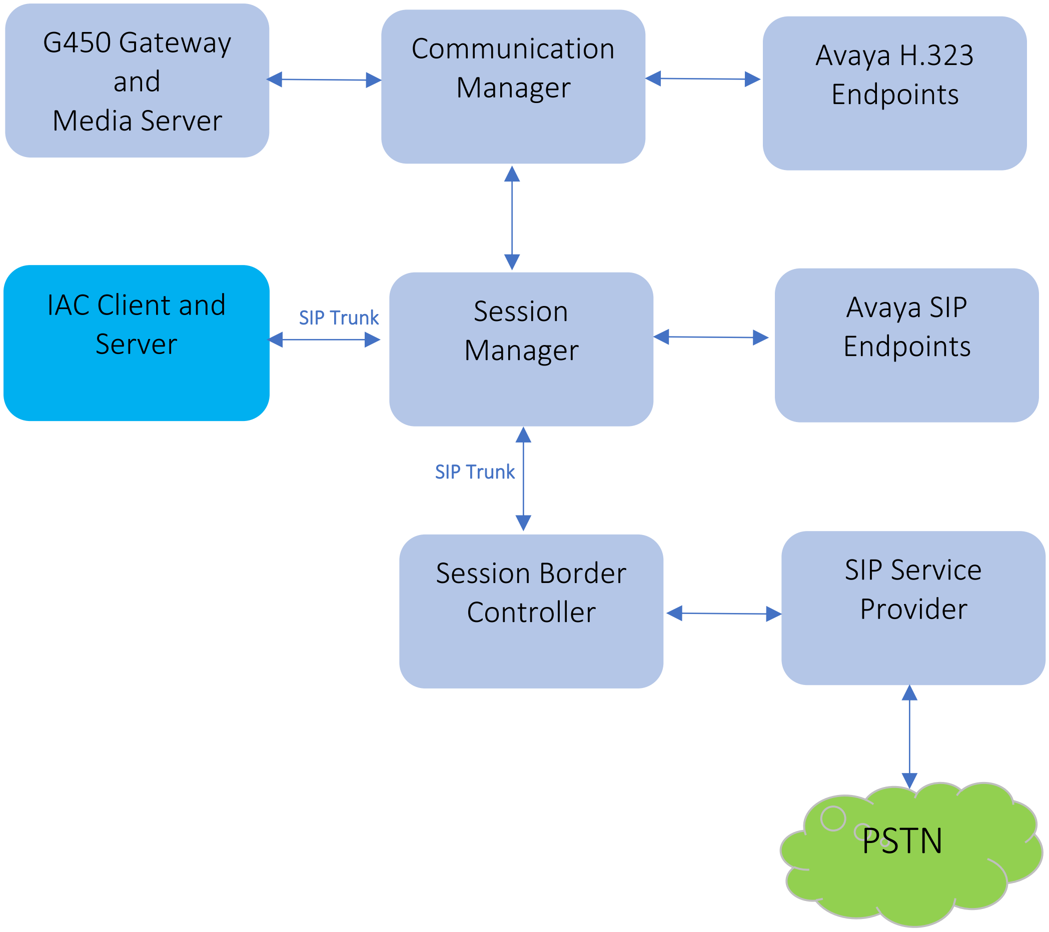


Figure 1: Test Configuration Diagram

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya Aura® Communication Manager	10.1.2.0 FP2 01.0.974.0-27783
Avaya G450 Media Gateway	FW 42.18.0
Avaya Aura® Media Server	10.1.0.125
Avaya Aura® System Manager	10.1.2.0 Feature Pack 2 10.1.2.0.0715476
Avaya Aura® Session Manager	10.1.2.0 Feature Pack 2 10.1.0.02.1012016
Avaya Session Border Controller	10.1.1.0-35-21872
Avaya 96x1 Series IP Deskphones	6.8.5.4.10 (H.323)
Avaya 96x1 Series IP Deskphones	7.1.15.2.1 (SIP)
Avaya J100 Series SIP Deskphones	4.1.0.0.9
Avaya Workplace for Windows Softphone	3.32.0.75
Enghouse Intuition Advanced Console	7.0

5. Configure Avaya Aura® Communication Manager

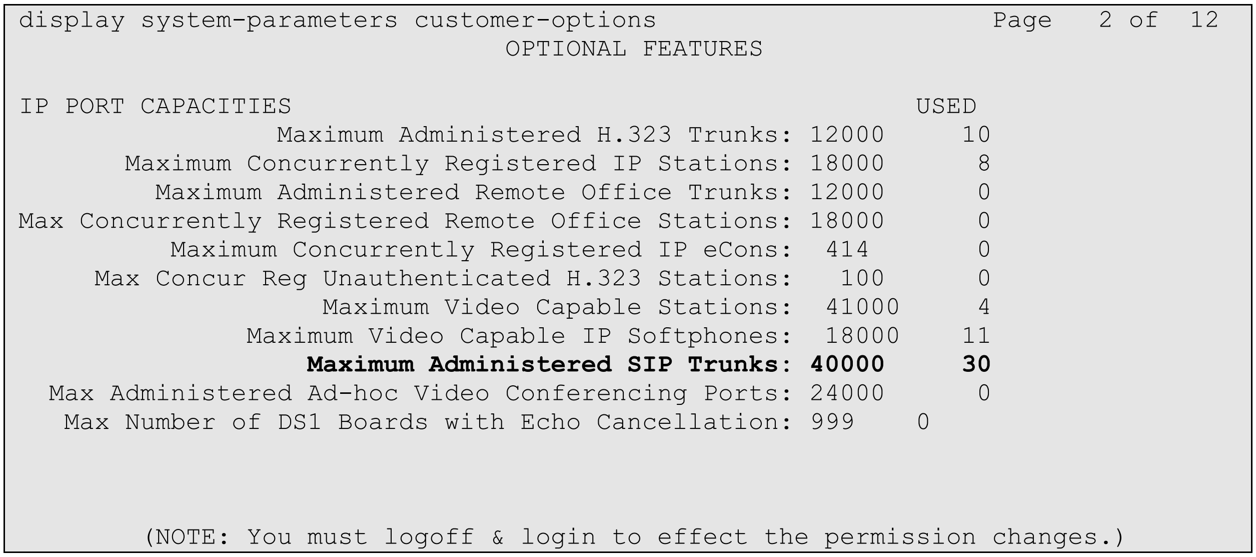
Configuration and verification operations on Communication Manager illustrated in this section were all performed using Avaya Site Administrator Emulation Mode. The information provided in this section describes the configuration of Communication Manager for this solution. For all other provisioning information such as initial installation and configuration, please refer to the product documentation in **Section 10**.

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 Signaling group
- Administer SIP Trunk Group
- Administer IP Network Region
- Administer IP Codec Set
- Administer Route Pattern
- Administer Private Numbering
- Administer Dialing Plan

5.1. Verify License

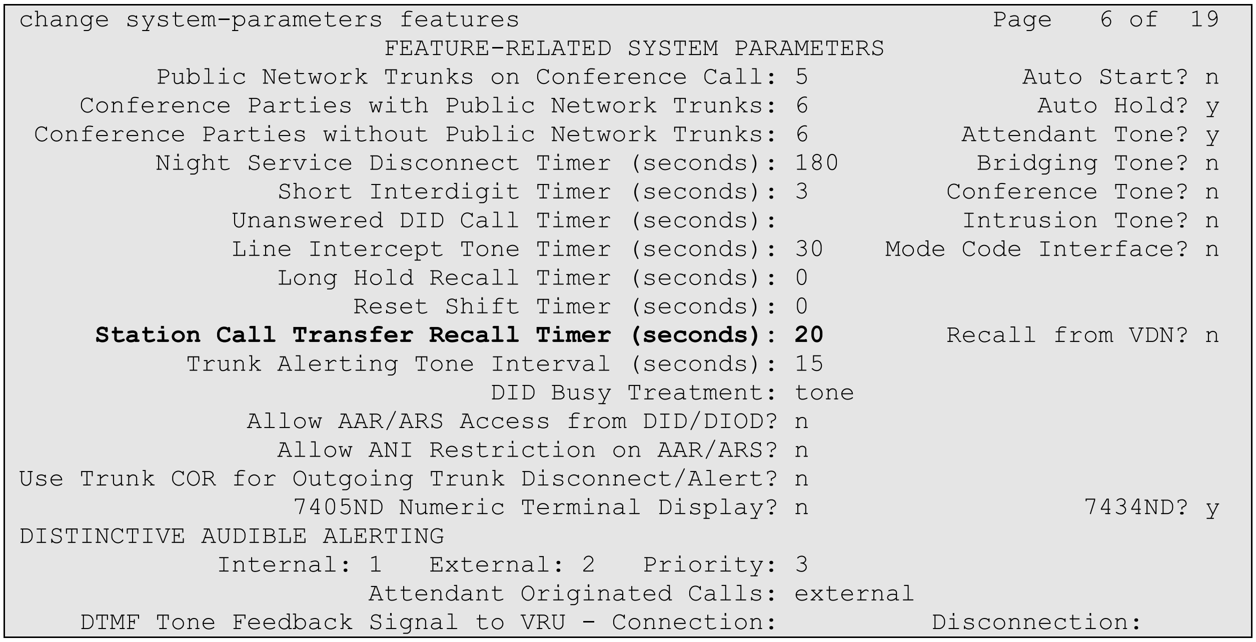
Log in to the System Access Terminal to verify that the Communication Manager license has proper permissions for features illustrated in these Application Notes. Use the “display system-parameters customer-options” command. Navigate to **Page 2** and verify that there is sufficient remaining capacity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



```
display system-parameters customer-options                      Page   2 of  12
                                OPTIONAL FEATURES

IP PORT CAPACITIES                                          USED
                 Maximum Administered H.323 Trunks: 12000     10
       Maximum Concurrently Registered IP Stations: 18000      8
         Maximum Administered Remote Office Trunks: 12000      0
Max Concurrently Registered Remote Office Stations: 18000      0
          Maximum Concurrently Registered IP eCons:  414       0
     Max Concur Reg Unauthenticated H.323 Stations:   100      0
                    Maximum Video Capable Stations:  41000     4
               Maximum Video Capable IP Softphones:  18000    11
                   Maximum Administered SIP Trunks: 40000     30
  Max Administered Ad-hoc Video Conferencing Ports: 24000      0
   Max Number of DS1 Boards with Echo Cancellation: 999    0



        (NOTE: You must logoff & login to effect the permission changes.)
```

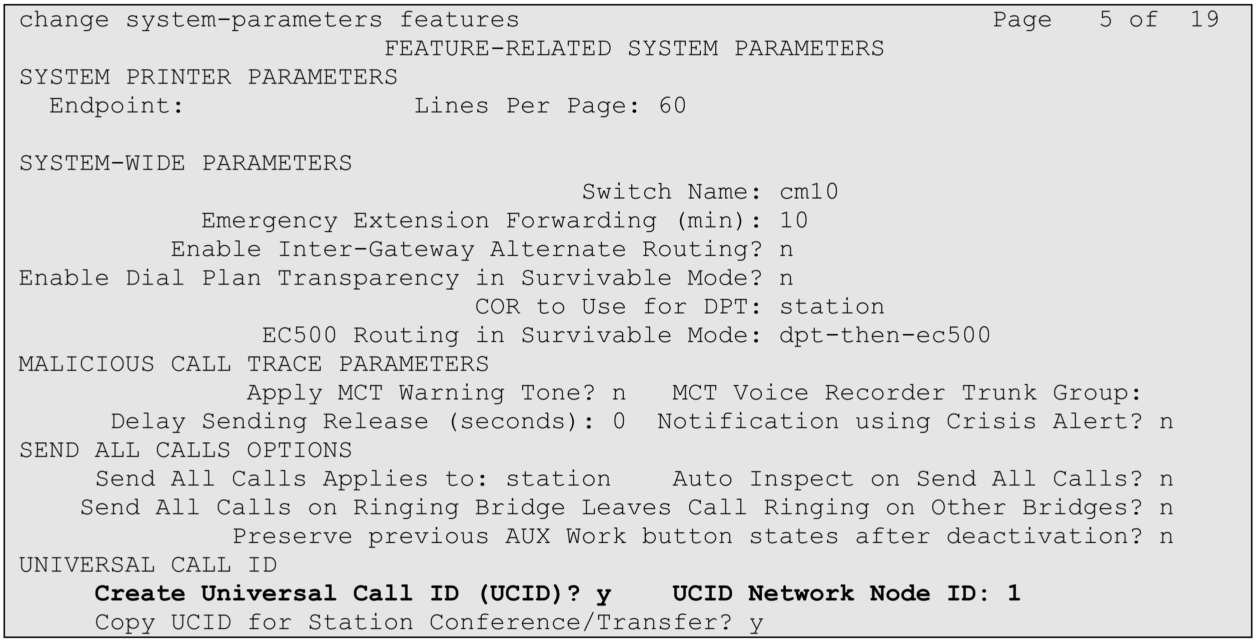
5.2. Administer System Parameter Features

During compliance testing IAC 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**.



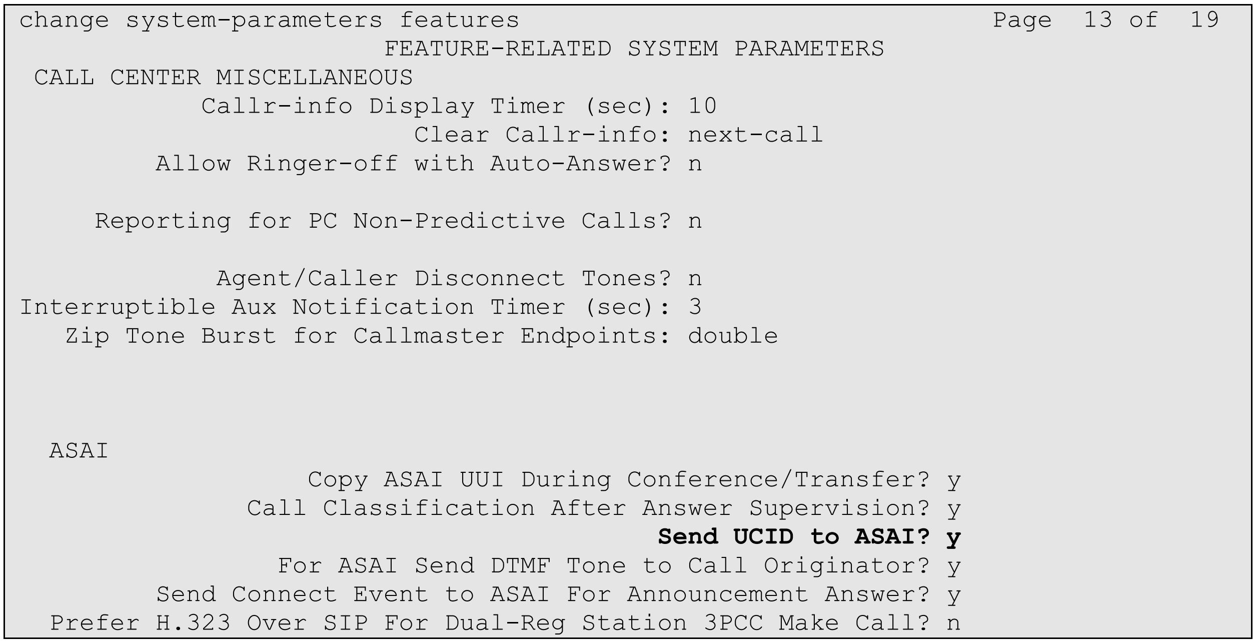
```
change system-parameters features                               Page   6 of  19
                        FEATURE-RELATED SYSTEM PARAMETERS
         Public Network Trunks on Conference Call: 5              Auto Start? n
    Conference Parties with Public Network Trunks: 6               Auto Hold? y
 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
DISTINCTIVE AUDIBLE ALERTING
             Internal: 1   External: 2   Priority: 3
                       Attendant Originated Calls: external
    DTMF Tone Feedback Signal to VRU - Connection:         Disconnection:
```

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



```
change system-parameters features                               Page   5 of  19
                        FEATURE-RELATED SYSTEM PARAMETERS
SYSTEM PRINTER PARAMETERS
  Endpoint:               Lines Per Page: 60

SYSTEM-WIDE PARAMETERS
                                     Switch Name: cm10
            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  Notification using Crisis Alert? n
SEND ALL CALLS OPTIONS
     Send All Calls Applies to: station    Auto Inspect on Send All Calls? n
    Send All Calls on Ringing Bridge Leaves Call Ringing on Other Bridges? n
              Preserve previous AUX Work button states after deactivation? n
UNIVERSAL CALL ID
     Create Universal Call ID (UCID)? y    UCID Network Node ID: 1
     Copy UCID for Station Conference/Transfer? y
```

Navigate to **Page 13** and enable **Send UCID to ASAI**. This parameter allows for the universal call ID to be sent to ICA 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 UUI During Conference/Transfer? y
               Call Classification After Answer Supervision? y
                                          Send UCID to ASAI? y
                 For ASAI Send DTMF Tone to Call Originator? y
         Send Connect Event to ASAI For Announcement Answer? y
  Prefer H.323 Over SIP For Dual-Reg Station 3PCC Make Call? n
```

5.3. Administer IP Node Names

Use the “change node-names ip” command (not shown) and add an entry for Session Manager. In this case, **SM10** and **10.33.1.42** are entered as **Name** and **IP Address**. Note the **procr** and **10.33.1.43** 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 0**.

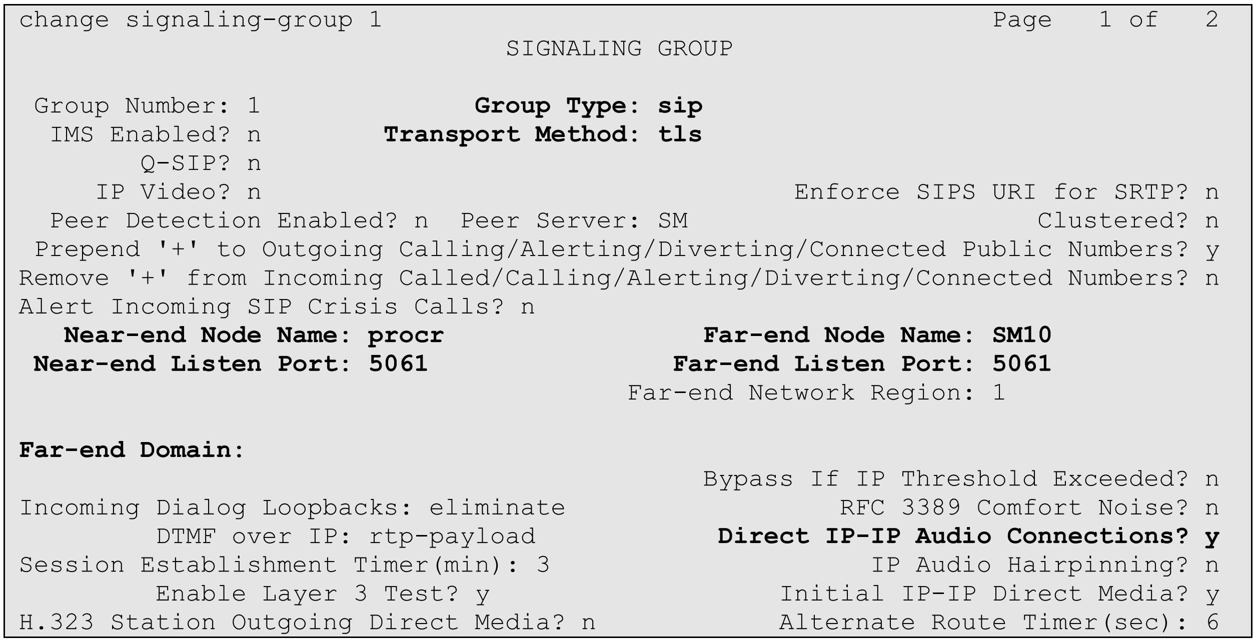
```
change node-names ip                                              Page   1 of   2
                                  IP NODE NAMES
    Name                 IP Address
SM10                    10.33.1.42
default                 0.0.0.0
lsp                     10.33.1.7
procr                   10.33.1.43
( 16 of 18   administered node-names were displayed )
Use 'list node-names' command to see all the administered node-names
Use 'change node-names ip xxx' to change a node-name 'xxx' or add a node-name
```

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:** “tls”.
- **Near-end Node Name:** An existing C-LAN node name or “procr” from **Section 0**.
- **Far-end Node Name:** The existing node name for Session Manager from **Section 0**.
- **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:** Leave this field empty as CM accepts any incoming call.
- **Direct IP-IP Audio Connections?:** “y”.

Note: If the **Far-end domain** field is set to a specific domain and incoming call from the ICA server has a different domain such as having IP address in the URI, the incoming call is rejected.



```
change 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? n
  Peer Detection Enabled? n  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: SM10
 Near-end Listen Port: 5061                Far-end Listen Port: 5061
                                        Far-end Network Region: 1

Far-end Domain:
                                             Bypass If IP Threshold Exceeded? n
Incoming Dialog Loopbacks: eliminate                  RFC 3389 Comfort Noise? n
         DTMF over IP: rtp-payload            Direct IP-IP Audio Connections? y
Session Establishment Timer(min): 3                     IP Audio Hairpinning? n
         Enable Layer 3 Test? y                   Initial IP-IP Direct Media? y
H.323 Station Outgoing Direct Media? n            Alternate Route Timer(sec): 6
```

5.5. Administer SIP Trunk Group

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

- **Group Type:** “sip”.
- **Group Name:** A descriptive name.
- **TAC:** An available trunk access code.
- **Service Type:** “tie”.
- **Signaling Group:** Set it to the signaling group number 1 as defined in **Section 5.4**.
- **Number of Members:** Enter a number of SIP trunk, in this case 10 SIP trunk members used.

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

Group Number: 1                    Group Type: sip           CDR Reports: y
  Group Name: Private Trunk               COR: 1        TN: 1        TAC: #01
   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
```

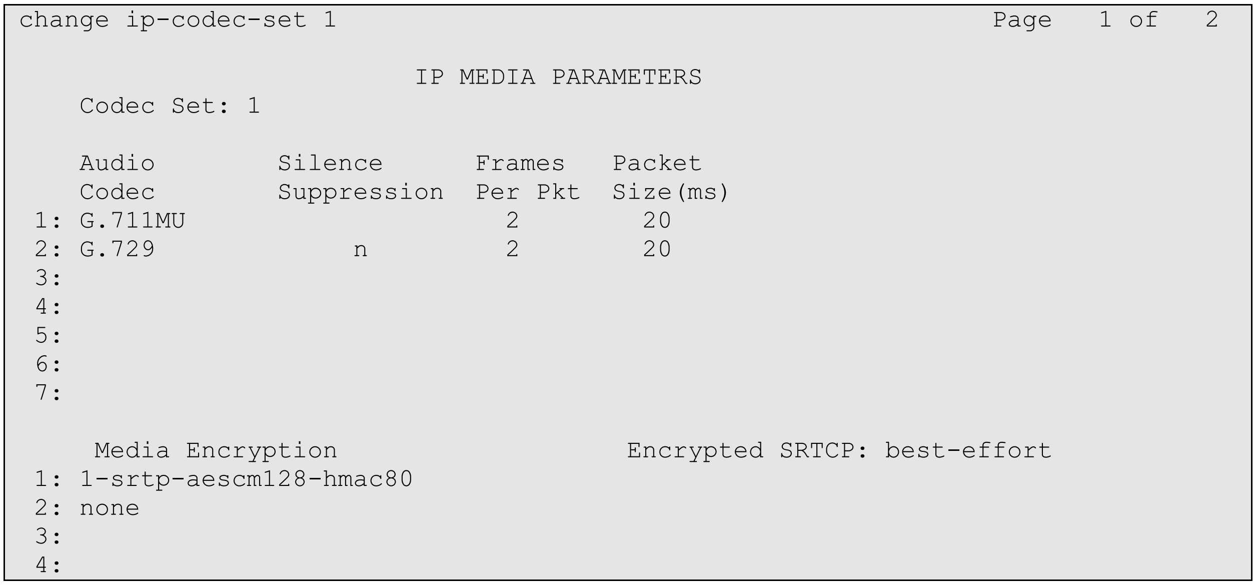
5.6. Administer IP Network Region

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 IAC.

```
change ip-network-region 1                                      Page   1 of  20
                               IP NETWORK REGION
  Region: 1       NR Group: 1
Location: 1       Authoritative Domain: avayalab.com
    Name: Loc-1                 Stub Network Region: n
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: yes
      Codec Set: 1              Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 2048                      IP Audio Hairpinning? n
   UDP Port Max: 3329
DIFFSERV/TOS PARAMETERS
 Call Control PHB Value: 46
        Audio PHB Value: 46
        Video PHB Value: 26
802.1P/Q PARAMETERS
 Call Control 802.1p Priority: 6
        Audio 802.1p Priority: 6
        Video 802.1p Priority: 5      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                       RSVP Enabled? n
```

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. Configure the codec as shown below. Note that Enghouse supports various codecs in different regions, since the compliance test was done in North America, the G.711 Mulaw was used.

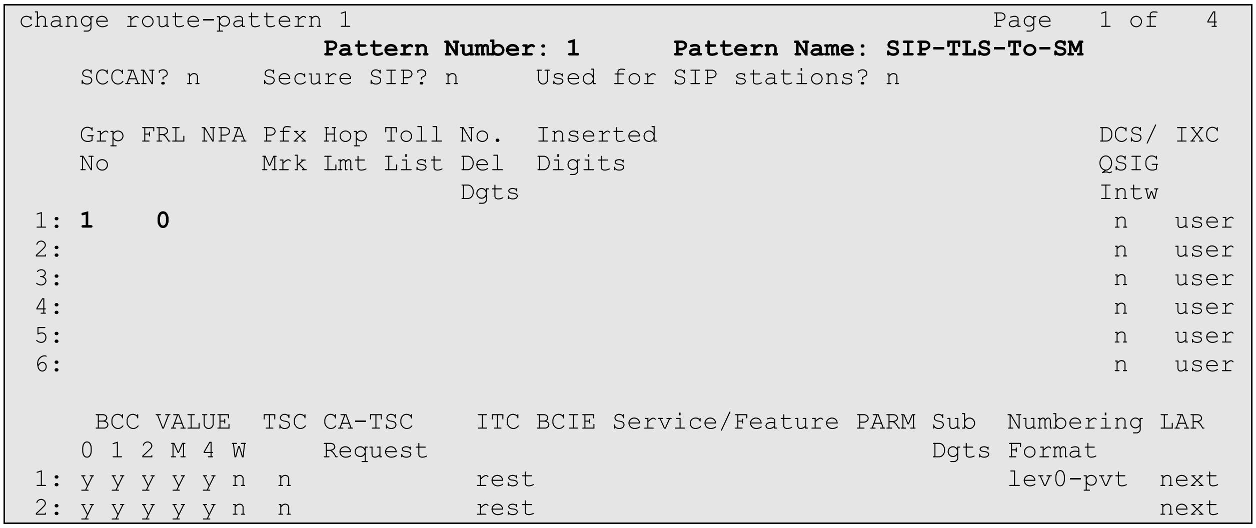


```
change ip-codec-set 1                                           Page   1 of   2

                          IP MEDIA PARAMETERS
    Codec Set: 1

    Audio        Silence      Frames   Packet
    Codec        Suppression  Per Pkt  Size(ms)
 1: G.711MU                     2        20
 2: G.729             n         2        20
 3:
 4:
 5:
 6:
 7:

     Media Encryption                    Encrypted SRTCP: best-effort
 1: 1-srtp-aescm128-hmac80
 2: none
 3:
 4:
```

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 IAC, 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 5.5**.
- **FRL:** A level that allows access to this trunk, with 0 being least restrictive.



```
change route-pattern 1                                          Page   1 of   4
                    Pattern Number: 1      Pattern Name: SIP-TLS-To-SM
    SCCAN? n    Secure SIP? n     Used for SIP stations? n

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

5.9. Administer Private Numbering

Use the “change private-numbering 0” command, to define the calling party number to send to IAC. Add an entry for the trunk group defined in **Section 5.5**. In the example shown below, all calls originating from a 4-digit extension beginning with “3” and routed to trunk group all trunks will result in a 4-digit calling number. The calling party number will be in the SIP “From” header.

```
change private-numbering 0                                      Page   1 of   2
                           NUMBERING - PRIVATE FORMAT

Ext Ext                 Trk        Private          Total
Len Code                Grp(s)     Prefix           Len
 4  3                                               4  Total Administered: 15
```

5.10.Administer Dialing Plan

Use the “change dialplan analysis” command to add a dialing entry “52” with 4-digit length and AAR call type used to route calls to the IAC server.

```
change dialplan analysis                                        Page   1 of  12
                             DIAL PLAN ANALYSIS TABLE
                                   Location: all          Percent Full: 6

    Dialed   Total  Call      Dialed   Total  Call      Dialed   Total  Call
    String   Length Type      String   Length Type      String   Length Type
 0             1  udp       40           4  aar       78           5  aar
 0             3  fac       411          3  udp       8            1  fac
 1             4  ext       43           4  aar       9            1  fac
 1             11 udp       44           4  udp       *            3  dac
 52            4  aar       441          12 udp       #            3  dac
```

Use the “change aar analysis 0” command and add an entry in the AAR table to specify how to route calls to 52xx. In the example shown below, calls with digits 52 will be routed as an AAR call using route pattern “1” from **Section 5.8**.

```
change aar analysis 5                                      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
    52                    4    4     1        aar          n
```

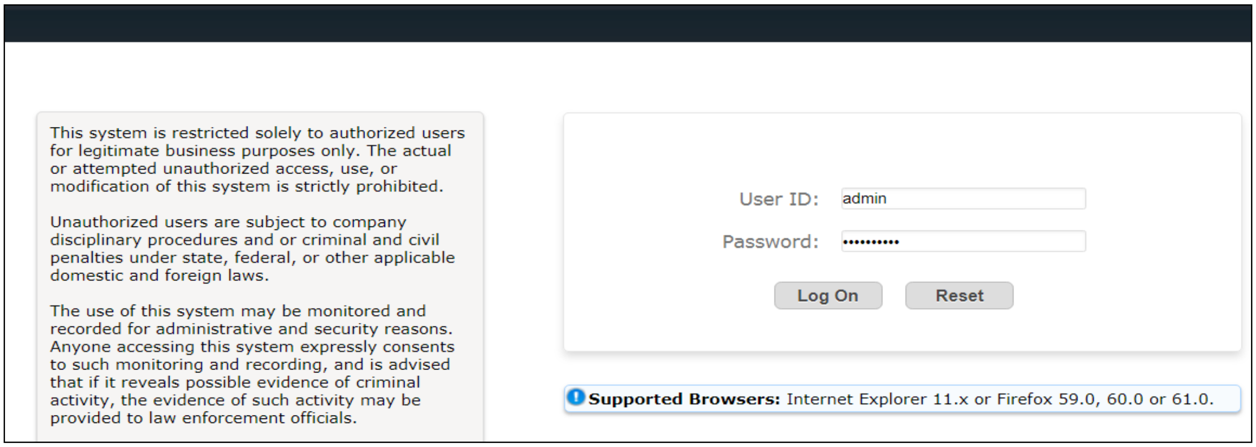
6. Configure Avaya Aura® Session Manager

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

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

6.1. Launch System Manager

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



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

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

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

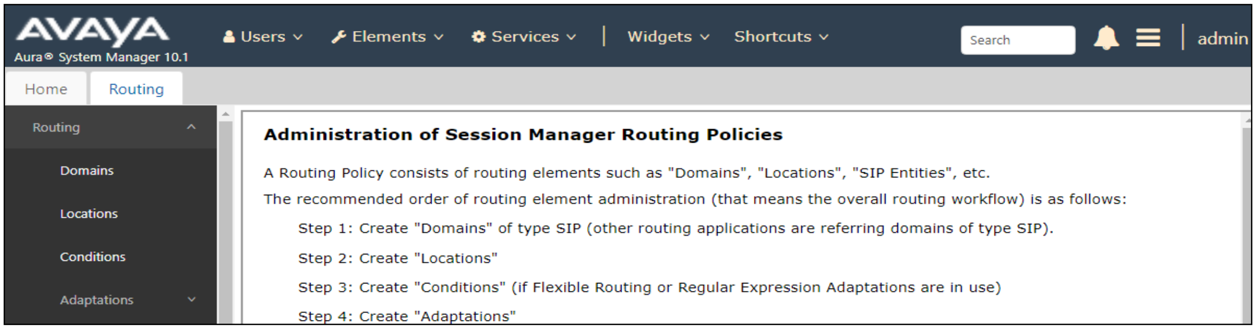
User ID: admin

Password: ••••••••••

Supported Browsers: Internet Explorer 11.x or Firefox 59.0, 60.0 or 61.0.

6.2. Administer Locations

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



Administration of Session Manager Routing Policies

A Routing Policy consists of routing elements such as "Domains", "Locations", "SIP Entities", etc.

The recommended order of routing element administration (that means the overall routing workflow) is as follows:

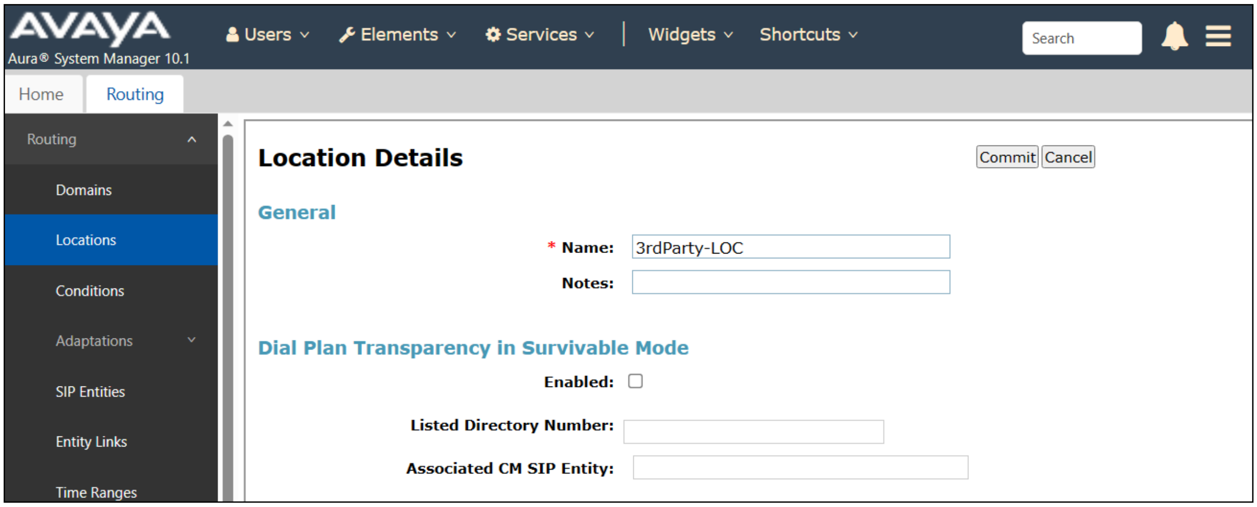
Step 1: Create "Domains" of type SIP (other routing applications are referring domains of type SIP).

Step 2: Create "Locations"

Step 3: Create "Conditions" (if Flexible Routing or Regular Expression Adaptations are in use)

Step 4: Create "Adaptations"

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.



Location Details

General

* Name: 3rdParty-LOC

Notes:

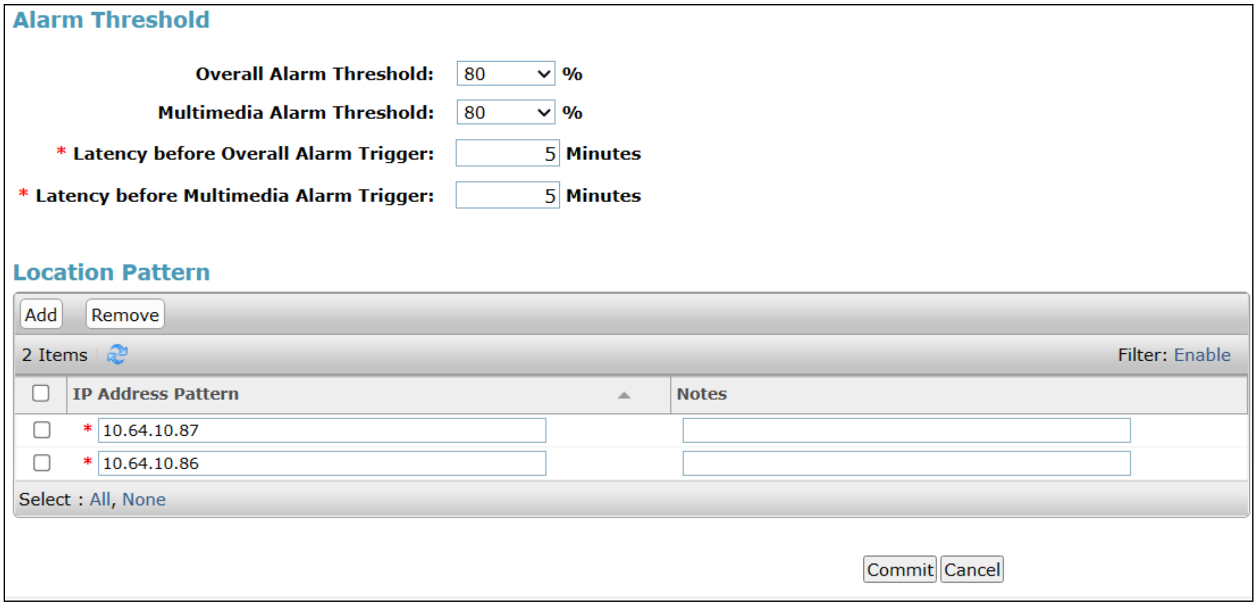
Dial Plan Transparency in Survivable Mode

Enabled: □

Listed Directory Number:

Associated CM SIP Entity:

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



Alarm Threshold

Overall Alarm Threshold: 80 %

Multimedia Alarm Threshold: 80 %

* Latency before Overall Alarm Trigger: 5 Minutes

* Latency before Multimedia Alarm Trigger: 5 Minutes

Location Pattern

2 Items

□	IP Address Pattern	Notes
□	* 10.64.10.87	
□	* 10.64.10.86	

6.3. Administer Adaption

Session Manager can be configured to use Adaptation Modules to modify the From header of the incoming INVITE message sent from Session Manager to the IAC server.

During compliance testing, to make the call from and to Communication Manager via Session Manager, an Adaptation is used to translate the IP address into a domain name for the IAC 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).

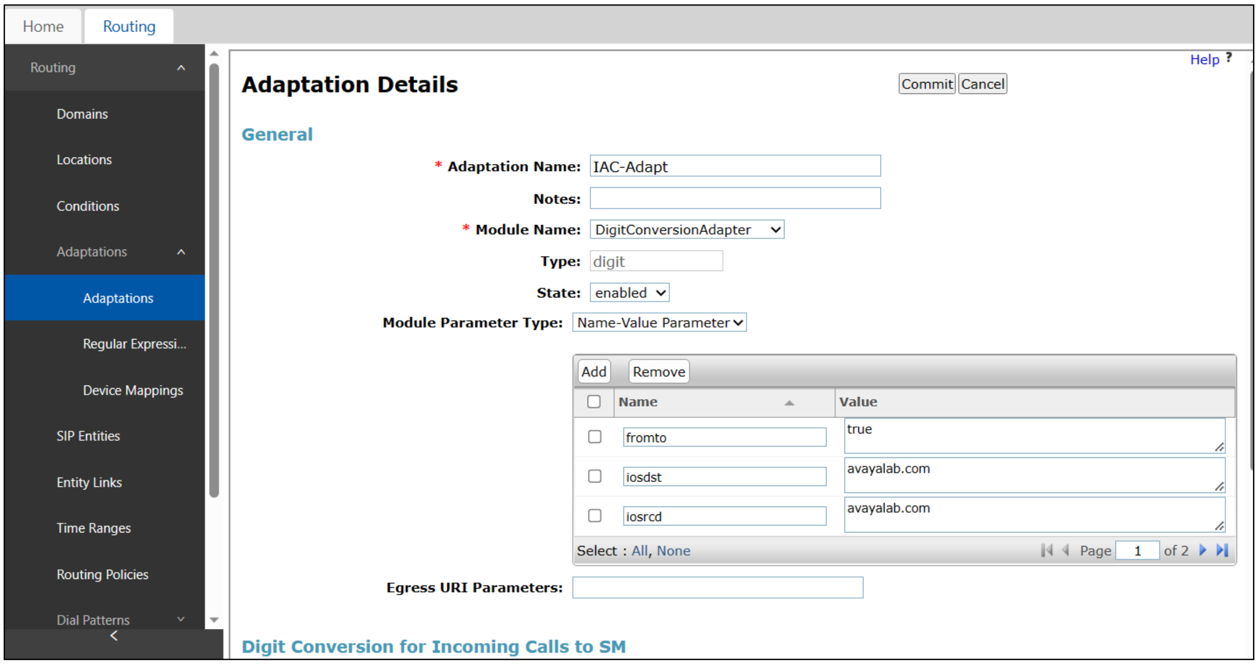
Enter the following for the IAC Adaptation.

- **Adaptation Name:** An informative name (e.g., IAC-Adapt).
- **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.: **avayalab.com**
iosrcd	Enter the domain name of system, e.g.: **avayalab.com**
odstd	Enter IP address of ICA SIP Server, e.g.: **10.64.10.87**
osrcd	Enter IP address of Session Manager Server, e.g.: **10.33.1.42**

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



Adaptation Details

General

* Adaptation Name: IAC-Adapt

Notes:

* Module Name: DigitConversionAdapter

Type: digit

State: enabled

Module Parameter Type: Name-Value Parameter

☐	Name	Value
☐	fromto	true
☐	iosdst	avayalab.com
☐	iosrcd	avayalab.com

Select : All, None Page 1 of 2

Egress URI Parameters:

Digit Conversion for Incoming Calls to SM

6.4. Administer SIP Entities

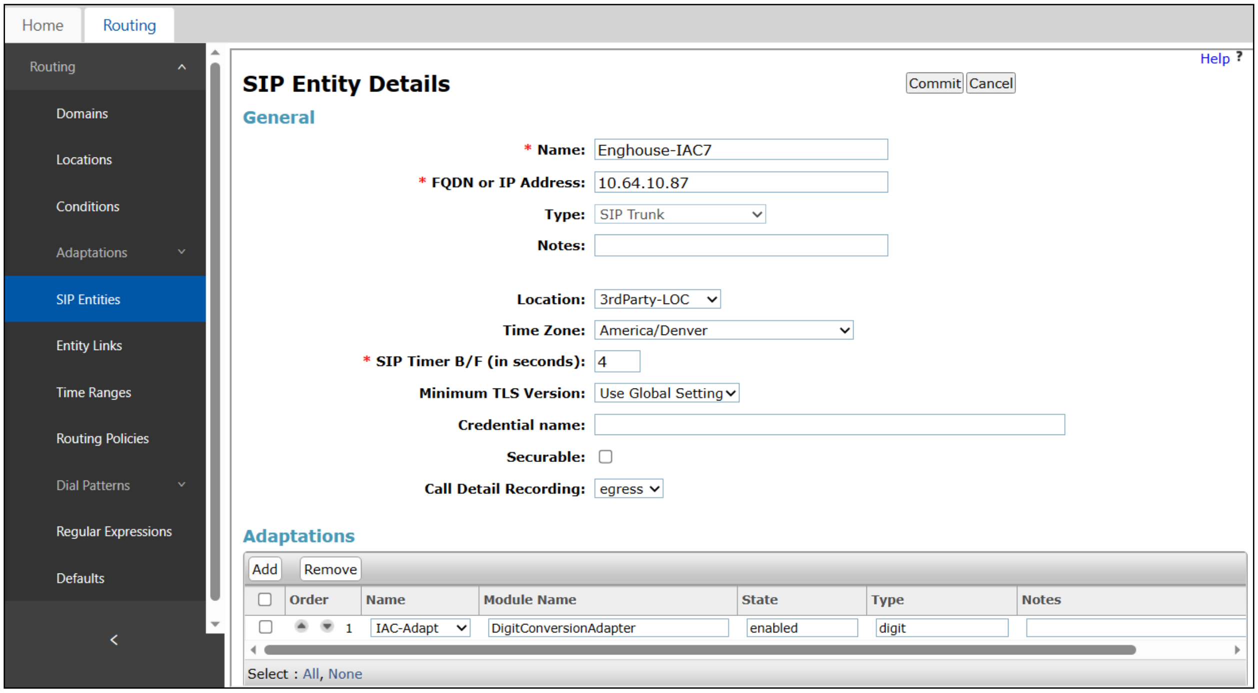
Two SIP entities were added, one for IAC and another one for Communication Manager.

6.4.1. SIP Entity for IAC

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

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 IAC server.
Type:	"SIP trunk"
Notes:	Any desired notes.
Location:	Select the location name as defined from **Section 6.2**.
Time Zone:	Select the applicable time zone.



SIP Entity Details

General

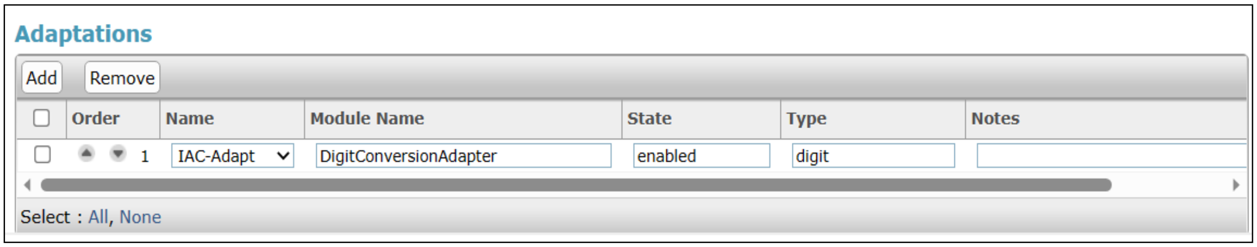
* **Name:**	Enghouse-IAC7
* **FQDN or IP Address:**	10.64.10.87
Type:	SIP Trunk
Notes:	
Location:	3rdParty-LOC
Time Zone:	America/Denver
* **SIP Timer B/F (in seconds):**	4
Minimum TLS Version:	Use Global Setting
Credential name:	
Securable:	□
Call Detail Recording:	egress

Adaptations

□	Order	Name	Module Name	State	Type	Notes
□	1	IAC-Adapt	DigitConversionAdapter	enabled	digit	

Select : All, None

In the **Adaptations** section, select **Add** to add the IAC adaptation as configured in **Section 6.3**.



Adaptations

Add | Remove

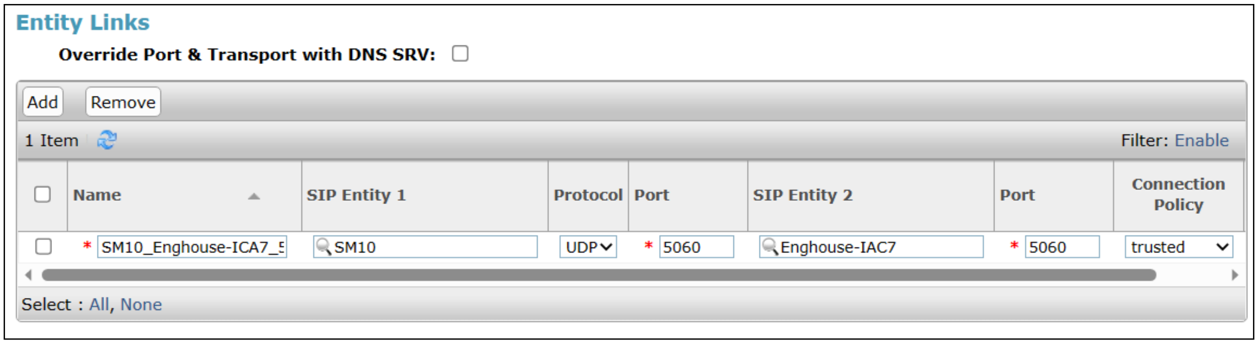
□	Order	Name	Module Name	State	Type	Notes
□	▲ ▼ 1	IAC-Adapt	DigitConversionAdapter	enabled	digit	

Select : All, None

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 "SM10".
- **Protocol:** "UDP"
- **Port:** "5060"
- **SIP Entity 2:** The ICA entity name from this section.
- **Port:** "5060"
- **Connection Policy:** "trusted"

Note that ICA can support UDP and TCP, and the compliance testing used the UCP protocol.



Entity Links

Override Port & Transport with DNS SRV: □

Add | Remove

1 Item Filter: Enable

□	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy
□	* SM10_Enghouse-ICA7_5	SM10	UDP	* 5060	Enghouse-IAC7	* 5060	trusted

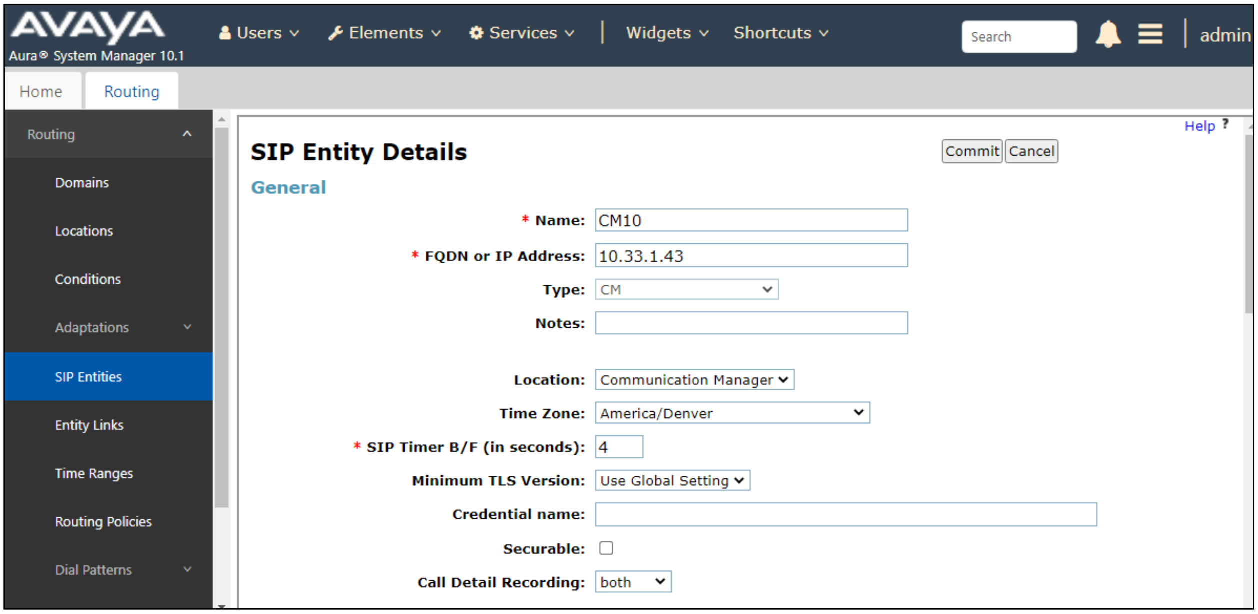
Select : All, None

6.4.2. 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 IAC.

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.



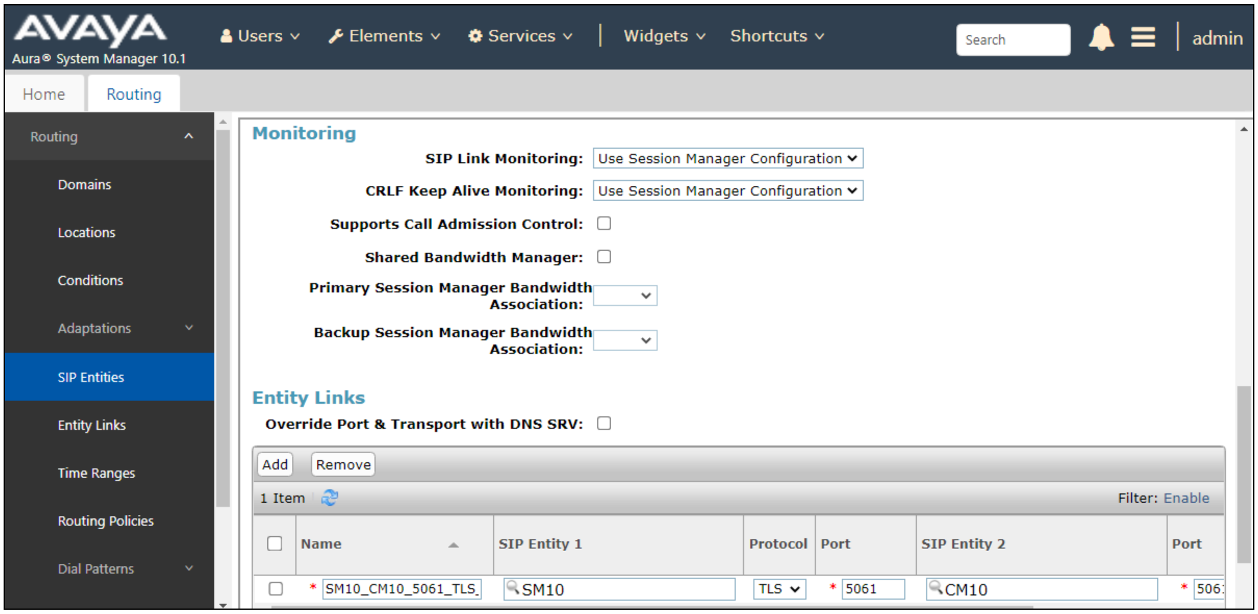
SIP Entity Details

General

* Name:	CM10
* FQDN or IP Address:	10.33.1.43
Type:	CM
Notes:	
Location:	Communication Manager
Time Zone:	America/Denver
* SIP Timer B/F (in seconds):	4
Minimum TLS Version:	Use Global Setting
Credential name:	
Securable:	☐
Call Detail Recording:	both

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 "SM10".
- **Protocol:** Select TLS protocol.
- **Port:** Enter the TLS port 5061.
- **SIP Entity 2:** The Communication Manager entity name from this section.
- **Port:** Enter the TLS port 5061.
- **Connection Policy:** "trusted"



Monitoring

SIP Link Monitoring: Use Session Manager Configuration

CRLF Keep Alive Monitoring: Use Session Manager Configuration

Supports Call Admission Control: □

Shared Bandwidth Manager: □

Primary Session Manager Bandwidth Association:

Backup Session Manager Bandwidth Association:

Entity Links

Override Port & Transport with DNS SRV: □

□	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port
□	* SM10_CM10_5061_TLS_	SM10	TLS	* 5061	CM10	* 506

6.5. Administer Routing Policies

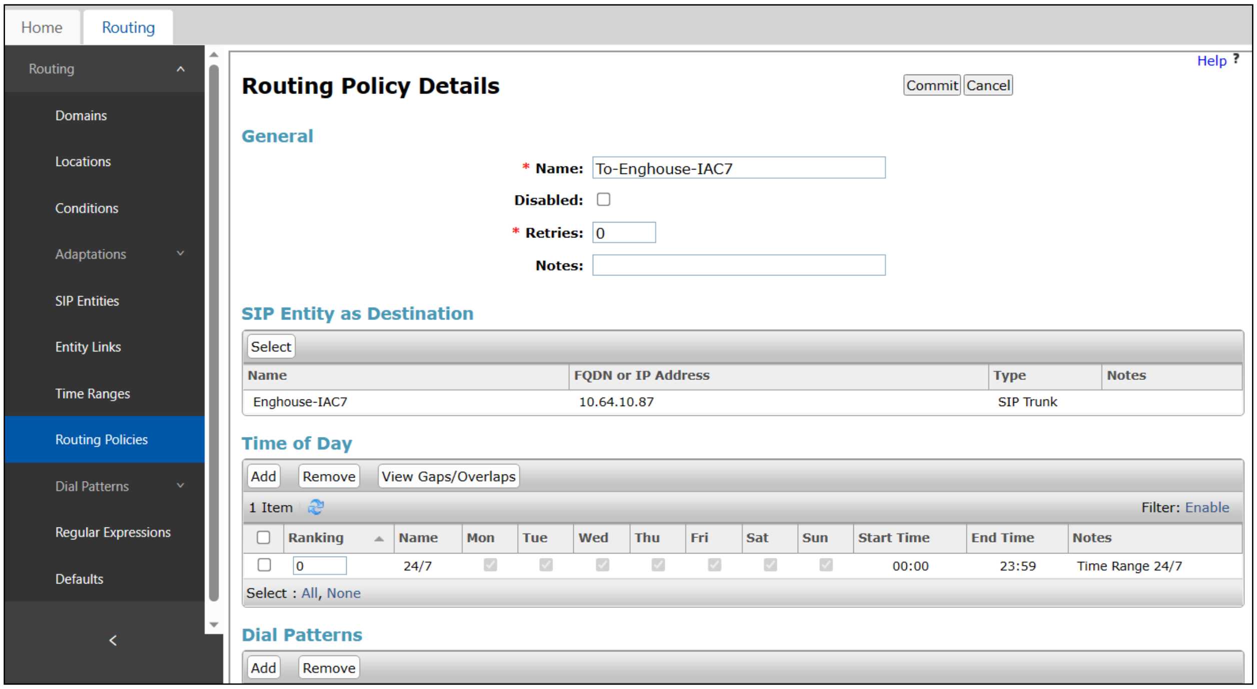
Add two new routing policies, one for IAC and one for the new SIP trunks with Communication Manager.

6.5.1. Routing Policy for IAC

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

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

In the **SIP Entity as Destination** sub-section, click **Select** and select the **Enghouse-IAC7** SIP Entity name from **Section 6.4.1**. The screen below shows the result of the selection.



Routing Policy Details

General

* Name: To-Enghouse-IAC7

Disabled: □

* Retries: 0

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
Enghouse-IAC7	10.64.10.87	SIP Trunk	

Time of Day

Add Remove View Gaps/Overlaps

1 Item Filter: Enable

□	Ranking	Name	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
□	0	24/7	☑	☑	☑	☑	☑	☑	☑	00:00	23:59	Time Range 24/7

Select : All, None

Dial Patterns

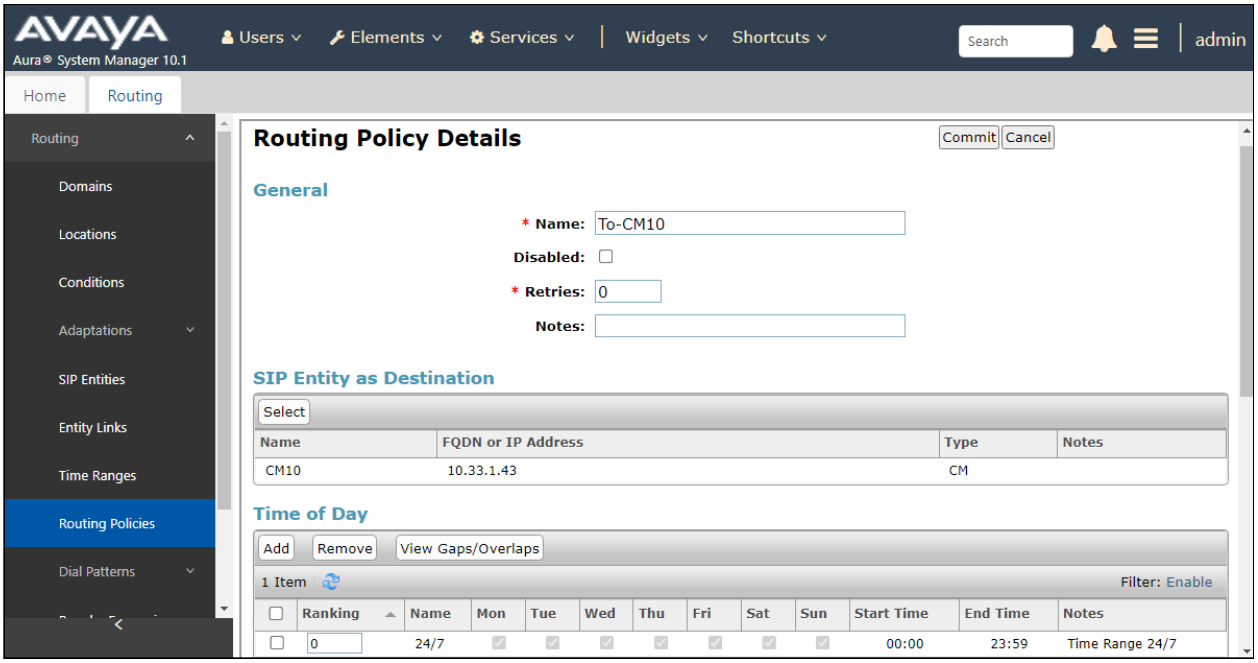
Add Remove

6.5.2. 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** section, enter a descriptive **Name**. Enter optional **Notes** 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 6.4.2**. The screen below shows the result of the selection.



Routing Policy Details

General

* Name: To-CM10

Disabled: □

* Retries: 0

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
CM10	10.33.1.43	CM	

Time of Day

Add | Remove | View Gaps/Overlaps

1 Item Filter: Enable

□	Ranking	Name	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
□	0	24/7	☑	☑	☑	☑	☑	☑	☑	00:00	23:59	Time Range 24/7

6.6. Administer Dial Patterns

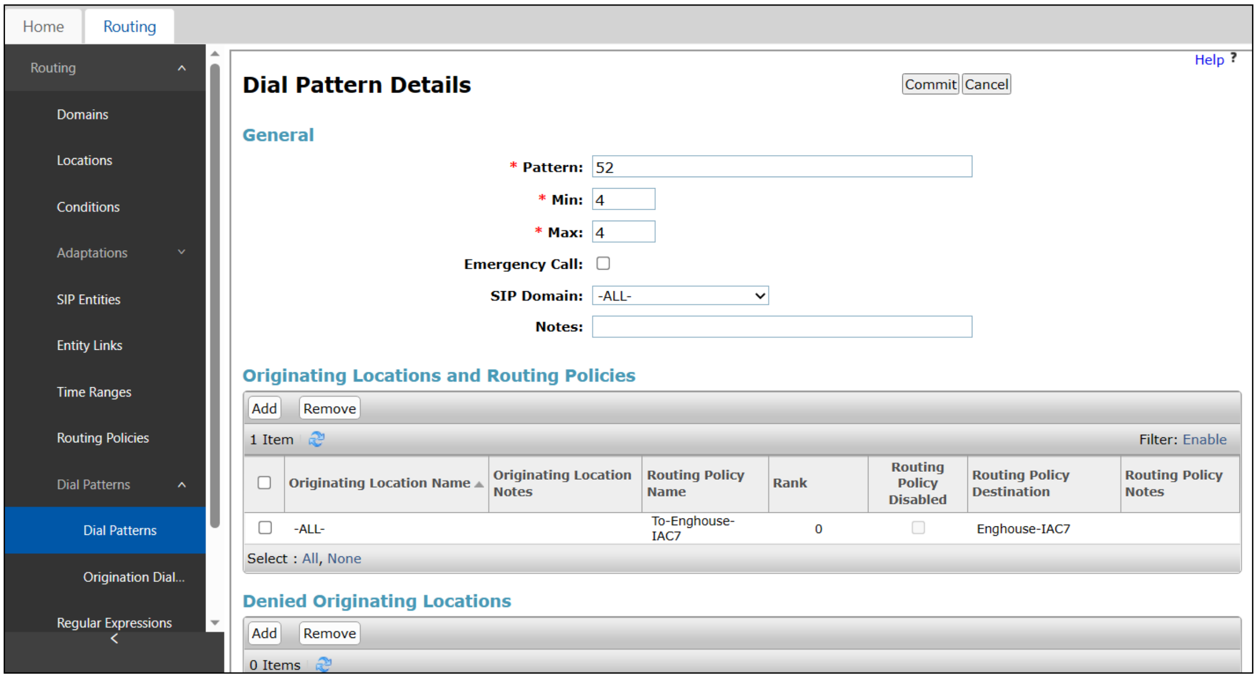
Add a new dial pattern for ICA and update existing dial patterns for Communication Manager.

6.6.1. Dial Pattern for IAC

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 the IAC server. 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 "52".
- **Min:** The minimum number of digits to match, in this case "4" was used.
- **Max:** The maximum number of digits to match, in this case "4" was used.
- **SIP Domain:** Select the applicable domain, in this case "All" selected.

In the **Originating Locations and Routing Policies** sub-section, click **Add** and create an entry for reaching the IAC server. In the compliance testing, the entry allowed for call originations from Communication Manager endpoint in locations "All". The routing policy **To-Enghouse-IAC7** from **Section 6.5.1** were selected as shown below.



Dial Pattern Details

General

* Pattern:	52
* Min:	4
* Max:	4
Emergency Call:	□
SIP Domain:	-ALL-
Notes:	

Originating Locations and Routing Policies

1 Item Filter: Enable

□	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
□	-ALL-		To-Enghouse-IAC7	0	□	Enghouse-IAC7	

Select : All, None

Denied Originating Locations

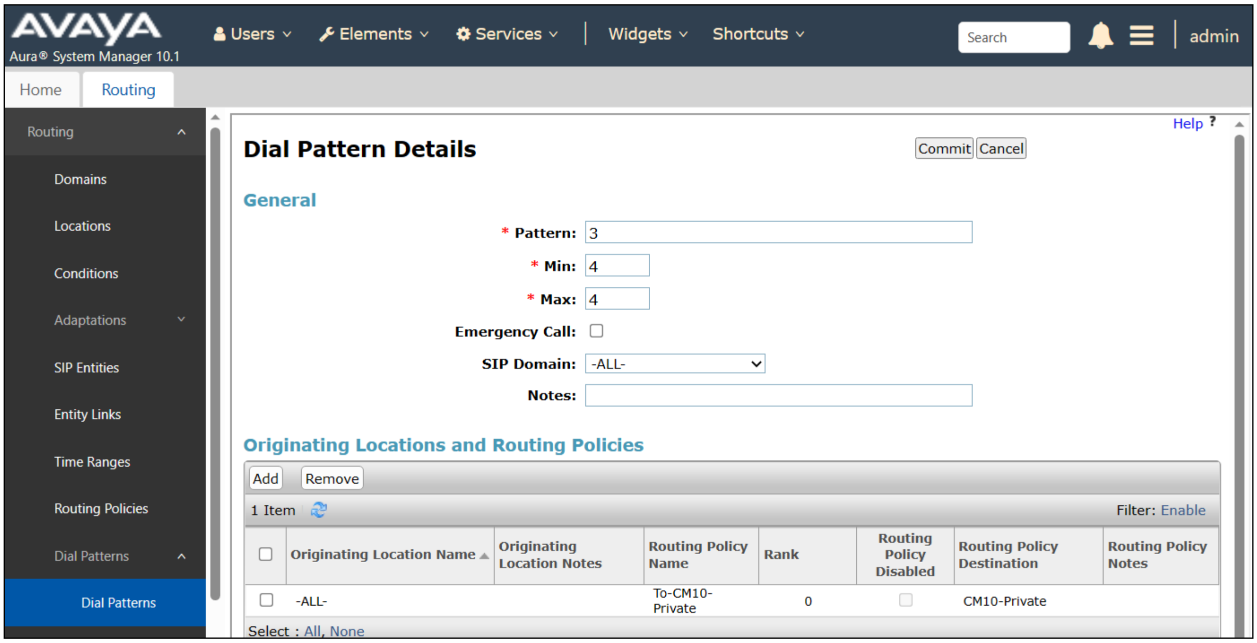
0 Items

6.6.2. 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 "3".
- **Min:** The minimum number of digits to match.
- **Max:** The maximum number of digits to match.
- **SIP Domain:** Select the applicable domain, in this case "All".

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 Communication Manager endpoint in locations "All". The Communication Manager routing policy from **Section 6.5.2** was selected as shown below.



Dial Pattern Details

General

* Pattern:	3
* Min:	4
* Max:	4
Emergency Call:	□
SIP Domain:	-ALL-
Notes:	

Originating Locations and Routing Policies

Add Remove

1 Item Filter: Enable

□	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
□	-ALL-		To-CM10-Private	0	□	CM10-Private	

Select : All, None

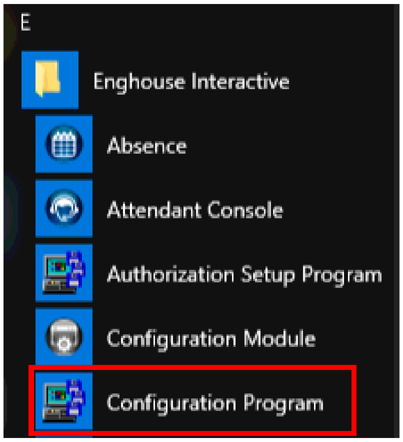
7. Configure Enghouse IAC

This section shows how to configure IAC to successfully connect to Session Manager. The installation of the IAC software is assumed to be completed and the IAC services are up.

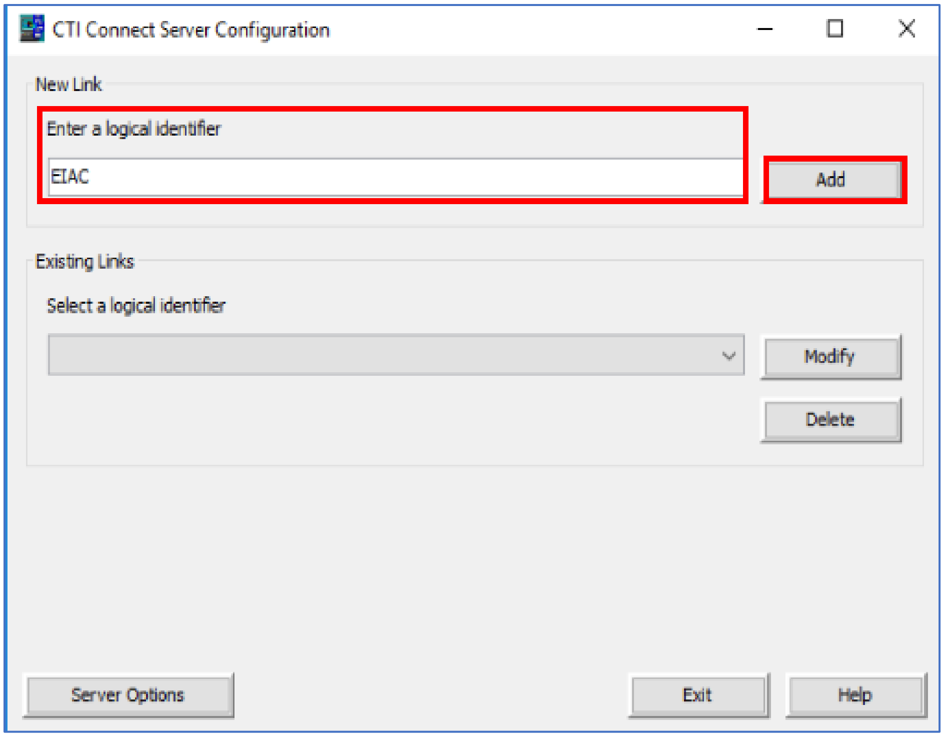
The steps to configure SIP Trunks are as follows:

- Configure IAC to use SIP Trunks
- Configure Absence
- Configure Intuition Advanced Console Attendant

- Launch the "configuration program".

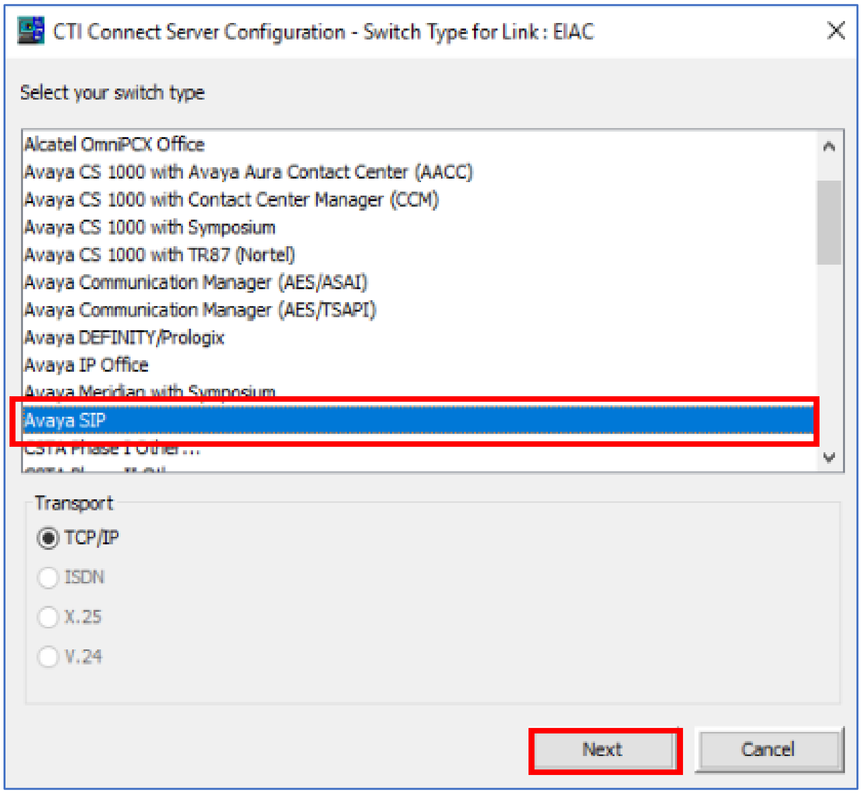


- Enter "EIAC" as logical identifier and click **Add**.


CTI Connect Server Configuration
New Link
Enter a logical identifier
Add
Existing Links
Select a logical identifier
Modify
Delete
Server Options
Exit
Help

EIAC

- Select **Avaya SIP**.



CTI Connect Server Configuration - Switch Type for Link : EIAC

Select your switch type

Alcatel OmniPCX Office
Avaya CS 1000 with Avaya Aura Contact Center (AACC)
Avaya CS 1000 with Contact Center Manager (CCM)
Avaya CS 1000 with Symposium
Avaya CS 1000 with TR87 (Nortel)
Avaya Communication Manager (AES/ASAI)
Avaya Communication Manager (AES/TSAPI)
Avaya DEFINITY/Prologix
Avaya IP Office
Avaya Meridian with Symposium
Avaya SIP
CSTA Phase I Other...

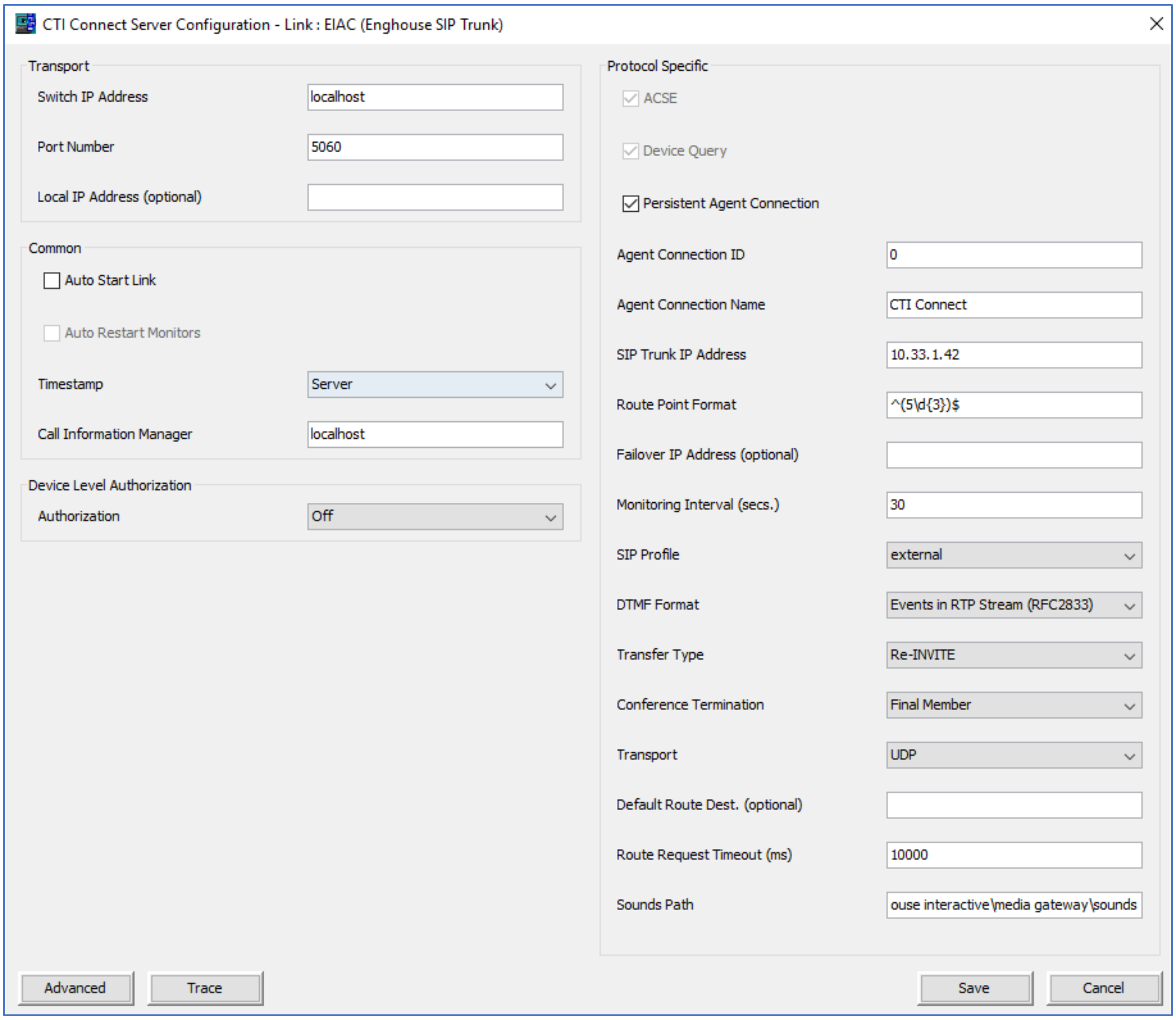
Transport

● TCP/IP
○ ISDN
○ X.25
○ V.24

- Enter parameters according to table below, leave all other configuration as default, click **Save** when done.

Port Number	5060
SIP Trunk IP Address	10.33.1.42

The attendant uses a regular Communication Manager telephone to make and receive calls, which are directed to the telephone by the IAC server.



CTI Connect Server Configuration - Link : EIAC (Enghouse SIP Trunk)

Transport

Switch IP Address	localhost
Port Number	5060
Local IP Address (optional)	

Common

☐ Auto Start Link

☐ Auto Restart Monitors

Timestamp	Server
Call Information Manager	localhost

Device Level Authorization

Authorization	Off

Protocol Specific

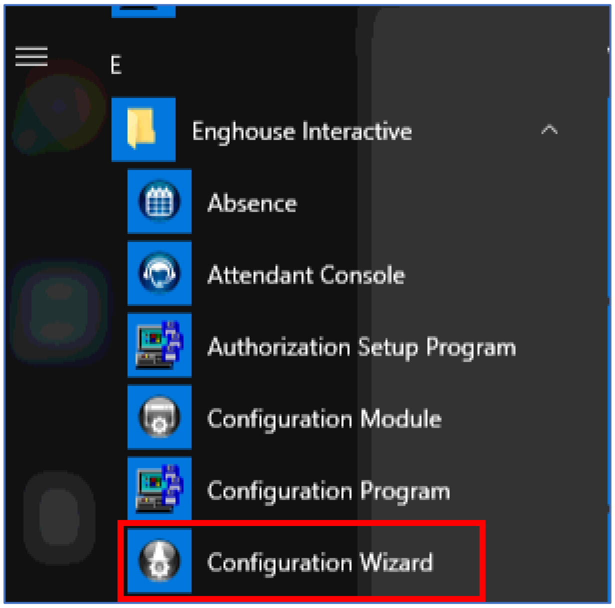
☑ ACSE

☑ Device Query

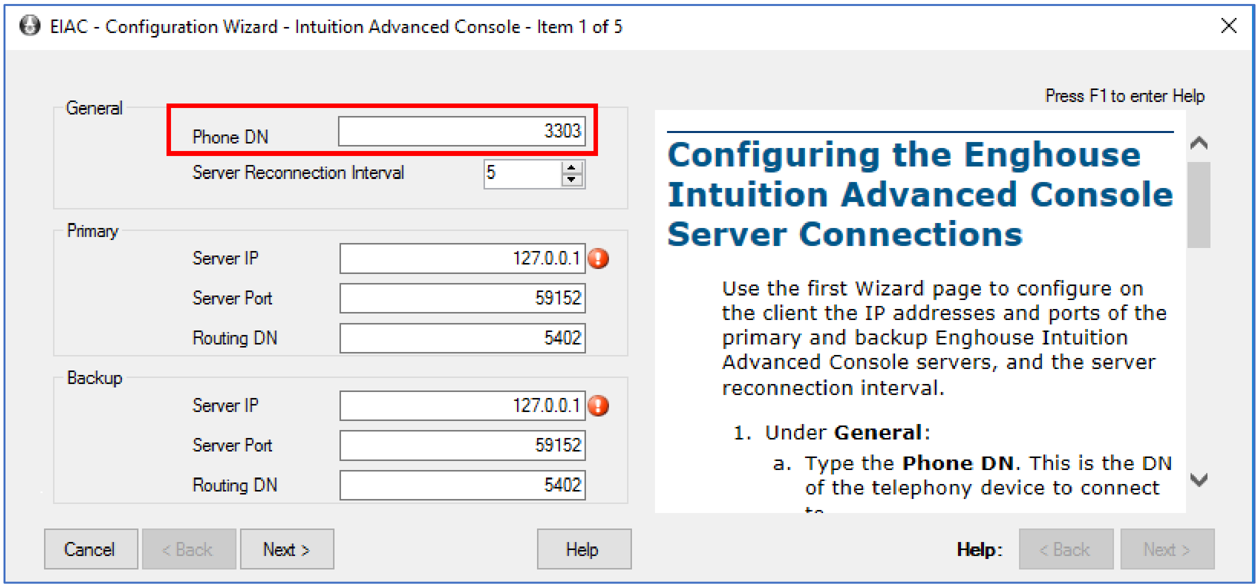
☑ Persistent Agent Connection

Agent Connection ID	0
Agent Connection Name	CTI Connect
SIP Trunk IP Address	10.33.1.42
Route Point Format	^(5\d{3})$
Failover IP Address (optional)	
Monitoring Interval (secs.)	30
SIP Profile	external
DTMF Format	Events in RTP Stream (RFC2833)
Transfer Type	Re-INVITE
Conference Termination	Final Member
Transport	UDP
Default Route Dest. (optional)	
Route Request Timeout (ms)	10000
Sounds Path	ouse interactive\media gateway\sounds

- Launch **Configuration Wizard**.



- Enter the attendant **Phone DN** and click **Next**.



EIAC - Configuration Wizard - Intuition Advanced Console - Item 1 of 5

General

Phone DN: 3303

Server Reconnection Interval: 5

Primary

Server IP: 127.0.0.1

Server Port: 59152

Routing DN: 5402

Backup

Server IP: 127.0.0.1

Server Port: 59152

Routing DN: 5402

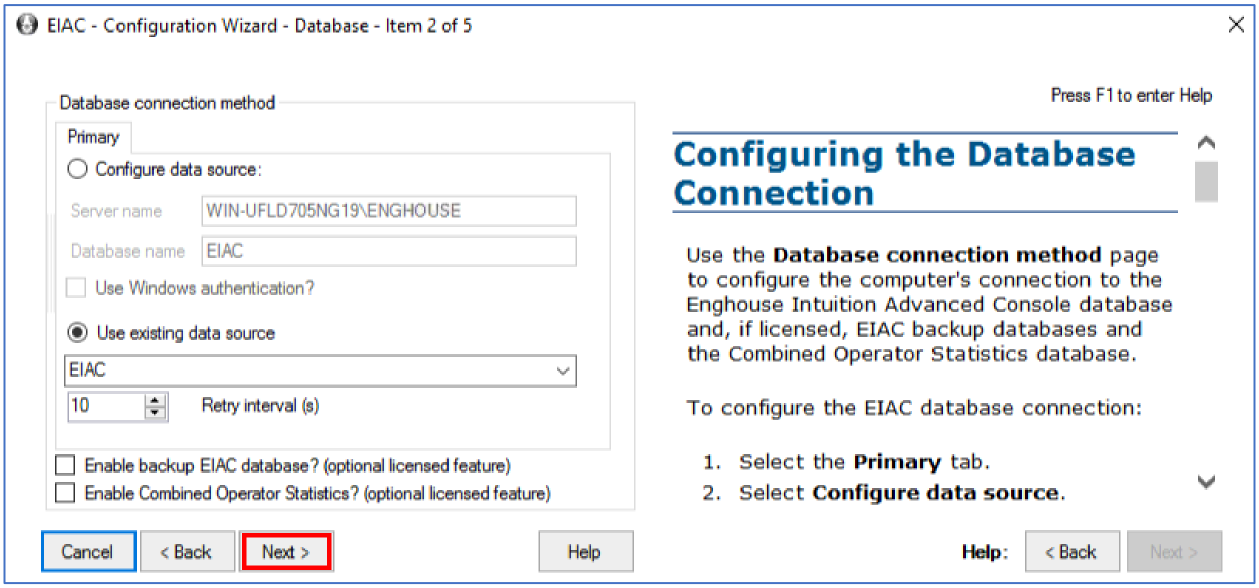
Press F1 to enter Help

Configuring the Enghouse Intuition Advanced Console Server Connections

Use the first Wizard page to configure on the client the IP addresses and ports of the primary and backup Enghouse Intuition Advanced Console servers, and the server reconnection interval.

1. Under **General**:
   a. Type the **Phone DN**. This is the DN of the telephony device to connect to

- Leave as default and click **Next**.



EIAC - Configuration Wizard - Database - Item 2 of 5

Database connection method

Primary

○ Configure data source:

Server name: WIN-UFLD705NG19\ENGHOUSE

Database name: EIAC

□ Use Windows authentication?

● Use existing data source

EIAC

10 Retry interval (s)

□ Enable backup EIAC database? (optional licensed feature)

□ Enable Combined Operator Statistics? (optional licensed feature)

Press F1 to enter Help

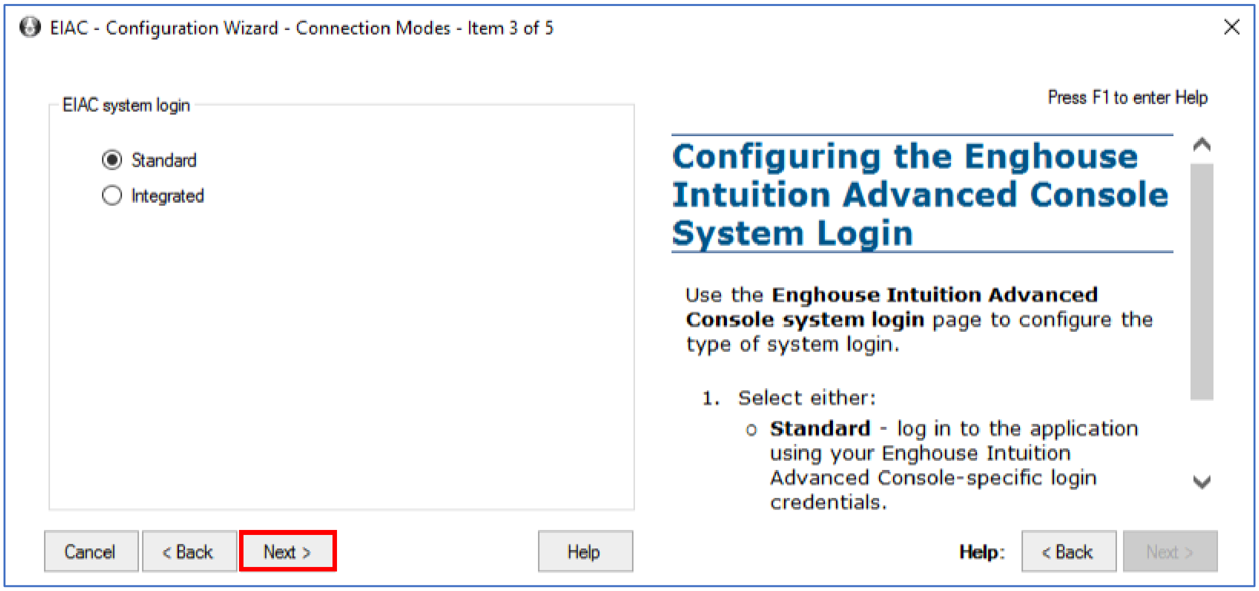
Configuring the Database Connection

Use the **Database connection method** page to configure the computer's connection to the Enghouse Intuition Advanced Console database and, if licensed, EIAC backup databases and the Combined Operator Statistics database.

To configure the EIAC database connection:

1. Select the **Primary** tab.
2. Select **Configure data source**.

- Leave as default and click **Next**.



EIAC - Configuration Wizard - Connection Modes - Item 3 of 5

EIAC system login

● Standard

○ Integrated

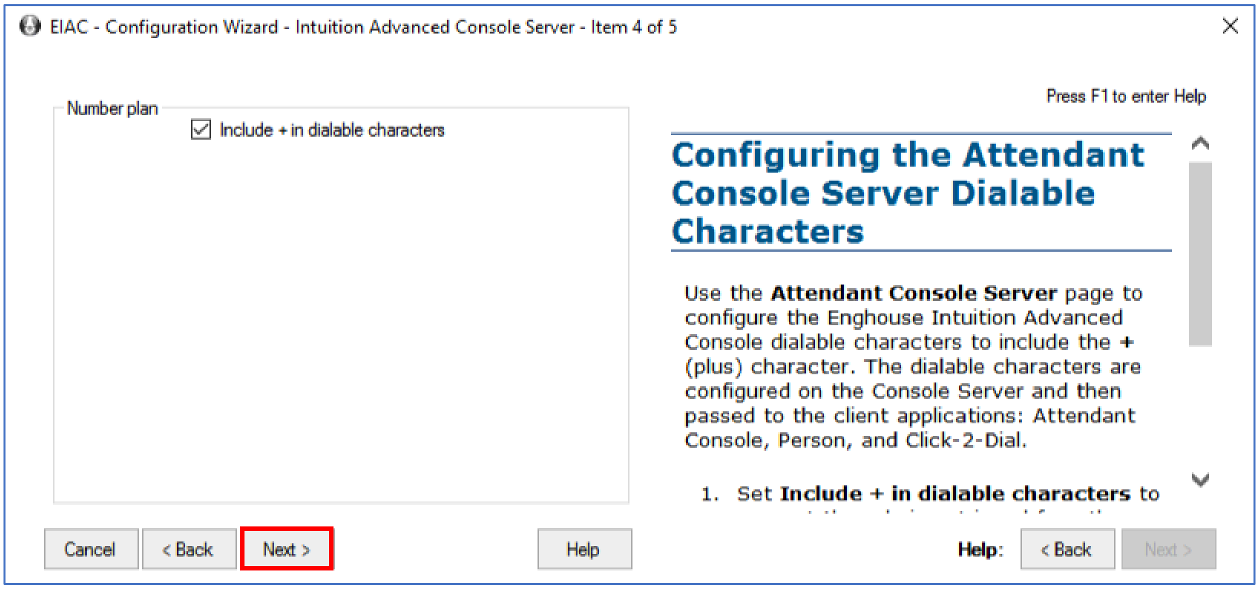
Press F1 to enter Help

Configuring the Enghouse Intuition Advanced Console System Login

Use the **Enghouse Intuition Advanced Console system login** page to configure the type of system login.

1. Select either:
   - **Standard** - log in to the application using your Enghouse Intuition Advanced Console-specific login credentials.

- Leave as default and click **Next**.



EIAC - Configuration Wizard - Intuition Advanced Console Server - Item 4 of 5

Number plan

☑ Include + in dialable characters

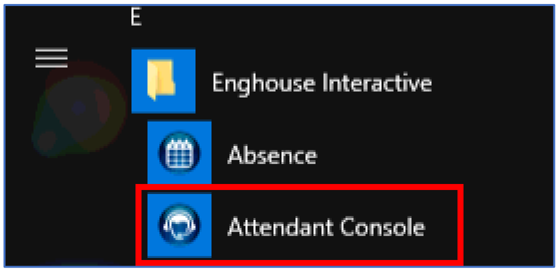
Press F1 to enter Help

Configuring the Attendant Console Server Dialable Characters

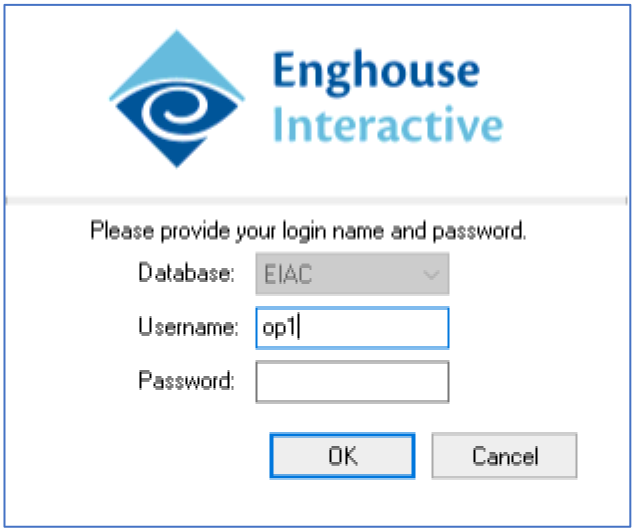
Use the **Attendant Console Server** page to configure the Enghouse Intuition Advanced Console dialable characters to include the **+** (plus) character. The dialable characters are configured on the Console Server and then passed to the client applications: Attendant Console, Person, and Click-2-Dial.

1. Set **Include + in dialable characters** to

- Launch the **Attendant Console**.



- Enter the appropriate credentials and click **OK**.



Please provide your login name and password.

Database: EIAC

Username: op1

Password:

8. Verification Steps

This section provides the tests that can be performed to verify proper configuration of Communication Manager, Session Manager, and ICA.

8.1. Verify Avaya Aura® Communication Manager

From the SAT interface, verify the status of the SIP trunk groups by using the “status trunk n” command, where “n” is the trunk group number administered in **Section** Error! Reference source not found.. Verify that all trunks are in the “in-service/idle” state as shown below.

```
status trunk 1

                             TRUNK GROUP STATUS

Member   Port     Service State      Mtce Connected Ports
                                     Busy

0001/001 T00001   in-service/idle    no
0001/002 T00002   in-service/idle    no
0001/003 T00003   in-service/idle    no
0001/004 T00004   in-service/idle    no
0001/005 T00005   in-service/idle    no
0001/006 T00006   in-service/idle    no
0001/007 T00007   in-service/idle    no
0001/008 T00008   in-service/idle    no
0001/009 T00009   in-service/idle    no
0001/010 T00010   in-service/idle    no
0001/011 T00011   in-service/idle    no
0001/012 T00012   in-service/idle    no
0001/013 T00013   in-service/idle    no
0001/014 T00014   in-service/idle    no
```

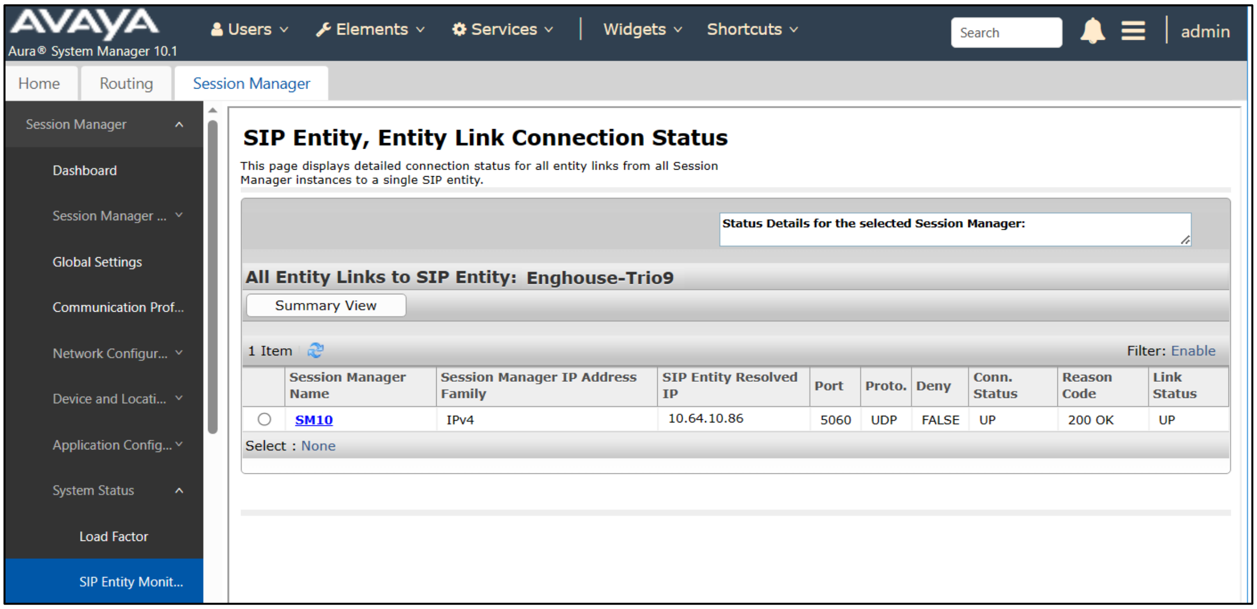
Verify the status of the SIP signaling groups by using the “status signaling-group n” command, where “n” is the signaling group number administered in **Section 5.4**. Verify that the **Group State** is “in-service”, as shown below.

```
status signaling-group 1
                         STATUS SIGNALING GROUP

        Group ID: 1
      Group Type: sip

     Group State: in-service
```

8.2. Verify Session Manager

From the System Manager home page (not shown), select **Elements → Session Manager** to display the **Session Manager Dashboard** screen (not shown).

Select **Session Manager → System Status → SIP Entity Monitoring** from the left pane to display the **SIP Entity Link Monitoring Status Summary** screen (not shown). Click the **Enghouse-ICA9** entity name. The **SIP Entity**, **Entity Link Connection Status** screen is displayed. Verify that the **Conn Status** and **Link Status** are “UP”, as shown below.



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: Enghouse-Trio9

1 Item

	Session Manager Name	Session Manager IP Address Family	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
○	SM10	IPv4	10.64.10.86	5060	UDP	FALSE	UP	200 OK	UP

8.3. Verify ICA Attendant

ICA calls the enterprise station to make it as the attendant and ready to receive incoming call, PSTN user places a call to the ICA. The ICA bridges the call to the attendant and now the call is established between the ICA attendant and PSTN user.

9. Conclusion

These Application Notes describe the procedures required to configure Intuition Advanced Console 7 from Enghouse Interactive AB to interoperate with Avaya Aura® Communication Manager and Avaya Aura® Session Manager using SIP Trunks. All feature functionality test cases described in **Section** Error! Reference source not found. were passed.

10. Additional References

This section references the Avaya documentation that are relevant to these Application Notes. Product documentation for Avaya Aura® Session Manager, including the following, is available at: http://support.avaya.com/

[1] Administering Avaya Aura® Session Manager, Document 03-300509, Issue 10, Release 10.1, August 2022

[2] Administering Avaya Aura® System Manager, Issue 9.0, Release 10.1, August 2022

[3] Administering Avaya Aura® Communication Manager, Document 03-300509, Issue 10, Release 10.1, August 2022

[4] Avaya Aura® Communication Manager Feature Description and Implementation, Document 555-245-205, Issue 9.0, Release 10.1, May 2022

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.