Application Notes for Computer Instruments eONE with Avaya Aura® Communication Manager and Avaya Aura® Session Manager using SIP Trunks – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for Computer Instruments eONE to interoperate with Avaya Aura® Communication Manager and Avaya Aura® Session Manager using SIP trunks. Computer Instruments eONE is an IVR development platform that includes a number of self-service IVR and Web applications.

In the compliance testing, Computer Instruments eONE used SIP trunks to Avaya Aura® Session Manager to support inbound and outbound IVR applications.

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 describe the configuration steps required for Computer Instruments eONE to interoperate with Avaya Aura® Communication Manager and Avaya Aura® Session Manager using SIP trunks. Computer Instruments eONE is an IVR development platform that includes a number of self-service IVR and Web applications.

In the compliance testing, Computer Instruments eONE used SIP trunks to Avaya Aura® Session Manager to support inbound and outbound IVR applications.

The Computer Instruments eONE server used in the testing included the Dialogic Host Media Processing Software for support of SIP protocol.

2. General Test Approach and Test Results

The feature test cases were performed manually. The eONE inbound application was tested by manually placing calls from users on the PSTN and on Communication Manager to the eONE inbound application. The associated eONE inbound application played greeting announcements and collected DTMF input from the caller to decide on the feature to provide, such as transfer to internal or external destinations. eONE outbound application to PSTN and Communication Manager were also tested.

The serviceability test cases were performed manually by disconnecting and reconnecting the Ethernet connection to eONE.

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 test included feature and serviceability testing.

The feature testing included G.711MU codec, codec negotiation, media shuffling, session refresh, hold/reconnect, inbound DTMF, invalid number, busy destination, and outgoing call screening.

The serviceability testing focused on verifying the ability of eONE to recover from adverse conditions, such as disconnecting/reconnecting the Ethernet connection to eONE.

2.2. Test Results

All test cases were executed and passed.

2.3. Support

Technical support on eONE can be obtained through the following:

- **Phone:** (888) 451-0851
- **Email:** support@instruments.com

3. Reference Configuration

As shown in **Figure 1**, SIP trunks were used between eONE and Session Manager, and the applicable domain name used was “avaya.com”.

A five digit Uniform Dial Plan (UDP) was used to facilitate routing with eONE. Unique extension ranges were assigned to users on Communication Manager (7200x – H.323 and 7202x – SIP), and to eONE (72061).

The configuration of Session Manager is performed via the web interface of System Manager. The detailed administration of basic connectivity between Communication Manager, System Manager, and Session Manager is not the focus of these Application Notes and will not be described.

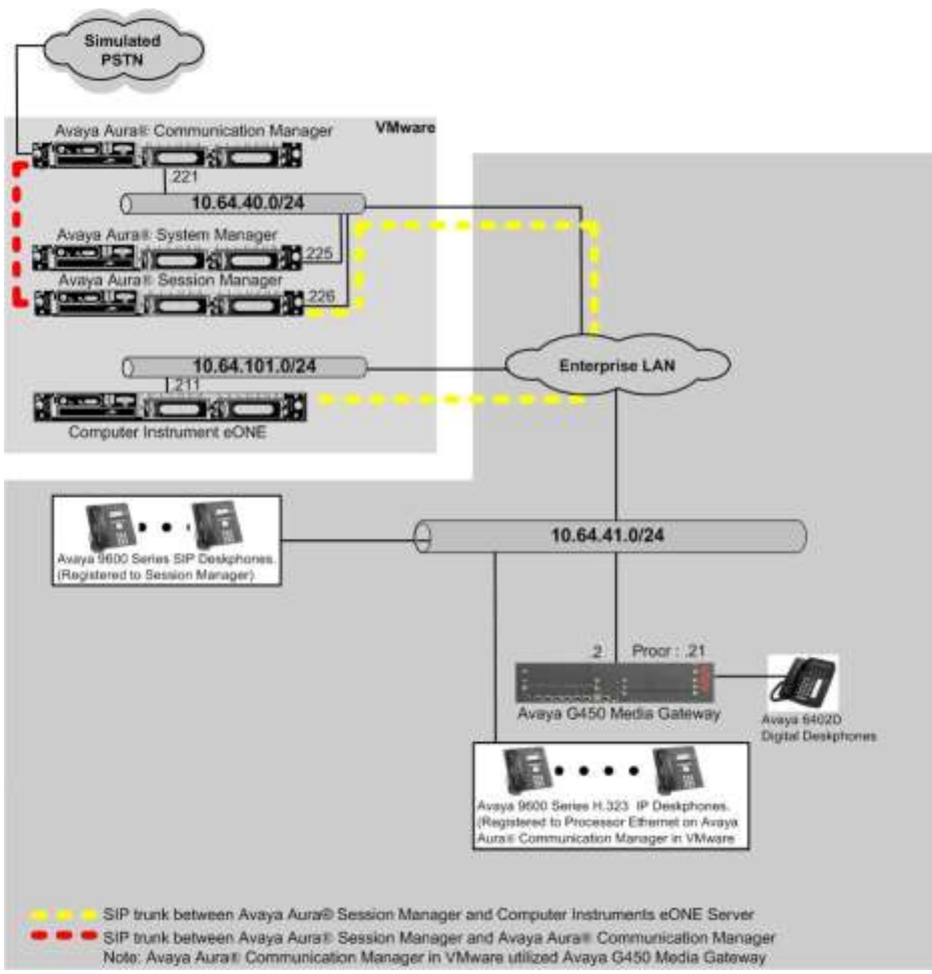


Figure 1: Computer Instruments eONE with Avaya Aura® Session Manager

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 on Avaya S8300D Server with Avaya G450 Media Gateway	7.0 (R017x.00.0.441.0) 37.19.0
Avaya Aura® Session Manager	7.0.0.0.700007
Avaya Aura® System Manager	7.0.0.0
Avaya 96x0 IP Deskphone (H.323)	3.25
Avaya 96x1 IP Deskphone (H.323)	6.6
Avaya 96x0 IP Deskphone (SIP)	2.6.14
Avaya 96x1G IP Deskphone (SIP)	7.0.0.39
Computer Instruments eONE on Windows Server 2008 R2 • Service Manager • Dialogic Host Media Processing Manager	6.1.1 3.7 GA 3.0 Service Update 357

5. Configure Avaya Aura® Communication Manager

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

- 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 uniform dial plan
- Administer AAR analysis
- Administer PSTN trunk group
- Administer tandem calling party number

In the compliance testing, a separate set of codec set, network region, trunk group, and signaling group were used for integration with eONE.

5.1. Verify License

Log into the System Access Terminal (SAT) 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.

The license file installed on the system controls the maximum permitted. If there is insufficient capacity, contact an authorized Avaya sales representative to make the appropriate changes.

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

IP PORT CAPACITIES                                            USED
                     Maximum Administered H.323 Trunks: 4000  17
           Maximum Concurrently Registered IP Stations: 2400  8
             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  0
                   Maximum Video Capable IP Softphones: 2400  1
                       Maximum Administered SIP Trunks: 4000  15
  Maximum Administered Ad-hoc Video Conferencing Ports: 4000  0
   Maximum Number of DS1 Boards with Echo Cancellation: 80    0
```

5.2. Administer System Parameters Features

Use the "change system-parameters features" command to allow for trunk-to-trunk transfers.

For ease of interoperability testing, the **Trunk-to-Trunk Transfer** field was set to "all" to enable all trunk-to-trunk transfers on a system wide basis. Note that this feature poses significant security risk, and must be used with caution. For alternatives, the trunk-to-trunk feature can be implemented on the Class Of Restriction or Class Of Service levels. Refer to [1] for more details.

```
change system-parameters features                               Page   1 of  19
                            FEATURE-RELATED SYSTEM PARAMETERS
                               Self Station Display Enabled? n
                                    Trunk-to-Trunk Transfer: all
               Automatic Callback with Called Party Queuing? n
    Automatic Callback - No Answer Timeout Interval (rings): 3
                       Call Park Timeout Interval (minutes): 10
        Off-Premises Tone Detect Timeout Interval (seconds): 20
                                 AAR/ARS Dial Tone Required? y

              Music (or Silence) on Transferred Trunk Calls? all
              DID/Tie/ISDN/SIP Intercept Treatment: attendant
    Internal Auto-Answer of Attd-Extended/Transferred Calls: transferred
                  Automatic Circuit Assurance (ACA) Enabled? n




             Abbreviated Dial Programming by Assigned Lists? n
       Auto Abbreviated/Delayed Transition Interval (rings): 2
                    Protocol for Caller ID Analog Terminals: Bellcore
    Display Calling Number for Room to Room Caller ID Calls? 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 “92”. This trunk group is used between Communication Manager and Session Manager. 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 92                                              Page   1 of  21
                                TRUNK GROUP

Group Number: 92                   Group Type: sip          CDR Reports: y
  Group Name: SM70                        COR: 1        TN: 1        TAC: 1092
   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:
                                                     Number of Members:
```

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

```
add trunk-group 92                                              Page   3 of  21
TRUNK FEATURES
          ACA Assignment? n            Measured: none
                                                          Maintenance Tests? y



                     Numbering Format: private
                                               UUI Treatment: service-provider

                                                Replace Restricted Numbers? n
                                               Replace Unavailable Numbers? n


                                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 "92". 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" in this case.
- **Far-end Node Name:** The existing node name for Session Manager.
- **Near-end Listen Port:** An available port for integration with Communication 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 eONE.
- **Far-end Domain:** The applicable domain name for the network. The empty Far-end Domain indicates "any" domain.

```
add signaling-group 92                                          Page   1 of   2
                                SIGNALING GROUP

 Group Number: 92             Group Type: sip
  IMS Enabled? n        Transport Method: tls
        Q-SIP? n
     IP Video? y          Priority Video? y        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: SM70
 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 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 “5”.

```
change trunk-group 92                                          Page   1 of  21
                                TRUNK GROUP

Group Number: 92                   Group Type: sip           CDR Reports: y
  Group Name: SM70                        COR: 1        TN: 1        TAC: 1092
   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: 92
                                                     Number of Members: 5
```

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**, if needed. 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 eONE.

```
change ip-network-region 1                                          Page   1 of  20
                               IP NETWORK REGION
  Region: 1
Location: 1       Authoritative Domain: avaya.com
    Name:                     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: 16390                   IP Audio Hairpinning? n
   UDP Port Max: 16999
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
  H.323 Link Bounce Recovery? y
 Idle Traffic Interval (sec): 20
   Keep-Alive Interval (sec): 5
            Keep-Alive Count: 5
```

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. Note that eONE only supports the G.711 codec variant. The codec shown below was used in the compliance testing.

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

                          IP CODEC SET
    Codec Set: 1

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

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 eONE via Session Manager, in this case "92". 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 92                                         Page   1 of   3
                    Pattern Number: 92     Pattern Name: Route2SM70
    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: 92   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                                         none
 2: y y y y y n  n            rest                                         none
 3: y y y y y n  n            rest                                         none
 4: y y y y y n  n            rest                                         none
 5: y y y y y n  n            rest                                         none
 6: y y y y y n  n            rest                                         none
```

5.9. Administer Private Numbering

Use the “change private-numbering 0” command, to define the calling party number to send to eONE. 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 720 and routed to trunk group 92 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  720              92                            5     Total Administered: 2
 5  777                                            4        Maximum Entries: 540
```

5.10. Administer Uniform Dial Plan

This section provides a sample uniform dialplan used for routing calls with dialed digits 7206x to eONE. 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 digits 7206x, 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
7206               5   0                 aar  n
```

5.11. Administer AAR Analysis

Use the “change aar analysis 7” command, and add an entry to specify how to route calls to 7206x. In the example shown below, calls with digits 7206x will be routed as an unku call type using route pattern “92” from **Section 0**.

```
change aar analysis 7                                           Page   1 of   2
                             AAR DIGIT ANALYSIS TABLE
                                   Location: all            Percent Full: 3

          Dialed          Total      Route     Call   Node   ANI
          String        Min  Max   Pattern    Type   Num    Reqd
    7206                5    5      92        unku          n
```

5.12. Administer PSTN Trunk Group

Use the "change trunk-group n" command, where "n" is the existing trunk group number used to reach the PSTN, in this case "80".

Navigate to **Page 3**. For **Modify Tandem Calling Number**, enter "tandem-cpn-form" to allow the calling party number from eONE to be modified.

```
change trunk-group 80                                           Page   3 of  22
TRUNK FEATURES
          ACA Assignment? n            Measured: none      Wideband Support? n
                                 Internal Alert? n       Maintenance Tests? y
                               Data Restriction? n     NCA-TSC Trunk Member: 10
                                      Send Name: y      Send Calling Number: y
            Used for DCS? n                            Send EMU Visitor CPN? y
   Suppress # Outpulsing? n    Format: private
 Outgoing Channel ID Encoding: preferred     UUI IE Treatment: service-provider

                                                 Replace Restricted Numbers? n
                                                Replace Unavailable Numbers? n
                                                      Send Connected Number: y
Network Call Redirection: none                    Hold/Unhold Notifications? n
             Send UUI IE? y     Modify Tandem Calling Number: tandem-cpn-form
               Send UCID? n
 Send Codeset 6/7 LAI IE? y                         Ds1 Echo Cancellation? n

    Apply Local Ringback? n              US NI Delayed Calling Name Update? n
 Show ANSWERED BY on Display? y      Invoke ID for USNI Calling Name: variable
                             Network (Japan) Needs Connect Before Disconnect? n
```

5.13. Administer Tandem Calling Party Number

Use the "change tandem-calling-party-num" command, to define the calling party number to send to PSTN for tandem calls from eONE.

In the example shown below, all calls originating from a 5-digit extension beginning with 72 and routed to trunk group 80 will result in a 10-digit calling number. For **Outgoing Number Format**, use an applicable format, in this case "pub-unk". Since the inserted number is a publically defined number, the actual number is not shown.

```
change tandem-calling-party-num                                 Page   1 of   9
                         CALLING PARTY NUMBER CONVERSION
                                 FOR TANDEM CALLS
                      Incoming Outgoing                             Outgoing
      CPN             Number   Trunk                                Number
 Len  Prefix          Format   Group(s)     Delete  Insert          Format
 5    72                        80         5       xxxyyyzzzz       pub-unk
```

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 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.

6.2. Administer SIP Entities

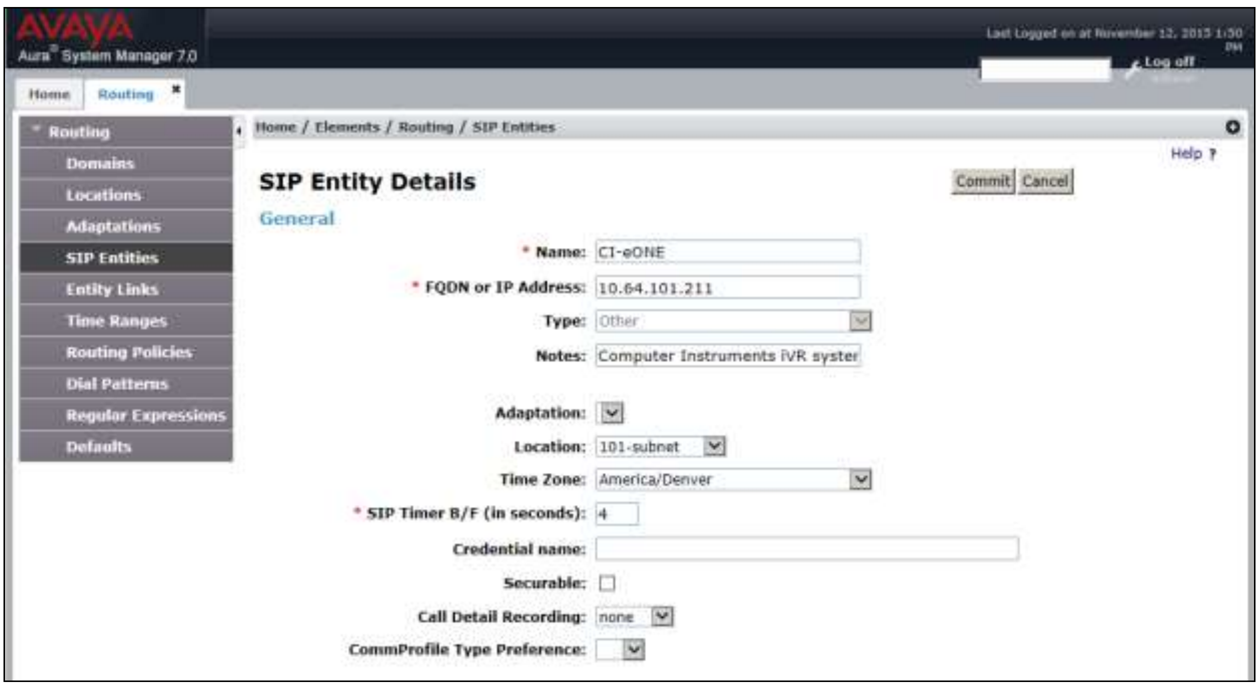
Add two new SIP entities, one for eONE and one for the new SIP trunks with Communication Manager.

6.2.1. SIP Entity for eONE

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

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

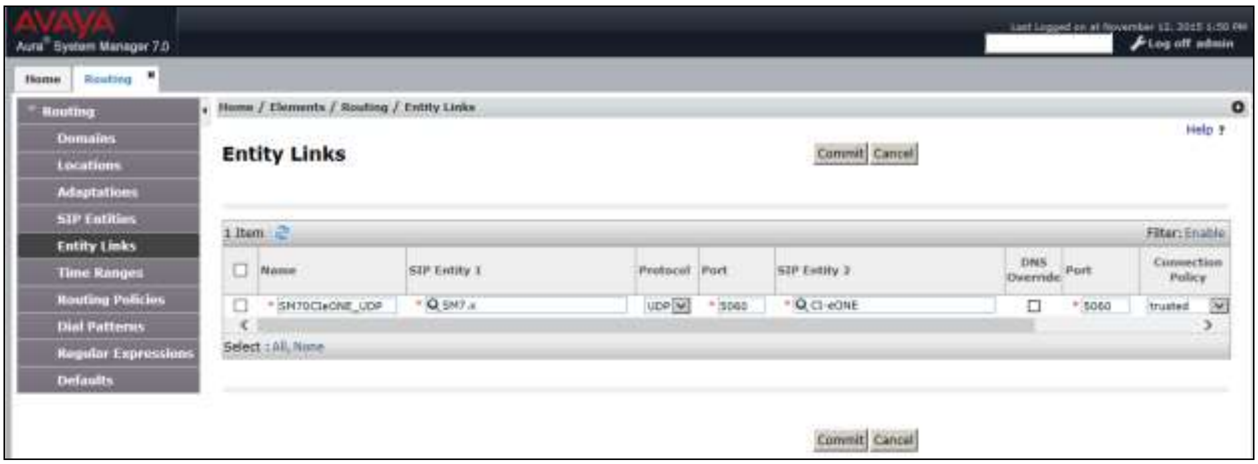
- **Name:** A descriptive name.
- **FQDN or IP Address:** The IP address of the eONE server.
- **Type:** "Other"
- **Notes:** Any desired notes.
- **Location:** Select the eONE location name.
- **Time Zone:** Select the applicable time zone.



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.

- **SIP Entity 1:** The Session Manager entity name, in this case "SM7.x".
- **Protocol:** "UDP"
- **Port:** "5060"
- **SIP Entity 2:** The eONE entity name from this section.
- **Port:** "5060"
- **Connection Policy:** "trusted"

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

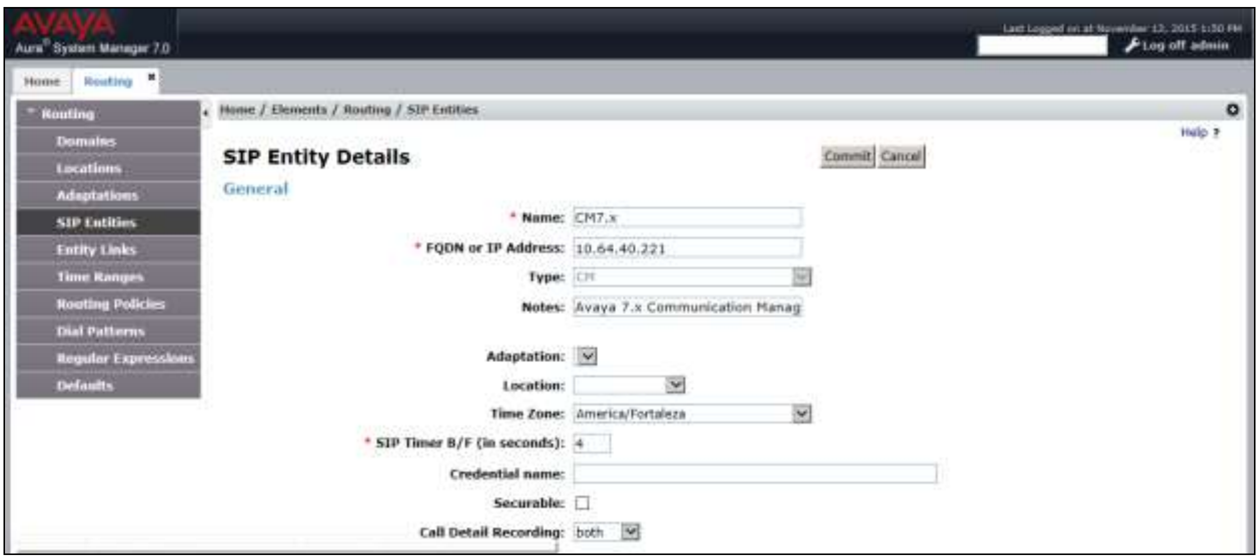


6.2.2. SIP Entity for Communication Manager

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 eONE.

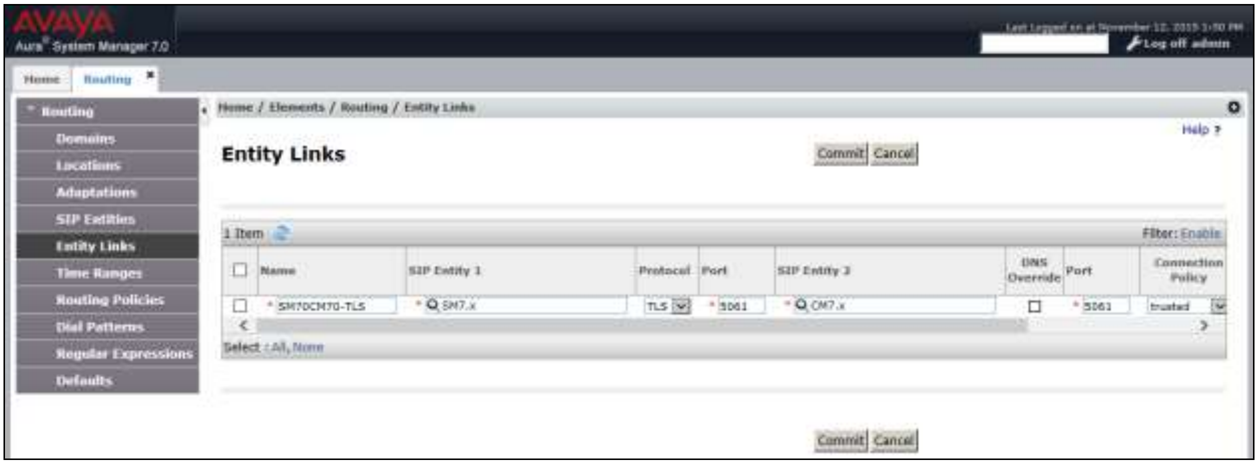
The **SIP Entity Details** screen is displayed. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **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.
- **Adaptation:** Select the applicable adaptation for Communication Manager.
- **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.

- **SIP Entity 1:** The Session Manager entity name, in this case "SM7.x".
- **Protocol:** The signaling group transport method from **Section 5.4**.
- **Port:** The signaling group listen port number from **Section 5.4**.
- **SIP Entity 2:** The Communication Manager entity name from this section.
- **Port:** The signaling group listen port number from **Section 5.4**.
- **Connection Policy:** "trusted"



6.3. Administer Routing Policies

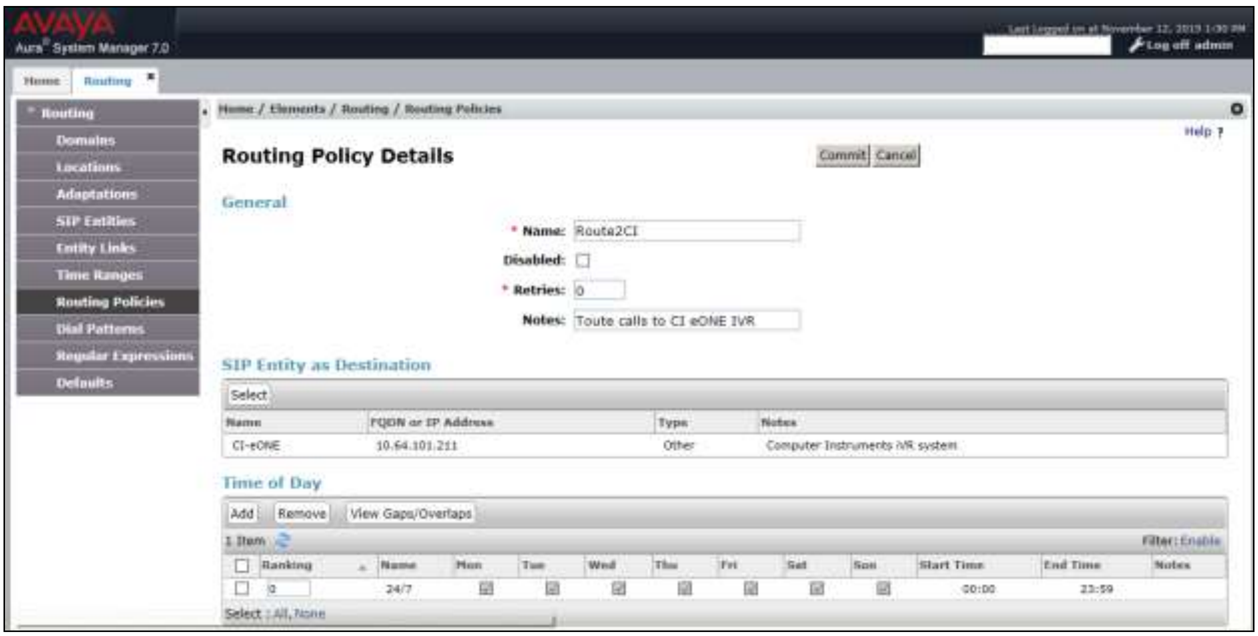
Add two new routing policies, one for eONE and one for the new SIP trunks with Communication Manager.

6.3.1. Routing Policy for eONE

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

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 eONE entity name from **Section 6.2.1**. The screen below shows the result of the selection.

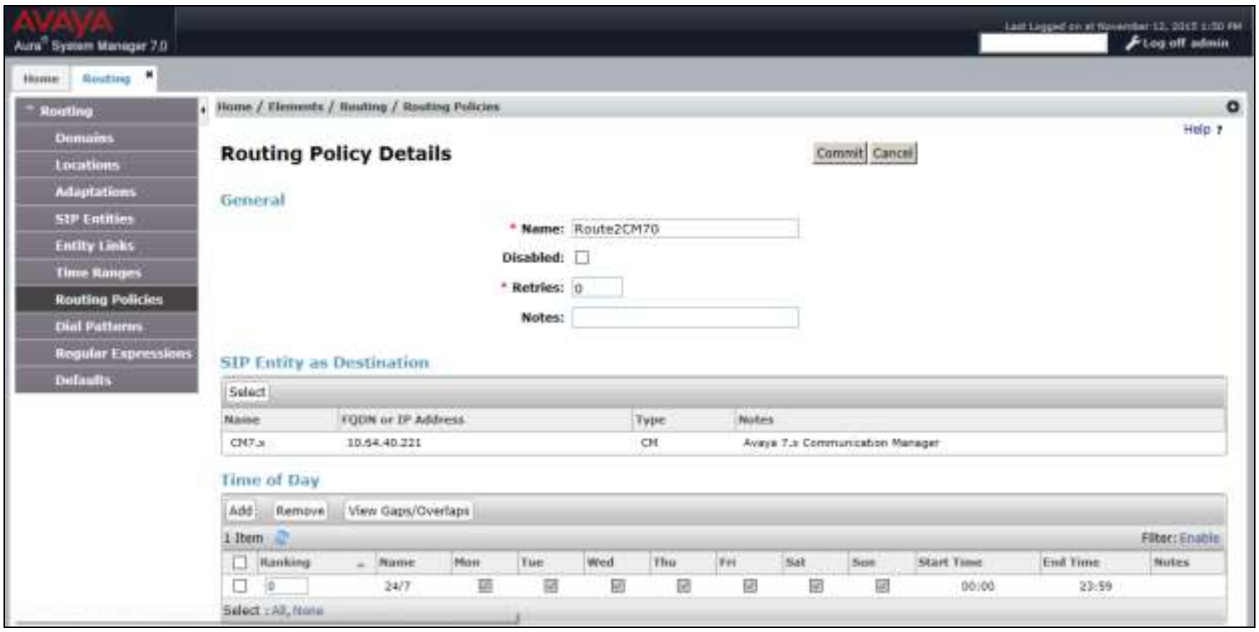


6.3.2. Routing Policy for Communication Manager

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 6.2.2**. The screen below shows the result of the selection.



6.4. Administer Dial Patterns

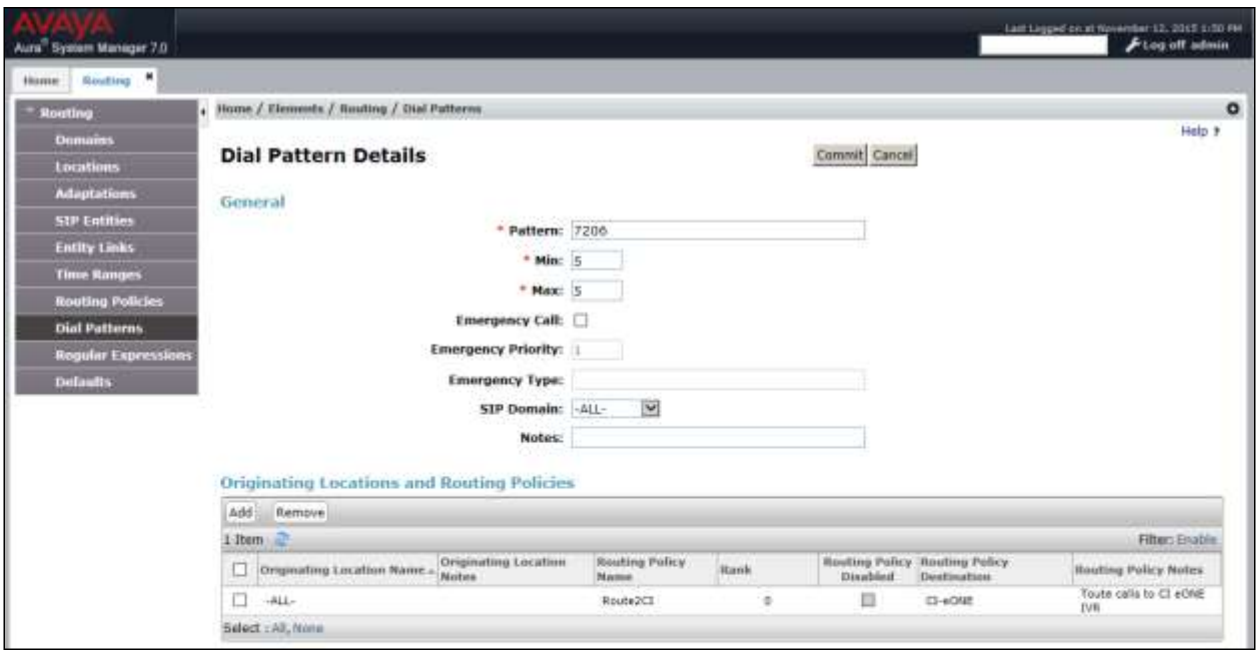
Add a new dial pattern for eONE, and update existing dial patterns for Communication Manager.

6.4.1. Dial Pattern for eONE

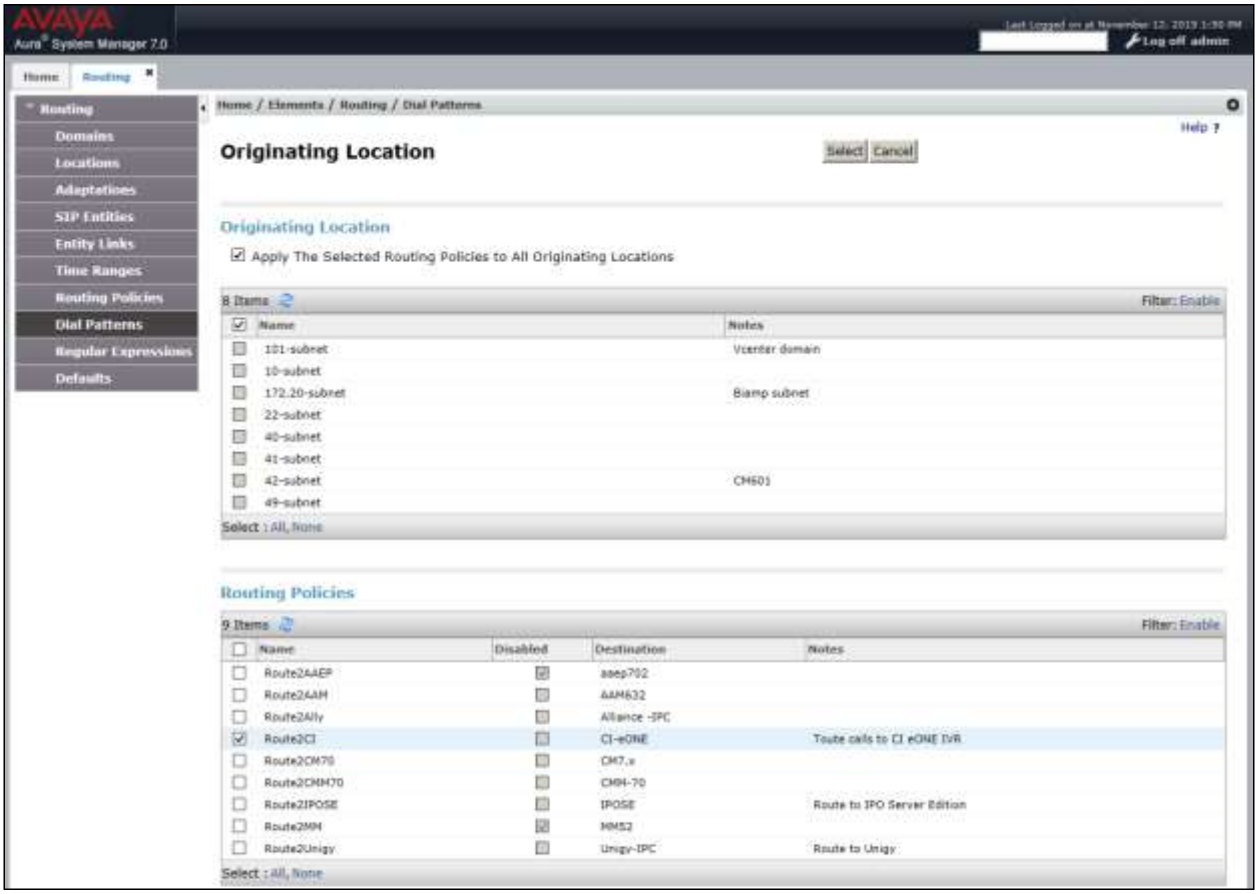
Select **Routing → Dial Patterns** from the left pane, and click **New** in the subsequent screen (not shown) to add a new dial pattern to reach eONE. The **Dial Pattern Details** screen is displayed. In the **General** sub-section, enter the following values for the specified fields, and retain the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

- **Pattern:** A dial pattern to match, in this case "7206".
- **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 a new policy for reaching eONE.



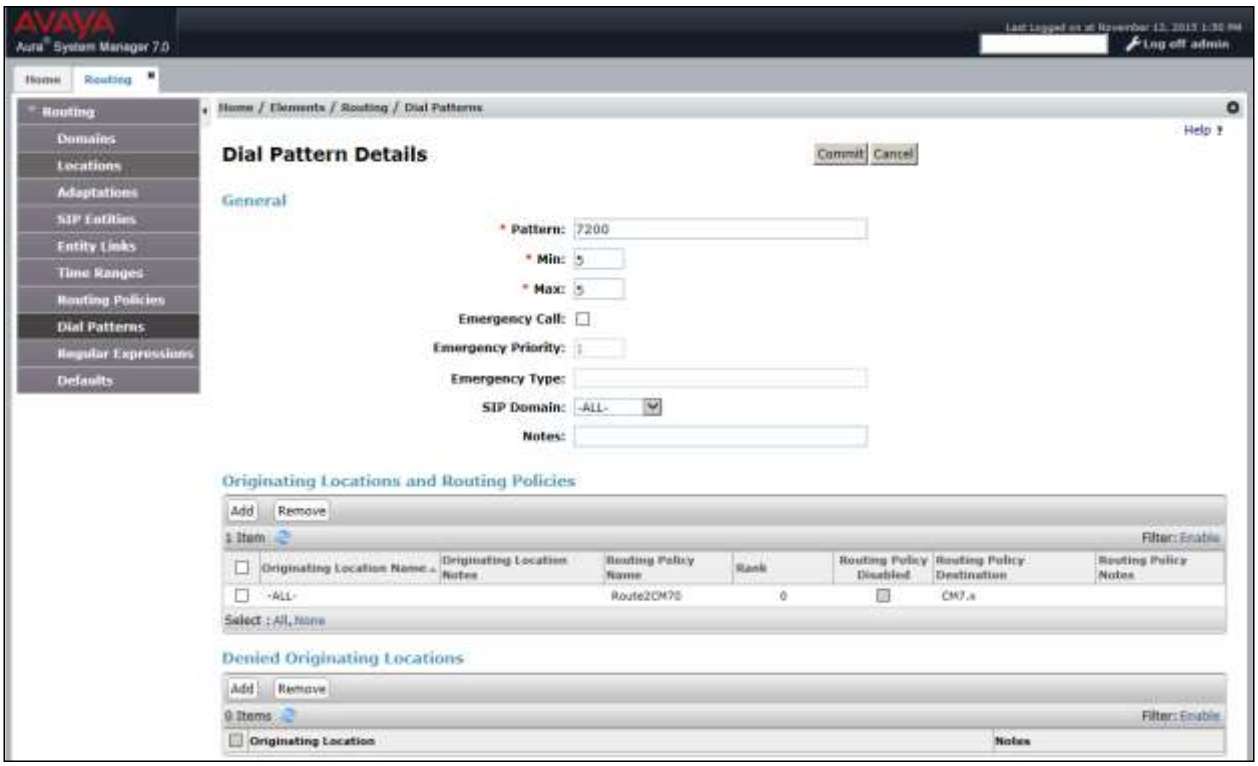
In the compliance testing, the policy allowed for call origination from “ALL”, and the eONE routing policy from **Section 6.3.1** was selected as shown below.



6.4.2. Dial Pattern for Communication Manager

Select **Routing → Dial Patterns** from the left pane, and click on the first existing dial pattern for Communication Manager in the subsequent screen, in this case dial pattern "7200" (not shown). The **Dial Pattern Details** screen is displayed.

In the **Originating Locations and Routing Policies** sub-section, click **Add** and create a new policy as necessary for calls from eONE. In the compliance testing, the new policy allowed for call origination from the eONE location from **Section** Error! Reference source not found., and the Communication Manager routing policy from **Section 6.3.2** was selected as shown below. Retain the default values in the remaining fields.



7. Configure Computer Instruments eONE

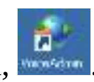
This section provides the procedures for configuring eONE. The procedures include the following areas:

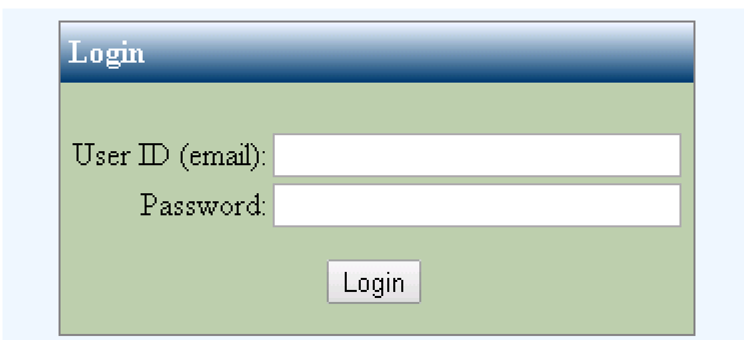
- Administer system config
- Administer EIVR.ini
- Restart service

7.1. Administer System Config

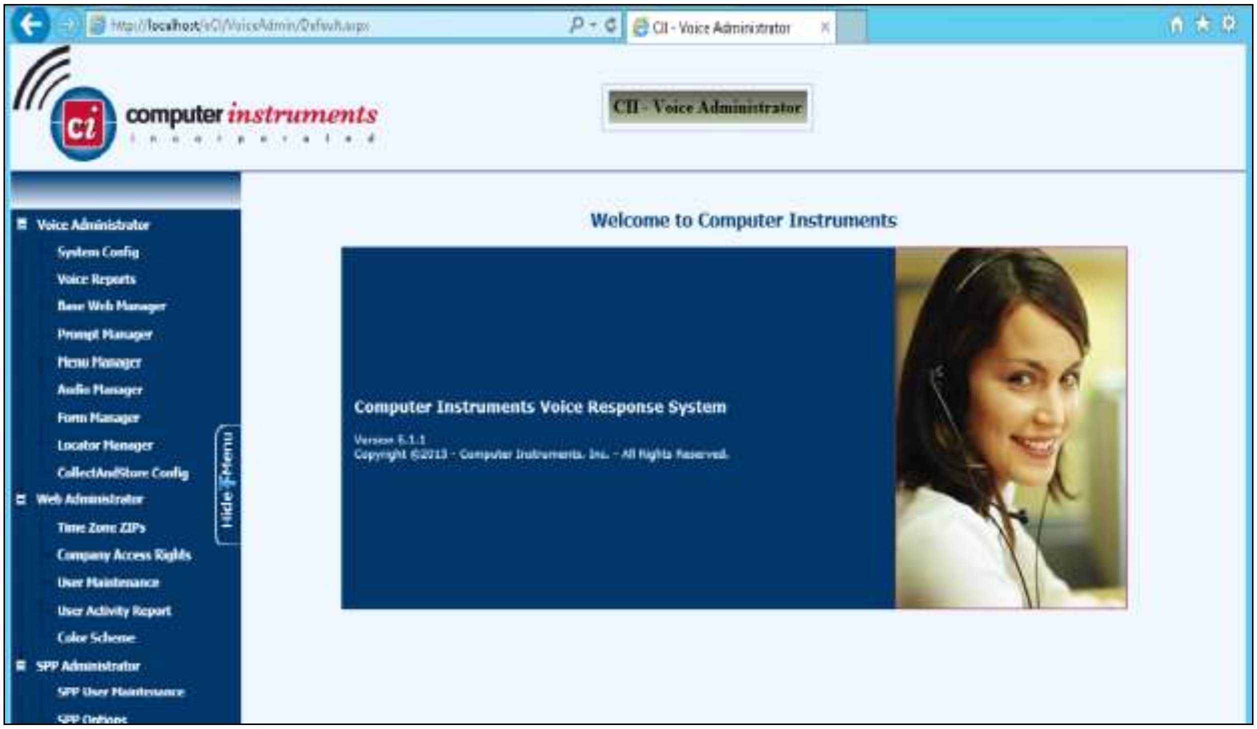
Note: Prior to the actual test, a Computer Instruments engineer logged in remotely to the server and completed the installation, licensing and configuration. This section shows what was configured by the Computer Instruments engineer. For more information, please contact the Computer Instruments support, mentioned in **Section 2.3**.

To access the **CII-Voice Administrator** page (Main), follow the link

http://localhost/eCI/VoiceAdmin/Default.aspx or click the shortcut icon created, .
Provide appropriate credentials in the Login page.



In the **CII-Voice Administrator** page, select **Voice Administrator → System Config** in the left pane to display the **Base System Configuration** screen.



Select the Defaults tab from the top of the **Base System Configuration** pop-up screen. Select "Avaya Definity" for **PBX Integration**. For **Dial Plan Digits**, enter the maximum length of internal extensions on Communication Manager. For **Outside Line Access Prefix**, enter the applicable prefix for calls to the PSTN, as required by Communication Manager. For outbound calls to the PSTN, eONE will automatically prepend the **Outside Line Access Prefix** value defined below, plus the digit "1".

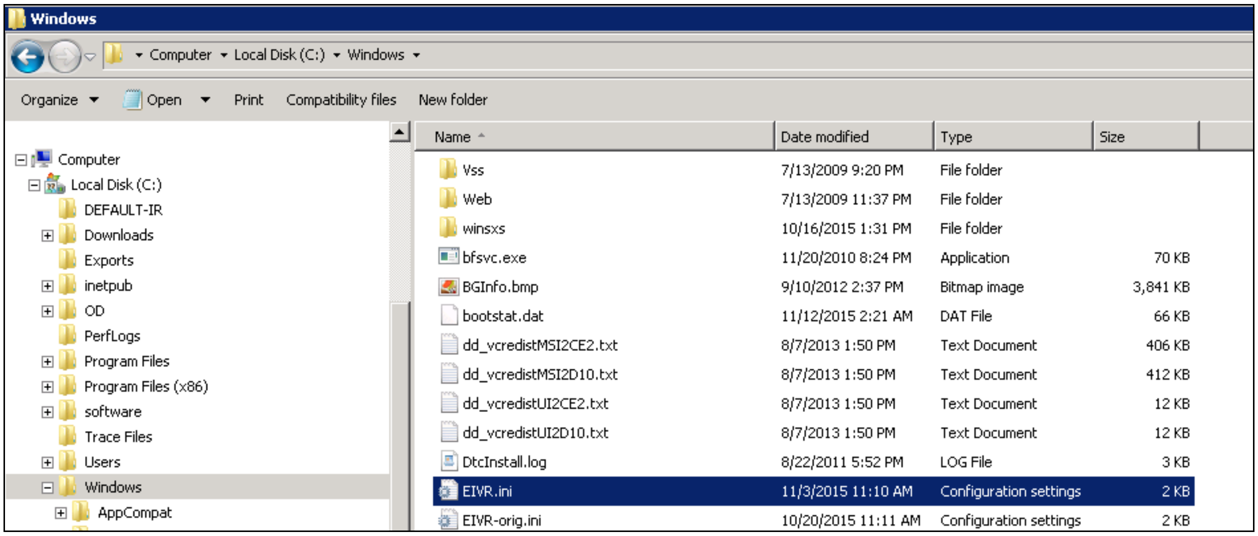
Select the **Channel** tab from the top of the **Base System Configuration** pop-up screen.

In the **Channel Setting** sub-section, select the first channel entry. For **Extension**, enter the applicable extension used for the inbound application, in this case “72061”. By default, all third party channel resources are used for inbound applications unless otherwise specified. Note that the compliance testing used five channel resources, which is governed by the Dialogic license.

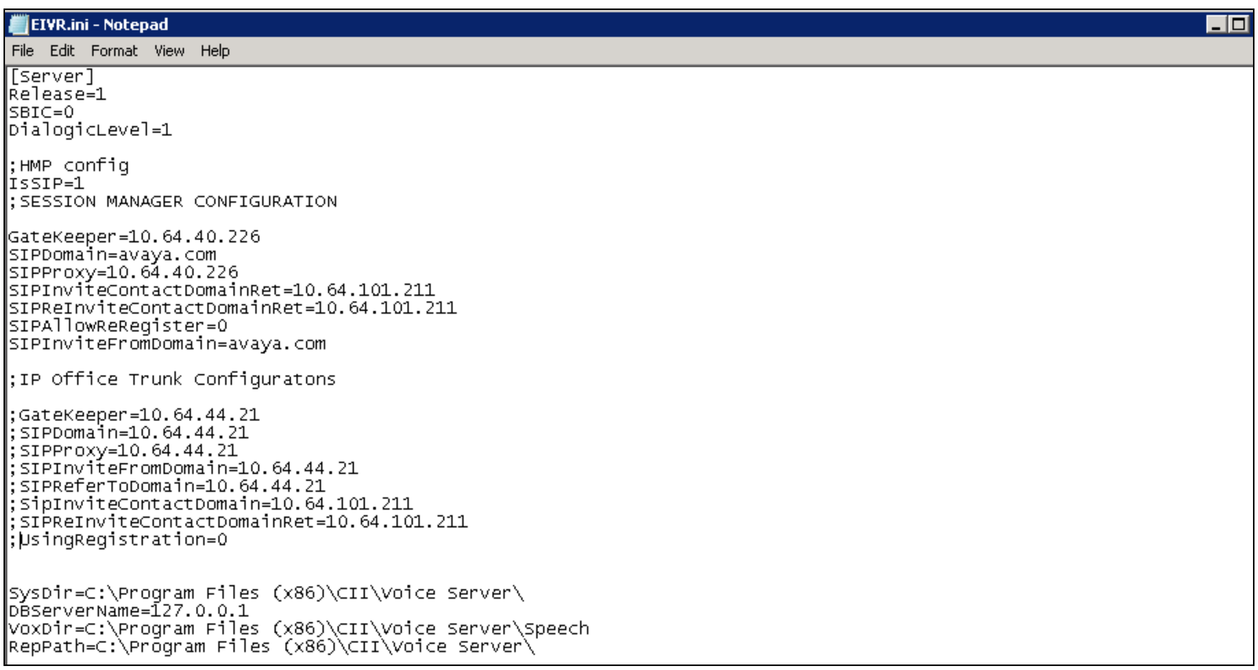
In the compliance testing, only one inbound application was used, and therefore only the first channel resource needs the extension mapping.

7.2. Administer EIVR.ini

From the eONE server, navigate to the **C:\Windows** directory to locate the **EIVR.ini** file shown below.

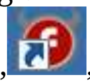


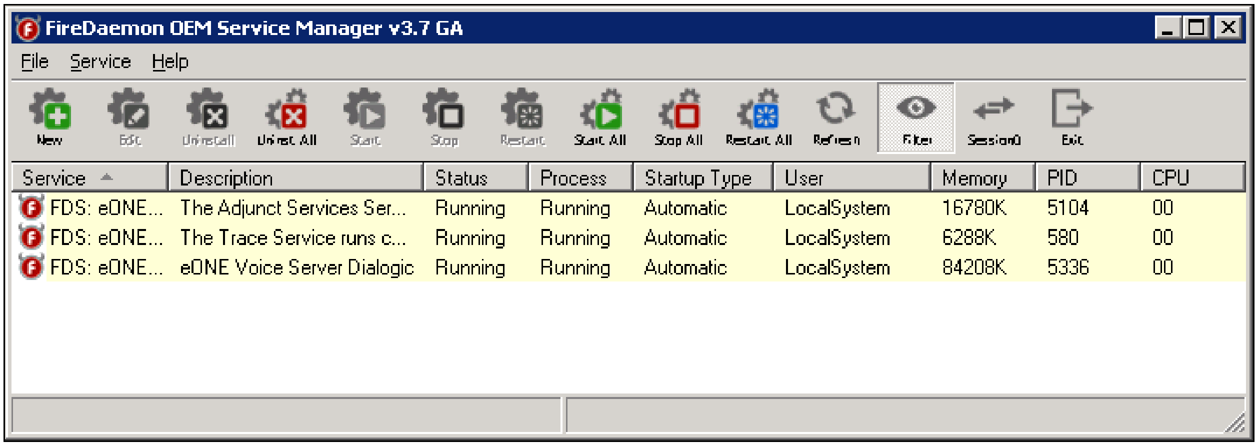
Open the **EIVR.ini** file with the Notepad application. Configure the parameters as shown below, where "10.64.40.226" is the IP address of the Session Manager signaling interface, "10.64.101.211" is the IP address of the eONE server, and "avaya.com" is the domain name from **Section 5.6**.




```
[Server]
Release=1
SBIC=0
DialogicLevel=1

;HMP config
IsSIP=1
;SESSION MANAGER CONFIGURATION

GateKeeper=10.64.40.226
SIPDomain=avaya.com
SIPProxy=10.64.40.226
SIPInviteContactDomainRet=10.64.101.211
SIPReInviteContactDomainRet=10.64.101.211
SIPAllowReRegister=0
SIPInviteFromDomain=avaya.com

;IP Office Trunk Configuratons

;GateKeeper=10.64.44.21
;SIPDomain=10.64.44.21
;SIPProxy=10.64.44.21
;SIPInviteFromDomain=10.64.44.21
;SIPReferToDomain=10.64.44.21
;SipInviteContactDomain=10.64.101.211
;SIPReInviteContactDomainRet=10.64.101.211
;UsingRegistration=0


SysDir=C:\Program Files (x86)\CII\Voice Server\
DBServerName=127.0.0.1
VoxDir=C:\Program Files (x86)\CII\Voice Server\Speech
RepPath=C:\Program Files (x86)\CII\Voice Server\
```

7.3. Restart Service

Run the c:\Program Files (x86)\FireDaemon OEM\FireDaemonUI.exe or select the **Service Manager** icon, , from Desktop to display the screen below. Restart the **eONE Voice Server Dialogic** service.



8. Verification Steps

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

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 5.3**. Verify that all trunks are in the "in-service/idle" state as shown below.

```
status trunk 92

                             TRUNK GROUP STATUS

Member   Port     Service State      Mtce Connected Ports
                                     Busy

0092/001 T00006   in-service/idle    no
0092/002 T00007   in-service/idle    no
0092/003 T00008   in-service/idle    no
0092/004 T00009   in-service/idle    no
0092/005 T00010   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.

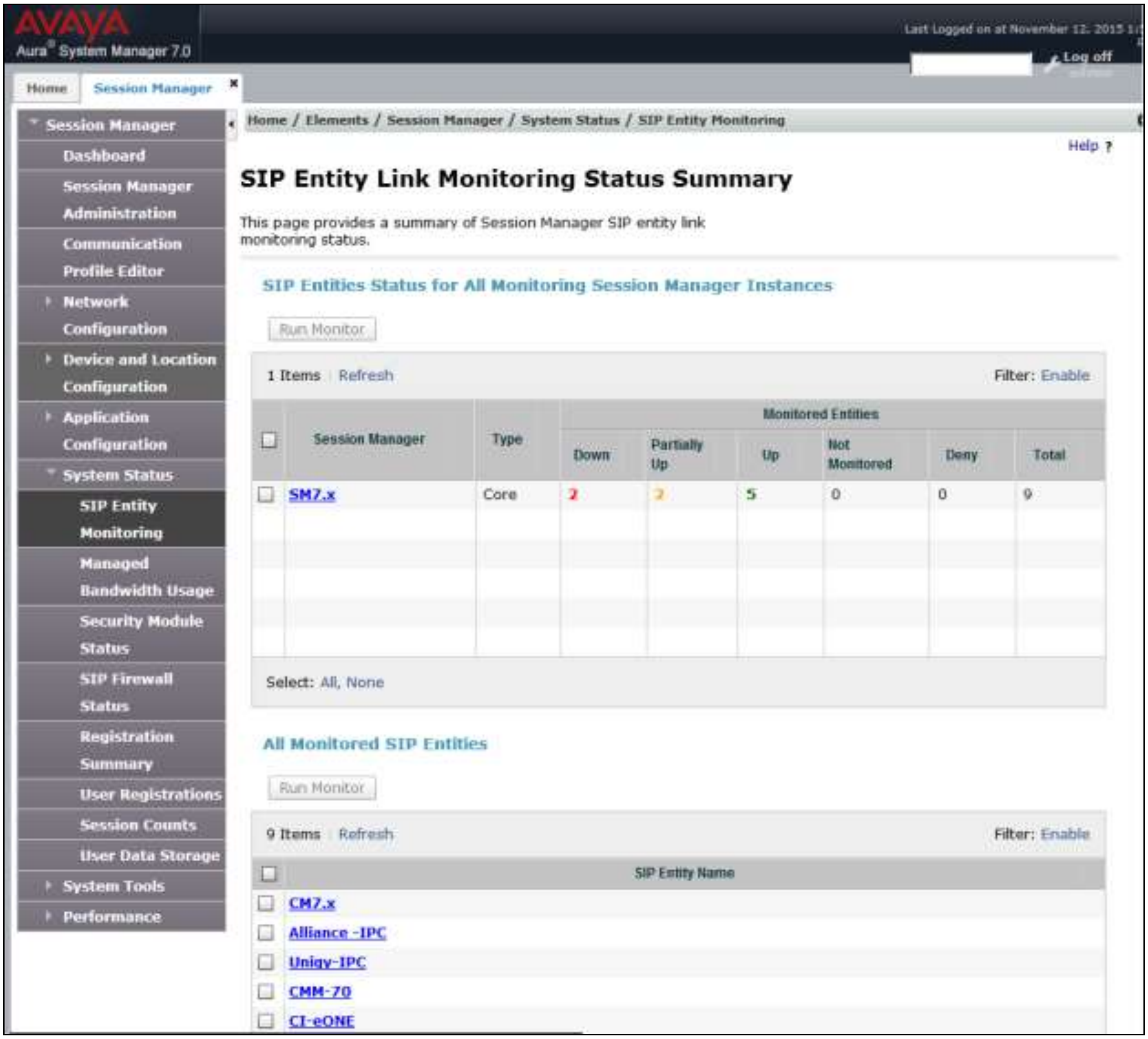
```
status signaling-group 92
                         STATUS SIGNALING GROUP

        Group ID: 92
      Group Type: sip

     Group State: in-service
```

8.2. Verify Avaya Aura® Session Manager

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

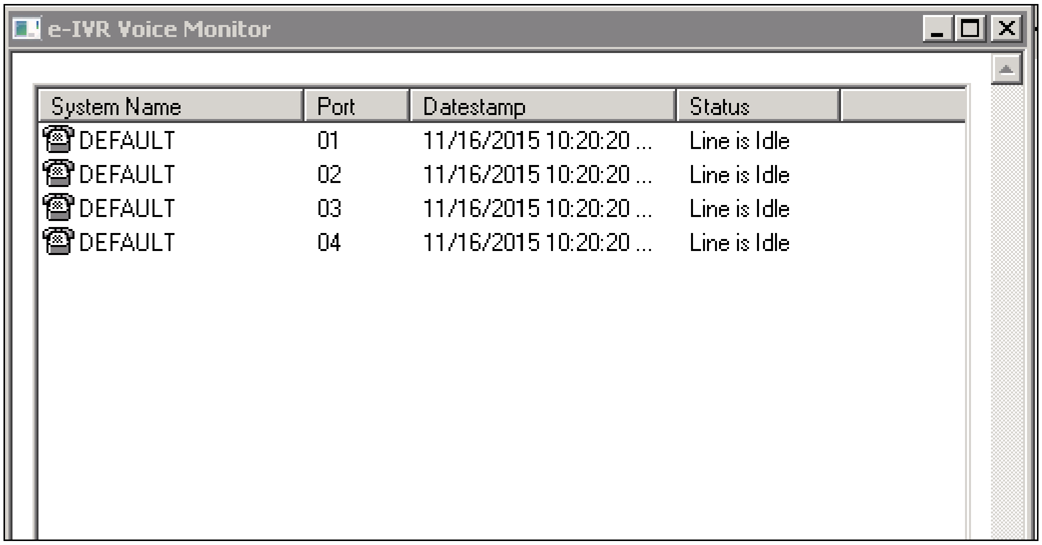
Select **Session Manager → System Status → SIP Entity Monitoring** from the left pane to display the **SIP Entity Link Monitoring Status Summary** screen. Click the eONE entity name from **Section 6.2.1**.

The **SIP Entity, Entity Link Connection Status** screen is displayed. Verify that the **Conn Status** and **Link Status** are "Up".



8.3. Verify Computer Instruments eONE

Select the **Voice Monitor** icon, , from Desktop to display the **eONE Voice Monitor** screen. Verify that the **Status** for all ports is "Line is Idle", as shown below.



9. Conclusion

These Application Notes describe the configuration steps required for Computer Instruments eONE to successfully interoperate with Avaya Aura® Communication Manager and Avaya Aura® Session Manager using SIP trunks. All feature and serviceability test cases were completed.

10. Additional References

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

1. *Administering Avaya Aura® Communication Manager*, Document 03-300509, Issue 1, Release 7.0, August 2015, available at http://support.avaya.com.

2. *Administering Avaya Aura® Session Manager*, Release 7.0 Issue 1, August 2015, available at http://support.avaya.com.

3. *Installing eONE*, available from http://www.instruments.com.

4. *eONE Application Server*, available from http://www.instruments.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.