



## **Avaya Solution & Interoperability Test Lab**

---

# **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.

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

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

# 1. Introduction

These Application Notes describe the configuration steps required for Computer Instruments eONE to interoperate with Avaya Aura® Communication Manager (Communication Manager) and Avaya Aura® Session Manager (Session Manager) using SIP trunks. Computer Instruments eONE (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 was deployed on cloud.

## 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.

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.

This test was conducted in a lab environment simulating a basic customer enterprise network environment. The testing focused on the standards-based interface between the Avaya solution and the third party solution. The results of testing are therefore considered to be applicable to either a premise-based deployment or to a hosted or cloud deployment where some elements of the third party solution may reside beyond the boundaries of the enterprise network, or at a different physical location from the Avaya components.

Readers should be aware that network behaviors (e.g. jitter, packet loss, delay, speed, etc.) can vary significantly from one location to another, and may affect the reliability or performance of the overall solution. Different network elements (e.g. session border controllers, soft switches, firewalls, NAT appliances, etc.) can also affect how the solution performs.

If a customer is considering implementation of this solution in a cloud environment, the customer should evaluate and discuss the network characteristics with their cloud service provider and network organizations, and evaluate if the solution is viable to be deployed in the cloud.

The network characteristics required to support this solution are outside the scope of these Application Notes. Readers should consult the appropriate Avaya and third party documentation for the product network requirements. Avaya makes no guarantee that this solution will work in all potential deployment configurations

## **2.1. Interoperability Compliance Testing**

The interoperability compliance test included feature and serviceability testing.

The feature testing included G.711MU, 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.

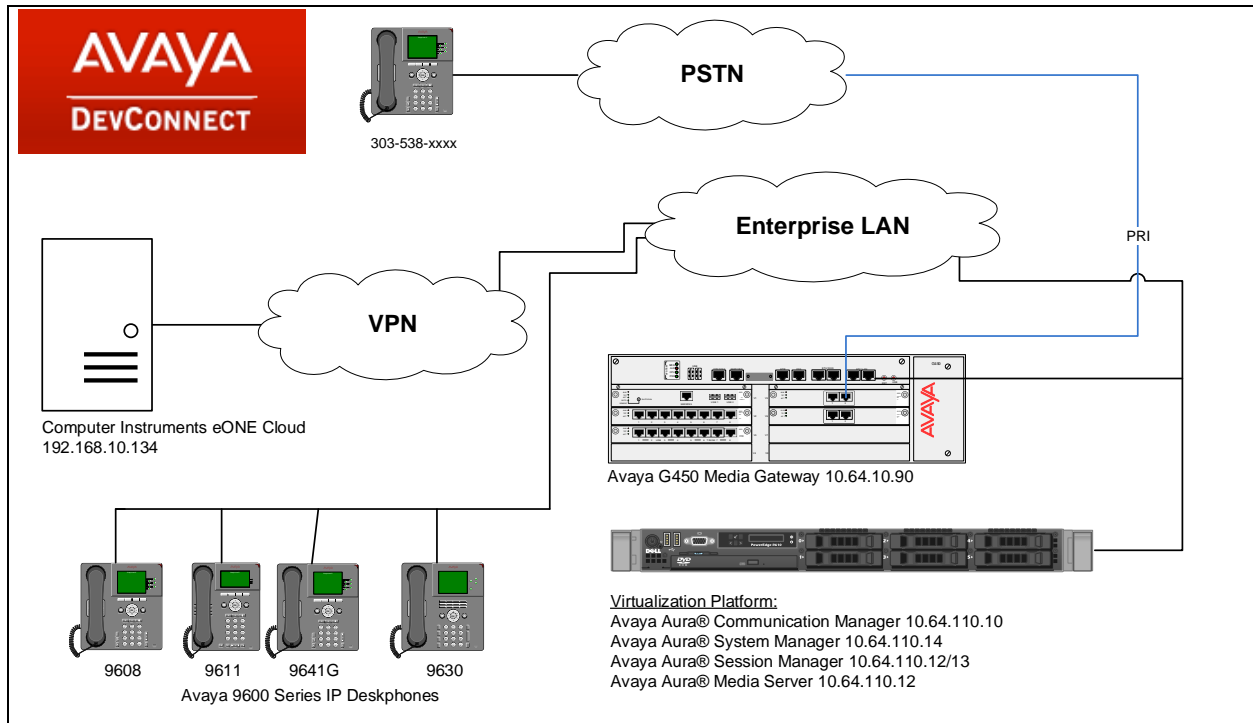
## **2.3. Support**

Technical support on eONE can be obtained through the following:

- **Phone:** (888) 451-0851
- **Email:** [support@instruments.com](mailto:support@instruments.com)
- **WEB:** [http://instruments.com/support/email\\_form.html](http://instruments.com/support/email_form.html) (monitored 24x7)

### 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”. 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	7.1.2.0.0.532.24184 37.19.0
Avaya Aura® Session Manager	7.1.1.0.711008
Avaya Aura® System Manager	7.1.1.0.046931
Avaya 96x0 IP Deskphone (H.323)	3.2.8
Avaya 96x1 IP Deskphone (H.323)	6.6.6
Avaya 96x0 IP Deskphone (SIP)	2.6.17
Avaya 96x1G IP Deskphone (SIP)	7.1.1.0
Computer Instruments eONE	6.1.5

## 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:	12000	0
Maximum Concurrently Registered IP Stations:	18000	3
Maximum Administered Remote Office Trunks:	12000	0
Maximum Concurrently Registered Remote Office Stations:	18000	0
Maximum Concurrently Registered IP eCons:	128	0
Max Concur Registered Unauthenticated H.323 Stations:	100	0
Maximum Video Capable Stations:	36000	0
Maximum Video Capable IP Softphones:	18000	3
<b>Maximum Administered SIP Trunks:</b>	<b>12000</b>	<b>10</b>
Maximum Administered Ad-hoc Video Conferencing Ports:	12000	0
Maximum Number of DS1 Boards with Echo Cancellation:	522	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 1		Page 1 of 22	
TRUNK GROUP			
Group Number: 1	<b>Group Type: sip</b>	CDR Reports: y	
<b>Group Name: asm</b>	COR: 1	TN: 1	<b>TAC: 101</b>
Direction: two-way	Outgoing Display? n	Night Service:	
Dial Access? n			
Queue Length: 0			
<b>Service Type: tie</b>	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 1		Page 3 of 22	
TRUNK FEATURES			
ACA Assignment? n	Measured: none	Maintenance Tests? y	
Suppress # Outpulsing? n	<b>Numbering Format: private</b>		
	UI Treatment: shared		
	Maximum Size of UI Contents: 128		
	Replace Restricted Numbers? n		
	Replace Unavailable Numbers? n		
	Hold/Unhold Notifications? y		
	Modify Tandem Calling Number: no		
Send UCID? y			



## 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” 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 1		Page 1 of 2
SIGNALING GROUP		
Group Number: 1	Group Type: sip	
IMS Enabled? n	Transport Method: tls	
Q-SIP? n		
IP Video? n	Enforce SIPS URI for SRTP? y	
Peer Detection Enabled? y	Peer Server: SM	
Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? y		
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? n		
Alert Incoming SIP Crisis Calls? n		
Near-end Node Name: procr	Far-end Node Name: asm	
Near-end Listen Port: 5061	Far-end Listen Port: 5061	
	Far-end Network Region: 1	
Far-end Domain:		
Incoming Dialog Loopbacks: eliminate	Bypass If IP Threshold Exceeded? n	
DTMF over IP: rtp-payload	RFC 3389 Comfort Noise? n	
Session Establishment Timer(min): 65	Direct IP-IP Audio Connections? y	
Enable Layer 3 Test? y	IP Audio Hairpinning? n	
H.323 Station Outgoing Direct Media? n	Initial IP-IP Direct Media? n	
	Alternate Route Timer(sec): 6	

## 5.5. 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 “10”.

change trunk-group 1		Page 1 of 22	
TRUNK GROUP			
Group Number: 1	Group Type: sip	CDR Reports: y	
Group Name: asm	COR: 1	TN: 1	TAC: 101
Direction: two-way	Outgoing Display? n	Night Service:	
Dial Access? n			
Queue Length: 0			
Service Type: tie	Auth Code? n	Member Assignment Method: auto	
		<b>Signaling Group: 1</b>	
		<b>Number of Members: 10</b>	

## 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 desired. 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          NR Group: 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: 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
    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:	<b>G.711MU</b>	<b>n</b>	<b>2</b>	<b>20</b>		
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 “1”. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Pattern Name:** A descriptive name.
- **Grp No:** The SIP trunk group number from **Section 5.3**.
- **FRL:** A level that allows access to this trunk, with 0 being least restrictive.
- **Numbering Format:** “lev0-pvt”

change route-pattern 1														Page	1 of	3
Pattern Number: 1														Pattern Name:		
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	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 5 and routed to any trunk group will result in a 5-digit calling number. The calling party number will be in the SIP “From” header.

change private-numbering 0					Page 1 of 2	
NUMBERING - PRIVATE FORMAT						
Ext	Ext	Trk	Private	Total		
Len	Code	Grp(s)	Prefix	Len		
5	5			5	Total Administered: 1	
					Maximum Entries: 540	

## 5.10. Administer AAR Analysis

Use the “change aar analysis 511” command, and add an entry to specify how to route calls to 51111. In the example shown below, calls with digits 51111 will be routed as an aar call type using route pattern “1” from **Section 0**.

change aar analysis 511							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	
51111		5	5	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 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.

Recommended access to System Manager is via FQDN.

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

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

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

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

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

User ID:

Password:

[Change Password](#)

**Supported Browsers:** Internet Explorer 11.x or Firefox 48.0, 49.0 and 50.0.

## 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** (not shown) 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 SIP interface.
- **Type:** “SIP Trunk”
- **Notes:** Any desired notes.
- **Location:** Select the eONE location name.
- **Time Zone:** Select the applicable time zone.

The screenshot displays the Avaya Aura System Manager 7.1 web interface. The top navigation bar shows 'Home' and 'Routing' tabs, with 'Routing' selected. The left sidebar contains a tree view with 'SIP Entities' highlighted. The main content area is titled 'SIP Entity Details' and shows the 'General' tab. The form contains the following fields and values:

- Name:** eOne
- FQDN or IP Address:** 192.168.10.134
- Type:** SIP Trunk
- Notes:** (empty)
- Adaptation:** eOne
- Location:** DevConnect
- Time Zone:** America/Fortaleza
- SIP Timer B/F (in seconds):** 4
- Minimum TLS Version:** Use Global Setting
- Credential name:** (empty)
- Securable:** ☐
- Call Detail Recording:** egress

Buttons for 'Commit', 'Cancel', and 'Help ?' are located at the top right of the form area.

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

- **SIP Entity 1:** The Session Manager entity name, in this case “asm”.
- **Protocol:** “UDP”
- **Port:** “5060”
- **SIP Entity 2:** The eONE entity name from this section.
- **Port:** “5060”

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

AVAYA  
Aura® System Manager 7.1

Last Logged on at February 1, 2018 10:55 AM  
Go... Log off admin

Home Routing

Home / Elements / Routing / Entity Links

**Entity Links** Commit Cancel

1 Item Filter: Enable

<input type="checkbox"/>	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	DNS Override
<input type="checkbox"/>	*asm_eOne_5060_UDP	*asm	UDP	*5060	*eOne	*5060	<input type="checkbox"/>

Select : All, None



### 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.
- **Location:** Select the applicable location for Communication Manager.
- **Time Zone:** Select the applicable time zone.

The screenshot shows the Avaya Aura System Manager 7.1 interface. The left navigation pane is expanded to 'Routing', and 'SIP Entities' is selected. The main content area displays the 'SIP Entity Details' form. The form has a 'General' tab selected. The fields and their values are as follows:

- Name:** acm
- FQDN or IP Address:** 10.64.110.10
- Type:** CM
- Notes:** (empty)
- Adaptation:** (empty)
- Location:** DevConnect
- Time Zone:** America/Denver
- SIP Timer B/F (in seconds):** 4
- Minimum TLS Version:** Use Global Setting
- Credential name:** (empty)
- Securable:** ☐
- Call Detail Recording:** 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.

- **SIP Entity 1:** The Session Manager entity name, in this case “asm”.
- **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**.

Avaya Aura System Manager 7.1

Last Logged on at February 1, 2018 10:55 AM

Go... Log off admin

Home Routing

Home / Elements / Routing / Entity Links

Entity Links

Commit Cancel

1 Item Filter: Enable

	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	DNS Override
<input type="checkbox"/>	asm_acm_5061_TLS	asm	TLS	5061	acm	5061	

Select : All, None

## 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.

AVAYA  
Aura® System Manager 7.1

Last Logged on at February 1, 2018  
10:55 AM  
GO... Log off admin

Home Routing x

Home / Elements / Routing / Routing Policies

Routing Policy Details

Commit Cancel

General

\* Name: eOne

Disabled: ☐

\* Retries: 0

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
eOne	192.168.10.134	SIP Trunk	

### 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.

AVAYA  
Aura® System Manager 7.1

Last Logged on at February 1, 2018 10:55 AM  
Go... Log off admin

Home Routing

Home / Elements / Routing / Routing Policies

**Routing Policy Details** Commit Cancel Help ?

**General**

\* Name: acm

Disabled: ☐

\* Retries: 0

Notes:

**SIP Entity as Destination**

Select

Name	FQDN or IP Address	Type	Notes
acm	10.64.110.10	CM	

## 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 “51111”.
- **Min:** The minimum number of digits to match.
- **Max:** The maximum number of digits to match.

In the **Originating Locations and Routing Policies** sub-section, click **Add** and select the routing policy for reaching eONE.

**AVAYA**  
Aura® System Manager 7.1

Last Logged on at February 1, 2018 10:55 AM  
Go... Log off admin

Home Routing x

Home / Elements / Routing / Dial Patterns

### Dial Pattern Details

Commit Cancel Help ?

**General**

\* Pattern: 51111

\* Min: 5

\* Max: 5

Emergency Call: ☐

Emergency Priority: 1

Emergency Type:

SIP Domain: -ALL- ▼

Notes:

**Originating Locations and Routing Policies**

Add Remove

1 Item Filter: Enable

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

Select : All, None

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

The screenshot displays the Avaya Aura System Manager 7.1 web interface. The top navigation bar includes the Avaya logo, the text 'Aura® System Manager 7.1', and a 'Go...' search field. The user is logged in as 'admin' and the session was last logged on at February 1, 2018, 10:55 AM. The left sidebar shows a tree view with 'Routing' expanded, containing sub-items like Domains, Locations, Adaptations, SIP Entities, Entity Links, Time Ranges, Routing Policies, **Dial Patterns**, Regular Expressions, and Defaults. The main content area shows the breadcrumb 'Home / Elements / Routing / Dial Patterns' and a 'Help ?' link. The 'Originating Location' section has a 'Select' button and a 'Cancel' button. Below it, a checkbox 'Apply The Selected Routing Policies to All Originating Locations' is present. A table lists 1 item with columns 'Name' and 'Notes'. The item 'DevConnect' is checked. Below this table is a 'Select : All, None' dropdown. The 'Routing Policies' section shows a table with 10 items, columns 'Name', 'Disabled', 'Destination', and 'Notes'. The item 'eOne' is checked in the 'Name' column. The 'Destination' column shows 'aac', 'aaep', 'acm', 'aps', 'cmm', 'eOne', and 'eq-mgmt'.

**Originating Location**

Select Cancel

**Originating Location**

☐ Apply The Selected Routing Policies to All Originating Locations

1 Item Filter: Enable

<input checked="" type="checkbox"/>	Name	Notes
<input checked="" type="checkbox"/>	DevConnect	

Select : All, None

**Routing Policies**

10 Items Filter: Enable

<input type="checkbox"/>	Name	Disabled	Destination	Notes
<input type="checkbox"/>	aac	<input type="checkbox"/>	aac	
<input type="checkbox"/>	aaep	<input type="checkbox"/>	aaep	
<input type="checkbox"/>	acm	<input type="checkbox"/>	acm	
<input type="checkbox"/>	aps	<input type="checkbox"/>	aps	
<input type="checkbox"/>	cmm	<input type="checkbox"/>	cmm	
<input checked="" type="checkbox"/>	eOne	<input type="checkbox"/>	eOne	
<input type="checkbox"/>	eq-mgmt	<input type="checkbox"/>	eq-mgmt	

### 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.

Follow the procedures in this section to make similar changes to applicable Communication Manager dial patterns to reach the PSTN. In the compliance testing, eONE will add the prefix “9” for outbound calls to the PSTN, and therefore the existing dial pattern for “9” was also changed (not shown below).

**AVAYA**  
Aura® System Manager 7.1

Last Logged on at February 1, 2018 10:55 AM  
Go... Log off admin

Home Routing

Home / Elements / Routing / Dial Patterns

### Dial Pattern Details

Commit Cancel Help ?

**General**

\* Pattern: 9

\* Min: 12

\* Max: 12

Emergency Call: ☐

Emergency Priority: 1

Emergency Type:

SIP Domain: -ALL-

Notes:

**Originating Locations and Routing Policies**

Add Remove

1 Item Filter: Enable

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

Select : All, None

## 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

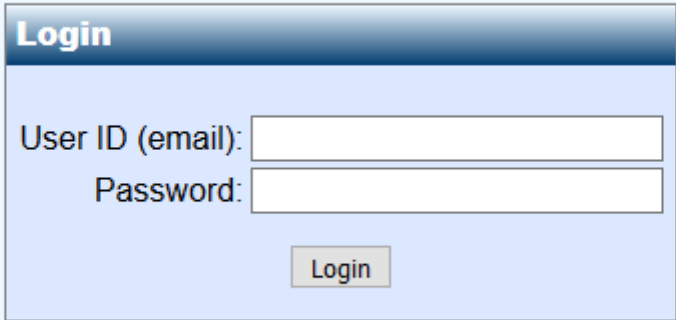
### 7.1. Administer System Config

Computer Instruments engineers installed/licensed/configured eONE cloud IVR. This section shows what was configured by the Computer Instruments engineers. For more information, please contact the Computer Instruments support, mentioned in **Section 2.3**.

To access the **System Config** page, navigate to:

<http://<ip-address>/eCI/VoiceAdmin/Default.aspx>, where <ip-address> is the ip address of eONE server.

Provide appropriate credentials on 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** screen. Select “Avaya Definity” for **PBX Integration**. For **Dial Plan Digits**, enter the maximum length of internal extensions on Avaya IP Office. For **Outside Line Access Prefix**, enter the applicable prefix for calls to the PSTN via Avaya IP Office.

OUTCALL GROUP	START	END
Message Lamp	1	1
Notification Outcall	1	1
Call Me Back Now!	1	4

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 “51111”. By default, all third party channel resources are used for inbound applications unless otherwise specified. Select **Update** to update the extension value.

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

The screenshot shows the 'Base System Configuration' window with the 'Channel' tab selected. The 'Channel Settings' section is active, showing a table of channel entries. The first entry, with extension 51111, is highlighted. Below the table, the 'Extension' field is set to 51111, and the 'Update' button is visible. The 'DNIS/MODE Settings' section is also visible on the right.

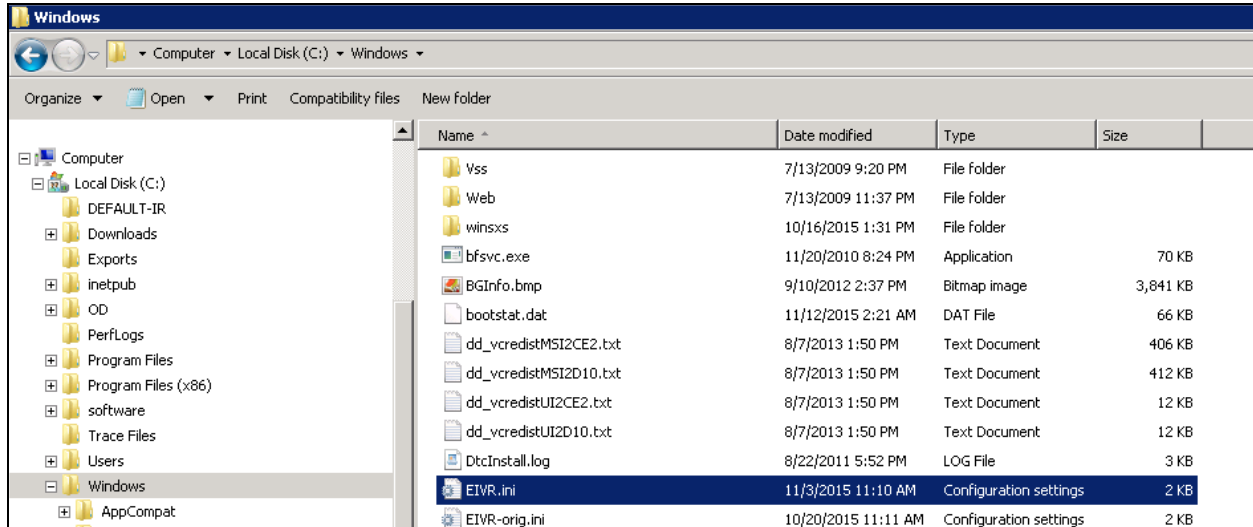
EXTENSION	APPLICATION	REG ?	Ch. #
51111	Default Application	False	1
51112	Default Application	False	2
51113	Default Application	False	3

Application: 1000 - Default Application  
Extension: 51111  
REG ? ☐ Update

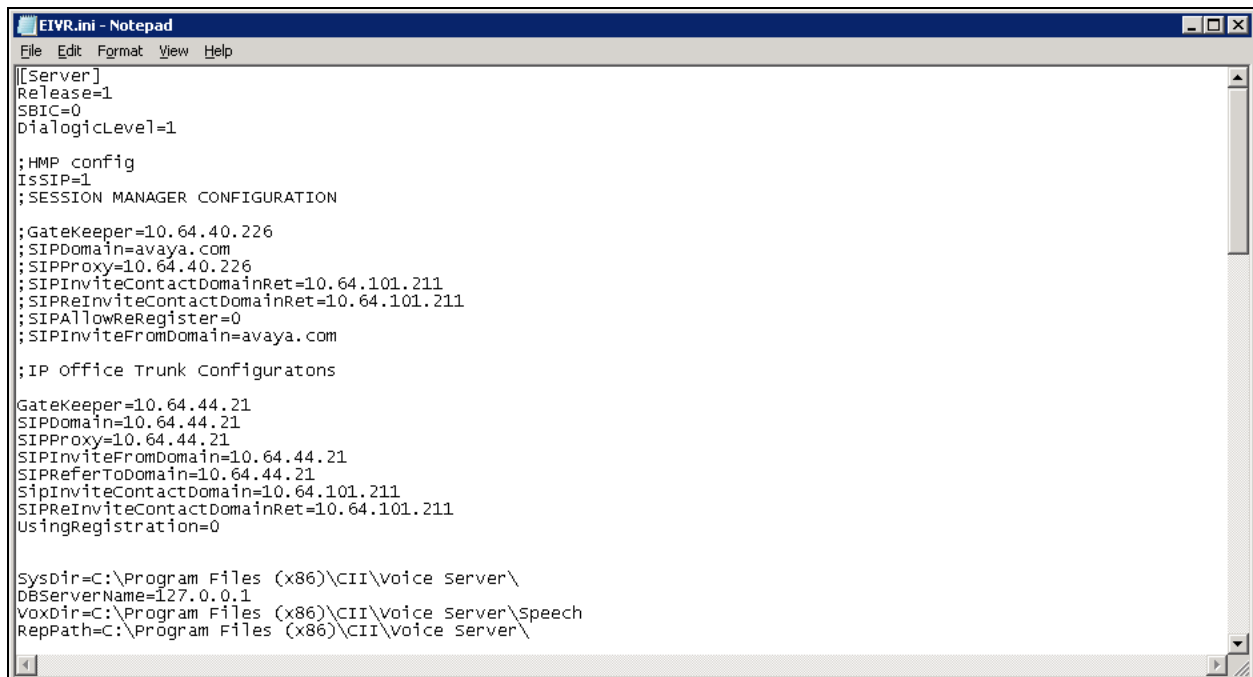
DNIS:   
Application:   
Save Delete

## 7.2. Administer EIVR.ini

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




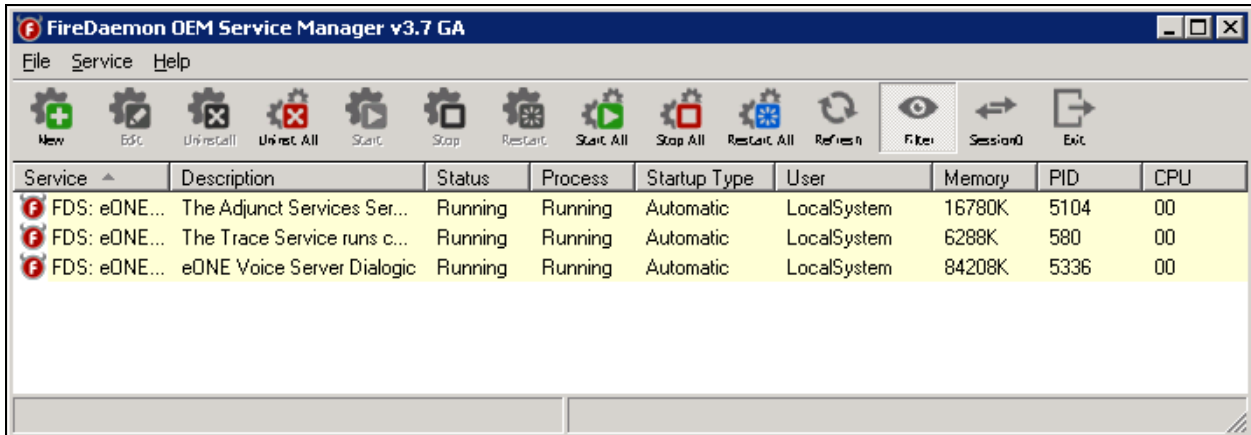
Open the **EIVR.ini** file with the Notepad application. Configure the parameters as shown below, where “10.64.110.65” is the IP address of Session Manager, “192.168.10.134” is the IP address of the eONE server, and “avaya.com” is the domain name. During the compliance test, the domain name is converted to IP address in the hosts file.



### 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 and verify that the **Status** is *Running* as shown below.



The screenshot shows the FireDaemon OEM Service Manager v3.7 GA application window. The title bar is blue with the text "FireDaemon OEM Service Manager v3.7 GA". Below the title bar is a menu bar with "File", "Service", and "Help". Under the "Service" menu, there is a toolbar with icons for New, Edit, Uninstall, Uninstall All, Start, Stop, Restart, Start All, Stop All, Restart All, Refresh, Filter, Session, and Exit. The main area contains a table with the following data:

Service	Description	Status	Process	Startup Type	User	Memory	PID	CPU
FDS: eONE...	The Adjunct Services Ser...	Running	Running	Automatic	LocalSystem	16780K	5104	00
FDS: eONE...	The Trace Service runs c...	Running	Running	Automatic	LocalSystem	6288K	580	00
FDS: eONE...	eONE Voice Server Dialogic	Running	Running	Automatic	LocalSystem	84208K	5336	00

## 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 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
```

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 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”.

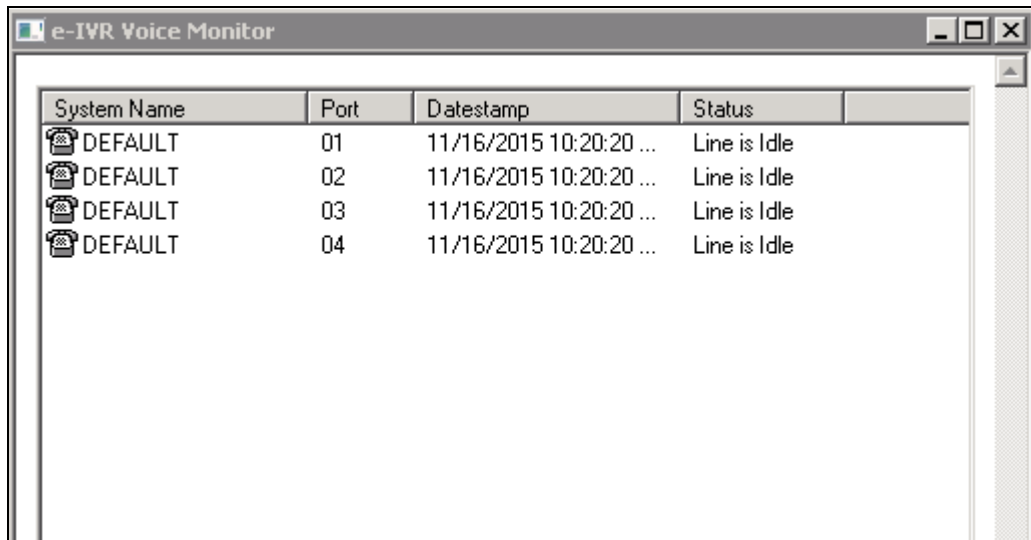
The screenshot shows the Avaya Aura System Manager 7.1 interface. The top navigation bar includes 'Home', 'Routing', and 'Session Manager'. The left sidebar contains a tree view with 'Session Manager' expanded, showing 'Dashboard', 'Session Manager', 'Administration', 'Global Settings', 'Communication Profile Editor', 'Network Configuration', 'Device and Location Configuration', 'Application Configuration', 'System Status', 'SIP Entity Monitoring' (selected), 'Managed Bandwidth Usage', 'Security Module Status', 'SIP Firewall Status', 'Registration Summary', 'User Registrations', and 'Session Counts'. The main content area is titled 'SIP Entity, Entity Link Connection Status' and includes a description: 'This page displays detailed connection status for all entity links from all Session Manager instances to a single SIP entity.' Below this, there is a section for 'All Entity Links to SIP Entity: eOne' with a 'Summary View' button. A table displays the connection status for the selected entity. The table has columns: Session Manager Name, IP Address Family, SIP Entity Resolved IP, Port, Proto., Deny, Conn. Status, Reason Code, and Link Status. The first row shows 'asm' with IP Address Family 'IPv4', SIP Entity Resolved IP '192.168.10.134', Port '5060', Proto. 'UDP', Deny 'FALSE', Conn. Status 'UP', Reason Code '200 OK', and Link Status 'UP'. The table is filtered by 'Enable' and shows 1 item.

Session Manager Name	IP Address Family	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
asm	IPv4	192.168.10.134	5060	UDP	FALSE	UP	200 OK	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.

A screenshot of the 'e-IVR Voice Monitor' application window. The window has a title bar with the text 'e-IVR Voice Monitor' and standard Windows window controls (minimize, maximize, close). Inside the window is a table with four columns: 'System Name', 'Port', 'Datestamp', and 'Status'. There are four rows of data, all showing 'DEFAULT' for the system name, ports 01 through 04, a datestamp of '11/16/2015 10:20:20 ...', and a status of 'Line is Idle'.

System Name	Port	Datestamp	Status
DEFAULT	01	11/16/2015 10:20:20 ...	Line is Idle
DEFAULT	02	11/16/2015 10:20:20 ...	Line is Idle
DEFAULT	03	11/16/2015 10:20:20 ...	Line is Idle
DEFAULT	04	11/16/2015 10:20:20 ...	Line is Idle

## 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 10, Release 7.1, August 2017, available at <http://support.avaya.com>.
2. *Administering Avaya Aura® Session Manager*, Release 7.1, Issue 7, September 2017, 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>.



---

**©2018 Avaya Inc. All Rights Reserved.**

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

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