



Avaya Solution & Interoperability Test Lab

Application Notes for Computer Instruments 7.0 with Avaya Aura® Session Manager 8.1 – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for Computer Instruments eONE 7.0 to interoperate with Avaya Aura® Session Manager 8.1 and Avaya Aura® Communication Manager 8.1. Computer Instruments eONE is an IVR development platform that provides self-service IVR and Web applications.

In the compliance testing, Computer Instruments eONE used SIP trunk with 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 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 DevConnect Program at the Avaya Solution and Interoperability Test Lab.

1. Introduction

These Application Notes describe the configuration steps required for the Computer Instruments eONE 7.0 to interoperate with Avaya Aura® Session Manager 8.1 and Avaya Aura® Communication Manager 8.1. eONE is an IVR development platform that provides self-service IVR and Web applications.

In the compliance testing, eONE used SIP trunk with Session Manager to support inbound and outbound IVR applications.

The eONE solution consisted of distributed components across multiple servers. The eONE solution used in the compliance testing utilized two servers – an eONE server and a Media server. The eONE server is responsible for eONE configuration via a web-based interface and included the CIMedia MRCP Connector for support of text-to-speech (TTS). The Media server is responsible for SIP trunk connection with Session Manager and included the CIMedia ARC SIP Telecom Services for support of SIP protocol and the CIMedia ARC VXML Services for support of VXML.

eONE supports both on-premise and cloud deployments, and the compliance testing used the on-premise deployment method with eONE residing in the DevConnect test lab.

To facilitate testing, two custom applications were developed by Computer Instruments for testing of inbound and outbound applications that included greetings, menu option selection via DTMF, announcements, and transfer to internal and external destinations.

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 eONE inbound application played greeting and collected DTMF input from the caller to decide on the feature to provide, such as announcement playback and transfer to internal or external destinations.

The eONE outbound application was tested by manually requesting callbacks to users on the PSTN and on Communication Manager. The callback requests were initiated from the Web page associated with the eONE outbound application.

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.

For the testing associated with these Application Notes, the SIP trunk interface between Session Manager and eONE did not include use of any specific encryption features as requested by Computer Instruments.

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 OPTIONS, G.711MU, media shuffling, session refresh, REFER, hold/reconnect, inbound DTMF, dial ahead, outgoing call screening, multiple calls, call forwarding, inbound, outbound, and blind transfer via REFER to internal and external destinations.

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

2.2. Test Results

All test cases were executed and verified.

2.3. Support

Technical support on eONE can be obtained through the following:

- **Phone:** (888) 451-0851
- **Web:** http://instruments.com/tech_support.html
- **Email:** support@instruments.com

3. Reference Configuration

The configuration used for the compliance testing is shown in **Figure 1**. SIP trunk was used between Session Manager and eONE and the applicable domain name was “dr220.com”.

A five-digit Uniform Dial Plan (UDP) was used to facilitate routing with eONE. Unique extensions were assigned to users on Communication Manager (6xxxx) and to eONE (53000).

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.

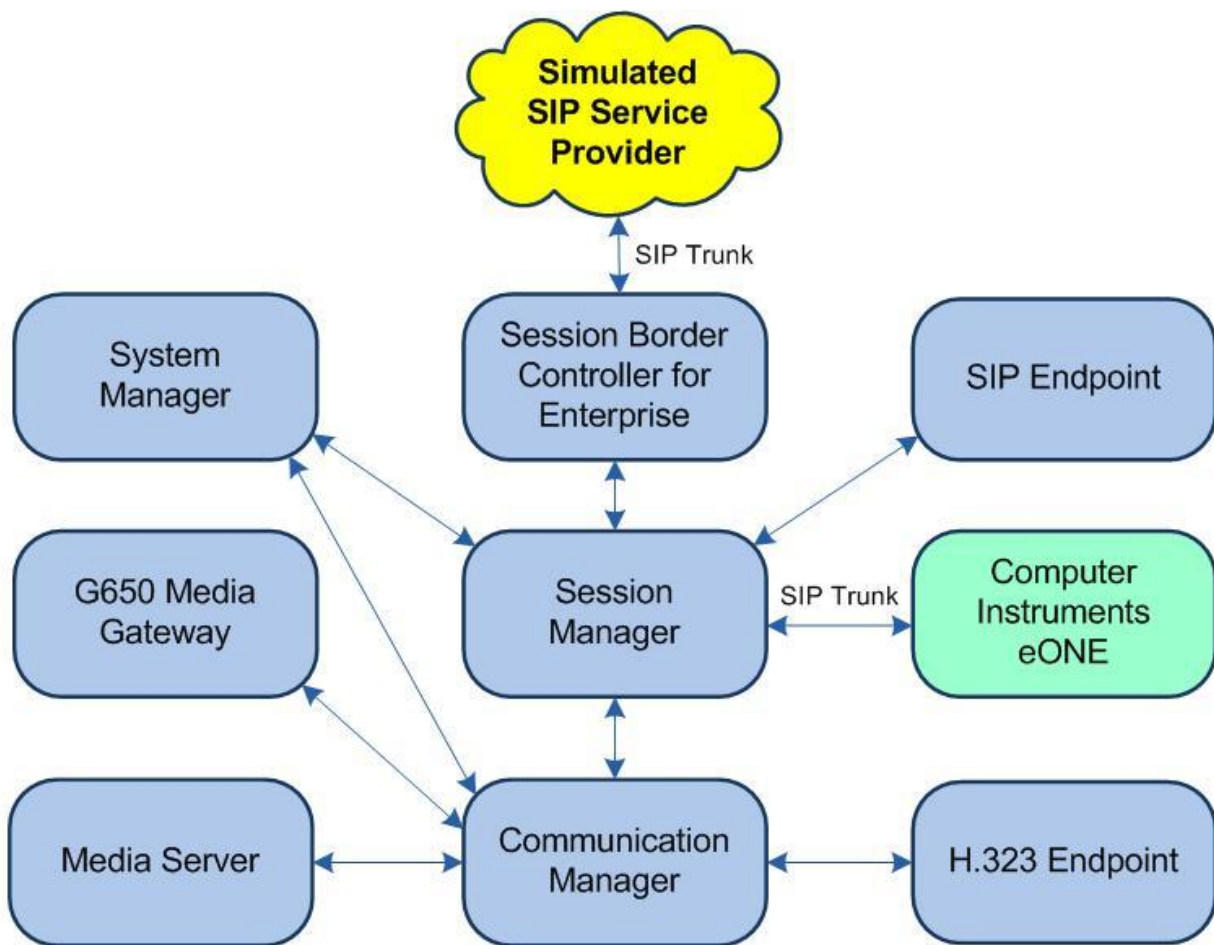


Figure 1: Compliance Testing Configuration

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 in Virtual Environment	8.1 (8.1.2.0.0.890.26095)
Avaya G650 Media Gateway	NA
Avaya Aura® Media Server in Virtual Environment	8.0.2.127
Avaya Aura® Session Manager in Virtual Environment	8.1 (8.1.2.1.812101)
Avaya Aura® System Manager in Virtual Environment	8.1 (8.1.2.0.0611517)
Avaya 9611G IP Deskphone (H.323)	6.8202
Avaya J179 IP Deskphone (SIP)	4.0.2.1.3
Computer Instruments eONE <ul style="list-style-type: none">• CIMedia ARC SIP Telecom Services on Linux• CIMedia arcVXML3.6 Services• CIMedia Arc MRCP Connector	7.0 3.6 Build 12 3.6 Build 11 4.0 Build 24

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 node names
- Administer codec set
- Administer network region
- Administer SIP trunk group
- Administer SIP signaling group
- Administer SIP trunk group members
- 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, the Avaya endpoints used encrypted signaling connections with encrypted media, and a separate set of trunk group, signaling group, network region, and codec set 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 capacity for SIP trunks by comparing the **Maximum Administered SIP Trunks** 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	10	
Maximum Concurrently Registered IP Stations: 18000	2	
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	0	
Maximum Video Capable IP Softphones: 18000	0	
Maximum Administered SIP Trunks: 40000	40	

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? call-wait
      DID/Tie/ISDN/SIP Intercept Treatment: attendant
      Internal Auto-Answer of Attd-Extended/Transferred Calls: transferred
      Automatic Circuit Assurance (ACA) Enabled? n
```

5.3. Administer Node Names

Use the “display node-names ip” command. Note the **Name** and **IP Address** of the processor or existing C-LAN circuit pack that will be used for connectivity with eONE, in this case “procr” and “10.64.101.236”.

Also note the **Name** and **IP Address** of the Session Manager signaling interface, in this case “sm7-sig” and “10.64.101.238”.

```
display node-names ip                                         Page 1 of 2
      IP NODE NAMES
      Name      IP Address
      G430      192.168.200.43
      aes7      10.64.101.239
      clan      10.64.125.32
      default   0.0.0.0
      gateway   10.64.125.1
      medpro    10.64.125.33
      ms7       10.64.101.233
      procr     10.64.101.236
      procr6    ::
      sm7-sig   10.64.101.238
```


5.4. Administer Codec Set

Administer a codec set for integration with eONE. Use the “change ip-codec-set n” command, where “n” is an existing codec set number to use for interoperability.

For **Audio Codec**, enter the pertinent G.711 variant as shown below. Note that eONE only supports the G.711 codec variant. For **Media Encryption** and **Encrypted SRTCP**, retain the default values of “none” and “enforce-unenc-srtcp” as shown below. Retain the default values for the remaining fields.

```
change ip-codec-set 3                                     Page 1 of 2

                                IP MEDIA PARAMETERS

Codec Set: 3

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

Media Encryption                               Encrypted SRTCP: enforce-unenc-srtcp
1: none
```

5.5. Administer Network Region

Administer a network region for integration with eONE. Use the “change ip-network-region n” command, where “n” is an existing network region number to use for interoperability.

Enter the following values for the specified fields and retain the default values for the remaining fields.

- **Authoritative Domain:** The SIP domain from **Section 3**.
- **Name:** A descriptive name.
- **Codec Set:** The codec set number from **Section 5.4**.

```
change ip-network-region 3                               Page 1 of 20

                                IP NETWORK REGION

Region: 3      NR Group: 3
Location:      Authoritative Domain: dr220.com
Name: eONE     Stub Network Region: n
MEDIA PARAMETERS      Intra-region IP-IP Direct Audio: yes
Codec Set: 3          Inter-region IP-IP Direct Audio: yes
UDP Port Min: 2048    IP Audio Hairpinning? n
UDP Port Max: 3329
DIFFSERV/TOS PARAMETERS
Call Control PHB Value: 46
Audio PHB Value: 46
Video PHB Value: 26
```

5.6. Administer SIP Trunk Group

Use the “add trunk-group n” command, where “n” is an available trunk group number, in this case “53”. 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 53		Page 1 of 4	
TRUNK GROUP			
Group Number: 53	Group Type: sip	CDR Reports: y	
Group Name: CI eONE	COR: 1	TN: 1	TAC: 1053
Direction: two-way	Outgoing Display? n	Night Service:	
Dial Access? n	Auth Code? n		
Queue Length: 0	Member Assignment Method: auto		
Service Type: tie	Signaling Group:		
	Number of Members: 0		

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

add trunk-group 53		Page 3 of 4	
TRUNK FEATURES			
ACA Assignment? n	Measured: none	Maintenance Tests? y	
Suppress # Outpulsing? n	Numbering Format: private	UUI Treatment: service-provider	
	Replace Restricted Numbers? n	Replace Unavailable Numbers? n	
	Hold/Unhold Notifications? y	Modify Tandem Calling Number: no	
Show ANSWERED BY on Display? y			

5.7. Administer SIP Signaling Group

Use the “add signaling-group n” command, where “n” is an available signaling group number, in this case “53”. 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:** The processor node name from **Section 5.3**.
- **Far-end Node Name:** The Session Manager node name from **Section 5.3**.
- **Near-end Listen Port:** An available port for integration with eONE.
- **Far-end Listen Port:** The same port number as in **Near-end Listen Port**.
- **Far-end Network Region:** The network region number from **Section 5.5**.
- **Far-end Domain:** The domain name from **Section 3**.

add signaling-group 53		Page 1 of 2
SIGNALING GROUP		
Group Number: 53	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: Others	Clustered? n
Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? n		
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? y		
Alert Incoming SIP Crisis Calls? n		
Near-end Node Name: procr		Far-end Node Name: sm7-sig
Near-end Listen Port: 5361		Far-end Listen Port: 5361
		Far-end Network Region: 3
Far-end Domain: dr220.com		
Incoming Dialog Loopbacks: eliminate		Bypass If IP Threshold Exceeded? n
DTMF over IP: rtp-payload		RFC 3389 Comfort Noise? n
Session Establishment Timer(min): 3		Direct IP-IP Audio Connections? y
Enable Layer 3 Test? y		IP Audio Hairpinning? n
H.323 Station Outgoing Direct Media? n		Initial IP-IP Direct Media? n
		Alternate Route Timer(sec): 6

5.8. Administer SIP Trunk Group Members

Use the “change trunk-group n” command, where “n” is the trunk group number from **Section 5.6**. 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 5.7**.
- **Number of Members:** The desired number of members, in this case “4”.

change trunk-group 53		Page 1 of 4	
TRUNK GROUP			
Group Number: 53	Group Type: sip	CDR Reports: y	
Group Name: CI eONE	COR: 1	TN: 1	TAC: 1053
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: 53			
Number of Members: 4			

5.9. Administer Route Pattern

Use the “change route-pattern n” command, where “n” is an existing route pattern number to be used for integration with eONE, in this case “53”. 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 5.6**.
- **FRL:** A level that allows access to this trunk, with 0 being least restrictive.
- **Numbering Format:** “lev0-pvt”

change route-pattern 53		Page 1 of 4	
Pattern Number: 53		Pattern Name: eONE	
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	
		Intw	
1: 53	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 No. 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

5.10. 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 5.6**.

In the example shown below, all calls originating from a 5-digit extension beginning with 6 and routed to trunk group 53 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	6	66		5	Total Administered: 1
5	6	53		5	Maximum Entries: 540

5.11. Administer Uniform Dial Plan

This section provides a sample AAR routing used for routing calls with dialed digits 53000 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 of digits 53000, 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	
53000	5	0	aar	n	

5.12. Administer AAR Analysis

Use the “change aar analysis 0” command and add an entry to specify how to route calls to eONE at 53000. In the example shown below, calls with digits 53000 will be routed as an AAR call using route pattern “53” from **Section 5.9**.

change aar analysis 0					Page 1 of 2
AAR DIGIT ANALYSIS TABLE					
Location: all					Percent Full: 2
Dialed		Total	Route	Call	Node
String		Min Max	Pattern	Type	Num
53000		5 5	53	aar	n

5.13. 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 “212”. Navigate to **Page 3**.

For **Modify Tandem Calling Number**, enter “tandem-cpn-form” to allow modification of calling party number for calls to the PSTN.

change trunk-group 212		Page 3 of 5
TRUNK FEATURES		
ACA Assignment? n	Measured: none	Maintenance Tests? y
Suppress # Outpulsing? n	Format: public	
	UUI IE Treatment: shared	
	Maximum Size of UUI Contents? 128	
	Replace Restricted Numbers? n	
	Replace Unavailable Numbers? n	
	Hold/Unhold Notifications? n	
	Modify Tandem Calling Number: tandem-cpn-form	
Send UCID? y		
Show ANSWERED BY on Display? y		

5.14. Administer Tandem Calling Party Number

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

In the example shown below, all calls originating from 53000 and routed to the PSTN trunk group in **Section 5.13** will result in a 10-digit calling number. For **Outgoing Number Format**, use an applicable format, in this case “pub-unk”.

change tandem-calling-party-num						Page 1 of 67
CALLING PARTY NUMBER CONVERSION						
FOR TANDEM CALLS						
	CPN	Incoming	Outgoing			Outgoing
		Number	Trunk			Number
Len	Prefix	Format	Group(s)	Delete	Insert	Format
5	53000		212		30353	pub-unk

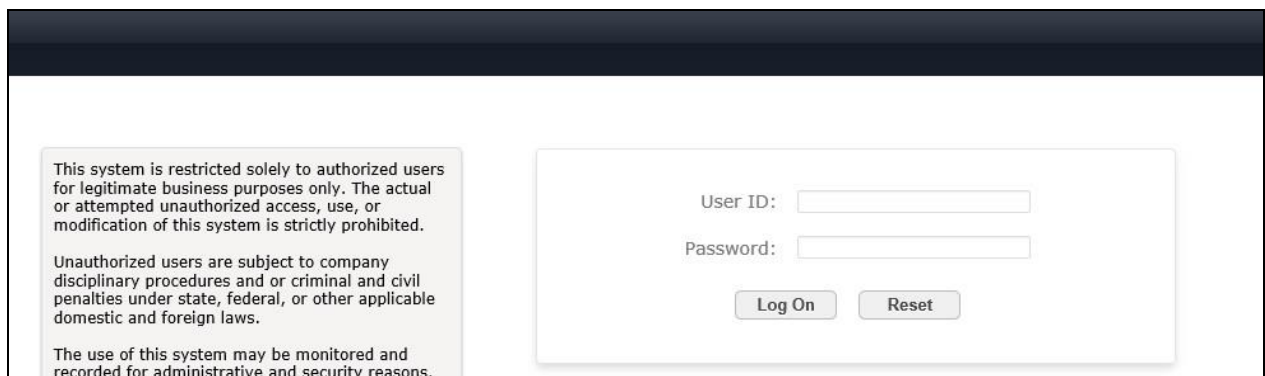
6. Configure Avaya Aura® Session Manager

This section provides the procedures for configuring Session Manager, which is performed via the web interface of System Manager. The procedures include the following areas:

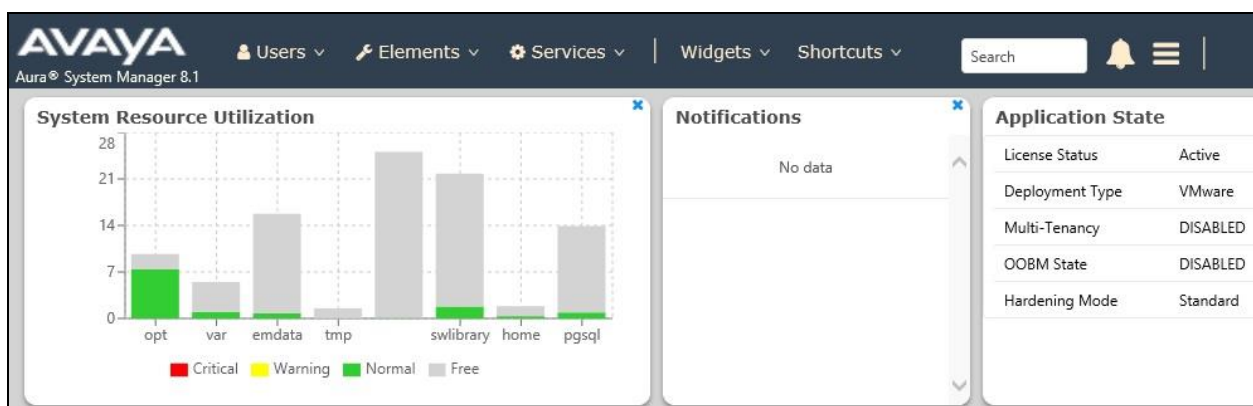
- Launch System Manager
- Administer locations
- Administer SIP entities
- Administer routing policies
- Administer dial patterns

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.

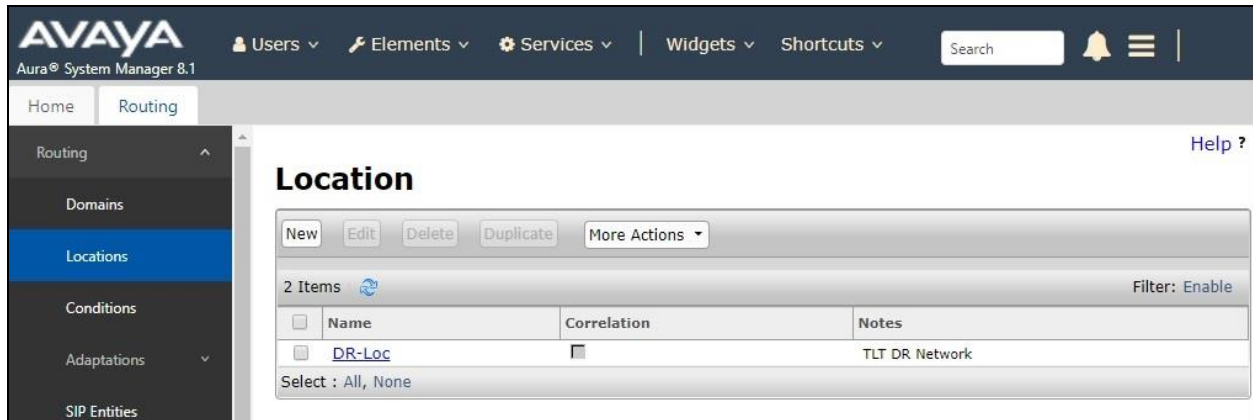


The screen below is displayed next.

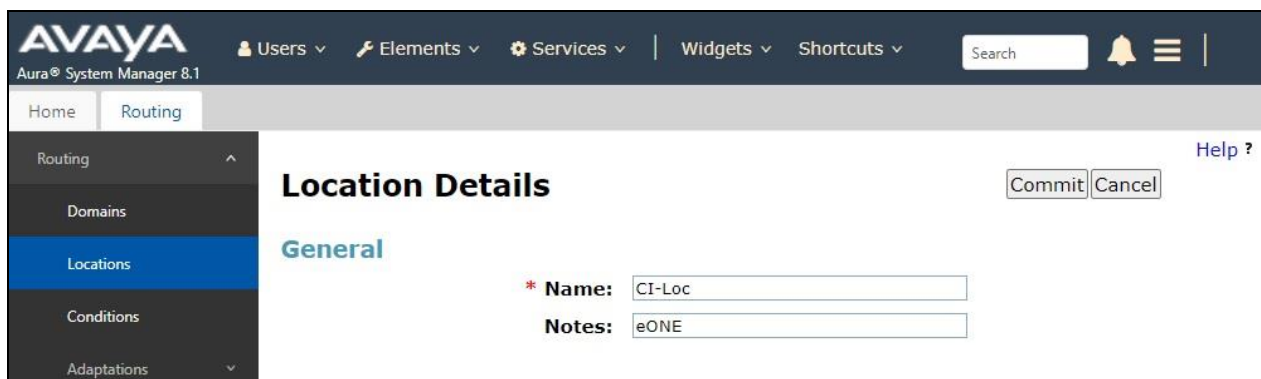


6.2. Administer Locations

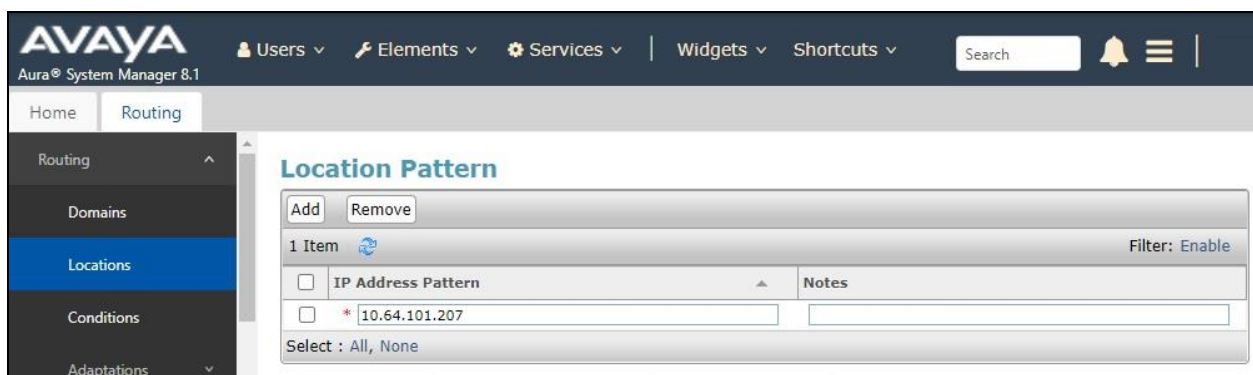
Select **Elements** → **Routing** → **Locations** from the top menu to display the **Location** screen below. Select **New** to add a new location for eONE.



The **Location Details** screen is displayed next. In the **General** sub-section, enter a descriptive **Name** and optional **Notes**.



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



6.3. Administer SIP Entities

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

6.3.1. SIP Entity for eONE

Select **Routing** → **SIP Entities** from the left menu 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 Media server.
- **Type:** “SIP Trunk”
- **Location:** Select the eONE location name from **Section 6.2**.
- **Time Zone:** Select the applicable time zone.

The screenshot shows the Avaya Aura System Manager 8.1 interface. The top navigation bar includes the Avaya logo, 'Aura® System Manager 8.1', and various menu items like Users, Elements, Services, Widgets, and Shortcuts. A search bar and a bell icon are also present. The left-hand navigation menu is expanded, showing 'Routing' as the selected category, with 'SIP Entities' highlighted. The main content area displays the 'SIP Entity Details' form. The form has a 'General' tab selected, showing fields for Name, FQDN or IP Address, Type, Notes, Adaptation, Location, Time Zone, SIP Timer B/F, Minimum TLS Version, Credential name, Securable, and Call Detail Recording. The 'Loop Detection' tab is visible at the bottom. The form includes 'Commit' and 'Cancel' buttons in the top right corner.

Field	Value
Name	eONE
FQDN or IP Address	10.64.101.207
Type	SIP Trunk
Notes	eONE Media Server
Adaptation	
Location	CI-Loc
Time Zone	America/New_York
SIP Timer B/F (in seconds)	4
Minimum TLS Version	Use Global Setting
Credential name	
Securable	<input type="checkbox"/>
Call Detail Recording	egress

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 “DR-SM”.
- **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, TCP, and TLS, with UDP used in the testing.

Entity Links

Override Port & Transport with DNS SRV: ☐

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy
* SM-eONE	DR-SM	UDP	* 5060	eONE	* 5060	trusted

Select : All, None

6.3.2. SIP Entity for Communication Manager

Select **Routing** → **SIP Entities** from the left menu 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 processor or C-LAN circuit pack IP address from **Section 5.3**.
- **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 8.1 interface. The top navigation bar includes the Avaya logo, 'Aura® System Manager 8.1', and various menu items: Users, Elements, Services, Widgets, and Shortcuts. A search bar and a help icon are also present. The left sidebar shows a list of navigation options: Home, Routing, Domains, Locations, Conditions, Adaptations, SIP Entities (selected), Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area displays the 'SIP Entity Details' screen. The title 'SIP Entity Details' is at the top, with 'Commit' and 'Cancel' buttons. Below the title is the 'General' tab. The form contains the following fields:

- Name:** DR-CM-5361
- FQDN or IP Address:** 10.64.101.236
- Type:** CM
- Notes:** CM port 5361 for eONE
- Adaptation:** (empty dropdown)
- Location:** DR-Loc
- Time Zone:** America/New_York
- SIP Timer B/F (in seconds):** 4
- Minimum TLS Version:** Use Global Setting
- Credential name:** (empty text field)
- Securable:** ☐
- Call Detail Recording:** none

At the bottom of the form, the 'Loop Detection' tab is visible.

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 “DR-SM”.
- **Protocol:** The signaling group transport method from **Section 5.7**.
- **Port:** The signaling group far-end listen port number from **Section 5.7**.
- **SIP Entity 2:** The Communication Manager entity name from this section.
- **Port:** The signaling group near-end listen port number from **Section 5.7**.
- **Connection Policy:** “trusted”

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
* SM-CM-5361	DR-SM	TLS	* 5361	DR-CM-5361	* 5361	trusted

Select : All, None

SIP Responses to an OPTIONS Request

6.4. Administer Routing Policies

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

6.4.1. 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**. 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 eONE entity name from **Section 6.3.1**. The screen below shows the result of the selection.

AVAYA

Aura® System Manager 8.1

Users

Elements

Services

Widgets

Shortcuts

Search

Home

Routing

Domains

Locations

Conditions

Adaptations

SIP Entities

Entity Links

Time Ranges

Routing Policies

Dial Patterns

Routing Policy Details

Commit Cancel

Help ?

General

* Name: To-eONE

Disabled: ☐

* Retries: 0

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
eONE	10.64.101.207	SIP Trunk	eONE Media Server

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 **SIP Entity as Destination** sub-section, click **Select** and select the Communication Manager entity name from **Section 6.3.2**. The screen below shows the result of the selection.

AVAYA

Aura® System Manager 8.1

Users

Elements

Services

Widgets

Shortcuts

Search

Home

Routing

Routing

Domains

Locations

Conditions

Adaptations

SIP Entities

Entity Links

Time Ranges

Routing Policies

Routing Policy Details

Commit Cancel

Help ?

General

* Name: To-CM-5361

Disabled: ☐

* Retries: 0

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
DR-CM-5361	10.64.101.236	CM	CM port 5361 for eONE

6.5. Administer Dial Patterns

Add a new dial pattern for eONE and update existing dial patterns for Communication Manager to allow calls from eONE.

6.5.1. 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:** The eONE extension from **Section 3**.
- **Min:** The minimum number of digits to match.
- **Max:** The maximum number of digits to match.

In the **Originating Locations and Routing Policies** sub-section, click **Add** and create an entry for reaching eONE. In the compliance testing, the policy allowed for call origination from Communication Manager location “DR-Loc”. The eONE routing policy from **Section 6.4.1** was selected as shown below.

The screenshot displays the Avaya Aura System Manager 8.1 interface. The left navigation pane shows the 'Routing' menu expanded, with 'Dial Patterns' selected. The main content area is titled 'Dial Pattern Details' and includes 'Commit' and 'Cancel' buttons. The 'General' section contains the following fields:

- Pattern:** 53000
- Min:** 5
- Max:** 5
- Emergency Call:** ☐
- SIP Domain:** -ALL- (dropdown)
- Notes:** (text area)

The 'Originating Locations and Routing Policies' section features an 'Add' button and a table with 2 items. The table has the following columns: Originating Location Name, Originating Location Notes, Routing Policy Name, Rank, Routing Policy Disabled, Routing Policy Destination, and Routing Policy Notes.

Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/> DR-Loc	TLT DR Network	To-eONE	0	<input type="checkbox"/>	eONE	

6.5.2. Dial Pattern for Communication Manager

Select **Routing** → **Dial Patterns** from the left pane and click on the applicable dial pattern for Communication Manager in the subsequent screen, in this case dial pattern “6” (not shown). The **Dial Pattern Details** screen is displayed.

In the **Originating Locations and Routing Policies** sub-section, click **Add** and create a new entry as necessary for calls from eONE. In the compliance testing, the new entry allowed for call origination from the eONE location from **Section 6.2** and the Communication Manager routing policy from **Section 6.4.2** were selected as shown below. Retain the default values in the remaining fields.

Repeat this section to make similar changes to applicable Communication Manager dial pattern to reach the PSTN. In the compliance testing, eONE will add the prefix “91” for outbound calls to the PSTN, and therefore the existing dial pattern for “91” was also changed (not shown below).

AVAYA
Aura® System Manager 8.1

Users ▾ Elements ▾ Services ▾ | Widgets ▾ Shortcuts ▾ Search 🔍 🔔 ☰ |

Home Routing

R...

Dial Pattern Details Commit Cancel Help ?

General

* **Pattern:** 6

* **Min:** 5

* **Max:** 5

Emergency Call: ☐

SIP Domain: -ALL- ▾

Notes: To CM

Originating Locations and Routing Policies

Add Remove

3 Items 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"/>	CI-Loc	eONE	To-CM-5361	0	<input type="checkbox"/>	DR-CM-5361	
<input type="checkbox"/>	DR-Loc	TLT DR Network	To-CM	0	<input type="checkbox"/>	DR-CM	

7. Configure Computer Instruments eONE

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

- Launch web interface
- Administer company management
- Administer system configuration
- Administer collect and store
- Administer extension manager
- Administer menu manager
- Administer VXML file

The configuration of eONE is typically performed by Computer Instruments deployment engineers, and the procedural steps are presented in these Application Notes for informational purposes.

7.1. Launch Web Interface

Access the eONE web interface by using the URL **http://ip-address/eci/voiceadmin/LoginPage.aspx** in a browser window, where “ip-address” is the IP address of the eONE server with the web-based interface.

The **Login** screen below is displayed. Log in using the appropriate credentials.



The screenshot shows a web-based login interface. It features a light blue background. In the center, there is a white rectangular box with a blue header bar containing the word "Login" in white. Below the header, there are two input fields: "User ID:" followed by a text box, and "Password:" followed by a text box. Below these fields is a small button labeled "Login".

The **Welcome to Computer Instruments** screen is displayed next.

Note that the relevant tenant in this case is “CIProduction (19)” as shown below, which was pre-configured.



7.2. Administer Company Management

Expand and select **Web Administrator** → **Company Management** from the left pane to display the **Company Management** screen. Scroll down to the bottom of the screen to select the pertinent company entry and click **Edit** (not shown).

For **PBX Domain/IP**, enter “x|y” where “x” is IP address of the Session Manager signaling interface from **Section 5.3** and “y” is the pertinent IP address of Communication Manager from **Section 5.3**.

For **Time Zone**, select the appropriate zone. For **ASR & TTS**, uncheck resources that are not used. In the compliance testing, only **TTS** was used.

Retain the pre-configured values in the remaining fields.

Company Management

Company Name: CIProduction

PBX Domain/IP: 10.64.101.238|10.64.101.236

Prompt recordings Path: D:\Program Files\CII\Speech\CIProduction\

Exports Path: D:\Exports\CIProduction\

Imports Path: D:\Imports\CIProduction\

VTSystem Database Host (Name or IP): localhost

☒ Use Standard 'VTSystem' credentials

User ID for VTSystem:

VTSystem Password:

Confirm VTSystem Password:

☒ Use Standard 'User' credentials for 'subscriber' schema

User ID for 'subscriber' Schema:

User Password for 'subscriber' Schema:

Confirm User Password:

Time Zone: Eastern Standard Time

Form filler type: Standard

ASR & TTS: ☐ ASR ☒ TTS

☐ Google Resources

OC Priority: 5

Max OCs:

Transfer Type: ☒ Blind Transfer ☐ Supervised Transfer

Tenant Creation & Copy eONE Data: Log and Status

7.3. Administer System Configuration

Expand and select **Voice Administrator** → **System Config** from the left pane to display the **Base System Defaults** screen.

Enter the following values for the specified fields and retain the default values for the remaining fields.

- **PBX Integration:** “Avaya CM/SM”
- **Dial Plan Digits:** The maximum length of internal extensions, in this case “5”.
- **Outside Line Access Prefix:** The applicable prefix for calls to the PSTN, in this case “9”.
- **Outbound From:** The eONE extension from **Section 3**.

Note that for outbound calls from eONE to the PSTN, eONE will insert the value of the **Outside Line Access Prefix** plus the digit “1” as the called number.

The screenshot displays the 'Base System Configuration' web interface. The left sidebar contains a navigation menu with options: Voice Administrator, System Config, Voice Reports, Prompt Manager, Menu Manager, Audio Manager, Extension Manager, Form Manager, Locator Manager, CollectAndStore Config, Configurations, Grammar Manager, Import Manager, Web Administrator, and Log-Out. The main content area is titled 'Base System Configuration' and has tabs for Defaults, Application, Channel, Dialing, and ASR User Directory. The 'System Defaults' tab is active, showing a form with various configuration fields. The fields are organized into sections: PBX Integration (Avaya CM/SM), Default Application (1000 - Default Application), Default Operator (100 - OPERATOR, DEFAULT), Default Language (English), Default Gender (Female), Dial Plan Digits (5), Max Mode Digits (15), Outside Line Access Prefix (9), Transfer Dress (checked), Transfer Prefix, Transfer Suffix, Toll Call Suffix, Local Call Suffix, Intl. Call Prefix, Intl. Call Suffix, Clear UV Call Data (unchecked), Transfer Fix Phone (checked), Outbound From (53000), and Consultation tfr. Audio. To the right of the main form are three sections: 'Max Tries' (Count: 3, Action: Direct Transfer, Parameter: 100 - Operator, Default), 'Tech Trouble' (Action: Direct Transfer, Parameter: 100 - Operator, Default, Enable SOC unchecked), and 'Resources' (ASR: No ASR, TTS: Default TTS, Advanced TTS button). At the bottom right is a 'Company / Tenant Notes' section. A 'Save Settings' button is located at the bottom center of the form.

Select the **Channel** tab. In the **DNIS/Channel Settings** sub-section, select the default entry. For **Application**, select the applicable pre-configured inbound application, in this case “1011 – SIL_Inbound”.

For **Extension**, enter the eONE extension from **Section 3**.

Retain the default values in the remaining fields.

The screenshot displays the 'Base System Configuration' window with the 'Channel' tab selected. The 'DNIS/Channel Setting' sub-section is active, showing a table with one entry: '0' under 'EXTENSION' and 'Default Application' under 'APPLICATION'. Below the table, the 'Application' dropdown is set to '1011 - SIL_Inbound' and the 'Extension' field contains '53000'. The 'Report Setting' sub-section is also visible, showing a table with one entry: '0' under 'NUMBER' and 'Default Application' under 'APPLICATION'. Below this table, the 'DNIS' and 'Application' fields are empty, and 'Save' and 'Delete' buttons are present.

EXTENSION	APPLICATION	Ch. #
0	Default Application	

Application: 1011 - SIL_Inbound
Extension: 53000

NUMBER	APPLICATION
0	Default Application

DNIS:
Application:
Save Delete

7.4. Administer Collect and Store

Expand and select **Voice Administrator** → **CollectAndStore Config** from the left pane to display the **Collect And Store** screen.

For **Description**, select the pertinent pre-configured entry associated with the inbound application, in this case “1006-SIL_InboundGetANIDNIS”.

In the custom inbound application, parameter **UV4** stores the external transfer-to destination. Update content of **UV4** to the desired external destination as shown below. Retain the default values in the remaining fields.

The screenshot shows the 'Collect And Store' configuration window. On the left is a navigation pane with 'Voice Administrator' expanded and 'CollectAndStore Config' selected. The main area is titled 'Collect and store configuration:'. It contains a 'Description' dropdown set to '1006-SIL_InboundGetANIDNIS', a 'Type' dropdown set to 'ECI Call Header Collection', and a 'Definition' text area containing the text: '%UV1%=SESSION_ANI,%UV2%=SESSION_DNIS,%UV3%='1234',%UV4%='2126630031''. Below the definition area are 'Action' and 'Parameter' dropdowns, both set to 'Direct Audio' and '1022 - SIL_InboundWelcome' respectively. 'Save' and 'Cancel' buttons are at the bottom right.

Repeat the procedures in this section to update the external transfer-to destination associated with the outbound application, as shown below.

The screenshot shows the 'Collect And Store' configuration window for an outbound application. The 'Description' dropdown is set to '1007-SIL_OutboundSetData'. The 'Type' dropdown is set to 'ECI Call Header Collection'. The 'Definition' text area contains the text: '%UV3%='2298',%UV4%='7037030032''. The 'Action' and 'Parameter' dropdowns are set to 'Direct Audio' and '1023 - SIL_OutboundWelcome' respectively. 'Save' and 'Cancel' buttons are at the bottom right.

7.5. Administer Extension Manager

Expand and select **Voice Administrator** → **Extension Manager** from the left pane to display the **Extension Manager** screen.

Follow reference [3] to create an entry for every internal extension that can be used by eONE as transfer destination. In the compliance testing, an entry was created for the Avaya H.323 endpoint at 65001 and an entry created for the Avaya SIP endpoint at 66007, as shown below.

The screenshot shows the 'Extension Manager' web interface. On the left is a navigation pane with 'Voice Administrator' expanded, showing sub-items like 'System Config', 'Voice Reports', 'Prompt Manager', 'Menu Manager', 'Audio Manager', 'Extension Manager' (selected), 'Form Manager', 'Locator Manager', 'CollectAndStore Config', 'Configurations', 'Grammar Manager', and 'Import Manager'. Below this are 'Web Administrator' and 'Log-Out'. The main content area has a title bar 'Extension Manager' and a dropdown menu 'Select Extension: 65001 - Avaya, H323' with an 'Add' button. Below this are two tabs: 'Extension' (active) and 'Mailbox'. The 'Extension' tab contains a form with fields for 'First Name' (H323), 'Last Name' (Avaya), 'Email Address', 'Email Server(Name or IP)', 'Email Server Type' (POP3/SMTP), 'Email Login(User Name)', and 'Email Password'. There are three checkboxes: 'Allow Call Transfer' (checked), 'Transcriber', and 'Administrator'. Below these are two sections: 'Re-Route Transfers to Another Extension' and 'Execute An Application', each with a dropdown menu. At the bottom are 'Save', 'Renumber', and 'Bulk Add' buttons.

The screenshot shows the 'Extension Manager' web interface for extension 66007. The navigation pane is identical to the previous screenshot. The main content area has a title bar 'Extension Manager' and a dropdown menu 'Select Extension: 66007 - Avaya, SIP' with an 'Add' button. Below this are two tabs: 'Extension' (active) and 'Mailbox'. The 'Extension' tab contains a form with fields for 'First Name' (SIP), 'Last Name' (Avaya), 'Email Address', 'Email Server(Name or IP)', 'Email Server Type' (POP3/SMTP), 'Email Login(User Name)', and 'Email Password'. There are three checkboxes: 'Allow Call Transfer' (checked), 'Transcriber', and 'Administrator'. Below these are two sections: 'Re-Route Transfers to Another Extension' and 'Execute An Application', each with a dropdown menu. At the bottom are 'Save', 'Renumber', and 'Bulk Add' buttons.

7.6. Administer Menu Manager

Select **Voice Administrator** → **Menu Manager** from the left pane to display the **Menu Manager** screen.

For **Menu**, select the pertinent pre-configured menu entry associated with the inbound application, in this case “1003 - SIL_MENU”.

Under **Spanish prompt and settings**, press the keypad associated with the menu option for transfer to internal destination, in this case “3”.

For **Button Parameter**, select the desired internal destination as shown below.

Repeat the procedures in this section to administer the transfer internal destination for the outbound application where applicable. In the compliance testing, the same menu entry was used for both the inbound and outbound applications.

The screenshot displays the 'Menu Manager' web interface. On the left is a navigation pane with options: Voice Administrator, System Config, Voice Reports, Prompt Manager, Menu Manager (selected), Audio Manager, Extension Manager, Form Manager, Locator Manager, CollectAndStore Config, Configurations, Grammar Manager, Import Manager, Web Administrator, and Log-Out. The main content area is titled 'Menu Manager' and shows configuration for 'Menu: 1003 - SIL_MENU'. It includes fields for 'TTS: Default TTS', 'Type: Standard DTMF Menu', 'Max Tries Options: Count: 3', 'Action: Disconnect', and 'Parameter: [[DISCONNECT]]'. Below this is the 'English prompt and settings' section with a text area containing prompts for short and long announcements and transfer options. The 'Spanish prompt and settings' section is active, showing a checked 'Use Auto-Transfer Keys?' option, a numeric keypad with '3' highlighted, and a 'Menu Button 3' configuration box. This box has 'Button Action: Direct Transfer' and 'Button Parameter: 66007 - Avaya SIP'. There is also a 'Change Language / Gender' section with 'English' and 'Female' selected. A 'Save' button is at the bottom right.

7.7. Administer VXML File

Log into the Linux shell of the eONE Media server containing the CIMedia ARC VXML Services component.

Navigate to the **/home/arc/.ISP/Telecom/Exec/vxi** directory and use the copy command to create a new VXML configuration file as shown below, where “arcVXML2.vxml.cfg” is the pre-existing default configuration file for ARC VXML 2.0 application and “53000” is the eONE extension from **Section 3**. Note that the eONE extension must be used as part of the name of the new configuration file.

```
[xxx@CI-TESTMS ~]# cd /home/arc/.ISP/Telecom/Exec/vxi
[xxx@CI-TESTMS vxi]#
[xxx@CI-TESTMS vxi]# cp arcVXML2.vxml.cfg arcVXML2.53000.vxml.cfg
```

Open the newly created file, in this case “arcVXML2.53000.vxml.cfg”. Scroll down to the bottom of the file.

For **APP_NAME**, enter any descriptive name. For **SCRIPT**, enter the URL shown below where “10.64.101.206” is the IP address of the eONE server.

Retain the default values in the remaining fields.

```
#APP_NAME=arcVXML2
CACHE_DIR=/tmp/VXML2
KEEP_CACHE_DIR=1
SPEECH_REC=0
RESERVE_SPEECH_RESOURCE=0
VALIDATE_SCRIPTS=0
DEFAULT_COMPRESSION=COMP_WAV
#TRANSFER_MODE=BLIND
TRANSFER_MODE=LISTEN_ALL
#TRANSFER_FORMAT=IP
TRANSFER_FORMAT=NONE
#TTS_SERVER=LOQUENDO,MSS
TTS_SERVER=MSS
TTS_LANGUAGE=ENGLISH_AMERICAN
SR_LANGUAGE=ENGLISH_AMERICAN
#HTTP_VERSION=1.0
MRCP_ASR=MSS
NETWORK_ANNOUNCEMENT=0
#SKIP_TIME_IN_SECONDS=2
SCRIPT_MAXAGE=0
SCRIPT_MAXSTALE=0
APP_NAME=SIL_Inbound
SCRIPT=http://10.64.101.206/eCI/VXML/eONEMS_Inbound.vxml
```

8. Verification Steps

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

8.1. Verify Avaya Aura® Communication Manager

On Communication Manager, verify status of the SIP trunk group by using the “status trunk n” command, where “n” is the trunk group number administered in **Section 5.6**. Verify that all ports are in the “in-service/idle” state as shown below.

```
status trunk 53
```

TRUNK GROUP STATUS			
Member	Port	Service State	Mtce Connected Ports Busy
0053/001	T00087	in-service/idle	no
0053/002	T00113	in-service/idle	no
0053/003	T00114	in-service/idle	no
0053/004	T00115	in-service/idle	no

Verify status of the SIP signaling group by using the “status signaling-group n” command, where “n” is the signaling group number administered in **Section 5.7**. Verify that the **Group State** is “in-service” as shown below.

```
status signaling-group 53
```

STATUS SIGNALING GROUP	
Group ID:	53
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 on the eONE entity name from Section 6.3.1.

Session Manager	Type	Monitored Entities					
		Down	Partially Up	Up	Not Monitored	Deny	Total
<input type="checkbox"/> DR-SM	Core	4	0	9	0	0	13

Select : All, None

All Monitored SIP Entities

Run Monitor

13 Items Filter: Enable

SIP Entity Name
<input type="checkbox"/> eONE

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: eONE

Summary View

1 Item Filter: Enable

Session Manager Name	Session Manager IP Address Family	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
<input type="radio"/> DR-SM	IPv4	10.64.101.207	5060	UDP	FALSE	UP	200 OK	UP

Select : None

8.3. Verify Computer Instruments eONE

This section provides the tests that can be performed to verify the eONE inbound and outbound applications.

8.3.1. Inbound Application

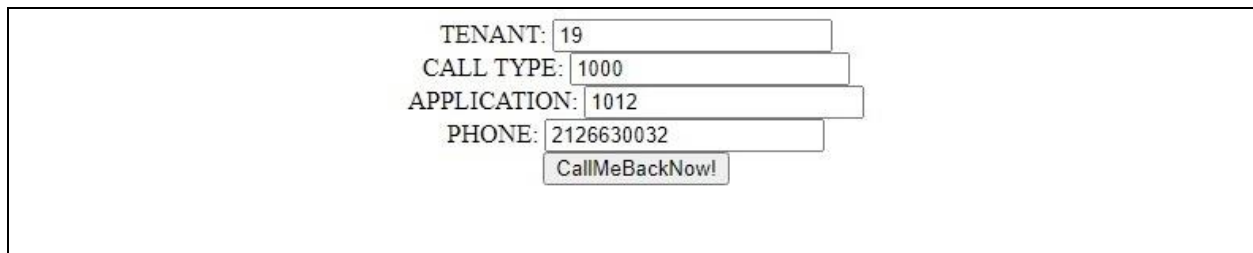
Establish an incoming trunk call from PSTN with eONE. Verify that the calling party hears the appropriate greeting associated with the inbound application.

8.3.2. Outbound Application

In a browser window, enter the URL associated with the eONE outbound application, in this case **<http://10.64.101.206/makeacall.html>** where “10.64.101.206” is the eONE server with the web-based interface.

The screen below is displayed. For **PHONE**, enter the phone number associated with an external destination on the PSTN. Retain the default values in the remaining fields and click **CallMeBackNow!**

Verify that an outbound call is initiated from eONE to the external destination. Answer the call at the external destination and verify that the called party hears the appropriate greeting associated with the outbound application.



The screenshot displays a web form with the following fields and values:

TENANT:	19
CALL TYPE:	1000
APPLICATION:	1012
PHONE:	2126630032

Below the fields is a button labeled **CallMeBackNow!**

9. Conclusion

These Application Notes describe the configuration steps required for Computer Instruments 7.0 to successfully interoperate with Avaya Aura® Session Manager 8.1 and Avaya Aura® Communication Manager 8.1.

10. Additional References

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

1. *Administering Avaya Aura® Communication Manager*, Release 8.1.x, Issue 6, March 2020, available at <http://support.avaya.com>.
2. *Administering Avaya Aura® Session Manager*, Release 8.1.x, Issue 6, August 2020, available at <http://support.avaya.com>.
3. *eONE User's Manual*, Version 7.0, 2020, available at <http://instruments.com>.

©2020 Avaya Inc. All Rights Reserved.

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

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