



## Avaya Solution & Interoperability Test Lab

---

# Application Notes for Enghouse Interactive Communications Portal 10.4 using Dialogic Host Media Processing 3.0 with Avaya Aura® Session Manager 8.1.3.3 and Avaya Aura® Communication Manager 8.1.3.3 with TLS/SRTP- Issue 1.0

### Abstract

These Application Notes describe the configuration steps for Enghouse Interactive Communications Portal 10.4 using Dialogic Host Media Processing 3.0 to successfully interoperate with Avaya Aura® Session Manager 8.1.3.3 and Avaya Aura® Communication Manager 8.1.3.3. Communications Portal is an IVR application that connects to Session Manager via a SIP Trunk.

Readers should pay attention to **Section 2**, in particular the scope of testing as outlined in **Section 2.1**, as well as 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 for Enghouse Interactive Communications Portal 10.4 using Dialogic Host Media Processing (DHP) 3.0 to successfully interoperate with Avaya Aura® Session Manager 8.1.3.3 and Avaya Aura® Communication Manager 8.1.3.3 using Transport Layer Security (TLS) and Secure Real-time Transport Protocol (SRTP) via a SIP Trunk. Enghouse Interactive Communications Portal is an open, standards-based platform with integrated application development and management components. Enghouse Interactive Communications Portal provide voice self service solutions, such as interactive voice response, outbound dialing, voice recording and speech enabled self service systems.

## 2. General Test Approach and Test Results

Interoperability testing contained functional tests mentioned in **Section 2.1**. All test cases were performed manually. The general test approach was to validate successful handling of inbound/outbound calls to and from the Communications Portal (CP) to verify IVR application telephony functionality. The IVR application telephony functionality of CP was the only module tested. This IVR application (CP script) connects to Session Manager via a SIP Trunk. Session Manager directs inbound calls over SIP trunk to CP script which in turn handles the call based on the digits dialed using SIP signaling. CP uses Dialogic HMP to perform all telephony functions on the server.

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 this Application Note, the interface between Avaya systems and Enghouse Interactive Communications Portal solution utilized enabled securities capabilities with TLS/SRTP.

## 2.1. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability testing. Feature testing included the validation of the following:

- **Basic Inbound/Outbound** – Tests inbound/outbound calls to and from CP.
- G.711A, G.711U codecs support and negotiation (without shuffling).
- **Call Forward** from Avaya Endpoints to CP.
- **Call Hold** – Tests held calls to/from CP.
- **Call Transfer** – Tests transferred calls to/from CP.
- **IVR Functionality** – Tests of various IVR features such as ANI/DNIS detection, voice recording, DTMF collection on the CP.
- **Failover/Service** – Tests the behaviour of CP when there are certain failed conditions such as Media shuffling, session refresh, options, long hold, multiple calls, isolated network from CP server, power off/on CP server

## 2.2. Test Results

The testing was successful. All test cases passed.

## 2.3. Support

Technical support on Communications Portal can be obtained for Enghouse Interactive as follows:  
USA

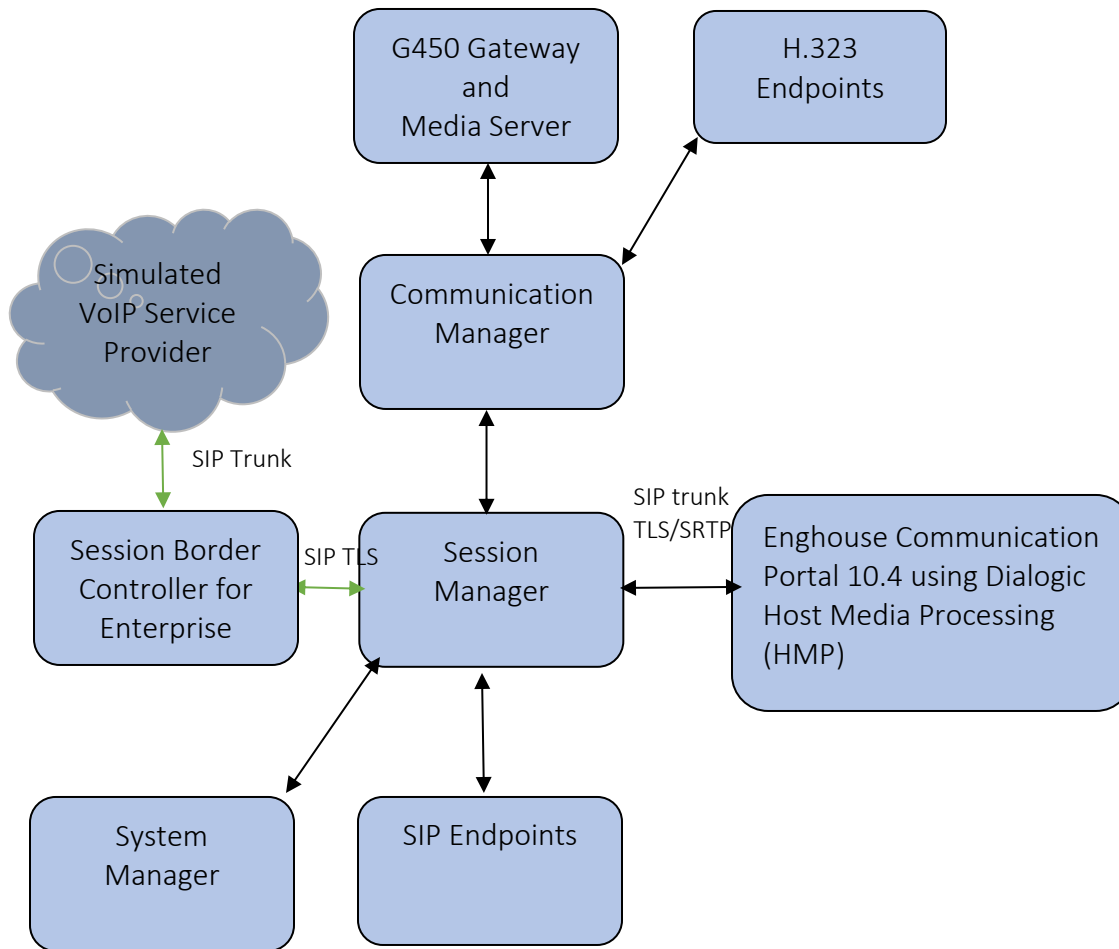
- Email: [scpsupport@enghouse.com](mailto:scpsupport@enghouse.com)
- Website: <http://enghouseinteractive.com/support.php>
- Phone: +1 800.788.9730 Self-Service
- Phone: +1 800.872.2272 Live-Service

EMEA

- Email: [envoxsupport@enghouse.com](mailto:envoxsupport@enghouse.com) / [supportenvox@syntellect.com](mailto:supportenvox@syntellect.com)
- Website: <http://www.enghouseinteractive.com/services/support/>
- Phone: +44 870.220.2205

### 3. Reference Configuration

**Figure 1** illustrates a sample configuration that consists of Avaya products and CP with Dialogic HMP.



**Figure 1:** Test Configuration for Enghouse Interactive Communications Portal using Dialogic Host Media Processing (HMP) and the Avaya Platform.

## 4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya Aura® System Manager in Virtual Environment	8.1.3.3
Avaya Aura® Session Manager in Virtual Environment	8.1.3.3
Avaya Aura® Communication Manager in Virtual Environment	8.1.3.3
Avaya G450 Media Gateway	41.16.30
Avaya Aura® Media Server in Virtual Environment	8.0.2.43
Avaya Session Border Controller for Enterprise in Virtual Environment	8.1.3.0
Avaya J159 H323 Deskphone	6.8
Avaya Workplace Client for Windows	3.22.0
Avaya J179 & J189 SIP Deskphone	4.0.9
Avaya Vantage™ K175 & K155	3.1.0.0
Enghouse Communications Portal - Dialogic Host Media Processing	10.4.19.9632 3.0 Service Update 525

## 5. Configure Avaya Aura® Communication Manager

The configuration and verification operations illustrated in this section were all performed using Communication Manager System Administration Terminal (SAT). The information provided in this section describes the configuration of Communication Manager for this solution. For all other provisioning information such as initial installation and configuration, please refer to the product documentation in **Section 10**.

It is assumed that the general installation and configuration of Avaya Aura® environment and simulated PSTN SIP Trunk have been previously completed and is not discussed here.

The configuration operations described in this section can be summarized as follows:

- Verify System Parameters Customer Options
- System Features and Access Codes
- Configure Network Region and IP Codec
- Configure SIP Signaling Group and Trunk Group
- Administer Dial Plan
- Administer Route Selection for Communications Portal calls

### 5.1. Verify System Parameters Customer Options

The license file installed on the system controls these attributes. If a required feature is not enabled or there is insufficient capacity, contact an authorized Avaya sales representative. Use the **display system-parameters customer-options** command to determine these values. On **Page 2**, verify that **Maximum Administered SIP Trunks** has sufficient capacity. Each call that receives IVR treatment from uses a minimum of one SIP trunk. Calls that are routed back to stations commissioned on Communication Manager or calls that are routed back to Communication Manager to access the PSTN, use two SIP trunks.

display system-parameters customer-options			Page	2 of	12
OPTIONAL FEATURES					
IP PORT CAPACITIES			USED		
Maximum Administered H.323 Trunks:			4000		0
Maximum Concurrently Registered IP Stations:			1000		2
Maximum Administered Remote Office Trunks:			4000		0
Max Concurrently Registered Remote Office Stations:			1000		0
Maximum Concurrently Registered IP eCons:			68		0
Max Concur Reg Unauthenticated H.323 Stations:			100		0
Maximum Video Capable Stations:			2400		0
Maximum Video Capable IP Softphones:			1000		41
<b>Maximum Administered SIP Trunks:</b>			<b>4000</b>		<b>305</b>
Max Administered Ad-hoc Video Conferencing Ports:			4000		0
Max Number of DS1 Boards with Echo Cancellation:			80		0
(NOTE: You must logoff & login to effect the permission changes.)					

On **Page 4**, ensure that both **ARS** and **ARS/AAR Partitioning** are set to **y**.

```
display system-parameters customer-options                                Page   4 of  12
                                OPTIONAL FEATURES

Abbreviated Dialing Enhanced List? y      Audible Message Waiting? y
Access Security Gateway (ASG)? y          Authorization Codes? y
Analog Trunk Incoming Call ID? y          CAS Branch? n
A/D Grp/Sys List Dialing Start at 01? y   CAS Main? n
Answer Supervision by Call Classifier? y   Change COR by FAC? n
                                ARS? y      Computer Telephony Adjunct Links? y
                                ARS/AAR Partitioning? y  Cvg Of Calls Redirected Off-net? y
ARS/AAR Dialing without FAC? y            DCS (Basic)? y
ASAI Link Core Capabilities? y            DCS Call Coverage? y
ASAI Link Plus Capabilities? y            DCS with Rerouting? y
Async. Transfer Mode (ATM) PNC? n         Digital Loss Plan Modification? y
Async. Transfer Mode (ATM) Trunking? n    DS1 MSP? y
ATM WAN Spare Processor? n                DS1 Echo Cancellation? y
ATMS? y
Attendant Vectoring? y

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

On **Page 6**, ensure that **Uniform Dialing Plan** is set to **y**.

```
display system-parameters customer-options                                Page   6 of  12
                                OPTIONAL FEATURES

Multinational Locations? n                Station and Trunk MSP? y
Multiple Level Precedence & Preemption? y  Station as Virtual Extension? y
Multiple Locations? n
No-License Mode Disabled? y              System Management Data Transfer? n
Personal Station Access (PSA)? y          Tenant Partitioning? y
PNC Duplication? n                       Terminal Trans. Init. (TTI)? y
Port Network Support? y                  Time of Day Routing? y
Posted Messages? y                       TN2501 VAL Maximum Capacity? y
                                Uniform Dialing Plan? y
Private Networking? y                    Usage Allocation Enhancements? y
Processor and System MSP? y
Processor Ethernet? y                    Wideband Switching? y
                                           Wireless? n
Remote Office? y
Restrict Call Forward Off Net? y
Secondary Data Module? y

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



## 5.2. System Features and Access Codes

For the testing, **Trunk-to Trunk Transfer** was set to **all** on **Page 1** of the **system-parameters features** page. This is a system wide setting that allows calls to be routed from one trunk to another and is usually turned off to help prevent toll fraud. An alternative to enabling this feature on a system wide basis is to control it using COR (Class of Restriction). See **Section 10** for supporting documentation.

```
display 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
```

Use the **display feature-access-codes** command to verify that a FAC (feature access code) has been defined for both AAR and ARS. Note that **\*50** is used for AAR and **9** for ARS routing.

```
display feature-access-codes                                     Page 1 of 12
      FEATURE ACCESS CODE (FAC)
      Abbreviated Dialing List1 Access Code:
      Abbreviated Dialing List2 Access Code:
      Abbreviated Dialing List3 Access Code:
      Abbreviated Dial - Prgm Group List Access Code:
      Announcement Access Code:
      Answer Back Access Code:
      Attendant Access Code:
      Auto Alternate Routing (AAR) Access Code: *50
      Auto Route Selection (ARS) - Access Code 1: 9      Access Code 2: *51
      Automatic Callback Activation: *52      Deactivation: *53
```

### 5.3. Configure Network Region and IP Codec

In the **IP Network Region** form, the **Authoritative Domain** field is configured to match the domain name configured on Session Manager in **Section 6.2**. In this configuration, the domain name is **devconnect.com**. The **IP Network Region** form also specifies the **Codec Set** to be used. This codec set will be used for calls routed over the SIP trunk to Session manager as **ip-network region 1** is specified in the SIP signaling group.

change ip-network-region 1		Page 1 of 20
IP NETWORK REGION		
Region: 1	NR Group: 1	
Location: 1	<b>Authoritative Domain: devconnect.com</b>	
Name: SaiGon	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? y	
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		

In the **IP Codec Set** form, select the audio codecs supported for calls routed over the SIP trunk to CP. The form is accessed via the **change ip-codec-set n** command. Note that IP codec set 1 was specified in IP Network Region 1 shown above. Multiple codecs may be specified in the **ip-codec-set** form in order of preference; the **ip-codec-set 1** example below includes **G.711A** (a-law) and **G.711MU** which are supported by Communications Portal. The **Media Encryption** have **none** as an option, **Media Encryption** from Communication Manager by using a codec-set that doesn't have **none** as an option for calls between network regions with encryption forced. By adding **none**, if an unsecure call comes in, the call can still be processed with non-secure RTP calls will also be sent.

change ip-codec-set 1 Page 1 of 2

IP MEDIA PARAMETERS

Codec Set: 1

Audio Codec	Silence Suppression	Frames Per Pkt	Packet Size (ms)
1: G.711MU	n	2	20
2: G.722-64K		2	20
3: G.729	n	2	20
4: OPUS-WB20K		1	20
5: G.711A	n	2	20
6:			
7:			

Media Encryption

Encrypted SRTP: best-effort

1: 10-srtp-aescm256-hmac80  
2: 1-srtp-aescm128-hmac80  
3: **none**  
3:  
4:  
5:

In the **node-names ip** form, note the IP address of the **procr** and the Session Manager (**smsip92**). The host names will be used throughout the other configuration screens of Communication Manager and Session Manager. Type **display node-names ip** to show all the necessary node names.

change node-names ip Page 1 of 2

IP NODE NAMES

Name	IP Address
aes95	10.30.5.95
ams94	10.30.5.94
default	0.0.0.0
<b>procr</b>	<b>10.30.5.93</b>
procr6	::
<b>smsip92</b>	<b>10.30.5.92</b>

( 7 of 7 administered node-names were displayed )

Use 'list node-names' command to see all the administered node-names

Use 'change node-names ip xxx' to change a node-name 'xxx' or add a node-name

## 5.4. Configure SIP Signaling Group and Trunk Group

Prior to configuring a SIP trunk group for communication with Session Manager, a SIP signaling group must be configured. Use the **add signaling-group** command to create a signaling group between Communication Manager and Session Manager. This signaling group and trunk group is used for internal calls between Avaya Endpoints and used for calls to and from CP. For the compliance test, signaling group 1 was used and was configured using the parameters highlighted below, shown on the screen on the next page:

- Set the **Group Type** field to **sip**.
- Set the **Transport Method** to the desired transport method, for compliance testing this was set to **tls**.
- The **Peer Detection Enabled** field should be set to **n** and **Peer Server** set to **SM**.
- Specify the node names for the procr and the Session Manager node name as the two ends of the signaling group in the **Near-end Node Name** field and the **Far-end Node Name** field, respectively. These values are taken from the **IP Node Names** form shown above.
- Set the **Near-end Node Name** to **procr**. This value is taken from the **IP Node Names** form shown above.
- Set the **Far-end Node Name** to the node name defined for the Session Manager (node name **smsip92**), as per **Section 5.5**.
- Ensure that the recommended TLS port value of **5061** is configured in the **Near-end Listen Port** and the **Far-end Listen Port** fields.
- In the **Far-end Network Region** field, enter the IP Network Region configured above. This field logically establishes the **far-end** for calls using this signaling group as network region 1.
- **Far-end Domain** was set to the domain used during compliance testing.
- The **DTMF over IP** field should remain set to the default value of **rtp-payload**. This value enables Communication Manager to send DTMF transmissions using RFC 2833.
- The **Direct IP-IP Audio Connections** field is set to **y**.
- The default values for the other fields may be used.

```
change signaling-group 1                                     Page 1 of 3
                                SIGNALING GROUP

Group Number: 1                      Group Type: sip
IMS Enabled? n                      Transport Method: tls
  Q-SIP? n
  IP Video? y                      Priority Video? y          Enforce SIPS URI for SRTP? y
Peer Detection Enabled? n Peer Server: SM                      Clustered? n
Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? y
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? y
Alert Incoming SIP Crisis Calls? n
  Near-end Node Name: procr                      Far-end Node Name: smsip92
  Near-end Listen Port: 5061                      Far-end Listen Port: 5061
                                                Far-end Network Region: 1

Far-end Domain: devconnect.com

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

Configure the **Trunk Group** form as shown below. Enter a descriptive name in the **Group Name** field. Set the **Group Type** field to **sip**. Enter a **TAC** code compatible with the Communication Manager dial plan. Set the **Service Type** field to **tie**. Specify the signaling group associated with this trunk group in the **Signaling Group** field, and specify the **Number of Members** supported by this SIP trunk group. Accept the default values for the remaining fields.

change trunk-group 1		Page 1 of 4	
TRUNK GROUP			
Group Number: 1	Group Type: <b>sip</b>	CDR Reports: y	
Group Name: <b>InternalCalls</b>	COR: 1	TN: 1	TAC: <b>#01</b>
Direction: two-way	Outgoing Display? n	Night Service:	
Dial Access? n			
Queue Length: 0			
Service Type: <b>tie</b>	Auth Code? n	Member Assignment Method: auto	
		Signaling Group: <b>1</b>	
		Number of Members: 50	

On **Page 2** of the trunk-group form the **Preferred Minimum Session Refresh Interval (sec)** field should be set to a value mutually agreed with Enghouse Interactive to prevent unnecessary SIP messages during call setup. Session refresh is used throughout the duration of the call, to check the other side has not gone away, for the compliance test a value of **900** was used.

change trunk-group 1		Page 2 of 4	
Group Type: sip			
TRUNK PARAMETERS			
Unicode Name: auto			
Redirect On OPTIM Failure: 5000			
SCCAN? n	Digital Loss Group: 18		
Preferred Minimum Session Refresh Interval(sec): <b>900</b>			
Disconnect Supervision - In? y Out? y			
XOIP Treatment: auto Delay Call Setup When Accessed Via IGAR? n			
Caller ID for Service Link Call to H.323 1xC: station-extension			

Settings on **Page 3** can be left as default. However, the **Numbering Format** in the example below is set to **private**.

```
change trunk-group 1                                     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? y
                                                    Replace Unavailable Numbers? y

    Modify Tandem Calling Number: no

    Show ANSWERED BY on Display? y

    DSN Term? n
```

Settings on **Page 4** are as follow.

```
change trunk-group 1                                     Page 4 of 4
                                                    PROTOCOL VARIATIONS

    Mark Users as Phone? n
Prepend '+' to Calling/Alerting/Diverting/Connected Number? n
    Send Transferring Party Information? n
    Network Call Redirection? y
    Build Refer-To URI of REFER From Contact For NCR? y
    Send Diversion Header? y
    Support Request History? n
    Telephone Event Payload Type:

    Convert 180 to 183 for Early Media? n
    Always Use re-INVITE for Display Updates? n
    Resend Display UPDATE Once on Receipt of 481 Response? y
    Identity for Calling Party Display: P-Asserted-Identity
    Block Sending Calling Party Location in INVITE? n
    Accept Redirect to Blank User Destination? n
    Enable Q-SIP? n
    Interworking of ISDN Clearing with In-Band Tones: keep-channel-active
    Request URI Contents: may-have-extra-digits
```

**Note:** With the field **Resend Display UPDATE once on Receipt of 481 Response** is set to **y**, Communication Manager will send a SIP UPDATE message for 481 response received from far end to avoid display incorrectly in some race condition cases.

## 5.5. Administer Dial Plan

It was decided for the compliance testing that all calls beginning with 3 and a total length of 5 digits were to be sent across the SIP trunk to Session Manager and therefore to CP. In order to achieve this, automatic alternate routing (aar) would be used to route the calls. The dial plan and aar routing analysis need to be changed to allow this.

Type **change dialplan analysis**, in order to make changes to the dial plan. Ensure that **3** is added with a **Total Length** of **5** and a **Call Type** of uniform dialing plan (**udp**) table.

change dialplan analysis						Page 1 of 12			
DIAL PLAN ANALYSIS TABLE									
Location: all						Percent Full: 2			
	Dialed	Total	Call	Dialed	Total	Call	Dialed	Total	Call
	String	Length	Type	String	Length	Type	String	Length	Type
0		10	udp						
3		5	udp						
4		10	udp						
7		5	ext						
8		5	ext						
9		1	fac						
*		3	fac						
#		3	dac						

## 5.6. Administer Route Selection for Communications Portal Calls

As digits 3xxxx were defined in the dial plan as udp (**Section 5.5**) use the **change uniform-dialplan** command to configure the routing of the dialed digits. In the example below, calls to numbers beginning with 3 that are 5 digits in length will be matched. No further digits are deleted or inserted. Calls are sent to **aar** for further processing.

change uniform-dialplan 3						Page 1 of 2	
UNIFORM DIAL PLAN TABLE							
						Percent Full: 0	
Matching				Insert		Node	
Pattern	Len	Del		Digits	Net Conv	Num	
3	5	0			aar	n	
4	10	0			ars	n	
						n	

Use the **change aar analysis x** command to further configure the routing of the dialed digits. Calls to Communications Portal begin with **3** and are matched with the AAR entry shown below. Calls are sent to **Route Pattern 1**, which contains the SIP Trunk Group with Session Manager.

change aar analysis 0							Page	1 of	2
AAR DIGIT ANALYSIS TABLE									
Location: all							Percent Full: 2		
	Dialed String	Total Min	Total Max	Route Pattern	Call Type	Node Num	ANI	Reqd	
0		10	10	4	lev0		n		
<b>3</b>		<b>5</b>	<b>5</b>	<b>1</b>	lev0		n		
6		5	5	1	lev0		n		
7		5	5	1	lev0		n		
8		5	5	1	lev0		n		
899		5	5	1	lev0		n		

Use the **change route-pattern n** command to add the SIP trunk group to the route pattern that AAR selects. In this configuration, **Route Pattern Number 1** is used to route calls to trunk group (**Grp No**) **1**, this is the SIP Trunk with Session Manager

change route-pattern 1												Page	1 of	4	
Pattern Number: 1												Pattern Name: DevC-Int			
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



## 6. Configure Avaya Aura® Session Manager

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

- Configure SIP Entities
- Configure Routing Policies
- Configure Dial Patterns

### 6.1. Configure SIP Entities

This section provides the procedures for configuring SIP Trunk from Session Manager to Communication Manager and CP

#### 6.1.1. Configure SIP Entity for Communications Portal

Configuration of SIP Entities is performed via System Manager. Access the System Manager Administration web interface by entering the System Manager (SMGR) URL in a web browser. Log in using 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.

---

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

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

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

All users must comply with all corporate instructions regarding the protection of information assets.

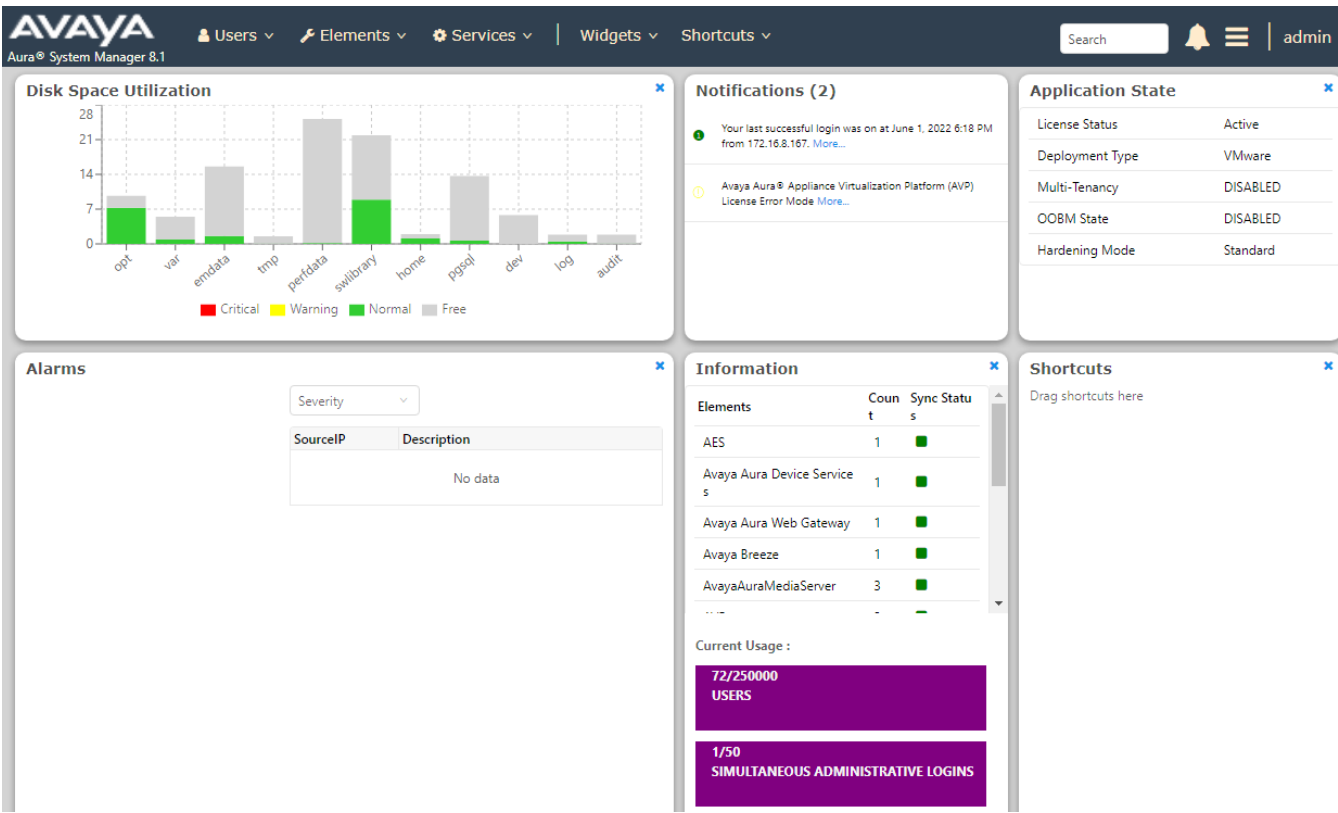
User ID:

Password:

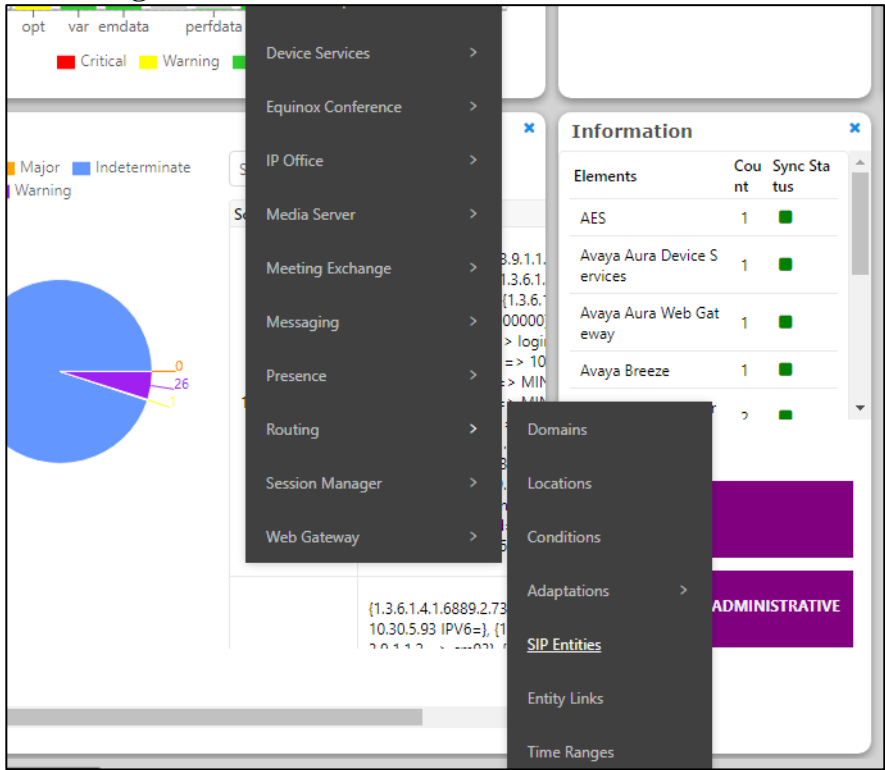
[Change Password](#)

**Supported Browsers:** Internet Explorer 11.x or Firefox (minimum version 65.0).

Once logged in, the following screen is displayed.



Select **Elements** → **Routing** → **SIP Entities**.



On **SIP Entities** page, press **New** to create new **SIP Entity**.

The screenshot displays the Avaya Aura System Manager 8.1 interface. The top navigation bar includes the Avaya logo, 'Aura® System Manager 8.1', and several menu items: Users, Elements, Services, Widgets, and Shortcuts. A search bar is located on the right. The left sidebar shows a navigation menu with 'Routing' expanded, and 'SIP Entities' selected. The main content area is titled 'SIP Entities' and features a table with 17 items. The table has columns for Name, FQDN or IP Address, Type, and Notes. A 'New' button is highlighted in the top action bar.

<input type="checkbox"/>	Name	FQDN or IP Address	Type	Notes
<input type="checkbox"/>	<a href="#">BTCluster</a>	btcluster.avaya.com	Endpoint Concentrator	
<input type="checkbox"/>	<a href="#">DevConnect-AACC148</a>	10.30.5.148	SIP Trunk	
<input type="checkbox"/>	<a href="#">DevConnect-AAWG138</a>	10.30.5.138	SIP Trunk	
<input type="checkbox"/>	<a href="#">DevConnect-BSM134</a>	10.30.5.134	Session Manager	
<input type="checkbox"/>	<a href="#">DevConnect-CM93</a>	10.30.5.93	CM	
<input type="checkbox"/>	<a href="#">DevConnect-CM93PSTN</a>	10.30.5.93	SIP Trunk	
<input type="checkbox"/>	<a href="#">DevConnect-CM96</a>	cm96.hcm.com	CM	
<input type="checkbox"/>	<a href="#">DevConnect-IP Office</a>	10.128.226.178	SIP Trunk	
<input type="checkbox"/>	<a href="#">DevConnect-MPP144</a>	10.30.5.144	Voice Portal	
<input type="checkbox"/>	<a href="#">DevConnect-Officelinx145</a>	10.30.5.145	Other	
<input type="checkbox"/>	<a href="#">DevConnect-Presence</a>	10.30.5.135	Avaya Breeze	
<input type="checkbox"/>	<a href="#">DevConnect-PresenceService</a>	10.30.5.135	Presence Services	
<input type="checkbox"/>	<a href="#">DevConnect-SBC140</a>	10.30.5.140	SIP Trunk	

Enter a suitable **Name** and ensure that the correct **Location** and **Time Zone** are entered correctly, click on **Commit** to save the new entity.

- **Name:** A descriptive name, example **Enghouse CP**.
- **FQDN or IP Address:** The proc IP address of CP.
- **Type:** **SIP Trunk**
- **Notes:** Any desired notes.
- **Location:** Select the applicable location.
- **Time Zone:** Select the applicable time zone.

**Note:** The setup of a Location is specific to each site, this can be added by clicking on **Locations** on the left panel on the screen shot below, the setup of the location for this site has not been documented as part of this setup as it would be already setup as part of the site installation.

The screenshot displays the Avaya Aura System Manager 8.1 web interface. The top navigation bar includes the Avaya logo, a search bar, and dropdown menus for Users, Elements, Services, Widgets, and Shortcuts. The left sidebar shows a navigation tree with options like Domains, Locations, Conditions, Adaptations, SIP Entities (highlighted), Entity Links, Time Ranges, Routing Policies, Dial Patterns, and Regular Expressions. The main content area is titled 'SIP Entity Details' and contains a 'General' tab. The form fields are as follows:

Field	Value
Name	Enghouse CP
FQDN or IP Address	10.103.3.220
Type	SIP Trunk
Notes	
Adaptation	
Location	SaiGon
Time Zone	Asia/Ho_Chi_Minh
SIP Timer B/F (in seconds)	4
Minimum TLS Version	Use Global Setting
Credential name	
Securable	<input type="checkbox"/>
Call Detail Recording	egress

Buttons for 'Commit' and 'Cancel' are located at the top right of the form.

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 **DevConnect-SMSIP**.
- **Protocol:** **TLS**
- **Port:** **5061**
- **SIP Entity 2:** The Communications Portal entity name from this section, in this case “Enghouse CP”.
- **Port:** **5061**
- **Connection Policy:** **trusted**

#### Entity Links

Override Port & Transport with DNS SRV: ☐

<input type="checkbox"/>	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Deny New Service
<input type="checkbox"/>	* DevConnect-SMSIP_Engh	DevConnect-SMSIP	TLS	* 5061	Enghouse CP	* 5061	trusted	<input type="checkbox"/>

Select : All, None

### 6.1.2. Configure SIP Entity for Communication Manager

Add new 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.

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, example **DevConnect-CM93**.
- **FQDN or IP Address:** The proc IP address of Communication Manager.
- **Type:** **CM**
- **Notes:** Any desired notes.
- **Location:** Select the applicable location.
- **Time Zone:** Select the applicable time zone.

### SIP Entity Details

CommitCancel

#### General

\* Name: DevConnect-CM93

\* FQDN or IP Address: 10.30.5.93

Type: CM

Notes:

Adaptation:

Location: SaiGon

Time Zone: Asia/Ho\_Chi\_Minh

\* SIP Timer B/F (in seconds): 4

Minimum TLS Version: Use Global Setting

Credential name:

Securable: ☐

Call Detail Recording: none

#### Loop Detection

Loop Detection Mode: On

Loop Count Threshold: 5

Loop Detection Interval (in msec): 200

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 **DevConnect-SMSIP**.
- **Protocol:** **TLS**
- **Port:** **5061**
- **SIP Entity 2:** The Communication Manager entity name from this section, in this case **DevConnect-CM93**
- **Port:** **5061**
- **Connection Policy:** **trusted**

**Entity Links**

Override Port & Transport with DNS SRV: ☐

Add Remove

1 Item Filter: Enable

<input type="checkbox"/>	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Deny New Service
<input type="checkbox"/>	* DevConnect-SMSIP_DevC	DevConnect-SMSIP	TLS	* 5061	DevConnect-CM93	* 5061	trusted	<input type="checkbox"/>

Select : All, None

## 6.2. Configure Routing Policy for Communications Portal

This section to add a new routing policy for routing calls to Communications Portal. Select **Routing** → **Routing Policies** from the left pane and click **New** in the subsequent screen (not shown) to add a new routing policy to Communication Manager.

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 Communications Portal entity name from **Section 6.1.1**.

**Routing Policy Details** Commit Cancel

**General**

\* Name: To\_CP

Disabled: ☐

\* Retries: 0

Notes:

**SIP Entity as Destination**

Select

Name	FQDN or IP Address	Type	Notes
Enghouse CP	10.103.3.220	SIP Trunk	

**Time of Day**

Add Remove View Gaps/Overlaps

1 Item

<input type="checkbox"/>	Ranking	Name	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
<input type="checkbox"/>	0	24/7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	00:00	23:59	Time Range 24/7

Select : All, None

## 6.3. Configure Dial Pattern for Communications Portal

In order to route calls to the Communications Portal a dial pattern is created pointing to the SIP Entity. Select **Dial Patterns** from the left window and click on **New** in the main window.

The screenshot displays the Avaya Aura System Manager 8.1 interface. The top navigation bar includes the Avaya logo, the text 'Aura® System Manager 8.1', and several menu items: 'Users', 'Elements', 'Services', 'Widgets', and 'Shortcuts'. Below this, a secondary navigation bar shows 'Home' and 'Routing' (with a close icon). The left sidebar is expanded to show 'Routing' and its sub-items: 'Domains', 'Locations', 'Conditions', 'Adaptations', 'SIP Entities', 'Entity Links', 'Time Ranges', 'Routing Policies', 'Dial Patterns' (highlighted in blue), and 'Origination Dial...'. The main content area is titled 'Dial Patterns' and features a toolbar with 'New' (highlighted in yellow), 'Edit', 'Delete', 'Duplicate', and 'More Actions'. Below the toolbar, it indicates '12 Items' with a refresh icon. A table lists the dial patterns with columns for selection, pattern, minimum length, maximum length, emergency call status, and emergency service. The table contains 12 rows of data. At the bottom of the table, there is a 'Select : All, None' option.

<input type="checkbox"/>	Pattern	Min	Max	Emergency Call	Emergency Service
<input type="checkbox"/>	<a href="#">0</a>	10	10	<input type="checkbox"/>	
<input type="checkbox"/>	<a href="#">+1</a>	11	12	<input type="checkbox"/>	
<input type="checkbox"/>	<a href="#">113</a>	3	3	<input checked="" type="checkbox"/>	Police
<input type="checkbox"/>	<a href="#">114</a>	3	3	<input checked="" type="checkbox"/>	Fire Truck
<input type="checkbox"/>	<a href="#">115</a>	3	3	<input checked="" type="checkbox"/>	Ambulance
<input type="checkbox"/>	<a href="#">3</a>	5	5	<input type="checkbox"/>	
<input type="checkbox"/>	<a href="#">5</a>	4	4	<input type="checkbox"/>	
<input type="checkbox"/>	<a href="#">6</a>	5	5	<input type="checkbox"/>	
<input type="checkbox"/>	<a href="#">7</a>	5	5	<input type="checkbox"/>	
<input type="checkbox"/>	<a href="#">8</a>	5	5	<input type="checkbox"/>	
<input type="checkbox"/>	<a href="#">89999</a>	5	5	<input type="checkbox"/>	
<input type="checkbox"/>	<a href="#">9</a>	11	14	<input type="checkbox"/>	

Select : All, None



The **Dial Pattern Details** screen is displayed. Enter the number to be routed noting this will be the same number outlined in **Section 5.5**. In the **Originating Locations and Routing Policies** sub-section, click **Add**.

Dial Pattern Details

CommitCancel

General

\* Pattern: 3

\* Min: 5

\* Max: 5

Emergency Call: ☐

SIP Domain: -ALL- ▼

Notes: Enghouse CP

Originating Locations and Routing Policies

AddRemove

Select a preconfigured **Originating Location** and select the **Routing Polices** created in previous **Section 6.2** (not shown). The configuration below shows calls to **3xxxx** were routed to Communications Portal. Click on **Commit** as shown below to save configuration.

Dial Pattern Details

CommitCancel

General

\* Pattern: 3

\* Min: 5

\* Max: 5

Emergency Call: ☐

SIP Domain: -ALL- ▼

Notes: Enghouse CP

Originating Locations and Routing Policies

AddRemove

1 Item

<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"/>	-ALL-		To_CP	0	<input type="checkbox"/>	Enghouse CP	

Select : All, None

## 7. Configure Enghouse Interactive Communications Portal

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

- Generate CSR and Private key for TLS SIP Trunk
- Configuration of Communications Portal

### 7.1. Generate CSR and Private key for TLS SIP Trunk

To enable TLS, generating a Cert Signing Request (CSR) and private key on the CP server system first.

- Use command prompt and open folder <Communications Portal install folder>\Tools\OpenSSL and enter following command:

```
openssl_scp.exe req -out ENGHOUSECP.csr -new -newkey rsa:2048 -nodes -sha256 -keyout ENGHOUSECP.key -config openssl.cnf
```

Enter following information as below:

Country Name (2 letter code) [AU]:**VN**

State or Province Name (full name) [Some-State]:**HCM**

Locality Name (eg, city) []:**PN**

Organization Name (eg, company) [Internet Widgits Pty Ltd]:**Avaya**

Organizational Unit Name (eg, section) []:**DevConnect**

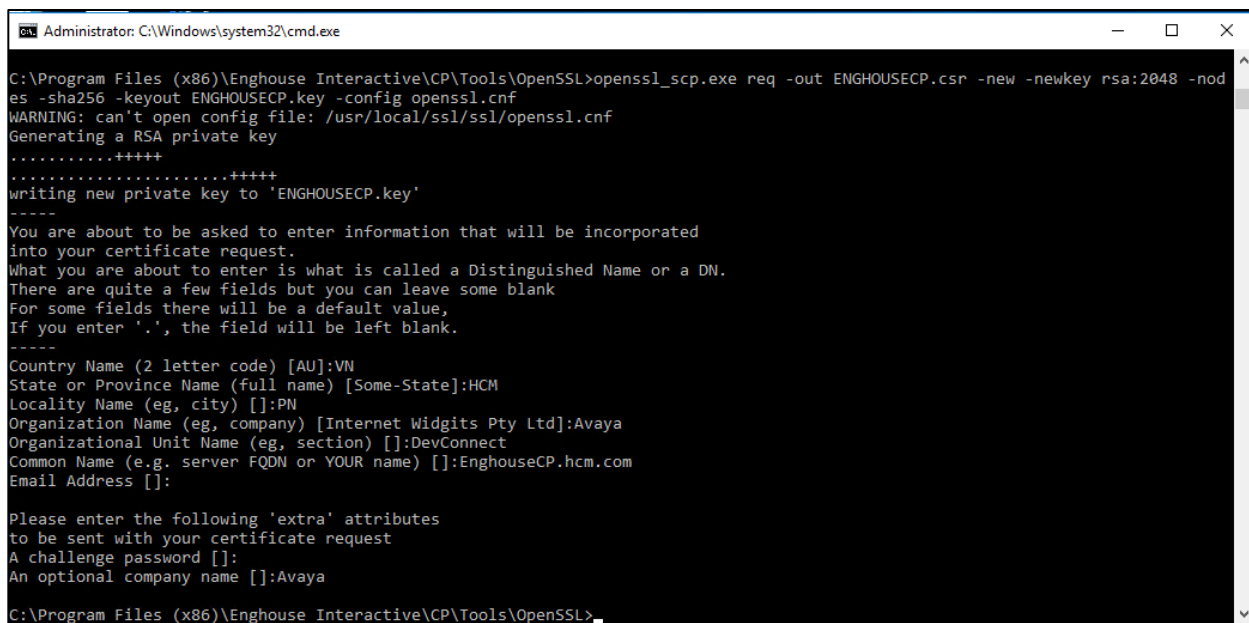
Common Name (e.g. server FQDN or YOUR name) []:**EnghouseCP.hcm.com**

Email Address []:

Please enter the following 'extra' attributes  
to be sent with your certificate request

A challenge password []:

An optional company name []:**Avaya**



```
Administrator: C:\Windows\system32\cmd.exe
C:\Program Files (x86)\Enghouse Interactive\CP\Tools\OpenSSL>openssl_scp.exe req -out ENGHOUSECP.csr -new -newkey rsa:2048 -nodes -sha256 -keyout ENGHOUSECP.key -config openssl.cnf
WARNING: can't open config file: /usr/local/ssl/ssl/openssl.cnf
Generating a RSA private key
.....+++++
.....+++++
writing new private key to 'ENGHOUSECP.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:VN
State or Province Name (full name) [Some-State]:HCM
Locality Name (eg, city) []:PN
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Avaya
Organizational Unit Name (eg, section) []:DevConnect
Common Name (e.g. server FQDN or YOUR name) []:EnghouseCP.hcm.com
Email Address []:

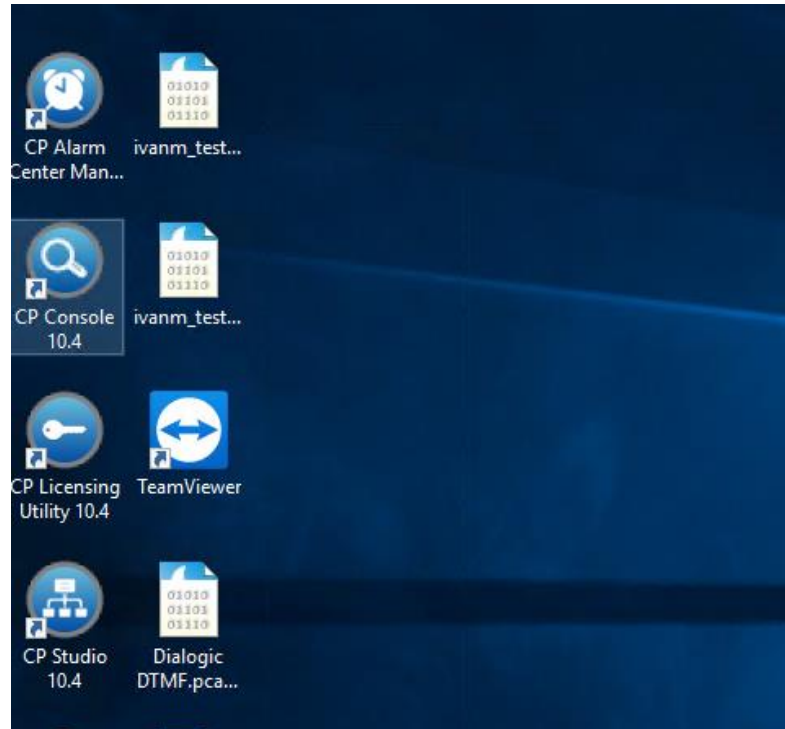
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:Avaya

C:\Program Files (x86)\Enghouse Interactive\CP\Tools\OpenSSL>
```

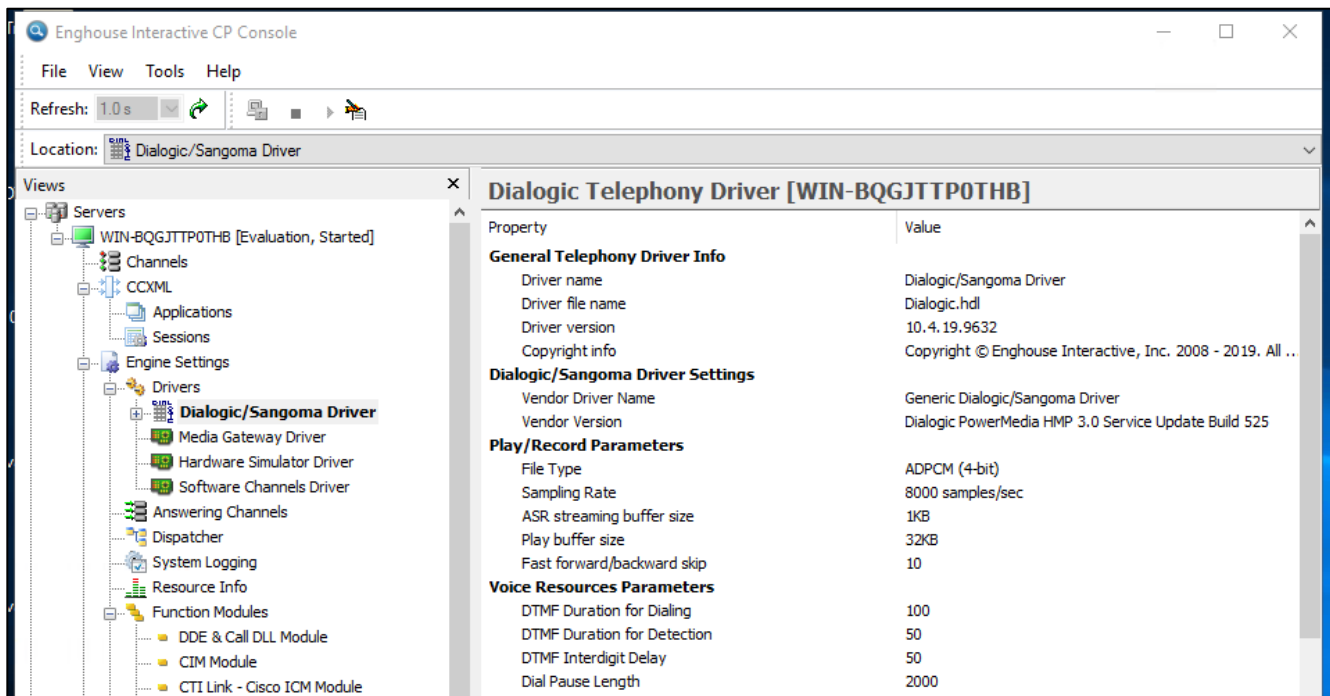
Cert Signing Request (CSR) file **ENGHOUSECP.csr** and private key file **ENGHOUSECP.key** are generated. CSR file then can be sent to Avaya which can make the Identity Certificate (.pem file).

## 7.2. Configuration of Communications Portal

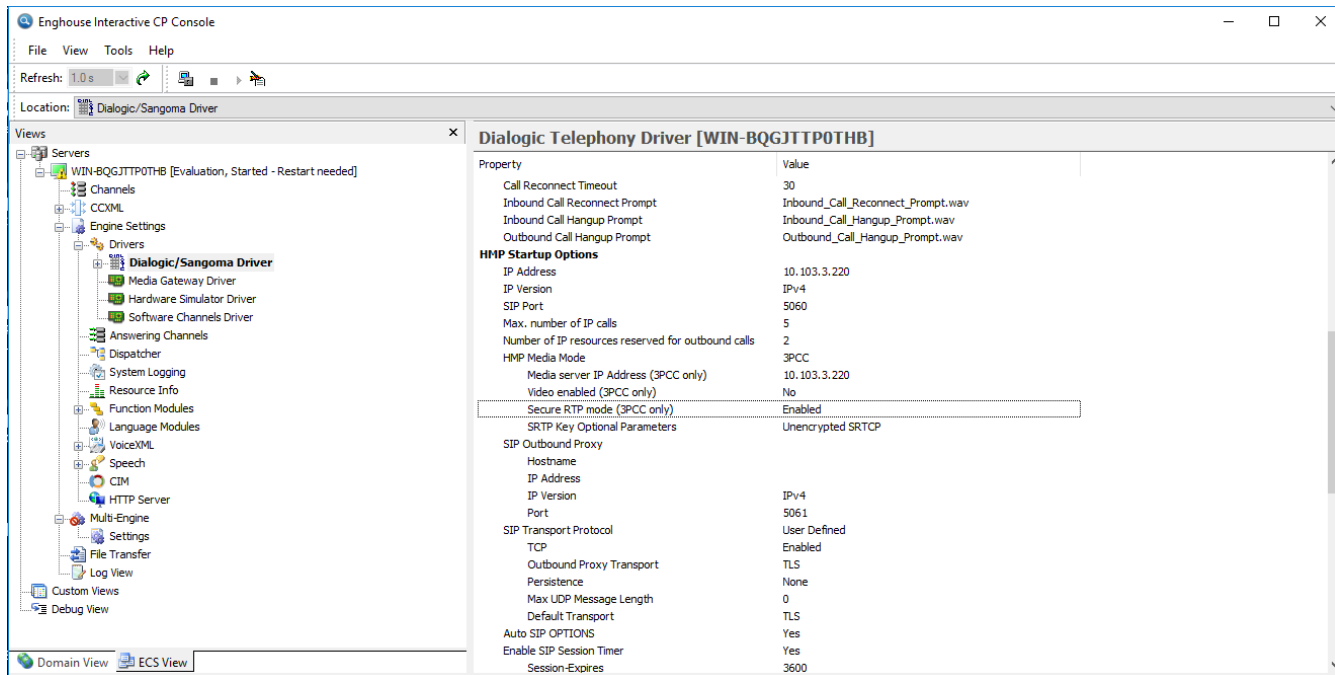
The Telephony module of Communications Portal which provides the connection to Session Manager is provided by a Dialogic Boards Driver. This driver completely caters for the telephony module of this solution. To configure the Dialogic Boards Driver, open the **CP Console 10.4** by double clicking on the shortcut as shown below.



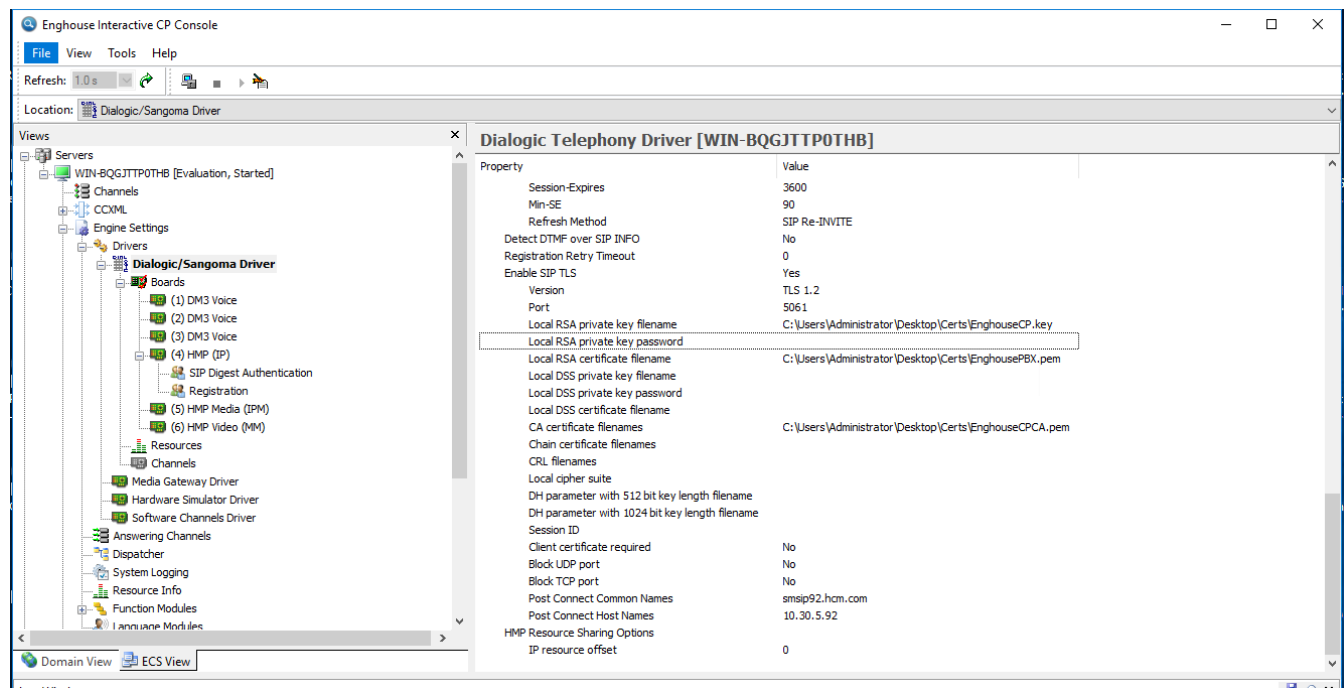
In the left window, navigate to **Servers**→[Server Name]→**Engine Settings** → **Drivers** → **Dialogic/Sangoma Driver**.



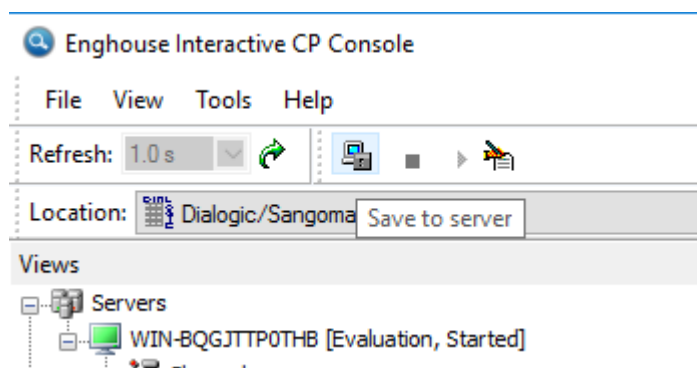
In the main window scroll down to **HMP Startup Options**, ensure that **Auto SIP OPTIONS** is set to **Yes**. **SIP Transport Protocol** is set to **User Defined** and **TLS** is **enabled**, also note the **Default Transport** is set to **TLS**. And in **HMP Media Mode** select **3PCC**.



Scroll down, Select **Enable SIP TLS** as **Yes** with **Version TLS 1.2** and **Port 5061**. In **Local RSA private key filename** field select private key with full location path already created on **Section 7.1**. Select **Local RSA certificate filename** with identity certificate and **CA certificate filenames** with all trusted CA certificate. Enter **Post Connect Common Names** with Avaya Session Manager SIP FQDN and **Post Connect Host Names** with SM SIP IP Address.



Click Save to server to save all configuration and restart CP.

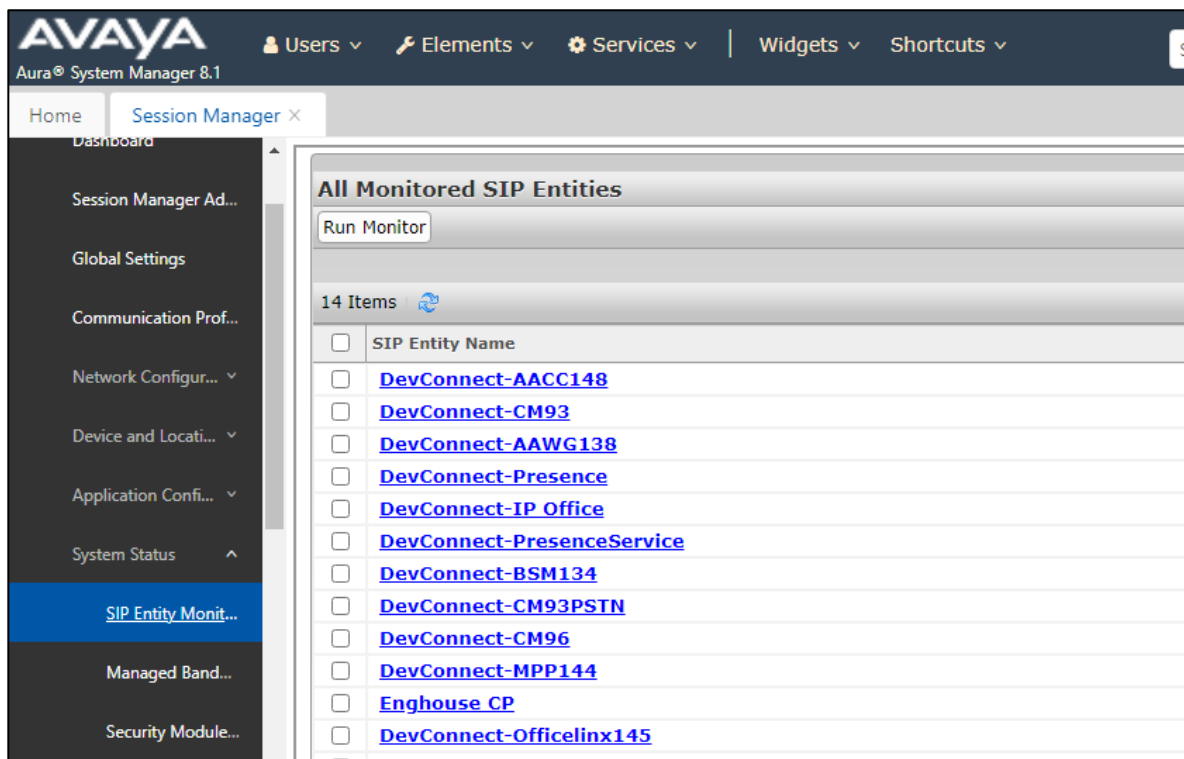


## 8. Verification Steps

To verify a successful configuration of Enghouse Interactive Communications Portal and Session Manager/Communication Manager, a call is placed from a PSTN telephone to the Communications Portal with the caller getting answered successfully hearing clear and audible speech.

### 8.1. Verify Avaya Aura® Session Manager

To verify SIP connectivity to Communications Portal, on System Manager, navigate to **Elements** → **Session Manager** → **System Status** → **SIP Entity Monitoring**. Under the **All Monitored SIP Entities**, select the **Enghouse CP** Entity.



Verify **Conn. Status** is **UP**.

All Entity Links to SIP Entity: Enghouse CP									
Summary View									
1 Item <span>Filter: Enable</span>									
	Session Manager Name	Session Manager IP Address Family	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
<input type="radio"/>	<a href="#">DevConnect-SMSIP</a>	IPv4	10.103.3.220	5061	TLS	FALSE	UP	200 OK	UP
Select : None									

## 8.2. Verify SRTP is being used via Avaya Aura® Communication Manager

When calls are active on CP, verify that SRTP is being used by checking the status of the SIP trunk between Communication Manager and Session Manager that's being used for the call. Use the `status trunk` command and navigate to Page 3 to verify that SRTP is being used for the call as shown below. Use the **status trunk 1** command to determine which trunk member is active, example trunk member **11** is active as shown below

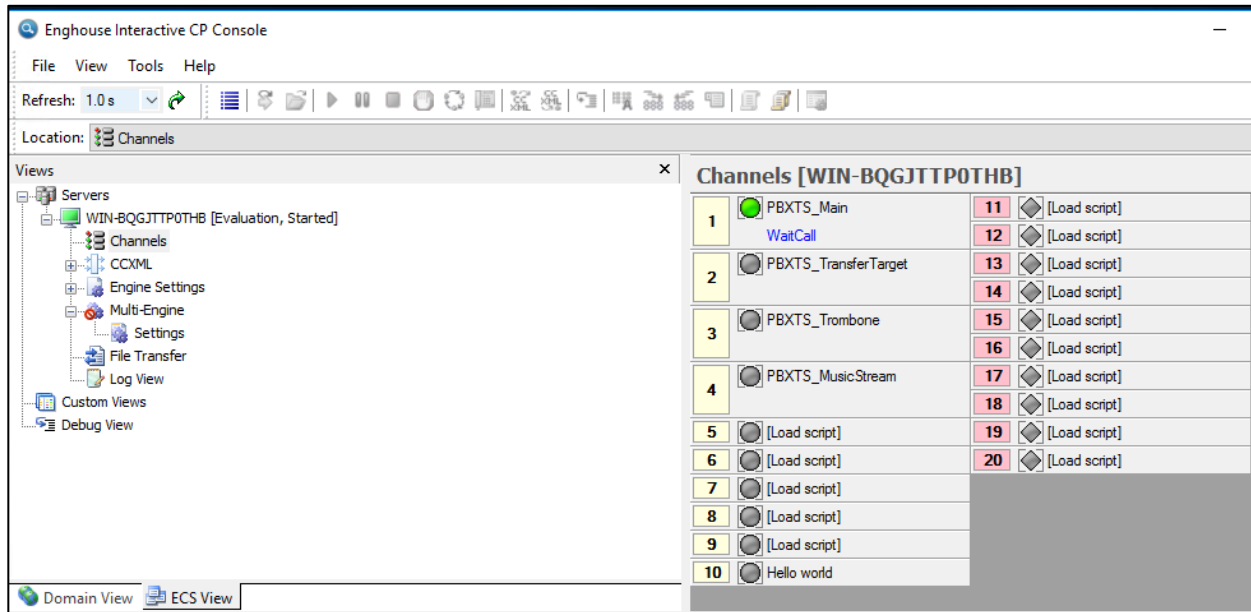
status trunk 1				Page	1
TRUNK GROUP STATUS					
Member	Port	Service State	Mtce Connected Ports	Busy	
0001/0001	T000001	in-service/idle	no		
0001/0002	T000002	in-service/idle	no		
0001/0003	T000003	in-service/idle	no		
0001/0004	T000004	in-service/idle	no		
0001/0005	T000005	in-service/idle	no		
0001/0006	T000006	in-service/idle	no		
0001/0007	T000007	in-service/idle	no		
0001/0008	T000008	in-service/idle	no		
0001/0009	T000009	in-service/idle	no		
0001/0010	T000010	in-service/idle	no		
<b>0001/0011</b>	<b>T000011</b>	<b>in-service/active</b>	<b>no</b>	<b>T000249</b>	
0001/0012	T000012	in-service/idle	no		
0001/0013	T000013	in-service/idle	no		
0001/0014	T000014	in-service/idle	no		

Use **command status trunk 01/011**, on **page 3** to check RTP status of the call, example for media shuffling enable (Direct IP-IP Audio Connections set to y) as shown below

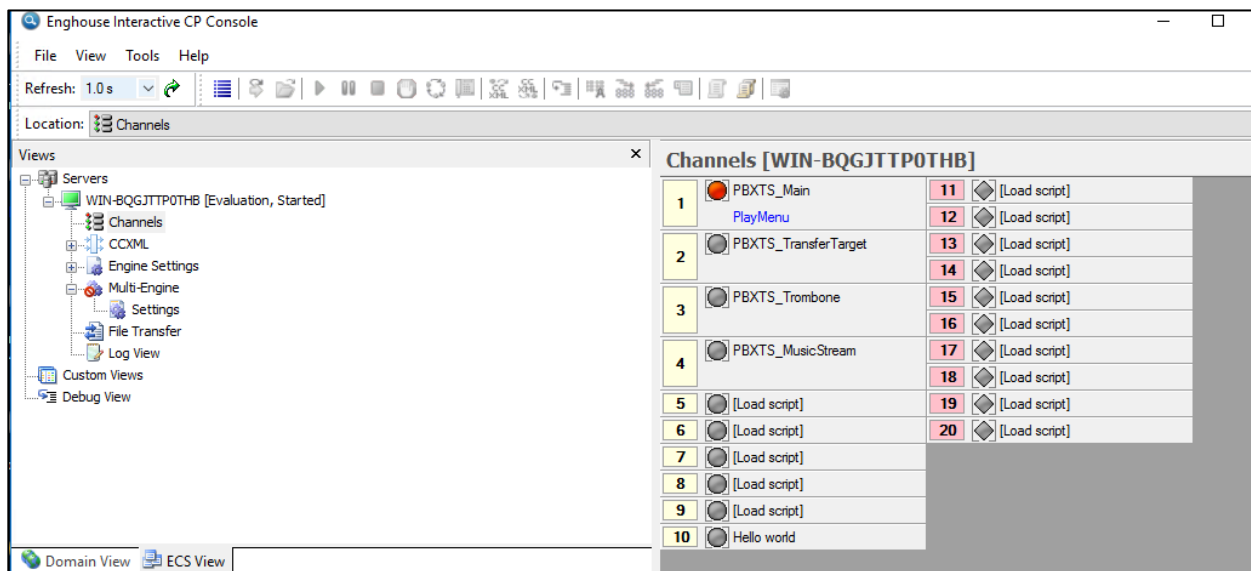
status trunk 01/11		Page	3 of	3
SRC PORT TO DEST PORT TALKPATH				
src port: T000011				
T000011:TX:10.103.3.220:29016/g711u/20ms/1-srtp-aescm128-hmac80				
T000249:RX:10.30.5.99:37392/g711u/20ms/1-srtp-aescm128-hmac80				
dst port: T000249				

### 8.3. Verify Enhouse Interactive Communications Portal

On **CP Console 10.4**, monitor the Channel 1 below show as green that mean CP is available to receive the call.



Place a call from the PSTN to CP ensure the call can be answered by CP. Monitor the Channel 1 below should also show as Red.





## 9. Conclusion

These Application Notes describe the configuration steps required for Enghouse Interactive Communications Portal 10.4 to successfully interoperate with Avaya Aura® Session Manager 8.1.3.3 and Avaya Aura® Communication Manager 8.1.3.3. All feature functionality and serviceability test cases were completed successfully as outlined in **Section 2.2**.

## 10. Additional References

Documentation related to Avaya can be obtained from <https://support.avaya.com>.

1. *Administering Avaya Aura® Communication Manager*, Release 8.1.x, Issue 12, July 2021
2. *Administering Avaya Aura® Session Manager*, Release 8.1.x, Issue 10, Sept 2021
3. *Administering Avaya Aura® System Manager*, Release 8.1.x, Issue 17, Nov 2021
- 4.

---

**©2022 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.

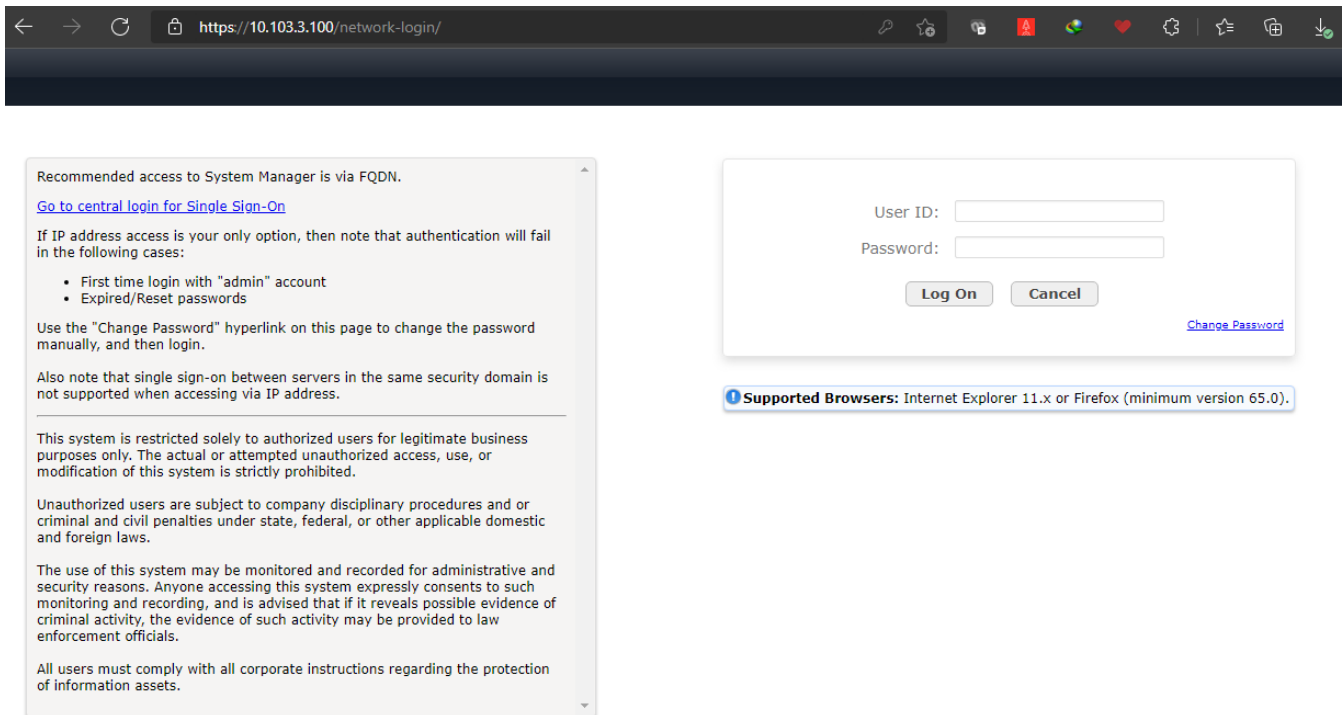
Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya DevConnect Program at [devconnect@avaya.com](mailto:devconnect@avaya.com).

## Appendix

The following section shows the creation of the Enghouse Communications Portal End Entity on the SMGR CA in order to sign the CSR generated by Communications Portal.

### Add End Entity

The 3<sup>rd</sup> party endpoint (Communications Portal) is added to the CA as an end entity. Log in to the Certificate Authority, in this case a System Manager.



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.

---

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

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

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

All users must comply with all corporate instructions regarding the protection of information assets.

User ID:

Password:

[Change Password](#)

**Supported Browsers:** Internet Explorer 11.x or Firefox (minimum version 65.0).

Click on **Services** → **Security** → **Certificates** → **Authority** from the main menu.

The screenshot shows the Avaya Aura System Manager 8.1 interface. The top navigation bar includes 'Users', 'Elements', 'Services', 'Widgets', and 'Shortcuts'. The 'Services' menu is expanded, showing options like 'Backup and Restore', 'Bulk Import and Export', 'Configurations', 'Events', 'Geographic Redundancy', 'Inventory', 'Licenses', 'Replication', 'Reports', 'Scheduler', 'Security', 'Shutdown', 'Solution Deployment Manager', 'Templates', and 'Tenant Management'. The 'Security' option is highlighted, and its sub-menu is shown, including 'Certificates', 'Configuration', 'Authority', 'Enrollment Password', 'Manage Certificate Revocation', and 'Manage Entity Classes'. The 'Authority' option is selected, leading to the 'Authority' page. The 'Authority' page displays 'Current Usage' as 63/250000 USERS and 2/50 SIMULTANEOUS ADMINISTRATIVE LOGINS.

Click on **Add End Entity**

The screenshot shows the 'Authority' page in the Avaya Aura System Manager 8.1 interface. The left sidebar shows the navigation path: 'Security' → 'Certificates' → 'Authority'. The 'Add End Entity' option is highlighted in the 'RA Functions' section. The main content area displays 'Welcome smgr100.hcm.com to EJBCA Administration.' and 'Node hostname : smgr100.hcm.com'. It also shows 'Server time : 2021-09-27 12:30:09+07:00' and 'CA health state [?]'. A table shows the 'CA Name', 'CA Service', and 'CRL Status' for 'tmdefaultca', with both 'CA Service' and 'CRL Status' marked as '✓'. The 'Publish queue status [?]' is also shown, with a table indicating 'No publishers defined.'.

The following is an example of the **End Entity** that was added for compliance testing. Take note of the **Password (or Enrollment Code)**, this will be required later, the **IP address** will be that of the Communications Portal and the **Common name** and **Username** should be hostname associated with the Communications Portal. Click on **Save** once the information has been filled in correctly.

**AVAYA** Aura® System Manager 8.1

Users ▾ Elements ▾ Services ▾ | Widgets ▾ Shortcuts ▾

Home Security ×

Security ▾  
Certificates ▾  
**Authority**  
Enrollment Password  
Manage Certificate ...  
Manage Entity Clas...  
Configuration ▾

**CA Functions**  
CA Activation  
CA Structure & CRLs  
Certificate Profiles  
Certification Authorities  
Crypto Tokens  
Publishers  
**RA Functions**  
Add End Entity  
End Entity Profiles  
Search End Entities  
User Data Sources  
**Supervision Functions**  
Approve Actions  
View Log  
**System Functions**  
Administrator Roles  
Internal Key Bindings  
Services  
**System Configuration**  
CMP Configuration  
SCEP Configuration

## Add End Entity

End Entity Profile	EXTERNAL_CSR_PROFILE ▾	Required
Username	EnghouseCP	<input checked="" type="checkbox"/>
Password (or Enrollment Code)	*****	<input checked="" type="checkbox"/>
Confirm Password	*****	
E-mail address	<input type="text"/> @ <input type="text"/>	<input type="checkbox"/>
<b>Subject DN Attributes</b>		
CN, Common name	Enghouse.hcm.com	<input checked="" type="checkbox"/>
CN, Common name	<input type="text"/>	<input type="checkbox"/>
O, Organization	AVAYA	<input type="checkbox"/>
C, Country (ISO 3166)	VN	<input type="checkbox"/>
OU, Organizational Unit	DevConnect	<input type="checkbox"/>
L, Locality	PN	<input type="checkbox"/>
ST, State or Province	HCM	<input type="checkbox"/>
<b>Other subject attributes</b>		
<b>Subject Alternative Name</b>		
DNS Name	Enghouse.hcm.com	<input type="checkbox"/>
DNS Name	<input type="text"/>	<input type="checkbox"/>
IP Address	10.103.3.220	<input type="checkbox"/>
<b>Main certificate data</b>		
Certificate Profile	ID_CLIENT_SERVER ▾	<input checked="" type="checkbox"/>
CA	tmdefaultca ▾	<input checked="" type="checkbox"/>
Token	User Generated ▾	<input checked="" type="checkbox"/>
Add Reset		

Made by PrimeKey Solutions AB, 2002–2014.

## Generate the Identity Certificate

From the CA, click on the **Public Web** down the left side of the page.

**AVAYA** Aura® System Manager 8.1

Users ▾ Elements ▾ Services ▾ | Widgets ▾ Shortcuts ▾

Home Security ×

**Security** ▴

Certificates ▴

**Authority**

Enrollment Password

Manage Certificate ...

Manage Entity Clas...

Configuration ▾

**CA Functions**

- CA Activation
- CA Structure & CRLs
- Certificate Profiles
- Certification Authorities
- Crypto Tokens
- Publishers

**RA Functions**

- Add End Entity
- End Entity Profiles
- Search End Entities
- User Data Sources

**Supervision Functions**

- Approve Actions
- View Log

**System Functions**

- Administrator Roles
- Internal Key Bindings
- Services

**System Configuration**

- CMP Configuration
- SCEP Configuration
- System Configuration

**My Preferences**

**Public Web**

**Welcome smgr100.hcm.com to EJBCA Administration.**

Node hostname : smgr100.hcm.com  
Server time : 2021-09-27 12:37:24+07:00  
**CA health state [?]**

**Publish queue status [?]**

CA Name	CA Service	CRL Status	Publisher	Length
tmdefaultca	✓	✓	No publishers defined.	

Made by PrimeKey Solutions AB, 2002–2014.

The following web page is opened, click on **Create Certificate from CSR**

**EJBCA**  
PKI BY PRIMEKEY

**Enroll**

- Create Browser Certificate
- Create Certificate from CSR**
- Create Keystore
- Create CV certificate

**Register**

- Request Registration

**Retrieve**

- Fetch CA Certificates
- Fetch CA CRLs
- List User's Certificates
- Fetch User's Latest Certificate

**Inspect**

- Inspect certificate/CSR
- Check Certificate Status

**Miscellaneous**

- Administration
- Documentation

**Welcome to the public EJBCA pages**

**Enroll**

- Create Browser Certificate - Install a certificate in your web browser. This certificate may be exportable depending on browser and browser settings.
- Create Certificate from CSR - Send a PKCS#10 certificate request generated by your server, and receive a certificate that can be installed on the server. Consult your server documentation.
- Create Keystore - Create a server generated keystore in PEM, PKCS#12 or JKS format and save to your disc. This keystore can be installed in a server, browser or in other applications.
- Create CV Certificate - Used for EU EAC ePassport PKI. Send a CVC certificate request generated by an Inspection System, and receive a CV certificate. Note: this can not be used for regular certificates, CV certificates are completely different.

**Retrieve**

- Fetch CA Certificates - Browse and download CA certificates.
- Fetch CA CRLs - Download Certificate Revocation Lists.
- Fetch User's Latest Certificate - Download the last issued certificate for a user for whom you know the certificate Distinguished Name.

**Inspect**

- Inspect certificate/CSR - Inspect a dump of a CSR or a certificate. This gives an output of a CVC or ASN.1 dump, suitable for technical inspection and debugging.

**Miscellaneous**

- List User's Certificates - List certificates for a user for whom you know the certificate Distinguished Name.
- Check Certificate Status - Check revocation status for a certificate where you know the Issuer Distinguished Name and the serial number.

Choose CSR file **EnghouseCP.csr**, this is taken from the CSR generated by Enghouse as shown on the previous page. Select Result type with **PEM – full certificate chain** and click **OK** to download **Identity Certificate**.

## Certificate enrollment from a CSR

Please give your username and enrollment code, select a PEM- or DER-formatted certification request file (C: PEM-formatted request into the field below and click OK to fetch your certificate.

A PEM-formatted request is a BASE64 encoded certificate request starting with

-----BEGIN CERTIFICATE REQUEST-----

and ending with

-----END CERTIFICATE REQUEST-----

Enroll

Username

Enrollment code

Request file  EnghouseCP.csr

or pasted request

Result type

