



Avaya Solution & Interoperability Test Lab

Application Notes for configuring Enghouse Interactive Communications Portal 10.1 using CTIC Media Gateway for SIP 8.2 with Avaya Aura® Session Manager R7.0 and Avaya Aura® Communication Manager R7.0 using TLS and SRTP - Issue 1.0

Abstract

These Application Notes describe the configuration steps for Enghouse Interactive Communications Portal 10.1 using CTIC Media Gateway for SIP 8.2 to successfully interoperate with Avaya Aura® Session Manager R7.0 and Avaya Aura® Communication Manager R7.0 using TLS/SRTP. Communications Portal is an IVR application that connects to Session Manager as a SIP Entity.

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

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

1. Introduction

These Application Notes describe the configuration steps for Enghouse Interactive Communications Portal 10.1 to successfully interoperate with Avaya Aura® Session Manager R7.0 and Avaya Aura® Communication Manager R7.0 using Transport Layer Security (TLS) and Secure Real-time Transport Protocol (SRTP). Enghouse Interactive Communications Portal (formerly Syntellect Communications Portal) is an open, standards-based platform with integrated application development and management components.

- Voice self-service solutions, such as interactive voice response (IVR), interactive voice and video response (IVVR), outbound dialing, and speech-enabled self-service systems.
- SMS, email, standards-based voice mail.
- Contact center solutions, including outbound dialing, intelligent routing applications and screen pop applications.
- Unified communications solutions, including standards-based voice-mail systems and applications that combine traditional voice, IP telephony, video messaging, SMS, email, and fax communication.

The primary goal of the Transport Layer Security (TLS) protocol is to provide privacy and data integrity between two communicating computer applications. When secured by TLS, connections between a client (e.g., Enghouse Interactive Communications Portal 10.1) and a server (e.g., Avaya Aura® Session Manager) have one or more of the following properties:

- The connection is private because symmetric cryptography is used to encrypt the data transmitted. The keys for this symmetric encryption are generated uniquely for each connection and are based on a shared secret negotiated at the start of the session. The server and client negotiate the details of which encryption algorithm and cryptographic keys to use before the first byte of data is transmitted. The negotiation of a shared secret is both secure and reliable.
- The identity of the communicating parties can be authenticated using public-key cryptography. This authentication can be made optional, but is generally required for at least one of the parties (typically the server).
- The connection is reliable because each message transmitted includes a message integrity check using a message authentication code to prevent undetected loss or alteration of the data during transmission.

The Secure Real-time Transport Protocol (or SRTP) defines a profile of RTP (Real-time Transport Protocol), intended to provide encryption, message authentication and integrity, and replay protection to the RTP data in both unicast and multicast applications. Since RTP is closely related to RTCP (Real Time Control Protocol) which can be used to control the RTP session, SRTP also has a sister protocol, called Secure RTCP (or SRTCP); SRTCP provides the same security-related features to RTCP, as the ones provided by SRTP to RTP. Utilization of SRTP or SRTCP is optional to the utilization of RTP or RTCP; but even if SRTP/SRTCP are used, all provided features (such as encryption and authentication) are optional and can be separately enabled or disabled. The only exception is the message authentication feature which is indispensably required when using SRTCP.

2. General Test Approach and Test Results

The IVR application telephony functionality of Communications Portal 10.1 (CP) was the only module tested. This IVR application (CP script) connects to Session Manager as a SIP Trunk entity and can be integrated with Communication Manager by passing SIP calls to and from the PBX. Session Manager directs the call over SIP trunks to CP scripts which in turn handles the call depending on the digits dialled using SIP signaling. Communications Portal utilizes CTI Media Gateway driver to perform all telephony functions on the server. This CTI Media Gateway facilitates the Communications Portal connectivity to Session Manager.

Note: It is assumed that all TLS connections are already established between System Manager, Session Manager and Communication Manager along with the H323 and SIP deskphones that were used as part of the compliance testing. The description of any such setup is deemed as being outside the scope of these Application Notes.

Note: All test cases were performed with Direct IP –IP Audio Connection set to N. Note that any other setting does not work when using SRTP.

DevConnect Compliance Testing is conducted jointly by Avaya and DevConnect members. The jointly-defined test plan focuses on exercising APIs and/or standards-based interfaces pertinent to the interoperability of the tested products and their functionalities. DevConnect Compliance Testing is not intended to substitute full product performance or feature testing performed by DevConnect members, nor is it to be construed as an endorsement by Avaya of the suitability or completeness of a DevConnect member's solution.

2.1. Interoperability Compliance Testing

The interoperability compliance test included both feature functionality and serviceability testing. The feature functionality testing focused on placing various calls to the Communications Portal IVR:

- **Basic Inbound/Outbound** – Tests inbound calls to Enghouse Interactive Communications Portal.
- **Call Hold** – Tests held calls to/from Enghouse Interactive Communications Portal.
- **Call Transfer** – Tests transferred calls to/from Enghouse Interactive Communications Portal.
- **IVR Functionality** – Tests of various IVR features like is ANI/DNIS detection, leaving voice message/voice mail (Recording), DTMF collection, Barge-in and Trombone Referral on the Enghouse Interactive Communications Portal.
- **Failover/Service** – Tests the behaviour of Enghouse Interactive Communications Portal when there are certain failed conditions and verifying the ability of Communications Portal to recover from disconnection and reconnection to the Avaya solution.

2.2. Test Results

All functionality and serviceability test cases were completed successfully, however the following issues were observed.

- All test cases were performed with Direct IP –IP Audio Connection set to N. Note that any other setting does not work when using SRTP. See **Section 5.6**.
- Setting Encrypted SRTCP to any other option but best-effort would not establish a new call. See **Section 5.5**.
- CLID on phone called by CP is not updated with the correct CLID after transfer is completed. To resolve this, the script was updated to send the FROM information. This is configurable on a per customer basis and is not hardcoded as part of the SIP firmware.
- Compliance testing was also carried out using TCP/RTP and all test cases passed with Direct IP –IP Audio Connection set to both Y and N.

2.3. Support

Technical support can be obtained for Enghouse Interactive as follows:

USA

- Email: 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 / supportenvox@syntellect.com
- Website: <http://www.enghouseinteractive.com/services/support/>
- Phone: +44 870.220.2205

3. Reference Configuration

The configuration in **Figure 1** was used to compliance test Enghouse Interactive Communications Portal 10.1 with Session Manager and Communication Manager using SIP signalling over SIP trunks to route calls from Communication Manager to Communications Portal 10.1. The TLS protocol is to provide privacy and data integrity between two communicating computer applications and SRTP used to provide encryption, message authentication and integrity, and replay protection to the RTP data.

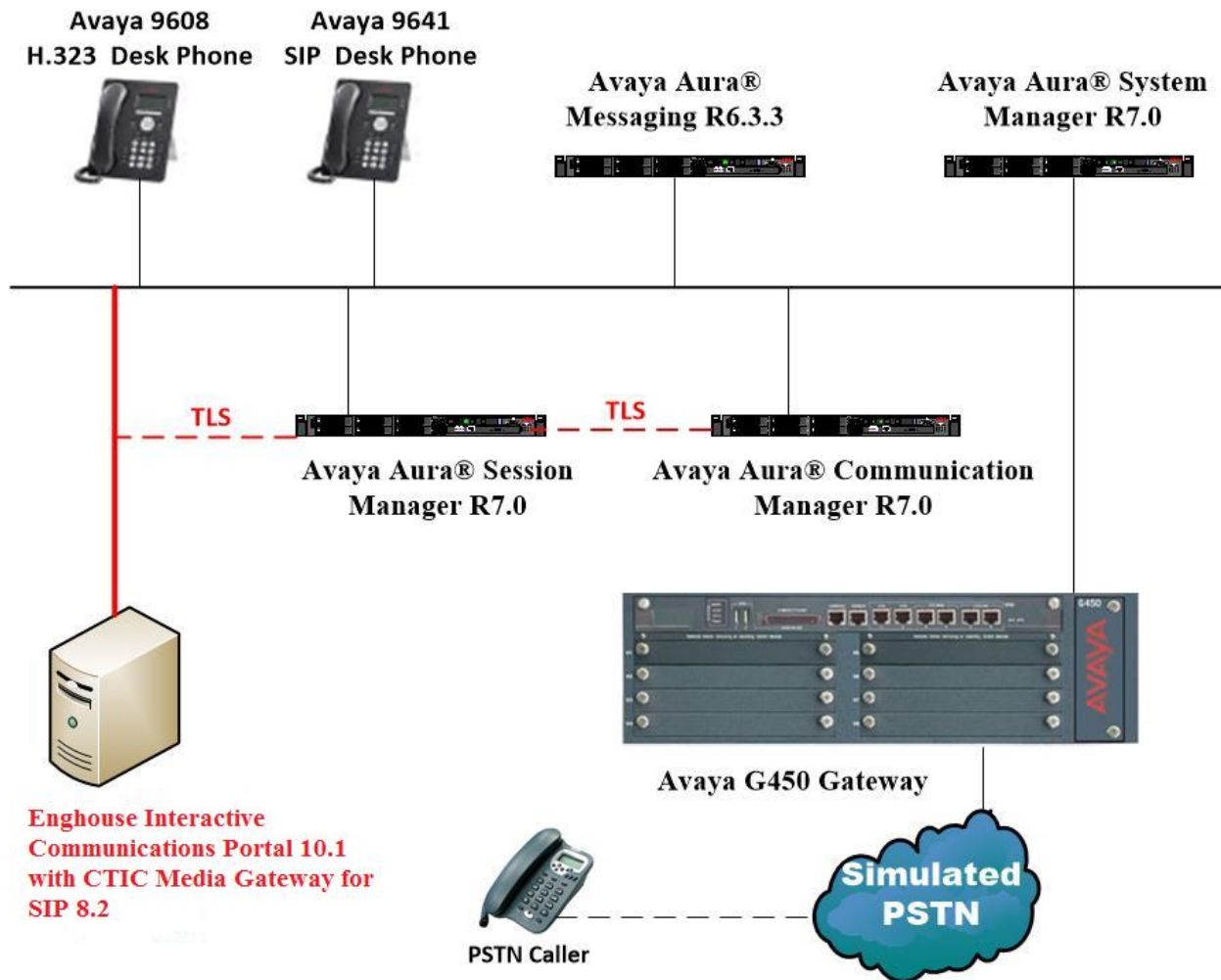


Figure 1: Connection of Enghouse Interactive Communications Portal 10.1 with Avaya Aura® Session Manager R7.0 and Avaya Aura® Communication Manager R7.0

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 running on a virtual server | System Manager 7.0.1.0 Build No. - 7.0.0.0.16266 Software Update Revision No: 7.0.1.0.064859 Feature Pack 1 |
| Avaya Aura® Session Manager running on a virtual server | Session Manager R7.0 SP1 Build No. – 7.0.1.0.701007 |
| Avaya Aura® Communication Manager running on a virtual server | R7.0 R017x.00.0.441.0 00.0.441.0-23012 |
| Avaya Aura® Messaging running on a virtual server | R6.3.3 |
| Avaya G450 Gateway | 37.19.0 /1 |
| Avaya 9608 H323 Deskphone | 96x1 H323 Release 6.6.028 |
| Avaya 9608 SIP Deskphone | 96x1 SIP Release 7.0.0.39 |
| Enghouse Interactive Communications Portal running on Windows 2012 R2 | Communications Portal 10.1 with CTIC Media Gateway for SIP 8.2 SP1F |

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 11**.

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

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

Note: The configuration of PSTN trunks and routes are outside the scope of these Application Notes.

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 Communications Portal 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 2 SIP trunks.

| display system-parameters customer-options | | Page | 2 of 11 |
|---|------------------|------|---------|
| OPTIONAL FEATURES | | | |
| IP PORT CAPACITIES | USED | | |
| Maximum Administered H.323 Trunks: | 12000 250 | | |
| Maximum Concurrently Registered IP Stations: | 18000 2 | | |
| Maximum Administered Remote Office Trunks: | 12000 0 | | |
| Maximum Concurrently Registered Remote Office Stations: | 18000 0 | | |
| Maximum Concurrently Registered IP eCons: | 414 0 | | |
| Max Concur Registered Unauthenticated H.323 Stations: | 100 0 | | |
| Maximum Video Capable Stations: | 18000 0 | | |
| Maximum Video Capable IP Softphones: | 18000 0 | | |
| Maximum Administered SIP Trunks: | 24000 319 | | |
| Maximum Administered Ad-hoc Video Conferencing Ports: | 24000 0 | | |

On **Page 3**, ensure that both **ARS** and **ARS/AAR Partitioning** are set to **y**.

| | |
|--|-------------------------------------|
| display system-parameters customer-options | Page 3 of 11 |
| OPTIONAL FEATURES | |
| Abbreviated Dialing Enhanced List? y | Audible Message Waiting? y |
| Access Security Gateway (ASG)? n | 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 |

On **Page 5**, ensure that **Uniform Dialing Plan** is set to **y**.

| | |
|--|------------------------------------|
| display system-parameters customer-options | Page 5 of 11 |
| OPTIONAL FEATURES | |
| Multinational Locations? n | Station and Trunk MSP? y |
| Multiple Level Precedence & Preemption? n | Station as Virtual Extension? y |
| Multiple Locations? n | 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 |

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 11** 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? no | |
| DID/Tie/ISDN/SIP Intercept Treatment: attd | |
| 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 **8** is used for AAR and **9** for ARS routing.

| | |
|--|-------------------|
| display feature-access-codes | Page 1 of 10 |
| 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: 8 | |
| Auto Route Selection (ARS) - Access Code 1: 9 | Access Code 2: |
| Automatic Callback Activation: *25 | Deactivation: #25 |

5.3. Administer Dial Plan

It was decided for compliance testing that all calls beginning with 62 with a total length of 4 digits were to be sent across the SIP trunk to Session Manager and therefore to Communications Portal. 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 **6** is added with a **Total Length** of **4** and a **Call Type** of **udp**.

| | | | | | | | | |
|--------------------------|--------------|-----------|---------------|--------------|-----------|-----------------|--------------|-----------|
| change dialplan analysis | | | | | | Page 1 of 12 | | |
| DIAL PLAN ANALYSIS TABLE | | | | | | | | |
| Location: all | | | | | | Percent Full: 2 | | |
| Dialed String | Total Length | Call Type | Dialed String | Total Length | Call Type | Dialed String | Total Length | Call Type |
| 2 | 4 | ext | | | | | | |
| 3 | 4 | ext | | | | | | |
| 4 | 4 | udp | | | | | | |
| 5 | 4 | ext | | | | | | |
| 6 | 4 | udp | | | | | | |
| 7 | 3 | dac | | | | | | |
| 8 | 1 | fac | | | | | | |
| 9 | 1 | fac | | | | | | |
| * | 3 | fac | | | | | | |
| # | 3 | fac | | | | | | |

5.4. Administer Route Selection for Communications Portal Calls

As digits **6xxx** were defined in the dial plan as udp (**Section 5.3**) use the **change uniform-dialplan** command to configure the routing of the dialed digits. In the example below calls to numbers beginning with **62** that are **4** digits in length will be matched. No further digits are deleted or inserted. Calls are sent to **aar** for further processing.

| | | | | | | | | | |
|---------------------------|-----|-----|--------|-----|------|------|--|--|--|
| change uniform-dialplan 6 | | | | | | | | | |
| UNIFORM DIAL PLAN TABLE | | | | | | | | | |
| Page 1 of 2 | | | | | | | | | |
| Percent Full: 0 | | | | | | | | | |
| Matching | | | Insert | | | Node | | | |
| Pattern | Len | Del | Digits | Net | Conv | Num | | | |
| 62 | 4 | 0 | | aar | n | | | | |
| | | | | | | n | | | |

Use the **change aar analysis x** command to further configure the routing of the dialed digits. Calls to Communications Portal begin with **62** and are matched with the AAR entry shown below. Calls are sent to **Route Pattern 1**, which contains the outbound SIP Trunk Group.

| | | | | | | | | | |
|--------------------------|-------|-----|---------|------|------|------|-----------------|--|--|
| change aar analysis 62 | | | | | | | Page 1 of 2 | | |
| AAR DIGIT ANALYSIS TABLE | | | | | | | | | |
| Location: all | | | | | | | Percent Full: 1 | | |
| Dialed | Total | | Route | Call | Node | ANI | | | |
| String | Min | Max | Pattern | Type | Num | Reqd | | | |
| 62 | 4 | 4 | 1 | unku | | 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 configured in **Section 5.6**.

| | | | | | | | | | | | | | | | | | | | |
|------------------------|-----|-----|-----|-----|------|-----|----------|------|------|----------------------|--------|-------------|------|-----------------|------|-----|-----------|-----|--|
| change route-pattern 1 | | | | | | | | | | Page | 1 | of | 3 | | | | | | |
| Pattern Number: 1 | | | | | | | | | | Pattern Name: SIPTRK | | | | | | | | | |
| SCCAN? n | | | | | | | | | | Secure SIP? n | | | | | | | | | |
| Grp | FRL | NPA | Pfx | Hop | Toll | No. | Inserted | DCS/ | IXC | | | | | | | | | | |
| No | | | Mrk | Lmt | List | Del | Digits | QSIG | | | | | | | | | | | |
| | | | | | | | | 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 | No. | Numbering | LAR | |
| 0 1 2 M 4 W | | | | | | | | | | Request | | | | | | | | | |
| | | | | | | | | | | | | Dgts Format | | | | | | | |
| | | | | | | | | | | | | Subaddress | | | | | | | |
| 1: | y | y | y | y | y | n | n | unre | | | | | 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: | y | y | y | y | y | n | n | rest | | | | | none | | | | | | |

5.5. Configure Network Region and IP Codec

In the Node Names IP form, note the IP Address of the **procr** and the Session Manager (**sm70vmpg**). 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.

| display node-names ip | | Page 1 of 2 |
|-----------------------|--------------------|-------------|
| IP NODE NAMES | | |
| Name | IP Address | |
| AMS77vmpg | 10.10.40.17 | |
| CMS18vmpg | 10.10.40.36 | |
| IPO500V2 | 10.10.40.20 | |
| IPOSE | 10.10.40.25 | |
| PGDECT | 10.10.40.50 | |
| aes70vmpg | 10.10.40.26 | |
| default | 0.0.0.0 | |
| procr | 10.10.40.13 | |
| procr6 | :: | |
| sm70vmpg | 10.10.40.12 | |

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.local**. The **IP Network Region** form also specifies the **IP 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.

| display ip-network-region 1 | | Page 1 of 20 |
|---------------------------------|---|---------------------------------------|
| IP NETWORK REGION | | |
| Region: 1 | | |
| Location: 1 | Authoritative Domain: devconnect.local | |
| Name: Default region | | |
| MEDIA PARAMETERS | | Intra-region IP-IP Direct Audio: yes |
| Codec Set: 1 | | Inter-region IP-IP Direct Audio: yes |
| UDP Port Min: 2048 | | IP Audio Hairpinning? n |
| UDP Port Max: 3329 | | |
| DIFFSERV/TOS PARAMETERS | | |
| Call Control PHB Value: 46 | | |
| Audio PHB Value: 46 | | |
| Video PHB Value: 26 | | |
| 802.1P/Q PARAMETERS | | |
| Call Control 802.1p Priority: 6 | | |
| Audio 802.1p Priority: 6 | | |
| Video 802.1p Priority: 5 | | |
| H.323 IP ENDPOINTS | | AUDIO RESOURCE RESERVATION PARAMETERS |
| H.323 Link Bounce Recovery? y | | RSVP Enabled? n |
| Idle Traffic Interval (sec): 20 | | |
| Keep-Alive Interval (sec): 5 | | |
| Keep-Alive Count: 5 | | |

In the **IP Codec Set** form, select the audio codec's supported for calls routed over the SIP trunk to Communications Portal. 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 example below includes **G.711A** (a-law), which is supported by Communications Portal. Note the **Media Encryption** has been set to **1-srtp-aescm128-hmac80**, this is the encryption that is support by Communications Portal and must be set correctly on each side to allow secure RTP (SRTP). In order for SRTP to work properly, **Encrypted SRTCP** needed to be set to **best-effort** as shown below.

Note: Setting **Encrypted SRTCP** to any other option would not establish a new call.

change ip-codec-set 1
Page 1 of 2

IP CODEC SET

Codec Set: 1

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

Media Encryption
 1: **1-srtp-aescm128-hmac80**
 2:
 3:
 4:
 5:

Encrypted SRTCP: best-effort

5.6. Configure SIP Trunk

Prior to configuring a SIP trunk group for communication with Session Manager, a SIP signaling group must be configured. Configure the Signaling Group form shown below as follows:

- 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 **y** allowing the Communication Manager to automatically detect if the peer server is a Session Manager.
- 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 **sm70vmpg**), 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 **n**.
- The default values for the other fields may be used.

| change signaling-group 1 | | Page 1 of 2 |
|---|------------------------------------|-------------|
| SIGNALING GROUP | | |
| Group Number: 1 | Group Type: sip | |
| IMS Enabled? n | Transport Method: tls | |
| Q-SIP? n | | |
| IP Video? n | Enforce SIPS URI for SRTP? n | |
| Peer Detection Enabled? y Peer Server: SM | | |
| Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? y | | |
| Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? n | | |
| Alert Incoming SIP Crisis Calls? n | | |
| Near-end Node Name: procr | Far-end Node Name: sm70vmpg | |
| Near-end Listen Port: 5061 | Far-end Listen Port: 5061 | |
| Far-end Network Region: 1 | | |
| Far-end Domain: devconnect.local | | |
| 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? n | |
| Enable Layer 3 Test? y | IP Audio Hairpinning? n | |
| Alternate Route Timer(sec): 6 | | |

Configure the **Trunk Group** form as shown below. This trunk group is used for calls to and from Communications Portal. 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 21 | |
| TRUNK GROUP | | | |
| Group Number: 1 | Group Type: sip | CDR Reports: y | |
| Group Name: SIP TRK | COR: 1 | TN: 1 | TAC: *11 |
| Direction: two-way | Outgoing Display? y | Night Service: | |
| Dial Access? n | | | |
| Queue Length: 0 | | | |
| Service Type: tie | Auth Code? n | | |
| | | Member Assignment Method: auto | |
| | | Signaling Group: 1 | |
| | | Number of Members: 10 | |

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 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 **600** was used.

| | | | |
|---|------------------------|--|--|
| change trunk-group 1 | | Page 2 of 21 | |
| 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): 600 | | | |
| Disconnect Supervision - In? y Out? y | | | |
| XOIP Treatment: auto | | Delay Call Setup When Accessed Via IGAR? n | |

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 21 |
| 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 | |

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

| | |
|---|------------------------|
| change trunk-group 1 | Page 4 of 21 |
| PROTOCOL VARIATIONS | |
| | Mark Users as Phone? n |
| Prepend '+' to Calling/Alerting/Diverting/Connected Number? n | |
| Send Transferring Party Information? y | |
| Network Call Redirection? y | |
| Build Refer-To URI of REFER From Contact For NCR? n | |
| Send Diversion Header? n | |
| Support Request History? y | |
| Telephone Event Payload Type: 101 | |
| Convert 180 to 183 for Early Media? n | |
| Always Use re-INVITE for Display Updates? n | |
| 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 | |

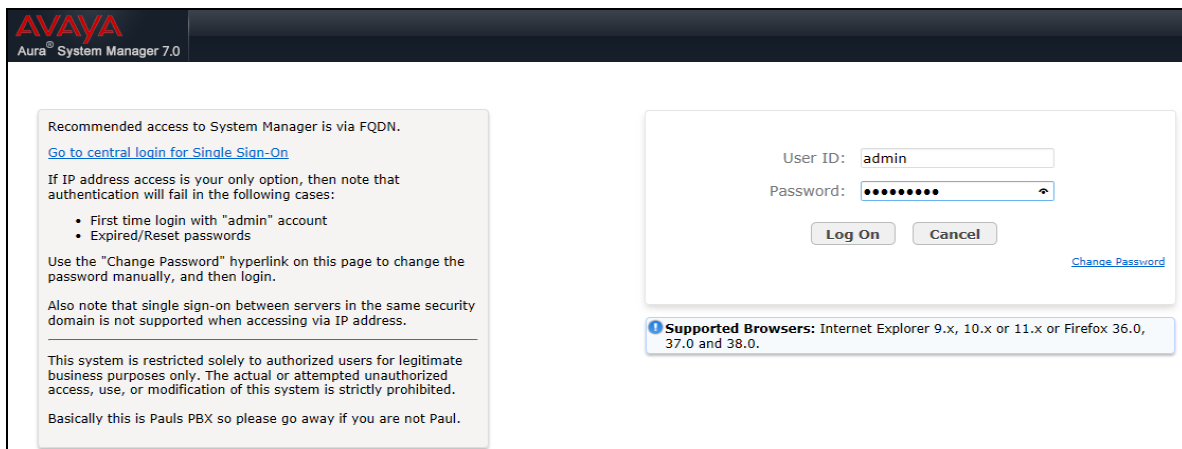
6. Configure Avaya Aura® Session Manager

This section provides the procedures for configuring Session Manager. Session Manager is configured using a web browser connecting to System Manager. The procedures include the following areas:

- Log in to Avaya Aura® System Manager.
- Display configured SIP Domain.
- Configure SIP Entities.
- Configure Routing Policies.
- Configure Dial Patterns.

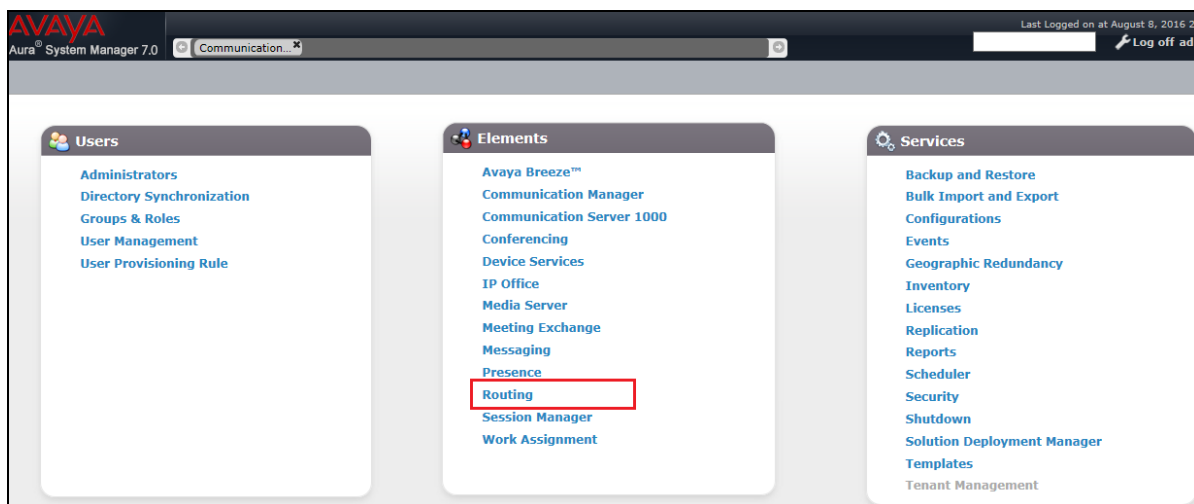
6.1. Log in to Avaya Aura® System Manager

Access the System Manager using a web browser by entering **http://<FQDN>/SMGR**, where **<FQDN>** is the fully qualified domain name of System Manager or **http://<IP Address>/SMGR**. Log in using appropriate credentials.



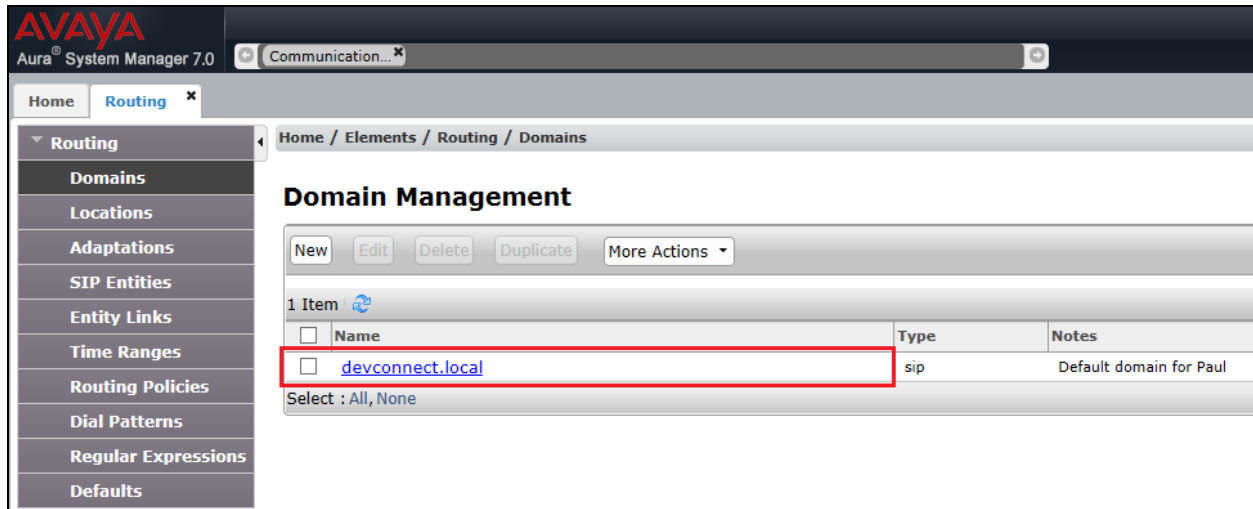
The screenshot shows the Avaya Aura System Manager 7.0 login page. The header includes the Avaya logo and 'Aura System Manager 7.0'. The main content area is divided into two sections. The left section contains instructions for recommended access via FQDN, a link to 'Go to central login for Single Sign-On', and a note about IP address access. It lists cases where authentication might fail: 'First time login with "admin" account' and 'Expired/Reset passwords'. It also provides a 'Change Password' link and a disclaimer about single sign-on. The right section is the login form, featuring 'User ID' (admin) and 'Password' (masked with dots) fields, 'Log On' and 'Cancel' buttons, and a 'Change Password' link. A 'Supported Browsers' banner at the bottom right lists Internet Explorer 9.x, 10.x, 11.x, and Firefox 36.0, 37.0, and 38.0.

Once logged in click on **Routing** as highlighted.



6.2. Display configured SIP Domain

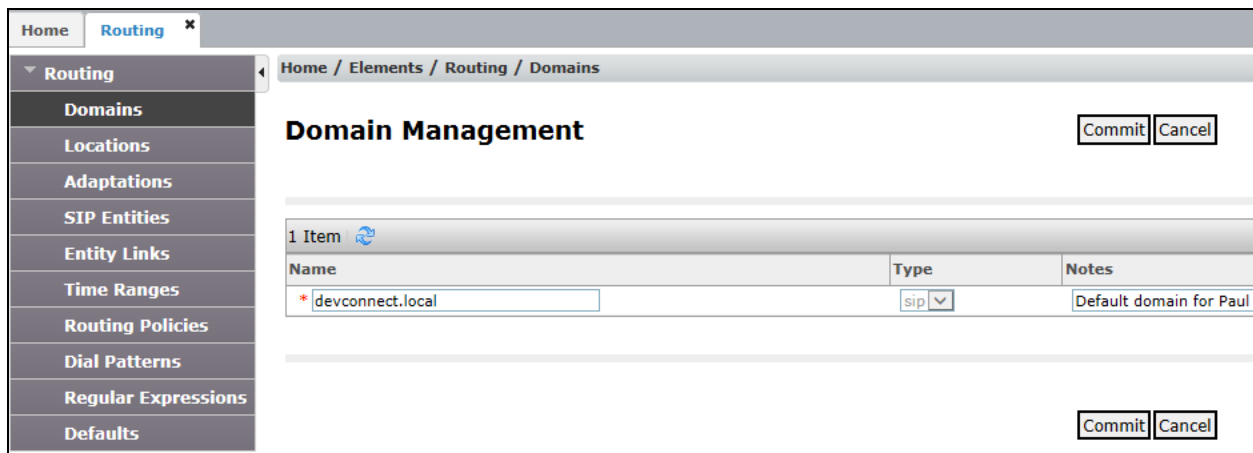
Click on **Domains** in the left window. For compliance testing a domain had already been previously added called **devconnect.local**, this is displayed below and if there is not a domain already configured click on **New**.



The screenshot shows the Avaya Aura System Manager 7.0 interface. The left sidebar has a 'Routing' menu with 'Domains' selected. The main area is titled 'Domain Management' and shows a table with one item: 'devconnect.local'. The table has columns for Name, Type, and Notes. The 'Name' column contains 'devconnect.local', the 'Type' column contains 'sip', and the 'Notes' column contains 'Default domain for Paul'. A red box highlights the 'devconnect.local' entry in the table.

| Name | Type | Notes |
|------------------|------|-------------------------|
| devconnect.local | sip | Default domain for Paul |

If a new domain is to be added this should be entered as shown below. Click on **Commit** once done.

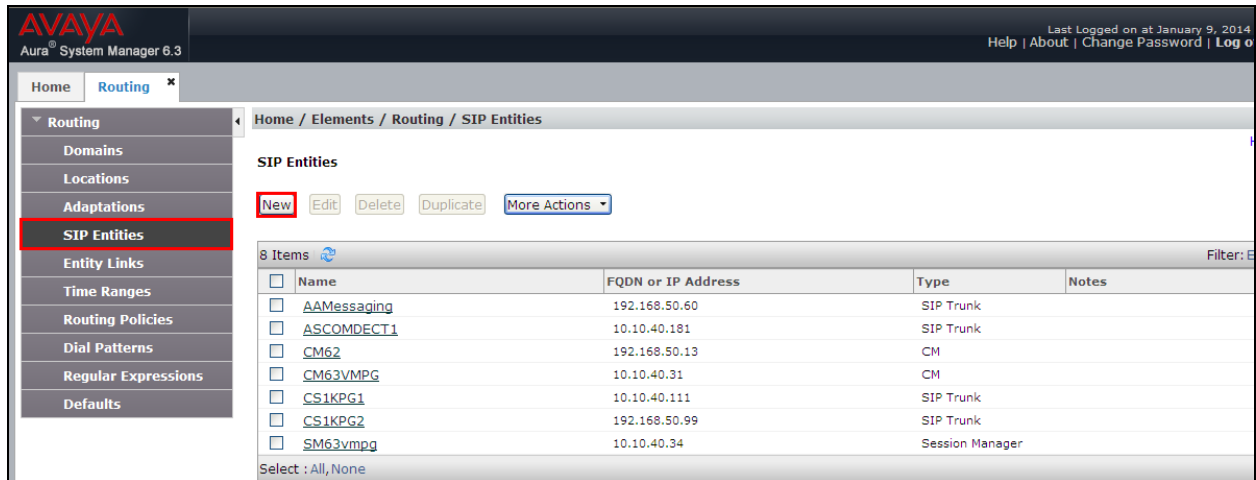


The screenshot shows the Avaya Aura System Manager 7.0 interface. The left sidebar has a 'Routing' menu with 'Domains' selected. The main area is titled 'Domain Management' and shows a form to add a new domain. The form has fields for Name, Type, and Notes. The 'Name' field contains 'devconnect.local', the 'Type' field contains 'sip', and the 'Notes' field contains 'Default domain for Paul'. There are 'Commit' and 'Cancel' buttons at the top right and bottom right of the form.

| Name | Type | Notes |
|------------------|------|-------------------------|
| devconnect.local | sip | Default domain for Paul |

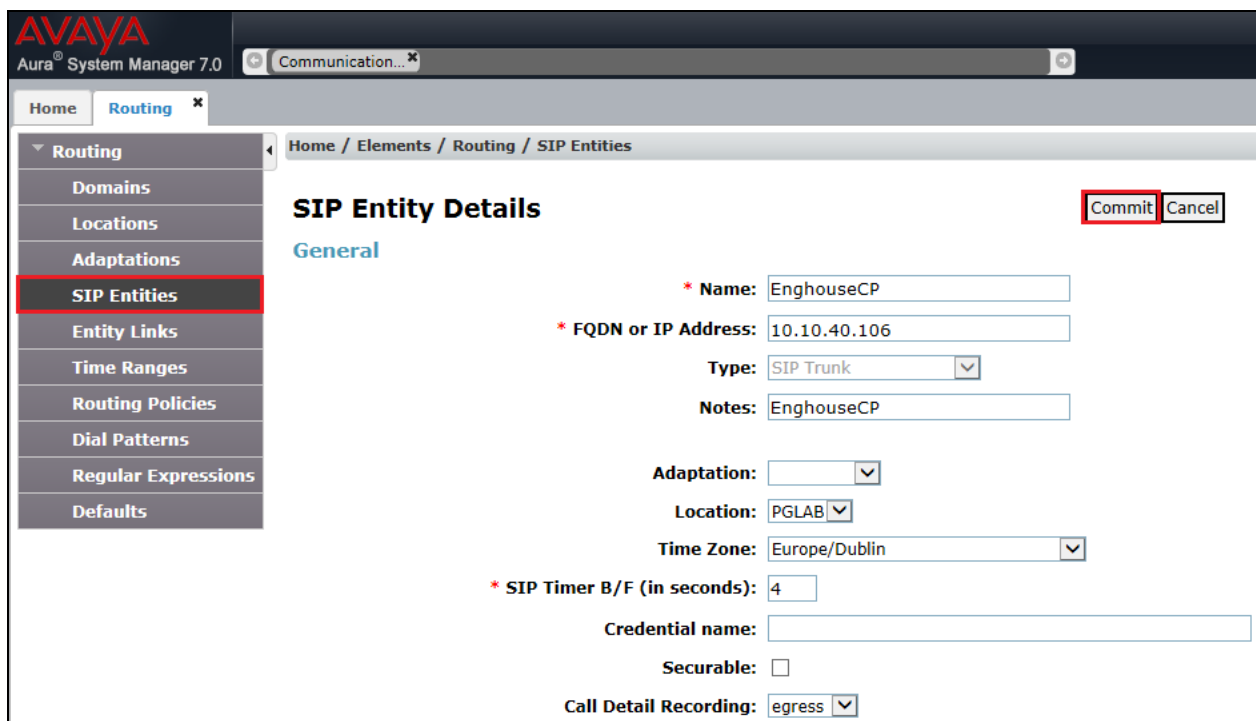
6.3. Configure SIP Entity for Enghouse Interactive Communications Portal

Select **SIP Entities** from the left window and click on **New** in the main window.



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

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.



6.4. Configure Entity Link for Enghouse Interactive Communications Portal

Select **Entity Link** from the left window and click on **New** in the main window.

AVAYA Aura System Manager 6.3

Home / Elements / Routing / Entity Links

Entity Links

New Edit Delete Duplicate More Actions

7 Items

| | Name | SIP Entity 1 | Protocol | Port | SIP Entity 2 | DNS Override | Port | Connection Policy | Deny New Service | Notes |
|--------------------------|----------------------------|--------------|----------|------|--------------|--------------------------|------|-------------------|--------------------------|-------|
| <input type="checkbox"/> | AAMessaging | SM63vmpg | TCP | 5060 | AAMessaging | <input type="checkbox"/> | 5060 | trusted | <input type="checkbox"/> | |
| <input type="checkbox"/> | ASCOMDECT1 | SM63vmpg | TCP | 5060 | ASCOMDECT1 | <input type="checkbox"/> | 5060 | trusted | <input type="checkbox"/> | |
| <input type="checkbox"/> | SM63vmpg_CM62_5061_TLS | SM63vmpg | TLS | 5061 | CM62 | <input type="checkbox"/> | 5061 | trusted | <input type="checkbox"/> | |
| <input type="checkbox"/> | SM63vmpg_CM63VMGP_5060_TCP | SM63vmpg | TCP | 5060 | CM63VMGP | <input type="checkbox"/> | 5060 | trusted | <input type="checkbox"/> | |

Select the correct **SIP Entity** that was created in **Section 6.3** and ensure that **TLS** is used as the **Protocol**. Note the **Port** is **5061**. Click on **Commit** once the information is entered correctly.

Entity Links

Commit Cancel

1 Item

| | Name | SIP Entity 1 | Protocol | Port | SIP Entity 2 | DNS Override | Port | Connection Policy | Notes |
|--------------------------|------------------|--------------|----------|--------|--------------|--------------------------|--------|-------------------|-------|
| <input type="checkbox"/> | * EnghouseCP_TLS | * sm70vmpg | TLS | * 5061 | * EnghouseCP | <input type="checkbox"/> | * 5061 | trusted | |

Select : All, None

6.5. Configure Routing Policy for Enghouse Interactive Communications Portal

Select **Routing Policies** from the left window and click on **New** in the main window.

AVAYA Aura System Manager 6.3

Home / Elements / Routing / Routing Policies

Routing Policies

New Edit Delete Duplicate More Actions

6 Items

| | Name | Disabled | Retries | Destination | Notes |
|--------------------------|------------|--------------------------|---------|-------------|-------|
| <input type="checkbox"/> | ToCM62 | <input type="checkbox"/> | 0 | CM62 | |
| <input type="checkbox"/> | ToCM63VMGP | <input type="checkbox"/> | 0 | CM63VMGP | |
| <input type="checkbox"/> | ToCS1KPG1 | <input type="checkbox"/> | 0 | CS1KPG1 | |
| <input type="checkbox"/> | ToCS1KPG2 | <input type="checkbox"/> | 0 | CS1KPG2 | |

Select : All, None

Enter a suitable **Name** and click on **Select** highlighted in order to associate this routing policy with a SIP Entity.

Home / Elements / Routing / Routing Policies

Routing Policy Details

General

* Name:

Disabled: ☐

* Retries:

Notes:

SIP Entity as Destination

Select

| Name | FQDN or IP Address | Type |
|------|--------------------|------|
| | | |

Commit Cancel

Select the **EnghouseCP** SIP Entity created in **Section 6.3** and click on **Commit** when done (not shown).

SIP Entities **Select** **Cancel**

SIP Entities

12 Items Filter: Enable

| | Name | FQDN or IP Address | Type | Notes |
|----------------------------------|------------------|--------------------|-----------------------|-----------------------|
| <input type="radio"/> | aacc64SIPvmppg | 10.10.40.55 | SIP Trunk | |
| <input type="radio"/> | AACC70vmppg | 10.10.40.80 | SIP Trunk | AACC70vmppg |
| <input type="radio"/> | AscomDECT_Master | 10.10.40.181 | Endpoint Concentrator | untrusted entity link |
| <input type="radio"/> | AscomDECT_Slave | 10.10.40.182 | Endpoint Concentrator | untrusted entity link |
| <input type="radio"/> | cm63vmppg | 10.10.40.31 | CM | R6.3 CM |
| <input type="radio"/> | cm70vmppg | 10.10.40.13 | CM | |
| <input type="radio"/> | CS1000E | 10.10.40.111 | Other | CS1KPG1 |
| <input checked="" type="radio"/> | EnghouseCP | 10.10.40.106 | SIP Trunk | EnghouseCP |
| <input type="radio"/> | Etrali_OT | 172.29.187.244 | SIP Trunk | |
| <input type="radio"/> | IPO500V2 | 10.10.40.20 | SIP Trunk | |
| <input type="radio"/> | messaging63vmppg | 10.10.40.22 | SIP Trunk | AA Messaging R6.3 |
| <input type="radio"/> | sm70vmppg | 10.10.40.12 | Session Manager | Sm100 IP |

Select : None

6.6. Configure Dial Pattern for Enghouse Interactive 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.

Avaya Aura System Manager 6.3

Home / Elements / Routing / Dial Patterns

Dial Patterns

New Edit Delete Duplicate More Actions

6 Items Filter:

| Pattern | Min | Max | Emergency Call | Emergency Type | Emergency Priority | SIP Domain | Notes |
|---------|-----|-----|--------------------------|----------------|--------------------|------------------|----------------|
| 10 | 4 | 4 | <input type="checkbox"/> | | | devconnect.local | |
| 2 | 4 | 4 | <input type="checkbox"/> | | | devconnect.local | CM63 |
| 30 | 4 | 4 | <input type="checkbox"/> | | | -ALL- | CS1KPG1 |
| 5999 | 4 | 5 | <input type="checkbox"/> | | | -ALL- | AURA_Messaging |
| 70 | 4 | 4 | <input type="checkbox"/> | | | devconnect.local | CS1KPG1 |

Select : All, None

Enter the number to be routed noting this will be the same number outlined in **Section 5.4**. Note the **SIP Domain** is that configured in **Section 6.2**. Click on **Add** to select the SIP Entity.

Dial Pattern Details

Commit Cancel

General

* Pattern: 620

* Min: 4

* Max: 4

Emergency Call: ☐

Emergency Priority: 1

Emergency Type:

SIP Domain: devconnect.local

Notes: To Enghouse

Originating Locations and Routing Policies

Add Remove

1 Item Filter: Enable

| Originating Location Name | Originating Location Notes | Routing Policy Name | Rank | Routing Policy Disabled | Routing Policy Destination | Routing Policy Notes |
|---------------------------|----------------------------|---------------------|------|-------------------------|----------------------------|----------------------|
| | | | | | | |

Select : All, None

Tick on the **Originating Location** as shown below and select the **Enghouse** Routing Policy. Click on **Select** once complete.

Originating Location
Select Cancel

Originating Location

☐ Apply The Selected Routing Policies to All Originating Locations

1 Item
Filter: Enable

| <input checked="" type="checkbox"/> | Name | Notes |
|-------------------------------------|-------|-----------|
| <input checked="" type="checkbox"/> | PGLAB | Pauls Lab |

Select : All, None

Routing Policies

9 Items
Filter: Enable

| <input type="checkbox"/> | Name | Disabled | Destination | Notes |
|-------------------------------------|-------------------|--------------------------|----------------|--------------------|
| <input type="checkbox"/> | To_aacc64SIPvmppg | <input type="checkbox"/> | aacc64SIPvmppg | aacc64SIPvmppg |
| <input type="checkbox"/> | To_AACC70vmppg | <input type="checkbox"/> | AACC70vmppg | To_AACC70vmppg |
| <input type="checkbox"/> | To_cm63vmppg | <input type="checkbox"/> | cm63vmppg | Routing to CM63 |
| <input type="checkbox"/> | To_cm70vmppg | <input type="checkbox"/> | cm70vmppg | |
| <input type="checkbox"/> | To_CS1000E | <input type="checkbox"/> | CS1000E | Routing to CS1KPG1 |
| <input checked="" type="checkbox"/> | To_EnghouseCP | <input type="checkbox"/> | EnghouseCP | |
| <input type="checkbox"/> | To Etrali | <input type="checkbox"/> | Etrali_OT | Etrali |
| <input type="checkbox"/> | To IPO500V2 | <input type="checkbox"/> | IPO500V2 | To IPO500V2 |

With the new Routing Policy in place, click on **Commit** as shown below.

Dial Pattern Details
Commit Cancel

General

* Pattern: 620

* Min: 4

* Max: 4

Emergency Call: ☐

Emergency Priority: 1

Emergency Type:

SIP Domain: devconnect.local

Notes: To Enghouse

Originating Locations and Routing Policies

Add Remove

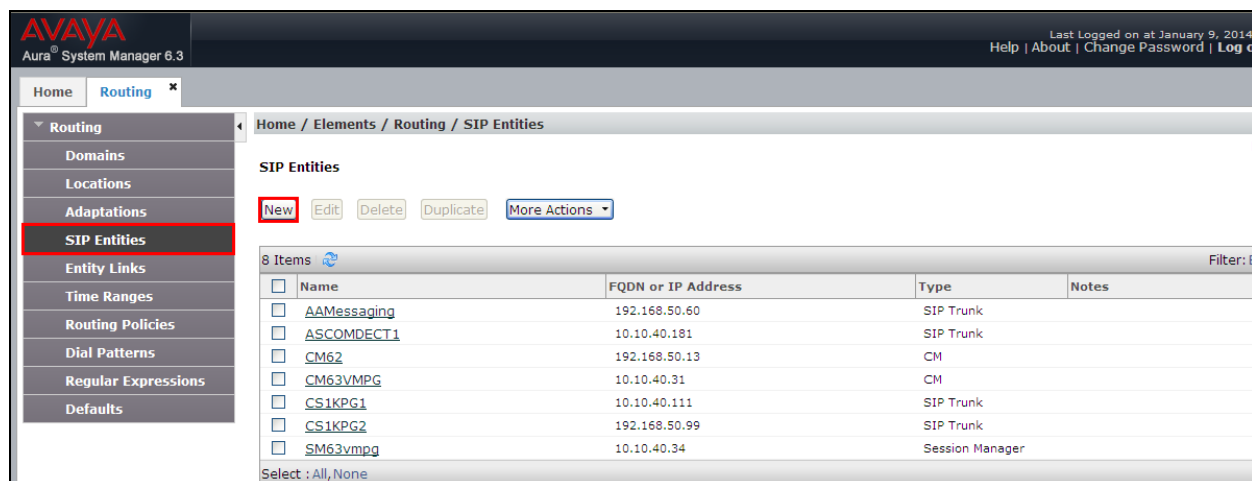
1 Item
Filter: Enable

| <input type="checkbox"/> | Originating Location Name | Originating Location Notes | Routing Policy Name | Rank | Routing Policy Disabled | Routing Policy Destination | Routing Policy Notes |
|--------------------------|---------------------------|----------------------------|---------------------|------|--------------------------|----------------------------|----------------------|
| <input type="checkbox"/> | PGLAB | Pauls Lab | To_EnghouseCP | 0 | <input type="checkbox"/> | EnghouseCP | |

Select : All, None

6.7. Configure Avaya Aura® Communication Manager SIP Entity

The following SIP Entity, SIP Entity Link, Routing Policy and Dial Pattern were already in place prior to compliance testing. The following sections are included to show an example of how to add these in the event they are not already present. Select **SIP Entities** from the left window and click on **New** in the main window.



Enter a suitable **Name** and ensure the **Location** and the correct **Time Zone** is entered. Click on **Commit** once all is entered correctly.

SIP Entity Details

General

Name: cm70vmpg

FQDN or IP Address: 10.10.40.13

Type: CM

Notes:

Adaptation:

Location: PGLAB

Time Zone: Europe/Dublin

SIP Timer B/F (in seconds): 4

Credential name:

Securable: ☐

Call Detail Recording: none

Commit **Cancel**

6.8. Configure Avaya Aura® Communication Manager Entity Link

Select **Entity Link** from the left window and click on **New** in the main window.

AVAYA
Aura® System Manager 6.3

Home / Elements / Routing / Entity Links

Entity Links

New Edit Delete Duplicate More Actions

7 Items Filter: Enable

| <input type="checkbox"/> | Name | SIP Entity 1 | Protocol | Port | SIP Entity 2 | DNS Override | Port | Connection Policy | Deny New Service | Notes |
|--------------------------|----------------------------|--------------|----------|------|--------------|--------------------------|------|-------------------|--------------------------|-------|
| <input type="checkbox"/> | AAMessaging | SM63vmpg | TCP | 5060 | AAMessaging | <input type="checkbox"/> | 5060 | trusted | <input type="checkbox"/> | |
| <input type="checkbox"/> | ASCOMDECT1 | SM63vmpg | TCP | 5060 | ASCOMDECT1 | <input type="checkbox"/> | 5060 | trusted | <input type="checkbox"/> | |
| <input type="checkbox"/> | SM63vmpg_CM62_5061_TLS | SM63vmpg | TLS | 5061 | CM62 | <input type="checkbox"/> | 5061 | trusted | <input type="checkbox"/> | |
| <input type="checkbox"/> | SM63vmpg_CM63VMPG_5060_TCP | SM63vmpg | TCP | 5060 | CM63VMPG | <input type="checkbox"/> | 5060 | trusted | <input type="checkbox"/> | |

Select the correct **SIP Entity** that was created in **Section 6.7** and ensure that **TLS** is used as the **Protocol**. Note the **Port** is **5061**. Click on **Commit** once entered correctly.

Entity Links

Commit Cancel

1 Item Filter: Enable

| <input type="checkbox"/> | Name | SIP Entity 1 | Protocol | Port | SIP Entity 2 | DNS Override | Port | Connection Policy |
|--------------------------|---------------|--------------|----------|-------|--------------|--------------------------|-------|-------------------|
| <input type="checkbox"/> | *CM70vmpg_TLS | *sm70vmpg | TLS | *5061 | *cm70vmpg | <input type="checkbox"/> | *5061 | trusted |

Select : All, None

6.9. Configure Avaya Aura® Communication Manager Routing Policy

Select **Routing Policies** from the left window and click on **New** in the main window.

AVAYA
Aura® System Manager 6.3

Home / Elements / Routing / Routing Policies

Routing Policies

New Edit Delete Duplicate More Actions

6 Items Filter: Enable

| <input type="checkbox"/> | Name | Disabled | Retries | Destination | Notes |
|--------------------------|------------|--------------------------|---------|-------------|-------|
| <input type="checkbox"/> | ToCM62 | <input type="checkbox"/> | 0 | CM62 | |
| <input type="checkbox"/> | ToCM63VMPG | <input type="checkbox"/> | 0 | CM63VMPG | |
| <input type="checkbox"/> | ToCS1KPG1 | <input type="checkbox"/> | 0 | CS1KPG1 | |
| <input type="checkbox"/> | ToCS1KPG2 | <input type="checkbox"/> | 0 | CS1KPG2 | |

Select : All, None

Enter a suitable **Name** and click on **Select** highlighted in order to associate this routing policy with a SIP Entity. Select the **Communication Manager** SIP Entity created in **Section 6.7** (not shown) and click on **Commit** when done.

Routing Policy Details

CommitCancel

General

* Name: To_cm70vmppg

Disabled: ☐

* Retries: 0

Notes:

SIP Entity as Destination

Select

| Name | FQDN or IP Address | Type | Notes |
|-----------|--------------------|------|-------|
| cm70vmppg | 10.10.40.13 | CM | |

6.10. Configure Avaya Aura® Communication Manager Dial Pattern

In order to route calls to Communication Manager 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 two dial patterns highlighted below were added in the same manner as outlined in **Section 6.6**.

Dial Patterns

NewEditDeleteDuplicateMore Actions

11 Items

Filter: Enable

| <input type="checkbox"/> | Pattern | Min | Max | Emergency Call | Emergency Type | Emergency Priority | SIP Domain | Notes |
|--------------------------|---------|-----|-----|--------------------------|----------------|--------------------|------------------|----------------------------|
| <input type="checkbox"/> | 10 | 4 | 4 | <input type="checkbox"/> | | | devconnect.local | Ext 10xx on CM63vmppg |
| <input type="checkbox"/> | 2016 | 4 | 4 | <input type="checkbox"/> | | | devconnect.local | SIP Trunk to CM63 |
| <input type="checkbox"/> | 3 | 4 | 4 | <input type="checkbox"/> | | | devconnect.local | To CS1000E |
| <input type="checkbox"/> | 51 | 4 | 4 | <input type="checkbox"/> | | | devconnect.local | To Etrali |
| <input type="checkbox"/> | 52 | 4 | 4 | <input type="checkbox"/> | | | devconnect.local | IP Office 500 V2 |
| <input type="checkbox"/> | 5999 | 4 | 4 | <input type="checkbox"/> | | | devconnect.local | Messaging (Voicemail) |
| <input type="checkbox"/> | 6000 | 4 | 4 | <input type="checkbox"/> | | | devconnect.local | aacc64SIPvmppg |
| <input type="checkbox"/> | 6111 | 4 | 4 | <input type="checkbox"/> | | | devconnect.local | aacc64SIPvmppg |
| <input type="checkbox"/> | 620 | 4 | 4 | <input type="checkbox"/> | | | devconnect.local | To Enghouse |
| <input type="checkbox"/> | 65 | 4 | 4 | <input type="checkbox"/> | | | devconnect.local | AACC70vmppg |
| <input type="checkbox"/> | Z | 4 | 4 | <input type="checkbox"/> | | | devconnect.local | cm70vmppg H.323 extensions |

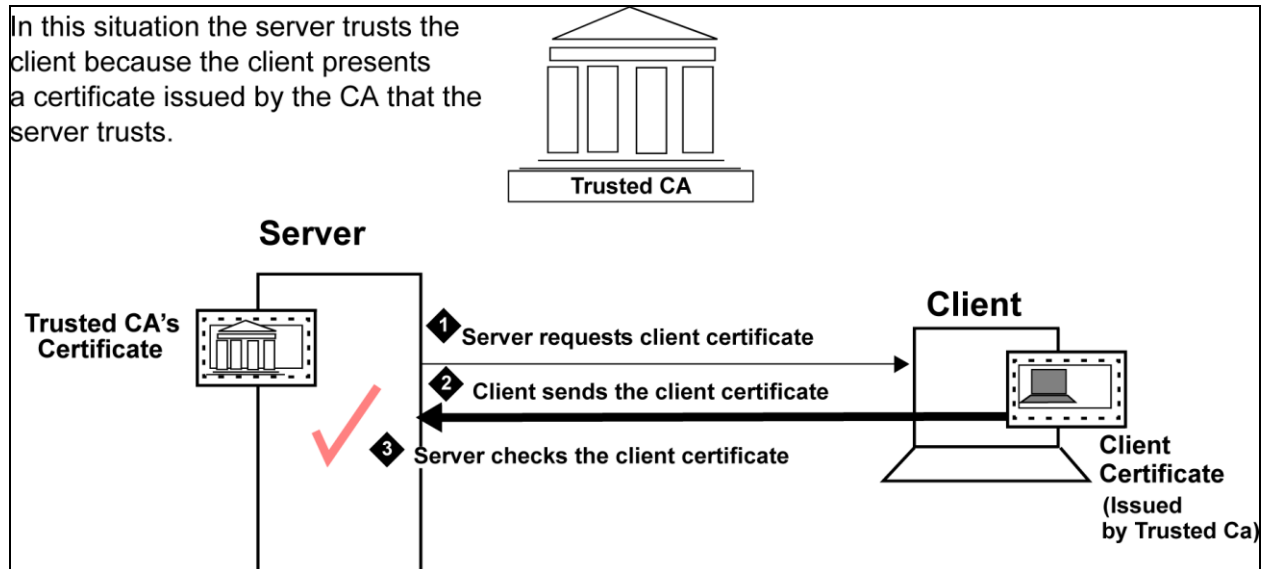
Select : All, None

7. TLS Management

Transport Layer Security (TLS) establishes unique cryptographically secure sessions for each connection request. When an entity (client) establishes a TLS session to a remote entity (server), TLS provides authentication, privacy and reliability. The following section describes TLS certificate installation so that clients authenticate servers or, optionally, servers authenticate clients.

Client authentication is similar to server authentication, except that the roles are reversed. The client authentication comes into play for encrypted connections with **mutual authentication**, and applies in addition to server authentication.

As shown below, the server also sends a request to the client for the client identity certificate, the client then sends its identity certificate to the server, and the server checks the received client identity certificate against the CA certificates that are saved in its trust store, to verify that the client identity certificate is indeed signed by a CA that the server trusts.



In the mutual authentication case, in addition to everything that was required for server authentication, the client must also have a client identity certificate created and signed by a trusted CA, and the server must have a copy of the CA certificate to be used in authenticating the client identity certificate.

In summary, the required additional manual procedures include:

- Avaya Aura® System Manager provides the third-party CA trusted Root Certificate. Install third-party CA trusted Root Certificate on Enghouse Communication Portal Server.
- Generate Certificate Signing Request and Private Key on Enghouse Communication Portal Server. Enghouse supplies a Certificate Signing Request (CSR) which is then signed by the Avaya Aura® System Manager Certificate Authority (CA).
- The resulting Identity Certificate is then installed on the Enghouse Communication Portal Server. Install the Third-Party Signed Identity Certificate into Enghouse Communication Portal Server.

Note: It is assumed the generating of the third-party CA trusted Root Certificate has been previously completed and is not discussed here. See the **Appendix** for the procedure for adding the Communication Portal Entity on the Certificate Authority and for generating the signed identity certificate.

8. Configuration of Enghouse Interactive Communications Portal 9.0

This section describes the steps required to configure Enghouse Interactive Communications Portal 10.1 to interoperate with Session Manager and Communication Manager. These steps include:

- Media Gateway Driver Configuration.
- Configuration file creation.
- Change Outbound Dial plan.
- Set the SIP transfer type parameter.
- Enable TLS and SRTP in the CTIC Media Gateway for SIP.

8.1. Media Gateway driver configuration

When using Media Gateway perform the following steps to modify the configuration parameters in the Media Gateway configuration files.

- Create the *avaya.xml* gateway configuration file.
- Change the outbound dial plan.
- Set the SIP transfer type parameter.

8.2. Create the *avaya.xml* gateway configuration file

To configure CP for this integration, prepare a gateway configuration file by performing the following steps.

- In the <Media Gateway install folder>\conf\sip_profiles\external folder, create a new text (.txt) file named *avaya.xml* with the following content. By default, Media Gateway is installed to C:\Program Files\Enghouse Interactive\Media Gateway.
- <include>
- <gateway name="AVAYA">
- Enter the IP address for Session Manager in the **realm** parameter value.
- <param name="realm" value="xxx.xxx.xxx.xxx"/>
- <param name="username" value="not-used"/>
- <param name="password" value="not-used"/>
- <param name="register" value="false"/>
- <param name="caller-id-in-from" value="false"/>
- <param name="register-transport" value="tcp"/>
- </gateway>
- </include>

8.3. Change the outbound dial plan

To configure CP for this integration, you must change the outbound dial plan configuration file by performing the following steps.

- In the <Media Gateway install folder>\conf\autoload_configs folder, edit the csdialplan.conf.xml file.
- Comment the following line: `<!-- <param pattern="^(.+@.+)$" value="sofia/external/$1"/> -->`
- Add the following line immediately below the line you commented: `<param pattern="^(.+@.+)$" value="sofia/gateway/AVAYA/$1"/>`
- Save the changes.

8.4. Set the SIP transfer type parameter

By default, the SIP transfer type is set to Refer. You must change transfer type to re-Invite with following steps.

- In the <Media Gateway install folder>\conf\autoload_configs folder, edit the csinterface.conf.xml file.
- Change the parameter `<param name="sip_transfer_type" value="refer"/>` to `<param name="sip_transfer_type" value="reinvite"/>`.
- Save the changes.

8.5. Enable TLS and SRTP in the CTIC Media Gateway for SIP

To enable TLS you need to generate a Cert Signing Request (CSR) and private key on the CP server system first.

- To do that open and update “openssl.cnf” file located in <Communications Portal install folder>\Tools\OpenSSL:

```
[ CA_default ]
default_md = sha256 # use public key default MD

[ req ]
default_md = sha256

[ req_distinguished_name ]
countryName = Country Name (2 letter code)
countryName_default = IE
countryName_min = 2
countryName_max = 2
stateOrProvinceName = State or Province Name (full name)
stateOrProvinceName_default = Connacht
localityName = Locality Name (eg, city)
localityName_default = Galway
organizationName = Organization Name (eg, company)
organizationName_default = Avaya
```

organizationalUnitName = Organizational Unit Name (eg, section)
organizationalUnitName_default = DEVCONNECT
commonName = Common Name (e.g. server FQDN or YOUR name)
commonName_default = ENGHOUSE2012CP

// Extensions to add to a certificate request
basicConstraints = CA:FALSE
keyUsage = nonRepudiation, digitalSignature, keyEncipherment, dataEncipherment,
keyAgreement
extendedKeyUsage = serverAuth, clientAuth
subjectAltName = @alt_names

[alt_names]
DNS.1 = smgr1bgvm.avaya.com

When it is asking use default values in [] by pressing ENTER.

- Use command prompt and open folder <Communications Portal install folder>\Tools\OpenSSL and enter following command:
openssl_scp.exe req -out ENGHOUSE2012CP.csr -new -newkey rsa:2048 -nodes -sha256 -keyout ENGHOUSE2012CP.key -config openssl.cnf
Cert Signing Request (CSR) .csr file and private key file are generated. CSR file then can be sent to Avaya which can make the Identity Certificate (.pem file).

- Manually concatenate your private key file, Identity Certificate file and Root Certificate Authority (provided by Avaya, too) file into “**tls.pem**” file. Copy that file into <Media Gateway install folder>\conf\ssl folder.
- In the <Media Gateway install folder>\conf folder, edit the vars.xml file. In the <!-- External SIP Profile --> section change the parameter
<X-PRE-PROCESS cmd="set" data="external_ssl_enable=false"/> to **<X-PRE-PROCESS cmd="set" data="external_ssl_enable=true"/>**
- In the <Media Gateway install folder>\conf\sip_profiles\external folder, edit avaya.xml file. Edit the parameter
<param name="register-transport" value="tcp"/> to **<param name="register-transport" value="tls"/>**

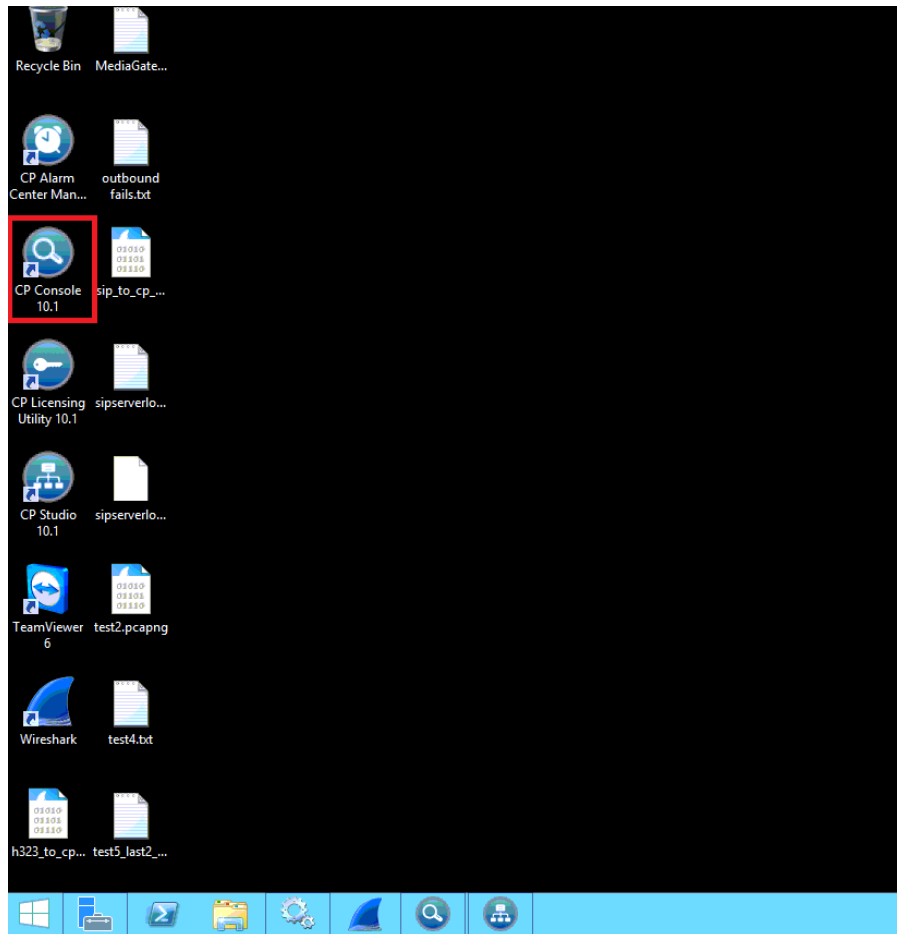
This completes the steps to set TLS with Media Gateway. To complete the Media Gateway configuration, SRTP has to be enabled too.

- In the <Media Gateway install folder>\conf\autoload_configs folder, edit the csdialplan.conf.xml file. Change the parameter:
<param pattern="^(.+@.+) \$" value="sofia/gateway/AVAYA/\$1"/> to **<param pattern="^(. @.) \$" value="**

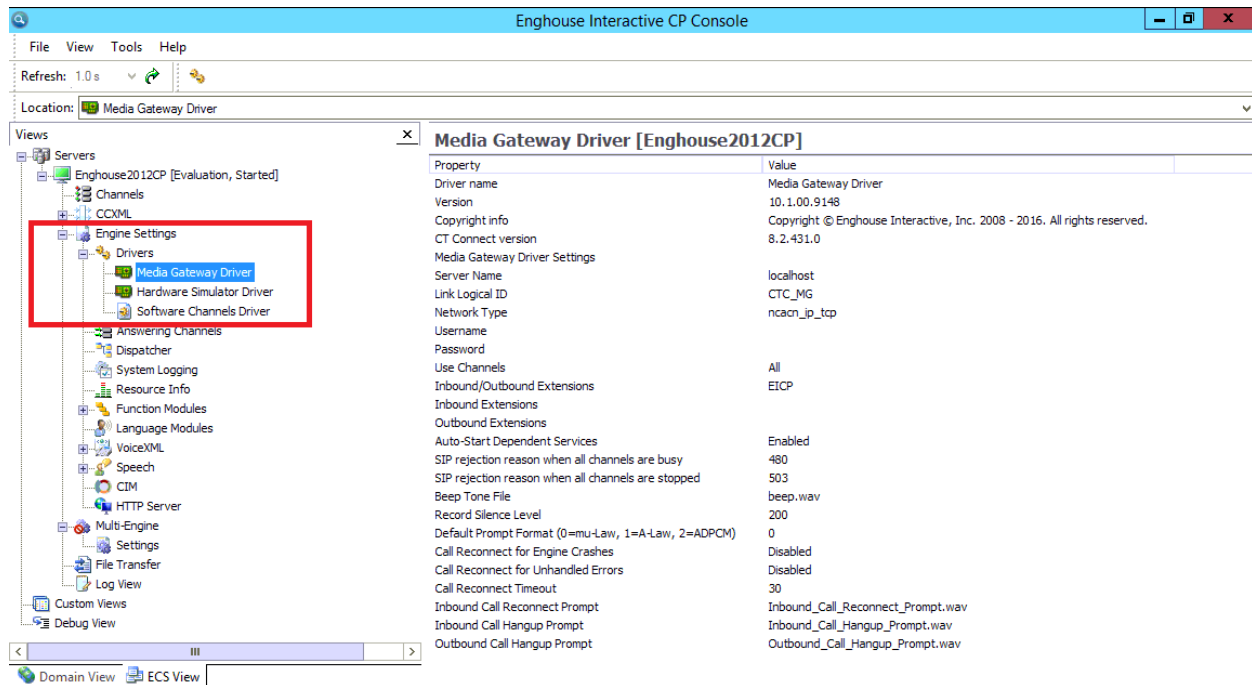
```
{sip_secure_media=true,rtp_secure_media=true:AES_CM_128_HMAC_SHA1_80,sdp_secure_savp_only=true} sofia/gateway/AVAYA/$1"/>
```

To complete the CP configuration, you must stop the CP engine, stop the Media Gateway service (if it is already started) and restart the CP Engine.

To configure the Media Gateway Driver open the **CP Console 9.0** by double clicking on the shortcut as shown below.



In the left window, navigate to **Servers** → [Server Name] → **Engine Settings** → **Drivers** → **Media Gateway Driver**.



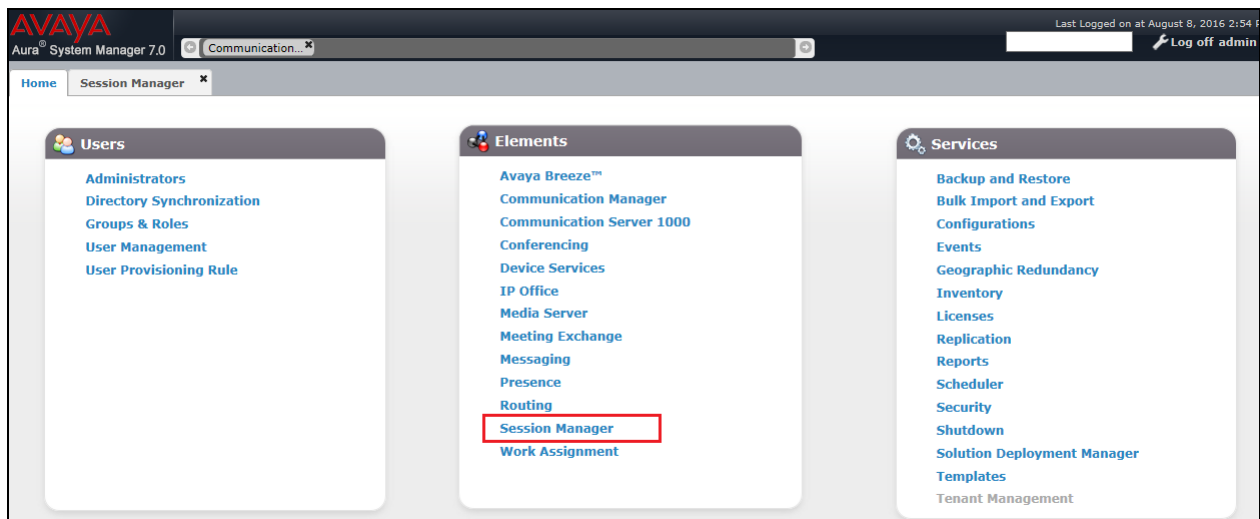
Please note that configuration of Communications Portal with regards to the setup of the IVR is outside the scope of these Application Notes, for more information on this setup please refer to **Section 11** of these Application Notes.

9. Verification Steps

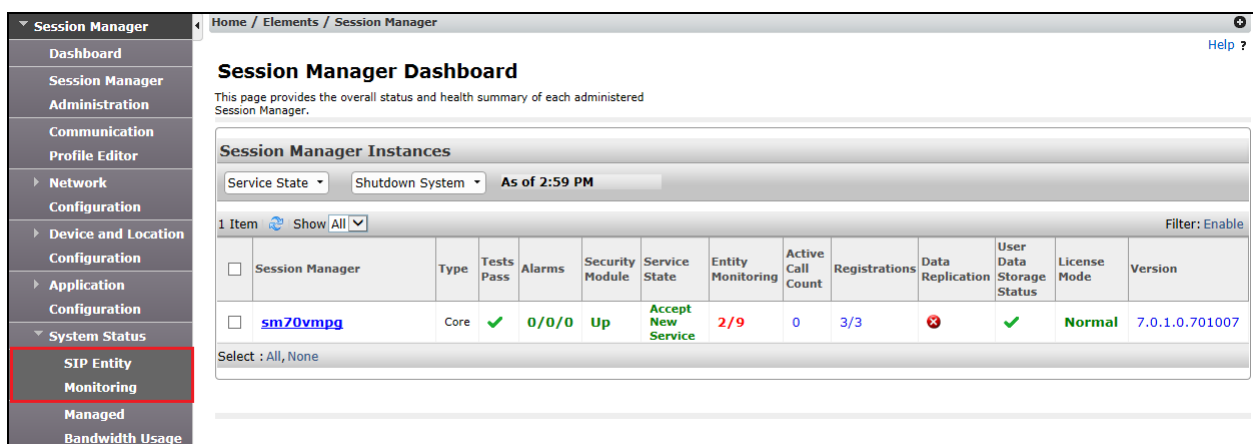
To verify a successful configuration of Enghouse Interactive Communications Portal and Session Manager/Communication Manager a call is placed from a Communication Manager telephone to the Communications Portal with the caller getting answered successfully hearing clear and audible speech.

9.1. Verify Enghouse Interactive Communications Portal SIP Entity is up

Log in to System Manager as per **Section 6.1**. From the main menu select Session Manager as shown below.



Navigate to **System Status** → **SIP Entity Monitoring**.



Select the **EnghouseCP** SIP Entity.

Application Configuration
System Status
SIP Entity Monitoring
Managed
Bandwidth Usage
Security Module Status
SIP Firewall Status
Registration Summary
User Registrations
Session Counts
User Data Storage
System Tools
Performance

| Session Manager | Type | Monitored Entities | | | | | Total |
|---|------|--------------------|--------------|----|---------------|------|-------|
| | | Down | Partially Up | Up | Not Monitored | Deny | |
| <input type="checkbox"/> sm70vmpq | Core | 2 | 1 | 6 | 0 | 0 | 9 |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |

Select: All, None

All Monitored SIP Entities

Run Monitor

9 Items | Refresh Filter: Enable

| SIP Entity Name |
|--|
| <input type="checkbox"/> messaging63vmpq |
| <input type="checkbox"/> cm63vmpq |
| <input type="checkbox"/> aacc64SIPvmpq |
| <input type="checkbox"/> AACC70vmpq |
| <input type="checkbox"/> Etrali_OT |
| <input checked="" type="checkbox"/> EnghouseCP |
| <input type="checkbox"/> cm70vmpq |
| <input type="checkbox"/> CS1000E |

Select: All, None < Previous | Page 1 of 2 | Next >

Note that both the **Conn. Status** and **Link Status** show **UP**.

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.

All Entity Links to SIP Entity: EnghouseCP

Summary View

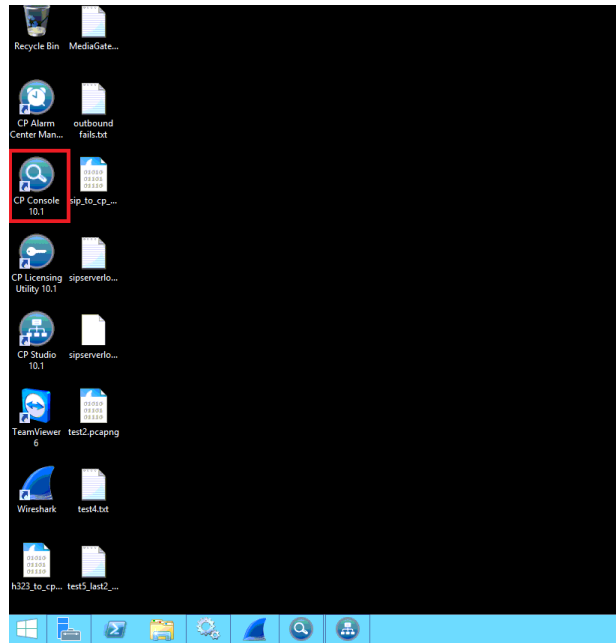
Status Details for the selected Session Manager:

1 Items | Refresh Filter: Enable

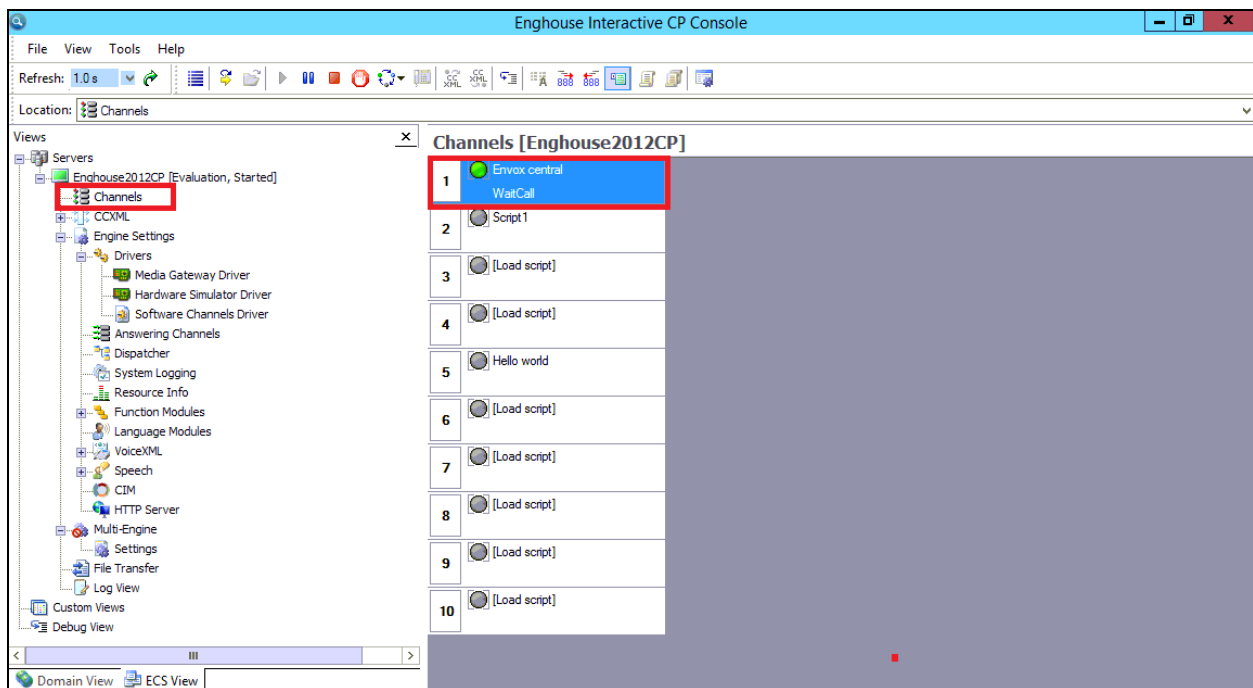
| Session Manager Name | SIP Entity Resolved IP | Port | Proto. | Deny | Conn. Status | Reason Code | Link Status |
|--|------------------------|------|--------|-------|--------------|-------------|-------------|
| <input type="radio"/> sm70vmpq | 10.10.40.106 | 5061 | TLS | FALSE | UP | 200 OK | UP |

9.2. Verify Enghouse Interactive Communications Portal IVR script

Open the **CP Console 9.0** by double clicking on the shortcut as shown below.



Channel 1 below has the script **Envox Central** associated with it, this should also show as green.



10.Conclusion

These Application Notes describe the configuration steps required for Enghouse Interactive Communications Portal 10.1 to successfully interoperate with Avaya Aura® Session Manager R7.0 and Avaya Aura® Communication Manager R7.0. All feature functionality and serviceability test cases were completed successfully as outlined in **Section 2.2**.

11.Additional References

This section references the Avaya and Enghouse product documentation that are relevant to these Application Notes.

Product documentation for Avaya products may be found at <http://support.avaya.com>.

- [1] *Administering Avaya Aura® Communication Manager*, Document ID 03-300509
- [2] *Avaya Aura® Communication Manager Feature Description and Implementation*, Document ID 555-245-205
- [3] *Administering Avaya Aura® Session Manager*, Release 7.0, 03-603324

Product documentation for Enghouse Interactive Communications Portal can be obtained by visiting the following website, www.enghouseinteractive.com

Appendix

The following section shows the creation of the Enghouse Communications Portal End Entity on the 3rd party CA in order to sign the CSR generated by Communications Portal.

Add End Entity

The 3rd 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.

The screenshot shows the AVAYA Aura System Manager 7.0 login interface. On the left, there is a sidebar with recommended access instructions and security notices. On the right, there is a login form with fields for User ID (admin) and Password (masked with dots). Below the password field are 'Log On' and 'Cancel' buttons, and a 'Change Password' link. At the bottom, a blue box lists supported browsers: Internet Explorer 9.x, 10.x or 11.x or Firefox 36.0, 37.0 and 38.0.

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.

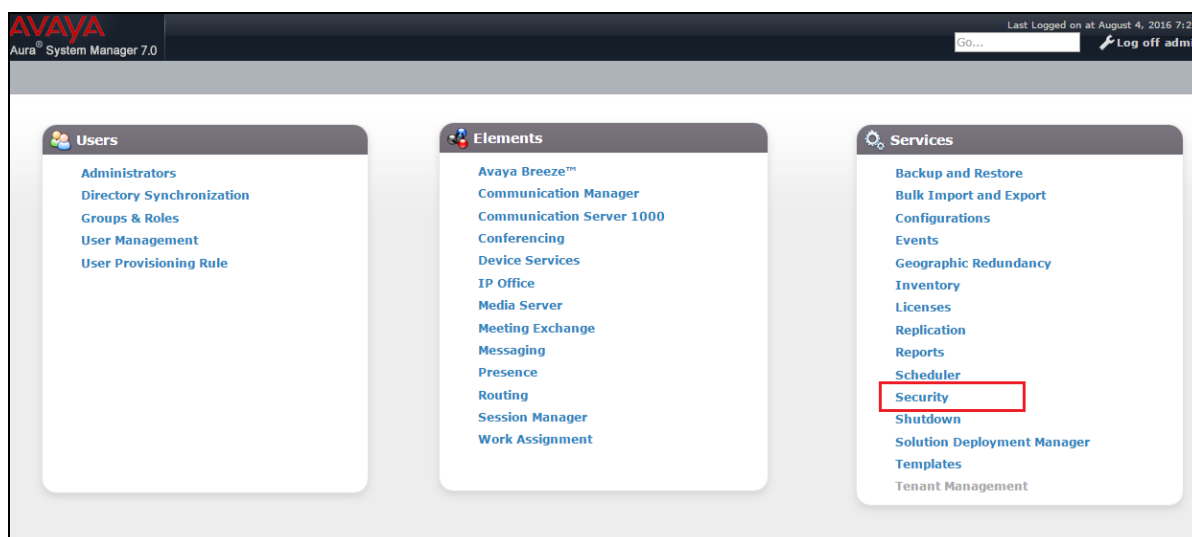
User ID:

Password:

[Change Password](#)

Supported Browsers: Internet Explorer 9.x, 10.x or 11.x or Firefox 36.0, 37.0 and 38.0.

Click on **Security** from the main menu.



Click on **Certificates**.

| Security | | |
|------------------------------|--|---|
| Sub Pages | | |
| Action | Description | Help |
| Certificates | Administer the Certificate Authority (CA) and set the Enrollment Password to provision certificates. | Certificate Authority and Enrollment Password |

Click on **Add End Entity**.

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

Welcome com.avaya.mgmt to EJBCA Administration.

Node hostname : gsscp-ca.avaya.com
Server time : 2016-08-08 14:08:38+01:00

CA health state [?]

| CA Name | CA Service | CRL Status |
|-------------|------------|------------|
| tmdefaultca | ✓ | ⚠ |

Publish queue status [?]

| Publisher | Length |
|------------------------|--------|
| No publishers defined. | |

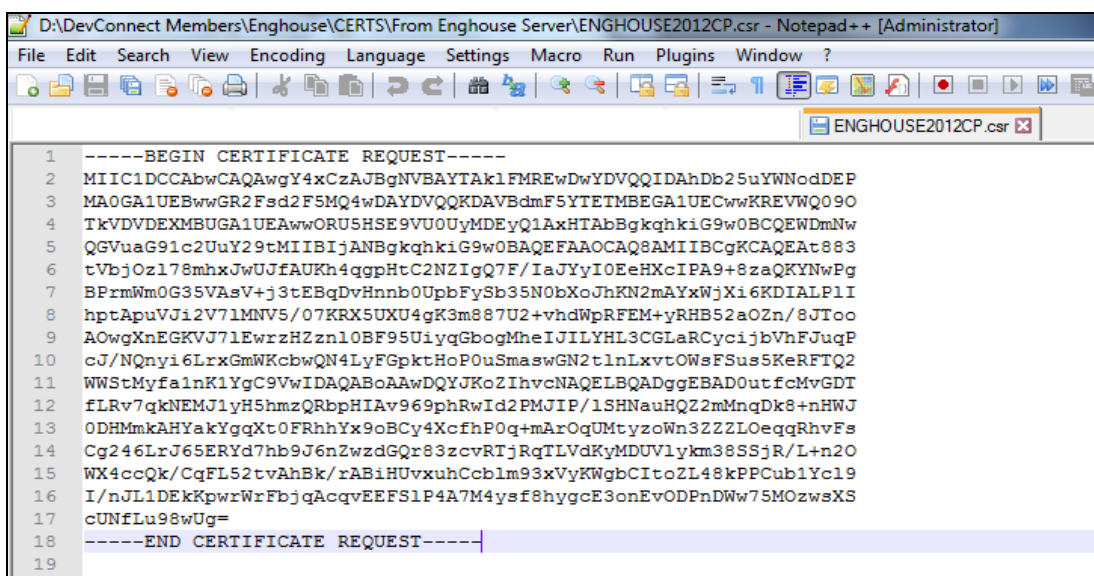
Made by PrimeKey Solutions AB, 2002–2014.

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 Enghouse Communications Portal and the **Common name** and **Username** should be hostname associated with the Enghouse Communications Portal. Click on **Save** once the information has been filled in correctly.

| End Entity | | Required |
|--|---|-------------------------------------|
| End Entity Profile GSSCP_TLS | | |
| Status | Generated ▼ | <input type="button" value="Save"/> |
| Username | ENGHOUSE2012CP | <input checked="" type="checkbox"/> |
| Password (or Enrollment Code) | | <input checked="" type="checkbox"/> |
| Confirm Password | | |
| Maximum number of failed login attempts | <input type="radio"/> <input type="text"/> <input checked="" type="radio"/> Unlimited | |
| Remaining login attempts | <input type="text"/> <input type="checkbox"/> Reset login attempts | |
| E-mail address | <input type="text"/> @ <input type="text"/> | <input type="checkbox"/> |
| Subject DN | | |
| CN, Common name | ENGHOUSE2012CP | <input checked="" type="checkbox"/> |
| CN, Common name | | <input type="checkbox"/> |
| O, Organization | Avaya | <input type="checkbox"/> |
| C, Country (ISO 3166) | IE | <input type="checkbox"/> |
| OU, Organizational Unit | DEVCONNECT | <input type="checkbox"/> |
| L, Locality | Galway | <input type="checkbox"/> |
| ST, State or Province | Connacht | <input type="checkbox"/> |
| Other subject attributes | | |
| Subject Alternative Name | | |
| DNS Name | | <input type="checkbox"/> |
| DNS Name | | <input type="checkbox"/> |
| IP Address | 10.10.40.106 | <input type="checkbox"/> |
| Main certificate data | | |
| Certificate Profile | GSSCP_ID ▼ | <input checked="" type="checkbox"/> |
| CA | tmdefaultca ▼ | <input checked="" type="checkbox"/> |
| Token | User Generated ▼ | <input checked="" type="checkbox"/> |
| <input type="button" value="Save"/> <input type="button" value="Close"/> | | |

Generate the certificate signing request

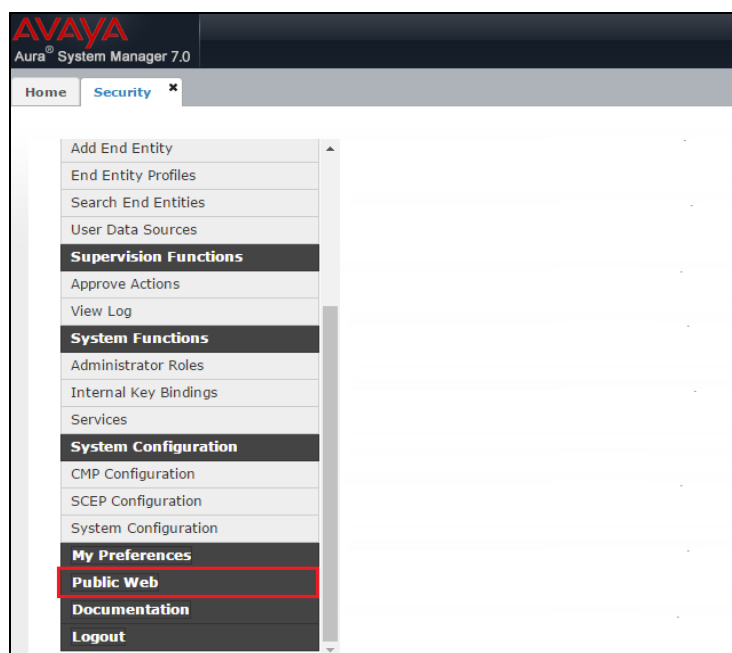
In public key infrastructure (PKI) systems, a certificate signing request (also CSR or certification request) is a message sent from an applicant to a certificate authority in order to apply for a digital identity certificate. The most common format for CSRs is the PKCS #10 specification and another is the Signed Public Key and Challenge Spkac format generated by some Web browsers. The 3rd party application will generate the CSR, the following is the CSR generated by Enghouse.



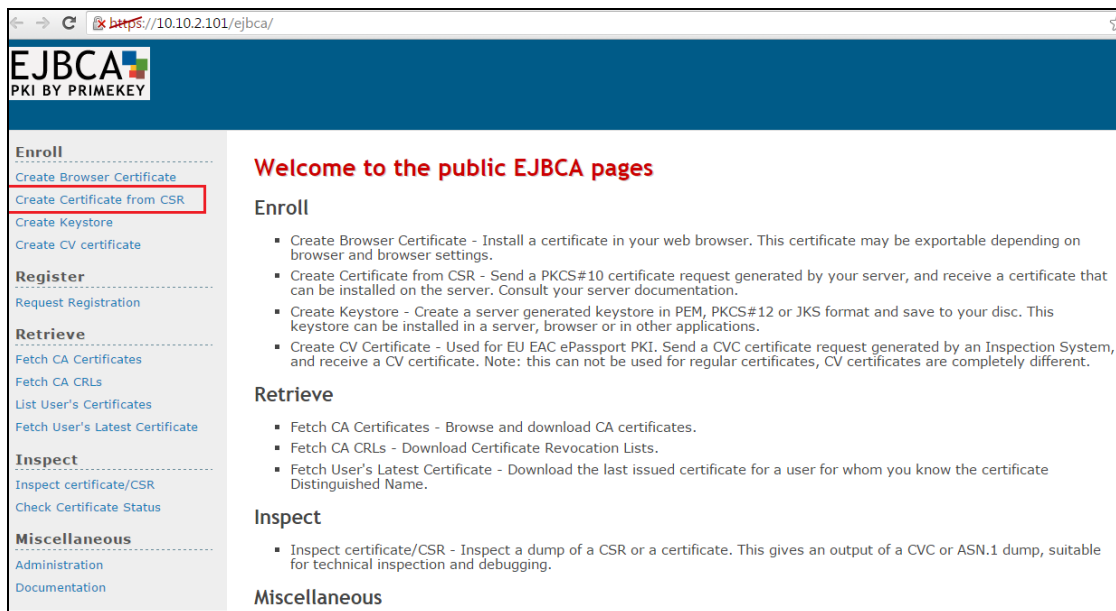
```
1 -----BEGIN CERTIFICATE REQUEST-----
2 MIIC1DCCAbwCAQAwY4xCzAJBgNVBAYTAk1FMREwDwYDVQQIDAhDb25uYWNodDEP
3 MA0GA1UEBwwGR2Fsd2F5MQ4wDAYDVQQKDAVBdmF5YETMBEGA1UECwwKREVWQ090
4 TkVDVDEXBmUGA1UEAwwORU5HSE9VU0UyMDEyYQ1AxHTAbBgkqhkiG9w0BCQEWDMNw
5 QGVuaG91c2UuY29tMIIIBjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAt883
6 tVbjOz178mhxJwUJfAUKh4qgpHtC2NZIqQ7F/IaJYyIOEeHXcIPA9+8zaQKYNwPg
7 BPrmWm0G35VasV+j3tEBqDvHnnb0UpbFySb35N0bXoJhKN2mAYxWjXi6KDIALP1I
8 hptApuVJi2V7LMNV5/07KRX5UXU4gK3m887U2+vhdWpRFEM+yRHB52aOZn/8JT0o
9 AOwgXnEGKVJ71EwrzH2zn10BF95UiyqGbogMheIJILYHL3CGLaRCycijbVhFJuqP
10 cJ/NQny16LrxGmWKcbwQN4LyFGpktHoP0uSmaswGN2tlnLxvtOWsFSus5KeRFTQ2
11 WWStMyfalnK1YgC9VwIDAQABAAwDQYJKoZIhvcNAQELBQADggEBAD0utfcMvGDT
12 fLRv7qkNEMJ1yH5hmzQRbpHIAv969phRwId2PMJIP/1SHNauHQZ2mMnqDk8+nHWJ
13 ODHmMkAHYakYgqXt0FRhhYx9oBCy4XcFhP0q+mArOgUMtyzoWn3ZZZLOeqqRhvFs
14 Cg246LrJ65ERYd7hb9J6nZwzdGQR83zcvtRTjRqTLVdKyMDUV1ykm38SSjR/L+n2O
15 WX4ccQk/CqFL52tvAhBk/rABiHUvxuhCcblm93xVyKWgbCitoZL48kPPCub1Yc19
16 I/nJL1DEkKpwrWrFbjqAcqvEEFS1P4A7M4ysf8hygcE3onEvODPnDWw75MOzwsXS
17 cUNfLu98wUg=
18 -----END CERTIFICATE REQUEST-----
19
```

Generate the Identity Certificate

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



The following web page is opened where a **Certificate from CSR** can be generated.



Copy and paste in the CSR request, this is taken from the CSR generated by Enghouse as shown on the previous page.

Certificate enrollment from a CSR

Please give your username and enrollment code, select a PEM- or DER-formatted certification request file (CSR) for upload, or paste a 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: No file chosen

or pasted request

```
TkYDVDEXMBUGA1UEAwORU5HSE9VU0UyMDEyQ1AxHTAbBqkqhkiG9w0BCQEWdmNw
QSVuaG91c2UyY29tMIIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBcGKCAQEAt883
tVbJ0z178mhxJwUJfAUkh4qgpHtC2N2IgQ7F/IaJYyIOEeHXcIPA9+8zaQKYNwPq
BPFmMm0G35VA5v+j3tEBGdVHnnb0UpbFy8b35N0bXoJhKN2mAYxWjXi6KDIALFLI
hptApuVJi2V7lMNV5/07KRX5UXU4gK3m887U2+yhdWpRFEM+yRHB52a02n/8JToc
AOwgXnEGKvJ7lEwrzH2zn10BF95UiyqGbgMheIJILYHL3CGLaRCyciibVhFJugP
cJ/NQnyi6LrxGmWKcbwQN4LyFGpktHoP0uSmaswGN2tlnLxvtOWeFSus5KeRFTQ2
WWSStMyfalnK1YgC9YwIDAQABoAAwDQYJKoZIhvcNAQELBQADggEBADOutfcMrGDT
fLRv7gkNEMJ1yH5hmzQRbpHIAv969phRwId2PMJIP/1SHNauHQ22mMngDk8+nHWJ
ODHMmAHYakYggXt0FRhhY9oBCy4XcfhP0q+mArOgUMtyzoWn3Z2ZLOeggRhVFs
Cq246LrJ65ERYd7hb9J6n2wzdGQr83zcvtRtRqTLVdKyMDUV1ykm3888jR/L+n2Q
WX4ccQk/CqFL52tvAhBk/rABiHUVxuhCobl93xVvKWgbCIt02L48kPFCub1Ycl9
I/nJLlDEkKpwrNrFbiqAcqvEEFS1F4A7M4ysf8hygcE3onEvODPnDww75MOzwsXs
cUNfLu98wUg=
-----END CERTIFICATE REQUEST-----
```

Result type:

Mutual Authentication

Mutual Authentication is determined in the Certificate Profile. Click on **Certificate Profiles** in the left window, this will display a list of profiles and edit the appropriate profile as shown below.

AVAYA
Aura® System Manager 7.0

Home Security

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

Manage Certificate Profiles

List of Certificate Profiles

| Name | Action |
|------------------|--|
| ENDUSER | <input type="button" value="Edit"/> <input type="button" value="Delete"/> <input type="button" value="Rename"/> <input type="button" value="Clone"/> |
| GSSCP_ID | <input type="button" value="Edit"/> <input type="button" value="Delete"/> <input type="button" value="Rename"/> <input type="button" value="Clone"/> |
| ID_CLIENT | <input type="button" value="Edit"/> <input type="button" value="Delete"/> <input type="button" value="Rename"/> <input type="button" value="Clone"/> |
| ID_CLIENT_SERVER | <input type="button" value="Edit"/> <input type="button" value="Delete"/> <input type="button" value="Rename"/> <input type="button" value="Clone"/> |
| ID_SERVER | <input type="button" value="Edit"/> <input type="button" value="Delete"/> <input type="button" value="Rename"/> <input type="button" value="Clone"/> |
| OCSPSIGNER | <input type="button" value="Edit"/> <input type="button" value="Delete"/> <input type="button" value="Rename"/> <input type="button" value="Clone"/> |
| ROOTCA | <input type="button" value="Edit"/> <input type="button" value="Delete"/> <input type="button" value="Rename"/> <input type="button" value="Clone"/> |
| SERVER | <input type="button" value="Edit"/> <input type="button" value="Delete"/> <input type="button" value="Rename"/> <input type="button" value="Clone"/> |
| SUBCA | <input type="button" value="Edit"/> <input type="button" value="Delete"/> <input type="button" value="Rename"/> <input type="button" value="Clone"/> |

Import/Export

Import Profiles from Zip file: No file chosen

The profile below shows that both Server and Client Authentication are selected.

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

Key Usage

☒ Digital Signature ☒ Data encipherment ☐ CRL sign

☒ Non-repudiation ☒ Key agreement ☐ Encipher only

☒ Key encipherment ☐ Key certificate sign ☐ Decipher only

☒ Use... ☐ Critical

Extended Key Usage [?]

Any Extended Key Usage

- ☒ Server Authentication
- ☒ Client Authentication
- Code Signing
- Email Protection
- 1.3.6.1.5.5.7.3.5
- 1.3.6.1.5.5.7.3.6
- 1.3.6.1.5.5.7.3.7
- Time Stamping
- OCSP Signer

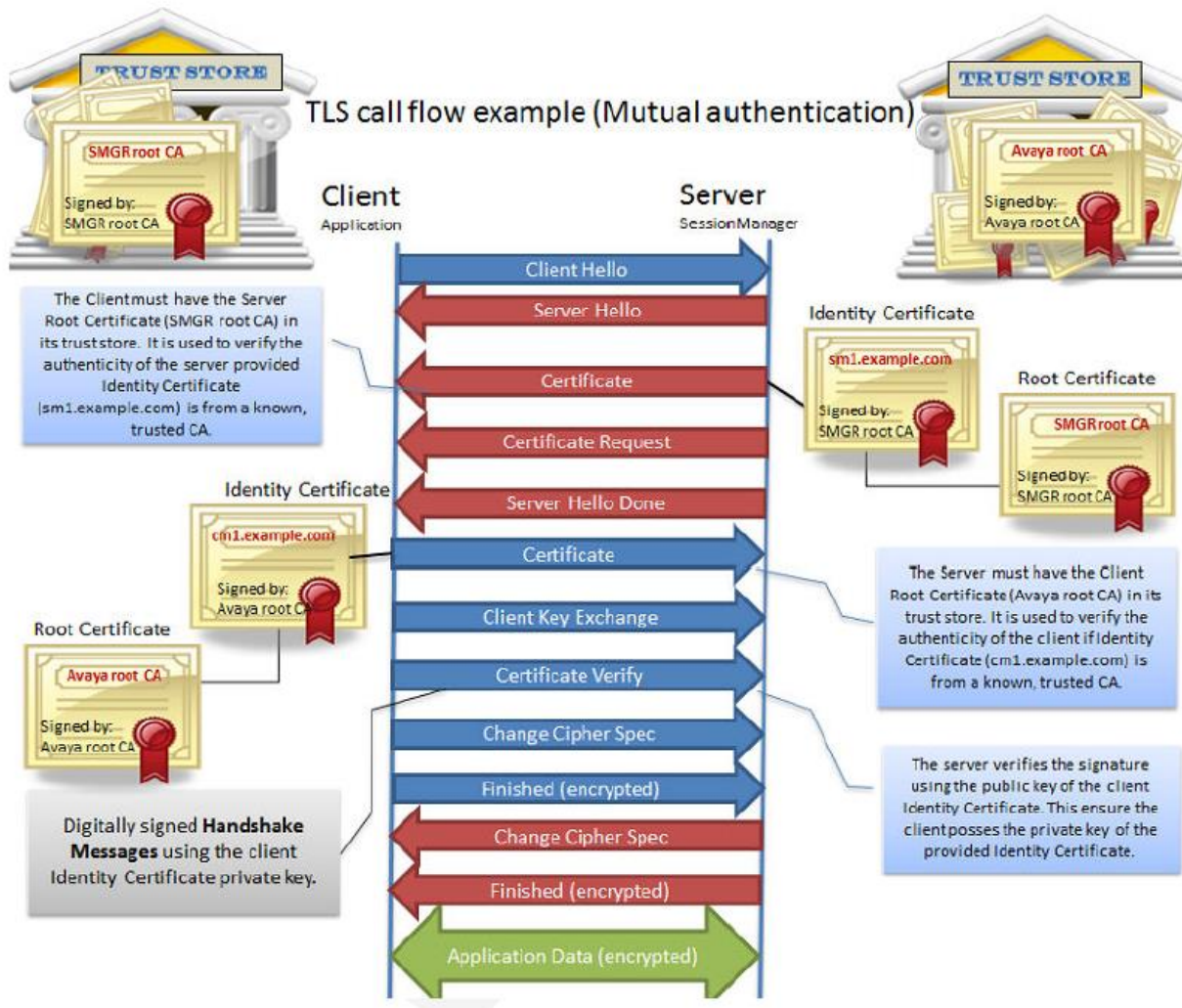
Subject Alternative Name ☒ Use... ☐ Critical

Issuer Alternative Name [?] ☒ Use... ☐ Critical

Subject Directory Attributes ☐ Use

Name Constraints [?] ☐ Use... ☐ Critical

The flow below show what happens in the Mutual Authentication scenario.



©2016 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.