



Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Convergys Voice Portal with Avaya Aura® Communication Manager and Avaya Aura® Session Manager via a SIP Trunking Interface – Issue 1.0

Abstract

The These Application Notes describe the procedures required for Convergys Voice Portal to successfully interoperate with Avaya Aura® Communication Manager and Avaya Aura® Session Manager using a SIP trunk.

Avaya SIP, H.323, and digital telephones were used to originate and terminate calls with User-to-User Information to and from the Convergys Voice Portal server. The overall objective of the interoperability compliance testing is to verify proper signaling and call establishment with the Convergys Voice Portal in an Avaya IP Telephony environment.

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

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

1. Introduction

These Application Notes describe the procedures required for Convergys Voice Portal to successfully interoperate with Avaya Aura® Communication Manager and Avaya Aura® Session Manager (SM) using a SIP trunk. Avaya SIP, H.323, and digital telephones were used to originate and terminate calls with User-to-User Information (UII) to and from the Convergys Voice Portal server. The overall objective of the interoperability compliance testing is to verify proper signaling and call establishment with the Convergys Voice Portal in an Avaya IP environment.

Convergys Voice Portal provides IVR and Messaging functionality via a SIP/VOIP telephony interface. Callers interact with the system via DTMF or Speech input, and may be transferred to agents, as needed.

These Application Notes assume that Communication Manager and Session Manager have already been installed and that basic configuration steps have been performed. Only steps relevant to the configuration used for compliance testing will be described in this document. For further details on configuration steps not covered in this document, consult references in **Section 10**.

2. General Test Approach and Test Results

This section describes the testing used to verify the interoperability of Convergys Voice Portal with the Avaya SIP infrastructure that consists of Communication Manager and Session Manager.

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 testing included feature and serviceability testing. The focus of the testing was primarily on verifying the SIP protocol messages between Session Manager and the Convergys Voice Portal server. The following features were exercised:

- Basic call between Convergys Voice Portal and various phone types including H322, SIP, digital and analog telephones
- Codecs G.711MU and G.729 with different payloads, including 10ms, 20ms and 30ms
- Blind, consult, and bridge transfer from Convergys Voice Portal to local, external and PSTN destinations
- DTMF RFC2833

- User-to-User Information (UUI) from and to Convergy's Voice Portal
- ANI/DNIS
- Response to OPTIONS message
- TLS/SRTP
- T.38 Fax
- Failover and load distribution

The serviceability testing included Communication Manager, Session Manager, and Convergy's Voice Portal failure scenarios to verify that Convergy's Voice Portal could properly recover from each failure.

2.2. Test Results

All test cases were executed and passed successfully with the following observations.

- The signaling group that is configured for the SIP trunk to call to/from Convergy's Voice Portal needs to have Video capability disabled in order for analog and digital telephones to have audio from the Convergy's Voice Portal.
- Convergy's Voice Portal does not provide ring back tone or music to a caller for Consult and Bridge transfers while destination phone is ringing.
- The IP address of the signaling interface of Session Manager needs to be used in the Common Name (CN) of Session Manager's certificate instead of the FQDN. This configuration is needed for TLS/SRTP to work in specific call scenarios such as Blind transfers because Convergy's Voice Portal authenticates caller based on the Contact header value prior to invoking the REFER transfer.
- The Convergy's Voice Portal supports crypto with encrypted SRTCP for secure media (SRTP) while Avaya IP telephones does not support this encryption. The recommendation is to use a secure media flow through the Avaya G450 Media Gateway or Avaya Aura® Media server (without shuffling the media) to have a secure media path with Convergy's Voice Portal.

2.3. Support

Technical support for the Convergy's Voice Portal can be obtained through the following:

- Phone: 800-955-4688
- Web: <http://www.convergys.com/realcare>

3. Reference Configuration

Figure 1 illustrates a sample configuration consisting of Avaya Aura® System Manager, Avaya Aura® Session Manager, Avaya Aura® Communication Manager, and Avaya Aura® Media Server running on Virtualized Environment. The Avaya G450 Media Gateway registers to Communication Manager and has PRI/T1 trunk to the PSTN. The Convergys Voice Portal system was built on one physical server using VMware; two VMs are built for two separate Convergys Voice Portals (IVRs).

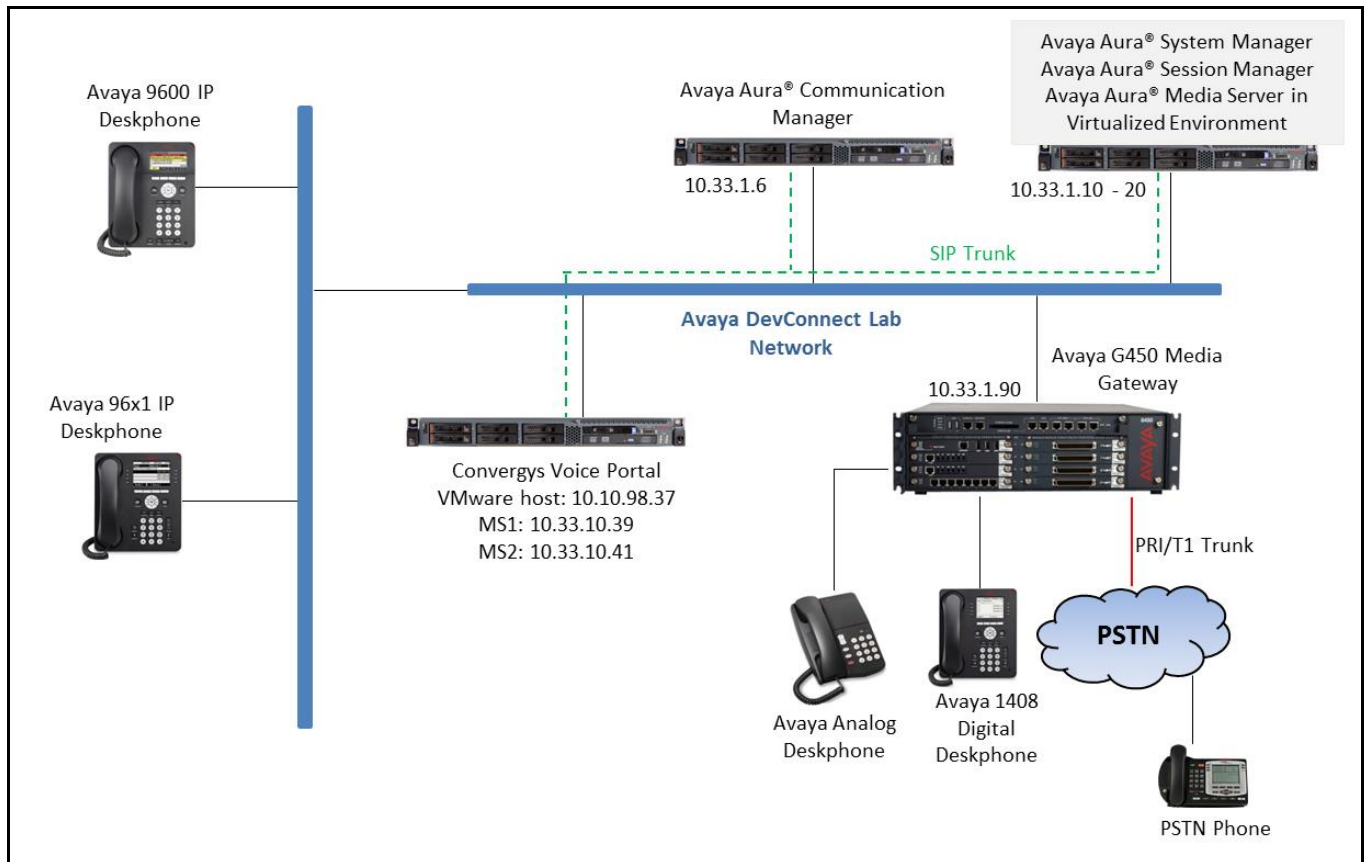


Figure 1: Test Configuration Diagram

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya Aura® Communication Manager running on Virtualized Environment	7.0.1.1.1-FP1SP1 R R017x.00.0.441.0
Avaya Aura® System Manager running on Virtualized Environment	7.0.1.1.065378 SP1
Avaya Aura® Session Manager running on Virtualized Environment	7.0.1.1.701114
Avaya Aura® Media Server running on Virtualized Environment	7.7.0.395
Avaya G450 Media Gateway	37.39.0
Avaya 96x1 Series IP Deskphone <ul style="list-style-type: none">• H323• SIP	Avaya one-X® Deskphone 6.6.29 Avaya one-X® Deskphone 7.0.1.2
Avaya 9600 Series IP Deskphone <ul style="list-style-type: none">• H323• SIP	Avaya one-X® Deskphone 3.25a Avaya one-X® Deskphone 2.6.9
Avaya 1408 Digital Telephone	-
Avaya Analog Telephone	-
Convergys Voice Portal running on Windows 2012R2 VM	IVP 10.0

5. Configure Avaya Aura® Communication Manager

This section describes the Communication Manager configuration required to interoperate with the Session Manager. It focuses on the configuration of the SIP trunk connecting Communication Manager and Session Manager. The configuration of the Communication Manager was performed using the System Access Terminal (SAT). After the completion of the configuration, perform a “save translation” command to make the changes permanent. The procedures for configuring Communication Manager include the following areas:

- Verify Communication Manager license
- Administer IP Node Names
- Administer IP network regions
- Administer IP codec set
- Administer SIP signaling group
- Administer SIP trunk group
- Administer route pattern
- Administer AAR analysis for routing calls to Session Manager

5.1. Verify Communication Manager License

Use the display **system-parameters customer-options** command to verify that the Communication Manager license has proper permissions for features illustrated in these Application Notes. Navigate to Page 2, and verify that there is sufficient remaining capacity for SIP trunks by comparing the Maximum Administered SIP Trunks field value with the corresponding value in the USED column.

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

display system-parameters customer-options		Page	2 of	12
OPTIONAL FEATURES				
IP PORT CAPACITIES		USED		
Maximum Administered H.323 Trunks:		12000	0	
Maximum Concurrently Registered IP Stations:		18000	4	
Maximum Administered Remote Office Trunks:		12000	0	
Maximum Concurrently Registered Remote Office Stations:		18000	0	
Maximum Concurrently Registered IP eCons:		128	0	
Max Concur Registered Unauthenticated H.323 Stations:		100	0	
Maximum Video Capable Stations:		36000	0	
Maximum Video Capable IP Softphones:		18000	5	
Maximum Administered SIP Trunks:		12000	38	
Maximum Administered Ad-hoc Video Conferencing Ports:		12000	0	
Maximum Number of DS1 Boards with Echo Cancellation:		522	0	

5.2. Administer IP Node Names

Use the **change node-names ip** command to administer a Name and IP Address for Session Manager. In the configuration used for compliance testing, the **procr** and **interopASM** nodes were utilized to administer a SIP trunk between Communication Manager and Session Manager.

change node-names ip		Page	1 of	2
IP NODE NAMES				
Name	IP Address			
AMS1	10.33.1.30			
CMS18	10.33.1.20			
aes70	10.33.1.4			
default	0.0.0.0			
interopASM	10.33.1.12			
lsp	10.33.1.17			
procr	10.33.1.6			
procr6	::			

5.3. Administer IP Network Region

This section describes the steps for administering an IP network region in Communication Manager for communication between Communication Manager and Session Manager. All IP endpoints were located in IP network region 1 using the parameters described below. Use the **change ip-network-region** command to view these settings. The example below shows the values used during compliance testing.

- The **Authoritative Domain** field was configured to match the domain name configured on Session Manager. In this configuration, the domain name is **bvwdev.com**. This name appears in the “From” header of SIP messages originating from this IP region.
- A descriptive name was entered for the **Name** field.
- IP-IP Direct Audio (Media Shuffling) was enabled to allow audio traffic to be sent directly between IP endpoints without using media resources in the Avaya Media Gateway. This was done for both intra-region and inter-region IP-IP Direct Audio. This is the default setting. Media Shuffling can be further restricted at the trunk level on the Signaling Group form.
- The **Codec Set** field was set to the IP codec set to be used for calls within this IP network region. In this case, IP codec set 1, configured in **Section 5.4**, was selected.
- The default values were used for all other fields.

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

5.4. Administer IP Codecs

Use the **change ip-codec-set** command to verify that G.711MU is contained in the codec list. The example below shows the value used for compliance testing. Note, codecs G.711MU and G.729A were tested during the compliance test. The “*best-effort*” is used in the **Encrypted SRTCP** field so that Communication Manager will be flexible in using either encrypted SRTCP or unencrypted SRTCP, depending on what kind of SRTCP is supported from other side.

change ip-codec-set 1

Page 1 of 2

IP CODEC SET

Codec Set: 1

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

Media Encryption

Encrypted SRTCP: best-effort

1:	1-srtp-aescm128-hmac80
2:	2-srtp-aescm128-hmac32
3:	none

5.5. Administer Signaling Group

For compliance testing, the signaling group shown below and the associated SIP trunk are used for routing calls to and from the Convergys Voice Portal server via Session Manager. Signaling group 1 was configured using the parameters highlighted below. All other fields were set as default.

- **Group Type** was set to *sip*.
- **Transport Method** was set to *tls*. As a result, **Near-end Listen Port** and **Far-end Listen Port** are automatically set to 5061.
- **IP Video** was set to **n**. Note that if IP Video was set to **y** the analog and digital phones have issue with audio.
- **Peer Detection Enabled** was set to **y**.
- **Near-end Node Name** was set to *procr*. Node names are defined in **Section 5.2** above.
- **Far-end Node Name** was set to **interopASM**. This node name maps to the IP address of the Session Manager as defined using the **change node-names ip** command.
- **Far-end Network Region** was set to **1**.
- **Direct IP-IP Audio Connections** was set to **y**. This field must be set to **y** to enable Media Shuffling on the trunk level.

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? n	Enforce SIPS URI for SRTP? y		
Peer Detection Enabled? n	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: interopASM		
Near-end Listen Port: 5061	Far-end Listen Port: 5061		
	Far-end Network Region: 1		
Far-end Domain: bvwdev.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? n		
Enable Layer 3 Test? y	Initial IP-IP Direct Media? n		
H.323 Station Outgoing Direct Media? n	Alternate Route Timer(sec): 6		

5.6. Administer Trunk Group

For compliance testing, trunk group 1 was used for the SIP trunk group for routing calls to and from the Convergys Voice Portal server via Session Manager. Trunk group 1 was configured using the parameters highlighted below.

On Page 1:

- **Group Type** field was set to *sip*.
- A descriptive name was entered for the **Group Name**.
- An available trunk access code (TAC) that was consistent with the existing dial plan was entered in the **TAC** field.
- **Service Type** field was set to *tie*.
- **Signaling Group** was set to the signaling group configured in the previous step.
- **Member Assignment method** was set to *auto*.
- **Signaling Group** was set to *1* (see **Section 5.5**).
- **The Number of Members** field contained the number of trunks in the SIP trunk group. It determines how many simultaneous SIP calls can be supported by the configuration.

change trunk-group 1		Page 1 of 21	
TRUNK GROUP			
Group Number: 1	Group Type: sip	CDR Reports: y	
Group Name: For-Private	COR: 1	TN: 1	TAC: #01
Direction: two-way	Outgoing Display? n	Night Service:	
Dial Access? n			
Queue Length: 0			
Service Type: tie	Auth Code? n	Member Assignment Method: auto	
		Signaling Group: 1	
		Number of Members: 14	

On Page 3:

- **Numbering Format** was set to *private*. This field specifies the format of the calling party number sent to the far-end.
- **UI Treatment** was set to *shared*.
- **Maximum Size of UI Contents** was set to *128*.
- Default values may be used for all other fields.

```
change trunk-group 1                                     Page 3 of 22

TRUNK FEATURES
    ACA Assignment? n                               Measured: none
                                                    Maintenance Tests? y

    Suppress # Outpulsing? n  Numbering Format: private
                                UI Treatment: shared
                                Maximum Size of UI Contents: 128
                                Replace Restricted Numbers? y
                                Replace Unavailable Numbers? y

                                Hold/Unhold Notifications? y
                                Modify Tandem Calling Number: no

                                Send UCID? n
    Show ANSWERED BY on Display? y
```

5.7. Administer Route Pattern

Use the **change route-pattern** command to create a route pattern that will route calls to the SIP trunk that connects Communication Manager to Session Manager.

The example below shows the route pattern used during compliance testing. A descriptive name was entered for the **Pattern Name** field. The **Grp No** field was set to the trunk group created in **Section 5.6**. The Facility Restriction Level (**FRL**) field was set to a level that allows access to this trunk for all users that require it. The value of *0* is the least restrictive level. **Numbering Format** was set to *lev0-pvt*. The default values were used for all other fields.

```
change route-pattern 1                                     Page 1 of 3
    Pattern Number: 1          Pattern Name: SIP-TLS-To-SM
    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
2:
3:
4:
5:
6:

    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 next
2: y y y y y n    n          rest          none
```

5.8. Administer Automatic Alternate Routing

Automatic Alternate Routing (AAR) was used to route calls to Convergys Voice Portal via Session Manager. Two places need to be changed to support this routing. First, use the **change dialplan analysis** command to create an entry in the dial plan. The example below shows entries previously created using the **change dialplan analysis** command. The 4th entry specifies that numbers that begin with 20 are of **Call Type aar**. Second, use the **change aar analysis** command to create an entry in the AAR Digit Analysis Table.

change dialplan analysis						Page 1 of 12		
DIAL PLAN ANALYSIS TABLE								
Location: all						Percent Full: 3		
Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type
1	4	ext	8	1	fac			
13	5	aar	9	1	fac			
14	5	aar	*	3	dac			
20	4	aar	#	3	dac			
23	5	aar						
24	5	aar						
28	5	aar						
30	4	aar						

The example below shows entries previously created using the **change aar analysis 2** command. The entry specifies that numbers that begin with **20** and are **4** digits long use route pattern **1**. Route pattern 1 routes calls to Session Manager.

change aar analysis 2							Page 1 of 2
AAR DIGIT ANALYSIS TABLE							
Location: all					Percent Full: 2		
	Dialed String	Total		Route	Call	Node	ANI
		Min	Max	Pattern	Type	Num	Reqd
20		4	4	1	aar		n
23		5	5	1	aar		n
24		5	5	1	aar		n
28		5	5	4	aar		n
3		4	4	1	unku		n

6. Configure Avaya Aura® Session Manager

This section provides the procedures for configuring Session Manager. Session Manager must be administered via System Manager.

The following sections assume that Session Manager and System Manager have been installed and that network connectivity exists between the two platforms.

The procedures described in this section include configurations in the following areas:

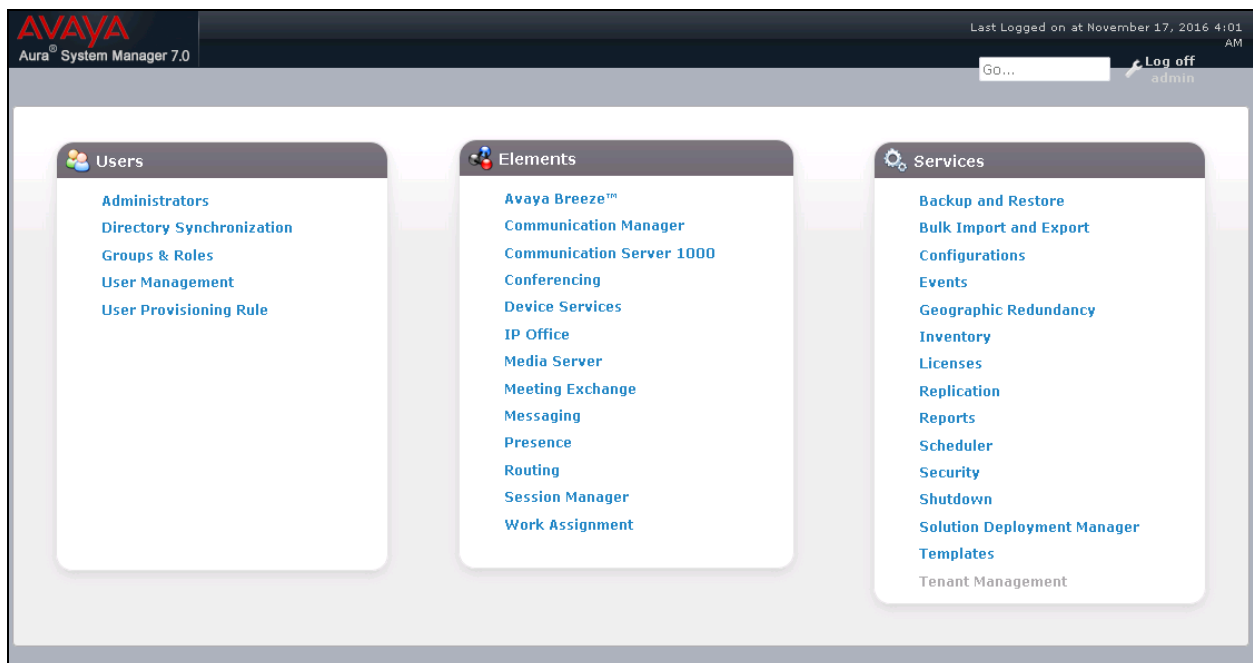
- Log in System Manager
- Administer SIP domain
- Administer logical/physical **Locations** where SIP Entities may reside
- Administer **SIP Entities** corresponding to the SIP telephony systems including Communication Manager, the Convergys Voice Portal server, and Session Manager itself
- Administer **Entity Links** which define the SIP trunk parameters used by Session Manager when routing calls to/from SIP Entities
- Administer **Routing Policies** which control call routing between the SIP Entities
- Administer **Dial Patterns** which govern to which SIP Entity a call is routed
- Information corresponding to the **Session Manager** server to be managed by System Manager

6.1. Log in System Manager

Access the System Manager Web interface by using the URL “https://ip-address” in an Internet browser window, where “ip-address” is the IP address of the System Manager server. Log in using the appropriate credentials.

The screenshot shows the Avaya Aura System Manager 7.0 login interface. On the left, there is a text box with instructions: "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." On the right, there is a login form with fields for "User ID:" (containing "admin") and "Password:" (masked with dots). Below the password field are "Log On" and "Cancel" buttons. A "Change Password" link is also present. At the bottom right, a blue box states: "Supported Browsers: Internet Explorer 9.x, 10.x or 11.x or Firefox 36.0, 37.0 and 38.0."

Click the **Elements** → **Routing** link. The sub-menus displayed in the left column (see picture in next section) will be used to configure the items in **Section 6.2-6.7**.



6.2. Administer SIP Domain

Add the SIP domain for which the communications infrastructure will be authoritative. Select **Domains** on the left and click the **New** button (not shown) on the right. Fill in the following:

- **Name:** Enter the domain name **bvwdev.com** which is specified to be the Authoritative Domain on the IP Network Region form on Communication Manager in **Section 5.3**
- **Type:** Select *sip*
- **Notes:** Descriptive text (optional)

Click **Commit**.

AVAYA
Aura® System Manager 7.0

Last Logged on at November 17, 2016 4:01 AM

Go... Log off admin

Home Routing

Home / Elements / Routing / Domains

Domain Management

Commit Cancel

1 Item Filter: Enable

Name	Type	Notes
* bvwdev.com	sip	SIP Domain

Commit Cancel

6.3. Administer Locations

Locations can be used to identify logical and/or physical locations where SIP Entities reside for purposes of routing and bandwidth management. To add a location, select **Locations** on the left and click on the **New** button (not shown) on the right. Fill in the following:

Under **General**:

- **Name:** A descriptive name
- **Notes:** Descriptive text (optional)

The remaining fields under **General** can be filled in to specify bandwidth management parameters between Session Manager and this location. The default values were used for compliance testing.

Next, fill in the following.

Under **Location Pattern**:

IP Address Pattern: An IP address pattern used to logically identify the location

Notes: Descriptive text (optional)

The screen below shows addition of the “10.33.1.*” subnet Location which includes the Communication Manager, Session Manager, and the Convergys Voice Portal server.

Click **Commit** to save the Location definition.

Aura System Manager 7.0 | Home / Elements / Routing / Locations | Log off admin

Location Details [Commit] [Cancel] [Help ?]

General

* Name: BvwDevSIL

Notes:

Dial Plan Transparency in Survivable Mode

Enabled: ☐

Listed Directory Number:

Associated CM SIP Entity:

Overall Managed Bandwidth

Managed Bandwidth Units: Kbit/sec

Total Bandwidth:

Multimedia Bandwidth:

Audio Calls Can Take Multimedia Bandwidth: ☒

Per-Call Bandwidth Parameters

Maximum Multimedia Bandwidth (Intra-Location): 2000 Kbit/Sec

Maximum Multimedia Bandwidth (Inter-Location): 2000 Kbit/Sec

* Minimum Multimedia Bandwidth: 64 Kbit/Sec

* Default Audio Bandwidth: 80 Kbit/sec

Alarm Threshold

Overall Alarm Threshold: 80 %

Multimedia Alarm Threshold: 80 %

* Latency before Overall Alarm Trigger: 5 Minutes

* Latency before Multimedia Alarm Trigger: 5 Minutes

Location Pattern

Add Remove

4 Items Filter: Enable

IP Address Pattern	Notes
<input checked="" type="checkbox"/> * 10.33.1.*	Net 10.33.1.0 for Aura System

Select : All, None

[Commit] [Cancel]

6.4. Administer SIP Entity

A SIP Entity must be added for Session Manager and for each SIP telephony system connected to it, which includes Communication Manager and Convergy's Voice Portal.

To add a new SIP Entity, navigate to **Routing** → **SIP Entities** in the left navigation pane and click **New** button in the right pane (not shown).

In the **General** section, enter the following values. Use default values for all remaining fields:

- **Name:** Enter a descriptive name.
- **FQDN or IP Address:** Enter the FQDN or IP address of the SIP Entity that is used for SIP signaling.
- **Type:** Select *Session Manager* for Session Manager, *CM* for Communication Manager and *SIP Trunk* for the Convergy's Voice Portal.
- **Location:** Select the location defined in **Section Error! Reference source not found.**
- **Time Zone:** Select the time zone for the location above.

The following screen shows the addition of Session Manager SIP Entity. The IP address of the Session Manager signaling interface is entered for **FQDN or IP Address**

The screenshot displays the Avaya Aura System Manager 7.0 web interface. The top navigation bar includes the Avaya logo, 'Aura System Manager 7.0', and a 'Last Logged on at November 17, 2016 11:03 AM' status. The left sidebar shows a navigation menu with 'Routing' selected. The main content area is titled 'SIP Entity Details' and contains a 'General' section with the following fields: 'Name' (ASM70A), 'FQDN or IP Address' (10.33.1.12), 'Type' (Session Manager), 'Location' (BvwDevSIL), 'Outbound Proxy', 'Time Zone' (America/Toronto), and 'Credential name'. Below the 'General' section is the 'SIP Link Monitoring' section, which includes a 'SIP Link Monitoring' dropdown set to 'Use Session Manager Configuration'. Buttons for 'Commit' and 'Cancel' are visible in the top right of the form area.

To define the ports used by Session Manager, scroll down to the **Port** section of the **SIP Entity Details** screen. This section is only present for the **Session Manager** SIP Entity.

In the **Port** section, click **Add** and enter following values. Use default values for all remaining fields:

- **Listen Ports:** Port number on which the Session Manager can listen for SIP requests.

- **Protocol:** Transport protocol to be used to receive SIP requests.
- **Default Domain:** The domain used for the enterprise.

Defaults can be used for the remaining fields. Click **Commit** to save (not shown).

The compliance test used **Listen Ports** entry **5061** with **TLS** for connecting to Communication Manager and **5060** with **TCP** for connecting to the Convergys Voice Portal.

Listen Ports

TCP Failover port:
TLS Failover port:

Add Remove

6 Items Filter: [Enable](#)

<input type="checkbox"/>	Listen Ports	Protocol	Default Domain	Endpoint	Notes
<input type="checkbox"/>	<input type="text" value="5060"/>	TCP	<input type="text" value="bvwddev.com"/>	<input checked="" type="checkbox"/>	<input type="text"/>
<input type="checkbox"/>	<input type="text" value="5060"/>	UDP	<input type="text" value="bvwddev.com"/>	<input checked="" type="checkbox"/>	<input type="text"/>
<input type="checkbox"/>	<input type="text" value="5061"/>	TLS	<input type="text" value="bvwddev.com"/>	<input checked="" type="checkbox"/>	<input type="text"/>
<input type="checkbox"/>	<input type="text" value="5062"/>	TLS	<input type="text" value="bvwddev.com"/>	<input type="checkbox"/>	<input type="text"/>
<input type="checkbox"/>	<input type="text" value="5067"/>	TLS	<input type="text" value="bvwddev.com"/>	<input type="checkbox"/>	<input type="text"/>
<input type="checkbox"/>	<input type="text" value="5080"/>	TCP	<input type="text" value="bvwddev.com"/>	<input type="checkbox"/>	<input type="text"/>

Select : [All](#), [None](#)

The following screen shows the addition of the Communication Manager SIP Entity. In order for Session Manager to send SIP traffic on an entity link to Communication Manager, it is necessary to create a SIP Entity for Communication Manager. The **FQDN or IP Address** field is set to IP address of Communication Manager and **Type** to **CM**. The **Location** and **Time Zone** parameters are set as shown in screen below.

AVAYA
Aura® System Manager 7.0

Last Logged on at November 17, 2016 11:03 AM

GO... Log off admin

Home Routing

Home / Elements / Routing / SIP Entities

SIP Entity Details

Commit Cancel

Help ?

General

* Name: ACM-Trunk1-Private

* FQDN or IP Address: 10.33.1.6

Type: CM

Notes:

Adaptation:

Location: BvwDevSIL

Time Zone: America/Toronto

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

Credential name:

Securable: ☐

Call Detail Recording: ingress

Loop Detection

Loop Detection Mode: On

Loop Count Threshold: 5

Loop Detection Interval (in msec): 200

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

Supports Call Admission Control: ☐

Shared Bandwidth Manager: ☐

Primary Session Manager Bandwidth Association:

The following screen shows the addition of the SIP Entity for the Convergys Voice Portal. The **FQDN or IP Address** field is set to the IP address of the Convergys Voice Portal. Select **Type** as **SIP Trunk**. Select **SIP Link Monitoring** as **Link Monitoring Enabled** with the interval of **120** seconds. This setting allows Session Manager to send outbound OPTIONS heartbeat every **120** seconds to the Convergys Voice Portal to query the status of the SIP trunk.

AVAYA
Aura® System Manager 7.0

Last Logged on at November 17, 2016 11:03 AM
GO... Log off admin

Home Routing

Home / Elements / Routing / SIP Entities

SIP Entity Details Commit Cancel

General

* Name: Convergys_IVR

* FQDN or IP Address: 10.10.98.39

Type: SIP Trunk

Notes:

Adaptation:

Location: BywDevSIL

Time Zone: America/Toronto

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

Credential name:

Securable: ☐

Call Detail Recording: none

Loop Detection

Loop Detection Mode: On

Loop Count Threshold: 5

Loop Detection Interval (in msec): 200

SIP Link Monitoring

SIP Link Monitoring: Link Monitoring Enabled

* Proactive Monitoring Interval (in seconds): 120

* Reactive Monitoring Interval (in seconds): 120

* Number of Tries: 1

6.5. Administer Entity Links

A SIP trunk between Session Manager and a telephony system is described by an Entity link. In the configuration used for compliance testing, two Entity Links were configured; one for Session Manager to Communication Manager and one for Session Manager to the Convergys Voice Portal server.

To add an Entity Link, select **Entity Links** on the left and click on the **New** button (not shown) on the right. For the link to Communication Manager, fill in the following fields in the new row that is displayed:

- **Name:** A descriptive name
- **SIP Entity 1:** Select the Session Manager SIP Entity configured in previous step
- **Protocol:** Select “TLS”
- **Port:** Port number to which the other system sends SIP requests
- **SIP Entity 2:** Select the Communication Manager SIP Entity configured in previous step
- **Port:** Port number on which the other system receives SIP requests
- **Trusted:** Select “trusted”

Click **Commit** to save the configuration.

The screen below shows the first **Entity Link** configured between Session Manager and Communication Manager.

AVAYA
Aura® System Manager 7.0

Last Logged on at November 17, 2016 11:03 AM

GO... Log off admin

Home Routing

Home / Elements / Routing / Entity Links

Entity Links

Commit Cancel

1 Item Filter: Enable

Name	SIP Entity 1	Protocol	Port	SIP Entity 2
*ASM70_ACM_Trunk1_50	*ASM70A	TLS	*5061	*ACM-Trunk1-Private

Select : All, None

The second **Entity Link** between Session Manager and the Convergy's Voice Portal server is similarly configured. The screen below shows the configured Entity Link. Select “TCP” for the **Protocol**, 5060 for each **Port**, and the Convergy's Voice Portal server SIP Entity for **SIP Entity 2**.

AVAYA
Aura® System Manager 7.0

Last Logged on at November 17, 2016 11:03 AM

GO... Log off admin

Home Routing

Home / Elements / Routing / Entity Links

Entity Links

Commit Cancel

1 Item Filter: Enable

Name	SIP Entity 1	Protocol	Port	SIP Entity 2
*ASM70A_Convergys_IVR	*ASM70A	TCP	*5060	*Convergys_IVR

Select : All, None

6.6. Administer Routing Policies

A routing policy should be created for each “Routing Destination”. A routing policy must be added for routing calls to Communication Manager (from the Convergys Voice Portal server). Likewise, a routing policy must be added for routing calls to the Convergys Voice Portal server (from Communication Manager).

To add a routing policy, select **Routing Policies** on the left and click on the **New** button (not shown) on the right. The following screen is displayed. Fill in the following:

In the **General** section, configure the following fields:

- **Name:** Enter a descriptive name.
- **Notes:** Add a brief description (optional).

In **SIP Entity as Destination** section, click **Select**. The **SIP Entity List** page opens (not shown). Select the appropriate SIP entity to which this routing policy applies and click **Select**. The selected SIP Entity is displayed in the **Routing Policy Details** page as shown below. Use default values for remaining fields. Click **Commit** to save.

The following screen shows the Routing Policy used for routing calls from the Convergys Voice Portal server to Communication Manager.

AVAYA
Aura® System Manager 7.0

Last Logged on at November 17, 2016 11:03 AM
GO... Log off admin

Home Routing

Routing
Domains
Locations
Adaptations
SIP Entities
Entity Links
Time Ranges
Routing Policies
Dial Patterns
Regular Expressions
Defaults

Home / Elements / Routing / Routing Policies

Routing Policy Details

Commit Cancel

General

* Name: To-CM-Trunk1

Disabled: ☐

* Retries: 0

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
ACM-Trunk1-Private	10.33.1.6	CM	

The following screens show the Routing Policy for the Convergys Voice Portal.

The screenshot displays the Avaya Aura System Manager 7.0 web interface. The top header shows the Avaya logo and 'Aura® System Manager 7.0'. The user is logged in as 'admin' and the session expires at 11:03 AM on November 17, 2016. The left sidebar contains a navigation menu with options: Home, Routing (selected), Domains, Locations, Adaptations, SIP Entities, Entity Links, Time Ranges, Routing Policies (highlighted), Dial Patterns, Regular Expressions, and Defaults. The main content area is titled 'Routing Policy Details' and includes 'Commit' and 'Cancel' buttons. Under the 'General' tab, the 'Name' is 'To-Convergys', 'Disabled' is unchecked, 'Retries' is '0', and there is a 'Notes' field. Below this is the 'SIP Entity as Destination' section, which includes a 'Select' button and a table with the following data:

Name	FQDN or IP Address	Type	Notes
Convergys_IVR	10.10.98.39	SIP Trunk	

6.7. Administer Dial Patterns

A Dial Pattern is associated with a Routing Policy to direct calls to a destination based on dialed digits. To add a dial pattern, select **Dial Patterns** on the left and click on the **New** button (not shown) on the right. Fill in the following, as shown in the screens below:

Under General:

- **Pattern:** Dialed number or prefix
- **Min:** Minimum length of dialed number
- **Max:** Maximum length of dialed number
- **SIP Domain:** SIP domain specified in **Section 6.2** of this section, or ALL.
- **Notes:** Comment on purpose of dial pattern.

Under Originating Locations and Routing Policies:

Click **Add**, and then select the appropriate **Location** (or “ALL”) for Originating **Location Name** field and select the appropriate Routing Policy from the list.

Defaults can be used for the remaining fields. Click **Commit** to save the Dial Pattern.

The entry under **Originating Locations and Routing Policies** on the following screen shows the Dial Pattern defined for routing calls to Communication Manager. Any call made to a 4 digit number starting with “33” will be routed to Communication Manager.

AVAYA
Aura® System Manager 7.0

Last Logged on at November 17, 2016 11:03 AM

Home / Elements / Routing / Dial Patterns

Dial Pattern Details

Commit Cancel

General

* Pattern: 33

* Min: 4

* Max: 4

Emergency Call: ☐

Emergency Priority: 1

Emergency Type:

SIP Domain: bvwddev.com

Notes:

Originating Locations and Routing Policies

Add Remove

1 Item Filter: Enable

<input type="checkbox"/>	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	BvwDevSIL		To-CM-Trunk1	0	<input type="checkbox"/>	ACM-Trunk1-Private	

Select : All, None

The entry under **Originating Locations and Routing Policies** on the following screen shows the Dial Pattern defined for routing calls to the Convergys Voice Portal server. Any call made to a 4 digit number starting with “20” will be routed to the Convergys Voice Portal server.

AVAYA
Aura® System Manager 7.0

Last Logged on at November 17, 2016 11:03 AM
Go... Log off admin

Home Routing

Home / Elements / Routing / Dial Patterns

Dial Pattern Details

Commit Cancel

General

* Pattern: 20

* Min: 4

* Max: 4

Emergency Call: ☐

Emergency Priority: 1

Emergency Type:

SIP Domain: bvwddev.com

Notes:

Originating Locations and Routing Policies

Add Remove

1 Item Filter: Enable

<input type="checkbox"/>	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	BvwDevSIL		To-Convergys	0	<input type="checkbox"/>	Convergys_IVR	

Select : All, None

6.8. Administer Session Manager

The creation of a Session Manager element provides the linkage between System Manager and Session Manager. This is most likely done as part of the initial Session Manager installation. To add a Session Manager, navigate to **Home → Elements → Session Manager → Session Manager Administration** in the left navigation pane and click **New** button in the right pane (not shown). If the Session Manager Instance already exists, click **View** (not shown) to view the configuration. Enter/verify the data as described below and shown in the following screen:

In the **General** section, configure the following fields:

- **SIP Entity Name:** Select the SIP Entity created for Session Manager.
- **Description:** Add a brief description (optional).
- **Management Access Point Host Name/IP:** Enter the IP address of the Session Manager management interface.
- **Directs Routing to Endpoints:** Enabled, to enable call routing on the Session Manager.

In the **Security Module** section, enter the following values:

- **SIP Entity IP Address:** Should be filled in automatically based on the SIP Entity Name.
- **Network Mask:** Enter the network mask corresponding to the IP address of Session Manager.
- **Default Gateway:** Enter the IP address of the default gateway for Session Manager.
- Use default values for the remaining fields. Click **Commit** to save (not shown).

AVAYA
Aura® System Manager 7.0

Last Logged on at November 17, 2016 11:03 AM

Go... Log off admin

Home / Elements / Session Manager

View Session Manager

Return

General | Security Module | Monitoring | CDR | Personal Profile Manager (PPM) - Connection Settings | Event Server | Expand All | Collapse All

General

SIP Entity Name

Description

Management Access Point Host Name/IP

Direct Routing to Endpoints

Data Center ·

Avaya Aura Device Services Server Pairing ·

Maintenance Mode ☐

Security Module

SIP Entity IP Address

Network Mask

Default Gateway

Call Control PHB

*SIP Firewall Configuration

Monitoring

Enable Monitoring ☒

Proactive cycle time (secs)

Reactive cycle time (secs)

Number of Tries

6.9. Configure Session Manager Certificate

From the home page of System Manager, navigate to **Services → Inventory → Manage Elements** the Manage Element page displays in the right side, select Session Manager Element and select **More Actions → Configure Identity Certificates** (not shown).

In the **Identity Certificates** page, select **Security Module SIP** and select **Replace** button to re-generate the SM identity certificate. The screenshot below shows the identity certificate of Session Manager with IP address in **CN**.

Home / Services / Inventory / Manage Elements

Manage Elements | Discovery

Identity Certificates

Replace | Export | Renew

5 Items | Filter: Enable

	Service Name	Common Name	Valid To	Expired	Service Description
<input type="radio"/>	SPIRIT	spiritalias	Sun Apr 15 05:44:36 EDT 2018	No	SPIRIT Service
<input type="radio"/>	Security Module HTTPS	securitymodule_https	Sun Apr 15 05:44:38 EDT 2018	No	Security Module HTTPS Service
<input checked="" type="radio"/>	Security Module SIP	securitymodule_sip	Wed Nov 21 09:28:16 EST 2018	No	Security Module SIP Service
<input type="radio"/>	WebSphere	websphere	Sun Apr 15 05:44:38 EDT 2018	No	Internal TLS communication between Security Module and WebSphere
<input type="radio"/>	Management	mgmt	Sun Apr 15 05:44:35 EDT 2018	No	Management Service

Select : None

Certificate Details

Subject Details: C=US, O=Avaya, CN=10.33.1.12

Valid From: Mon Nov 21 09:28:16 EST 2016 | Valid To: Wed Nov 21 09:28:16 EST 2018

Key Size: 2048

Issuer Name: O=AVAYA, OU=MGMT, CN=SystemManager CA

Certificate Fingerprint: 14cf1e5b65763d1b32e10ffefc297317e839fb22

Subject Alternative Name: dNSName=interopASM.bvwdev.com, IPAddress=10

7. Configure Convergy's Voice Portal

This section provides steps to configure Convergy's Voice Portal. Convergy's installs, configures, and customizes the Voice Portal application for end customers. This section describes the initial Voice Portal configuration.

Launch a web browser, enter <http://localhost:8070/ccportal/portal> in the URL. Log in with the appropriate credentials and click the **Accept** button on the following screen (not shown) to access the **System View** page.

The screenshot shows a web browser window displaying the 'CONVERGYS Control Center' login page. The header features the Convergy's logo with the tagline 'Outthinking Outdoing' and a banner image of four business professionals. The main heading is 'Welcome to Control Center'. Below this, there are input fields for 'Username' and 'Password', followed by a 'Login' button. At the bottom, there is a link for 'Browser Configuration Information'. The browser's status bar at the bottom right shows a zoom level of 100%.

CONVERGYS
Outthinking Outdoing

Control Center

Welcome to Control Center

Username

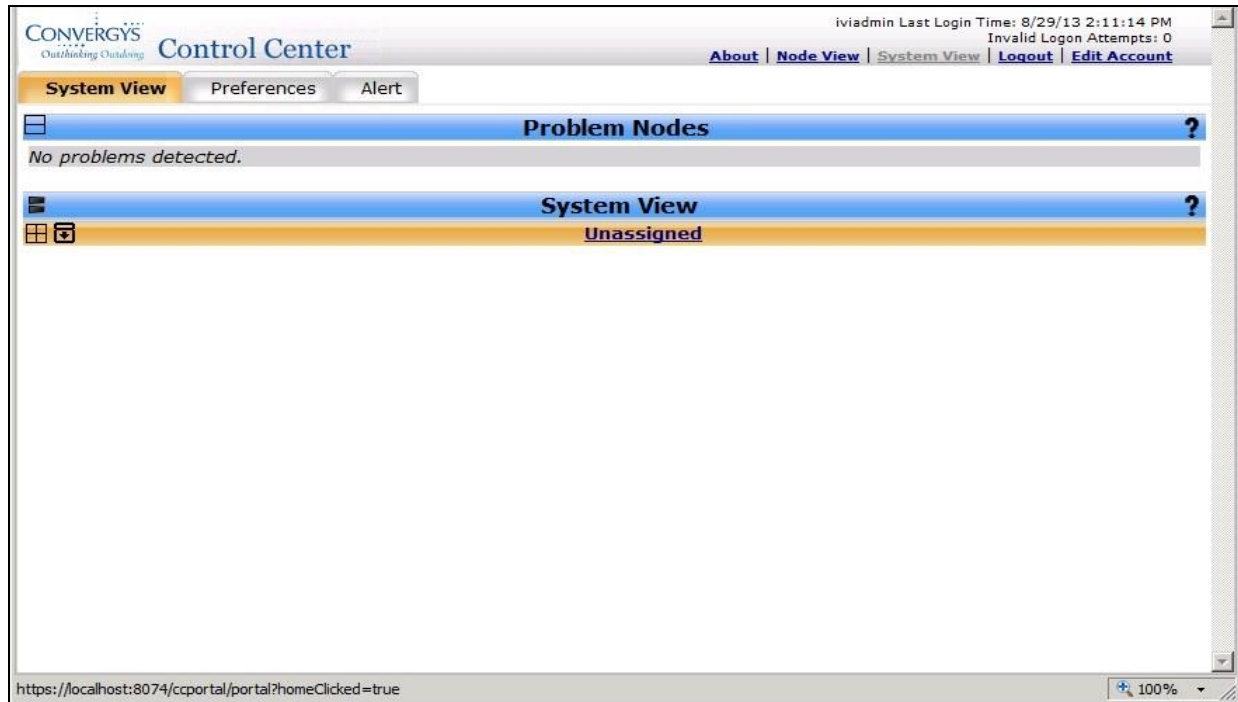
Password

Login

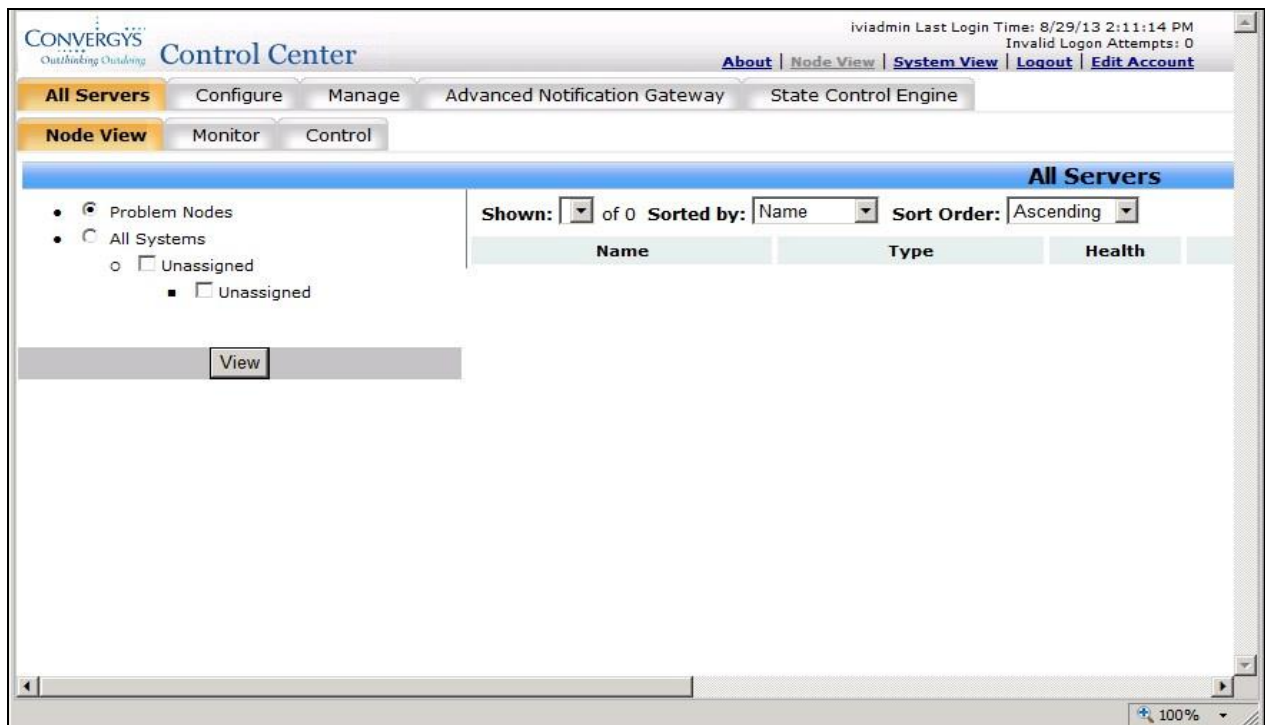
[Browser Configuration Information](#)

100%

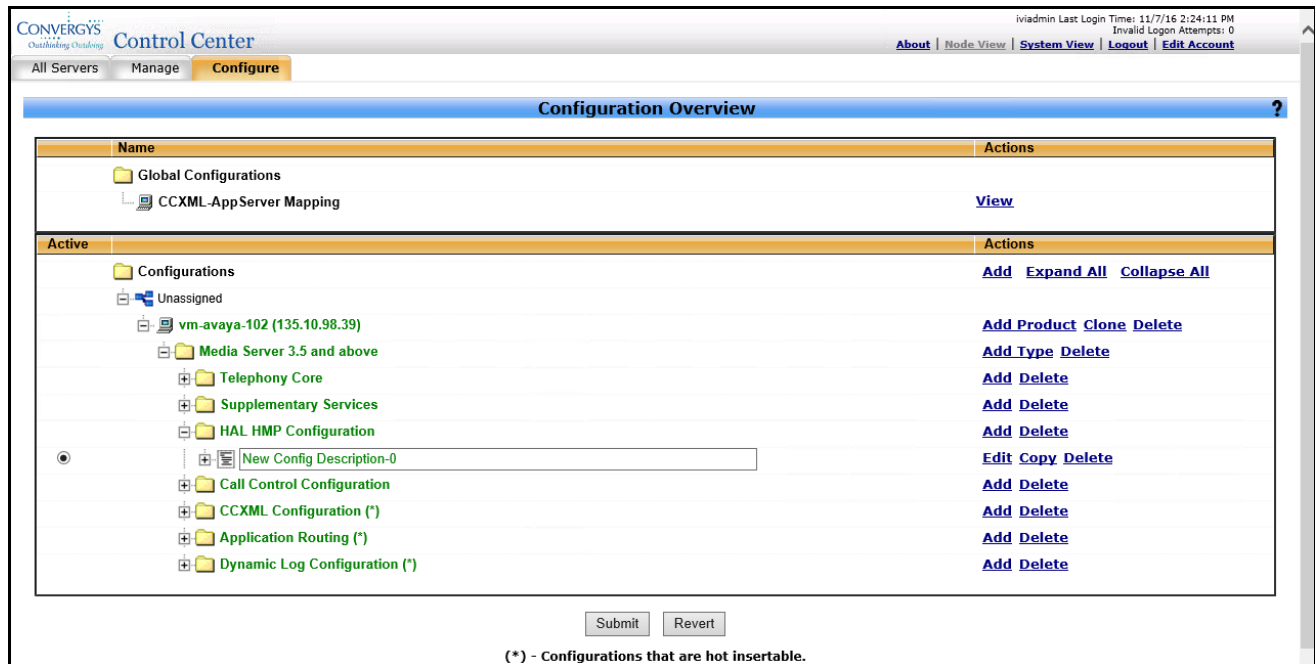
Select the **Node View** link at the top right.



Click the **Configure** tab on the top left to start configuring ConvergyS Voice Portal.



Expand and navigate to the server to be configured. In this example it is **Unassigned** → **vm-avaya-102 (135.10.98.39)** → **Media Server 3.5 and above** → **HAL HMP Configuration** → **New Config Description-0**. Click the **Edit** link next to the **New Config Description-0** field.



CONVERGYS Control Center

iviadmin Last Login Time: 11/7/16 2:24:11 PM
Invalid Logon Attempts: 0

[About](#) | [Node View](#) | [System View](#) | [Logout](#) | [Edit Account](#)

All Servers | Manage | **Configure**

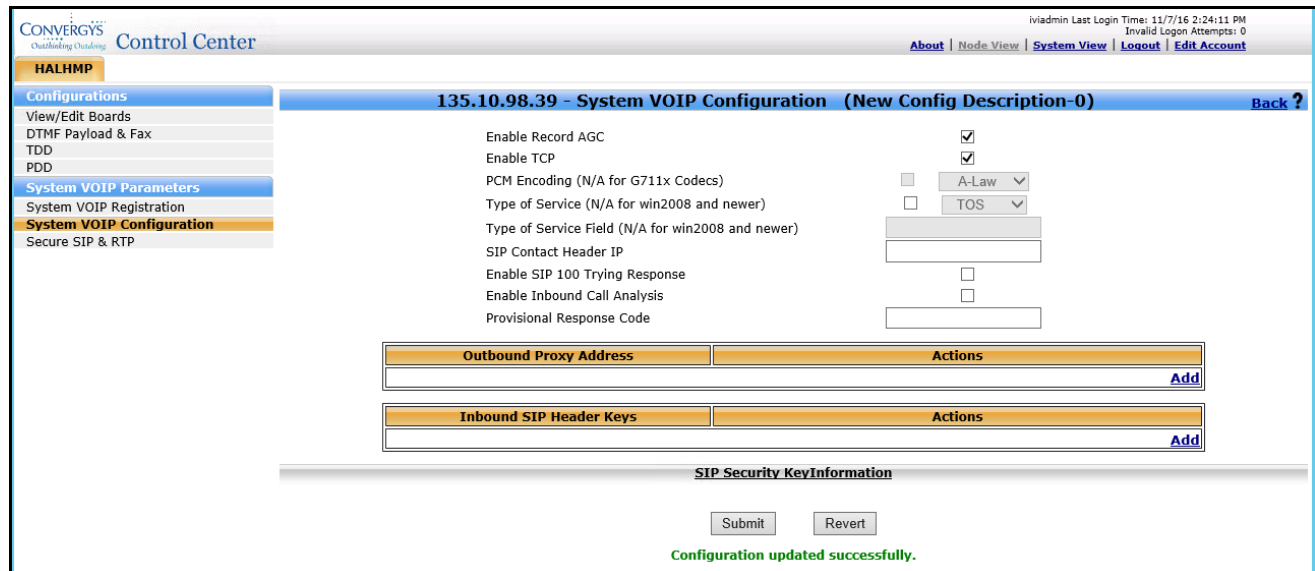
Configuration Overview ?

Name	Actions
Global Configurations	
CCXML-AppServer Mapping	View
Active	
Configurations	Add Expand All Collapse All
Unassigned	
vm-avaya-102 (135.10.98.39)	Add Product Clone Delete
Media Server 3.5 and above	Add Type Delete
Telephony Core	Add Delete
Supplementary Services	Add Delete
HAL HMP Configuration	Add Delete
New Config Description-0	Edit Copy Delete
Call Control Configuration	Add Delete
CCXML Configuration (*)	Add Delete
Application Routing (*)	Add Delete
Dynamic Log Configuration (*)	Add Delete

[Submit](#) [Revert](#)

(*) - Configurations that are hot insertable.

Select **System VOIP Configuration** under the System VOIP Parameters menu on the left. Select **Enable TCP**, and **Enable Record AGC**.



CONVERGYS Control Center

iviadmin Last Login Time: 11/7/16 2:24:11 PM
Invalid Logon Attempts: 0

[About](#) | [Node View](#) | [System View](#) | [Logout](#) | [Edit Account](#)

HALHMP

Configurations

View/Edit Boards
DTMF Payload & Fax
TDD
PDD

System VOIP Parameters

System VOIP Registration
System VOIP Configuration
Secure SIP & RTP

135.10.98.39 - System VOIP Configuration (New Config Description-0) [Back ?](#)

Enable Record AGC ☒
 Enable TCP ☒
 PCM Encoding (N/A for G711x Codecs) ☐ A-Law
 Type of Service (N/A for win2008 and newer) ☐ TOS
 Type of Service Field (N/A for win2008 and newer)
 SIP Contact Header IP
 Enable SIP 100 Trying Response ☐
 Enable Inbound Call Analysis ☐
 Provisional Response Code

Outbound Proxy Address **Actions**
 [Add](#)

Inbound SIP Header Keys **Actions**
 [Add](#)

SIP Security Key Information

[Submit](#) [Revert](#)

Configuration updated successfully.

Select **DTMF Payload and Fax** under the Configurations menu on the left. Use the **DTMF Detect Scheme** drop down menu to select the appropriate setting (*RFC2833_INBAND* is shown in the example below).

CONVERGYS Control Center

HALHMP

Configurations

View/Edit Boards

DTMF Payload & Fax

TDD

PDD

System VOIP Parameters

System VOIP Registration

System VOIP Configuration

Secure SIP & RTP

135.10.98.39 - DTMF Payload & Fax (New Config Description-0) [Back ?](#)

DTMF Detect Scheme: RFC2833_INBAND

DTMF Payload: 101

Fax Detect Scheme: ReinviteT38

Fax Detect Duration(ms): 150

Select **View/Edit Boards** under the Configurations menu on the left. Select the **Edit** link for the board.

CONVERGYS Control Center

HALHMP

Configurations

View/Edit Boards

DTMF Payload & Fax

TDD

PDD

System VOIP Parameters

System VOIP Registration

System VOIP Configuration

Secure SIP & RTP

135.10.98.39 - View/Edit Boards (New Config Description-0) [Back ?](#)

Board ID	Actions
0	Edit Delete

[Add Board](#)

Select **Codec** under the Configurations menu on the left. Click the **Add** link.

CONVERGYS Control Center

HMP Board

Configurations

Board

Board VOIP Registration

Codec

Alarm

135.10.98.39 - Codec - Board 0 [Back ?](#)

Codec Information				
Codec Family	Type	Frame Size	Frames per Packet	Actions
G711Codecs	G711M	30	1	Delete
G729Codecs	G729-ANNEX-A-B	10	2	Delete
				Add

Use the drop down menus to select the appropriate settings for **Codec Family**, **Type**, **Frame Size**, and **Frames per Packet**. Most installations will only require G711M, 30ms Frame Size, and 1 Frames Per Packet. Hit Submit after all Codecs have been defined.

Select the **Node View** link at the top right.

Click the **Configure** tab on the top left to start configuring the CCXML Configuration.

Expand and navigate to the server to be configured. In this example it is **Unassigned** → **vm-avaya-102 (135.10.98.39)** → **Media Server 3.5 and above** → **CCXML Configuration** → **New Config Description-0**. Click the **Edit** link next to the **New Config Description-0** field.

CONVERGYS
Outsourcing Outsourcing

Control Center

ivladmin Last Login Time: 11/9/16 7:58:06 AM
Invalid Logon Attempts: 0

About | Node View | System View | Logout | Edit Account

All Servers | Manage | **Configure**

Configuration Overview ?

Name	Actions
Global Configurations	
CCXML-AppServer Mapping	View

Active	Actions
Configurations	Add Expand All Collapse All
Unassigned	
vm-avaya-102 (135.10.98.39)	Add Product Clone Delete
Media Server 3.5 and above	Add Type Delete
Telephony Core	Add Delete
Supplementary Services	Add Delete
HAL HMP Configuration	Add Delete
Call Control Configuration	Add Delete
CCXML Configuration (*)	Add Delete
New Config Description-0	Edit Copy Delete
Application Routing (*)	Add Delete
Dynamic Log Configuration (*)	Add Delete

(*) - Configurations that are not insertable.

Click the **Edit** link.

CONVERGYS
Outsourcing Outsourcing

Control Center

ivladmin Last Login Time: 11/9/16 7:58:06 AM
Invalid Logon Attempts: 0

About | Node View | System View | Logout | Edit Account

CCXML

Browser Configuration

Instances

135.10.98.39 - Configuration Instances - (New Config Description-0) [Back ?](#)

CCXML Instances

Instance ID	Actions
default	Edit

[Add](#)

Click the **Properties** link on the left side menu. Then click **Add** to the Parameters actions. Add the **SIP_AAI_VENDOR** with a value of **avaya** as shown.

Click **Submit**.

The screenshot shows the ConvergyS Control Center interface. The top header includes the logo, navigation links (About, Node View, System View, Logout, Edit Account), and user information (ivadmin Last Login Time: 11/9/16 7:58:06 AM, Invalid Logon Attempts: 0). The left sidebar has a 'Browser Instance' tab and a 'Configuration' menu with options: Scripts, Processors, Platform, Logging, Resiliency, and Properties (selected). The main content area is titled '135.10.98.39 - Properties - default (New Config Description-0)' with a 'Back ?' link. It contains three sections: 'Session History' (empty), 'Http Settings' (Default Cache and Timeout fields), and 'Parameters' (a table with one row: SIP_AAI_VENDOR, avaya, with Delete and Add actions). At the bottom are 'Submit' and 'Revert' buttons.

Name	Value	Actions
SIP_AAI_VENDOR	avaya	Delete Add

8. Verification Steps

The following steps may be used to verify the configuration:

- End-to-end verification: Place a call to the Convergy's Voice Portal server. Verify the call is answered and voice prompts are played. Verify the SIP messages using a network protocol analyzer.
- DTMF Tones: Place a call to the Convergy's Voice Portal server and select the appropriate prompt to enter DTMF tones. Verify Convergy's Voice Portal properly identified each DTMF tone.
- Transfer: Place a call to Convergy's Voice Portal and select the appropriate prompt to have the call transferred to an Agent or station in Communication Manager. Verify the call is delivered to the Agent and answer the call. Verify there is a two-way talk path.

9. Conclusion

These Application Notes have described the administration steps required to integrate the Convergy's Voice Portal with Avaya Aura® Communication Manager and Avaya Aura® Session Manager via SIP trunk. All test cases passed with observations noted in **Section** Error! Reference source not found..

10. Additional References

This section references the documentation relevant to these Application Notes. Additional Avaya product documentation is available at <http://support.avaya.com>.

- [1] *What's New in Avaya Aura Release 7.0*, Release 7.0, 03-601818, Issue 1, August 2015.
- [2] *Deploying Avaya Aura® System Manager*, Release 7.0, Issue 1, October 2015.
- [3] *Administering Avaya Aura® System Manager for Release 7.0*, Issue 1, August 2015.
- [4] *Administering Avaya Aura® Session Manager*, Release 7.0, Issue 1, August 2015.
- [5] *Deploying Avaya Aura Communication Manager in Virtualized Environment*, Release 7, Issue 1, August 2015.
- [6] *RFC 3261 SIP: Session Initiation Protocol*, <http://www.ietf.org/>
- [7] *RFC 3515, The Session Initiation Protocol (SIP) Refer Method*, <http://www.ietf.org/>
- [8] *RFC 2833 RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals*, <http://www.ietf.org/>

©2017 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.