



**Application Notes for VHT Callback 8.0 with Avaya Aura®  
Application Enablement Services 6.3 and Avaya Aura®  
Session Manager 6.3 using Genesys T-Server for Avaya  
TSAPI 8.1 – Issue 1.0**

**Abstract**

These Application Notes describe the configuration steps required for VHT Callback 8.0 to interoperate with Avaya Aura® Communication Manager 6.3, Avaya Aura® Application Enablement Services 6.3, and Avaya Aura® Session Manager 6.3, using Genesys T-Server for Avaya TSAPI 8.1. VHT Callback is a contact center solution that calculates expected wait time and maintains caller position in virtual queue.

The integration used the Avaya Telephony Services Application Programming Interface from Avaya Aura® Application Enablement Services, and the SIP trunks interface from Avaya Aura® Session Manager.

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

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

# 1. Introduction

These Application Notes describe the configuration steps required for VHT Callback 8.0 to interoperate with Avaya Aura® Communication Manager 6.3, Avaya Aura® Application Enablement Services 6.3, and Avaya Aura® Session Manager 6.3, using Genesys T-Server for Avaya TSAPI 8.1. VHT Callback is a contact center solution that calculates expected wait time and maintains caller position in virtual queue.

VHT Callback can call users back and connect to agents when the caller's turn comes up. The integration used the Avaya Telephony Services Application Programming Interface (TSAPI) from Avaya Aura® Application Enablement Services, and the SIP trunks interface from Avaya Aura® Session Manager. In the compliance testing, VHT Callback used the Genesys T-Server for Avaya TSAPI to support all TSAPI communications with Avaya Aura® Application Enablement Services.

The TSAPI interface is used by VHT Callback to monitor VDNs, skill group, and agent stations, and to query status of ACD queues. The information obtained from the TSAPI event reports is used to calculate the expected wait time. All incoming ACD calls are routed by VHT Callback using the TSAPI adjunct routing capabilities. When the expected wait time for an ACD queue reaches a pre-defined threshold, then VHT Callback specifies for the call to route over Avaya Aura® Session Manager SIP trunks to the Interactive Voice Gateway (IVG) component of VHT Callback. The IVG will play the expected wait time announcement and provide caller with options to continue to wait in queue or to be called back.

Callers that decide to wait in queue will be transferred by VHT Callback to a Hold VDN on Communication Manager, which queues the call to the ACD skill group.

Callers that decide to be called back will be prompted for callback number and time, and VHT Callback will track the caller position in the virtual queue. When it is almost time for the caller to be serviced from the virtual queue, VHT Callback will place an outbound callback call via IVG and Avaya Aura® Session Manager SIP trunks to the PSTN destination, with call progress tones and tone detection handled by IVG. When the callback call is connected and accepted by the PSTN destination, VHT Callback then uses SIP REFER to transfer the callback call to a Callback VDN on Communication Manager, which queues the call to the ACD skill group with priority.

## 2. General Test Approach and Test Results

The feature test cases were performed both automatically and manually. Upon start of the Callback application, the application automatically sends TSAPI queries for skill group and agent stations, route registers for the Entry VDN, and requests monitoring of VDNs, skill group, and agent stations. For the manual part of the testing, incoming calls were made to the monitored VDNs to enable adjunct route and event reports to be sent to Callback. Manual call controls from the customer and agent telephones were exercised to verify remaining event reports, and the proper scheduling and delivering of callback calls.

The UUI data test cases were performed by using vector variables to assign UUI data to inbound calls, and verified by reviewing the TSAPI log and the SIP REFER message associated with inbound transferred and outbound callback calls.

The serviceability test cases were performed manually by disconnecting/reconnecting the Ethernet connection to the Callback server and to the IVG component.

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 feature and serviceability testing.

The feature testing focused on verifying the following on Callback:

- Use of TSAPI query service to query status on skill group and agent stations.
- Use of TSAPI event report service to monitor VDNs, skill group, and agent stations.
- Use of TSAPI routing service to route incoming calls.
- Use of SIP messages to answer and transfer inbound calls, and to initiate and transfer outbound callback calls.
- Proper handling of call scenarios involving G.711, DTMF, REFER, expected wait time under and over the threshold, transfer of inbound calls with received UUI data, initiation and transfer of outbound callback calls with priority and saved UUI data, and unsuccessful callback calls.

The serviceability testing focused on verifying the ability of Callback to recover from adverse conditions, such as disconnecting/reconnecting the Ethernet connection to the Callback server and to the IVG component.

## 2.2. Test Results

All test cases were executed and verified. The following were observations on Callback from the compliance testing.

- The calling party number was not available on the outbound callback calls.
- Upon receipt of the BYE message from Session Manager as part of a transferred call, IVG sent a 480 Temporarily Unavailable without any noticeable adverse impact.

## 2.3. Support

Technical support on Callback can be obtained through the following:

- **Phone:** (866) 670-2223
- **Email:** [support@virtualhold.com](mailto:support@virtualhold.com)

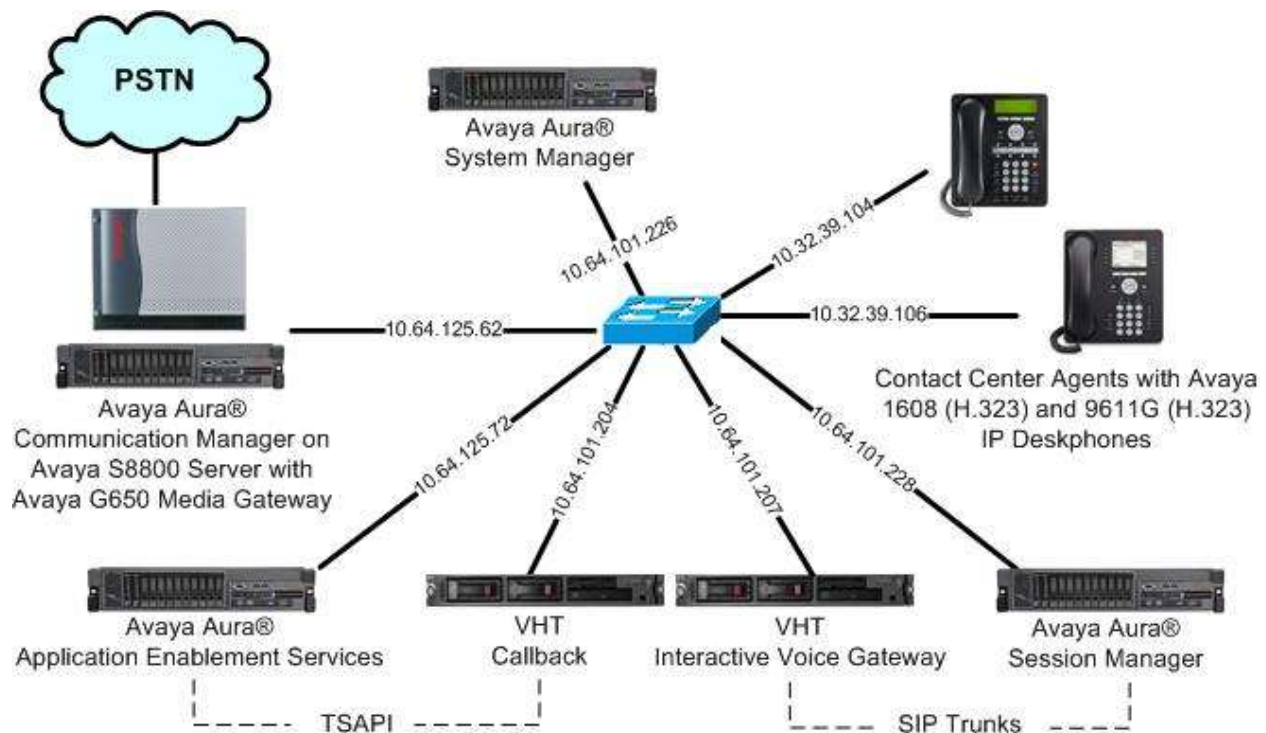
### 3. Reference Configuration

The configuration used for the compliance testing is shown in **Figure 1**. The Callback configuration consisted of the Callback server, and an IVG that connected via SIP trunks with Session Manager.

The configuration of Session Manager was performed via the web interface of System Manager. The detailed administration of basic connectivity between Communication Manager, System Manager, Session Manager, Application Enablement Services, and of contact center devices is not the focus of these Application Notes and will not be described.

The pre-existing contact center devices used in the compliance testing are shown in the table below. Additional vectors and VDNs need to be created, as described in **Section 5.4**. The applicable domain for the network is “dr220.com”. A five digit Uniform Dial Plan was used to facilitate routing of calls with Callback. In the compliance testing, calls to 32xxx were routed to the IVG component of Callback.

Device Type	Value
Skill Group Number and Extension	81, 65081
Agent Stations	65001, 65002
Agent IDs	65881, 65882



**Figure 1: Compliance Testing Configuration**

## 4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya Aura® Communication Manager on Avaya S8800 Server with Avaya G650 Media Gateway	6.3.9 (R016x.03.0.124.0-21971)
Avaya Aura® Application Enablement Services	6.3.3 SP1 (6.3.3.1.10-0)
Avaya Aura® Session Manager	6.3.11.0.631103
Avaya Aura® System Manager	6.3.11.8.2933
Avaya 1616 IP Deskphone (H.323)	1.350B
Avaya 9611G IP Deskphone (H.323)	6.4.0.14
VHT Callback on Microsoft Windows Server 2008 R2 Enterprise <ul style="list-style-type: none"><li>Microsoft SQL Server 2008 R2</li><li>Genesys T-Server for Avaya TSAPI</li><li>Avaya TSAPI Windows Client (csta32.dll)</li></ul>	8.0.6.1075 SP 1 10.50.1600.1 8.1.001.14 5.2.1.474
VHT IVG on CentOS	1.1.0-20150320145933 6.5

## 5. Configure Avaya Aura® Communication Manager

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

- Verify license
- Administer CTI link
- Administer system parameters features
- Administer vectors and VDNs
- Administer SIP signaling group
- Administer SIP trunk group
- Administer IP network region
- Administer IP codec set
- Administer route pattern
- Administer uniform dial plan
- Administer AAR analysis

In the compliance testing, a separate set of codec set, network region, trunk group, and signaling group was used for integration with Callback.

### 5.1. Verify License

Log into the System Access Terminal (SAT) to verify that the Communication Manager license has proper permissions for features illustrated in these Application Notes. Use the “display system-parameters customer-options” command. Navigate to **Page 2**, and verify that there is sufficient remaining capacity for **Maximum Administered SIP Trunks**.

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

```
display system-parameters customer-options                               Page 2 of 11
                                OPTIONAL FEATURES

IP PORT CAPACITIES                                                    USED
      Maximum Administered H.323 Trunks: 12000 10
    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: 414 0
    Max Concur Registered Unauthenticated H.323 Stations: 100 0
      Maximum Video Capable Stations: 41000 0
      Maximum Video Capable IP Softphones: 18000 0
      Maximum Administered SIP Trunks: 24000 30
    Maximum Administered Ad-hoc Video Conferencing Ports: 24000 0
```

Navigate to **Page 3**, and verify that the **Computer Telephony Adjunct Links** customer option is 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	<b>Computer Telephony Adjunct Links? y</b>	
ARS/AAR Partitioning? y	Cvg Of Calls Redirected Off-net? y	
ARS/AAR Dialing without FAC? n	DCS (Basic)? y	
ASAI Link Core Capabilities? n	DCS Call Coverage? y	
ASAI Link Plus Capabilities? n	DCS with Rerouting? y	

Navigate to **Page 6**, and verify that the **Vectoring (Basic)** customer option is set to “y”.

display system-parameters customer-options		Page 6 of 11
CALL CENTER OPTIONAL FEATURES		
Call Center Release: 6.0		
ACD? y	Reason Codes? y	
BCMS (Basic)? y	Service Level Maximizer? n	
BCMS/VuStats Service Level? y	Service Observing (Basic)? y	
BSR Local Treatment for IP & ISDN? y	Service Observing (Remote/By FAC)? y	
Business Advocate? n	Service Observing (VDNs)? y	
Call Work Codes? y	Timed ACW? y	
DTMF Feedback Signals For VRU? y	<b>Vectoring (Basic)? y</b>	
Dynamic Advocate? n	Vectoring (Prompting)? y	
Expert Agent Selection (EAS)? y	Vectoring (G3V4 Enhanced)? y	
EAS-PHD? y	Vectoring (3.0 Enhanced)? y	

## 5.2. Administer CTI Link

Add a CTI link using the “add cti-link n” command, where “n” is an available CTI link number. Enter an available extension number in the **Extension** field. Note that the CTI link number and extension number may vary. Enter “ADJ-IP” in the **Type** field, and a descriptive name in the **Name** field. Default values may be used in the remaining fields.

add cti-link 2		Page 1 of 3
CTI LINK		
CTI Link: 2		
<b>Extension: 60100</b>		
<b>Type: ADJ-IP</b>		
COR: 1		
<b>Name: AES CTI Link</b>		



### 5.3. Administer System Parameters Features

Use the “change system-parameters features” command to enable **Create Universal Call ID (UCID)**, which is located on **Page 5**. For **UCID Network Node ID**, enter an available node ID.

```
change system-parameters features                                     Page 5 of 20
                           FEATURE-RELATED SYSTEM PARAMETERS

SYSTEM PRINTER PARAMETERS
  Endpoint:                  Lines Per Page: 60

SYSTEM-WIDE PARAMETERS
  Switch Name:
  Emergency Extension Forwarding (min): 10
  Enable Inter-Gateway Alternate Routing? n
  Enable Dial Plan Transparency in Survivable Mode? n
  COR to Use for DPT: station
  EC500 Routing in Survivable Mode: dpt-then-ec500
MALICIOUS CALL TRACE PARAMETERS
  Apply MCT Warning Tone? n    MCT Voice Recorder Trunk Group:
  Delay Sending RElease (seconds): 0
SEND ALL CALLS OPTIONS
  Send All Calls Applies to: station    Auto Inspect on Send All Calls? n
  Preserve previous AUX Work button states after deactivation? n
UNIVERSAL CALL ID
  Create Universal Call ID (UCID)? y    UCID Network Node ID: 27
```

Navigate to **Page 13**, and enable **Send UCID to ASAI**. This parameter allows for the universal call ID to be sent to Callback.

```
change system-parameters features                                     Page 13 of 20
                           FEATURE-RELATED SYSTEM PARAMETERS

CALL CENTER MISCELLANEOUS
  Callr-info Display Timer (sec): 10
  Clear Callr-info: next-call
  Allow Ringer-off with Auto-Answer? n

  Reporting for PC Non-Predictive Calls? n

  Agent/Caller Disconnect Tones? n
  Interruptible Aux Notification Timer (sec): 3
  Zip Tone Burst for Callmaster Endpoints: double

ASAI
  Copy ASAI UII During Conference/Transfer? y
  Call Classification After Answer Supervision? y
  Send UCID to ASAI? y
  For ASAI Send DTMF Tone to Call Originator? n
  Send Connect Event to ASAI For Announcement Answer? n
```

## 5.4. Administer Vectors and VDNs

Administer three sets of vectors and VDNs shown below for routing of calls to Callback. Note that the VDN extensions and vector numbers can vary.

VDN	Vector	Purpose
60901	901	Entry vector & VDN for adjunct route and failure coverage
60902	902	Hold vector & VDN for queuing inbound calls to skill at medium priority
60903	903	Callback vector & VDN for queuing outbound calls to skill at high priority

### 5.4.1. Entry Vector and VDN

Modify an available vector using the “change vector n” command, where “n” is an existing vector number. The vector will be used to provide adjunct route to the CTI link defined in **Section 5.2**.

Note that the vector **Number**, **Name**, **wait-time** and **route-to number** parameter settings may vary. The **route-to number** is used as the covering point to provide failure coverage in case of failures from the adjunct routing step. In the compliance testing, the covering point is the Hold VDN, which is administered in **Section 5.4.2**.

```
change vector 901                                     Page 1 of 6
                                                    CALL VECTOR

  Number: 901                      Name: VHT Entry
Multimedia? n      Attendant Vectoring? n      Meet-me Conf? n      Lock? n
  Basic? y          EAS? y      G3V4 Enhanced? y      ANI/II-Digits? y      ASAI Routing? y
  Prompting? y      LAI? n      G3V4 Adv Route? y      CINFO? y      BSR? y      Holidays? y
  Variables? y      3.0 Enhanced? y
01 adjunct          routing link 2
02 wait-time        10 secs hearing music
03 route-to         number 60902          with cov n if unconditionally
04
```

Add a VDN using the “add vdn n” command, where “n” is an available extension number. Enter a descriptive **Name**, and the vector number from above for **Vector Number**. Retain the default values for all remaining fields.

```
add vdn 60901                                     Page 1 of 3
                                                    VECTOR DIRECTORY NUMBER

  Extension: 60901
  Name*: VHT Entry
  Destination: Vector Number          901
Attendant Vectoring? n
Meet-me Conferencing? n
  Allow VDN Override? n
  COR: 1
  TN*: 1
  Measured: none
```

### 5.4.2. Hold Vector and VDN

Modify an available vector to queue incoming calls to the ACD skill group at medium priority. Note that the vector **Number**, **Name**, **queue-to skill** and **wait-time** parameter settings may vary, and that “81” is the existing skill group number from **Section 3**.

```
change vector 902                                     Page 1 of 6
                                     CALL VECTOR

  Number: 902           Name: VHT Hold
Multimedia? n      Attendant Vectoring? n      Meet-me Conf? n      Lock? n
  Basic? y      EAS? y      G3V4 Enhanced? y      ANI/II-Digits? y      ASAI Routing? y
  Prompting? y      LAI? n      G3V4 Adv Route? y      CINFO? y      BSR? y      Holidays? y
  Variables? y      3.0 Enhanced? y
01 wait-time      0      secs hearing silence
02 queue-to      skill 81      pri m
03 wait-time      20      secs hearing ringback
04 goto step      3              if unconditionally
05
```

Add a VDN with an available extension as shown below. Enter a descriptive **Name**, and the vector number from above for **Vector Number**.

```
add vdn 60902                                     Page 1 of 3
                                     VECTOR DIRECTORY NUMBER

                                     Extension: 60902
                                     Name*: VHT Hold
                                     Destination: Vector Number      902
Attendant Vectoring? n
Meet-me Conferencing? n
Allow VDN Override? n
COR: 1
TN*: 1
Measured: none
```

### 5.4.3. Callback Vector and VDN

Modify an available vector to queue callback calls to the ACD skill group at high priority. Note that the vector **Number**, **Name**, **queue-to skill** and **wait-time** parameters may vary, and that “81” is the existing skill group number from **Section 3**.

change vector 903	CALL VECTOR	Page 1 of 6
<b>Number: 903</b> <b>Name: VHT Callback</b>		
Multimedia? n	Attendant Vectoring? n	Meet-me Conf? n                      Lock? n
Basic? y	EAS? y    G3V4 Enhanced? y	ANI/II-Digits? y    ASAI Routing? y
Prompting? y	LAI? n    G3V4 Adv Route? y	CINFO? y    BSR? y    Holidays? y
Variables? y	3.0 Enhanced? y	
01 queue-to	skill 81	pri h
02 wait-time	20 secs	hearing ringback
03		

Add a VDN with an available extension as shown below. Enter a descriptive name for **Name**, and the vector number from above for **Vector Number**.

add vdn 60903	VECTOR DIRECTORY NUMBER	Page 1 of 3
Extension: 60903		
<b>Name*: VHT Callback</b>		
<b>Destination: Vector Number</b>	<b>903</b>	
Attendant Vectoring? n		
Meet-me Conferencing? n		
Allow VDN Override? n		
COR: 1		
TN*: 1		
Measured: none		

## 5.5. Administer SIP Signaling Group

Use the “add signaling-group n” command, where “n” is an available signaling group number, in this case “32”. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Group Type:** “sip”
- **Transport Method:** “tls”
- **Near-end Node Name:** An existing C-LAN node name.
- **Far-end Node Name:** The existing node name for Session Manager.
- **Near-end Listen Port:** An available port for integration with Callback.
- **Far-end Listen Port:** The same port number as in **Near-end Listen Port**.
- **Far-end Network Region:** An existing network region to use with Callback.
- **Far-end Domain:** The applicable domain name for the network.

add signaling-group 32		Page 1 of 1
SIGNALING GROUP		
Group Number: 32	Group Type: sip	
IMS Enabled? n	Transport Method: tls	
Q-SIP? n		
IP Video? n	Enforce SIPS URI for SRTP? y	
Peer Detection Enabled? y	Peer Server: Others	
Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? n		
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? y		
Alert Incoming SIP Crisis Calls? n		
Near-end Node Name: clan	Far-end Node Name: DR-SMW-Sig	
Near-end Listen Port: 5032	Far-end Listen Port: 5032	
	Far-end Network Region: 3	
Far-end Domain: dr220.com		
Incoming Dialog Loopbacks: eliminate		Bypass If IP Threshold Exceeded? n
DTMF over IP: rtp-payload	RFC 3389 Comfort Noise? n	
Session Establishment Timer(min): 3	Direct IP-IP Audio Connections? y	
Enable Layer 3 Test? y	IP Audio Hairpinning? n	
H.323 Station Outgoing Direct Media? n	Initial IP-IP Direct Media? n	
	Alternate Route Timer(sec): 6	

## 5.6. Administer SIP Trunk Group

Use the “add trunk-group n” command, where “n” is an available trunk group number, in this case “32”. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Group Type:** “sip”
- **Group Name:** A descriptive name.
- **TAC:** An available trunk access code.
- **Service Type:** “tie”
- **Signaling Group:** The signaling group number from **Section 5.5**.
- **Number of Members:** The desired number of members, in this case “10”.

add trunk-group 32		Page 1 of 21	
TRUNK GROUP			
Group Number: 54	<b>Group Type: sip</b>	CDR Reports: y	
<b>Group Name: VHG IVG</b>	COR: 1	TN: 1	<b>TAC: 1032</b>
Direction: two-way	Outgoing Display? n	Night Service:	
Dial Access? n			
Queue Length: 0			
<b>Service Type: tie</b>	Auth Code? n		
		Member Assignment Method: auto	
		<b>Signaling Group: 32</b>	
		<b>Number of Members: 10</b>	

## 5.7. Administer IP Network Region

Use the “change ip-network-region n” command, where “n” is the existing far-end network region number used by the SIP signaling group from **Section 5.5**. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Authoritative Domain:** The applicable domain for the network.
- **Name:** A descriptive name.
- **Intra-region IP-IP Direct Audio:** “yes”
- **Inter-region IP-IP Direct Audio:** “yes”
- **Codec Set:** An available codec set for integration with Callback.

```
change ip-network-region 3                                     Page 1 of 20
                                IP NETWORK REGION
    Region: 3
Location:      Authoritative Domain: dr220.com
    Name: VHT IVG      Stub Network Region: n
MEDIA PARAMETERS      Intra-region IP-IP Direct Audio: yes
    Codec Set: 3      Inter-region IP-IP Direct Audio: yes
    UDP Port Min: 2048      IP Audio Hairpinning? n
    UDP Port Max: 3329
DIFFSERV/TOS PARAMETERS
    Call Control PHB Value: 46
    Audio PHB Value: 46
    Video PHB Value: 26
```

Navigate to **Page 4**, and specify this codec set to be used for calls with network region used by Avaya endpoints and by the trunk to the PSTN. In the compliance testing, network region “1” was used by the Avaya endpoints and by the trunk to the PSTN.

```
change ip-network-region 3                                     Page 4 of 20

Source Region: 3      Inter Network Region Connection Management      I      M
                                                                G      A      t
dst codec direct      WAN-BW-limits      Video      Intervening      Dyn      A      G      c
rgn set      WAN Units      Total Norm      Prio Shr Regions      CAC      R      L      e
1      3
2
3      3
4
5
6
7
8
```

## 5.8. Administer IP Codec Set

Use the “change ip-codec-set n” command, where “n” is the codec set number from **Section 5.7**. Update the audio codec types in the **Audio Codec** fields as necessary. G.711MU was the only codec covered in the compliance testing.

change ip-codec-set 3

Page 1 of 2

IP Codec Set

Codec Set: 3

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

## 5.9. Administer Route Pattern

Use the “change route-pattern n” command, where “n” is an existing route pattern number to be used to reach Callback, in this case “32”. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Pattern Name:** A descriptive name.
- **Grp No:** The SIP trunk group number from **Section 5.6**.
- **FRL:** A level that allows access to this trunk, with 0 being least restrictive.

change route-pattern 32												Page	1 of	3
Pattern Number: 54    Pattern Name: VHT IVG														
SCCAN? n    Secure SIP? n														
Grp	FRL	NPA	Pfx	Hop	Toll	No.	Inserted					DCS/	IXC	
No			Mrk	Lmt	List	Del	Digits					QSIG		
												Intw		
1:	32	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	rest				none		



## 5.10. Administer Uniform Dial Plan

This section provides a sample AAR routing used for routing of inbound calls to Callback at destination 32xxx, which will be returned by Callback as the adjunct route destination in the compliance testing. Note that other routing methods may be used.

Use the “change uniform-dialplan 0” command, and add an entry to specify the use of AAR for routing digits 32xxx, as shown below.

change uniform-dialplan 0					Page 1 of 2	
UNIFORM DIAL PLAN TABLE						
					Percent Full: 0	
Matching			Insert			Node
Pattern	Len	Del	Digits	Net	Conv	Num
32	5	0		aar	n	

## 5.11. Administer AAR Analysis

Use the “change aar analysis 0” command, and add an entry to specify how to route calls to 32xxx. In the example shown below, calls with digits 32xxx will be routed as an AAR call using route pattern “32” from **Section 5.9**.

change aar analysis 0							Page 1 of 2		
AAR DIGIT ANALYSIS TABLE									
Location: all							Percent Full: 2		
	Dialed	Total		Route	Call	Node	ANI		
	String	Min	Max	Pattern	Type	Num	Reqd		
32		5	5	32	aar		n		

## 6. Configure Avaya Aura® Application Enablement Services

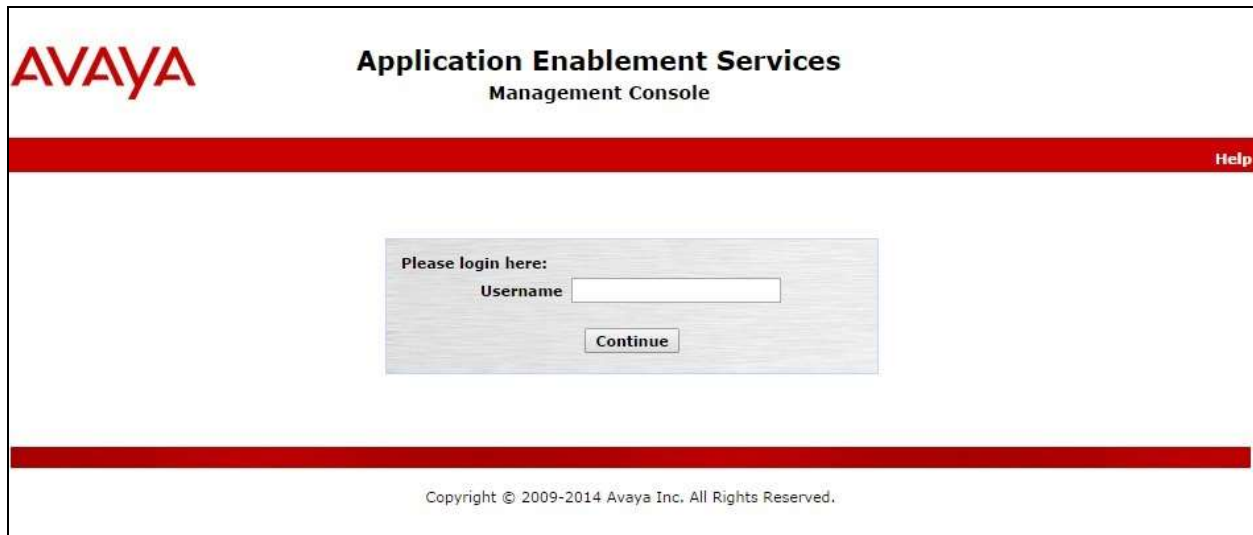
This section provides the procedures for configuring Application Enablement Services. The procedures include the following areas:

- Launch OAM interface
- Verify license
- Administer TSAPI link
- Administer TCP settings
- Restart service
- Obtain Tlink name
- Administer Callback user
- Verify security database

### 6.1. Launch OAM Interface

Access the OAM web-based interface by using the URL “https://ip-address” in an Internet browser window, where “ip-address” is the IP address of the Application Enablement Services server.

The **Please login here** screen is displayed. Log in using the appropriate credentials.



The screenshot shows the Avaya Application Enablement Services Management Console login interface. At the top left is the Avaya logo. To its right, the text "Application Enablement Services" and "Management Console" is displayed. A red horizontal bar spans the width of the page, with a "Help" link on the right. In the center, there is a login box with the text "Please login here:" followed by a "Username" label and a text input field. Below the input field is a "Continue" button. At the bottom of the page, a red horizontal bar is present, and below it, the copyright notice "Copyright © 2009-2014 Avaya Inc. All Rights Reserved." is displayed.

The **Welcome to OAM** screen is displayed next.

The screenshot displays the Avaya Application Enablement Services Management Console. The top header includes the Avaya logo, the title "Application Enablement Services Management Console", and a welcome message for the user. The left sidebar contains a navigation menu with options like AE Services, Communication Manager Interface, High Availability, Licensing, Maintenance, Networking, Security, Status, User Management, Utilities, and Help. The main content area shows the "Welcome to OAM" screen, which provides an overview of the OAM web and lists administrative domains: AE Services, Communication Manager Interface, High Availability, Licensing, Maintenance, Networking, Security, Status, User Management, Utilities, and Help. It also mentions that these domains can be served by one administrator for all domains or a separate administrator for each domain.

Welcome: User  
Last login: Tue Jan 20 06:55:31 2015 from 10.32.39.20  
Number of prior failed login attempts: 0  
HostName/IP: aes\_125\_72/10.64.125.72  
Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_SP  
SW Version: 6.3.3.1.10-0  
Server Date and Time: Tue Jan 20 06:57:01 MST 2015  
HA Status: Not Configured

Home | Help | Logout

**AE Services**  
Communication Manager Interface  
High Availability  
Licensing  
Maintenance  
Networking  
Security  
Status  
User Management  
Utilities  
Help

**Welcome to OAM**

The AE Services Operations, Administration, and Management (OAM) Web provides you with tools for managing the AE Server. OAM spans the following administrative domains:

- AE Services - Use AE Services to manage all AE Services that you are licensed to use on the AE Server.
- Communication Manager Interface - Use Communication Manager Interface to manage switch connection and dialplan.
- High Availability - Use High Availability to manage AE Services HA.
- Licensing - Use Licensing to manage the license server.
- Maintenance - Use Maintenance to manage the routine maintenance tasks.
- Networking - Use Networking to manage the network interfaces and ports.
- Security - Use Security to manage Linux user accounts, certificate, host authentication and authorization, configure Linux-PAM (Pluggable Authentication Modules for Linux) and so on.
- Status - Use Status to obtain server status informations.
- User Management - Use User Management to manage AE Services users and AE Services user-related resources.
- Utilities - Use Utilities to carry out basic connectivity tests.
- Help - Use Help to obtain a few tips for using the OAM Help system

Depending on your business requirements, these administrative domains can be served by one administrator for all domains, or a separate administrator for each domain.

## 6.2. Verify License

Select **Licensing** → **WebLM Server Access** in the left pane, to display the **Web License Manager** pop-up screen (not shown), and log in using the appropriate credentials.

The screenshot displays the Avaya Application Enablement Services Management Console with the "Licensing" section selected in the left sidebar. The main content area shows the "Licensing" screen, which provides instructions on how to set up and maintain the WebLM, import, set up, and maintain the license, and administer TSAPI Reserved Licenses or DMCC Reserved Licenses. It lists the following steps: WebLM Server Address, WebLM Server Access, and Reserved Licenses.

Welcome: User  
Last login: Tue Jan 20 06:55:31 2015 from 10.32.39.20  
Number of prior failed login attempts: 0  
HostName/IP: aes\_125\_72/10.64.125.72  
Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_SP  
SW Version: 6.3.3.1.10-0  
Server Date and Time: Tue Jan 20 06:57:01 MST 2015  
HA Status: Not Configured

Home | Help | Logout

**AE Services**  
Communication Manager Interface  
Licensing  
Maintenance  
Networking  
Security

**Licensing**

If you are setting up and maintaining the WebLM, you need to use the following:

- WebLM Server Address

If you are importing, setting up and maintaining the license, you need to use the following:

- WebLM Server Access

If you want to administer TSAPI Reserved Licenses or DMCC Reserved Licenses, you need to use the following:

- Reserved Licenses

The **Web License Manager** screen below is displayed. Select **Licensed products** → **APPL\_ENAB** → **Application\_Enablement** in the left pane, to display the **Application Enablement (CTI)** screen in the right pane.

Verify that there are sufficient licenses for **TSAPI Simultaneous Users**, as shown below. Also verify that there is an applicable advanced switch license, in this case **AES ADVANCED LARGE SWITCH** for the Avaya S8800 Server.

**Web License Manager (WebLM v6.3)**
Help About Change Password

WebLM Home  
Install license  
Licensed products  
APPL\_ENAB  
▼ Application\_Enablement  
View license capacity  
View peak usage  
Uninstall license  
Server properties  
Manage users  
Shortcuts  
Help for Installed Product

**Application Enablement (CTI) - Release: 6 - SID: 10503000**
**Standard License file**

You are here: Licensed Products > Application\_Enablement > View License Capacity  
License installed on: May 11, 2012 7:07:47 PM -04:00  

**License File Host IDs:**
00-16-3E-48-E0-82

**Licensed Features**

10 Items
Show ALL

Feature (License Keyword)	Expiration date	Licensed capacity
CVLAN ASAI VALUE_AES_CVLAN_ASAI	permanent	16
Unified CC API Desktop Edition VALUE_AES_AEC_UNIFIED_CC_DESKTOP	permanent	10000
AES ADVANCED SMALL SWITCH VALUE_AES_AEC_SMALL_ADVANCED	permanent	16
CVLAN Proprietary Links VALUE_AES_PROPRIETARY_LINKS	permanent	16
Product Notes VALUE_NOTES	permanent	SmallServerTypes: s8300c;s8300d;jcc;premio;tn8400;leaptop;CtiS MediumServerTypes: ibmx306;ibmx306m;del1950;xen;hs20;hs20_ LargeServerTypes: isp2100;ibmx305;dl380g3;dl385g1;dl385g2;u TrustedApplications: IPS_001, BasicUnrestricted DMCUnrestricted; IXP_001, BasicUnrestricted DMCUnrestricted; IXM_001, BasicUnrestricted DMCUnrestricted; PC_001, BasicUnrestricted DMCUnrestricted; CJE_001, BasicUnrestricted DMCUnrestricted; OSFC_001, BasicUnrestricted DMCUnrestricted; VP_001, BasicUnrestricted DMCUnrestricted; SAMETIME_001, VALUE_AES_UNIFIED_CC_DESKTOP_n; CCE_ AdvancedUnrestricted, DMCUnrestricted; CSI AdvancedUnrestricted, DMCUnrestricted; CSI AdvancedUnrestricted, DMCUnrestricted; AVA BasicUnrestricted, AdvancedUnrestricted, DMC CCT_ELITE_CALL_CTRL_001, BasicUnrestricted DMCUnrestricted, AgentEvents;
AES ADVANCED LARGE SWITCH VALUE_AES_AEC_LARGE_ADVANCED	permanent	16
TSAPI Simultaneous Users VALUE_AES_TSAPI_USERS	permanent	10000
DLG VALUE_AES_DLG	permanent	16
Device Media and Call Control VALUE_AES_DMCC_DMC	permanent	10000
AES ADVANCED MEDIUM SWITCH VALUE_AES_AEC_MEDIUM_ADVANCED	permanent	16

TLT; Reviewed:  
SPOC 7/2/2015

Solution & Interoperability Test Lab Application Notes  
©2015 Avaya Inc. All Rights Reserved.

20 of 62  
VH-Gen-AES63

### 6.3. Administer TSAPI Link

Select **AE Services** → **TSAPI** → **TSAPI Links** from the left pane of the **Management Console**, to administer a TSAPI link. The **TSAPI Links** screen is displayed, as shown below. Click **Add Link**.

The screenshot shows the Avaya Management Console interface. The top header includes the Avaya logo, the title "Application Enablement Services Management Console", and a welcome message for the user. The left navigation pane shows "AE Services" expanded, with "TSAPI" selected, and "TSAPI Links" highlighted. The main content area displays the "TSAPI Links" screen, which includes a table with columns: Link, Switch Connection, Switch CTI Link #, ASAI Link Version, and Security. Below the table are buttons for "Add Link", "Edit Link", and "Delete Link".

The **Add TSAPI Links** screen is displayed next.

The **Link** field is only local to the Application Enablement Services server, and may be set to any available number. For **Switch Connection**, select the relevant switch connection from the drop-down list. In this case, the existing switch connection "S8800" is selected. For **Switch CTI Link Number**, select the CTI link number from **Section 5.2**. Retain the default values in the remaining fields.

The screenshot shows the "Add TSAPI Links" screen in the Avaya Management Console. The left navigation pane is the same as the previous screenshot. The main content area displays the "Add TSAPI Links" form, which includes fields for Link, Switch Connection, Switch CTI Link Number, ASAI Link Version, and Security. The values entered are: Link: 1, Switch Connection: S8800, Switch CTI Link Number: 2, ASAI Link Version: 6, and Security: Unencrypted. Below the fields are buttons for "Apply Changes" and "Cancel Changes".

## 6.4. Administer TCP Settings

Select **Networking** → **TCP Settings** from the left pane, to display the **TCP Settings** screen in the right pane. For **TCP Retransmission Count**, select **TSAPI Routing Application Configuration**, as shown below.

The screenshot displays the Avaya Application Enablement Services Management Console. The top header includes the Avaya logo, the title "Application Enablement Services Management Console", and a welcome message for the user. The left navigation pane shows a tree structure with "Networking" selected and expanded, highlighting "TCP Settings". The main content area is titled "TCP Settings" and contains a "TCP Retransmission Count" section with two radio button options: "Standard Configuration (15)" and "TSAPI Routing Application Configuration (6)". The "TSAPI" option is selected. Below the options are "Apply Changes" and "Cancel Changes" buttons. A note explains that a smaller count reduces server wait time, and a warning states that the setting applies to all TCP and TLS sockets.

Welcome: User  
Last login: Tue Jan 20 06:55:31 2015 from 10.32.39.20  
Number of prior failed login attempts: 0  
HostName/IP: aes\_125\_72/10.64.125.72  
Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_SP  
SW Version: 6.3.3.1.10-0  
Server Date and Time: Tue Jan 20 06:57:01 MST 2015  
HA Status: Not Configured

**Networking | TCP Settings** [Home](#) | [Help](#) | [Logout](#)

**AE Services**  
Communication Manager Interface  
High Availability  
Licensing  
Maintenance  
▼ **Networking**  
AE Service IP (Local IP)  
Network Configure  
Ports  
**TCP Settings**  
Security

**TCP Settings**

TCP Retransmission Count

☐ Standard Configuration (15)  
☒ TSAPI Routing Application Configuration (6)

[Apply Changes](#) [Cancel Changes](#)

Note: A smaller TCP Retransmission Count reduces the amount of time that the server waits for a TCP acknowledgement before closing the socket. Select the Standard Configuration setting unless this AE Services server is used by TSAPI routing applications.

**Warning:** This setting applies to all TCP and TLS sockets on the AE Server and so it should be used with caution.



## 6.5. Restart Service

Select **Maintenance** → **Service Controller** from the left pane, to display the **Service Controller** screen in the right pane. Check **TSAPI Service** as shown below, and click **Restart Service**.



**Application Enablement Services**  
Management Console

Welcome: User  
Last login: Tue Jan 20 06:55:31 2015 from 10.32.39.20  
Number of prior failed login attempts: 0  
HostName/IP: aes\_125\_72/10.64.125.72  
Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_SP  
SW Version: 6.3.3.1.10-0  
Server Date and Time: Tue Jan 20 06:57:01 MST 2015  
HA Status: Not Configured

Maintenance | Service Controller

Home | Help | Logout

▶ AE Services

▶ Communication Manager Interface

▶ High Availability

▶ Licensing

▼ Maintenance

▶ Date Time/NTP Server

▶ Security Database

▶ Service Controller

▶ Server Data

▶ Networking

▶ Security

▶ Status

▶ User Management

Service Controller

Service	Controller Status
<input type="checkbox"/> ASAI Link Manager	Running
<input type="checkbox"/> DMCC Service	Running
<input type="checkbox"/> CVLAN Service	Running
<input type="checkbox"/> DLG Service	Running
<input type="checkbox"/> Transport Layer Service	Running
<input checked="" type="checkbox"/> TSAPI Service	Running

For status on actual services, please use [Status and Control](#)

Start

Stop

Restart Service

Restart AE Server

Restart Linux

Restart Web Server

## 6.6. Obtain Tlink Name

Select **Security** → **Security Database** → **Tlinks** from the left pane. The **Tlinks** screen shows a listing of the Tlink names. A new Tlink name is automatically generated for the TSAPI service. Locate the Tlink name associated with the relevant switch connection, which would use the name of the switch connection as part of the Tlink name. Make a note of the associated Tlink name, to be used later for configuring Callback.

In this case, the associated Tlink name is “AVAYA#S8800#CSTA#AES\_125\_72”. Note the use of the switch connection “S8800” from **Section 6.3** as part of the Tlink name.

The screenshot displays the Avaya Application Enablement Services Management Console. The top header includes the Avaya logo, the title "Application Enablement Services Management Console", and a welcome message for the user. The main navigation pane on the left lists various services, with "Security" expanded to show "Security Database" and "Tlinks" selected. The main content area shows the "Tlinks" configuration page, which includes a "Tlink Name" field with two radio button options: "AVAYA#S8300D#CSTA#AES\_125\_72" and "AVAYA#S8800#CSTA#AES\_125\_72". The second option is selected. A "Delete Tlink" button is also present.

Welcome: User  
Last login: Tue Dec 9 08:04:15 2014 from 10.32.39.20  
Number of prior failed login attempts: 0  
HostName/IP: aes\_125\_72/10.64.125.72  
Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_SP  
SW Version: 6.3.3.1.10-0  
Server Date and Time: Tue Dec 09 08:04:56 MST 2014  
HA Status: Not Configured

Security | Security Database | Tlinks Home | Help | Logout

AE Services  
Communication Manager Interface  
High Availability  
Licensing  
Maintenance  
Networking  
Security  
Account Management  
Audit  
Certificate Management  
Enterprise Directory  
Host AA  
PAM  
Security Database  
Control  
CTI Users  
Devices  
Device Groups  
Tlinks

Tlinks

Tlink Name:

☐ AVAYA#S8300D#CSTA#AES\_125\_72

☒ AVAYA#S8800#CSTA#AES\_125\_72


Delete Tlink



## 6.7. Administer Callback User

Select **User Management** → **User Admin** → **Add User** from the left pane, to display the **Add User** screen in the right pane.

Enter desired values for **User Id**, **Common Name**, **Surname**, **User Password**, and **Confirm Password**. For **CT User**, select “Yes” from the drop-down list. Retain the default value in the remaining fields.

**Application Enablement Services**  
Management Console

Welcome: User  
Last login: Tue Jan 6 12:12:42 2015 from 10.32.39.20  
Number of prior failed login attempts: 0  
HostName/IP: aes\_125\_72/10.64.125.72  
Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_SP  
SW Version: 6.3.3.1.10-0  
Server Date and Time: Tue Jan 06 12:14:09 MST 2015  
HA Status: Not Configured

User Management | User Admin | Add User

Home | Help | Logout

▶ AE Services

▶ Communication Manager Interface

▶ High Availability

▶ Licensing

▶ Maintenance

▶ Networking

▶ Security

▶ Status

▼ User Management

▶ Service Admin

▼ User Admin

■ Add User

■ Change User Password

■ List All Users

■ Modify Default Users

■ Search Users

▶ Utilities

▶ Help

Add User

Fields marked with \* can not be empty.

\* User Idvht

\* Common Namevht

\* Surnamevht

\* User Password\*\*\*\*\*

\* Confirm Password\*\*\*\*\*

Admin Note

Avaya RoleNone ▼

Business Category

Car License

CM Home

Css Home

CT UserYes ▼

Department Number

Display Name

Employee Number

Employee Type

Enterprise Handle

Given Name

## 6.8. Verify Security Database

Select **Security** → **Security Database** → **Control** from the left pane, to display the **SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services** screen in the right pane.

Make certain that **Enable SDB for TSAPI Service, JTAPI and Telephony Web Services** retained the default value of unchecked. In the event that security database is used by the customer with this parameter already enabled, then follow [2] to configure access privileges for the Callback user from **Section 6.7**.

The screenshot displays the Avaya Application Enablement Services Management Console. The top header includes the Avaya logo, the title "Application Enablement Services Management Console", and a welcome message for the user. The main navigation pane on the left lists various service categories, with "Security" expanded to show sub-options like "Account Management", "Audit", "Certificate Management", "Enterprise Directory", "Host AA", "PAM", "Security Database", and "Control". The "Control" option is selected. The right pane shows the "SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services" configuration page. It contains two unchecked checkboxes: "Enable SDB for DMCC Service" and "Enable SDB for TSAPI Service, JTAPI and Telephony Web Services", followed by an "Apply Changes" button.

AVAYA Application Enablement Services Management Console

Welcome: User  
Last login: Tue Jan 20 06:55:31 2015 from 10.32.39.20  
Number of prior failed login attempts: 0  
HostName/IP: aes\_125\_72/10.64.125.72  
Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_SP  
SW Version: 6.3.3.1.10-0  
Server Date and Time: Tue Jan 20 06:57:01 MST 2015  
HA Status: Not Configured

Security | Security Database | Control Home | Help | Logout

AE Services  
Communication Manager Interface  
High Availability  
Licensing  
Maintenance  
Networking  
Security  
Account Management  
Audit  
Certificate Management  
Enterprise Directory  
Host AA  
PAM  
Security Database  
Control

SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services

☐ Enable SDB for DMCC Service  
☐ Enable SDB for TSAPI Service, JTAPI and Telephony Web Services  
Apply Changes

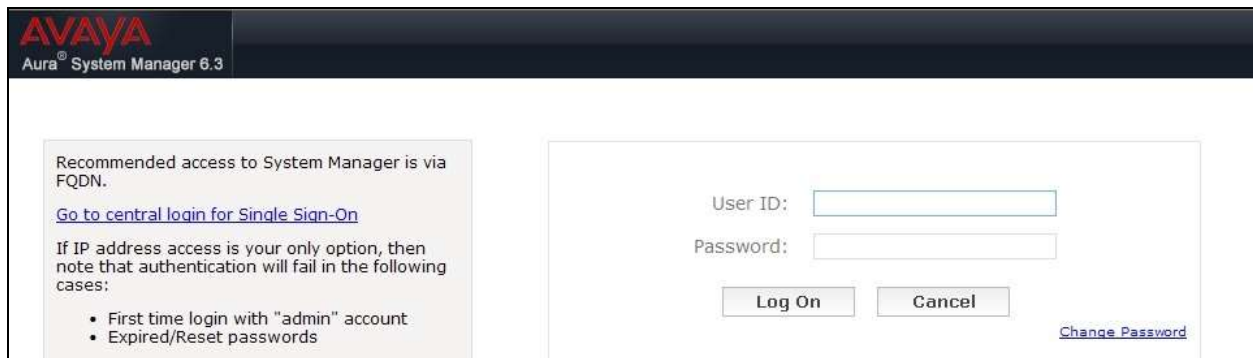
## 7. Configure Avaya Aura® Session Manager

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

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

### 7.1. Launch System Manager

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



The screenshot shows the Avaya Aura System Manager 6.3 login interface. The header includes the Avaya logo and the text 'Aura® System Manager 6.3'. The main content area is divided into two sections. The left section contains a message: '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

'. The right section contains a login form with fields for 'User ID:' and 'Password:', a 'Log On' button, a 'Cancel' button, and a [Change Password](#) link.

### 7.2. Administer Locations

In the subsequent screen (not shown), select **Elements → Routing** to display the **Introduction to Network Routing Policy** screen below. Select **Routing → Locations** from the left pane, and click **New** in the subsequent screen (not shown) to add a new location for IVG.



The screenshot shows the Avaya Aura System Manager 6.3 interface with the 'Routing' tab selected. The left navigation pane shows 'Routing' expanded with sub-items: 'Domains', 'Locations', 'Adaptations', 'SIP Entities', and 'Entity Links'. The main content area displays the 'Introduction to Network Routing Policy' screen. The breadcrumb trail is 'Home / Elements / Routing'. The page title is 'Introduction to Network Routing Policy'. The text states: 'Network Routing Policy consists of several routing applications like "Domains", "Locations", "SIP Entities", etc. The recommended order to use the routing applications (that means the overall routing workflow) to configure your network configuration is as follows:'. A 'Help ?' link is visible in the top right corner.

The **Location Details** screen is displayed. In the **General** sub-section, enter a descriptive **Name** and optional **Notes**. Retain the default values in the remaining fields.

AVAYA  
Aura® System Manager 6.3

Home Routing x

Home / Elements / Routing / Locations

Location Details

Help ?

Commit Cancel

General

\* Name: VHT-Loc

Notes: VHT IVG

Dial Plan Transparency in Survivable Mode

Enabled: ☐

Listed Directory Number:

Associated CM SIP Entity:

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

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

1 Item Filter: Enable

IP Address Pattern	Notes
* 10.64.101.207	

Select : All, None

Commit Cancel

## 7.3. Administer SIP Entities

Add two new SIP entities, one for IVG and one for the new SIP trunks with Communication Manager.

### 7.3.1. SIP Entity for IVG

Select **Routing** → **SIP Entities** from the left pane, and click **New** in the subsequent screen (not shown) to add a new SIP entity for IVG.

The **SIP Entity Details** screen is displayed. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Name:** A descriptive name.
- **FQDN or IP Address:** The IP address of IVG.
- **Type:** “SIP Trunk”
- **Notes:** Any desired notes.
- **Location:** Select the Callback location name from **Section 7.2**.
- **Time Zone:** Select the applicable time zone.

The screenshot shows the Avaya Aura System Manager 6.3 interface. The left navigation pane has 'Routing' expanded, and 'SIP Entities' is selected. The main content area is titled 'SIP Entity Details' and shows the 'General' tab. The form contains the following fields and values:

- Name:** VHT-IVG
- FQDN or IP Address:** 10.64.101.207
- Type:** SIP Trunk
- Notes:** (empty)
- Adaptation:** (empty)
- Location:** VHT-Loc
- Time Zone:** America/Denver
- SIP Timer B/F (in seconds):** 4
- Credential name:** (empty)
- Call Detail Recording:** egress
- Loop Detection Mode:** Off
- SIP Link Monitoring:** Use Session Manager Configuration

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

- **Name:** A descriptive name.
- **SIP Entity 1:** The Session Manager entity name, in this case “DR-SMW”.
- **Protocol:** “UDP”
- **Port:** “5060”
- **SIP Entity 2:** The IVG entity name from this section.
- **Port:** “5060”
- **Connection Policy:** “trusted”

Note that only UDP is supported by IVG.

### Entity Links

Override Port & Transport with DNS SRV: ☐

Add Remove

1 Item
Filter: Enable

<input type="checkbox"/>	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Deny New Service
<input type="checkbox"/>	* SMW2VHT	DR-SMW	UDP	* 5060	VHT-IVG	* 5060	trusted	<input type="checkbox"/>

Select : All, None

### SIP Responses to an OPTIONS Request

Add Remove

0 Items
Filter: Enable

<input type="checkbox"/>	Response Code & Reason Phrase	Mark Entity Up/Down	Notes
--------------------------	-------------------------------	---------------------	-------

Commit Cancel

### 7.3.2. SIP Entity for Communication Manager

Select **Routing** → **SIP Entities** from the left pane, and click **New** in the subsequent screen (not shown) to add a new SIP entity for Communication Manager. Note that this SIP entity is used for integration with IVG.

The **SIP Entity Details** screen is displayed. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Name:** A descriptive name.
- **FQDN or IP Address:** The IP address of an existing CLAN or the processor interface.
- **Type:** “CM”
- **Notes:** Any desired notes.
- **Adaptation:** Select any applicable adaptation for Communication Manager.
- **Location:** Select the applicable location for Communication Manager.
- **Time Zone:** Select the applicable time zone.

The screenshot shows the Avaya Aura System Manager 6.3 interface. The left-hand navigation pane is expanded to 'Routing', and 'SIP Entities' is selected. The main content area displays the 'SIP Entity Details' form. The form has a 'General' tab selected. The fields and their values are as follows:

- Name:** DR-CMW-5032
- FQDN or IP Address:** 10.64.125.32
- Type:** CM
- Notes:** CM Port 5032 for VHT
- Adaptation:** (empty dropdown)
- Location:** DR-Loc
- Time Zone:** America/Denver
- SIP Timer B/F (in seconds):** 4
- Credential name:** (empty text field)
- Call Detail Recording:** none
- Loop Detection Mode:** Off
- SIP Link Monitoring:** Use Session Manager Configuration




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

- **Name:** A descriptive name.
- **SIP Entity 1:** The Session Manager entity name, in this case “DR-SMW”.
- **Protocol:** The signaling group transport method from **Section 5.5**.
- **Port:** The signaling group listen port number from **Section 5.5**.
- **SIP Entity 2:** The Communication Manager entity name from this section.
- **Port:** The signaling group listen port number from **Section 5.5**.
- **Connection Policy:** “trusted”


### Entity Links

Override Port & Transport with DNS ☐  
SRV: ☐

1 Item 								Filter: Enable
<input type="checkbox"/>	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	
<input type="checkbox"/>	* DR-SMW2CMW-5032	DR-SMW ▼	TLS ▼	* 5032	DR-CMW-5032 ▼	* 5032	trusted ▼	

Select : All, None

### SIP Responses to an OPTIONS Request

0 Items 			Filter: Enable
<input type="checkbox"/>	Response Code & Reason Phrase	Mark Entity Up/Down	Notes



## 7.4. Administer Routing Policies

Add two new routing policies, one for IVG and one for the new SIP trunks with Communication Manager.

### 7.4.1. Routing Policy for IVG

Select **Routing** → **Routing Policies** from the left pane, and click **New** in the subsequent screen (not shown) to add a new routing policy for IVG.

The **Routing Policy Details** screen is displayed. In the **General** sub-section, enter a descriptive **Name**, and retain the default values in the remaining fields.

In the **SIP Entity as Destination** sub-section, click **Select** and select the IVG entity name from **Section 7.3.1**. The screen below shows the result of the selection.

AVAYA  
Aura® System Manager 6.3

Home Routing x

Home / Elements / Routing / Routing Policies

Routing Policy Details

Commit Cancel Help ?

General

\* Name: To-VHT

Disabled: ☐

\* Retries: 0

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
VHT-IVG	10.64.101.207	SIP Trunk	

## 7.4.2. Routing Policy for Communication Manager

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

The **Routing Policy Details** screen is displayed. In the **General** sub-section, enter a descriptive **Name**, and retain the default values in the remaining fields.

In the **SIP Entity as Destination** sub-section, click **Select** and select the Communication Manager entity name from **Section 7.3.2**. The screen below shows the result of the selection.

AVAYA  
Aura System Manager 6.3

Last Logged on at April 10, 2015 2:16 PM  
GO TO... Log off

Home Routing

Home / Elements / Routing / Routing Policies

Routing Policy Details

Commit Cancel Help ?

General

\* Name: To-DR-CMW-5032

Disabled: ☐

\* Retries: 0

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
DR-CMW-5032	10.64.125.32	CM	CM Port 5032 for VHT

## 7.5. Administer Dial Patterns

Add a new dial pattern for IVG, and update existing dial patterns for Communication Manager.

### 7.5.1. Dial Pattern for IVG

Select **Routing** → **Dial Patterns** from the left pane, and click **New** in the subsequent screen (not shown) to add a new dial pattern to reach IVG. The **Dial Pattern Details** screen is displayed. In the **General** sub-section, enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Pattern:** A dial pattern to match, in this case “32”.
- **Min:** The minimum number of digits to match.
- **Max:** The maximum number of digits to match.
- **SIP Domain:** The signaling group domain name from **Section 5.5**.

In the **Originating Locations and Routing Policies** sub-section, click **Add** and create a new policy for reaching IVG. In the compliance testing, the policy allowed for call origination from the Communication Manager location “DR-Loc”, and the IVG routing policy from **Section 7.4.1** was selected as shown below.

The screenshot displays the Avaya Aura System Manager 6.3 interface. The left navigation pane shows the 'Routing' menu expanded, with 'Dial Patterns' selected. The main content area shows the 'Dial Pattern Details' screen. The 'General' section is active, displaying the following fields:

- Pattern:** 32
- Min:** 5
- Max:** 5
- Emergency Call:** ☐
- Emergency Priority:** 1
- Emergency Type:**
- SIP Domain:** dr220.com
- Notes:**

The 'Originating Locations and Routing Policies' section is also visible, showing a table with one item:

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

## 7.5.2. Dial Pattern for Communication Manager

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

In the **Originating Locations and Routing Policies** sub-section, click **Add** and create a new entry as necessary for calls from IVG. In the compliance testing, the new entry allowed for call origination from the IVG location from **Section 7.2**, and the Communication Manager routing policy from **Section 7.4.2** was selected as shown below. Retain the default values in the remaining fields.

The screenshot displays the Avaya Aura System Manager 6.3 interface. The left navigation pane shows the 'Routing' section expanded, with 'Dial Patterns' selected. The main content area is titled 'Dial Pattern Details' and includes a 'Commit' button. The 'General' tab is active, showing the following fields:

- \* Pattern: 6
- \* Min: 5
- \* Max: 5
- Emergency Call: ☐
- Emergency Priority: 1
- Emergency Type:
- SIP Domain: dr220.com
- Notes: To CMW

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

Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
DR-Loc		To-DR-CMW	0	<input type="checkbox"/>	DR-CMW	
VHT-Loc	VHT IVG	To-DR-CMW-5032	0	<input type="checkbox"/>	DR-CMW-5032	

At the bottom of the table, there is a 'Select' dropdown menu with options 'All' and 'None'.

Follow the procedures in this section to make similar changes to any other applicable dial patterns that IVG will be using to reach Communication Manager. In the compliance testing, one other dial pattern to reach the PSTN via Communication Manager was applicable and updated, as shown below.

AVAYA  
Aura System Manager 6.3

Last Logged on at April 10, 2015 10:16 AM  
Log off

Home Routing

Home / Elements / Routing / Dial Patterns

Dial Pattern Details

Commit Cancel

General

\* Pattern: 9

\* Min: 11

\* Max: 11

Emergency Call: ☐

Emergency Priority: 1

Emergency Type:

SIP Domain: dr220.com

Notes: To PSTN

Originating Locations and Routing Policies

Add Remove

2 Items Filter: Enable

Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
DR-Loc		To-DR-CMW	0	<input type="checkbox"/>	DR-CMW	
VHT-Loc	VHT IVG	To-DR-CMW-5032	0	<input type="checkbox"/>	DR-CMW-5032	

Select : All, None

## 8. Configure VHT IVG

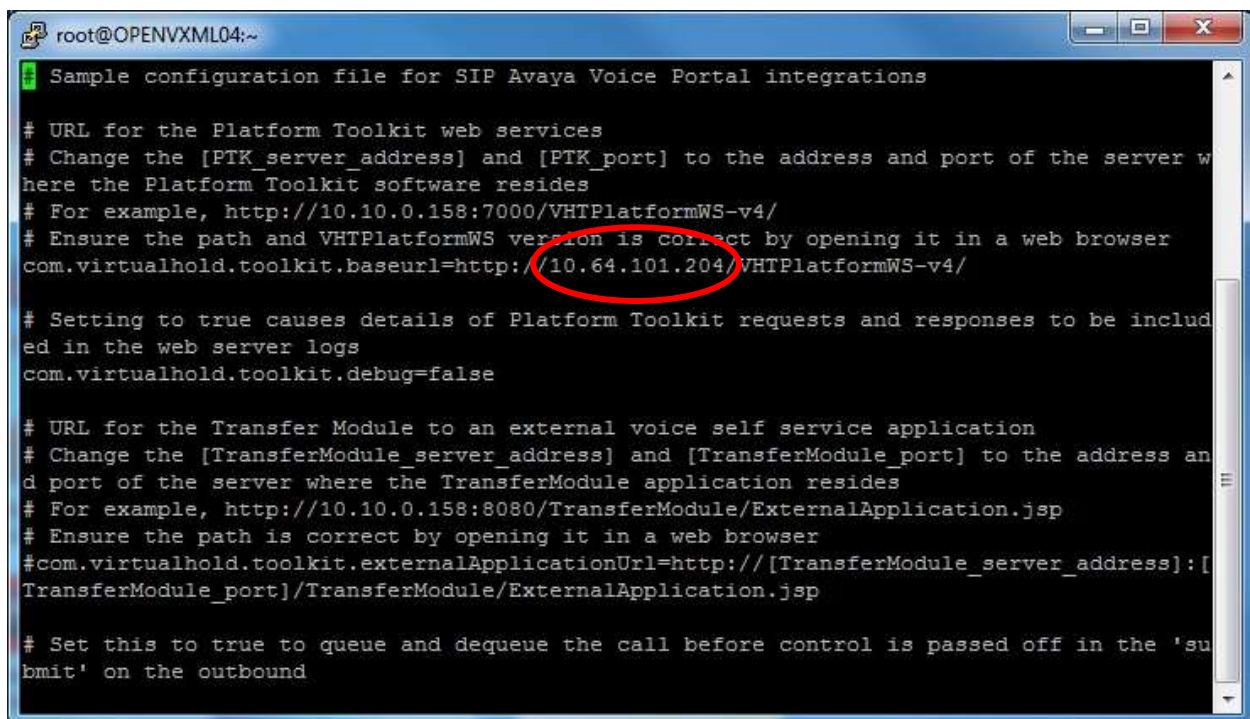
This section provides the procedures for configuring IVG. The procedures include the following areas:

- Administer toolkit properties
- Administer assigned extensions

The configuration of IVG is typically performed by VHT integration engineers. The procedural steps are presented in these Application Notes for informational purposes.

### 8.1. Administer Toolkit Properties

Log in to the Linux shell of IVG. Use the “vi /etc/VirtualHold/toolkit.properties” command to edit the file. Locate and replace the string “[PKT\_server\_address]:[PTK\_port]” with the IP address of the Callback server. The screenshot below was captured after the replacement.



```
root@OPENVXML04:~  
Sample configuration file for SIP Avaya Voice Portal integrations  
  
# URL for the Platform Toolkit web services  
# Change the [PTK_server_address] and [PTK_port] to the address and port of the server w  
here the Platform Toolkit software resides  
# For example, http://10.10.0.158:7000/VHTPlatformWS-v4/  
# Ensure the path and VHTPlatformWS version is correct by opening it in a web browser  
com.virtualhold.toolkit.baseurl=http://10.64.101.204/VHTPlatformWS-v4/  
  
# Setting to true causes details of Platform Toolkit requests and responses to be includ  
ed in the web server logs  
com.virtualhold.toolkit.debug=false  
  
# URL for the Transfer Module to an external voice self service application  
# Change the [TransferModule_server_address] and [TransferModule_port] to the address an  
d port of the server where the TransferModule application resides  
# For example, http://10.10.0.158:8080/TransferModule/ExternalApplication.jsp  
# Ensure the path is correct by opening it in a web browser  
#com.virtualhold.toolkit.externalApplicationUrl=http://[TransferModule_server_address]:[  
TransferModule_port]/TransferModule/ExternalApplication.jsp  
  
# Set this to true to queue and dequeue the call before control is passed off in the 'su  
bmit' on the outbound
```

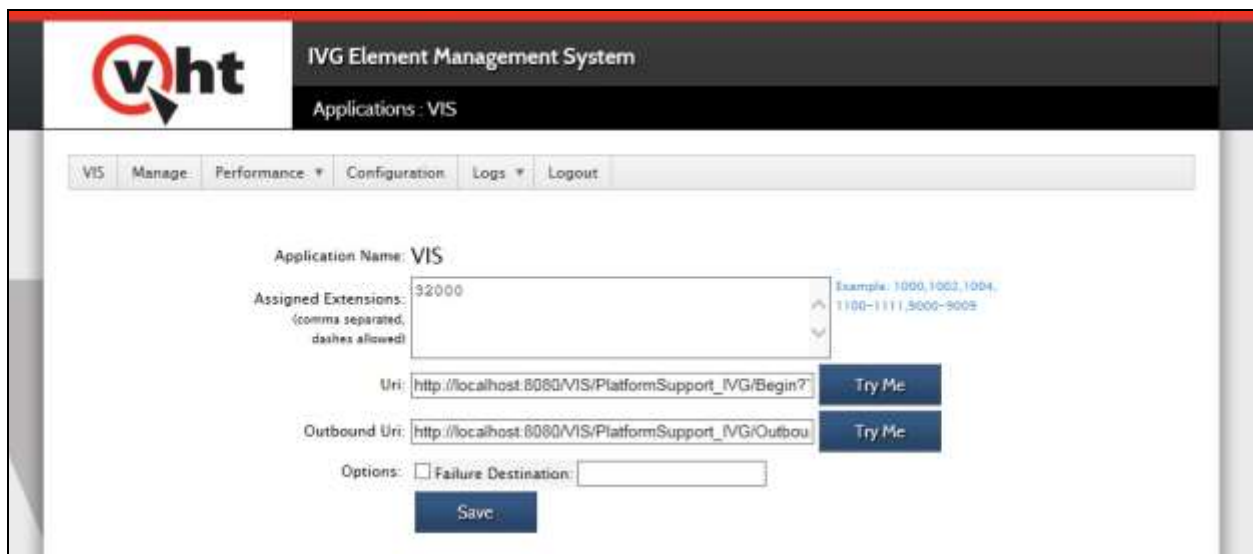
## 8.2. Administer Assigned Extensions

Access the IVG web interface by using the URL “http://ip-address:8080/ ivg-ems” in an Internet browser window, where “ip-address” is the IP address of IVG. Log in using the appropriate credentials.



The screenshot shows the VHT login page. At the top left is the VHT logo with the tagline "Empowering customer conversations". Below the logo is a "Sign In:" section. To the left of the login fields, there is a "Technical Support:" section with the text: "VHT technical support is available 24 hours a day, seven days a week, 365 days a year." and contact information: "866-670-2223" and "support@virtualhold.com". The login fields include "Username:" and "Password:" with corresponding input boxes. There is a "Remember Me" checkbox and a "Login" button. At the bottom, it says "Copyright 2014 Virtual Hold Technology LLC".

The **IVG Element Management System** screen is displayed. For **Assigned Extensions**, enter the extension assigned to IVG, in this case “32000”. Retain the default values in the remaining fields.



The screenshot shows the IVG Element Management System configuration page. At the top left is the VHT logo. The page title is "IVG Element Management System" and the application is "VIS". Below the title is a navigation bar with links: "VIS", "Manage", "Performance", "Configuration", "Logs", and "Logout". The main content area shows the "Application Name: VIS" and "Assigned Extensions: 32000" (with a note: "comma separated, dashes allowed"). There is a "Uri:" field with the value "http://localhost:8080/VIS/PlatformSupport\_IVG/Begin?" and a "Try Me" button. Below that is an "Outbound Uri:" field with the value "http://localhost:8080/VIS/PlatformSupport\_IVG/Outbou" and a "Try Me" button. At the bottom, there is an "Options:" section with a checkbox for "Failure Destination:" and a "Save" button.



## 9. Configure VHT Callback

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

- Administer Genesys T-Server for Avaya TSAPI
- Launch configuration wizard
- Administer switch connection
- Administer agent groups
- Administer queues
- Administer callback and holding queues
- Administer incoming extensions
- Administer phone number configurations
- Administer route destinations

The configuration of Callback is typically performed by VHT integration engineers, and the configuration of Genesys T-Server for Avaya TSAPI is typically performed by the end customer. The procedural steps are presented in these Application Notes for informational purposes.

### 9.1. Administer Genesys T-Server for Avaya TSAPI

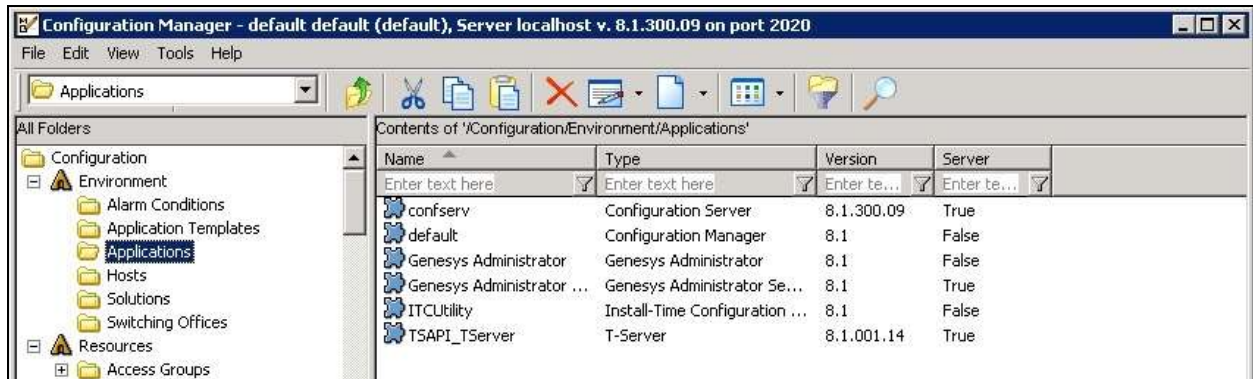
From the Callback server, navigate to **Start → All Programs → Genesys Solutions → Framework → Configuration Manager → Start Configuration Manager** to launch the Configuration Manager application, and log in using the appropriate credentials.





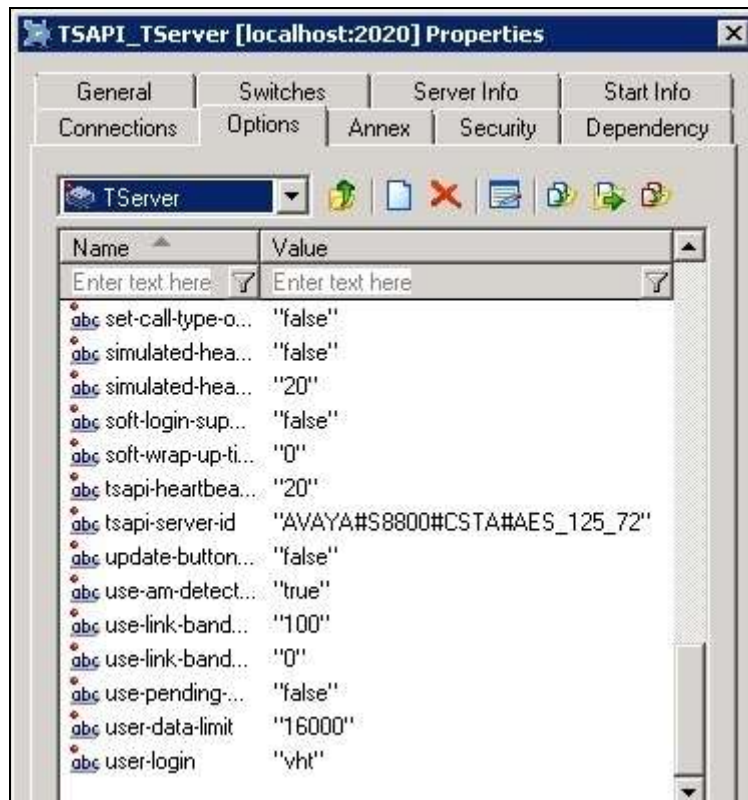
### 9.1.1. Application

Select **Configuration** → **Environment** → **Applications** in the left pane to display a list of pre-existing applications. Double click on the applicable application, in this case “TSAPI\_TServer”.



The screen below is displayed next. Select “TServer” from the drop-down list. Enter the following values for the specified fields, and retain the default values for the remaining fields.

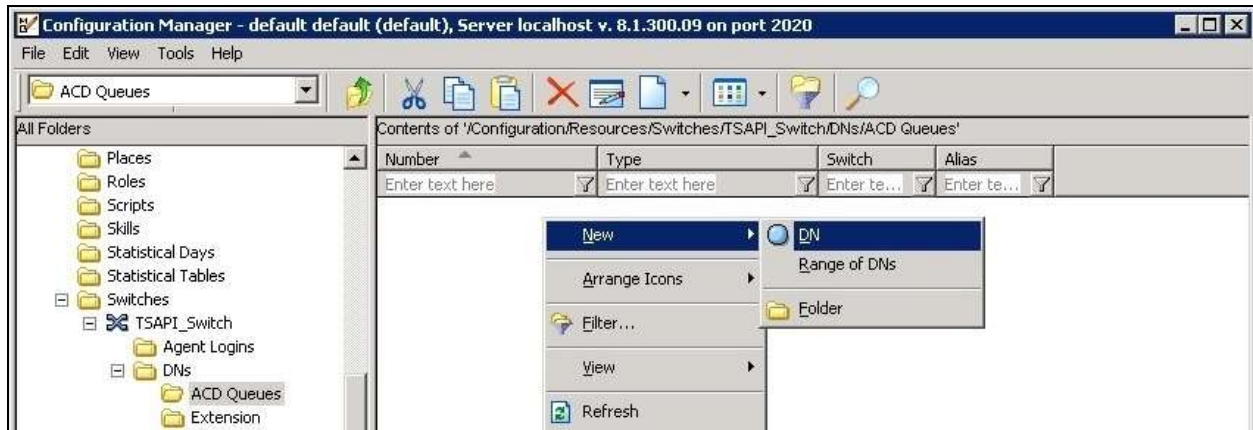
- **tsapi-server-id:** The Tlink name from **Section 6.6**.
- **user-login:** The Callback user credentials from **Section 6.7**.
- **password:** The Callback user credentials from **Section 6.7**.



### 9.1.2. ACD Queues

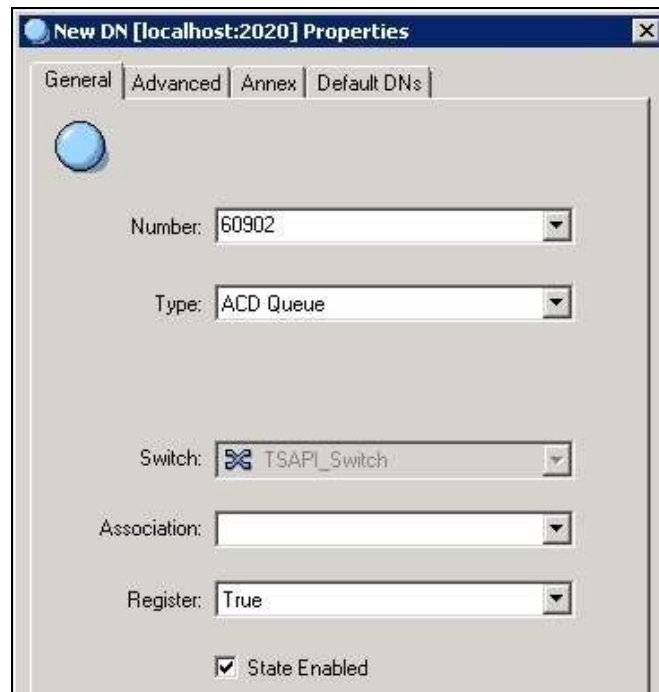
Expand and navigate to **Configuration → Resources → Switches → TSAPI\_Switch → DN** in the left pane, where **TSAPI\_Switch** is the name of the pre-existing switch.

Select **ACD Queues** in the left pane. Right click in the empty right pane and select **New → DN** to create an entry for the Hold VDN **Section 5.4.2**.



In the **General** tab, enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Number:** The Hold VDN extension from **Section 5.4.2**.
- **Type:** “ACD Queue”



Select the **Advanced** tab. For **Switch-specific Type**, enter “2” as shown below. Retain the default values in the remaining fields.

The screenshot shows the 'New DN [localhost:2020] Properties' dialog box with the 'Advanced' tab selected. The fields are as follows:

- Alias: [Empty]
- Route Type: Default
- Group: [None]
- Use Override: ☒ [Empty]
- Login ID: [Empty]
- Switch-specific Type: 2
- Number of Trunks: 0
- Cost contract: [None]
- Site: [None]

Buttons at the bottom: OK, Cancel, Make New, Help.

Repeat the same procedures to create an entry for the Callback VDN from **Section 5.4.3**. The screenshot below shows the two entries that were created in the compliance testing.

The screenshot shows the Configuration Manager interface. The left pane shows the folder structure: Switches > TSAPI\_Switch > DNs > ACD Queues. The right pane shows the contents of the selected folder as a table.

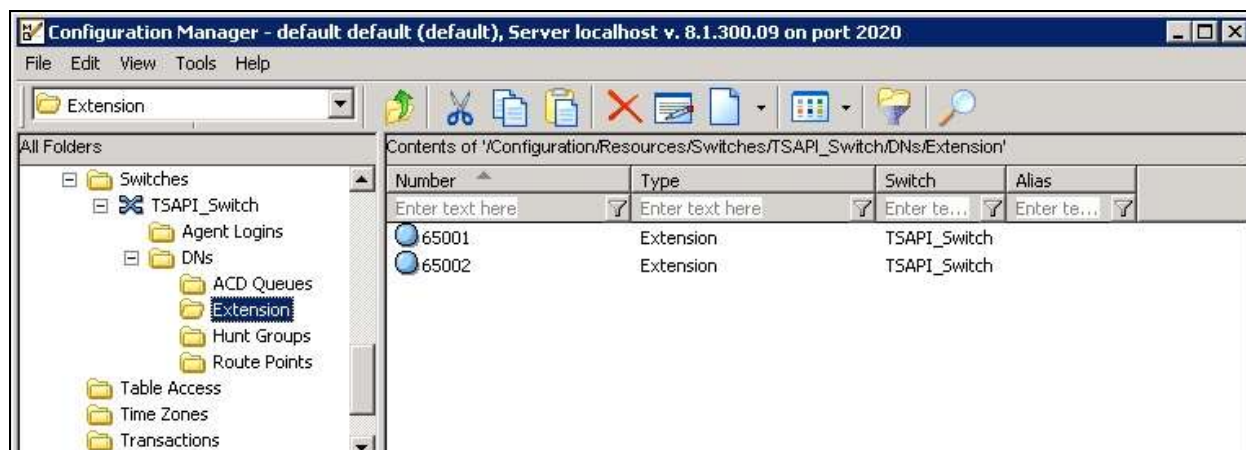
Number	Type	Switch	Alias
60902	ACD Queue	TSAPI_Switch	
60903	ACD Queue	TSAPI_Switch	

At the bottom, it indicates '2 object(s)' and 'ON line'.

### 9.1.3. Extension

Select **Extension** in the left pane. Right click in the empty right pane and select **New → DN** to create an entry for each agent station from **Section 3**. Enter the following values for the specified fields, and retain the default values for the remaining fields. The screenshot below shows the entries that were created.

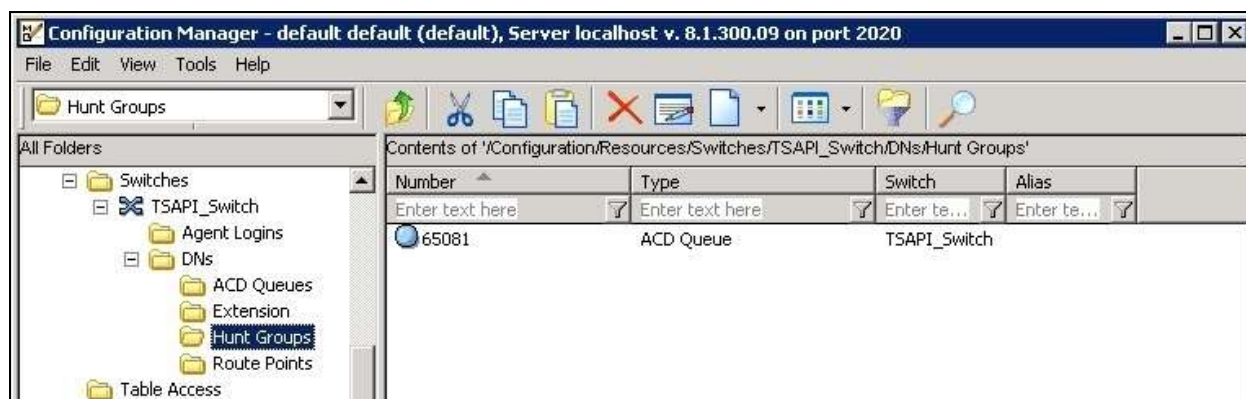
- **Number:** The agent station extension from **Section 3**.
- **Type:** “Extension”



### 9.1.4. Hunt Groups

Select **Hunt Groups** in the left pane. Right click in the empty right pane and select **New → DN** to create an entry for the skill group from **Section 3**. Enter the following values for the specified fields, and retain the default values for the remaining fields. The screenshot below shows the entry that was created.

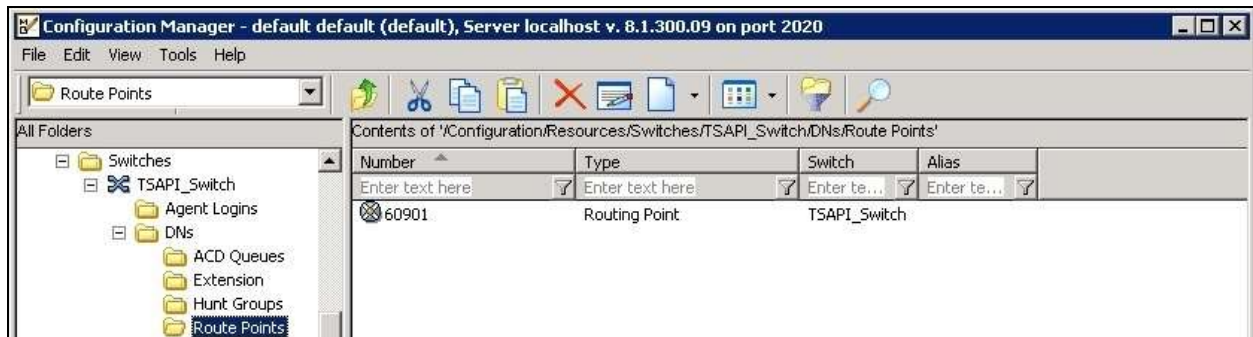
- **Number:** The skill group extension from **Section 3**.
- **Type:** “ACD Queue”



### 9.1.5. Route Points

Select **Route Points** in the left pane. Right click in the empty right pane and select **New → DN** to create an entry for the Entry VDN from **Section 5.4.1**. Enter the following values for the specified fields, and retain the default values for the remaining fields. The screenshot below shows the entry that was created.

- **Number:** The Entry VDN extension from **Section 5.4.1**.
- **Type:** “Routing Point”



### 9.2. Launch Configuration Wizard

From the Callback server, navigate to **Start → All Programs → Virtual Hold Technology → Configuration → VHT Configuration Wizard** to launch the wizard. The **Welcome to the Virtual Hold Configuration Wizard** screen is displayed. Click **Configure** to proceed.





### 9.3. Administer Switch Connection

The **Switch Connection** screen is displayed. Click **Add** to create a connection to the switch.



The **Switch Types** screen is displayed next. For **Switch Type**, select “TIALGenesys” from the drop-down list. Note that the value of **Site Name** was automatically populated, and was created as part of installation.

Retain the default values in the remaining fields.



The **Genesys CTI T-Server Connections** screen is displayed. Click **Add** to create a connection (not shown).



The **Genesys CTI** screen is displayed next. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **T-Server Switch Name:** The application switch name from **Section 9.1.2**.
- **Host IP Address A:** The IP address of the Callback server.
- **Host IP Address B:** The IP address of the Callback server.

Site Name:	VHT
T-Server Switch Name:	TSAPI_Switch
Host IP Address A:	10.64.101.204
Host Port A:	4000
Host IP Address B:	10.64.101.204
Host Port B:	
Redundancy Mode:	None
Reconnect Interval:	2000
Register All Devices:	FALSE

Create Close

## 9.4. Administer Agent Groups

The **Agent Groups** screen is displayed next. Click **Add**.



The screen below is displayed next. This screen is used to define the skill group. Retain the default value for **Site Name**. For **Starting Agent Group**, enter “x:y:z”, where “x” is the desired agent group name, “y” is the switch name from **Section 9.1.2**, and “y” is the skill group extension from **Section 3**.

In the compliance testing, the value “VHT\_TEST:TSAPI\_Switch:65081” was used.





## 9.5. Administer Queues

Continue with the wizard until the **Queues** screen is displayed (not shown). Click **Add** to create queues.

The **Queues Setup** screen is displayed next. Consult reference [3] for desired configuration of these parameters. The screenshot below shows the values used in the compliance testing.

The screenshot shows the 'Queues Setup' dialog box with the following configuration:

- Site Name:** VHT
- Queue ID:** VHT\_Test
- Buttons:** Use Production Defaults, Use Test Defaults
- QueueSettings:**
  - Op Mode:** Normal
  - Turn On Threshold (sec):** 0
  - Call Handle Time (secs):** 45
  - No Ans Period (sec):** 60
  - Name:** VHT\_Test
  - Script Number:** 1
  - Busy Attempts:** 3
  - Try Again Attempts:** 3
  - Mode:** Predictive
  - Agents Staffed Override:** TRUE
  - Busy Period (secs):** 60
  - Try Again Period (secs):** 60
  - Group:** VHT\_Test
  - Callback Threshold (secs):** 45
  - No Ans Attempts:** 3
  - Max Attempts:** 5
  - Default Number of Agents:** 1
- Business Hours:**
  - Day Of Week:** Sun, Mon, Tue, Wed, Thu, Fri, Sat (all checked)
  - Time Begin:** 00:00
  - Time End:** 23:59
- Callbacks Offered:**
  - Day Of Week:** Sun, Mon, Tue, Wed, Thu, Fri, Sat (all checked)
  - Time Begin:** 00:00
  - Time End:** 23:59
- Callbacks Allowed:**
  - Day Of Week:** Sun, Mon, Tue, Wed, Thu, Fri, Sat (all checked)
  - Sched callbacks allowed/15 min:** 15
- Buttons:** Create, Close

## 9.6. Administer Callback and Holding Queues

Continue with the wizard until the **Callback and Holding Queues** screen is displayed (not shown). Click **Add** to create queues. The screen below is displayed next.

In the **Callback Queues** sub-section, enter the Callback VDN extension from **Section 5.4.3** for **Callback Queue ID**. For **Transfer Device**, enter “sip:x@y”, where “x” is the Callback VDN extension, and “y” is the IP address of the Session Manager signaling interface.

In the **Holding Queues** sub-section, enter the Hold VDN extension from **Section 5.4.2** for **Holding Queue ID**. For **Route Device** and **Transfer Device**, enter “sip:x@y”, where “x” is the Hold VDN extension, and “y” is the IP address of the Session Manager signaling interface.

Retain the default values for the remaining fields.

Site Name: VHT

T-Server Switch Name: TSAPI\_Switch

Callback Queues

☒ Use T-Server Switch Name prefix

Callback Queue ID\*: 60903

Transfer Device: sip:60903@10.64.10

Create

Holding Queues

☒ Use T-Server Switch Name prefix

Holding Queue ID\*: 60902

Route Device: sip:60902@10.64.10

Transfer Device: sip:60902@10.64.10

Create

\*Please see the deployment guide before submitting this form. The syntax of these fields is switch specific.

\* Verify T-Server Switch Name

Close

## 9.7. Administer Incoming Extensions

Continue with the wizard until the **Incoming Extensions** screen is displayed (not shown). Click **Add** to create an incoming extension for Callback.

The screen below is displayed next. For **Extension**, enter the Entry VDN extension from **Section 5.4.1**. For **Treatment Type**, select “11”.

Retain the default values in the remaining fields.

**Incoming Extensions**

Site Name: VHT

Queue ID: VHT\_Test

T-Server Switch Name: TSAPI\_Switch

**Incoming Extensions**

Extension\*: 60901

Label: Extension

Country ID: 1

Treatment Type: 11

ScriptNumber:

\*Please see the deployment guide before entering a script number here.

IVR Group: IVR

Holding Queue ID: TSAPI\_Switch:60902

Callback Queue ID: TSAPI\_Switch:60903

UnderThreshold Queue ID: TSAPI\_Switch:60902

IB IVR Extension Group: NONE

OB IVR Extension Group: NONE

Create

\* Verify T-Server Switch Name

Close

Repeat the same procedures to create an incoming extension for IVG.

For **Extension**, enter the extension assigned to IVG, in this case “32000”. For **Treatment Type**, select “20”.

Retain the default values in the remaining fields, including blank for **T-Server Switch Name**.

**Incoming Extensions**

Site Name: VHT

Queue ID: VHT\_Test

T-Server Switch Name:

**Incoming Extensions**

Extension\*: 32000

Label: Extension

Country ID: 1

Treatment Type: 20

ScriptNumber:

\*Please see the deployment guide before entering a script number here.

IVR Group: IVR

Holding Queue ID: TSAPI\_Switch:60902

Callback Queue ID: TSAPI\_Switch:60903

UnderThreshold Queue ID: TSAPI\_Switch:60902

IB IVR Extension Group: NONE

OB IVR Extension Group: NONE

Create

\* Verify T-Server Switch Name

Close

## 9.8. Administer Phone Number Configurations

Continue with the wizard until the **Phone Number Configurations** screen is displayed (not shown). Click **Add** to create phone number configuration, the screen below is displayed next.

For **Country Search**, locate the applicable country, which will enable the **Dial Prefix** and **Dial Suffix** fields. For **Dial Prefix**, enter any applicable dialing prefix for the network. For **Dial Suffix**, enter “@y”, where “y” is the IP address of the Session Manager signaling interface.

Retain the default values in the remaining fields.

The screenshot shows a Windows-style dialog box titled "PhoneNumberValidation". It is divided into two panes. The left pane, titled "Update Country Id Dial Prefix and Suffix", contains a "Site Name" dropdown menu set to "VHT", a "Country Search" dropdown menu set to "1 - North America" with a list box below it also showing "1 - North America", a "Dial Prefix" text box containing "9", and a "Dial Suffix" text box containing "@10.64.101.228". The right pane, titled "Update Phone Number Validation Min/Max Length", contains a "Site Name" dropdown menu set to "VHT", a "Country Id" dropdown menu set to "1 - North America", a "Min Length" text box containing "10", and a "Max Length" text box containing "10". Both panes have an "Update" button at the bottom. The entire dialog has a "Close" button at the bottom right.

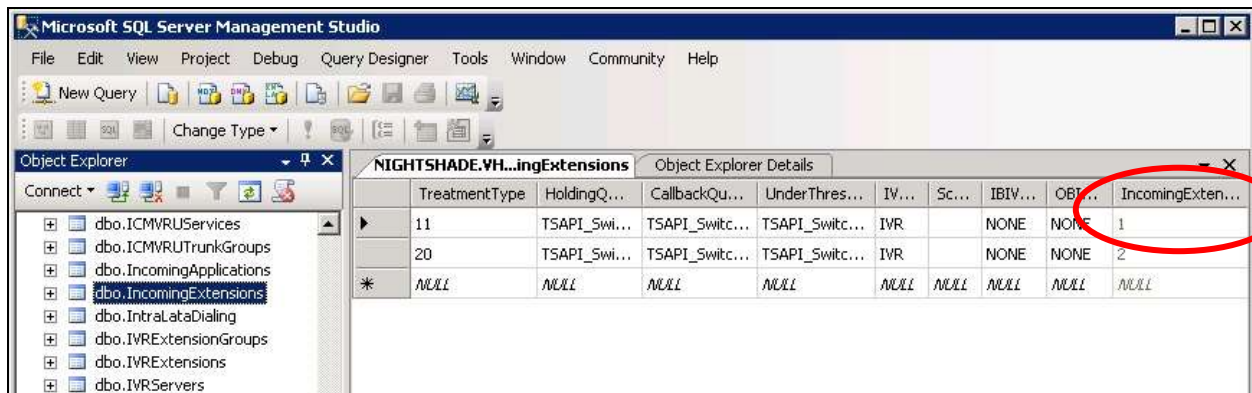
## 9.9. Administer Route Destination

From the Callback server, navigate to **Start → All Programs → Microsoft SQL Server 2008 R2 → SQL Server Management Studio** to launch and connect to the SQL server.



Navigate to **Databases → VHT\_Config → Tables → dbo.IncomingExtensions** in the left pane, right click the entry and select **Edit Top 200 Rows**.

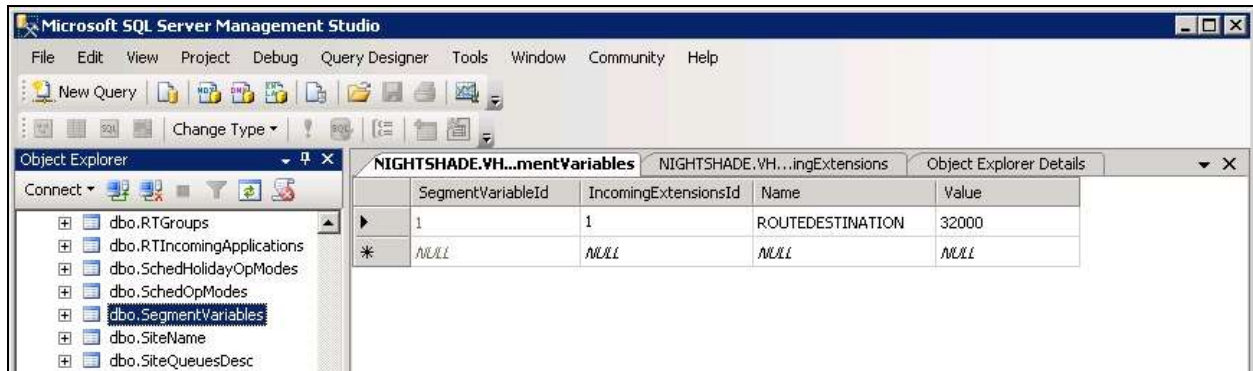
Locate the entry associated with Callback with “11” as **Treatment Type**. Make a note of the associated **IncomingExtensionsId** value, in this case “1”, as shown below.



Scroll down to **dbo.SegmentVariables** in the left pane, right click the entry and select **Edit Top 200 Rows**. Add an entry and enter the following values for the specified fields, and retain the default values for the remaining fields.

- **IncomingExtensionsId:** The value from the **dbo.IncomingExtensions** table from above.
- **Name:** “ROUTEDESTINATION”
- **Value:** The assigned extension to IVG, in this case “32000”.

Restart the VHT Core Monitor and VHT Peripheral Monitor services (not shown).





## 10. Verification Steps

This section provides the tests that can be performed to verify proper configuration of Communication Manager, Application Enablement Services, Session Manager, Callback and IVG.

### 10.1. Verify Avaya Aura® Communication Manager

On Communication Manager, verify the status of the administered CTI link by using the “status aesvcs cti-link” command. Verify that the **Service State** is “established” for the CTI link number administered in **Section 5.2**, as shown below.

```
status aesvcs cti-link
```

AE SERVICES CTI LINK STATUS						
CTI Link	Version	Mnt Busy	AE Services Server	Service State	Msgs Sent	Msgs Rcvd
1		no		down	0	0
2	6	no	aes_125_72	established	259	261

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

```
status trunk 32
```

TRUNK GROUP STATUS			
Member	Port	Service State	Mtce Connected Ports Busy
0032/001	T00113	in-service/idle	no
0032/002	T00114	in-service/idle	no
0032/003	T00115	in-service/idle	no
0032/004	T00116	in-service/idle	no
0032/005	T00117	in-service/idle	no
0032/006	T00118	in-service/idle	no
0032/007	T00119	in-service/idle	no
0032/008	T00120	in-service/idle	no
0032/009	T00121	in-service/idle	no
0032/010	T00122	in-service/idle	no



Verify the status of the SIP signaling groups by using the “status signaling-group n” command, where “n” is the signaling group number administered in **Section 5.5**. Verify that the **Group State** is “in-service”, as shown below.

```
status signaling-group 32
                        STATUS SIGNALING GROUP


      Group ID: 32
      Group Type: sip

      Group State: in-service
```

## 10.2. Verify Avaya Aura® Application Enablement Services

On Application Enablement Services, verify the status of the TSAPI link by selecting **Status → Status and Control → TSAPI Service Summary** from the left pane. The **TSAPI Link Details** screen is displayed.

Verify the **Status** is “Talking” for the TSAPI link administered in **Section 6.3**, and that the **Associations** column reflects the number of VDNs from **Section 5.3**.



**Application Enablement Services**  
 Management Console

Welcome: User  
 Last login: Wed Apr 15 07:17:34 2015 from 10.32.39.20  
 Number of prior failed login attempts: 0  
 HostName/IP: aes\_125\_72/10.64.125.72  
 Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_SP  
 SW Version: 6.3.3.1.10-0  
 Server Date and Time: Wed Apr 15 07:59:32 MDT 2015  
 HA Status: Not Configured

Status | Status and Control | TSAPI Service Summary
 Home | Help | Logout

AE Services  
 Communication Manager  
 Interface  
 High Availability  
 Licensing  
 Maintenance  
 Networking  
 Security  
 Status
 

Alarm Viewer  
 Log Manager  
 Logs  
 Status and Control
 

- CVLAN Service Summary
- DLG Services Summary
- DMCC Service Summary
- Switch Conn Summary
- TSAPI Service Summary

**TSAPI Link Details**  
☐ Enable page refresh every 60 seconds
 

	Link	Switch Name	Switch CTI Link ID	Status	Since	State	Switch Version	Associations	Msgs to Switch	Msgs from Switch	Msgs Period
+	1	S8800	2	Talking	Fri Jan 2 12:46:50 2015	Online	16	6	266	264	30
-	2	S8300D	1	Switch Down	Mon Mar 30 14:48:11 2015	Online	16	0	0	0	30

For service-wide information, choose one of the following:

### 10.3. Verify Avaya Aura® Session Manager

From the System Manager home page (not shown), select **Elements** → **Session Manager** to display the **Session Manager Dashboard** screen (not shown).

Select **Session Manager** → **System Status** → **SIP Entity Monitoring** from the left pane to display the **SIP Entity Link Monitoring Status Summary** screen. Click the IVG entity name from **Section 7.3.1**.

**AVAYA**  
Aura® System Manager 6.3

Last Logged on at April 14, 2015 4:30 PM  
Go to... Log off

Home / Elements / Session Manager / System Status / SIP Entity Monitoring

### SIP Entity Link Monitoring Status Summary

This page provides a summary of Session Manager SIP entity link monitoring status.

#### SIP Entities Status for All Monitoring Session Manager Instances

Run Monitor

1 Items Refresh Filter: Enable

Session Manager	Type	Monitored Entities					Total
		Down	Partially Up	Up	Not Monitored	Deny	
<input type="checkbox"/> <a href="#">DR-SMW</a>	Core	2	0	5	0	0	7

Select: All, None

#### All Monitored SIP Entities

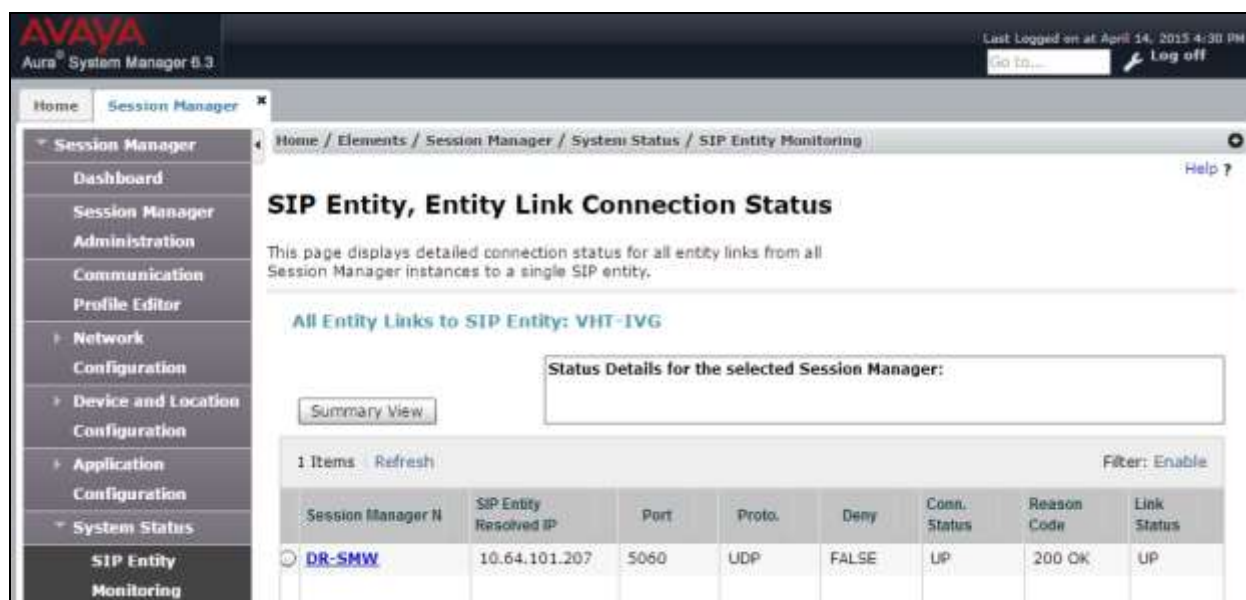
Run Monitor

7 Items Refresh Filter: Enable

SIP Entity Name
<input type="checkbox"/> <a href="#">DR-AAM</a>
<input type="checkbox"/> <a href="#">DR-CMW</a>
<input type="checkbox"/> <a href="#">DR-CMW-5032</a>
<input type="checkbox"/> <a href="#">NJ-IP500V2</a>
<input type="checkbox"/> <a href="#">DR-IPOSE</a>
<input type="checkbox"/> <a href="#">DR-IP500V2</a>
<input type="checkbox"/> <a href="#">VHT-IVG</a>

Select: All, None

The **SIP Entity, Entity Link Connection Status** screen is displayed. Verify that the **Conn. Status** and **Link Status** are “UP”, as shown below.



**AVAYA**  
Aura System Manager 6.3

Last Logged on at April 14, 2015 4:30 PM  
Log off

Home / Elements / Session Manager / System Status / SIP Entity Monitoring

### 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: VHT-IVG

Status Details for the selected Session Manager:

Summary View

1 Items Refresh Filter: Enable

Session Manager N	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
DR-SMW	10.64.101.207	5060	UDP	FALSE	UP	200 OK	UP

## 10.4. Verify VHT Callback and IVG

Access the Callback web-based EyeQueue application by using the URL “http://ip-address/EyeQueue” in an Internet browser window, where “ip-address” is the IP address of the Callback server. Log in using the appropriate credentials.



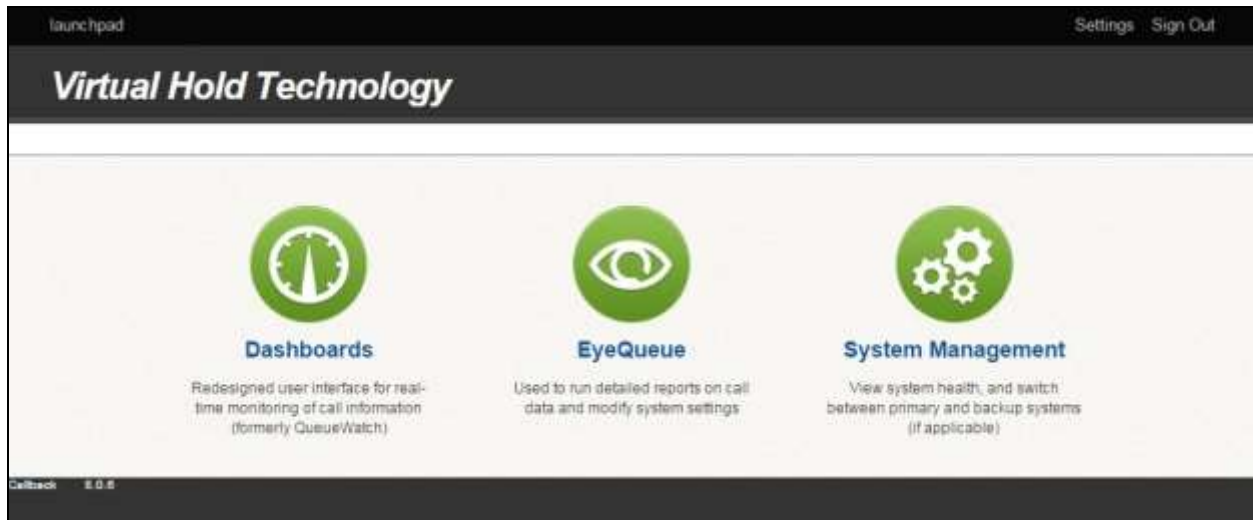
User name

Password

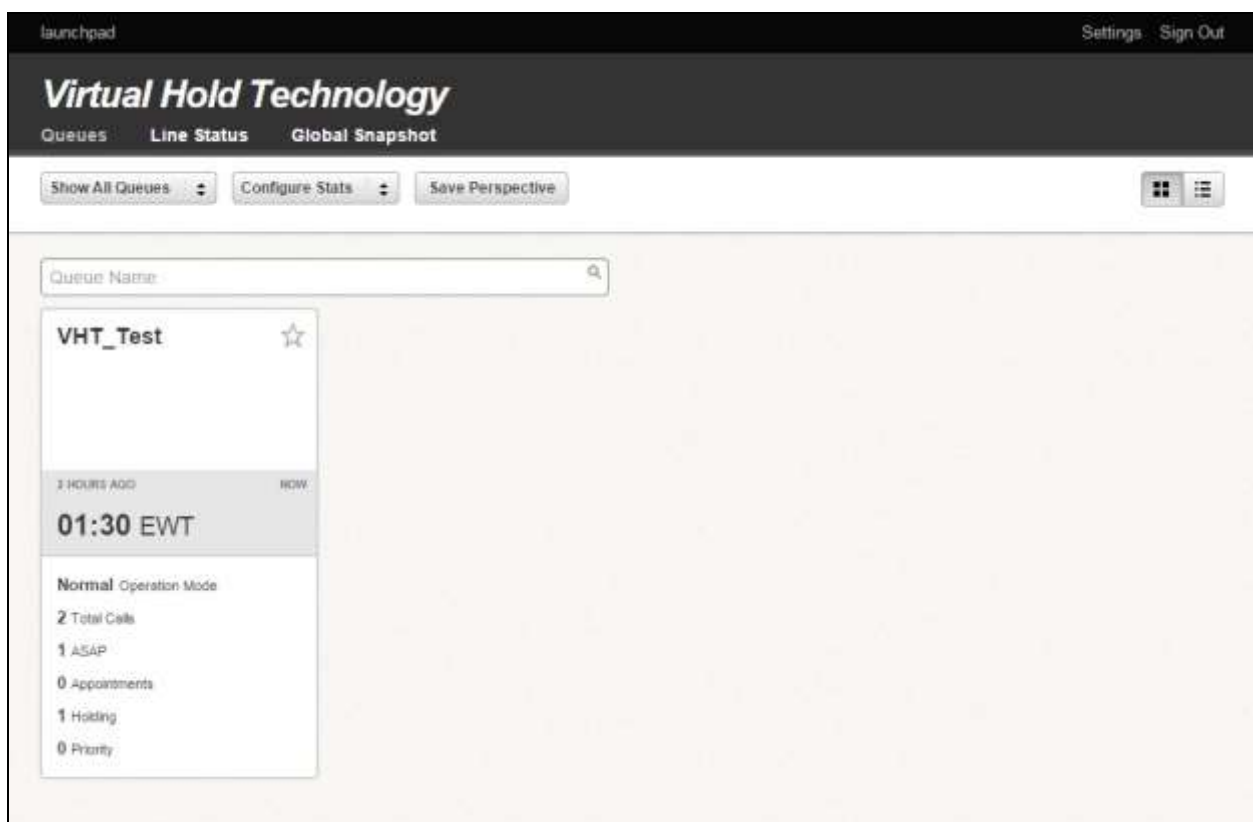
Clear Login

**vht**

The screen below is displayed. Select **Dashboards**.



Make a few incoming ACD calls. Verify that the screen is updated reflecting proper active calls and expected wait time (EWT), as shown below.



## 11. Conclusion

These Application Notes describe the configuration steps required for VHT Callback 8.0 to successfully interoperate with Avaya Aura® Communication Manager 6.3, Avaya Aura® Application Enablement Services 6.3, and Avaya Aura® Session Manager 6.3 using Genesys T-Server for Avaya TSAPI 8.1. All feature and serviceability test cases were completed with observations noted in **Section 2.2**.

## 12. Additional References

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

1. *Administering Avaya Aura® Communication Manager*, Document 03-300509, Issue 10, Release 6.3, June 2014, available at <http://support.avaya.com>.
2. *Avaya Aura® Application Enablement Services Administration and Maintenance Guide*, Release 6.3, 02-300357, June 2014, available at <http://support.avaya.com>.
3. *Virtual Hold Deployment Guide*, Version 8.0.6, available upon request to Virtual Hold Support.
4. *Interactive Voice Gateway (IVG) Configuration Guide*, Version 1.1.0, available upon request to Virtual Hold Support.

---

**©2015 Avaya Inc. All Rights Reserved.**

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

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