



## **Avaya Solution & Interoperability Test Lab**

---

# **Application Notes for VHT Callback using Native TSAPI, TLS/SRTP, and Secure TSAPI Connection with Avaya Aura® Communication Manager, Avaya Aura® Session Manager, and Avaya Aura® Application Enablement Services – Issue 1.0**

## **Abstract**

These Application Notes describe the steps required to integrate VHT Callback using Native TSAPI with Avaya Aura® Communication Manager, Avaya Aura® Session Manager, and Avaya Aura® Application Enablement Services. VHT Callback is a contact center solution that calculates expected wait time and maintains caller position in a virtual queue. The solution integrated with Avaya Aura® Session Manager via a SIP trunk using TLS/SRTP and Avaya Aura® Application Enablement Service using a secure Telephony Services Application Programming Interface (TSAPI) connection.

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 steps required to integrate VHT Callback using Native TSAPI with Avaya Aura® Communication Manager, Avaya Aura® Session Manager, and Avaya Aura® Application Enablement Services. VHT Callback is a contact center solution that calculates expected wait time and maintains caller position in a virtual queue. The solution integrated with Avaya Aura® Session Manager via a SIP trunk using TLS/SRTP and Avaya Aura® Application Enablement Service using a secure Telephony Services Application Programming Interface (TSAPI) connection.

The TSAPI interface is used by VHT Callback to monitor VDNs and to query status of ACD queues. The information obtained from the TSAPI events 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 exceeds a pre-defined threshold, then VHT Callback routes the call over Session Manager SIP trunk to the Interactive Voice Gateway (IVG) component of VHT Callback. 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.

VHT Callback supports **Predictive** and **Agent Priority** queue modes as described below:

- With **Predictive** queue mode, VHT Callback dials the customer first, ensuring the customer is connected, then transfers them to a priority holding queue where they will wait for the next available agent. The callback hold time, or the amount of time a caller is on hold after the callback has been made and the caller is transferred to the queue, assumes a predictive callback mode. If the customer does not confirm, the transfer of the call to the Callback VDN is not performed.
- With **Agent Priority** queue mode, VHT Callback dials an available agent first, allowing the agent time to preview the saved data associated with the callback and prepare of the call. When the agent is ready, a callback is made to the customer. Once the customer accepts the call, the customer is connected to the agent.

## 2. General Test Approach

The feature test cases were performed both automatically and manually. Upon startup of the Callback application, the application automatically sends TSAPI queries for ACD skill group status, route registers for the Entry VDN, and requests monitoring of VDNs. 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 User-to-User Information (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. In addition, it was verified that Communication Manager routed calls to an available agent or queued the call when the Callback or IVG servers were unavailable.

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

Avaya recommends our customers implement Avaya solutions using appropriate security and encryption capabilities enabled by our products. The testing referenced in this DevConnect Application Note included the enablement of supported encryption capabilities in the Avaya products. Readers should consult the appropriate Avaya product documentation for further information regarding security and encryption capabilities supported by those Avaya products.

Support for these security and encryption capabilities in any non-Avaya solution component is the responsibility of each individual vendor. Readers should consult the appropriate vendor-supplied product documentation for more information regarding those products.

For the testing associated with this Application Note, the interfaces between Avaya systems and VHT Callback used TLS mutual authentication, Secure RTP (SRTP), and an encrypted TSAPI client connection.

## 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.
- Use of TSAPI event report service to monitor VDNs.
- 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 below and over the threshold, transfer of inbound calls with received UII data, initiation and transfer of outbound callback calls with priority and saved UII data, and unsuccessful callback attempts.
- Queue statistics using TSAPI real-time adapter in Callback.
- SIP trunk between IVG server and Session Manager using TLS mutual authentication.
- SRTP between IVG server and Communication Manager or Avaya IP Deskphones.
- Secure TSAPI connection between Callback server and Application Enablement Services.
- Calls between VHT Callback and local Avaya SIP and H.323 Deskphones and the PSTN with Shuffling disabled.
- Predictive and Agent Priority queue modes on VHT Callback.
- IVG response to SIP OPTIONS messages from Session Manager.

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 and IVG servers.

## 2.2. Test Results

All test cases passed. When the wait time of incoming ACD calls exceeded a pre-defined threshold value, VHT Callback answered the call and gave the caller the option to be called back, schedule a callback, or continue waiting in queue. In addition, a queue statistics report was generated using the TSAPI real-time adapter.

The following observations were noted during testing:

- When Direct IP Media (Shuffling) was enabled, DTMF from an Avaya SIP Deskphone wasn't recognized by VHT Callback. In addition, the caller's name was not recorded when using the SIP deskphone with Shuffling enabled. The workaround was to disable Shuffling.
- After rebooting the VHT Callback server, the VHT Authorization and VHT Statistics services need to be restarted.

## 2.3. Support

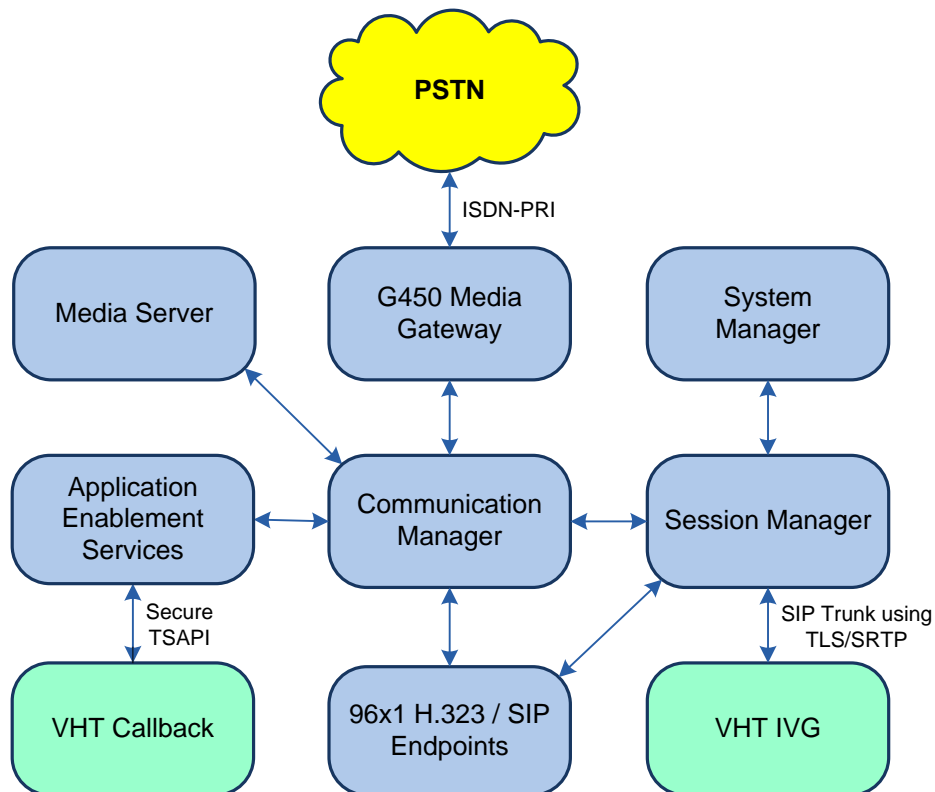
For technical support on VHT Callback, contact VHT Technical Support through one of the following:

- **Phone:** + 1 (866) 670-2223 (USA)  
+44 (0)20 3633 4644 (EMEA)
- **Website:** <https://www.vhtcx.com/contact/contact-center-technical-support/>
- **Email:** [support@vhctx.com](mailto:support@vhctx.com)

### 3. Reference Configuration

The configuration used for the compliance testing is shown in **Figure 1**. The Callback configuration consisted of the Callback server that integrated with Application Enablement Services using a secure TSAPI connection and IVG that connected via SIP trunks to Session Manager using TLS/SRTP. 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 “avaya.com”. A 5-digit Uniform Dial Plan was used to facilitate routing of calls with Callback. In the compliance testing, calls to 78701 were routed to the IVG component of Callback.

Device Type	Extension
Skill Group Number	77
Skill Group Extension	77200
Agent Stations	77301, 78030
Agent Login IDs	76301, 76302



**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	8.1.0.1.0-SP1
Avaya G450 Media Gateway	FW 40.25.0
Avaya Aura® Media Server	v.8.0.1.121
Avaya Aura® Application Enablement Services	8.1.0.0.0.9-1
Avaya Aura® System Manager	8.1.0.0 Build No. – 8.1.0.0.733078 Software Update Revision No: 8.1.0.0.079814
Avaya Aura® Session Manager	8.1.0.0.810007
Avaya 96x1 IP Deskphones	6.8003 (H.323) 7.1.5.0.11(SIP)
VHT Callback using Native TSAPI on Microsoft Windows Server 2012 R2 Standard with <ul style="list-style-type: none"><li>Avaya AES TSAPI Client</li></ul>	8.13.0.4343 8.0
VHT Interactive Voice Gateway (IVG) on CentOS <ul style="list-style-type: none"><li>Holly Voice Platform (HVP)</li><li>VXML Interactive Server (VIS)</li><li>Call Control Interaction Server (CCIS)</li></ul>	3.11.0.122 HVP-6.3.28-2862-44233 6.9.0 3.11.0

## 5. Configure Avaya Aura® Communication Manager

This section provides the steps for configuring Communication Manager. Administration of Communication Manager was performed using the System Access Terminal (SAT). The procedures include the following areas:

- Verify License
- Administer CTI Link
- Administer System Parameters Features
- Administer Vectors and VDNs
- Administer IP Node Names
- Administer IP Codec Set
- Administer IP Network Region
- Administer SIP Signaling Group
- Administer SIP Trunk Group
- Administer AAR Call Routing

### 5.1. Note: It is assumed that the switch connection between Communication Manager and Application Enablement Services is already configured. 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 12
OPTIONAL FEATURES		
IP PORT CAPACITIES	USED	
Maximum Administered H.323 Trunks:	12000	0
Maximum Concurrently Registered IP Stations:	2400	2
Maximum Administered Remote Office Trunks:	12000	0
Maximum Concurrently Registered Remote Office Stations:	2400	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:	2400	1
<b>Maximum Administered SIP Trunks:</b>	<b>12000</b>	<b>10</b>
Maximum Administered Ad-hoc Video Conferencing Ports:	12000	0
Maximum Number of DS1 Boards with Echo Cancellation:	688	0
(NOTE: You must logoff & login to effect the permission changes.)		



Navigate to **Page 4** and verify that the **Computer Telephony Adjunct Links** customer option is set to “y”.

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

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

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

Navigate to **Page 7** and verify that the **Vectoring (Basic)** customer option is set to “y”.

```
display system-parameters customer-options                                Page 7 of 12
                                CALL CENTER OPTIONAL FEATURES

                                Call Center Release: 8.0

    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      Vectoring (Basic)? y
    Dynamic Advocate? n                 Vectoring (Prompting)? y
    Expert Agent Selection (EAS)? y       Vectoring (G3V4 Enhanced)? y
    EAS-PHD? y                         Vectoring (3.0 Enhanced)? y
    Forced ACD Calls? n                 Vectoring (ANI/II-Digits Routing)? y
    Least Occupied Agent? y             Vectoring (G3V4 Advanced Routing)? y
    Lookahead Interflow (LAI)? y         Vectoring (CINFO)? y
    Multiple Call Handling (On Request)? y Vectoring (Best Service Routing)? y
    Multiple Call Handling (Forced)? y     Vectoring (Holidays)? y
    PASTE (Display PBX Data on Phone)? y  Vectoring (Variables)? y

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

## 5.2. Administer CTI Link

Add a CTI link using the **add cti-link** command. 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 1	Page 1 of 3
CTI LINK	
CTI Link: 1	
<b>Extension: 77700</b>	
<b>Type: ADJ-IP</b>	
<b>Name: AES TSAPI Link</b>	COR: 1
Unicode Name? n	

### 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 19
                        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 19
                        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? n
  Call Classification After Answer Supervision? n
  Send UCID to ASAI? y
  For ASAI Send DTMF Tone to Call Originator? y
  Send Connect Event to ASAI For Announcement Answer? n
  Prefer H.323 Over SIP For Dual-Reg Station 3PCC Make Call? n
```

## 5.4. Administer Vectors and VDNs

Administer four 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
77201	201	Entry vector & VDN for adjunct route and failure coverage
77202	202	Hold vector & VDN for queuing inbound calls to skill at medium priority
77203	203	Callback vector & VDN for queuing outbound calls to skill at high priority
77204	204	Route vector & VDN for routing calls to IVG and failure coverage

### 5.4.1. Entry Vector and VDN

Modify an available vector using the **change vector** command. 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 failure from the adjunct routing step. In the compliance test, the covering point is the Hold VDN, which is administered in **Section 5.4.2**.

change vector 201	Page 1 of 6
CALL VECTOR	
<b>Number: 201</b>	<b>Name: VHT Entry</b>
Multimedia? n	Attendant Vectoring? n
Basic? y	EAS? y
Prompting? y	LAI? y
Variables? y	3.0 Enhanced? y
01 adjunct	routing link 1
02 wait-time	10 secs hearing music
03 route-to	number 77202
04	with cov n if unconditionally

Add a VDN using the **add vdn** command. Enter a descriptive **Name** and the vector number specified above for **Vector Number**. Retain the default values for all remaining fields.

add vdn 77201	Page 1 of 3
VECTOR DIRECTORY NUMBER	
Extension: 77201	
<b>Name*: VHT Entry</b>	
<b>Destination: Vector Number 201</b>	
Attendant Vectoring? n	
Meet-me Conferencing? n	
Allow VDN Override? n	
COR: 1	
TN*: 1	
Measured: none	
Report Adjunct Calls as ACD*? n	

### 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 77 is the existing skill group number mentioned in **Section 3**.

```
change vector 202                                     Page 1 of 6
                                     CALL VECTOR

      Number: 202           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? y      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 77      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 specified above for **Vector Number**.

```
add vdn 77202                                     Page 1 of 3
                                     VECTOR DIRECTORY NUMBER

                                     Extension: 77202
                                     Name*: VHT Hold
                                     Destination: Vector Number      202
Attendant Vectoring? n
Meet-me Conferencing? n
  Allow VDN Override? n
      COR: 1
      TN*: 1
Measured: none      Report Adjunct Calls as ACD*? n
```

### 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 77 is the existing skill group number mentioned in **Section 3**.

change vector 203	CALL VECTOR	Page 1 of 6
<b>Number: 203</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? y    G3V4 Adv Route? y	CINFO? y    BSR? y    Holidays? y
Variables? y	3.0 Enhanced? y	
01 queue-to	skill 77	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 specified above for **Vector Number**.

add vdn 77203	VECTOR DIRECTORY NUMBER	Page 1 of 3
Extension: 77203		
<b>Name*: VHT Callback</b>		
<b>Destination: Vector Number</b>		<b>203</b>
Attendant Vectoring? n		
Meet-me Conferencing? n		
Allow VDN Override? n		
COR: 1		
TN*: 1		
Measured: none		Report Adjunct Calls as ACD*? n

#### 5.4.4. Route Vector and VDN

Modify an available vector for Callback server to route calls to IVG using extension 78701. If the call to IVG fails for any reason, the incoming ACD call will be routed to the ACD skill where the call will either be queued or answered by an available agent. This ensures that the call is properly routed by Communication Manager even if the call attempt to IVG fails.

change vector 204	Page 1 of 6
CALL VECTOR	
<b>Number: 204</b>	<b>Name: VHT Route</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? y G3V4 Adv Route? y CINFO? y BSR? y Holidays? y
Variables? y	3.0 Enhanced? y
01 wait-time	0 secs hearing silence
02 route-to	number 78701 with cov n if unconditionally
03 wait-time	2 secs hearing ringback
04 route-to	number 77202 with cov n if unconditionally
05 disconnect	after announcement none
06 stop	
07	

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

add vdn 77204	Page 1 of 3
VECTOR DIRECTORY NUMBER	
Extension: 77204	
<b>Name*: VHT Route</b>	
<b>Destination: Vector Number 204</b>	
Attendant Vectoring? n	
Meet-me Conferencing? n	
Allow VDN Override? n	
COR: 1	
TN*: 1	
Measured: none Report Adjunct Calls as ACD*? n	

#### 5.5. Administer IP Node Names

In the **IP Node Names** form, assign an IP address and host name for Communication Manager (*procr*) and Session Manager (*devcon-sm*). The host names will be used in other configuration screens of Communication Manager.

change node-names ip	Page 1 of 2
IP NODE NAMES	
Name	IP Address
default	0.0.0.0
devcon-ams	10.64.102.118
<b>devcon-sm</b>	<b>10.64.102.117</b>
<b>procr</b>	<b>10.64.102.115</b>
procr6	::

## 5.6. Administer IP Codec Set

In the **IP Codec Set** form, select the audio codec type supported for calls routed over the SIP trunk to IVG. The form is accessed via the **change ip-codec-set** command. Note the codec set number since it will be used in the IP Network Region covered in the next section. For the compliance test, *G.711MU* was used and SRTP was enabled.

**Note:** In the IP Codec Set associated with VHT Callback, the Media Encryption section should only list *1-srtp-aescm128-hmac80*.

change ip-codec-set 1

Page 1 of 2

IP MEDIA PARAMETERS

Codec Set: 1

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

Media Encryption

1: 1-srtp-aescm128-hmac80

2:

3:

4:

5:

Encrypted SRTCP: best-effort



## 5.7. Administer IP Network Region

In the **IP Network Region** form, the **Authoritative Domain** field is configured to match the domain name configured on Session Manager. In this configuration, the domain name is *avaya.com*. By default, **IP-IP Direct Audio** (shuffling) is enabled to allow audio traffic to be sent directly between IVG and IP endpoints without using media resources in the Avaya G450 Media Gateway or Avaya Media Server. For the compliance test, shuffling was disabled as noted in **Section 2.2**. Note that calls to the PSTN are not shuffled. The **IP Network Region** form also specifies the **IP Codec Set** to be used for calls routed over the SIP trunk to Session Manager. This codec set is used when its corresponding network region (i.e., IP Network Region 1) is specified in the SIP signaling group.

change ip-network-region 1		Page 1 of 20
IP NETWORK REGION		
Region: 1		
Location: 1	Authoritative Domain: avaya.com	
Name:	Stub Network Region: n	
MEDIA PARAMETERS		
Codec Set: 1	Intra-region IP-IP Direct Audio: no	
UDP Port Min: 2048	Inter-region IP-IP Direct Audio: no	
UDP Port Max: 3329	IP Audio Hairpinning? n	
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		

## 5.8. Administer SIP Signaling Group

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

- Set the **Group Type** field to *sip*.
- Set the **IMS Enabled** field to *n*.
- The **Transport Method** field was set to *tls*.
- Specify Communication Manager (*procr*) and the Session Manager (*devcon-sm*) as the two ends of the signaling group in the **Near-end Node Name** field and the **Far-end Node Name** field, respectively. These field values are taken from the **IP Node Names** form.
- Ensure that the TLS port value of *5061* is configured in the **Near-end Listen Port** and the **Far-end Listen Port** fields.
- The preferred codec for the call will be selected from the IP codec set assigned to the IP network region specified in the **Far-end Network Region** field.
- Enter the domain name of Session Manager in the **Far-end Domain** field. In this configuration, the domain name is *avaya.com*.
- The **DTMF over IP** field should be set to the default value of *rtp-payload*.
- **Direct IP-IP Audio Connections** may be disabled here or in the IP Network Region shown in **Section 5.7** to prevent calls from being shuffled.

Communication Manager supports DTMF transmission using RFC 2833. The default values for the other fields may be used.

add signaling-group 10		Page 1 of 2
SIGNALING GROUP		
Group Number: 10	<b>Group Type: sip</b>	
IMS Enabled? n	<b>Transport Method: tls</b>	
Q-SIP? n		
IP Video? n	Enforce SIPS URI for SRTP? n	
Peer Detection Enabled? y	Peer Server: SM	Clustered? n
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		
<b>Near-end Node Name: procr</b>		<b>Far-end Node Name: devcon-sm</b>
<b>Near-end Listen Port: 5061</b>		<b>Far-end Listen Port: 5061</b>
		<b>Far-end Network Region: 1</b>
<b>Far-end Domain: avaya.com</b>		
Incoming Dialog Loopbacks: eliminate		Bypass If IP Threshold Exceeded? n
<b>DTMF over IP: rtp-payload</b>		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

## 5.9. Administer SIP Trunk Group

Configure the **Trunk Group** form as shown below. This trunk group is used for SIP calls to IVG and SIP stations. Set the **Group Type** field to *sip*, set the **Service Type** field to *tie*, specify the signaling group associated with this trunk group in the **Signaling Group** field, and specify the **Number of Members** supported by this SIP trunk group. Accept the default values for the remaining fields.

add trunk-group 10		Page 1 of 22	
TRUNK GROUP			
Group Number: 10	<b>Group Type: sip</b>	CDR Reports: y	
Group Name: To devcon-sm	COR: 1	TN: 1	TAC: 1010
Direction: two-way	Outgoing Display? n		
Dial Access? n	Night Service:		
Queue Length: 0			
<b>Service Type: tie</b>	Auth Code? n		
		Member Assignment Method: auto	
		<b>Signaling Group: 10</b>	
		<b>Number of Members: 10</b>	

On **Page 3** of the trunk group form, set the **UI Treatment** field to *shared* and enable the **Send UCID** option.

add trunk-group 10		Page 3 of 22	
TRUNK FEATURES			
ACA Assignment? n	Measured: none	Maintenance Tests? y	
Suppress # Outpulsing? n	Numbering Format: private		
		<b>UI Treatment: shared</b>	
		Maximum Size of UI Contents: 128	
		Replace Restricted Numbers? n	
		Replace Unavailable Numbers? n	
		Hold/Unhold Notifications? y	
		Modify Tandem Calling Number: no	
<b>Send UCID? y</b>			
Show ANSWERED BY on Display? y			

## 5.10. Administer AAR Call Routing

Configure the uniform dial plan table to route calls using AAR for dialed digits that are 5-digits long and begin with '78'. This would cover call routing to IVG (i.e., 78701).

change uniform-dialplan 7				Page 1 of 2	
UNIFORM DIAL PLAN TABLE				Percent Full: 0	
Matching Pattern	Len	Del	Insert Digits	Net Conv	Node Num
78	5	0		aar n	

SIP calls to Session Manager are routed over a SIP trunk via AAR call routing. Configure the AAR analysis form and add an entry that routes digits beginning with "78" to route pattern 10 as shown below. Note that the **Call Type** was set to *lev0*. This entry routes calls to IVG and SIP stations.

change aar analysis 7				Page 1 of 2	
AAR DIGIT ANALYSIS TABLE				Percent Full: 2	
Location: all					
Dialed String	Total Min	Max	Route Pattern	Call Type	Node Num ANI Req'd
7	7	7	254	aar	n
<b>78</b>	<b>5</b>	<b>5</b>	<b>10</b>	<b>lev0</b>	<b>n</b>
8	7	7	254	aar	n
9	7	7	254	aar	n

Configure a preference in **Route Pattern** 10 to route calls over SIP trunk group 10 as shown below.

change route-pattern 10										Page	1 of	3
Pattern Number: 10										Pattern Name: To devcon-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:	10	0								n	user	
2:								n	user			
3:								n	user			
4:								n	user			
5:								n	user			
6:								n	user			
BCC VALUE		TSC	CA-TSC		ITC BCIE		Service/Feature	PARM	Sub	Numbering	LAR	
0 1 2 M 4 W			Request						Dgts	Format		
1:	y	y	y	y	y	n	n	rest		unk-unk	none	
2:	y	y	y	y	y	n	n	rest			none	
3:	y	y	y	y	y	n	n	rest			none	
4:	y	y	y	y	y	n	n	rest			none	
5:	y	y	y	y	y	n	n	rest			none	
6:	y	y	y	y	y	n	n	rest			none	

## 6. Configure Avaya Aura® Session Manager

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

- Launch System Manager
- Administer SIP Entities
- Administer Routing Policies
- Administer Dial Patterns
- Import VHT IVG TLS Certificate

**Note:** 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.

### 6.1. Launch System Manager

Configuration is accomplished by accessing the browser-based GUI of Avaya Aura® System Manager using the URL “https://<ip-address>”, where <ip-address> is the IP address of Avaya Aura® System Manager. Log in with the appropriate credentials.

Recommended access to System Manager is via FQDN.  
[Go to central login for Single Sign-On](#)

If IP address access is your only option, then note that authentication will fail in the following cases:

- First time login with "admin" account
- Expired/Reset passwords

Use the "Change Password" hyperlink on this page to change the password manually, and then login.

Also note that single sign-on between servers in the same security domain is not supported when accessing via IP address.

User ID:

Password:

[Change Password](#)

**Supported Browsers:** Internet Explorer 11.x or Firefox 65.0, 66.0 and 67.0.

## 6.2. Administer SIP Entities

In the sample configuration, two SIP entities were added for Communication Manager and IVG.

### 6.2.1. SIP Entity for Communication Manager

A SIP Entity must be added for Communication Manager. To add a SIP Entity, select **SIP Entities** on the left and click on the **New** button on the right (not shown). The following screen is displayed. Fill in the following:

Under *General*:

- **Name:** A descriptive name.
- **FQDN or IP Address:** IP address of the signaling interface (e.g., procr) on the telephony system.
- **Type:** Select *CM*.
- **Location:** Select one of the locations defined previously (not shown).
- **Time Zone:** Time zone for this location.

Defaults can be used for the remaining fields. Click **Commit** to save each SIP Entity definition.

The screenshot displays the Avaya Aura System Manager 8.1 web interface. The top navigation bar includes the Avaya logo, 'Aura System Manager 8.1', and various menu items like Users, Elements, Services, Widgets, and Shortcuts. A search bar and a user profile 'admin' are also present. The left sidebar shows a tree view with 'Routing' selected, and 'SIP Entities' highlighted. The main content area is titled 'SIP Entity Details' and contains a 'General' tab. The form fields are as follows:

- Name:** devcon-cm
- \* FQDN or IP Address:** 10.64.102.115
- Type:** CM (dropdown)
- Notes:** (empty text area)
- Adaptation:** (empty dropdown)
- Location:** Thornton (dropdown)
- Time Zone:** America/New\_York (dropdown)
- \* SIP Timer B/F (in seconds):** 4
- Minimum TLS Version:** Use Global Setting (dropdown)
- Credential name:** (empty text area)
- Securable:** (checkbox, unchecked)
- Call Detail Recording:** none (dropdown)

Below the General tab is the 'Loop Detection' section:

- Loop Detection Mode:** On (dropdown)
- Loop Count Threshold:** 5
- Loop Detection Interval (in msec):** 200

At the bottom is the 'Monitoring' section:

- SIP Link Monitoring:** Use Session Manager Configuration (dropdown)
- CRLF Keep Alive Monitoring:** Use Session Manager Configuration (dropdown)

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

Scroll down to the **Entity Links** sub-section and click **Add** to add an entity link. The SIP trunk from Session Manager to Communication Manager is described by an Entity link. Fill in the following fields in the new row that is displayed:

- **Name:** A descriptive name (e.g., *devcon-cm link*).
- **SIP Entity 1:** Select the Session Manager.
- **Protocol:** Select the *TLS* protocol to allow secure SIP signaling to CM.
- **Port:** Port number to which the other system sends SIP requests.
- **SIP Entity 2:** Select the name of Communication Manager.
- **Port:** Port number on which the other system receives SIP requests.
- **Connection Policy:** Select *Trusted*.

Click **Commit** to save the Entity Link definition.

#### 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"/>	* devcon-cm Link	devcon-sm	TLS	* 5061	devcon-cm	* 5061	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		
<input type="checkbox"/>					

Commit Cancel

### 6.2.2. SIP Entity for IVG

A SIP Entity must be added for IVG. To add a SIP Entity, select **SIP Entities** on the left and click on the **New** button on the right (not shown). The following screen is displayed. Fill in the following:

Under *General*:

- **Name:** A descriptive name.
- **FQDN or IP Address:** IP address of IVG.
- **Type:** Select *SIP Trunk*.
- **Location:** Select one of the locations defined previously (not shown).
- **Time Zone:** Time zone for this location.

Defaults can be used for the remaining fields. Click **Commit** to save each SIP Entity definition.

The screenshot displays the Avaya Aura System Manager 8.1 web interface. The top navigation bar includes the Avaya logo, 'Aura® System Manager 8.1', and various menu items: Users, Elements, Services, Widgets, and Shortcuts. A search bar and a user profile icon labeled 'admin' are also present. The left sidebar shows a tree view with categories like Routing, Domains, Locations, Conditions, Adaptations, SIP Entities (highlighted), Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area is titled 'SIP Entity Details' and features a 'General' tab. The form includes fields for Name (VHT-IVG), FQDN or IP Address (10.64.102.107), Type (SIP Trunk), Notes, Adaptation, Location (Thornton), Time Zone (America/New\_York), SIP Timer B/F (4), Minimum TLS Version (Use Global Setting), Credential name, Securable (unchecked), Call Detail Recording (egress), Loop Detection Mode (On), Loop Count Threshold (5), Loop Detection Interval (200), SIP Link Monitoring (Use Session Manager Configuration), and CRLF Keep Alive Monitoring (Use Session Manager Configuration). 'Commit' and 'Cancel' buttons are located at the top right of the form area.



Scroll down to the **Entity Links** sub-section and click **Add** to add an entity link. The SIP trunk from Session Manager to IVG is described by an Entity link. Fill in the following fields in the new row that is displayed:

- **Name:** A descriptive name (e.g., *VHT-IVG Link*).
- **SIP Entity 1:** Select the Session Manager.
- **Protocol:** Select the appropriate protocol (e.g., *TLS*).
- **Port:** Port number to which the other system sends SIP requests.
- **SIP Entity 2:** Select the name of IVG.
- **Port:** Port number on which the other system receives SIP requests.
- **Connection Policy:** Select *Trusted*.

Click **Commit** to save the Entity Link definition.

#### Entity Links

Override Port & Transport with DNS SRV: ☐

Add Remove		Filter: Enable						
1 Item								
<input type="checkbox"/>	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Deny New Service
<input type="checkbox"/>	* VHT-IVG Link	devcon-sm	TLS	* 5061	VHT-IVG	* 5061	trusted	<input type="checkbox"/>

Select : All, None

#### SIP Responses to an OPTIONS Request

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

Commit Cancel

## 6.3. Administer Routing Policies

Routing policies describe the conditions under which calls will be routed to the SIP Entities specified in **Section 6.2**. Routing policies were added for Communication Manager and IVG.

### 6.3.1. Routing Policy for 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:

Under *General*:

Enter a descriptive name in **Name**.

Under *SIP Entity as Destination*:

Click **Select**, and then select the appropriate SIP entity to which this routing policy applies.

Defaults can be used for the remaining fields. Click **Commit** to save the Routing Policy definition.

The screenshot displays the Avaya Aura System Manager 8.1 interface. The top navigation bar includes the Avaya logo, version information, and various menu items like Users, Elements, Services, Widgets, and Shortcuts. A search bar and user profile (admin) are also present. The left sidebar shows a tree view of the system configuration, with 'Routing Policies' selected. The main content area is titled 'Routing Policy Details' and contains three sections: 'General', 'SIP Entity as Destination', and 'Time of Day'. The 'General' section has fields for Name (devcon-cm Policy), Disabled (checkbox), Retries (0), and Notes. The 'SIP Entity as Destination' section has a 'Select' button and a table listing the selected entity 'devcon-cm' with its FQDN or IP Address (10.64.102.115) and Type (CM). The 'Time of Day' section has buttons for 'Add', 'Remove', and 'View Gaps/Overlaps', and a table showing a single time range item for 24/7.

**Routing Policy Details** Commit Cancel Help ?

**General**

\* **Name:** devcon-cm Policy

**Disabled:** ☐

\* **Retries:** 0

**Notes:**

**SIP Entity as Destination**

Select

Name	FQDN or IP Address	Type	Notes
devcon-cm	10.64.102.115	CM	

**Time of Day**

Add Remove View Gaps/Overlaps

1 Item Filter: Enable

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

Select : All, None

### 6.3.2. Routing Policy for IVG

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:

Under *General*:

Enter a descriptive name in **Name**.

Under *SIP Entity as Destination*:

Click **Select**, and then select the appropriate SIP entity to which this routing policy applies.

Defaults can be used for the remaining fields. Click **Commit** to save the Routing Policy definition.

The screenshot displays the Avaya Aura System Manager 8.1 interface. The top navigation bar includes the Avaya logo, version information, and user roles (Users, Elements, Services, Widgets, Shortcuts). A search bar and a user profile (admin) are also present. The left sidebar shows a tree view of the system configuration, with 'Routing Policies' selected. The main content area is titled 'Routing Policy Details' and contains three sections: 'General', 'SIP Entity as Destination', and 'Time of Day'. The 'General' section has fields for 'Name' (VHT-IVG Policy), 'Disabled' (checkbox), 'Retries' (0), and 'Notes'. The 'SIP Entity as Destination' section has a 'Select' button and a table with columns 'Name', 'FQDN or IP Address', 'Type', and 'Notes'. The 'Time of Day' section has 'Add', 'Remove', and 'View Gaps/Overlaps' buttons, a table with columns 'Ranking', 'Name', 'Mon', 'Tue', 'Wed', 'Thu', 'Fri', 'Sat', 'Sun', 'Start Time', 'End Time', and 'Notes', and a 'Filter: Enable' button. The table shows one item with a ranking of 0 and a time range of 24/7.

Name	FQDN or IP Address	Type	Notes
VHT-IVG	10.64.102.107	SIP Trunk	

Ranking	Name	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
0	24/7	✓	✓	✓	✓	✓	✓	✓	00:00	23:59	Time Range 24/7

## 6.4. Administer Dial Patterns

Dial patterns must be defined to direct calls to the appropriate SIP Entity. Dial patterns were added for Communication Manager and IVG.

### 6.4.1. Dial Patterns for Communication Manager

In the sample configuration, 5-digit extensions starting with '7' and 10-digit numbers prepended with the ARS access code '9' and prefix code '1' were routed to local stations and PSTN, respectively, via Communication Manager. 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:

Under *General*:

- **Pattern:** Dialed number or prefix.
- **Min** Minimum length of dialed number.
- **Max** Maximum length of dialed number.
- **SIP Domain** SIP domain of dial pattern.
- **Notes** Comment on purpose of dial pattern (optional).

Under *Originating Locations and Routing Policies*:

Click **Add**, and then select the appropriate location and routing policy from the list.

Default values can be used for the remaining fields. Click **Commit** to save this dial pattern. The following screen shows the dial pattern definition for routing calls to local stations on Communication Manager.

The screenshot displays the Avaya Aura System Manager 8.1 interface. The top navigation bar includes the Avaya logo, 'Aura® System Manager 8.1', and various menu items like Users, Elements, Services, Widgets, and Shortcuts. A search bar and a user profile icon labeled 'admin' are also present. The left sidebar shows a tree view with 'Routing' selected, and 'Dial Patterns' highlighted under the 'Routing' category. The main content area is titled 'Dial Pattern Details' and contains two tabs: 'General' and 'Originating Locations and Routing Policies'. The 'General' tab is active, showing the following fields: 'Pattern' (7), 'Min' (5), 'Max' (5), 'Emergency Call' (unchecked), 'SIP Domain' (-ALL-), and 'Notes' (CM Stations). The 'Originating Locations and Routing Policies' tab is also visible, showing a table with one item: 'Thornton', 'devcon-cm Policy', Rank 0, 'Routing Policy Disabled' (unchecked), and 'Routing Policy Destination' devcon-cm. The table has columns for 'Originating Location Name', 'Originating Location Notes', 'Routing Policy Name', 'Rank', 'Routing Policy Disabled', 'Routing Policy Destination', and 'Routing Policy Notes'. The 'Add' and 'Remove' buttons are visible above the table. The 'Filter: Enable' button is also present.

AVAYA

Aura® System Manager 8.1

Users

Elements

Services

Widgets

Shortcuts

Search

admin

Home

Routing

Routing

Domains

Locations

Conditions

Adaptations

SIP Entities

Entity Links

Time Ranges

Routing Policies

Dial Patterns

Origination Dial...

Dial Pattern Details

CommitCancel

Help

General

\* Pattern: 91

\* Min: 12

\* Max: 12

Emergency Call: ☐

SIP Domain: -ALL-

Notes: PSTN

Originating Locations and Routing Policies

AddRemove

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"/>	Thornton		devcon-cm Policy	0	<input type="checkbox"/>	devcon-cm	

Select : All, None

## 6.4.2. Dial Pattern for IVG

In the sample configuration, 78701 was routed to IVG. 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:

Under *General*:

- **Pattern:** Dialed number or prefix.
- **Min** Minimum length of dialed number.
- **Max** Maximum length of dialed number.
- **SIP Domain** SIP domain of dial pattern.
- **Notes** Comment on purpose of dial pattern (optional).

Under *Originating Locations and Routing Policies*:

Click **Add**, and then select the appropriate location and routing policy from the list.

Default values can be used for the remaining fields. Click **Commit** to save this dial pattern. The following screen shows the dial pattern definition for routing calls to IVG.

**AVAYA** Aura® System Manager 8.1

Users ▾ Elements ▾ Services ▾ | Widgets ▾ Shortcuts ▾ Search 🔍 🔔 ≡ admin

Home Routing

**Dial Pattern Details** Commit Cancel [Help ?](#)

**General**

\* Pattern: 78701

\* Min: 5

\* Max: 5

Emergency Call: ☐

SIP Domain: -ALL- ▾

Notes: VHT IVG

**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"/>	Thornton		VHT-IVG Policy	0	<input type="checkbox"/>	VHT-IVG	

Select : All, None

## 6.5. Import VHT IVG TLS Certificate

Import the IVG TLS certificate as part of configuring mutual authentication TLS. Navigate to **Services → Inventory → Manage Elements** and select the Session Manager (i.e., *devcon-sm*) as shown below. In the **More Actions** drop-down field, select **Manage Trusted Certificates**.

The screenshot shows the Avaya Aura System Manager 8.1 interface. The top navigation bar includes the Avaya logo, 'Aura® System Manager 8.1', and navigation links for Users, Elements, Services, Widgets, and Shortcuts. A search bar and a user profile 'admin' are also present. The left sidebar shows a tree view with 'Inventory' expanded, and 'Manage Elements' selected. The main content area is titled 'Manage Elements' and contains a table of system elements. The 'devcon-sm' element is selected, and the 'More Actions' dropdown menu is open, showing options like 'Manage Trusted Certificates', 'Manage Identity Certificates', 'Import', and others.

Name	Node	Type	SEID	Reg. Status
Corporate Directory	10.64.102.120	UCM		
devcon-cm	10.64.102.115	Com Man		
devcon-sm	10.64.102.116	Sess		
devcon-smgr.avaya.com (primary)	10.64.102.120	UCM		
IPSec	10.64.102.120	UCMApp		
Numbering Groups	10.64.102.120	UCMApp		
Patches	10.64.102.120	UCMApp		
Secure FTP Token	10.64.102.120	UCMApp		
SNMP Profiles	10.64.102.120	UCMApp		
Software Deployment	10.64.102.120	UCMApp		
System Manager	10.64.102.120	System Manager		

In the **Manage Trusted Certificates** web page, click the **Add** button.

The screenshot shows the Avaya Aura System Manager 8.1 interface. The top navigation bar includes the Avaya logo, 'Aura® System Manager 8.1', and various menu items like 'Users', 'Elements', 'Services', 'Widgets', and 'Shortcuts'. A search bar and a user profile 'admin' are also present. The left sidebar contains a tree view with 'Inventory' expanded, showing 'Manage Elements' as the selected option. The main content area is titled 'Manage Trusted Certificates' and includes a 'Done' button. Below the title is a table with 24 items. The table has columns for 'Store Description', 'Store Type', and 'Subject Name'. The 'Add' button is located in the top right of the table area.

	Store Description	Store Type	Subject Name
<input type="checkbox"/>	Used for validating TLS client identity certificates	SECURITY_MODULE_HTTP	EMAILADDRESS=support@holly-connects.com, CN=hvp03.qalab.local, O=Holly Connects, L=Default City, C=XX
<input type="checkbox"/>	Used for validating TLS client identity certificates	SECURITY_MODULE_HTTP	EMAILADDRESS=support@holly-connects.com, CN=hvp03.qalab.local, O=Holly Connects, L=Default City, C=XX
<input type="checkbox"/>	Used for validating TLS client identity certificates	SECURITY_MODULE_HTTP	O=AVAYA, OU=MGMT, CN=System Manager CA
<input type="checkbox"/>	Used for validating TLS client identity certificates	SECURITY_MODULE_HTTP	CN=devcon-epm.avaya.com, OU=SIP CA, O=Avaya
<input type="checkbox"/>	Used for validating TLS client identity certificates	SAL_AGENT	O=AVAYA, OU=MGMT, CN=System Manager CA
<input type="checkbox"/>	Used for validating TLS client identity certificates	SAL_AGENT	EMAILADDRESS=support@holly-connects.com, CN=hvp03.qalab.local, O=Holly Connects, L=Default City, C=XX



Select the **Import from file** radio button and click the **Choose File** button to select the `certificate.pem` file from **Step 2** on **Page 56**. Next, click the **Retrieve Certificate** button to review the certificate details. Click the **Commit** button. The IVG TLS certificate has now been imported into System Manager.

The screenshot shows the Avaya Aura System Manager 8.1 web interface. The top navigation bar includes the Avaya logo, version information, and links for Users, Elements, Services, Widgets, and Shortcuts. A search bar and a user profile (admin) are also present. The left sidebar contains a menu with options like Home, Inventory, Manage Elements, and various configuration settings. The main content area is titled 'Add Trusted Certificate' and features a 'Manage Elements' tab. It includes a 'Select Store Type to add trusted certificate' dropdown set to 'All'. Below this are four radio button options: 'Import from file' (selected), 'Import as PEM certificate', 'Import from existing certificates', and 'Import using TLS'. A table shows a file named 'certificate.pem' with a 'Remove' action link. A 'Choose File' button is present, followed by the text 'No file chosen'. A message states: 'You must click the Retrieve certificate button and review the certificate details before you can continue.' Below this is a 'Retrieve Certificate' button. At the bottom right of the form are 'Commit' and 'Cancel' buttons.

AVAYA  
Aura® System Manager 8.1

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

Home Inventory

Inventory ^

Manage Elements

Create Profiles and Disc...

Element Type Access

Subnet Configuration

Manage Serviceabilit... ▾

Synchronization ▾

Connection Pooling ▾

Help ?

Manage Elements Discovery

**Add Trusted Certificate** [Help ?](#)

Select Store Type to add trusted certificate All ▾

☒ Import from file  
☐ Import as PEM certificate  
☐ Import from existing certificates  
☐ Import using TLS

Filename	Action
certificate.pem	<a href="#">Remove</a>

\* Please select a file

No file chosen

You must click the Retrieve certificate button and review the certificate details before you can continue.

## 7. Configure Avaya Aura® Application Enablement Services

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

- Launch OAM Interface
- Verify License
- Administer TSAPI Link
- Restart Service
- Obtain Tlink Name
- Administer Callback User
- Verify Security Database
- Export CA Trusted Certificate for VHT Callback

**Note:** It is assumed that the switch connection between Communication Manager and Application Enablement Services is already configured.

### 7.1. 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 login screen is displayed. Log in using the appropriate credentials.



#### Application Enablement Services Management Console


Help

Please login here:

Username

Copyright © 2009-2019 Avaya Inc. All Rights Reserved.

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

**Application Enablement Services**  
Management Console

Welcome: User cust  
Last login: Mon Aug 5 14:02:37 2019 from 192.168.100.251  
Number of prior failed login attempts: 0  
HostName/IP: devcon-aes/10.64.102.119  
Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE  
SW Version: 8.1.0.0.9-1  
Server Date and Time: Thu Aug 08 11:04:41 EDT 2019  
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.

Copyright © 2009-2019 Avaya Inc. All Rights Reserved.

## 7.2. Verify License

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

**Application Enablement Services**  
Management Console

Welcome: User cust  
Last login: Mon Aug 5 14:02:37 2019 from 192.168.100.251  
Number of prior failed login attempts: 0  
HostName/IP: devcon-aes/10.64.102.119  
Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE  
SW Version: 8.1.0.0.9-1  
Server Date and Time: Thu Aug 08 11:14:12 EDT 2019  
HA Status: Not Configured

Licensing | Help | Logout

- AE Services
- Communication Manager Interface
- High Availability
- Licensing
  - WebLM Server Address
  - WebLM Server Access
  - Reserved Licenses
- Maintenance
- Networking

### 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 MEDIUM SWITCH** for the virtual server.

WebLM Home	<b>Application Enablement (CTI) - Release: 8 - SID: 10503000</b> <b>Standard License file</b>																																					
Install license	You are here: Licensed Products > Application_Enablement > View License Capacity																																					
Licensed products	License installed on: June 28, 2019 12:26:36 PM -04:00																																					
APPL_ENAB																																						
▼ Application_Enablement																																						
View license capacity	License File Host IDs: V7-94-F5-41-87-5E-01																																					
View peak usage																																						
ASBCE	<b>Licensed Features</b>																																					
►Session_Border_Controller_E_AE																																						
COMMUNICATION_MANAGER	13 Items Show All ▼																																					
►Call_Center	<table border="1"> <thead> <tr> <th>Feature (License Keyword)</th> <th>Expiration date</th> <th>Licensed capacity</th> </tr> </thead> <tbody> <tr> <td>Device Media and Call Control VALUE_AES_DMCC_DMC</td> <td>permanent</td> <td>10000</td> </tr> <tr> <td>AES ADVANCED LARGE SWITCH VALUE_AES_AEC_LARGE_ADVANCED</td> <td>permanent</td> <td>16</td> </tr> <tr> <td>AES HA LARGE VALUE_AES_HA_LARGE</td> <td>permanent</td> <td>1</td> </tr> <tr> <td>AES ADVANCED MEDIUM SWITCH VALUE_AES_AEC_MEDIUM_ADVANCED</td> <td>permanent</td> <td>16</td> </tr> <tr> <td>Unified CC API Desktop Edition VALUE_AES_AEC_UNIFIED_CC_DESKTOP</td> <td>permanent</td> <td>10000</td> </tr> <tr> <td>CVLAN ASAI VALUE_AES_CVLAN_ASAI</td> <td>permanent</td> <td>16</td> </tr> <tr> <td>AES HA MEDIUM VALUE_AES_HA_MEDIUM</td> <td>permanent</td> <td>1</td> </tr> <tr> <td>AES ADVANCED SMALL SWITCH VALUE_AES_AEC_SMALL_ADVANCED</td> <td>permanent</td> <td>16</td> </tr> <tr> <td>DLG VALUE_AES_DLG</td> <td>permanent</td> <td>16</td> </tr> <tr> <td>TSAPI Simultaneous Users VALUE_AES_TSAPI_USERS</td> <td>permanent</td> <td>10000</td> </tr> <tr> <td>CVLAN Proprietary Links VALUE_AES_PROPRIETARY_LINKS</td> <td>permanent</td> <td>16</td> </tr> </tbody> </table>		Feature (License Keyword)	Expiration date	Licensed capacity	Device Media and Call Control VALUE_AES_DMCC_DMC	permanent	10000	AES ADVANCED LARGE SWITCH VALUE_AES_AEC_LARGE_ADVANCED	permanent	16	AES HA LARGE VALUE_AES_HA_LARGE	permanent	1	AES ADVANCED MEDIUM SWITCH VALUE_AES_AEC_MEDIUM_ADVANCED	permanent	16	Unified CC API Desktop Edition VALUE_AES_AEC_UNIFIED_CC_DESKTOP	permanent	10000	CVLAN ASAI VALUE_AES_CVLAN_ASAI	permanent	16	AES HA MEDIUM VALUE_AES_HA_MEDIUM	permanent	1	AES ADVANCED SMALL SWITCH VALUE_AES_AEC_SMALL_ADVANCED	permanent	16	DLG VALUE_AES_DLG	permanent	16	TSAPI Simultaneous Users VALUE_AES_TSAPI_USERS	permanent	10000	CVLAN Proprietary Links VALUE_AES_PROPRIETARY_LINKS	permanent	16
Feature (License Keyword)	Expiration date	Licensed capacity																																				
Device Media and Call Control VALUE_AES_DMCC_DMC	permanent	10000																																				
AES ADVANCED LARGE SWITCH VALUE_AES_AEC_LARGE_ADVANCED	permanent	16																																				
AES HA LARGE VALUE_AES_HA_LARGE	permanent	1																																				
AES ADVANCED MEDIUM SWITCH VALUE_AES_AEC_MEDIUM_ADVANCED	permanent	16																																				
Unified CC API Desktop Edition VALUE_AES_AEC_UNIFIED_CC_DESKTOP	permanent	10000																																				
CVLAN ASAI VALUE_AES_CVLAN_ASAI	permanent	16																																				
AES HA MEDIUM VALUE_AES_HA_MEDIUM	permanent	1																																				
AES ADVANCED SMALL SWITCH VALUE_AES_AEC_SMALL_ADVANCED	permanent	16																																				
DLG VALUE_AES_DLG	permanent	16																																				
TSAPI Simultaneous Users VALUE_AES_TSAPI_USERS	permanent	10000																																				
CVLAN Proprietary Links VALUE_AES_PROPRIETARY_LINKS	permanent	16																																				
►Communication_Manager																																						
MESSAGING																																						
►Messaging																																						
MSR																																						
►Media_Server																																						
SYSTEM_MANAGER																																						
►System_Manager																																						
SessionManager																																						
►SessionManager																																						
VSS																																						
►Voice_Portal																																						
Uninstall license																																						
Server properties																																						
Shortcuts																																						
Help for Licensed products																																						

### 7.3. 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**.

**Application Enablement Services**  
Management Console

Welcome: User cust  
Last login: Mon Aug 5 14:02:37 2019 from 192.168.100.251  
Number of prior failed login attempts: 0  
HostName/IP: devcon-aes/10.64.102.119  
Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE  
SW Version: 8.1.0.0.0.9-1  
Server Date and Time: Thu Aug 08 11:15:41 EDT 2019  
HA Status: Not Configured

AE Services | TSAPI | TSAPI LinksHome | Help | Logout


▼ AE Services

- ▶ CVLAN
- ▶ DLG
- ▶ DMCC
- ▶ SMS
- ▼ TSAPI
  - TSAPI Links
  - TSAPI Properties

**TSAPI Links**

Link	Switch Connection	Switch CTI Link #	ASAI Link Version	Security
<a href="#">Add Link</a>	<a href="#">Edit Link</a>	<a href="#">Delete Link</a>		

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 *devcon* is selected. For **Switch CTI Link Number**, select the CTI link number from **Section 5.2**. Set **Security** to *Both* or *Encrypted* to provide an encrypted client connection. Retain the default values in the remaining fields.

**Application Enablement Services**  
Management Console

Welcome: User cust  
Last login: Mon Nov 25 11:40:30 2019 from 192.168.100.251  
Number of prior failed login attempts: 0  
HostName/IP: devcon-aes/10.64.102.119  
Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE  
SW Version: 8.1.0.0.0.9-1  
Server Date and Time: Mon Nov 25 12:33:34 EST 2019  
HA Status: Not Configured

AE Services | TSAPI | TSAPI LinksHome | Help | Logout

▼ AE Services

- ▶ CVLAN
- ▶ DLG
- ▶ DMCC
- ▶ SMS
- ▼ TSAPI
  - TSAPI Links
  - TSAPI Properties
- ▶ TWS

**Edit TSAPI Links**

Link: 1

Switch Connection: devcon ▼

Switch CTI Link Number: 1 ▼


ASAI Link Version: 10 ▼

Security: Both ▼

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

## 7.4. 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 cust  
Last login: Mon Aug 5 14:02:37 2019 from 192.168.100.251  
Number of prior failed login attempts: 0  
HostName/IP: devcon-aes/10.64.102.119  
Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE  
SW Version: 8.1.0.0.0.9-1  
Server Date and Time: Thu Aug 08 11:19:22 EDT 2019  
HA Status: Not Configured

Maintenance | Service ControllerHome | 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

▶ Utilities

▶ Help

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](#)

StartStopRestart ServiceRestart AE ServerRestart LinuxRestart Web Server

## 7.5. Obtain Tlink Name

Select **Security** → **Security Database** → **Tlinks** from the left pane. The **Tlinks** screen shows a listing of 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#DEVCON#CSTA-S#DEVCON-AES”, which provides an secure, encrypted client connection. Note the use of the switch connection “DEVCON” from **Section 7.3** as part of the Tlink name.

**Application Enablement Services**  
Management Console

Welcome: User cust  
Last login: Thu Nov 21 12:25:28 2019 from 192.168.100.250  
Number of prior failed login attempts: 0  
HostName/IP: devcon-aes/10.64.102.119  
Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE  
SW Version: 8.1.0.0.9-1  
Server Date and Time: Mon Nov 25 11:41:14 EST 2019  
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#DEVCON#CSTA#DEVCON-AES

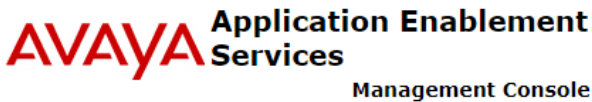
☐ AVAYA#DEVCON#CSTA-S#DEVCON-AES

Delete Tlink

## 7.6. 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.



Welcome: User cust  
Last login: Thu Aug 8 11:52:26 2019 from 192.168.100.250  
Number of prior failed login attempts: 0  
HostName/IP: devcon-aes/10.64.102.119  
Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE  
SW Version: 8.1.0.0.9-1  
Server Date and Time: Thu Aug 08 12:10:18 EDT 2019  
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 Id

vht

\* Common Name

vht

\* Surname

vht

\* User Password

.....

\* Confirm Password

.....

Admin Note

Avaya Role

None ▼

Business Category

Car License

CM Home

Css Home

CT User

Yes ▼

Department Number

Display Name

Employee Number


Employee Type



## 7.7. 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.

Verify that **Enable SDB for TSAPI Service, JTAPI and Telephony Web Services** is unchecked. In the event that security database is used by the customer with this parameter already enabled, then follow [3] to configure access privileges for the Callback user from **Section 7.6**.

 **Application Enablement Services**  
Management Console

Welcome: User cust  
Last login: Thu Aug 8 11:52:26 2019 from 192.168.100.250  
Number of prior failed login attempts: 0  
HostName/IP: devcon-aes/10.64.102.119  
Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE  
SW Version: 8.1.0.0.0.9-1  
Server Date and Time: Thu Aug 08 12:11:39 EDT 2019  
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
    - ⊕ CTI Users

**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

## 7.8. Export CA Trusted Certificate for VHT Callback

Export the CA Trusted Certificate to be copied to VHT Callback to establish a secure, encrypted TSAPI client connection as described in **Section 9.11**. Navigate to **Security → Certificate Management → CA Trusted Certificates** and selected the System Manager CA trusted certificate as shown below. Click the **Export** button.



# Application Enablement Services

## Management Console

Welcome: User cust

Last login: Mon Nov 25 12:30:49 2019 from 192.168.100.251

Number of prior failed login attempts: 0

HostName/IP: devcon-aes-10.64.102.119

Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE

SW Version: 8.1.0.0.0-9-1

Server Date and Time: Wed Nov 27 11:20:28 EST 2019





HA Status: Not Configured

Security | Certificate Management | CA Trusted Certificates
Home | Help | Logout


- ▶ AE Services
- ▶ Communication Manager Interface
- ▶ High Availability
- ▶ Licensing
- ▶ Maintenance
- ▶ Networking
- ▼ Security
  - ▶ Account Management
  - ▶ Audit
  - ▼ Certificate Management
    - CA Trusted Certificates
    - Server Certificates
    - Revocation Configuration

### CA Trusted Certificates

View
Import
Export
Delete

Alias	Status	Issued To	Issued By	Expiration Date
 serverCertDefault	valid	devcon-aes-035993595-labUseOnly	devcon-aes-035993595-labUseOnly	Jul 7, 2020
 avayaprcs	valid	Avaya Product Root CA	Avaya Product Root CA	Aug 14, 2033
 avaya_sipca	valid	SIP Product Certificate Authority	SIP Product Certificate Authority	Aug 17, 2027
 caSMGR	valid	System Manager CA	System Manager CA	Jun 24, 2029

The **Trusted Certificate Export** webpage is displayed with the content of the certificate. Copy and paste the certificate into a file with the .cer extension (e.g., *SystemManagerCA.cer*) and copy it to the Callback server.



# Application Enablement Services

## Management Console

Welcome: User root

Last login: Mon Nov 25 12:30:49 2019 from 192.168.100.25

Number of prior failed login attempts: 0

HostName/IP: devcon-aes/10.64.102.119

Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE

SW Version: 8.1.0.0.0.9-1

Server Date and Time: Wed Nov 27 11:37:13 EST 2019

HA Status: Not Configured

---

**Security | Certificate Management | CA Trusted Certificates**
**Home | Help | Logout**

- ▶ AE Services
- ▶ Communication Manager Interface
- ▶ High Availability
- ▶ Licensing
- ▶ Maintenance
- ▶ Networking
- ▼ Security
  - Account Management
  - Audit
  - ▼ Certificate Management
    - CA Trusted Certificates
    - Server Certificates
    - Revocation Configuration
  - Enterprise Directory
- ▶ Host AA
- ▶ PAM
- ▶ Security Database
- Session Timeouts
- Standard Reserved Ports

### Trusted Certificate Export

**Issued To:** System Manager CA  
**Issued By:** System Manager CA  
**Expiration Date:** Jun 24, 2029

**Certificate PEM:**

```
-----BEGIN CERTIFICATE-----
MIIDWZCCAkoGAgIBAgIJ8GlydYe4AUwDQYJKoZIhvcNAQELBQAwwOzEaMBgGA1UEAwRU3lzdGVtIEI1bmFnZXIgdXN0ExDTALBgNVBASBE1HTVQxQjAMBgNVBAoMBUFWQVBI MBM4XDTE5MDYyYnZAYmJkyM10xOTDI5MDYyNDAYMjkYK1owOzEaMBgGA1UEAwRU3lzdGVtIEI1bmFnZXIgdXN0ExDTALBgNVBASMBE1HTVQxQjAMBgNVBAoMBUFWQVBI MBIBJANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEak1PN0dsObS1lrQGcbIsCZR09LH8h911UgHtaCSmgRKvr7JI9Pzc6dkXgUTTUC8h5S9nLe1GP9CZd/Mq r6e3HsouQvQd84sbwQBcQagBREK8+28XrBiU5APqEGKO5SRAK1NG3dvN/cj4KUAAOWXG+ZYm8Gof Fld9TSLSXeP4w7rnPkav05HerWG258L287E8QQp+anO3K3QEBARxg6nfEvEMwTLUcyblgZ4LvOVY TaSswU9/ZOO5/9clt9o2A1y9aIEFzgQuwu66tsmtcw6eU9w6PybQrSMS7Vqox7MC9ZluBA2pyCF7 AMhAWNGM3T+vn+hkvYVnFj4cUvkIQnBqUQIDAABo2MwyTAPBgNVHRMBAf8EBTADAQH/MB8GA1Ud IwQYMBAAFIJ9kNv34SKOVSz/ruw/up6CCrU3MBOGA1UdDgQWBBSbfZDb9+EijlUm f67sp7qeggg1 N2AoBGNVHQ8BAf8EBACAYYwDQYJKoZIhvcNAQELBQAQdgEBAANNod6Ny4BxxLABZRO851BIHCc kKmTGouy7HK9W4j3fwxfUSEWEVFQemp1ZH936TSq8BuHDjfi33ZEzqCBk0svobzh2odLo063gs S7mCoRxyFAAG36RNQRiz4TyfuR1nkM4LNbPgppHs56ivsz/BzkWM9NMKn+nDKAgEisOwtQza5Zp4Z RUDhdIPer2R9oa7T+/7LyR4dB2ukUmmWyX1G9rdjY2dq8y9zbvj9caENULUZQHJ3S4dpWdHI33hg 9b55eFeVjz7dSIltq/Ctz86VTQ+cN+T2LiXlj6/6oaH5RAufjMuyFl2ex+rK5wn66aZLZENx50H GYB6oE1keAA=
-----END CERTIFICATE-----
```

Close

## 8. Configure VHT Interactive Voice Gateway (IVG)

This section covers the configuration of IVG, including a sub-section on the configuration of TLS/SRTP. Configuration is accomplished by accessing the browser-based IVG management system using the URL “http://<ip-address>:2020”, where <ip-address> is the IP address of the IVG server. Log in with the appropriate credentials (not shown).

From the IVG management system, navigate to **Administration** → **Service Providers** to display the **Service Provider Editor** shown below. In the **Service Provider** field, select the appropriate site name (e.g., *VHT-ServiceProvider*) and enter the desired **Domain Name** and **Domain Properties**. Scroll down to the **License Port Allocation** section and set the **Max Available Ports**.

**Note:** Alternatively, the VHT IVG application provisioning can be configured automatically during the install using the IVG installer. Refer to [6] for details.

The screenshot displays the VHT Service Provider Editor web interface. At the top, there is a header bar with the VHT logo (a red 'v' inside a circle followed by 'ht') and the text 'Powered by the Holly Voice Platform'. To the right of the logo, the text 'HVP-6.3.28-2862-44233' is visible. Below the logo, there are navigation tabs: 'Administration', 'Reports', 'Configuration', and 'Dashboard'. To the right of these tabs, there are dropdown menus for '<all service providers>', '<all affiliates>', and '<all applications>'. Further right, it shows 'user: administrator' and a 'Logout' link. The main content area has a title 'Service Provider Editor' in orange. Below this title, there are three main sections: 1. 'Select Service Provider' (with a close button): This section contains three input fields. 'Service Provider:' is a dropdown menu with 'VHT-ServiceProvider' selected. 'Domain Name:' and 'Domain Description:' are text input fields, both containing 'VHT-ServiceProvider'. Below these fields is a button labeled 'Edit Affiliates...'. 2. 'Service Provider Contact Details' (with a close button): This section contains four input fields labeled 'Name:', 'Email:', 'Phone:', and 'Address:', each with an empty text box next to it. 3. 'Licence Port Allocation' (with a close button): This section contains two input fields. 'Max Available Ports:' has a text box with '999' entered. 'Warn Ports:' has a text box with '990' entered.

Scroll down to the **Application Parameters** section and click **Save Service Provider**. In the **Numbers Available** section, add the **DNIS Numbers**. The DNIS numbers were set to **78701**, which is used to route calls to IVG, and *outbound* as shown below.

The screenshot displays two configuration windows. The top window, titled "Application Parameters", features a "Key:" label followed by an empty text input field, and a "Value:" label followed by another empty text input field. Below these is a large, empty list box. To the right of the list box are three buttons: "Set", "Replace", and "Delete". Below the list box is a "Preset Parameters:" label followed by a dropdown menu currently showing "Set Application Type To CCXML". To the right of the dropdown is a "Set" button. At the bottom of this window are three buttons: "Delete the Service Provider", "Revert", and "Save Service Provider".

Below the first window is a section header "Service Provider Numbers" in orange text. Underneath is a second window titled "Numbers Available". It has a "DNIS Numbers:" label followed by two empty text input fields separated by a hyphen. Below these is a list box containing the following items: "78701 - 78701", "agntpriority - agntpriority", "outbound - outbound", "outreach - outreach", and "prec - prec". To the right of the list box are three buttons: "Add", "Replace", and "Delete".

Navigate to **Administration** → **Affiliates** to display the **Affiliate Editor** shown below. In the **Service Provider** field, select the appropriate site name (e.g., *VHT-ServiceProvider*) and enter the desired **Domain Name** and **Domain Properties**. During the initial configuration of the affiliate, the **Affiliate** field should be set to *<new affiliate>* from the drop-down menu.

**vht** Powered by the Holly Voice Platform HVP-6.3.28-2862-44233

<all service providers> <all affiliates> <all applications>

Administration Reports Configuration Dashboard user: administrator Logout

## Affiliate Editor

**Select Affiliate**

Service Provider: VHT-ServiceProvider

Affiliate: VHT-Affiliate

Domain Name: VHT-Affiliate

Domain Description: VHT-Affiliate

Edit Service Provider... Edit Applications...

**Affiliate Contact Details**

Name:

Email:

Phone:

Address:

**Licence Port Allocation**

Max Available Ports: 0 Warn Ports: 0 (Available 999)

Scroll down to the **Application Parameters** section and click **Save Affiliate**. In the **Numbers Available** section, add the **DNIS Numbers**. The DNIS numbers were set to *78701*, which is used to route calls to IVG, and *outbound* as shown below.

The screenshot displays two configuration windows. The top window, titled "Application Parameters", features a "Key:" label followed by an empty text input field, and a "Value:" label followed by another empty text input field. Below these is a large, empty list box. To the right of the list box are three buttons: "Set", "Replace", and "Delete". Below the list box is a "Preset Parameters:" label followed by a dropdown menu currently showing "Set Application Type To CCXML". To the right of the dropdown is a "Set" button. At the bottom of this window are three buttons: "Delete the Affiliate", "Revert", and "Save Affiliate".

The bottom window, titled "Numbers Available", has a "DNIS Numbers:" label followed by two empty text input fields separated by a hyphen. Below this is a list box containing the following entries: "78701 - 78701", "agntpriority - agntpriority", "outbound - outbound", "outreach - outreach", and "prec - prec". To the right of the list box are three buttons: "Add", "Replace", and "Delete".

Navigate to **Administration → Applications** to display the **Application Editor** shown below. This section will cover the **Inbound** application. In the **Service Provider** field, select the appropriate site name (e.g., *VHT-ServiceProvider*) and affiliate added in the previous step. During the initial configuration of the application, the **Application** field should be set to *<new application>* from the drop-down menu. Next, enter the desired **Name** and **Description**.

Scroll down to the URLs section and insert the appropriate **URL** (e.g., [http://localhost:8080/VIS/PlatformSupport\\_HVP/Begin?Tenant=VHT&MODE=HVPavaya](http://localhost:8080/VIS/PlatformSupport_HVP/Begin?Tenant=VHT&MODE=HVPavaya)).

The screenshot displays the VHT Application Editor interface. At the top, the VHT logo is visible with the text "Powered by the Holly Voice Platform". The navigation bar includes "Administration", "Reports", "Configuration", and "Dashboard". The user is logged in as "administrator".

The "Application Editor" section is active. It contains a "Select Application" panel with the following fields:

- Service Provider: VHT-ServiceProvider
- Affiliate: VHT-Affiliate
- Application: VHT\_Inbound
- Name: VHT\_Inbound
- Description: VHT\_Inbound
- Licence Exception URL: (empty)

An "Edit Affiliate..." button is located to the right of the "Select Application" panel.

The "URLs" section is also visible, containing a table with the following data:

URL:	Fetch Time Out:	URLs:	Actions:
	sec	<a href="http://localhost:8080/VIS/PlatformSupport_HVP/Begin?Tenant=VHT&amp;MODE=HVPavaya">http://localhost:8080/VIS/PlatformSupport_HVP/Begin?Tenant=VHT&amp;MODE=HVPavaya</a>	<div>Add</div> <div>Replace</div> <div>Delete</div> <div>Move Up</div> <div>Move Down</div>

In the **Application Parameters** section, add the following **Keys**:

- **ap.connhdrstodlg** = *1*
- **type** = *application/voicexml+xml*

Click **Save Application**. In the **Numbers Available** section, add the **DNIS Number**. The DNIS number that was added was *78701* as shown below.

The screenshot displays two configuration windows. The top window, titled "Application Parameters", features a "Key:" and "Value:" input area. Below this is a list of parameters: "ap.connhdrstodlg = 1", "failure\_destination =", and "type = application/voicexml+xml". To the right of the list are buttons for "Set", "Replace", and "Delete". Below the list is a "Preset Parameters:" section with a dropdown menu showing "Set Application Type To CCXML" and a "Set" button. At the bottom of this window are buttons for "Delete the Application", "Revert", and "Save Application". The bottom window, titled "Numbers Available", has a "DNIS Numbers:" label followed by two input fields separated by a hyphen. Below these is a list containing "78701 - 78701". To the right of the list are buttons for "Add", "Replace", and "Delete".



Repeat the above steps for the **Outbound** application. In the **Service Provider** field, select the appropriate site name (e.g., *VHT-ServiceProvider*) and affiliate added in the previous step. During the initial configuration of the application, the **Application** field should be set to *<new application>* from the drop-down menu. Next, enter the desired **Name** and **Description**.

Scroll down to the URLs section and insert the appropriate **URL** (e.g., [http://localhost:8080/VIS/PlatformSupport\\_HVP/Outbound?MODE=HVPavaya](http://localhost:8080/VIS/PlatformSupport_HVP/Outbound?MODE=HVPavaya)).

The screenshot displays the VHT Application Editor interface. At the top, the VHT logo is shown with the text "Powered by the Holly Voice Platform". The top navigation bar includes links for "Administration", "Reports", "Configuration", and "Dashboard". On the right, there are dropdown menus for "call service providers", "call affiliates", and "call applications", along with the user "administrator" and a "Logout" link. The main heading is "Application Editor". Below this, the "Select Application" section contains fields for "Service Provider" (VHT-ServiceProvider), "Affiliate" (VHT-Affiliate), "Application" (VHT\_Outbound), "Name" (VHT\_Outbound), "Description" (VHT\_Outbound), and "Licence Exception URL". An "Edit Affiliate..." button is located to the right. The "URLs" section below has a "URL:" field, a "Fetch Time Out:" field set to "sec", and a "URLs:" list containing the URL "http://localhost:8080/VIS/PlatformSupport\_HVP/Outbound?MODE=HVPavaya". To the right of the URL list are buttons for "Add", "Replace", "Delete", "Move Up", and "Move Down".

In the **Application Parameters** section, add the following **Key**:

- **type** = *application/voicexml+xml*

Click **Save Application**. The DNIS number that was added was *outbound* as shown below.

The screenshot displays two configuration windows. The top window, titled "Application Parameters", features a "Key:" label and an input field, a "Value:" label and an input field, and a list box containing "type = application/voicexml+xml". To the right of the list box are three buttons: "Set", "Replace", and "Delete". Below the list box is a "Preset Parameters:" label and a dropdown menu showing "Set Application Type To CCXML", with a "Set" button to its right. At the bottom of this window are three buttons: "Delete the Application", "Revert", and "Save Application". The bottom window, titled "Application Numbers", has a "DNIS Numbers:" label and two input fields separated by a hyphen. Below these is a list box containing "outbound - outbound". To the right of the list box are three buttons: "Add", "Replace", and "Delete".

Navigate to **Administration → Applications** to display the **Application Editor** shown below. This section will cover the **Agent Priority** application. With Agent Priority, Callback dials the agent first and then calls the customer. If the customer accepts the callback, the customer will be transferred to the agent. Agent Priority is enabled via the **EyeQueue** web page (refer to **Section 10.4** on accessing EyeQueue) under **Configuration → Call Flow → Treatment**. The **Queue Mode** would be set to *Agent Priority* instead of *Predictive*, where Callback dials the customer first. In the **Service Provider** field, select the appropriate site name (e.g., *VHT-ServiceProvider*) and affiliate added above. During the initial configuration of the application, the **Application** field should be set to *<new application>* from the drop-down menu. Next, enter the desired **Name** and **Description**.

Scroll down to the URLs section and insert the appropriate **URL** (e.g., *http://localhost:8080/VIS/AgentPriority*).

**VHT** Powered by the Holly Voice Platform

Administration Reports Configuration Dashboard user: administrator Logout

### Application Editor

**Select Application**

Service Provider: VHT-ServiceProvider

Affiliate: VHT-Affiliate

Application: VHT\_AgentPriority

Name: VHT\_AgentPriority

Description: VHT\_AgentPriority

Licence Exception URL:

Edit Affiliate...

**URLs**

URL:		Add
Fetch Time Out:	sec	
URLs:	http://localhost:8080/VIS/AgentPriority	Replace Delete Move Up Move Down

In the **Application Parameters** section, add the following **Keys**:

- **agent\_preview** = #1
- **type** = *application/voicexml+xml*

Click **Save Application**. In the **Numbers Available** section, add *agntpriority* as shown below.

The image shows two screenshots of a configuration interface. The top screenshot is the 'Application Parameters' window. It has a 'Key:' field and a 'Value:' field. Below these is a text area containing 'agent\_preview\_complete = #1' and 'type = application/voicexml+xml'. To the right of the text area are buttons for 'Set', 'Replace', and 'Delete'. Below the text area is a 'Preset Parameters:' dropdown menu set to 'Set Application Type To CCXML', with a 'Set' button next to it. At the bottom of the window are buttons for 'Delete the Application', 'Revert', and 'Save Application'. The bottom screenshot is the 'Numbers Available' window. It has a 'DNIS Numbers:' field with a hyphen between two input boxes. Below this is a text area containing 'agntpriority - agntpriority'. To the right of the text area are buttons for 'Add', 'Replace', and 'Delete'.

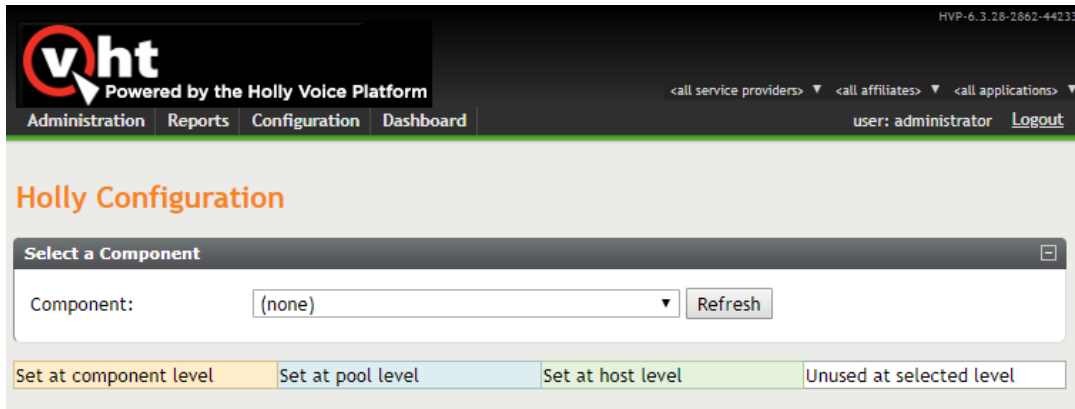
From an IVG SSL session, open the `/etc/VirtualHold/toolkit.properties` file and set the `com.virtualhold.toolkit.baseurl` parameter to <http://10.64.102.108/VHTPlatformWS-V5/>, which specifies the IP address of the Callback server as shown below. This allows IVG to communicate with the Callback system.

```
# Sample configuration file for SIP Avaya - Interactive Voice Gateway integrations

# URL for the Platform Toolkit web services
# Change the [PTK_server_address] and [PTK_port] to the address and port of the server
where the Platform Toolkit software resides
# For example, http://10.10.0.158:7000/VHTPlatformWS-v5/
# Ensure the path and VHTPlatformWS version is correct by opening it in a web browser
com.virtualhold.toolkit.baseurl=http://10.64.102.108/VHTPlatformWS-v5/
```

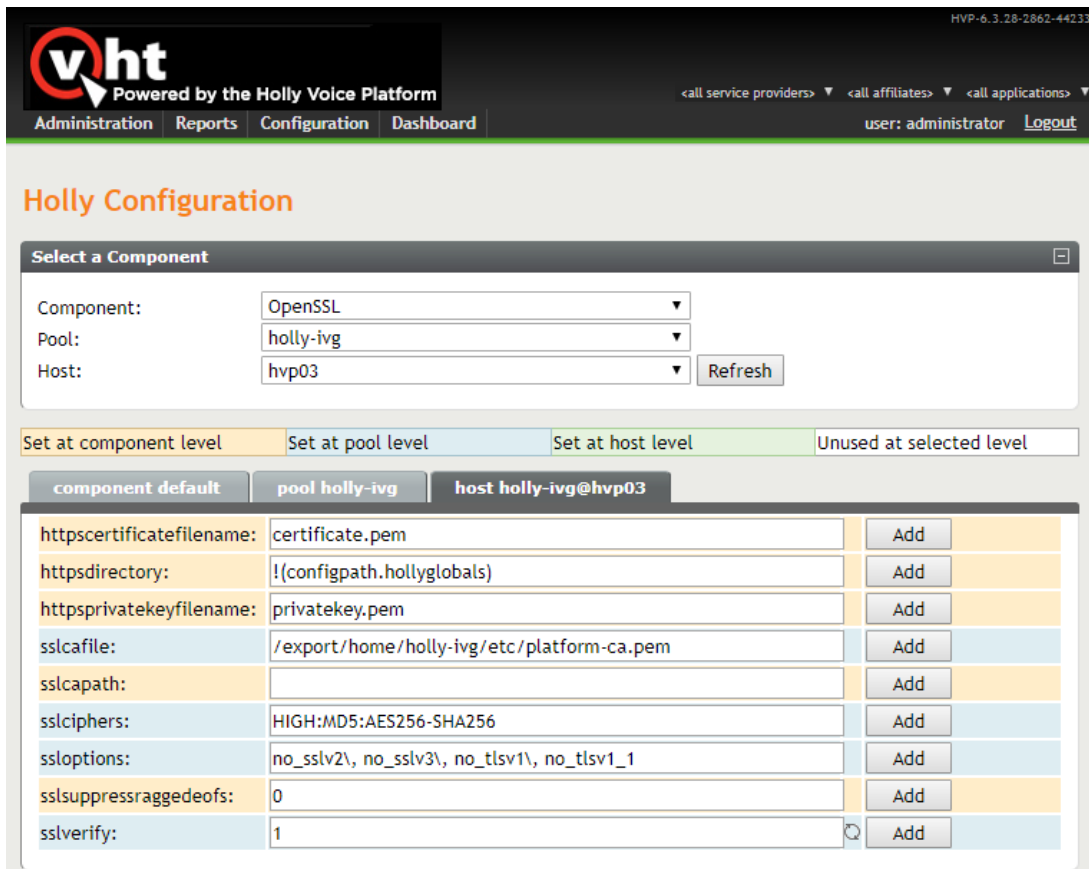
## 8.1. Configure TLS/SRTP on VHT IVG

This section covers the configuration of TLS/SRTP on IVG. In the browser-based IVG management system, navigate to **Configuration → Holly Configuration** to display the web page below.



The screenshot shows the VHT web interface. The top navigation bar includes 'Administration', 'Reports', 'Configuration', and 'Dashboard'. The 'Configuration' tab is active. Below the navigation bar, the 'Holly Configuration' section is displayed. A 'Select a Component' dropdown menu is set to '(none)'. Below the dropdown, there are four tabs: 'Set at component level' (selected), 'Set at pool level', 'Set at host level', and 'Unused at selected level'.


In the **Component** field, select *openssl* and set the **sslcafile** to the full path of the `platform-ca.pem` file created in **Step 4** on **Page 58** and click the **Add** button.



The screenshot shows the VHT web interface with the 'Holly Configuration' section. The 'Select a Component' dropdown menu is now set to 'OpenSSL'. Below the dropdown, there are three more dropdowns: 'Pool' set to 'holly-ivg', 'Host' set to 'hvp03', and a 'Refresh' button. Below these, there are four tabs: 'Set at component level' (selected), 'Set at pool level', 'Set at host level', and 'Unused at selected level'. Under the 'Set at host level' tab, there is a table with configuration fields and their values. The 'sslcafile' field is highlighted in blue and contains the path '/export/home/holly-ivg/etc/platform-ca.pem'. Each field has an 'Add' button next to it.

Field	Value	Action
httpscertificatefilename:	certificate.pem	Add
httpsdirectory:	!(configpath.hollyglobals)	Add
httpsprivatekeyfilename:	privatekey.pem	Add
sslcafile:	/export/home/holly-ivg/etc/platform-ca.pem	Add
sslcapath:		Add
sslciphers:	HIGH:MD5:AES256-SHA256	Add
ssloptions:	no_sslv2\, no_sslv3\, no_tlsv1\, no_tlsv1_1	Add
sslsuppressraggedeof:	0	Add
sslverify:	1	Add

Scroll down to the **codsupport** field and specify G.711 codec and RFC2833 as shown below and click the **Add** button.



Powered by the Holly Voice Platform

[Administration](#)
[Reports](#)
[Configuration](#)
[Dashboard](#)

HVP-6.3.28-2862-44233

[<all service providers>](#)
[<all affiliates>](#)
[<all applications>](#)

user: administrator
[Logout](#)

## Holly Configuration

Select a Component

Component:

Audio Provider - SIP

Pool:

holly-ivg

Host:

hvp03

Refresh

Set at component level

Set at pool level

Set at host level

Unused at selected level

component default

pool holly-ivg

host holly-ivg@hvp03

aaiheader:	User-to-User		Add
ackretries:	0		Add
alawoverride:	0		Add
amddetect:	1		Add
amddetectduration:	60.000		Add
answerearlymedia:	1		Add
basertpserverport:	11000		Add
busydetect:	1		Add
byertries:	6		Add
cancelnewcallresponse:	503		Add
cancelretries:	6		Add
caps:	0		Add
capx:	1		Add
codsupport:	g711ulaw,g711alaw,rfc2833		Add
decadicdetect:	0		Add

Lastly, scroll down and set **siptransport** to *TLS*, **srtpsupport** to 2 to enable SRTP, and **tlslistenport** to *5061*, and click the **Add** button by each modified field.

rfc2833payloadid:	101		Add
rfc3325display:	0	🔍	Add
rfc3325privacy:		🔍	Add
rtpbindhost:	S(FQDN)		Add
rtpchecksrc:	0	🔍	Add
rtpipexternal:		🔍	Add
rtpsendifthisearly:	0.003000	🔍	Add
rtptransmitinterval:	0.020000	🔍	Add
sendringingmessage:	1	🔍	Add
silencefilter:	1	🔍	Add
sipbindhost:	S(FQDN)		Add
sipipexternal:		🔍	Add
siplistenport:	5060		Add
siplistenport2:	5070		Add
siptransport:	TLS	🔍	Add
specialdetect:	1	🔍	Add
specialnoanswer:	0	🔍	Add
srtpsupport:	2	🔍	Add
sslcafile:	!(sslcafile.openssl)		Add
sslcapath:	!(sslcapath.openssl)		Add
sslciphers:	!(sslciphers.openssl)		Add
ssloptions:	!(ssloptions.openssl)		Add
sslsuppressraggedeof:	!(sslsuppressraggedeof.openssl)		Add
sslverify:	!(sslverify.openssl)	🔍	Add
subnetmask:	255.255.255.0	🔍	Add
tdddetect:	1	🔍	Add
tdddetectduration:	30.000	🔍	Add
tlslistenport:	5061		Add
tlslistenport2:	5071		Add
tonedetect:	1	🔍	Add

The next part of the configuration is performed from an IVG SSL session to manage the TLS certificates.

1. Change directory to /export/home/holly-ivg/etc.
2. Download the certificate.pem file, which will be imported to System Manager to establish mutual authentication TLS. This procedure to import the IVG certificate into System Manager is covered in **Section 6.5**.
3. Run the command: `openssl s_client -connect 10.64.102.117:5061 -showcerts` to retrieve the TLS certificate from Session Manager. The command output is displayed below. Copy the certificate (highlighted in **bold**) into the platform-ca.pem file (in the same directory as the certificate.pem file).

```
[root@hvp03 etc]# openssl s_client -connect 10.64.102.117:5061 -showcerts
CONNECTED(00000003)
depth=1 CN = System Manager CA, OU = MGMT, O = AVAYA
verify error:num=19:self signed certificate in certificate chain
verify return:0
140322587502408:error:14094410:SSL routines:SSL3_READ_BYTES:ssl3 alert handshake
failure:s3_pkt.c:1275:SSL alert number 40
140322587502408:error:140790E5:SSL routines:SSL23_WRITE:ssl handshake
failure:s23_lib.c:184:
---
Certificate chain
 0 s:/CN=10.64.102.117/O=Avaya/C=US
  i:/CN=System Manager CA/OU=MGMT/O=AVAYA
-----BEGIN CERTIFICATE-----
MIIEfjCCA2agAwIBAgIIa3Sx1Ps12w8wDQYJKoZIhvcNAQELBQAwOzEaMBGGA1UE
AwwRU3lzdGVtIE1hbmFnZXIqQ0ExDTALBgNVBAsMIBE1HTVQxXjAMBGNVBAoMBUFW
QVlBMB4XDTE5MDYyODAwMDAxNloXDTEyMDkyNjAwMDAxNlowNTEWMBQGA1UEAwWN
MTAuNjQ1MTAyLjExNzEOMAwGA1UECgwFQXZheWExCzAJBgNVBAYTA1VTMIIIBIjAN
BgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAvpsZqfT93R5ZiLnyM54kBlcDsk3E
pV/PsrSqBixBmfXPUID2iEGuYkcdh9pfEXFvdpFrNIPKhDaeOVHJaVnc6UgxQYk
wm+qKOsPpGiu8EFsP3kGcf82EZ7K0hSHy4B2nCGHwGH7hSEEUG0FEtYLS4f6zxH5
6PG5viHccQ5DF4ecWYscw2QsUHX1zoT9Z1UGWL5Ww/IXzqvxEcNtPYeb1kCAs8a0
oykdPtfmH5jtulCv135kZjWxdTOiukAlF20W2t680GSTQymbIdHh1K4xvgjDSS2
8f4f05hUJnH8F17YGFDE6wnTRffuIP4iPhKfslRGJM720hoEvMi3K/eqGwIDAQAB
o4IBijCCAYYwFAYDVR0RBA0wC4IjYXZheWEuY29tMAwGA1UdEwEB/wQCMAAwHwYD
VR0jBBGwFoAUm32Q2/fhIo5VJn+u7D+6noIKtTcwVQYIKwYBBQUHAQEESTBHMEUG
CCsGAQUFBzABhJlodHRwOi8vdmlldmNvb1lzbWdyLmF2YX1hLmNvbS9lamJjYS9w
dWJsaWN3ZWlvc3RhZHVzL29jc3AwDwYJKwYBBQUHMAEFBAIFADAdBgNVHSUEfjAU
BggrBgEFBQcDAQYIKwYBBQUHAWIwYyYGA1UdHwSBGDB+MHygeqB4hnZodHRwOi8v
dmRldmNvb1lzbWdyLmF2YX1hLmNvbS9lamJjYS9wdWJsaWN3ZWlvd2ViZGlzdC9j
ZXJ0ZGlzdD9jbWQ9Y3JsJmlzc3Vlcj1DTj1TeXN0ZW01MjBNYw5hZ2VvJT1wQ0Es
T1U9TUdNVCxPPUFWQVlBMB0GA1UdDgQWBRRfok7iXKnPKLOiWTEhhHKZjPWjSZA0
BgNVHQ8BAf8EBAMCA/gwDQYJKoZIhvcNAQELBQADggEABG8P9Q+KrZaHHcBNbI5a
8zRFH0hdESo6t31dG8xQTSBHWNcBJke5TCKkzzUmel93HvM2YSkXPwMuadqPfqN2
NTcwJGBejAPtNM+JnX5xHSihF4m8dNgptwuaVayCbS3NfxcZptb8LVG4SrUr6VbX
3eGN8pfa6RZom4VXYPLCIn5qGKkEqLdRnk/6d11JA5+rgYOE/hu5FfmKkIoNUG8i
6+TA7dAzaaqBvOsYJ9qARCAtoBlGxndjbVOJCLE4RnwU71Tn5VvRgfJvTdbrgM6s
9sRO/vZiW073sTzu8wSonMG+3/UOmWxtNnd2vQu9ow3LqG/7f8gTfMvTTnmRc5vI
uZw=
```



```

-----END CERTIFICATE-----
1 s:/CN=System Manager CA/OU=MGMT/O=AVAYA
i:/CN=System Manager CA/OU=MGMT/O=AVAYA
-----BEGIN CERTIFICATE-----
MIIDWzCCAkoGAWIBAgIIJ8GlydYe4AUWdQYJKoZIhvcNAQELBQAwOzEaMBGGA1UE
AwwRU3lzdGVtIE1hbmFnZXIqQ0ExDTALBgNVBAsMBE1HTVQxDjAMBGNVBAoMBUFW
QVlBMB4XDTE5MDYyNzAyMjkyM1oXDTI5MDYyNDAYMjkyM1owOzEaMBGGA1UEAwWR
U3lzdGVtIE1hbmFnZXIqQ0ExDTALBgNVBAsMBE1HTVQxDjAMBGNVBAoMBUFWQVlB
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEak1PNoDs0bSlqrQGcblsC
ZrRO9L8h911UgHtcaISmgRKVr7JI9Pzcd6kXgUTTUC8h8S9nLe1GP9CZd/Mqr6e3
HsouQvQDB4sbnWQbCqagBREK8+28XrBIu5APqEgKOnSRak1NG3dvN/cj4KUAoWXG
+ZYm8GofF1d9TSSLeXp4w7rnPKavO5HerWG258L287E8QQp+anO3K3QEBaRxg6nf
EVeMwTLCUyblgZ4LvOvyTaSswU9/Z005/9clt9o2A1y9aIEFzgQmuW66tsmtcw6e
U9w6PYbQrSMS7Vqox7MC9zluBA2pYCF7AMhAWNGM3T+vn+khvYVnFj4cUvkiQnBq
UQIDAQABo2MwYTAPBgNVHRMBAf8EBTADAQH/MB8GA1UdIwQYMBaAFJt9kNv34SKO
VSZ/ruw/up6CCrU3MB0GA1UdDgQWBBSbfZDb9+EijlUmf67sP7qeggq1NzAOBgNV
HQ8BAf8EBAMCAYYwDQYJKoZIhvcNAQELBQADggEBAAANNod6NY4BxxLABZRO851B
IHcCkKCMtG0uY7HKi9W4j3FwXfUSEWEVfQemP1ZH936TSq8BuHDjfi33ZEzqCbK0
svobzh2odLp063gsS7m9CoRxYfAG36RNQRiz4TyfUR1nkM4LNbPgppHs56ivsz/B
zkWM9NKn+nDkAgEisOwTQa5Zp4ZhRUdHdlPER2R9oa7T+/7Lyr4dB2ukUmmWYx1G
9rdjY2dq8y9zvbj9caENULUZQHj3S4dpWdHI33hg9b55eFVIjz7dSiIwq/cTz86Y
TQ+cn+T2LiLx6j/60aH5RaUfjMuyF12ex+rK5wnt6a6ZLzENx50HGYB6oE1keAA=
-----END CERTIFICATE-----

---
Server certificate
subject=/CN=10.64.102.117/O=Avaya/C=US
issuer=/CN=System Manager CA/OU=MGMT/O=AVAYA
---
No client certificate CA names sent
Server Temp Key: ECDH, prime256v1, 256 bits
---
SSL handshake has read 2498 bytes and written 138 bytes
---
New, TLSv1/SSLv3, Cipher is ECDHE-RSA-AES256-GCM-SHA384
Server public key is 2048 bit
Secure Renegotiation IS supported
Compression: NONE
Expansion: NONE
SSL-Session:
    Protocol : TLSv1.2
    Cipher : ECDHE-RSA-AES256-GCM-SHA384
    Session-ID:
    Session-ID-ctx:
    Master-Key:
D144FB2F1B4ADFB15FBB6690BF5D4C3EE80AEEA2501CE98ED9E859A368D43BC91BBCED2F559CAD4E8ABBF3
CF95FF0AA4
    Key-Arg : None
    Krb5 Principal: None
    PSK identity: None
    PSK identity hint: None
    Start Time: 1574789438
    Timeout : 300 (sec)
    Verify return code: 19 (self signed certificate in certificate chain)
---

```

4. Copy the content of the `certificate.pem` file to the `platform-ca.pem` file by using the following command: `cat certificate.pem >> platform-ca.pem`
5. Run the command: `su - holly-ivg`
6. Run the command: `hvpctl restart`

## 9. Configure VHT Callback

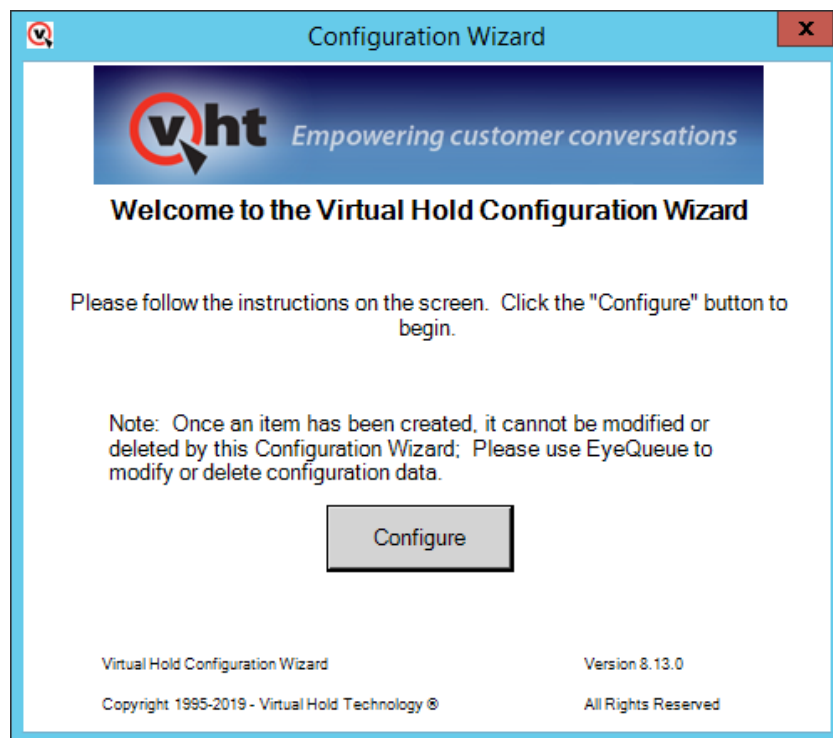
This section provides the procedures for configuring Callback. The procedures include the following areas:

- Launch VHT Configuration Wizard
- Administer Switch Connection
- Administer IVR Servers
- Administer Queues
- Administer Callback and Holding Queues
- Administer Incoming Extensions
- Administer Phone Number Configurations
- Administer Segment Variables
- Modify `site.config` File
- Configure TSAPI Real-Time Adapter
- Copy Application Enablement Services TLS Certificate for Avaya TSAPI Client

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

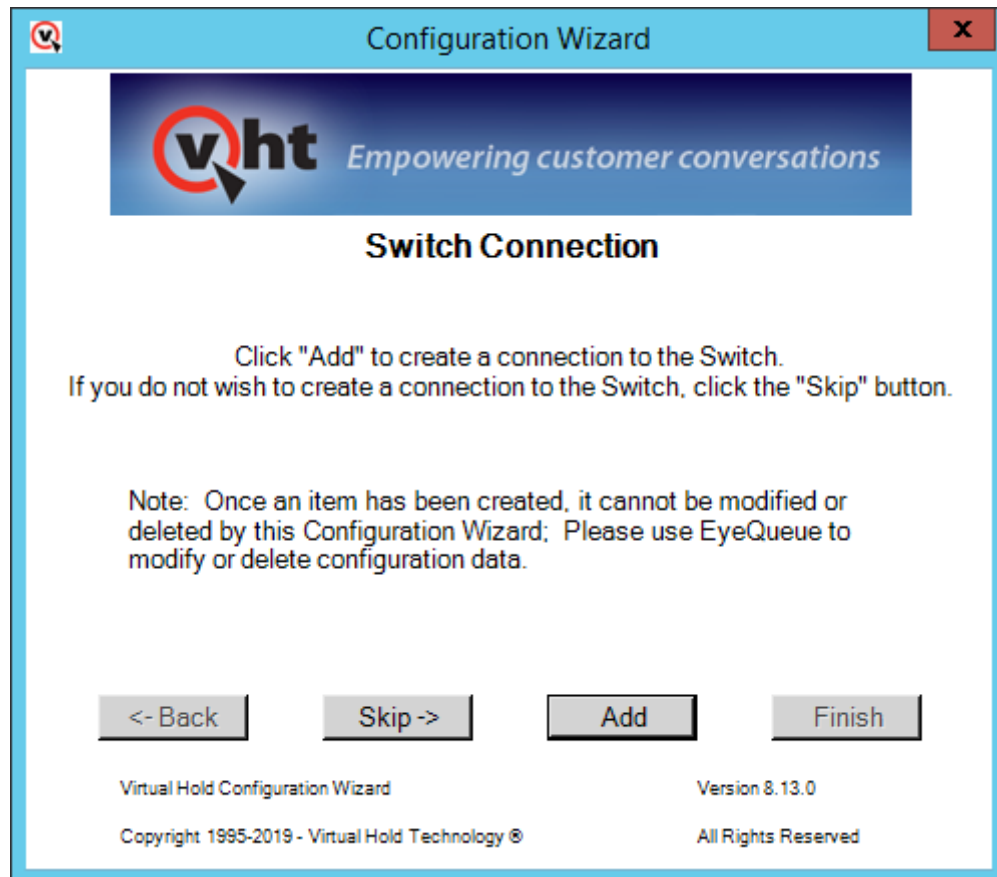
### 9.1. Launch Configuration Wizard

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.

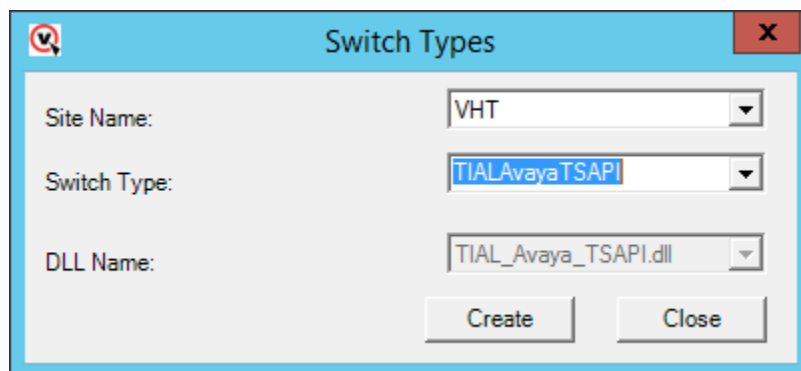


## 9.2. Administer Switch Connection

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 *TIALAvayaTSAPI* 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 **AES Avaya CTI** screen is displayed. Enter the following values for the specified fields and retain the default values for the remaining fields.

- **VH Server ID:** A descriptive name.
- **Server ID:** The Tlink name from **Section 7.5**.
- **Login ID:** The Callback user credentials from **Section 7.6**.
- **Password:** The Callback user credentials from **Section 7.6**.
- **Send Extra Buffers:** The desired extra buffers.
- **Receive Queue Size:** The desired queue size.
- **Use Private Data:** Set to *TRUE*.
- **Private Data Version:** Set to '8'.

**Note:** After configuring the **Server ID** to the secure TSAPI link, the **Server ID** column in the **dboAESAvayaCTIConfig** SQL table should be set to the same secure link.

The screenshot shows the 'AES Avaya CTI' configuration window. The fields are as follows:

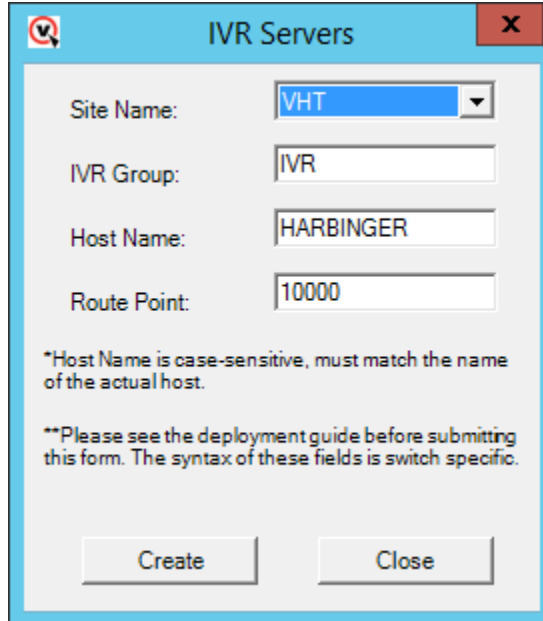
Field	Value
Site Name	VHT
VH Server ID	VHT_Test_01
Server ID	AVAYA#DEVCON#CSTA-S#DE
Invoke ID Type	LIB_GEN_ID
Login ID	vht
Password	Interop123!
Application Name	virtualhold
API Version	TS2
Send Queue Size	0
Send Extra Buffers	0
Receive Queue Size	0
Receive Extra Buffers	0
Use Private Data	TRUE
Private Data Version	8

At the bottom right, there is a 'Create' button.

### 9.3. Administer IVR Servers

Continue with the wizard until the **IVR Servers** screen is displayed (not shown). Click **Add** to create IVR server.

The screen below is displayed next. Set **Host Name** to the host name of the Callback server. Even though IVG is the IVR server, the Callback server initiates the callback. The **Route Point** is just a place holder at this point.



The screenshot shows a window titled "IVR Servers" with a standard Windows-style title bar (minimize, maximize, close buttons). The window contains the following fields and text:

- Site Name:** A dropdown menu with "VHT" selected.
- IVR Group:** A text input field containing "IVR".
- Host Name:** A text input field containing "HARBINGER".
- Route Point:** A text input field containing "10000".
- Footnote 1:** "\*Host Name is case-sensitive, must match the name of the actual host."
- Footnote 2:** "\*\*Please see the deployment guide before submitting this form. The syntax of these fields is switch specific."
- Buttons:** "Create" and "Close" buttons at the bottom.

## 9.4. 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 [4] 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:** (empty)
  - 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

**Queue 'VHT\_Test' created.**

**Buttons:** Create, Close

## 9.5. Administer Callback and Holding Queues

Continue with the wizard until the **Callback and Holding Queues** screen is displayed (not shown). Click **Add** to create callback and holding 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 (e.g., *sip:77203@10.64.102.117*).

In the **Holding Queues** sub-section, enter the Hold VDN extension from **Section 5.4.2** for **Holding Queue ID** and **Route Device**. For **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 (e.g., *sip:77202@10.64.102.117*).

Retain the default values for the remaining fields.

Callback and Holding Queues

Site Name: VHT

VH Server Switch Name: VHT\_Test\_01

Callback Queues

☒ Use VH Server Switch Name prefix

Callback Queue ID\*: 77203

Transfer Device: sip:77203@10.64.10

Callback Queue VHT\_Test\_01:77203 created.

Create

Holding Queues

☒ Use VH Server Switch Name prefix

Holding Queue ID\*: 77202

Route Device: 77202

Transfer Device: sip:77202@10.64.10

Holding Queue VHT\_Test\_01:77202 created.

Create

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

\* Verify VH Server Switch Name Close



## 9.6. 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

VH Server Switch Name: VHT\_Test\_01

Incoming Extensions

Extension\*: 77201

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: VHT\_Test\_01:77202

Callback Queue ID: VHT\_Test\_01:77203

UnderThreshold Queue ID: VHT\_Test\_01:77202

IB IVR Extension Group: NONE

OB IVR Extension Group: NONE

Incoming Extension: 77201 created.

Create

\* Verify VH 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 *78701*. For **Treatment Type**, select *20*. Retain the default values in the remaining fields, including blank for **VH Server Switch Name**.

**Incoming Extensions**

Site Name: VHT

Queue ID: VHT\_Test

VH Server Switch Name:

Incoming Extensions

Extension\*: 78701

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: VHT\_Test\_01:77202

Callback Queue ID: VHT\_Test\_01:77203

UnderThreshold Queue ID: VHT\_Test\_01:77202

IB IVR Extension Group: NONE

OB IVR Extension Group: NONE

Incoming Extension: 78701 created. **Create**

\* Verify VH Server Switch Name **Close**

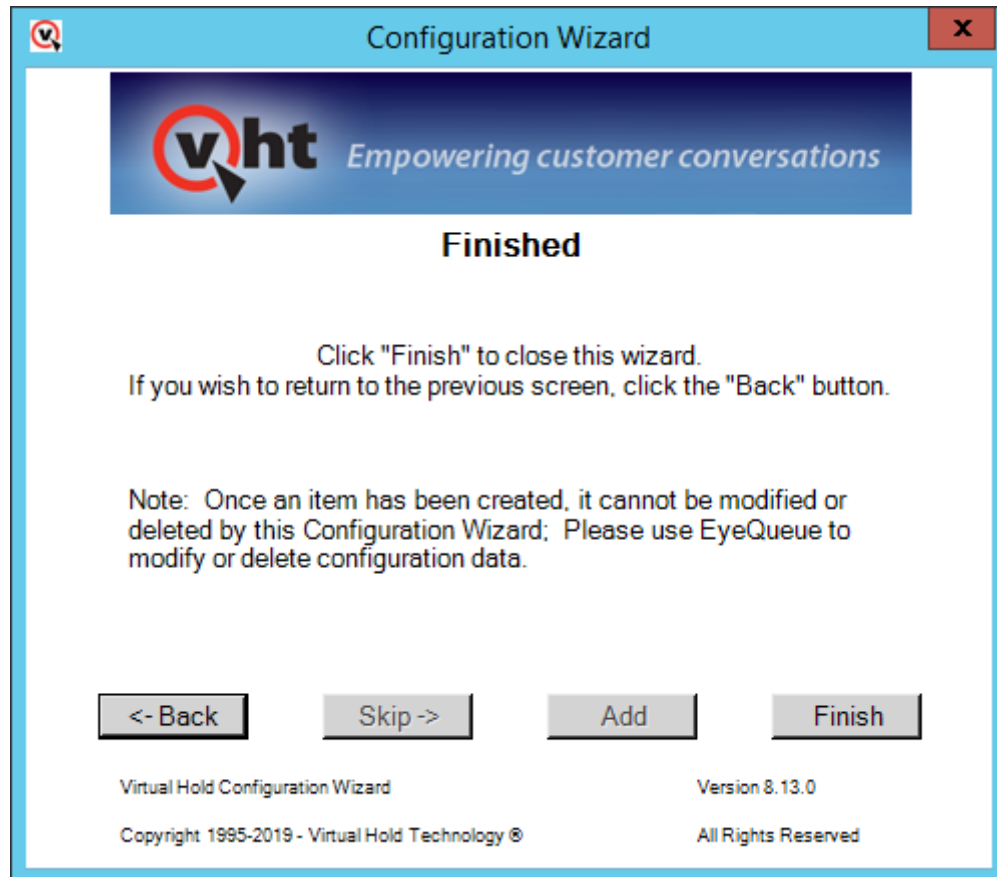
## 9.7. Administer Phone Number Configurations

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 and select the applicable country as shown below. For the compliance test, the **Min Length** field was set to '5' to allow callbacks to 5-digit extensions corresponding to local IP stations and the **Max Length** field was set to '12' to allow callbacks to 10-digit PSTN number prepended with a '9' (ARS access code) + '1' prefix code. Retain the default values in the remaining fields.

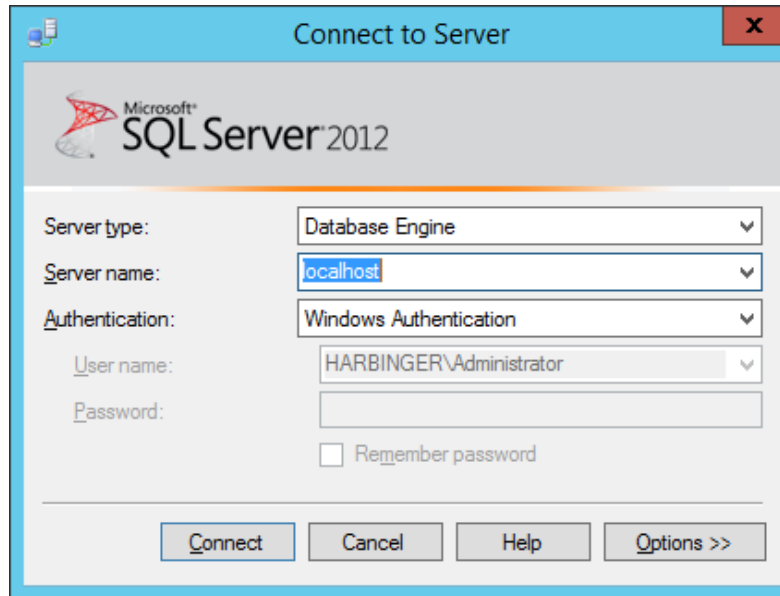
The screenshot shows a dialog box titled "PhoneNumberValidation" with a close button (X) in the top right corner. The dialog is divided into two main sections: "Update Country Id Dial Prefix and Suffix" on the left and "Update Phone Number Validation Min/Max Length" on the right. Both sections have a "Site Name" dropdown menu set to "VHT". In the left section, the "Country Search" dropdown is set to "1 - North America", and a list box below it also shows "1 - North America". There are empty text boxes for "Dial Prefix" and "Dial Suffix", and an "Update" button at the bottom. In the right section, the "Country Id" dropdown is set to "1 - North America", the "Min Length" text box contains "5", and the "Max Length" text box contains "12". Below these fields, it says "Update Successful", "Min Length: 5", and "Max Length: 12", followed by an "Update" button. At the bottom right of the dialog is a "Close" button.

When done, click **Finish** to exit the configuration wizard.



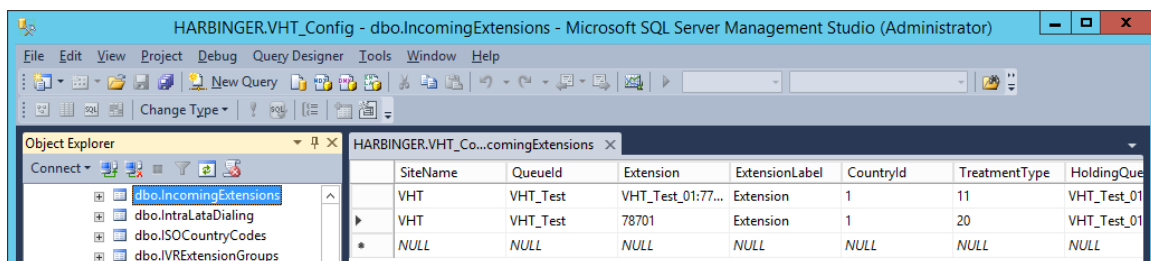
## 9.8. Administer Segment Variables

From the Callback server, navigate to **Start → Apps → Microsoft SQL Server 2012 → SQL Server Management Studio** to launch and connect to the SQL server.

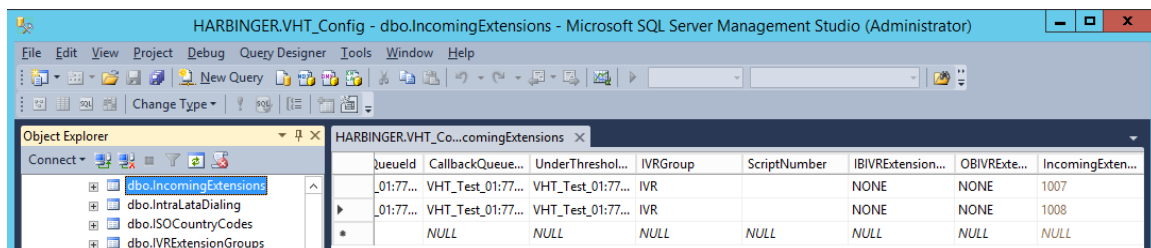


Navigate to **Databases → VHT\_Config → Tables → dbo.IncomingExtensions** in the left pane, right-click the entry and select **Edit Top 200 Rows**.

Locate the entry associated with Callback with “11” as **Treatment Type**.



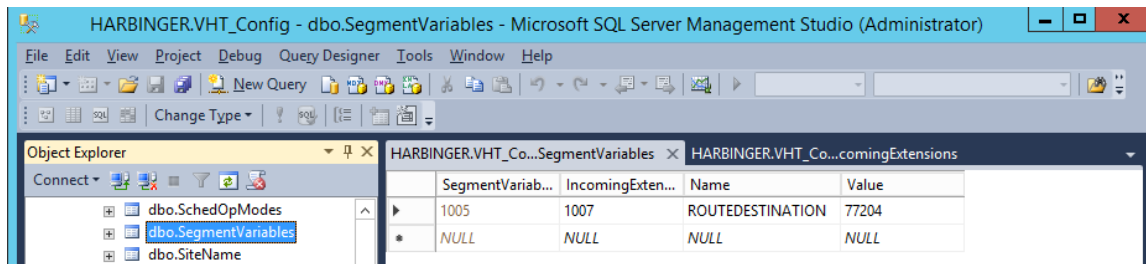
Scroll to the right to make a note of the associated **IncomingExtensionsId** value, in this case ‘1007’, as shown below.



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:** Set to *ROUTEDESTINATION*.
- **Value:** Set to the route VDN extension 77204.

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



## 9.9. Modify site.config File

Open the `site.config` file located in the `C:\Program Files (x86)\Virtual Hold Technology\Peripheral Monitor\` directory of the Callback server and modify the entries in bold to include the Callback server IP address (10.64.102.108), the IVG IP address (10.64.102.107), the Session Manager IP address (10.64.102.117), and the TLS port. The **ani** should include `<ani>@<Session Manager IP Address>`, where `<ani>` is the Automatic Number Identifier of the Callback server (e.g., [8005555555@10.64.102.117:5061](#)). Note that the TLS port 5061 was specified. The other entries may be left with their default values.

```

{vht_outbound_contact_client,
  [{voice_platform,ivg_plugin},
   {ivg_environment,avaya},
   {queue_manager_connection_ping_in_seconds,15},
   {ivr_group_name,"IVR"},
   {ivr_server_name,"harbinger"},
   {ivr_port_send_interval_ms,2000},
   {disposition_url,"http://10.64.102.108:4153/vht/occ"},
   {disposition_timeout,55000},
   {agent_priority_disposition_timeout,125000},
   {exclude_connections_on_failure,true},
   {time_to_exclude_on_failure_ms,150000},
   {default_connection_attributes,
    [{outdial_http_options,[{timeout,5000},{connect_timeout,5000}]},
     {request_header,
      [{"Accept","application/x-www-form-urlencoded"},
       {"Content-Type","application/x-www-form-urlencoded"}]},
     {enable_amd,true},
     {ring_no_answer_timeout,50000},
     {ccxml_fetch_timeout,5000},
     {agent_connect_timeout,25000},
     {agent_answer_timeout,35000},
     {agent_preview_timeout,60000},
     {tenant,"VHT"}]},
   {load_balanced_connections,
    [[{outdial_url,"http://10.64.102.107:8040/createsession"},
      {sip_endpoint,"10.64.102.117:5061"},
      {failure_destination,[]},
      {dnis,"outbound"},
      {vht_ccis_uri,"http://10.64.102.107:8080/CCIS/vht_hvp.ccxml"},
      {ani,"sip:8005555555@10.64.102.117:5061"},
      {node_id,7},
      {agent_priority_dnis,"agntpriority"},
      {outreach_dnis,"outreach"}]]]]].

```

## 9.10. Configure TSAPI Real-Time Adapter

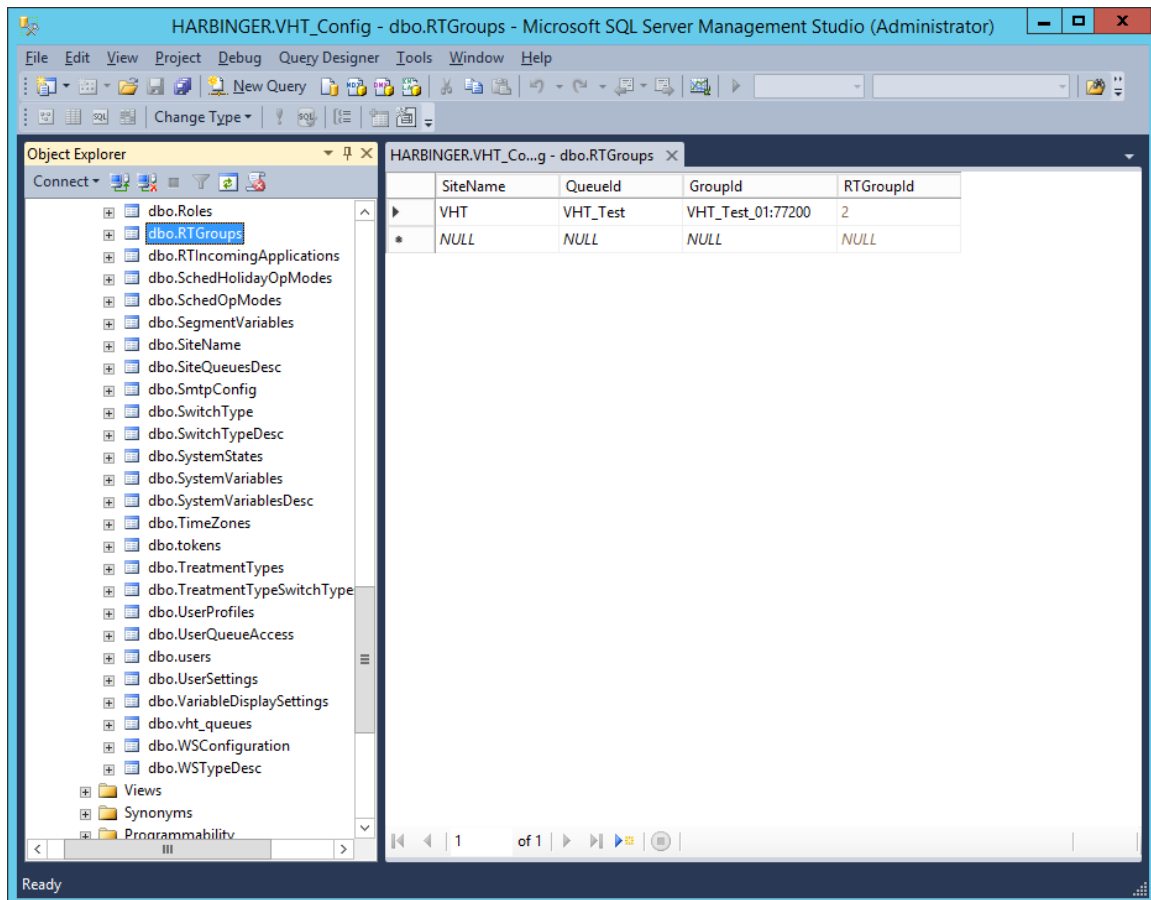
The Callback TSAPI Real-Time Adapter captures queue statistics, such as agent status of a monitored skill/split and can be displayed as shown in **Section 10.4**.

Open the `VHT_TsapiRealTimeAdapter_Console.exe.config` file located in the `C:\Program Files (x86)\Virtual Hold Technology\RealTimeAdapter\` directory of the Callback server and modify the entries in bold to include the Callback server IP address (10.64.102.108) for the **bolded** entries as shown below. In addition, the **SiteName** should be set to the appropriate value.

```
<?xml version="1.0" encoding="utf-8"?>
<configuration>
  <configSections>
    <sectionGroup name="VHTConfiguration">
      <section name="vhtLogging"
type="VHT.Common.Library.Configuration.Logging.VHTLoggingSection, VHT.Common.Library"
allowLocation="true" allowDefinition="Everywhere"/>
      <section name="vhtCommunication"
type="VHT.Common.Library.Configuration.Communication.VHTCommunicationSection,
VHT.Common.Library" allowLocation="true" allowDefinition="Everywhere"/>
    </sectionGroup>
  </configSections>
  <VHTConfiguration>
    <vhtLogging>
      <application level="10" name="TsapiRealTimeAdapter"
logFilePath="C:\Program Files (x86)\Virtual Hold Technology\VHLogs"/>
    </vhtLogging>
    <vhtCommunication>
      <QMCL reconnectIntervalSeconds="3">
        <Connections>
          <Connection connectionType="Primary">
            <Server ipAddress="10.64.102.108" port="6999"/>
            <Client ipAddress="10.64.102.108" port="0"/>
          </Connection>
        </Connections>
      </QMCL>
    </vhtCommunication>
  </VHTConfiguration>
  <appSettings>
    <add key="VhqmwmsUrl" value="http://10.64.102.108/VHQMWS/VHQMWS.asmx"/>
    <add key="SiteName" value="VHT"/>
    <add key="FrequencyMS" value="3000"/>
    <add key="UseDefaultsOnConnectionLost" value="false"/>
  </appSettings>
  <startup>
    <supportedRuntime version="v4.0" sku=".NETFramework,Version=v4.6.1"/>
  </startup>
</configuration>
```



Next, launch **SQL Server Management Studio** to launch and connect to the SQL server. Navigate to **Databases → VHT\_Config → Tables → dbo.RTGroups** in the left pane, right-click the entry and select **Edit Top 200 Rows**. Ensure that an entry exists with the appropriate **SiteName**, **QueueId**, and **GroupID**, which includes the VH server ID and hunt group extension (e.g., *VHT\_Test\_01:77200*) as shown below.



Lastly, navigate to `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Virtual Hold` in the Windows Registry and add **ExternalTrackingId** parameter as a string value and set it to *UCID*.

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

## 9.11. Copy Application Enablement Services TLS Certificate for Avaya TSAPI Client

Copy the CA Trusted Certificate (e.g., *SystemManagerCA.cer*) from **Section 0** to the Callback server. Store the certificate in the Program Files (x86)\Avaya\AE Services\TSAPI Client\certs\ca directory.

Next, edit the TSLIB.INI file in the Program Files (x86)\Avaya\AE Services\TSAPI Client directory and set the **Trusted CA File** parameter to the full path of the certificate file: C:\Program Files (x86)\Avaya\AE Services\TSAPI Client\certs\ca\SystemManagerCA.cer

When done, restart the VHT Core Monitor service.

```
[Telephony Servers]
10.64.102.119=450

; This is a list of the servers offering Telephony Services via TCP/IP.
; Either domain name or IP address may be used; default port number is 450
; The form is: host_name=port_number   For example:
;
; tserver.mydomain.com=450
; 127.0.0.1=450
;

[Config]

; When accessing Telephony Services via a secure, encrypted connection, the
; Application Enablement (AE) Services server sends its certificate to the
; TSAPI client, and the TSAPI client verifies that the certificate is signed
; by a trusted Certificate Authority (CA).
;
; If your organization has installed its own certificate on the AE Server,
; then the TSAPI client must have access to the trusted CA certificate(s)
; for the AE Services server certificate. Provide the location of a file
; containing the trusted CA certificate(s) here. For example:
;
Trusted CA File=C:\Program Files (x86)\Avaya\AE Services\TSAPI
Client\certs\ca\SystemManagerCA.cer
```

## 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	10	no	devcon-aes	established	146	141

Verify the status of the SIP trunk groups by using the **status trunk** command for the trunk group number administered in **Section 5.9**. Verify that all trunks are in the *service/idle* state as shown below.

```
status trunk 10
```

TRUNK GROUP STATUS			
Member	Port	Service State	Mtce Connected Ports Busy
0010/001	T00001	in-service/idle	no
0010/002	T00002	in-service/idle	no
0010/003	T00003	in-service/idle	no
0010/004	T00004	in-service/idle	no
0010/005	T00005	in-service/idle	no
0010/006	T00006	in-service/idle	no
0010/007	T00007	in-service/idle	no
0010/008	T00008	in-service/idle	no
0010/009	T00009	in-service/idle	no
0010/010	T00010	in-service/idle	no

Verify the status of the SIP signaling groups by using the **status signaling-group** command for the signaling group number administered in **Section 5.8**. Verify that the **Group State** is *in-service* as shown below.

```
status signaling-group 10
STATUS SIGNALING GROUP

Group ID: 10
Group Type: sip


Group State: in-service
```

When calls are active on VHT Callback, verify that SRTP is being used by checking the status of the SIP trunk between Communication Manager and Session Manager that's being used for the call. Use the **status trunk** command and navigate to **Page 3** to verify that SRTP is being used for the call as shown below.

```
status trunk 10/1
SRC PORT TO DEST PORT TALKPATH
src port: T000001
T000001:TX:192.168.100.59:5004/g711u/20ms/1-srtp-aescm128-hmac80
T000009:RX:10.64.102.107:11740/g711u/20ms/1-srtp-aescm128-hmac80
dst port: T000009
```

## 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 7.3**.



**Application Enablement Services**  
 Management Console

Welcome: User cust  
 Last login: Wed Nov 27 11:33:40 2019 from 192.168.100.250  
 Number of prior failed login attempts: 0  
 HostName/IP: devcon-aes/10.64.102.119  
 Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE  
 SW Version: 8.1.0.0.0.9-1  
 Server Date and Time: Wed Nov 27 12:01:28 EST 2019  
 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
  - ▶ Logs
  - ▶ Log Manager
  - ▼ **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
<input checked="" type="radio"/>	1	devcon	1	Talking	Wed Nov 20 15:25:55 2019	Online	18	3	142	147	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 (not shown). Click the IVG entity name from **Section 6.2.2**.

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

The screenshot shows the Avaya Aura System Manager 8.1 interface. The left sidebar contains a navigation menu with options like Home, Session Manager, Dashboard, Session Manager Ad..., Global Settings, Communication Prof..., Network Configur..., Device and Locati..., Application Confi..., System Status, and SIP Entity Monit... The main content area is titled "SIP Entity, Entity Link Connection Status" and includes a description: "This page displays detailed connection status for all entity links from all Session Manager instances to a single SIP entity." Below this, there's a section for "All Entity Links to SIP Entity: VHT-IVG" with a "Summary View" button. A table displays the connection status for one item, "devcon-sm", showing it is UP with a 200 OK reason code. The table has columns for Session Manager Name, IP Address Family, SIP Entity Resolved IP, Port, Proto., Deny, Conn. Status, Reason Code, and Link Status.

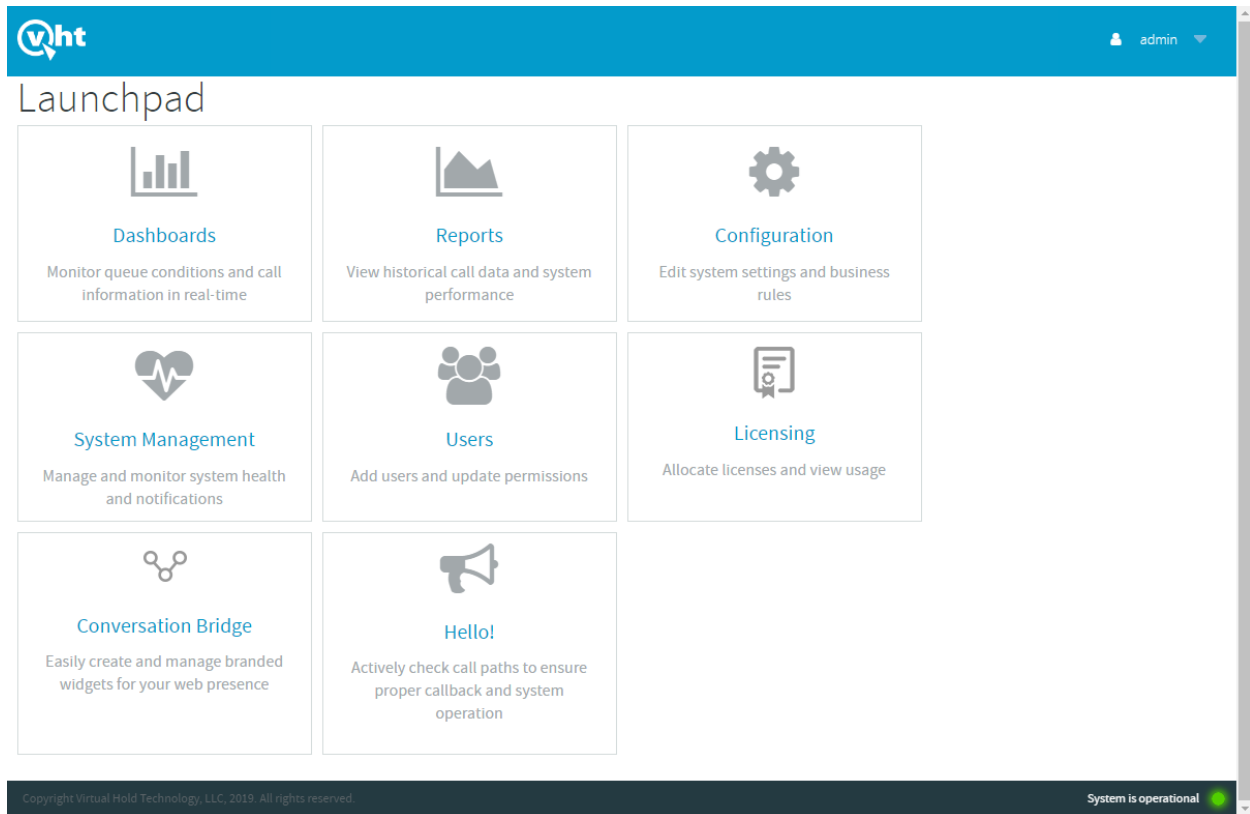
Session Manager Name	IP Address Family	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
devcon-sm	IPv4	10.64.102.107	5061	TLS	FALSE	UP	200 OK	UP

### 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.

The screenshot shows a login form for the VHT application. It includes fields for "User name" and "Password", a "Clear" button, and a "Login" button. The VHT logo is visible in the bottom right corner.

The **Launchpad** screen below is displayed. Select **System Management**.



In **System Status**, verify that the components are in-service and that the system is operational as shown below.

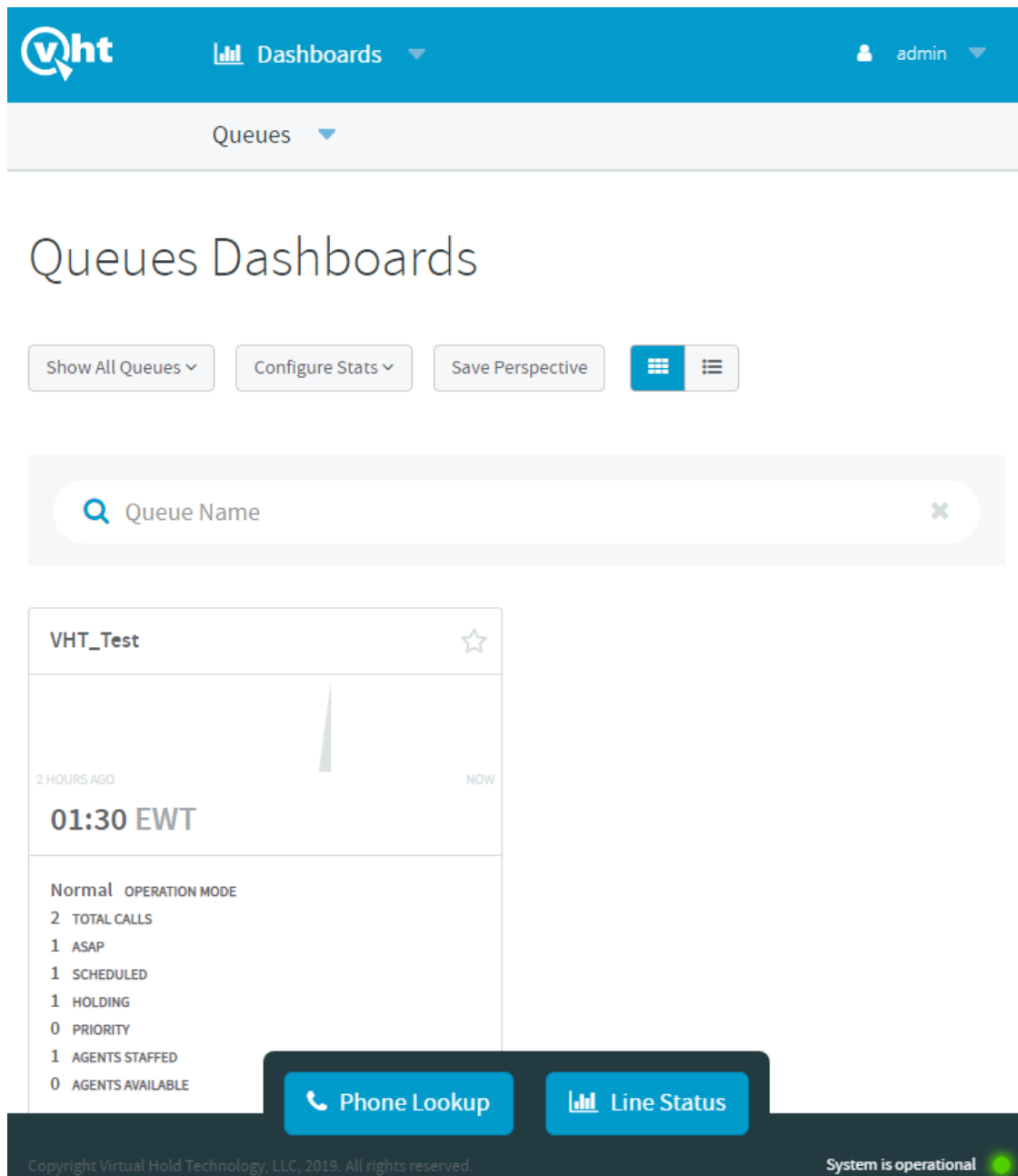
The screenshot displays the VHT System Management web interface. The top navigation bar is blue with the VHT logo on the left, a heart icon and 'System Management' in the center, and a user profile icon labeled 'admin' on the right. Below this is a light gray bar with a 'Status' dropdown menu. The main content area has a large 'System Status' heading on the left and a 'Manage Components' button on the right. The central part of the interface is a light green box containing two columns of component status cards. The left column, titled 'Core (HARBINGER)', shows the mode as 'STANDALONE' with a gear icon, followed by a list of components: CTI Connector, Queue Manager, License Server, Opmode Server, Provider, Real-Time Adapter, and Report Writer. The right column, titled 'Management (HARBINGER)', lists: Launchpad, Platform Toolkit, Web Monitor, Message Bus, Outbound Contact Client, and QWatch Client. Each component name is preceded by a green circular icon with a white upward-pointing arrow. At the bottom of the interface, a dark gray footer bar contains the copyright text 'Copyright Virtual Hold Technology, LLC, 2019. All rights reserved.' on the left and 'System is operational' with a green status indicator on the right.

Core (HARBINGER)	Management (HARBINGER)
Mode: STANDALONE	Launchpad
CTI Connector	Platform Toolkit
Queue Manager	Web Monitor
License Server	Message Bus
Opmode Server	Outbound Contact Client
Provider	QWatch Client
Real-Time Adapter	
Report Writer	

Copyright Virtual Hold Technology, LLC, 2019. All rights reserved. System is operational

From the **Launchpad** or from the drop-down menu at the top of the webpage, select **Dashboards**.

Make a few incoming ACD calls with an active call at the agent, call optioned to stay in queue, call scheduled for callback, and a call queue to the ACD split. Verify that the queue statistics in the screen below is updated in real-time to reflect proper active calls and expected wait time (EWT).





## 11. Conclusion

These Application Notes describe the steps required to integrate VHT Callback using Native TSAPI with Avaya Aura® Communication Manager, Avaya Aura® Session Manager, and Avaya Aura® Application Enablement Services. VHT Callback successfully handled callback requests from callers, provided estimated wait time, and reported real-time queue statistics. 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*, Release 8.1.x, Issue 2, July 2019, available at <http://support.avaya.com>.
2. *Administering Avaya Aura® Session Manager*, Release 8.1, Issue 1, June 2019, available at <http://support.avaya.com>.
3. *Administering and Maintaining Avaya Aura® Application Enablement Services*, Release 8.1.x, Issue 2, August 2019, available at <http://support.avaya.com>.
4. *VHT Callback Configuration Guide Version 8.11 or Later*, available at <https://insight.vhtcx.com>.
5. *VHT Callback Installation Guide Version 8.10.1 or Later*, available at <https://insight.vhtcx.com>.
6. *VHT Interactive Voice Gateway (IVG) Avaya Version 3.9*, available at <https://insight.vhtcx.com>.

---

**©2019 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).