



Avaya Solution & Interoperability Test Lab

Application Notes for Configuring VHT Callback using Genesys T-Server with Avaya Aura[®] Communication Manager, Avaya Aura[®] Session Manager, Avaya Aura[®] Application Enablement Services, and Avaya Aura[®] Experience Portal - Issue 1.0

Abstract

These Application Notes describe the configuration steps required to integrate VHT Callback using Genesys T-Server with Avaya Aura[®] Communication Manager, Avaya Aura[®] Session Manager, Avaya Aura[®] Application Enablement Services, and Avaya Aura[®] Experience Portal. VHT Callback is a contact center solution that calculates the expected wait time and maintains the caller's position in a virtual queue. VHT Callback can call the user back and connect to an agent when the caller's turn comes up. The integration with Avaya Aura[®] Communication Manager is achieved through Genesys T-Server and the Avaya Aura[®] Application Enablement Service TSAPI service for event monitoring and adjunct routing support. The integration with Avaya Aura[®] Experience Portal is achieved through an inbound and outbound VXML application. Calls to VHT Callback VXML applications are routed over a SIP trunk from Avaya Aura[®] Communication Manager via Avaya Aura[®] Session Manager.

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

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

TABLE OF CONTENTS

1.	Introduction.....	4
2.	General Test Approach	5
2.1.	Interoperability Compliance Testing.....	6
2.2.	Test Results	6
2.3.	Support	6
3.	Reference Configuration.....	7
4.	Equipment and Software Validated	8
5.	Configure Avaya Aura® Communication Manager.....	9
5.1.	Verify License	9
5.2.	Administer System Parameters Features.....	11
5.3.	Administer CTI Link.....	12
5.4.	Administer Vectors and VDNs	13
5.4.1.	Entry Vector and VDN	13
5.4.2.	Hold Vector and VDN	14
5.4.3.	Callback Vector and VDN	15
5.4.4.	Route Vector and VDN.....	16
5.5.	Enable UI Treatment for SIP Trunk Group.....	17
5.6.	Administer AAR Call Routing.....	18
6.	Configure Avaya Aura® Session Manager	19
6.1.	Launch System Manager.....	19
6.2.	Administer SIP Entity for Experience Portal	20
6.3.	Administer Routing Policy for Experience Portal.....	22
6.4.	Administer Dial Pattern for Experience Portal	23
7.	Configure Avaya Aura® Application Enablement Services	24
7.1.	Launch OAM Interface	24
7.2.	Verify License	25
7.3.	Administer TSAPI Link	27
7.4.	Restart Service.....	28
7.5.	Obtain Tlink Name.....	29
7.6.	Administer Callback User	30
7.7.	Verify Security Database	31
8.	Configure Avaya Aura® Experience Portal	32
8.1.	Launch Experience Portal Manager	32
8.2.	Administer VoIP Connection.....	33
8.3.	Administer Web Services User	34
8.4.	Administer Applications	35
8.4.1.	Configure Inbound Application	35
8.4.2.	Configure Outbound Application	38
9.	Configure VHT Callback.....	40
9.1.	Launch Configuration Wizard.....	40
9.2.	Administer Switch Connection	41
9.3.	Configure Genesys CTI T-Server Connections	42
9.4.	Administer IVR Servers.....	43
9.5.	Administer Queues.....	44

9.6.	Administer Callback and Holding Queues.....	45
9.7.	Administer Incoming Extensions.....	46
9.8.	Administer Phone Number Configurations.....	48
9.9.	Administer Segment Variables.....	50
9.10.	Configure Callback Outbound Application.....	52
9.11.	Configure TSAPI Real-Time Adapter.....	56
10.	Configure Genesys T-Server.....	59
10.1.	Launch Configuration Manager.....	59
10.2.	Administer DNS.....	60
10.3.	Administer TSAPI Connection.....	61
10.4.	Install Experience Portal Certificate.....	64
11.	Verification Steps.....	75
11.1.	Avaya Aura® Experience Portal.....	75
11.2.	Avaya Aura® Session Manager.....	76
11.3.	Verify VHT Callback.....	76
12.	Conclusion.....	80
13.	Additional References.....	80

1. Introduction

These Application Notes describe the configuration steps required to integrate VHT Callback using Genesys T-Server with Avaya Aura® Communication Manager, Avaya Aura® Session Manager, Avaya Aura® Application Enablement Services, and Avaya Aura® Experience Portal. VHT Callback is a contact center solution that calculates the expected wait time and maintains the caller's position in a virtual queue. VHT Callback can call the user back and connect to an agent when the caller's turn comes up. The integration with Avaya Aura® Communication Manager is achieved through Genesys T-Server and the Avaya Aura® Application Enablement Service TSAPI service for event monitoring and adjunct routing support. The integration with Avaya Aura® Experience Portal is achieved through an inbound and outbound VXML application. Calls to VHT Callback VXML applications are routed over a SIP trunk from Avaya Aura® Communication Manager via Avaya Aura® Session Manager.

As calls come into the contact center, VHT Callback monitors the expected wait time (EWT) and determines how calls are treated. If the EWT is less than the turn-on threshold, the calls are routed to a queue, as normal, to be answered by an agent. If the EWT is more than the turn-on threshold, the callers are offered several options. One option is to save the caller's places in line and call back when it is their turn. Another option is to stay in the queue to wait for an agent. The third option is to receive a callback at a later time chosen by the caller. If the first option is chosen, the caller provides phone number and name and then hangs up. When it is nearly the caller's turn in queue, VHT Callback calls the caller back, verifies that the caller is on the line, and transfers the call to the agent queue at high priority, which makes the call the next one to be answered by an agent.

VHT Callback uses Genesys T-Server to interact with the Avaya Aura® Application Enablement Services TSAPI service to query and monitor the agent's state and service speed, and uses the provided TSAPI event reports to calculate the EWT. Incoming calls are routed to the inbound VXML application via Avaya Aura® Experience Portal, where VHT Callback can play the EWT to the caller and provide the caller with options. VHT Callback VXML Interaction Server uses the Application Interface Web Service provided by Avaya Aura® Experience Portal to launch the outbound VXML application and send callback requests.

Calls to VHT Callback VXML applications are routed using a SIP trunk from Avaya Aura® Communication Manager via Avaya Aura® Session Manager.

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 (UII) data test cases were performed by using vector variables to assign UII 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 simulating a network outage to the Callback server and rebooting it. In addition, it was verified that Communication Manager routed calls to an available agent or queued the call when Callback was 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 interface between Avaya systems and VHT Callback using Genesys T-Server did not include use of any specific encryption features as requested by VHT.

2.1. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability testing.

- The event testing used internal logs to verify receiving and proper handling of CTI events by VHT Callback.
- The feature testing entailed placing calls manually from local SIP and H.323 Deskphones and PSTN phones to VHT Callback and verifying the following:
 - Adjunct route by Virtual Hold.
 - VHT Callback VXML applications launch.
 - Experience Portal using SIP as VoIP Connections.
 - VHT Callback playing Estimated Wait Time.
 - VHT Callback handling of caller options including callback, scheduled callback, and staying in queue.
 - VHT Callback storing and passing UI in callback calls.
- Calls between VHT Callback and local Avaya SIP and H.323 Deskphones and the PSTN with Shuffling enabled.
- The serviceability testing focused on verifying the ability of Experience Portal and VHT Callback to recover after a network outage or server reboot.

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:

- 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 using Genesys T-Server, 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

3. Reference Configuration

The configuration used for the compliance testing is shown in **Figure 1**. The configuration consisted of Callback using Genesys T-Server integrating with Application Enablement Services using a TSAPI connection and Experience Portal connected Session Manager via a SIP trunk. 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 78700 were routed to Experience Portal.

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

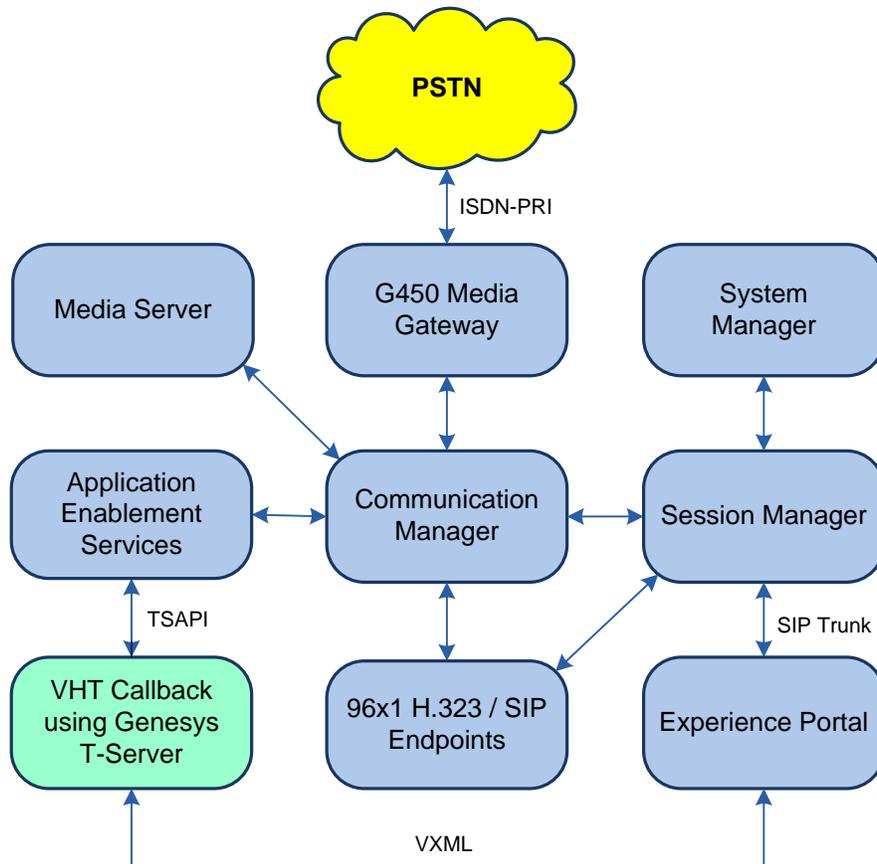


Figure 1: Compliance Testing Configuration

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	8.1.0.0.9-1
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 Aura® Experience Portal	7.2.2
Avaya 96x1 IP Deskphones	6.8003 (H.323) 7.1.5.0.11(SIP)
Avaya J179 SIP Deskphone	4.0.2.0.8
VHT Callback using Genesys T-Server on Microsoft Windows Server 2012 R2 Standard with <ul style="list-style-type: none">▪ VXML Interaction Server (VIS)▪ Genesys T-Server	8.13.0.4343 6.9.0 8.1.010.20

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 System Parameters Features
- Administer CTI Link
- Administer Vectors and VDNs
- Administer IP Node Names
- Enable UI Treatment for SIP Trunk Group
- Administer AAR Call Routing

Note: It is assumed that the SIP trunk between Communication Manager and Session Manager has already been configured. However, this section will cover enabling UI Treatment for the SIP trunk.

5.1. Verify License

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

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

```
display system-parameters customer-options                               Page 2 of 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
      Maximum Administered SIP Trunks: 12000 10
      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 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 UUI 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
```

5.3. 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
Extension: 77700
  Type: ADJ-IP
                                                    COR: 1
  Name: AES TSAPI Link
Unicode Name? 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 Experience Portal 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 Error! Reference source not found.**

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
Number: 201                Name: VHT Entry
Multimedia? n      Attendant Vectoring? n      Meet-me Conf? n      Lock? n
Basic? y          EAS? y      G3V4 Enhanced? y      ANI/II-Digits? y      ASAI Routing? y
Prompting? y      LAI? y      G3V4 Adv Route? y      CINFO? y      BSR? y      Holidays? y
Variables? y      3.0 Enhanced? y
01 adjunct        routing link 1
02 wait-time     10 secs hearing music
03 route-to     number 77202                with cov n if unconditionally
04
```

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
Name*: VHT Entry
Destination: Vector Number      201
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                                     Page 1 of 6
                                                    CALL VECTOR
Number: 203                                     Name: VHT Callback
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                                         Page 1 of 3
                                                    VECTOR DIRECTORY NUMBER
                                                    Extension: 77203
                                                    Name*: VHT Callback
                                                    Destination: Vector Number      203
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 Experience Portal using extension 78700. If the call to Experience Portal 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 Experience Portal fails.

```
change vector 204                                     Page 1 of 6
                                                    CALL VECTOR
Number: 204                                           Name: VHT Route
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 78700      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
Name*: VHT Route
Destination: Vector Number      204
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. Enable UI Treatment for SIP Trunk Group

On **Page 3** of the SIP trunk between Communication Manager and Session Manager, 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
                                                    UI Treatment: shared
                                                    Maximum Size of UI Contents: 128
                                                    Replace Restricted Numbers? n
                                                    Replace Unavailable Numbers? n

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

Show ANSWERED BY on Display? y
```

5.6. 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 Experience Portal (i.e., 78700).

```
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 Experience Portal and SIP stations.

```
change aar analysis 7                                       Page 1 of 2
                                AAR DIGIT ANALYSIS TABLE
                                Location: all
                                Percent Full: 2
```

Dialed String	Total Min	Total Max	Route Pattern	Call Type	Node Num	ANI Reqd
7	7	7	254	aar		n
78	5	5	10	lev0		n
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 No	FRL	NPA	Pfx	Hop	Toll	No.	Inserted Digits	DCS/ QSIG Intw	IXC
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

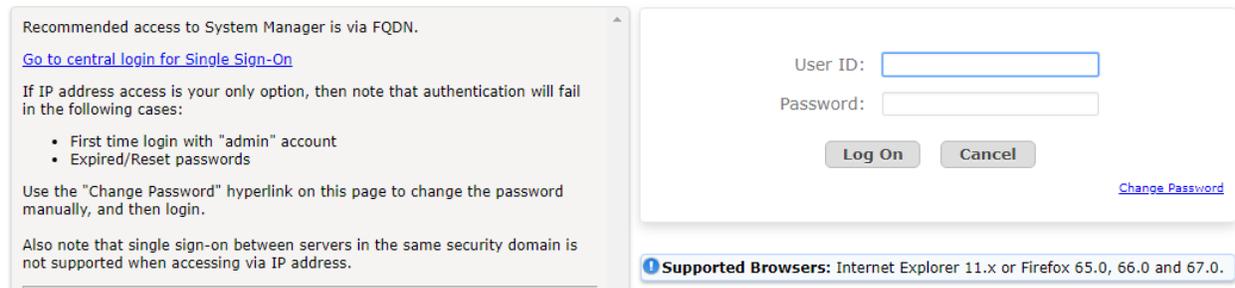
This section provides the procedures for configuring Session Manager. The procedures include the following areas:

- Launch System Manager
- Administer SIP Entity for Experience Portal
- Administer Routing Policy for Experience Portal
- Administer Dial Pattern for Experience Portal

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, and Application Enablement Services 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.



6.2. Administer SIP Entity for Experience Portal

A SIP Entity must be added for Experience Portal. To add a SIP Entity, select **SIP Entities** in the left pane 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 Experience Portal MPP.
- **Type:** Select *Voice Portal*.
- **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 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 visible. The left sidebar shows a navigation tree with 'SIP Entities' selected. The main content area is titled 'SIP Entity Details' and contains a 'General' section with the following fields:

- Name:** devcon-mpp
- FQDN or IP Address:** 10.64.102.111
- Type:** Voice Portal
- Notes:** (empty)
- Adaptation:** (empty)
- Location:** Thornton
- Time Zone:** America/New_York
- SIP Timer B/F (in seconds):** 4
- Minimum TLS Version:** Use Global Setting
- Credential name:** (empty)
- Securable:**
- Call Detail Recording:** none

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

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

At the bottom is the 'Monitoring' section:

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

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 Experience Portal 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-mpp link*).
- **SIP Entity 1:** Select the Session Manager.
- **Protocol:** Select the *TLS* protocol to allow secure SIP signaling to Experience Portal.
- **Port:** Port number to which the other system sends SIP requests.
- **SIP Entity 2:** Select the name of Experience Portal.
- **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										Filter: Enable	
<input type="checkbox"/>	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Deny New Service			
<input type="checkbox"/>	* devcon-mpp Link	devcon-sm	TLS	* 5061	devcon-mpp	* 5061	trusted	<input type="checkbox"/>			
Select : All, None											

SIP Responses to an OPTIONS Request

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

6.3. Administer Routing Policy for Experience Portal

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 shows the Avaya Aura System Manager 8.1 interface. The top navigation bar includes the Avaya logo, user information (Users), and various menu items (Elements, Services, Widgets, Shortcuts). A search bar and a user profile (admin) are also visible. The main content area is titled "Routing Policy Details" and contains the following sections:

- General**: Fields for Name (devcon-mpp Policy), Disabled (checkbox), Retries (0), and Notes (Experience Portal MPP).
- SIP Entity as Destination**: A "Select" button and a table listing SIP entities.
- Time of Day**: Buttons for "Add", "Remove", and "View Gaps/Overlaps", along with a table for defining time ranges.

Name	FQDN or IP Address	Type	Notes
devcon-mpp	10.64.102.111	Voice Portal	

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

6.4. Administer Dial Pattern for Experience Portal

In the sample configuration, extension 78700 was routed to the VHT inbound application on Experience Portal. 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.

AVAYA Aura® System Manager 8.1

Users | Elements | Services | Widgets | Shortcuts | Search | admin

Home | Routing

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

General

* **Pattern:** 78700

* **Min:** 5

* **Max:** 5

Emergency Call:

SIP Domain: -ALL-

Notes: VHT Callback on AEP

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		devcon-mpp Policy	0	<input type="checkbox"/>	devcon-mpp	Experience Portal MPP

Select : All, None

Denied Originating Locations

Add Remove

0 Items

<input type="checkbox"/>	Originating Location	Notes
--------------------------	----------------------	-------

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

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.

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

AVAYA Application Enablement Services Management Console

Home

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.

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

Home | Help | Logout

AVAYA Application Enablement Services Management Console

Licensing

Home | 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

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

The **Web License Manager** screen below is displayed. Select **Licensed Products** → **APPL_ENAB** → **Application_Enablement** in the left pane to display the **Application Enablement (CTI)** screen in the right pane.

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

WebLM Home	Application Enablement (CTI) - Release: 8 - SID: 10503000		Standard License file																																				
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	<div style="border: 1px solid black; padding: 5px; text-align: center;"> License File Host IDs: V7-94-F5-41-87-5E-01 </div>																																						
▼ Application_Enablement	<div style="border: 1px solid black; padding: 5px;"> Licensed Features </div>																																						
View license capacity	<div style="border: 1px solid black; padding: 5px;"> 13 Items Show All ▼ <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: left;">Feature (License Keyword)</th> <th style="text-align: left;">Expiration date</th> <th style="text-align: left;">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> </div>			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																																					
View peak usage																																							
ASBCE																																							
►Session_Border_Controller_E_AE																																							
COMMUNICATION_MANAGER																																							
►Call_Center																																							
►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**.

The screenshot shows the AVAYA Application Enablement Services Management Console. The top right corner displays system information: 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 11:15:41 EDT 2019, HA Status: Not Configured. The navigation bar includes 'AE Services | TSAPI | TSAPI Links' and 'Home | Help | Logout'. The left sidebar shows a tree view with 'AE Services' expanded to 'TSAPI Links'. The main content area is titled 'TSAPI Links' and contains a table with columns: Link, Switch Connection, Switch CTI Link #, ASAI Link Version, and Security. Below the table are buttons for 'Add Link', 'Edit Link', and 'Delete Link'.

The **Add TSAPI Links** screen is displayed next. The **Link** field is only local to the Application Enablement Services server and may be set to any available number. For **Switch Connection**, select the relevant switch connection from the drop-down list. In this case, the existing switch connection *devcon* is selected. For **Switch CTI Link Number**, select the CTI link number from **Section 5.3**. Set **Security** to *Both* or *Unencrypted* to provide an unencrypted client connection. Retain the default values in the remaining fields.

The screenshot shows the AVAYA Application Enablement Services Management Console. The top right corner displays system information: 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: 8.1.0.0.9-1, Server Date and Time: Mon Nov 25 12:33:34 EST 2019, HA Status: Not Configured. The navigation bar includes 'AE Services | TSAPI | TSAPI Links' and 'Home | Help | Logout'. The left sidebar shows a tree view with 'AE Services' expanded to 'TSAPI Links'. The main content area is titled 'Edit TSAPI Links' and contains a form with fields: Link (text input with value 1), Switch Connection (dropdown menu with value devcon), Switch CTI Link Number (dropdown menu with value 1), ASAI Link Version (dropdown menu with value 10), and Security (dropdown menu with value Both). Below the form are buttons for 'Apply Changes', 'Cancel Changes', and '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**.

AVAYA 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 11:19:22 EDT 2019
HA Status: Not Configured

Maintenance | Service Controller Home | Help | Logout

- ▶ AE Services
- ▶ Communication Manager Interface
- ▶ High Availability
- ▶ Licensing
- ▼ Maintenance
 - Date Time/NTP Server
 - ▶ Security Database
 - Service Controller**
 - ▶ Server Data
- ▶ Networking
- ▶ Security
- ▶ Status
- ▶ User Management
- ▶ 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](#)

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#DEVCON-AES”. Note the use of the switch connection “DEVCON” from **Section 7.3** as part of the Tlink name.

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: 8.1.0.0.0.9-1
Server Date and Time: Mon Nov 25 11:41:14 EST 2019
HA Status: Not Configured

AVAYA Application Enablement Services
Management Console

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: 8.1.0.0.0.9-1
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	<input type="text" value="vht"/>
* Common Name	<input type="text" value="vht"/>
* Surname	<input type="text" value="vht"/>
* User Password	<input type="password" value="....."/>
* Confirm Password	<input type="password" value="....."/>
Admin Note	<input type="text"/>
Avaya Role	<input type="text" value="None"/>
Business Category	<input type="text"/>
Car License	<input type="text"/>
CM Home	<input type="text"/>
Css Home	<input type="text"/>
CT User	<input type="text" value="Yes"/>
Department Number	<input type="text"/>
Display Name	<input type="text"/>
Employee Number	<input type="text"/>
Employee Type	<input type="text"/>

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**.

The screenshot displays the Avaya Application Enablement Services Management Console. At the top right, system information is shown: 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.

The main interface features a red navigation bar with "Security | Security Database | Control" and "Home | Help | Logout". A left-hand navigation pane lists various service categories, with "Security" expanded to show "Security Database" and "Control" selected. The main content area is titled "SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services" and contains two unchecked checkboxes: "Enable SDB for DMCC Service" and "Enable SDB for TSAPI Service, JTAPI and Telephony Web Services". An "Apply Changes" button is located below the checkboxes.

8. Configure Avaya Aura® Experience Portal

This section provides the steps for configuring Experience Portal using the Experience Portal Manager (EPM) web interface to support the VHT Callback solution. The procedure includes the following areas:

- Launch Experience Portal Manager
- Administer VoIP Connection
- Administer Web Services User
- Administer Applications

8.1. Launch Experience Portal Manager

In a web browser, enter **http://<ip-addr>** as the URL, where <ip-addr> is the IP address of Experience Portal Manager. Log in with the appropriate credentials.



The image shows a screenshot of the Avaya Aura Experience Portal 7.2.2 login page. At the top, the Avaya logo is displayed in red. Below it, a red banner contains the text "Avaya Aura® Experience Portal 7.2.2 (ExperiencePortal)". The main content area is white and features a "User Name:" label followed by a text input field. Below the input field is a "Submit" button. At the bottom left, there is a link labeled "Change Password".

8.2. Administer VoIP Connection

From the left pane of Experience Portal Manager, click **VoIP Connections**. To add a **SIP Connection**, select the **SIP** tab (not shown) on the **VoIP Connections** page and then click **Add**.

- **Name:** Provide descriptive name (e.g., *Session Manager*).
- **Proxy Transport:** Set to appropriate transport protocol (e.g., *TLS*).
- **Address:** Set to IP address of signaling interface of Session Manager.
- **Port:** Set to port used by Session Manager (e.g., *5061*).
- **Listener Port:** Set to port used by listener (e.g., *5061*).
- **SIP Domain:** Set to domain in which the SIP connection is configured.
- **Maximum Simultaneous Calls:** Set to maximum number of calls trunk can handle.

Default values may be used for remaining fields.

The screenshot shows the Avaya Aura Experience Portal 7.2.2 (ExperiencePortal) interface. The top navigation bar includes the Avaya logo, the user name 'Welcome, epadmin', and the last login time 'Last logged in Nov 22, 2019 at 7:35:22 AM PST'. The main navigation menu on the left lists various system management and configuration options. The main content area is titled 'Change SIP Connection' and contains the following configuration fields:

- Name:** Session Manager
- Enable:** Yes No
- Proxy Transport:** TLS (dropdown)
- Proxy Servers:** Proxy Servers DNS SRV Domain
- Proxy Servers Table:**

Address	Port	Priority	Weight	
10.64.102.117	5061	0	0	Remove
- Additional Proxy Server:**
- Listener Port:** 5061
- SIP Domain:** avaya.com
- P-Asserted-Identity:**
- Maximum Redirection Attempts:** 0
- Consultative Transfer:** INVITE with REPLACES REFER
- SIP Reject Response Code:** ASM (503) SES (480) Custom 503
- SIP Timers:**
 - T1:** 250 milliseconds
 - T2:** 2000 milliseconds
 - B and F:** 4000 milliseconds
- Call Capacity:**
 - Maximum Simultaneous Calls:** 10
 - All Calls can be either inbound or outbound
 - Configure number of inbound and outbound calls allowed
- SRTP:**
 - Enable:** Yes No
 - Encryption Algorithm:** AES_CM_128 NONE
 - Authentication Algorithm:** HMAC_SHA1_80 HMAC_SHA1_32
 - RTCP Encryption Enabled:** Yes No
 - RTP Authentication Enabled:** Yes No

An **Add** button is located at the bottom right of the configuration area.

8.3. Administer Web Services User

Create a web service user. Click on **Users** in the left pane and then click **Add** (not shown). Provide a descriptive name, select the **Web Services** radio button, and specify a password.

The screenshot displays the Avaya Aura Experience Portal 7.2.2 interface. At the top, the Avaya logo is on the left, and the user 'epadmin' is logged in, with a timestamp 'Last logged in Nov 22, 2019 at 7:35:22 AM PST'. A red navigation bar contains 'Avaya Aura® Experience Portal 7.2.2 (ExperiencePortal)', 'Home', 'Help', and 'Logoff' links. Below this, a breadcrumb trail reads 'Home > User Management > Users > Change User'. The left sidebar lists various system management options, with 'Users' under 'User Management' being the active section. The main content area, titled 'Change User', provides instructions: 'Use this page to modify a EPM user account. You can change the user role and password.' The form includes: Name: webservice; Enable: Yes (selected) / No; Roles: Administration, Auditor, Maintenance, Operations, Privacy Manager, Reporting, User Manager, and Web Services (checked); Created: 11/19/19 11:22 AM; Password and Verify Password fields; and Enforce Password Longevity: checked. Action buttons for Save, Apply, Cancel, and Help are located at the bottom of the form.

8.4. Administer Applications

This section covers the configuration of the inbound and outbound VHT Callback applications.

8.4.1. Configure Inbound Application

On the left pane, navigate to **System Configuration → Applications**. The **Applications** screen is displayed (not shown). Click **Add**. The **Add Application** screen is displayed. The following screen displays the configured inbound application used for the compliance test.

- **Name:** Provide descriptive name (e.g., *VHT-Inbound*).
- **Type:** Select *VoiceXML* from the drop-down menu.
- **VoiceXML URL:** Set to http://10.64.102.109:8080/VIS/PlatformSupport_AVP/Begin/?Tenant=VHT&MODE=AVPSIP, where *10.64.102.109* and *8080* are the IP address and Tomcat Port of the VHT Callback server.
- **Inbound:** Under **Application Launch** section, select *Inbound*.
- **Called Number:** Set to callback number (e.g., *78700*) as mentioned in **Section 6.4**. Calls to this number will be routed to Experience Portal via Session Manager.

Expand All | Collapse All

- ▼ **User Management**
 - Roles
 - Users
 - Login Options
- ▼ **Real-time Monitoring**
 - System Monitor
 - Active Calls
 - Port Distribution
- ▼ **System Maintenance**
 - Audit Log Viewer
 - Trace Viewer
 - Log Viewer
 - Alarm Manager
- ▼ **System Management**
 - EPM Manager
 - MPP Manager
 - Software Upgrade
 - System Backup
- ▼ **System Configuration**
 - Applications
 - EPM Servers
 - MPP Servers
 - SNMP
 - Speech Servers
 - VoIP Connections
 - Zones
- ▼ **Security**
 - Certificates
 - Licensing
- ▼ **Reports**
 - Standard
 - Custom
 - Scheduled
- ▼ **Multi-Media Configuration**
 - Email
 - HTML
 - SMS

You are here: [Home](#) > [System Configuration](#) > [Applications](#) > Change Application

Change Application

Use this page to change the configuration of an application.

Name: VHT-Inbound
Enable: Yes No
Type: VoiceXML
Reserved SIP Calls: None Minimum Maximum
Requested:

URI

Single Fail Over Load Balance

VoiceXML URL: **Verify**

Mutual Certificate Authentication: Yes No
Basic Authentication: Yes No

ASR Speech Servers

ASR:	Engine Types	Selected Engine Types
	Nuance	<None>

TTS Speech Servers

TTS:

Application Launch

Inbound Inbound Default Outbound

Number Number Range URI

Called Number: **Add**

Remove

Expand the **Advanced Parameters** section and configure the following fields:

- **Generate UCID:** Set to *Yes*.
- **Operation Mode:** Set to *Shared UUI*.
- **Transport UCID in Shared Mode:** Set to *Yes*.

Advanced Parameters ▾

Support Remote DTMF Processing: Yes No

DTMF Type Ahead Enabled: Yes No

Converse-On: Yes No

Network Media Service: Yes No

Early Media: Yes No

Sync FROM and PAI Headers: Yes No

Dialog URL Pattern:

VoiceXML Event Handler: ▾

CCXML Event Handler: ▾

Generate UCID: Yes No

Operation Mode: ▾

Transport UCID in Shared Mode: Yes No

Maximum UUI Length:

Fax Detection Enabled: Yes No

Fax Phone Number:

Video Enabled: Yes No

Video Screen Format: ▾

Video Minimum Picture Interval:

Save **Apply** **Cancel** **Help**

8.4.2. Configure Outbound Application

On the left pane, navigate to **System Configuration** → **Applications**. The **Applications** screen is displayed (not shown). Click **Add**. The **Add Application** screen is displayed. The following screen displays the configured inbound application used for the compliance test.

- **Name:** Provide descriptive name (e.g., *VHT-Outbound*).
- **Type:** Select *VoiceXML* from the drop-down menu.
- **VoiceXML URL:** Set to http://10.64.102.109:8080/VIS/PlatformSupport_AVP/Outbound/?Tenant=VHT&MODE=AVPSIP, where *10.64.102.109* and *8080* are the IP address and Tomcat Port of the VHT Callback server.
- **Outbound:** Under **Application Launch** section, select *Outbound*.

The screenshot displays the 'Change Application' configuration page in the Avaya Aura Experience Portal. The page title is 'Change Application' and the breadcrumb trail is 'Home > System Configuration > Applications > Change Application'. The page content includes the following sections:

- Name:** VHT-Outbound
- Enable:** Yes No
- Type:** VoiceXML
- Reserved SIP Calls:** None Minimum Maximum
- Requested:** [Empty field]
- URI:** Single Fail Over Load Balance
- VoiceXML URL:**
- Mutual Certificate Authentication:** Yes No
- Basic Authentication:** Yes No
- ASR Speech Servers:** Engine Types: Nuance; Selected Engine Types: <None>
- TTS Speech Servers:** TTS: No TTS
- Application Launch:** Inbound Inbound Default Outbound
- Speech Parameters:** [Collapsible section]
- Reporting Parameters:** [Collapsible section]
- Advanced Parameters:** [Collapsible section]

The page includes a left navigation menu with categories such as User Management, Real-time Monitoring, System Maintenance, System Management, System Configuration, Security, Reports, and Multi-Media Configuration. The bottom toolbar contains buttons for Save, Apply, Cancel, and Help.

Expand the **Advanced Parameters** section and configure the following fields:

- **Generate UCID:** Set to *Yes*.
- **Operation Mode:** Set to *Shared UUI*.
- **Transport UCID in Shared Mode:** Set to *Yes*.

Advanced Parameters ▾

Support Remote DTMF Processing: Yes No

DTMF Type Ahead Enabled: Yes No

Converse-On: Yes No

Network Media Service: Yes No

Early Media: Yes No

Sync FROM and PAI Headers: Yes No

Dialog URL Pattern:

VoiceXML Event Handler: ▾

CCXML Event Handler: ▾

Generate UCID: Yes No

Operation Mode: ▾

Transport UCID in Shared Mode: Yes No

Maximum UUI Length:

Fax Detection Enabled: Yes No

Fax Phone Number:

Video Enabled: Yes No

Video Screen Format: ▾

Video Minimum Picture Interval:

Save **Apply** **Cancel** **Help**

9. Configure VHT Callback

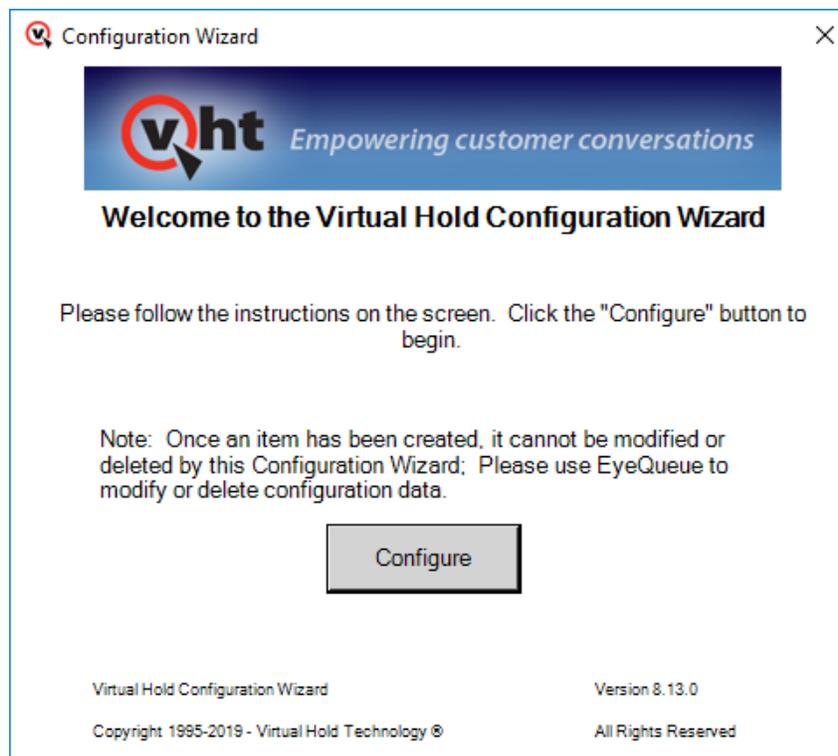
This section provides the procedures for configuring Callback. The procedures include the following areas:

- Launch VHT Configuration Wizard
- Administer Switch Connection
- Configure Genesys CTI T-Server Connections
- Administer IVR Servers
- Administer Queues
- Administer Callback and Holding Queues
- Administer Incoming Extensions
- Administer Phone Number Configurations
- Administer Segment Variables
- Configure Callback Outbound Application
- Configure TSAPI Real-Time Adapter

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

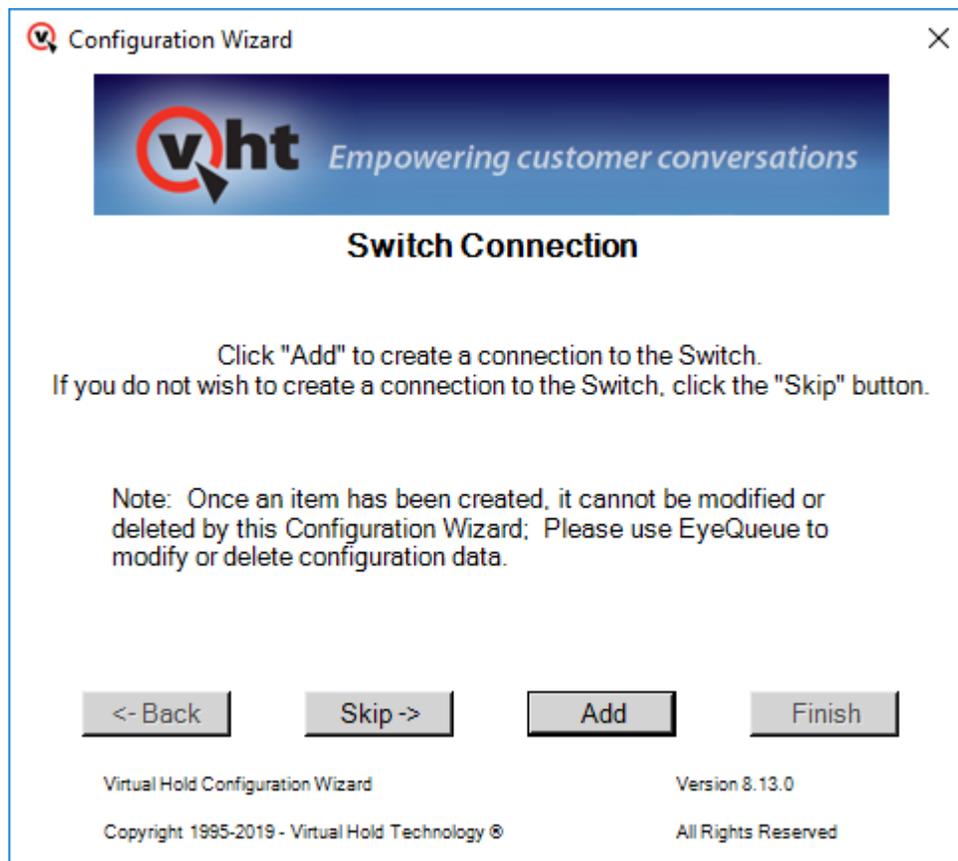
9.1. Launch Configuration Wizard

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.

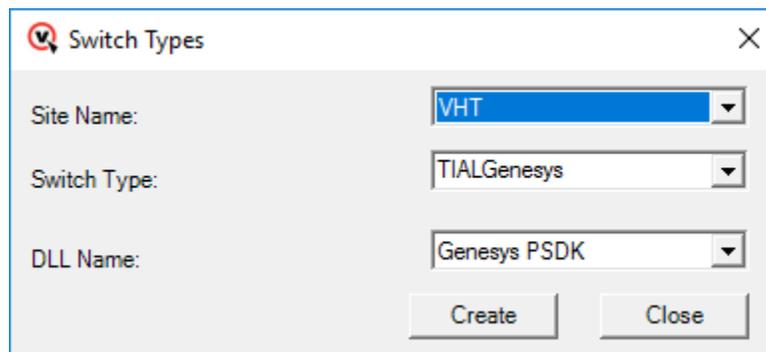


9.2. Administer Switch Connection

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 *TIALGenesys* from the drop-down list. Note that the value of **Site Name** was automatically populated and was created as part of installation. Retain the default values in the remaining fields.



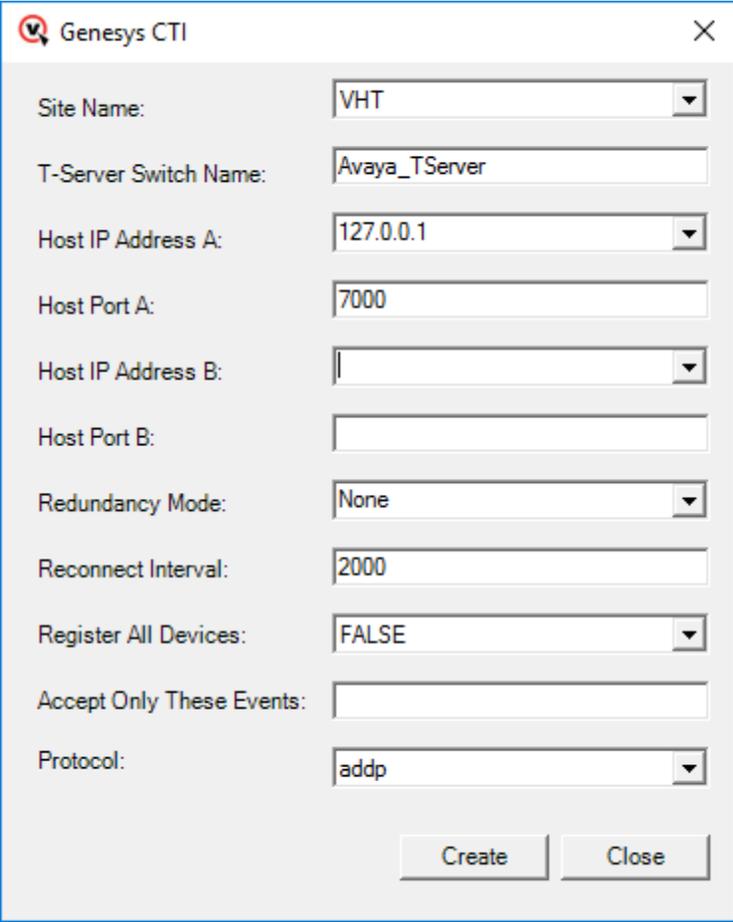
9.3. Configure Genesys CTI T-Server Connections

Continue with the wizard until the **Genesys CTI T-Server Connections** screen is displayed (not shown). Click **Add**.

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

- **T-Server Switch Name:** A descriptive name.
- **Host IP Address A:** The IP address of the Genesys T-Server.
- **Host Port A:** Set to *7000*.
- **Register All Devices:** Set to *FALSE*.
- **Protocol:** Set to *addp*.

Click **Create** followed by **Close**.



The screenshot shows a dialog box titled "Genesys CTI" with a close button (X) in the top right corner. The dialog contains several configuration fields:

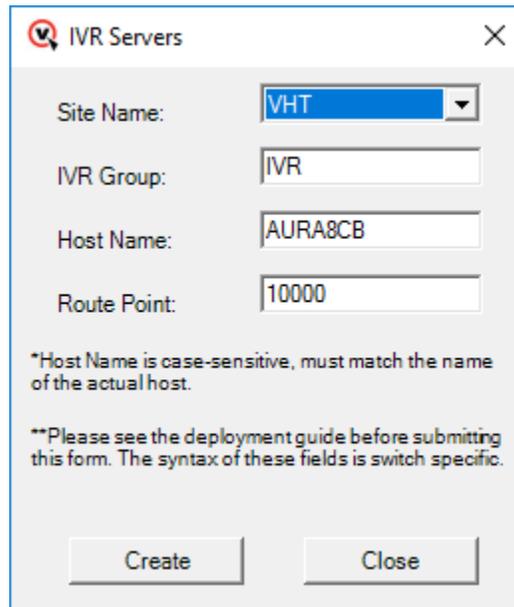
- Site Name:** A dropdown menu with "VHT" selected.
- T-Server Switch Name:** A text input field containing "Avaya_TServer".
- Host IP Address A:** A dropdown menu with "127.0.0.1" selected.
- Host Port A:** A text input field containing "7000".
- Host IP Address B:** A dropdown menu that is currently empty.
- Host Port B:** A text input field that is currently empty.
- Redundancy Mode:** A dropdown menu with "None" selected.
- Reconnect Interval:** A text input field containing "2000".
- Register All Devices:** A dropdown menu with "FALSE" selected.
- Accept Only These Events:** A text input field that is currently empty.
- Protocol:** A dropdown menu with "addp" selected.

At the bottom of the dialog, there are two buttons: "Create" and "Close".

9.4. 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. The **Route Point** is just a place holder at this point. Click **Create** followed by **Close**.



The screenshot shows a dialog box titled "IVR Servers" with a close button (X) in the top right corner. The dialog 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 "AURA8CB".
- Route Point:** A text input field containing "10000".

Below the fields, there is a note: "*Host Name is case-sensitive, must match the name of the actual host." and another note: "**Please see the deployment guide before submitting this form. The syntax of these fields is switch specific." At the bottom of the dialog, there are two buttons: "Create" and "Close".

9.5. Administer Queues

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

The **Queues Setup** screen is displayed next. Consult reference [4] for desired configuration of these parameters. The screenshot below shows the values used in the compliance testing. Click **Create** followed by **Close**.

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

- Site Name: VHT
- Queue ID: VHT_Test_DLG
- Buttons: Use Production Defaults, Use Test Defaults
- QueueSettings section:
 - Op Mode: Normal
 - Turn On Threshold (sec): 0
 - Call Handle Time (secs): 45
 - No Ans Period (sec): 60
 - Name: VHT_Test_DLG
 - 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 section:
 - Day Of Week: Sun, Mon, Tue, Wed, Thu, Fri, Sat (all checked)
 - Time Begin: 00:00
 - Time End: 23:59
- Callbacks Offered section:
 - Day Of Week: Sun, Mon, Tue, Wed, Thu, Fri, Sat (all checked)
 - Time Begin: 00:00
 - Time End: 23:59
- Callbacks Allowed section:
 - Day Of Week: Sun, Mon, Tue, Wed, Thu, Fri, Sat (all checked)
 - Sched callbacks allowed/15 min: 15
- Buttons: Create, Close

9.6. Administer Callback and Holding Queues

Continue with the wizard until the **Callback and Holding Queues** screen is displayed (not shown). Click **Add** to create 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 *tel:77203*, where *77203* is the Callback VDN extension. Click **Create**.

In the **Holding Queues** sub-section, enter the Hold VDN extension from **Section 5.4.2** for **Holding Queue ID**. For **Route Device** and **Transfer Device**, enter *tel:77202*, where *77202* is the Hold VDN extension. Click **Create** followed by **Close**.

Retain the default values for the remaining fields.

Callback and Holding Queues

Site Name: VHT

T-Server Switch Name: Avaya_TServer

Callback Queues

Use T-Server Switch Name prefix

Callback Queue ID*: 77203

Transfer Device: tel:77203

Create

Holding Queues

Use T-Server Switch Name prefix

Holding Queue ID*: 77202

Route Device: tel:77202

Transfer Device: tel:77202

Create

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

* Verify T-Server Switch Name Close

9.7. Administer Incoming Extensions

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

The screen below is displayed next. For **Extension**, enter the Entry VDN extension from **Section 5.4.1**. For **Treatment Type**, select *11*. Retain the default values in the remaining fields. Click **Create** followed by **Close**.

Incoming Extensions

Site Name: VHT

Queue ID: VHT_Test_DLG

T-Server Switch Name: Avaya_TServer

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: Avaya_TServer:77202

Callback Queue ID: Avaya_TServer:77203

UnderThreshold Queue ID: Avaya_TServer:77202

IB IVR Extension Group: NONE

OB IVR Extension Group: NONE

Create

* Verify T-Server Switch Name

Close

Repeat the same procedures to create an incoming extension for Experience Portal inbound application. For **Extension**, enter the extension assigned to inbound application, in this case 78700. For **Treatment Type**, select 20. Retain the default values in the remaining fields, including blank for **VH Server Switch Name**. Click **Create** followed by **Close**.

Incoming Extensions

Site Name: VHT

Queue ID: VHT_Test_DLG

T-Server Switch Name:

Incoming Extensions

Extension*: 78700

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: Avaya_TServer:77202

Callback Queue ID: Avaya_TServer:77203

UnderThreshold Queue ID: Avaya_TServer:77202

IB IVR Extension Group: NONE

OB IVR Extension Group: NONE

Create

* Verify T-Server Switch Name

Close

9.8. Administer Phone Number Configurations

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

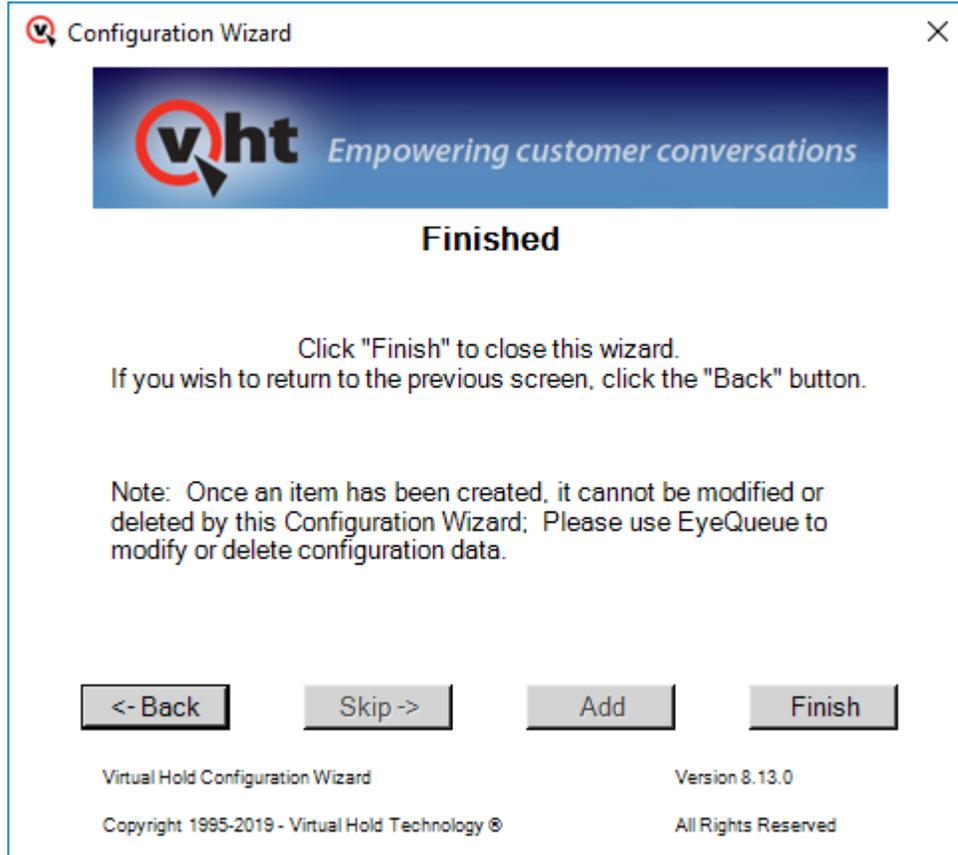
For **Country Search**, locate and select the applicable country as shown below. For the compliance test, the **Min Length** field was set to '5' to allow callbacks to 5-digit extensions corresponding to local IP stations and the **Max Length** field was set to '10' to allow callbacks to 10-digit PSTN numbers. Retain the default values in the remaining fields. Click **Update** followed by **Close**.

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:**
 - Site Name: VHT (dropdown)
 - Country Search: 1 - North America (dropdown with a list below showing "1 - North America" selected)
 - Dial Prefix: (text input)
 - Dial Suffix: (text input)
 - Update button
- Update Phone Number Validation Min/Max Length:**
 - Site Name: VHT (dropdown)
 - Country Id: 1 - North America (dropdown)
 - Min Length: 5 (text input)
 - Max Length: 10 (text input)
 - Update button

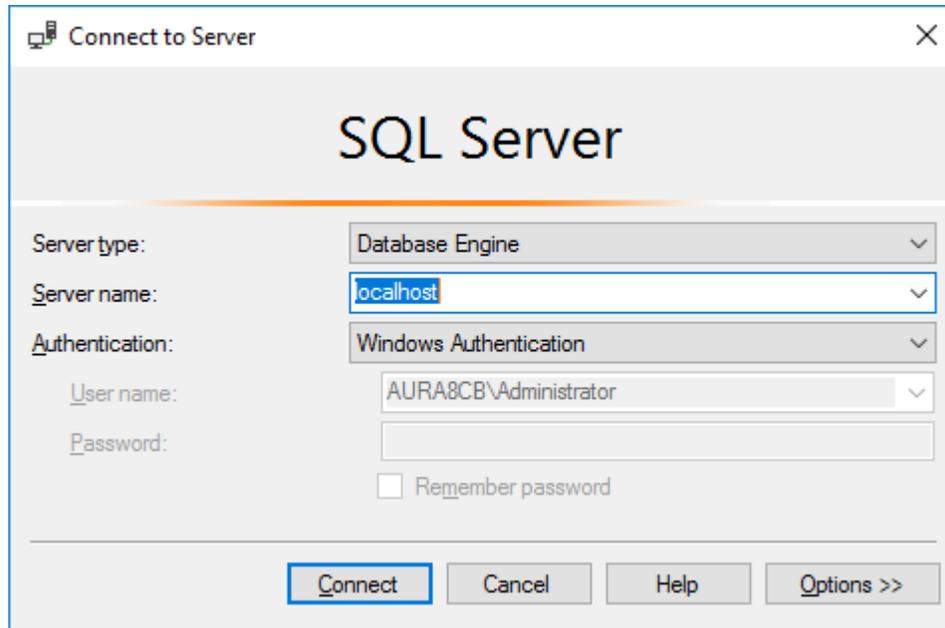
At the bottom right of the dialog is a "Close" button.

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



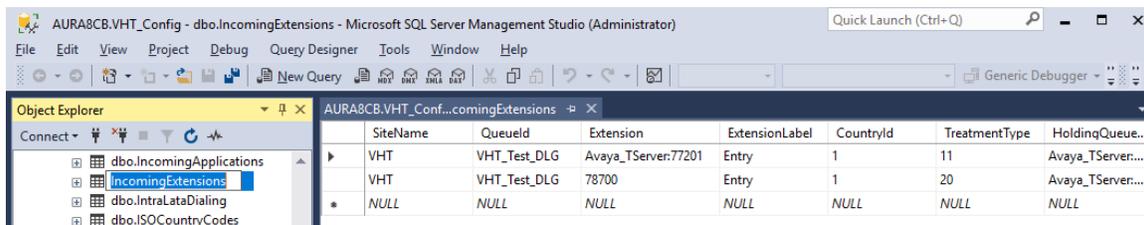
9.9. Administer Segment Variables

From the Callback server, navigate to **Start → Apps → Microsoft SQL Server 2016 → SQL Server Management Studio** to launch and connect to the SQL server.

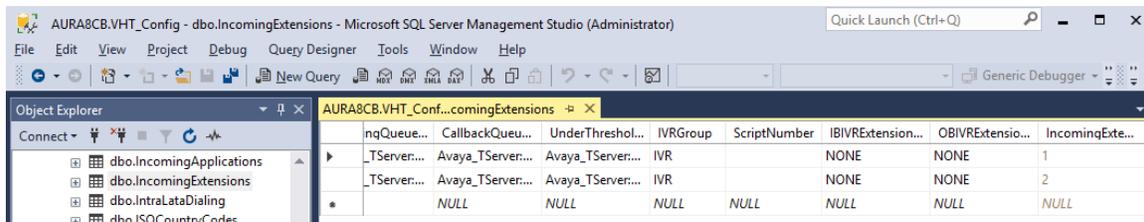


Navigate to **Databases → VHT_Config → Tables → dbo.IncomingExtensions** in the left pane, right-click the entry and select **Edit Top 200 Rows**.

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



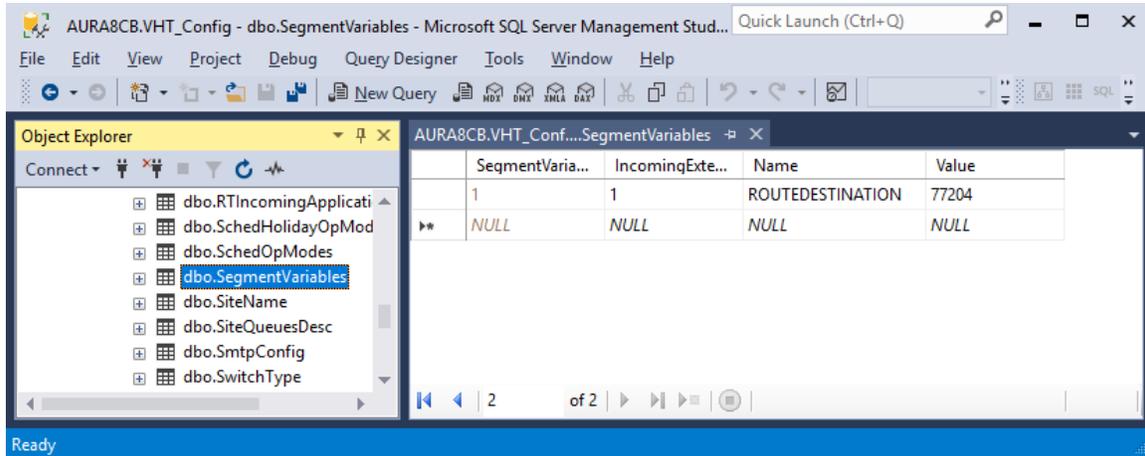
Scroll to the right to make a note of the associated **IncomingExtensionsId** value, in this case ‘1’, as shown below.



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

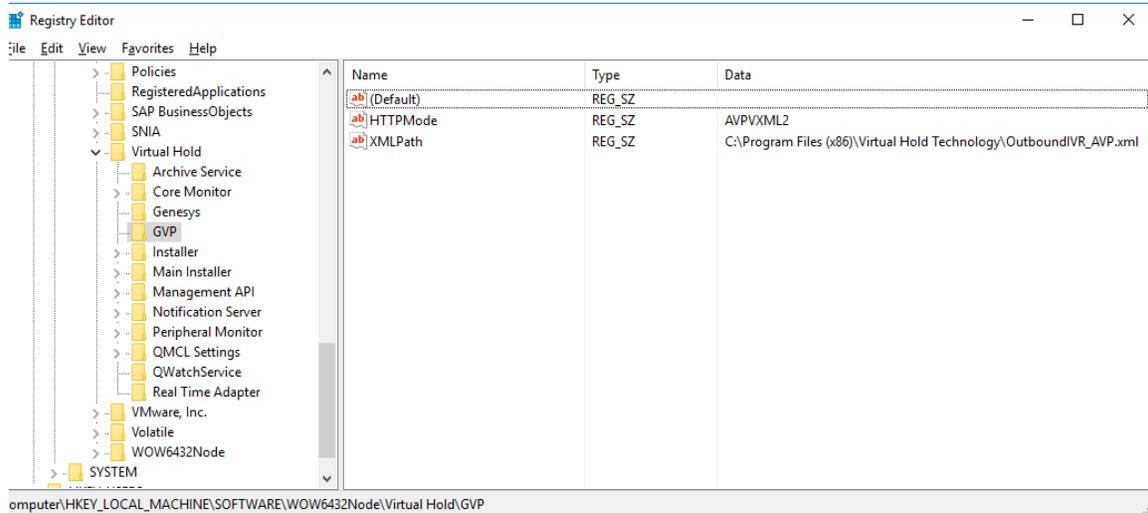
- **IncomingExtensionsId:** The value from the **dbo.IncomingExtensions** table from above.
- **Name:** Set to *ROUTEDESTINATION*.
- **Value:** Set to the route VDN extension *77204*.

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



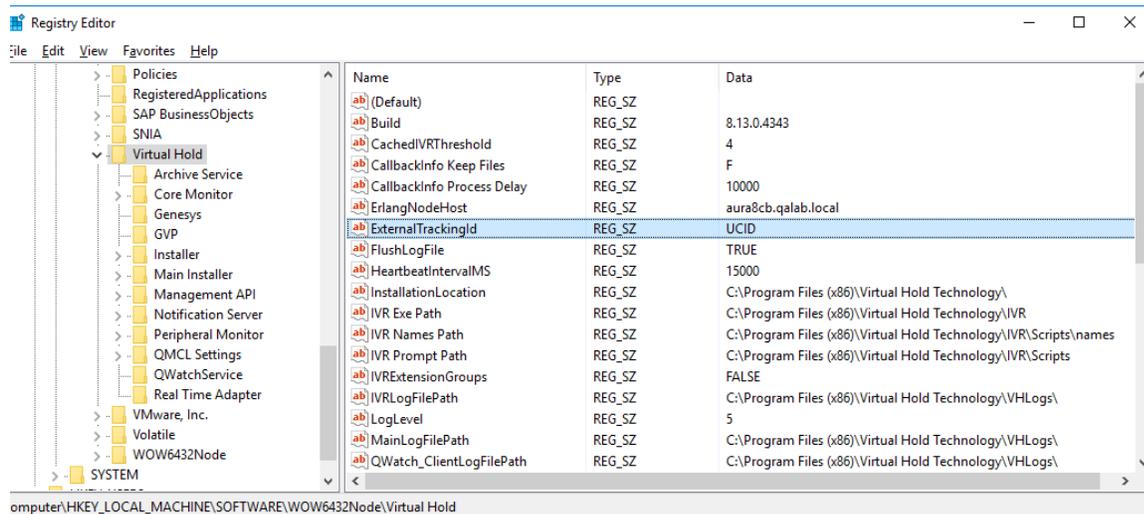
9.10. Configure Callback Outbound Application

Navigate to HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Virtual Hold in the Windows Registry and verify that the **XMLPath** parameter is set to the full path of the OutboundIVR_AVP.xml file 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).



Navigate to **C:\Program Files (x86)\Virtual Hold Technology** folder and open **OutboundIVR_AVP.xml**.

- Replace the IP address in the **URI** field with the IP address of Experience Portal Manager.
- Set **ApplicationName** to the name of the outbound application configured in **Section 8.4.2**.
- Set **AppInterfaceUsername** and **AppInterfacePassword** to the **Username** and **Password** configured for an Experience Portal user configured in **Section 8.3**.

```
<?xml version="1.0" encoding="utf-8"?>
<LoadBalancerManager>
  <DefaultID>NONE</DefaultID>
  <NumberOfConnectionSets>1</NumberOfConnectionSets>
  <ConnectionSet1>
    <Count>1</Count>
    <Identifier>VHT_Test_DLG</Identifier>
    <FirstConnection>Connection1</FirstConnection>
    <LastConnection>Connection1</LastConnection>
    <Connection1>
      <!-- <URI>http://AVPSERVER:8080/axis/services/AppIntfWS</URI> -->
      <URI>https://devcon-epm.avaya.com/axis2/services/VPAppIntfService</URI>
      <OutboundANI>8005555555</OutboundANI>
      <!-- AVP provisioned Virtual Hold outbound application -->
      <ApplicationName>VHT-Outbound</ApplicationName>
      <CcxmlApplicationName></CcxmlApplicationName>
      <AppInterfaceUsername>webservice</AppInterfaceUsername>
      <AppInterfacePassword>xxxxxxxx</AppInterfacePassword>
      <ConnectTimeout>30</ConnectTimeout>
      <MaxConcurrentOutboundDialRequests>2</MaxConcurrentOutboundDialRequests>
    </Connection1>
  </ConnectionSet1>
  <WebServiceClientTimeoutInMilliseconds>180000</WebServiceClientTimeoutInMilliseconds>
  <SessionParameters>enable_call_classification=false;detect_greeting_end=true</SessionParameters>
  <URLParameters></URLParameters>
  <TimeToExcludeOnFailure>150000</TimeToExcludeOnFailure>
  <NextConnectionOnSuccess>Connection1</NextConnectionOnSuccess>
  <NextConnectionOnFailure>Connection1</NextConnectionOnFailure>
  <NextConnectionOnNoResourcesAvailable>Connection1</NextConnectionOnNoResourcesAvailable>
</LoadBalancerManager>
```

Navigate to the **C:\VirtualHold** folder and open toolkit.properties using notepad.

- Replace the IP address in the **baseurl**, **mediaserver**, and **webaudiopath** parameters with the IP address of the VHT Callback server.
- Set the **useDnisAsSegment** parameter to **true**.
- Set the **useexternalrouting** parameter to **false**.

```
# Sample configuration file for SIP Avaya Voice Portal integrations

# URL for the Platform Toolkit web services
# Change the [PTK_server_address] and [PTK_port] to the address and port of the server
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://10.64.102.109/VHTPlatformWS-v5/

# Setting to true causes details of Platform Toolkit requests and responses to be
included in the web server logs
com.virtualhold.toolkit.debug=true

# Set this to true to queue and dequeue the call before control is passed off in the
'submit' on the outbound
com.virtualhold.toolkit.outbound.cleanupcallbeforesubdialog=true

# Set this to true if you want to use the call's DNIS as the incoming Platform Toolkit
segment
com.virtualhold.toolkit.useDnisAsSegment=true

# Total number of media servers where voice files will be played from
external.mediaserver.count=1

# Media server url configuration
# This url is resolved by the voice browser so localhost will not work
# For additional entries, just increase the number on the end of the property name
# For example, external.mediaserver.2
external.mediaserver.1=http://10.64.102.109:8080/voices/

# Distribution method options
# failover - Goes top to bottom attempting to fetch the media file and will play from
the location where it first finds the media file
# balanced - Load balances the media file fetching from the media servers, will
failover if needed
external.mediaserver.distribution=failover

# Media server failure logging options
# none - will not log any media server failures
# first - will log the first time that a media server error occurs
# all - will log a media server error every time it occurs
external.mediaserver.logging=first

# Local path to the ASAP and Scheduled callback name files for recording
# Change the [web_server_install_directory] to the local path of the web server
# For example, C:/Program Files/Apache Software Foundation/Tomcat
6.0_Tomcat/webapps/ROOT
com.virtualhold.toolkit.audiopath=C:/Program Files/Apache Software Foundation/Tomcat
7.0/webapps/ROOT/namefiles

# Web path to the ASAP and Scheduled callback name files for playback
# Change the [web_server_address] and [web_server_port] to the URL and port of the web
```

```

server
# For example, http://10.10.0.245:8080/
com.virtualhold.toolkit.webaudiopath=http://10.64.102.109:8080/namefiles

# Used in day/time selection
# The ) and ] characters have unique properties when used to define the end of time
group ranges
# For example, (12:00 am|6:00 am) includes times starting at 12:00 am through and
including 6:00 am)
# For example, (12:00 am|6:00 am] includes times starting at 12:00 am through and
including 5:59 am]
com.virtualhold.toolkit.earlymorning=(12:00 am|6:00 am]
com.virtualhold.toolkit.morning=(6:00 am|12:00 pm]
com.virtualhold.toolkit.afternoon=(12:00 pm|5:00 pm]
com.virtualhold.toolkit.evening=(5:00 pm|9:00 pm]
com.virtualhold.toolkit.night=(9:00 pm|11:59 pm]

# Default transfer destination during an inbound call, if destination cannot be
retrieved from the Platform Toolkit
# Change the [default_transfer_destination] to the VDN inbound calls should be
transferred to if calls default transfer from VIS to queue
# Enter the Avaya code followed by the VDN, for example, tel:5000 or tel:45623
com.virtualhold.toolkit.defaultdestination=tel:77202

# Default transfer destination during an outbound call, if destination cannot be
retrieved from the Platform Toolkit
# Change the [default_transfer_destination] to the VDN outbound calls should be
transferred to if default transferred from VIS to queue
# Enter the Avaya tel code followed by the VDN, for example, tel:5000 or tel:45623
com.virtualhold.toolkit.outbound.defaultdestination=tel:46263

# Inbound call routing control
# Determines whether VIS will control call routing or pass control back to the Avaya
CM
# This property can be overridden with the URL query string parameter
UseExternalRouting
com.virtualhold.toolkit.inbound.useexternalrouting=false

# Outbound call routing control
# Determines whether VIS will control call routing or pass control back to the Avaya
CM
# This property can be overridden with the URL query string parameter
UseExternalRouting
com.virtualhold.toolkit.outbound.useexternalrouting=false

# Used in UUI-based routing
# Tells what format Queue Manager uses when storing UUI data for re-attaching to a
callback.
# Values: false - hexadecimal format, true - ASCII format
# Usage:
#     Inbound leg uses SIP - false
#     Inbound leg is H.323 and Avaya encodes UUI as ASCII - true
com.virtualhold.toolkit.avp.uuistoredinascii=false

com.virtualhold.toolkit.transferprefix=tel:

```

9.11. Configure TSAPI Real-Time Adapter

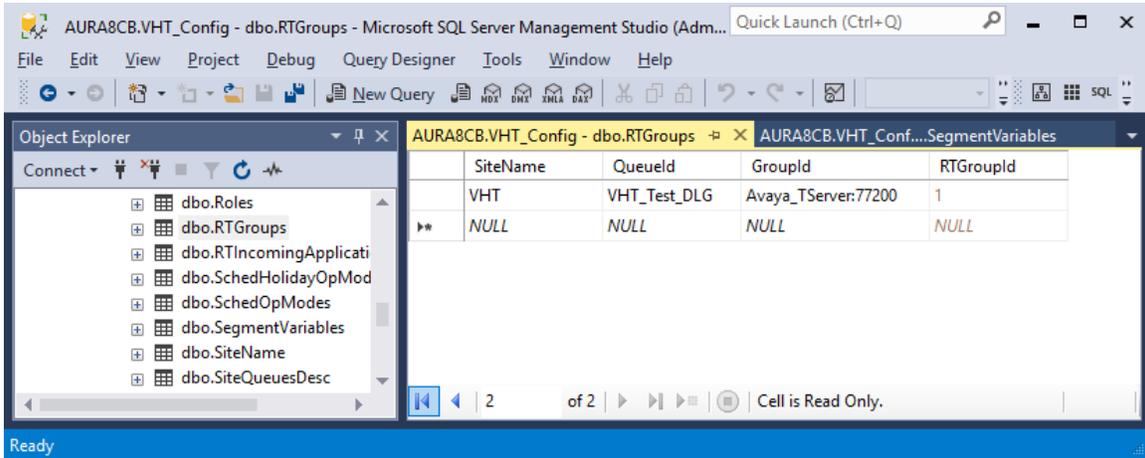
The Callback TSAPI Real-Time Adapter captures queue statistics, such as agent status of a monitored skill/split and can be displayed as shown in **Section 11.3**.

Open the `VHT_GenesysRealTimeAdapter_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 (10.64.102.109) 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"/>
      <section name="statServer"
type="RealTimeAdapters.Configuration.Sections.StatServerSection, RealTimeAdapters"
allowLocation="true" allowDefinition="Everywhere"/>
    </sectionGroup>
  </configSections>
  <VHTConfiguration>
    <vhtLogging>
      <application level="10" name="GenesysRealTimeAdapter"
logFilePath="C:\Program Files (x86)\Virtual Hold Technology\VHLogs"/>
    </vhtLogging>
    <vhtCommunication>
      <QMCL reconnectIntervalSeconds="3">
        <Connections>
          <Connection connectionType="Primary">
            <Server ipAddress="10.64.102.109" port="6999"/>
            <Client ipAddress="10.64.102.109" port="0"/>
          </Connection>
        </Connections>
      </QMCL>
    </vhtCommunication>
    <statServer tenant="Environment" password="" clientName="VHTGenRTAdapter"
intervalFrequencySecs="15"> <!-- ipVersion -->
      <servers>
        <add name="primary" host="10.64.102.109" port="7001"/>
      </servers>
      <!-- <callsInAcd statType="" /> -->
      <agentsAvailable statType="VHT_CurrNumberWaitStatuses"
category="CurrentNumber" subject="AgentStatus" mainMask="WaitForNextCall"/>
      <agentsStaffed statType="VHT_CurrAgentsLoggedIn" category="CurrentNumber"
subject="AgentStatus" mainMask="*, ~NotMonitored, ~LoggedOut"/>
    </statServer>
  </VHTConfiguration>
</configuration>
```

```
</VHTConfiguration>
<appSettings>
  <add key="VhqmwsUrl" value="http://10.64.102.109/VHQMWS/VHQMWS.asmx"/>
  <add key="SiteName" value="VHT"/>
  <add key="UseTialAdapter" value="TRUE"/>
  <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 VHT server ID and hunt group extension (e.g., *VHT_TServer:77200*) as shown below.



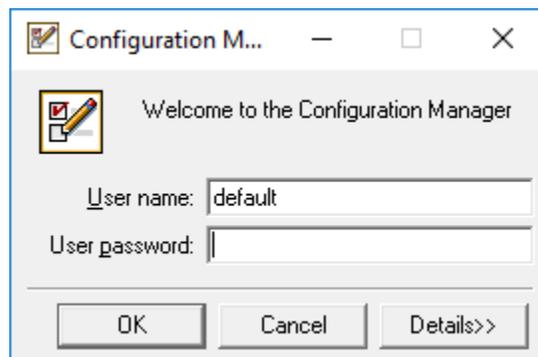
10. Configure Genesys T-Server

This section covers the configuration of Genesys T-Server and covers the following areas:

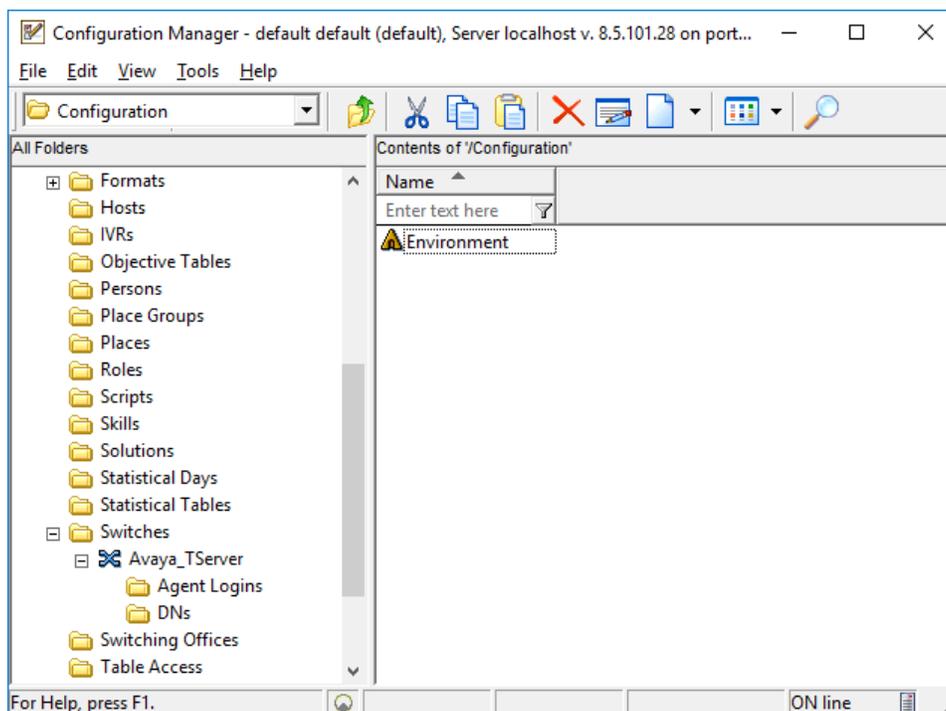
- Launch Configuration Manager
- Administer DNs
- Administer TSAPI Connection
- Install Experience Portal Certificate

10.1. Launch Configuration Manager

On the VHT Callback server, open **Genesys Configuration Manager** and log in with the appropriate credentials.

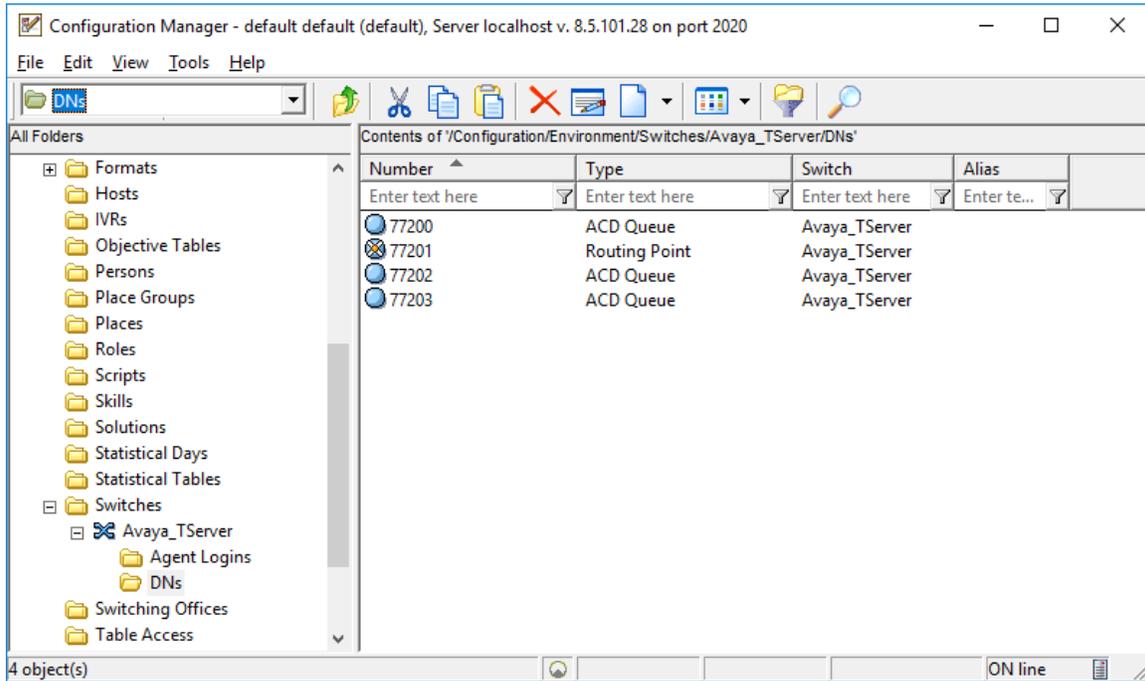


The Configuration Manager window is displayed as shown below.



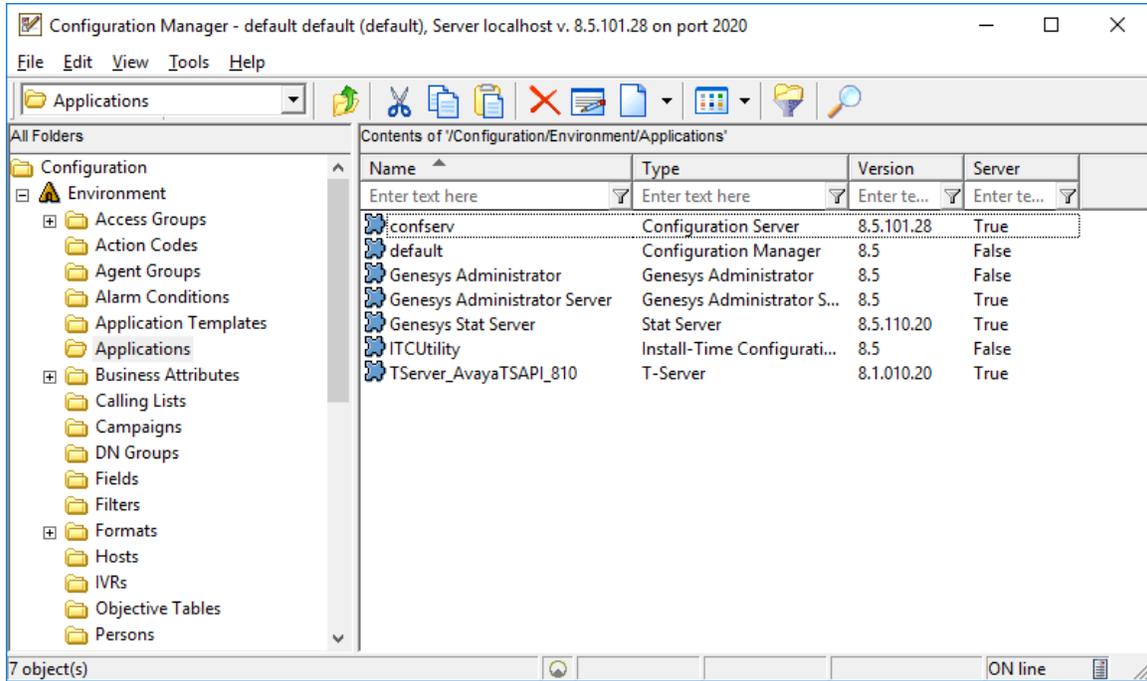
10.2. Administer DNs

From the left pane, navigate to **Configuration** → **Environment** → **Switches** → **Avaya_TServer** → **DNs**. Right-click on the window and select **New** → **DN** to create a DN for the Hunt Group extension, Entry VDN, Hold VDN, and Callback VDN. Note that Hunt Group 77 was a pre-defined hunt group mentioned in **Section 3**, and its extension is 77200. The screen below shows the four DNs after they've been added.



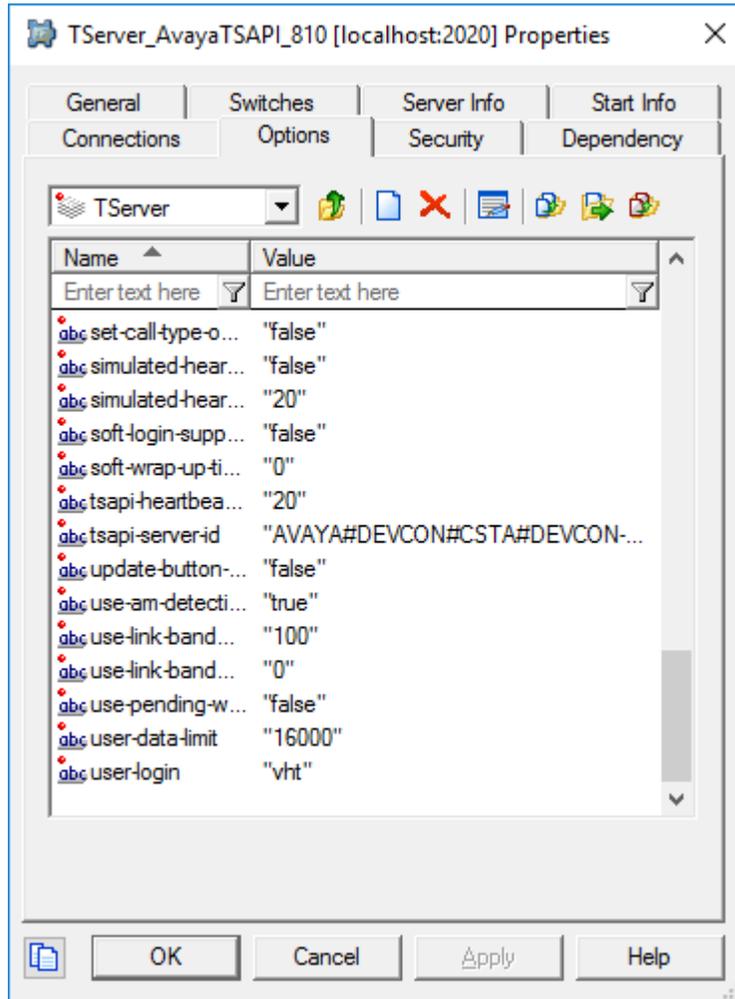
10.3. Administer TSAPI Connection

From the left pane, navigate to **Configuration** → **Environment** → **Applications**. Double-click **TServer_AvayaTSAPI_810** in the right pane.

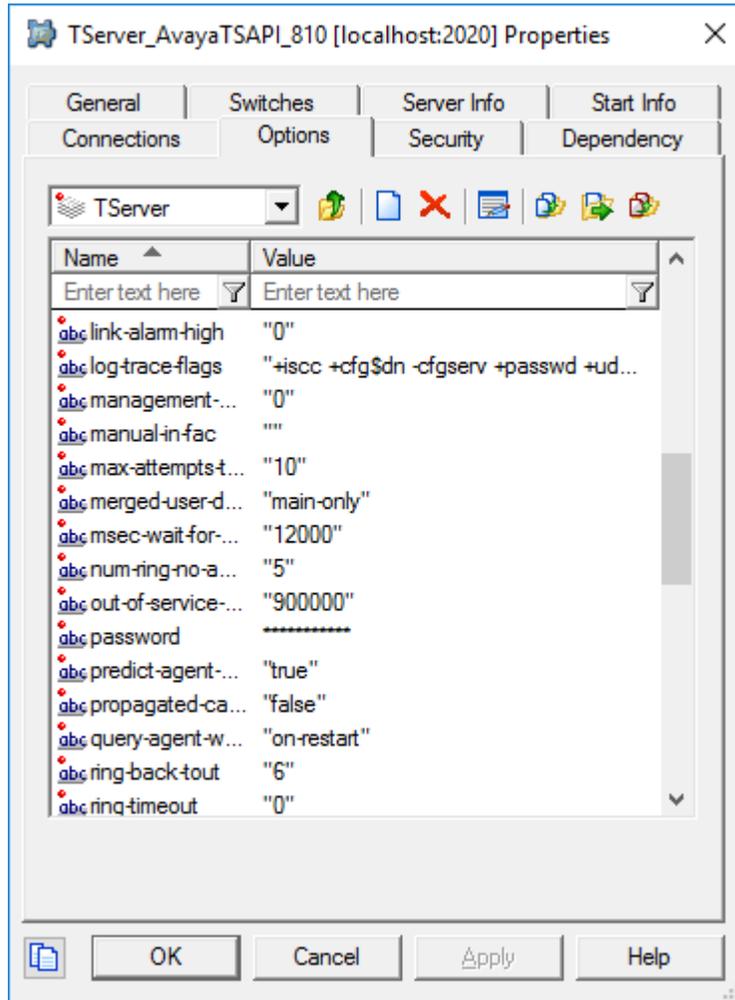


The **TServer_AvayaTSAPI_810 Properties** window is displayed. Select the **Options** tab and double-click the **TServer** line (not shown).

The **TServer** section is displayed below. Set the **user-login** and **password** fields to the **User Id** and **User Password** values configured in **Section 7.6**. Set the **tsapi-server-id** field to the link noted in **Section 7.5**. The **user-login** and **tsapi-server_id** is set in the screen below.

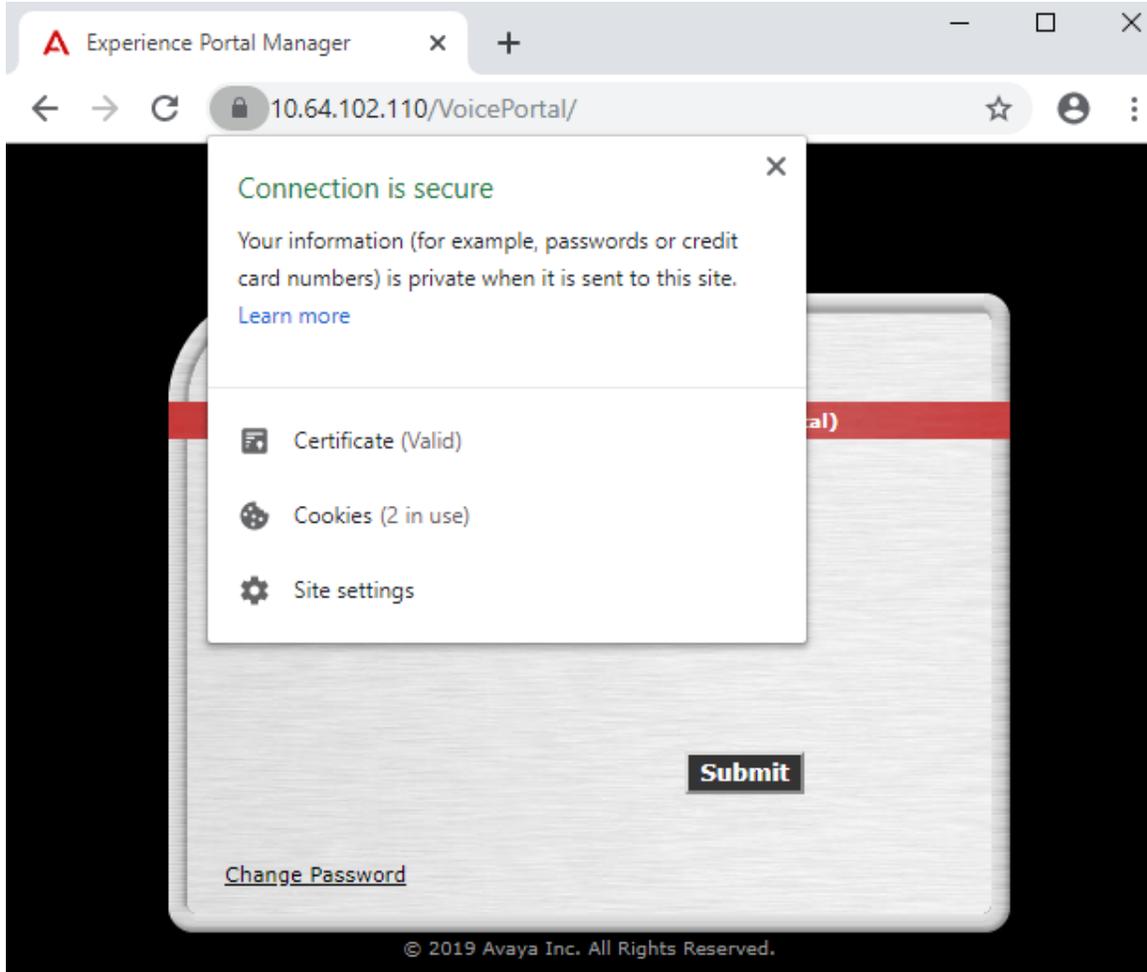


Scroll to the **password** field and set its value as shown below.

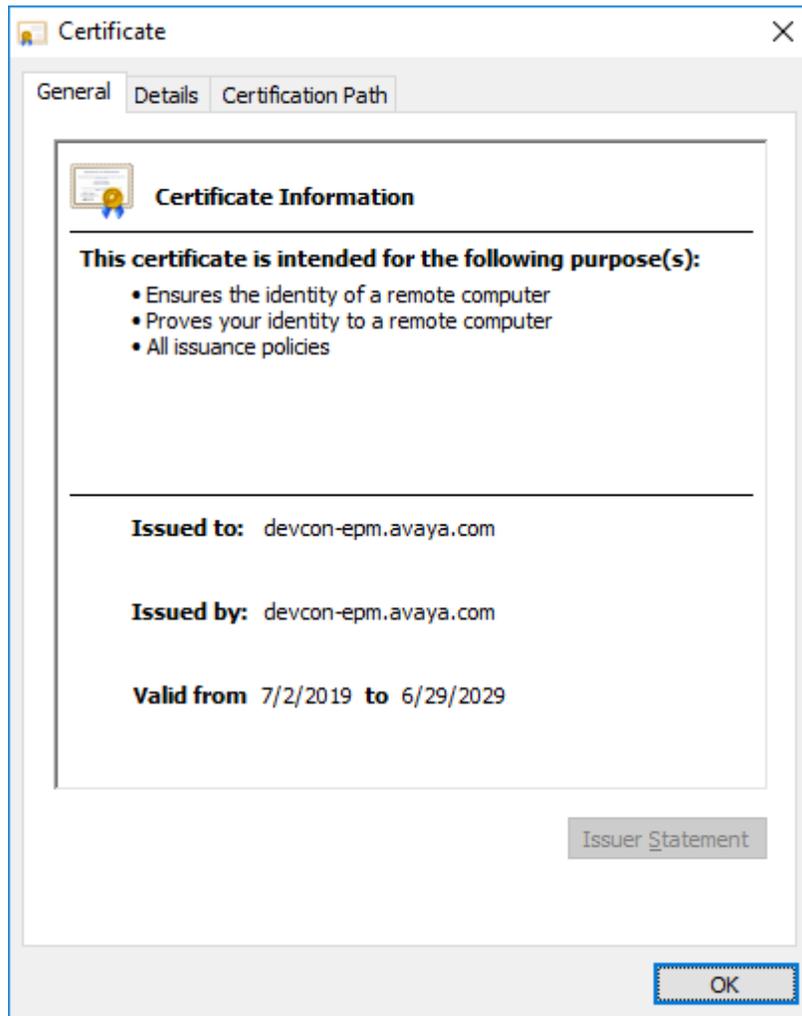


10.4. Install Experience Portal Certificate

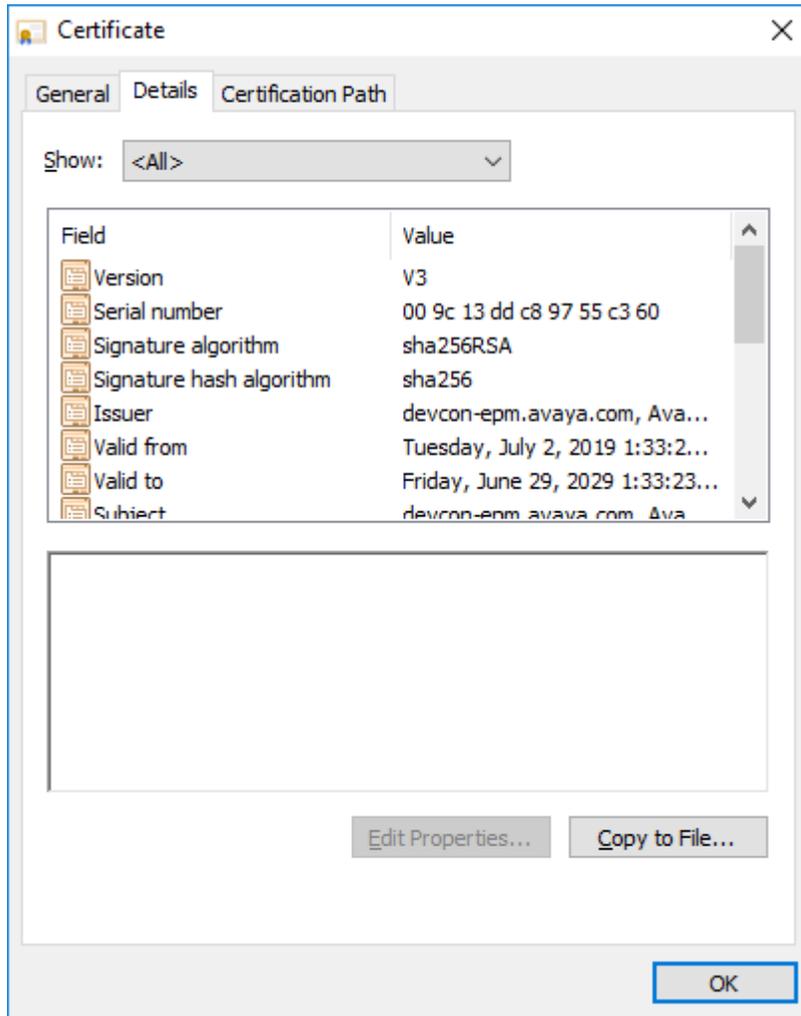
Install the Experience Portal certificate on VHT Callback server. Via a browser, go to <https://<AEP-IP-Address>>. The screen below is from using Chrome. Click on **Certificate** to view the certificate.



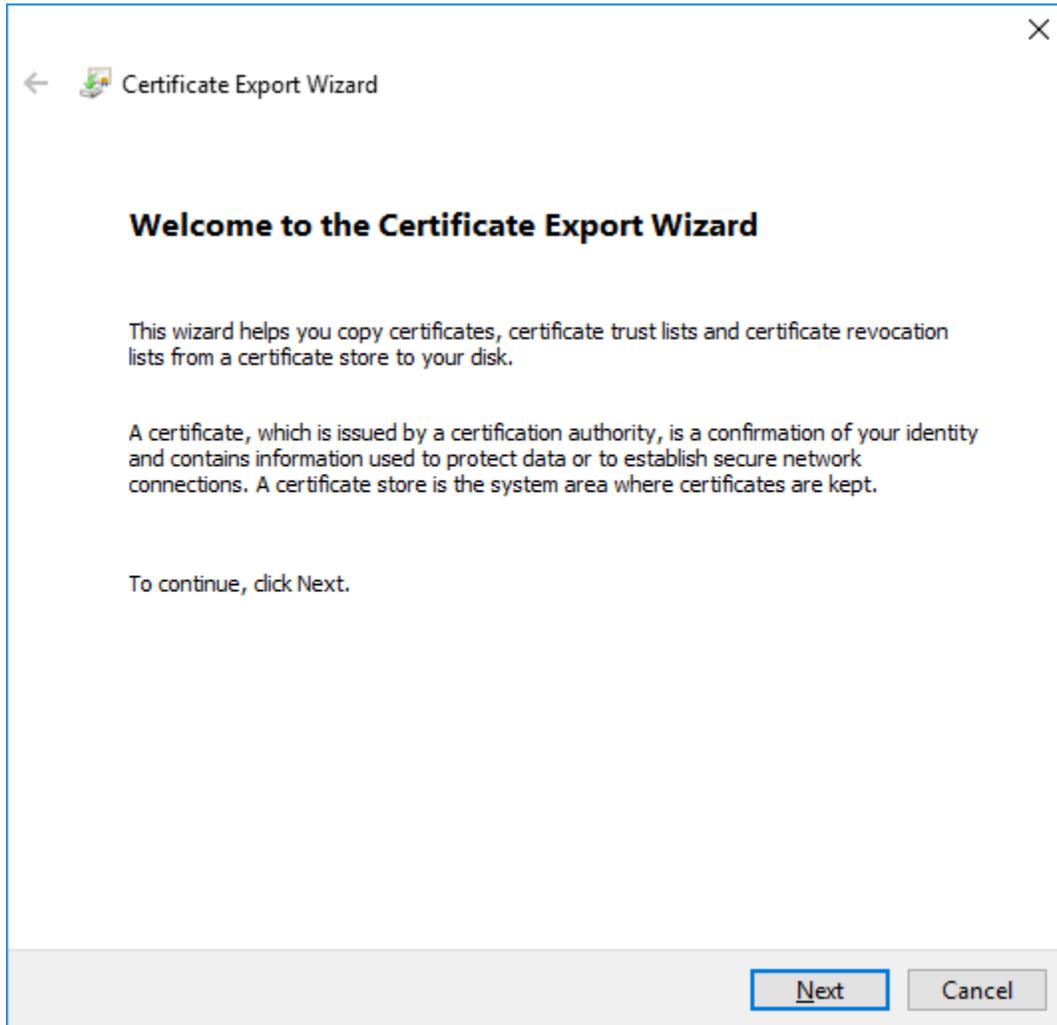
The **Certificate** window is displayed as shown below.



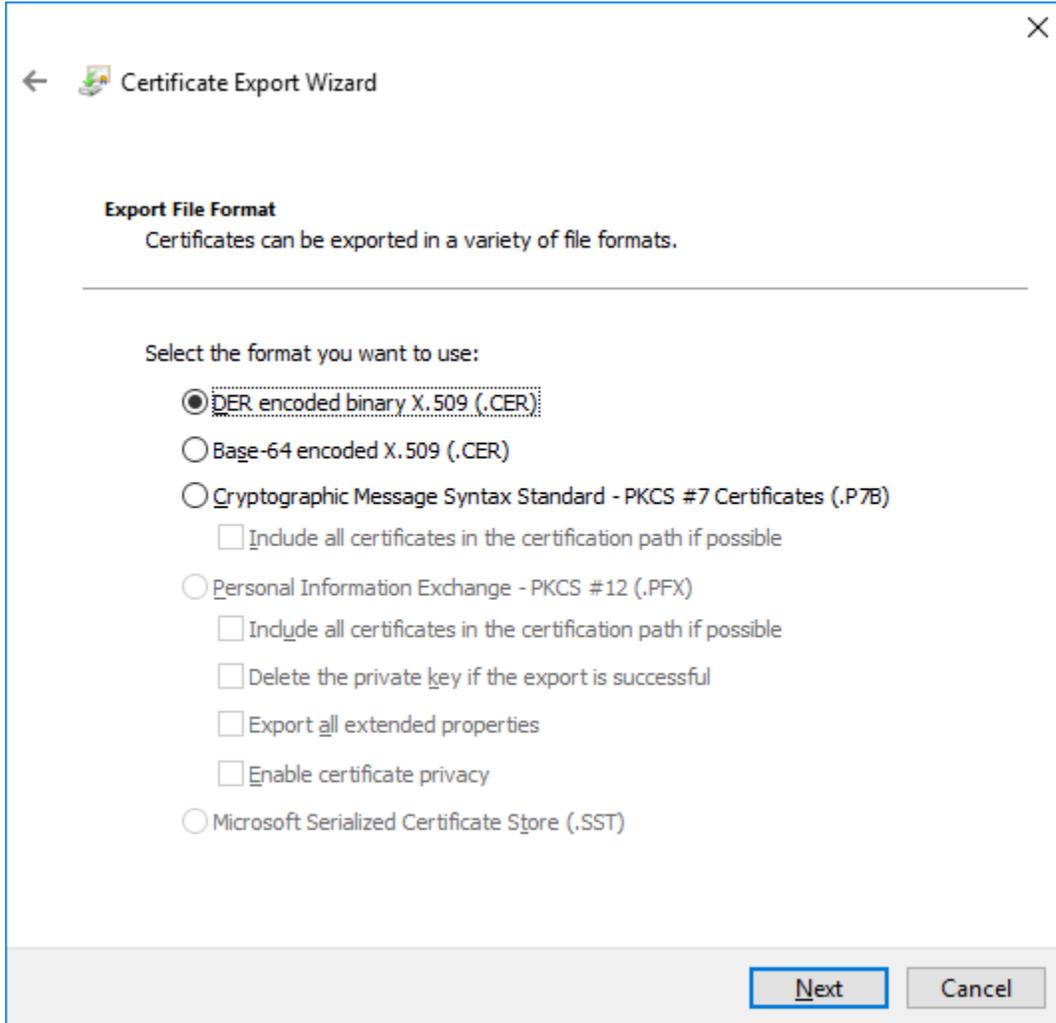
Select the **Details** tab and then click the **Copy to File...** button. The **Certificate Export Wizard** is displayed.



In the **Certificate Export Wizard**, click **Next**.



Accept the default setting and click **Next**.



The image shows a Windows dialog box titled "Certificate Export Wizard". It has a back arrow icon on the left and a close 'X' icon on the right. The main content area is titled "Export File Format" and contains the text "Certificates can be exported in a variety of file formats." Below this is a horizontal line and the instruction "Select the format you want to use:". There are five radio button options: "DER encoded binary X.509 (.CER)" (selected), "Base-64 encoded X.509 (.CER)", "Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)", "Personal Information Exchange - PKCS #12 (.PFX)", and "Microsoft Serialized Certificate Store (.SST)". Under the "Cryptographic Message Syntax Standard" and "Personal Information Exchange" options, there are several checkboxes: "Include all certificates in the certification path if possible", "Delete the private key if the export is successful", "Export all extended properties", and "Enable certificate privacy". At the bottom right, there are two buttons: "Next" (highlighted with a blue border) and "Cancel".

← Certificate Export Wizard

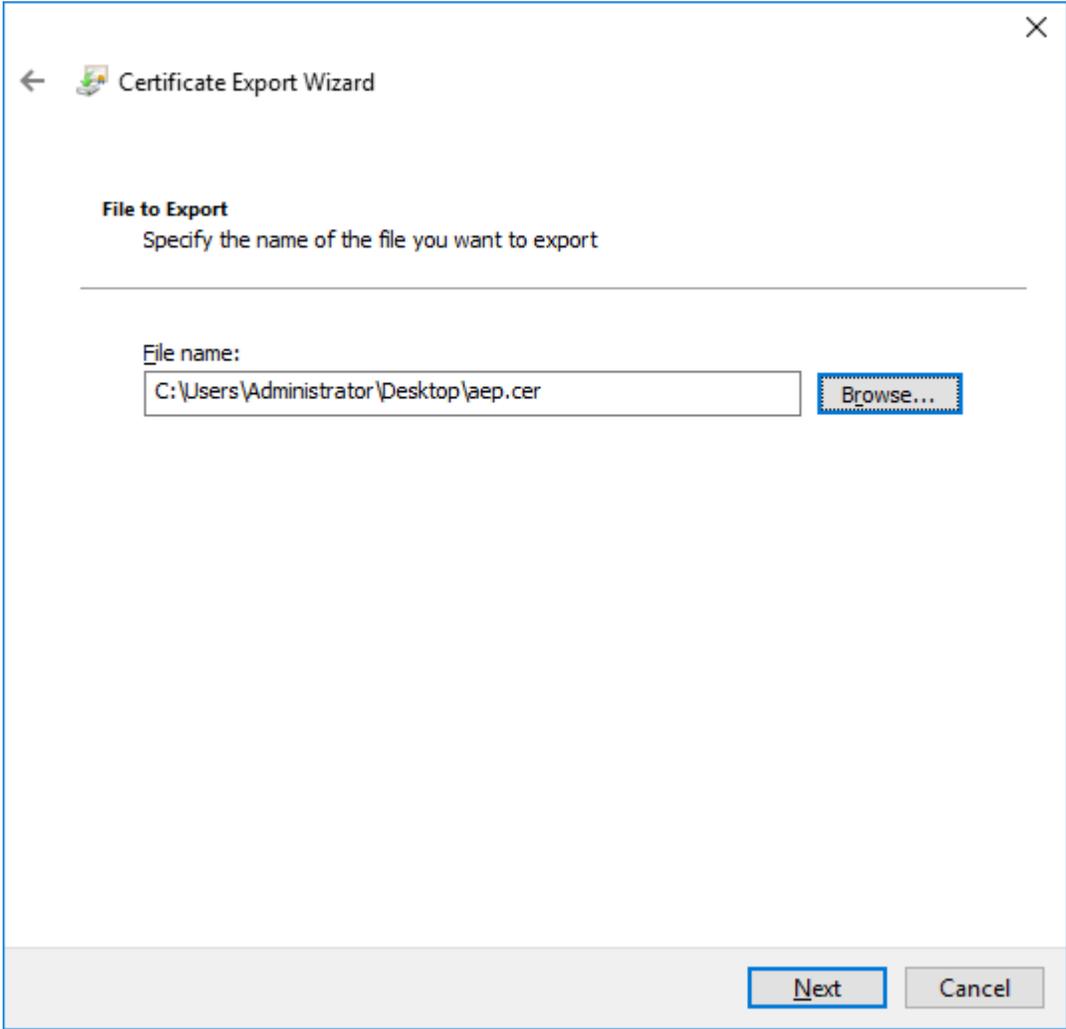
Export File Format
Certificates can be exported in a variety of file formats.

Select the format you want to use:

- DER encoded binary X.509 (.CER)
- Base-64 encoded X.509 (.CER)
- Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)
 - Include all certificates in the certification path if possible
- Personal Information Exchange - PKCS #12 (.PFX)
 - Include all certificates in the certification path if possible
 - Delete the private key if the export is successful
 - Export all extended properties
 - Enable certificate privacy
- Microsoft Serialized Certificate Store (.SST)

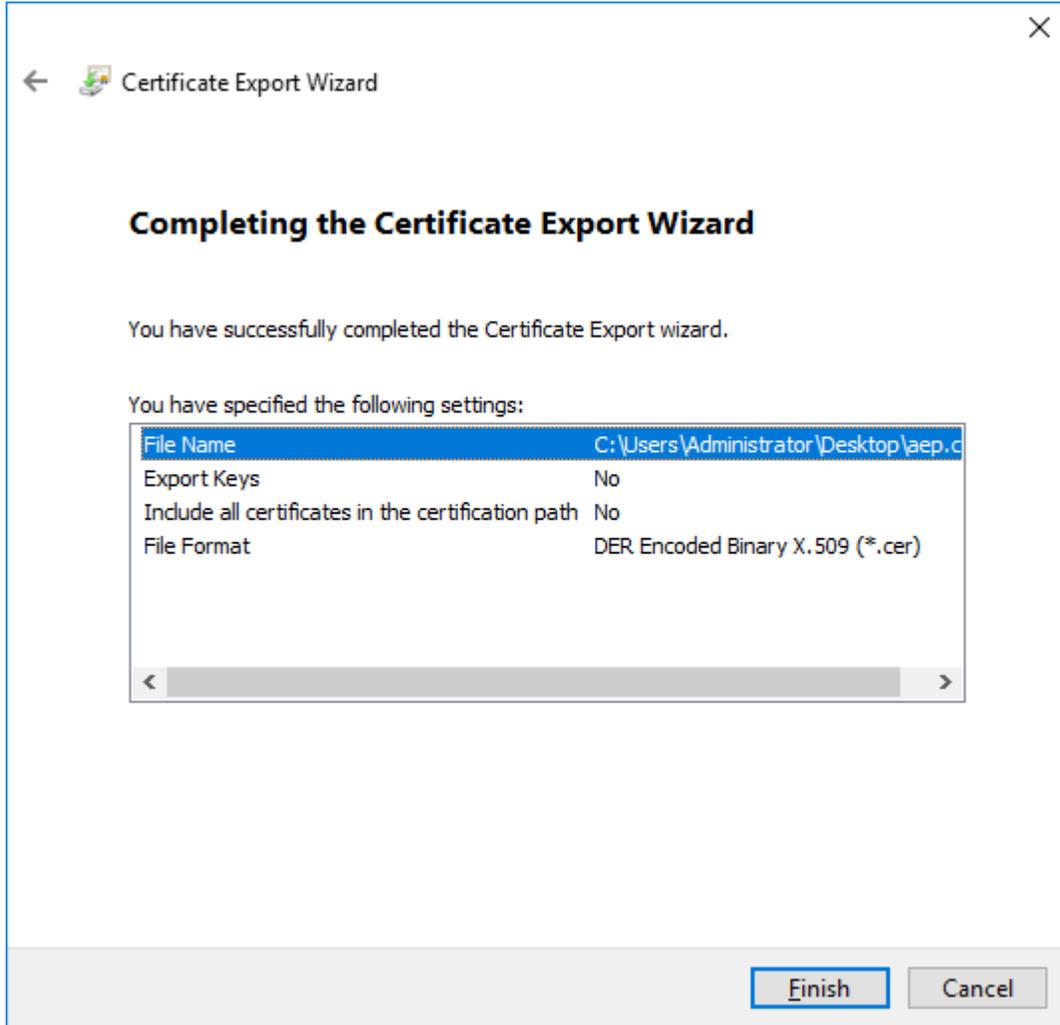
Next Cancel

For the **File Name**, specify the full path of the certificate file name with a `.cer` suffix as shown below. Click **Next**.

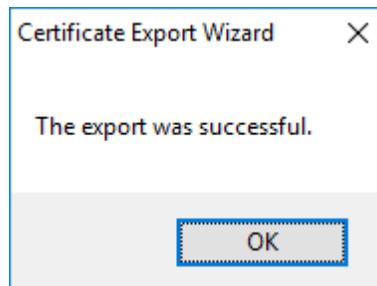


The image shows a Windows dialog box titled "Certificate Export Wizard". The window has a standard title bar with a close button (X) in the top right corner. Below the title bar, there is a back arrow icon and the text "Certificate Export Wizard". The main content area is titled "File to Export" and contains the instruction "Specify the name of the file you want to export". Below this instruction is a horizontal line. Underneath the line, the text "File name:" is followed by a text input field containing the path "C:\Users\Administrator\Desktop\jep.cer". To the right of the input field is a "Browse..." button. At the bottom right of the dialog box, there are two buttons: "Next" and "Cancel".

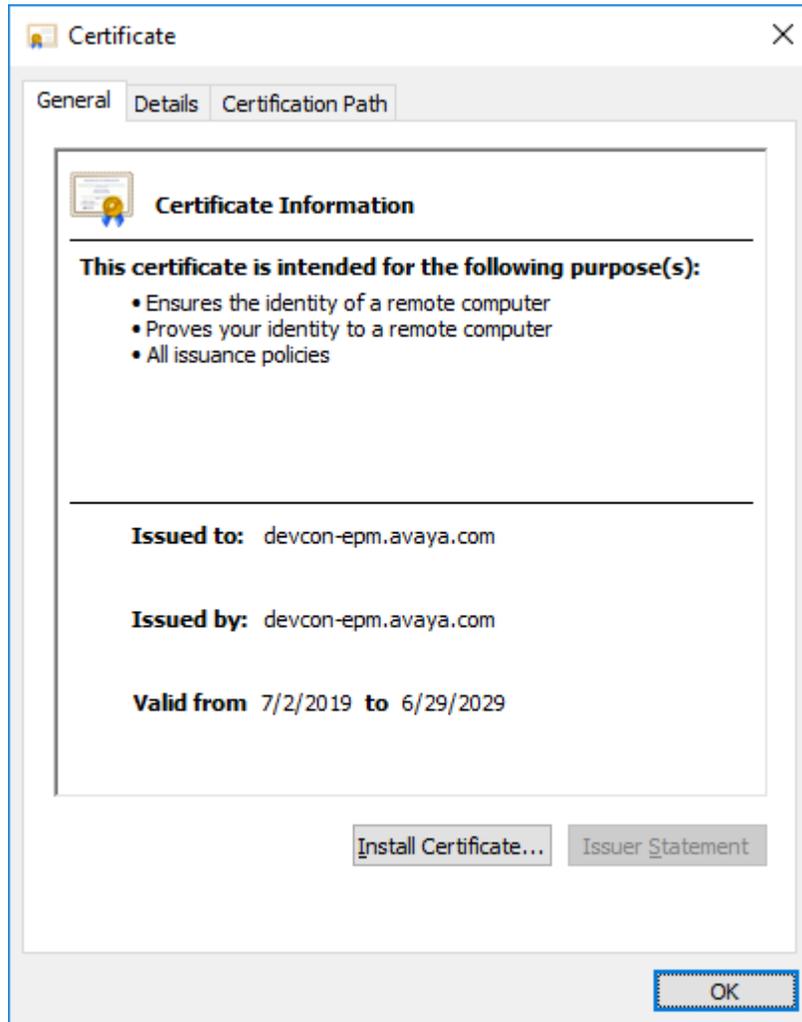
Click **Finish**.



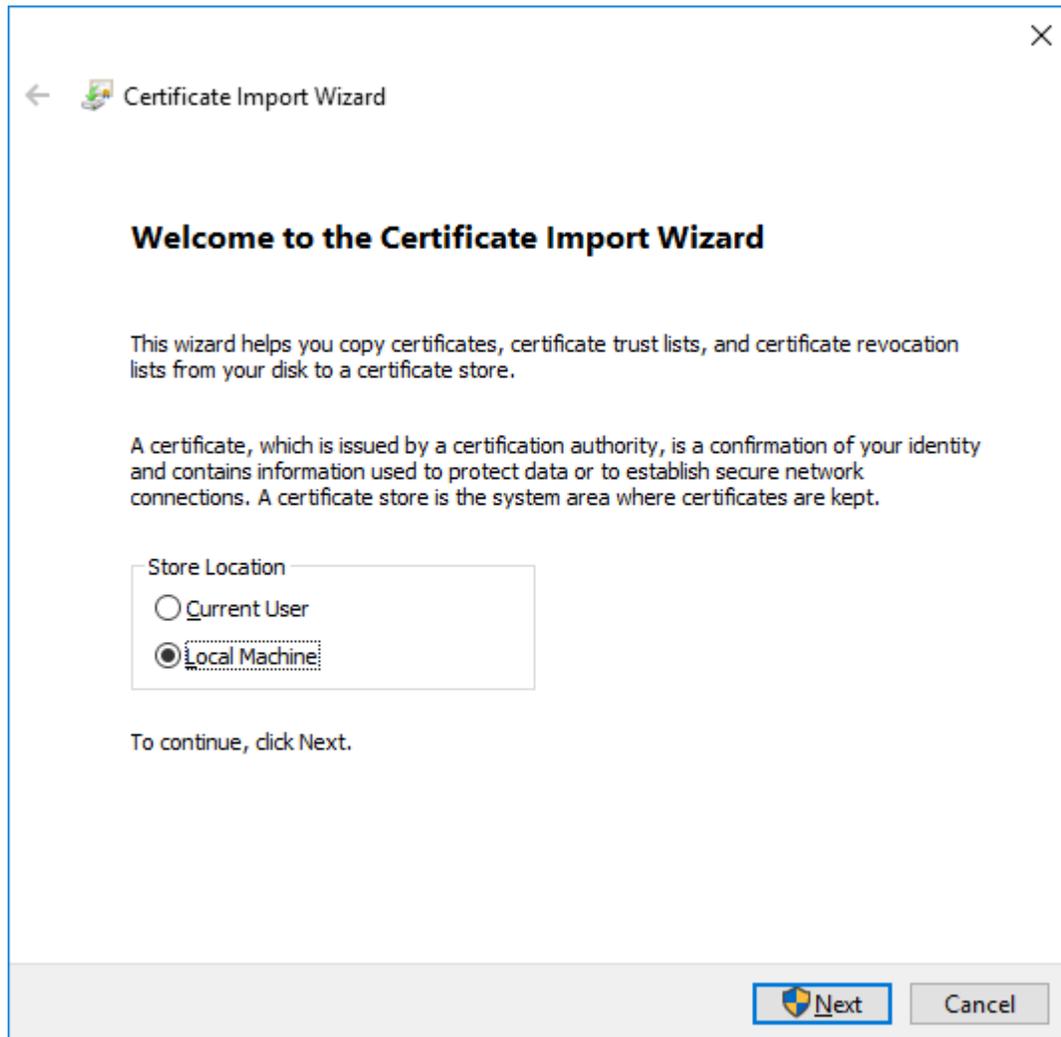
The Experience Portal certificate is saved to the specified location. Click **OK**.



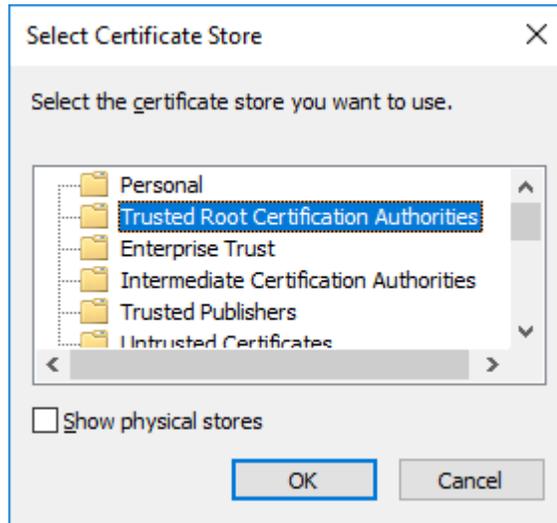
Navigate to the folder where the certificate was saved. Open the certificate and select **Install Certificate**.



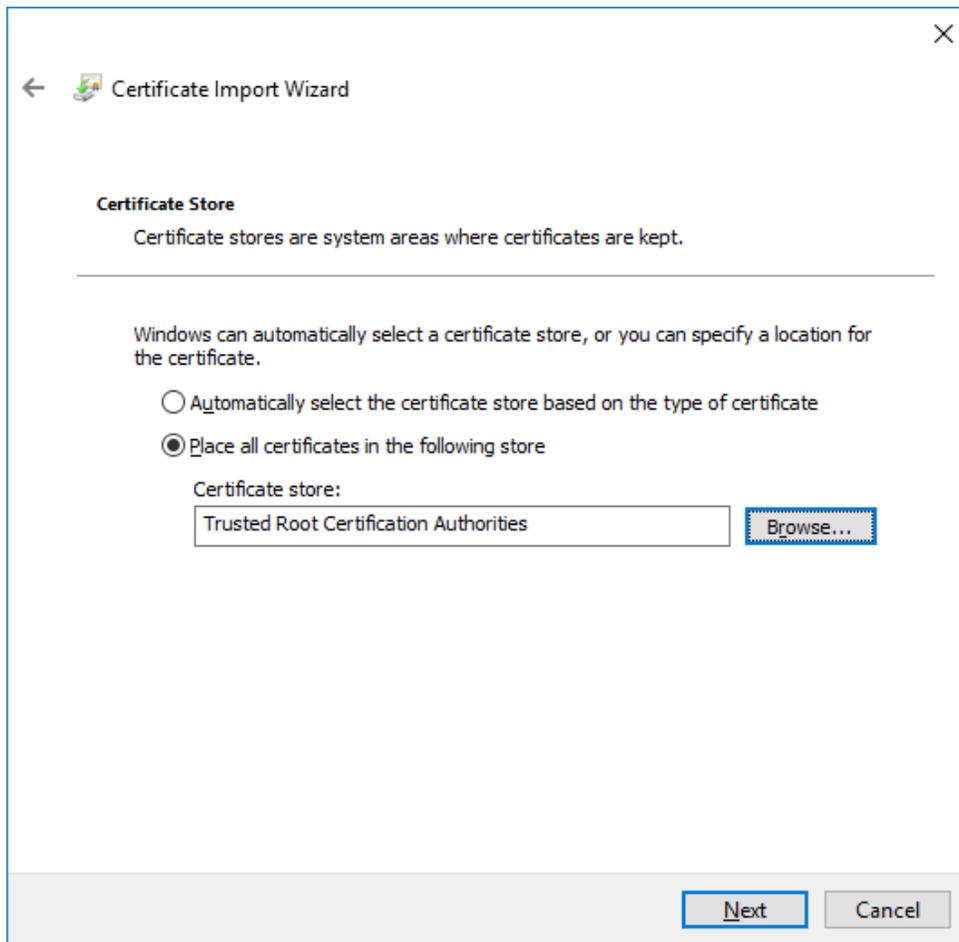
Select **Local Machine** and then click **Next**.



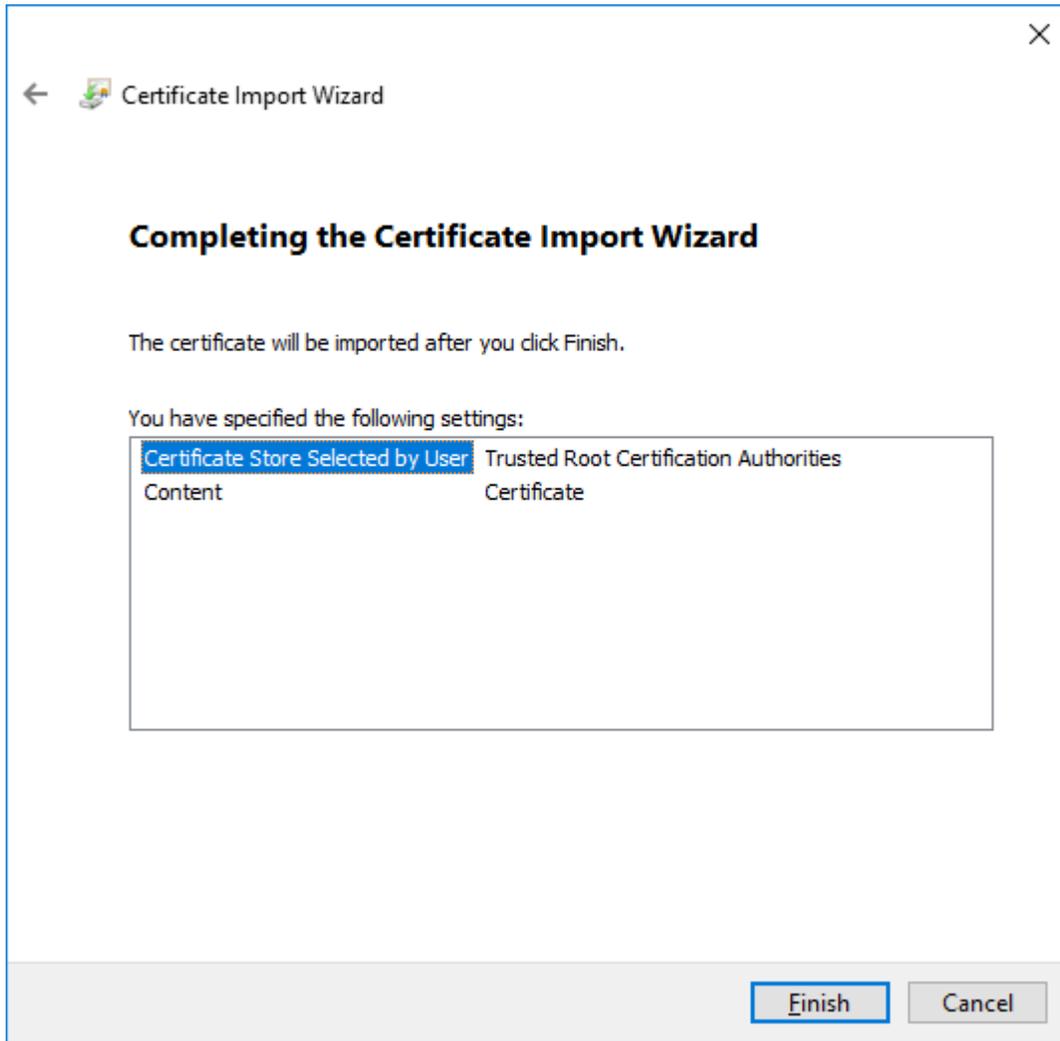
In the **Select Certificate Store** window, select **Trusted Root Certification Authorities** followed by **OK**.



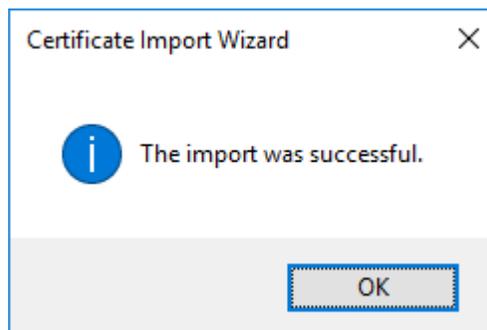
Select **Next** in the window below.



Click **Finish** to complete the wizard.



On the **Security Warning** windows, select **Yes** to install the certificate (not shown). The following window indicates successful installation of the certificate on the VHT Callback server.

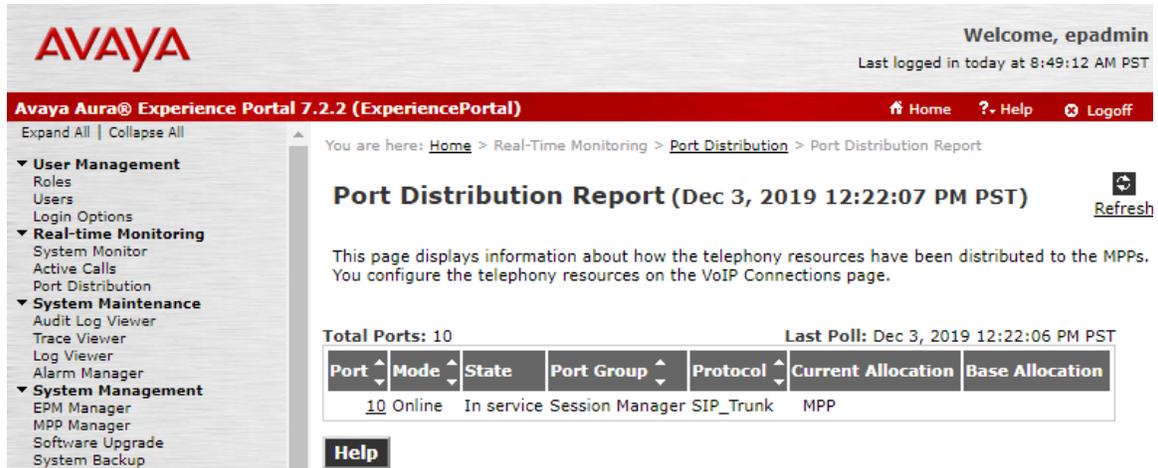


11. Verification Steps

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

11.1. Avaya Aura® Experience Portal

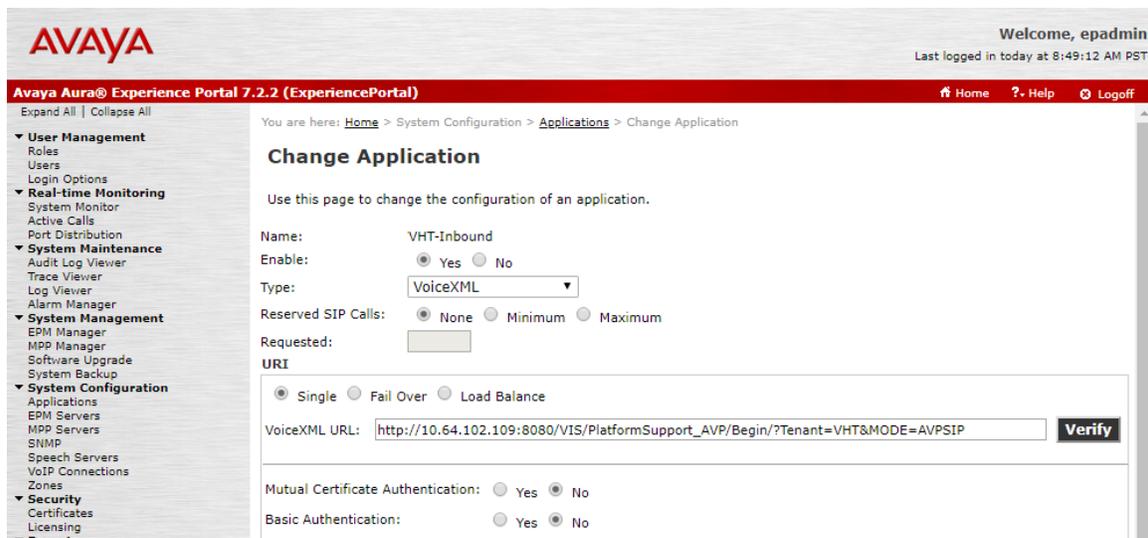
To verify VoIP connections in Experience Portal, click **Real Time Monitoring** → **Port Distribution** in the left pane. The **State** for the configured ports should be *In service*.



The screenshot shows the Avaya Aura Experience Portal 7.2.2 interface. The left navigation pane is expanded to show 'Real-time Monitoring' > 'Port Distribution'. The main content area displays the 'Port Distribution Report (Dec 3, 2019 12:22:07 PM PST)'. Below the report title, there is a summary: 'Total Ports: 10' and 'Last Poll: Dec 3, 2019 12:22:06 PM PST'. A table shows the distribution of ports:

Port	Mode	State	Port Group	Protocol	Current Allocation	Base Allocation
10	Online	In service	Session Manager	SIP_Trunk	MPP	

Select **System Configuration** → **Applications** from the left pane to display the **Applications** page (not shown). Click the **VHT-Inbound** application link on the page. The **Change Application** page is displayed. Click the **Verify** button next to the **VoiceXML URL** field and verify that the VXML application is displayed. Repeat this procedure for the **VHT-Outbound** application.



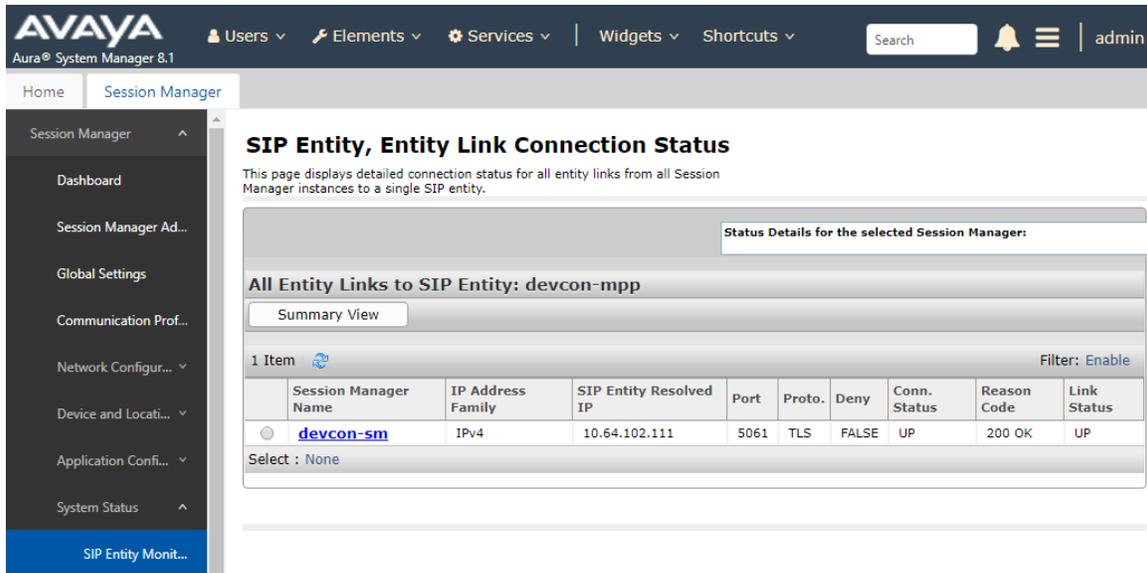
The screenshot shows the 'Change Application' page for the 'VHT-Inbound' application. The page includes the following configuration options:

- Name: VHT-Inbound
- Enable: Yes No
- Type: VoiceXML
- Reserved SIP Calls: None Minimum Maximum
- Requested: [Empty field]
- URI: Single Fail Over Load Balance
- VoiceXML URL: **Verify**
- Mutual Certificate Authentication: Yes No
- Basic Authentication: Yes No

11.2. Avaya Aura® Session Manager

This step verifies connectivity to Experience Portal. 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 Experience Portal entity name from **Section 6.2**.

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 navigation options: Session Manager, Dashboard, Session Manager Ad..., Global Settings, Communication Prof..., Network Configur..., Device and Locati..., Application Conf..., System Status, and SIP Entity Monit... The main content area is titled "SIP Entity, Entity Link Connection Status" and includes a sub-header "All Entity Links to SIP Entity: devcon-mpp". Below this is a table with one item, "devcon-sm", showing connection details.

Session Manager Name	IP Address Family	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
devcon-sm	IPv4	10.64.102.111	5061	TLS	FALSE	UP	200 OK	UP

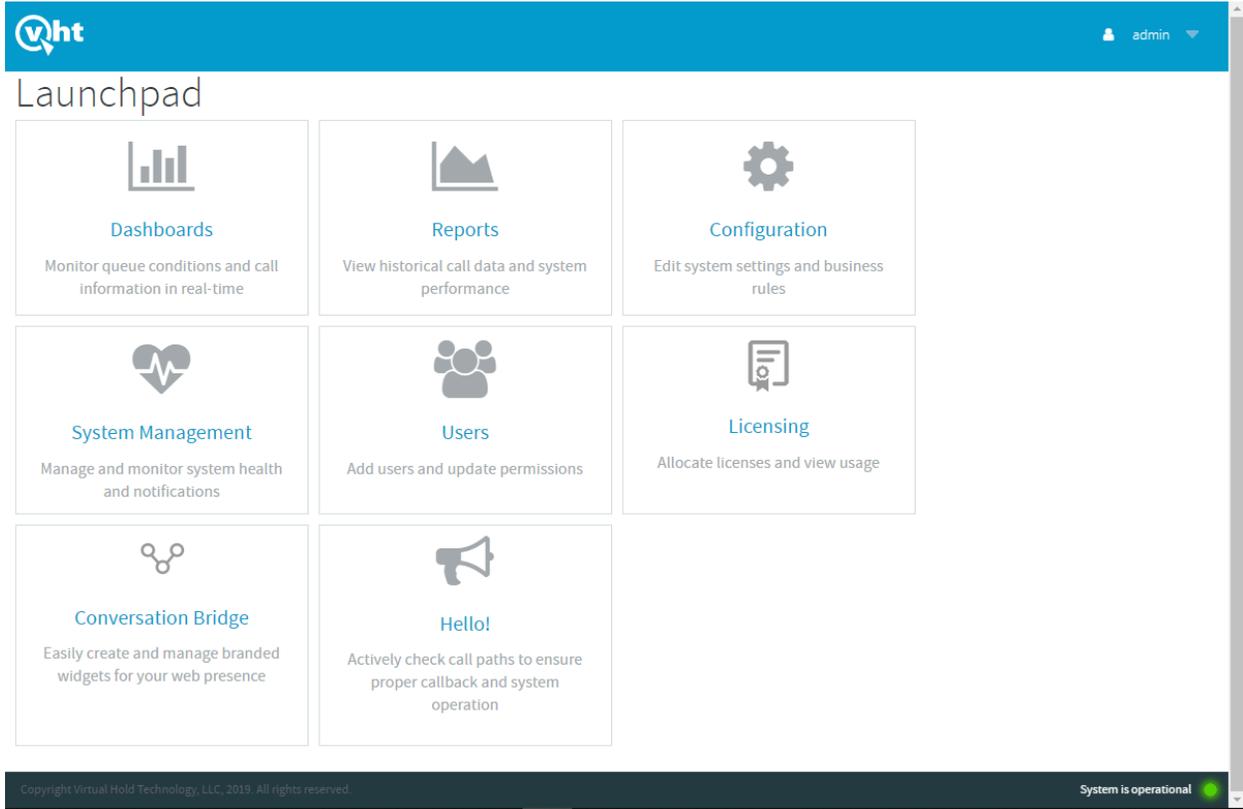
11.3. Verify VHT Callback

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 with two input fields: "User name" and "Password". Below the fields are two buttons: "Clear" and "Login". The VHT logo is visible in the bottom right corner of the form area.

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.

System Status

Manage Components ▾

The screenshot displays the 'System Status' interface. It features two main columns of components. The left column is titled 'Core (AURA8CB)' and includes a 'Mode: STANDALONE' indicator with a gear icon. Below this, a list of components is shown, each with a green status icon: CTI Connector, Queue Manager, License Server, Opmode Server, Provider, Real-Time Adapter, and Report Writer. The right column is titled 'Management (AURA8CB)' and lists: Launchpad, Platform Toolkit, Web Monitor, Message Bus, Outbound IVR, and QWatch Client. At the bottom of the dashboard, a dark bar contains the text 'Copyright Virtual Hold Technology, LLC, 2019. All rights reserved.' on the left and 'System is operational' with a green light indicator on the right.

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 and make various callback requests. Verify that the queue statistics in the screen below is updated in real-time to reflect proper active calls and expected wait time (EWT).

The screenshot displays the VHT Queues Dashboards interface. At the top, there is a blue navigation bar with the VHT logo, a 'Dashboards' dropdown menu, and a user profile for 'admin'. Below this is a grey bar with a 'Queues' dropdown menu. The main content area is titled 'Queues Dashboards' and includes three buttons: 'Show All Queues', 'Configure Stats', and 'Save Perspective'. A search bar labeled 'Queue Name' is positioned below the buttons. The primary data card is for the queue 'VHT_Test_DLG', which shows a '00:00 EWT' (Expected Wait Time) and a 'Normal' operation mode. Below the EWT, a list of statistics is shown: 0 TOTAL CALLS, 0 ASAP, 0 SCHEDULED, 0 HOLDING, and 0 PRIORITY. At the bottom of the dashboard, there are two buttons: 'Phone Lookup' and 'Line Status'. The footer contains the copyright notice 'Copyright Virtual Hold Technology, LLC, 2019. All rights reserved.' and a green indicator light stating 'System is operational'.

12. Conclusion

These Application Notes describe the steps required to integrate VHT Callback using Genesys T_Server with Avaya Aura® Communication Manager, Avaya Aura® Session Manager, Avaya Aura® Application Enablement Services, and Avaya Aura® Experience Portal. 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**.

13. 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. *Administering Avaya Aura® Experience Portal*, Release 7.2.2, Issue 1, March 2019, available at <http://support.avaya.com>.
5. *VHT Callback Configuration Guide Version 8.11 or Later*, available at <https://insight.vhtcx.com>.
6. *VHT Callback Installation Guide Version 8.10.1 or Later*, available at <https://insight.vhtcx.com>.

©2020 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.