Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Virtual Hold Queue Manager using Genesys T-Server with Avaya Aura® Experience Portal, Avaya Aura® Application Enablement Services, Avaya Aura® Session Manager, and Avaya Aura® Communication Manager - Issue 1.0

Abstract

These Application Notes describe the configuration steps required to integrate Virtual Hold Queue Manager using Genesys T-Server with Avaya Aura® Experience Portal, Avaya Aura® Application Enablement Services, Avaya Aura® Session Manager, and Avaya Aura® Communication Manager.

Virtual Hold Queue Manager is a contact center solution that calculates the estimated wait time for an incoming call and maintains the caller's position in a virtual queue. Virtual Hold Queue Manager can call the user back and connect to an agent when the caller's turn comes up. The integration with Avaya Aura® Experience Portal is achieved through an inbound and an outbound VXML application. 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. Calls to Virtual Hold VXML applications are routed using SIP connections 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.

©2016 Avaya Inc. All Rights Reserved.

TABLE OF CONTENTS

1. Introduction 3
2. General Test Approach and Test Results 4
   2.1. Interoperability Compliance Testing 4
   2.2. Test Results 5
   2.3. Support 5
3. Reference Configuration 6
4. Equipment and Software Validated 7
5. Configure Avaya Aura® Communication Manager 8
6. Configure Avaya Aura® Application Enablement Services 18
   Restart TSAPI Service 22
7. Configure Avaya Aura® Session Manager 25
8. Configure Avaya Aura® Experience Portal 32
9. Configure Virtual Hold 40
10. Verification Steps 69
   10.1. Avaya Aura® Experience Portal 69
   10.2. Avaya Aura® Session Manager 71
11. Conclusion 71
12. Additional References 71

©2016 Avaya Inc. All Rights Reserved.

1. Introduction

These Application Notes describe the configuration steps required to integrate Virtual Hold Queue Manager (VHT) using Genesys T-Server with Avaya Aura® Experience Portal, Avaya Aura® Application Enablement Services (AES), Avaya Aura® Session Manager, and Avaya Aura® Communication Manager.

Virtual Hold is a contact center intelligent queue management solution that calculates the Estimated Wait Time (EWT) for an incoming call and maintains the caller's position in a virtual queue. Virtual Hold can call the user back and connect to an agent when the caller's turn comes up. Virtual Hold consists of Virtual Hold Queue Manager and Virtual Hold VXML Interaction Server (VIS). Virtual Hold Queue Manager is responsible for making routing decisions and maintaining the virtual queue. Virtual Hold VXML Interaction Server allows for Avaya Aura® Experience Portal supported VXML applications, developed by VHT for inbound and outbound calls, and is responsible for interactions with Avaya Aura® Experience Portal. The integration with Avaya Aura® Communication Manager is achieved through Genesys T-Server and the AES TSAPI service for event monitoring and adjunct routing support.

As calls come into the contact center, Virtual Hold monitors the 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 being answered by 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, Virtual Hold 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.

Virtual Hold uses a Genesys T-Server element 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 CTI event reports to calculate the EWT. Incoming calls are routed to the inbound VXML application via Avaya Aura® Experience Portal, where Virtual Hold can play the EWT to the caller and provide the caller with options. Virtual Hold 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 Virtual Hold VXML applications are routed using SIP connections from Avaya Aura® Communication Manager via Avaya Aura® Session Manager.

©2016 Avaya Inc. All Rights Reserved.

2. General Test Approach and Test Results

This section describes the compliance test approach, test coverage, test results, and the support information.

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

2.1. Interoperability Compliance Testing

The purpose of this compliance testing was to verify interoperability between Virtual Hold and Avaya products including Experience Portal, Application Enablement Services, Session Manager, and Communication Manager.

The testing was performed using Experience Portal, Session Manager, and Communication Manager connected via SIP connections

The interoperability compliance test included events, feature, and serviceability testing.

- The event testing used internal logs to verify receiving and proper handling of CTI events by Virtual Hold.
- The feature testing entailed placing calls manually from a PSTN phone to Experience Portal and verifying the following:
    - Adjunct route by Virtual Hold.
    - Virtual Hold VXML applications launch.
    - Experience Portal using SIP as VoIP Connections.
    - Experience Portal Call Detail Report and Alarm/Warning generation.
    - Virtual Hold playing Estimated Wait Time.
    - Virtual Hold handling of caller options including callback, scheduled callback, and staying in queue.
    - Virtual Hold storing and passing UUI in callback calls.
- The serviceability testing focused on verifying the ability of Experience Portal and Virtual Hold to recover after a network outage or server reboot.

©2016 Avaya Inc. All Rights Reserved.

2.2. Test Results

All test cases were executed and passed. Note that the testing was completed using a special patch 23255 for Communication Manager. The patch fixes an issue where the "Queued" event isn't being delivered for the calls that are redirected to Communication Manager by Experience Portal. The issue occurs when PSTN calls are routed over a SIP/PRI trunk to Experience Portal via Communication Manager and Session Manager, with Experience Portal routing the call back to Communication Manager for queuing. The observed behavior is that after the call is transferred back to Communication Manager, the previous call (Experience Portal) is seen as connected. This patch is scheduled to be generally available in December 2016. Customer deploying Virtual Hold Manager with Communication Manager Release 7.0 may request the patch from Avaya.

2.3. Support

To obtain technical support for Virtual Hold:

- **Web:** www.virtualhold.com
- **Email:** support@virtualhold.com
- **Phone:** (866) 670 - 2223

©2016 Avaya Inc. All Rights Reserved.

3. Reference Configuration

The diagram below illustrates the test configurations. Experience Portal and Communication Manager connected via SIP connections using Session Manager.

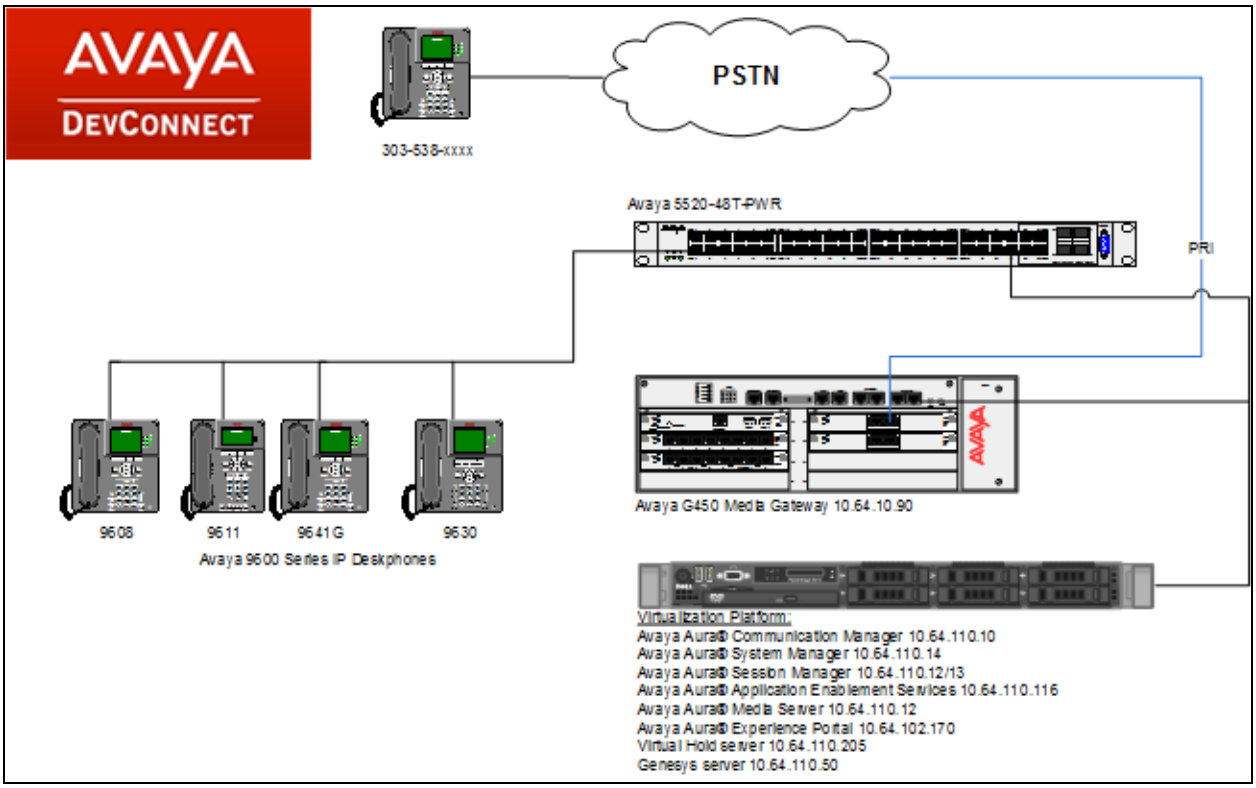


Figure 1: Test Configuration

©2016 Avaya Inc. All Rights Reserved.

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya Aura® Communication Manager	R017x.00.0.441.0 – 23255
Avaya Aura® Application Enablement Services	7.0.1.0.2.15-0
Avaya Aura® Session Manager	7.0.1.1.701114
Avaya Aura® System Manager	7.0.1.1.065378
Avaya Aura® Experience Portal	7.0.2
Avaya Aura® Media Server	7.7.0.334 A15
Avaya G450 Media Gateway	37.19.0
Avaya 9600 Series IP Telephones	
9641/9611/9608 (H.323) 9630 (H.323)	6.6.2 3.2.6
Virtual Hold	
Queue Manager	8.6.0.809
VXML Interaction Server (biz)	5.11.0.804
Genesys T-Server	8.1.001.06

©2016 Avaya Inc. All Rights Reserved.

5. Configure Avaya Aura® Communication Manager

This section describes the Communication Manager configuration for supporting the Virtual Hold solution.

It is assumed that the following administration is already in place and will not be described in this section.

- SIP trunk group to Session Manager
- Route Pattern that maps to the SIP trunk group

The configuration of Communication Manager was performed using the System Access Terminal (SAT). After the completion of the configuration, perform a **save translation** command to make the changes permanent.

The configuration procedures fall into the following areas:

- Verify Communication Manager Licenses
- Configure System Parameters Features
- Configure Cti-link
- Configure Hunt Group for Contact Center Agents
- Configure Automatic Alternate Routing (AAR)
- Configure VDNs and Vectors
- Configure UUI Treatment for Trunk Group

©2016 Avaya Inc. All Rights Reserved.

Step	Description
1.	**Communication Manager Licenses** Verify that the Communication Manager license has proper permissions for features illustrated in these Application Notes. Use the **display system-parameters customer-options** command to verify that the **Computer Telephony Adjunct Links** option is set to **y** on **Page 3**. If this option is not set to **y**, then contact the Avaya sales team or business partner for a proper license file.

```
change system-parameters customer-options                       Page   3 of  11
                                OPTIONAL FEATURES

    Abbreviated Dialing Enhanced List? y           Audible Message Waiting? y
        Access Security Gateway (ASG)? n               Authorization Codes? y
        Analog Trunk Incoming Call ID? y                          CAS Branch? n
 A/D Grp/Sys List Dialing Start at 01? y                            CAS Main? n
Answer Supervision by Call Classifier? y                  Change COR by FAC? n
                                ARS? y  Computer Telephony Adjunct Links? y
                 ARS/AAR Partitioning? y   Cvg Of Calls Redirected Off-net? y
          ARS/AAR Dialing without FAC? y                       DCS (Basic)? y
          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
```

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

```
change system-parameters customer-options                       Page   6 of  11
                         CALL CENTER OPTIONAL FEATURES

                          Call Center Release: 6.0

                                ACD? y                          Reason Codes? y
                       BCMS (Basic)? y               Service Level Maximizer? y
         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
```


©2016 Avaya Inc. All Rights Reserved.

Step	Description
2.	**System-Parameters Features** Enter the **change system-parameters features** command and navigate to **Page 5**. Set the **Create Universal Call ID (UCID)** field to **y.**

```
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: 1
```

On **Page 13,** set the **Send UCID to ASAI** field to **y.**

```
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
```


©2016 Avaya Inc. All Rights Reserved.

Step	Description
3.	**Create a Cti-link** Add a CTI link using the **add cti-link n** command; where **n** is an available CTI link number. Enter an available extension number in the **Extension** field. Note that the CTI link number and extension number may vary. Enter **ADJ-IP** in the **Type** field, and a descriptive name in the **Name** field. Default values may be used in the remaining fields. add cti-link 1 Page 1 of 3 CTI LINK CTI Link: 1 **Extension: 19999** **Type: ADJ-IP** COR: 1 **Name: aes**

©2016 Avaya Inc. All Rights Reserved.

Step	Description
4.	**Create Hunt Group for Contact Center Agents** Administer a hunt group for Call Center Agents by using the **add hunt-group n** command; where **n** is an available hunt group number. On **Page 1**, enter a descriptive name in the **Group Name** field and an available extension in the **Group Extension** field. Set **ACD**, **Queue,** and **Vector** fields to **y**.

```
add hunt-group 1                                                Page   1 of   4
                                    HUNT GROUP

            Group Number: 1                                   ACD? y
              Group Name: Hunt Group 1                      Queue? y
          Group Extension: 12001                           Vector? y
               Group Type: ucd-mia
                       TN: 1
                      COR: 1                     MM Early Answer? n
           Security Code:                Local Agent Preference? n
 ISDN/SIP Caller Display:

             Queue Limit: unlimited
 Calls Warning Threshold:      Port:
  Time Warning Threshold:      Port:
```

On **Page 2**, set the **Skill** field to **y**.

```
add hunt-group 1                                                Page   2 of   4
                                    HUNT GROUP

                     Skill? y      Expected Call Handling Time (sec): 180
                       AAS? n        Service Level Target (% in sec): 80 in 20
                  Measured: both
     Supervisor Extension:


      Controlling Adjunct: none


        VuStats Objective:

   Multiple Call Handling: none


 Timed ACW Interval (sec):          After Xfer or Held Call Drops? n
```

For the compliance testing, three agents with extensions 11001 and 11002 and agent Login ids 1101 and 1102 were configured as available agents for the above hunt group.

```
list agent-loginID 1101 count 2

                                AGENT LOGINID
Login ID     Name           Extension     Dir Agt  AAS/AUD        COR Ag Pr SO
               Skil/Lv Skil/Lv Skil/Lv Skil/Lv Skil/Lv Skil/Lv Skil/Lv Skil/Lv

1101         IP Agent 1     unstaffed                                1   lvl
                 1/01     /       /       /       /       /       /       /
1102         IP Agent 2     unstaffed                                1   lvl
                 1/01     /       /       /       /       /       /       /
```


©2016 Avaya Inc. All Rights Reserved.

Step	Description
5.	**Automatic Alternate Routing (AAR) (SIP Configuration only)** For the compliance test, AAR was used to route calls to Experience Portal via a SIP trunk to Session Manager. Route Pattern 1 was pre-configured to use Trunk Group 1, which is a SIP trunk connected to Session Manager. For the compliance test, use the **change aar analysis** command to add an entry to AAR table as follows: • Enter **113** in the **Dialed String** field. • Enter **5** and **5** to the **Total Min** and **Total Max** fields. • Enter **1** to the **Route Pattern** field. • Enter **aar** in the **Call Type** field. With the above entry, all calls with dialed digits of 113xx will be routed over Trunk Group 1 to Session Manager. In the compliance test, extension 11301 is associated with the Experience Portal inbound application. change aar analysis 113 Page 1 of 2 AAR DIGIT ANALYSIS TABLE Location: all Percent Full: 0 Dialed Total Route Call Node ANI String Min Max Pattern Type Num Reqd **113 5 5 1 aar n**

©2016 Avaya Inc. All Rights Reserved.

Step	Description

6.	**VDNs and Vectors for SIP Configuration**
	Administer a set of Vector Directory Numbers (VDNs) and vectors as follows:
	• Entry VDN/vector: To perform adjunct route with the Virtual Hold Queue Manager
	• Holding VDN/vector: To queue incoming calls to the agent skill at medium priority.
	• Callback VDN/vector: To queue callback calls to the agent skill at high priority.
	
	Entry VDN and Vector
	Modify an available vector using the **change vector n** command, where **n** is an existing vector number.
	
	Following configuration was used during compliance testing.
	
	`change vector 101  Page 1 of 6`
	`CALL VECTOR`
	`Number: 101  Name: Incoming`
	`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 set  A  = none  CATR  12345`
	`03 adjunct  routing link 1`
	`04 wait-time  10  secs hearing ringback`
	`05 route-to  number 12202  with cov n if unconditionally`
	`06 disconnect  after announcement none`
	`07 stop`
	
	Add a VDN using the **add vdn n** command, where **n** is an available extension number. Enter a descriptive **Name**, and the vector number from above for **Vector Number**.
	
	Retain the default values for all remaining fields.
	
	`add vdn 12201  Page 1 of 3`
	`VECTOR DIRECTORY NUMBER`
	`Extension: 12201`
	`**Name*: VHT - Incoming**`
	`**Destination: Vector Number  101**`
	`Attendant Vectoring? n`
	`Meet-me Conferencing? n`
	`Allow VDN Override? y`
	`COR: 1`
	`TN*: 1`
	`Measured: none  Report Adjunct Calls as ACD*? n`
	
	Continue on the next page.

©2016 Avaya Inc. All Rights Reserved.

Step	Description

	Holding VDN and Vector
	Modify an available vector using the **change vector n** command, where **n** is an existing vector number.
	
	Following configuration was used during compliance testing.
	
	`change vector 102  Page 1 of 6`
	`CALL VECTOR`
	
	`Number: 102  Name: Holding`
	`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 1  pri m`
	`03 wait-time  30  secs hearing ringback`
	`04 goto step  3  if unconditionally`
	`05 disconnect  after announcement none`
	`06 stop`
	
	Add a VDN using the **add vdn n** command, where **n** is an available extension number. Enter a descriptive **Name**, and the vector number from above for the **Destination** field. Retain the default values for all remaining fields.
	
	`add vdn 12202  Page 1 of 3`
	`VECTOR DIRECTORY NUMBER`
	
	`Extension: 12202`
	`**Name*: VHT - Hold**`
	`**Destination: Vector Number  102**`
	`Attendant Vectoring? n`
	`Meet-me Conferencing? n`
	`Allow VDN Override? n`
	`COR: 1`
	`TN*: 1`
	`Measured: none  Report Adjunct Calls as ACD*? n`
	
	Continue on the next page.

©2016 Avaya Inc. All Rights Reserved.

Step	Description

	Callback VDN and Vector
	Modify an available vector using the **change vector n** command, where **n** is an existing vector number.
	
	Following configuration was used during compliance testing.
	
	`change vector 103  Page 1 of 6`
	`CALL VECTOR`
	
	`Number: 103  Name: 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 wait-time  0 secs hearing silence`
	`02 queue-to  skill 1  pri h`
	`03 wait-time  30 secs hearing ringback`
	`04 goto step  3  if unconditionally`
	`05 disconnect  after announcement none`
	`06 stop`
	
	Add a VDN using the **add vdn n** command, where **n** is an available extension number. Enter a descriptive **Name**, and the vector number from above for the **Destination** field. Retain the default values for all remaining fields.
	
	`add vdn 12203  Page 1 of 3`
	`VECTOR DIRECTORY NUMBER`
	
	`Extension: 12203`
	`**Name*: VHT - Callback**`
	`**Destination: Vector Number  103**`
	`Attendant Vectoring? n`
	`Meet-me Conferencing? n`
	`Allow VDN Override? n`
	`COR: 1`
	`TN*: 1`
	`Measured: none  Report Adjunct Calls as ACD*? n`

©2016 Avaya Inc. All Rights Reserved.

Step	Description

7.	**UUI Treatment for SIP Trunk Group (SIP Configuration only)**
	Enter the **change trunk-group n** command where **n** is the trunk group number of the SIP trunk to Session Manager. Set the **UUI Treatment** field to **shared** and **Send UCID** field to **yes**.
	
	`change trunk-group 1  Page  3 of  22`
	`TRUNK FEATURES`
	`ACA Assignment? n  Measured: none`
	`Maintenance Tests? y`
	
	`Suppress # Outpulsing? n  Numbering Format: public`
	`UUI Treatment: shared`
	`Maximum Size of UUI Contents: 128`
	`Replace Restricted Numbers? n`
	`Replace Unavailable Numbers? n`
	
	`Hold/Unhold Notifications? y`
	`Modify Tandem Calling Number: no`
	`Send UCID? y`
	
	`Show ANSWERED BY on Display? y`

©2016 Avaya Inc. All Rights Reserved.

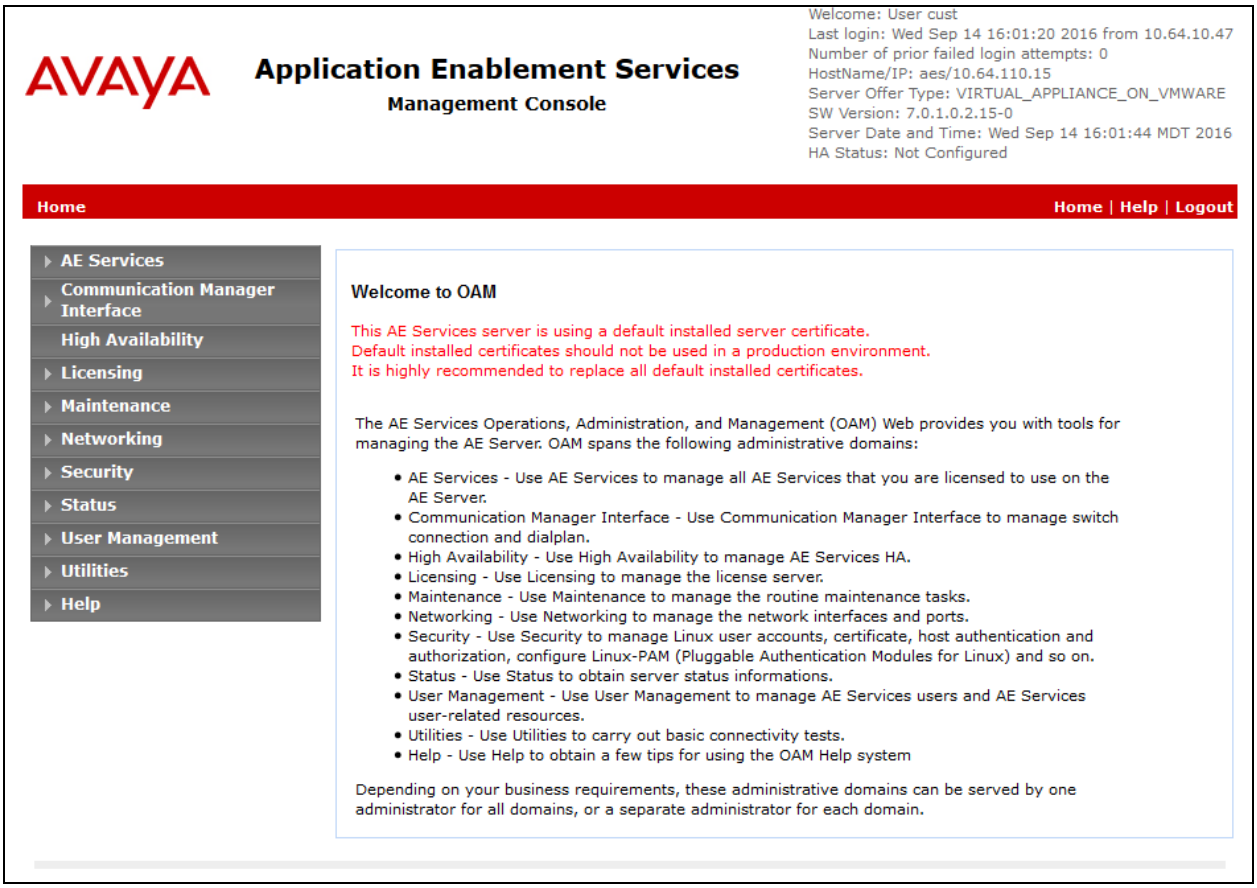
6. Configure Avaya Aura® Application Enablement Services

The configuration of Application Enablement Services is performed via a web browser. Enter **https://<ip-addr>** in the URL field of a web browser where **<ip-addr>** is the IP address of the Application Enablement Services server. After a login step, the **Welcome to OAM** page is displayed.

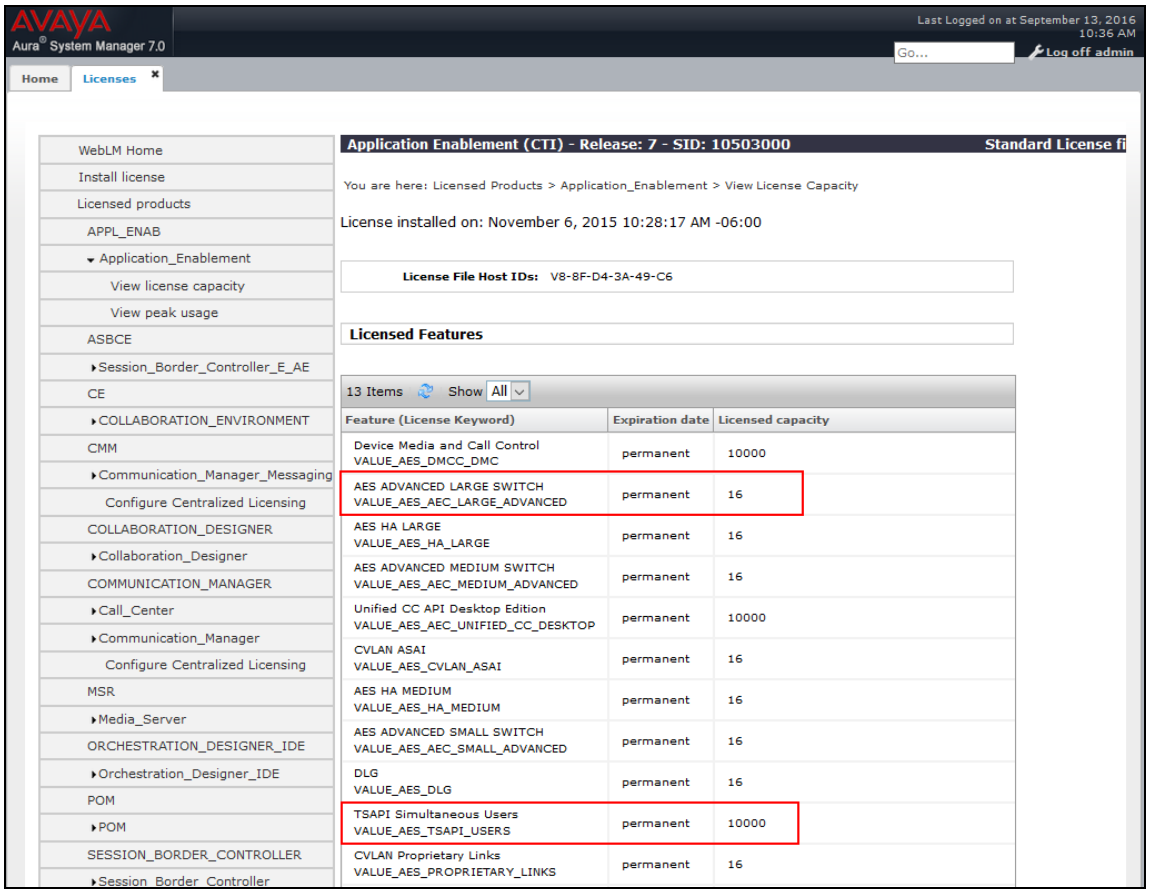
The configuration procedures fall into the following areas:

- Confirm TSAPI Licenses
- Add TSAPI Links
- Note the Tlink Information
- Restart TSAPI Service
- Configure Virtual Hold User
- Enable Unrestricted Access for Virtual Hold User

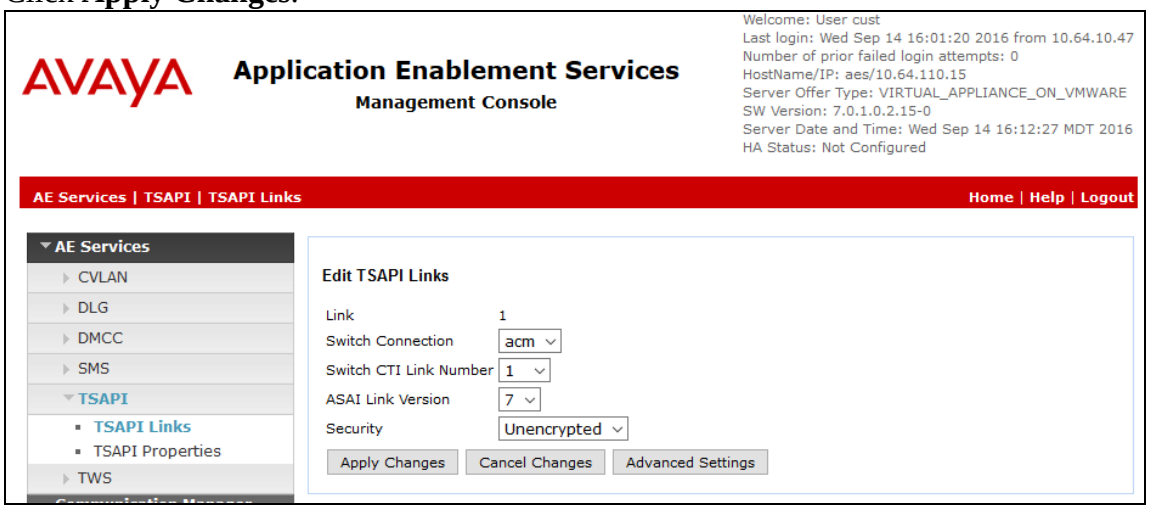
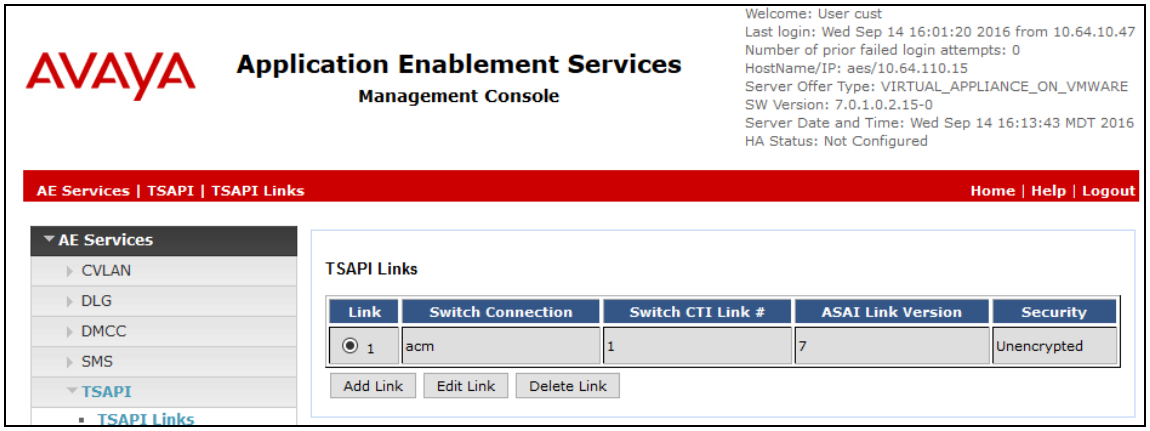
It is assumed that the configuration of a switch connection to Communication Manager is already in place and therefore will not be described here.



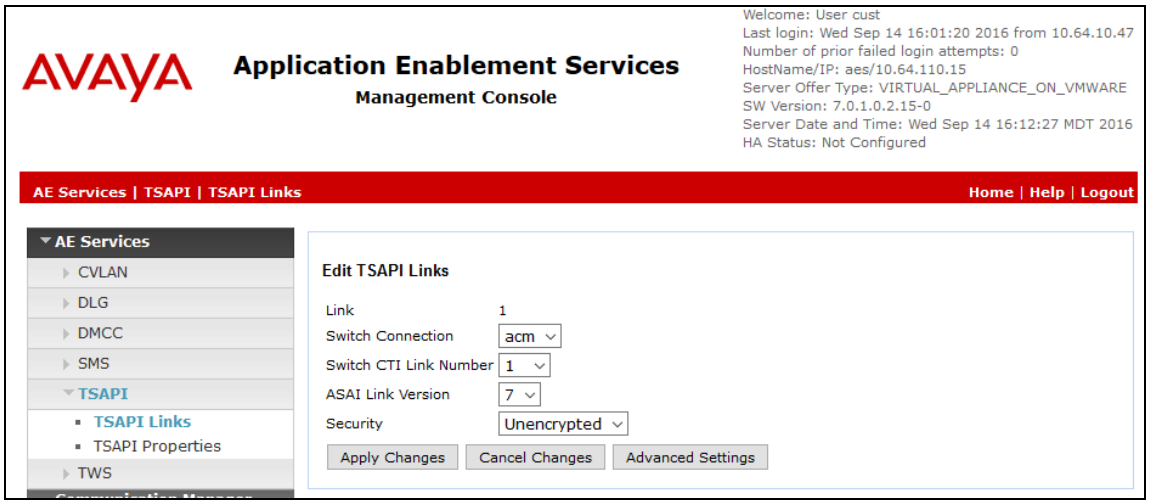
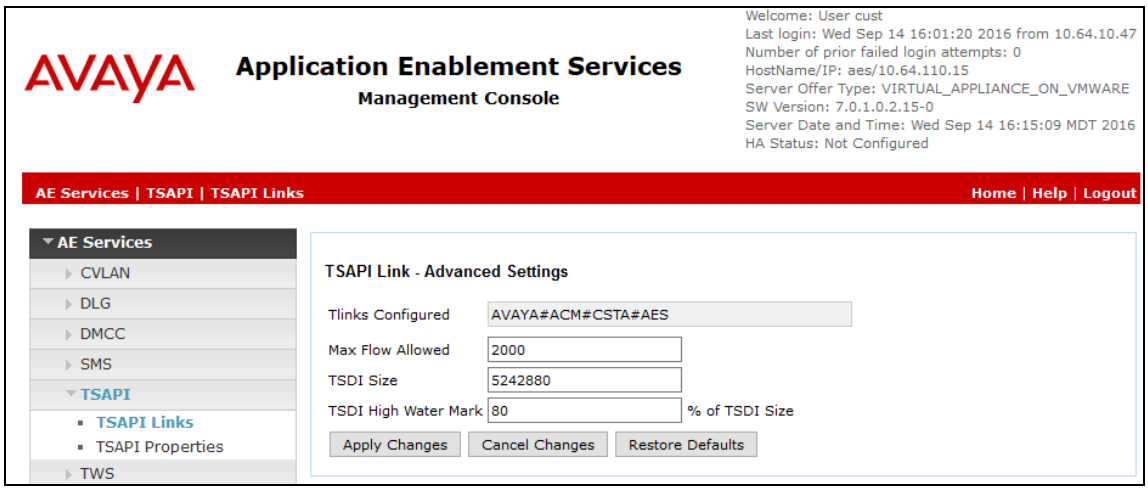
©2016 Avaya Inc. All Rights Reserved.

Step	Description
1.	**Confirm TSAPI Licenses** Virtual Hold uses a TSAPI Advanced (**VALUE_AES_AEC_xxxxx_ADVANCED)** license for adjunct routing and a TSAPI Basic (**VALUE_AES_TSAPI_USERS**) license for each VDN being monitored. If the licensed quantities are not sufficient for the implementation, contact the Avaya sales team or business partner for a proper license file. From the left pane of the Application Enablement Services Management Console, click **Licensing → WebLM Server Access**. A **Web License Manager** login window is displayed. Enter proper credentials to log in. Click **Licensed products → APPL_ENAB → Application_Enablement** from the left pane. The Application Enablement Services license is displayed in the right pane. Ensure that there are enough **VALUE_AES_AEC_xxxxx_ADVANCED** and **VALUE_AES_TSAPI_USERS** licenses available. 

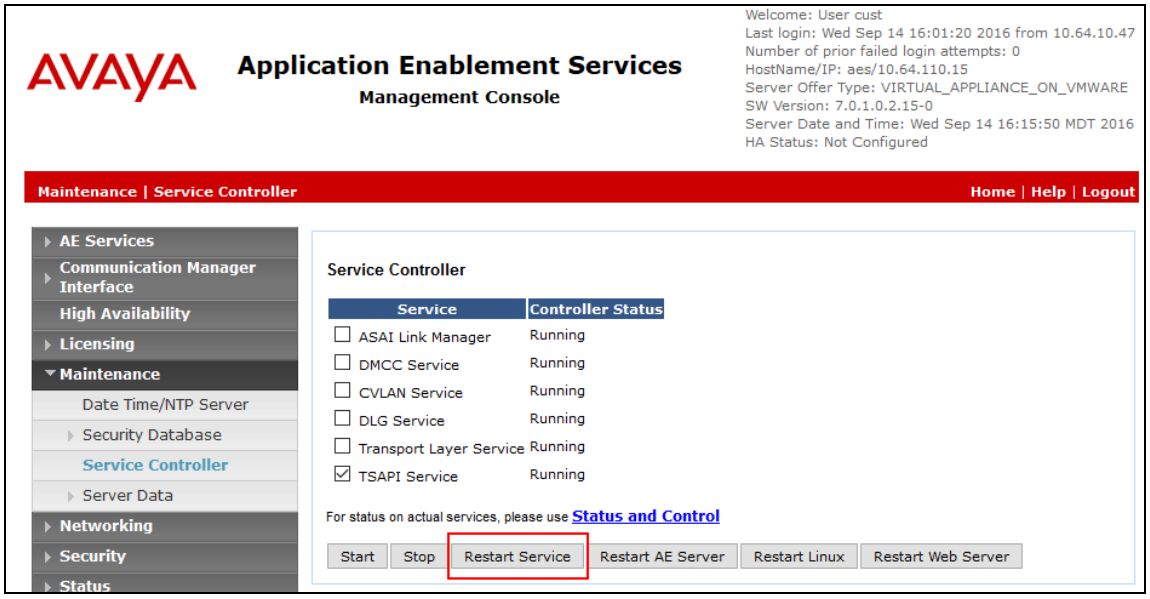
©2016 Avaya Inc. All Rights Reserved.

Step	Description
2.	**Add TSAPI Links** Navigate to the **AE Services → TSAPI → TSAPI Links** page to add a TSAPI Link. Click **Add Link** (not shown). Select a **Switch Connection** and the **Switch CTI Link Number** using the drop down menus. The **Switch CTI Link Number** must match the number configured in the **cti-link** form in **Section 5**, **Step 3**. Select **Unencrypted** for the **Security** field. Click **Apply Changes**.  It returns to the **TSAPI Links** screen which shows that the **acm** link has been added. 

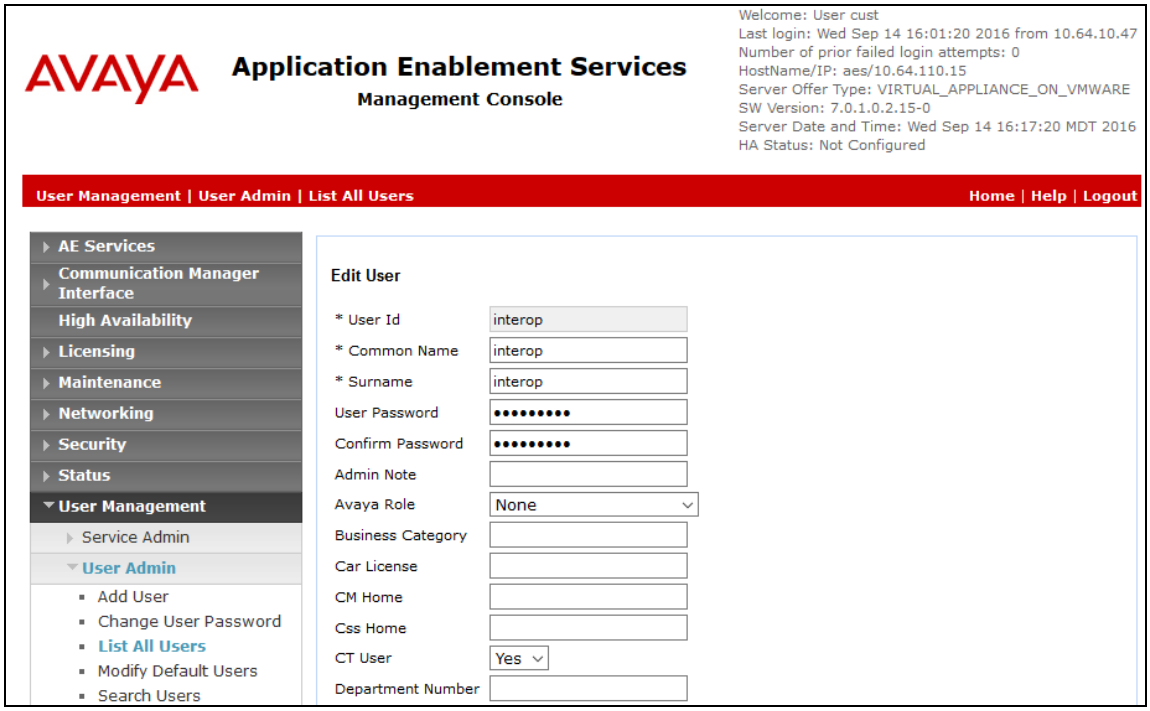
©2016 Avaya Inc. All Rights Reserved.

Step	Description
3.	**Note the Tlink Information** Select the **acm** TSAPI Link and click **Edit Link**. The **Edit TSAPI Links** screen is displayed.  Click the **Advanced Settings** button. The **TSAPI Link – Advanced Settings** screen is displayed. Note the value in the **Tlinks Configured** field which will be used for Virtual Hold configuration in **Section 9**. 

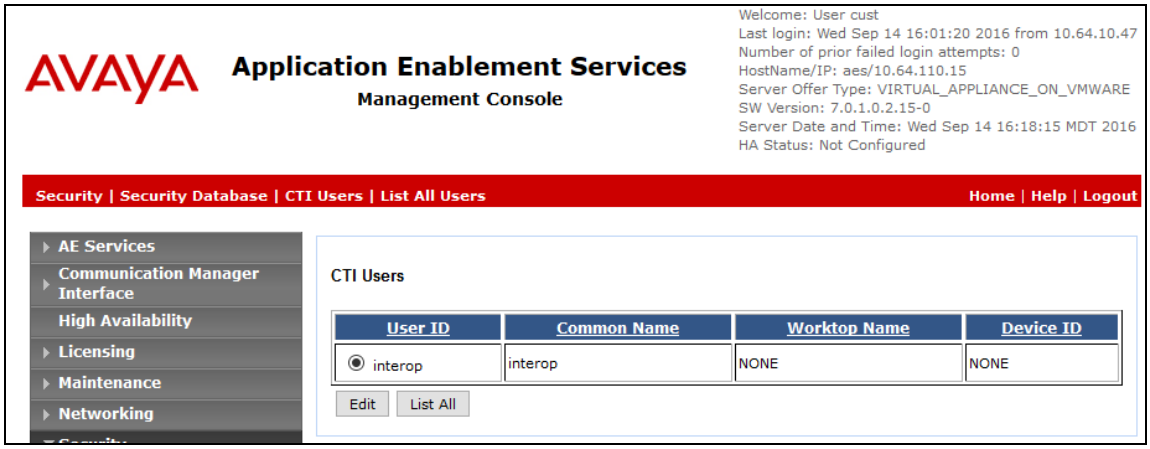
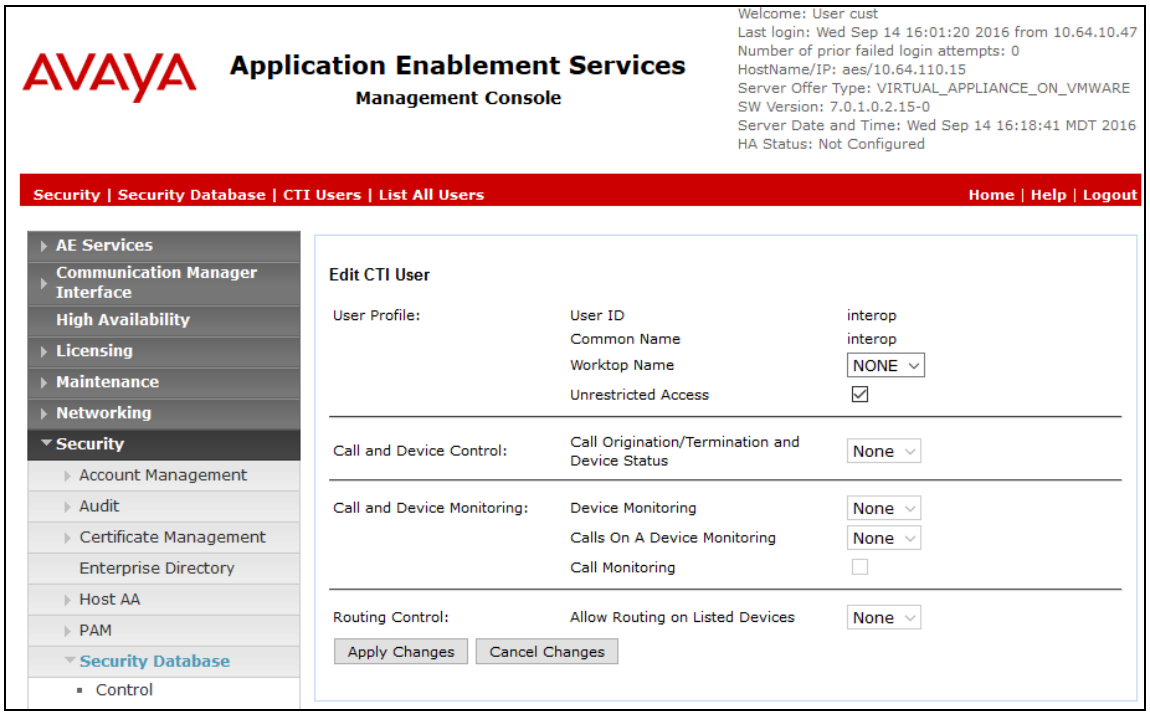
©2016 Avaya Inc. All Rights Reserved.

Step	Description
4.	**Restart TSAPI Service** Select **Maintenance → Service Controller** from the left pane, to display the **Service Controller** screen in the right pane. Check the **TSAPI Service**, and click **Restart Service**. 

©2016 Avaya Inc. All Rights Reserved.

Step	Description
5.	**Configure Virtual Hold user** In the left pane, select **User Management → User Admin → Add User**. The **Add User** panel will be displayed. Enter an appropriate **User Id, Common Name, Surname,** and **User Password**. Select **Yes** from the **CT User** dropdown list. Click **Apply** at the bottom of the page (not shown) to save the entry. 

©2016 Avaya Inc. All Rights Reserved.

Step	Description
6.	**Enable Unrestricted Access for Virtual Hold User** If the Security Database (SDB) is enabled on Application Enablement Services, set the Virtual Hold user account to Unrestricted Access to enable access to any device. This step avoids the need to duplicate administration. Navigate to **Security → Security Database → CTI Users → List All Users**. The **CTI Users** screen is displayed. Select the **interop** user and click **Edit**.  On the **Edit CTI User** page, check the **Unrestricted Access** box and click the **Apply Changes** button. Click **Apply** when asked to confirm the change on the **Apply Changes to CTI User Properties** dialog (not shown). 

©2016 Avaya Inc. All Rights Reserved.

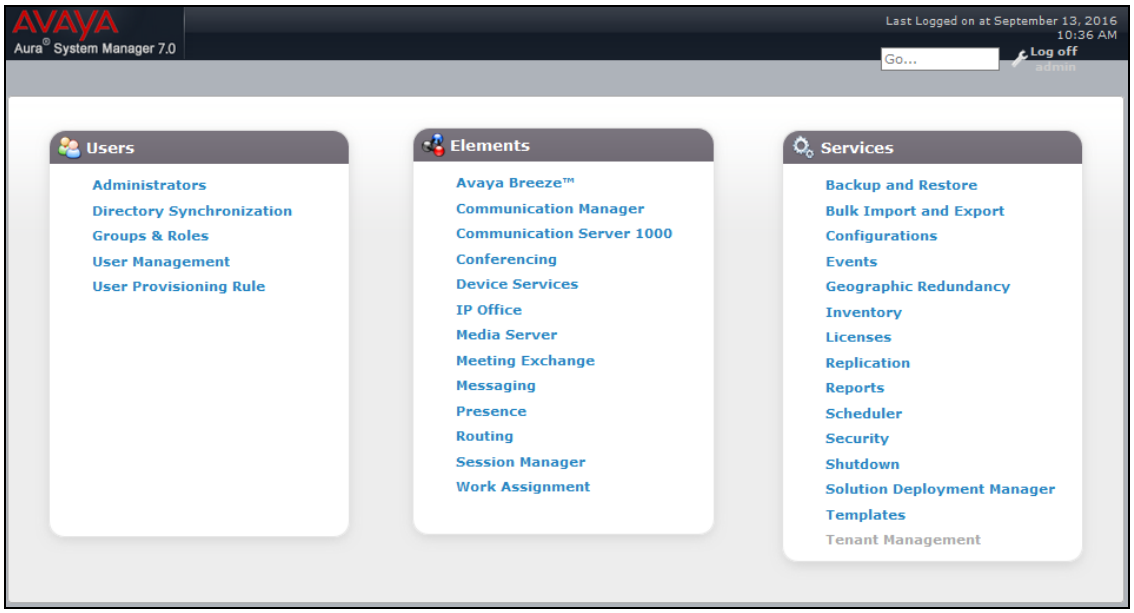
7. Configure Avaya Aura® Session Manager

This section provides the steps for configuring Session Manager to route calls to Experience Portal. It is assumed that basic administration for Session Manager such as Domain, Locations, and Time Range, as well as the configuration for an entity link to Communication Manager are already in place and therefore will not be described here.

The configuration procedures fall into the following areas:

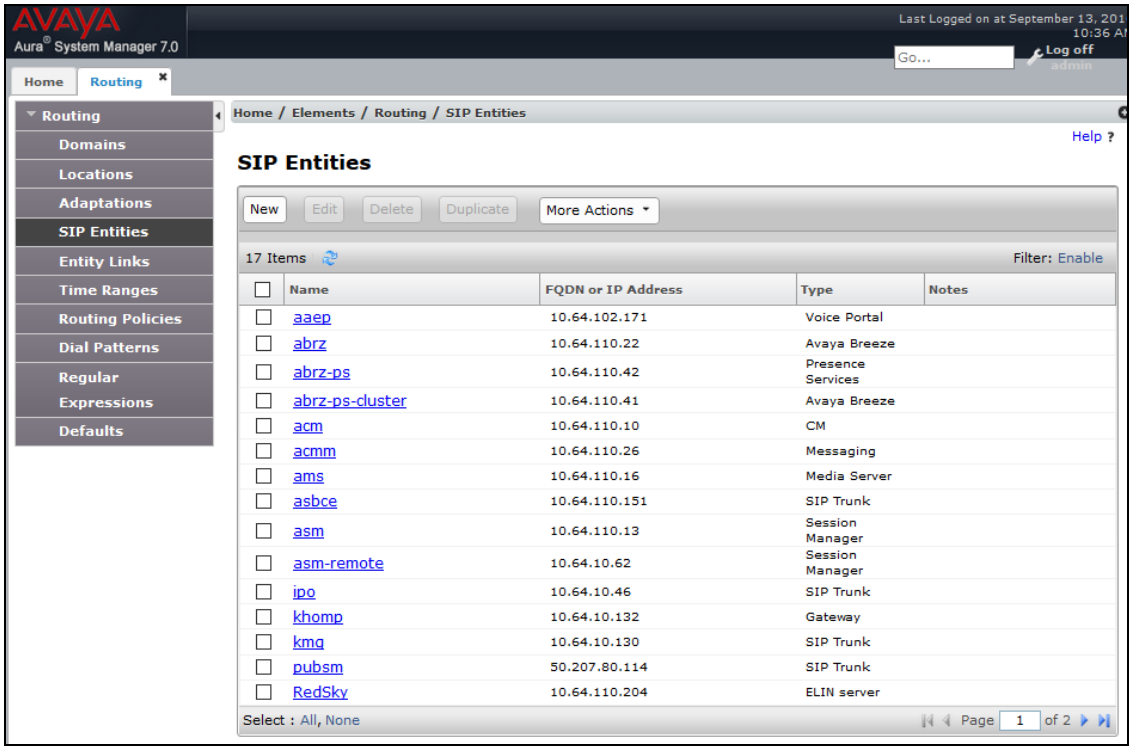
- Launch System Manager
- Configure SIP Entity for Experience Portal
- Configure Entity Link for Experience Portal
- Configure Routing Policy for Experience Portal
- Configure Dial Pattern for Experience Portal

©2016 Avaya Inc. All Rights Reserved.

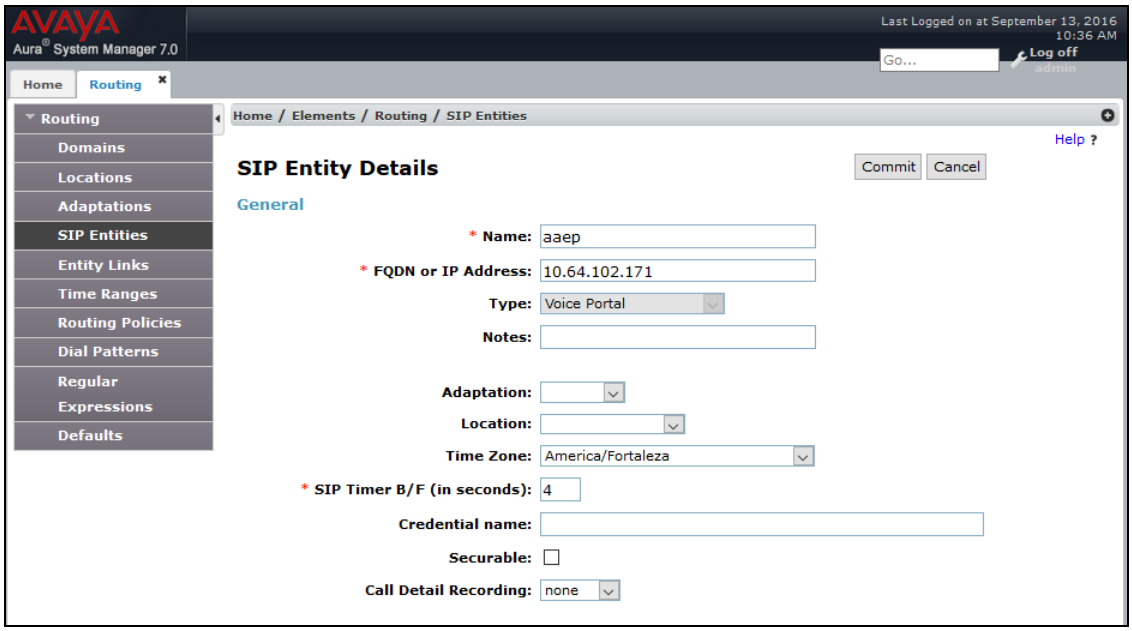
Step	Description
1.	**Launch System Manager** Session Manager is configured using browser access to System Manager. Enter **https://<*ip-addr*>** into the URL field of a web browser, where **<*ip-addr*>** is the IP address or qualified domain name of the System Manager. Log in using appropriate credentials. The home page is a navigation screen as shown below. Each of these links will open a new tab from which to navigate to the details of the managed environment. Click **Routing** under **Elements**. 

©2016 Avaya Inc. All Rights Reserved.

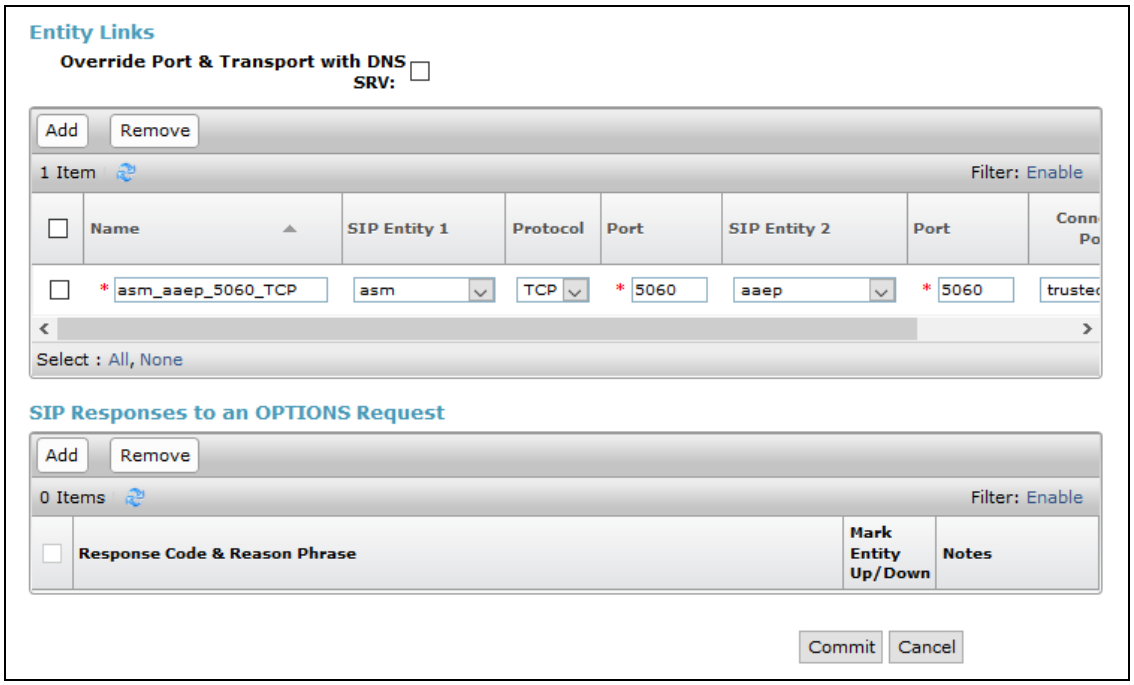
Step	Description
2.	**Configure SIP Entity for Experience Portal** On the left pane, click **SIP Entities**. The **SIP Entities** screen is displayed.



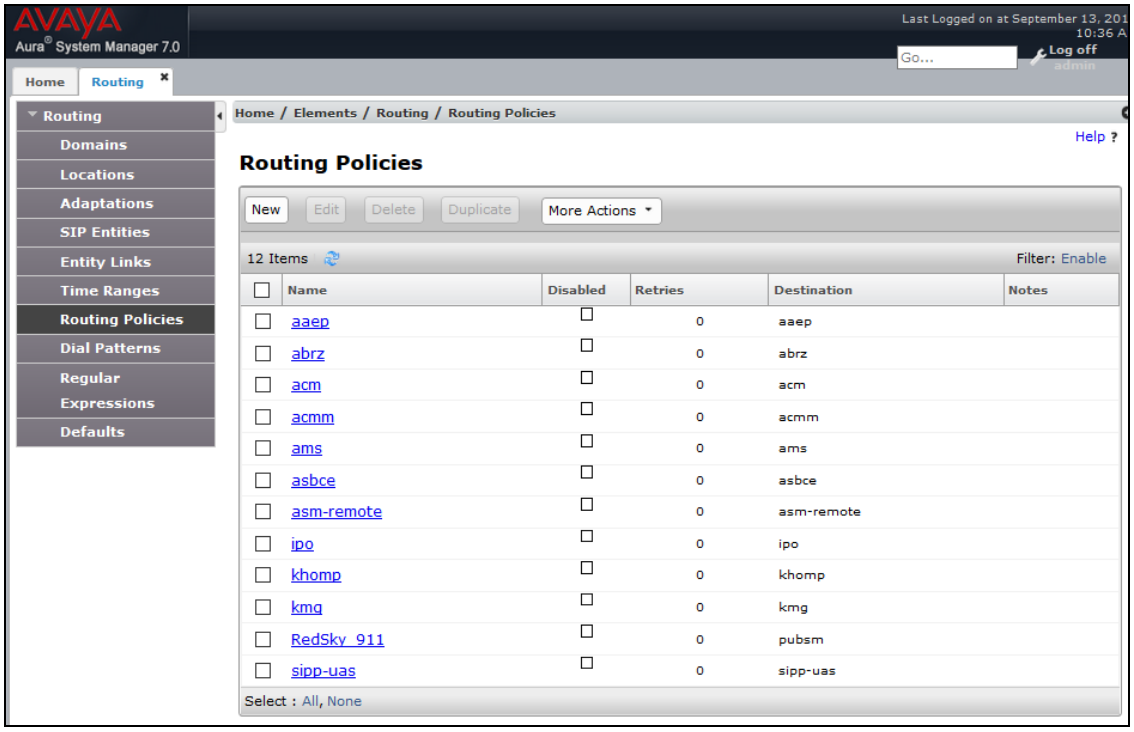
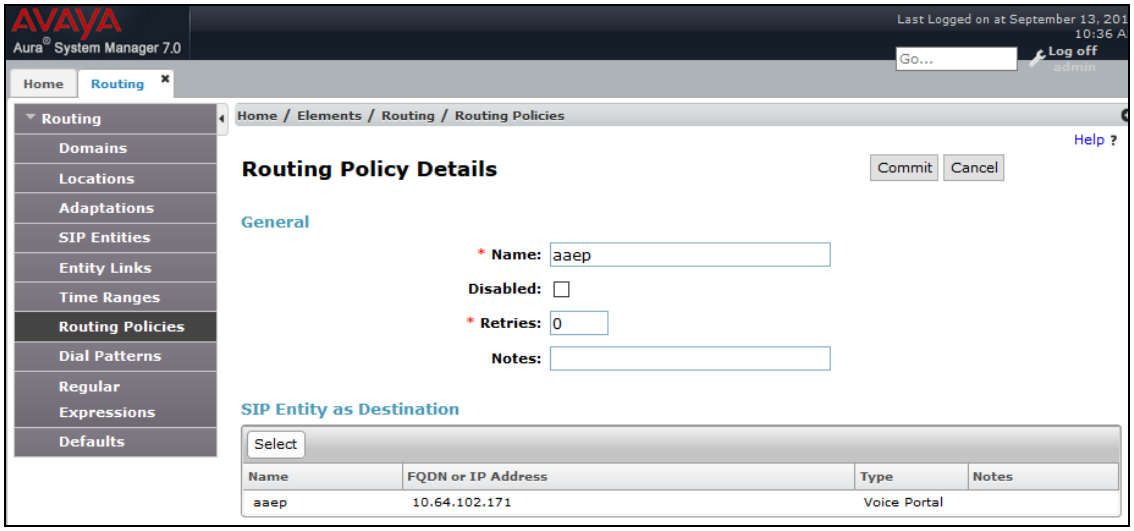
Click **New**. The **SIP Entity Details** screen is displayed. Enter a descriptive name to the **Name** field and the IP Address or Fully Qualified Domain Name of the Experience Portal to the **FQDN or IP Address** field. Select **Voice Portal** from the dropdown menu of the **Type** field. Set the **Location** and **Time Zone** fields to proper values.



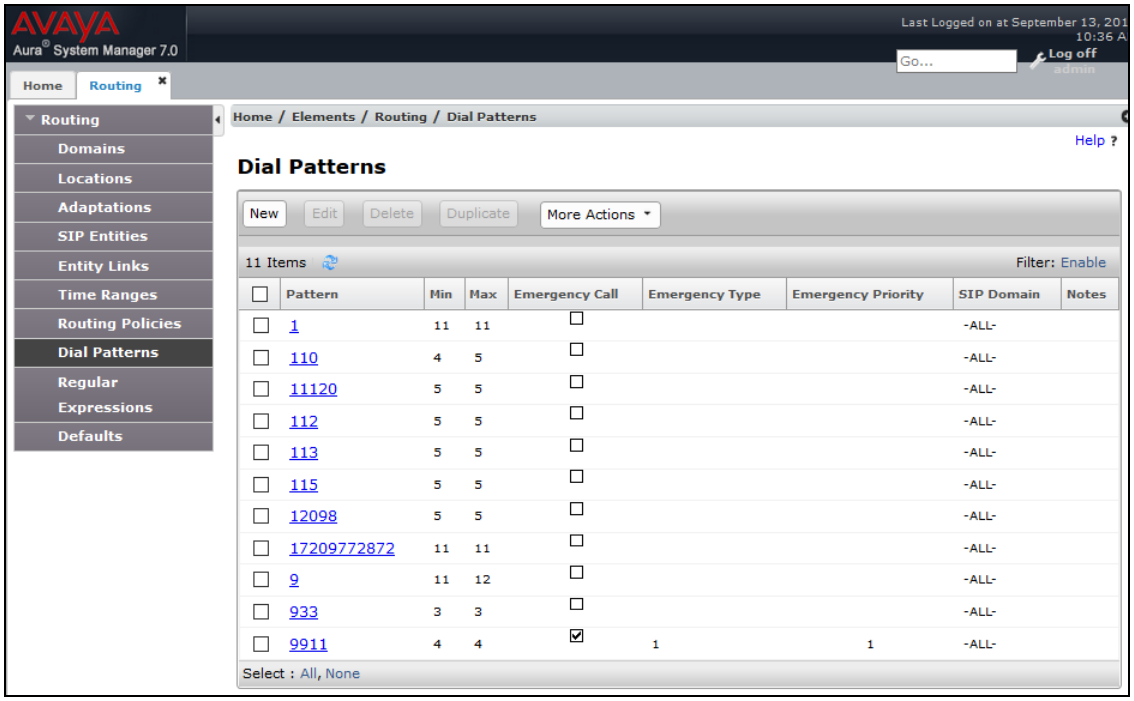
©2016 Avaya Inc. All Rights Reserved.

Step	Description
	Continuing on the same screen, scroll down to the bottom of the page, select **Add** under **Entity links**. • Set the **SIP Entity 1** field to **asm** which is the SIP entity for Session Manager. • Set the **Protocol** field to **TCP**. • Set the **SIP Entity 2** to the SIP Entity being configured. • Set the **Connection Policy** field to **trusted**. Click **Commit** to save changes. 

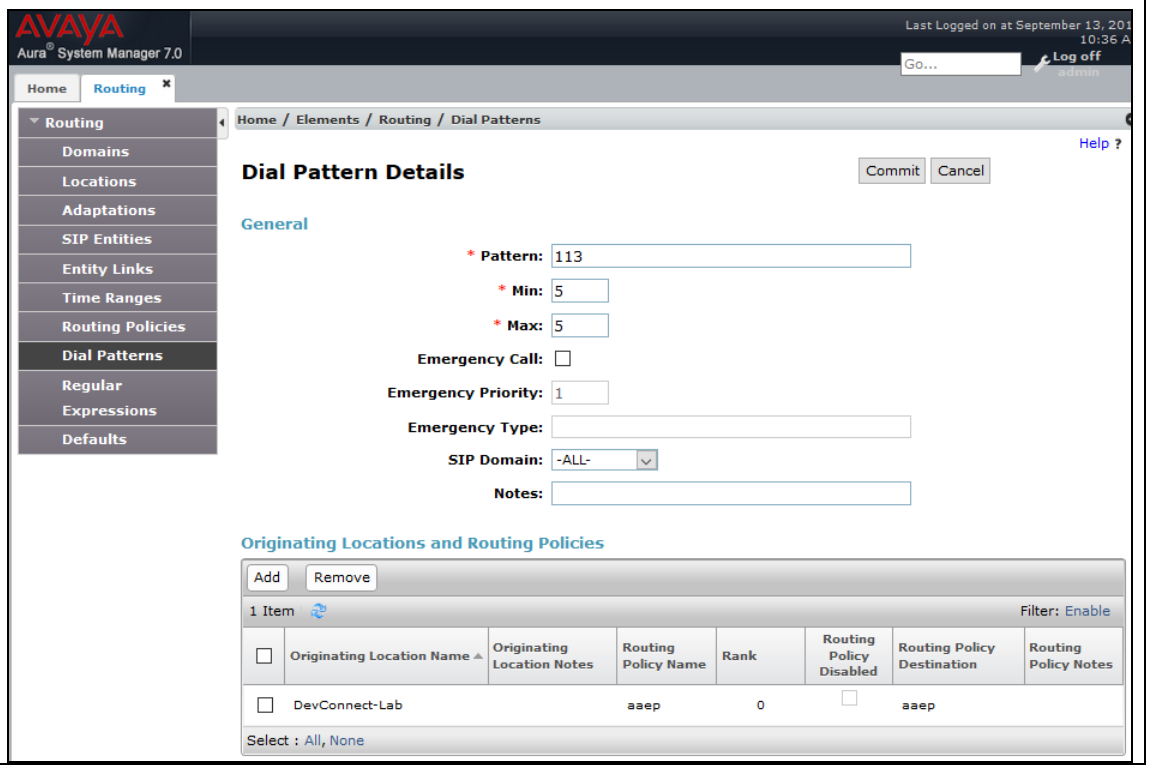
©2016 Avaya Inc. All Rights Reserved.

Step	Description
3.	**Configure Routing Policy** On the left pane, click **Routing Policies**. The **Routing Policies** screen is displayed.  Click **New**. The **Routing Policy Details** screen is displayed. Configure the following and click **Commit**. • Enter a descriptive name to the **Name** field. • Under **SIP Entity as Destination** section, click **Select.** A new window is displayed (not shown). Check box the SIP Entity configured in **Step 2**. Click **Select**. 

©2016 Avaya Inc. All Rights Reserved.

Step	Description
4.	**Configure Dial Pattern for Experience Portal** On the left pane, click **Dial Patterns**. The **Dial Patterns** screen is displayed. 

©2016 Avaya Inc. All Rights Reserved.

Step	Description
5.	Click **New**. The **Dial Pattern Details** screen is displayed. Configure the following and click **Commit**. • Set the **Pattern** field to **113**. • Set the **Min** and **Max** fields to **5** and **5**. • Set the **SIP Domain** field to **-ALL-**. • Under the **Originating Locations and Routing Policies** section, click **Add.** A new window is displayed (not shown). Select the **Routing Policy** configured in **Step 4** and then check the **Apply The Selected Routing Policies to All Originating Locations** checkbox. Click **Select.** • Click **Commit**. The Dial Pattern configuration directs all calls with 113xx destinations to Experience Portal. 

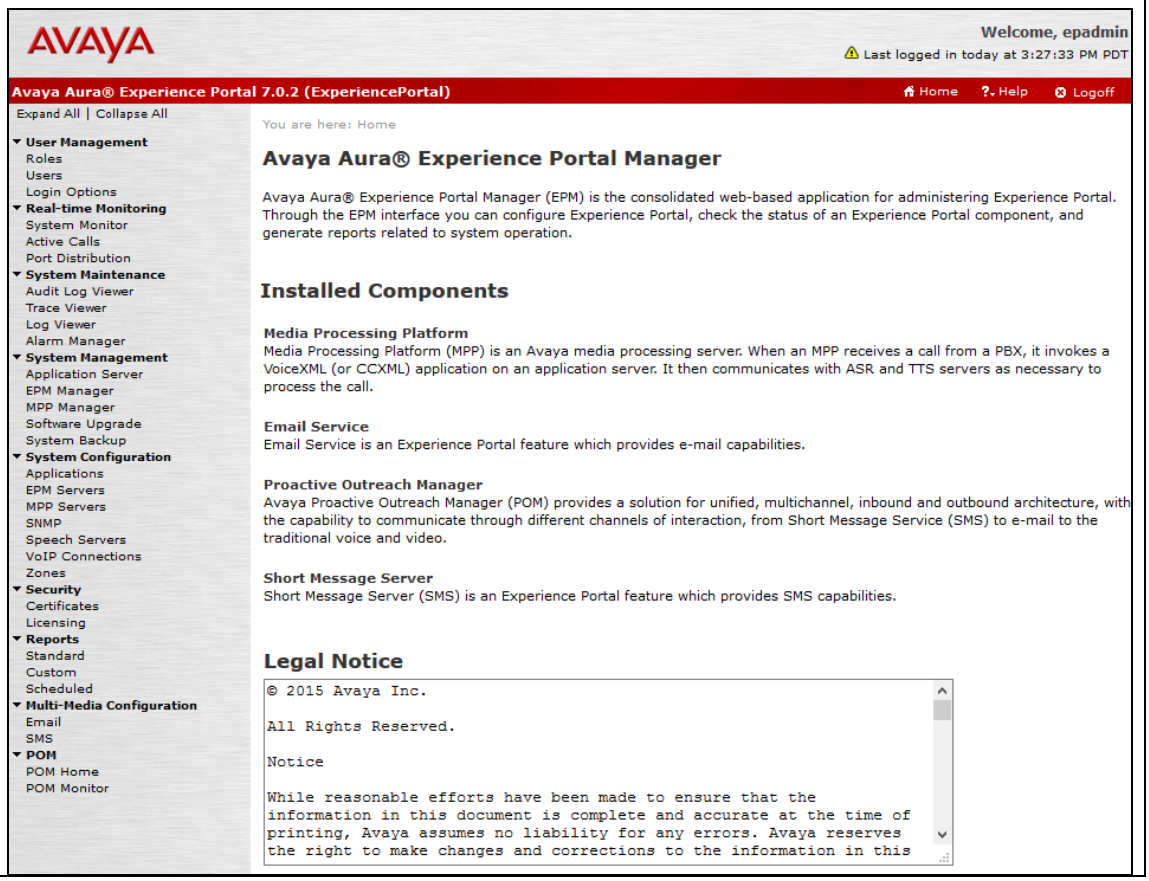
©2016 Avaya Inc. All Rights Reserved.

8. Configure Avaya Aura® Experience Portal

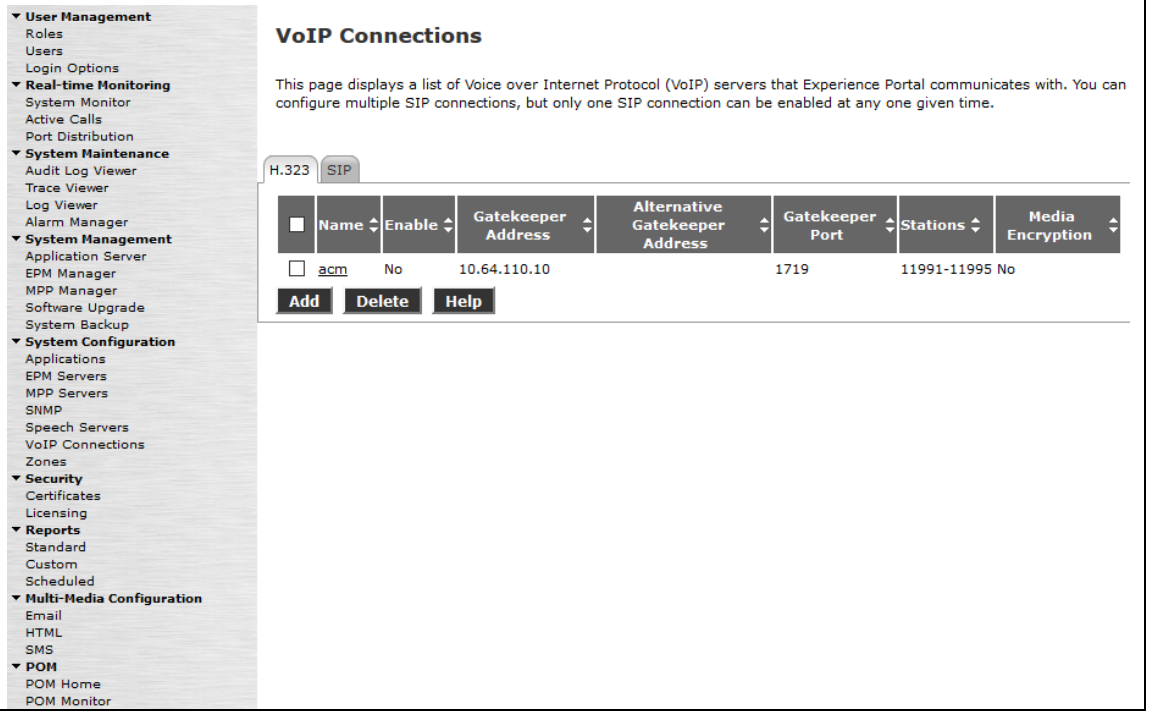
This section provides the steps to configure Experience Portal using the Experience Portal Manager (EPM) web interface to support the Virtual Hold solution.

The configuration procedures fall into the following areas:

- Launch Experience Portal Manager
- Configure VoIP Connections for SIP Configuration
- Configure Web Services Authentication Parameters
- Configure Applications for SIP Configuration

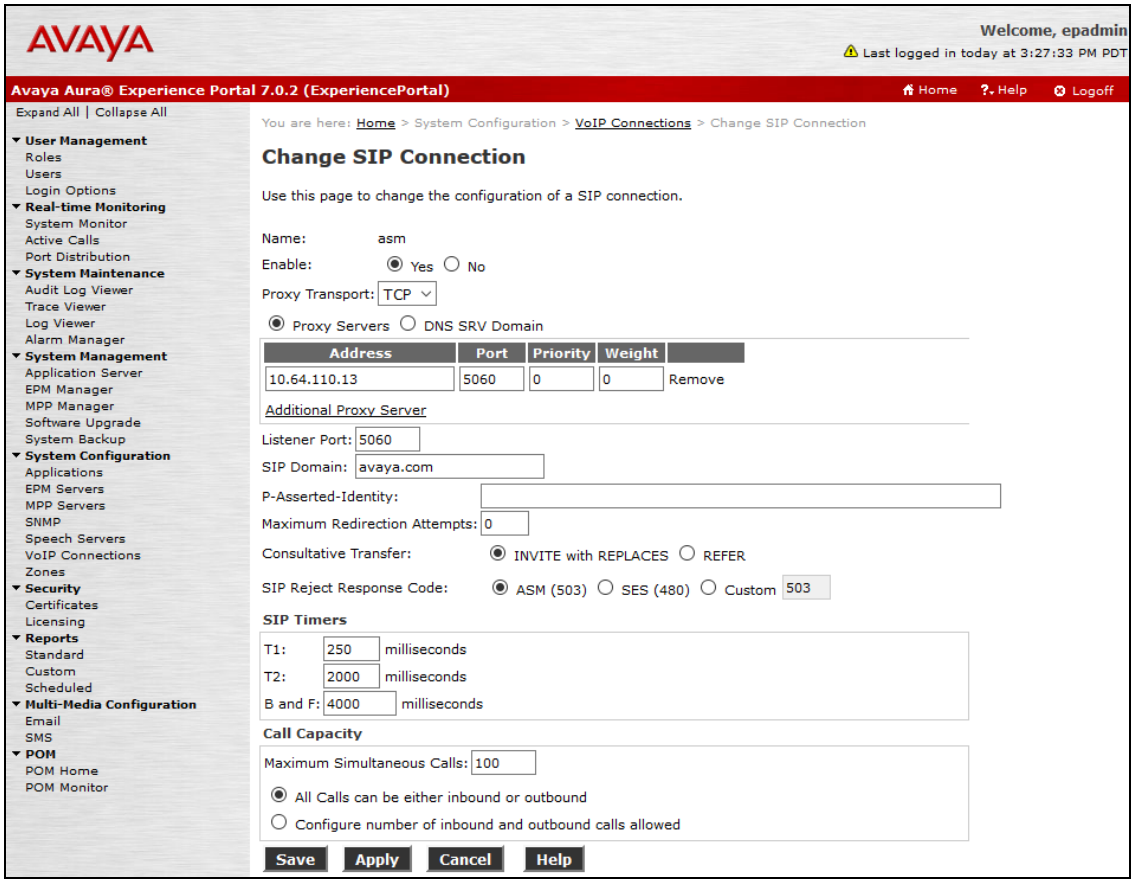
Step	Description
1.	**Launch Experience Portal Manager** Type in **http://<*ip-addr*>/** as the URL in a web browser, where **<*ip-addr*>** is the IP address of Experience Portal Manager. Log in with proper credentials. 

©2016 Avaya Inc. All Rights Reserved.

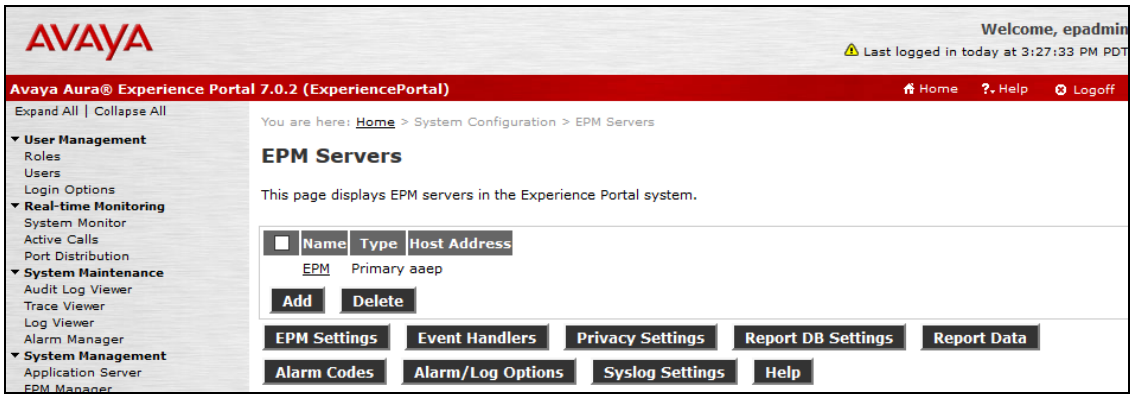
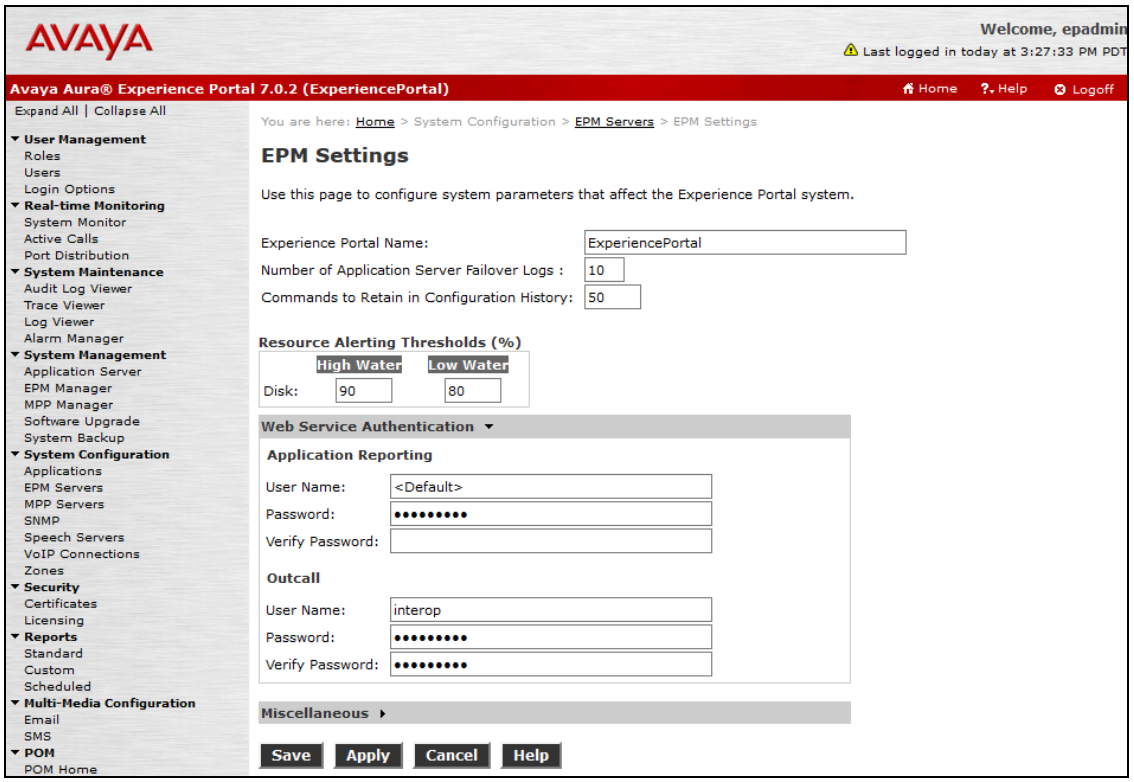
Step	Description
2.	**Configure VoIP Connections** On the left pane, click **VoIP Connections**. 

©2016 Avaya Inc. All Rights Reserved.

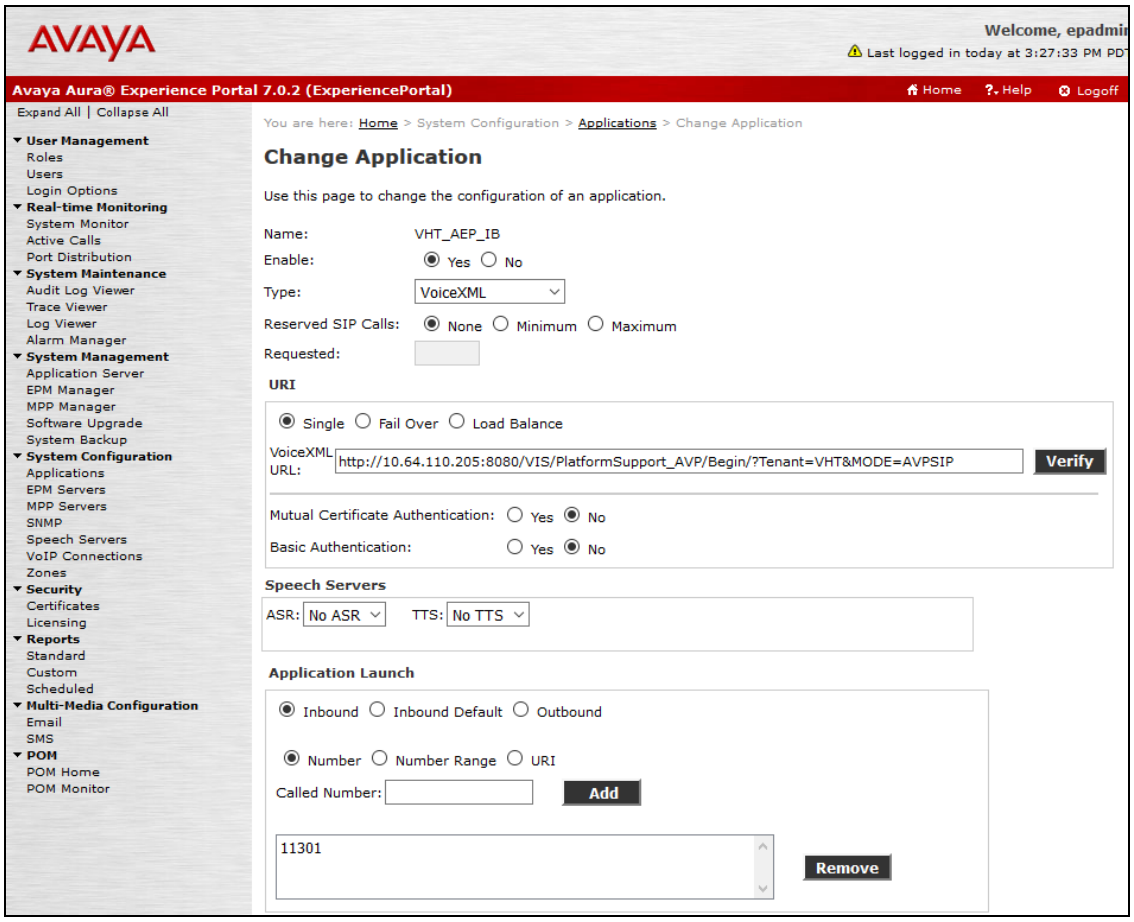
Step	Description
3.	**Configure SIP Connections** To add a **SIP Connection**, click **SIP** tab (not shown) on the **VoIP Connections** page and then click **Add**. • Fill in **Name**. • Set **Proxy Transport** to **TCP**. • In the **Address** and **Port** fields, fill the the IP address and Port of Session Manager. • In the **SIP Domain** field, type in the domain pre-configured in Session Manager. • Set the **Maximum Simultaneous Calls** based on the license for Experience Portal. • The rest of the values are left at **default values**. • Click **Save.**



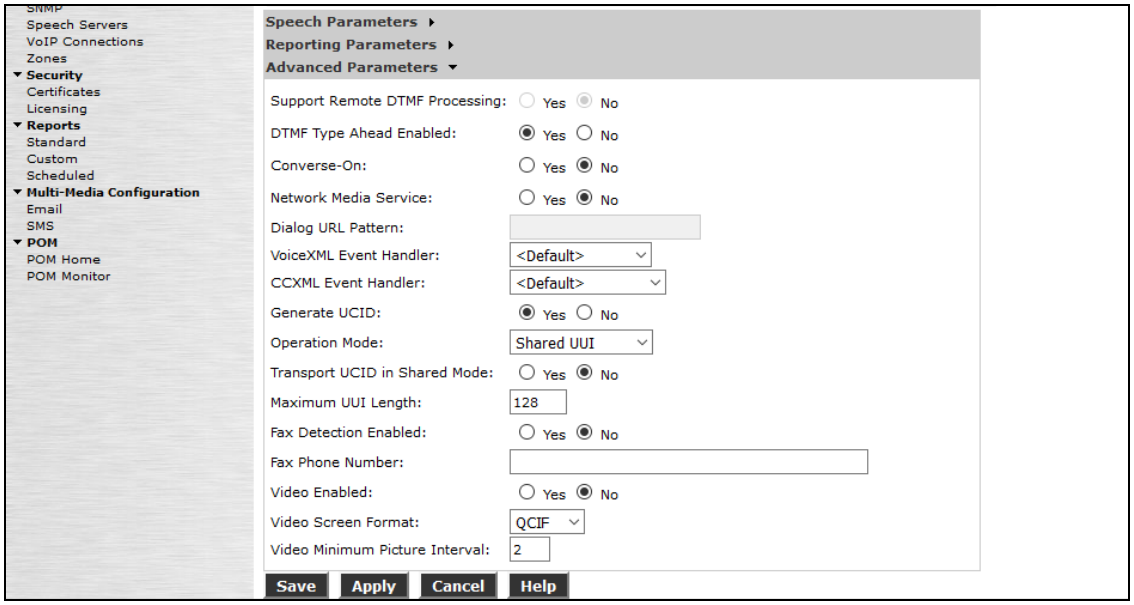
©2016 Avaya Inc. All Rights Reserved.

Step	Description
4.	**Configure Web Service Authentication Parameters** On the left pane, click **System Configuration → EPM Servers** (not shown). The **EPM Servers** screen is displayed.  Click **EPM Settings**. The **EPM Settings** screen is displayed. Under the **Web Service Authentication** section, **Outcall** sub-section, type in **Username, Password** and **Verify Password**. This information will be used by Virtual Hold to initiate an outbound call. Click **Save**. 

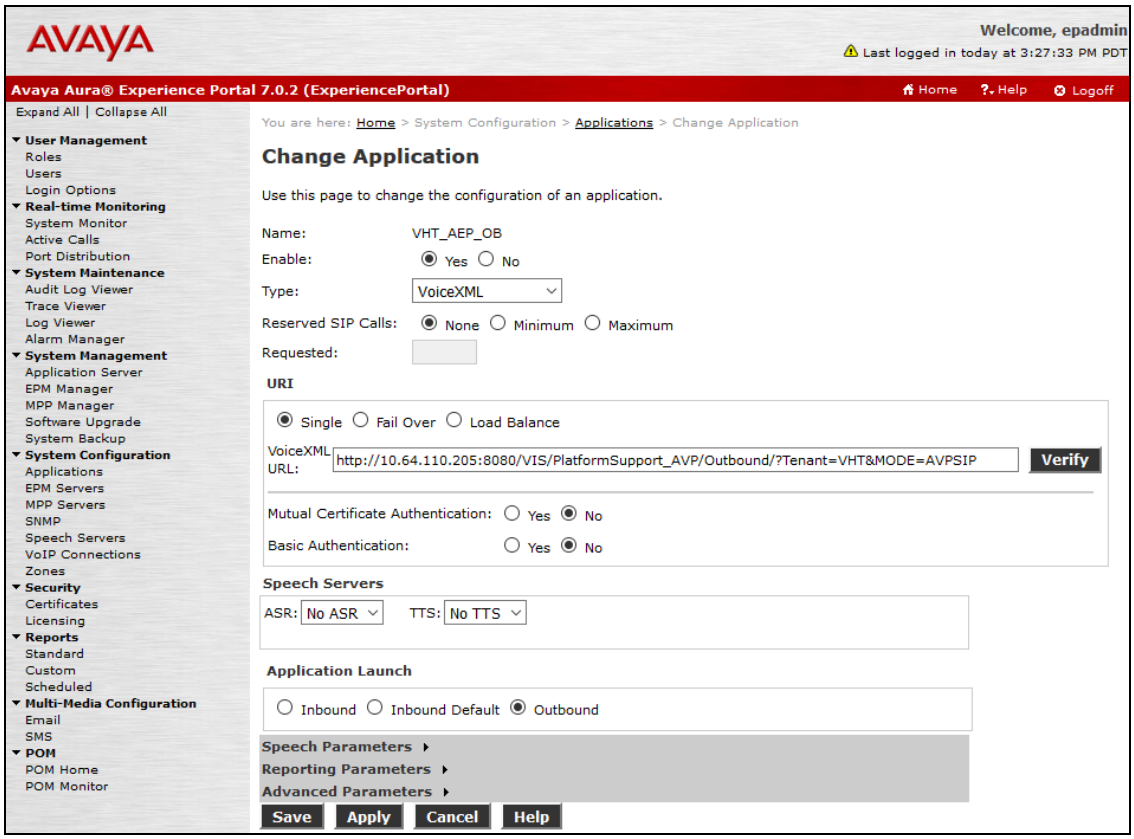
©2016 Avaya Inc. All Rights Reserved.

Step	Description
5.	**Configure Inbound Application** On the left pane, navigate to **System Configuration → Applications**. The **Application screen** is displayed (not shown). Click **Add**. The **Add Application** screen is displayed. The screen capture displays the configured application during the compliance testing. • Fill in **Name**. • For **Type**, select **VoiceXML** from the drop down menu. • Fill in **VoiceXML URL**: http://10.64.110.205:8080/VIS/PlatformSupport_AVP/Begin/?Tenant=VHT&MODE=AVPSIP, where **10.64.110.205** and **8080** are the IP Address and Tomcat Port of the Virtual Hold Server. • Set the **Called Number** field to **11301,** and click **Add**. Calls to this number will be routed to Experience Portal via Session Manager.  Continue on the next page.

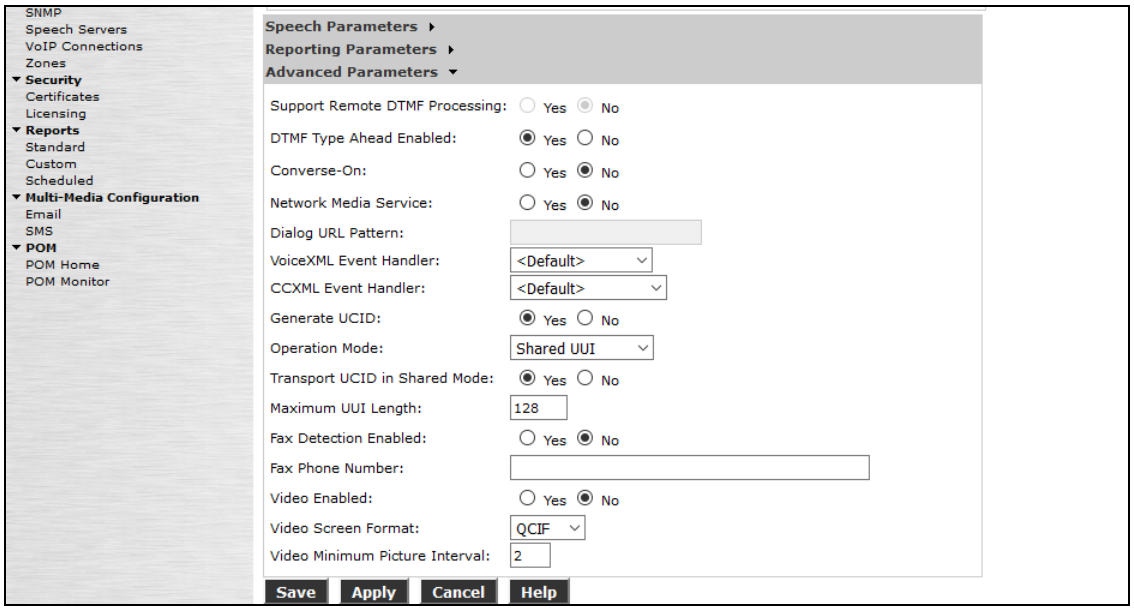
©2016 Avaya Inc. All Rights Reserved.

Step	Description
	Click **Advanced Parameters** to expand. • Set the **Generate UCID** field to **Yes**. • Set the **Operation Mode** field to **Shared UUI**. • Click **Save**. 

©2016 Avaya Inc. All Rights Reserved.

Step	Description
6.	**Configure Outbound Application** On the Application screen (not shown), click **Add**. The **Add Application** screen is displayed. The screen capture displays the configured application during the compliance testing. • Fill in **Name**. • For **Type**, select **VoiceXML** from the drop down menu. • Fill in **VoiceXML URL**: http://10.64.110.205:8080/VIS/PlatformSupport_AVP/Outbound/?Tenant=VHT&MODE=AVPSIP, where **10.64.110.205** and **8080** are the IP Address and Tomcat Port of the Virtual Hold Server • Set the **Application Launch** section to **Outbound**.  Continue on the next page.

©2016 Avaya Inc. All Rights Reserved.

Step	Description
	Click **Advanced Parameters** to expand. • Set the **Generate UCID** field to **Yes**. • Set the **Operation Mode** field to **Shared UUI**. • Set the **Transport UCID in Shared Mode** field to **Yes**. • Click **Save**. 

©2016 Avaya Inc. All Rights Reserved.

9. Configure Virtual Hold

The Virtual Hold software was run under Windows 2012 Server R2 64-bit operating system. Configuration of Virtual Hold is done through the following elements:

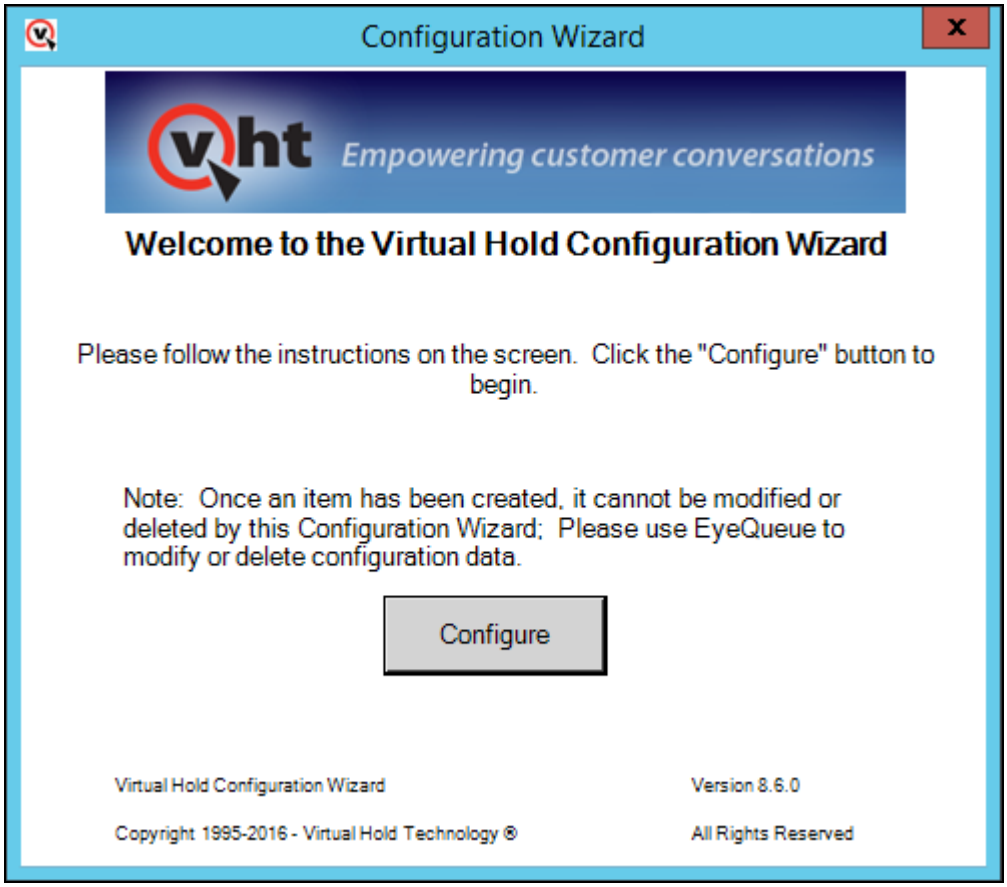
- VHT Configuration Wizard
- SQL Server Management Studio
- Genesys Configuration Manager
- Text based configuration files

The configuration procedures fall into the following areas:

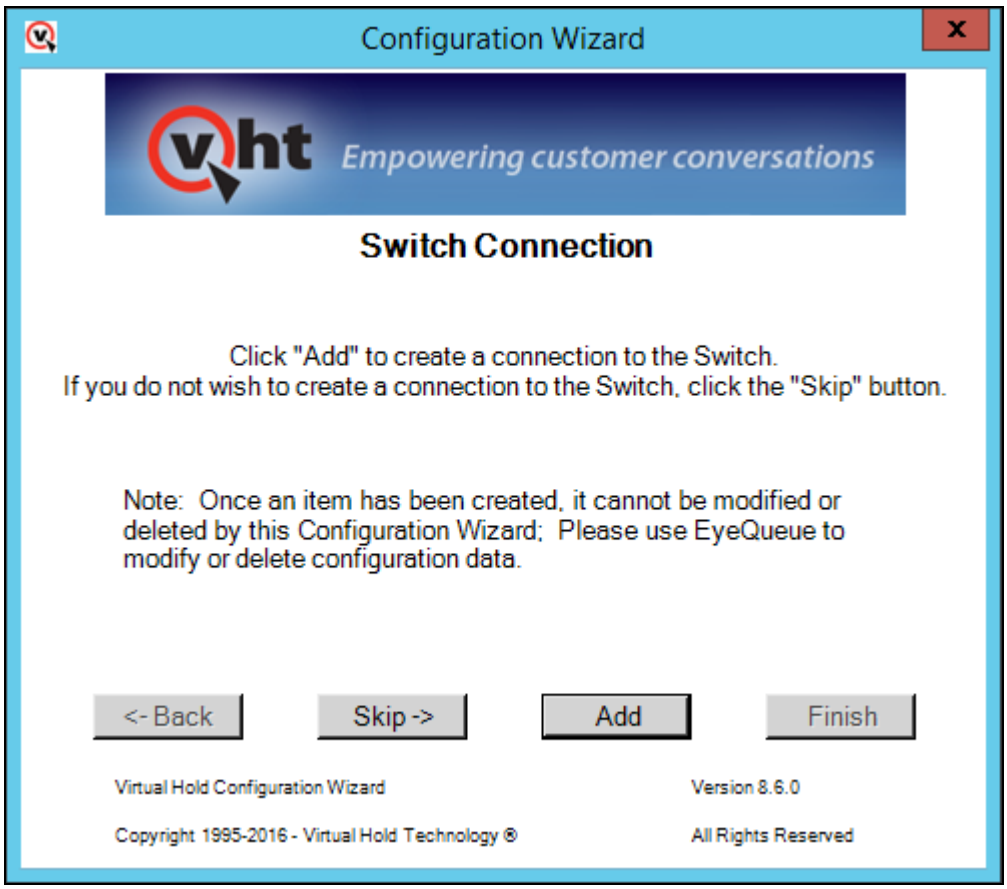
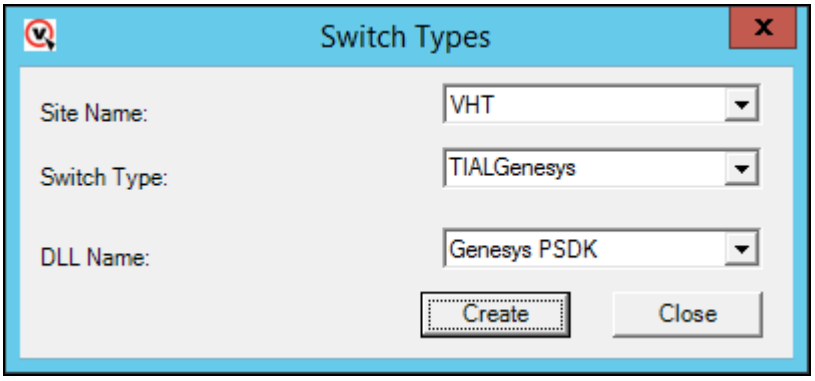
- Using VHT Configuration Wizard
  - Launch VHT Configuration Wizard
  - Configure Switch Connection
  - Configure Genesys CTI T-Server Connection
  - Configure IVR Servers
  - Configure Queues
  - Configure Callback and Holding Queues
  - Configure Incoming Extensions
  - Configure Phone Number Configuration
- Using SQL Server Management Studio
  - Configure Segment Variables
- Using Genesys Configuration Manager
  - Configure Route Points
  - Configure Hunt Groups
  - Configure Agent Extensions
  - Configure ACD Queues
  - Configure Connection Parameters
- Using text files
  - OutboundIVR_AVP.xml
  - toolkit.properties

Step	Description
1.	Log in the Virtual Hold server with proper credentials. Open **VHT Configuration Wizard** by navigating to **Start →All Programs → Virtual Hold Technology → Configuration → VHT Configuration Wizard**.

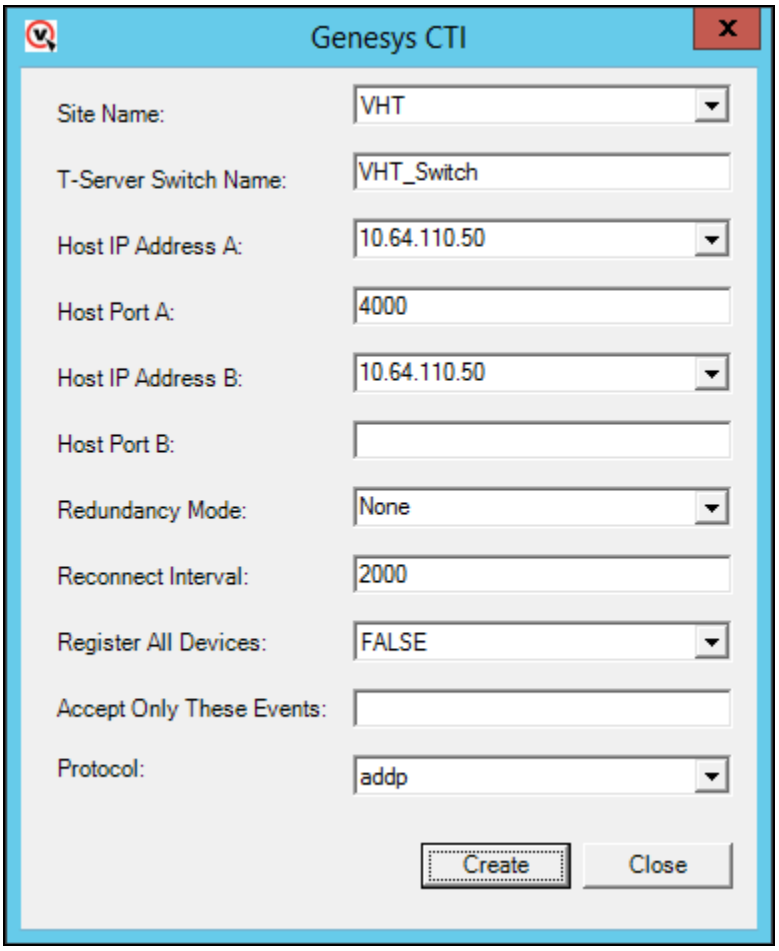
©2016 Avaya Inc. All Rights Reserved.

Step	Description
2.	On the **Welcome to the Virtual Hold Configuration Wizard** page, click **Configure.** 

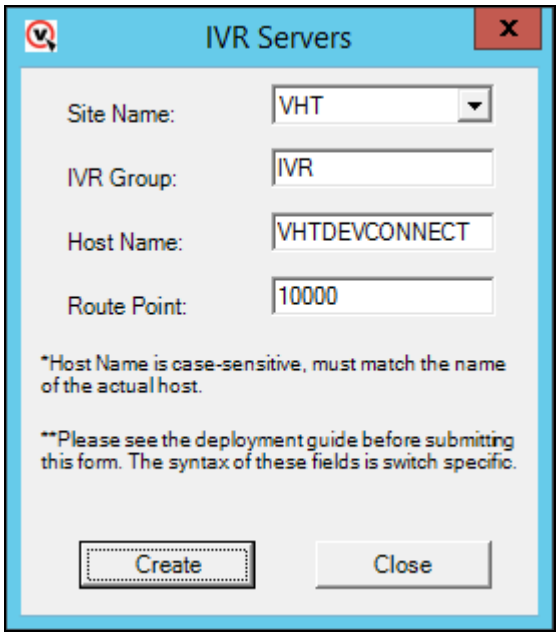
©2016 Avaya Inc. All Rights Reserved.

Step	Description
3.	On the **Switch Connection** page, click **Add**. 
4.	The **Switch Types** window is displayed with the **Site Name** already populated. Select **TIALGenesys** from the drop-down menu of the **Switch Type** field. Click **Create**. 

©2016 Avaya Inc. All Rights Reserved.

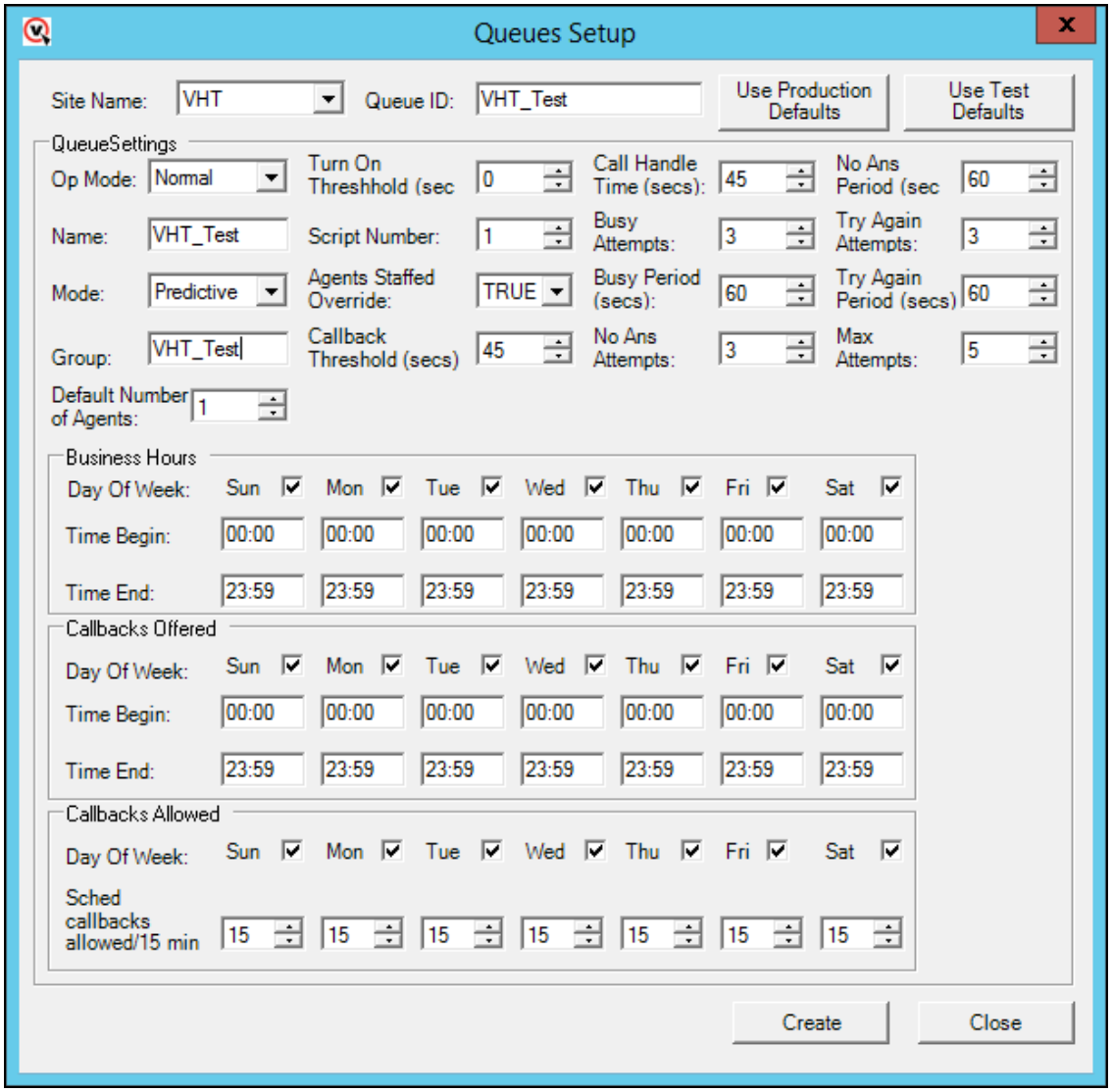
Step	Description
5.	The **Genesys CTI** window is displayed. • Set the **T-Server Switch Name** field to the Genesys T-Server switch name • Set the **Host IP Address A** field to the IP address of Genesys server • Set the **Host Port A** to **4000** • Set the **Host IP Address B** field to the IP address of Genesys server • Set the **Register All Devices** field to **FALSE** • Set the **Protocol** field to **addp** Click **Create** followed by **Close**. 

©2016 Avaya Inc. All Rights Reserved.

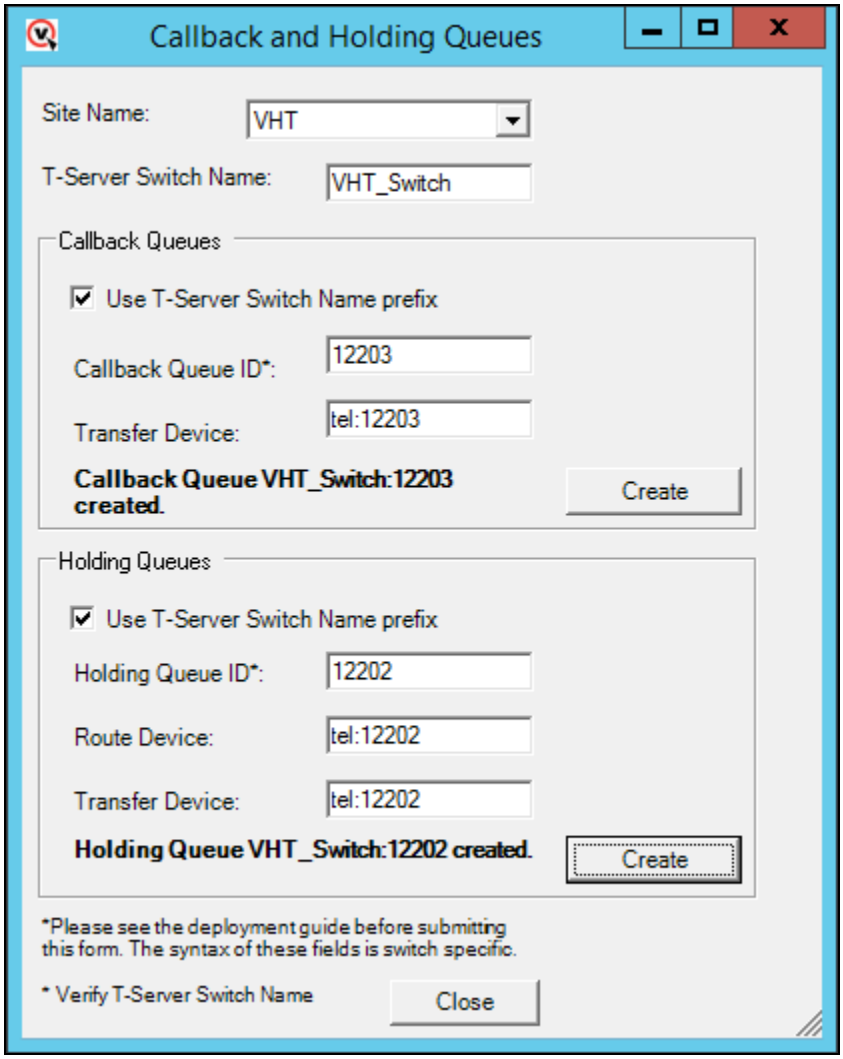
Step	Description
6.	Skip the **Agent Groups** and **Agents** page (not shown). On the **IVR Servers** page, click **Add** (not shown). Keep the default values and click **Create** followed by **Close**. 

©2016 Avaya Inc. All Rights Reserved.

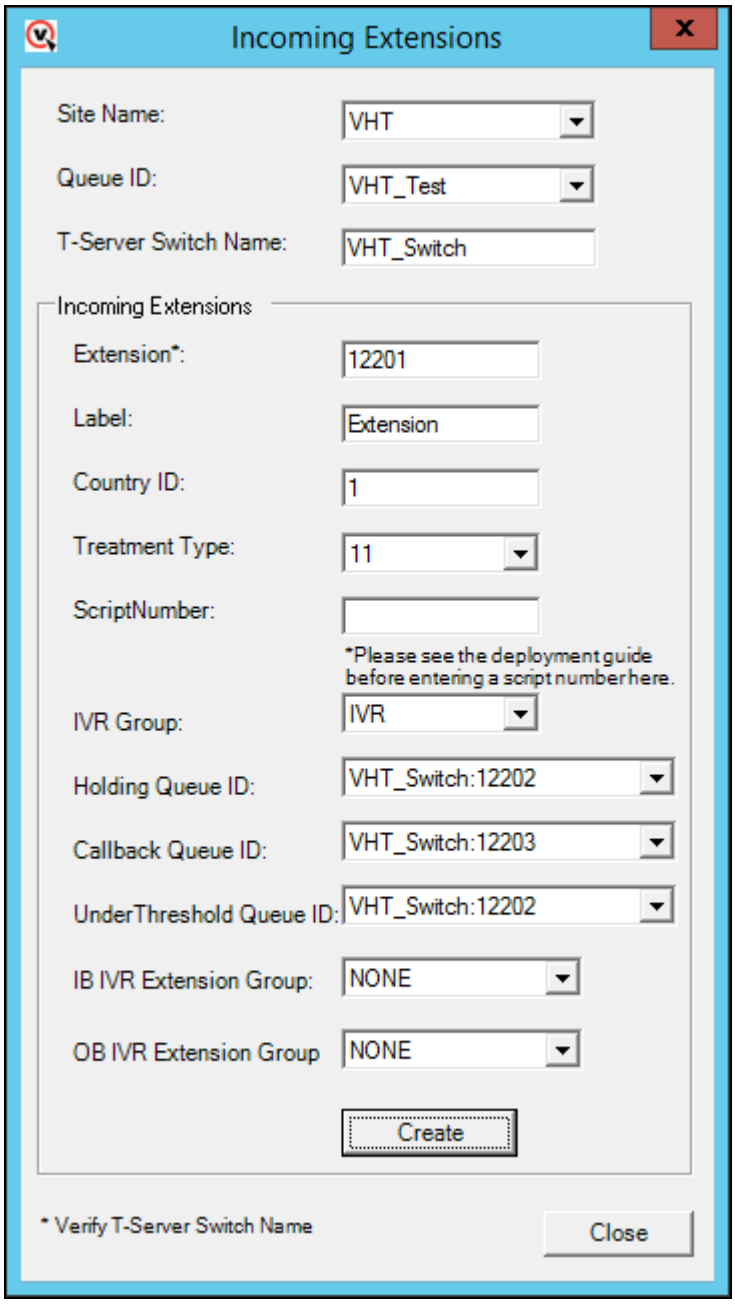
Step	Description
7.	Skip the **IVR Extensions** page and click **Add** on the **Queues** page (not shown). The **Queues Setup** window is displayed. Enter a group name in the **Group** field (for reporting purpose) and accept the defaults value for all other fields. Click **Create** followed by **Close**.



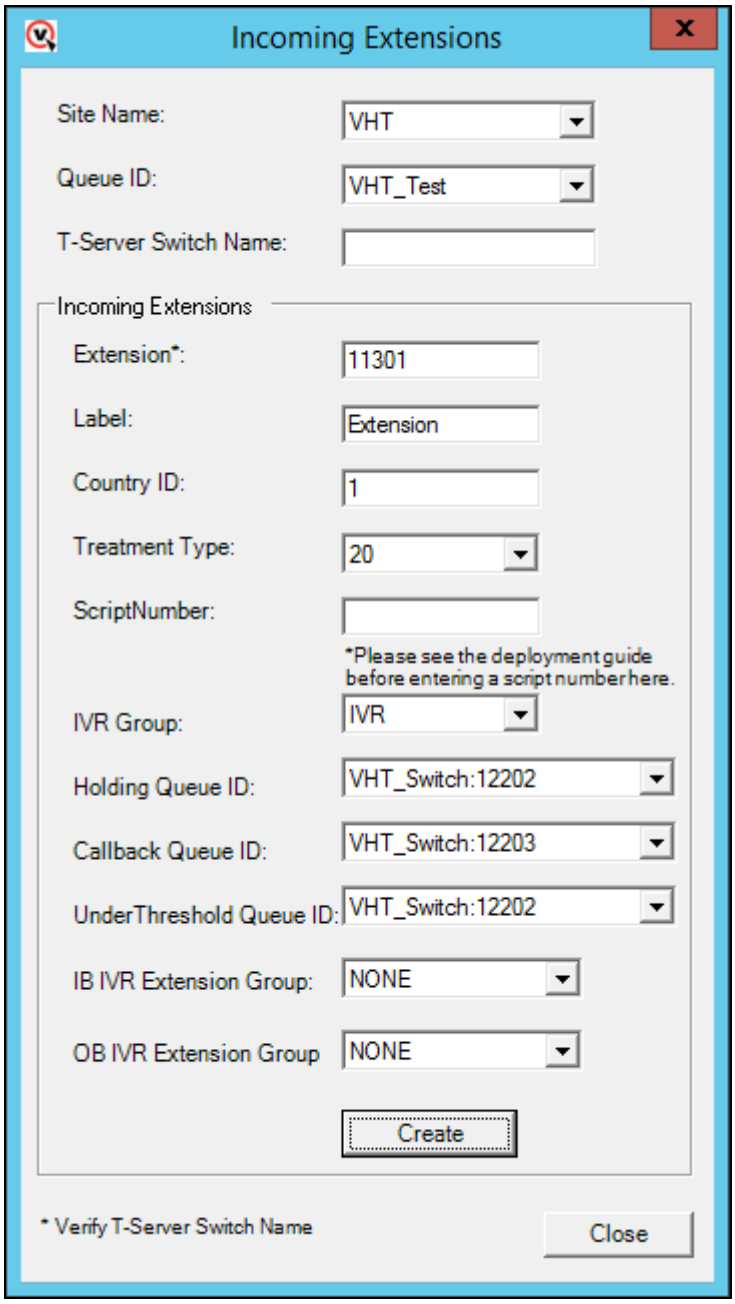
©2016 Avaya Inc. All Rights Reserved.

Step	Description
8.	On the **Callback** and **Holding Queues** page, click **Add** (not shown). The **Callback and Holding Queues** window is displayed. In the **Callback Queues** section, enter the Callback VDN configured in **Section 5**, **Step 6** (**12203**) in the **Callback Queue ID** field. Enter the same value with the string **tel:** appended to it in the **Transfer Device** field. Click **Create**. In the **Holding Queues** section, enter the Holding VDN configured in **Section 5**, **Step 6** (**12202**) in the **Holding Queue ID** field. Enter the same value with the string **tel:** appended to it in the **Route Device** field and the **Transfer Device** field. Click **Create** followed by **Close**. 

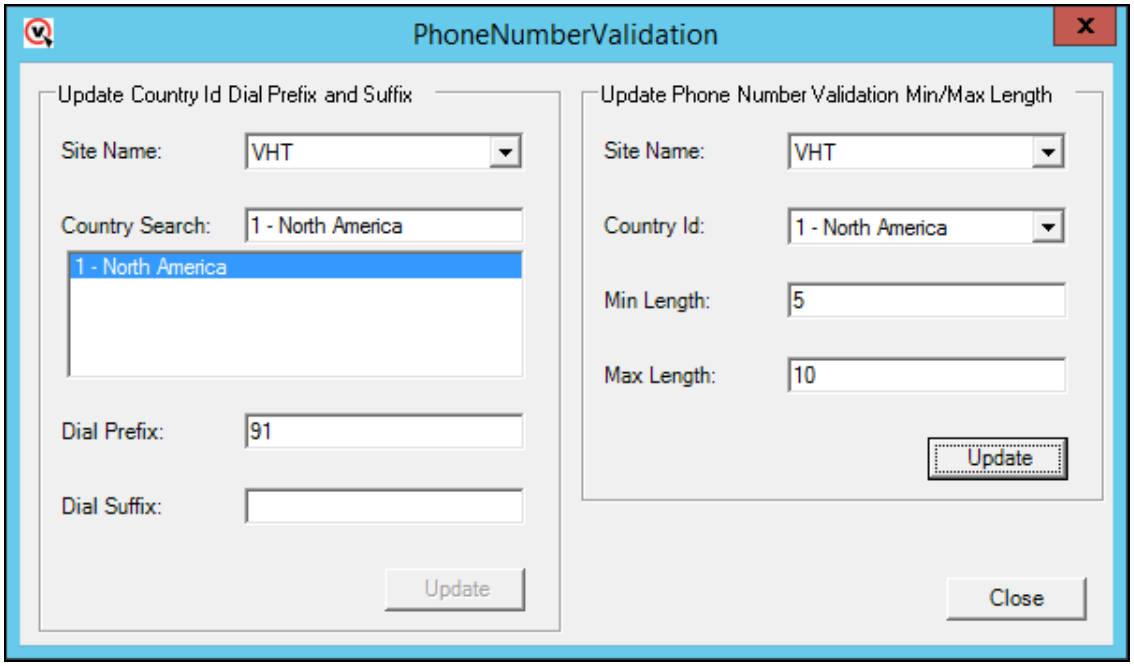
©2016 Avaya Inc. All Rights Reserved.

Step	Description
9.	On the **Incoming Extensions** page, click **Add** (not shown). The **Incoming Extensions** window is displayed. Enter the Entry VDN configured in **Section 5**, **Step 6** (**12201**) in the **Extension** field and **11** in the **Treatment Type** field. Click **Create**.  Continue on the next page.

©2016 Avaya Inc. All Rights Reserved.

Step	Description
	Repeat the step and enter the extension associated with the Experience Portal inbound application, configured in **Section 8**, **Step 5** (**11301**), in the **Extension** field and **20** in the **Treatment Type** field. Click **Create** followed by **Close**. 

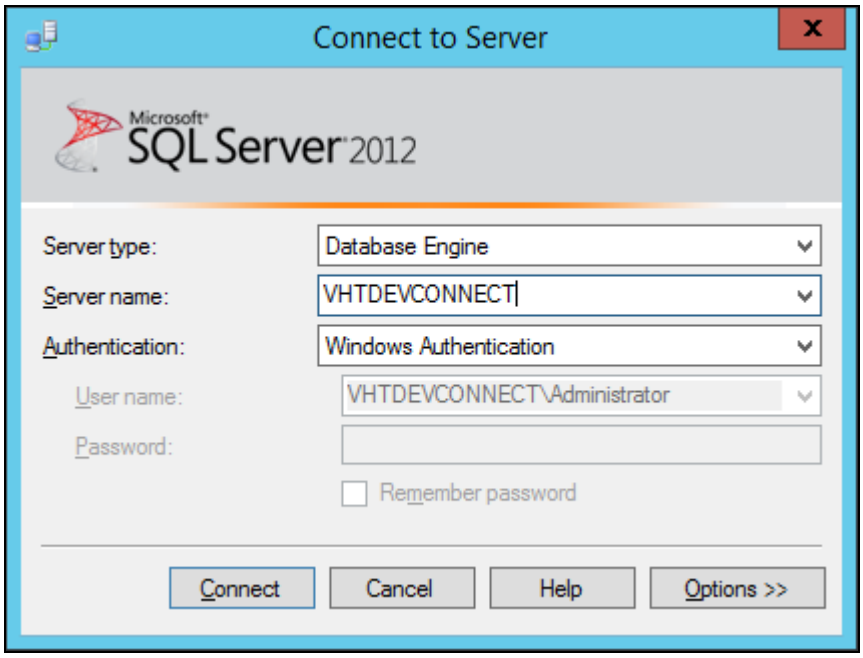
©2016 Avaya Inc. All Rights Reserved.

Step	Description
10.	Skip the **Incoming Application** page. On the **Phone Number Configuration** page, click **add** (not shown). The **PhoneNumberValidation** window is displayed. From the drop-down menu of the **Country Search** field select **1 – North America**. Enter **91** in the **Dial Prefix** field which allows out bound calls to use the ARS (Automatic Route Selection) capability in Communication Manager. Enter **5** in the **Min Length** field and **10** in the **Max Length** field. Click **Update** in the right pane followed by **Close**. 

©2016 Avaya Inc. All Rights Reserved.

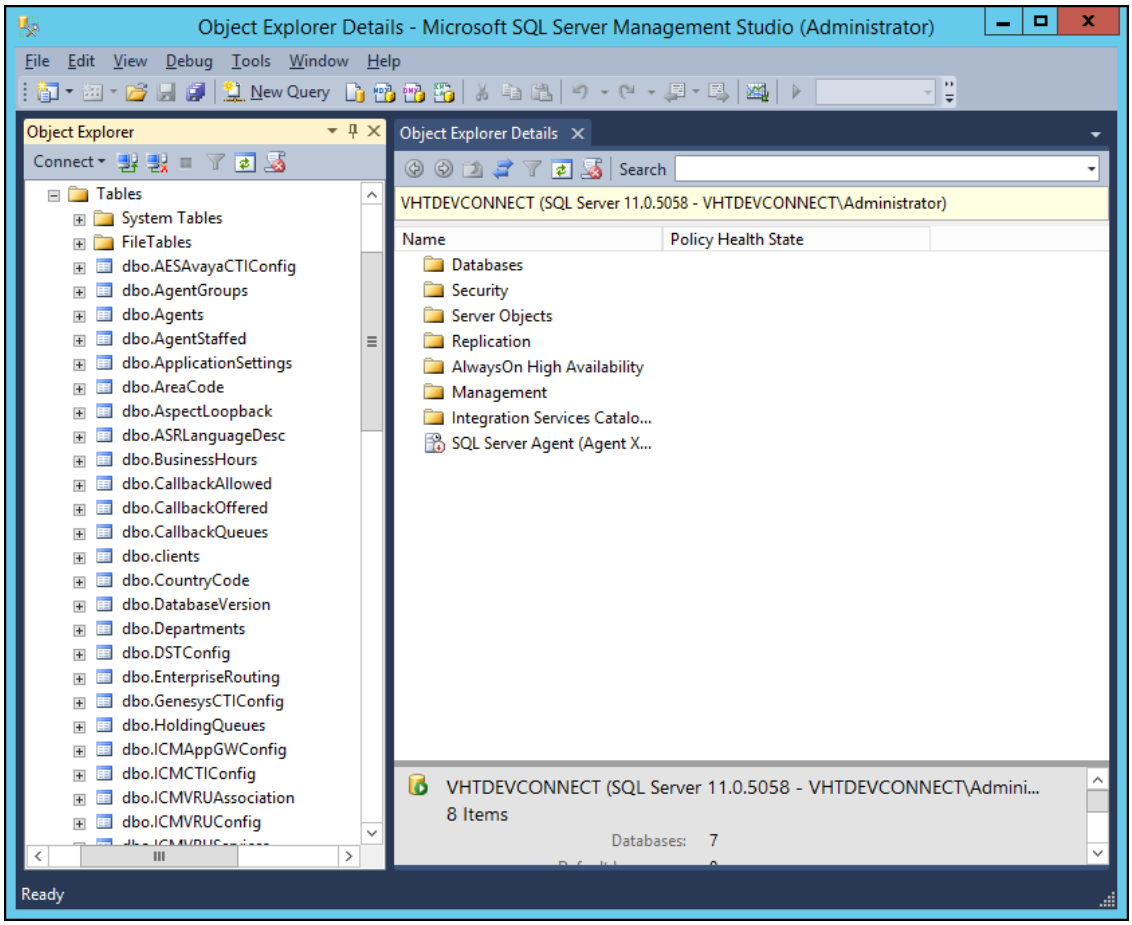
Step	Description
11.	The **Finished** page is displayed. Click **Finish**.

©2016 Avaya Inc. All Rights Reserved.

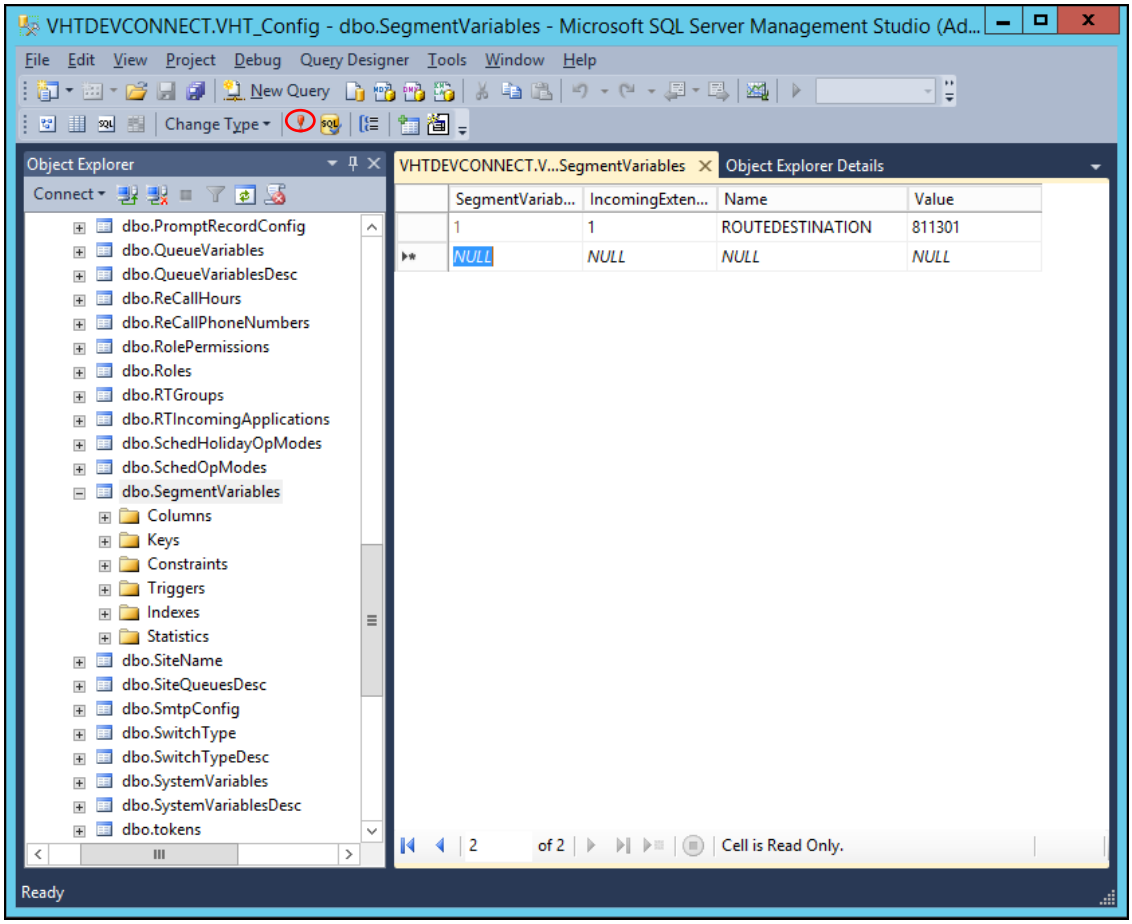
Step	Description
12.	On the Virtual Hold server, open **SQL Server Management Studio** by navigating to **Start →All Programs → Microsoft SQL Server 2012 → SQL Server Management Studio**. The **Connect to Server** window is displayed. Click **Connect**. 

©2016 Avaya Inc. All Rights Reserved.

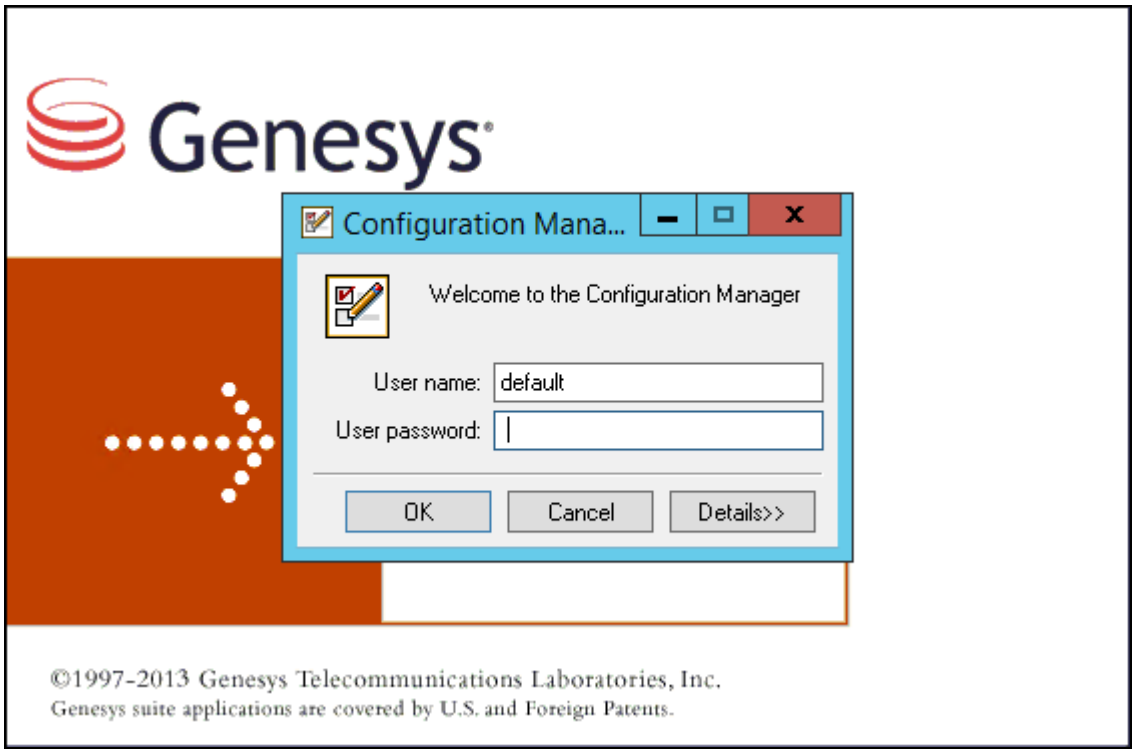
Step	Description
13.	From the left pane under **Object Explorer**, navigate to **<Server Hostname>→ Databases → VHT_Config → Tables** where the **<Server Hostname>** is the hostname of the database server.



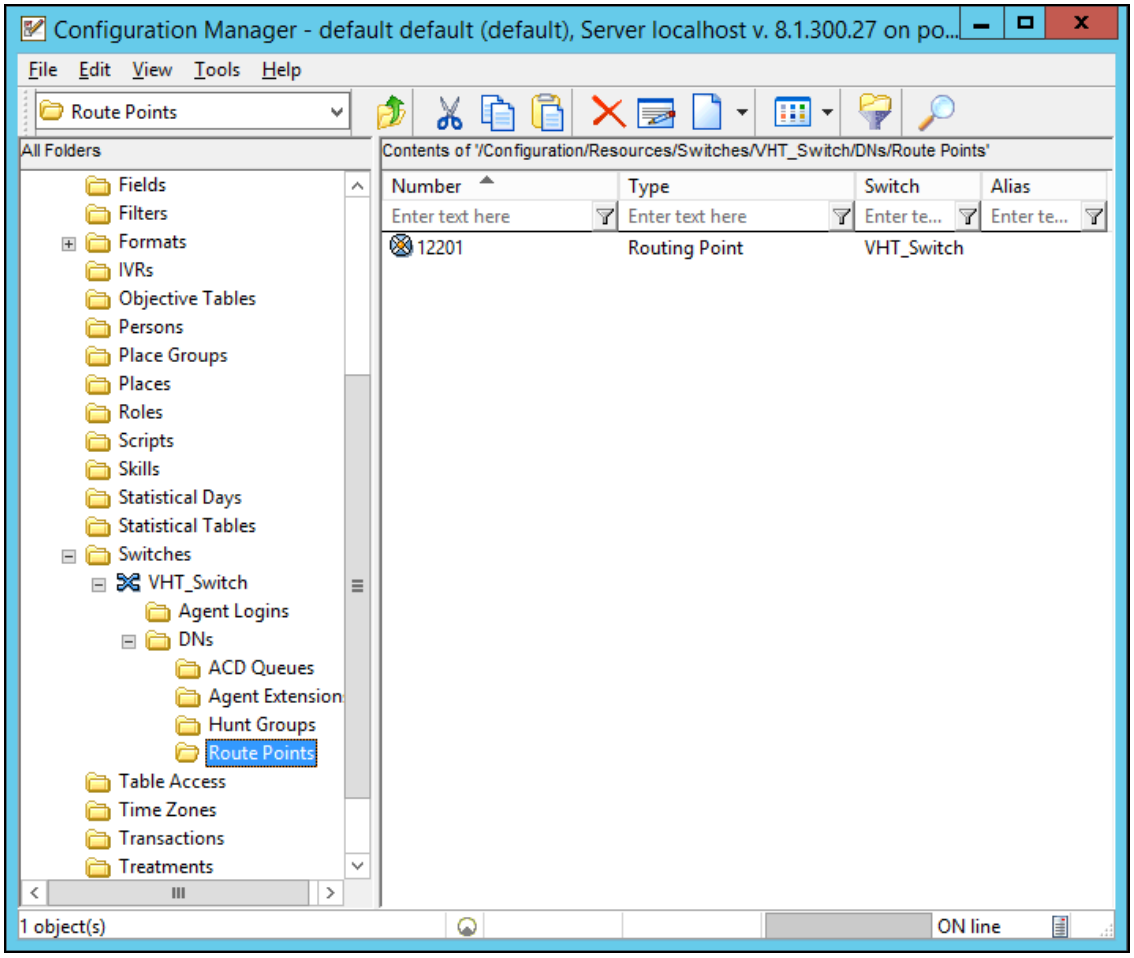
©2016 Avaya Inc. All Rights Reserved.

Step	Description
14.	An entry has to be created in the **SegmentVariables** table to map an Entry VDN as an incoming extension (See **Section 9**, **Step 9**) to a route destination. Right click **dbo.SegmentVariables** in the left pane and click **Edit Top 200 Rows** (not shown). Enter the **Incoming Extension Id** assigned to the Entry VDN (**1**) in the **IncomingExtensionId** field. The **Incoming Extension Id** can be found in the **IncomingExtension** table (not shown). Enter **ROUTEDESTINATION** in the **Name** field and **8** followed by the extension associated with the Experience Portal inbound application, configured in **Section 8**, **Step 5** (**811301**), in the **Value** field. Click the **Execute SQL** (not shown) button in the **Tools** bar. **Note:** 8 in the **Value** field is the AAR routing prefix configured in Communication Manager. From the Virtual Hold server, navigate to **Start → Control Panel → Administrative Tools → Services**, restart the **VHT_QueueManager** service. 

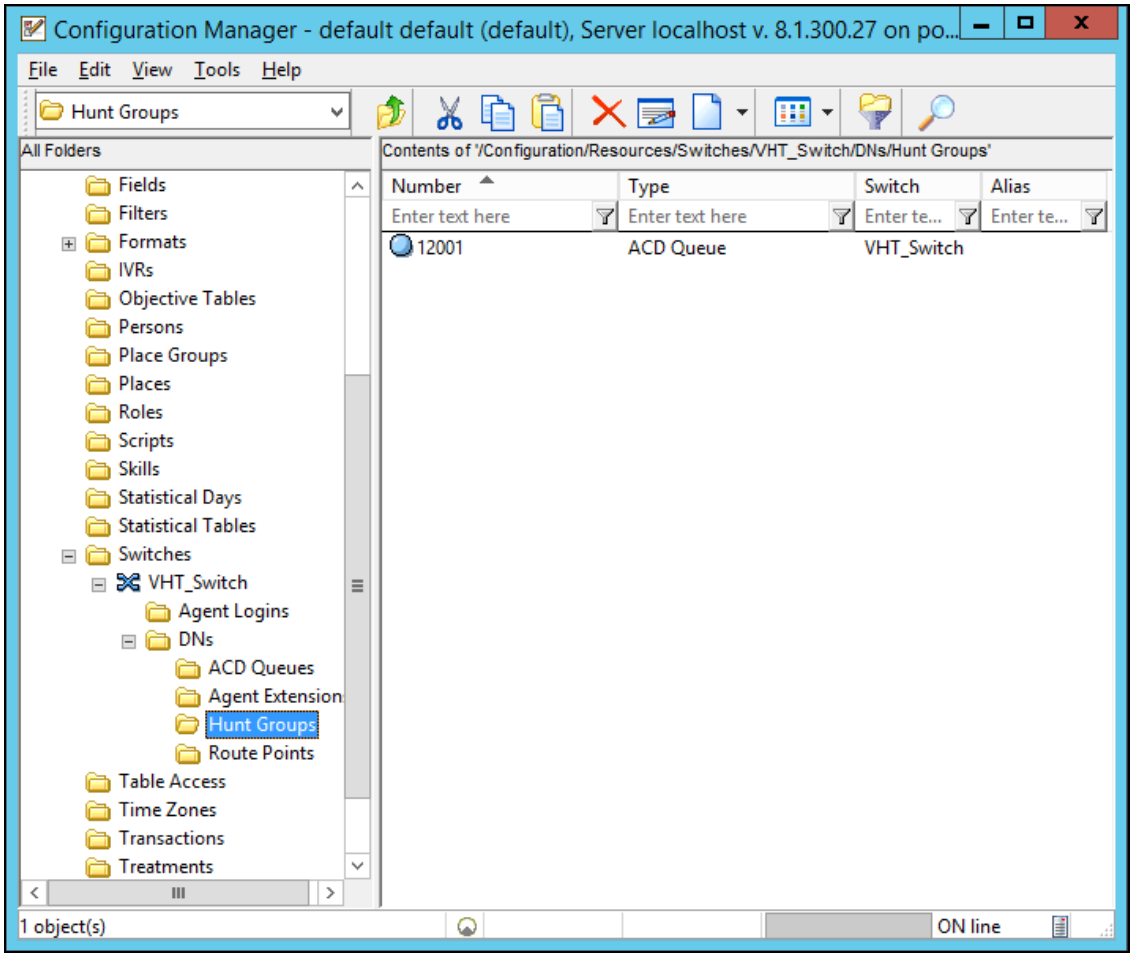
©2016 Avaya Inc. All Rights Reserved.

Step	Description
15.	On the Virtual Hold server, open **Genesys Configuration Manager** by navigating to **"C:\Program Files (x86)\GCTI\Configuration Manager\sce.exe"**. The **Genesys Configuration Manager** window is displayed. Enter proper credentials and click **OK**. 

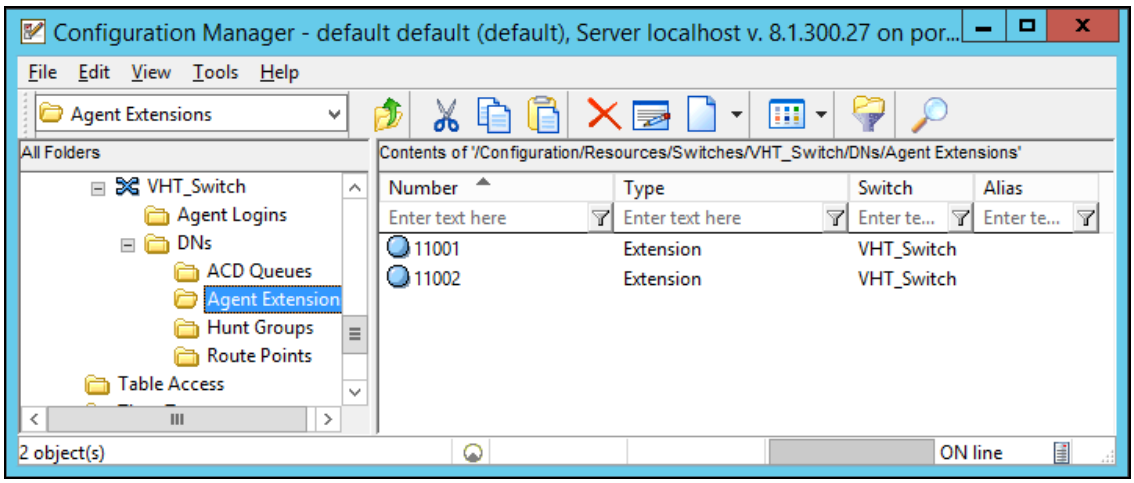
©2016 Avaya Inc. All Rights Reserved.

Step	Description
16.	From the left pane, navigate to **Configuration → Resources → Switches → VHT_Switch → DNs → Route Points**. Right click **Route Points** and click **New → DN**. Enter the Entry VDN configured in **Section 5**, **Step 6** (**12201**) in the **Number** field and select **Routing Point** for the **Type** field. Click **OK**. 

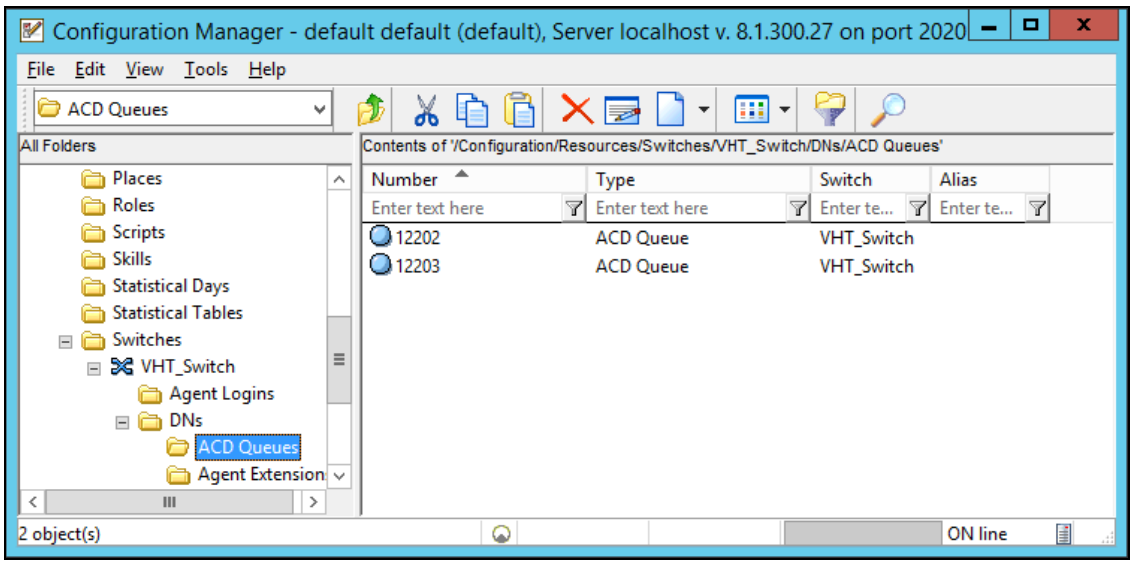
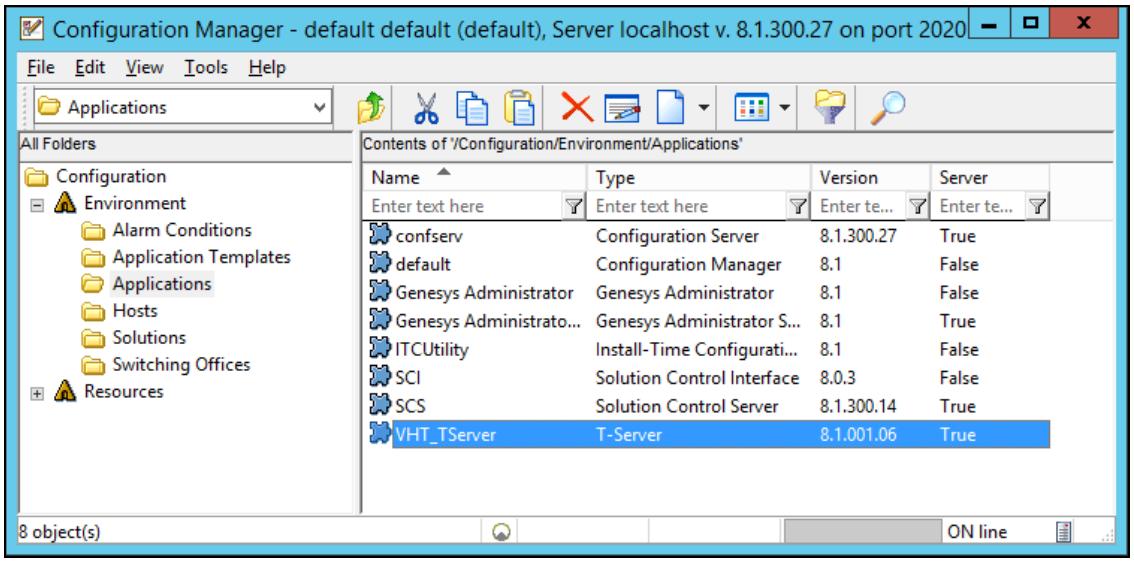
©2016 Avaya Inc. All Rights Reserved.

Step	Description
17.	From the left pane, navigate to **Configuration → Resources → Switches → VHT_Switch → DNs → Hunt Groups**. Right click **Hunt Groups** and click **New → DN**. Enter the Hunt Group extensions configured in **Section 5**, **Step 4** (**12001**) in the **Number** field and select **ACD Queue** for the **Type** field. Click **OK**. 

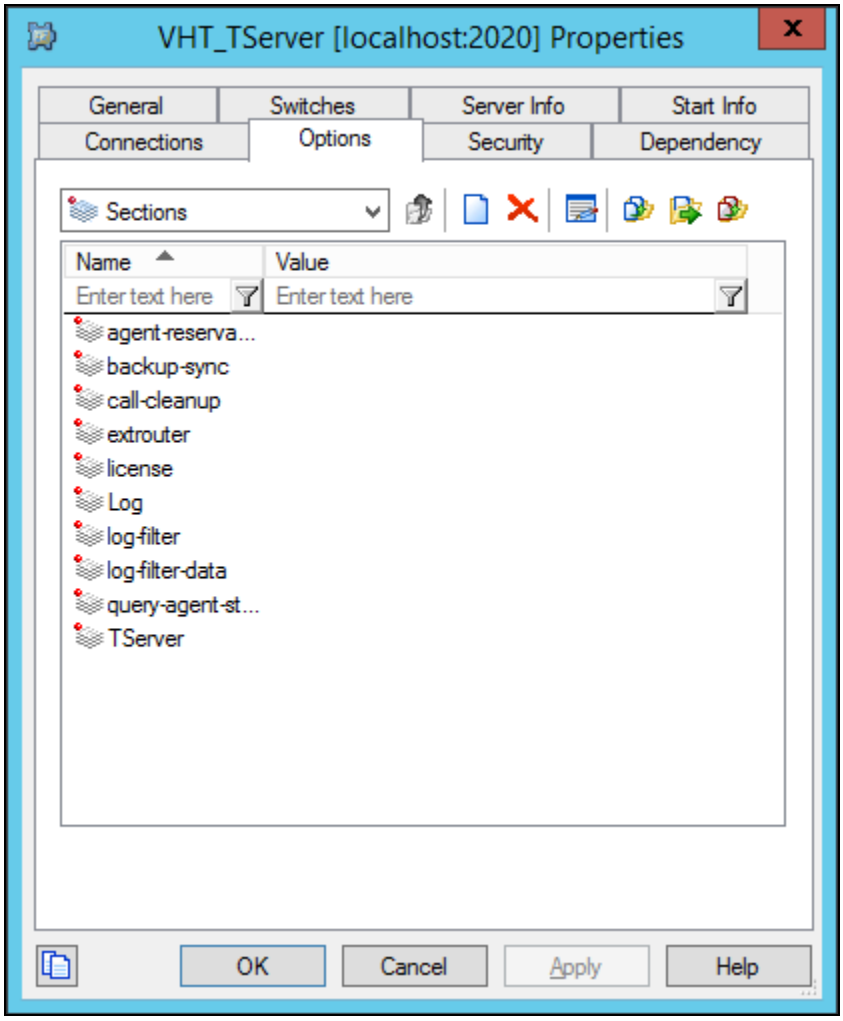
©2016 Avaya Inc. All Rights Reserved.

Step	Description
18.	From the left pane, navigate to **Configuration → Resources → Switches → VHT_Switch → DNs → Agent Extensions**. Right click **Agent Extensions** and click **New → DN**. Enter the first station extension configured in **Section 5**, **Step 4** (**11001**) in the **Number** field and select **Extension** for the **Type** field. Click **OK**. Repeat the procedure for the second station extension configured in **Section 5**, **Step 4** (**11002**). The screenshot below shows the two station extensions added. 

©2016 Avaya Inc. All Rights Reserved.

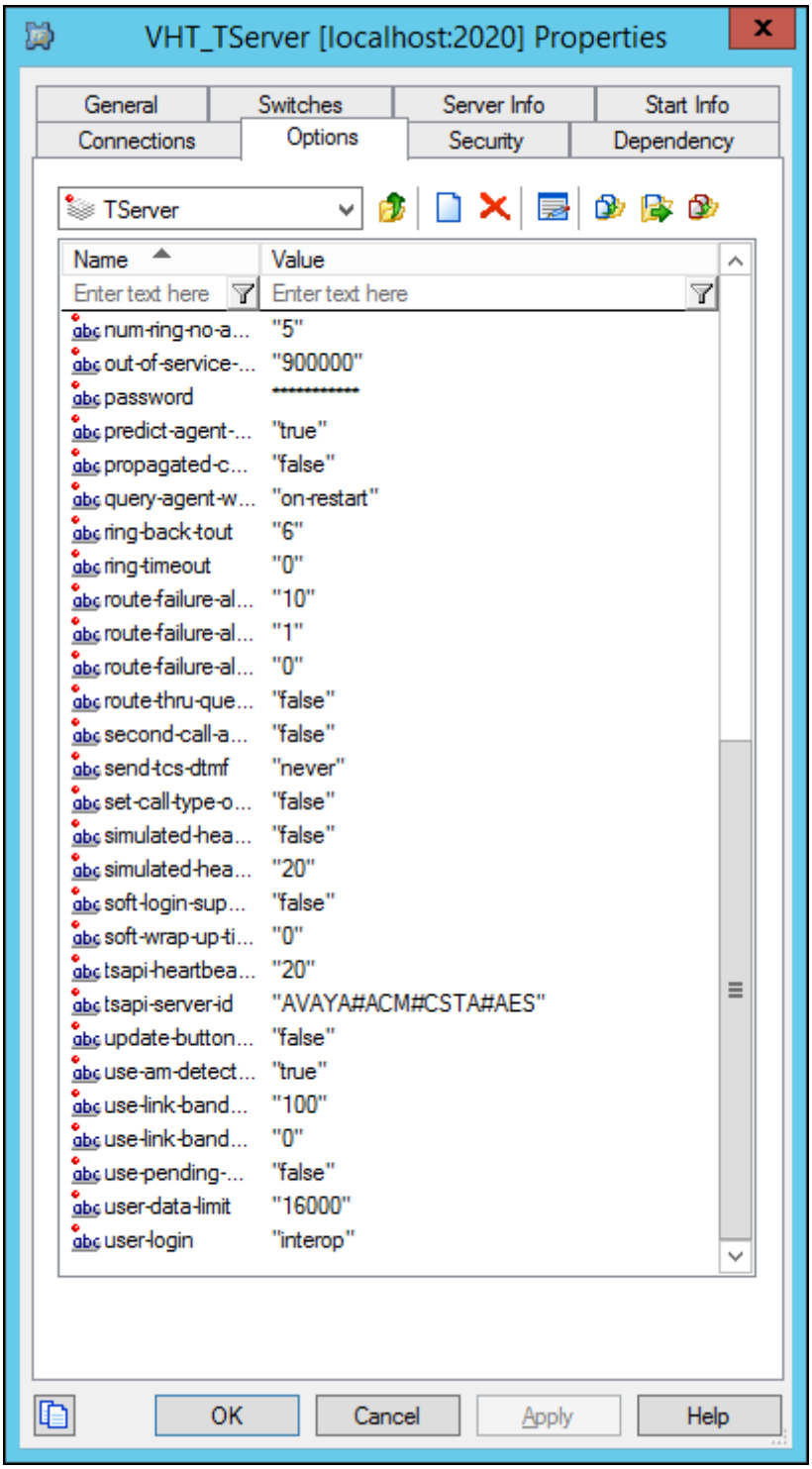
Step	Description
19.	From the left pane, navigate to **Configuration → Resources → Switches → VHT_Switch → DNs → ACD Queues**. Right click **ACD Queues** and click **New → DN**. Enter the Routing VDN configured in **Section 5**, **Step 6** in the **Number** field and select **ACD Queue** for the **Type** field. Click **OK**. Repeat the procedure for Callback VDN configured in **Section 5**, **Step 6** and the VDNs configured in **Section 5**, **Step 6**. The screenshot below shows the two VDNs added. 
20.	From the left pane, navigate to **Configuration → Environment → Applications**. Double click **VHT_TServer** in the right pane. 

©2016 Avaya Inc. All Rights Reserved.

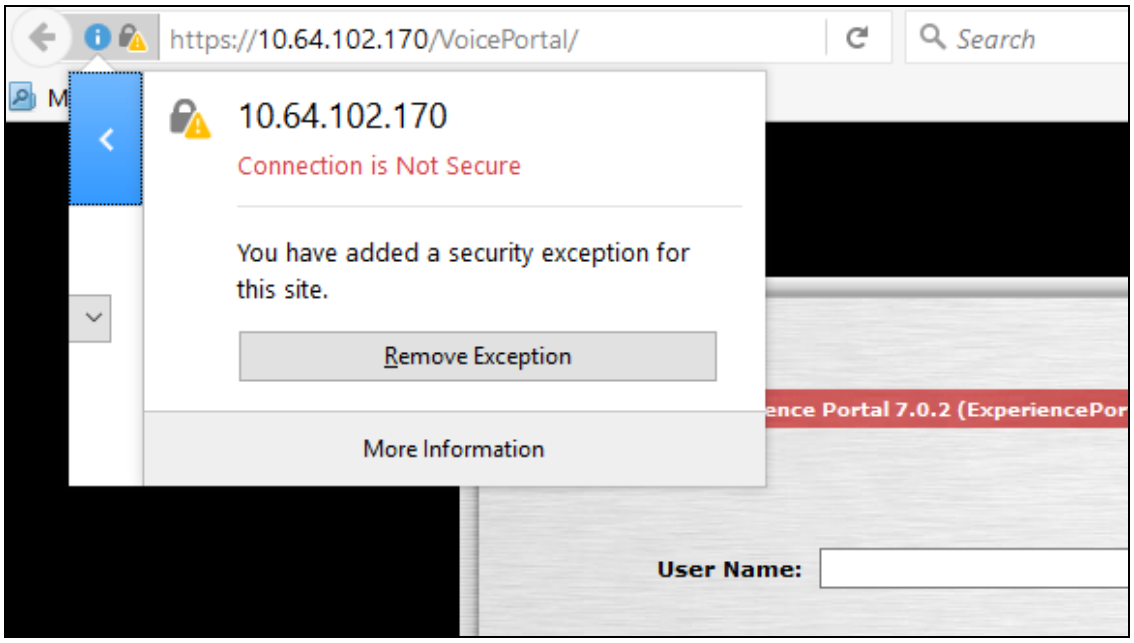
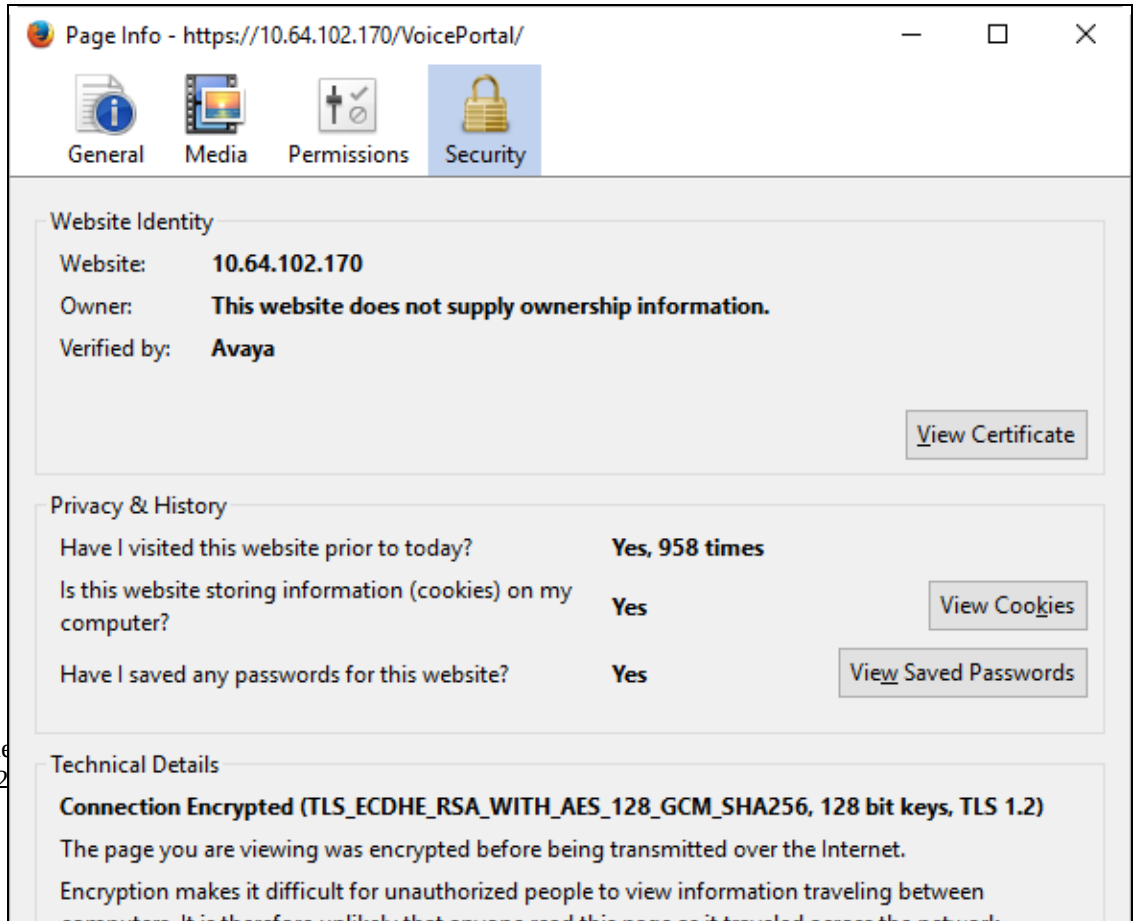
Step	Description
21.	The **VHT_TServer Properties** window is displayed. Select the **Options** tab and double click the **TServer** line. 

©2016 Avaya Inc. All Rights Reserved.

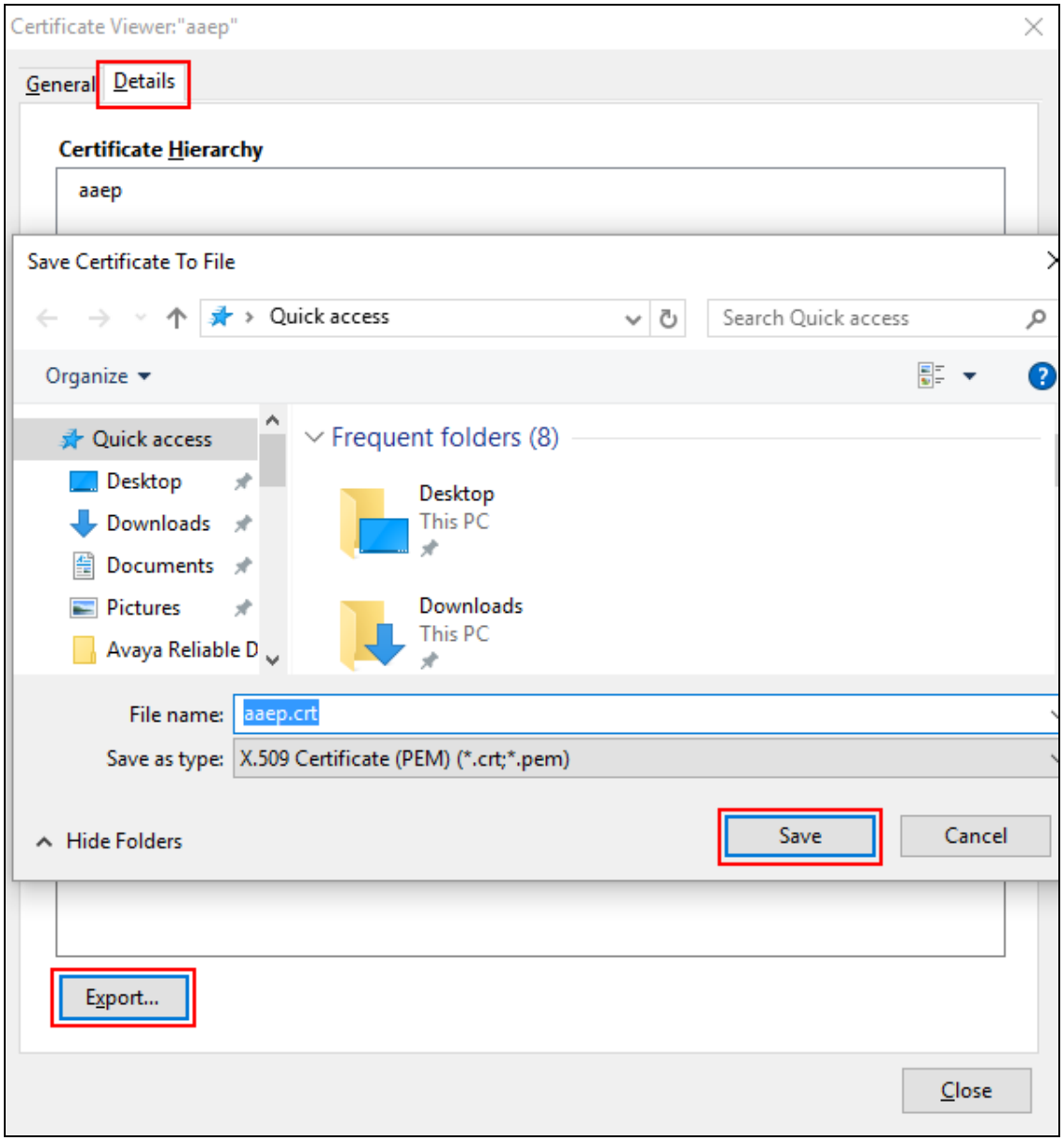
Step	Description
22.	The **TServer** section is displayed. Set the **user-login** and **password** fields to the **User Id** and **User Password** values configured in **Section 6**, **Step 5**. Set the **tsapi-server-id** field to one of the tlinks noted in **Section 6**, **Step 3.**



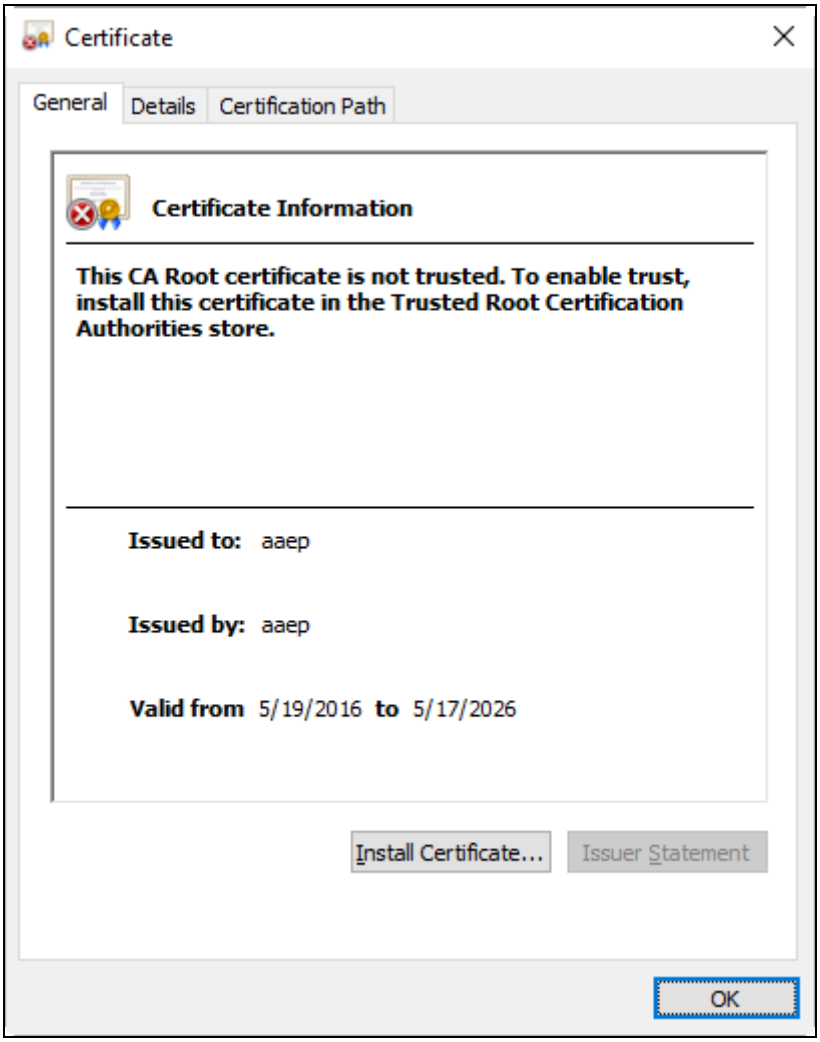
©2016 Avaya Inc. All Rights Reserved.

Step	Description
23.	Install the Experience Portal certificate on Virtual Hold server. Via a browser, go to https://<AES_IP_Address>. The screen captures below the steps when using Firefox as a browser. Select the information icon followed by **More Information.**  Select **View Certificate**. 

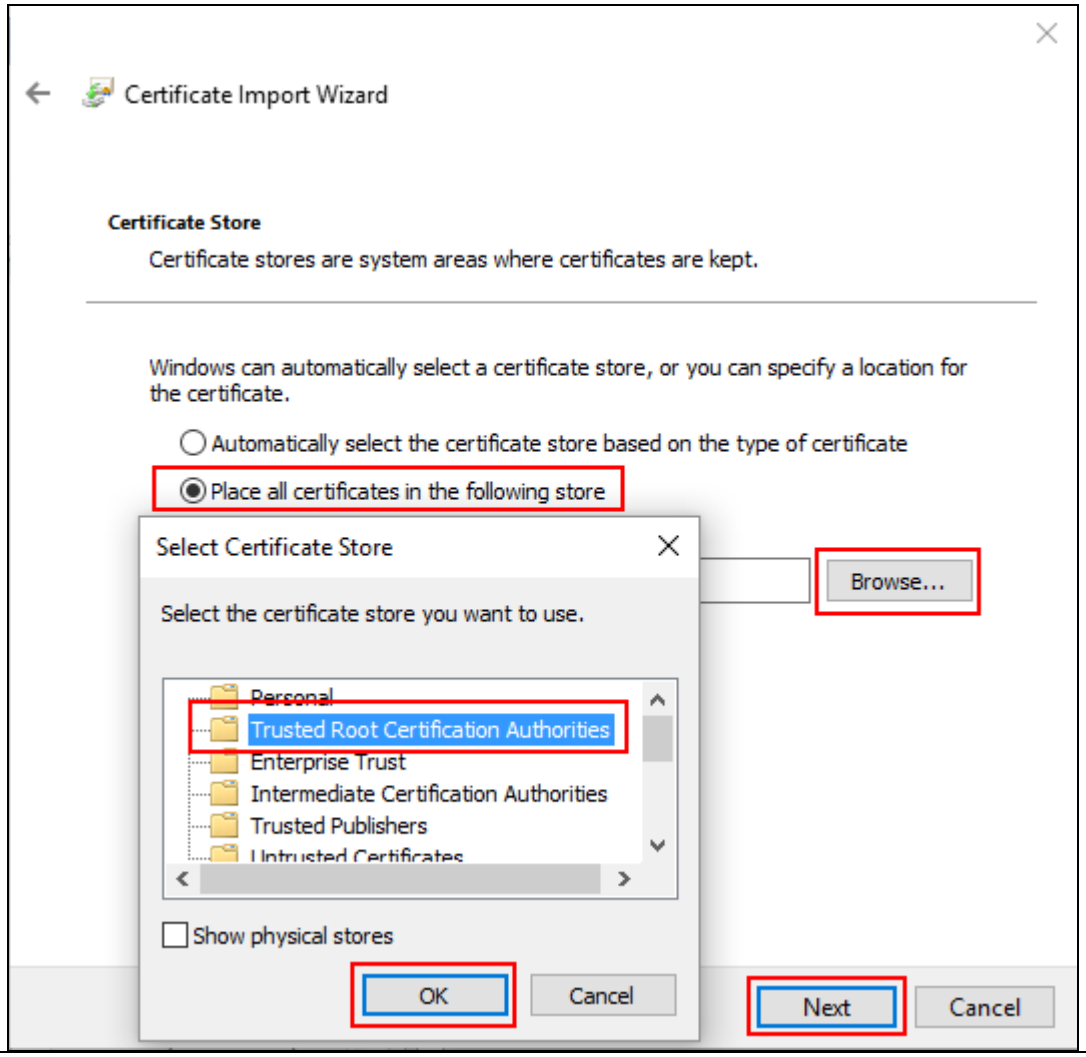
Step	Description
24.	Select the **Details** tab followed by **Export…** On the **Save Certificate File** window, navigate to a desired folder to save the certificate and select **Save**.



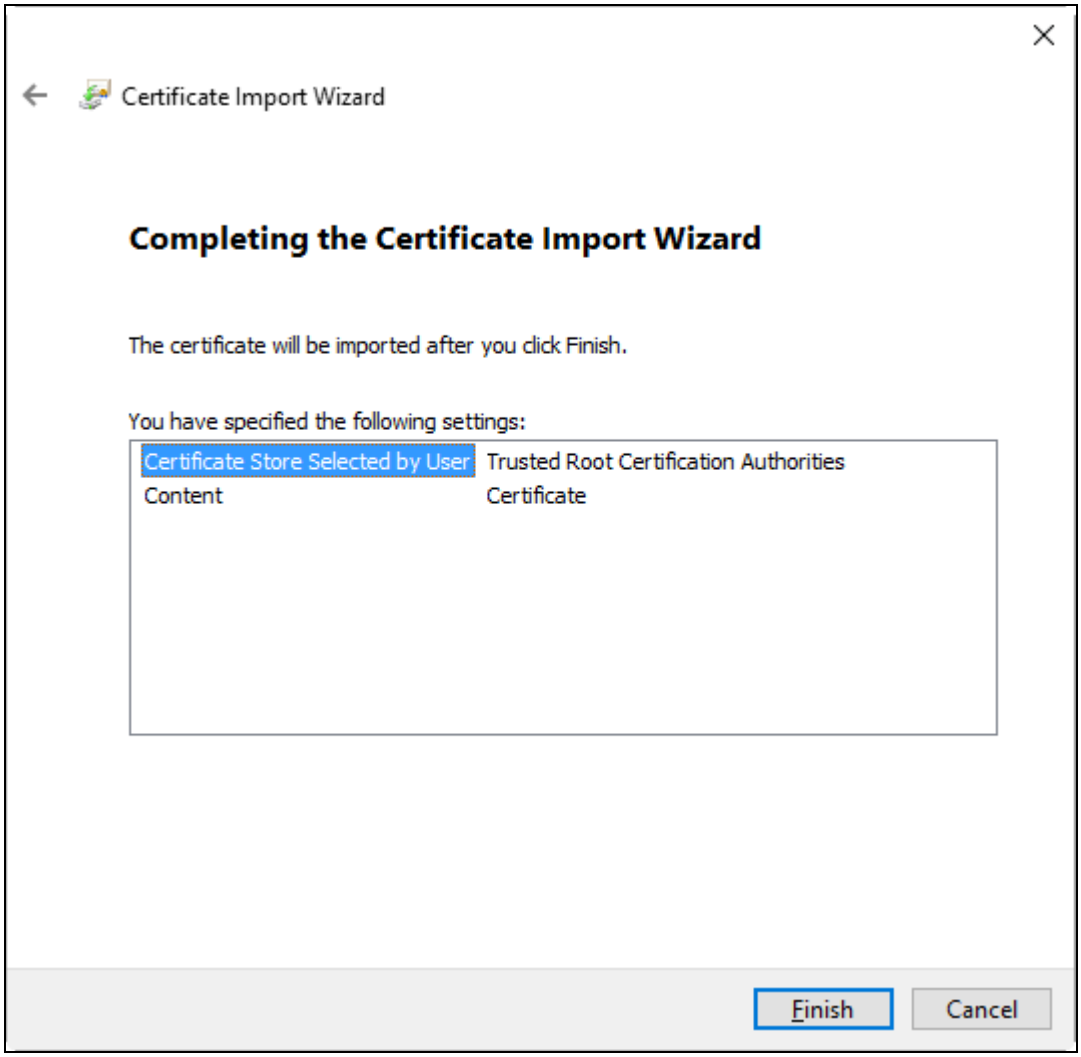
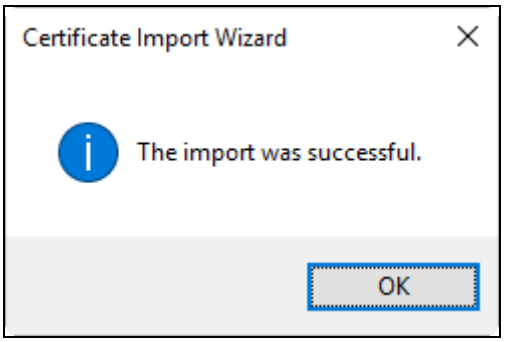
©2016 Avaya Inc. All Rights Reserved.

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

©2016 Avaya Inc. All Rights Reserved.

Step	Description
	Select **Next** on the **Certificate Import Wizard** window (not shown). Select **Place all certificates in the following store** followed by **Browse…** On the **Select Certificate Store** box, select **Trusted Root Certification Authorities** followed by **OK**. Select **Next**. 

©2016 Avaya Inc. All Rights Reserved.

Step	Description
	Select **Finish,** to complete the wizard.  On the **Security Warning** windows, select **Yes** to install the certificate (not shown). Following window shows successful installation of the certificate on the Virtual Hold server. 

©2016 Avaya Inc. All Rights Reserved.

Step	Description

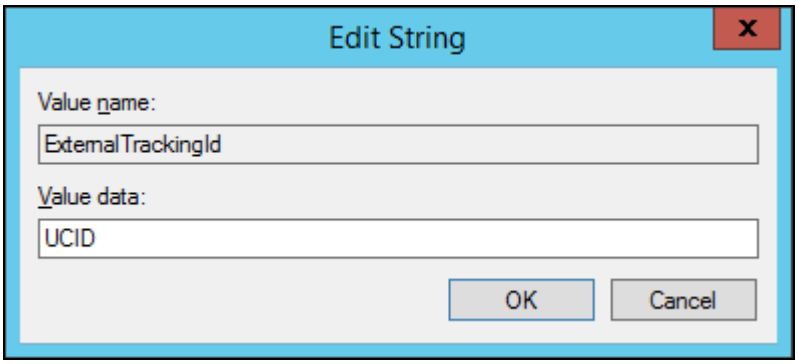
	Navigate to **C:\Program Files (x86)\Virtual Hold Technology** folder and open **OutboundIVR_AVP.xml** using notepad.
	
	• Replace the IP Address in the **URI** field with the IP Address of Experience Portal Manager.
	• Set **ApplicationName** to the name of the outbound application configured in **Section 8**, **Step 5**.
	• Set **AppInterfaceUsername** and **AppInterfacePassword** to the **Username** and **Password** configured for an Experience Portal user. This user is configured on Experience Portal, **User Management → Users.**
	
	`<?xml version="1.0" encoding="utf-8"?>`
	`<LoadBalancerManager>`
	`  <DefaultID>VHT_Test</DefaultID>`
	`  <NumberOfConnectionSets>1</NumberOfConnectionSets>`
	`  <ConnectionSet1>`
	`  <Count>1</Count>`
	`  <Identifier>VHT_Test</Identifier>`
	`  <FirstConnection>Connection1</FirstConnection>`
	`  <LastConnection>Connection1</LastConnection>`
	`  <Connection1>`
	`  <!--`
	`<URI>http://AVPSERVER:8080/axis/services/AppIntfWS</URI> -->`
	`  <URI>`**`https://aaep/axis2/services/VPAppIntfService</URI>`**
	`  <OutboundANI>8005555555</OutboundANI>`
	`  <!-- AVP provisioned Virtual Hold outbound application -->`
	`<ApplicationName>VHT_AEP_OB</ApplicationName>`
	`  <CcxmlApplicationName></CcxmlApplicationName>`
	`<AppInterfaceUsername>interop</AppInterfaceUsername>`
	`<AppInterfacePassword>XXXXXXX</AppInterfacePassword>`
	`  <ConnectTimeout>30</ConnectTimeout>`
	
	`<MaxConcurrentOutboundDialRequests>2</MaxConcurrentOutboundDialRequest`
	`s>`
	
	`<WebServiceClientTimeoutInMilliSeconds>180000</WebServiceClientTimeout`
	`InMilliSeconds>`
	
	`<SessionParameters>enable_call_classification=true;detect_greeting_end`
	`=true</SessionParameters>`
	`  <URLParameters></URLParameters>`

©2016 Avaya Inc. All Rights Reserved.

Step	Description

25.	Navigate to the **C:\VirtualHold** folder and open toolkit.properties using notepad.
	
	• Replace the IP address in the **baseurl** and **webaudiopath** parameters with the IP address of the Virtual Hold server.
	• Set the **defaultdestination** parameter to the Holding VDN configured in **Section 5**, **Step 6** with a prefix of **tel:** (**tel:12202)**
	• 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-v4/`
	`# Ensure the path and VHTPlatformWS version is correct by opening it in a web browser`
	`com.virtualhold.toolkit.baseurl=http://10.64.110.205/VHTPlatformWS-v5/`
	
	`# 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://10.64.110.205:8080/`
	
	`# 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:12202`
	
	`# Set this to true if you want to use the call's DNIS as the incoming Platform Toolkit segment`
	`com.virtualhold.toolkit.useDnisAsSegment=true`
	
	`# 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`

©2016 Avaya Inc. All Rights Reserved.

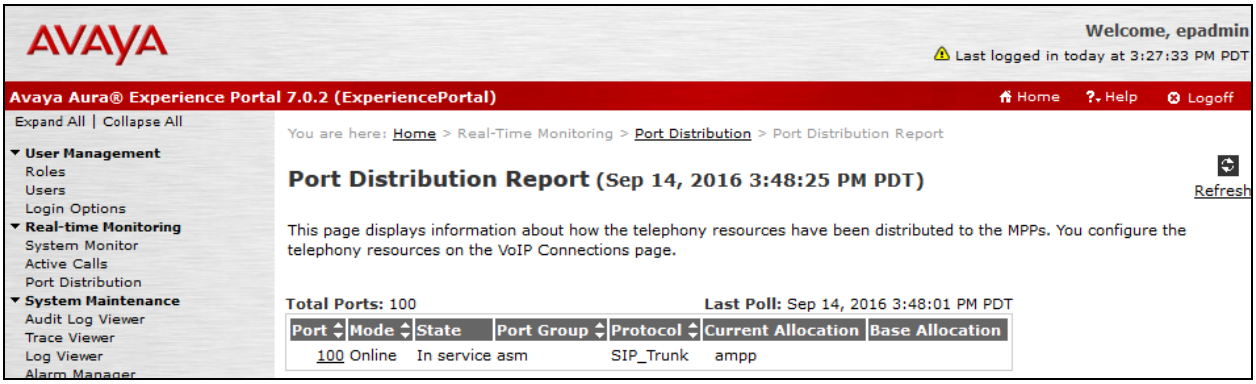
Step	Description
26.	On the Virtual Hold Server, open Registry Editor. Navigate to **HKEY_LOCAL_MACHINE → SOFTWARE → Wow6432Node → Virtual Hold.** Right click on the right side pane and select **New → String Value** (not shown). Type in **ExternalTrackingID** in **Value name** and **UCID** in the **Value data** field. Click **OK** once done. 

©2016 Avaya Inc. All Rights Reserved.

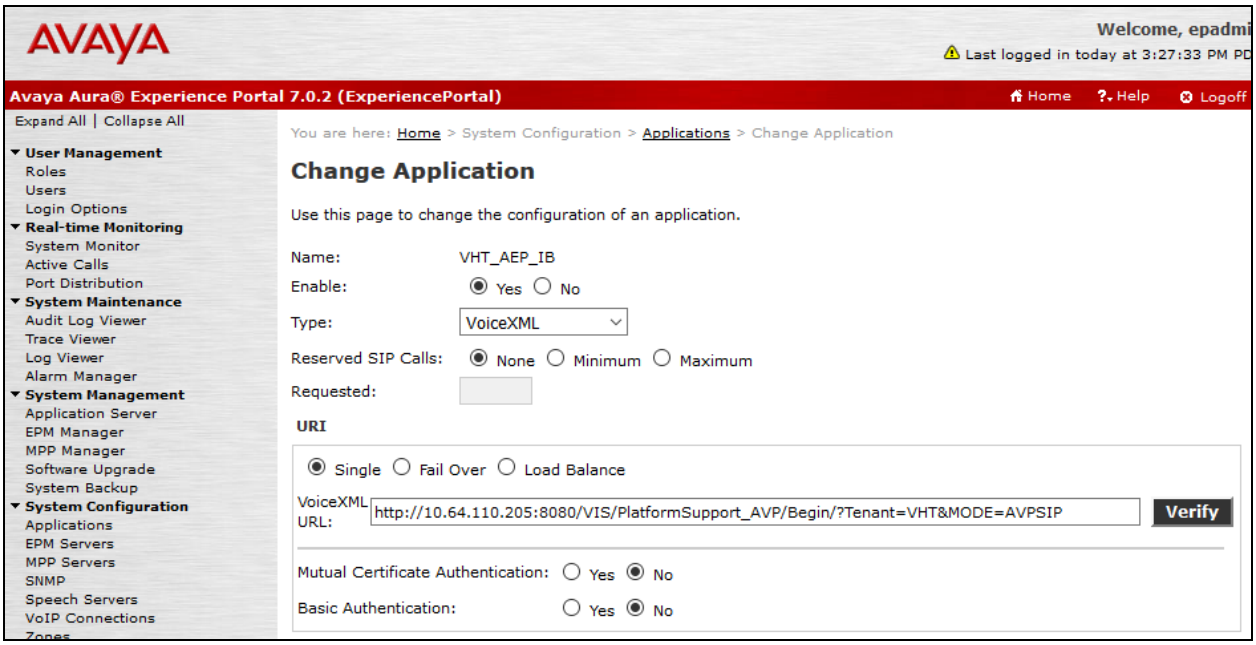
10. Verification Steps

10.1. 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**.



Click **System Configuration → Applications** in the left pane to display the **Applications** page (not shown). Click the **VHT_AEP_IB** application link on the page. The **Change Application** page is displayed. Click the **Verify** button next to the **VoiceXML URL** field.



©2016 Avaya Inc. All Rights Reserved.

Verify that that the following page is displayed as an indication that the application is accessible.


```
- <vxml version="2.1">
    <property name="documentmaxage" value="0"/>
    <property name="documentmaxstale" value="0"/>
  - <form id="InitialForm" scope="document">
      <var name="PLATFORM_ANI" expr=""/>
      <var name="PLATFORM_DNIS" expr=""/>
      <var name="avpUCID" expr=""/>
      <var name="avpAAI" expr=""/>
    - <block name="InitialBlock">
        <assign name="PLATFORM_ANI" expr="session.connection.remote.uri"/>
        <assign name="PLATFORM_DNIS" expr="session.connection.local.uri"/>
        <assign name="avpUCID" expr="session.avaya.ucid"/>
        <assign name="avpAAI" expr="session.connection.aai"/>
        <submit next="/VIS/-/next?Action_07381e87a39f48a5b7add4802eb951f7=success.filled&MODE=AVPSIP" method="post"
        namelist="PLATFORM_ANI PLATFORM_DNIS avpUCID avpAAI"/>
      </block>
    - <catch event="connection.disconnect.hangup">
        <goto next="/VIS/-/next?Action_07381e87a39f48a5b7add4802eb951f7=error.disconnect.hangup&MODE=AVPSIP"/>
      </catch>
    - <catch event="externalmessage.cpa.machine">
        <goto next="/VIS/-/next?Action_07381e87a39f48a5b7add4802eb951f7=externalmessage.cpa.machine&MODE=AVPSIP"/>
      </catch>
    - <catch event="externalmessage.cpa.beep">
        <goto next="/VIS/-/next?Action_07381e87a39f48a5b7add4802eb951f7=externalmessage.cpa.beep&MODE=AVPSIP"/>
      </catch>
    - <catch event="externalmessage.cpa">
        <goto next="/VIS/-/next?Action_07381e87a39f48a5b7add4802eb951f7=externalmessage.cpa&MODE=AVPSIP"/>
      </catch>
    </form>
  - <catch event="connection.disconnect.hangup">
      <goto next="/VIS/-/abort?MODE=AVPSIP"/>
    </catch>
  </vxml>
```


Repeat the procedure for the **VHT_AEP_OB** application.

©2016 Avaya Inc. All Rights Reserved.

10.2. Avaya Aura® Session Manager

To verify connectivity to Experience Portal, click on **Session Manager** on the Home page of System Manager web interface. Navigate to **Session Manager → System Status → SIP Entity Monitoring**. Locate the SIP Entity for Experience Portal under **All Monitored SIP Entities** and click on it. The **Conn. Status** and **Link Status** fields should display **UP**.

1 Items | Refresh Filter: Enable

Session Manager	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
asm	10.64.102.17	5060	TCP	FALSE	UP	200 OK	UP

11. Conclusion

These Application Notes describe the configuration steps required to integrate Virtual Hold Queue Manager using Genesys T-Server with Avaya Aura® Experience Portal, Avaya Aura® Session Manager, Avaya Aura® Communication Manager, and Avaya Aura® Application Enablement Services. All feature and serviceability test cases were completed successfully with observations noted in **Section 2.2**.

12. Additional References

This section references the Avaya and Virtual Hold documentation relevant to these Application Notes. The Avaya product documentation is available at http://support.avaya.com.

[1] *Administering Avaya Aura® Communication Manager, Release 7.0.1, 03-300509, Issue 2, May 2016.*
[2] *Administering Avaya Aura® Avaya Aura® Application Enablement Services, Release 7.0.1, Issue 2, May 2016.*
[3] *Administering Aura® Experience Portal, Release 7.0.1, April 2015*
[4] Virtual Hold for AVP and AEP Integration Guide – Aug 10, 2016
[5] Virtual Hold ACD Configuration Guide for Avaya – 5/13/2014
[6] EyeQueue User Guide Version 8.6 - Oct 10, 2016
[7] Virtual Hold Release Notes Version 8.6.x – Sept 23, 2016
[8] High Availability System Requirements Version 8.6 – Sept 23, 2016
[9] Standalone System Requirements Version 8.6– Sept 23, 2016

©2016 Avaya Inc. All Rights Reserved.

©2016 Avaya Inc. All Rights Reserved.
Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

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