DevConnect Program

Application Notes for VHT Callback using Native TSAPI 9.5 with Avaya Aura® Application Enablement Services 10.1, Avaya Aura® Communication Manager 10.1 and Avaya Aura® Session Manager 10.1 – Issue 1.0

Abstract

These Application Notes describe the steps required to integrate VHT Callback using Native TSAPI 9.5 with Avaya Aura® Application Enablement Services 10.1, Avaya Aura® Communication Manager 10.1, and Avaya Aura® Session Manager 10.1. VHT Callback is a contact center solution that calculates expected wait time and maintains caller position in a virtual queue. The integration used the Avaya Telephony Services Application Programming Interface from Avaya Aura® Application Enablement Services and the SIP trunk interface from Avaya Aura® Session Manager.

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

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

1. Introduction

These Application Notes describe the steps required to integrate VHT Callback using Native TSAPI with Avaya Aura® Application Enablement Services, Avaya Aura® Communication Manager, and Avaya Aura® Session Manager. VHT Callback is a contact center solution that calculates expected wait time and maintains caller position in a virtual queue. The integration used the Avaya Telephony Services Application Programming Interface from Avaya Aura® Application Enablement Services and the SIP trunk interface from Avaya Aura® Session Manager.

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

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

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

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

2. General Test Approach and Test Results

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

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

The serviceability test cases were performed manually by disconnecting/reconnecting the Ethernet connection to the Callback server and to the IVG component. In addition, it was verified that Communication Manager routed calls to an available agent or queued the call when the Callback or IVG servers were unavailable.

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

Avaya recommends our customers implement Avaya solutions using appropriate security and encryption capabilities enabled by our products. The testing referenced in these DevConnect Application Notes 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 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 feature testing focused on verifying the following on Callback:

- Use of TSAPI query service to query status on skill group.
- Use of TSAPI event report service to monitor VDNs.
- Use of TSAPI routing service to route incoming calls.
- Use of SIP messages to answer and transfer inbound calls and to initiate and transfer outbound callback calls.
- Proper handling of call scenarios involving G.711, DTMF, REFER, expected wait time below and over the threshold, transfer of inbound calls with received UUI data, initiation and transfer of outbound callback calls with priority and saved UUI data, and unsuccessful callback attempts.
- Queue statistics using TSAPI real-time adapter in Callback.
- SIP trunk between IVG server and Session Manager using UDP transport.
- IVG response to SIP OPTIONS messages from Session Manager.

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

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.

2.3. Support

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

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

3. Reference Configuration

The configuration used for the compliance testing is shown in **Figure 1**. The Callback configuration consisted of the Callback server and IVG that connected via SIP trunks to Session Manager. 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 787xx were routed to the IVG component of Callback.

Device Type	Extension
Skill Group Number	1
Skill Group Extension	61001
Agent Stations	65001, 66006
Agent Login IDs	65881, 65882

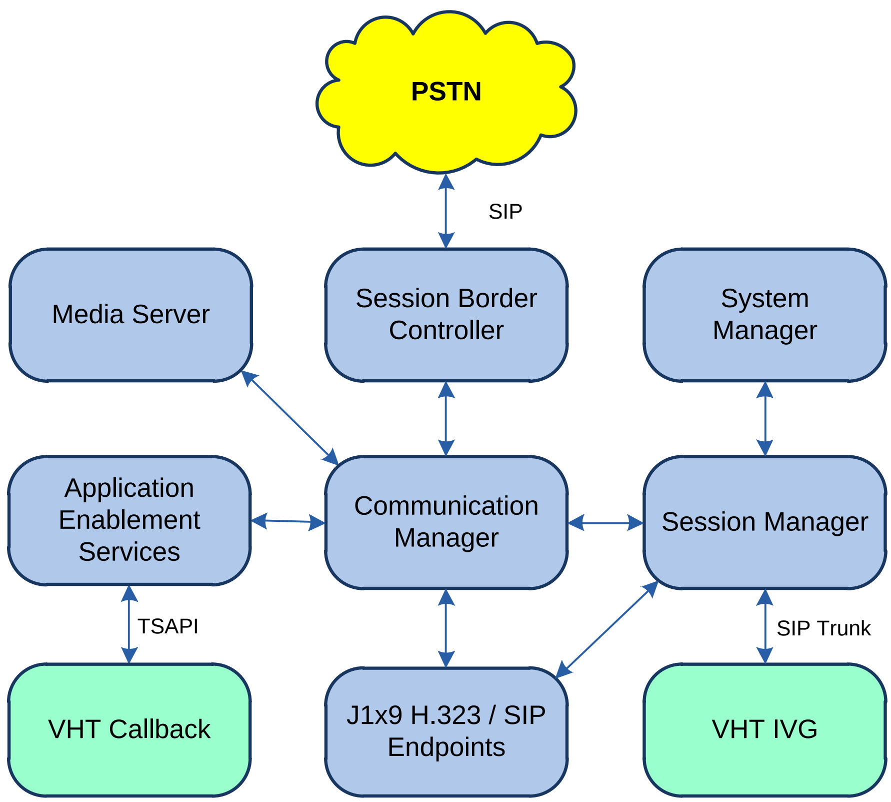


Figure 1: Compliance Testing Configuration

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya Aura® Communication Manager in Virtual Environment	10.1.3 (10.1.3.0.1.974.27893)
Avaya G430 Media Gateway	42.8.0
Avaya Aura® Media Server in Virtual Environment	10.1 (10.1.0.154)
Avaya Aura® Application Enablement Services in Virtual Environment	10.1. (10.1.3.0.0.11-0)
Avaya Aura® Session Manager in Virtual Environment	10.1.3 (10.1.3.0.1013007)
Avaya Aura® System Manager in Virtual Environment	10.1.3 (10.1.3.0.0715713)
Avaya Session Border Controller in Virtual Environment	10.1 (10.1.2.0-64-23285)
Avaya Agent for Desktop (H.323 & SIP)	2.0.6.0.10
Avaya 9611G IP Desk phone (H.323)	6.8.5.3.2
Avaya J169 IP Desk phone (SIP)	4.0.13.0.6
Avaya J179 IP Desk phone (H.323)	6.8.5.3.2
Mindful Callback using Native TSAPI on Microsoft Windows Server 2019 Standard with ▪ Avaya AES TSAPI Client	Base version 9.5.0 with Patch 9.5.3.1244 5.2.1 8.1.0 Build 9
Mindful Interactive Voice Gateway (IVG) on CentOS 7.9 ▪ Holly Voice Platform (HVP) ▪ VXML Interactive Server (VIS) ▪ Call Control Interaction Server (CCIS)	5.3 7.2.20 7.11 5.3

5. Configure Avaya Aura® Communication Manager

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

- Verify License
- Administer CTI Link
- Administer System Parameters Features
- Administer Vectors and VDNs
- Administer IP Node Names
- Administer IP Network Region
- Administer IP Codec Set

- Administer SIP Signaling Group
- Administer SIP Trunk Group
- Administer AAR Call Routing

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: 7.0

                                ACD? y                        Reason Codes? y
                       BCMS (Basic)? y           Service Level Maximizer? n
         BCMS/VuStats Service Level? y         Service Observing (Basic)? y
  BSR Local Treatment for IP & ISDN? y  Service Observing (Remote/By FAC)? y
                  Business Advocate? n          Service Observing (VDNs)? y
                    Call Work Codes? y                         Timed ACW? y
      DTMF Feedback Signals For VRU? y                 Vectoring (Basic)? y
                   Dynamic Advocate? n             Vectoring (Prompting)? y
       Expert Agent Selection (EAS)? y         Vectoring (G3V4 Enhanced)? y
                            EAS-PHD? y          Vectoring (3.0 Enhanced)? y
                   Forced ACD Calls? n  Vectoring (ANI/II-Digits Routing)? y
               Least Occupied Agent? y  Vectoring (G3V4 Advanced Routing)? y
          Lookahead Interflow (LAI)? y                 Vectoring (CINFO)? y
Multiple Call Handling (On Request)? y   Vectoring (Best Service Routing)? y
    Multiple Call Handling (Forced)? y              Vectoring (Holidays)? y
  PASTE (Display PBX Data on Phone)? y             Vectoring (Variables)? y
        (NOTE: You must logoff & login to effect the permission changes.)
```

5.2. Administer CTI Link

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

```
add cti-link 1                                              Page   1 of   3
                                    CTI LINK
 CTI Link: 1
Extension: 77700
     Type: ADJ-IP
                                                                       COR: 1
     Name: AES CTI Link
Unicode Name? n
```

5.3. Administer System Parameters Features

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

```
change system-parameters features                               Page   5 of  19
                        FEATURE-RELATED SYSTEM PARAMETERS

SYSTEM PRINTER PARAMETERS
  Endpoint:               Lines Per Page: 60

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

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

```
change system-parameters features                               Page  13 of  19
                        FEATURE-RELATED SYSTEM PARAMETERS
 CALL CENTER MISCELLANEOUS
           Callr-info Display Timer (sec): 10
                         Clear Callr-info: next-call
        Allow Ringer-off with Auto-Answer? n

    Reporting for PC Non-Predictive Calls? n

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

  ASAI
                    Copy ASAI 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
```

5.4. 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
44201	201	Entry vector & VDN for adjunct route and failure coverage
44202	202	Hold vector & VDN for queuing inbound calls to skill at medium priority
44203	203	Callback vector & VDN for queuing outbound calls to skill at high priority
44204	204	Route vector & VDN for routing calls to IVG and failure coverage

5.4.1. Entry Vector and VDN

Modify an available vector using the **change vector** command. The vector will be used to provide adjunct route to the CTI link defined in **Section 5.2**.

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

```
change vector 201                                              Page   1 of   6
                                  CALL VECTOR

    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 44202            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: 44201
                                 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 *1* is the existing skill group number mentioned in **Section** Error! Reference source not found..

```
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 1   pri m
03 wait-time    60  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 44202                                               Page   1 of   3
                            VECTOR DIRECTORY NUMBER

                             Extension: 44202
                                 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 *1* is the existing skill group number mentioned in **Section** Error! Reference source not found..

```
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 1   pri h
02 wait-time    60  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 44203                                              Page   1 of   3
                            VECTOR DIRECTORY NUMBER

                             Extension: 44203
                                 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 IVG using extension 48701. If the call to IVG fails for any reason, the incoming ACD call will be routed to the ACD skill where the call will either be queued or answered by an available agent. This ensures that the call is properly routed by Communication Manager even if the call attempt to IVG fails.

```
change vector 204                                               Page   1 of   6
                                  CALL VECTOR

    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 48701            with cov n if unconditionally
03 wait-time    2   secs hearing ringback
04 route-to     number 44202            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 44204                                                Page   1 of   3
                            VECTOR DIRECTORY NUMBER

                             Extension: 44204
                                 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. Administer IP Node Names

In the **IP Node Names** form, assign an IP address and host name for Communication Manager (*procr*) and Session Manager (*sm7-sig*). The host names will be used in other configuration screens of Communication Manager.

```
change node-names ip                                            Page   1 of   2
                                  IP NODE NAMES
    Name              IP Address
default             0.0.0.0
ms7                 10.64.101.233
sm7-sig             10.64.101.238
procr               10.64.101.236
procr6              ::
```

5.6. Administer IP Codec Set

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

```
change ip-codec-set 1                                           Page   1 of   2

                          IP CODEC SET
    Codec Set: 1

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

5.7. Administer IP Network Region

In the **IP Network Region** form, the **Authoritative Domain** field is configured to match the domain name configured on Session Manager. In this configuration, the domain name is *dr220.com*. By default, **IP-IP Direct Audio** (shuffling) is enabled to allow audio traffic to be sent directly between IVG and IP endpoints without using media resources in the Avaya G450 Media Gateway or Avaya Media Server. Note that calls to the PSTN are not shuffled. The **IP Network Region** form also specifies the **IP Codec Set** to be used for calls routed over the SIP trunk to Session Manager. This codec set is used when its corresponding network region (i.e., IP Network Region 1) is specified in the SIP signaling group.

```
change ip-network-region 1                                      Page   1 of  20
                               IP NETWORK REGION
  Region: 1       NR Group: 1
Location: 1       Authoritative Domain: dr220.com
    Name:                       Stub Network Region: n
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: yes
      Codec Set: 1              Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 2048                      IP Audio Hairpinning? n
   UDP Port Max: 65535
DIFFSERV/TOS PARAMETERS
 Call Control PHB Value: 46
        Audio PHB Value: 46
        Video PHB Value: 26
802.1P/Q PARAMETERS
 Call Control 802.1p Priority: 6
        Audio 802.1p Priority: 6
        Video 802.1p Priority: 5      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                       RSVP Enabled? n
  H.323 Link Bounce Recovery? y
 Idle Traffic Interval (sec): 20
   Keep-Alive Interval (sec): 5
            Keep-Alive Count: 5
```

5.8. Administer SIP Signaling Group

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

- Set the **Group Type** field to *sip*.
- Set the **IMS Enabled** field to *n*.
- The **Transport Method** field was set to *tls*.
- Specify Communication Manager (*procr*) and the Session Manager (*sm7-sig*) as the two ends of the signaling group in the **Near-end Node Name** field and the **Far-end Node Name** field, respectively. These field values are taken from the **IP Node Names** form.
- Ensure that the TLS port value of *5061* is configured in the **Near-end Listen Port** and the **Far-end Listen Port** fields.
- The preferred codec for the call will be selected from the IP codec set assigned to the IP network region specified in the **Far-end Network Region** field.
- Enter the domain name of Session Manager in the **Far-end Domain** field. In this configuration, the domain name is *dr220.com*.
- The **DTMF over IP** field should be set to the default value of *rtp-payload*.
- Enable **Direct IP-IP Audio Connections** to allow the call to be shuffled.

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

```
add signaling-group 66                                     Page   1 of   2
                                SIGNALING GROUP

 Group Number: 66             Group Type: sip
  IMS Enabled? n        Transport Method: tls
        Q-SIP? n
     IP Video? n                                   Enforce SIPS URI for SRTP? y
  Peer Detection Enabled? y  Peer Server: SM                       Clustered? n
 Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? y
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? n
Alert Incoming SIP Crisis Calls? n
   Near-end Node Name: procr                    Far-end Node Name: sm7-sig
 Near-end Listen Port: 5061                   Far-end Listen Port: 5061
                                           Far-end Network Region: 1

Far-end Domain: dr220.com
                                             Bypass If IP Threshold Exceeded? n
Incoming Dialog Loopbacks: eliminate                  RFC 3389 Comfort Noise? n
         DTMF over IP: rtp-payload            Direct IP-IP Audio Connections? y
Session Establishment Timer(min): 3                     IP Audio Hairpinning? n
         Enable Layer 3 Test? y                     Initial IP-IP Direct Media? n
H.323 Station Outgoing Direct Media? n              Alternate Route Timer(sec): 6
```

5.9. Administer SIP Trunk Group

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

```
add trunk-group 66                                           Page   1 of  22
                                TRUNK GROUP

Group Number: 66                   Group Type: sip           CDR Reports: y
  Group Name: SIP Trunks to SM7                COR: 1        TN: 1        TAC: 1066
   Direction: two-way        Outgoing Display? n
 Dial Access? n                                   Night Service:
Queue Length: 0
Service Type: tie                    Auth Code? n
                                              Member Assignment Method: auto
                                                       Signaling Group: 66
                                                     Number of Members: 10
```

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

```
add trunk-group 66                                           Page   3 of  22
TRUNK FEATURES
          ACA Assignment? n            Measured: none
                                                          Maintenance Tests? y



   Suppress # Outpulsing? n  Numbering Format: private
                                                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
```

5.10. Administer AAR Call Routing

Configure the uniform dial plan table to route calls using AAR for dialed digits that are 5-digits long and begin with '4'. This would cover call routing to IVG (i.e., 48701).

```
change uniform-dialplan 4                                      Page   1 of   2
                       UNIFORM DIAL PLAN TABLE
                                                             Percent Full: 0

  Matching                   Insert              Node
  Pattern       Len Del      Digits      Net Conv Num
 48              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 "48" to route pattern 10 as shown below. Note that the **Call Type** was set to *lev0*. This entry routes calls to IVG and SIP stations.

```
change aar analysis 48                                          Page   1 of   2
                             AAR DIGIT ANALYSIS TABLE
                                   Location: all           Percent Full: 2

          Dialed           Total     Route    Call   Node  ANI
          String          Min  Max  Pattern   Type   Num   Reqd
    48                    5    5     66       lev0         n
```

Configure a preference in **Route Pattern** 10 to route calls over SIP trunk group 66 as shown below.

```
change route-pattern 66                                        Page   1 of   3
                    Pattern Number: 66     Pattern Name: To SM
    SCCAN? n    Secure SIP? n     Used for SIP stations? n

    Grp FRL NPA Pfx Hop Toll No.  Inserted                              DCS/ IXC
    No          Mrk Lmt List Del  Digits                                QSIG
                             Dgts                                       Intw
 1: 66   0                                                               n   user
 2:                                                                      n   user
 3:                                                                      n   user
 4:                                                                      n   user
 5:                                                                      n   user
 6:                                                                      n   user

     BCC VALUE  TSC CA-TSC    ITC BCIE Service/Feature PARM Sub  Numbering LAR
    0 1 2 M 4 W     Request                                 Dgts Format
 1: y y y y y n  n            rest                               unk-unk   none
 2: y y y y y n  n            rest                                         none
 3: y y y y y n  n            rest                                         none
 4: y y y y y n  n            rest                                         none
 5: y y y y y n  n            rest                                         none
 6: y y y y y n  n            rest                                         none
```

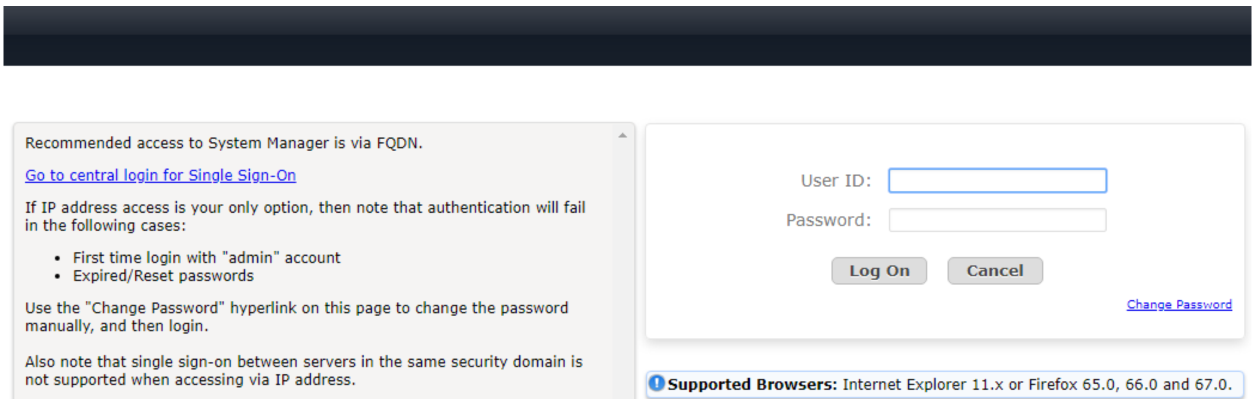
6. Configure Avaya Aura® Session Manager

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

- Launch System Manager
- Administer SIP Entities
- Administer Routing Policies
- Administer Dial Patterns

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 Entities

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

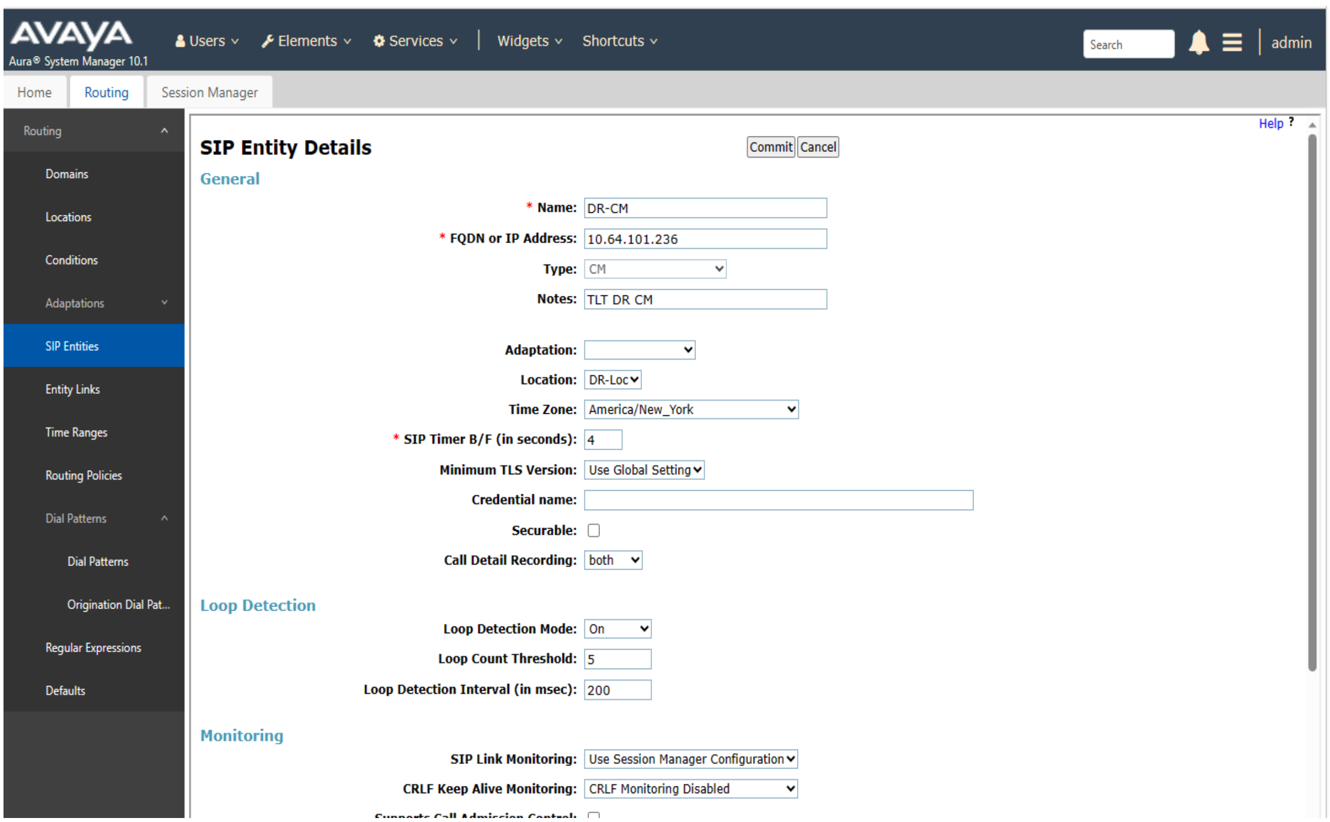
6.2.1. SIP Entity for Communication Manager

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

Under *General*:

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

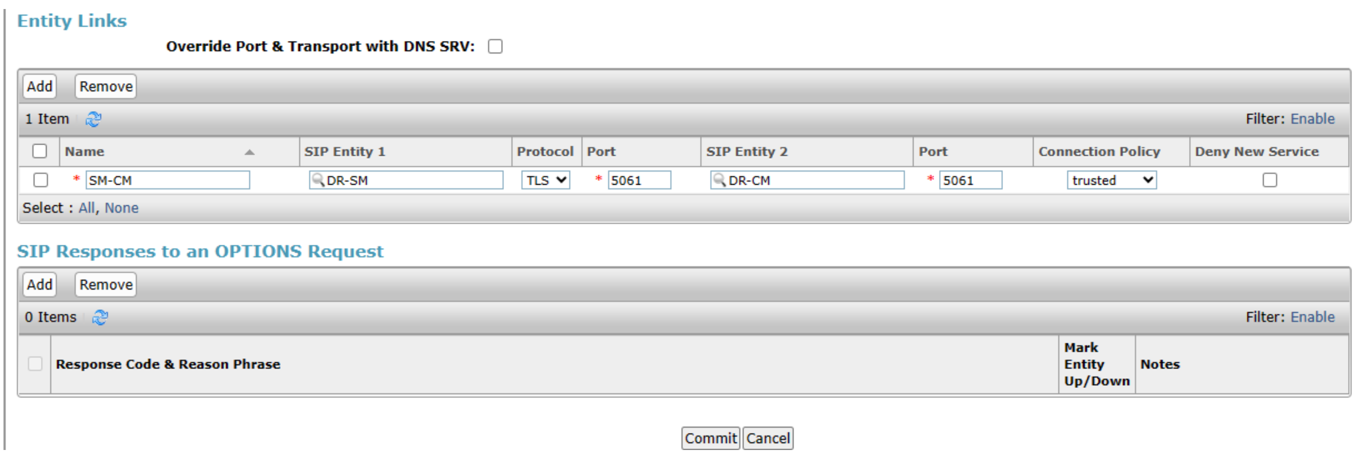
Defaults can be used for the remaining fields. Click **Commit** to save each SIP Entity definition.



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

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

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



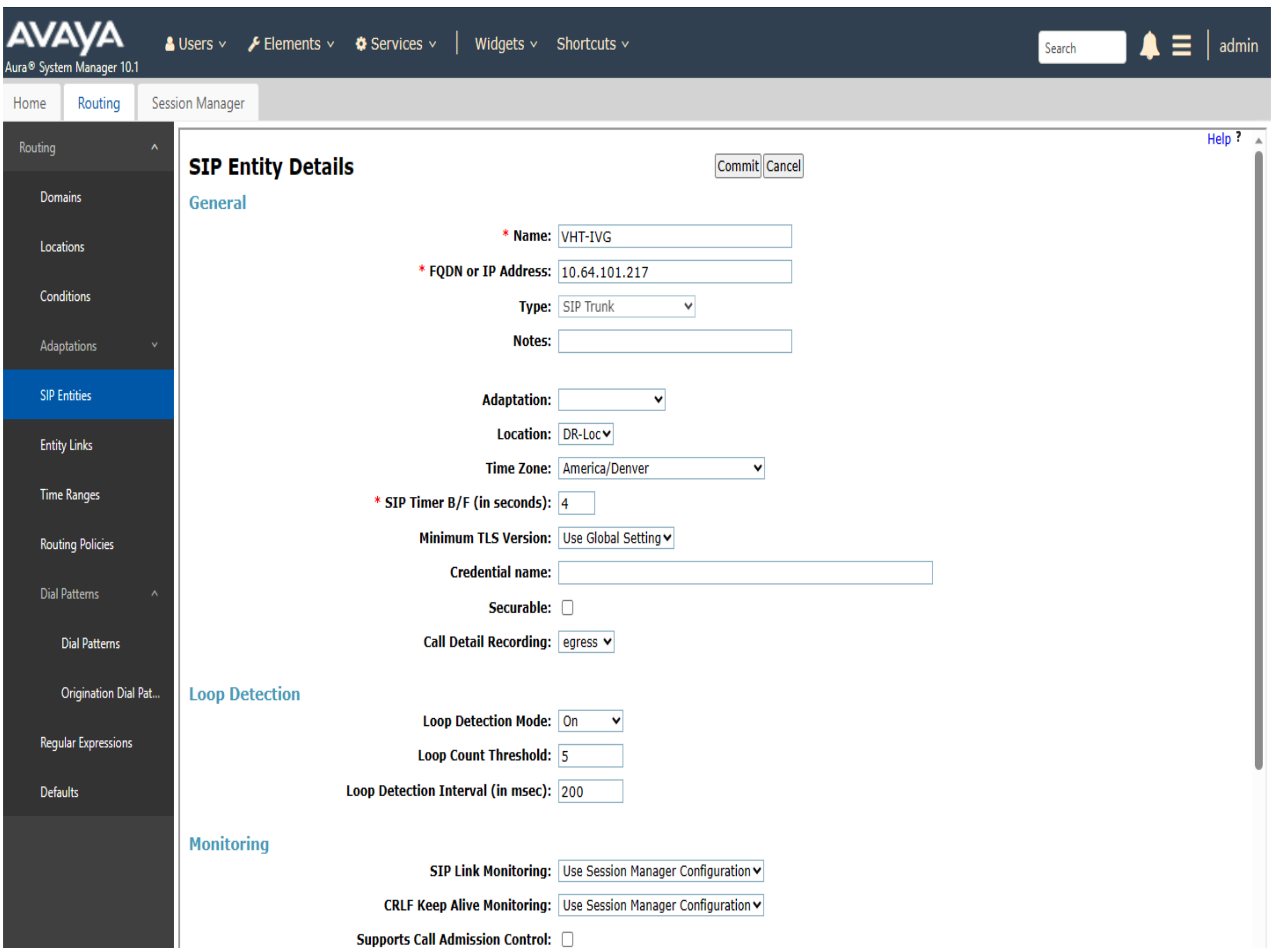
6.2.2. SIP Entity for IVG

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

Under *General*:

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

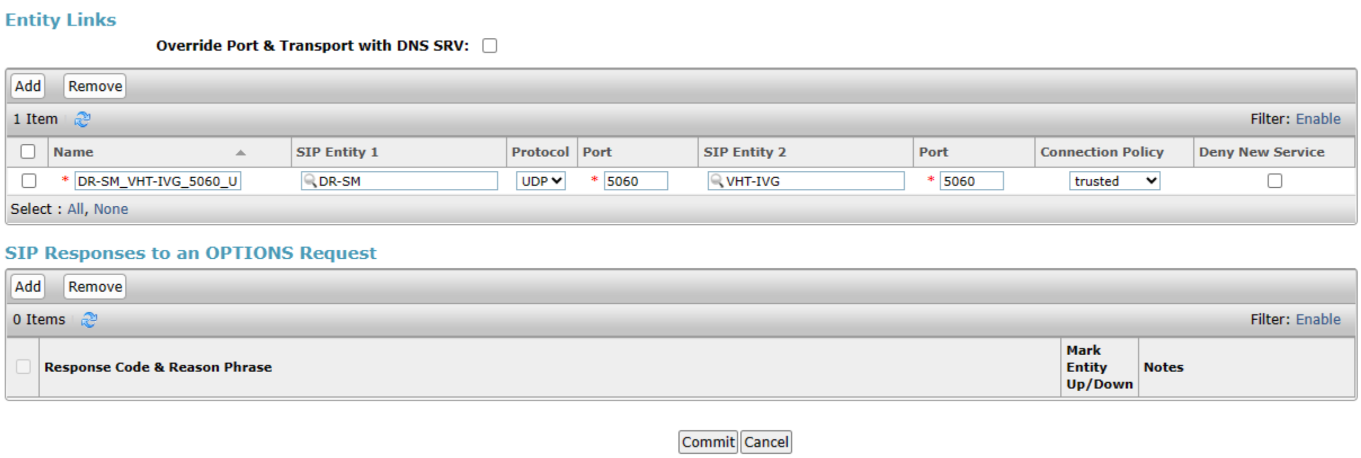
Defaults can be used for the remaining fields. Click **Commit** to save each SIP Entity definition.



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

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

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



6.3. Administer Routing Policies

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

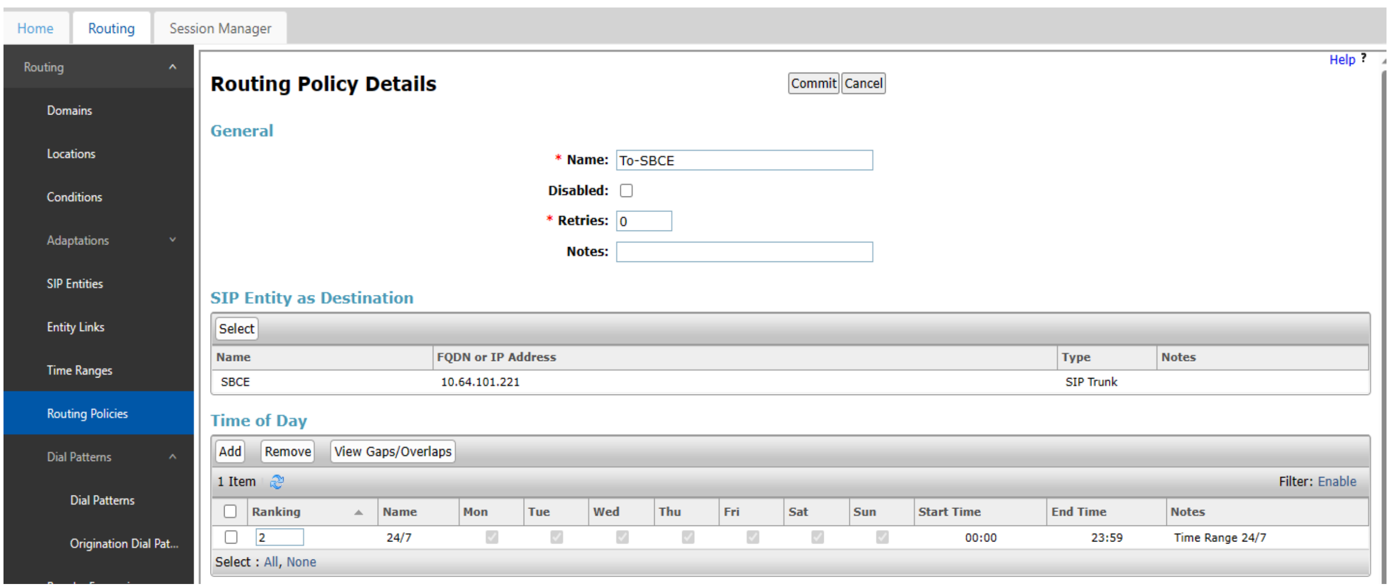
6.3.1. Routing Policy for Communication Manager

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

Under *General*:
Enter a descriptive name in **Name**. In this case the name is "To-SBCE"

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.



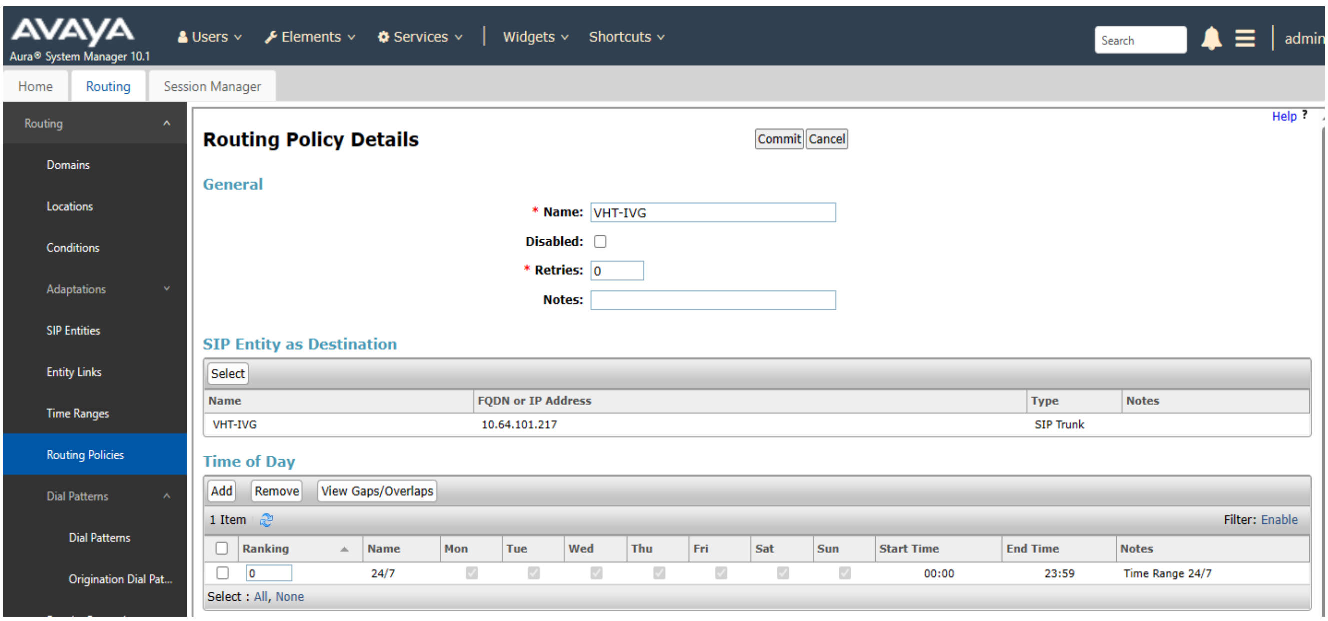
6.3.2. Routing Policy for IVG

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

Under *General*:
Enter a descriptive name in **Name**.

Under *SIP Entity as Destination*:
Click **Select**, and then select the appropriate SIP entity to which this routing policy applies.

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



6.4. Administer Dial Patterns

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

6.4.1. Dial Patterns for Communication Manager

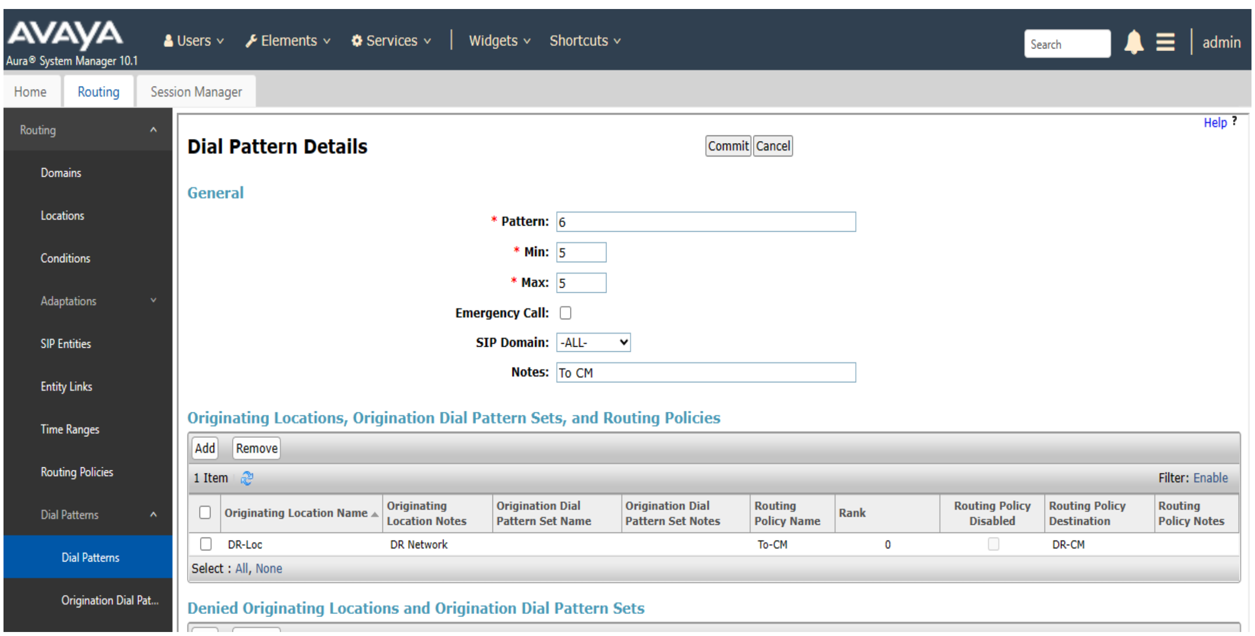
In the sample configuration, 5-digit extensions starting with '6' and 11-digit numbers prepended with the prefix code '+1' were routed to local stations and PSTN, respectively, via Communication Manager. To add a dial pattern, select **Dial Patterns** on the left and click on the **New** button (not shown) on the right. Fill in the following:

Under *General*:

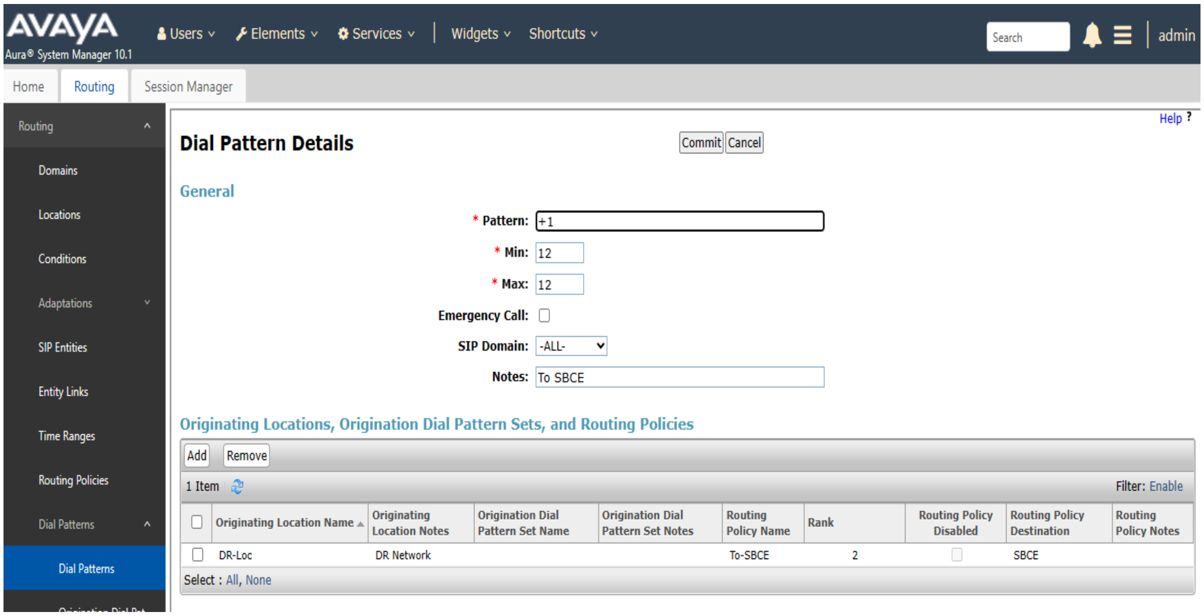
- **Pattern:** Dialed number or prefix.
- **Min** Minimum length of dialed number.
- **Max** Maximum length of dialed number.
- **SIP Domain** SIP domain of dial pattern.
- **Notes** Comment on purpose of dial pattern (optional).

Under *Originating Locations and Routing Policies*:
Click **Add**, and then select the appropriate location and routing policy from the list.

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



The following screen shows the dial pattern definition for routing calls to PSTN via Communication Manager.



6.4.2. Dial Pattern for IVG

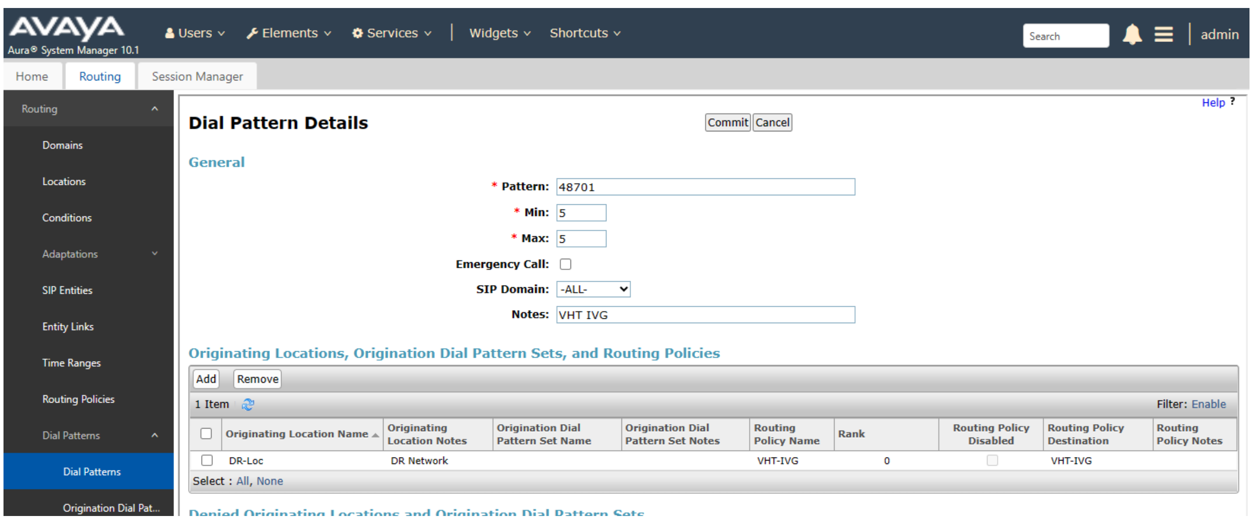
In the sample configuration, *48701* was routed to IVG. To add a dial pattern, select **Dial Patterns** on the left and click on the **New** button (not shown) on the right. Fill in the following:

Under *General*:

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

Under *Originating Locations and Routing Policies*:
Click **Add**, and then select the appropriate location and routing policy from the list.

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



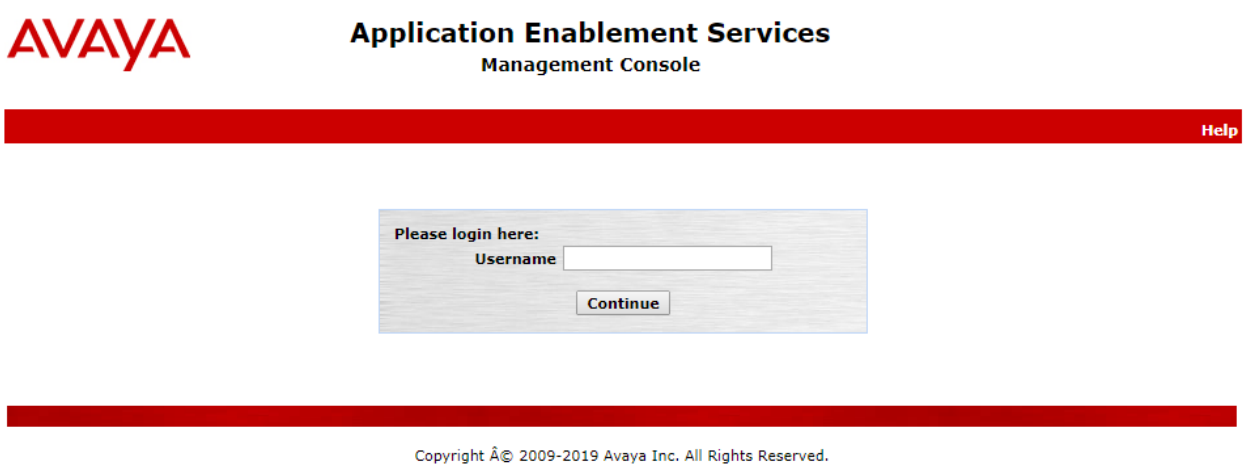
7. Configure Avaya Aura® Application Enablement Services

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

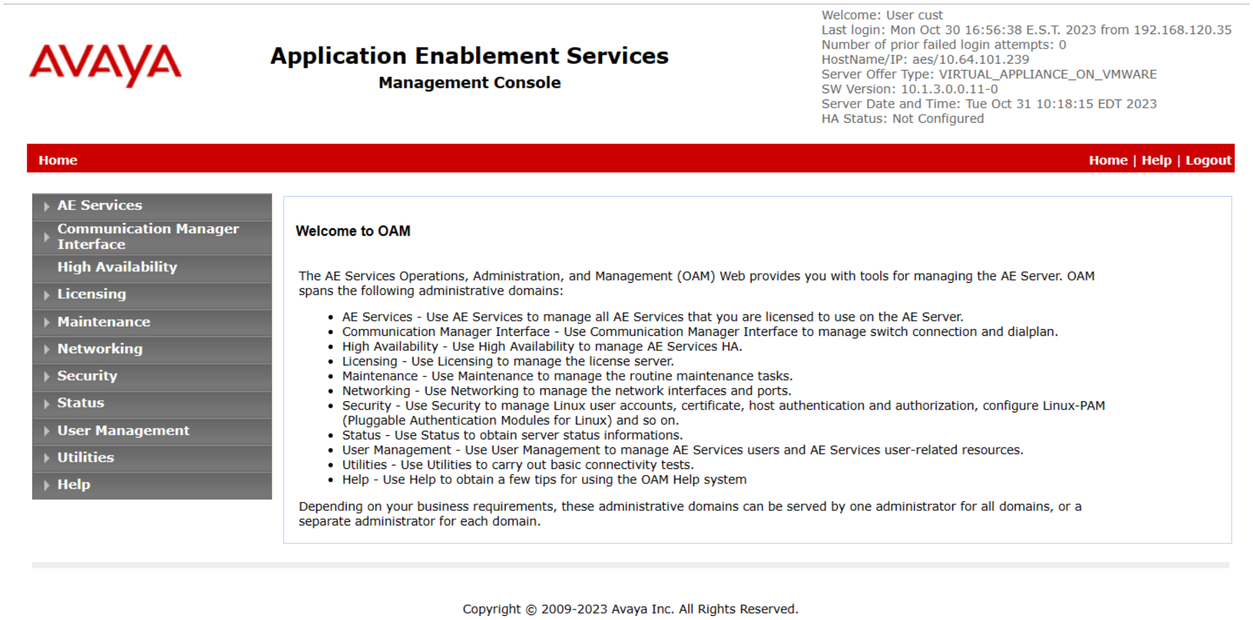
- Launch OAM Interface
- Verify License
- Administer TSAPI Link
- Administer TCP Settings
- Restart Service
- Obtain Tlink Name
- Administer User
- Verify Security Database

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.

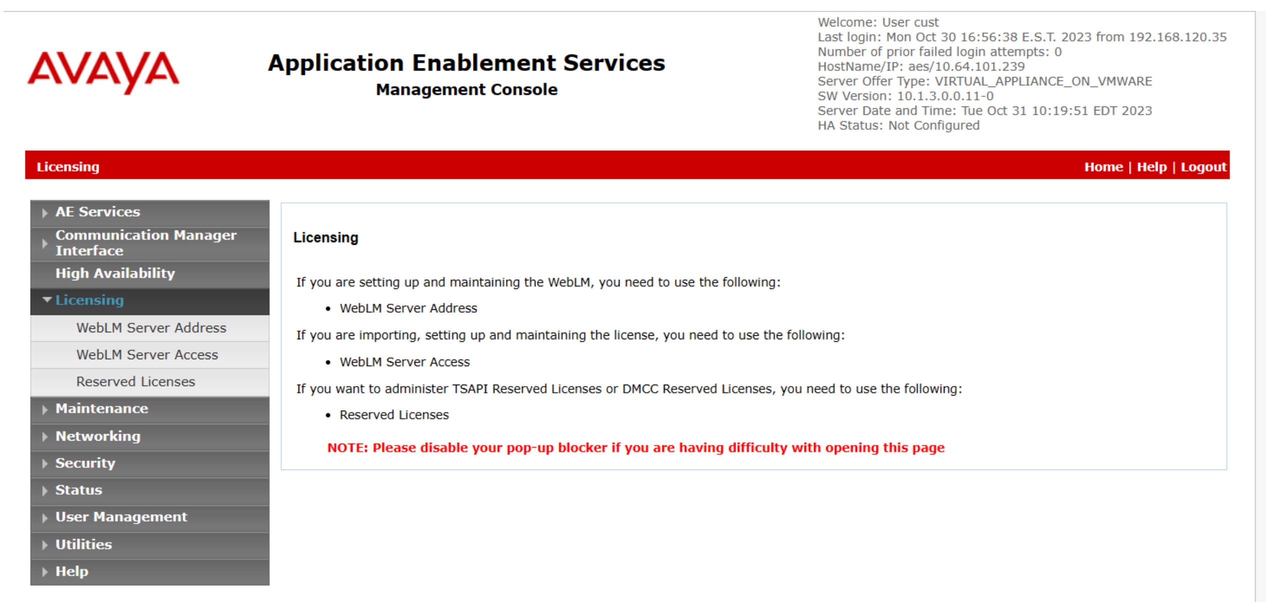


The **Welcome to OAM** screen is displayed next.



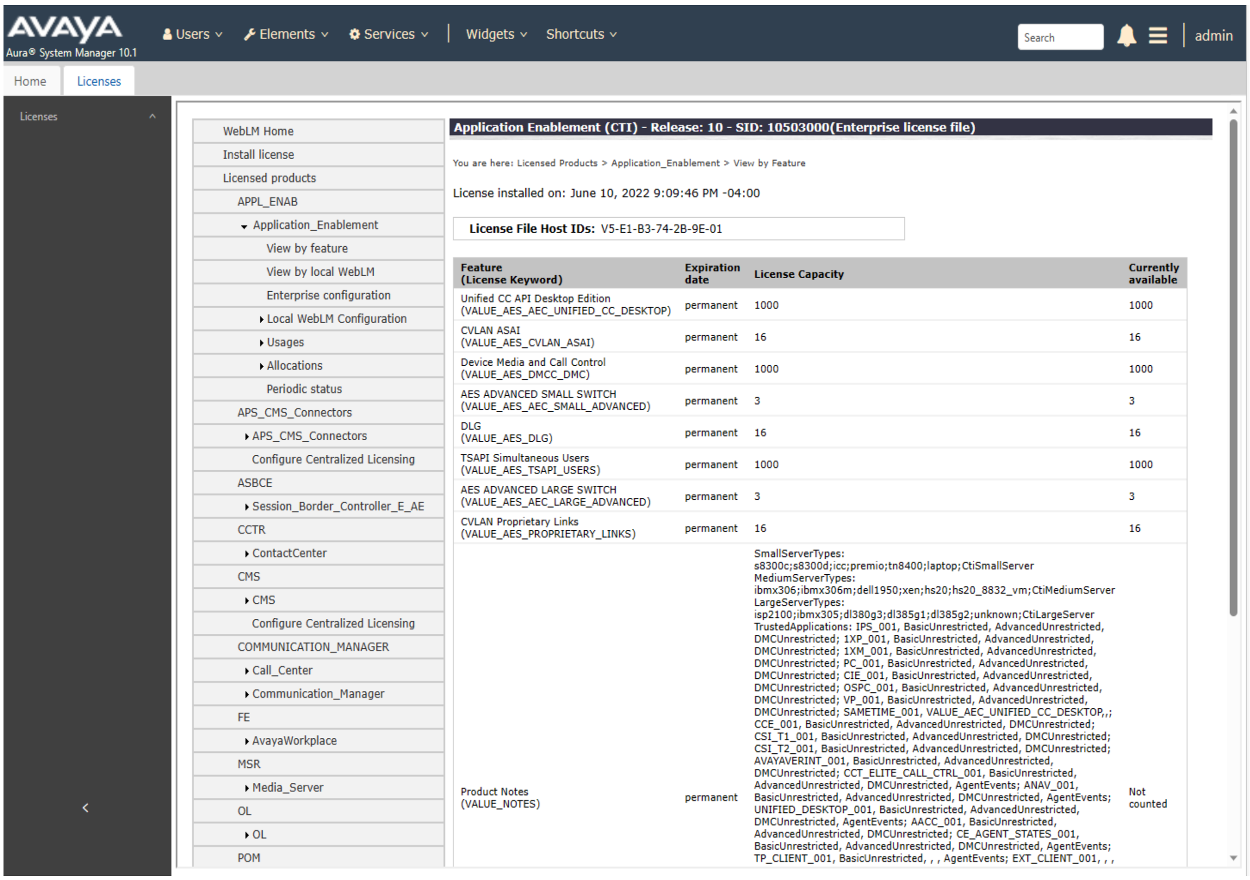
7.2. Verify License

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.



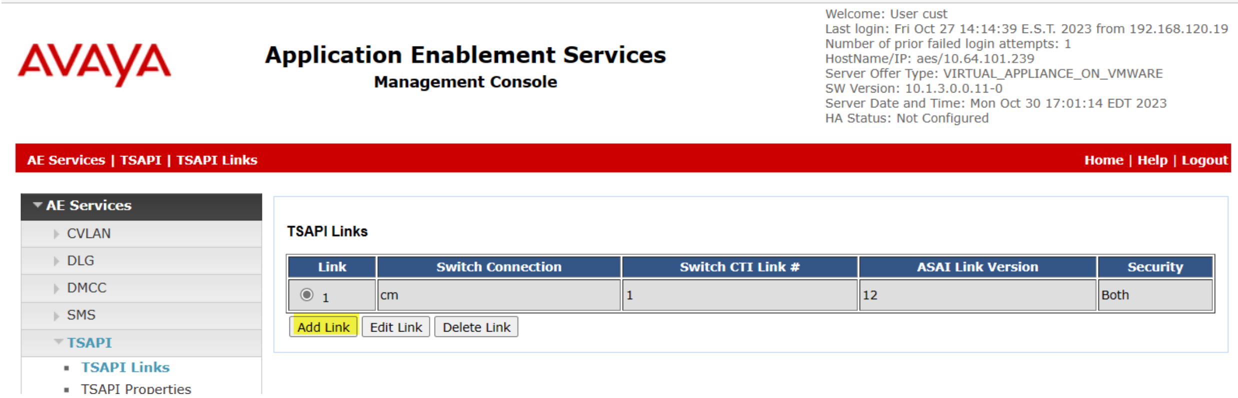
The **Web License Manager** screen below is displayed. Select **Licensed Products → APPL_ENAB → Application_Enablement** in the left pane to display the **Application Enablement (CTI)** screen in the right pane.

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 SMALL SWITCH** for the virtual server.

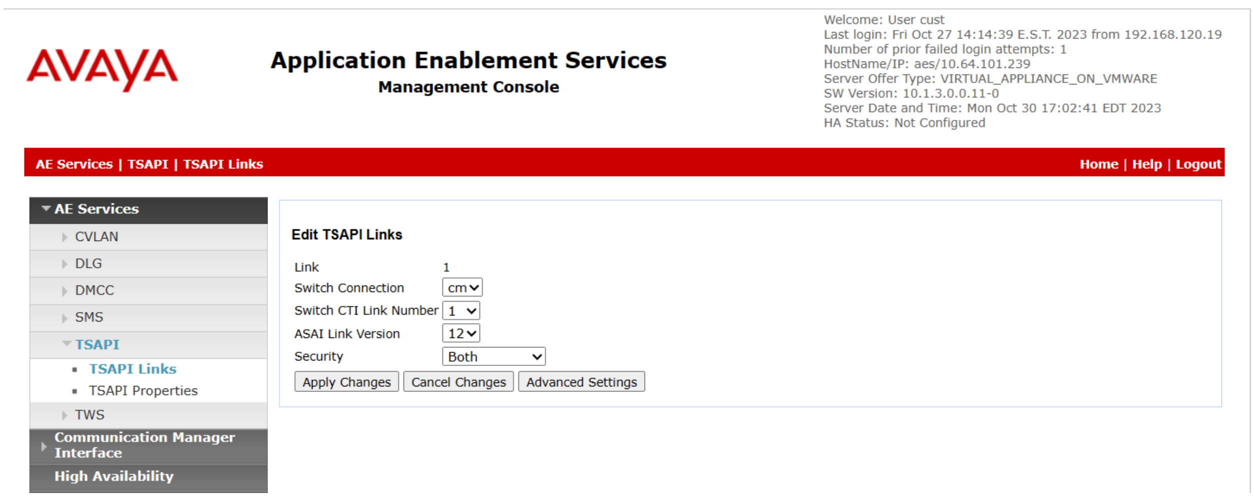


7.3. Administer TSAPI Link

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**.

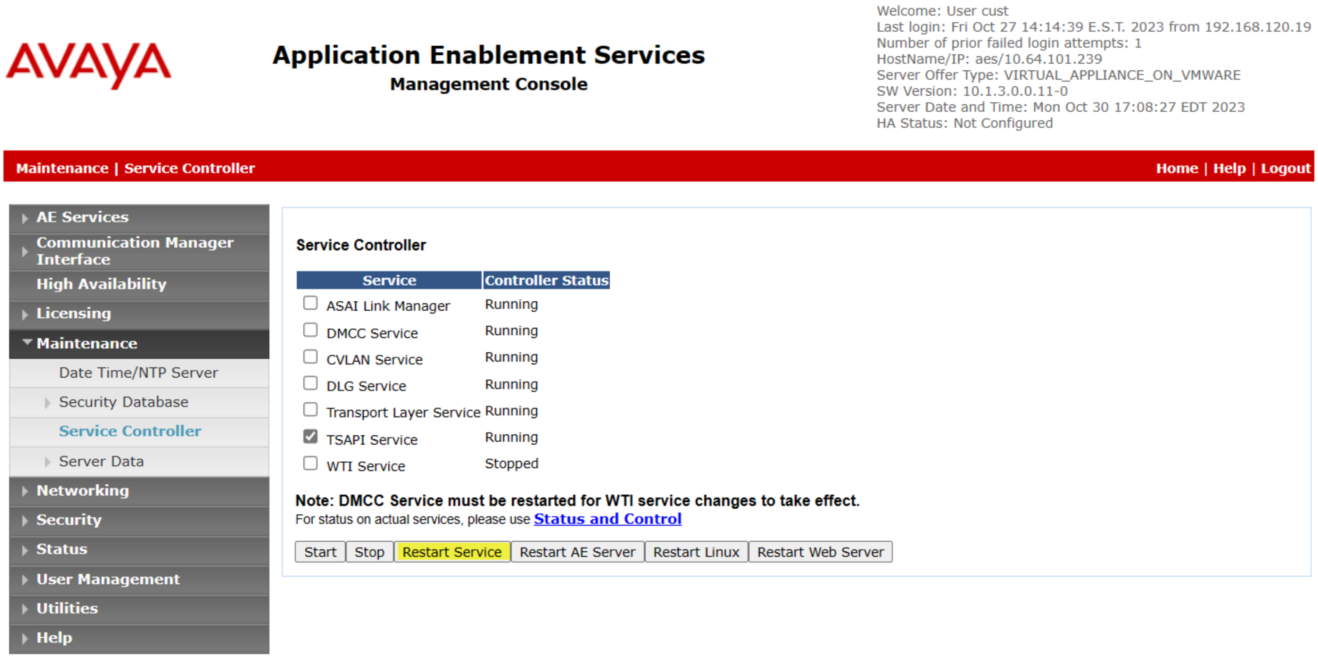


The **Add TSAPI Links** screen is displayed next. The **Link** field is only local to the Application Enablement Services server and may be set to any available number. For **Switch Connection**, select the relevant switch connection from the drop-down list. In this case, the existing switch connection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



7.4. Restart Service

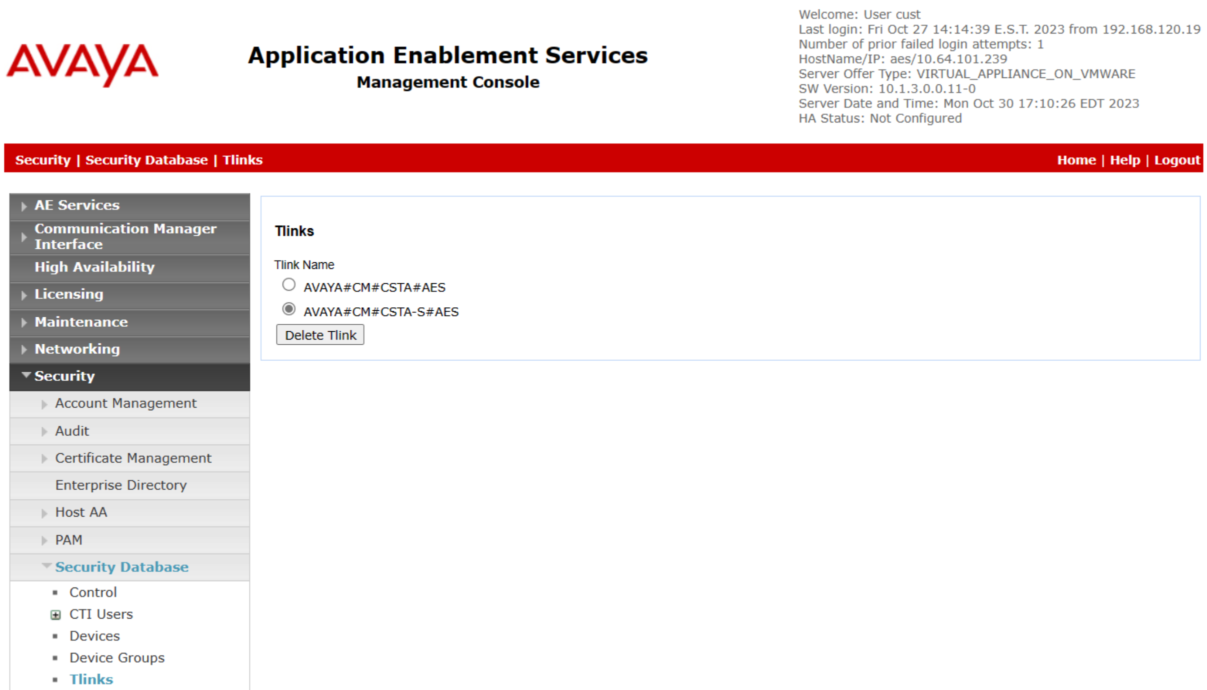
Select **Maintenance → Service Controller** from the left pane to display the **Service Controller** screen in the right pane. Check **TSAPI Service**, as shown below, and click **Restart Service**.


AVAYA
Application Enablement Services
Management Console
Welcome: User cust
Last login: Fri Oct 27 14:14:39 E.S.T. 2023 from 192.168.120.19
Number of prior failed login attempts: 1
HostName/IP: aes/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 10.1.3.0.0.11-0
Server Date and Time: Mon Oct 30 17:08:27 EDT 2023
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
ASAI Link Manager
Running
DMCC Service
Running
CVLAN Service
Running
DLG Service
Running
Transport Layer Service
Running
TSAPI Service
Running
WTI Service
Stopped
Note: DMCC Service must be restarted for WTI service changes to take effect.
For status on actual services, please use Status and Control
Start
Stop
Restart Service
Restart AE Server
Restart Linux
Restart Web Server

7.5. Obtain Tlink Name

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

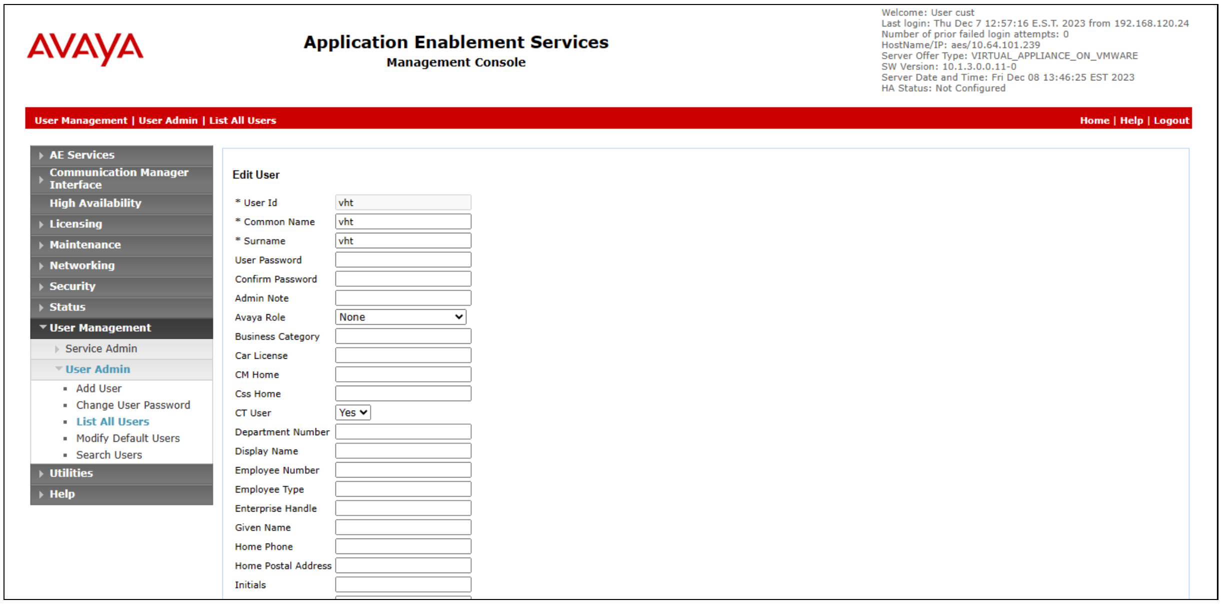
In this case, the associated Tlink name is "AVAYA#CM#CSTA# AES." Note the use of the switch connection "CM" from **Section 7.3** as part of the Tlink name.



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.

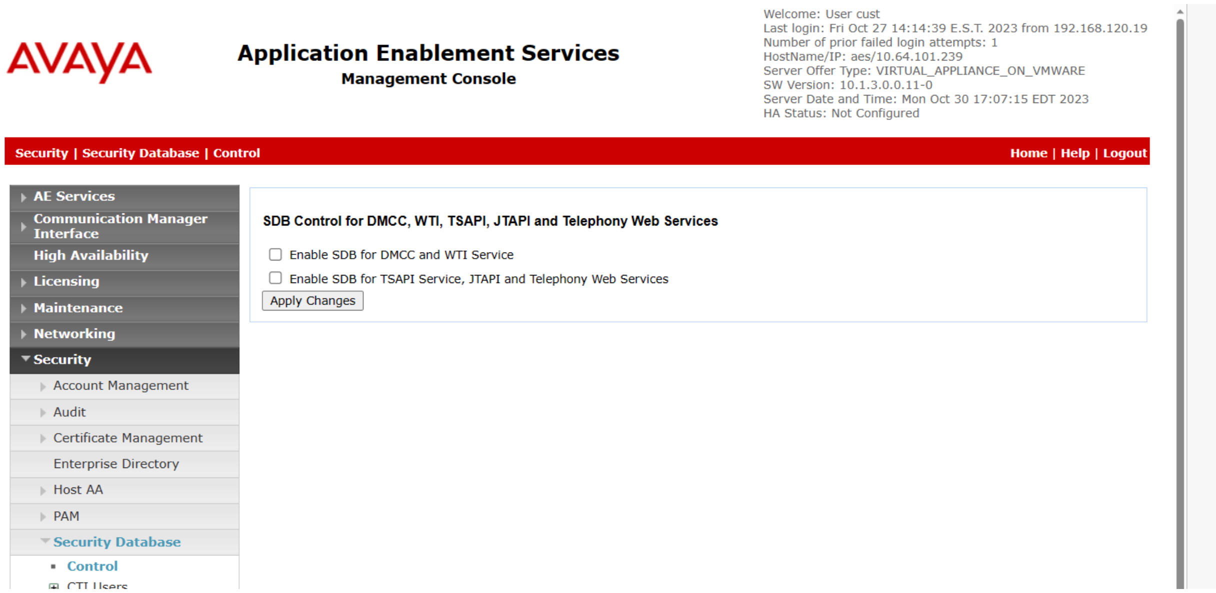
Enter desired values for **User Id**, **Common Name**, **Surname**, **User Password**, and **Confirm Password**. For **CT User**, select "Yes" from the drop-down list. Retain the default value in the remaining fields.



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** retained the default value of unchecked. In the event that security database is used by the customer with this parameter already enabled, then follow [2] to configure access privileges for the Callback user from **Section 7.6**.

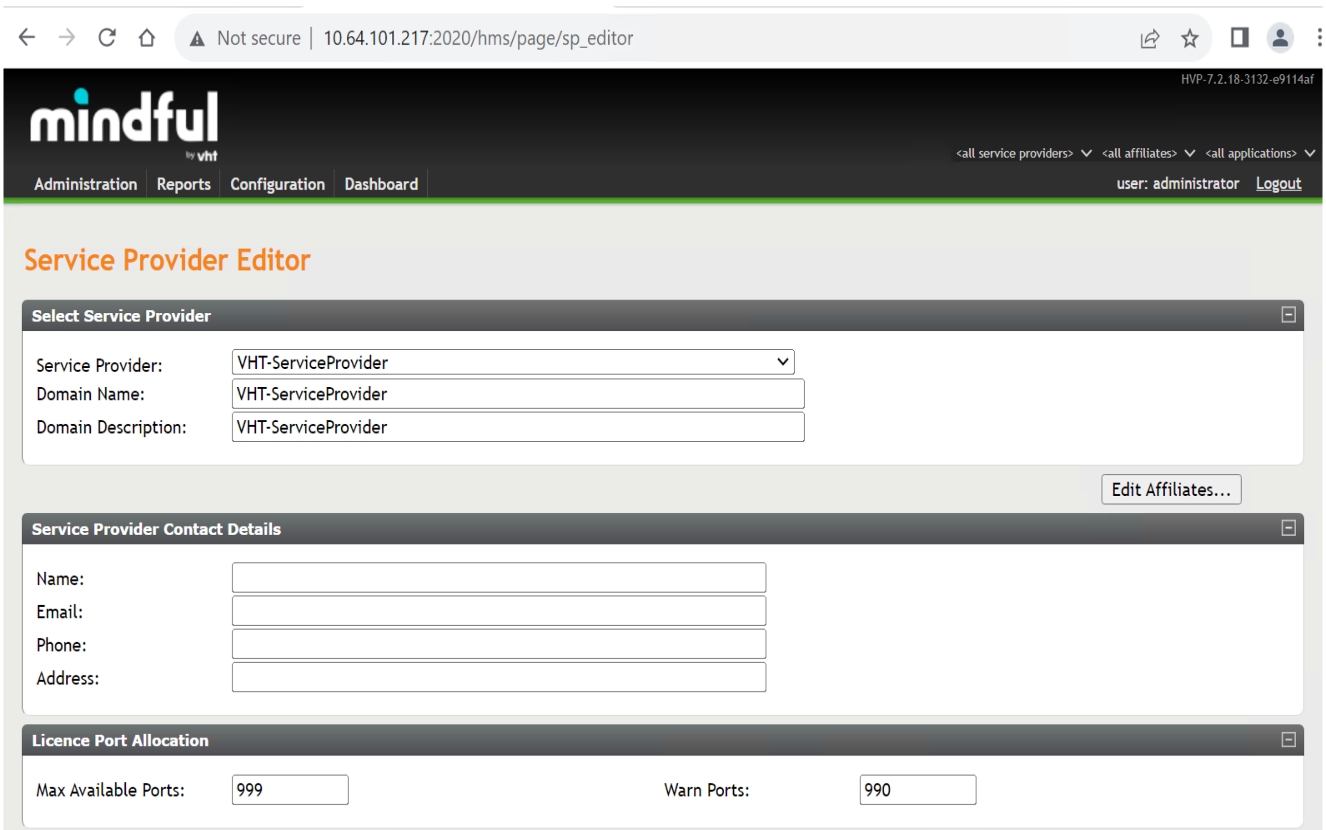


8. Configure VHT Interactive Voice Gateway (IVG)

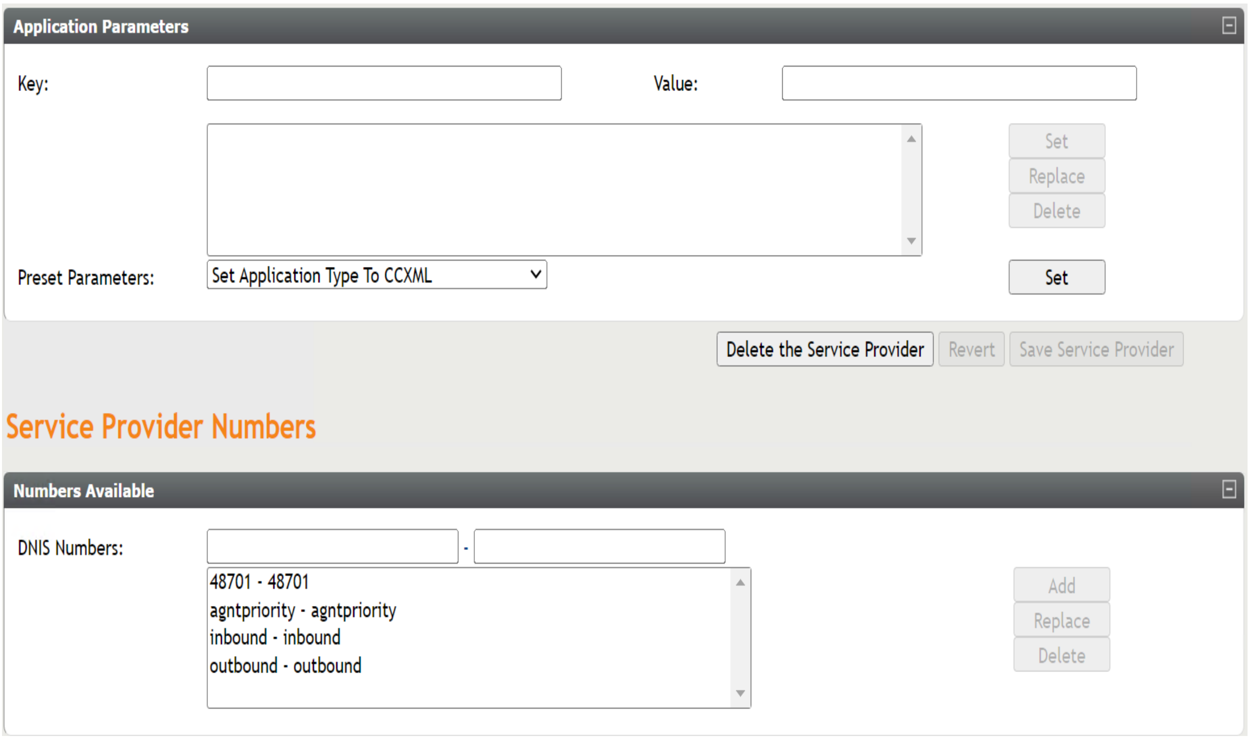
Configuration is accomplished by accessing the browser-based IVG management system using the URL "http://<*ip-address*>*:2020*", where <*ip-address*> is the IP address of the IVG server. Log in with the appropriate credentials (not shown).

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

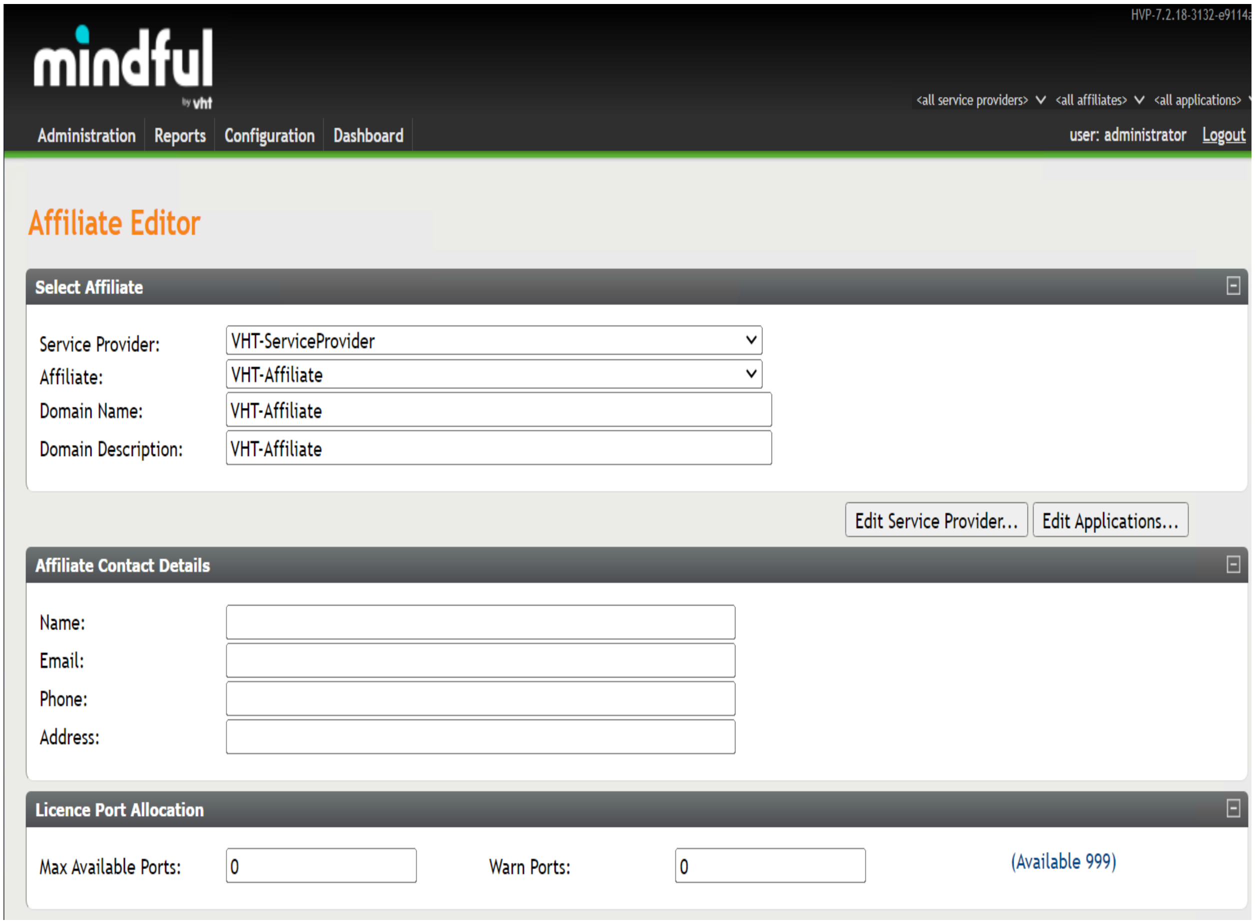
Note: Alternatively, the VHT IVG application provisioning can be configured automatically during the install using the IVG installer.



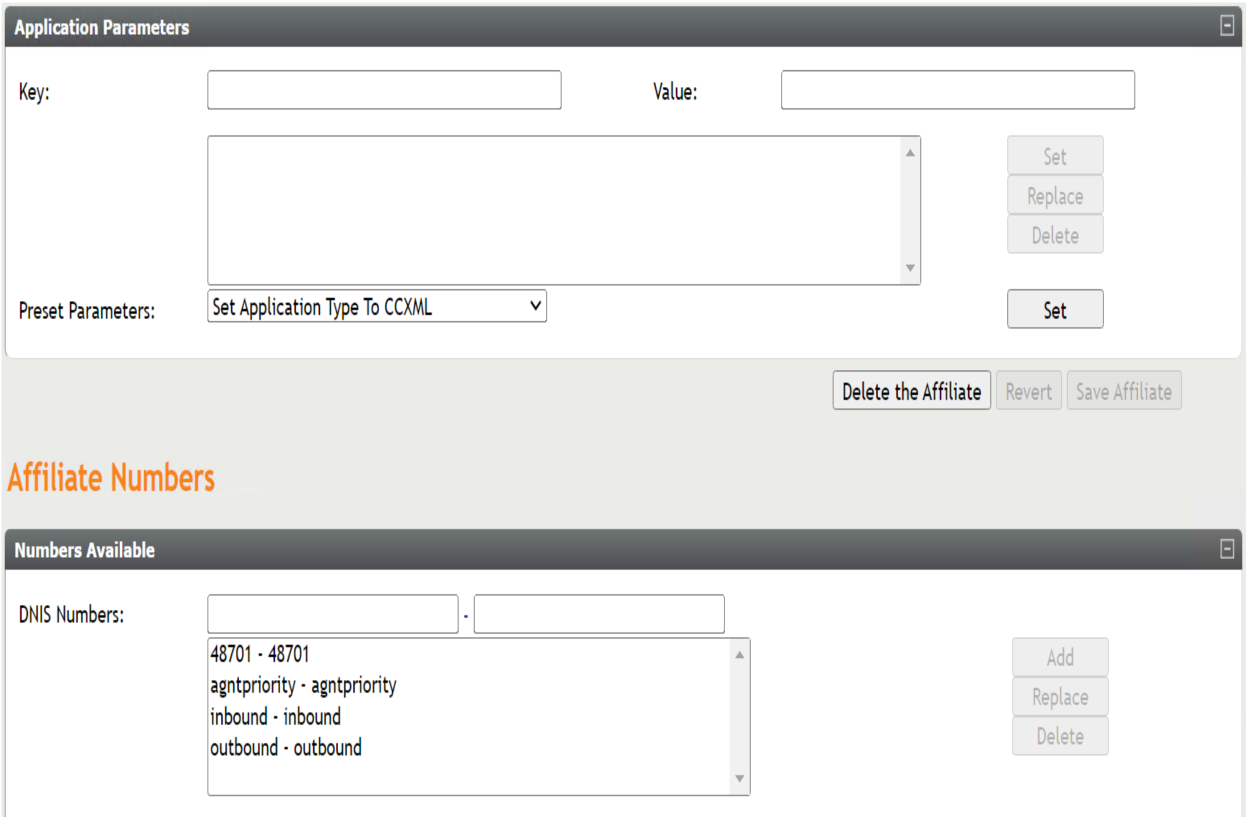
Scroll down to the **Application Parameters** section and click **Save Service Provider**. In the **Numbers Available** section, add the **DNIS Numbers**. The DNIS numbers were set to 4*8701*, which is used to route calls to IVG, and *outbound* as shown below.



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

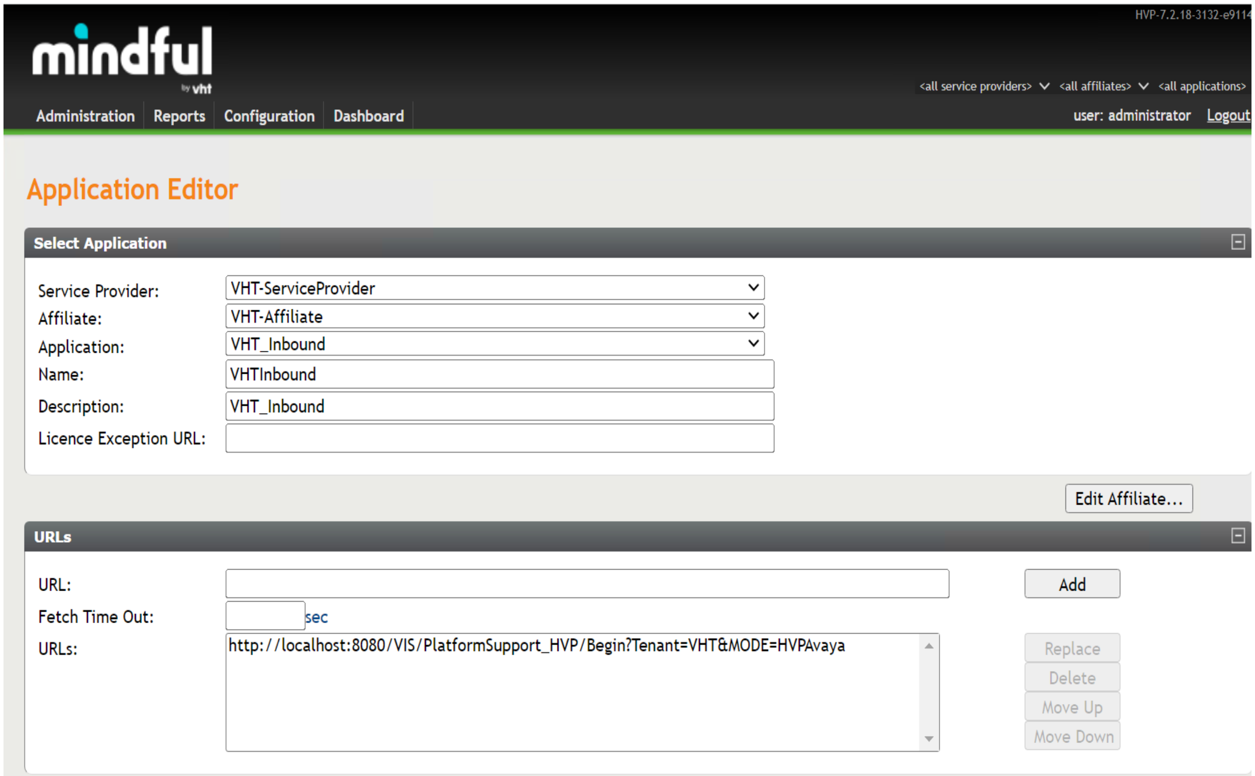


Scroll down to the **Application Parameters** section and click **Save Affiliate**. In the **Numbers Available** section, add the **DNIS Numbers**. The DNIS numbers were set to *48701*, which is used to route calls to IVG, and *outbound* as shown below.



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

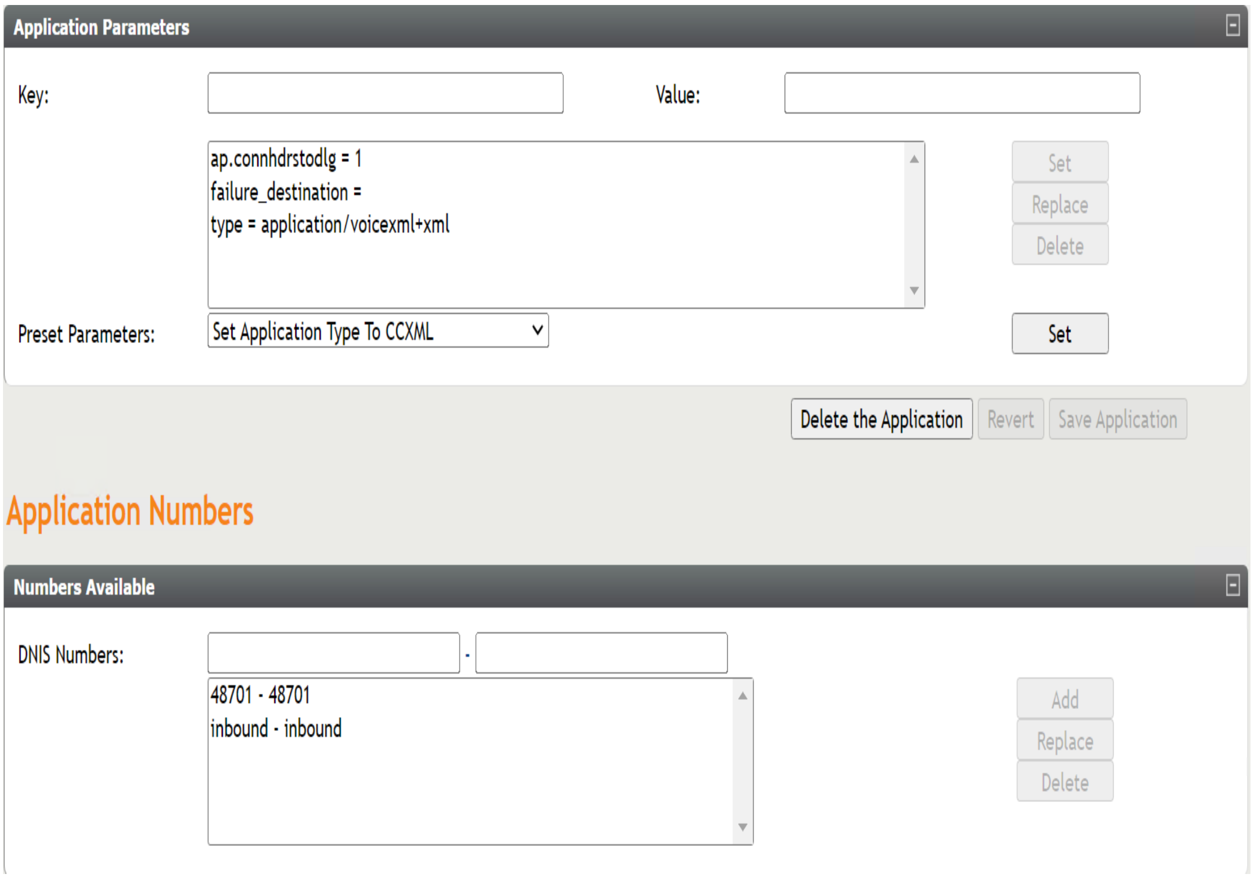
Scroll down to the URLs section and insert the appropriate **URL** (e.g., *http://localhost:8080/VIS/PlatformSupport_HVP/Begin?Tenant=VHT&MODE=HVPAvaya*).



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

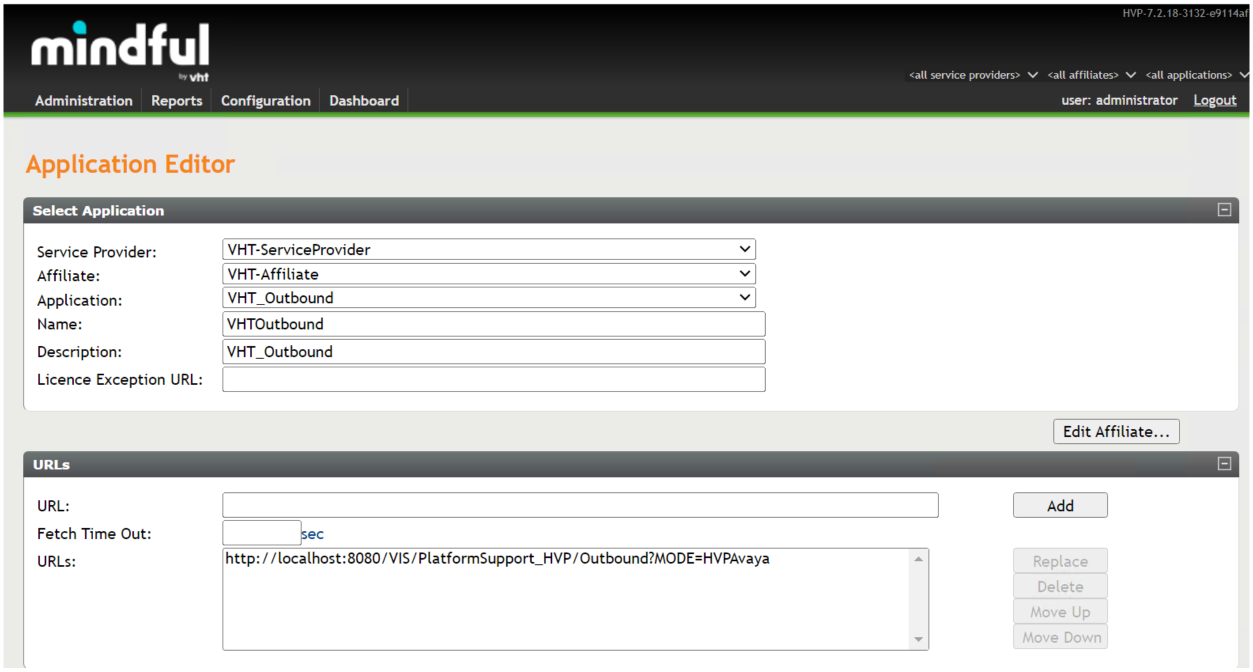
- **ap.connhdrstodlg** = *1*
- **type** = *application/voicexml+xml*

Click **Save Application**. In the **Numbers Available** section, add the **DNIS Number**. The DNIS number that was added was *48701* as shown below.



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

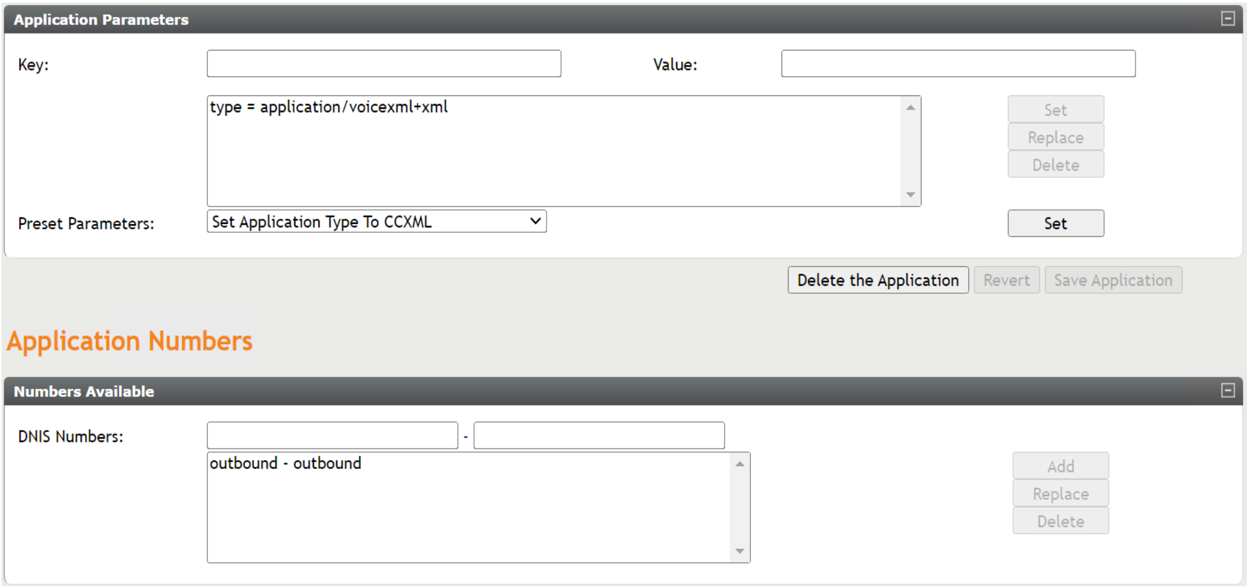
Scroll down to the URLs section and insert the appropriate **URL** (e.g., *http://localhost:8080/VIS/PlatformSupport_HVP/Outbound?MODE=HVPAvaya*).



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

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

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



Lastly, open the **/etc/VirtualHold/toolkit.properties** file and set the **com.virtualhold.toolkit.baseurl** parameter to *http://10.64.101.218/VHTPlatformWS-V5/*, which specifies the IP address of the Callback server as shown below. This allows IVG to communicate with the Callback system.

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

# URL for the Platform Toolkit web services
# Change the [PTK_server_address] and [PTK_port] to the address and port of the server
where the Platform Toolkit software resides
# For example, http://10.10.0.158:7000/VHTPlatformWS-v5/
# Ensure the path and VHTPlatformWS version is correct by opening it in a web browser
com.virtualhold.toolkit.baseurl=http://10.64.101.218/VHTPlatformWS-v5/
```

9. Configure VHT Callback

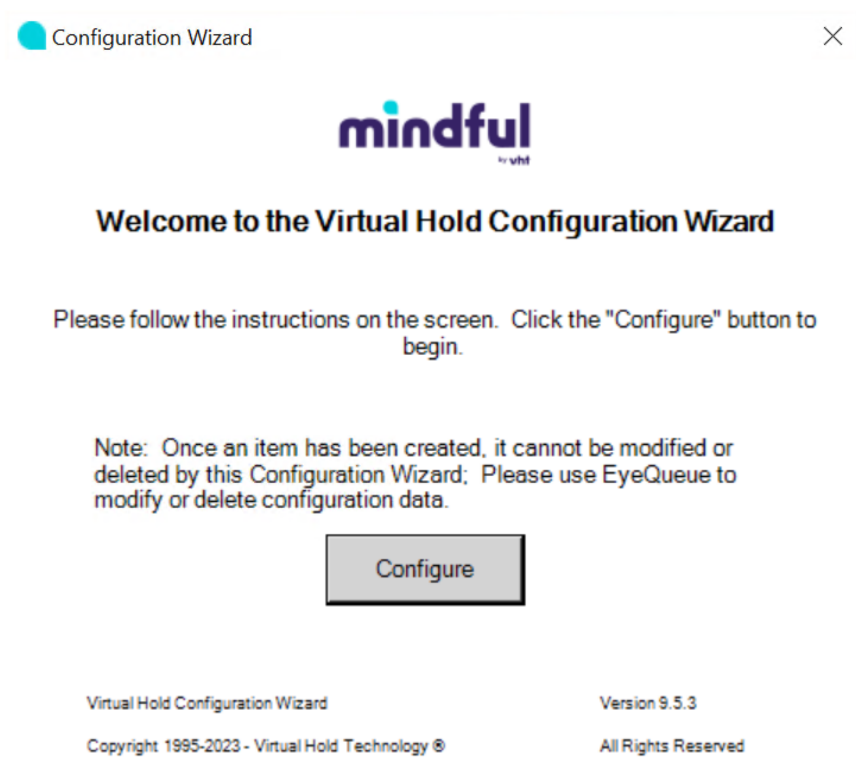
This section provides the procedures for configuring Callback. The procedures include the following areas:

- Launch VHT Configuration Wizard
- Administer Switch Connection
- Administer IVR Servers
- Administer Queues
- Administer Callback and Holding Queues
- Administer Incoming Extensions
- Administer Phone Number Configurations
- Administer Segment Variables
- Modify `site.config` File
- Configure TSAPI Real-Time Adapter

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

9.1. Launch Configuration Wizard

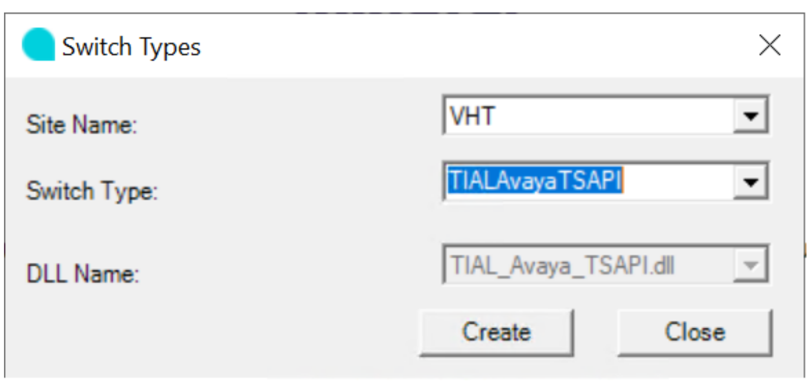
From the Callback server, navigate to **Start** → **All Programs** → **Virtual Hold Technology** → **Configuration** → **VHT Configuration Wizard** to launch the wizard. The **Welcome to the Virtual Hold Configuration Wizard** screen is displayed. Click **Configure** to proceed.



9.2. Administer Switch Connection

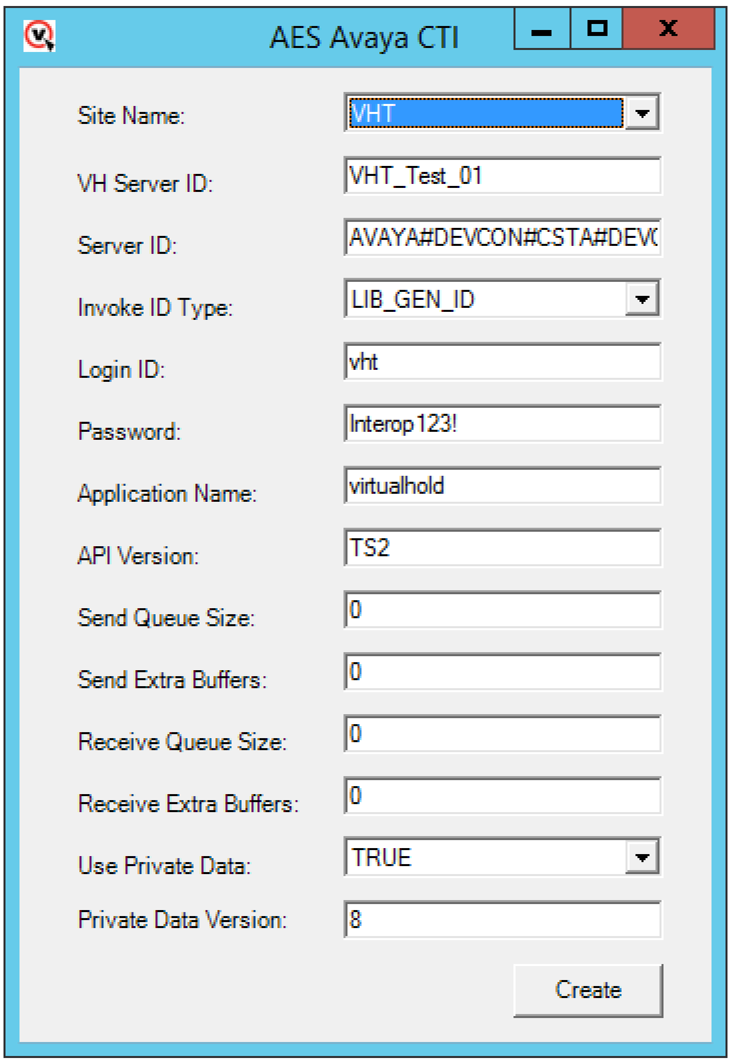
The **Switch Connection** screen is displayed. Click **Add** to create a connection to the switch.

The **Switch Types** screen is displayed next. For **Switch Type**, select *TIALAvayaTSAPI* from the drop-down list. Note that the value of **Site Name** was automatically populated and was created as part of installation. Retain the default values in the remaining fields.



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

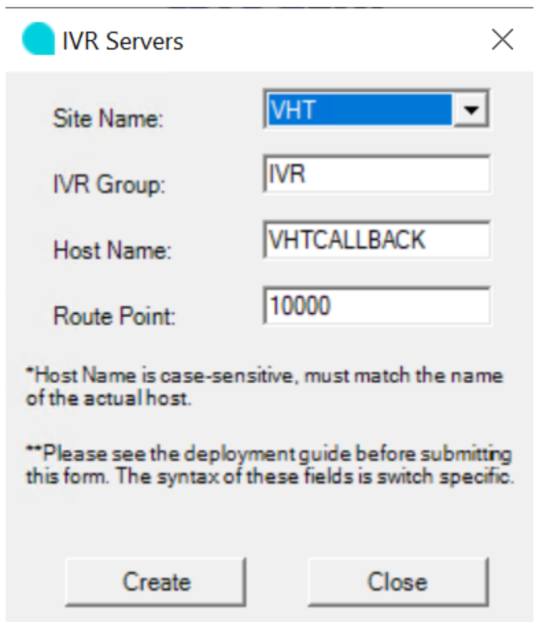
- **VH Server ID:** A descriptive name.
- **Server ID:** The Tlink name from **Section 7.5**.
- **Login ID:** The Callback user credentials from **Section 7.6**.
- **Password:** The Callback user credentials from **Section 7.6**.(The displayed value is for example purposes only and not normally displayed)
- **Send Extra Buffers:** The desired extra buffers.
- **Receive Queue Size:** The desired queue size.
- **Use Private Data:** Set to *TRUE*.
- **Private Data Version:** Set to '8'.



9.3. Administer IVR Servers

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

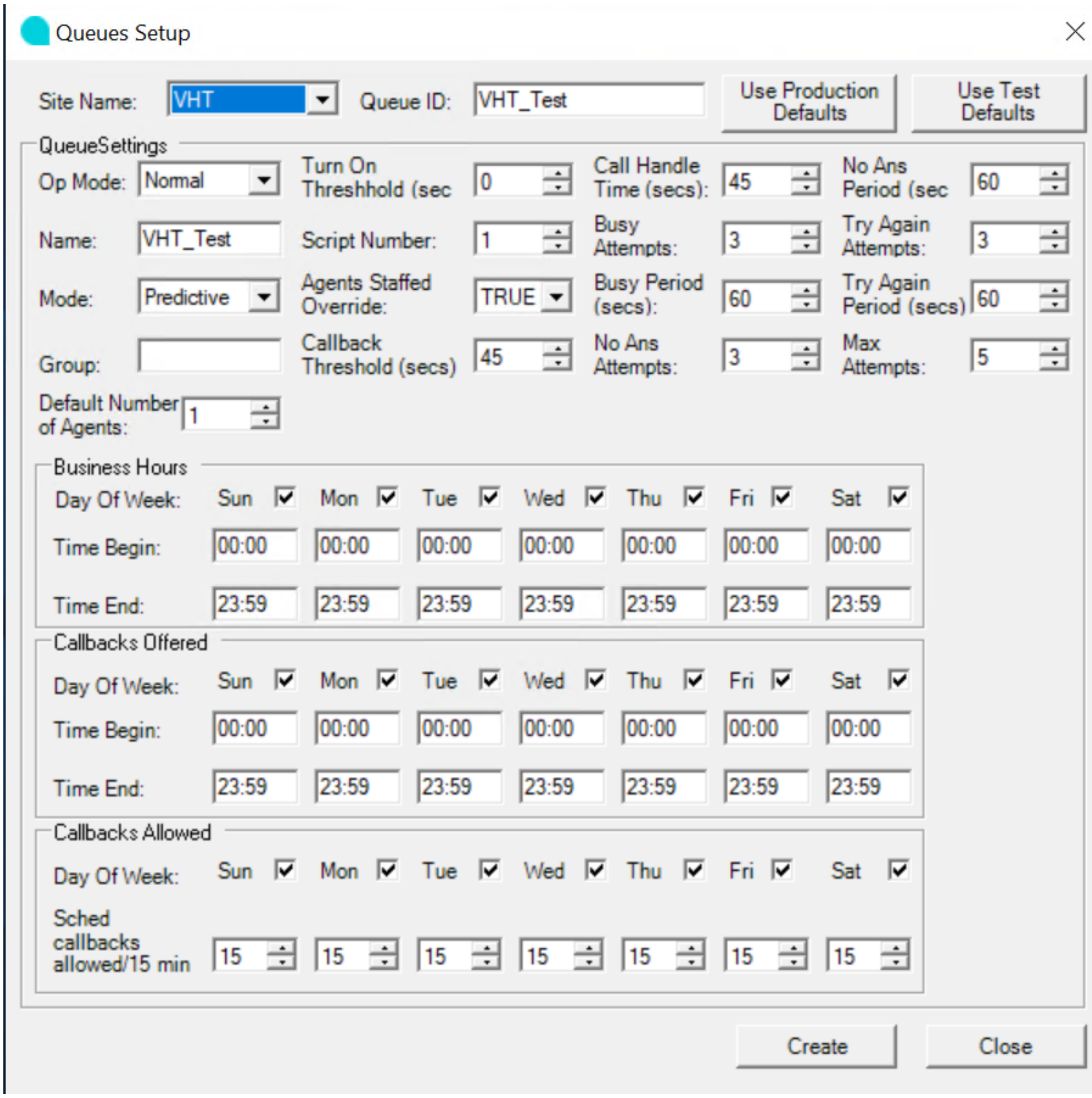
The screen below is displayed next. Set **Host Name** to the host name of the Callback server. Even though IVG is the IVR server, the Callback server initiates the callback. The **Route Point** is just a place holder at this point.



9.4. Administer Queues

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

The **Queues Setup** screen is displayed next. The screenshot below shows the values used in the compliance testing.



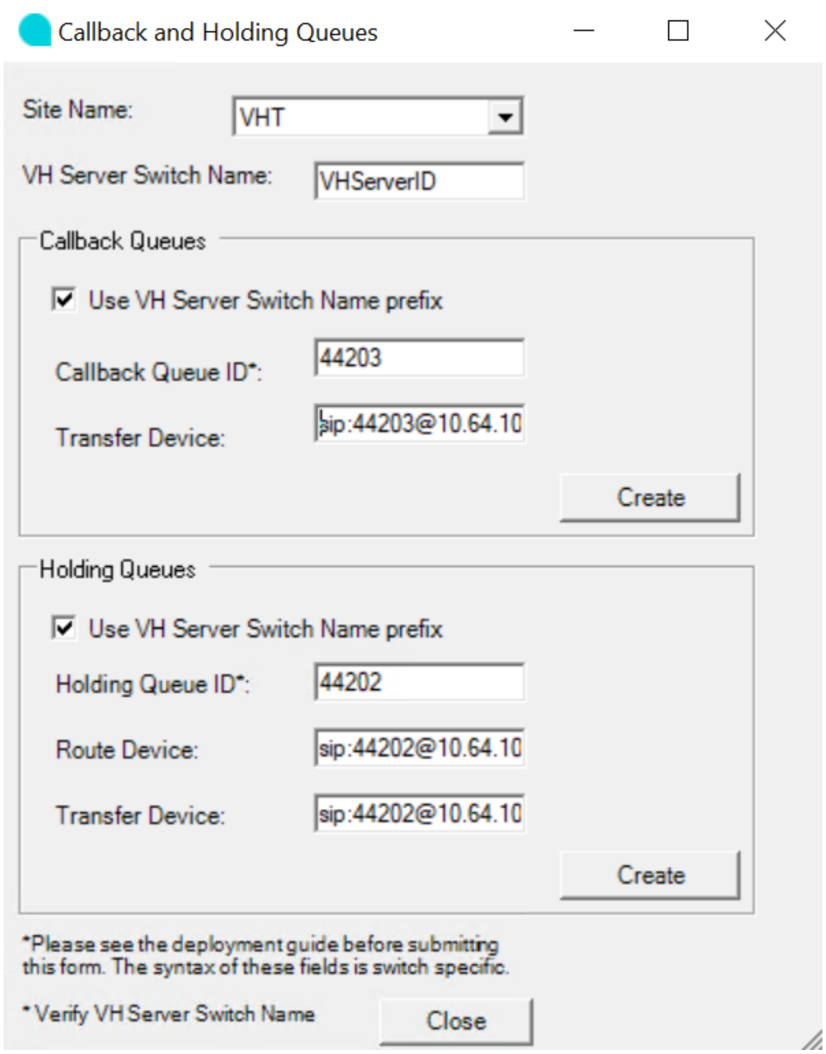
9.5. Administer Callback and Holding Queues

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

In the **Callback Queues** sub-section, enter the Callback VDN extension from **Section 5.4.3** for **Callback Queue ID**. For **Transfer Device**, enter "sip:x@y," where "x" is the Callback VDN extension, and "y" is the IP address of the Session Manager signaling interface (e.g., *sip:44203@10.64.101.217*).

In the **Holding Queues** sub-section, enter the Hold VDN extension from **Section 5.4.2** for **Holding Queue ID** and **Route Device**. For **Transfer Device**, enter "sip:x@y," where "x" is the Hold VDN extension, and "y" is the IP address of the Session Manager signaling interface (e.g., *sip:44202@10.64.101.217*).

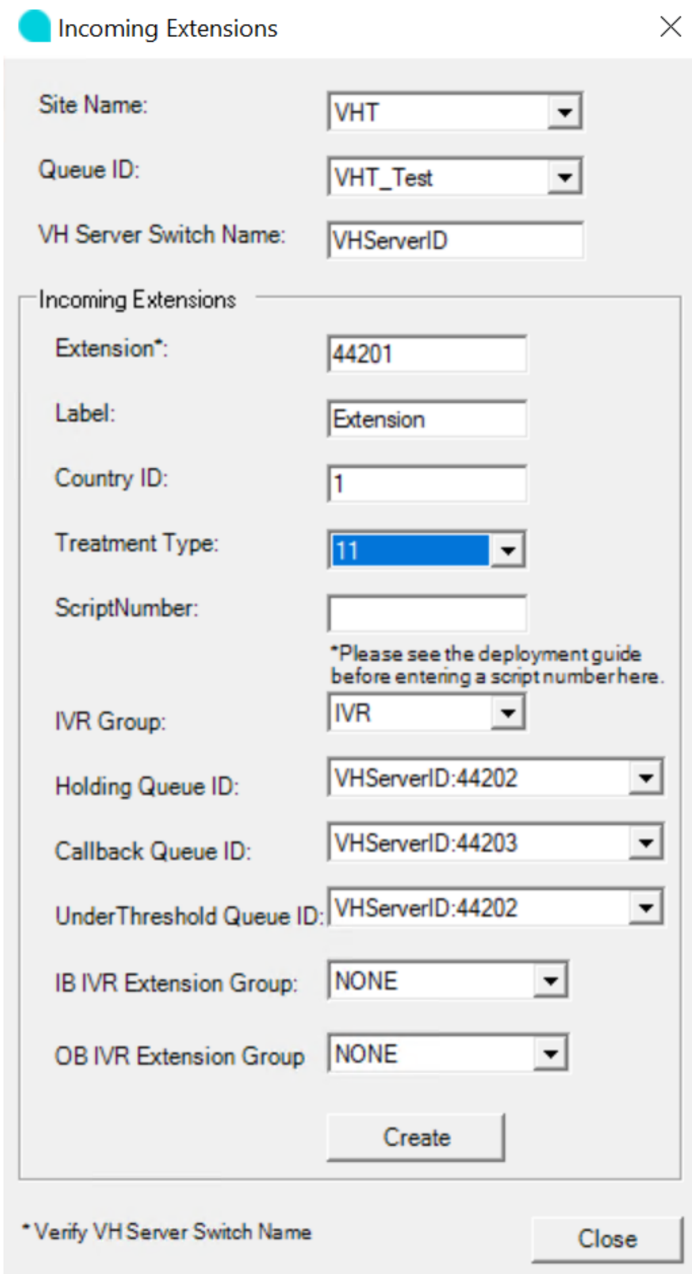
Retain the default values for the remaining fields.



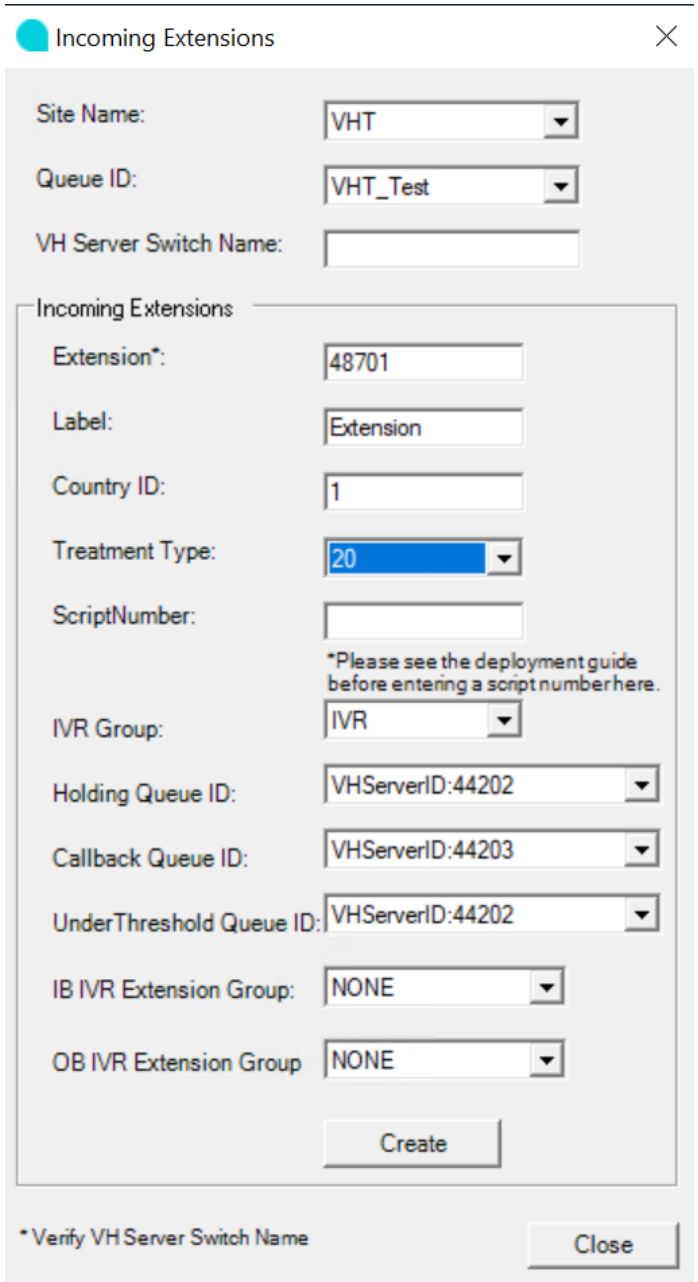
9.6. Administer Incoming Extensions

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

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



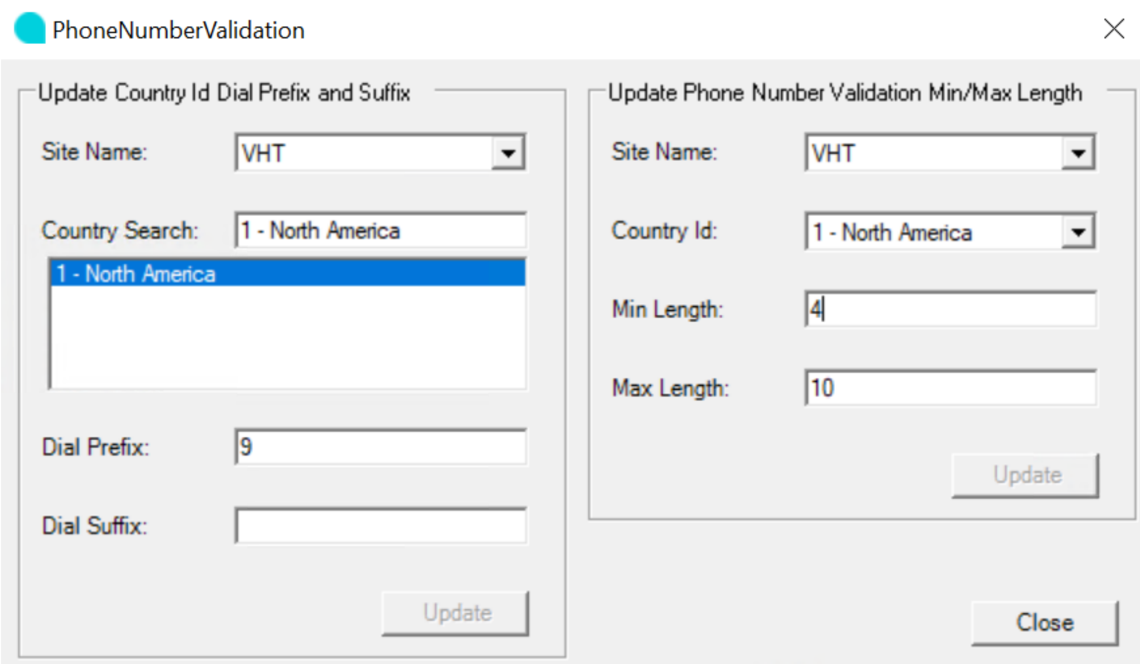
Repeat the same procedures to create an incoming extension for IVG. For **Extension**, enter the extension assigned to IVG, in this case *48701*. For **Treatment Type**, select *20*. Retain the default values in the remaining fields, including blank for **VH Server Switch Name**.



9.7. Administer Phone Number Configurations

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

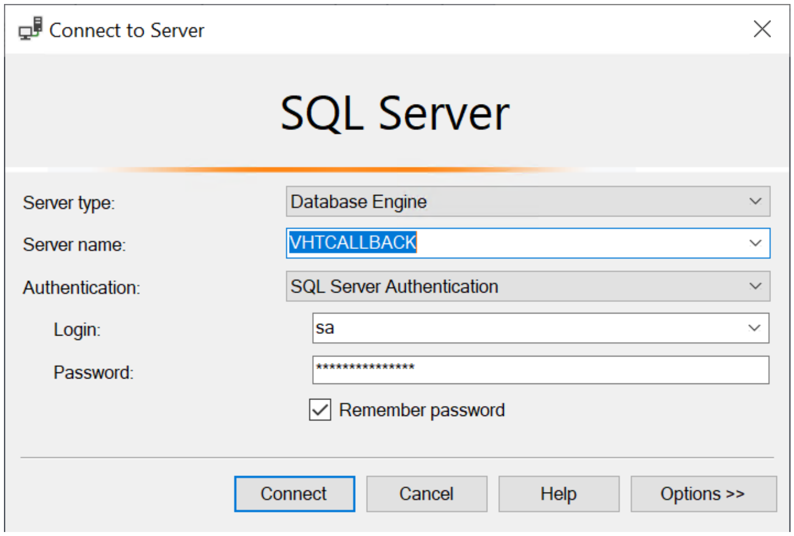
For **Country Search**, locate and select the applicable country as shown below. Below shows the default values for the system, for the compliance test, the Min Length field was modified to '5' to allow callbacks to 5-digit extensions corresponding to local IP stations and the Max Length field was modified to '12' to allow callbacks to 10-digit PSTN number prepended with a '+1' prefix code. Retain the default values in the remaining fields.



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

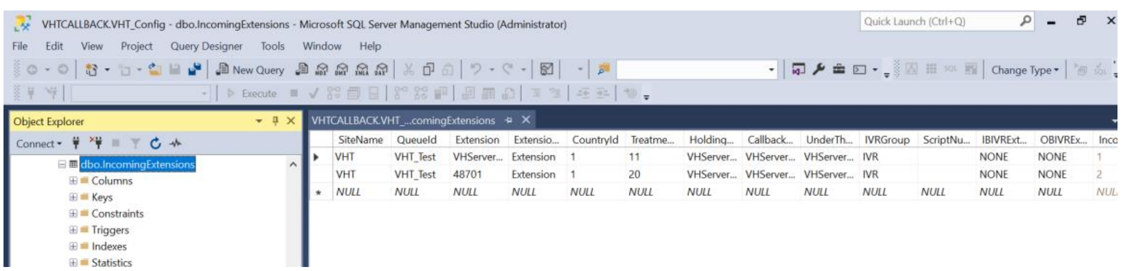
9.8. Administer Segment Variables

From the Callback server, navigate to **Start → Apps → Microsoft SQL Server 2019 → SQL Server Management Studio** to launch and connect to the SQL server.

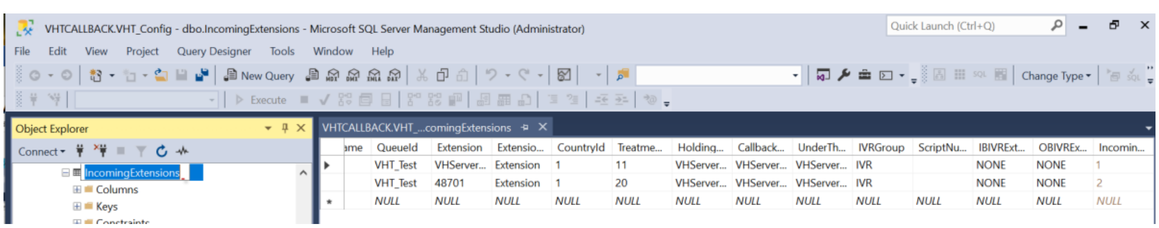


Navigate to **Databases → VHT_Config → Tables → dbo.IncomingExtensions** in the left pane, right-click the entry and select **Edit Top 200 Rows**.

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



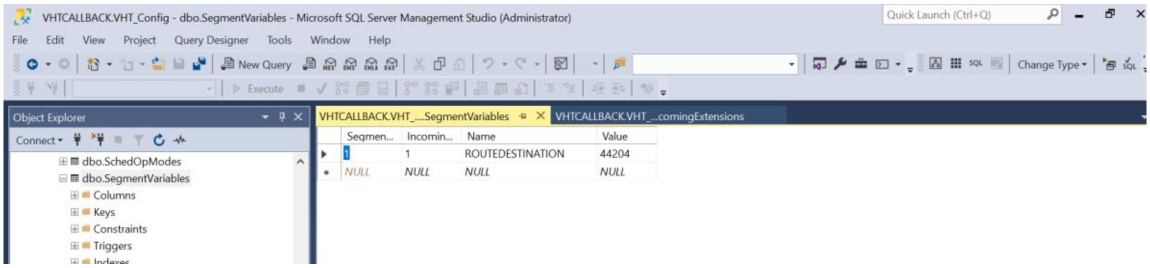
Scroll to the right to make a note of the associated **IncomingExtensionsId** value, in this case '1007', as shown below.



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

- **IncomingExtensionsId:** The value from the **dbo.IncomingExtensions** table from above.
- **Name:** Set to *ROUTEDESTINATION*.
- **Value:** Set to the route VDN extension *44204*.

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



9.9. Modify `site.config` File

Open the `site.config` file located in the `C:\Program Files (x86)\Virtual Hold Technology\Peripheral Monitor\` directory of the Callback server and modify the entries in bold to include the Callback server IP address (10.64.101.218), the IVG IP address (10.64.101.217), or the Session Manager IP address (10.64.101.238). The **ani** should include *<ani>@<Session Manager IP Address>*, where *<ani>* is the Automatic Number Identifier of the Callback server (e.g., *8005555555@10.64.101.217*). The other entries may be left with their default values.

```
{vht_outbound_contact_client,
    [
      {voice_platform, ivg_plugin},
      {ivg_environment, avaya},
      {queue_manager_connection_ping_in_seconds, 15},
      {ivr_group_name, "IVR"},
      {ivr_server_name, "harbinger"},
      {ivr_port_send_interval_ms, 2000},
      {disposition_url, "http://10.64.101.218:4153/vht/occ"},
      {disposition_timeout, 55000},
      {exclude_connections_on_failure, true},
      {time_to_exclude_on_failure_ms, 150000},
      {default_connection_attributes,
        [
          {outdial_http_options,
            [
              {timeout, 5000},
              {connect_timeout, 5000}
            ]
          },
          {request_header,
            [
              {"Accept", "application/x-www-form-urlencoded"},
              {"Content-Type", "application/x-www-form-urlencoded"}
            ]
          },
          {enable_amd, true},
          {ring_no_answer_timeout, 50000},
          {ccxml_fetch_timeout, 5000},
          {tenant, "VHT"}
        ]
      },
      {load_balanced_connections,
        [
          [
            {outdial_url, "http://10.64.101.217:8040/createsession"},
            {sip_endpoint, "10.64.101.217"},
            {failure_destination, ""},
            {dnis, "outbound"},
            {vht_ccis_uri, "http://10.64.101.217:8080/CCIS/vht_hvp.ccxml"},
            {ani, "8005555555@10.64.101.217"},
            {node_id, 7},
            {agent_priority_dnis, "agntpriority"},
            {outreach_dnis, "outreach"}
          ]
        ]
      }
    ]
  }
```

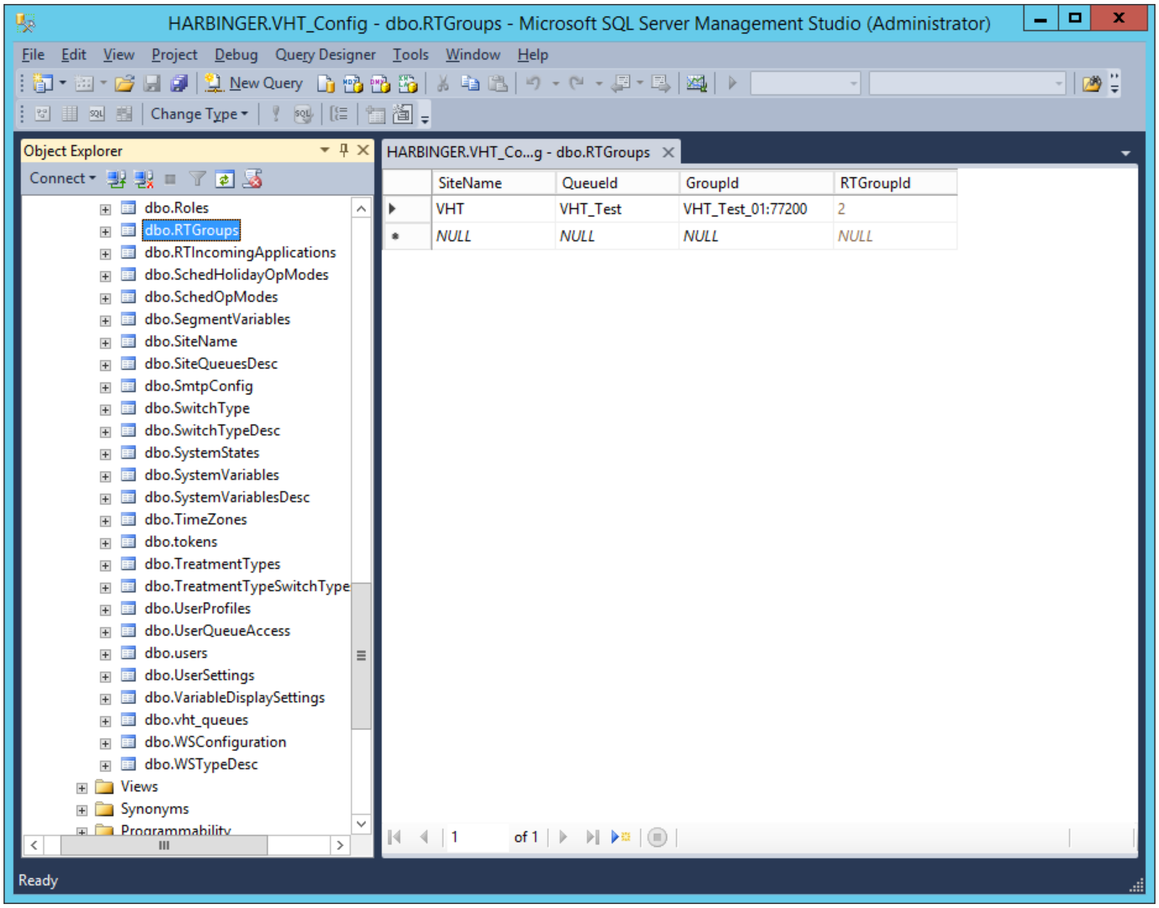
9.10. Configure TSAPI Real-Time Adapter

The Callback TSAPI Real-Time Adapter captures queue statistics, such as agent status of a monitored skill/split and can be displayed as shown in **Section 11.4**.

Open the `VHT_TsapiRealTimeAdapter_Console.exe.config` file located in the `C:\Program Files (x86)\Virtual Hold Technology\RealTimeAdapter\` directory of the Callback server and modify the entries in bold to include the Callback server IP address (10.64.101.218) 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>
        </sectionGroup>
    </configSections>
    <VHTConfiguration>
        <vhtLogging>
            <application level="10" name="TsapiRealTimeAdapter"
logFilePath="C:\Program Files (x86)\Virtual Hold Technology\VHLogs"/>
        </vhtLogging>
        <vhtCommunication>
            <QMCL reconnectIntervalSeconds="3">
                <Connections>
                    <Connection connectionType="Primary">
                        <Server ipAddress="10.64.101.218" port="6999"/>
                        <Client ipAddress="10.64.101.218" port="0"/>
                    </Connection>
                </Connections>
            </QMCL>
        </vhtCommunication>
    </VHTConfiguration>
    <appSettings>
        <add key="VhqmwsUrl" value="http://10.64.101.218/VHQMWS/VHQMWS.asmx"/>
        <add key="SiteName" value="VHT"/>
        <add key="FrequencyMS" value="3000"/>
        <add key="UseDefaultsOnConnectionLost" value="false"/>
    </appSettings>
    <startup>
        <supportedRuntime version="v4.0" sku=".NETFramework,Version=v4.6.1"/>
    </startup>
</configuration>
```

Next, launch **SQL Server Management Studio** to launch and connect to the SQL server. Navigate to **Databases → VHT_Config → Tables → dbo.RTGroups** in the left pane, right-click the entry and select **Edit Top 200 Rows**. Ensure that an entry exists with the appropriate **SiteName**, **QueueId**, and **GroupID**, which includes the VH server ID and hunt group extension (e.g., *VHT_Test_01:77200*) as shown below.



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

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

11. Verification Steps

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

11.1. Verify Avaya Aura® Communication Manager

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

```
status aesvcs cti-link

                          AE SERVICES CTI LINK STATUS

CTI   Version  Mnt   AE Services      Service       Msgs
Link           Busy  Server           State         Sent     Rcvd

1     12        no    aes       established   134      134
```

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

```
status trunk 66

                             TRUNK GROUP STATUS

Member   Port     Service State      Mtce Connected Ports
                                     Busy

0066/001 T00001   in-service/idle    no
0066/002 T00002   in-service/idle    no
0066/003 T00003   in-service/idle    no
0066/004 T00004   in-service/idle    no
0066/005 T00005   in-service/idle    no
0066/006 T00006   in-service/idle    no
0066/007 T00007   in-service/idle    no
0066/008 T00008   in-service/idle    no
0066/009 T00009   in-service/idle    no
0066/010 T00010   in-service/idle    no
```

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

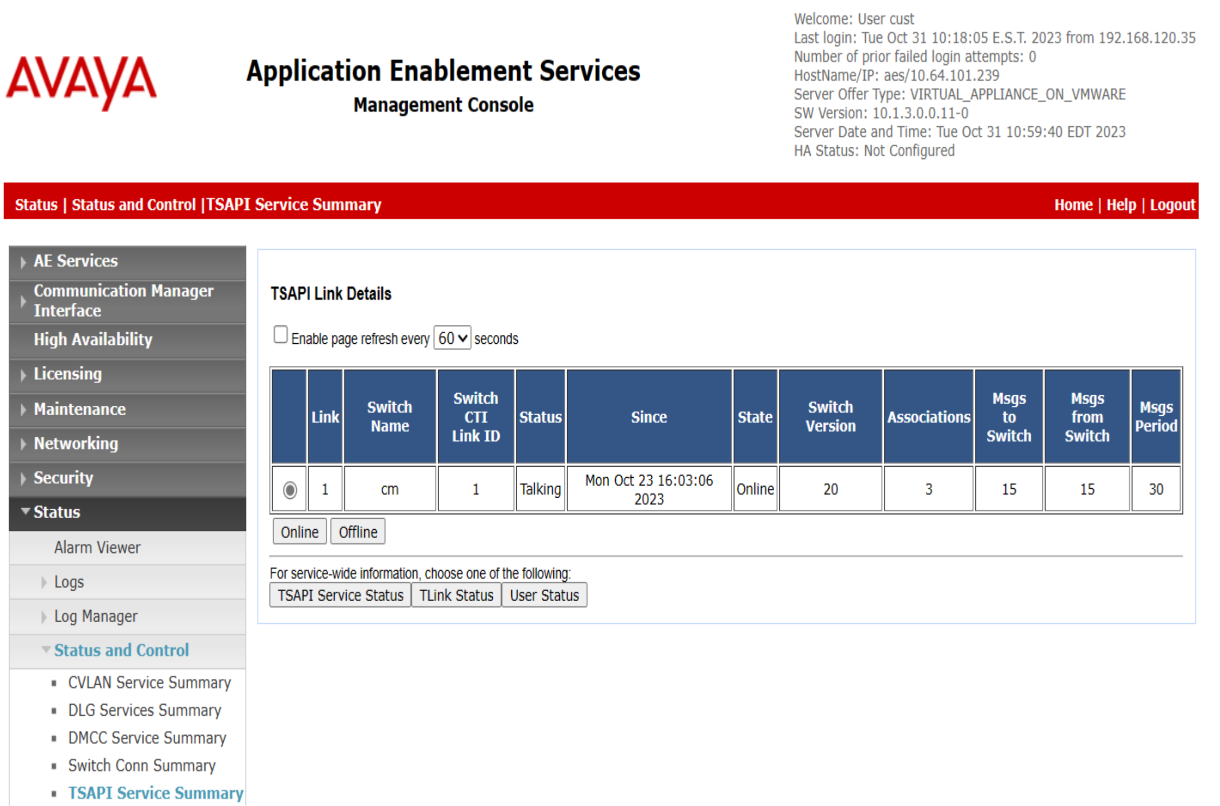
```
status signaling-group 66
                                STATUS SIGNALING GROUP


          Group ID: 66
        Group Type: sip

      Group State: in-service
```

11.2. Verify Avaya Aura® Application Enablement Services

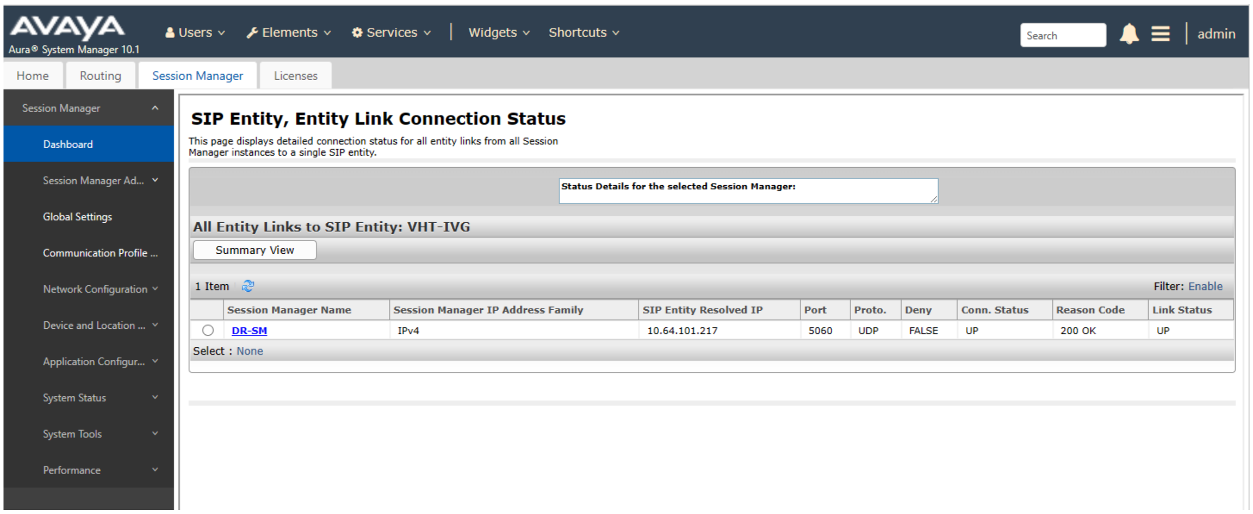
On Application Enablement Services, verify the status of the TSAPI link by selecting **Status → Status and Control → TSAPI Service Summary** from the left pane. The **TSAPI Link Details** screen is displayed. Verify the **Status** is *Talking* for the TSAPI link administered in **Section 7.3**.



11.3. Verify Avaya Aura® Session Manager

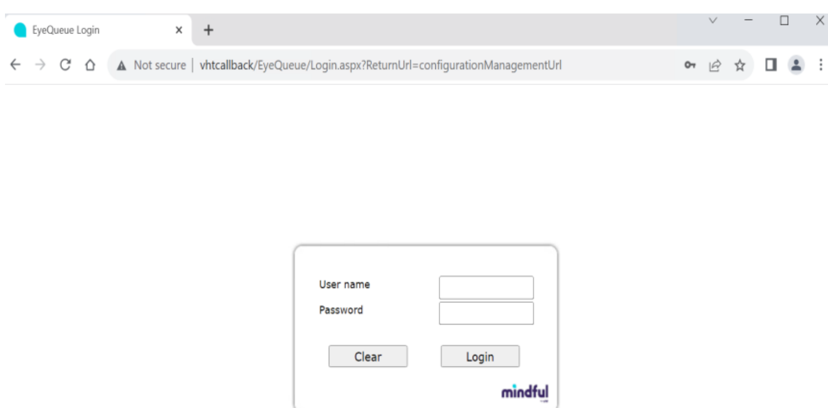
From the System Manager home page (not shown), select **Elements → Session Manager** to display the **Session Manager Dashboard** screen (not shown). Select **Session Manager → System Status → SIP Entity Monitoring** from the left pane to display the **SIP Entity Link Monitoring Status Summary** screen (not shown). Click the IVG entity name from **Section 6.2.2**.

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

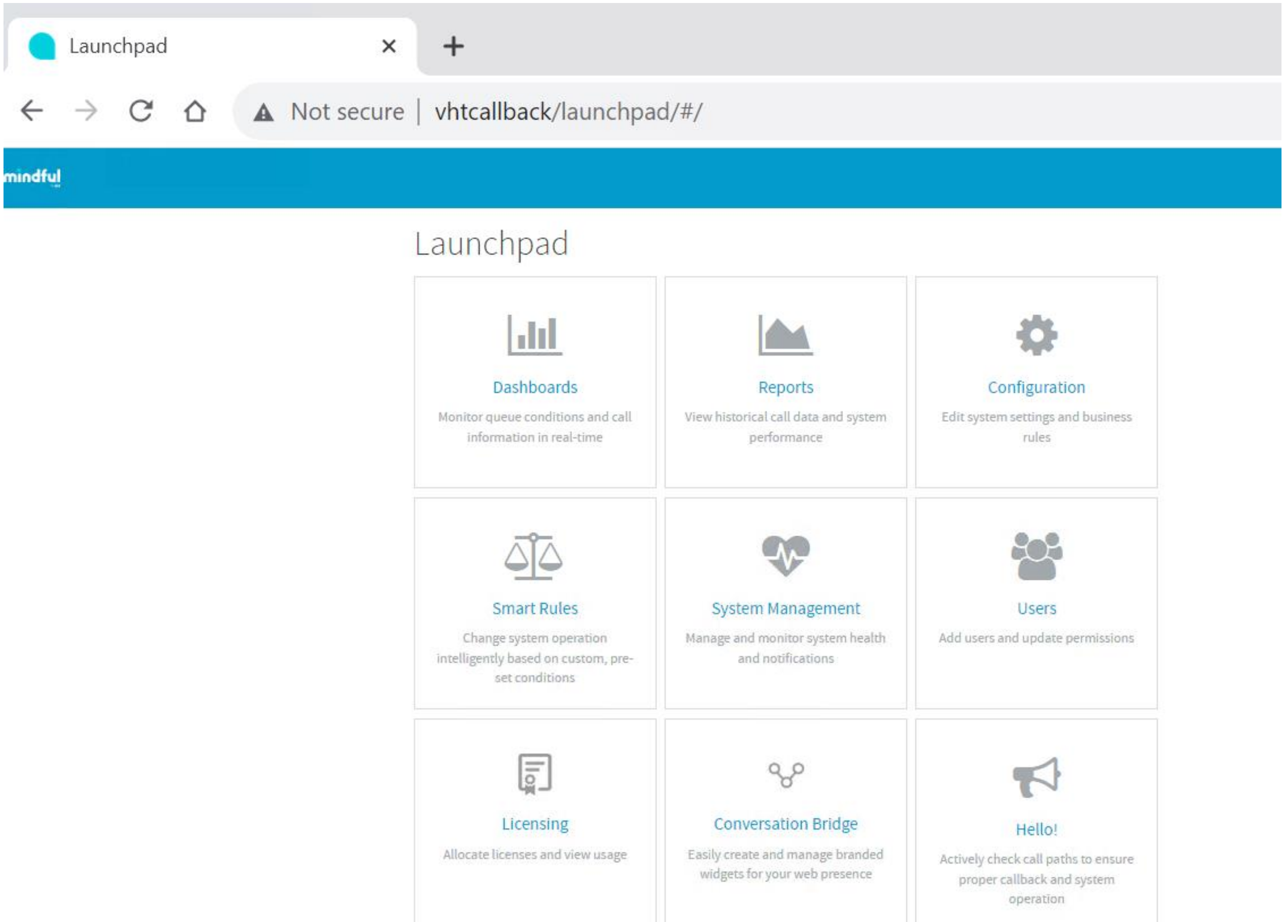


11.4. Verify VHT Callback and IVG

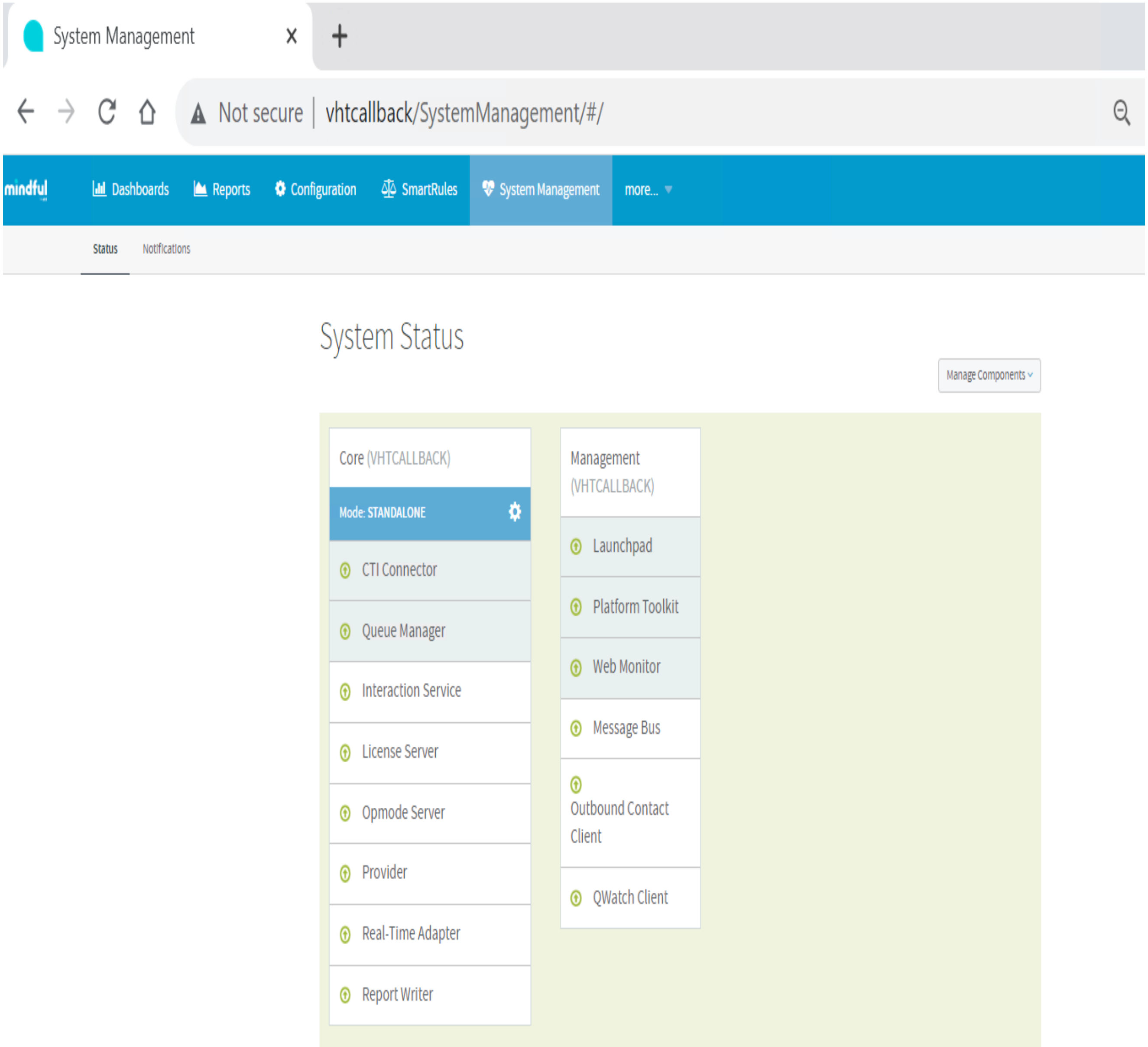
Access the Callback web-based EyeQueue application by using the URL "http://<*ip-address*>/EyeQueue" in an Internet browser window, where <*ip-address*> is the IP address of the Callback server. Log in using the appropriate credentials.



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

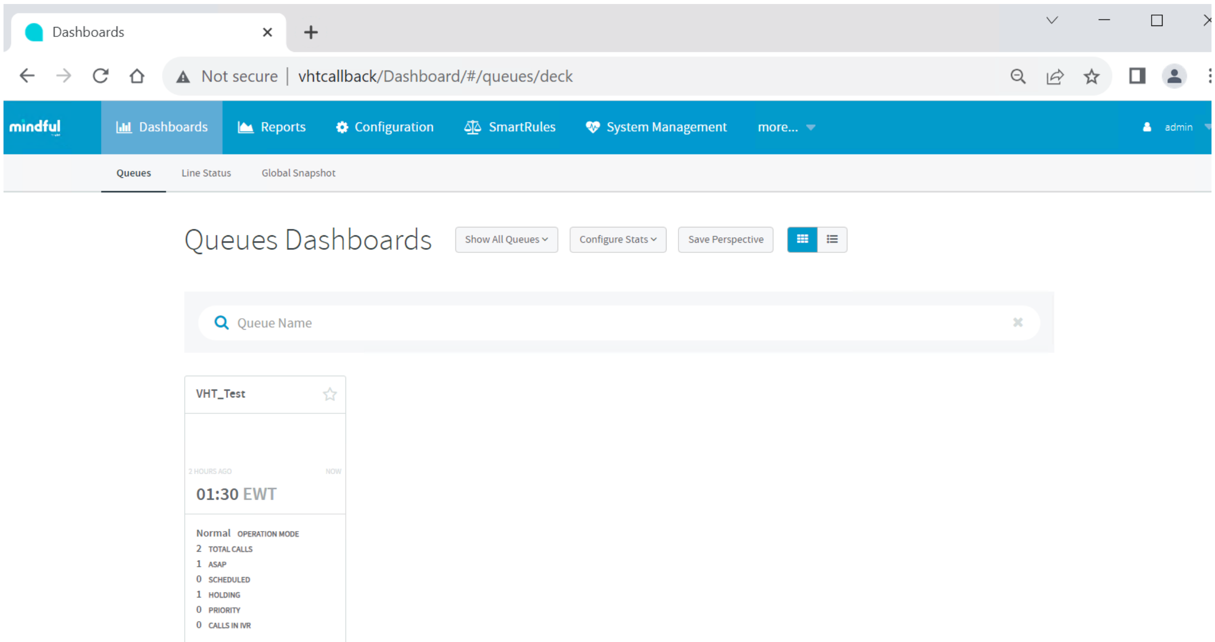


In **System Status**, verify that the components are in-service and that the system is operational as shown below.



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

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



12. Conclusion

These Application Notes describe the steps required to integrate VHT Callback using Native TSAPI with Avaya Aura® Communication Manager, Avaya Aura® Application Enablement Services, and Avaya Aura® Session Manager. VHT Callback successfully handled callback requests from callers, provided estimated wait time, and reported real-time queue statistics.

13. Additional References

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

1. *Administering Avaya Aura® Communication Manager*, Release 10.1.x, Issue 6, May 2023, available at http://support.avaya.com.

2. *Administering Avaya Aura® Application Enablement Services*, Release 10.1.x, Issue 7, May 2023, available at http://support.avaya.com.

3. *Administering Avaya Aura® Session Manager*, Release 10.1.x, Issue 6, May 2023, available at http://support.avaya.com.

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.