Avaya Solution & Interoperability Test Lab

Application Notes for TetraVX Customer Experience Platform (ICX) Callback with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for TetraVX Customer Experience Platform (ICX) Callback to interoperate with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services. ICX Callback is a contact center application.

In the compliance testing, ICX Callback used Device, Media, and Call Control interface from Avaya Aura® Application Enablement Services to provide callback options to customers when the expected wait time exceeds the threshold.

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

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

1. Introduction

These Application Notes describe the configuration steps required for TetraVX Customer Experience Platform (ICX) Callback (hereafter referred to as Callback) to interoperate with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services. Callback is a contact center application, and an optional component of ICX.

In the compliance testing, Callback used the Device, Media, and Call Control (DMCC) interface from Avaya Aura® Application Enablement Services to provide callback options to customers when the expected wait time exceeds the threshold. The DMCC API used by Callback is Java.

Using the Vectoring feature on Avaya Aura® Communication Manager, each incoming ACD call is checked against the expected wait time (EWT). When the EWT exceeds the configured threshold, then the caller is prompted by Avaya Aura® Communication Manager with options to continue to wait in queue or to be called back.

Callers that opted to be called back are routed by Avaya Aura® Communication Manager to Callback over an available inbound virtual IP softphone as member of an inbound hunt group. Callback uses the DMCC interface to answer the call, play media files that are stored on Avaya Aura® Application Enablement Services, and detect tones entered by PSTN caller to collect pertinent information for the callback call such as selection of available callback time slots and callback destination number.

The callback calls are originated by Callback using an available outbound virtual IP softphone to an outbound VDN that routes to a proper skill group with live agents. After the call is answered by an available agent, then Callback uses DMCC call control to perform a consultation call to the callback destination number and transfers the call to the agent.

The compliance test covered the default out-of-box sample call flows and media files, which were provided by TetraVX and expected to be customized by end customers. Any customized call flows and media files are outside the scope of this compliance test.

2. General Test Approach and Test Results

The feature test cases were performed both automatically and manually. Upon start of the Callback application, the application automatically registers and monitors all inbound and outbound virtual IP softphones.

For the manual part of the testing, incoming ACD calls were made to the inbound VDNs. Manual call control from the customer and agent telephones were exercised to verify scheduling and delivering of callback calls.

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

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.

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 these Application Notes, the interface between Avaya systems and ICX utilized enabled capabilities of secure TSAPI and DMCC links.

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 DMCC registration and monitoring services to register and monitor the virtual IP softphones.
- Use of DMCC voice unit and tone collection services to play media files and to collect tones via the virtual IP softphones.
- Use of DMCC call control services to control inbound and outbound calls for the virtual IP softphones.
- Call scenarios involving proper handling and scheduling of inbound calls with callback call options from the inbound virtual IP softphones.
- Call scenarios involving proper originating, handling, and transferring of outbound callback calls from the outbound virtual IP softphones, and proper handling of invalid number, busy destination, no answer, retries, and simultaneous callbacks.

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.

2.2. Test Results

All test cases were executed, and no observations were found on Callback.

2.3. Support

Technical support on Callback can be obtained through the following:

- Phone: +1-877-4963698
- Email: getservice@netrixllc.com

3. Reference Configuration

Figure 1 illustrates a sample configuration consisting of Avaya Aura® components and ICX.

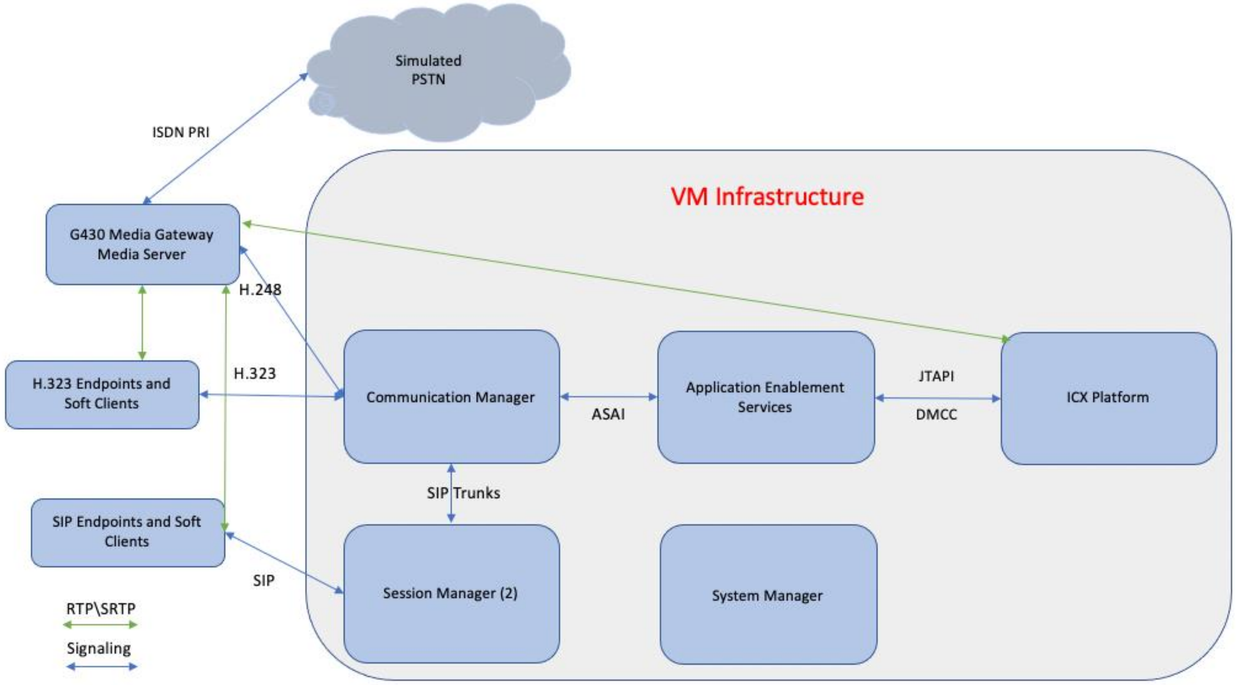


Figure 1: Test Configuration of ICX with Avaya Aura®

4. Equipment and Software Validated

The following equipment and software were used for the test configuration.

Equipment	Release/Version
Avaya Aura® Communication Manager	8.1.2.0.0.890.26095 (FP2)
Avaya Aura® Session Manager	8.1.2.1.812101
Avaya Aura® System Manager	8.1.2.0.0611588 (FP2)
Avaya Aura® Application Enablement Services	8.1.2.1.1.6-0
ICX • Callback	15.3

5. Configure Avaya Aura® Communication Manager

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

- Verify System Capacity (License)
- Administer CTI link
- Administer virtual IP softphones
- Administer inbound hunt group
- Administer inbound vectors
- Administer inbound VDNs
- Administer outbound vectors
- Administer outbound VDNs
- Administer IP codec set

These steps were performed using an SSH Terminal session.

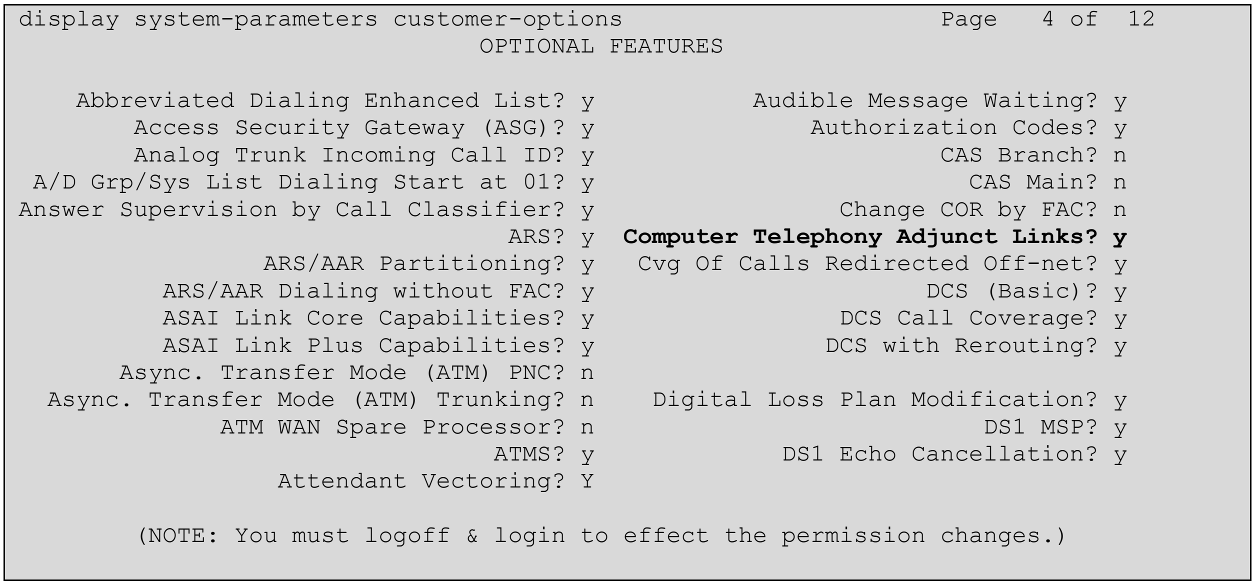
The callback solution utilizes several VDNs to manage calls. Following is a summary:

- Inbound VDN (31500) – Callers are offered a Callback option on this VDN
- Intermediate VDN (31502) – VDN that callers opting to accept the Callback option will be routed to.
- Immediate Callback Out VDN (31503) – Used for immediate Callback requests.
- Scheduled Callback Out VDN (31504) – Used for Scheduled Callbacks

5.1. Verify System Capacity (License)

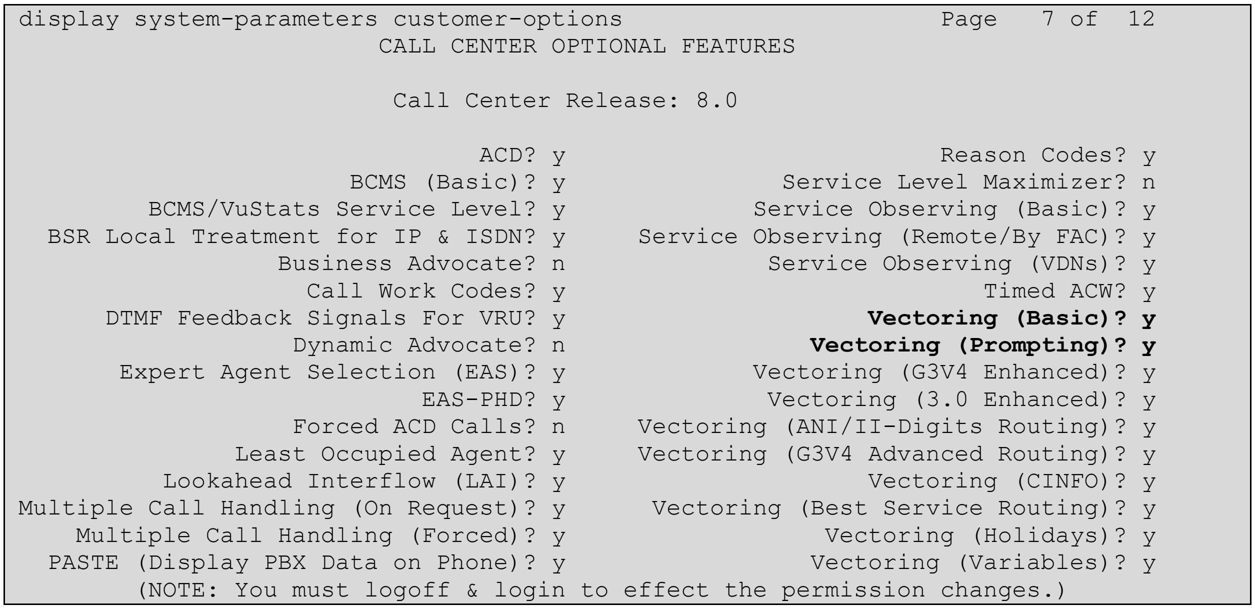
The license file installed on the system controls these attributes. If a required feature is not enabled or there is insufficient capacity, contact an authorized Avaya sales representative.

Use the **display system-parameters customer-options** command to determine these values. On **Page 4**, verify that the **Computer Telephony Adjunct Links** feature is enabled.



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

    Abbreviated Dialing Enhanced List? y           Audible Message Waiting? y
        Access Security Gateway (ASG)? y               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

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

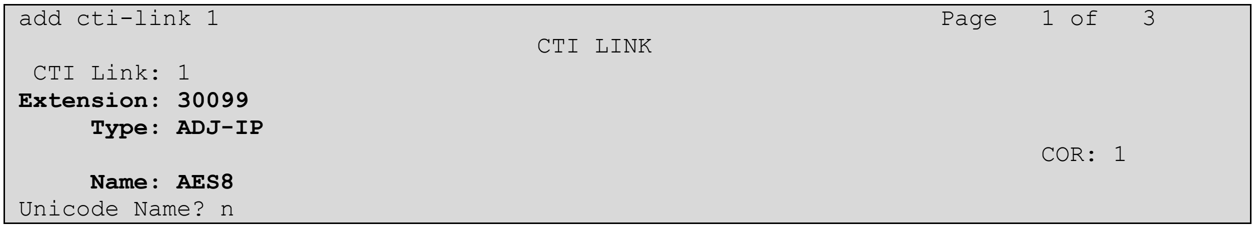
Navigate to Page 7 and verify that **Vectoring (Basic)** and **Vectoring (Prompting)** options are set to “y”.



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

                          Call Center Release: 8.0

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

5.2. Administer CTI Link

Add a CTI link using the “add cti-link n” command, where “n” is an available CTI link number. Enter an available extension number in the **Extension** field. Note that the link number and extension may vary. Enter “ADJ-IP” in the **Type** field, and a descriptive name in the **Name** field. Remaining entries are default.

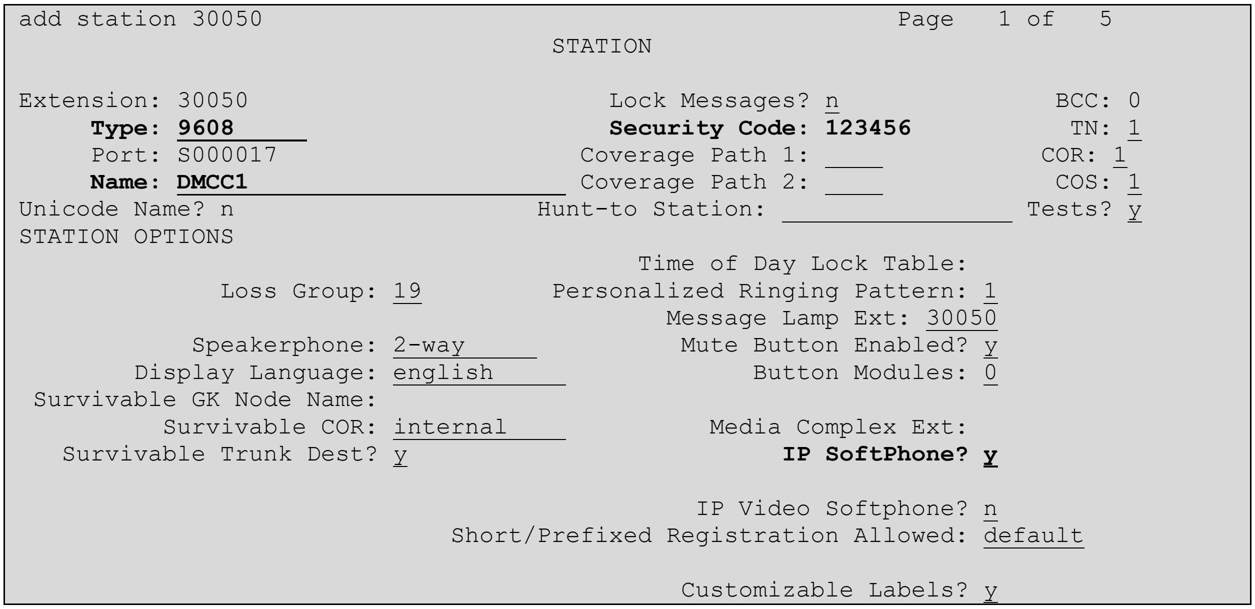


```
add cti-link 1                                                  Page   1 of   3
                                    CTI LINK
 CTI Link: 1
Extension: 30099
     Type: ADJ-IP
                                                                       COR: 1
     Name: AES8
Unicode Name? n
```

5.3. Administer Virtual IP Softphones

Add virtual softphones which will be used for initiating callbacks using the “add station n” command. Use an available extension number for “n”. Enter the following values for the specified fields and retain default values for the remaining fields.

- **Type:** 9608
- **Name:** Any descriptive name
- **Security Code:** Any desired value
- **IP Softphone:** “y”



```
add station 30050                                            Page   1 of   5
                                     STATION

Extension: 30050                         Lock Messages? n               BCC: 0
     Type: 9608                          Security Code: 123456           TN: 1
     Port: S000017                     Coverage Path 1:                COR: 1
     Name: DMCC1                       Coverage Path 2:                 COS: 1
Unicode Name? n                     Hunt-to Station:                  Tests? y
STATION OPTIONS
                                           Time of Day Lock Table:
              Loss Group: 19         Personalized Ringing Pattern: 1
                                             Message Lamp Ext: 30050
            Speakerphone: 2-way               Mute Button Enabled? y
        Display Language: english                  Button Modules: 0
 Survivable GK Node Name:
          Survivable COR: internal                Media Complex Ext:
   Survivable Trunk Dest? y                            IP SoftPhone? y

                                               IP Video Softphone? n
                              Short/Prefixed Registration Allowed: default

                                              Customizable Labels? y
```

Repeat this section to administer the desired number of virtual IP softphones for handling inbound and outbound calls. In the compliance testing, three virtual IP softphones were configured. The first two softphones with extensions 30050-1 were used for handling inbound callback requests, and the last softphone with extension 30052 was used for handling outbound callback calls.

5.4. Administer Inbound Hunt Group

In the test configuration, a standard EAS Hunt Group was used for routing to agents. The Vector is used for routing inbound calls, checked expected wait times and routed to a callback specific hunt group to capture a DMCC port to play announcements stored on Application Enablement Services, and capture the caller’s phone number for later callback. This section covers the administration used to accomplish the desired functionality.

Administer a hunt group to be used for routing of inbound calls for callbacks. Use the “add hunt-group n” command, where “n” is an available hunt group number. Enter the following values for the specified fields and retain the default values for the remaining fields.

- **Group Name:** **ICX CBC Inbound**
- Group Extension: **31010**
- ACD: “n”
- Queue: “n”
- Vector: “n”

```
add hunt-group 10                                           Page   1 of  60
                                  HUNT GROUP

            Group Number: 10                              ACD? n
              Group Name: ICX CBC Inbound               Queue? n
         Group Extension: 31010                        Vector? n
              Group Type: ucd-mia                 Coverage Path:
                      TN: 1          Night Service Destination:
                     COR: 1                   MM Early Answer? n
           Security Code:               Local Agent Preference? n
 ISDN/SIP Caller Display:
```

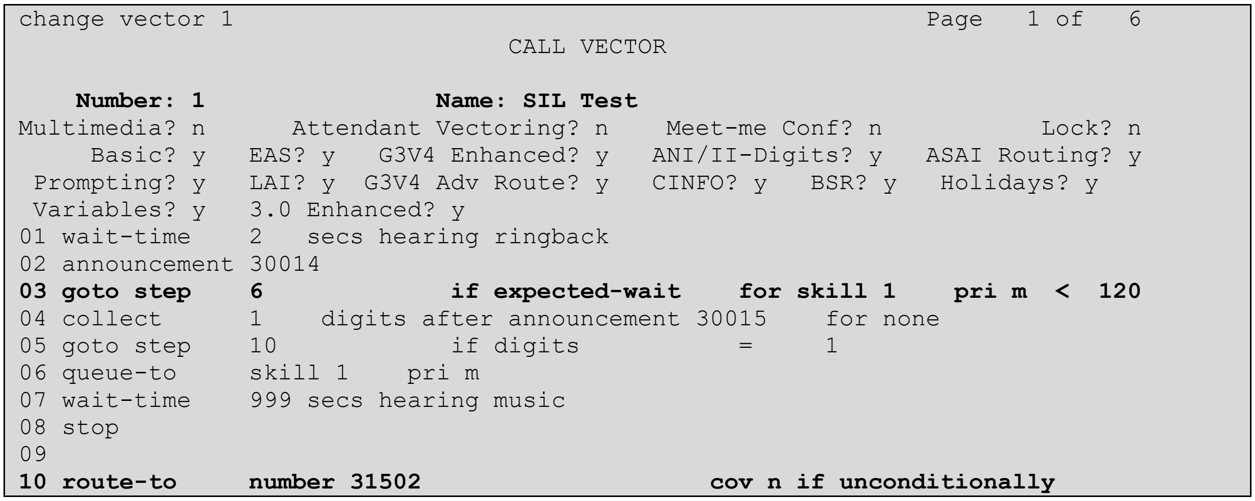
Navigate to **Page 3** and enter the extensions of all inbound virtual IP softphones from **Section 5.3** as members. Calls to this hunt group will be routed over an available inbound virtual IP softphone to Callback.

```
add hunt-group 10                                           Page   3 of  60
                                  HUNT GROUP
  Group Number: 10    Group Extension: 31010             Group Type: ucd-mia
  Member Range Allowed: 1 - 1500      Administered Members (min/max): 1   /2
                                          Total Administered Members: 2
GROUP MEMBER ASSIGNMENTS
      Ext           Name(16 characters)      Ext           Name(16 characters)
   1: 30050           DMCC1              14:
   2: 30051           DMCC2              15:
```

5.5. Administer Inbound Vectors

Modify an available vector using the “change vector n” command, where “n” is an existing vector number. The vector will be used to handle incoming ACD calls, to check EWT, and route calls to Callback when the EWT is over the desired threshold with customer opted to be called back.

Note that the vector steps may vary, and below is a sample vector used in the compliance testing. In the screenshot below, skill 1 is an existing skill group that can handle calls to this vector. The extension used in the route-to number step needs to match the VDN (31502) that routes calls to the inbound hunt group from **Section 5.4.**

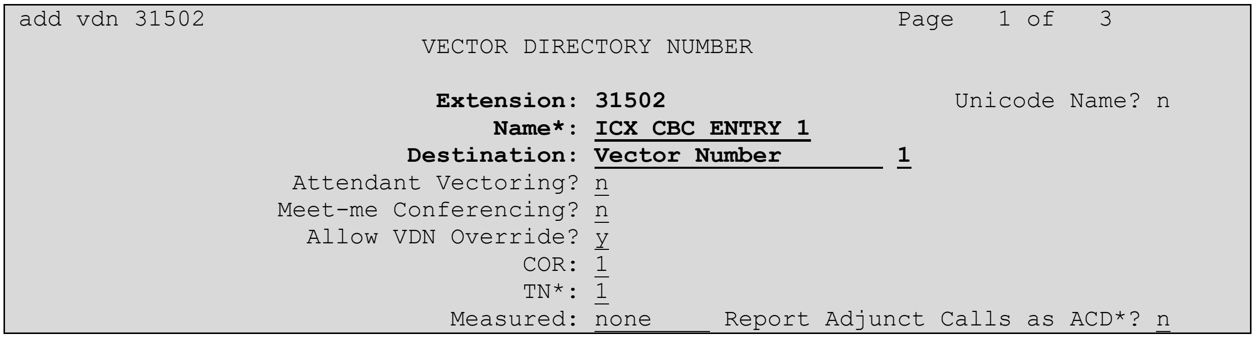


```
change vector 1                                                Page   1 of   6
                                  CALL VECTOR

    Number: 1                Name: SIL Test
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    2   secs hearing ringback
02 announcement 30014
03 goto step    6            if expected-wait    for skill 1    pri m  <  120
04 collect      1    digits after announcement 30015    for none
05 goto step    10           if digits           =     1
06 queue-to     skill 1    pri m
07 wait-time    999 secs hearing music
08 stop
09
10 route-to     number 31502                    cov n if unconditionally
```

Repeat for all inbound vectors to be used where the callback option will be offered.

5.6. Administer Inbound VDNs

For inbound calls that will be routed to the callback application, 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 **Section 5.5** for Vector Number. Retain the default values for all remaining fields. Repeat for all inbound queues with the callback option.

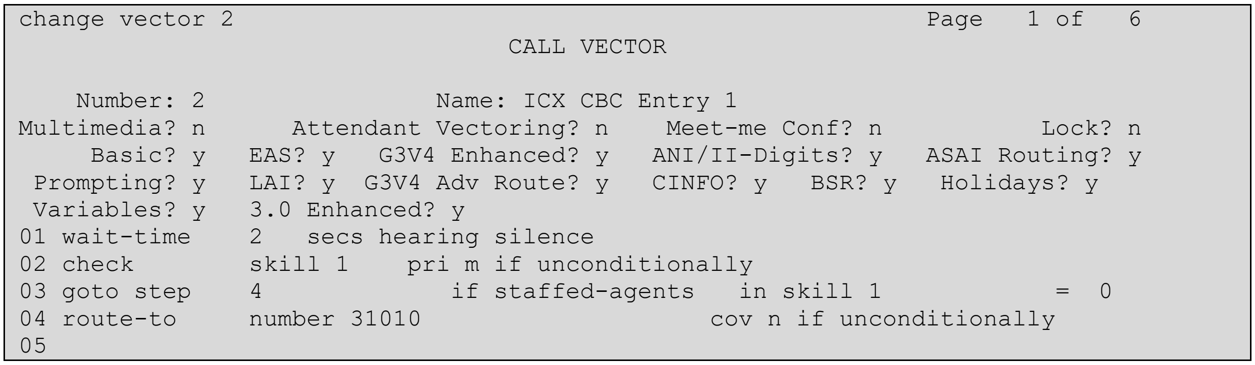


```
add vdn 31502                                                Page   1 of   3
                            VECTOR DIRECTORY NUMBER

                                 Extension: 31502               Unicode Name? n
                                     Name*: ICX CBC ENTRY 1
                               Destination: Vector Number        1
                       Attendant Vectoring? n
                      Meet-me Conferencing? n
                        Allow VDN Override? y
                                       COR: 1
                                       TN*: 1
                                  Measured: none     Report Adjunct Calls as ACD*? n
```

5.7. Administer Outbound Vectors

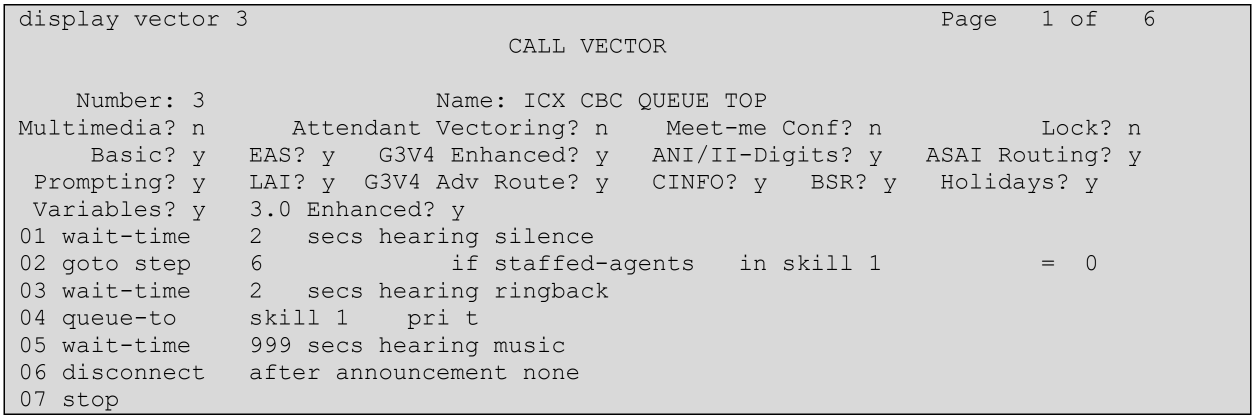
Modify an available vector using the “change vector n” command, where “n” is an existing vector number. This vector will be used to route outbound callback calls to the proper skill group.

Note that the vector steps may vary, and below is a sample vector used in the compliance testing. In the screenshot below, **skill 1** is the skill group number associated with the first inbound vector in **Section 5.5**.

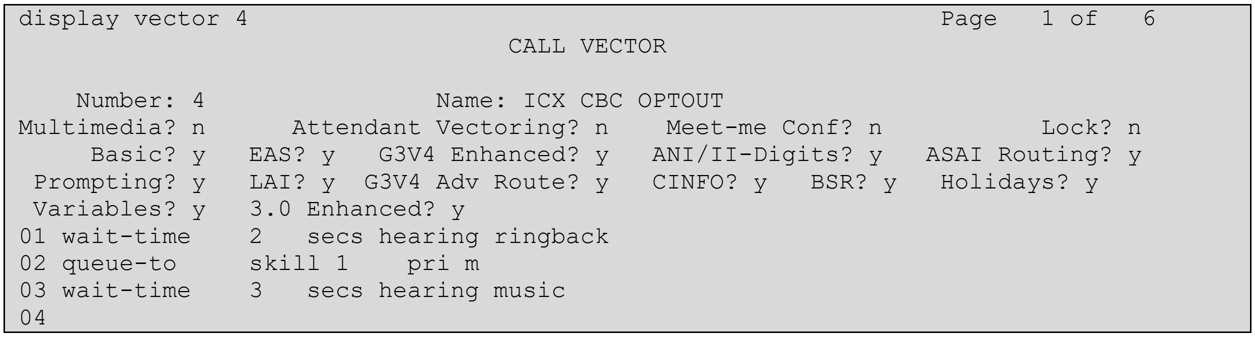


```
change vector 2                                                 Page   1 of   6
                                  CALL VECTOR

    Number: 2                Name: ICX CBC Entry 1
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    2   secs hearing silence
02 check        skill 1    pri m if unconditionally
03 goto step    4            if staffed-agents   in skill 1            =  0
04 route-to     number 31010                    cov n if unconditionally
05
```

Repeat this section to administer an outbound vector for each inbound vector with callback options from **Section** Error! Reference source not found..



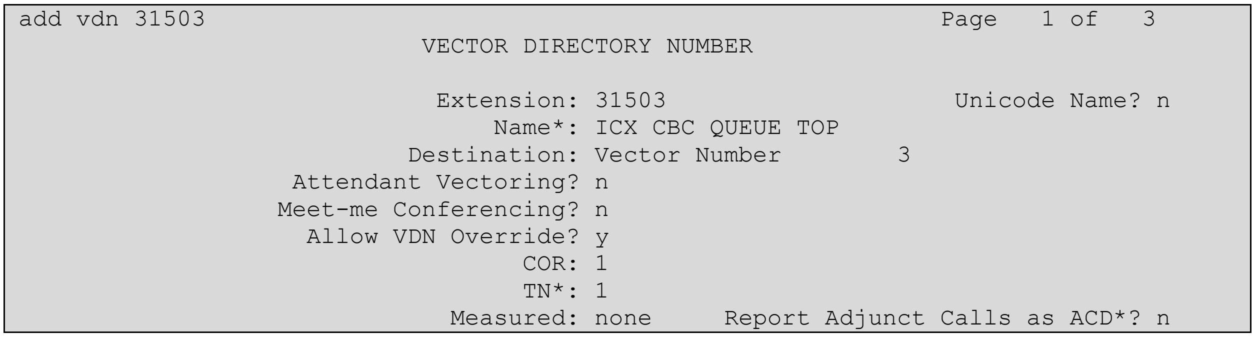
```
display vector 3                                                 Page   1 of   6
                                  CALL VECTOR

    Number: 3                Name: ICX CBC QUEUE TOP
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    2   secs hearing silence
02 goto step    6            if staffed-agents   in skill 1           =  0
03 wait-time    2   secs hearing ringback
04 queue-to     skill 1    pri t
05 wait-time    999 secs hearing music
06 disconnect   after announcement none
07 stop
```



```
display vector 4                                                 Page   1 of   6
                                  CALL VECTOR

    Number: 4                Name: ICX CBC OPTOUT
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    2   secs hearing ringback
02 queue-to     skill 1    pri m
03 wait-time    3   secs hearing music
04
```

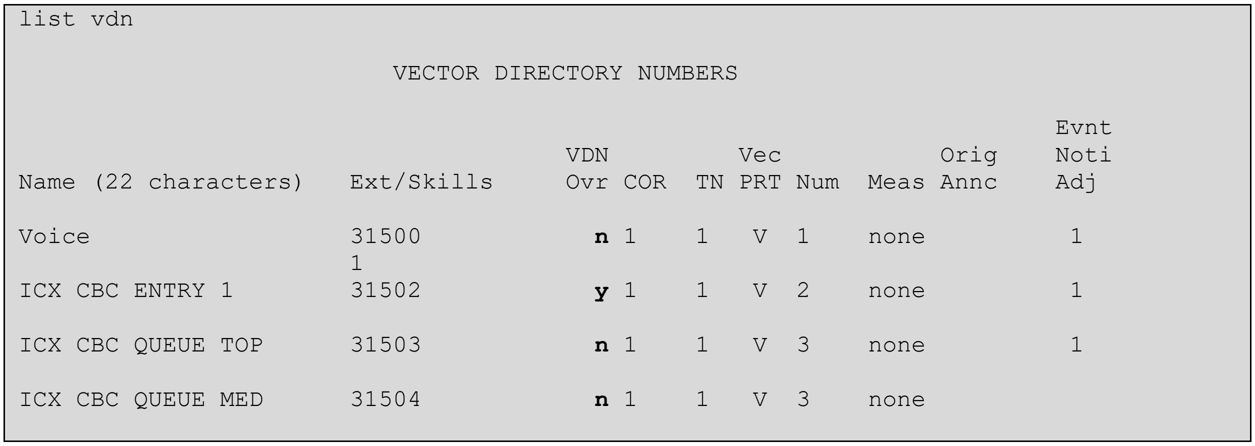
5.8. Administer Outbound VDNs

Add a VDN using the “add vdn n” command, where “n” is an available extension number. Enter a descriptive **Name**, and the first vector number from **Section 5.7** for **Vector Number**. Retain the default values for all remaining fields.



```
add vdn 31503                                                 Page   1 of   3
                            VECTOR DIRECTORY NUMBER

                             Extension: 31503                  Unicode Name? n
                                 Name*: ICX CBC QUEUE TOP
                           Destination: Vector Number        3
                   Attendant Vectoring? n
                  Meet-me Conferencing? n
                    Allow VDN Override? y
                                   COR: 1
                                   TN*: 1
                              Measured: none     Report Adjunct Calls as ACD*? n
```

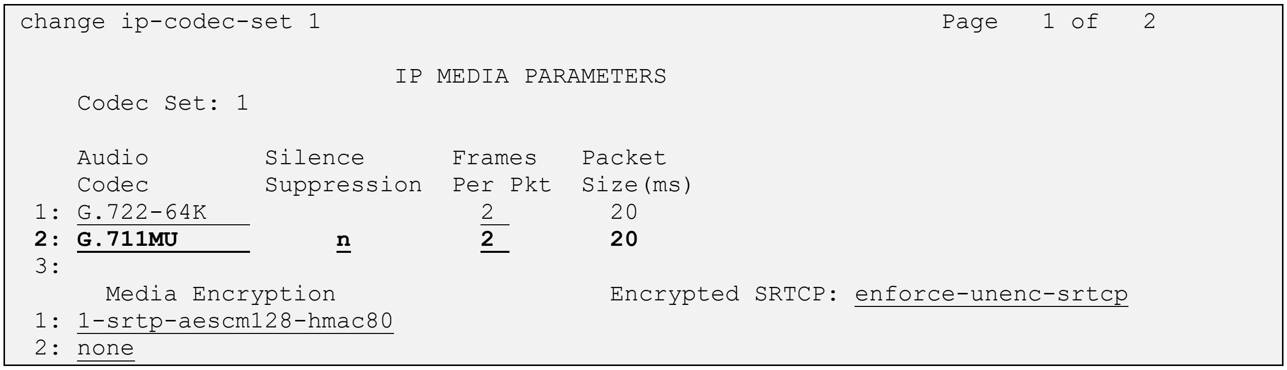
Repeat this section to administer a VDN for each vector from **Section 5.7**. In the compliance testing, the outbound VDNs were configured as shown below.



```
list vdn

                          VECTOR DIRECTORY NUMBERS

                                                                        Evnt
                                      VDN         Vec           Orig    Noti
Name (22 characters)    Ext/Skills     Ovr  COR   TN PRT Num   Meas Annc    Adj

Voice                   31500            n 1     1   V  1     none          1
                        1
ICX CBC ENTRY 1         31502            y 1     1   V  2     none          1

ICX CBC QUEUE TOP       31503            n 1     1   V  3     none          1

ICX CBC QUEUE MED       31504            n 1     1   V  3     none
```

5.9. Administer IP Codec Set

Use the “change ip-codec-set n” command, where “n” is an existing codec set number used by the ACD agents and the virtual IP softphones. Make certain the **Audio Codec** listing contains the codec used by the media files. The compliance testing used the sample media files from Callback, which were recorded with **G.711A**.



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

                          IP MEDIA PARAMETERS
    Codec Set: 1

    Audio        Silence      Frames   Packet
    Codec        Suppression  Per Pkt  Size(ms)
 1: G.722-64K                   2        20
 2: G.711MU          n          2        20
 3:
      Media Encryption                   Encrypted SRTCP: enforce-unenc-srtcp
 1: 1-srtp-aescm128-hmac80
 2: none
```

6. Configure Avaya Aura® Application Enablement Services

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

- Transfer media files
- Launch OAM interface
- Verify license
- Administer media properties
- Administer TSAPI link
- Administer H.323 gatekeeper
- Administer ICX user
- Administer security database
- Administer ports
- Obtain Tlink name
- Restart services

6.1. Transfer Media Files

Log in to the Linux shell of the Application Enablement Services server with appropriate permissions and navigate to the **/var** directory.

Enter the command "**cd /var**", followed by "**mkdir ICX**" to create a directory. Note that the name of the directory can vary.

Enter "**chmod 777 ICX**" to change the access permission for the directory. This directory will be used to store the media files.

```
[cust@sildvaes8 ~]$ cd /var

[cust@sildvaes8 ~]$ mkdir ICX

[cust@sildvaes8 ~]$ chmod 777 ICX
```

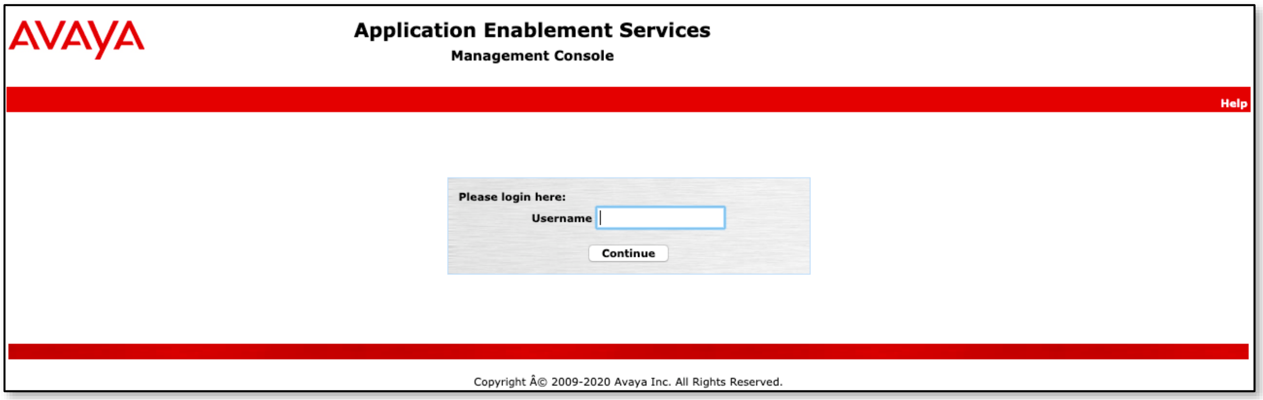
A set of sample media files used by the out-of-box call flows is provided by ICX. Customers are expected to customize the call flows along with professionally recorded media files. The compliance testing used the sample media files and the out-of-box call flows.

Use SCP to transfer the media files to Application Enablement Services. Place the media files under the directory that was created above, as shown below.

```
[cust@sildvaes8 ICX]$ ls -l
total 3872
-rw-r--r-- 1 cust susers  25274 Nov 25 12:56 02ImmediateCallback_en.wav
-rw-r--r-- 1 cust susers  35518 Nov 25 12:56 02ImmediateCallback_es.wav
-rw-r--r-- 1 cust susers  26522 Nov 25 12:56 03ScheduledCallback_en.wav
-rw-r--r-- 1 cust susers  35170 Nov 25 12:56 03ScheduledCallback_es.wav
-rw-r--r-- 1 cust susers  58898 Nov 25 12:56 CallbackOnAniMenu_en.wav
-rw-r--r-- 1 cust susers  99602 Nov 25 12:56 CallbackOnAniMenu_es.wav
-rw-r--r-- 1 cust susers  28390 Nov 25 12:56 cbc_49_en.wav
```

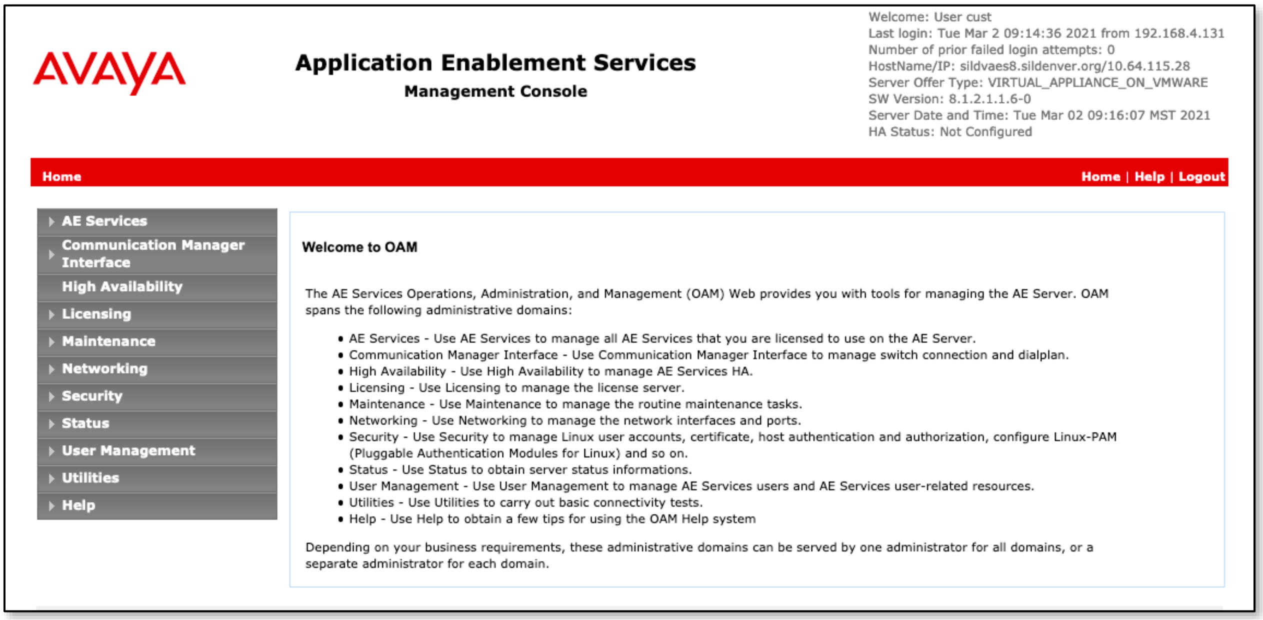
6.2. Launch OAM Interface

Access the OAM web-based interface by using the URL “https://ip-address” in an Internet browser window, where “ip-address” is the IP address of the Application Enablement Services server. The **Please login here** screen is displayed. Log in using the appropriate credentials.



Copyright Â© 2009-2020 Avaya Inc. All Rights Reserved.

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



Welcome: User cust
Last login: Tue Mar 2 09:14:36 2021 from 192.168.4.131
Number of prior failed login attempts: 0
HostName/IP: sildvaes8.sildenver.org/10.64.115.28
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.1.2.1.1.6-0
Server Date and Time: Tue Mar 02 09:16:07 MST 2021
HA Status: Not Configured

Welcome to OAM

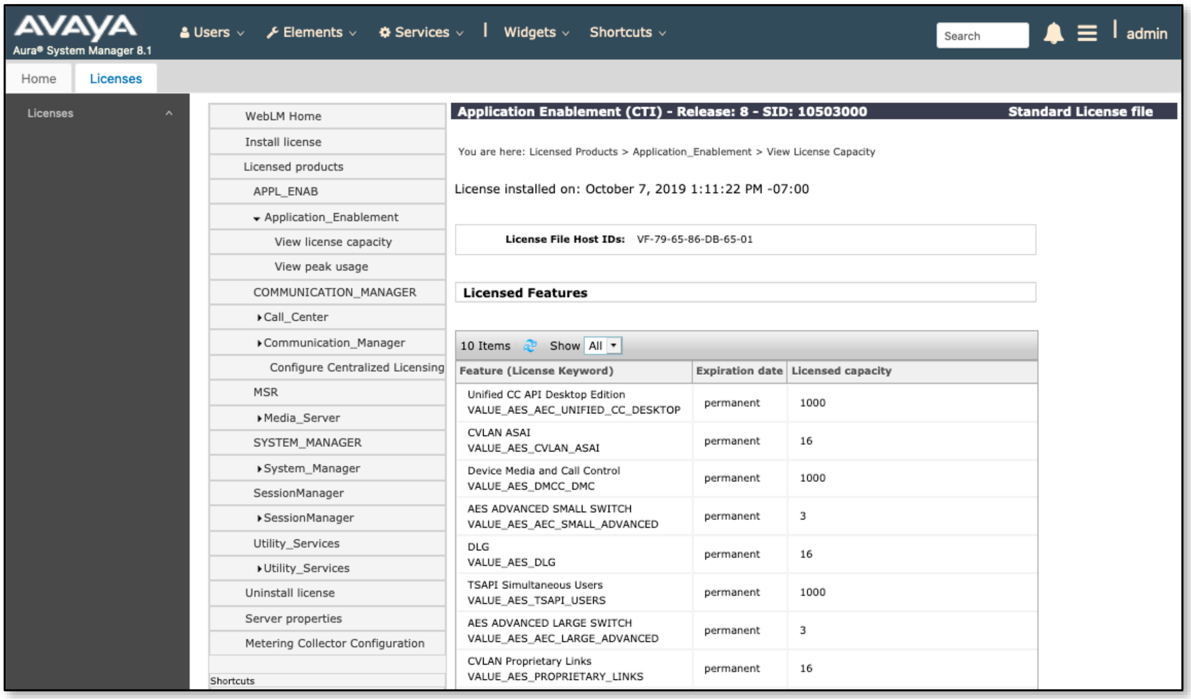
The AE Services Operations, Administration, and Management (OAM) Web provides you with tools for managing the AE Server. OAM spans the following administrative domains:

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

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

6.3. Verify License

System Manager was used as a central license server for the test environment. Log in using the appropriate credentials and navigate to display installed licenses. On System Manager, navigate to **Services → Licenses → Application_Enablement**.



Application Enablement (CTI) - Release: 8 - SID: 10503000 **Standard License file**

You are here: Licensed Products > Application_Enablement > View License Capacity

License installed on: October 7, 2019 1:11:22 PM -07:00

License File Host IDs: VF-79-65-86-DB-65-01

Licensed Features

10 Items Show All

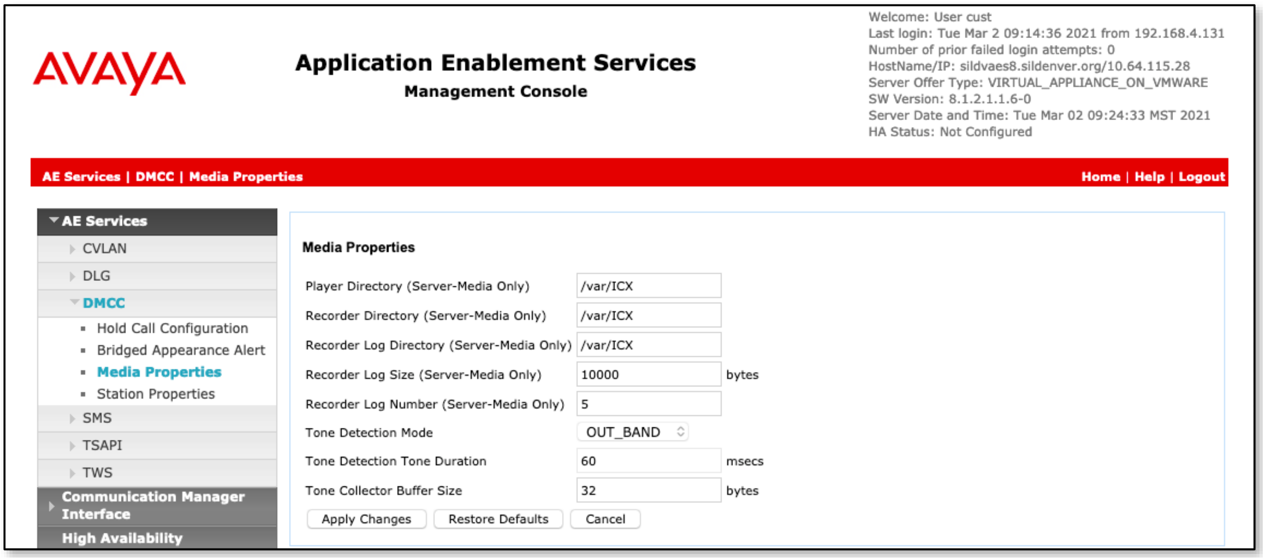
Feature (License Keyword)	Expiration date	Licensed capacity
Unified CC API Desktop Edition VALUE_AES_AEC_UNIFIED_CC_DESKTOP	permanent	1000
CVLAN ASAI VALUE_AES_CVLAN_ASAI	permanent	16
Device Media and Call Control VALUE_AES_DMCC_DMC	permanent	1000
AES ADVANCED SMALL SWITCH VALUE_AES_AEC_SMALL_ADVANCED	permanent	3
DLG VALUE_AES_DLG	permanent	16
TSAPI Simultaneous Users VALUE_AES_TSAPI_USERS	permanent	1000
AES ADVANCED LARGE SWITCH VALUE_AES_AEC_LARGE_ADVANCED	permanent	3
CVLAN Proprietary Links VALUE_AES_PROPRIETARY_LINKS	permanent	16

Verify that there are sufficient licenses for **TSAPI Simultaneous Users** and **Device Media and Call Control**, as shown above. Note that the TSAPI license is used for monitoring and call control via DMCC, and the DMCC license is used for the virtual IP softphones.

6.4. Administer Media Properties

Select **AE Services** → **DMCC** → **Media Properties** from the left pane of the **Management Console**. The **Media Properties** screen is displayed, as shown below.

For **Player Directory**, **Recorder Directory**, and **Recorder Log Directory**, enter the path to the media files from **Section 6.1**, as shown below. Retain the default values in the remaining fields.



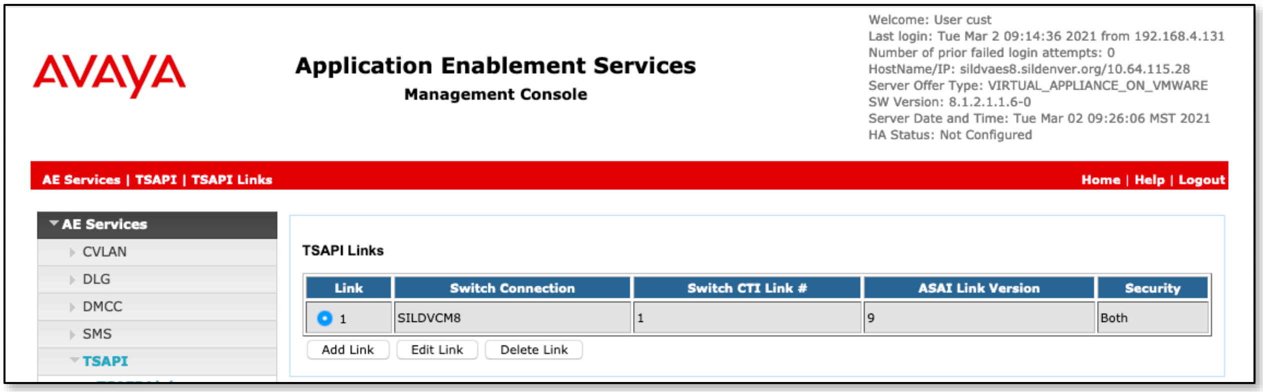
Welcome: User cust
Last login: Tue Mar 2 09:14:36 2021 from 192.168.4.131
Number of prior failed login attempts: 0
HostName/IP: sildvaes8.sildenver.org/10.64.115.28
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.1.2.1.1.6-0
Server Date and Time: Tue Mar 02 09:24:33 MST 2021
HA Status: Not Configured

Media Properties

Player Directory (Server-Media Only)	/var/ICX	
Recorder Directory (Server-Media Only)	/var/ICX	
Recorder Log Directory (Server-Media Only)	/var/ICX	
Recorder Log Size (Server-Media Only)	10000	bytes
Recorder Log Number (Server-Media Only)	5	
Tone Detection Mode	OUT_BAND	
Tone Detection Tone Duration	60	msecs
Tone Collector Buffer Size	32	bytes

6.5. 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**, note that an existing TSAPI Link was used for testing, details are displayed using the **Edit Link** button.



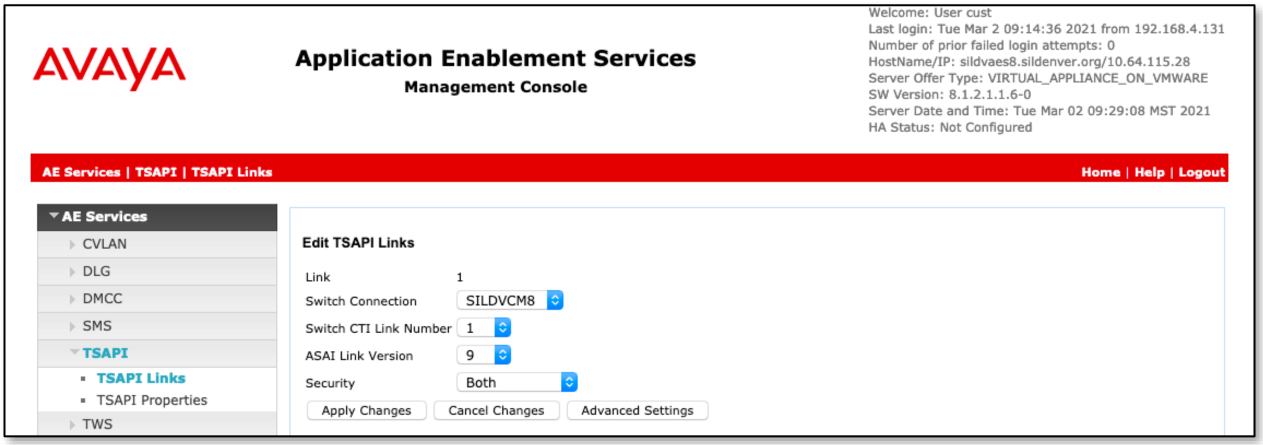
Welcome: User cust
Last login: Tue Mar 2 09:14:36 2021 from 192.168.4.131
Number of prior failed login attempts: 0
HostName/IP: sildvaes8.sildenver.org/10.64.115.28
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.1.2.1.1.6-0
Server Date and Time: Tue Mar 02 09:26:06 MST 2021
HA Status: Not Configured

TSAPI Links

Link	Switch Connection	Switch CTI Link #	ASAI Link Version	Security
● 1	SILDVCM8	1	9	Both

The **Add (or Edit) 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 "**SILDVCM8**" is selected. For **Switch CTI Link Number**, select the CTI link number from **Section** Error! Reference source not found.. Retain the default values in the remaining fields.



Welcome: User cust
Last login: Tue Mar 2 09:14:36 2021 from 192.168.4.131
Number of prior failed login attempts: 0
HostName/IP: sildvaes8.sildenver.org/10.64.115.28
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.1.2.1.1.6-0
Server Date and Time: Tue Mar 02 09:29:08 MST 2021
HA Status: Not Configured

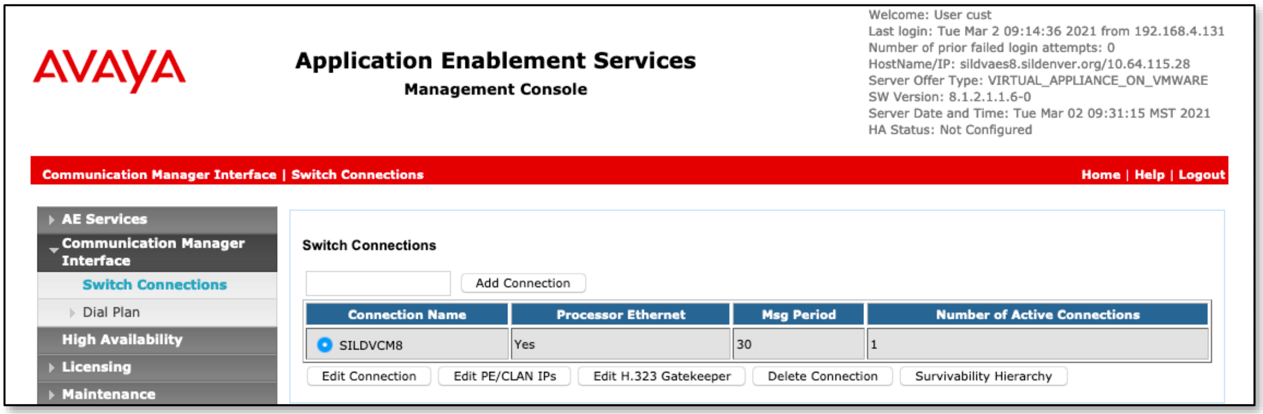
Edit TSAPI Links

Link	1
Switch Connection	SILDVCM8
Switch CTI Link Number	1
ASAI Link Version	9
Security	Both

6.6. Administer H.323 Gatekeeper

Select **Communication Manager Interface → Switch Connections** from the left pane. The **Switch Connections** screen shows a listing of existing switch connections.

Locate the connection name associated with the relevant Communication Manager, in this case "**SILDVCM8**", and select the corresponding radio button. Click **Edit H.323 Gatekeeper**.

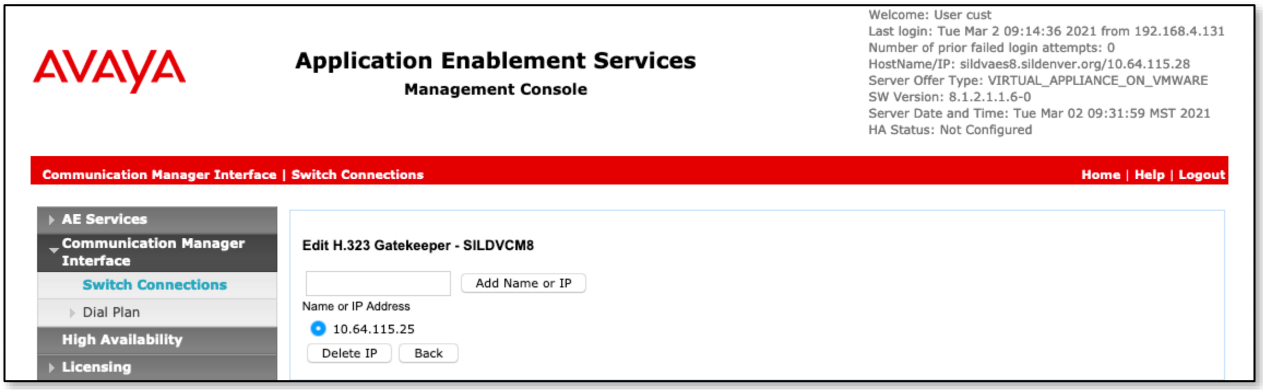


Welcome: User cust
Last login: Tue Mar 2 09:14:36 2021 from 192.168.4.131
Number of prior failed login attempts: 0
HostName/IP: sildvaes8.sildenver.org/10.64.115.28
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.1.2.1.1.6-0
Server Date and Time: Tue Mar 02 09:31:15 MST 2021
HA Status: Not Configured

Switch Connections

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections
● SILDVCM8	Yes	30	1

The **Edit H.323 Gatekeeper** screen is displayed. Enter the IP address of the Processor (procr) on Communication Manager to use as H.323 gatekeeper, in this case "10.64.115.25" as shown below. Click **Add Name or IP**.



Welcome: User cust
Last login: Tue Mar 2 09:14:36 2021 from 192.168.4.131
Number of prior failed login attempts: 0
HostName/IP: sildvaes8.sildenver.org/10.64.115.28
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.1.2.1.1.6-0
Server Date and Time: Tue Mar 02 09:31:59 MST 2021
HA Status: Not Configured

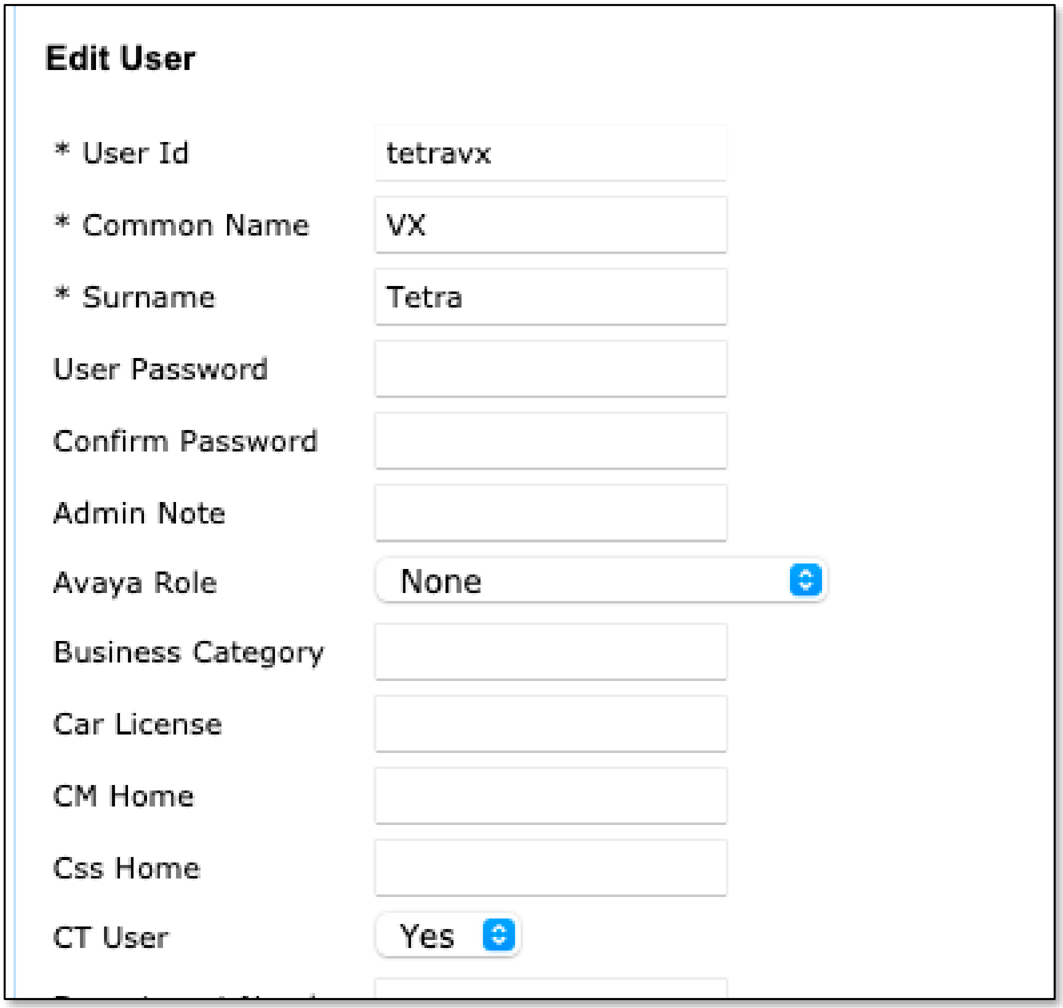
Edit H.323 Gatekeeper - SILDVCM8

Name or IP Address
● 10.64.115.25

6.7. Administer ICX 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. Following is the account after creation:

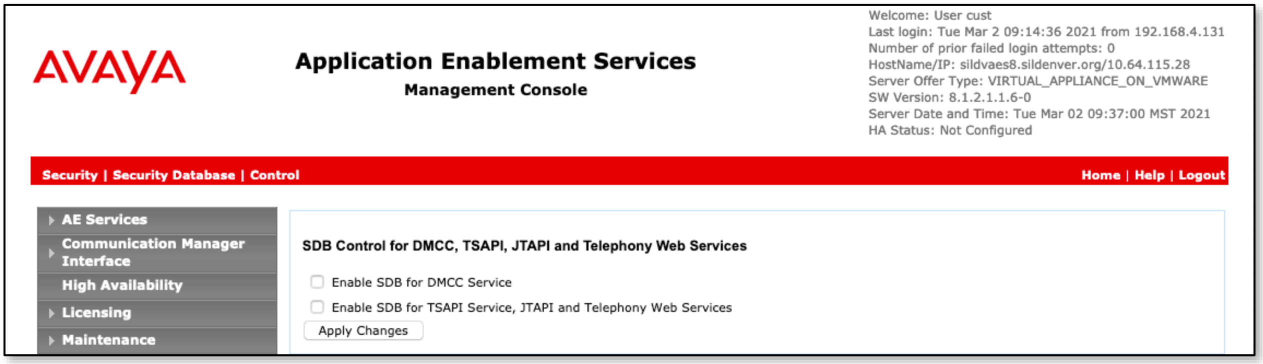


Edit User

* User Id	tetravx
* Common Name	VX
* Surname	Tetra
User Password	
Confirm Password	
Admin Note	
Avaya Role	None
Business Category	
Car License	
CM Home	
Css Home	
CT User	Yes

6.8. Administer Security Database

Select **Security → Security Database → Control** from the left pane, to display the **Enable SDB Control for DMCC Service** and **Enable SDB for TSAPI Service, JTAPI and Telephony Web Services** screen in the right pane. Make certain both parameters are unchecked, as shown below.



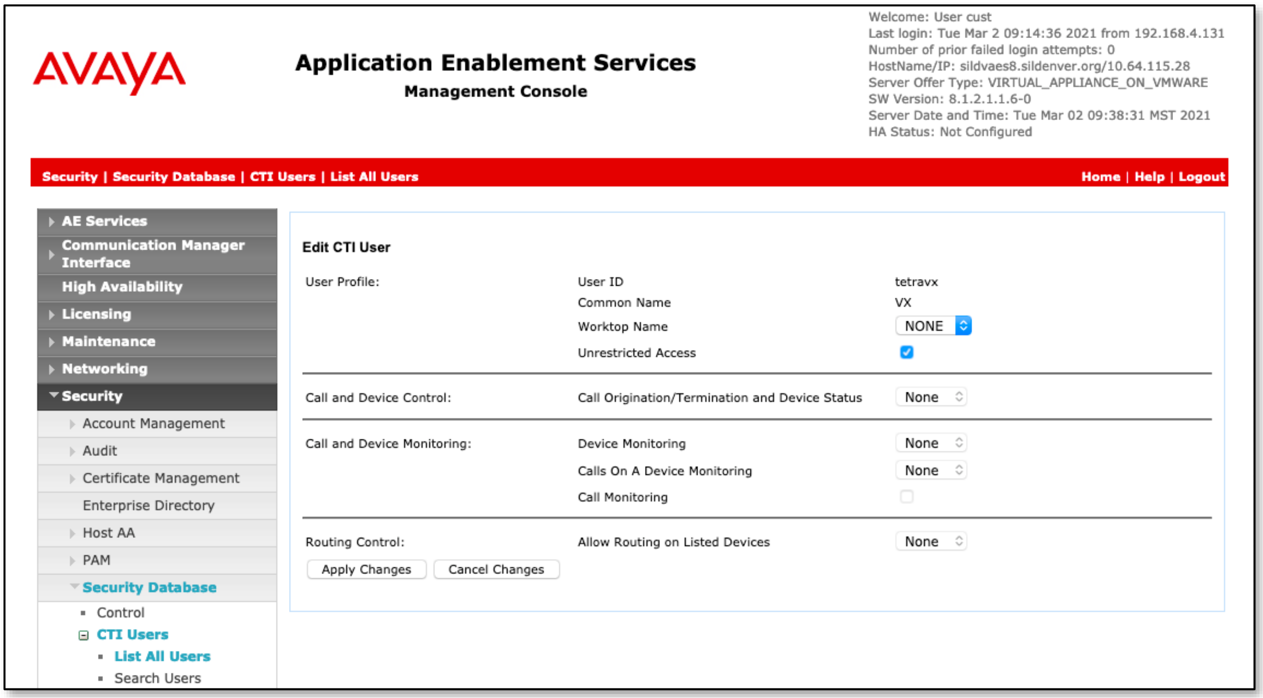
Welcome: User cust
Last login: Tue Mar 2 09:14:36 2021 from 192.168.4.131
Number of prior failed login attempts: 0
HostName/IP: sildvaes8.sildenver.org/10.64.115.28
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.1.2.1.1.6-0
Server Date and Time: Tue Mar 02 09:37:00 MST 2021
HA Status: Not Configured

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

☐ Enable SDB for DMCC Service

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

In the event that the security database is used by the customer with parameter enabled, then navigate to **Security → Security Database → CTI Users → List All Users** and select the user created in **Section 6.7** (not shown) and click the Edit button. On the Edit CTI User screen, check **Unrestricted Access** to grant access to any devices administered in the ICX application.



Welcome: User cust
Last login: Tue Mar 2 09:14:36 2021 from 192.168.4.131
Number of prior failed login attempts: 0
HostName/IP: sildvaes8.sildenver.org/10.64.115.28
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.1.2.1.1.6-0
Server Date and Time: Tue Mar 02 09:38:31 MST 2021
HA Status: Not Configured

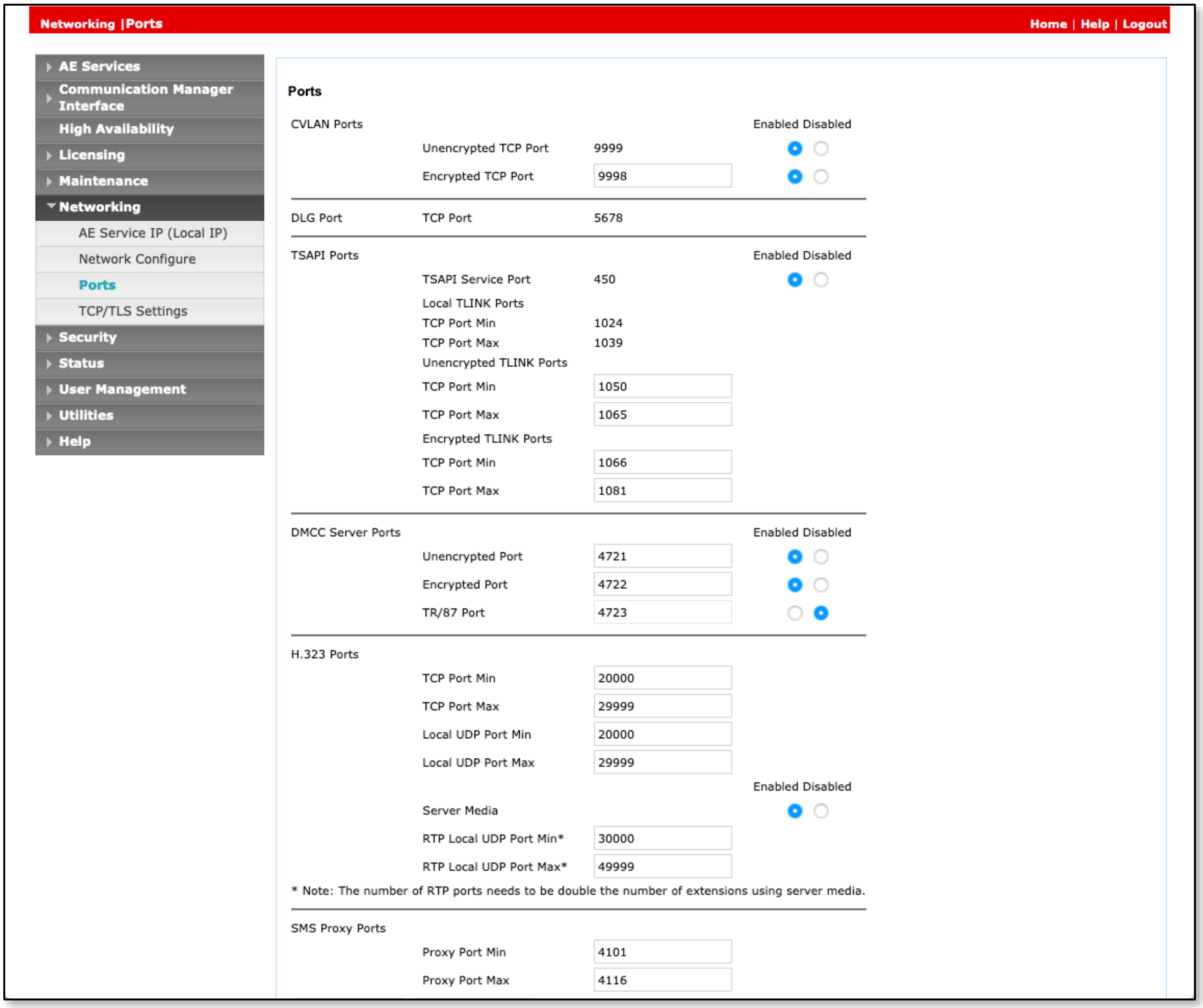
Edit CTI User

User Profile:	User ID	tetravx
	Common Name	VX
	Worktop Name	NONE
	Unrestricted Access	☑
Call and Device Control:	Call Origination/Termination and Device Status	None
Call and Device Monitoring:	Device Monitoring	None
	Calls On A Device Monitoring	None
	Call Monitoring	☐
Routing Control:	Allow Routing on Listed Devices	None

6.9. Administer Ports

Select **Networking → Ports** from the left pane, to display the **Ports** screen in the right pane.

Enable the **TSAPI Ports → TSAPI Service Port 450**, and the **DMCC Server Ports → Unencrypted Port 4721** and **Encrypted Port 4722** as shown below.



Ports

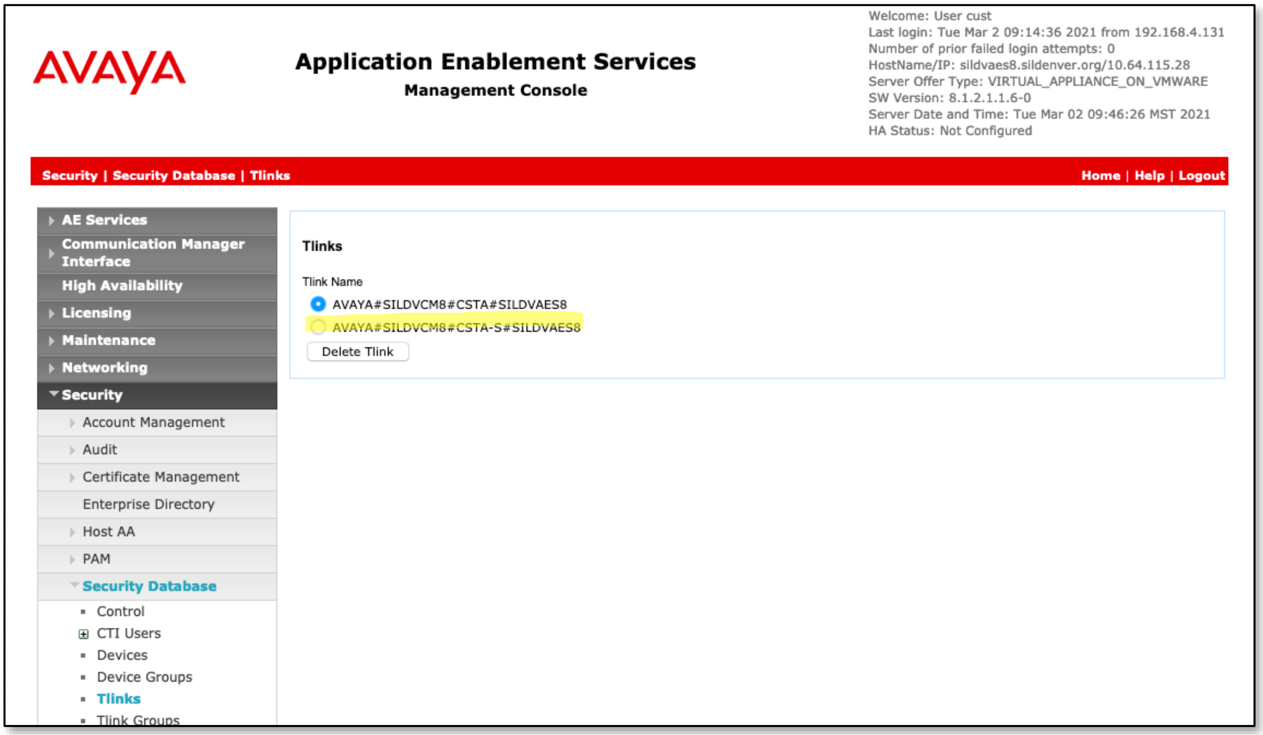
			Enabled	Disabled
CVLAN Ports			Enabled	Disabled
	Unencrypted TCP Port	9999	●	○
	Encrypted TCP Port	9998	●	○
DLG Port	TCP Port	5678		
TSAPI Ports			Enabled	Disabled
	TSAPI Service Port	450	●	○
	Local TLINK Ports			
	TCP Port Min	1024		
	TCP Port Max	1039		
	Unencrypted TLINK Ports			
	TCP Port Min	1050		
	TCP Port Max	1065		
	Encrypted TLINK Ports			
	TCP Port Min	1066		
	TCP Port Max	1081		
DMCC Server Ports			Enabled	Disabled
	Unencrypted Port	4721	●	○
	Encrypted Port	4722	●	○
	TR/87 Port	4723	○	●
H.323 Ports				
	TCP Port Min	20000		
	TCP Port Max	29999		
	Local UDP Port Min	20000		
	Local UDP Port Max	29999		
			Enabled	Disabled
	Server Media		●	○
	RTP Local UDP Port Min*	30000		
	RTP Local UDP Port Max*	49999		
SMS Proxy Ports				
	Proxy Port Min	4101		
	Proxy Port Max	4116		

* Note: The number of RTP ports needs to be double the number of extensions using server media.

6.10. Obtain Tlink Name

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

In this case, the associated Tlink name is "AVAYA#**SILDVCM8**#CSTA-S#**SILDVAES8**". Note the use of the switch connection from **Section 6.5** as part of the Tlink name.



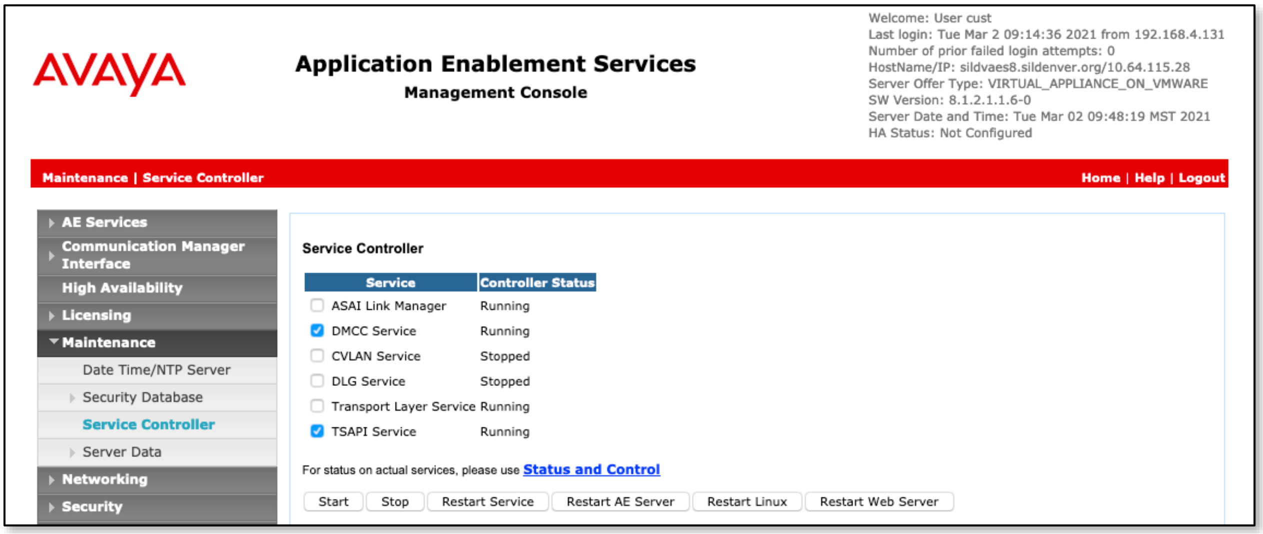
Welcome: User cust
Last login: Tue Mar 2 09:14:36 2021 from 192.168.4.131
Number of prior failed login attempts: 0
HostName/IP: sildvaes8.sildenver.org/10.64.115.28
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.1.2.1.1.6-0
Server Date and Time: Tue Mar 02 09:46:26 MST 2021
HA Status: Not Configured

Tlinks

Tlink Name
● AVAYA#SILDVCM8#CSTA#SILDVAES8
○ AVAYA#SILDVCM8#CSTA-S#SILDVAES8

6.11. Restart Services

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



Welcome: User cust
Last login: Tue Mar 2 09:14:36 2021 from 192.168.4.131
Number of prior failed login attempts: 0
HostName/IP: sildvaes8.sildenver.org/10.64.115.28
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.1.2.1.1.6-0
Server Date and Time: Tue Mar 02 09:48:19 MST 2021
HA Status: Not Configured

Service Controller

Service	Controller Status
☐ ASAI Link Manager	Running
☑ DMCC Service	Running
☐ CVLAN Service	Stopped
☐ DLG Service	Stopped
☐ Transport Layer Service	Running
☑ TSAPI Service	Running

For status on actual services, please use Status and Control

7. Configure ICX Callback

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

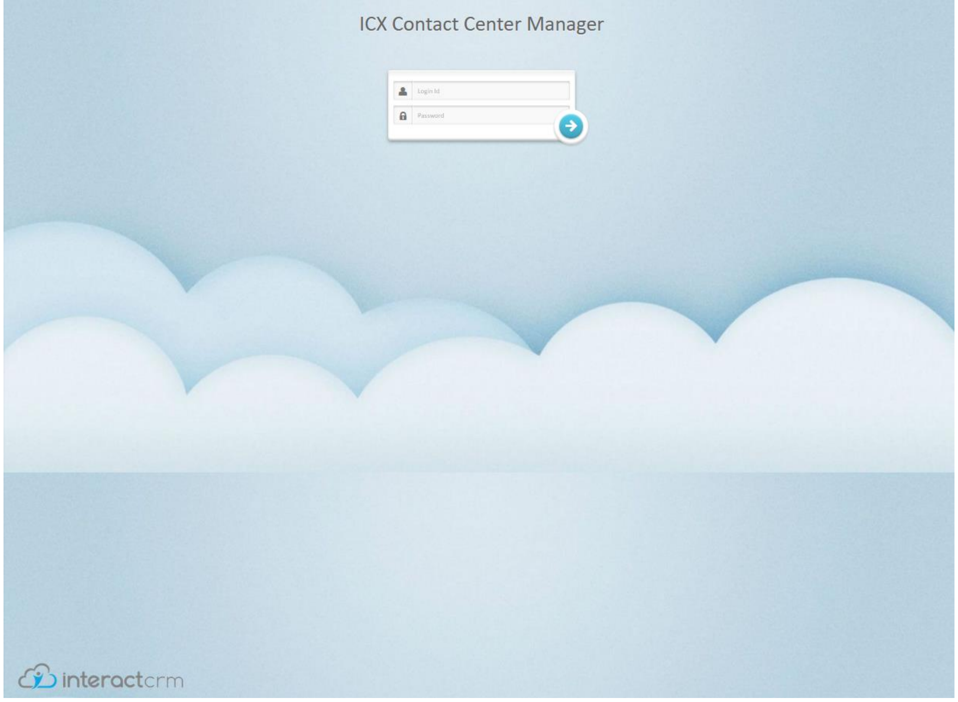
- Launch web interface
- Administer enterprise level properties
- Administer host config
- Administer stations
- Administer VDN settings

The configuration of Callback is performed by Interactcrm implementation specialists. The procedural steps are presented in these Application Notes for informational purposes. This section assumes the callback execution and offer slots have already been configured based on reference **[3]**.

7.1. Launch Web Interface

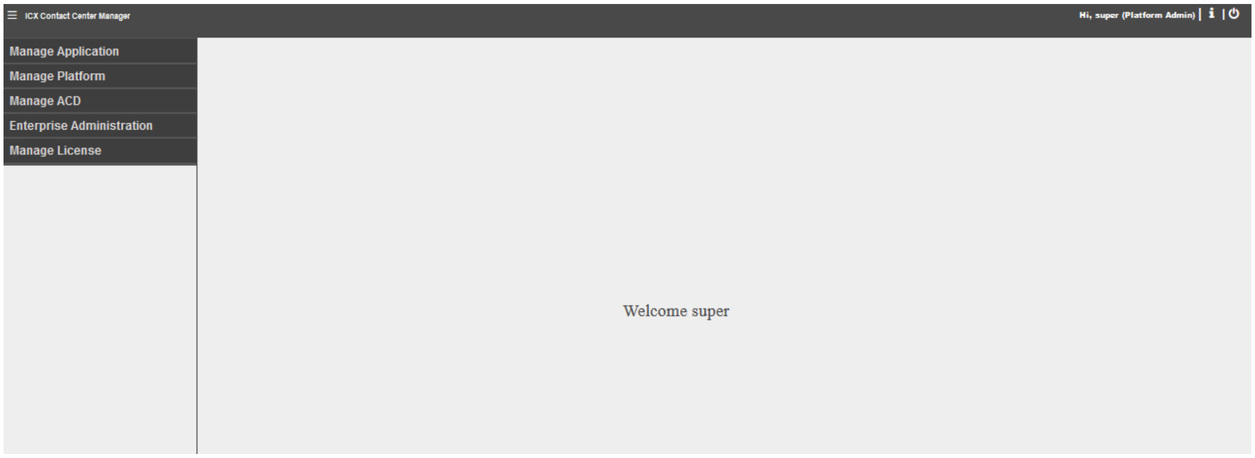
Launch the web interface by using the URL "https://ip-address:15050/ContactCenterManager" in an Internet Explorer browser window, where "ip-address" is the IP address of the ICX server running the Contact Center Manager component.

The **ICX Contact Center Manager** screen below is displayed. Log in using the appropriate credentials.



7.2. Administer Enterprise Level Properties

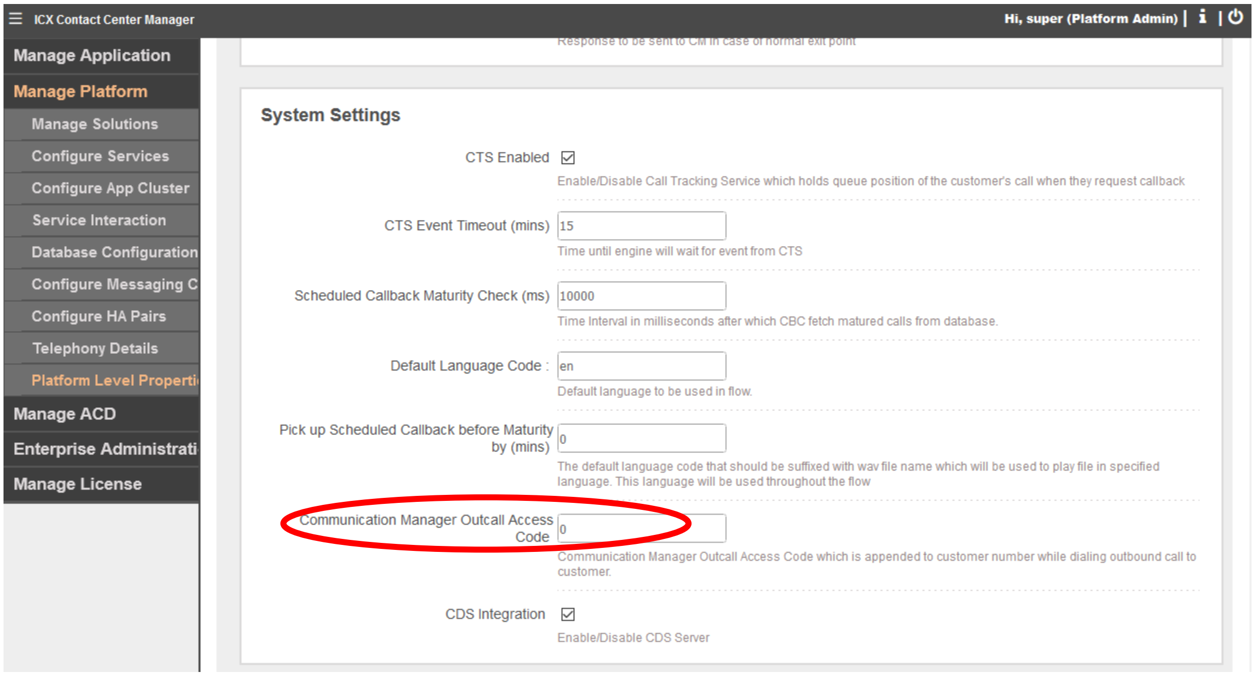
The **WELCOME** screen below is displayed


ICX Contact Center Manager
Hi, super (Platform Admin)
Manage Application
Manage Platform
Manage ACD
Enterprise Administration
Manage License

Welcome super

Select **Manage Platform → Platform Level Properties** in the left pane, to display the **Advanced Properties** screen. For **Section**, select “CallbackConnect” to display additional parameters (not shown).

Set **Communication Manager Outcall Access Code** to match the required ARS or AAR dialing prefix by Communication Manager for outbound calls to the PSTN. In the compliance testing, “0” is the ARS dialing prefix required by Communication Manager.



Response to be sent to CM in case of normal exit point

System Settings

CTS Enabled ☑
Enable/Disable Call Tracking Service which holds queue position of the customer's call when they request callback

CTS Event Timeout (mins) 15
Time until engine will wait for event from CTS

Scheduled Callback Maturity Check (ms) 10000
Time Interval in milliseconds after which CBC fetch matured calls from database.

Default Language Code : en
Default language to be used in flow.

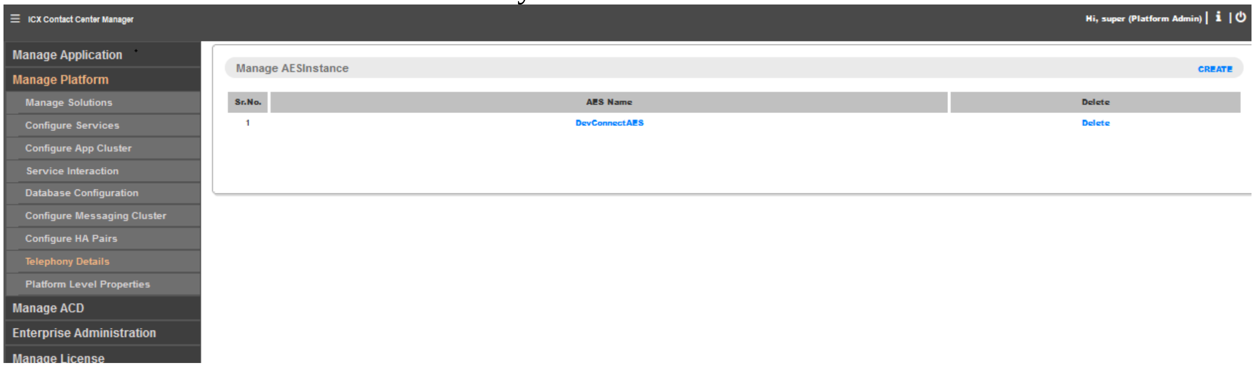
Pick up Scheduled Callback before Maturity by (mins) 0
The default language code that should be suffixed with wav file name which will be used to play file in specified language. This language will be used throughout the flow

Communication Manager Outcall Access Code 0
Communication Manager Outcall Access Code which is appended to customer number while dialing outbound call to customer.

CDS Integration ☑
Enable/Disable CDS Server

7.3. Administer Telephony Details

Select **Manage Platform→ Telephony Details** from the left pane, to display the Manage **AES Instance** screen. Click on the **AES** entry.

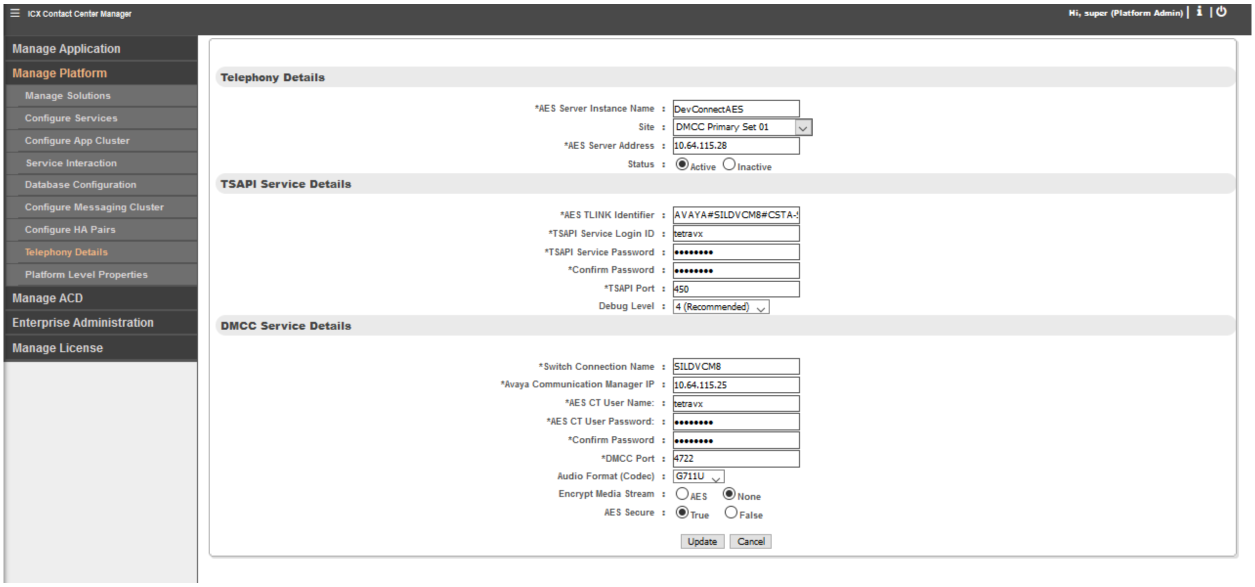


Sr.No.	AES Name	Delete
1	DevConnectAES	Delete

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

- **Switch Connection Name:** The switch connection name from **Section 6.5**.
- **Avaya CM IP:** IP address of the H.323 gatekeeper from **Section 0**.
- **AES Server Address:** IP address of Application Enablement Services.
- **AES CT UserName:** The ICX user credential from **Section 6.7**.
- **AES Password:** The ICX user credential from **Section 6.7**.
- **Confirm Password:** The ICX user credential from **Section 6.7**.
- **AES PORT:** The DMCC encrypted port number from **Section 6.9**.
- **Status:** "Active"

After the configuration has been created, edit the configuration, and set **Status** to **Active**.



Telephony Details

*AES Server Instance Name :	DevConnectAES
Site :	DMCC Primary Set 01
*AES Server Address :	10.64.115.28
Status :	● Active ○ Inactive

TSAPI Service Details

*AES TLINK Identifier :	AVAYA#SILDVCM8#CSTA-
*TSAPI Service Login ID :	tetravx
*TSAPI Service Password :	●●●●●●●●●
*Confirm Password :	●●●●●●●●●
*TSAPI Port :	450
Debug Level :	4 (Recommended)

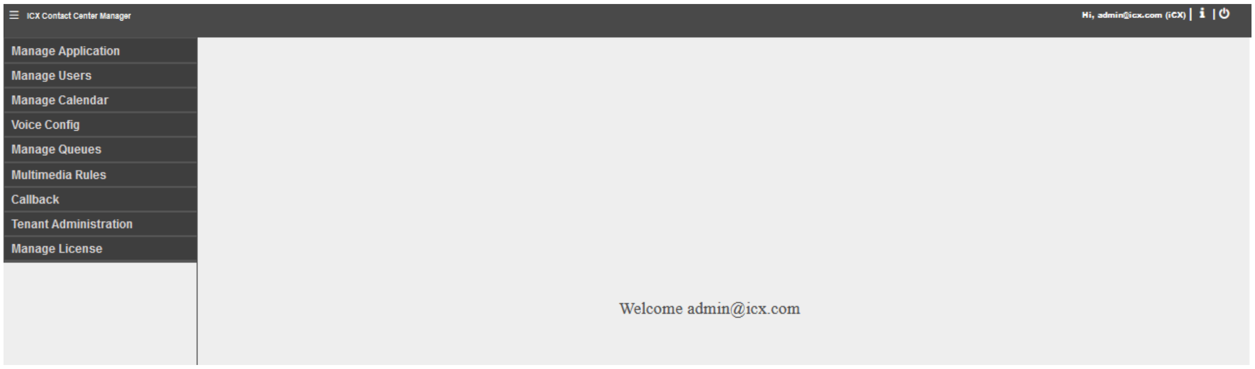
DMCC Service Details

*Switch Connection Name :	SILDVCM8
*Avaya Communication Manager IP :	10.64.115.25
*AES CT User Name: :	tetravx
*AES CT User Password: :	●●●●●●●●●
*Confirm Password :	●●●●●●●●●
*DMCC Port :	4722
Audio Format (Codec) :	G711U
Encrypt Media Stream :	○ AES ● None
AES Secure :	● True ○ False

7.4. Administer Stations

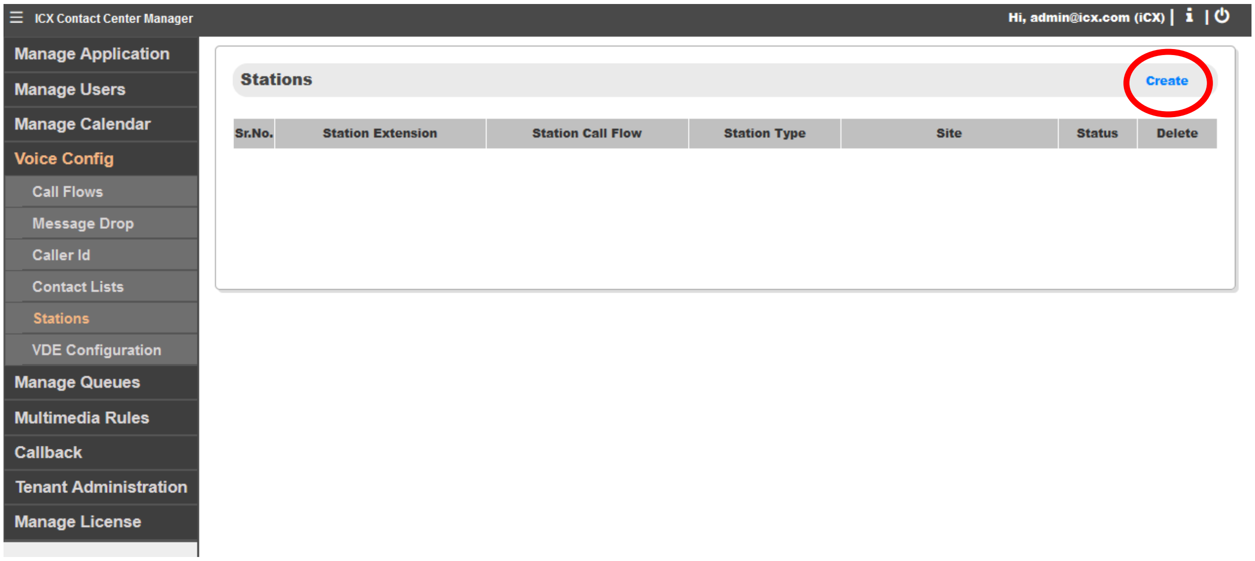
Follow reference **[3]** to create a tenant group and an administrative user for the tenant group.

Use the procedures in **Section 7.1** to launch the web interface, and log in using an administrative account, in this case admin@icx.com



Welcome admin@icx.com

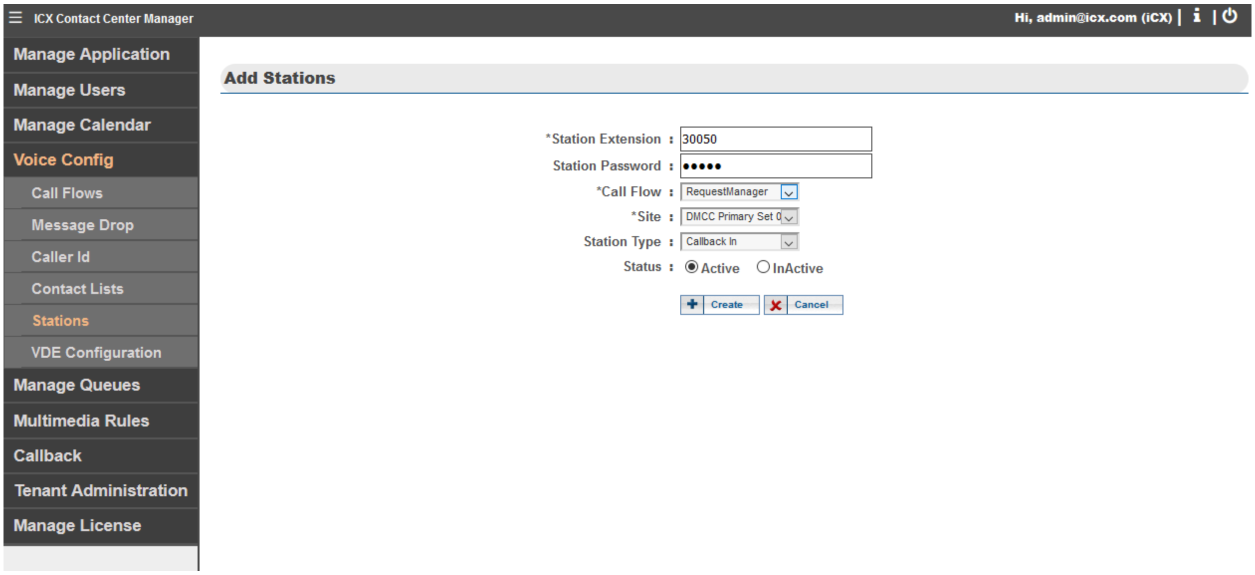
Select **Voice Config → Stations** in the left pane, to display the **Stations** screen. Click **Create**.



Sr.No.	Station Extension	Station Call Flow	Station Type	Site	Status	Delete

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

- **Station Extension:** The first virtual IP softphone extension from **Section** Error! Reference source not found..
- **Station Password:** The first virtual IP softphone security code from **Section** Error! Reference source not found..
- **Call Flow:** "RequestManager"
- **Site:** Select the applicable site.
- **Station Type:** "Callback In"
- **Status:** "Active"

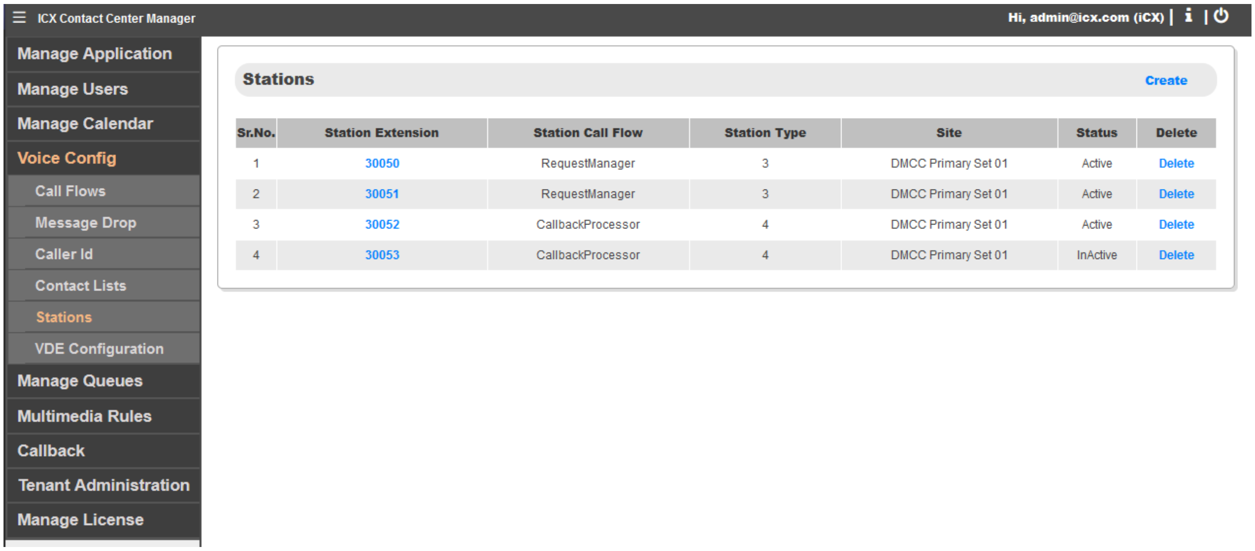


Add Stations

*Station Extension : 30050
Station Password : ●●●●●
*Call Flow : RequestManager
*Site : DMCC Primary Set 0
Station Type : Callback In
Status : ● Active ○ InActive

Repeat this section to create a station for each virtual IP softphone from **Section** Error! Reference source not found.. For **Station Call Flow** and **Station Type**, select "RequestManager" and "CBC Inbound" for the inbound virtual IP softphones, and "CallbackProcessor" and "CBC Outbound" for the outbound virtual IP softphones.

In the compliance testing, four stations were created, as shown below.

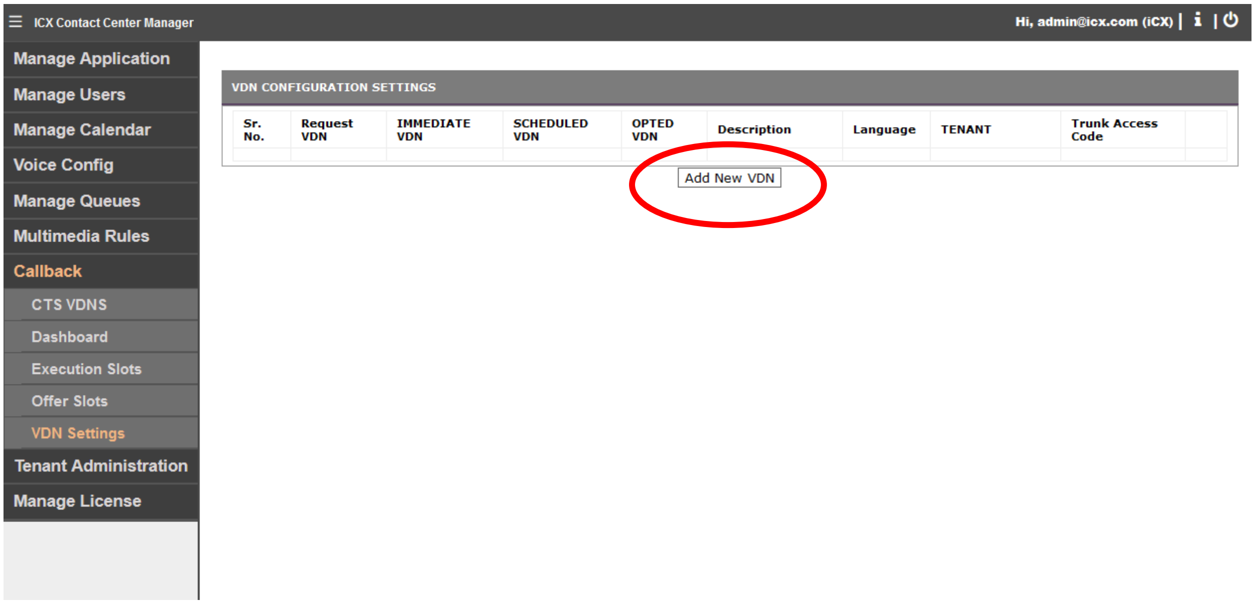


Stations

Sr.No.	Station Extension	Station Call Flow	Station Type	Site	Status	Delete
1	30050	RequestManager	3	DMCC Primary Set 01	Active	Delete
2	30051	RequestManager	3	DMCC Primary Set 01	Active	Delete
3	30052	CallbackProcessor	4	DMCC Primary Set 01	Active	Delete
4	30053	CallbackProcessor	4	DMCC Primary Set 01	InActive	Delete

7.5. Administer VDN Settings

Scroll the left pane as necessary and select **Callback → VDN Settings** to display the **VDN CONFIGURATION SETTINGS** screen. Click **Add New VDN**.

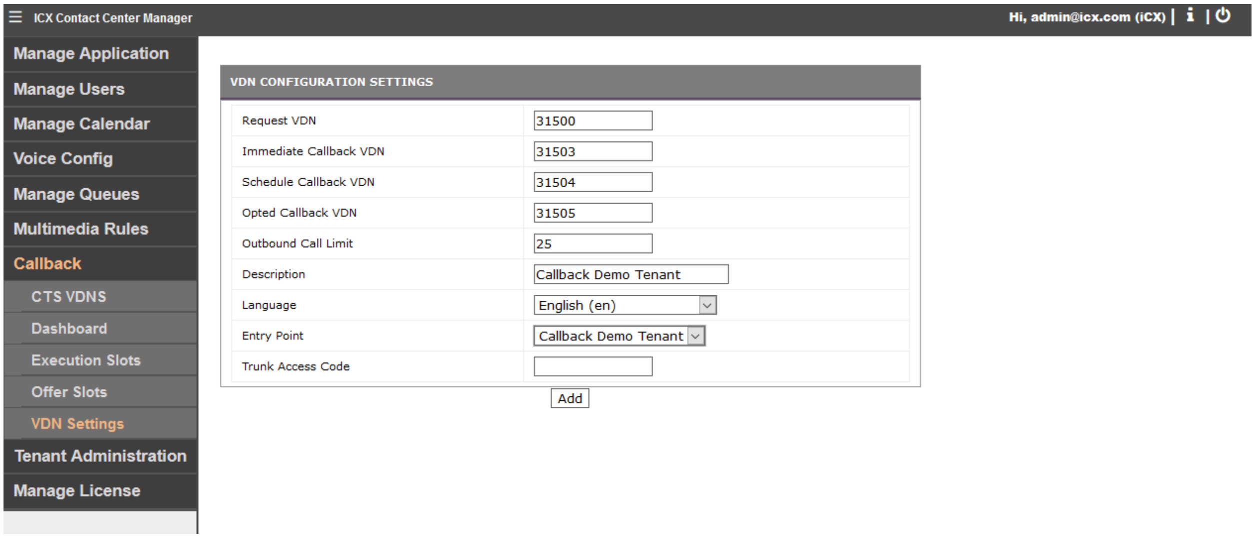


VDN CONFIGURATION SETTINGS

Sr. No.	Request VDN	IMMEDIATE VDN	SCHEDULED VDN	OPTED VDN	Description	Language	TENANT	Trunk Access Code

The **VDN CONFIGURATION SETTINGS** screen is displayed. Enter the following values for the specified fields and retain the default values for the remaining fields.

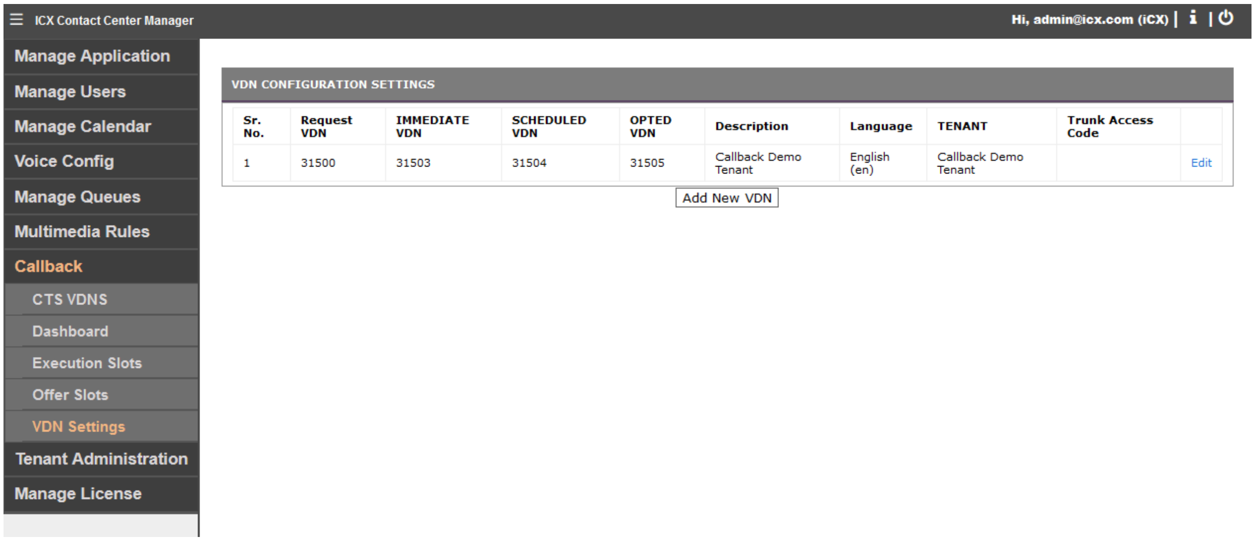
- **Request VDN:** The first inbound VDN extension from **Section** Error! Reference source not found..
- **Immediate Callback VDN:** The first outbound VDN extension from **Section 5.8**.
- **Schedule Callback VDN:** The first outbound VDN extension from **Section 5.8**.
- **Opted Callback VDN:** The first outbound VDN extension from **Section 5.8**.
- **Description:** A desired description.



VDN CONFIGURATION SETTINGS

Request VDN	31500
Immediate Callback VDN	31503
Schedule Callback VDN	31504
Opted Callback VDN	31505
Outbound Call Limit	25
Description	Callback Demo Tenant
Language	English (en)
Entry Point	Callback Demo Tenant
Trunk Access Code	

Repeat this section to map all inbound VDN from **Section** Error! Reference source not found. to outbound VDN in **Section 5.8**. In the compliance testing, one VDN mappings were created, as shown below.



VDN CONFIGURATION SETTINGS

Sr. No.	Request VDN	IMMEDIATE VDN	SCHEDULED VDN	OPTED VDN	Description	Language	TENANT	Trunk Access Code	
1	31500	31503	31504	31505	Callback Demo Tenant	English (en)	Callback Demo Tenant		Edit

8. Verification Steps

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

8.1. 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** Error! Reference source not found., as shown below.

```
status aesvcs cti-link

                          AE SERVICES CTI LINK STATUS

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

1     9        no    sildvaes8        established   15       15
```

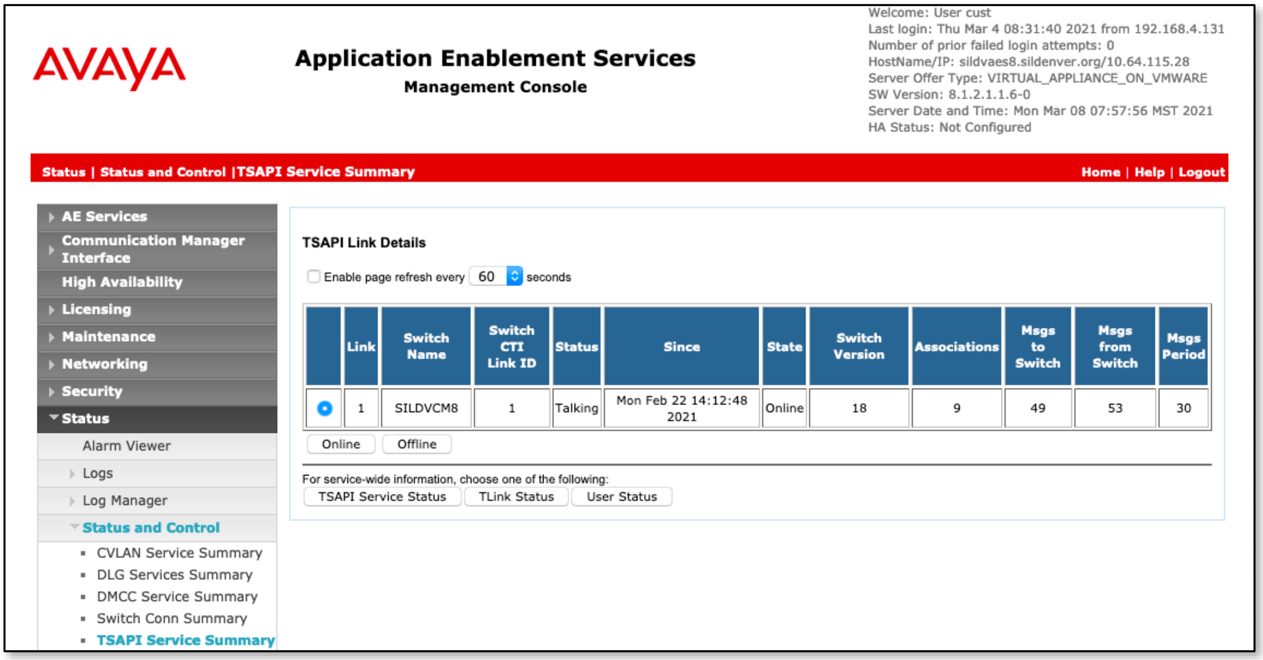
Verify the registration status of virtual IP softphones by using the “list registered-ip-stations” command. Verify that all virtual IP softphone extensions from **Section 5.3** are displayed along with the IP address of the Application Enablement Services server, as shown below.

```
list registered-ip-stations

                            REGISTERED IP STATIONS

Station Ext      Set Type/ Prod ID/    Station IP Address/
or Orig Port     Net Rgn   Release     Gatekeeper IP Address
  Socket
30002            9611      IP_Phone    192.168.4.133
  tcp            2         6.6506      10.64.115.25
30004            9650      IP_Phone    10.64.115.31
  tcp            1         3.280A      10.64.115.25
30007            9650      IP_Agent    10.64.115.36
  tcp            1         9.0         10.64.115.25
30008            9650      IP_Agent    10.64.115.34
  tcp            1         9.0         10.64.115.25
30050            9608      IP_API_A    10.64.115.28
  tcp            2         3.2040      10.64.115.25
30051            9608      IP_API_A    10.64.115.28
  tcp            2         3.2040      10.64.115.25
30052            9608      IP_API_A    10.64.115.28
  tcp            2         3.2040      10.64.115.25
```

8.2. 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 that the **Status** is "Talking" for the TSAPI link administered in **Section 6.5**, as shown below. Also verify that the corresponding **Associations** value reflects the total number of virtual IP softphones from **Section** Error! Reference source not found., this should reflect the number of agents logged in, and the number of Callback DMCC ports registered.



Welcome: User cust
Last login: Thu Mar 4 08:31:40 2021 from 192.168.4.131
Number of prior failed login attempts: 0
HostName/IP: sildvaes8.sildenver.org/10.64.115.28
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.1.2.1.1.6-0
Server Date and Time: Mon Mar 08 07:57:56 MST 2021
HA Status: Not Configured

TSAPI Link Details

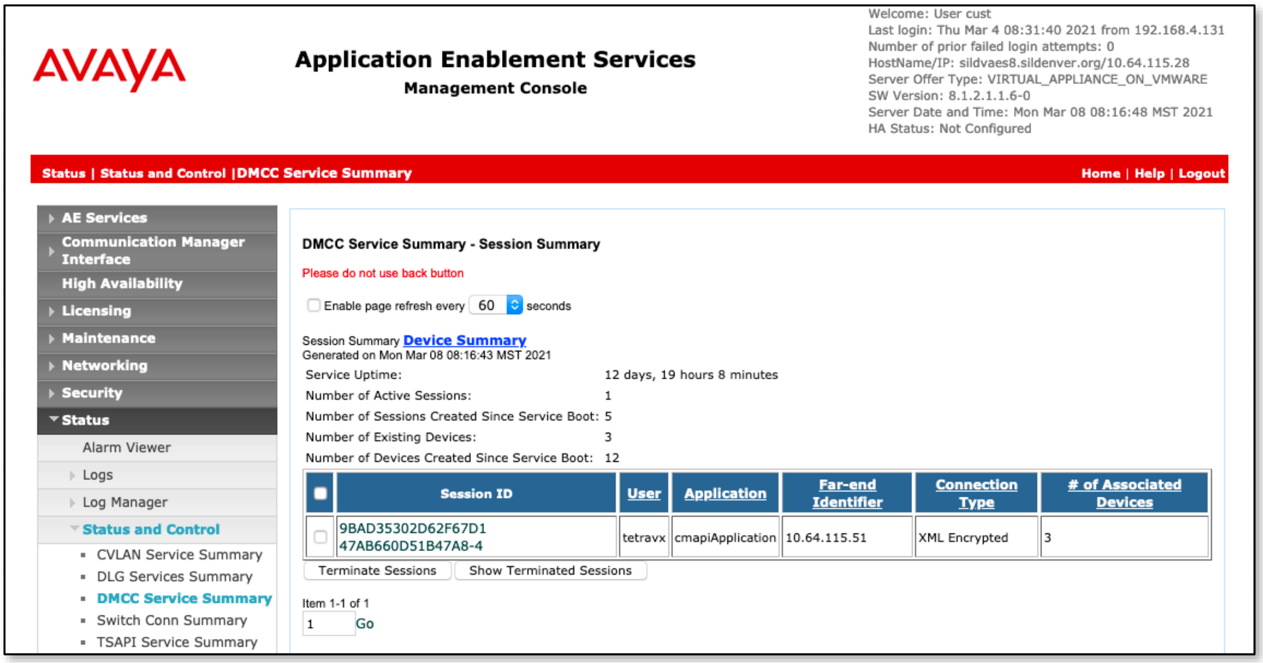
☐ Enable page refresh every 60 seconds

	Link	Switch Name	Switch CTI Link ID	Status	Since	State	Switch Version	Associations	Msgs to Switch	Msgs from Switch	Msgs Period
●	1	SILDVCM8	1	Talking	Mon Feb 22 14:12:48 2021	Online	18	9	49	53	30

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

Verify the status of the DMCC link by selecting **Status → Status and Control → DMCC Service Summary** from the left pane. The **DMCC Service Summary – Session Summary** screen is displayed.

In the lower portion of the screen, verify that the **User** column shows an active session with the ICX user name from **Section 6.7**, and that the **# of Associated Devices** column reflects the number of virtual IP softphones from **Section** Error! Reference source not found..



Welcome: User cust
Last login: Thu Mar 4 08:31:40 2021 from 192.168.4.131
Number of prior failed login attempts: 0
HostName/IP: sildvaes8.sildenver.org/10.64.115.28
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.1.2.1.1.6-0
Server Date and Time: Mon Mar 08 08:16:48 MST 2021
HA Status: Not Configured

DMCC Service Summary - Session Summary

Please do not use back button

☐ Enable page refresh every 60 seconds

Session Summary Device Summary
Generated on Mon Mar 08 08:16:43 MST 2021

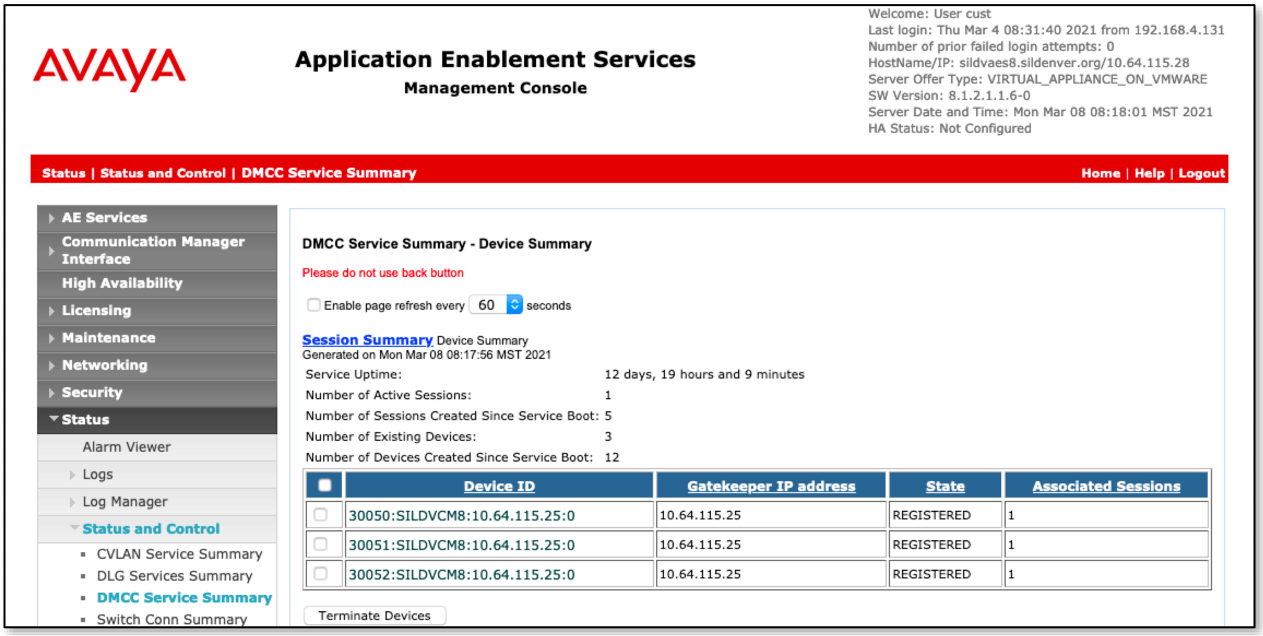
Service Uptime:	12 days, 19 hours 8 minutes
Number of Active Sessions:	1
Number of Sessions Created Since Service Boot:	5
Number of Existing Devices:	3
Number of Devices Created Since Service Boot:	12

☐	Session ID	User	Application	Far-end Identifier	Connection Type	# of Associated Devices
☐	9BAD35302D62F67D1 47AB660D51B47A8-4	tetravx	cmapiApplication	10.64.115.51	XML Encrypted	3

Item 1-1 of 1

1

Click on the **Device Summary** link (above) to verify the DMCC ports registered to Callback.



Welcome: User cust
Last login: Thu Mar 4 08:31:40 2021 from 192.168.4.131
Number of prior failed login attempts: 0
HostName/IP: sildvaes8.sildenver.org/10.64.115.28
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.1.2.1.1.6-0
Server Date and Time: Mon Mar 08 08:18:01 MST 2021
HA Status: Not Configured

DMCC Service Summary - Device Summary

Please do not use back button

☐ Enable page refresh every 60 seconds

Session Summary Device Summary
Generated on Mon Mar 08 08:17:56 MST 2021

Service Uptime:	12 days, 19 hours and 9 minutes
Number of Active Sessions:	1
Number of Sessions Created Since Service Boot:	5
Number of Existing Devices:	3
Number of Devices Created Since Service Boot:	12

☐	Device ID	Gatekeeper IP address	State	Associated Sessions
☐	30050:SILDVCM8:10.64.115.25:0	10.64.115.25	REGISTERED	1
☐	30051:SILDVCM8:10.64.115.25:0	10.64.115.25	REGISTERED	1
☐	30052:SILDVCM8:10.64.115.25:0	10.64.115.25	REGISTERED	1

8.3. Verify ICX Callback

Place an incoming ACD call to an inbound VDN with the skill group EWT exceeding the configured threshold. Verify that the caller hears the proper announcement from Communication Manager and can enter DTMF input to select the callback option.

Upon selecting the callback option, verify that the caller hears the proper playback of the media file directed to be played by Callback, and can enter DTMF input to schedule a callback call.

When time to place the callback call, verify that Callback launches an outbound call to the proper outbound VDN. When the callback call is answered by an available agent, verify that Callback adds the original caller onto the call with the agent.

9. Conclusion

These Application Notes describe the configuration steps required for ICX Callback to successfully interoperate with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services. All feature and serviceability test cases were completed with observations noted in **Section** Error! Reference source not found..

10. Additional References

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

1. *Administering Avaya Aura® Communication Manager*, Release 8.1.X available at http://support.avaya.com.

2. *Administering and Maintaining Aura® Application Enablement Services*, Release 8.1.X, available at http://support.avaya.com.

3. *Interactcrm ICX Callback Installation Guide*, ICX Version 3.17.6.1, available upon request to Interactcrm Support.

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.