Application Notes for Interactcrm 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 Interactcrm 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 Interactcrm Customer Experience Platform (ICX) 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 based.

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 Interactcrm 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.

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 the following were observations on Callback:

- The application does not support TSAPI user credentials that contained the special character semicolon.

- The default out-of-box call flows and sample media files played the same busy announcement to the agent regardless of whether the outbound callback call to the customer received busy or invalid number results.

2.3. Support

Technical support on Callback can be obtained through the following:

- **Phone:** (510) 795-7645
- **Email:** usa@interactcrm.com

3. Reference Configuration

ICX with Callback can be configured on a single server or with components distributed across multiple servers. The compliance test configuration used a single server configuration, as shown in **Figure 1**.

The detailed administration of basic connectivity between Communication Manager and Application Enablement Services, and of contact center devices are not the focus of these Application Notes and will not be described.

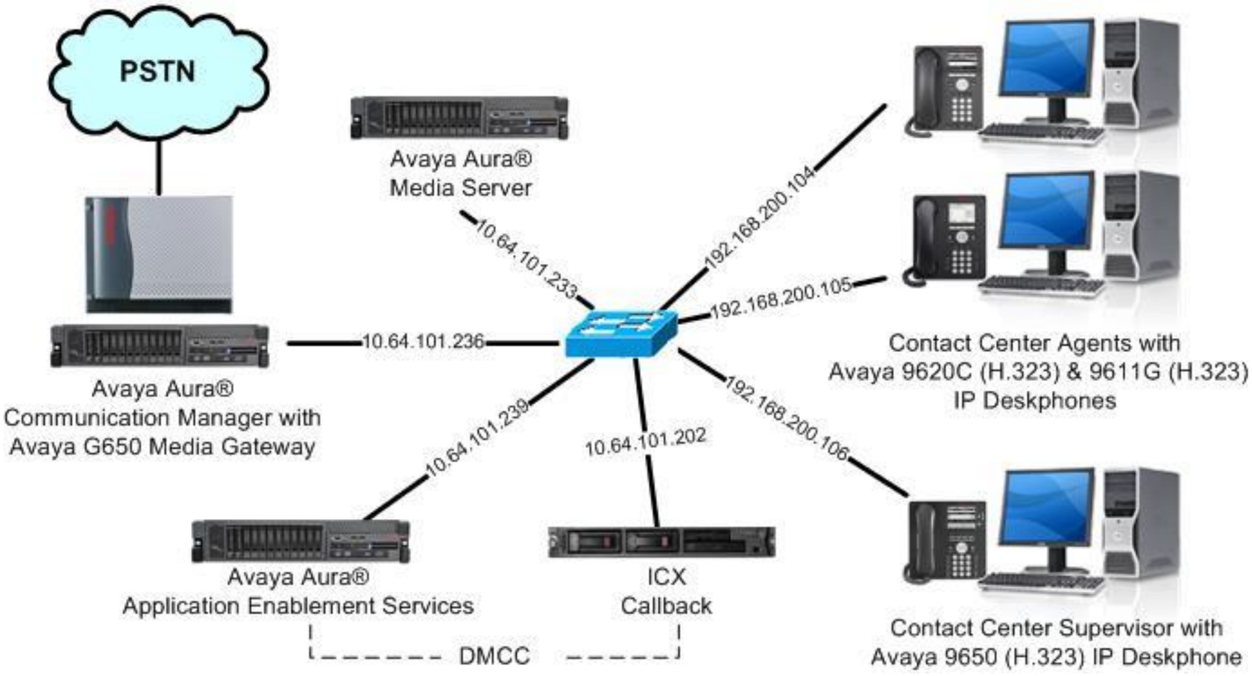


Figure 1: Compliance Testing Configuration

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	7.0.1 (7.0.1.0.0.441.23012)
Avaya G650 Media Gateway	NA
Avaya Aura® Media Server in Virtual Environment	7.7.0.334
Avaya Aura® Application Enablement Services in Virtual Environment	7.0.1 (7.0.1.0.1.15)
Avaya 9620C & 9650 IP Deskphones (H.323)	3.260A
Avaya 9611G IP Deskphone (H.323)	6.6115
ICX on Windows Server 2012 R2 Standard • Callback • Avaya DMCC Java Windows SDK	3.0.16 (Build 118) NA 4.2.6.3_test 6.2.0.69

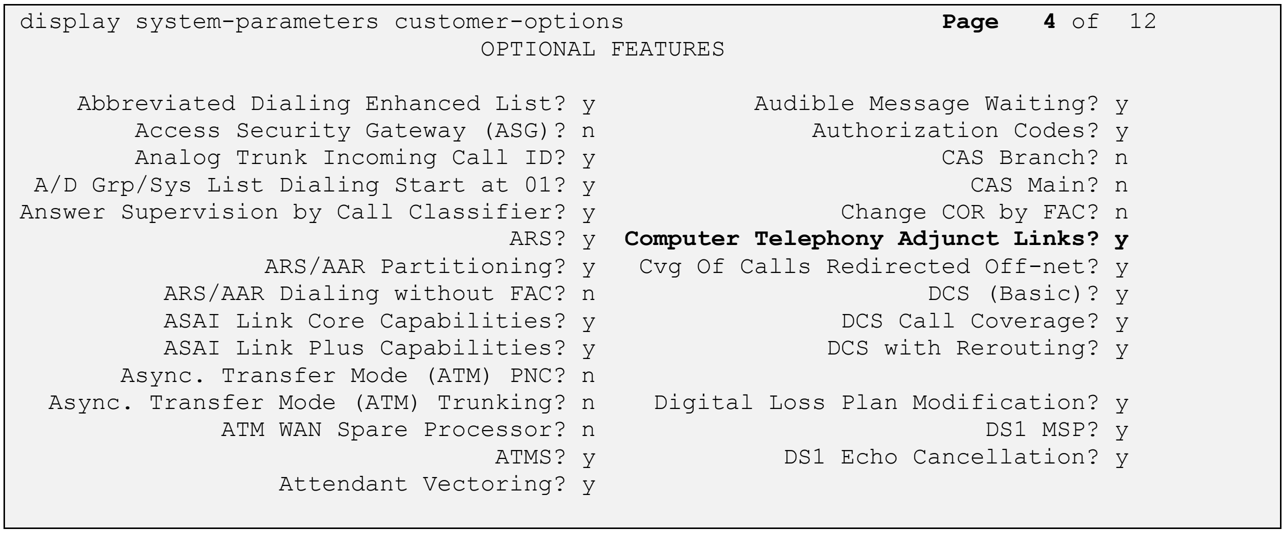
5. Configure Avaya Aura® Communication Manager

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

- Verify 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

5.1. Verify License

Log in to the System Access Terminal 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 to verify that the **Computer Telephony Adjunct Links** customer option is set to "y" on **Page 4**. If this option is not set to "y", then contact the Avaya sales team or business partner for a proper license file.



```
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
```

Navigate to **Page 7**, and verify that the **Vectoring (Basic)** and **Vectoring (Prompting)** customer options are 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
```

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 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: 60111
     Type: ADJ-IP
                                                                    COR: 1

     Name: AES CTI Link
```

5.3. Administer Virtual IP Softphones

Add a virtual IP softphone using the "add station n" command, where "n" is an available extension number. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Type:** "4620"
- **Name:** A descriptive name.
- **Security Code:** A desired value.
- **IP SoftPhone:** "y"

```
add station 65991                                               Page   1 of   5
                                     STATION

Extension: 65991                         Lock Messages? n               BCC: 0
     Type: 4620                          Security Code: 123456           TN: 1
     Port: IP                          Coverage Path 1:                 COR: 1
     Name: ICX DMCC Inb #1             Coverage Path 2:                 COS: 1
                                       Hunt-to Station:               Tests? y
STATION OPTIONS
                Location:                      Time of Day Lock Table:
              Loss Group: 19         Personalized Ringing Pattern: 1
                                                 Message Lamp Ext: 65991
            Speakerphone: 2-way                Mute Button Enabled? y
        Display Language: english                Expansion Module? n
 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
```

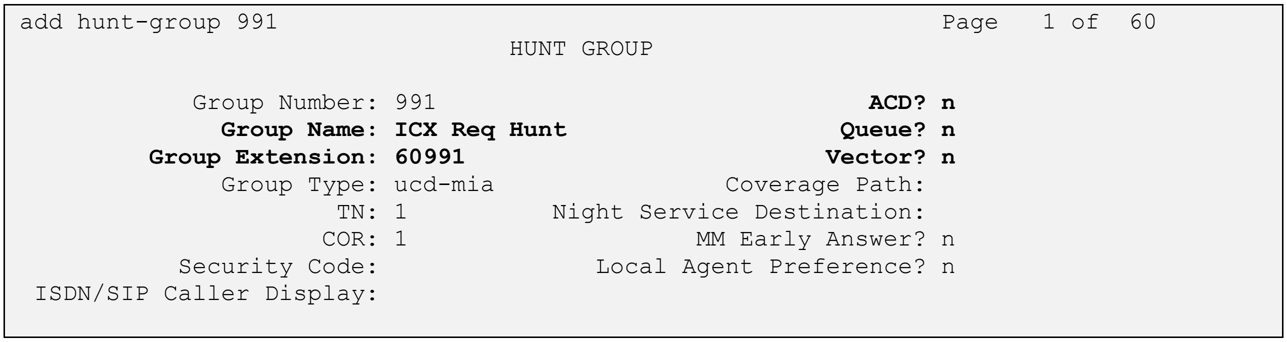
Repeat this section to administer the desired number of virtual IP softphones for handling inbound and outbound calls. In the compliance testing, four virtual IP softphones were configured as shown below. The first two softphones with extensions 65991-2 were used for handling inbound callback requests, and the last two softphones with extensions 65993-4 were used for handling outbound callback calls.

```
list station 65991 count 4

                                  STATIONS

Ext/          Port/   Name/                       Room/       Cv1/ COR/   Cable/
 Hunt-to       Type      Surv GK NN        Move    Data Ext    Cv2  COS TN Jack

65991         S00113  ICX DMCC Req1                                 1
               4620                        no                        1
65992         S00116  ICX DMCC Req2                                 1
               4620                        no                        1
65993         S00120  ICX DMCC CB1                                  1
               4620                        no                        1
65994         S00123  ICX DMCC CB2                                  1
               4620                        no                        1
```

5.4. Administer Inbound Hunt Group

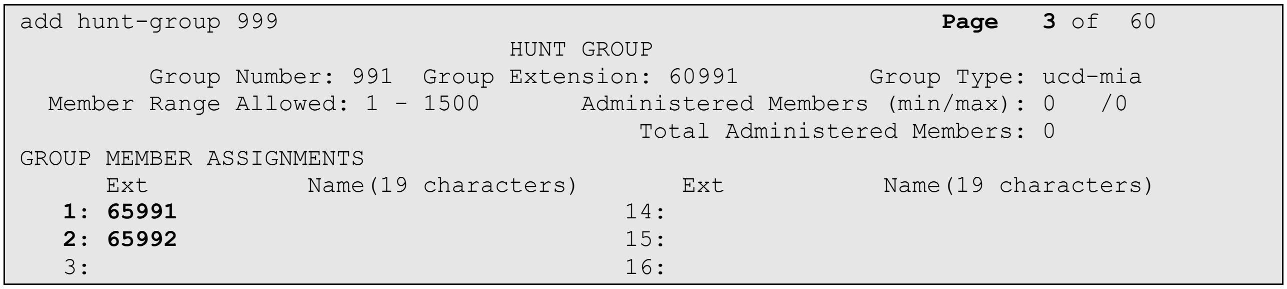
Administer a hunt group to be used for routing of inbound calls to Callback. Use the "add hunt-group n" command, where "n" is an available hunt group number. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Group Name:** A descriptive name.
- **Group Extension:** An available extension number.
- **ACD:** "n"
- **Queue:** "n"
- **Vector:** "n"



```
add hunt-group 991                                                Page   1 of  60
                                  HUNT GROUP

            Group Number: 991                             ACD? n
              Group Name: ICX Req Hunt                  Queue? n
         Group Extension: 60991                        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.

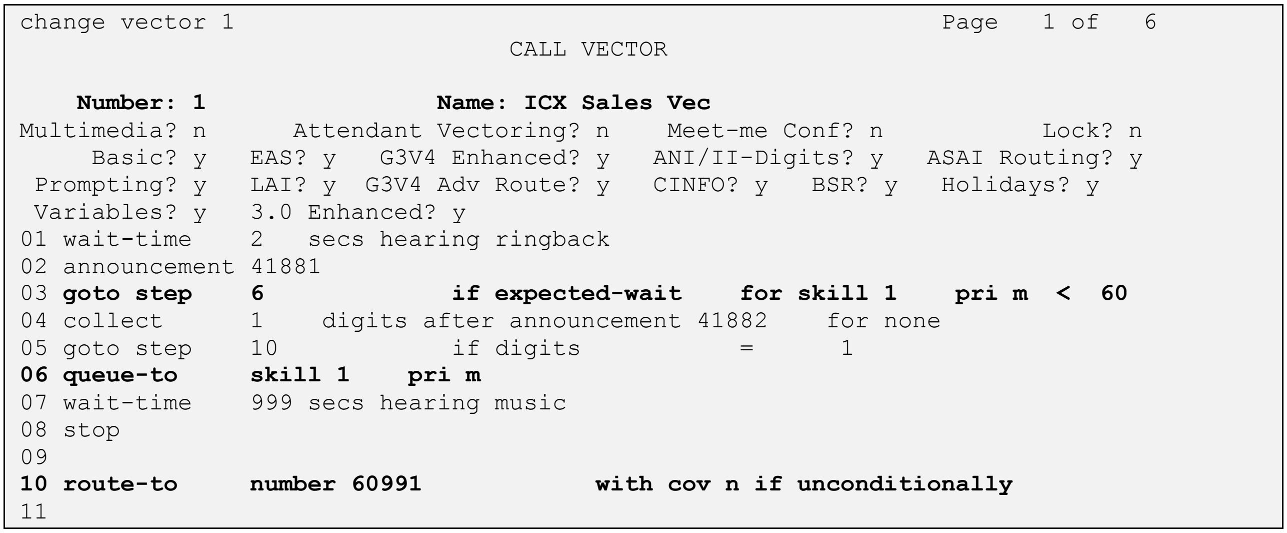


```
add hunt-group 999                                                Page   3 of  60
                                  HUNT GROUP
         Group Number: 991  Group Extension: 60991         Group Type: ucd-mia
  Member Range Allowed: 1 - 1500       Administered Members (min/max): 0   /0
                                           Total Administered Members: 0
GROUP MEMBER ASSIGNMENTS
      Ext           Name(19 characters)       Ext           Name(19 characters)
   1: 65991                              14:
   2: 65992                              15:
   3:                                    16:
```

5.5. Administer Inbound Vectors

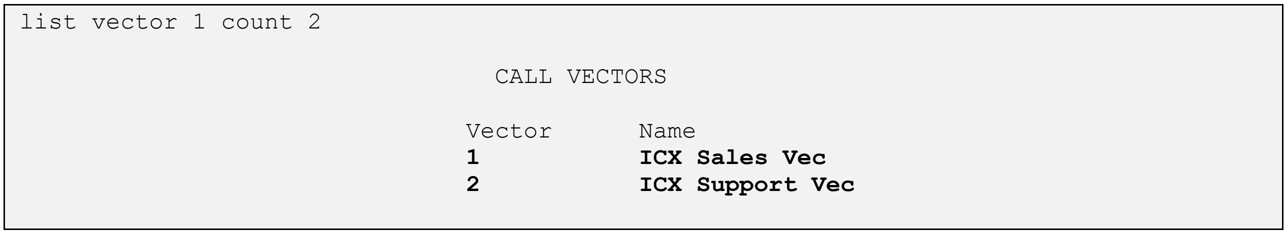
Modify an available vector using the “change vector n” command, where “n” is an existing vector number. The vector will be used to handle incoming ACD calls, to check EWT, and route calls to Callback when the EWT is over the desired threshold with customer opted to be called back.

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 inbound hunt group extension from **Section 5.4**.



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

    Number: 1                Name: ICX Sales Vec
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 41881
03 goto step    6            if expected-wait    for skill 1    pri m  <  60
04 collect      1    digits after announcement 41882    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 60991            with cov n if unconditionally
11
```

Repeat this section to administer all desired vectors where callback option is to be provided. In the compliance testing, two inbound vectors were configured as shown below.



```
list vector 1 count 2

                                 CALL VECTORS

                               Vector      Name
                               1           ICX Sales Vec
                               2           ICX Support Vec
```

5.6. Administer Inbound 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 5.5** for **Vector Number**. Retain the default values for all remaining fields.

```
add vdn 60001                                                 Page   1 of   3
                            VECTOR DIRECTORY NUMBER

                             Extension: 60001
                                 Name*: ICX Sales
                           Destination: Vector Number        1
                   Attendant Vectoring? n
                  Meet-me Conferencing? n
                    Allow VDN Override? n
                                   COR: 1
                                   TN*: 1
                              Measured: none     Report Adjunct Calls as ACD*? n
```

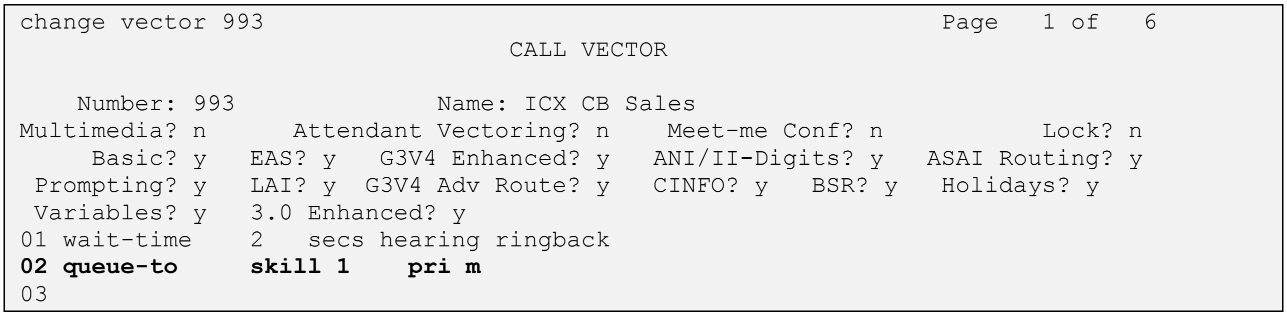
Repeat this section to administer a VDN for each vector from **Section 5.5**. In the compliance testing, two inbound VDNs were configured as shown below.

```
list vdn 60001 count 2

                          VECTOR DIRECTORY NUMBERS

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

ICX Sales              60001           n   1   1    V  1    none

ICX Support            60002           n   1   1    V  2    none
```

5.7. Administer Outbound Vectors

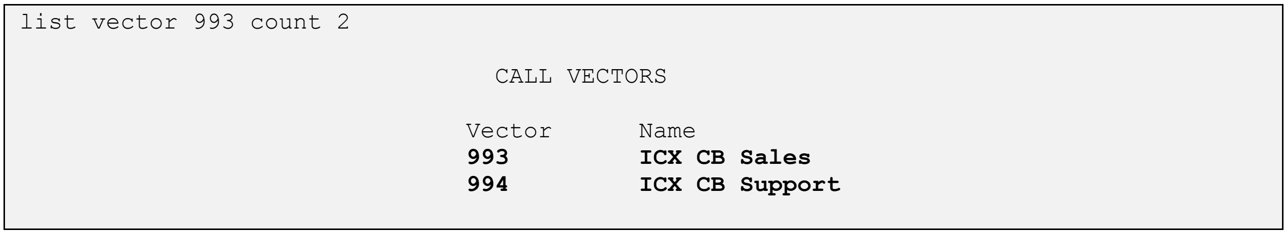
Modify an available vector using the “change vector n” command, where “n” is an existing vector number. This vector will be used to route outbound callback calls to the proper skill group.

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 993                                               Page   1 of   6
                                  CALL VECTOR

    Number: 993              Name: ICX CB Sales
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
```

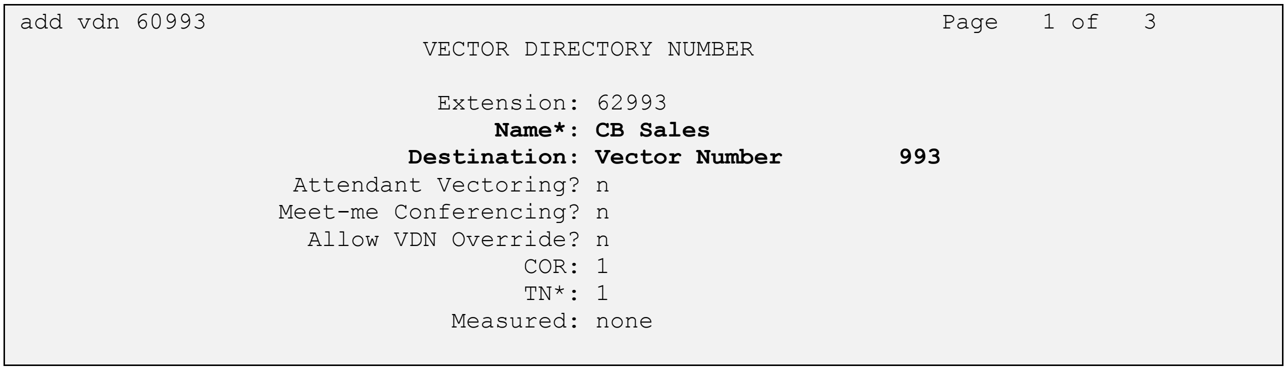
Repeat this section to administer an outbound vector for each inbound vector with callback options from **Section 5.5**. In the compliance testing, two outbound vectors were configured as shown below.



```
list vector 993 count 2

                                 CALL VECTORS

                               Vector      Name
                               993         ICX CB Sales
                               994         ICX CB Support
```

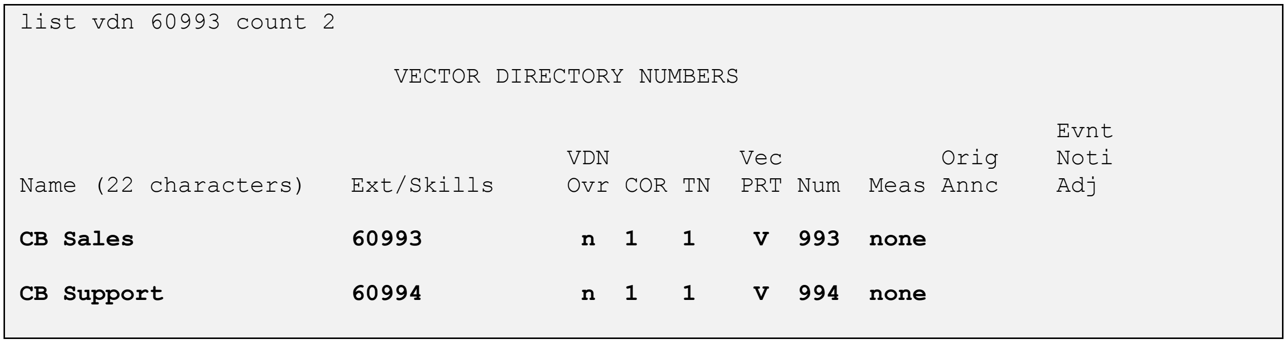
5.8. Administer Outbound VDNs

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 60993                                                   Page   1 of   3
                            VECTOR DIRECTORY NUMBER

                             Extension: 62993
                                 Name*: CB Sales
                           Destination: Vector Number        993
                   Attendant Vectoring? n
                  Meet-me Conferencing? n
                    Allow VDN Override? n
                                   COR: 1
                                   TN*: 1
                              Measured: none
```

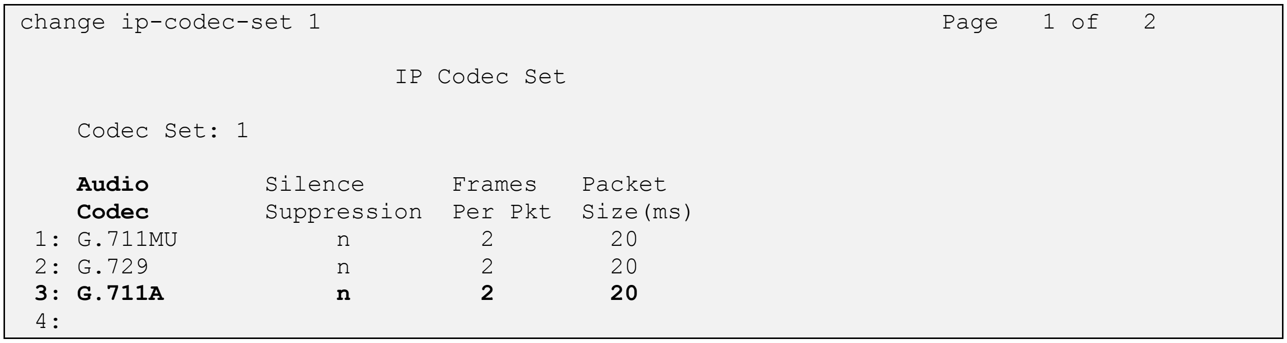
Repeat this section to administer a VDN for each vector from **Section 5.7**. In the compliance testing, two outbound VDNs were configured as shown below.



```
list vdn 60993 count 2

                          VECTOR DIRECTORY NUMBERS

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

CB Sales                 60993           n  1   1    V  993  none

CB Support               60994           n  1   1    V  994  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 Codec Set

    Codec Set: 1

    Audio        Silence      Frames   Packet
    Codec        Suppression  Per Pkt  Size(ms)
 1: G.711MU          n          2        20
 2: G.729            n          2        20
 3: G.711A           n          2        20
 4:
```

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
- Restart services
- Obtain Tlink name

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.

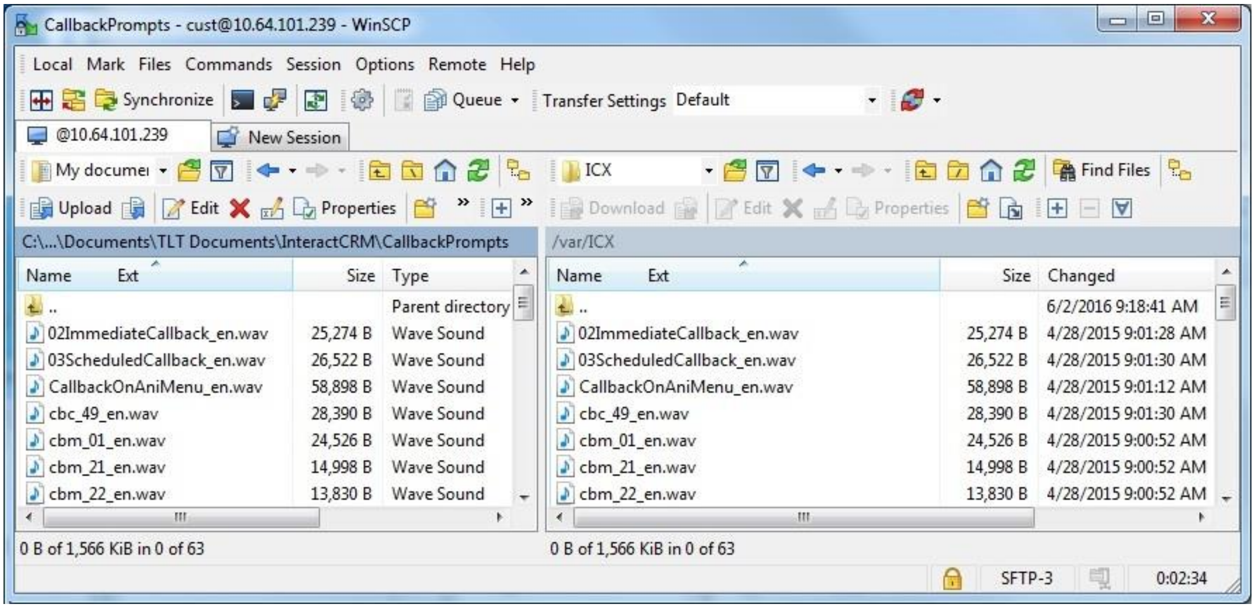
Enter the command “cd /var”, followed by “mkdir ICX” to create a directory. Note that the name of the directory can vary.

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

```
[xx@aes7 ~]# cd /var

[xx@aes7 var]# mkdir ICX

[xx@aes7 var]# chmod 777 ICX
```

A set of sample media files used by the out-of-box call flows is provided by Interactcrm. 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 a tool such as WinSCP to transfer the media files to Application Enablement Services. Place the media files under the directory that was created above, as shown below.


CallbackPrompts - cust@10.64.101.239 - WinSCP
Local Mark Files Commands Session Options Remote Help
Synchronize
Queue
Transfer Settings Default
@10.64.101.239
New Session
My docume
Upload Edit Properties
ICX
Find Files
Download Edit Properties

C:\...\Documents\TLT Documents\InteractCRM\CallbackPrompts

Name Ext	Size	Type
..		Parent directory
02ImmediateCallback_en.wav	25,274 B	Wave Sound
03ScheduledCallback_en.wav	26,522 B	Wave Sound
CallbackOnAniMenu_en.wav	58,898 B	Wave Sound
cbc_49_en.wav	28,390 B	Wave Sound
cbm_01_en.wav	24,526 B	Wave Sound
cbm_21_en.wav	14,998 B	Wave Sound
cbm_22_en.wav	13,830 B	Wave Sound

0 B of 1,566 KiB in 0 of 63

/var/ICX

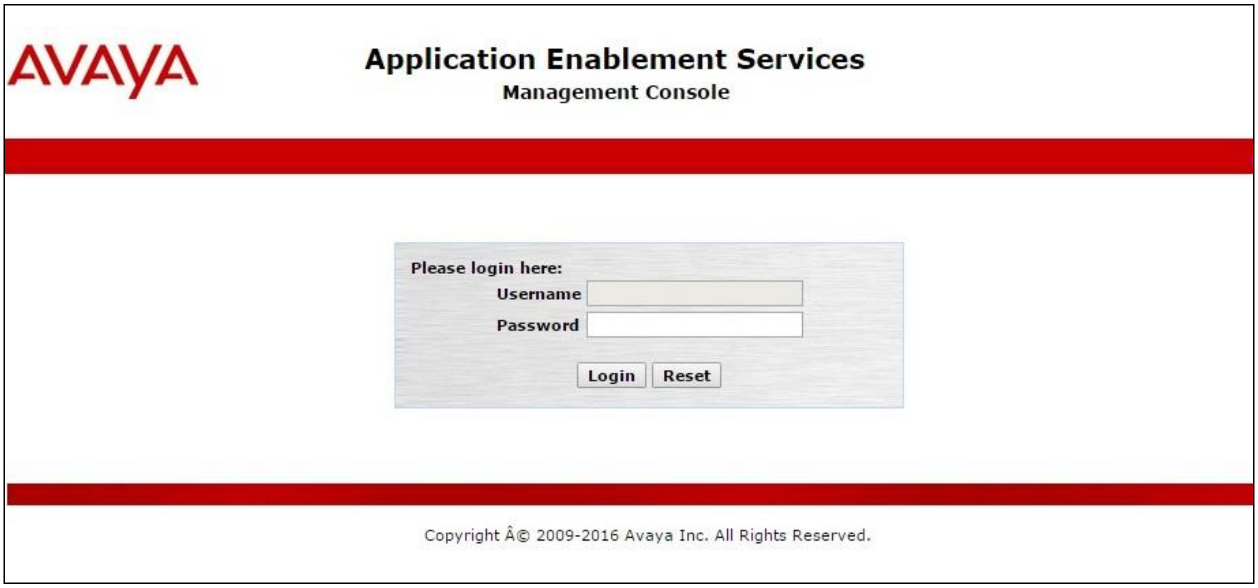
Name Ext	Size	Changed
..		6/2/2016 9:18:41 AM
02ImmediateCallback_en.wav	25,274 B	4/28/2015 9:01:28 AM
03ScheduledCallback_en.wav	26,522 B	4/28/2015 9:01:30 AM
CallbackOnAniMenu_en.wav	58,898 B	4/28/2015 9:01:12 AM
cbc_49_en.wav	28,390 B	4/28/2015 9:01:30 AM
cbm_01_en.wav	24,526 B	4/28/2015 9:00:52 AM
cbm_21_en.wav	14,998 B	4/28/2015 9:00:52 AM
cbm_22_en.wav	13,830 B	4/28/2015 9:00:52 AM

0 B of 1,566 KiB in 0 of 63

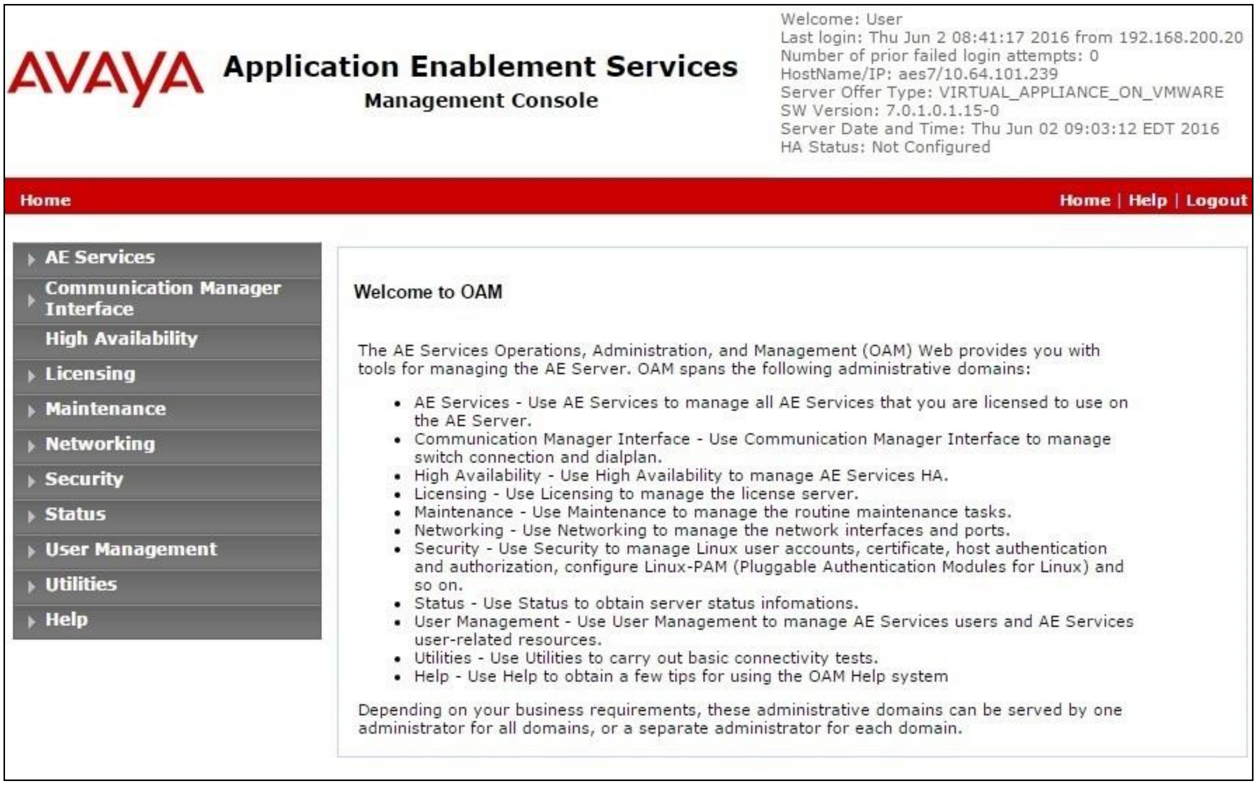
SFTP-3 0:02:34

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.


AVAYA
Application Enablement Services
Management Console
Please login here:
Username
Password
Login
Reset
Copyright Â© 2009-2016 Avaya Inc. All Rights Reserved.

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



Welcome: User
Last login: Thu Jun 2 08:41:17 2016 from 192.168.200.20
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.1.0.1.15-0
Server Date and Time: Thu Jun 02 09:03:12 EDT 2016
HA Status: Not Configured

Welcome to OAM

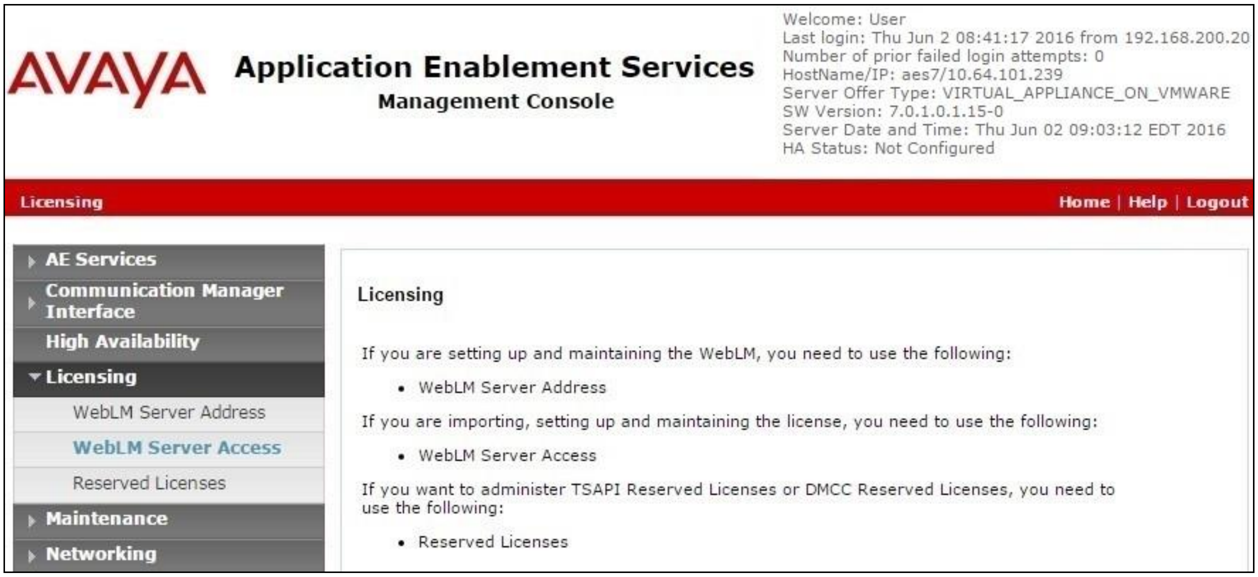
The AE Services Operations, Administration, and Management (OAM) Web provides you with tools for managing the AE Server. OAM spans the following administrative domains:

- 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 infomations.
- 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

Select **Licensing → WebLM Server Access** in the left pane, to display the applicable WebLM server log in screen (not shown). Log in using the appropriate credentials, and navigate to display installed licenses (not shown).



Welcome: User
Last login: Thu Jun 2 08:41:17 2016 from 192.168.200.20
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.1.0.1.15-0
Server Date and Time: Thu Jun 02 09:03:12 EDT 2016
HA Status: Not Configured

Licensing

If you are setting up and maintaining the WebLM, you need to use the following:

- WebLM Server Address

If you are importing, setting up and maintaining the license, you need to use the following:

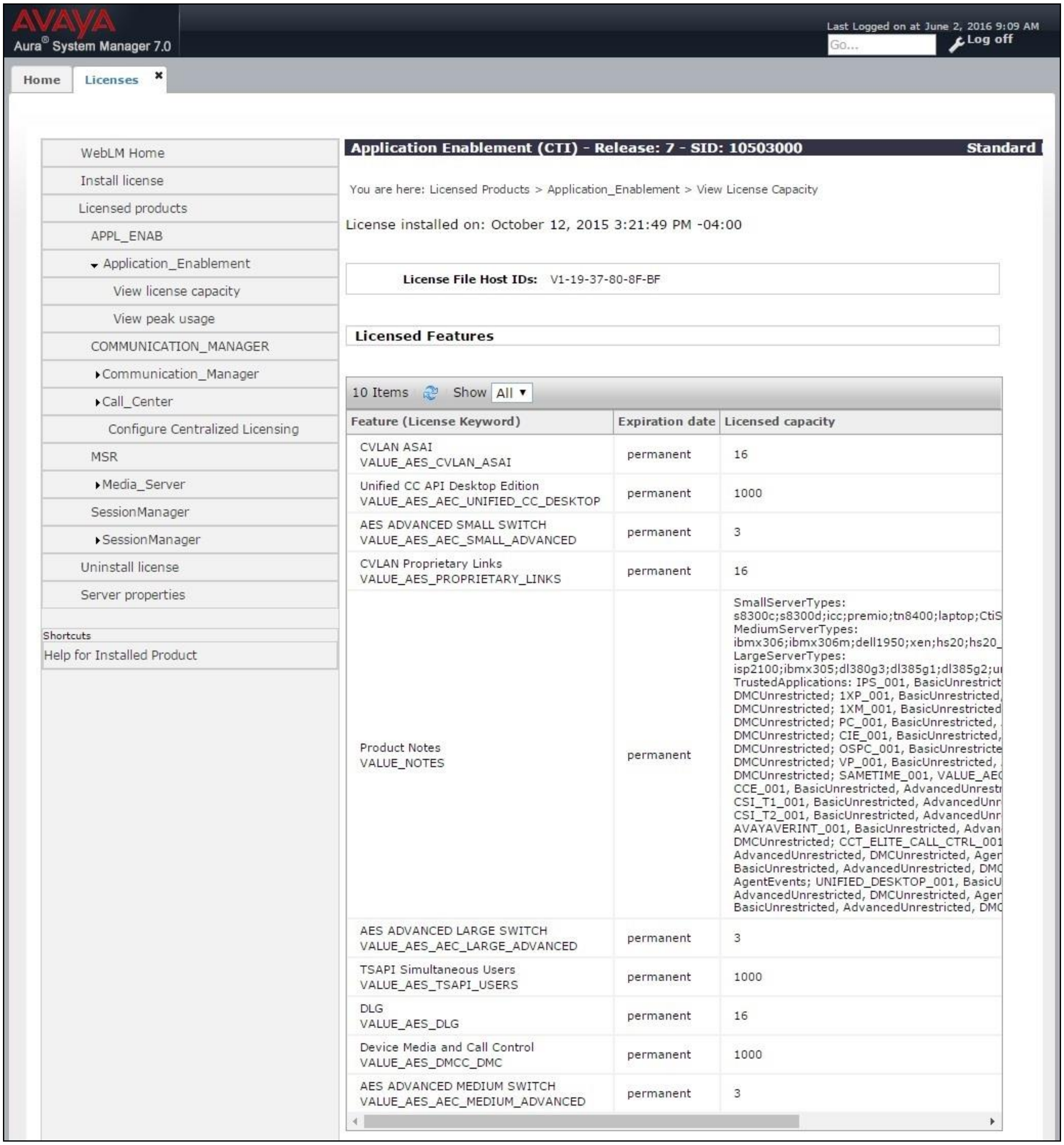
- WebLM Server Access

If you want to administer TSAPI Reserved Licenses or DMCC Reserved Licenses, you need to use the following:

- Reserved Licenses

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** and **Device Media and Call Control**, as shown below. 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.



Application Enablement (CTI) - Release: 7 - SID: 10503000 **Standard**

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

License installed on: October 12, 2015 3:21:49 PM -04:00

License File Host IDs: V1-19-37-80-8F-BF

Licensed Features

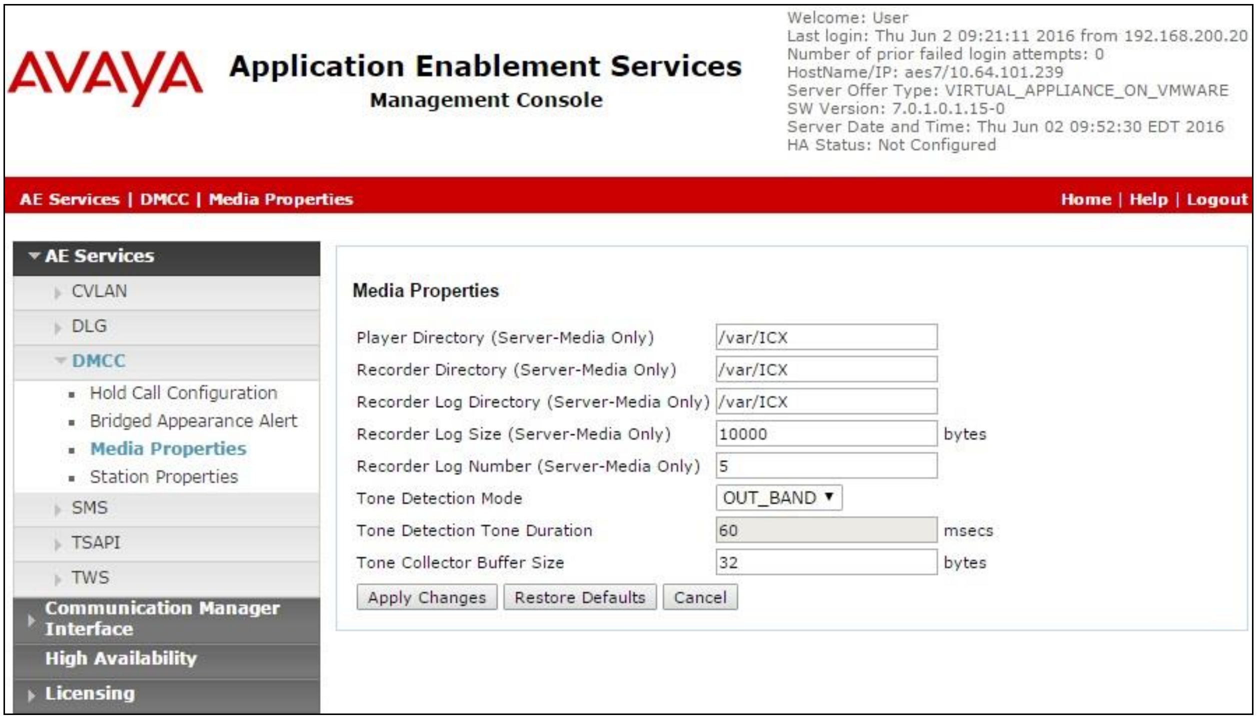
10 Items Show All ▾

Feature (License Keyword)	Expiration date	Licensed capacity
CVLAN ASAI VALUE_AES_CVLAN_ASAI	permanent	16
Unified CC API Desktop Edition VALUE_AES_AEC_UNIFIED_CC_DESKTOP	permanent	1000
AES ADVANCED SMALL SWITCH VALUE_AES_AEC_SMALL_ADVANCED	permanent	3
CVLAN Proprietary Links VALUE_AES_PROPRIETARY_LINKS	permanent	16
Product Notes VALUE_NOTES	permanent	SmallServerTypes: s8300c;s8300d;icc;premio;tn8400;laptop;CtiS MediumServerTypes: ibmx306;ibmx306m;dell1950;xen;hs20;hs20_ LargeServerTypes: isp2100;ibmx305;dl380g3;dl385g1;dl385g2;u TrustedApplications: IPS_001, BasicUnrestrict DMCUnrestricted; 1XP_001, BasicUnrestricted, DMCUnrestricted; 1XM_001, BasicUnrestricted DMCUnrestricted; PC_001, BasicUnrestricted, DMCUnrestricted; CIE_001, BasicUnrestricted, DMCUnrestricted; OSPC_001, BasicUnrestricte DMCUnrestricted; VP_001, BasicUnrestricted, DMCUnrestricted; SAMETIME_001, VALUE_AE CCE_001, BasicUnrestricted, AdvancedUnrest CSI_T1_001, BasicUnrestricted, AdvancedUnr CSI_T2_001, BasicUnrestricted, AdvancedUnr AVAYAVERINT_001, BasicUnrestricted, Advan DMCUnrestricted; CCT_ELITE_CALL_CTRL_001 AdvancedUnrestricted, DMCUnrestricted, Ager BasicUnrestricted, AdvancedUnrestricted, DMC AgentEvents; UNIFIED_DESKTOP_001, BasicU AdvancedUnrestricted, DMCUnrestricted, Ager BasicUnrestricted, AdvancedUnrestricted, DMC
AES ADVANCED LARGE SWITCH VALUE_AES_AEC_LARGE_ADVANCED	permanent	3
TSAPI Simultaneous Users VALUE_AES_TSAPI_USERS	permanent	1000
DLG VALUE_AES_DLG	permanent	16
Device Media and Call Control VALUE_AES_DMCC_DMC	permanent	1000
AES ADVANCED MEDIUM SWITCH VALUE_AES_AEC_MEDIUM_ADVANCED	permanent	3

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.



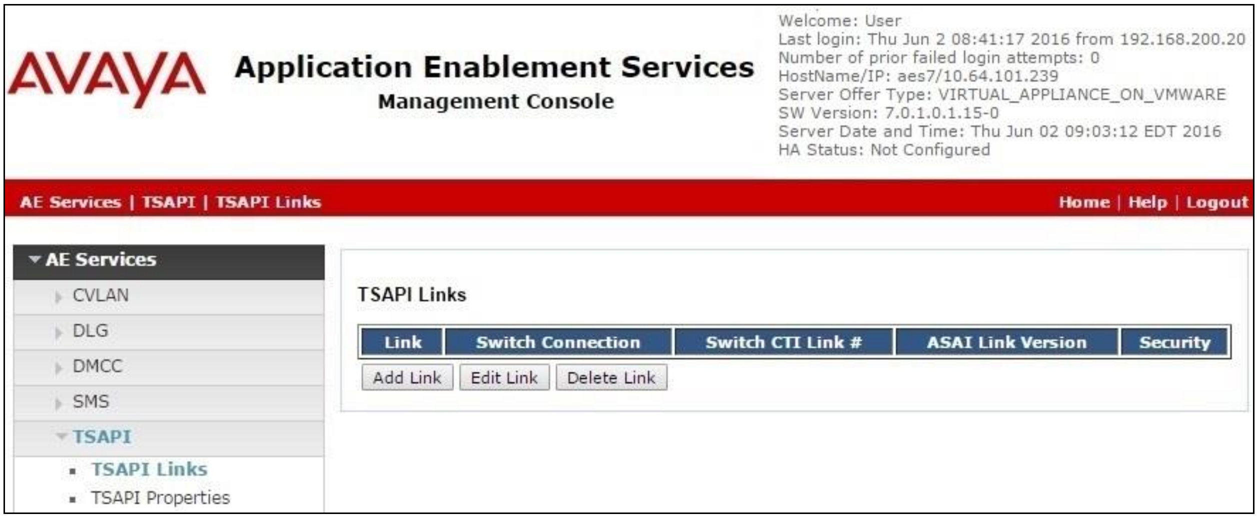
Welcome: User
Last login: Thu Jun 2 09:21:11 2016 from 192.168.200.20
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.1.0.1.15-0
Server Date and Time: Thu Jun 02 09:52:30 EDT 2016
HA Status: Not Configured

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**.



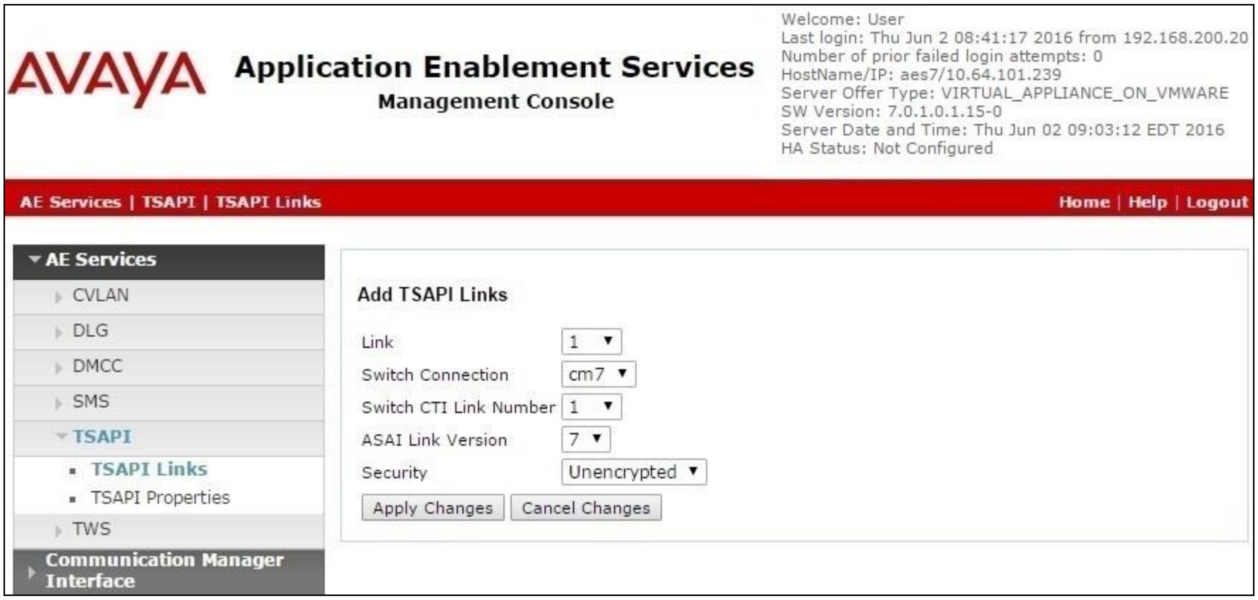
Welcome: User
Last login: Thu Jun 2 08:41:17 2016 from 192.168.200.20
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.1.0.1.15-0
Server Date and Time: Thu Jun 02 09:03:12 EDT 2016
HA Status: Not Configured

TSAPI Links

Link	Switch Connection	Switch CTI Link #	ASAI Link Version	Security

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 "cm7" is selected. For **Switch CTI Link Number**, select the CTI link number from **Section 5.2**. Retain the default values in the remaining fields.



Welcome: User
Last login: Thu Jun 2 08:41:17 2016 from 192.168.200.20
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.1.0.1.15-0
Server Date and Time: Thu Jun 02 09:03:12 EDT 2016
HA Status: Not Configured

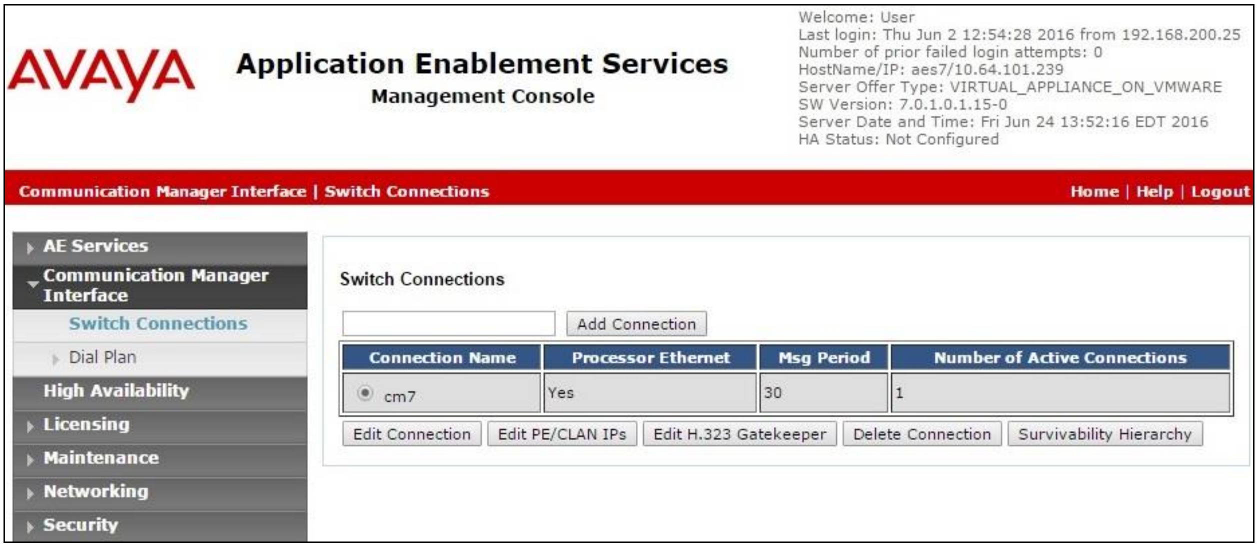
Add TSAPI Links

Link	1 ▼
Switch Connection	cm7 ▼
Switch CTI Link Number	1 ▼
ASAI Link Version	7 ▼
Security	Unencrypted ▼

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 "cm7", and select the corresponding radio button. Click **Edit H.323 Gatekeeper**.

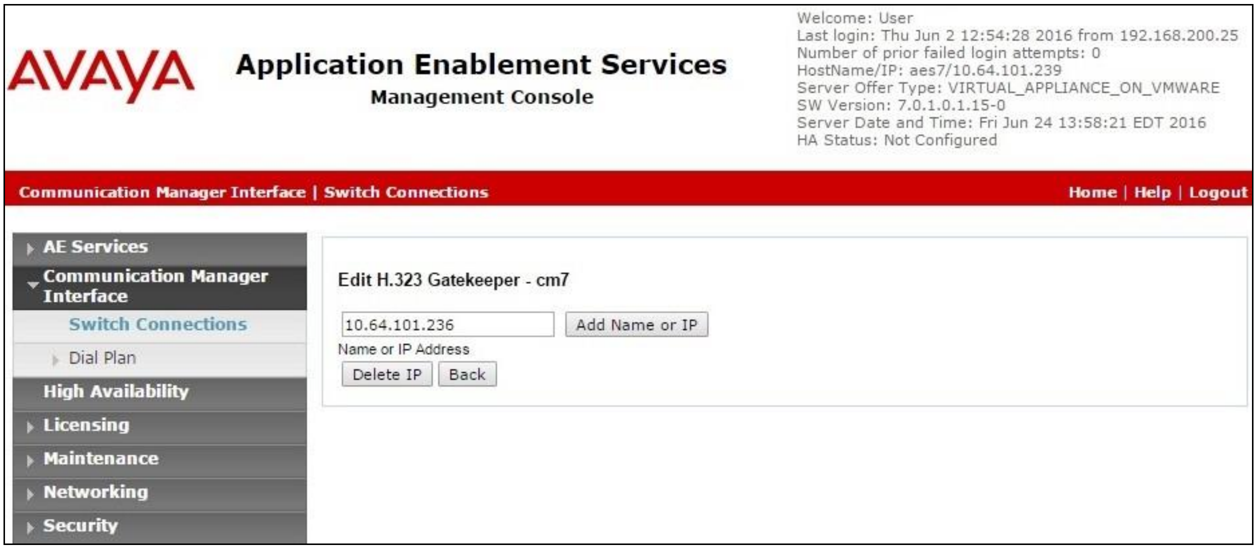


Welcome: User
Last login: Thu Jun 2 12:54:28 2016 from 192.168.200.25
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.1.0.1.15-0
Server Date and Time: Fri Jun 24 13:52:16 EDT 2016
HA Status: Not Configured

Switch Connections

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections
● cm7	Yes	30	1

The **Edit H.323 Gatekeeper** screen is displayed. Enter the IP address of a C-LAN circuit pack or the Processor C-LAN on Communication Manager to use as H.323 gatekeeper, in this case "10.64.101.236" as shown below. Click **Add Name or IP**.



Welcome: User
Last login: Thu Jun 2 12:54:28 2016 from 192.168.200.25
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.1.0.1.15-0
Server Date and Time: Fri Jun 24 13:58:21 EDT 2016
HA Status: Not Configured

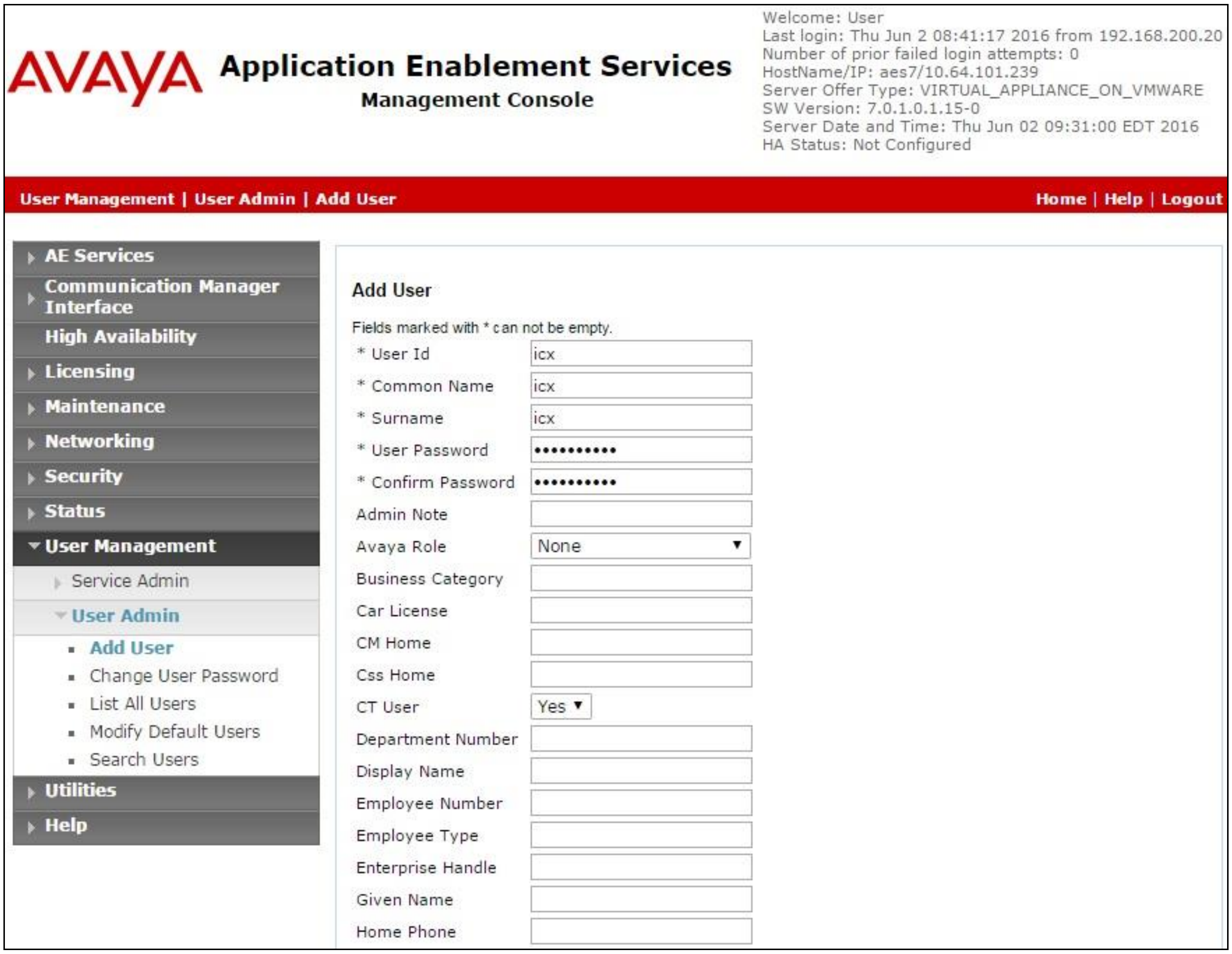
Edit H.323 Gatekeeper - cm7

10.64.101.236
Name or IP Address

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.



Welcome: User
Last login: Thu Jun 2 08:41:17 2016 from 192.168.200.20
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.1.0.1.15-0
Server Date and Time: Thu Jun 02 09:31:00 EDT 2016
HA Status: Not Configured

Add User

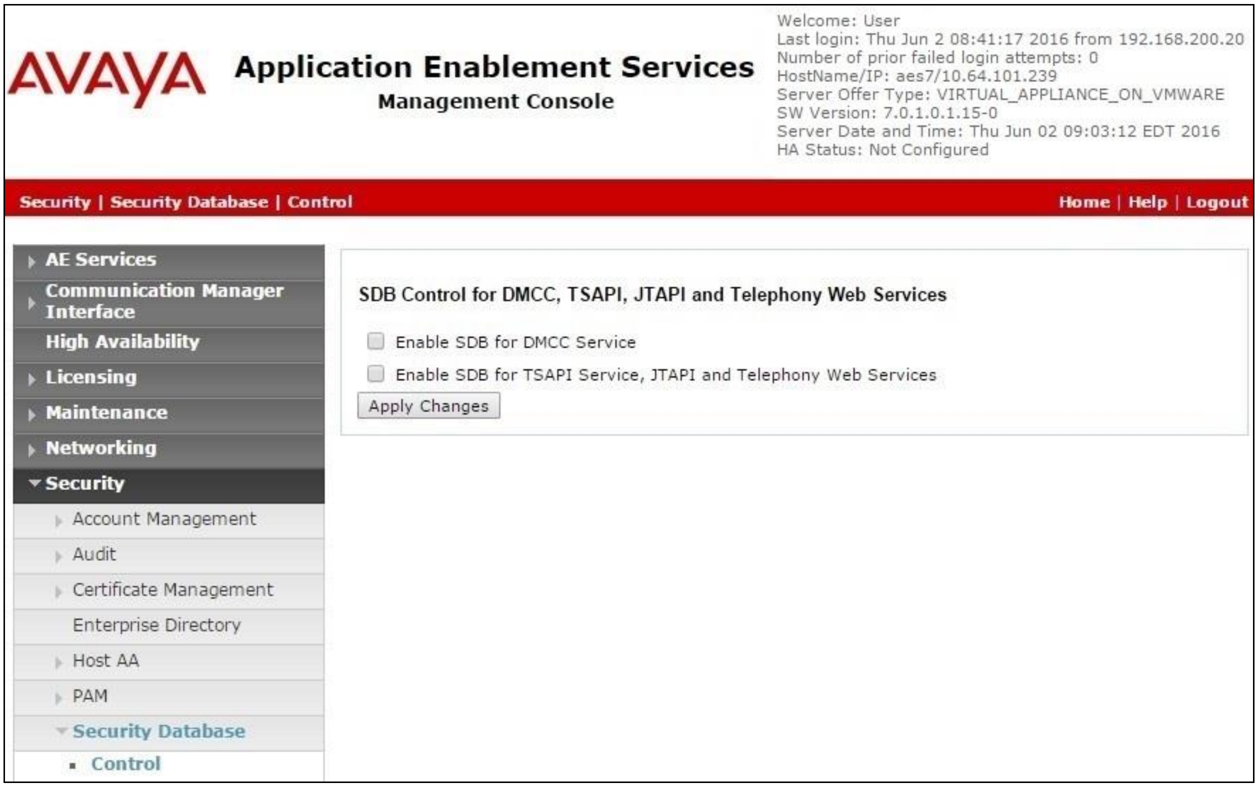
Fields marked with * can not be empty.

* User Id	icx
* Common Name	icx
* Surname	icx
* User Password	••••••••••
* Confirm Password	••••••••••
Admin Note	
Avaya Role	None ▾
Business Category	
Car License	
CM Home	
Css Home	
CT User	Yes ▾
Department Number	
Display Name	
Employee Number	
Employee Type	
Enterprise Handle	
Given Name	
Home Phone	

6.8. Administer 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. Make certain both parameters are unchecked, as shown below.

In the event that the security database is used by the customer with parameter enabled, then follow reference [2] to configure appropriate access privileges for the ICX user from **Section 6.7**.



Welcome: User
Last login: Thu Jun 2 08:41:17 2016 from 192.168.200.20
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.1.0.1.15-0
Server Date and Time: Thu Jun 02 09:03:12 EDT 2016
HA Status: Not Configured

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

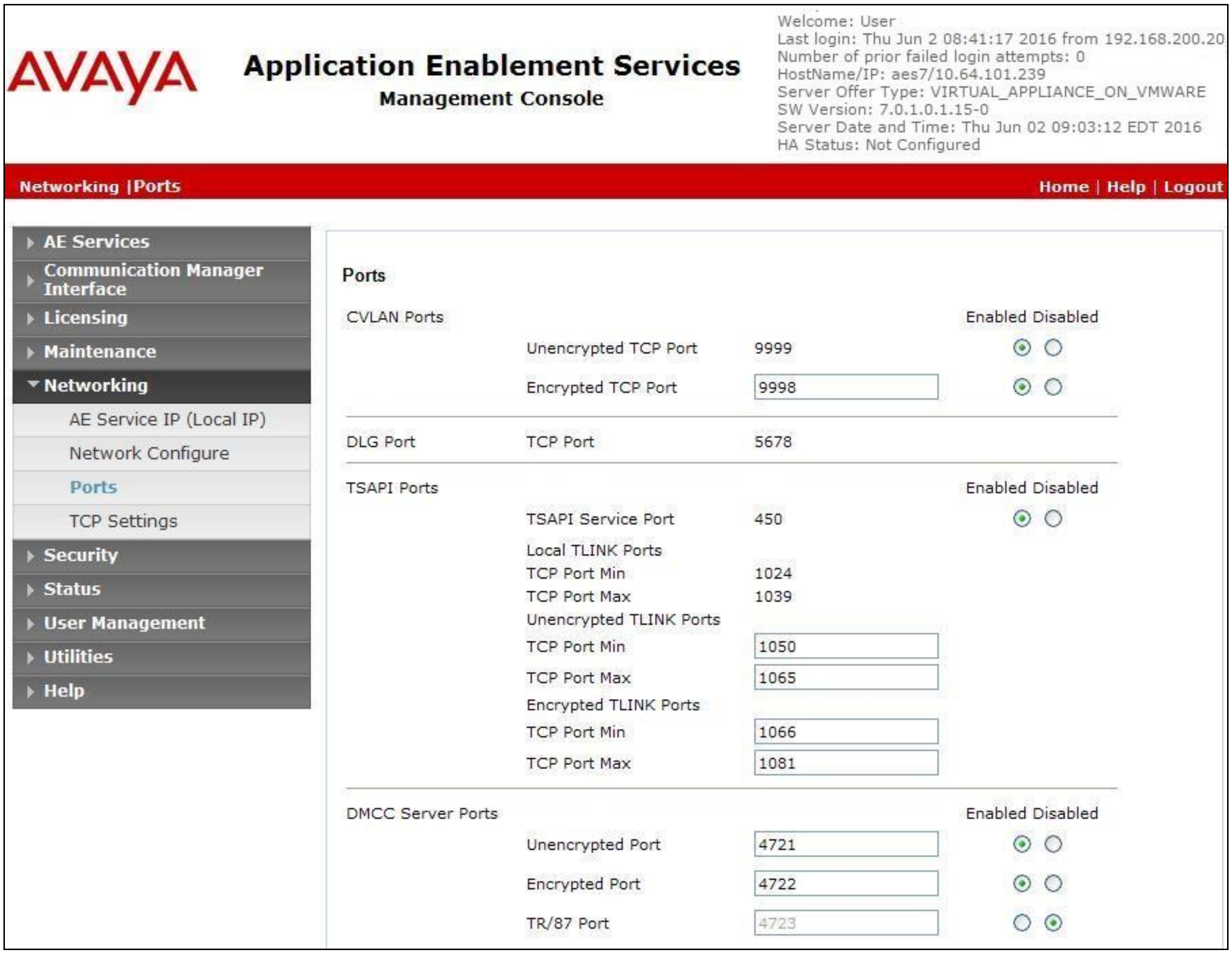
☐ Enable SDB for DMCC Service

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

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** as shown below.



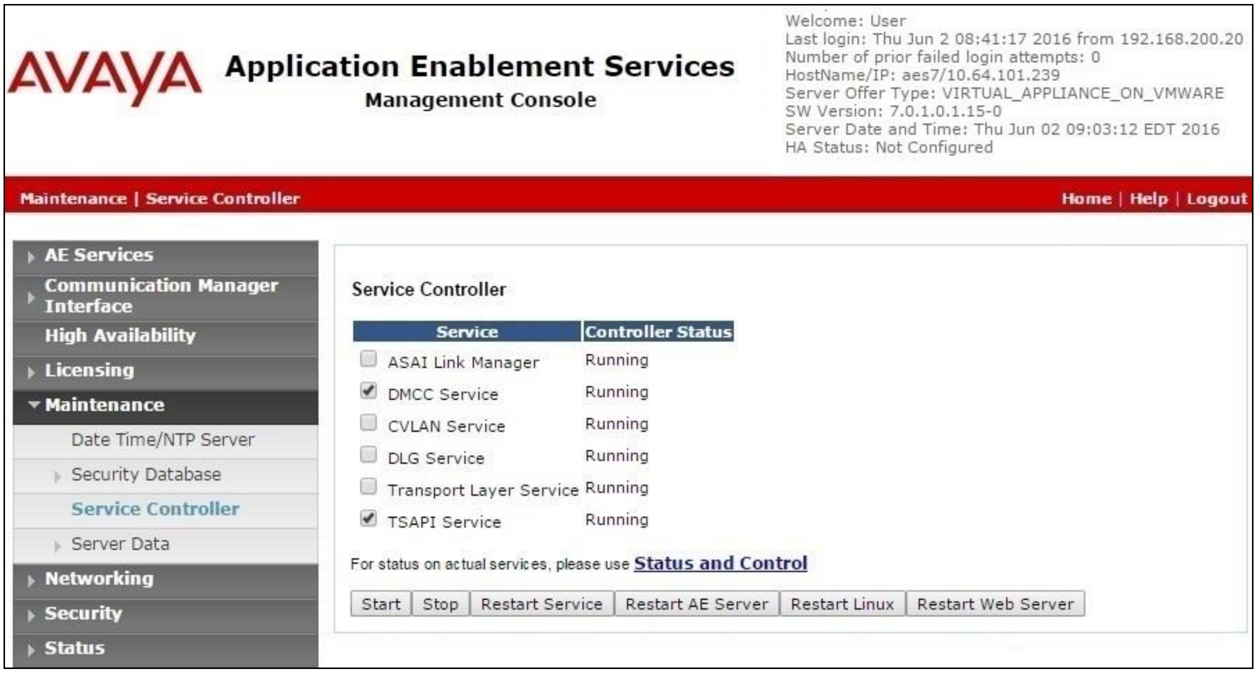
Welcome: User
Last login: Thu Jun 2 08:41:17 2016 from 192.168.200.20
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.1.0.1.15-0
Server Date and Time: Thu Jun 02 09:03:12 EDT 2016
HA Status: Not Configured

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	○	●

6.10. 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
Last login: Thu Jun 2 08:41:17 2016 from 192.168.200.20
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.1.0.1.15-0
Server Date and Time: Thu Jun 02 09:03:12 EDT 2016
HA Status: Not Configured

Service Controller

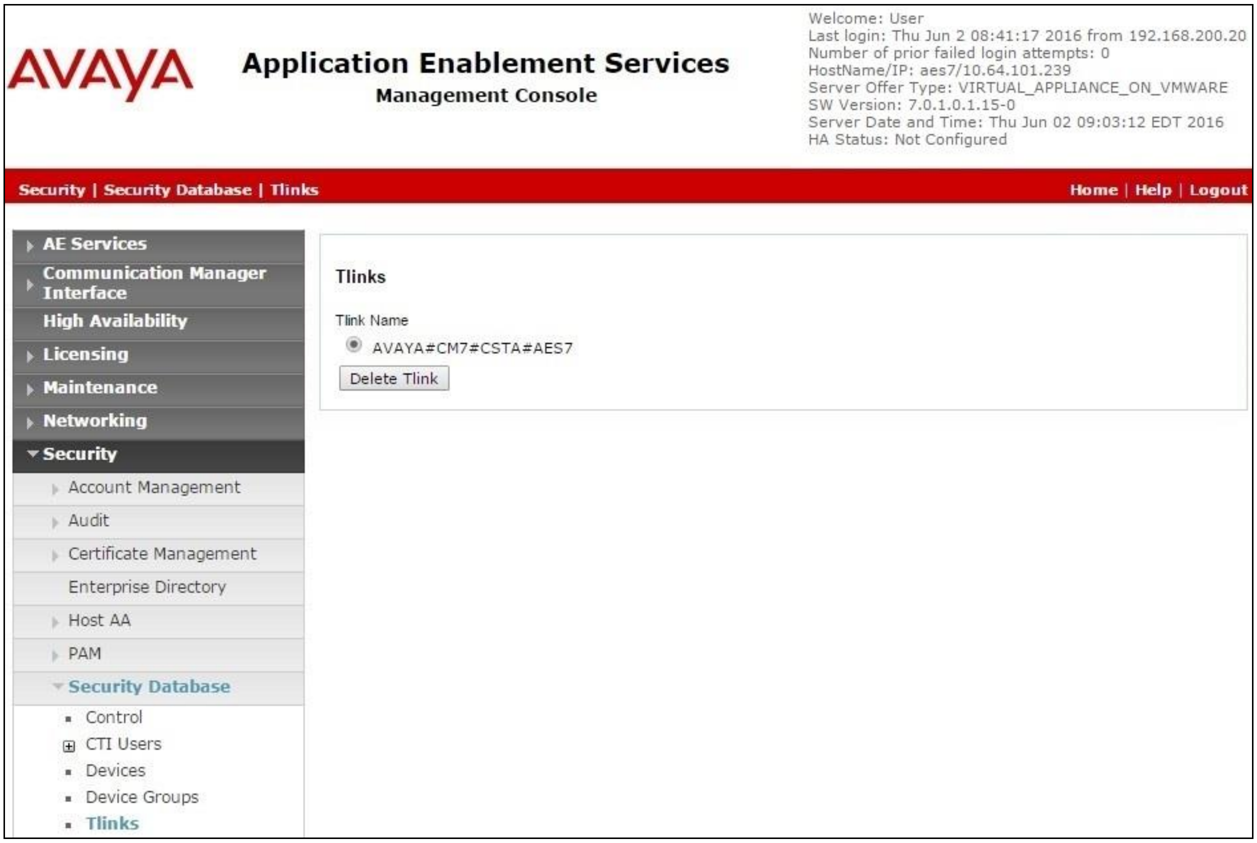
Service	Controller Status
□ ASAI Link Manager	Running
☑ DMCC Service	Running
□ CVLAN Service	Running
□ DLG Service	Running
□ Transport Layer Service	Running
☑ TSAPI Service	Running

For status on actual services, please use Status and Control

6.11. 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#**CM7**#CSTA#AES7". Note the use of the switch connection "CM7" from **Section 6.5** as part of the Tlink name.



Welcome: User
Last login: Thu Jun 2 08:41:17 2016 from 192.168.200.20
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.1.0.1.15-0
Server Date and Time: Thu Jun 02 09:03:12 EDT 2016
HA Status: Not Configured

Tlinks

Tlink Name

● AVAYA#CM7#CSTA#AES7

7. Configure ICX Callback

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

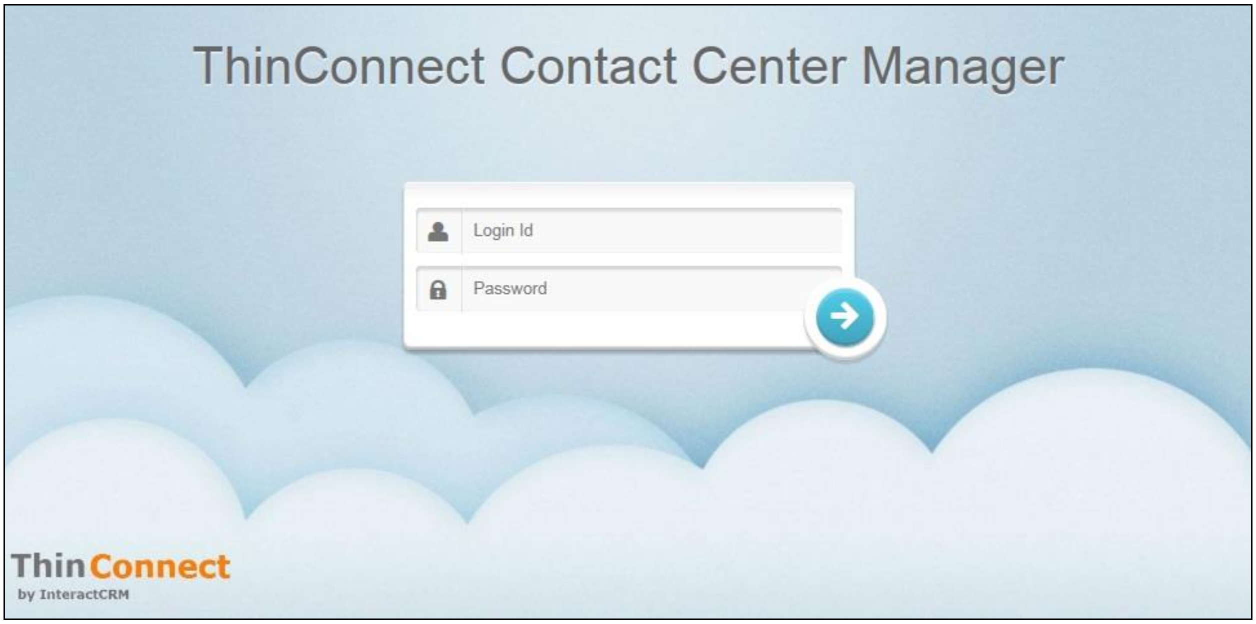
- Launch web interface
- Administer enterprise level properties
- Administer host config
- Administer stations
- Administer VDN settings

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

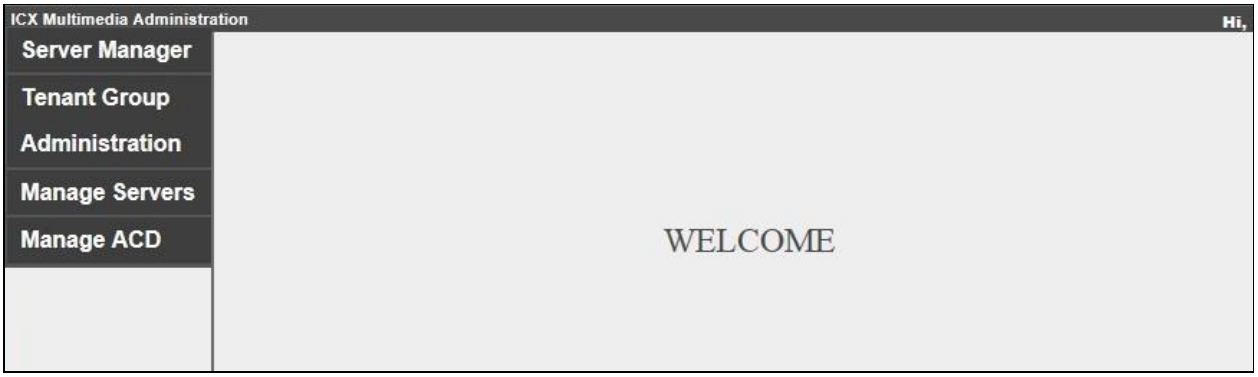
Launch the web interface by using the URL "http://ip-address:15050/ContactCenterManager" in an Internet Explorer browser window, where "ip-address" is the IP address of the ICX server running the Contact Center Manager component.

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



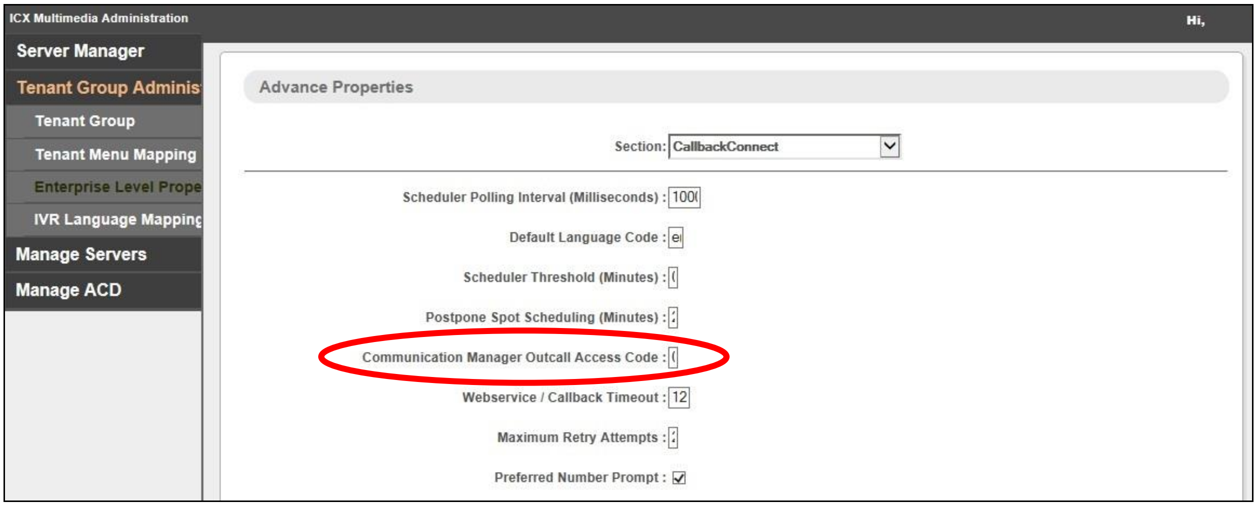
7.2. Administer Enterprise Level Properties

The **WELCOME** screen below is displayed



Select **Tenant Group Administration → Enterprise Level Properties** in the left pane, to display the **Advanced Properties** screen. For **Section**, select "CallbackConnect" to display additional parameters.

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, "9" is the ARS dialing prefix required by Communication Manager.



Section: CallbackConnect

Scheduler Polling Interval (Milliseconds) : 100(

Default Language Code : e

Scheduler Threshold (Minutes) : (

Postpone Spot Scheduling (Minutes) : :

Communication Manager Outcall Access Code : (

Webservice / Callback Timeout : 12

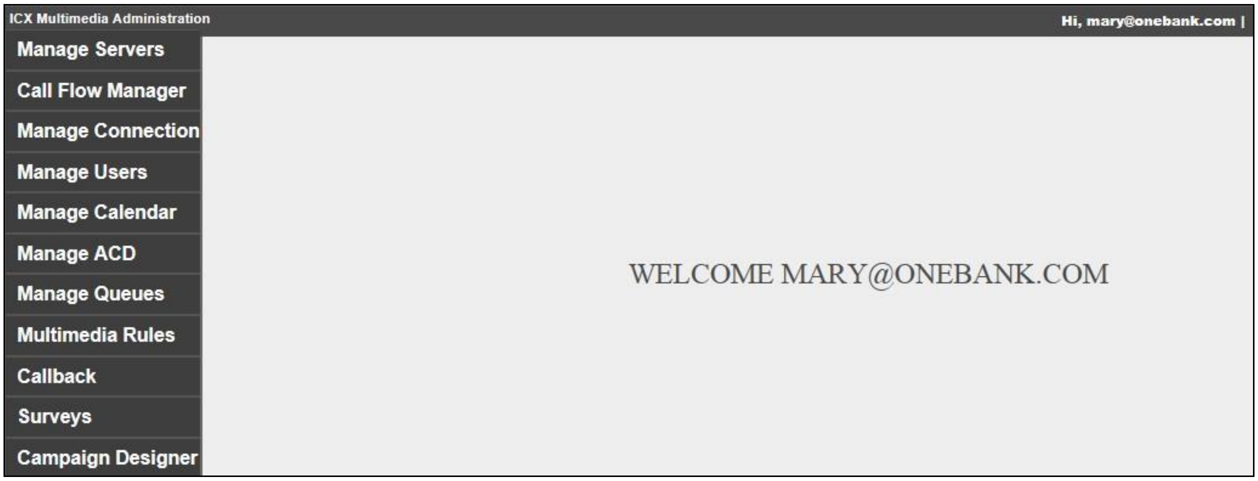
Maximum Retry Attempts : :

Preferred Number Prompt : ☑

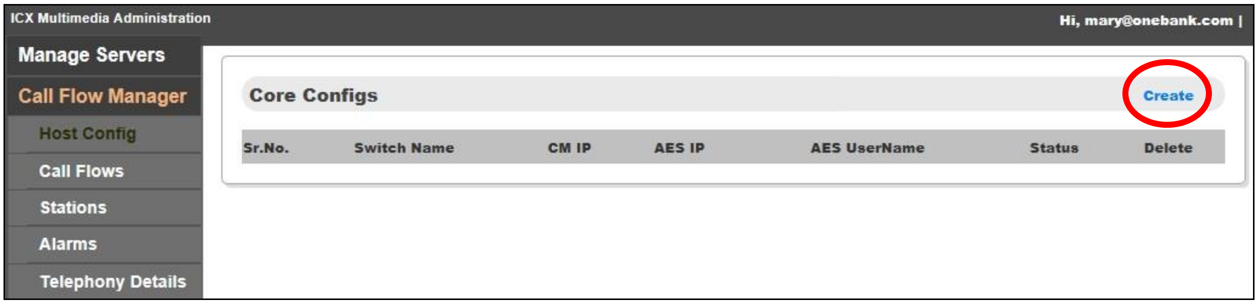
7.3. Administer Host Config

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 mary@onebank.com.



The **ICX Multimedia Administration** screen is displayed. Select **Call Flow Manager → Host Config** in the left pane, to display the **Core Configs** screen. Click **Create**.

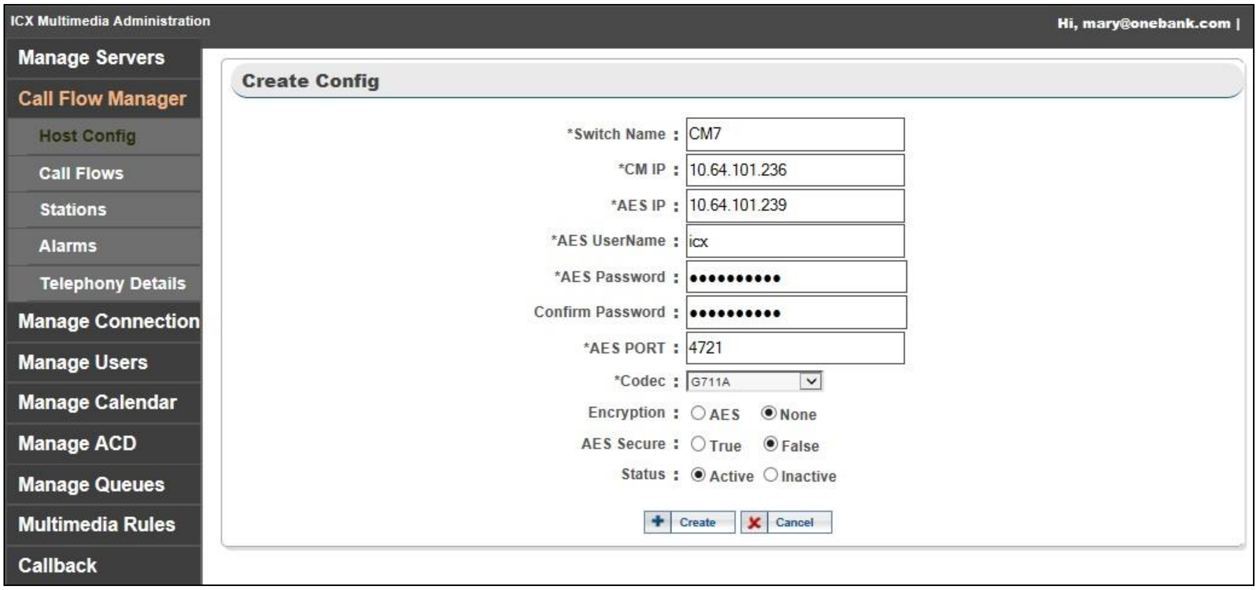


Sr.No.	Switch Name	CM IP	AES IP	AES UserName	Status	Delete

The **Create Config** screen is displayed. Enter the following values for the specified fields, and retain the default values for the remaining fields.

• **Switch Name:**	The switch connection name from **Section 6.5**.
• **CM IP:**	IP address of the H.323 gatekeeper from **Section 6.6**.
• **AES IP:**	IP address of Application Enablement Services.
• **AES 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 unencrypted port number from **Section 6.9**.
• **Status:**	“Active”

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

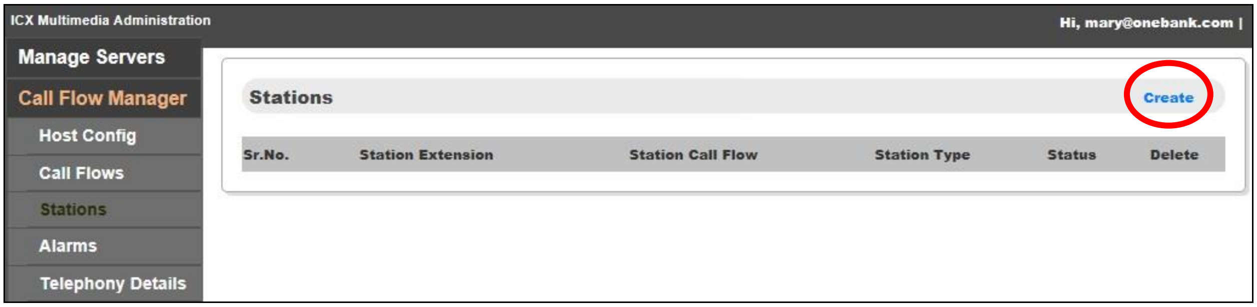


Create Config

*Switch Name :	CM7
*CM IP :	10.64.101.236
*AES IP :	10.64.101.239
*AES UserName :	icx
*AES Password :	••••••••••
Confirm Password :	••••••••••
*AES PORT :	4721
*Codec :	G711A
Encryption :	○ AES ● None
AES Secure :	○ True ● False
Status :	● Active ○ Inactive

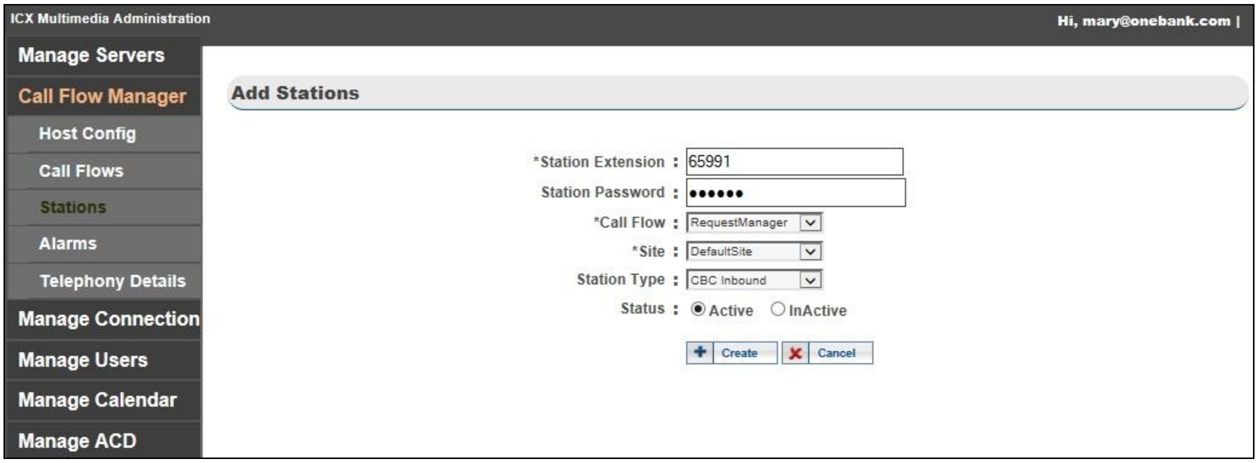
7.4. Administer Stations

Select **Call Flow Manager → Stations** in the left pane, to display the **Stations** screen. Click **Create**.



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

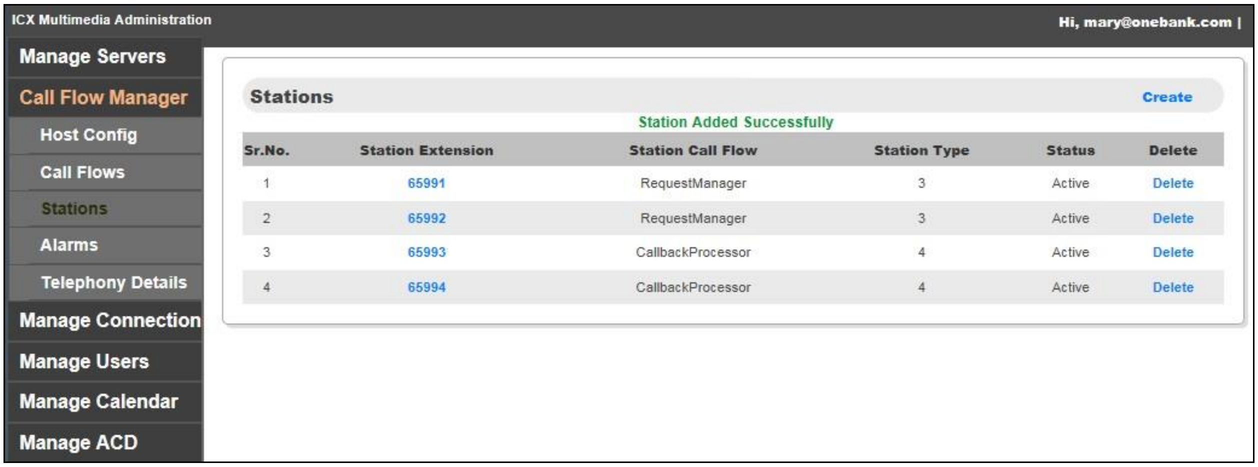
- **Station Extension:** The first virtual IP softphone extension from **Section 5.3**.
- **Station Password:** The first virtual IP softphone security code from **Section 5.3**.
- **Call Flow:** "RequestManager"
- **Site:** Select the applicable site, in this case "DefaultSite".
- **Station Type:** "CBC Inbound"
- **Status:** "Active"



*Station Extension : 65991
Station Password : ••••••
*Call Flow : RequestManager
*Site : DefaultSite
Station Type : CBC Inbound
Status : ● Active ○ InActive

Repeat this section to create a station for each virtual IP softphone from **Section 5.3**. 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.

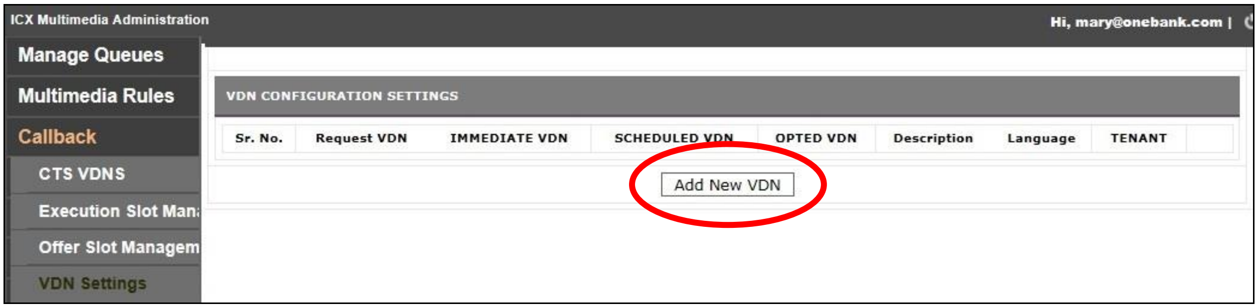


Station Added Successfully

Sr.No.	Station Extension	Station Call Flow	Station Type	Status	Delete
1	65991	RequestManager	3	Active	Delete
2	65992	RequestManager	3	Active	Delete
3	65993	CallbackProcessor	4	Active	Delete
4	65994	CallbackProcessor	4	Active	Delete

7.5. Administer VDN Settings

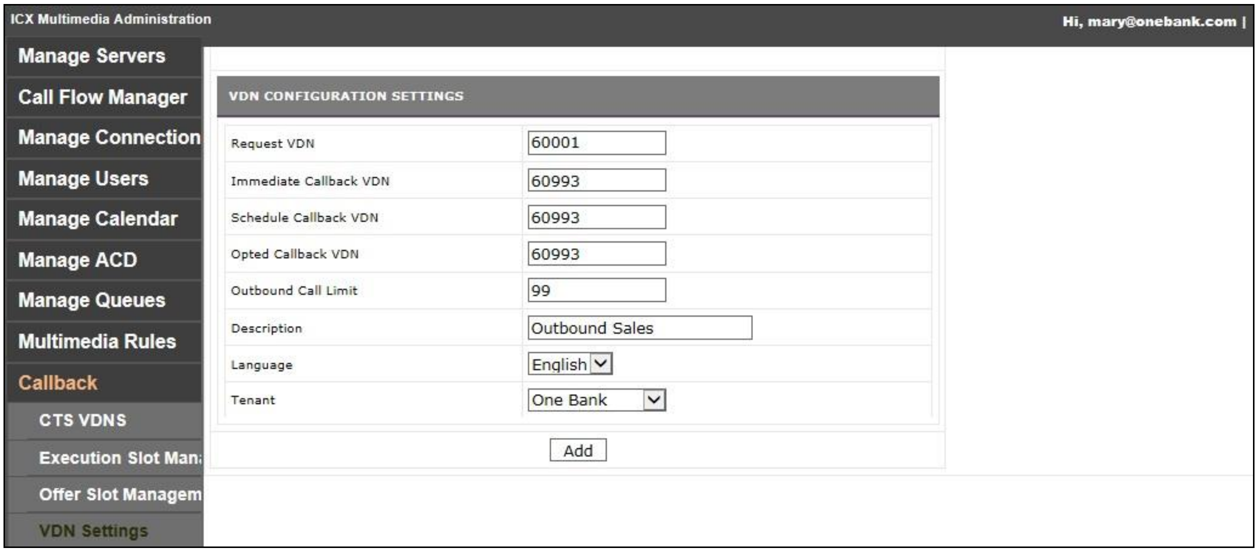
Scroll the left pane as necessary, and select **Callback → VDN Settings** to display the **VDN CONFIGURATION SETTINGS** screen. Click **Add New VDN**.



Sr. No.	Request VDN	IMMEDIATE VDN	SCHEDULED VDN	OPTED VDN	Description	Language	TENANT

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

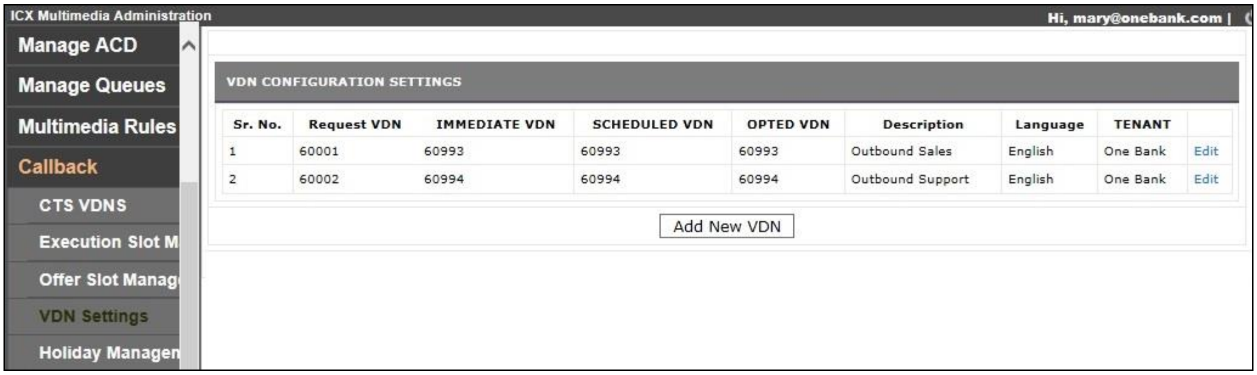
• **Request VDN:**	The first inbound VDN extension from **Section 5.6**.
• **Immediate Callback VDN:**	The first outbound VDN extension from **Section 5.8**.
• **Schedule Callback VDN:**	The first outbound VDN extension from **Section 5.8**.
• **Opted Callback VDN:**	The first outbound VDN extension from **Section 5.8**.
• **Description:**	A desired description.
• **Tenant:**	Select the applicable tenant, in this case "One Bank".



VDN CONFIGURATION SETTINGS

Request VDN	60001
Immediate Callback VDN	60993
Schedule Callback VDN	60993
Opted Callback VDN	60993
Outbound Call Limit	99
Description	Outbound Sales
Language	English
Tenant	One Bank

Repeat this section to map all inbound VDN from **Section 5.6** to outbound VDN in **Section 5.8**. In the compliance testing, two VDN mappings were created, as shown below.



VDN CONFIGURATION SETTINGS

Sr. No.	Request VDN	IMMEDIATE VDN	SCHEDULED VDN	OPTED VDN	Description	Language	TENANT	
1	60001	60993	60993	60993	Outbound Sales	English	One Bank	Edit
2	60002	60994	60994	60994	Outbound Support	English	One Bank	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 5.2**, 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     7        no    aes7             established   167      159
```

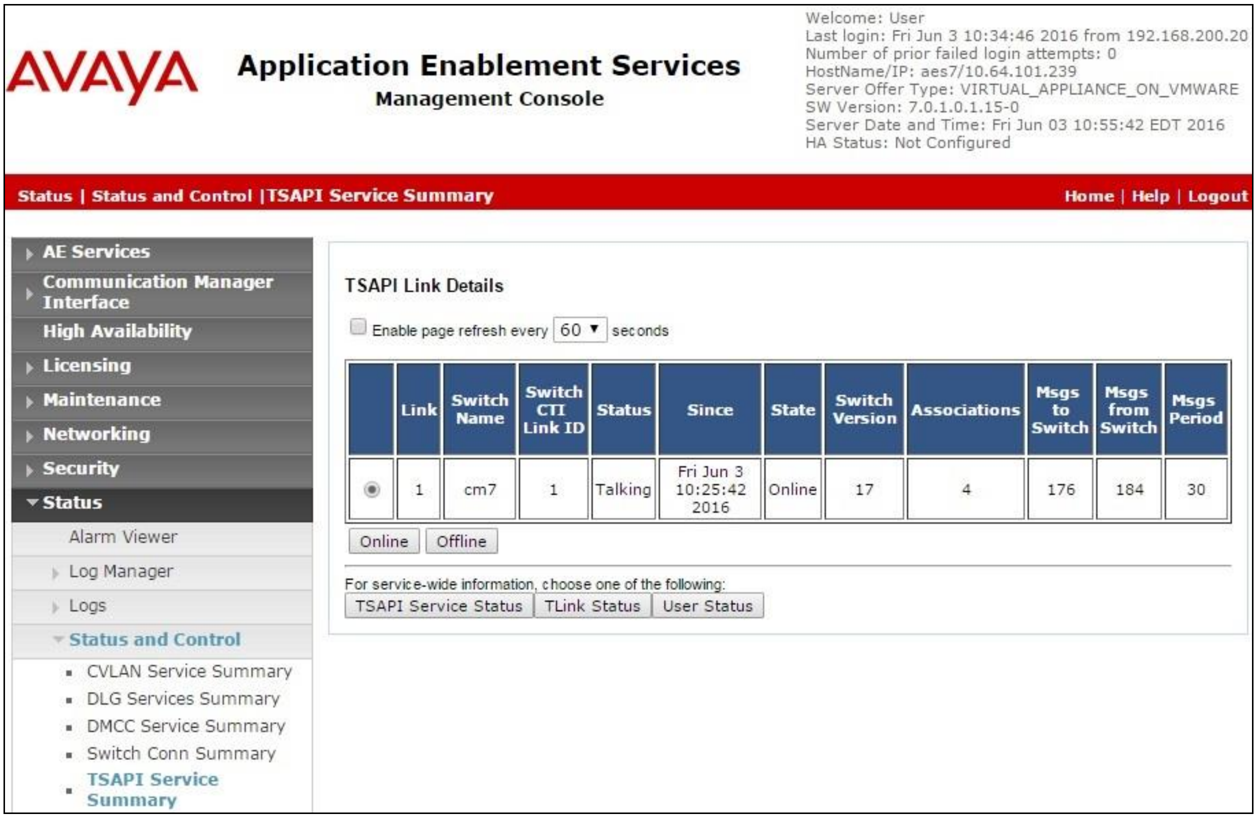
Verify the registration status of virtual IP softphones by using the "list registered-ip-stations" command. Verify that all virtual IP softphone extensions from **Section 5.3** are displayed along with the IP address of the Application Enablement Services server, as shown below.

```
list registered-ip-stations                                            Page   1

                            REGISTERED IP STATIONS

Station Ext   Set Type/ Prod ID/   TCP Station IP Address/
or Orig Port  Net Rgn   Release    Skt Gatekeeper IP Address
------------- --------- ---------- --- ---------------------------------------
65000         9650      IP_Phone    y  192.168.200.106
              1         3.260A         10.64.101.236
65001         9620      IP_Phone    y  192.168.200.104
              1         3.260A         10.64.101.236
65002         9611      IP_Phone    y  192.168.200.105
              1         6.6115         10.64.101.236
65991         4620      IP_API_A    y  10.64.101.239
              1         3.2040         10.64.101.236
65992         4620      IP_API_A    y  10.64.101.239
              1         3.2040         10.64.101.236
65993         4620      IP_API_A    y  10.64.101.239
              1         3.2040         10.64.101.236
65994         4620      IP_API_A    y  10.64.101.239
              1         3.2040         10.64.101.236
```

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 5.3**, in this case "4".



Application Enablement Services
Management Console

Welcome: User
Last login: Fri Jun 3 10:34:46 2016 from 192.168.200.20
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.1.0.1.15-0
Server Date and Time: Fri Jun 03 10:55:42 EDT 2016
HA Status: Not Configured

Status | Status and Control |TSAPI Service Summary

TSAPI Link Details

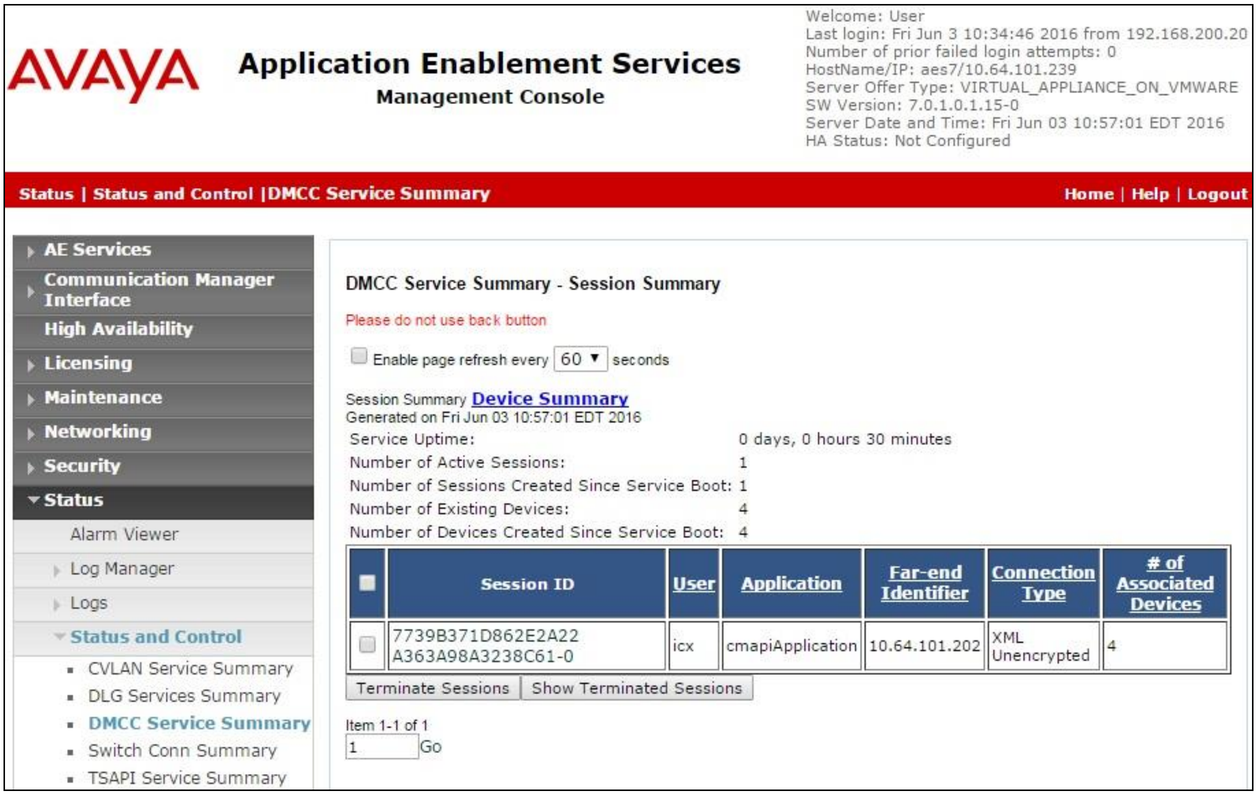
☐ Enable page refresh every 60 seconds

	Link	Switch Name	Switch CTI Link ID	Status	Since	State	Switch Version	Associations	Msgs to Switch	Msgs from Switch	Msgs Period
●	1	cm7	1	Talking	Fri Jun 3 10:25:42 2016	Online	17	4	176	184	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 5.3**.



Welcome: User
Last login: Fri Jun 3 10:34:46 2016 from 192.168.200.20
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.1.0.1.15-0
Server Date and Time: Fri Jun 03 10:57:01 EDT 2016
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 Fri Jun 03 10:57:01 EDT 2016

Service Uptime:	0 days, 0 hours 30 minutes
Number of Active Sessions:	1
Number of Sessions Created Since Service Boot:	1
Number of Existing Devices:	4
Number of Devices Created Since Service Boot:	4

□	Session ID	User	Application	Far-end Identifier	Connection Type	# of Associated Devices
□	7739B371D862E2A22 A363A98A3238C61-0	icx	cmapiApplication	10.64.101.202	XML Unencrypted	4

Item 1-1 of 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 an observation noted in **Section 2.2**.

10. Additional References

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

1. *Administering Avaya Aura® Communication Manager*, Release 7.0, Issue 1, August 2015, available at http://support.avaya.com.

2. *Administering and Maintaining Aura® Application Enablement Services*, Release 7.0, Issue 1, August 2015, available at http://support.avaya.com.

3. *Interactcrm ICX Callback Installation Manual*, ICX Version 3.0.16, April 2016, 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.