Avaya Solution & Interoperability Test Lab

Application Notes for CXM 5.2 with Avaya Aura® Communication Manager 7.0 and Avaya Aura® Application Enablement Services 7.0 – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for CXM 5.2 to interoperate with Avaya Aura® Communication Manager 7.0 and Avaya Aura® Application Enablement Services 7.0. CXM is a call recording solution.

In the compliance testing, CXM used the Telephony Services Application Programming Interface and Device, Media, and Call Control interface from Avaya Aura® Application Enablement Services to monitor contact center devices on Avaya Aura® Communication Manager, and to capture media associated with the monitored agents for call recording purposes via the Single Step Conference method.

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 CXM 5.2 to interoperate with Avaya Aura® Communication Manager 7.0 and Avaya Aura® Application Enablement Services 7.0. CXM is a call recording solution.

In the compliance testing, CXM used the Telephony Services Application Programming Interface (TSAPI) and Device, Media, and Call Control (DMCC) .NET interface from Avaya Aura® Application Enablement Services to monitor contact center devices on Avaya Aura® Communication Manager, and to capture media associated with the monitored agents for call recording purposes via the Single Step Conference method.

The DMCC interface is used by CXM to register virtual IP softphones to Communication Manager. The TSAPI interface is used by CXM to monitor VDNs, skill groups, and agent stations on Avaya Aura® Communication Manager, and to add virtual IP softphones to active calls using the Single Step Conference method.

When there is an active call at the monitored agent, CXM is informed of the call via event reports from the TSAPI interface. CXM starts the call recording by using the Single Step Conference feature from the TSAPI interface to add a virtual IP softphone to the active call to obtain the media. The event reports are also used to determine when to stop the call recordings.

2. General Test Approach and Test Results

The feature test cases were performed both automatically and manually. Upon start of the CXM application, the application automatically requests monitoring on VDNs, skill groups, and agent stations, performs device queries using TSAPI, and registers the virtual IP softphones using DMCC.

For the manual part of the testing, each call was handled manually on the agent station with generation of unique audio content for the recordings. Necessary user actions such as hold and resume were performed from the agent telephones to test the various call scenarios.

The serviceability test cases were performed manually by disconnecting/reconnecting the Ethernet connection to CXM.

The verification of tests included use of CXM logs for proper message exchanges, and use of CXM web interface for proper logging and playback of calls.

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 CXM:

- Use of DMCC registration services to register and un-register the virtual IP softphones.
- Handling of TSAPI messages in areas of event notification and value queries.
- Use of TSAPI call control services and DMCC monitoring services to activate Single Step Conference for virtual IP softphones and to obtain the media for call recording.
- Proper recording, logging, and playback of calls for scenarios involving inbound, outbound, internal, external, ACD, non-ACD, hold, resume, multiple calls, multiple agents, conference, transfer, and long duration.

The serviceability testing focused on verifying the ability of CXM to recover from adverse conditions, such as disconnecting/reconnecting the Ethernet connection to CXM.

2.2. Test Results

All test cases were executed, and the following were observations on CXM:

- CXM is designed to produce cradle to grave reporting, with call continue to be recorded even after the monitored agent left the call. An example is after a monitored agent transferred the ACD call to a non-monitored supervisor, the virtual IP softphone stayed on the remaining call between the non-monitored supervisor with the PSTN. As such, the provisioning of number of virtual IP softphones needs to take this design into account.
- For an internal call between two monitored agents, two recording entries were created with same audio and call duration. The reported direction for both entries is Outbound by design.
- The application assumes all virtual IP softphones can register without problems. Should the first virtual IP softphone fail the registration due to invalid credentials, then no recordings can take place. This can be managed by verifying all virtual IP softphones can register successfully as part of initial configuration.
- For a call that experienced an Ethernet disruption, a recording entry was generated post recovery; however, the recording cannot be played back. Subsequent calls post recovery were recorded and played back without problems.

2.3. Support

Technical support on CXM can be obtained through the following:

Phone:	(866) 400-4296
Email:	support@cxmrecord.com
Web :	http://www.cxmrecord.com

3. Reference Configuration

CXM can be configured on a single server or with components distributed across multiple servers. The compliance test used a single server configuration.

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

In the compliance testing, CXM monitored the VDNs, skill groups, and agent stations shown in the table below.

Device Type	Extension
VDN	60001, 60002
Skill Group	61001, 61002
Supervisor	65000
Agent Station	65001, 66002
Agent ID	65881, 65882

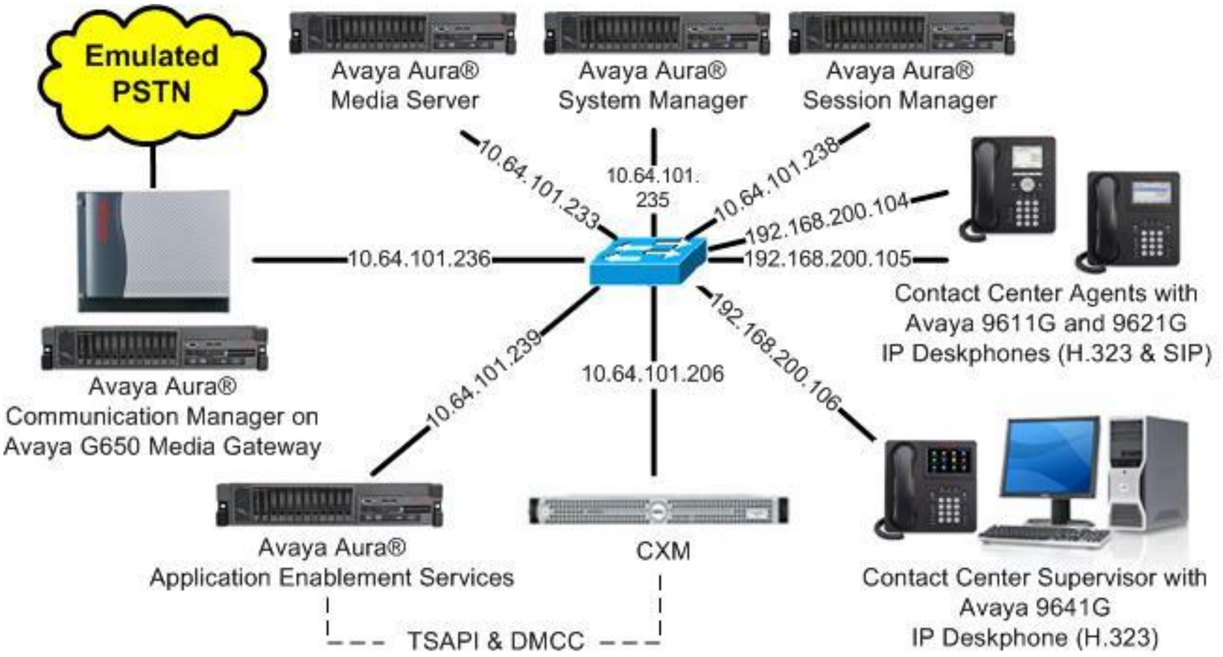

Emulated PSTN
Avaya Aura® Media Server
Avaya Aura® System Manager
Avaya Aura® Session Manager
10.64.101.233
10.64.101.235
10.64.101.238
192.168.200.104
192.168.200.105
10.64.101.236
Contact Center Agents with Avaya 9611G and 9621G IP Deskphones (H.323 & SIP)
192.168.200.106
10.64.101.239
10.64.101.206
Avaya Aura® Communication Manager on Avaya G650 Media Gateway
Avaya Aura® Application Enablement Services
CXM
TSAPI & DMCC
Contact Center Supervisor with Avaya 9641G IP Deskphone (H.323)

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	7.0.1.1 (7.0.1.1.0.441.23169)
Avaya G650 Media Gateway	NA
Avaya Aura® Media Server in Virtual Environment	7.7 (7.7.0.359)
Avaya Aura® Application Enablement Services in Virtual Environment	7.0.1 (7.0.1.0.2.15-0)
Avaya Aura® Session Manager in Virtual Environment	7.0.1.1 (7.0.1.1.70114)
Avaya Aura® System Manager in Virtual Environment	7.0.1.1 (7.0.1.1.065378)
Avaya 9611G & 9641G IP Deskphone (H.323)	6.6302
Avaya 9621G IP Deskphone (SIP)	7.0.1.2.9
CXM on Windows Server 2008 • Avaya Recorder • Avaya TSAPI Windows Client (csta32.dll) • Avaya DMCC .NET (ServiceProvider.dll)	5.2.4.12 R2 Standard 5.2.7.999 7.0.0.138 6.2.0.29

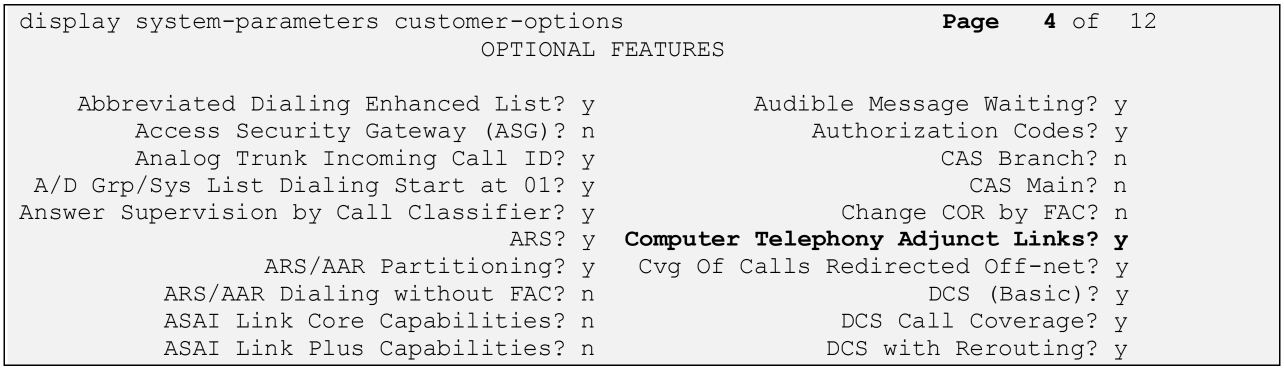
5. Configure Avaya Aura® Communication Manager

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

- Verify license
- Administer CTI link
- Administer system parameters features
- Administer virtual IP softphones
- Obtain VDN data
- Obtain skill group data
- Obtain station data
- Obtain agent data

5.1. Verify License

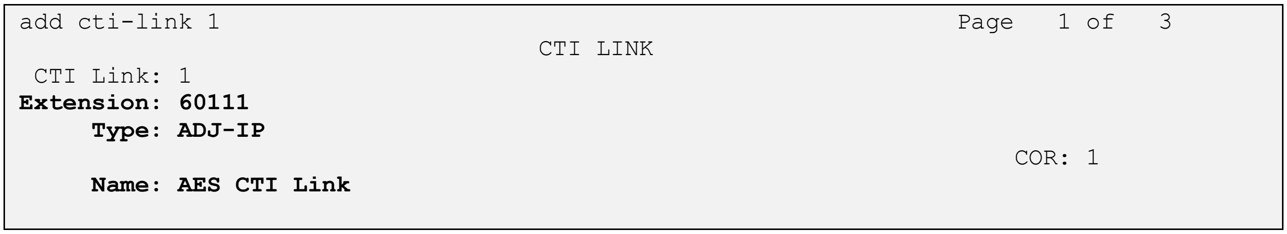
Log in to the System Access Terminal to verify that the Communication Manager license has proper permissions for features illustrated in these Application Notes. Use the "display system-parameters customer-options" command to verify that the **Computer Telephony Adjunct Links** customer option is set 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? n                 DCS Call Coverage? y
          ASAI Link Plus Capabilities? n                DCS with Rerouting? y
```

5.2. Administer CTI Link

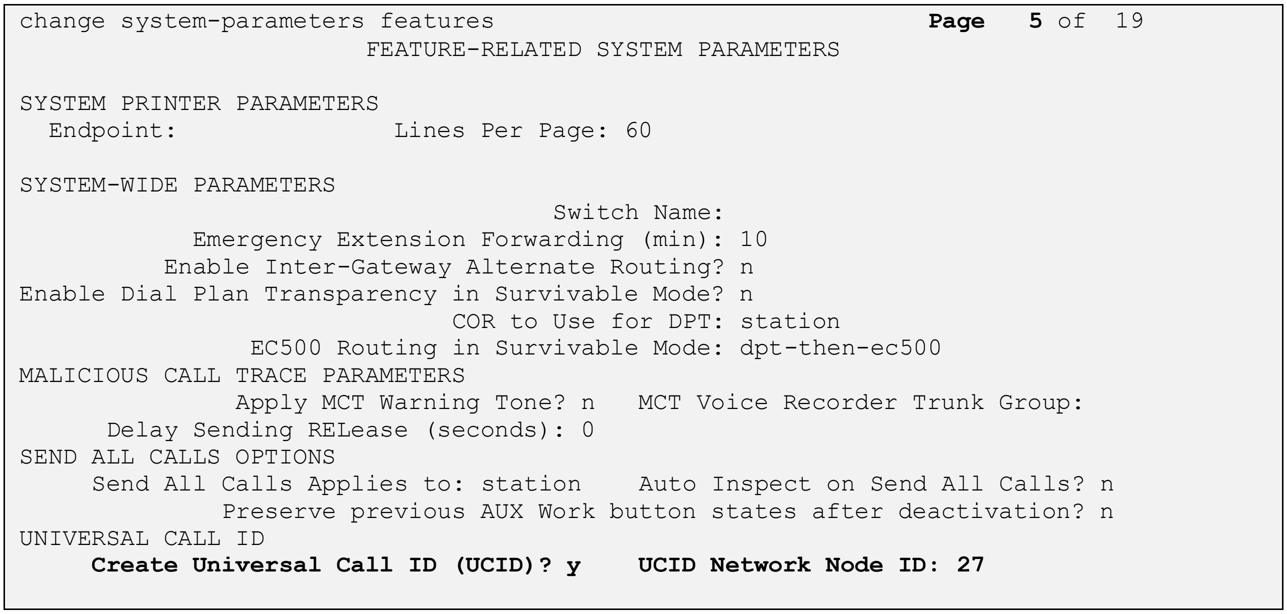
Add a CTI link using the "add cti-link n" command, where "n" is an available CTI link number. Enter an available extension number in the **Extension** field. Note that the CTI link number and extension number may vary. Enter "ADJ-IP" in the **Type** field, and a descriptive name in the **Name** field.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

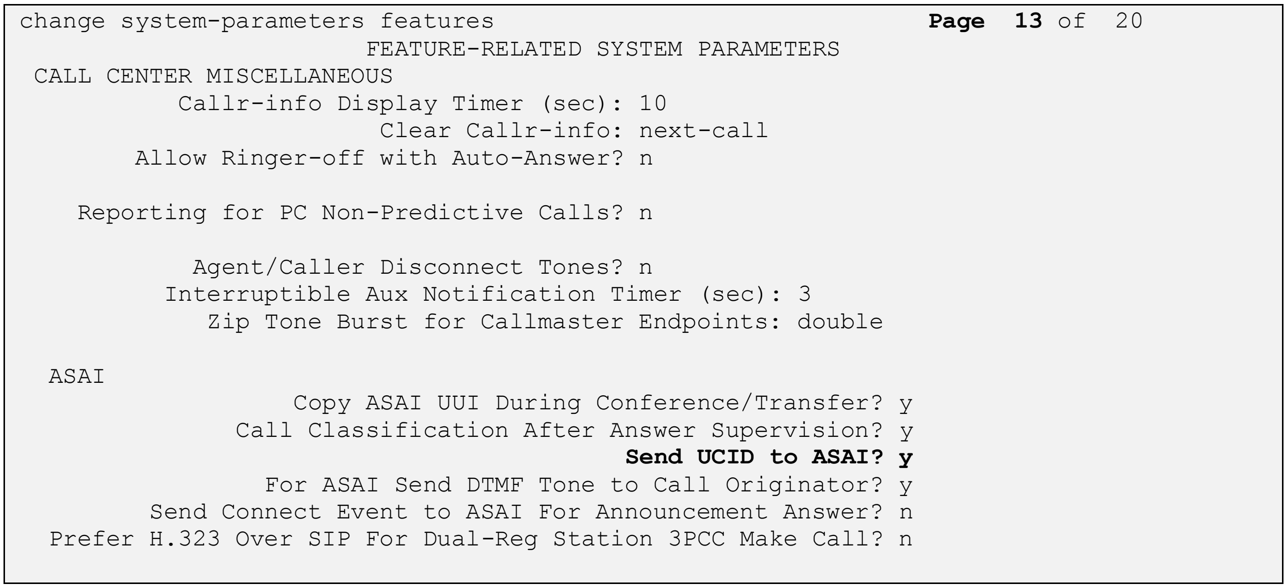
5.3. Administer System Parameters Features

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



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

SYSTEM PRINTER PARAMETERS
  Endpoint:               Lines Per Page: 60

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

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

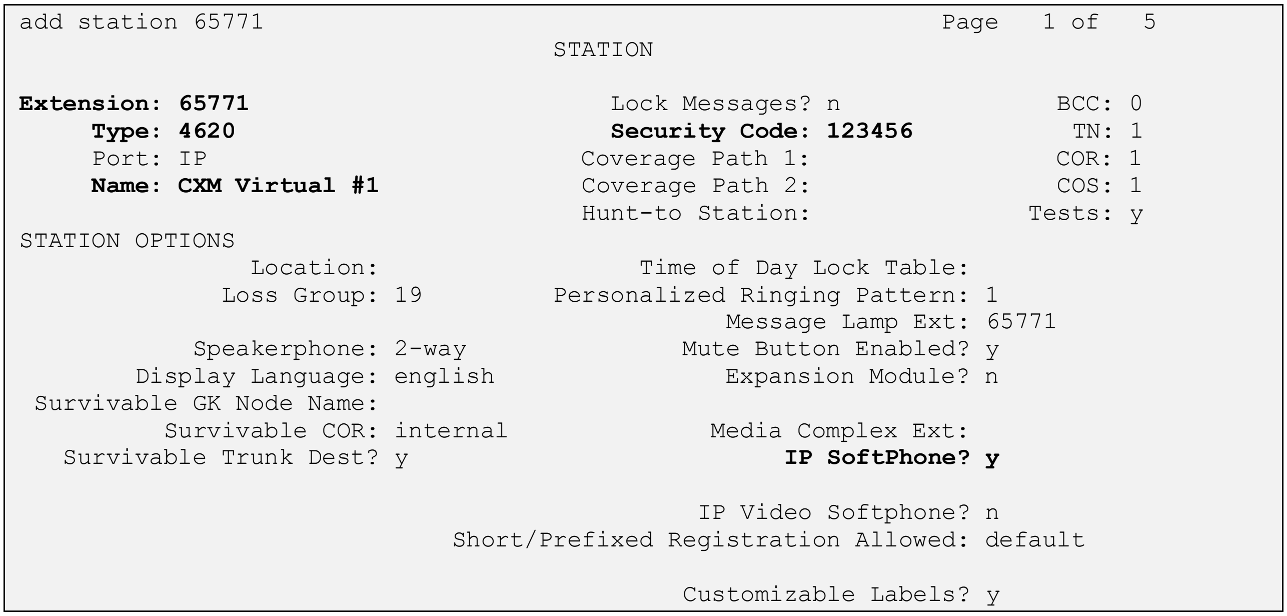


```
change system-parameters features                             Page  13 of  20
                        FEATURE-RELATED SYSTEM PARAMETERS
 CALL CENTER MISCELLANEOUS
           Callr-info Display Timer (sec): 10
                         Clear Callr-info: next-call
        Allow Ringer-off with Auto-Answer? n

    Reporting for PC Non-Predictive Calls? n

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

  ASAI
                   Copy ASAI UUI During Conference/Transfer? y
               Call Classification After Answer Supervision? y
                                          Send UCID to ASAI? y
                 For ASAI Send DTMF Tone to Call Originator? y
         Send Connect Event to ASAI For Announcement Answer? n
  Prefer H.323 Over SIP For Dual-Reg Station 3PCC Make Call? n
```

5.4. Administer Virtual IP Softphones

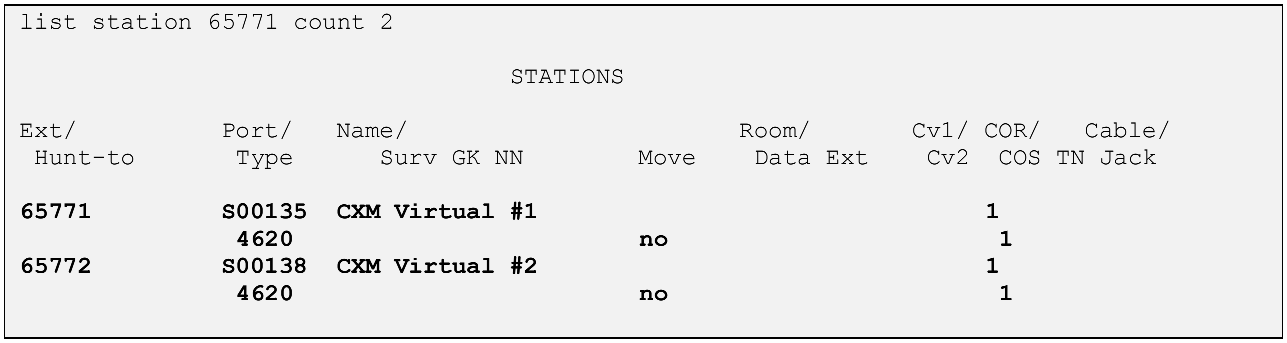
Add a virtual IP softphone using the “add station n” command, where “n” is an available extension number. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Extension:** The available extension number.
- **Type:** A desired IP type, such as “4620”.
- **Name:** A descriptive name.
- **Security Code:** A desired code.
- **IP SoftPhone:** “y”



```
add station 65771                                               Page   1 of   5
                                     STATION

Extension: 65771                         Lock Messages? n               BCC: 0
     Type: 4620                          Security Code: 123456           TN: 1
     Port: IP                          Coverage Path 1:                 COR: 1
     Name: CXM Virtual #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: 65771
            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

                                              Customizable Labels? y
```

Repeat this section to administer the desired number of virtual IP softphones, using the same security code for all virtual IP softphones as required by CXM. When possible, use sequential extensions for the virtual IP softphones, for ease of configuring CXM later. In the compliance testing, two virtual IP softphones were administered as shown below.



```
list station 65771 count 2

                                  STATIONS

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

65771         S00135  CXM Virtual #1                               1
               4620                        no                       1
65772         S00138  CXM Virtual #2                               1
               4620                        no                       1
```

5.5. Obtain VDN Data

Use the “list vdn” command to display a list of pre-configured VDNs. Make a note of the **Name**, and **Ext** for the VDNs that will be used to integrate with CXM. In the compliance testing, the two VDNs shown below were used.

```
list vdn                                                               Page   1

                          VECTOR DIRECTORY NUMBERS

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

CXM Sales              60001           n  1   1    V  1    none

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

5.6. Obtain Skill Group Data

Use the “list hunt-group” command to display a list of pre-configured hunt and skill groups. Make a note of the **Grp Name** and **Ext** for the skill groups that will be used to integrate with CXM. In the compliance testing, the two skill groups shown below were used.

```
list hunt-group

                                HUNT GROUPS
Grp  Grp
No.  Name/           Grp     ACD/              No. Cov  Notif/  Dom   Message
     Ext             Type    MEAS Vec MCH  Que Mem Path Ctg Adj Ctrl  Center

81   CXM Sales Skill
     61001           ucd-mia y/I  SK  none y   0        n             n
82   CXM Support Skill
     61002           ucd-mia y/I  SK  none y   0        n             n
```

5.7. Obtain Station Data

Use the “list station” command to display a list of pre-configured stations. Make a note of the **Ext, Name,** and **Type** for the agent stations that will be used to integrate with CXM. In the compliance testing, the two agent stations highlighted below were used.

```
list station

                                  STATIONS

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

65000         S00036  CM7 Supervisor                         7    1
               9641                        no                      0
65001         S00102  CM7 Station 1                          1    1
               9611                        no                      1
65771         S00135  CXM Virtual 1                               1
               4620                        no                      1
65772         S00138  CXM Virtual 2                               1
               4620                        no                      1
66002         S00004  Avaya, SIP 2                           1    1
               9621SIPCC                   no                      1
```

5.8. Obtain Agent Data

Use the “list agent-loginID” command to display a list of pre-configured agent login IDs. Make a note of the **Login ID** and **Name** for the agents that will be used to integrate with CXM. In the compliance testing, two agent login IDs shown below were used.

```
list agent-loginID

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

65881        Agent 1    unstaffed                                  1   lvl
                  1/01    2/01     /       /       /       /       /       /
65882        Agent 2    unstaffed                                  1   lvl
                  1/01    2/01     /       /       /       /       /       /
```

6. Configure Avaya Aura® Application Enablement Services

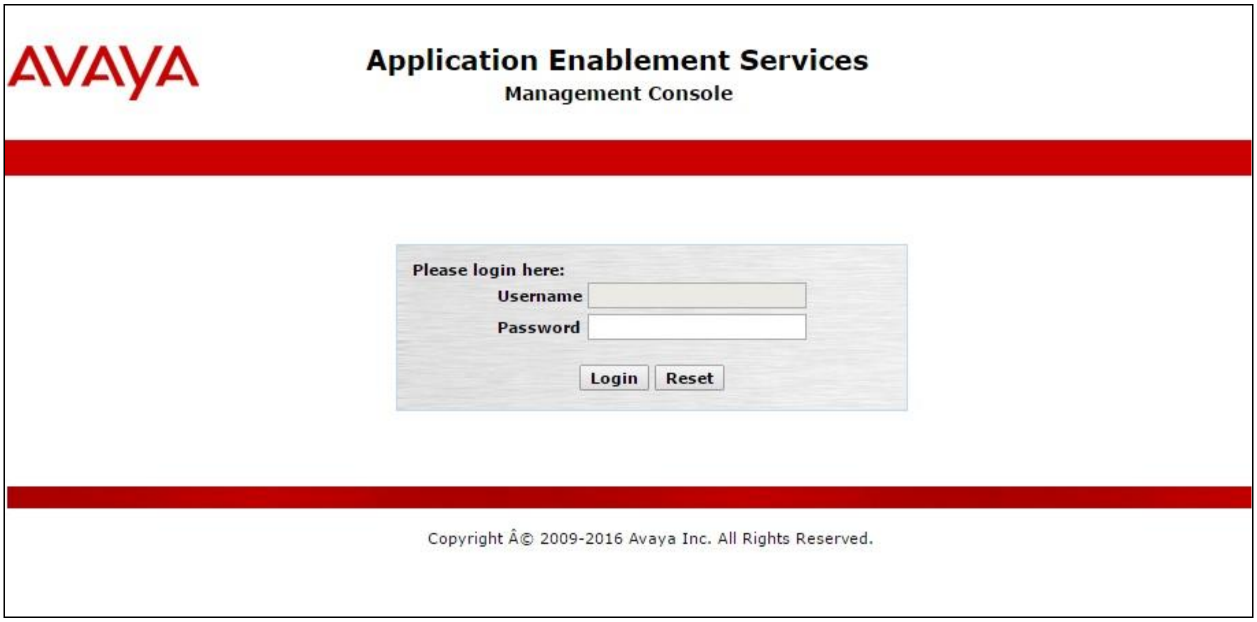
This section provides the procedures for configuring Application Enablement Services. The procedures include the following areas:

- Launch OAM interface
- Verify license
- Administer TSAPI link
- Administer H.323 gatekeeper
- Administer CXM user
- Administer security database
- Administer ports
- Administer TLS settings
- Restart Web server and AE server
- Obtain Tlink name
- Export CA certificate

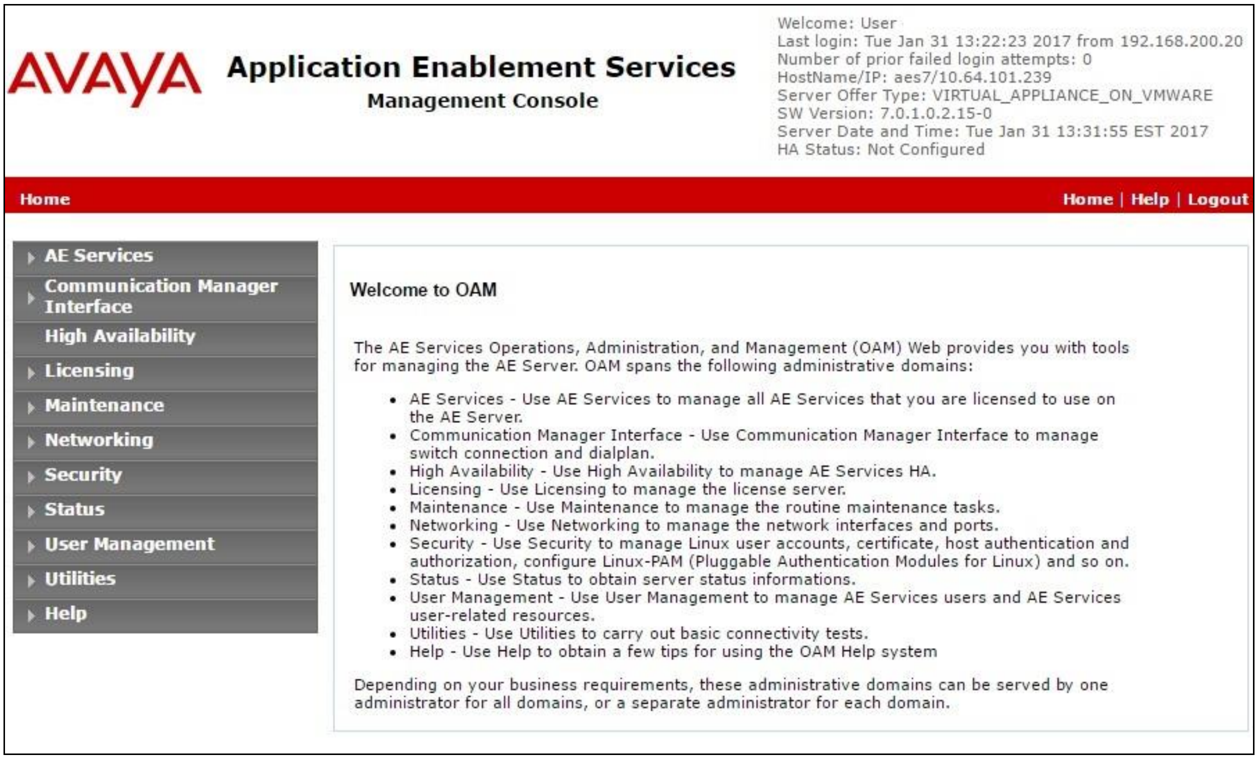
6.1. Launch OAM Interface

Access the OAM web-based interface by using the URL "https://ip-address" in an Internet browser window, where "ip-address" is the IP address of the Application Enablement Services server.

The **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: Tue Jan 31 13:22:23 2017 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: 7.0.1.0.2.15-0
Server Date and Time: Tue Jan 31 13:31:55 EST 2017
HA Status: Not Configured

Welcome to OAM

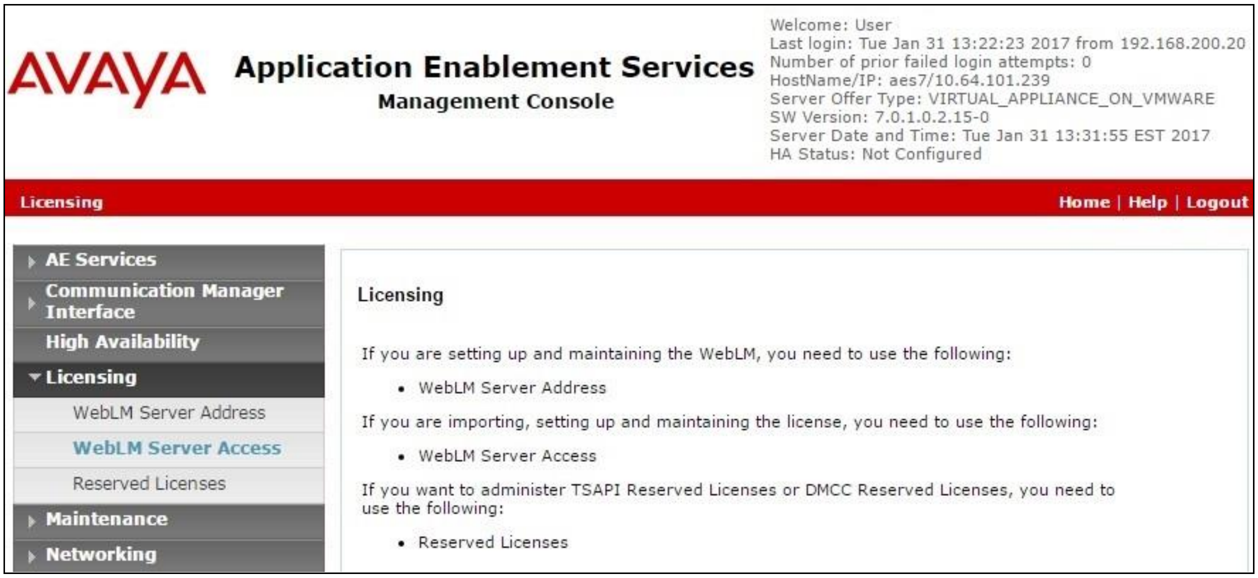
The AE Services Operations, Administration, and Management (OAM) Web provides you with tools for managing the AE Server. OAM spans the following administrative domains:

- 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.

6.2. 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: Tue Jan 31 13:22:23 2017 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: 7.0.1.0.2.15-0
Server Date and Time: Tue Jan 31 13:31:55 EST 2017
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:

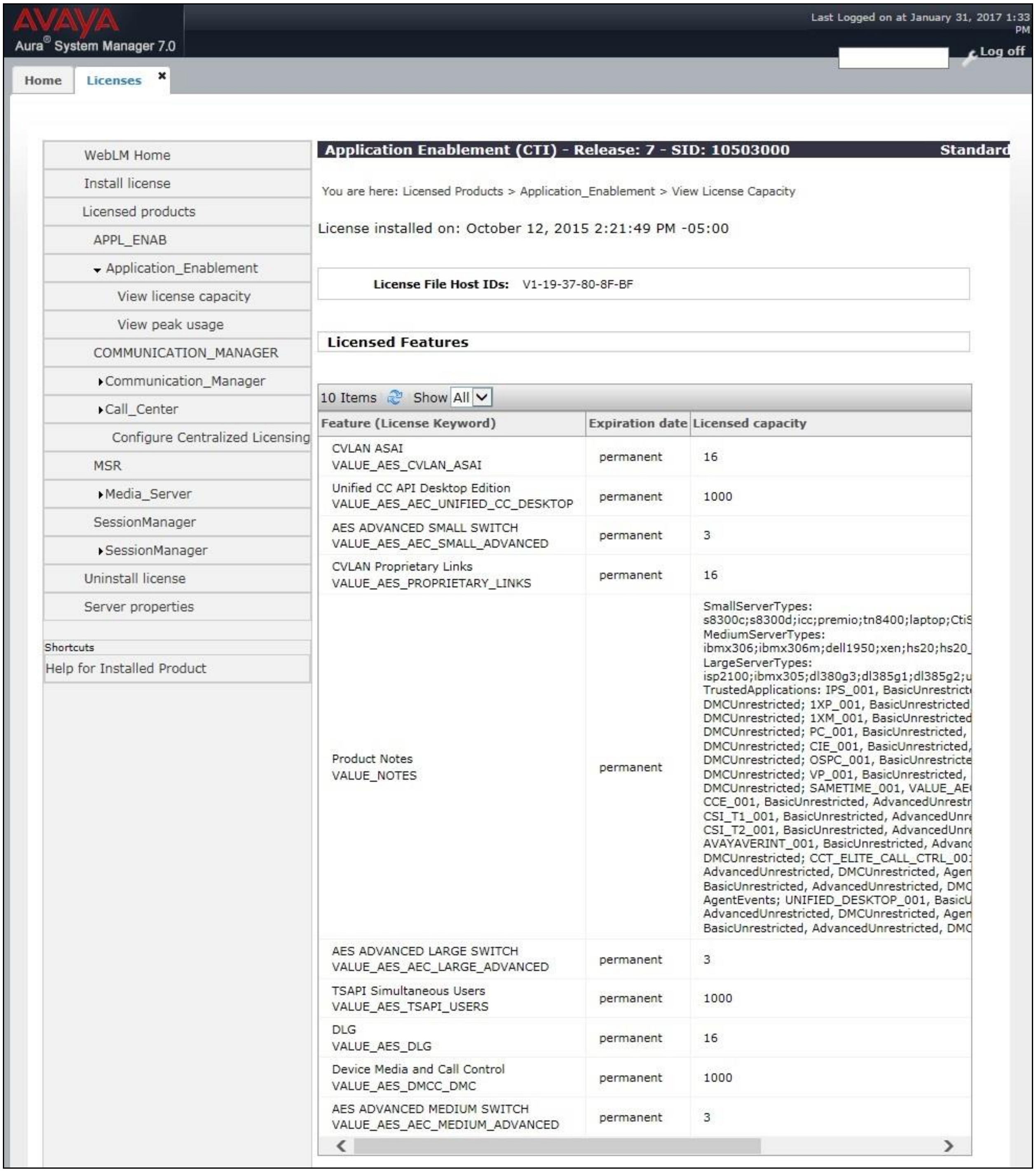
- WebLM Server Access

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 device monitoring, 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 2:21:49 PM -05:00

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

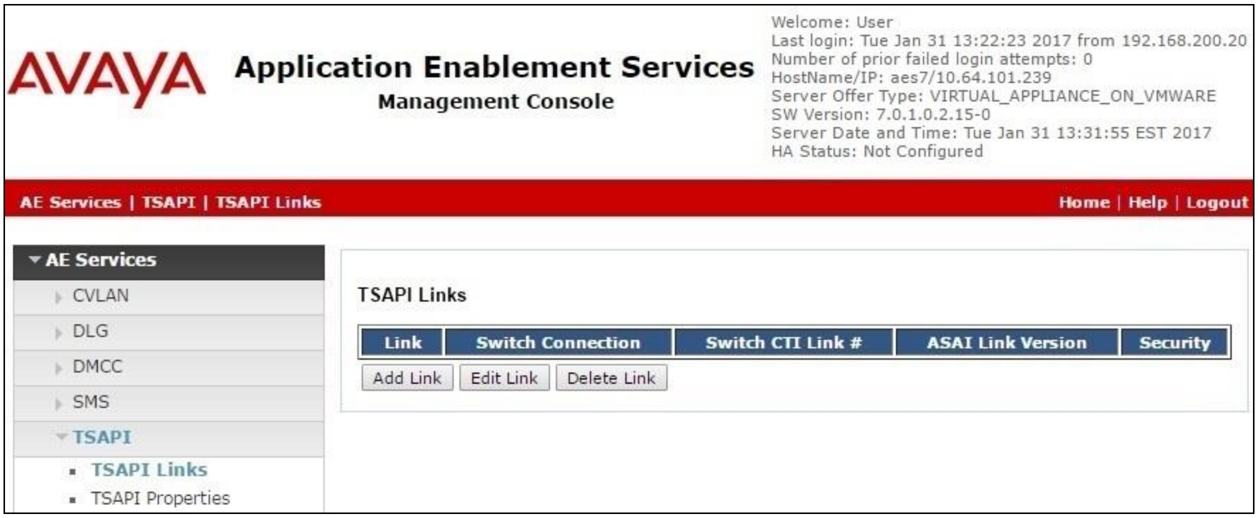
Licensed Features

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;Cti 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, AdvancedUnrestr CSI_T1_001, BasicUnrestricted, AdvancedUnre CSI_T2_001, BasicUnrestricted, AdvancedUnre AVAYAVERINT_001, BasicUnrestricted, Advanc DMCUnrestricted; CCT_ELITE_CALL_CTRL_00 AdvancedUnrestricted, DMCUnrestricted, Agen BasicUnrestricted, AdvancedUnrestricted, DMC AgentEvents; UNIFIED_DESKTOP_001, BasicU AdvancedUnrestricted, DMCUnrestricted, Agen 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

6.3. Administer TSAPI Link

Select **AE Services → TSAPI → TSAPI Links** from the left pane of the **Management Console**, to administer a TSAPI link. The **TSAPI Links** screen is displayed, as shown below. Click **Add Link**.



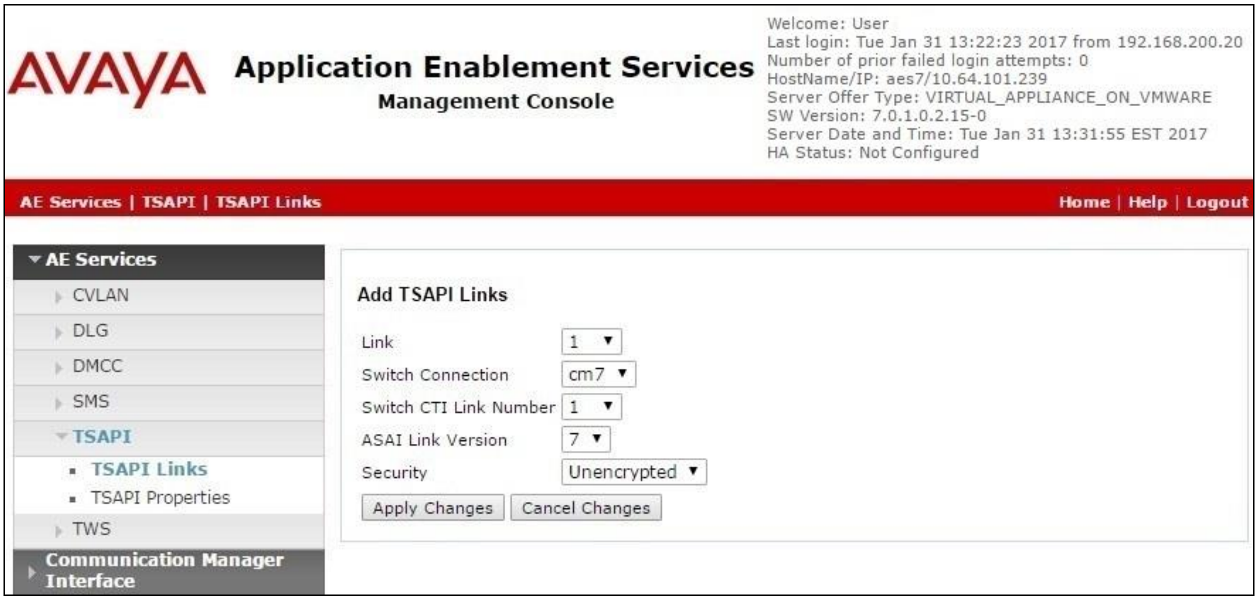
Welcome: User
Last login: Tue Jan 31 13:22:23 2017 from 192.168.200.20
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.1.0.2.15-0
Server Date and Time: Tue Jan 31 13:31:55 EST 2017
HA Status: Not Configured

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: Tue Jan 31 13:22:23 2017 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: 7.0.1.0.2.15-0
Server Date and Time: Tue Jan 31 13:31:55 EST 2017
HA Status: Not Configured

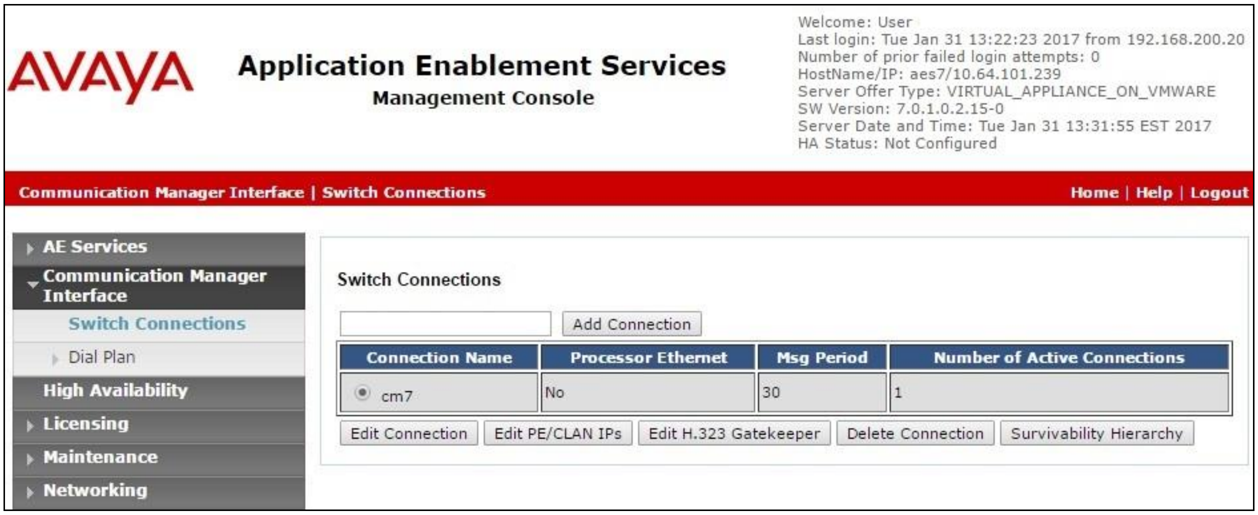
Add TSAPI Links

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

6.4. Administer H.323 Gatekeeper

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

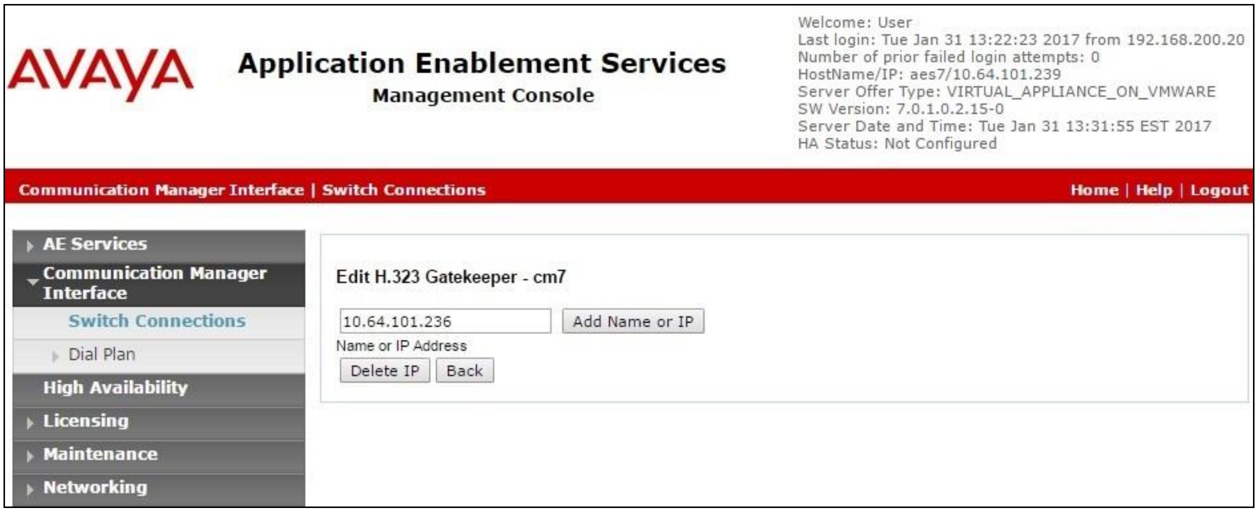


Welcome: User
Last login: Tue Jan 31 13:22:23 2017 from 192.168.200.20
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.1.0.2.15-0
Server Date and Time: Tue Jan 31 13:31:55 EST 2017
HA Status: Not Configured

Switch Connections

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections
● cm7	No	30	1

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



Welcome: User
Last login: Tue Jan 31 13:22:23 2017 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: 7.0.1.0.2.15-0
Server Date and Time: Tue Jan 31 13:31:55 EST 2017
HA Status: Not Configured

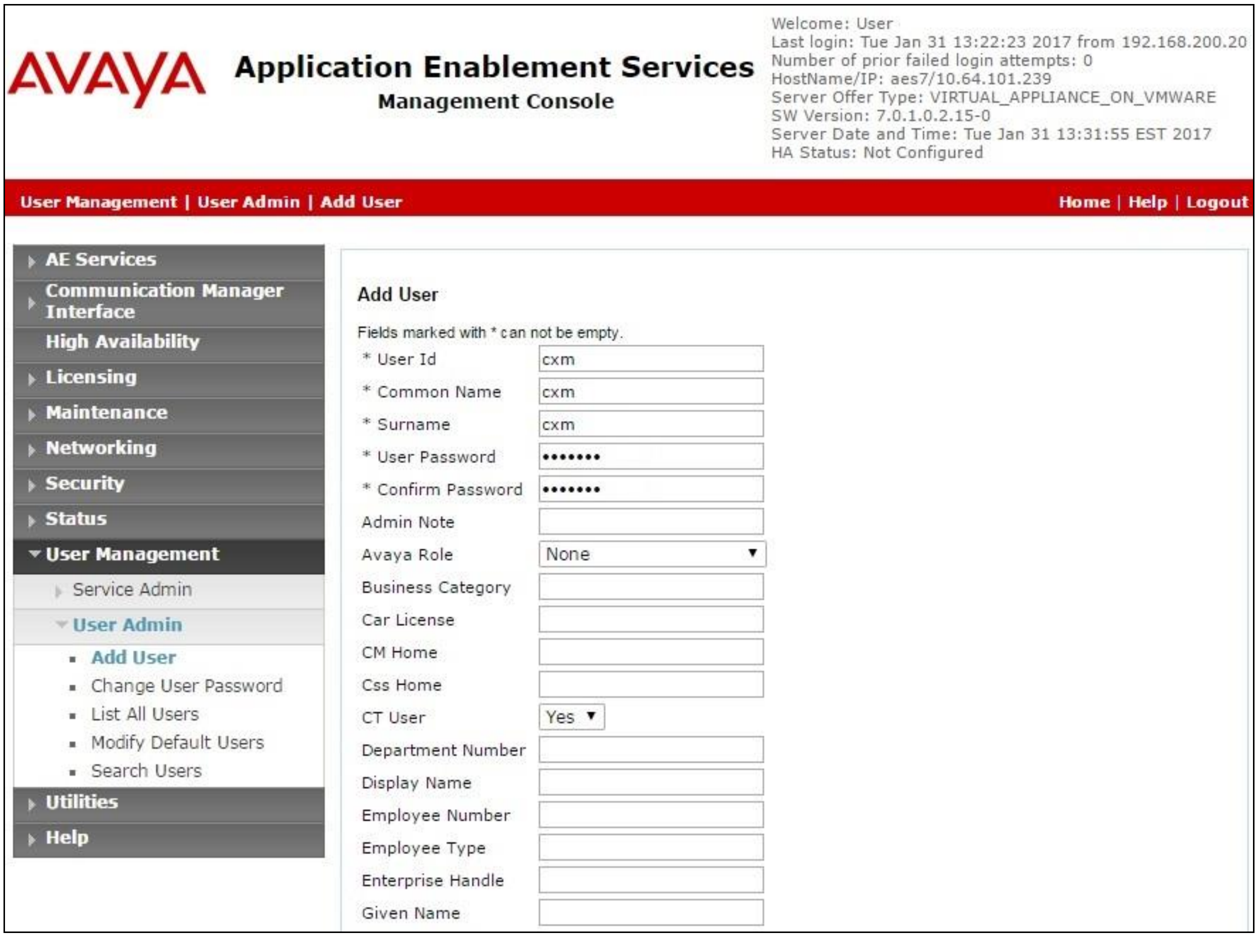
Edit H.323 Gatekeeper - cm7

Name or IP Address: 10.64.101.236

6.5. Administer CXM 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: Tue Jan 31 13:22:23 2017 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: 7.0.1.0.2.15-0
Server Date and Time: Tue Jan 31 13:31:55 EST 2017
HA Status: Not Configured

Add User

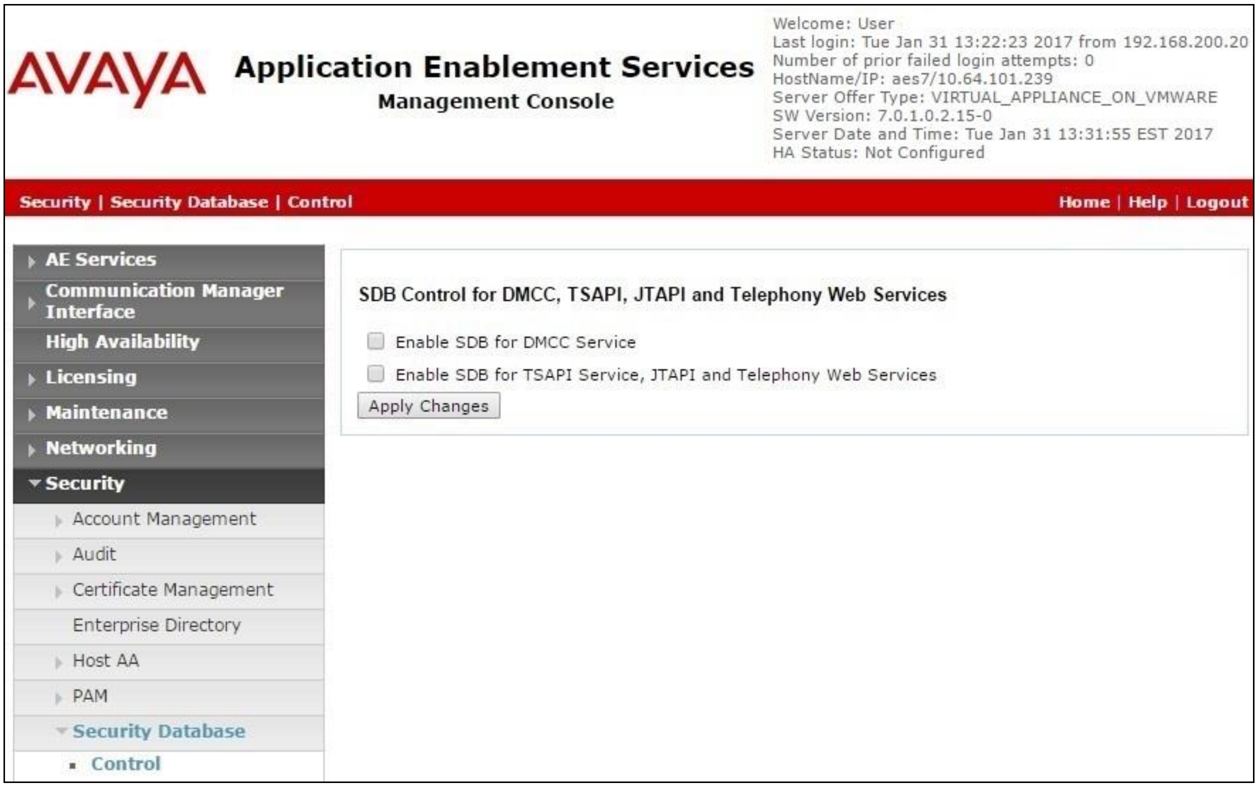
Fields marked with * can not be empty.

* User Id	cxm
* Common Name	cxm
* Surname	cxm
* 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	

6.6. 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 that both parameters are unchecked, as shown below.

In the event that the security database is used by the customer with parameters already enabled, then follow reference [2] to configure access privileges for the CXM user from **Section 6.5**.



Welcome: User
Last login: Tue Jan 31 13:22:23 2017 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: 7.0.1.0.2.15-0
Server Date and Time: Tue Jan 31 13:31:55 EST 2017
HA Status: Not Configured

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

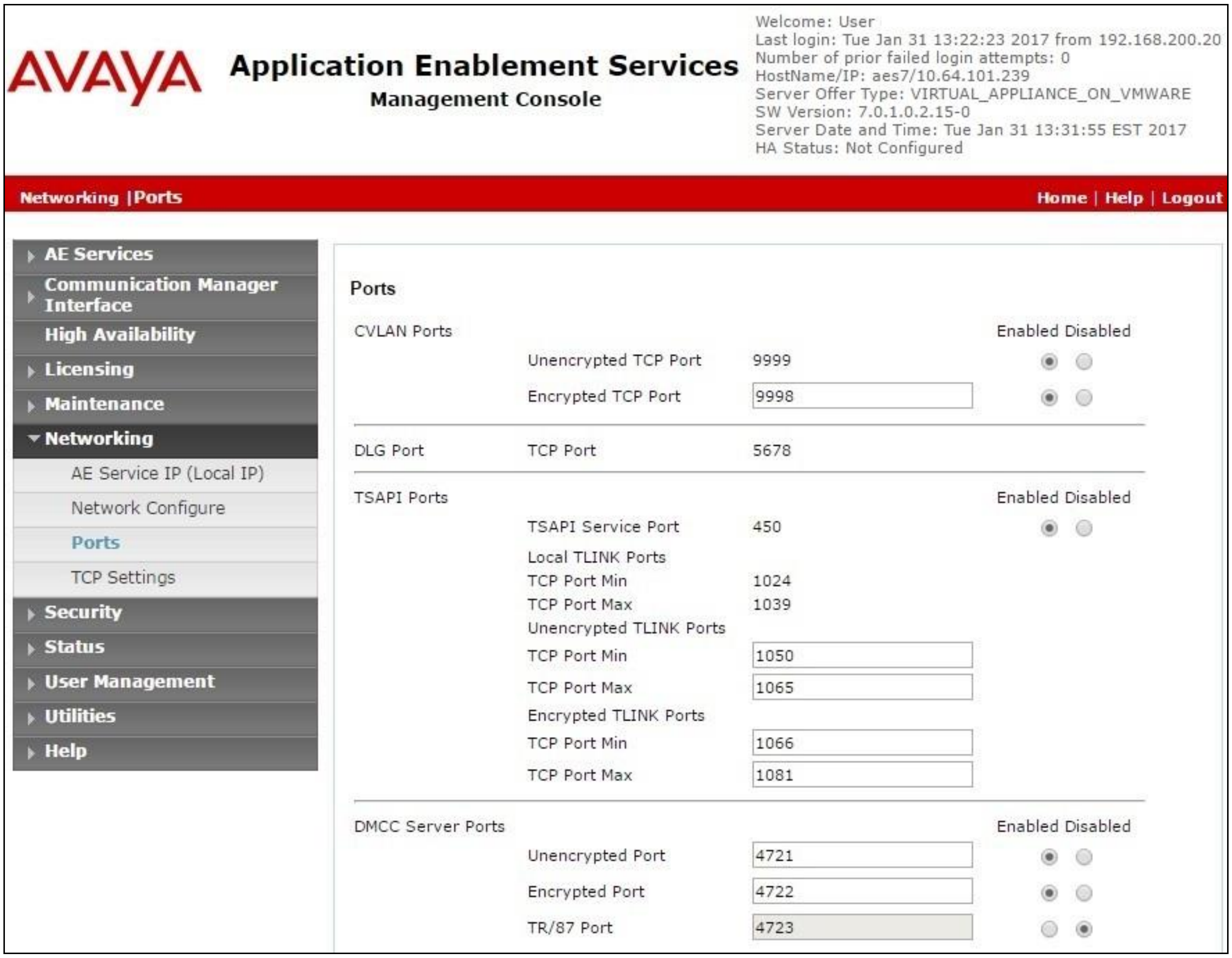
☐ Enable SDB for DMCC Service

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

6.7. Administer Ports

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

In the **DMCC Server Ports** section, select the radio button for **Encrypted Port** under the **Enabled** column, as shown below. Retain the default values in the remaining fields.



Welcome: User
Last login: Tue Jan 31 13:22:23 2017 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: 7.0.1.0.2.15-0
Server Date and Time: Tue Jan 31 13:31:55 EST 2017
HA Status: Not Configured

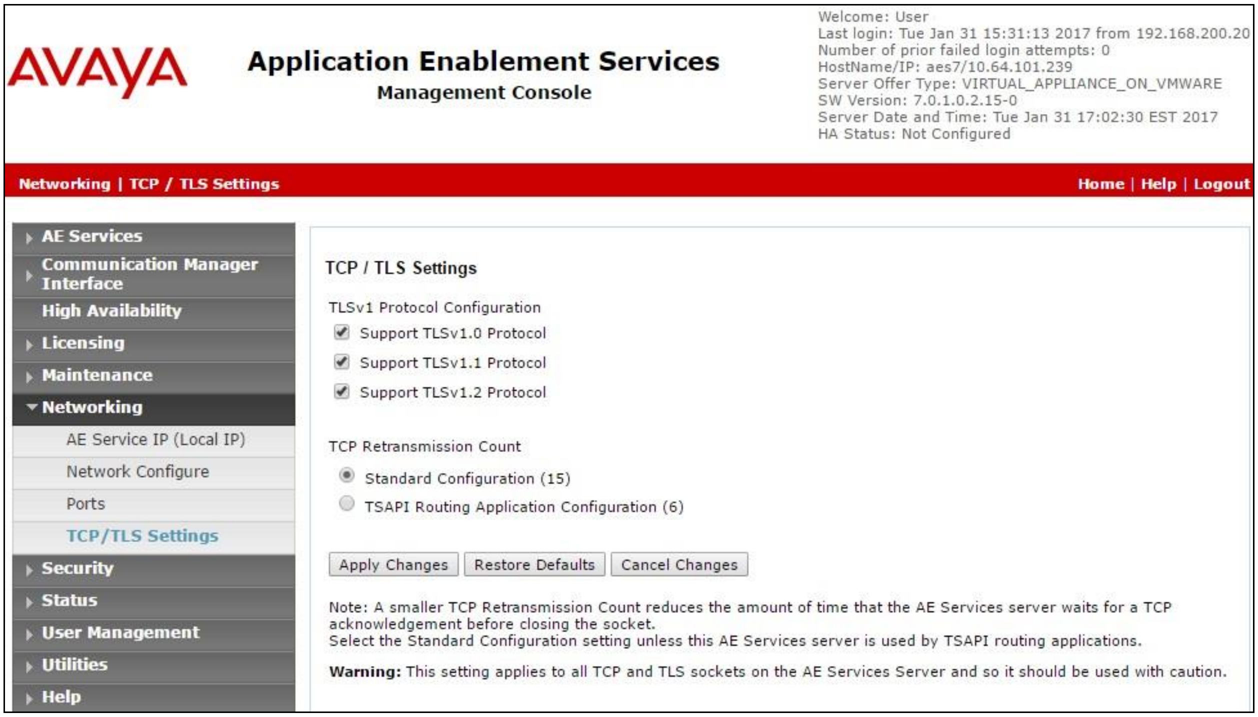
Ports

			Enabled	Disabled
CVLAN Ports				
	Unencrypted TCP Port	9999	●	○
	Encrypted TCP Port	9998	●	○
DLG Port	TCP Port	5678		
TSAPI Ports				
	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				
	Unencrypted Port	4721	●	○
	Encrypted Port	4722	●	○
	TR/87 Port	4723	○	●

6.8. Administer TLS Settings

Select **Networking → TCP/TLS Settings** from the left pane, to display the **TCP/TLS Settings** screen in the right pane. Check **Support TLSv1.0 Protocol** and **Support TLSv1.1 Protocol** as shown below, and retain the default values in the remaining fields.

Note that TLS versions 1.0 and 1.1 are needed in this integration, due to use of pre-7.0 version of DMCC SDK by CXM for encrypted connections.



Welcome: User
Last login: Tue Jan 31 15:31:13 2017 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: 7.0.1.0.2.15-0
Server Date and Time: Tue Jan 31 17:02:30 EST 2017
HA Status: Not Configured

TCP / TLS Settings

TLSv1 Protocol Configuration

☑ Support TLSv1.0 Protocol
☑ Support TLSv1.1 Protocol
☑ Support TLSv1.2 Protocol

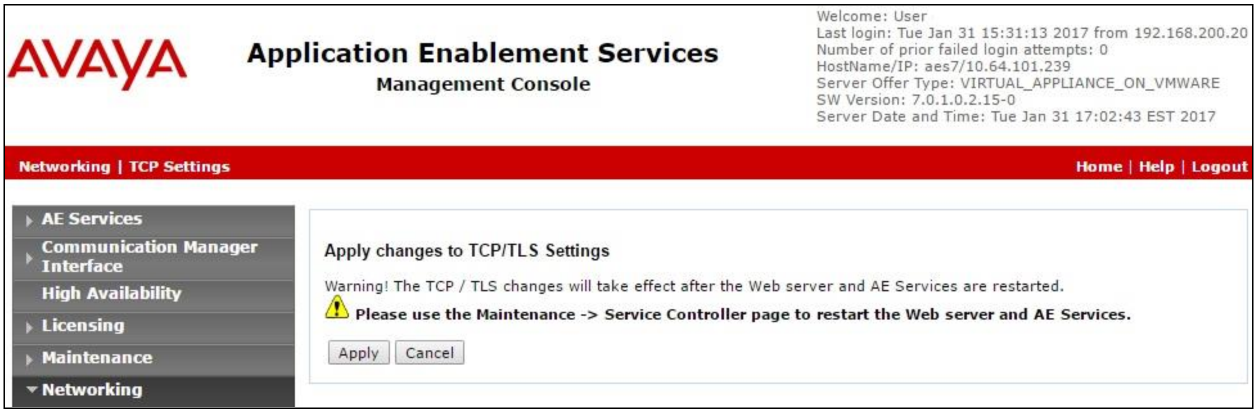
TCP Retransmission Count

● Standard Configuration (15)
○ TSAPI Routing Application Configuration (6)

Note: A smaller TCP Retransmission Count reduces the amount of time that the AE Services server waits for a TCP acknowledgement before closing the socket.
Select the Standard Configuration setting unless this AE Services server is used by TSAPI routing applications.

Warning: This setting applies to all TCP and TLS sockets on the AE Services Server and so it should be used with caution.

The screen below is displayed next.



Welcome: User
Last login: Tue Jan 31 15:31:13 2017 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: 7.0.1.0.2.15-0
Server Date and Time: Tue Jan 31 17:02:43 EST 2017

Apply changes to TCP/TLS Settings

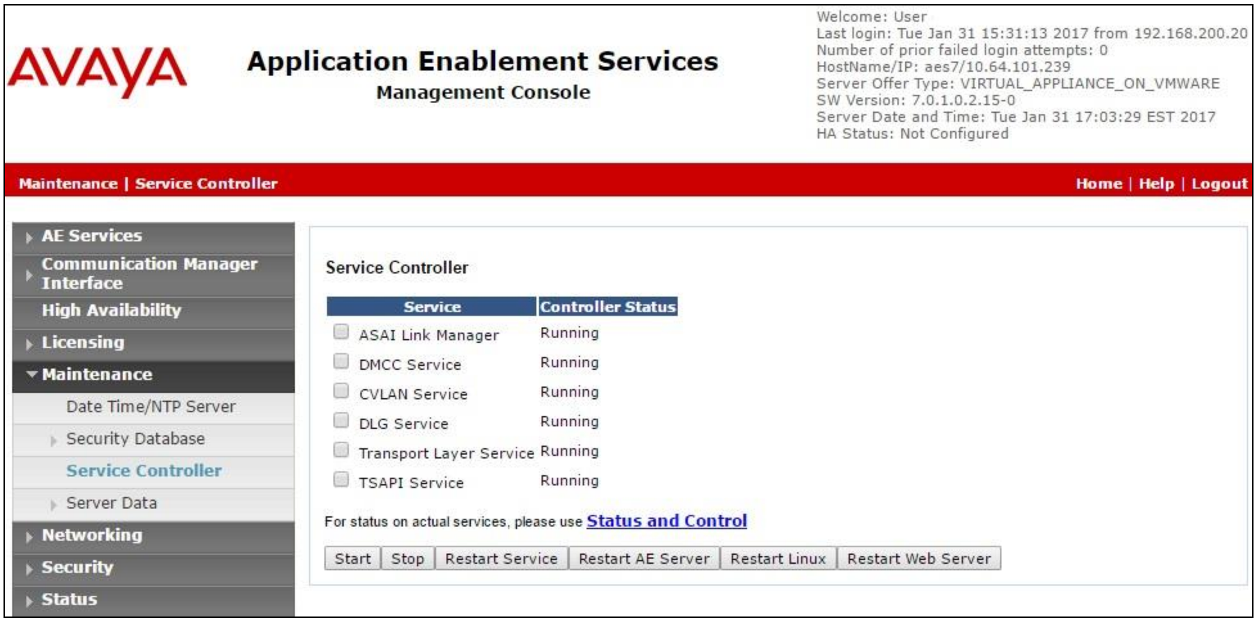
Warning! The TCP / TLS changes will take effect after the Web server and AE Services are restarted.

⚠ **Please use the Maintenance -> Service Controller page to restart the Web server and AE Services.**

6.9. Restart Web Server and AE Server

Select **Maintenance → Service Controller** from the left pane, to display the **Service Controller** screen in the right pane. Click **Restart Web Server** to restart the Web server.

After the Web server is restarted, log back into the web interface and select **Maintenance → Service Controller** to display the **Service Controller** screen again. Click **Restart AE Server** to restart services.



Welcome: User
Last login: Tue Jan 31 15:31:13 2017 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: 7.0.1.0.2.15-0
Server Date and Time: Tue Jan 31 17:03:29 EST 2017
HA Status: Not Configured

Service Controller

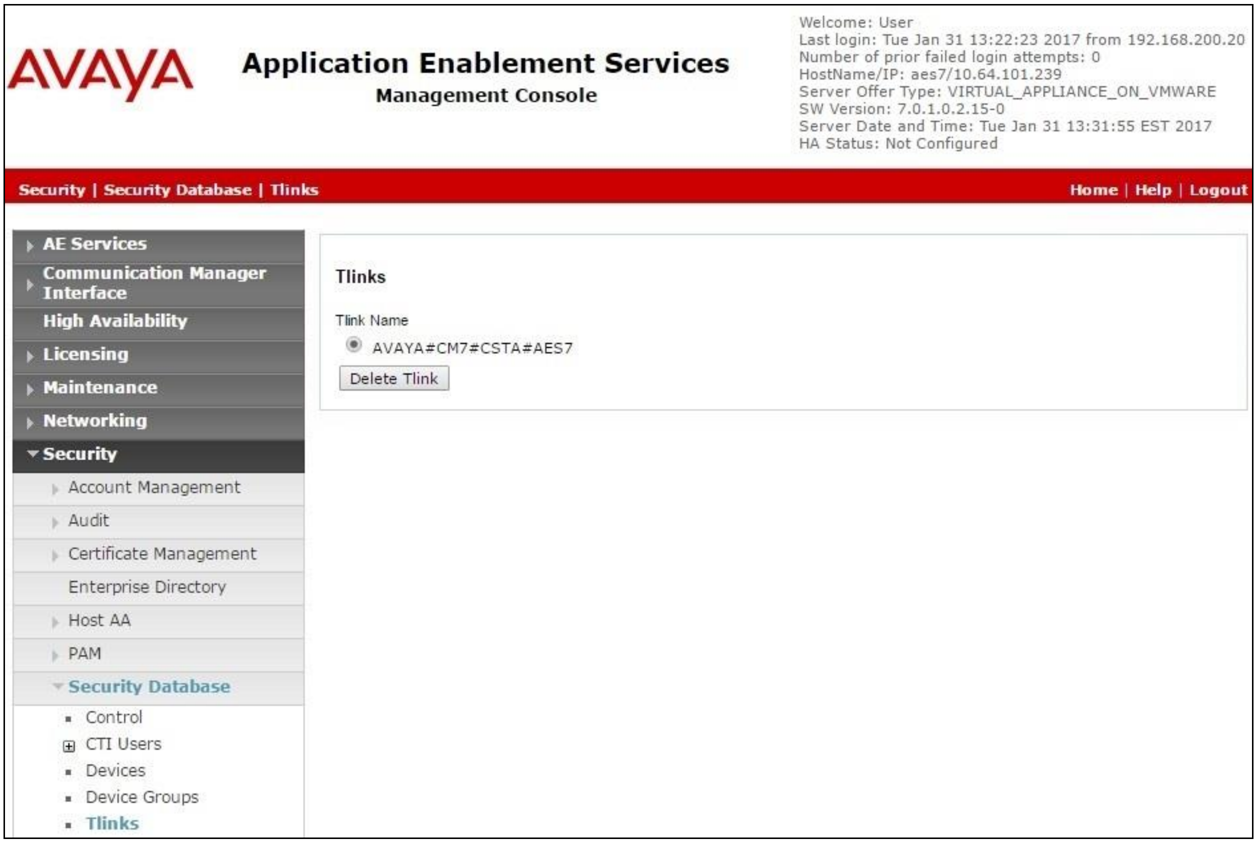
Service	Controller Status
□ ASAI Link Manager	Running
□ DMCC Service	Running
□ CVLAN Service	Running
□ DLG Service	Running
□ Transport Layer Service	Running
□ TSAPI Service	Running

For status on actual services, please use Status and Control

6.10. 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 CXM.

In this case, the associated Tlink name is "AVAYA#**CM7**#CSTA#**AES7**". Note the use of the switch connection "CM7" from **Section 6.3** as part of the Tlink name.



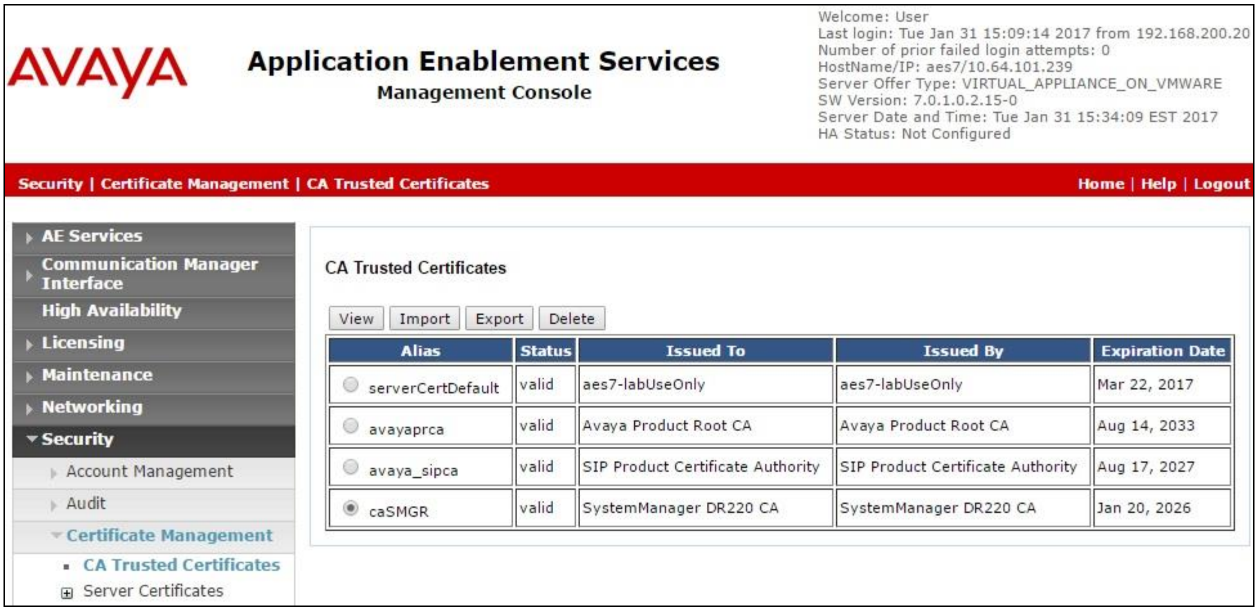
Welcome: User
Last login: Tue Jan 31 13:22:23 2017 from 192.168.200.20
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.1.0.2.15-0
Server Date and Time: Tue Jan 31 13:31:55 EST 2017
HA Status: Not Configured

Tlinks

Tlink Name
● AVAYA#CM7#CSTA#AES7

6.11. Export CA Certificate

Select **Security → Certificate Management → CA Trusted Certificates** from the left pane, to display the **CA Trusted Certificates** screen. Select the pertinent CA certificate for secure connection with client applications, in this case “caSMGR”, and click **Export**.

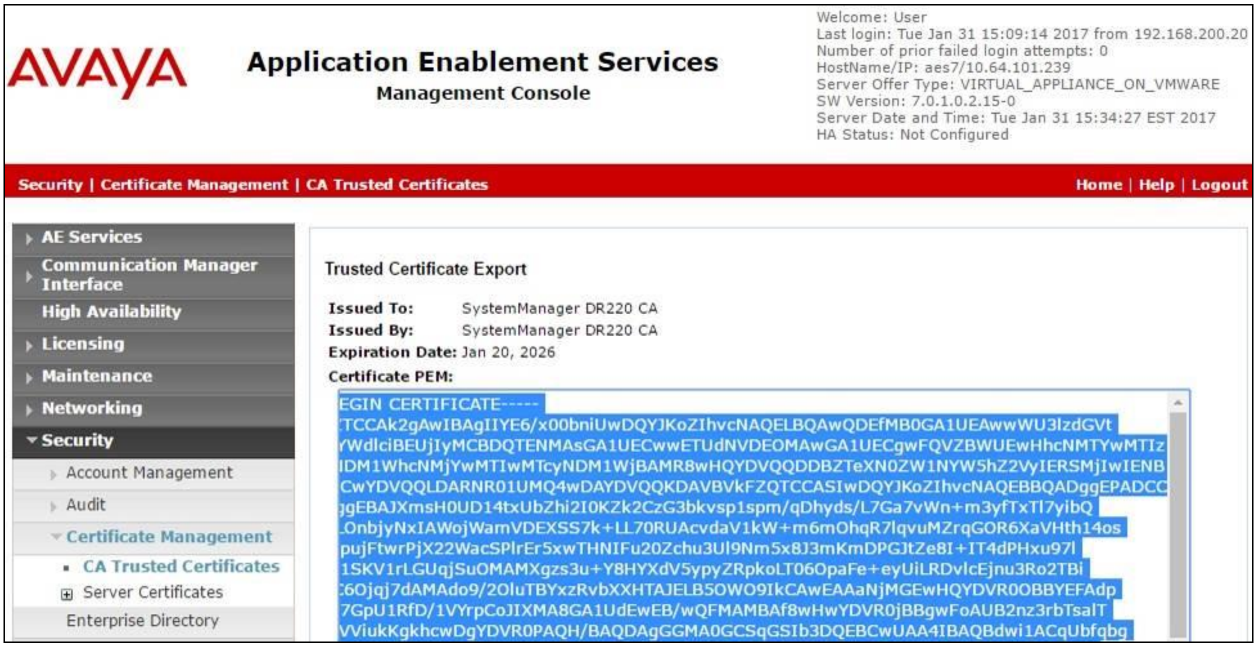


Welcome: User
Last login: Tue Jan 31 15:09:14 2017 from 192.168.200.20
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.1.0.2.15-0
Server Date and Time: Tue Jan 31 15:34:09 EST 2017
HA Status: Not Configured

CA Trusted Certificates

Alias	Status	Issued To	Issued By	Expiration Date
○ serverCertDefault	valid	aes7-labUseOnly	aes7-labUseOnly	Mar 22, 2017
○ avayaprca	valid	Avaya Product Root CA	Avaya Product Root CA	Aug 14, 2033
○ avaya_sipca	valid	SIP Product Certificate Authority	SIP Product Certificate Authority	Aug 17, 2027
● caSMGR	valid	SystemManager DR220 CA	SystemManager DR220 CA	Jan 20, 2026

The **Trusted Certificate Export** screen is displayed next. Copy everything in the text box as shown below, including the **BEGIN CERTIFICATE** and **END CERTIFICATE** lines. Paste the copied content to a Notepad file, and save with the file name **avaya.crt**, as required by CXM.



Welcome: User
Last login: Tue Jan 31 15:09:14 2017 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: 7.0.1.0.2.15-0
Server Date and Time: Tue Jan 31 15:34:27 EST 2017
HA Status: Not Configured

Trusted Certificate Export

Issued To: SystemManager DR220 CA
Issued By: SystemManager DR220 CA
Expiration Date: Jan 20, 2026
Certificate PEM:

```
EGIN CERTIFICATE-----
'TCCAk2gAwIBAgIIYE6/x00bniUwDQYJKoZIhvcNAQELBQAwQDEfMB0GA1UEAwwWU3lzdGVt
'WdlciBEUjIyMCBDQTENMAsGA1UECwwETUdNVDEOMAwGA1UECgwFQVZBWUEwHhcNMTYwMTIz
IDM1WhcNMjYwMTIwMTcyNDM1WjBAMR8wHQYDVQQDDBZTeXN0ZW1NYW5hZ2VyIERSMjIwIENB
CwYDVQQLDARNR01UMQ4wDAYDVQQKDAVBVkFZQTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCC
jgEBAJXmsH0UD14txUbZhi2I0KZk2CzG3bkvsp1spm/qDhyds/L7Ga7vWn+m3yfTxTl7yibQ
.OnbjyNxIAWojWamVDEXSS7k+LL70RUAcvdaV1kW+m6mOhqR7lqvuMZrqGOR6XaVHth14os
pujFtwrPjX22WacSPlrEr5xwTHNIFu20Zchu3Ul9Nm5x8J3mKmDPGJtZe8I+IT4dPHxu97l
1SKV1rLGUqjSuOMAMXgzs3u+Y8HYXdV5ypyZRpkoLT06OpaFe+eyUiLRDvlcEjnu3Ro2TBi
:6Ojqj7dAMAdo9/2OluTBYxzRvbXXHTAJELB5OWO9IkCAwEAAaNjMGEwHQYDVR0OBBYEFAdp
7GpU1RfD/1VYrpCoJIXMA8GA1UdEwEB/wQFMAMBAf8wHwYDVR0jBBgwFoAUB2nz3rbTsalT
VViukKgkhcwDgYDVR0PAQH/BAQDAgGGMA0GCSqGSIb3DQEBCwUAA4IBAQBdwi1ACqUbfqbg
```

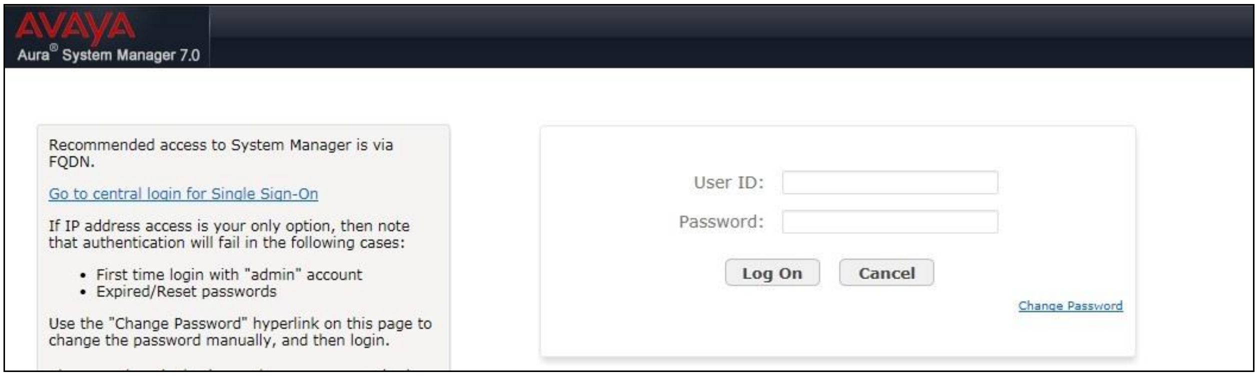
7. Configure Avaya Aura® Session Manager

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

- Launch System Manager
- Administer users

7.1. Launch System Manager

Access the System Manager web interface by using the URL "https://ip-address" in an Internet browser window, where "ip-address" is the IP address of System Manager. Log in using the appropriate credentials.



Recommended access to System Manager is via FQDN.

If IP address access is your only option, then note that authentication will fail in the following cases:

- First time login with "admin" account
- Expired/Reset passwords

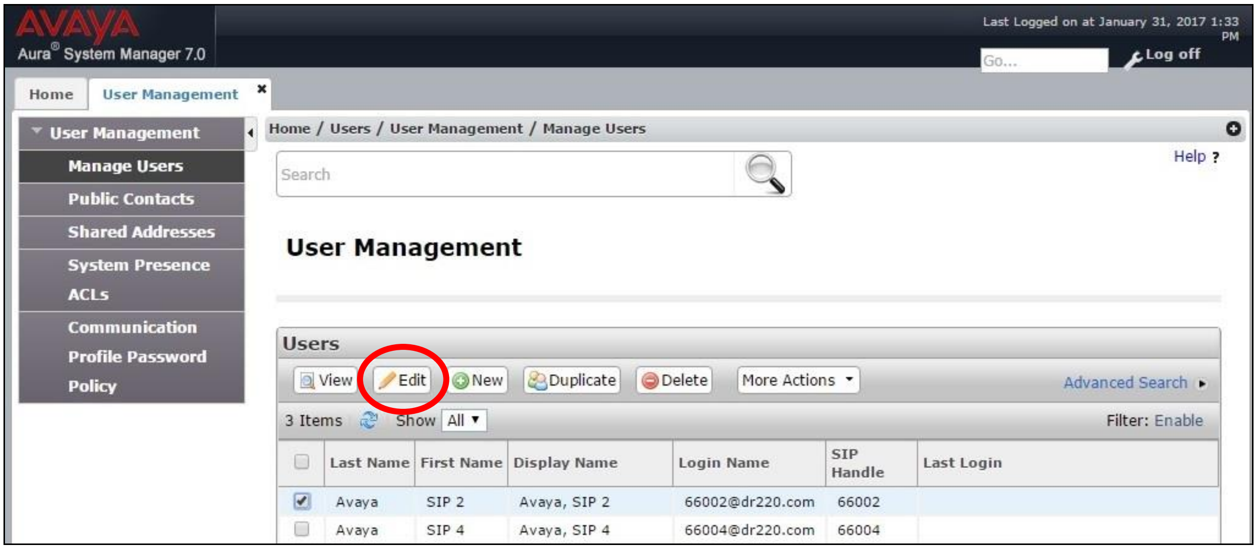
Use the "Change Password" hyperlink on this page to change the password manually, and then login.

User ID:

Password:

7.2. Administer Users

In the subsequent screen (not shown), select **Users → User Management**. Select **User Management → Manage Users** from the left pane to display the **User Management** screen below. Select the entry associated with the first SIP agent station from **Section 3**, in this case "66002", and click **Edit**.



User Management

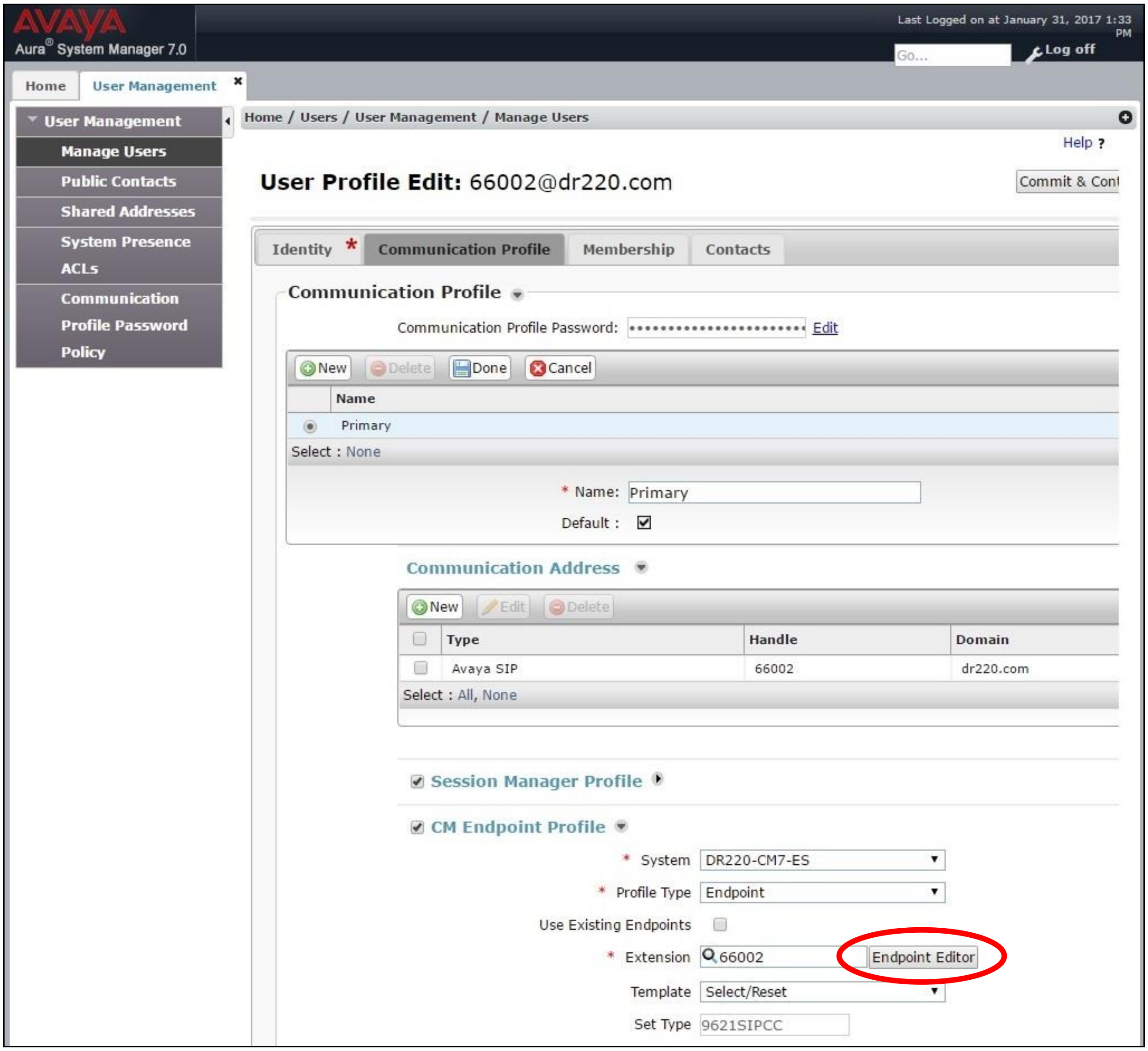
Users

3 Items

☐	Last Name	First Name	Display Name	Login Name	SIP Handle	Last Login
☑	Avaya	SIP 2	Avaya, SIP 2	66002@dr220.com	66002	
☐	Avaya	SIP 4	Avaya, SIP 4	66004@dr220.com	66004	

The **User Profile Edit** screen is displayed. Select the **Communication Profile** tab to display the screen below.

Navigate to the **CM Endpoint Profile** sub-section, and click **Endpoint Editor**.



User Profile Edit: 66002@dr220.com

Communication Profile

Communication Profile Password: •••••••••••••••••••••••• Edit

	Name
●	Primary

Select : None

* Name: Primary

Default : ☑

Communication Address

□	Type	Handle	Domain
□	Avaya SIP	66002	dr220.com

Select : All, None

☑ Session Manager Profile

☑ CM Endpoint Profile

* System DR220-CM7-ES

* Profile Type Endpoint

Use Existing Endpoints □

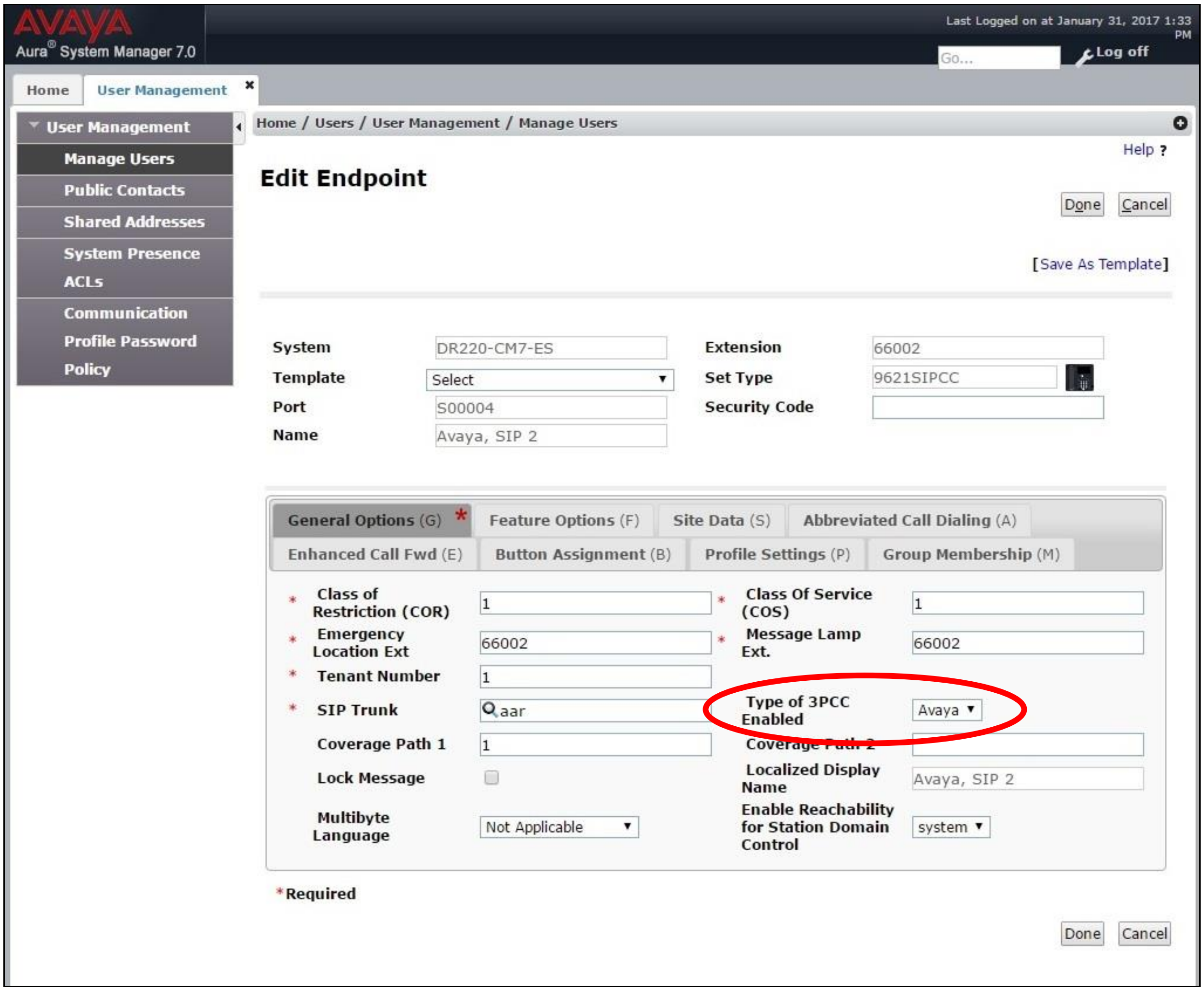
* Extension 66002

Template Select/Reset

Set Type 9621SIPCC

The **Edit Endpoint** screen is displayed next. For **Type of 3PCC Enabled**, select “Avaya” from the drop-down list as shown below. Retain the default values in the remaining fields.

Repeat this section for all SIP agent users.



Edit Endpoint

System	DR220-CM7-ES	Extension	66002
Template	Select	Set Type	9621SIPCC
Port	S00004	Security Code	
Name	Avaya, SIP 2		

* Class of Restriction (COR)	1	* Class Of Service (COS)	1
* Emergency Location Ext	66002	* Message Lamp Ext.	66002
* Tenant Number	1		
* SIP Trunk	aar	Type of 3PCC Enabled	Avaya
Coverage Path 1	1	Coverage Path 2	
Lock Message	□	Localized Display Name	Avaya, SIP 2
Multibyte Language	Not Applicable	Enable Reachability for Station Domain Control	system

*Required

8. Configure CXM

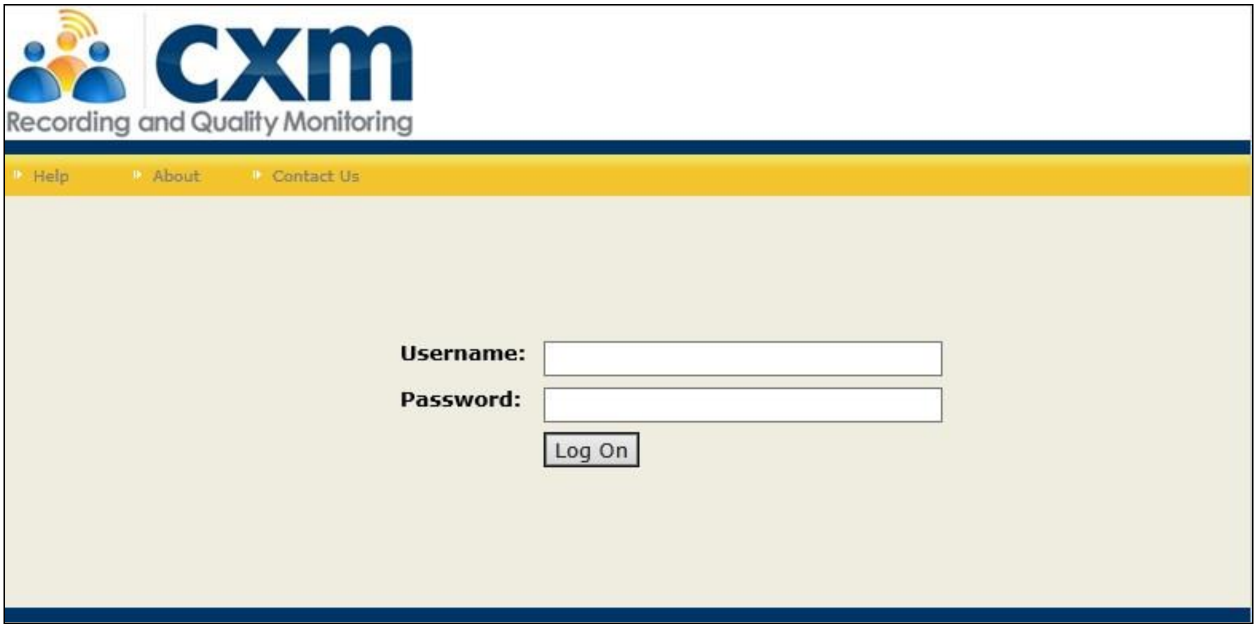
This section provides the procedures for configuring CXM. The procedures include the following areas:

- Launch web interface
- Administer switch setup
- Administer conference stations
- Administer stations
- Administer VDNs
- Administer skills
- Administer agents
- Install CA certificate
- Administer CXM services

The configuration of CXM is performed by the CXM install technicians. The procedural steps are presented in these Application Notes for informational purposes.

8.1. Launch Web Interface

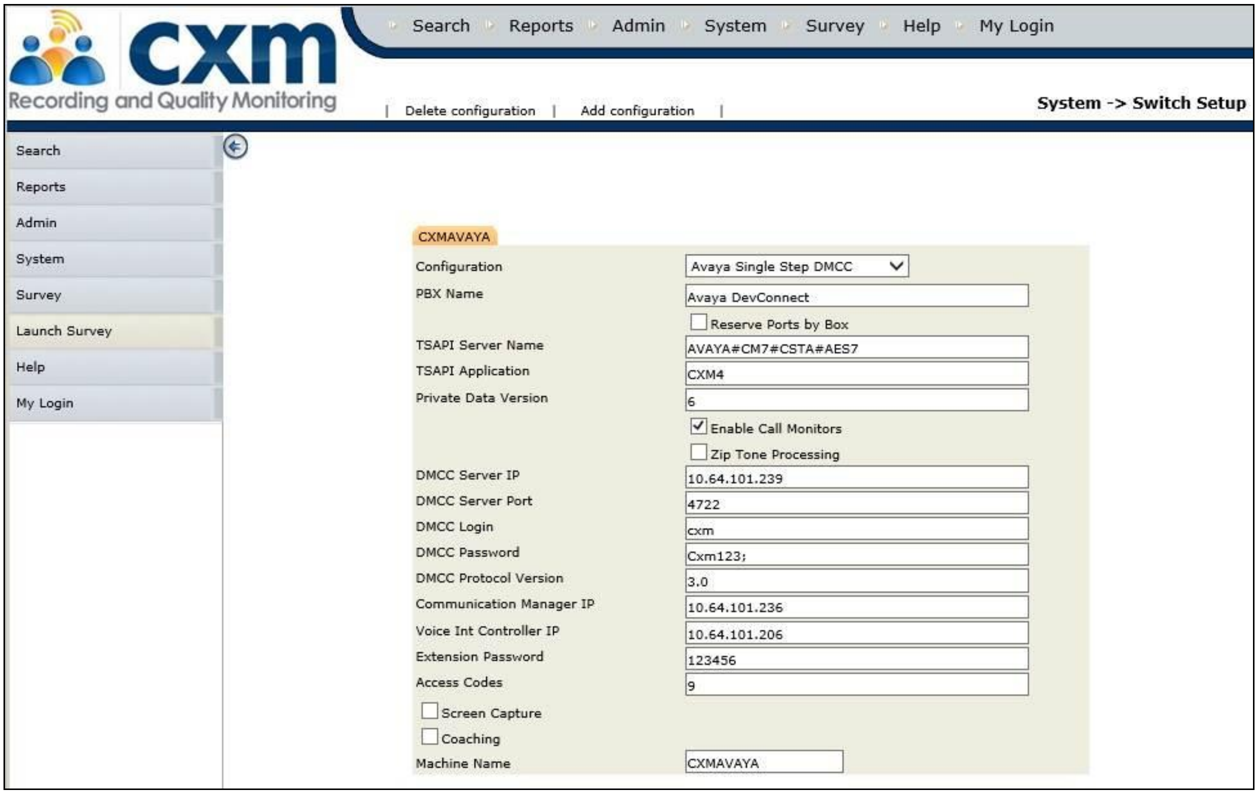
Access the CXM web-based interface by using the URL "http://ip-address/cxm" in an Internet Explorer browser window, where "ip-address" is the IP address of the CXM server. Note that only the Internet Explorer browser is supported by CXM. Log in using the appropriate credentials.



8.2. Administer Switch Setup

In the subsequent screen (not shown), select **System → Switch Setup** from the top menu to display the screen below. Enter the following values for the specified fields, and retain the default values in the remaining fields.

- **Configuration:** "Avaya Single Step DMCC"
- **PBX Name:** A desired name.
- **TSAPI Server Name:** The Tlink name from **Section 6.10**.
- **TSAPI Application:** A desired name.
- **Private Data Version:** "6"
- **Enable Call Monitors:** Check this field.
- **DMCC Server IP:** The IP address of Application Enablement Services.
- **DMCC Server Port:** The DMCC encrypted port from **Section 6.7**.
- **DMCC Login:** The CXM user credentials from **Section 6.5**.
- **DMCC Password:** The CXM user credentials from **Section 6.5**.
- **DMCC Protocol Version:** Retain the default value, with parameter not used by CXM.
- **Communication Manager IP:** The H.323 gatekeeper IP address from **Section 6.4**.
- **Voice Int Controller IP:** The IP address of the CXM server.
- **Extension Password:** The security code for the IP softphones from **Section 5.4**.
- **Access Codes:** The pertinent access code for the network, in this case "9".
- **Machine Name**: The computer name of the CXM server.



CXMAVAYA

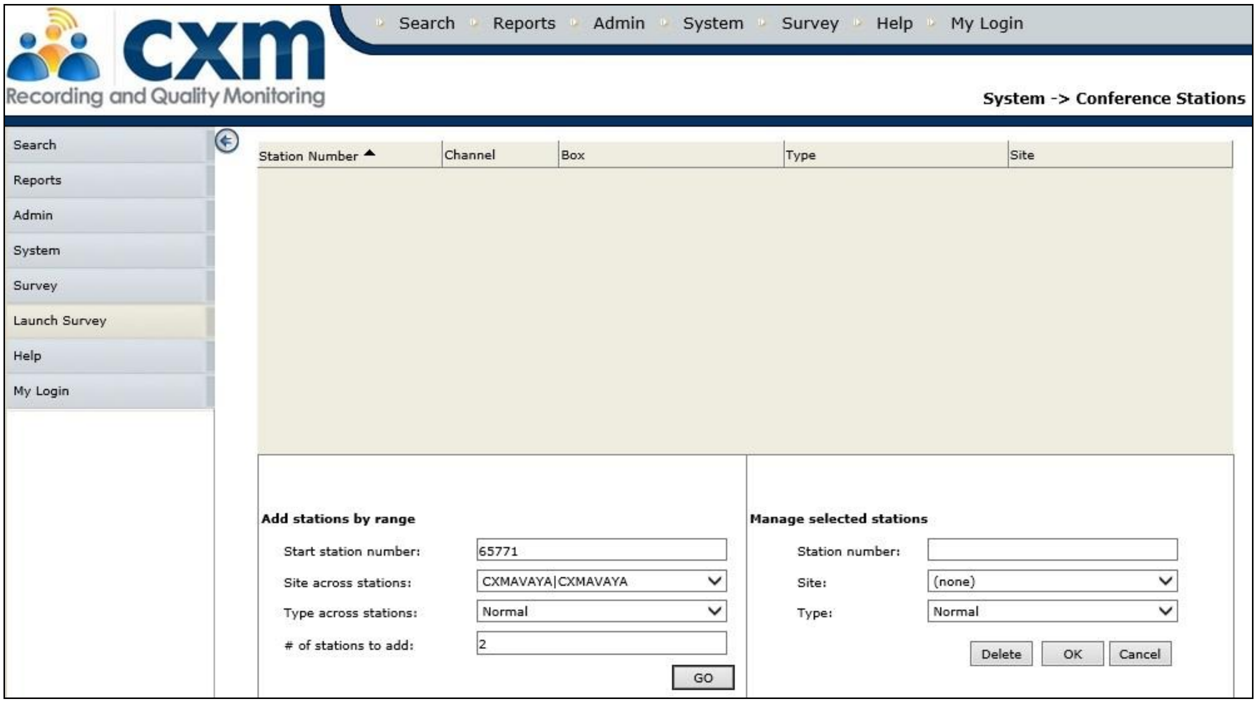
Configuration	Avaya Single Step DMCC
PBX Name	Avaya DevConnect
	□ Reserve Ports by Box
TSAPI Server Name	AVAYA#CM7#CSTA#AES7
TSAPI Application	CXM4
Private Data Version	6
	☑ Enable Call Monitors
	□ Zip Tone Processing
DMCC Server IP	10.64.101.239
DMCC Server Port	4722
DMCC Login	cxm
DMCC Password	Cxm123;
DMCC Protocol Version	3.0
Communication Manager IP	10.64.101.236
Voice Int Controller IP	10.64.101.206
Extension Password	123456
Access Codes	9
□ Screen Capture	
□ Coaching	
Machine Name	CXMAVAYA

8.3. Administer Conference Stations

Select **System → Conference Stations** from the top menu to display the screen below. Enter the following values for the specified fields, and retain the default values in the remaining fields.

- **Start station number:** The first virtual IP softphone extension from **Section 5.4**.
- **Site across stations:** Select the applicable pre-configured site.
- **Type across stations:** The desired type, in this case "Normal" for inbound and outbound.
- **# of stations to add:** The number of virtual IP softphones from **Section 5.4**.

In the case that the extensions of the virtual IP softphones are not sequential, then the conference stations can be added one at a time.



Station Number ▲	Channel	Box	Type	Site

Add stations by range

Start station number: 65771

Site across stations: CXMAVAYA|CXMAVAYA

Type across stations: Normal

# of stations to add: 2

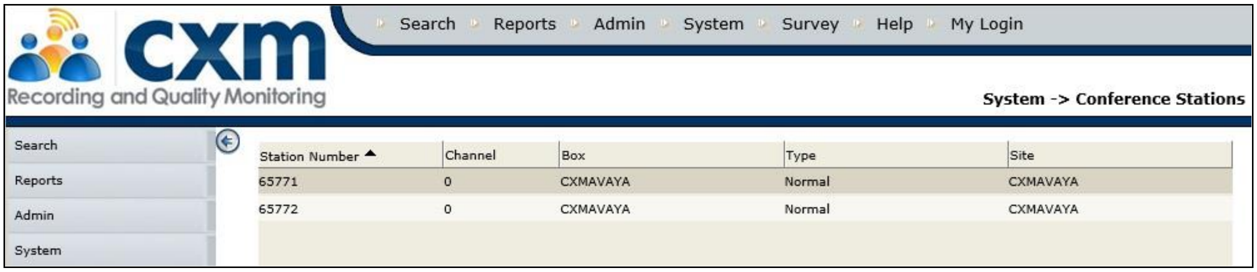
Manage selected stations

Station number:

Site: (none)

Type: Normal

In the compliance testing, two conference stations were configured, as shown below.

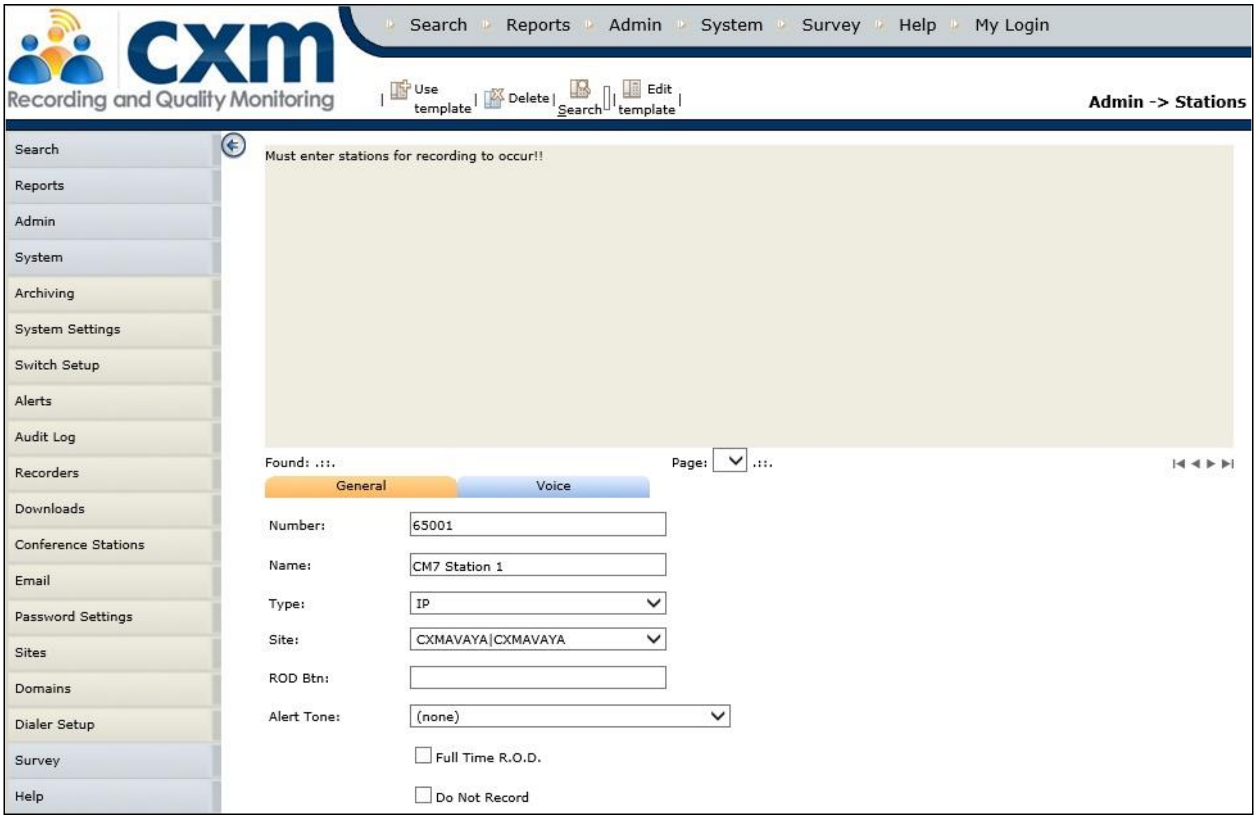


Station Number ▲	Channel	Box	Type	Site
65771	0	CXMAVAYA	Normal	CXMAVAYA
65772	0	CXMAVAYA	Normal	CXMAVAYA

8.4. Administer Stations

Select **Admin → Stations** from the top menu to display the screen below. Enter the following values for the specified fields, and retain the default values in the remaining fields.

- **Number:** The first agent station extension from **Section 5.7**.
- **Name:** The first agent station name from **Section 5.7**.
- **Type:** Select the applicable type for the first agent from **Section 5.7**, in this case "IP".
- **Site:** Select the applicable pre-configured site.
- **ROD Btn:** Parameter not applicable to this integration, and was set to blank in the testing.



Must enter stations for recording to occur!!

Number: 65001

Name: CM7 Station 1

Type: IP

Site: CXMAVAYA|CXMAVAYA

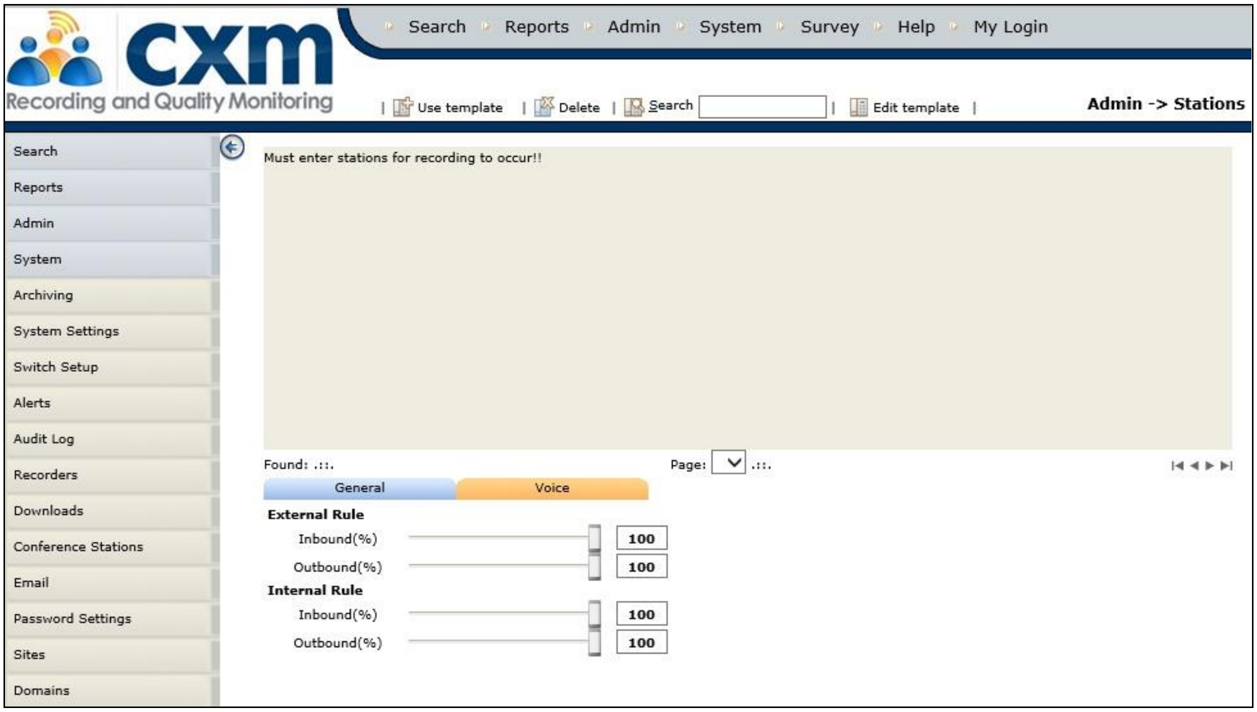
ROD Btn:

Alert Tone: (none)

☐ Full Time R.O.D.

☐ Do Not Record

Select the **Voice** tab in the bottom pane. Adjust the scroll bars to set the desired percentage for various types of calls to be recorded. In the compliance testing, the percentages were set to 100 for recording of all calls.



Must enter stations for recording to occur!!

External Rule

Inbound(%) 100

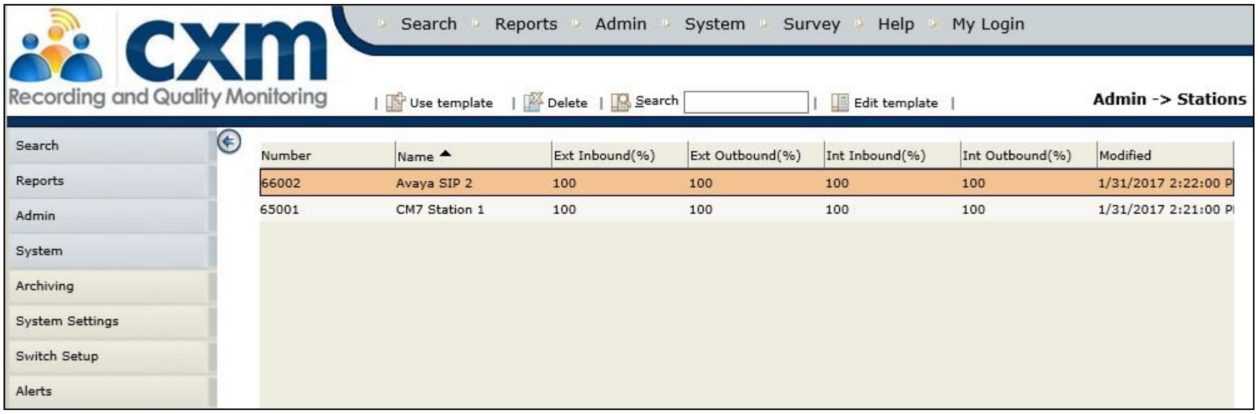
Outbound(%) 100

Internal Rule

Inbound(%) 100

Outbound(%) 100

Repeat this section to configure all agent stations from **Section 5.7**. In the compliance testing, two agent stations were configured, as shown below.

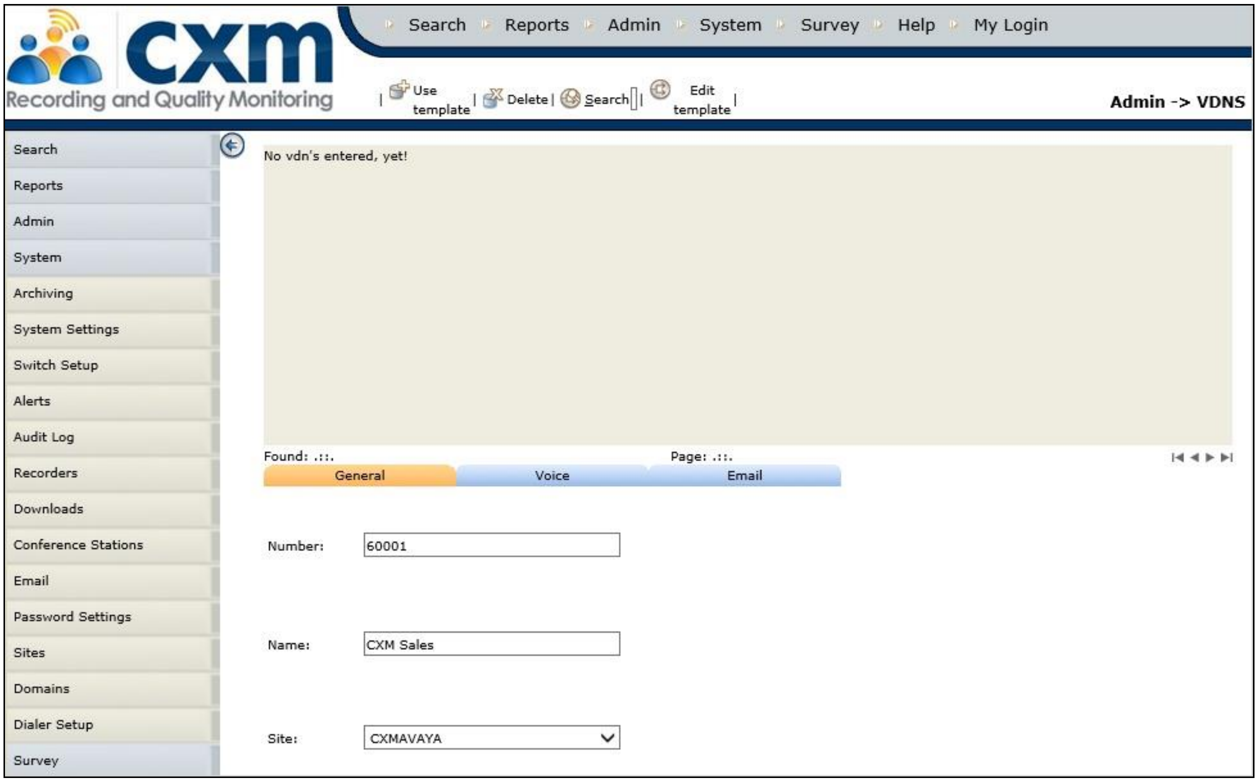


Number	Name ▲	Ext Inbound(%)	Ext Outbound(%)	Int Inbound(%)	Int Outbound(%)	Modified
66002	Avaya SIP 2	100	100	100	100	1/31/2017 2:22:00 P
65001	CM7 Station 1	100	100	100	100	1/31/2017 2:21:00 P

8.5. Administer VDNs

Select **Admin → VDNS** from the top menu to display the screen below. Enter the following values for the specified fields, and retain the default values in the remaining fields.

- **Number:** The first VDN extension from **Section 5.5**.
- **Name:** The first VDN name from **Section 5.5**.
- **Site:** Select the applicable pre-configured site.



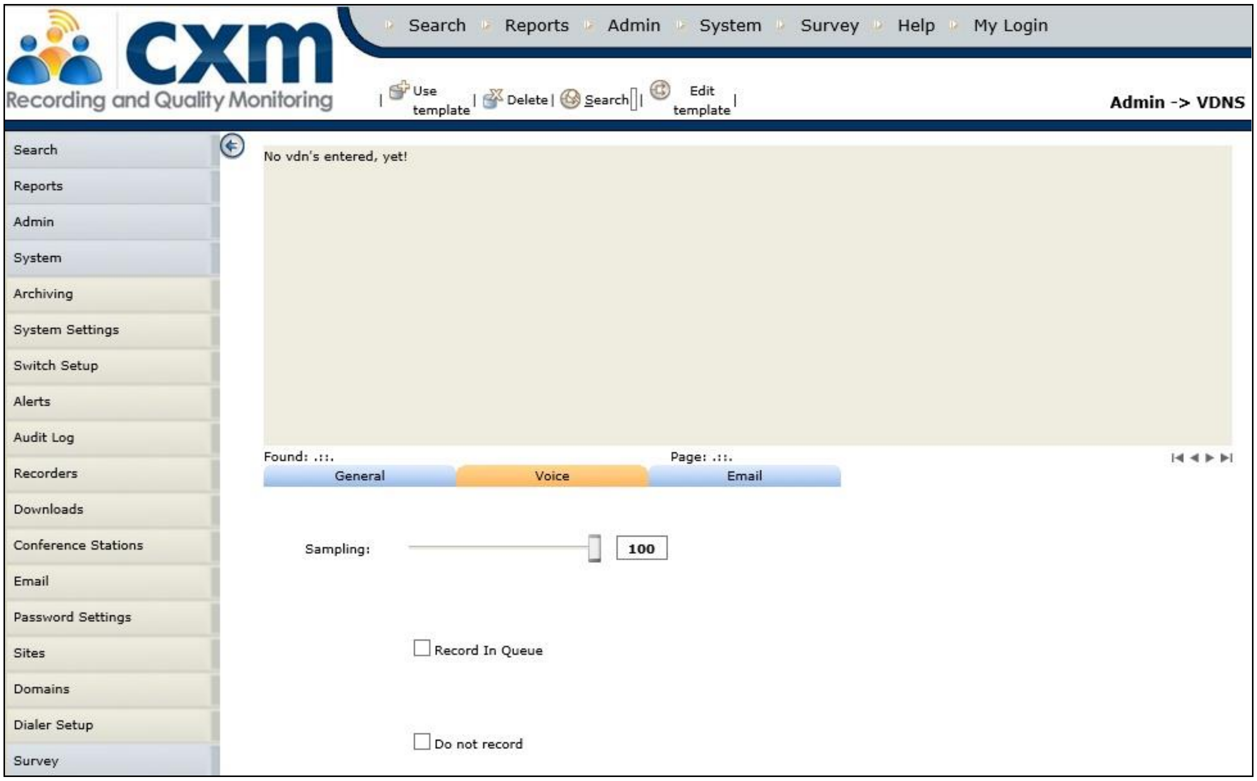
No vdn's entered, yet!

Number: 60001

Name: CXM Sales

Site: CXMAVAYA

Select the **Voice** tab in the bottom pane. Adjust the scroll bar to set the desired percentage of calls to be recorded. In the compliance testing, the percentage was set to 100 for recording of all calls.



No vdn's entered, yet!

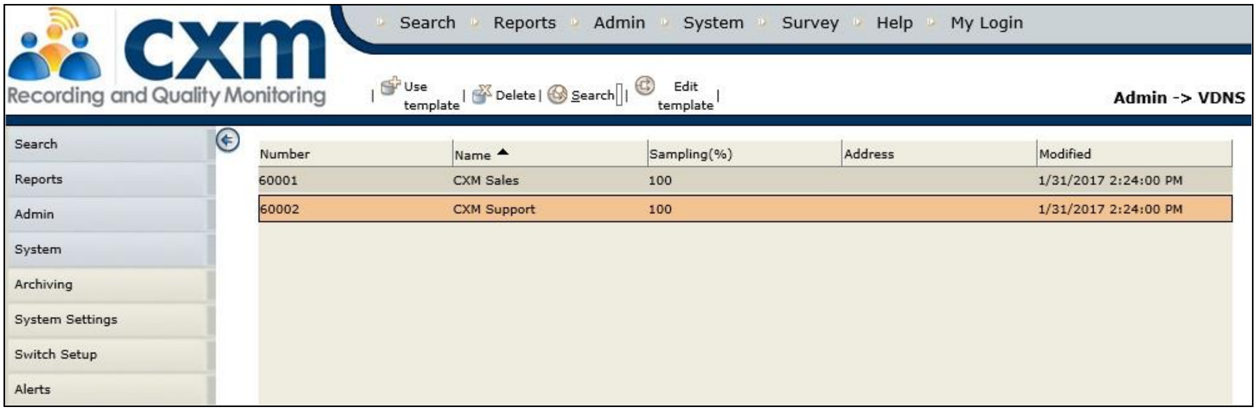
Found: .::. Page: .::.

Sampling: 100

□ Record In Queue

□ Do not record

Repeat this section to configure all VDNs from **Section 5.5**. In the compliance testing, two VDNs were configured, as shown below.



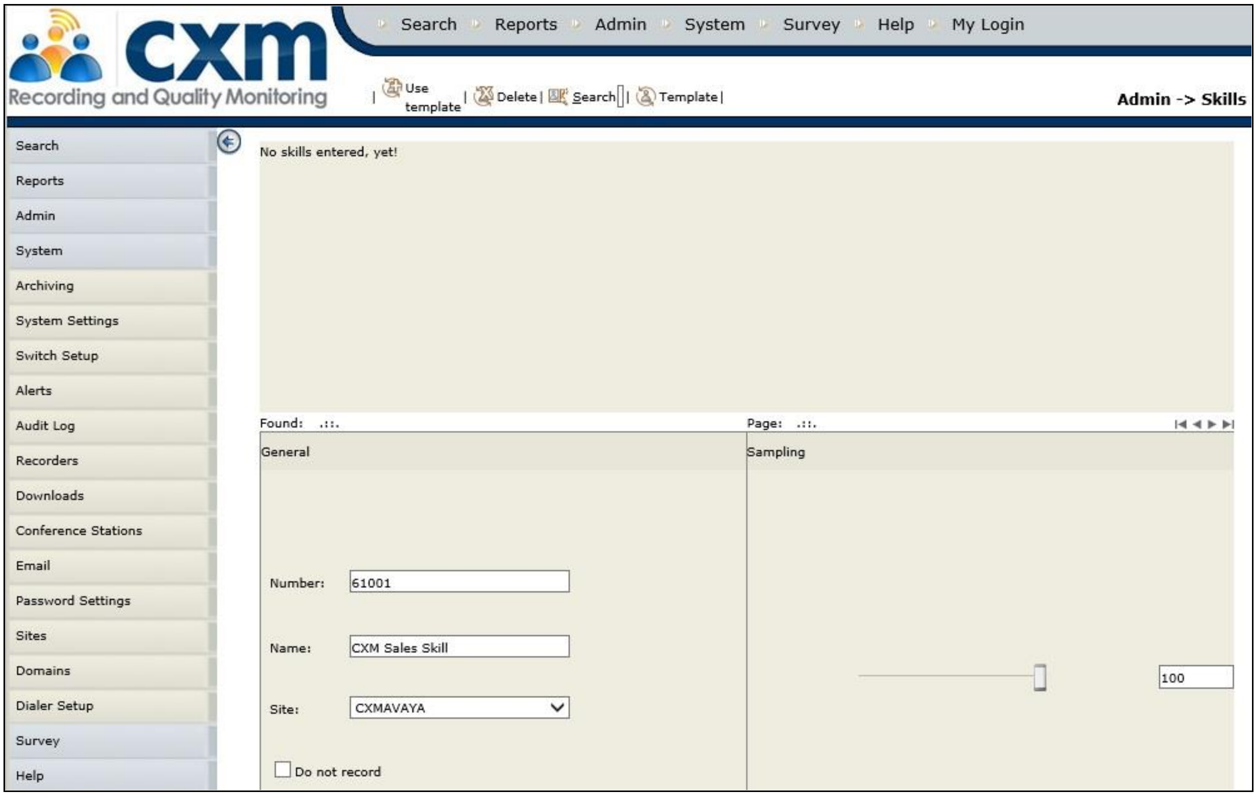
Number	Name ▲	Sampling(%)	Address	Modified
60001	CXM Sales	100		1/31/2017 2:24:00 PM
60002	CXM Support	100		1/31/2017 2:24:00 PM

8.6. Administer Skills

Select **Admin → Skills** from the top menu to display the screen below. Enter the following values for the specified fields, and retain the default values in the remaining fields.

- **Number:** The first skill group extension from **Section 5.6**.
- **Name:** The first skill group name from **Section 5.6**.
- **Site:** Select the applicable pre-configured site.

For **Sampling**, adjust the scroll bar to set the desired percentage of calls to be recorded. In the compliance testing, the percentage was set to 100 for recording of all calls.



No skills entered, yet!

Number: 61001

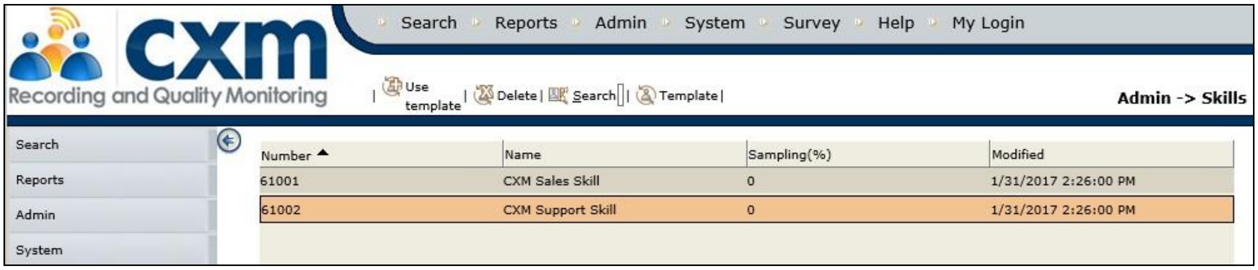
Name: CXM Sales Skill

Site: CXMAVAYA

Sampling: 100

□ Do not record

Repeat this section to configure all skill groups from **Section 5.6**. In the compliance testing, two skill groups were configured, as shown below.

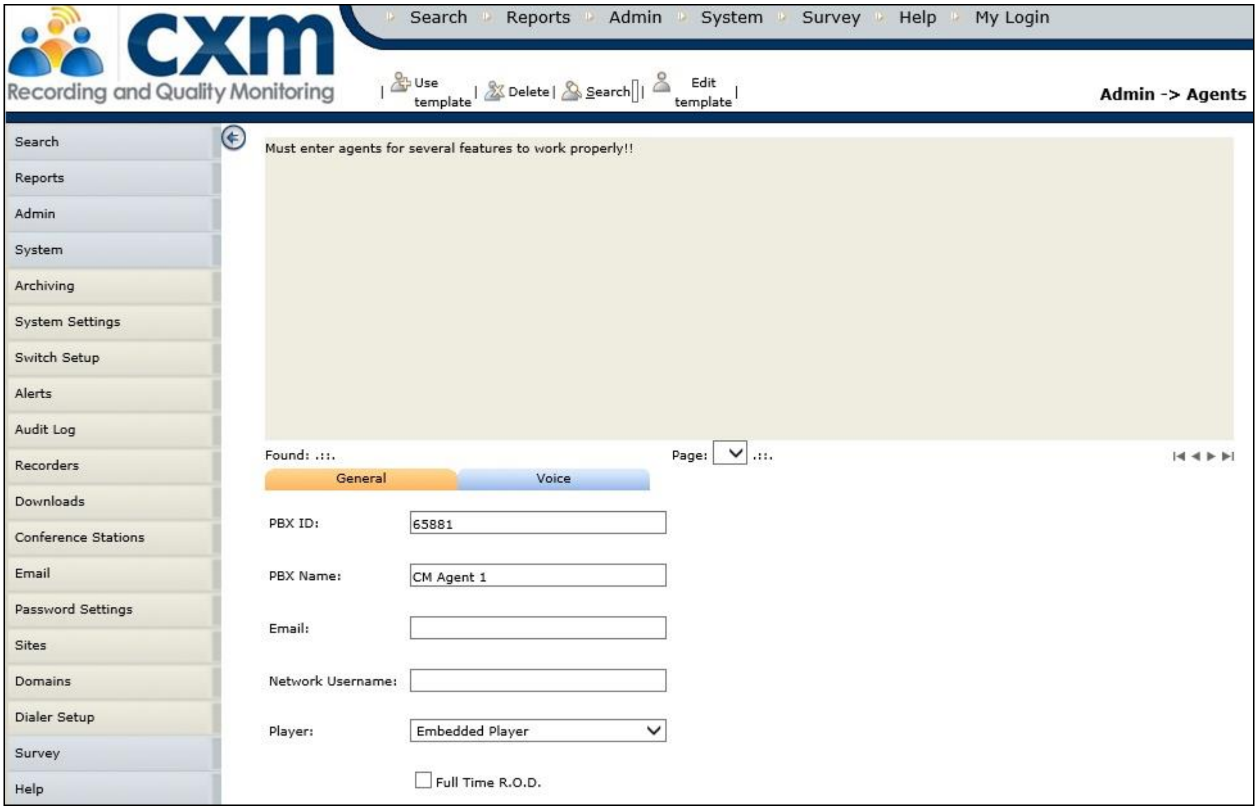


Number ▲	Name	Sampling(%)	Modified
61001	CXM Sales Skill	0	1/31/2017 2:26:00 PM
61002	CXM Support Skill	0	1/31/2017 2:26:00 PM

8.7. Administer Agents

Select **Admin → Agents** from the top menu to display the screen below. Enter the following values for the specified fields, and retain the default values in the remaining fields.

- **PBX ID:** The first agent login ID from **Section 5.8**.
- **PBX Name:** The first agent name from **Section 5.8**.



Must enter agents for several features to work properly!!

PBX ID: 65881

PBX Name: CM Agent 1

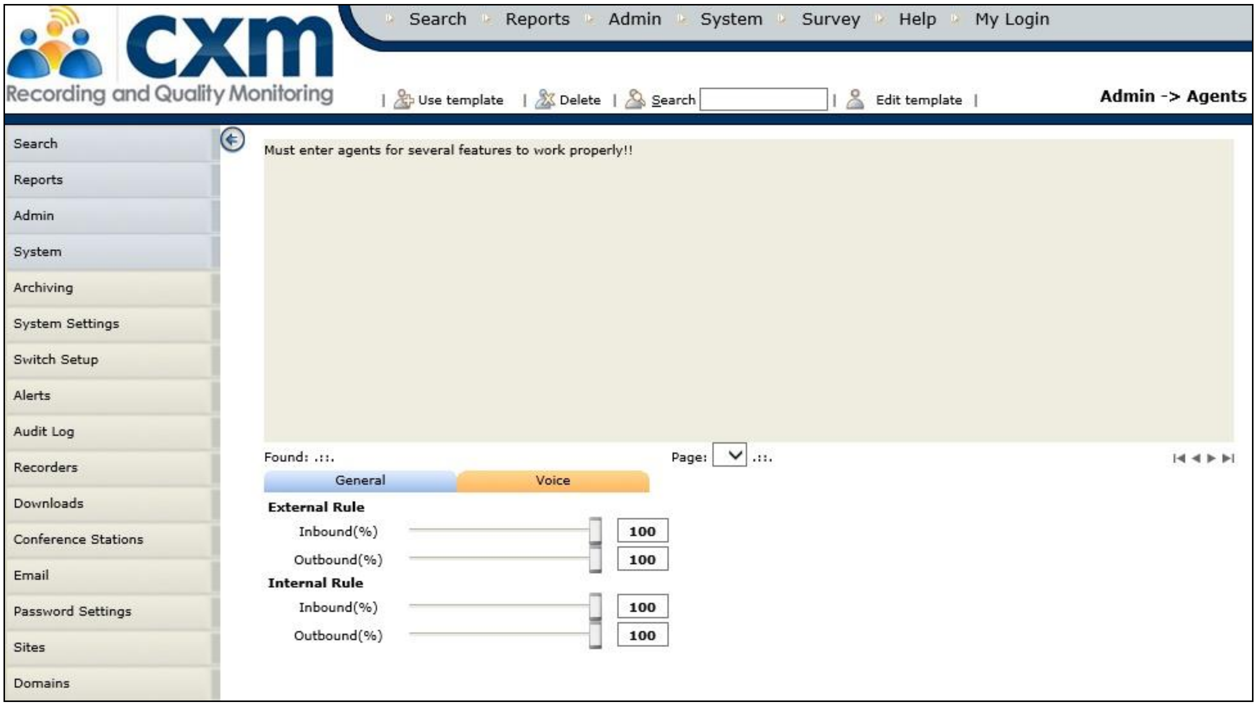
Email:

Network Username:

Player: Embedded Player

□ Full Time R.O.D.

Select the **Voice** tab in the bottom pane. Adjust the scroll bars to set the desired percentage for various types of calls to be recorded. In the compliance testing, the percentages were set to 100 for recording of all calls.



Must enter agents for several features to work properly!!

External Rule

Inbound(%) 100

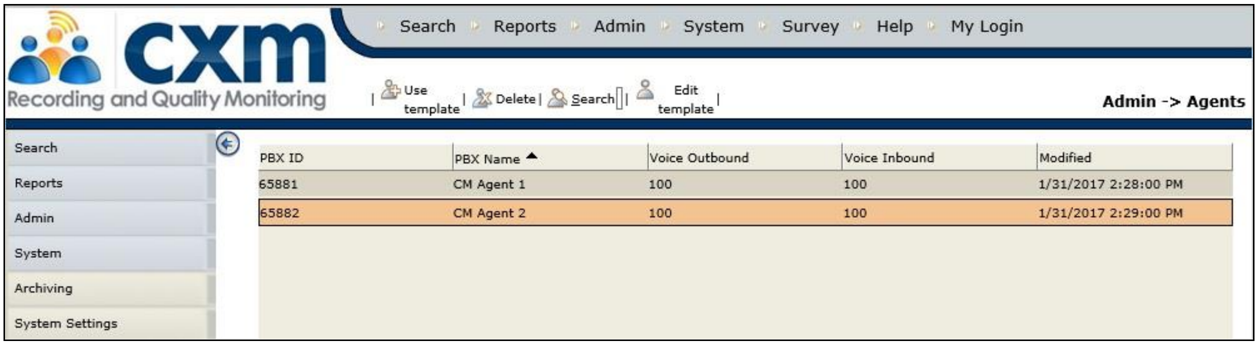
Outbound(%) 100

Internal Rule

Inbound(%) 100

Outbound(%) 100

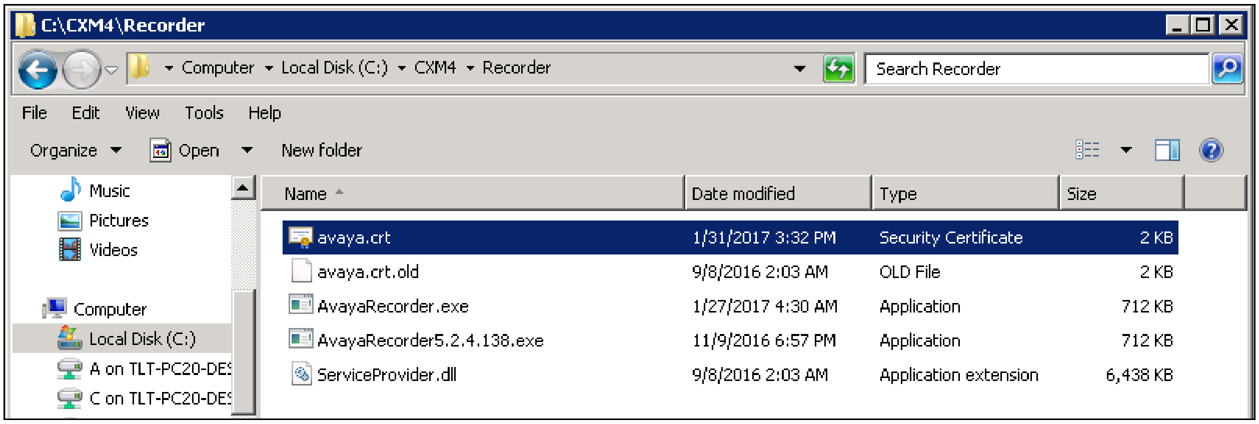
Repeat this section to configure all agents from **Section 5.8**. In the compliance testing, two agents were configured, as shown below.



PBX ID	PBX Name ▲	Voice Outbound	Voice Inbound	Modified
65881	CM Agent 1	100	100	1/31/2017 2:28:00 PM
65882	CM Agent 2	100	100	1/31/2017 2:29:00 PM

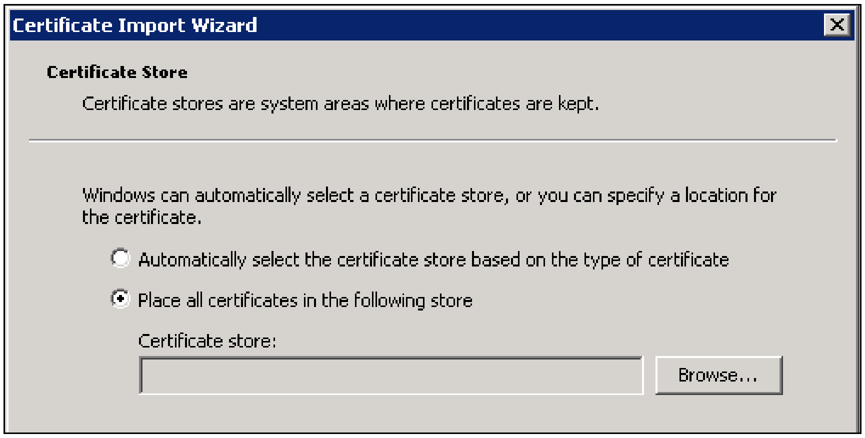
8.8. Install CA Certificate

From the CXM server, navigate to **C:\CXM4\Recorder**, and place the CA certificate **avaya.crt** from **Section 6.11** under this directory. Double click on **avaya.crt** to install the certificate.



Name	Date modified	Type	Size
avaya.crt	1/31/2017 3:32 PM	Security Certificate	2 KB
avaya.crt.old	9/8/2016 2:03 AM	OLD File	2 KB
AvayaRecorder.exe	1/27/2017 4:30 AM	Application	712 KB
AvayaRecorder5.2.4.138.exe	11/9/2016 6:57 PM	Application	712 KB
ServiceProvider.dll	9/8/2016 2:03 AM	Application extension	6,438 KB

When the **Certificate Import Wizard** screen below is displayed, select **Place all certificates in the following store**, and click **Browse**.



Certificate Store

Certificate stores are system areas where certificates are kept.

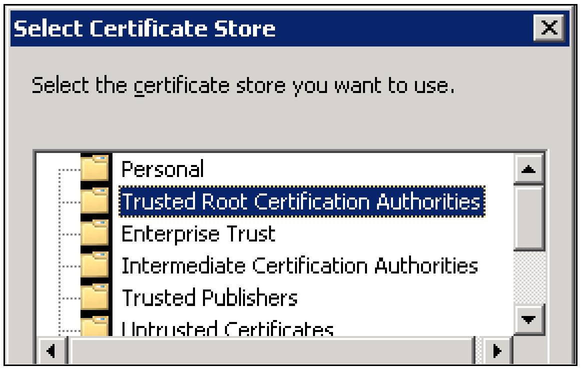
Windows can automatically select a certificate store, or you can specify a location for the certificate.

○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

Certificate store:

In the **Select Certificate Store** pop-up box, select **Trusted Root Certification Authorities**, as shown below. Proceed to complete the certificate installation.

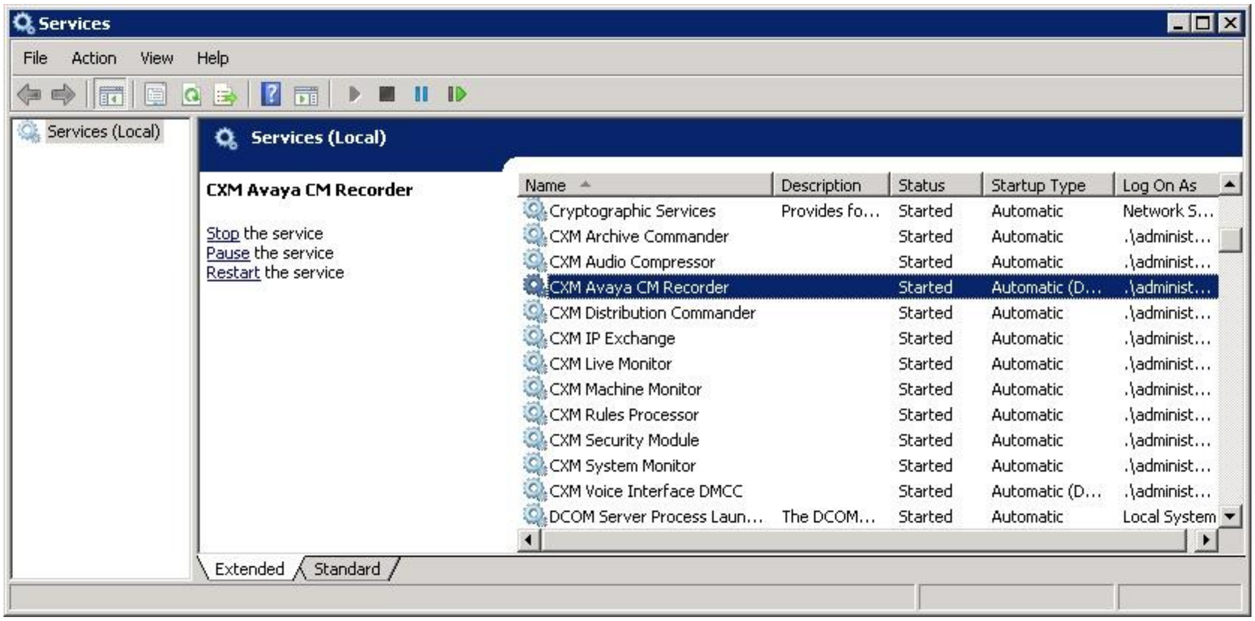


Select the certificate store you want to use.

- Personal
- Trusted Root Certification Authorities
- Enterprise Trust
- Intermediate Certification Authorities
- Trusted Publishers
- Untrusted Certificates

8.9. Administer CXM Services

From the CXM server, select **Start → Administrative Tools → Services** to display the **Services** screen. Change the **Startup Type** of each CXM service to "Automatic", and start the service, as shown below.



CXM Avaya CM Recorder

Stop the service
Pause the service
Restart the service

Name	Description	Status	Startup Type	Log On As
Cryptographic Services	Provides fo...	Started	Automatic	Network S...
CXM Archive Commander		Started	Automatic	.\administ...
CXM Audio Compressor		Started	Automatic	.\administ...
CXM Avaya CM Recorder		Started	Automatic (D...	.\administ...
CXM Distribution Commander		Started	Automatic	.\administ...
CXM IP Exchange		Started	Automatic	.\administ...
CXM Live Monitor		Started	Automatic	.\administ...
CXM Machine Monitor		Started	Automatic	.\administ...
CXM Rules Processor		Started	Automatic	.\administ...
CXM Security Module		Started	Automatic	.\administ...
CXM System Monitor		Started	Automatic	.\administ...
CXM Voice Interface DMCC		Started	Automatic (D...	.\administ...
DCOM Server Process Laun...	The DCOM...	Started	Automatic	Local System

9. Verification Steps

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

9.1. 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    72       28
```

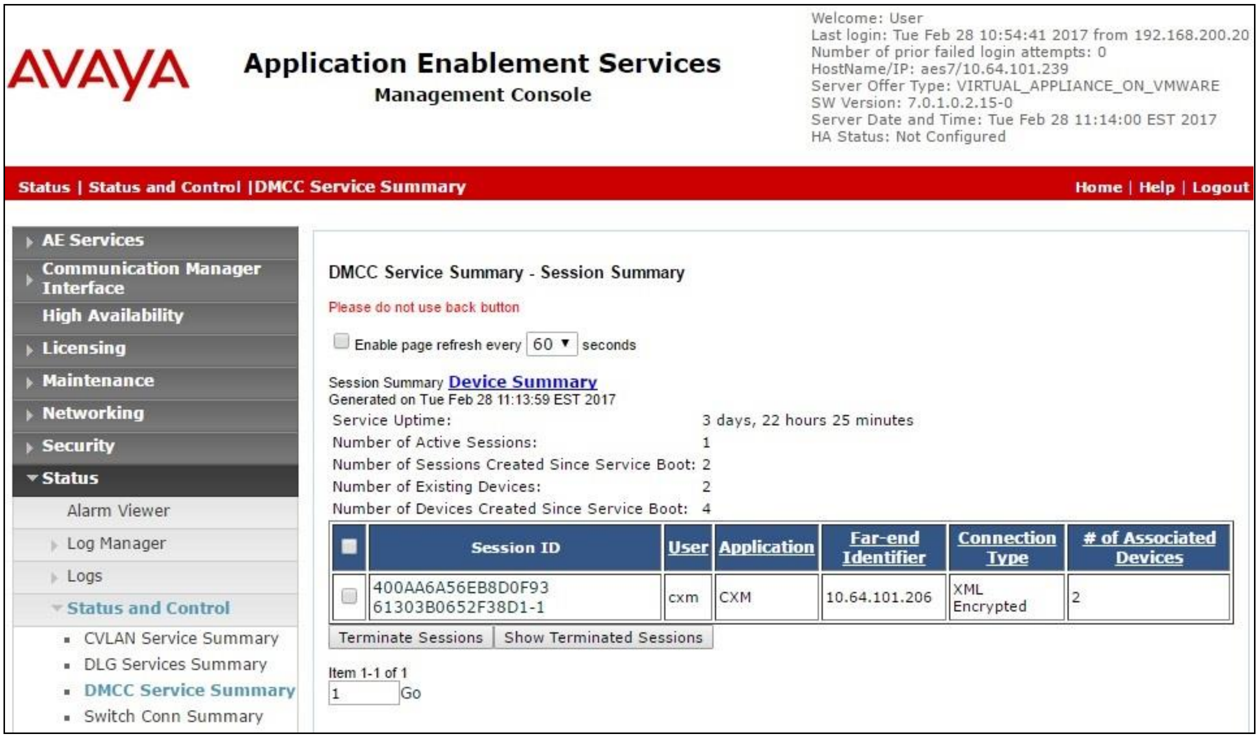
Verify the registration status of the virtual IP softphones by using the “list registered-ip-stations” command. Verify that all virtual IP softphone extensions from **Section 5.4** are displayed along with the IP address of the Application Enablement Services server, as shown below.

```
list registered-ip-stations

                            REGISTERED IP STATIONS

Station Ext    Set Type/ Prod ID/       Station IP Address/
or Orig Port   Net Rgn   Release    Skt Gatekeeper IP Address
------------- --------- ---------- --- ---------------------------------------
65000          9641      IP_Phone   tls 192.168.200.106
               1         6.6302         10.64.101.236
65001          9611      IP_Phone   tls 192.168.200.104
               1         6.6302         10.64.101.236
65771          4620      IP_API_A   tcp 10.64.101.239
               1         3.2040         10.64.101.236
65772          4620      IP_API_A   tcp 10.64.101.239
               1         3.2040         10.64.101.236
```

9.2. Verify Avaya Aura® Application Enablement Services

On Application Enablement Services, verify the status of the DMCC service by selecting **Status → Status and Control → DMCC Service Summary** from the left pane. The **DMCC Service Summary – Session Summary** screen is displayed.

Verify the **User** column shows an active session with the CXM user name from **Section 6.5**, and that the **# of Associated Devices** column reflects the total number of virtual IP softphones from **Section 5.4**.



Welcome: User
Last login: Tue Feb 28 10:54:41 2017 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: 7.0.1.0.2.15-0
Server Date and Time: Tue Feb 28 11:14:00 EST 2017
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 Tue Feb 28 11:13:59 EST 2017

Service Uptime:	3 days, 22 hours 25 minutes
Number of Active Sessions:	1
Number of Sessions Created Since Service Boot:	2
Number of Existing Devices:	2
Number of Devices Created Since Service Boot:	4

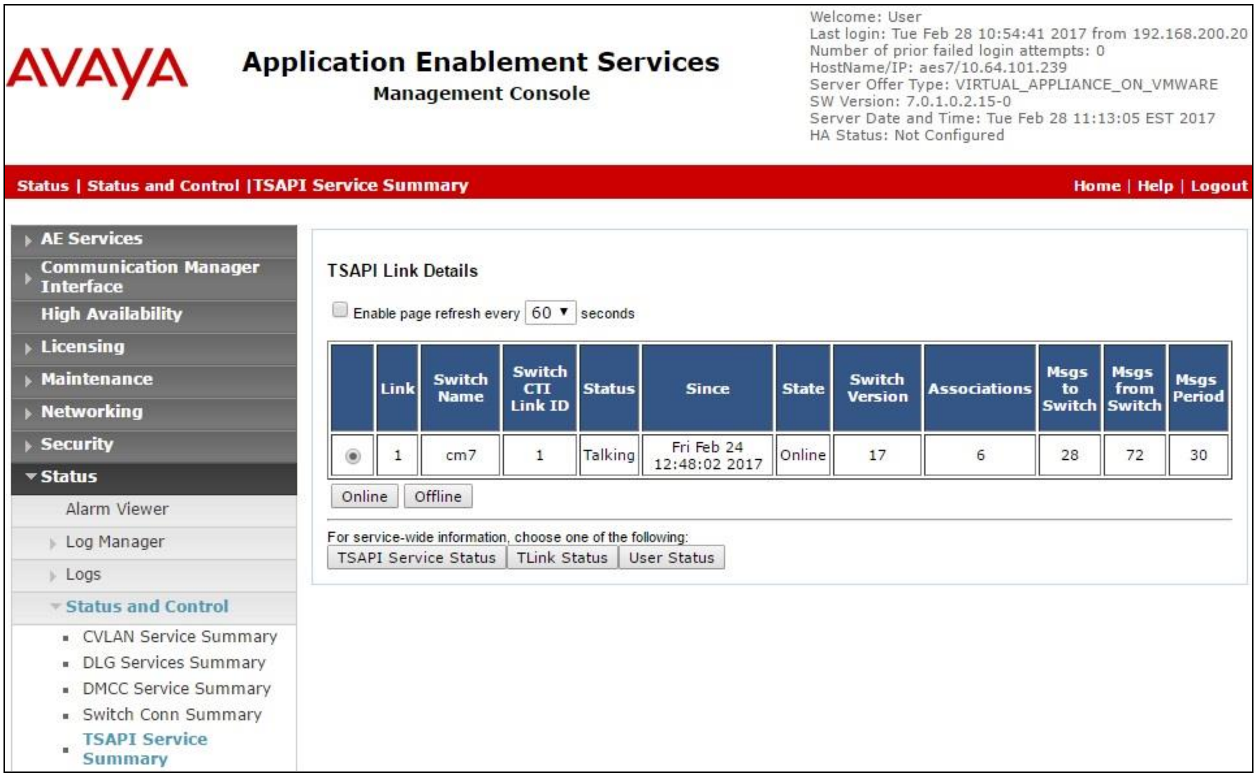
□	Session ID	User	Application	Far-end Identifier	Connection Type	# of Associated Devices
□	400AA6A56EB8D0F93 61303B0652F38D1-1	cxm	CXM	10.64.101.206	XML Encrypted	2

Terminate Sessions | Show Terminated Sessions

Item 1-1 of 1
1 Go

Verify the status of the TSAPI service by selecting **Status → Status and Control → TSAPI Service Summary** from the left pane. The **TSAPI Link Details** screen is displayed.

Verify the **Status** is "Talking" for the TSAPI link administered in **Section 6.3**, and that the **Associations** column reflects the total number of monitored VDNs, skill groups, and agent stations from **Section 3**.



Welcome: User
Last login: Tue Feb 28 10:54:41 2017 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: 7.0.1.0.2.15-0
Server Date and Time: Tue Feb 28 11:13:05 EST 2017
HA Status: Not Configured

TSAPI Link Details

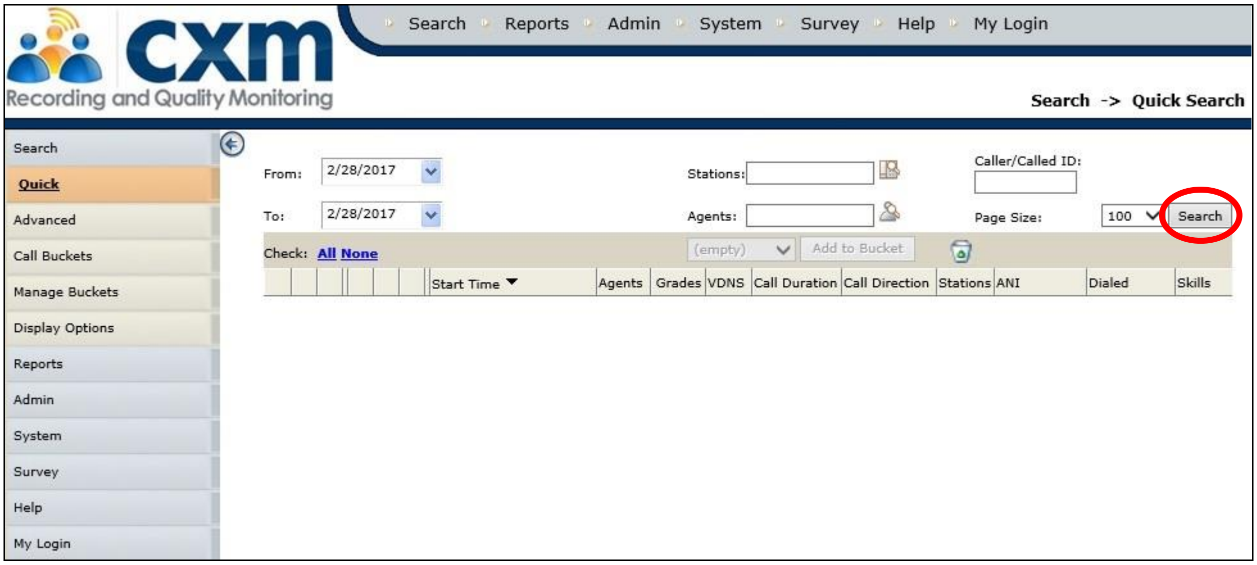
□ Enable page refresh every 60 ▾ seconds

	Link	Switch Name	Switch CTI Link ID	Status	Since	State	Switch Version	Associations	Msgs to Switch	Msgs from Switch	Msgs Period
●	1	cm7	1	Talking	Fri Feb 24 12:48:02 2017	Online	17	6	28	72	30

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

9.3. Verify Co-nexus CXM

Log an agent into the skill group to handle and complete an ACD call. Follow the procedures in **Section 8.1** to launch the web interface and log in using the appropriate credentials. The screen below is displayed. Click on **Search** to display a list of call recording entries for the current day.



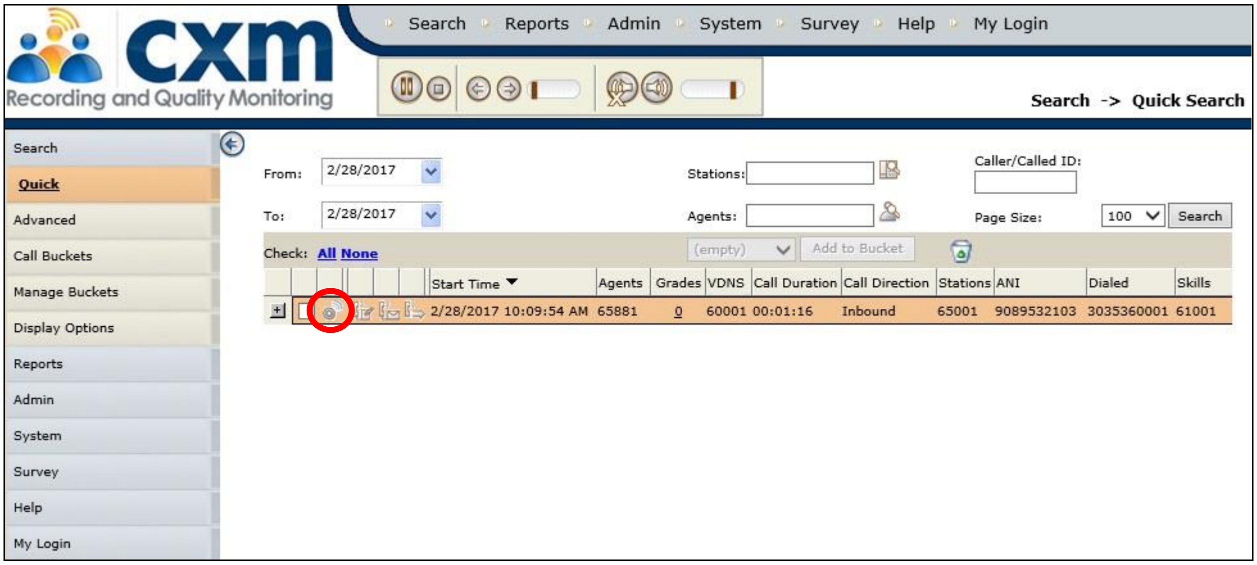
From: 2/28/2017

To: 2/28/2017

Page Size: 100

Start Time	Agents	Grades	VDNS	Call Duration	Call Direction	Stations	ANI	Dialed	Skills

The screen is updated as shown below. Verify that there is an entry reflecting the last call, with proper values in the relevant fields. Click on the associated **Listen to call** icon, and verify that the recording can be played back.



From: 2/28/2017

To: 2/28/2017

Page Size: 100

Start Time	Agents	Grades	VDNS	Call Duration	Call Direction	Stations	ANI	Dialed	Skills
2/28/2017 10:09:54 AM	65881	0	60001	00:01:16	Inbound	65001	9089532103	3035360001	61001

10. Conclusions

These Application Notes describe the configuration steps required for CXM 5.2 to successfully interoperate with Avaya Aura® Communication Manager 7.0 and Avaya Aura® Application Enablement Services 7.0. All feature and serviceability test cases were completed with observations noted in **Section 2.2**.

11. Additional References

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

1. *Administering Avaya Aura® Communication Manager*, Release 7.0.1, Issue 2.1, August 2016, available at http://support.avaya.com.

2. *Administering and Maintaining Aura® Application Enablement Services*, Release 7.0.1, Issue 2, August 2016, available at http://support.avaya.com.

3. *CXM Recording and Quality Monitoring Administration Guide*, Release 5.0, available from Co-nexus Support.

©2017 Avaya Inc. All Rights Reserved.
Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

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