Avaya Solution & Interoperability Test Lab

Application Notes for TeleComp CXM 6.1 with Avaya Aura® Communication Manager 8.1 and Avaya Aura® Application Enablement Services 8.1 – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for TeleComp CXM 6.1.5.1 to interoperate with Avaya Aura® Communication Manager 8.1.3 and Avaya Aura® Application Enablement Services 8.1.3. TeleComp CXM is a call recording solution.

In the compliance testing, TeleComp CXM used the Telephony Services Application Programming Interface and Device, Media, and Call Control interface from Avaya Aura® Application Enablement Services to monitor call center devices on Avaya Aura® Communication Manager, and to capture media associated with monitored agents for call recording 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 TeleComp CXM 6.1.5.1 to interoperate with Avaya Aura® Communication Manager 8.1.3 and Avaya Aura® Application Enablement Services 8.1.3. 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 Application Enablement Services to monitor call center devices on Communication Manager, and to capture media associated with monitored agents for call recording 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 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 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 recording.

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 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.

Avaya recommends our customers implement Avaya solutions using appropriate security and encryption capabilities enabled by our products. The testing referenced in these DevConnect Application Notes included the enablement of supported encryption capabilities in the Avaya products. Readers should consult the appropriate Avaya product documentation for further information regarding security and encryption capabilities supported by those Avaya products.

Support for these security and encryption capabilities in any non-Avaya solution component is the responsibility of each individual vendor. Readers should consult the appropriate vendor-supplied product documentation for more information regarding those products.

For testing associated with these Application Notes, the interfaces between Application Enablement Services and CXM included encrypted signaling and authentication for TSAPI and DMCC, and did not include encryption for the DMCC RTP, as requested by CXM.

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, G.711, forwarding, 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 verified. The following were observations on CXM from the compliance testing.

- The Dialed parameter in the Search Calls output only showed the first ten digits of the called number. In the compliance testing, the called number consisted of eleven digits with use of E.164 format, and only the first ten digits of the called number were shown.

- By design, for transfer and conference scenarios involving two agents, all associated recording entries reported both agent stations in the Stations parameter and both agent IDs in the Agents parameter.

- For transfer and conference scenarios involving agent and non-monitored supervisor, the remaining conversation between the supervisor and the PSTN is recorded in the conference scenarios but not in the transfer scenarios.

- For attended conference scenarios involving agent and non-monitored supervisor, one of the recording entries reported the agent station twice in the Stations parameter.

- After a busy out and release of the CTI link on Communication Manager, subsequent recording entries no longer reports the VDN number and name.

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 call 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 (H.323), 66002 (SIP)
Agent ID	65881, 65882

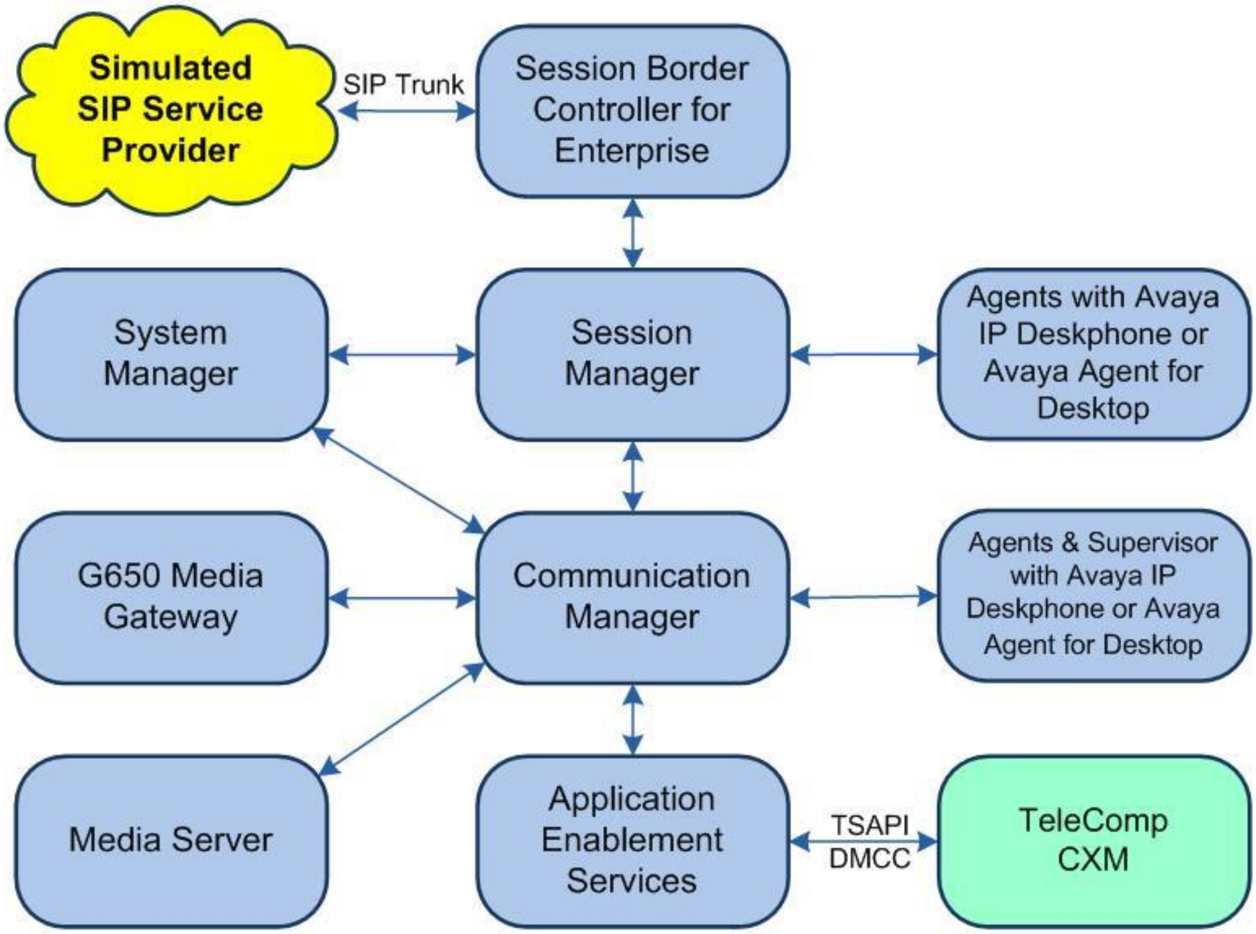

Simulated SIP Service Provider
SIP Trunk
Session Border Controller for Enterprise
System Manager
Session Manager
Agents with Avaya IP Deskphone or Avaya Agent for Desktop
G650 Media Gateway
Communication Manager
Agents & Supervisor with Avaya IP Deskphone or Avaya Agent for Desktop
Media Server
Application Enablement Services
TSAPI
DMCC
TeleComp CXM

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	8.1.3 (8.1.3.0.1.890.26685)
Avaya G650 Media Gateway	NA
Avaya Aura® Media Server in Virtual Environment	8.0.2.138
Avaya Aura® Application Enablement Services in Virtual Environment	8.1.3 (8.1.3.0.0.25-0)
Avaya Aura® Session Manager in Virtual Environment	8.1.3 (8.1.3.0.813014)
Avaya Aura® System Manager in Virtual Environment	8.1.3 (8.1.3.0.1012091)
Avaya Session Border Controller for Enterprise in Virtual Environment	8.1.2 (8.1.2.0-31-19809)
Avaya Agent for Desktop (H.323 & SIP)	2.0.6.0.10
Avaya 9611G & J179 IP Deskphone (H.323)	6.8502
Avaya J169 IP Deskphone (SIP)	4.0.7.1.5
TeleComp CXM on Windows Server 2012 • Avaya TSAPI Windows Client (csta32.dll) • Avaya DMCC .NET (ServiceProvider.dll)	6.1.5.1 R2 Standard 8.0.0.38 7.1.1.54

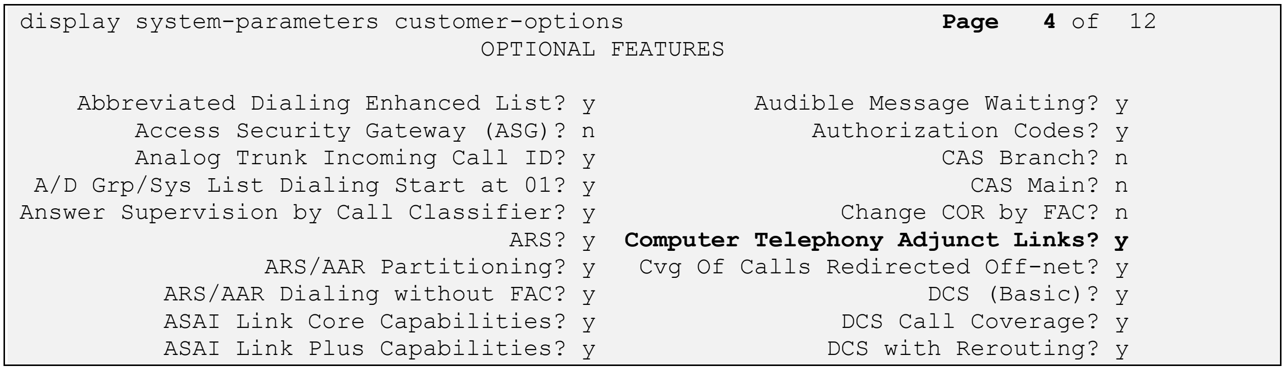
5. Configure Avaya Aura® Communication Manager

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

- Verify license
- Administer CTI link
- Administer IP codec set
- Administer system parameters features
- Administer virtual IP softphones

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.

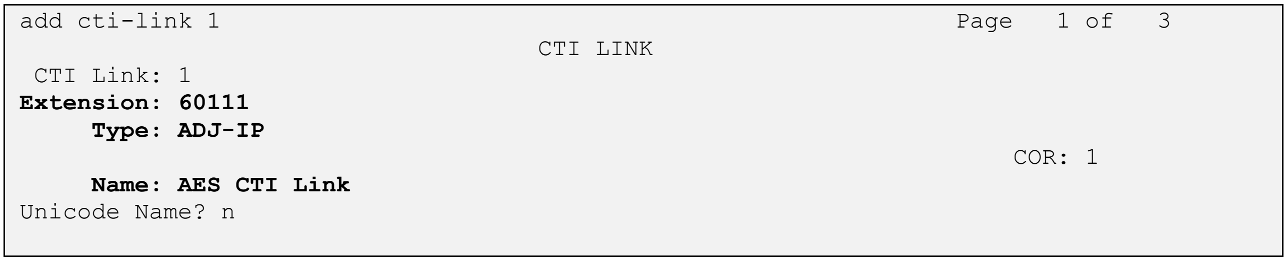


```
display system-parameters customer-options                    Page   4 of  12
                                OPTIONAL FEATURES

    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? y                      DCS (Basic)? y
          ASAI Link Core Capabilities? y                DCS Call Coverage? y
          ASAI Link Plus Capabilities? y               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.



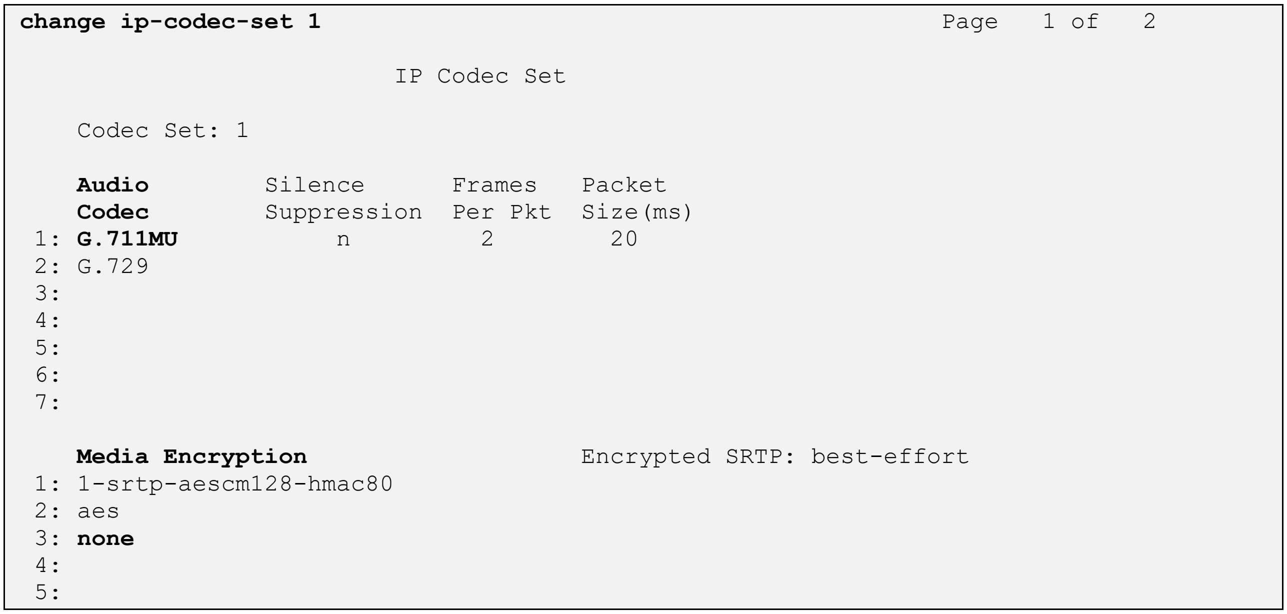
```
add cti-link 1                                                 Page   1 of   3
                                    CTI LINK
 CTI Link: 1
Extension: 60111
     Type: ADJ-IP
                                                                   COR: 1
     Name: AES CTI Link
Unicode Name? n
```

5.3. Administer IP Codec Set

Use the “change ip-codec-set n” command, where “n” is an existing codec set number to be used by the virtual IP softphones. For **Audio Codec**, make certain that variant of the G711 codec is configured, as shown below. Note that CXM only supports the G711 codec variants.

For **Media Encryption**, make certain that “none” is included.

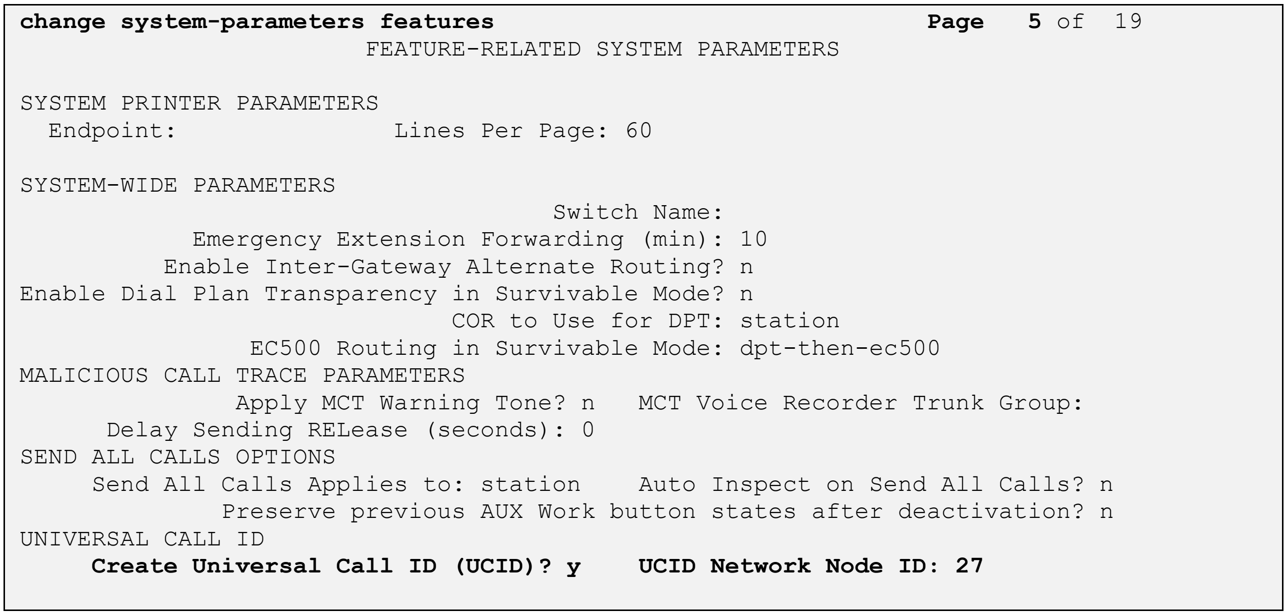
In the compliance testing, this codec was used by the virtual IP softphones and by the agent stations.



```
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
 3:
 4:
 5:
 6:
 7:

    Media Encryption                   Encrypted SRTP: best-effort
 1: 1-srtp-aescm128-hmac80
 2: aes
 3: none
 4:
 5:
```

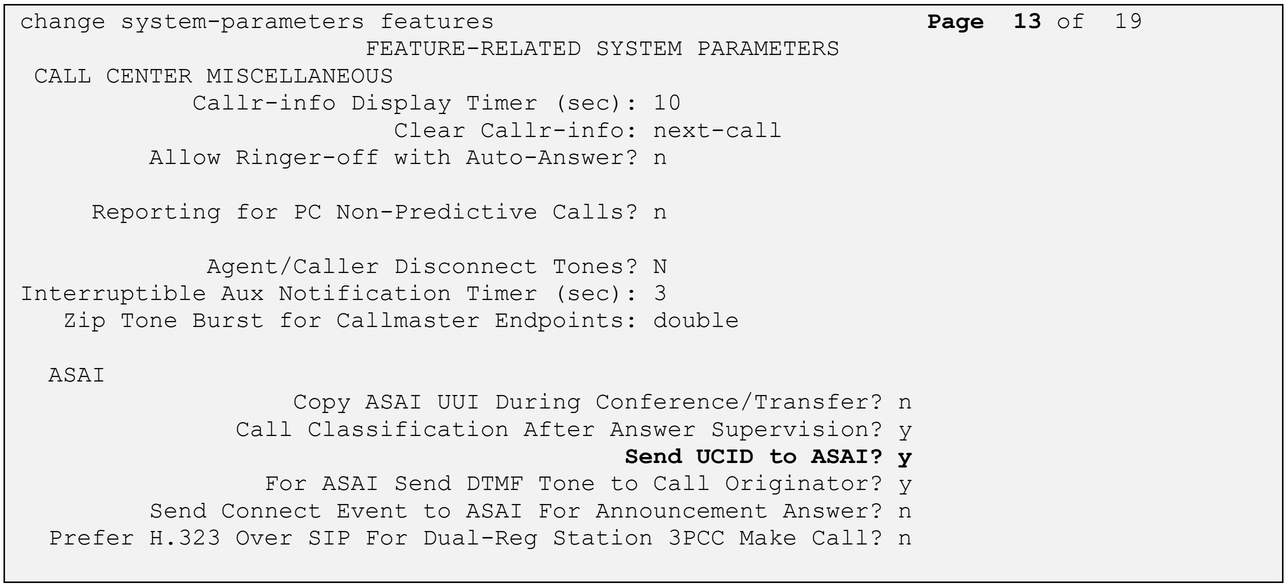
5.4. Administer System Parameters Features

Log into the System Access Terminal. 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  19
                        FEATURE-RELATED SYSTEM PARAMETERS
 CALL CENTER MISCELLANEOUS
            Callr-info Display Timer (sec): 10
                          Clear Callr-info: next-call
         Allow Ringer-off with Auto-Answer? n

     Reporting for PC Non-Predictive Calls? n

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

  ASAI
                   Copy ASAI UUI During Conference/Transfer? n
               Call Classification After Answer Supervision? 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
```

5.5. 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 security code.
- **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: CXM Virtual 1               Coverage Path 2:                 COS: 1
Unicode Name? n                     Hunt-to Station:                  Tests? y
STATION OPTIONS
                                           Time of Day Lock Table:
              Loss Group: 19       Personalized Ringing Pattern: 1
                                             Message Lamp Ext: 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

                                              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 65991 count 2

                                  STATIONS

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

65991            S000108 CXM Virtual 1                                 1
                 4620                      no                         1  1
65992            S000109 CXM Virtual 2                                  1
                 4620                      no                         1  1
```

6. Configure Avaya Aura® Application Enablement Services

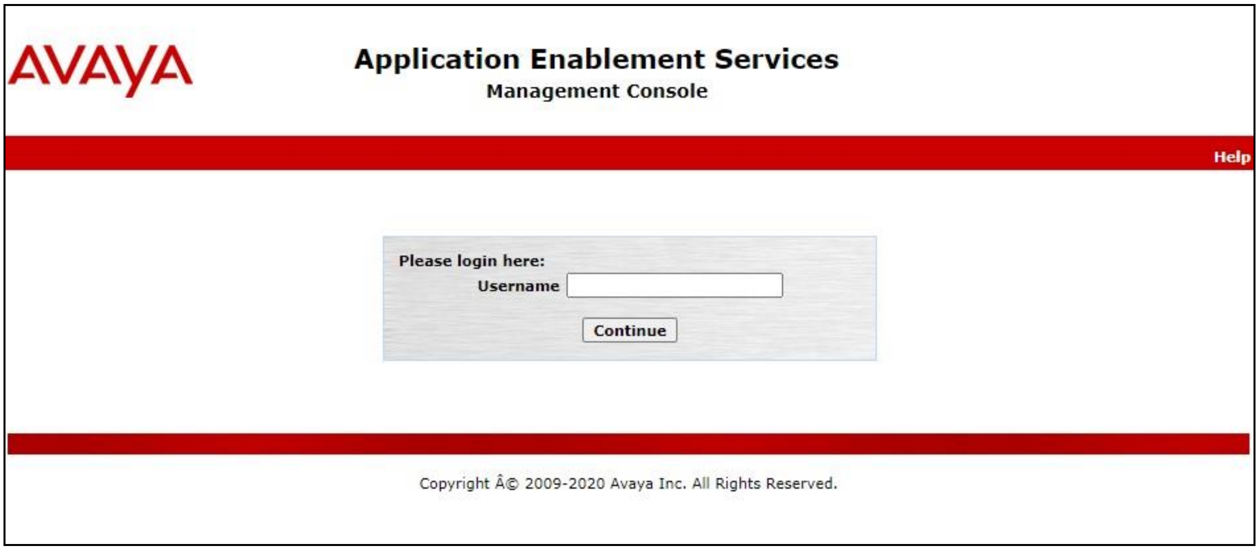
This section provides the procedures for configuring Application Enablement Services. The procedures include the following areas:

- Launch OAM interface
- Verify license
- Administer TSAPI link
- Administer H.323 gatekeeper
- Administer CXM user
- Administer security database
- Administer ports
- Restart service
- 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.

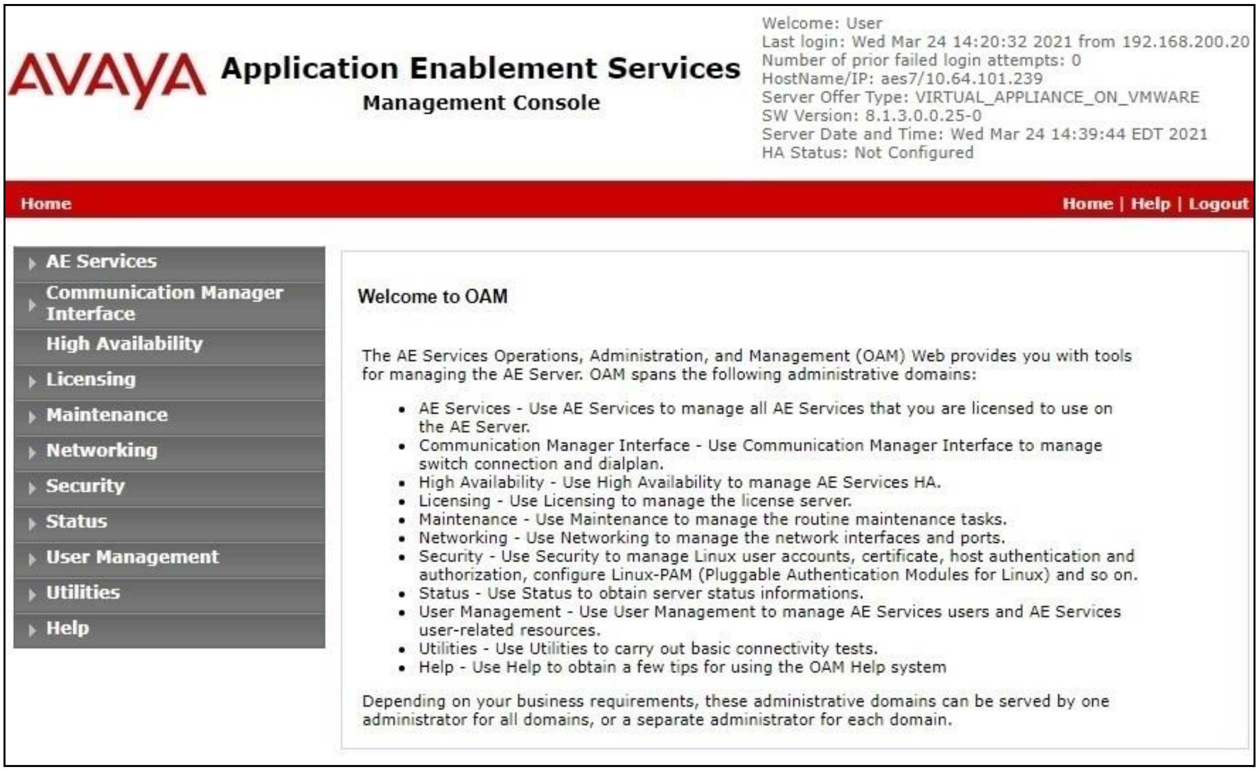


Application Enablement Services
Management Console

Please login here:
Username

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

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



Welcome: User
Last login: Wed Mar 24 14:20:32 2021 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: 8.1.3.0.0.25-0
Server Date and Time: Wed Mar 24 14:39:44 EDT 2021
HA Status: Not Configured

Welcome to OAM

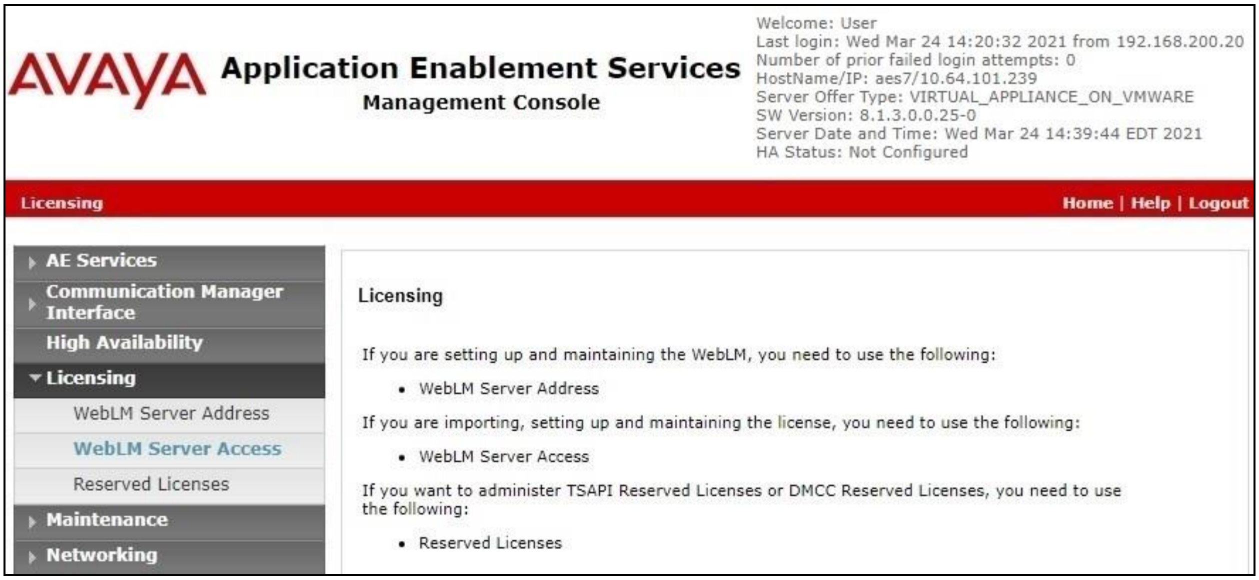
The AE Services Operations, Administration, and Management (OAM) Web provides you with tools for managing the AE Server. OAM spans the following administrative domains:

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

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

6.2. 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: Wed Mar 24 14:20:32 2021 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: 8.1.3.0.0.25-0
Server Date and Time: Wed Mar 24 14:39:44 EDT 2021
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:

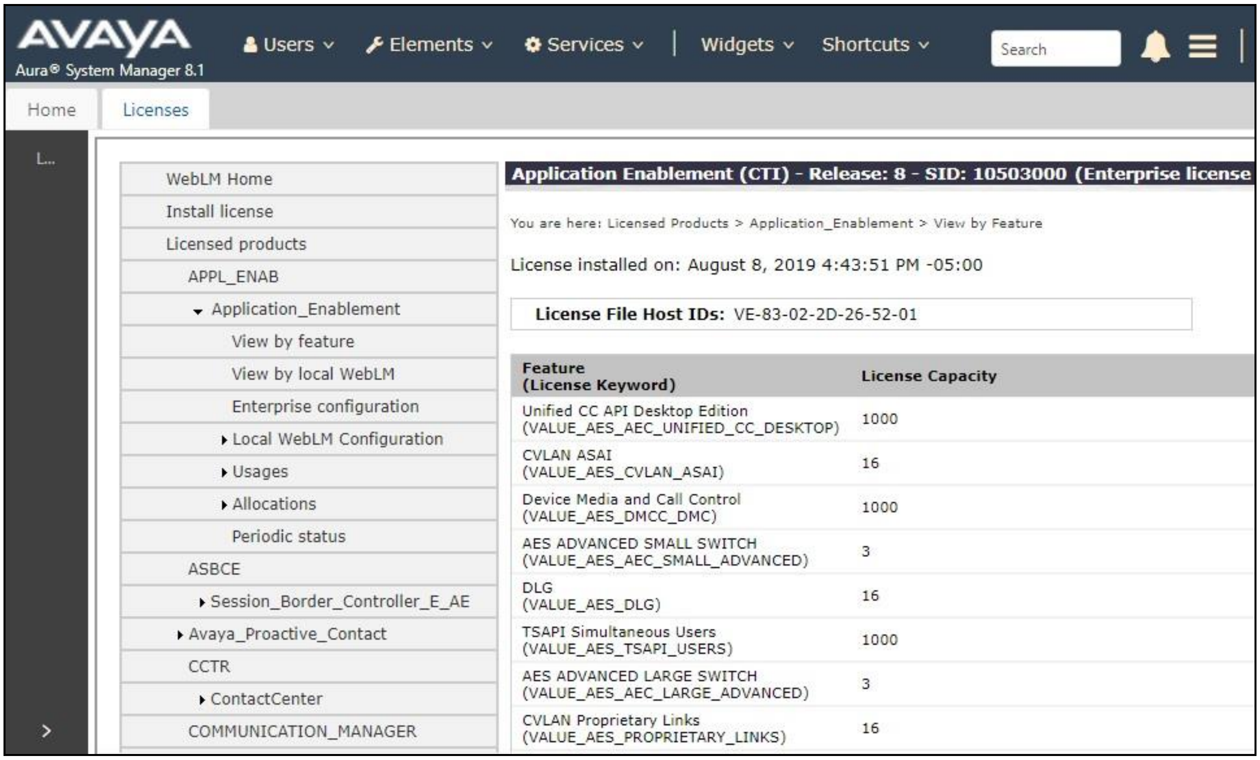
- WebLM Server Access

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 **Device Media and Call Control** and **TSAPI Simultaneous Users**, as shown below. Note that the DMCC license is used for the virtual IP softphones, and the TSAPI license is used for device monitoring and call control.



Application Enablement (CTI) - Release: 8 - SID: 10503000 (Enterprise license

You are here: Licensed Products > Application_Enablement > View by Feature

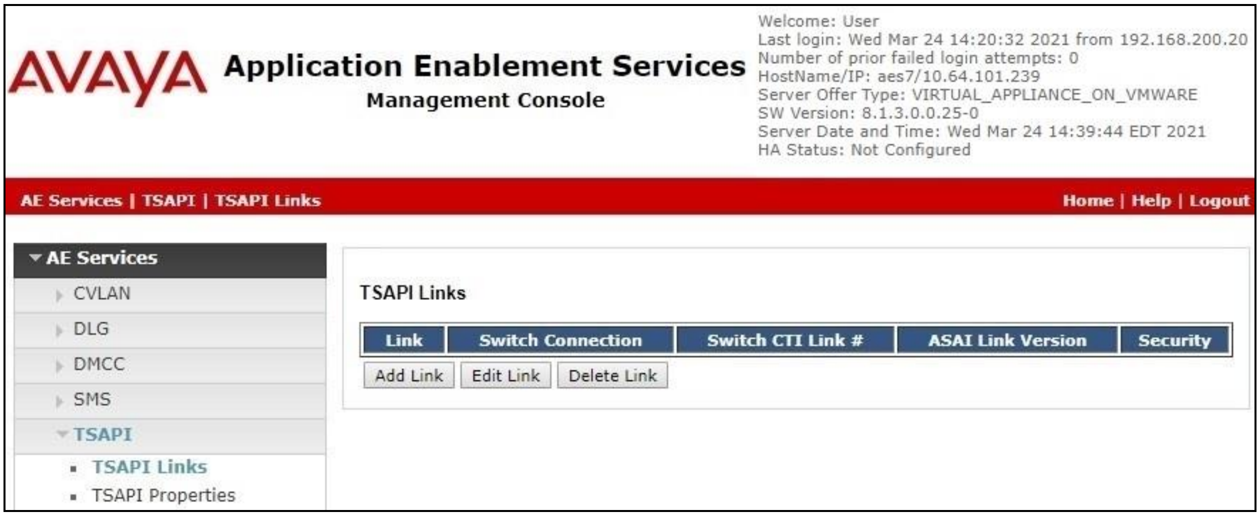
License installed on: August 8, 2019 4:43:51 PM -05:00

License File Host IDs: VE-83-02-2D-26-52-01

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

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**.



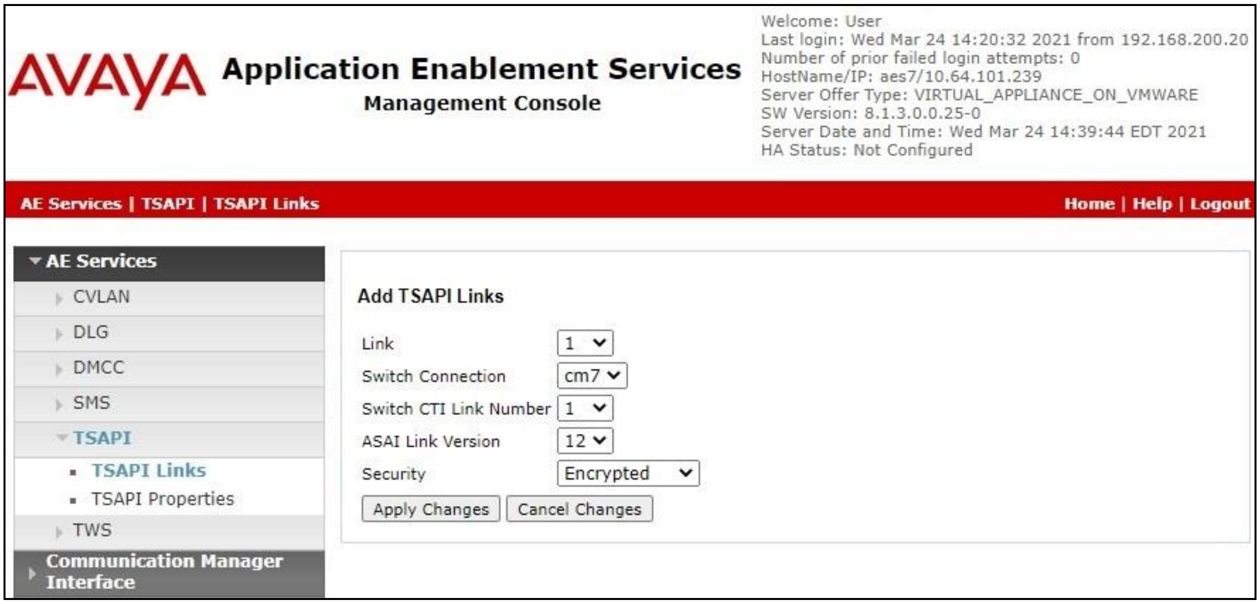
Welcome: User
Last login: Wed Mar 24 14:20:32 2021 from 192.168.200.20
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.1.3.0.0.25-0
Server Date and Time: Wed Mar 24 14:39:44 EDT 2021
HA Status: Not Configured

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**. For **Security**, select "Encrypted". Retain the default values in the remaining fields.



Welcome: User
Last login: Wed Mar 24 14:20:32 2021 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: 8.1.3.0.0.25-0
Server Date and Time: Wed Mar 24 14:39:44 EDT 2021
HA Status: Not Configured

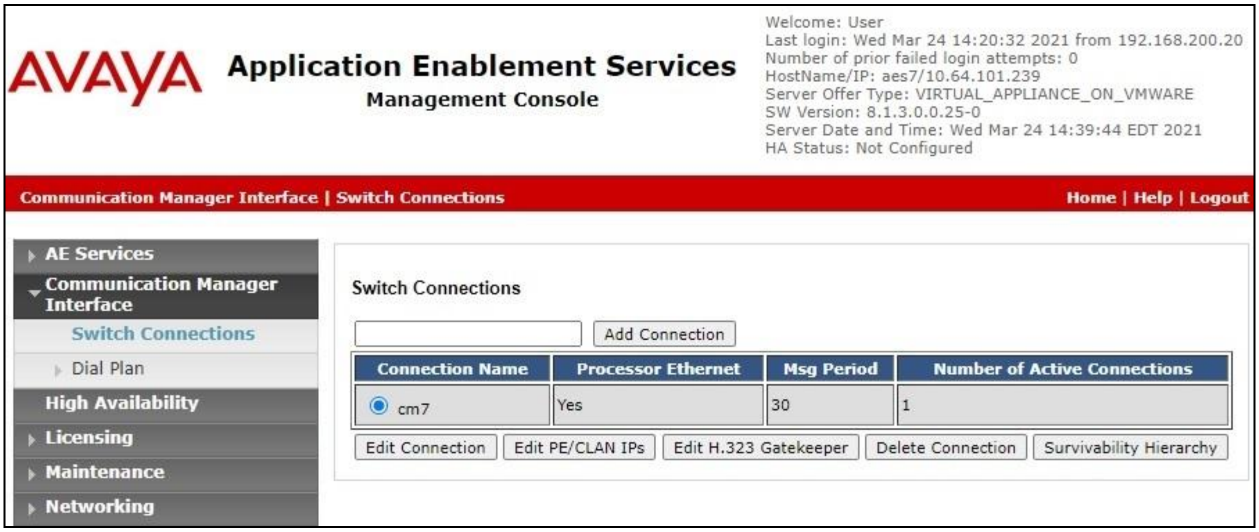
Add TSAPI Links

Link	1
Switch Connection	cm7
Switch CTI Link Number	1
ASAI Link Version	12
Security	Encrypted

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**.

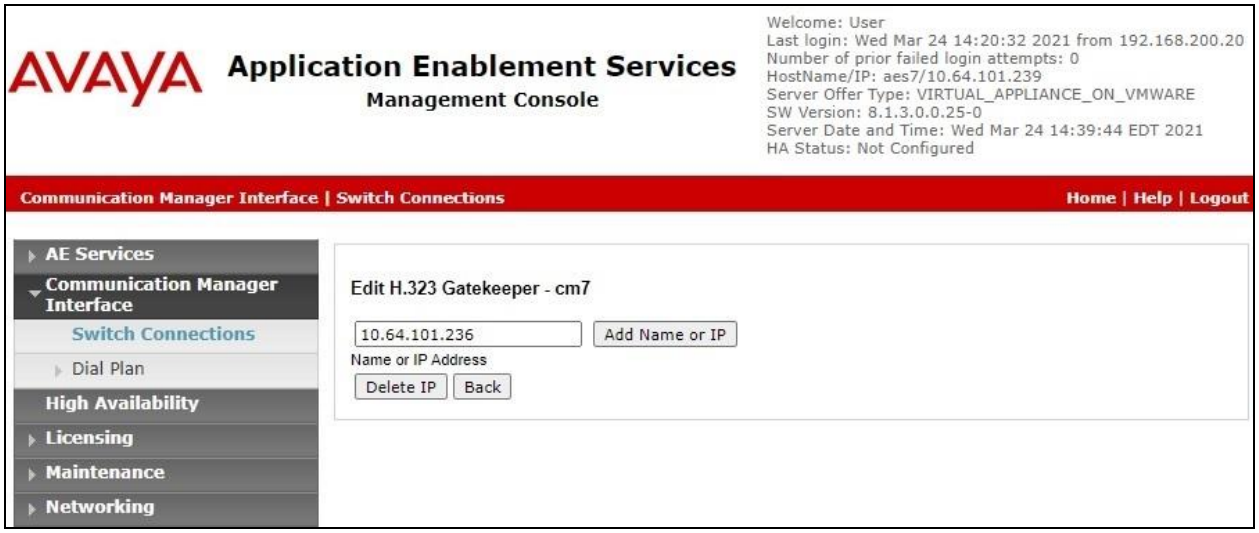


Welcome: User
Last login: Wed Mar 24 14:20:32 2021 from 192.168.200.20
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.1.3.0.0.25-0
Server Date and Time: Wed Mar 24 14:39:44 EDT 2021
HA Status: Not Configured

Switch Connections

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

The **Edit H.323 Gatekeeper** screen is displayed 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: Wed Mar 24 14:20:32 2021 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: 8.1.3.0.0.25-0
Server Date and Time: Wed Mar 24 14:39:44 EDT 2021
HA Status: Not Configured

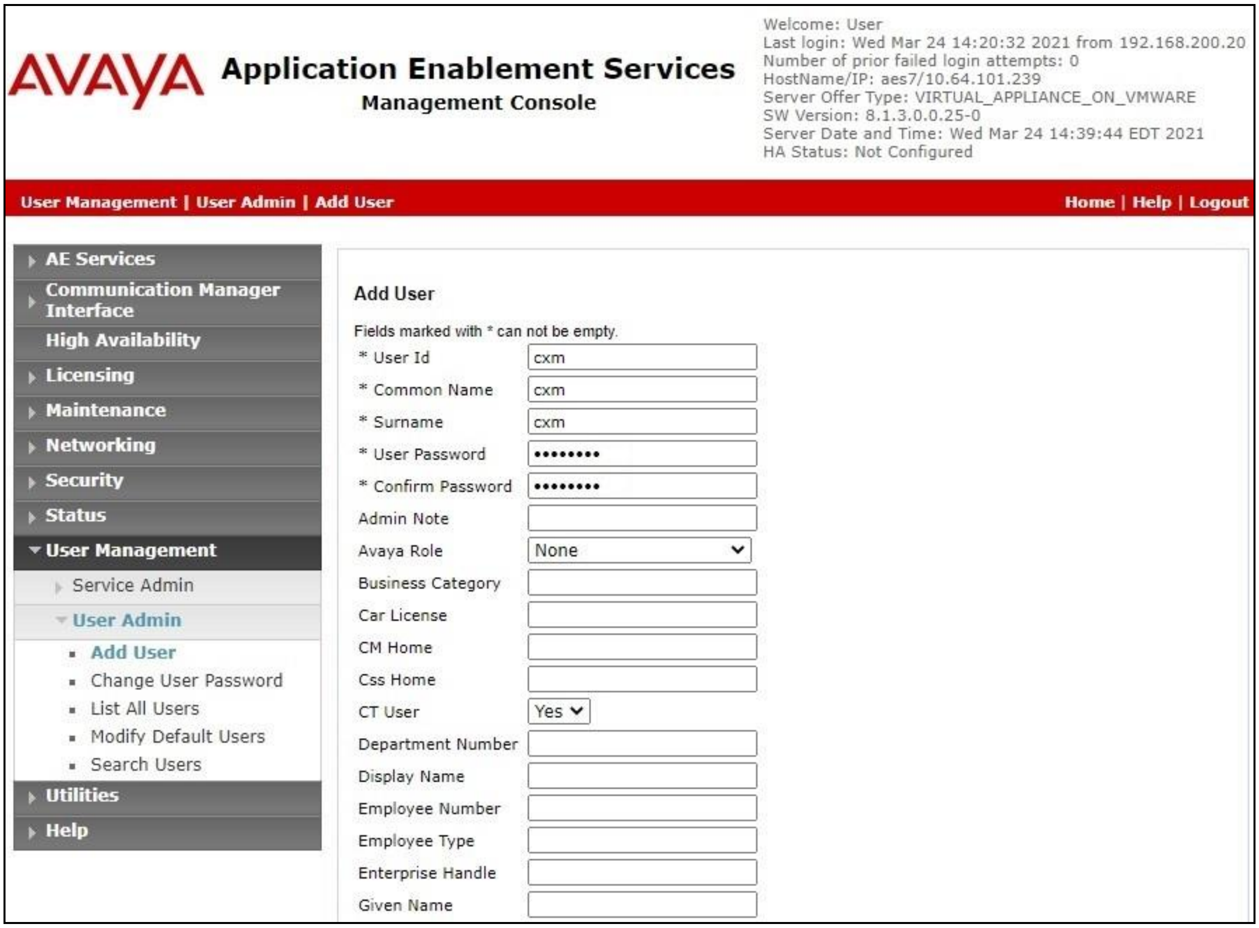
Edit H.323 Gatekeeper - cm7

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 (not shown).

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: Wed Mar 24 14:20:32 2021 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: 8.1.3.0.0.25-0
Server Date and Time: Wed Mar 24 14:39:44 EDT 2021
HA Status: Not Configured

Add User

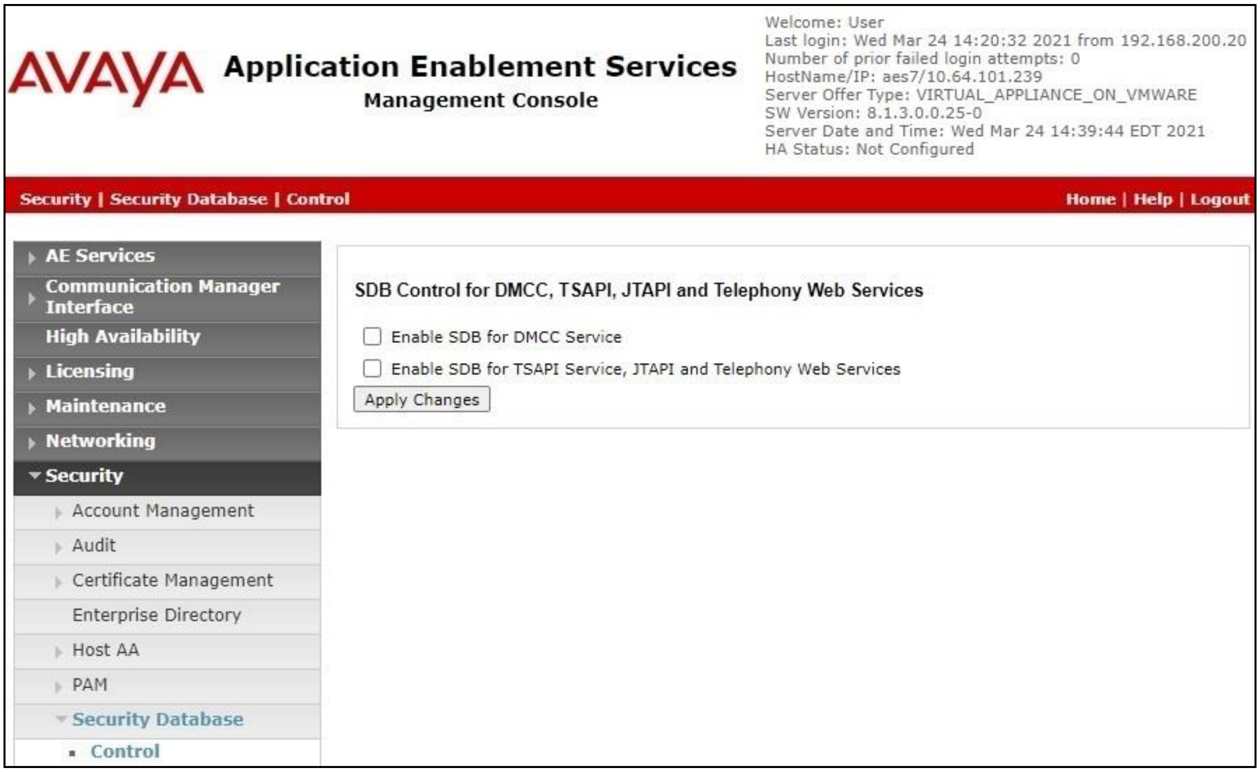
Fields marked with * can not be empty.

* 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 **Enable SDB for DMCC Service** is unchecked, as shown below.

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



Welcome: User
Last login: Wed Mar 24 14:20:32 2021 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: 8.1.3.0.0.25-0
Server Date and Time: Wed Mar 24 14:39:44 EDT 2021
HA Status: Not Configured

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

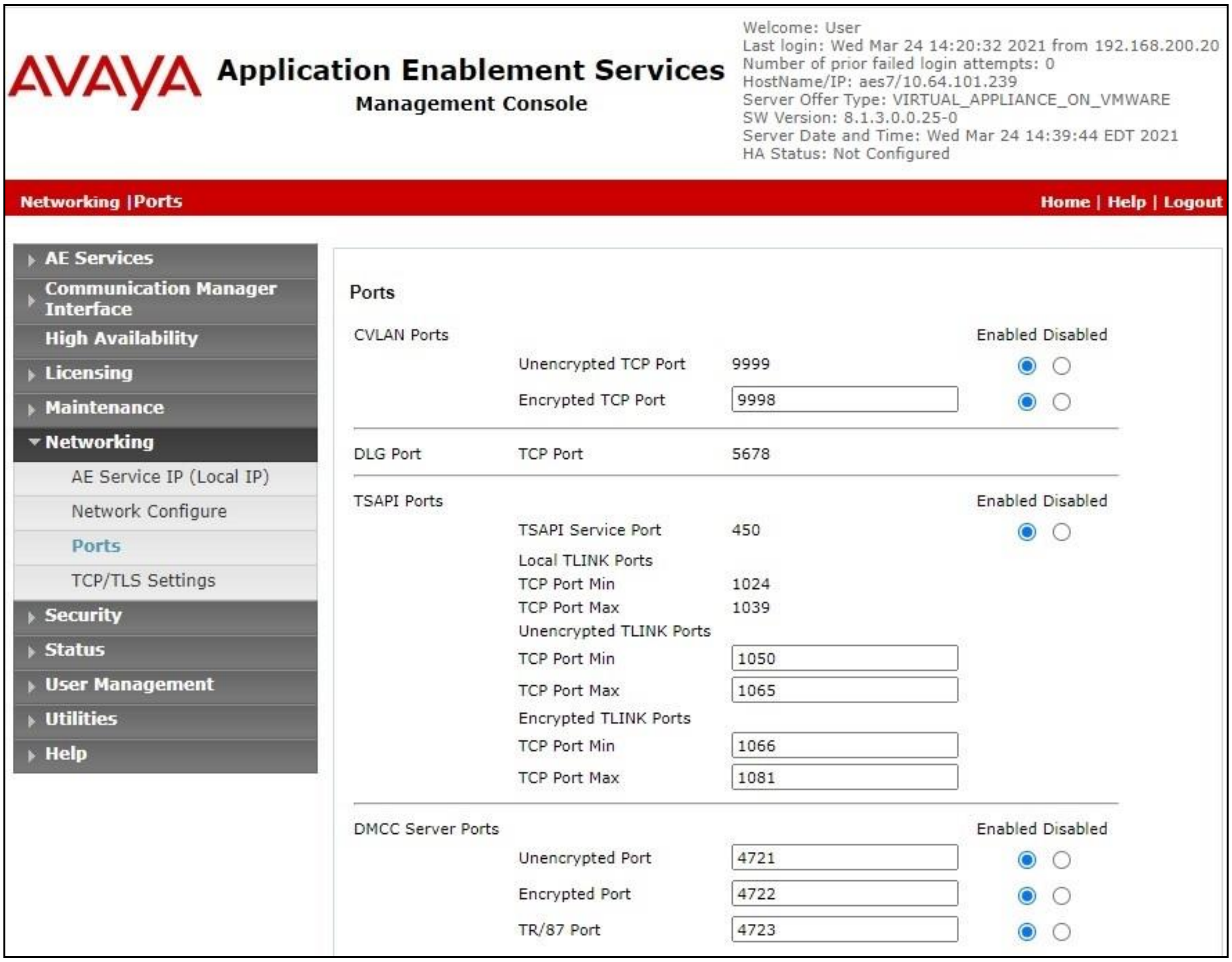
☐ Enable SDB for DMCC Service

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

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.



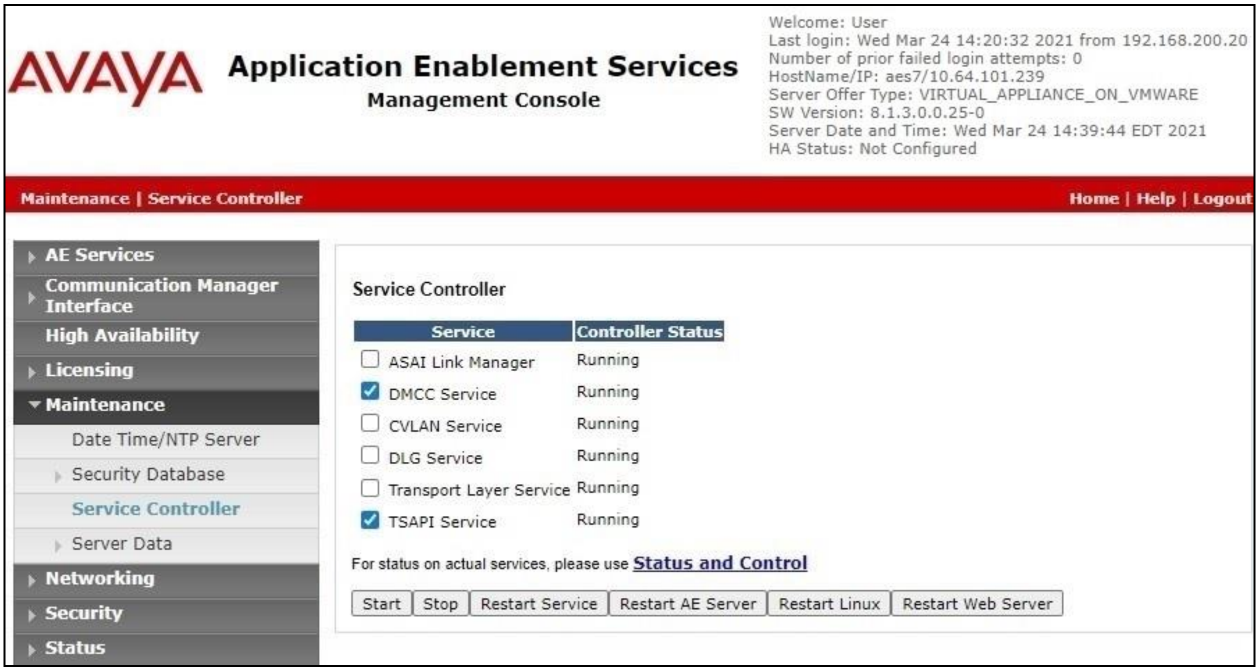
Welcome: User
Last login: Wed Mar 24 14:20:32 2021 from 192.168.200.20
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.1.3.0.0.25-0
Server Date and Time: Wed Mar 24 14:39:44 EDT 2021
HA Status: Not Configured

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	●	○

6.8. Restart Service

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: Wed Mar 24 14:20:32 2021 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: 8.1.3.0.0.25-0
Server Date and Time: Wed Mar 24 14:39:44 EDT 2021
HA Status: Not Configured

Service Controller

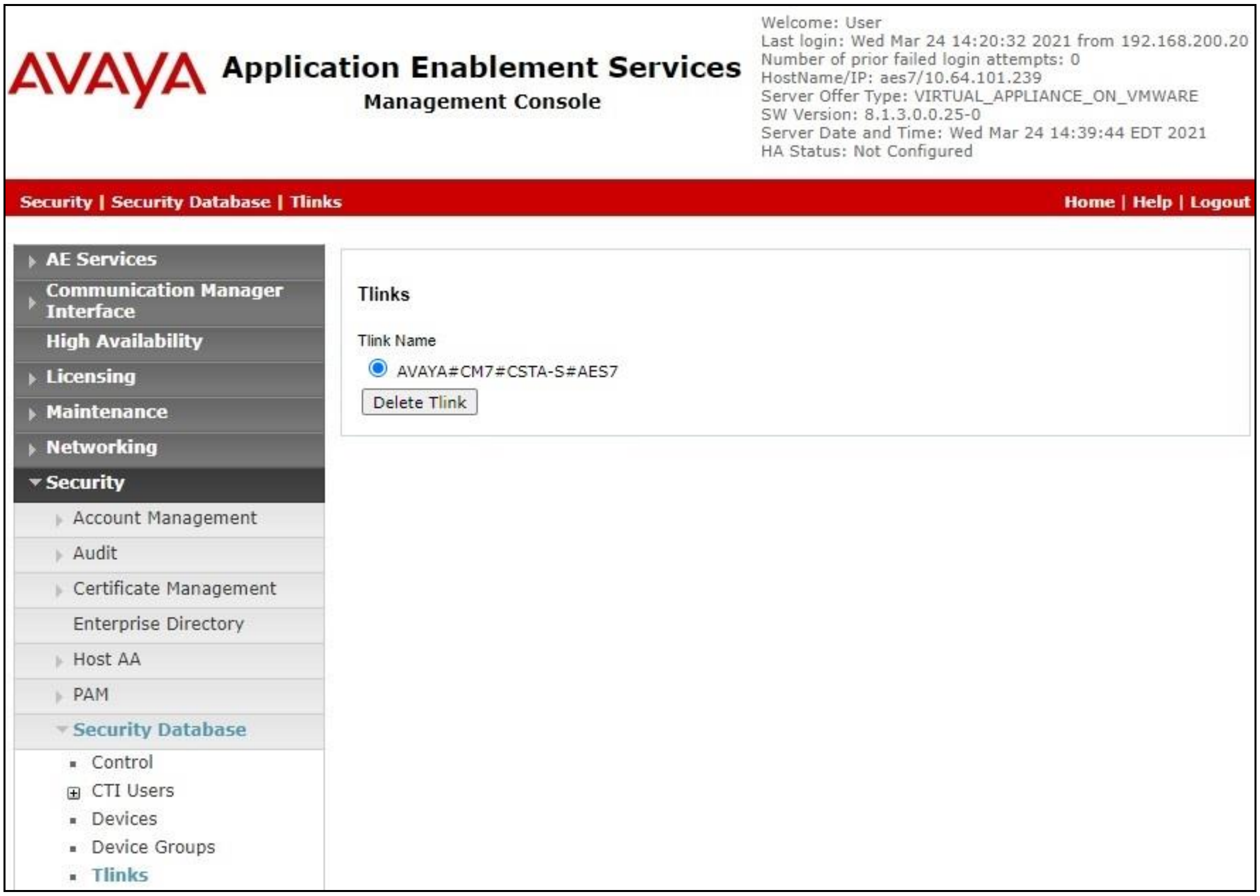
Service	Controller Status
□ ASAI Link Manager	Running
☑ DMCC Service	Running
□ CVLAN Service	Running
□ DLG Service	Running
□ Transport Layer Service	Running
☑ TSAPI Service	Running

For status on actual services, please use Status and Control

6.9. 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-S#**AES7**". Note the use of the switch connection "CM7" from **Section 6.3** as part of the Tlink name.



Welcome: User
Last login: Wed Mar 24 14:20:32 2021 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: 8.1.3.0.0.25-0
Server Date and Time: Wed Mar 24 14:39:44 EDT 2021
HA Status: Not Configured

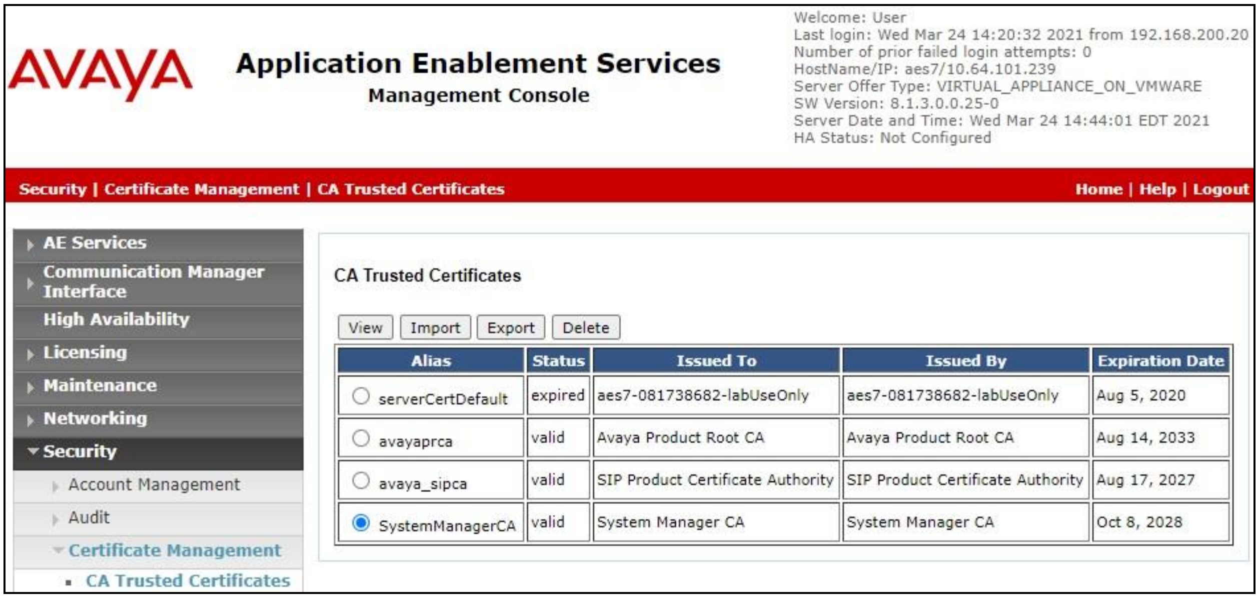
Tlinks

Tlink Name

● AVAYA#CM7#CSTA-S#AES7

6.10. 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 “SystemManagerCA”, and click **Export**.

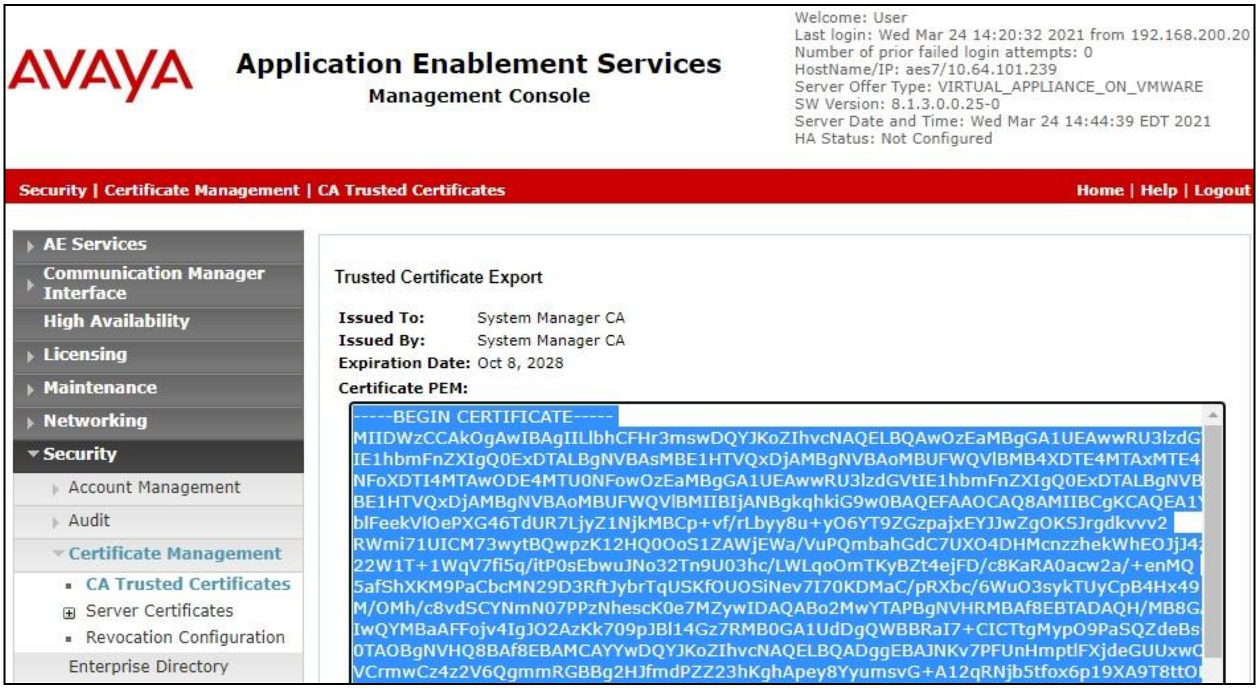


Welcome: User
Last login: Wed Mar 24 14:20:32 2021 from 192.168.200.20
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.1.3.0.0.25-0
Server Date and Time: Wed Mar 24 14:44:01 EDT 2021
HA Status: Not Configured

CA Trusted Certificates

	Alias	Status	Issued To	Issued By	Expiration Date
○	serverCertDefault	expired	aes7-081738682-labUseOnly	aes7-081738682-labUseOnly	Aug 5, 2020
○	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
●	SystemManagerCA	valid	System Manager CA	System Manager CA	Oct 8, 2028

The **Trusted Certificate Export** screen is displayed next. Copy everything in the text box, including the **BEGIN CERTIFICATE** and **END CERTIFICATE** (not shown) lines.



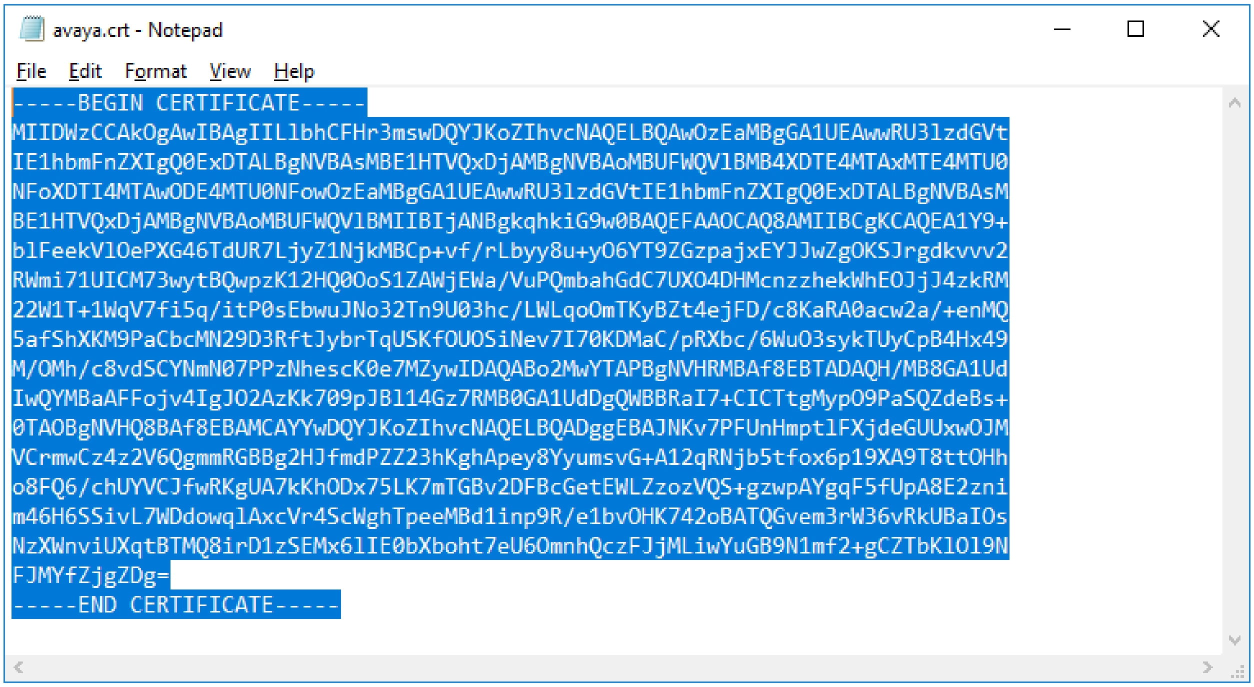
Welcome: User
Last login: Wed Mar 24 14:20:32 2021 from 192.168.200.20
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.1.3.0.0.25-0
Server Date and Time: Wed Mar 24 14:44:39 EDT 2021
HA Status: Not Configured

Trusted Certificate Export

Issued To: System Manager CA
Issued By: System Manager CA
Expiration Date: Oct 8, 2028
Certificate PEM:

```
-----BEGIN CERTIFICATE-----
MIIDWzCCAkOgAwIBAgIILlbhCFHr3mswDQYJKoZIhvcNAQELBQAwOzEaMBgGA1UEAwwRU3lzdG
IE1hbmFnZXIgQ0ExDTALBgNVBAsMBE1HTVQxDjAMBgNVBAoMBUFWQVlBMB4XDTE4MTAxMTE4
NFoXDTI4MTAwODE4MTU0NFowOzEaMBgGA1UEAwwRU3lzdGVtIE1hbmFnZXIgQ0ExDTALBgNVB
BE1HTVQxDjAMBgNVBAoMBUFWQVlBMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA1Y
blFeekVlOePXG46TdUR7LjyZ1NjkMBCp+vf/rLbyy8u+yO6YT9ZGzpajxEYJJwZgOKSJrgdkvvv2
RWmi71UICM73wytBQwpzK12HQ0OoS1ZAWjEWa/VuPQmbahGdC7UXO4DHMcnzzhekWhEOJjJ4
22W1T+1WqV7fi5q/itP0sEbwuJNo32Tn9U03hc/LWLqoOmTKyBZt4ejFD/c8KaRA0acw2a/+enMQ
5afShXKM9PaCbcMN29D3RftJybrTqUSKfOUOSiNev7I70KDMaC/pRXbc/6WuO3sykTUyCpB4Hx49
M/OMh/c8vdSCYNmN07PPzNhescK0e7MZywIDAQABo2MwYTAPBgNVHRMBAf8EBTADAQH/MB8G
IwQYMBaAFFojv4IgJO2AzKk709pJBl14Gz7RMB0GA1UdDgQWBBRaI7+CICTtgMypO9PaSQZdeBs
0TAOBgNVHQ8BAf8EBAMCAYYwDQYJKoZIhvcNAQELBQADggEBAJNKv7PFUnHmptlFXjdeGUUxwC
VCrmwCz4z2V6QgmmRGBBg2HJfmdPZZ23hKghApey8YyumsvG+A12qRNjb5tfox6p19XA9T8ttO
```

Paste the copied content to a Notepad file, and save with a desired file name using **.crt** as suffix, such as **avaya.crt** in the compliance testing.



```
-----BEGIN CERTIFICATE-----
MIIDWzCCAkOgAwIBAgIILlbhCFHr3mswDQYJKoZIhvcNAQELBQAwOzEaMBgGA1UEAwwRU3lzdGVt
IE1hbmFnZXIgQ0ExDTALBgNVBAsMBE1HTVQxDjAMBgNVBAoMBUFWQVlBMB4XDTE4MTAxMTE4MTU0
NFoXDTI4MTAwODE4MTU0NFowOzEaMBgGA1UEAwwRU3lzdGVtIE1hbmFnZXIgQ0ExDTALBgNVBAsM
BE1HTVQxDjAMBgNVBAoMBUFWQVlBMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA1Y9+
blFeekVlOePXG46TdUR7LjyZ1NjkMBCp+vf/rLbyy8u+yO6YT9ZGzpajxEYJJwZgOKSJrgdkvvv2
RWmi71UICM73wytBQwpzK12HQ0OoS1ZAWjEWa/VuPQmbahGdC7UXO4DHMcnzzhekWhEOJjJ4zkRM
22W1T+1WqV7fi5q/itP0sEbwuJNo32Tn9U03hc/LWLqoOmTKyBZt4ejFD/c8KaRA0acw2a/+enMQ
5afShXKM9PaCbcMN29D3RftJybrTqUSKfOUOSiNev7I70KDMaC/pRXbc/6WuO3sykTUyCpB4Hx49
M/OMh/c8vdSCYNmN07PPzNhescK0e7MZywIDAQABo2MwYTAPBgNVHRMBAf8EBTADAQH/MB8GA1Ud
IwQYMBaAFFojv4IgJO2AzKk709pJBl14Gz7RMB0GA1UdDgQWBBRaI7+CICTtgMypO9PaSQZdeBs+
0TAOBgNVHQ8BAf8EBAMCAYYwDQYJKoZIhvcNAQELBQADggEBAJNKv7PFUnHmptlFXjdeGUUxwOJM
VCrmwCz4z2V6QgmmRGBBg2HJfmdPZZ23hKghApey8YyumsvG+A12qRNjb5tfox6p19XA9T8ttOHh
o8FQ6/chUYVCJfwRKgUA7kKhODx75LK7mTGBv2DFBcGetEWLZzozVQS+gzwpAYgqF5fUpA8E2zni
m46H6SSivL7WDdowqlAxcVr4ScWghTpeeMBd1inp9R/e1bvOHK742oBATQGvem3rW36vRkUBaIOs
NzXWnviUXqtBTMQ8irD1zSEMx6lIE0bXboht7eU6OmnhQczFJjMLiwYuGB9N1mf2+gCZTbKlOl9N
FJMYfZjgZDg=
-----END CERTIFICATE-----
```

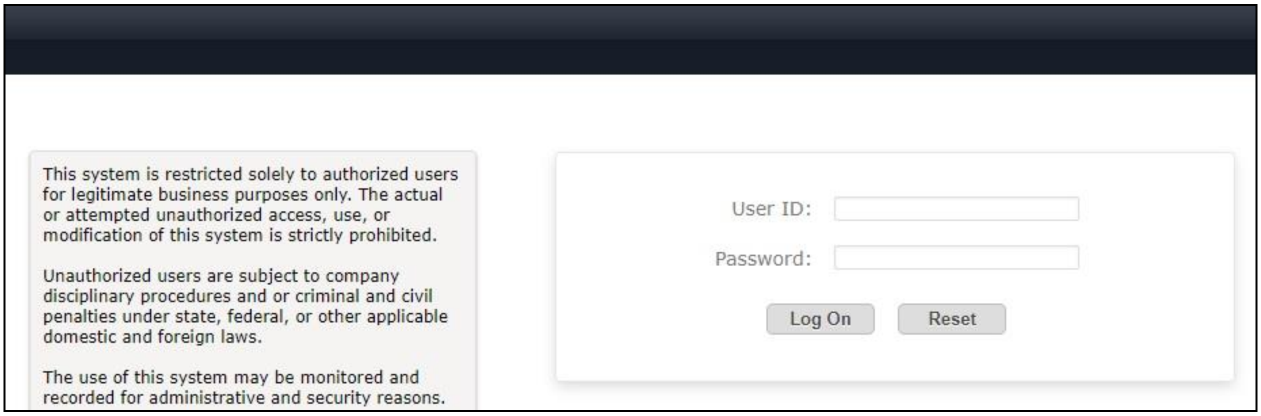
7. Configure Avaya Aura® Session Manager

This section provides the procedures for configuring Session Manager, which is performed via the web interface of System 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.



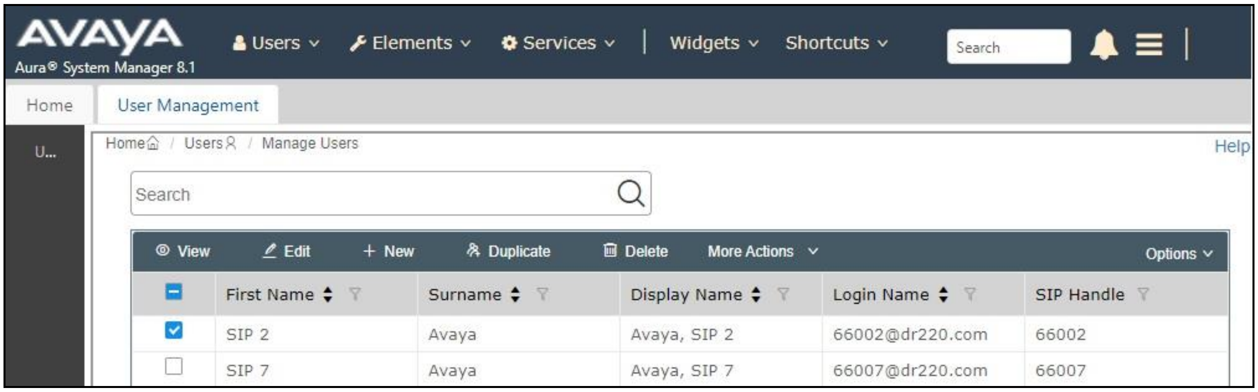
This system is restricted solely to authorized users for legitimate business purposes only. The actual or attempted unauthorized access, use, or modification of this system is strictly prohibited.

Unauthorized users are subject to company disciplinary procedures and or criminal and civil penalties under state, federal, or other applicable domestic and foreign laws.

The use of this system may be monitored and recorded for administrative and security reasons.

7.2. Administer Users

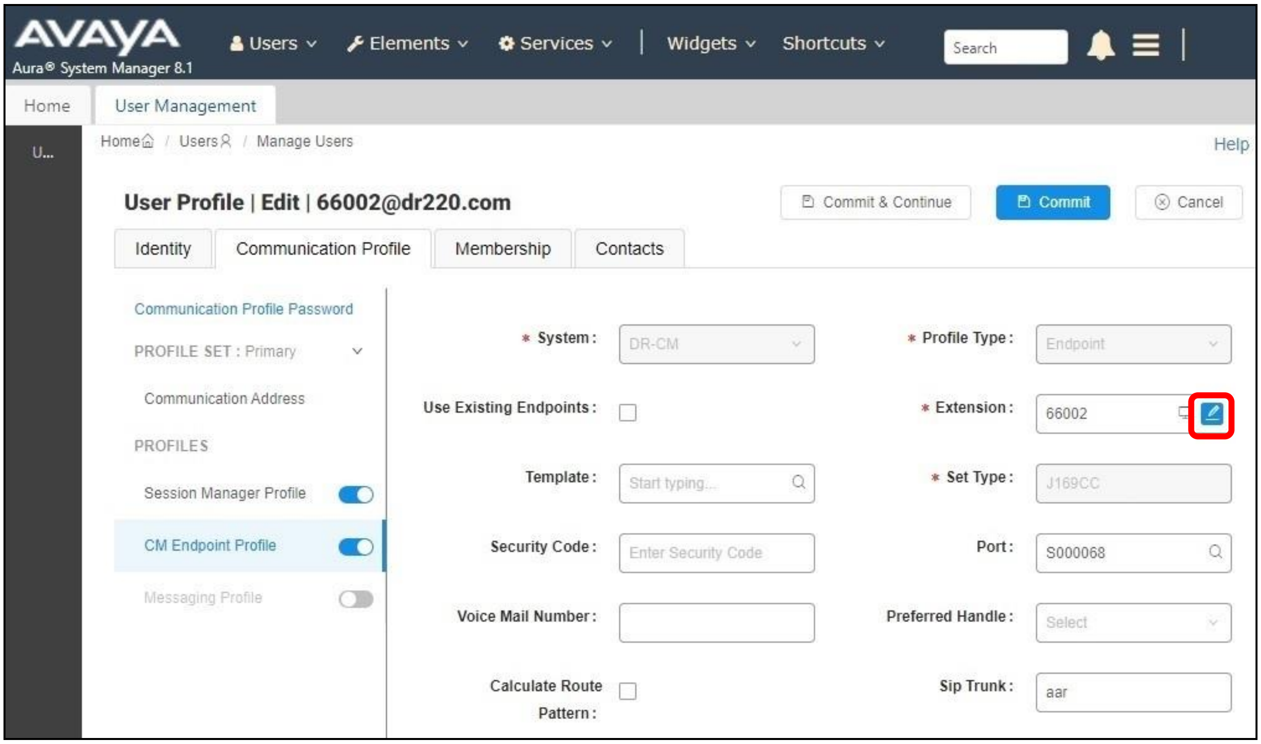
In the subsequent screen (not shown), select **Users → User Management** from the top menu. Select **User Management → Manage Users** (not shown) from the left pane to display the screen below. Select the entry associated with the first SIP agent station from **Section 3**, in this case "66002", and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



☐	First Name	Surname	Display Name	Login Name	SIP Handle
☑	SIP 2	Avaya	Avaya, SIP 2	66002@dr220.com	66002
☐	SIP 7	Avaya	Avaya, SIP 7	66007@dr220.com	66007

The **User Profile | Edit** screen is displayed. Select the **Communication Profile** tab, followed by **CM Endpoint Profile** to display the screen below.

Click on the **Editor** icon shown below.

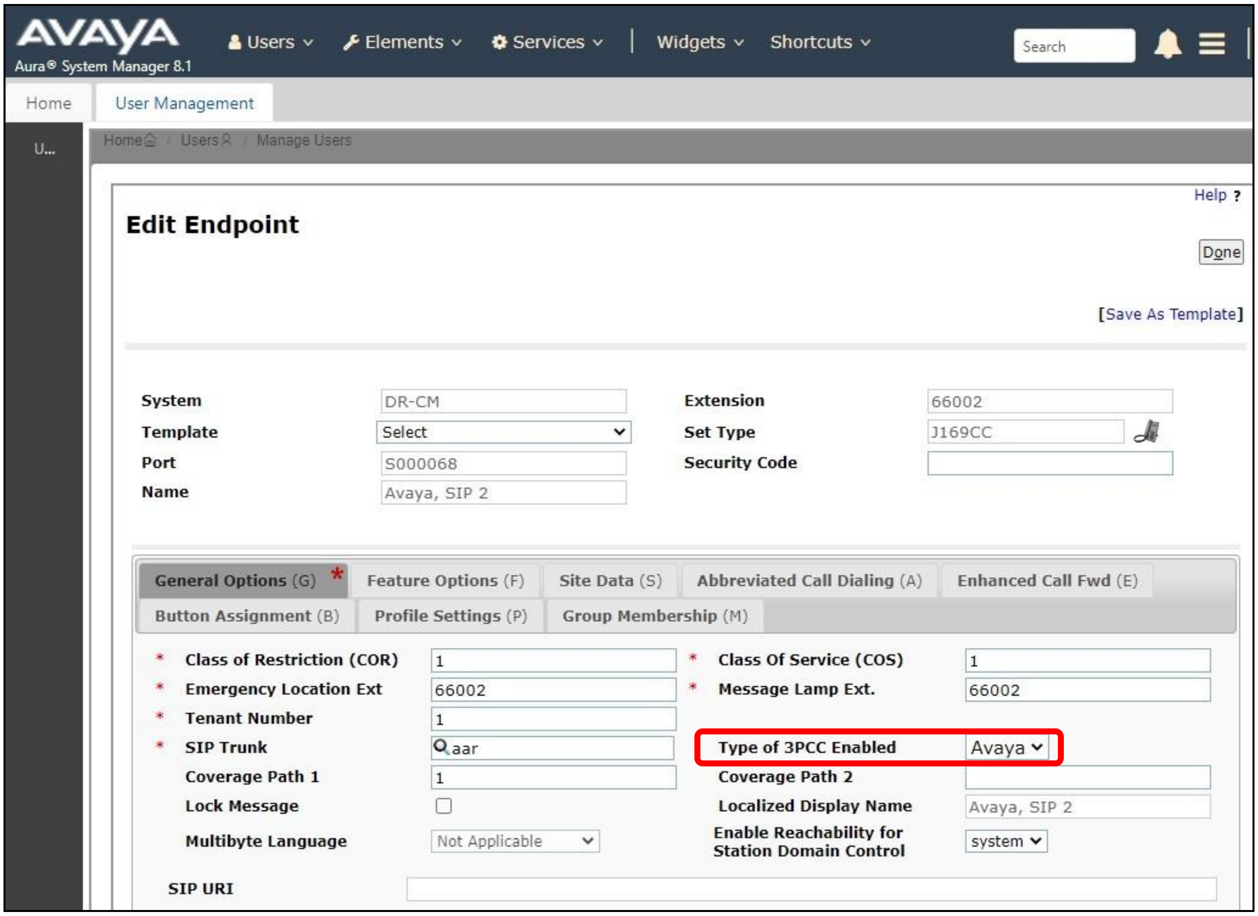


User Profile | Edit | 66002@dr220.com

* System :	DR-CM	* Profile Type :	Endpoint
Use Existing Endpoints :	□	* Extension :	66002
Template :	Start typing...	* Set Type :	J169CC
Security Code :	Enter Security Code	Port :	S000068
Voice Mail Number :		Preferred Handle :	Select
Calculate Route Pattern :	□	Sip Trunk :	aar

The **Edit Endpoint** pop-up screen is displayed. For **Type of 3PCC Enabled**, select “Avaya” as shown below.

Repeat this section for all SIP agent stations from **Section 3**. In the compliance testing, one SIP agent station 66002 was configured.



Edit Endpoint

System	DR-CM	Extension	66002
Template	Select	Set Type	J169CC
Port	S000068	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
SIP URI			

8. Configure TeleComp CXM

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

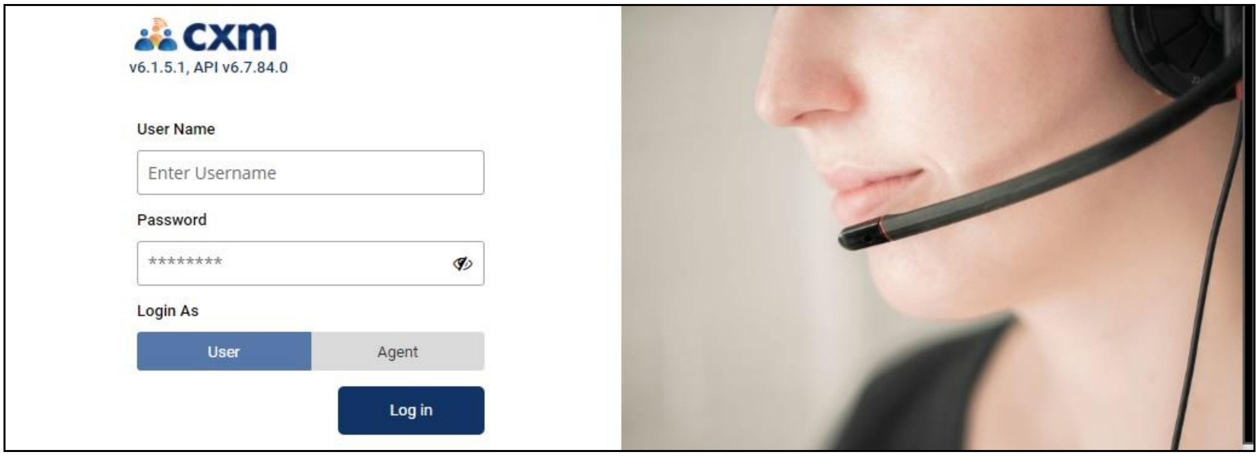
- Launch web interface
- Administer switch setup
- Administer conference stations
- Administer stations
- Administer VDNs
- Administer skills
- Administer agents
- Install CA certificate
- Administer TSLIB.INI
- Restart CXM services

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

Prior to configuration, a site and a recorder are assumed to have been created.

8.1. Launch Web Interface

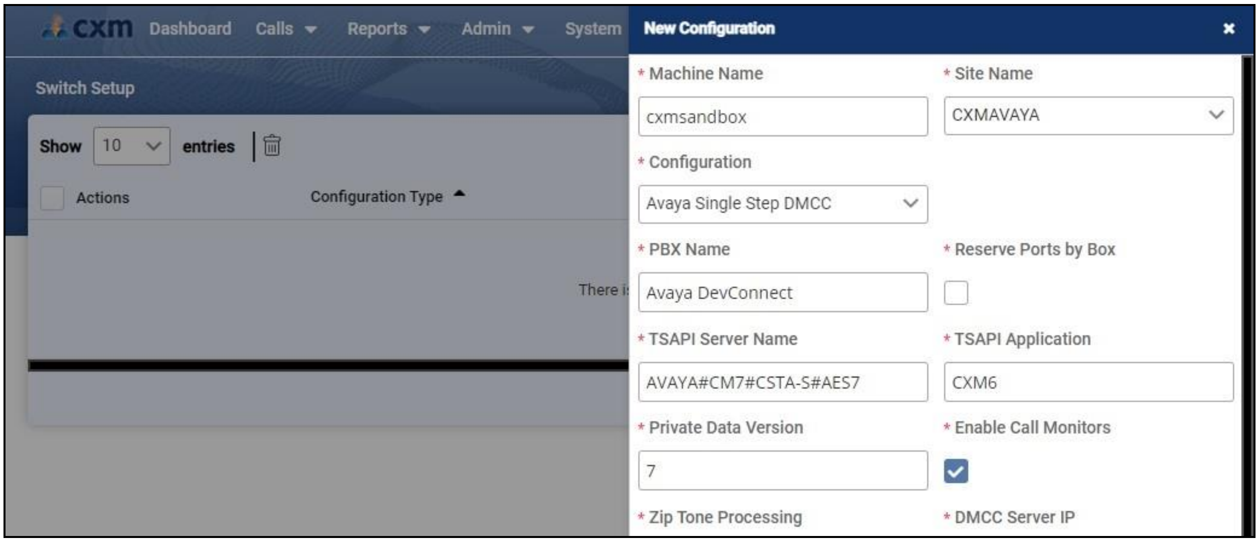
Access the CXM web-based interface by using the URL "https://hostname/cxmui" in a browser window, where "hostname" is the host name of the CXM server. Log in using the appropriate credentials.



8.2. Administer Switch Setup

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

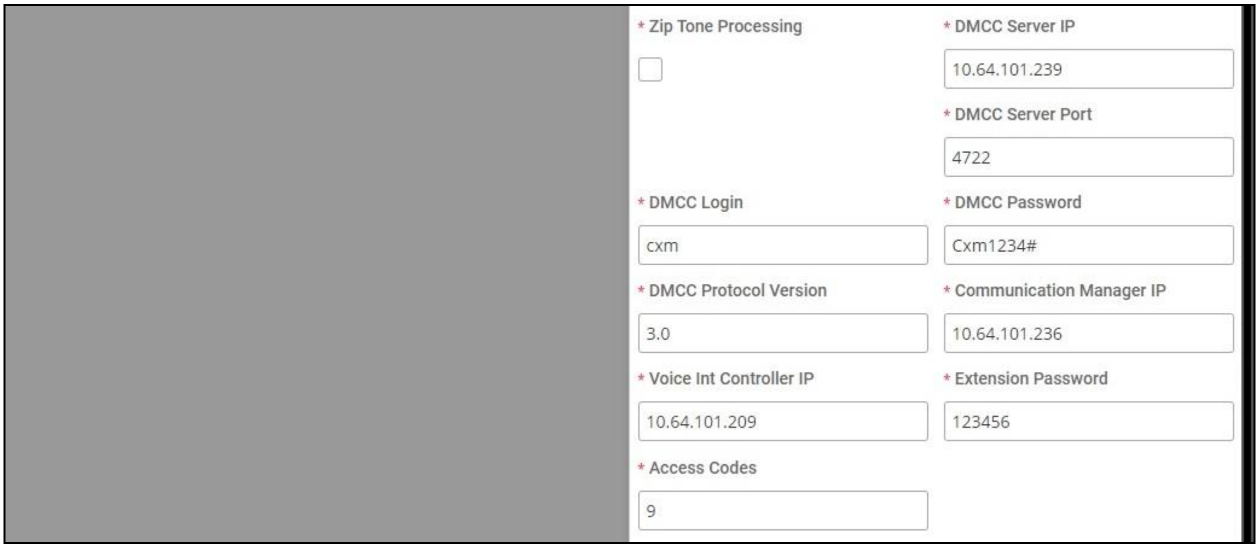
- **Machine Name:** The host name of the CXM server.
- **Site Name:** Select the applicable pre-configured site.
- **Configuration:** "Avaya Single Step DMCC"
- **PBX Name:** A desired name.
- **TSAPI Server Name:** The Tlink name from **Section 6.9**.
- **TSAPI Application:** A desired name.
- **Private Data Version:** "7"
- **Enable Call Monitors:** Check this field.



New Configuration

* Machine Name: cxmsandbox	* Site Name: CXMAVAYA
* Configuration: Avaya Single Step DMCC	
* PBX Name: Avaya DevConnect	* Reserve Ports by Box: ☐
* TSAPI Server Name: AVAYA#CM7#CSTA-S#AES7	* TSAPI Application: CXM6
* Private Data Version: 7	* Enable Call Monitors: ☑
* Zip Tone Processing	* DMCC Server IP

- **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 5.5**.
- **Access Codes:** The pertinent access code for the network, in this case "9".



* Zip Tone Processing
□

* DMCC Server IP
10.64.101.239

* DMCC Server Port
4722

* DMCC Login
cxm

* DMCC Password
Cxm1234#

* DMCC Protocol Version
3.0

* Communication Manager IP
10.64.101.236

* Voice Int Controller IP
10.64.101.209

* Extension Password
123456

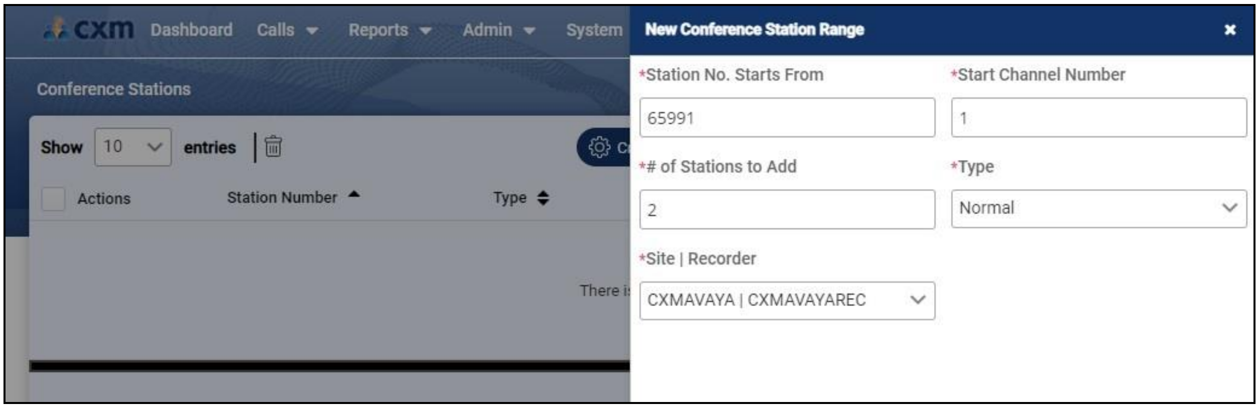
* Access Codes
9

8.3. Administer Conference Stations

Select **System → Conference Stations** from the top menu followed by **Create Conference Station Range** (not shown) to display the screen below. Enter the following values for the specified fields, and retain the default values in the remaining fields.

- **Station No. Starts From:** The first virtual IP softphone extension from **Section 5.5**.
- **Start Channel Number:** "1"
- **# of Stations to Add:** The number of virtual IP softphones from **Section 5.5**.
- **Type:** A desired type, in this case "Normal" for inbound and outbound.
- **Site | Recorder:** Select the applicable pre-configured site and recorder.

In the event that the virtual IP softphone extensions are not sequential, then add the conference stations one at a time.



New Conference Station Range

*Station No. Starts From: 65991

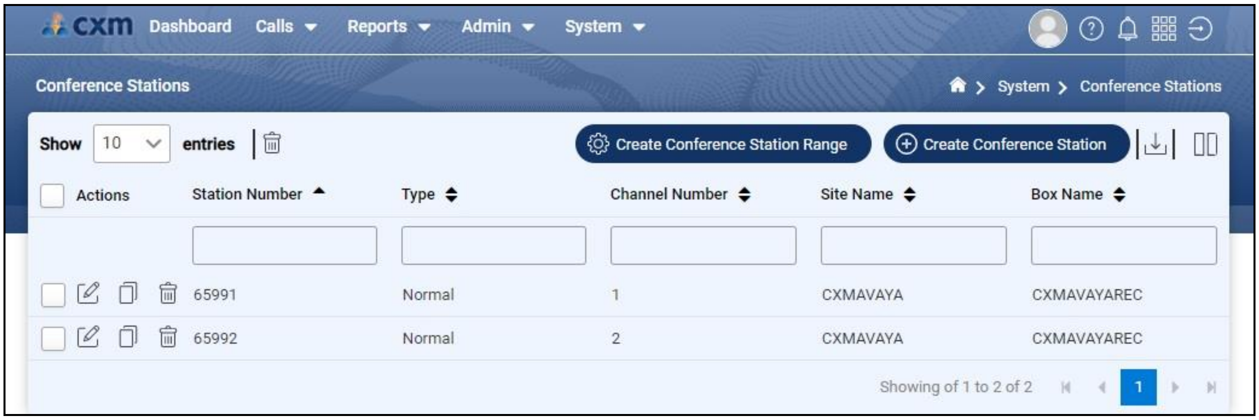
*Start Channel Number: 1

*# of Stations to Add: 2

*Type: Normal

*Site | Recorder: CXMAVAYA | CXMAVAYAREC

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



Actions	Station Number	Type	Channel Number	Site Name	Box Name
	65991	Normal	1	CXMAVAYA	CXMAVAYAREC
	65992	Normal	2	CXMAVAYA	CXMAVAYAREC

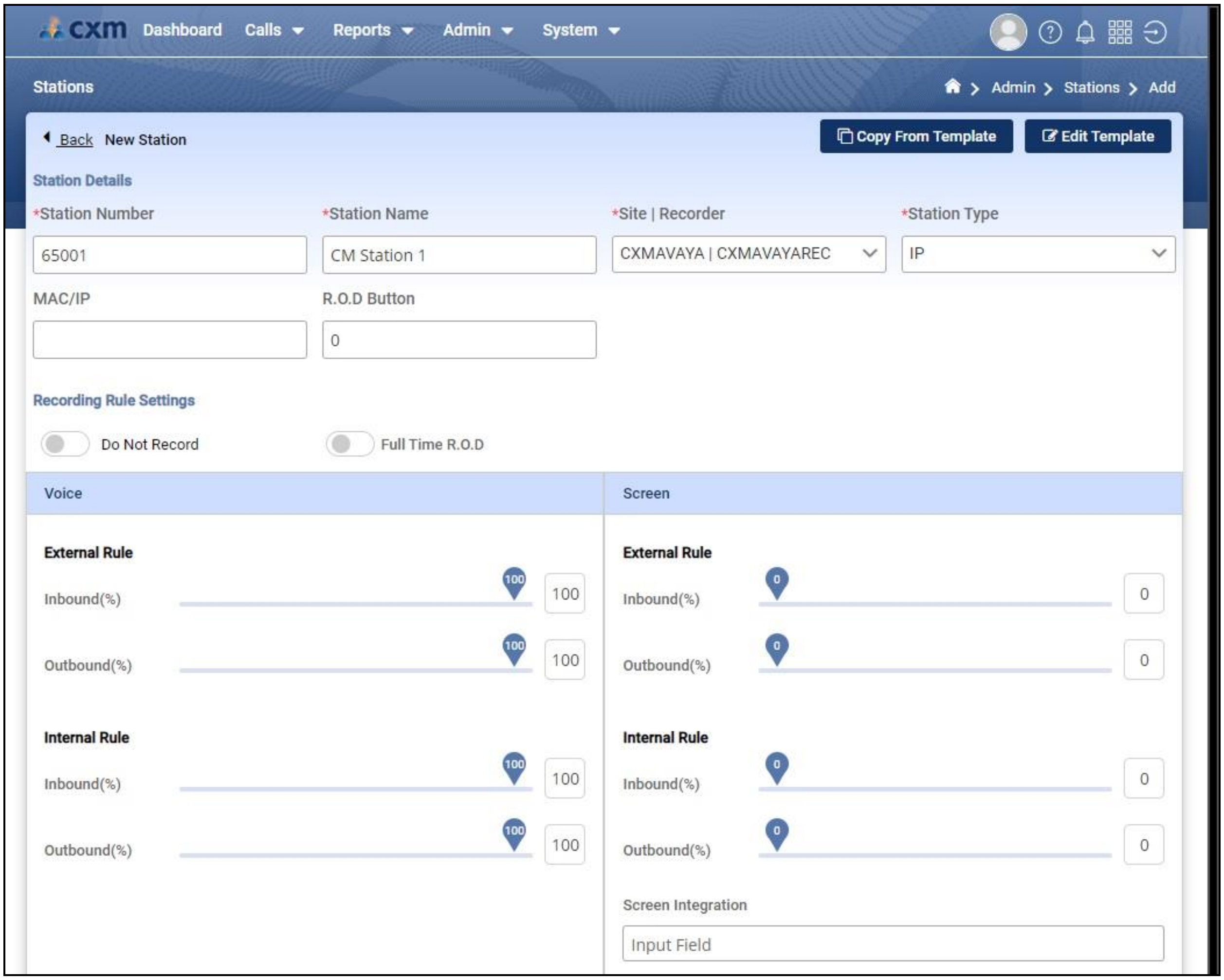
8.4. Administer Stations

Select **Admin → Stations** from the top menu followed by **Create Station** (not shown) to display the screen below. Enter the following values for the specified fields, and retain the default values in the remaining fields.

- **Station Number:** The first agent station extension from **Section 3**.
- **Station Name:** A desired agent station name.
- **Site | Recorder:** Select the applicable pre-configured site and recorder.
- **Station Type:** The applicable type of the agent station, in this case "IP".

In the **Voice** subsection, adjust the scroll bars to set desired percentage for types of calls to be recorded. In the compliance testing, all percentages were set to 100 for recording of all call types.

Repeat this section to configure all agent stations from **Section 3**. In the compliance testing, two agent stations with numbers "65001" and "66002" were created.



*Station Number: 65001
*Station Name: CM Station 1
*Site | Recorder: CXMAVAYA | CXMAVAYAREC
*Station Type: IP
MAC/IP:
R.O.D Button: 0

○ Do Not Record
○ Full Time R.O.D

Voice		Screen	
External Rule		**External Rule**	
Inbound(%)	100	Inbound(%)	0
Outbound(%)	100	Outbound(%)	0
Internal Rule		**Internal Rule**	
Inbound(%)	100	Inbound(%)	0
Outbound(%)	100	Outbound(%)	0

Screen Integration: Input Field

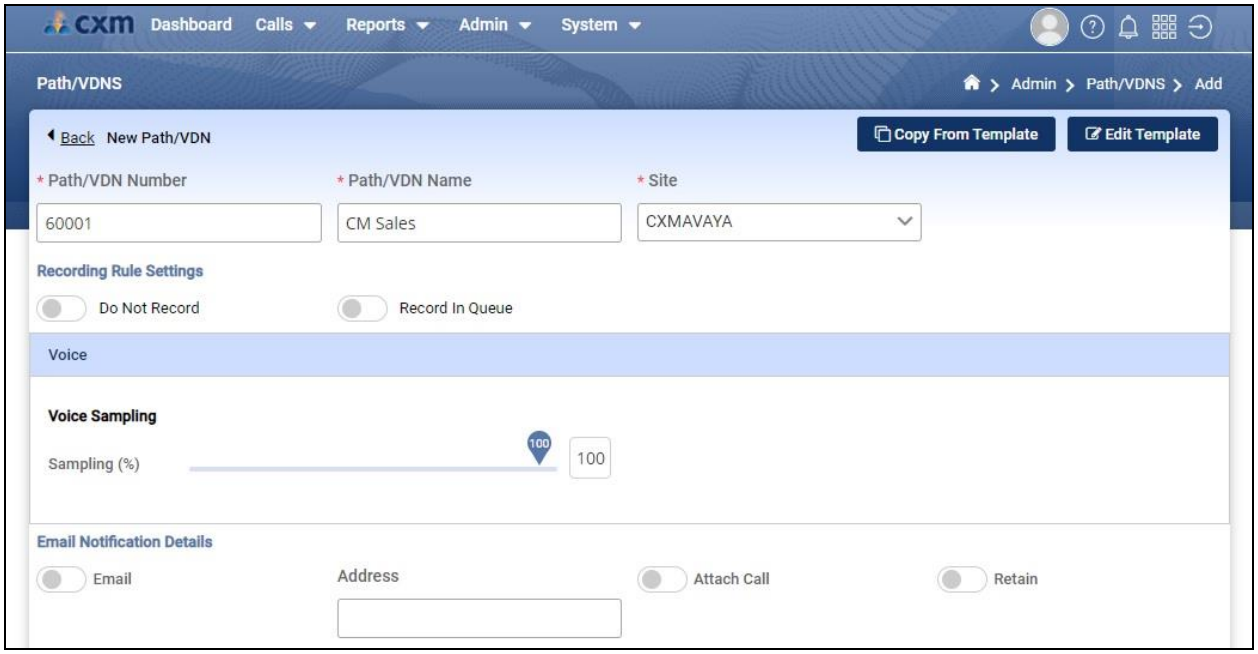
8.5. Administer VDNs

Select **Admin → Path/VDN** from the top menu followed by **Create Path/VDN** (not shown) to display the screen below. Enter the following values for the specified fields, and retain the default values in the remaining fields.

- **Path/VDN Number:** The first VDN extension from **Section 3**.
- **Path/VDN Name:** A desired VDN name.
- **Site:** Select the applicable pre-configured site.

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

Repeat this section to configure all VDNs from **Section 3**. In the compliance testing, two VDNs with numbers "60001" and "60002" were created.



* Path/VDN Number: 60001
* Path/VDN Name: CM Sales
* Site: CXMAVAYA

Recording Rule Settings
Do Not Record
Record In Queue

Voice

Voice Sampling
Sampling (%): 100

Email Notification Details
Email
Address
Attach Call
Retain

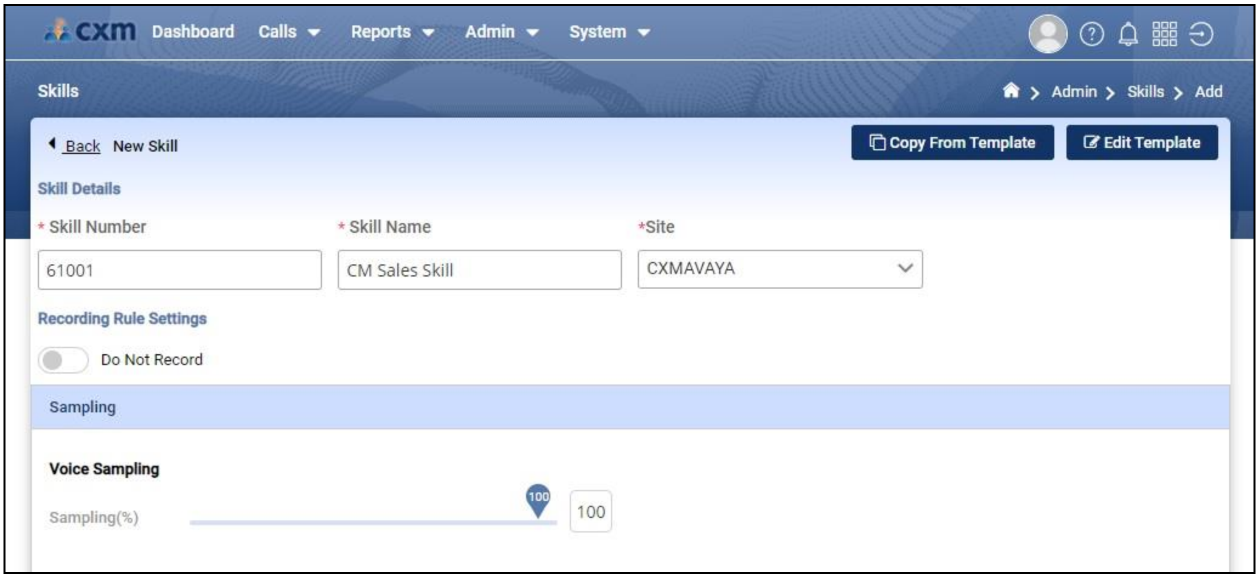
8.6. Administer Skills

Select **Admin** → **Skills** from the top menu followed by **Create Skill** (not shown) to display the screen below. Enter the following values for the specified fields, and retain the default values in the remaining fields.

- **Skill Number:** The first skill group extension from **Section 3**.
- **Skill Name:** A desired skill group name.
- **Site:** Select the applicable pre-configured site.

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

Repeat this section to configure all skill groups from **Section 3**. In the compliance testing, two skill groups with numbers “61001” and “61002” were created.



* Skill Number: 61001
* Skill Name: CM Sales Skill
*Site: CXMAVAYA

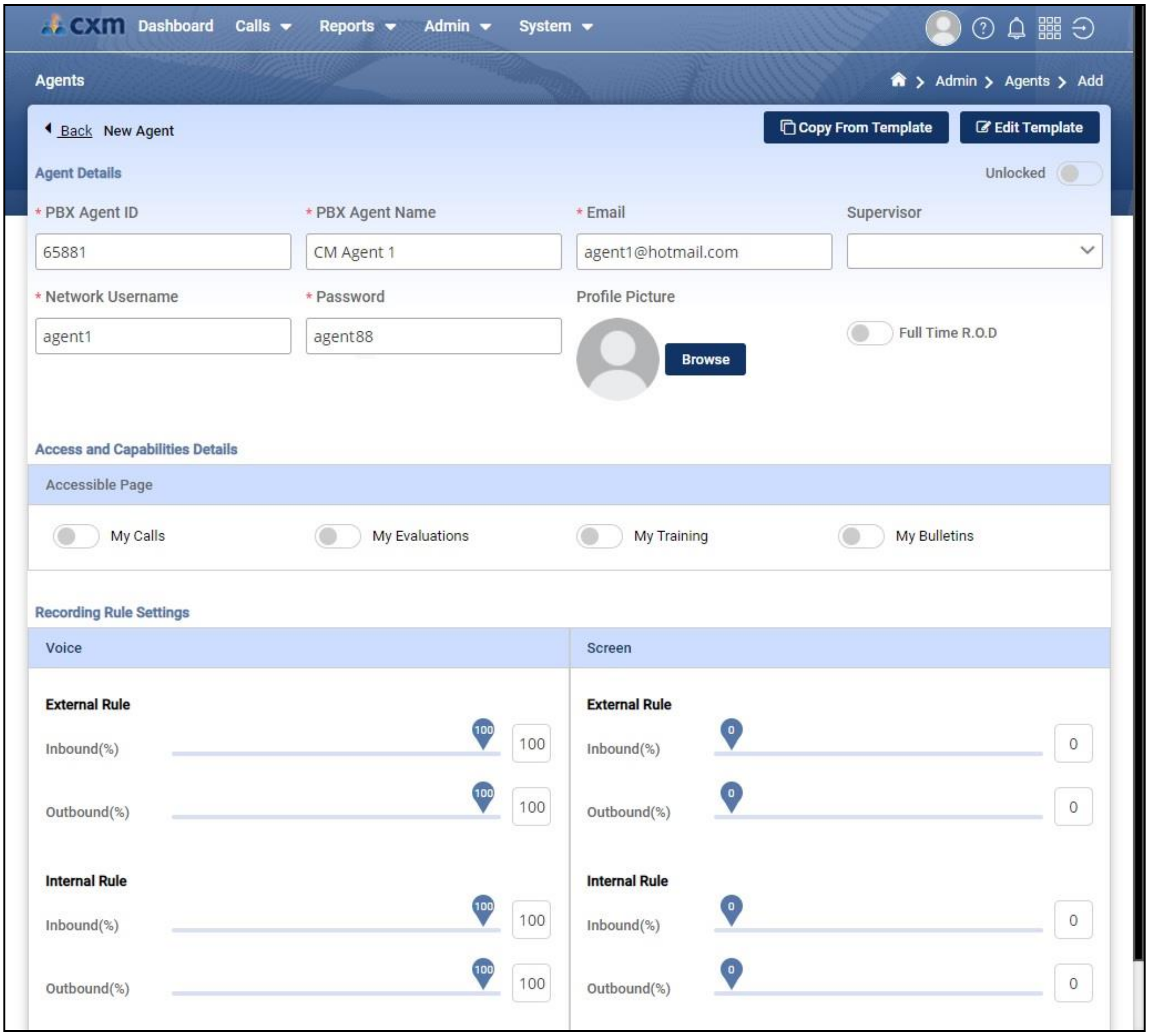
Sampling(%): 100

8.7. Administer Agents

Select **Admin → Agents** from the top menu followed by **Create Agent** (not shown) to display the screen below. Enter the following values for the specified fields, and retain the default values in the remaining fields.

- **PBX Agent ID:** The first agent ID from **Section 3**.
- **PBX Agent Name:** A desired agent name.
- **Email:** An applicable agent email.
- **Network Username:** A desired user name for the agent.
- **Password:** A desired password for the agent.

In the **Voice** subsection, adjust the scroll bars to set desired percentage for types of calls to be recorded. In the compliance testing, all percentages were set to 100 for recording of all call types. Repeat this section to configure all agent IDs from **Section 3**. In the compliance testing, two agent IDs with numbers "65881" and "65882" were created.



Agent Details

Unlocked

* PBX Agent ID	* PBX Agent Name	* Email	Supervisor
65881	CM Agent 1	agent1@hotmail.com	

* Network Username	* Password	Profile Picture	
agent1	agent88		Full Time R.O.D

Access and Capabilities Details

Accessible Page

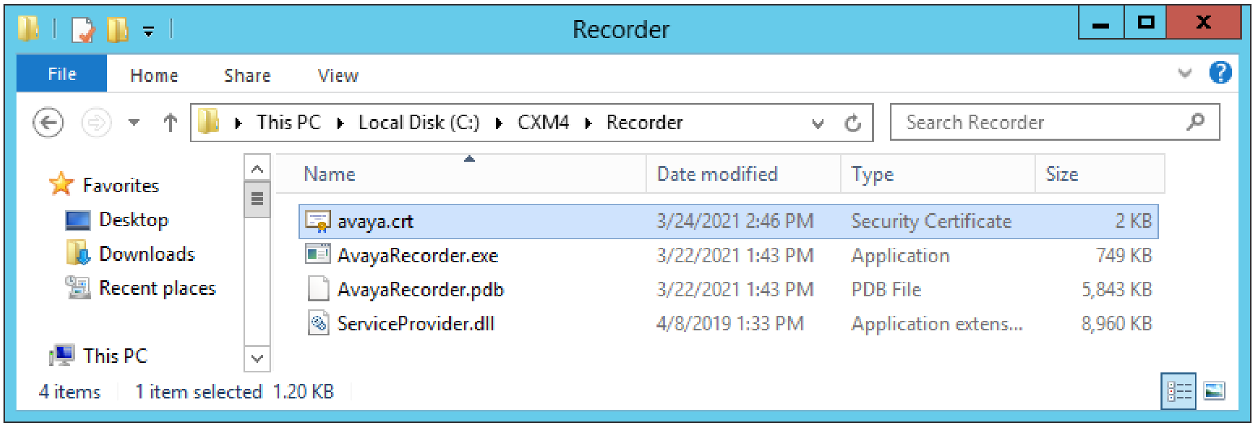
○ My Calls ○ My Evaluations ○ My Training ○ My Bulletins

Recording Rule Settings

Voice		Screen	
External Rule		**External Rule**	
Inbound(%)	100	Inbound(%)	0
Outbound(%)	100	Outbound(%)	0
Internal Rule		**Internal Rule**	
Inbound(%)	100	Inbound(%)	0
Outbound(%)	100	Outbound(%)	0

8.8. Install CA Certificate

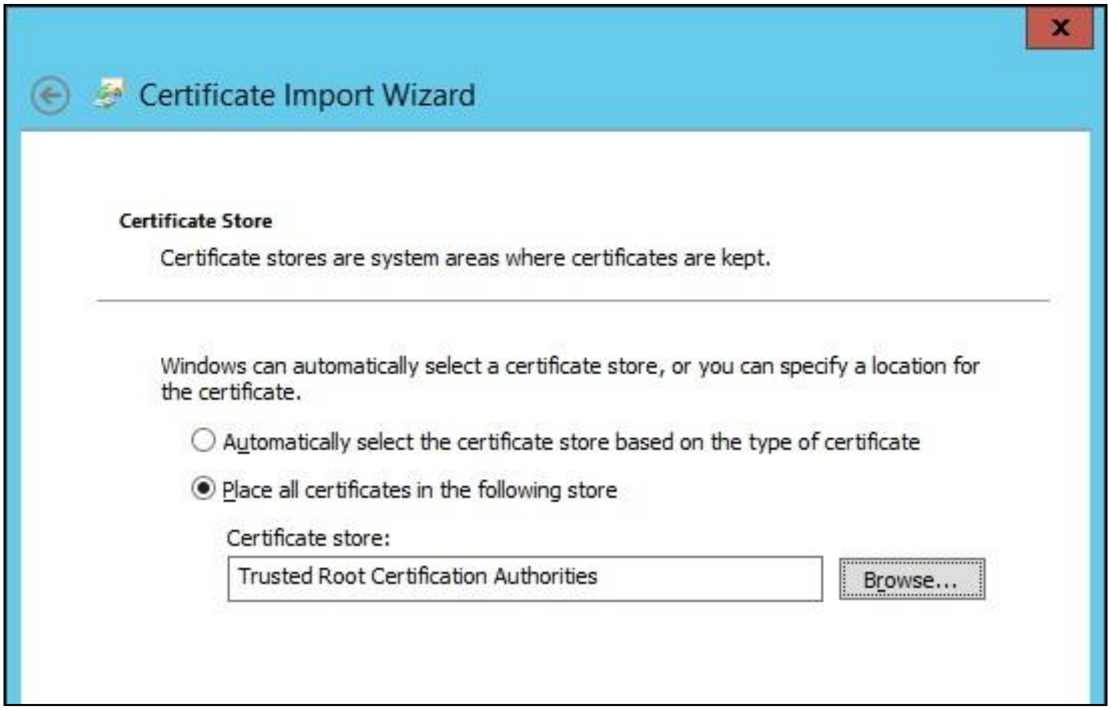
From the CXM server, navigate to **C:\CXM4\Recorder**, and place the CA certificate **avaya.crt** from **Section 6.10** under this directory. Double click on **avaya.crt** to install the certificate.



Name	Date modified	Type	Size
avaya.crt	3/24/2021 2:46 PM	Security Certificate	2 KB
AvayaRecorder.exe	3/22/2021 1:43 PM	Application	749 KB
AvayaRecorder.pdb	3/22/2021 1:43 PM	PDB File	5,843 KB
ServiceProvider.dll	4/8/2019 1:33 PM	Application extens...	8,960 KB

4 items   1 item selected 1.20 KB

When the **Certificate Import Wizard** screen below is displayed, select **Place all certificates in the following store**, followed by **Trusted Root Certification Authorities** in the subsequent **Browse** pop-up window (not shown).



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

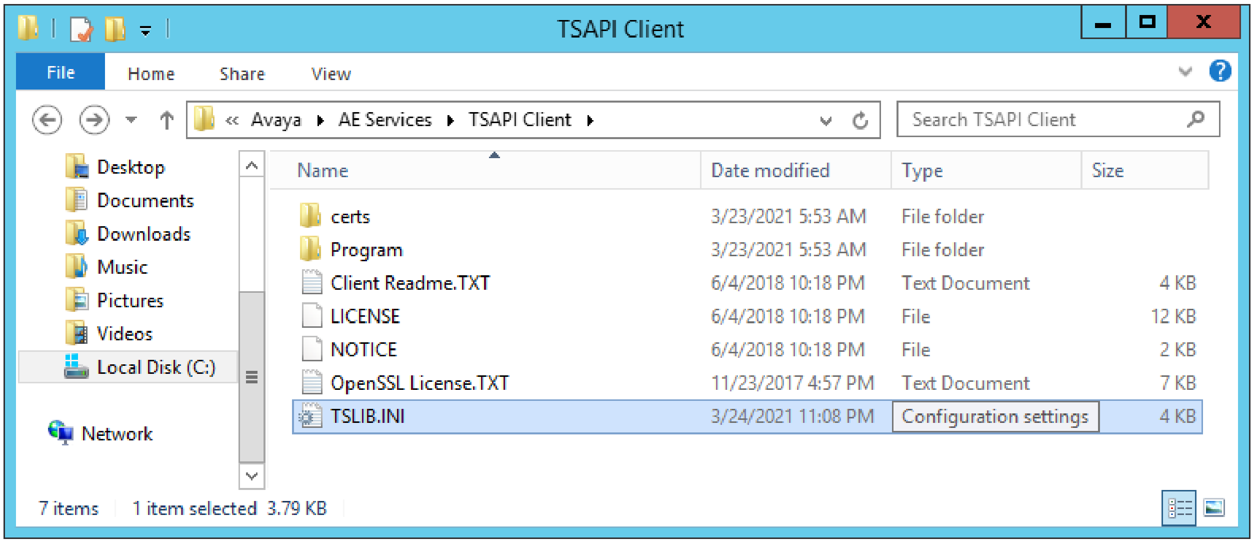
● Place all certificates in the following store

Certificate store:

Trusted Root Certification Authorities

8.9. Administer TSLIB.INI

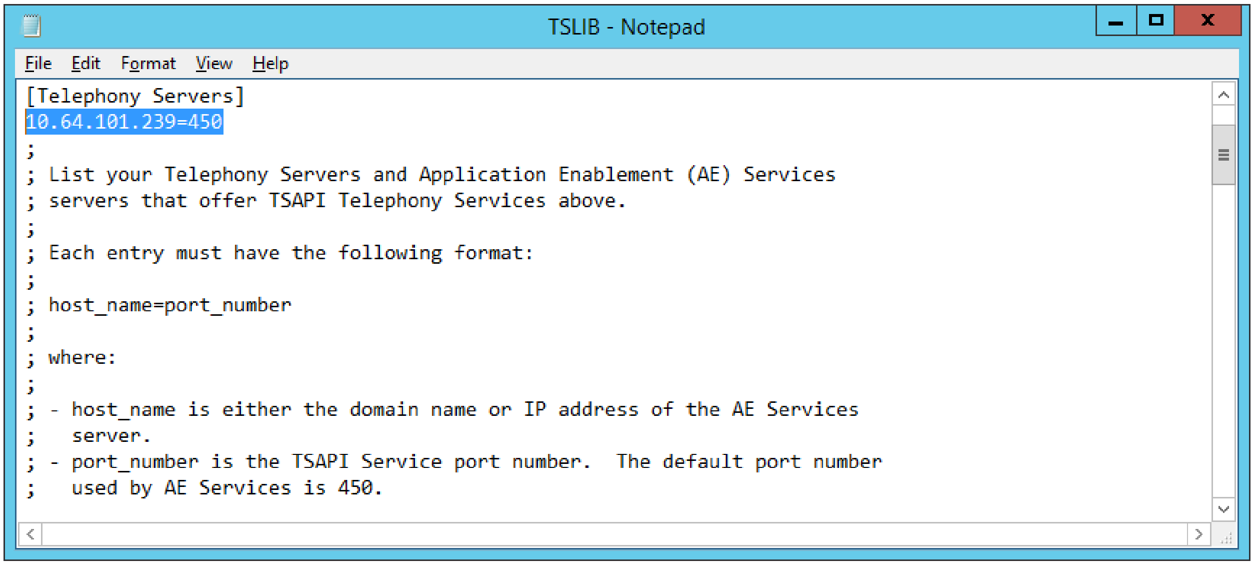
From the CXM server, navigate to **C:\Program Files (x86)\Avaya\AE Services\TSAPI Client** to edit the **TSLIB.INI** file shown below.



Name	Date modified	Type	Size
certs	3/23/2021 5:53 AM	File folder	
Program	3/23/2021 5:53 AM	File folder	
Client Readme.TXT	6/4/2018 10:18 PM	Text Document	4 KB
LICENSE	6/4/2018 10:18 PM	File	12 KB
NOTICE	6/4/2018 10:18 PM	File	2 KB
OpenSSL License.TXT	11/23/2017 4:57 PM	Text Document	7 KB
TSLIB.INI	3/24/2021 11:08 PM	Configuration settings	4 KB

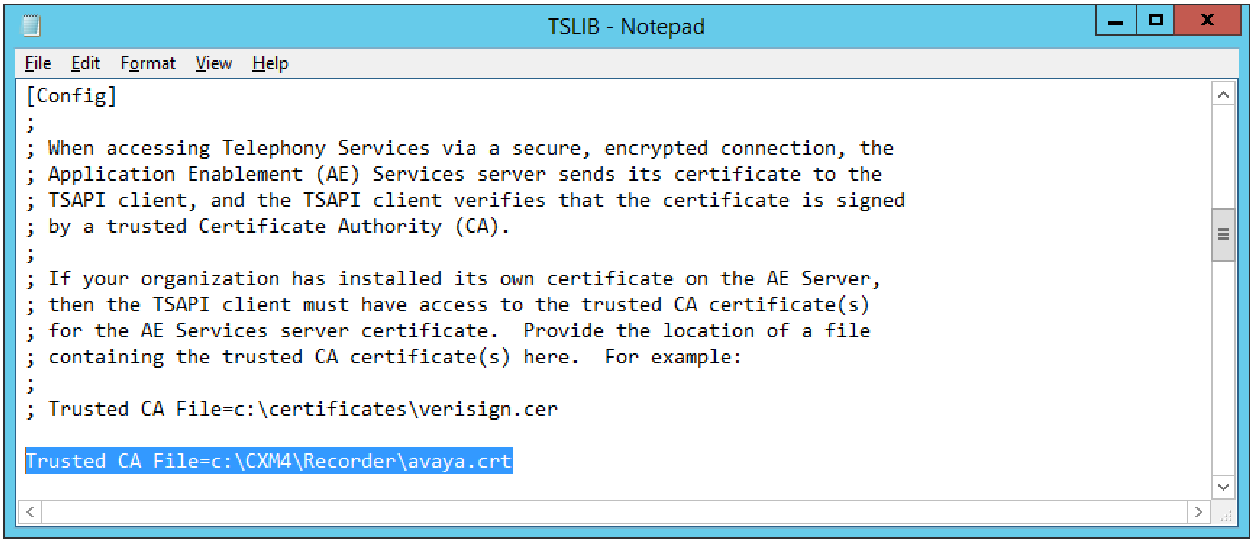
7 items 1 item selected 3.79 KB

In the **Telephony Servers** subsection, enter an entry shown below, where “10.64.101.239” is the IP address of Application Enablement Services.



```
[Telephony Servers]
10.64.101.239=450
;
; List your Telephony Servers and Application Enablement (AE) Services
; servers that offer TSAPI Telephony Services above.
;
; Each entry must have the following format:
;
; host_name=port_number
;
; where:
;
; - host_name is either the domain name or IP address of the AE Services
;   server.
; - port_number is the TSAPI Service port number.  The default port number
;   used by AE Services is 450.
```

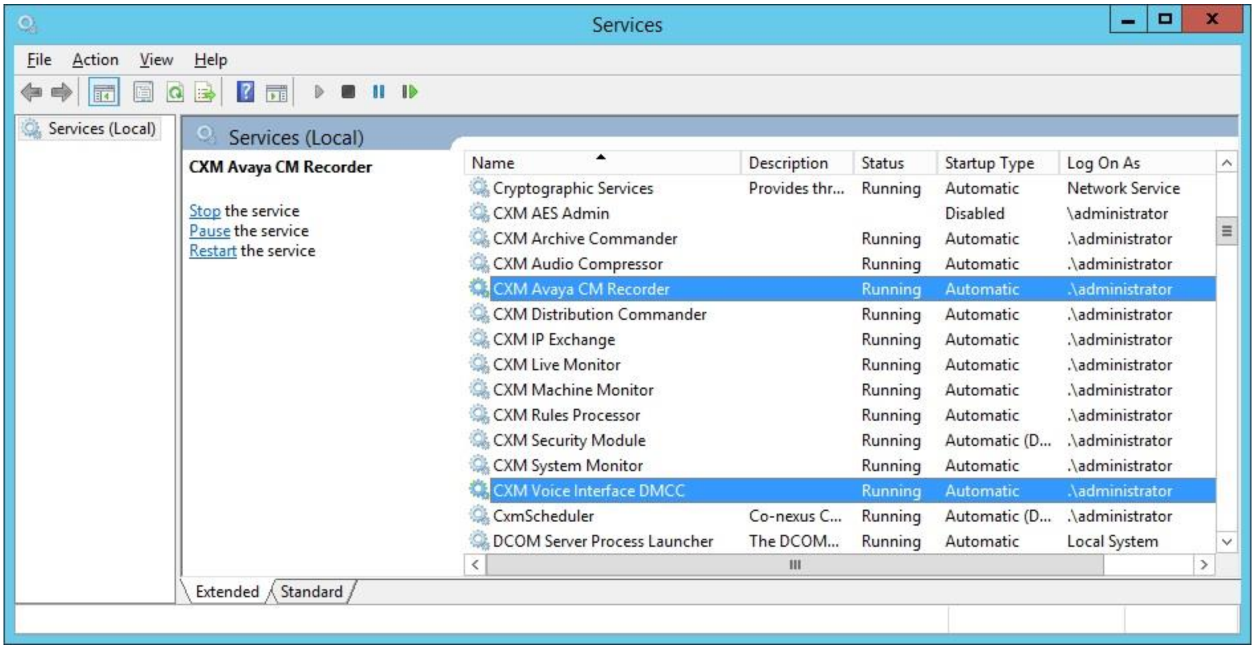
Scroll down to the **Config** subsection, enter an entry shown below, where "c:\CXM4\Recorder\avaya.crt" is the path to the CA certificate from **Section 8.8**.



```
[Config]
;
; When accessing Telephony Services via a secure, encrypted connection, the
; Application Enablement (AE) Services server sends its certificate to the
; TSAPI client, and the TSAPI client verifies that the certificate is signed
; by a trusted Certificate Authority (CA).
;
; If your organization has installed its own certificate on the AE Server,
; then the TSAPI client must have access to the trusted CA certificate(s)
; for the AE Services server certificate.  Provide the location of a file
; containing the trusted CA certificate(s) here.  For example:
;
; Trusted CA File=c:\certificates\verisign.cer

Trusted CA File=c:\CXM4\Recorder\avaya.crt
```

8.10. Restart CXM Services

From the CXM server, select **Start → Administrative Tools → Services** to display the **Services** screen. Restart the **CXM Avaya CM Recorder** and the **CXM Voice Interface DMCC** services shown below.



Name	Description	Status	Startup Type	Log On As
Cryptographic Services	Provides thr...	Running	Automatic	Network Service
CXM AES Admin			Disabled	\administrator
CXM Archive Commander		Running	Automatic	.\administrator
CXM Audio Compressor		Running	Automatic	.\administrator
CXM Avaya CM Recorder		Running	Automatic	.\administrator
CXM Distribution Commander		Running	Automatic	.\administrator
CXM IP Exchange		Running	Automatic	.\administrator
CXM Live Monitor		Running	Automatic	.\administrator
CXM Machine Monitor		Running	Automatic	.\administrator
CXM Rules Processor		Running	Automatic	.\administrator
CXM Security Module		Running	Automatic (D...	.\administrator
CXM System Monitor		Running	Automatic	.\administrator
CXM Voice Interface DMCC		Running	Automatic	.\administrator
CxmScheduler	Co-nexus C...	Running	Automatic (D...	.\administrator
DCOM Server Process Launcher	The DCOM...	Running	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 status of the administered CTI link by using the “status aesvcs cti-link” command. Verify that the **Service State** is “established” for the CTI link number administered in **Section 5.2**, as shown below.

```
status aesvcs cti-link

                          AE SERVICES CTI LINK STATUS

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

1     12       no    aes7             established   24       24
```

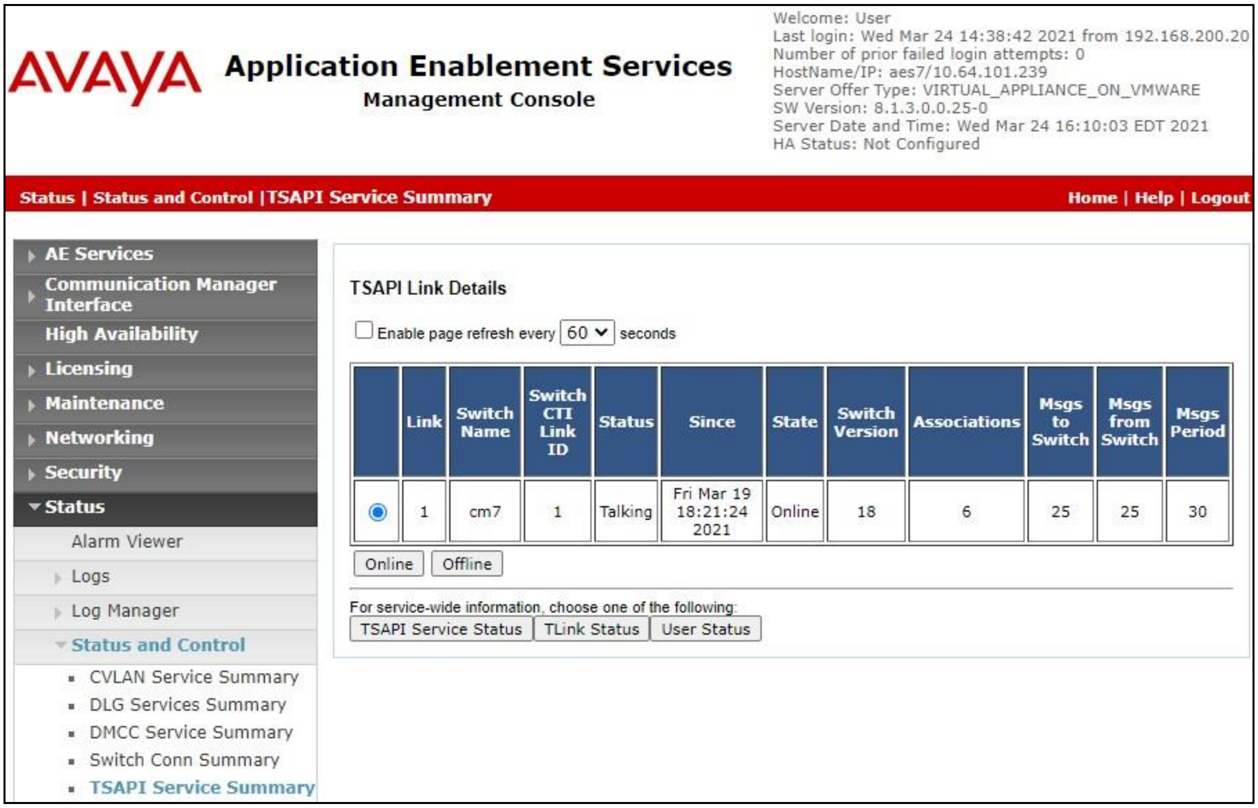
Verify registration status of the virtual IP softphones by using the “list registered-ip-stations” command. Verify that all virtual IP softphone extensions from **Section 5.5** are displayed along with the IP address of the Application Enablement Services server, as shown below.

```
list registered-ip-stations

                            REGISTERED IP STATIONS

Station Ext      Set Type/ Prod ID/    Station IP Address/
or Orig Port     Net Rgn   Release     Gatekeeper IP Address
  Socket
65000            9611      IP_Phone    192.168.200.219
  tls            1         6.8502      10.64.101.236
65001            9611      IP_Phone    192.168.200.125
  tls            1         6.8502      10.64.101.236
65991            4620      IP_API_A    10.64.101.239
  tcp            1         3.2040      10.64.101.236
65992            4620      IP_API_A    10.64.101.239
  tcp            1         3.2040      10.64.101.236
```

9.2. Verify Avaya Aura® Application Enablement Services

On Application Enablement Services, verify 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 **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**, in this case "6".



Welcome: User
Last login: Wed Mar 24 14:38:42 2021 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: 8.1.3.0.0.25-0
Server Date and Time: Wed Mar 24 16:10:03 EDT 2021
HA Status: Not Configured

TSAPI Link Details

☐ Enable page refresh every 60 seconds

	Link	Switch Name	Switch CTI Link ID	Status	Since	State	Switch Version	Associations	Msgs to Switch	Msgs from Switch	Msgs Period
●	1	cm7	1	Talking	Fri Mar 19 18:21:24 2021	Online	18	6	25	25	30

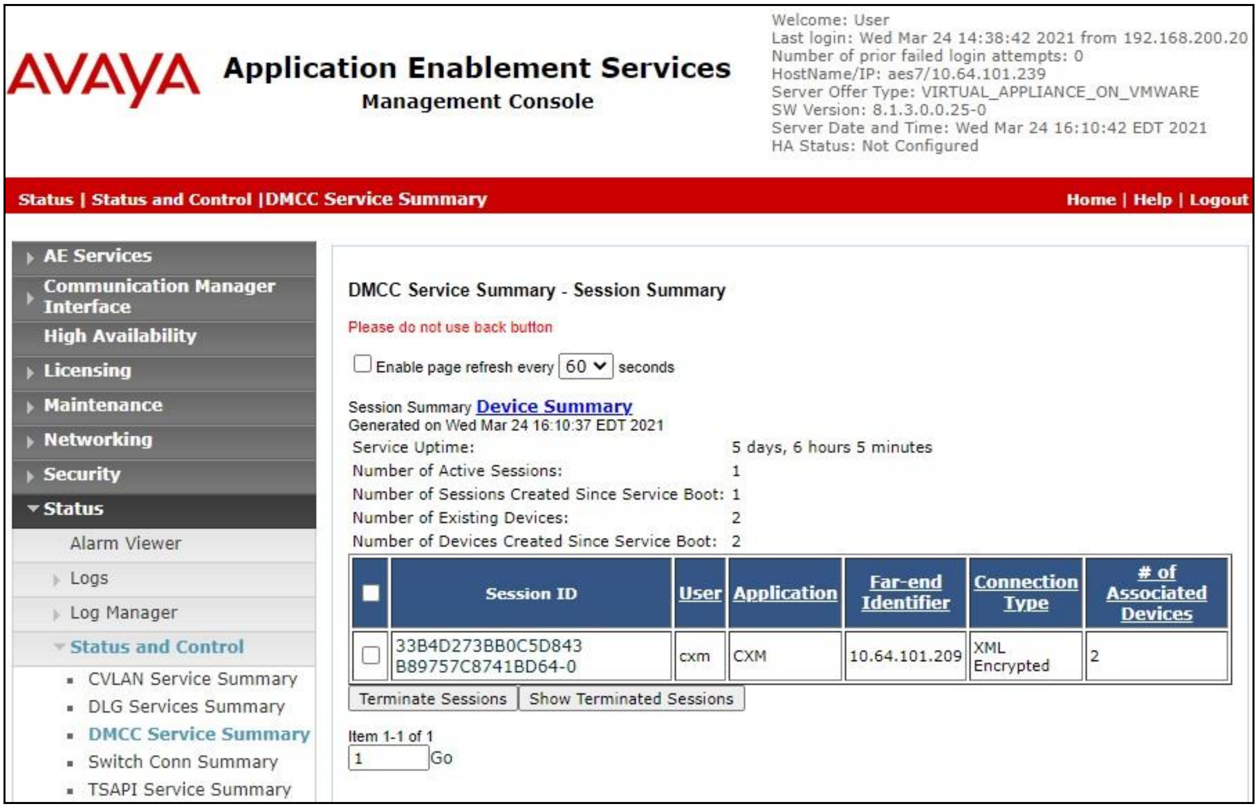
Online | Offline

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

TSAPI Service Status | TLink Status | User Status

Verify 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 5.5**.



Welcome: User
Last login: Wed Mar 24 14:38:42 2021 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: 8.1.3.0.0.25-0
Server Date and Time: Wed Mar 24 16:10:42 EDT 2021
HA Status: Not Configured

DMCC Service Summary - Session Summary

Please do not use back button

☐ Enable page refresh every 60 seconds

Session Summary Device Summary
Generated on Wed Mar 24 16:10:37 EDT 2021

Service Uptime:	5 days, 6 hours 5 minutes
Number of Active Sessions:	1
Number of Sessions Created Since Service Boot:	1
Number of Existing Devices:	2
Number of Devices Created Since Service Boot:	2

☐	Session ID	User	Application	Far-end Identifier	Connection Type	# of Associated Devices
☐	33B4D273BB0C5D843 B89757C8741BD64-0	cxm	CXM	10.64.101.209	XML Encrypted	2

Terminate Sessions | Show Terminated Sessions

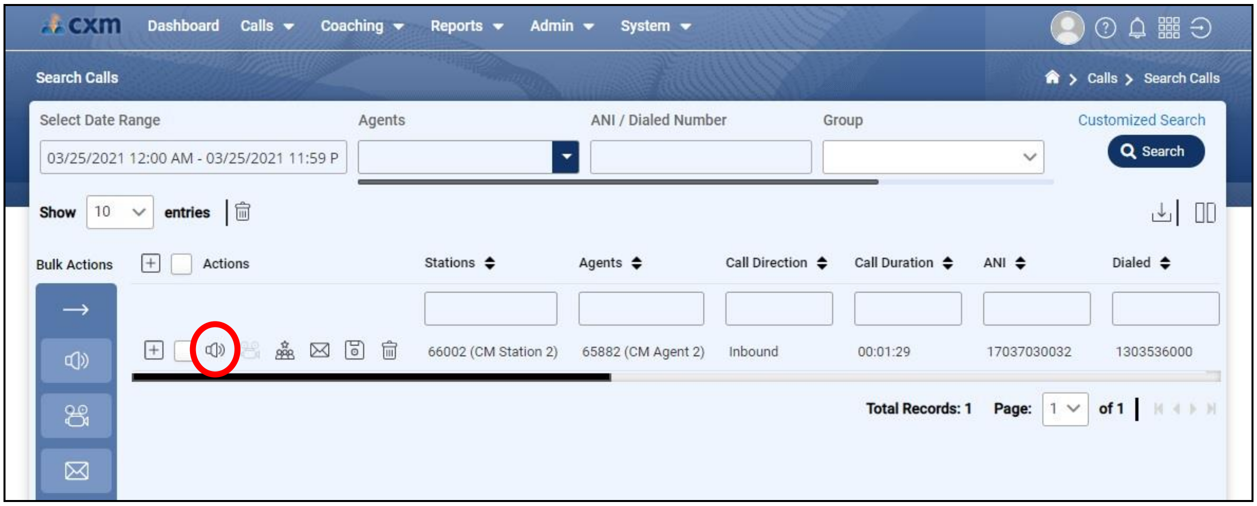
Item 1-1 of 1
1 Go

9.3. Verify TeleComp 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 CXM web interface and log in using an appropriate credential. The screen below is displayed.

Click on **Calls → Search Calls** from the top menu followed by **Search** (not shown) in the subsequent screen to display a list of call recording entries for the current day.

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 **Play Audio** icon shown below.



Select Date Range: 03/25/2021 12:00 AM - 03/25/2021 11:59 P

Agents

ANI / Dialed Number

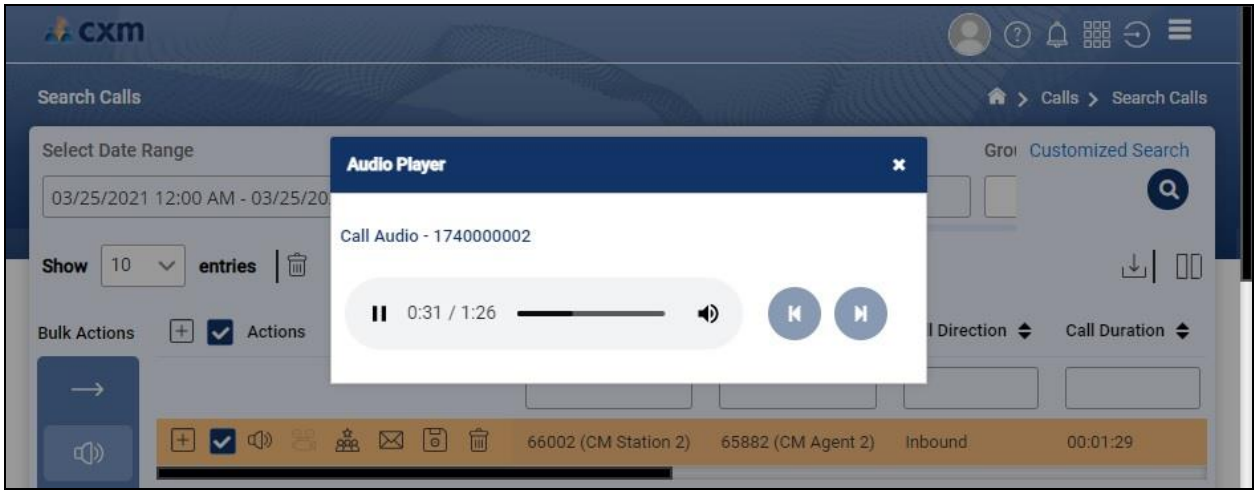
Group

Show 10 entries

Stations	Agents	Call Direction	Call Duration	ANI	Dialed
66002 (CM Station 2)	65882 (CM Agent 2)	Inbound	00:01:29	17037030032	1303536000

Total Records: 1 Page: 1 of 1

Verify that the recording can be played back.



Select Date Range: 03/25/2021 12:00 AM - 03/25/20

Show 10 entries

Call Audio - 1740000002

0:31 / 1:26

l Direction	Call Duration
66002 (CM Station 2) 65882 (CM Agent 2) Inbound	00:01:29

10. Conclusion

These Application Notes describe the configuration steps required for TeleComp CXM 6.1.5.1 to successfully interoperate with Avaya Aura® Communication Manager 8.1.3 and Avaya Aura® Application Enablement Services 8.1.3. 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 8.1.x, Issue 8, November 2020, available at http://support.avaya.com.

2. *Administering Avaya Aura® Application Enablement Services*, Release 8.1.x, Issue 8, December 2020, available at http://support.avaya.com.

3. *CXM Recording and Quality Monitoring Administration Guide*, Release 6.0, available from CXM 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.