



## **Avaya Solution & Interoperability Test Lab**

---

# **Application Notes for CXM 5.3 with Avaya Aura® Communication Manager 8.0 and Avaya Aura® Application Enablement Services 8.0 – Issue 1.0**

## **Abstract**

These Application Notes describe the configuration steps required for CXM 5.3 to interoperate with Avaya Aura® Communication Manager 8.0 and Avaya Aura® Application Enablement Services 8.0. 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 call center devices on Avaya Aura® Communication Manager, and to capture the 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 CXM 5.3 to interoperate with Avaya Aura® Communication Manager 8.0 and Avaya Aura® Application Enablement Services 8.0. 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 Application Enablement Services to monitor call center devices on Communication Manager, and to capture the 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 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.

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 the following were observations on CXM:

- By design, CXM produces cradle to grave recording, with call continued to be recorded even after the monitored agent has left the call. An example is after a monitored agent transfers an ACD call to a non-monitored supervisor, the virtual IP softphone stayed on the call to capture the conversation between the non-monitored supervisor with the PSTN. As such, the provisioning on the number of virtual IP softphones needs to take this design into account.
- By design, an internal call between two monitored agents produced two recording entries with the same audio and call duration, and the reported direction is Outbound for both entries.
- The application assumes all virtual IP softphones can register without problems. Should the first virtual IP softphone registration fail due to invalid credential, 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 may not be able to 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](mailto:support@cxmrecord.com)
- **Web :** <http://www.cxmrecord.com>

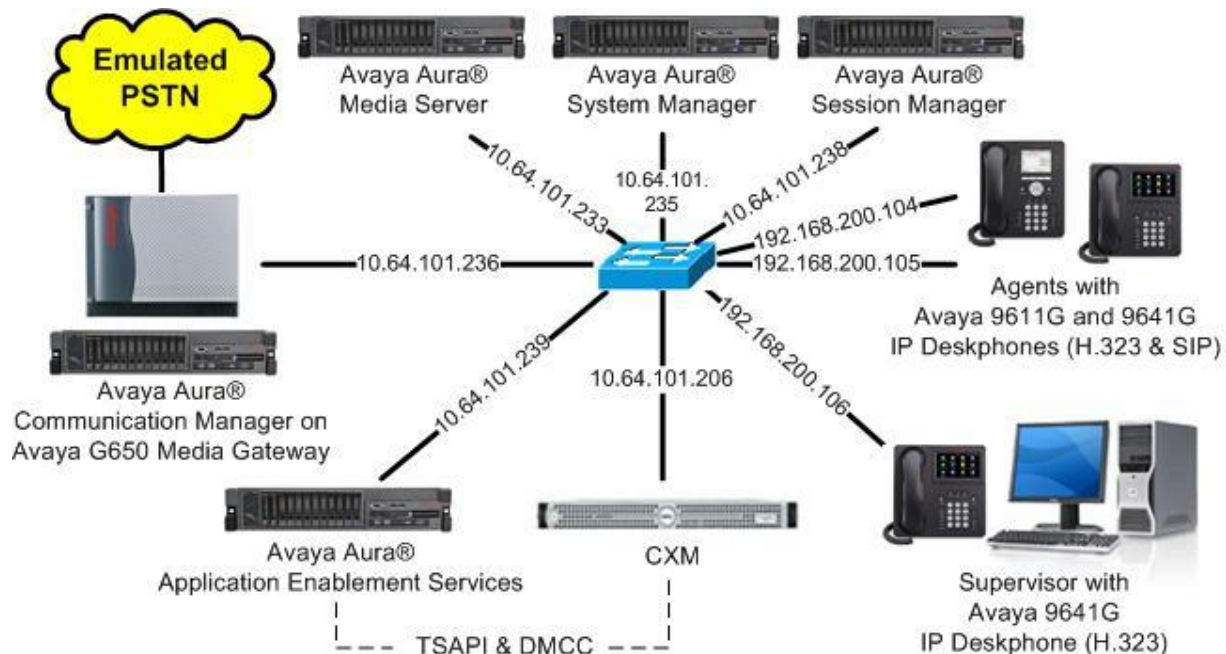
### 3. Reference Configuration

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, 66006
Agent ID	65881, 65882



**Figure 1: Compliance Testing Configuration**

## 4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya Aura® Communication Manager in Virtual Environment	8.0 (8.0.0.1.2.822.24826)
Avaya G650 Media Gateway	NA
Avaya Aura® Media Server in Virtual Environment	8.0 (8.0.0.150)
Avaya Aura® Application Enablement Services in Virtual Environment	8.0 (8.0.0.0.0.6-0)
Avaya Aura® Session Manager in Virtual Environment	8.0 (8.0.0.0.80035)
Avaya Aura® System Manager in Virtual Environment	8.0 (8.0.0.0.098174)
Avaya 9611G & 9641G IP Deskphone (H.323)	6.6604
Avaya 9641G IP Deskphone (SIP)	7.1.3.0.11
CXM on Windows Server 2008 <ul style="list-style-type: none"><li>Avaya TSAPI Windows Client (csta32.dll)</li><li>Avaya DMCC .NET (ServiceProvider.dll)</li></ul>	5.3.3 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 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	<b>Computer Telephony Adjunct Links? y</b>	
ARS/AAR Partitioning? y	Cvg Of Calls Redirected Off-net? y	
ARS/AAR Dialing without FAC? n	DCS (Basic)? y	
ASAI Link Core Capabilities? y	DCS Call Coverage? y	
ASAI Link Plus Capabilities? y	DCS with Rerouting? y	

### 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		
<b>Extension: 60111</b>		
<b>Type: ADJ-IP</b>		
COR: 1		
<b>Name: AES CTI Link</b>		

### 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 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 UI 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
```



## 5.4. 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 65991
```

Page 1 of 5

STATION		
<b>Extension: 65991</b>	Lock Messages? n	BCC: 0
<b>Type: 4620</b>	<b>Security Code: 123456</b>	TN: 1
Port: IP	Coverage Path 1:	COR: 1
<b>Name: CXM Virtual 1</b>	Coverage Path 2:	COS: 1
	Hunt-to Station:	Tests: y

STATION OPTIONS

Location:	Time of Day Lock Table:
Loss Group: 19	Personalized Ringing Pattern: 1
	Message Lamp Ext: 65991
Speakerphone: 2-way	Mute Button Enabled? y
Display Language: english	Expansion Module? n
Survivable GK Node Name:	
Survivable COR: internal	Media Complex Ext:
Survivable Trunk Dest? y	<b>IP SoftPhone? y</b>
	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/ Hunt-to	Port/ Type	Name/ Surv GK NN	Move	Cable	Room/ Jack	Cv1/ Cv2 COR/ COS TN
<b>65991</b>	<b>S00013</b>	<b>CXM Virtual 1</b>				<b>1</b>
	<b>4620</b>		<b>no</b>			<b>1 1</b>
<b>65992</b>	<b>S00016</b>	<b>CXM Virtual 2</b>				<b>1</b>
	<b>4620</b>		<b>no</b>			<b>1 1</b>

## 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											
Name (22 characters)	Ext/Skills	VDN			Vec		Orig		Evt		
		Ovr	COR	TN	PRT	Num	Meas	Annc	Noti	Adj	
<b>CM Sales</b>	<b>60001</b>	<b>n</b>	<b>1</b>	<b>1</b>	<b>V</b>	<b>1</b>	<b>none</b>				
<b>CM Support</b>	<b>60002</b>	<b>n</b>	<b>1</b>	<b>1</b>	<b>V</b>	<b>2</b>	<b>none</b>				

## 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	Name/	Grp	ACD/	No. Cov			Notif/		Dom	Message		
No.	Ext	Type	MEAS Vec MCH	Que	Mem	Path	Ctg	Adj	Ctrl	Center		
<b>1</b>	<b>CM Sales Skill</b>											
	<b>61001</b>	<b>ucd-mia</b>	<b>y/I</b>	<b>SK</b>	<b>none</b>	<b>y</b>	<b>0</b>	<b>n</b>		<b>n</b>		
<b>2</b>	<b>CM Support Skill</b>											
	<b>61002</b>	<b>ucd-mia</b>	<b>y/I</b>	<b>SK</b>	<b>none</b>	<b>y</b>	<b>0</b>	<b>n</b>		<b>n</b>		

## 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/ Hunt-to	Port/ Type	Name/ Surv GK NN	Move	Cable	Room/ Jack	Cv1/ Cv2	COR/ COS	TN	
65000	S00002	CM Supervisor				7	1		
	9641		no				1	1	
<b>65001</b>	<b>S00102</b>	<b>CM Station 1</b>				<b>1</b>	<b>1</b>		
	<b>9611</b>		<b>no</b>				<b>1</b>	<b>1</b>	
65991	S00013	CXM Virtual 1					1		
	4620		no				1	1	
65992	S00016	CXM Virtual 2					1		
	4620		no				1	1	
<b>66006</b>	<b>S00018</b>	<b>Avaya, SIP 6</b>					<b>1</b>		
	<b>9641SIPCC</b>		<b>no</b>				<b>1</b>	<b>1</b>	

## 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	AgPr	SO	
	Skil/Lv	Skil/Lv	Skil/Lv	Skil/Lv	Skil/Lv	Skil/Lv	Skil/Lv	Skil/Lv	
<b>65881</b>	<b>CM Agent 1</b>	<b>unstaffed</b>					<b>1</b>	<b>lv1</b>	
	<b>1/01</b>	<b>2/01</b>	<b>/</b>	<b>/</b>	<b>/</b>	<b>/</b>	<b>/</b>	<b>/</b>	
<b>65882</b>	<b>CM Agent 2</b>	<b>unstaffed</b>					<b>1</b>	<b>lv1</b>	
	<b>1/01</b>	<b>2/01</b>	<b>/</b>	<b>/</b>	<b>/</b>	<b>/</b>	<b>/</b>	<b>/</b>	

## 6. Configure Avaya Aura® Application Enablement Services

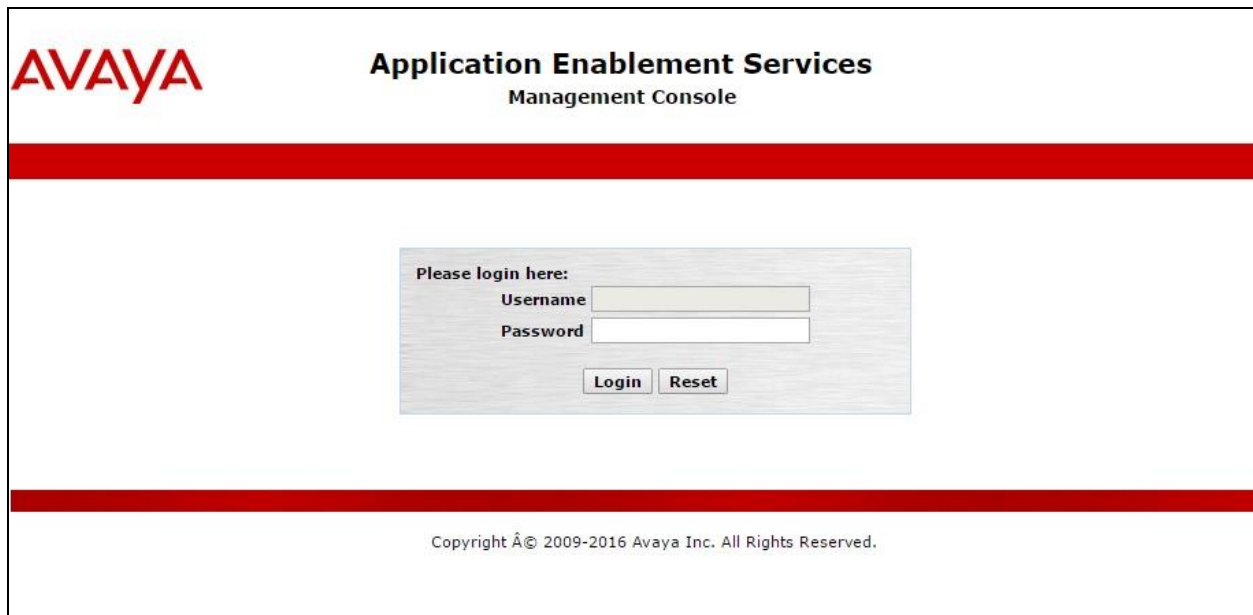
This section provides the procedures for configuring Application Enablement Services. The procedures include the following areas:

- 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.



The screenshot shows the Avaya Application Enablement Services Management Console login interface. At the top left is the Avaya logo. To its right, the text "Application Enablement Services" is displayed in a large, bold font, with "Management Console" in a smaller font below it. A thick red horizontal bar spans the width of the page. Below this bar is a light gray rectangular box containing the login form. The form has the heading "Please login here:" followed by two input fields: "Username" and "Password". Below these fields are two buttons: "Login" and "Reset". Another thick red horizontal bar is located below the login box. At the bottom of the page, centered, is the copyright notice: "Copyright © 2009-2016 Avaya Inc. All Rights Reserved."

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

The screenshot displays the Avaya Application Enablement Services Management Console. The top header includes the Avaya logo and the title "Application Enablement Services Management Console". A red navigation bar at the top contains "Home", "Help", and "Logout" links. On the left, a sidebar lists various services: AE Services, Communication Manager Interface, High Availability, Licensing, Maintenance, Networking, Security, Status, User Management, Utilities, and Help. The main content area is titled "Welcome to OAM" and provides an overview of the console's purpose and the administrative domains it manages. It lists several domains: AE Services, Communication Manager Interface, High Availability, Licensing, Maintenance, Networking, Security, Status, User Management, Utilities, and Help, each with a brief description of its function. A note at the bottom states that these domains can be managed by a single administrator or separate administrators.

Welcome: User  
Last login: Tue Nov 20 10:04:45 2018 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: 8.0.0.0.6-0  
Server Date and Time: Tue Nov 27 10:26:29 EST 2018  
HA Status: Not Configured

Home | Help | Logout

**AE Services**  
Communication Manager Interface  
High Availability  
Licensing  
Maintenance  
Networking  
Security  
Status  
User Management  
Utilities  
Help

### 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).

The screenshot displays the Avaya Application Enablement Services Management Console with the "Licensing" section selected in the left sidebar. The main content area is titled "Licensing" and provides instructions on how to set up and maintain the WebLM. It lists three steps: 1. WebLM Server Address, 2. WebLM Server Access, and 3. Reserved Licenses. Each step includes a brief description of the task. The sidebar on the left shows the "Licensing" section expanded, with "WebLM Server Access" highlighted. The top header and navigation bar are the same as in the previous screenshot.

Welcome: User  
Last login: Tue Nov 20 10:04:45 2018 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: 8.0.0.0.6-0  
Server Date and Time: Tue Nov 27 10:27:19 EST 2018  
HA Status: Not Configured

Home | Help | Logout

**AE Services**  
Communication Manager Interface  
High Availability  
Licensing  
WebLM Server Address  
WebLM Server Access  
Reserved Licenses  
Maintenance  
Networking

### 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.

The screenshot shows the Avaya Aura System Manager 8.0 interface. The left pane displays a navigation tree with the following items: WebLM Home, Install license, Licensed products, APPL\_ENAB, Application\_Enablement (expanded), View by feature, View by local WebLM, Enterprise configuration, Local WebLM Configuration, Usages, Allocations, Periodic status, COMMUNICATION\_MANAGER, Call\_Center, Communication\_Manager, MESSAGING, Messaging, and MSR. The right pane shows the 'Application Enablement (CTI) - Release: 8 - SID: 10503000 (Enterprise license file)' screen. It includes a breadcrumb trail: 'You are here: Licensed Products > Application\_Enablement > View by Feature'. Below this, it states 'License installed on: October 13, 2018 3:09:09 AM +00:00' and 'License File Host IDs: V4-42-5D-06-BF-08-01'. A table lists the features and their license capacities:

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**.

The screenshot shows the AVAYA Application Enablement Services Management Console. The top header includes the AVAYA logo and the title "Application Enablement Services Management Console". On the right, a welcome message for the user is displayed, including login details and system status. The left navigation pane shows a tree structure with "AE Services" expanded, and "TSAPI" selected. Under "TSAPI", "TSAPI Links" is highlighted. The main content area is titled "TSAPI Links" and contains a table with columns: "Link", "Switch Connection", "Switch CTI Link #", "ASAI Link Version", and "Security". Below the table are buttons for "Add Link", "Edit Link", and "Delete Link".

The **Add TSAPI Links** screen is displayed next.

The **Link** field is only local to the Application Enablement Services server, and may be set to any available number. For **Switch Connection**, select the relevant switch connection from the drop-down list. In this case, the existing switch connection “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.

The screenshot shows the AVAYA Application Enablement Services Management Console with the "Add TSAPI Links" screen. The left navigation pane shows "AE Services" expanded, and "TSAPI" selected. Under "TSAPI", "TSAPI Links" is highlighted. The main content area is titled "Add TSAPI Links" and contains a form with the following fields: "Link" (dropdown menu with value 1), "Switch Connection" (dropdown menu with value cm7), "Switch CTI Link Number" (dropdown menu with value 1), "ASAI Link Version" (dropdown menu with value 9), and "Security" (dropdown menu with value Encrypted). Below the form are buttons for "Apply Changes" and "Cancel Changes".



## 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**.

The screenshot shows the Avaya Application Enablement Services Management Console. The left navigation pane is expanded to 'Communication Manager Interface' and 'Switch Connections'. The main content area displays a table of switch connections. The table has four columns: Connection Name, Processor Ethernet, Msg Period, and Number of Active Connections. The first row shows 'cm7' with 'Yes' for Processor Ethernet, '30' for Msg Period, and '1' for Number of Active Connections. Below the table are buttons for 'Edit Connection', 'Edit PE/CLAN IPs', 'Edit H.323 Gatekeeper', 'Delete Connection', and 'Survivability Hierarchy'. The top right corner shows system information: Welcome: User, Last login: Tue Nov 20 10:04:45 2018 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: 8.0.0.0.6-0, Server Date and Time: Tue Nov 27 10:31:01 EST 2018, HA Status: Not Configured.

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections
<input checked="" type="radio"/> 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**.

The screenshot shows the Avaya Application Enablement Services Management Console. The left navigation pane is expanded to 'Communication Manager Interface' and 'Switch Connections'. The main content area displays the 'Edit H.323 Gatekeeper - cm7' screen. It has a text input field containing '10.64.101.236' and a button 'Add Name or IP'. Below the input field are buttons for 'Delete IP' and 'Back'. The top right corner shows system information: Welcome: User, Last login: Tue Nov 20 10:04:45 2018 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: 8.0.0.0.6-0, Server Date and Time: Tue Nov 27 10:31:29 EST 2018, HA Status: Not Configured.



## 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.

**AVAYA** **Application Enablement Services**  
Management Console

Welcome: User  
Last login: Tue Nov 20 10:04:45 2018 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: 8.0.0.0.0.6-0  
Server Date and Time: Tue Nov 27 10:33:13 EST 2018  
HA Status: Not Configured

User Management | User Admin | Add User

Home | Help | Logout

AE Services

Communication Manager Interface

High Availability

Licensing

Maintenance

Networking

Security

Status

User Management

Service Admin

User Admin

Add User

Change User Password

List All Users

Modify Default Users

Search Users

Utilities

Help

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**.

The screenshot displays the Avaya Application Enablement Services Management Console. The top header includes the Avaya logo and the title "Application Enablement Services Management Console". A welcome message in the top right corner states: "Welcome: User", "Last login: Tue Nov 20 10:04:45 2018 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: 8.0.0.0.6-0", "Server Date and Time: Tue Nov 27 10:34:07 EST 2018", and "HA Status: Not Configured".

The main navigation bar is red and contains the text "Security | Security Database | Control" on the left and "Home | Help | Logout" on the right. The left sidebar is a dark grey menu with the following items: "AE Services", "Communication Manager Interface", "High Availability", "Licensing", "Maintenance", "Networking", "Security" (expanded), "Account Management", "Audit", "Certificate Management", "Enterprise Directory", "Host AA", "PAM", "Security Database" (expanded), and "Control" (selected).

The main content area is titled "SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services". It contains two unchecked checkboxes: "Enable SDB for DMCC Service" and "Enable SDB for TSAPI Service, JTAPI and Telephony Web Services". Below these checkboxes is an "Apply Changes" button.

## 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.

**AVAYA** Application Enablement Services  
Management Console

Welcome: User  
Last login: Tue Nov 20 10:04:45 2018 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: 8.0.0.0.6-0  
Server Date and Time: Tue Nov 27 10:34:27 EST 2018  
HA Status: Not Configured

Networking | Ports

Home | Help | Logout

▶ AE Services

▶ Communication Manager Interface

▶ High Availability

▶ Licensing

▶ Maintenance

▼ Networking

▶ AE Service IP (Local IP)

▶ Network Configure

▶ Ports

▶ TCP/TLS Settings

▶ Security

▶ Status

▶ User Management

▶ Utilities

▶ Help

Ports

CVLAN Ports

Unencrypted TCP Port9999

Encrypted TCP Port9999

DLG PortTCP Port5678

TSAPI Ports

TSAPI Service Port450

Local TLINK Ports

TCP Port Min1024

TCP Port Max1039

Unencrypted TLINK Ports

TCP Port Min1050

TCP Port Max1065

Encrypted TLINK Ports

TCP Port Min1066

TCP Port Max1081

DMCC Server Ports

Unencrypted Port4721

Encrypted Port4722

TR/87 Port4723

Enabled Disabled

☒ ☐

☒ ☐

☒ ☐

☒ ☐

☒ ☐

☒ ☐

☒ ☐

☒ ☐

☒ ☐

☐ ☒

☐ ☒

☐ ☒

## 6.8. Restart Service

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

**AVAYA** **Application Enablement Services**  
Management Console

Welcome: User  
Last login: Fri Nov 30 14:34:26 2018 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: 8.0.0.0.6-0  
Server Date and Time: Tue Dec 04 15:19:09 EST 2018  
HA Status: Not Configured

Maintenance | Service ControllerHome | Help | Logout

▶ AE Services

▶ Communication Manager Interface

High Availability

▶ Licensing

▼ Maintenance

Date Time/NTP Server

▶ Security Database

Service Controller

▶ Server Data

▶ Networking

▶ Security

▶ Status

Service Controller

Service	Controller Status
<input type="checkbox"/> ASAI Link Manager	Running
<input type="checkbox"/> DMCC Service	Running
<input type="checkbox"/> CVLAN Service	Running
<input type="checkbox"/> DLG Service	Running
<input type="checkbox"/> Transport Layer Service	Running
<input checked="" type="checkbox"/> TSAPI Service	Running

For status on actual services, please use [Status and Control](#)

StartStopRestart ServiceRestart AE ServerRestart LinuxRestart Web Server

## 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.

The screenshot displays the Avaya Application Enablement Services Management Console. The top header includes the Avaya logo and the text "Application Enablement Services Management Console". On the right side of the header, there is a welcome message for the user, including login details and system status. Below the header, a red navigation bar contains the links "Security | Security Database | Tlinks" and "Home | Help | Logout". The left sidebar shows a tree view of the application's structure, with "Security" expanded to show "Security Database", which in turn has "Tlinks" selected. The main content area, titled "Tlinks", shows a single Tlink named "AVAYA#CM7#CSTA-S#AES7" with a "Delete Tlink" button next to it.

Welcome: User  
Last login: Fri Nov 30 14:34:26 2018 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: 8.0.0.0.6-0  
Server Date and Time: Tue Dec 04 15:19:58 EST 2018  
HA Status: Not Configured

Security | Security Database | Tlinks Home | Help | Logout

AE Services  
Communication Manager Interface  
High Availability  
Licensing  
Maintenance  
Networking  
Security  
Account Management  
Audit  
Certificate Management  
Enterprise Directory  
Host AA  
PAM  
Security Database  
Control  
CTI Users  
Devices  
Device Groups  
Tlinks

Tlinks  
Tlink Name  
AVAYA#CM7#CSTA-S#AES7  
Delete Tlink



## 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**.

The screenshot shows the Avaya Application Enablement Services Management Console. The left navigation pane is expanded to 'Security' > 'Certificate Management' > 'CA Trusted Certificates'. The main content area displays a table of CA Trusted Certificates with columns: Alias, Status, Issued To, Issued By, and Expiration Date. The 'SystemManagerCA' certificate is selected.

Alias	Status	Issued To	Issued By	Expiration Date
serverCertDefault	valid	aes7-316871052-labUseOnly	aes7-316871052-labUseOnly	Oct 10, 2019
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.

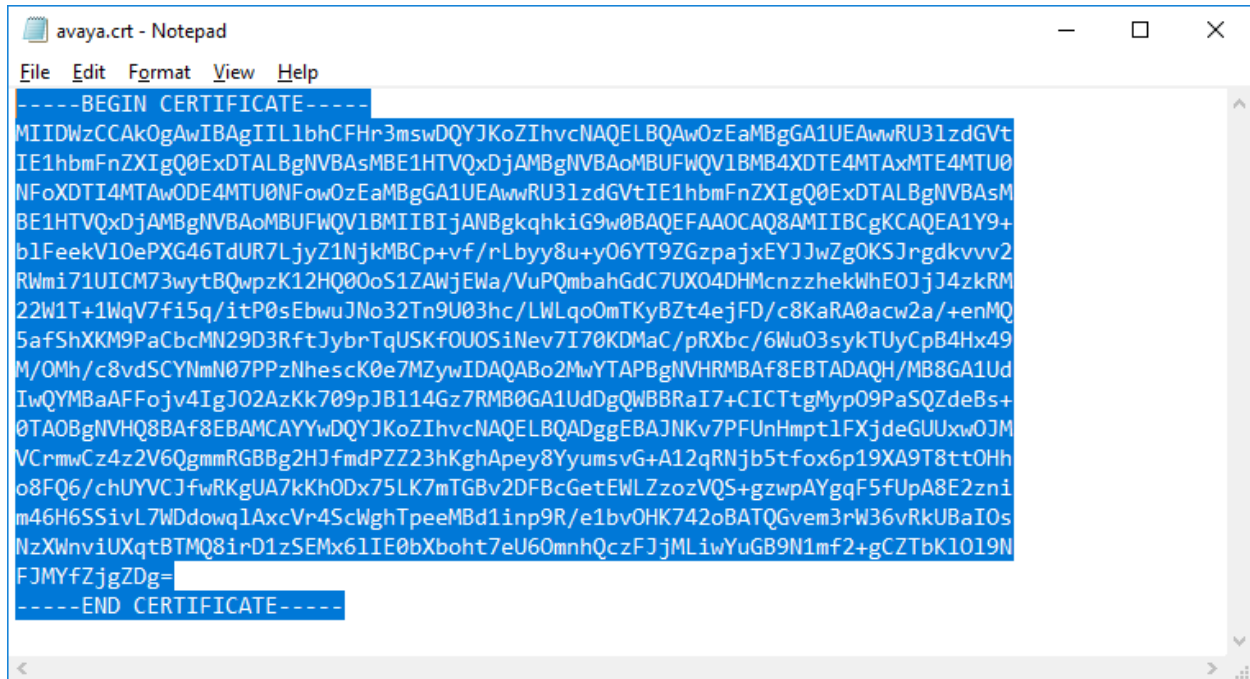
The screenshot shows the Avaya Application Enablement Services Management Console. The left navigation pane is expanded to 'Security' > 'Certificate Management' > 'CA Trusted Certificates'. The main content area displays the 'Trusted Certificate Export' screen for the 'SystemManagerCA' certificate. It shows the 'Issued To', 'Issued By', and 'Expiration Date' information, and a text box containing the certificate's PEM format.

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

**Certificate PEM:**

```
-----BEGIN CERTIFICATE-----
MIIDWzCCAkOgAwIBAgIILbCFHr3mswDQYJKoZIhvcNAQELBQAwOzEaMBGGA1UEAwRU3lzdG
IE1hbmFnZXIgaXQ0ExDjALBgNVBAsMBE1HTVQxODJhbmFnZXIgaXQ0ExDjALBgNVBAsM
BE1HTVQxODJhbmFnZXIgaXQ0ExDjALBgNVBAsMBE1HTVQxODJhbmFnZXIgaXQ0ExDjAL
blFeekVlOePXG46TdUR7LjYzNjNjMBCp+vf/rLbyy8u+yO6YT9ZGzpjxjYJwZgOKSjrgdkv
RWmi71UICM73wyTBQwpzK12HQ00oS1ZAWjEwa/VuPQmbahGdC7UXO4DHMczzhekWhEOJj4;
22W1T+1WqV7fi5q/itP0sEbwuJNo32Tn9U03hc/LWLqoOmTKyBZt4ejFD/c8KaRA0acw2a/+enMQ
5afShXKM9PaCbcMN29D3RftJybrTqUSKfOUOSiNev7I70KDMaC/pRXbc/6Wu03sykTUyCpB4Hx49
M/OMh/c8vdSCYNmN07PPzNhesck0e7MZyWIDAQABo2MwYTAzBgNVHRMBAf8EBTADAQH/MB8G
IwYMBaAFFojv4Igo2AZKk709pJBI14Gz7RMB0GA1UdDgQWBBrA17+C1CTtgMypO9PaSQZdeBs
0TAOBgNVHQ8BAf8EBAMCAAYwDQYJKoZIhvcNAQELBQADggEBAJNkV7PFUnHmptlFXjdeGUUxwC
VCrmwCz4z2V6QgmmRGBB2HJfmdPZZ23hKghApey8YyumsVG+A12qRnj5f5ox6p19XA9T8ttOI
```

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-----
MIIDWzCCA0gAwIBAgIIL1bhCFHr3mswDQYJKoZIhvcNAQELBQAwOzEaMBGGA1UEAwwRU31zdGVt
IE1hbmFnZXIgaQ0ExDTALBgNVBAsMIBE1HTVQxDjAMBgNVBAoMBUFWQV1BMB4XDTE4MTAxMTE4MTU0
NFoXDTI4MTAwODE4MTU0NFowOzEaMBGGA1UEAwwRU31zdGVtIE1hbmFnZXIgaQ0ExDTALBgNVBAsM
BE1HTVQxDjAMBgNVBAoMBUFWQV1BMBIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA1Y9+
b1FeekV10ePXG46TdUR7LjyZ1NjkmBCp+vf/rLbyy8u+y06YT9ZGzpaJxYJJwZgOKSJrgdkvvv2
RWmi71UICM73wyTBQwpzK12HQ00oS1ZAwjEwa/VuPQmbahGdC7UX04DHMczzhekWhE0JjJ4zkRM
22W1T+1WqV7f15q/itP0sEbwuJNo32Tn9U03hc/LWLqoOmTKyBZt4ejFD/c8KaRA0acw2a/+enMQ
5afShXKM9PaCbcMN29D3RftJybrTqUSKf0UOSiNev7I70KDMaC/pRXbc/6Wu03sykTuyCpB4Hx49
M/OMh/c8vdSCYNmN07PPzNhescK0e7MZywIDAQABo2MwYTAPBgNVHRMBAf8EBTADAQH/MB8GA1Ud
IwQYMBaAFFoJv4IgJ0AZKk709pJB114Gz7RMB0GA1UdDgQWBBRaI7+CICTtgMyp09PaSQZdeBs+
0TA0BgNVHQ8BAf8EBAMCAYYwDQYJKoZIhvcNAQELBQADggEBAJNKv7PFUnHmpt1FXjdeGUUxw0JM
VCrmwCz4z2V6QgmmRBBB2HJfmdPZZ23hKghApey8YyumsvG+A12qRNjb5tfox6p19XA9T8tt0Hh
o8FQ6/chUYVCJfwRKgUA7kKhODx75LK7mTGBv2DFBcGetEWLZzozVQS+gzwpAYgqF5fUpA8E2zni
m46H6SSivL7WDdowq1AxcVr4SclWghTpeeMBd1inp9R/e1bv0HK742oBATQGvem3rW36vRkUBaIOs
NzXWnviUXqtBTMQ8irD1zSEMx61IE0bXboht7eU60mnhQczFJjMLiwYuGB9N1mf2+gCZTbK1019N
FJMYfZjgZDg=
-----END CERTIFICATE-----
```

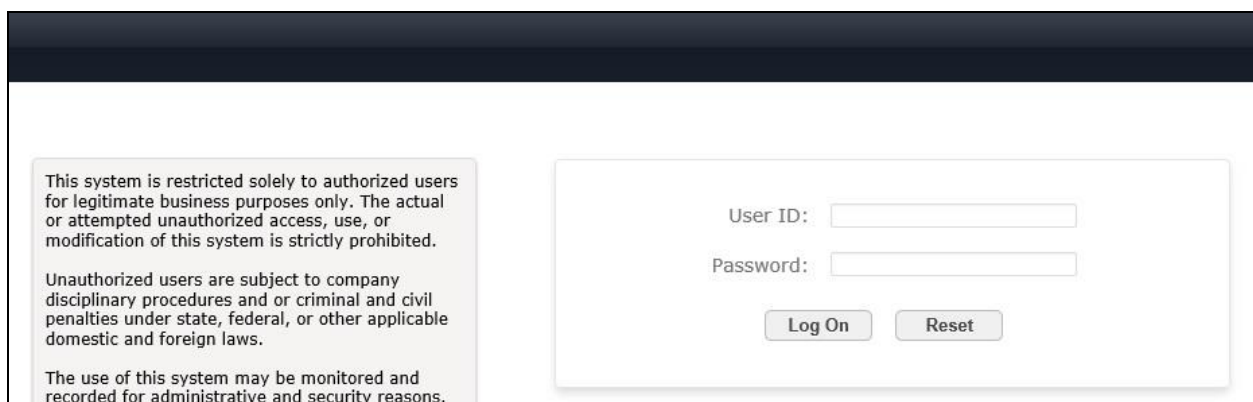
## 7. Configure Avaya Aura® Session Manager

This section provides the procedures for configuring Session Manager, which is performed via System Manager. The procedures include the following areas:

- Launch System Manager
- Administer users

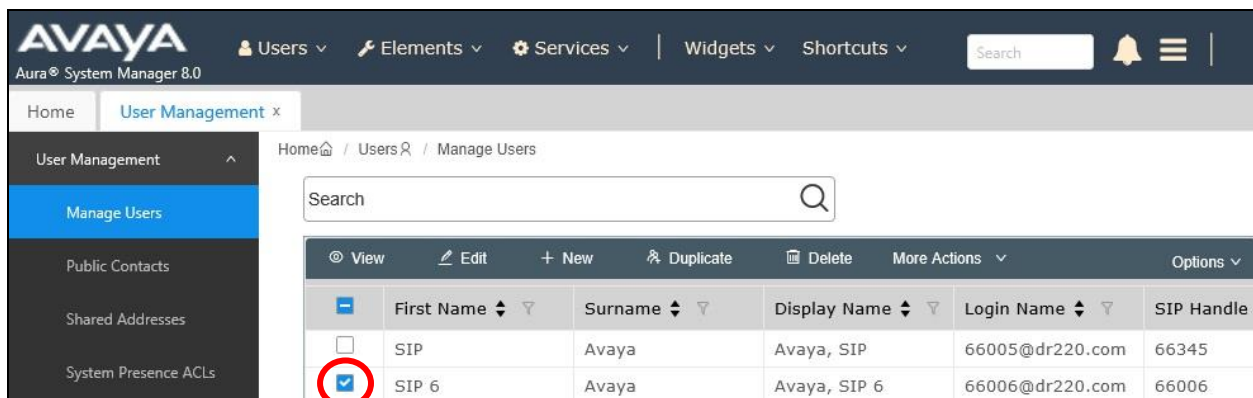
### 7.1. Launch System Manager

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.



### 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 “66006”, and click **Edit**.



	First Name	Surname	Display Name	Login Name	SIP Handle
<input type="checkbox"/>	SIP	Avaya	Avaya, SIP	66005@dr220.com	66345
<input checked="" type="checkbox"/>	SIP 6	Avaya	Avaya, SIP 6	66006@dr220.com	66006



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.

The screenshot shows the Avaya Aura System Manager 8.0 interface. The top navigation bar includes the Avaya logo, "Aura® System Manager 8.0", and tabs for Users, Elements, Services, Widgets, and Shortcuts. A search bar and notification bell are also present. The left sidebar shows the "User Management" menu with options like "Manage Users", "Public Contacts", "Shared Addresses", "System Presence ACLs", and "Communication Profile...". The main content area is titled "User Profile | Edit | 66006@dr220.com" and has tabs for Identity, Communication Profile, Membership, and Contacts. The "Communication Profile" tab is active, showing fields for "System" (DR-CM), "Profile Type" (Endpoint), "Extension" (66006), "Set Type" (9641SIPCC), "Port" (S00018), "Preferred Handle" (Select), and "Sip Trunk" (aar). The "CM Endpoint Profile" is highlighted in the left sidebar. The "Extension" field has an Editor icon circled in red.

In the popped up screen, scroll the screen as necessary to locate the **Type of 3PCC Enabled** parameter, and 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.

The screenshot shows the Avaya Aura System Manager 8.0 interface. The top navigation bar includes the Avaya logo, 'Aura System Manager 8.0', and tabs for Users, Elements, Services, Widgets, and Shortcuts. A search bar and notification bell are on the right. The left sidebar shows 'User Management' with a sub-menu 'Manage Users' highlighted. The main content area is titled 'User Profile | Edit | 66006@dr220.com' and has tabs for Identity, Communication Profile, Membership, and Contacts. The 'Communication Profile' tab is active, showing various configuration options. A red box highlights the 'Type of 3PCC Enabled' dropdown menu, which is set to 'Avaya'. Other visible fields include Class of Restriction (COR), Emergency Location Ext, Tenant Number, SIP Trunk, Coverage Path 1, Lock Message, Multibyte Language, Class Of Service (COS), Message Lamp Ext., Coverage Path 2, Localized Display Name, and Enable Reachability for Station Domain Control. At the bottom, there are sections for SIP URI, Primary Session Manager (IPv4: 10.64.101.238, IPv6: ), and Secondary Session Manager. A checkbox for 'Allow H.323 and SIP Endpoint Dual' is also present.

General Options (G) *		Feature Options (F)		Site Data (S)		Abbreviated Call Dialing (A)	
Enhanced Call Fwd (E)		Button Assignment (B)		Profile Settings (P)		Group Membership (M)	
* Class of Restriction (COR)	1	* Class Of Service (COS)	1				
* Emergency Location Ext	66006	* Message Lamp Ext.	66006				
* Tenant Number	1	Type of 3PCC Enabled		Avaya			
* SIP Trunk	Qaar	Coverage Path 1		Coverage Path 2			
Coverage Path 1		Lock Message	<input type="checkbox"/>	Localized Display Name	Avaya, SIP 6		
Multibyte Language	Not Applicable	Enable Reachability for Station Domain Control	system				
SIP URI							
Primary Session Manager							
IPv4:		10.64.101.238		IPv6:			
Secondary Session Manager							

Allow H.323 and SIP Endpoint Dual ☐

## 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 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.

### 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.



The screenshot shows the CXM web interface. At the top left is the CXM logo, which consists of three stylized human figures in blue and orange, followed by the text "cxm" in a large, bold, blue font. Below the logo is the text "Recording and Quality Monitoring" in a smaller, blue font. To the right of the logo is a navigation bar with three links: "Help", "About", and "Contact Us", each preceded by a small blue square icon. The main content area is a light gray rectangle. In the center of this area is a login form. The form has two labels: "Username:" and "Password:", each followed by a white text input field. Below the password field is a "Log On" button with a gray border and a light gray background. The entire page is framed by a dark blue border at the top and bottom.

## 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 6.9**.
- **TSAPI Application:** A desired name.
- **Private Data Version:** “7”
- **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.

The screenshot shows the CXM web interface with the following configuration details:

Field	Value
Configuration	Avaya Single Step DMCC
PBX Name	Avaya DevConnect
TSAPI Server Name	AVAYA#CM7#CSTA-S#AES7
TSAPI Application	CXM4
Private Data Version	7
Enable Call Monitors	<input checked="" type="checkbox"/>
Zip Tone Processing	<input type="checkbox"/>
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	10.64.101.208
Extension Password	123456
Access Codes	9
Screen Capture	<input type="checkbox"/>
Coaching	<input checked="" type="checkbox"/>
Machine Name	CXMAVAYA

### 8.3. Administer Conference Stations

Select **System** → **Conference Stations** from the left pane 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:** A 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 event that the virtual IP softphone extensions are not sequential, then add the conference stations one at a time.


The screenshot shows the CXM web interface. The top navigation bar includes links for Search, Coaching, Reports, Admin, System, Survey, Help, and My Login. The left sidebar lists various system functions, with 'Conference Stations' highlighted. The main content area is titled 'System -> Conference Stations' and features a table with columns for Station Number, Channel, Box, Type, and Site. Below the table, there are two main sections: 'Add stations by range' and 'Manage selected stations'. The 'Add stations by range' section contains fields for 'Start station number' (65991), 'Site across stations' (CXMAVAYA), 'Type across stations' (Normal), and '# of stations to add' (2). The 'Manage selected stations' section includes fields for 'Station number', 'Site' (none), and 'Type' (Normal), along with 'Delete', 'OK', and 'Cancel' buttons. A 'GO' button is located at the bottom right of the configuration area.

Station Number ▲	Channel	Box	Type	Site
------------------	---------	-----	------	------

**Add stations by range**  
Start station number:   
Site across stations:    
Type across stations:    
# of stations to add:

**Manage selected stations**  
Station number:   
Site:    
Type:

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

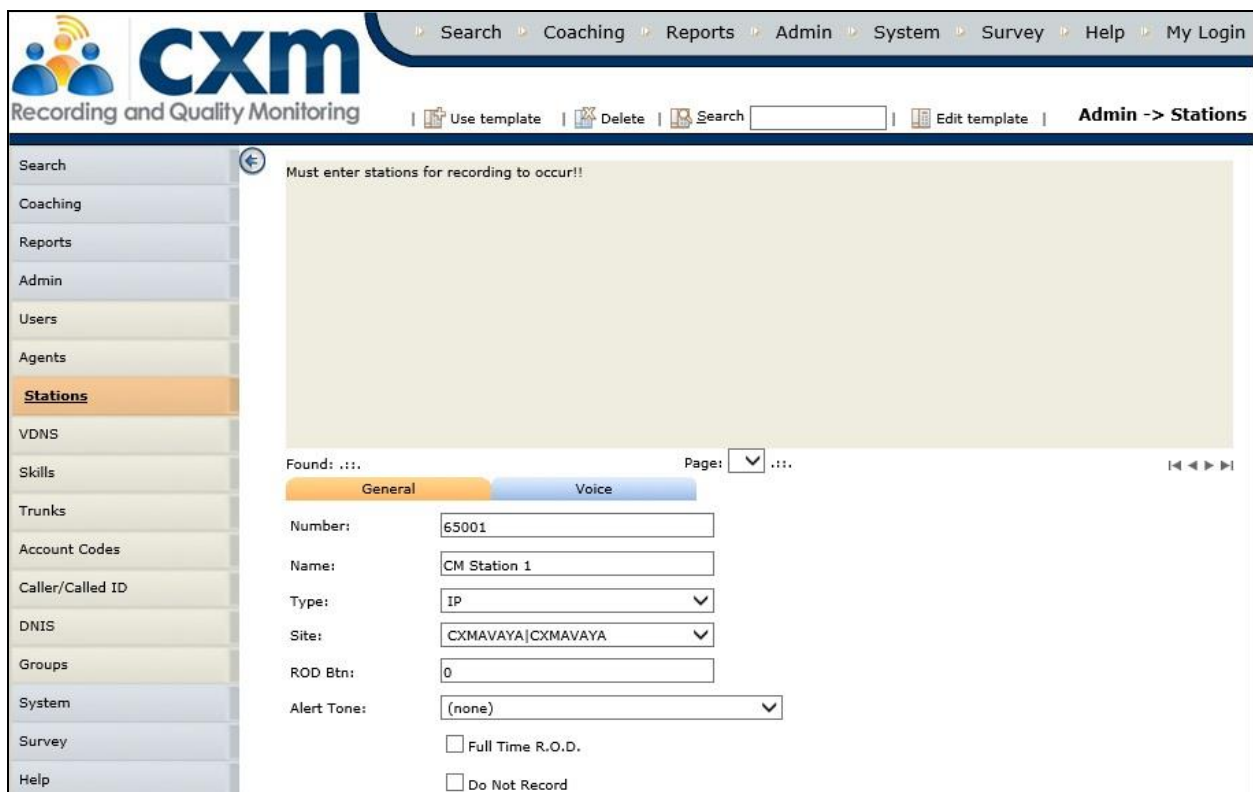


Station Number	Channel	Box	Type	Site
65991	0	CXMAVAYA	Normal	CXMAVAYA
65992	0	CXMAVAYA	Normal	CXMAVAYA

## 8.4. Administer Stations

Select **Admin** → **Stations** from the left pane 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:** The applicable type for the first agent station 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 “0” in the testing.



Must enter stations for recording to occur!!

Found: ... Page: ...

**General** Voice

Number: 65001

Name: CM Station 1

Type: IP

Site: CXMAVAYA

ROD Btn: 0

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.

The screenshot shows the CXM 'Stations' configuration page. The 'Voice' tab is selected, and the 'External Rule' and 'Internal Rule' settings are visible. The 'Inbound(%)' and 'Outbound(%)' values are set to 100 for both rules.

Rule Type	Direction	Percentage (%)
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.

The screenshot shows the CXM 'Stations' configuration page with a list of configured stations. The table below represents the data shown in the screenshot.

Number	Name	Ext Inbound(%)	Ext Outbound(%)	Int Inbound(%)	Int Outbound(%)	Modified
66006	Avaya SIP 2	100	100	100	100	11/28/2018 1:53:0
65001	CM Station 1	100	100	100	100	11/28/2018 1:51:0



## 8.5. Administer VDNs

Select **Admin** → **VDNS** from the left pane 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.

The screenshot shows the CXM (Recording and Quality Monitoring) application interface. The top navigation bar includes links for Search, Coaching, Reports, Admin, System, Survey, Help, and My Login. The left sidebar contains a menu with the following items: Search, Coaching, Reports, Admin, Users, Agents, Stations, **VDNS** (highlighted), Skills, Trunks, Account Codes, Caller/Called ID, DNIS, Groups, System, and Survey. The main content area is titled 'Admin -> VDNS' and displays a message 'No vdn's entered, yet!'. Below this message, there are three tabs: General (selected), Voice, and Email. The form fields are as follows:

Field	Value
Number:	60001
Name:	CM 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.

The screenshot shows the CXM (Recording and Quality Monitoring) Admin interface for VDNS configuration. The left sidebar lists various menu items, with 'VDNS' highlighted. The main content area shows the 'Voice' tab selected. A message states 'No vdn's entered, yet!'. Below this, there is a 'Found: ...' and 'Page: ...' section with tabs for 'General', 'Voice', and 'Email'. The 'Voice' tab is active. A 'Sampling' slider is set to 100. There are two checkboxes: 'Record In Queue' and 'Do not record', both of which are currently unchecked.

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

The screenshot shows the CXM Admin interface for VDNS configuration, displaying a list of configured VDNs. The left sidebar lists various menu items, with 'VDNS' highlighted. The main content area shows a table with the following data:

Number	Name	Sampling(%)	Address	Modified
60001	CM Sales	100		11/28/2018 1:55:00 PM
60002	CM Support	100		11/28/2018 1:56:00 PM

## 8.6. Administer Skills

Select **Admin** → **Skills** from the left pane 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.

Search

Coaching

Reports

Admin

Users

Agents

Stations

VDNS

**Skills**

Trunks

Account Codes

Caller/Called ID

DNIS

Groups

System

Survey

Search

Coaching

Reports

Admin

System

Survey

Help

My Login

Use template

Delete

Search

Template

Admin -> Skills

No skills entered, yet!

Found: 1/1 Page: 1/1

General

Number: 61001

Name: CXM Sales Skill

Site: CXMAVAYA

☐ Do not record

Sampling

100

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

Search

Coaching

Reports

Admin

Users

Search

Coaching

Reports

Admin

System

Survey

Help

My Login

Use template

Delete

Search

Template

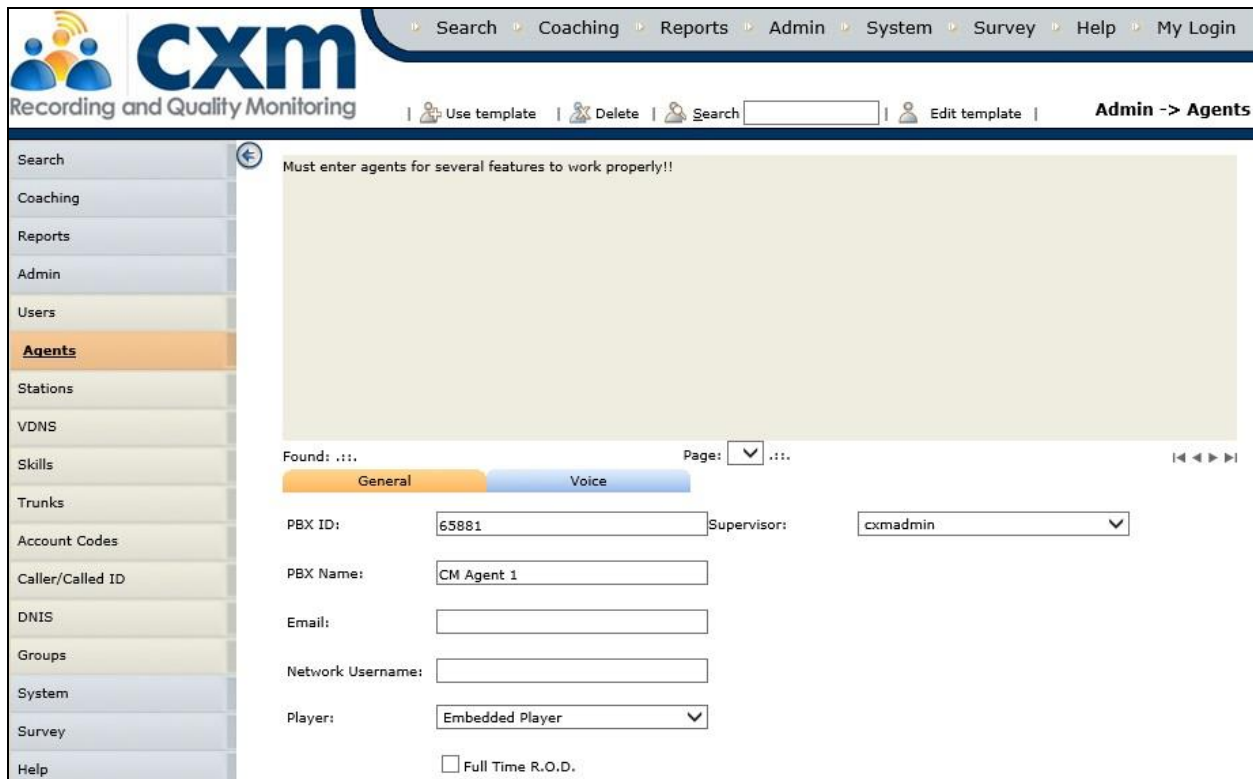
Admin -> Skills

Number	Name	Sampling(%)	Modified
61001	CXM Sales Skill	100	11/28/2018 1:57:00 PM
61002	CXM Support Skill	100	11/28/2018 1:57:00 PM

## 8.7. Administer Agents

Select **Admin** → **Agents** from the left pane 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**.



The screenshot shows the CXM (Recording and Quality Monitoring) Admin interface. The top navigation bar includes links for Search, Coaching, Reports, Admin, System, Survey, Help, and My Login. The left sidebar lists various modules, with 'Agents' highlighted. The main content area displays a message: 'Must enter agents for several features to work properly!!'. Below this, there are tabs for 'General' and 'Voice'. The 'General' tab is active, showing fields for PBX ID (65881), Supervisor (cxmadmin), PBX Name (CM Agent 1), Email, Network Username, and Player (Embedded Player). A checkbox for 'Full Time R.O.D.' is also present.

Search   Coaching   Reports   Admin   System   Survey   Help   My Login

Recording and Quality Monitoring | Use template | Delete | Search | Edit template | Admin -> Agents

Search   Coaching   Reports   Admin   Users   **Agents**   Stations   VDNS   Skills   Trunks   Account Codes   Caller/Called ID   DNIS   Groups   System   Survey   Help

Must enter agents for several features to work properly!!

Found: ... Page: ...

General   Voice

PBX ID: 65881 Supervisor: cxmadmin

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.

The screenshot shows the CXM Admin interface with the 'Agents' tab selected. The 'Voice' tab is active, displaying configuration options for recording percentages. The 'External Rule' and 'Internal Rule' sections each have sliders for 'Inbound(%)' and 'Outbound(%)', all set to 100. A message at the top states: 'Must enter agents for several features to work properly!!'.

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

The screenshot shows the CXM Admin interface with the 'Agents' tab selected. The table below lists the configured agents:

PBX ID	PBX Name	Voice Outbound	Voice Inbound	Modified
65881	CM Agent 1	100	100	11/28/2018 1:59:00 PM
65882	CM Agent 2	100	100	11/28/2018 1:59:00 PM

## 8.8. Install CA Certificate

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



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

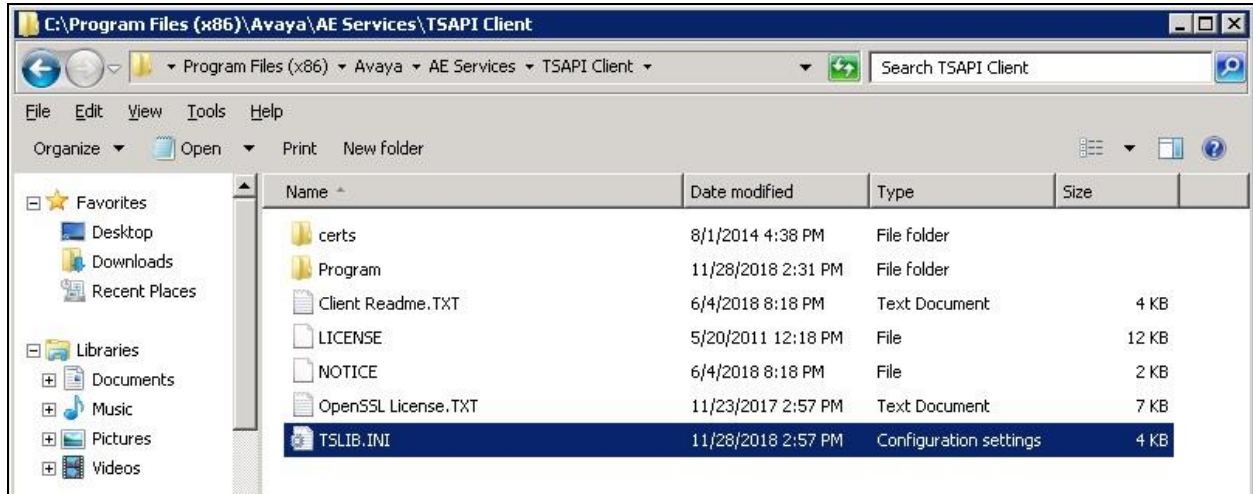


In the **Select Certificate Store** pop-up box, select **Trusted Root Certification Authorities**, as shown below. Proceed to complete the certificate installation.

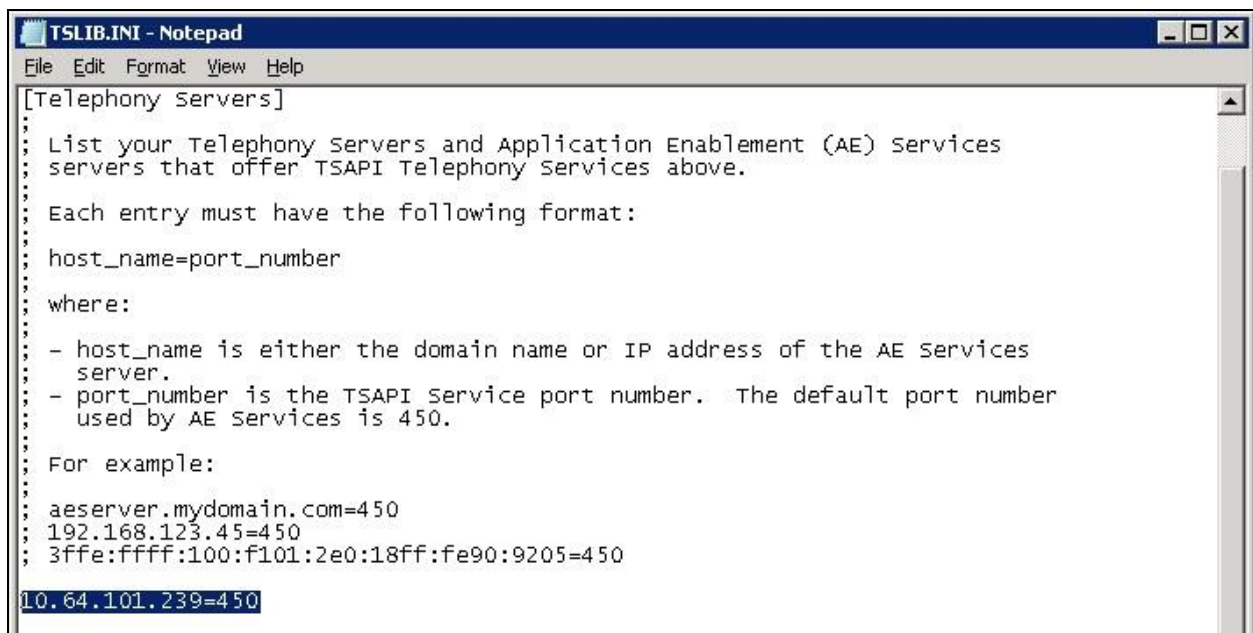


## 8.9. Administer TSLIB.INI

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



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



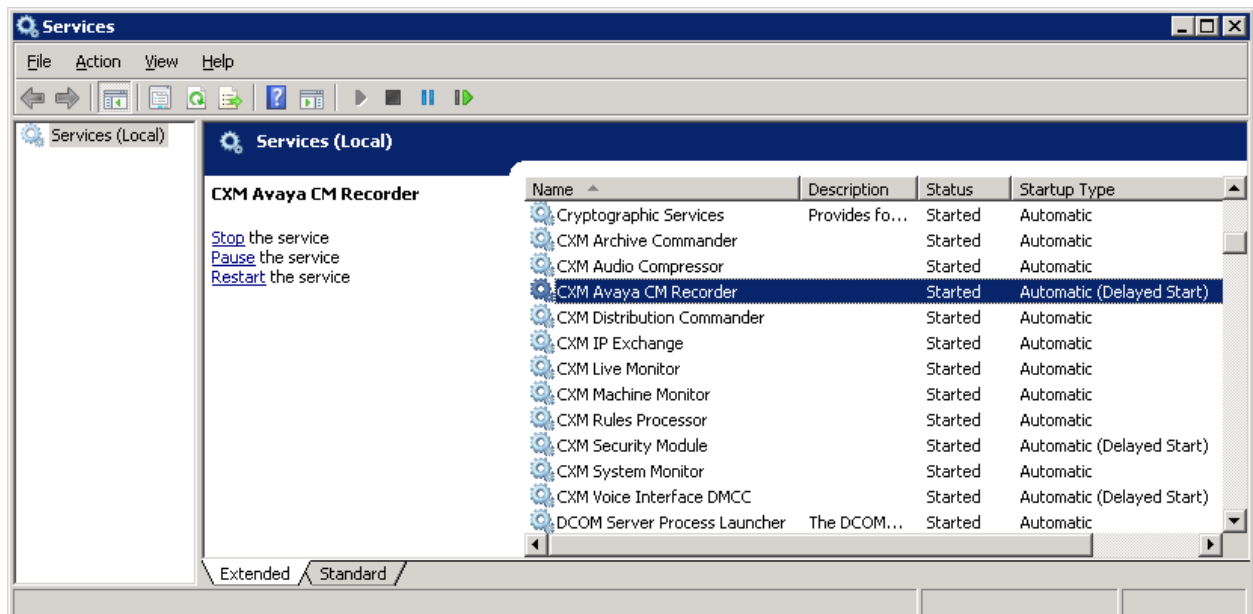


Scroll down to the **Config** sub-section, enter an entry shown below, where “C:\CXM4\Recorder\avaya.crt” is the path to the CA certificate from **Section 8.8**.



## 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.



## 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 Link	Version	Mnt Busy	AE Services Server	Service State	Msgs Sent	Rcvd
1	9	no	aes7	established	17	15

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 5.4** 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 or Orig Port Socket	Set Type/ Net Rgn	Prod ID/ Release	Station IP Address/ Gatekeeper IP Address
65000	9641	IP_Phone	192.168.200.106
tls	1	6.6604	10.64.101.236
65001	9611	IP_Phone	192.168.200.104
tls	1	6.6604	10.64.101.236
<b>65991</b>	<b>4620</b>	<b>IP_API_A</b>	<b>10.64.101.239</b>
<b>tcp</b>	<b>1</b>	<b>3.2040</b>	<b>10.64.101.236</b>
<b>65992</b>	<b>4620</b>	<b>IP_API_A</b>	<b>10.64.101.239</b>
<b>tcp</b>	<b>1</b>	<b>3.2040</b>	<b>10.64.101.236</b>



## 9.2. Verify Avaya Aura® Application Enablement Services

On Application Enablement Services, Verify 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**.

**AVAYA** Application Enablement Services  
Management Console

Welcome: User  
Last login: Wed Nov 28 16:41:58 2018 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: 8.0.0.0.6-0  
Server Date and Time: Thu Nov 29 08:52:48 EST 2018  
HA Status: Not Configured

Status | Status and Control | TSAPI Service SummaryHome | Help | Logout

▶ AE Services

▶ Communication Manager Interface

▶ High Availability

▶ Licensing

▶ Maintenance

▶ Networking

▶ Security

▼ Status

Alarm Viewer

▶ Logs

▶ Log Manager

▼ Status and Control

■ CVLAN Service Summary

■ DLG Services Summary

■ DMCC Service Summary

■ Switch Conn Summary

■ TSAPI Service Summary

TSAPI Link Details

☐ Enable page refresh every 60 seconds

	Link	Switch Name	Switch CTI Link ID	Status	Since	State	Switch Version	Associations	Msgs to Switch	Msgs from Switch	Msgs Period
<input checked="" type="radio"/>	1	cm7	1	Talking	Wed Nov 28 16:04:40 2018	Online	18	6	15	17	30


OnlineOffline

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

TSAPI Service StatusTLink StatusUser 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 5.4**.



# Application Enablement Services

## Management Console

Welcome: User  
 Last login: Wed Nov 28 16:41:58 2018 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: 8.0.0.0.6-0  
 Server Date and Time: Thu Nov 29 08:58:29 EST 2018  
 HA Status: Not Configured

Status | Status and Control | **DMCC Service Summary**
Home | Help | Logout

- ▶ AE Services
- ▶ Communication Manager Interface
- ▶ High Availability
- ▶ Licensing
- ▶ Maintenance
- ▶ Networking
- ▶ Security
- ▼ **Status**
  - Alarm Viewer
  - ▶ Logs
  - ▶ Log Manager
  - ▼ **Status and Control**
    - CVLAN Service Summary
    - DLG Services Summary
    - **DMCC Service Summary**
    - Switch Conn Summary
    - TSAPI Service Summary

### DMCC Service Summary - Session Summary

Please do not use back button

☐ Enable page refresh every  seconds

Session Summary [Device Summary](#)  
 Generated on Thu Nov 29 08:58:29 EST 2018

Service Uptime: 0 days, 16 hours 52 minutes

Number of Active Sessions: 1

Number of Sessions Created Since Service Boot: 3

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
■	006AB1B8EB1D4DD05 DD9AD6377F6C9D5-3	cxm	CXM	10.64.101.208	XML Encrypted	2

Item 1-1 of 1  
 Go

### 9.3. Verify 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 **Search** to display a list of call recording entries for the current day.

The screenshot shows the CXM web interface with the following elements:

- Header: Search Coaching Reports Admin System Survey Help My Login
- Left Navigation: Search, Quick, Advanced, Call Buckets, Manage Buckets, Display Options, Coaching, Reports
- Main Content Area:
  - From: 11/29/2018
  - To: 11/29/2018
  - Stations: [Empty]
  - Agents: [Empty]
  - Caller/Called ID: [Empty]
  - Page Size: 100
  - Check: All None
  - (empty) Add to Bucket
  - Search button (highlighted with a red circle)
- Table Headers: Start Time, Agents, Grades, VDNS, Call Duration, Call Direction

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.

The screenshot shows the CXM web interface with the following elements:

- Header: Search Coaching Reports Admin System Survey Help My Login
- Left Navigation: Search, Quick, Advanced, Call Buckets, Manage Buckets, Display Options, Coaching, Reports, Admin
- Main Content Area:
  - From: 11/29/2018
  - To: 11/29/2018
  - Stations: [Empty]
  - Agents: [Empty]
  - Caller/Called ID: [Empty]
  - Page Size: 100
  - Check: All None
  - (empty) Add to Bucket
  - Search button
- Table:

	Start Time	Agents	VDNS	Call Duration	Call Direction	Stations	ANI	Dialed	Skills
[Listen to call icon]	11/29/2018 8:03:03 AM	65881	60001	00:01:38	Inbound	65001	9089532103	3035360001	61001

## 10. Conclusions

These Application Notes describe the configuration steps required for CXM 5.3 to successfully interoperate with Avaya Aura® Communication Manager 8.0 and Avaya Aura® Application Enablement Services 8.0. 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 8.0, Issue 2.1, November 2018, available at <http://support.avaya.com>.
2. *Administering Aura® Application Enablement Services*, Release 8.0, Issue 1, July 2018, available at <http://support.avaya.com>.
3. *CXM Recording and Quality Monitoring Administration Guide*, Release 5.0, available from CXM Support.

---

**©2019 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](mailto:devconnect@avaya.com).