



Avaya Solution & Interoperability Test Lab

Application Notes for Co-nexus CXM with Avaya AuraTM Communication Manager and Avaya AuraTM Application Enablement Services – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for Co-nexus CXM to interoperate with Avaya AuraTM Communication Manager and Avaya AuraTM Application Enablement Services.

Co-nexus CXM is a call recording solution that interfaces with Communication Manager and Application Enablement Services (AES). Co-nexus CXM can be configured to automatically record all calls full-time, record calls on-demand, record calls based on defined triggers, or even at random. Co-nexus CXM uses the Telephony Service API (TSAPI) to receive call related events. It also uses the Device, Media & Call Control (DMCC) API to register a number of softphones, DMCC recording devices. The softphones are single step conferenced into calls in order to obtain the audio for call recording.

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 a compliance tested configuration that comprised of an Avaya Aura™ Communication Manager, an Avaya Aura™ Application Enablement Services server, and a Co-nexus CXM server and client.

Co-nexus CXM is a call recording solution that interfaces with Avaya Communication Manager and Avaya Application Enablement Services. Co-nexus CXM uses a TSAPI CTI link to an Application Enablement Services server to monitor stations, agents, and hunt groups to obtain recording triggers and call information. Co-nexus CXM also uses the DMCC interface of Application Enablement Services to register softphones with Communication Manager. Co-nexus CXM uses the softphones as recording devices. When recording of a call is desired, Co-nexus CXM uses the Single Step Conference feature to conference a softphone into the call to obtain the audio.

1.1. Interoperability Compliance Testing

The interoperability compliance testing focused on feature functionality, serviceability, and performance. The feature functionality testing evaluated the ability of Co-nexus CXM to monitor and record calls placed to and from stations on Communication Manager. The serviceability testing introduced failure conditions to see if CXM could properly resume recording calls after each failure recovery. The performance testing stressed CXM by continuously placing calls over extended periods of time.

The compliance testing validated the monitoring and recording performed by CXM of calls placed to and from analog phones, digital phones, IP phones, softphones, agents, Vector Directory Numbers (VDNs), and hunt groups on Communication Manager.

1.2. Support

Technical support for Co-nexus CXM can be obtained by contacting Co-nexus at:

- Phone: 866.400.4CXM (4296)
- Web: <http://www.4cxm.com/cont.asp>
- Email: SupportCXM@4cxm.com

2. Reference Configuration

The figure below shows the configuration used during compliance testing. Site A is comprised of an Avaya S8500 Media Server with an Avaya G650 Media Gateway. Site B is comprised of an Avaya S8300 Media Server with an Avaya G450 Media Gateway. The two Communication Manager systems are connected to each other via an IP (H.323) trunk and an ISDN-PRI trunk. The various telephones shown are used to generate intra-switch calls, outbound and inbound calls to and from the PSTN, and inter-switch calls. The Co-nexus CXM server is set up to record calls at Site A.

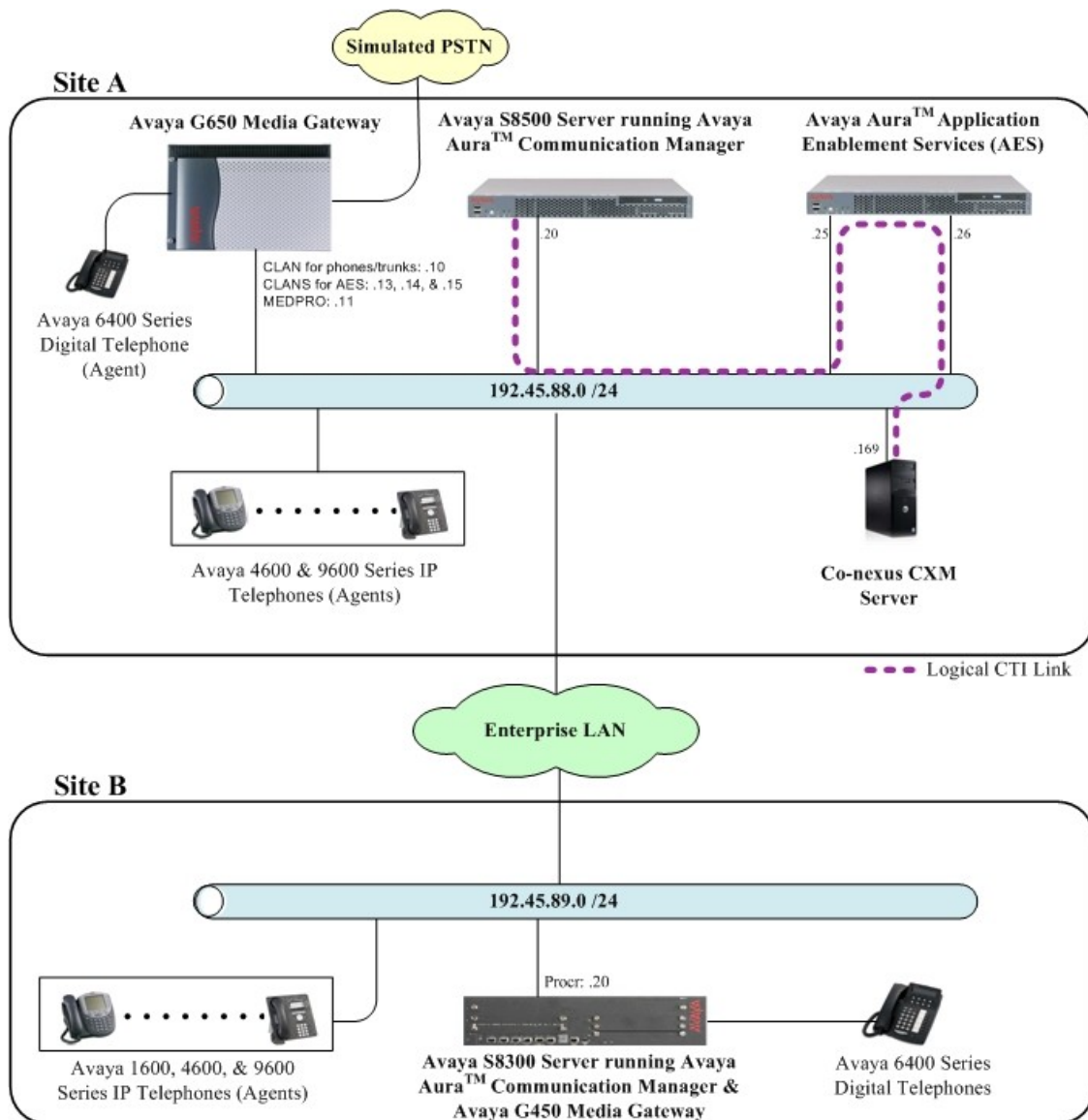


Figure 1: Co-nexus CXM with Communication Manager and AES

3. Equipment and Software Validated

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

Equipment	Software
Avaya S8500 Server (w/ G650)	Avaya Aura™ Communication Manager 5.2 (R015x.02.0.947.3)
Avaya S8300 Server (w/ G450)	Avaya Aura™ Communication Manager 5.2 (R015x.02.0.947.3)
Avaya G650 Media Gateway: TN799DP (C-LAN) TN2602AP (MEDPRO) TN2312BP (IPSI)	HW01, FW026 HW02, FW007 HW15, FW030
Avaya G450 Media Gateway : MM710BP (DS1) MM712AP (DCP)	HW11, FW044 HW07, FW009
Avaya Aura™ Application Enablement Services (AES) Server	4.2
Avaya C364T-PWR Converged Stackable Switch	4.5.14
Avaya 1600 Series IP Phones : 1608SW (H.323) 1616SW (H.323)	1.0.3 1.0.3
Avaya 4600 Series IP Phones: 4610SW (H.323) 4620SW (H.323) 4621SW (H.323)	2.9 2.9 2.9
Avaya 9600 Series IP Phones: 9620 (H.323) 9230 (SIP)	3.002 2.4.1
Avaya 6400 Series Digital Phones	-
Co-nexus CXM Server	4.5
Co-nexus CXM Client	4.5

4. Configure Communication Manager

All the configuration changes in this section for Communication Manager are performed through the System Access Terminal (SAT) interface. For more information on configuring Communication Manager, refer to the Avaya product documentation, **Reference [1]**.

The information shown on the screens throughout this section indicate the values that were used during compliance testing.

4.1. Configure IP Codec Sets & IP-Network Regions

This section provides the steps required for configuring ip-codec-set and ip-network regions.

1. Enter the **change ip-codec-set <codec set number>** command, where **<codec set number>** is the codec set number to be used with the Co-nexus recording solution.
 - In the **Audio Codec** field, type **G.711MU**.

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

Media Encryption
1: none
2:
3:
```

2. Enter the **change ip-network-region <region number>** command, where **<region number>** is the ip network region number to be used with the Co-nexus recording solution.
 - In the **Code Set** field, type the codec set number administered in **Step 1**. The **Codec Set** field reflects the codec set that must be used for connections between phones within this region or between phones and media processor boards within this region.

```

change ip-network-region 1                                     Page 1 of 19
                                IP NETWORK REGION
Region: 1
Location: 1           Authoritative Domain: dev8.com
Name: interop
MEDIA PARAMETERS
    Codec Set: 1
    UDP Port Min: 2048
    UDP Port Max: 65535
    Intra-region IP-IP Direct Audio: yes
    Inter-region IP-IP Direct Audio: yes
    IP Audio Hairpinning? y
DIFFSERV/TOS PARAMETERS
    Call Control PHB Value: 48
    Audio PHB Value: 48
    Video PHB Value: 26
    RTCP Reporting Enabled? y
    RTCP MONITOR SERVER PARAMETERS
    Use Default Server Parameters? y
802.1P/Q PARAMETERS
    Call Control 802.1p Priority: 6
    Audio 802.1p Priority: 6
    Video 802.1p Priority: 5
    AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS
    H.323 Link Bounce Recovery? y
    Idle Traffic Interval (sec): 20
    Keep-Alive Interval (sec): 5
    Keep-Alive Count: 5
    RSVP Enabled? n

```

During compliance testing, two IP Network regions were used. It is best practice for all CLANs dedicated to AE Services to be in a separate network region from those CLANs servicing endpoints (i.e. phones). For compliance testing, a single CLAN in network region 1 was used to service endpoints, while 3 CLANs in network region 2 were dedicated to Application Enablement Services. Both IP network regions were configured to use IP codec set 1.

4.2. Configure Connectivity to AES and Endpoints

This section provides the steps required for configuring connectivity from Communication Manager to Application Enablement Services and endpoints.

The Application Enablement Services server communicates with Communication Manager by using one or more CLANs to create a switch connection. The following steps show only the configuration required in Communication Manager to set up a switch connection. See **Section 5.1** for the configuration steps required in Application Enablement Services to complete the administration of the switch connection.

1. Enter the **change node-names ip** command.

- In the **Name** field, type a descriptive name to assign to a CLAN.
- In the **IP Address** field, type the IP address that will be assigned to the CLAN.

change node-names ip		Page 1 of 2
IP NODE NAMES		
Name	IP Address	
8300	192.45.89.20	
CLAN	192.45.88.10	
CLAN2	192.45.88.13	
CLAN3	192.45.88.14	
CLAN4	192.45.88.15	
LSP-8300	192.45.88.30	
Member-CDR	192.168.199.69	
RDTT-CDR	192.45.88.45	
SES	192.45.88.50	
cf-medpro	192.45.88.11	
default	0.0.0.0	
ipoffice	192.45.88.40	
procr	192.45.88.20	

Repeat this step for each CLAN.

In the compliance tested configuration, the **CLAN** node was used for registering endpoints and the **CLAN2**, **CLAN3**, and **CLAN4** nodes were used for connectivity to Application Enablement Services.

2. Enter the **add ip-interface <board location>** command, where **<board location>** is the board location for the CLAN, for example: 01A02.

- In the **Enable Interface** field, type **y**.
- In the **Network Region** field, type the network region number administered in **Section 4.1**.
- In the **Node Name** field, type **<CLAN name>**, where **<CLAN name>** is the **Name** from **Step 1**.
- In the **Ethernet Link** field, type an available Ethernet link number.

add ip-interface 01a08		Page 1 of 3	
IP INTERFACES			
Type: C-LAN	Target socket load and Warning level: 400		
Slot: 01A02	Receive Buffer TCP Window Size: 8320		
Code/Suffix: TN799 D	Allow H.323 Endpoints? y		
Enable Interface? y	Allow H.248 Gateways? y		
VLAN: n	Gatekeeper Priority: 5		
Network Region: 1			
IPV4 PARAMETERS			
Node Name: CLAN			
Subnet Mask: /24			
Gateway Node Name:			
Ethernet Link: 1			

Repeat this step for each CLAN

In the compliance tested configuration, the **CLAN** node was assigned to network region 1 and the **CLAN2**, **CLAN3**, and **CLAN4** nodes were assigned to network region 2.

3. Enter the **change ip-services** command.

- In the **Service Type** field, type **AESVCS**.
- In the **Enabled** field, type **y**.
- In the **Local Node** field type **<nodename>**, where **<nodename>** is the name of the CLAN board used for connectivity to Application Enablement Services.
- In the **Local Port** field, accept the default port (**8765**).

change ip-services				Page	1 of 4
IP SERVICES					
Service Type	Enabled	Local Node	Local Port	Remote Node	Remote Port
AESVCS	y	CLAN2	8765		
AESVCS	y	CLAN3	8765		
AESVCS	y	CLAN4	8765		

Repeat this step for each CLAN used for connectivity to Application Enablement Services.

On **Page 4**,

- In the **AE Services Server** field, type the <name> of the Application Enablement Services server. On the Application Enablement Services server, the name can be obtained by typing “uname -n” at the command prompt. The name entered on Communication Manager must match the Application Enablement Services server name exactly.
- In the **Password** field, enter an alphanumeric password. The passwords must exactly match on both Communication Manager and Application Enablement Services (administered in **Section 5.1**).
- In the **Enabled** field, type y.

change ip-services				Page 4 of 4
AE Services Administration				
Server ID	AE Services Server	Password	Enabled	Status
1:	aeserver25	xxxxxxxxxxxxxx	y	in use
2:				
3:				

This section provides the steps required for configuring a CTI link on Communication Manager. See **Section 5.3** for the configuration steps required on Application Enablement Services to complete the administration.

1. Enter the **display system-parameters customer-options** command.
 - On **Page 3**, verify that the **Computer Telephony Adjunct Links** field is set to **y**. If not, contact an authorized Avaya account representative to obtain the license.

```

display system-parameters customer-options
                                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? n    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? n
ARS/AAR Dialing without FAC? y             DCS (Basic)? y
ASAI Link Core Capabilities? y             DCS Call Coverage? y
ASAI Link Plus Capabilities? y             DCS with Rerouting? y
Async. Transfer Mode (ATM) PNC? n
Async. Transfer Mode (ATM) Trunking? n      Digital Loss Plan Modification? y
ATM WAN Spare Processor? n                 DS1 MSP? y
ATMS? y                                    DS1 Echo Cancellation? y
Attendant Vectoring? y

```

2. Enter **add cti-link <link number>** command, where **<link number>** is an available CTI link number.
 - In the **Extension** field, type **<station extension>**, where **<station extension>** is a valid station extension.
 - In the **Type** field, type **ADJ-IP**.
 - In the **Name** field, type a descriptive name.

add cti-link 10		Page 1 of 3
CTI LINK		
CTI Link: 10		
Extension: 39010		
Type: ADJ-IP		
		COR: 1
Name: TSAPI Link 1 - aeserver25		

4.4. Configure Stations (DMCC Recording Devices)

This section provides the steps required for configuring stations on Communication Manager that will function as recording devices for Co-nexus CXM.

For the purpose of this document, devices that have been registered using the DMCC service will be called “DMCC devices”. When a client application registers itself as a DMCC device at an extension, it can act like an IP softphone to control and monitor physical aspects of the extension (button pushes, lamps, the display, etc.) or access and control the media streams at the extension. For a client application to be able to control the media at an extension, and record calls at that extension, it must register itself as a DMCC device with the media mode set to “Client”. Client media mode indicates that the client application will handle the media streams from the DMCC device. DMCC devices that have been registered in the Client media mode will be called “DMCC recording devices”.

The DMCC recording devices used by Co-nexus CXM are administered as IP softphones on Avaya Communication Manager. Each DMCC recording device requires either an “IP_API_A” license on Communication Manager or a “VALUE_DMCC_DMC” license on Application Enablement Services.

Note that these licenses are separate and independent from the Avaya IP Softphone licenses required on Communication Manager for Avaya IP Softphones, but not for DMCC recording devices.

1. Enter the **display system-parameters customer-options** command to verify that there are sufficient **IP_API_A** licenses for the DMCC recording devices. If not, contact an authorized Avaya account representative to obtain these licenses.

display system-parameters customer-options			Page 10 of 11
MAXIMUM IP REGISTRATIONS BY PRODUCT ID			
Product ID	Rel. Limit	Used	
IP_API_A	: 1000	0	
IP_API_B	: 1000	0	
IP_API_C	: 1000	0	
IP_Agent	: 1000	0	
IP_IR_A	: 0	0	
IP_Phone	: 2400	3	
IP_ROMax	: 2400	0	
IP_Soft	: 2	0	
IP_eCons	: 0	0	
oneX_Comm	: 2400	0	
	: 0	0	

2. Enter the **add station <extension>** command, where **<extension>** is a valid station extension.
 - In the **Type** field, type an IP telephone set type with configurable buttons; for example, **4620**.
 - In the **Security Code**, type the value entered for **<extension>** (the station extension and security code must match).
 - In the **Name** field, type a descriptive name.
 - In the **IP SoftPhone**, type **y**.

add station 31126		Page 1 of 5
STATION		
Extension: 31126	Lock Messages? n	BCC: 0
Type: 4620	Security Code: 31126	TN: 1
Port: IP	Coverage Path 1:	COR: 1
Name: DMCC Softphone	Coverage Path 2:	COS: 1
Hunt-to Station:		
STATION OPTIONS		
Loss Group: 19	Time of Day Lock Table:	
Speakerphone: 2-way	Personalized Ringing Pattern: 1	
Display Language: english	Message Lamp Ext: 31126	
Survivable GK Node Name:	Mute Button Enabled? y	
Survivable COR: internal	Expansion Module? n	
Survivable Trunk Dest? y	Media Complex Ext:	
	IP SoftPhone? y	
	IP Video? n	
Customizable Labels? Y		

This completes the Avaya Aura™ Communication Manager configuration.

5. Configure Application Enablement Services

The Application Enablement Services (AES) server enables Computer Telephony Interface (CTI) applications to monitor and control telephony resources on Communication Manager. The Application Enablement Services server receives requests from CTI applications, and forwards them to Communication Manager. Conversely, the Application Enablement Services server receives responses and events from Communication Manager and forwards them to the appropriate CTI applications.

This section assumes that the installation and basic administration of the Application Enablement Services server has already been performed. For more information on administering Application Enablement Services, refer to the Avaya product documentation, **Reference [2]**.

1. Launch a web browser and enter <https://<IP address of AES Server>> in the address field.
Click **AE Server Administration**.



[AE Server Administration](#)
[WebLM Administration](#)

Welcome to Avaya Application Enablement Services

These web pages are provided for the administration and maintenance of this Avaya Application Enablement Server.

Before You Begin:

.....

*** WARNING NOTICE ***

This system is restricted solely to Avaya authorized users for legitimate business purposes only. The actual or attempted unauthorized access, use, or modification of this system is strictly prohibited by Avaya. Unauthorized users are subject to Company disciplinary proceedings 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. Anyone accessing this system expressly consents to such monitoring and is advised that if monitoring reveals possible evidence of criminal activity, Avaya may provide the evidence of such activity to law enforcement officials. All users must comply with Avaya Security Instructions regarding the protection of Avaya's information assets.

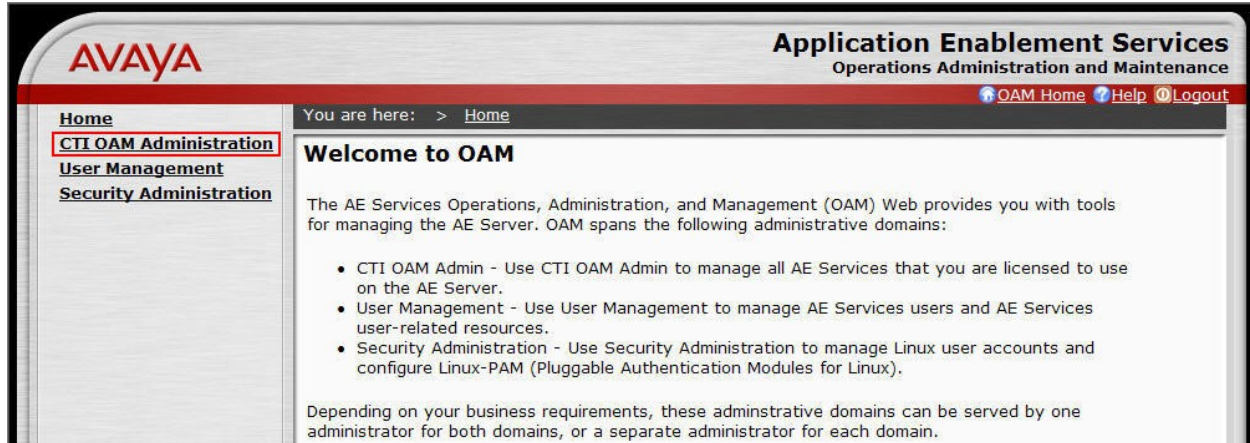
.....

© 2007 Avaya Inc. All Rights Reserved.

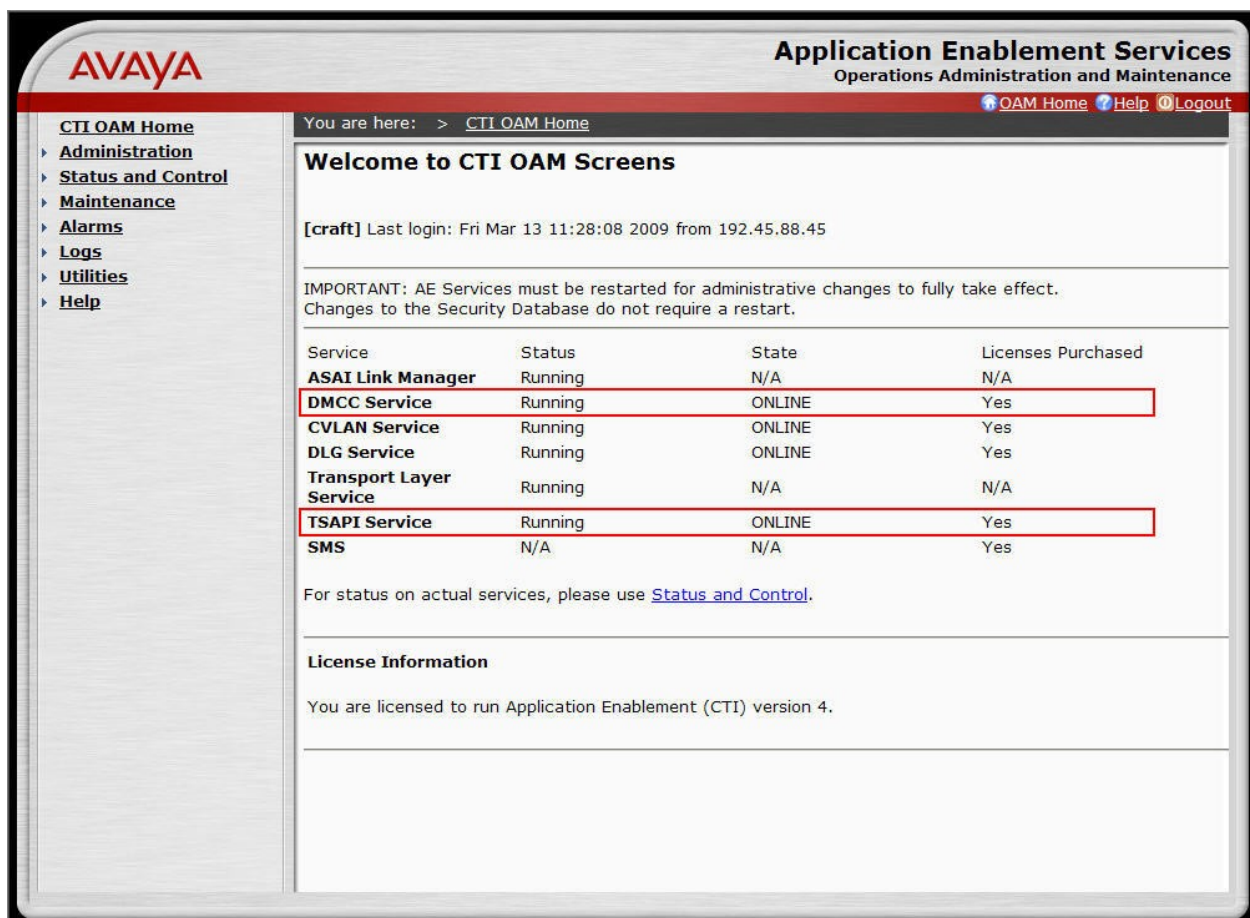
2. Log in with the appropriate credentials for accessing the Application Enablement Services CTI OAM web pages.

A screenshot of the Avaya Application Enablement Services login page. The page has a silver, metallic-looking background. At the top, the Avaya logo is in red. Below it, a red banner contains the text "Application Enablement Services" and a "? Help" link. The main content area is white and contains the text "Please log on." followed by "Logon:" and "Password:" labels next to input fields. A "Login" button is positioned below the password field. At the bottom, a small copyright notice reads "©2007 Avaya, Inc. All Rights Reserved."

- Click **CTI OAM Administration** in the left pane menu.



- Verify that Application Enablement Services is licensed for the TSAPI and DMCC services. If these services are not licensed, contact an authorized Avaya account representative to obtain these licenses.



- Each DMCC recording device used by Co-nexus CXM requires either an “IP_API_A” license on Avaya Communication Manager or a “VALUE_DMCC_DMC” license on Application Enablement Services. If “VALUE_DMCC_DMC” licenses are being used, log in to the Avaya Web License Manager (WebLM) and verify that there are sufficient licenses for the DMCC recording devices. Additionally, verify there are sufficient TSAPI licenses to monitor and control Communication Manager resources for call events and Single Step Conferencing. If not, contact an authorized Avaya account representative to obtain these licenses.

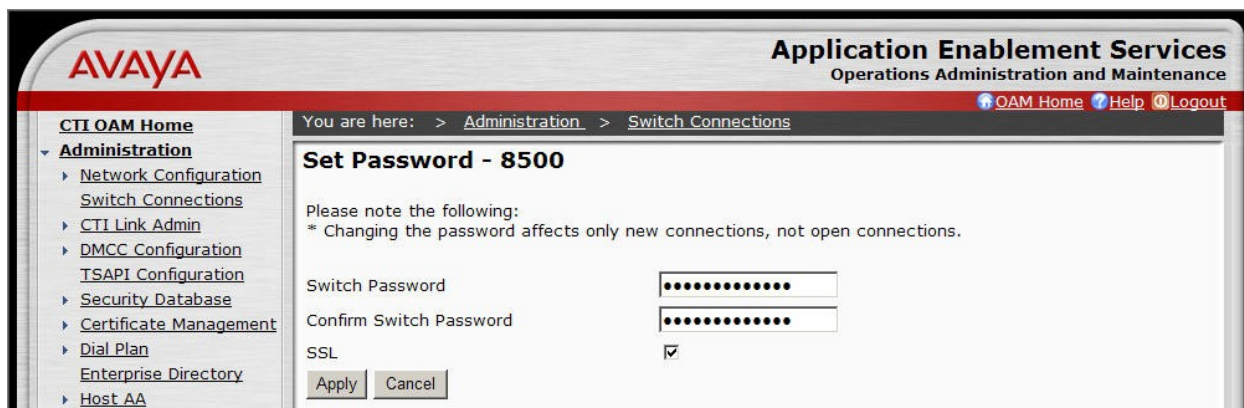
5.1. Configure a Switch Connection

This section provides the steps required for configure a Switch Connection. A Switch Connection defines a connection between the Application Enablement Services server and Communication Manager.

- Select **Administration > Switch Connections** from the left pane menu. In the **Add Connection** field, type a descriptive name and click **Add Connection**.

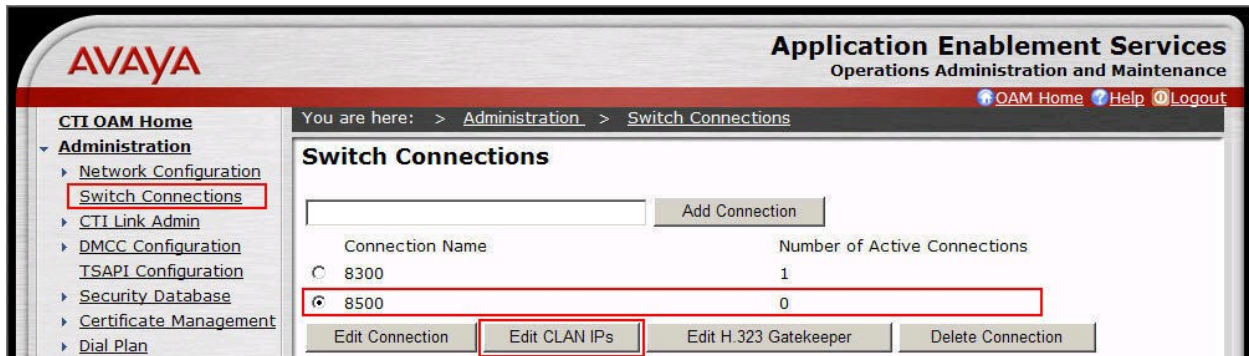


- In the **Switch Password** field, type the password that was entered during **Step 3** of **Section 4.2**. Re-type the password in the **Confirm Switch Password** field. Leave **SSL** checked if using a secure connection to Communication Manager. Click **Apply**.

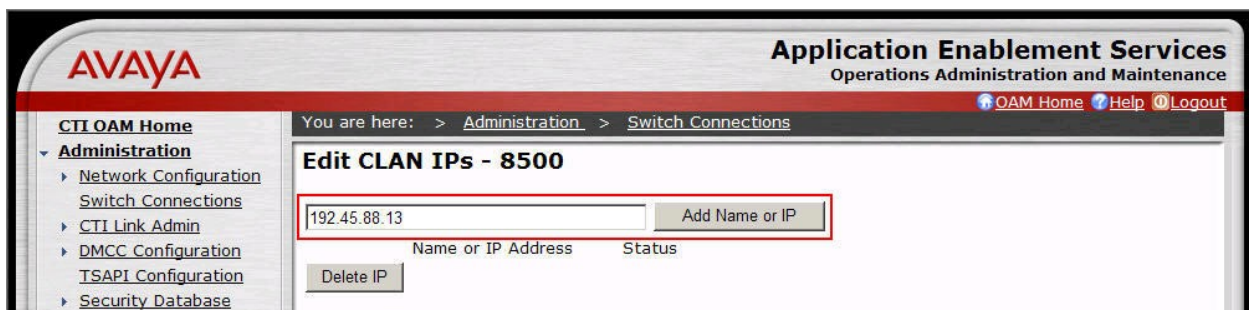


OAM adds the switch connection and returns to the “Switch Connections” page.

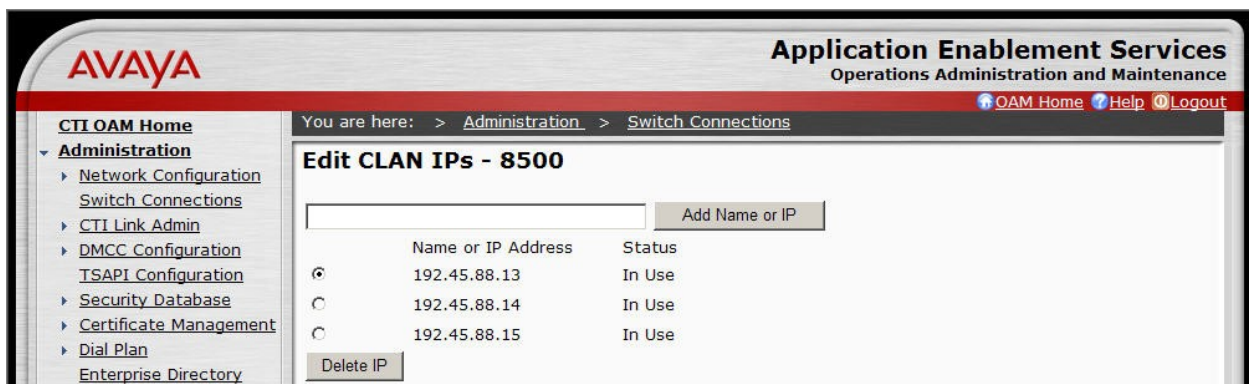
3. From the “Switch Connections” page, select the newly added switch connection, and click **Edit CLAN IPs**.



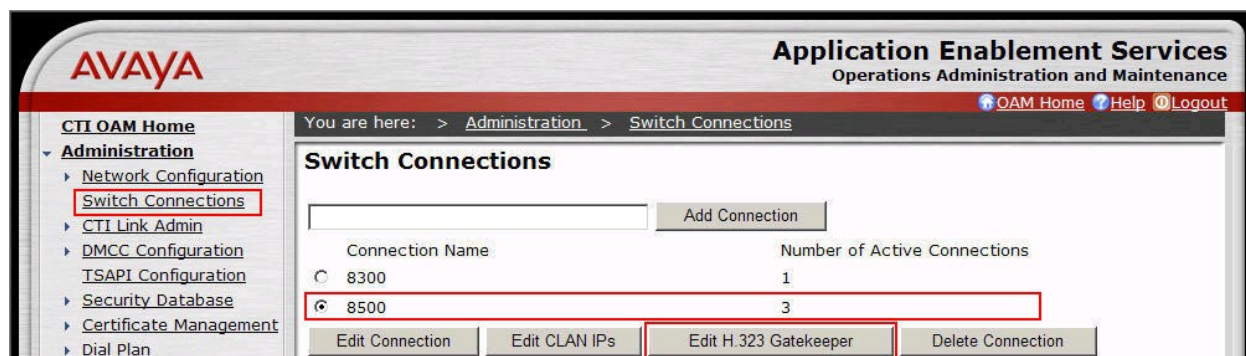
4. In the **Add Name or IP** field, type the <Host Name> or the <IP Address> of the CLAN, and click **Add Name or IP** (use the Host Name or IP address of the CLAN that was administered for Application Enablement Services connectivity in **Section 4.2**).



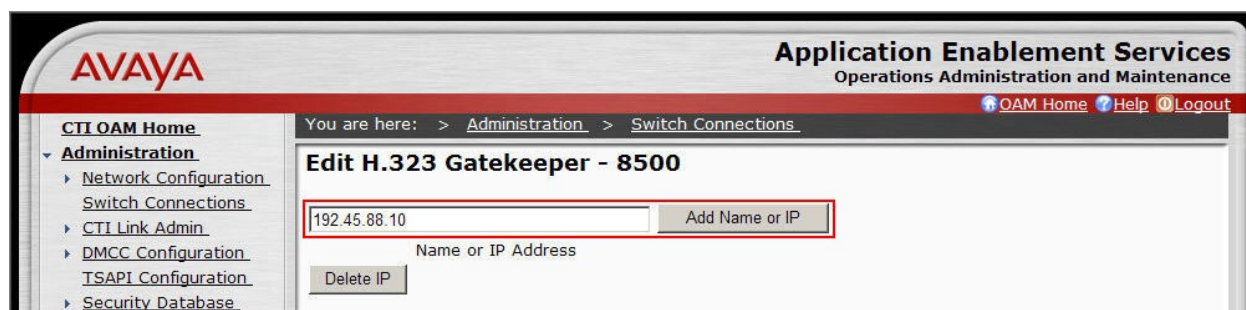
Repeat this step for each CLAN. The screen below shows the CLANs that were used during compliance testing.



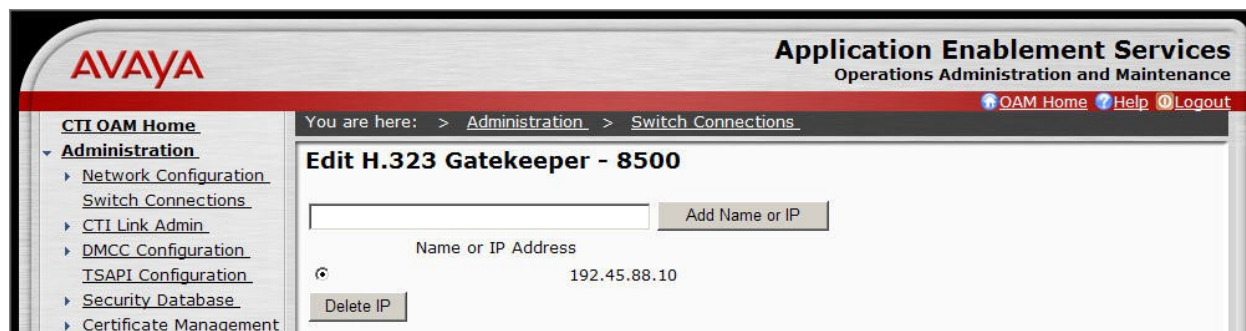
5. Navigate back to **Administration > Switch Connections**. Select the switch connection, and click **Edit H.323 Gatekeeper**.



6. In the **Add Name or IP** field, type the <Host Name> or <IP address> of the CLAN to be used. Click **Add Name or IP**.



Repeat this step as necessary to add multiple H.323 Gatekeepers. The screen below shows the CLANs that were used during compliance testing.



5.2. Configure DMCC Server Ports

This section provides the steps required for configuring DMCC server ports.

1. Navigate to the **CTI OAM Home > Administration > Ports** page. During compliance testing, the default port values shown in the screen below were utilized. Set either the **Encrypted Port** or the **Unencrypted Port** field to **Enabled**. During compliance testing, the encrypted port was used. Click the **Apply Changes** button (not shown) at the bottom of the screen to complete the process.

AVAYA Application Enablement Services
Operations Administration and Maintenance

You are here: > Administration > Network Configuration > Ports

Ports

CVLAN Ports

			Enabled	Disabled
Unencrypted TCP Port	9999		<input checked="" type="radio"/>	<input type="radio"/>
Encrypted TCP Port	9998		<input type="radio"/>	<input checked="" type="radio"/>

DLG Port

TCP Port	
5678	

TSAPI Ports

		Enabled	Disabled
TSAPI Service Port	450	<input checked="" type="radio"/>	<input type="radio"/>
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		

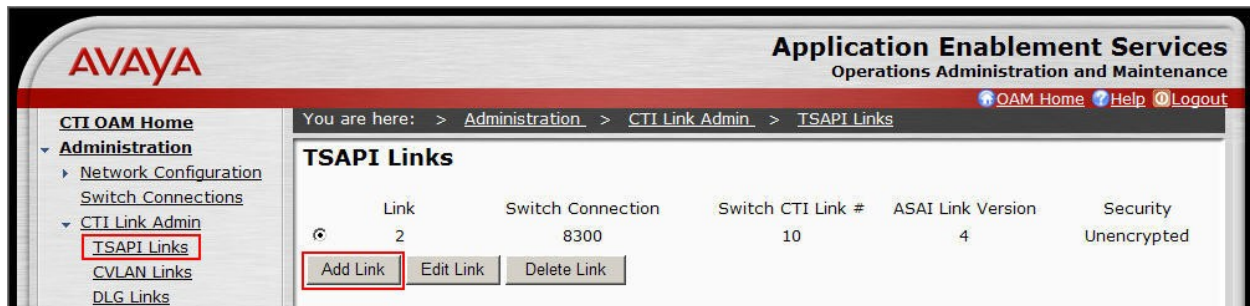
DMCC Server Ports

		Enabled	Disabled
Unencrypted Port	4721	<input type="radio"/>	<input checked="" type="radio"/>
Encrypted Port	4722	<input checked="" type="radio"/>	<input type="radio"/>
TR/87 Port	4723	<input type="radio"/>	<input checked="" type="radio"/>

5.3. Configure TSAPI Link

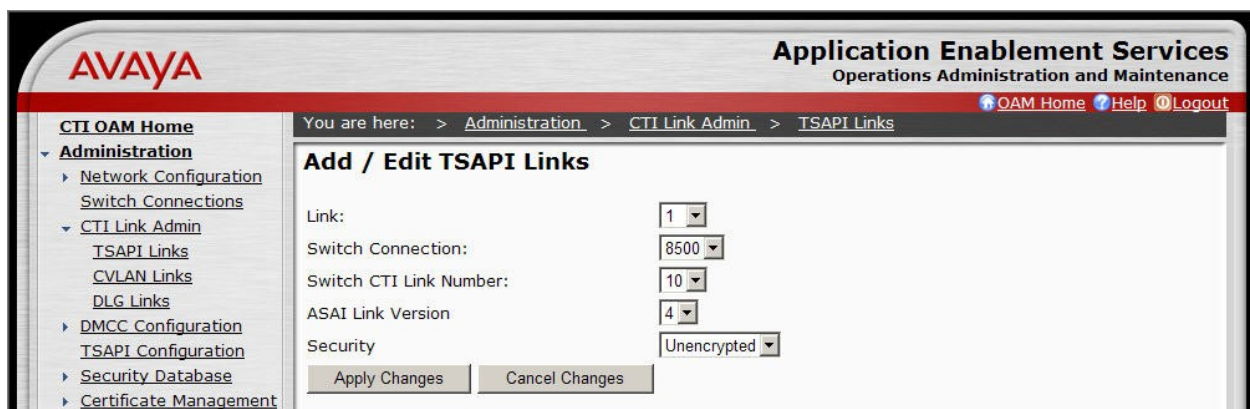
This section provides the steps required for configuring a TSAPI Link.

1. From the CTI OAM main menu select **Administration > CTI Link Admin > TSAPI Links**. Click **Add Link**.



2. Complete the “Add / Edit TSAPI Links” page as follows:

- In the **Link** field, select an available link number.
- In the **Switch Connection** field, select the switch connection configured in **Section 5.1**.
- In the **Switch CTI Link Number** field, select the CTI link number that was administered on Communication Manager in **Step 2** of **Section 4.3**.
- In the **ASAI Link Version** field, select the default value, **4**.
- In the **Security** field, select the appropriate encryption option for connectivity to the Co-nexus CXM server.

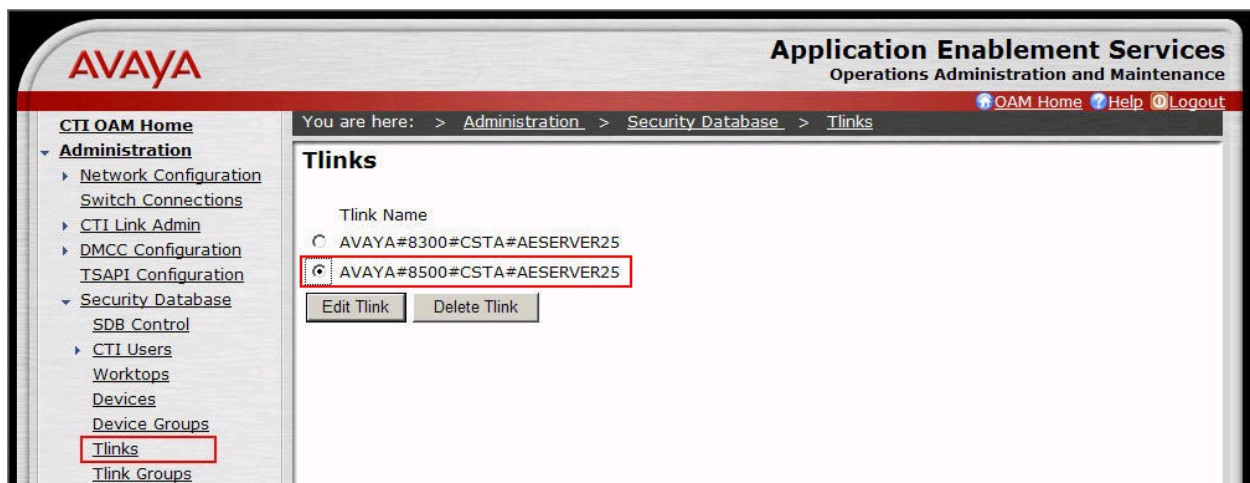


5.4. Display Tlink

This section provides the steps required to display Tlinks.

Tlinks are service identifiers (names) dynamically created by the TSAPI Service. Tlinks are created automatically once the TSAPI CTI links are created. The appropriate Tlink name will be needed during the configuration of the Co-nexus CXM server. This section just illustrates how to obtain the Tlink name.

1. Navigate to **Administration > Security Database > CTI Users > Tlinks**.



To identify the correct Tlink, note that a Tlink has the following format:

AVAYA#switch_connection_name#service_type#AE_server_name

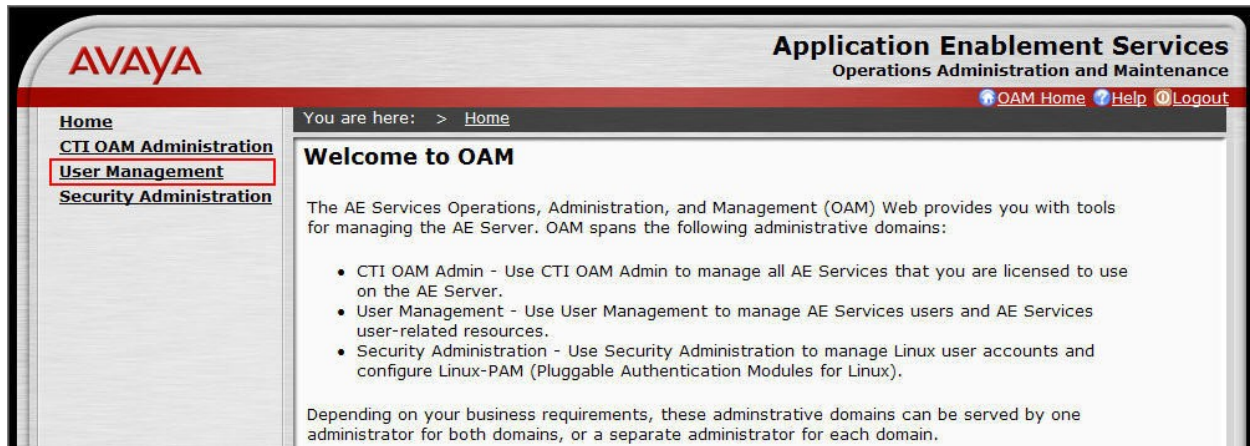
where:

- **AVAYA** is a fixed constant.
- **switch_connection_name** represents the Switch Connection name administered in **Section 5.1**.
- **service_type** refers to the CSTA service type. It can be either of the following:
 - **CSTA**, if the TSAPI Link was administered as unencrypted in **Section 5.3**.
 - **CSTA-S**, if the TSAPI Link was administered as encrypted in **Section 5.3**.
- **AE_server_name** represents the Application Enablement Services Server name.

5.5. Configure CTI Users

This section provides the steps required to configure a CTI user. If necessary, log in to the Application Enablement Services server again with the appropriate credentials for accessing the “User Management” pages.

1. Navigate to the “OAM Home” page. Select **User Management** from the left pane menu.



2. Navigate to **User Management > Add User**. On the “Add User” page, provide the following information:

- In the **User Id** field, type the user ID being assigned to the user.
- In the **Common Name** field, enter the name the user prefers to use.
- In the **Surname** field, type the surname.
- In the **User Password** field, type the password being assigned to the user.
- In the **Confirm Password** field, re-type the assigned password.
- In the **CT User field**, select **Yes** to add the user as a member of the Security Database (SDB).

Click the **Apply** button (not shown) at the bottom of the screen.

AVAYA Application Enablement Services
Operations Administration and Maintenance

[OAM Home](#) [Help](#) [Logout](#)

User Management Home You are here: > [User Management](#) > [Add User](#)

Add User

Fields marked with * can not be empty.

* User Id

* Common Name

* Surname

* User Password

* Confirm Password

Admin Note

Avaya Role

Business Category

Car License

CM Home

Css Home

CT User

Department Number

3. Select **OAM Home** in upper right and navigate to the **CTI OAM Administration** → **Security Database** → **CTI Users** → **List All Users** page. Select the **User ID** created in **Step 2**, and click the **Edit** button to set the permissions of the user.

AVAYA Application Enablement Services
Operations Administration and Maintenance

You are here: > Administration > Security Database > CTI Users > List All Users

CTI Users

	User ID	Common Name	Worktop Name	Device ID
<input checked="" type="radio"/>	DevConnect	DevConnect	NONE	NONE
<input type="radio"/>	test0	test0	NONE	NONE
<input type="radio"/>	test1	test1	NONE	NONE
<input type="radio"/>	test2	test2	NONE	NONE
<input type="radio"/>	test3	test3	NONE	NONE
<input type="radio"/>	test4	test4	NONE	NONE
<input type="radio"/>	test5	test5	NONE	NONE
<input type="radio"/>	test6	test6	NONE	NONE
<input type="radio"/>	test7	test7	NONE	NONE
<input type="radio"/>	test8	test8	NONE	NONE
<input type="radio"/>	test9	test9	NONE	NONE

4. Provide the user with unrestricted access privileges by clicking the **Enable** button on the **Unrestricted Access** field. A Warning screen will be displayed (not shown). Click **Apply**.

AVAYA Application Enablement Services
Operations Administration and Maintenance

You are here: > Administration > Security Database > CTI Users > List All Users

Edit CTI User

User ID: DevConnect
Common Name: DevConnect
Worktop Name: NONE
Unrestricted Access:

Call Origination and Termination: None

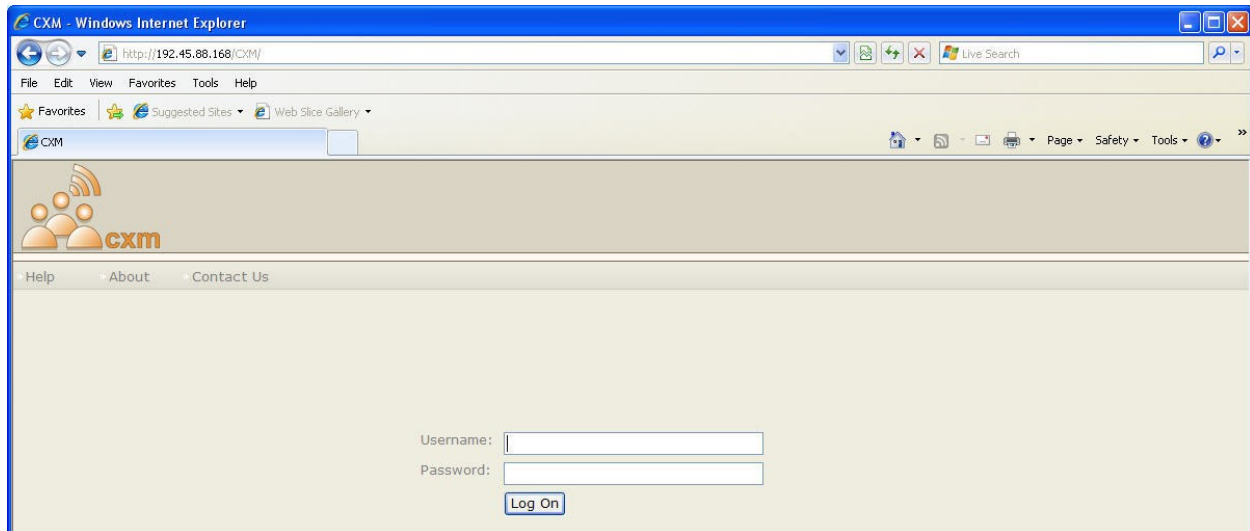
Device / Device: None
Call / Device: None
Call / Call: ☐

Allow Routing on Listed Device: None

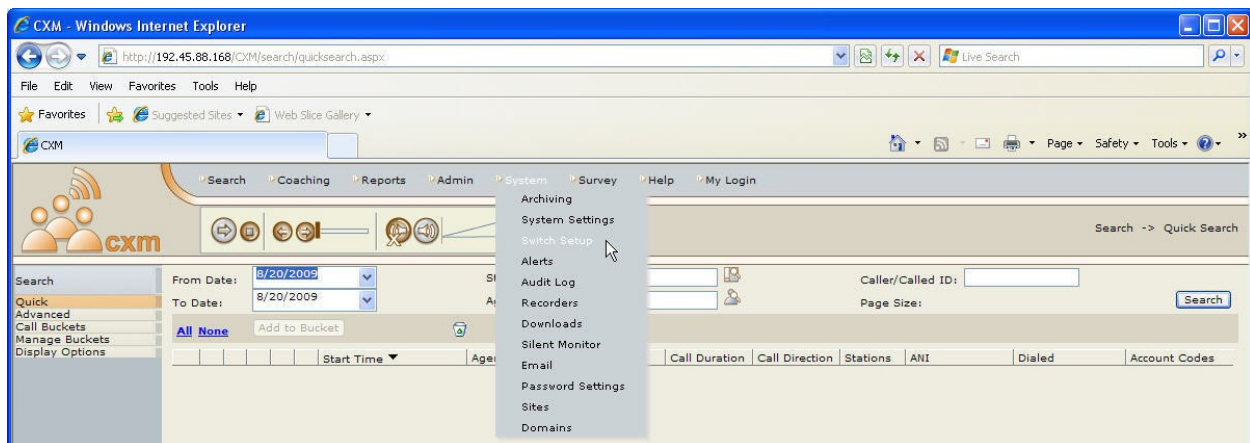
6. Configure Co-nexus CXM

This section describes the configuration required for the Co-nexus CXM server to interface with Application Enablement Services and Communication Manager.

1. Launch a web browser, enter <http://<IP address of Co-nexus server>/CXM> in the URL, and log in with the appropriate credentials.



2. Use the menu on top of the screen to select the **System → Switch Setup** link.



3. On the **Switch Setup** screen, provide the following information:

- In the **Configuration** drop down menu, select **Avaya Single Step DMCC**.
- In the **PBX Name** field, enter the switch connection name from **Section 5.1**.
- In the **DMCC Server IP** field, enter the IP address of the Application Enablement Services server.
- In the **DMCC Server Port** field, enter the DMCC port from **Section 5.2**.
- In the **DMCC Login** and **DMCC Password** fields, enter the user ID and password from **Section 5.5**.
- In the **Communication Manager IP** field, enter the CLAN IP address from **Section 4.2**.
- If the **Extension Password** field, enter the Security Code of the DMCC recording devices from **Section 4.4**.

CXM - Windows Internet Explorer

http://192.45.88.168/CXM/sys/switchsetup.aspx

File Edit View Favorites Tools Help

Search Coaching Reports Admin System Survey Help My Login

System -> Switch Setup

Configuration: Avaya Single Step DMCC

PBX Name: 8500

TSAPI Server Name: AVAYA#8500#CSTA#AESERVER25

TSAPI Application: CXM4

Private Data Version: 6

☒ Enable Call Monitors

☐ Zip Tone Processing

DMCC Server IP: 192.45.88.25

DMCC Server Port: 4722

DMCC Login: DevConnect

DMCC Password: DevConnect123.

DMCC Protocol Version: 3.0

Communication Manager IP: 192.45.88.10

Voice Int Controller IP: 192.45.88.168

Extension Password: 123456

Access Codes: 9

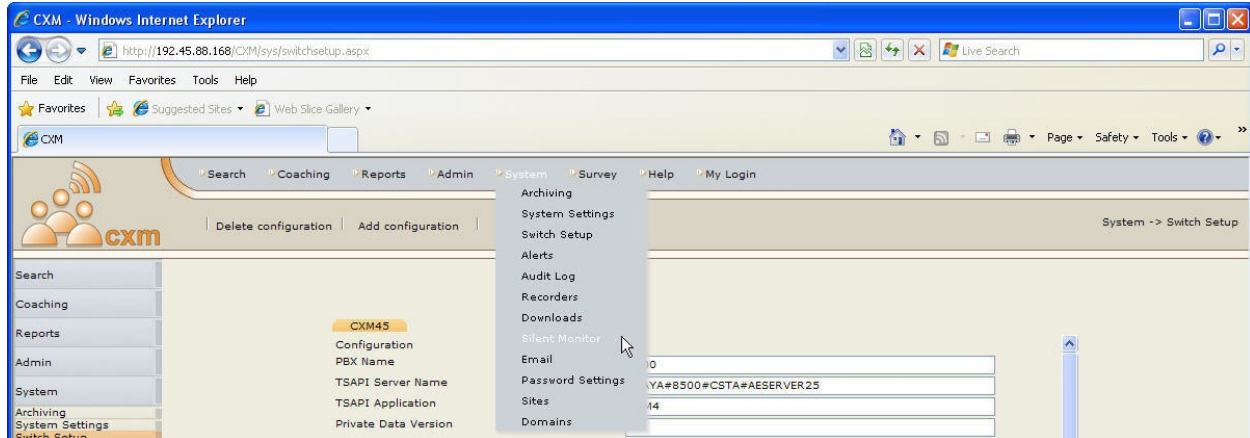
☐ Screen Capture

☒ Coaching

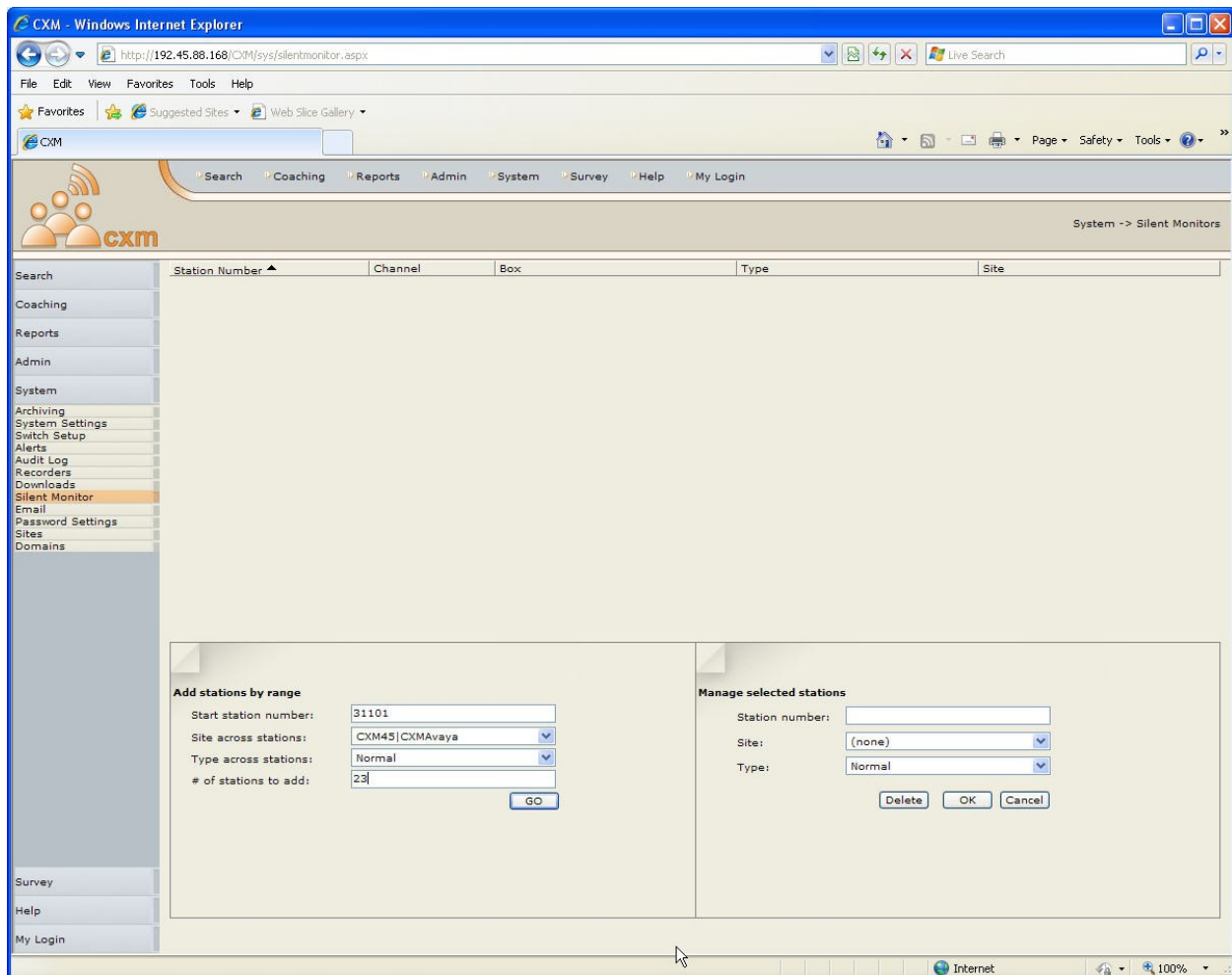
Machine Name: CXMAVAYA

OK

4. Use the menu on top of the screen to select the **System → Silent Monitor** link.



5. Use the **Add stations by range** fields to add the DMCC recording devices from **Section 4.4**.



The screen below shows a subset of the DMCC recording devices used during compliance testing.

The screenshot displays the CXM web application running in a Windows Internet Explorer browser. The address bar shows the URL `http://192.45.88.168/CXM/sys/silentmonitor.aspx`. The application has a navigation menu on the left with options like Search, Coaching, Reports, Admin, System, Survey, Help, and My Login. The main content area shows a table of recording devices under the 'System -> Silent Monitors' section.

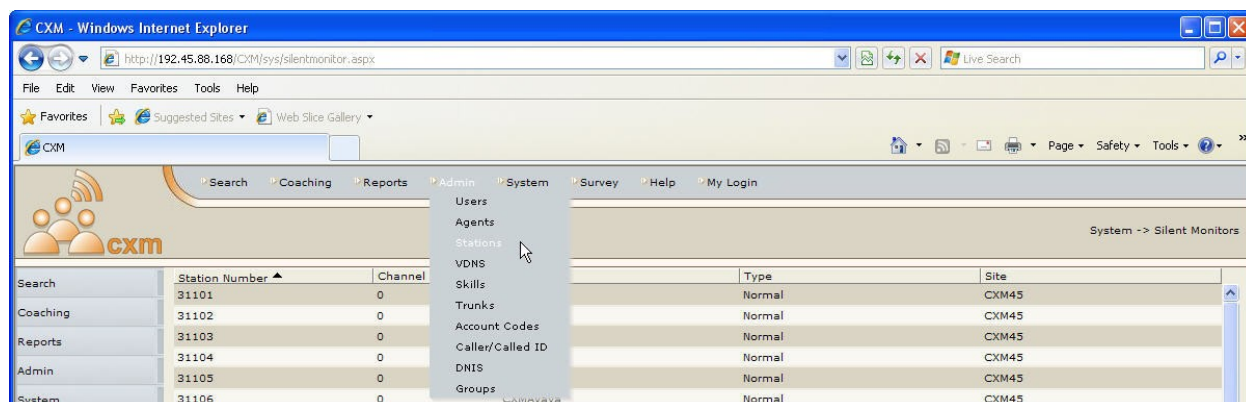
Station Number	Channel	Box	Type	Site
31101	0	CXMAvaya	Normal	CXM45
31102	0	CXMAvaya	Normal	CXM45
31103	0	CXMAvaya	Normal	CXM45
31104	0	CXMAvaya	Normal	CXM45
31105	0	CXMAvaya	Normal	CXM45
31106	0	CXMAvaya	Normal	CXM45
31107	0	CXMAvaya	Normal	CXM45
31108	0	CXMAvaya	Normal	CXM45
31109	0	CXMAvaya	Normal	CXM45
31110	0	CXMAvaya	Normal	CXM45
31111	0	CXMAvaya	Normal	CXM45
31112	0	CXMAvaya	Normal	CXM45
31113	0	CXMAvaya	Normal	CXM45
31114	0	CXMAvaya	Normal	CXM45
31115	0	CXMAvaya	Normal	CXM45
31116	0	CXMAvaya	Normal	CXM45
31117	0	CXMAvaya	Normal	CXM45
31118	0	CXMAvaya	Normal	CXM45

Below the table, there are two panels for managing stations:

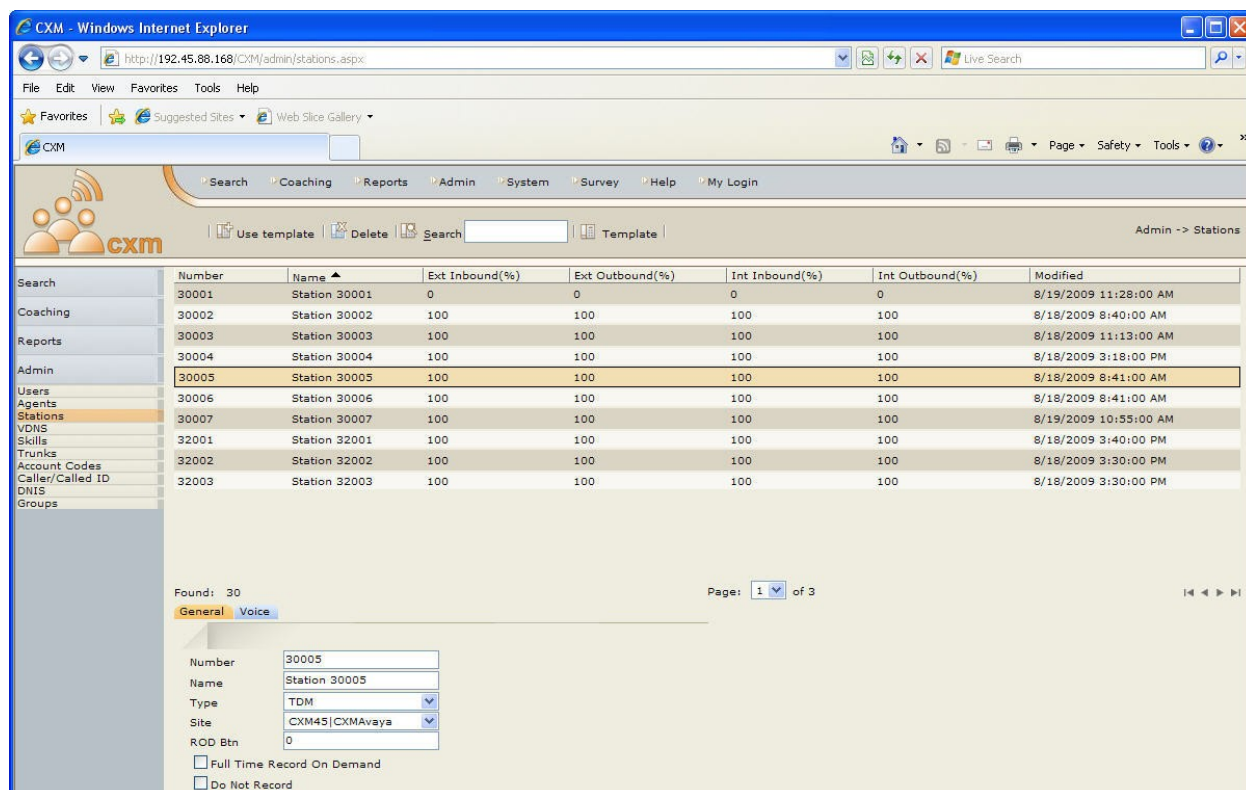
- Add stations by range:** Includes fields for 'Start station number', 'Site across stations' (set to '(none)'), 'Type across stations' (set to 'Normal'), and '# of stations to add'. A 'GO' button is present.
- Manage selected stations:** Includes fields for 'Station number', 'Site' (set to '(none)'), and 'Type' (set to 'Normal'). 'Delete', 'OK', and 'Cancel' buttons are present.

A green status message at the bottom left reads: 'Stations successfully added!'.

- Use the **Admin** menu on top of the screen to select objects to be administered. Refer to the Co-nexus documentation for more details. During compliance testing, Agents, Stations, and VDNs were administered. As an example, to administer the stations to be recorded, select the **Admin → Stations** link.



The screen below shows a subset of the stations that were used during compliance testing.



7. General Test Approach and Test Results

The general test approach was to place calls and use basic telephony operations to verify that Co-nexus CXM could properly record the calls, associate the calls with the correct stations and agents, and to confirm that quality recordings could be retrieved and played back. The test cases were broken down into three categories: feature testing, serviceability testing, and performance testing.

For feature testing, several types of calls were placed, including:

- Internal calls
- Inbound trunk calls
- Outbound trunk calls
- Transfer and Conference calls

The calls were placed to and from various endpoints, including: stations, agents, VDNs, and hunt groups.

For serviceability testing, failure conditions were introduced into the test configuration, such as network cable pulls, CTI link busyouts, and server resets to verify that Co-nexus CXM could properly resume operation after failure recovery.

For performance testing, a sustained volume of calls were generated for an extended period of time to verify that Co-nexus CXM could record all the calls during that time period.

All test cases were executed and passed.

8. Verification Steps

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

8.1. Verify Communication Manager

This section provides the steps required to verify the status of the link(s) to Application Enablement Services and the CTI link.

1. Enter the **status aesvcs link** command. Verify the **Remote IP** is the IP address of the Application Enablement Services server, the **Local Node** displays each CLAN used for connectivity to Application Enablement Services, and that there is appropriate message traffic over the links (**Msgs Sent** and **Msgs Rcvd**).

status aesvcs link						
AE SERVICES LINK STATUS						
Srvr/ Link	AE Services Server	Remote IP	Remote Port	Local Node	Msgs Sent	Msgs Rcvd
01/01	aeserver25	192. 45. 88. 25	56300	CLAN2	207	192
01/02	aeserver25	192. 45. 88. 25	56302	CLAN4	180	180
01/03	aeserver25	192. 45. 88. 25	56304	CLAN3	180	180

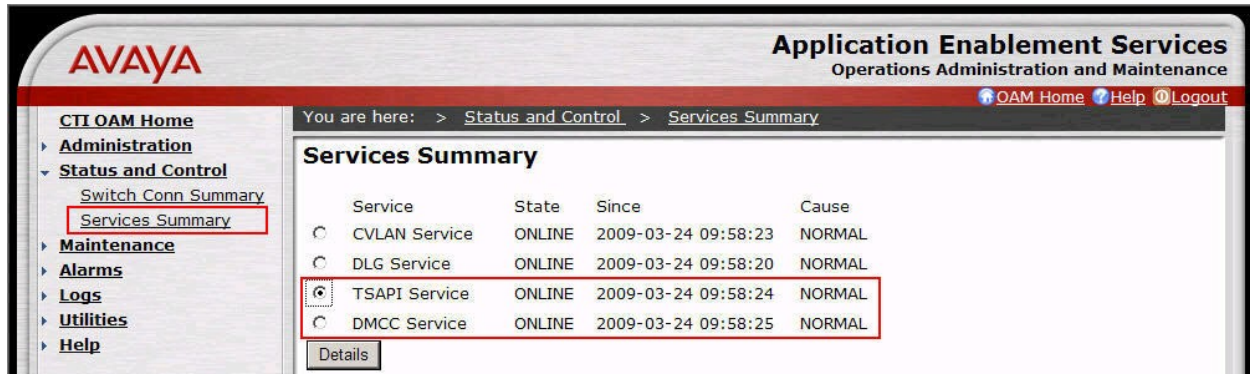
2. Enter the **status aesvcs cti-link** command. Verify the **Service State** is **established** for the CTI link number administered in **Section 4.3**.

status aesvcs cti-link						
AE SERVICES CTI LINK STATUS						
CTI Link	Version	Mnt Busy	AE Services Server	Service State	Msgs Sent	Msgs Rcvd
1		no		down	0	0
2		no		down	0	0
3		no		down	0	0
4		no		down	0	0
5		no		down	0	0
6		no		down	0	0
7		no		down	0	0
8		no		down	0	0
9		no		down	0	0
10	4	no	aeserver25	established	15	15

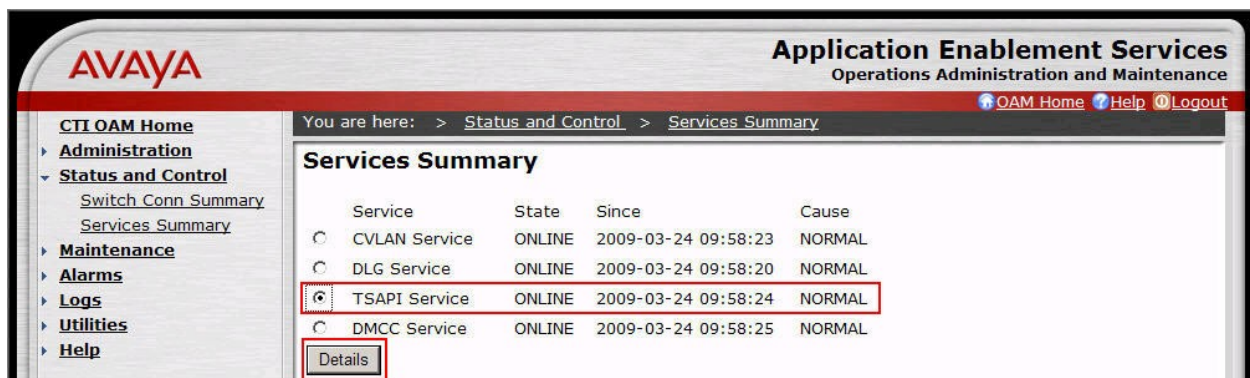
8.2. Verify Application Enablement Services

This section provides the steps required to verify the status of the TSAPI and DMCC services.

1. From the Application Enablement Services “CTI OAM Admin” web pages, navigate to **Status and Control > Services Summary** in the left pane menu. Verify that the **State** of the **TSAPI Service** and the **DMCC Service** is **ONLINE**.



2. Select the radio button for **TSAPI Service**, and click **Details**.



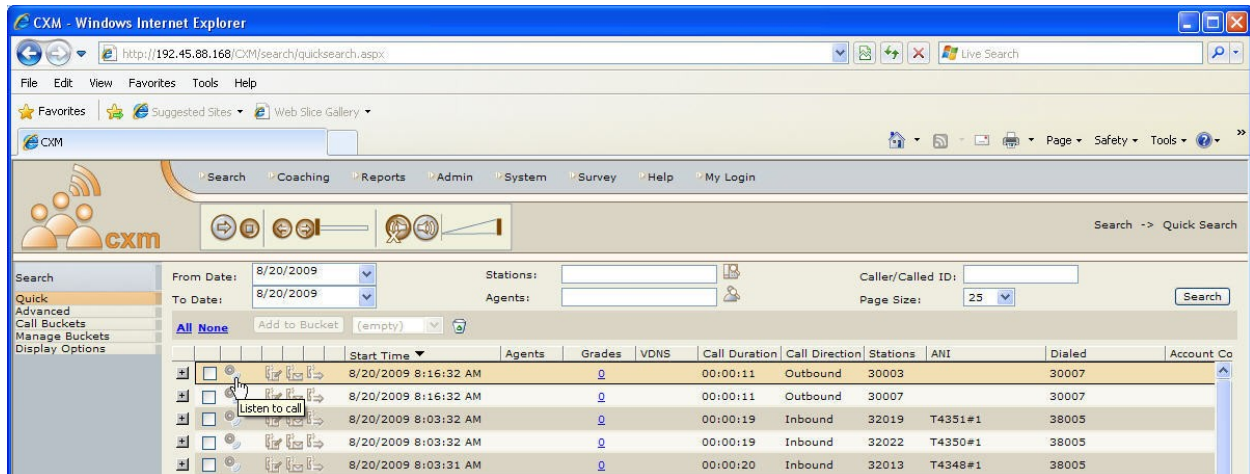
3. Verify that the **Conn Status** is **Talking** for the TSAPI link administered in **Section 5.3**.

8.3. Verify Co-nexus CXM Call Recordings

This section provides the steps required to verify calls are being recorded properly by the Co-nexus CXM server.

1. Place several calls to and from recorded stations. Use the menu on top of the screen to select the **Search → Quick** link.

2. Click the **Listen to call** icon to listen to one of the recorded calls. Verify the entire call was recorded and verify the quality of the recording.



- Click the “+” icon at the beginning of the row to expand the call details. Verify the call details are correct.

The screenshot displays the CXM web application interface. The top navigation bar includes links for Search, Coaching, Reports, Admin, System, Survey, Help, and My Login. The left sidebar contains a search filter menu with options like Quick, Advanced, Call Buckets, Manage Buckets, and Display Options. The main content area shows a search results table for calls on 8/20/2009. The table has columns for Start Time, Agents, Grades, VDNS, Call Duration, Call Direction, Stations, ANI, Dialed, and Account Co. The first row is expanded, showing detailed call events for Station 30003.

Start Time	Agents	Grades	VDNS	Call Duration	Call Direction	Stations	ANI	Dialed	Account Co
8/20/2009 8:16:32 AM				00:00:11	Outbound	30003		30007	
8/20/2009 8:16:32 AM - Station 30003 originated a call.									
8/20/2009 8:16:32 AM - Station 30003 call was delivered.									
8/20/2009 8:16:32 AM - Station 30007 received the call.									
8/20/2009 8:16:32 AM - Station 30003 call was delivered.									
8/20/2009 8:16:32 AM - Station 30007 received the call.									
8/20/2009 8:16:33 AM - The call established at Station 30003.									
8/20/2009 8:16:43 AM - Connection cleared.									
8/20/2009 8:16:43 AM - Connection cleared.									
8/20/2009 8:16:43 AM - Call cleared.									
8/20/2009 8:16:32 AM				00:00:11	Outbound	30007		30007	
8/20/2009 8:03:32 AM				00:00:19	Inbound	32019	T4351#1	38005	
8/20/2009 8:03:32 AM				00:00:19	Inbound	32022	T4350#1	38005	
8/20/2009 8:03:31 AM				00:00:20	Inbound	32013	T4348#1	38005	
8/20/2009 8:03:31 AM				00:00:20	Inbound	32021	T4349#1	38005	
8/20/2009 8:03:27 AM				00:00:24	Inbound	32002	T4331#1	38005	
8/20/2009 8:03:27 AM				00:00:23	Inbound	32012	T4330#1	38005	
8/20/2009 8:03:26 AM				00:00:24	Inbound	32008	T4329#1	38005	
8/20/2009 8:03:00 AM				00:00:30	Inbound	32022	T4327#1	38005	
8/20/2009 8:03:00 AM				00:00:30	Inbound	32019	T4328#1	38005	
8/20/2009 8:02:59 AM				00:00:30	Inbound	32013	T4325#1	38005	
8/20/2009 8:02:59 AM				00:00:31	Inbound	32021	T4326#1	38005	
8/20/2009 8:02:58 AM				00:00:31	Inbound	32016	T4323#1	38005	
8/20/2009 8:02:58 AM				00:00:31	Inbound	32014	T4324#1	38005	

Events: 10789 Page: 1 of 432

9. Conclusion

These Application Notes describe the configuration steps required for Co-nexus CXM 4.5 to interoperate with Avaya Aura™ Communication Manager and Avaya Aura™ Application Enablement Services. All feature, serviceability, and performance test cases were completed and passed.

10. Additional References

This section references the Avaya and Co-nexus product documentation that are relevant to these Application Notes.

The following Avaya product documentation can be found at <http://support.avaya.com>:

[1] *Administering Avaya Aura™ Communication Manager*, Doc ID: 03-300509, Issue 5.0, Release 5.2, May 2009

[2] *Avaya MultiVantage Application Enablement Services Administration and Maintenance Guide*, Doc ID: 02-300357, Release 4.2, Issue 10, May 2008

Co-nexus CXM product documentation can be obtained by contacting Co-nexus. Contact information for Co-nexus can be found at <http://www.4cxm.com/cont.asp>.

©2009 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.