

Avaya Solution & Interoperability Test Lab

## Application Notes for Co-nexus CXM with Avaya Aura<sup>TM</sup> Communication Manager and Avaya Aura<sup>TM</sup> Application Enablement Services – Issue 1.0

### Abstract

These Application Notes describe the configuration steps required for Co-nexus CXM to interoperate with Avaya Aura<sup>TM</sup> Communication Manager and Avaya Aura<sup>TM</sup> 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<sup>TM</sup> Communication Manager, an Avaya Aura<sup>TM</sup> 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. Conexus CXM uses the softphones as recording devices. When recording of a call is desired, Conexus 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: <u>SupportCXM@4cxm.com</u>

## 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.

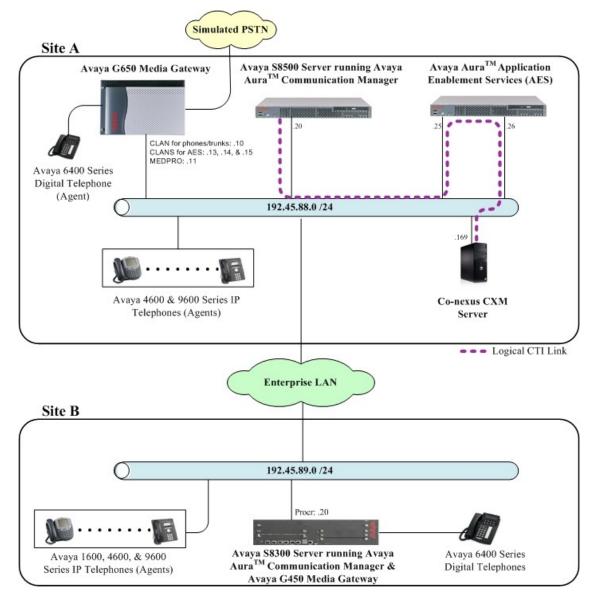


Figure 1: Co-nexus CXM with Communication Manager and AES

MJH; Reviewed: SPOC 9/28/2009 Solution & Interoperability Test Lab Application Notes ©2009 Avaya Inc. All Rights Reserved.

## 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 <sup>TM</sup>
	Communication Manager
	5.2 (R015x.02.0.947.3)
Avaya S8300 Server (w/ G450)	Avaya Aura <sup>TM</sup>
	Communication Manager
	5.2 (R015x.02.0.947.3)
Avaya G650 Media Gateway:	
TN799DP (C-LAN)	HW01, FW026
TN2602AP (MEDPRO)	HW02, FW007
TN2312BP (IPSI)	HW15, FW030
Avaya G450 Media Gateway :	
MM710BP (DS1)	HW11, FW044
MM712AP (DCP)	HW07, FW009
Avaya Aura <sup>TM</sup> Application Enablement Services (AES)	4.2
Server	
Avaya C364T-PWR Converged Stackable Switch	4.5.14
Avaya 1600 Series IP Phones :	
1608SW (H.323)	1.0.3
1616SW (H.323)	1.0.3
Avaya 4600 Series IP Phones:	
4610SW (H.323)	2.9
4620SW (H.323)	2.9
4621SW (H.323)	2.9
Avaya 9600 Series IP Phones:	
9620 (H.323)	3.002
9230 (SIP)	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
                                                                                      1 of
                                                                                               2
                                                                              Page
                               IP Codec Set
    Codec Set: 1
AudioSilenceFramesPacketCodecSuppressionPer PktSize(ms)1: G.711MUn220
 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
                Authoritative Domain: dev8.com
Location: 1
    Name: interop
MEDIA PARAMETERS
                                    Intra-region IP-IP Direct Audio: yes
                              Intra-region IP-IP Direct Audio: yes
Inter-region IP-IP Direct Audio: yes
      Codec Set: 1
   UDP Port Min: 2048
                                                  IP Audio Hairpinning? y
   UDP Port Max: 65535
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
UDP Port Max: 65535
DIFFSERV/TOS PARAMETERS
         Video PHB Value: 26
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
                                                                  RSVP Enabled? n
 H.323 Link Bounce Recovery? y
 Idle Traffic Interval (sec): 20
  Keep-Alive Interval (sec): 5
             Keep-Alive Count: 5
```

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	s ip			P	age	1 of	2
-	I	P 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						
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
           Slot: 01A02Target socket load and Warning level: 400Code/Suffix: TN799DReceive Buffer TCP Window Size: 8320
                   Slot: 01A02
      Enable Interface? y
                                                        Allow H.323 Endpoints? y
                                                         Allow H.248 Gateways? y
                   VLAN: n
        Network Region: 1
                                                           Gatekeeper Priority: 5
                                    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-s	ervices				Page	<b>1</b> of	4
Service Type AESVCS AESVCS AESVCS	Enabled Y Y Y	Local Node CLAN2 CLAN3 CLAN4	IP SERVICES Local Port 8765 8765 8765	Remote Node	Remote Port		

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-ser	rvices			Page	<b>4</b> of	4
	Al	E Services Administ	ration			
Server ID	AE Services Server	Password	Enabled	Status		
1: 2:	aeserver25	*****	У	in use		
3:						

#### 4.3. Configure CTI Link

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 **3** of 11 Page OPTIONAL FEATURES Audible Message Waiting? y Access Security Gateway (ASG)? n Analog Trunk Incoming Call ID? y CAS Branch? n Abbreviated Dialing Enhanced List? y 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

      CTI LINK

      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 sys	tem-parameters c	ustomer-options	Page 10 of 11
	MAXIMU	M 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
                                        Lock Messages? n
Security Code: 31126
Extension: 31126
                                                                      BCC: 0
    Type: 4620
                                                                       TN: 1
                                      Coverage Path 1:
                                                                       COR: 1
    Port: IP
                                                                      COS: 1
    Name: DMCC Softphone
                                      Coverage Path 2:
                                     Hunt-to Station:
STATION OPTIONS
                                          Time of Day Lock Table:
             Loss Group: 19 Personalized Ringing Pattern: 1
      Speakerphone: 2-way
Display Language: english
vable GK Node Name:
                                                Message Lamp Ext: 31126
                                            Mute Button Enabled? y
                                               Expansion Module? n
Survivable GK Node Name:
        Survivable COR: internal Media Complex Ext:
  Survivable Trunk Dest? y
                                                    IP SoftPhone? y
                                                        IP Video? n
                                             Customizable Labels? Y
```

This completes the Avaya Aura<sup>TM</sup> 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 <u>https://<IP address of AES Server></u> in the address field. Click **AE Server Administration**.

VAYA	Application Enablement Service
Server Administration	
bLM 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 oriminal 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 oriminal 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.

Application Enablement Servi	ices ? Hel
Please log on.	
Logon:	
Password:	
	Login

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

ΑνΑγΑ	Application Enablement Service Operations Administration and Maintenar
	G OAM Home @Help @Log
Home	You are here: > <u>Home</u>
CTI OAM Administratio	Welcome to OAM
Security Administration	for managing the AE Server. OAM spans the following administrative domains:
	<ul> <li>CTI OAM Admin - Use CTI OAM Admin to manage all AE Services that you are licensed to use on the AE Server.</li> <li>User Management - Use User Management to manage AE Services users and AE Services</li> </ul>
	User Management - Use User Management to manage AE Services users and AE Services     user-related resources.
	<ul> <li>Security Administration - Use Security Administration to manage Linux user accounts and configure Linux-PAM (Pluggable Authentication Modules for Linux).</li> </ul>
	Depending on your business requirements, these adminstrative domains can be served by one administrator for both domains, or a separate administrator for each domain.

4. 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.

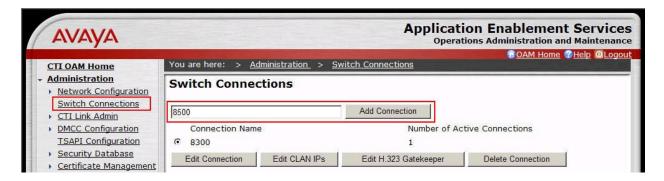
<u>ministration</u> tus and Control intenance rms 15		OAM Screen	5			
	[craft] Last login: Fri M	Welcome to CTI OAM Screens [craft] Last login: Fri Mar 13 11:28:08 2009 from 192.45.88.45				
l <u>ities</u> P	IMPORTANT: AE Service Changes to the Securit		for administrative changes quire a restart.	to fully take effect.		
	Service	Status	State	Licenses Purchased		
	ASAI Link Manager	Running	N/A	N/A		
	DMCC Service	Running	ONLINE	Yes		
	CVLAN Service	Running	ONLINE	Yes		
	DLG Service	Running	ONLINE	Yes		
	Transport Layer Service	Running	N/A	N/A		
	TSAPI Service	Running	ONLINE	Yes		
	SMS For status on actual se	N/A rvices, please use <u>Si</u>	N/A atus and Control.	Yes		
	License Information	Application Enablem	ent (CTI) version 4.			

Solution & Interoperability Test Lab Application Notes ©2009 Avaya Inc. All Rights Reserved. 5. 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.

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

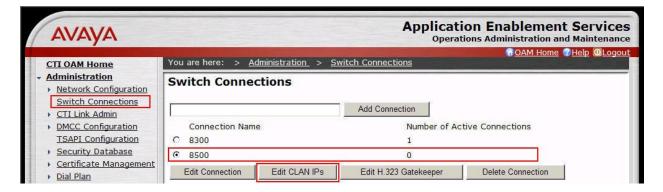


In the Switch Password field, type the password that was entered during Step 3 of Section
 4.2. Re-type the password in the Confirm Switch Password field. Leave SSL checked if using a secure connection to Communication Manager. Click Apply.

AVAYA		Application Enablement Services Operations Administration and Maintenance
CTI OAM Home	You are here: > <u>Administration</u>	> <u>Switch Connections</u>
<ul> <li>Administration</li> <li>Network Configuration</li> </ul>	Set Password - 8500	
Switch Connections CTI Link Admin DMCC Configuration	Please note the following: * Changing the password affects or	nly new connections, not open connections.
TSAPI Configuration  Security Database	Switch Password	•••••
<u>Certificate Management</u>	Confirm Switch Password	•••••
<ul> <li><u>Dial Plan</u></li> <li><u>Enterprise Directory</u></li> <li><u>Host AA</u></li> </ul>	SSL Apply Cancel	<u>ञ</u>

Solution & Interoperability Test Lab Application Notes ©2009 Avaya Inc. All Rights Reserved. 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).

AVAYA			n Enablement Services s Administration and Maintenance
CTI OAM Home Administration Network Configuration	You are here: > <u>Administration</u> > Edit CLAN IPs - 8500	Switch Connections	GOAM Home @Help @Logout
Switch Connections CTI Link Admin DMCC Configuration TSAPI Configuration Security Database	192.45.88.13 Name or IP Address Delete IP	Add Name or IP Status	

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

Αναγα			A	pplication Enablement Services Operations Administration and Maintenance
CTI OAM Home	You are h	nere: > <u>Administration</u>	> <u>Switch Connections</u>	OAM Home @Help @Logout
Administration     Network Configuration     Switch Connections     GTL Link Admin	Edit C	LAN IPs - 8500	Add Name or IP	0
<u>CTI Link Admin</u> DMCC Configuration		Name or IP Address	Status	
TSAPI Configuration	œ	192.45.88.13	In Use	
Security Database	0	192.45.88.14	In Use	
<u>Certificate Management</u> <u>Dial Plan</u> <u>Enterprise Directory</u>	C Delete I	192.45.88.15 P	In Use	

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

AVAYA		Application Enablement Serv Operations Administration and Mainte	
CTI OAM Home	You are here: > <u>Administration</u> > <u>S</u>	Switch Connections	Logou
Administration     Network Configuration	Switch Connections		
Switch Connections CTI Link Admin		Add Connection	
DMCC Configuration	Connection Name	Number of Active Connections	
TSAPI Configuration	C 8300	1	
Security Database	© 8500	3	
<u>Certificate Management</u> <u>Dial Plan</u>	Edit Connection Edit CLAN IPs	Edit H.323 Gatekeeper Delete Connection	

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.

Αναγα			eration Enablement Services erations Administration and Maintenance
CTI OAM Home	You are here: > <u>Administra</u>	ation > <u>Switch Connections</u>	
Administration     Network Configuration	Edit H.323 Gatekee	eper - 8500	
Switch Connections CTI Link Admin	192.45.88.10	Add Name or IP	
DMCC Configuration     TSAPI Configuration     Security Database	Name or IP Add Delete IP	ress	

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

Αναγα	A	pplication Enablement Services Operations Administration and Maintenance
CTI OAM Home	You are here: > <u>Administration</u> > <u>Switch Connections</u>	G <u>OAM Home</u> @Help @Logout
Administration     Network Configuration     Switch Connections     CTI Link Admin	Edit H.323 Gatekeeper - 8500 Add Name or IP	
CITLUNK Admin     DMCC Configuration     TSAPI Configuration     Security Database     Certificate Management.	Name or IP Address          Image: Organization of the second se	

### 5.2. Configure DMCC Server Ports

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

 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.

VAYA			whb	Operat	ions Adm	ablement So
OAM Home	You are here:	> <u>Administration &gt; Networ</u>	k Configuration	> Port	<u>s_</u>	CAM Home CHe
inistration	Ports					
etwork Configuration						
<u>ocal IP</u>	CVLAN Ports			Enabled	d Disabled	
orts		Unencrypted TCP Port	9999	c	0	
tch Connections		Encrypted TCP Port	9998	o	С	
Link Admin				5		1
CC Configuration	DLG Port	TCP Port	5678			
API Configuration	*					
tificate Management	TSAPI Ports		1000		Disabled	
Plan		TSAPI Service Port	450	(•)	0	
erprise Directory		Local TLINK Ports				
st AA		TCP Port Min	1024			
5 Configuration		TCP Port Max	1039			
bLM Configuration						
Iged Alert Config		Unencrypted TLINK Ports				
s and Control		TCP Port Min	1050			
IS		TCP Port Max	1065			
			80			
es		Encrypted TLINK Ports				
		TCP Port Min	1066			
		TCP Port Max	1081			
	DMCC Server			Enabled	d Disabled	1
	i orta	Unencrypted Port	4721	e	0	1
		Encrypted Port	4722	ē	С	
		TR/87 Port	4723		C	1

#### 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.

AVAYA				tion Enablem ations Administration	
CTI OAM Home	You are here: >	<u>Administration &gt; CTI Lin</u>	<u>k Admin</u> > <u>TSAPI Lin</u>		ome @Help OLogo
<ul> <li>Network Configuration Switch Connections</li> <li>CTI Link Admin</li> <li>TSAPI Links</li> <li>CVLAN Links</li> <li>DLG Links</li> </ul>	Link C 2 Add Link Edit L	Switch Connection 8300 ink Delete Link	Switch CTI Link # 10	ASAI Link Version 4	Security Unencrypted

- 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 Conexus CXM server.

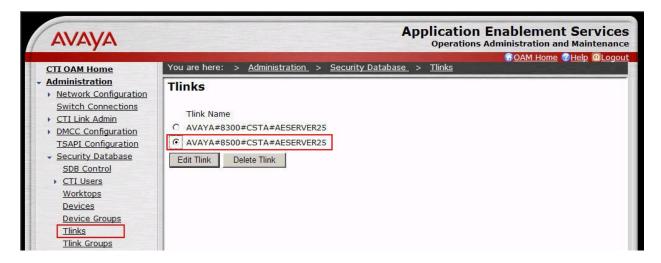
Αναγα		Application Enablement Servic Operations Administration and Maintena
CTI OAM Home	You are here: > <u>Administration</u>	<u>CTI Link Admin</u> > <u>TSAPI Links</u>
Administration     Network Configuration	Add / Edit TSAPI Links	
Switch Connections CTI Link Admin	Link:	
<u>TSAPI Links</u> <u>CVLAN Links</u>	Switch Connection: Switch CTI Link Number:	8500 -
DLG Links DMCC Configuration TSAPI Configuration	ASAI Link Version Security	4  Unencrypted
Security Database     Certificate Management	Apply Changes Cancel Chan	ges

#### 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.

Αναγα	Application Enablement Services Operations Administration and Maintenance	
Home	You are here: > <u>Home</u>	
CTI OAM Administration User Management	Welcome to OAM	
Security Administration	The AE Services Operations, Administration, and Management (OAM) Web provides you with tools for managing the AE Server. OAM spans the following administrative domains:	
	<ul> <li>CTI OAM Admin - Use CTI OAM Admin to manage all AE Services that you are licensed to use on the AE Server.</li> </ul>	
	<ul> <li>User Management - Use User Management to manage AE Services users and AE Services user-related resources.</li> </ul>	
	<ul> <li>Security Administration - Use Security Administration to manage Linux user accounts and configure Linux-PAM (Pluggable Authentication Modules for Linux).</li> </ul>	
	Depending on your business requirements, these adminstrative domains can be served by one administrator for both domains, or a separate administrator for each domain.	

- 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.

Αναγα		Application Enablement Services Operations Administration and Maintenance
User Management Home	You are here: > <u>User Management</u> > <u>Add User</u>	
<ul> <li>User Management. List All Users</li> <li>Add User</li> <li>Search Users</li> <li>Modify Default User. Change User Password</li> <li>Service Management.</li> <li>Help.</li> </ul>	Add User Fields marked with * can not be empty.	
	* User Id DevConnect * Common Name DevConnect * Surname DevConnect * User Password * Confirm Password	
	Admin Note Avaya Role None Business Category Car License CM Home Css Home CT User Yes • 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.

ΑνΑγΑ						Enablement Service
CTI OAM Home	You are he	ere: > <u>Administr</u>	ation > <u>Sec</u> ı	irity Databa	se_ > CTIUsers_ >	OAM Home 7Help OLogou List All Users
Administration     Network Configuration     Switch Connections	CTI Us	ers				
<u>CTI Link Admin</u>		User ID	Common Nam	e Worktop N	Name Device ID	
DMCC Configuration     TSAPI Configuration	e	DevConnect	DevConnect	NONE	NONE	
Security Database	0	test0	test0	NONE	NONE	
SDB Control	0	test1	test1	NONE	NONE	
<u>CTI Users</u>	0	test2	test2	NONE	NONE	
List All Users	0	test3	test3	NONE	NONE	
Search Users	0	test4	test4	NONE	NONE	
Worktops Devices	0	test5	test5	NONE	NONE	
Device Groups	C	test6	test6	NONE	NONE	
Tlinks	C	test7	test7	NONE	NONE	
Tlink Groups		test8	test8	NONE	NONE	
<ul> <li><u>Certificate Management</u></li> <li><u>Dial Plan</u></li> </ul>	c	test9	test9	NONE	NONE	
Enterprise Directory Host AA SMS Configuration WebLM Configuration	Edit Lis	t All				

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
CTI OAM Home	You are here: > <u>Administration</u> > <u>Se</u>	©OAM Home @Help @Logout curity Database_ > CTI Users_ > List All Users_
<ul> <li>Administration         <ul> <li>Network Configuration Switch Connections</li> <li>CTI Link Admin.</li> <li>DMCC Configuration TSAPI Configuration</li> <li>Security Database SDB Control</li> <li>CTI Users List All Users</li> </ul> </li> </ul>	Edit CTI User         User ID       DevConne         Common Name       DevConne         Worktop Name       NONE          Unrestricted Access       Enable         Call Origination and Termination       None	
Search Users Worktops Devices Device Groups Tlinks Tlink Groups • Certificate Management • Dial Plan	Device / Device None  Call / Device None  Call / Call Allow Routing on Listed Device None  Apply Changes Cancel	

## 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.

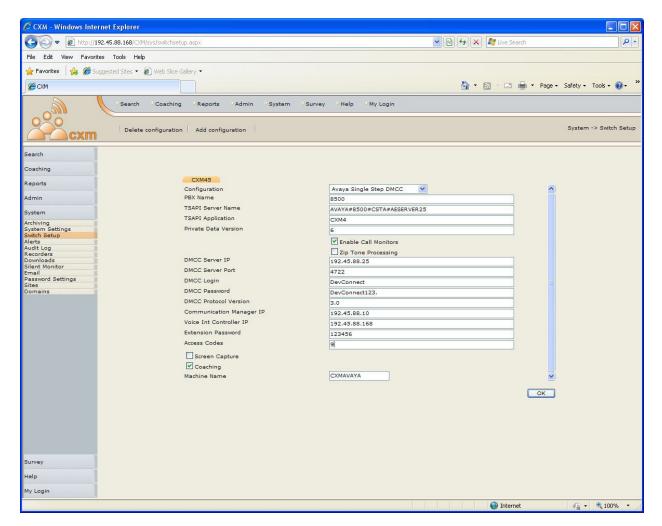
1. Launch a web browser, enter <u>http://<IP address of Co-nexus server>/CXM</u> in the URL, and log in with the appropriate credentials.

CXM - Windows Internet Explorer		
	💌 🗟 🚧 🗙 ಶ Live Search	P -
File Edit View Favorites Tools Help		
🖕 Favorites 🛛 🚖 🍘 Suggested Sites 🔹 🖻 Web Slice Gallery 🔹		
<i>€</i> CXM	🏠 🔻 🔝 🚽 🗔 🕈 Page + Safety + Tools + (	0- »
2°Cxm		
Help About Contact Us		
	ssword:	
	Log On	

2. Use the menu on top of the screen to select the System  $\rightarrow$  Switch Setup link.

CXM - Windows Internet Explorer			
🚱 🕤 🔻 🔊 http://192.45.88.168/CXM/search/quicksearch.aspx		💌 🗟 😽 🗙 🖉 Live Search	5
File Edit View Favorites Tools Help			
🚖 Favorites 🛛 🚔 🏉 Suggested Sites 👻 🙋 Web Slice Gallery 👻			
€ CXM		🏠 🔻 🔝 🚽 🗁 👘 👻 Page + Safety +	Tools 🔹 🔞 🔹 🎇
Search Coaching Reports Admin of Search Coaching Reports Admin of Search Coaching Compared Coal Booket Search To Date: 8/20/2009 V Advanced Call Buckets Display Options Start Time ▼ Age	Archiving Archiving System Settings Suitch Setup Alerts Audit Log Recorders Downloads Silent Monitor Email Passvord Settings Sites Domains	Search	-> Quick Search Search

- 3. On the **Switch Setup** screen, provide the following information:
  - In the Configuration drop down menu, select Avaya Single Step DMMC.
  - 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 **DMMC 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.



4. Use the menu on top of the screen to select the System  $\rightarrow$  Silent Monitor link.

CXM - Windows Internet Explore	r				
🚱 🗢 🙋 http://192.45.88.168/C	XM/sys/switchsetup.aspx			💌 🗟 😽 🗙 💐 Live Search	• 9
File Edit View Favorites Tools H	lelp				
🖕 Favorites 🛛 👍 🏉 Suggested Sites 🔹	🕖 Web Slice Gallery 👻				
<i>€</i> CXM				🏠 🔹 🗟 👘 📼 👼 🕶 Pa	age + Safety + Tools + 🔞 + 🎽
Search Dele	h <sup>12</sup> Coaching <sup>12</sup> Reports <sup>12</sup> Admin te configuration   Add configuration	P System P Survey Archiving System Settings Switch Setup	PHelp PMy Login		System -> Switch Setup
Search Coaching		Alerts Audit Log Recorders			
Reports	CXM45 Configuration PBX Name	Downloads Silent Monitor Email			•
Admin System Archiving System Settings Switch Setup	PEX Name TSAPI Server Name TSAPI Application Private Data Version	Password Settings Sites Domains	0 \YA#8500#CSTA#AESERVER2 14	5	

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

CXM - Windows Inte	rnet Explorer					
🔆 💽 🗢 🖻 http://1	92.45.88.168/CXM/sys/silentmonito	r.aspx		▼ 8	👌 😽 🗶 🧗 Live Search	P-
File Edit View Favori	tes Tools Help					
🚖 Favorites 🛛 🚖 🏉 S	uggested Sites 👻 🙋 Web Slice Gal	iery 🔻				
CXM					🏠 🔹 🔝 🕘 🖃 🖶 🔹 Page	🔹 Safety 🕶 Tools 👻 🔞 👻 🎽
2 Cxm	Search Coaching	PReports PAdmin	P System P Survey	P Help → My Login		System -> Silent Monitors
Search	Station Number	Channel	Box	Туре	Site	
Coaching						
Reports						
Admin						
System						
Archiving System Settings						
Switch Setup Alerts						
Audit Log Recorders						
Downloads Silent Monitor						
Email Password Settings						
Sites Domains						
Survey	Add stations by range Start station number: Site across stations: Type across stations: # of stations to add:	31101 CXM45]CXMAvaya Normal 23			none) V ormal V Delete OK Cancel	
Help						
My Login						
					😜 Internet	🖓 • 🔍 100% • 🚲

Solution & Interoperability Test Lab Application Notes ©2009 Avaya Inc. All Rights Reserved. The screen below shows a subset of the DMCC recording devices used during compliance testing.

🕒 🗢 🖉 http:	(//192.45.88.168/CXM/sys/silentmonito	or.aspx		~	🔁 😽 🗙 ಶ Live Search	2
File Edit View Fav	vorites Tools Help					
🖕 Favorites 🛛 👍 🏉	🕽 Suggested Sites 🔹 🔊 Web Slice Ga	allery 🕶				
<i>€</i> CXM					🏠 • 🔊 - 🖃 ఉ • Page • Safe	ty + Tools + 🔞 +
×						
2 cxr	P Search Coaching	Reports Adm	in System Survey	≥Help ≥My Login	Syste	m -> Silent Monitor
earch	Station Number	Channel	Box	Туре	Site	
	31101	0	CXMAvaya	Normal	CXM45	4
oaching	31102	0	CXMAvaya	Normal	CXM45	
eports	31103	0	CXMAvaya	Normal	CXM45	
dmin	31104	0	CXMAvaya	Normal	CXM45	
Imin	31105	0	CXMAvaya	Normal	CXM45	
ystem	31106	0	CXMAvaya	Normal	CXM45	
chiving	31107	0	CXMAvaya	Normal	CXM45	
stem Settings itch Setup	31108	0	CXMAvaya	Normal	CXM45	
erts	31109	0	CXMAvaya	Normal	CXM45	
idit Log ecorders	31110	0	CXMAvaya	Normal	CXM45	
ownloads lent Monitor	31111	0	CXMAvaya	Normal	CXM45	
mail	31112	0	CXMAvaya	Normal	CXM45	
assword Settings tes	31113	0	CXMAvaya	Normal	CXM45	
omains	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	
	31118	0	СХМАУауа	Normai	CXM45	1
	4			-		
	Add stations by range			Manage selected station	5	
	Start station number:			Station number:		
	Site across stations:	(none)	~	Site:	(none)	
	Type across stations:	Normal	~			
	# of stations to add:			Type:	Normal	
			GO		Delete OK Cancel	
urvey						
elp						
	Stations successfully added!			1		
y Login						

6. 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.

CAM - WIIIdow	vs Internet Explorer					
G 🖸 🔻 🖻	http://192.45.88.168/CXM/sys/silentmor	nitor.aspx		~	🖌 🗟 😽 🗙 💐 Live Search	- ۹
File Edit View	Favorites Tools Help					
🖕 Favorites 🛛 👍	🌾 🏉 Suggested Sites 👻 🔊 Web Slice	Gallery 🕶				
CXM					🏠 • 🔝 - 🖃 🖶 • Page • Safi	ety + Tools + 🔞 + 🕺
	Search Coaching	g Reports	Admin System Survey	PHelp PMy Login		
	Search Coaching	g Reports	Users Agents	Help My Login	Syst	em -> Silent Monitors
		g Reports	Users Agents Stations VDNS	Type	Syst	em -> Silent Monitors
	xm	-	Users Agents Stations VDNS Skills			em -> Silent Monitors
Search	XM Station Number ▲	Channel	Users Agents Stations VDNS Skills Trunks	Туре	Site	
Search Coaching	Station Number * 31101	Channel 0	Users Agents Stations VDNS Skills Trunks Account Codes	Type Normal	Site CXM45	
Search Coaching Reports	Station Number	Channel 0 0	Users Agents Etation VDNS Skills Trunks Account Codes Caller/Called ID	Type Normal Normal	Site CXM45 CXM45	
Search Coaching Reports Admin	Station Number    Station Number    Station Number	Channel 0 0 0	Users Agents Stations VDNS Skills Trunks Account Codes	Type Normal Normal Normal	Site CXM45 CXM45 CXM45	

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

CXM - Windows	Internet Explorer						
🔆 🕞 🗢 🔁 htt	p://192.45.88.168/CXM	1/admin/stations.aspx				🖌 🗟 😽 🗙 🔊 Live Sea	arch 🖉 🔎
File Edit View Fa	avorites Tools Help						
🚖 Favorites 🛛 🚕 👔	🖉 Suggested Sites 👻 ,	🔊 Web Slice Gallery 🔹					
CXM						🙆 • 📓 · 🖃	🚔 🔹 Page 🔹 Safety 👻 Tools 👻 🔞 👻
	Search	P Coaching P Report	s PAdmin PSyste	m <sup>P</sup> Survey <sup>P</sup> Help	<sup>⊙</sup> My Login		
	n I 🕼 Use	template   🎬 Delete	B Search	🚺 Template			Admin -> Statio
earch	Number	Name 📥	Ext Inbound(%)	Ext Outbound(%)	Int Inbound(%)	Int Outbound(%)	Modified
arch	30001	Station 30001	0	0	0	0	8/19/2009 11:28:00 AM
oaching	30002	Station 30002	100	100	100	100	8/18/2009 8:40:00 AM
ports	30003	Station 30003	100	100	100	100	8/18/2009 11:13:00 AM
	30004	Station 30004	100	100	100	100	8/18/2009 3:18:00 PM
min	30005	Station 30005	100	100	100	100	8/18/2009 8:41:00 AM
ers ents	30006	Station 30006	100	100	100	100	8/18/2009 8:41:00 AM
ations	30007	Station 30007	100	100	100	100	8/19/2009 10:55:00 AM
NS ills	32001	Station 32001	100	100	100	100	8/18/2009 3:40:00 PM
unks count Codes	32002	Station 32002	100	100	100	100	8/18/2009 3:30:00 PM
ount Codes aller/Called ID IIS oups	32003	Station 32003	100	100	100	100	8/18/2009 3:30:00 PM
	Found: 30 General Voi				Page: 1 💙 of 3		14 A Þ
	Number	30005					
	Name	Station 30005					
	Туре	TDM	~				
	Site	CXM45 CXMAvaya	~				
	ROD Btn	0					
	Full Tim	e Record On Demand					
	Do Not F	Record					

## 7. General Test Approach and Test Results

The general test approach was to place calls and use basic telephony operations to verify that Conexus 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/	AE Services	Remote IP	Remote Local Node	Msgs	Msgs
Link	Server		Port	Sent	Rcvd
01/01	aeserver25	192. 45. 88. 25	56302 CLAN4	207	192
01/02	aeserver25	192. 45. 88. 25		180	180
01/03	aeserver25	192. 45. 88. 25		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.

statu	is aesvcs	cti-li	nk			
			AE SERVICES	S CTI LINK STAT	rus	
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.

AVAYA						n Enablement Service
CTI OAM Home	You	are here: > <u>Sta</u>	tus and Co	ntrol > <u>Services Sum</u>	nary	OAM Home @Help @Logou
Administration Status and Control	Se	rvices Summ	ary			
Switch Conn Summary Services Summary Maintenance	c	Service CVLAN Service	State ONLINE	Since 2009-03-24 09:58:23	Cause NORMAL	
<u>Alarms</u> Logs	0	DLG Service TSAPI Service	ONLINE	2009-03-24 09:58:20 2009-03-24 09:58:24	NORMAL	
Utilities Help	0	DMCC Service	ONLINE	2009-03-24 09:58:25	NORMAL	

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

Αναγα				4		n Enablement Services s Administration and Maintenanc
CTI OAM Home	_		itus and Co	ntrol > <u>Services Sum</u> r	mary	OAM Home @Help OLogou
Status and Control     Switch Conn Summary	Sei	rvices Summ	nary			
Services Summary		Service	State	Since	Cause	
Maintenance	0	CVLAN Service	ONLINE	2009-03-24 09:58:23	NORMAL	
Alarms	0	DLG Service	ONLINE	2009-03-24 09:58:20	NORMAL	
Logs	C	TSAPI Service	ONLINE	2009-03-24 09:58:24	NORMAL	
Utilities	C	DMCC Service	ONLINE	2009-03-24 09:58:25	NORMAL	
Help	De	tails				

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

AVAYA						Ар			blement S	
CTI OAM Home > Administration - Status and Control	_		here: > <u>Sta</u> [ <mark>Link Det</mark>	atus and Cont	<u>rol</u> > <u>Ser</u>	vices Summary	L	6	OAM Home @H	lelp OLogo
Switch Conn Summary     Services Summary     Maintenance		Link	Switch	Switch CTI Link Number	Conn Status	Since	Service State	Switch Version	Number of Associations	ASAI Message Rate
Alarms Logs	•	1	8500	10	Talking	2009-03-24 09:58:23.0	Online	15	0	16
> <u>Utilities</u> > <u>Help</u>	0	2	8300	10	Talking	2009-03-24 09:58:23.0	Online	15	0	16

#### 8.3. Verify Co-nexus CXM Call Recordings

This section provides the steps required to verify calls are being recorded properly by the Conexus 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.

CXM - Windows Internet Explorer						
🚱 😔 🔻 🙋 http://192.45.88.168/CXM/admin/stations	.aspx				🖉 😣 😽 🗙 🔊 Live Sea	irch 🛛 🔎 🔹
File Edit View Favorites Tools Help						
🙀 Favorites 🛛 🚔 🏉 Suggested Sites 👻 🔊 Web Slice G	allery 🕶					
<b>€</b> CXM					🏠 • 📾 • 🖃	🖶 🔹 Page 🔹 Safety 🔹 Tools 🔹 🔞 👻
Quick	Reports	RAdmin System	Survey Help	My Login		
Advanced CXIII Buckets	Colete	§earch	Template			Admin -> Stations
Search Nurr Display Options	-	Ext Inbound(%)	Ext Outbound(%)	Int Inbound(%)	Int Outbound(%)	Modified
300ui Station	30001	0	0	0	0	8/19/2009 11:28:00 AM

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.

CVW - MIIIIOM2 I	Internet Explorer										
🕒 🗢 🖉 http	p://192.45.88.168/O	(M/search/quickse	arch.aspx				*	8 4 >	🕻 🔊 Live S	Search	٩
File Edit View Fa	avorites Tools He	elp									
🖕 Favorites 🛛 👍 🄏	🗿 Suggested Sites 🝷	🖉 Web Slice G	allery <del>•</del>								
CXM								<u>6</u> -	<b>S</b> - <b>E</b>	🛛 🖶 🝷 Page 🔹	• Safety • Tools • 🔞 •
000	0			-							Search -> Ouick Sear
earch	From Date:	8/20/2009		Stations:				Caller/Call	ed ID:		Search -> Quick Sear
iearch Quick				Stations: Agents:				Caller/Call Page Size:	S20 S212		Search ** Quick Search
iearch Quick Idvanced Jall Buckets	From Date:	8/20/2009	× ×		[	1000			S20 S212		
learch Quick Idvanced Sall Buckets Janage Buckets	From Date: To Date:	8/20/2009 8/20/2009	× ×		Grades	2	uration Call Direct	Page Size:	25	V Diale	Search
learch Quick Idvanced Sall Buckets Janage Buckets	From Date: To Date:	8/20/2009 8/20/2009	t (empty) V G	Agents:	Grades	2		Page Size:	25		Search
learch Quick Idvanced Sall Buckets Janage Buckets	From Date: To Date: All None	8/20/2009 8/20/2009 Add to Bucke	t (empty) V (a)	Agents: Agents	-	VDNS Call D	11 Outbound	Page Size: ion Stations	25	Diale	Gearch d Account C
earch Quick dvanced Jall Buckets Ianage Buckets	From Date: To Date: All None	  8/20/2009  8/20/2009  Add to Bucke	✓     ✓     ✓     ✓     ✓     ✓     ✓     ✓     ✓     ✓     Start Time ▼     8/20/2009 8:16:32 AB	Agents: Agents M	<u>0</u>	VDNS   Call Do	11 Outbound 11 Outbound	Page Size: ion Stations 30003	25	Diale 3000	d Account C 7 4
Search Quick Advanced Call Buckets Manage Buckets Display Options	From Date: To Date: All None	8/20/2009 8/20/2009 Add to Bucke	✓     ✓     ✓     ✓     ✓     ✓     ✓     ✓     Start Time ▼     8/20/2009 8:16:32 AN     8/20/2009 8:16:32 AN	Agents: Agents M M	<u>0</u> 0	VDNS Call D 00:00: 00:00:	11 Outbound 11 Outbound 19 Inbound	Page Size: ion Stations 30003 30007	25	Diale 3000 3000	d Account C 7 2 5

3. Click the "+" icon at the beginning of the row to expand the call details. Verify the call details are correct.

	1102 4E 99 169/CVM/coards/mickeesesh and				44		Dina Saarah		Q
S S + ttp://192.45.88.168/CXM/search/quicksearch.aspx					💌 🖄 😽 🗶 🜆 Live Search				
File Edit View Favo	orites Tools Help								
🍃 Favorites 🛛 🚔 🏉	Suggested Sites 🔹 😰 Web Slice Gallery 🔹								
<i>€</i> CXM						- 🚯	S - 🖃 🖶 -	Page - S	afety 🔹 Tools 👻 🔞 🕶
	Search Coaching Repor	ts PAdmin PSystem	Survey PHelp	My Login		12.00			
	n 60 60 .							s	earch -> Quick Searc
earch	From Date: 8/20/2009	Stations:		B		Caller/Call	ed ID:		
uick	To Date: 8/20/2009	Agents:		2		Page Size:	25 💌		Search
lvanced all Buckets	All None Add to Bucket (empty	) 🗸 🗟							
anage Buckets splay Options	Start Tir		Grades VDNS	Call Duration	n Call Directio	n Stations		Dialed	Account C
		09 8:16:32 AM	0	00:00:11	Outbound	30003	1000	30007	Account
	8/20/2009 8:16:32 AM -	Station 30003 orig							
	8/20/2009 8:16:32 AM -	Station 30003 call							
	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.							
	🔳 📄 🔍 🔓 🖾 🖾 8/20/20	D9 8:16:32 AM	Q	00:00:11	Outbound	30007		30007	
	1 9 ir in i > 8/20/20	09 8:03:32 AM	<u>0</u>	00:00:19	Inbound	32019	T4351#1	38005	
		09 8:03:32 AM	Q	00:00:19	Inbound	32022	T4350#1	38005	
	🛨 🗖 💁 🕼 🖾 🖾 8/20/20	09 8:03:31 AM	<u>0</u>	00:00:20	Inbound	32013	T4348#1	38005	
	I ○ ○ If Im I⇒ 8/20/20	D9 8:03:31 AM	<u>0</u>	00:00:20	Inbound	32021	T4349#1	38005	
	🛨 🗖 🌖 👔 🖾 🖙 8/20/20	09 8:03:27 AM	<u>0</u>	00:00:24	Inbound	32002	T4331#1	38005	
	🔳 🗖 🎭 🔓 🕼 🛱 8/20/20	09 8:03:27 AM	<u>0</u>	00:00:23	Inbound	32012	T4330#1	38005	-
	🛨 🗖 🍫 🚺 🖾 🖙 8/20/20	09 8:03:26 AM	2	00:00:24	Inbound	32008	T4329#1	38005	
aching	🖪 🖸 🔍 🔓 🕼 🛱 8/20/20	D9 8:03:00 AM	٥	00:00:30	Inbound	32022	T4327#1	38005	
ports	± □ • ir is i⇒ 8/20/20	D9 8:03:00 AM	<u>0</u>	00:00:30	Inbound	32019	T4328#1	38005	
min	I □ 9 If I ⇒ 8/20/20	D9 8:02:59 AM	<u>0</u>	00:00:30	Inbound	32013	T4325#1	38005	
stem		09 8:02:59 AM	<u>0</u>	00:00:31	Inbound	32021	T4326#1	38005	
		09 8:02:58 AM	<u>0</u>	00:00:31	Inbound	32016	T4323#1	38005	
rvey		09 8:02:58 AM	<u>0</u>	00:00:31	Inbound	32014	T4324#1	38005	
lp	<								
Login	Events: 10789		Page	1 Y of 432					4 ●

### 9. Conclusion

These Application Notes describe the configuration steps required for Co-nexus CXM 4.5 to interoperate with Avaya Aura<sup>TM</sup> Communication Manager and Avaya Aura<sup>TM</sup> 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 <u>http://support.avaya.com</u>:

[1] Administering Avaya Aura<sup>™</sup> 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 <u>http://www.4cxm.com/cont.asp</u>.

#### ©2009 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by  $\mathbb{R}$  and <sup>TM</sup> 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 <u>devconnect@avaya.com</u>.