



Avaya Solution & Interoperability Test Lab

Application Notes for Cogito Enterprise Platform with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for Cogito Enterprise Platform to interoperate with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services. Cogito Enterprise Platform is a call recording and analysis solution.

In the compliance testing, Cogito Enterprise Platform used the Device, Media, and Call Control interface from Avaya Aura® Application Enablement Services to monitor contact center devices on Avaya Aura® Communication Manager, and to capture the media associated with the monitored agents for call recording and analysis using the Single Step Conference method.

Readers should pay attention to **Section 2**, in particular the scope of testing as outlined in **Section 2.1** as well as any observations noted in **Section 2.2**, to ensure that their own use cases are adequately covered by this scope and results.

Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

1. Introduction

These Application Notes describe the configuration steps required for Cogito Enterprise Platform to interoperate with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services. Cogito Enterprise Platform is a call recording and analysis solution.

In the compliance testing, Cogito Enterprise Platform used the Device, Media, and Call Control (DMCC) Java interface from Avaya Aura® Application Enablement Services to monitor agent stations on Avaya Aura® Communication Manager, to register virtual IP softphones, and to capture media associated with the monitored agents for call recording and analysis using the Single Step Conference method.

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

2. General Test Approach and Test Results

The feature test cases were performed both automatically and manually. Upon start of the Enterprise Platform application, the application automatically requests monitoring on agent stations, and registers the virtual IP softphones using DMCC.

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

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

The verification of tests included use of Enterprise Platform logs for proper message exchanges, and use of the Cogito Dialog client application for proper analysis and logging and playback of calls.

DevConnect Compliance Testing is conducted jointly by Avaya and DevConnect members. The jointly-defined test plan focuses on exercising APIs and/or standards-based interfaces pertinent to the interoperability of the tested products and their functionalities. DevConnect Compliance Testing is not intended to substitute full product performance or feature testing performed by DevConnect members, nor is it to be construed as an endorsement by Avaya of the suitability or completeness of a DevConnect member's solution.

2.1. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability testing.

The feature testing focused on verifying the following on Enterprise Platform:

- Use of DMCC registration services to register and un-register the virtual IP softphones.
- Use of DMCC monitoring services to monitor agent stations and existing calls.
- Use of DMCC call control services to activate Single Step Conference and Third Party Selective Listening Hold, and to obtain the media for call recording.
- Proper recording, logging, and playback of calls for scenarios involving inbound, outbound, internal, external, ACD, non-ACD, hold, resume, multiple calls, multiple agents, conference, and transfer.
- Sanity test of call analysis with proper reflection of speaking parties in the signal charts and wave line.

The serviceability testing focused on verifying the ability of Enterprise Platform to recover from adverse conditions, such as disconnecting/reconnecting the Ethernet connection to the Telephone Audio Server component of Enterprise Platform.

2.2. Test Results

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

- Current design of Enterprise Platform is to only record conversation between two parties when none of the internal party on the call has any other active call. As such, private conversation between internal parties as part of the attended transfer and conference scenarios, and joint conversation among more than two parties as part of the conference scenarios were not recorded by design.
- The Telephone Audio Server used in the compliance testing included a customization to use generic port 80 for communication with the Common Services Component. The actual connectivity port may differ in the customer environment.

2.3. Support

Technical support on Enterprise Platform can be obtained through the following:

- **Phone:** (617) 580-3101
- **Email:** avayasupport@cogitocorp.com

3. Reference Configuration

Enterprise Platform consists of the Telephone Audio Server, the Common Services Component, and the Cogito Dialog client application. In the compliance testing configuration shown in **Figure 1**, the Telephone Audio Server was located in the same network as Application Enablement Services, the Common Services Component was located on the WAN, and the Cogito Dialog application was running on the local supervisor and agent desktops.

The detailed administration of basic connectivity between Communication Manager and Application Enablement Services, and of contact center devices are not the focus of these Application Notes and will not be described. In the compliance testing, Enterprise Platform monitored the agent stations shown in the table below.

Device Type	Extension
VDN	60001, 60002
Skill Group	65081, 65082
Supervisor	65000
Agent Station	65001, 66002
Agent ID	65881, 65882

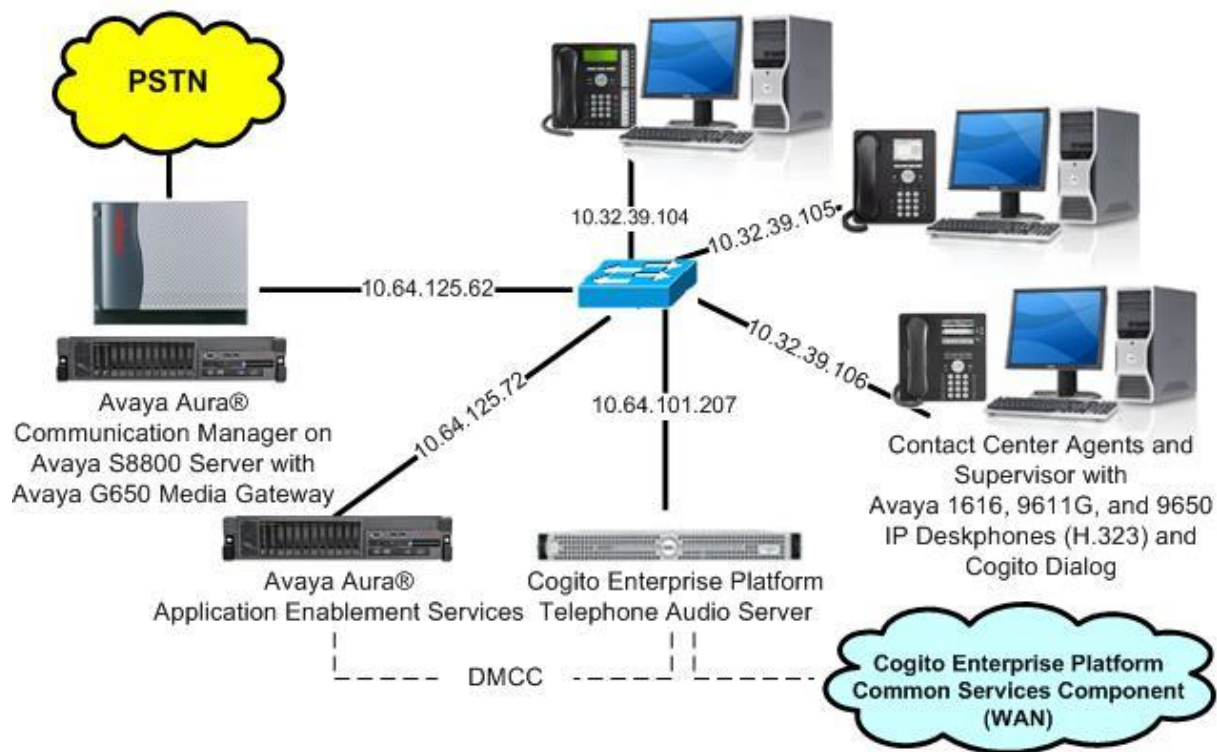


Figure 1: Compliance Testing Configuration

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya Aura® Communication Manager on Avaya S8800 Server with Avaya G650 Media Gateway	6.3.6 (R016x.03.0.124.0-21591)
Avaya Aura® Application Enablement Services	6.3.3 SP1 (6.3.3.1.10-0)
Avaya Aura® Session Manager	6.3.8
Avaya Aura® System Manager	6.3.8
Avaya 1616 IP Deskphone (H.323)	1.350B
Avaya 9611G IP Deskphone (H.323)	6.4014
Avaya 9650 IP Deskphone (H.323)	3.230A
Cogito Enterprise Platform on CentOS <ul style="list-style-type: none">Telephone Audio ServerAvaya DMCC Java (api.jar)	1.5.0 6.6 1.5.0 6.1.0.501
Cogito Enterprise Platform on CentOS <ul style="list-style-type: none">Common Services Component	1.5.0 6.6 1.5.0
Cogito Dialog	2.1.0

5. Configure Avaya Aura® Communication Manager

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

- Verify license
- Administer CTI link
- Administer IP codec set
- Administer virtual IP softphones

5.1. Verify License

Log in to the System Access Terminal to verify that the Communication Manager license has proper permissions for features illustrated in these Application Notes. Use the “display system-parameters customer-options” command. On **Page 1**, verify that there is sufficient remaining capacity for the virtual IP softphones by comparing the **Maximum Stations** field value with the corresponding value in the **USED** column. Note that two virtual IP softphones are needed for every monitored agent station.

The license file installed on the system controls the maximum permitted. If there is insufficient capacity, contact an authorized Avaya sales representative to make the appropriate changes.

```
display system-parameters customer-options                               Page 1 of 11
                                OPTIONAL FEATURES

G3 Version: V16                                     Software Package: Enterprise
Location: 2                                           System ID (SID): 1
Platform: 28                                         Module ID (MID): 1

                                USED
Platform Maximum Ports: 65000 163
Maximum Stations: 41000 21
Maximum XMOBILE Stations: 41000 0
Maximum Off-PBX Telephones - EC500: 41000 0
Maximum Off-PBX Telephones - OPS: 41000 3
Maximum Off-PBX Telephones - PBFMC: 41000 0
Maximum Off-PBX Telephones - PVFMC: 41000 0
Maximum Off-PBX Telephones - SCCAN: 0 0
Maximum Survivable Processors: 313 0
```

Navigate to **Page 3**, and verify that the **Computer Telephony Adjunct Links** customer option is set to “y”.

display system-parameters customer-options		Page 3 of 11
OPTIONAL FEATURES		
Abbreviated Dialing Enhanced List? y	Audible Message Waiting? y	
Access Security Gateway (ASG)? n	Authorization Codes? y	
Analog Trunk Incoming Call ID? y	CAS Branch? n	
A/D Grp/Sys List Dialing Start at 01? y	CAS Main? n	
Answer Supervision by Call Classifier? y	Change COR by FAC? n	
ARS? y	Computer Telephony Adjunct Links? y	
ARS/AAR Partitioning? y	Cvg Of Calls Redirected Off-net? y	
ARS/AAR Dialing without FAC? n	DCS (Basic)? y	
ASAI Link Core Capabilities? n	DCS Call Coverage? y	
ASAI Link Plus Capabilities? n	DCS with Rerouting? y	
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	

5.2. Administer CTI Link

Add a CTI link using the “add cti-link n” command, where “n” is an available CTI link number. Enter an available extension number in the **Extension** field. Note that the CTI link number and extension number may vary. Enter “ADJ-IP” in the **Type** field, and a descriptive name in the **Name** field. Default values may be used in the remaining fields.

add cti-link 2		Page 1 of 3
CTI LINK		
CTI Link: 1		
Extension: 60100		
Type: ADJ-IP		
COR: 1		
Name: AES CTI Link		

5.3. Administer IP Codec Set

Use the “change ip-codec-set n” command, where “n” is an existing codec set number used for integration with Enterprise Platform. Update the audio codec types in the **Audio Codec** fields as necessary to include a G.711 variant, which is the only codec variant supported by Enterprise Platform for the virtual IP softphones. In the compliance testing, this IP codec set was used by the agent stations and virtual IP softphones.

change ip-codec-set 1		Page 1 of 2
IP Codec Set		
Codec Set: 1		
Audio Codec	Silence Suppression	Frames Per Pkt
1: G.711MU	n	2
2: G.729	n	2
3:		

5.4. Administer Virtual IP Softphones

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

- **Extension:** The available extension number.
- **Type:** A desired IP type, such as “1608”.
- **Name:** A descriptive name.
- **Security Code:** A desired code.
- **IP SoftPhone:** “y”

```
add station 65991
```

Page 1 of 5

STATION		
Extension: 65991	Lock Messages? n	BCC: 0
Type: 1608	Security Code: 12345	TN: 1
Port: IP	Coverage Path 1:	COR: 1
Name: Cogito Virtual #1	Coverage Path 2:	COS: 1
	Hunt-to Station:	Tests: y

STATION OPTIONS

Loss Group: 19	Time of Day Lock Table:
	Personalized Ringing Pattern: 1
Speakerphone: 2-way	Message Lamp Ext: 65991
Display Language: english	Mute Button Enabled? y
Survivable GK Node Name:	Expansion Module? n
Survivable COR: internal	Media Complex Ext:
Survivable Trunk Dest? y	IP SoftPhone? y
	IP Video Softphone? n
	Short/Prefixed Registration Allowed: default

Repeat this section to administer two virtual IP softphones for every monitored agent station. In the compliance testing, four virtual IP softphones shown below were administered, for simultaneous recording of two monitored agents.

```
list station 65991 count 2
```

STATIONS									
Ext/ Hunt-to	Port/ Type	Name/ Surv GK NN	Move	Room/ Data Ext	Cv1/ Cv2	COR/ COS	Cable/ TN	Jack	
65991	S00072	Cogito Virtual #1				1			
	1608		no			1	1		
65992	S00075	Cogito Virtual #2				1			
	1608		no			1	1		
65993	S00078	Cogito Virtual #3				1			
	1608		no			1	1		
65994	S00081	Cogito Virtual #4				1			
	1608		no			1	1		

6. Configure Avaya Aura® Application Enablement Services

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

- Launch OAM interface
- Verify license
- Administer TSAPI link
- Administer H.323 gatekeeper
- Disable security database
- Restart services
- Obtain Tlink name
- Administer Cogito user
- Enable ports

6.1. Launch OAM Interface

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

The **Please login here** screen is displayed. Log in using the appropriate credentials.



The screenshot shows the Avaya Application Enablement Services Management Console login interface. At the top left is the Avaya logo. To its right, the text "Application Enablement Services" and "Management Console" is displayed. A red horizontal bar spans the width of the page, with a "Help" link on the right. In the center, there is a login box with the text "Please login here:" followed by a "Username" label and a text input field. Below the input field is a "Continue" button. At the bottom of the page, a red horizontal bar is present, and below it, the copyright notice "Copyright © 2009-2014 Avaya Inc. All Rights Reserved." is displayed.

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

The screenshot displays the Avaya Application Enablement Services Management Console. The top header includes the Avaya logo, the title "Application Enablement Services Management Console", and a welcome message for the user. The left sidebar contains a navigation menu with options: AE Services, Communication Manager Interface, High Availability, Licensing, Maintenance, Networking, Security, Status, User Management, Utilities, and Help. The main content area shows the "Welcome to OAM" screen, which provides an overview of the OAM web and lists the administrative domains it manages: AE Services, Communication Manager Interface, High Availability, Licensing, Maintenance, Networking, Security, Status, User Management, Utilities, and Help. A note at the bottom states that these domains can be served by one administrator for all domains or a separate administrator for each domain.

AVAYA Application Enablement Services Management Console

Welcome: User
Last login: Wed Nov 5 07:15:23 2014 from 10.32.39.20
Number of prior failed login attempts: 0
HostName/IP: aes_125_72/10.64.125.72
Server Offer Type: VIRTUAL_APPLIANCE_ON_SP
SW Version: 6.3.3.1.10-0
Server Date and Time: Wed Nov 05 07:15:48 MST 2014
HA Status: Not Configured

Home | Help | Logout

Home

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

Welcome to OAM

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

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

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

6.2. Verify License

Select **Licensing** → **WebLM Server Access** in the left pane, to display the **Web License Manager** pop-up screen (not shown), and log in using the appropriate credentials.

The screenshot displays the Avaya Application Enablement Services Management Console with the "Licensing" section selected in the left sidebar. The main content area shows the "Licensing" screen, which provides instructions on how to set up and maintain the WebLM, import, set up, and maintain the license, and administer TSAPI Reserved Licenses or DMCC Reserved Licenses. The left sidebar shows the navigation menu with options: AE Services, Communication Manager Interface, Licensing, Maintenance, Networking, Security, and Status. The "Licensing" section is expanded, showing sub-options: WebLM Server Address, WebLM Server Access, and Reserved Licenses.

AVAYA Application Enablement Services Management Console

Welcome: User
Last login: Wed Nov 5 07:15:23 2014 from 10.32.39.20
Number of prior failed login attempts: 0
HostName/IP: aes_125_72/10.64.125.72
Server Offer Type: VIRTUAL_APPLIANCE_ON_SP
SW Version: 6.3.3.1.10-0
Server Date and Time: Wed Nov 05 07:15:48 MST 2014
HA Status: Not Configured

Home | Help | Logout

Licensing

AE Services
Communication Manager Interface
Licensing
Maintenance
Networking
Security

Licensing

If you are setting up and maintaining the WebLM, you need to use the following:

- WebLM Server Address

If you are importing, setting up and maintaining the license, you need to use the following:

- WebLM Server Access

If you want to administer TSAPI Reserved Licenses or DMCC Reserved Licenses, you need to use the following:

- Reserved Licenses

The **Web License Manager** screen below is displayed. Select **Licensed products** → **APPL_ENAB** → **Application_Enablement** in the left pane, to display the **Application Enablement (CTI)** screen in the right pane.

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

Also verify that there is an applicable advanced switch license, in this case **AES ADVANCED LARGE SWITCH** for the Avaya S8800 Server.

Web License Manager (WebLM v6.3)

[Help](#) | [About](#) | [Change Password](#)

WebLM Home

Install license

Licensed products

APPL_ENAB

▼ Application_Enablement

View license capacity

View peak usage

Uninstall license

Server properties

Manage users

Shortcuts

Help for Installed Product

Application Enablement (CTI) - Release: 6 - SID: 10503000
Standard License file

You are here: Licensed Products > Application_Enablement > View License Capacity
License installed on: May 11, 2012 7:07:47 PM -04:00

License File Host IDs: 00-16-3E-48-ED-82

Licensed Features

10 Items Show ALL

Feature (License Keyword)	Expiration date	Licensed capacity
CVLAN ASAI VALUE_AES_CVLAN_ASAI	permanent	16
Unified CC API Desktop Edition VALUE_AES_AEC_UNIFIED_CC_DESKTOP	permanent	10000
AES ADVANCED SMALL SWITCH VALUE_AES_AEC_SMALL_ADVANCED	permanent	16
CVLAN Proprietary Links VALUE_AES_PROPRIETARY_LINKS	permanent	16
Product Notes VALUE_NOTES	permanent	SmallServerTypes: s8300c;s8300d;icc;premio;tn8400;laptop;CtiS MediumServerTypes: ibmx306;ibmx306m;del1950;xen;hs20;hs20_ LargeServerTypes: isp2100;ibmx305;dl380g3;dl385g1;dl385g2;u TrustedApplications: IPS_001, BasicUnrestrict DMCUnrestricted; 1XP_001, BasicUnrestricted DMCUnrestricted; 1XM_001, BasicUnrestricted DMCUnrestricted; PC_001, BasicUnrestricted, DMCUnrestricted; CIE_001, BasicUnrestricted DMCUnrestricted; OSPC_001, BasicUnrestrict DMCUnrestricted; VP_001, BasicUnrestricted, DMCUnrestricted; SAMETIME_001, VALUE_AES_UNIFIED_CC_DESKTOP,,, CCE_ AdvancedUnrestricted, DMCUnrestricted; CSI AdvancedUnrestricted, DMCUnrestricted; CSI AdvancedUnrestricted, DMCUnrestricted; AVA BasicUnrestricted, AdvancedUnrestricted, DMC CCT_ELITE_CALL_CTRL_001, BasicUnrestrict DMCUnrestricted, AgentEvents;
AES ADVANCED LARGE SWITCH VALUE_AES_AEC_LARGE_ADVANCED	permanent	16
TSAPI Simultaneous Users VALUE_AES_TSAPI_USERS	permanent	10000
DLG VALUE_AES_DLG	permanent	16
Device Media and Call Control VALUE_AES_DMCC_DMC	permanent	10000
AES ADVANCED MEDIUM SWITCH VALUE_AES_AEC_MEDIUM_ADVANCED	permanent	16

6.3. Administer TSAPI Link

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

The screenshot shows the Avaya Application Enablement Services Management Console. The top header includes the Avaya logo, the title "Application Enablement Services Management Console", and a welcome message for the user. The left navigation pane shows "AE Services" expanded, with "TSAPI" selected, and "TSAPI Links" highlighted. The main content area displays the "TSAPI Links" screen, which includes a table with columns: Link, Switch Connection, Switch CTI Link #, ASAI Link Version, and Security. Below the table are buttons for "Add Link", "Edit Link", and "Delete Link".

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

The **Link** field is only local to the Application Enablement Services server, and may be set to any available number. For **Switch Connection**, select the relevant switch connection from the drop-down list. In this case, the existing switch connection "S8800" is selected. For **Switch CTI Link Number**, select the CTI link number from **Section 5.2**. Retain the default values in the remaining fields.

The screenshot shows the "Add TSAPI Links" screen in the Avaya Application Enablement Services Management Console. The left navigation pane is the same as the previous screenshot. The main content area displays the "Add TSAPI Links" form, which includes fields for Link, Switch Connection, Switch CTI Link Number, ASAI Link Version, and Security. The values entered are: Link: 1, Switch Connection: S8800, Switch CTI Link Number: 2, ASAI Link Version: 6, and Security: Unencrypted. Below the form are buttons for "Apply Changes" and "Cancel Changes".

6.4. Administer H.323 Gatekeeper

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

Locate the connection name associated with the relevant Communication Manager, in this case “S8800”, and select the corresponding radio button. Click **Edit H.323 Gatekeeper**.

The screenshot shows the Avaya Application Enablement Services Management Console. The left navigation pane is expanded to 'Communication Manager Interface' and 'Switch Connections'. The main content area displays a table of switch connections. The table has four columns: Connection Name, Processor Ethernet, Msg Period, and Number of Active Connections. A single connection named 'S8800' is listed with 'No' for Processor Ethernet, '30' for Msg Period, and '1' for Number of Active Connections. Below the table are buttons for 'Edit Connection', 'Edit PE/CLAN IPs', 'Edit H.323 Gatekeeper', 'Delete Connection', and 'Survivability Hierarchy'. The top right corner shows user information and system status.

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections
S8800	No	30	1

The **Edit H.323 Gatekeeper** screen is displayed. Enter the IP address of a C-LAN circuit pack or the Processor C-LAN on Communication Manager to use as the H.323 gatekeeper, in this case “10.64.125.32” as shown below. Click **Add Name or IP**.

The screenshot shows the 'Edit H.323 Gatekeeper - S8800' screen. The left navigation pane is the same as the previous screenshot. The main content area has a text input field containing '10.64.125.32' and an 'Add Name or IP' button. Below the input field are buttons for 'Delete IP' and 'Back'. The top right corner shows user information and system status.

6.5. Disable Security Database

Select **Security** → **Security Database** → **Control** from the left pane, to display the **SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services** screen in the right pane. Uncheck both fields below.

The screenshot displays the Avaya Application Enablement Services Management Console. The top header includes the Avaya logo, the title "Application Enablement Services Management Console", and a welcome message for the user. The main navigation pane on the left lists various services, with "Security" expanded to show "Security Database" and "Control" selected. The right pane shows the "SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services" configuration page, which contains two unchecked checkboxes: "Enable SDB for DMCC Service" and "Enable SDB for TSAPI Service, JTAPI and Telephony Web Services". An "Apply Changes" button is located below the checkboxes.

Welcome: User
Last login: Wed Nov 5 07:15:23 2014 from 10.32.39.20
Number of prior failed login attempts: 0
HostName/IP: aes_125_72/10.64.125.72
Server Offer Type: VIRTUAL_APPLIANCE_ON_SP
SW Version: 6.3.3.1.10-0
Server Date and Time: Wed Nov 05 07:15:48 MST 2014
HA Status: Not Configured

Security | Security Database | Control

Home | Help | Logout

AE Services
Communication Manager Interface
High Availability
Licensing
Maintenance
Networking
Security
Account Management
Audit
Certificate Management
Enterprise Directory
Host AA
PAM
Security Database
Control

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

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

Apply Changes

6.6. Restart Services

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



Application Enablement Services
Management Console

Welcome: User
Last login: Wed Nov 5 07:15:23 2014 from 10.32.39.20
Number of prior failed login attempts: 0
HostName/IP: aes_125_72/10.64.125.72
Server Offer Type: VIRTUAL_APPLIANCE_ON_SP
SW Version: 6.3.3.1.10-0
Server Date and Time: Wed Nov 05 07:15:48 MST 2014
HA Status: Not Configured

Maintenance | Service Controller

Home | Help | Logout

▶ AE Services

▶ Communication Manager Interface

▶ High Availability

▶ Licensing

▼ Maintenance

▶ Date Time/NTP Server

▶ Security Database

▶ Service Controller

▶ Server Data

▶ Networking

▶ Security

▶ Status

▶ User Management

Service Controller

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

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

Start

Stop

Restart Service

Restart AE Server

Restart Linux

Restart Web Server

6.7. Obtain Tlink Name

Select **Security** → **Security Database** → **Tlinks** from the left pane. The **Tlinks** screen shows a listing of the Tlink names. A new Tlink name is automatically generated for the TSAPI service. Locate the Tlink name associated with the relevant switch connection, which would use the name of the switch connection as part of the Tlink name. Make a note of the associated Tlink name, to be used later for configuring Enterprise Platform.

In this case, the associated Tlink name is “AVAYA#S8800#CSTA#AES_125_72”. Note the use of the switch connection “S8800” from **Section 6.3** as part of the Tlink name.

The screenshot displays the Avaya Application Enablement Services Management Console. The top header includes the Avaya logo, the title "Application Enablement Services Management Console", and a welcome message for the user. The main navigation pane on the left lists various services, with "Security" expanded to show "Security Database" and "Tlinks" selected. The main content area shows a single Tlink entry with the name "AVAYA#S8800#CSTA#AES_125_72" and a "Delete Tlink" button.

AVAYA Application Enablement Services Management Console

Welcome: User
Last login: Wed Nov 5 07:15:23 2014 from 10.32.39.20
Number of prior failed login attempts: 0
HostName/IP: aes_125_72/10.64.125.72
Server Offer Type: VIRTUAL_APPLIANCE_ON_SP
SW Version: 6.3.3.1.10-0
Server Date and Time: Wed Nov 05 07:15:48 MST 2014
HA Status: Not Configured

Security | Security Database | Tlinks Home | Help | Logout

Tlinks

Tlink Name
AVAYA#S8800#CSTA#AES_125_72
Delete Tlink

6.8. Administer Cogito User

Select **User Management** → **User Admin** → **Add User** from the left pane, to display the **Add User** screen in the right pane.

Enter desired values for **User Id**, **Common Name**, **Surname**, **User Password**, and **Confirm Password**. For **CT User**, select “Yes” from the drop-down list. Retain the default value in the remaining fields.

AVAYA **Application Enablement Services**
Management Console

Welcome: User
Last login: Wed Nov 5 07:15:23 2014 from 10.32.39.20
Number of prior failed login attempts: 0
HostName/IP: aes_125_72/10.64.125.72
Server Offer Type: VIRTUAL_APPLIANCE_ON_SP
SW Version: 6.3.3.1.10-0
Server Date and Time: Wed Nov 05 07:15:48 MST 2014
HA Status: Not Configured

User Management | User Admin | Add UserHome | Help | Logout

▶ AE Services

▶ Communication Manager Interface

▶ High Availability

▶ Licensing

▶ Maintenance

▶ Networking

▶ Security

▶ Status

▼ User Management

▶ Service Admin

▼ User Admin

■ Add User

■ Change User Password

■ List All Users

■ Modify Default Users

■ Search Users

▶ Utilities

▶ Help

Add User

Fields marked with * can not be empty.

* User Idcogito

* Common Namecogito

* Surnamecogito

* User Password*****

* Confirm Password*****

Admin Note

Avaya RoleNone ▼

Business Category

Car License

CM Home

Css Home

CT UserYes ▼

Department Number

Display Name

Employee Number

Employee Type

Enterprise Handle

Given Name

6.9. Enable Ports

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

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

AVAYA

Application Enablement Services
Management Console

Welcome: User
Last login: Wed Nov 5 07:15:23 2014 from 10.32.39.20
Number of prior failed login attempts: 0
HostName/IP: aes_125_72/10.64.125.72
Server Offer Type: VIRTUAL_APPLIANCE_ON_SP
SW Version: 6.3.3.1.10-0
Server Date and Time: Wed Nov 05 07:15:48 MST 2014
HA Status: Not Configured

Networking | Ports

Home | Help | Logout

▶ AE Services

▶ Communication Manager Interface

▶ High Availability

▶ Licensing

▶ Maintenance

▼ Networking

AE Service IP (Local IP)

Network Configure

Ports

TCP Settings

▶ Security

▶ Status

▶ User Management

▶ Utilities

▶ Help

Ports

CVLAN Ports

Unencrypted TCP Port9999

Enabled Disabled

Encrypted TCP Port9998

DLG Port

TCP Port5678

TSAPI Ports

TSAPI Service Port450

Local TLINK Ports

TCP Port Min1024

TCP Port Max1039

Unencrypted TLINK Ports

TCP Port Min1050

TCP Port Max1065

Encrypted TLINK Ports

TCP Port Min1066

TCP Port Max1081

DMCC Server Ports

Unencrypted Port4721

Enabled Disabled

Encrypted Port4722

TR/87 Port4723

7. Configure Cogito Enterprise Platform

The configuration of Enterprise Platform is performed by Cogito engineers, and is not described in these Application Notes. Any administration issues or questions should be addressed to Cogito Support in **Section 2.3**.

Prior to configuration of Enterprise Platform, customers need to provide Cogito with the following information:

- Agent station extensions from **Section 3**
- Agent login IDs from **Section 3**
- Virtual IP softphone extensions and security codes from **Section 5.4**
- IP address of the H.323 Gatekeeper from **Section 6.4**
- IP address of Application Enablement Services
- Switch connection name from **Section 6.3**
- The Cogito user credential from **Section 6.8**

8. Verification Steps

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

8.1. Verify Avaya Aura® Communication Manager

On Communication Manager, verify the status of the administered CTI link by using the “status aesvcs cti-link” command. Verify that the **Service State** is “established” for the CTI link number administered in **Section 5.2**, as shown below.

```
status aesvcs cti-link
```

AE SERVICES CTI LINK STATUS						
CTI Link	Version	Mnt Busy	AE Services Server	Service State	Msgs Sent	Msgs Rcvd
2	6	no	aes_125_72	established	326	317

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


```
list registered-ip-stations
```

REGISTERED IP STATIONS						
Station Ext or Orig Port	Set Type/ Net Rgn	Prod ID/ Release	TCP Skt	Station IP Address/ Gatekeeper	IP Address	
65000	9650	IP_Phone	y	10.32.39.106		
	1	3.230A		10.64.125.62		
65001	1616	IP_Phone	y	10.32.39.104		
	1	1.350B		10.64.125.62		
65002	9611	IP_Phone	y	10.32.39.105		
	1	6.4014		10.64.125.62		
65991	1608	IP_API_A	y	10.64.125.72		
	1	3.2040		10.64.125.32		
65992	1608	IP_API_A	y	10.64.125.72		
	1	3.2040		10.64.125.32		
65993	1608	IP_API_A	y	10.64.125.72		
	1	3.2040		10.64.125.32		
65994	1608	IP_API_A	y	10.64.125.72		
	1	3.2040		10.64.125.32		

8.2. Verify Avaya Aura® Application Enablement Services

On Application Enablement Services, verify the status of the TSAPI link by selecting **Status** → **Status and Control** → **TSAPI Service Summary** from the left pane. The **TSAPI Link Details** screen is displayed.

Without any active calls at the agents, verify the **Status** is “Talking” for the TSAPI link administered in **Section 6.3**, and that the **Associations** column reflects the number of agent stations from **Section 3**.



Application Enablement Services

Management Console

Welcome: User
Last login: Wed Nov 5 13:32:05 2014 from 10.32.39.20
Number of prior failed login attempts: 0
HostName/IP: aes_125_72/10.64.125.72
Server Offer Type: VIRTUAL_APPLIANCE_ON_SP
SW Version: 6.3.3.1.10-0
Server Date and Time: Wed Nov 05 13:50:27 MST 2014
HA Status: Not Configured

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

▶ AE Services

▶ Communication Manager Interface

▶ High Availability

▶ Licensing

▶ Maintenance

▶ Networking

▶ Security

▼ Status

Alarm Viewer

Log Manager

▶ Logs

▼ Status and Control

■ CVLAN Service Summary

■ DLG Services Summary

■ DMCC Service Summary

■ Switch Conn Summary

■ TSAPI Service Summary

TSAPI Link Details


☐ Enable page refresh every seconds

	Link	Switch Name	Switch CTI Link ID	Status	Since	State	Switch Version	Associations	Msgs to Switch	Msgs from Switch	Msgs Period
<input checked="" type="radio"/>	1	S8800	2	Talking	Mon Oct 27 11:28:03 2014	Online	16	2	314	325	30
<input type="radio"/>	2	S8300D	1	Switch Down	Mon Oct 27 10:26:02 2014	Online	16	0	0	0	30

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

Verify the status of the DMCC link by selecting **Status → Status and Control → DMCC Service Summary** from the left pane. The **DMCC Service Summary – Session Summary** screen is displayed.

Verify the **User** column shows an active session with the Cogito user name from **Section 6.8**, and that the **# of Associated Devices** column reflects the total number of virtual IP softphones from **Section 5.4**.



Application Enablement Services

Management Console

Welcome: User
 Last login: Thu Nov 6 08:20:27 2014 from 10.32.39.20
 Number of prior failed login attempts: 0
 HostName/IP: aes_125_72/10.64.125.72
 Server Offer Type: VIRTUAL_APPLIANCE_ON_SP
 SW Version: 6.3.3.1.10-0
 Server Date and Time: Thu Nov 06 08:59:04 MST 2014
 HA Status: Not Configured

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

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

DMCC Service Summary - Session Summary

Please do not use back button

☐ Enable page refresh every 60 seconds

Session Summary [Device Summary](#)
 Generated on Thu Nov 06 08:59:04 MST 2014

Service Uptime: 9 days, 23 hours 32 minutes

Number of Active Sessions: 1

Number of Sessions Created Since Service Boot: 42

Number of Existing Devices: 4

Number of Devices Created Since Service Boot: 32

■	Session ID	User	Application	Far-end Identifier	Connection Type	# of Associated Devices
☐	5189C4FC15A54C245 420257092C70EEF-42	cogito	cmapiApplication	10.64.101.207	XML Unencrypted	4

Terminate Sessions
Show Terminated Sessions

Item 1-1 of 1
1 Go

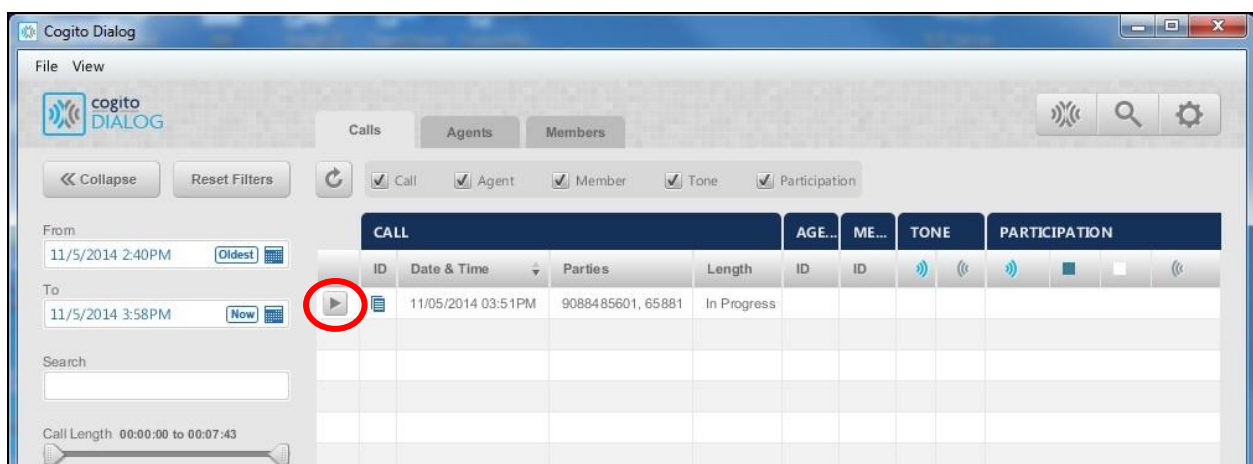
8.3. Verify Cogito Enterprise Platform

Establish an ACD call with an available agent. From the supervisor or the answering agent desktop running the Cogito Dialog application, select **Start → All Program → Cogito Dialog 2.1.0 → Cogito Dialog 2.1.0** to launch the application. The **Cogito Dialog** screen below is displayed. Log in using the appropriate credentials.

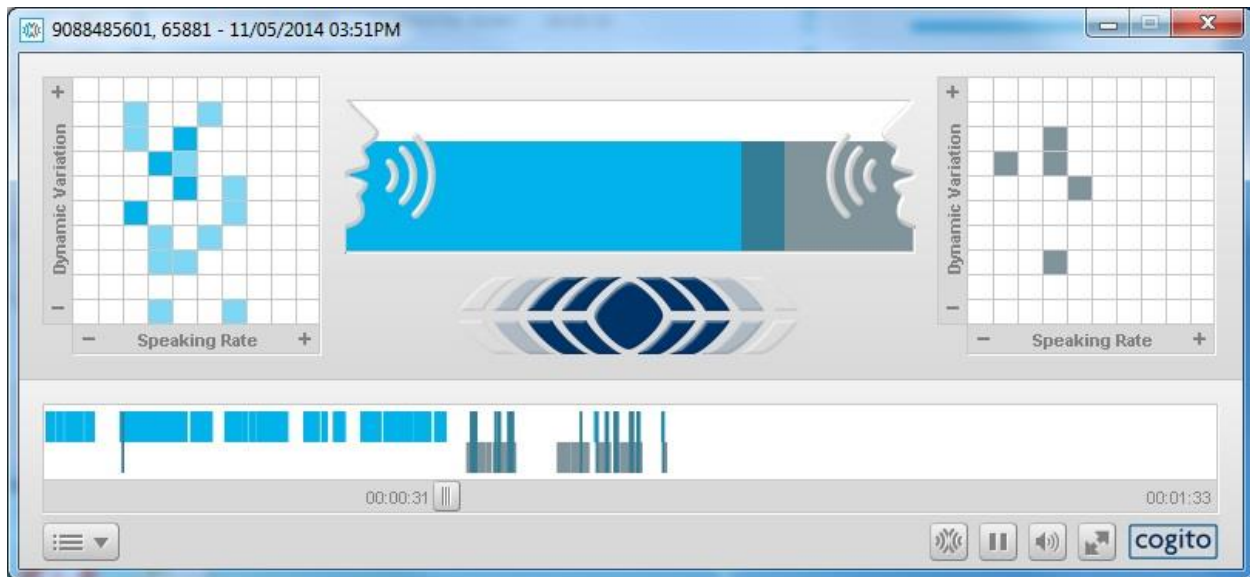


Adjust the time range in the left pane as necessary, and select **View → Show Unidentified Calls** from the top menu. Verify that the right pane is updated to include an entry for the current call, with the appropriate **Parties** information, and “In Progress” in the **Length** column as shown below.

Click on the play icon associated with the entry.



Verify that the screen below is displayed, and that the active recording is being played back. Also verify that as parties speak, the proper signal is populated in the left and/or right charts in the top pane, along with proper wave line representation in the bottom pane, as shown below.



9. Conclusion

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

10. Additional References

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

1. *Administering Avaya Aura® Communication Manager*, Document 03-300509, Issue 10, Release 6.3, June 2014, available at <http://support.avaya.com>.
2. *Avaya Aura® Application Enablement Services Administration and Maintenance Guide*, Release 6.3, 02-300357, June 2014, available at <http://support.avaya.com>.
3. *Integrating Cogito TAS with Avaya CM and AES*, available upon request to Cogito Support.

©2015 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.