



Avaya Solution & Interoperability Test Lab

Application Notes for OAISYS Recording Server with Avaya Aura® Communication Manager 6.2 and Avaya Aura® Application Enablement Services 6.2 Using Station Tap – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for OAISYS Recording Server to interoperate with Avaya Aura® Communication Manager 6.2 and Avaya Aura® Application Enablement Services 6.2 using station tap. OAISYS Recording Server is a call recording solution.

In the compliance testing, OAISYS Recording Server used the Telephony Services Application Programming Interface from Avaya Aura® Application Enablement Services to monitor contact center devices on Avaya Aura® Communication Manager, and the station tap method to capture the media associated with the monitored agents 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 the configuration steps required for OAISYS Recording Server to interoperate with Avaya Aura® Communication Manager 6.2 and Avaya Aura® Application Enablement Services 6.2 using station tap. OAISYS Recording Server is a call recording solution.

In the compliance testing, OAISYS Recording Server used the Telephony Services Application Programming Interface (TSAPI) from Avaya Aura® Application Enablement Services to monitor skill groups and agent stations on Avaya Aura® Communication Manager, and used the station tap method to capture the media associated with the monitored agent stations for call recording.

2. General Test Approach and Test Results

The feature test cases were performed both automatically and manually. Upon start of the Recording Server application, the application automatically obtains a list of configured security devices from Application Enablement Services, and requests monitoring on the skill groups and agent stations.

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

The serviceability test cases were performed manually by disconnecting/reconnecting the Ethernet cable to Recording Server.

The verification of tests included using the Application Enablement Services logs for proper message exchanges, and using the OAISYS Management Studio application for proper logging and playback of calls.

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

2.1. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability testing.

The feature testing focused on verifying the following on Recording Server:

- Handling of TSAPI messages in the areas of event notification and value queries.
- Proper recording, logging, and playback of calls for scenarios involving inbound, outbound, internal, external, ACD, non-ACD, hold, reconnect, simultaneous, conference, and transfer.

The serviceability testing focused on verifying the ability of Recording Server to recover from adverse conditions, such as disconnecting/reconnecting the Ethernet cable to Recording Server

2.2. Test Results

All test cases were executed and verified. The following were observations on Recording Server from the compliance testing.

- Held periods were included in the call recordings, and appeared in grey.
- Each blind transfer and blind conference scenario produced two recording entries, with the second recording entry appeared in grey with a short duration that corresponded to the transfer/conference actions.
- Each attended transfer and conference scenario produced two recording entries, with the second recording entry containing grey for the period corresponding to the transfer/conference actions, followed by the private conversation between the internal parties.
- The majority of the transfer and conference recording entries used the transfer-to and conference-to for Extension, with all party extensions shown in the Detailed View.
- An internal call between two agents generates one call recording, with the called agent used for Extension.
- For a call that stayed up during a link disruption, two call recordings were generated for the call to capture the conversation before and after the disruption.

2.3. Support

Technical support on Recording Server can be obtained through the following:

- **Phone:** (888) 496-9040
- **Web:** http://www.oaisys.com/technical_support.aspx
- **Email:** support@oaisys.com

3. Reference Configuration

As shown in the test configuration below, the Management Studio application was running on the supervisor PC, used for configuration of Recording Server and for verification of proper logging and playback of calls. In the compliance testing, the RTP stream for contact center agents with Avaya IP Deskphones were mirrored from the layer 2 switch, and replicated over to Recording Server.

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 addition, the port mirroring of the layer 2 switch is also outside the scope of these Application Notes and will not be described.

In the compliance testing, Recording Server monitored the skill groups and agent station extensions shown in the table below.

Device Type	Extension
Skill Group	48101, 48102
Agent Station	45001, 45002
Supervisor Station	45000
Agent ID	45881, 45882

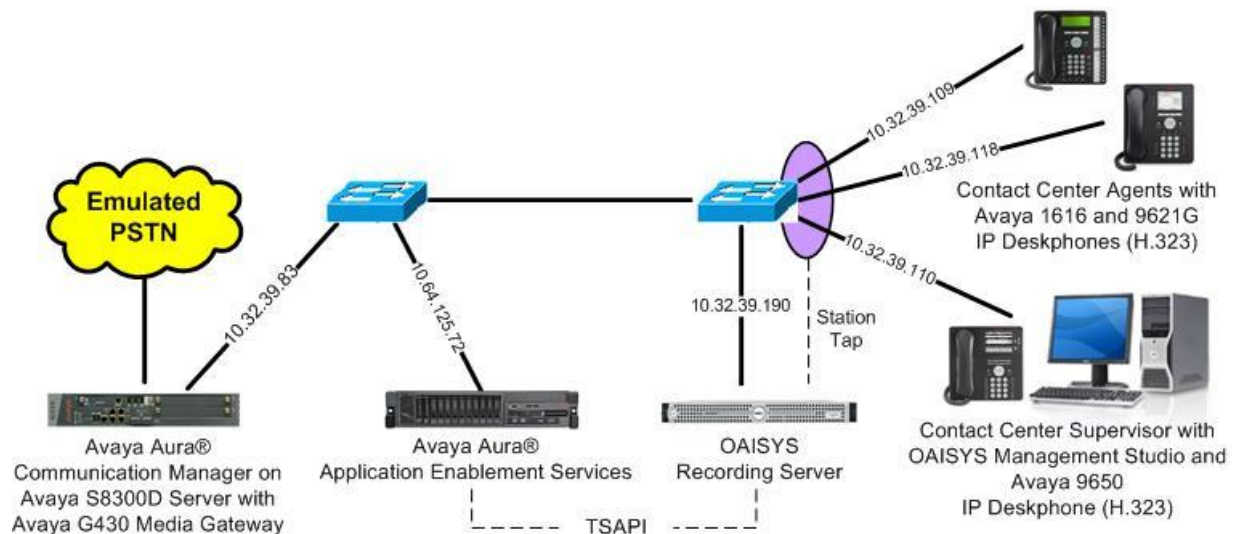


Figure 1: Compliance Testing Configuration

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 S8300D Server with Avaya G430 Media Gateway	6.2 SP3 (R016x.02.0.823.0-20001)
Avaya Aura® Application Enablement Services	6.2 (r6-2-0-18-0)
Avaya 1616 IP Deskphone (H.323)	1.302S
Avaya 9611G IP Deskphone (H.323)	6.2209
Avaya 9650 IP Deskphone (H.323)	3.105S
OAISYS Recording Server on Windows 7 Professional <ul style="list-style-type: none">• Avaya TSAPI Windows Client	7.2.1348 2009 SP1 6.2.0

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

5.1. Verify License

Log in to the System Access Terminal (SAT) to verify that the Communication Manager license has proper permissions for features illustrated in these Application Notes. Use the “display system-parameters customer-options” command to verify that the **Computer Telephony Adjunct Links** customer option is set to “y” on **Page 3**. If this option is not set to “y”, then contact the Avaya sales team or business partner for a proper license file.

display system-parameters customer-options		Page	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?	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			

5.2. Administer CTI Link

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

add cti-link 1		Page	1 of	3
CTI LINK				
CTI Link: 1				
Extension: 40001				
Type: ADJ-IP				
Name: TSAPI Link				
COR: 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 security devices
- Administer security device groups
- Restart TSAPI service
- Obtain Tlink name
- Administer OAISYS user
- Administer security CTI user

6.1. Launch OAM Interface

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

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



The screenshot shows the Avaya Application Enablement Services Management Console login interface. At the top left is the Avaya logo. To its right, the text "Application Enablement Services" is displayed in a large, bold font, with "Management Console" in a smaller font below it. A thick red horizontal bar spans the width of the page. Below this bar, centered, is a light gray rectangular box containing the login form. The form has the heading "Please login here:" followed by two input fields: "Username" and "Password". Below these fields is a blue "Login" button. At the bottom of the page, another thick red horizontal bar is present, with the copyright notice "© Copyright © 2009-2012 Avaya Inc. All Rights Reserved." centered below it.

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

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 sidebar contains a navigation menu with options: AE Services, Communication Manager Interface, Licensing, Maintenance, Networking, Security, Status, User Management, Utilities, and Help. The main content area displays the "Welcome to OAM" message, explaining that the OAM Web provides tools for managing the AE Server across various administrative domains. A list of domains and their functions is provided, including AE Services, Communication Manager Interface, 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: Tue Dec 4 07:27:15 2012 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
SW Version: r6-2-0-18-0
Server Date and Time: Tue Dec 4 07:38:12 MST 2012

Home | Help | Logout

Home

- ▶ AE Services
- ▶ Communication Manager Interface
- ▶ 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.
- 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 with the appropriate credentials.

The screenshot shows the Avaya Application Enablement Services Management Console with the "Licensing" section selected in the left sidebar. The main content area displays the "Licensing" page, 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. A list of options is provided for each step, including WebLM Server Address, WebLM Server Access, and Reserved Licenses.

AVAYA Application Enablement Services Management Console

Welcome: User
Last login: Tue Dec 4 07:27:15 2012 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
SW Version: r6-2-0-18-0
Server Date and Time: Tue Dec 4 07:40:10 MST 2012

Home | Help | Logout

Licensing

- ▶ AE Services
- ▶ Communication Manager Interface
- ▼ Licensing
 - WebLM Server Address
 - WebLM Server Access
 - Reserved Licenses
- ▶ 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 **Licensed Features** in the right pane.

Verify that there are sufficient licenses for **TSAPI Simultaneous Users**, as shown below.



Web License Manager (WebLM v6.2)

Help | About | Change Password | Log off

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 6:07:47 PM -05:00

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

Licensed Features

Feature (Keyword)	Expiration date	Licensed	Acquired
CVLAN ASAI (VALUE_AES_CVLAN_ASAI)	permanent	16	0
Unified CC API Desktop Edition (VALUE_AES_AEC_UNIFIED_CC_DESKTOP)	permanent	10000	0
AES ADVANCED SMALL SWITCH (VALUE_AES_AEC_SMALL_ADVANCED)	permanent	16	0
CVLAN Proprietary Links (VALUE_AES_PROPRIETARY_LINKS)	permanent	16	0
Product Notes (VALUE_NOTES)	permanent	SmallServerTypes: s8300c;s8300d;icc;premio;tn8400;laptop;CtiSmallServer MediumServerTypes: ibmx306;ibmx306m;del11950;xen;hs20;hs20_8832_vm;CtiMediumServer LargeServerTypes: isp2100;ibmx305;dl380g3;dl385g1;dl385g2;unknown;CtiLargeServer TrustedApplications: IPS_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; 1XP_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; 1XM_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; PC_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; CIE_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; OSPC_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; VP_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; SAMETIME_001, VALUE_AES_UNIFIED_CC_DESKTOP,, CCE_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; CSI_T1_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; CSI_T2_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; AVAYAVERINT_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; CCT_ELITE_CALL_CTRL_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted, AgentEvents;	Not counted
AES ADVANCED LARGE SWITCH (VALUE_AES_AEC_LARGE_ADVANCED)	permanent	16	0
TSAPI Simultaneous Users (VALUE_AES_TSAPI_USERS)	permanent	10000	0
DLG (VALUE_AES_DLG)	permanent	16	0
Device Media and Call Control (VALUE_AES_DMCC_DMC)	permanent	10000	0

6.3. Administer TSAPI Link

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

The screenshot shows the Avaya Management Console interface. The top header includes the Avaya logo, "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" table with one link (Link 1, Switch Connection S8800, Switch CTI Link # 2, ASAI Link Version 4, Security Both). Below the table are buttons for "Add Link", "Edit Link", and "Delete Link".

Link	Switch Connection	Switch CTI Link #	ASAI Link Version	Security
1	S8800	2	4	Both

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 "S8300D" is selected. For **Switch CTI Link Number**, select the CTI link number from **Section 5.2**. Retain the default values in the remaining fields, and click **Apply Changes**.

The screenshot shows the "Add TSAPI Links" screen in the Avaya Management Console. The left navigation pane is the same as the previous screenshot. The main content area displays the "Add TSAPI Links" form with the following fields: Link (2), Switch Connection (S8300D), Switch CTI Link Number (1), ASAI Link Version (4), and Security (Unencrypted). Below the form are buttons for "Apply Changes" and "Cancel Changes".

6.4. Administer Security Devices

All devices that are monitored by OAISYS Recording Server needs to be configured in the security database. Select **Security** → **Security Database** → **Devices** from the left pane, to display the **Devices** screen.


Enter the first agent station extension from **Section 3**, and click **Add Device**.

The screenshot shows the Avaya Application Enablement Services Management Console. The left navigation pane has 'Security' expanded, with 'Security Database' and 'Devices' selected. The main area is titled 'Devices' and contains an 'Upload devices from file' section with a 'Browse...' button and an 'Upload' button. Below this is a text input field containing '45001' and an 'Add Device' button. At the bottom, there is a table with columns: Device ID, Tlink Group, Device Type, and Location. Below the table are 'Edit Device' and 'Delete Device(s)' buttons. The top right of the console displays user information: 'Welcome: User', 'Last login: Tue Dec 4 07:27:15 2012 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', 'SW Version: r6-2-0-18-0', and 'Server Date and Time: Tue Dec 4 07:40:10 MST 2012'.

The **Add Device** screen is displayed next. For **Device Type**, select “PHONE”. For **Tlink Group**, select “Any”. Click **Apply Changes**.

The screenshot shows the 'Add Device' screen in the Avaya Application Enablement Services Management Console. The left navigation pane is the same as the previous screenshot. The main area is titled 'Add Device' and contains form fields for 'Device ID' (containing '45001'), 'Location' (empty), 'Device Type' (a dropdown menu with 'PHONE' selected), and 'Tlink Group' (a dropdown menu with 'Any' selected). At the bottom are 'Apply Changes' and 'Cancel Changes' buttons. The top right of the console displays the same user information as the previous screenshot.

Repeat this section to add all monitored station and skill group extensions from **Section 3**, using “PHONE” as **Device Type** for agent station extensions, and “ACD” as **Device Type** for skill group extension, as shown below.



Application Enablement Services

Management Console

Welcome: User
 Last login: Tue Dec 4 07:27:15 2012 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
 SW Version: r6-2-0-18-0
 Server Date and Time: Tue Dec 4 07:40:10 MST 2012

Security | Security Database | Devices
Home | Help | Logout

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

Devices

Upload devices from file

■	Device ID	Tlink Group	Device Type	Location
<input type="checkbox"/>	45001	Any	PHONE	
<input type="checkbox"/>	45002	Any	PHONE	
<input type="checkbox"/>	48101	Any	ACD	
<input type="checkbox"/>	48102	Any	ACD	

6.5. Administer Security Device Groups

Select **Security** → **Security Database** → **Device Groups** from the left pane (not shown below), to display the **Device Groups** screen. Enter a desired device group name, and click **Add Device Group**.



Application Enablement Services

Management Console

Welcome: User
 Last login: Tue Dec 4 07:27:15 2012 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
 SW Version: r6-2-0-18-0
 Server Date and Time: Tue Dec 4 07:40:10 MST 2012

Security | Security Database | Device Groups
Home | Help | Logout

- ▶ AE Services
- ▶ Communication Manager Interface
- ▶ Licensing
- ▶ Maintenance
- ▶ Networking
- ▼ Security
 - ▶ Account Management
 - ▶ Audit

Device Groups

Oaisys Device Group

■	Device Group	Exception Group?
<input type="checkbox"/>		

The **Add Device Group** screen is displayed. Check all configured security devices from **Section 6.4**, and click **Apply Changes**.

Welcome: User
 Last login: Tue Dec 4 07:27:15 2012 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
 SW Version: r6-2-0-18-0
 Server Date and Time: Tue Dec 4 07:40:10 MST 2012

Security | Security Database | Device Groups Home | Help | Logout

▶ AE Services
 ▶ Communication Manager Interface
 ▶ Licensing
 ▶ Maintenance
 ▶ Networking
 ▼ **Security**
 ▶ Account Management
 ▶ Audit
 ▶ Certificate Management
 ▶ Enterprise Directory

Add Device Group

Device Group

Exception Group ☐

Devices

<input checked="" type="checkbox"/>	45001
<input checked="" type="checkbox"/>	45002
<input checked="" type="checkbox"/>	48101
<input checked="" type="checkbox"/>	48102

6.6. Restart TSAPI Service

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

Welcome: User
 Last login: Tue Dec 4 07:27:15 2012 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
 SW Version: r6-2-0-18-0
 Server Date and Time: Tue Dec 4 07:40:10 MST 2012

Maintenance | Service Controller Home | Help | Logout

▶ AE Services
 ▶ Communication Manager Interface
 ▶ Licensing
 ▼ **Maintenance**
 ▶ Date Time/NTP Server
 ▶ Security Database
 Service Controller
 ▶ Server Data
 ▶ Networking
 ▶ Security
 ▶ Status

Service Controller

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

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

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 Recording Server.

In this case, the associated Tlink name is “AVAYA#S8300D#CSTA#AES_125_72”. Note the use of the switch connection “S8300D” 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 bar shows "Security | Security Database | Tlinks" and links for "Home | Help | Logout". The left sidebar contains a tree view with categories like "AE Services", "Communication Manager Interface", "Licensing", "Maintenance", "Networking", and "Security". Under "Security", the "Security Database" is expanded, showing sub-items like "Control", "CTI Users", "Devices", "Device Groups", and "Tlinks". The main content area, titled "Tlinks", lists three Tlink names with radio buttons for selection: "AVAYA#S8300D#CSTA#AES_125_72" (selected), "AVAYA#S8800#CSTA#AES_125_72", and "AVAYA#S8800#CSTA-S#AES_125_72". A "Delete Tlink" button is also present.

Welcome: User
Last login: Tue Dec 4 07:27:15 2012 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
SW Version: r6-2-0-18-0
Server Date and Time: Tue Dec 4 07:40:10 MST 2012

Security | Security Database | Tlinks Home | Help | Logout

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

Tlinks

Tlink Name

☒ AVAYA#S8300D#CSTA#AES_125_72
☐ AVAYA#S8800#CSTA#AES_125_72
☐ AVAYA#S8800#CSTA-S#AES_125_72

Delete Tlink

6.8. Administer OAISYS 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. Click **Apply** at the bottom of the screen (not shown below).

AVAYA **Application Enablement Services**
Management Console

Welcome: User
Last login: Tue Dec 4 07:27:15 2012 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
SW Version: r6-2-0-18-0
Server Date and Time: Tue Dec 4 07:40:10 MST 2012

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

▶ AE Services

▶ Communication Manager Interface

▶ Licensing

▶ Maintenance

▶ Networking

▶ Security

▶ Status

▼ User Management

▶ Service Admin

▼ User Admin

▪ Add User

▪ Change User Password

▪ List All Users

▪ Modify Default Users

▪ Search Users

▶ Utilities

▶ Help

Add User

Fields marked with * can not be empty.

* User Id

oaisys

* Common Name

oaisys

* Surname

oaisys

* User Password

••••••••

* Confirm Password

••••••••

Admin Note

Avaya Role

None

Business Category

Car License

CM Home

Css Home

CT User

Yes

Department Number

Display Name

Employee Number

Employee Type

Enterprise Handle

6.9. Administer Security CTI User

Select **Security** → **Security Database** → **CTI Users** > **List All Users** from the left pane (not shown below), to display the **CTI Users** screen. Select the OAISYS user from **Section 6.8**, and click **Edit**.

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 user "craft" with login details. A red navigation bar contains "Security | Security Database | CTI Users | List All Users" and links for "Home | Help | Logout". On the left, a sidebar menu shows "Security" expanded. The main content area, titled "CTI Users", displays a table with one user, "oaisys".

User ID	Common Name	Worktop Name	Device ID
oaisys	oaisys	NONE	NONE

Buttons for "Edit" and "List All" are located below the table.

The **Edit CTI User** screen is displayed next. For **Call Origination/Termination and Device Status** and **Calls On A Device Monitoring**, select "Any". For **Device Monitoring**, select the security device group from **Section 6.5**. Check **Call Monitoring**, and click **Apply Changes**.

The screenshot shows the "Edit CTI User" screen in the Avaya Application Enablement Services Management Console. The top header and navigation bar are identical to the previous screen. The sidebar menu shows "Security Database" expanded, with "CTI Users" and "List All Users" visible. The main content area is titled "Edit CTI User" and contains a form for editing the "oaisys" user profile.

User Profile:

- User ID: oaisys
- Common Name: oaisys
- Worktop Name: NONE (dropdown)
- Unrestricted Access: ☐

Call and Device Control:

- Call Origination/Termination and Device Status: Any (dropdown)

Call and Device Monitoring:

- Device Monitoring: Oaisys Device Group (dropdown)
- Calls On A Device Monitoring: Any (dropdown)
- Call Monitoring: ☒

Routing Control:

- Allow Routing on Listed Devices: None (dropdown)

Buttons for "Apply Changes" and "Cancel Changes" are at the bottom.

7. Configure OAISYS Recording Server

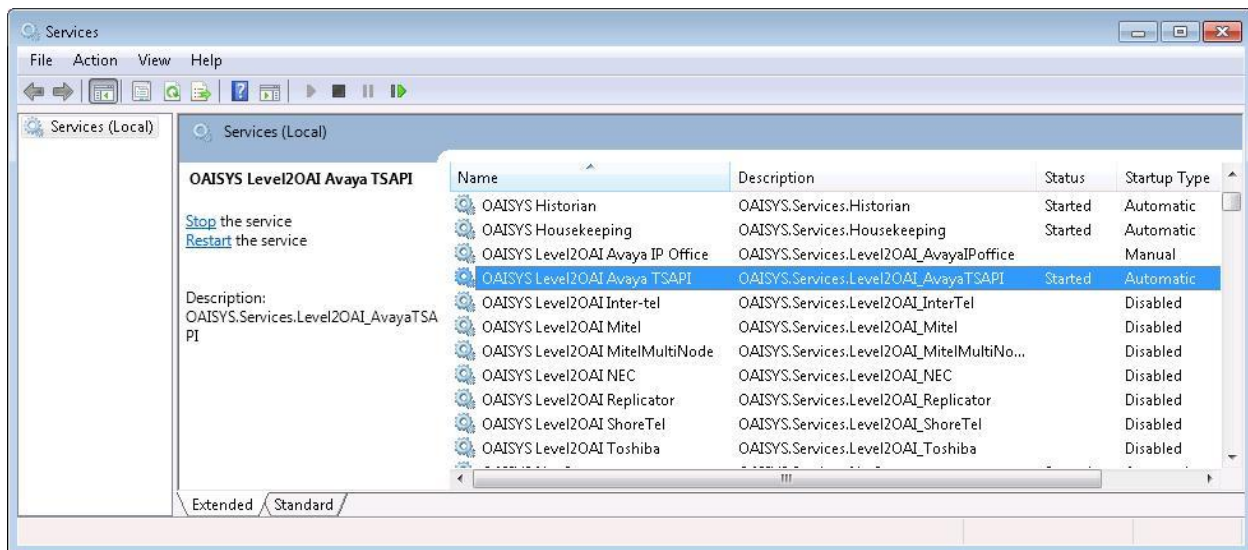
This section provides the procedures for configuring Recording Server. The procedures include the following areas:

- Administer TSAPI service
- Launch Management Studio
- Administer CTI port settings
- Administer recording ports

The configuration of Recording Server is performed by authorized third party integrators. The procedural steps are presented in these Application Notes for informational purposes.

7.1. Administer TSAPI Service

From the Recording Server, select **Start → Control Panel → Administrative Tools > Services** to display the **Services** screen. Configure the **OAISYS Level2OAI Avaya TSAPI** service to be “Automatic”, and start the service as shown below.



7.2. Launch Management Studio

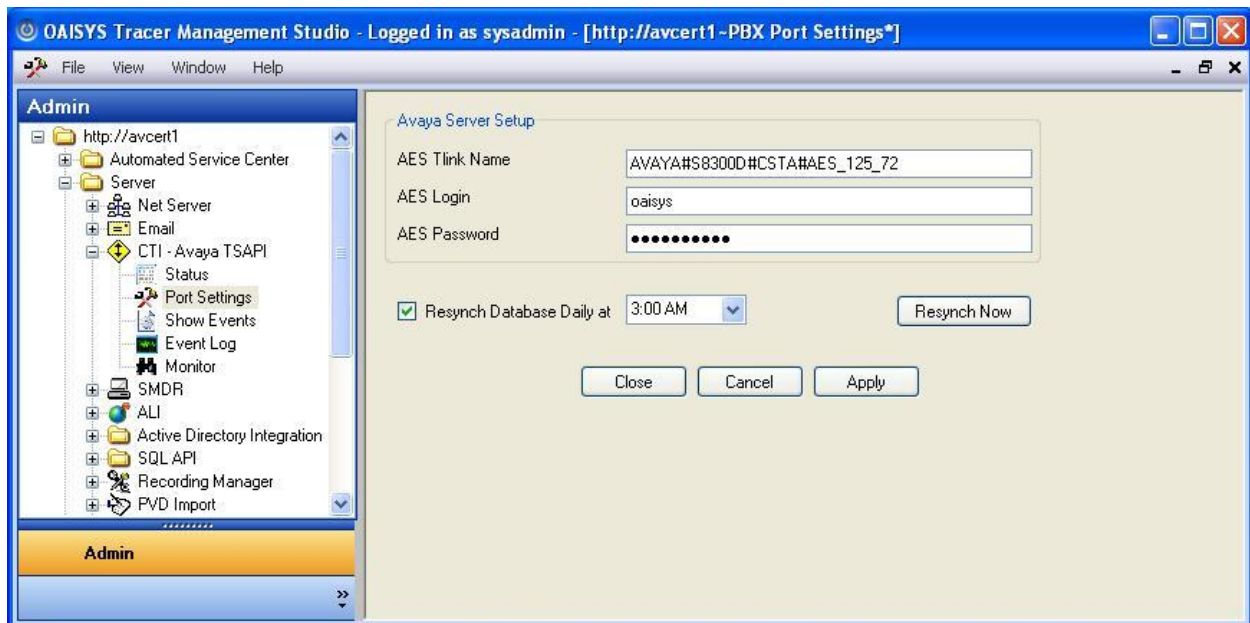
From a PC running the Management Studio application, select **Start → All Programs → OAISYS → OAISYS Management Studio** to launch the application, and log in using administrative credentials.



7.3. Administer CTI Port Settings

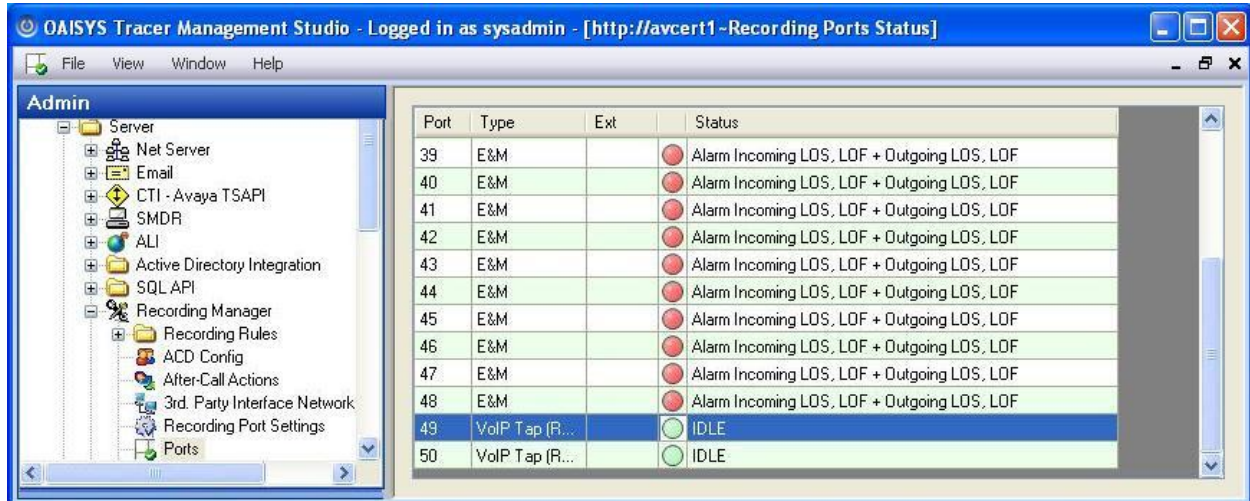
The OAISYS Tracer Management Studio screen is displayed. Select **Server → CTI – Avaya TSAPI → Port Settings** in the left pane, to display the **Avaya Server Setup** screen. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **AES Tlink Name:** The Tlink name from **Section 6.7**.
- **AES Login:** The OAISYS user credentials from **Section 6.8**.
- **AES Password:** The OAISYS user credentials from **Section 6.8**.



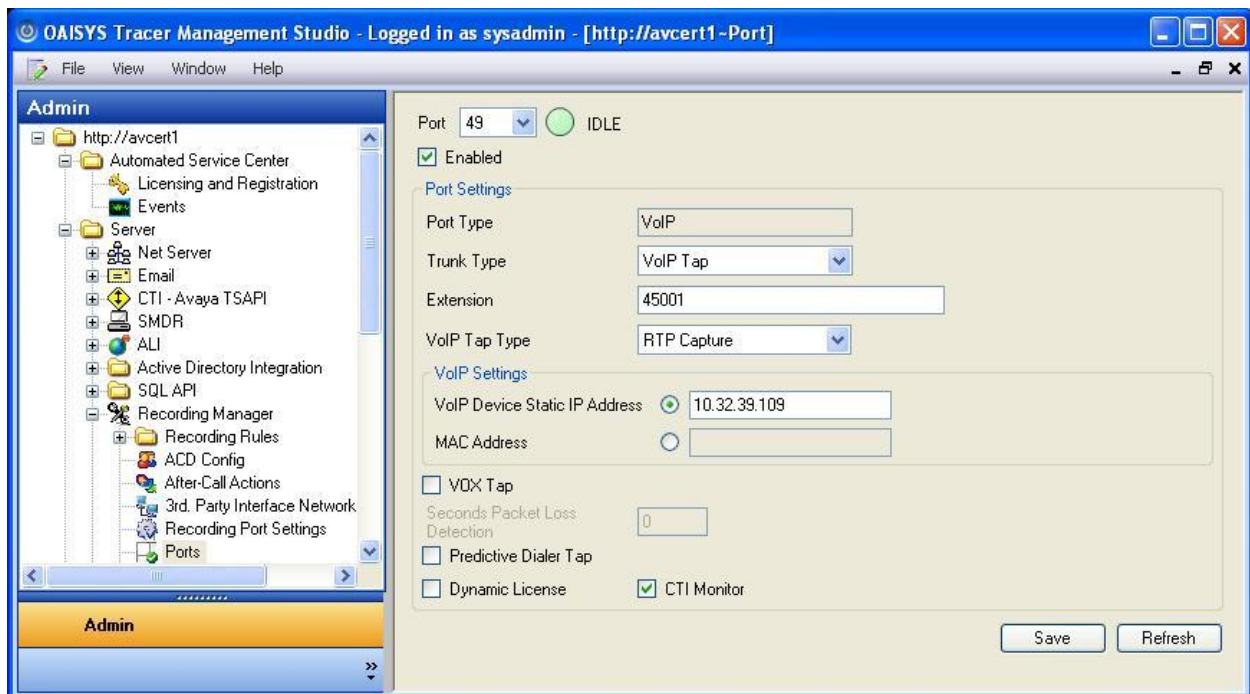
7.4. Administer Recording Ports

Select **Server** → **Recording Manager** → **Ports** in the left pane, to display a list of ports. Scroll down as necessary to select and double-click on the first VoIP port, in this case port “49”.



In the updated screen shown below, check **Enabled**. For **Extension**, enter the first agent station extension from **Section 3**. For **VoIP Device Static IP Address**, enter the IP address of the first agent station. Retain the default values in the remaining fields.

Repeat this section to configure a port for each monitored agent. In the compliance testing, two ports were configured with agent station extensions “45001” and “45002”.



8. Verification Steps

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

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
1	4	no	aes_125_72	established	60	30

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.

Verify that the **Status** is “Talking” for the TSAPI link administered in **Section 6.3**, as shown below. Also verify that the corresponding **Associations** value reflects the total number of monitored devices from **Section 3**.

**Application Enablement Services**
Management Console

Welcome: User
Last login: Tue Dec 4 07:43:39 2012 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
SW Version: r6-2-0-18-0
Server Date and Time: Tue Dec 4 11:15:02 MST 2012

Status | Status and Control | TSAPI Service Summary

Home | Help | Logout

▶ AE Services

▶ Communication Manager Interface

▶ Licensing

▶ Maintenance

▶ Networking

▶ Security

▼ Status

Alarm Viewer

▶ 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 60 seconds

	Link	Switch Name	Switch CTI Link ID	Status	Since	State	Switch Version	Associations	Msgs to Switch	Msgs from Switch	Msgs Period
○	1	S8800	2	Talking	Fri Nov 9 10:40:32 2012	Online	16	2	15	15	30
●	2	S8300D	1	Talking	Tue Dec 4 09:11:40 2012	Online	16	4	30	60	30

Online Offline

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

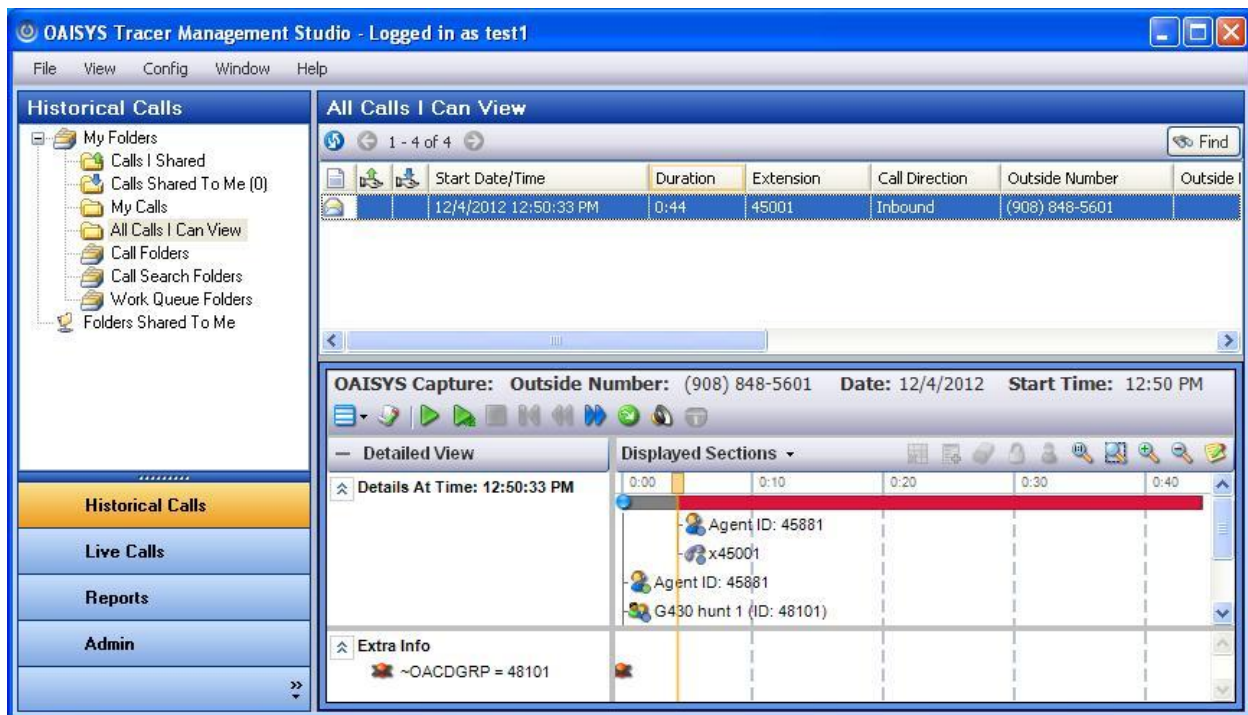
TSAPI Service Status TLink Status User Status

8.3. Verify OAISYS Recording Server

Log an agent in to the skill group to handle and complete an ACD call. Follow the procedural steps in **Section 7.2** to launch the Management Studio application, and log in using the appropriate user credentials.

Select **Historical Calls** in the lower left pane, followed by **My Folder → All Calls I Can View** in the upper left pane. Verify that there is an entry reflecting the last call, with proper values in the relevant fields.

Double click on the entry to listen to the playback. Verify that the call recording can be played back.



9. Conclusion

These Application Notes describe the configuration steps required for OAISYS Recording Server to successfully interoperate with Avaya Aura® Communication Manager 6.2 and Avaya Aura® Application Enablement Services 6.2 using station tap. 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 7.0, Release 6.2, July 2012, available at <http://support.avaya.com>.
2. *Avaya Aura® Application Enablement Services Administration and Maintenance Guide*, Release 6.2, Issue 1, July 2012, available at <http://support.avaya.com>.
3. *OAISYS Administration Guide*, Version 7.2, May 29, 2012, available at http://www.oaisys.com/downloads/OAISYS_Version_7.2_Administration_Guide.pdf.
4. *OAISYS Management Studio User Guide*, Version 7.2, May 23, 2012, available at http://www.oaisys.com/downloads/OAISYS_Version_7.2_Management_Studio_User_guide.pdf.

©2013 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.