



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

---

# **Application Notes for KnoahSoft Harmony with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services using Multiple Registrations – Issue 1.0**

### **Abstract**

These Application Notes describe the configuration steps required for KnoahSoft Harmony to interoperate with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services using the Multiple Registrations method. KnoahSoft Harmony is a solution that can provide monitoring, recording, quality assurance, reporting, and analytic features for contact centers. The compliance testing focused on the call recording feature.

In the compliance testing, KnoahSoft Harmony used the Telephony Services Application Programming Interface from Avaya Aura® Application Enablement Services to monitor skill groups and agents on Avaya Aura® Communication Manager, and used the Multiple Registration feature via the Avaya Aura® Application Enablement Services Device, Media, and Call Control interface 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 KnoahSoft Harmony to interoperate with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services using the Multiple Registrations method. KnoahSoft Harmony is a solution that can provide monitoring, recording, quality assurance, reporting, and analytic features for contact centers. The compliance testing focused on the call recording feature.

In the compliance testing, KnoahSoft Harmony used the Telephony Services Application Programming Interface (TSAPI) from Avaya Aura® Application Enablement Services to monitor skill groups and agents on Avaya Aura® Communication Manager, and used the Multiple Registrations feature via the Avaya Aura® Application Enablement Services Device, Media, and Call Control (DMCC) interface to capture the media associated with the monitored agents for call recording.

The TSAPI interface is used by KnoahSoft Harmony to monitor the agents to be recorded, and the DMCC interface is used by KnoahSoft Harmony to register a virtual recording device against each monitored agent extension to pick up the media for call recording. When there is an active call at the monitored agent, KnoahSoft Harmony is informed of the call via event reports from the TSAPI interface, and starts the call recording by using the media from the recording device associated with the monitored agent. The TSAPI 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 Harmony application, the application automatically queries on the logical agent IDs and requests monitoring on the skill groups and agent extensions using TSAPI, and registers a recording device for each monitored agent extension using DMCC.

For the manual part of the testing, each call was handled manually on the agent telephone 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 the Harmony server.

The verification of tests included using the Harmony logs for proper message exchanges, and using the Harmony web interface for proper logging and playback of the calls.

## 2.1. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability testing.

The feature testing focused on verifying the following on Harmony:

- Handling of TSAPI messages in the areas of event notification and value queries.
- Use of DMCC registration services to register and un-register the recording devices.
- Use of DMCC monitoring services and media control events to obtain the media from the recording devices.
- 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 Harmony to recover from adverse conditions, such as disconnecting/reconnecting the Ethernet cable to Harmony.

## 2.2. Test Results

All test cases were executed. The following were the observations on Harmony from the compliance testing.

- In the attended transfer scenario, the reported ANI for the outbound call associated with the transfer-from agent will contain the other agent's extension instead of the calling party extension by design. The same holds true for the conference and internal call scenarios.
- After a link recovery, any call established before the outage and dropped during the outage will continue to record until new calls occur at the agent. The call recording included the link outage period until the new call occurs, and the recording playback contained silence for these periods, which can vary in duration. The recording for the first couple of new calls for the agent may be lumped with the call that was dropped after the link disruption.
- For calls established during a link disruption and dropped after the restoration, the call will continue to record until new calls occur at the agent, with recording for the agent may not resume until after the first couple of new calls.

## 2.3. Support

Technical support on Harmony can be obtained through the following:

- **Phone:** (650) 385-6795
- **Email:** [support@knoahsoft.com](mailto:support@knoahsoft.com)
- **Web:** <http://www.knoahsoft.com/support.html>

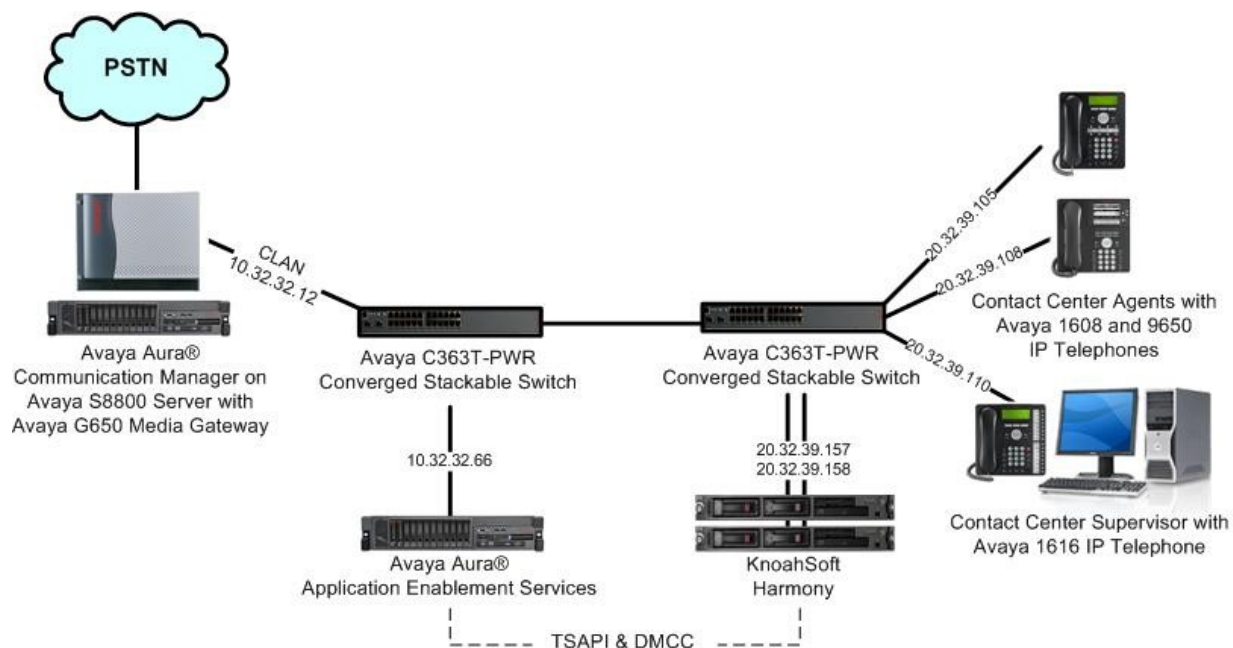
### 3. Reference Configuration

Harmony can be configured on a single server or with components distributed across multiple servers. The compliance test used a two-server configuration, as shown in the figure below.

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, the contact center devices consist of resources shown in the table below. Harmony used the agent IDs with TSAPI queries to obtain the associated agent telephone extensions, and requested monitoring on the skill group and agent extensions.

Device Type	Extension
VDN	65000
Skill Group	65555
Supervisor Extension	65005
Agent IDs	65881, 65882
Agent Extensions	65001, 65002



## 4. Equipment and Software Validated

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

Equipment	Software
Avaya Aura® Communication Manager on Avaya S8800 Server	6.0.1 SP 5.01 (R016x.00.1.510.1-19303)
Avaya G650 Media Gateway <ul style="list-style-type: none"><li>TN799DP C-LAN Circuit Pack</li><li>TN2302AP IP Media Processor</li></ul>	HW01 FW040 HW20 FW122
Avaya Aura® Application Enablement Services	6.1.1
Avaya 1600 Series IP Telephone (H.323)	1.3
Avaya 9650 IP Telephone (H.323)	2.6.4
KnoahSoft Harmony on Windows 2003 Server with Service Pack 2 <ul style="list-style-type: none"><li>Recorder</li><li>AES Adapter</li><li>Avaya Adapter</li><li>Avaya TSAPI Windows Client</li></ul>	3.4.0 3.4.0 with Patch 01192012_0003 3.4.0 3.4.0 6.1.0.396
KnoahSoft Harmony on Windows 2008 Server with Service Pack 2 <ul style="list-style-type: none"><li>Web Application Server</li><li>RMS</li><li>Database Server</li></ul>	3.4.0 3.4.0 3.4.0 Microsoft SQL Server 2008

## 5. Configure Avaya Aura® Communication Manager

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

- Verify license
- Administer CTI link
- Administer system parameters features
- Administer stations
- Administer IP codec set

### 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)?	y	Authorization Codes?	y	
Analog Trunk Incoming Call ID?	y	CAS Branch?	n	
A/D Grp/Sys List Dialing Start at 01?	y	CAS Main?	n	
Answer Supervision by Call Classifier?	y	Change COR by FAC?	n	
ARS?	y	<b>Computer Telephony Adjunct Links?</b>	<b>y</b>	
ARS/AAR Partitioning?	y	Cvg Of Calls Redirected Off-net?	y	
ARS/AAR Dialing without FAC?	n	DCS (Basic)?	y	
ASAI Link Core Capabilities?	y	DCS Call Coverage?	y	
ASAI Link Plus Capabilities?	y	DCS with Rerouting?	y	
Async. Transfer Mode (ATM) PNC?	n	Digital Loss Plan Modification?	y	
Async. Transfer Mode (ATM) Trunking?	n	DS1 MSP?	y	
ATM WAN Spare Processor?	n	DS1 Echo Cancellation?	y	
ATMS?	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			
<b>Extension:</b>	60100			
<b>Type:</b>	ADJ-IP			
		COR:	1	
<b>Name:</b>	CTI Link			

### 5.3. Administer System Parameters Features

Use the “change system-parameters features” command to enable **Create Universal Call ID (UCID)**, which is located on **Page 5**. For **UCID Network Node ID**, enter an available node ID.

```
change system-parameters features                                     Page 5 of 19
      FEATURE-RELATED SYSTEM PARAMETERS

SYSTEM PRINTER PARAMETERS
  Endpoint:                               Lines Per Page: 60

SYSTEM-WIDE PARAMETERS
      Switch Name: S8500-SAL
      Emergency Extension Forwarding (min): 10
      Enable Inter-Gateway Alternate Routing? n
      Enable Dial Plan Transparency in Survivable Mode? n
      COR to Use for DPT: station

MALICIOUS CALL TRACE PARAMETERS
      Apply MCT Warning Tone? n      MCT Voice Recorder Trunk Group:
      Delay Sending RElease (seconds): 0

SEND ALL CALLS OPTIONS
      Send All Calls Applies to: station      Auto Inspect on Send All Calls? n
      Preserve previous AUX Work button states after deactivation? n

UNIVERSAL CALL ID
      Create Universal Call ID (UCID)? y      UCID Network Node ID: 1
```

Navigate to **Page 13**, and enable **Send UCID to ASAI**. This parameter allows for the universal call ID to be sent to Harmony.

```
change system-parameters features                                     Page 13 of 19
      FEATURE-RELATED SYSTEM PARAMETERS

CALL CENTER MISCELLANEOUS
      Callr-info Display Timer (sec): 10
      Clear Callr-info: next-call
      Allow Ringer-off with Auto-Answer? y

      Reporting for PC Non-Predictive Calls? n

      Agent/Caller Disconnect Tones? n
      Interruptible Aux Notification Timer (sec): 3
      Zip Tone Burst for Callmaster Endpoints: double

ASAI
      Copy ASAI UII During Conference/Transfer? y
      Call Classification After Answer Supervision? y
      Send UCID to ASAI? y
      For ASAI Send DTMF Tone to Call Originator? y
```

## 5.4. Administer Stations

Use the “change station n” command, where “n” is the first agent extension from **Section Error! Reference source not found.** Enable **IP SoftPhone**, to allow a recording device to be registered against the station. For **Security Code**, enter a desired code. Note that Harmony requires the same security code to be used by all agents.

change station 65001		Page 1 of 4
STATION		
Extension: 65001	Lock Messages? n	BCC: 0
Type: 1608	<b>Security Code: 65000</b>	TN: 1
Port: S00000	Coverage Path 1: 1	COR: 1
Name: Harmony Agent #1	Coverage Path 2:	COS: 6
	Hunt-to Station:	
STATION OPTIONS		
Loss Group: 19	Time of Day Lock Table:	
	Personalized Ringing Pattern: 1	
Speakerphone: 2-way	Message Lamp Ext: 65001	
Display Language: english	Mute Button Enabled? y	
Survivable GK Node Name:		
Survivable COR: internal	Media Complex Ext:	
Survivable Trunk Dest? y	<b>IP SoftPhone? y</b>	
	IP Video Softphone? n	
	Short/Prefixed Registration Allowed: default	

Repeat this section to administer all stations to be monitored. In the compliance testing, two stations were administered as shown below.

list station 65001 count 2									
STATIONS									
Ext/ Hunt-to	Port/ Type	Name/ Surv GK NN	Move	Room/ Data Ext	Cv1/ Cv2	COR/ COS	Cable/ TN	Jack	
65001	S00000	Harmony Agent #1			1	1			
	1608		no			1	1		
65002	S00045	Harmony Agent #2			1	1			
	9650		no			1	1		



## 5.5. Administer IP Codec Set

Use the “change ip-codec-set n” command, where “n” is an existing codec set number used for integration with Harmony. For **Audio Codec**, enter the desired codec, in this case “G.711MU”. Note that Harmony only supports the G.711MU and G.729 variants, and requires the same codec type to be used by all agents.

change ip-codec-set 1				Page 1 of 2	
IP Codec Set					
Codec Set: 1					
Audio		Silence	Frames	Packet	
Codec		Suppression	Per Pkt	Size (ms)	
1:	<b>G.711</b>	<b>n</b>	<b>2</b>	<b>20</b>	
2:					
3:					

## 6. Configure Avaya Aura® Application Enablement Services

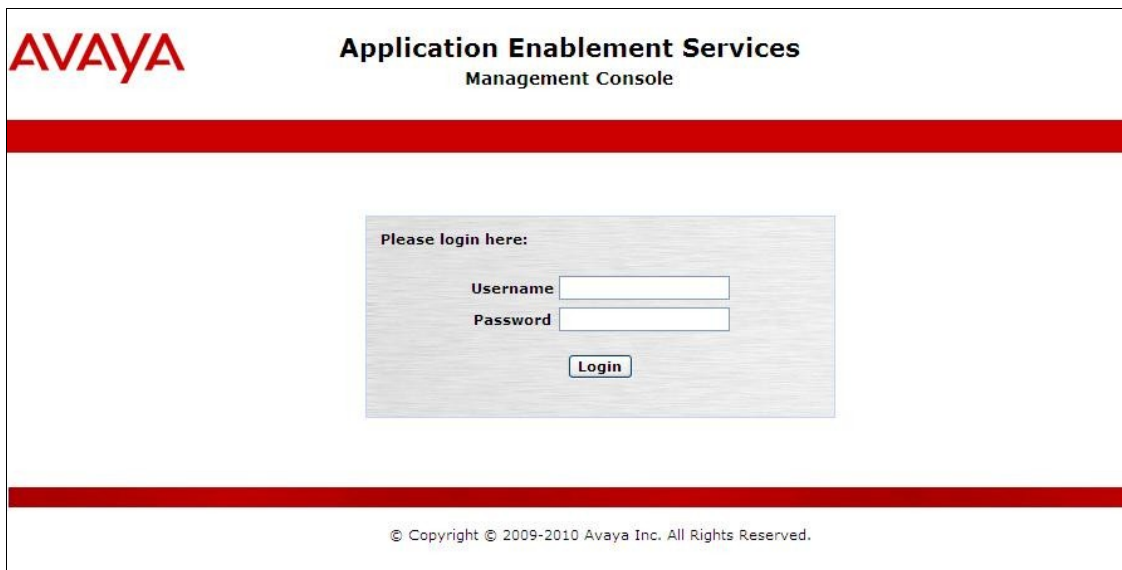
This section provides the procedures for configuring Application Enablement Services. The procedures include the following areas:

- Launch OAM interface
- Verify license
- Administer TSAPI link
- Administer H.323 gatekeeper
- Disable security database
- Restart TSAPI service
- Obtain Tlink name
- Administer Harmony user
- Enable DMCC unencrypted port

### 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 separates the header from the main content area. In the center of the page is a light gray rectangular box containing the text "Please login here:" followed by two input fields labeled "Username" and "Password", and a "Login" button below them. Another thick red horizontal bar is located below the login box. At the bottom of the page, a small copyright notice reads: "© Copyright © 2009-2010 Avaya Inc. All Rights Reserved."

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

The screenshot displays the Avaya Application Enablement Services Management Console. The top header includes the Avaya logo, the title "Application Enablement Services Management Console", and a welcome message for user "craft" with login details. A red navigation bar contains the "Licensing" tab and links for "Home", "Help", and "Logout". On the left, a sidebar menu lists "AE Services", "Communication Manager Interface", "Licensing" (selected), "WebLM Server Address", "WebLM Server Access", "Reserved Licenses", "Maintenance", "Networking", and "Security". The main content area, titled "Licensing", provides instructions for setting up and maintaining the WebLM, listing "WebLM Server Address", "WebLM Server Access", and "Reserved Licenses" as required items.

**AVAYA Application Enablement Services Management Console**

Welcome: User craft  
Last login: Fri Jan 13 12:50:35 2012 from 20.32.39.20  
HostName/IP: AES2-S8800/10.32.32.66  
Server Offer Type: VIRTUAL\_APPLIANCE  
SW Version: r6-1-1-30-0

**Licensing** Home | Help | Logout

- ▶ 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

## 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.

This screenshot is identical to the one above, showing the Avaya Application Enablement Services Management Console with the "Licensing" page selected in the sidebar. It displays the same header, navigation bar, sidebar menu, and main content area with instructions for WebLM setup and license management.

**AVAYA Application Enablement Services Management Console**

Welcome: User craft  
Last login: Fri Jan 13 12:50:35 2012 from 20.32.39.20  
HostName/IP: AES2-S8800/10.32.32.66  
Server Offer Type: VIRTUAL\_APPLIANCE  
SW Version: r6-1-1-30-0

**Licensing** Home | Help | Logout

- ▶ 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** screen in the right pane.

Verify that there are sufficient licenses for **TSAPI Simultaneous Users** and **Device Media and Call Control**, as shown below.


Web License Manager (WebLM v4.6)

 [Logout](#)

Install License

▼ Licensed Products

▼ APPL\_ENAB

Application\_Enablement

Uninstall License

Change Password

Server Properties

Manage Users

Logout

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

You are here: Licensed products > Application Enablement (CTI)

License installed on: Dec 6, 2011 5:02:20 PM EST

[View Peak Usage](#)

**Licensed Features**

Feature (Keyword)	Expiration Date	Licensed	Acquired
CVLAN ASAI (VALUE_AES_CVLAN_ASAI)	2012/12/06	16	0
Unified CC API Desktop Edition (VALUE_AES_AEC_UNIFIED_CC_DESKTOP)	2012/12/06	1000	0
AES ADVANCED SMALL SWITCH (VALUE_AES_AEC_SMALL_ADVANCED)	2012/12/06	3	0
CVLAN Proprietary Links (VALUE_AES_PROPRIETARY_LINKS)	2012/12/06	16	0
Product Notes (VALUE_NOTES)	2012/12/06	SmallServerTypes: s8300c;s8300d;icc;premio;tn8400;laptop;CtiSmallServer MediumServerTypes: ibmx306;ibmx306m;dell1950;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; CSL_T1_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; CSL_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)	2012/12/06	3	0
TSAPI Simultaneous Users (VALUE_AES_TSAPI_USERS)	2012/12/06	1000	3
DLG (VALUE_AES_DLG)	2012/12/06	16	0
Device Media and Call Control (VALUE_AES_DMCC_DMC)	2012/12/06	1000	3
AES ADVANCED MEDIUM SWITCH (VALUE_AES_AEC_MEDIUM_ADVANCED)	2012/12/06	3	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 Application Enablement Services Management Console. The top navigation bar includes "AE Services | TSAPI | TSAPI Links" and "Home | Help | Logout". The left sidebar shows a tree view with "AE Services" expanded, containing "CVLAN", "DLG", "DMCC", "SMS", "TSAPI" (expanded), "TSAPI Links", and "TSAPI Properties". The main content area is titled "TSAPI Links" and contains a table with the following data:

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

Below the table are three buttons: "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 AVAYA Application Enablement Services Management Console with the "Add TSAPI Links" screen. The top navigation bar and left sidebar are the same as in the previous screenshot. The main content area is titled "Add TSAPI Links" and contains the following form fields:

- Link: 1
- Switch Connection: S8800
- Switch CTI Link Number: 1
- ASAI Link Version: 4
- Security: Unencrypted

Below the form fields are two buttons: "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' > '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'. One connection is listed: 'S8800' 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 'Edit H.323 Gatekeeper' button is highlighted.

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 be used as H.323 gatekeeper, in this case “10.32.32.12” as shown below. Click **Add Name or IP**.

The screenshot shows the 'Edit H.323 Gatekeeper - S8800' screen. The left navigation pane is expanded to 'Communication Manager Interface' > 'Switch Connections'. The main content area has a text input field containing '10.32.32.12' and an 'Add Name or IP' button. Below the input field is a 'Name or IP Address' label and two buttons: 'Delete IP' and 'Back'.

## 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, and click **Apply Changes**.

The screenshot shows the Avaya Application Enablement Services Management Console. The left navigation pane has 'Security' expanded, with 'Security Database' and 'Control' selected. The main content area is titled 'SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services'. It contains two unchecked checkboxes: 'Enable SDB for DMCC Service' and 'Enable SDB for TSAPI Service, JTAPI and Telephony Web Services'. Below these is an 'Apply Changes' button. The top right of the console displays user information: 'Welcome: User craft', 'Last login: Fri Jan 13 12:50:35 2012 from 20.32.39.20', 'HostName/IP: AES2-S8800/10.32.32.66', 'Server Offer Type: VIRTUAL\_APPLIANCE', and 'SW Version: r6-1-1-30-0'.

## 6.6. Restart TSAPI Service

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

The screenshot shows the Avaya Application Enablement Services Management Console. The left navigation pane has 'Maintenance' expanded, with 'Service Controller' selected. The main content area is titled 'Service Controller'. It contains a table with two columns: 'Service' and 'Controller Status'. The table lists several services, with 'TSAPI Service' checked and 'Running'. Below the table is a link 'Status and Control'. At the bottom, there are buttons for 'Start', 'Stop', 'Restart Service', 'Restart AE Server', 'Restart Linux', and 'Restart Web Server'. The top right of the console displays the same user information as the previous screenshot.

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

## 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 Harmony.

In this case, the associated Tlink name is “AVAYA#S8800#CSTA-S#AES2-S8800”. 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 user "craft" with login details. A red navigation bar contains "Security | Security Database | Tlinks" and links for "Home | Help | Logout". On the left, a sidebar menu shows various categories, with "Security Database" expanded to highlight "Tlinks". The main content area, titled "Tlinks", shows a single entry: "AVAYA#S8800#CSTA#AES2-S8800" with a green status icon and a "Delete Tlink" button.



## 6.8. Administer Harmony 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).

**AVAYA**

**Application Enablement Services**  
Management Console

Welcome: User craft  
Last login: Fri Jan 13 12:50:35 2012 from 20.32.39.20  
HostName/IP: AES2-S8800/10.32.32.66  
Server Offer Type: VIRTUAL\_APPLIANCE  
SW Version: r6-1-1-30-0

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 Idharmony

\* Common Nameharmony

\* Surnameharmony

\* 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

## 6.9. Enable DMCC Unencrypted Port

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 **Unencrypted Port** under the **Enabled** column, as shown below.

**AVAYA**

**Application Enablement Services**  
Management Console

Welcome: User craft  
Last login: Fri Jan 13 12:50:35 2012 from 20.32.39.20  
HostName/IP: AES2-S8800/10.32.32.66  
Server Offer Type: VIRTUAL\_APPLIANCE  
SW Version: r6-1-1-30-0

Networking | PortsHome | Help | Logout

▶ AE Services

▶ Communication Manager Interface

▶ Licensing

▶ Maintenance

▼ Networking

AE Service IP (Local IP)

Network Configure

Ports

TCP Settings

▶ Security

▶ Status

▶ User Management

▶ Utilities

▶ Help

### Ports

CVLAN Ports

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

DLG Port

TCP Port	
5678	

TSAPI Ports

			Enabled	Disabled
TSAPI Service Port	450		<input checked="" type="radio"/>	<input type="radio"/>
Local TLINK Ports				
TCP Port Min	1024			
TCP Port Max	1039			
Unencrypted TLINK Ports				
TCP Port Min	<input type="text" value="1050"/>			
TCP Port Max	<input type="text" value="1065"/>			
Encrypted TLINK Ports				
TCP Port Min	<input type="text" value="1066"/>			
TCP Port Max	<input type="text" value="1081"/>			

DMCC Server Ports

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

## 7. Configure KnoahSoft Harmony

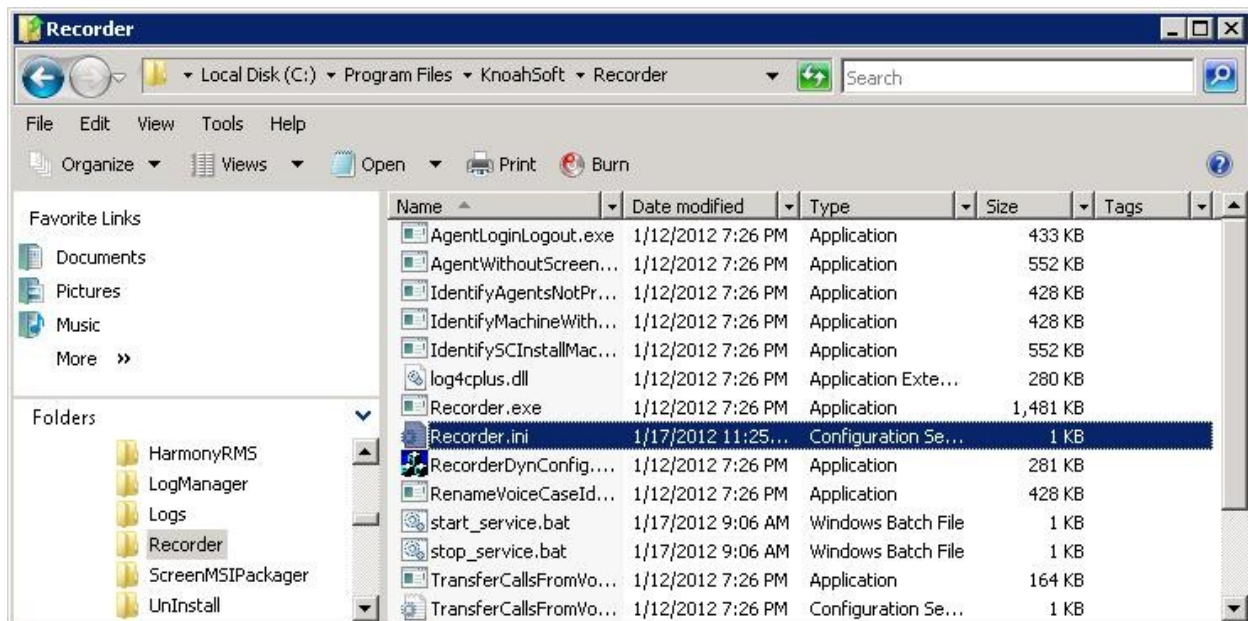
This section provides the procedures for configuring Harmony. The procedures include the following areas:

- Administer Recorder.ini
- Administer AESAdapter.ini
- Administer Avaya adapter properties
- Administer AESAdapter
- Launch web interface
- Administer agents
- Administer virtual recorders

The configuration of Harmony is performed by KnoahSoft installers and partners. The procedural steps are presented in these Application Notes for informational purposes.

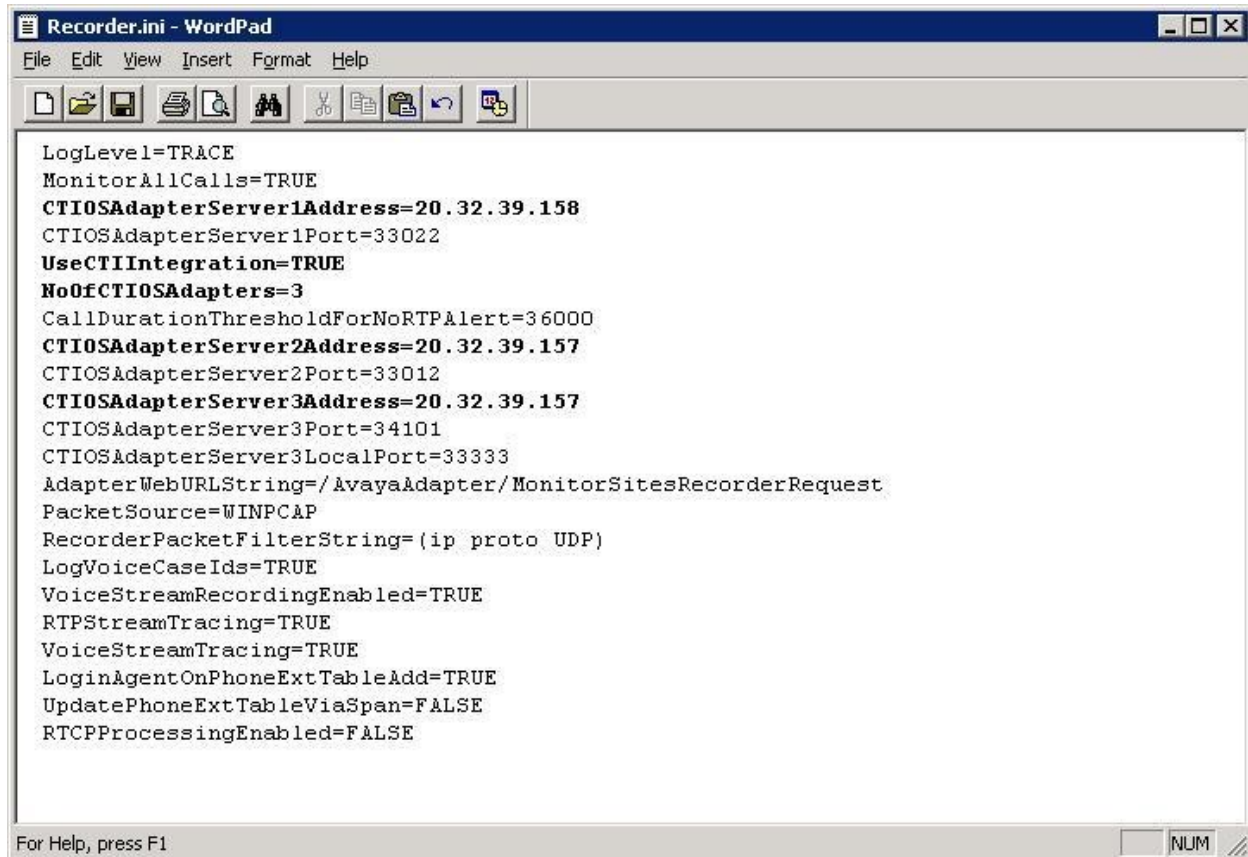
### 7.1. Administer Recorder.ini

From the Harmony server running the Recorder service, navigate to the **C:\Program Files\KnoahSoft\Recorder** directory to locate the **Recorder.ini** file shown below.



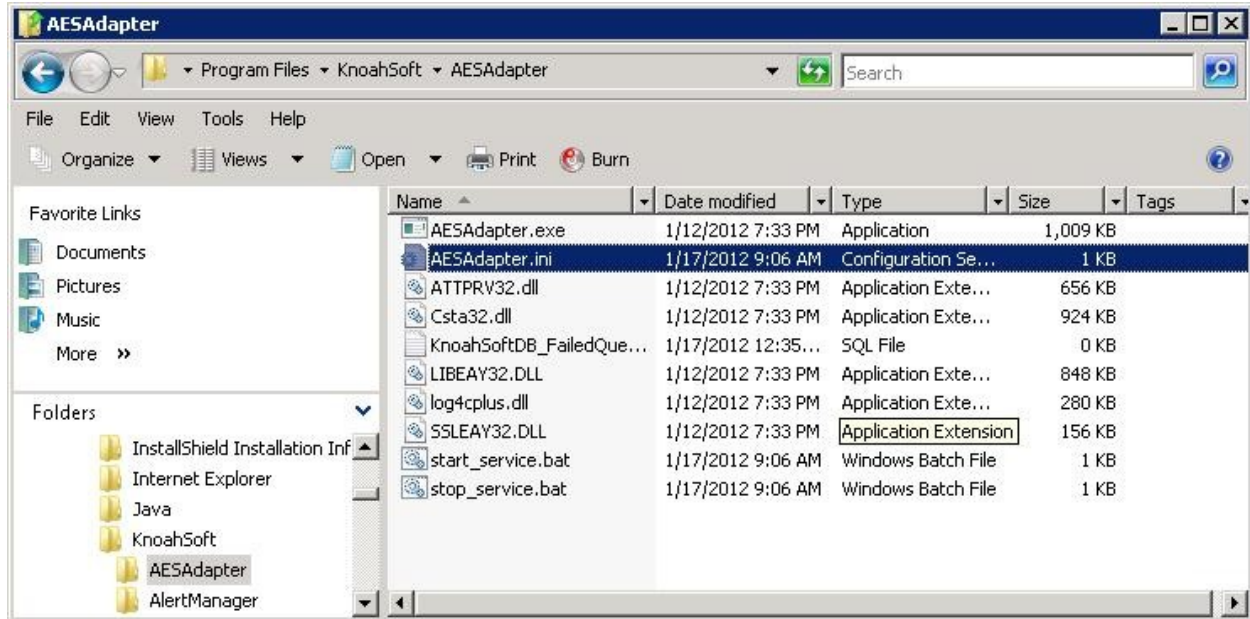
Open the **Recorder.ini** file with the WordPad application. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **CTIOSAdapterServer1Address:** IP address of server with RMS component.
- **UseCTIIIntegration:** "TRUE"
- **NoOfCTIOSAdapters:** "3"
- **CTIOSAdapterServer2Address:** IP address of server with AES adapter component.
- **CTIOSAdapterServer3Address:** IP address of server with Avaya adapter component.

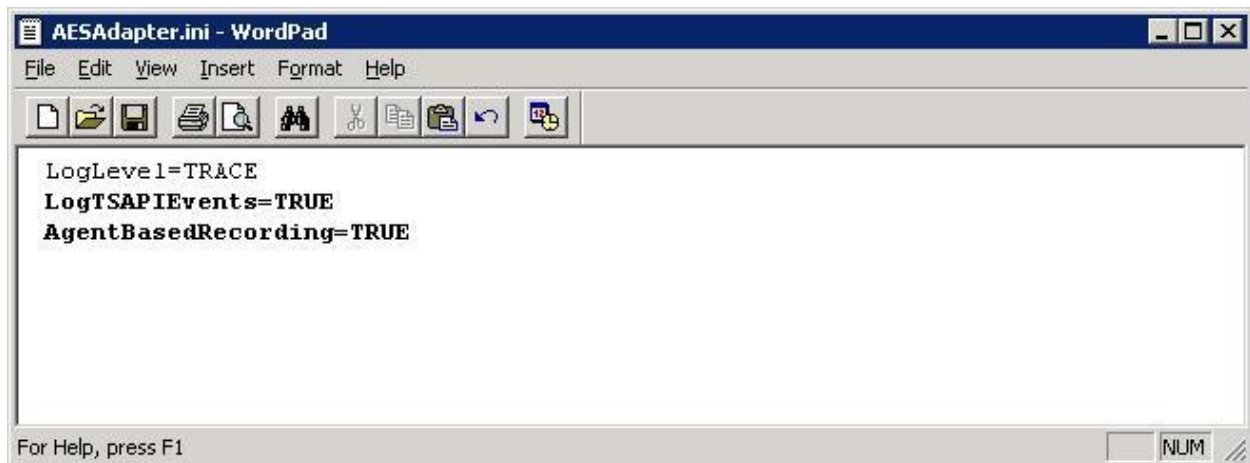


## 7.2. Administer AESAdapter.ini

From the Harmony server running the AES adapter component, navigate to the **C:\Program Files\KnoahSoft\AESAdapter** directory to locate the **AESAdapter.ini** file shown below.



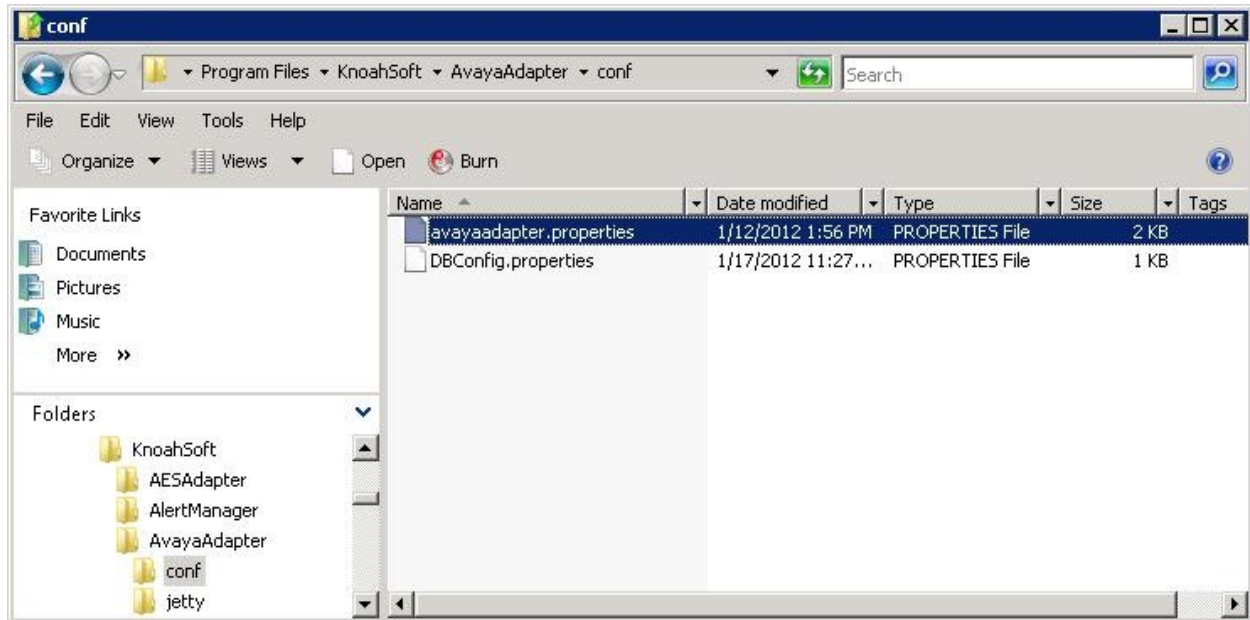
Open the **AESAdapter.ini** file with the WordPad application. Add the **LogTSAPIEvents** and **AgentBasedRecording** parameters and set the values to "TRUE", as shown below. The TSAPI events log were used in the compliance testing for verification purposes.





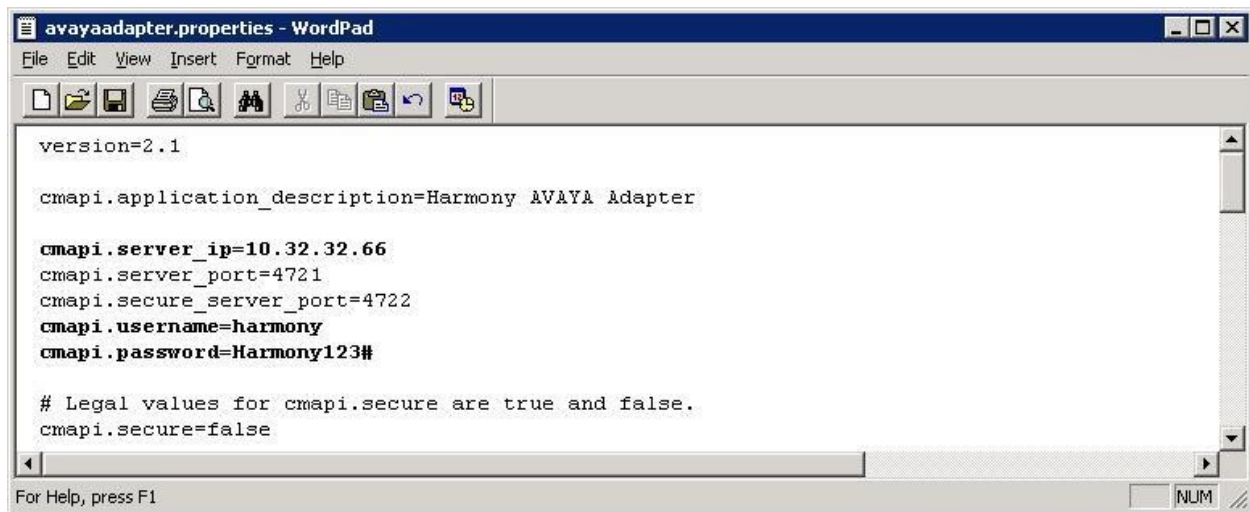
### 7.3. Administer Avaya Adapter Properties

From the Harmony server running the Avaya adapter component, navigate to the **C:\Program Files\KnoahSoft\AvayaAdapter\conf** directory to locate the **avayaadapter.properties** file shown below.



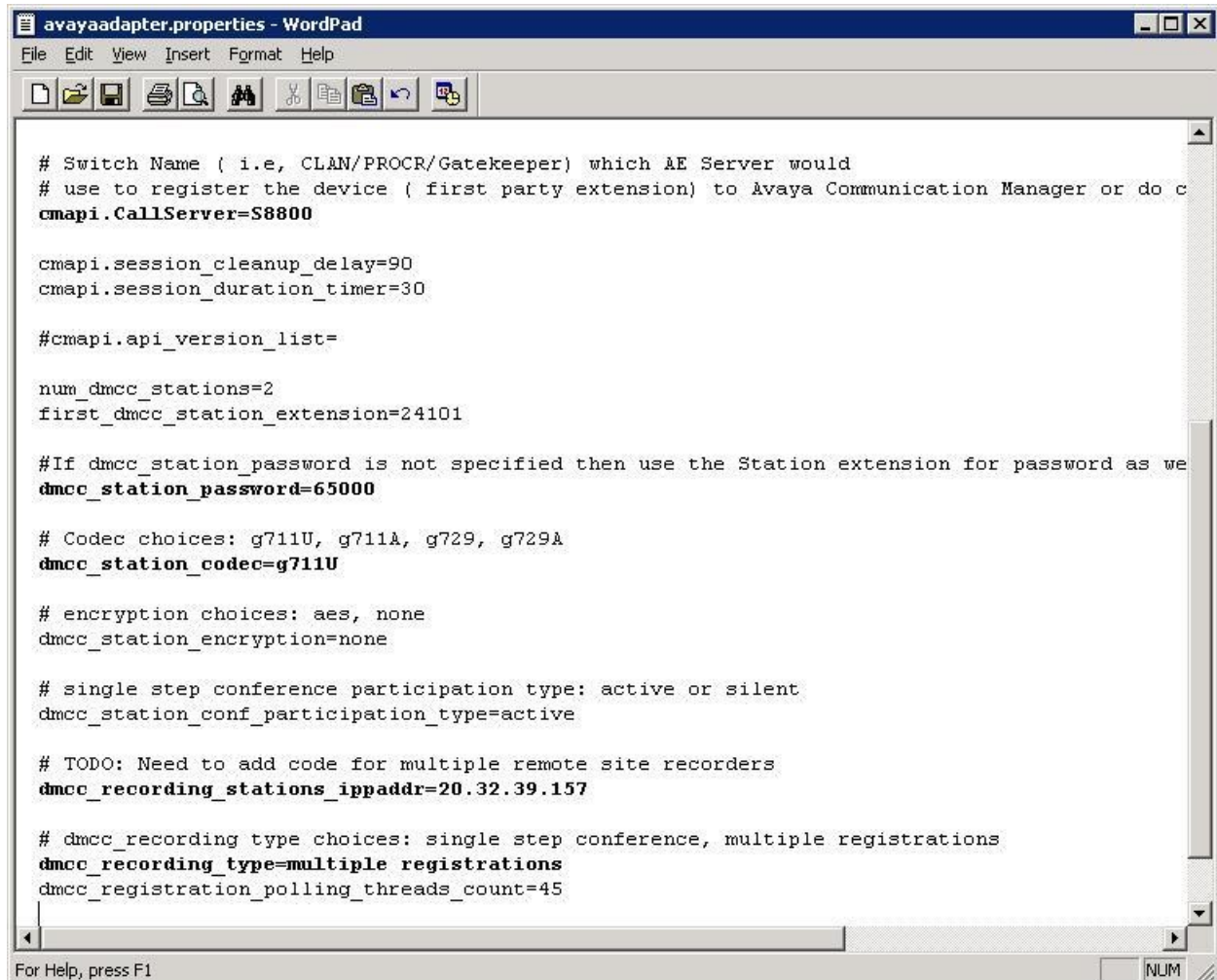
Open the **avayaadapter.properties** file with the WordPad application. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **cmapi.server\_ip:** IP address of the Application Enablement Services server.
- **cmapi.username:** The Harmony user credentials from **Section 6.8**.
- **cmapi.password:** The Harmony user credentials from **Section 6.8**.



Scroll the screen as necessary to enter the following values for the specified fields, and retain the default values for the remaining fields.

- **cmapi.CallServer:** The switch connection name from **Section 6.3**.
- **dmcc\_station\_password:** The security code from **Section 5.4**.
- **dmcc\_station\_codec:** The audio codec from **Section 5.5**.
- **dmcc\_recording\_stations\_ippaddr:** IP address of server with Avaya adapter component.
- **dmcc\_recording\_type:** “multiple registrations”



```
# Switch Name ( i.e, CLAN/PROCR/Gatekeeper) which AE Server would
# use to register the device ( first party extension) to Avaya Communication Manager or do c
cmapi.CallServer=S8800

cmapi.session_cleanup_delay=90
cmapi.session_duration_timer=30

#cmapi.api_version_list=

num_dmcc_stations=2
first_dmcc_station_extension=24101

#If dmcc_station_password is not specified then use the Station extension for password as we
dmcc_station_password=65000

# Codec choices: g711U, g711A, g729, g729A
dmcc_station_codec=g711U

# encryption choices: aes, none
dmcc_station_encryption=none

# single step conference participation type: active or silent
dmcc_station_conf_participation_type=active

# TODO: Need to add code for multiple remote site recorders
dmcc_recording_stations_ippaddr=20.32.39.157

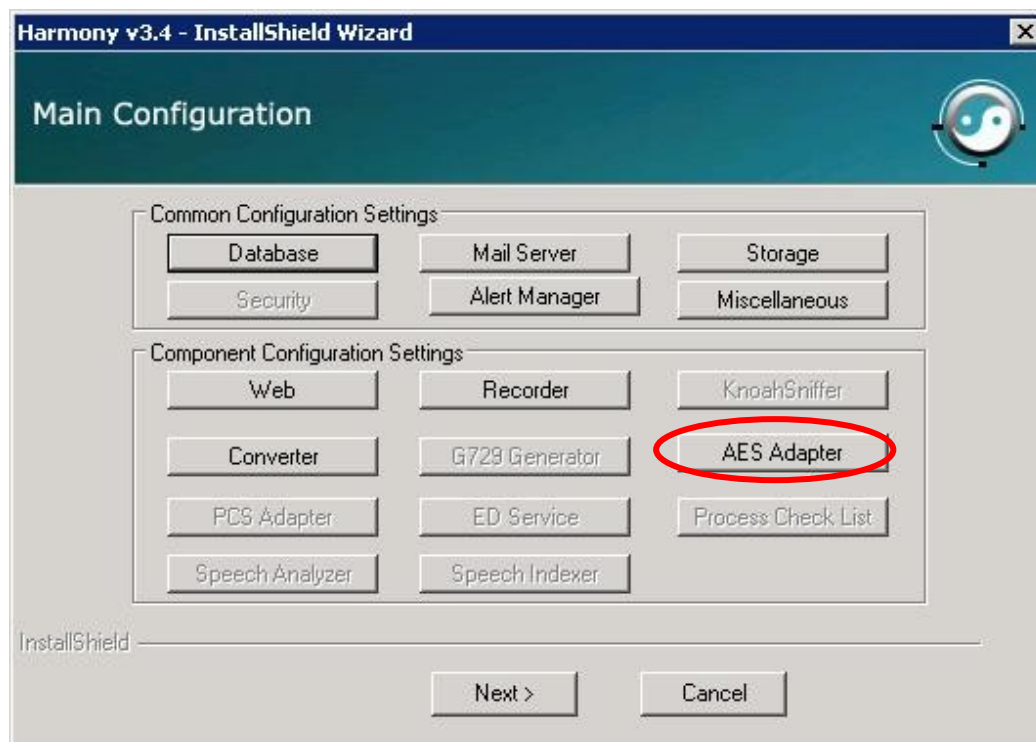
# dmcc_recording type choices: single step conference, multiple registrations
dmcc_recording_type=multiple registrations
dmcc_registration_polling_threads_count=45
```

## 7.4. Administer AESAdapter

From the Harmony server running the AES adapter component, select **Start > All Programs > KnoahSoft > KnoahSoft Config**, to display the **User Login Information** screen. Log in using the appropriate credentials.



The **Main Configuration** screen is displayed. Select **AES Adapter**.





The **AESAdapter configuration settings** screen is displayed. For **Host Data IP**, enter the IP address of the server hosting the AES adapter component. For **Hunt Group Extensions**, enter the skill group extensions from **Section 3**, separated by commas. For **AESAdapter Server Port**, enter “33012”.

Harmony v3.4 - InstallShield Wizard

AESAdapter configuration settings

\* Host Data IP: 20.32.39.157

\* Hunt Group Extensions: 65555

\* AESAdapter Server Port: 33012

InstallShield

< Back Next > Cancel

Screen 1 of 2

The second page of the **AESAdapter configuration settings** screen is displayed next. For **AES Server ID**, enter the Tlink name from **Section 6.7**. For **Login User Name** and **Password**, enter the Harmony user credentials from **Section 6.8**.

Harmony v3.4 - InstallShield Wizard

AESAdapter configuration settings

\* AES Server ID: AVAYA#S8800#CSTA#A

\* Login User Name: harmony

\* Password: [Masked]

InstallShield

< Back Next > Cancel

Screen 2 of 2

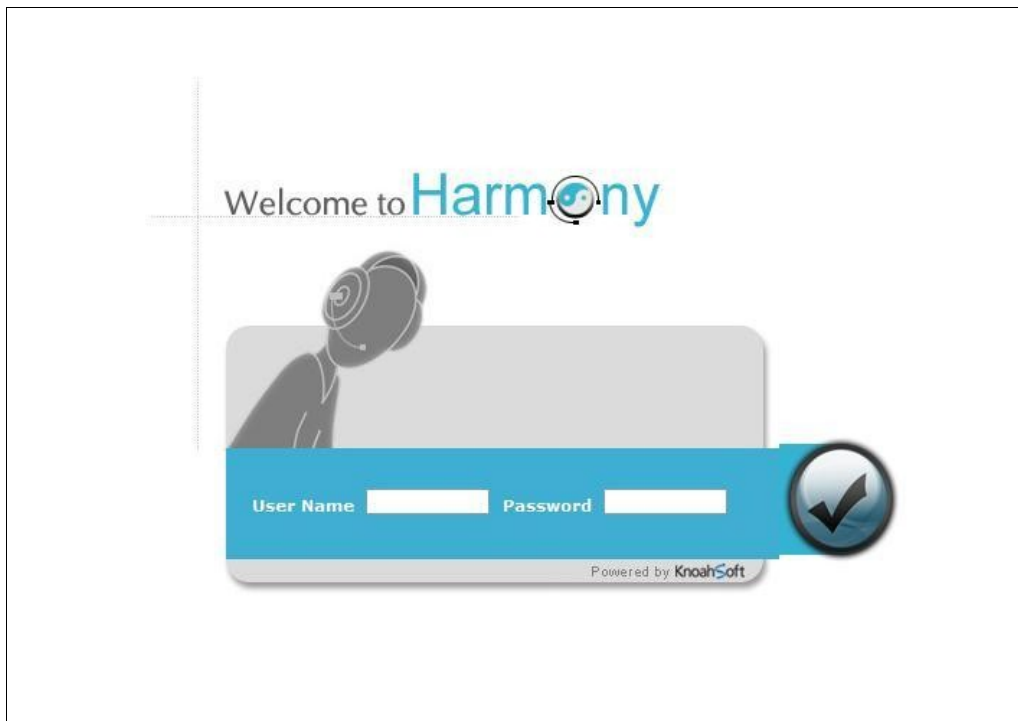
Page forward to the **Choose components you want to start** screen shown below. Check **AESAdapter**, and click **Finish** to complete the wizard.



## 7.5. Launch Web Interface

Launch the Harmony web interface by using the URL “https://ip-address:8080/knoahsoft” in an Internet browser window, where “ip-address” is the IP address of the Harmony server running the web server component.

The **Welcome to Harmony** screen is displayed. Log in using the administrator credentials.



## 7.6. Administer Agents

The **Harmony** screen is displayed. Select the **Employee Management** tab, and click on **Go** to display a list of pre-configured employees in the left pane.

Select the entry corresponding to the first agent from **Section 3** in the left pane, in this case “Agent1”, and the right pane is populated with pre-configured information for this agent. Retain all pre-configured values.

**Harmony** Powered by KnoahSoft

Jan 17, 2012 Admin (Administrator) - Help About Us

Administration

Organization Work Type **Employee Management** Voice Configuration Custom Groups Message Thresholds Rules

Employee Management

Search By Employee Code Look For **Go**

Employee Code Employee Name

002	Agent1
003	Agent2
004	Agent3
005	EXTN_Agent1
006	EXTN_Agent2
007	EXTN_Agent3
001	Supervisor

Agent License - 0 / 900 Seat License - 0 / 300

Photo Upload  Browse...

IMAGE NOT FOUND

\* Employee Code 002

\* Employee First Name Agent1

\* Email Agent1@ks.com

\* Status Active

\* Alias Agent1

Employee Last Name Agent1

\* Hire Date 01/17/2012

\* Network Id Agent1

Is a Harmony User? ☒ Reset Password Release Lock

1 2 3 4

Reporting Profile Recording Rules **User Feature Permissions** Report Feature Permissions

\* Location My Site

\* Department Operations

\* Designation Agent

Supervisor

\* Belongs To Client ☒ My Client

Client/Work Type

Client

<input checked="" type="checkbox"/>	My Client
-------------------------------------	-----------

Work Type

<input checked="" type="checkbox"/>	INBOUND [MYCLI]
<input checked="" type="checkbox"/>	OUTBOUND [MYCLI]

Select step 2 **Recording Rules**, followed by **Add New Extension**.

For **Extension**, enter the first agent ID from **Section 3**. Check the **Enable Recording** field, and retain the default values in the remaining fields.

Repeat this section to configure all agents. In the compliance testing, two agents with employee codes of “002” and “003” were configured.

**Harmony** Powered by KnoahSoft

Broadcast Change Password Jan 17, 2012 Admin ( Administrator ) - Help

**Administration**

Organization Work Type **Employee Management** Voice Configuration Custom Groups Message Thresholds Rules

**Employee Management**

Search By Employee Code Look For Go

Employee Code	Employee Name
002	Agent1
003	Agent2
004	Agent3
005	EXTN_Agent1
006	EXTN_Agent2
007	EXTN_Agent3
001	Supervisor

Agent License - 0 / 900 Seat License - 0 / 300 Photo Upload Browse...

IMAGE NOT FOUND

\* Employee Code 002 \* Employee First Name Agent1 \* Alias Agent1  
 \* Email Agent1@ks.com \* Hire Date 01/17/2012 \* Network Id Agent1  
 \* Status Active

Is a Harmony User ? ☒ Reset Password Release Lock

1 Reporting Profile 2 **Recording Rules** 3 User Feature Permissions 4 Report Feature Permissions

Voip Extensions and Recording Rules Add New Extension

	Extension	Enable Recording	Recording Type	No of Calls (Recording)	Enable Screen Capture	Screen Capture Type	No of Calls (Screen Capture)	Screen Capture Interval (in sec)	Call Type
Delete Extension	65881	<input checked="" type="checkbox"/>	Continuous	All	<input type="checkbox"/>	Continuous	All	5	All

Save Save & Add New Add New

## 7.7. Administer Virtual Recorders

Select the **Employee Management** tab. Click on **Go** to display a list of pre-configured employees in the left pane.

Select the entry corresponding to the first virtual recorder from the left pane, in this case “EXTN\_Agent1”, and the right pane is populated with pre-configured information for this virtual recorder.

The screenshot displays the Harmony Employee Management interface. The top navigation bar includes 'Administration', 'Organization', 'Work Type', 'Employee Management' (selected), 'Voice Configuration', 'Custom Groups', 'Message Thresholds', and 'Rules'. The 'Employee Management' section is active, showing a search bar with 'Employee Code' selected and a 'Go' button circled in red. Below the search bar is a table of employees:

Employee Code	Employee Name
002	Agent1
003	Agent2
004	Agent3
005	EXTN_Agent1
006	EXTN_Agent2
007	EXTN_Agent3
001	Supervisor

To the right of the table, the configuration for 'EXTN\_Agent1' is displayed. It includes fields for Employee Code (005), Employee First Name (EXTN\_Agent1), Employee Last Name (EXTN\_Agent1), Email (EXTN\_Agent1@ks.com), Status (Active), Alias (EXTN\_Agent1), Hire Date (01/17/2012), and Network Id (EXTN\_Agent1). There is also a 'Photo Upload' button and a 'Browse...' link. Below these fields is a section for 'Is a Harmony User?' with a checkbox and buttons for 'Reset Password' and 'Release Lock'. A progress bar shows four steps: 1. Reporting Profile, 2. Recording Rules, 3. User Feature Permissions, and 4. Report Feature Permissions. The 'Reporting Profile' section includes dropdowns for Location (My Site), Department (Operations), Designation (Agent), and Supervisor (Supervisor). The 'Report Feature Permissions' section includes a checkbox for 'Belongs To Client' (checked) and a dropdown for 'My Client'. At the bottom, there is a 'Client/Work Type' section with two tables: 'Client' and 'Work Type'. The 'Client' table has a checkbox for 'My Client' (checked). The 'Work Type' table has checkboxes for 'INBOUND [MYCLI]' and 'OUTBOUND [MYCLI]' (both checked).

Select step 2 **Recording Rules**, followed by **Add New Extension**.

For **Extension**, enter the first agent extension from **Section 3**. Check the **Enable Recording** field, and retain the default values in the remaining fields.

Repeat this section to configure all virtual recorders. In the compliance testing, two virtual recorders with employee codes of “005” and “006” were configured.

**Harmony** Powered by KnoahSoft

Jan 17, 2012 Admin (Administrator) - Help | About Us

**Administration**

Organization Work Type **Employee Management** Voice Configuration Custom Groups Message Thresholds Rules

**Employee Management**

Search By: Employee Code  
Look For:  (Go)

Employee Code	Employee Name
002	Agent1
003	Agent2
004	Agent3
005	EXTN_Agent1
006	EXTN_Agent2
007	EXTN_Agent3
001	Supervisor

Agent License - 2 / 900 Seat License - 2 / 300

Photo Upload  Browse...

IMAGE NOT FOUND

\* Employee Code: 005  
 \* Employee First Name: EXTN\_Agent1  
 \* Email: EXTN\_Agent1@ks.com  
 \* Status: Active

\* Alias: EXTN\_Agent1  
 Employee Last Name: EXTN\_Agent1  
 \* Hire Date: 01/17/2012  
 \* Network Id: EXTN\_Agent1

Is a Harmony User? ☐ Reset Password Release Lock

1 Reporting Profile 2 **Recording Rules** 3 User Feature Permissions 4 Report Feature Permissions

Voip Extensions and Recording Rules + Add New Extension

	Extension	Enable Recording	Recording Type	No of Calls (Recording)	Enable Screen Capture	Screen Capture Type	No of Calls (Screen Capture)	Screen Capture Interval (in sec)	Call Type
Delete Extension	65001	<input checked="" type="checkbox"/>	Continuous	All	<input type="checkbox"/>	Continuous	All	5	All

Save Save & Add New Add New

## 8. Verification Steps

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

### 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
<b>1</b>	<b>4</b>	<b>no</b>	<b>AES2-S8800</b>	<b>established</b>	<b>103</b>	<b>32</b>

Verify the registration status of the recording devices by using the “list registered-ip-stations” command. Verify that there is an entry for each virtual recorder from **Section 7.7**, with the client IP address of Application Enablement Services as **Station IP Address**, 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	
65001	1608	IP_Phone	y	20.32.39.105	
	1	1.3000		10.32.32.12	
<b>65001</b>	<b>1608</b>	<b>IP_API_A</b>	<b>y</b>	<b>10.32.32.66</b>	
	<b>1</b>	<b>3.2040</b>		<b>10.32.32.12</b>	
65002	1616	IP_Phone	y	20.32.39.108	
	1	1.3000		10.32.32.12	
<b>65002</b>	<b>1616</b>	<b>IP_API_A</b>	<b>y</b>	<b>10.32.32.66</b>	
	<b>1</b>	<b>3.2040</b>		<b>10.32.32.12</b>	



## 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 **Status** is “Talking”, and that **Associations** reflect the total number of skill groups and agent station extensions from **Section 3**.

**Application Enablement Services**  
Management Console

Welcome: User craft  
Last login: Wed Jan 18 09:58:25 2012 from 20.32.39.20  
HostName/IP: AES2-S8800/10.32.32.66  
Server Offer Type: VIRTUAL\_APPLIANCE  
SW Version: r6-1-1-30-0

Status | Status and Control | TSAPI Service SummaryHome | 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	1	Talking	Thu Jan 12 08:08:26 2012	Online	16	3	35	40	30

Online

Offline

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


TSAPI Service Status

TLink Status

User Status

Verify 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.

In the lower portion of the screen, verify that there is an active session with the Harmony user from **Section 6.8**, and that **# of Associated Devices** reflects the number of virtual recorders from **Section 7.7**.


**Application Enablement Services**  
Management Console

Welcome: User craft  
Last login: Wed Jan 18 09:58:25 2012 from 20.32.39.20  
HostName/IP: AES2-S8800/10.32.32.66  
Server Offer Type: VIRTUAL\_APPLIANCE  
SW Version: r6-1-1-30-0

Status | Status and Control | DMCC 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

### DMCC Service Summary - Session Summary

☐ Enable page refresh every 60 seconds

Session Summary [Device Summary](#)  
Generated on Thu Jan 19 13:08:06 EST 2012

Service Uptime: 43 days, 2 hours 4 minutes  
Number of Active Sessions: 1  
Number of Sessions Created Since Service Boot: 33  
Number of Existing Devices: 2  
Number of Devices Created Since Service Boot: 105

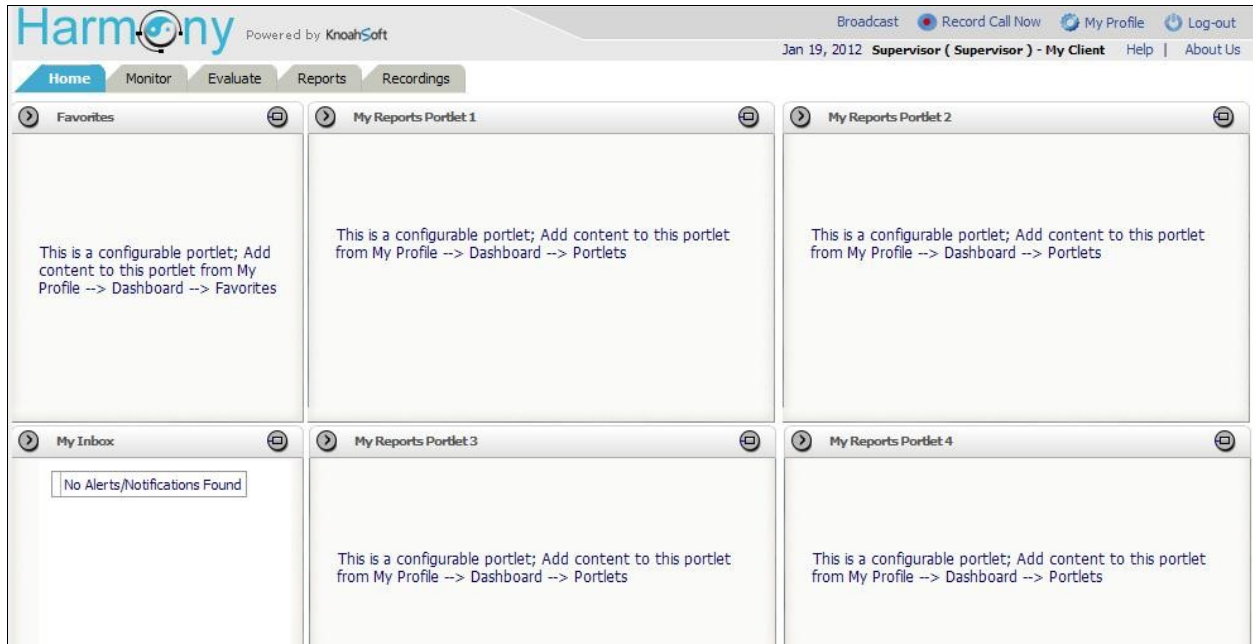
	Session ID	User	Application	Far-end Identifier	Connection Type	# of Associated Devices
<input type="checkbox"/>	E2FEAFF7DEB0BA7F2 61C4558B9DE648D-95	harmony	cmapiApplication	20.32.39.157	XML Unencrypted	2

Item 1-1 of 1

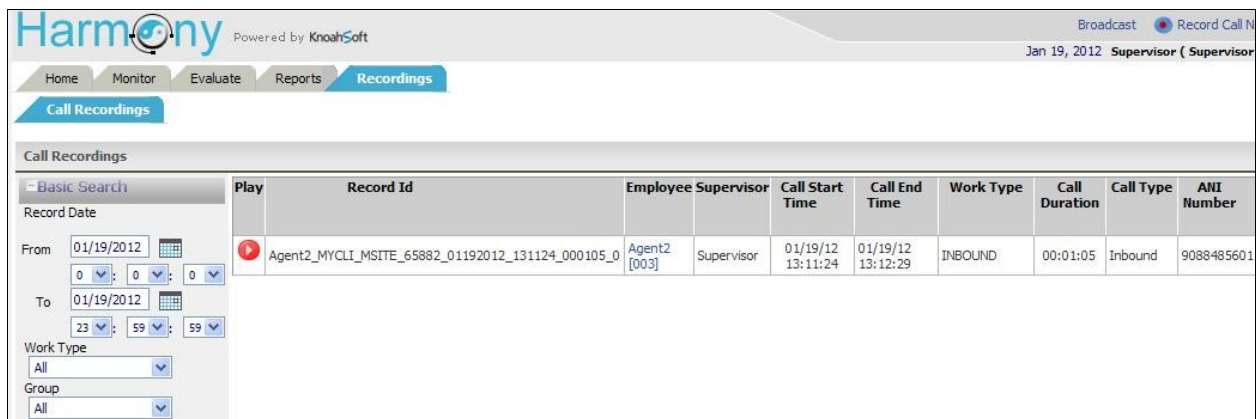
### 8.3. Verify KnochSoft Harmony

Log an agent into the skill group to handle and complete an ACD call. From the supervisor PC, follow the navigation in **Section 7.5** to launch the Harmony web interface, and log in with supervisor credentials. The **Harmony** screen is displayed.

Select the **Recordings** tab. In the subsequent screen (not shown), retain the default values and click **Search** in the left pane.



The Harmony screen is updated with a list of recordings for the current day. Verify that there is an entry reflecting the last call, with proper values in the relevant fields. Click on the associated icon in the **Play** column.



### Call Comments

[Submit](#)

### Previous Comments

Previous call comments doesn't exist.

---

### Customer Interaction

Start Time	01/19/2012 13:11:24
End Time	01/19/2012 13:12:29
Dialed In From(ANI)	9088485601
Dialed To(DNIS)	6137717521
Duration	00:01:05
Total No of Holds	0
Total Hold Time	00:00:00
Total No of Transfers	0
Total No of Conferences	0

### Segment Details

Record ID	Agent2_MYCLI_MSITE_65882_01192012_131124_000105_0
Start Time	01/19/2012 13:11:24
End Time	01/19/2012 13:12:29
Duration	00:01:05
Emp Code	003
Employee Name	Agent2
Extension	65882
Location	My Site
Group	SUPERVISOR_GROUP
Supervisor	Supervisor
Channel	Voice
Screen	No
Number of Holds	0
Total Hold Time	00:00:00
Transfer No	-


  

**Hold Details** [\*Calls with Zero or One Second Hold duration are not displayed]

Total Duration: 00:01:05

13:11
01:05

Agent2 [003]



Song: Agent2\_MYCLI\_MSITE\_65882\_01192012\_131124\_000105\_0

Harmony

## 9. Conclusion

These Application Notes describe the configuration steps required for KnoahSoft Harmony to successfully interoperate with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services using the Multiple Registration method. All feature and serviceability test cases were completed with observations noted in **Section 0**.

## 10. Additional References

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

1. *Administering Avaya Aura™ Communication Manager*, Document 03-300509, Issue 6.0, Release 6.0, June 2010, available at <http://support.avaya.com>.
2. *Avaya Aura® Application Enablement Services Administration and Maintenance Guide*, Release 6.1, Issue 2, February 2011, available at <http://support.avaya.com>.
3. *KnoahSoft Harmony Administration Guide*, Version 3.4, available on the Harmony server as part of installation.
4. *KnoahSoft Harmony Enterprise Edition User Guide*, Version 3.4, available on the Harmony server as part of installation.

---

**©2012 Avaya Inc. All Rights Reserved.**

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya DevConnect Program at [devconnect@avaya.com](mailto:devconnect@avaya.com).