



Avaya Solution & Interoperability Test Lab

Application Notes for ASC telecom MARATHON EVOLUTION Voice Recorder with Avaya Aura™ Communication Manager and Avaya Aura™ Application Enablement Services Using Trunk Side Monitoring – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for ASC telecom MARATHON EVOLUTION voice recorder to interoperate with Avaya Aura™ Communication Manager using Avaya Aura™ Application Enablement Services. ASC telecom MARATHON EVOLUTION voice recorder is a call recording solution. In the compliance testing, ASC telecom MARATHON EVOLUTION voice recorder used the Telephony Services Application Programming Interface from Avaya Aura™ Application Enablement Services to monitor stations on Avaya Aura™ Communication Manager, and used passive monitoring of the PSTN trunk to capture the media associated with the monitored stations for call recording.

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

Table of Contents

1.	Introduction.....	3
1.1.	Interoperability Compliance Testing	3
1.2.	Support.....	3
2.	Reference Configuration.....	4
3.	Equipment and Software Validated	5
4.	Configuration	6
4.1.	Configure Avaya Aura™ Communication Manager	6
4.1.1.	Verify system-parameters customer-options	6
4.1.2.	Configure Interface to Avaya Aura™ Application Enablement Services	8
4.1.3.	Configure Stations	9
4.1.4.	Configure Hunt Group	10
4.2.	Configure Avaya Aura™ Application Enablement Services	11
4.3.	Configure MARATHON EVOLUTION Server.....	21
4.3.1.	Configure ASC DataManager.....	21
4.3.2.	Configure ASC RIA Server	29
5.	General Test Approach and Test Results.....	38
6.	Verification Steps.....	38
7.	References.....	41
8.	Conclusion	41

1. Introduction

These Application Notes describe the configuration used to enable the ASC telecom MARATHON EVOLUTION voice recording server to interoperate with Avaya Aura™ Communication Manager, and Avaya Aura™ Application Enablement Services.

1.1. Interoperability Compliance Testing

The following tests were performed as part of the compliance testing:

- The following test scenarios were used to test the various MARATHON EVOLUTION features:
 - Basic call
 - Hold/retrieve
 - Transfer / Blind transfer
 - Conferencing
 - Call forwarding
 - Hunt group calls
 - Calls to/from bridged appearances
- MARATHON EVOLUTION's robustness was tested by verifying its ability to recover from interruptions to its external connections including:
 - The LAN connection between MARATHON EVOLUTION and the network
 - The LAN connection between RI*Apassive* and the network
 - The connection of the PBX to the network
- MARATHON EVOLUTION's robustness was further tested by verifying ability to recover from power interruptions to the following components:
 - The MARATHON EVOLUTION server
 - The RI*Apassive* server
 - The Communication Manager used by MARATHON EVOLUTION.

1.2. Support

Support for ASC telecom MARATHON EVOLUTION is available at:

ASC telecom AG
Seibelstrasse 2-4
63768 Hoesbach
Germany
Phone +49 6021 5001-0
Fax +49 6021 5001-310
E-Mail hq@asctelecom.com
<http://www.asctelecom.com>

The following diagram shows the configuration used for conformance testing.

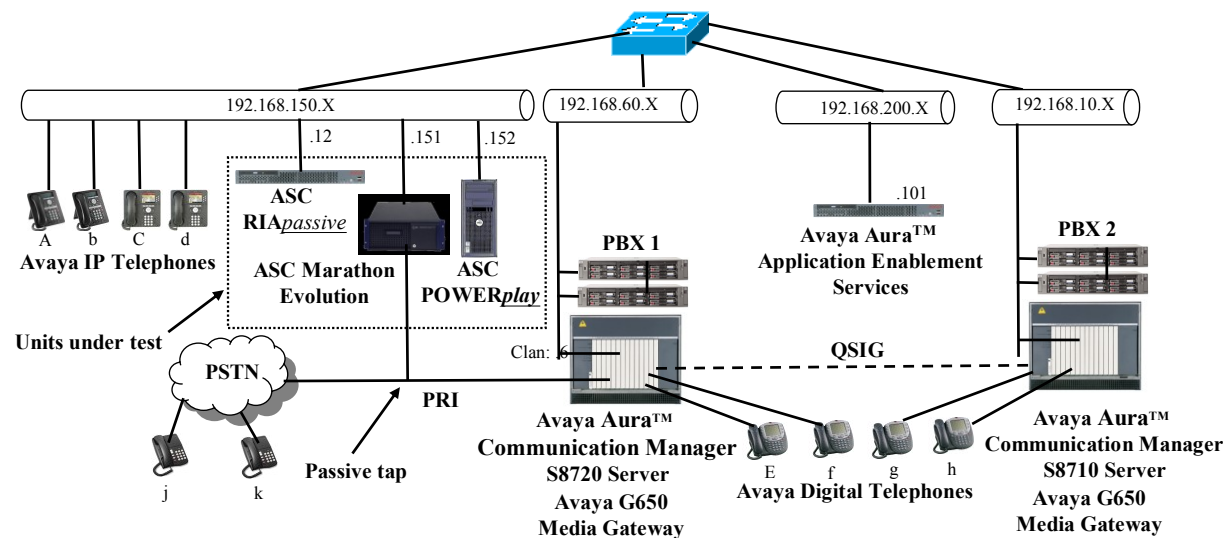


Figure 1: MARATHON EVOLUTION Reference Configuration

In the above diagram, the ASC MARATHON EVOLUTION records voice conversations from telephones attached to PBX 1. The speech recorder is attached to the PSTN PRI trunk via a passive tap. The ASC RIA passive receives events from the Avaya Aura™ Application Enablement Services server when the state of calls associated with PBX 1 change, and informs the MARATHON EVOLUTION of these transitions. The TSAPI service provided by Application Enablement Services is used to monitor call activity associated with PBX 1.

PBX 2 is included in the configuration solely to test the ability to monitor conversations which traverse a trunk to a networked PBX. The stations attached to PBX 2 are not monitored by ASC MARATHON EVOLUTION. The PBX 2 system is attached to PBX 1 via an IP/QSIG trunk, and is used as a networked PBX system. This allows remote networked telephones (g, h) to be included in the test.

The ASC POWER_{play} client provides playback and administration for voice files.

The telephones depicted in these Application Notes are designated by an upper case letter if configured to be monitored by the MARATHON EVOLUTION voice recorder. A lower case letter designates those terminals which have been configured to not be monitored or are possibly unable to be monitored.

The following table contains additional information about each of the telephones shown in **Figure 1**. A “*” in the “Monitored” column indicated that the telephone is monitored by the MARATHON EVOLUTION voice recorder.

Phone	Monitored	Model	Extension
A	*	Avaya 1616	60071
b		Avaya 1608	60062
C	*	Avaya 9640G	60093
d		Avaya 9630G	60184
E	*	Avaya 2410	60007
f		Avaya 2410	60008
g		Avaya 2420	10007
h		Avaya 2420	10008
j		N/A	069 xxxx 6176
k		N/A	069 xxxx 6630
L		Hunt Group (A & C)	61000

Table 1: Device Monitor Configuration

3. Equipment and Software Validated

Software Component	Version
Avaya Aura™ Communication Manager	5.2.1 R015x.02.1.016.4 Patch: 17774
Avaya TN2312BP IP SERVER INTEFC	HW11/FW049
Avaya TN799DP CONTROL-LAN	HW01/FW032
Avaya TN2302AP IP MEDIA PROCESSOR	HW20/FW120
Avaya 1608 IP Telephone	1.2.11
Avaya 1616 IP Telephone	1.2.11
Avaya 9630G IP Telephone	H.323 / 3.1
Avaya 9640G IP Telephone	H.323 / 2.4.2
Avaya Aura™ Application Enablement Services	5.2
ASC Marathon Evolution SW	9.0
ASC RIA _{passive}	6.0
ASC RIA _{passive} platform OS	Microsoft XP SP3
ASC POWER _{play}	9.0
ASC POWER _{play} platform OS	Microsoft XP SP3

Table 2: Hardware/Software Component Versions

4. Configuration

The configuration information in this section covers only PBX 1 – the system to which the MARATHON EVOLUTION voice recorder is attached.

4.1. Configure Avaya Aura™ Communication Manager

The configuration and verification operations illustrated in this section were all performed using the Communication Manager System Administration Terminal (SAT) via SSH port 5022.

The information provided in this section describes the configuration of Communication Manager for this solution. For all other provisioning information such as installation and configuration, please refer to the product documentation in references [1] and [2].

4.1.1. Verify system-parameters customer-options

Use the **display system-parameters customer options** command to verify that Communication Manager is configured to meet the minimum requirements to run MARATHON EVOLUTION. Those items shown in **bold** indicate required values or minimum capacity requirements associated with the system license. If these are not met in the configuration, please contact an Avaya representative for further assistance.

Parameter	Usage
Maximum Concurrently Registered IP Stations (p.2)	This must be sufficient to support the total number of IP stations.
IP Stations? (p.4)	This parameter must be set to “y”.
IP_Phone (p.10)	This parameter must be set the number of IP stations.

Table 3: System-Parameters Customer-Options Parameters

display system-parameters customer-options		Page 2 of 11
OPTIONAL FEATURES		
IP PORT CAPACITIES		USED
Maximum Administered H.323 Trunks:	1000	70
Maximum Concurrently Registered IP Stations:	18000	6
Maximum Administered Remote Office Trunks:	0	0
Maximum Concurrently Registered Remote Office Stations:	0	0
Maximum Concurrently Registered IP eCons:	10	0
Max Concur Registered Unauthenticated H.323 Stations:	0	0
Maximum Video Capable H.323 Stations:	0	0
Maximum Video Capable IP Softphones:	1000	0
Maximum Administered SIP Trunks:	1000	255
Maximum Administered Ad-hoc Video Conferencing Ports:	0	0
Maximum Number of DS1 Boards with Echo Cancellation:	10	0
Maximum TN2501 VAL Boards:	10	1
Maximum Media Gateway VAL Sources:	0	0
Maximum TN2602 Boards with 80 VoIP Channels:	128	1
Maximum TN2602 Boards with 320 VoIP Channels:	128	0
Maximum Number of Expanded Meet-me Conference Ports:	0	0

Figure 2: System-Parameters Customer-Options Screen, p. 2

display system-parameters customer-options

Page 4 of 11

OPTIONAL FEATURES

Emergency Access to Attendant? y

Enable 'dadmin' Login? y

Enhanced Conferencing? y

Enhanced EC500? y

Enterprise Survivable Server? n

Enterprise Wide Licensing? n

ESS Administration? n

Extended Cvg/Fwd Admin? y

External Device Alarm Admin? n

Five Port Networks Max Per MCC? n

Flexible Billing? n

Forced Entry of Account Codes? n

Global Call Classification? n

Hospitality (Basic)? y

Hospitality (G3V3 Enhancements)? n

IP Trunks? y

IP Attendant Consoles? y

IP Stations? y

ISDN Feature Plus? n

ISDN/SIP Network Call Redirection? y

ISDN-BRI Trunks? y

ISDN-PRI? y

Local Survivable Processor? n

Malicious Call Trace? n

Media Encryption Over IP? n

Mode Code for Centralized Voice Mail? n

Multifrequency Signaling? y

Multimedia Call Handling (Basic)? n

Multimedia Call Handling (Enhanced)? n

Multimedia IP SIP Trunking? n

Figure 3: System-Parameters Customer-Options Screen, p. 4

display system-parameters customer-options

Page 10 of 11

MAXIMUM IP REGISTRATIONS BY PRODUCT ID

Product ID	Rel. Limit	Used
IP_API_A	: 1000	0
IP_API_B	: 1000	0
IP_API_C	: 1000	0
IP_Agent	: 1000	0
IP_IR_A	: 1000	0
IP_Phone	: 12000	4
IP_ROMax	: 12000	0
IP_Soft	: 1000	0
IP_eCons	: 128	0
oneX_Comm	: 12000	0

Figure 4: System-Parameters Customer-Options Screen p. 10

4.1.2. Configure Interface to Avaya Aura™ Application Enablement Services

Use the **change ip-services** command to configure the interface to the Application Enablement Services server, as shown in the following table.

Parameter	Usage
Service Type (p.1)	Enter “AESVCS”.
Enabled (p.1)	Enter “y” to enable the service.
Local Node (p.1)	Enter the IP node name for the CLAN interface.
Local Port (p.1)	Enter “8765”.
AE Services Server (p.4)	Enter the name that was assigned to the Application Enablement Services server when it was installed.
Password (p.4)	Enter the password that was assigned to the switch connection, as shown in Figure 16 .
Enabled (p.4)	Enter “y” to enable the connection.

Table 4: IP Services Parameters

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

Figure 5: IP Services Screen, p. 1

change ip-services				Page	4 of	4
AE Services Administration						
Server ID	AE Services Server	Password	Enabled	Status		
1:	aes-server1	XXXXXXXXXXXXXXXXXX	y	in use		

Figure 6: IP Services Screen, p. 4

Use the **add cti-link** command to add a CTI link for use by TSAPI. The link number can be any value between 1 and 64 which is not currently assigned to another link. The link number specified must be the same value that is used in the “Switch CTI Link Number” field shown in **Figure 19**. Use an unused extension as the value for the “Extension” parameter. The value chosen for the “Name” parameter is a matter of personal preference.

change cti-link 4		Page 1 of 3	
CTI LINK			
CTI Link: 4			
Extension: 69996			
Type: ADJ-IP			
		COR: 1	
Name: AES-devcon223-tsapi			

Figure 7: Cti-link Screen

4.1.3. Configure Stations

Use the **add station** command to create a station for each of the IP phones listed in **Table 1**, using the values shown in the following table.

Parameter	Usage
Extension	Use an unused extension which is compatible with the dial plan.
Type	Use a type value which corresponds to the physical station to be used.
Name	Any alphanumeric string can be assigned as an extension name, which is used for identification purposes.
Security Code	Enter an appropriate numeric string to be used as a security code.

Table 5: Configuration IP Stations

add station 60071		Page 1 of 5
STATION		
Extension: 60071	Lock Messages? n	BCC: 0
Type: 1616	Security Code: 123456	TN: 1
Port: S00123	Coverage Path 1:	COR: 1
Name: extn 60071	Coverage Path 2:	COS: 1
	Hunt-to Station:	
STATION OPTIONS		
	Time of Day Lock Table:	
Loss Group: 19	Personalized Ringing Pattern: 1	
	Message Lamp Ext: 60071	
Speakerphone: 2-way	Mute Button Enabled? y	
Display Language: english	Button Modules: 0	
Survivable GK Node Name:		
Survivable COR: internal	Media Complex Ext:	
Survivable Trunk Dest? y	IP SoftPhone? n	
	Customizable Labels? y	

Figure 8: IP Station Screen

4.1.4. Configure Hunt Group

Use the **add hunt-group** command to create a hunt group which is used to test the ability of MARATHON EVOLUTION to monitor hunt groups. Assign an unused extension to the hunt group. Add extensions for telephones “A” and “C” to the hunt group, which are assigned to IP phones which are monitored by MARATHON EVOLUTION.

Parameter	Usage
Group Name	Any alphanumeric string can be used as a Group Name.
Group Extension	Use an unused extension which is compatible with the dial plan.
MEMBER ASSIGNMENTS	Add the extensions which are to be assigned to this hunt group to this list. For this test, extensions 60071 and 60093 are used.

Table 6: Configuration IP Stations

add hunt-group 4	Page 1 of 60
HUNT GROUP	
Group Number: 4	ACD? n
Group Name: asc	Queue? n
Group Extension: 61000	Vector? n
Group Type: ucd-mia	Coverage Path:
TN: 1	Night Service Destination:
COR: 1	MM Early Answer? n
Security Code:	Local Agent Preference? n
ISDN/SIP Caller Display:	

Figure 9: Hunt Group Screen, p. 1

add hunt-group 4	Page 3 of 60
HUNT GROUP	
Group Number: 4	Group Extension: 61000
Group Type: ucd-mia	
Member Range Allowed: 1 - 1500	Administered Members (min/max): 1 /2
Total Administered Members: 2	
GROUP MEMBER ASSIGNMENTS	
Ext	Name(19 characters)
1: 60071	extn 60071
2: 60093	extn 60093
3:	
4:	
5:	
6:	
7:	
8:	
9:	
10:	
11:	
12:	
13:	
At End of Member List	

Figure 10: Hunt Group Screen, p. 3

4.2. Configure Avaya Aura™ Application Enablement Services

The Application Enablement Services server is configured via a web browser by accessing the following URL:

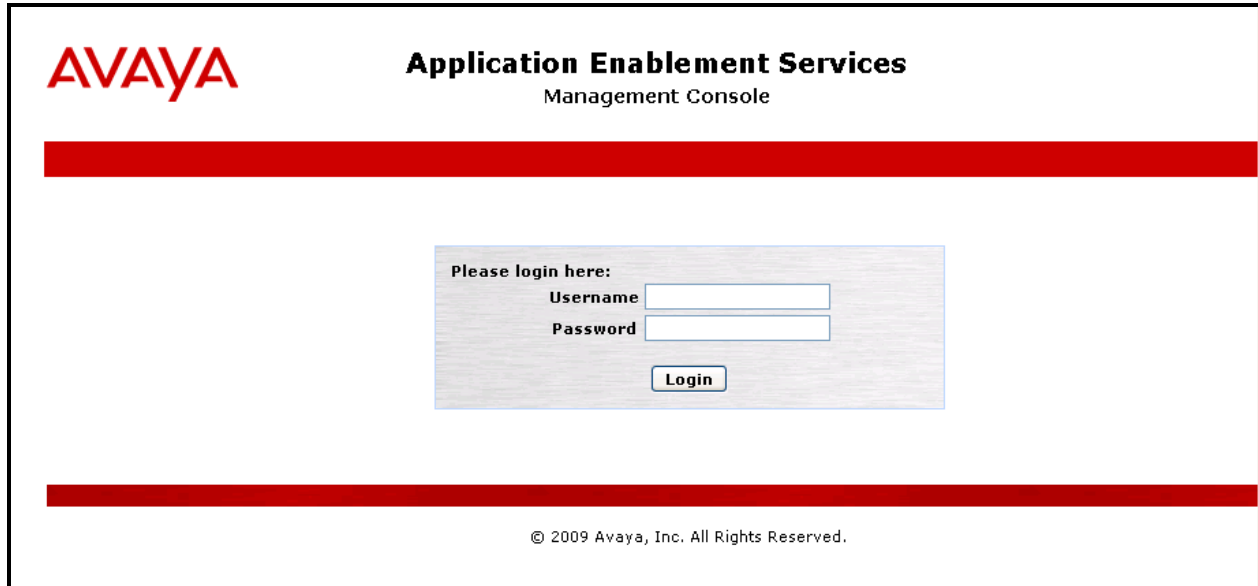
http://<AES server address>/

Click “Continue To Login”.



Figure 11: Avaya Aura™ Application Enablement Services Welcome Screen

Once the login screen appears, enter the credentials for performing administrative activities.

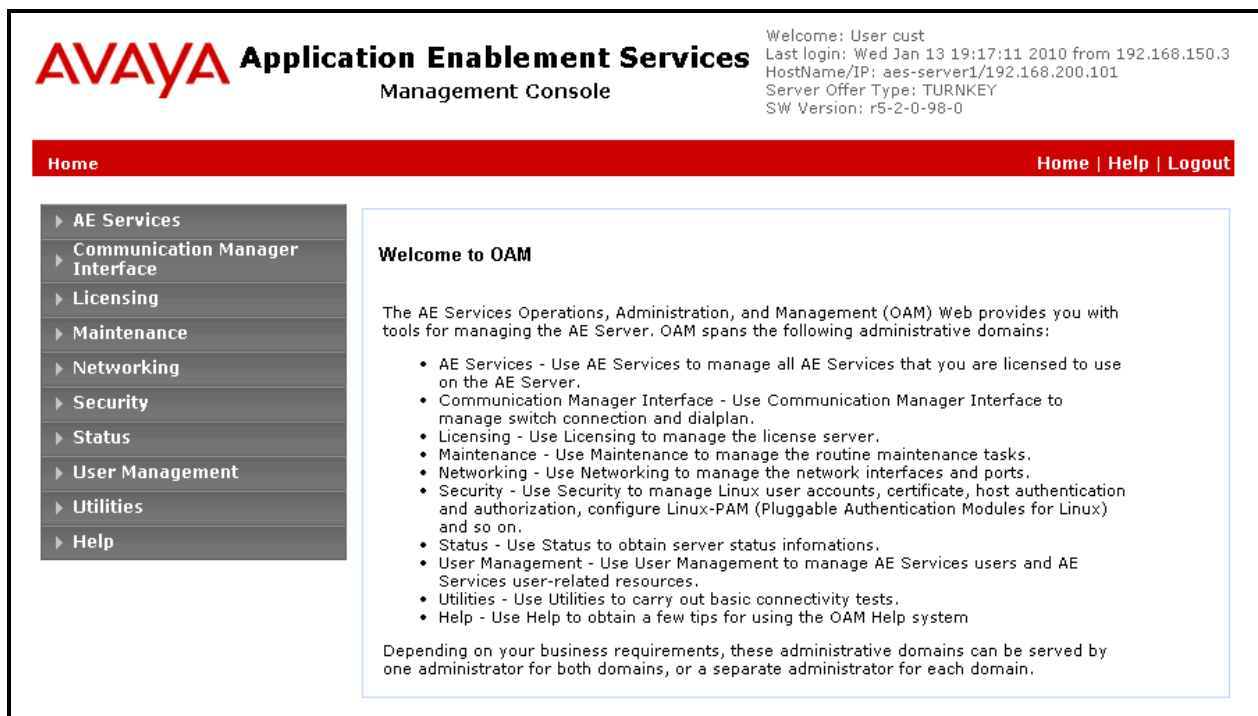


The login screen features the Avaya logo in red at the top left. To its right, the text "Application Enablement Services" is displayed in bold, with "Management Console" underneath it. A thick red horizontal bar spans the width of the page below the header. In the center, a light gray box contains the login form. The form is titled "Please login here:" and includes two input fields: "Username" and "Password". Below these fields is a "Login" button. Another thick red horizontal bar is located at the bottom of the page, just above the copyright notice.

© 2009 Avaya, Inc. All Rights Reserved.

Figure 12: Avaya Aura™ Application Enablement Services Login Screen

Click “AE Services” in left frame.



The main screen displays the Avaya logo and "Application Enablement Services Management Console" at the top. On the right side, a welcome message is shown: "Welcome: User cust", "Last login: Wed Jan 13 19:17:11 2010 from 192.168.150.3", "HostName/IP: aes-server1/192.168.200.101", "Server Offer Type: TURNKEY", and "SW Version: r5-2-0-98-0". Below the header, a red navigation bar contains "Home", "Help", and "Logout" links. On the left, a vertical menu lists various services: "AE Services", "Communication Manager Interface", "Licensing", "Maintenance", "Networking", "Security", "Status", "User Management", "Utilities", and "Help". The main content area, titled "Welcome to OAM", explains that the OAM Web provides tools for managing the AE Server and lists the administrative domains: AE Services, Communication Manager Interface, Licensing, Maintenance, Networking, Security, Status, User Management, Utilities, and Help. It also notes that these domains can be managed by one administrator for both or separate administrators for each.

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 both domains, or a separate administrator for each domain.

Figure 13: Avaya Aura™ Application Enablement Services Main Screen

Verify that the Application Enablement Services server installation has a TSAPI service license. If this is not the case, please contact an Avaya representative regarding licensing.


Application Enablement Services
Management Console

Welcome: User cust
Last login: Mon Jan 18 15:53:03 2010 from 192.168.150.3
HostName/IP: aes-server1/192.168.200.101
Server Offer Type: TURNKEY
SW Version: r5-2-0-98-0

AE Services
[Home](#) | [Help](#) | [Logout](#)

AE Services

- CVLAN
- DLG
- DMCC
- SMS
- TSAPI
- Communication Manager Interface
- Licensing
- Maintenance
- Networking
- Security
- Status
- User Management
- Utilities
- Help

AE Services

IMPORTANT: AE Services must be restarted for administrative changes to fully take effect. Changes to the Security Database do not require a restart.

Service	Status	State	License Mode	Cause*
ASAI Link Manager	N/A	Running	N/A	N/A
CVLAN Service	OFFLINE	Running	N/A	N/A
DLG Service	ONLINE	Running	NORMAL MODE	N/A
DMCC Service	ONLINE	Running	NORMAL MODE	N/A
TSAPI Service	ONLINE	Running	NORMAL MODE	N/A
Transport Layer Service	N/A	Running	N/A	N/A

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


* -- For more detail, please mouse over the Cause, you'll see the tooltip, or go to help page.

License Information

You are licensed to run Application Enablement (CTI) version 5.0

Figure 14: Avaya Aura™ Application Enablement Services Top Level Screen

Navigate to **Communication Manager Interface ->Switch Connections**. Enter the name of the Switch Connection to be added, and click on the “Add Connection” button.


Application Enablement Services
Management Console

Welcome: User cust
Last login: Wed Jan 13 19:17:11 2010 from 192.168.150.3
HostName/IP: aes-server1/192.168.200.101
Server Offer Type: TURNKEY
SW Version: r5-2-0-98-0

Communication Manager Interface | Switch Connections
Home | Help | Logout

▶ AE Services
▼ Communication Manager Interface
Switch Connections
▶ Dial Plan
▶ Licensing
▶ Maintenance
▶ Networking
▶ Security
▶ Status
▶ User Management
▶ Utilities
▶ Help

Switch Connections

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections
<input checked="" type="radio"/> S8500	No	30	0
<input type="radio"/> S8710	No	30	1

Figure 15: Switch Connection Screen

This causes the following screen to be presented. At this point, enter the screen fields as described in the following table, and click the “Apply” button.

Parameter	Usage
Switch Password	The Switch Password must be the same as was entered into the Communication Manager AE Services Administration form via the “change ip-services” command, described in Figure 6 . Passwords must consist of 12 to 16 alphanumeric characters
SSL	SSL (Secure Socket Layer) is enabled by default. Keep the default setting unless you are adding a Switch Connection for a DEFINITY Server CSI

Table 7: Configuration of Switch Password

AVAYA Application Enablement Services Management Console

Welcome: User cust
Last login: Wed Jan 13 19:17:11 2010 from 192.168.150.3
HostName/IP: aes-server1/192.168.200.101
Server Offer Type: TURNKEY
SW Version: r5-2-0-98-0

Communication Manager Interface | Switch Connections [Home](#) | [Help](#) | [Logout](#)

Navigation Menu:

- ▶ AE Services
- ▼ Communication Manager Interface
 - Switch Connections
 - ▶ Dial Plan
- ▶ Licensing
- ▶ Maintenance
- ▶ Networking
- ▶ Security
- ▶ Status
- ▶ User Management
- ▶ Utilities
- ▶ Help

Connection Details - S8720

Switch Password

Confirm Switch Password

Msg Period Minutes (1 - 72)

SSL ☒

Processor Ethernet ☐


Figure 16: Set Switch Password Screen

From the **Communication Manager Interface->Switch Connections** screen, click the “Edit CLAN IPs” button to display the screen show below. Enter the IP address of the CLAN which Application Enablement Services is to use for communication with the switch, and click the “Add Name or IP” button.

The screenshot displays the Avaya Application Enablement Services Management Console. At the top left is the Avaya logo and the text 'Application Enablement Services Management Console'. At the top right, a welcome message reads: 'Welcome: User cust', 'Last login: Wed Jan 13 19:17:11 2010 from 192.168.150.3', 'HostName/IP: aes-server1/192.168.200.101', 'Server Offer Type: TURNKEY', and 'SW Version: r5-2-0-98-0'. Below this is a red navigation bar with 'Communication Manager Interface | Switch Connections' on the left and 'Home | Help | Logout' on the right. A left-hand menu contains several options: 'AE Services', 'Communication Manager Interface' (expanded), 'Switch Connections' (highlighted), 'Dial Plan', 'Licensing', 'Maintenance', 'Networking', 'Security', 'Status', 'User Management', 'Utilities', and 'Help'. The main content area is titled 'Edit CLAN IPs - S8720' and contains a text input field with the value '192.168.60.6' and a button labeled 'Add Name or IP'.

Figure 17: CLAN Screen

On the left margin of the screen, navigate to **Administration-> AE Services ->TSAPI Links**.
The following screen is displayed. Click the “Add Link” button.


Application Enablement Services
Management Console

Welcome: User cust
Last login: Wed Jan 13 19:17:11 2010 from 192.168.150.3
HostName/IP: aes-server1/192.168.200.101
Server Offer Type: TURNKEY
SW Version: r5-2-0-98-0

AE Services | TSAPI | TSAPI Link
Home | Help | Logout

▼ AE Services

▶ CVLAN

▶ DLG

▶ DMCC

▶ SMS

▼ TSAPI

▪ TSAPI Links

▪ TSAPI Properties

▶ Communication Manager Interface

▶ Licensing

▶ Maintenance

▶ Networking

▶ Security

▶ Status

▶ User Management

▶ Utilities

▶ Help

TSAPI Links

Link	Switch Connection	Switch CTI Link #	ASAI Link Version	Security
1	S8710	4	5	Unencrypted
2	S8500	4	UNKNOWN	Unencrypted

Add Link
Edit Link
Delete Link

Figure 18: TSAPI Links Screen

Fill in the parameters for the link to be added. The “Link” parameter must be a value between 1 and 16 which is not assigned to another link. The “Switch Connection” parameter should be the name of the Avaya Server which is to be controlled by this link. The value for the TSAPI “Switch CTI Link Number” must be a value between 1 and 64, and must be the same as was used in the Communication Manager “add cti-link” configuration command in **Figure 7**. Click the “Apply Changes” button.

The screenshot displays the Avaya Application Enablement Services Management Console. The top header includes the Avaya logo and the text 'Application Enablement Services Management Console'. A welcome message for user 'cust' is shown in the top right corner, along with login details. A red navigation bar contains links for 'AE Services | TSAPI | TSAPI Link', 'Home | Help | Logout'. The left sidebar shows a tree view with 'AE Services' expanded, containing 'CVLAN', 'DLG', 'DMCC', 'SMS', 'TSAPI' (selected), and 'Communication Manager Interface'. Under 'TSAPI', 'TSAPI Links' is selected. The main content area is titled 'Add TSAPI Links' and contains the following form fields: 'Link' (text input with value '1'), 'Switch Connection' (dropdown menu with value 'S8720'), 'Switch CTI Link Number' (dropdown menu with value '4'), 'ASAI Link Version' (dropdown menu with value '4'), and 'Security' (dropdown menu with value 'Unencrypted'). At the bottom of the form are two buttons: 'Apply Changes' and 'Cancel Changes'.

Figure 19: Add TSAPI Link Screen

Navigate to **User Management -> User Admin -> Add User**.

The “CT User” field for this user must be set to “Yes”. In this case, the Application Enablement Services user is the ASC RIA Server, which uses Application Enablement Services to monitor stations. The “User Id” and “User Password” must be the same as those configured for ASC DataManager in **Figure 33**.

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 with system information. A red navigation bar contains links for 'User Management', 'User Admin', 'List All Users', 'Home', 'Help', and 'Logout'. On the left, a sidebar menu lists various system functions, with 'User Management' expanded to show 'User Admin' options. The main content area is titled 'Add User' and contains a form with the following fields: * User Id (text box with 'asc'), * Common Name (text box with 'asc'), * Surname (text box with 'Marathon'), User Password (text box), Confirm Password (text box), Admin Note (text box), Avaya Role (dropdown menu with 'None' selected), Business Category (text box), Car License (text box), CM Home (text box), Cms Home (text box), CT User (dropdown menu with 'Yes' selected), Department Number (text box), Display Name (text box), Employee Number (text box), Employee Type (text box), Enterprise Handle (text box), and Given Name (text box).

Figure 20: Add User Screen

Navigate to **Administration -> Security Database -> CTI Users -> List All Users**, and then click “Edit User” for the newly added user “asc”. Enable “Unrestricted Access” and click “Apply Changes”.

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 'cust' along with login details. A red navigation bar contains links for 'Security | Security Database | CTI Users | List All Users' and 'Home | Help | Logout'.

On the left is a sidebar menu with categories: AE Services, Communication Manager Interface, Licensing, Maintenance, Networking, and Security. Under Security, the 'Security Database' is expanded, showing options like Control, CTI Users (selected), Search Users, Devices, Device Groups, and Tlinks. Under CTI Users, 'List All Users' is selected.

The main content area is titled 'Edit CTI User' and shows the configuration for user 'asc'. The 'User Profile' section includes fields for User ID (asc), Common Name (asc), Worktop Name (NONE), and Unrestricted Access (checked). Below this, the 'Call Origination and Termination / Device Status' is set to None. The 'Call and Device Monitoring' section has Device (None), Call / Device (None), and Call (unchecked). The 'Routing Control' section has Allow Routing on Listed Devices (None). At the bottom are 'Apply Changes' and 'Cancel Changes' buttons.

Figure 21: Edit CTI User Screen

4.3. Configure MARATHON EVOLUTION Server

The ASC MARATHON EVOLUTION Voice Recorder has an integrated web server and can be configured remotely via a web browser by selecting its IP address as the target URL from the browser. Selection of this URL causes the following to be displayed.

4.3.1. Configure ASC DataManager

Select the **ASC DataManager** application from the left frame

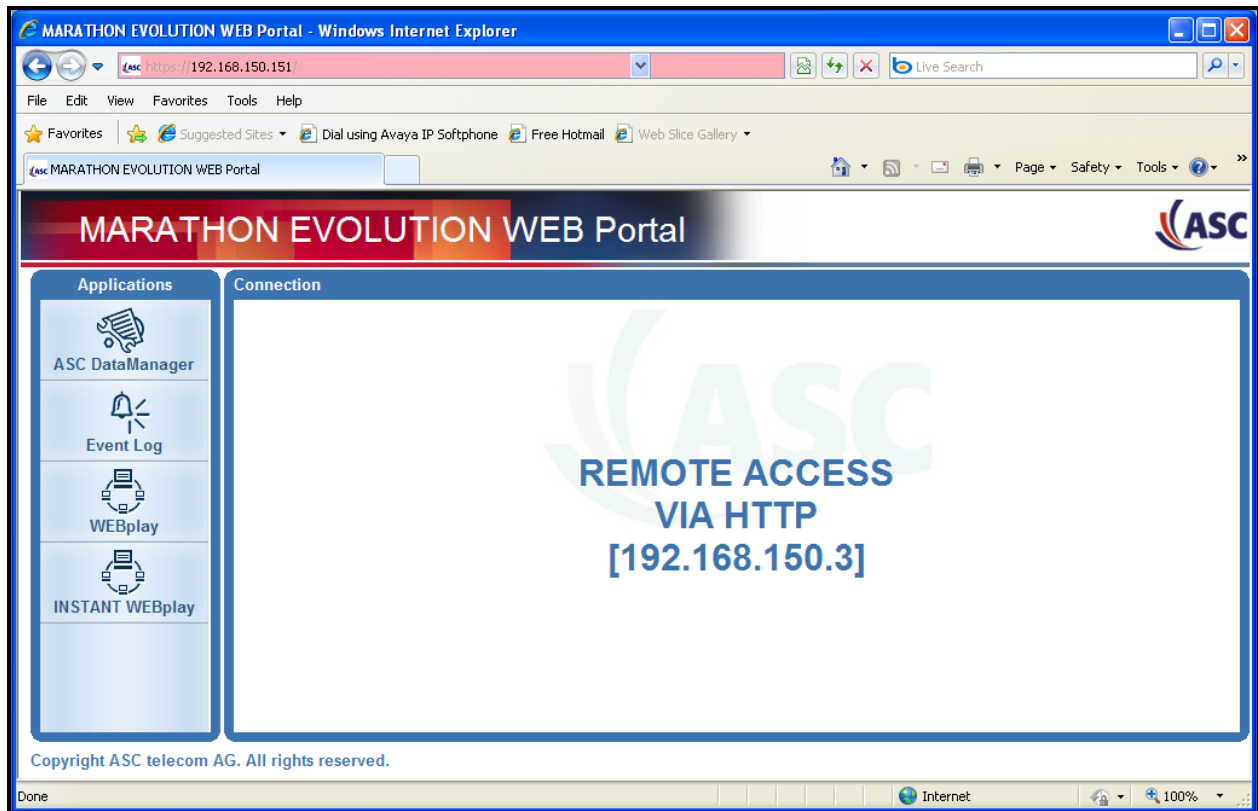


Figure 22: MARATHON EVOLUTION Welcome Screen

Enter appropriate user credentials and hit the “enter” key.



Figure 23: DataManager Login Screen

Click to expand the “ASC DataManager” -> “Configuration” -> “System” menu item in the left frame of the screen.



Figure 24: DataManager Welcome Screen

Expand the “RIA” menu point from the left frame, and select the *RIApasive* menu point. Set the *RIApasive* parameters as described in the following table, and click the “Save” button.

Parameter	Usage
NumInstances	Set this parameter to “1”.
Enabled	Set this parameter to “Yes”.
Name	Enter an appropriate name to identify the monitoring instance.
LogLevel	Enter “Medium”.

Table 8: DataManager *RIApasive* Parameters

The screenshot shows the 'ASC DataManager' interface. On the left is a navigation tree with categories like 'User Administration', 'Configuration', 'System', 'Alarm Notifications', 'Channels', 'EVOip channels', 'EVOip active channels', 'RIA', 'RIActive', 'RIApasive' (selected), 'DevConnect', 'RIAtagger', 'Auto Tagging', 'Channel Guard', 'Recording Planner', 'Recording Decision Preview', 'Recorder Information (OAGC)', 'Archive Client', 'SDDM Client', 'Database', 'Registry', and 'Information'. The main panel is titled 'RIApasive' and contains a 'Configuration' tab. Below the tab is a table with columns: State, Name, Description, and Value(s). The table lists several parameters, including 'Licensed', 'NumInstances', 'Enabled', 'Name', and 'LogLevel'. The 'NumInstances' parameter is set to '1', 'Enabled' is set to 'Yes', 'Name' is set to 'DevConnect', and 'LogLevel' is set to 'Medium'.

State	Name	Description	Value(s)
	Licensed	Shows if you have a license for RIApasive	Yes
	NumInstances	The number of RIApasive instances	1
Instances			
DevConnect			
	Enabled	Enables or disables this RIApasive-instance	Yes
	Name	The name for this RIApasive-instance	DevConnect
	LogLevel	The log level for this RIApasive-instance	Medium

Figure 25: DataManager *RIApasive* Configuration Screen

Click on the name of the *RIAPassive* monitoring instance created in the previous step in the left frame of the screen, and enter configuration parameters as shown in the following table into the “Protocol-Interface” tab.

Parameter	Usage
Statemachine	Select “RIAServerTagging” from the drop-down menu.
EventBuffer	Select “No buffering” from the drop-down menu.
PIF-Type	Select “PIFAvayaCM” from the drop-down menu.
Mode	Select “Start, stop and tag” from the drop-down menu.
Connection-Type	Select “TCP” from the drop-down menu.
Server-IP	Enter the address of the <i>RIAPassive</i> server, as shown in Figure 1 .
Server-Port	Enter the port value of 9000.
Inactivity-Timeout	Enter “30”.
LogBinaryData	Select “No” from the drop-down menu.

Table 9: Configuration IP Stations

ASC DataManager

DevConnect

Protocol-Interface

Devices

State	Name	Description	Value(s)
	Statemachine	The statemachine grammar to use for this RIAPassive-Connection	RIAserverTagging
	EventBuffer	The buffer size for events.	No buffering
	PIF-Type	The protocol interface adapter to use for this RIAPassive-Connection	PIFAvayaCM
	Mode	Should the PIF be used to detect start/stop and/or taggings	Start, stop and tag
<div>PIF-Config</div> <div>Connection</div>			
	Connection-Type	The connection type to use.	TCP
	Server-IP	The ip address to connect to.	192.168.150.12
	Server-Port	The port to use for the connection.	9000
	Inactivity-Timeout	Close connections after this duration of inactivity. Unit is seconds, '0' means no inactivity timeout.	30
	LogBinaryData	Log the incoming binary data	No

Figure 26: DataManager RIAPassive Instance Protocol-Interface Screen

Select the “Devices” tab, and double-click on each of the entries shown in the table, and enter the configuration parameters as shown in **Figure 28**.

ASC DataManager

DevConnect

Protocol-Interface **Devices**

State	Name	Description	Value(s)
	DeviceMap		
	<input type="button" value="Import from CSV"/> <input type="button" value="Export to CSV"/>		
	PhonelineID	PhysicalPbxID	PhysicalDeviceID
	Channel 001	0	6
	Channel 002	0	7
	Channel 003	0	8
	Channel 004	0	9
	Channel 005	0	10
	Channel 006	0	11
	Channel 007	0	12
	Channel 008	0	13
	Channel 009	0	14
	Channel 010	0	15
	Channel 011	0	16
	Channel 012	0	17
	Channel 013	0	18
	Channel 014	0	19
	Channel 015	0	20
	Channel 016	0	21
	Channel 017	0	22
	Channel 018	0	23
	Channel 019	0	24
	Channel 020	0	25
	Channel 021	0	26
	Channel 022	0	27
	Channel 023	0	28
	Channel 024	0	29
	Channel 025	0	30
	Channel 026	0	31
	Channel 027	0	32
	Channel 028	0	33
	Channel 029	0	34
	Channel 030	0	35

Figure 27: DataManager RI~~Active~~ Instance Devices Screen

Configure the channels with the parameters shown in the following table.

Parameter	Usage
RecordStartMode	Select “RIA_CONNECT” from the drop-down menu.
StorageMode	Select “EXTERN_DELETE” from the drop-down menu.
InputSource1	Select “COMMAN (Analog / PCM30)” from the drop-down menu.
InputType1	Select “PRI_PASSIVE_INCOMING_TIMESLOT”.
InputSlot1	Enter “1” (for the first channel, 2 for the second and so on...). There is a gap for the 16 th and 31 th channel, as these are the D-channels from the PRI line.

Table 10: DataManager Channel Configuration Parameters

The screenshot displays the 'Channels' configuration window in the DataManager application. The window title is 'Channels' and it includes a toolbar with icons for information, print, save, and other functions. Below the title bar, there is a table showing the status of channels (Channel 001 and Channel 002) with columns for State, ChannelDescription, and ChannelID. The main area is titled 'Configuration of Channel 001' and contains a list of parameters for configuration. Each parameter has a 'State' column, a 'Name' column, a 'Description' column, and a 'Value(s)' column with a '(De-/Select all)' link. The parameters are: RecordStartMode (Start recording by: DTMF-SEQUENCE, RING, RIA_ALERTING, RIA_CONNECT), RecordStopMode (Stop recording by: (Use the triggers from recording start), HOST, VOX, COR), StorageMode (Recording mode: EXTERN_DELETE), VoxLevel (Threshold value for sensitivity of signal detection: 20 dB), Timespan_Until_Deletion (Time to keep a call in the database: 00:00:00:00:00), CLIEnable (Enable CLI detection: No), DTMFEnable (Enable DTMF detection: No), PreTrigger (PreTrigger to use by record start: 20), Compression (Compression to use for audio data: PCM_A_LAW), VoxPostTime (Minimum duration for silence before recording stop: 79), VoxTimeMin (Minimum signal duration before recording start: 1000 ms), IdlePostTime (Minimum duration for silence before recording stop: 19), IdleTimeMin (Minimum signal duration before recording start: 1000 ms), PackageTimeout (Time to wait before call packages get finally processed: 100), AGCEnable (Enable AGC mode: Enabled (Mono)), ActiveHook (Take and record analog PBX-conference calls: Off), BeepToneEnable (Beep tone insertion: Off), AnalogGain (Gain for analog lines: 0 dB), AGCRaiseTime1 (AGC raise time for the first input channel: 608 ms), AGCMaxGain1 (AGC maximum gain for the first input channel: 41 dB), InputSource1 (Type of recording interface: COMMAN (Analog / PCM30)), InputType1 (Signal Input: PRI_PASSIVE_INCOMING_TIMESLOT), InputSlot1 (The time slot number of the recording interface: 1), InputSource2 (Type of correspondent recording interface: COMMAN (Analog / PCM30)), InputType2 (The input type of the second input source: PRI_PASSIVE_OUTGOING_TIMESLOT), InputSlot2 (The time slot number of the correspondent recording interface: 1), and Availability (This channel is physically available: Yes).

Figure 28: DataManager Channel Configuration Screen

4.3.2. Configure ASC RIA Server

Enter the URL of the RIA Server into a web browser, and click “RIA Server Configurator”.



Figure 29: RIA Server Welcome Screen

Enter appropriate user credentials and hit the “enter” key.

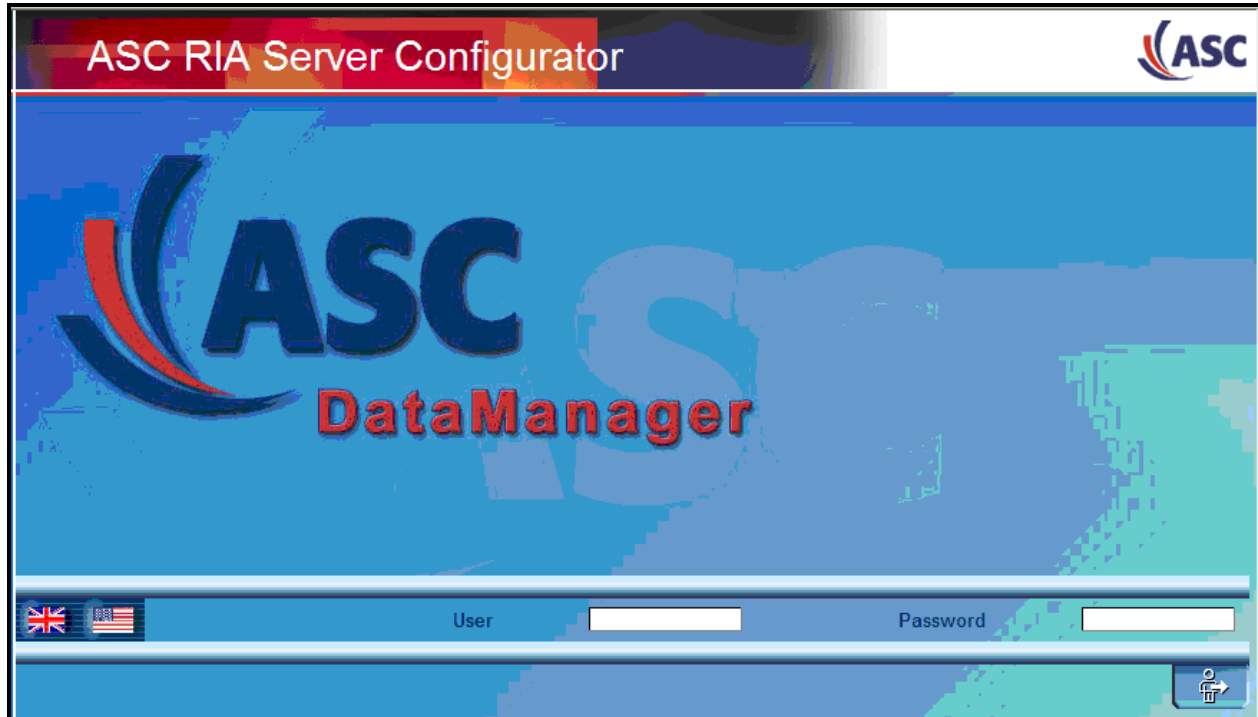


Figure 30: ASC RIA Server Login Screen

Select the “AvayaCM”, enter the name of the monitoring instance which was created in **Figure 25**, and hit the “enter” key.



Figure 31: RIA Server PBX Instance Creation Screen

Expand the “Avaya CM” menu point in the left frame of the screen, select the “Class of recording” menu item, and enter the parameters shown in the following table.

Parameter	Usage
Recording type	Select “Trunk Side” from the drop-down menu.
RIA server role	Select “Active” from the drop-down menu.
Recording mode	Select “Automatic” from the drop-down menu.
Class of channel	Select “Class of Channel 1” from the drop-down menu.
Display feedback	Select “no” from the drop-down menu.
Description	Enter a descriptive comment to describe this item.

Table 11: RIA Server Class of Recording Parameters

ASC RIA Server Configurator

Class of recording configuration

ID	Description
5	Standard class of recording for Avaya

Details

Class of recording configuration

Recording type: Trunk Side

RIA server role: Active

Recording mode: Automatic

Class of channel: Class of Channel 1

Display feedback: no

Description: Standard class of recording for Ave

Figure 32: RIA Server Class of Recording Screen

Click on the name of the PBX instance which was created in **Figure 25** in the left frame of the screen and enter the parameters shown in the following table.

Parameter	Usage
PBX Name	Enter the name of the recording instance which was created in Figure 25 .
Hostname	Enter the name composed of the elements shown in Table 13 separated by “#” characters.
Port	Enter “1”.
Login	Enter the user name which was created in Figure 20 .
Password	Enter the user name which was assigned in Figure 20 .

Table 12: RIA Server PBX Instance Configuration Parameters

Parameter	Value
AVAYA	This is a fixed value.
S8720	This is the name that was assigned to the switch connection which was assigned to the PBX within the Switch Connection screen shown in Figure 15 of this document.
CSTA	This is a fixed value.
AES-SERVER1	This is the name that was assigned to the Application Enablement Services server when it was installed. This name is contained in the ip-services screen, shown in Figure 6 .

Table 13: Hostname Parameter Components

The screenshot shows the 'ASC RIA Server Configurator' application. The title bar reads 'ASC RIA Server Configurator'. Below it, a blue header bar says 'Avaya CM PBX (DevConnect) configuration'. The main content area is titled 'PBX configuration' and contains the following fields:

- PBX Name: DevConnect
- Country code: 1
- Hostname: AVAYA#S8720#CSTA#AES-SERV
- Area code: 1
- Port: 1
- Net code: 1
- Login: asc
- PBX ID: 9
- Password: (masked with dots)

The left sidebar shows a tree view with the following items: ASC RIA Server Conf, User Administration, Avaya CM, RIA connection, Class of recording, DevConnect (selected), Extensions, Trunk channels, Silent monitor int, Buttons, Overview, and Text.

Figure 33: RIA Server PBX Instance Configuration Screen

Click “Extensions” under the PBX instance menu point in the left frame. Select one of the unused items in the list.

ASC RIA Server Configurator

Extension (DevConnect) configuration

Extension number	pbx	Monitorpoint
9,1	DevConnect	No
9,2	DevConnect	No
9,3	DevConnect	No
9,4	DevConnect	No
9,5	DevConnect	No
9,6	DevConnect	No
9,7	DevConnect	No
9,8	DevConnect	No
9,9	DevConnect	No
9,10	DevConnect	No
9,11	DevConnect	No
9,12	DevConnect	No
9,13	DevConnect	No

Details

Extension configuration

PBX ID:

Extension type:

Language:

Class of recording:

ExtensionNumber:

Persi name:

Note:

Extension number:

Range: -

Overwrite existing: ☐

Set only monitor enabled value: ☐

Copy to extension number(s)

Monitorpoint enabled:

Schedule active monitor: ☐

From: to:

Figure 34: RIA Server Extensions Screen

Enter the parameters shown in the following table. Repeat this for each of the extensions in the list.

Parameter	Usage
Extension type	Select “Extension” from the drop-down menu.
Language	Select “en_GB” from the drop-down menu for English.
Class of recording	Select “Standard class of recording for...” from the drop-down menu.
ExtensionNumber	Enter the number of a station which is to be recorded from Table 1 .
Monitorpoint enabled	Select “Yes” from the drop-down menu.

Table 14: RIA Server Extension Configuration Parameters

ASC RIA Server Configurator

Extension (DevConnect) configuration

Extension Number	Extension Type	Monitorpoint enabled
9,20	DevConnect	No
9,21	DevConnect	No
9,22	DevConnect	No
9,23	DevConnect	No
9,24	DevConnect	No
9,25	DevConnect	No
9,26	DevConnect	No
9,27	DevConnect	No
9,28	DevConnect	No
9,29	DevConnect	No
9,30	DevConnect	No
80071	DevConnect	Yes
80093	DevConnect	Yes
80007	DevConnect	Yes

Details

Extension configuration

PBX ID: 3

Extension type: Extension

Language: en_GB

Class of recording: Standard class of recording for

ExtensionNumber: 80071

Persi name:

Note:

Extension number: []

Range: [] - []

Overwrite existing: ☐

Set only monitor enabled value: ☐

Copy to extension number(s)

Monitorpoint enabled: yes

Schedule active monitor: ☐

From: 01/01/1990 00:00:00 to 01/01/1990 00:00:00

Assigned Buttons
no buttons assigned!

Figure 35: RIA Server Extension Configuration Screen

Click “Trunk channels” under the PBX instance menu point in the left frame. Select one of the unused items in the list.

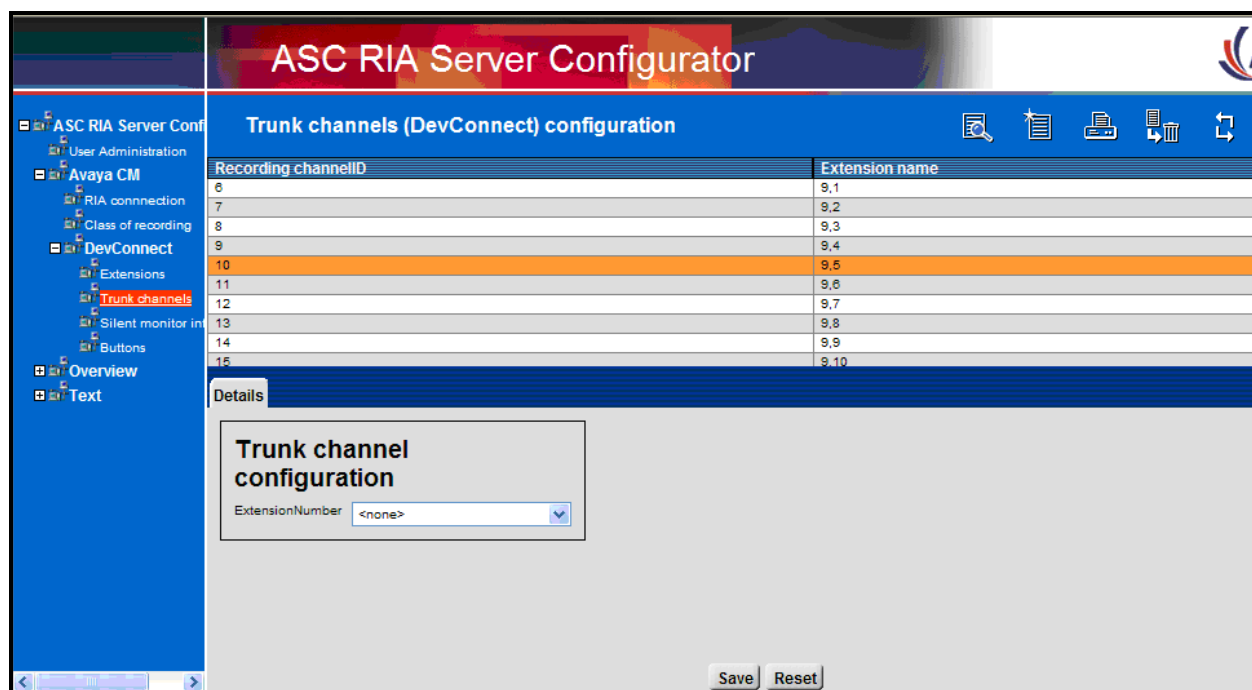


Figure 36: RIA Server Channel Configuration Screen

For each of the “Recording channels” shown in the “Trunk channels” list, select a channel. Use the “Trunk channel configuration ExtensionNumber” drop-down menu to assign an unused extension designation. Repeat this for all of the Trunk channels in the list.

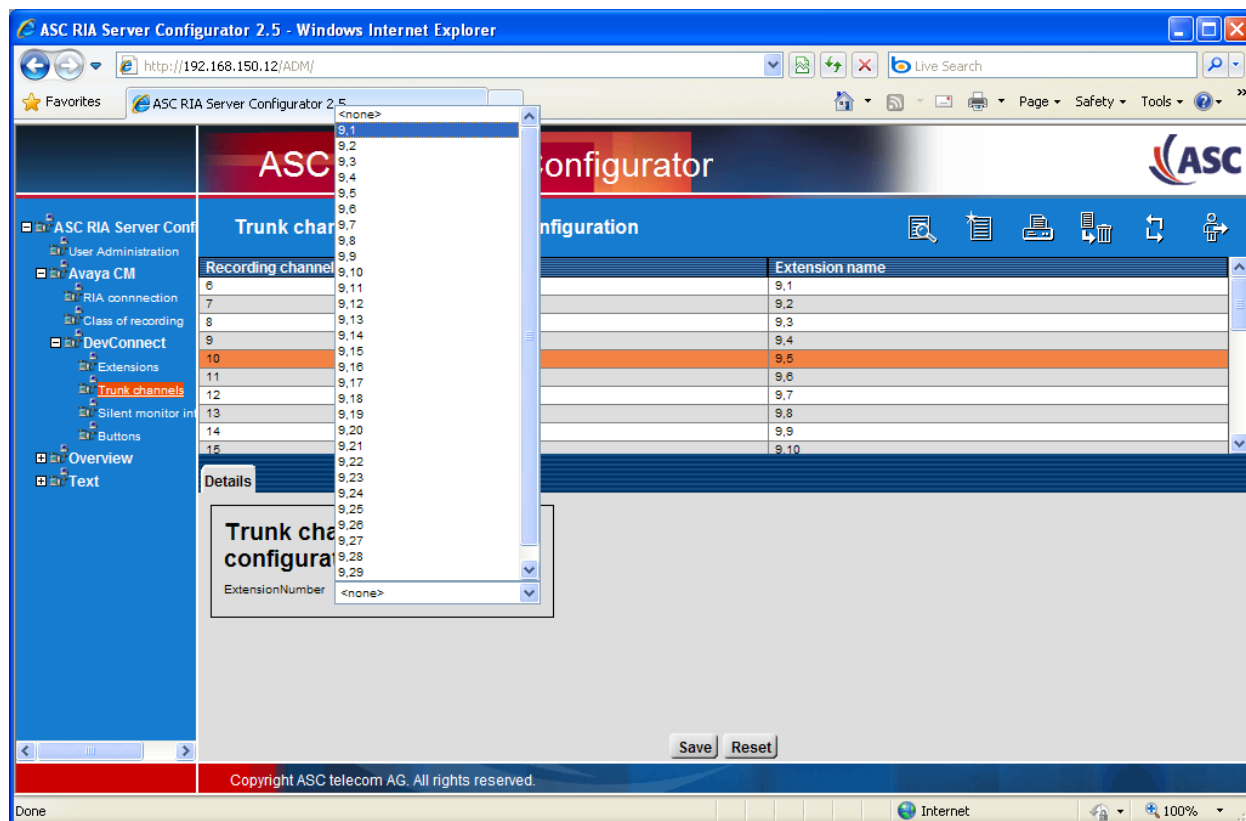


Figure 37: RIA Server Channel Assignment Screen

5. General Test Approach and Test Results

The compliance testing was performed manually. The tests were all functional in nature, and no performance testing was done. The test method employed can be described as follows:

- Communication Manager was configured to support various local IP telephones, as well as a networked PBX connection and a PSTN connection.
- A PSTN interface was attached to Communication Manager, which was used to communicate with external telephones.
- The MARATHON EVOLUTION was configured to monitor various telephones and trunks attached to Communication Manager.
- The major MARATHON EVOLUTION features and functions were verified using the above-mentioned local and external telephones, including the ability to record calls made to and from
 - Locally attached IP and digital telephones
 - Telephones attached to the PSTN via E1 trunk
 - Telephones attached to a networked PBX via QSIG trunk

The tests which were performed are shown in **Section 1.1**. All tests which were performed produced the expected result.

6. Verification Steps

The correct installation and configuration of MARATHON EVOLUTION voice recorder can be verified by performing the following steps using the SAT terminal from PBX 1.


- Use the “status aesvcs cti-link” command to verify that the TSAPI link allocated in **Figure 7** is “established”.

```
status aesvcs cti-link
```

AE SERVICES CTI LINK STATUS						
CTI Link	Version	Mnt Busy	AE Services Server	Service State	Msgs Sent	Msgs Rcvd
1		no		down	0	0
2		no		down	0	0
3		no		down	0	0
4	4	no	aes-server1	established	15	15

Figure 38: Status Aesvcs Cti-link Screen

- Login to Avaya Aura™ Application Enablement Services, and navigate to the “AE Services” screen. Verify that the TSAPI Service is licensed, ONLINE, and Running.


Application Enablement Services
Management Console

Welcome: User cust
Last login: Mon Jan 18 15:53:03 2010 from 192.168.150.3
HostName/IP: aes-server1/192.168.200.101
Server Offer Type: TURNKEY
SW Version: r5-2-0-98-0

AE Services
Home | Help | Logout

▼ AE Services

- ▶ CVLAN
- ▶ DLG
- ▶ DMCC
- ▶ SMS
- ▶ TSAPI
- ▶ Communication Manager Interface
- ▶ Licensing
- ▶ Maintenance
- ▶ Networking
- ▶ Security
- ▶ Status
- ▶ User Management
- ▶ Utilities
- ▶ Help

AE Services

IMPORTANT: AE Services must be restarted for administrative changes to fully take effect. Changes to the Security Database do not require a restart.

Service	Status	State	License Mode	Cause*
ASAI Link Manager	N/A	Running	N/A	N/A
CVLAN Service	OFFLINE	Running	N/A	N/A
DLG Service	ONLINE	Running	NORMAL MODE	N/A
DMCC Service	ONLINE	Running	NORMAL MODE	N/A
TSAPI Service	ONLINE	Running	NORMAL MODE	N/A
Transport Layer Service	N/A	Running	N/A	N/A

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


* -- For more detail, please mouse over the Cause, you'll see the tooltip, or go to help page.

License Information

You are licensed to run Application Enablement (CTI) version 5.0

Figure 39: Avaya Aura™ Application Enablement Services AE Services Screen

- Navigate to “Status” → “Status and Control” → “Switch Conn Summary” select the PBX 1, and click “Switch Connection Details”. Verify that the connection state is “Online” and “Talking”.



**Application Enablement
Services**
Management Console


Welcome: User cust
Last login: Fri Jan 15 21:27:32 2010 from 192.168.150.3
HostName/IP: aes-server1/192.168.200.101
Server Offer Type: TURNKEY
SW Version: r5-2-0-98-0

Status | Status and Control | Switch Conn 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**

Switch Connection Details - S8720

☐ Enable page refresh every 60 seconds

	Hostname or IP Address	Connection State	Online/Offline	Since	Msgs To Switch	Msgs From Switch	Msg Period
	192.168.60.6	Talking	Online	Thu Jan 14 17:51:54 2010	616	631	30

Online Offline Message Period Back

Figure 40: Application Enablement Services Switch Connection Details Screen

- Navigate to “Status” → “Status and Control” → “TSAPI Service Summary” and click “Details” for “TSAPI Service”. Verify that the TSAPI service for PBX 1 is “Online” and “Talking”.

Application Enablement Services
Management Console

Welcome: User cust
Last login: Fri Jan 15 21:27:32 2010 from 192.168.150.3
HostName/IP: aes-server1/192.168.200.101
Server Offer Type: TURNKEY
SW Version: r5-2-0-98-0

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	S8720	4	Talking	Thu Jan 14 17:51:54 2010	Online	15	4	15	15	30
	2	S8500	4	Switch Down	Wed Jan 13 19:14:32 2010	Online	15	0	0	0	30
	3	S8710	4	Talking	Wed Jan 13 19:14:32 2010	Online	15	0	15	15	30

Figure 41: TSAPI Link Details Screen

7. References

- [1] *Administering Avaya Aura™ Communication Manager*, May 2009, Document Number 03-300509.
- [2] *Avaya Aura™ Communication Manager Feature Description and Implementation*, May 2009, Issue 7, Document Number 555-245-205.
- [3] *Avaya Aura™ Application Enablement Services Administration and Maintenance Guide*, November 2009, Document Number 02-300357
- [4] ASC telecom product descriptions: http://www.asctelecom.com/english/index_e.html

8. Conclusion

These Application Notes describe the conformance testing of the ASC telecom MARATHON EVOLUTION voice recorder with Communication Manager. The passive tap recording method offered by the MARATHON EVOLUTION was tested. A detailed description of the configuration required for both the Avaya and the ASC telecom equipment is documented within these Application Notes. The MARATHON EVOLUTION passed all of the tests performed, which included both functional and robustness tests.

©2010 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.