



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

---

# **Application Notes for ASC telecom MARATHON EVOLUTION Voice Recorder with Avaya Communication Manager Using Single Step Conferencing – Issue 1.1**

### **Abstract**

These Application Notes describe the conformance testing of the ASC telecom MARATHON EVOLUTION voice recorder with Avaya Communication Manager using the Single Step Conferencing feature. These Application Notes contain an extensive description of the configurations for both MARATHON EVOLUTION and Avaya Communication Manager which were used for testing. The testing which was performed tested the major functions of the MARATHON EVOLUTION product.

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

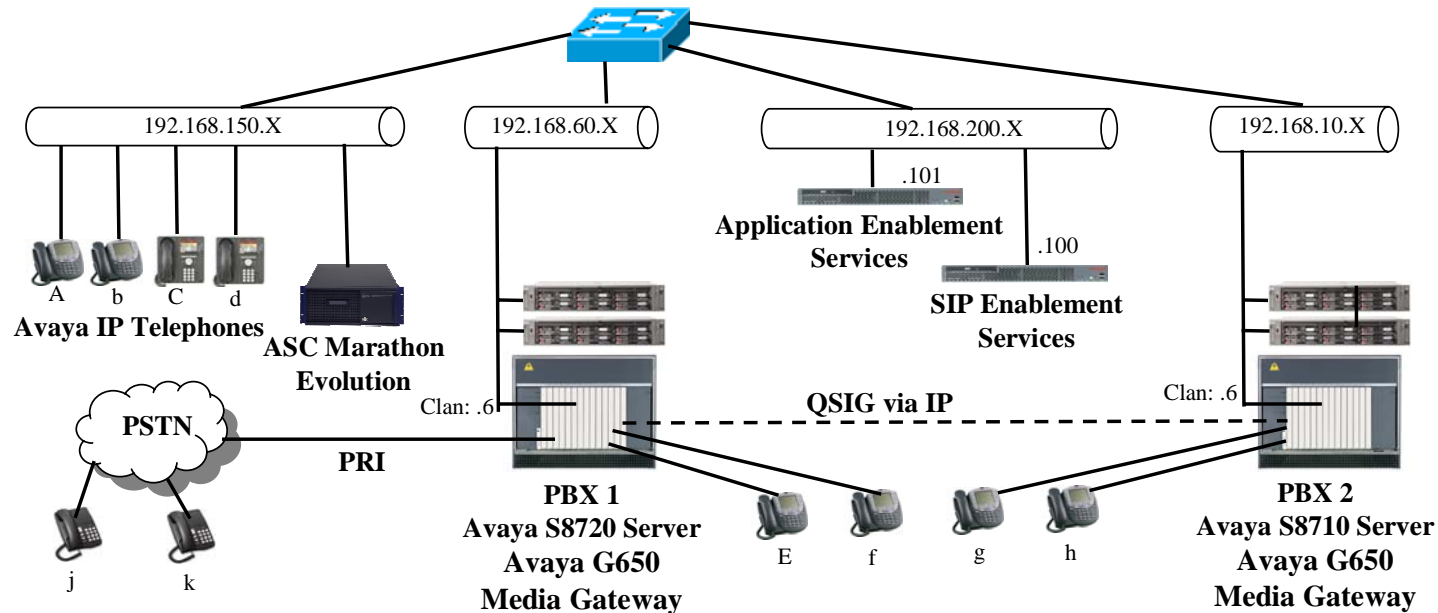
1.	Introduction.....	5
2.	Equipment and Software Validated .....	7
3.	Configuration .....	7
3.1.	Configure Avaya Communication Manager.....	7
3.1.1.	Verify system-parameters customer-options .....	8
3.1.2.	Configure Dial Plan .....	10
3.1.3.	Configure IP Network Interface.....	10
3.1.4.	Configure Interface to AES .....	12
3.1.5.	Configure Stations .....	14
3.1.5.1	Configure H.323 IP Stations .....	14
3.1.5.2	Configure SIP Stations.....	15
3.1.5.3	Configure Virtual CTI Stations.....	17
3.1.6.	Configure Hunt Group .....	18
3.1.7.	Configure Interface to SIP Enablement Services.....	19
3.2.	Configure Avaya AES .....	22
3.3.	Avaya SIP Enablement Services.....	30
3.3.1.	Install License .....	31
3.3.2.	Setup Dataservice.....	35
3.3.3.	Setup SIP Domain.....	36
3.3.4.	Add Media Server Interface.....	38
3.3.5.	Add Hosts.....	39
3.3.6.	Add Users.....	40
3.4.	Configure MARATHON EVOLUTION Server.....	42
3.5.	Configure Marathon RIA <i>active</i> .....	56
4.	Interoperability Compliance Testing .....	61
4.1.	General Test Approach .....	61
4.2.	Test Results .....	62
5.	Verification Steps.....	62
6.	Support.....	62
7.	References.....	63
8.	Conclusion .....	63
9.	Change History .....	63
Figure 1: MARATHON EVOLUTION Test Configuration .....		5
Figure 2: System-Parameters Customer-Options Screen (p.2) .....		8
Figure 3: System-Parameters Customer-Options Screen (p.3) .....		9
Figure 4: System-Parameters Customer-Options Screen (p.4) .....		9
Figure 5: System-Parameters Customer-Options Screen (p.10) .....		9
Figure 6: Dialplan Analysis Screen .....		10
Figure 7: Node-Names IP Screen .....		10
Figure 8: IP-Network-Region Form, p.2.....		11
Figure 9: IP-Codec-Set Form.....		12
Figure 10: IP Services Screen, p. 1 .....		12

Figure 11: IP Services Screen, p. 4 .....	12
Figure 12: CTI-link Screen .....	13
Figure 13: IP Station Screen .....	14
Figure 14: SIP IP Stations Screen .....	15
Figure 15: SIP Off-Pbx-Telephone Station-Mapping Screen, p. 1 .....	16
Figure 16: SIP Off-Pbx-Telephone Station-Mapping Screen, p. 2 .....	16
Figure 17: Virtual CTI Station Screen .....	17
Figure 18: Hunt Group Screen, p. 1 .....	18
Figure 19: Hunt Group Screen, p. 3 .....	18
Figure 20: Signaling-Group Form .....	19
Figure 21: Trunk-Group Form, p.1 .....	20
Figure 22: off-pbx-telephone station-mapping Screen, p.1 .....	21
Figure 23: off-pbx-telephone station-mapping Screen, p.2 .....	21
Figure 24: AES Welcome Screen .....	22
Figure 25: AES CTI OAM Welcome Screen .....	23
Figure 26: Switch Connection Screen.....	24
Figure 27: Set Switch Password Screen.....	25
Figure 28: CLAN Screen .....	26
Figure 29: TSAPI Links Screen.....	26
Figure 30: Add TSAPI Link Screen.....	27
Figure 31: Add User Screen.....	28
Figure 32: AES Port Configuration .....	29
Figure 33: Launch Maintenance Web Interface Screen.....	30
Figure 34: Select License from Top SES Screen.....	31
Figure 35: Select WebLM from License Screen.....	32
Figure 36: WebLM Login Screen .....	33
Figure 37: Initiate “Setup” from Top SES Configuration Screen.....	34
Figure 38: Initiate “Setup Dataservice” from Top Setup Screen.....	35
Figure 39: “Setup Master Administration” Screen .....	36
Figure 40: “Setup SIP Domain” Screen.....	36
Figure 41: System Properties Screen .....	37
Figure 42: SES Add Media Server Interface Screen .....	38
Figure 43: SES Add Host Screen.....	39
Figure 44: SES Add User Screen.....	40
Figure 45: SES Add Media Server Extension Screen.....	41
Figure 46: MARATHON EVOLUTION Welcome Screen.....	42
Figure 47: DataManager Welcome Screen .....	43
Figure 48: DataManager Select AvayaInterface Mode .....	44
Figure 49: DataManager AvayaInterface Operation Mode .....	45
Figure 50: DataManager AvayaInterface Communication Manager.....	46
Figure 51: DataManager AES Server Interface Screen .....	47
Figure 52: DataManager Softphones Screen .....	48
Figure 53: DataManager Recorder Screen.....	49
Figure 54: Select EVOip Screen .....	50
Figure 55: DataManager EVOip Calldata Screen.....	51
Figure 56: DataManager Channels Screen .....	52

Figure 57: EVOip Channel Configuration Screen .....	52
Figure 58: DataManager RIAactive Screen .....	53
Figure 59: DataManager RIAactive_1 Protocol Interface Screen .....	54
Figure 60: DataManager RIAactive_1 Devices Screen .....	55
Figure 61: RIAactive Login Screen .....	56
Figure 62: RIAactive PBX Configuration Screen .....	57
Figure 63: RIAactive Extension Configuration Screen .....	58
Figure 64: RIAactive Silent Monitor Configuration Screen.....	59
Figure 65: RIAactive Server Port Screen.....	60

# 1. Introduction

These Application Notes describe the configuration used to enable the ASC telecom MARATHON EVOLUTION voice recording server to interoperate with Avaya Communication Manager and Avaya Application Enablement Services (AES). The MARATHON EVOLUTION voice recorder offers various methods of voice recording. For the purpose of the tests described by these Application Notes, the Avaya Communication Manager Single Step Conference facility was used.



**Figure 1: MARATHON EVOLUTION Test Configuration**

In the above diagram, the ASC MARATHON EVOLUTION and ASC RIAactive components act in concert to record voice conversations from telephones attached to PBX 1. The RIAactive receives events from the Avaya AES server when the state of calls associated with PBX 1 change, and informs the MARATHON EVOLUTION of these transitions. The DMCC service provided by Avaya AES is used to monitor call activity associated with PBX 1. The ASC MARATHON EVOLUTION voice recorder is attached to PBX 1 via the local area network. PBX 2 is included in the configuration solely to test the ability to monitor conversations which traverse a trunk to a networked PBX.

When a call is to be recorded, the MARATHON EVOLUTION voice recorder initiates a single-step conference with the station being monitored using one of its Virtual CTI Stations, and thus includes itself in the call which it wishes to record. The voice stream for such calls is received via the LAN interface to PBX 1.

The PBX 2 system is attached to PBX 1 via an IP/QSIG interface, and is used as a networked PBX system. This allows remote networked telephones (g, h) to be included in the test.

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. Note that one Virtual CTI Station is required for each conversation to be monitored, as these are used by MARATHON EVOLUTION to create single step conferences with the stations to be monitored. Since a Virtual CTI Station can be used to monitor only one call at a time, the number of Virtual CTI Stations must be equal to the maximum number of simultaneous monitored calls. Note that calls between parties which are both monitored and conferences among monitored participants require additional Virtual CTI Stations.

Phone	Monitored	Model	Extension
A	*	Avaya 4610SW IP	60113
b		Avaya 4610SW IP	60114
C	*	Avaya 9620 (SIP)	60171
d		Avaya 9620 (SIP)	60172
E	*	Avaya 2410	60007
f		Avaya 2410	60008
g		Avaya 2420	1000013
h		Avaya 2420	1000014
j		N/A	069 7505 6176
k		N/A	069 7505 6630
L		Hunt Group (A & C)	
x		Virtual CTI Station	61401
y		Virtual CTI Station	61402
z		Virtual CTI Station	61403

**Table 1: Device Monitor Configuration**

## 2. Equipment and Software Validated

Software Component	Version
Avaya Communication Manager	R015x.00.0.825.4
Avaya TN2312BP IP Server Interface	HW15/FW042
Avaya TN799DP Control LAN	HW01/FW026
Avaya TN2302AP Media Processor	HW20/FW033
Avaya TN2464CP DS1 Interface	HW01/FW19
Avaya Application Enablement Services	r4-1-0-31-2-0
Avaya SIP Enablement Services	SES-5.0.0.0-825.31
Avaya 4610SW IP Telephone (H.323)	2.887
Avaya 9620 IP Telephone (SIP)	2.0.3.0
ASC MARATHON EVOLUTION SW	8.0
ASC MARATHON EVOLUTION platform OS	SuSE Linux
ASC <u>RIAactive</u>	5.0
ASC <u>RIAactive</u> platform OS	MS Windows XP 2003

**Table 2: Hardware/Software Component Versions**

## 3. Configuration

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

### 3.1. Configure Avaya Communication Manager

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

The information provided in this section describes the configuration of Avaya 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].

### 3.1.1. Verify system-parameters customer-options

Use the **display system-parameters customer options** command to verify that Avaya 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. 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 used.
Computer Telephony Adjunct Links? (p.3)	This parameter must be set to “y”.
IP Stations? (p.4)	This parameter must be set to “y”.
IP_API_A (p.10)	This parameter must be set the number of Virtual CTI Stations.
IP Phone (p.10)	This parameter must be set the number of IP stations plus the number of Virtual CTI 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:	100	60
<b>Maximum Concurrently Registered IP Stations:</b>	<b>12000</b>	<b>4</b>
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:	0	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	0
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 3 of 11
OPTIONAL FEATURES	
Abbreviated Dialing Enhanced List? n	Audible Message Waiting? n
Access Security Gateway (ASG)? n	Authorization Codes? y
Analog Trunk Incoming Call ID? n	CAS Branch? n
A/D Grp/Sys List Dialing Start at 01? n	CAS Main? n
Answer Supervision by Call Classifier? n	Change COR by FAC? n
ARS? y	<b>Computer Telephony Adjunct Links? y</b>
ARS/AAR Partitioning? y	Cvg Of Calls Redirected Off-net? n
ARS/AAR Dialing without FAC? n	DCS (Basic)? n
ASAI Link Core Capabilities? y	DCS Call Coverage? n
ASAI Link Plus Capabilities? y	DCS with Rerouting? n
Async. Transfer Mode (ATM) PNC? n	
Async. Transfer Mode (ATM) Trunking? n	Digital Loss Plan Modification? n
ATM WAN Spare Processor? n	DS1 MSP? n
ATMS? n	DS1 Echo Cancellation? y
Attendant Vectoring? n	

**Figure 3: System-Parameters Customer-Options Screen (p.3)**

display system-parameters customer-options	Page 4 of 11
OPTIONAL FEATURES	
Emergency Access to Attendant? y	<b>IP Stations? y</b>
Enable 'dadmin' Login? y	
Enhanced Conferencing? y	ISDN Feature Plus? n
Enhanced EC500? y	ISDN/SIP Network Call Redirection? y
Enterprise Survivable Server? n	ISDN-BRI Trunks? y
Enterprise Wide Licensing? n	ISDN-PRI? y
ESS Administration? n	Local Survivable Processor? n
Extended Cvg/Fwd Admin? y	Malicious Call Trace? n
External Device Alarm Admin? n	Media Encryption Over IP? n
Five Port Networks Max Per MCC? n	Mode Code for Centralized Voice Mail? n
Flexible Billing? n	
Forced Entry of Account Codes? n	Multifrequency Signaling? y
Global Call Classification? n	Multimedia Call Handling (Basic)? n
Hospitality (Basic)? y	Multimedia Call Handling (Enhanced)? n
Hospitality (G3V3 Enhancements)? n	Multimedia IP SIP Trunking? n
IP Trunks? y	
IP Attendant Consoles? y	

**Figure 4: 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 5: System-Parameters Customer-Options Screen (p.10)**

### 3.1.2. Configure Dial Plan

Use the **change dialplan analysis** command to specify that dialed strings which begin with “1”, or “6” are extensions. Include the strings “\*01”, “\*83”, and “\*9” which are Trunk Access Codes.

change dialplan analysis						Page 1 of 12			
DIAL PLAN ANALYSIS TABLE									
Location: all						Percent Full: 0			
Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type	
0	1	fac							
1	7	ext							
6	6	ext							
*01	3	dac							
*83	3	dac							
*9	2	dac							

**Figure 6: Dialplan Analysis Screen**

### 3.1.3. Configure IP Network Interface

Use the **change node-names ip** command to configure IP address, as shown in the following table.

Parameter	Usage
clan	Enter the IP address of the CLAN interface of PBX1.
ses	Enter the IP address of the SES server.

**Table 4: Node-Names IP Parameters**

change node-names ip		Page 1 of 2
IP NODE NAMES		
Name	IP Address	
clan	192.168.60.6	
default	0.0.0.0	
ses	192.168.200.100	

**Figure 7: Node-Names IP Screen**

Use the **change ip-network-region <x>** command to designate a network region to be used for the IP telephone communications using the parameters shown in the following table, where <x> is the network region assigned to the clan IP interface. In this case “1” is used, as the procr IP interface is assigned to default network region of “1”.

Parameter	Usage
Location	Enter “1”.
Authoritative Domain	Enter the domain name to be used for SIP communications.
Name	Enter a name to identify the region.
Codec Set	Enter the number of the codec set defined in <b>Figure 9</b> .

**Table 5: IP-Network-Region Parameters**

```

change ip-network-region 1                                     Page 1 of 19
                                IP NETWORK REGION
  Region: 1
Location: 1      Authoritative Domain: ffm.com
    Name: FFM
MEDIA PARAMETERS      Intra-region IP-IP Direct Audio: yes
    Codec Set: 1      Inter-region IP-IP Direct Audio: yes
      UDP Port Min: 2048      IP Audio Hairpinning? n
      UDP Port Max: 3329
DIFFSERV/TOS PARAMETERS      RTCP Reporting Enabled? y
  Call Control PHB Value: 46      RTCP MONITOR SERVER PARAMETERS
    Audio PHB Value: 46      Use Default Server Parameters? y
    Video PHB Value: 26
802.1P/Q PARAMETERS
  Call Control 802.1p Priority: 6
    Audio 802.1p Priority: 6
    Video 802.1p Priority: 5      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS      RSVP Enabled? n
  H.323 Link Bounce Recovery? y
  Idle Traffic Interval (sec): 20
  Keep-Alive Interval (sec): 5
    Keep-Alive Count: 5

```

**Figure 8: IP-Network-Region Form, p.2**

Use the **change ip-codec-set** command to designate a codec set to be used. Testing was done with the G.711A codec.

Parameter	Usage
Audio Codec	Enter “G.711A”.

**Table 6: IP-Codec-Set Parameters**

```

change 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: G.711A      n          2        20

```

**Figure 9: IP-Codec-Set Form**

### 3.1.4. Configure Interface to AES

Use the **change ip-services** command to configure the interface to the AES 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 AES server when it was installed.
Password (p.4)	Enter the password that was assigned to the switch connection, as shown in <b>Figure 27</b> .
Enabled (p.4)	Enter “y” to enable the connection.

**Table 7: IP Services Parameters**

```

change ip-services
Page 1 of 4

IP SERVICES
Service  Enabled  Local  Local  Remote  Remote
Type      y      Node  Port   Node    Port
AESVCS

```

**Figure 10: IP Services Screen, p. 1**

```

change ip-services
Page 4 of 4

AE Services Administration

Server ID  AE Services  Password  Enabled  Status
          Server
1: aes_server_1  XXXXXXXXXXXXXXXX  y  in use

```

**Figure 11: 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 30**. 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: 4	CTI LINK
Extension: 69996	
Type: ADJ-IP	
	COR: 1
Name: AES-devcon223-tsapi	

**Figure 12: CTI-link Screen**

### 3.1.5. Configure Stations

#### 3.1.5.1 Configure H.323 IP Stations

Use the **add station** command to create an IP station for extensions A and b 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.

**Table 8: Configuration IP Stations**

change station 60113	Page 1 of 5	
STATION		
Extension: 60113	Lock Messages? n	BCC: 0
Type: 4610	Security Code: 31106	TN: 1
Port: S00101	Coverage Path 1: 1	COR: 1
Name: extn 60113	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: 60113	
Speakerphone: 2-way	Mute Button Enabled? y	
Display Language: english		
Survivable GK Node Name:		
Survivable COR: internal	Media Complex Ext:	
Survivable Trunk Dest? y	IP SoftPhone? n	
	Customizable Labels? y	

**Figure 13: IP Station Screen**

### 3.1.5.2 Configure SIP Stations

Use the **add station** command to create SIP IP station for extension 60171, using the values shown below. Repeat this section for extension 60172.

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.

**Table 9: Configuration SIP IP Stations**

change station 60171	Page 1 of 6
STATION	
Extension: 60171	Lock Messages? n
Type: 9620	Security Code:
Port: S00126	Coverage Path 1:
Name: extn 60171	Coverage Path 2:
	Hunt-to Station:
STATION OPTIONS	
Loss Group: 19	Time of Day Lock Table:
Speakerphone: 2-way	Personalized Ringing Pattern: 1
Display Language: english	Message Lamp Ext: 60171
Survivable GK Node Name:	Mute Button Enabled? y
Survivable COR: internal	Media Complex Ext:
Survivable Trunk Dest? y	IP SoftPhone? n
Customizable Labels? y	

**Figure 14: SIP IP Stations Screen**

Use the **add off-pbx-telephone station-mapping** command for each of the SIP stations added in the previous step.

Parameter	Usage
Extension (p.1)	Enter the extension of the SIP telephone from <b>Figure 15</b> .
Application (p.1)	Enter “OPS”.
Phone Number (p.1)	Enter the extension of the SIP telephone from <b>Figure 15</b> .
Trunk Selection (p.1)	Enter the number of the SIP trunk which was allocated in <b>Figure 22</b> .
Call Limit (p.2)	Enter a value which is sufficient for the user to participate in transfer operations or conference calls. A value of “3” was used for these tests.

**Table 10: Configuration Off-Pbx-Telephone Station-Mapping**

add off-pbx-telephone station-mapping						Page 1 of 2
STATIONS WITH OFF-PBX TELEPHONE INTEGRATION						
Station Extension	Application	Dial Prefix	CC	Phone Number	Trunk Selection	Config Set
60171	OPS	-	-	60171	83	1

**Figure 15: SIP Off-Pbx-Telephone Station-Mapping Screen, p. 1**

add off-pbx-telephone station-mapping						Page 2 of 2
STATIONS WITH OFF-PBX TELEPHONE INTEGRATION						
Station Extension	Call Limit	Mapping Mode	Calls Allowed	Bridged Calls	Location	
60171	3	both	all	none		

**Figure 16: SIP Off-Pbx-Telephone Station-Mapping Screen, p. 2**



### 3.1.5.3 Configure Virtual CTI Stations

Use the **add station** command to create a station for each of the Virtual CTI Stations listed in **Table 1**. Sufficient Virtual CTI Stations must be created to monitor the maximum number of simultaneous monitored conversations. These stations are subsequently assigned by the ASC DataManager for monitoring in **Figure 52**. Note that the station numbers must be sequential.

Parameter	Usage
Type	Enter “4620”.
Name	Any alphanumeric string can be assigned as an extension name.
Security Code	Enter a security code which identical to the extension.
IP Softphone	Enter “y”.

**Table 11: Virtual CTI Station Parameters**

add station 61401		Page 1 of 5
STATION		
Extension: 61401	Lock Messages? n	BCC: 0
<b>Type: 4620</b>	<b>Security Code: 61401</b>	TN: 1
Port: S00104	Coverage Path 1:	COR: 1
<b>Name: CTI 61401</b>	Coverage Path 2:	COS: 1
	Hunt-to Station:	
STATION OPTIONS		
Loss Group: 19	Time of Day Lock Table:	
	Personalized Ringing Pattern: 1	
Speakerphone: 2-way	Message Lamp Ext: 61401	
Display Language: english	Mute Button Enabled? y	
Survivable GK Node Name:	Expansion Module? n	
Survivable COR: internal	Media Complex Ext:	
Survivable Trunk Dest? y	<b>IP SoftPhone? y</b>	
	IP Video Softphone? n	
	Customizable Labels? y	

**Figure 17: Virtual CTI Station Screen**

### 3.1.6. 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 60113 and 60171 are used.

**Table 12: 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: 61304	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 18: Hunt Group Screen, p. 1**

change hunt-group 4	Page 3 of 60
HUNT GROUP	
Group Number: 4	Group Extension: 61304
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: 60113	extn 60113
2: 60171	extn 60171
3:	
4:	
5:	
6:	
7:	
8:	
9:	
10:	
11:	
12:	
13:	
At End of Member List	

**Figure 19: Hunt Group Screen, p. 3**

### 3.1.7. Configure Interface to SIP Enablement Services

Use the **add signaling-group** command to allocate a signaling group for interface to SES using the following parameters:

Parameter	Usage
Group Type	Enter “sip”.
Near-end Node Name	Enter “clan” (defined in <b>Figure 7</b> ) to designate the Control LAN as the near end node name.
Far-end Node Name	Enter “ses” to assign the SES server as the far end node name.
DTMF over IP	Enter “rtp-payload”. This value used to have Avaya Communication Manager send DTMF transmissions using RFC 2833 ([7]).
Direct IP-IP Audio Connections	Enter “y” to allow direct IP-IP endpoint connections (shuffling).

**Table 13: Signaling-Group Parameters**

```
add signaling-group 83                                     Page 1 of 1
                  SIGNALING GROUP
Group Number: 1      Group Type: sip
                    Transport Method: tls

Near-end Node Name: clan      Far-end Node Name: ses
Near-end Listen Port: 5061    Far-end Listen Port: 5061
Far-end Domain:              Far-end Network Region: 1

                                Bypass If IP Threshold Exceeded? n
DTMF over IP: rtp-payload      Direct IP-IP Audio Connections? y
                                IP Audio Hairpinning? n
Enable Layer 3 Test? n
Session Establishment Timer(min): 3
```

**Figure 20: Signaling-Group Form**

Use the **add trunk-group** <*n*> command, where <*n*> is an unused trunk number, to allocate a trunk group to be used as an interface to the SIP Enablement Services server. Use the parameters shown in the following table.

Parameter	Usage
Group Type (p.1)	Enter “sip”.
Group Name (p.1)	Assign a name for identification purposes.
TAC (p.1)	Enter the Trunk Access Code allocated in <b>Figure 6</b> .
Service Type (p.1)	Enter “tie”.
Signaling Group (p.1)	Enter the number of the signaling group allocated in <b>Figure 20</b> .
Number of Members (p.1)	Enter a number large enough to support the maximum number of anticipated simultaneous calls to be made via the SIP trunk.

**Table 14: Trunk-Group Parameters**

add trunk-group 83		Page 1 of 21	
TRUNK GROUP			
Group Number: 83	<b>Group Type: sip</b>	CDR Reports: y	
<b>Group Name: SIP</b>	COR: 1	TN: 1	<b>TAC: *83</b>
Direction: two-way	Outgoing Display? n	Night Service:	
Dial Access? n			
Queue Length: 0			
<b>Service Type: tie</b>	Auth Code? n		
		Signaling Group: 83	
		Number of Members: 255	

**Figure 21: Trunk-Group Form, p.1**

Use the **add off-pbx-telephone station-mapping <x>** command for each of the SIP stations shown in **Table 1**.

Parameter	Usage
Station Extension (p.1)	The extension of the SIP telephone. This extension should have been allocated as described in <b>Figure 14</b> .
Application (p.1)	Enter “OPS”.
Phone Number (p.1)	Enter the extension.
Trunk Selection (p.1)	Enter the number of the SIP trunk which allocated in <b>Figure 21</b> .
Call Limit (p.2)	Enter “3” to allow transfer/conference operations.

**Table 15: off-pbx-telephone station-mapping Parameters**

add off-pbx-telephone station-mapping 60171						Page 1 of 2
STATIONS WITH OFF-PBX TELEPHONE INTEGRATION						
Station Extension	Application	Dial Prefix	CC	Phone Number	Trunk Selection	Config Set
60171	OPS	-		60171	83	1

**Figure 22: off-pbx-telephone station-mapping Screen, p.1**

change off-pbx-telephone station-mapping 60171						Page 2 of 2
STATIONS WITH OFF-PBX TELEPHONE INTEGRATION						
Station Extension	Call Limit	Mapping Mode	Calls Allowed	Bridged Calls	Location	
60171	3	both	all	none		

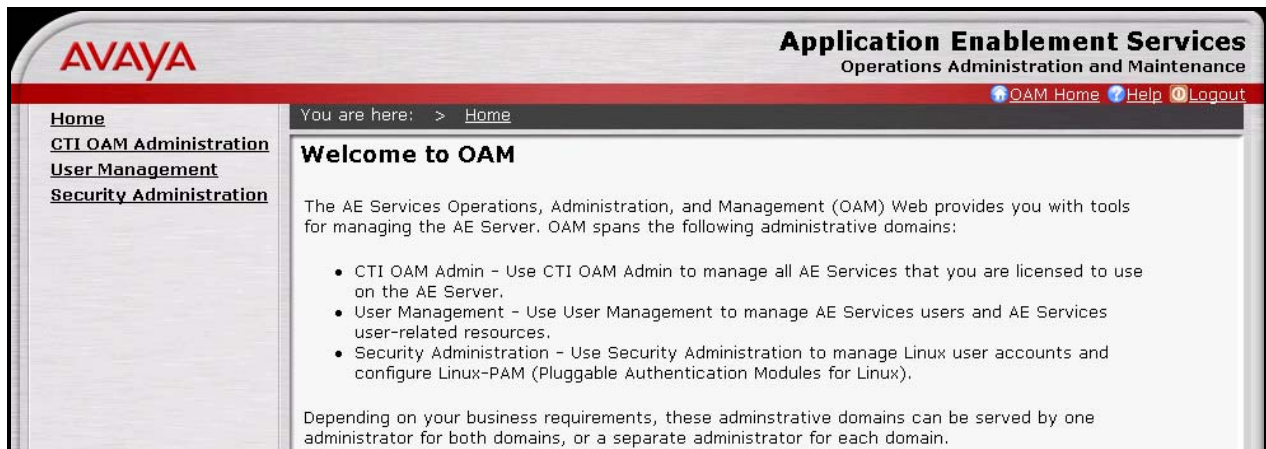
**Figure 23: off-pbx-telephone station-mapping Screen, p.2**

## 3.2. Configure Avaya AES

The AES server is configured via a web browser by accessing the following URL:

`https://<AES server address>:8443/MVAP/`

Once the login screen appears, enter either the appropriate login ID/password for performing administrative activities or user management.



**Figure 24: AES Welcome Screen**

After logging in, select “CTI OAM Admin” which displays the following screen. Verify that the AES server installation has a TSAPI service license. If this is not the case, please contact an Avaya representative regarding licensing.

**AVAYA** **Application Enablement Services**  
Operations Administration and Maintenance

[OAM Home](#) [Help](#) [Logout](#)

You are here: > [CTI OAM Home](#)

**CTI OAM Home**  
▶ [Administration](#)  
▶ [Status and Control](#)  
▶ [Maintenance](#)  
▶ [Alarms](#)  
▶ [Logs](#)  
▶ [Utilities](#)  
▶ [Help](#)

### Welcome to CTI OAM Screens

[craft] Last login: Tue Apr 29 15:08:25 2008 from 192.168.150.5

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

Service	Controller Status
<b>ASAI Link Manager</b>	Running
<b>DMCC Service</b>	Running
<b>CVLAN Service</b>	Running
<b>DLG Service</b>	Running
<b>Transport Layer Service</b>	Running
<b>TSAPI Service</b>	Running

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

### License Information

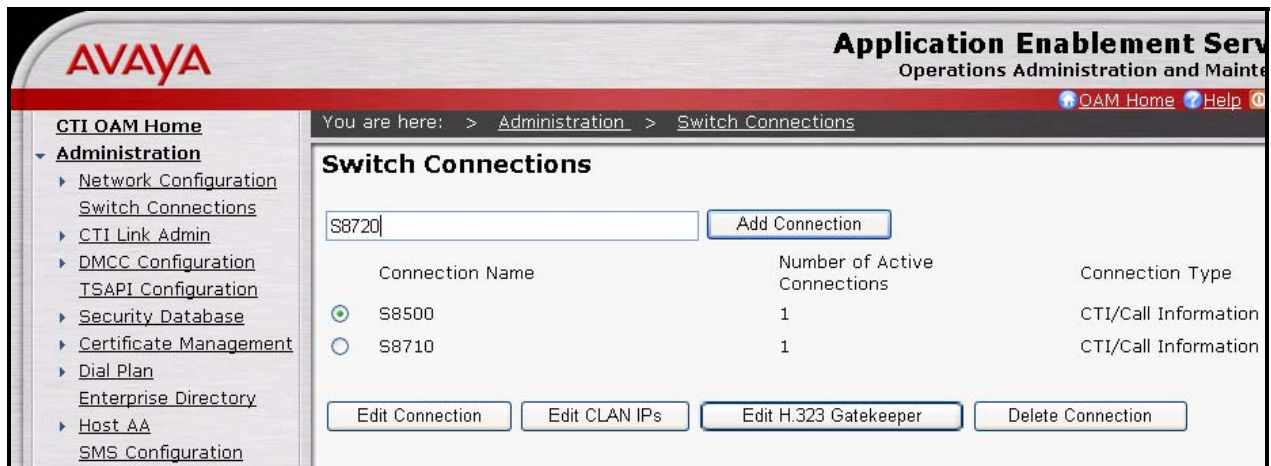
You are licensed to run Application Enablement (CTI) version 4.1.

You are licensed for the following services

- DLG
- CVLAN
- TSAPI
- SMS

**Figure 25: AES CTI OAM Welcome Screen**

Navigate to **Administration->Switch Connections**. Enter the name of the Switch Connection to be added, and click on the “Add Connection” button. This name should match that which is used by the ASC DataManager in **Figure 50**.



**Figure 26: 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 Connection Type	Specify a type of CTI/Call Information.
Switch Password	The Switch Password must be the same as was entered into the Avaya Communication Manager AE Services Administration form via the “change ip-services” command, described in <b>Figure 11</b> . 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 16: Configuration of Switch Password**

**AVAYA** Application Engine Operations Administration

You are here: > Administration > Switch Connections

### Set Password - S8720

Please note the following:

- \* A password is not required for a H323 Gatekeeper Connection.
- \* Changing the password affects only new connections, not open connections.

Switch Connection Type: CTI/Call Information

Switch Password: [Masked]

Confirm Switch Password: [Masked]

SSL: ☒

**Figure 27: Set Switch Password Screen**

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



**Figure 28: CLAN Screen**

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



**Figure 29: 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 Avaya Communication Manager “add cti-link” configuration command in **Figure 12**. Click the “Apply Changes” button.

The screenshot displays the Avaya Application Operations web interface. The top header features the Avaya logo and the text 'Application Operations'. A breadcrumb trail indicates the current path: 'You are here: > Administration > CTI Link Admin > TSAPI Links'. The left sidebar contains a navigation menu with the following items: 'CTI OAM Home', 'Administration' (expanded), 'Network Configuration', 'Switch Connections', 'CTI Link Admin' (expanded), 'TSAPI Links' (selected), 'CVLAN Links', 'DLG Links', 'DMCC Configuration', 'TSAPI Configuration', 'Security Database', and 'Certificate Management'. The main content area is titled 'Add / Edit TSAPI Links' and contains the following form fields: 'Link' (value: 1), 'Switch Connection' (value: S8720), 'Switch CTI Link Number' (value: 4), 'ASAI Link Version' (value: 1), and 'Security' (value: Unencrypted). At the bottom of the form are two buttons: 'Apply Changes' and 'Cancel Changes'.

**Figure 30: Add TSAPI Link Screen**

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

The “CT User” field for this user must be set to “Yes”. In this case, the AES user is the MARATHON EVOLUTIONCT application, which uses AES to monitor stations and initiate switching operations. The “User Id” and “User Password” must be the same as those configured for ASC DataManager in **Figure 51**.

**AVAYA** Application Operations

**User Management Home** You are here: > [User Management](#) > [Add User](#)

**Add User**

Fields marked with \* can not be empty.

\* User Id

\* Common Name

\* Surname

\* User Password

\* Confirm Password

Admin Note

Avaya Role

Business Category

Car License

CM Home

Ciss Home

CT User

**Figure 31: Add User Screen**

Navigate to **Administration -> Network Configuration -> Ports** and configure the DMCC Server Ports as shown in the following table.

Parameter	Usage
Unencrypted Port	Set this port to 4721, enabled to match the value in <b>Figure 51</b> .
Encrypted Port	Set this port to 4722, enabled to match the value in <b>Figure 51</b> .

**Table 17: DataManager AES Server Interface Parameters**

You are here: > [Administration](#) > [Network Configuration](#) > [Ports](#)

### 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"/>
H.323 Ports			
TCP Port Min	<input type="text" value="3000"/>		
TCP Port Max	<input type="text" value="4100"/>		
Local UDP Port Min	<input type="text" value="7000"/>		
Local UDP Port Max	<input type="text" value="8100"/>		
RTP Local UDP Port Min	<input type="text" value="5000"/>		
RTP Local UDP Port Max	<input type="text" value="5300"/>		

**Figure 32: AES Port Configuration**

### 3.3. Avaya SIP Enablement Services

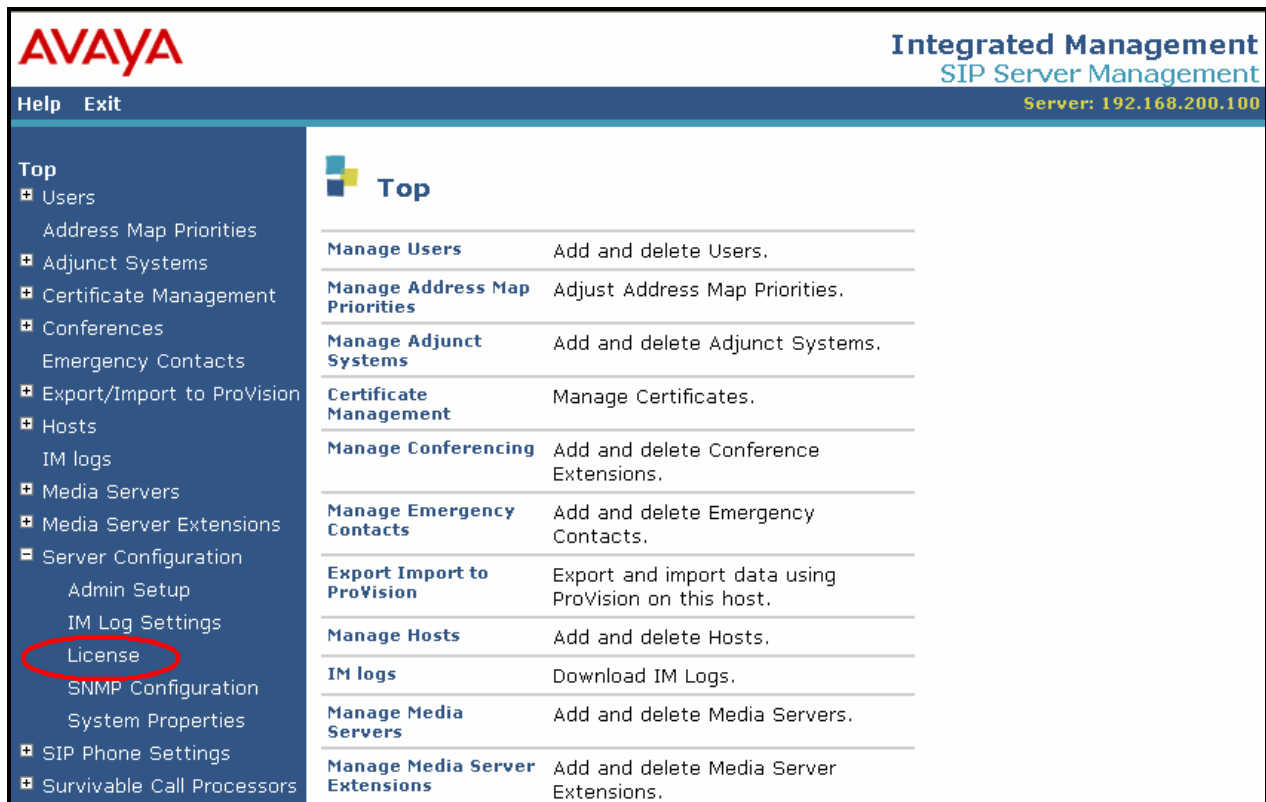
Configure SES by entering “<SES IP Address>/admin/” in a web browser. After entering the administrator name and password, the following screen content is displayed. Select “Launch Administration Web Interface”.



**Figure 33: Launch Maintenance Web Interface Screen**

### 3.3.1. Install License

From the “Top” menu navigate to **Server Configuration -> License**.



**AVAYA** Integrated Management SIP Server Management  
Server: 192.168.200.100

Help Exit

**Top**

- ▣ Users
  - Address Map Priorities
- ▣ Adjunct Systems
- ▣ Certificate Management
- ▣ Conferences
  - Emergency Contacts
- ▣ Export/Import to ProVision
- ▣ Hosts
  - IM logs
- ▣ Media Servers
- ▣ Media Server Extensions
- ▣ Server Configuration
  - Admin Setup
  - IM Log Settings
  - License**
  - SNMP Configuration
  - System Properties
- ▣ SIP Phone Settings
- ▣ Survivable Call Processors

**Top**

<b>Manage Users</b>	Add and delete Users.
<b>Manage Address Map Priorities</b>	Adjust Address Map Priorities.
<b>Manage Adjunct Systems</b>	Add and delete Adjunct Systems.
<b>Certificate Management</b>	Manage Certificates.
<b>Manage Conferencing</b>	Add and delete Conference Extensions.
<b>Manage Emergency Contacts</b>	Add and delete Emergency Contacts.
<b>Export Import to ProVision</b>	Export and import data using ProVision on this host.
<b>Manage Hosts</b>	Add and delete Hosts.
<b>IM logs</b>	Download IM Logs.
<b>Manage Media Servers</b>	Add and delete Media Servers.
<b>Manage Media Server Extensions</b>	Add and delete Media Server Extensions.

**Figure 34: Select License from Top SES Screen**

Click “Access WebLM”.

The screenshot shows a web interface with a blue sidebar on the left and a white main content area on the right. The sidebar contains a 'Top' section with a list of menu items: Setup, Users, Address Map Priorities, Adjunct Systems, Conferences, Emergency Contacts, Export/Import to ProVision, Hosts, IM logs, Media Servers, Media Server Extensions, and Server Configuration. The 'Server Configuration' item is expanded, showing sub-items: Admin Setup, IM Log Settings, and License. The main content area has a title 'List Licenses' with a small logo. Below the title is a table with three columns: 'Proxy Name', 'Name', and 'Message'. The table contains three rows of data. The first row has 'sipserver' in the 'Proxy Name' column, 'Basic Proxy' in the 'Name' column, and an empty 'Message' column. The second row has 'sipserver' in the 'Proxy Name' column, 'Edge Proxy' in the 'Name' column, and an empty 'Message' column. The third row has 'sipserver' in the 'Proxy Name' column, 'Home Seats' in the 'Name' column, and an empty 'Message' column. To the left of the table, there are three 'Show' links. Below the table, the text 'Access WebLM' is circled in red.

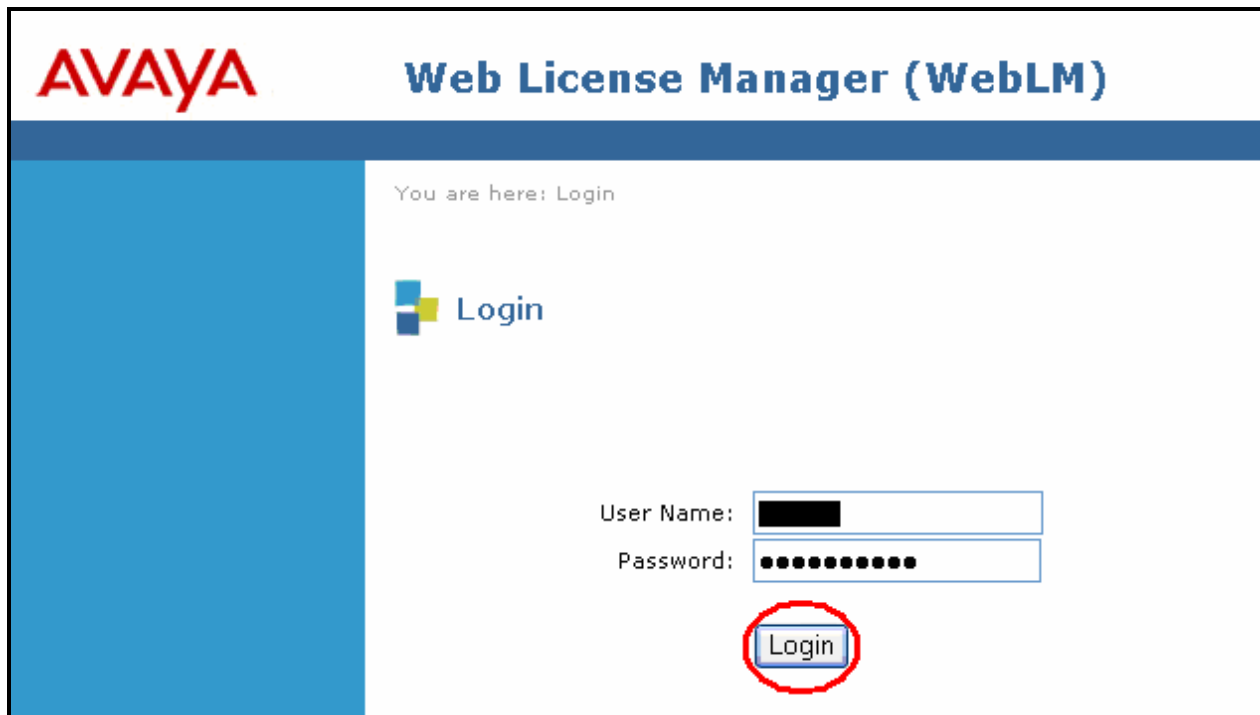
	<u>Proxy Name</u>	<u>Name</u>	<u>Message</u>
<a href="#">Show</a>	sipserver	Basic Proxy	
<a href="#">Show</a>	sipserver	Edge Proxy	
<a href="#">Show</a>	sipserver	Home Seats	

**Access WebLM**

**Figure 35: Select WebLM from License Screen**



Log in to WebLM with the appropriate administrative user name and password. Read the license file when instructed by WebLM. Exit WebLM. Re-enter the URI “http:<SES IP address>/admin” into the Web browser.



The image shows the Web License Manager (WebLM) login screen. At the top left is the AVAYA logo in red. To its right is the title "Web License Manager (WebLM)" in blue. Below the title is a blue horizontal bar. On the left side of the page is a large blue vertical rectangle. The main content area is white and contains the text "You are here: Login" in a small font. Below this is a "Login" link with a small icon of three squares (blue, yellow, blue). Further down are two input fields: "User Name:" followed by a text box containing a blacked-out name, and "Password:" followed by a text box containing ten black dots. Below the password field is a "Login" button, which is a blue rectangle with the word "Login" in white text. The "Login" button is circled with a red hand-drawn circle.

**Figure 36: WebLM Login Screen**

Click “Setup” on the Top SES menu.



**AVAYA** Integrated Management  
SIP Server Management  
Help Exit Server: 192.168.200.100

**Top**  
**Setup**  
+ Users  
Address Map Priorities  
+ Adjunct Systems  
+ Conferences  
Emergency Contacts  
+ Export/Import to ProVision  
+ Hosts  
IM logs  
+ Media Servers  
+ Media Server Extensions  
+ Server Configuration  
+ SIP Phone Settings  
+ Survivable Call Processors  
System Status  
+ Trace Logger  
+ Trusted Hosts

**Top**

<b>Manage Users</b>	Add and delete Users.
<b>Manage Address Map Priorities</b>	Adjust Address Map Priorities.
<b>Manage Adjunct Systems</b>	Add and delete Adjunct Systems.
<b>Manage Conferencing</b>	Add and delete Conference Extensions.
<b>Manage Emergency Contacts</b>	Add and delete Emergency Contacts.
<b>Export Import to ProVision</b>	Export and import data using ProVision on this host.
<b>Manage Hosts</b>	Add and delete Hosts.
<b>IM logs</b>	Download IM Logs.
<b>Manage Media Servers</b>	Add and delete Media Servers.
<b>Manage Media Server Extensions</b>	Add and delete Media Server Extensions.
<b>Server Configuration</b>	View Properties of the system.
<b>Manage SIP Phone Settings</b>	Add/Delete Phone Settings
<b>Manage Survivable Call Processors</b>	Add and delete Survivable Call Processors.
<b>System Status</b>	View System Status.
<b>Trace Logger</b>	Manage SIP Trace Logs.
<b>Manage Trusted Hosts</b>	Add and delete Trusted Hosts.

**Figure 37: Initiate “Setup” from Top SES Configuration Screen**

### 3.3.2. Setup Dataservice

Click “Setup Dataservice”.



**Figure 38: Initiate “Setup Dataservice” from Top Setup Screen**

Select “This server is the SES Master Administration System for the SES Network”, and click “Setup”, and “Continue” for the screen that follows.

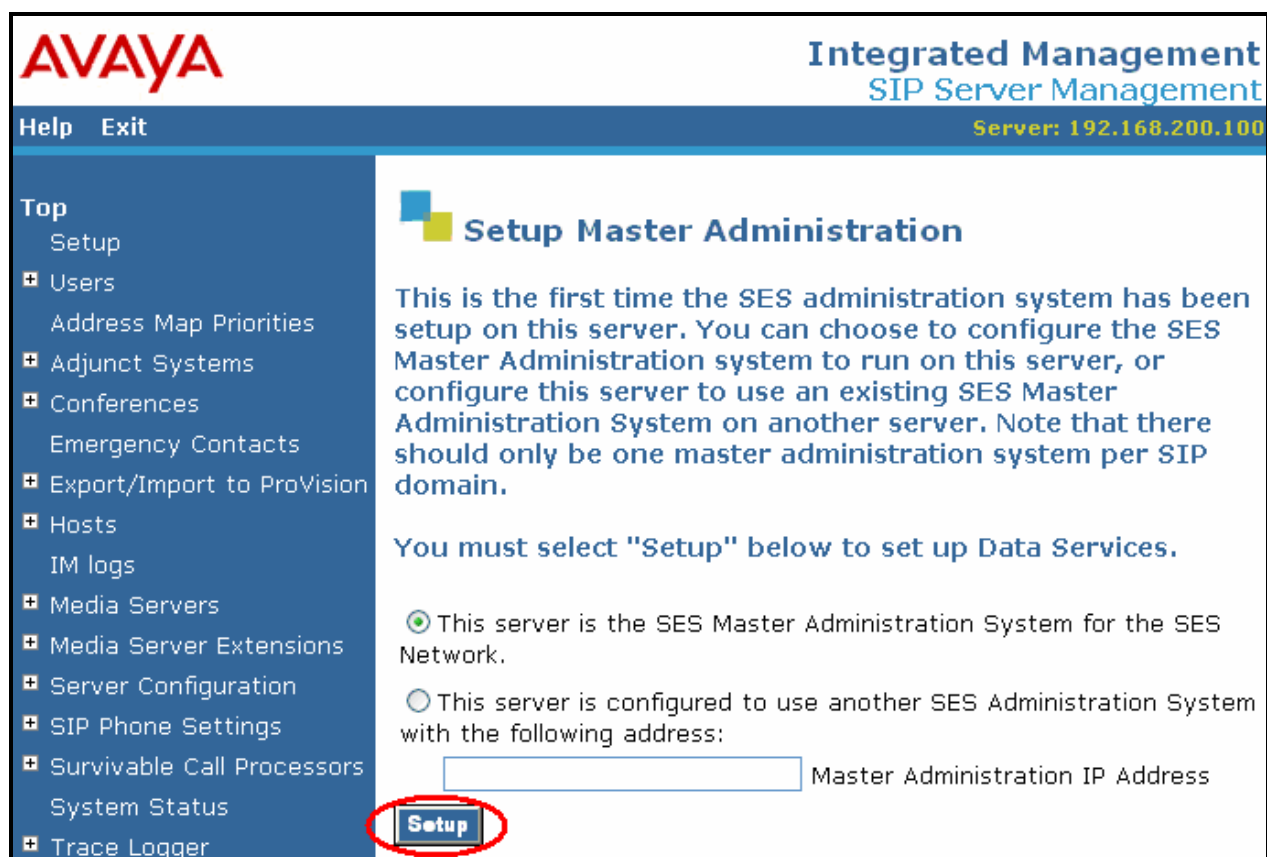


Figure 39: “Setup Master Administration” Screen

### 3.3.3. Setup SIP Domain

Click “Setup SIP domain”.



Figure 40: “Setup SIP Domain” Screen

Enter values in this screen as shown in the following table, and click “Update”, followed by “Ok” for the following screen.

Parameter	Usage
SIP Domain	Enter the same value as was used for “Authoritative Domain” in <b>Figure 8</b> .
License Host	Enter the IP address of the license host, in this case the IP address of the SES server.

**Table 18: Parameters for System Properties**

**AVAYA** Integrated Management SIP Server Management  
Server: 192.168.200.100

Help Exit

**Top**

- Users
  - Address Map Priorities
- Adjunct Systems
- Certificate Management
- Conferences
  - Emergency Contacts
- Export/Import to ProVision
- Hosts
  - IM logs
- Media Servers
- Media Server Extensions
- Server Configuration
  - Admin Setup
  - IM Log Settings
  - License

**View System Properties**

SES Version SES-5.0.0.0-825.31  
System Configuration simplex  
Host Type SES combined home-edge

SIP Domain\* ffm.com

Note that the DNS domain is ffm.com

If you are unsure about this field, most often the SIP domain should be the root level DNS domain. For example, for a DNS domain of eastcoast.example.com, the SIP domain would likely be configured to example.com. This allows SIP calls and instant messages to users with handles of the format handle@example.com

SIP License Host\* 192.168.200.100

**Figure 41: System Properties Screen**

### 3.3.4. Add Media Server Interface

Navigate to **Media Servers → Add** from the “Top” level menu shown in **Figure 34**, and specify the interface parameters as shown in the following table.

Parameter	Usage
Media Server Interface Name	Enter a descriptive name for this interface.
SIP Trunk IP Address	Enter the IP address of the S8300 Server, or the address of the CLAN interface if an G650 gateway is used.
Media Server Admin Address	Enter the IP address of the S8300 Server administration interface.
Media Server Admin Login	Enter an administrator user ID for the media server.
Media Server Admin Password	Enter the password for the above user.

**Table 19: “Add Media Server Interface” Parameters**

The screenshot shows the Avaya Integrated Management SIP Server Management interface. The top header includes the Avaya logo, the title 'Integrated Management SIP Server Management', and the server IP '192.168.200.100'. A left sidebar contains a 'Top' menu with options like Users, Address Map Priorities, Adjunct Systems, Certificate Management, Conferences, Emergency Contacts, Export/Import to ProVision, Hosts, IM logs, Media Servers (with sub-options Add and List), Media Server Extensions, Server Configuration, SIP Phone Settings, and Survivable Call Processors. The main content area is titled 'Edit Media Server Interface' and contains the following fields:

- Media Server Interface Name\***: A text box containing 'S8720'.
- Host**: A text box containing '192.168.200.100'.
- SIP Trunk Link Type**: Radio buttons for TCP and TLS, with TLS selected.
- SIP Trunk IP Address\***: A text box containing '192.168.60.6'.
- Media Server Admin Address (see Help)**: A text box containing '192.168.60.100'.
- Media Server Admin Port**: A text box containing '5023'.
- Media Server Admin Login**: A text box with a blacked-out value.
- Media Server Admin Password**: A text box with masked characters (dots).
- Media Server Admin Password Confirm**: A text box with masked characters (dots).

**Figure 42: SES Add Media Server Interface Screen**

### 3.3.5. Add Hosts

Navigate to **Hosts** → **Add Host** from the top level screen shown in **Figure 34**. Enter values in this screen as shown in the following table, accepting the default values for those parameters which are not listed. Click the “Add” button upon completion and the “Continue” button when the following screen is displayed.

Parameter	Usage
Host IP Address	Enter the IP address of the SES server.
Profile Service Password	Enter the password which was entered from the initial setup script when SES was installed.

**Table 20: “Add Host” Parameters**

**Figure 43: SES Add Host Screen**

### 3.3.6. Add Users

From the “Users” menu in the left frame, click “Add”, and enter the parameters shown in the following screen, for each of the SIP telephones shown in **Table 1**.

Parameter	Usage
Primary Handle	Enter the extension to be assigned to the user.
User ID	Enter the extension to be assigned to the user.
Password / Confirm	Enter the password to be assigned to the telephone.
First / Last Name	Enter a name for identification purposes.
Add Media Server Extension	Check this box, to add an extension for this user.

**Table 21: User Configuration Parameters**

**AVAYA** Integrated Management SIP Server Management  
Server: 192.168.200.100

Help Exit

**Add User**

Primary Handle\* 60171

User ID 60171

Password\* .....

Confirm Password\* .....

Host\* 192.168.200.100

First Name\* Extn

Last Name\* 60171

Address 1 Kleyerstr 94

Address 2

Office

City Frankfurt

State

Country Germany

Zip 60326

Survivable Call Processor none

Add Media Server Extension ☒

Fields marked \* are required.

**Figure 44: SES Add User Screen**



The “Add Media Server Extension” screen will appear after the user has been added in the previous step. Enter the “Extension” for the SIP telephone from **Table 1** for the user which was created in the previous step, select the corresponding “Media Server” from the drop-down list, and click “Add”. Note that the extensions must match those which were allocated to the stations added in **Figure 14**.

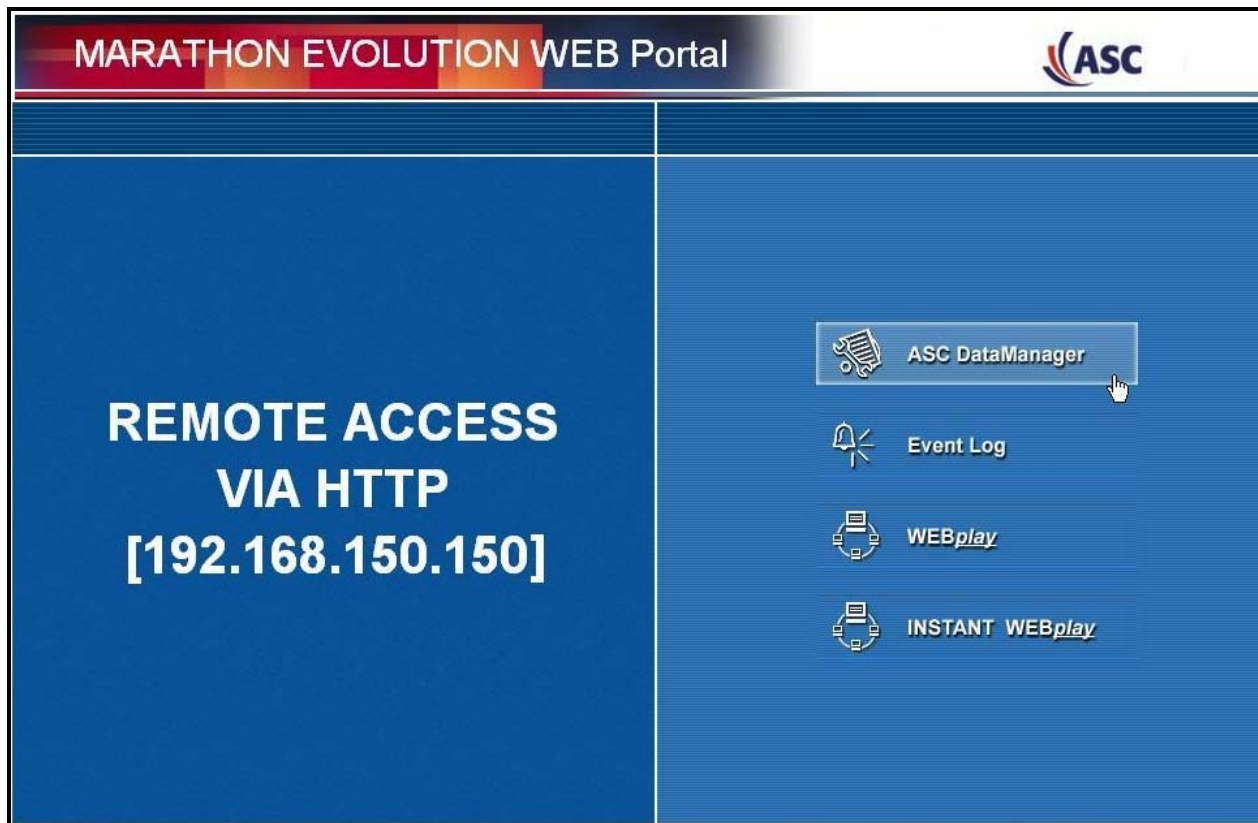
The screenshot displays the Avaya Integrated Management SIP Server Management interface. The top header features the Avaya logo and the title 'Integrated Management SIP Server Management' with the server IP '192.168.200.100'. A sidebar on the left contains navigation links: 'Top', 'Users', 'Add', 'Default Profile', 'Delete', 'Edit', 'List', 'Password', 'Search', and 'Manage All Registered'. The main content area is titled 'Add Media Server Extension' and shows a form for adding a media server extension for user 60171. The form includes two input fields: 'Extension' with the value '60171' and 'Media Server' with a dropdown menu showing 'S8720'. A red box highlights the 'Add' button. Below the form, a note states 'Fields marked \* are required.'

**Figure 45: SES Add Media Server Extension Screen**

### 3.4. 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.

The Marathon configuration tool is available by selecting the **ASC DataManager** application on the right.



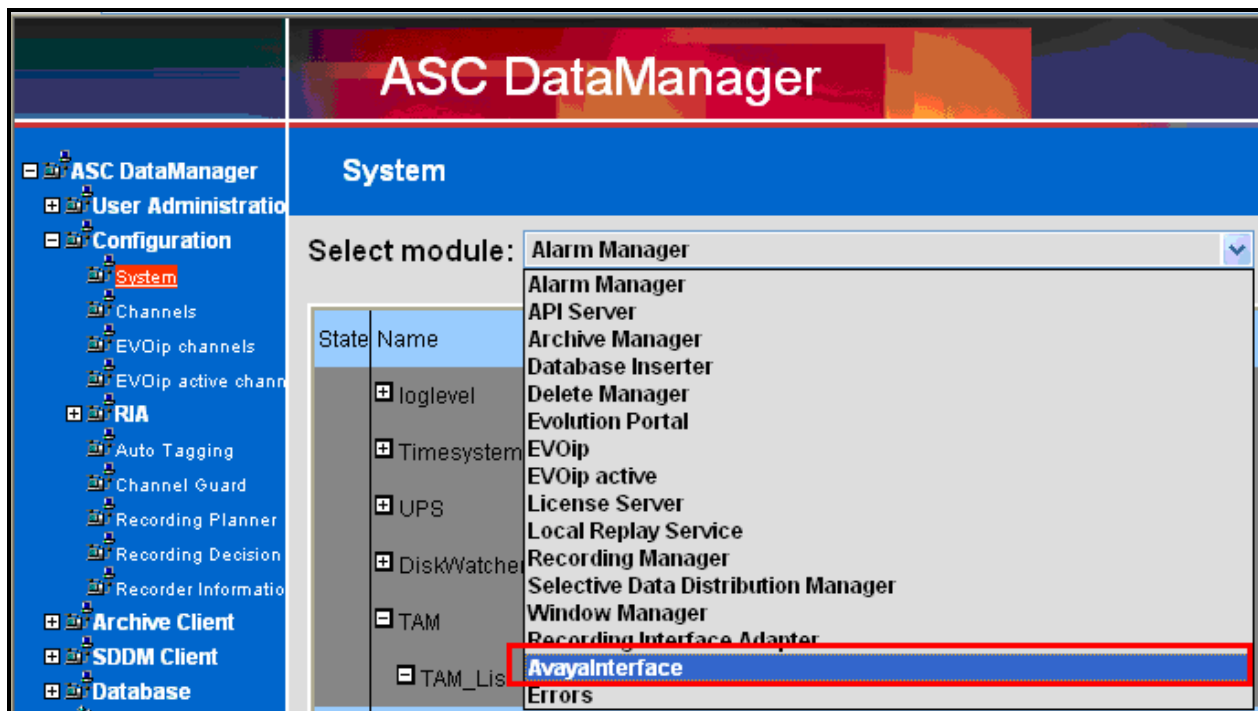
**Figure 46: MARATHON EVOLUTION Welcome Screen**

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



**Figure 47: DataManager Welcome Screen**

Select “AvayaInterface” from the “Select module” drop-down menu.



**Figure 48: DataManager Select AvayaInterface Mode**

Set “State” parameters as described in the following table.

Parameter	Usage
Activate	Set this parameter to “Yes”.
OperationMode / CTI	Set this parameter to “Yes” for Single Step Conference operation.

**Table 22: DataManager AvayaInterface Operation Mode Parameters**

The screenshot shows the 'ASC DataManager' application window. The 'System' tab is active, and the 'Select module' dropdown is set to 'AvayaInterface'. Below this, a table displays the configuration parameters:

State	Name	Description	Value(s)
	Activate	Activate Avaya Interface	Yes
	OperationMode		
	CTI	CTI mode	Yes

**Figure 49: DataManager AvayaInterface Operation Mode**

Configure the “AvayaInterface” “Communication Manager” parameters as shown in the following table.

Parameter	Usage
IP	Enter the IP address of the Communication Manager clan interface as configured in <b>Figure 7</b> .
Name	Enter the name which was assigned to the switch connection in <b>Figure 26</b> .

**Table 23: Configuration IP Stations**

**ASC DataManager**

**System**

Select module: **AvayaInterface**

State	Name	Description	Value(s)
	<i>Activate</i>	Activate Avaya Interface	Yes
	OperationMode		
	CommunicationManager		
	<i>IP</i>	IP address of CM	192.168.60.6
	<i>Name</i>	Name of CM	S8720

**Figure 50: DataManager AvayaInterface Communication Manager**

Configure the “AvayaInterface” “AES Server” parameters as shown in the following table.

Parameter	Usage
IP	Enter the IP address of the AES Server.
PortEncrypted	Enter the same value which is specified in <b>Figure 32</b> .
PortUnencrypted	Enter the same value which is specified in <b>Figure 32</b> .
Secure	Enter “No”.
User	Enter the same value which is specified in <b>Figure 31</b> .
Password	Enter the same value which is specified in <b>Figure 31</b> .

**Table 24: DataManager AES Server Interface Parameters**

State	Name	Description	Value(s)
	Activate	Activate Avaya Interface	Yes
	OperationMode		
	CommunicationManager		
	AESServer		
	IP	IP address of AES server	192.168.200.101
	PortEncrypted	Encrypted IP port of AES server	4722
	PortUnencrypted	Unencrypted IP port of AES server	4721
	Secure	Encryption enabled	No
	TrustStoreLocation	Location of certificate file	
	User	Login username	asc
	Password	Login password	Marathon-123
	SessionDurationTimer	Timeout for session duration	60
	SessionCleanupDelay	Delay for session cleanup	0
	ReconnectDelay	Delay for reconnection to AES server	5

**Figure 51: DataManager AES Server Interface Screen**

Configure the “AvayaInterface” “Softphones” parameters as shown in the following table.

Parameter	Usage
RangeStart	Enter the extension of the first Virtual CTI Station which was allocated for monitoring, as defined in <b>Figure 17</b> .
RangeLen	Enter the number of Virtual CTI Stations used for monitoring.

**Table 25: DataManager Softphones Parameters**

State	Name	Description	Value(s)
	Activate	Activate Avaya Interface	Yes
	OperationMode		
	CommunicationManager		
	AESServer		
	Softphones		
	SoftphoneRange_0		
	RangeStart	First ext number of this range	61401
	RangeLen	Length of ext number range	3

**Figure 52: DataManager Softphones Screen**



Configure the “AvayaInterface” “Recorder” parameters as shown in the following table.

Parameter	Usage
IP	Enter the IP address of the MARATHON EVOLUTION server.
ReconnectDelay	Enter “15”.

**Table 26: DataManager Recorder Parameters**

**ASC DataManager**

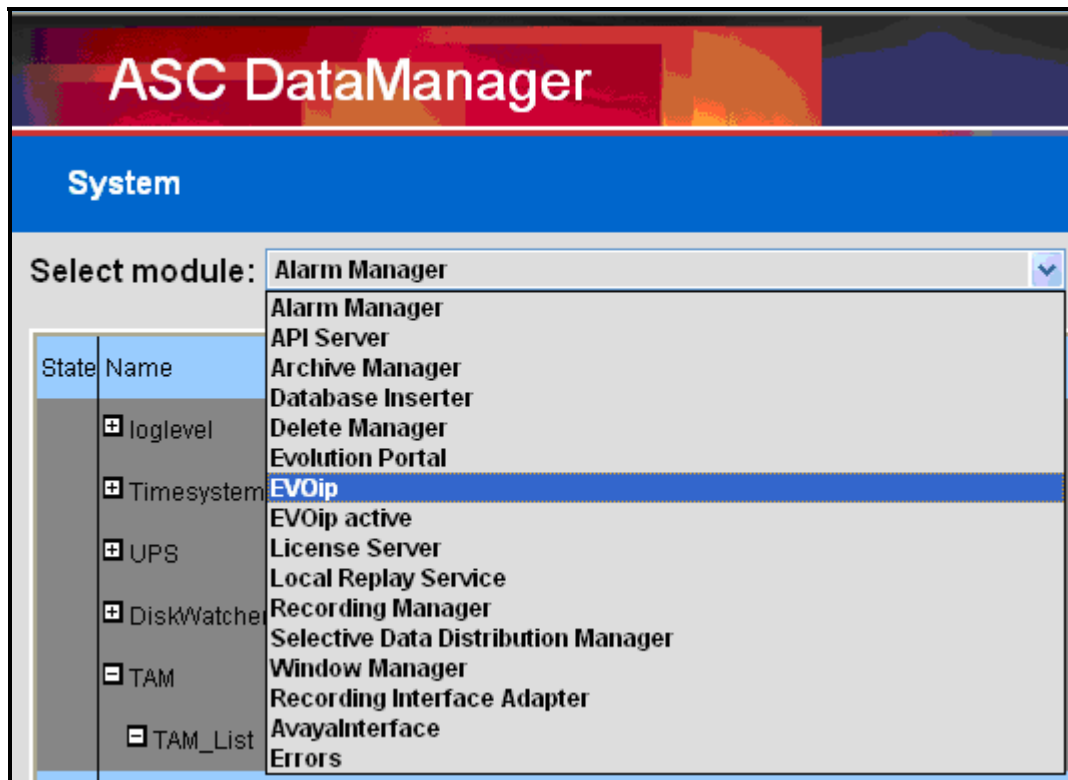
**System**

Select module: AvayaInterface

State	Name	Description	Value(s)
	Activate	Activate Avaya Interface	Yes
	OperationMode		
	CommunicationManager		
	AESServer		
	Softphones		
	Recorder		
	IP	IP address of recorder	192.168.150.150
	MsgPort	IP port for exchanging XML messages	8765
	ReconnectDelay	Delay for reconnection to recorder	15

**Figure 53: DataManager Recorder Screen**

From the DataManager top-level menu, select the “EVOip” module.



**Figure 54: Select EVOip Screen**

Set the “Calldata” “EnableCallTagging” parameter to “No” for SSC operation.

**ASC DataManager**

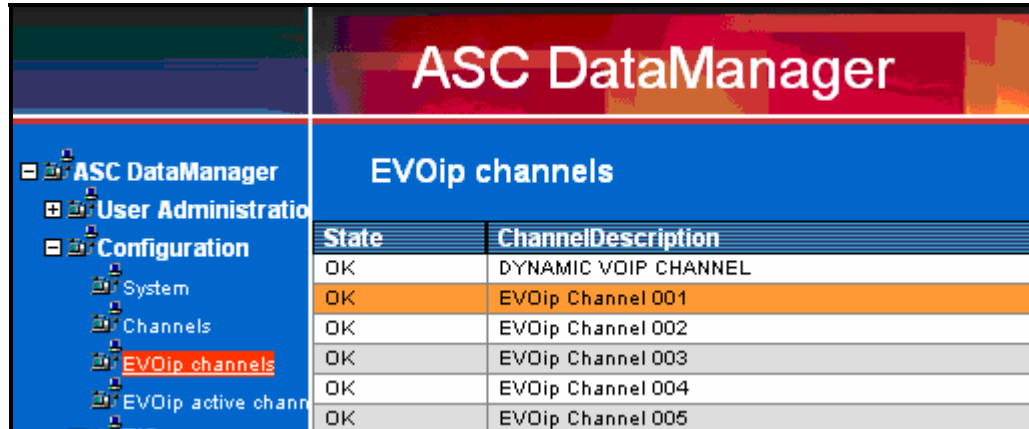
**System**

Select module: **EVOip**

State	Name	Description	Value(s)
	ExpertMode		
	Devices		
	Sniffer		
	SIP		
	SCCP		
	SIFA		
	Receiver		
	Calldata		
	<i>EnableCallTagging</i>	Enables tagging of call related data. May be disabled if a CTIC is used.	No
	<i>ForceAvayaDMCCTagging</i>	Forces tagging of Avaya DMCC call related data.	No
	<i>LocalIPField</i>	Specifies the DB field to store the local party's IP address in	disabled
	<i>PartnerIPField</i>	Specifies the DB field to store the other party's IP address in	disabled
	<i>LocalNameField</i>	Specifies the DB field to store the local party's display text (if available) in	disabled
	<i>PartnerNameField</i>	Specifies the DB field to store the other party's display text (if available) in	disabled
	<i>SCCPOriginalCalledNumber</i>	Specifies the DB field to store the originally called party's number (if available) in	disabled
	<i>SCCPOriginalCalledName</i>	Specifies the DB field to store the originally called party's name text (if available) in	disabled

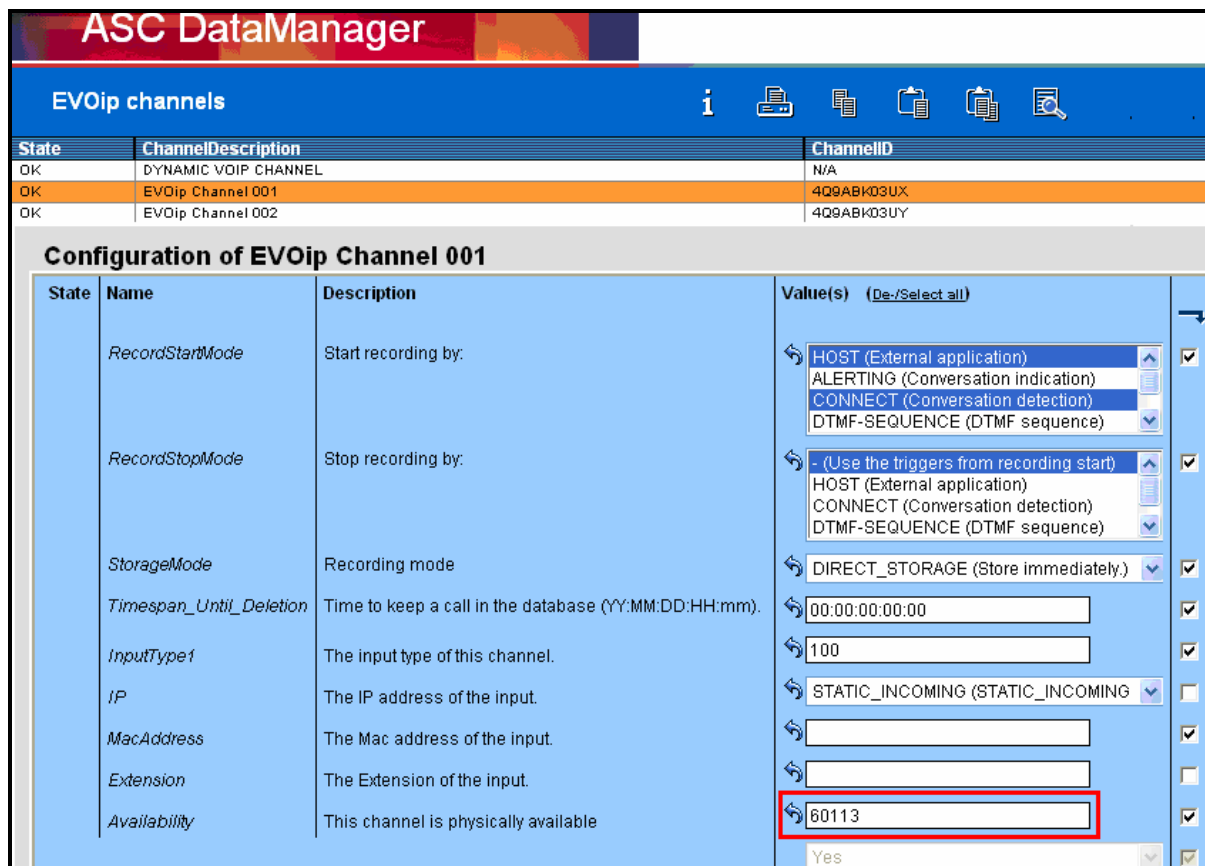
**Figure 55: DataManager EVOip Calldata Screen**

Select the EVOip channels menu point from the main menu.



**Figure 56: DataManager Channels Screen**

Configure each of the allocated channels as shown in the screen below. Repeat this for the other extensions in **Table 1** which are to be monitored by channels 2 and 3.

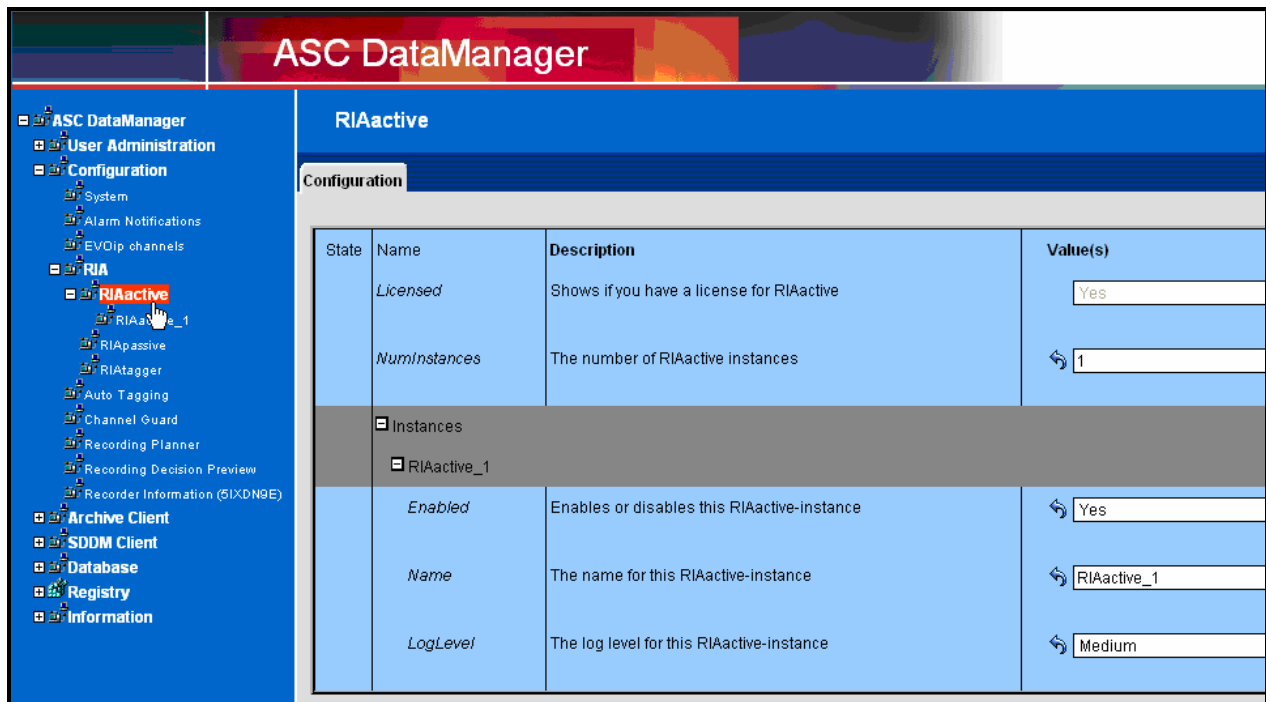


**Figure 57: EVOip Channel Configuration Screen**

Select “Configuration” -> “RIA” -> “RIAActive” from the left frame, and enter the parameters shown in the following table.

Parameter	Usage
NumInstances	Enter “1”.
Enabled	Set this parameter to “Yes”.
Name	Accept the default name.
LogLevel	Accept the default log level of “Medium”.

**Table 27: DataManager RIAActive Parameters**



**Figure 58: DataManager RIAActive Screen**

Select “Configuration” -> “RIA” -> “RIAactive” -> “RIAactive \_1” from the left frame, and enter the parameters shown in the following table.

Parameter	Usage
Statemachine	Enter “RIAServer”.
EventBuffer	Enter “1000 Events”.
PIF-Type	Enter “PIFAvayaCM”.
Connection-Type	Enter “TCP”.
Server-IP	Enter the address assigned to the <u>RIAactive</u> server.
Server-Port	Enter the port number assigned in <b>Figure 65</b> .
Inactivity-Timeout	Enter “60”.
LogBinaryData	Enter “No”.

**Table 28: DataManager RIAactive\_1 Parameters**

The screenshot shows the 'ASC DataManager' interface. On the left, a tree view lists various configuration categories, with 'RIAActive' expanded and 'RIAactive\_1' selected. The main window displays the 'RIAactive\_1' configuration page, which is divided into 'Protocol-Interface' and 'Devices' tabs. The 'Protocol-Interface' tab is active, showing a table of parameters for the 'RIAactive\_1' connection. The table has four columns: 'State', 'Name', 'Description', and 'Value(s)'. The parameters listed are: 'Statemachine' (Value: RIAServer), 'EventBuffer' (Value: 1000 Events), 'PIF-Type' (Value: PIFAvayaCM), 'Connection-Type' (Value: TCP), 'Server-IP' (Value: 192.168.200.110), 'Server-Port' (Value: 9000), 'Inactivity-Timeout' (Value: 60), and 'LogBinaryData' (Value: No).

State	Name	Description	Value(s)
	Statemachine	The statemachine grammar to use for this RIAactive-Connection	RIAServer
	EventBuffer	The buffer size for events.	1000 Events
	PIF-Type	The protocol interface adapter to use for this RIAactive-Connection	PIFAvayaCM
PIF-Config			
Connection			
	Connection-Type	The connection type to use.	TCP
	Server-IP	The ip address to connect to.	192.168.200.110
	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.	60
	LogBinaryData	Log the incoming binary data	No

**Figure 59: DataManager RIAactive\_1 Protocol Interface Screen**

Select “Configuration” -> “RIA” -> “RIAActive” -> “RIAActive\_1” from the left frame, select the “Devices” tab, and set the “PhysicalPbxID” for “EVOip Channel 001” through “EVOip Channel 003” to “active”.

**ASC DataManager**

**RIAActive\_1**

Protocol-Interface **Devices**

State	Name	Description	Value(s)
DeviceMap			
Import from CSV		Export to CSV	
PhonelineID	PhysicalPbxID	PhysicalDeviceID	
EVOip Channel 001	active	1	
Stereo EVOip Channel 001			
EVOip Channel 002	active	2	
Stereo EVOip Channel 002			
EVOip Channel 003	active	3	
Stereo EVOip Channel 003			

**Figure 60: DataManager RIAActive\_1 Devices Screen**

### 3.5. Configure Marathon RIAactive

Install the RIAactive software from the distribution medium, and reboot the system. Access the RIAactive server via web browser either from the local system, or remotely and log in with the appropriate user name and password.



**Figure 61: RIAactive Login Screen**



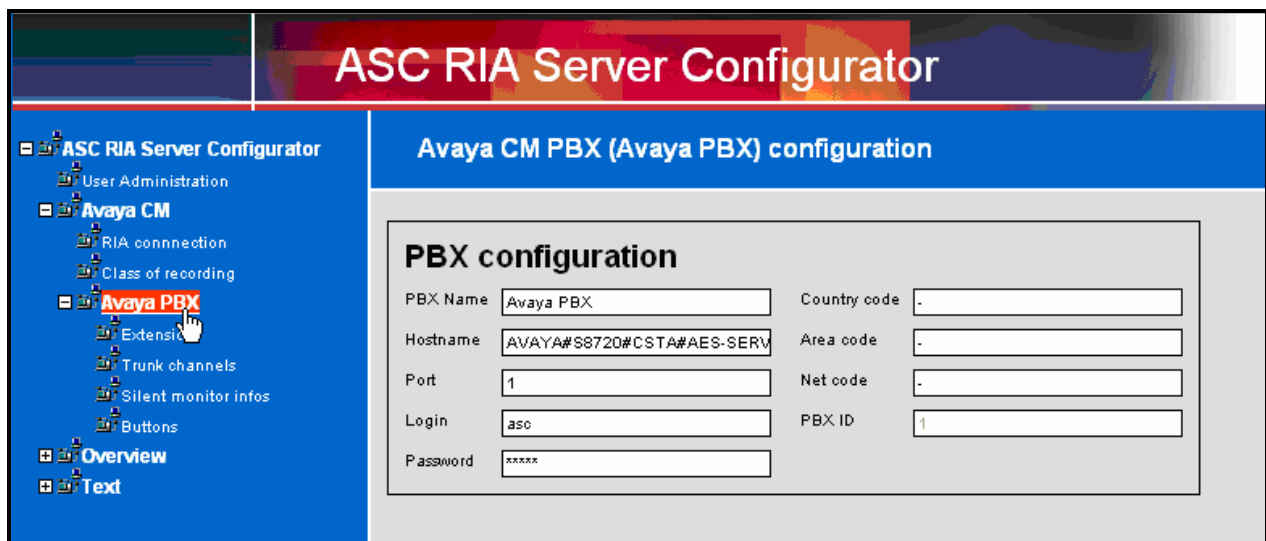
Select “Avaya CM” -> “Avaya PBX” from the left frame of the screen, and enter the parameters shown in the following table.

Parameter	Usage
PBX Name	Enter a name for identification purposes.
Hostname	Enter the name allocated to Communication Manager by AES, which is composed of the four text strings in <b>Table 30</b> , which are separated from another with a “#” character.
Port	Enter “1”.
Login	Enter the user name assigned by AES in <b>Figure 31</b> .
Password	Enter the password name assigned by AES in <b>Figure 31</b> .

**Table 29: RIAactive PBX Parameters**

Strings	Usage
AVAYA	This is a fixed value.
S8720	This is the name that was assigned to the Switch Connection, which was assigned on the Avaya AES Administration -> Switch Connections screen (see <b>Figure 26</b> ).
CSTA	This is a fixed value.
AES-SERVER1	This is the name that was assigned to the Avaya AES server when the Avaya AES software installation was performed.

**Table 30: Composition of the “hostname” Parameter**



**Figure 62: RIAactive PBX Configuration Screen**

For each of the extensions to be monitored, Select “Avaya CM” -> “Avaya PBX” -> “Extensions” from the left frame of the screen, and enter the parameters shown in the following table.

Parameter	Usage
Extension type	Select “Extension”.
Language	Select the language used by the user of the extension.
Class of recording	Select “Standard class of recording”.
ExtensionNumber	Leave the default extension set to the default value.
Monitorpoint enabled	Set this parameter to “yes”.

**Table 31: RIAactive PBX Parameters**

**ASC RIA Server Configurator**

**Extension (Avaya PBX) configuration**

Extension number	pbx	Monitor
60007	Avaya PBX	Yes
60113	Avaya PBX	Yes
60171	Avaya PBX	Yes

**Details**

**Extension configuration**

PBX ID: 1

Extension type: Extension

Language: en\_US

Class of recording: Standard class of recording for .

ExtensionNumber: 60007

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: 1990-01-01 00:00 to 1990-01-01 00:00

**Figure 63: RIAactive Extension Configuration Screen**

For each of the extensions to be monitored, Select “Avaya CM” -> “Avaya PBX” -> “Silent monitor infos” from the left frame of the screen, and enter the parameters shown in the following table.

**ASC RIA Server Configurator**

**Silent monitor infos (Avaya PBX) configuration**

Silent monitor ID	Silent monitor name
1	61401
2	61402
3	61403

**Details**

**Silent monitor infos configuration**

Recording channel ID:

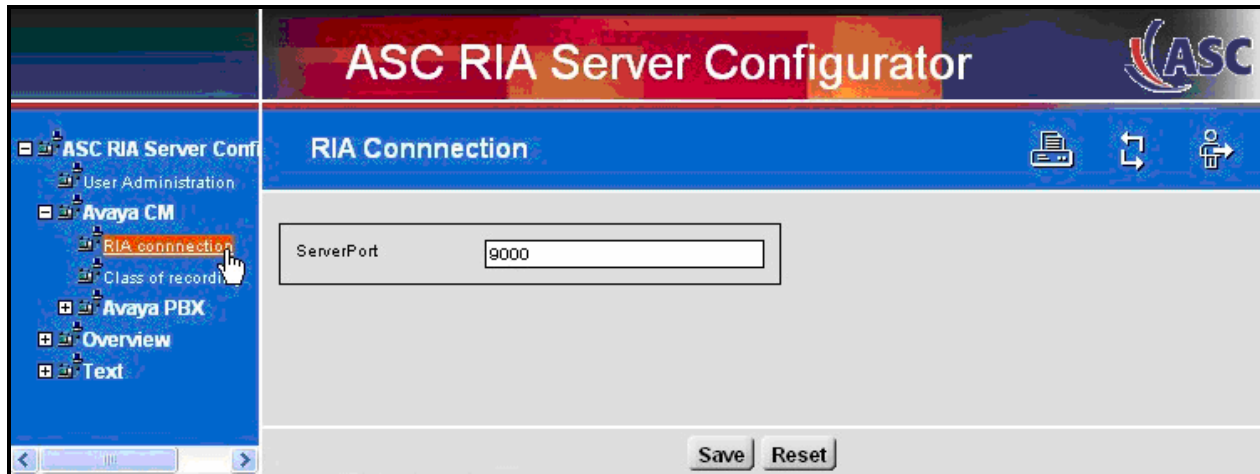
Class of channel:

Note:

Number:

**Figure 64: RIAactive Silent Monitor Configuration Screen**

Select “Avaya CM” -> “RIA connect” from the left frame of the screen, and set the ServerPort to an otherwise unused value. This must be the same value set in **Figure 59**.



**Figure 65: RIAactive Server Port Screen**

## 4. Interoperability Compliance Testing

The objective of the compliance testing done on the ASC telecom MARATHON EVOLUTION product was to verify that it is compatible with Avaya Communication Manager. This includes verifying that the essential MARATHON EVOLUTION features function properly when used with Avaya Communication Manager, and that Avaya Communication Manager features are not hindered by the interaction with MARATHON EVOLUTION. Furthermore, MARATHON EVOLUTION's robustness was verified.

### 4.1. General Test Approach

The test method employed can be described as follows:

- Avaya Communication Manager was configured to support various local IP telephones, as well as a networked PBX connection and a PSTN connection.
- A simulated PSTN interface was attached to Avaya Communication Manager, equipped with telephones that were used to simulate external callers.
- The MARATHON EVOLUTION was configured to monitor various telephones and trunks attached to Avaya Communication Manager.
- The major MARATHON EVOLUTION features and functions were verified using the above-mentioned local and external telephones, including the ability to monitor
  - Locally attached IP and digital telephones
  - Telephones attached to the PSTN
  - Telephones attached to a networked PBX
- The following MARATHON EVOLUTION methods were verified in these tests:
  - Single step conferencing
- The following test scenarios were used to test the various MARATHON EVOLUTION features:
  - Basic call
  - Hold/retrieve
  - Transfer
  - Blind transfer
  - Conferencing
  - Hunt group calls
- MARATHON EVOLUTION's robustness was tested by verifying its ability to recover from interruptions to its external connections including:
  - The LAN connection between and the MARATHON EVOLUTION and the network
  - The LAN connection between and the ASC RIAactive and 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 ASC CTI Controller
  - The Avaya Communication Server to which the MARATHON EVOLUTION is attached.

All testing was performed manually. The tests were all functional in nature, and no performance testing was done.

## **4.2. Test Results**

All tests which were performed produced the expected result.

## **5. Verification Steps**

The following steps can be performed to verify the correct installation and configuration of MARATHON EVOLUTION:

- Verify that the Avaya AES and MARATHON EVOLUTION systems can ping each other.
- Verify that the various telephones can call each other.
- Log into the Avaya AES as described in Section 3.2 and perform the following:
  - Verify that CTI OAM Status and Control “Switch Connection Summary” shows that the connection between Avaya AES and Avaya Communication Manager is operational.
  - Verify that CTI OAM Status and Control “Services Summary” shows that TSAPI service is operational.

## **6. Support**

Support for 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](mailto:hq@asctelecom.com)  
<http://www.asctelecom.com>

## 7. References

- [1] *Administrator Guide for Avaya Communication Manager*, January 2008, Issue 4.0, Document Number 03-300509.
- [2] *Feature Description and Implementation for Avaya Communication Manager*, January 2008, Issue 6, Document Number 555-245-205.
- [3] *Installing and Administering SIP Enablement Services*, January 2008, Issue 5.0, Document Number 03-600768.
- [4] *SIP Enablement Services (SES) Implementation Guide*, January 2008, Issue 5, Document Number 16-300140.
- [5] *4600 Series IP Telephone LAN Administrator Guide*, October 2007, Issue 7, Document Number 555-233-507.
- [6] ASC telecom product descriptions: [http://www.asctelecom.com/english/index\\_e.html](http://www.asctelecom.com/english/index_e.html)
- [7] “RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals”, May 2000, RFC 2833, available at <http://www.ietf.org/rfc.html>

## 8. Conclusion

These Application Notes describe the conformance testing of the ASC telecom MARATHON EVOLUTION voice recorder with Avaya Communication Manager. Silent monitoring via the single step conferencing 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.

## 9. Change History

Issue	Date	Reason
1.1	8/15/2008	Remove unrequired license entries from <b>Table 3</b> and <b>Figure 3</b> . Change Security Code description in <b>Table 11</b> .
1.0	8/8/2008	Initial issue

---

**©2008 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).