



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

---

# **Application Notes for ASC telecom MARATHON EVOLUTION Voice Recorder with Avaya Communication Manager Using Service Observing – Issue 1.0**

### **Abstract**

These Application Notes describe the conformance testing of the ASC telecom MARATHON EVOLUTION voice recorder with Avaya Communication Manager using the Service Observing 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.

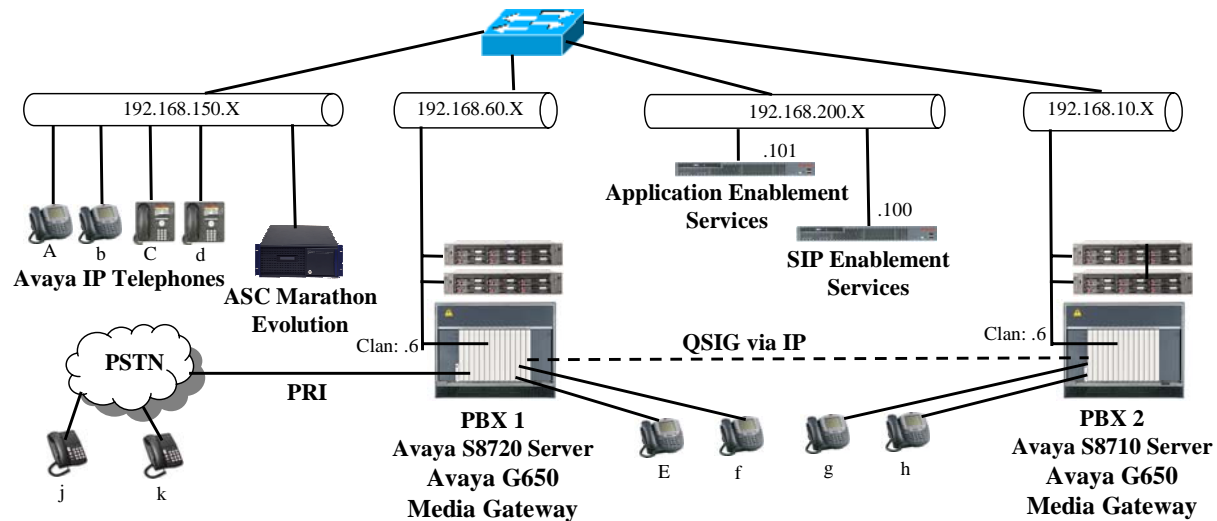
Information in these Application Notes has been obtained through compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

# Table of Contents

1.	Introduction.....	3
2.	Equipment and Software Validated .....	5
3.	Configuration .....	5
3.1.	Configure Avaya Communication Manager .....	5
3.1.1.	Verify system-parameters customer-options .....	6
3.1.2.	Verify system-parameters features .....	8
3.1.3.	Configure Dial Plan .....	8
3.1.4.	Configure IP Network Interface.....	9
3.1.5.	Configure Interface to AES .....	11
3.1.6.	Configure Stations .....	12
3.1.6.1	Configure Class of Service .....	12
3.1.6.2	Configure H.323 IP Stations .....	13
3.1.6.3	Configure SIP Stations.....	14
3.1.6.4	Configure Virtual CTI Stations.....	15
3.1.7.	Configure Hunt Group .....	17
3.1.8.	Configure Interface to SIP Enablement Services.....	18
3.2.	Configure Avaya AES .....	21
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
4.	Interoperability Compliance Testing .....	53
4.1.	General Test Approach .....	53
4.2.	Test Results .....	54
5.	Verification Steps.....	54
6.	Support.....	54
7.	References.....	55
8.	Conclusion .....	55

# 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, Avaya Application Enablement Services (AES), and Avaya SIP Enablement Services. 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 Service Observing feature was used.



**Figure 1: MARATHON EVOLUTION Test Configuration**

In the above diagram, the ASC MARATHON EVOLUTION records voice conversations from telephones attached to PBX 1. 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. The stations attached to PBX 2 are not monitored by ASC MARATHON EVOLUTION.

When a call is to be recorded, the MARATHON EVOLUTION voice recorder uses the Avaya Communication Manager Service Observing feature to monitor calls 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 telephone station which is to be monitored, as these are used by MARATHON EVOLUTION to initiate Service Observe operations.

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

**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.
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 IP Stations
IP_Phone (p.10)	This parameter must be set the number of IP stations plus 1 for each station which is to be monitored.

**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: 12000</b>		4
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. Verify system-parameters features

Use the **display system-parameters features** command to set system features as shown in the following table.

Parameter	Usage
Service Observing: Warning Tone? or Conference Tone?	Set both of these parameters to “n”.
Allow Two Observers in Same Call?	Set this parameter to “y”.

**Table 4: System-Parameters Features**

change system-parameters features	Page 11 of 17
FEATURE-RELATED SYSTEM PARAMETERS	
CALL CENTER SYSTEM PARAMETERS	
EAS	
Expert Agent Selection (EAS) Enabled? y	
Minimum Agent-LoginID Password Length: 5	
Direct Agent Announcement Extension:	Delay:
Message Waiting Lamp Indicates Status For: station	
VECTORIZING	
Converse First Data Delay: 0	Second Data Delay: 2
Converse Signaling Tone (msec): 100	Pause (msec): 30
Reverse Star/Pound Digit For Collect Step? n	
Store VDN Name in Station's Local Call Log? n	
SERVICE OBSERVING	
Service Observing: Warning Tone? n	or Conference Tone? n
Service Observing Allowed with Exclusion? y	
Allow Two Observers in Same Call? y	

**Figure 6: System-Parameters Features, p. 11**

### 3.1.3. 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 7: Dialplan Analysis Screen**



### 3.1.4. 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 5: 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 8: 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. This must be the same as is specified in <b>Figure 43</b> .
Name	Enter a name to identify the region.
Codec Set	Enter the number of the codec set defined in <b>Figure 10</b> .

**Table 6: 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 9: IP-Network-Region Form, p.1**

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 7: 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 10: IP-Codec-Set Form**

### 3.1.5. 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”. This must match the “MsgPort” specified in <b>Figure 55</b> .
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 28</b> .
Enabled (p.4)	Enter “y” to enable the connection.

**Table 8: 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 11: 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_server_1	XXXXXXXXXXXXXXXXXX	y	in use		

**Figure 12: 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 31**. 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 13: Cti-link Screen**

### 3.1.6. Configure Stations

#### 3.1.6.1 Configure Class of Restriction

Use the **change cor** command to configure Service Observing Class of Restriction parameters as required for Service Observe monitoring. For the purpose of the tests described by these application notes, a common Class of Restriction was shared by the stations being monitored (**Figure 15** and **Figure 16**) and the Virtual CTI Stations which were used for monitoring (**Figure 17**). In this case, both the “Can Be Service Observed” and “Can Be A Service Observer” parameters in the following screen must be set to “y”.

change cor 1	Page 1 of 23
CLASS OF RESTRICTION	
COR Number: 1	
COR Description:	
FRL: 0	APLT? y
Can Be Service Observed? y	Calling Party Restriction: none
Can Be A Service Observer? y	Called Party Restriction: none
Partitioned Group Number: 1	Forced Entry of Account Codes? n
Priority Queuing? n	Direct Agent Calling? n
Restriction Override: none	Facility Access Trunk Test? n
Restricted Call List? n	Can Change Coverage? n
Access to MCT? y	Fully Restricted Service? n
Group II Category For MFC: 7	Add/Remove Agent Skills? n
Send ANI for MFE? n	Automatic Charge Display? y
MF ANI Prefix:	PASTE (Display PBX Data on Phone)? n
Hear System Music on Hold? y	Can Be Picked Up By Directed Call Pickup? y
	Can Use Directed Call Pickup? y
	Group Controlled Restriction: inactive

**Figure 14: Class of Restriction Screen**

### 3.1.6.2 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.
Security Code	Enter an appropriate numeric string to be used as a security code.
COR	Enter the number of the Class of Restriction which was defined in <b>Figure 14</b> .

**Table 9: Configuration IP Stations**

change station 60113	Page 1 of 5
STATION	
Extension: 60113	Lock Messages? n
Type: 4610	Security Code: 31106
Port: S00101	Coverage Path 1: 1
Name: extn 60113	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: 60113
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 15: IP Station Screen**

### 3.1.6.3 Configure SIP Stations

Use the **add station** command to create SIP IP station for extension 60171, using the values shown below. Repeat this 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.
COR	Enter the number of the Class of Restriction which was defined in <b>Figure 14</b> .

**Table 10: Configuration SIP IP Stations**

change station 60171	Page 1 of 6
STATION	
Extension: 60171	Lock Messages? n
<b>Type: 9620</b>	Security Code:
Port: S00126	Coverage Path 1:
<b>Name: extn 60171</b>	Coverage Path 2:
	Hunt-to Station:
	BCC: 0
	TN: 1
	<b>COR: 1</b>
	COS: 1
STATION OPTIONS	
	Time of Day Lock Table:
Loss Group: 19	Personalized Ringing Pattern: 1
	Message Lamp Ext: 60171
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 16: SIP IP Stations Screen**

### 3.1.6.4 Configure Virtual CTI Stations

Use the **add station** command to create a station for each of the Virtual CTI Stations listed in **Table 1**. A separate Virtual CTI Station is required for each station to be monitored. These stations are subsequently assigned by the ASC DataManager for monitoring in **Figure 54**. Note that the station numbers must be sequential.

Parameter	Usage
Type (p. 1)	Enter “4620”.
Name (p. 1)	Any alphanumeric string can be assigned as an extension name.
Security Code (p. 1)	Enter a security code which is the same as the extension number.
IP Softphone (p. 1)	Enter “y”.
COR	Enter the number of the Class of Restriction which was defined in <b>Figure 14</b> .
BUTTON ASSIGNMENTS (p. 4)	Create a “serv-obsrv” button to be used to my MARATHON EVOLUTION to initiate monitoring operations.

**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:	<b>COR: 1</b>
<b>Name: CTI 61401</b>	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: 61401	
Speakerphone: 2-way	Mute Button Enabled? y	
Display Language: english	Expansion Module? n	
Survivable GK Node Name:		
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, p. 1**

add station 61401		Page 4 of 5	
STATION			
SITE DATA			
Room:		Headset?	n
Jack:		Speaker?	n
Cable:		Mounting:	d
Floor:		Cord Length:	0
Building:		Set Color:	
ABBREVIATED DIALING			
List1:	List2:	List3:	
BUTTON ASSIGNMENTS			
1: call-appr	5:		
2: call-appr	6:		
3: call-appr	7:		
4: serv-obsrv	8:		

**Figure 18: Virtual CTI Station Screen, p. 4**



### 3.1.7. 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 19: 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 20: Hunt Group Screen, p. 3**

### 3.1.8. Configure Interface to SIP Enablement Services

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

Parameter	Usage
Group Type	Enter “sip”.
Near-end Node Name	Enter “clan” (defined in <b>Figure 8</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 Network Region: 1	
Far-end Domain:		
	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 21: 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 7</b> .
Service Type (p.1)	Enter “tie”.
Signaling Group (p.1)	Enter the number of the signaling group allocated in <b>Figure 21</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 22: 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 16</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 is allocated in <b>Figure 22</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 23: 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		

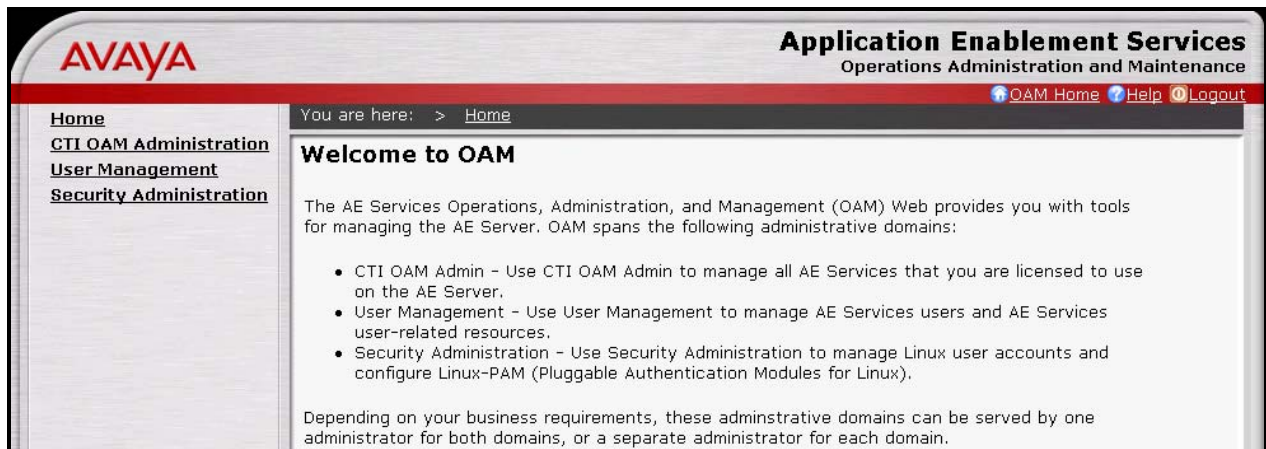
**Figure 24: off-pbx-telephone station-mapping Screen, p. 2**

## 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 25: 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

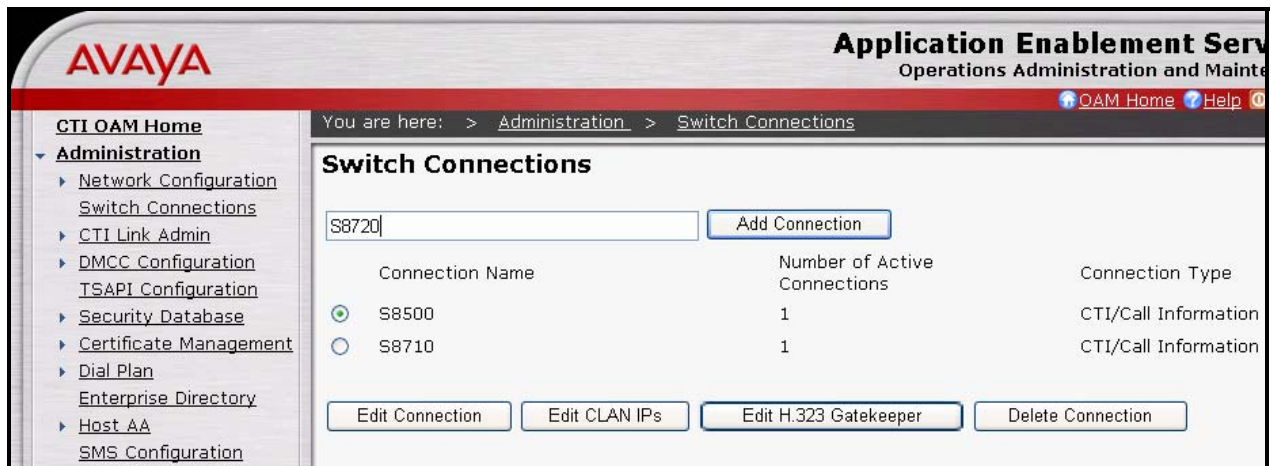
You are licensed to run Application Enablement (CTI) version 4.1.

You are licensed for the following services

- DLG
- CVLAN
- TSAPI
- SMS

**Figure 26: 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 52**.



**Figure 27: 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 12</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**

The screenshot shows the Avaya Application Engine Operations Administration interface. The left sidebar contains a navigation menu with categories like CTI OAM Home, Administration, Status and Control, Maintenance, Alarms, Logs, Utilities, and Help. The main content area is titled 'Set Password - S8720' and includes a breadcrumb trail: 'You are here: > Administration > Switch Connections'. Below the title, there are instructions: 'Please note the following: \* A password is not required for a H323 Gatekeeper Connection. \* Changing the password affects only new connections, not open connections.' The form contains four fields: 'Switch Connection Type' (a dropdown menu set to 'CTI/Call Information'), 'Switch Password' (a text box with 12 dots), 'Confirm Switch Password' (a text box with 12 dots), and 'SSL' (a checked checkbox). At the bottom of the form are 'Apply' and 'Cancel' buttons.

**Figure 28: Set Switch Password Screen**

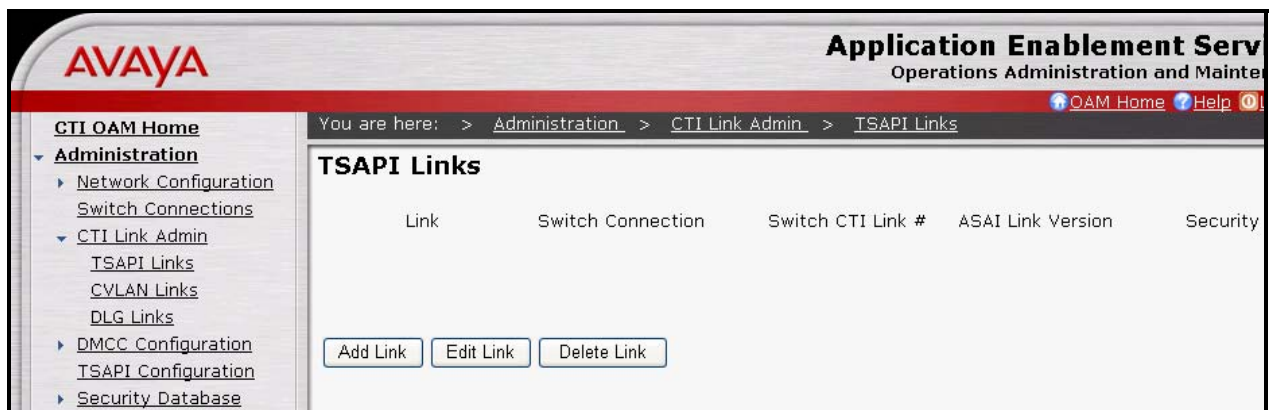


From the **Administration->Switch Connections** screen, click the “Edit CLAN IPs” button to display the screen show below. Enter the IP address of the CLAN with which AES is to use for communication with the switch, and click the “Add Name or IP” button.



**Figure 29: 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 30: 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 13**. Click the “Apply Changes” button.

**AVAYA** **Application Operations**

**CTI OAM Home**

- Administration
  - Network Configuration
  - Switch Connections
  - CTI Link Admin
    - TSAPI Links**
    - CVLAN Links
    - DLG Links
  - DMCC Configuration
  - TSAPI Configuration
  - Security Database
  - Certificate Management

You are here: > Administration > CTI Link Admin > TSAPI Links

### Add / Edit TSAPI Links

Link: 1

Switch Connection: S8720

Switch CTI Link Number: 4

ASAI Link Version: 1

Security: Unencrypted

**Figure 31: 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 EVOLUTION 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 53**.

The screenshot displays the Avaya Application Operations interface. The top header features the Avaya logo and the text 'Application Operations'. A breadcrumb trail indicates the current location: 'You are here: > User Management > Add User'. The left sidebar contains a 'User Management Home' section with links for 'List All Users', 'Add User', 'Search Users', 'Modify Default User', and 'Change User Password'. Below this are links for 'Service Management' and 'Help'. The main content area is titled 'Add User' and includes a note: 'Fields marked with \* can not be empty.' The form contains the following fields: '\* User Id' (text input with value 'asc'), '\* Common Name' (text input with value 'asc'), '\* Surname' (text input with value 'Marathon'), '\* User Password' (password input with masked characters), '\* Confirm Password' (password input with masked characters), 'Admin Note' (text input), 'Avaya Role' (dropdown menu with value 'userservice.useradmin'), 'Business Category' (text input), 'Car License' (text input), 'CM Home' (text input), 'Css Home' (text input), and 'CT User' (checkbox with value 'Yes').

**Figure 32: 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 Operations Administration interface. The top header shows the Avaya logo and the title 'Application Enablement Operations Administration'. A breadcrumb trail indicates the current location: 'You are here: > Administration > Security Database > CTI Users > List All Users'. The left sidebar contains a navigation menu with categories like 'Administration', 'Security Database', and 'CTI Users'. The main content area is titled 'Edit CTI User' and shows configuration details for a user named 'asc'. The 'Unrestricted Access' checkbox is checked, and the 'Apply Changes' button is highlighted with a red box. Other fields include 'User ID', 'Common Name', 'Worktop Name', 'Call Origination and Termination', 'Device / Device', 'Call / Device', 'Call / Call', and 'Allow Routing on Listed Device'.

User ID	asc
Common Name	asc
Worktop Name	NONE
Unrestricted Access	<input checked="" type="checkbox"/>
Call Origination and Termination	None
Device / Device	None
Call / Device	None
Call / Call	<input type="checkbox"/>
Allow Routing on Listed Device	None

**Figure 33: Edit CTI 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 53</b> .
Encrypted Port	Set this port to 4722, enabled to match the value in <b>Figure 53</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

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 34: 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 35: Launch Maintenance Web Interface Screen**

### 3.3.1. Install License

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

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 address "192.168.200.100". A navigation menu on the left lists various options, with "License" under the "Top" section highlighted by a red circle. The main content area displays a list of management tasks under the "Top" heading.

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 36: Select License from Top SES Screen**

Click “Access WebLM”.

The screenshot shows a web interface with a blue sidebar on the left and a main content area on the right. The sidebar contains a 'Top' section with links like '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'. Under 'Server Configuration', there are links for 'Admin Setup', 'IM Log Settings', and 'License'. The main content area is titled 'List Licenses' and features a table with three columns: 'Proxy Name', 'Name', and 'Message'. The table contains three rows of data. Below the table, the text 'Access WebLM' is circled in red.

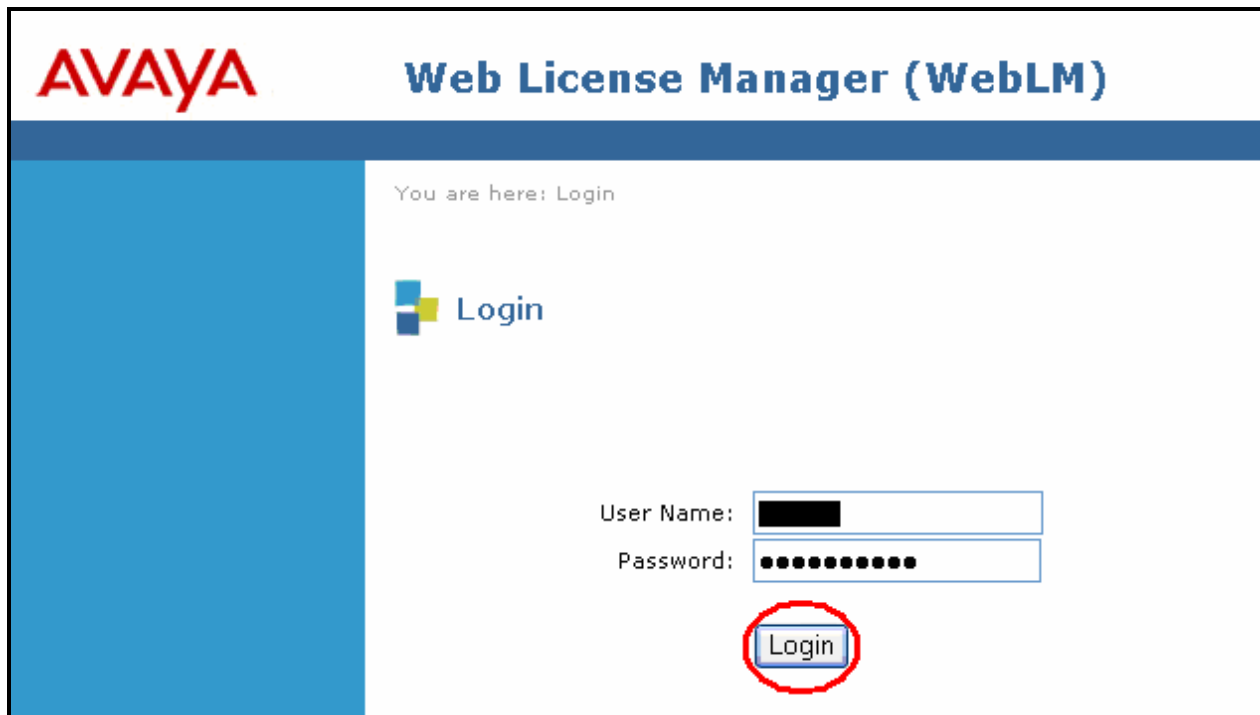
	<u>Proxy Name</u>	<u>Name</u>	<u>Message</u>
<a href="#">Show</a>	sipserver	Basic Proxy	
<a href="#">Show</a>	sipserver	Edge Proxy	
<a href="#">Show</a>	sipserver	Home Seats	

**Access WebLM**

**Figure 37: 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. This button is circled with a red hand-drawn circle.

**Figure 38: 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 39: Initiate “Setup” from Top SES Configuration Screen**

### 3.3.2. Setup Dataservice

Click “Setup Dataservice”.



**Figure 40: 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.

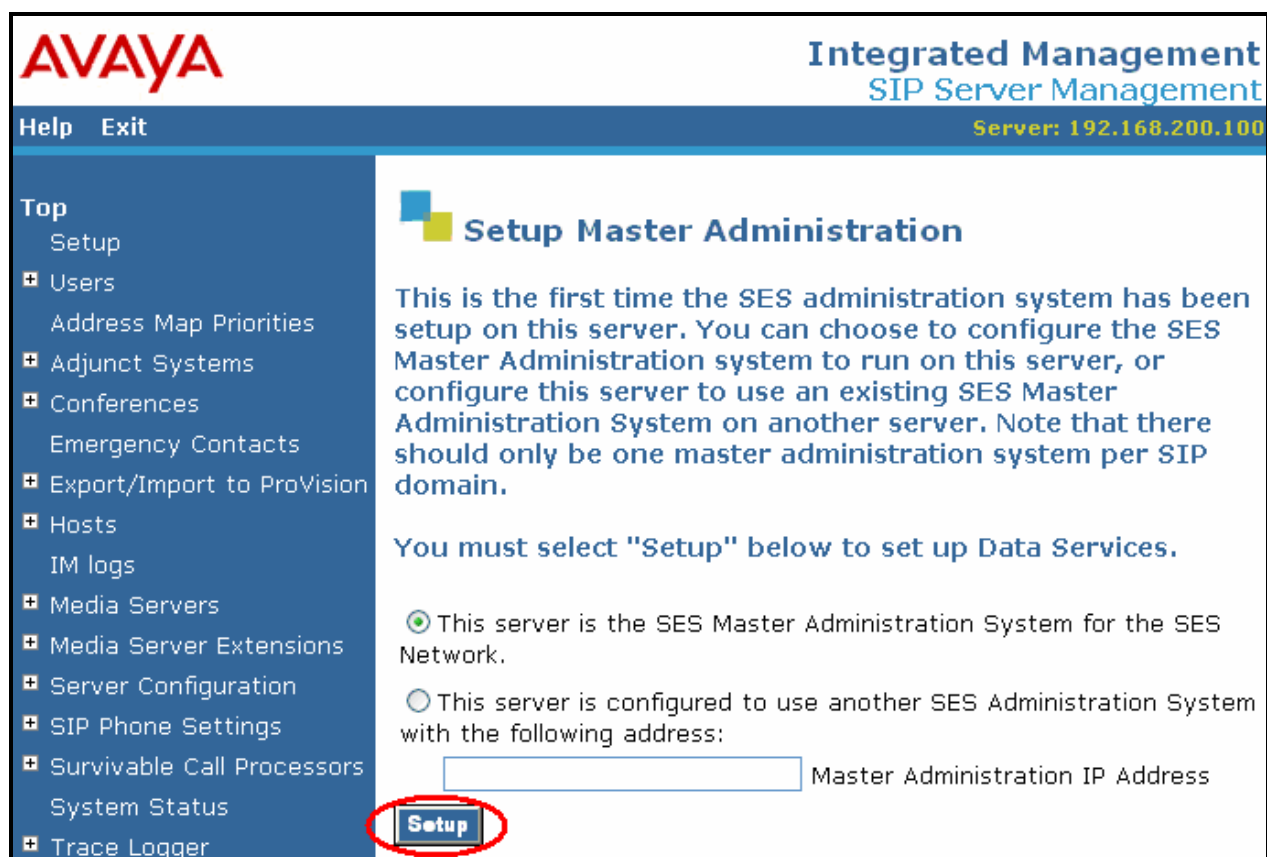


Figure 41: “Setup Master Administration” Screen

### 3.3.3. Setup SIP Domain

Click “Setup SIP domain”.



Figure 42: “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 9</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 43: System Properties Screen**

### 3.3.4. Add Media Server Interface

Navigate to **Media Servers → Add** from the “Top” level menu shown in **Figure 36**, 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 displays the Avaya Integrated Management SIP Server Management interface. The top header shows the Avaya logo and the title 'Integrated Management SIP Server Management' with the server IP '192.168.200.100'. The 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 (highlighted), 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\***: S8720
- Host**: 192.168.200.100
- SIP Trunk Link Type**: TCP (selected), TLS
- SIP Trunk IP Address\***: 192.168.60.6
- Media Server Admin Address (see Help)**: 192.168.60.100
- Media Server Admin Port**: 5023
- Media Server Admin Login**: [Redacted]
- Media Server Admin Password**: [Redacted]
- Media Server Admin Password Confirm**: [Redacted]

**Figure 44: SES Add Media Server Interface Screen**

### 3.3.5. Add Hosts

Navigate to **Hosts** → **Add Host** from the top level screen shown in **Figure 36**. 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**

**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
  - List
  - Migrate Home/Edge
  - IM logs
- Media Servers
- Media Server Extensions
- Server Configuration
- SIP Phone Settings
- Survivable Call Processors
- System Status
- Trace Logger
- Trusted Hosts

**Add Host**

Host IP Address\* 192.168.200.100

Profile Service Password\* .....

Host Type SES combined home-edge

Parent none

Listen Protocols ☒ UDP ☒ TCP ☒ TLS

Link Protocols ☐ UDP ☐ TCP ☒ TLS

Access Control Policy (Default) ☒ Allow All ☐ Deny All

Emergency Contacts Policy ☒ Allow ☐ Deny

Minimum Registration (seconds) 300 Registration Expiration Timer (seconds)\* 86400

Line Reservation Timer (seconds) 30

\* Outbound Routing Allowed ☒ Internal ☒ External From

**Figure 45: 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 46: 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 each extension which is added must have a corresponding. Note that the extensions must match those which were allocated to the stations added in **Figure 16**.

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

Help Exit

Top  
Users  
Add  
Default Profile  
Delete  
Edit  
List  
Password  
Search  
Manage All Registered

### Add Media Server Extension

Add Media Server extension for user 60171

Extension

Media Server

Fields marked \* are required.

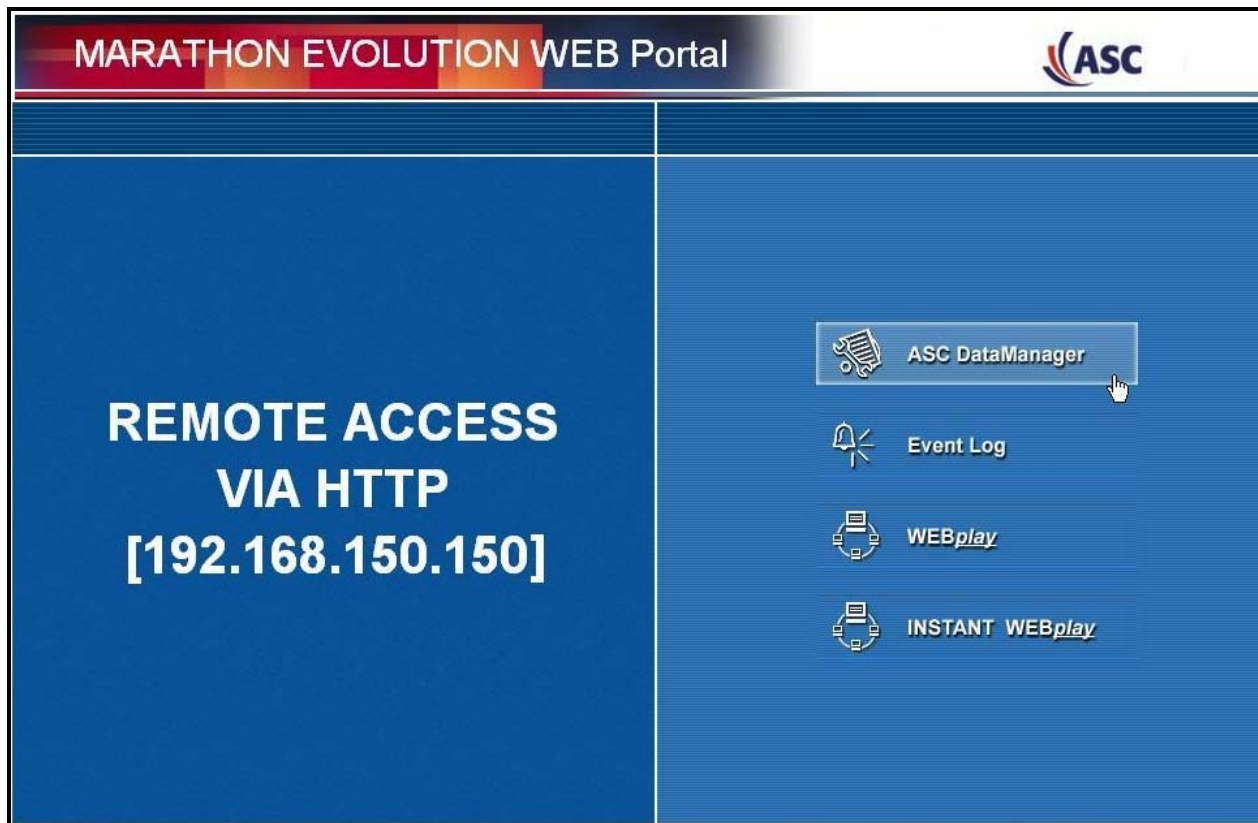
**Add**

**Figure 47: 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.



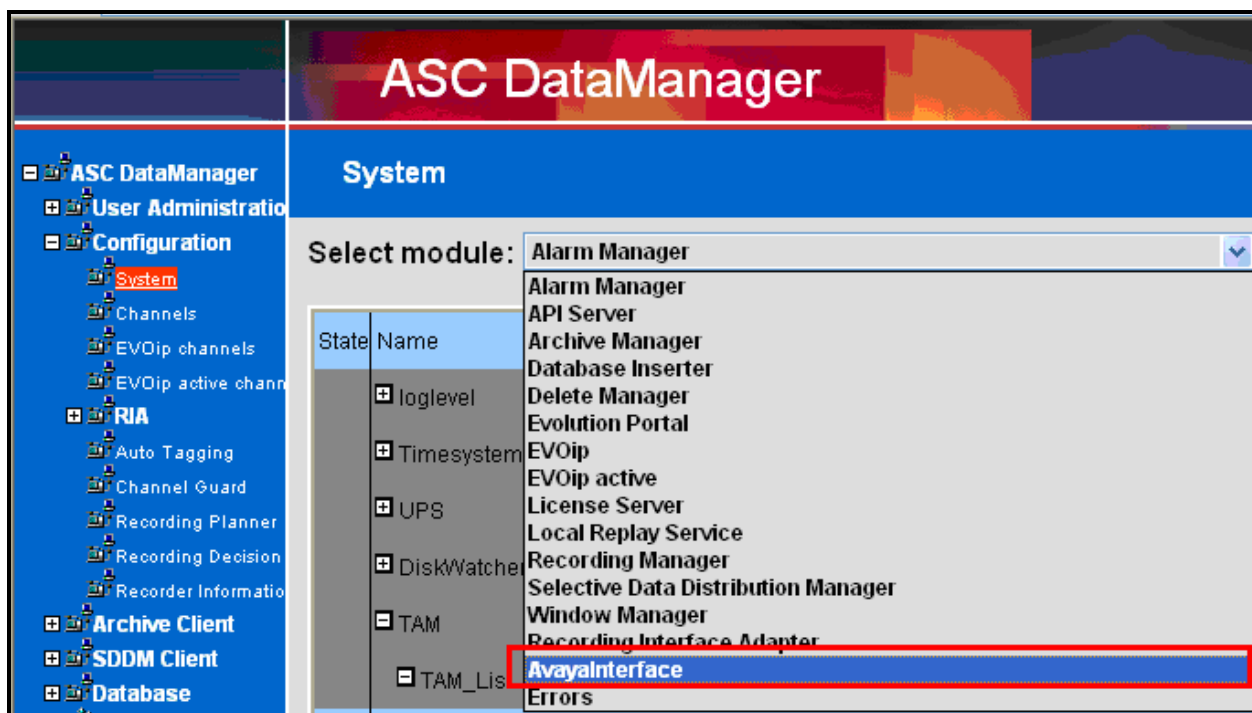
**Figure 48: MARATHON EVOLUTION Welcome Screen**

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



**Figure 49: DataManager Welcome Screen**

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



**Figure 50: 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 “No” for Service Observe operation.

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

State	Name	Description	Value(s)
	Activate	Activate Avaya Interface	Yes
	OperationMode		
	CTI	CTI mode	No

**Figure 51: 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 8</b> .
Name	Enter the name which was assigned to the switch connection in <b>Figure 27</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 52: 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 34</b> .
PortUnencrypted	Enter the same value which is specified in <b>Figure 34</b> .
Secure	Enter “No”.
User	Enter the same value which is specified in <b>Figure 32</b> .
Password	Enter the same value which is specified in <b>Figure 32</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 53: 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**

**ASC DataManager**

**System**

Select module: **AvayaInterface**

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 54: 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.
MsgPort	Retain the default value of “8765”. This must match the value of the “Local Port” parameter in <b>Figure 11</b> .
ReconnectDelay	Enter “15”.

**Table 26: DataManager Recorder Parameters**

**ASC DataManager**

**System**

Select module: **AvayaInterface**

State	Name	Description	Value(s)
	Activate	Activate Avaya Interface	Yes
	<div> <div>+</div> <div>OperationMode</div> </div> <div> <div>+</div> <div>CommunicationManager</div> </div> <div> <div>+</div> <div>AESServer</div> </div> <div> <div>+</div> <div>Softphones</div> </div> <div> <div>-</div> <div>Recorder</div> </div>		
	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 55: DataManager Recorder Screen**

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

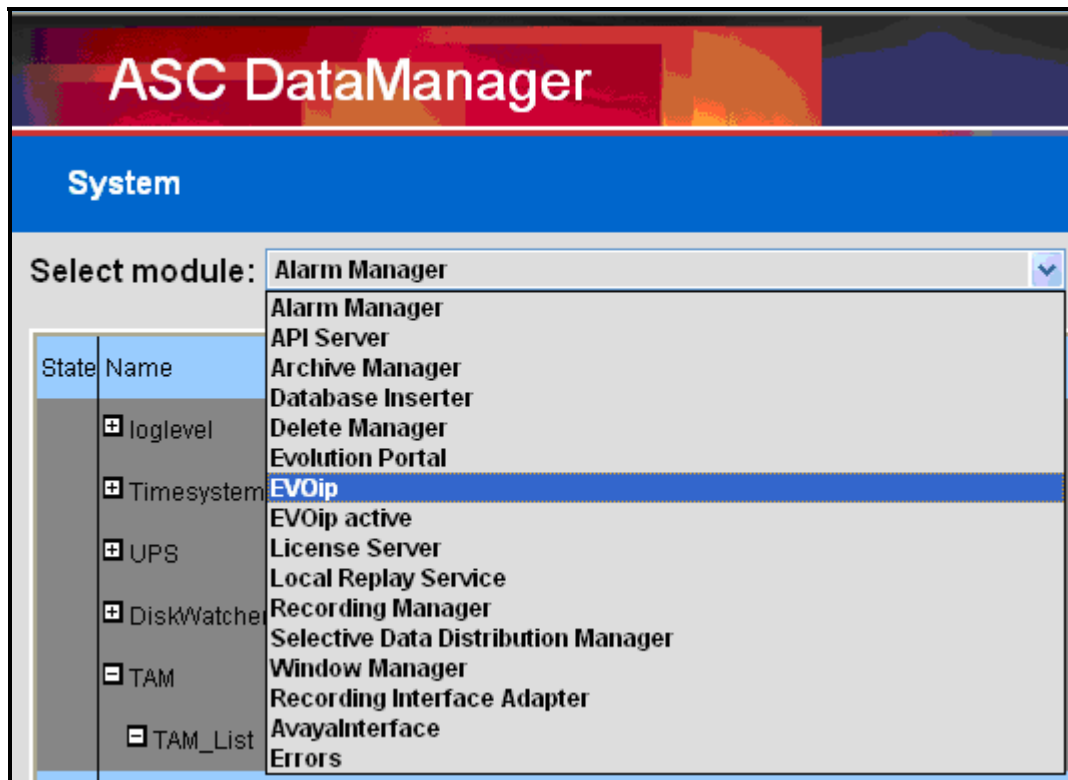


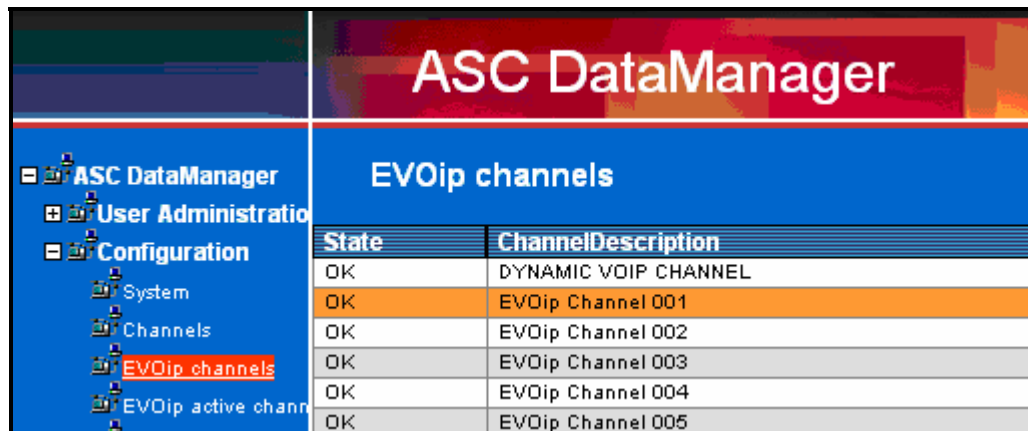
Figure 56: Select EVOip Screen

Set the “Calldata” “EnableCallTagging” parameter to “Yes” for Service Observe operation.

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

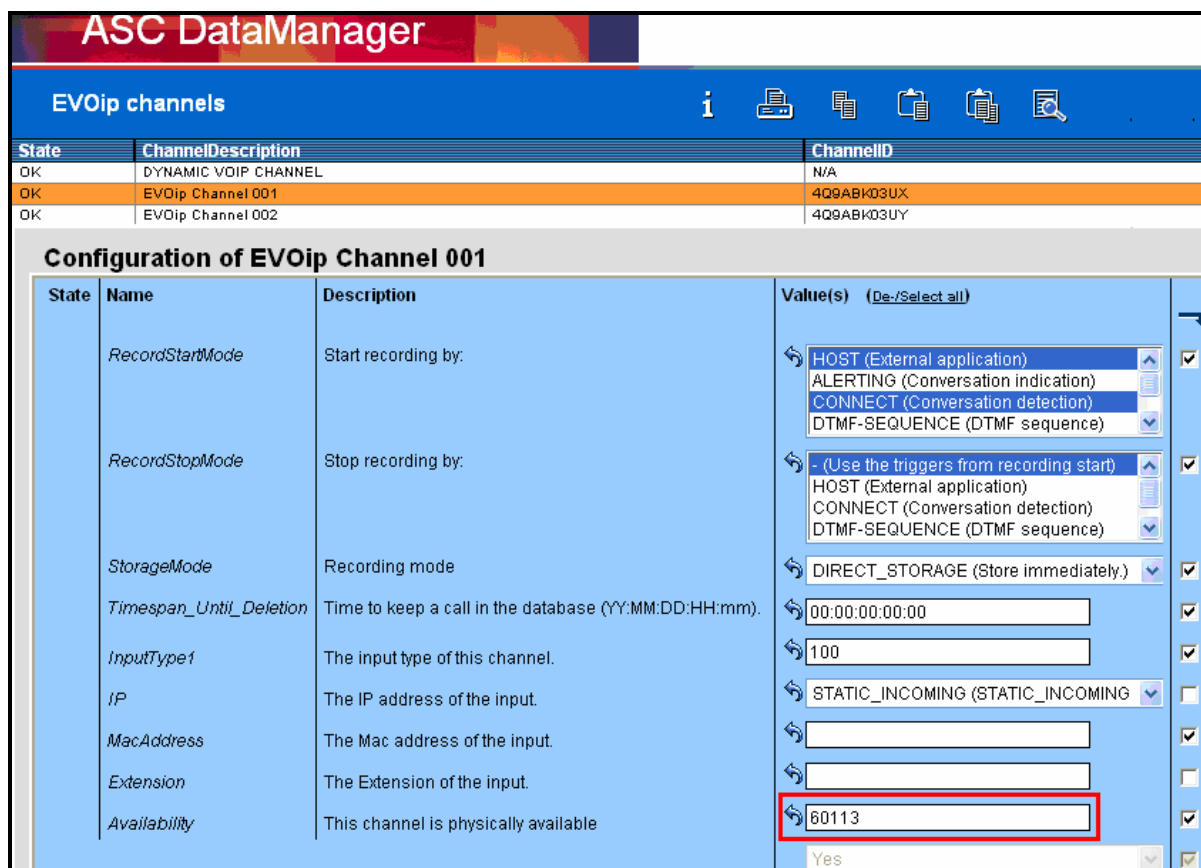
**Figure 57: DataManager EVOip Calldata Screen**

Select the “EVOip channels” menu point from the main menu.



**Figure 58: 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 59: EVOip Channel Configuration 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 PSTN interface was attached to Avaya Communication Manager, which was used to communicate with external telephones.
- 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:
  - Service Observe monitoring.
- 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 LAN connection between and the MARATHON EVOLUTION 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 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 Service Observe 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.

---

**©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).